

# User Manual



**EWS330AP**  
version 1.3

Dual Band AC1300 Indoor Access Point

# IMPORTANT

To install this Access Point please refer to the **Quick Installation Guide** included in the product packaging.

# Table of Contents

<b>Chapter 1 Product Overview.....</b>	<b>4</b>	Wireless MAC Filtering.....	41
Key Features/Introduction.....	5	<b>Chapter 8 Management.....</b>	<b>43</b>
System Requirements/Package Contents.....	6	Management VLAN Settings.....	44
Technical Specifications.....	7	Advanced Settings.....	45
Physical Interface.....	9	Time Zone.....	48
<b>Chapter 2 Before You Begin .....</b>	<b>10</b>	Auto Reboot Settings.....	49
Computer Settings.....	11	Wi-Fi Scheduler.....	50
Mounting the Access Point.....	16	Tools.....	51
<b>Chapter 3 Configuring Your Access Point.....</b>	<b>18</b>	Account/Firmware.....	54
Default Settings.....	19	Backup/Restore .....	55
<b>Chapter 4 Building a Wireless Network.....</b>	<b>20</b>	Log.....	57
Access Point Mode.....	21	Logout/Reset.....	58
AP Mesh Mode.....	22	<b>Appendix .....</b>	<b>59</b>
<b>Chapter 5 Overview.....</b>	<b>23</b>	FCC Interference Statement.....	60
Overview.....	24	IC Interference Statement.....	61
Connections.....	26	CE Interference Statement.....	63
<b>Chapter 6 Network .....</b>	<b>28</b>		
Basic/IP Settings/Spanning Tree Settings.....	29		
<b>Chapter 7 2.4 GHz &amp; 5 GHz Wireless.....</b>	<b>31</b>		
Wireless Settings.....	32		
2.4 GHz/5 GHz Wireless Network.....	33		
2.4GHz/5 GHz SSID Profile.....	33		
Wireless Security.....	34		
Wireless Advanced.....	37		
Guest Network Settings.....	39		
RSSI Threshold .....	40		

# Chapter 1

# **Product Overview**



# Introduction - EWS330AP

## Key Features

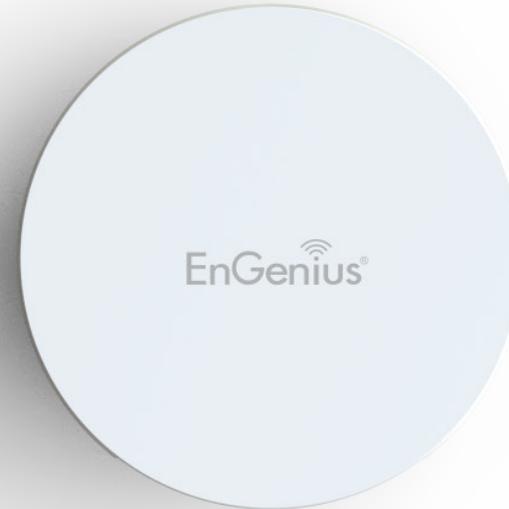
- Built-in Turbo Engine solution with a Quad-core powerful chipset solution to process multiple tasks for driving and enhancing performance effectively.
- Dual radio 2x2 802.11 ac wave2/ac/a/b/g/n Access Point with multi-user MIMO (MU-MIMO)
- Support up to 867 Mbps in 5GHz frequency band and 400 Mbps in 2.4GHz frequency band (with 2ss/VHT40 clients)
- High powered amplifiers to improve the wireless coverage and uses a special radio frequency pattern to increase its receiver sensitivity for improved performance.
- Support 802.11 ac Wave 2.0 technology to enhance overall bandwidth and speed to wireless client devices.
- 360° omni-directional antennas to achieve comprehensive coverage for networking client devices under a pervasive environment.
- Compliance with 802.3af or 48V PoE Input for flexible installation over 100 meters (328 feet)
- Choose an operating mode to meet your management and deployment requirement.

## Introduction

**EnGenius Wireless Management Access Point solution is designed for deploying on the versatile indoor application. To meet today's requirement on varied networking environment, EnGenius would like to provide the solution as flexible, robust and effective as the**

**organization they desire.**

**The state-of-the-art 802.11 ac and MU-MIMO technology brings revolutionary connecting speed and bandwidth for diversity of multimedia applications. EWS330AP equips with two powerful RF interfaces that support up to 867 Mbps in 5GHz frequency band and 400 Mbps in**



Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment, and mix of devices in the network. Features and specifications subject to change without notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright © 2018 EnGenius Technologies, Inc. All rights reserved.

**2.4GHz frequency band (with 4ss/VHT40 clients).**

## **System Requirements**

The following are the Minimum System Requirements in order to configure the device:

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7, 8), or Mac OS, Linux-based operating systems
- Web-browsing application (i.e. Edge, Internet Explorer, Chrome, Firefox, Safari, or another similar browser application)

## **Package Contents**

The EWS330AP package contains the following items (all items must be in package to issue a refund):

- One EWS330AP Access Point
- Power Adapter (12V/1A)
- T-Rail Mounting kit (9/16" and 15/16")
- Quick Installation Guide
- Wall Mount screw set

# Technical Specifications - EWS330AP

## Radio Specification

### Dual Concurrent Radio:

- 2.4 GHz: 802.11b/g/n with max data rate up to 400 Mbps
- 5 GHz: 802.11a/n/ac with max data rate up to 867 Mbps

### Transmit Power:

- Max transmit power is limited by regulatory power

### Radio Chains/Spatial Streams:

- 2 x 2: 2

### Supported Radio Technology:

- 802.11b: Direct-Sequence Spread-Spectrum (DSSS)
- 802.11a/g/n/ac: Orthogonal Frequency-Division Multiplexing (OFDM)

### Channelization:

- 802.11ac with 20/40/80 MHz channel width
- 802.11n with 20/40 MHz channel width
- 802.11a/b/g with 20 MHz channel width

### Supported Modulation:

- 802.11b: BPSK, QPSK, CCK
- 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM
- 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

### Supported data rates (Mbps):

- 802.11b: 1, 2, 5.5, 11
- 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
- 802.11n: 6.5 to 400 (MCS0 to MCS15)
- 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS= 1 to 2)

## Physical & Environment

### Power Source:

- PoE: compatible with 802.3af
- DC IN, 12V/1A

### Internal Antenna:

- 5.0 dBi 2.4 GHz antennas
- 5.0 dBi 5 GHz antennas

## Interface:

- 1 x 10/100/1000 BASE-T RJ-45 Ethernet Ports
- 1 x DC Jack
- 1 x Reset button
- LED Indicators

## Dimensions (W x D x H):

- 132.4 mm x 37.4mm

## Weight (Without accessories):

179g

## Mounting:

- Wall mount (Mount Access Point on a flat wall) / Ceiling Mounting (Assemble a mounting bracket for drop ceiling)

## Environment:

- Operating temperature: 0°C~40°C
- Operating humidity: 0%~90% typical
- Storage temperature: -40°C~80°C

## Wireless

### Operating Mode:

AP Mode

Mesh AP Mode

### Auto Channel Selection:

- Setting varies by regulatory domains

### SSIDs:

- Supports up to 8 SSIDs per frequency band

VLAN Tag / VLAN Pass-through

Wireless Client List

### Guest Network:

- Allocates a separate network segment for guest access within the same WLAN

QoS:

# Technical Specifications - EWS330AP continued

## Band Steering

### Mobility:

- PMKSA support for fast roaming

### Security:

- WEP encryption: 64/128/152-bitSecurity:
- WEP encryption: 64/128/152-bitLED Indicator
- WPA/WPA2 Enterprise/PSK
- Hidden SSID
- MAC address filtering (up to 50 MAC)
- Client isolation

## Management

### Deployment Options

- Standalone Mode
- Managed Mode (by Neutron Switch or ezMaster)

### Configuration

- Web Interface (HTTP)
- SNMP v1/v2c/v3 with MIB I/II and private MIB
- CLI (Telnet)

### Firmware Upgrade

- Web interface or CLI (FTP/HTTP)

### Backup / Restore Settings

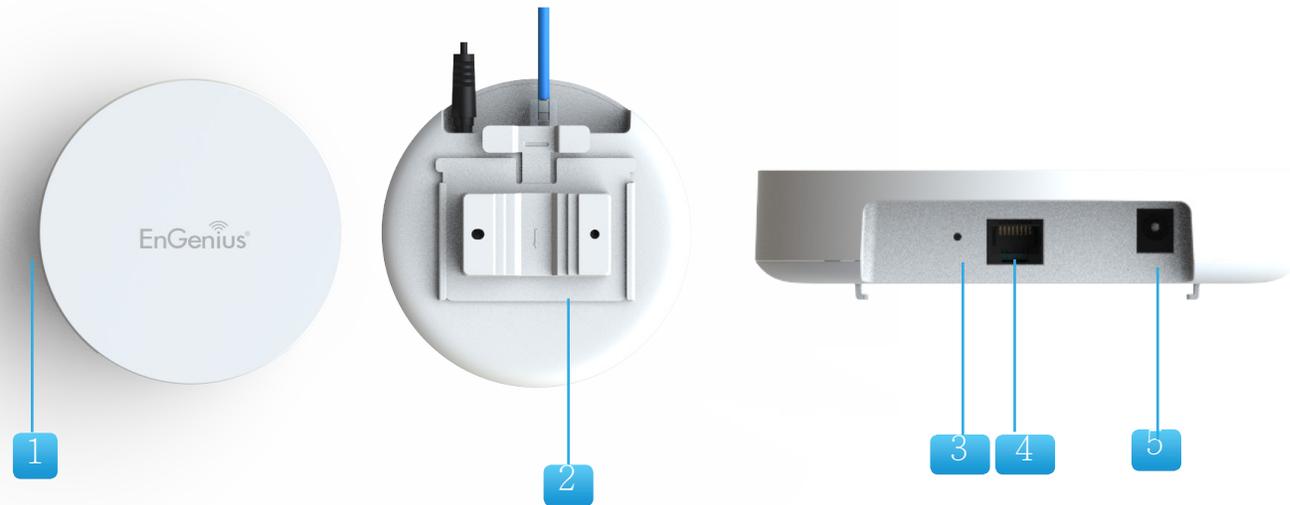
- Revert to factory default settings

### Schedule Reboot:

- Specifies interval to reboot system periodically

### E-mail Alert/Syslog Notification

# Physical Interface (EWS330AP)



1. LED Indicator
2. Ceiling (Wall) Mount Hole: Using the provided hardware, the EWS330AP can be attached to a ceiling or wall.
3. Reset Button: Press and hold for over 10 seconds to reset to factory default settings.
4. 10/100 LAN Ports: One RJ45 access port
5. DC-Jack 12V DC IN for Power

# Chapter 2

## **Before You Begin**



# Computer Settings

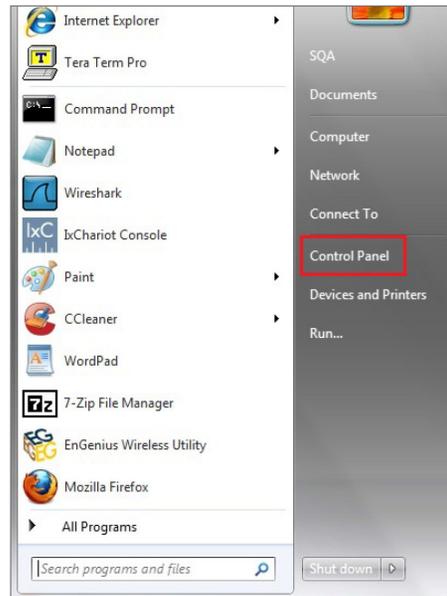
## Windows XP/Windows 7/Windows 8/Windows 10

In order to use the Access Point, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

1a. Click the **Start** button and open the **Control Panel**

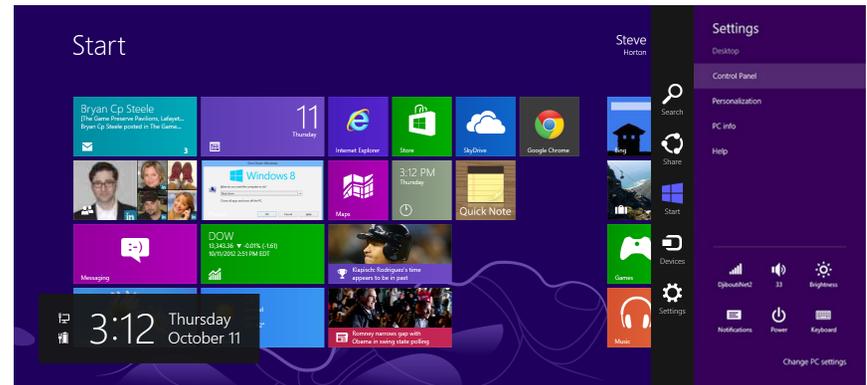


Windows XP



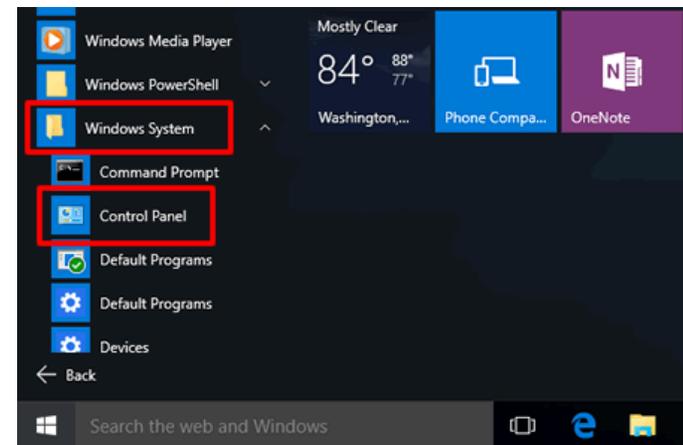
Windows 7

1b. Move your mouse to the lower right hot corner to display the Charms Bar and select the **Control Panel** in Windows 8 OS.



Windows 8

1c. In Windows 10, click **Start** to select **All APPs** to enter the folder of **Windows system** for selecting **Control Panel**.

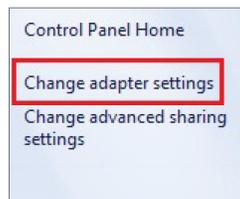


Windows 10

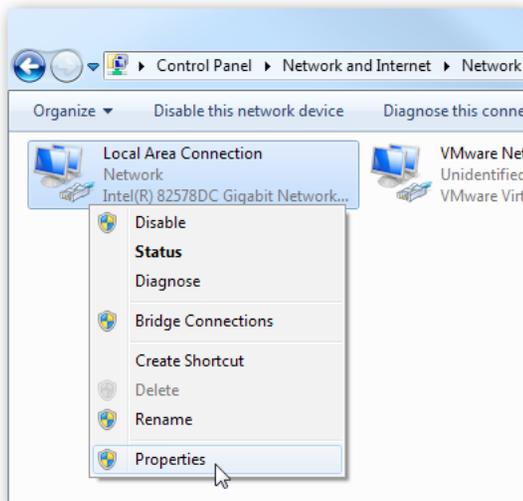
2a. In Windows XP, click **Network Connections**.



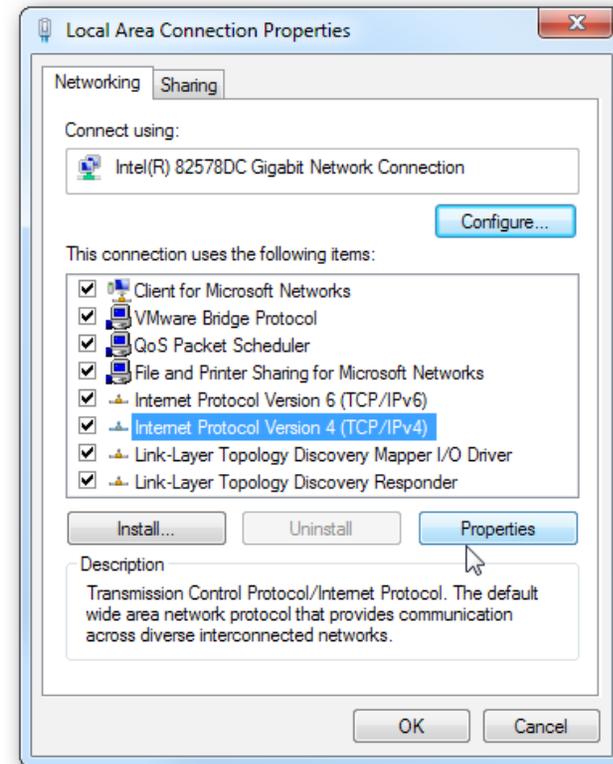
2b. In Windows 7/Windows 8/Windows 10, click **View Network Status and Tasks** in the **Network and Internet** section, then select **Change adapter settings**.



3. Right click on **Local Area Connection** and select **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



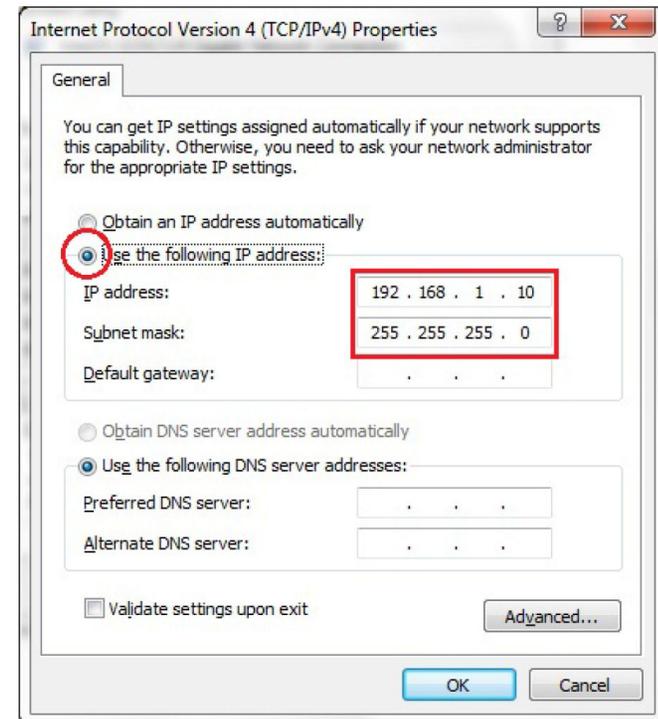
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

**Note:** Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: AP IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.255

PC Subnet mask: 255.255.255.0



## Apple Mac OS X

1. Go to **System Preferences** (Which can be opened in the Applications folder or selecting it in the Apple Menu).
2. Select **Network** in the **Internet & Network** section.



3. Highlight **Ethernet**.

4. In **Configure IPv4**, select **Manually**.
5. Enter an IP address that is different from the Access Point and Subnet mask then press **OK**.

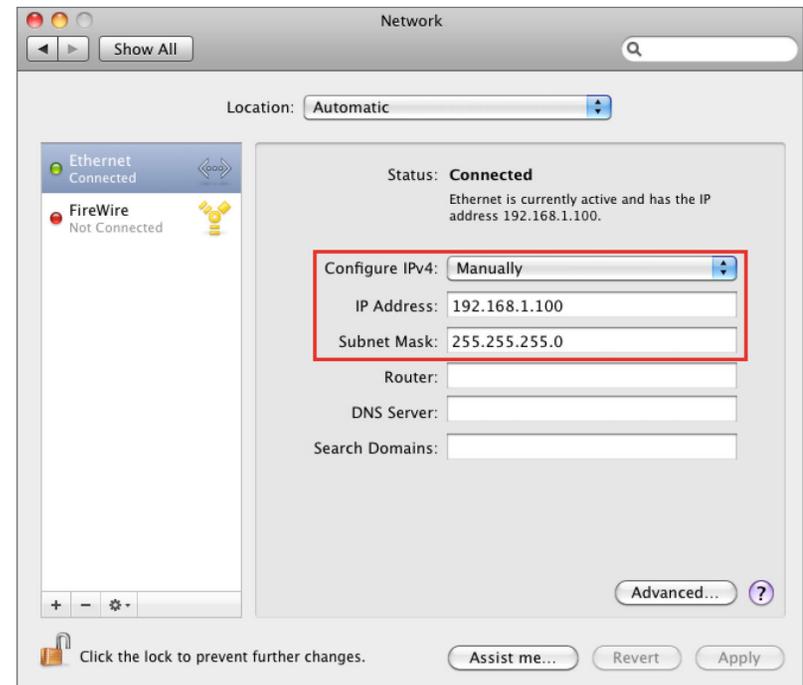
**Note:** Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: A device IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.255

PC Subnet mask: 255.255.255.0

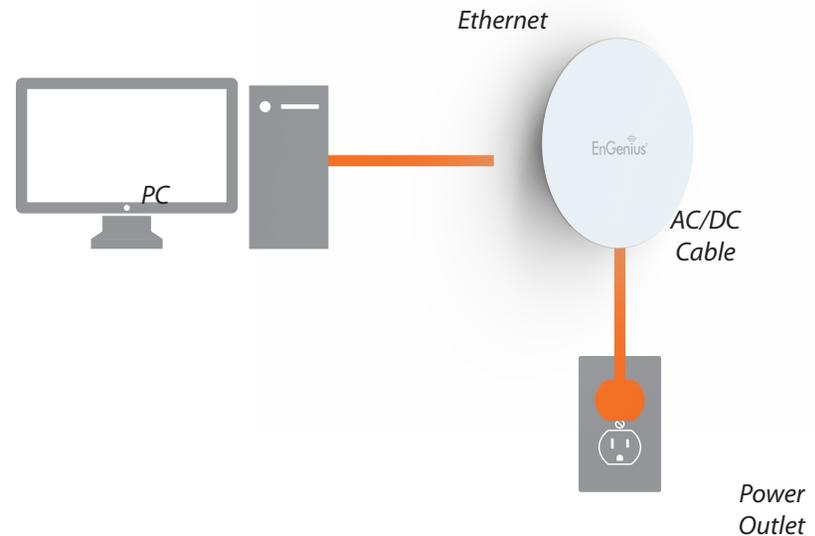
6. Click **Apply** when done.



# Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller port (RJ-45 Ethernet Port). For more information, verify with your computer's user manual.
2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the EWS330AP and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the EWS330AP and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the EWS330AP and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:
  - a) Ensure that the **POWER** light is on (it will be **orange**).
  - b) Ensure that the 2.4 GHz/5 GHz WLAN light is on (it will be **blue** for 2.4G, and **green** for 5G).
  - c) Ensure that the LAN (Computer EWS330AP Connection) light is on (it will be **blue**).
  - d) Once all three lights are on, proceed to set up the Access Point using the computer.

This diagram depicts the hardware configuration.



# Mounting the EWS330AP

Attaching the EWS330AP to a ceiling :

1. Slide the ceiling mount base into the slot of this Access Point.
2. Hold the Access Point with one hand to reach the other hand over the T-rail side of the bracket. Then hook the stationary end of the ceiling mount bracket on to the T-rail.

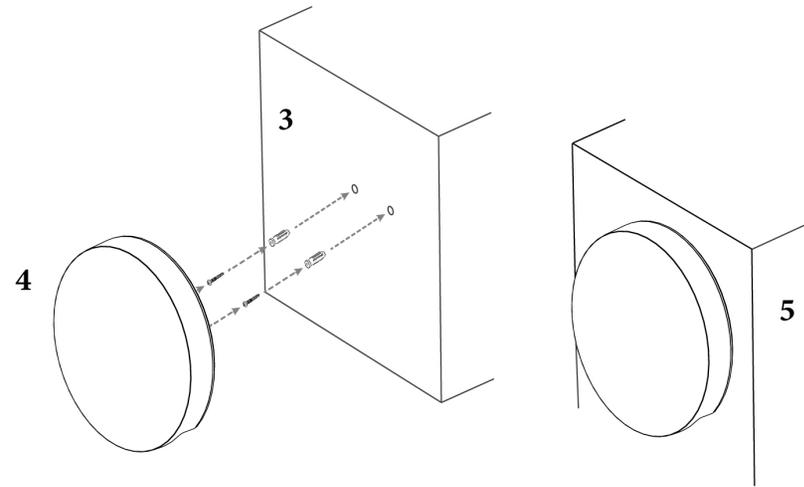
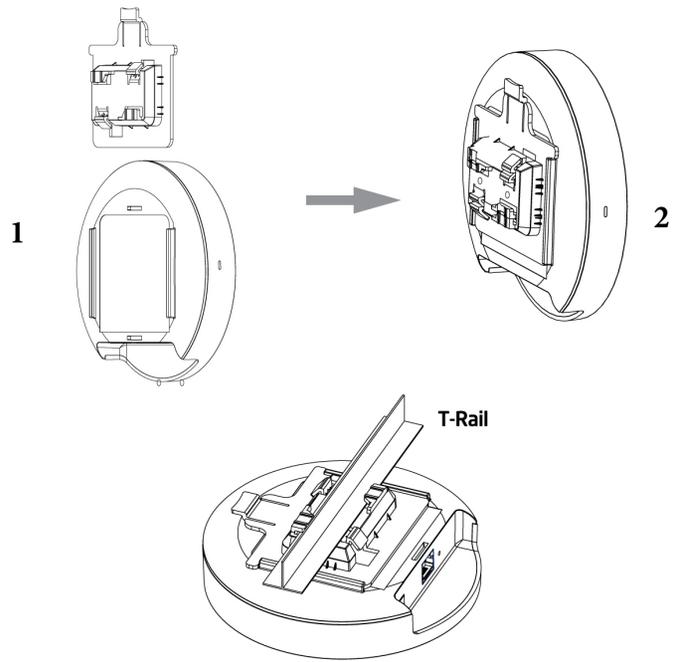
Attaching the EWS330AP to a wall :

3. Continue from A, determine the where the Access Point to be placed and mark location on the surface for the two mounting holes. Use the appropriate drill bit to drill two 8.1mm diameter and 26mm depth holes in the markings and hammer the bolts into the openings.
4. Screw the anchors onto the holes until they are flush

with the wall; screw the included screw into the anchors.

5. Place the Access point against the wall with the mounting screw heads

Note: Mounting hardware kit are included 15/16in (2.38cm) and 9/16in (1.43cm). If extra space is required to accommodate drop ceiling tiles, use the provided spacers and long screws.



## Chapter 3

# Configuring Your Access Point



# Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

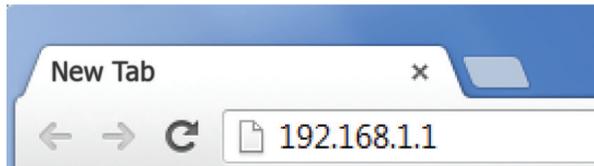
## Default Settings

Please use your Ethernet port or wireless network adapter to connect the Access Point.

IP Address	192.168.1.1
Username/Password	admin/admin

## Web Configuration

1. Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address **http://192.168.1.1**.

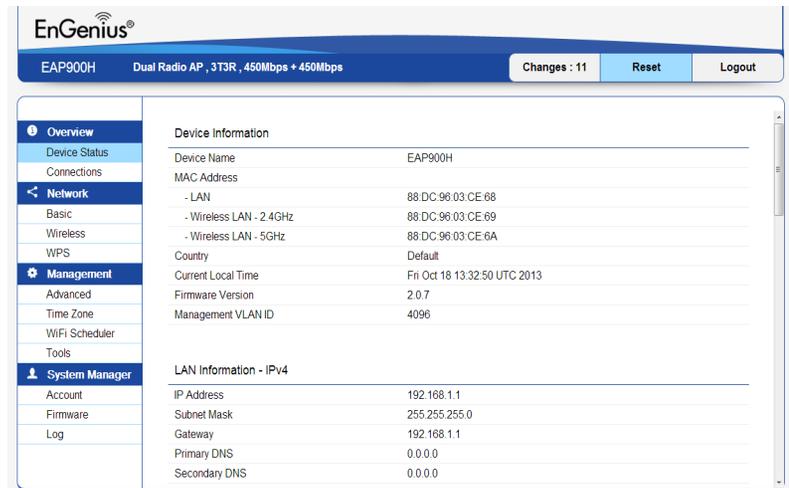


**Note:** If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

2. The default username and password are: **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-based configuration page.



- \* The model name will be varied in the web browser.
3. If successful, you will be logged in and see the EAP User Menu.



## Chapter 4

# Building a Wireless Network



The EWS330AP has the ability to operate in various modes. This chapter describes the operating modes of above three models.

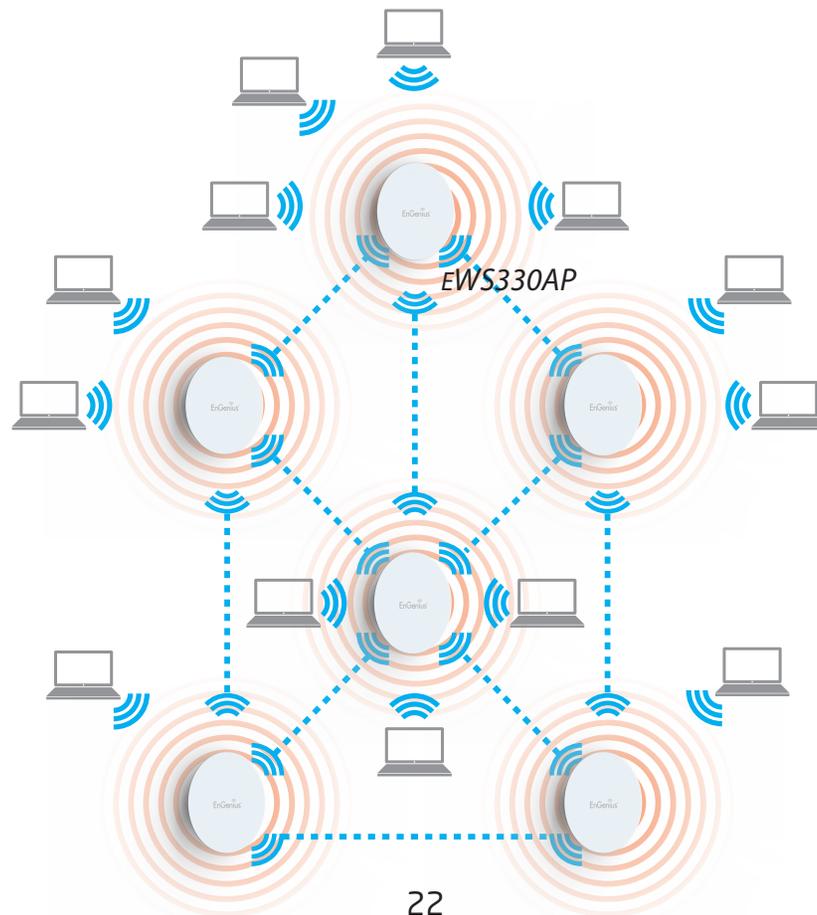
## Access Point Mode

In Access Point Mode, the EWS330AP behaves like a central connection for stations or clients that support IEEE 802.11 a/b/g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the EWS330AP. The EWS330AP supports up to eight (8) SSIDs per band (16 total) at the same time for secure access.



## AP Mesh Mode

Under the AP Mesh mode, the EWS330AP can be used as the central connection hub for station or clients that support IEEE 802.11 b/g/n network. Under this mode, the EWS330AP can be configured with the same Mesh SSID and security password in order to associate with other EWS330AP, as well as connect with clients under the same SSID and encryption signatures. For example, you would use one band to connect Access Points in range with Mesh mode and the other band to broadcast traffic on the network.



# Chapter 5

# **Overview**



# Overview

## Save Changes

This page lets you save and apply the settings shown under **Unsaved changes list**, or Revert the unsaved changes and revert to the previous settings that were in effect.

The screenshot shows the EnGenius web interface for device ENS620EXT. The main content area is titled 'Configuration / Changes' and displays a list of configuration items. A legend at the top indicates the status of each item: green for 'Section added', red for 'Section removed', light green for 'Option changed', and light red for 'Option removed'. The items listed are:

- dhcp.cfg02411c (Section added)
- dhcp.cfg02411c.domain=ENS620EXT (Option changed)
- network.lan (Section added)
- network.lan.hostname=ENS620EXT (Option changed)
- wireless.wifi1 (Section added)
- wireless.wifi1.channel\_config\_status=1 (Option changed)
- wireless.wifi1.htmode=HT80 (Option changed)
- wireless.wifi0 (Section added)
- wireless.wifi0.channel\_config\_status=1 (Option changed)

Buttons for 'Apply' and 'Revert' are located at the bottom of the configuration list.

## Device Status

Clicking the **Device Status** link under the **Overview** menu shows the status information about the current operating mode.

- The **Device Information** section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID

**Note:** VLAN ID is only applicable in Access Point, WDS AP or WDS BR mode.

### Device Information

Device Name	ENS620EXT
MAC Address	
- LAN1	88:DC:96:00:00:10
- LAN2	88:DC:96:00:00:11
- Wireless LAN - 2.4GHz	88:DC:96:00:00:12
- Wireless LAN - 5GHz	88:DC:96:00:00:13
Country	USA
Current Local Time	Tue Jul 12 11:45:00 2016
Uptime	0h 4m 57s
Firmware Version	1.0.0
Management VLAN ID	Untagged

- The **Memory Information** section shows usage of memory such as Total Available, Free, Cached, Buffered

### Memory Information

Total Available	128884 kB / 236336 kB (54%)
Free	95352 kB / 236336 kB (40%)
Cached	24908 kB / 236336 kB (10%)
Buffered	8624 kB / 236336 kB (3%)

- The **LAN Information** section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, Primary DNS Address, Secondary DNS Address, status of DHCP client, and status of Spanning Tree protocol (STP).

#### LAN Information - IPv4

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disable
Spanning Tree Protocol(STP)	Disable

The **Wireless LAN Information 2.4 GHz/5 GHz** section shows wireless information such as Operation Mode, Frequency, and Channel. Since this Access Point supports multiple-SSIDs, information about each SSID, the ESSID, and security settings, are displayed

**Note:** Profile Settings are only applicable in Access Point and WDS AP modes.

#### Wireless LAN Information - 2.4GHz

Operation Mode	Access Point			
Wireless Mode	802.11 B/G/N			
Channel Bandwidth	20 MHz			
Channel	2.412 GHz(Channel 1)			
Profile	SSID	Security	VID	802.1Q
#1	EnGenius_Test	None	1	Disable
#2	EnGenius-mac-_2-2.4GHz	None	2	Disable
#3	EnGenius-mac-_3-2.4GHz	None	3	Disable
#4	EnGenius-mac-_4-2.4GHz	None	4	Disable
#5	EnGenius-mac-_5-2.4GHz	None	5	Disable
#6	EnGenius-mac-_6-2.4GHz	None	6	Disable
#7	EnGenius-mac-_7-2.4GHz	None	7	Disable
#8	EnGenius-mac-_8-2.4GHz	None	8	Disable
#9	EnGenius-2.4GHz_GuestNetwork	None		Disable

#### Wireless LAN Information - 5GHz

Operation Mode	WDS Access Point			
Wireless Mode	802.11 N/AC			
Channel Bandwidth	80 MHz			
Channel	5.180 GHz(Channel 36)			
Profile	SSID	Security	VID	802.1Q
#1	EnGenius_Test	None	51	Disable
#2	EnGenius-mac-_2-5GHz	None	52	Disable
#3	EnGenius-mac-_3-5GHz	None	53	Disable
#4	EnGenius-mac-_4-5GHz	None	54	Disable

- The **Statistics** section shows Mac information such as SSID, MAC address, RX and TX.

#### Statistics

SSID	MAC	RX(Packets)	TX(Packets)
Ethernet	88:DC:96:00:00:10	134.37 KB(829 Pkts.)	893.75 KB(857 Pkts.)
EnGenius-mac-_1-2.4GHz	88:DC:96:00:00:12	0.00 B(0 Pkts.)	21.34 KB(149 Pkts.)
EnGenius-mac-_1-5GHz	88:DC:96:00:00:13	0.00 B(0 Pkts.)	8.02 KB(44 Pkts.)

# Connections

## 2.4 GHz/5 GHz Connection List

Click the connection link under the Overview menu displays the connection list of clients associated to the AP's 2.4 GHz/5 GHz, along with the MAC addresses and signal strength for each client. Clicking **Refresh** updates the client list.

**Note:** Only applicable in Access Point and WDS AP modes.

## 2.4 GHz/5 GHz WDS Link List

Click the connection link under the Overview menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

**Note:** Only applicable in WDS AP and WDS Bridge modes.

### Connection List - 2.4GHz

SSID	MAC Address	TX	RX	RSSI	Block
------	-------------	----	----	------	-------

### WDS Link List - 5GHz

WDS Link ID#	MAC Address	Link Status	RSSI(dBm)
--------------	-------------	-------------	-----------

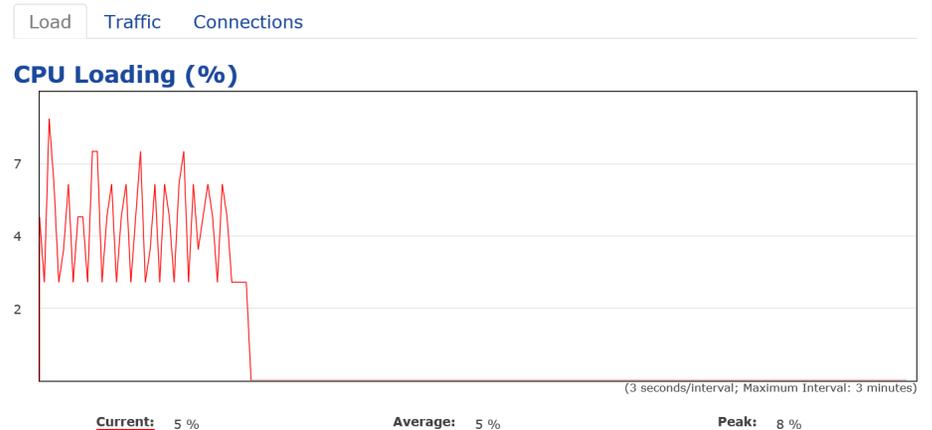
Refresh

# Realtime

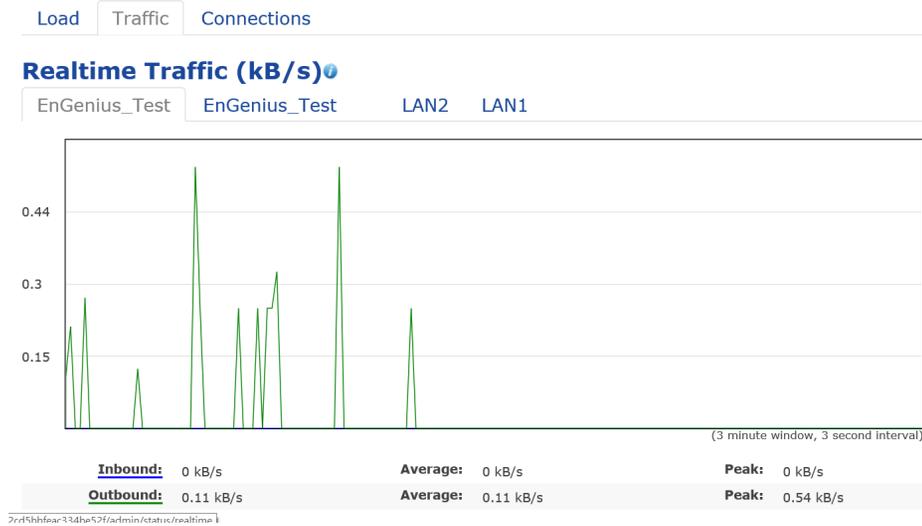
## Realtime

The Realtime section contains the following options:

**CPU Loading:** 3 minutes CPU loading percentage information, it displays current loading, average loading and peak loading status. Left bar is loading percentage; button is time tracing. Interval is every 3 seconds



**Traffic Loading:** 2.4GHz and 5GHz and Ethernet port inbound and outbound traffic by current, average and peak time.



**Realtime Connection (Pkts):** Overview on current active network connections. It displays UDP and TCP packets information and other connection status. UDP connections curve is in blue; TCP connection curve is in green; others curve is in red. Below of chart shows connections source and destination.

# Chapter 6

# **Network**



# Basic

## IPv4/IPv6 Settings

This page allows you to modify the device's IP settings.

### IPv4 Settings

IP Network Setting	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS	<input type="text" value="0.0.0.0"/>
Secondary DNS	<input type="text" value="0.0.0.0"/>

### IPv6 Settings

Link-local Address

IP Address	<input type="text"/>
Subnet Prefix Length	<input type="text"/>
Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

**IP Network Settings:** Select whether the device IP address will use a static IP address specified in the IP address field or be obtained automatically when the device connects to a DHCP server.

**IP Address:** The IP address of this device.

**Subnet Mask:** The IP Subnet mask of this device.

**Gateway:** The Default Gateway of this device. Leave it blank if you are unsure of this setting.

**Primary/Secondary DNS:** The primary/secondary DNS address for this device.

**Save:** Click **Save** to confirm the changes.

## Spanning Tree Protocol (STP) Settings

This page allows you to modify the Spanning Tree settings. Enabling the Spanning Tree protocol will prevent network loops in your LAN network.

### Spanning Tree Protocol (STP) Settings

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Hello Time	<input type="text" value="2"/>	seconds (1-10)
Max Age	<input type="text" value="20"/>	seconds (6-40)
Forward Delay	<input type="text" value="15"/>	seconds (4-30)
Priority	<input type="text" value="32768"/>	(0-65535)

**Spanning Tree Status:** Enables or Disables the Spanning Tree function. Default is Disable.

**Hello Time:** Specifies Bridge Hello Time in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.

**Max Age:** Specifies Bridge Max Age in seconds. If another

bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be inactive.

**Forward Delay:** Specifies Bridge Forward Delay in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it analyzes data traffic before participating in the network.

**Priority:** Specifies the Priority Number. A smaller number has a greater priority than a larger number.

**Save:** Click **Save** to confirm the changes.

## Chapter 7

# 2.4 GHz & 5 GHz Wireless



# Wireless

## Wireless Settings

### Wireless Settings

Device Name	EWS330AP
-------------	----------

**Device Name:** Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.

**Band Steering (Available on ENS620EXT):** Enable Band Steering to send 802.11n clients to the 5 GHz band, where 802.11b/g clients cannot go, and leave 802.11b/g clients in 2.4GHz to operate at their slower rates. Before implementing this feature, we suggest you to assure the both 2.4GHz and 5GHz SSID, as well as security settings must be the same. EnGenius Band Steering supports following advanced settings,

Wireless Settings	
Device Name	ENS620EXT
Country / Region	USA
Band Steering	Force 5GHz
<b>INFORMATION:</b> When band steering is configured to Force 5GHz mode, the AP will not allow a dual band client to connect to the 2.4GHz band only if the client is not currently associated on the 2.4GHz radio of this AP. <b>NOTE:</b> In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.	

\***Force 5GHz:** When band steering is configured to Force 5GHz mode, the AP will not dual band capable client

devices to network to the 2.4GHz band only if the client devices are not currently associated on 2.4GHz radio in this AP.

Band Steering	Prefer 5GHz	5GHz RSSI	-75	dBm
<b>NOTE:</b> In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.				

\***Prefer 5GHz:** When band steering is configured to Prefer 5GHz mode, the AP will steer dual band capable client devices to 5GHz radio when the RSSI value of these client devices on 5GHz radio is more than set one. The allowed RSSI value for default setting is -75dBm.

Band Balance	5GHz RSSI	-75	dBm	Percent of clients on 5GHz radio	75	%
<b>NOTE:</b> In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.						

\***Band Balance:** When band steering is configured to Band Balance mode, the AP will steer dual band capable client devices to 5GHz when the RSSI value of these client devices on 5GHz radio is more than set one. To evenly allocate RF resource on the both 2.4GHz and 5GHz radios, users also can set the portion of client devices on 5GHz radio to assure smoothly connection. The default value of the 5GHz radio is 75%.

**Save:** Click **Save** to confirm the changes.

This page displays the current status of the Wireless settings of this AP.

## 2.4 GHz/5 GHz Wireless Network

	2.4GHz	5GHz
Operation Mode	Access Point <input checked="" type="checkbox"/> Green	Access Point <input checked="" type="checkbox"/> Green
Wireless Mode	802.11 B/G/N	802.11 AC/N
Channel HT Mode	20MHz	40MHz
Channel	<a href="#">Configuration</a>	
Transmit Power	Auto	Auto
Data Rate	Auto	Auto
RTS/CTS Threshold (1 - 2346)	2346	2346
Client Limits	127 <input checked="" type="radio"/> Enable <input type="radio"/> Disable	127 <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)	
AP Detection	<a href="#">Scan</a>	<a href="#">Scan</a>
Distance (1-30km)	1 (0.6miles)	1 (0.6miles)

**Operation Mode:** Scrow down this list to select operation modes for implementing on this radio. The default operation mode is **Access Point** on base stations and Access Points and is **Client Bridge** on Client Premise Equipements (CPE). Meanwhile, EnGenius outdoor devices also support WDS modes for peer to peer or peer to peer to multi-peer connections.

**Wireless Mode:** Scrow down this list to select wireless broadcasting standard on 2.4GHz and 5GHz frequency bands.

**Channel HT Mode:** Scrow down this list to select bandwidth for operating under a frequency band. The default channel bandwidth is 20 MHz on 2.4GHz frequency radio and 40 MHz on 5GHz frequency radio. Considering the different applications, users can decide to implement a channel bandwidth to fulfill real applications. The larger the channel, the greater the transmission quality and speed.

**Transmit Power (Tx Power):** Default Tx power is Auto to obey regularatory power of each country.

**Channel:** Click Configuration button to open a new windows to configure channels for performing wireless service.

2.4GHz		5GHz	
All	None	All	None
1,6,11	1,4,8,11	U-NII-1	U-NII-2A
1,7	1,5,9	U-NII-2B	U-NII-3
Ch 01 : 2.412 GHz	Ch 02 : 2.417 GHz	Ch 36 : 5.180 GHz	Ch 40 : 5.200 GHz
Ch 03 : 2.422 GHz	Ch 04 : 2.427 GHz	Ch 44 : 5.220 GHz	Ch 48 : 5.240 GHz
Ch 05 : 2.432 GHz	Ch 06 : 2.437 GHz	Ch 52 : 5.260 GHz	Ch 56 : 5.280 GHz
Ch 07 : 2.442 GHz	Ch 08 : 2.447 GHz	Ch 60 : 5.300 GHz	Ch 64 : 5.320 GHz
Ch 09 : 2.452 GHz	Ch 10 : 2.457 GHz	Ch100 : 5.500 GHz	Ch104 : 5.520 GHz
Ch 11 : 2.462 GHz		Ch108 : 5.540 GHz	Ch112 : 5.560 GHz
		Ch132 : 5.660 GHz	Ch136 : 5.680 GHz
		Ch149 : 5.745 GHz	Ch153 : 5.765 GHz
		Ch157 : 5.785 GHz	Ch161 : 5.805 GHz

[Save](#) Save current setting(s)

## Wireless Security

The *Wireless Security* section lets you configure the AP's security modes

Wireless Security - 2.4GHz	
Security Mode	WEP ▾
Auth Type	Open System ▾
Input Type	Hex ▾
Key Length	40/64-bit (10 hex digits or 5 A ▾
Default Key	Key #1 ▾
Key #1	<input type="text"/>
Key #2	<input type="text"/>
Key #3	<input type="text"/>
Key #4	<input type="text"/>

**Security Mode:** Including WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you to use WPA2-PSK mode.

\* **Setting of WEP mode:**

**Auth Type:** Select **Open System** or **Shared Key**.

**Input Type:**

ASCII: Regular Text (recommended)

Hexadecimal Numbers (For advanced users)

**Key Length:** Select the desired option and ensure that wireless clients use the same setting. Your choices are 64, 128, and 152-bit password lengths.

**Default Key:** Select the Key you wish to be the default. Transmitted data is **ALWAYS** encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key.

**Encryption Key Number:** Enter the Key Value or values you wish to use. Only the Key selected as Default is required. The others are optional.

Wireless Security - 5GHz	
Security Mode	WPA-PSK ▼
Encryption	AES ▼
Passphrase	<input type="text"/>
Group Key Update Interval	3600

**\* Setting of WPA-PSK, WPA2-PSK and WPA-PSK Mixed (Pre-Shared Key):**

**Encryption:** You may select AES, TKIP or Both (TKIP+AES) to be the encryption type you would like. Please ensure that your wireless clients use the same settings.

**Passphrase:** Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

**Group Key Update Interval:** Specifies how often, in seconds, the Group Key changes. The default value is 3600.

Wireless Security - 5GHz	
Security Mode	WPA-Enterprise ▼
Encryption	AES ▼
Group Key Update Interval	3600
Radius Server	<input type="text"/>
Radius Port	1812 Default 1812
Radius Secret	<input type="text"/>
Radius Accounting	Disable ▼
Radius Accounting Server	<input type="text"/>
Radius Accounting Port	1813
Radius Accounting Secret	<input type="text"/>
Interim Accounting Interval	600

**\* Setting of WPA-Enterprise & WPA2-Enterprise (Pre-Shared Key):**

**Encryption:** Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

**Radius Server:** Enter the IP address of the Radius server.

**Radius Port:** Enter the port number used for connections to the Radius server.

**Radius Secret:** Enter the secret required to connect to the Radius server.

**Radius Accounting:** Enable or disable accounting feature.

**Radius Accounting Server:** Enter the IP address of the Radius accounting server.

**Radius Accounting Port** Enter the port number used for connections to the Radius accounting server.

**Radius Accounting Secret:** Enter the secret required to connect to the Radius accounting server.

**Interim Accounting Interval:** Specifies how often, in seconds, the accounting data sends.

**Note:** 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

# Wireless Advanced

## Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Wireless Traffic Shaping	
Enable Traffic Shaping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Download Limit	<input type="text" value="100"/> <input type="checkbox"/> Per User Mbps (1-999)
Upload Limit	<input type="text" value="100"/> <input type="checkbox"/> Per User Mbps (1-999)

**Enable Traffic Shaping:** Default is disable. You may check this option to enable Wireless Traffic Shaping per SSID.

**Download Limit:** Specifies the wireless transmission speed used for downloading.

**Upload Limit:** Specifies the wireless transmission speed used for uploading.

**Per User:** Check this option to enable wireless traffic shaping per user function. This function allow users to limit the maximum download / upload bandwidth for each client devices on this SSID.

**Save:** Click **Save** to confirm the changes.

## Fast Roaming

Enable the function to serve mobile client devices that roam from Access Point to Access Point. Some applications running on Client devices require fast re-association when they roam to a different Access Point

Please enter the settings of the SSID and initialize the Security mode to WPA enterprise, as well as to set the Radius Server firstly. Users can enable the Fast Roaming and implement the advanced search.

Please also set the same enterprise Encryption under the same SSID on other Access Points and enable the Fast Roaming. When the configuration is realized on different Access Point, the mobile client devices can run the voice service and require seamless roaming to prevent delay in conversation from Access Point to Access Point.

Fast Roaming 

Enable Fast Roaming

Enable  Disable

**Enable Fast Roaming:** Enable or disable fast roaming feature.

**Enable Advanced Search:** Enable or disable advanced search feature.

# Guest Network Settings

Adding a guest network to allow visitors to use the internet without giving out your office or company wireless security. You can add a guest network to each wireless network in the 2.4GHz frequencies and 5GHz frequencies.

Guest Network Settings

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
<input type="checkbox"/>	EnGenius-2.4GHz_GuestNet	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	EnGenius-5GHz_GuestNet	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Manual IP Settings

- IP Address	192.168.200.1
- Subnet Mask	255.255.255.0

Automatic DHCP Server Settings

- Starting IP Address	192.168.200.100
- Ending IP Address	192.168.200.200
- WINS Server IP	0.0.0.0

**SSID:** Specified the SSID for the current profile.. Choices given are: Disabled, Deny MAC in the list, or Allow MAC in the list.

**Hidden SSID:** Check this option to hide SSID from clients, If checked, this SSID will not appear in the AP detect.

**Client Isolation:** Click the appropriate radio button to allow or prevent communication between client devices.

**IP address:** The IP Address of this device.

**Subnet Mask:** The IP Subnet mask of this device.

**Starting IP Address:** The first IP Address in the range of the addresses by the DHCP server.

**Ending IP Address:** The last IP Address in the range of addresses assigned by the DHCP server.

# RSSI Threshold

## Fast Handover

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RSSI	<input type="text" value="-70"/> dBm (Range: -60dBm ~ -100dBm)

**Enable :** Enable the Fast Handover feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vicinity of that client to coordinate which of them should serve the client best.

**RSSI:** Enter the RSSI (Received Signal Strength Index) in order to determine the handover procedure which the current wireless link will terminate. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.

# Wireless MAC Filtering

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access EAP1750H. The default setting is: **Disable Wireless MAC Filter**.

**Note:** Only applicable in Access Point and WDS AP mode.

Wireless MAC Filter

ACL Mode: Disabled

MAC Address: [ ] . [ ] . [ ] . [ ] . [ ] . [ ] [ Add ]

No.	MAC Address
-----	-------------

**ACL (Access Control List) Mode:** Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Choices given are: Disabled, Deny MAC in the list, or Allow MAC in the list.

**MAC Address:** Enter the MAC address of the wireless client you wish to configure for.

**Add:** Click **Add** to add the MAC address to the MAC Address table.

**Delete:** Deletes the selected entries.

**Save:** Click **Save** to apply the changes.

# Wireless Advanced

This page allows you to configure advanced wireless settings for the EWS550AP/EWS510AP/EWS511AP. It is recommended that the default settings are used unless the user has experience with more advanced networking features.

## 2.4 GHz/5 GHz Wireless Advanced

	2.4GHz	5GHz
Operation Mode	Access Point <input type="checkbox"/> Green	Access Point <input type="checkbox"/> Green
Wireless Mode	802.11 B/G/N	802.11 A/N
Channel HT Mode	20/40 MHz	40 MHz
Extension Channel	Upper Channel	Lower Channel
Channel	Auto	Auto
Transmit Power	Auto	Auto
Data Rate	Auto	Auto
RTS / CTS Threshold (1 - 2348)	2348	2348
Client Limits	127 <input type="checkbox"/> Enable	127 <input type="checkbox"/> Enable
Aggregation	Enable <input type="checkbox"/> 32 Frames	Enable <input type="checkbox"/> 32 Frames
AP Detection	50000 Bytes(Max) <input type="button" value="Scan"/>	50000 Bytes(Max) <input type="button" value="Scan"/>

**Data Rate:** Select a data rate from the drop-down list. The data rate affects throughput of data in the EAP1750H. The lower the data rate, the lower the throughput, though transmission distance will be lowered as well.

**Transmit Power:** Sets the power output of the wireless signal.

**RTS/CTS Threshold:** Specifies the threshold package size for RTS/CTS. A smaller number causes RTS/CTS packets to be sent more often and in turn consumes more bandwidth.

**Distance:** Specifies the distance between Access Points and clients. Longer distances may drop high-speed connections.

**Aggregation:** Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes.

**Save:** Click **Save** to confirm the changes.

# Chapter 8

# Management



# MGMT VLAN Settings

## Management VLAN Settings

This page allows you to assign a VLAN tag to packets sent over the network. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

**Note:** Only applicable in Access Point and WDS AP modes.

Management VLAN Settings 

Status  Enable  Disable 4094

**Caution:** If you encounter disconnection issue during the configuration process, verify that the switch and the DHCP server can support the new VLAN ID and then connect to the new IP address.

**Management VLAN:** If your network includes VLANs, you can enable **Management VLAN ID** for packets passing through the Access Point with a tag.

**Save:** Click **Save** to confirm the changes or **Cancel** to cancel and return to previous settings.

**Note:** If you reconfigure the Management VLAN ID, you may lose your connection to this AP. Verify that the

DHCP server supports the reconfigured VLAN ID and then reconnect to this AP using the new IP address.

# Advanced Settings

## SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for a Simple Network Management Protocol (SNMP). SNMP is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) returns the data stored in their Management Information Bases.

SNMP Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read Write)	<input type="text" value="private"/>
Trap Destination	
- Port	<input type="text" value="162"/>
- IP Address	<input type="text"/>
- Community Name	<input type="text" value="public"/>
SNMPv3 Settings	
- Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
- Username	<input type="text" value="admin"/> (1-31 Characters)
- Authorized Protocol	<input type="text" value="MD5"/>
- Authorized Key	<input type="text" value="12345678"/> (8-32 Characters)
- Private Protocol	<input type="text" value="DES"/>
- Private Key	<input type="text" value="12345678"/> (8-32 Characters)
- Engine ID	<input type="text"/>

**SNMP Enable/Disable:** Enables or disables the SNMP feature.

**Contact:** Specifies the contact details of the device.

**Location:** Specifies the location of the device.

**Community Name (Read Only):** Specifies the password for the SNMP community for read only access.

**Community Name (Read/Write):** Specifies the password for the SNMP community with read/write access.

**Trap Destination Address:** Specifies the IP address of the computer that will receive the SNMP traps.

**Trap Destination Community Name:** Specifies the password for the SNMP trap community.

**SNMPv3:** Enables or disables the SNMPv3 feature.

**User Name:** Specifies the username for SNMPv3.

**Auth Protocol:** Selects the authentication protocol type: MDS or SHA.

**Auth Key:** Specifies the authentication key.

**Priv Protocol:** Selects the privacy protocol type: DES.

**Priv Key:** Specifies the privacy key for privacy.

**Engine ID:** Specifies the engine ID for SNMPv3.

**Apply Save:** Click **Apply Save** to apply the changes.

## CLI Settings

### CLI Setting

Status  Enable  Disable

### SSH Setting

Status  Enable  Disable

### HTTPS Settings

Status  Enable  Disable

HTTPS forward  Enable  Disable

**CLI:** The Command Line Interface (CLI) allows you to type commands instead of choosing them from a menu or selecting an icon.

**SSH:** Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.

**HTTPS:** Enable HTTPS to transfer and display web content securely. The Hypertext Transfer Protocol over SSL (Secure Socket Layer) is a TCP/IP protocol used by web servers to transfer and display web content securely.

## Email Alert

You can use the Email Alert feature to send messages to the configured email address when particular system events occur.

Note: Do **NOT** use your personal email address as it can unnecessarily expose your personal email login credentials. Use a separate email account made for this feature instead

### Email Alert

Status	<input checked="" type="checkbox"/> Enable
- From	<input type="text"/>
- To	<input type="text"/>
- Subject	[Email-Alert][ENS620EXT][88:...
Email Account	
- Username	<input type="text"/>
- Password	<input type="password"/> 
- SMTP Server	<input type="text"/> Port: 25
- Security Mode	None <input type="button" value="Send Test Mail"/>

**Apply** Apply saved settings to take effect

**Status:** Enable this function for further settings.

**From:** Enter the email address to show the sender of the email.

**To:** Enter the address to receive email alerts.

**Subject:** Enter the text to appear in the email subject line.

**Username:** Enter the username for the email account that will be used to send emails.

**Password:** Enter the password for the email account that will be used to send emails.

**SMTP Server:** Enter the IP address or hostname of the outgoing SMTP server.

**Port:** Enter the SMTP port number to use for outbound emails.

# Time Zone

## Time Setting

This page allows you to set the internal clock of the AP.

### Date and Time Settings

Manually Set Date and Time

Date:  /  /

Time:  :  (24-Hour)

Automatically Get Date and Time

NTP Server:

### Time Zone

Time Zone:

Enable Daylight Saving

Start:

End:

Apply saved settings to take effect

**Manually Set Date and Time:** Manually specify the date and time.

**Synchronize with PC:** Click this button to synchronize Date and time of this AP with the PC.

**Automatically Get Date and Time:** Select Automatically Get Date and Time and check whether you wish to enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.

**Time Zone:** Choose a time zone to implement the service for this AP.

**Enable Daylight Saving:** Check whether daylight savings applies to your area.

**Start:** Select the day, month, and time when daylight savings time starts.

**Enable Daylight Saving:** Select the day, month, and time when daylight savings times ends.

# Auto Reboot Settings

You can specify how often you wish to reboot the AP.

## Auto Reboot Setting

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Timer	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday
	<input type="text" value="0"/> : <input type="text" value="0"/>

**Auto Reboot Setting:** Enables or disables the Auto Reboot function.

**Timer:** Select the day and enter the time you would like to reboot automatically.

**Save:** Click **Save** to apply the changes.

# Wi-Fi Scheduler

The Wi-Fi Scheduler can be created for use in enforcing rules. For example, if you wish to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu and Fri while entering a Start time of 3pm and End Time of 8pm to limit access to these times.

## Wi-Fi Scheduler

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small>NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler</small>
Wireless Radio	2.4GHz ▾
SSID Selection	EnGenius330052_1-2.4GHz ▾
Schedule Templates	Choose a template ▾

	Day	Available	Duration
Schedule Table	Sunday	available ▾	00 : 00 ~ 24 : 00
	Monday	available ▾	00 : 00 ~ 24 : 00
	Tuesday	available ▾	00 : 00 ~ 24 : 00
	Wednesday	available ▾	00 : 00 ~ 24 : 00
	Thursday	available ▾	00 : 00 ~ 24 : 00
	Friday	available ▾	00 : 00 ~ 24 : 00
	Saturday	available ▾	00 : 00 ~ 24 : 00

**Status:** Enables or disables the Wi-Fi scheduler function.

**Wireless Radio:** Select 2.4 GHz or 5 GHz from the drop-down list for the preferred band type.

**SSID Selection:** Select a SSID from the drop-down list.

**Schedule Templates:** Select a schedule template from the drop-down list.

**Day(s):** Place a checkmark in the boxes for the desired days or select the **All Week** radio button to select all seven days of the week.

**Duration:** The Start Time is entered in two fields. The first box is for hours and the second box is for minutes. The End Time is entered in the same format as the Start time.

# Tools

## Ping Test Parameters

This page allows you to analyze the connection quality of the AP and trace the routing table to a target in the network.

Ping Test Parameters	
Target IP / Domain Name	<input type="text"/>
Ping Packet Size	<input type="text" value="64"/> Bytes
Number of Pings	<input type="text" value="4"/>
<input type="button" value="Start"/>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

Traceroute Test Parameters	
Target IP / Domain Name	<input type="text"/>
<input type="button" value="Start"/> <input type="button" value="Stop"/>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

**Target IP:** Enter the IP address you would like to search.

**Ping Packet Size:** Enter the packet size of each ping.

**Number of Pings:** Enter the number of times you wish to ping.

**Start Ping:** Click **Start Ping** to begin pinging the target device (via IP).

**Traceroute Target:** Enter the IP address or domain name you wish to trace.

**Start Traceroute:** Click **Start Traceroute** to begin the trace route operation.

## Speed Test Parameters / LED Control

This page allows you to implement speed test to realize the throughput of a target DUT.

### Speed Test Parameters

Target IP / Domain Name	<input type="text"/>
Time Period	<input type="text" value="20"/> Sec
Check Interval	<input type="text" value="5"/> Sec
IPv4Port	<input type="text" value="5001"/>
IPv6Port	<input type="text" value="5002"/>
<input type="button" value="Start"/>	

**Target IP / Domain Name:** Enter an IP address or domain name you wish to implement a speed test for realizing the variance on wireless speed.

**Time Period:** Enter the time in seconds that you would like the test to implement for and in how many intervals.

**IPv4/IPv6 Port:** This Access Points uses IPv4 5001 and IPv6 5002 port for the speed test.

**Start:** Click start to implement speed test.

## LED Control

Control LED on/off for Power, LAN interface, or 2.4 GHz/5 GHz WLAN interface.

### LED Control

Power	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WLAN-2.4GHz	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WLAN-5GHz	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> Apply saved settings to take effect	

**Power:** Enables or disables the Power LED indicator.

**LAN:** Enables or disables the LAN LED indicator.

**WLAN-2.4 GHz:** Enables or disables the WLAN-2.4 GHz LED indicator.

**WLAN-5 GHz:** Enables or disables the WLAN-5 GHz LED indicator.

## Device Discovery

This page allows you to discover devices from network for Operation Mode, IP Address, System MAC Address and Firmware version.

### Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version
-------------	----------------	------------	--------------------	------------------

Scan

# Account

This page allows you to change the AP username and password. By default, the username is: **admin** and the password is: **admin**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.

## Account Settings

### Account Settings

Administrator Username	<input type="text"/>
Current Password	<input type="password"/> 
New Password	<input type="password"/> 
Verify Password	<input type="password"/> 

**Administrator Username:** Enter a new username for logging in to the New Name entry box.

**Current Password:** Enter the old password for logging in to the Old Password entry box.

**New Password:** Enter the new password for logging in to the New Password entry box.

**Verify Password:** Re-enter the new password in the Confirm Password entry box for confirmation.

**Apply:** Click **Apply** to apply the changes.

# Firmware

## Firmware Upgrade

This page allows you to upgrade the firmware of the AP.

### Firmware Upgrade

Current Firmware Version: 1.0.0

Select the new firmware from your hard disk.

<input type="text"/>	<input type="button" value="瀏覽"/>	<input type="button" value="Upload"/>
----------------------	-----------------------------------	---------------------------------------

### To Perform the Firmware Upgrade:

1. Click the **Choose File** button and navigate the OS file system to the location of the upgrade file.
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the **Upload** button to commence the firmware upgrade.

**Note:** The device is unavailable during the Firmware upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

# Backup/Restore

This page allows you to save the current device configurations. When you save your configurations, you also can reload the saved configurations into the device through the Restore Saved Settings from a file section. If extreme problems occur, or if you have set the AP incorrectly, you can use the **Reset** button in the Revert to Factory Default Settings section to restore all the configurations of the AP to the original default settings.

**Backup Setting:** Click **Export** to save the current configured settings.

**Restore New Setting:** To restore settings that have been previously backed up, click **Browse**, select the file, and click **Restore**.

**Restore to Default:** Click **Reset** button to restore the AP to its factory default settings.

## Backup/Restore Settings

Factory Setting	
- Backup Setting ⓘ	Export
- Restore New Setting	選擇檔案 未選擇任何檔案 Import
- Reset to Default ⓘ	Reset
User Setting	
- Back Up Setting as Default	Backup
- Restore to User Default ⓘ	Restore
<b>- Caution:</b> Please write down your account number and password before saving. The user settings will now become the new default settings at the next successful login.	

## User Setting

The function allows you to backup the current device configurations into the AP as the default value. If extreme problems occur, or if you have set the AP incorrectly, you can push the Reset button to revert all the configurations of the AP to the user default.

**Back Up Setting as Default:** Click **Backup** to backup the user settings you would like to the device's memory for the default settings.

**Restore to User Default:** Click **Restore** to restore user settings to the factory standard settings.

**Note1:** After setting the current settings as the default, you should click the **Restore to Default** on the web interface for reverting the settings into the factory default instead of pushing the reset button.

**Note2:** Please **write down** your account and password before saving. The user settings will now become the new default settings at the next successful login.

# Log

## System Log

The AP automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **Log** link under the System Manager menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

**System Log**

Status  Enable  Disable

Log type

Refresh

Clear

```
Tue Jul 12 12:20:01 2016 cron.info crond[4186]: crond: USER root pid 7926 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:18:01 2016 cron.info crond[4186]: crond: USER root pid 7915 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:16:01 2016 cron.info crond[4186]: crond: USER root pid 7904 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:14:01 2016 cron.info crond[4186]: crond: USER root pid 7893 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:12:01 2016 cron.info crond[4186]: crond: USER root pid 7882 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:10:01 2016 cron.info crond[4186]: crond: USER root pid 6070 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:08:01 2016 cron.info crond[4186]: crond: USER root pid 6045 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:06:01 2016 cron.info crond[4186]: crond: USER root pid 6034 cmd /etc/init.d/system start ntp_
Tue Jul 12 12:04:01 2016 cron.info crond[4186]: crond: USER root pid 6023 cmd /etc/init.d/system start ntp_
```

**Status:** Enable/Disable this function.

- ALL
- Debug
- Information
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

**Log type:** You may choose one of log types to display logs in the following window. The default log types is All.

Remote Log  Enable  Disable

Log Server IP Address

## Remote Log

This page allows you to setup the Remote Log functions for this AP.

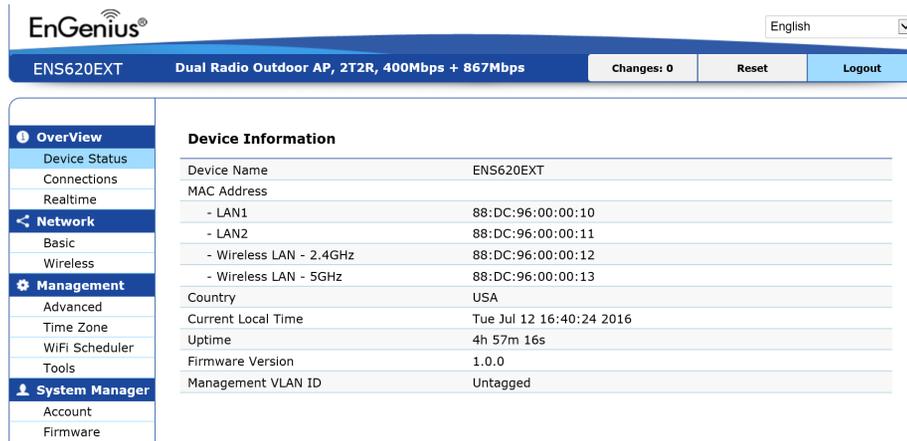
**Remote Log:** Enable/Disable this function.

**Log Server IP Address:** Enter the IP address of the log server.

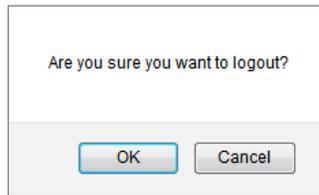
**Apply:** Click **Apply** to apply the changes.

# Logout

Logout: Click Logout in Management menu to logout.

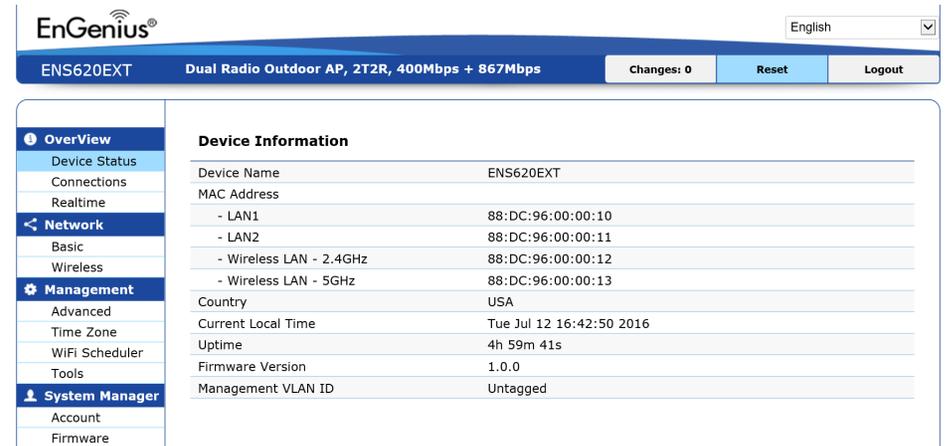


Please confirm again to logout the system or not.



# Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reset** to reboot the AP.



Once you click reset button, you will see the options for reboot or restore this AP.

Reboot the device: Click it to reboot this device.

Restore to Factory Default: Click it to reset this device to factory default setting.

Restore to User Default: Click it to reset this device to user default settings. For realizing the setting method, you may refer page 66 and page 67.

## Reboot the device

**Caution:** Pressing this button will cause the device to reboot.

Reboot the device

## Restore the device to default settings

**Caution:** All settings will be cleared and reset to either factory default or user default.

Restore to Factory Default

Restore to User Default

# Appendix



# Appendix A

## Federal Communication Commission Interference Statement

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

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



### **FCC Caution:**

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

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

## **IMPORTANT NOTE:**

### **Radiation Exposure Statement**

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operation of this device is restricted to indoor use only.

# Appendix B - IC Interference Statement

## Industry Canada Statement

This device complies with RSS-247 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.



### Caution:

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.
- (iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.



### Avertissement:

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.
- (iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

## **FOR MOBILE DEVICE USAGE Radiation Exposure Statement**

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

## **Pour l'utilisation de dispositifs mobiles) Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.

# Appendix C - CE Interference Statement

## Europe - EU Declaration of Conformity

This device complies with Directive 2014/53/EU issued by the Commission of the European Community.

- Declaration of Conformity

Please added certification standard in your user manual which depended on the test standards your device performed. or

- If the DoC should be a simplified version, please take below as reference –

Hereby, EnGenius Networks declares that the EWS550AP/EWS510AP/EWS511AP are in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

Importer: EnGenius Networks Europe B.V.

Importer Address: ESP 240, 5633 AC Eindhoven, The Netherlands

Manufacturer : EnGenius Networks. Inc.

Manufacturer Address: No.500, Fusing 3rd Rd., Hwa-Ya Technology Park Kuei-Shan Dist., Taoyuan City, Taiwan (R.O.C.)

CE DoC Link: <https://www.engeniusnetworks.eu/ens500ext-ac-ens500-ac-enstation5-accedoc>