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

	How to Use This Guide	3				
	Contents	4				
	LED Light Instructions	5				
	Connecting to the Web Interface	7				
	Logging on to the equipment					
	Quick Setup	10				
Section I	Wireless 5G	13				
	1. BASIC SETTING	31				
	2. ADVANCED	17				
	3. SECRITY	20				
	4. ACCESS CONTROL	26				
	5. WPS	29				
Section II	Wireless 2.4G	31				
	6. BASIC SETTING	31				
	7. ADVANCED	35				
	8. SECRITY	38				
	9. ACCESS CONTROL	44				
	10. WPS	47				
Section III	TCP/IP	49				
	11.LAN SETTING	49				
Section IV	MANAGEMENT	51				
	12. STATUS	51				
	13. STATISTICS	52				
	14. UPGRADE FIRMWARE	53				
	15. SAVE/RELOAD SETTING	54				
	16. PASSWORD	57				

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
<u> </u>		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 $192.168.1.2 \sim 192.168.1.254$, and then click **OK**, to return to the previous page, click **OK**.

Ethernet Properties	×	Internet Protocol Version 4 (TCP/IPv4)	Properties	×
Networking Sharing		General		
Connect using:		You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator	
Configure		Obtain an IP address automatical	у	
This connection uses the following items:	_	• Use the following IP address:		
☑ S Packet Scheduler ☑ Internet Protocol Version 4 (TCP/IPv4)	^	IP address:	192.168.1.2	
Image: Microsoft Network Adapter Multiplexor Protocol		Subnet mask:	255.255.255.0	
 Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6) 		Default gateway:		
 Link-Layer Topology Discovery Responder Link-Layer Topology Discovery Mapper I/O Driver 	~	Obtain DNS server address autom	natically	
< >>		• Use the following DNS server addr	resses:	
Install Uninstall Properties		Preferred DNS server:		
Description	- 1	Alternate DNS server:		
vide area network protocol/internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.		⊠Validate settings upon exit	Advanced	
OK Can	cel		OK Cance	!

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.

G	->	<i>e</i> 192	.168.1.1			,0 - →
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	F <u>a</u> vorites	<u>T</u> ools	<u>H</u> elp	

leve	lone		WRE-8011E AC120)0 Wireless Range Ext	ender	
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT	
WIZARD	Wireless Site Survey					
	WIZARD This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. Site Survey Next>>					

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

leve	lone	WRE	- 8011E AC1200 W	/ireless Range Exte	nder
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
WIZARD	Wireless	Site Survey			
	This page provides it manually when Site Survey	s tool to scan the wireless client mode is enabled.	network. If any Access Poir	nt or IBSS is found, you c	ould choose to connect

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.

Please wait Site survey now!	
Site Survey	Next>>

his page provides tool	to scan the wireless	network. If	any Ac	cess Point o	r IBSS is	found, you
uid choose to connec	t it manually when ci	ient mode is	s enabl	ea.		
Site Survey						
					<u> </u>	
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
LevelOne WAP-8122	00:11:6b:74:ca:3a	48 (A+N)	AP	WPA2-PSK	69	
5.8G						

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

Wireless Sit	e Survey
This page provides tool to could choose to connect	o scan the wireless network. If any Access Point or IBSS is found, you t manually when client mode is enabled.
Pre-Shared Key:	66666666

4. Please wait... 140 s

Wireless	Site Survey
This page provides could choose to cor	tool to scan the wireless network. If any Access Point or IBSS is found, you nect it manually when client mode is enabled.
Please wait	

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

WAP-8122							
Home		Static DHCP DHCP List				×	
_		SN	Name	IP Address	MAC Address	DHCP Lease Time	
		1	sherlock-MBP-2	192.168.1.56	00:0E:C1:B1:01:1A	0Day23H57M23S	
Wizard		2	•	192.168.1.204	94:46:96:13:95:20	0Day23H57M41S	
WIFI							
Network							
Security							
Manage							

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

•••	192.168.1.204/home.htm	× +				
← → C f	🟠 📑 192.168.1.204 -					
	I leve	lone		WRE-8011E AC1	1200 Wireless Range Ex	ender
	WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
	STATUS	Access Po	int Status			
	STATISTICS	This page shows the	current status and some b	asic settings of the		
	UPGRADE FIRMWARE					
	SAVE/RELOAD SETTING	APInfrastructure Clien System	ntAPInfrastructure Client			
	PASSWORD	Firmware Version Build Time	RE12B_v3411d_Lev Tue Sep 4 16:49:30	_005 CST 2018		
		Band	5 GHz (A+N+AC)			
		Channel Number	48	5.80_30_EXT		
		Virtual AP1 Config	uration			
		Band	5 GHz (A+N+AC)	1		
		Encryption	Disabled	1		
		BSSID	78:8c:54:10:a7:13			
		Associated Clients	; 0	Alon .		
		SSID	LevelOne WAP-8122	100n		
		Encryption	WPA2 Mixed	. 5100		
		BSSID	00:11:6b:74:ca:3a			
		State	Connected			
		Band	2.4 GHz (B+G+N)			
		SSID	LevelOne WAP-8122	5.8G_EXT		
		Channel Number	4			
		Wireless 2 4G Ren	WPAZ MIXED	ration		
		SSID	RTK 11n AP RPT1			
		Encryption	Disabled			
		BSSID	00:00:00:00:00:00			
		State	Scanning			
		Attain IP Protocol	DHCP			
		IP Address	192.168.1.204			
		Subnet Mask	255.255.255.0			
		MAC Address	94:46:96:13:95:20			
			5.1.10150125155120			



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.

leve	lone		WRE-8011E AC1200	Wireless Range Ex	ttender
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING 🚩	Wireles	s Basic Settings	s -5G		
ADVANCED	This page is use change wireless	d to configure the parameters fo encryption settings as well as w	r wireless LAN clients which m ireless network parameters.	ay connect to your Acce	ess Point. Here you may
SECURITY	Disable W	ireless LAN Interface	· · · ·		
ACCESS CONTROL	Band:	5 GHz (A+N+AC) 🗘			
WPS	Mode:	AP 🗘 Multi	pleAP		
	Network Type:	Infrastructure			
	SSID:	LevelOne WAP-8122 5.8G_5G	EXT Add to Pr	ofile	
	Channel Width:	80MHz 🕈			
	Control Sideband:	(Auto 🗘			
	Channel Number:	48 🗘			
	Broadcast SSID:	Enabled \$			
	WMM:	Enabled \$			
	Data Rate:	Auto 🗘			
	TX restrict:	0 Mbps (0:no restrict)			
	RX restrict:	0 Mbps (0:no restrict)			
	Clients:	Show Active Clients			
	 Enable U client simulta SSID of Extent 	niversal Repeater Mode (Act neouly) ded Interface:	ing as AP and Add to Pr	ofile	
	LevelOne WAP	8122 5.86			
	Enable W Wireless Profil	ireless Profile e List:			
	SSI	DE	ncrypt	Select	
	Delete Selected	DeleteAll			
	Save Save	& Apply Reset			

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
	5 GHz (AC) 5 GHz (N+AC) 5 GHz (A+N+AC)
Mode	Configure the Wireless LAN Interface to AP, Client, WDS, AP + WDS mode
	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
	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.
	20MHz 40MHz 80MHz
Control Sideband	Choose a Control Sideband from the pull-down menu.
Channel	Choose a Channel Number from the pull-down menu.
Number	Auto 36 40 44 48
Broadcast SSID	Broadcast or Hide SSID to your Network.

Figure 1: Wireless Network page

	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
	✓ Auto
	6M
	9M 12M
	12M
	24M
	36M
	48M
	54M MCS0
	MCS1
	MCS2
	MCS3
	MCS4
	MCS6
	MCS7
	MCS8
	MCS9
	MCS10
	MCS12
	MCS13
	MCS14
	MCS15
	NSS1-MCS0 NSS1-MCS1
	NSS1-MCS2
	NSS1-MCS3
	NSS1-MCS4
	NSS1-MCS5 NSS1-MCS6
	NSS1-MCSO
	NSS1-MCS8
	NSS1-MCS9
	NSS2-MCS0
	NSS2-MCS1 NSS2-MCS2
	NSS2-MCS3
	NSS2-MCS4
	NSS2-MCS5
	NSS2-MCS6 NSS2-MCS7
	NSS2-MCS8
	NSS2-MCS9
Associated	Show Active Wireless Client Table
Clients	
	This table shows the MAC address, transmission, receiption packet counters and encrypted
	status for each associated wireless client.
Enable Mac	Enable Mac Clone (Single Ethernet Client)
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).



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.

levelone			WRE-	8011E AC1200	Wireless Range Ex	tender
WLAN Access Point	SETUP	WIRELESS	5G WI	RELESS 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING	Wireless Ad	vanced	l Setting	s -5G		
ADVANCED 🕨	These settings are only for	or more techni	ically advanced us	ers who have a sufficie	ent knowledge about wi	reless LAN. These settings
SECURITY		liess you know	w what enect the o	changes will have on y	our Access Point.	
	Fragment Threshold:	2346	(256-2346)			
ACCESS CONTROL	RTS Threshold:	2347	(0-2347)			
WPS	Beacon Interval:	100	(20-1024 ms)			
	IAPP:	Enabled	O Disabled			
	Protection:	Enabled	Disabled			
	Aggregation:	Enabled	 Disabled 			
	Short GI:	Enabled	 Disabled 			
	WLAN Partition:	Enabled	Disabled			
	STBC:	Enabled	 Disabled 			
	LDPC:	Enabled	 Disabled 			
	TX Beamforming:	Enabled	 Disabled 			
	MU MIMO:	 Enabled 	Disabled			
	Mutilcast to Unicast:	Enabled	 Disabled 			
	TDLS Prohibited:	Enabled	Disabled			
	TDLS Channel Switch Prohibited:	Enabled	Disabled			
	RF Output Power:	100%	070% 050%	0 35% 0 15%		
	Save Save & Apply	Reset				

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.

	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



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:

levelone

WRE-8011E AC1200 Wireless Range Extender

	\sim						
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT		
BASIC SETTING	Wireless	Security Set	tup -5G				
ADVANCED	This page allows y unauthorized acce	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.					
SECURITY							
ACCESS CONTROL	Select SSID: Root AP - Repeater-139520_5G Save Save & Apply Reset						
WPS							
		WEP WPA2 WPA-Mixed					

WEP

Encryption:	WEP \$
802.1x Authentication:	
Authentication:	Open System OShared Key OAuto
Key Length:	64-bit 🛟
Key Format:	Hex (10 characters)
Encryption Key:	******

WPA2

Encryption:	(WPA2 \$
Authentication Mode:	Enterprise (RADIUS) • Personal (Pre-Shared Key)
WPA2 Cipher Suite:	TKIP 🗹 AES
Management Frame Protection:	conone ○capable ○required
Pre- Shared Key Format:	Passphrase 🛟
Pre-Shared Key:	

WPA-Mixed

Encryption:	WPA-Mixed \$
Authentication Mode:	Enterprise (RADIUS) OPersonal (Pre-Shared Key)
WPA Cipher Suite:	✓ TKIP ✓ AES
WPA2 Cipher Suite:	✓ TKIP ✓ AES
Pre- Shared Key Format:	Passphrase 🛟
Pre-Shared Key:	

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	Port: Type the port number of RADIUS Server
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.

Wireless Security Setup -5G

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.

Select SSID: Root AP - Repe	ater-139520_5G Save Save & Apply Reset
Encryption:	WEP \$
802.1x Authentication:	
Authentication:	Open System OShared Key OAuto
Key Length:	64-bit 🗘
Key Format:	Hex (10 characters) 💠
Encryption Key:	*******

6.Click	OK bi	utton.
---------	-------	--------

if WEP is turn on, WPS2.0 will be disabled		
	取消	好

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

Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 11 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.

Select	SSID: Root AP - Repe	ater-13952	20 🛟	Save	Save &	Apply	Reset
	Encryption:	WEP	\$				
	802.1x Authentication:	2					
	Authentication:	Open	System Shar	ed Key 💿	Auto		
	Key Length:	_64 Bi	ts 💽 128 Bits				
	RADIUS Server IP A	ddress:	192.168.1.250				
	RADIUS Server Port	:	1812				
	RADIUS Server Pass	sword:	•••••				

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.

Select SSID: Root AP - Repeater-139520_5G Save Save Apply Reset						
Encryption:	(WPA2 \$					
Authentication Mode:	Enterprise (RADIUS) • Personal (Pre-Shared Key)					
WPA2 Cipher Suite:	TKIP ZAES					
Management Frame Protection:	onone Capable required					
Pre- Shared Key Format:	Passphrase					
Pre-Shared Key:						

• 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.

Select SSID: Root AP - Repea	tter-139520_5G Save Save Apply Reset
Encryption:	WPA-Mixed 🗘
Authentication Mode:	Enterprise (RADIUS) OPersonal (Pre-Shared Key)
WPA Cipher Suite:	✓ TKIP ✓ AES
WPA2 Cipher Suite:	✓ TKIP ✓ AES
Pre- Shared Key Format:	Passphrase
Pre-Shared Key:	•••••

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

Select SSID: Root AP - Repea	ater-139520_5G 🛟	Save Save	& Apply Reset
Encryption: Authentication Mode: WPA2 Cipher Suite: Management Frame Protection:	WPA2 • Enterprise (RADIUS) TKIP Ø AES • none capable r	Personal (Pre-	Shared Key)
RADIUS Server IP Ac RADIUS Server Port: RADIUS Server Pass	ddress: 1812 word:		

WPA

Select SSID: Root AP - Repea	ater-139520)_5G 🛟	Save	Save & A	Apply	Reset
Encryption: Authentication Mode: WPA Cipher Suite: WPA2 Cipher Suite:	WPA-Mix • Enterp • TKIP • TKIP	xed ♀ prise (RADIUS) ⊘AES ⊘AES	Personal	l (Pre-Sh	ared Key	Y)
RADIUS Server IP A RADIUS Server Port: RADIUS Server Pass	ddress: : word:	1812				



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:

leve	elone	WRE-8011E A	C1200 Wire	less Range Exten	der
WLAN Access Point	SETUP WIRELESS	G WIRELES	S 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING	Wireless Access C	ontrol -5G			
ADVANCED	If you choose 'Allowed Listed', only th to connect to your Access Point. When	ose clients whose wirele Deny Listed' is selecte	ess MAC addre ed, these wirel	sses are in the access ess clients on the list w	control list will be able vill not be able to
SECURITY	connect the Access Point.				
ACCESS CONTROL	Wireless Access Control Mode:	Disable 🗘			
WPS	MAC Address:	Comment:			
	Save Save & Apply Reset				
	Current Access Control List:				
	MAC Address	Comment	Select		
	Delete Selected Delete All Res	et			

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.

Wireless Access Control Mode:	Allow Listed 🔻
MAC Address: 001122334455	Comment: 001122334455
Save Save & Apply Reset	
5.Click OK button.	

Message from webpage



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

 \times



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

Current Access Control List:					
MAC Address	Comment	Select			
00:11:22:33:44:55	001122334455				
Delete Selected Delete All	Reset				

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.

Wireless Access Control Mode:	Deny Listed 🔻
MAC Address: 001122334455	Comment: 001122334455
Save Save & Apply Reset	

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

Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 19 seconds ...



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:

leve	elone	w	RE-801:	1E AC1200 Wi	ireless Range Exte	nder
WLAN Access Point	SETUP	WIRELESS 5G	w	IRELESS 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING	/ Wi-Fi Prote	cted Set	up			
ADVANCED	This page allows you to o client automically syncro	hange the setting	g for WPS (d connect f	Wi-Fi Protected Setu to the Access Point i	up). Using this feature on a minute without any	ould let your wireless hassle.
SECURITY	Disable WPS					
ACCESS CONTROL	Save Save & Apply	Reset				
WPS 🤟						
	WPS Status:			Configured U	nConfigured	
	Auto-lock-down state	: unlocked		Unlock	_	
	Self-PIN Number:		:	14169564		
	Push Button Configur	ation: Start	PBC			
	STOP WSC	Stop V	NSC			
	Client PIN Number:			Start PIN		
	Current Key Info:					
	Authentication	Encryption	Key			
	WPA2-Mixed PSK	TKIP+AES	6666666	6		
	-Virtual Client- Self-PIN Number: PIN Configuration: Push Button Configur Client PIN Number:	141695 Start I ation: Start I	564 РІЛ РВС	Start PIN		

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.

leve	elone	WR	E- 8011E AC1200 Wi	ireless Range Exter	nder
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING 🗡	Wireless	Basic Setti	1gs -2.4G		
ADVANCED	This page is used to may change wireles	o configure the paramete ss encryption settings as	rs for wireless LAN clients wh well as wireless network para	nich may connect to your ameters.	Access Point. Here you
SECURITY	Disphie Wire				
ACCESS CONTROL	Band:	2.4 GHz (B+G+N) \$			
WPS	Mode:	(AP +)	MultipleAP		
	Network Type:	Infrastructure 🔹			
	SSID:	LevelOne WAP-8122 5.8G_E	хт	Add to Profile	
	Channel Width:	(40MHz \$			
	Control Sideband:	Upper 🔹			
	Channel Number:	Auto 🗘			
	Broadcast SSID:	Enabled			
	WMM:	Enabled			
	Data Rate:	Auto 🗘			
	TX restrict:	0 Mbps (0:no res	strict)		
	RX restrict:	0 Mbps (0:no res	strict)		
	Associated Clients:	Show Active Clients			
	Enable Univ simultaneouly)	ersal Repeater Mode (Acting as AP and client		
	SSID of Extende	ed Interface: RTK 11n A	AP RPT1	Add to Profile	
	Enable Wirele Wireless Profile I	ss Profile List:			
	SSID		Encrypt	Select	
	Delete Selected	DeleteAll			

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
	2.4 GHz (G) 2.4 GHz (N) 2.4 GHz (B+G) 2.4 GHz (G+N) ✓ 2.4 GHz (B+G+N)
Mode	Configure the Wireless LAN Interface to AP, Client, WDS, AP + WDS
	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.

Figure 1: Wireless Network page

Broadcast SSID	✓ Auto 5 6 7 8 9 10 11 12 13
	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 IM IM 2M 5.5M 11M 6M 9M 12M 8M 24M 36M 48M 55.5 MCS1 MCS5 MCS5 MCS6 MCS10 MCS11 MCS12 MCS13 MCS14 MCS15
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.

leve	elone	WRE-8011E AC1200 Wireless Range Extender
WLAN Access Point	SETUP	WIRELESS 5G WIRELESS 2.4G TCP/IP MANAGEMENT
BASIC SETTING	Wireless A	dvanced Settings -2.4G
ADVANCED	These settings are only settings should not be	y for more technically advanced users who have a sufficient knowledge about wireless LAN. These
SECURITY		
	Fragment Threshold	d: 2346 (256-2346)
ACCESS CONTROL	RTS Threshold:	2347 (0-2347)
WPS	Beacon Interval:	100 (20-1024 ms)
	Preamble Type:	Long Preamble Short Preamble
	IAPP:	Enabled Disabled
	Protection:	Enabled Olisabled
	Aggregation:	• Enabled Oisabled
	Short GI:	• Enabled Oisabled
	WLAN Partition:	Enabled Olisabled
	STBC:	Enabled Disabled
	LDPC:	• Enabled Oisabled
	20/40MHz Coexist:	Enabled Olisabled
	TX Beamforming:	• Enabled Obisabled
	MU MIMO:	Enabled Disabled
	Mutilcast to Unicast	t: OEnabled ODisabled
	TDLS Prohibited:	Enabled Oisabled
	TDLS Channel Switc Prohibited:	Ch Enabled Olisabled
	RF Output Power:	 ● 100% ● 70% ● 50% ● 35% ● 15%
	Save Save & Apply	Reset

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



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:

leve	elone	WR	RE-8011E AC1200 V	Vireless Range Exter	nder
WI AN Access Point	SETUD		WIDELESS 2.40	TCP/IP	MANAGEMENT
BASIC SETTING	Wireless	Security Se	etup -2.4G		MANAGEMENT
ADVANCED	This page allows ye unauthorized acces	ou setup the wireless see ss to your wireless netwo	curity. Turn on WEP or WPA lork.	by using Encryption Keys o	could prevent any
SECURITY	Select SSID:	Poot AD - Depostor 120520	 Coup Coup 	a & Apply Bocat	
ACCESS CONTROL	Select 3510.	Koot AF - Repeater-159520		Reset	
WPS	Encryptic	Disable	•		

WEP

Encryption:	WEP \$
802.1x Authentication:	
Authentication:	Open System OShared Key OAuto
Key Length:	64-bit 🗘
Key Format:	Hex (10 characters)
Encryption Key:	******

WPA2

Encryption:	(WPA2 \$)
Authentication	Enterprise (RADIUS) • Personal (Pre-Shared Key)
Mode: WPA2 Cipher Suite:	TKIP ZAES
Management Frame Protection:	• • none Capable required
Pre- Shared Key Format:	Passphrase 🛟
Pre-Shared Key:	•••••••••••••••••••••••••••••••••••••••

WPA-Mixed

Encryption:	WPA-Mixed \$
Authentication Mode:	OEnterprise (RADIUS) OPersonal (Pre-Shared Key)
WPA Cipher Suite:	✓ TKIP ✓ AES
WPA2 Cipher Suite:	✓ TKIP ✓ AES
Pre- Shared Key Format:	Passphrase
Pre-Shared Key:	•••••

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	Port: Type the port number of RADIUS Server
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.

Wireless Security Setup -2.4G

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.

Select SSID: Root AP - Rep	eater-139520 Save Save & Apply Reset
Encryption:	WEP \$
802.1x Authentication:	
Authentication:	Open System Shared Key OAuto
Key Length:	64-bit 🗘
Key Format:	Hex (10 characters) 💠
Encryption Key:	*****

6.Click	OK bi	utton.
---------	-------	--------

if WEP is turn on, WPS2.0 will be disabled		
	取消	好

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

Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 11 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.

Select SSID: Root AP - Re	eater-139520	\$ Save	Save & Apply	Reset
Encryption:	WEP \$			
802.1x Authentication:	O			
Authentication:	Open System	Shared Key 💿	Auto	
Key Length:	064 Bits 💿 128	Bits		
RADIUS Server IP	Address: 192.168.1	1.250		
RADIUS Server Po	t: 1812			
RADIUS Server Pa	sword:	•••••		

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.

Select SSID: Root AP - Repea	ter-139520_5G
Encryption:	(WPA2 \$
Authentication Mode:	Enterprise (RADIUS) • Personal (Pre-Shared Key)
WPA2 Cipher Suite:	TKIP ZAES
Management Frame Protection:	onone Capable required
Pre- Shared Key Format:	Passphrase
Pre-Shared Key:	

• 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.

Select SSID: Root AP - Repea	tter-139520_5G Save Save Apply Reset
Encryption:	WPA-Mixed 🗘
Authentication Mode:	Enterprise (RADIUS) OPersonal (Pre-Shared Key)
WPA Cipher Suite:	✓ TKIP ✓ AES
WPA2 Cipher Suite:	✓ TKIP ✓ AES
Pre- Shared Key Format:	Passphrase
Pre-Shared Key:	•••••

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

Select SSID: Root AP - Repea	ater-139520 \$ Save & Apply Reset
Encryption:	(WPA2 \$
Authentication Mode:	• Enterprise (RADIUS) Personal (Pre-Shared Key)
WPA2 Cipher Suite:	TKIP ZAES
Management Frame Protection:	
RADIUS Server IP Ad	ddress: 192.168.1.250
RADIUS Server Port:	1812
RADIUS Server Pass	sword:

WPA

Select SSID: Root AP - Repe	ter-139520 \$ Save	Save & Apply Reset
Encryption:	WPA-Mixed 🛟	
Authentication Mode:	• Enterprise (RADIUS) OPersonal	(Pre-Shared Key)
WPA Cipher Suite:	✓ TKIP ✓ AES	
WPA2 Cipher Suite:	✓ TKIP ✓ AES	
RADIUS Server IP A	dress: 192.168.1.250	
RADIUS Server Port	1812	
RADIUS Server Pass	vord:	



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:

leve	elone	WR	E- 8011E AC	C1200 Wire	less Range Exter	nder		
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS	2.4G	TCP/IP	MANAGEMENT		
BASIC SETTING	Wireless	Access Con	trol -2.4	G				
ADVANCED	If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able							
SECURITY	connect the Acces	s Point. Disa	ble	u, triese wirele	iss clients on the list			
ACCESS CONTROL	Wireless Access Control Mode: Allow Listed Deny Listed							
WPS	MAC Address: Comment:							
	Save Save &	Apply Reset						
	Current Access	Control List:						
	MAC Address Comment Select							
	Delete Selected	Delete All Reset						

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.

Wireless Access Control Mode:	Allow Listed 🔻
MAC Address: 001122334455	Comment: 001122334455
Save Save & Apply Reset	
5.Click OK button.	

Message from webpage



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

 \times



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

Current Access Control List:		
MAC Address	Comment	Select
00:11:22:33:44:55	001122334455	
Delete Selected Delete All	Reset	

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.

Wireless Access Control Mode:	Deny Listed 🔻
MAC Address: 001122334455	Comment: 001122334455
Save Save & Apply Reset	

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

Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 19 seconds ...



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:

leve	elone	W	RE-8011E AC1200 W	ireless Range Exte	nder
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
BASIC SETTING	/ Wi-Fi Prot	ected Set	up		
ADVANCED	This page allows you client automically syn	to change the setting cronize its setting an	g for WPS (Wi-Fi Protected Set d connect to the Access Point	up). Using this feature o in a minute without any	ould let your wireless hassle.
SECURITY	Disable W	PS			
ACCESS CONTROL	Save Save & App	ly Reset			
WPS				- C f I	
	WPS Status:		Reset to UnConfigure		
	Auto-lock-down st	ate: unlocked	Unlock	_	
	Self-PIN Number:		14169564		
	Push Button Config	Push Button Configuration: Start PBC			
	STOP WSC	Stop \	vsc		
	Client PIN Number		Start PIN		
	Current Key Info:				
	Authentication	Encryption	Кеу		
	Open	None	N/A		
	-Virtual Clien Self-PIN Number: PIN Configuration: Push Button Config Client PIN Number	t- 14169 Start guration: Start	564 PIN PBC Start PIN		

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.)



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...

ſ	e	m	71	17 1	Ì	1
			b	9	Į	
ľ	V	(c	t	e	è

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:

leve	elone	WRE	-8011E AC1200 \	Wireless Range Exter	nder
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
LAN SETTING	LAN Inte	rface Setup			
	This page is used to Point. Here you ma	o configure the parameters y change the setting for If	s for local area network w addresss, subnet mask,	hich connects to the LAN p DHCP, etc	oort of your Access
	IP Address:	192.168.1.1			
	Subnet Mask:	255.255.255.0			
	DHCP:	Server 🗘			
	DHCP Client Ran	ge: 192.168.100 -	192.168.1.200		
	DHCP Lease Time	e: 480 (1 ~ 10	080 minutes)		
	Domain Name:	repeater.nw			
	802.1d Spanning Tree:	Disabled \$			
	Save Save & Ap	Reset			

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





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.

leve	lone	WR	RE-8011E AC1200 W	/ireless Range Ex	tender
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
STATUS	Access Po	oint Status			
STATISTICS	This page shows the device.	e current status and some	e basic settings of the		
UPGRADE FIRMWARE	APInfrastructure Clier	tAPInfrastructure Client			
SAVE/RELOAD SETTING	System				
	Uptime	0day:2h:13m:21	S		
PASSWORD	Firmware Version	n RE12B_v3411d_	Lev_005		
	Build Time	Tue Sep 4 16:49	:30 CST 2018		
	Wireless 5G Config	uration			
	Band	5 GHz (A+N+AC)		
	SSID	Repeater-139520)_5G		
	Channel Number	36			
	Encryption	WEP 64bits			
	Wireless 5G Repea	ter Interface Configurat	tion		
	SSID	RTK 11n AP RPT	0		
	Encryption	Disabled			
	BSSID	00:00:00:00:00:	00		
	State	Scanning			
	Wireless 2.4G Cont	figuration			
	Band	2.4 GHz (B+G+N	1)		
	SSID	Repeater-139520)		
	Channel Number	4			
	Encryption	Disabled			
	Wireless 2.4G Rep	eater Interface Configur	ation		
	SSID	RTK 11n AP RPT	1		
	Encryption	Disabled			
	BSSID	00:00:00:00:00:	00		
	State	Scanning			
	TCP/IP Configurat	ion			
	Attain IP Protoco	Fixed IP			
	IP Address	192.168.1.1			
	Subnet Mask	255.255.255.0			
	DHCP Server	Enabled			
	MAC Address	94:46:96:13:95:	20		



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:

leve	lone	w	RE-8011E AC1200) Wireless Range Ext	ender
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
STATUS	Statistics				
STATISTICS	This page shows the	packet counters for trar	nsmission and reception re	garding to wireless and Etl	hernet networks.
UPGRADE FIRMWARE		Sent Packets	253		
	Wireless 1 LAN	Received Packets	24565		
SAVE/RELOAD SETTING	Wireless 1	Sent Packets	208		
PASSWORD	Repeater LAN	Received Packets	0		
	Wireless 2 I AN	Sent Packets	267		
	WITCIESS 2 LAIT	Received Packets	3315		
	Wireless 2	Sent Packets	624		
	Repeater LAN	Received Packets	0		
	Ethernet I AN	Sent Packets	746		
	Line net LAN	Received Packets	612		
	Refresh				



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.

leve	VEIONE WRE-8011E AC1200 Wireless Range Extender					
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT	
STATUS	/ Upgrade	Firmware				
STATISTICS	This page allows yo the upload because	This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during				
UPGRADE FIRMWARE						
SAVE/RELOAD SETTING	Firmware Versio Select File:	n: R	E12B_v3411d_Lev_005 選擇檔案 尚未選取檔案			
PASSWORD	Upload Reset					

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 ...



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:

WRE-8011E AC1200 Wireless Range Extender						
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT	
STATUS	/ Save/Re	load Setting	S			
STATISTICS	This page allows y you could reset th	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				
UPGRADE FIRMWARE	<u>.</u>					
SAVE/RELOAD SETTING	Save Settings t	o File: Save				
PASSWORD	Load Settings f	rom File: 選擇檔案 尚未	選取檔案	oad		
	Reset Settings Default:	to Reset				

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

Save Settings to File: 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.

Opening config. dat	×
You have chosen to open:	
config.dat which is: dat File (9.0 KB) from: http://192.168.1.1	
What should Firefox do with this file?	
Open with Browse	
⊙ Save File	
Do this automatically for files like this from now on.	
OK Cancel)

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:

Save/Reload Settings

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.

Save Settings to File:	Save	
Load Settings from File:	Choose File No file chosen	Upload
Reset Settings to Default:	Reset	

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

Load Settings from File:	Choose File	No file chosen	Up	load	l
--------------------------	-------------	----------------	----	------	---

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

Load Settings from File:	Choose File	config.dat		Upload	
--------------------------	-------------	------------	--	--------	--

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

Change setting successfully!

Do not turn off or reboot the Device during this time.

Please wait 44 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:

Save/Reload Settings				
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.				
Save Settings to File: Load Settings from File:	Save Choose File No file chosen	Upload		
Reset Settings to Default:	Reset			
2. Click on Reset				
Reset Settings to Default:	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 ...



Please wait 59 seconds ...



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:

WRE-8011E AC1200 Wireless Range Extender					ender
WLAN Access Point	SETUP	WIRELESS 5G	WIRELESS 2.4G	TCP/IP	MANAGEMENT
STATUS	Passwor	d Setup			
STATISTICS	This page is used the protection.	to set the account to acces	s the web server of Access	Point. Empty user name	and password will disable
UPGRADE FIRMWARE					
SAVE/RELOAD SETTING	User Name: New Password:				
PASSWORD	Confirmed Password:				
	Save Save & A	Apply Reset			

2. Currently Defined Administration Password: Setup page

Password Setup 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.				
New Password:	••••••			
Confirmed Password:				
Save Save & Apply	Reset			