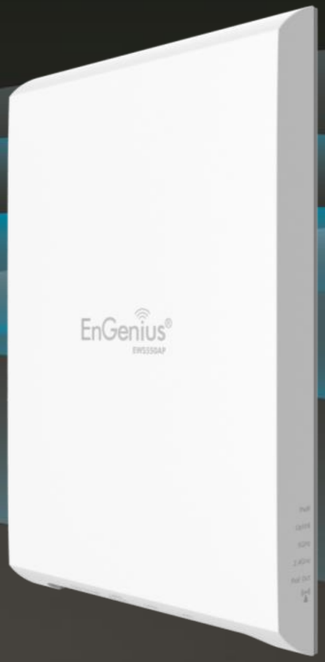
EnGenius

User Manual



EWS550AP

version 1.0

Wireless Managed Wall Plate Access Point

Table of Contents

Chapter 1
Product Overview

Introduction

Key Features

- Deploy and manage with ease using EWS Series Wireless Management Switches.
- Dual radio 2x2 802.11ac/a/b/g/n Access Point with multi-user MIMO (MU-MIMO) and 3 port Ethernet switch.
- Built-in “Turbo Engine” with a powereful quad-core chipset to process multiple tasks for driving and enhancing performance.
- Gigabit Ethernet uplink provides high speed Internet access.
- 3 x 10/100/1000 Mbps Ethernet ports for wired device connectivity (1 port includes PoE output).
- Supports 802.11ac Wave 2.0 technology to enhance overall bandwidth and speed to wireless client devices.
- Supports Tx Beamforming to enlarge the transmition distance.
- Performs 256-QAM under the 2.4 GHz band to enhance data rate to 400 Mbps.
- Additional RJ45 pass-through port for connecting to phone systems.
- Power-over-Ethernet supports 802.3af output when PoE input is 802.3at.
- Internal high-performance antennas support the wall plate AP’s low profile design.
- Effective and flexible bandwidth management.
- Secure Guest Network option available.
- Ideal for audio, video, and voice applications.
- Mounts onto any standard wall box.

Introduction

The EWS550AP is an enhanced-powered, long-range wireless access point. It is designed to operate in numerous environments; from large homes, small and medium-sized businesses, multiple-floor offices, hotels, and other venues, to larger enterprise deployments. The AP's enhanced-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that do not have the range and reach to connect to a growing number of wireless users who wish to access a large hotspot or business network.

To protect sensitive data during wireless transmissions, the device offers different encryption settings for wireless communications, including industry standard WPA and WPA2 encryption. The AP also includes MAC address filtering to allow network administrators to provide network access only to known computers and other devices based on their MAC addresses.

Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment, and mix of devices in the network. Features and specifications are subjected to change without prior notice. Trademarks and registered trademarks are the property of their respective owners.

System Requirements

The following are the Minimum System Requirements needed to configure the device:

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

Package Contents

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

- EWS Wall Plate Access Point
- Mounting Bracket
- Bracket Screw
- Quick Installation Guide

Applications

Wireless LAN (WLAN) products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of WLANs:

- **Difficult-to-Wire Environments:** There are many situations where wires cannot be installed, deployed easily, or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas that make the installation of a Ethernet-based LAN impossible, impractical or expensive are sites where WLAN can be a network solution.
- **Temporary Workgroups:** Create temporary workgroups/networks in more open areas within a building; auditoriums, amphitheaters classrooms, ballrooms, arenas, exhibition centers, or temporary offices where one wants either a permanent or temporary Wireless LAN established.
- **The Ability to Access Real-Time Information:** Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.
- **Frequently Changing Environments:** Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).
- **Small Office and Home Office (SOHO) Networks:** SOHO users require a cost-effective, easy and quick installation of a small network.
- **Training/Educational Facilities:** Training sites at corporations or students at universities use wireless connectivity to exchange information between peers and easily access information for learning purposes.

Technical Specifications

EWS550AP

Radio Specification

Dual Concurrent Radio:

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

Transmit Power:

- Max transmit power is limited by regulatory power

Radio Chains/Spatial Streams:

- 2 x 2: 2

Supported Radio Technology:

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

Channelization:

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

Supported Modulation:

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

Supported data rates (Mbps):

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

Physical & Environment

Power Source:

- PoE: compatible with 802.3af/at
  Supports 802.3af output when PoE input is 802.3at

Internal Antenna:

- 4 dBi/5.5 dBi 2.4 GHz antennas
- 6 dBi/5.3 dBi 5 GHz antennas

Interface:

- 1 x 10/100/1000 Mbps Uplink Port with 802.3af/at PoE
- 3 x 10/100/1000 Mbps Switched Ports
- 1 x 10/100/1000 Mbps Access Port with PoE Output
- 2 x RJ45 Pass Through Ports
- 2 x 110 Punch Down Blocks
- 1 x Reset button
- 1 x Kensington Security Slot

Dimensions (W x D x H):

- 125 x 188 x 26 mm

Mounting:

- Wall mount (standard US/EU single gang wall jack)

Environment:

- Operating temperature: 0°C~40°C
- Operating humidity: 0%~90% typical
- Storage temperature: -30°C~70°C

Wireless

Operating Mode:

- AP Mode
- Mesh AP Mode

Auto Channel Selection:

- Setting varies by regulatory domains

SSIDs:

- Supports up to 8 SSIDs per frequency band

VLAN Tag / VLAN Pass-through

Wireless Client List

Guest Network:

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

QoS:

- 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 or ezMaster)

Configuration

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

Firmware Upgrade

- Web interface or CLI (FTP/HTTP)

Backup / Restore Settings

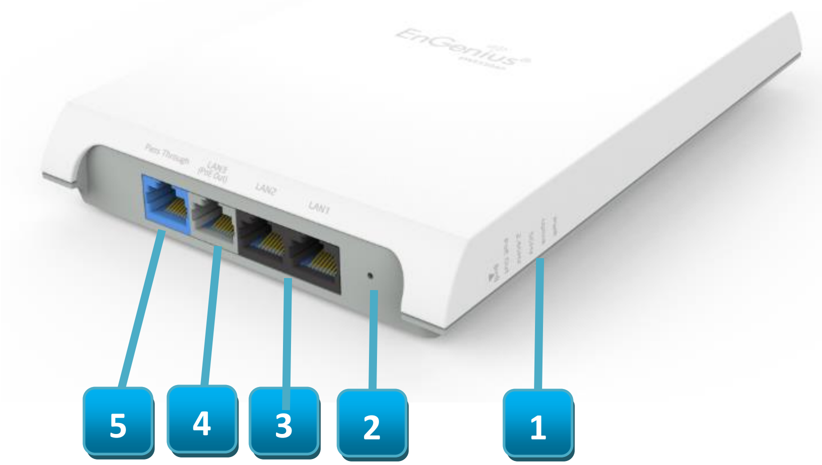
- Revert to factory default settings

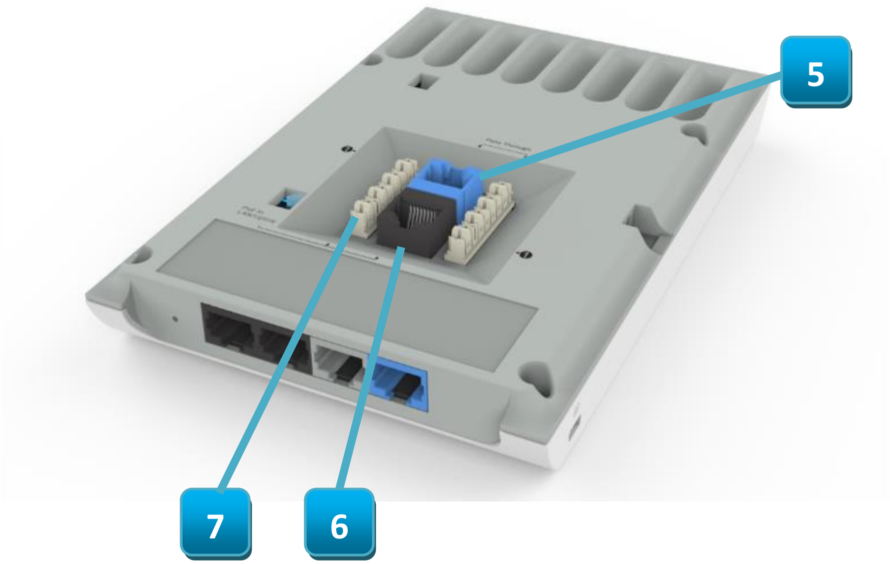
Schedule Reboot:

- Specifies interval to reboot system periodically

E-mail Alert/Syslog Notification

Physical Interface





1. LED Indicators: LEDs for Power, Uplink, 5 GHz, 2.4 GHz, PoE Out, Reserve
2. Reset Button: Press, hold for over 10 seconds to reset to factory default settings
3. 10/100/1000 LAN Ports: Two RJ45 access ports
4. 10/100/1000 LAN Port (PoE Out): RJ45 access port with PoE Out (support 802.3af output when PoE input is 802.3at)
5. RJ45 Pass Through Port: Pass through port
6. 10/100/1000 RJ45 Uplink (PoE In): Uplink port that supports 802.3af/at PoE input
7. 110 Punch Down Block

Chapter 2
Before You Begin

Before You Begin

This section will guide you through the installation process. Placement of the EnGenius Access Point is essential to maximize the its performance. Avoid placing the Access Point in an enclosed space such as a closet, cabinet, or stairwell.

Considerations for Wireless Installation

The operating distance of all wireless devices can often not be pre-determined due to a number of unknown obstacles in the environment in which the device is deployed. Obstacles such as the number, thickness, and location of walls, ceilings, or other objects that the Access Point's wireless signals must pass through can weaken the signal. Here are some key guidelines for allowing the Access Point to have an optimal wireless range during setup.

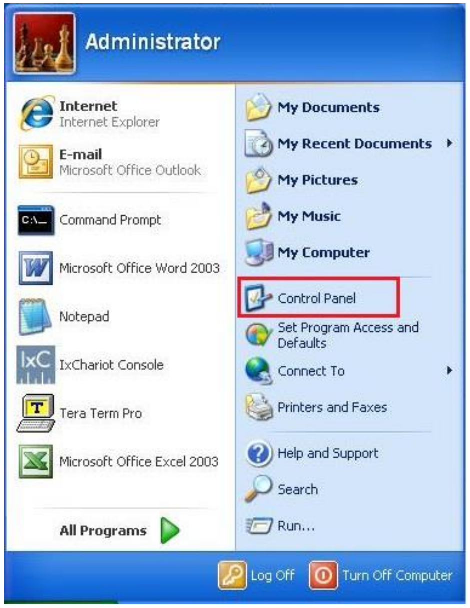
- Keep the number of walls and/or ceilings between the Access Point and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in a lower overall signal strength.
- Building materials make a difference. A solid metal door and/or aluminum stubs may have a significantly negative effect on the signal strength of the Access Point. Locate your wireless devices carefully so the signal can pass through drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets, and/or brick can also diminish wireless signal strength.
- Interference from your other electrical devices and/or appliances that generate RF noise can also diminish the Access Point's signal strength. The most common types of devices are microwaves or cordless phones.

Computer Settings

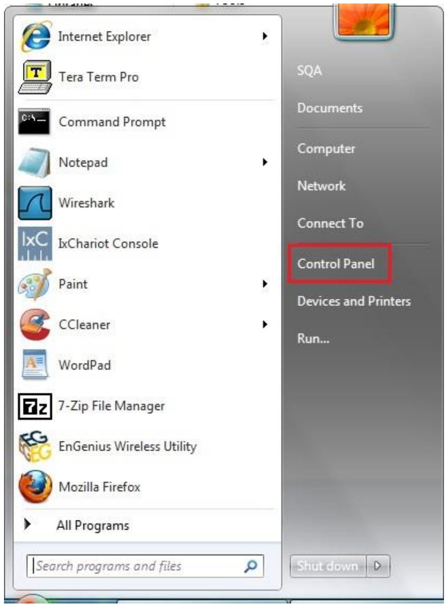
Windows XP/Windows 7

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

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

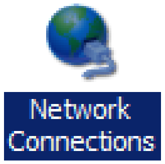


Windows XP

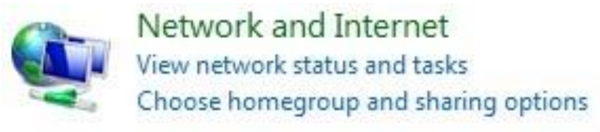


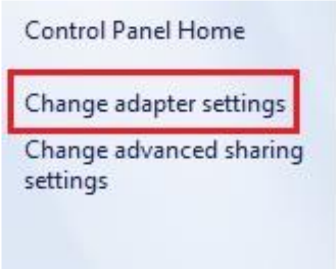
Windows 7

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

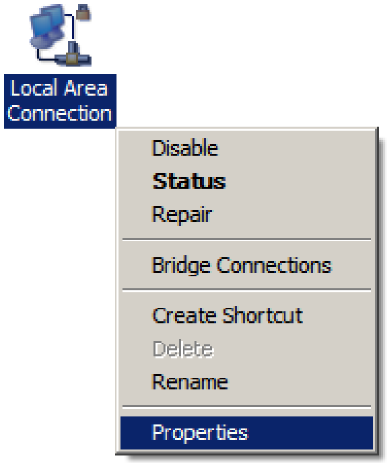


2b. In **Windows 7**, click **View network status and tasks** in the **Network and Internet** section, and then select **Change adapter settings.**

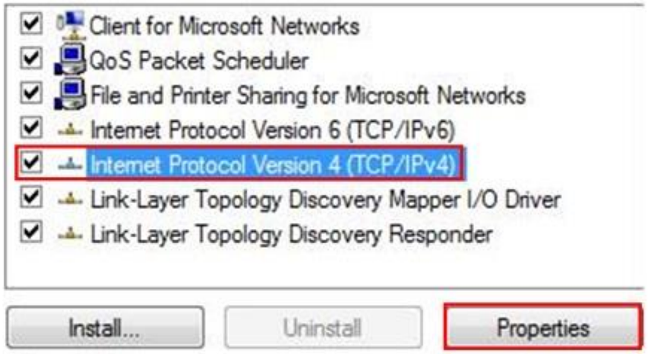

Network and Internet
View network status and tasks
Choose homegroup and sharing options



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



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



☑ Client for Microsoft Networks
☑ 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

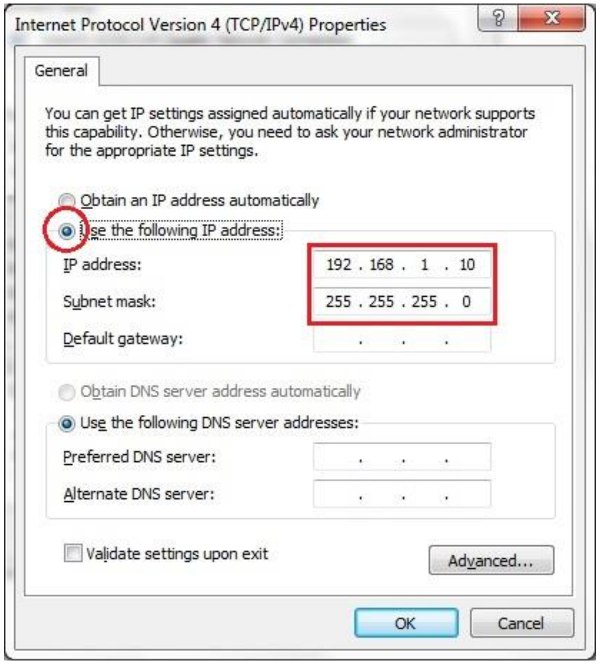
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

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

For example: Access Point IP address: 192.168.1.1

PC IP address: 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: . . .

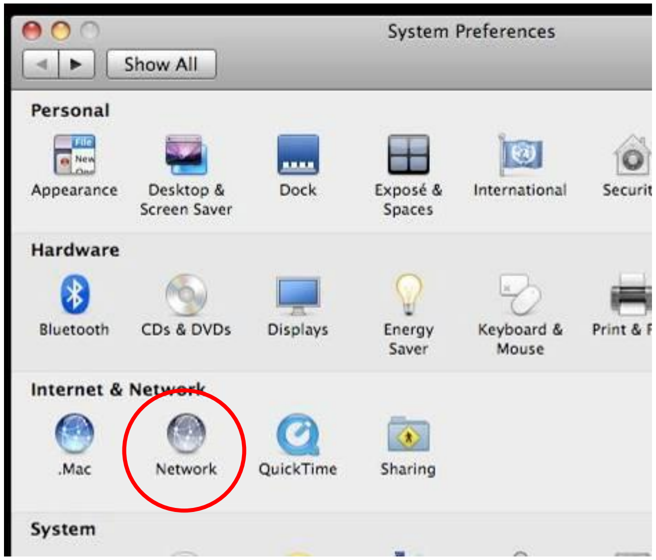
Alternate DNS server: . . .

□ Validate settings upon exit

Apple Mac OS X

1. Go to **System Preferences** (it can be opened in the **Applications** folder or by 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 click **OK**.

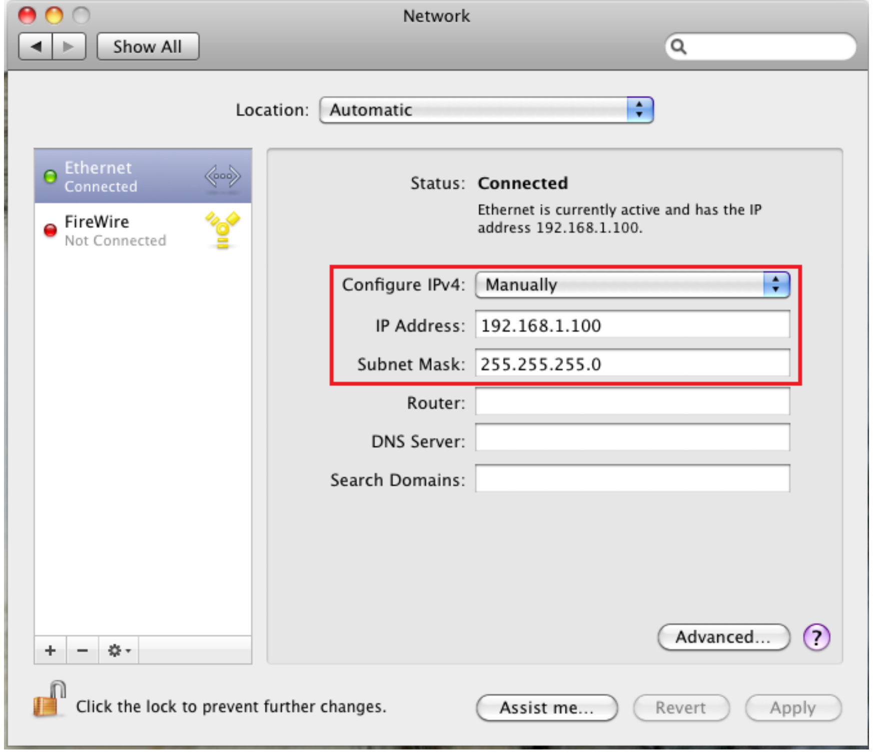
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: Access Point 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 finished.



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:

Click the lock to prevent further changes.

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.

> ⚠ DO NOT connect a PoE injector to any of the four access ports on the front as this could cause damage to the device.

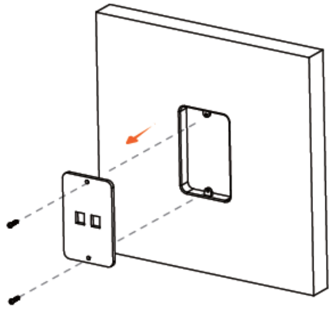
2. Connect the other end of the RJ45 Ethernet cable to a **PoE Ethernet switch** or the **PoE Out port** on the **PoE injector**.
3. Using another RJ45 Ethernet cable, connect one end to the **Ethernet port** on the computer, and connect the other end to another port on the **PoE Ethernet switch** or 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.**

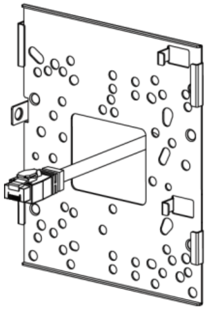
Mounting the Access Point

The EWS Wall Plate AP mounts onto an electrical outlet box.

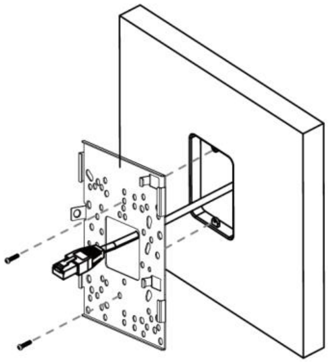
1. Remove the cover from the outlet box, retaining the original cover screws.



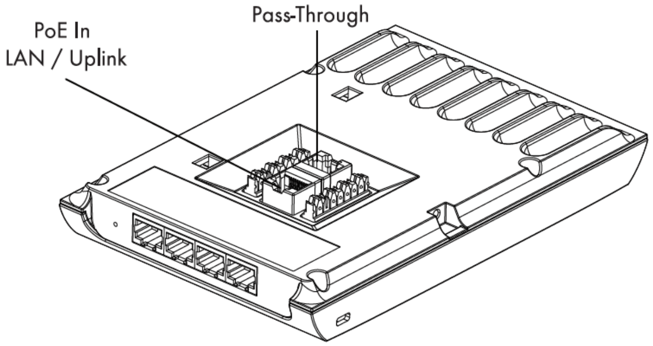
2. Gently pull the required cables through the center of the mounting bracket.



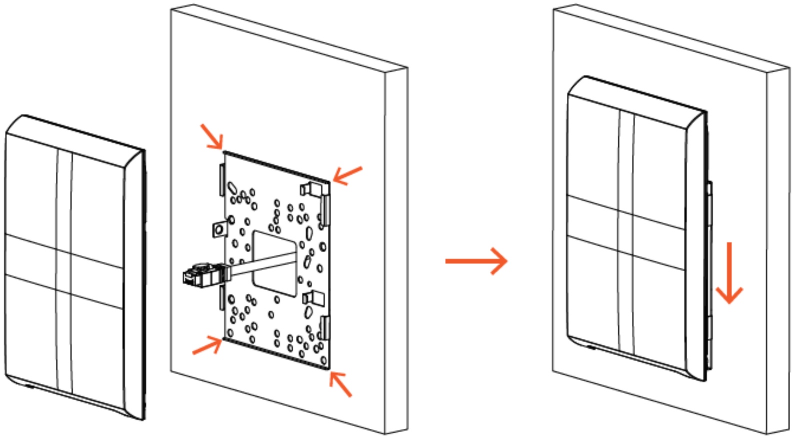
3. Align the mounting bracket with the outlet box and affix the mounting bracket to the outlet box using the original cover screws.



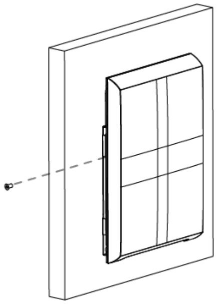
4. Connect the cables to the access point before mounting it to the bracket.



5. Hook the two tabs on the bottom of the bracket into the slots on the bottom of the AP and slide the AP down gently until it holds in place.

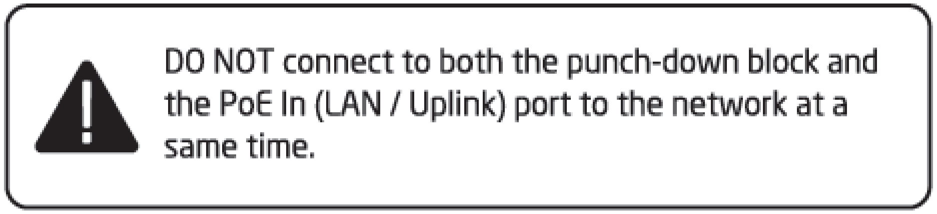


6. Use the bracket screw provided to secure the AP to the bracket.

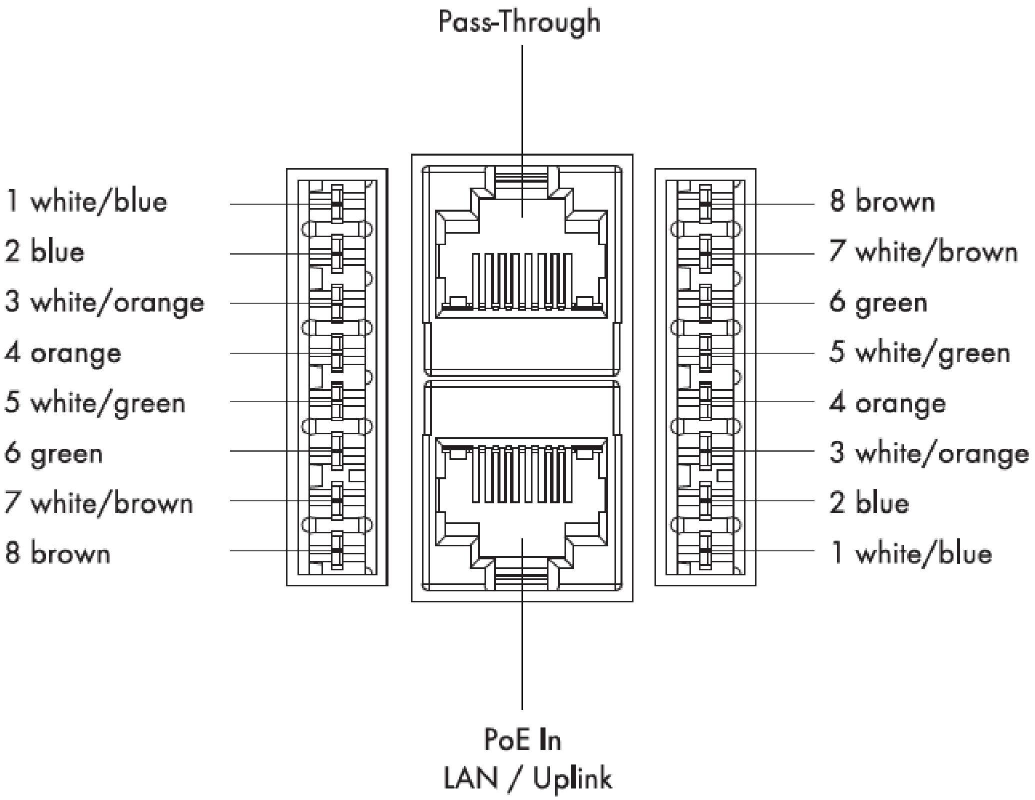


Connecting using the 110 Punch-down block

The 110 punch-down block can be used to connect the AP to the network instead of the RJ45 connector.



DO NOT connect to both the punch-down block and the PoE In (LAN / Uplink) port to the network at a same time.


Pass-Through
1 white/blue
2 blue
3 white/orange
4 orange
5 white/green
6 green
7 white/brown
8 brown
8 brown
7 white/brown
6 green
5 white/green
4 orange
3 white/orange
2 blue
1 white/blue
PoE In
LAN / Uplink

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.

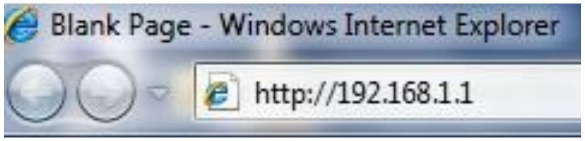
Default Settings

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 (Chrome/Internet Explorer/Firefox/Safari) and enter the IP Address http://192.168.1.1.

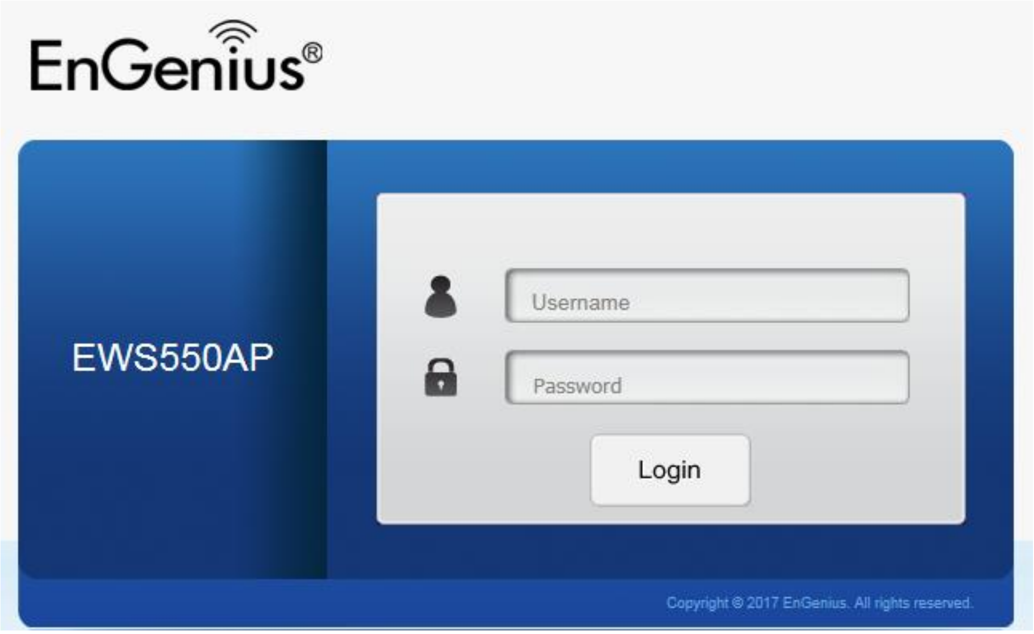


Blank Page - Windows Internet Explorer

http://192.168.1.1

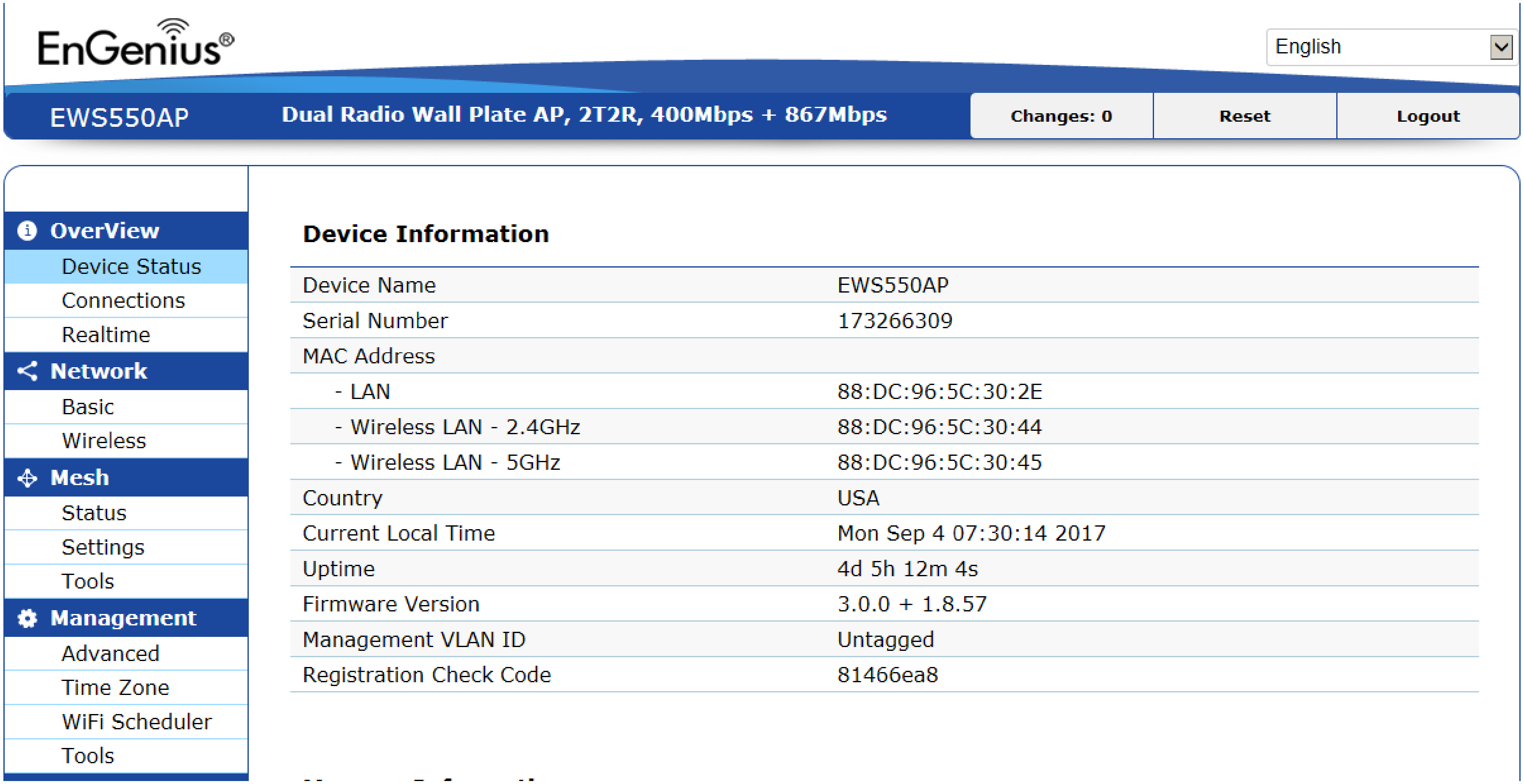
Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

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.



Copyright © 2017 EnGenius. All rights reserved.

3. If successful, you will be logged in and see the Access Point User Interface.
*Model name varies depending on model.



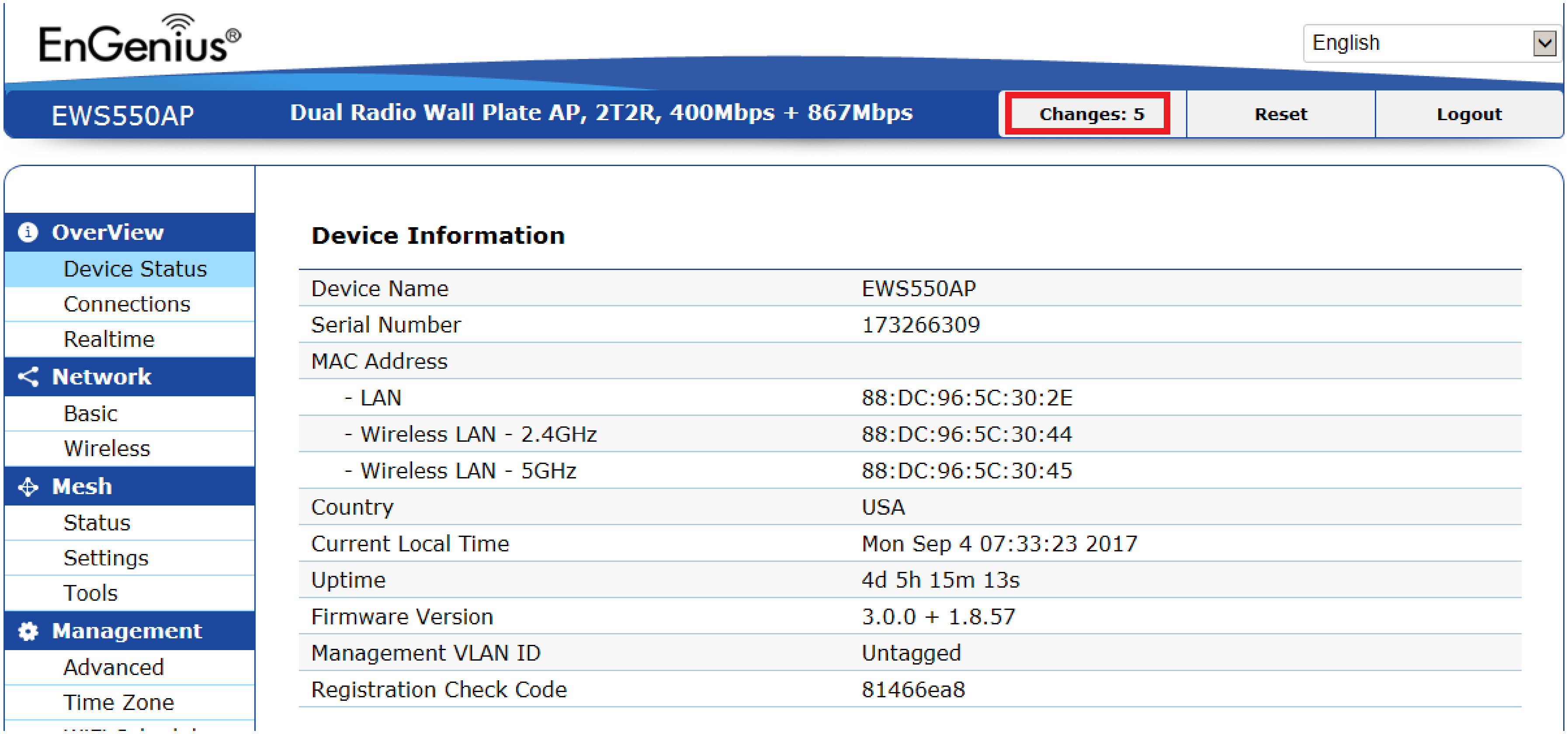
Device Information

Device Name	EWS550AP
Serial Number	173266309
MAC Address	
- LAN	88:DC:96:5C:30:2E
- Wireless LAN - 2.4GHz	88:DC:96:5C:30:44
- Wireless LAN - 5GHz	88:DC:96:5C:30:45
Country	USA
Current Local Time	Mon Sep 4 07:30:14 2017
Uptime	4d 5h 12m 4s
Firmware Version	3.0.0 + 1.8.57
Management VLAN ID	Untagged
Registration Check Code	81466ea8

Chapter 4
Overview

Overview

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 Information

Device Name	EWS550AP
Serial Number	173266309
MAC Address	
- LAN	88:DC:96:5C:30:2E
- Wireless LAN - 2.4GHz	88:DC:96:5C:30:44
- Wireless LAN - 5GHz	88:DC:96:5C:30:45
Country	USA
Current Local Time	Mon Sep 4 07:33:23 2017
Uptime	4d 5h 15m 13s
Firmware Version	3.0.0 + 1.8.57
Management VLAN ID	Untagged
Registration Check Code	81466ea8

The **Overview** section contains the following options:

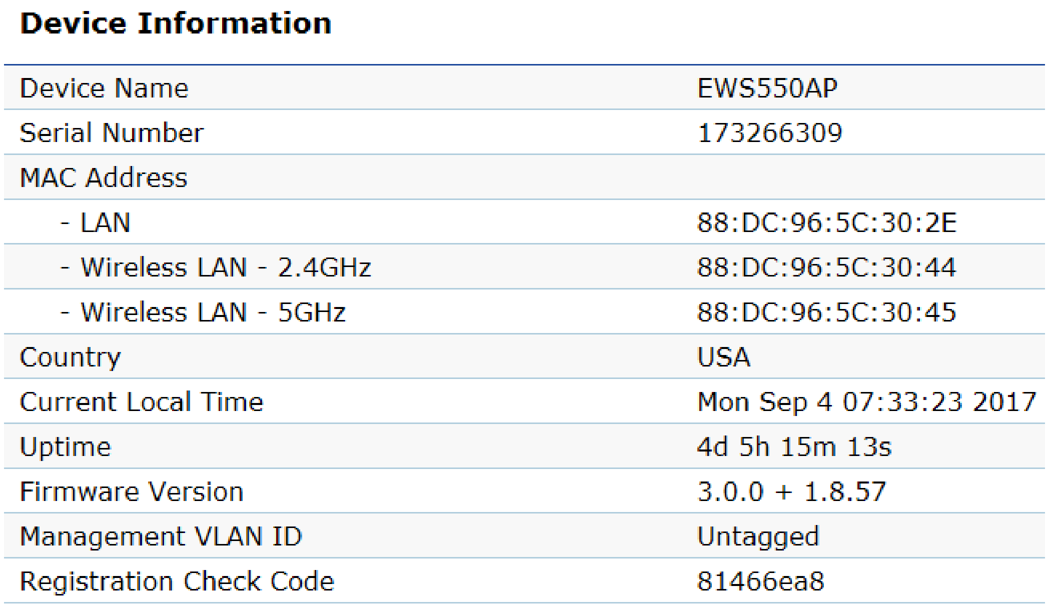
- Device Status
- Connections
- Real-Time

The following sections describe these options:

Device Status

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

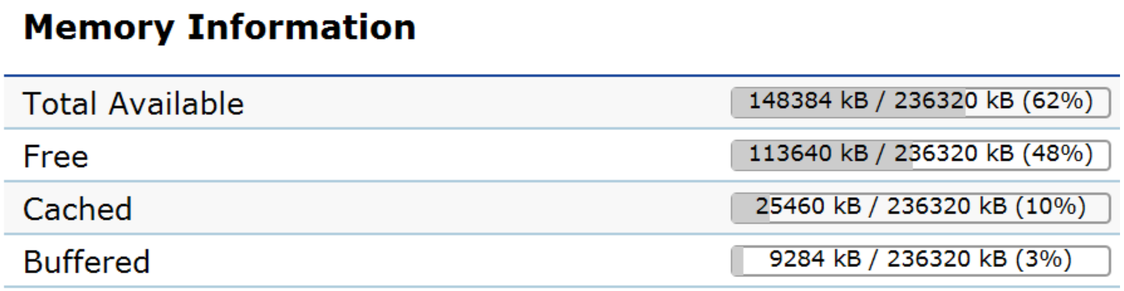
- The **Device Information** section shows general system information such as Device Name, MAC address, Current Time, Firmware Version, and Management VLAN ID



Device Information

Device Name	EWS550AP
Serial Number	173266309
MAC Address	
- LAN	88:DC:96:5C:30:2E
- Wireless LAN - 2.4GHz	88:DC:96:5C:30:44
- Wireless LAN - 5GHz	88:DC:96:5C:30:45
Country	USA
Current Local Time	Mon Sep 4 07:33:23 2017
Uptime	4d 5h 15m 13s
Firmware Version	3.0.0 + 1.8.57
Management VLAN ID	Untagged
Registration Check Code	81466ea8

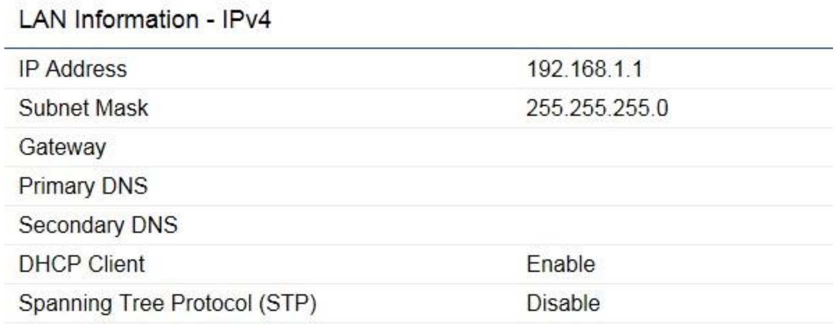
- The Memory Information section shows usage of memory such as Total Available, Free, Cached, Buffered.



Memory Information

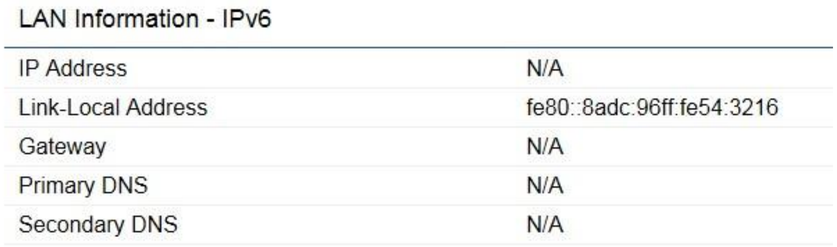
Total Available	148384 kB / 236320 kB (62%)
Free	113640 kB / 236320 kB (48%)
Cached	25460 kB / 236320 kB (10%)
Buffered	9284 kB / 236320 kB (3%)

- The **LAN Information** section shows the Local Area Network settings such as the LAN IP Address, Subnet Mask, Gateway, DNS Address, DHCP Client, and Spanning Tree Protocal (STP) status.



LAN Information - IPv4

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

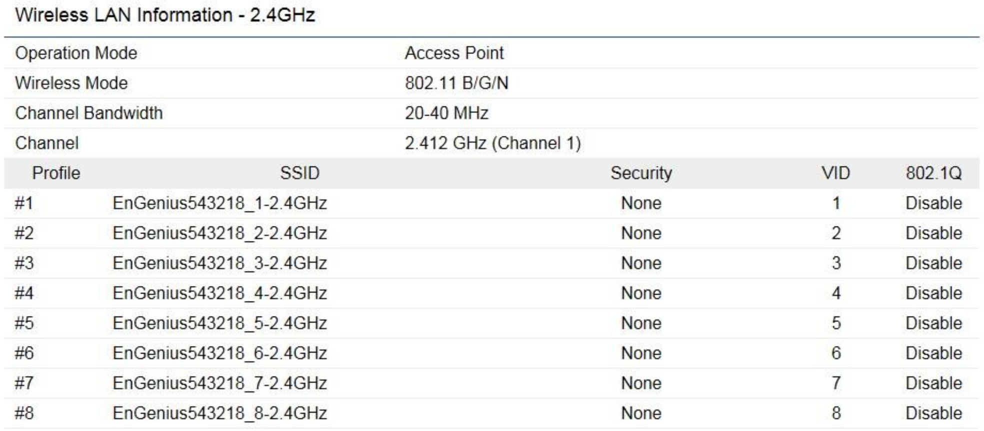


LAN Information - IPv6

IP Address	N/A
Link-Local Address	fe80::8adc:96ff:fe54:3216
Gateway	N/A
Primary DNS	N/A
Secondary DNS	N/A

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

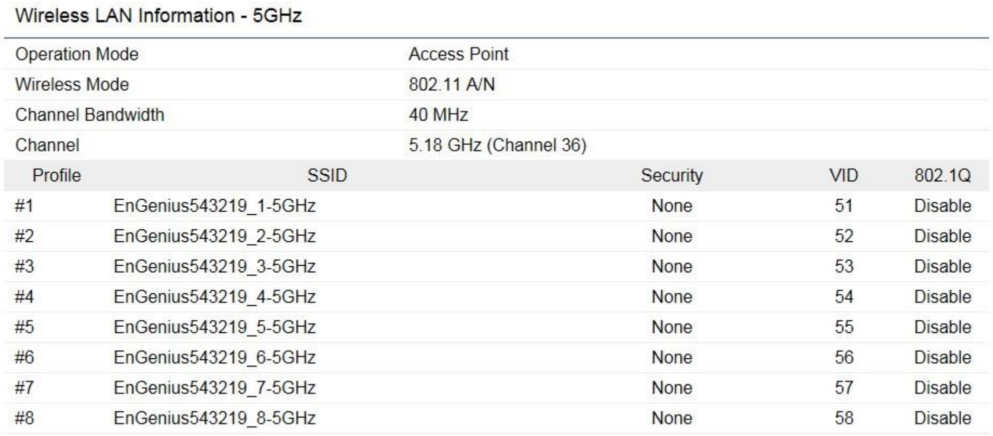
  *Wireless LAN Information – 5 GHz only available for 5 GHz capable models.



Wireless LAN Information - 2.4GHz

Operation Mode	Access Point
Wireless Mode	802.11 B/G/N
Channel Bandwidth	20-40 MHz
Channel	2.412 GHz (Channel 1)

Profile	SSID	Security	VID	802.1Q
#1	EnGenius543218_1-2.4GHz	None	1	Disable
#2	EnGenius543218_2-2.4GHz	None	2	Disable
#3	EnGenius543218_3-2.4GHz	None	3	Disable
#4	EnGenius543218_4-2.4GHz	None	4	Disable
#5	EnGenius543218_5-2.4GHz	None	5	Disable
#6	EnGenius543218_6-2.4GHz	None	6	Disable
#7	EnGenius543218_7-2.4GHz	None	7	Disable
#8	EnGenius543218_8-2.4GHz	None	8	Disable

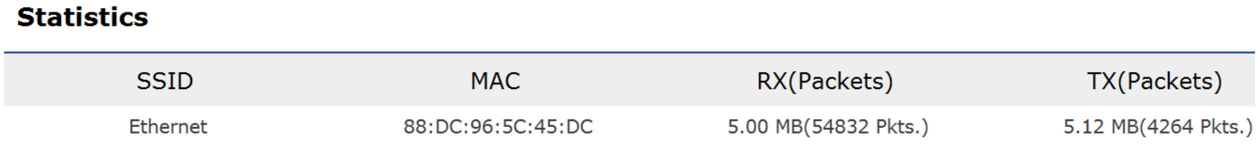


Wireless LAN Information - 5GHz

Operation Mode	Access Point
Wireless Mode	802.11 A/N
Channel Bandwidth	40 MHz
Channel	5.18 GHz (Channel 36)

Profile	SSID	Security	VID	802.1Q
#1	EnGenius543219_1-5GHz	None	51	Disable
#2	EnGenius543219_2-5GHz	None	52	Disable
#3	EnGenius543219_3-5GHz	None	53	Disable
#4	EnGenius543219_4-5GHz	None	54	Disable
#5	EnGenius543219_5-5GHz	None	55	Disable
#6	EnGenius543219_6-5GHz	None	56	Disable
#7	EnGenius543219_7-5GHz	None	57	Disable
#8	EnGenius543219_8-5GHz	None	58	Disable

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

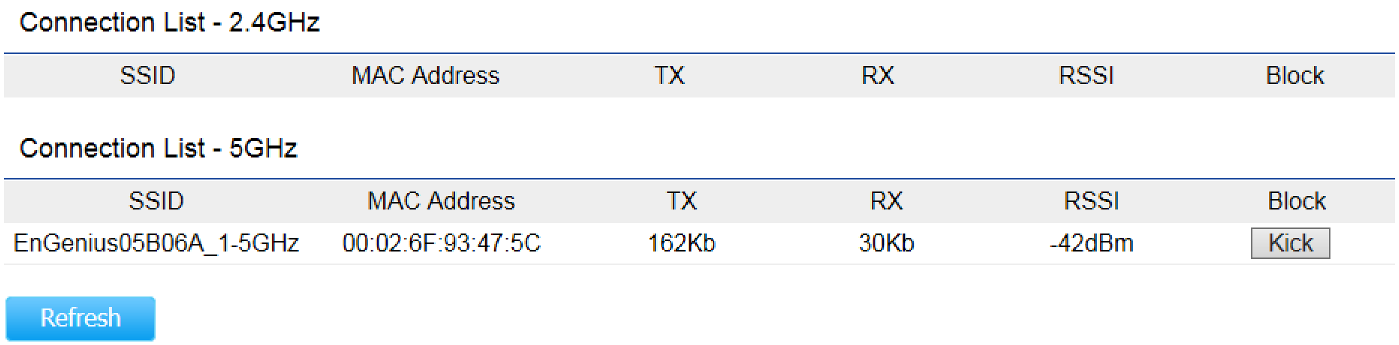


Statistics

SSID	MAC	RX(Packets)	TX(Packets)
Ethernet	88:DC:96:5C:45:DC	5.00 MB(54832 Pkts.)	5.12 MB(4264 Pkts.)

Connections

Clicking the **Connections** link under the **Device Status** menu displays the list of clients associated to the Access Point's 2.4 GHz/5 GHz, along with the MAC address, TX, RX and signal strength for each client. Clicking **Kick** in the Block column removes this client.



Connection List - 2.4GHz

SSID	MAC Address	TX	RX	RSSI	Block

Connection List - 5GHz

SSID	MAC Address	TX	RX	RSSI	Block
EnGenius05B06A_1-5GHz	00:02:6F:93:47:5C	162Kb	30Kb	-42dBm	Kick

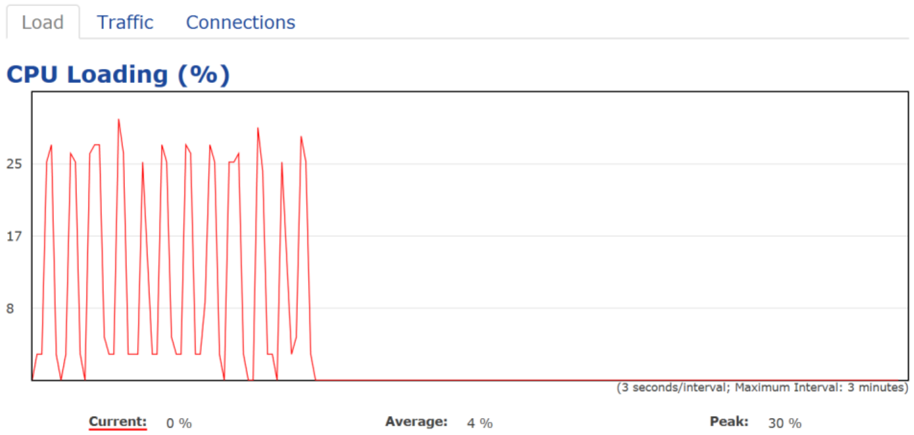
Click **Refresh** to refresh the Connection List page.

Real-Time

Real-Time

The Real-time section contains the following options:

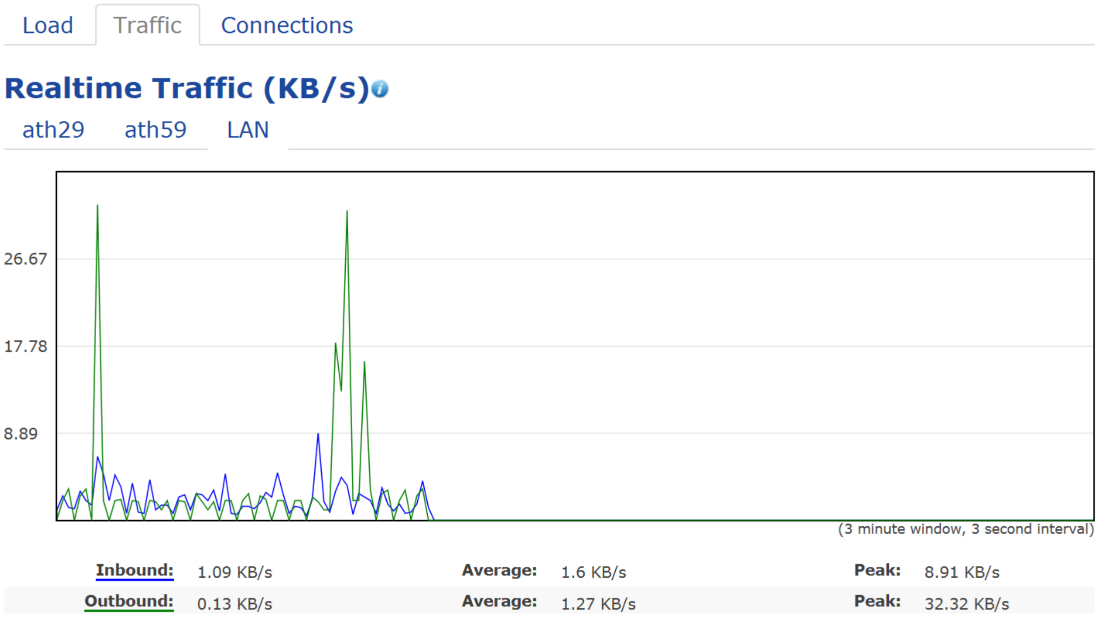
CPU Loading: 3 minutes CPU loading percentage information, it displays current loading, average loading and peak loading status. Left bar is loading percentage; button is time tracing. Interval is every 3 seconds.



CPU Loading (%)

Current: 0 % Average: 4 % Peak: 30 %

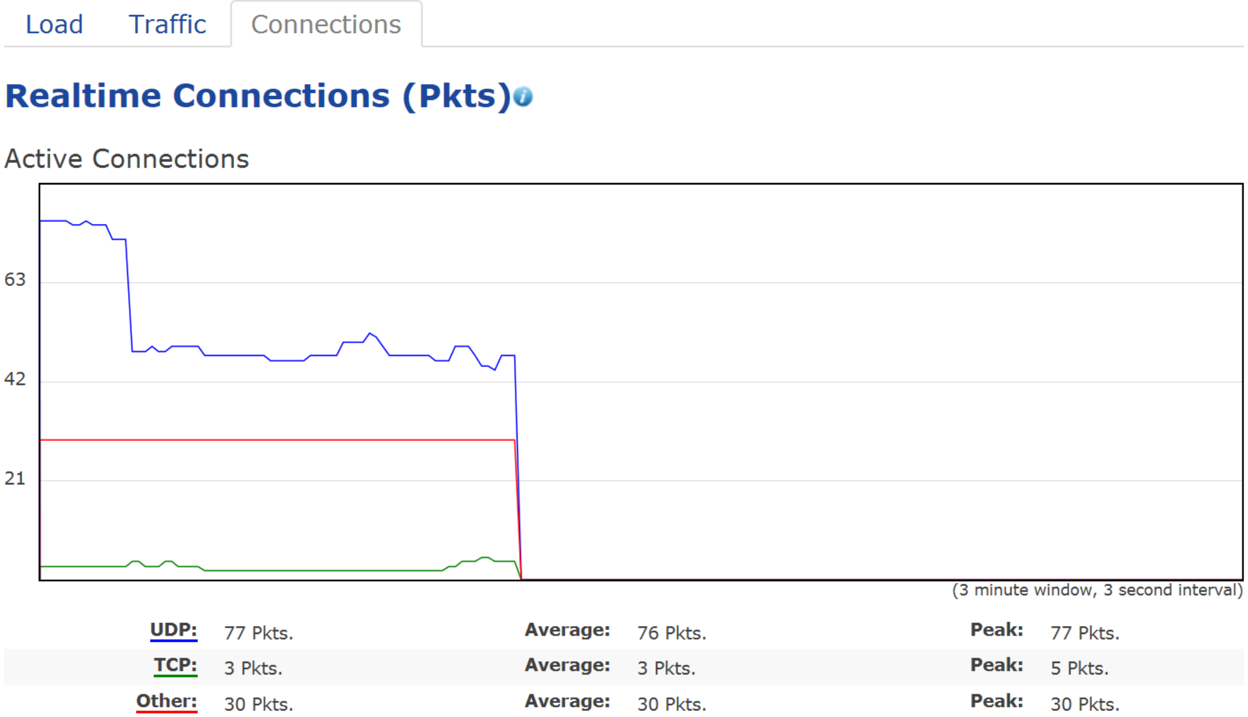
Traffic Loading: 2.4 GHz and 5 GHz and Ethernet port inbound and outbound traffic by current, average, and peak time.



Realtime Traffic (KB/s)

Inbound:	1.09 KB/s	Average:	1.6 KB/s	Peak:	8.91 KB/s
Outbound:	0.13 KB/s	Average:	1.27 KB/s	Peak:	32.32 KB/s

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



Realtime Connections (Pkts)

Active Connections

(3 minute window, 3 second interval)

UDP:	77 Pkts.	Average:	76 Pkts.	Peak:	77 Pkts.
TCP:	3 Pkts.	Average:	3 Pkts.	Peak:	5 Pkts.
Other:	30 Pkts.	Average:	30 Pkts.	Peak:	30 Pkts.

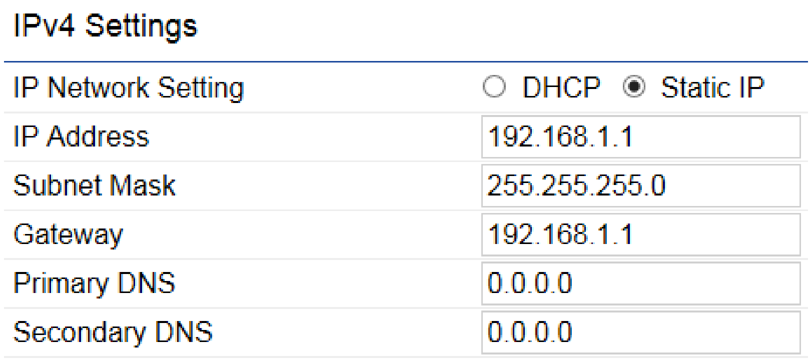
Chapter 5

Network

Basic

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

IPv4 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

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

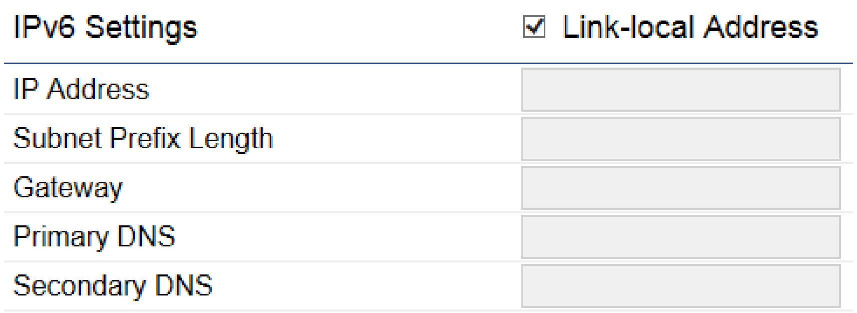
IP Address: The IP Address of this device.

IP 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.

IPv6 Settings



IPv6 Settings ☑ Link-local Address

IP Address	
Subnet Prefix Length	
Gateway	
Primary DNS	
Secondary DNS	

Link-Local Address: Check this if you want to use Link-Local Address.

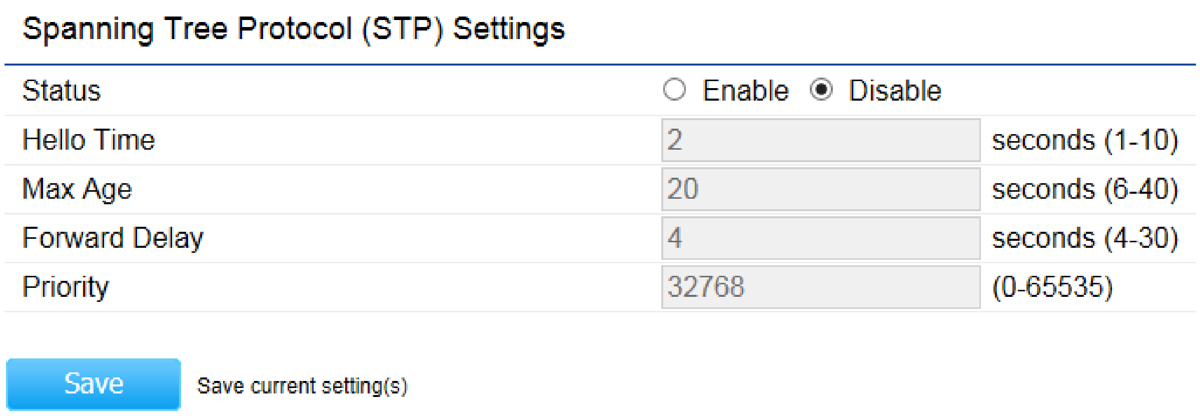
IP Address: The IPv6 IP Address of this device.

Subnet Prefix Length: The IPv6 Subnet Prefix Length of this device.

Gateway: The IPv6 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.

Spanning Tree Settings



Spanning Tree Protocol (STP) Settings

Status	○ Enable ● Disable	
Hello Time	2	seconds (1-10)
Max Age	20	seconds (6-40)
Forward Delay	4	seconds (4-30)
Priority	32768	(0-65535)

Save current setting(s)

Status: Enables or disables the Spanning Tree function.

Hello Time: Specify 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.

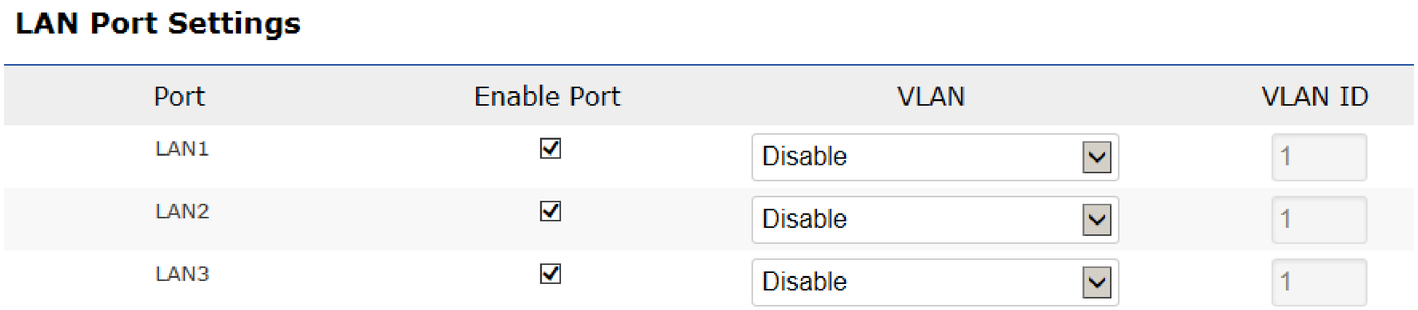
Max Age: Specify Bridge Max Age, in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be inactive.

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.

Priority: Specify the Priority Number. A smaller number has greater priority.

Save: Click Save to confirm the changes.

LAN Port Settings



LAN Port Settings

Port	Enable Port	VLAN	VLAN ID
LAN1	☑	Disable	1
LAN2	☑	Disable	1
LAN3	☑	Disable	1

Enable Port: All Ethernet ports are enabled by default. Unchecking this box disables that port. If you do not want to provide wired access through the AP, uncheck box next to the corresponding LAN port.

VLAN: Check this box to enable VLAN for the LAN port.

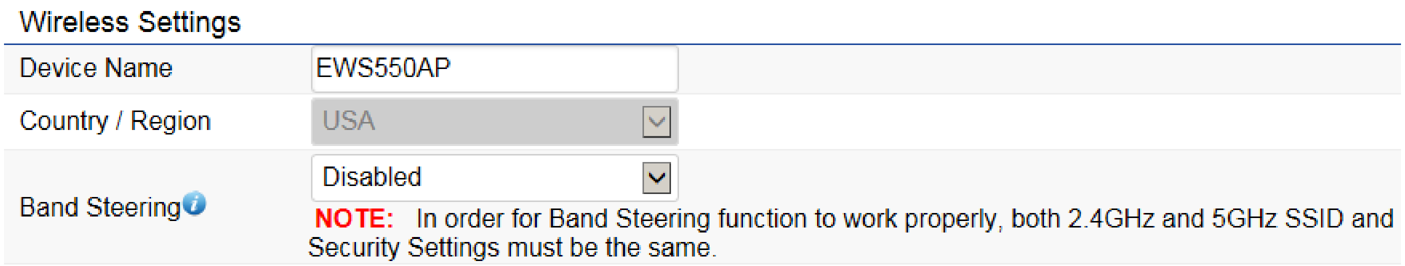
VLAN ID: Enter a VLAN ID to segment traffic arriving on this port to a specific VLAN.

Chapter 6

2.4 GHz & 5 GHz Wireless

Basic

Wireless Settings

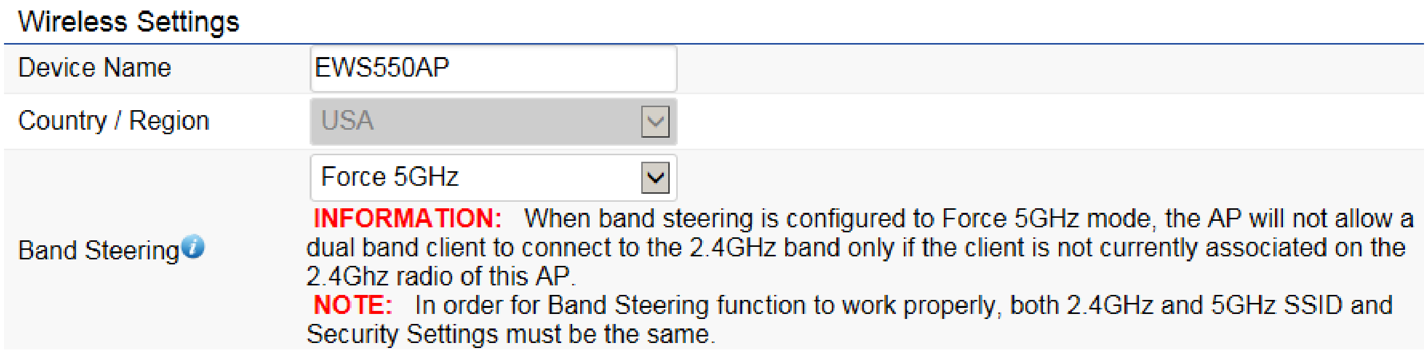


Wireless Settings

Device Name	EWS550AP
Country / Region	USA
Band Steering	Disabled **NOTE:** In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

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.

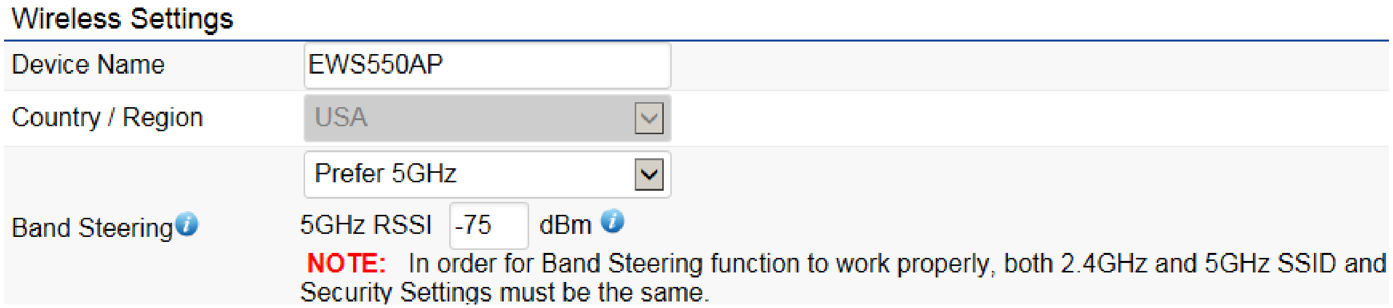
Band Steering: Enable Band Steering to send 802.11a/n/ac clients to the 5 GHz band, where 802.11b/g clients cannot go, and leave 802.11b/g clients in 2.4 GHz to operate at their slower rates. Before implementing this feature, we suggest you to assure the both 2.4 GHz and 5 GHz SSID, as well as security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



Wireless Settings

Device Name	EWS550AP
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. **NOTE:** In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

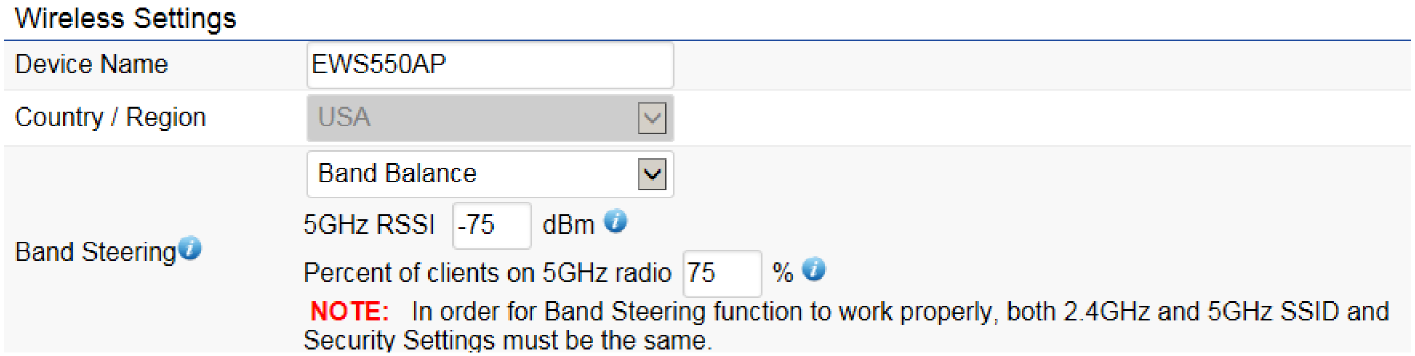
*Force 5 GHz: When band steering is configured to Force 5 GHz mode, the AP will connect dual band capable client devices to the 2.4 GHz band only if the client devices are not currently associated on 2.4 GHz radio in this AP.



Wireless Settings

Device Name	EWS550AP
Country / Region	USA
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 5 GHz**: When band steering is configured to Prefer 5 GHz mode, the AP will steer dual band capable client devices to the 5 GHz radio when the RSSI value of these client devices on the 5 GHz radio is more than set one. The allowed RSSI value for default setting is -75dBm.



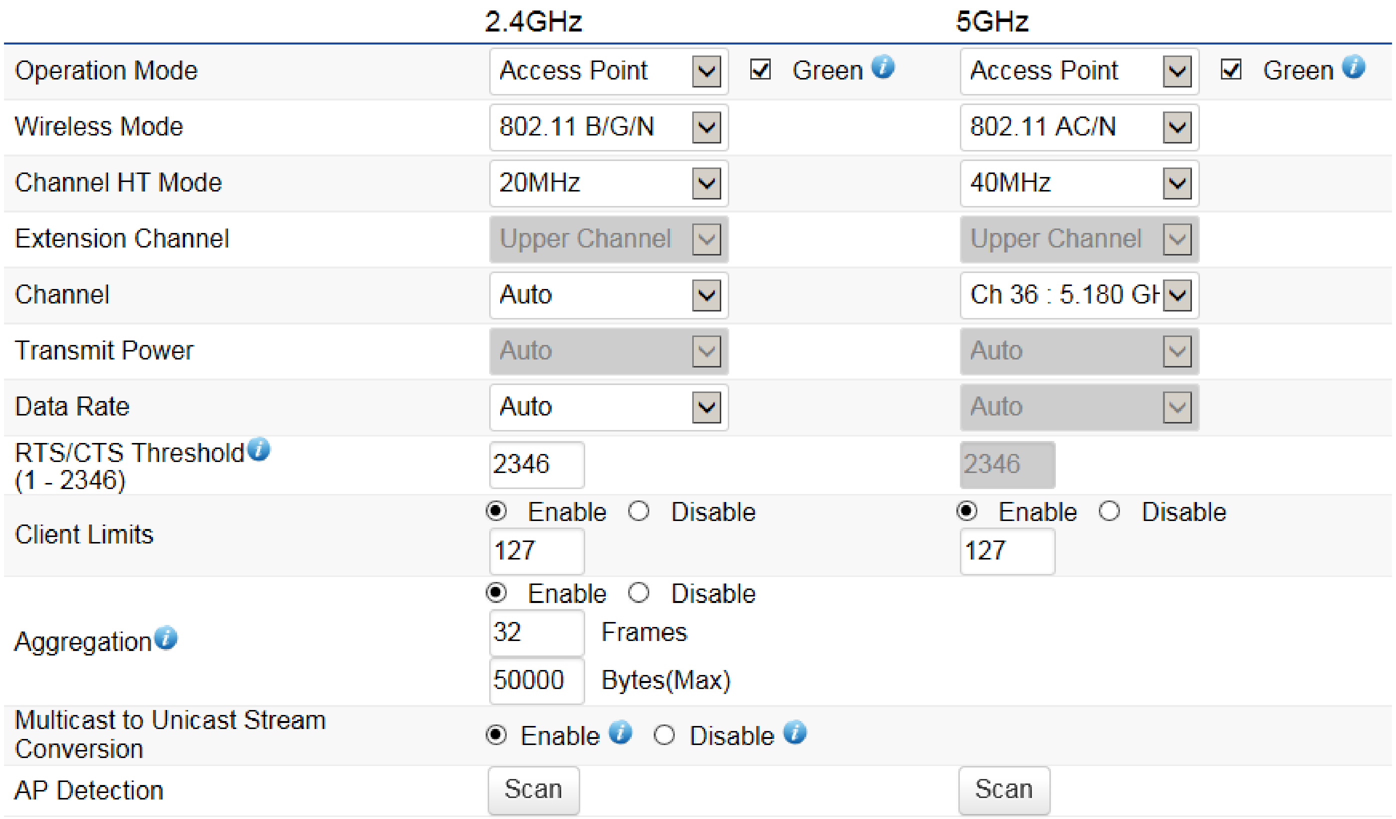
Wireless Settings

Device Name	EWS550AP
Country / Region	USA
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 5 GHz when the RSSI value of these client devices on the 5 GHz radio is more than set one. To evenly allocate RF resource on both the 2.4 GHz and 5 GHz radios, users can also set the portion of client devices on 5 GHz radio to assure smoothly connection. The default value of the 5 GHz radio is 75%.

Save: Click Save to confirm the changes.

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
Extension Channel	Upper Channel	Upper Channel
Channel	Auto	Ch 36 : 5.180 GH
Transmit Power	Auto	Auto
Data Rate	Auto	Auto
RTS/CTS Threshold (1 - 2346)	2346	2346
Client Limits	● Enable ○ Disable 127	● Enable ○ Disable 127
Aggregation	● Enable ○ Disable 32 Frames 50000 Bytes(Max)	
Multicast to Unicast Stream Conversion	● Enable ○ Disable	
AP Detection	Scan	Scan

Operation Mode: Scroll down this list to select operation modes (Access Point, WDS Access Point, and WDS Bridge) for implementing on this radio. The default operation mode is Access Point.

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

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

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

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

*__Default Configuration__: Default setting of channel selection is "**All**" to perform auto channel on existing channel list.

*__None__: Click "None" to disable the setting on this radio. This radio is disabled.

*__Group Configuration__: Click specific groups of channels for performing auto channel function. For example, users can click U-NII-1 and U-NII-3 to perform auto channel on these bands; the mechanism of this AP will select the relatively optimal channel to perform the wireless service.

Data Rate: Select a data rate from the drop-down list. The data rate effects throughput of data in the AP. Select the best balance for you and your network, but note that the lower the data rate, the lower the throughput. The though transmission distance is also lowered.

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

Client Limits: Limits the total number of clients on this radio. Once you set the ceiling of client numbers allowed, the maximum associated client devices will be restricted to this number.

Aggregation: Integrate multiple data packets into one packet to deliver to client devices. This option reduces the number of packets, but also increases packet sizes.

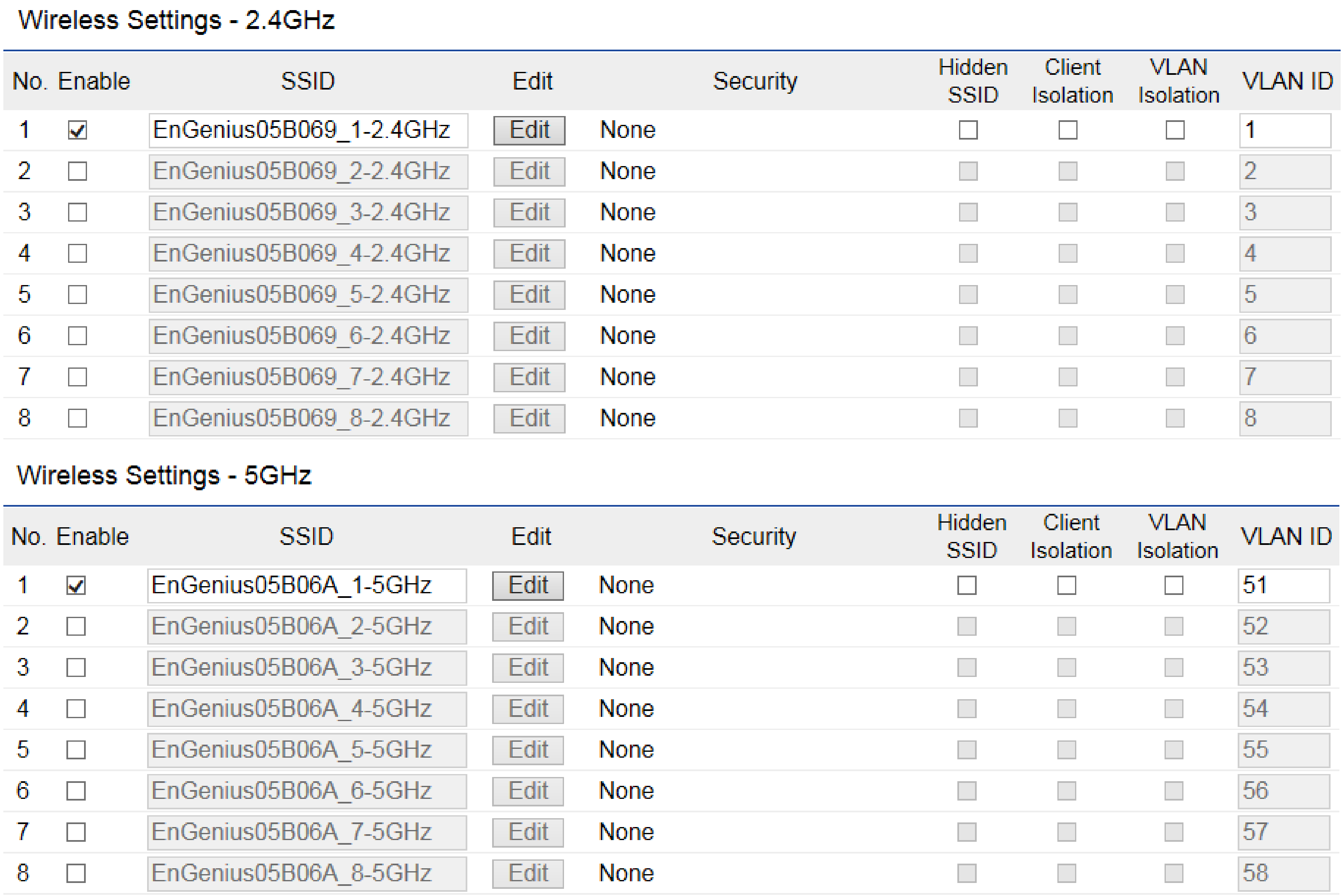
AP Detection: AP Detection can select the best channel to use by scanning nearby areas for Access Points.

Distance: Specifies the distance between Access Points and client devices. The proper setting for this parameter may assist Access Points in avoiding the improper operation when transmitting data under a filed application.

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

2.4 GHz/5 GHz SSID Profile

Under **Wireless Settings**, you can edit the SSID profile to fit your needs. Click **Edit** under the SSID you would like to make changes to.



Wireless Settings - 2.4GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	☑	EnGenius05B069_1-2.4GHz	Edit	None	□	□	□	1
2	□	EnGenius05B069_2-2.4GHz	Edit	None	□	□	□	2
3	□	EnGenius05B069_3-2.4GHz	Edit	None	□	□	□	3
4	□	EnGenius05B069_4-2.4GHz	Edit	None	□	□	□	4
5	□	EnGenius05B069_5-2.4GHz	Edit	None	□	□	□	5
6	□	EnGenius05B069_6-2.4GHz	Edit	None	□	□	□	6
7	□	EnGenius05B069_7-2.4GHz	Edit	None	□	□	□	7
8	□	EnGenius05B069_8-2.4GHz	Edit	None	□	□	□	8

Wireless Settings - 5GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	☑	EnGenius05B06A_1-5GHz	Edit	None	□	□	□	51
2	□	EnGenius05B06A_2-5GHz	Edit	None	□	□	□	52
3	□	EnGenius05B06A_3-5GHz	Edit	None	□	□	□	53
4	□	EnGenius05B06A_4-5GHz	Edit	None	□	□	□	54
5	□	EnGenius05B06A_5-5GHz	Edit	None	□	□	□	55
6	□	EnGenius05B06A_6-5GHz	Edit	None	□	□	□	56
7	□	EnGenius05B06A_7-5GHz	Edit	None	□	□	□	57
8	□	EnGenius05B06A_8-5GHz	Edit	None	□	□	□	58

Current Profile: You can configure up to sixteen (16) different SSIDs (eight (8) per band). If multiple client devices will be accessing the network, you can arrange the devices into SSID groups. Click **Edit** to configure the profile and check whether you want to enable the extra SSID.

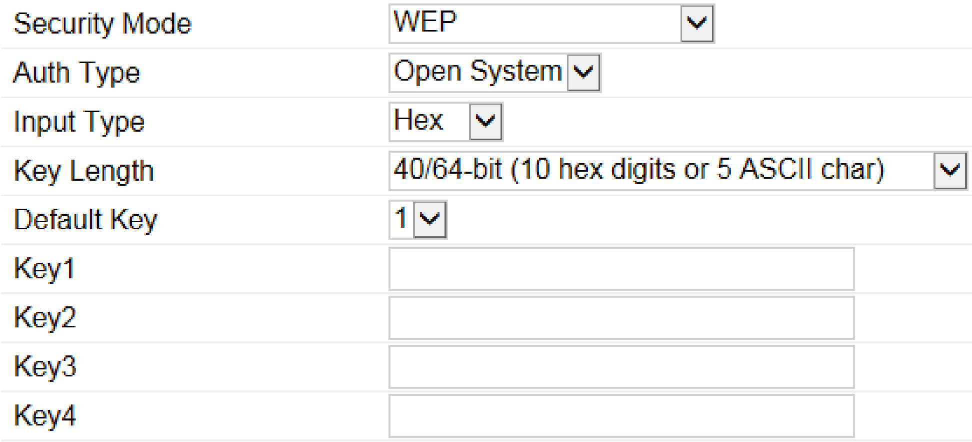
Enable: Check this option to enable this profile.
SSID: Specifies the SSID for the current profile.
Security: Displays the Security Mode the SSID uses. You can click **Edit** to change the security mode. For more details, see the next section.
Hidden SSID: Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
Client Isolation: Check this option to prevent communication between client devices.
VLAN Isolation: Check this option to enable VLAN Isolation feature.
VLAN ID: Specifies the VLAN ID for the SSID profile.

Wireless Security

The Wireless Security section lets you configure the Access Point's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA-Enterprise, WPA2-Enterprise and WPA Mixed Enterprise.

It is strongly recommended that you use **WPA2-PSK**. Click on the **Edit** button under Wireless Settings next to the SSID to change the security settings.

WEP



Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Auth. Type: Select Open System or Shared Key.

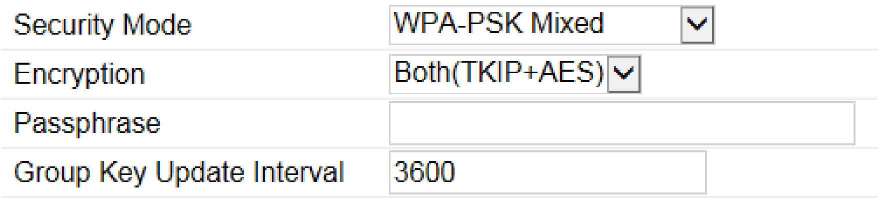
Input Type: ASCII: Regular Text (Recommended) or HEX: Hexadecimal Numbers (For advanced users).

Key Length: Select the desired option and ensure the 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 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: Enter the Key Value or values you wish to use. The default is none.

WPA-PSK/WPA2-PSK (Pre-Shared Key)



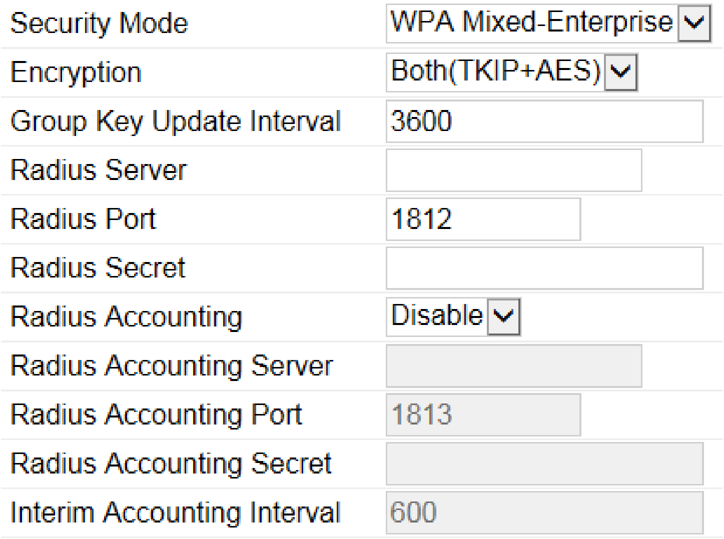
Security Mode	WPA-PSK Mixed
Encryption	Both(TKIP+AES)
Passphrase	
Group Key Update Interval	3600

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard). 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: Specify how often, in seconds, the Group Key changes.

WPA/WPA2-Enterprise



Security Mode	WPA Mixed-Enterprise
Encryption	Both(TKIP+AES)
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP (Temporal Key Integrity Protocol) and

AES (Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.

Group Key Update Interval: Specify how often, in seconds, the group key changes.

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: Enables or disables the 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.

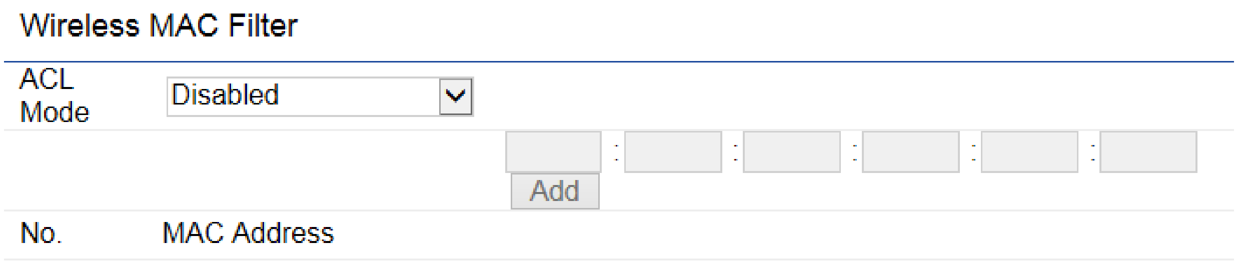
Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

Interim Accounting Interval: Specify 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 MAC Filter

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



ACL Mode: Disabled

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.

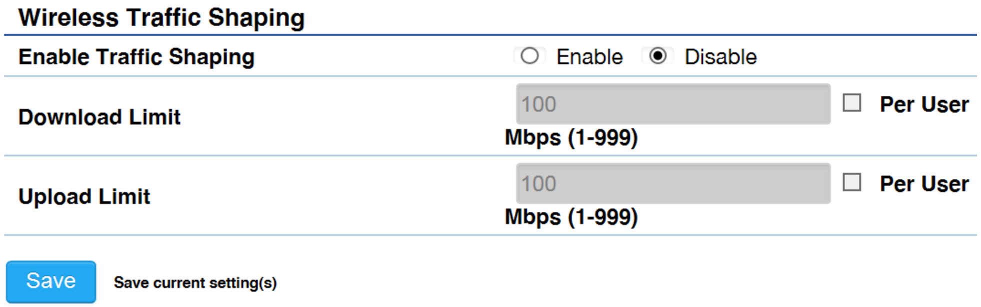
MAC Address: Enter the MAC address of the wireless client.

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

Delete: Deletes the selected entries.

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)

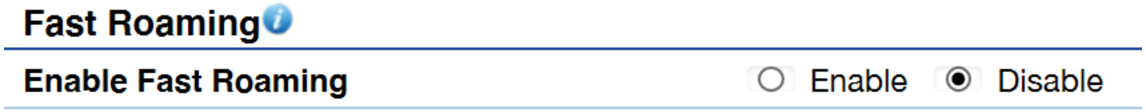
Enable Traffic Shaping: Select to Enable or Disable Wireless Traffic Shaping.
Download Limit: Specifies the wireless transmission speed used for downloading.
Upload Limit: Specifies the wireless transmission speed used for uploading.
Per User: Check this option to enable wireless traffic shaping per user function. This function allow users to limit the maximum download/upload bandwidth for each client devices on this SSID.
Save: Click **Save** to apply 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

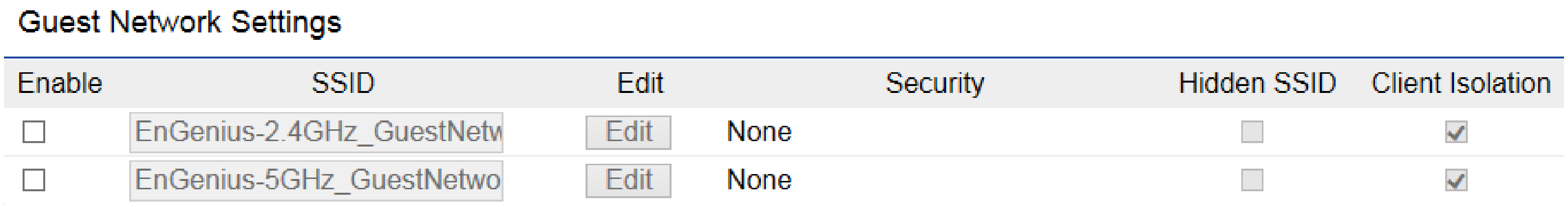
Enable Fast Roaming ○ Enable ● Disable

Enable Fast Roaming: Enable or disable fast roaming feature.

Enable Advanced Search: Enable or disable advanced search feature.

Guest Network

The Guest Network function allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.



Guest Network Settings

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
□	EnGenius-2.4GHz_GuestNetw	Edit	None	□	☑
□	EnGenius-5GHz_GuestNetwo	Edit	None	□	☑

Enable SSID: Select to Enable or Disable SSID broadcasting.

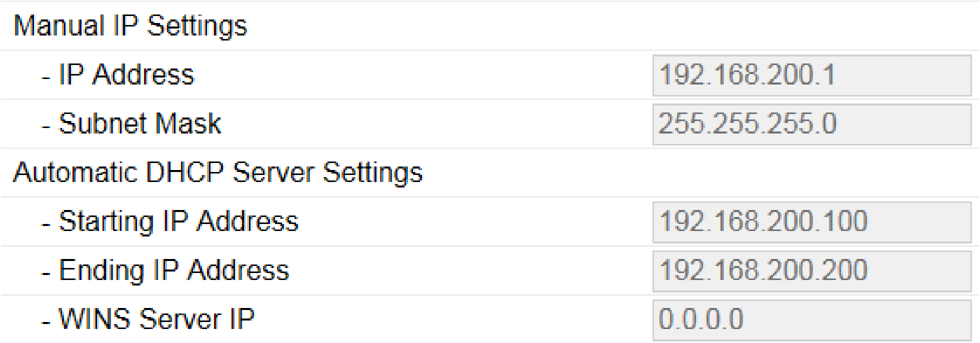
SSID: Specify the SSID for the current profile. This is the name visible on the network to wireless clients.

Security: You can use None or WPA-PSK / WPA2-PSK security for this guest network.

Hidden SSID: Check this option to hide the SSID from broadcasting to discourage wireless users from connecting to a particular SSID.

Client Isolation: Check this option to prevent wireless clients associated with your access point to communicate with other wireless devices connected to the AP.

After enabling Guest Network in the SSID Config page, assign an IP Address, Subnet Mask, and DHCP server IP address range for this Guest Network.



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

Manual IP Settings

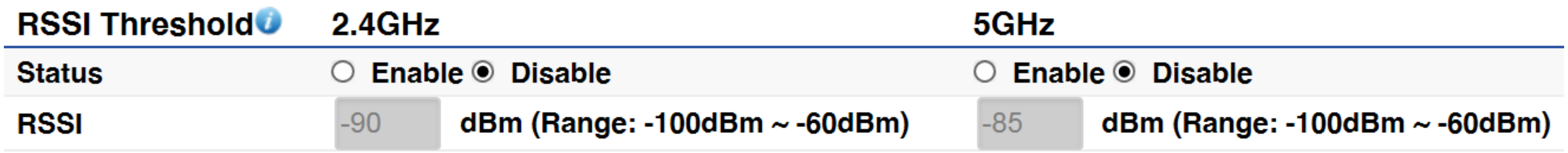
IP Address: Specify an IP Address for the Guest Network
Subnet Mask: Specify the the Subnet Mask IP Address for the Guest Network

Automatic DHCP Server Settings

Starting IP Address: Specify the starting IP Address range for the Guest Network.
Ending IP Address: Specify the ending IP Address range for the Guest Network.
WINS Server IP: Specify the WINS Server IP Address for the Guest Network. WINS means Windows Internet Name Service. It is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

RSSI Threshold

With RSSI Threshold enabled, the AP will send a disassociation request to the wireless client and let it find another AP to handover and associate upon detecting the wireless client’s RSSI value lower than specified. The RSSI value can be adjusted to allow more clients to stay associated to this AP. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently.



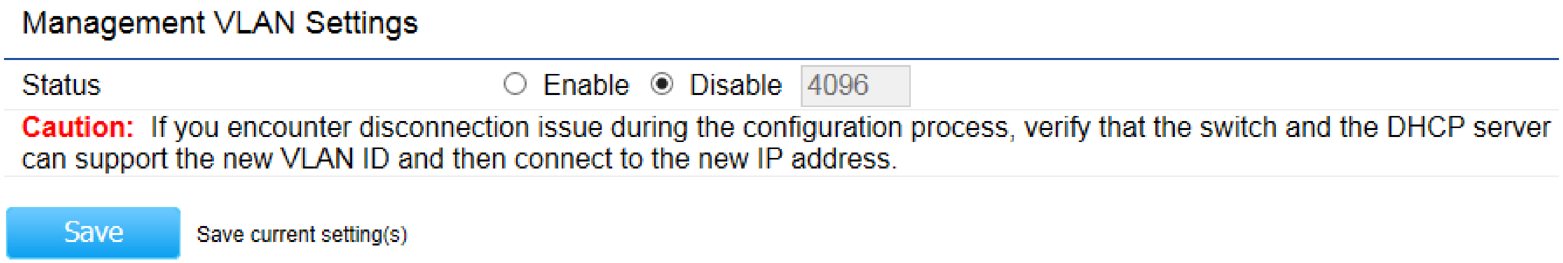
RSSI Threshold	2.4GHz	5GHz
Status	○ Enable ● Disable	○ Enable ● Disable
RSSI	-90 dBm (Range: -100dBm ~ -60dBm)	-85 dBm (Range: -100dBm ~ -60dBm)

RSSI Threshold: Enable the RSSI Threshold 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.

Management VLAN Settings

This section allows you to assign a VLAN tag to the packets. 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 a VLAN do not have to be physically located next to one another on the LAN.



Management VLAN Settings

Status ○ Enable ● Disable 4096

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.

Status: If your network includes VLANs and if tagged packets need to pass through the Access Point, select **Enable** and enter the VLAN ID. Otherwise, click **Disable**.

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

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the Access Point. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the Access Point using the new IP address.

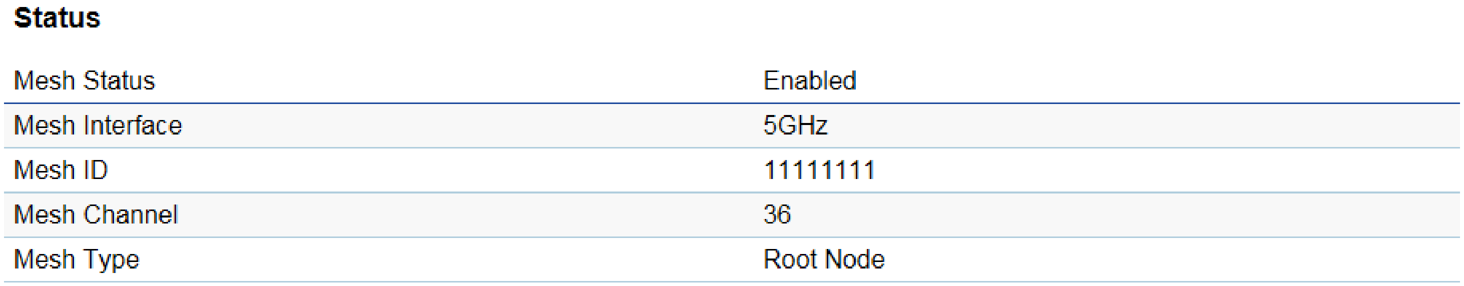
Chapter 7

Mesh

It is simple to deploy and create a mesh network with the EWS controller or ezMaster software in minutes. For stand-alone mode, without these two applications, the user needs to configure the same settings of the Mesh network in each device once the EWS550AP is plugged into any power source. The EnGenius mesh devices automatically optimize routes between wireless mesh devices and creates a truly adaptive mesh infrastructure with other mesh devices in the system. As the wireless environment changes, such as the addition of a new node or broken link, data paths are re-evaluated, and the mesh network self-tunes automatically to maintain its performance. All self-tuning processes are dynamic, occurring in the background and in real time.

Status

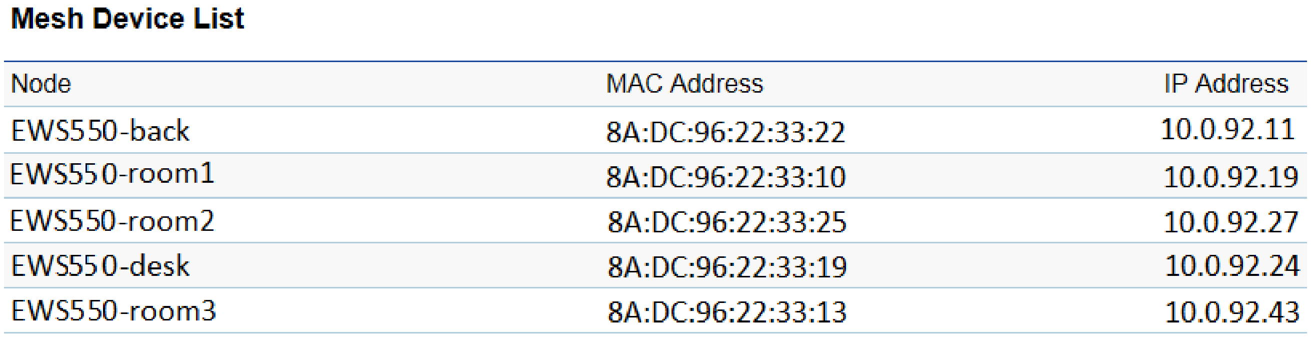
Shows the current status of the mesh network, such as Enable/Disable, Interface, ID, Channel, and Type.



Status

Mesh Status	Enabled
Mesh Interface	5GHz
Mesh ID	11111111
Mesh Channel	36
Mesh Type	Root Node

For this mesh device list, the system will display the information as device name, MAC address, and IP address, which are connected to the mesh network. You can click the “Refresh” button to get a new status again.



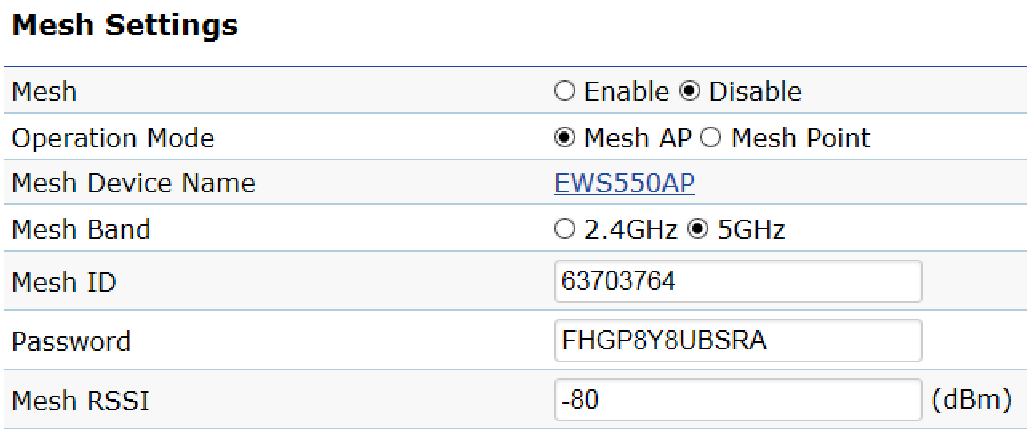
Mesh Device List

Node	MAC Address	IP Address
EWS550-back	8A:DC:96:22:33:22	10.0.92.11
EWS550-room1	8A:DC:96:22:33:10	10.0.92.19
EWS550-room2	8A:DC:96:22:33:25	10.0.92.27
EWS550-desk	8A:DC:96:22:33:19	10.0.92.24
EWS550-room3	8A:DC:96:22:33:13	10.0.92.43

Settings

Each device must have the same settings in this setting page.

Note: If you have changed the settings in the Network Wireless page, please be aware that all the settings must be the same in each device.



Mesh Settings

Mesh	○ Enable ● Disable
Operation Mode	● Mesh AP ○ Mesh Point
Mesh Device Name	EWS550AP
Mesh Band	○ 2.4GHz ● 5GHz
Mesh ID	63703764
Password	FHGP8Y8UBSRA
Mesh RSSI	-80 (dBm)

Mesh: Enable or Disable the mesh function. The system will save the settings even when the mesh function is disabled.

Operation Mode: The **Mesh AP** mode is the mesh point with the wireless AP function. The system will auto disable the wireless AP function when the user selects the **Mesh Point** mode.

Mesh Device Name: Click the hyper link to modify the Mesh device's name from the wireless setting page.

Mesh Band: Select the 2.4 GHz or 5 GHz band for the mesh backbone connection.

Mesh ID: The mesh ID should be a maximum of up to 8 characters in numbers 0 ~ 9.

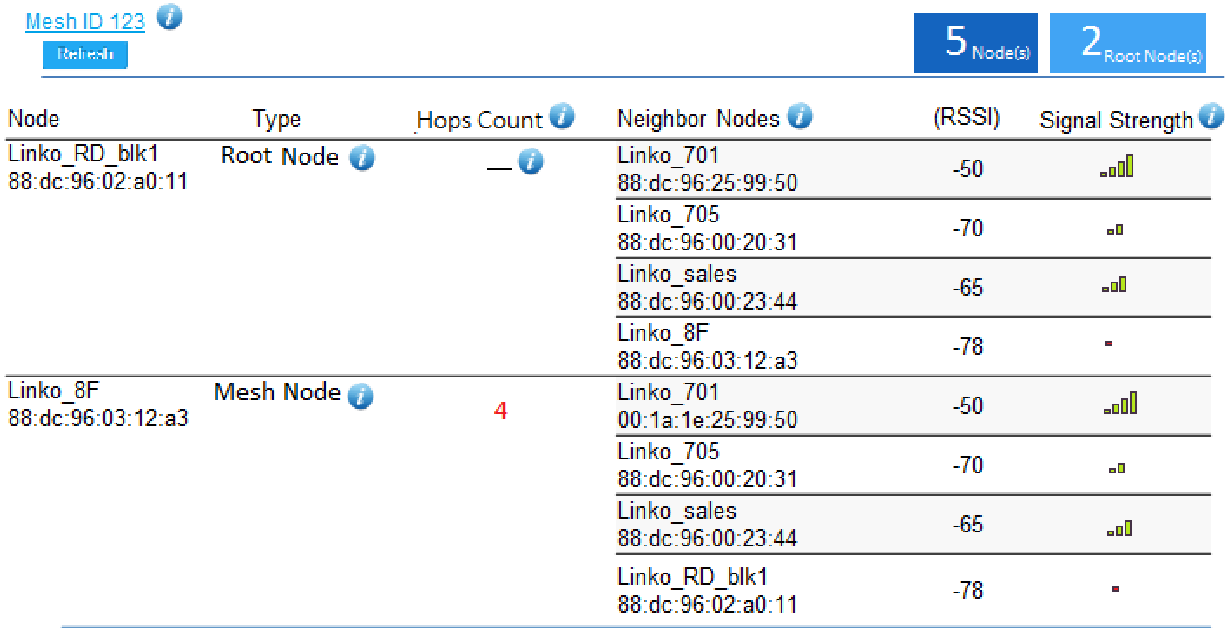
Password: The mesh password should be a maximum of up to 12 characters.

Mesh RSSI: Enter the Mesh RSSI in order to determine the connection procedure which the current wireless link will terminate. The higher the RSSI number, the stronger the signal.

Tools

This diagnostic tools page provides easy ways to check the current status of the mesh network. This section contains the following options:

Node List



Mesh ID 123

Refresh

5 Node(s)

2 Root Node(s)

Node	Type	Hops Count	Neighbor Nodes	(RSSI)	Signal Strength
Linko_RD_blk1 88:dc:96:02:a0:11	Root Node	—	Linko_701 88:dc:96:25:99:50	-50	▂▃▅▇
			Linko_705 88:dc:96:00:20:31	-70	▂▃
			Linko_sales 88:dc:96:00:23:44	-65	▂▃▅
			Linko_8F 88:dc:96:03:12:a3	-78	▪
Linko_8F 88:dc:96:03:12:a3	Mesh Node	4	Linko_701 00:1a:1e:25:99:50	-50	▂▃▅▇
			Linko_705 88:dc:96:00:20:31	-70	▂▃
			Linko_sales 88:dc:96:00:23:44	-65	▂▃▅
			Linko_RD_blk1 88:dc:96:02:a0:11	-78	▪

All connected Mesh nodes will be displayed in this page.

Node: Shows the device's name and MAC address.

Type: There are two types of nodes. The **Root node** is uplinked to the gateway by Ethernet wire, and connected with other mesh nodes by wireless simultaneously.

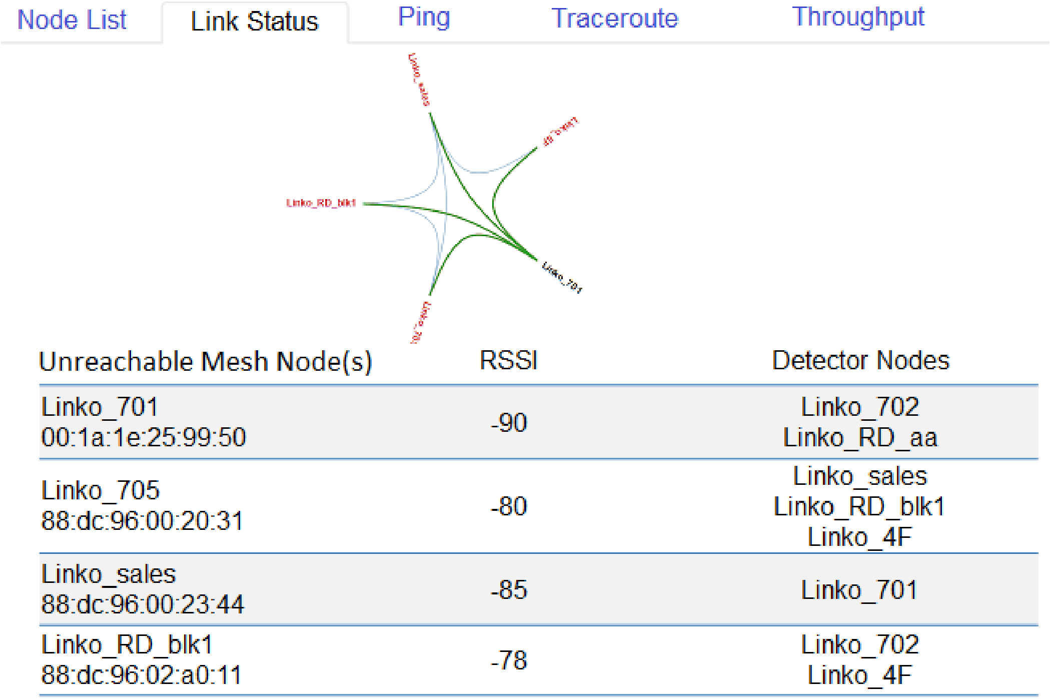
Hops Count: Refers to the number of intermediate devices through which data must pass between the Mesh node and Root node. If the Hops Count number is more than 3, we recommend that you optimize your deployment of the device's location. System shows "—" when the node is a Root or stand-alone node.

Neighbor Nodes: Display all the neighbor nodes which are discovered by an individual mesh node, no matter whether or not its signal strength allows it to link or not.

RSSI: The current signal strength of the node.

Signal Strength: There are four RSSI levels the signal bar will display. If the RSSI is below -76db, then it will display a red bar.

Link Status



Unreachable Mesh Node(s)	RSSI	Detector Nodes
Linko_701 00:1a:1e:25:99:50	-90	Linko_702 Linko_RD_aa
Linko_705 88:dc:96:00:20:31	-80	Linko_sales Linko_RD_blk1 Linko_4F
Linko_sales 88:dc:96:00:23:44	-85	Linko_701
Linko_RD_blk1 88:dc:96:02:a0:11	-78	Linko_702 Linko_4F

The Mesh network view is an overview for all mesh nodes.

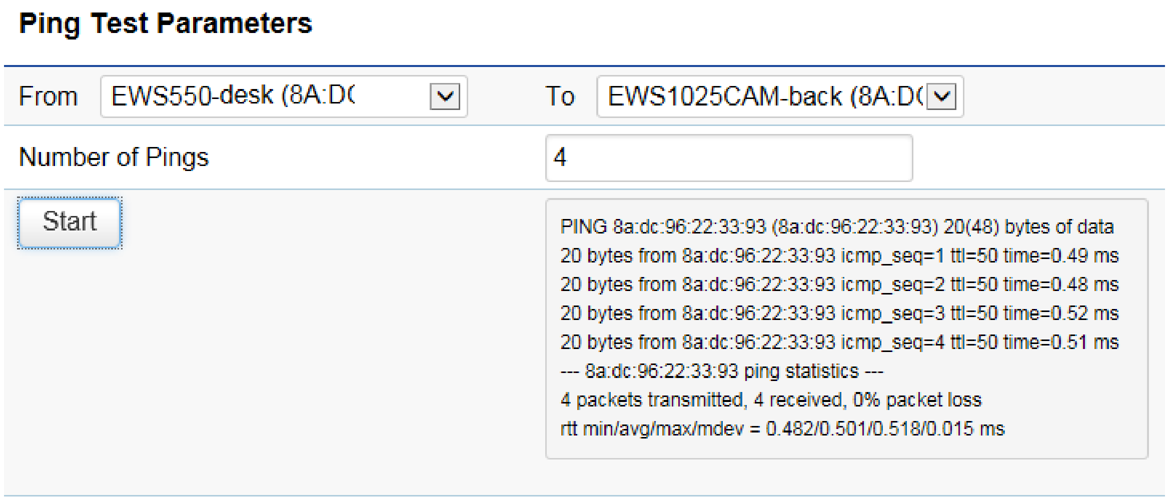
Mesh View: Mouse over any Mesh node (black) to see the linking status, which is linked to other Mesh nodes (blue) with a green line.

Unreachable Mesh Node(s): The nodes that cannot be connected to the mesh network due to a weak signal detected by neighboring nodes.

RSSI: The node is not allowed to link with mesh if its current signal strength is continuously lower than the Mesh RSSI in the mesh settings page.

Detector Nodes: The neighbor node(s) that detect the unreachable mesh node.

Ping



Ping Test Parameters

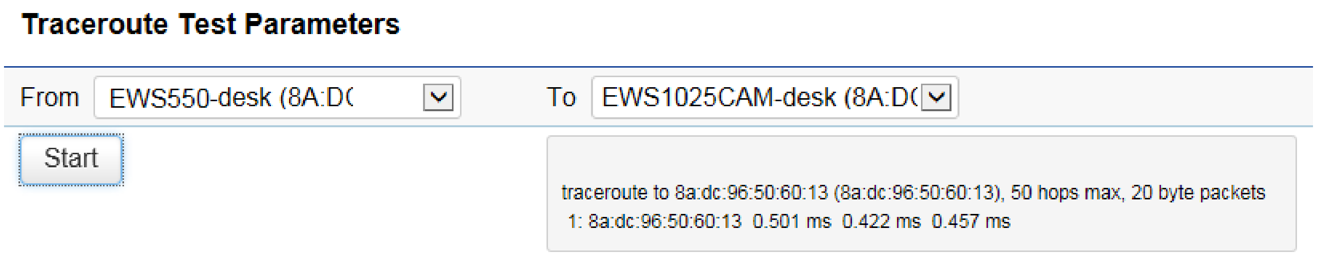
From EWS550-desk (8A:D(To EWS1025CAM-back (8A:D(

Number of Pings 4

```
PING 8a:dc:96:22:33:93 (8a:dc:96:22:33:93) 20(48) bytes of data
20 bytes from 8a:dc:96:22:33:93 icmp_seq=1 ttl=50 time=0.49 ms
20 bytes from 8a:dc:96:22:33:93 icmp_seq=2 ttl=50 time=0.48 ms
20 bytes from 8a:dc:96:22:33:93 icmp_seq=3 ttl=50 time=0.52 ms
20 bytes from 8a:dc:96:22:33:93 icmp_seq=4 ttl=50 time=0.51 ms
--- 8a:dc:96:22:33:93 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss
rtt min/avg/max/mdev = 0.482/0.501/0.518/0.015 ms
```

This page allows you to analyze the connection quality of a mesh node to another mesh node in the mesh network.

Trace Route



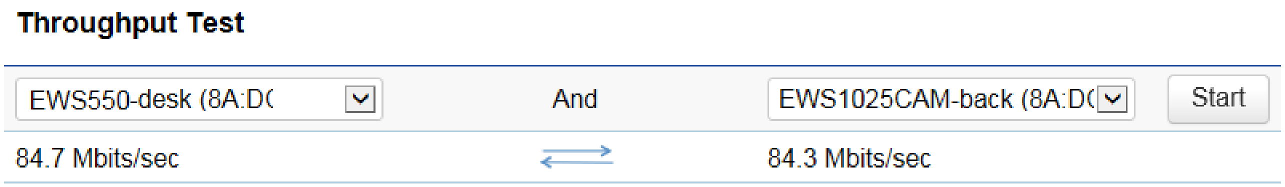
Traceroute Test Parameters

From EWS550-desk (8A:D(To EWS1025CAM-desk (8A:D(

```
traceroute to 8a:dc:96:50:60:13 (8a:dc:96:50:60:13), 50 hops max, 20 byte packets
 1: 8a:dc:96:50:60:13  0.501 ms  0.422 ms  0.457 ms
```

This page allows you to analyze the routing table to a target from a mesh node to another mesh node in the mesh network.

Throughput



Throughput Test

EWS550-desk (8A:D(	And	EWS1025CAM-back (8A:D(	Start
84.7 Mbits/sec	⇄	84.3 Mbits/sec	

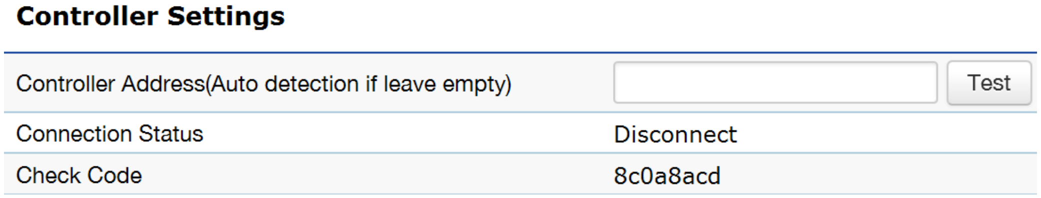
This page allows you to analyze the throughput from a mesh node to another mesh node in the mesh network.

Chapter 8

Management

Controller Settings

With an EnGenius EWS switch or ezMaster management, user can add the Access Point to the management list by its check code.



Controller Settings

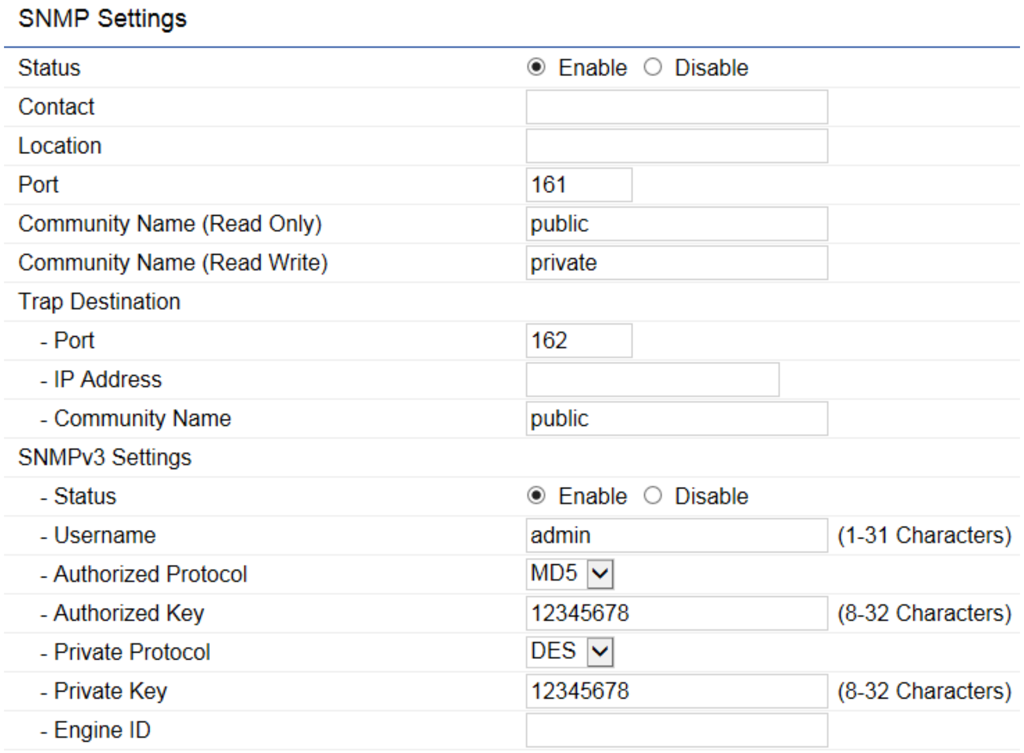
Controller Address(Auto detection if leave empty)	
Connection Status	Disconnect
Check Code	8c0a8acd

Controller Address: Input the IP address of the EnGenius EWS switch or ezMaster, then click “Test.”

Connection Status: After clicking “Test,” it will display the connection between the Access Point and the EnGenius EWS switch or ezMaster.

SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This 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) return the data stored in their Management Information Bases. To configure SNMP Settings, click under the **Advanced** tab on the side bar under **Management**.



SNMP Settings

Status	● Enable ○ Disable	
Contact		
Location		
Port	161	
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		

Status: Enables or Disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device.

Port: Displays the port number.

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 port and IP address of the computer that will receive the SNMP traps.

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

SNMPv3 Status: Enables or Disables the SNMPv3 feature.

User Name: Specifies the username for the SNMPv3 feature.

Auth. Protocol: Select the Authentication Protocol type: MDS or SHA.

Auth. Key: Specify the Authentication Key for authentication.

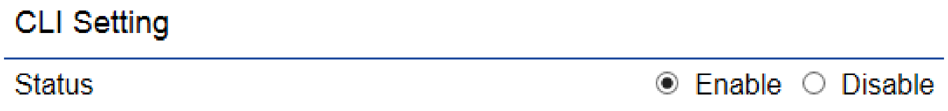
Priv. Protocol: Select the Privacy Protocol type: DES.

Priv. Key: Specifies the privacy key for privacy.

Engine ID: Specifies the Engine ID for SNMPv3.

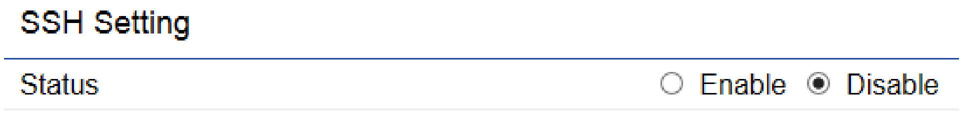
CLI/SSH Settings

Most users will configure the device through the graphical user interface (GUI). However, for those who prefer an alternative method, there is the command line interface (CLI). The CLI can be accessed through a command console, modem or Telnet connection. For security concerns, you can enable SSH (Secure Shell) to establish a secure data communication.



CLI Setting

Status ● Enable ○ Disable



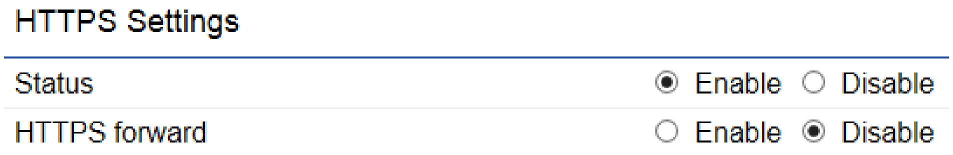
SSH Setting

Status ○ Enable ● Disable

CLI Status: Select **Enable** or **Disable** to modify the Access Point via a command line interface (CLI).
SSH Status: Select **Enable** or **Disable** to modify the Access Point via a command line interface (CLI) with a secure channel.

HTTPS Settings

Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.



HTTPS Settings

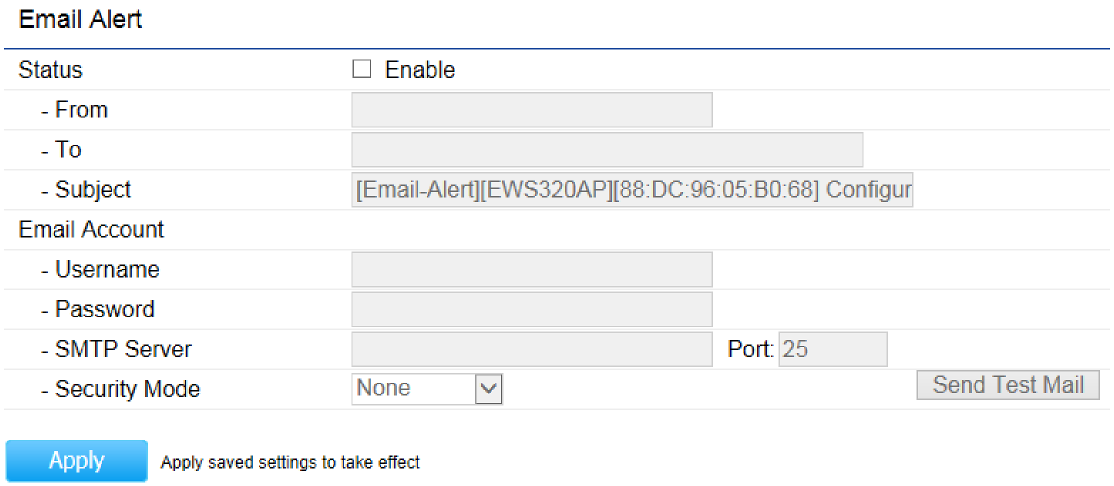
Status	● Enable ○ Disable
HTTPS forward	○ Enable ● Disable

Status: Select **Enable** or **Disable** to modify the Access Point via HTTPS.

HTTPS Forward: Enabling this option will forward the AP modification to HTTPS if the user tries HTTP to access the Access Point.

Email Alert

The Access Point will send email alerts when configurations have been changed.



Email Alert

Status	□ Enable
- From	
- To	
- Subject	[Email-Alert][EWS320AP][88:DC:96:05:B0:68] Configur
Email Account	
- Username	
- Password	
- SMTP Server	Port: 25
- Security Mode	None ▾ Send Test Mail

Apply   Apply saved settings to take effect

Status: Check **Enable** for Email Alert feature.

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

To: Enter the email address to show the email recipient.

Subject: Enter the subject to show a clearly identifiable email subject.

Email Account

Username/Password: Enter the username and password required to connect to the SMTP server.

SMTP Server/Port: Enter the IP address/domain name and port of the SMTP server. The default port of SMTP Server is port 25.

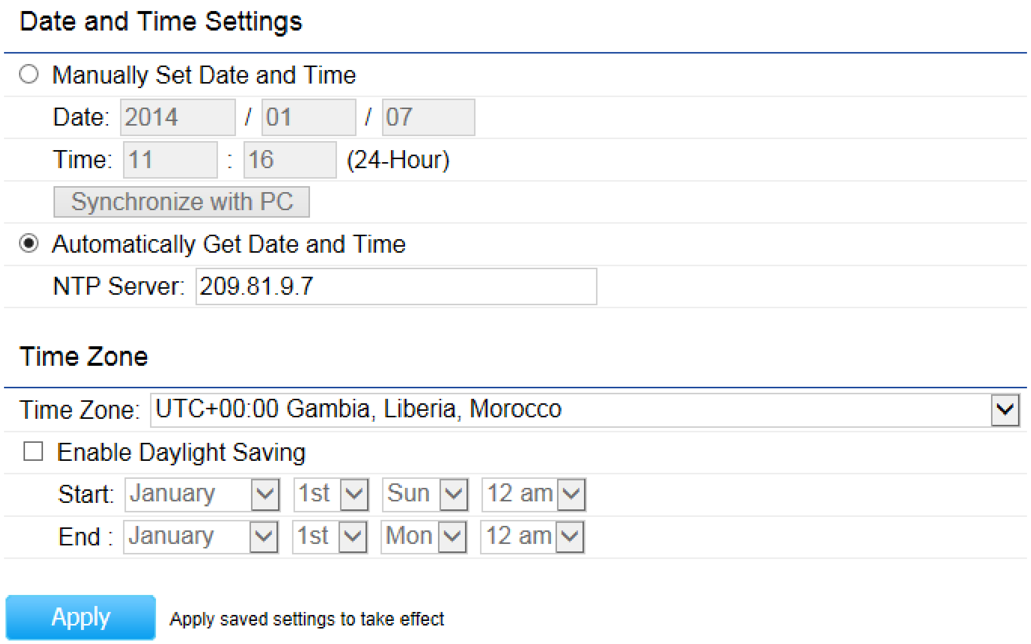
Security Mode: Select the security mode for the Email alert. The options are None, SSL/TLS, and STARTTLS.

Send Test Mail: Click **Send Test Mail** button to test the Email Alert setup.

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

Date and Time Settings

This page allows you to set the internal clock of the Access Point. To access the Date and Time settings, click **Time Zone** under the **Management** tab on the side bar.



Date and Time Settings

○ Manually Set Date and Time

Date: 2014 / 01 / 07

Time: 11 : 16 (24-Hour)

Synchronize with PC

● Automatically Get Date and Time

NTP Server: 209.81.9.7

Time Zone

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

□ Enable Daylight Saving

Start: January 1st Sun 12 am

End : January 1st Mon 12 am

Apply — Apply saved settings to take effect

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

Synchronize with PC: Click to synchronize the Access Point's internal clock with the computer's time.

Automatically Get Date and Time: Enter the IP address of a network time protocol (NTP) server or use the default NTP server to have the internal clock set automatically.

Time Zone: Choose the time zone you would like to use from the drop-down list.

Enable Daylight Savings: Check the box to enable or disable daylight savings time for the Access Point. Next, enter the dates that correspond to the present year's daylight savings time.

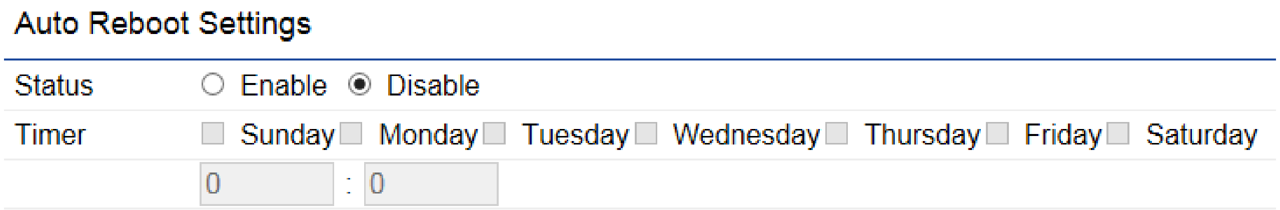
Click **Apply** to save the changes.

Wi-Fi Scheduler

Use the schedule function to reboot the Access Point or control the wireless availability on a routine basis. The Schedule function relies on the GMT time setting acquired from an NTP server. For details on how to connect the Access Point to an NTP server, see Date and Time Settings.

Auto Reboot Settings

Specify how often you would like to reboot the Access Point.



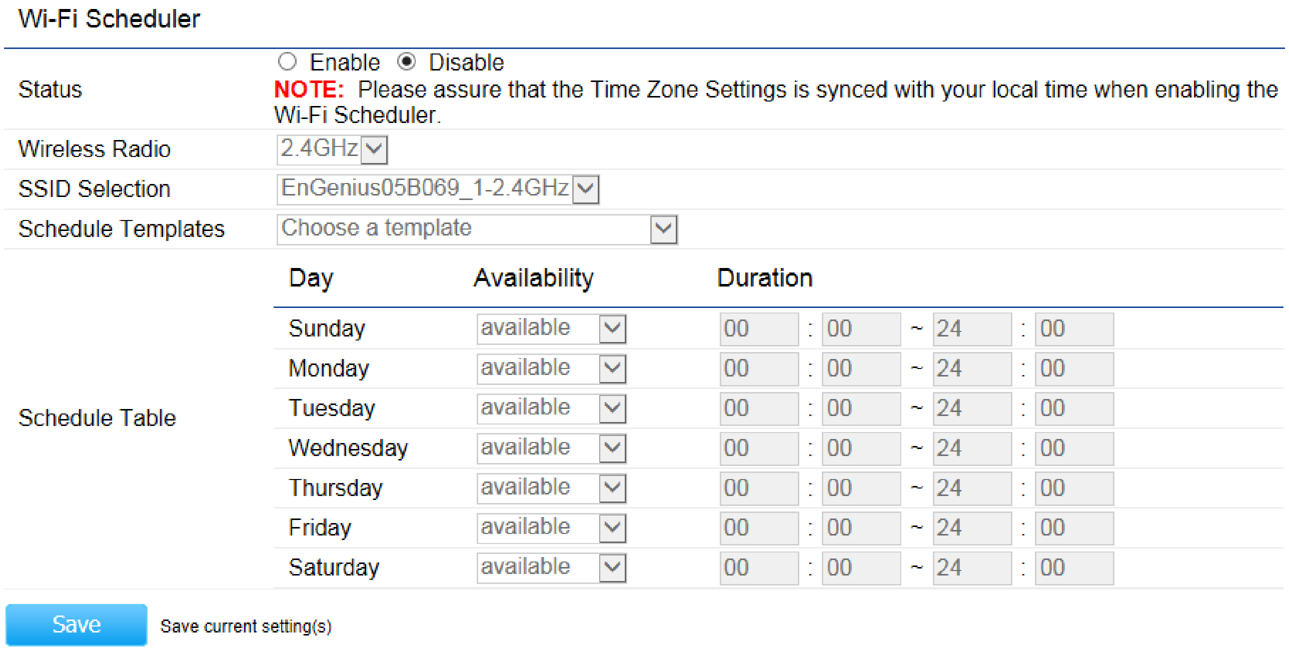
Auto Reboot Settings

Status	○ Enable ● Disable
Timer	□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
	0 : 0

Status: Enables or disables the Auto Reboot function.

Timer: Specifies the time and frequency in rebooting the Access Point by Min., Hour, and Day.

Wi-Fi Scheduler



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	EnGenius05B069_1-2.4GHz
Schedule Templates	Choose a template

Schedule Table

Day	Availability	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 to use Wi-Fi Schedule.

SSID Selection: Select a SSID to use Wi-Fi Schedule.

Schedule Templates: There are three (3) templates available: Always available, Available 8-5 daily, and Available 8-5 daily except weekends. Select **Custom** schedule if you want to set the schedule manually.

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

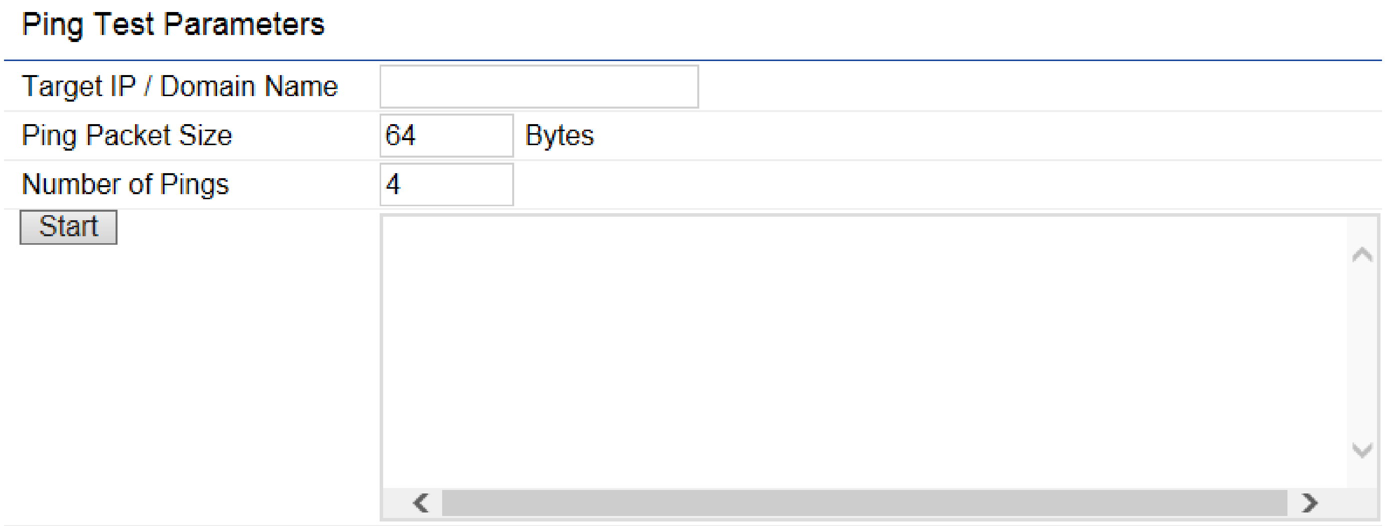
Duration: The Start Time is entered in two fields. The first box is for hours and the second box is for minutes. The End Time is entered in the same format as the Start Time.

Schedule Table: Set the schedule manually.

Tools

This section allows you to analyze the connection quality of the Access Point and trace the routing table to a target in the network.

Ping Test Parameters



Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

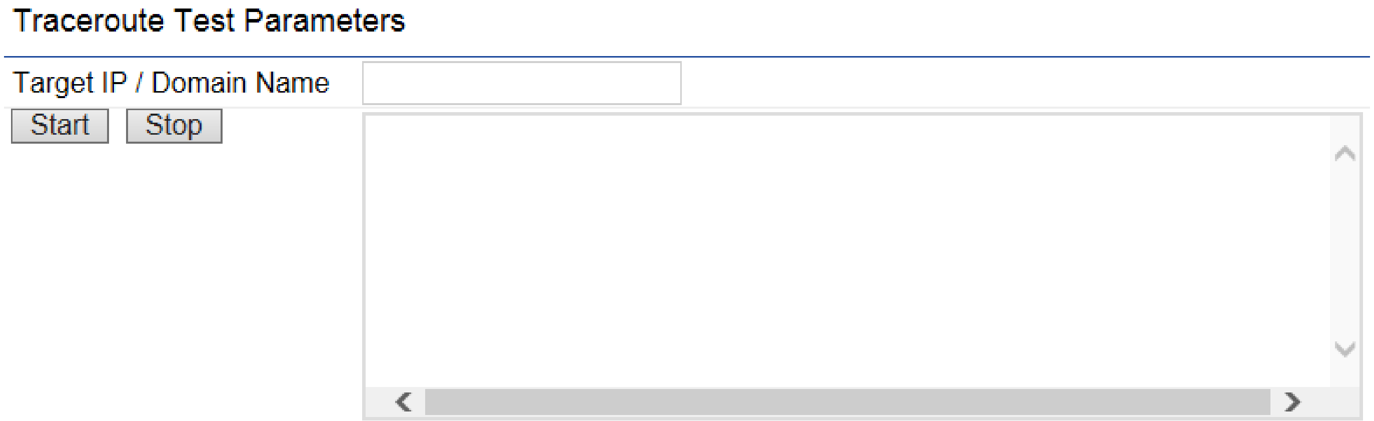
Target IP/Domain Name: Enter the IP address or Domain name you would like to search.

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

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

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

Traceroute Parameters

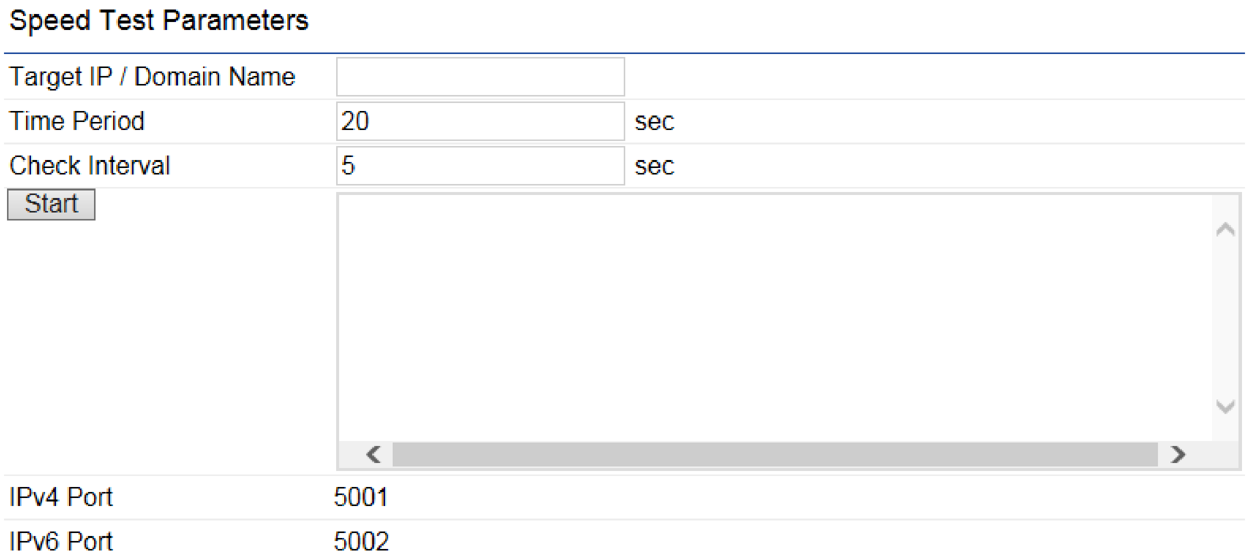


Target IP/Domain Name: Enter an IP address or domain name you wish to trace.

Start: Click **Start** to begin the traceroute operation.

Stop: Halts the traceroute test.

Speed Test Parameters



Speed Test Parameters

Target IP / Domain Name		
Time Period	20	sec
Check Interval	5	sec
IPv4 Port	5001	
IPv6 Port	5002	

Target IP/Domain Name: Enter an IP address or domain name on which you want to run a Speed Test.

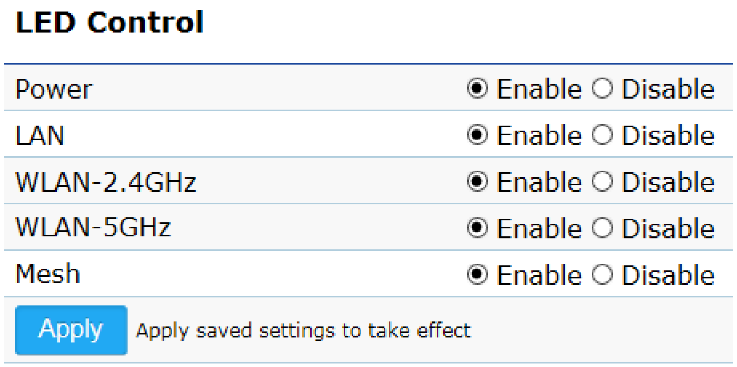
Time Period: Enter the time in seconds that you would like the test to run, and in how many intervals.

Start: Starts the Speed Test.

IPv4/IPv6 Port: The Access Point uses IPv4 port 5001 and IPv6 port 5002 for the speed test.

LED Control

This section allows you to control the LED control functions: Power status, LAN interface, and 2.4 GHz/5 GHz WLAN interface.



LED Control

Power	● Enable ○ Disable
LAN	● Enable ○ Disable
WLAN-2.4GHz	● Enable ○ Disable
WLAN-5GHz	● Enable ○ Disable
Mesh	● 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.

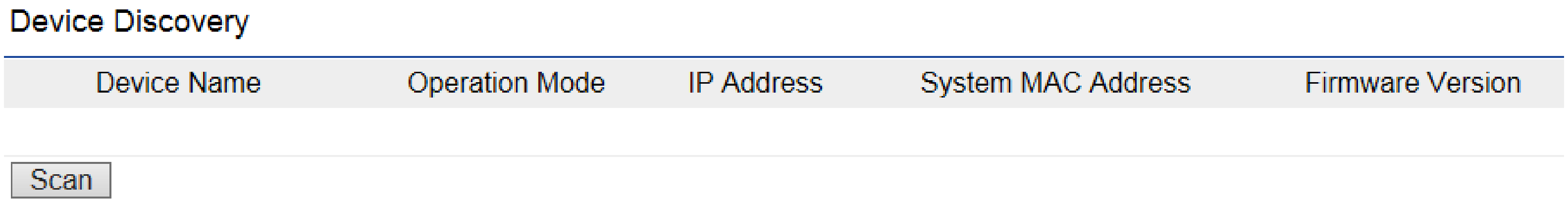
WLAN-5 GHz: Enables or disables the WLAN-5 GHz LED indicator.

Mesh: Enables or disables the Mesh LED indicator.

Click **Apply** to save the settings after selecting your choices from the boxes.

Device Discovery

Under Device Discovery, choose the Access Point to automatically scan for local devices to connect to. Click **Scan** to begin the process.



Device Discovery

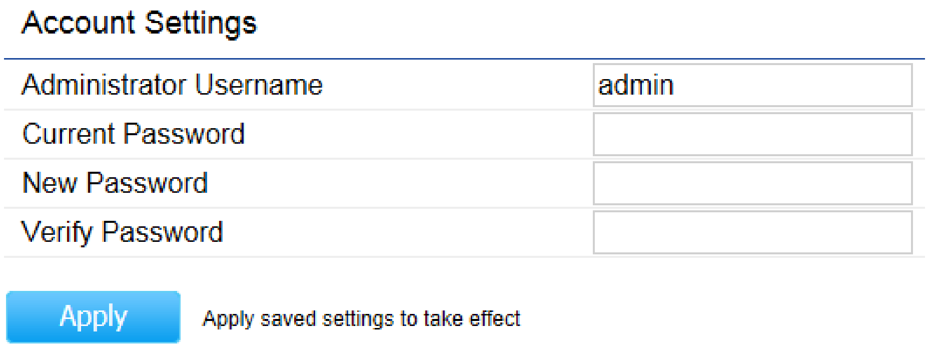
Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

Chapter 9

System Manager

Account Setting

This page allows you to change the username and password of the device. 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

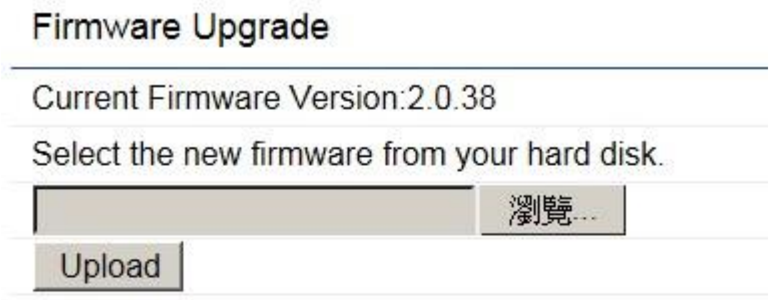
Administrator Username	admin
Current Password	
New Password	
Verify Password	

Administrator Username: Enter a new username for logging in to the Administrator Username entry box.
Current Password: Enter the old password for logging in to the Current 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 Verify Password entry box for confirmation.
Apply: Click **Apply** to save the changes.

Note: It is highly recommended that you change your password to something more unique for greater security.

Firmware Upgrade

This page allows you to upgrade the Firmware of the Access Point.



Firmware Upgrade

Current Firmware Version:2.0.38

Select the new firmware from your hard disk.

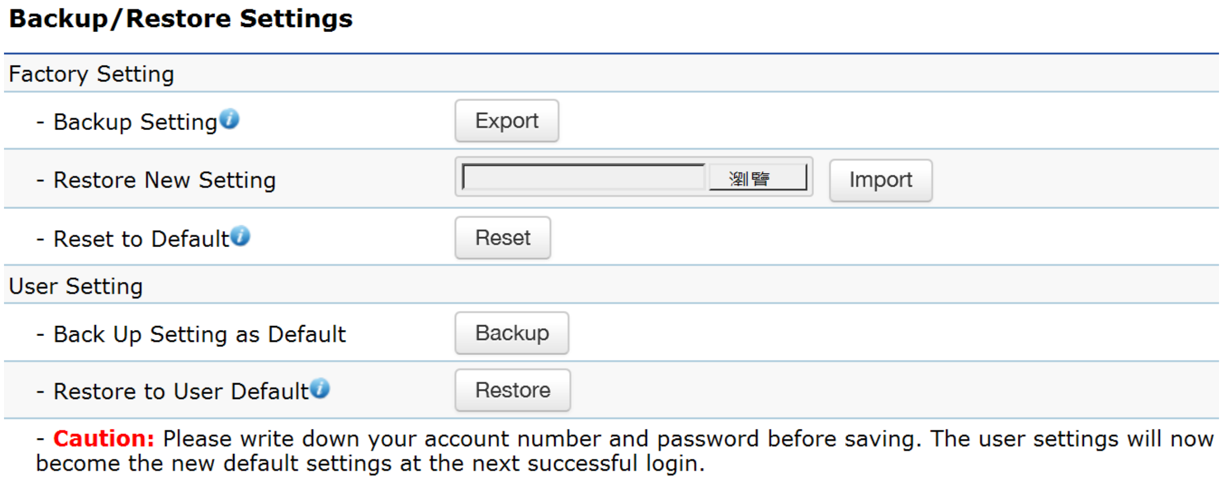
To Perform the Firmware Upgrade:

1. Click the **Browse…** button and navigate the OS File System to the location of the Firmware 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 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 the configurations, you can also reload the saved configurations into the device through the **Restore New Settings** from a file folder. If extreme problems occur, or if you have set the Access Point incorrectly, you can use the **Reset** button in the **Reset to Default** section to restore all the configurations of the Access Point to the original default settings. To configure the Backup/Restore Settings, click **Firmware** under the **Systems Manager** tab.



Backup/Restore Settings

Factory Setting	
- Backup Setting	Export
- Restore New Setting	瀏覽 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.

Factory Setting

Backup Setting: Click **Export** to save the current device configurations to a file.

Restore New Setting: Choose the file you wish to restore for settings and click **Import**.

Reset to Default: Click the **Reset** button to restore the Access Point to its factory default settings.

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 use as the default settings.

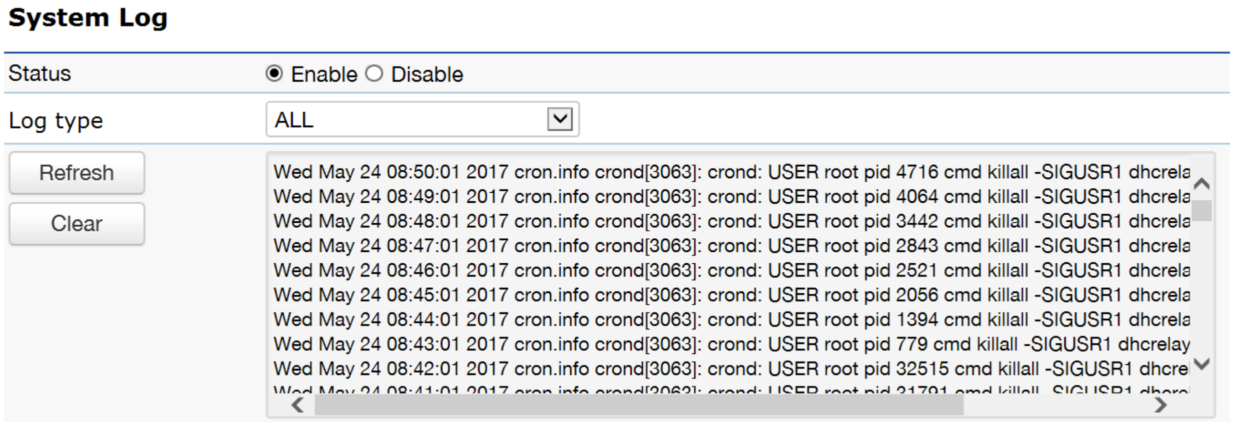
Restore to User Default: Click **Restore** to restore the Access Point to the user's default settings.

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.

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.



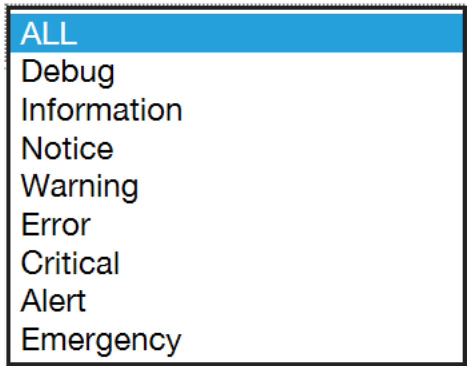
System Log

Status ● Enable ○ Disable

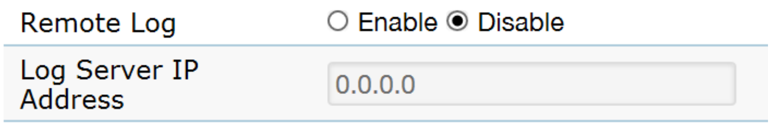
Log type ALL

```
Wed May 24 08:50:01 2017 cron.info crond[3063]: crond: USER root pid 4716 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:49:01 2017 cron.info crond[3063]: crond: USER root pid 4064 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:48:01 2017 cron.info crond[3063]: crond: USER root pid 3442 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:47:01 2017 cron.info crond[3063]: crond: USER root pid 2843 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:46:01 2017 cron.info crond[3063]: crond: USER root pid 2521 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:45:01 2017 cron.info crond[3063]: crond: USER root pid 2056 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:44:01 2017 cron.info crond[3063]: crond: USER root pid 1394 cmd killall -SIGUSR1 dhcrela
Wed May 24 08:43:01 2017 cron.info crond[3063]: crond: USER root pid 779 cmd killall -SIGUSR1 dhcrelay
Wed May 24 08:42:01 2017 cron.info crond[3063]: crond: USER root pid 32515 cmd killall -SIGUSR1 dhcre
Wed May 24 08:41:01 2017 cron.info crond[3063]: crond: USER root pid 31791 cmd killall -SIGUSR1 dhcre
```

Status: Enables or disables the System Log function.



Log Type: Select the Log Type mode you would like to use.



Remote Log	○ Enable ● Disable
Log Server IP Address	0.0.0.0

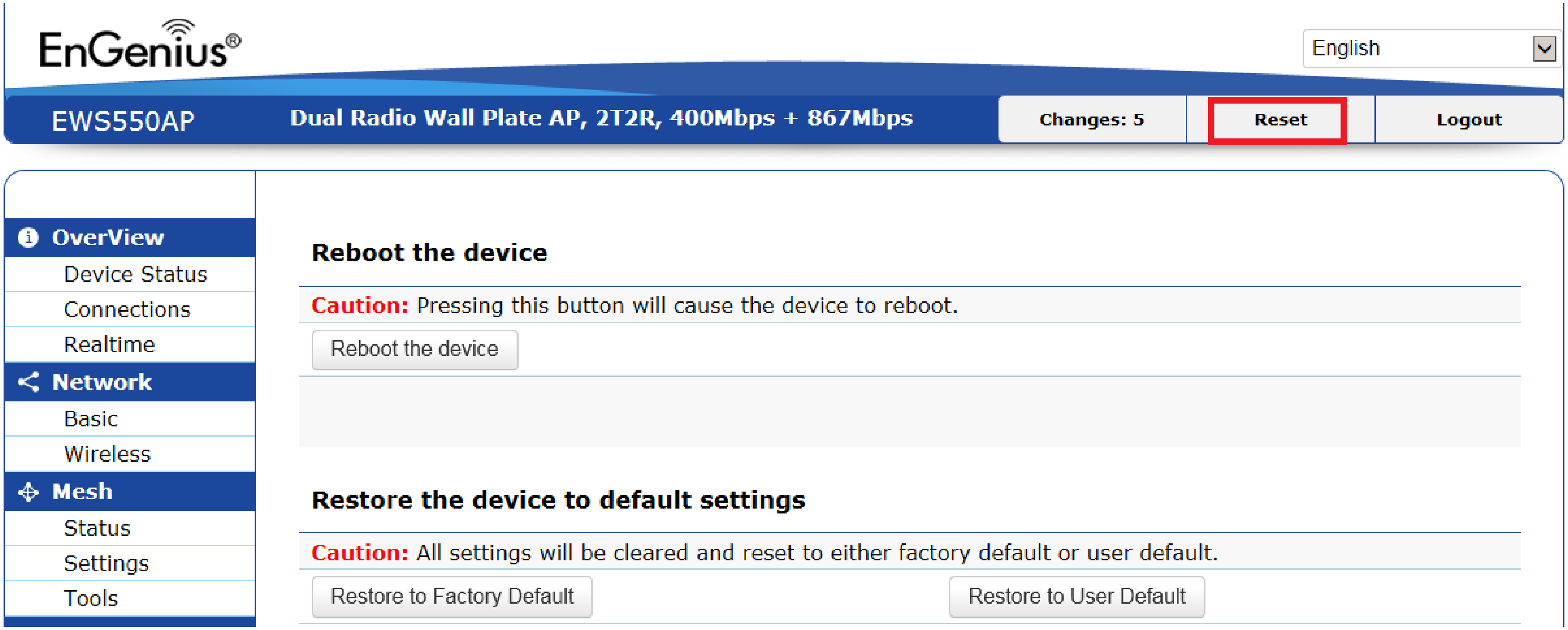
Remote Log: Enables or disables the Remote Log feature. If enabled, enter the IP address of the Log you would like to remote to.

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

Apply: Click **Apply** to save the changes

Reset

In some circumstances, you may be required to force the device to reboot. Click on **Reboot the Device**.



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.

Once you click the **Reset** button, you will see the options for rebooting or restoring this AP.

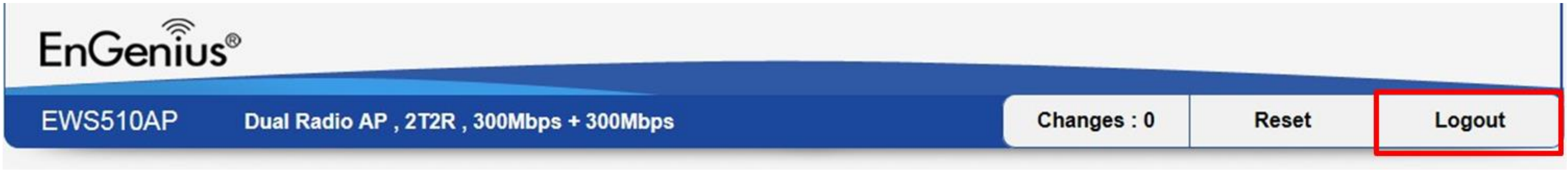
Reboot the device: Click to reboot this device.

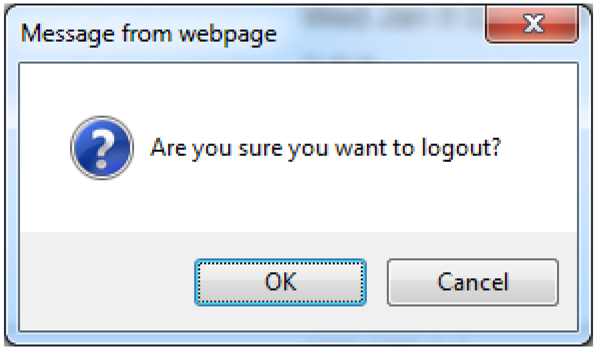
Restore to Factory Default: Click to reset this device to the factory default settings.

Restore to User Default: Click to reset this device to user default settings.

Logout

Click **Logout**, it will pop up a warning window. Click **OK** to logout.





Message from webpage

Are you sure you want to logout?

Appendix

Appendix A - FCC Interference Statement

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 - 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

CE0560(!)

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da 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.
de 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.
et 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.
en 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.
es 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.
el 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.
fr 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.
it 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.
nl 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.
mt 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.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[… típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt 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.
sl 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.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.