EnGenius®

The Neutron Series

User Manual

EWS210AP | EWS310AP | EWS320AP | EWS360AP

version 1.0

Dual Band

Wireless Managed Indoor Access Point

IMPORTANT

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

Table of Contents

Chapter 1
Product Overview

Introduction

The EnGenius Neutron series suite of Managed Indoor Access Points are enhanced -powered, long-range, Single or Dual Band concurrent Wireless 802.11a/b/g/n or 802.11a/b/g/n/ac Access Points. They are 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. Their extra power and long-range characteristics make them a cost effective alternative to ordinary Access Points that don't have the range or reach to confect to a growing number of wireless users who wish to connect to a large hotspot or business network.

The Neutron Series marks a new performance breakthrough for Indoor Wireless Managed Access Points. Wireless users with 802.11b/g/n or 802.111b/g/n/ac* laptops, tablets and other devices, who need to stream HD video or transfer files will find this powerful Access Point at an affordable price point and more than up to those tasks.

The EWS210AP is an 802.11b/g/n Wireless Managed 802.1n 2x2 high-powered, long-range, single radio Indoor Access Point with speeds up to 300 Mbps on the 2.4 GHz band that functions as part of an EnGenius Neutron Series Wireless Management Solution or as a stand-alone AP.

can be used with
802.3at
capable switches or injectors

The EWS310AP and EWS320AP delivers up to 6x faster wireless speeds compared to legacy 802.11a/b/g wireless devices. Even though the EWS310AP and EWS320AP have been designed and engineered for heavy traffic and demanding business environments, in larger housing environments as it can efficiently extend the wireless range of an existing home router. This makes it especially ideal in architecturally-challenging structures, providing whole home connectivity.

For more robust needs, the EWS360AP offers up to 450 Mbps on 2.4 GHz band and 1300 Mbps on the 5 GHz frequency band for faster file transfers and smoother video streaming, enabling it to deliver AC speeds and performance. Its high transmit power on each band provides more than twice the wireless coverage over mainstream competitors and enables the wireless signal for faster connectivity to client devices and enables the wireless signal to penetrate floors, ceilings, and walls. Its Internal 3D sectorized MIMO antenna array design provides better reception and performance as clients change their orientation.

All Neutron Series Access Points can operate as stand-alone Access Points connecting to third-party PoE-capable Switches but more control and versatile management of an Access Point is achievable when it is part of an EnGenius Neutron Series wireless network management solution because the AP includes firmware that enables it to be immediately discovered, configured, monitored and managed from a compatible Neutron Series PoE+ Layer 2 Switch (**EWS5912FP**, **EWS7928P**, **EWS7928FP** or **EWS7952FP**). This capability enables IT managers to deploy and manage up to 50 Neutron Series Access Points, allowing for simplified management from one browser-based interface including simultaneous firmware upgrades, monitoring, bandwidth steering and many other features that can be reset or reconfigured from the convenience of the IT manager's desktop.

*Some features availble only on certain models. Please refer to the comparison chart to determine your Access Point's capabilities and features. All Neutron Series Access Points must be connected to a Neutron Series compatible Switch to provide full management features.

Key Features

- Access Point Mode / Mesh AP Mode*

  (with Controller Interface)
- Sectorized 3D Antenna (select models)
- Dynamic Channel Optimization
- Guest Network
- Band Steering
- Fast Roaming, Fast Handover
- Supports connectivity of up to 100+ users**
- Encryption: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise
- 16 SSIDs (8 SSIDS per frequency band)****
- Wireless Traffic Shaping
- 802.1q VLAN
- QoS
- IPv6
- Spanning Tree Protocol (STP)
- SSID-to-VLAN Mapping
- SNMP
- CLI/SSH/https
- VLAN Isolation
- Client Isolation
- Ping Test/Traceroute Test/Speed Test
- Email Alerts***

*Available soon as a firmware upgrade.

**User capacity performance results may vary based on topology configuration, structural and architectural elements, environmental factors, type of data traffic, RF capabilities of client devices, distance, RF interference in the operating environment and other factors.

***In stand-alone mode only

****Not applicable to EWS210AP model. The EWS210AP supports 8 SSIDS, 4 per frequency band.

Package Contents

can be used with **802.3at** capable switches or injectors

Your EnGenius EWS Access Point package will contain the following items:*

- EnGenius Neutron Series Access Point (**EWS210AP**, **EWS310AP**, **EWS320AP**, or **EWS360AP**)
- Power Cord
- RJ-45 Ethernet Cable
- T-Rail Mounting Kit
- Ceiling and Wall Mount Screw Kit
- Quick Installation Guide
- Powr Adapter (12V/2A)

*(all items must be in package to issue a refund):

Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on distance between devices or traffic and bandwidth load in the network. Features and specifications subject to change without notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright ©2014 EnGenius Technologies, Inc. All rights reserved. Compliant with FCC - This equipment has been tested and found to comply with the limits for a Class A 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. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

System Requirements

The following are the Minimum System Requirements in order configure the Access Point:

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7), Mac OS X, or Linux-based operating systems
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or other similar browser application)

Technical Specifications

Quick Reference Guide

Model	EWS210AP	EWS310AP	EWS320AP	EWS360AP
RF	RF: 2.4 GHz Frequency Band	RF: 2.4 and 5 GHz Frequency Band	RF: 2.4 and 5 GHz Frequency Band	RF: 2.4 and 5 GHz Frequency Band
Standard	IEEE 802.11b/g/n	IEEE 802.11a/b/g/n	IEEE 802.11a/b/g/n	IEEE 802.11a/b/g/n/ac
Data Rate	Up to 300 Mbps on 2.4 GHz	Up to 300 Mbps on 2.4 GHz Up to 300 Mbps on 5 GHz	Up to 450 Mbps on 2.4 GHz Up to 450 Mbps on 5 GHz	Up to 450 Mbps on 2.4 GHz Up to 1300 Mbps on 5 GHz
Transmit Power	Up to 29 dBm on 2.4 GHz	Up to 29 dBm on 2.4 GHz Up to 26 dBm on 5 GHz	Up to 28 dBm on 2.4 GHz Up to 28 dBm on 5 GHz	Up to 28 dBm on 2.4 GHz Up to 26 dBm on 5 GHz
Memory	128MB	64MB	64MB	128MB
Flash Memory	16MB	16MB	16MB	16MB
Radio Chains/ Spatial Streams	2x2:2	2x2:3	3x3:3	3x3:3
Antenna Array	2 x 5 dBi Integrated 2.4 GHz antennas	2 x 5 dBi Integrated 2.4 GHz antennas 2 x 5 dBi Integrated 5 GHz antennas	3 x 5 dBi Integrated 2.4 GHz antennas 3 x 5 dBi Integrated 5 GHz antennas	3 x 3 dBi Integrated 2.4 GHz antennas 3 x 5 dBi Integrated 5 GHz antennas
Operation Mode	AP/Mesh AP			
Peak Power Consumption	up to 9W	up to 15.6W	up to 22W	up to 22W
Multiple BSSID	8 SSIDs	16 SSIDs	16 SSIDs	16 SSIDs
LAN	IP (check validity and DHCP server IP range) MAC			
SSID-toVLAN Tagging	Supports 802.1q SSID-to-VLAN tagging			
Spanning Tree Protocol	Supports 802.1d Spanning Tree Protocol			

WARNING!

This switch should be connected only to PoE networks without routing to the outside plant.

Wireless Management Features

Web-based support
Access Point Auto Discovery and Provisioning
Access Point Auto IP Assignment
Access Point Cluster Management
Remote Access Point Rebooting
Access Point Device Name Editing
Access Point Radio Settings
Band Steering
Traffic Shaping
Fast Handover
Seamless Roaming (requires RADIUS server)
Access Point Client Limiting
Mesh Network*
Wireless Security (WEP, WPA/WPA2 Enterprise, WPA/WPA2 PSK)
VLANs for Access Point- Multiple SSIDs
Guest Network
Access Point Status Monitoring
Wireless Client Monitoring
Wireless Traffic & Usage Statistics
Visual Topology View
Floor Plan View
Map View
Secure Control Messaging
SSL Certificate
Local MAC Address Database
Remote MAC Address Database (RADIUS)
Unified Configuration Import/Export
Bulk Firmware Upgrade Capability
Intelligent Diagnostics

Tx Power Control:
Adjust transmit power by dBm

Configuration:
Web-based configuration (http)

Firmware Upgrade:
Via web browser, settings are reserved after upgrade

Administrator Settings:
Administrator Username and Password Change

Reset Settings:
Reboot (press and hold for 2 seconds).
Reset to factory default (press and hold for 10 seconds)

System Monitoring:
Status Statistic and Event Log

SNMP:
V1, V2c, V3

MIB:
MIB I, MIB II (RFC1213) and private MIB

Traffic Shaping:
Incoming and outgoing wireless traffic shaping

LED Control:
On/Off

AP Detection:
Scanning for available EnGenius APs

Auto-channel Selection:
Automatically selecting least congested channel

Bandwidth Measurement:
IP range and bandwidth management

Auto Reboot:
Reboot Access Point by minute, hour, day, or week

Backup and Restore:
Save and restore settings through Web interface

CLI:
Supports Command Line Interface

Diagnosis:
IP pinging statistics

Log:
SysLog and Local Log support

Wireless Security

WPA/WPA2 Personal (WPA-PSK using TKIP or AES)
WPA/WPA2 Enterprise (WPA-EAP using TKIP)
802.1X RADIUS Authenticator: MD5/TLS/TTLS, PEAP
SSID broadcast enable/disable
MAC Address Filtering, Up to 50 field
L2 Isolation (Access Point mode)

QoS (Quality of Service)

WMM (Wireless Multimedia)

Environment & Mechanical:

Temperature Range

Operating: 32°F to 122°F/0°C to 50°C

Storage temperature: 4°F to 140°F/-20°C to 60°C

Humidity (non-condensing)

Operating: 90% or less

Storage: 90% or less

Humidity (non-condensing)

Operating: 90% or less

Storage: 90% or less

Certifications

FCC, IC

Package Contents

Neutron Series Indoor Access Point
12V/2A Power Adapter
T-Rail Mounting Kit
Ceiling Mount and Wall Screw Kit
Mounting Bracket
RJ-45 Ethernet Cable
Quick Installation Guide

Warranty

1 Year

* Mesh networking mode available soon as a free firmware upgrade

Physical Interface

Dimensions & Weights

EWS210AP

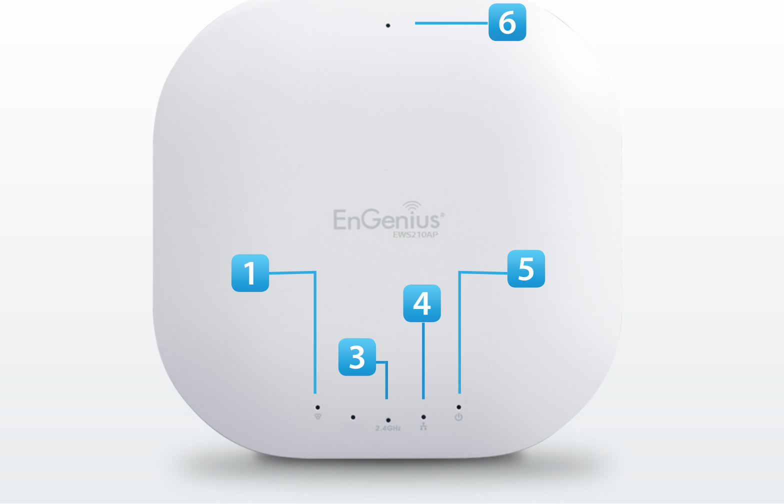
Width: 6.36” Length: 6.36” Height: 1.64” Weight: 0.8 lbs.

Dimensions & Weights

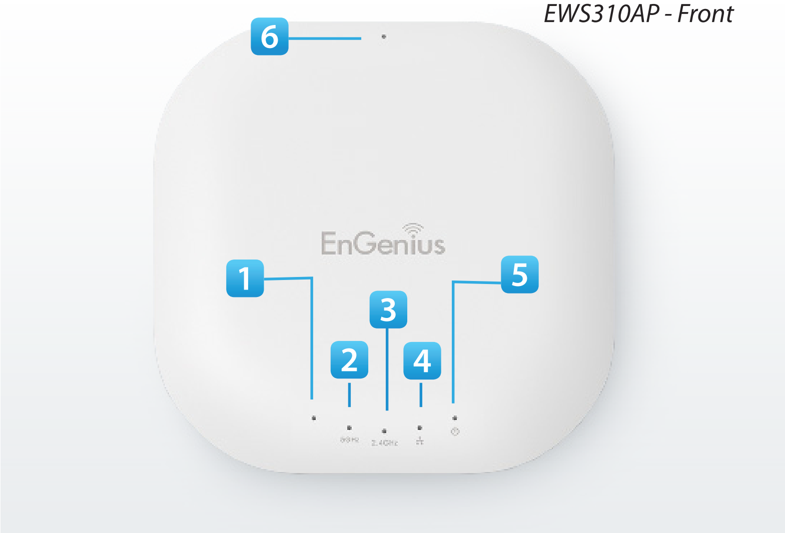
EWS310AP

Width: 6.36” Length: 6.36” Height: 1.64” Weight: 0.8 lbs.

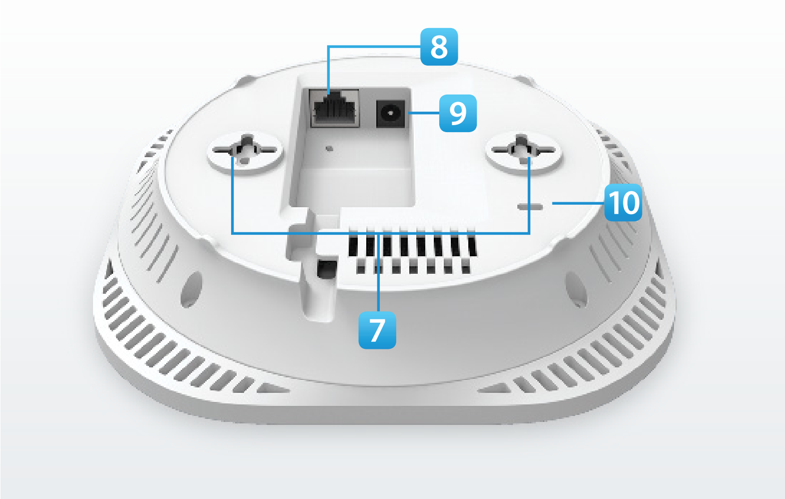
EWS210AP - Front



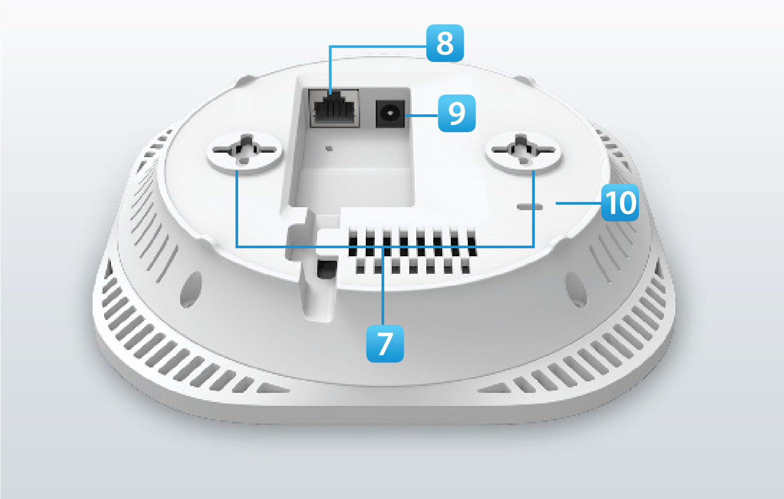
EWS310AP - Front



EWS210AP- Back



EWS310AP - Back

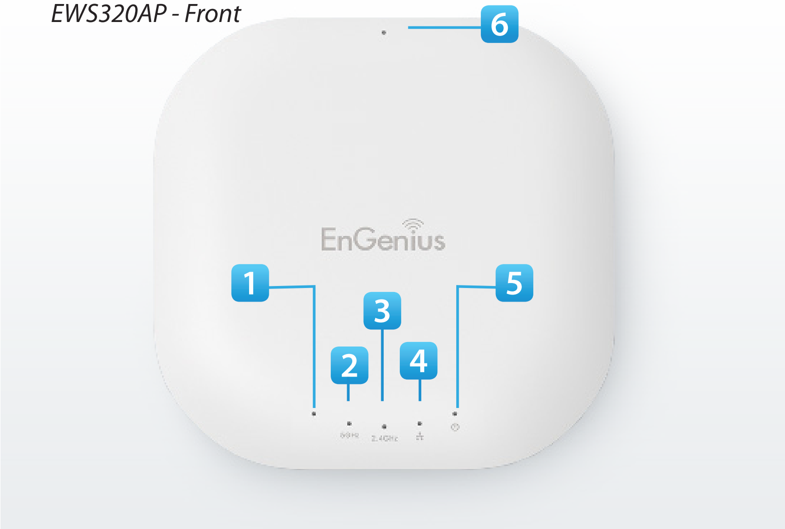


Dimensions & Weights

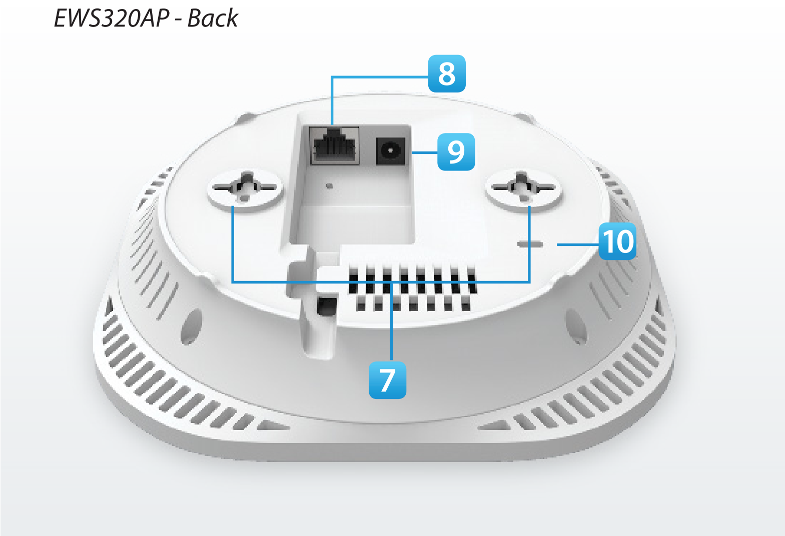
EWS320AP

Width: 6.36” Length: 6.36” Height: 1.64” Weight: 0.8 lbs.

EWS320AP - Front



EWS320AP - Back

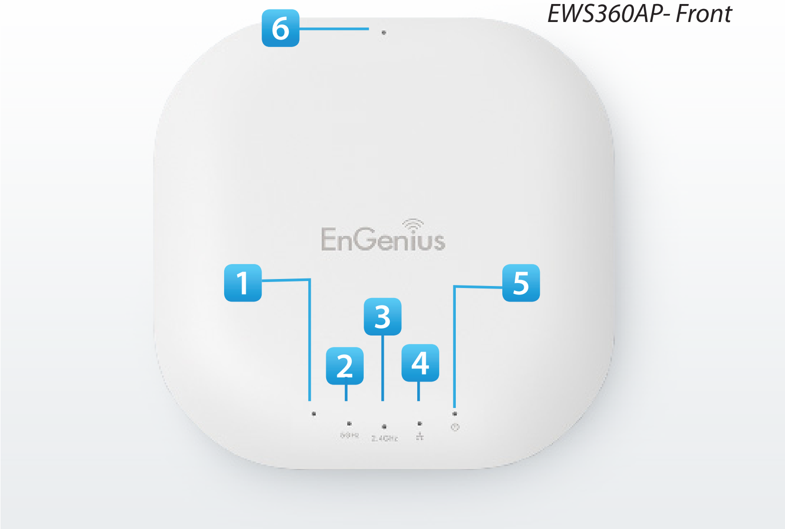


Dimensions & Weights

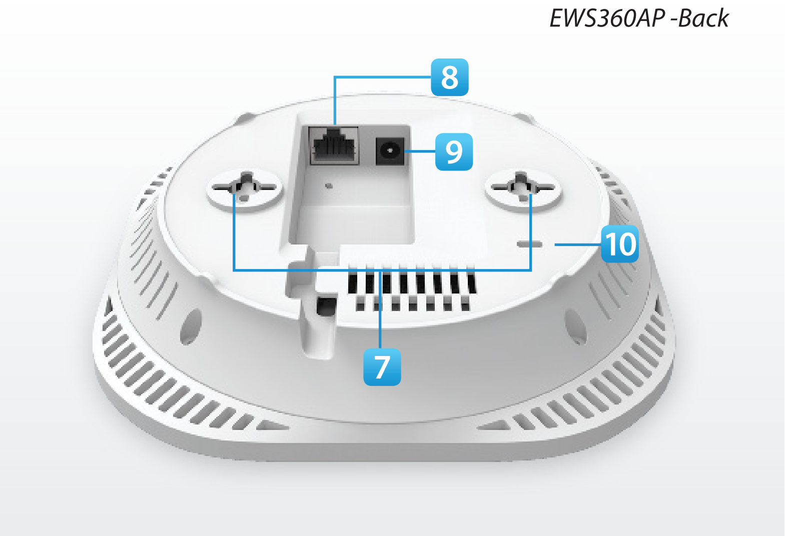
EWS360AP

Width: 6.36” Length: 6.36” Height: 1.64” Weight: 0.8 lbs.

EWS360AP- Front



EWS360AP -Back



1. **Mesh LED***
2. **5 GHz LED**
3. **Power LED**
4. **2.4 GHz LED**
5. **Ethernet Port LED**
6. **Power LED**
7. **Reset Button:** Press and hold for over **10** seconds to reset to factory default settings.
8. **Ceiling/Wall Mount Slots:** Using the provided hardware, the Access Point can be mounted to a ceiling or a wall.
9 **LAN Port (802.3at PoE):** Ethernet Port for RJ45 cable.
10. **Power Connector:** 12V DC IN for Power
11. **Kensington Security Slot:** To protect your Access Point, use the Kensington Security Slot to attach a cable lock (not included).

* Mesh networking mode available soon as a free firmware upgrade

Compatibility

Your Neutron Series Wireless Access Point supports the following Neutron Series EWS Switch models*:

EWS5912FP

- 8-Port Layer 2 PoE+ Wireless Management Switch with 2 SFP
- Supports up to 20 Neutron Series Access Points

EWS7928P

- 24-Port Layer 2 PoE+ Wireless Management Switch with 4 SFP
- Supports up to 50 Neutron Series Access Points

EWS7928FP

- 24-Port Layer 2 PoE+ Wireless Management Switch with 4 SFP
- Supports up to 50 Neutron Series Access Points

EWS7952FP

- 48-Port Layer 2 PoE+ Wireless Management Switch with 4 SFP
- Supports up to 50 Neutron Series Access Points

*Future firmware releases will support additional models.

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 can't be intsalled, deployed easily, or can't be hidden from view. Older buildings, sites with multiple buildings, and/or areas that makes the installation of an Ethernet based LAN impossible, impratical, or expensive are sites where WLAN can be a network solution.

- **Temporary Workgroups:** Create temporary workgroups or networks in more open areas within a building; auditoriums, amphitheatres, classrooms, ballrooms, arenas, exhibition centers, or temporary offices where one wants either a permanant or temporary Wireless LAN established.

- **The Ability to Access Real-time Information:** Doctors and registered Nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers, and/or processing information.

- **Frequently Changing Environments:** Setup networks in environments that change frequently (i.e: show rooms, conventions, exhibits, etc.).

- **Small Office & Home Office:** 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.

Chapter 2
Connecting Your Access Point

Installation

This section will guide you through the installation process. Placement of the 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. If there are any terms you are unfamilar with, please refer to the glossary on page 93.

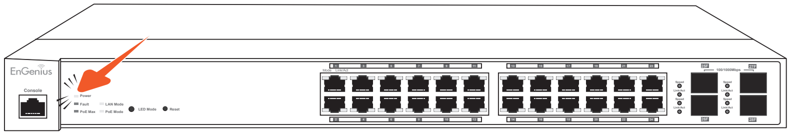
Considerations for Wireless Installation

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 AP's wireless signals must pass through can weaken the signal. Here are some key guidelines for allowing the AP to have an optimal wireless range during setup:

- Keep the number of walls and/or ceilings between the AP 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 AP. 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 AP's signal strength. The most common types of devices are microwaves or cordless phones.

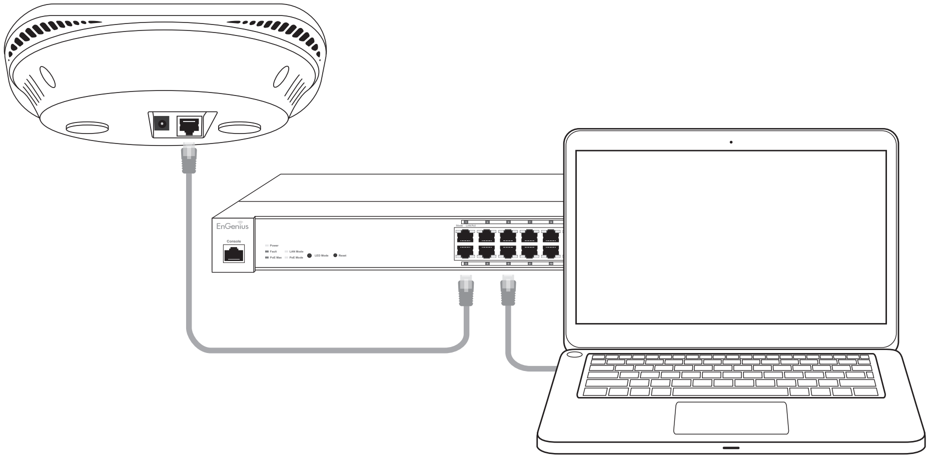
Connecting to the Neutron Series Switch

A) Connect the supplied **Power Cord** to the EWS Switch and plug the other end into an electrical outlet. Verify the Power LED indicator is lit on the EWS Switch. Wait for the EWS Switch to complete boot up. It might take few minutes to complete the process.



B) Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch's front panel and the other end to the Ethernet Port on the computer. Verify that the LED on the Ethernet port of the Switch is green.

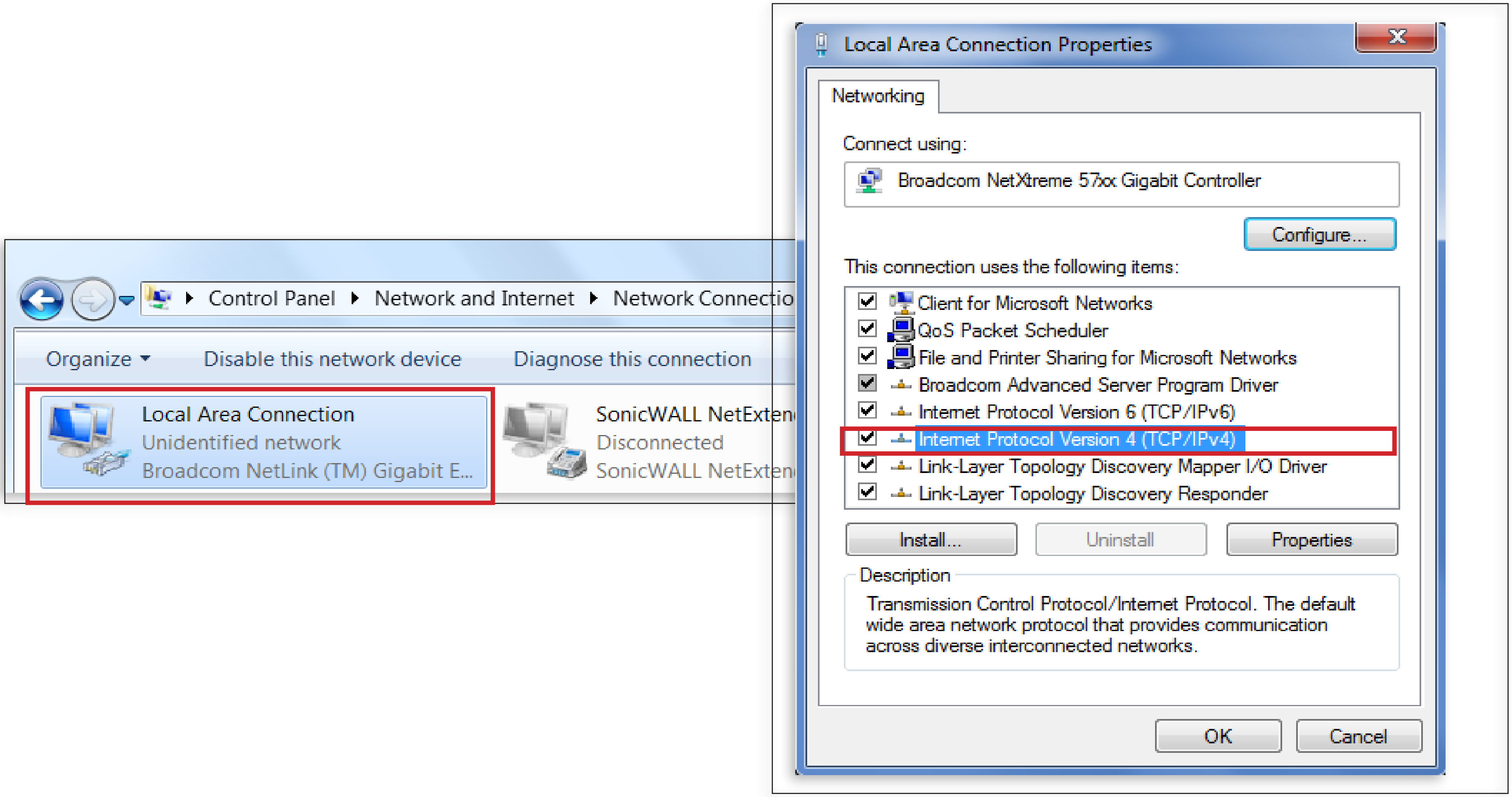
C) Connect the EWS AP(s) to the EWS Switch. Verify that the LED on the Ethernet port(s) of the EWS Switch is **green**.



IP Address Configuration

Windows XP, 7, 8

A) Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open Network Connections and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**.


Control Panel ▸ Network and Internet ▸ Network Connectio
Organize ▾
Disable this network device
Diagnose this connection
Configure...
Install...
Uninstall
Properties
OK
Cancel

Local Area Connection
Unidentified network
Broadcom NetLink (TM) Gigabit E...

SonicWALL NetExten
Disconnected
SonicWALL NetExten

Local Area Connection Properties

Networking

Connect using:

Broadcom NetXtreme 57xx Gigabit Controller

This connection uses the following items:

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

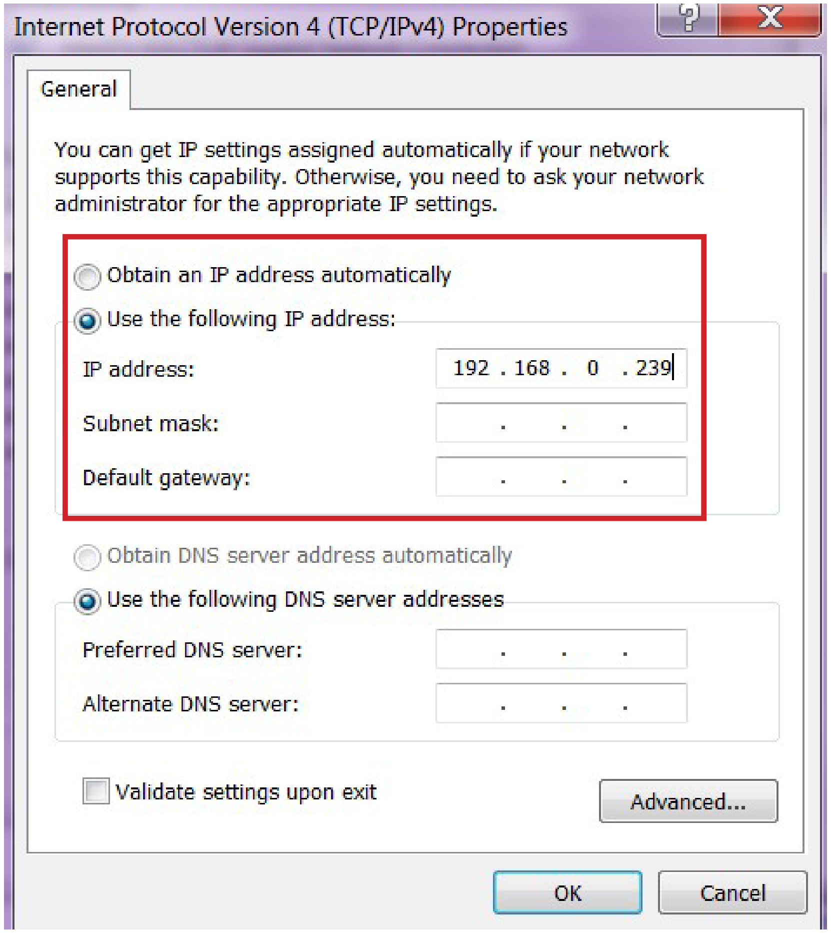
Description

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

B) If your computer is already on a network, ensure that you have set it to a Static IP Address on the interface. Please fill in the IP address, Subnet Mask, and Default Gateway you would like to use based on how you utilizing the Access Point. The Access Point can be setup to be managed in groups via an EWS Switch or in Standalone mode.

Managed: 192.168.0.239

Standalone: 192.168.1.XX



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.

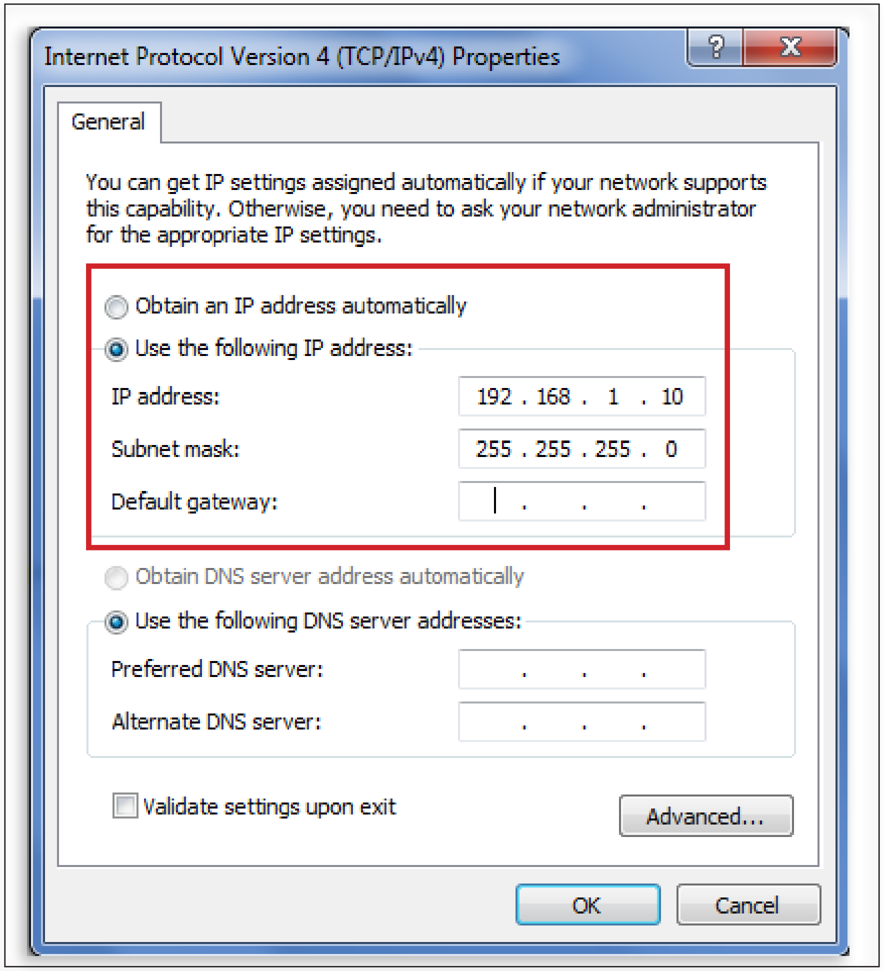
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 239
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit



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: . . .

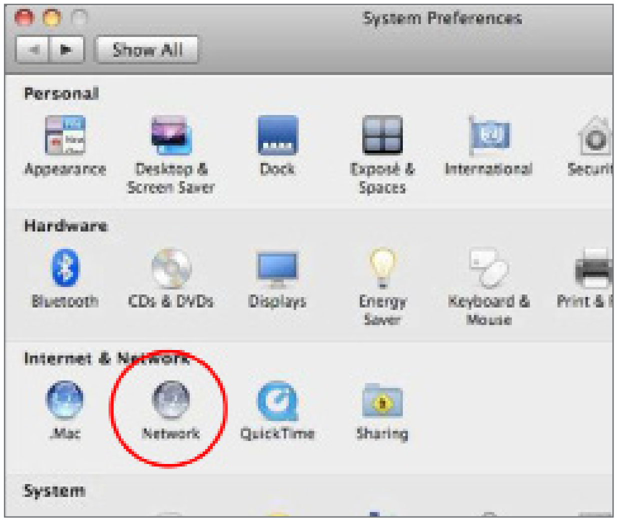
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Apple Mac OS X

A) Go to **System Preferences** (it can be opened in the Applications folder or by electing it in the Apple Menu).
B) Select **Network** in the **Internet & Network** section.



C) Highlight **Ethernet.**

D) In **Configure IPv4**, select **Manually.**

E) Enter an IP address that is different from the AP and Subnet mask, then click **OK.**

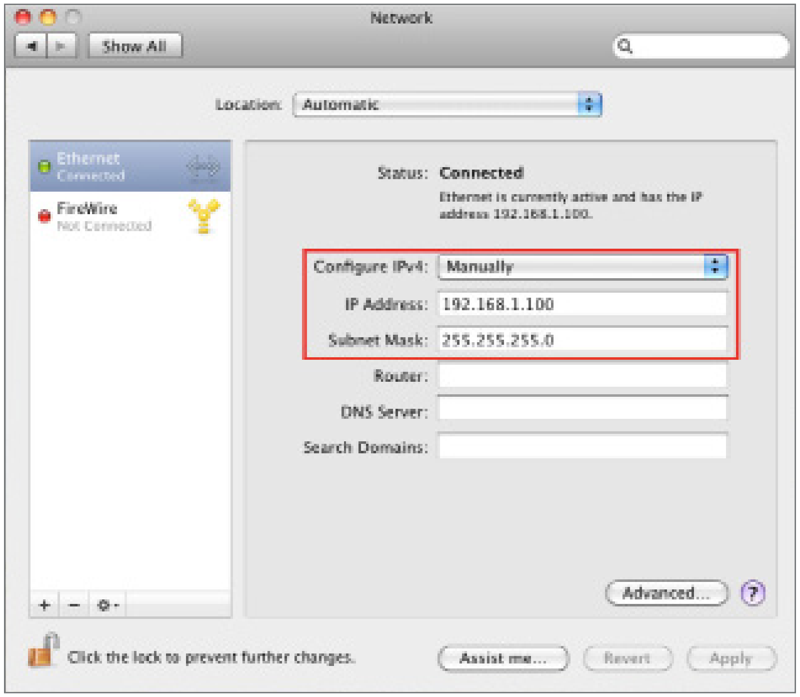
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: EWS320AP IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

PC Subnet mask: 255.255.255.0

F) 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:

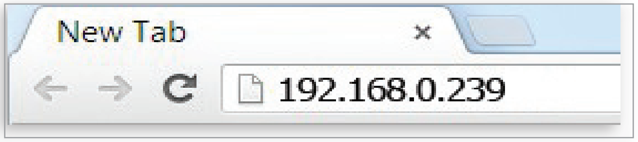
DNS Server:

Search Domains:

Click the lock to prevent further changes.

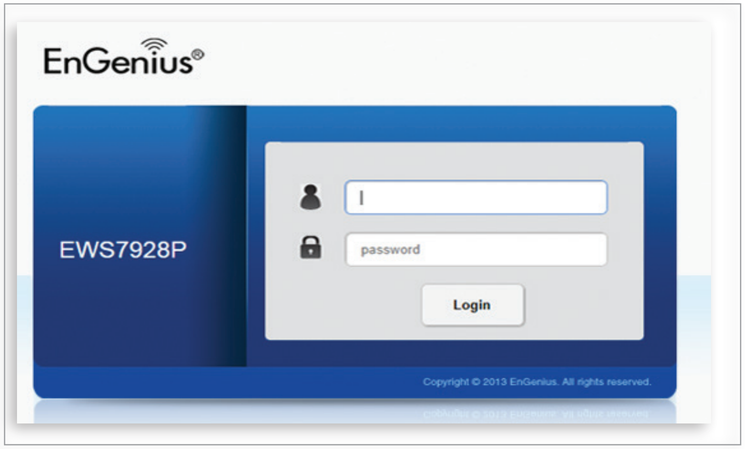
Wireless Management Switch Setup

A) Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **enter**.

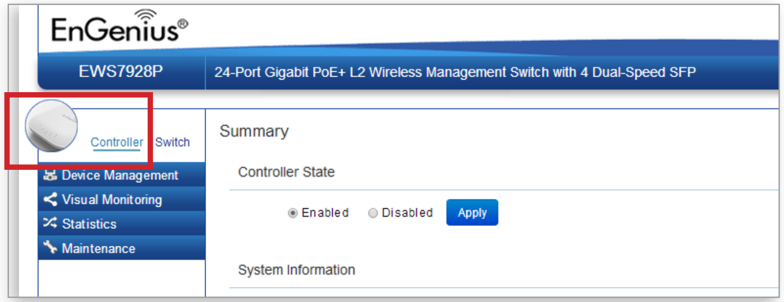


192.168.0.239

B) A login screen will appear. By default, username is **admin** and the password is **password**. Enter the current username and password of the Wireless Management Switch and then click **Login**.



C) The EnGenius Wireless Management Switch User Interface will appear. Make sure the **Controller State** is set to **Enabled**.



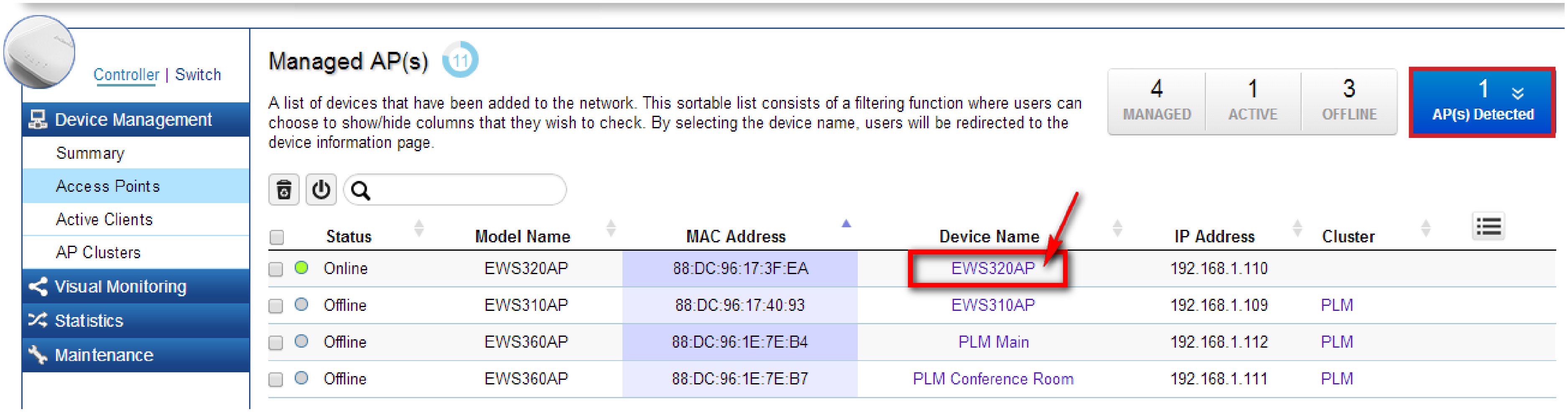
Controller State

● Enabled ○ Disabled

Device Management

Locating Wireless Managed AP(s)

A) Go to Device Management and select **Access Points** on the EWS Switch. All Managed AP(s) connected to the same network as the Wireless Management Switch will appear on the right side of the screen, under the Access Point AP(s) Detected list.



Managed AP(s)

A list of devices that have been added to the network. This sortable list consists of a filtering function where users can choose to show/hide columns that they wish to check. By selecting the device name, users will be redirected to the device information page.

□	Status	Model Name	MAC Address	Device Name	IP Address	Cluster
□	● Online	EWS320AP	88:DC:96:17:3F:EA	EWS320AP	192.168.1.110	
□	○ Offline	EWS310AP	88:DC:96:17:40:93	EWS310AP	192.168.1.109	PLM
□	○ Offline	EWS360AP	88:DC:96:1E:7E:B4	PLM Main	192.168.1.112	PLM
□	○ Offline	EWS360AP	88:DC:96:1E:7E:B7	PLM Conference Room	192.168.1.111	PLM

B) To manage the Access Points, select the desired Managed AP(s) by checking the boxes and click **Add**.

C) You will be prompted to enter an IP Address range for the Managed AP(s).

General Settings

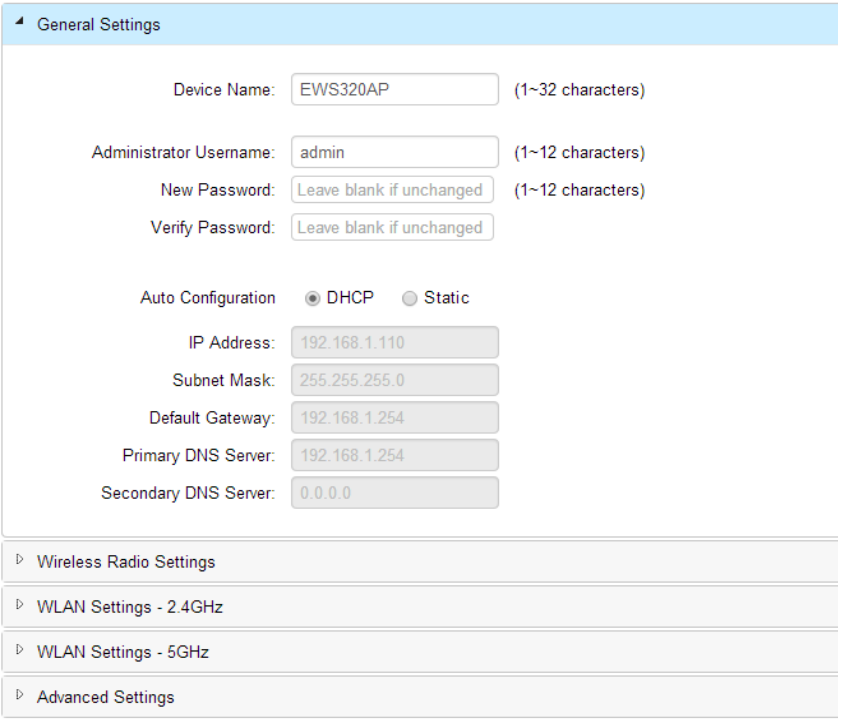
A) Enter the Device Name for the Access Point so that you can differentiate itself if you plan to use more than one AP.

B) Enter the Administrator acccount username and password to create an account that can access all features of the AP. next, enter the password again for verification.

C) Select DHCP or Static to determine how IP addresses will be assigned for the AP:

- Select **DHCP** for an IP Address to be assigned automatically if there is a DHCP server in the network.
- Select **Static** to enter the IP Address, Subnet Mask, Gateway, and DNS Server manually.

Please refer to page 46 for more detailed information on General Settings. Click **Apply** to continue.

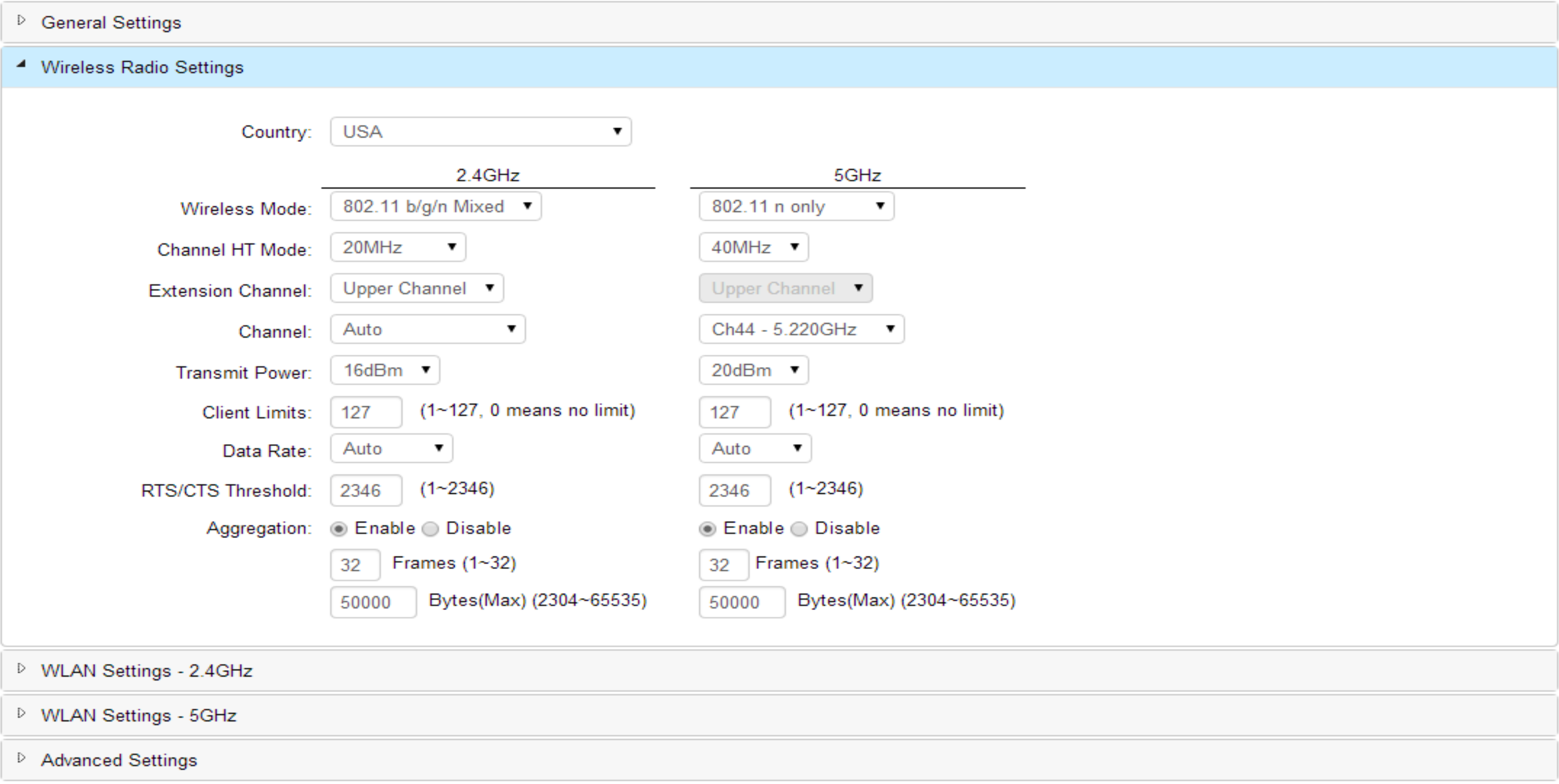


◢ General Settings

Device Name:	EWS320AP	(1~32 characters)
Administrator Username:	admin	(1~12 characters)
New Password:	Leave blank if unchanged	(1~12 characters)
Verify Password:	Leave blank if unchanged	
Auto Configuration	● DHCP ○ Static	
IP Address:	192.168.1.110	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.254	
Primary DNS Server:	192.168.1.254	
Secondary DNS Server:	0.0.0.0	

Wireless Radio Settings

After configuring the General Settings page, you will need to configure the Wireless Radio settings. Enter information pertaining to each frequency band that applies to your AP. Once finished, click **Apply** to continue. Please refer to page 52-53 for more detailed information on Wireless Radio Settings.



▷ General Settings

◢ Wireless Radio Settings

Country: USA ▼

	2.4GHz	5GHz
Wireless Mode:	802.11 b/g/n Mixed ▼	802.11 n only ▼
Channel HT Mode:	20MHz ▼	40MHz ▼
Extension Channel:	Upper Channel ▼	Upper Channel ▼
Channel:	Auto ▼	Ch44 - 5.220GHz ▼
Transmit Power:	16dBm ▼	20dBm ▼
Client Limits:	127 (1~127, 0 means no limit)	127 (1~127, 0 means no limit)
Data Rate:	Auto ▼	Auto ▼
RTS/CTS Threshold:	2346 (1~2346)	2346 (1~2346)
Aggregation:	● Enable ○ Disable	● Enable ○ Disable
	32 Frames (1~32)	32 Frames (1~32)
	50000 Bytes(Max) (2304~65535)	50000 Bytes(Max) (2304~65535)

▷ WLAN Settings - 2.4GHz

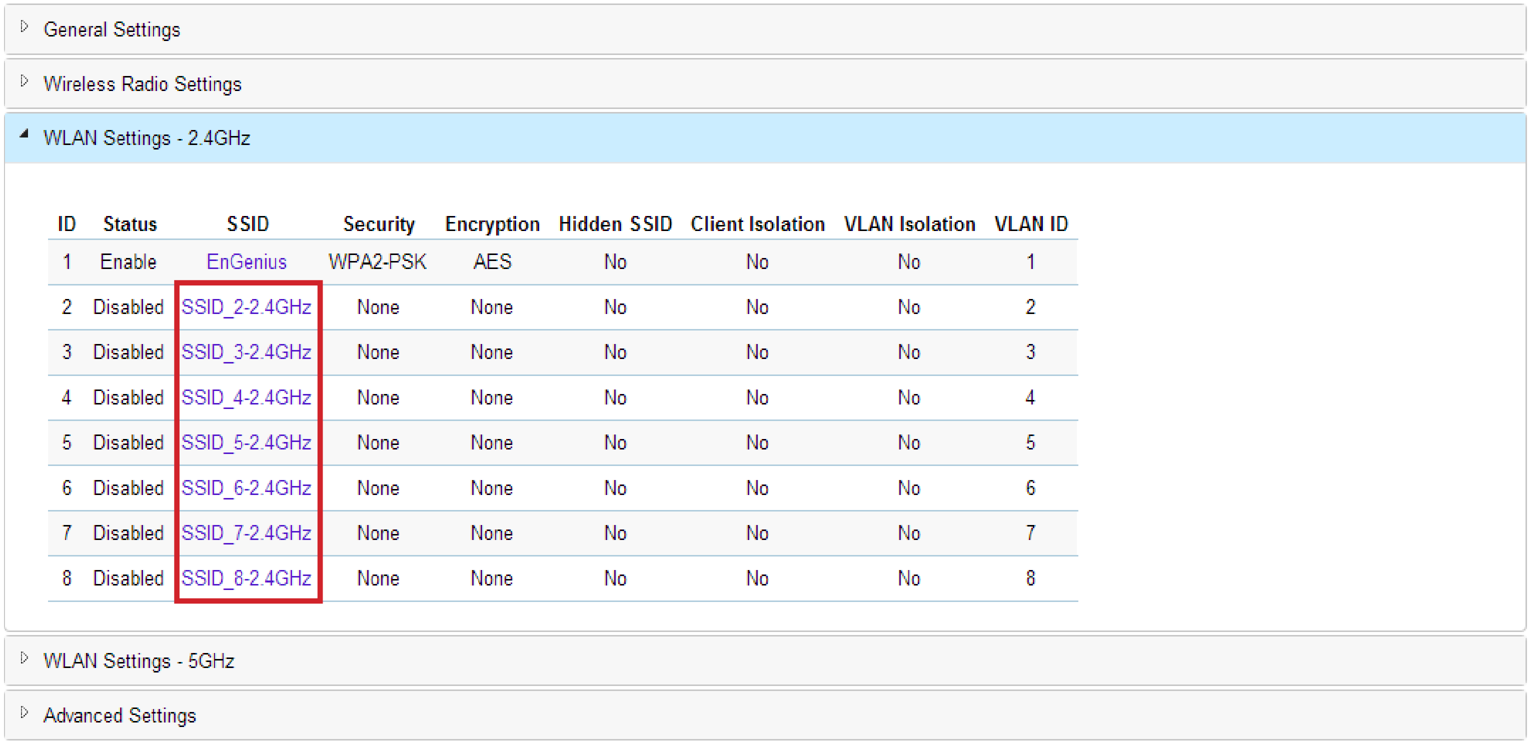
▷ WLAN Settings - 5GHz

▷ Advanced Settings

Note: The **EWS210AP** does **NOT** support the 5 GHz band and will only display settings for the 2.4 GHz band.

WLAN Settings 2.4/5 GHz

Next, you will need to configure the WLAN settings for each band. Click on an SSID to access Basic, Traffic, Fast Roaming, and Security settings. Once finished, click **Save** to apply the settings to the SSID. Please refer to page 54-66 for more detailed information on WLAN Settings. Once you have applied your configurations for each SSID, click **Apply** to continue.

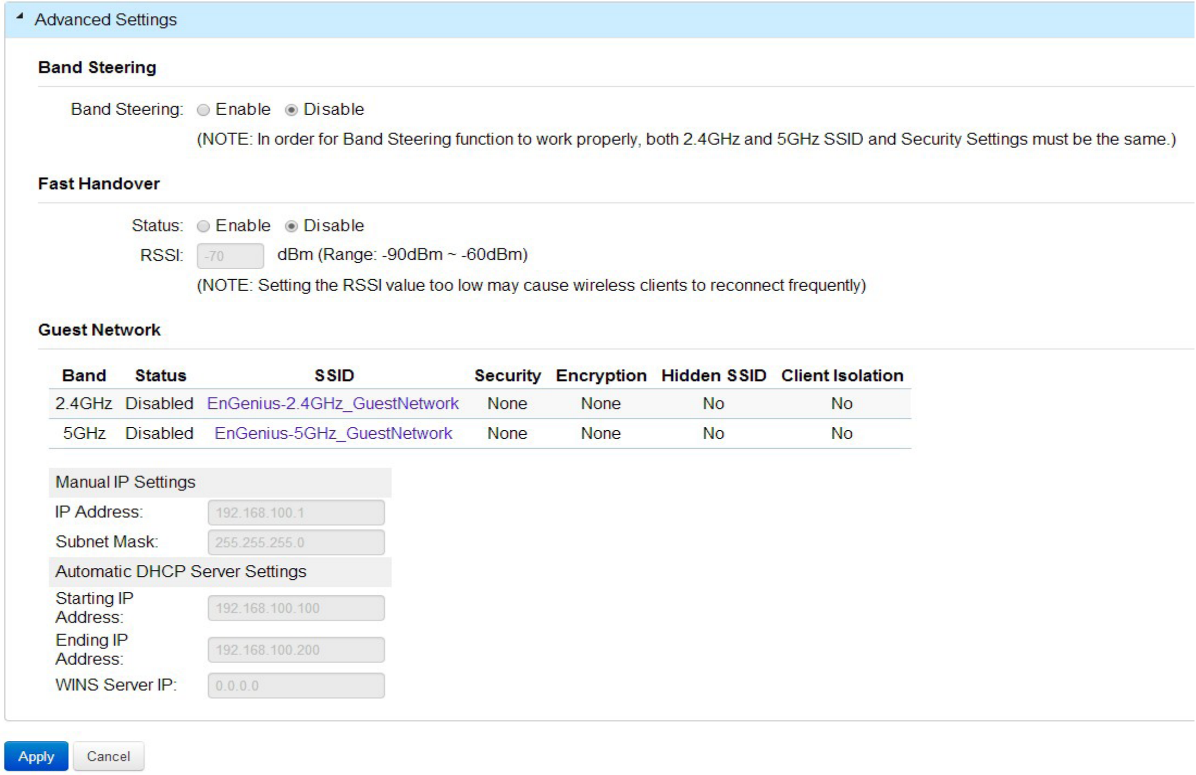


ID	Status	SSID	Security	Encryption	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	Enable	EnGenius	WPA2-PSK	AES	No	No	No	1
2	Disabled	SSID_2-2.4GHz	None	None	No	No	No	2
3	Disabled	SSID_3-2.4GHz	None	None	No	No	No	3
4	Disabled	SSID_4-2.4GHz	None	None	No	No	No	4
5	Disabled	SSID_5-2.4GHz	None	None	No	No	No	5
6	Disabled	SSID_6-2.4GHz	None	None	No	No	No	6
7	Disabled	SSID_7-2.4GHz	None	None	No	No	No	7
8	Disabled	SSID_8-2.4GHz	None	None	No	No	No	8

Note: The **EWS210AP** does **NOT** support the 5 GHz band and will only display settings for the 2.4 GHz band.

Adavnced Settings

Next, you will need to configure the Advanced settings for the Access Point. Please refer to page 51 for Band Steering, 66 for Fast Handover, 63 for Guest Networks, and 56 for Wireless Security for more detailed information on these advanced features. Once finished, click **Apply** to continue.



Advanced Settings

Band Steering

Band Steering: ○ Enable ● Disable

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

Fast Handover

Status: ○ Enable ● Disable

RSSI: -70 dBm (Range: -90dBm ~ -60dBm)

(NOTE: Setting the RSSI value too low may cause wireless clients to reconnect frequently)

Guest Network

Band	Status	SSID	Security	Encryption	Hidden SSID	Client Isolation
2.4GHz	Disabled	EnGenius-2.4GHz_GuestNetwork	None	None	No	No
5GHz	Disabled	EnGenius-5GHz_GuestNetwork	None	None	No	No

Manual IP Settings

IP Address: 192.168.100.1

Subnet Mask: 255.255.255.0

Automatic DHCP Server Settings

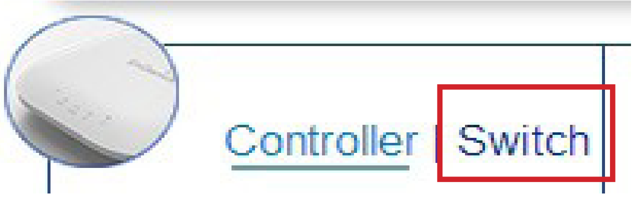
Starting IP Address: 192.168.100.100

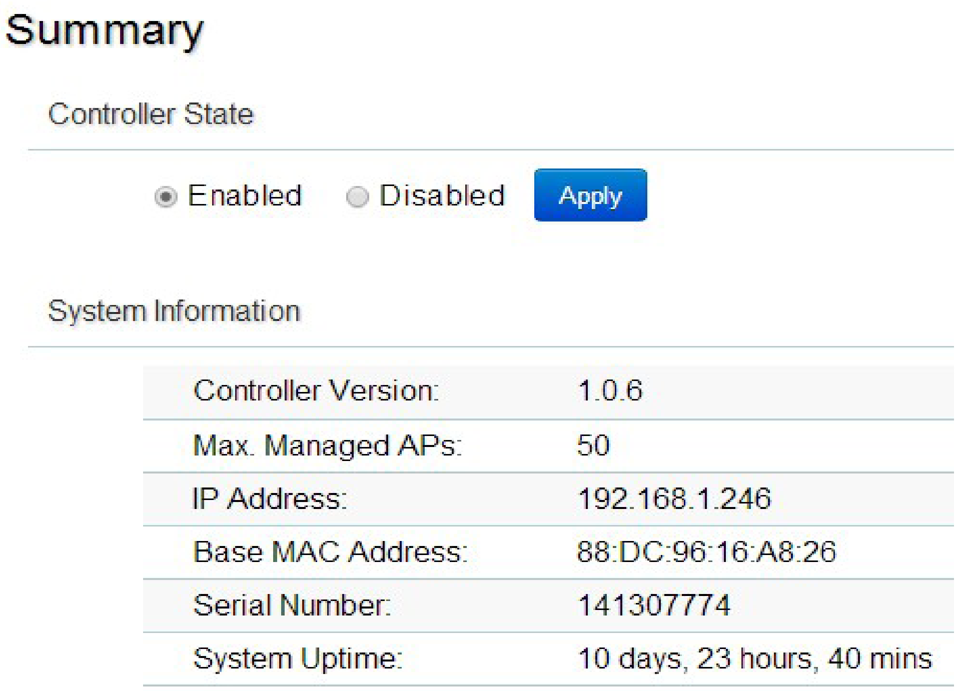
Ending IP Address: 192.168.100.200

WINS Server IP: 0.0.0.0

Managing A Wireless Management Switch

For further Switch configurations, click on Switch at the top left of the dash board. Refer to the Wireless Management Switch User Manual for more information on these configuration settings.





Summary

Controller State

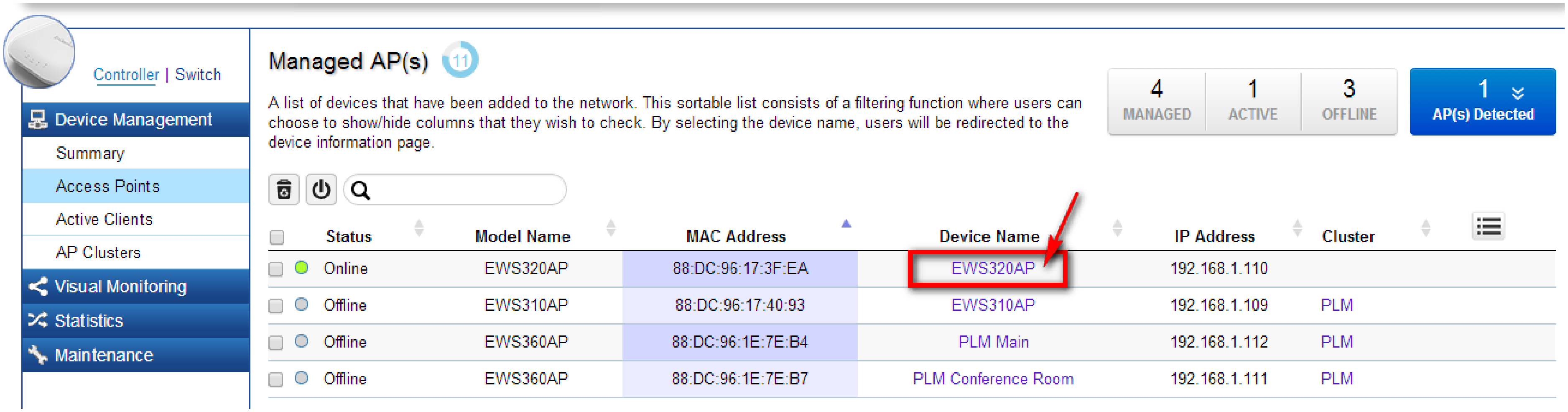
● Enabled ○ Disabled

System Information

Controller Version:	1.0.6
Max. Managed APs:	50
IP Address:	192.168.1.246
Base MAC Address:	88:DC:96:16:A8:26
Serial Number:	141307774
System Uptime:	10 days, 23 hours, 40 mins

Managing Wireless Managed Access Points

The Managed AP(s) that are successfully being managed will be listed under the Managed AP(s) list. Click on the **Device Name** to access to its configuration settings. Please refer to the Wireless Management Switch User Manual for more information on configuration settings.



Managed AP(s)

A list of devices that have been added to the network. This sortable list consists of a filtering function where users can choose to show/hide columns that they wish to check. By selecting the device name, users will be redirected to the device information page.

□	Status	Model Name	MAC Address	Device Name	IP Address	Cluster
□	● Online	EWS320AP	88:DC:96:17:3F:EA	EWS320AP	192.168.1.110	
□	○ Offline	EWS310AP	88:DC:96:17:40:93	EWS310AP	192.168.1.109	PLM
□	○ Offline	EWS360AP	88:DC:96:1E:7E:B4	PLM Main	192.168.1.112	PLM
□	○ Offline	EWS360AP	88:DC:96:1E:7E:B7	PLM Conference Room	192.168.1.111	PLM

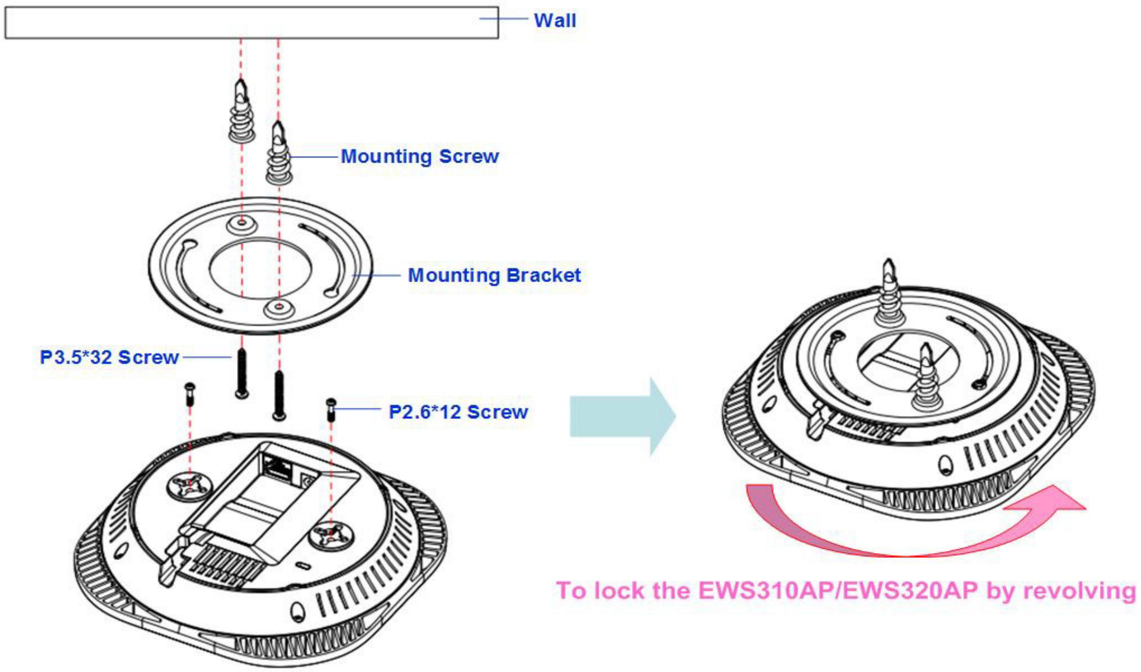
Mounting the Access Point

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

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

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

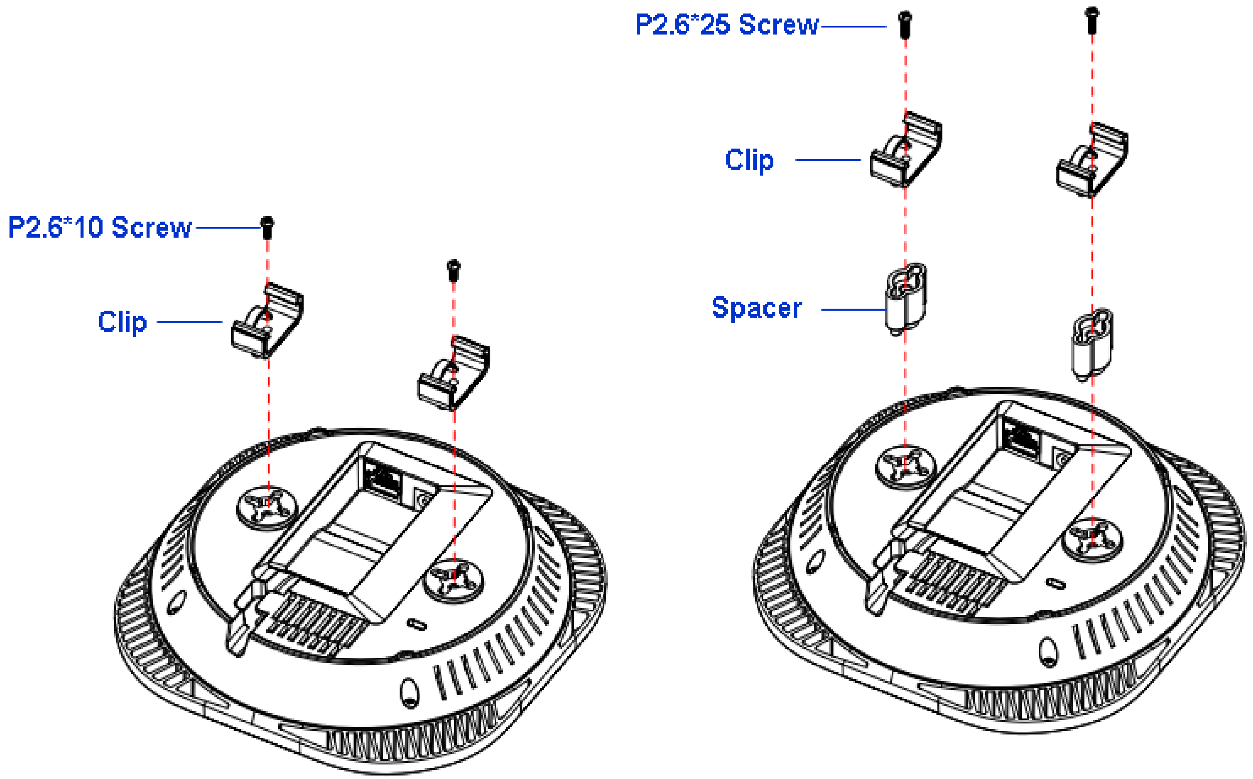
2. Insert the provided short screws into the bottom cover of the AP. Leave enough of the screws exposed to ensure that the unit can be attached to the mounting bracket. If extra space is required, use the provided spacers and long screws from the T-Rail mounting hardware kit to increase the space between the unit and the mounting bracket.



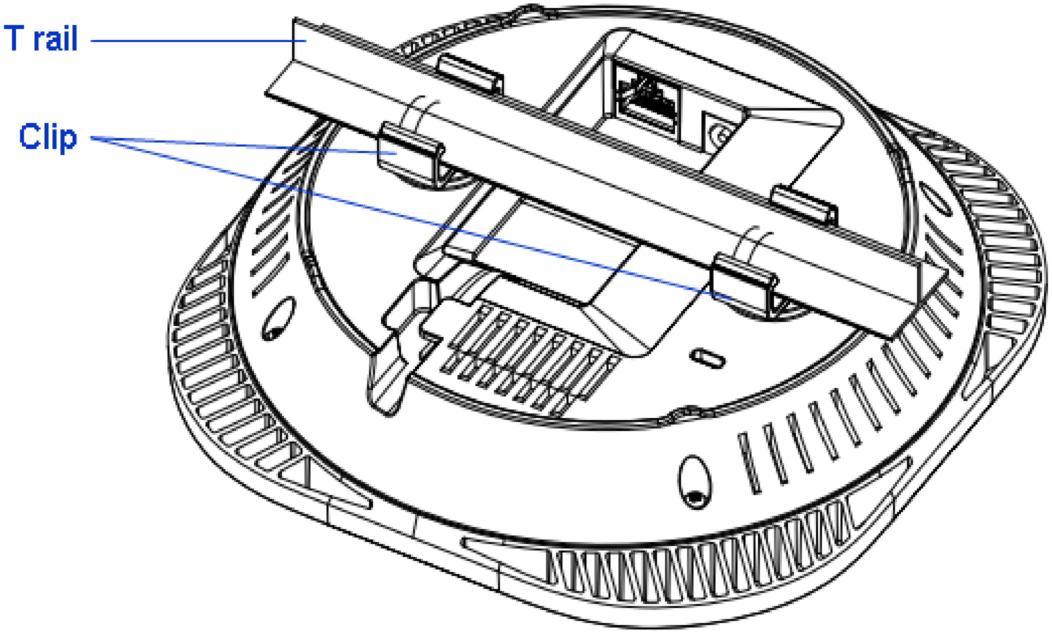
3. Mount the AP on the mounting bracket by rotating the unit clockwise about 90 degrees to secure it in place.

Attaching the AP to a ceiling using the provided T-Rail connectors:

1. Attach the T-Rail connectors to the bottom cover of the AP using the provided short screws.
Note: Two sizes of T-Rail connectors are included in the mounting hardware kit: 15/16in (2.38cm) and 9/16in (1.43cm). If extra space is required to accommodate drop ceiling tiles, use the provided spacers and long screws.



2. Line up the connected T-Rail connectors with an appropriately sized rail and press the unit onto the rail until it snaps into place.



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

Chapter 3
Configuration

Configuring Your Access Point

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

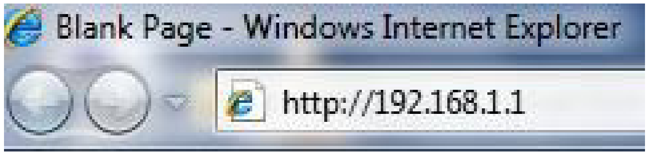
Default Settings

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

IP Address: 192.168.1.1
Username: admin
Password: admin

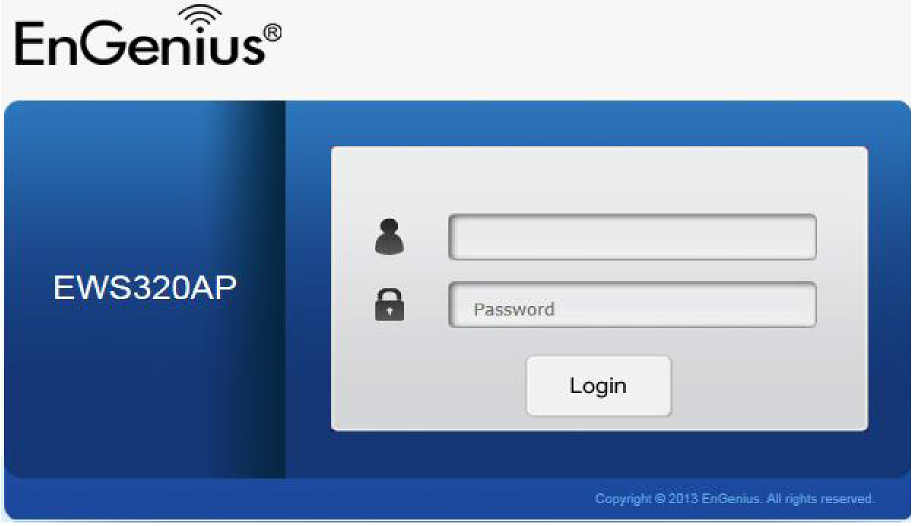
Web Configuration

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

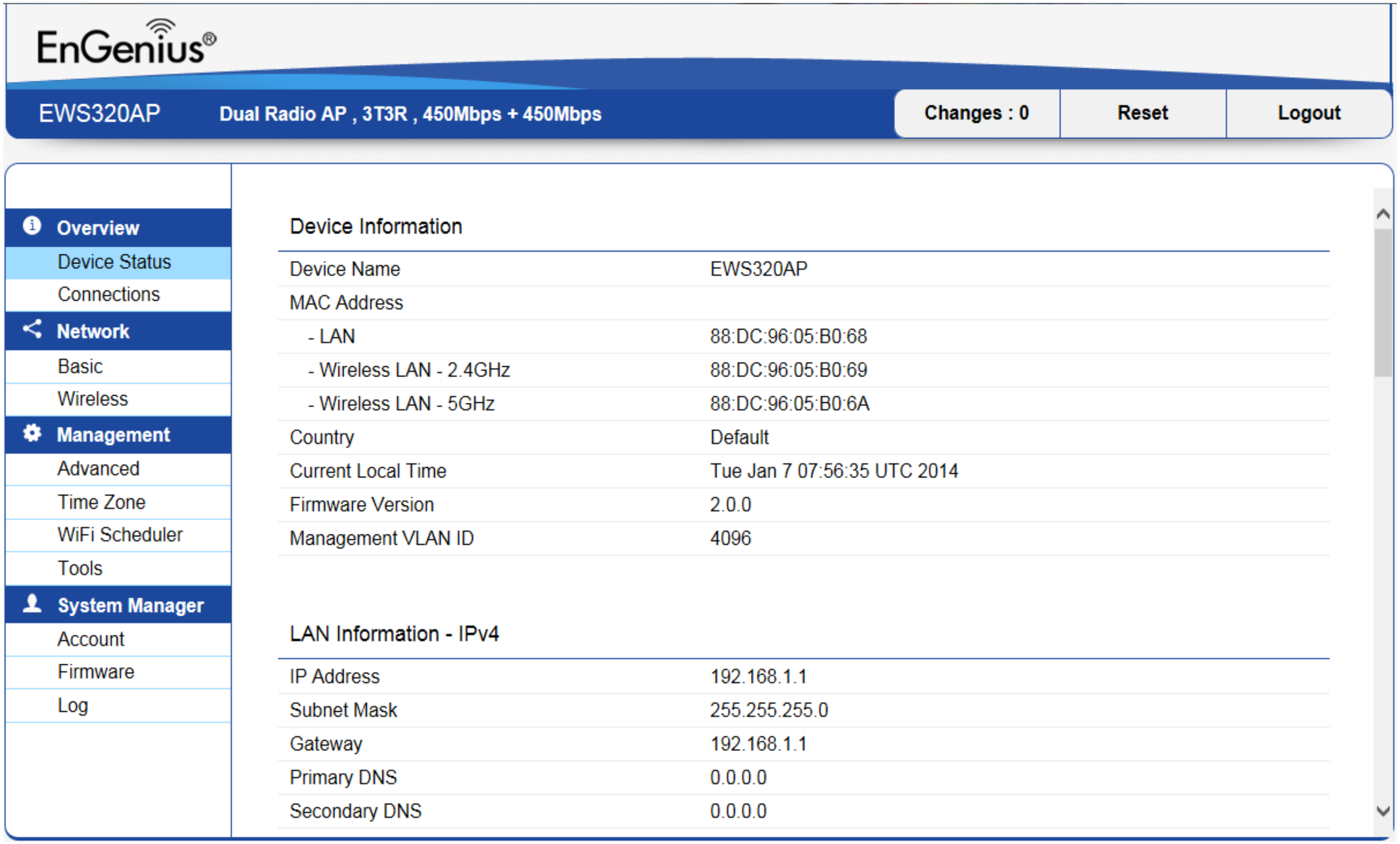


Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

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 EWS AP User Interface Menu.



Device Information

Device Name	EWS320AP
MAC Address	
- LAN	88:DC:96:05:B0:68
- Wireless LAN - 2.4GHz	88:DC:96:05:B0:69
- Wireless LAN - 5GHz	88:DC:96:05:B0:6A
Country	Default
Current Local Time	Tue Jan 7 07:56:35 UTC 2014
Firmware Version	2.0.0
Management VLAN ID	4096

LAN Information - IPv4

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Chapter 4 **Overview**

Overview

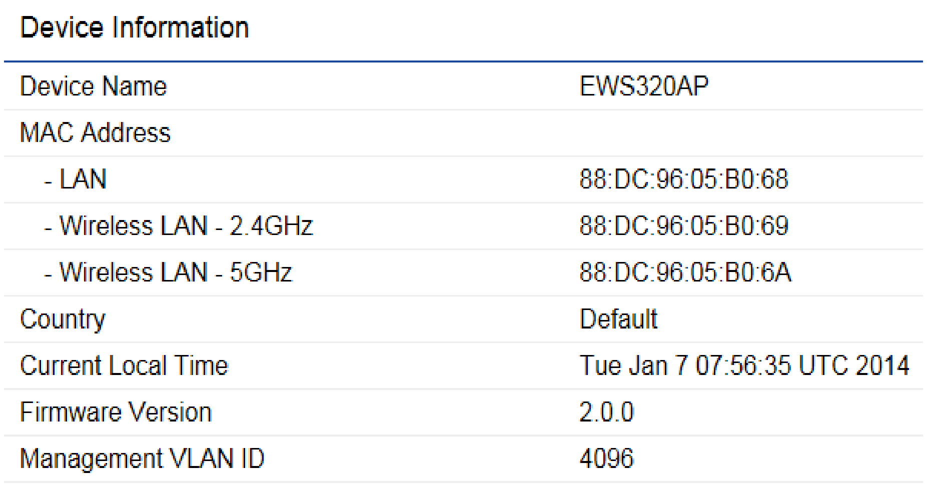
The Overview section contains the following options:

- Device Status
- Connections

The following sections describe these options.

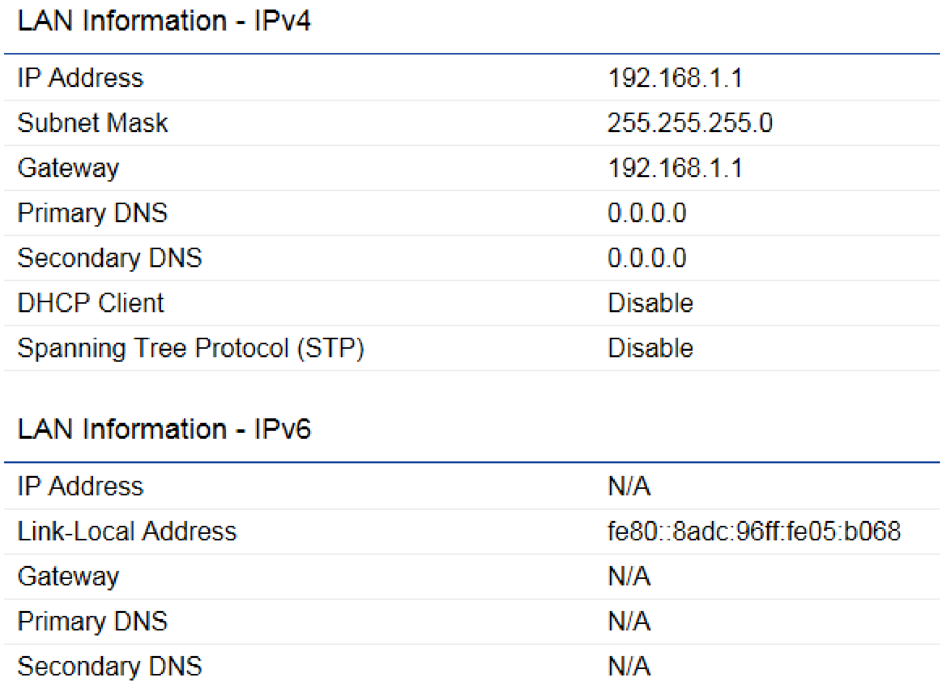
Device Status

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.



Device Information

Device Name	EWS320AP
MAC Address	
- LAN	88:DC:96:05:B0:68
- Wireless LAN - 2.4GHz	88:DC:96:05:B0:69
- Wireless LAN - 5GHz	88:DC:96:05:B0:6A
Country	Default
Current Local Time	Tue Jan 7 07:56:35 UTC 2014
Firmware Version	2.0.0
Management VLAN ID	4096



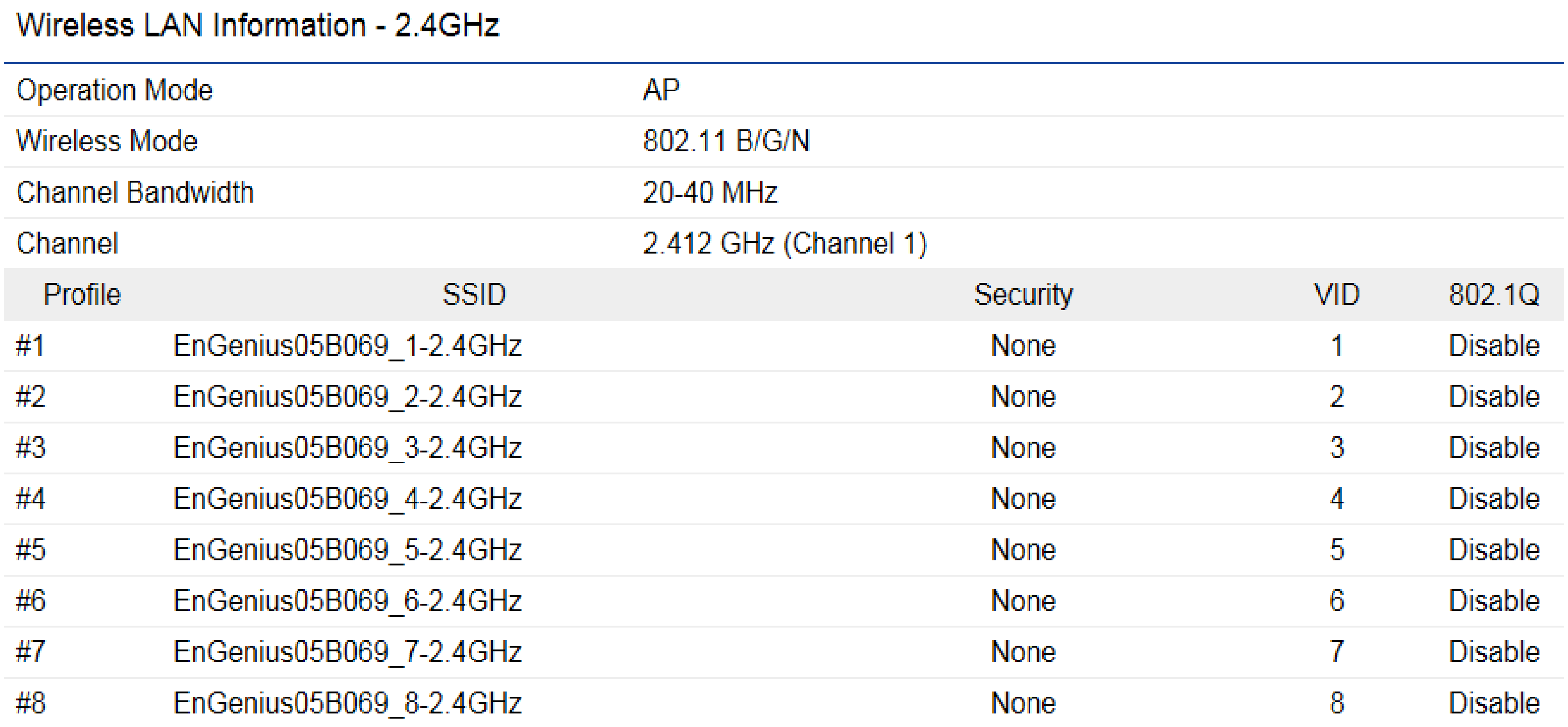
LAN Information - IPv4

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

LAN Information - IPv6

IP Address	N/A
Link-Local Address	fe80::8adc:96ff:fe05:b068
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 EWS AP supports multiple-SSIDs, information about each SSID and security settings are displayed.



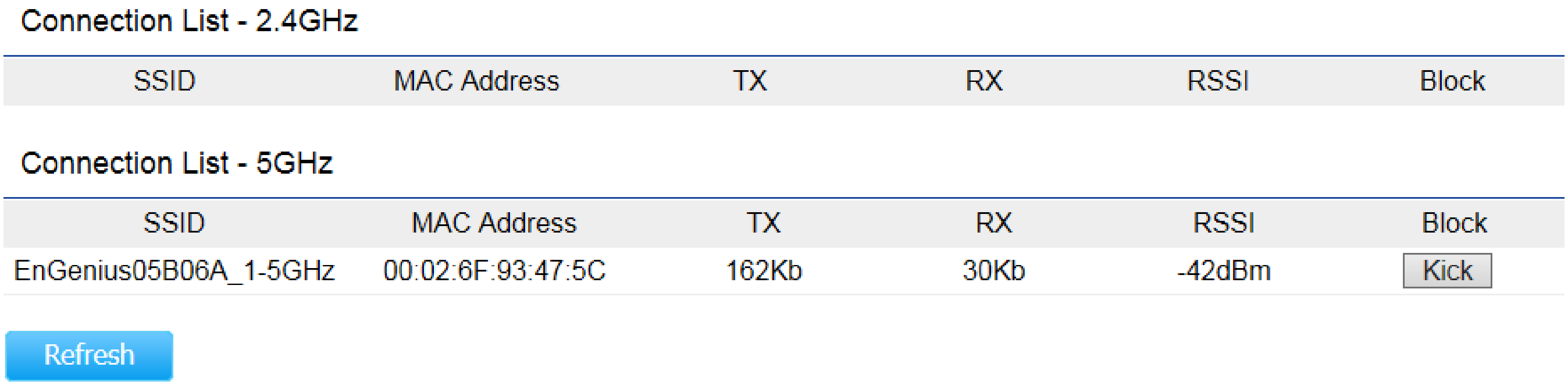
Wireless LAN Information - 2.4GHz

Operation Mode	AP
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	EnGenius05B069_1-2.4GHz	None	1	Disable
#2	EnGenius05B069_2-2.4GHz	None	2	Disable
#3	EnGenius05B069_3-2.4GHz	None	3	Disable
#4	EnGenius05B069_4-2.4GHz	None	4	Disable
#5	EnGenius05B069_5-2.4GHz	None	5	Disable
#6	EnGenius05B069_6-2.4GHz	None	6	Disable
#7	EnGenius05B069_7-2.4GHz	None	7	Disable
#8	EnGenius05B069_8-2.4GHz	None	8	Disable

Connections

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



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

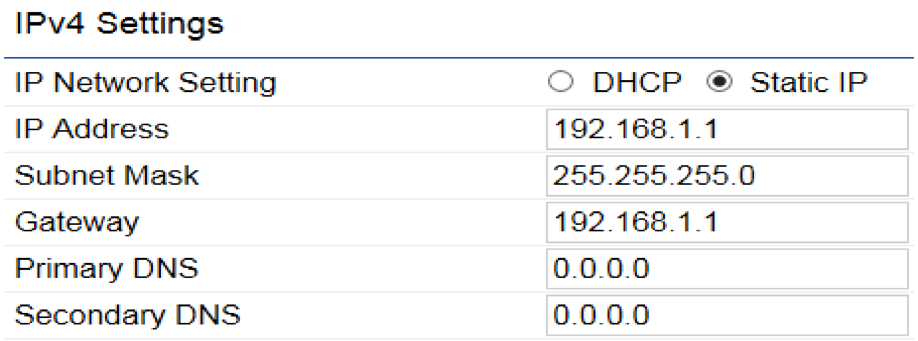
Click **Refresh** to refresh the Connections list page.

Chapter 5
Network

Basic

This page allows you to modify the device's IP settings and the Spanning Tree settings. Enabling the 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 Settings
Select whether the device's IP address will use the static IP address specified or be obtained automatically when the device connects to a DHCP server.

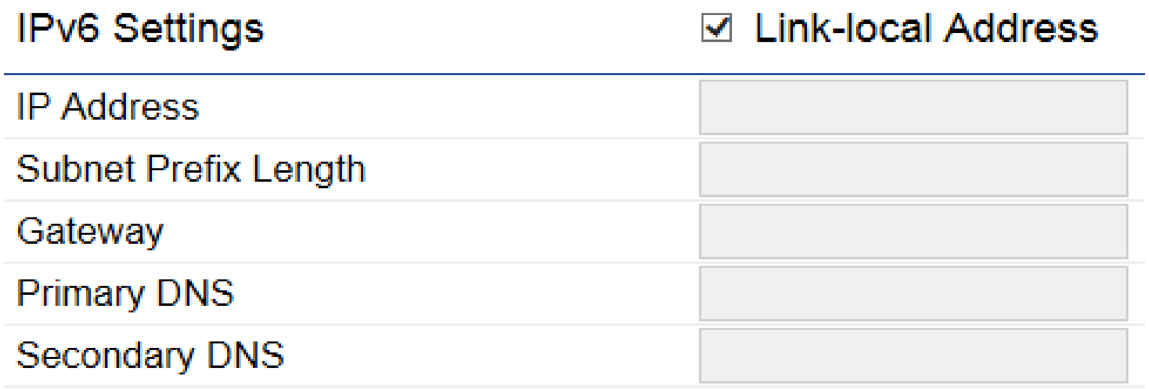
IP Address
Displays the IP address of this device.

IP Subnet Mask
Displays the IP Subnet mask of this device. A subnet is a logically visible subdivision of an IP network. A is mask used to determine what subnet an IP address belongs to.

Gateway
Displays the Default Gateway of this device. Leave it blank if you are unsure of this setting.

Primary/Secondary DNS
Displays 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 a Link-Local Address. A Link-Local Address is a network address that is valid for communications within the network segment or the broadcast domain that the host is connected to.

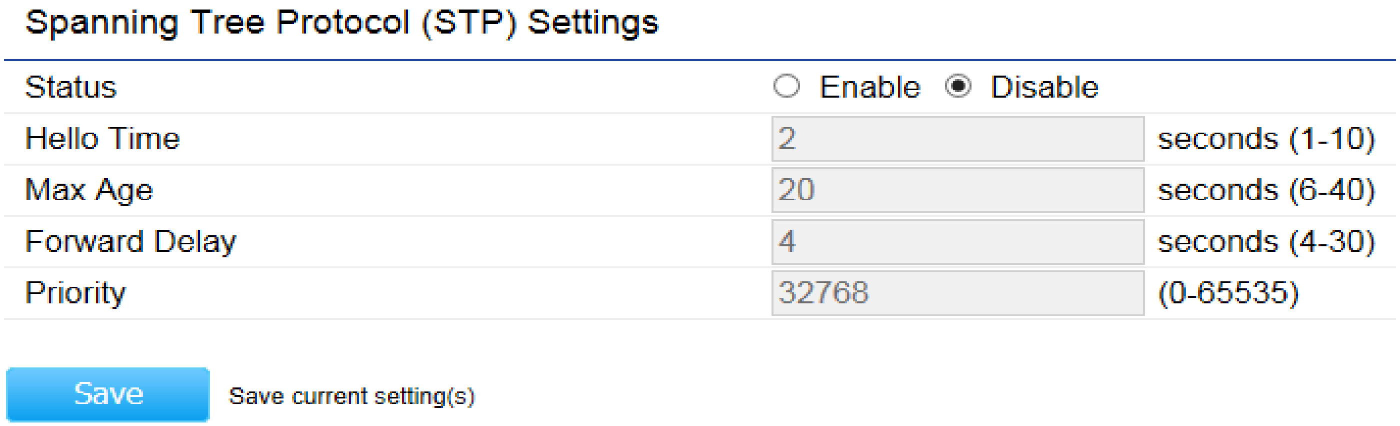
IP Address
Displays the IPv6 IP Address of this device.

Subnet Prefix Length
Displays the IPv6 Subnet Prefix Length of this device.

Gateway
Displays the IPv6 Default Gateway of this device. Leave it blank if you are unsure of this setting.

Primary/Secondary DNS
Displays the primary/secondary DNS address for this device. DNS stands for Domain Name System, which refers to a naming system for computers, services, or other resources connected to a private network or the Internet.

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 Protocol feature. The Spanning Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths

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

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

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

Priority
Specifies the Priority Number. A smaller number has greater priority.

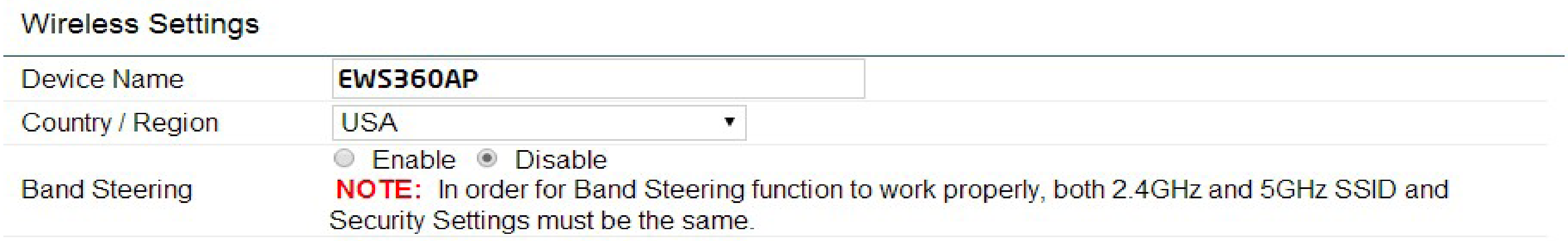
Save
Click **Save** to confirm the changes.

Chapter 6
Wireless

Wireless Network

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

Wireless Settings



Wireless Settings

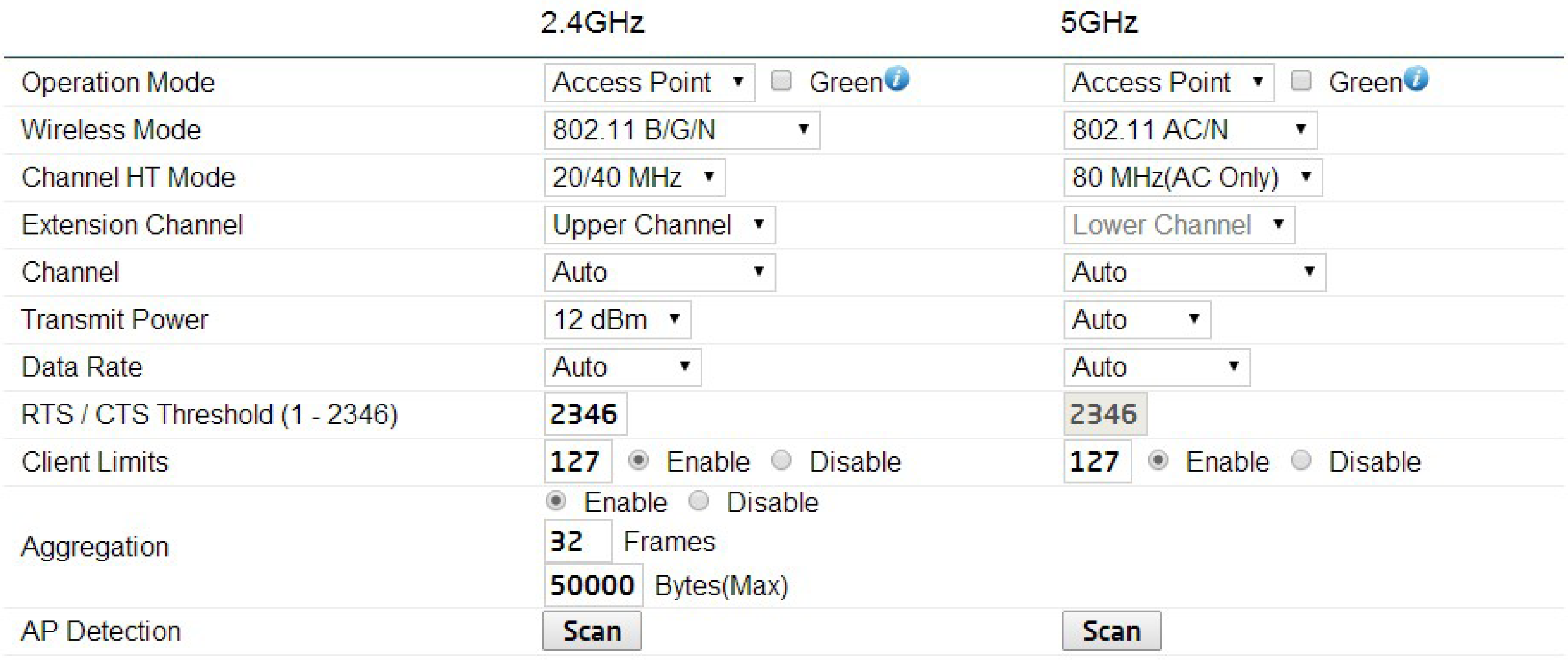
Device Name	EWS360AP
Country / Region	USA ▾
Band Steering	○ Enable ● Disable NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

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.

Country/Region
Select a Country/Region to conform to local regulations.

Band Steering
The Band Steering feature detects Dual Band clients and shifts them to the 5 GHz band to relieve network congestion on the 2.4 GHz band to maintain optimal data traffic flow, helping clients on both bands.

Note: In order for the Band Steering feature to work properly, both the 2.4GHz and the 5 GHz SSID and security settings must be configured with the same settings. Band Steering is not available for the **EWS210AP**.



	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	20/40 MHz ▾	80 MHz(AC Only) ▾
Extension Channel	Upper Channel ▾	Lower Channel ▾
Channel	Auto ▾	Auto ▾
Transmit Power	12 dBm ▾	Auto ▾
Data Rate	Auto ▾	Auto ▾
RTS / CTS Threshold (1 - 2346)	2346	2346
Client Limits	127 ● Enable ○ Disable	127 ● Enable ○ Disable
Aggregation	● Enable ○ Disable 32 Frames 50000 Bytes(Max)	
AP Detection	Scan	Scan

Wireless Mode

Supports 802.11b/g/n mixed mode in 2.4 GHz and 802.11ac/n mixed mode in 5 GHz.

Channel HT Mode

The default channel bandwidth is 20/40MHz. The larger the channel bandwidth, the better the transmission quality and speed. This option is only available for 802.11n modes. For 802.11ac under 5 GHz, you must select 80 MHz.

Extension Channel

Use the drop-down list to set the Extension Channel as the upper or lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase the range to 40MHz, allowing for greater bandwidth. This option is only available when the Wireless Mode is 802.11n and the Channel HT Mode is 20/40 MHz or 40MHz.

Channel
Select the channel appropriate for your country's regulation.

Transmit Power
Select the transmit power for the radio. Increasing the power improves performance, but if two or more access points are operating in the same area on the same channel, it may cause interference.

Data Rate
Use the drop-down list to set the available transmit data rates permitted for wireless clients. The data rate affects the throughput of the access point. The lower the data rate, the lower the throughput, but the longer transmission distance.

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. The range is from 1~2346.

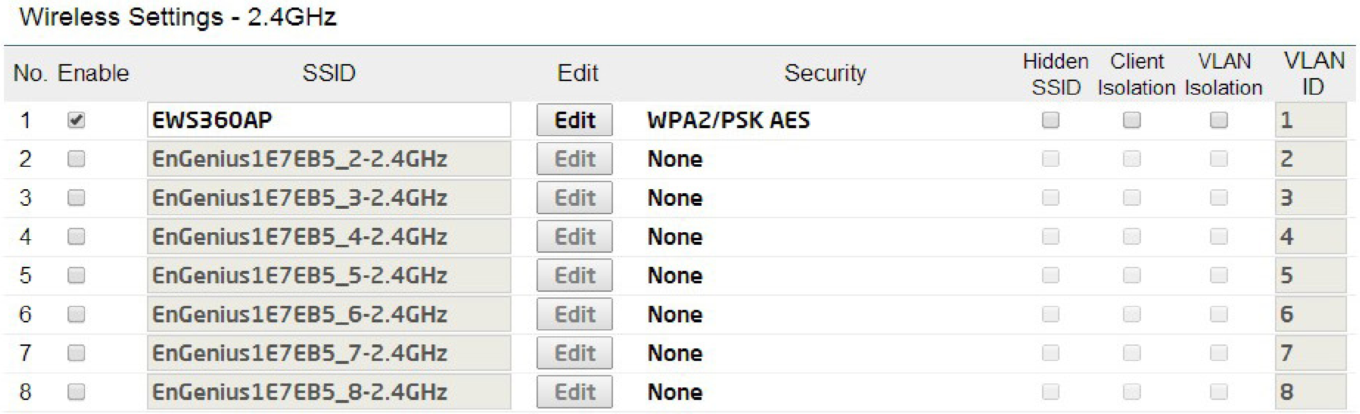
Client Limits
Click the bubble to enable or disable the client limit. The Client lists limits the total number of clients per frequency band.

Aggregation
Merges data packets into one packet. 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.

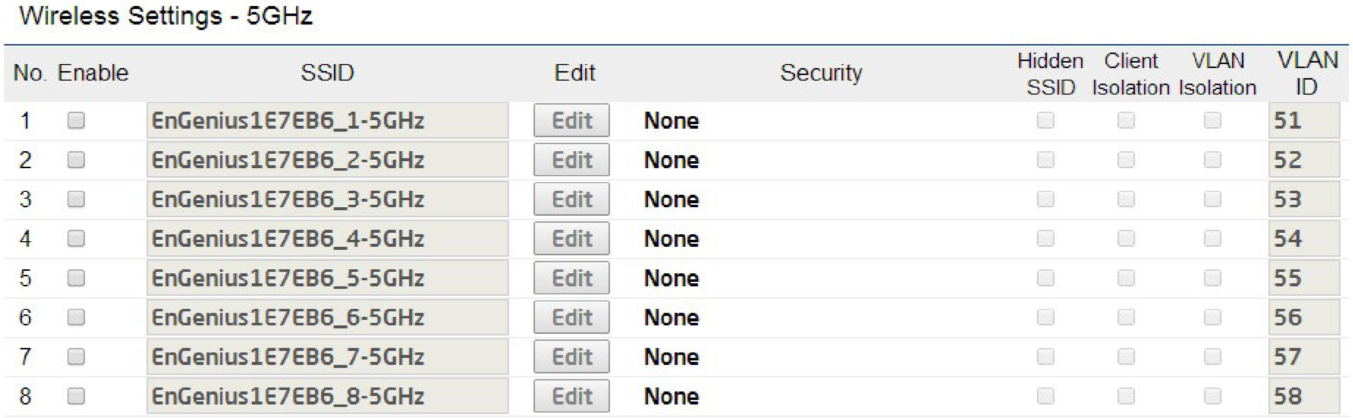
2.4 GHz/5 GHz SSID Profile

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	☑	EWS360AP	Edit	WPA2/PSK AES	□	□	□	1
2	□	EnGenius1E7EB5_2-2.4GHz	Edit	None	□	□	□	2
3	□	EnGenius1E7EB5_3-2.4GHz	Edit	None	□	□	□	3
4	□	EnGenius1E7EB5_4-2.4GHz	Edit	None	□	□	□	4
5	□	EnGenius1E7EB5_5-2.4GHz	Edit	None	□	□	□	5
6	□	EnGenius1E7EB5_6-2.4GHz	Edit	None	□	□	□	6
7	□	EnGenius1E7EB5_7-2.4GHz	Edit	None	□	□	□	7
8	□	EnGenius1E7EB5_8-2.4GHz	Edit	None	□	□	□	8



Wireless Settings - 5GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	□	EnGenius1E7EB6_1-5GHz	Edit	None	□	□	□	51
2	□	EnGenius1E7EB6_2-5GHz	Edit	None	□	□	□	52
3	□	EnGenius1E7EB6_3-5GHz	Edit	None	□	□	□	53
4	□	EnGenius1E7EB6_4-5GHz	Edit	None	□	□	□	54
5	□	EnGenius1E7EB6_5-5GHz	Edit	None	□	□	□	55
6	□	EnGenius1E7EB6_6-5GHz	Edit	None	□	□	□	56
7	□	EnGenius1E7EB6_7-5GHz	Edit	None	□	□	□	57
8	□	EnGenius1E7EB6_8-5GHz	Edit	None	□	□	□	58

Enable
Check this option to enable this profile for client use.

SSID
Specifies the SSID name for the current profile.

Security
Displays the Security Mode the SSID uses. You can click **Edit** to change the security mode. For more details, refer 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.

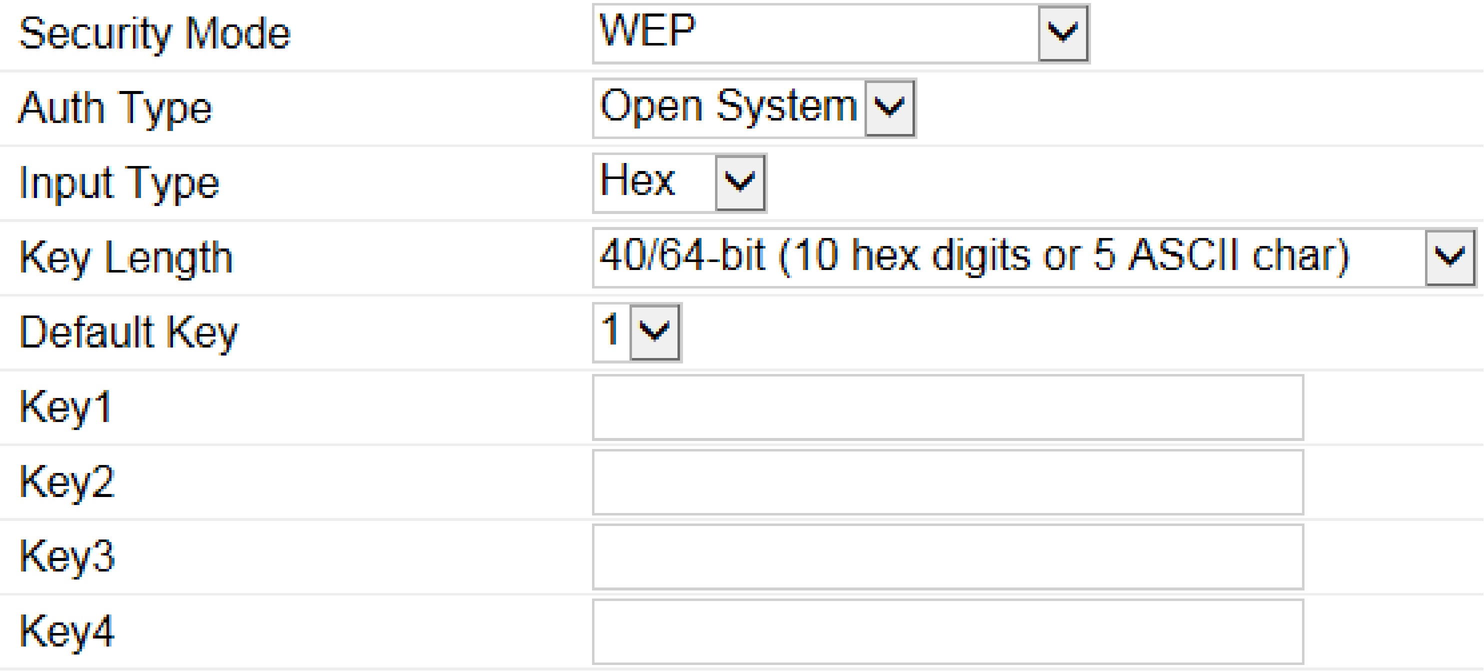
VLAN Isolation
Check this option to enable the VLAN Isolation feature. VLAN Isolation refers to Layer 2 (L2) connectivity without access via a route to devices on other TCP/IP networks from the network switching perspective. These types of VLANs are used for when multiple interfaces are needed to which you can dedicate certain roles to the security zone associated with the fully isolated VLAN.

VLAN ID
Specifies the VLAN ID number for the SSID profile for your reference.

Wireless Security

The Wireless Security section lets you configure the EWS AP’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 manage 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.

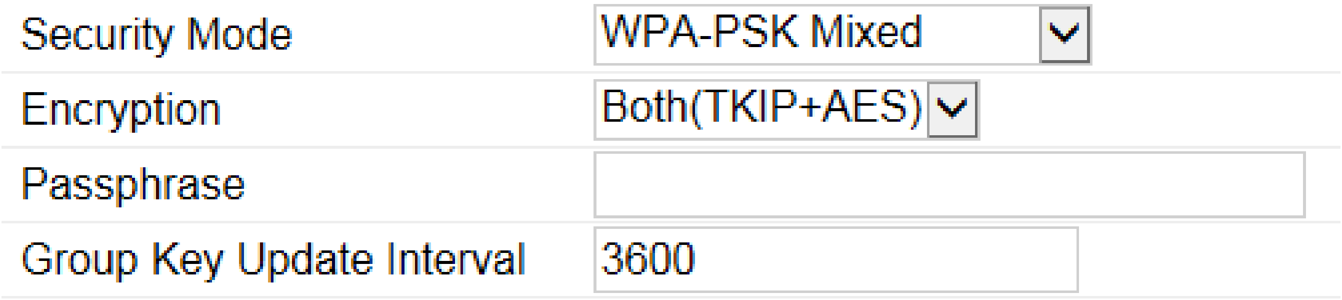
Default Key

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)



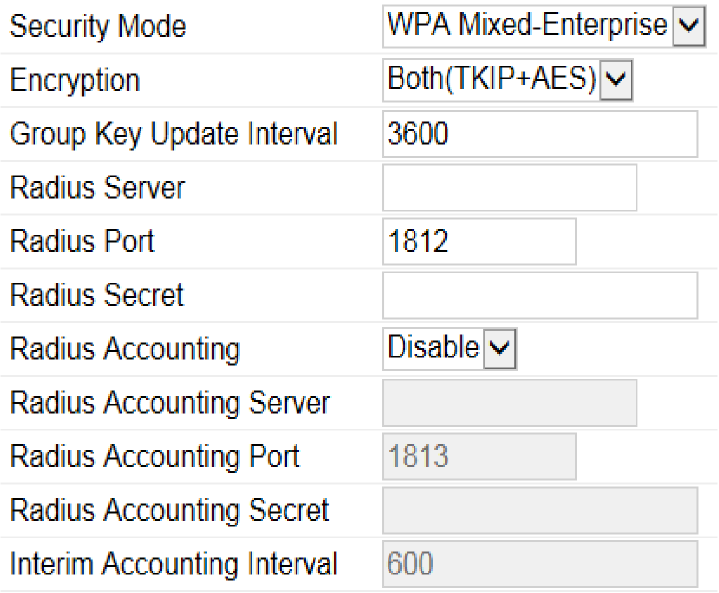
Security Mode	WPA-PSK Mixed
Encryption	Both(TKIP+AES)
Passphrase	
Group Key Update Interval	3600

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.

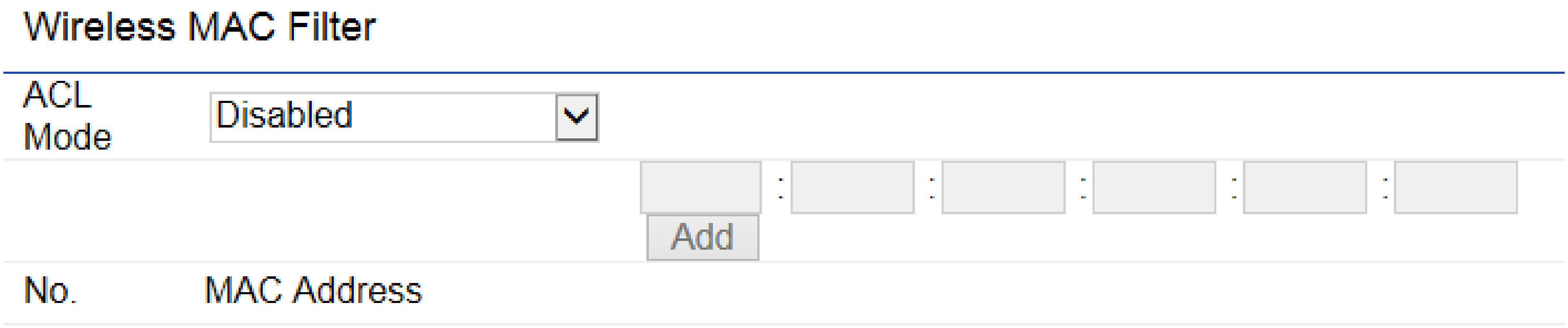
Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

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 modes. The connection mode will automatically change from 802.11n to 802.11g.

Wireless MAC Filter

The Wireless MAC Filter feature 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 AP. The default setting is: **Disable Wireless MAC Filter**.



Wireless MAC Filter

ACL Mode: Disabled

No.	MAC Address

ACL (Access Control List) Mode

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

MAC Address

Enter the MAC address of the wireless client.

Add

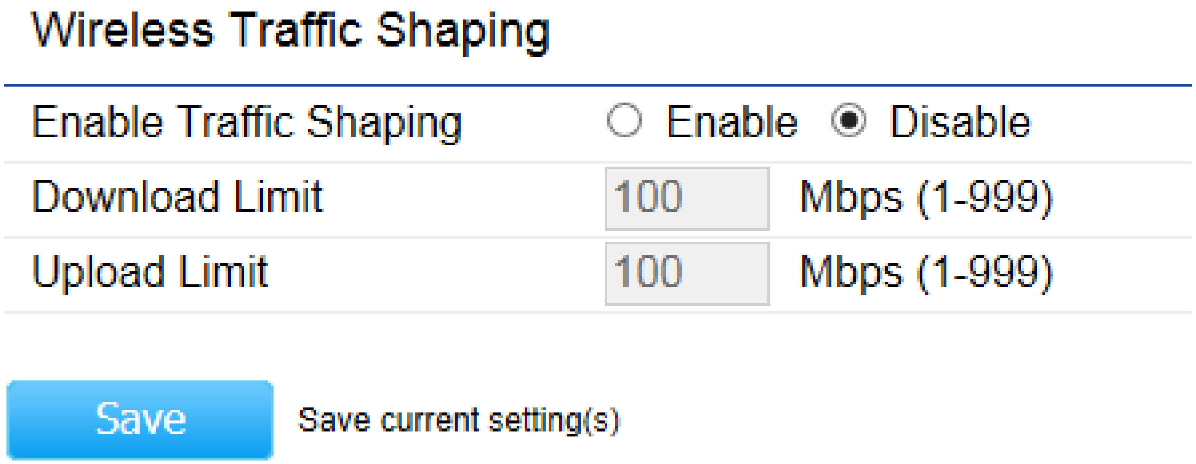
Click **Add** to add the MAC address to the MAC Address table.

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 Mbps (1-999)
Upload Limit	100 Mbps (1-999)

Enable Traffic Shaping
Select to enable or disable Wireless Traffic Shaping for the AP.

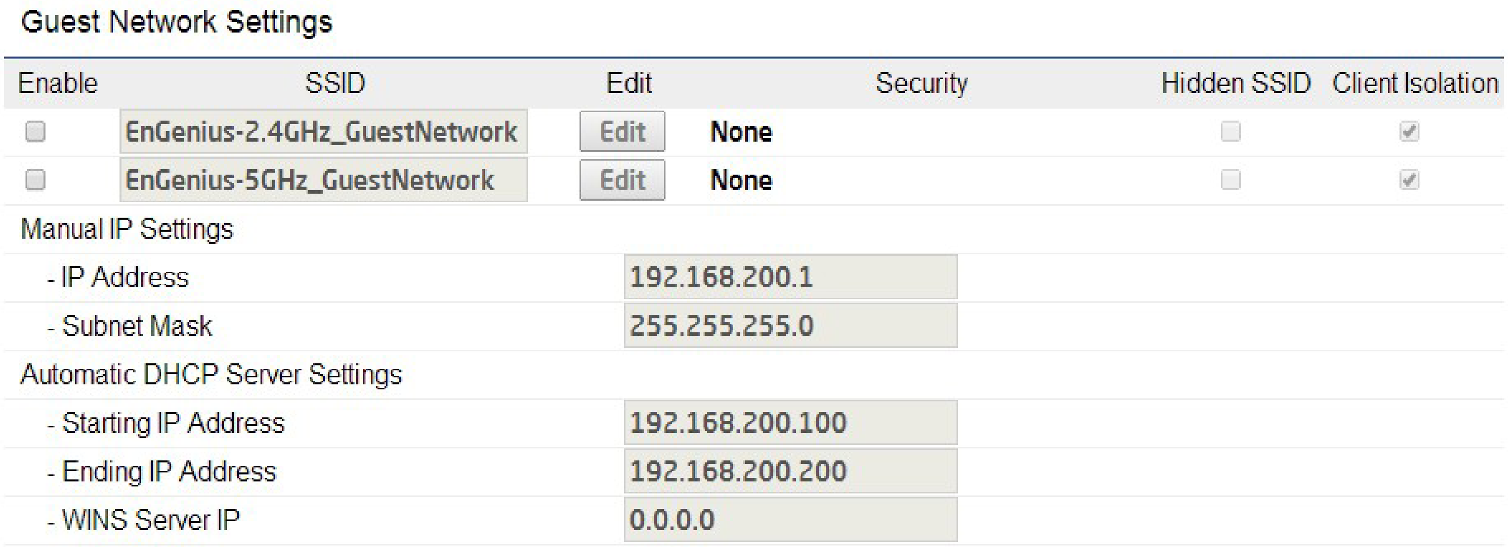
Download Limit
Specifies the wireless transmission speed used for downloading. The range is from 1~999 Mbps.

Upload Limit
Specifies the wireless transmission speed used for uploading. The range is from 1~999 Mbps.

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

Guest Network

The Guest Network feature 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_GuestNetwork	Edit	None	□	☑
□	EnGenius-5GHz_GuestNetwork	Edit	None	□	☑

Manual IP Settings	
- IP Address	192.168.200.1
- Subnet Mask	255.255.255.0
Automatic DHCP Server Settings	
- Starting IP Address	192.168.200.100
- Ending IP Address	192.168.200.200
- WINS Server IP	0.0.0.0

Enable SSID

Select to enable or disable SSID broadcasting.

SSID

Specifies 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.

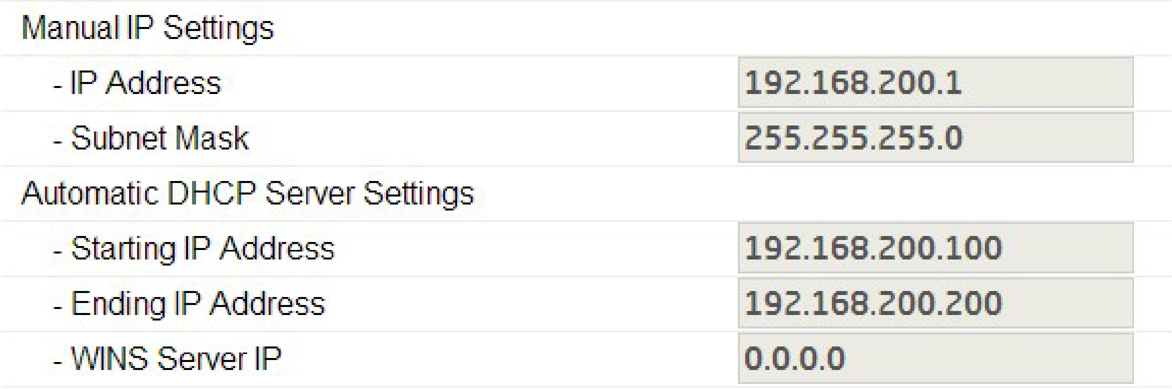
Hidden SSID

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 the Guest Network in the SSID Configuration page, assign an IP Address, Subnet mask and DHCP server IP address range.



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

Specifies an IP address for the Guest Network.

Subnet Mask

Specifies the the Subnet mask IP Address for the Guest Network.

Automatic DHCP Server Settings

Starting IP Address

Specifies the starting IP address range for the Guest Network.

Ending IP Address

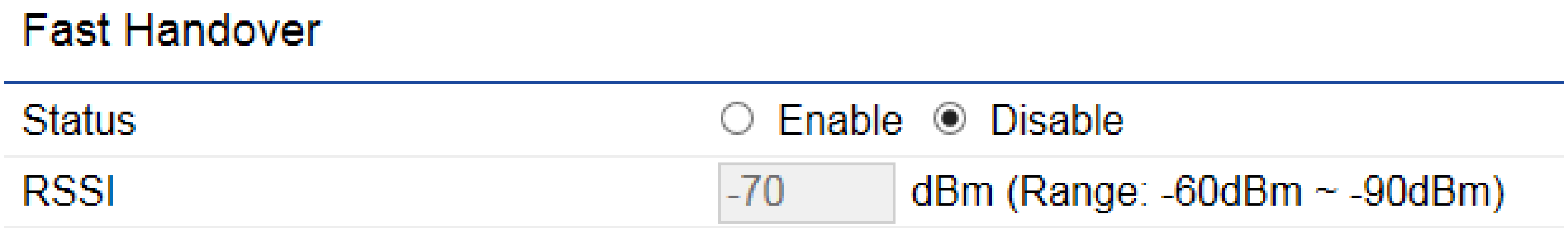
Specifies the ending IP address range for the Guest Network.

WINS Server IP

Specifies 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.

Fast Handover

With Fast Handover 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 as 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. The range is from -60dBm~-90dBm.

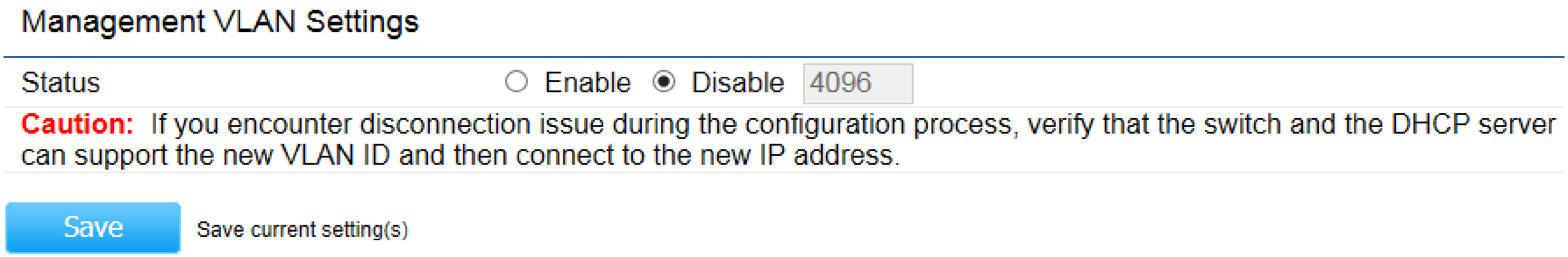


Fast Handover

Status	○ Enable ● Disable
RSSI	-70 dBm (Range: -60dBm ~ -90dBm)

Management VLAN Settings

This section allows you to assign a VLAN tag to 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**.

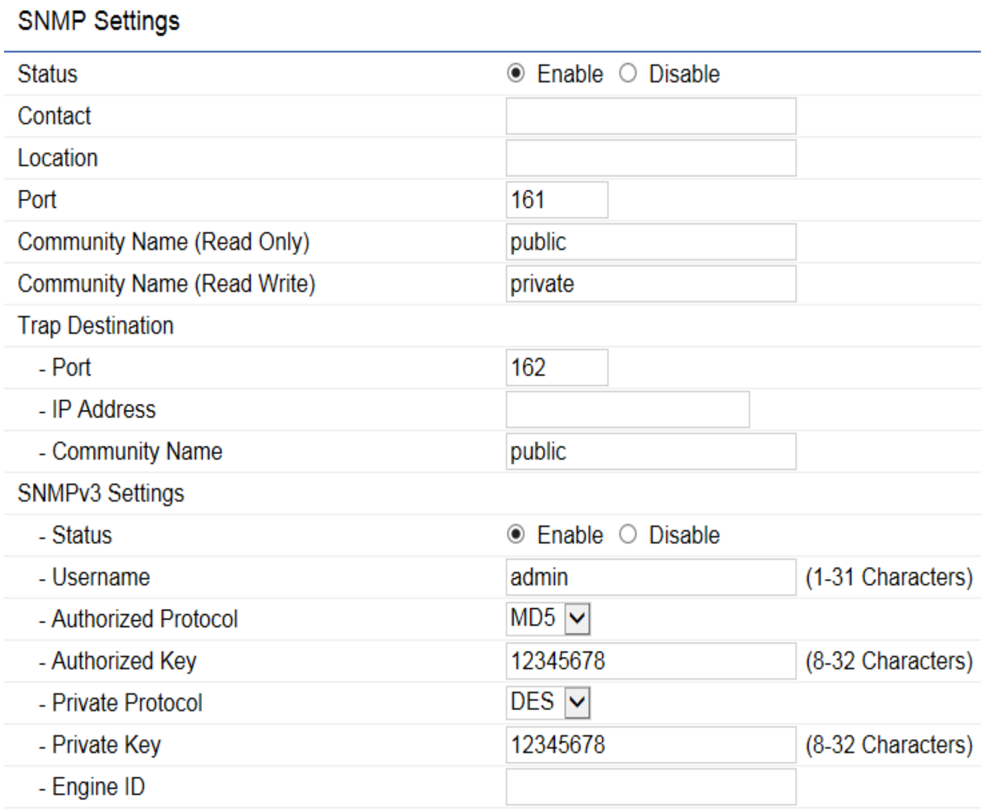
Save
Click **Save** to apply the changes.

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the AP. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the EWS AP 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 the **Advanced** under the **Management** section.



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 in use for the device.

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

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

Trap Destination Address
Specifies the port and IP address of the computer that will receive the SNMP traps. Traps in this context refer to or notifications used to advise an administrator.

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: **MD5** or **SHA**.

MD5: Message-Digest algorithm, a 128-bit typically expressed in text format as a 32 digit hexadecimal number.

SHA: Secure Hash Algorithm, a 160-bit hash value typically expressed in text format as a, 40 digits hexadecimal number.

Auth Key

Specifies the Authentication Key.

Priv Protocol

Select the Privacy Protocol type you wish to use: DES or None. DES stands for Data Encryption Standard, a symmetric-key algorithm for the encryption of electronic data.

Priv Key

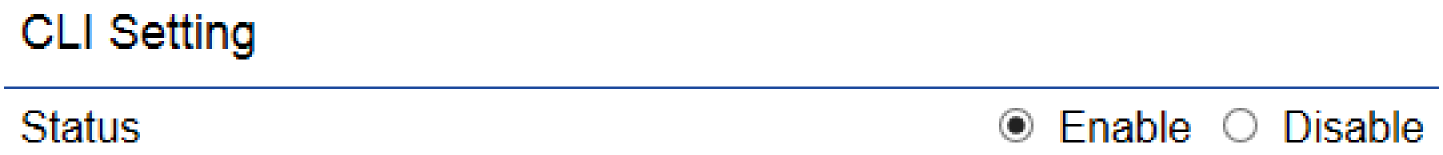
Specifies the privacy key.

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 a more secure connection, you can enable SSH (Secure Shell) to establish a secure data communication.

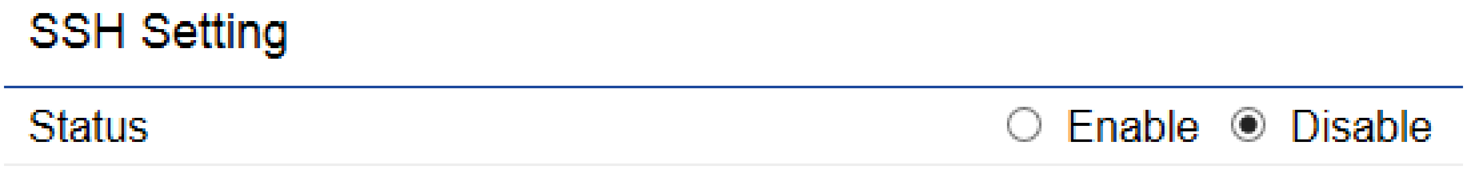


CLI Setting

Status ● Enable ○ Disable

CLI Status

Select to enable or disable the ability to modify the AP via the command line interface (CLI).



SSH Setting

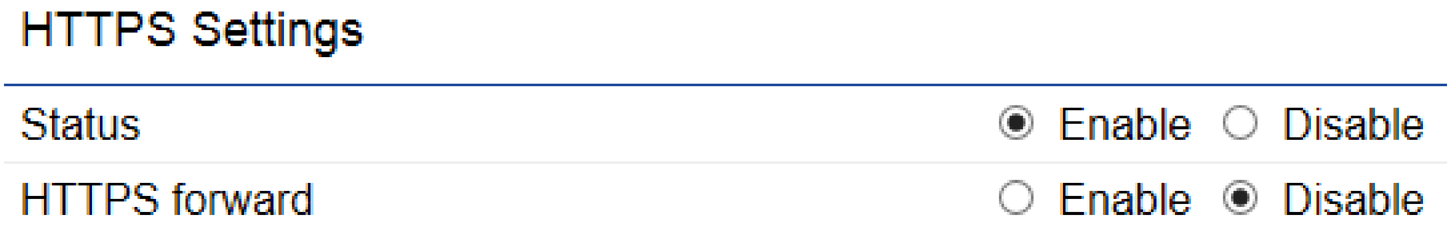
Status ○ Enable ● Disable

SSH Status

Select to enable or disable the ability to modify the AP 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; it is rather 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

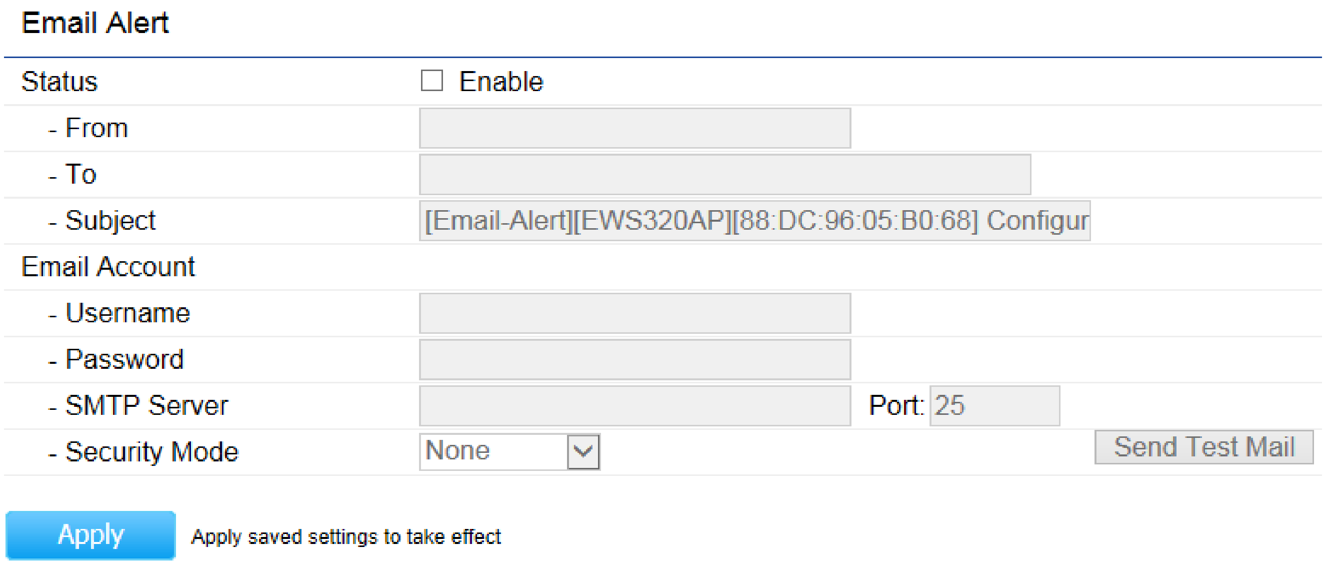
Status	● Enable ○ Disable
HTTPS forward	○ Enable ● Disable

Status
Select to enable or disable the ability to modify the AP via HTTPS.

HTTPS forward
When this option is enabled, the HTTP service will be forwarded to HTTPS if the user uses HTTP to access the AP.

Email Alerts

The Access Point will send email alerts when the AP's settings have been changed for your convenience.



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	

Apply saved settings to take effect

Status
Check to enable the Email Alert feature.

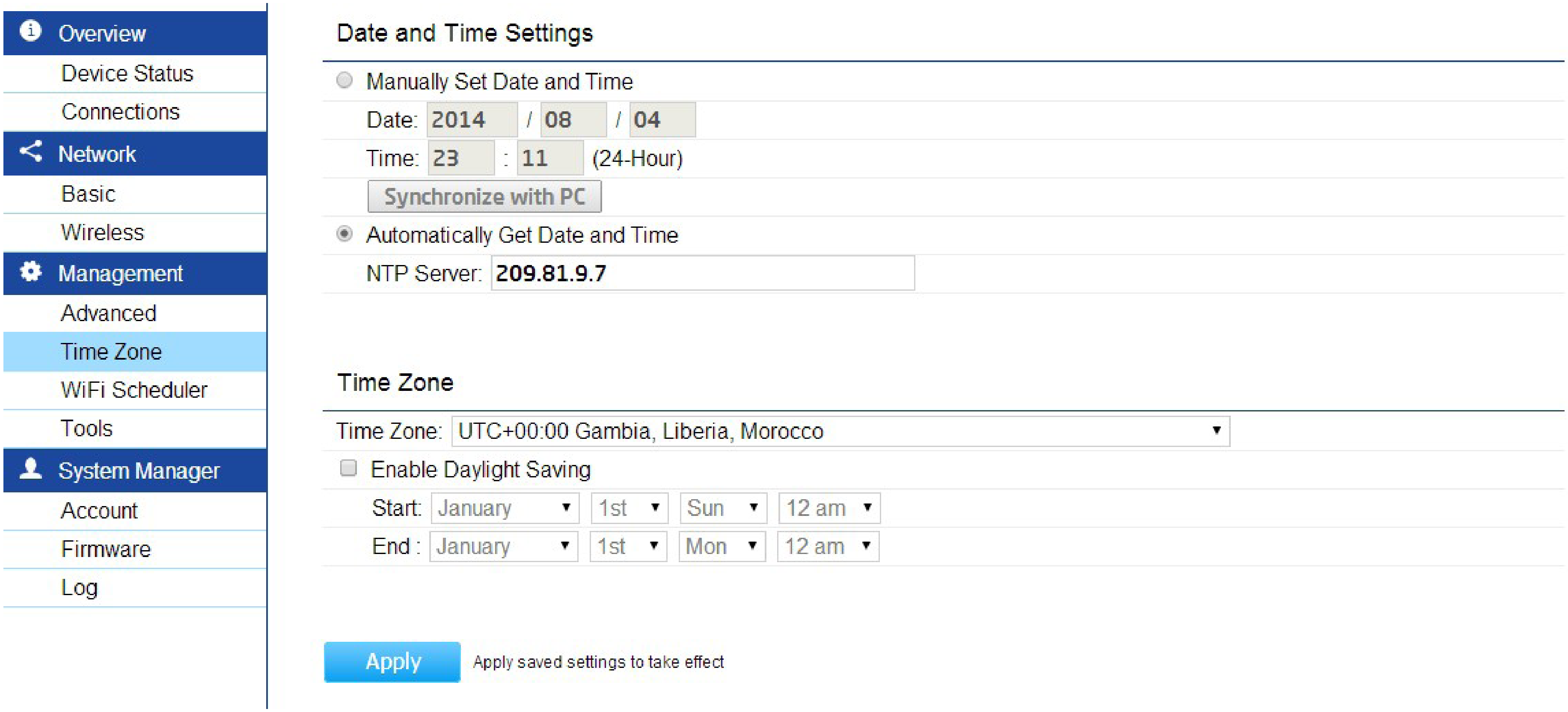
From
Enter the sender address you would like to use.

To
Enter the recipient address.

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

Date and Time Settings

This page allows you to set the internal clock for the AP. To access the Date and Time settings, click **Time Zone** under the **Management** section.



Date and Time Settings

○ Manually Set Date and Time

Date: 2014 / 08 / 04

Time: 23 : 11 (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 AP with the computer's internal clock.

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.

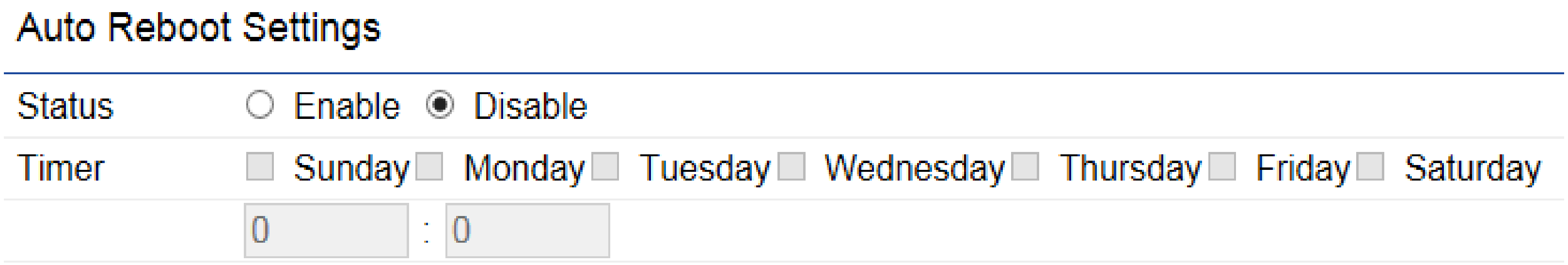
Time Zone
Choose the time zone you would like to use from the drop-down list.

Enable Daylight Savings
Check the box to enable or disable daylight savings time for the AP. Next, enter the dates that correspond to the present year's daylight savings start and end times.

Click **Apply** to save the changes.

Auto Reboot Settings

You can specify how often you would like to reboot the AP.



Auto Reboot Settings

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

Status

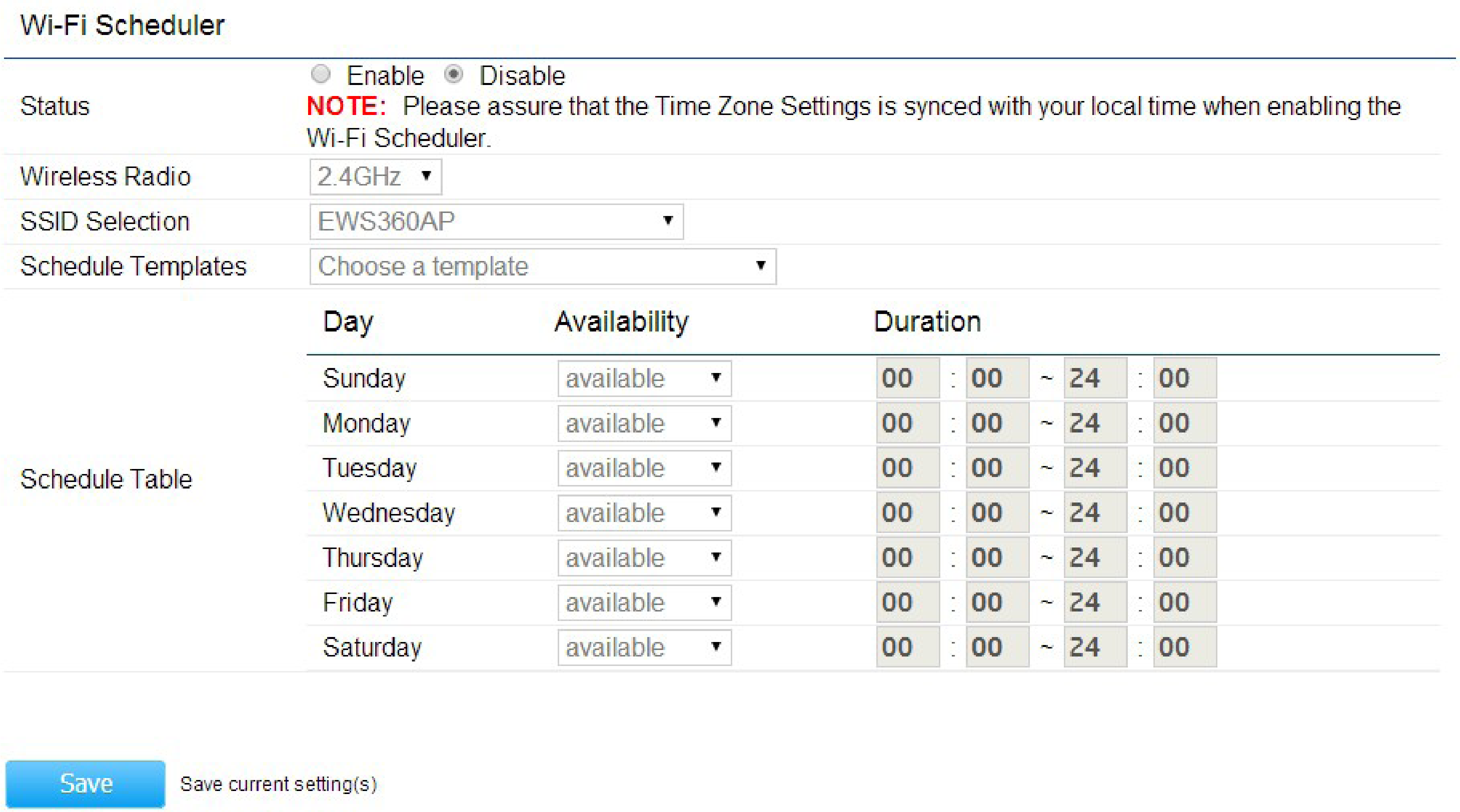
Enables or disables the Auto Reboot feature.

Timer

Specifies the time and frequency in rebooting the AP by Min, Hour and Day.

Wi-Fi Scheduler

Use the Scheduler feature to reboot the AP or control the wireless availability of the AP on a routine basis. The Scheduler feature relies on the GMT time setting acquired from a Network Time Protocol (NTP) server. For details on how to connect the AP to an NTP server, see **Date and Time Settings** on the previous page.



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	EWS360AP
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 current setting(s)

Status
Enables or disables the Wi-Fi Scheduler feature.

Wireless Radio
Select **2.4 GHz** or **5 GHz** to use the Wi-Fi Scheduler feature on that particular frequency band.

Note: 5 GHz options are not available for the **EWS210AP** model.

SSID Selection
Select a SSID to use for the Wi-Fi Scheduler feature.

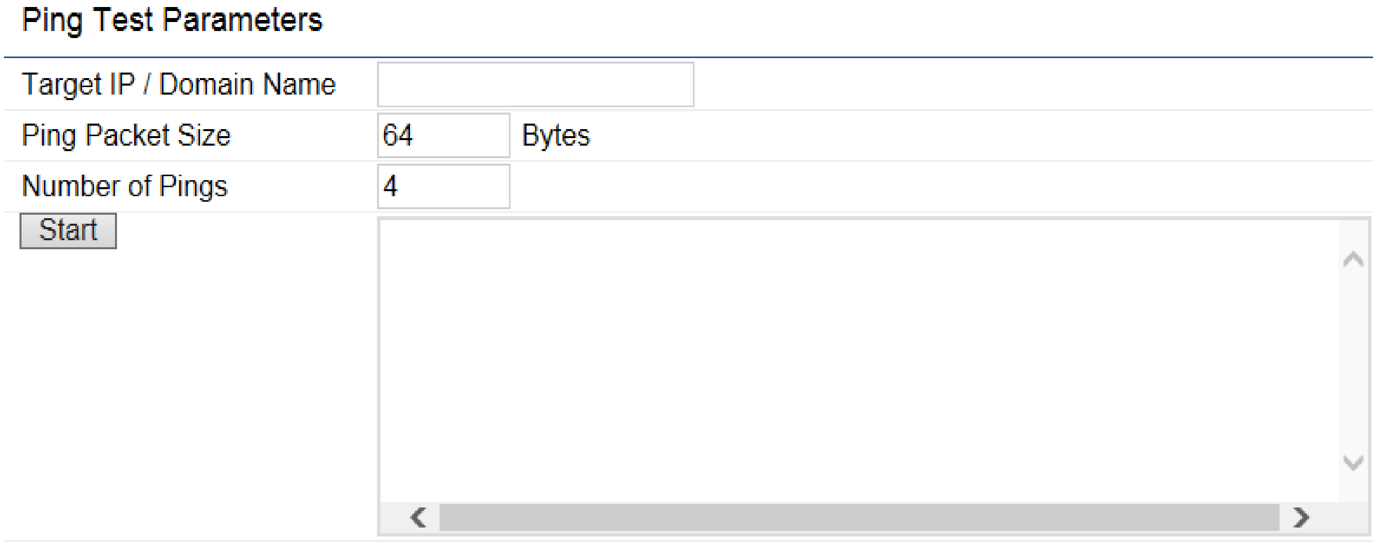
Schedule Templates
The AP provides three templates for your convenience: **Always available**, **Available 8-5 daily**, and **Available 8-5 daily except weekends**. Select **Custom Schedule** if you wish to set the schedule manually.

Schedule Table
Enables the schedule to be set manually.

Tools

This section allows you to analyze the connection quality of the AP 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 use for the target.

Ping Packet Size

Enter the packet size of each ping.

Number of Pings

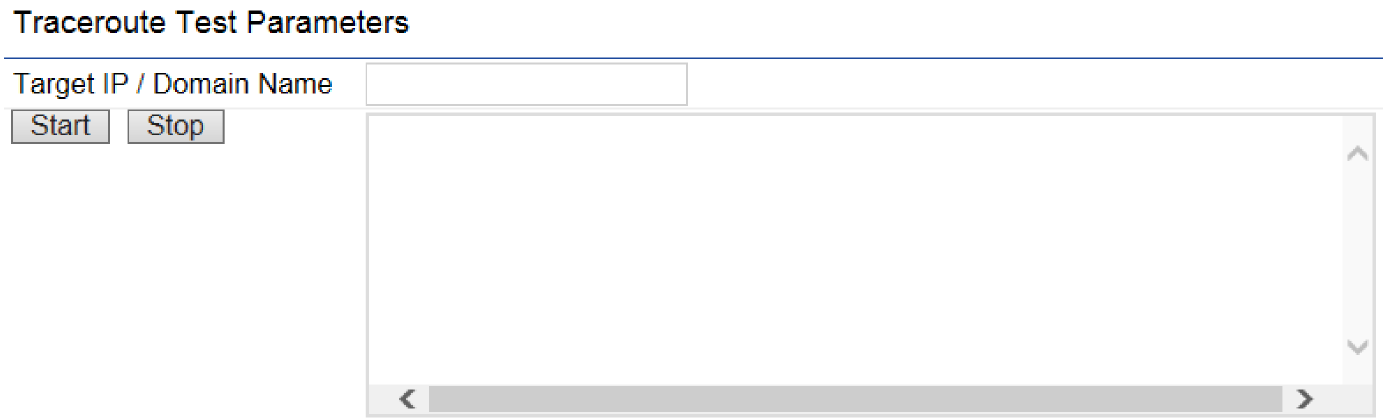
Enter the number of times you wish to ping.

Start

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

Traceroute Parameters

A Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. A Traceroute Test can be run to discern if there are any packet delays across the network.


Traceroute Test Parameters

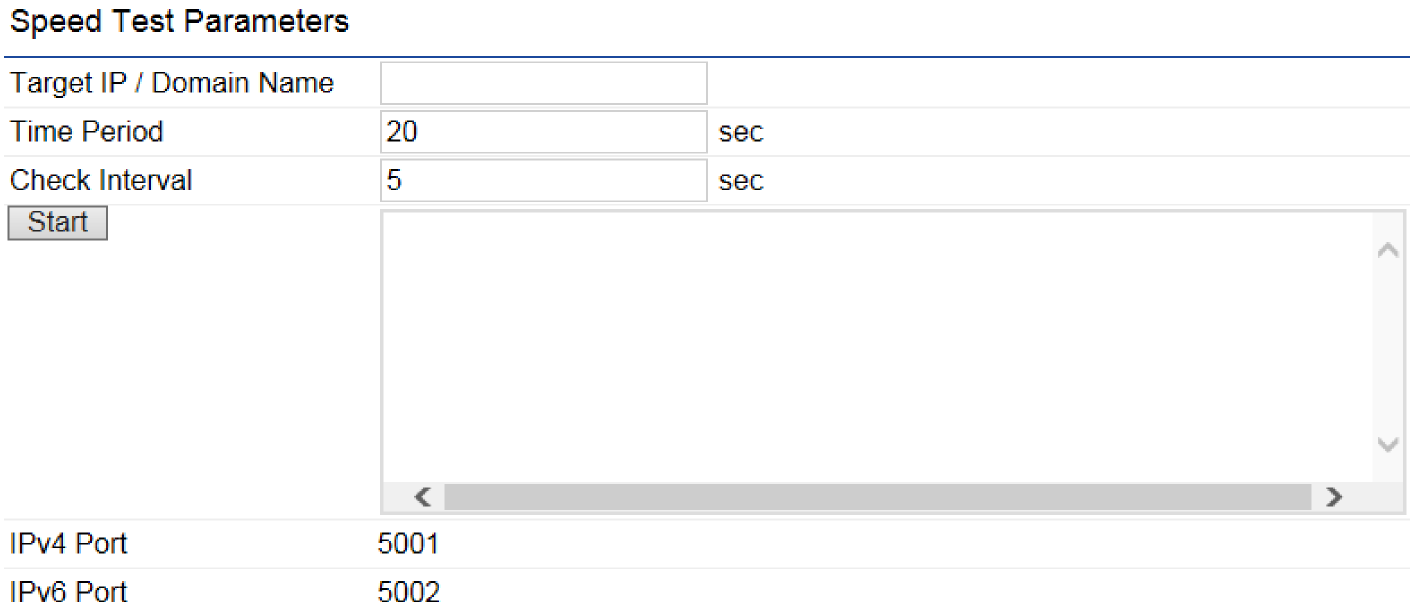
Target IP / Domain Name

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

Start
Click **Start** to begin the traceroute test.

Stop
Click **Stop** to halt 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 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

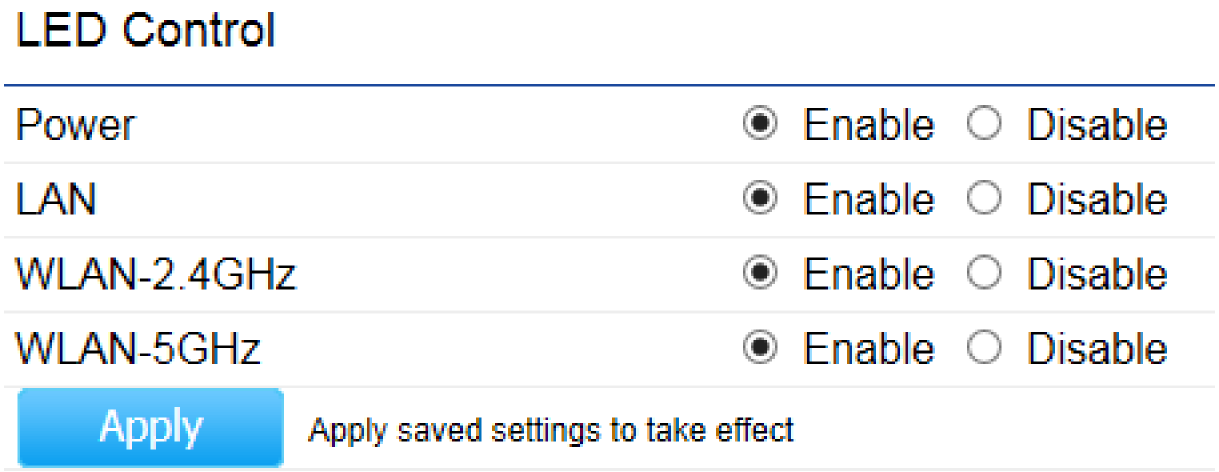
Click to start the Speed Test.

IPv4/IPv6 Port

The AP uses IPv4 port **5001** and IPv6 port **5002** for the speed test.

LED Control

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



LED Control

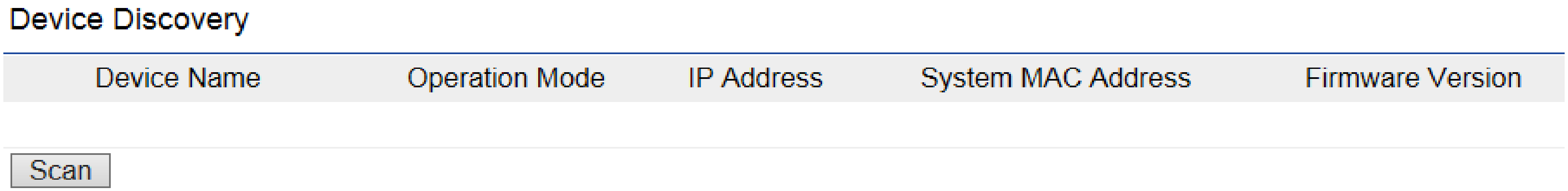
Power	● Enable	○ Disable
LAN	● Enable	○ Disable
WLAN-2.4GHz	● Enable	○ Disable
WLAN-5GHz	● Enable	○ Disable

Apply saved settings to take effect

Note: The 5 GHz WLAN LED interface option is not applicable for the EWS210AP.

Device Discovery

Under Device Discovery, you can choose for the AP to automatically scan for local devices to connect to. Click **Scan** to begin the process.



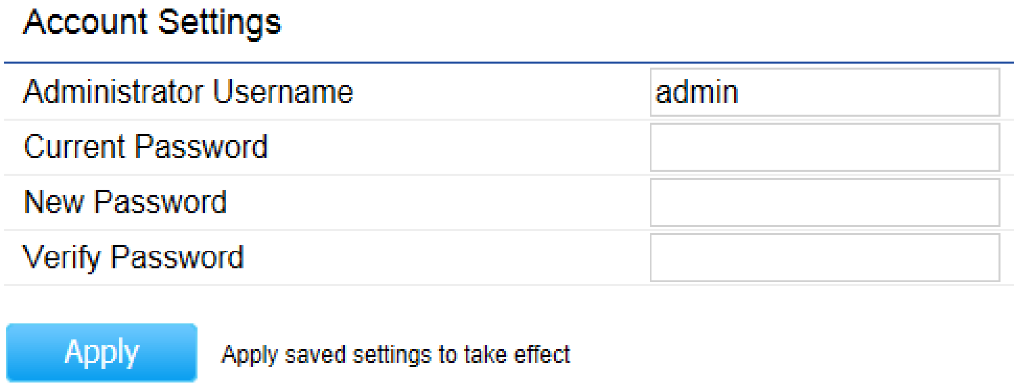
Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

Chapter 8
Maintenance

Account Settings

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



Account Settings

Administrator Username	admin
Current Password	
New Password	
Verify Password	

Apply   Apply saved settings to take effect

Administrator Username

Enter a new username in the entry field.

Current Password

Enter the old password in the entry field.

New Password

Enter a new password in the entry field.

Verify Password

Re-enter the new password for confirmation.

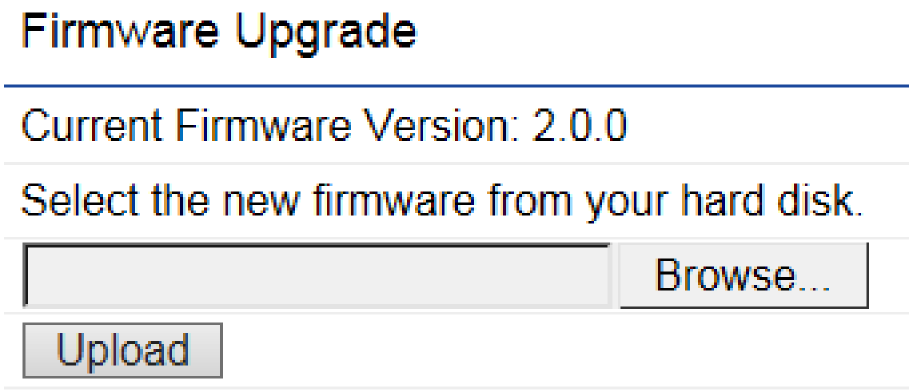
Apply

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 EWS AP. Please visit **www.engeniustech.com** to see the most current firmware version available for your model.



Firmware Upgrade

Current Firmware Version: 2.0.0

Select the new firmware from your hard disk.

To Perform a Firmware Upgrade:

1. Click the **Browse...** button and navigate the OS File System to the location of the Firmware upgrade file.

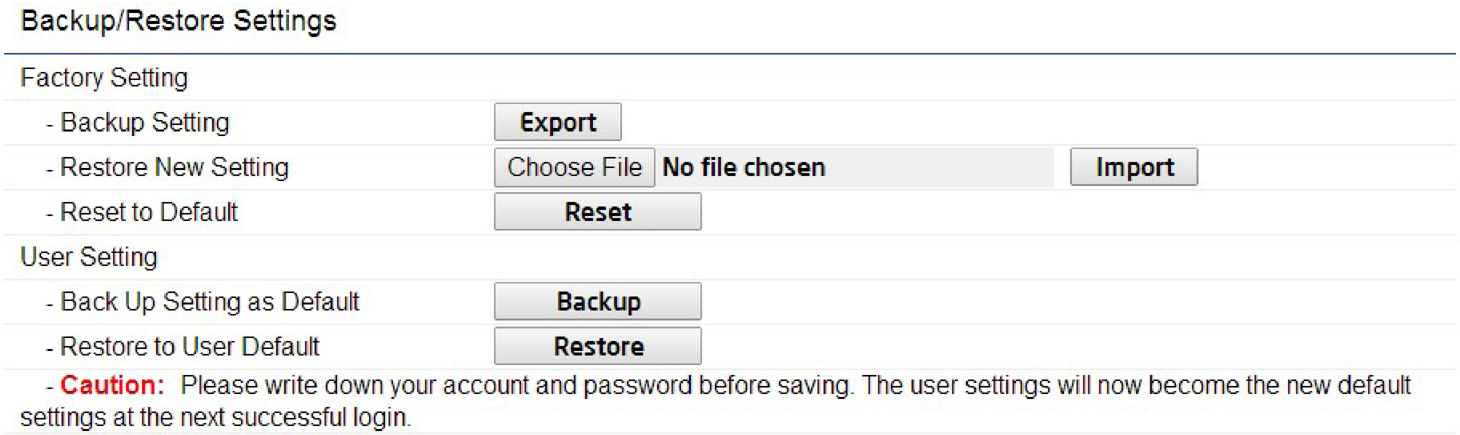
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.

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 current setting configurations for the device. When you save the configurations, you can also reload the saved configurations into the device through the Restore New Settings feature from a file folder. If extreme problems occur, or if you have set the AP incorrectly, you can use the Reset button in the Reset to Default section to restore all the configurations of the EWS AP to its original default settings. To Configure the Backup/Restore Settings, click **Firmware** under the Systems Manager section.



Backup/Restore Settings

Factory Setting		
- Backup Setting	Export	
- Restore New Setting	Choose File No file chosen	Import
- Reset to Default	Reset	
User Setting		
- Back Up Setting as Default	Backup	
- Restore to User Default	Restore	

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

Factory Settings

Backup Settings

Click **Export** to save the current device configurations to a folder.

Restore New Settings

Choose the file you wish restore and click **Import**.

Reset to Default

Click the **Reset** button to restore the EWS AP to its factory default settings.

User Settings

Backup Settings as Default

Click **Backup** to backup any user account default settings for the AP to a file folder.

Restore to User Default

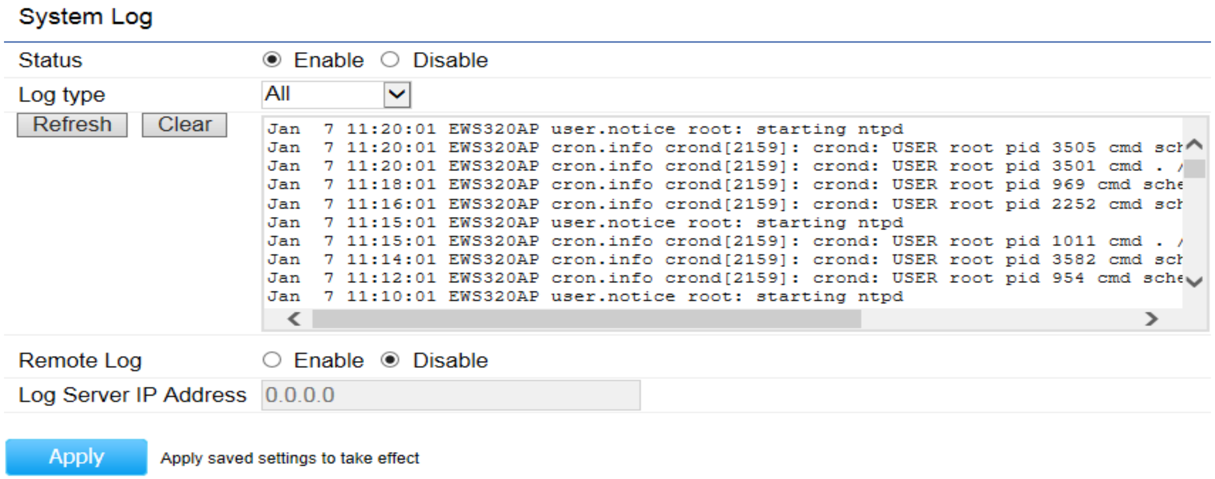
Click Restore to return to factory default user account settings for the AP.

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

Log

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

System Log



System Log

Status ● Enable ○ Disable

Log type: All

```
Jan  7 11:20:01 EWS320AP user.notice root: starting ntpd
Jan  7 11:20:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3505 cmd sch
Jan  7 11:20:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3501 cmd . /
Jan  7 11:18:01 EWS320AP cron.info crond[2159]: crond: USER root pid 969 cmd sche
Jan  7 11:16:01 EWS320AP cron.info crond[2159]: crond: USER root pid 2252 cmd sch
Jan  7 11:15:01 EWS320AP user.notice root: starting ntpd
Jan  7 11:15:01 EWS320AP cron.info crond[2159]: crond: USER root pid 1011 cmd . /
Jan  7 11:14:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3582 cmd sch
Jan  7 11:12:01 EWS320AP cron.info crond[2159]: crond: USER root pid 954 cmd sche
Jan  7 11:10:01 EWS320AP user.notice root: starting ntpd
```

Remote Log ○ Enable ● Disable

Log Server IP Address: 0.0.0.0

Apply saved settings to take effect

Status

Enables or disables the System Log feature.

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

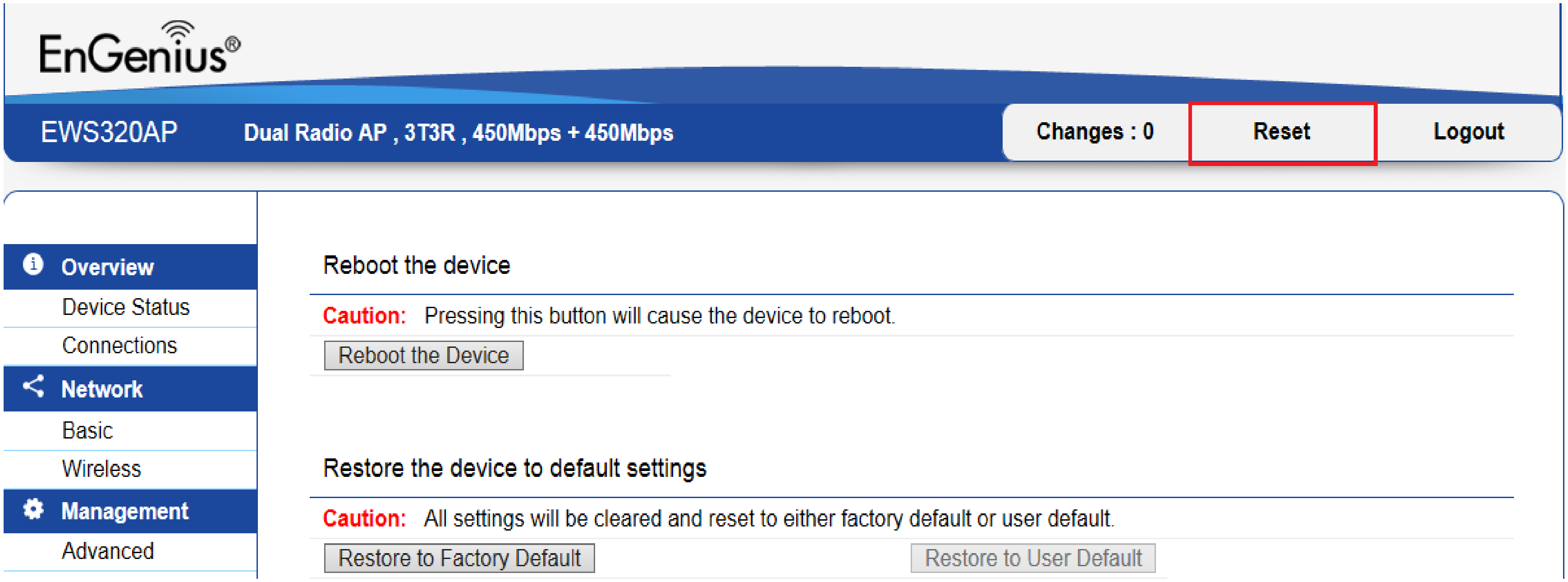
Enter the IP address of the log server.

Apply

Click **Apply** to save the changes.

Reset

In some circumstances, you may be required to force the device to reset. Click on **Reboot the Device** to reboot the Access Point. If an issue arises that you need to restore the AP to its original factory default settings and configurations, click on **Restore to Factory Default**. Please note that this will erase any custom configurations. To save time on restoring the device to a customized setup after a reset, refer to page 88 on how to backup these configurations to a file folder on your computer for later use.



Reboot the device

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

Reboot the Device

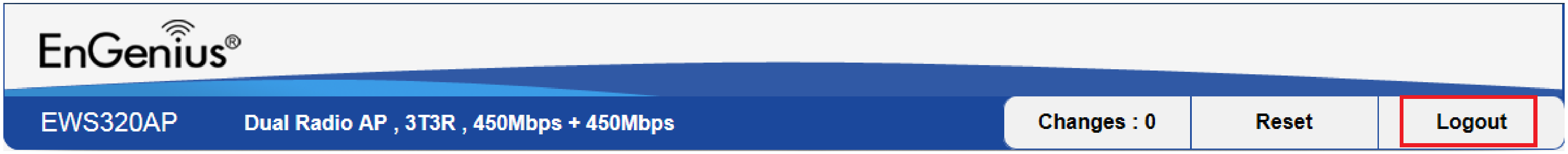
Restore the device to default settings

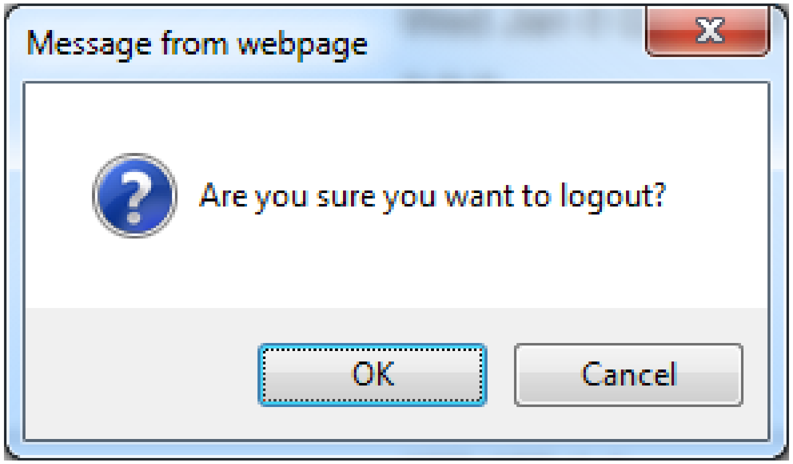
Caution: All settings will be cleared and reset to either factory default or user default.

Restore to Factory Default   Restore to User Default

Logout

To logout of your account, click **Logout**. A warning window will pop up to confirm your choice. Click **OK** to logout.




Message from webpage

Are you sure you want to logout?

Glossary

6to4	6to4 allows IPv6 packets to be transmitted over an IPv4 network.
ACL	The Access Control List specifies which users or processes are granted access to objects, as well as which operations are allowed.
Access Point Mode	In Access Point mode, the EPG600 allows wireless devices to connect to a wired network using Wi-Fi, or other related standards. You can choose to have the router associate only with certain iterations (IEEE standards) and by doing so this will either positively or negatively affect the router's speed and throughput performance.
AES	An Advanced Encryption Standard is an encryption algorithm. You can chose 128, 192 or 256-bit long key size for encryption and decryption of text.
ALG	Application Layer Gateway serves as a window between correspondent application processes so that they may exchange information on an open environment.
Backup	A copy of a set of files made for replacement purposes in case the original set is damaged or lost.
Bandwidth	Bandwidth refers to the information-carrying capacity of a network or component of a network expressed in bits per second.
Bit Rate	The rate at which bits are transmitted or received during communication, expressed as the number bits in a given amount of time, usually one second.
Boot	A computer's startup operation.
Community String	A text string that acts as a password and is used to authenticate messages sent between a management station and a router containing a SNMP agent. The community string is sent in every packet between the manager and the agent.
Default Gateway	A Deafult Gateway is the device that passes traffic from the local subnet to devices on other subnets. It is usually the IP address of the router to which your network is connected.
DES	A Data Encryption Standard is an encryption type that enhances the encryption capabilities of SNMP version 3.
DDNS	Dynamic Domain Name Service (DDNS) allows for an Internet domain name to be assigned to a computer with a varying (dynamic) IP address.
DHCP	The Dynamic Host Cnfiguation protocol is used for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
DLNA	The Digital Living Network Alliance DLNA is a nonprofit collaborative trade organization that is responsible for defining interoperability guidelines to enable the sharing of digital media between multimedia devices. Some HDTVs, Gaming Consoles, and other media devices adhere to DLNA guidelines.

DNS	A Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. This allows the recognition of domain names such as www.yahoo.com instead of 98.139.183.24, which is more difficult to remember.
Domain	A portion of the spanning hierarchy tree that refers to general groupings of networks based on organization type or geography.
DoS	Denial of Service is an interruption in an authorized user's access to a computer network and is typically caused with malicious intent. Although the process and targets of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to a network.
Download	The transfer of a file from a remote computer to a local computer.
Dynamic IP	An IP address that is assigned and changed periodically. Dynamic IP addresses can change each time you connect to the Internet, while static IP addresses are reserved for you statically and don't change over time.
Encryption	The application of a specific algorithm to data so as to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.
Firewall	A router or access server, or several routers or access servers designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
Firmware	A collection of programmed routines and instructions that is implemented in a computer chip or similar hardware form instead of a software form. Please check www.engeniustech.com for firmware updates.
FTP	An application protocol that uses the TCP/IP protocols. It is used to exchange files between computers/devices on networks.
Gateway	A gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway,and a Switch, which furnishes the actual path in and out of the gateway for a given packet.
Guest Network	A guest network is a section of an computer network designed for use by temporary visitors. This subnetwork often provides full Internet connectivity, but also strictly limits access to any internal Web sites or files.

GUI	Graphical User Interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored.
IGMP	The Internet Group Multicast Protocol is a protocol that provides the means for a host to inform its attached router that an application running wants to join a specific multicast group.
IP	The Internet Protocol is a method transmitting data over a network. Data to be sent is divided into individual and completely independent "packets." Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender's address and the receiver's address. The Internet Protocol ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, (which means that there is no established connection between the communication end-points) packets can be sent via different routes and do not need to arrive at the destination in the correct order. Once the data packets have arrived at the correct destination, another protocol, Transmission Control Protocol (TCP) puts them in the right order.
IP Address	An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and to pass data back and forth. To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed, so that it does not change, or it can be assigned dynamically (and automatically) by DHCP. An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. One part represent the network number or address, and other part represents the local machine address.
IPv6	IPv6 provides an identification and location system for computers on networks and routes that traffic across the Internet.
L2TP	The Layer 2 Tunneling Protocol is used to support VPNs or as part of the delivery of services by ISPs.
LAN	A communication infrastructure that supports data and resource sharing within a small area that is completely contained on the premises of a single owner.
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.
MAC Address Filtering	Mac Address Filtering permits and denies network access to specific devices based on a device's MAC address.
MD5	A Message-Digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number.

Mesh Mode	Mesh Networks are a network topology in which each node (called a mesh node) relays data for the network. All nodes cooperate in the distribution of data in the network. In the event that a node fails, other nodes can automatically reconfigure or “fill in“ for another Wireless AP in the network (called Self-healing) and pickup a signal that otherwise would have been dropped.
MTU	Maximum Transmission Unit. A specification in a data link protocol that defines the maximum number of bytes that can be carried in any one packet on that link.
NAT	Network Address Translation is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NTP Sevrer	The Network Time Protocol is used for clock synchronization between computer systems.
Packet	A discrete chunk of communication in a pre-defined format.
Port Forwarding	Port Forwarding allows remote computers to connect to a specific computer or service within a private LAN.
Port Mapping	Port Mapping allows you to redirect a particular range of service port numbers from the WAN to a particular LAN IP address.
Port Triggering	Port Triggering lets you map a local port or range of ports to a specific public port. Sending packets out over the local port triggers the router to open an incoming local port that is mapped to the same public port and application as the outgoing local port(s). The local application can communicate over the incoming and outgoing ports without the need for creating a fixed address.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. PPPoE can be used to have an office or building-full of users share a common DSL, cable modem, or wireless connection to the Internet.
PPTP	A protocol that allows corporations to extend their own corporate network through private “tunnels” over the public Internet. In this way a corporation can effectively use a WAN as a large single LAN.
Priority Queue	A Priority queue is a queue where an element with a high priority is served before an element with low priority. If two elements happen to have the same priority, they are served according to their order in the queue.
QoS	Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. It is espcially important for applications like multimedia streaming and VoIP.
RADIUS	Remote Authentication Dial In User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for users that connect and use a network service.

RAM	Random Access Memory. A group of memory locations that are numerically identified to allow high speed access by a CPU. In random access, any memory location can be accessed at any time by referring to its numerical identifier as compared to sequential access, where memory location 6 can only be accessed after accessing memory locations 1-5.
Reboot	A user activity where the user starts a computing device without interrupting its source of electrical power.
Router	A device that determines the next network point to which a packet should be forwarded to on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network Switch.
Server	In general, a server is a computer program that provides services to other computer programs within the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. A web server is the computer program that supplies the requested HTML pages or files to the client (browser).
SHA	A Secure Hash Algorithm produces a 160-bit (20-byte) hash value typically rendered as a hexadecimal number, 40 digits long.
Static IP	An IP address that is unchanging. It is more reliable when dealing with VoIP, online gaming, and VPNs.
SSID	A Service Set Identifier is a set consisting of all the devices associated with a WLAN.
Subnet Mask	A representation of a user's Internet address where all of the bit positions corresponding to the user's network and subnetwork id are 1's and the bit corresponding to the user's host id are 0's.
Throughput	Rate of information arriving at, and possibly passing through, a particular point in a network system.
Time-Out	Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. The resulting time-out usually results in a re-transmission of information or the dissolving of the session between the two devices.
TKIP	Temporal Key Integrity Protocol is a stopgap security protocol used in IEEE 802.11 wireless networking standards used to replace WEP.
UID	A Unique Identifier is a unique reference number used as an identifier.
Upload	The activity of transferring a file from a user's computer system to a remote system.
UPnP	Universal Plug n Play is a protocol that permits networked devices to seamlessly discover each other's presence on the network.

VLAN	A Virtual Local Area network allows a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together.
VoIP	Voice over IP is a technology used for the delivery of voice communications and multimedia sessions over IP networks rather than a PSTN line.
VPN	A Virtual Private Network creates a secure "tunnel" between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. The VPN network can be within a company LAN (Local Area Network), but different sites can also be connected over the Internet in a secure way. One common use for VPN is for connecting a remote computer to the corporate network, via e.g. a direct phone line or the Internet.
VPN Tunnel	VPN Tunneling is a link which connects a network directly to another network. The connection between the complementary links is called a VPN tunnel VPN comprises with a VPN server and a VPN client. A VPN client is usually a software program which can be configured to the VPN server.
WAN	A Wide Area Network is a network that covers a broad area over long distances using private or public network transports between different LANs, MANs and other localised computer networking architectures.
WDS Mode	Wireless Distribution System Mode is a MAC address-based system enabling the wireless interconnection of Access Points in an IEEE 802.11 network.
WEP	Wired Equivalent Privacy is a is a security protocol for wireless networks that encrypts transmitted data.
WLAN	A Wireless LAN is a LAN that links two or more devices using some wireless distribution method. This gives users the ability to move around within a local coverage area and still be connected to the network.
WOL	Wake on LAN allows a computer to be turned on or awakened by a network message.
WPA /WPA2	Wi-Fi Protected Access and Wi-Fi Protected Access II are security protocols and security certification programs used to secure wireless computer networks. They are reccomended over WEP.

Appendix

Professional Installation Instruction

1. Installation Personnel
This product is designed for specific application and needs to be installed by a qualified personnel who has RF and related rule knowledge. The general user shall not attempt to install or change the settings.

2. Installation Location
The product shall be installed at a location where the radiating antenna can be kept at least **23cm** from nearby persons in normal operating conditions to meet regulatory RF exposure requirement.

3. Installation Procedure
Please refer to the user's manual for details.

4. Warning!
Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of this rule could lead to serious federal penalties.

Instructions D’installation Professionnelle

1. Installation

Ce produit est destine a un usage specifique et doit etre installe par un personnel qualifie maitrisant les radiofrequences et les regles s’y rapportant. L’installation et les reglages ne doivent pas etre modifies par l’utilisateur final.

2. Emplacement D’installation

En usage normal, afin de respecter les exigences reglementaires concernant l’exposition aux radiofrequences, ce produit doit etre installe de facon a respecter une distance de **23cm** entre l’antenne emettrice et les personnes.

3. Procedure D’installation

Consulter le manuel d’utilisation.

4. Avertissement!

Choisir avec soin la position d’installation et s’assurer que la puissance de sortie ne depasse pas les limites en vigueur. La violation de cette regle peut conduire a de serieuses penalites federales.

Appendix A

Federal Communication Commission Interference Statement

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

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

WARNING!

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 fol- lowing 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.

Radiation Exposure Statement

WARNING! This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 23cm 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.

Appendix C - CE Interference Statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **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

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

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

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

CE 0560 (!)

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

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