EnGenius®

User Manual

EAP 11AC Series
version 1.3

Dual Band Indoor Ceiing Mount Access Point

IMPORTANT

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

Table of Contents

Chapter 1
Product Overview

Introduction - EAP1750H

Key Features

- High transmit power, enabling long range connectivity

- Supports IEEE802.11ac/b/g/n wireless standards with up to 450 Mbps data rate on 2.4GHz and 1300Mbps data rate on 5GHz

- Three internal 5 dBi (2.4 GHz) and three 5dBi (5 GHz) omni-directional MIMO antennas

- Can be monitored after deployment with EnGenius EZ Controller™ software for Windows (Free online download)

- Can be used with included power adapter or via PoE with PoE 802.3at - capable Switches or Injectors

- Dual Band/Three Stream

- Advanced Traffic shaping can be assisted users to control upload/ download wirelss speed per SSID

- Band Steering shifts dual band clients to the 5 GHz band for to relieve network congestion on the 2.4 GHz band

- Secured Guest Network

can be used with
802.3at
capable switches or injectors

Introduction

The EAP1750H leverages the breakthrough speed and performance 802.11ac for connecting to laptops and other devices that need to wirelessly stream HD video or transfer large files. The EAP1750H is an 802.11ac 3x3 Indoor Access Point. This high-powered ceiling mount Dual Band Access Point features speeds up to 450 Mbps on 2.4 GHz and up to 1300 Mbps on the 5 GHz band when associated with AC client devices. It can be configured as an Access Point, Repeater and WDS (AP & Bridge) and features a high transmit RF power of 28 dBm transmit RF power on the 2.4 GHz band and 28 dBm on the 5 GHz band for long range connectivity. The EAP1750H includes a Gigabit Ethernet port for connecting to 802.3at-capable PoE Switches and an enhanced receive sensitivity MIMO (Multiple In / Multiple

Out) integrated sectorized 3D antenna array. It's an ideal solution for spacious interior environments such as large homes, small and medium-sized businesses, multiple-floor buildings, hotels, hospitals, and other venues.

System Requirements

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

- Computer with an Ethernet interface or wireless network capability

- Windows OS (7, 8, 10), Mac OS, or Linux-based operating systems

- Web-Browsing Application (i.e. : Edge, Internet Explorer, Firefox, Chrome, Safari, or another similar browser application)

Package Contents

The EAP1750H/EAP1300 package contains the following items (all items must be in package to issue a refund):

- One Access Point

- 12V Power Adapter

- RJ-45 Ethernet Cable

- Quick Installation Guide

- Ceiling and Wall Mount Screw kit

- T-Rail Mounting kit

- Mounting Bracket

The EAP1250 package contains the following items (all items must be in package to issue a refund):

- One Access Point

- 12V Power Adapter

- Quick Installation Guide

- Wall Mount screw set

- T-Rail Mounting kit (9/16" and 15/16")

* The 3-Pack package is provided the optional adapter for purchasing.

Introduction - EAP1300 (EXT)

Key Features

- High transmit power, enabling long range connectivity

- Supports IEEE802.11ac wave2/b/g/n wireless standards with up to 400 Mbps data rate on 2.4GHz and 867Mbps data rate on 5GHz

- Two internal 4 dBi (2.4 GHz) and two 5dBi (5 GHz) omni-directional MIMO antennas (EAP1300)

- Two RP-SMA 6 dBi (2.4 GHz) and two RP-SMA5dBi (5 GHz) omni-directional MIMO antennas(EAP1300EXT)

- Support Wave 2 MU-MIMO function on 5GHz radio.

- Support Tx Beamforming to enlarge the transmitting distance.

- Can be monitored after deployment with EnGenius ezMaster from local side and remote end side easil.

- Can be used with included power adapter or via PoE with PoE 802.3af/at - capable Switches or Injectors

- Advanced Traffic shaping can be assisted users to control upload/download wirelss speed per SSID / per user

- Band Steering shifts dual band clients to the 5 GHz band for to relieve network congestion on the 2.4 GHz band

- Secured Guest Network option available

Introduction

The AP is 802.11 ac wave2/a/b/g/n Outdoor Access Point with speeds up to 400 Mbps on 2.4GHz and 867Mbps on 5GHz band. It can be configured as an Access Point, Repeater or WDS (AP, Station & Bridge). The AP is an affordable solution which is built in high-powered radios and long-range settings to replace the ordinary Access Points that do not have the range and reach to connect to a growing number of wireless users. With Wave2 features, the Access Point could reduce the handling period on client devices and network with more client devices at the same time.

Introduction - EAP1250

Key Features

- High transmit power, enabling long range connectivity

- Supports IEEE802.11ac wave2/b/g/n wireless standards with up to 400 Mbps data rate on 2.4GHz and 867Mbps data rate on 5GHz

- Support Wave 2 MU-MIMO function on 5GHz radio.

- Support Tx Beamforming to enlarge the transmitting distance.

- Can be monitored after deployment with EnGenius ezMaster from local side and remote end side easil.

- Can be used with included power adapter or via PoE with PoE 802.3af/at - capable Switches or Injectors

- Advanced Traffic shaping can be assisted users to control upload/ download wirelss speed per SSID / per user

- Band Steering shifts dual band clients to the 5 GHz band for to relieve network congestion on the 2.4 GHz band

- Secured Guest Network option available

Introduction

The AP is 802.11 ac wave2/a/b/g/n Outdoor Access Point with speeds up to 400 Mbps on 2.4GHz and 867Mbps on 5GHz band. It can be configured as an Access Point, or WDS (AP, Station & Bridge). The AP is an affordable solution which is built in high-powered radios and long-range settings to replace the ordinary Access Points that do not have the range and reach to connect to a growing number of wireless users. With Wave2 features, the Access Point could reduce the handling period on client devices and network with more client devices at the same time.

Technical Specifications - EAP1750H

Standard:
IEEE802.11b/g/n on 2.4 GHz
IEEE 802.11ac/a/n on 5 GHz
IEEE802.3at

Physical Interface
1 x 10/100/1000 Gigabit Ethernet Port
1 x Reset Button
1 x Power Connector

LED Indicator
Power
WPS
WLAN (Wireless Connection)
LAN

Power Requirements
External Power Adapter
DC IN, 12V/2A
Active Ethernet (Power-over-Ethernet)
802.3at PoE Input

Operation Modes
Access Point
WDS AP
WDS Bridge
Repeater (Available in December, 2017)

Security
WEP (64/128bit)
WPA/WPA2 (TKIP/AES)
Hidden SSID
MAC address filtering, up to 32 fields per SSID

L2 Isolation
802.1X Authenticator (MD5/TLS/TTLS/PEAP)
Guest Network

QoS (Quality of Service)
WMM (Wireless Multimedia)

Wireless Management
Web interface (HTTP/HTTPS)
SNMP v1/v2c/v3 with MIB I/II and private MIB
CLI (Telnet/SSH)
Firmware Upgrade
Backup/Restore Settings
Save Configuration as Default
Auto Reboot
E-mail Alert/Syslog Notification

Physical Security
Kensington Security Slot

Physical/Environment Conditions
Operating:
Temperature: 32°F to 104°F (0°C to 40°C)
Humidity (Non-condensing): 90% or less
Storage:
Temperature: -4°F to 140°F (-20°C to 60 °C)
Humidity (Non-condensing): 90% or less

Technical Specifications - EAP1300(EXT)

Standard:
IEEE802.11b/g/n on 2.4 GHz
IEEE 802.11ac/a/n on 5 GHz
IEEE802.3af

Physical Interface
1 x 10/100/1000 Gigabit Ethernet Port
1 x Reset Button
1 x Power Connector

LED Indicator
Power
WPS
WLAN (Wireless Connection)
LAN

Power Requirements
External Power Adapter
DC IN, 12V/1A
Active Ethernet (Power-over-Ethernet)
802.3af/at PoE Input

Operation Modes
Access Point
WDS AP
WDS Bridge
Repeater (Available in December, 2017)

Security
WEP (64/128bit)
WPA/WPA2 (TKIP/AES)
Hidden SSID

MAC address filtering, up to 32 fields per SSID
L2 Isolation
802.1X Authenticator (MD5/TLS/TTLS/PEAP)
Guest Network

QoS (Quality of Service)
WMM (Wireless Multimedia)

Wireless Management
Web interface (HTTP/HTTPS)
SNMP v1/v2c/v3 with MIB I/II and private MIB
CLI (Telnet/SSH)
Firmware Upgrade
Backup/Restore Settings
Save Configuration as Default
Auto Reboot
E-mail Alert/Syslog Notification

Physical/Environment Conditions
Operating:
 Temperature: 32°F to 104°F (0°C to 40°C)
 Humidity (Non-condensing): 90% or less
Storage:
 Temperature: -4°F to 140°F (-20°C to 60 °C)
 Humidity (Non-condensing): 90% or less

Technical Specifications - EAP1250

Standard:

IEEE802.11b/g/n on 2.4 GHz

IEEE 802.11ac/a/n on 5 GHz

IEEE802.3af

Physical Interface

1 x 10/100/1000 Gigabit Ethernet Port

1 x Reset Button

1 x Power Connector

LED Indicator

Power Requirements

External Power Adapter

DC IN, 12V/1A

Active Ethernet (Power-over-Ethernet)

802.3af/at PoE Input

Operation Modes

Access Point

WDS AP

WDS Bridge

Security

WEP (64/128bit)

WPA/WPA2 (TKIP/AES)

Hidden SSID

MAC address filtering, up to 32 fields per SSID

L2 Isolation

802.1X Authenticator (MD5/TLS/TTLS/PEAP)

Guest Network

QoS (Quality of Service)

WMM (Wireless Multimedia)

Wireless Management

Web interface (HTTP/HTTPS)

SNMP v1/v2c/v3 with MIB I/II and private MIB

CLI (Telnet/SSH)

Firmware Upgrade

Backup/Restore Settings

Save Configuration as Default

Auto Reboot

E-mail Alert/Syslog Notification

Physical/Environment Conditions

Operating:

    Temperature: 32°F to 104°F (0°C to 40°C)

    Humidity (Non-condensing): 90% or less

Storage:

    Temperature: -4°F to 140°F (-20°C to 60 °C)

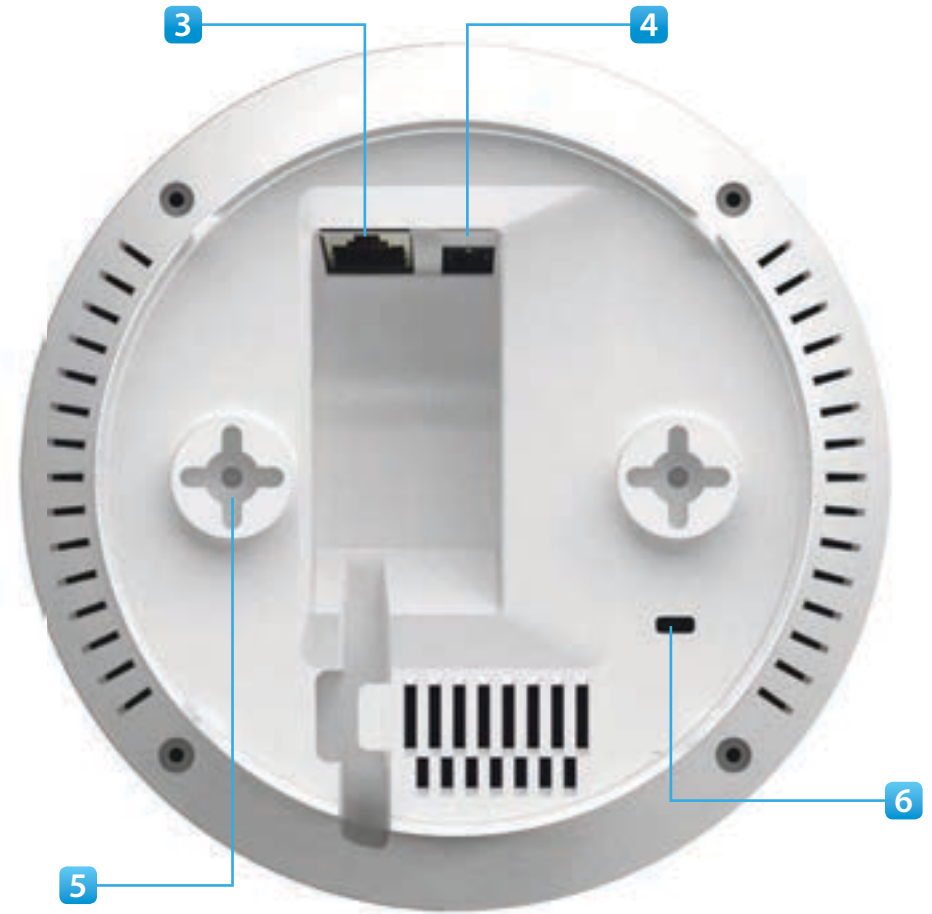   Humidity (Non-condensing): 90% or less

Physical Interface (EAP1750H/EAP1300(EXT))

Dimensions and Weights
Diameter: 6.36"
Height: 1.64"
Weight: 0.65 lbs.

1 **Reset Button:** Press and hold for **over** 10 seconds to reset to factory default settings.

2 **LED Indicators:** LED lights for WPS, WLAN 5GHz, WLAN 2.4GHz, Ethernet port, and Power

3 **LAN Port (PoE):** Ethernet port for RJ-45 cable.

4 **Power Connector:** 12V DC IN for Power.

5 **Ceiling (Wall) Mount Hole:** Using the provided hardware, the EAP AP can be attached to a ceiling or wall.

6 **Kensington Security Slot:** To protect your EAP1750H, use the Kensington Security Slot to attach a cable lock*. (EAP1750H Only)
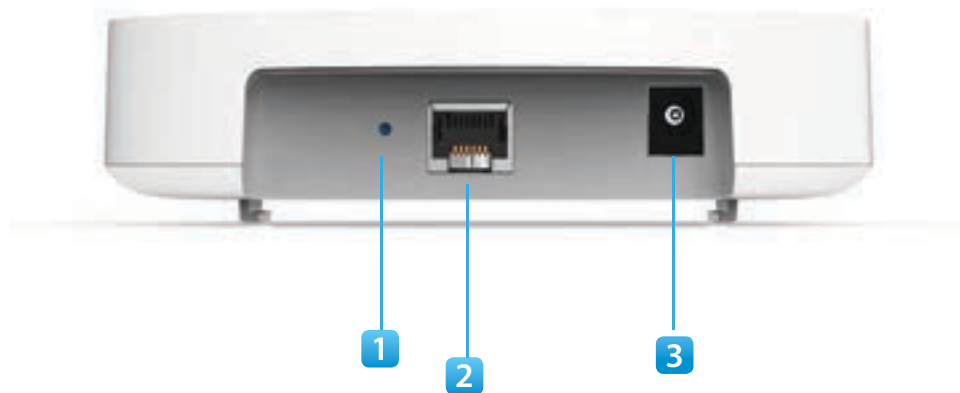
*cable lock not included

Physical Interface (EAP1250)

Dimensions and Weights
Diameter: 132.4mm (5.22")
Height: 37.4mm (1.47")
Weight: 220g (0.49 lbs.)

1 **Reset Button:** Press and hold for **over** 10 seconds to reset to factory default settings.

2 **LAN Port (PoE):** Ethernet port for RJ-45 cable.

3 **Power Connector:** 12V DC IN for Power.

4 **Ceiling (Wall) Mount Hole:** Using the provided hardware, the EAP AP can be attached to a ceiling or wall.

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**
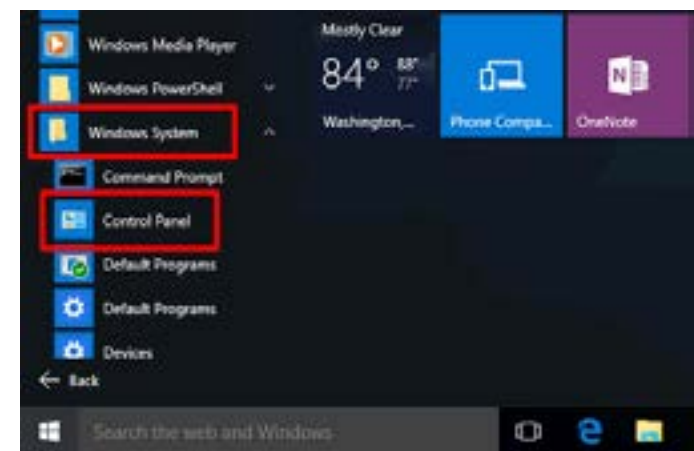

Windows XP   *Windows 7*

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.**
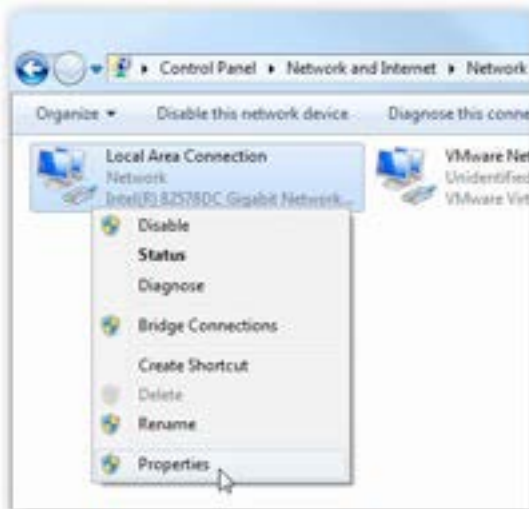

Windows 10

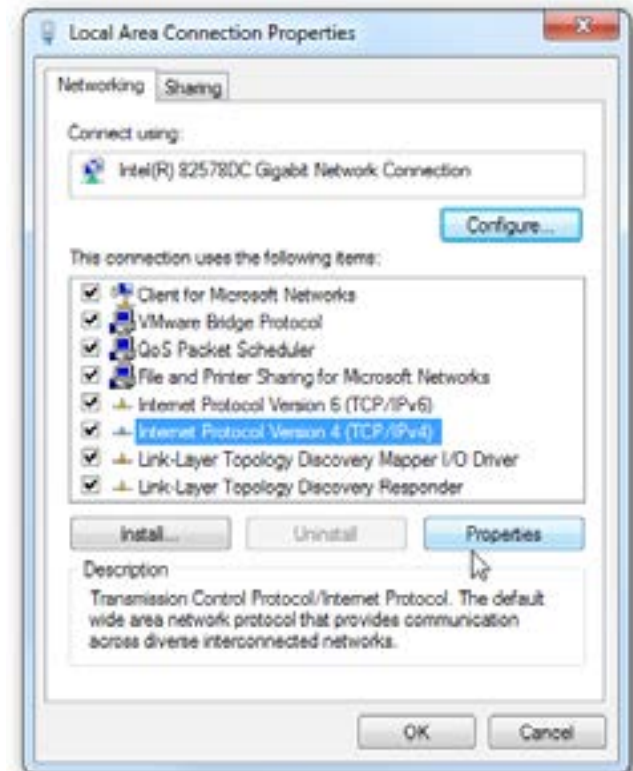**2a.** In **Windows XP,** click **Network Connections.**

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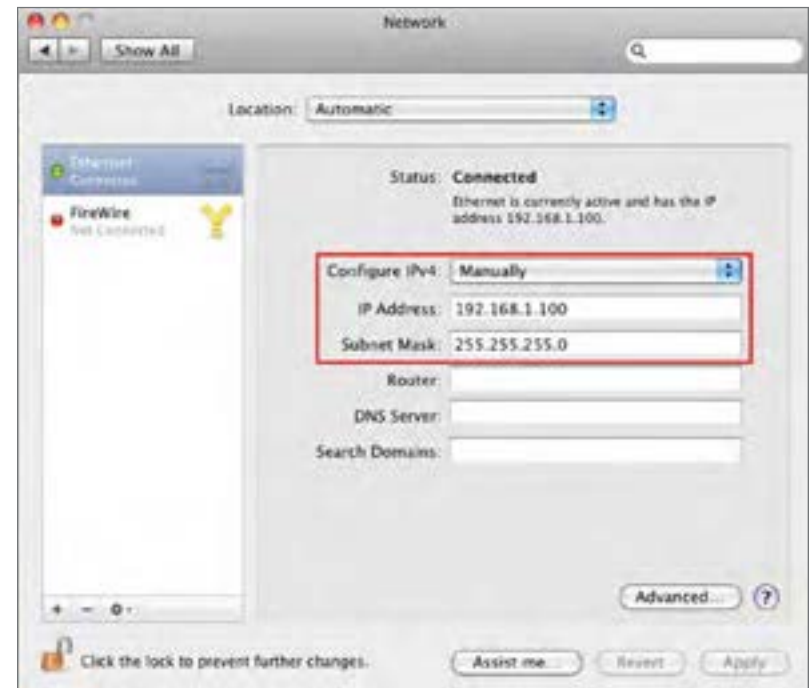
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

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 EAP1750H and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the EAP1750H and the computer.

3. Connect the Power Adapter DC connector to the DC-IN port of the EAP1750H 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 EAP1750H 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.

PC

Ethernet

AC/DC
Cable

Power
Outlet
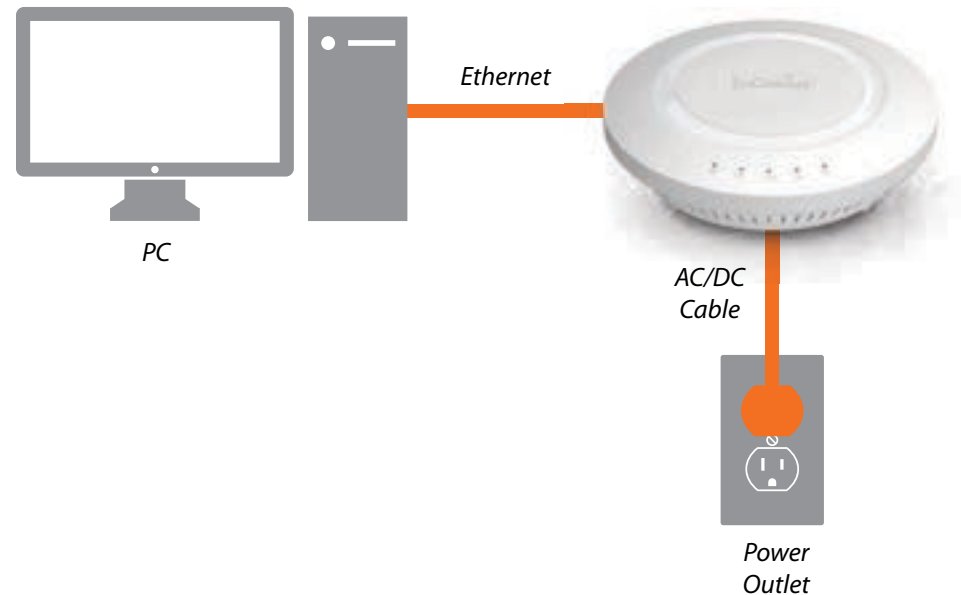
Mounting the EAP1750H / EAP1300(EXT)

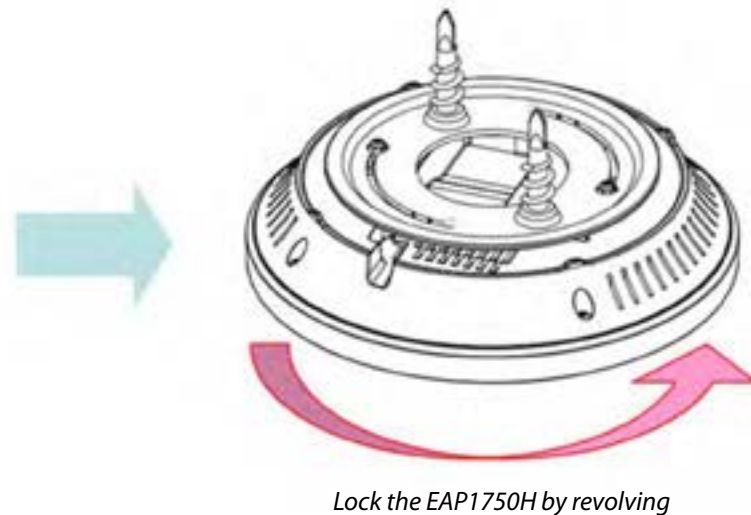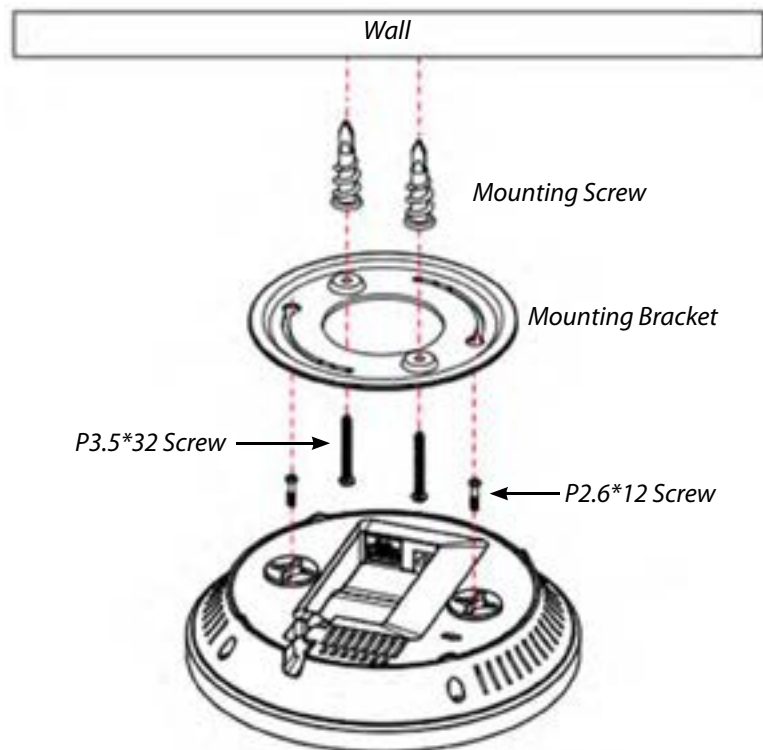Using the provided hardware, the EAP1750H/EAP1300 can be attached to a ceiling or wall.

To attach the EAP AP to a ceiling or wall using the mounting bracket:

1. Attach the mounting bracket to the wall or ceiling using the provided wall/ceiling mounting hardware kit.

2. Insert the provided short screws into the bottom cover of the EAP.

Leave enough of the screws exposed to ensure that the unit can be attached to the mounting bracket.

If extra space is required, use the provided spacers and long screws from the T-Rail mounting hardware kit to increase the space between the unit and the mounting bracket.

3. Mount the EAP on the mounting bracket by rotating the unit clockwise about 90 degrees to secure it in place.

Wall

Mounting Screw

Mounting Bracket

*P3.5*32 Screw*

*P2.6*12 Screw*

Lock the EAP1750H by revolving

Attaching the EAP1750H/EAP1300 to a ceiling using the provided T-Rail connectors:

1. Attach the T-Rail connectors to the bottom cover of the EAP using the provided short screws.

Note: Two sizes of T-Rail connectors are included in the mounting hardware kit: 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.
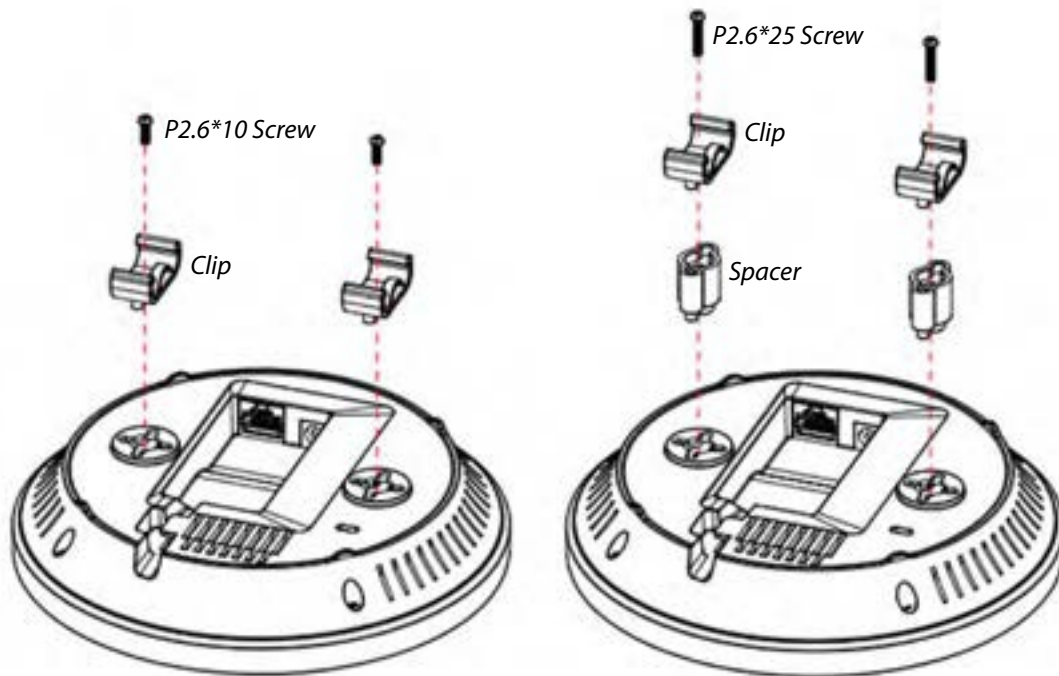
2. Line up the connected T-Rail connectors with an appropriately sized rail and press the unit onto the rail until it snaps into place.

Note: To protect your EAP, use the Kensington Security Slot to attach a cable lock (cable lock is not included).

P2.6*10 Screw
Clip

P2.6*25 Screw
Clip
Spacer
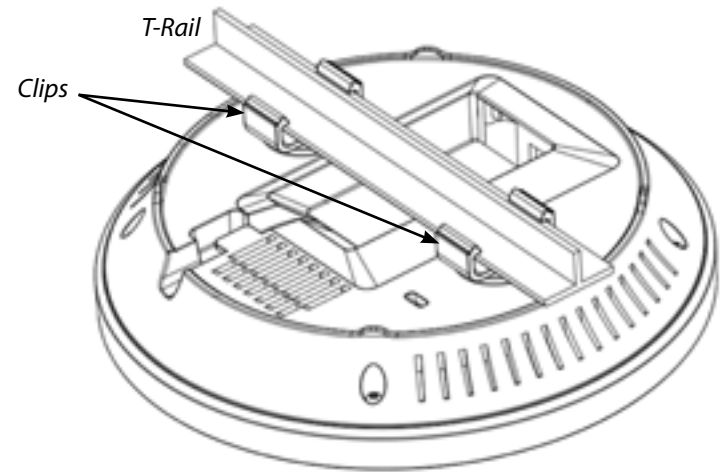
T-Rail
Clips

Attaching the EAP1250 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 EAP1250 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 diagram and 26mm depth holes in the markings and hammer the bolts into the openings.

4. Screw the anchors unto the holes until they are flush with the wall; screw the included screw into the achors.

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.

1

2

T-Rail

3

4

5
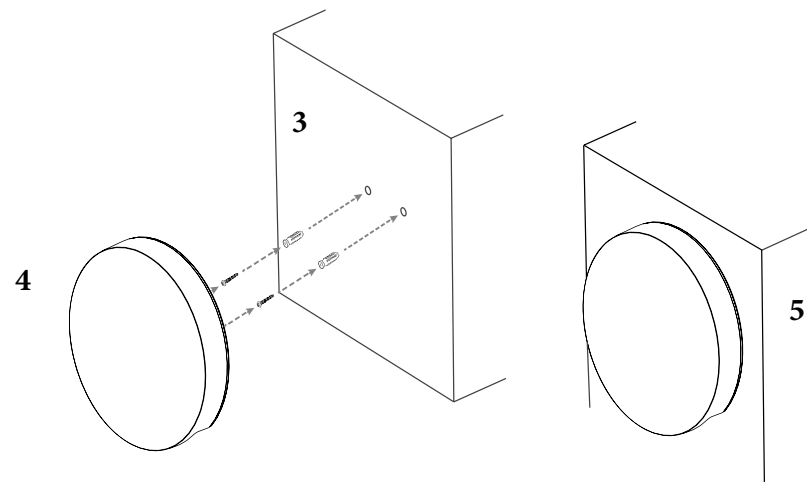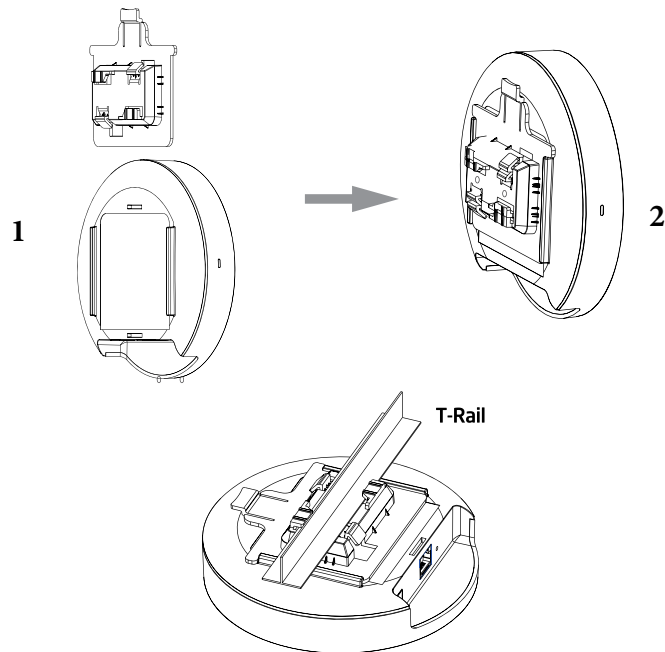
Chapter 3
Configuring Your Access Point

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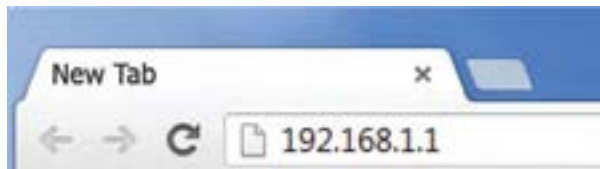
Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

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 EAP1750H has the ability to operate in various modes. This chapter describes the operating modes of the EAP1750H.

Access Point Mode

In Access Point Mode, the EAP1750H behaves like a central connection for stations or clients that support IEEE 802.11a/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 EAP1750H. The EAP1750H supports up to eight (8) SSIDs per band (16 total) at the same time for secure access.

WDS AP Mode

The EAP1750H also supports WDS AP mode. This operating mode allows wireless connections to the EAP1750H using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports up to four (4) AP MAC addresses.

WDS Bridge Mode

In WDS Bridge Mode, the EAP1750H can wirelessly connect different LANs by configuring the MAC address and security settings of each EAP1750H device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the EAP1750H to wirelessly connect two wired LANs, as shown in the following figure. WDS Bridge Mode can establish up to four (4) WDS links, creating a star-like network.

> **Note:** WDS Bridge Mode does **not** act as an Access Point because Access Points linked by WDS use the same frequency channel. More Access Points connected together may lower throughput. This configuration can also be susceptible to generate endless network loops in your network, so it is recommended to enable the Spanning Tree feature to prevent this from happening. You can find information about the Spanning Tree Function on page **29**.

Client
Computer

EAP1750H
WDS Bridge

Client
Computer

EAP1750H
WDS Bridge

Client
Computer

EAP1750H
WDS Bridge

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.

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.

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

- 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.

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
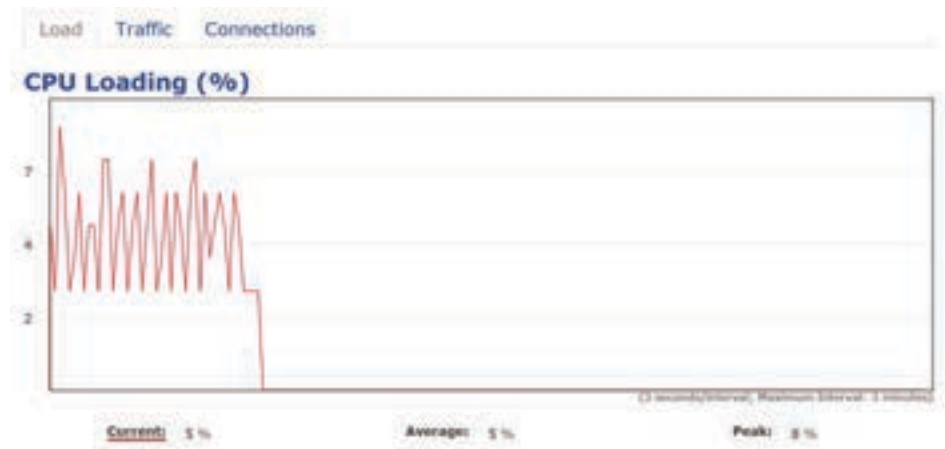
Traffic Loading: 2.4GHz and 5GHz and Ethernet port inbound and outbound traffic by current, average and peak time.
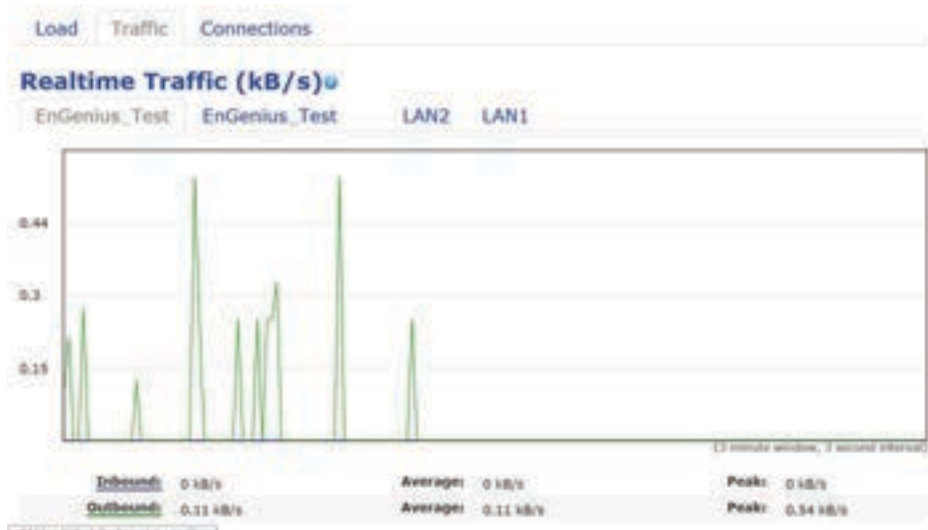
Realtime Connection (Pkts): Overview on current active network connections. It displays UDP and TCP packets information and other connection status. UDP connections curve is in blue; TCP connection curve is in green; others curve is in red. Below of chart shows connections source and destination.

Chapter 6
Network

Basic

IPv4/IPv6 Settings

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

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 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

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 welll as security settings must be the same. EnGenius Band Steering supports following advanced settings,

 ***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.

 ***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**: 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

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 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 regulartory power of each country.

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

Wireless Security

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

Secuirty 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	
Group Key Update Interval	3600

Wireless Security - 5GHz

Security Mode	WPA-Enterprise
Encryption	AES
Group Key Update Interval	3600
Radius Server	
Radius Port	1812 Default 1812
Radius Secret	
Radius Accounting	Disable
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

* 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.

* 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.

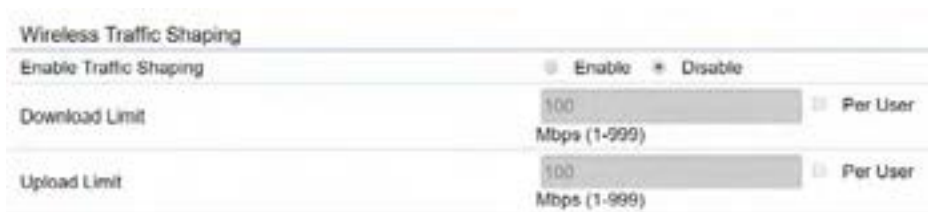**Interim Accounting Interval**: Specifies how often, in seconds, the accounting data sends.

> **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.

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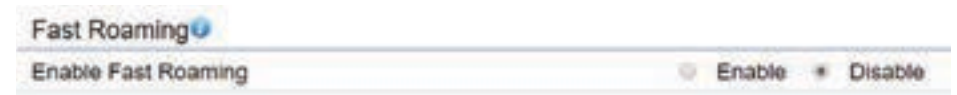
Enable Fast Roaming: Enable or disable fast roaming feature.

Enable Advanced Search: Enable or disable advanced search feature.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.
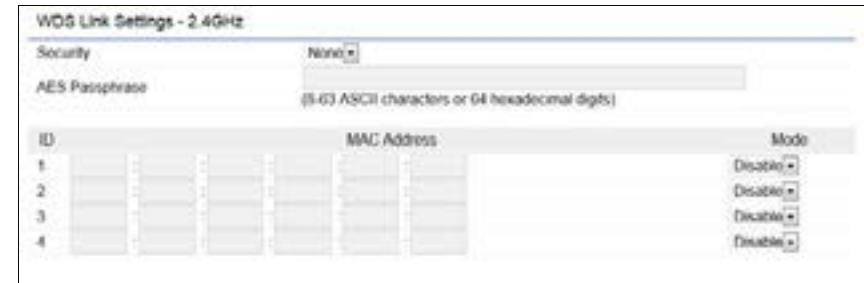
> **Note:** Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

> **Also note:** All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four Access Points.

> **Note:** Only applicable in WDS AP and WDS Bridge modes.
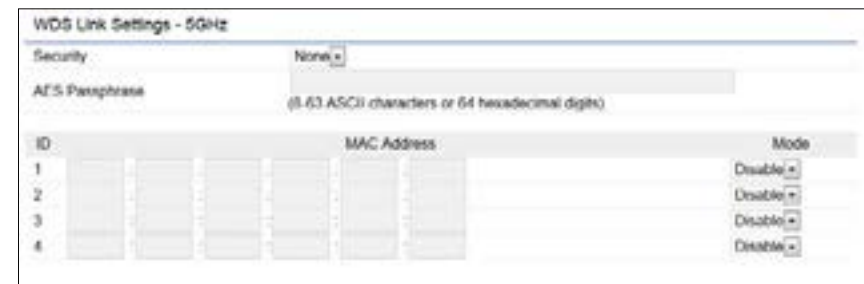
2.4 GHz/5 GHz WDS Link Settings

Security: Select **None** or **AES** from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

Mode: Select to disable or enable from the drop-down list.

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

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.

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	○ Enable ● Disable
RSSI	-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 vincinity 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.

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 EAP1750H. 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

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 RTC/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.

WPS (Wi-Fi Protected Setup)

The Wi-Fi Protected Setup (WPS) feature complies with the Wi-Fi Alliance WPS standard and makes it easier to quickly add client devices to an established, security-enabled Wi-Fi network.

WPS reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

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

WPS (Wi-Fi Protected Setup)

WPS: Select to enable or disable the WPS feature.

WPS Current Status: Shows whether the WPS feature is **Configured** or **Unconfigured.** When it is configured, the WPS has been used to authorize a connection between the device and wireless clients.

Self Pin Code: The PIN code for this device.

SSID: The SSID (wireless network name) used when connecting using WPS.

Authentication Mode: Displays the encryption method used by the WPS process.

Passphrase Key: This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempt to connect to the wireless network.

WPS via Push Button: Click the **Start** button to initialize the WPS feature using the Push Button method.

WPS via PIN: Enter the PIN code for the wireless device and click this button to initialize WPS feature using the PIN method.

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

WDS Link Settings

Using WDS (Wireless Distribution System) will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also Note: All Access Points in the WDS network must use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS network. There can be a maximum of four (4) Access Points.

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

2.4 GHz/5 GHz WDS Link Settings

Security: Select None or AES from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to which you want to extend the wireless area.

Mode: Select **Disable** or **Enable** from the drop-down list.

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: 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 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: 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

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.

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

Synchorize with PC: Click this button to synchorize 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.
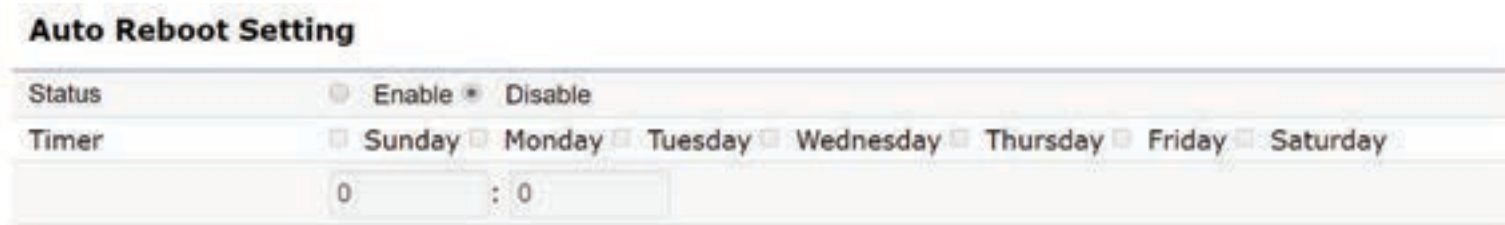
Enable Daylight Saving: Check whether daylight savings applies to your area.

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	○ Enable ● Disable						
Timer	☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday						
	0 : 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.

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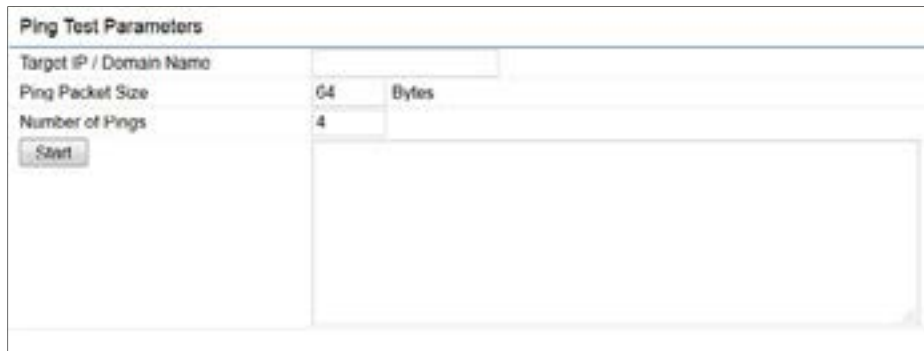
Day(s): Place a checkmark in the boxes for the desired days or select the **All Week** radio button to select all seven days of the week.

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.

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		
Time Period	20	Sec
Check Interval	5	Sec
IPv4Port	5001	
IPv6Port	5002	

Start

Target IP / Domain Name: Enter an IP address or domain name you wish to impelement 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	● Enable ○ Disable
LAN	● Enable ○ Disable
WLAN-2.4GHz	● Enable ○ Disable
WLAN-5GHz	● Enable ○ Disable

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

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.

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

- **Caution:** 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.
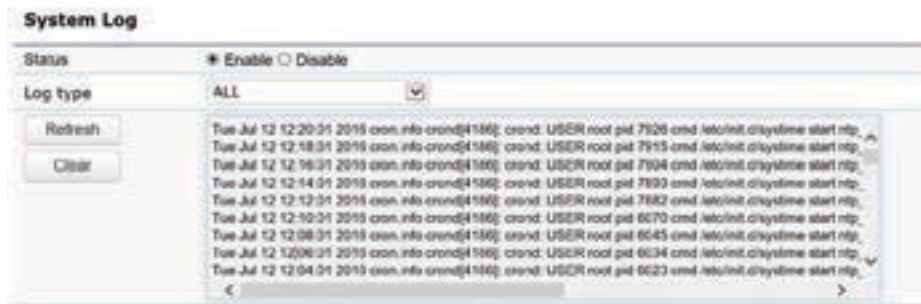
Status: Enable/Disable this function.
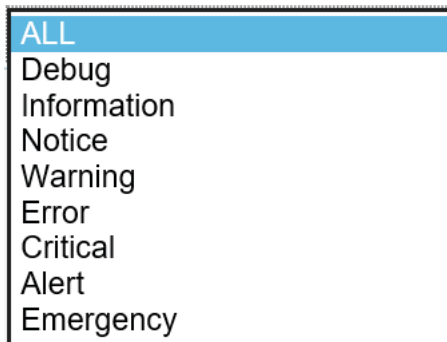
Log type: You may choose one of log types to display logs in the following window. The default log types is All.

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.
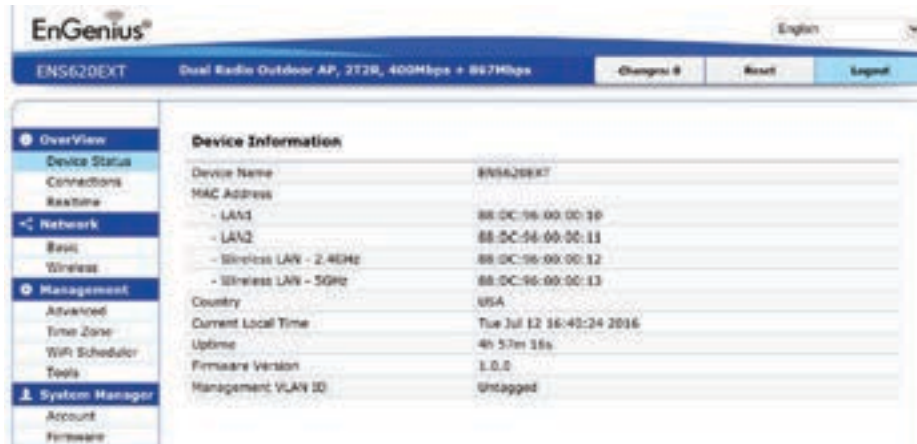
Please confirm again to logout the system or not.
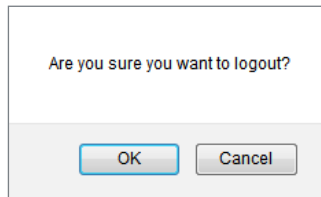
Reset

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.

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 EAP1750H/EAP1300/EAP1300EXT /EAP1250 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

Appendix D - DETACHABLE ANTENNA USAGE

This radio transmitter (IC: 10103A-EAP1300 / Model: EAP1300/EAP1300EXT) has been approved by ISED to operate with the antenna type listed below with maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 10103A-EAP1300 / Model: EAP1300/EAP1300EXT) a été approuvé par ISED pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Internal antenna

Type	PIFA				
Connecter	IPEX				
Gain (dBi)					
Frequency	2.4GHz			5GHz		
	4			5		

External antenna

Type	Dipole				
Connecter	RSMA				
Gain (dBi)					
Frequency (MHz)	2400	2410	2420	2430	2440	2450
	4.50	4.67	4.89	4.63	4.94	4.98
	2460	2470	2480	2490	2500	
	5.67	4.78	4.78	4.84	4.81	
	5000	5100	5150	5250	5350	5450
	3.55	3.70	3.01	3.32	3.76	4.31
	5550	5650	5725	5750	5800	5825
	4.85	4.99	4.86	4.48	4.46	4.71
	5850	5900	5950	6000		
	4.50	4.33	4.44	4.56		