EWS Wireless Management Switch

User Guide

V1.0.0

EWS2910P
EWS5912FP
EWS7928P
EWS7928FP
EWS7952FP

Table of contents

Product Overview

Introduction

The EnGenius EWS Series of Wireless Management Switches is an affordable centralized wired/wireless management system developed specifically for entry-level small-to-medium businesses. This powerful device can be easily deployed and operated by non-tech experts and installed effortless and quickly. Any organization with limited IT engineer and budget can create a stable and secure wireless network in no time. The system integrates seamlessly with existing routers, switches, firewalls, authentication servers and other network devices, and can be placed within any network, configured to act as a both a Wireless Controller as well as a Layer 2 PoE Gigabit switch, providing robust and centralized management of the whole network through one powerful system. With no additional costs or license purchasing necessary, network administrators can manage and monitor both wired and wireless nodes through a single web interface.

The system can automatically discover any supported EnGenius EWS Series Access Points connected to the network with a simple click of a mouse, self-configure and become instantly manageable. Simply log into the device via any standard web browser and assign APs into cluster groups. Wireless radio, wireless security and other wireless related configurations can all be easily applied to multiple APs simultaneously, eliminating the time consuming process of configuring each and every Wireless Access Points individually. The user friendly GUI provides instant access to a variety of client and network information including Managed AP List, Auto Discovered AP List, Cluster Grouping List, and Client List with complete MAC/IP Address, Incoming/Outgoing Traffic, Wireless Output Power and other relevant information. Statistics of AP and client traffics are automatically generated into easy-to-understand graphs, providing a visual representation of the network traffic. Not to forget the Topology View feature that allows administrators to quickly see the whole wired/wireless network topology at real-time for easier planning, troubleshooting and monitoring, as well as Floor Plan View and Map View which allows for quickly locating deployed APs, a helpful feature for large scale AP deployment and multi-site management. There's also an Intelligent Diagnostics feature for administrators to check the status of Wireless APs and provide easy troubleshooting for offline units and even capable of rebooting APs remotely.

Maximum data rates are based on IEEE 802.3ab 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: 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.

Package Contents

Your EnGenius EWS Switch package will contain the following items.*

For EWS5912FP / EWS7928P / EWS7928FP / EWS7952FP:

- EnGenius Switch
- Power Cord
- RJ45 Console Cable
- Rack Mount Kit
- Quick Installation Guide

For EWS2910P

- EnGenius Switch
- Power Adapter
- Power Cord
- Wall Mount Kit
- Ground Screw Set
- Quick Installation Guide

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

Technical Specifications

EWS2910P

General Features

- Switching Capacity: 20Gbps
- Forwarding Mode: Store and Forward
- SDRAM: 256MB
- Flash Memory: 32MB

Port Functions

- 10 10/100/1000Mbps Ports
- 2 100/1000Mbps SFP Slots

PoE Capability

- PoE Standard: supports IEEE 802.3af
- PoE Capable Ports: Port 1~8 output up to 15W
- Total PoE Power Budget: 61.6Watts

LED Indicators

- Device: Power LED, Fault LED, PoE Max LED, LAN Mode LED, PoE Mode LED
- Copper Ports: LAN/PoE Mode, Link/Act
- SFP Ports: Speed, Link/Act

Physical

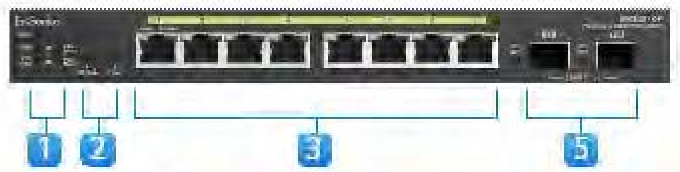
- Dimensions (W x D x H): 240 x 105 x 27 mm (9.45 x 4.13 x 1.06 inches)
- Weight: 0.63kg (1.39lbs)

Environmental

- Operating Temperature: 0 ~ 40°C (32 ~ 104°F)
- Storage Temperature: -40 ~ 70°C (-40 ~ 158°F)
- Humidity: 5 ~ 95% non-condensing

Physical Interface

1. LED Indicators
2. Mode Selector & Reset button
3. PoE RJ45 Ethernet Ports
4. Dual-Speed SFP Slots



EWS5912FP

General Features

- Switching Capacity: 24Gbps
- Forwarding Mode: Store and Forward
- SDRAM: 256MB
- Flash Memory: 32MB

Port Functions

- 10 10/100/1000Mbps Ports
- 2 100/1000Mbps SFP Slots
- 1 RJ45 Console Port

PoE Capability

- PoE Standard: supports IEEE 802.3af/at
- PoE Capable Ports: Port 1~8 output up to 30W
- Total PoE Power Budget: 130Watts

LED Indicators

- Device: Power LED, Fault LED, PoE Max LED, LAN Mode LED, PoE Mode LED
- Copper Ports: LAN/PoE Mode, Link/Act
- SFP Ports: Speed, Link/Act

Physical

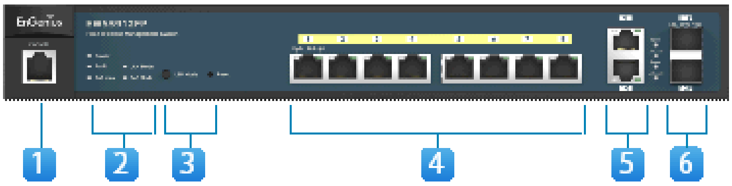
- Dimensions (W x D x H): 330 x 230 x 44 mm (13 x 9 x 1.73 inches)
- Weight: 1.996kg (4.4lbs)

Environmental

- Operating Temperature: 0 ~ 50°C (32 ~ 122°F)
- Storage Temperature: -40 ~ 70°C (-40 ~ 158°F)
- Humidity: 5 ~ 95% non-condensing

Physical Interface

1. RJ45 Console Port
2. LED Indicators
3. Mode Selector & Reset button
4. PoE RJ45 Ethernet Ports
5. RJ45 Ethernet Ports
6. Dual-Speed SFP Slots



EWS7928P

General Features

- Switching Capacity: 56Gbps
- Forwarding Mode: Store and Forward
- SDRAM: 256MB
- Flash Memory: 32MB

Port Functions

- 24 10/100/1000Mbps Ports
- 4 100/1000Mbps SFP Slots
- 1 RJ45 Console Port

PoE Capability

- PoE Standard: supports IEEE 802.3af/at
- PoE Capable Ports: Port 1~24 output up to 30W
- Total PoE Power Budget: 185Watts

LED Indicators

- Device: Power LED, Fault LED, PoE Max LED, LAN Mode LED, PoE Mode LED
- Copper Ports: LAN/PoE Mode, Link/Act
- SFP Ports: Speed, Link/Act

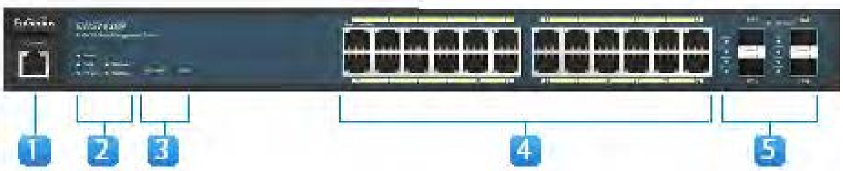
Physical

- Dimensions (W x D x H): 440 x 260 x 44mm (17.3 x 10.2 x 1.7 inches)
- Weight: 3.59kg (7.92lbs)

Environmental

- Operating Temperature: 0 ~ 50°C (32 ~ 122°F)
- Storage Temperature: -40 ~ 70°C (-40 ~ 158°F)
- Humidity: 5 ~ 95% non-condensing

Physical Interface
1. RJ45 Console Port
2. LED Indicators
3. Mode Selector & Reset button
4. PoE RJ45 Ethernet Ports
5. Dual-Speed SFP Slots



EWS7928FP

General Features

- Switching Capacity: 56Gbps
- Forwarding Mode: Store and Forward
- SDRAM: 256MB
- Flash Memory: 32MB

Port Functions

- 24 10/100/1000Mbps Ports
- 4 100/1000Mbps SFP Slots
- 1 RJ45 Console Port

PoE Capability

- PoE Standard: supports IEEE 802.3af/at
- PoE Capable Ports: Port 1~24 output up to 30W
- Total PoE Power Budget: 370Watts

LED Indicators

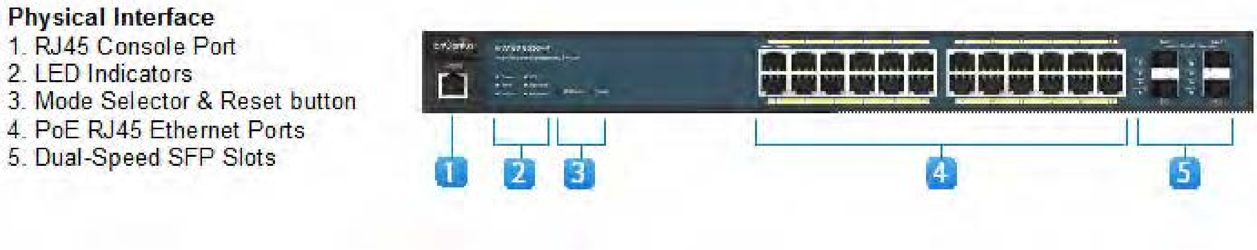
- Device: Power LED, Fault LED, RPS LED, PoE Max LED, LAN Mode LED, PoE Mode LED
- Copper Ports: LAN/PoE Mode, Link/Act
- SFP Ports: Speed, Link/Act

Physical

- Dimensions (W x D x H): 440 x 310 x 44mm (17.3 x 12.2 x 1.7 inches)
- Weight: 4.74kg (10.46lbs)

Environmental

- Operating Temperature: 0 ~ 50°C (32 ~ 122°F)
- Storage Temperature: -40 ~ 70°C (-40 ~ 158°F)
- Humidity: 5 ~ 95% non-condensing



Physical Interface

1. RJ45 Console Port
2. LED Indicators
3. Mode Selector & Reset button
4. PoE RJ45 Ethernet Ports
5. Dual-Speed SFP Slots

EWS7952FP

General Features

- Switching Capacity: 104Gbps
- Forwarding Mode: Store and Forward
- SDRAM: 256MB
- Flash Memory: 32MB

Port Functions

- 48 10/100/1000Mbps Ports
- 4 100/1000Mbps SFP Slots
- 1 RJ45 Console Port

PoE Capability

- PoE Standard: supports IEEE 802.3af/at
- PoE Capable Ports: Port 1~48 output up to 30W
- Total PoE Power Budget: 740Watts

LED Indicators

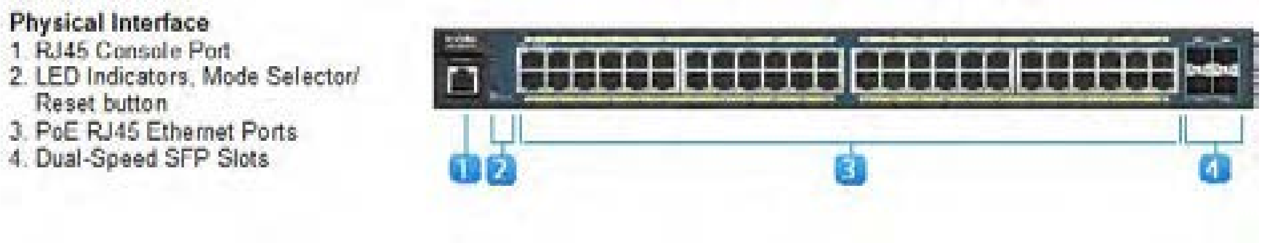
- Device: Power LED, Fault LED, PoE Max LED, LAN Mode LED, PoE Mode LED
- Copper Ports: LAN/PoE Mode, Link/Act
- SFP Ports: Speed, Link/Act

Physical

- Dimensions (W x D x H): 440 x 410 x 44mm (17.3 x 16.1 x 1.7 inches)
- Weight: 6.15kg (13.55lbs)

Environmental

- Operating Temperature: 0 ~ 50°C (32 ~ 122°F)
- Storage Temperature: -40 ~ 70°C (-40 ~ 158°F)
- Humidity: 5 ~ 95% non-condensing



Physical Interface

1. RJ45 Console Port
2. LED Indicators, Mode Selector/ Reset button
3. PoE RJ45 Ethernet Ports
4. Dual-Speed SFP Slots

Software Features

WLAN Management Features

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

L2 Switch Features

- VLAN Group
- Voice VLAN
- 802.3ad Link Aggregation
- 802.1D Spanning Tree (STP)
- 802.1w Rapid Spanning Tree (RSTP)
- 802.1s Multiple Spanning Tree (MSTP)
- Port Mirroring
- Port Trunking
- IGMP Snooping v1/v2/v3
- IGMP Fast Leave
- Power Class Configuration
- MLD Snooping
- Bandwidth Control
- IEEE 802.1X Guest VLAN
- CoS based on 802.1p Priority
- CoS based on Physical Port
- CoS based on TOS
- CoS based on DSCP
- 802.1X Port-based Access Control

- Port Security
- Storm Control
- Port Isolation
- Access Control List (ACL)
- SNMP v1/v2c/v3
- Power Feeding with Priority
- User Defined Power Limit
- Telnet Server
- IEEE802.3az (Energy Efficient Ethernet)
- BootP/DHCP Client
- Web-based Support
- SNMP v1/v2/v3 Support
- TFTP Client
- TFTP Upgrade
- Command Line Interface (CLI)
- SNTP
- SYSLOG
- Cable Diagnostics
- MIB Support (RFC1213, RFC1493, RFC1757, RFC2674)
- RMON v1
- SSH Server

Installing the EWS Switch

Basic installation instructions are included in the Quick Installation Guide that shipped with your EWS Switch. The steps are summarized below:

1. Connect the switch to a PC using a RJ45 cable.
2. Point your web browser to the switch's IP address. The default IP Address is ***192.168.0.239***.
3. Login the user interface by entering the user name and password. The default user name is ***admin*** and the default password is ***password***.
4. Begin using your EWS Switch.

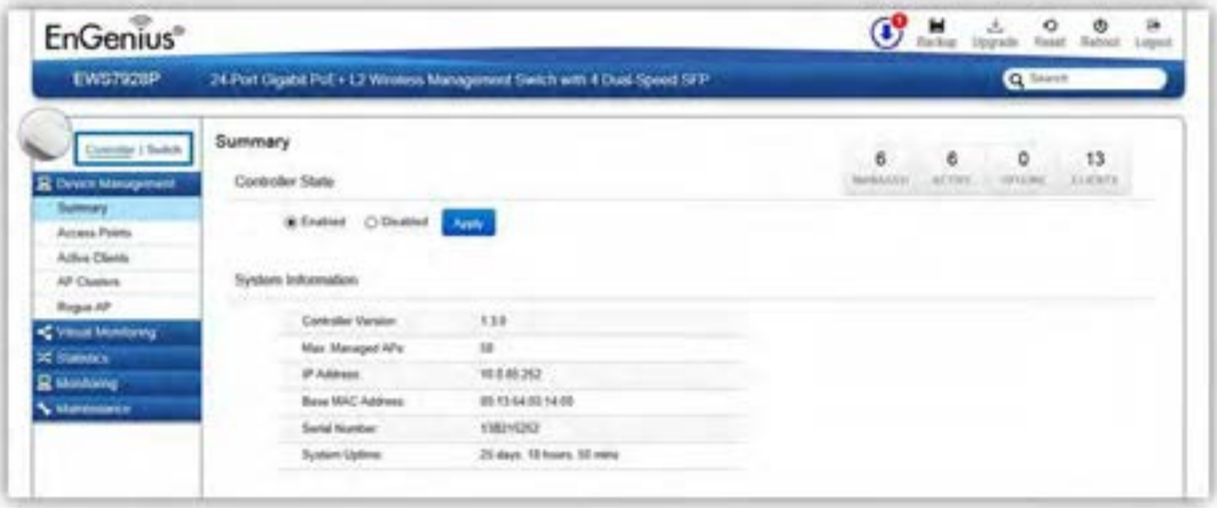
WARNING!

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

Using the EWS Switch

Using the EWS Switch

Besides the functions of a Wireless Controller, the EWS Wireless Management Switch also possesses functions of a full-featured Layer 2 PoE switch. Use the ***Controller / Switch tab*** on the upper left corner of the user interface to toggle between the Wireless Controller or Layer 2 Switch functions.



Summary

Controller State

● Enabled ○ Disabled

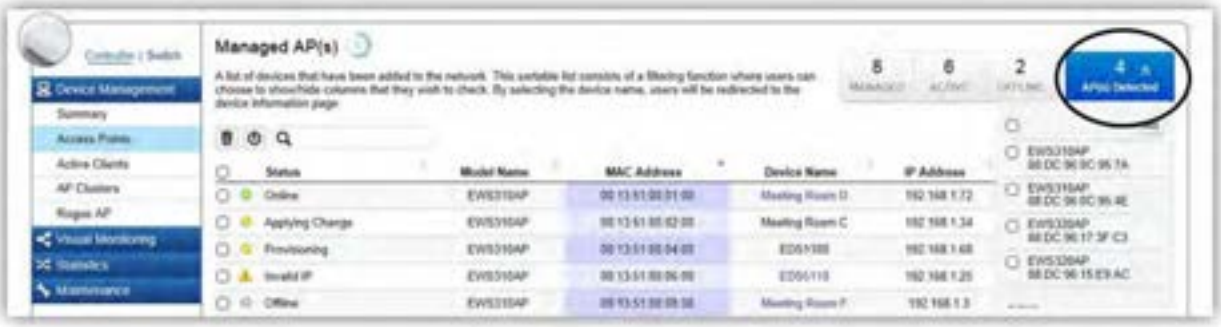
System Information

Controller Version	1.3.9
Max. Managed APs	50
IP Address	10.0.65.252
Base MAC Address	00:13:64:00:14:00
Serial Number	13B21Q262
System Uptime	25 days, 18 hours, 50 mins

WLAN Controller Features

Managing EWS Access Points

1. Access Points in the network will be automatically discovered by the EWS and will be listed under the AP(s) Detected list in the Access Point menu.



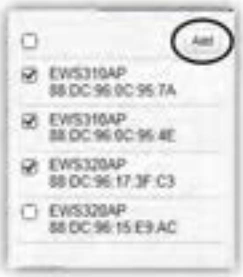
Managed AP(s)

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
□	Online	EWS310AP	00:13:51:00:01:00	Meeting Room D	192.168.1.72
□	Applying Change	EWS310AP	00:13:51:00:02:00	Meeting Room C	192.168.1.34
□	Provisioning	EWS310AP	00:13:51:00:04:00	EDS1100	192.168.1.48
□	Invalid IP	EWS310AP	00:13:51:00:06:00	EDS6110	192.168.1.25
□	Offline	EWS310AP	00:13:51:00:08:38	Meeting Room F	192.168.1.3

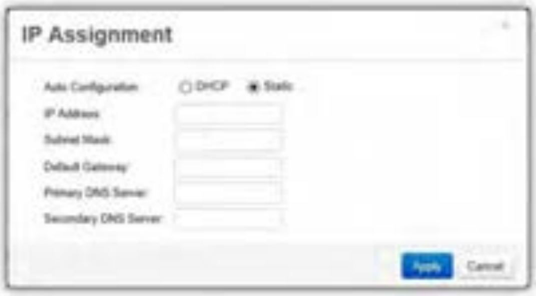
○ EWS310AP 88:DC:96:0C:95:7A
○ EWS310AP 88:DC:96:0C:95:4E
○ EWS320AP 88:DC:96:17:3F:C3
○ EWS320AP 88:DC:96:15:E9:AC

2. Select the Access Point(s) you wish to manage and click Add.



□
☑ EWS310AP 88:DC:96:0C:95:7A
☑ EWS310AP 88:DC:96:0C:95:4E
☑ EWS320AP 88:DC:96:17:3F:C3
□ EWS320AP 88:DC:96:15:E9:AC

3. You will be prompted to assign the IP Address under the IP Assignment screen.

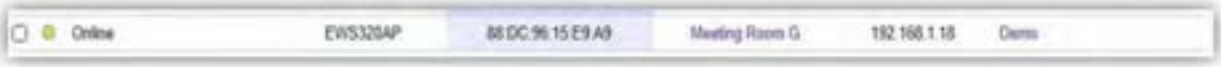


IP Assignment

Auto Configuration ○ DHCP ● Static
IP Address
Subnet Mask
Default Gateway
Primary DNS Server
Secondary DNS Server

DHCP	You can choose to auto assign an IP Address if there is a DHCP server in the network.
Static	If you wish to manually assign the IP Address, choose “Static”. Enter the IP Address you wish to assign to the AP(s) (if more than one AP is added, you’ll be prompted to enter a range of IP Address) and fill in the subnet mask and default gateway.

4. Click Apply and the Access Point(s) you’ve configured will be moved to the Managed list. Note that the status of the AP will change from *Connecting* to *Provisioning* to *Online*.
Once the status turns *Online*, your Access Point(s) have been successfully added to the Managed list.



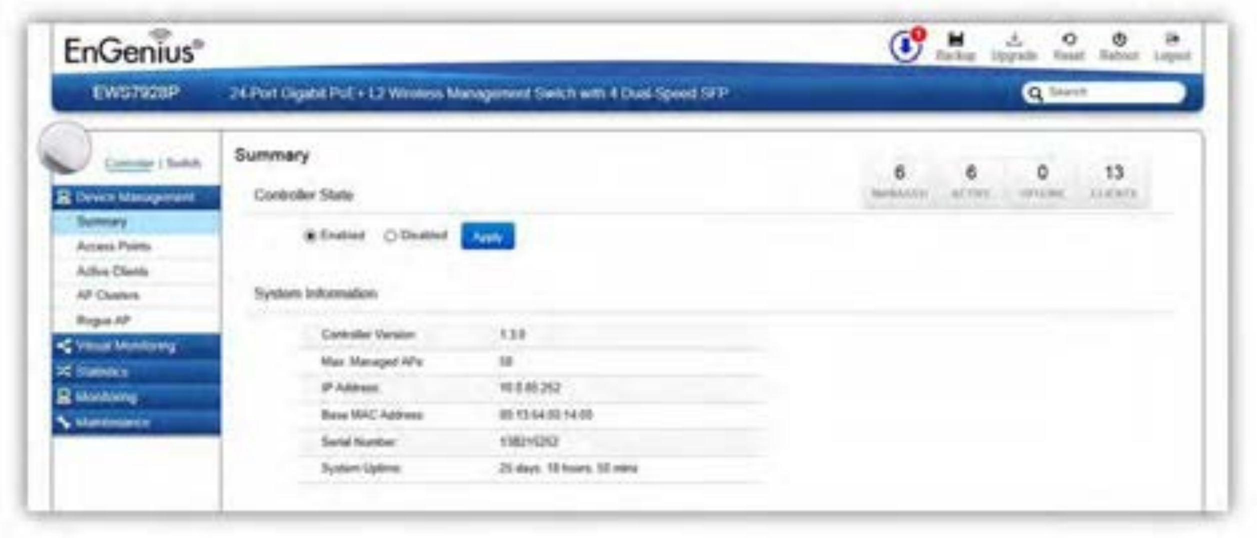
□ Online EWS320AP 88:DC:96:15:E9:A8 Meeting Room G 192.168.1.18 Demo

Device Management

Summary

Device Management > Summary

The Summary page shows general system information for the EWS Switch including the Controller Status, the software version, the maximum number of APs the system can manage, MAC Address, IP Address, serial number, and system uptime for the system.



Summary

6 MANAGED | 6 ACTIVE | 0 OFFLINE | 13 CLIENTS

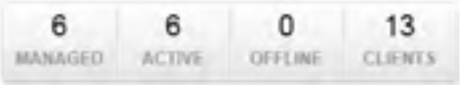
Controller State

● Enabled ○ Disabled Apply

System Information

Controller Version	1.3.0
Max. Managed APs	50
IP Address	10.0.85.252
Base MAC Address	[illegible]
Serial Number	[illegible]
System Uptime	25 days, 18 hours, 50 mins

Dashboard
The Dashboard on the upper right corner of the GUI shows the current status of EWS APs that has been managed by the EWS Switch.



6	6	0	13
MANAGED	ACTIVE	OFFLINE	CLIENTS

Managed	This shows the number of APs currently managed by the EWS Switch.
Active	This shows the number of managed APs that currently have an active connection with the EWS Switch.
Offline	This shows the number of managed APs that currently do not have an active connection with the EWS Switch.
Clients	This shows the total number of wireless clients currently connected to all the managed APs.

.

Controller State
Select whether to Enable or Disable the Controller feature on the Switch.
Click *Apply* to save the changes to the system.

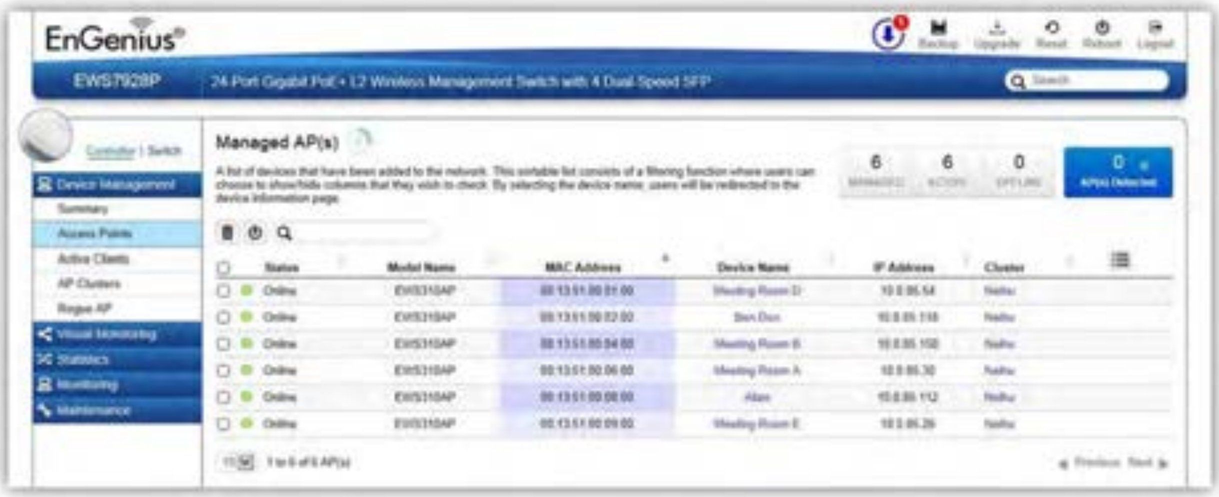
System Information

- Controller Version: This is the software version of the device.
- Max. Managed APs: The maximum number of APs the device is able to manage.
- IP Address: Displays the IP address of the device.
- Base MAC Address: Universally assigned network address.
- Serial Number: Displays the serial number of the device.
- System Uptime: Displays the number of days, hours, and minutes since the last system restart.

Access Points

Device Management > Access Points

This page displays the status of all EWS Access Points that your Controller is currently managing as well as all the EWS Access Points in the network that the Controller has discovered. Use this page to add EWS Access Points to your EWS Controller Access Point list. For the discovery procedure to succeed, the EWS Switch and the EWS Access Point must be connected in the same network. The EWS Switch can discover supported EWS Access Points with any IP address and Subnet 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.

6 MANAGED | 6 ACTIVE | 0 OFFLINE | 0 AP(s) Detected

	Status	Model Name	MAC Address	Device Name	IP Address	Cluster
□	● Online	EWS310AP	00:13:51:00:01:00	Meeting Room D	10.0.86.54	[illegible]
□	● Online	EWS310AP	00:13:51:00:02:00	Ben Dun	10.0.85.118	[illegible]
□	● Online	EWS310AP	00:13:51:00:04:00	Meeting Room B	10.0.85.150	[illegible]
□	● Online	EWS310AP	00:13:51:00:06:00	Meeting Room A	10.0.86.30	[illegible]
□	● Online	EWS310AP	00:13:51:00:08:00	Alan	10.0.86.112	[illegible]
□	● Online	EWS310AP	00:13:51:00:09:00	Meeting Room E	10.0.86.26	[illegible]

1 to 6 of 6 AP(s)

Previous Next

Managing Access Points

EWS Access Points can either be configured individually or configured as a group within a cluster.

To manage an Access Point individually, click on the **Device Name** field of the Access Point you wish to configure and you will be directed to a screen where you can configure settings for the Access Point.

To manage Access Points as a group, go to **Device Management > AP Clusters** to create a cluster and add members into the cluster. Click on the **Cluster** field of the cluster you wish to configure and you will be directed to a screen where you can configure settings for the Cluster.

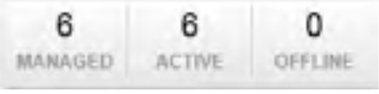
Cluster settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Transmit Power at Auto in the Wireless Radio Settings of the cluster, then click on the **Device Name** field of the Access Point (which is already in a cluster) you wish to configure and you will be directed to a screen where you can configure override settings for the selected Access Point.

Refresh Countdown Timer

This is the time left before the page auto-refreshes. The countdown is from 15 seconds.

Dashboard

The Dashboard shows the current status of all the EWS APs that has been managed by the EWS Switch.



6 MANAGED | 6 ACTIVE | 0 OFFLINE

Managed	This shows the number of APs in the managed AP database that are configured with the EWS Switch.
Active	This shows the number of managed APs that currently have an active connection with the EWS Switch.
Offline	This shows the number of managed APs that currently do not have an active connection with the EWS Switch.

AP(s) Detected List

Reveals a list of all APs in the network that the EWS Switch automatically discovers. Mouse over the discovered Access Point to show general information such as the MAC address, IP address, model name and firmware version.

Remove AP

The Remove button removes selected Access Point(s) from list. Access Points removed will be automatically set to standalone mode with all settings restored to their factory default settings.

Reboot AP

The Reboot button will reboot the selected Access Point(s).

Search Bar

Use the Search Bar to search for Access Points managed by the EWS Switch using the following criteria: Status, model name, MAC Address, Device name, IP address, Firmware Version, Cluster.

Status

This indicates the current status of the managed Access Point.

Status	Explanation
Online	AP is connected and managed by EWS Switch.
Provisioning	AP is currently in the process of connecting to the EWS Switch.
Applying Change	AP is currently applying system changes.
Connecting	AP is currently connecting to EWS Switch.
Offline	AP is currently offline.
Resetting	AP is resetting.
Firmware Upgrading	AP is currently undergoing firmware upgrade process.
Invalid IP	The subnet of managed AP's IP address is not the same as the EWS Switch. Please remove AP and reconfigure AP to the correct setting.
Incompatible Version	AP firmware is not compatible with EWS Switch.
Checking Certificate	EWS Switch is checking the SSL Certificate of AP.

Model Name

Shows the model name of the managed Access Point.

MAC Address

Shows the MAC address of the managed Access Point.

Device Name

Displays the device name of the managed Access Point.

- When the AP is not a cluster member, click on this field and you'll be redirected to the configuration page where you can edit settings such as device name, IP Address, Wireless Radio settings.
- When the AP is a cluster member, click on this field to configure settings for individual Access Points by overriding the cluster settings.

IP Address

Shows the IP address of the managed Access Point.

Firmware Version
Shows the firmware version of the managed Access Point.

Last Update
Display the time the Access Point was last detected and the information was last updated.

Uptime:
Displays the number of days, hours, and minutes since the AP last restarted.

Cluster
Displays the Cluster the Access Point is currently assigned to. Click on this field and you'll be redirected to the cluster configuration page.

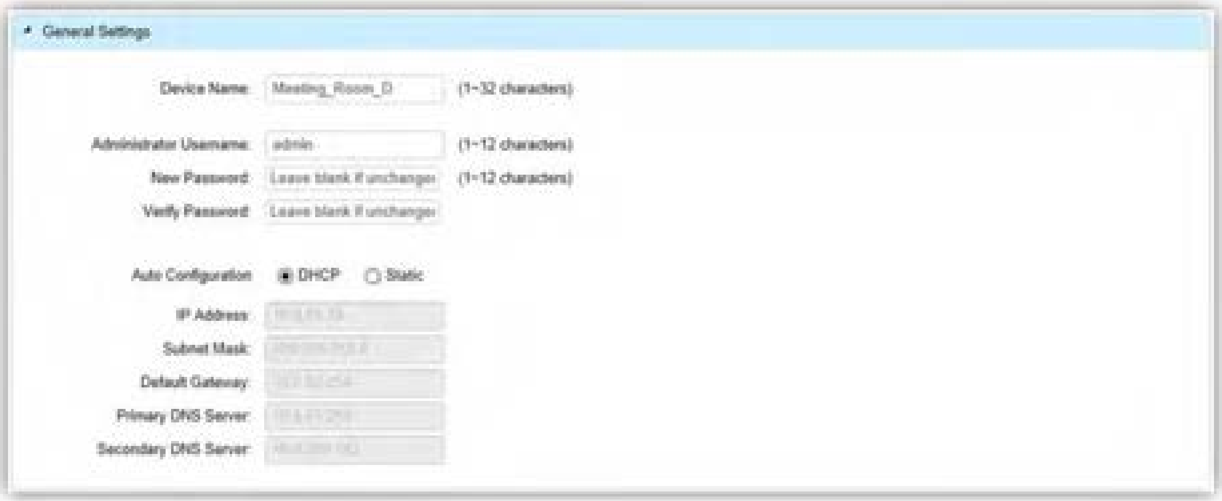
Column Filter
Shows or hides fields in the Access Point list.
☰

Wireless Settings

Device Management > Access Points > Wireless Settings

On this page, you can edit the AP's name and password, manually assign an IP address, or change the channel selection, transmit power and other wireless settings of a managed Access Point.

General Settings



General Settings

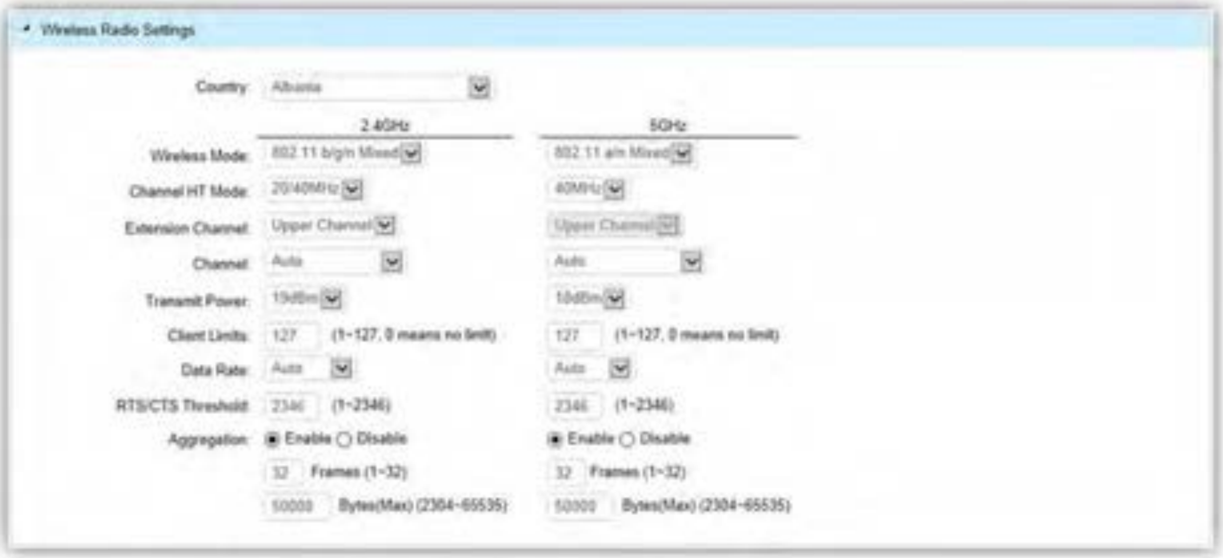
Device Name:	Meeting_Room_D	(1~32 characters)
Administrator Username:	admin	(1~12 characters)
New Password:	Leave blank if unchange	(1~12 characters)
Verify Password:	Leave blank if unchange	
Auto Configuration	● DHCP ○ Static	
IP Address:	[illegible]	
Subnet Mask:	[illegible]	
Default Gateway:	[illegible]	
Primary DNS Server:	[illegible]	
Secondary DNS Server:	[illegible]	

Device Name: The device name of the Access Point. Users can enter a custom name for the Access Point if they wish.

Administrator Username: Displays the current administrator login username for the Access Point. Enter a new Administrator username for the Access Point if you wish to change the username. The default username is: *admin*.
New Password: Enter a new password of between 1~12 alphanumeric characters.
Verify Password: Enter the password again for confirmation.

Auto Configuration: Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.
IP Address: Enter the IP address for the Access Point.
Subnet Mask: Enter the Subnet Mask for the Access Point.
Default Gateway: Enter the default Gateway for the Access Point.
Primary/Secondary DNS Server: Enter the Primary/Secondary DNS server name.

Wireless Radio Settings



Wireless Radio Settings

Country: Albania

	2.4GHz	5GHz
Wireless Mode:	802.11 b/g/n Mixed	802.11 a/n Mixed
Channel HT Mode:	20/40MHz	40MHz
Extension Channel:	Upper Channel	Upper Channel
Channel:	Auto	Auto
Transmit Power:	15dBm	10dBm
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)

Country: Select a Country/Region to conform to local regulations. Different regions have different rules that govern which channels can be used for wireless communications.

Wireless Mode: Select from the drop-down menu to set the wireless mode for the Access Point.

Channel HT Mode: Use the drop-down menu to select the channel width for 2.4GHz. A wider channel improves the performance, but some legacy devices operate only on either 20MHz or 40 MHz. This option is only available for 802.11n modes.

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

Channel: Select Auto or manually assign a channel for the 2.4GHz or 5GHz radio.

Transmit Power: Allows you to manually set the transmit power on 2.4GHz or 5GHz radios. Optimizing channel assignments reduces channel interference and channel utilization for the network, thereby improving overall network performance and increasing the network's client capacity. The list of available channels that can be assigned to radios is determined based on which country the Access Points are deployed in.

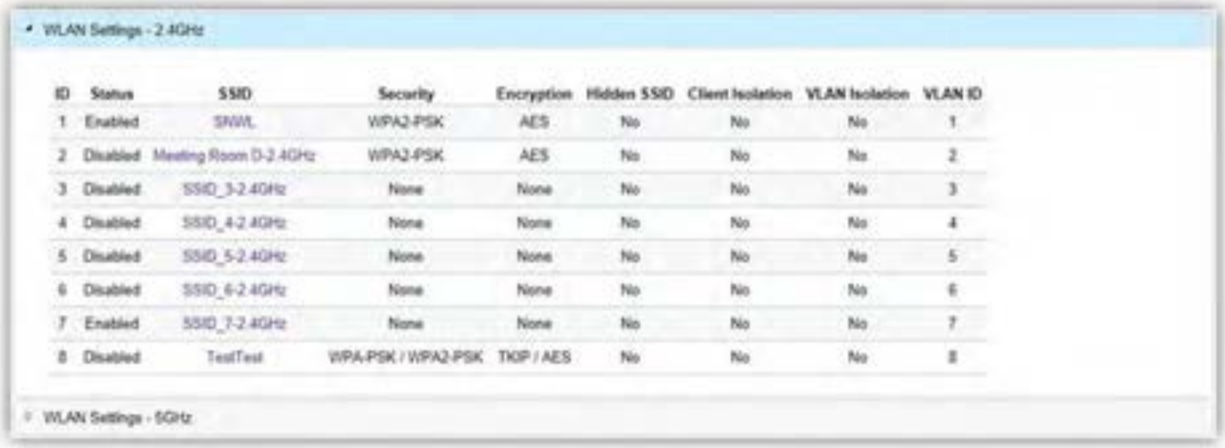
Client Limits: Limit the total number of clients that can associate with this Access Point.

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: Enter a Request to Send (RTS) Threshold value between 1~2346. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same Access Point. Changing the RTS threshold can help control traffic flow through the Access Point. If you specify a lower threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the Access Point. Sending out more RTS packets can help the network recover from interference or collisions which might occur on a busy network or on a network experiencing electromagnetic interference.

Aggregation: Select whether to enable or disable Aggregation for the Access Point. This function merges data packets into one packet, reducing the number of packets. This also increases the packet sizes, so please keep this in mind. Aggregation is useful for increasing bandwidth throughput in environments that are prone to high error rates. This mode is only available for 802.11n modes. Fill in the frame rate limit you wish to use. The range is from 1~32. Next, fill in the max byte limit. The range is from 2304~65535.

WLAN Settings - 2.4GHz/5GHz



WLAN Settings - 2.4GHz

ID	Status	SSID	Security	Encryption	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	Enabled	SNWL	WPA2-PSK	AES	No	No	No	1
2	Disabled	Meeting Room D-2.4GHz	WPA2-PSK	AES	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	Enabled	SSID_7-2.4GHz	None	None	No	No	No	7
8	Disabled	TestTest	WPA-PSK / WPA2-PSK	TKIP / AES	No	No	No	8

WLAN Settings - 5GHz

Basic Setting

Enable SSID: Select to enable or disable the SSID broadcasting.

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

Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

Client Isolation: When enabled, all communication between wireless clients connected to the same AP will be blocked.

L2 Isolation: When enabled, wireless client traffic from all hosts and clients on the same subnet will be blocked.

VLAN Isolation: When enabled, all communications between wireless clients and any other devices on different VLANs will be blocked. All frames from wireless clients connected to this SSID will be tagged a corresponded 802.1Q VLAN tag when going out from Ethernet port.

VLAN ID: Enter the VLAN ID for the SSID profile. The range is from 1~4094. When VLAN tagging is configured per SSID, all data traffic from wireless users associated to that SSID is tagged with the configured VLAN ID. Multiple SSIDs also can be configured to use the same VLAN tag. For instance, a single VLAN ID could be used to identify all wireless traffic traversing the network, regardless of the SSID. When the AP receives VLAN-tagged traffic from the upstream switch or router, it forwards that traffic to the correct SSID. The AP drops all packets with VLAN IDs that are not associated to the SSID.

Traffic Shaping: Traffic Shaping regulates the allowed maximum downloading/uploading throughput per SSID. Select to enable or disable Wireless Traffic Shaping for the SSID.

- **Download Limit**: Specifies the allowed maximum throughput for downloading.
- **Upload Limit**: Specifies the allowed maximum throughput for uploading.

Fast Roaming: This feature uses protocols defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure roaming from one AP to another. Coupled with 802.11k, wireless devices are able to quickly identify nearby APs that are available for roaming and once the signal strength of the current AP weakens and your device needs to roam to a new AP, it will already know which AP is the best to connect with. Note that not every wireless client supports 802.11k and 802.11r. Both the SSID and security options must be the same for this fast roaming to work. Fast Roaming is available when the following security methods are well configured:

WPA2-Enterprise	RADIUS server required
WPA-Mixed Enterprise	
WPA2-PSK	No RADIUS server required

WPA-Mixed	

Security: Select encryption method (WEP, WEP / WPA2 Enterprise, WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WEP: Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks which scrambles all data packets transmitted between the Access Point and
the wireless clients associated with it. Both the Access Point and the wireless client must use the same WEP key for data encryption and decryption.

- **Mode**: Select Open System or Shared Key.
- **WEP Key**: Select the WEP Key you wish to use.
- **Input Type**: ASCII: Regular Text or HEX. Select the key type. Your available options are ASCII and HEX.
  - **ASCII Key**: You can choose upper and lower case alphanumeric characters and special symbols such as @ and #.
  - **HEX Key**: You can choose to use digits from 0~9 and letters from A~F. Select the bit-length of the encryption key to be used in the WEP connection. Your available options are: 64, 128, and 152-bit password lengths.
- **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.
- **Key1/2/3/4**: Enter the Key value or values you wish to use.

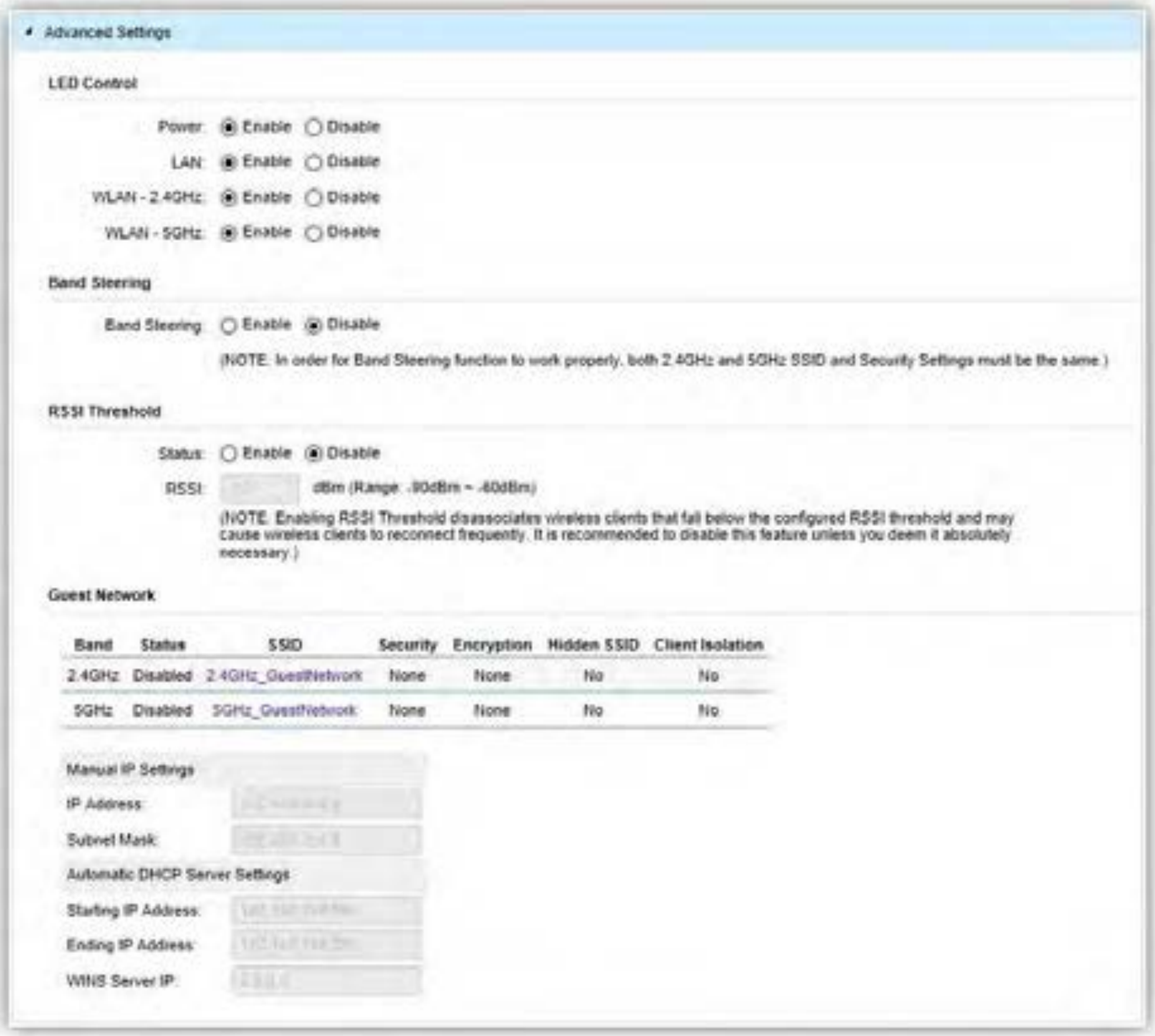
WPA / WPA2 Enterprise: WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i standards, which include AES and TKIP mechanisms.

- **Type**: Select the WPA type to use. Available options are Mixed, WPA and WPA2. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **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.
- **Update Interval**: Specify how often, in seconds, the group key changes. Select 0 to disable.
- **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.
- **Accounting Group Key Update Interval**: Specify how often, in seconds, the accounting data sends. The range is from 60~600 seconds.

WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

- **Type**: Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase**: Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval**: Specify how often, in seconds, the Group Key changes.

Advanced Settings



Advanced Settings

LED Control

Power: ● Enable ○ Disable

LAN: ● Enable ○ Disable

WLAN - 2.4GHz: ● Enable ○ Disable

WLAN - 5GHz: ● Enable ○ Disable

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.)

RSSI Threshold

Status: ○ Enable ● Disable

RSSI: [illegible] dBm (Range: -90dBm ~ -60dBm)

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

Guest Network

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

Manual IP Settings

IP Address: [illegible]

Subnet Mask: [illegible]

Automatic DHCP Server Settings

Starting IP Address: [illegible]

Ending IP Address: [illegible]

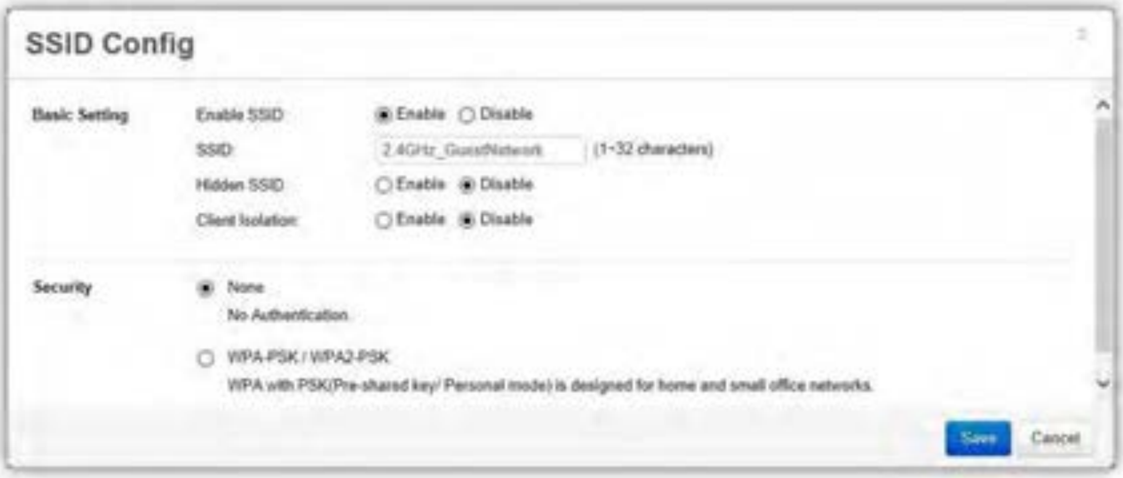
WINS Server IP: [illegible]

LED Control: In some environments, the blinking LEDs are not welcomed. This option allows you to enable or disable the devices LED indicators. Note that only indoor models support this feature.

Band Steering: When enabled, the AP detects whether or not the wireless client is dual-band capable, and if it is, it will force the client to connect to the less congested 5GHz network to relieve congestion and overcrowding on the mainstream 2.4GHz frequency. It does this by actively blocking the client's attempts to associate with the 2.4GHz network.
Note: Both 2.4GHz and 5GHz SSIDs must have the same security settings.

RSSI Threshold: With this feature enabled, in order to minimize the time the wireless client spends to passively scanning for a new AP to connect to, the AP will send a disassociation request to the wireless client upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow for more clients to stay associated to this Access Point. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.

Guest Network: The Guest Network feature allows administrators to grant Internet connectivity to visitors or guests while keeping other networking devices and sensitive personal or company information private and secure.



SSID Config

Basic Setting

Enable SSID: ● Enable ○ Disable

SSID: 2.4GHz_GuestNetwork (1~32 characters)

Hidden SSID: ○ Enable ● Disable

Client Isolation: ○ Enable ● Disable

Security

● None
No Authentication

○ WPA-PSK / WPA2-PSK
WPA with PSK(Pre-shared key/ Personal mode) is designed for home and small office networks.

Basic Setting

Enable SSID: Select to enable or disable the SSID broadcasting.

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

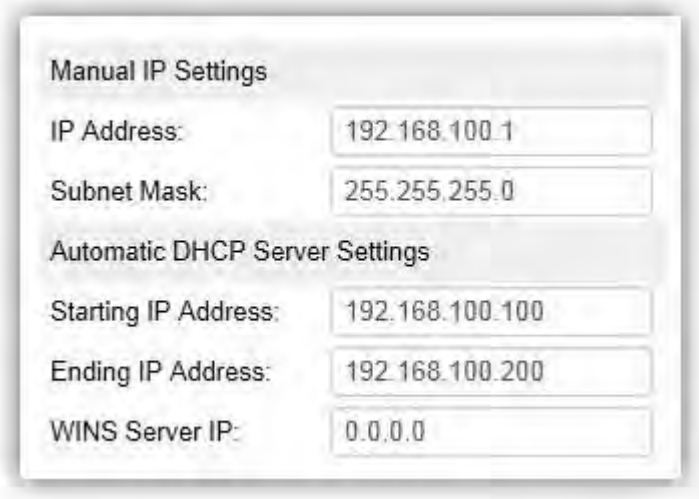
Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

Client Isolation: When enabled, all communication between wireless clients connected to the same AP will be blocked.

Security: Select encryption method (WPA-PSK / WPA2-PSK, or none) and encryption algorithm (AES or TKIP).

WPA-PSK / WPA2-PSK: WPA with PSK (Pre-shared key / Personal mode), designed for home and small office networks that don't require the complexity of an 802.1X authentication server.

- **Type**: Select the WPA-PSK type to use. Available options are Mixed, WPA-PSK and WPA2-PSK. Choose Mixed if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- **Encryption**: Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
  Note: Since TKIP is not permitted for 802.11n-based transmissions, setting the encryption algorithm to TKIP when you are using an 802.11n or 802.11ac AP will cause the network to operate in 802.11g mode.
- **WPA Passphrase**: Enter the Passphrase you wish to use. If you are using the ASCII format, the Key must be between 8~64 characters in length.
- **Group Key Update Interval**: Specify how often, in seconds, the Group Key changes.



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

Manual IP Settings

- **IP Address**: Enter the IP address for the default gateway of clients associated to the Guest Network.
- **Subnet Mask**: Enter the Subnet mask for the Guest Network.

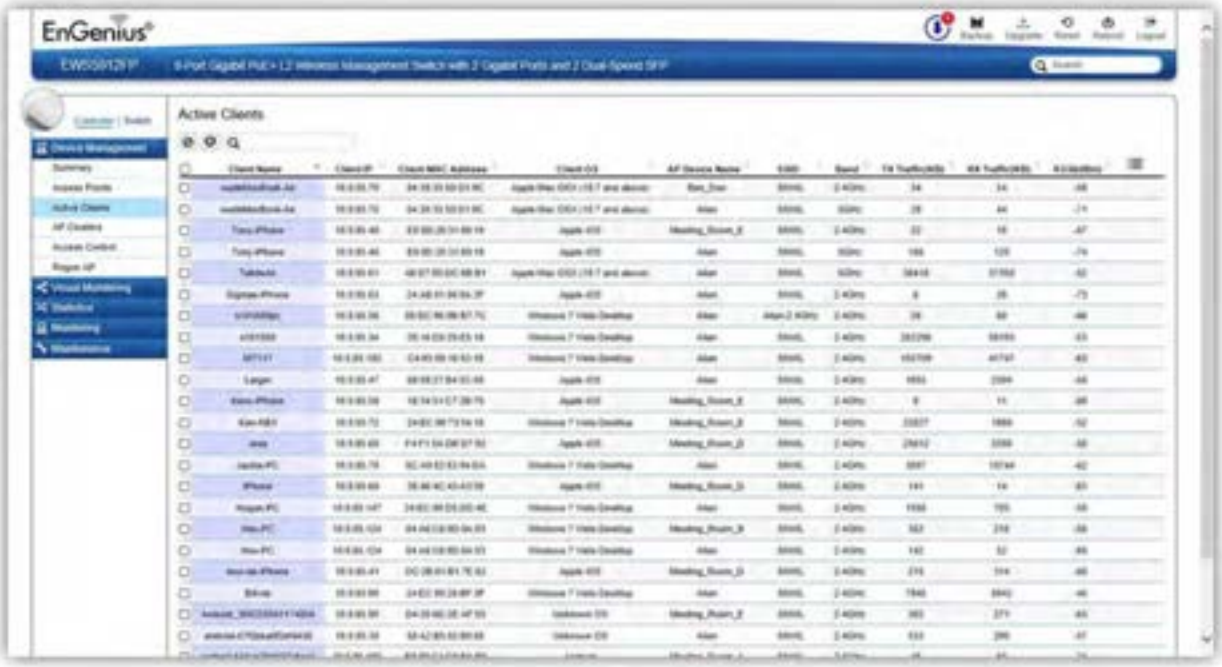
Automatic DHCP Server Settings

- **Starting IP Address/Ending IP Address**: Enter the pool range of IP addresses available for assignment.
- **WINS Server IP**: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

Active Clients

Device Management > Active Clients

From here, you can view information, temporarily disconnect and permanently block the wireless clients that are associated with the Access Points that the EWS Switch manages. The EWS Switch is able to identify client devices by their Operating System, device type and host name, if available. If multiple Access Points are connected to the network, use the search bar to find an Access Point by its name.



Kick Client
Use this function to temporarily disconnect a wireless client from the network. The disconnected client can simply reconnect manually if they wish to.

⊗

Ban Client
Use this function to permanently block a wireless client from the network.
Go to **Device Management > Access Control** to unblock the wireless client.

⊘

Search Bar
Use the Search Bar to search for Wireless Clients managed by the EWS Switch using the following criteria: Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band, TX Traffic, RX Traffic.

🔍

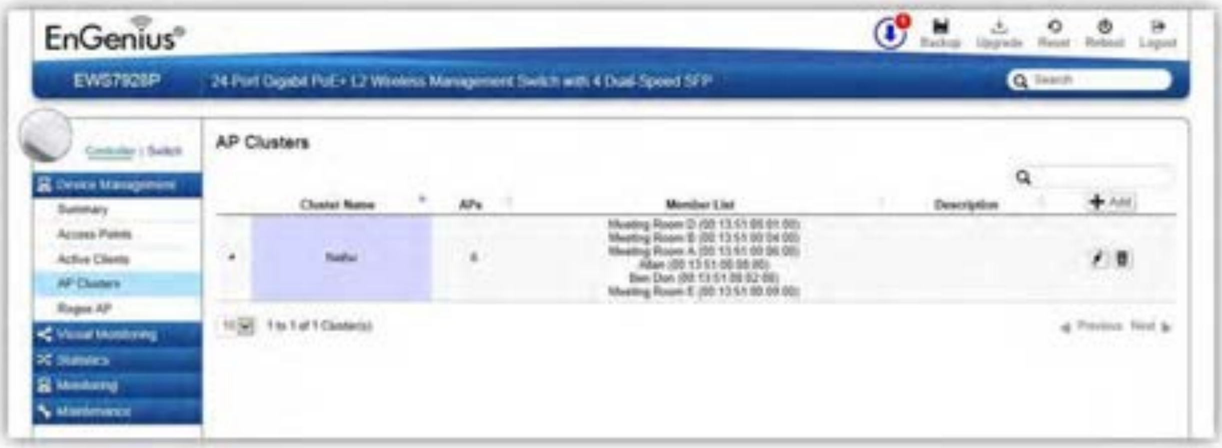
Client Name	Displays the name of the wireless client connected to the Access Point.
Client IP	Displays the IP address of the wireless client connected to the Access Point.
Client MAC Address	Displays the MAC address of the wireless client connected to the Access Point.
Client OS	Displays the type of operating system the wireless client connected to the Access Point is running on.
AP Device Name	Displays the name of the Access Point which the client is connected to.
AP MAC Address	Displays the MAC address of the Access Point which the client is connected to.
Model Name	Displays the model name of the Access Point which the client is connected to.
SSID	Displays the SSID of the Access Point which the client is connected to.
Band	Displays whether the wireless client is connected to the 2.4GHz or 5GHz radio.

TX Traffic (KB)	Displays the total traffic transmitted to the Wireless Client.
RX Traffic (KB)	Displays the total traffic received from the Wireless Client.
RSSI (dBm)	Displays the received signal strength indicator in terms of dBm.

AP Clusters

Device Management > AP Clusters

An Access Point Cluster can be used to define configuration options and apply them to a number of APs at once. If your wireless network covers a large physical environment and you want to provide wireless services with different settings and policies to different areas of your environment, you can use AP Clusters to do this instead of having to modify the settings of each AP individually. For example, if your wireless network covers two floors and you need to provide wireless access to visitors on the 1st Floor, you can simply setup two different clusters with different settings and policies to suit your application.



AP Clusters

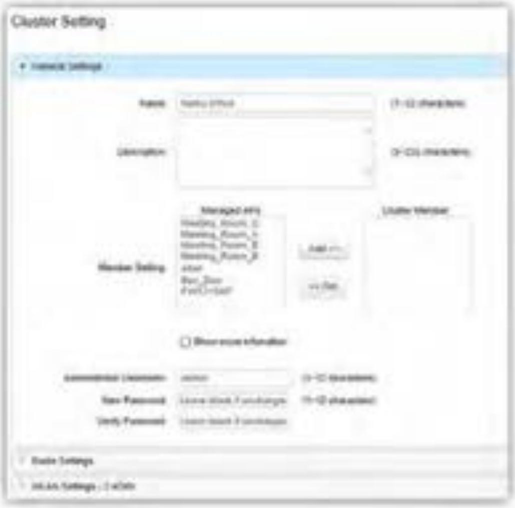
Cluster Name	APs	Member List	Description
Nathu	6	Meeting Room D (00:13:51:00:01:00) Meeting Room B (00:13:51:00:04:00) Meeting Room A (00:13:51:00:06:00) Alan (00:13:51:00:08:00) Ben Don (00:13:51:00:02:00) Meeting Room E (00:13:51:00:09:00)	

10 1 to 1 of 1 Cluster(s)

Creating a New Cluster

Follow the steps below to create a new cluster.

1. Click on **Add** button to create a new cluster.



2. Enter the name and description of the new cluster.
3. In the Member Setting section, all Access Points that are managed by the EWS Switch that are not currently assigned to a cluster will be listed on the left. Select the Access Points you wish to assign to this cluster and press **Add**. The Access Points will be moved to the right column.
4. Configure Radio, WLAN, and Advanced settings then click on Apply for settings to take effect.

Search Bar

Use the Search Bar to search for clusters in the list using the following criteria: Cluster Name, AP MAC, AP Name, Description.

Add Button

Use the Add Button to create a new cluster.

+ Add

Edit Button
Use the Edit Button to edit the configurations of the cluster.
✎

Delete Button
Use the Delete Button to remove a cluster.
🗑

Note:

Access Control

Device Management > Access Control

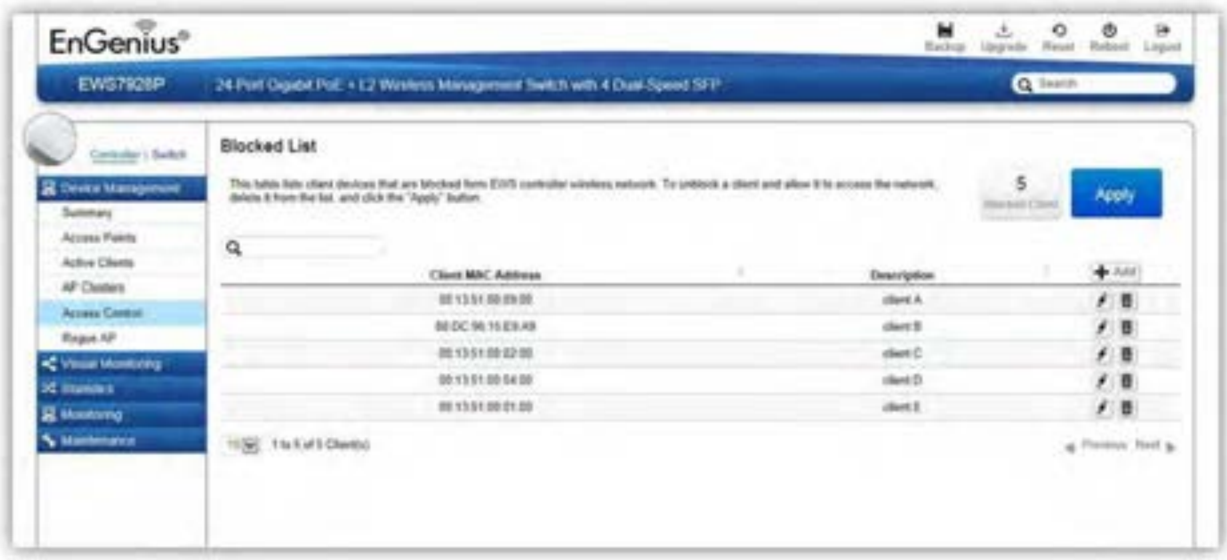
This page displays the list of wireless clients previously blocked from your network. If for any reason, you need to block a client device from your network, you can do so from this page by creating a new rule and entering the client's MAC address.

Blocking a Specific Client Device
Follow the steps below to permanently block a specific client device from the network.

1. Click the **Add** button to create a new block rule.
2. Enter the *MAC Address* and *Description* of the wireless client device you wish to block.
3. Click on **Apply** to create a new rule.
4. Click on the **Apply** button on the upper right to save settings made on this page.

Unblocking a Previously Blocked Client Device

1. Click on the **Delete** button on the client device you wish to unblock.
2. Click on the **Apply** button on the upper right to save settings made on this page.



Blocked List

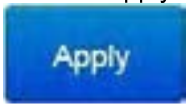
This table lists client devices that are blocked form EWS controller wireless network. To unblock a client and allow it to access the network, delete it from the list, and click the "Apply" button.

Client MAC Address	Description
00:13:51:00:09:00	client A
00:DC:96:15:E9:A9	client B
00:13:51:00:02:00	client C
00:13:51:00:04:00	client D
00:13:51:00:01:00	client E

10 1 to 5 of 5 Client(s)

Blocked Clients
Displays the total number of clients permanently blocked from the network.

Apply Button
Click on Apply to save changes made on this page.



Search Bar
Use the Search Bar to search for blocked clients in the list using the following criteria: Client MAC Address, Description.

Add Button
Use the Add Button to add a new block rule.

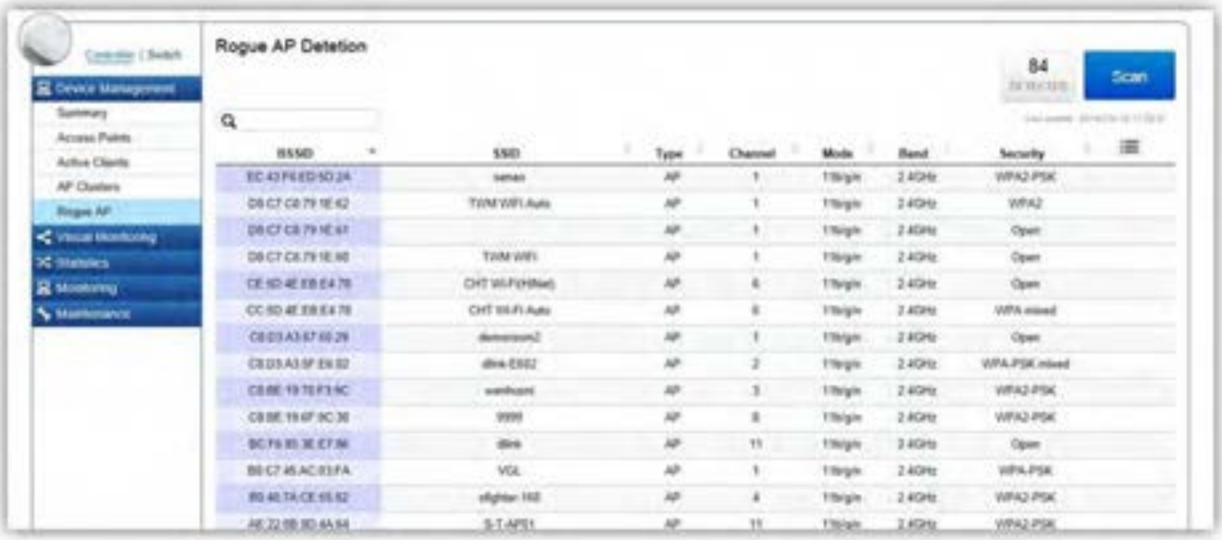
Edit Button
Use the Edit Button to edit the Client MAC Address or Description of the rule.
✎

Delete Button
Use the Delete Button to remove the rule.
🗑

Rogue AP

Device Management > Rogue AP Detection

Rogue Access Points refer to those unauthorized and often unmanaged APs attached to an existing wired network which could bring harm to the network or may be used to deliberately gain access to confidential company information. The Rogue AP Detection feature can be used to scan 2.4 and 5 GHz frequency bands to identify rogue wireless Access Points not managed by the EWS Switch and displays the rogue AP’s BSSID.



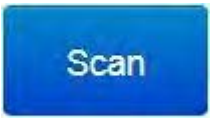
Rogue AP Detetion

BSSID	SSID	Type	Channel	Mode	Band	Security
EC:43:F6:ED:5D:2A	[illegible]	AP	1	11b/g/n	2.4GHz	WPA2-PSK
D8:C7:C8:79:1E:42	TWM WiFi Auto	AP	1	11b/g/n	2.4GHz	WPA2
D8:C7:C8:79:1E:41		AP	1	11b/g/n	2.4GHz	Open
D8:C7:C8:79:1E:40	TWM WiFi	AP	1	11b/g/n	2.4GHz	Open
CE:5D:4E:E8:E4:78	CHT Wi-Fi(HiNet)	AP	6	11b/g/n	2.4GHz	Open
CC:5D:4E:E8:E4:78	CHT Wi-Fi Auto	AP	6	11b/g/n	2.4GHz	WPA mixed
C8:D3:A3:67:60:28	[illegible]	AP	1	11b/g/n	2.4GHz	Open
C8:D3:A3:5F:E6:02	dlink-E602	AP	2	11b/g/n	2.4GHz	WPA-PSK mixed
C8:BE:19:70:F3:AC	[illegible]	AP	3	11b/g/n	2.4GHz	WPA2-PSK
C8:BE:19:6F:9C:30	9999	AP	8	11b/g/n	2.4GHz	WPA2-PSK
BC:F6:85:3E:E7:86	dlink	AP	11	11b/g/n	2.4GHz	Open
B0:C7:45:AC:03:FA	VGL	AP	1	11b/g/n	2.4GHz	WPA-PSK
B0:48:7A:CE:65:62	[illegible] 168	AP	4	11b/g/n	2.4GHz	WPA2-PSK
AE:72:9B:9D:4A:64	S-T-AP01	AP	11	11b/g/n	2.4GHz	WPA2-PSK

Search Bar
Use the Search Bar to search for Rogue Access Points discovered by the EWS Switch using the following criteria: Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band, TX Traffic, RX Traffic.

Rogue APs Detected
This shows the number of Rogue APs detected by the Access Points managed by the EWS Switch.

Scan Button
Click on *Scan* for EWS Access Points managed by the EWS Switch to start scanning for Rogus APs.



Column Filter
Shows or hides fields in the list.

☰

BSSID	Displays the BSSID of the rogue device detected.
SSID	Displays the SSID of the rogue device detected.
Type	Displays the type of the rogue device detected.
Channel	Displays the channel of the rogue device detected.
Mode	Displays the wireless mode of the rogue device detected.
Band	Displays the band of the rogue device detected.

Security	Displays the encryption method of the rogue device detected.

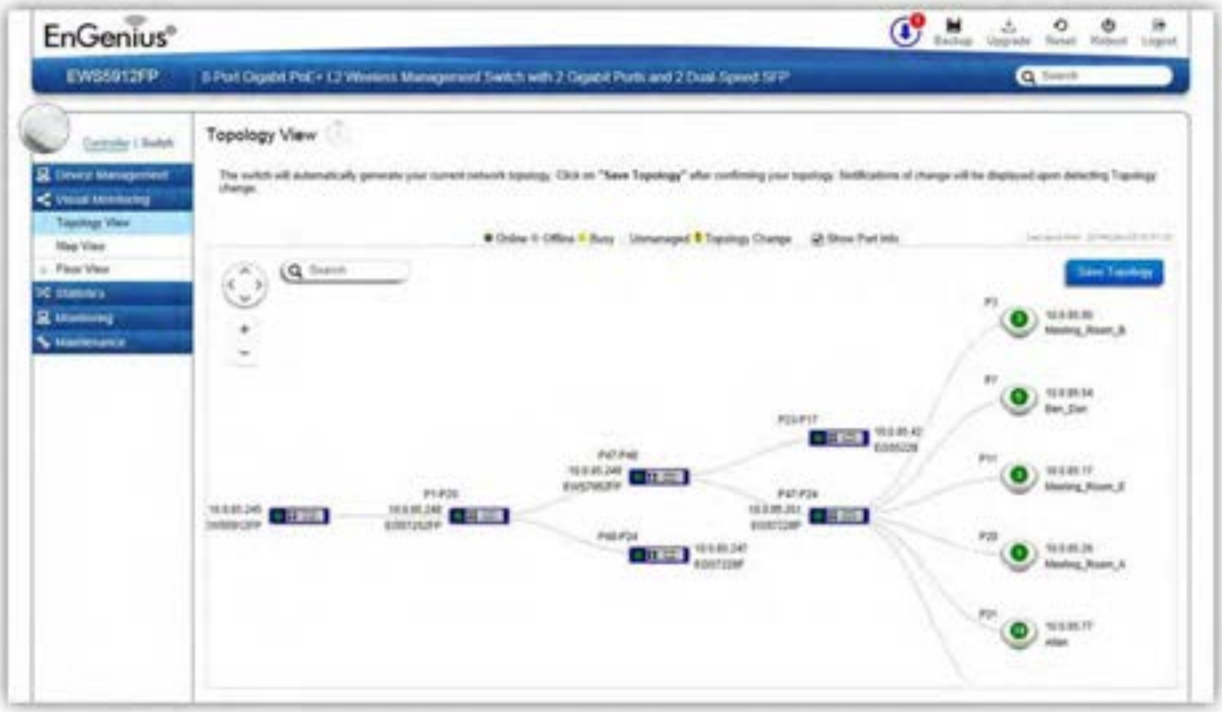
Visual Monitoring

Topology View

Visual Monitoring > Topology View

From here, you can see a visual view of the topology of all supported devices in the network. The EWS Switch automatically maps your network deployment and displays the device relationships across your network infrastructure. An essential feature for troubleshooting network issues that would otherwise require manual mapping, overlay monitoring software, or manually keeping track of MAC address tables.

Use the directional pad and the plus or minus buttons to navigate your view of the network. You can also search Access Points in the network via their IP or MAC address. Check the Show Port Info box to show whether you wish the search query to show port information.



The switch will automatically generate your current network topology. Click on "Save Topology" after confirming your topology. Notifications of change will be displayed upon detecting Topology change.

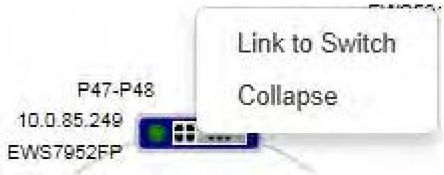
AP Status	Description
Online	The managed AP is currently online
Offline	The managed AP is currently offline
Busy	The managed AP is currently busy (applying new configuration settings)
Unmanaged	The AP is not managed by the controller
Topology Change	There is a change in topology for this device

Navigating Tips

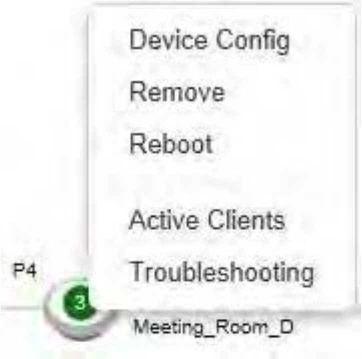
Use ✥ to scroll up, down, left, or right.

Use + − to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.



Left click on the Switch bring up a menu where you can redirect to switch or collapse topology tree.



Left click on the Access Point to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

You can search for an Access Point using the IP Address or MAC address.

Click on ☑ Show Port Info to show or hide port information on the Controller.

Click on Save Topology for the Controller to save the current network topology. Changes will be displayed upon detecting a topology change.

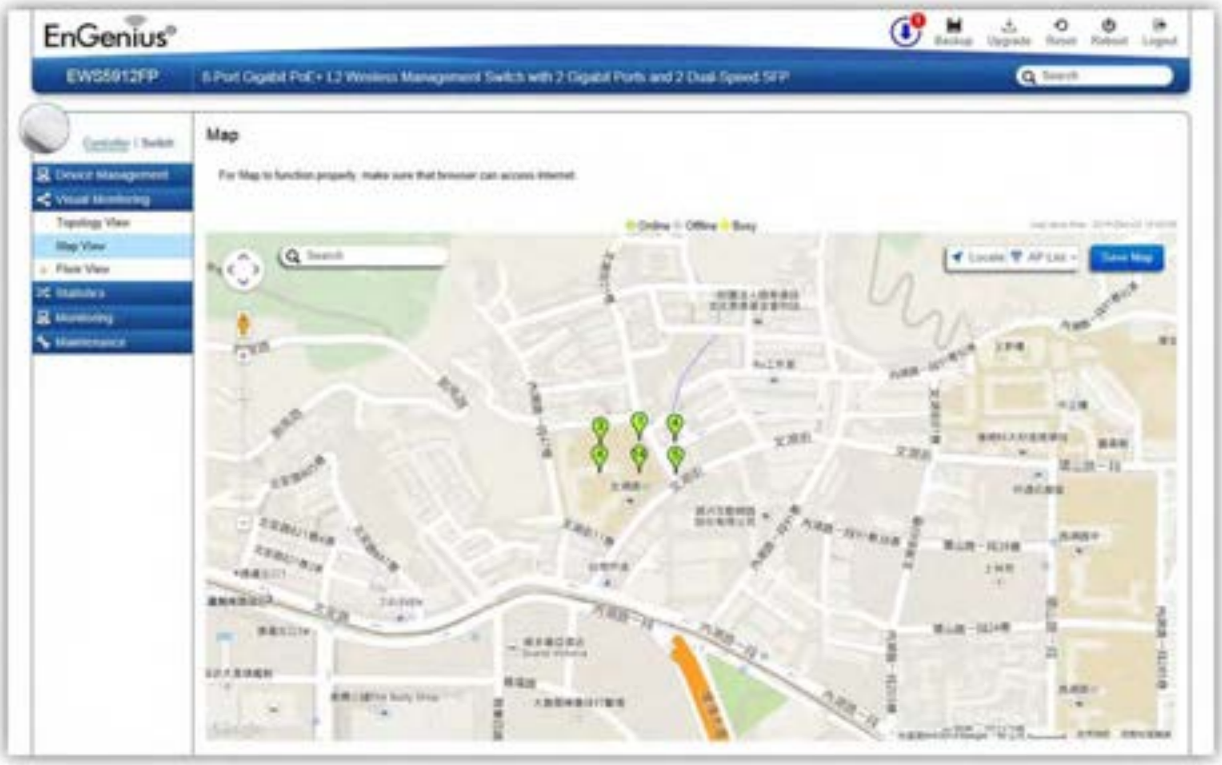
Note: The EWS Switch can only generate topologies with EnGenius L2 Series switches. Non-EnGenius switches will be marked as “Uncontrollable LAN Switches” in the generated topology.

Map View

Visual Monitoring > Map View

From here, you can view a geographical representation of Access Points in the network. Click AP List to display the list of Access Points managed by the EWS switch then simply click-and-drag the AP marker to the desired location on the map.

Note: Your browser need to be able to access the Internet for this function to work.



For Map to function properly, make sure that browser can access Internet.

AP Status	Description
Online	The managed AP is currently online
Offline	The managed AP is currently offline
Busy	The managed AP is currently busy (applying new configuration settings)

Navigating Tips

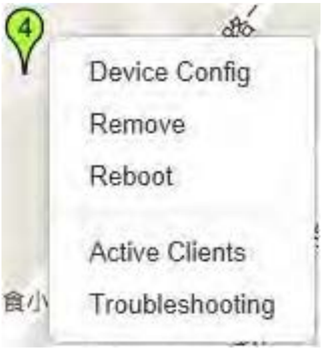
Use ✥ to scroll up, down, left, or right.

Use the slider bar to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Search

Use the **Search box** to search for locations by typing an address or the name of a landmark.

Use the **Locate** button to pinpoint the map to your current location. Note that the location provided is calculated based on your IP address and results might be inaccurate.



Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

Click on Save Map for the settings to take effect.

Floor View

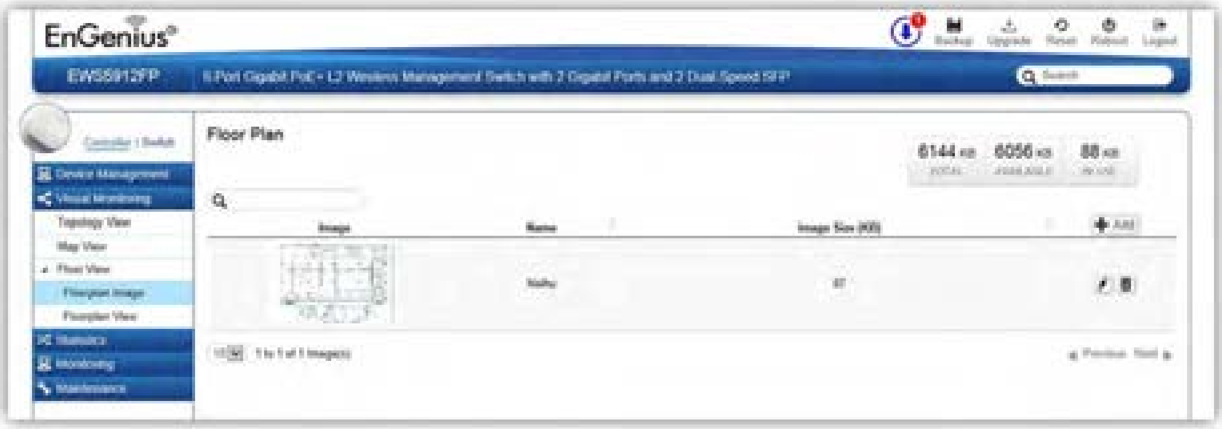
Visual Monitoring > Floor View

The Floor View feature enables an administrator to upload custom floor plans and place AP markers in relevant locations for better network visualization of a wireless network. Multiple images can be uploaded to visualize Access Point placement on multiple floors of an office building or different branch offices within an organization.

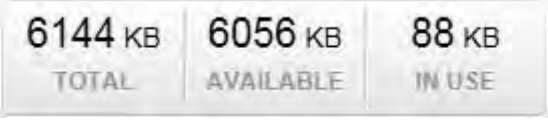
Floorplan Image

Visual Monitoring > Floor View > Floor Plan Image

From here, an administrator can add or delete a custom map or floor plan image. An unlimited number of floor plan images can be imported to the EWS Switch. However, the total
file size of all imported floor plans is limited to 6MB and the maximum file size per image is 512KB (a smaller image loads faster). Valid image file formats are .PNG, .GIF or .JPG.



Status Dashboard
Total: Displays the total memory storage space allocated for uploading custom floor plans.
Available: Display the memory storage space that is currently available.
In Use: Displays the memory storage space that is currently in use.



6144 KB	6056 KB	88 KB
TOTAL	AVAILABLE	IN USE

Add Button
Use the Add Button to import a new image.

+ Add

Edit Button
Use the Edit Button to edit the Name/Description of the imported image.

✎

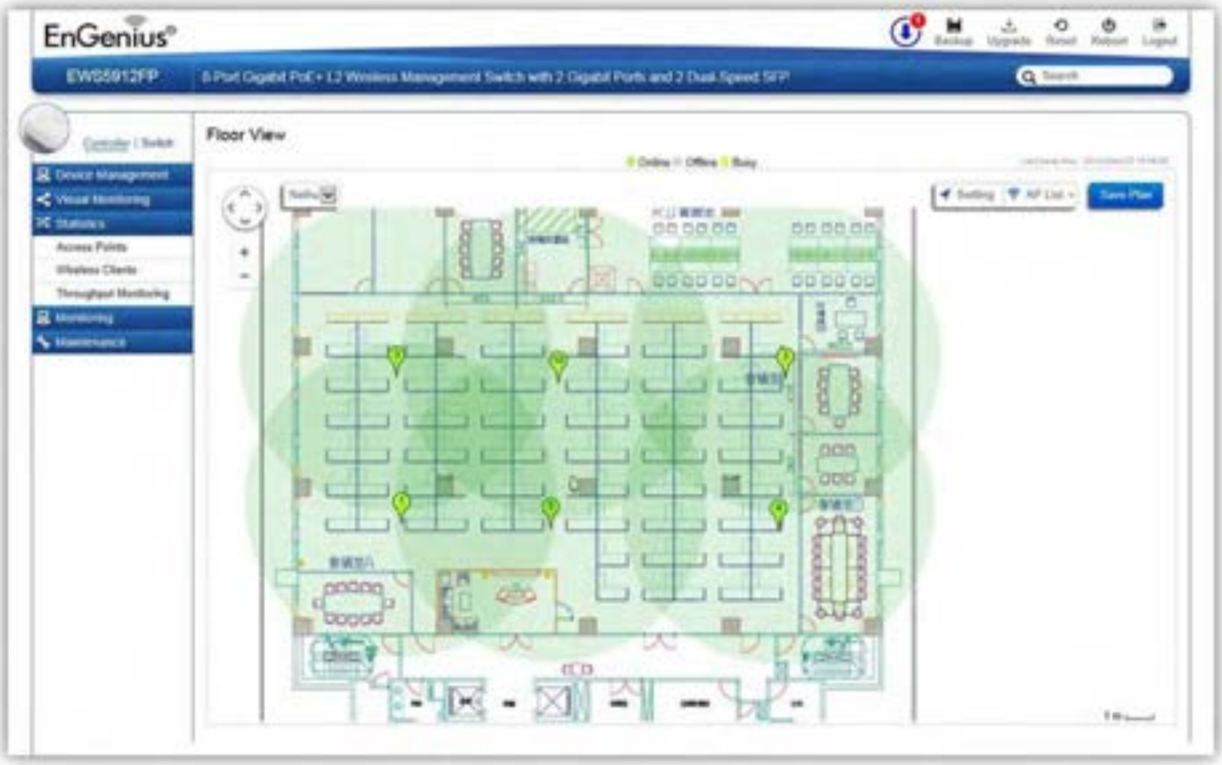
Delete Button
Use the Delete Button to remove the image.

🗑

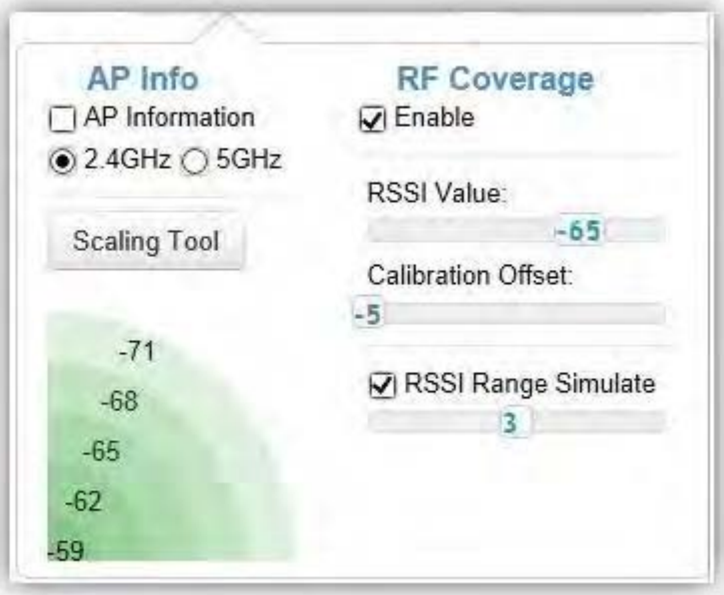
Floorplan View

Visual Monitoring > Floor View > Floor Plan View

After importing your floor plan image, you can distribute markers that represent the APs to the correct locations by clicking on **AP List** and dragging each marker icon to its correct location on the floor plan. Also, Wireless Coverage Display can be toggled on to indicate the coverage range of each AP, assisting IT managers to easily and accurately plan and deploy wireless networks in any indoor environment. Click on **Save Plan** when you're done to save settings.



Settings



AP Info

☐ AP Information

● 2.4GHz ○ 5GHz

Scaling Tool

RF Coverage

☑ Enable

RSSI Value: -65

Calibration Offset: -5

☑ RSSI Range Simulate 3

AP Info
AP Information: Select to toggle on/off AP detailed information to be shown on your floor plan.
2.4GHz / 5GHz: Select whether to display signal coverage of 2.4GHz or 5GHz radio. The wireless coverage displayed will be based on the transmit power settings of the Access Point.

Scaling Tool: Use the scaling tool to determine the exact distance on the floorplan.
Signal Indicator: The colored indicator displays the reference signal strength covered.

RF Coverage
Enable: Select to display wireless coverage on your floor plan.
RSSI Value: Adjust RSSI value to emulate using the slider bar.
Calibration Offset: Use the slider bar to adjust the offset value based on the deployment.
RSSI Range Simulate: Check the **RSSI Simulate** box to display RSSI reference on your floor plan. Adjust RSSI coverage range to emulate using the slider bar.

Navigating Tips

Use ✥ to scroll up, down, left, or right.

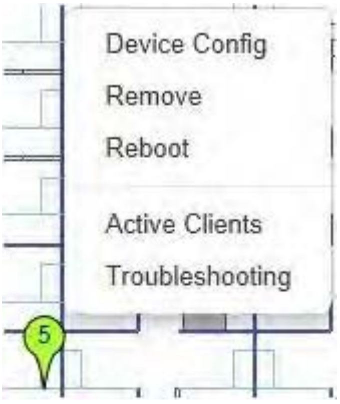
Use + − to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.

AP List ⌄

AP List: Click to reveal a list of APs that the EWS Switch is currently managing.

The number in the marker represents the number of wireless clients that are currently connected to the Access Point.



Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

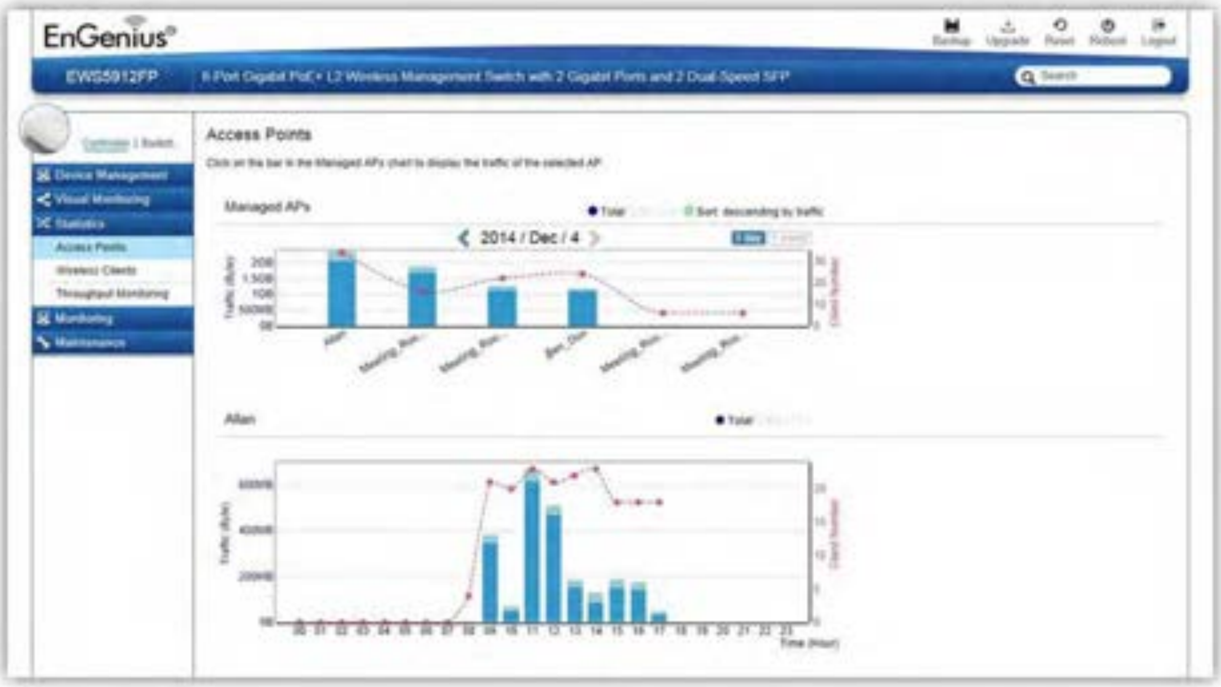
Click on Save Plan for the settings to take effect.

Statistics

Access Points

Statistics > Access Points

The page displays a visual chart of the network traffic of all the Access Points managed by the EWS Switch.



Access Points

Click on the bar in the Managed APs chart to display the traffic of the selected AP

Navigating Tips
Click **Sort** to sort the order from ascending/descending, depending on your preference.

Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

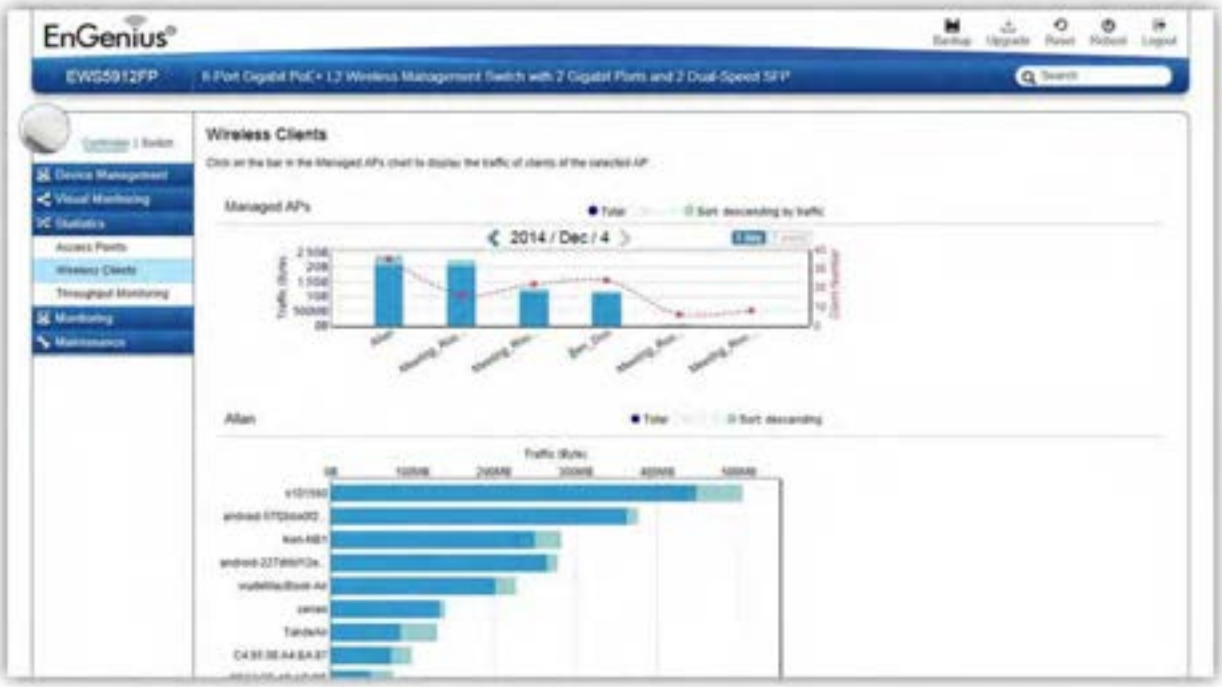
Place the mouse cursor over the bar on the chart to show detailed information.

Click on the bar in the Managed APs chart to display the traffic of the selected AP.

Wireless Clients

Statistics > Wireless Clients

In addition to viewing information based on specific Access Points, you can view data via specific clients as well for security purposes.



Navigating Tips
Click **Sort** to sort the order from ascending/descending, depending on your preference.

Click **Rx** to display Rx transmission, **Tx** to display Tx transmission or **Total** to display combined Rx and Tx transmission.

Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

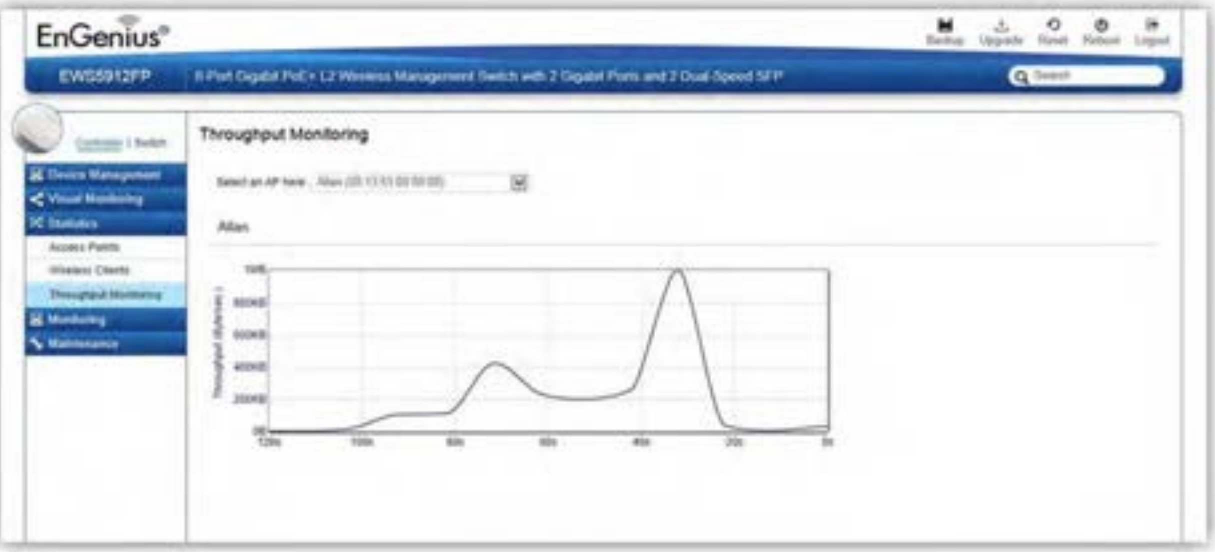
Place the mouse cursor over the bar on the chart to show detailed information.

Click on the bar in the Managed APs chart to display the wireless clients that has associated with the selected AP.

Throughput Monitoring

Statistics > Throughput Monitoring

This page displays the real-time network activity of the selected Access Point.



Throughput Monitoring

Select an AP here : Allan (00:11:11:00:00:00)

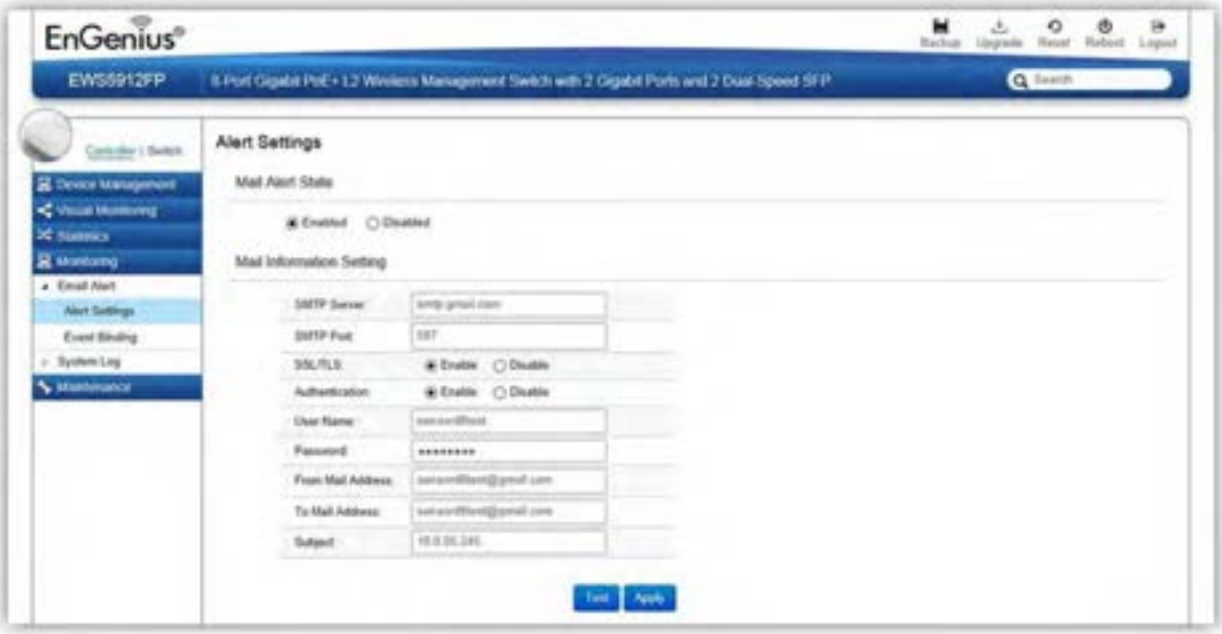
Monitoring

Email Alert

Alert Settings

Monitoring > Email Alert > Alert Settings

If an alert is detected, the EWS Switch will record it in the event log. The EWS Switch can also be configured to send email notifications for selected events.



Alert Settings

Mail Alert State

● Enabled ○ Disabled

Mail Information Setting

SMTP Server	smtp.gmail.com
SMTP Port	587
SSL/TLS	● Enable ○ Disable
Authentication	● Enable ○ Disable
User Name	[illegible]
Password	*********
From Mail Address	[illegible]@gmail.com
To Mail Address	[illegible]@gmail.com
Subject	[illegible]

Mail Alert State: Select whether to Enable/Disable email notification.

Mail Information Setting

- **SMTP Server**: Enter the name of the mail server.
- **SMTP Port**: Enter the SMTP port.
- **SSL/TSL**: Enable this option if your mail server uses SSL/TLS encryption.
- **Authentication**: Select this option to enable authentication.
- **User Name**: Enter the username required by the mail server.
- **Password**: Enter the password required by the mail server.
- **From Mail Address**: Enter the email address that will appear as the sender of the email alert.
- **To Mail Address**: Enter the email address which the EWS Switch will send alarm messages to. You can only send alarm messages to a single email address.
- **Subject**: Enter the subject of the email notification.

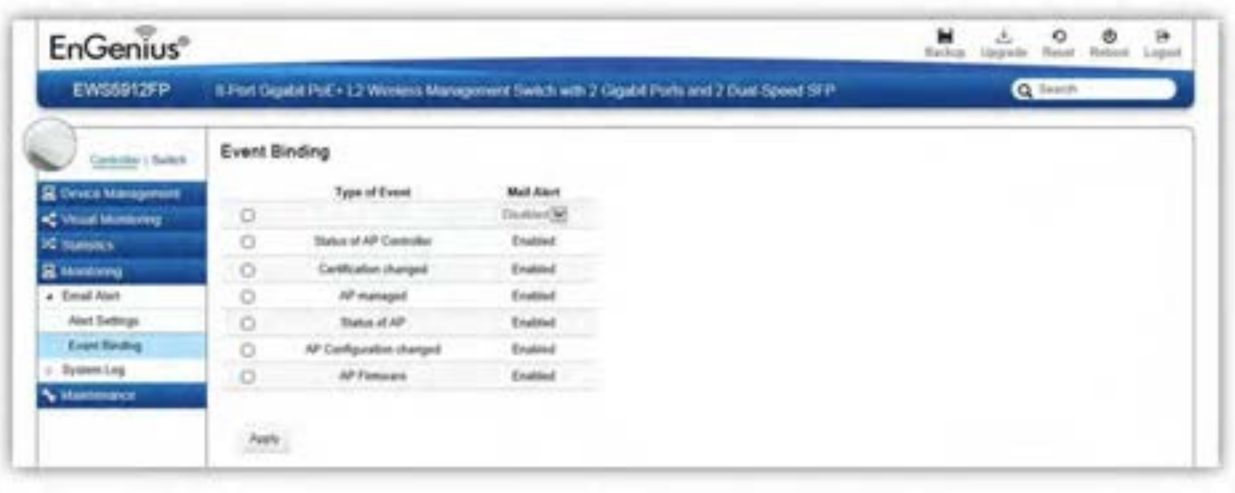
Test: To verify that the EWS Switch can send email notifications using the SMTP settings you configured, click the **Test** button.

Apply: Click **Apply** to save settings.

Event Binding

Monitoring > Email Alert > Event Binding

Use this page to choose which types of events will trigger the EWS Switch to send an email notification. When any of the selected events occur, the EWS Switch sends an email notification to the email address that you specified in the **Monitoring > Email Alert > Alert Settings** section.



Event Binding

	Type of Event	Mail Alert
○		Disabled
○	Status of AP Controller	Enabled
○	Certification changed	Enabled
○	AP managed	Enabled
○	Status of AP	Enabled
○	AP Configuration changed	Enabled
○	AP Firmware	Enabled

The table below provides explanations for EWS Controller syslog event messages.

Event Type	EWS Syslog Message	Severity Level
Status of AP Controller	Controller is enabled	INFO
Status of AP Controller	Controller is disabled	WARNING
Certificate Changed	SSL certificate updated	INFO
Certificate Changed	SSL certificate will expire in {value} days	WARNING
Certificate Changed	SSL certificate has expired	ERROR
Certificate Changed	[AP Name] [AP MAC]'s SSL certificate has been updated	INFO
AP Managed	[AP Name] [AP MAC] added to management list	INFO
AP Managed	[AP Name] [AP IP] removed from management list	INFO
Status of AP	[AP Name] [AP MAC] online	INFO
Status of AP	[AP Name] [AP MAC] reset	INFO
Status of AP	[AP Name] [AP MAC] offline	WARNING
Status of AP	[AP Name] [AP MAC] has invalid IP [IP Address]	WARNING
Status of AP	[AP Name] [AP MAC]'s active client number reaches client limits {value} of [2.4/5]GHz	WARNING
AP Configuration Changed	[AP Name] [AP MAC] configuration updated	INFO
AP Firmware	[AP Name] [AP MAC] firmware version is incompatible	WARNING
AP Firmware	[AP Name] [AP MAC] started to upgrade firmware from [old-ver] to [new-ver]	INFO
AP Firmware	[AP Name] [AP MAC] firmware upgrade failed	ERROR

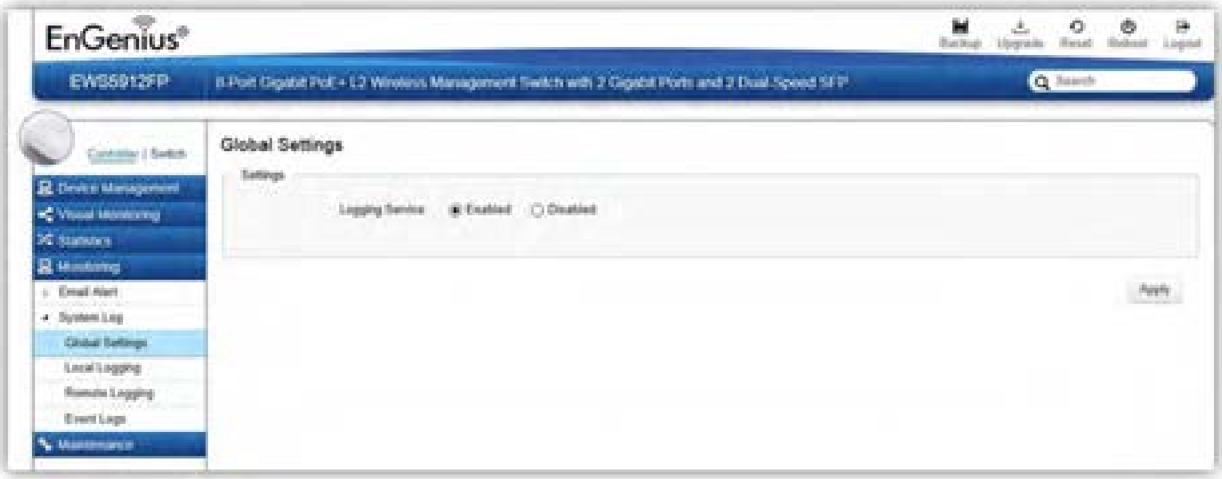
System Log

Monitoring > System Log

Global Settings

Monitoring > System Log > Global Settings

From here, you can Enable or Disable the Log settings for the EWS Switch.



Global Settings

Settings

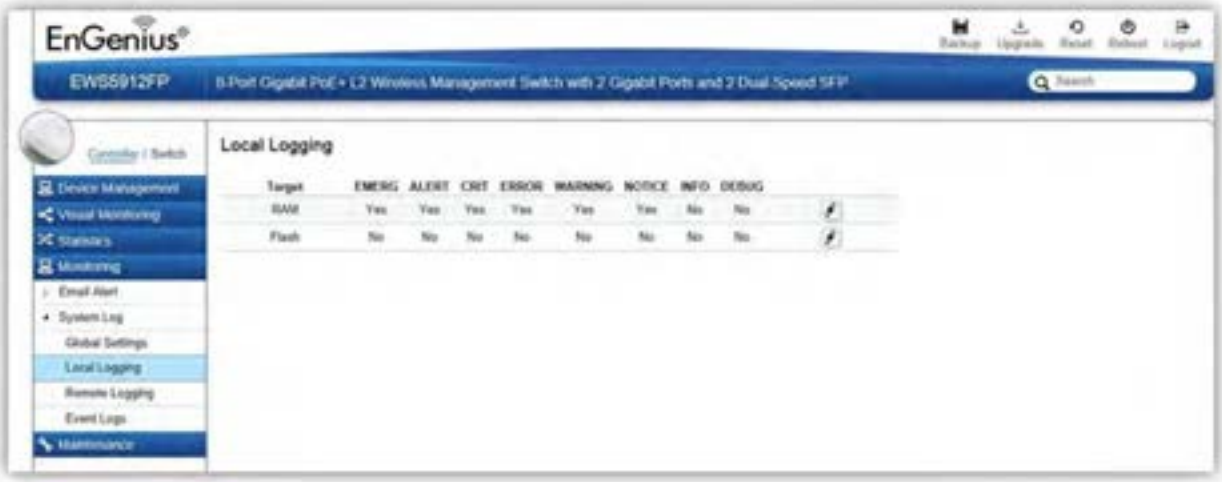
Logging Service ● Enabled ○ Disabled

Local Logging

Monitoring > System Log > Local Logging

The System Log is designed to monitor the operation of the EWS Switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

The EWS Switch supports log output to two directions: Flash and RAM. The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's Flash will be kept effective even if the Switch is rebooted or powered off. The log has a fixed capacity; at a certain level, the EWS Switch will start deleting the oldest entries to make room for the newest.



Local Logging

Target	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG
RAM	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Flash	No	No	No	No	No	No	No	No

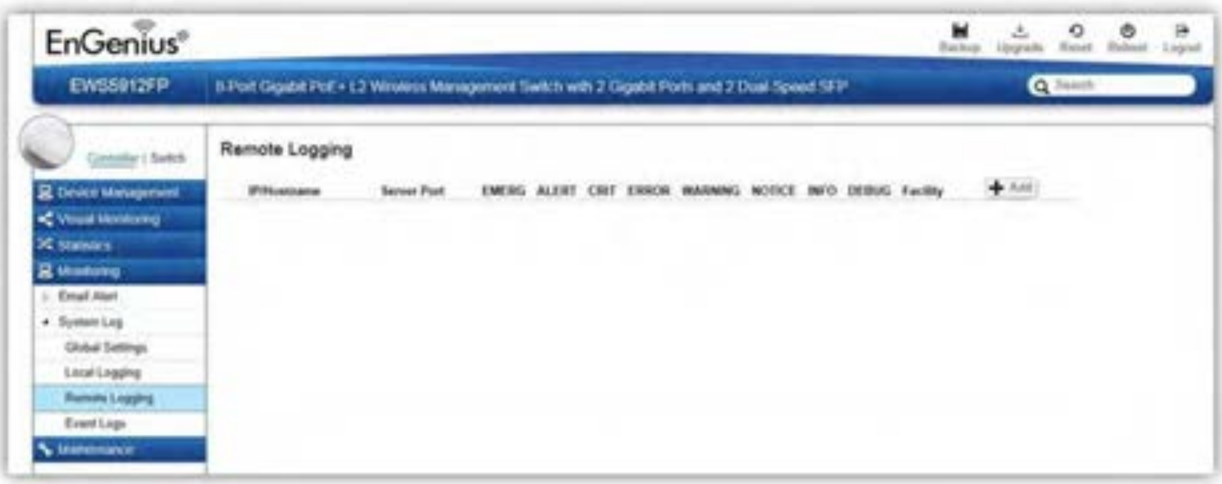
Severity Level
RFC 5424 defines eight severity levels:

Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	ALERT	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFO	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.

Remote Logging

Monitoring > System Log > Remote Logging

The internal log of the EWS Switch has a fixed capacity; at a certain level, the EWS Switch will start deleting the oldest entries to make room for the newest. If you want a permanent record of all logging activities, you can set up your syslog server to receive log contents from the EWS Switch. Use this page to direct all logging to the syslog server. Click the Add button, define your syslog server, and select the severity level of events you wish to log.



Remote Logging

IP/Hostname	Server Port	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG	Facility

IP/Hostname
Specify the IP address or host name of syslog server.

Server Port
Specify the port of the syslog server. The default port is 514.

Severity Level
RFC 5424 defines eight severity levels:

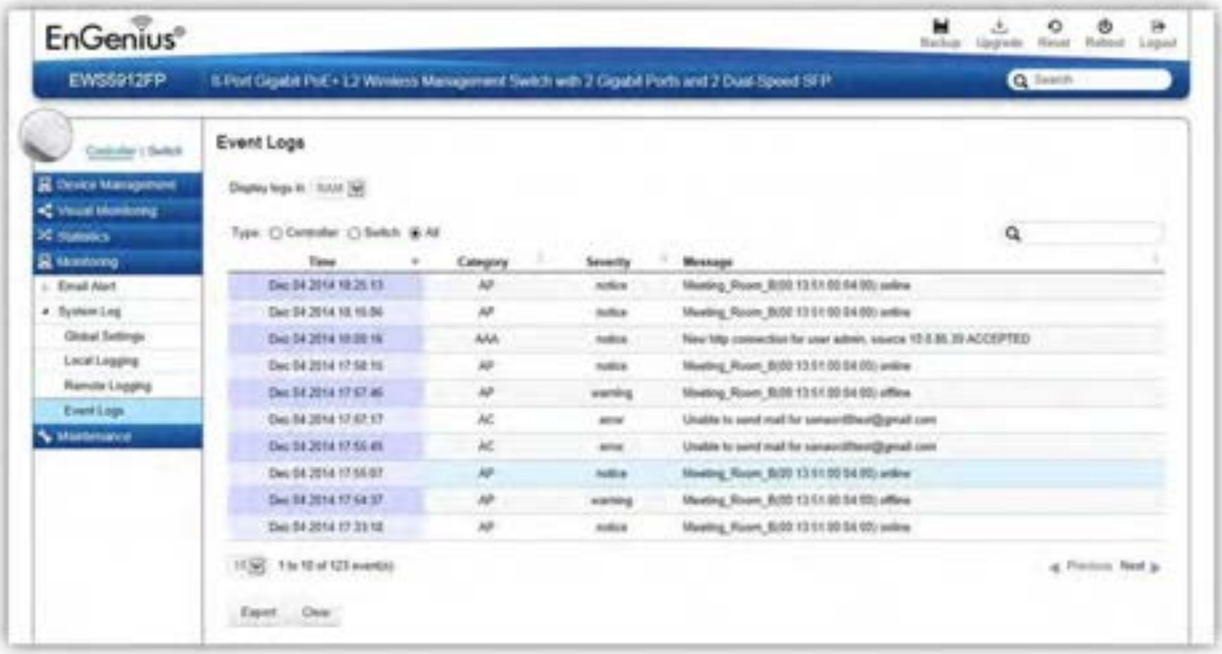
Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	ALERT	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFO	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.

Facility
The log facility is used to separate out log messages by application or by function, allowing you to send logs to different files in the syslog server. Use the drop-down menu to select local0, local1, local2, local3, local4, local5, local6, or local7.

Event Logs

Monitoring > System Log > Event Logs

This page displays the most recent records in the EWS Switch's internal log. Log entries are listed in reverse chronological order (with the latest logs at the top of the list). Click a column header to sort the contents by that category.



Event Logs

Display logs in: RAM

Type: ○ Controller ○ Switch ● All

Time	Category	Severity	Message
Dec 04 2014 18:25:13	AP	notice	Meeting_Room_B(00 13:51:00 04:00) online
Dec 04 2014 18:16:06	AP	notice	Meeting_Room_B(00 13:51:00 04:00) online
Dec 04 2014 18:08:16	AAA	notice	New http connection for user admin, source 10.0.86.39 ACCEPTED
Dec 04 2014 17:58:15	AP	notice	Meeting_Room_B(00 13:51:00 04:00) online
Dec 04 2014 17:57:46	AP	warning	Meeting_Room_B(00 13:51:00 04:00) offline
Dec 04 2014 17:57:17	AC	error	Unable to send mail for [illegible]@gmail.com
Dec 04 2014 17:55:45	AC	error	Unable to send mail for [illegible]@gmail.com
Dec 04 2014 17:55:07	AP	notice	Meeting_Room_B(00 13:51:00 04:00) online
Dec 04 2014 17:54:37	AP	warning	Meeting_Room_B(00 13:51:00 04:00) offline
Dec 04 2014 17:33:18	AP	notice	Meeting_Room_B(00 13:51:00 04:00) online

10 1 to 10 of 123 event(s)

Display logs in

- **RAM**: The information stored in the system’s RAM log will be lost after the Switch is rebooted or powered off
- **Flash**: The information stored in the system’s Flash will be kept effective even if the Switch is rebooted or powered off.

Type:

- **Controller**: Display controller related logs.
- **Switch**: Display switch related logs.
- **All**: Display logs for both controller and switch.

Export
Click Export button to export the current buffered log to a .txt file.

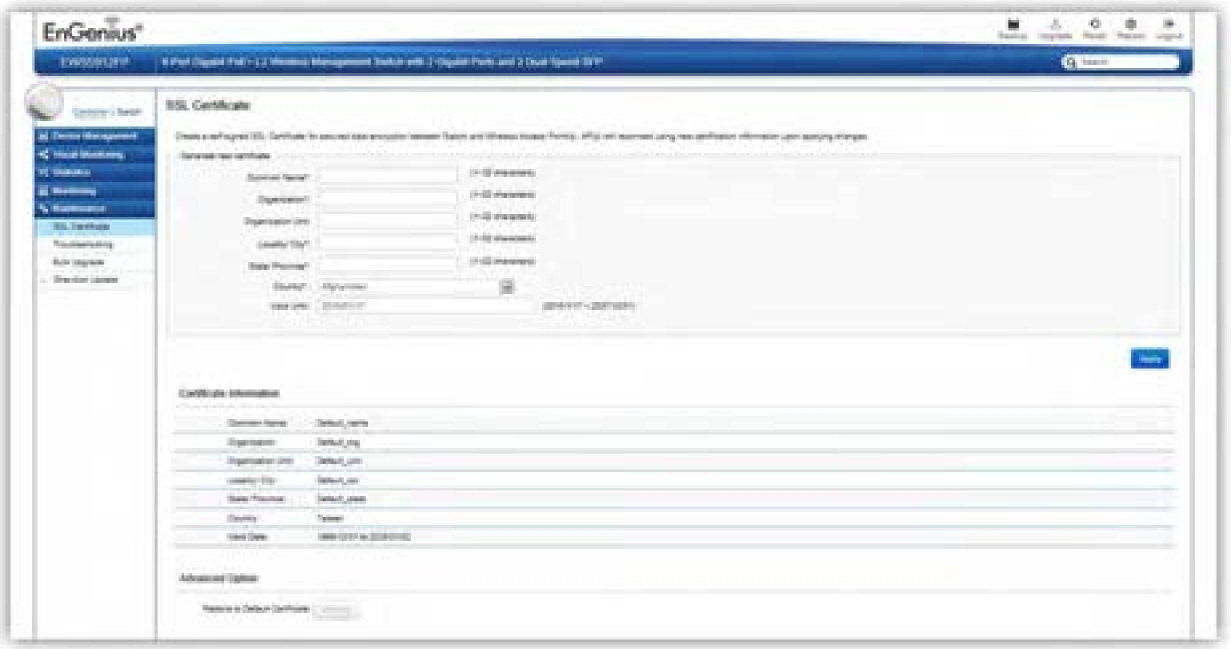
Clear
Click Clear button to clear the buffered log in the system's memory.

Maintenance

SSL Certificate

Maintenance > SSL Certificate

SSL certificates enables device or user identification, as well as secure communications. Administrators can create a self-signed SSL Certificate to secure communications between the Switch and Access Points. Note that Access Points will disconnect and reconnect using new certificate upon applying changes.



Generate New Certificate
Enter the information below to generate a request for an SSL certificate for the controller.

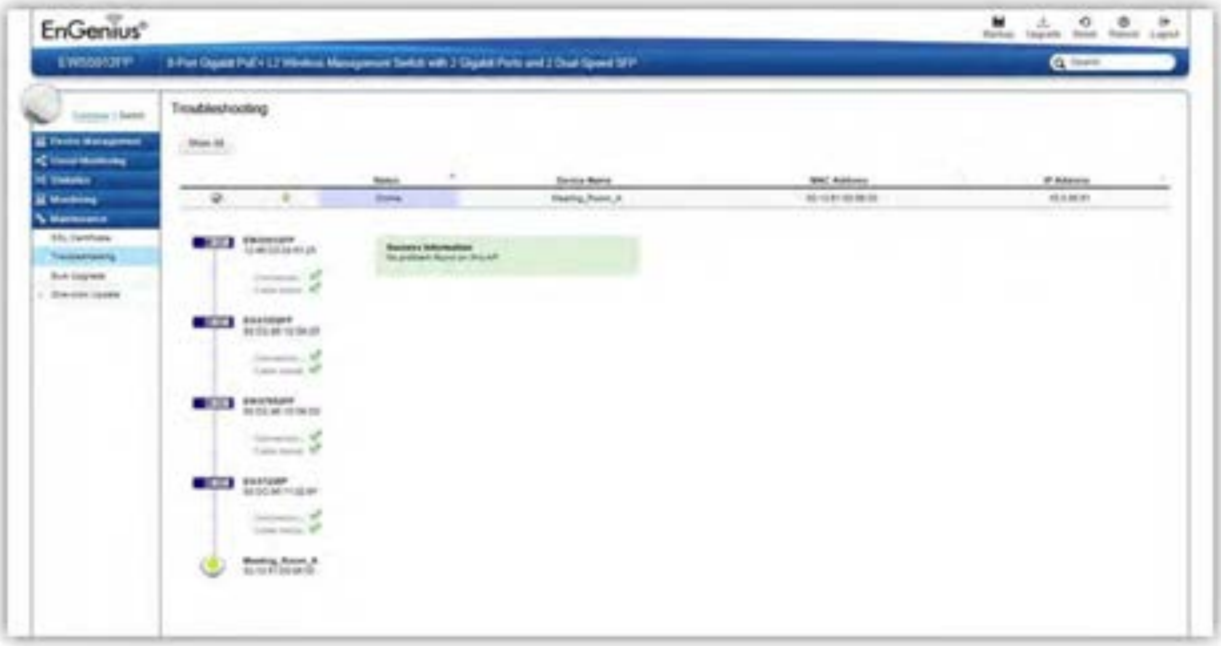
Common Name	Enter the name of the request.
Organization	Enter the organizations name.
Organization Unit	Enter a unit name (department, etc.).
Locality/City	Enter the locality or city.
State/Province	Enter the state or province.
Country	Enter the name of the country.
Valid Date	Enter the expiry date of the certificate.

Restore to Default Certificate
Click on Restore button under Advance Options to restore the default SSL Certificate settings.

Troubleshooting

Maintenance > Troubleshooting

From here, you can troubleshoot any issues you have with Access Points connected to the network. This feature is designed primarily for administrators to verify and test the link route between the Switch and the Access Point. A troubleshooting solution is provided by the system so that administrators can know where the problem lies. Note that the topology of the network needs to be saved for this function to work properly.

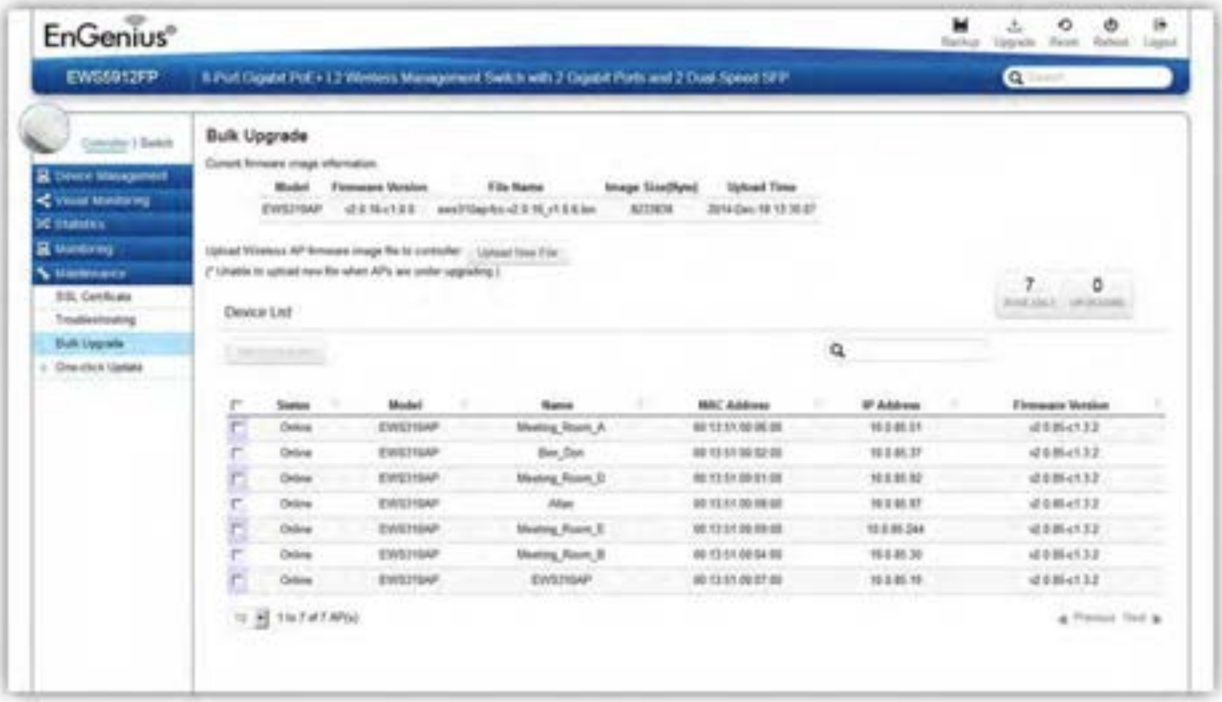


Choosing an Access Point to Diagnose
A list will show the current status of Access Points on the network. Select an Access Point to begin a diagnostic test. If multiple Access Points are connected, use the search bar to the top right of the page to find the Access Point you wish to troubleshoot. The controller will run a diagnostic test for the selected Access Point. Click Start to run the test. The test take a few seconds to complete. Afterwards, the results will display on the page.

Bulk Upgrade

Maintenance > Bulk Upgrade

The Bulk Upgrade feature allows administrators to upgrade the firmware of multiple Access Points at the same time. After uploading the firmware of an AP, the system will automatically display a list of Access Points the system is currently managing that the uploaded firmware is for.



Bulk Upgrade

Current firmware image information

Model	Firmware Version	File Name	Image Size(Byte)	Upload Time
EWS310AP	v2.0.16-c1.0.0	ews310ap-fcc-v2.0.16_c1.0.0.bin	8233836	2014-Dec-18 13:30:07

Upload Wireless AP firmware image file to controller: Upload New File
(* Unable to upload new file when APs are under upgrading.)

Device List

□	Status	Model	Name	MAC Address	IP Address	Firmware Version
□	Online	EWS310AP	Meeting_Room_A	[illegible]	10.0.85.11	v2.0.85-c1.3.2
□	Online	EWS310AP	Ben_Don	[illegible]	10.0.85.37	v2.0.85-c1.3.2
□	Online	EWS310AP	Meeting_Room_D	[illegible]	10.0.85.82	v2.0.85-c1.3.2
□	Online	EWS310AP	Allan	[illegible]	10.0.85.97	v2.0.85-c1.3.2
□	Online	EWS310AP	Meeting_Room_E	[illegible]	10.0.85.244	v2.0.85-c1.3.2
□	Online	EWS310AP	Meeting_Room_B	[illegible]	10.0.85.30	v2.0.85-c1.3.2
□	Online	EWS310AP	EWS310AP	[illegible]	10.0.85.19	v2.0.85-c1.3.2

10 1 to 7 of 7 AP(s)

To upgrade, please follow the steps below:

1. Click on Upload New File to mount AP firmware onto EWS Switch flash
2. Once the Access Point firmware is uploaded onto the Controller, the list of Access Points that the uploaded firmware is for will appear in the Device List.
3. Select the Access Points you wish to upgrade and click Add to Upgrade to start the firmware upgrading process.

NOTE: Upgrading APs will temporarily disconnect them (and any associated clients) from the network. To minimize network disruption, we recommend performing the firmware upgrading procedure at an off-peak time.

One-Click Update

Maintenance > One-Click Update

The EWS Switch can be configured to automatically check for new firmware updates for your EWS devices. The icon below will appear on the upper right corner of the user interface when a new update is available. Simply click on the icon and follow the on screen instructions to update your devices.

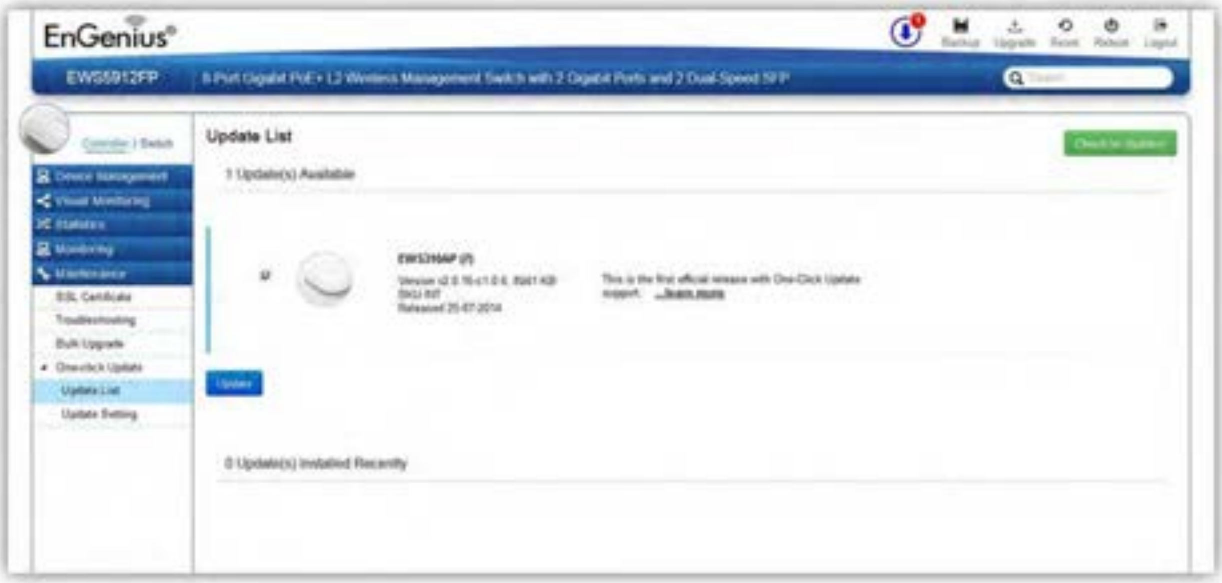
Note: An active Internet connection is required for this feature.

Update List

Maintenance > One-Click Update > Update List

This page displays the devices which has new firmware updates available. A release note states the purpose of the firmware. Click on Check for Updates for the EWS Switch to check for the latest firmware. Select the devices you wish to update and click on Update button to begin the updating process.

Note: Both the EWS Switch and the browser on the PC must be able to access the Internet for this function to work. One Click Update might also not be available if you are using a proxy server for Internet connections.



Update List

1 Update(s) Available

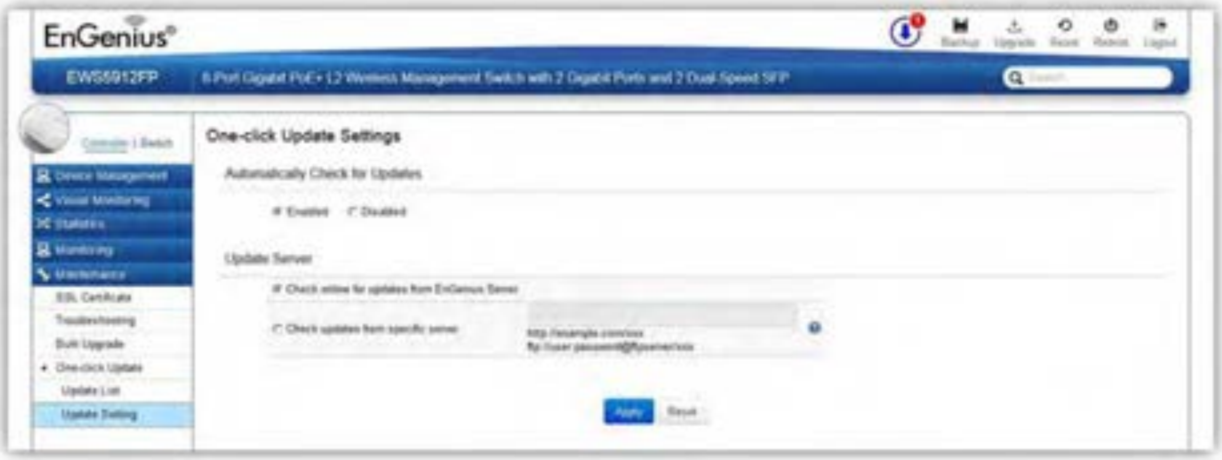
☑ EWS310AP (?)
Version v2.0.16-c1.0.6, 8561 KB
SKU INT
Released 25-07-2014

This is the first official release with One-Click Update support. ...learn more

0 Update(s) Installed Recently

Update Settings

Maintenance > One-Click Update > Update Settings



One-click Update Settings

Automatically Check for Updates

● Enabled ○ Disabled

Update Server

● Check online for updates from EnGenius Server

○ Check updates from specific server http://example.com/xxx ftp://user:password@ftpserver/xxx

Automatically Check for Updates
Enable/disable automatically check for new updates for your devices.

Update Server
Choose whether you wish to check for updates from EnGenius server or specify your own http/ftp server path.

Check updates from specific server
Apart from copying firmware image files into the specific http/ftp path, an index file is required in the same folder.

Follow the instructions below for creating the index file.

1. Create a new .txt file with the name "*lastfwlist.txt*".
2. In the file, create entries based on the format below and save the file.
   <Model Name>,<Firmware Version>,<File Name>,<MD5>,<SKU>

Field	**Description**	**Reference String**
Model Name	Enter model name.	*EWS310AP, EWS320AP, EWS660AP*
Firmware Version	Enter firmware version.	*v2.0.129-c1.3.5*
File Name	Enter complete filename with extension.	*ews310ap-fcc-v2.0.132.0-c1.3.5.bin*
MD5	Enter MD5 value of the firmware image	*4959e8d68536227d182b53a719dcdae4*
SKU	Enter in device SKU.	*FCC, ETSI, INT*

Example:

```
EWS210AP,v2.0.129-c1.3.5,ews210ap-fcc-v2.0.129.0-c1.3.5.bin,af44f429a5404e2f7bde651921366c33,FCC
EWS210AP,v2.0.129-c1.3.5,ews210ap-etsi-v2.0.129.0-
c1.3.5.bin,186cab281b7038e7c9b8909acfd9e63e,ETSI
EWS310AP,v2.0.132-c1.3.5,ews310ap-fcc-v2.0.132.0-
c1.3.5.bin,4959e8d68536227d182b53a719dcdae4,FCC
EWS310AP,v2.0.132-c1.3.5,ews310ap-etsi-v2.0.132.0-
c1.3.5.bin,0ee6663cc9b6c652b1139214455ed92e,ETSI
EWS320AP,v2.0.132-c1.3.5,ews320ap-fcc-v2.0.132.0-c1.3.5.bin,e584a03d0218a0f1a29a4c5550c99614,FCC
EWS320AP,v2.0.132-c1.3.5,ews320ap-etsi-v2.0.132.0-
c1.3.5.bin,967312acc588b6caad7e55a98fc19997,ETSI
EWS360AP,v2.0.130-c1.3.5,ews360ap-fcc-v2.0.130.0-c1.3.5.bin,3bff8f450f171c0f839032124cbe4860,FCC
EWS360AP,v2.0.130-c1.3.5,ews360ap-etsi-v2.0.130.0-
c1.3.5.bin,e2483bfc74259263dda18e8d86682183,ETSI
EWS660AP,v2.0.124-c1.3.5,ews660ap-int-v2.0.124.0-c1.3.5.bin,cc00b2871dec668b9a1b82f330a2611e,FCC
EWS660AP,v2.0.124-c1.3.5,ews660ap-etsi-v2.0.124.0-c1.3.5.bin,d67554b30fd98d06093f7da306cb8fd2,ETSI
EWS860AP,v2.0.124-c1.3.5,ews860ap-fcc-v2.0.124.0-c1.3.5.bin,39f5f935f7b83515c4a6c30ef4c61114,FCC
EWS860AP,v2.0.124-c1.3.5,ews860ap-etsi-v2.0.124.0-c1.3.5.bin,5b905debcce6696ffa1a7957faf77f19,ETSI
```

Appendix

Appendix A

Professional Installation Instructions

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 setting.

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. External Antenna

Only use the antennas which have been approved by the applicant. Any non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and therefore is prohibited.

4. Installation Procedure

Please refer to the user's manual for details.

5. 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. Antenn Externe.

Utiliser uniiquement les antennes approuvees par le fabricant. L’utilisation d’autres antennes peut conduire a un niveau de rayonnement essentiel ou non essentiel depassant les niveaux limites definis par FCC/IC, ce qui est interdit.

4. Procedure D’installation

Consulter le manuel d’utilisation.

5. 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 B

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 C

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.

FOR MOBILE DEVICE USAGE

Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21cm between the radiator & your body.

Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 21cm de distance entre la source de rayonnement et votre corps.

Appendix D

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.

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.