EnGenius

Turbo Engine Series

User Manual

EAP2200
version 1.0

Wireless Tri-Band Indoor Access Point

Chapter 1 ..... **4**
Key Features 5
Introduction 6
System Requirements 7
Package Contents 7
Applications 8
Technical Specifications 9
Physical Interface 11
Chapter 2 ..... **12**
Considerations for Wireless Installation 13
Computer Settings 14
Hardware Installation 18
Mounting the Access Point 19
Wall mount the Access Point 20
Chapter 3 ..... **21**
Default Settings 22
Web Configuration 23
Chapter 4 ..... **25**
Device Status 26
Connections 29
Chapter 5 ..... **30**
IPv4 Settings 31
IPv6 Settings 32
Spanning Tree Settings 33
LAN Port Settings 34
Chapter 6 ..... **35**
2.4GHz/5GHz SSID Profile 36

Wireless Security 38
Wireless MAC Filter 41
Traffic Shaping 42
Guest Network 43
RSSI Threshold 45
Management VLAN Settings 46
Chapter 7 47
SNMP Settings 48
CLI/SSH Settings 50
HTTPS Settings 51
Email Alert 52
Date and Time Settings 53
WiFi Scheduler 54
Tools 56
LED Control 59
Device Discovery 60
Chapter 8 61
Account Setting 62
Firmware Upgrade 63
Backup/Restore 64
System Log 64
Reset 66
Logout 67
Appendix 68
Appendix A - FCC Interference Statement 69
Appendix B - IC Interference Statement 71
Appendix C - CE Interference Statement 73

Chapter 1
Product Overview

Introduction

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.
- Proprietary 24V 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

The AP is a great performance, evenly coverage and long-range Dual-Band Wireless 802.11 ac/a/b/g/n Indoor Access Point with speeds up to 300 Mbps on 2.4GHz and 867Mbps on 5GHz band. It can be configure as an: Access Point, Client Bridge, or WDS (AP, Station & Bridge). Its high-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that don't have the range and reach to connect to a growing number of wireless users who wish to connect to a business network. The AP supports the 2.4GHz frequency band under 802.11 b/g/n modes while at the same time providing 5GHz band under 802.11 ac/a/n modes for communicating to and from 5GHz capable computers, tablets or smart phones or transferring files. Several APs can be deployed in a campus setting using the 5GHz band as a backhaul to provide multiple 2.4GHz wireless cells for computers or mobile devices in common indoor areas.

The AP is easy to install in virtually any location with PoE (Power over Ethernet). The AP enables network administrators to control its transmit power and feature settings for selecting narrow bandwidth and traffic shaping. The AP also supports wireless encryption including Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) Encryption, and IEEE 802.1x with RADIUS.

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. For United States of America: Copyright © 2017 EnGenius Technologies, Inc. All rights reserved.

System Requirements

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

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

Package Contents

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

- EAP Wall Plate Access Point
- Mounting Bracket
- Bracket Screw
- Quick Installation Guide
- Power Adaptor

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

EAP2200

Radio Specification

Dual Concurrent Radio:

- 2.4GHz: 802.11b/g/n with max data rate up to 300Mbps
- 5GHz: 802.11ac/n with max data rate up to 867Mbps

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:

- 802.11n 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

Environment:

- Operating temperature: 0°C~40°C
- Operating humidity: 0%~90% typical
- Storage temperature: -20°C~60°C

Wireless

Operating Mode:

- 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)

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

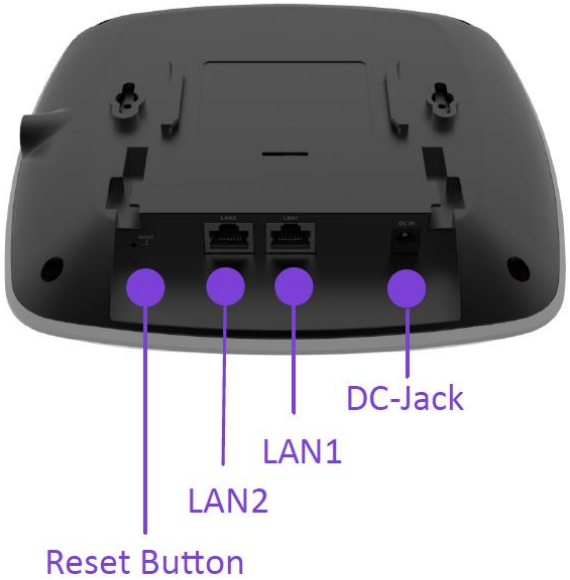
- Revert to factory default settings

Schedule Reboot:

- Specifies interval to reboot system periodically

E-mail Alert / Syslog Notification

Physical Interface



1. LED Indicators: LEDs for Power, WAN, 2.4Hz, 5GHz, LAN
2. Reset Button: Press and hold for over 10 seconds to reset to factory default settings.
3. DC12V Input: DC12V/1A power in
4. LAN1 : 10/100/1000 RJ45 Uplink (PoE In)that supports 802.3af/at PoE input
5. LAN2 :10/100/1000 RJ45

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 Access Point's 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 significant 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.

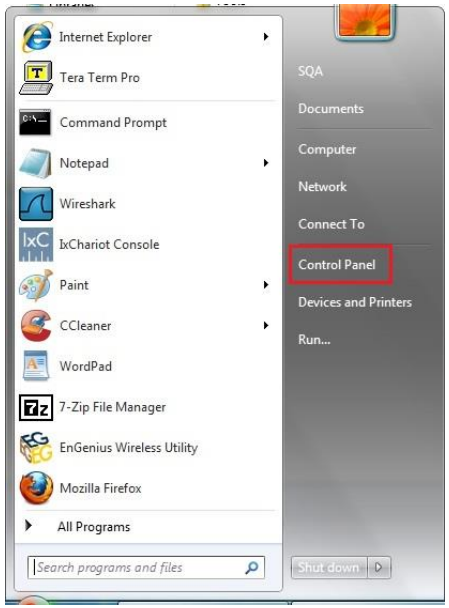
Computer Settings

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

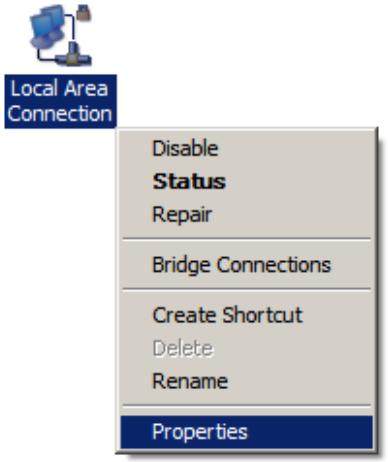


Windows 7

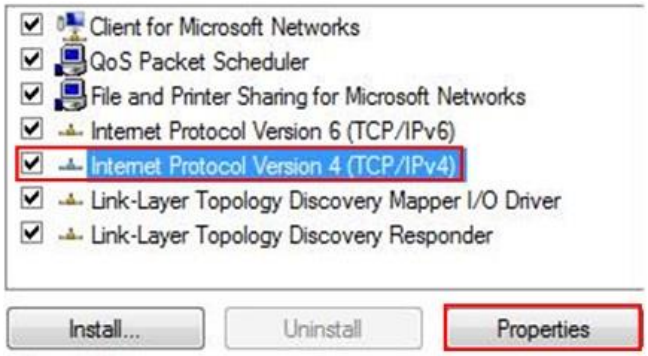
2a. In **Windows XP**, click on Network Connections.

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

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



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



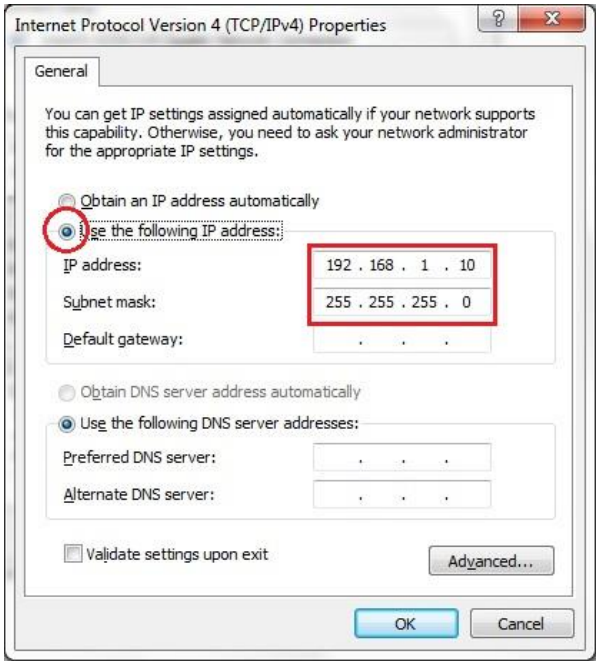
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

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

For example: 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



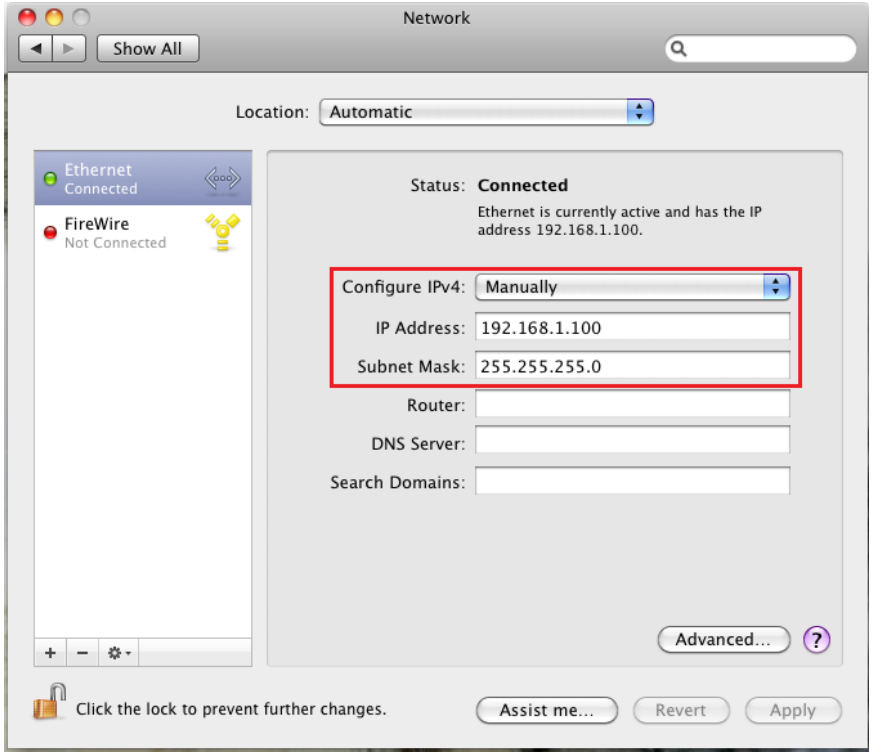
Apple Mac OS X

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.



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.**

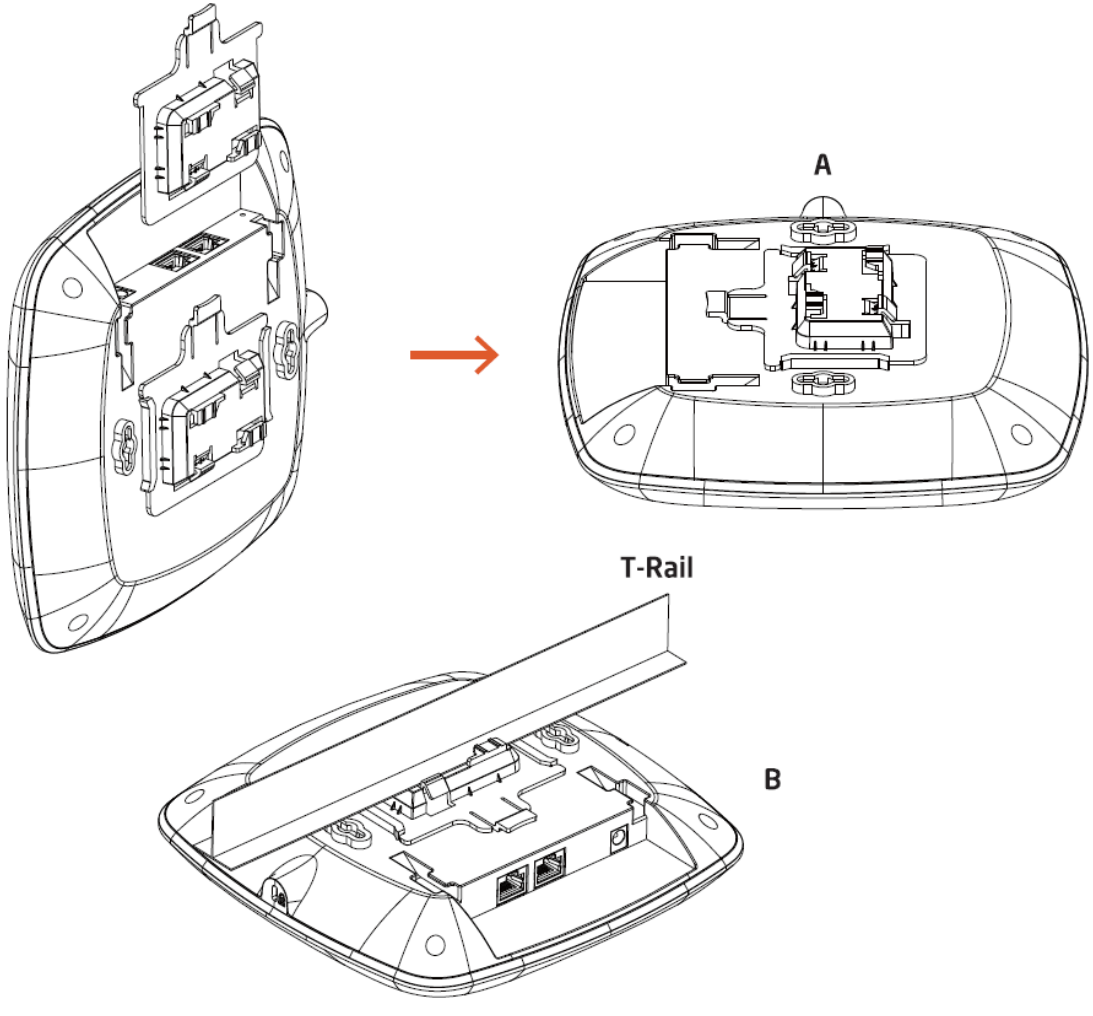
Mounting the Access Point

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

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

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

B) Hold the Access Point with one hand ti reach the other hand over the T-Rail sides of the bracket. Then hook the stationary end of the ceiling mount bracket onto the T-Rail.



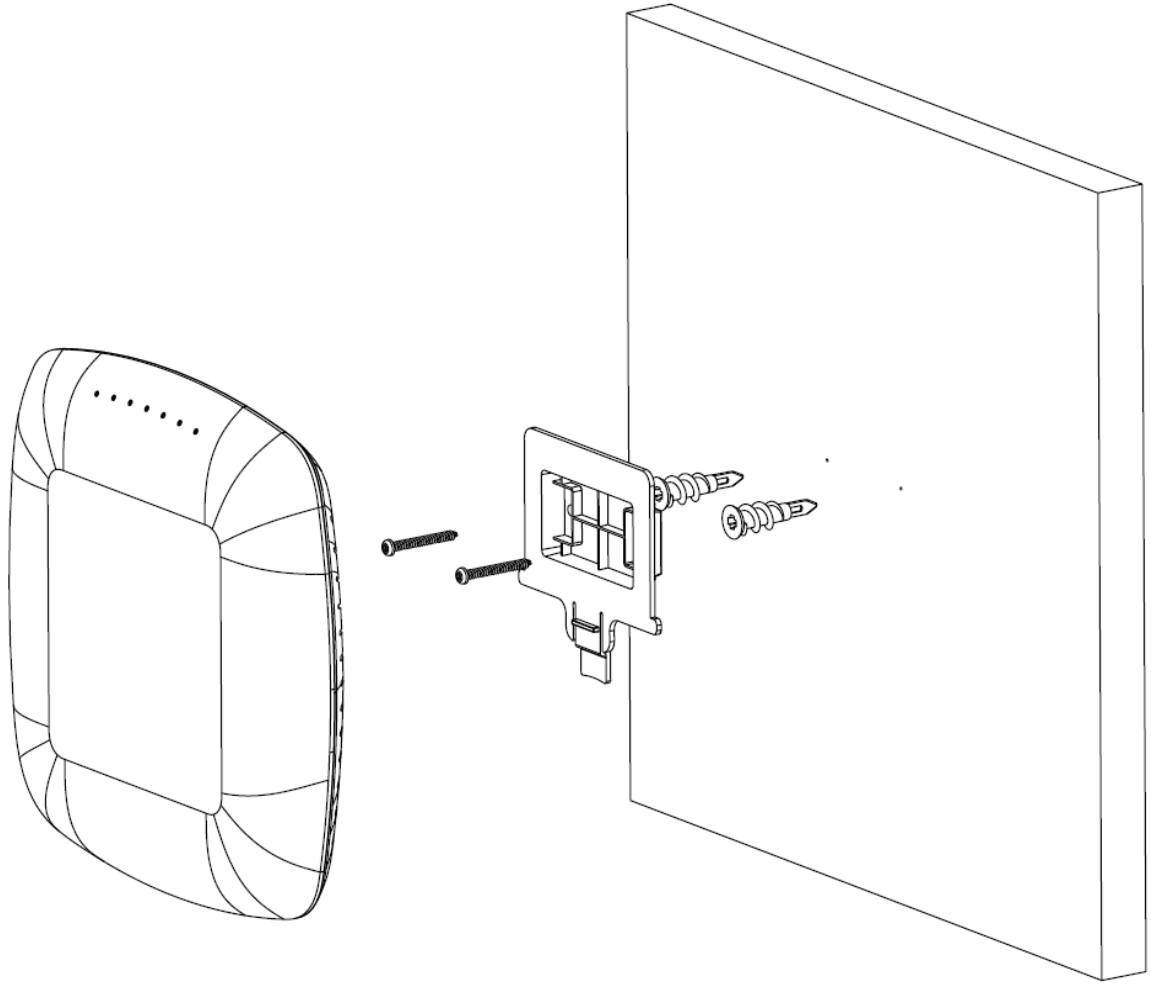
Wall mount the Access Point

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.

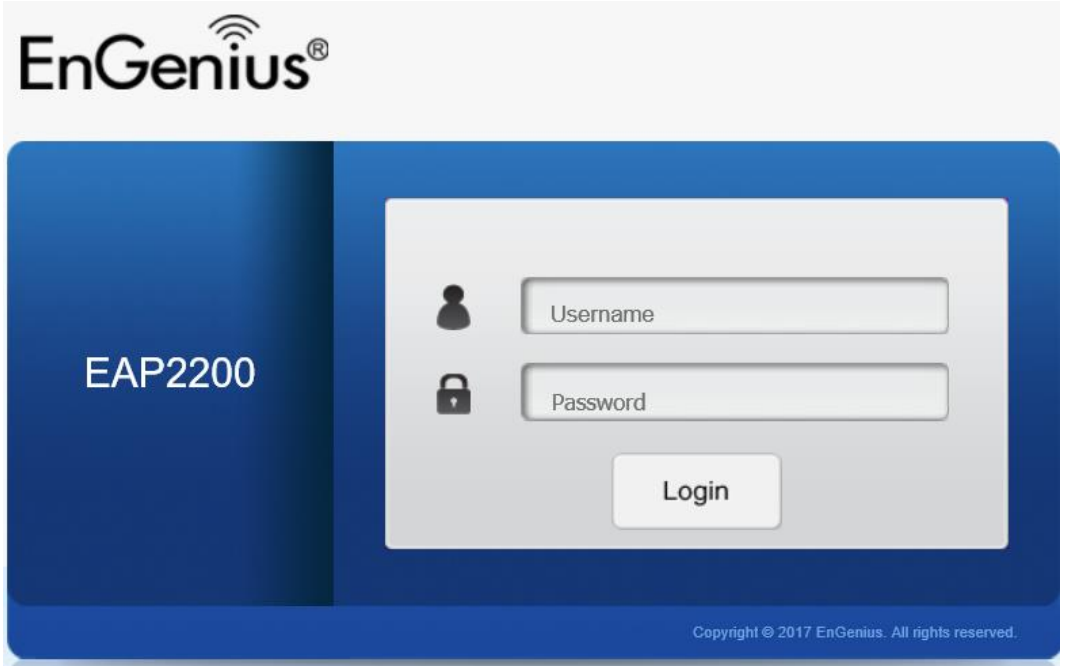
IP Address	192.168.1.1
Username/Password	admin/admin

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.



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

EnGenius

English

EAP2200 | Tri-band Indoor AP, 300Mbps + 867Mbps + 867Mbps | Changes: 0 | Reset | Logout

- **OverView**
  - Device Status
  - Connections
  - Realtime
- **Network**
  - Basic
  - Wireless
  - DDNS
- **Management**
  - Advanced
  - Time Zone
  - WiFi Scheduler
  - Tools
- **System Manager**
  - Account
  - Firmware
  - Log

Device Information

Device Name	EAP2200
Serial Number	000000001
MAC Address	
- LAN	00:00:00:E3:0C:54
- Wireless LAN - 2.4GHz	00:AA:BB:CC:DD:11
- Wireless LAN - 5GHz - 1	00:AA:BB:CC:DD:12
- Wireless LAN - 5GHz - 2	
Country	Netherlands
Current Local Time	Mon Jul 31 05:32:51 2017
Uptime	1h 33m 42s
Firmware Version	1.0.0 + 1.8.57
Management VLAN ID	Untagged
Registration Check Code	6d899865

Memory Information

Total Available	160212 kB / 236440 kB (67%)
Free	130680 kB / 236440 kB (55%)
Cached	21036 kB / 236440 kB (8%)
Buffered	8496 kB / 236440 kB (3%)

Chapter 4
Overview

Overview

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

- Device Status
- Connections

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	EAP2200
Serial Number	000000001
MAC Address	
- LAN	00:00:00:E3:0C:54
- Wireless LAN - 2.4GHz	00:AA:BB:CC:DD:11
- Wireless LAN - 5GHz - 1	00:AA:BB:CC:DD:12
- Wireless LAN - 5GHz - 2	
Country	Netherlands
Current Local Time	Mon Jul 31 05:32:51 2017
Uptime	1h 33m 42s
Firmware Version	1.0.0 + 1.8.57
Management VLAN ID	Untagged
Registration Check Code	6d899865

- The **LAN Information** section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, Gateway, DNS Address, DHCP Client, and 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/5GHz** 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 - 5GHz only available for 5GHz 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

Connections

Clicking the **Connections** link under the **Device Status** menu displays the list of clients associated to the Access Point's 2.4GHz/5GHz, 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

Refresh

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

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 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 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	☑	☐	1
LAN2	☑	☐	1
LAN3	☑	☐	1
LAN4	☑	☐	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

2.4GHz & 5GHz Wireless

Basic

2.4GHz/5GHz 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

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.

*5GHz settings only available for dual radio models.

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.

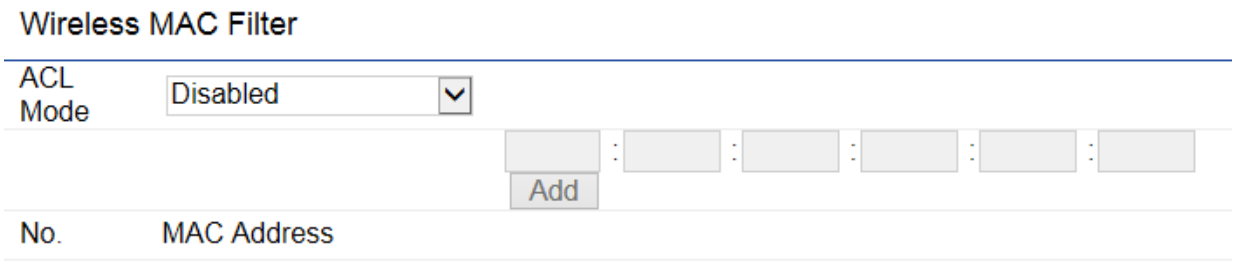
Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

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 (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.

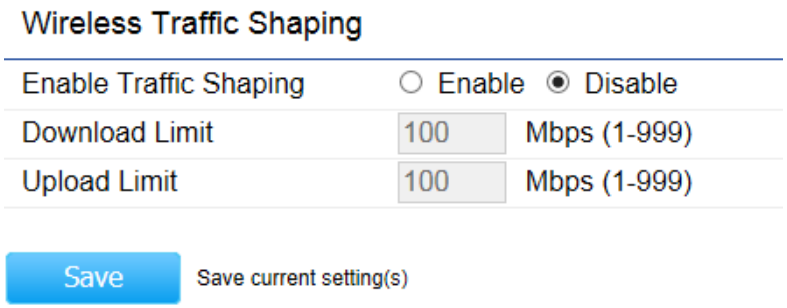
MAC Address: Enter the MAC address of the wireless client.

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.



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.

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

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.

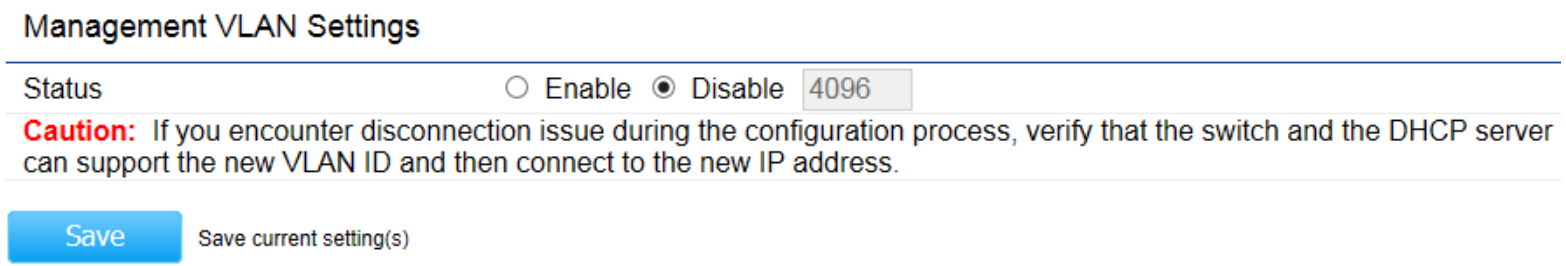
RSSI Threshold

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

CAUTION: Enabling RSSI Threshold disassociates wireless clients that fall below the configured RSSI threshold and may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.

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 VLAN do not have to be physically located next to one another on the LAN.



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

Management

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) returns 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.

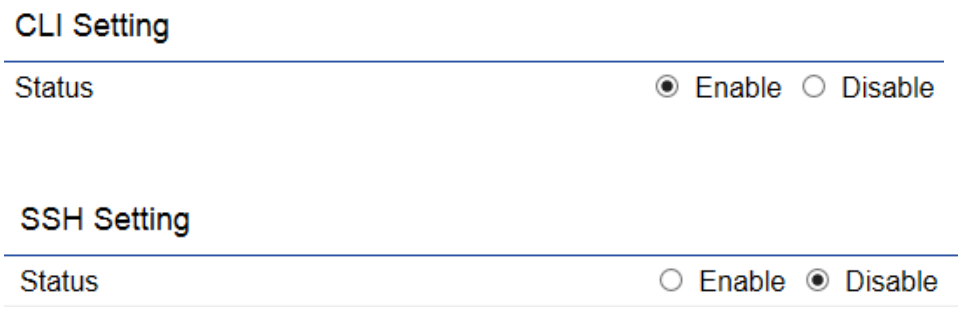
Priv Protocol: Select the Privacy Protocol type: DES.

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 access through a command console, modem or Telnet connection. For security's concern, you can enable SSH (Secure Shell) to establish a secure data communication.



CLI Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a command line interface (CLI).

SSH Status: Select **Enable** or **Disable** to enable or disable the ability 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

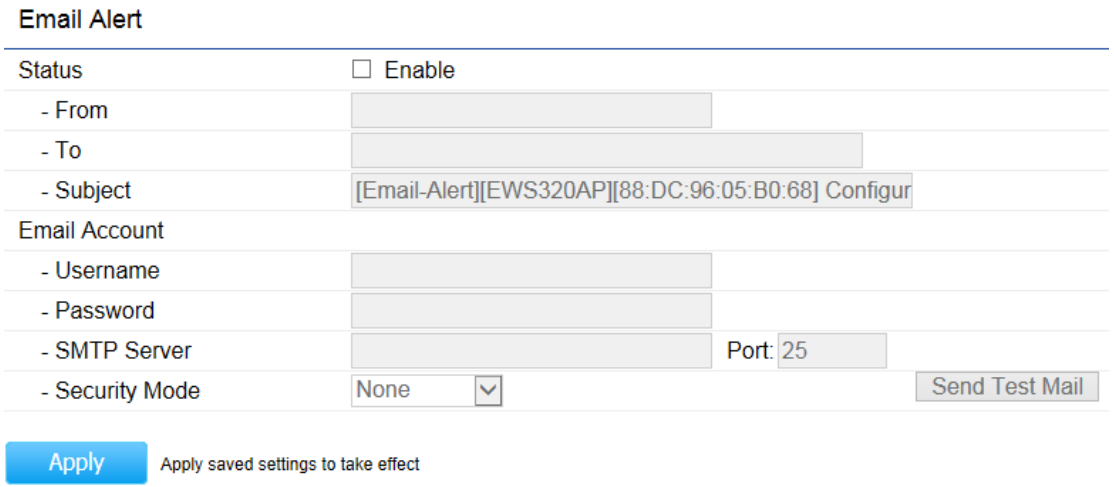
Status	◉ Enable ○ Disable
HTTPS forward	○ Enable ◉ Disable

Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a HTTPS.

HTTPS forward: Enable this option; it will be forwarded to HTTPS if user uses HTTP to access the Access Point.

Email Alert

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



Status: Check **Enable** to enable Email Alert feature.

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

To: Enter the address to show as the receiver of the email.

Subject: Enter the subject to show as the subject of the email.

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.

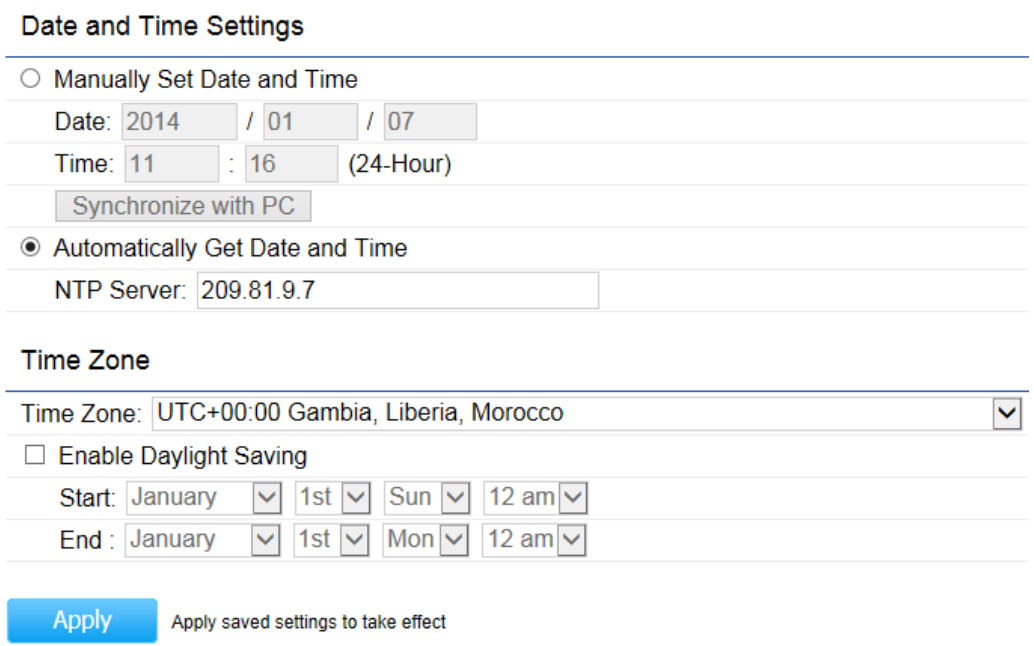
Security Mode: Select the mode of security for the Email alert. The options are None, SSL/TLS and STARTTLS.

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.



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 an 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.

WiFi 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 a network time protocol (NTP) server. For details on how to connect the Access Point to an NTP server, see Date and Time Settings.

Auto Reboot Settings

You can 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.

WiFi 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

Save Save current setting(s)

Status: Enables or disables the WiFi Scheduler function.

Wireless Radio: Select 2.4GHz or 5GHz* to use WiFi Schedule.

SSID Selection: Select a SSID to use WiFi Schedule.

Schedule Templates: There are 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.

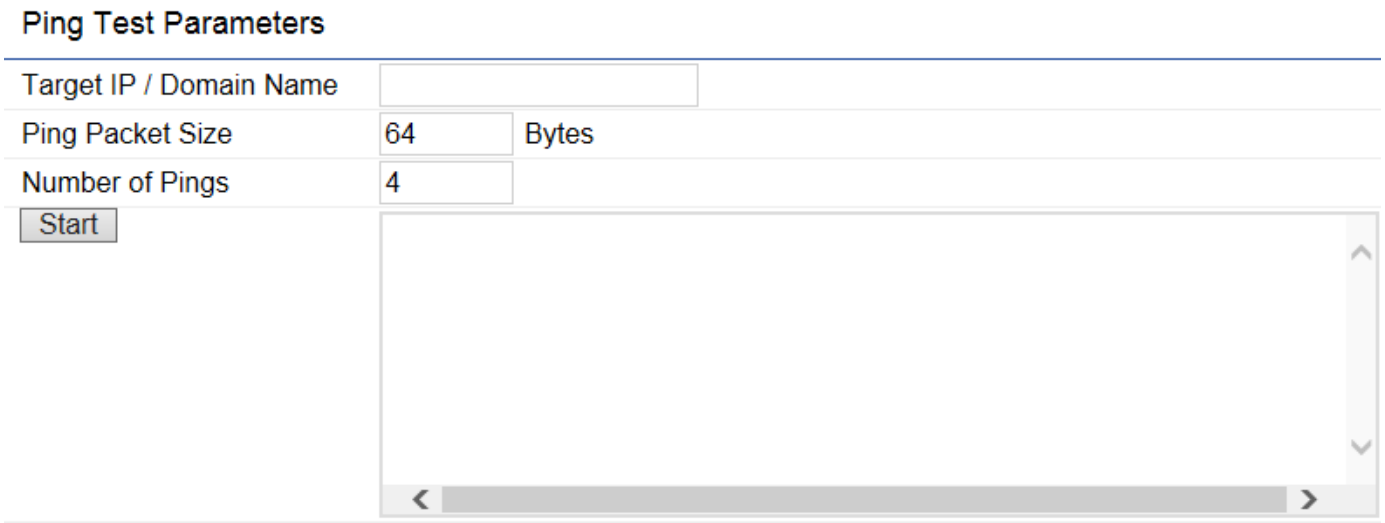
Schedule Table: Set the schedule manually.

*5GHz radio settings only available for dual radio models.

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



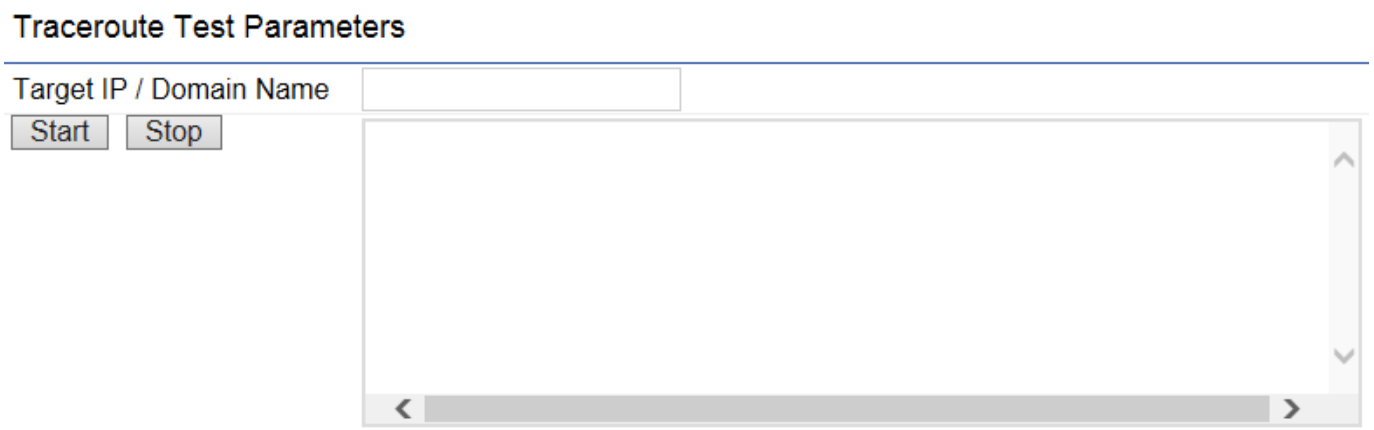
Target IP/Domain Name: Enter the IP address or Domain name you would like to search.

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 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 trace route operation.

Stop: Halts the traceroute test.

Speed Test Parameters

Speed Test Parameters

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

Target IP/Domain Name: Enter an IP address or domain name you wish to run a Speed Test for.

Time Period: Enter the time in seconds that you would like the test to run for 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 2.4GHz/5GHz WLAN interface.

LED Control

Power	◉ Enable	○ Disable
LAN	◉ Enable	○ Disable
WLAN-2.4GHz	◉ Enable	○ Disable
WLAN-5GHz	◉ Enable	○ Disable

Apply Apply saved settings to take effect

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

*5GHz settings only available for dual radio models.

Device Discovery

Under Device Discovery, you can choose for 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

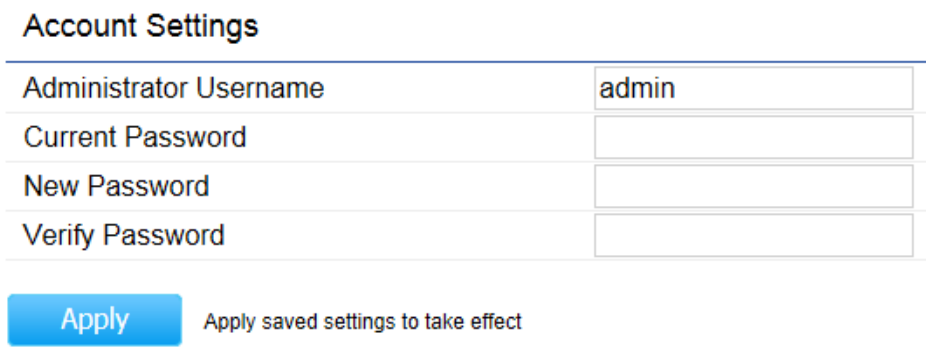
Scan

Chapter 8

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.

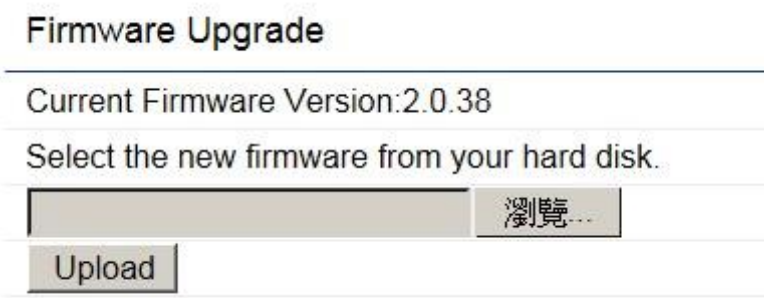


Administrator Username: Enter a new username for logging in to the Administrator Username entry box.
Current Password: Enter the old password for logging in to the Current Password entry box.
New Password: Enter the new password for logging in to the New Password entry box.
Verify Password: Re-enter 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.



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.

Factory Setting

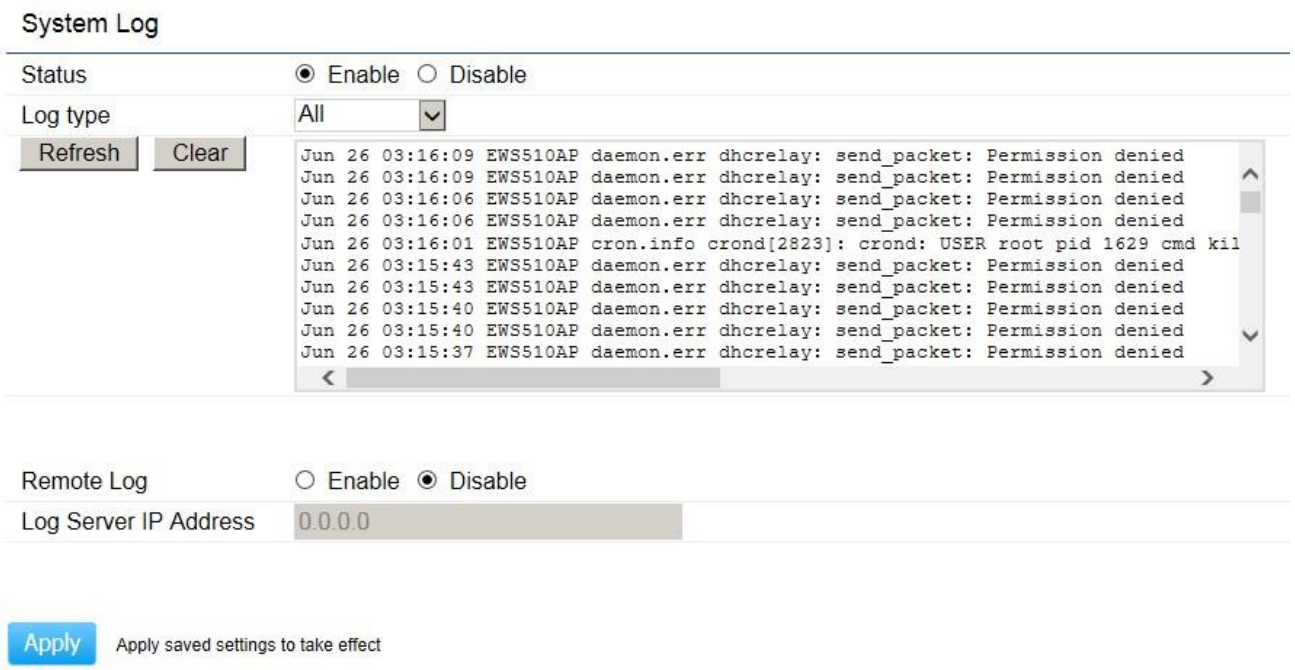
Backup Setting: Click **Export** to save the current device configurations to a file.
Restore New Setting: Choose the file you wish restore for settings and click **Import**.
Reset to Default: Click the **Reset** button to restore the Access Point to its factory default settings.

User Setting

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 user's default settings.

System Log

This page allows you to setup the System Log and local log functions of the Access Point. Click **Log** under the **Systems Manager** tab to open up the System Log page.



Status: Enables or disables the System Log function.

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

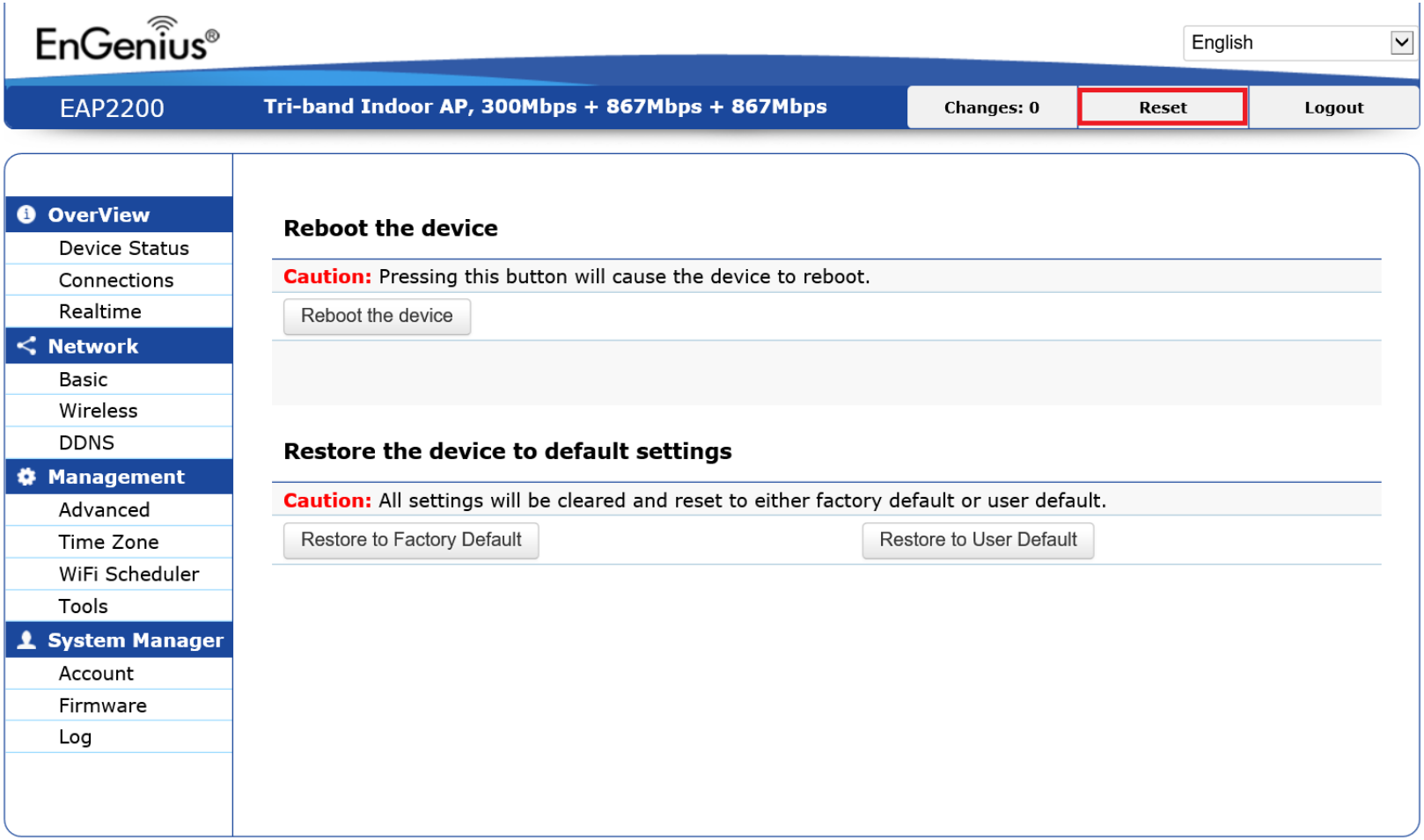
Remote Log: Enables or disables the Remote Log feature. If enabled, enter the IP address of the Log you would like to remote to.

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

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

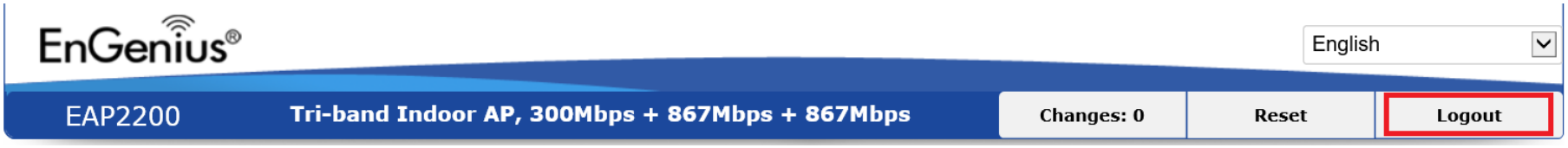
Reset

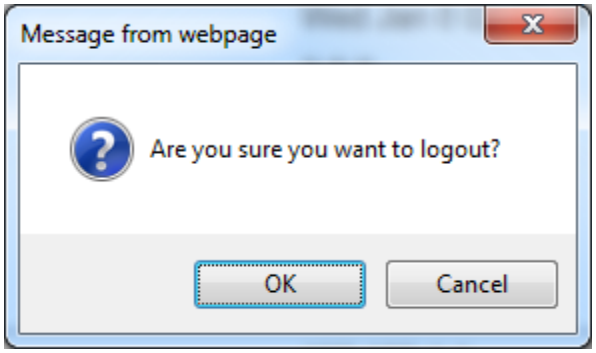
In some circumstances, you may be required to force the device to reboot. Click on **Reboot the Device** to reboot the device.



Logout

Click **Logout**, it will pop up a warning window. Click **OK** 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 - IC Interference Statement

Industry Canada Statement

This device complies with RSS-210 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-210 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.

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.

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 minimum distance 20cm between the radiator & your body.

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 !

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.
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.
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.
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.