EnGenius®

Business Solutions

User Manual

EWS385AP
version 1.0

Wireless Tri-Band Indoor 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.. 4

Key Features/Introduction.. 5

System Requirements / Package Contents 6

Technical Specifications.. 7

Physical Interface.. 9

Chapter 2 Before You Begin 10

Computer Settings.. 11

Mounting the Access Point.. 16

Chapter 3 Configuring Your Access Point........................ 18

Default Settings.. 19

Chapter 4 Building a Wireless Network........................... 20

Access Point Mode... 21

AP Mesh Mode.. 22

Chapter 5 Overview.. 23

Overview... 24

Connections... 26

Chapter 6 Network 28

Basic/IP Settings/SpanningTree Settings............................ 29

Chapter 7 2.4 GHz & 5 GHz Wireless................................. 31

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

Wireless MAC Filtering...41

Chapter 8 Management.. 43

Management VLAN Settings.. 44

Advanced Settings.. 45

Time Zone.. 48

Auto Reboot Settings.. 49

Wi-Fi Scheduler... 50

Tools.. 51

Account/Firmware.. 54

Backup/Restore 55

Log.. 57

Logout/Reset.. 58

Appendix 59

FCC Interference Statement.. 60

IC Interference Statement... 61

CE Interference Statement... 63

Chapter 1

Product Overview

Introduction - EWS385AP

Key Features

- Deploy and manage with ease using EWS Series Wireless Management Switches
- Supports IEEE802.11ac/a/b/g/n wireless standards
- Two 2.4 GHz Omni-directional antennas
- Two 5 GHz Omni-directional antennas
- Support Wave 2 MU-MIMO function on 5GHz radio.
- Support Tx Beamforming to enlarge the transmitting distance.
- IEEE802.11 PoE af Input design with Gigabits port supports.
- Flexible application by the built-in 2nd LAN port.
- More customized items on Band Steering for intellgent Management.
- Secured Guest Network option available

Introduction

EnGenius Wireless Management Access Point solution is designed for deploying on the versatile indoor application. To meet today’s requirement on varied net-working environment, EnGenius would like to provide the solution as flexible, robust and effective as the organization they desire.

The state-of-the-art 802.11ac and MU-MIMO technology brings revolutionary connecting speed and bandwidth for diversity of multimedia applications. EWS385AP equips with two powerful RF interfaces that support up to 867

Mbps + 867 Mbps in 5GHz frequency band and 400 Mbps in 2.4GHz frequency band (with 2ss/VHT40 clients).

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 (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 EWS385AP package contains the following items (all items must be in package to issue a refund):

- EWS Inddor Access Point
- Mounting Bracket (9/16" and 15/16"')
- Wall Mount screw set
- Quick Installation Guide

Technical Specifications - EWS385AP

Radio Specification

Dual Concurrent Radio:
-2.4GHz: 2400MHz ~ 2484MHz,
-Main 5GHz: 5725MHz~5850MHz
-Second 5GHz: 5150MHz~5250MHz,
Transmit Power:
- Max transmit power is limited by regulatory power

Radio Chains / Spatial Streams:
- 2 x 2 / 3

Supported Radio Technology:
- 802.11b: direct-sequence spread-spectrum (DSSS)
- 802.11a/g/n/ac: orthogonal frequency-division multiplexing (OFDM)

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

Supported Modulation:
- 802.11b: BPSK, QPSK, CCK
- 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-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 300 (MCS0 to MCS23)
- 802.11ac: 6.5 to 867 (MCS0 to MCS9)

Physical & Environment

Power Source:
- DC Input: DC12V/1A
- PoE: compatible with 802.3af

Internal Antenna
- 2 x 2.4GHz antennas
- 4 x 5GHz antennas

Interface:
- 2 x 10/100/1000Mbps Uplink Port with 802.3af/at PoE
- 1 x DC power connector
- 1 x Reset button

Dimensions:
20 x 20 x 4.5cm (7.87” x 7.87” x 1.77”)
Mounting:
- Wall mount, Ceiling mount

Environment:
- Operating temperature: 0°C~40°C
- Operating humidity: 0%~90% typical
- Storage temperature: -30°C~80°C

Wireless

Operating Mode:
- AP, Repeater, WDS

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

Technical Specifications - EWS385AP continued

QoS:
- Supports 802.11e/WMM

Band Steering

Mobility:
- PMKSA support for fast roaming

Security:
- WEP encryption: 64/128/152-bit
- 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)

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

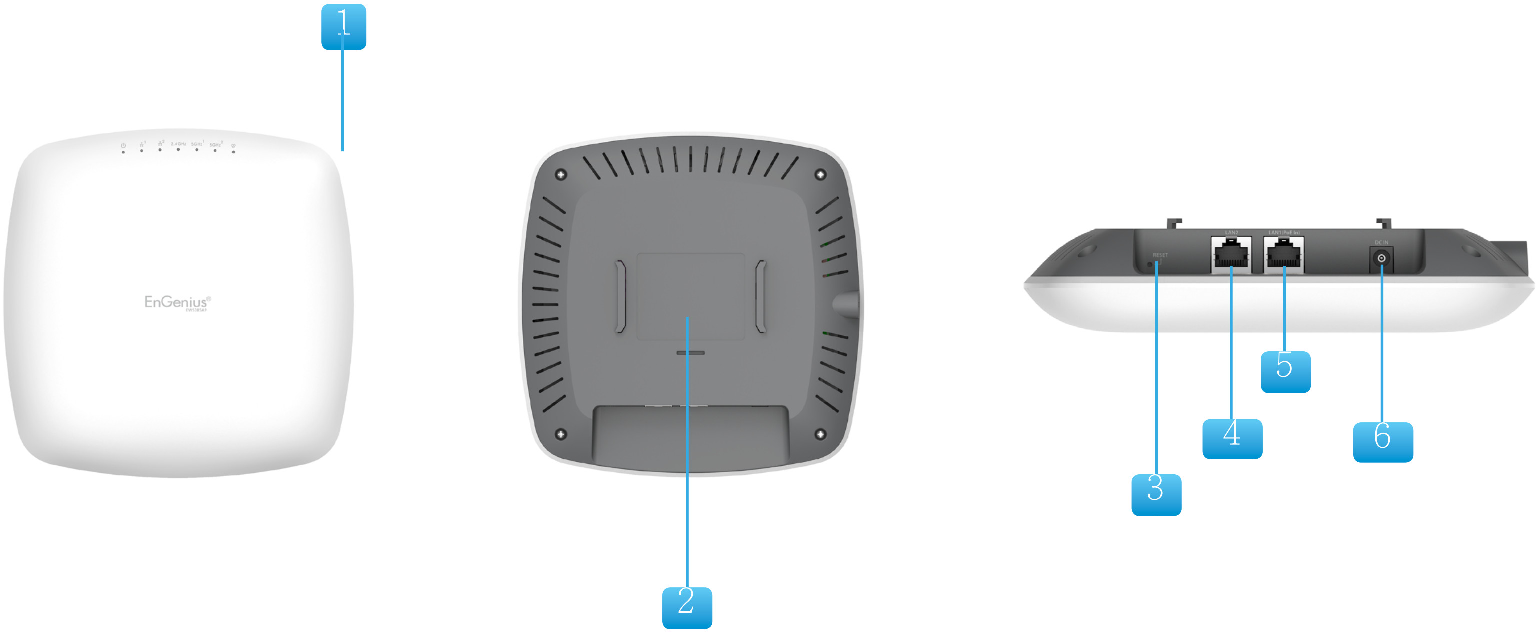
Firmware Upgrade
- Web interface or CLI (FTP/HTTP)

Backup / Restore Settings
- Revert to factory default settings

Schedule Reboot:
- Specifies interval to reboot system periodically

E-mail Alert / Syslog Notification

Physical Interface (EWS385AP)



1. LED Indicators: LEDs for Power, LAN-1, LAN-2, 2.4Hz, 5GHz-1, 5GHz-2, WAN.
2. Ceiling (Wall) Mount Hole: Using the provided hardware, the EWS385AP can be atached to a ceiling or wall.
3. Reset Button: Press and hold for over 10 seconds to reset to factory default settings.
4. LAN2 :10/100/1000 RJ45
5. LAN1 : 10/100/1000 RJ45 Uplink (PoE In)that supports 802.3af/at PoE input
6. DC-Jack 12V DC IN for Power

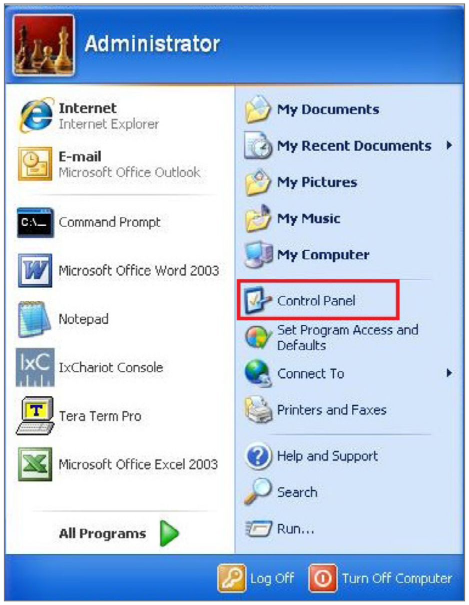
Chapter 2
Before You Begin

Computer Settings

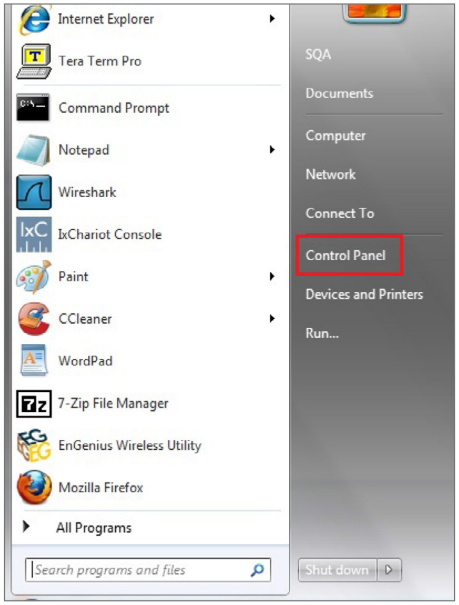
Windows XP/Windows 7/Windows 8/Windows 10

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

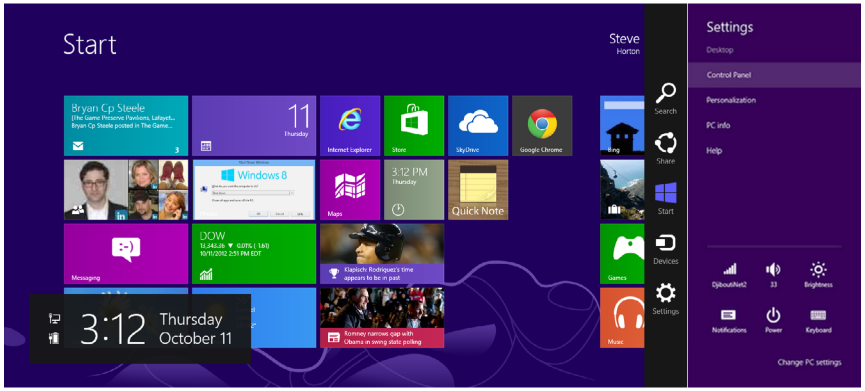


Windows XP



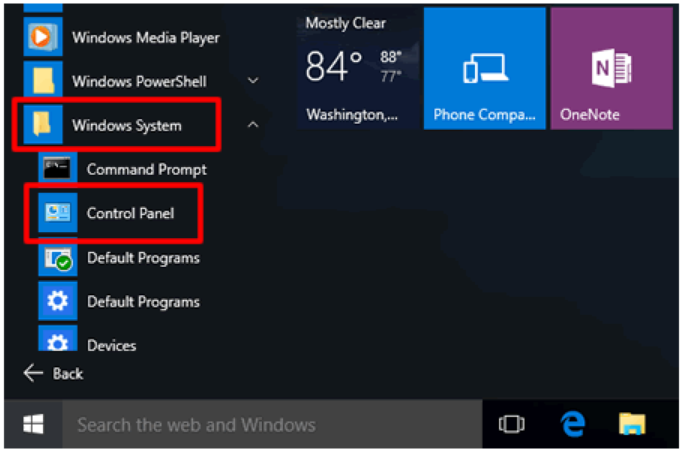
Windows 7

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



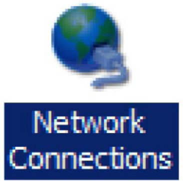
Windows 8

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

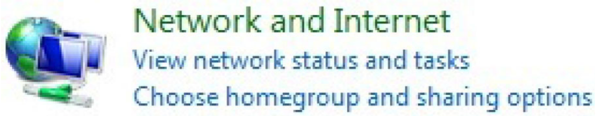


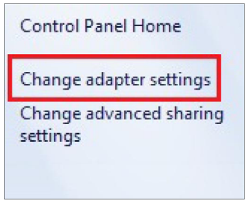
Windows 10

2a. In Windows XP, click Network Connections.

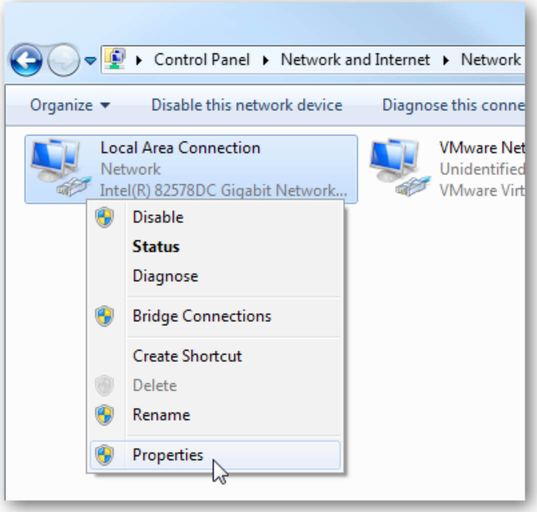


2b. In Windows 7/Windows 8/Windows 10, click View Network Status and Tasks in the Network and Internet section, then select Change adapter settings.

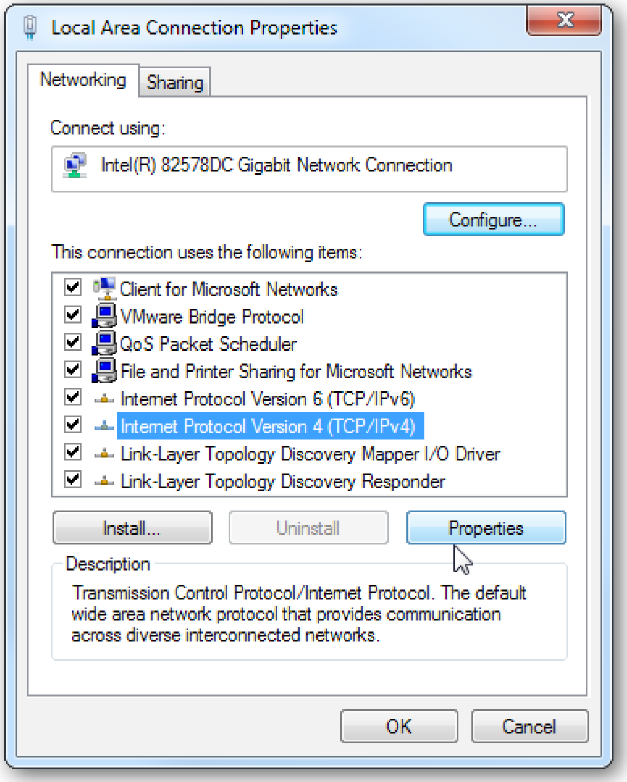

Network and Internet
View network status and tasks
Choose homegroup and sharing options



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



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



Connect using:

Intel(R) 82578DC Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

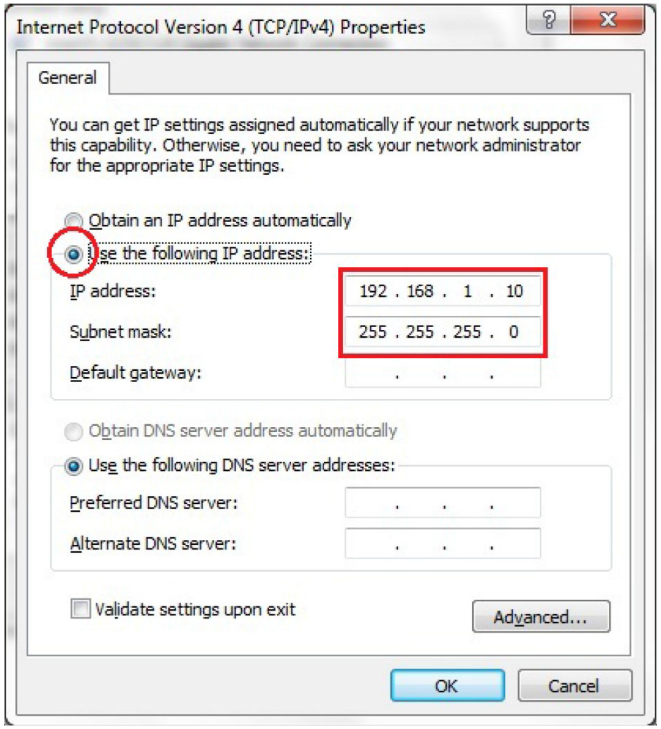
5. Select Use the following IP address and enter an IP address that is different from the Access Point and Subnet mask, then click OK.

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

PCIPaddress:192.168.1.2–192.168.1.255

PC Subnet mask: 255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

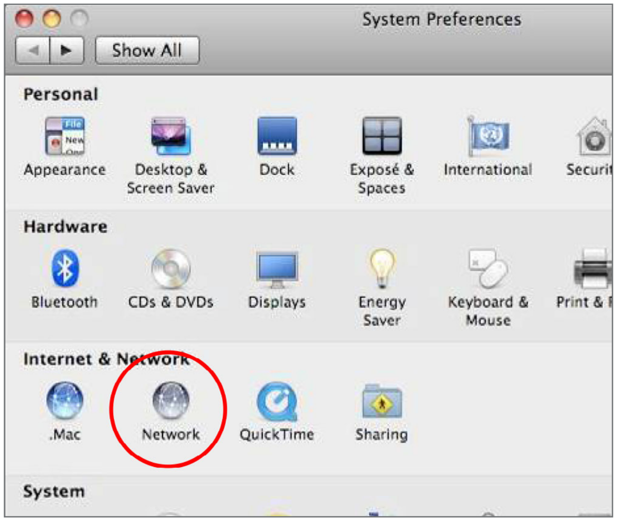
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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.



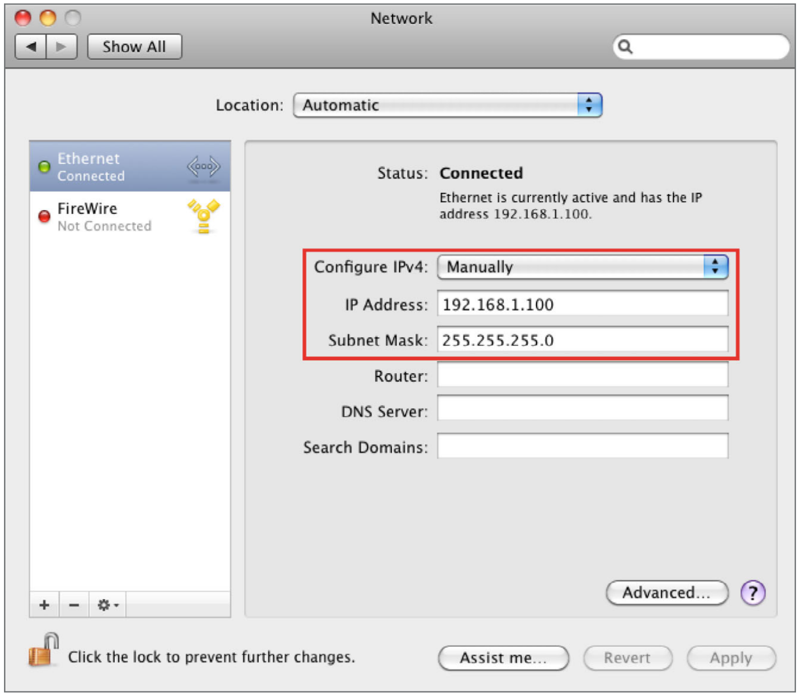
3. Highlight Ethernet.
4. In Configure IPv4, select Manually.
5. Enter an IP address that is different from the Access Point and Subnet mask then press OK.

   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.



Location: Automatic

Status: Connected

Ethernet is currently active and has the IP address 192.168.1.100.

Configure IPv4: Manually

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

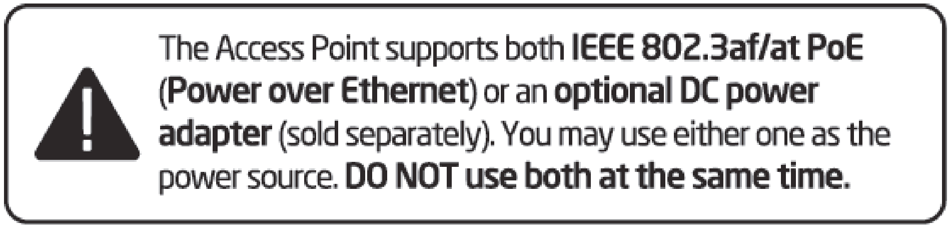
Router:

DNS Server:

Search Domains:

Hardware Installation

1. Connect one end of a RJ45 Ethernet cable to the PoE In (LAN/Uplink) port on the rear of the Access Point.
2. Connect the other end of the RJ45 Ethernet cable to a PoE Ethernet switch or the PoE Out port on the PoE injector.
3. Using another RJ45 Ethernet cable, connect one end to the Ethernet port on the computer, and connect the other end to another port on the PoE Ethernet switch or to the Data In port on the PoE injector.
4. Provide power to the PoE injector/switch.
5. Verify that the Power LED on the AP is steady orange.
6. Proceed to set up the Access Point using the computer.



⚠ The Access Point supports both **IEEE 802.3af/at PoE** (**Power over Ethernet**) or an **optional DC power adapter** (sold separately). You may use either one as the power source. **DO NOT use both at the same time.**

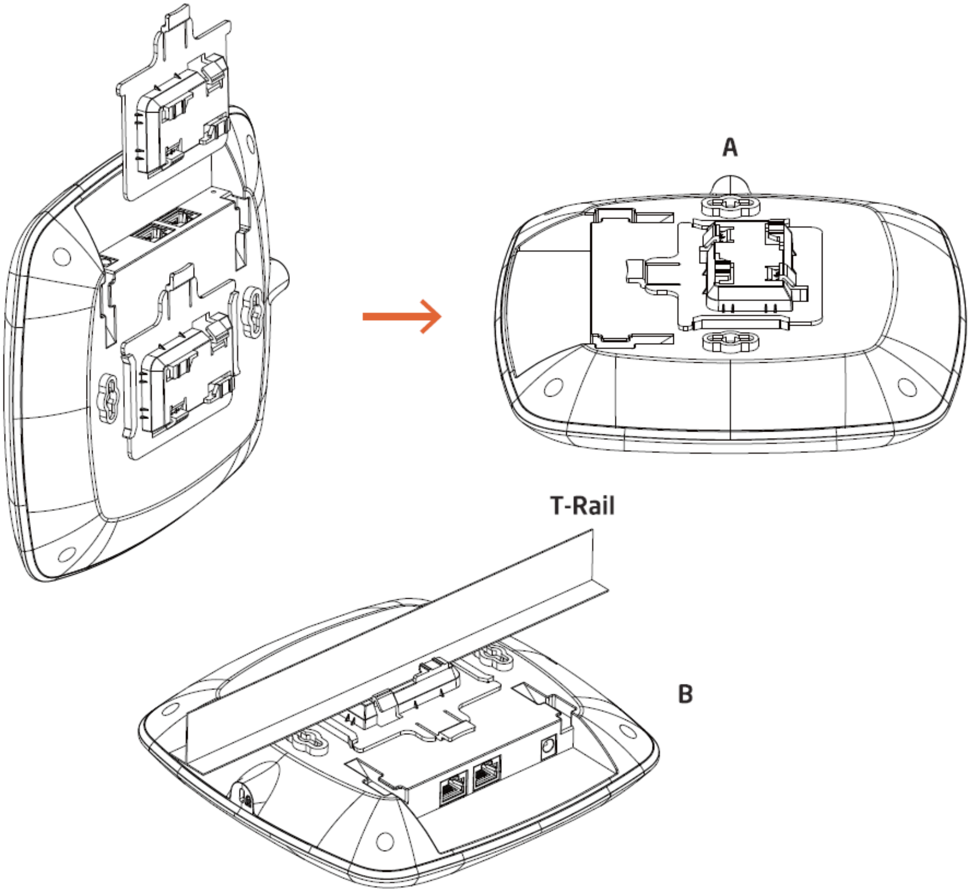
Mounting the Access Point

Using the provided hardware, the Access Point can be attached to a ceiling or wall.

To attach the Access Point to a ceiling or wall using the mounting bracket

A)   Slide the ceiling mount base into the slot of this Access Point.

B)   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.



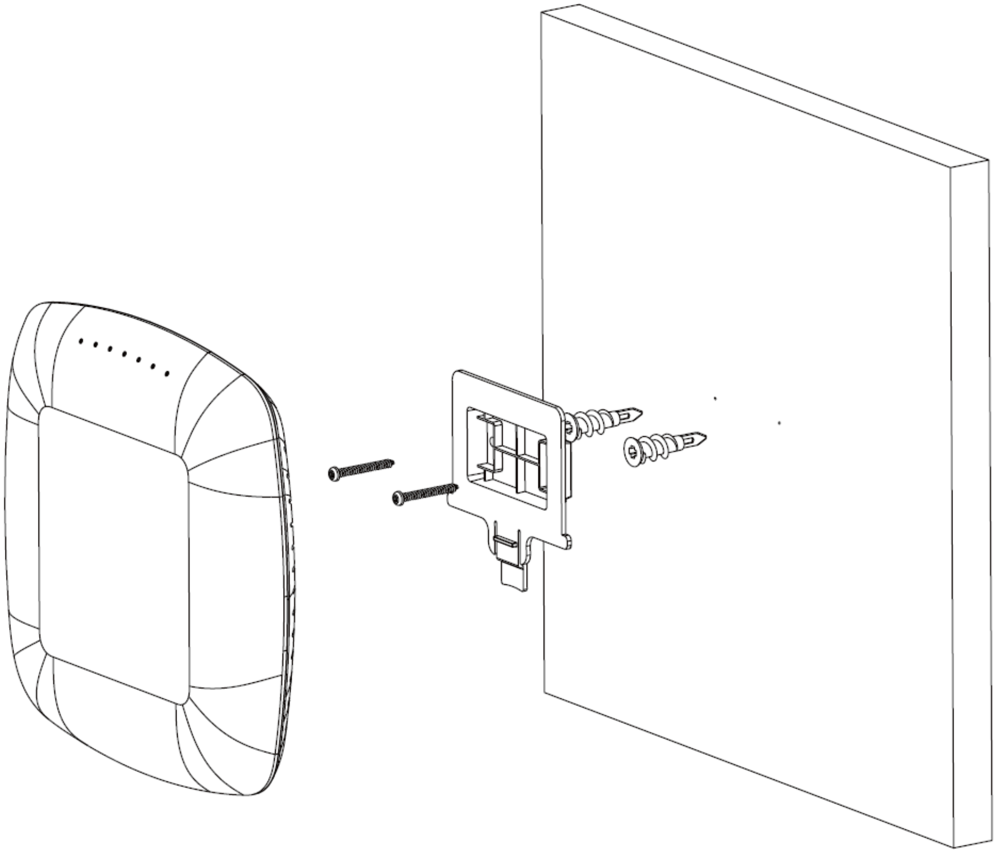
Wall mount the Access Point

A) Determine where the Access Point will be placed; mark the location for the two base plate mounting holes on the wall. Use the appropriate drill bit to drill a hole on each mark (1/3” or 8.1mm diameter; 1” or 26mm deep).

B) Screw the anchors into the holes until they are flush with the wall.

C) Screw the included screws into the anchors.

D) Slide the wall mount base into the slot of the Access Point.



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.

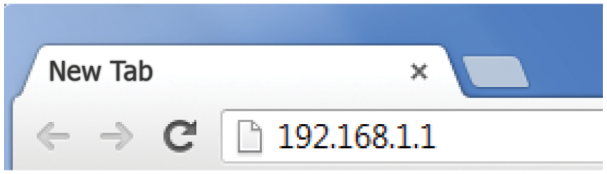
Default Settings

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

IP Address	192.168.1.1
Username/Password	admin/admin

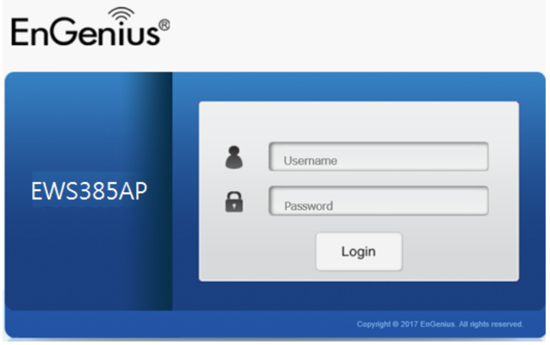
Web Configuration

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



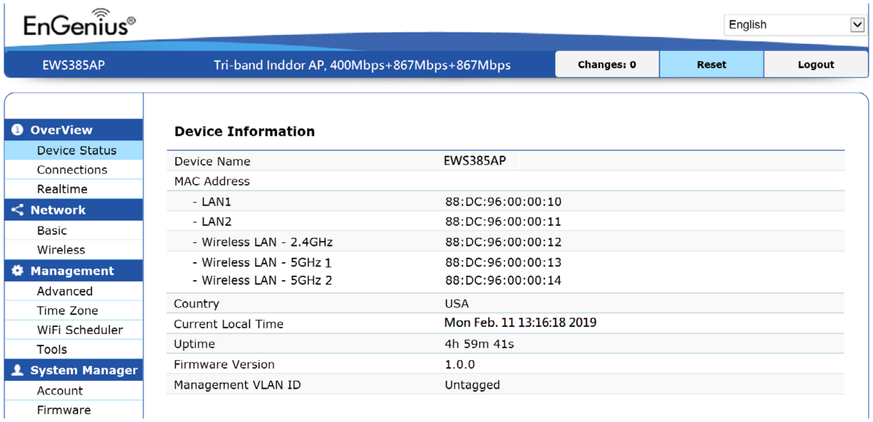
Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

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.



Device Information

Device Name	EWS385AP
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 1	88:DC:96:00:00:13
- Wireless LAN - 5GHz 2	88:DC:96:00:00:14
Country	USA
Current Local Time	Mon Feb. 11 13:16:18 2019
Uptime	4h 59m 41s
Firmware Version	1.0.0
Management VLAN ID	Untagged

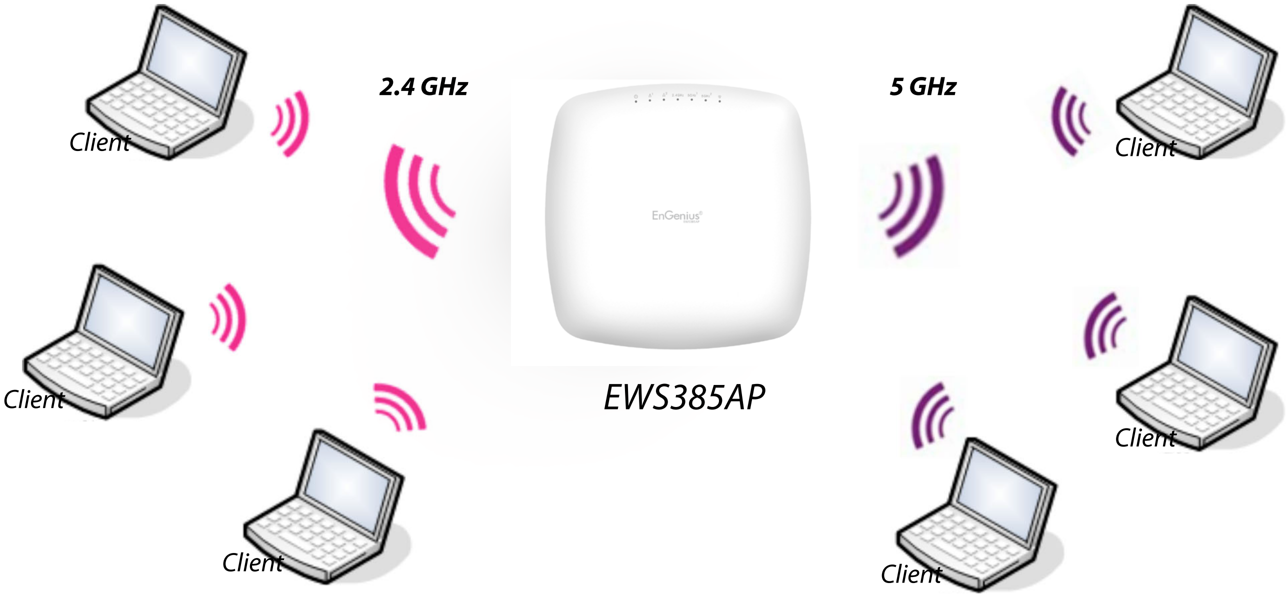
Chapter 4

Building a Wireless Network

The EWS385AP has the ability to operate in various modes. This chapter describes the operating modes of above three models.

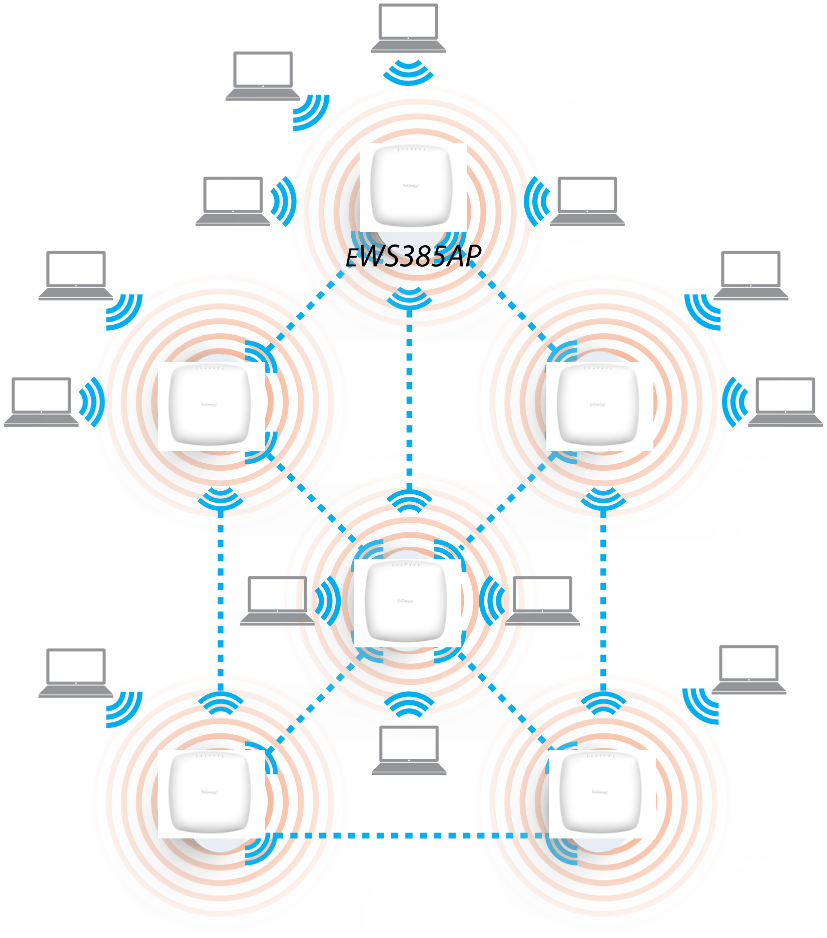
Access Point Mode

In Access Point Mode, the EWS385AP 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 EWS385AP.



AP Mesh Mode

Under the AP Mesh mode, the EWS385AP 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 EWS385AP can be configured with the same Mesh SSID and security password in order to associate with other EWS385AP, 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.

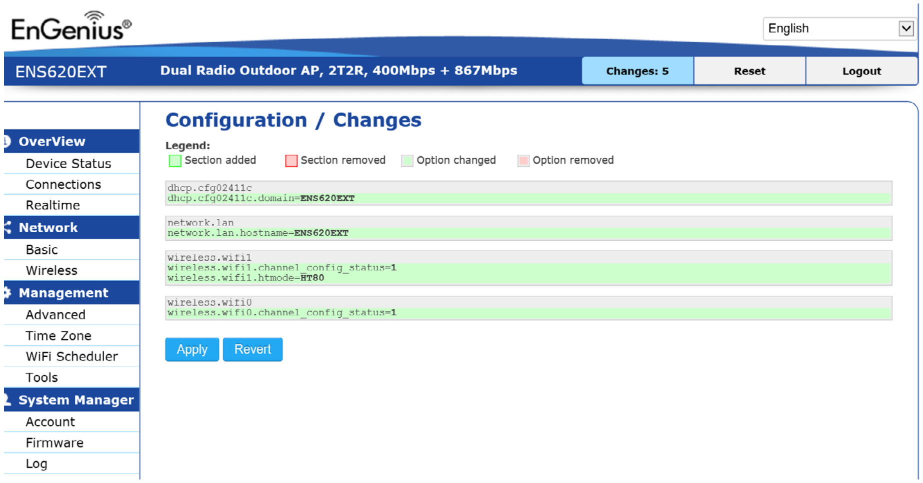


Chapter 5
Overview

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.



Configuration / Changes

Legend:
🟩 Section added 🟥 Section removed 🟩 Option changed 🟥 Option removed

```
dhcp.cfg02411c
dhcp.cfg02411c.domain=ENS620EXT

network.lan
network.lan.hostname=ENS620EXT

wireless.wifi1
wireless.wifi1.channel_config_status=1
wireless.wifi1.htmode=HT80

wireless.wifi0
wireless.wifi0.channel_config_status=1
```

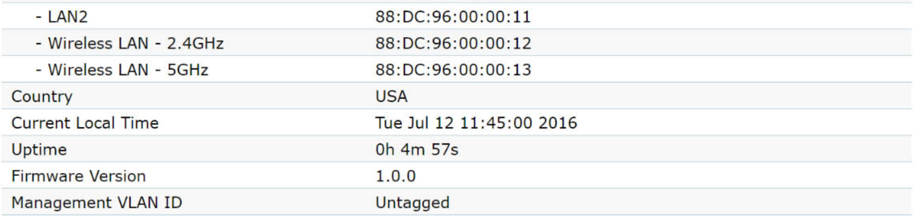
**The model name and description would be different by each EWS series model.

Device Status

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

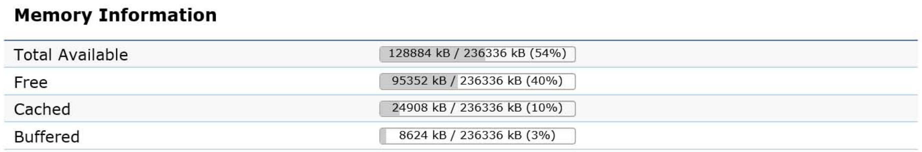
- The Device Information section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID

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



- 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

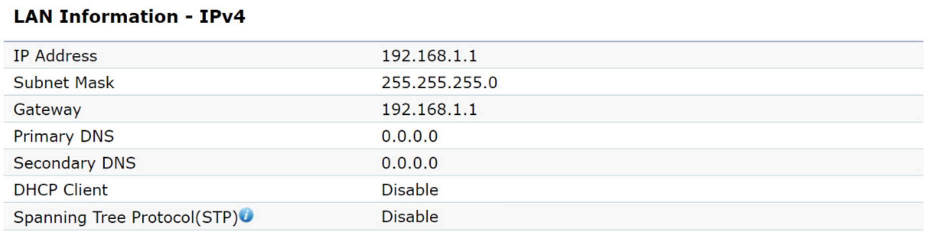
- The Memory Information section shows usage of memory such as Total Available, Free, Cached, Buffered



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).

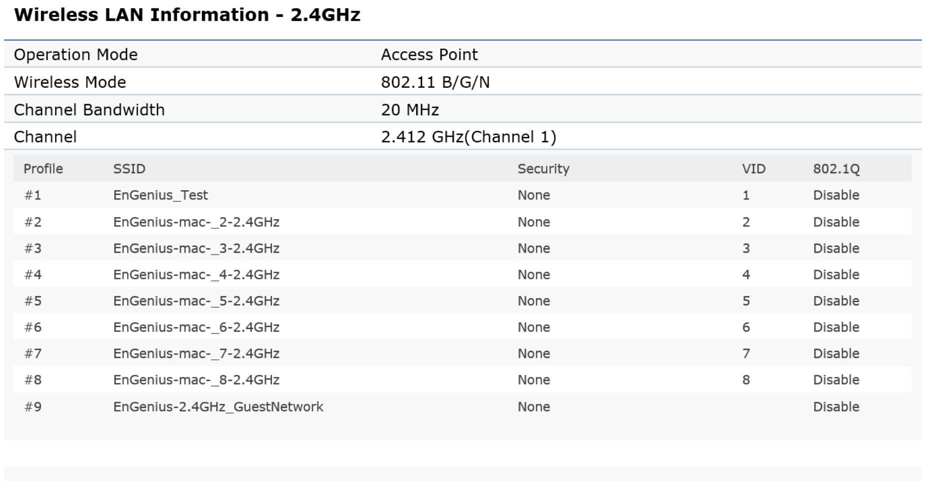


LAN Information - IPv4

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

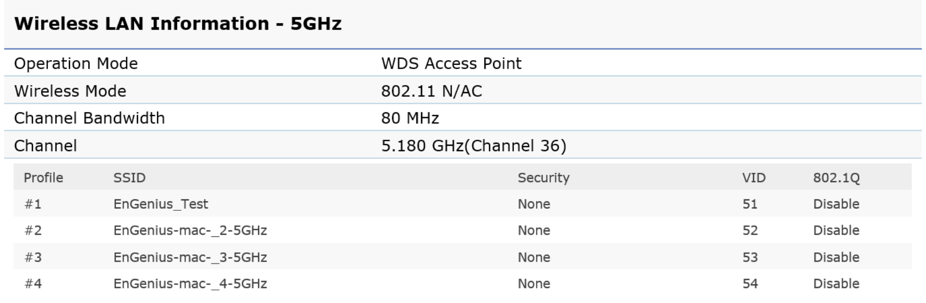
Note: Profile Settings are only applicable in Access Point and WDS AP modes.



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

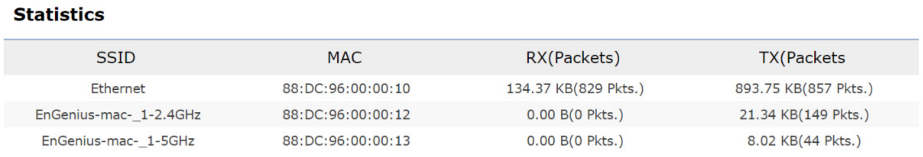


Wireless LAN Information - 5GHz

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

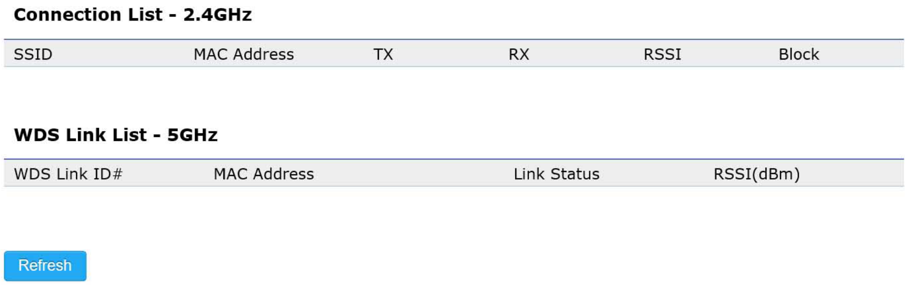
Click the connection link under the Overview menu displays the connection list of clients associated to the AP's 2.4 GHz/5 GHz, along with the MAC addresses and signal strength for each client. Clicking Refresh updates the client list.

> 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

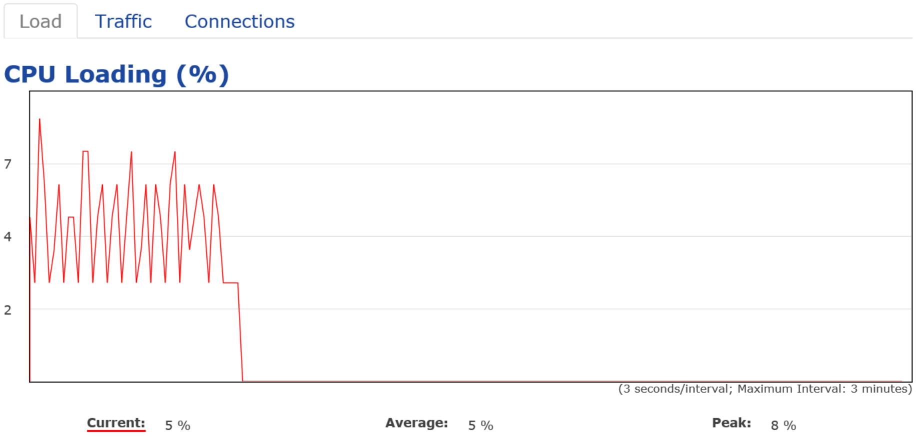
WDS Link ID#	MAC Address	Link Status	RSSI(dBm)

Realtime

Realtime

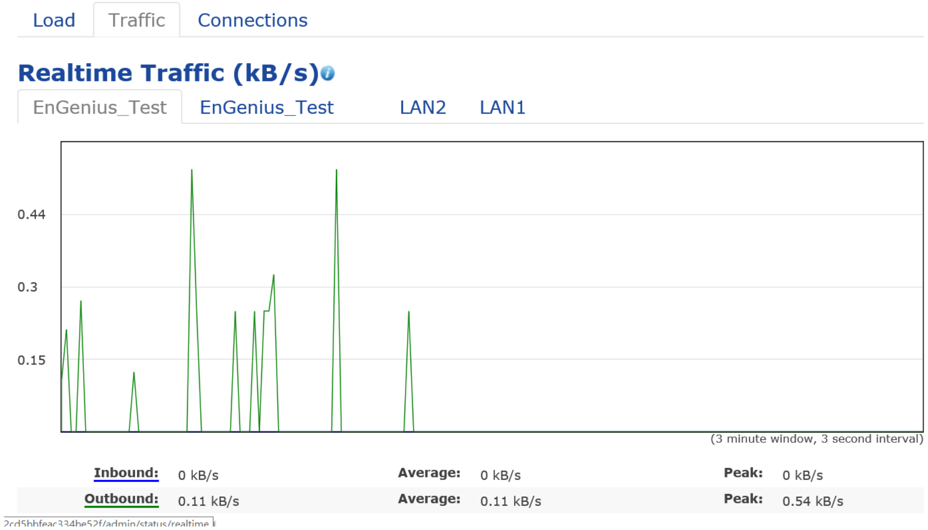
The Realtime section contains the following options:

> CPU Loading: 3 minutes CPU loading percentage information, it displays current loading, average loading and peak loading status. Left bar is loading percentage;



Current: 5 %   Average: 5 %   Peak: 8 %

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



Realtime Traffic (kB/s)

(3 minute window, 3 second interval)

Inbound:	0 kB/s	**Average:**	0 kB/s	**Peak:**	0 kB/s
Outbound:	0.11 kB/s	**Average:**	0.11 kB/s	**Peak:**	0.54 kB/s

2cd5bbfeac334be52f/admin/status/realtime

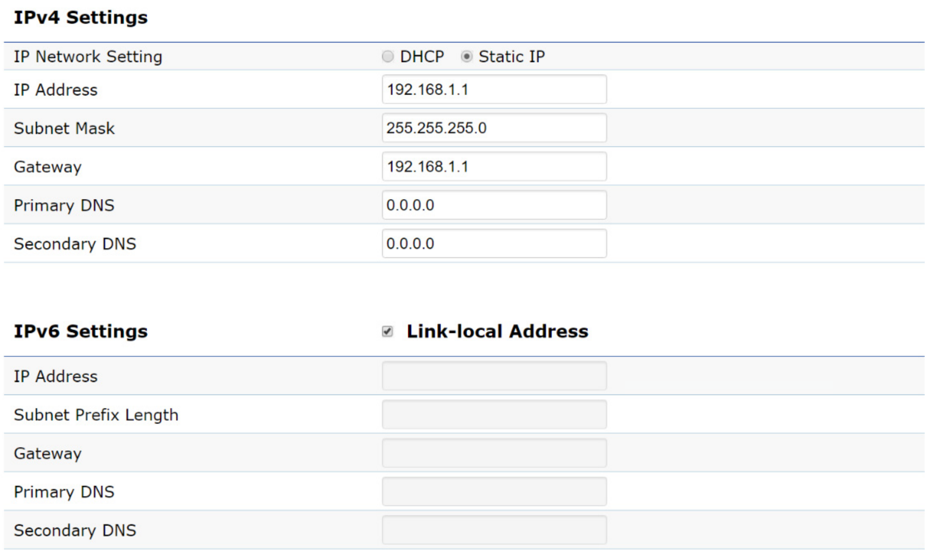
Realtime Connection (Pkts): Overview on current active network connections. It displays UDP and TCP packets information and other connection status. UDP connections curve is in blue; TCP connection curve is in green; others curve is in red. Below of chart shows connections source and destination.

Chapter 6
Network

Basic

IPv4/IPv6 Settings

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



IPv4 Settings

IP Network Setting	○ DHCP ● Static IP
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

IPv6 Settings ☑ **Link-local Address**

IP Address	
Subnet Prefix Length	
Gateway	
Primary DNS	
Secondary DNS	

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.

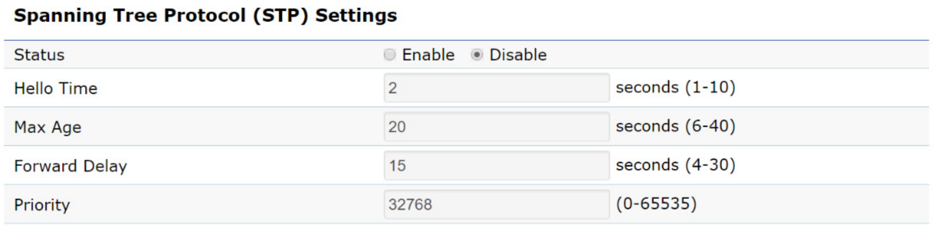
Gateway: The Default Gateway of this device. Leave it blank if you are unsure of this setting.

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	○ Enable ● Disable	
Hello Time	2	seconds (1-10)
Max Age	20	seconds (6-40)
Forward Delay	15	seconds (4-30)
Priority	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.

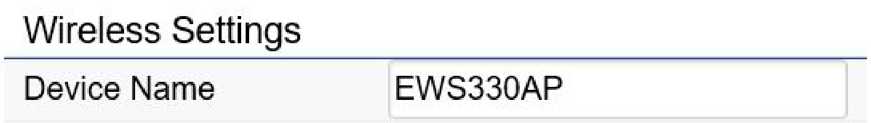
Priority: Specifies the Priority Number. A smaller number has a greater priority than a larger number.

Save: Click Save to confirm the changes.

Chapter 7
2.4 GHz & 5 GHz Wireless

Wireless

Wireless Settings



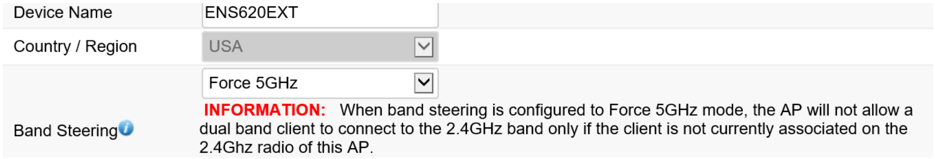
Wireless Settings

Device Name	EWS330AP

**The model name and description would be different by each EWS series model.

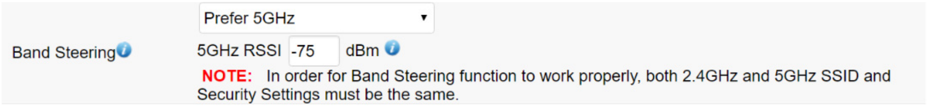
Device Name: Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.

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,



Device Name	ENS620EXT
Country / Region	USA
Band Steering	Force 5GHz INFORMATION: 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.

*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.

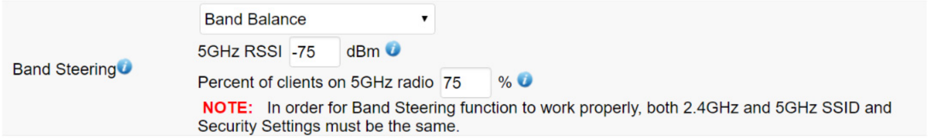


Band Steering: Prefer 5GHz

5GHz RSSI -75 dBm

NOTE: 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 Steering: Band Balance

5GHz RSSI -75 dBm

Percent of clients on 5GHz radio 75 %

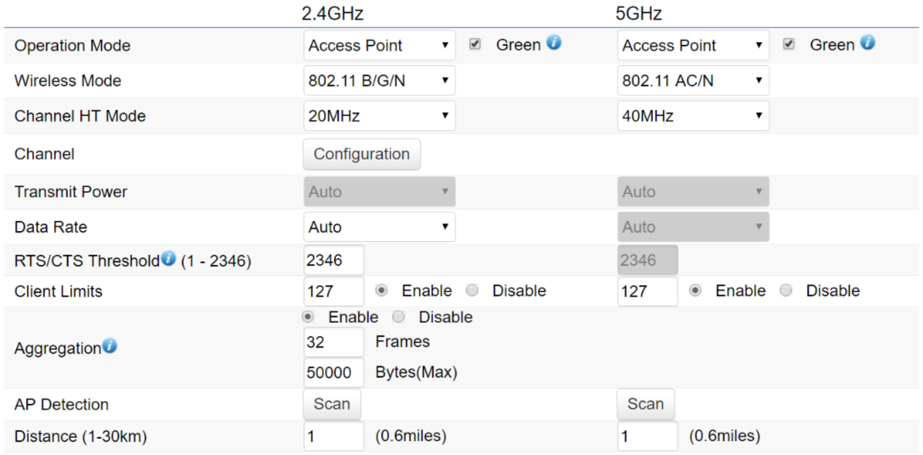
NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

*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 ▾	☑ Green	Access Point ▾	☑ Green
Wireless Mode	802.11 B/G/N ▾		802.11 AC/N ▾	
Channel HT Mode	20MHz ▾		40MHz ▾	
Channel	Configuration			
Transmit Power	Auto ▾		Auto ▾	
Data Rate	Auto ▾		Auto ▾	
RTS/CTS Threshold (1 - 2346)	2346		2346	
Client Limits	127	● Enable ○ Disable	127	● Enable ○ Disable
Aggregation	● Enable ○ Disable 32 50000	 Frames Bytes(Max)		
AP Detection	Scan		Scan	
Distance (1-30km)	1	(0.6miles)	1	(0.6miles)

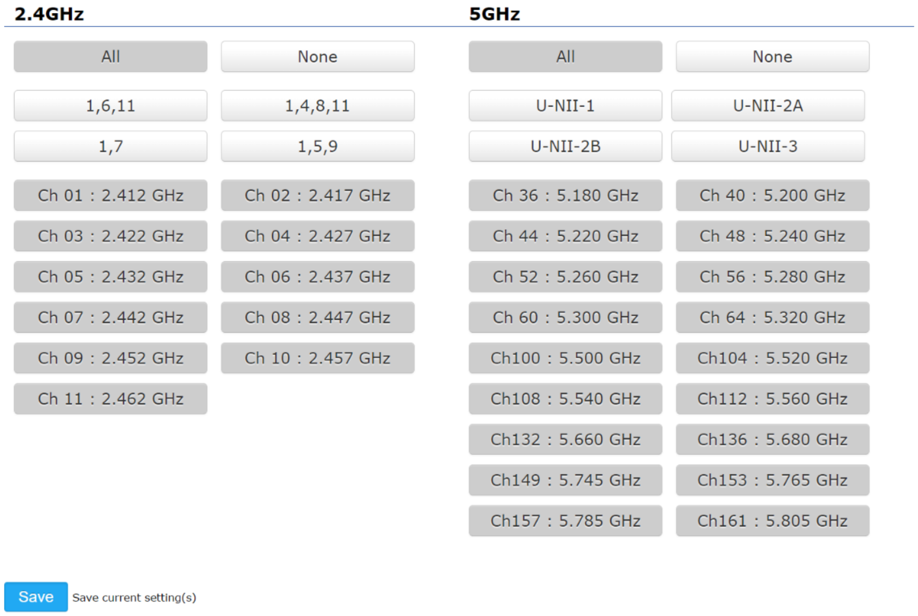
Operation Mode: Scrow down this list to select operation modes for implementing on this radio. The default operation mode is Access Point on base stations and Access Points and is Client Bridge on Client Premise Equipements (CPE). Meanwhile, EnGenius outdoor devices also support WDS modes for peer to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

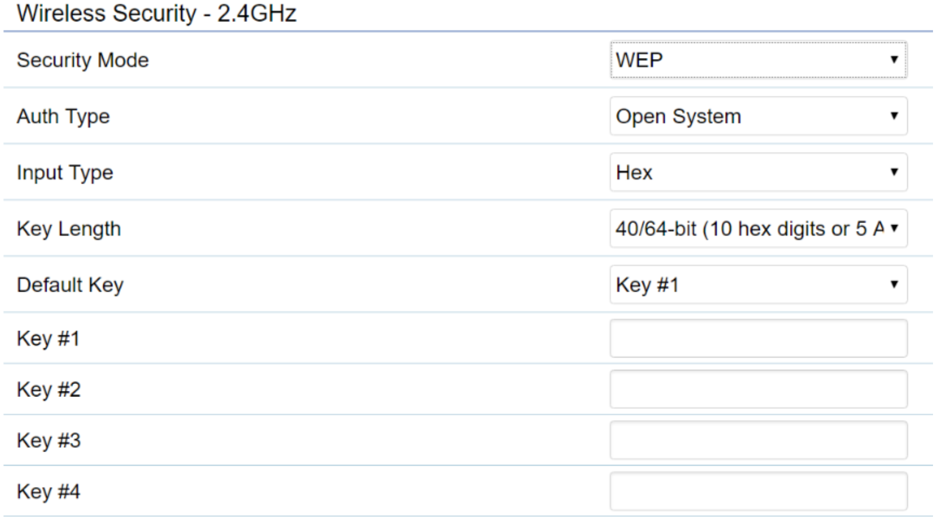


2.4GHz		5GHz	
All	None	All	None
1,6,11	1,4,8,11	U-NII-1	U-NII-2A
1,7	1,5,9	U-NII-2B	U-NII-3
Ch 01 : 2.412 GHz	Ch 02 : 2.417 GHz	Ch 36 : 5.180 GHz	Ch 40 : 5.200 GHz
Ch 03 : 2.422 GHz	Ch 04 : 2.427 GHz	Ch 44 : 5.220 GHz	Ch 48 : 5.240 GHz
Ch 05 : 2.432 GHz	Ch 06 : 2.437 GHz	Ch 52 : 5.260 GHz	Ch 56 : 5.280 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	
Key #2	
Key #3	
Key #4	

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:

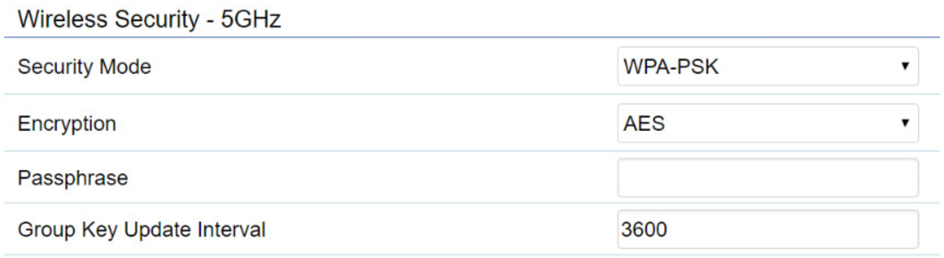
ASCII: Regular Text (recommended)

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

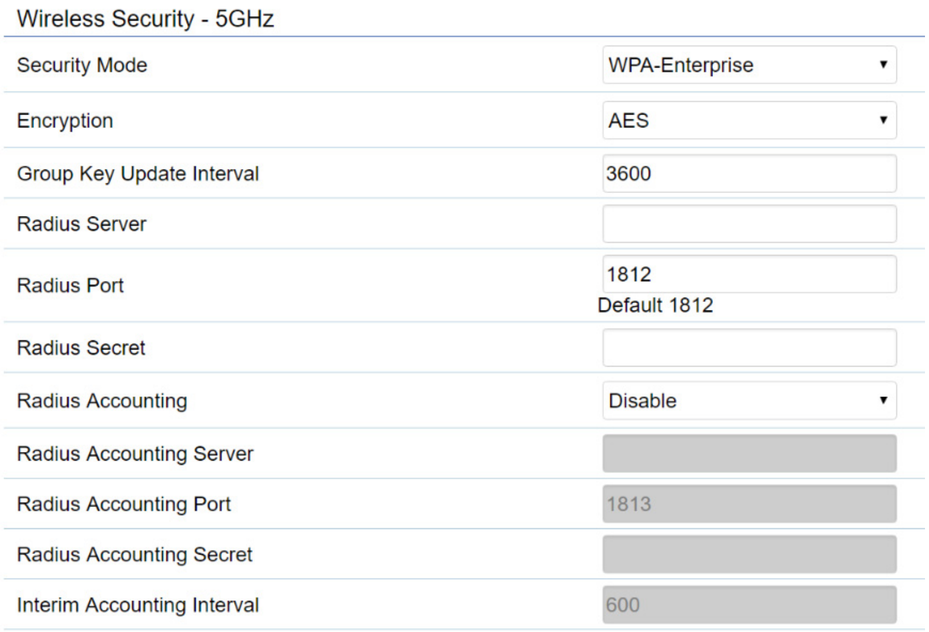
Security Mode	WPA-PSK ▾
Encryption	AES ▾
Passphrase	
Group Key Update Interval	3600

* 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	
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-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.

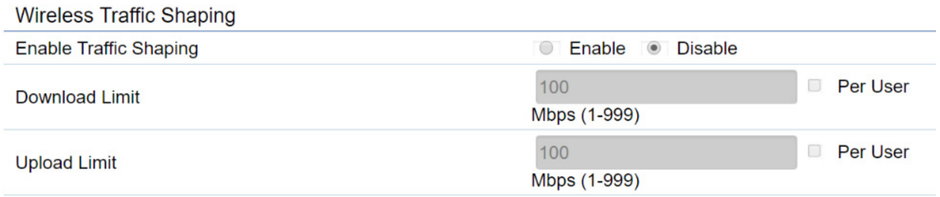
Interim Accounting Interval: Specifies how often, in seconds, the accounting data sends.

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	○ Enable ● Disable
Download Limit	100 □ Per User Mbps (1-999)
Upload Limit	100 □ 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.

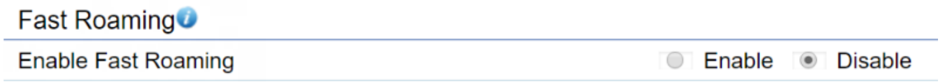
Save: Click Save to confirm the changes.

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

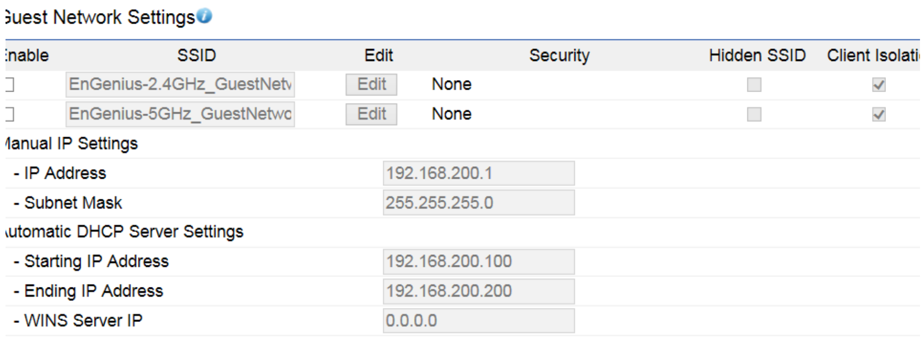
Enable Fast Roaming ○ Enable ● Disable

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 Isolati
□	EnGenius-2.4GHz_GuestNetw	Edit	None	□	☑
□	EnGenius-5GHz_GuestNetwo	Edit	None	□	☑

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.

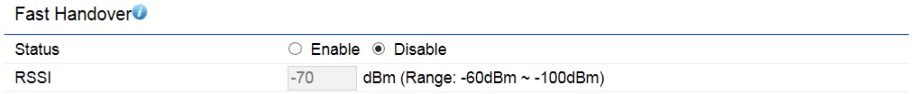
IP address: The IP Address of this device.

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	○ Enable ● Disable
RSSI	-70 dBm (Range: -60dBm ~ -100dBm)

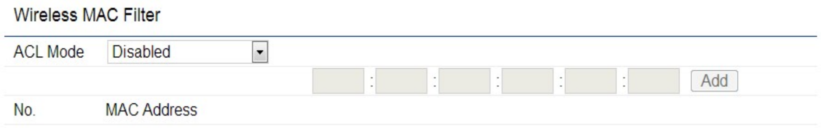
Enable : Enable the Fast Handover feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vincinity of that 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.



Wireless MAC Filter

ACL Mode: Disabled

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.

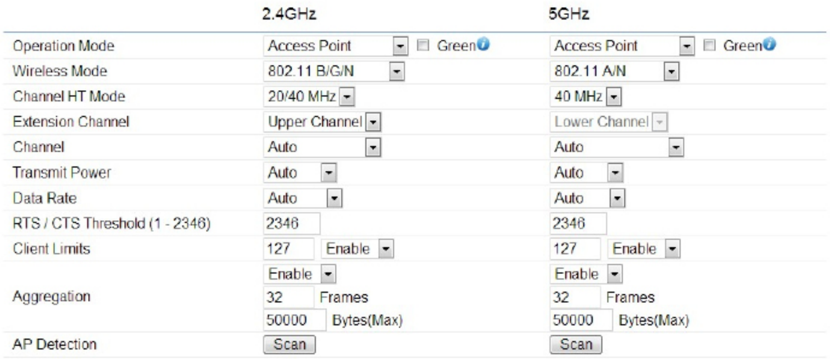
Delete: Deletes the selected entries.

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 ☐ Green	Access Point ☐ 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 - 2346)	2346	2346
Client Limits	127 Enable	127 Enable
Aggregation	Enable 32 Frames 50000 Bytes(Max)	Enable 32 Frames 50000 Bytes(Max)
AP Detection	Scan	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 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.

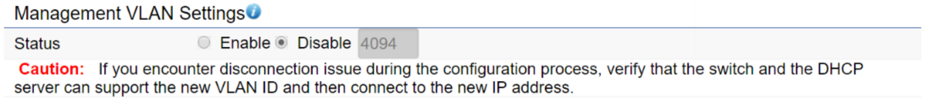
Chapter 8
Management

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.

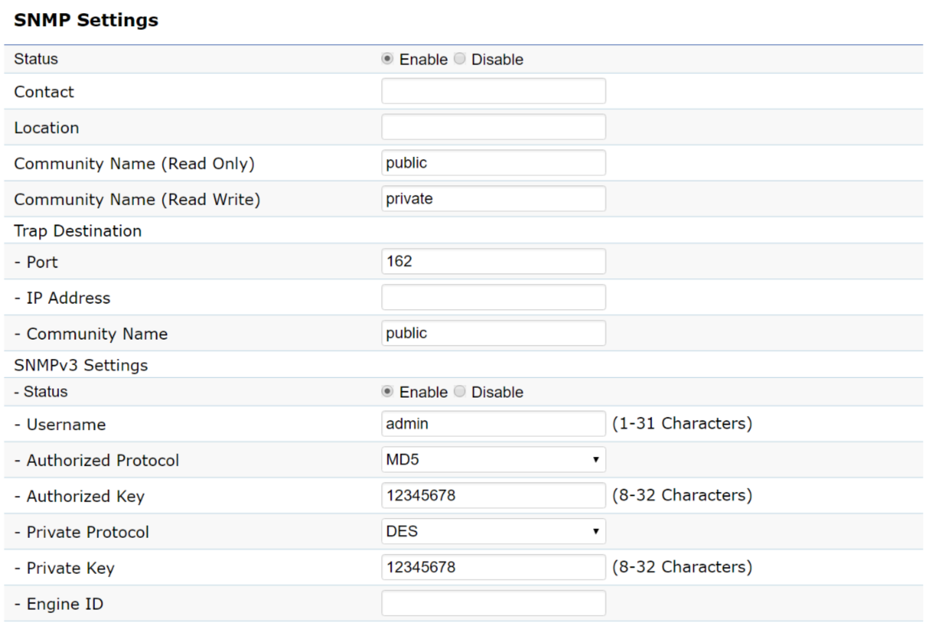
Save: Click Save to confirm the changes or Cancel to cancel and return to previous settings.

> 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	● Enable ○ Disable	
Contact		
Location		
Community Name (Read Only)	public	
Community Name (Read Write)	private	
Trap Destination		
- Port	162	
- IP Address		
- Community Name	public	
SNMPv3 Settings		
- Status	● Enable ○ Disable	
- Username	admin	(1-31 Characters)
- Authorized Protocol	MD5 ▾	
- Authorized Key	12345678	(8-32 Characters)
- Private Protocol	DES ▾	
- Private Key	12345678	(8-32 Characters)
- Engine ID		

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.

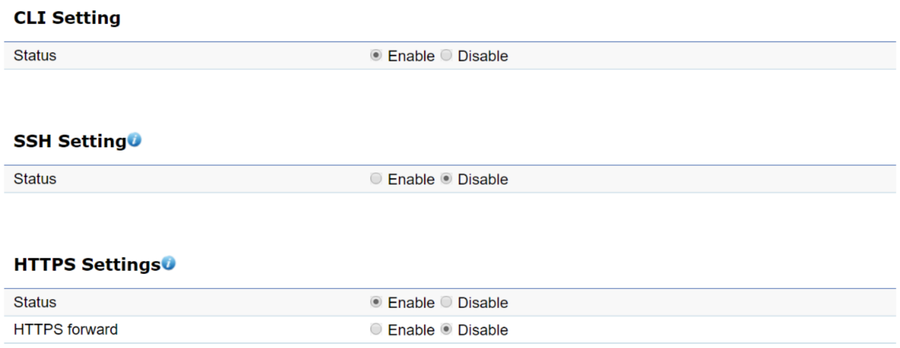
Priv Protocol: Selects the privacy protocol type: DES.

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.

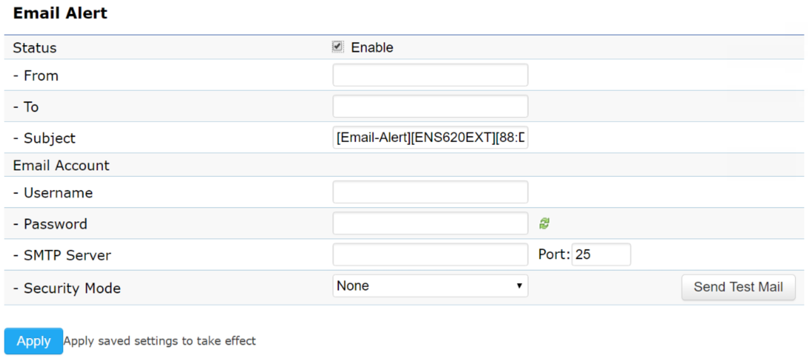
SSH: Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.

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	☑ Enable	
- From		
- To		
- Subject	[Email-Alert][ENS620EXT][88:D	
Email Account		
- Username		
- Password		
- SMTP Server		Port: 25
- Security Mode	None ▾	Send Test Mail

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.

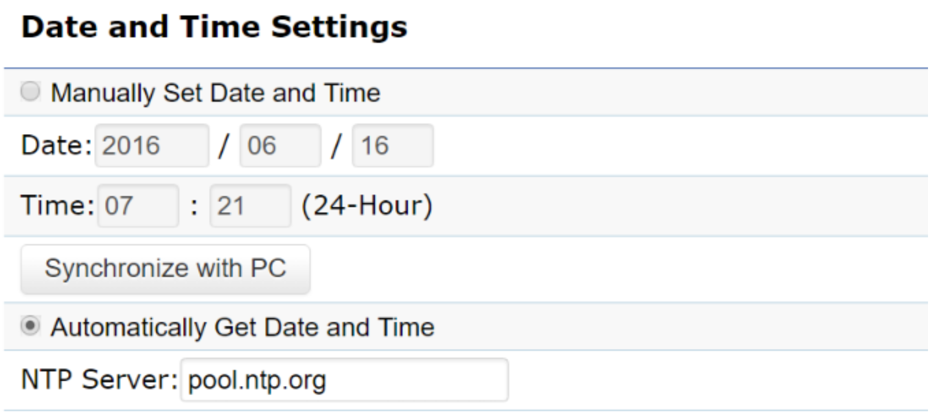
SMTP Server: Enter the IP address or hostname of the outgoing SMTP server.

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: 2016 / 06 / 16

Time: 07 : 21 (24-Hour)

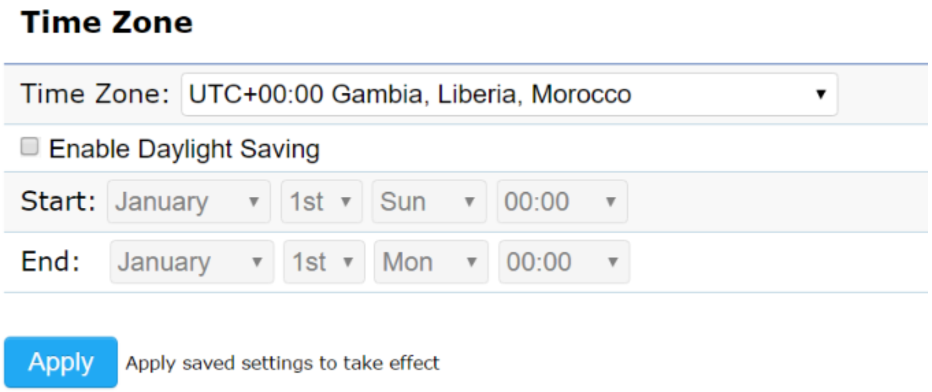
● Automatically Get Date and Time

NTP Server: pool.ntp.org

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

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

□ Enable Daylight Saving

Start: January 1st Sun 00:00

End: January 1st Mon 00:00

Apply saved settings to take effect

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

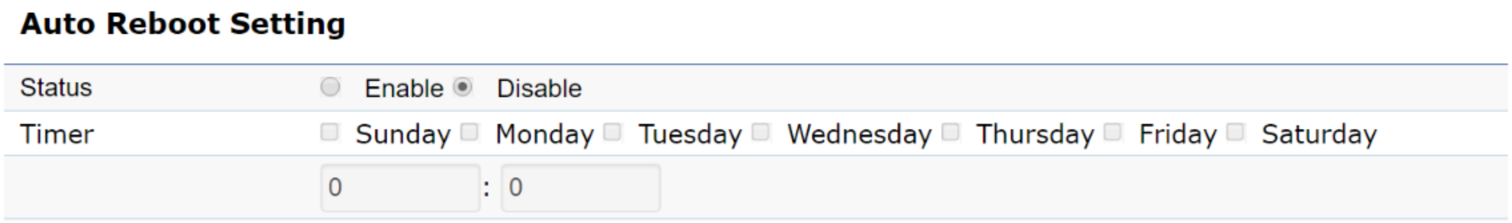
Enable Daylight Saving: Check whether daylight savings applies to your area.

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

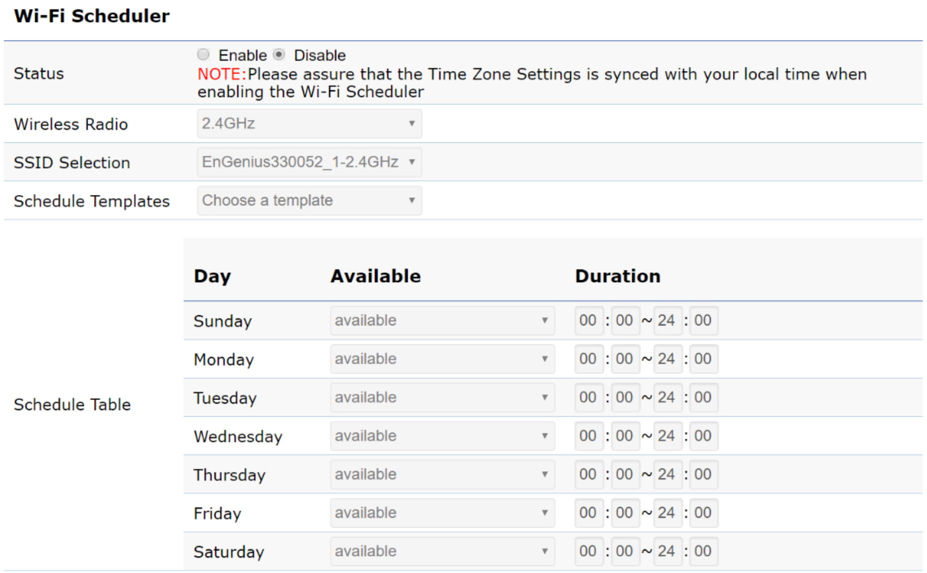
Auto Reboot Setting: Enables or disables the Auto Reboot function.

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.



Wi-Fi Scheduler

Status	○ Enable ● Disable NOTE:Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler
Wireless Radio	2.4GHz
SSID Selection	EnGenius330052_1-2.4GHz
Schedule Templates	Choose a template

Schedule Table

Day	Available	Duration
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.

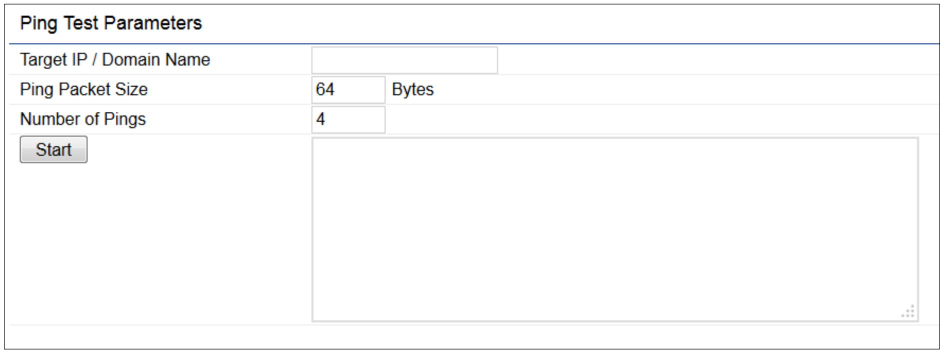
Day(s): Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

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

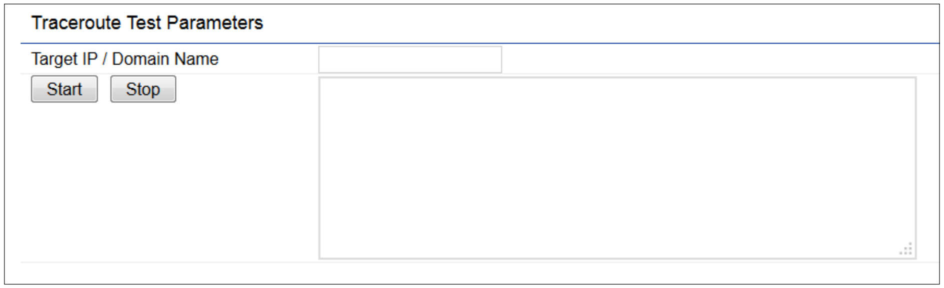
Ping Test Parameters

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	
Ping Packet Size	64 Bytes
Number of Pings	4



Traceroute Test Parameters

Target IP / Domain Name	

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.

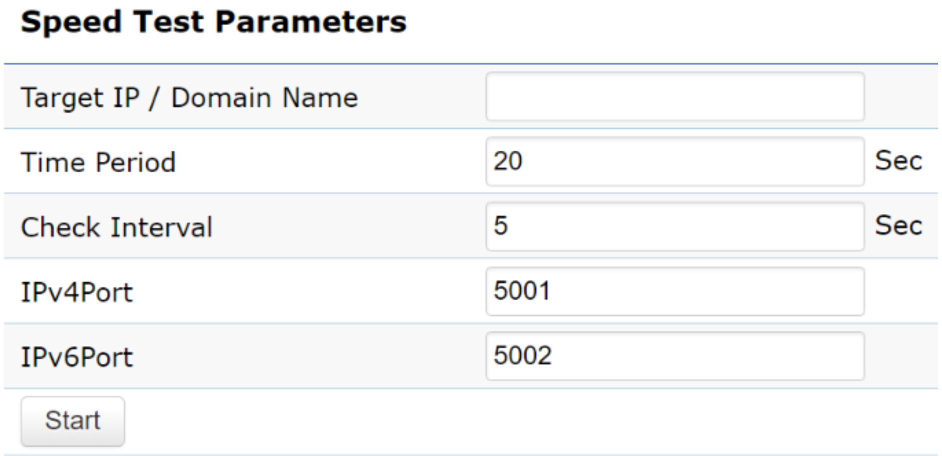
Start Ping: Click Start Ping to begin pinging the target device (via IP).

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	

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.

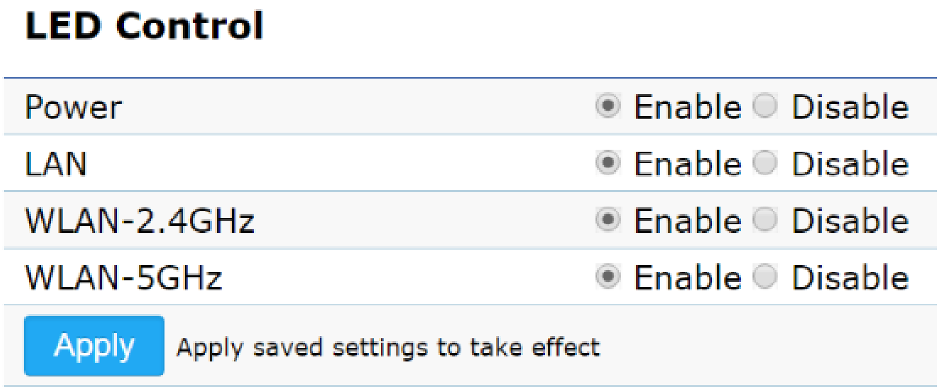
Time Period: Enter the time in seconds that you would like the test to implement for and in how many intervals.

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 saved settings to take effect

Power: Enables or disables the Power LED indicator.

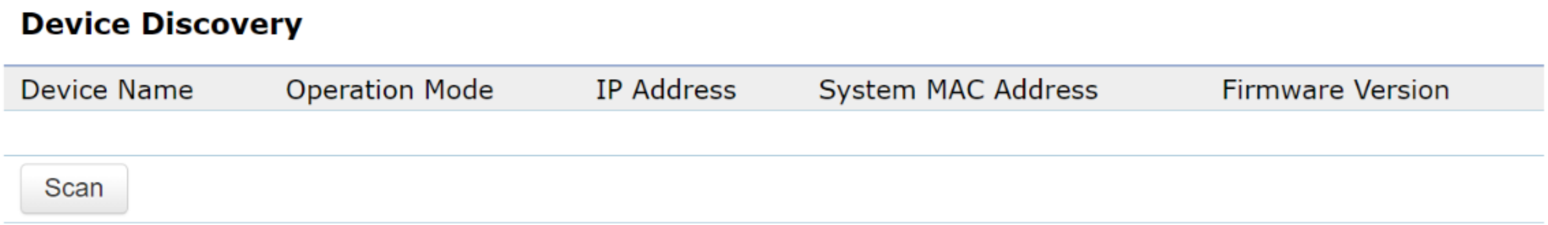
LAN: Enables or disables the LAN LED indicator.

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.



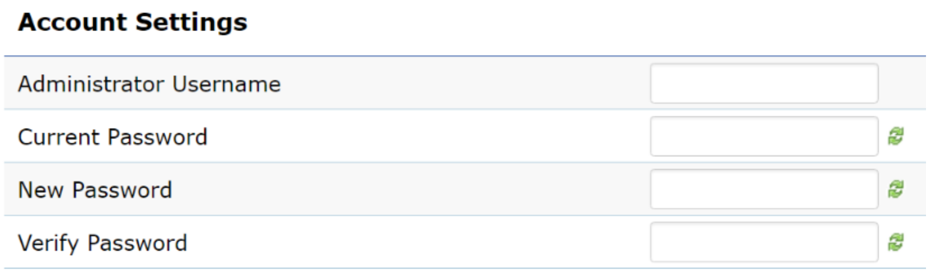
Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

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

Current Password

New Password

Verify 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.

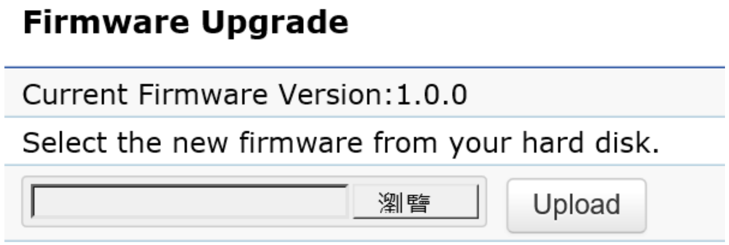
Verify Password: Re-enter the new password in the Confirm Password entry box for confirmation.

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.

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.

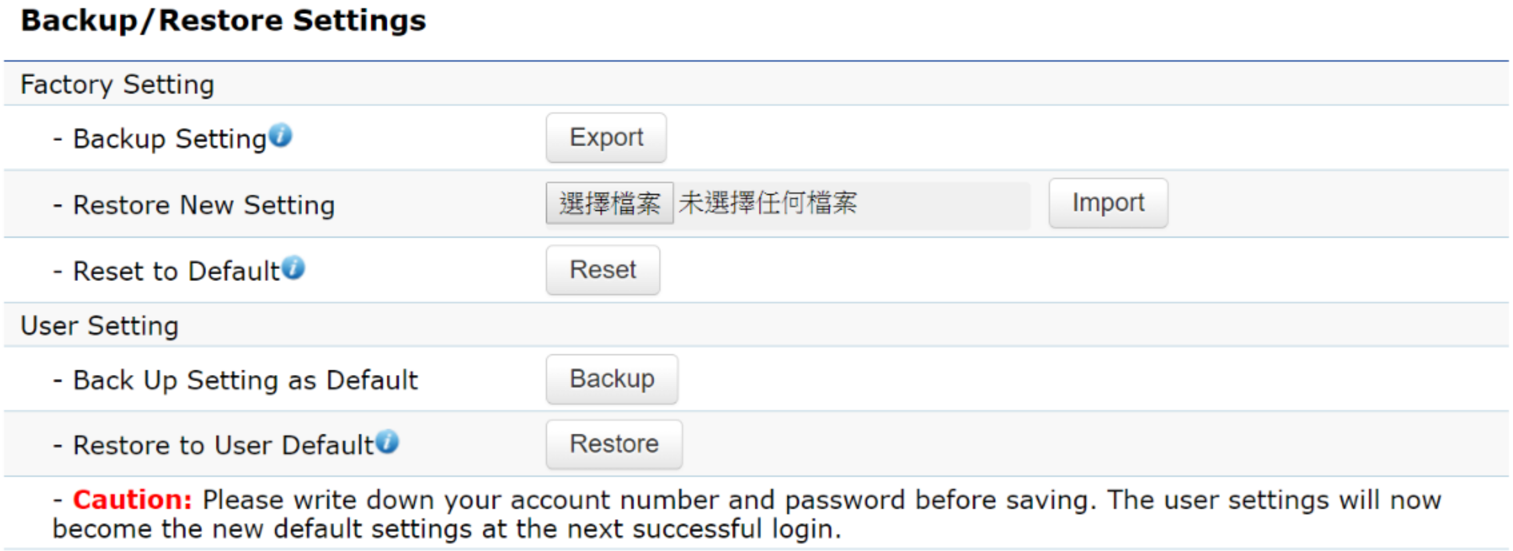
Backup/Restore

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.

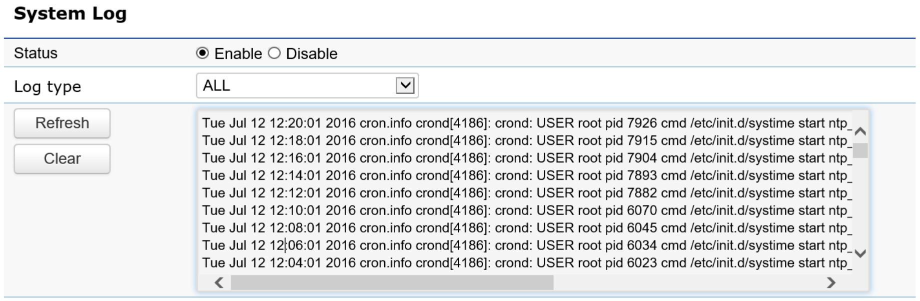
Note1: After setting the current settings as the default, you should click the Restore to Default on the web interface for reverting the settings into the factory default instead of pushing the reset button.

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.

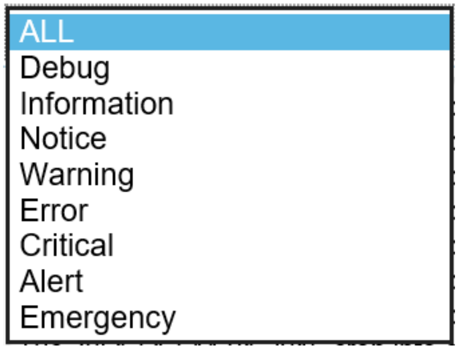


System Log

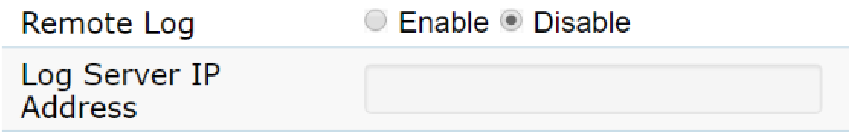
Status	● Enable ○ Disable
Log type	ALL

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

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	○ Enable ● Disable
Log Server IP Address	

Remote Log

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

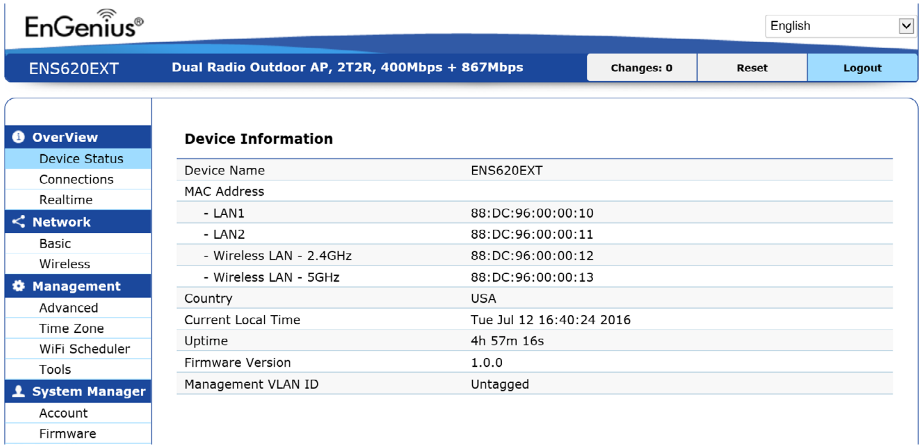
Remote Log: Enable/Disable this function.

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

Apply: Click Apply to apply the changes.

Logout

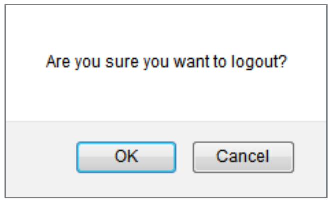
Logout: Click Logout in Management menu to logout.



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 16:40:24 2016
Uptime	4h 57m 16s
Firmware Version	1.0.0
Management VLAN ID	Untagged

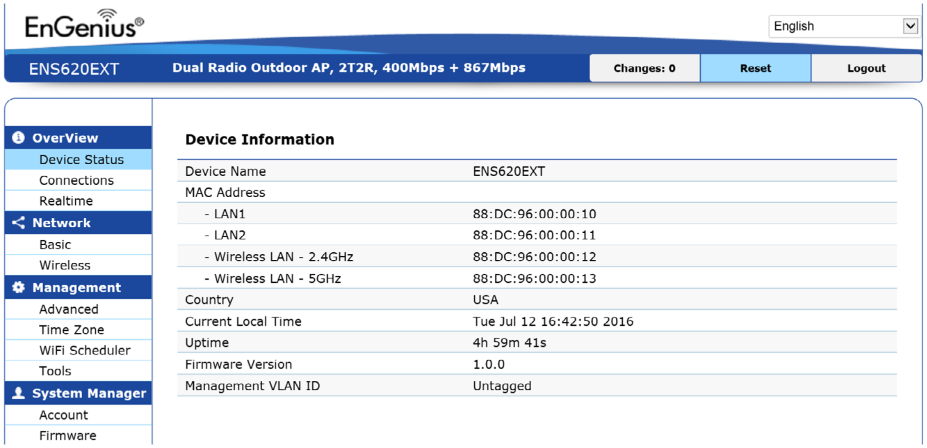
Please confirm again to logout the system or not.



Are you sure you want to logout?

Reset

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



Device Information

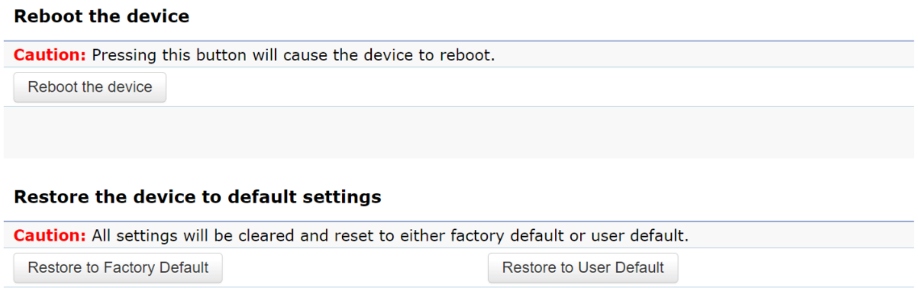
Device Name	ENS620EXT
MAC Address	
- LAN1	88:DC:96:00:00:10
- LAN2	88:DC:96:00:00:11
- Wireless LAN - 2.4GHz	88:DC:96:00:00:12
- Wireless LAN - 5GHz	88:DC:96:00:00:13
Country	USA
Current Local Time	Tue Jul 12 16:42:50 2016
Uptime	4h 59m 41s
Firmware Version	1.0.0
Management VLAN ID	Untagged

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.

Restore the device to default settings

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25 GHz band are restricted to indoor usage only.

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.

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

- EN60950-1

  Safety of Information Technology Equipment
- EN50385

  Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- EN 300 328

  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 893

  Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- EN 301 489-1

  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17

  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

CE 0560 (!)

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Česky [Czech]	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede [fabrikantens navn] erklærer herved, at følgende udstyr [udstyrets typebetegnelse] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt [Name des Herstellers], dass sich das Gerät [Gerätetyp] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab [tootja nimi = name of manufacturer] seadme [seadme tüüp = type of equipment] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, [name of manufacturer], declares that this [type of equipment] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente [nombre del fabricante] declara que el [clase de equipo] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [name of manufacturer] ΔΗΛΩΝΕΙ ΟΤΙ [type of equipment] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente [nom du fabricant] déclare que l'appareil [type d'appareil] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente [nome del costruttore] dichiara che questo [tipo di apparecchio] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [name of manufacturer / izgatavotāja nosaukums] deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [manufacturer name] deklaruoja, kad šis [equipment type] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart [naam van de fabrikant] dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, [isem tal-manifattur], jiddikjara li dan [il-mudel tal-prodott] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, [gyártó neve] nyilatkozom, hogy a [... típus] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym [nazwa producenta] oświadcza, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĹňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.