

User Manual

Gigabit Managed Smart Switch with Wireless Controller



EWS Switch Series

version 1.5

IMPORTANT

To install this device please refer to the Quick Installation Guide included in the product packaging.

Table of Contents

Product Overview	7
Introduction	8
Key Features	9
System Requirements	10
Package Contents	10
LED's behavior for EWS Switch.....	11
Technical Specifications.....	13
Getting Started.....	16
Installing the Switch	17
Management Interface	17
Connecting the Switch to a Network	18
Software Features	20
Using the Switch.....	21
Wireless Controller Features.....	22
Managing EWS Access Points.....	22
Device Management	24
Summary	24
Access Points.....	26
Access Point Settings.....	31
AP Groups.....	44
Access Control.....	46
Wireless Services.....	48
Monitor	49
Active Clients.....	49
Rogue AP Detection	51
System Log	53
Email Alert.....	58
Visualization	62
Topology View	62
Map View	65
Floor View	67
Statistics	72

Access Points.....	72
Wireless Clients.....	73
Real Time Throughput.....	74
Hotspot Services	75
Captive Portal.....	75
Guest Account.....	77
Maintenance	78
Schedule Tasks	78
Troubleshooting	79
Bulk Upgrade.....	80
One-Click Update	81
SSL Certificate.....	84
Check Codes	86
Migration to ezMaster	87
Ethernet Switch Features.....	88
System.....	88
Summary	88
IP Settings.....	89
System Time	92
Port Settings.....	94
PoE	96
EEE.....	99
L2 Feature.....	100
Link Aggregation.....	100
STP.....	107
MAC Address Table	118
LLDP.....	120
IGMP Snooping	124
MLD Snooping.....	130
Jumbo Frame.....	133
VLAN.....	134
802.1Q.....	135
PVID.....	136
Management VLAN	138

Voice VLAN	139
Management.....	142
System Information	142
User Management	143
Dual Image	144
SNMP.....	145
ACL	154
MAC ACL.....	155
MAC ACE	156
IPv4 ACL.....	158
IPv4 ACE	159
IPv6 ACL.....	161
IPv6 ACE	162
ACL Binding	164
QoS.....	165
Global Settings	166
CoS Mapping	167
DSCP Mapping.....	168
Port Settings	169
Storm Control.....	171
Security	173
802.1x.....	173
RADIUS Server.....	177
Access.....	178
Port Security.....	182
Port Isolation.....	183
DoS.....	184
Monitoring	186
Port Statistics.....	186
RMON.....	187
Log.....	192
Diagnostics	197
Cable Diagnostics	197
Ping Test	198

IPv6 Ping Test	199
Trace Route	200
Maintenance	201
Configuration Manager	201
Firmware Upgrade	202
Appendix.....	203
Appendix A - Federal Communications Commission (FCC) EMC Statement.....	204
Appendix B - IC Interference Statement	204
Appendix C - EU Declaration of Conformity.....	205

Chapter 1

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 effortlessly 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 both a Wireless Controller as well as a Layer 2 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 Point 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.

Key Features

- > 10/100/1000 Mbps Gigabit Ethernet Ports
- > Dedicated SFP / SFP+ slots for longer connectivity via fiber uplinks and for uplink redundancy and failover
- > IGMP and MLD snooping provides advanced multicast filtering
- > IEEE802.3ad Link Aggregation
- > STP/RSTP/MSTP
- > Access Control List/ Port Security
- > IEEE802.1X and RADIUS Authentication
- > RMON
- > SNMP v1/v2c/v3
- > Voice VLAN for fast and reliable deployment of VoIP
- > Energy Efficient Ethernet (IEEE802.3az) support for better energy saving when more EEE-compliant end devices are available in the market
- > Advanced QoS with IPv4/IPv6 ingress traffic filtering (ACLs) and prioritization
- > Easy to manage via Web-Based Management GUI for switch deployment
- > Standard-based technology, ensuring interoperability with any standard-based devices in the existing network
- > Dual firmware images, improving reliability and uptime for your network

System Requirements

The following are the minimum system requirements in order to configure the device:

- > Computer with an Ethernet interface or wireless network capability
- > Windows OS (XP, Vista, 7, 8, 10), Mac OS, or Linux-based operating systems
- > Web-Browsing Application (i.e. Internet Explorer, Firefox, Chrome, Safari, or another similar browser application)

Package Contents

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

[EWS2908P, EWS2910P](#)

- > EnGenius Switch
- > Power Adapter / Power Cord
- > Rubber Footpads
- > Wall-mount Kit
- > Quick Installation Guide

[EWS5912FP, EWS7928P, EWS1200-28TFP, EWS7926EFP, EWS7952P, EWS7952FP](#)

- > EnGenius Switch
- > Power Cord
- > RJ-45 Console Cable
- > Rack-mount Kit
- > Quick Installation Guide

LED's behavior for EWS Switch

EWS1200-28TFPv2 /EWS7928Pv2/EWS7952FPv3					
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps	
		Off	Light off	Speed 100 Mbps/10 Mbps	
	PoE Mode	Green	Solid Light	Power feeding	
		Off	Light off	No Power feeding	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
			Light off	No Link	
LED Per SFP Port	Speed	Green	Solid Light	Speed 1 Gbps	
		Off	Light off	No Link/Speed 100 Mbps	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
				Light off	No Link

EWS7952Pv2					
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps	
		Off	Light off	Speed 10 Mbps	
	PoE Mode	Green	Solid Light	Power feeding	
		Off	Light off	No Power feeding	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
			Light off	No Link	
LED Per SFP Port	Speed	Green	Solid Light	Speed 1 Gbps	
		Amber	Solid Light	Speed 100 Mbps	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
				Light off	No Link

EWS2908P/ EWS2910Pv2/ EWS5912FPv2

LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps
		Amber	Solid Light	Speed 100 Mbps
		Off	Light off	Speed 10 Mbps
	PoE Mode	Green	Solid Light	Power feeding
		Amber	Solid Light	Error Condition
		Off	Light off	No Power feeding
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
LED Per SFP Port	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

Technical Specifications

General

	EWS2908P	EWS2910P	EWS5912FP	EWS7928P	EWS1200-28T FP	EWS7926E P
10/100/1000Mbps Ports	8	8	10	24	24	24
100/1000Mbps SFP Slots	-	2	2	4	4	2 (10G)
RJ45 Console Ports	-	-	1	1	1	1
PoE Standard	IEEE 802.3 af			IEEE 802.3 af/at		
PoE Capable Ports	Port 1-8	Port 1-8	Port 1-8	Port 1-24	Port 1-24	Port 1-24
Total PoE Power Budget	55w	55W	130W	250W	410W	410W
Switching Capacity	16Gbps	20Gbps	24Gbps	56Gbps	56Gbps	88Gbps
Forwarding Mode	Store-and-Forward					
Packet Buffer Memory	512 KB	512 KB	512 KB	512 KB	512 KB	1.5MB
Mac Address Table Size	8K	8K	8K	8K	8K	16K
Jumbo Frame Size	9K	9K	9K	9K	9K	9K

	EWS7952P	EWS7952FP
10/100/1000Mbps Ports	48	48
100/1000Mbps SFP Slots	4	4
RJ45 Console Ports	1	1
PoE Standard	IEEE 802.3 af/at	
PoE Capable Ports	Port 1-48	Port 1-48
Total PoE Power Budget	410W	740W
Switching Capacity	104Gbps	104Gbps
Forwarding Mode	Store-and-Forward	
Packet Buffer Memory	1.5 MB	1.5 MB
Mac Address Table Size	16K	16K
Jumbo Frame Size	9K	9K

Software Features

Wireless Management Features

Access Point Auto Discovery and Provisioning
Access Point Auto IP Assignment
Access Point Group 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)
Configuration Import / Export

L2 Features

802.3ad Link Aggregation
- Maximum of 8 groups/8 ports per group
Port Mirroring
- One-to-One
- Many-to-One
Spanning Tree Protocol
- 802.1D Spanning Tree Protocol (STP)
- 802.1w Rapid Spanning Tree Protocol (RSTP)
- 802.1s Multiple Spanning Tree Protocol (MSTP)
MAC Address Table
- 8K entries
Static MAC Address

- 256 entries
802.1ab Link Layer Discovery Protocol
IGMP Snooping
- IGMP v1/v2/v3 Snooping
- Supports 256 IGMP groups
- IGMP per VLAN
- IGMP Snooping Querier
- IGMP Snooping Fast Leave
MLD Snooping
- MDL Snooping v1/v2
- Supports 256 MLD groups
- IGMP per VLAN
Jumbo Frame
- Up to 9216 bytes
802.3x Flow Control
802.3az Energy Efficient Ethernet

VLAN

802.1Q support
VLAN Group
- Max 4094 static VLAN groups
Voice VLAN

QoS

802.1p Quality of Service
- 8 queues per port
Queue Handling
- Strict
- Weighted Round Robin (WRR)
QoS based on:
- 802.1p Priority
- DSCP
Bandwidth Control
- Port-based (Ingress/Egress, 64 Kbps~1000 Mbps)
Broadcast/Unknown Multicast/ Unknown Unicast
Storm Control

Access Control List (ACL)

Layer 2/3
- Support maximum 32 entries (ACL)
- Support maximum 256 entries (ACE)
ACL based on:
- MAC address
- VLAN ID

- 802.1p priority
- Ethertype
- IP address
- Protocol type
- DSCP

Security

802.1X

- Guest VLAN
 - Port-based Access Control
- Supports RADIUS Authentication
- Port Security
- up to 256 MAC Addresses per port
- Port Isolation
- DoS Attack Prevention
- BPDU Attack Prevention

Monitoring

- Port Statistics
- System Log
- RMON

Management

- Web Graphical User Interface (GUI)
- Command Line Interface (CLI)
- BootP/DHCP Client/DHCPv6 Client
- SSH Server
- Telnet Server
- TFTP Client
- HTTPS
- SNMP
- Supports v1/v2c/v3
- SNMP Trap
- SNTP
- Configuration restore/backup
- Dual Images

Diagnostic

- Cable Diagnostic
- Ping Test
- Trace Route

MIB/RFC Standards

- RFC1213
- RFC1493

- RFC1757
- RFC2674
- RFC 2863

Environment Specifications

Operating Temperature

- 0 to 40°C (EWS2910P, EWS2908P)
- 0 to 50°C (EWS5912FP, EWS7928P, EWS1200-28TFP, EWS7926EFP, EWS7952P, EWS7952FP)

Storage Temperature

- 40°C to 70°C

Humidity (Non-condensing)

- 5% - 95%

Physical Specifications

Dimensions (W x D x H)

- EWS2908P: 240x105x27mm
- EWS2910P: 240x105x27mm
- EWS5912FP: 330x230x44mm
- EWS7928P: 440x260x44mm
- EWS1200-28TFP: 440x260x44mm
- EWS7926EFP: 440x260x44mm
- EWS7952P: 440x310x44mm
- EWS7952FP: 440x310x44mm

Chapter 2

Getting Started



Installing the Switch

This section will guide you through the installation process.

Management Interface

The Switch features an embedded Web interface for the monitoring and management of your device.

Management Interface Default Values

IP Address: 192.168.0.239

Username: admin

Password: password

Connecting the Switch to a Network

Discovery in a Network with a DHCP server

Use the procedure below to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
5. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
6. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
7. Click **IP Settings** under the **System tab** and select IPv4 or IPv6.
8. Click **DHCP** under Auto-Configuration.
9. Click **Apply** to save the settings.
10. Connect the Switch to your network (DHCP enabled).
11. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

Discovery in a Network with a DHCP server

This section describes how to set up the Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based management interface.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**.
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: **192.168.0.239** and the Subnet mask address as **255.255.255.0**).
6. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
7. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
8. Click **IP Settings** under the **System menu** and select **Static IP** to configure the IP settings of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Chapter 3

Software Features



Using the Switch

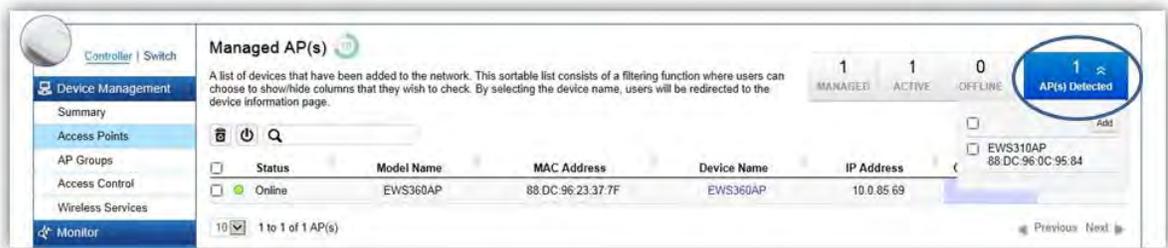
Besides the functions of a Wireless Controller, the EWS Wireless Management Switch also possesses functions of a full-featured Layer 2 Ethernet Switch. Use the Controller / Switch tab on the upper left corner of the user interface to toggle between the Wireless Controller or Layer 2 Switch functions.



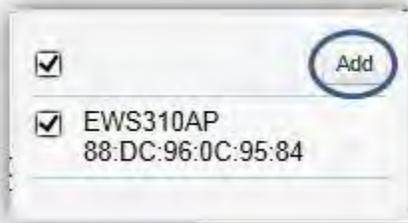
Wireless Controller Features

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.



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



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



Auto-Configuration	<p>DHCP: You can choose to auto assign IP address if there is a DHCP server in the network.</p> <p>Static: If you wish to manually assign the IP address, choose Static. Enter the IP address you wish to assign to the AP and fill in the subnet mask, default gateway and DNS server address.</p> <p>Keep AP's Settings: Select this option for the AP to use its current network settings.</p>
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 DNS Server	Enter the primary DNS server name.
Secondary DNS Server	Enter the secondary DNS server name (if necessary).

- 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.

<input type="checkbox"/>	Status	Model Name	MAC Address	Device Name	IP Address	Group
<input type="checkbox"/>	Online	EWS310AP	88:DC:96:0C:95:84	EWS310AP	10.0.85.69	

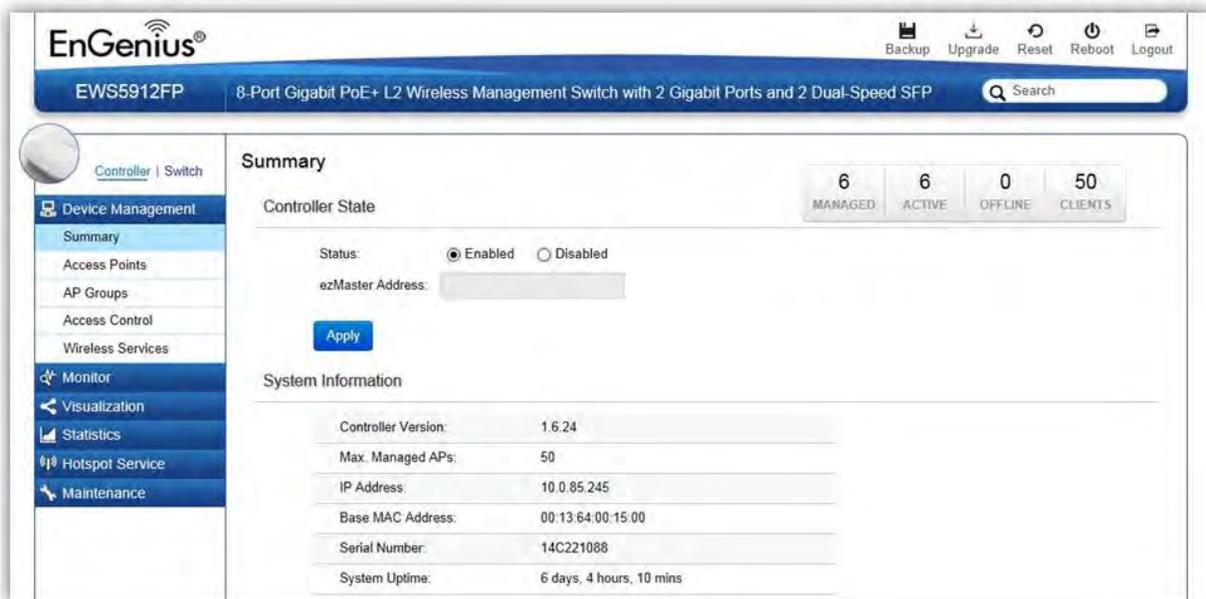
Note: If the status shows **Incompatible Version**, please check and make sure that the firmware of the Access Point and Switch are compatible.

<input type="checkbox"/>	Status	Model Name	MAC Address	Device Name	IP Address	Group
<input type="checkbox"/>	Incompatible Version	EWS310AP	88:DC:96:0C:95:84	EWS310AP	10.0.85.162	

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.



The screenshot shows the EnGenius web interface for the EWS5912FP switch. The top navigation bar includes links for Backup, Upgrade, Reset, Reboot, and Logout. The main content area is titled "Summary" and is divided into two sections: "Controller State" and "System Information".

Controller State:

- 6 MANAGED
- 6 ACTIVE
- 0 OFFLINE
- 50 CLIENTS

Controller State Configuration:

Status: Enabled Disabled
ezMaster Address:
[Apply](#)

System Information:

Controller Version:	1.6.24
Max. Managed APs:	50
IP Address:	10.0.85.245
Base MAC Address:	00:13:64:00:15:00
Serial Number:	14C221088
System Uptime:	6 days, 4 hours, 10 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

Status: Select whether to Enable or Disable the Controller feature on the Switch.

ezMaster Address: If you have an ezMaster server running and wants to have ezMaster manage this EWS Switch directly, enter the IP Address/domain name of the ezMaster server.

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

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.

The EWS Switch is able to manage supported EWS Series Access Points. 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.

The screenshot shows the EnGenius web interface for an EWS5912FP switch. The main content area is titled 'Managed AP(s)' and contains a table of 6 managed APs. The table has the following columns: Status, Model Name, MAC Address, Device Name, IP Address, and Group. All APs are listed as 'Online'. The device names include 'EWS310AP', 'EWS360AP', and several 'Neihu_7F_Meeting_Room' variants. The IP addresses are all in the 10.0.85.x range. Above the table, there are summary statistics: 6 MANAGED, 6 ACTIVE, 0 OFFLINE, and 1 AP(s) Detected. A search bar is located above the table. The sidebar on the left shows navigation options like 'Device Management', 'Monitor', and 'Maintenance'.

Status	Model Name	MAC Address	Device Name	IP Address	Group
Online	EWS310AP	88 DC 96 0C 95 84	EWS310AP	10.0.85.69	
Online	EWS360AP	88 DC 96 23 37 7F	EWS360AP	10.0.85.144	
Online	EWS310AP	00 13 51 00 06 00	Neihu_7F_Meeting_Room_D	10.0.85.236	
Online	EWS310AP	00 13 51 00 09 00	Neihu_7F_Meeting_Room_E	10.0.85.241	
Online	EWS310AP	00 13 51 00 08 00	Neihu_7F_Meeting_Room_A	10.0.85.239	
Online	EWS310AP	88 DC 96 22 02 27	Neihu_7F_Allan	10.0.85.240	

Managing Access Points

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

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 an AP group and add members into the group. Click on the **Group** field of the AP you wish to configure and you will be directed to a screen where you can configure settings for the AP Group.

Group 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 AP Group, then click on the **Device Name** field of the Access Point (which is already in a group) 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	6	0
MANAGED	ACTIVE	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.

Group

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

Column Filter

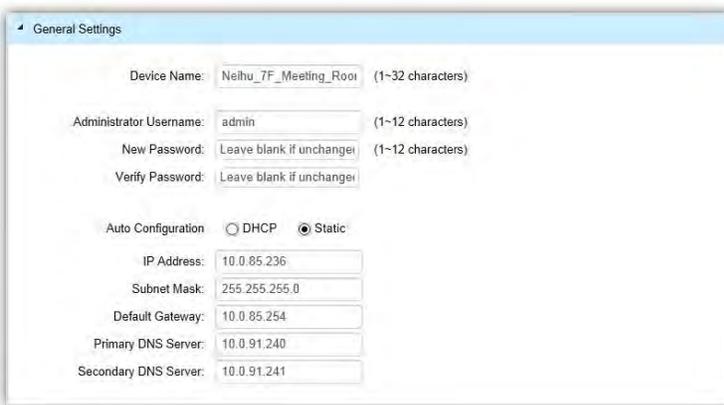
Shows or hides fields in the Access Point list.



Access Point 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



The screenshot shows the 'General Settings' configuration page for an Access Point. The fields and their values are as follows:

Field	Value	Constraint
Device Name	Neilhu_7F_Meeting_Room	(1-32 characters)
Administrator Username	admin	(1-12 characters)
New Password	Leave blank if unchanged	(1-12 characters)
Verify Password	Leave blank if unchanged	(1-12 characters)
Auto Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	10.0.85.236	
Subnet Mask	255.255.255.0	
Default Gateway	10.0.85.254	
Primary DNS Server	10.0.91.240	
Secondary DNS Server	10.0.91.241	

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

The screenshot shows the 'Wireless Radio Settings' window with the following configurations:

Setting	2.4GHz	5GHz
Country	USA	USA
Wireless Mode	802.11 b/g/n Mixed	802.11 a/n Mixed
Channel HT Mode	20MHz	40MHz
Extension Channel	Upper Channel	Upper Channel
Channel	Auto	Auto
Transmit Power	19dBm	18dBm
Client Limits	126 (1~127, 0 means no limit)	126 (1~127, 0 means no limit)
Data Rate	Auto	Auto
RTS/CTS Threshold	2346 (1~2346)	2346 (1~2346)
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation Frames	32 Frames (1~32)	32 Frames (1~32)
Aggregation Bytes	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. For 2.4GHz, the available options are 802.11b/g/n mixed, 802.11b, 802.11b/g mixed, 802.11g, and 802.11n. For 5GHz, the available options are 802.11a/n mixed, 802.11a, and 802.11n.

Channel HT Mode: Use the drop-down menu to select the Channel HT as 20MHz, 20/40MHz or 40MHz. 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: Use the drop-down menu to select the wireless channel the radio will operate on. 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.

Transmit Power: Allows you to manually set the transmit power on 2.4GHz or 5GHz radios. Increasing the power improves performance, but if two or more Access Points are operating in the same area on the same channel, it may cause interference.

Client Limits: Specify the maximum number of wireless clients that can associate with the radio. Enter a range from 1 to 127, or fill in 0 for an unlimited client limit.

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

Under the WLAN Settings, you can create and manage SSID configurations and profiles for the Access Points to fit your needs. An SSID is basically the name of the wireless network to which a wireless client can connect to. Multiple SSIDs allow administrators to use a single physical network to support multiple applications with different configuration requirements. Up to 8 SSIDs are available per radio. Click on the SSID you wish to make changes to and you'll be directed to the SSID Configuration page.

ID	Status	SSID	Security	Encryption	Hidden SSID	Client Isolation	L2 Isolation	VLAN Isolation	VLAN ID
1	Enabled	SNWL	WPA2-PSK	AES	No	No	No	No	1
2	Disabled	210_2-2.4GHz	WPA2-PSK	AES	No	No	No	No	2
3	Disabled	SSID_3-2.4GHz	None	None	No	No	No	No	3
4	Disabled	SSID_4-2.4GHz	None	None	No	No	No	No	4
5	Disabled	SSID_5-2.4GHz	None	None	No	No	No	No	5
6	Disabled	SSID_6-2.4GHz	None	None	No	No	No	No	6
7	Disabled	SSID_7-2.4GHz	None	None	No	No	No	No	7
8	Disabled	SSID_8-2.4GHz	None	None	No	No	No	No	8

ID	The ID displays the SSID profile identifier.
Status	This displays whether the current SSID profile is enabled or disabled.
SSID	Displays the SSID name as it appears to the wireless clients in the network.
Security	Displays the security mode the SSID uses.
Encryption	Displays the data encryption type the SSID uses.
Hidden SSID	Displays whether the hidden SSID is enabled or disabled.
Client Isolation	Displays whether Client Isolation feature is enabled or disabled.
L2 Isolation	Displays whether L2 Isolation feature is enabled or disabled.
VLAN Isolation	Displays whether VLAN Isolation feature is enabled or disabled.
VLAN ID	<p>Displays the VLAN ID associated with the SSID.</p> <p>Note: For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to EWS APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.</p>

SSID Config

SSID Config

Basic Setting

Enable SSID: Enable Disable

SSID: (1~32 characters)

Hidden SSID: Enable Disable

Client Isolation: Enable Disable

L2 Isolation: Enable Disable

VLAN Isolation: Enable Disable

VLAN ID: (1~4094)

Traffic Shaping

Enable Traffic Shaping: Enable Disable

Save **Cancel**

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



LED Control

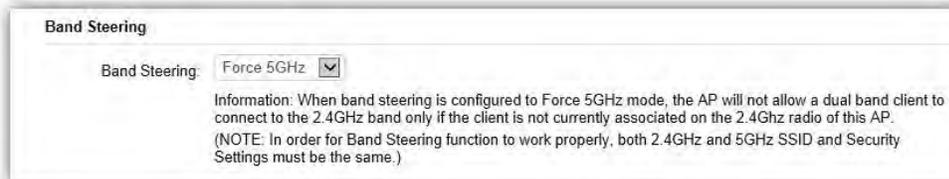
Power: Enable Disable

LAN: Enable Disable

WLAN - 2.4GHz: Enable Disable

WLAN - 5GHz: Enable Disable

LED Control: In some environments, the blinking LEDs on APs 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

Band Steering: Force 5GHz ▼

Information: When band steering is configured to Force 5GHz mode, the AP will not allow a dual band client to connect to the 2.4GHz band only if the client is not currently associated on the 2.4GHz radio of this AP.
(NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.)

Band Steering: When enabled, when the wireless client first associates with the AP, the AP will detect 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: For Band Steering to take effect, both 2.4GHz and 5GHz SSIDs must have the same SSID and security settings. Wireless clients must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.

- **Prefer 5GHz:** All dual-band clients with 5GHz RSSI above the threshold will be connected to the 5GHz band.
- **Force 5GHz:** All dual-band clients will connect to the 5GHz.
- **Band Balance:** Automatically balances the number of newly connected clients across both 2.4GHz and 5GHz bands.

IMPORTANT INFORMATION: Band Steering only defines the action when a wireless client associates with an AP for the first time, and the wireless client must be in both 2.4GHz and 5GHz wireless coverage zone when authenticating with the AP for the Band Steering algorithm to take effect.

RSSI Threshold

Status: Enable Disable

RSSI: 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.)

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.

Management VLAN

Status: Enable Disable

VLAN ID: (Range: 1 ~ 4094)

(WARNING: Enabling the management VLAN can cause the AP to lose connectivity with the controller. If you are utilizing the management VLAN, make sure that the controller and the AP are set to the same management VLAN to ensure proper connectivity.)

Management VLAN: Management VLAN can be used to separate management traffic from regular network traffic.

IMPORTANT INFORMATION: *When configuring or updating AP's Management VLAN settings, make sure that the same Management VLAN settings are applied to the EWS Switch as well.*

Guest Network

Band	Status	SSID	Security	Encryption	Hidden SSID
2.4GHz	Enabled	SNWL-Guest	None	None	No
5GHz	Enabled	SNWL-Guest	None	None	No

Captive Portal Settings

Captive Portal: Enable Disable

Manual IP Settings

IP Address:

Subnet Mask:

Automatic DHCP Server Settings

Starting IP Address:

Ending IP Address:

WINS Server IP:

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: (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.

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.

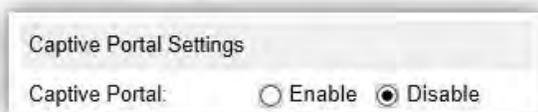
Hidden SSID: Enable this option if you do not want to broadcast this SSID. This can help to discourage wireless users from connecting to a particular SSID.

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.



Captive Portal: Select whether to Enable or Disable Captive Portal for Guest Network.

The image shows a network configuration dialog box with two sections. The first section, 'Manual IP Settings', contains three input fields: 'IP Address' with the value '192.168.100.1', 'Subnet Mask' with '255.255.255.0', and 'WINS Server IP' with '0.0.0.0'. The second section, 'Automatic DHCP Server Settings', contains two input fields: 'Starting IP Address' with '192.168.100.100' and 'Ending IP Address' with '192.168.100.200'.

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.

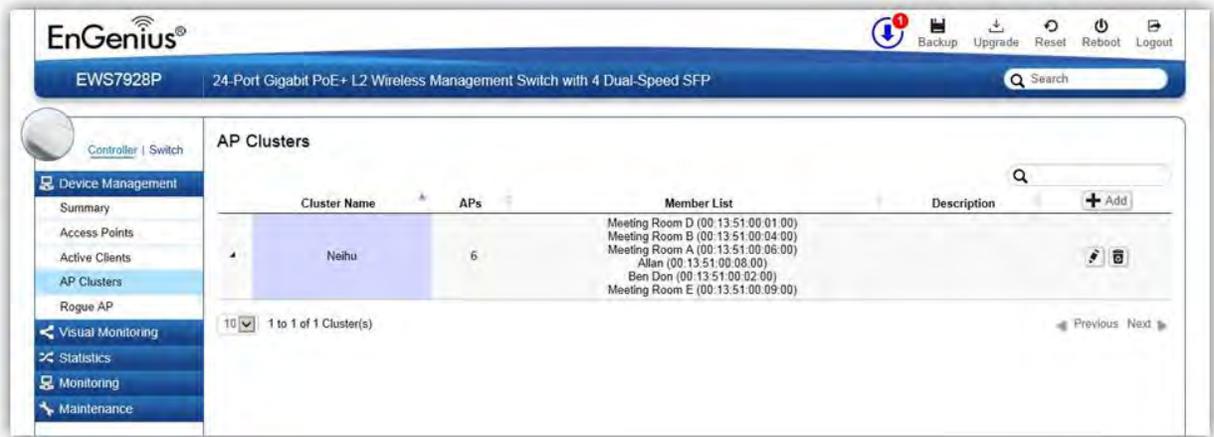
Automatic DHCP Server Settings

- **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.

After settings are changed, click **Apply** to save the changes to the system.

AP Groups

An AP Group 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 Groups 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 AP Groups with different settings and policies to suit your application.



Creating a New AP Group

Follow the steps below to create a new AP Group.

1. Click on **Add** button to create a new AP Group.



2. Enter the name and description of the new AP Group.

3. In the Member Setting section, all Access Points that are managed by the EWS Switch that are not currently assigned to an AP Group will be listed on the left. Select the Access Points you wish to assign to this group 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 keywords in the list using the following criteria: AP Group Name, AP MAC, AP Name, Description.



Add Button

Use the Add Button to create a new AP Group.



Edit Button

Use the Edit Button to edit the configurations of the AP Group.



Delete Button

Use the Delete Button to remove an AP Group.



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.

The screenshot shows the EnGenius web interface for a 24-Port Gigabit PoE + L2 Wireless Management Switch. The main content area is titled "Blocked List" and contains a table with the following data:

Client MAC Address	Description
00:13:51:00:09:00	client A
80: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

The interface also features a search bar, a "5 Blocked Client" indicator, and an "Apply" button. The left navigation menu includes options like "Device Management", "Access Points", "Active Clients", "AP Clusters", "Access Control", "Rogue AP", "Visual Monitoring", "Statistics", "Monitoring", and "Maintenance".

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.



Wireless Services



Background Scanning

With Background Scanning enabled, the controller periodically samples RF activity of all Access Points including channel utilization and surrounding devices in all available channels. Background scanning is the basis of Auto Channel, Auto Tx Power and Rogue AP detection, and must be enabled for these features to operate. You may, if you prefer, disable it if you feel it's not helpful, or adjust the scanning frequency, if you want scans at greater or fewer intervals.

Note: For latency-sensitive applications such as VoIP, it is recommended to set the background scan interval to a higher value, e.g. 5 or 10 minutes. For regular application, the recommended value is 30 seconds. This value will also be directly related on how long it takes for the AP to scan for rogue devices.

Auto TX Power

Using the information collected by Background Scanning, APs can automatically adjust their transmit power to optimize coverage. When enabled, APs will optimize their transmit power based on the time interval configured for Background Scanning.

Note: Background Scanning must be **enabled** and Tx Power of APs must be set to **Auto** (under Wireless Radio Settings) for this feature to operate.

Monitor

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.

Client Name	Client IP	Client MAC Address	Client OS	Band	TX Traffic(KB)	RX Traffic(KB)	RSSI(dBm)
lvuduMacBook-Air	10.0.85.110	84:38:35:50:D1:9C	Apple Mac OS X	5GHz	23088	7575	-69
WTFloWer	10.0.85.100	40:B3:95:5F:5B:12	Apple IOS	5GHz	66	143	-75
Tony-iPhone	10.0.85.74	E8:8D:28:31:89:19	Apple IOS	5GHz	2254	2502	-59
TakdaAir	10.0.85.93	48:D7:05:DC:6B:B1	Apple Mac OS X	5GHz	7054	1206	-88
TakdaAir	10.0.85.93	48:D7:05:DC:6B:B1	Apple Mac OS X	5GHz	11471	423	-72
takashimatPad	10.0.85.138	5C:9E:9D:9E:FF:C9	Apple IOS	5GHz	319	146	-59
Stanley-PC	10.0.85.104	70:1A:04:B3:2B:18	Windows 7/Vista/Server 2008	2.4GHz	2360	15236	-38
Signas-iPhone	10.0.85.65	24:AB:B1:86:8A:2F	Apple IOS	2.4GHz	5	13	-66
Signamato-iPad	10.0.85.66	64:20:0C:73:4F:53	Apple IOS	5GHz	418	311	-62
SemanoonePlus	10.0.85.60	9C:F3:87:03:F8:5C	Apple IOS	5GHz	82	126	-62
s101660b	10.0.85.117	08:ED:69:C2:0A:91	Windows 7/Vista/Server 2008	2.4GHz	6796	9139	-60
s101560	10.0.85.39	20:16:D8:29:E5:18	Windows 7/Vista/Server 2008	2.4GHz	184065	21574	-66
Remus	10.0.85.75	44:00:10:C5:86:F0	Apple IOS	5GHz	1398	905	-72
raymondjtkalMBP	10.0.85.32	F8:1E:DF:DD:3E:93	Apple Mac OS X	5GHz	739	529	-64
PC-de-iPhone	10.0.85.63	D8:CF:9C:7D:70:65	Apple IOS	5GHz	834	502	-87
MY-de-iPhone	10.0.85.6	44:00:10:D8:58:E3	Apple IOS	5GHz	76	176	-76
Mobile-Teddy	10.0.85.42	80:EA:96:CB:7D:99	Apple IOS	5GHz	136	405	-76
Michael-S	10.0.85.72	F8:F6:1C:6F:86:9D	Apple IOS	5GHz	0	7	-77

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

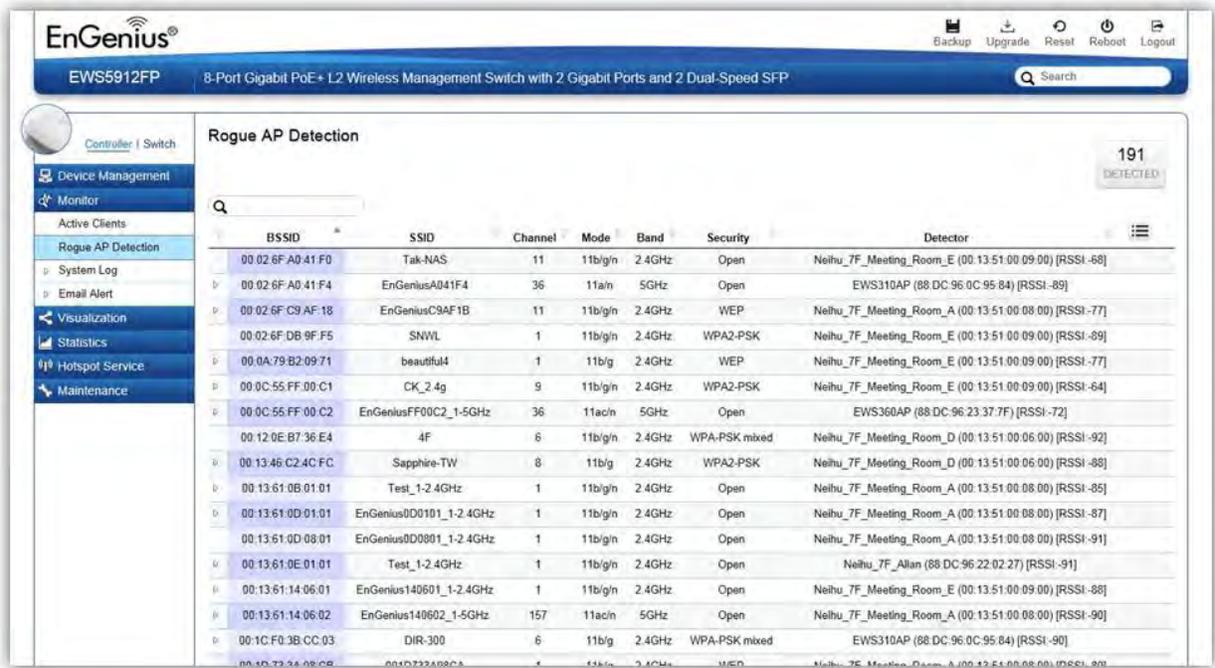
Use the Search Bar to search for Wireless Clients managed by the EWS Switch using the following criteria: Client Name, Client IP, Client MAC Address, Client OS, AP Device Name, AP MAC Address, Model Name, SSID, Band, TX Traffic, RX Traffic.



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.

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. With **Background Scanning** enabled, the Rogue AP Detection feature can be used to periodically scan 2.4 GHz and 5 GHz frequency bands to identify rogue wireless Access Points not managed by the EWS Switch.



Search Bar

Use the Search Bar to search for Rogue Access Points detected using the following criteria: BSSID, SSID, Type, Channel, Mode, Band, Security, Detector.



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.
Detector	Displays the name and MAC address of the managed AP which detected the rogue device.

Column Filter

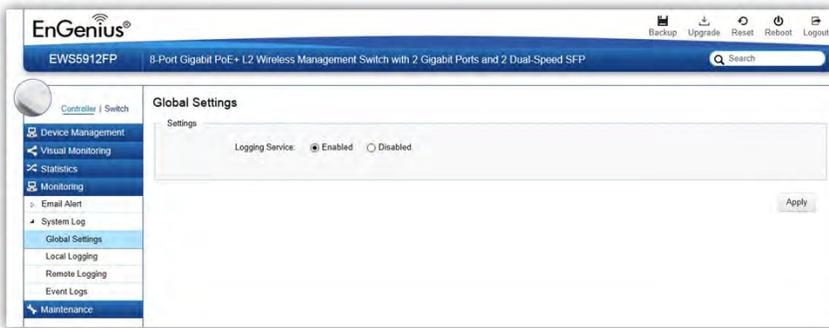
Shows or hides fields in the list.



System Log

Global Settings

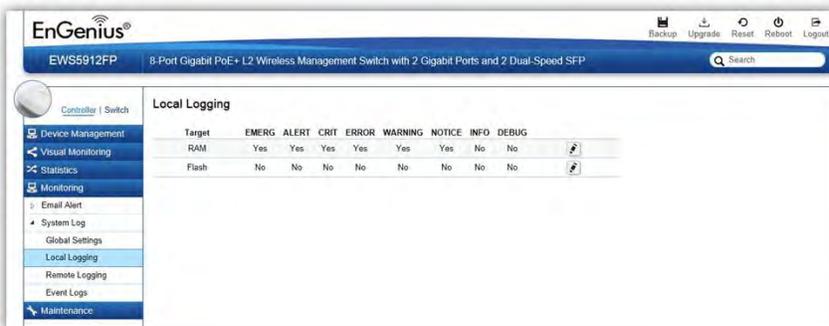
From here, you can Enable or Disable the Log settings for the EWS Switch.



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.



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

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.



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.

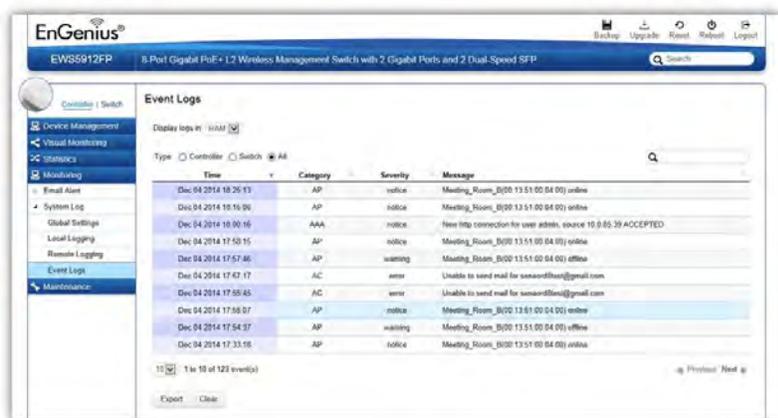
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might 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

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.



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.

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.

The screenshot shows the EnGenius web interface for the EWS5912FP switch. The page title is 'Alert Settings'. The left sidebar contains a navigation menu with the following items: Device Management, Visual Monitoring, Statistics, Monitoring, Email Alert, Alert Settings (highlighted), Event Binding, System Log, and Maintenance. The main content area is titled 'Alert Settings' and is divided into two sections: 'Mail Alert State' and 'Mail Information Setting'. In the 'Mail Alert State' section, there are two radio buttons: 'Enabled' (selected) and 'Disabled'. In the 'Mail Information Setting' section, there are several input fields: 'SMTP Server' (smtp.gmail.com), 'SMTP Port' (587), 'SSL/TLS' (radio buttons for 'Enable' selected and 'Disable'), 'Authentication' (radio buttons for 'Enable' selected and 'Disable'), 'User Name' (senaordstest), 'Password' (masked with asterisks), 'From Mail Address' (senaordstest@gmail.com), 'To Mail Address' (senaordstest@gmail.com), and 'Subject' (10.0.85.245). At the bottom right of the form, there are two buttons: 'Test' and 'Apply'.

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.

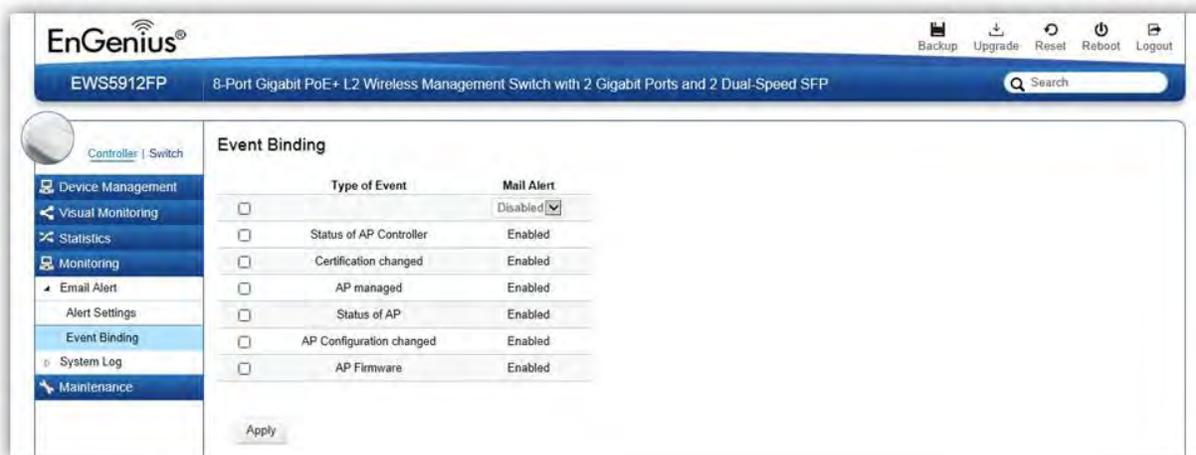
- **From Mail Address:** Enter the email address that will appear as the sender of the email alert.
- **To Mail Address:** Enter the email address which the EWS Switch will send alarm messages to. You can only send alarm messages to a single email address.
- **Subject:** Enter the subject of the email 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

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.



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

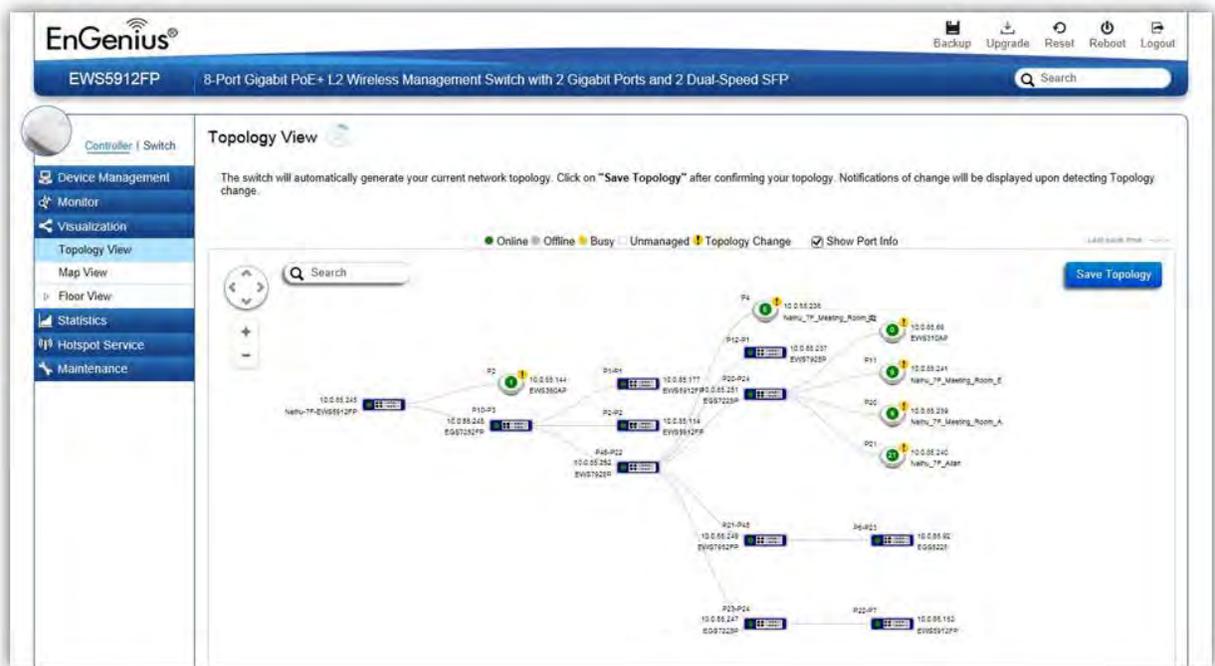
Status of AP	[AP Name] [AP MAC] offline	WARNING
Status of AP	[AP Name] [AP MAC] has invalid IP [IP Address]	WARNING
Status of AP	[AP Name] [AP MAC]'s active client number reaches client limits {value} of [2.4/5]GHz	WARNING
AP Configuration Changed	[AP Name] [AP MAC] configuration updated	INFO
AP Firmware	[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

Visualization

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.



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)

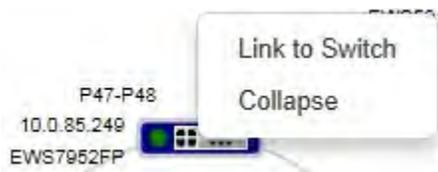
Unmanaged	The AP is not managed by the controller
Topology Change	There is a change in topology for this device

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.

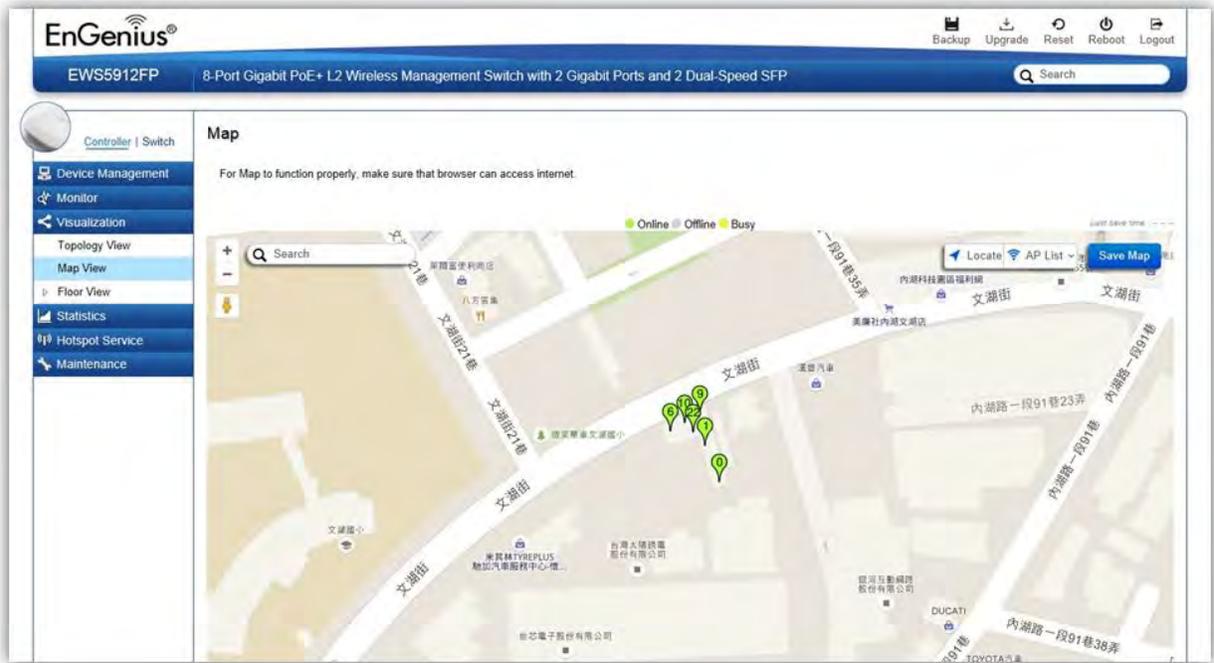
Click on for the Controller to save the current network topology. Changes will be displayed upon detecting a topology change.

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

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 needs to be able to access the Internet for this function to work.



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.



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.

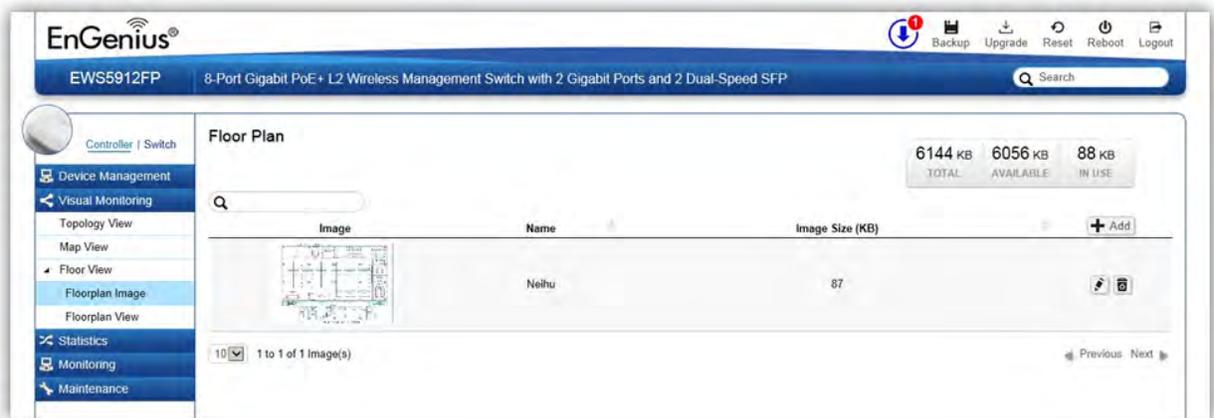
Floor View

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

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.

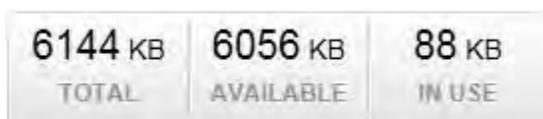


Status Dashboard

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.



Add Button

Use the Add Button to import a new image.



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

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: 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.

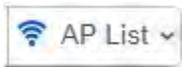
RSSI Range Simulate: Check the **RSSI Simulate** box to display RSSI reference on your floor plan. Adjust RSSI coverage range to emulate using the slider bar.

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: 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.



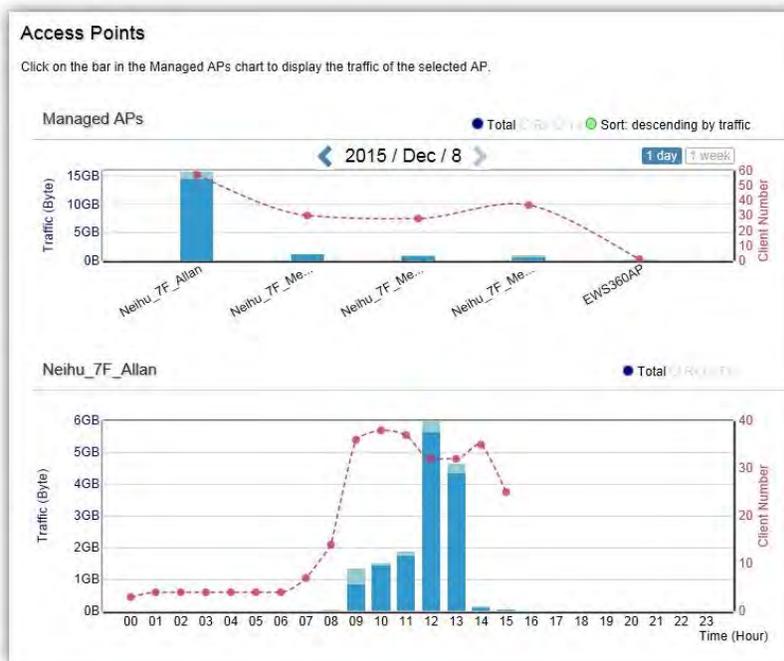
Left click on the Access Point marker to bring up a menu where you can configure AP settings, remove AP from management list, reboot AP, redirect to the Active Clients page or redirect to troubleshooting page.

Click on  for the settings to take effect.

Statistics

Access Points

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



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.

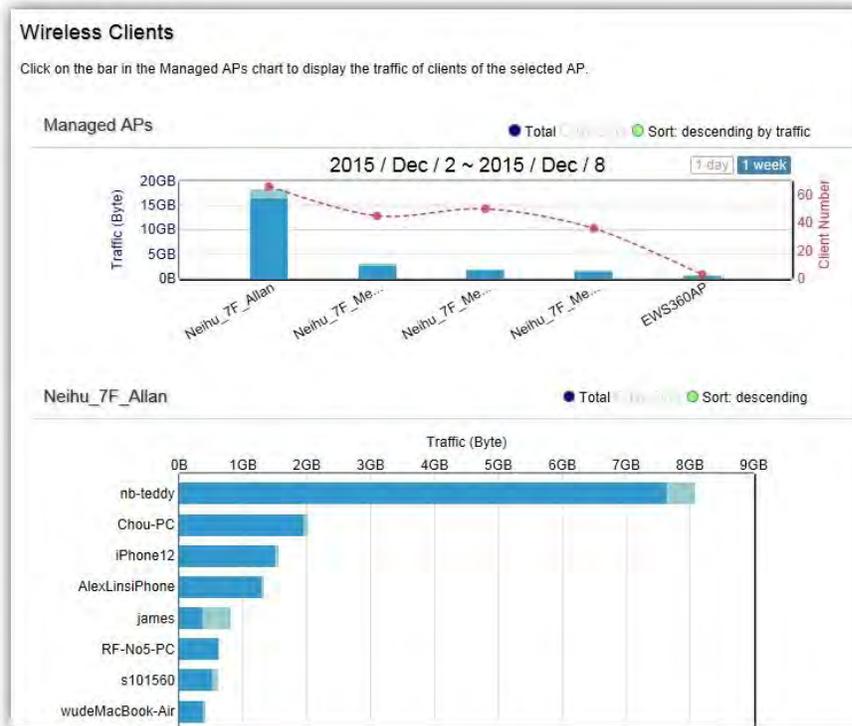
Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

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

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.

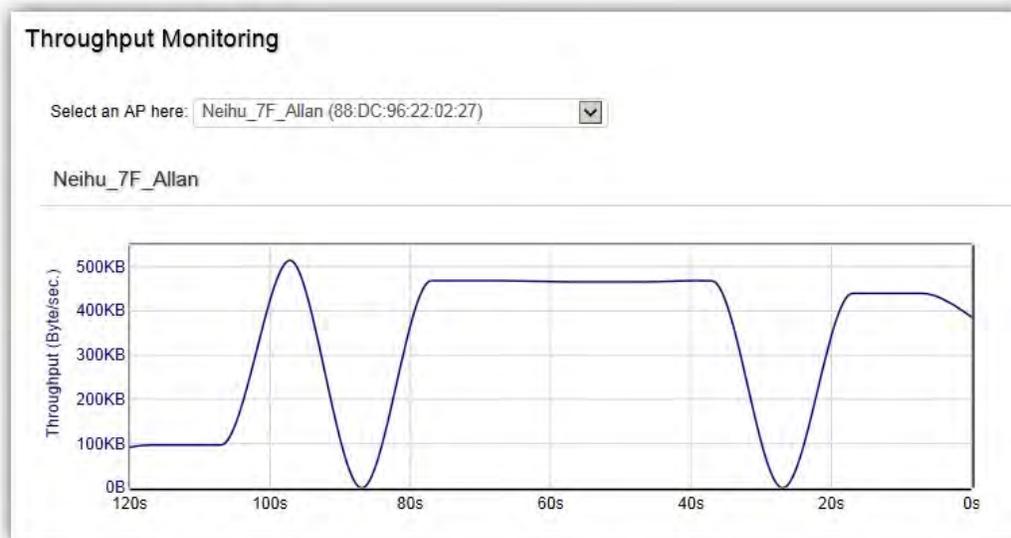
Click **1 day** or **1 week** button to select a time increment to monitor statistics by.

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.

Real Time Throughput

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



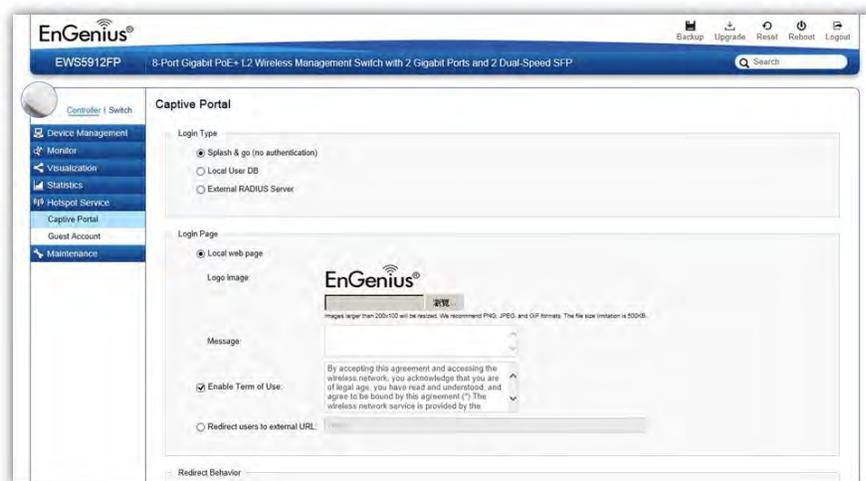
Hotspot Services

A hotspot is a wireless network that provides access through a captive portal. Use this feature to setup captive portal related configurations.

A captive portal provides registered users with network access while containing unregistered users. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot. Once a Captive Portal Profile is created, the administrator can apply this profile to multiple Guest Networks SSIDs.

Note: Captive portal profiles can only be assigned to the **Guest Network SSIDs**.

Captive Portal



Login Type: Defines the mechanism by which a wireless client gains access to the network after the client has associated to the SSID.

Splash & Go	The wireless client is granted network access without any further authentication as soon as it is associates to the SSID.
Local User DB	The wireless client is authenticated using the EWS Switch's local database (from <i>Hotspot Service</i> > <i>Guest Account</i>).
External RADIUS Server	The wireless client is authenticated using an external RADIUS server.

Login Page: A splash page is the web page which prompts the user to log in with a user name and password, or accept a network use policy once the client has associated to the SSID.

Local Web Page	Use the splash page hosted locally by EWS Switch. The local splash page enable administrators to eliminate the need to set up a local web server. Basic customizations like displaying a corporate logo, custom message and term of use is available.
Redirect users to external URL	External splash page enables the administrator to host their own the splash page web server, rather than having it hosted by the EWS Switch.

Redirect Behavior: Configure where users will be redirected after successful login. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected.

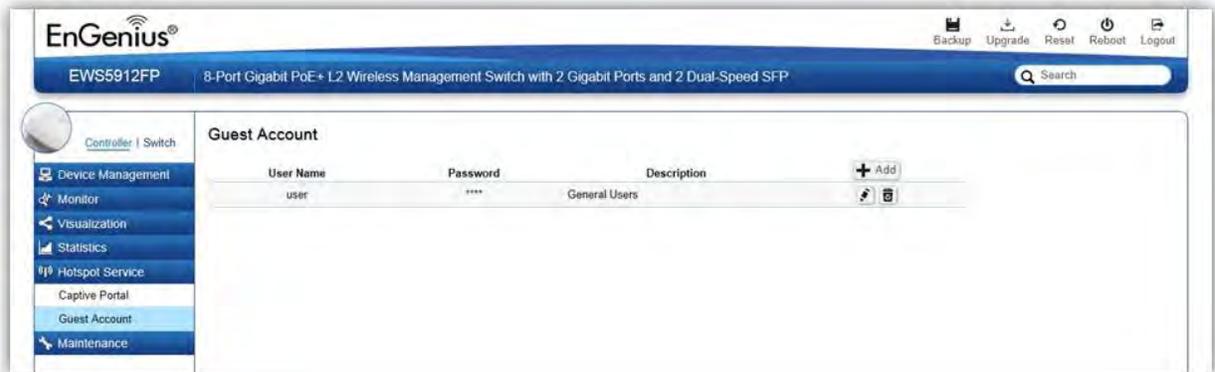
Redirect to the URL that the user was trying to visit	Select this option for ezMaster to cache the initial website from the client during the authentication process and then forward it to the originally targeted web server after the user successfully authenticates.
Redirect users to a specified URL after login	Select this option to redirect users to a specific URL after users successfully authenticates.

User Session: Configure session timeout and ideal timeout period.

Session Timeout	Specify a time limit after which users will be disconnected and required to log in again.
Idle Timeout	Specify a time limit for an idle client after which users will be disconnected and required to log in again.

Walled Garden: This option allows users to define network destinations that users can access before authentication. For example, your company's website.

Guest Account



On this page, an administrator can create, edit, and remove user accounts used for captive portal's local database authentication.

Add: Create a new user account.

Remove: Delete the selected user account.

Edit: Edit the settings of the selected user account.

Maintenance

Schedule Tasks

Schedule Settings

Task Settings

Task Name: (1~32 characters)

Enabled:

Action Settings

Type: Reboot AP(s) Change WLAN State Change Switch PoE State Switch PoE Reset

Switch Port: 1 2 3 4 5 6 7 8

State: Enable

Time Settings

Type: Day of Week Date

Sun Mon Tue Wed Thu Fri Sat

Hour Minute

Use the Schedule Tasks feature to control the time(s), or day(s) of a week, or date of a month to automatically perform the following task:

Reboot AP(s): Soft reboot AP

Change WLAN State: Enable/disable WLAN service

Change Switch PoE State: By port PoE enable or disable. Only available for PoE supported models.

Switch PoE Reset: Power cycle PoE port. Only available for PoE supported models.

NOTE: This feature will not work properly if the EWS Switch does not have the correct time settings.

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.

The screenshot displays the 'Troubleshooting' interface. At the top, there is a 'Show All' button. Below it is a table with columns for Status, Device Name, MAC Address, and IP Address. The table contains one entry for 'Neihu_7F_Allan' with a status of 'Online', MAC Address '88:DC:96:22:02:27', and IP Address '10.0.85.240'. Below the table, a vertical line represents the network topology, connecting the selected AP to four other APs: 'Neihu-7F-EWS5912FP', 'EGS7252FP', 'EWS7928P', and 'EGS7228P'. Each of these APs shows 'Connection' and 'Cable status' with green checkmarks. A green box on the right contains 'Success Information: No problem found on this AP.'

Status	Device Name	MAC Address	IP Address
Online	Neihu_7F_Allan	88:DC:96:22:02:27	10.0.85.240

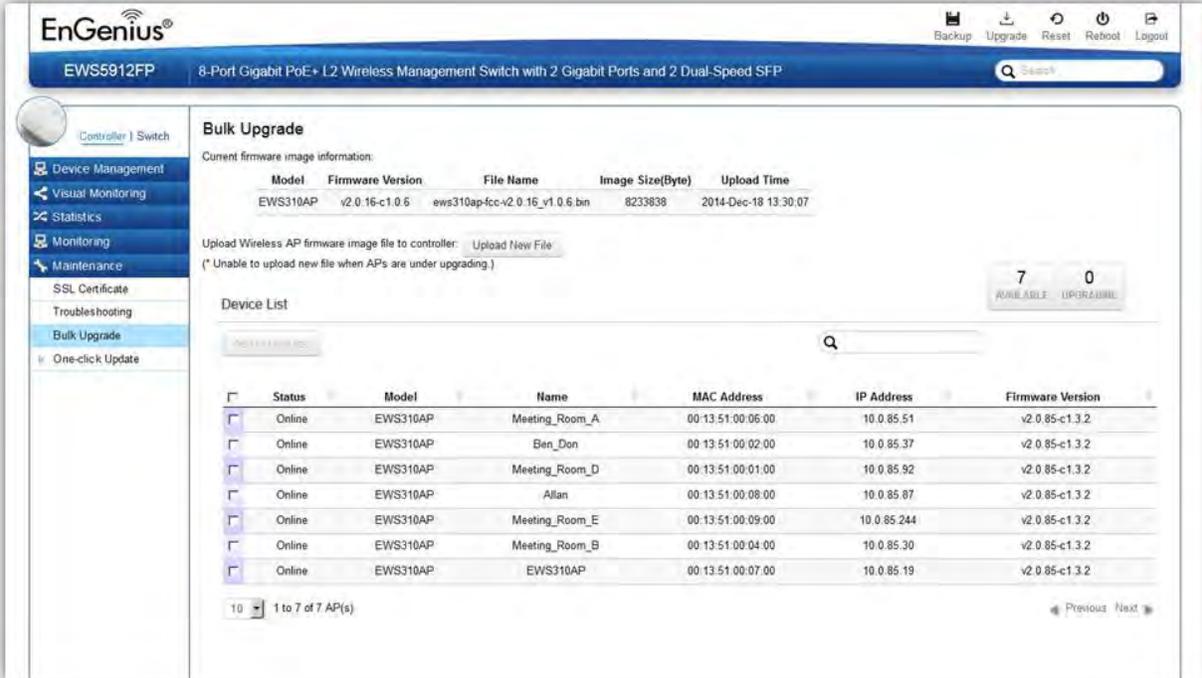
Success Information
No problem found on this AP.

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 takes a few seconds to complete. Afterwards, the results will display on the page.

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.



The screenshot shows the EnGenius web interface for an EWS5912FP switch. The 'Bulk Upgrade' section is active, showing current firmware information for EWS310AP. Below this, there is a 'Device List' table with 7 devices ready for upgrade and 0 currently upgrading.

Model	Firmware Version	File Name	Image Size(Byte)	Upload Time
EWS310AP	v2.0.16-c1.0.6	ews310ap-fcc-v2.0.16_v1.0.6.bin	8233838	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.)

7 AVAILABLE 0 UPGRADING

Status	Model	Name	MAC Address	IP Address	Firmware Version
Online	EWS310AP	Meeting_Room_A	00:13:51:00:06:00	10.0.85.51	v2.0.85-c1.3.2
Online	EWS310AP	Ben_Don	00:13:51:00:02:00	10.0.85.37	v2.0.85-c1.3.2
Online	EWS310AP	Meeting_Room_D	00:13:51:00:01:00	10.0.85.92	v2.0.85-c1.3.2
Online	EWS310AP	Allan	00:13:51:00:08:00	10.0.85.87	v2.0.85-c1.3.2
Online	EWS310AP	Meeting_Room_E	00:13:51:00:09:00	10.0.85.244	v2.0.85-c1.3.2
Online	EWS310AP	Meeting_Room_B	00:13:51:00:04:00	10.0.85.30	v2.0.85-c1.3.2
Online	EWS310AP	EWS310AP	00:13:51:00:07:00	10.0.85.19	v2.0.85-c1.3.2

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

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.

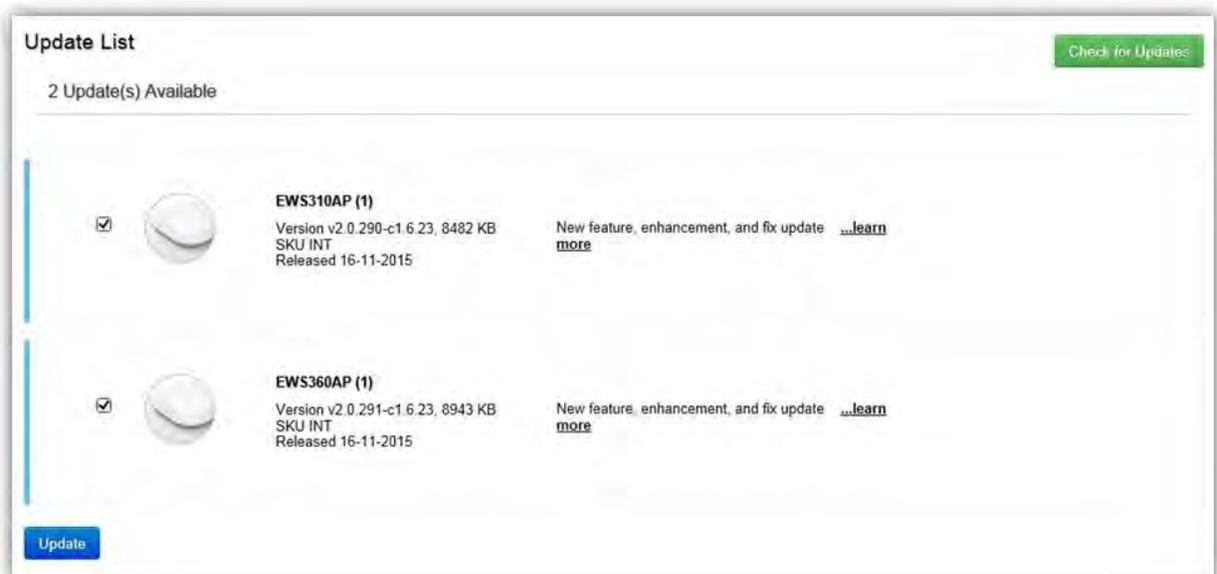


Note: An active Internet connection is required for this feature.

Update List

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.

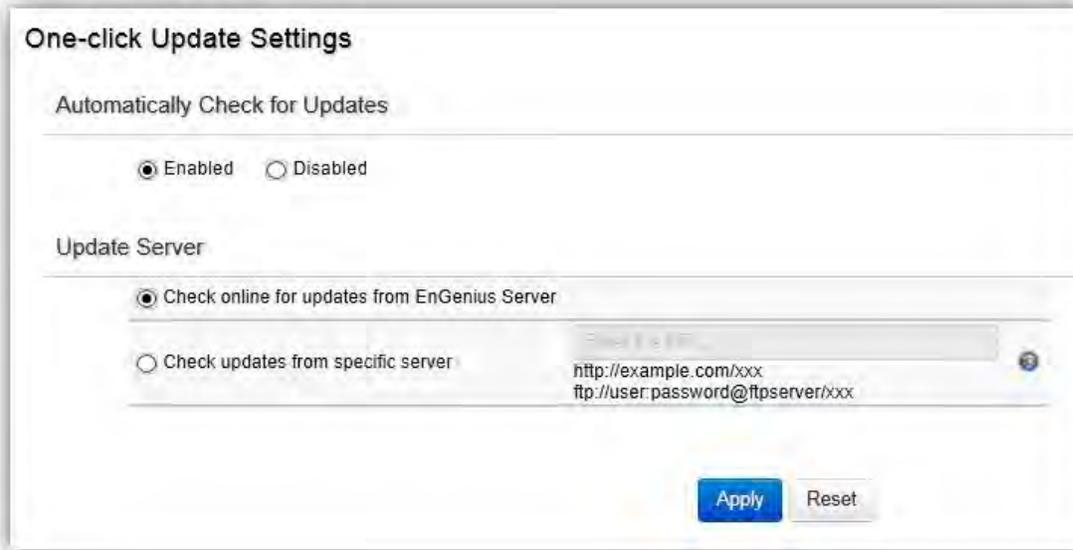


The screenshot shows a web interface titled "Update List" with a green "Check for Updates" button in the top right corner. Below the title, it says "2 Update(s) Available". There are two update entries, each with a checked checkbox, a device icon, and a description:

Device	Version	Size	Release Date	Description
EWS310AP (1)	v2.0.290-c1.6.23	8482 KB	16-11-2015	New feature, enhancement, and fix update learn more
EWS360AP (1)	v2.0.291-c1.6.23	8943 KB	16-11-2015	New feature, enhancement, and fix update learn more

At the bottom left of the update list, there is a blue "Update" button.

Update Settings



The screenshot shows a web interface titled "One-click Update Settings". It is divided into two main sections. The first section, "Automatically Check for Updates", contains two radio buttons: "Enabled" (which is selected) and "Disabled". The second section, "Update Server", contains two radio buttons: "Check online for updates from EnGenius Server" (selected) and "Check updates from specific server". Below the second radio button is a text input field with a "Clear" button on the right. The input field contains two lines of text: "http://example.com/xxx" and "ftp://user:password@ftpserver/xxx". At the bottom right of the form are two buttons: "Apply" (in blue) and "Reset" (in grey).

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.	<i>EWS310AP, EWS320AP, EWS660AP</i>
Firmware Version	Enter firmware version.	<i>v2.0.129-c1.3.5</i>
File Name	Enter complete filename with extension.	<i>ews310ap-fcc-v2.0.132.0-c1.3.5.bin</i>
MD5	Enter MD5 value of the firmware image	<i>4959e8d68536227d182b53a719dcdae4</i>
SKU	Enter in device SKU.	<i>FCC, ETSI, INT</i>

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

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.

SSL Certificate

Create a self-signed SSL Certificate for secured data encryption between Switch and Wireless Access Point(s). AP(s) will reconnect using new certification information upon applying changes.

Generate new certificate

Common Name*:	<input type="text"/>	(1-32 characters)
Organization*:	<input type="text"/>	(1-32 characters)
Organization Unit:	<input type="text"/>	(1-32 characters)
Locality/ City*:	<input type="text"/>	(1-32 characters)
State/ Province*:	<input type="text"/>	(1-32 characters)
Country*:	Afghanistan <input type="checkbox"/>	
Valid Until:	2016/01/07	(2016/1/7 - 2037/12/31)

Certificate Information

Common Name:	Default_name
Organization:	Default_org
Organization Unit:	Default_unit
Locality/ City:	Default_loc
State/ Province:	Default_state
Country:	Taiwan
Valid Date:	1999/12/31 to 2038/01/02

Advanced Option

Restore to Default Certificate:

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.

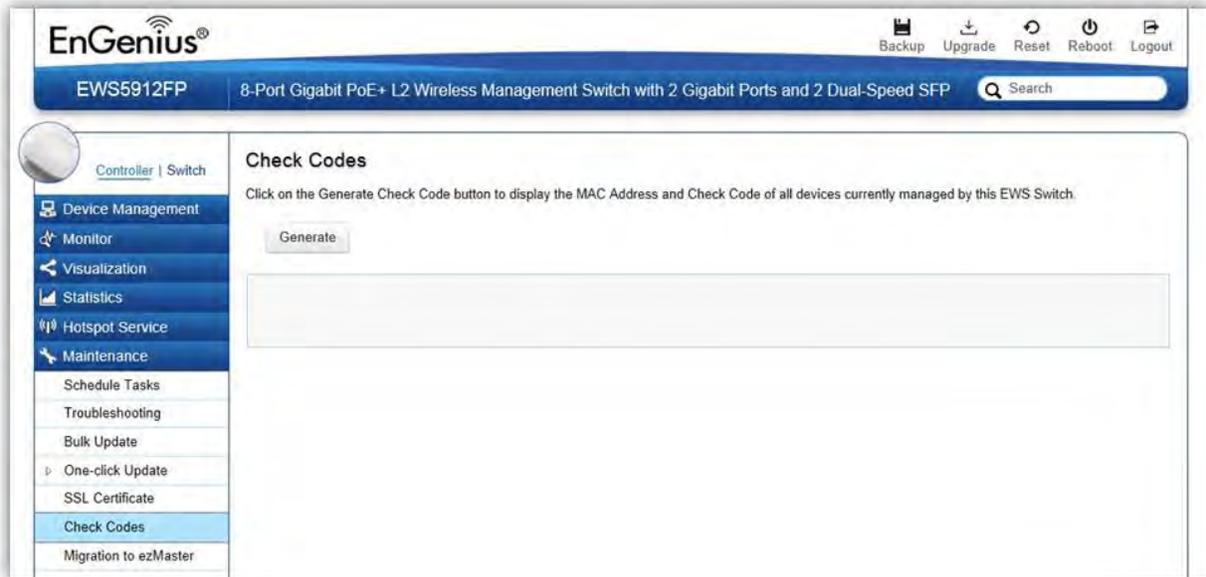
State/Province	Enter the state or province.
Country	Enter the name of the country.
Valid Date	Enter the expiry date of the certificate.

Restore to Default Certificate

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

Check Codes

Use this feature to generate a list of 'Check Codes' for the APs that your EWS Switch is currently managing. Check Codes are used for registering devices to ezMaster.



Migration to ezMaster

Migration to ezMaster

Steps

Step 1. Specify ezMaster to migrate to

Step 1: Specify ezMaster to migrate to

Step 2: Confirm Migration

Use this feature to migrate your EWS Switch and all managed APs to ezMaster. Before proceeding, take note of the following:

- The firmware of the switch and all APs has to be ezMaster compatible.
- Make sure the status of all APs are online.
- Management VLAN for APs must be disabled.
- Make sure the ezMaster you are migrating to has been registered to ezReg.
- Make sure that all devices you are about to migrate has not been already registered to ezMaster.
- Do not cancel the migration process.

Migration Settings

Project Name: ?

IP Address: ?

Port:

User Name: ?

Password:

Register to ezRegister:

This feature will help to migrate the EWS Switch and all the APs managed by the EWS Switch to ezMaster automatically without the need of manually entering the check code and MAC address of all the APs one by one.

Take note of the following before proceeding with the migration process:

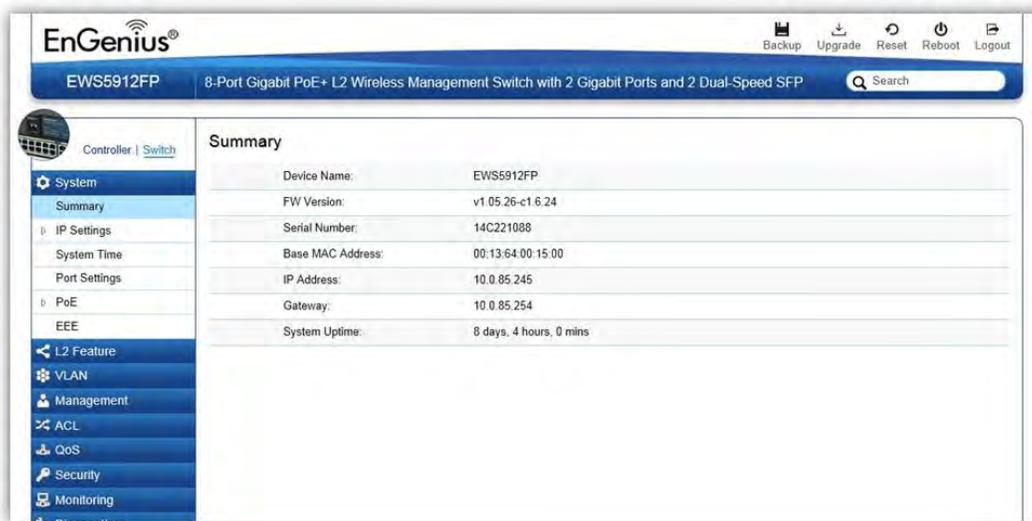
- The firmware of the switch and all APs has to be ezMaster compatible.
- Make sure the status of all APs are online.
- Management VLAN for APs must be disabled.
- Make sure the ezMaster you are migrating to has been registered to ezReg.
- Make sure that all devices you are about to migrate has not been already registered to ezMaster.
- Do not cancel the migration process.

Ethernet Switch Features

System

Summary

The Summary page shows general system information for the Switch including the device name, the software version, serial number, MAC address, IP Address, gateway address, and system uptime.



Device Name	Displays the model name of the device.
FW Version	Displays the installed firmware version of the device.
Serial Number	Displays the serial number of the device.
Base MAC Address	Displays the MAC address of the device.
IP Address	Displays the IP address of the device.
Gateway	Displays the Gateway IP address.
System Uptime	Displays the number of days, hours, and minutes since the last system restart. The System Uptime is displayed in the following format: days, hours, and minutes.

IP Settings

The IP Setting screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

To access the page, click **IP Settings** under the **System** menu.

IPv4

Select whether you wish to enable Static or DHCP for auto-configuration. Next, enter the information for the IP address, gateway, and DNS servers.

IPv4

IPv4 Address Settings

Auto Configuration: Static DHCP

IPv4 Address: 10.0.85.245

Subnet Mask: 255.255.255.0

Gateway: 10.0.85.254

DNS Server 1: 10.0.91.240

DNS Server 2: 0.0.0.0

Apply



Important:

If the device fails to retrieve an IP address through DHCP, the default IP address is **192.168.0.239** and the factory default subnet mask is **255.255.255.0**.

Dynamic IP Address (DHCP)	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway IP address, and a domain name server IP address automatically. Selecting this field disables the IP Address, Subnet Mask, and Gateway fields.
Static IP Address	Allows the entry of an IP address, subnet mask, and a default gateway for

	the Switch. Select this option if you don't have a DHCP server or if you wish to assign a static IP address to the Switch.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: 192.168.0.239
Subnet Mask	A subnet mask separates the IP address into the network and host addresses. A bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: 255.255.255.0
Gateway	Enter an IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway your network is not part of an Intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.
DNS Server (Domain Name System)	Used for mapping a domain name to its corresponding IP addresses and vice versa. Enter a DNS IP address in order to be able to use a domain name to access the Switch instead of using an IP address.

Click **Apply** to save settings.

IPv6

IPv6 is an upgraded version to IPv4, providing more available IP addresses as well as other benefits. To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway). To configure IPv6 for the Switch, select whether to you wish to enable **Auto-Configuration**, **Static**, or **DHCPv6 Client**. Next, enter the information for the IP address, range, and gateway.

IPv6

IPv6 Address Settings

IPv6 State: ▼

IPv6 Address: / (1-127)

Gateway:

Link Local Address: fe80::213:64ff:fe00:1500

IPv6 State	Select whether you wish to enable Auto Configuration, DHCPv6 Client, or Static for the IPv6 address.
Auto Configuration	Use this option to set the IPv6 address for the IPv6 network interface in Auto Configuration. The Switch will automatically generate and use a globally-unique IPv6 address based on the network prefix and its Ethernet MAC address.
DHCPv6 Client	This enables the IP address to be configured automatically by the DHCP server. Select this option if you have an IPv6 DHCP server that can assign the Switch an IPv6 address/prefix and a default gateway IP address.
Static	Allows the entry of an IPv6 address/prefix and a default gateway for the Switch. Select this option if you wish to assign static IPv6 address information to the Switch.
IPv6 Address	This field allows the entry of an IPv6 address/prefix to be assigned to this IP interface.
Gateway	Set the default gateway IPv6 address for the interface. Enter the default gateway IPv6 address.

Click **Apply** to save settings.

System Time

Use the System Time screen to view and adjust date and time settings.

The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This switch operates only as an SNTP client and cannot provide time services to other systems.

Current time	Displays the current system time.
Enable SNTP	Select whether to enable or disable system time synchronization with an SNTP server.
Time Zone	Configure the time zone setting either by setting GMT difference or by country.
Daylight Savings Time	Select from Disabled, Recurring or Non-recurring.
Daylight Savings Time Offset	Enter the time of Daylight Savings Time Offset.
Recurring From	Select the Day, Week, Month, and Hour from the list.
Recurring To	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address	Enter the IP address or hostname of the SNTP/NTP server.
Server Port	Enter the server port of the SNTP/NTP server.

To configure date/time through SNMP:

1. Next to the Enable SNTP, select Enable.
2. In the Time Zone Offset list, select by country or by the GMT time zone in which the Switch is located.
3. Next select Disabled, Recurring, or Non-Recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
4. In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.
5. Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1–65535. The default is: 123.
6. Click Apply to update the system settings.

To configure date/time manually:

1. Next to the Enable SNTP, select Disable.
2. In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.
3. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.
4. Next select Disabled, Recurring or Non-recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
5. Click Apply to update the system settings.

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings page allows you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports.

To access the page, click **Port Settings** under the **System** menu.

Port Settings				
	Port	Link Status	Mode	Flow Control
<input type="checkbox"/>			Auto	Disabled
<input type="checkbox"/>	1	Link Down	Auto	Disabled
<input type="checkbox"/>	2	Link Down	Auto	Disabled
<input type="checkbox"/>	3	Link Down	Auto	Disabled
<input type="checkbox"/>	4	Link Down	Auto	Disabled
<input type="checkbox"/>	5	Link Down	Auto	Disabled
<input type="checkbox"/>	6	Link Down	Auto	Disabled
<input type="checkbox"/>	7	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	8	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	9	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	10	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	11	Link Down	Auto	Disabled
<input type="checkbox"/>	12	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk1	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk2	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk3	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk4	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk5	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk6	Link Down	Auto	Disabled

Port	Displays the port number.
Link Status	Indicates whether the link is up or down.
Mode	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port

	uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.</p>

Click **Apply** to save settings.

PoE

The PoE Management screen contains system PoE information for monitoring the current power usage and assigns the total amount of power the Switch can provide to all of its PoE ports. To access the page, click PoE under the System menu.

Note: This feature is only available for PoE supported models listed below.

Model	PoE Capable Ports	PoE Standard	PoE Power Budget
EWS2908P	8	IEEE 802.3af	55 Watts
EWS2910P	8	IEEE 802.3af	55 Watts
EWS5912FP	8	IEEE 802.3af/at	130 Watts
EWS7928P	24	IEEE 802.3af/at	250 Watts
EWS1200-28TFP	24	IEEE 802.3af/at	410 Watts
EWS7926EFP	24	IEEE 802.3af/at	410 Watts
EWS7952P	48	IEEE 802.3af/at	410 Watts
EWS7952FP	48	IEEE 802.3af/at	740 Watts

Power Budget

Power Budget

Settings

Total Power Budget: Watts. (6~130 Watts)

Consumed Power: Watts.

Apply

Total Power Budget: Enter the amount of power the Switch can provide to all ports.

Consumed Power: Displays the total amount of power (in watts) currently being delivered to all PoE ports.

PoE Port Settings

Port	State	Priority	Power Limit Type	User Power Limit (W)	Status	Class	Output Voltage (V)	Output Current (mA)
<input type="checkbox"/>	Enabled	Low	Auto Class					
<input type="checkbox"/> 1	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 2	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 3	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 4	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 5	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 6	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 7	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 8	Enabled	Low	Auto Class		Searching			

Apply

Port	Displays the specific port for which PoE parameters are defined. PoE parameters are assigned to the powered device that is connected to the selected port.
State	Displays the active participating members of the trunk group.
Member Port	<p>Enable: Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery protocol lets the device discover powered devices attached to device interfaces and learns their classification.</p> <p>Disable: Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.</p>
Priority	<p>Select the port priority if the power supply is low. The field default is Low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power.</p> <p>Low: Sets the PoE priority level as low.</p> <p>Medium: Sets the PoE priority level as medium.</p> <p>High: Sets the PoE priority level as high.</p> <p>Critical: Sets the PoE priority level as critical.</p>
Class (Auto)	Shows the classification of the powered device. The class defines the maximum

	<p>power that can be provided to the powered device. The possible field values are:</p> <p>Class 0: The maximum power level at the Power Sourcing Equipment is 15.4 Watts.</p> <p>Class 1: The maximum power level at the Power Sourcing Equipment is 4.0 Watts.</p> <p>Class 2: The maximum power level at the Power Sourcing Equipment is 7.0 Watts.</p> <p>Class 3: The maximum power level at the Power Sourcing Equipment is 15.4 Watts.</p> <p>Class 4: The maximum power level at the Power Sourcing Equipment is 30 Watts.</p>
Class (User Defined)	Select this option to base the power limit on the value configured in the User Power Limit field.
User Power Limit	<p>Set the maximum amount of power that can be delivered by a port.</p> <p>Note: The User Power Limit can only be implemented when the Class value is set to User-Defined.</p>
Status	<p>Shows the port's PoE status. The possible field values are:</p> <p>Delivering Power: The device is enabled to deliver power via the port.</p> <p>Disabled: The device is disabled for delivering power via the port.</p> <p>Test Fail: The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.</p> <p>Testing: The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.</p> <p>Searching: The device is currently searching for a powered device. Searching is the default PoE operational status.</p> <p>Fault: The device has detected a fault on the powered device when the port is forced on. For example, the power supply voltage is out of range, a short occurs, a communication or there is a communication error with PoE devices, or an unknown error occurs.</p>

Click **Apply** to save settings.

EEE

Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 Switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard. The EEE compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet ideal time.

Use the **EEE** configuration page to configure Energy Efficient Ethernet.

Energy-Efficient Ethernet	
Port	EEE Status
<input type="checkbox"/>	Disabled
<input type="checkbox"/> 1	Disabled
<input type="checkbox"/> 2	Disabled
<input type="checkbox"/> 3	Disabled
<input type="checkbox"/> 4	Disabled
<input type="checkbox"/> 5	Disabled
<input type="checkbox"/> 6	Disabled
<input type="checkbox"/> 7	Disabled
<input type="checkbox"/> 8	Disabled
<input type="checkbox"/> 9	Disabled
<input type="checkbox"/> 10	Disabled

Apply

Port	Display the port for which the EEE setting is displayed.
EEE Status	Enable or disable EEE for the specified port.

Click **Apply** to save settings.

L2 Feature

The L2 Feature tab exhibits complete standard-based Layer 2 switching capabilities, including: Link Aggregation, 802.1D Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1s Multiple Spanning Tree Protocol, MAC Address Table, Internet Group Management Protocol (IGMP) Snooping, Port Mirroring, 802.1ab Link Layer Discovery Protocol (LLDP), and Multicast Listener Discovery (MLD) snooping. Utilize these features to configure the Switch to your preferences.

Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch. Link Aggregation is most commonly used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called Members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of the one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- > All ports within a LAG must be the same media/format type.
- > A VLAN is not configured on the port.
- > The port is not assigned to another LAG.
- > The Auto-negotiation mode is not configured on the port.
- > The port is in full-duplex mode.
- > All ports in the LAG have the same ingress filtering and tagged modes.

- > All ports in the LAG have the same back pressure and flow control modes.
- > All ports in the LAG have the same priority.
- > All ports in the LAG have the same transceiver type.
- > Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the participating Switches/devices that support the standard, to use it.

Port Trunking

Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger “pipe”.



Important:

You must enable Trunk Mode before you can add a port to a trunk group.

Group	Active Ports	Member Ports	Mode	
1			Disabled	
2			Disabled	
3			Disabled	
4			Disabled	
5			Disabled	
6			Disabled	
7			Disabled	
8			Disabled	

Group	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups and each group consisting up to 8 ports on the Switch.
Active Ports	Displays the active participating members of the trunk group.
Member Port	Select the ports you wish to add into the trunk group. Up to eight ports per group can be assigned. Static: The Link Aggregation is configured manually for specified trunk group. LACP: The Link Aggregation is configured dynamically for specified trunk group.
Mode	LACP allows for the automatic detection of links in a port trunking group when connected to a LACP-compliant Switch. You will need to ensure that both the Switch and device connected to are in the same mode in order for them to function, otherwise they will not work. Static configuration is used when connecting to a Switch that does not support LACP.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

LACP Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP) and is become for a backup link if a link goes down. The lowest system priority is allowed to make decisions about which ports it is actively participating in in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is: **32768**.



System Priority	Enter the LACP priority value to the system. The default is 32768 and the range is from 1 to 65535.
------------------------	---

Click **Apply** to save settings.

LACP Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between two members of aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is: **Long Timeout**.

	Port	Timeout
<input type="checkbox"/>		Long Timeout ▾
<input type="checkbox"/>	1	Long Timeout
<input type="checkbox"/>	2	Long Timeout
<input type="checkbox"/>	3	Long Timeout
<input type="checkbox"/>	4	Long Timeout
<input type="checkbox"/>	5	Long Timeout
<input type="checkbox"/>	6	Long Timeout
<input type="checkbox"/>	7	Long Timeout
<input type="checkbox"/>	8	Long Timeout
<input type="checkbox"/>	9	Long Timeout
<input type="checkbox"/>	10	Long Timeout
<input type="checkbox"/>	11	Long Timeout
<input type="checkbox"/>	12	Long Timeout

Apply

Timeout	Select the administrative LACP timeout. Long Timeout: The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds. Short Timeout: The LACP PDU will be sent every second. The timeout value is 3 seconds.
----------------	--

Click **Apply** to save settings.

Mirror Settings

Mirrors network traffic by forwarding copies of incoming and outgoing packets from specific ports to a monitoring port. The packet that is copied to the monitoring port will be the same format as the original packet.

Port mirroring is useful for network monitoring and can be used as a diagnostic tool. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring and predicting traffic patterns, and other correlating events. Port Mirroring is needed for traffic analysis on a Switch because a Switch normally sends packets only to the port to which the destination device is connected. The analyzer captures and evaluates the data without affecting the client on the original port. Port mirroring can consume significant CPU resources while active, so be cautious of such usage when configuring the Switch.

Session ID	Destination Port	Source TX Port	Source RX Port	Ingress State	Session State	
1	1			Disabled	Disabled	✓ ✕
2	N/A			Disabled	Disabled	
3	N/A			Disabled	Disabled	
4	N/A			Disabled	Disabled	

Session ID	A number identifying the mirror session. This Switch only supports up to 4 mirror sessions.
Destination Port	Select the port for traffic purposes from source ports mirrored to this port.
Source TX/RX Port	Sets the source port from which traffic will be mirrored. TX Port: Only frames transmitted from this port are mirrored to the destination port. RX Port: Only frames received on this port are mirrored to the destination port. Both: Frames received and transmitted on this port are mirrored to the specified destination port. None: Disables mirroring for this port.
Ingress State	Select whether to enable or disable ingress traffic forwarding.
Session State	Select whether to enable or disable port mirroring.



Note

You cannot mirror a faster port onto a slower port. For example, if you try to mirror the traffic from a 100Mbps port onto a 10Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

STP

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between Switches. This allows the Switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP provides a tree topology for the Switch. There are different types of Spanning tree versions, supported, including Spanning Tree Protocol (STP) IEEE 802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s. Please note that only one spanning tree can be active on the Switch at a time.

Global Settings

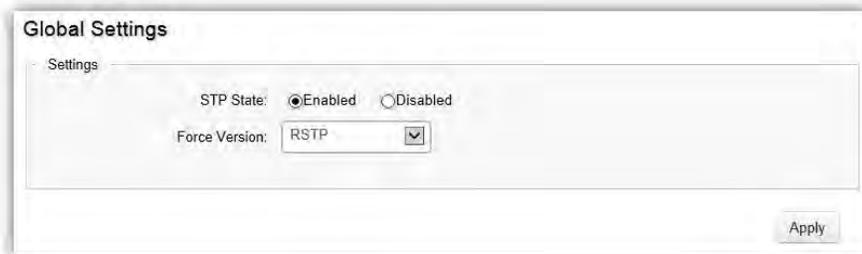
Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on Switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDU after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the Switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links is also accomplished automatically.

STP provides a tree topology and other Spanning tree versions supported include STP, Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP). Please note that only one spanning tree can be active on the Switch at a time. The default setting is: RSTP.



STP	Select whether to enable or disable the spanning tree operation on the Switch.
Force Version	Select the Force Protocol Version parameter for the Switch. STP (Spanning Tree Protocol): IEEE 802.1D RSTP (Rapid Spanning Tree Protocol): IEEE 802.1w MSTP (Multiple Spanning Tree Protocol): IEEE 802.1s

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficient to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network.

This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Select whether to Enable or Disable the Spanning Tree function for the Switch. Next, select whether you wish to enable STP, RSTP, or MSTP. Again, please note that only one Spanning tree function can be active at a time.

Click **Apply** to save settings.

Root Bridge

The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops. From here, you can view all the information regarding the Root Bridge within the STP.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the “root” of the constructed “tree” within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge ID includes two parts; the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is: 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges “listen” for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

Root Bridge	
Root Address:	00:02:6F:AA:AA:AB
Priority:	32768
Cost:	60000
Port:	10
Forward Delay:	15 (sec)
Maximum Age:	20 (sec)
Hello Time:	2 (sec)

Root Address	Displays the root bridge MAC address. Root in root bridge refers to the base of the spanning tree, which the Switch could be configured for.
Priority	Displays the priority for the bridge. When switches are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge.
Forward Delay	Displays the Switch Forward Delay Time. This is the time (in seconds) the root switch will wait before changing states (called listening to learning).
Maximum Age	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

CIST Instance Settings

The Common Instance Spanning Tree (CIST) protocol is formed by the spanning tree algorithm running among bridges that support the IEEE 802.1w, IEEE 802.1s, and IEEE 802.1D standard. A Common and Internal Spanning Tree (CIST) represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP.

The CIST inside a Multiple Spanning Tree Instance (MST) region is the same as the CST outside a region. All regions are bound together using a CIST, which is responsible for creating loop-free topology across regions, whereas the MSTI controls topology inside regions. CST instances allow different regions to communicate between themselves. CST is also used for traffic within the region for any VLANs not covered by a MSTI. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. Multiple regions and other STP bridges are interconnected using a single CST.

CIST Instance Settings

Settings

Priority: 28672 (4096*N)

Maximum Hop: 20 (1-40)

Forward Delay: 15 (4-30)

Maximum Age: 20 (6-40)

TX Hold Count: 6 (1-10)

Hello Time: 2 (1-10)

Apply

Enter the information to set up CIST for the Switch:

Root Address	Displays the root bridge MAC address. Root in root bridge refers to the base of the spanning tree, which the Switch could be configured for.
Priority	Displays the priority for the bridge. When switches are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge.
Forward Delay	Displays the Switch Forward Delay Time. This is the time (in seconds) the root

	switch will wait before changing states (called listening to learning).
Maximum Age	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

Click **Apply** to update the system settings.

CIST Port Settings

Use the CIST Ports Settings page to configure and view STA attributes for interfaces when the spanning tree mode is set to STP or RSTP. You may use a different priority or path cost for ports of the same media type to indicate a preferred path or edge port to indicate if the attached device can support fast forwarding or link type to indicate a point-to-point connection or shared-media connection.

CIST Port Settings															
Port	Priority	Internal Path Cost Conf / Oper	External Path Cost Conf / Oper	Path Cost	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Edge Port Conf / Oper	P2P MAC Conf / Oper	Port Role	Port State	Migration Start	
<input type="checkbox"/>	128			0=Aut											
<input type="checkbox"/>	1	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	2	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	3	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	4	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	5	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	6	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	7	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	8	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	9	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	10	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	280000	32768 / 0 / 88:DC:96:1D:0A:05	0	32768 / 0 / 88:DC:96:1D:0A:05	Yes / No	Auto / Yes	Root	Forwarding	--
<input type="checkbox"/>	11	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	12	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk1	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk2	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk3	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk4	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk5	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--

MST ID	Select the MST ID from the list.
Port	Port or trunked port identifier.
Priority	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a Switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the

	Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0 to 240, in steps of 16; and the default is: 128.
Internal Path Cost Conf/Oper	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
External Path Cost Conf/Oper	The External Path Cost setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge.
Designated Root Bridge	Displays the root bridge for the CST. It is comprised using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	This is the cost to the CIST regional root in a region.
External Root Cost	External root cost is the cost to the CIST root.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	Enter the cost of the port.
Edge Port Conf/Oper	Displays the edge port state.
Designated Bridge	This is the bridge identifier of the bridge of the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Port Role	Each MST bridge port that is enabled is assigned a port role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State	The forwarding state of this port. The state parameters are: Discarding, Learning, Forwarding, or Disabled.

Click **Apply** to update the system settings.

MST Instance Settings

Multiple Spanning Tree Protocol, or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications between STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support STP, RSTP, and MSTP protocols. Once you specify the VLANs you wish to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Click the Edit button to configure the MST settings. Next, enter information for the VLAN List and choose the priority you wish to use from the drop down list.

MST ID	VLAN List	Priority	Regional Root Bridge	Internal Root Cost	Designated Bridge	Root Port	
1		32768	--	0	--	--	
2		32768	--	0	--	--	
3		32768	--	0	--	--	
4		32768	--	0	--	--	
5		32768	--	0	--	--	
6		32768	--	0	--	--	
7		32768	--	0	--	--	
8		32768	--	0	--	--	
9		32768	--	0	--	--	
10		32768	--	0	--	--	
11		32768	--	0	--	--	
12		32768	--	0	--	--	
13		32768	--	0	--	--	
14		32768	--	0	--	--	
15		32768	--	0	--	--	

MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN List	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768. The range is from 0 to 61440. The bridge priority is a multiple of 4096.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the MST instance.
Designated Bridge	Displays the bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Root Port	Displays the port that accesses the designated root for MST instance.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MST Port Settings

This page displays the current MSTI configuration information for the Switch. From here you can update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.

MST Port Settings

	MST ID	Port	Priority	Internal Path Cost Conf / Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Port Role	Port State
<input type="checkbox"/>	1		128						
<input type="checkbox"/>	1	1	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	2	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	3	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	4	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	5	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	6	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	7	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	8	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	9	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	10	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	11	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	12	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk1	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk2	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk3	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk4	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk5	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk6	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk7	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk8	128	0 / 20000	--	--	--	--	--

Apply

MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
Port	Displays port or trunked port ID.
Priority	Select the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is: 32768. The valid range is from 0 to 61440.
Internal Path Cost Conf	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper	Displays the operation cost of the path from this bridge to the root bridge.

Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the selected MST instance.
Designated Bridge	Displays the bridge identifier of the bridge for the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest optimal route automatically for an interface.
Port Role:	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
Port State	Displays the state of the selected port.
Edge Port Ope	Displays the operating edge port state.
P2P MAC Conf	Displays the P2P MAC state.
P2P MAC Oper	Displays the operating P2P MAC state.
Port Role	Displays the port role. Shows each MST bridge port that is assigned a port role for each spanning tree.
Port State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken regarding traffic. The possible port states are: Disabled: STP is disabled on the port. The port forwards traffic while learning MAC addresses. Blocking: The port is blocked and cannot be used to forward traffic or learn MAC addresses. Listening: The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. Learning: The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. Forwarding: The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state.

Click **Apply** to update the system settings.

MAC Address Table

The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the dynamic address. A static address allows you to manually enter a MAC address to configure a specific port and VLAN.

Static MAC Address

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a static MAC address, you set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.



The screenshot shows a configuration window titled "Static MAC Address". It contains four main fields: "Index" with the value "1", "Port" with a dropdown arrow, "VID" with the value "1" and a dropdown arrow, and "MAC Address" with the placeholder text "xx:xx:xx:xx:xx:xx". To the right of the MAC Address field are two buttons: a checkmark icon (Apply) and a close icon (Cancel).

Index	Displays the index for the static MAC address table.
Port	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VID	Enter the VLAN ID on which the IGMP Snooping querier is administratively enabled and for which the VLAN exists in the VLAN database.
MAC Address	Enter a unicast MAC address for which the switch has forwarding or filtering information.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Dynamic MAC Address

The Switch will automatically learn the device's MAC address and store it to the dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The dynamic MAC address table shows the MAC addresses and their associated VLANs learned on the selected port.

MAC Address	VID	Port
00:00:00:01:02:03	1	10
00:02:6F:FE:94:46	1	2
00:02:6F:FE:94:47	1	2
00:02:6F:FE:94:48	1	2
00:04:5F:8D:2D:24	1	10
00:07:11:04:42:0F	1	9
00:08:9B:F1:8F:AE	1	10
00:0C:29:00:85:D3	1	10
00:0C:29:07:ED:6A	1	10
00:0C:29:0C:11:1D	1	10

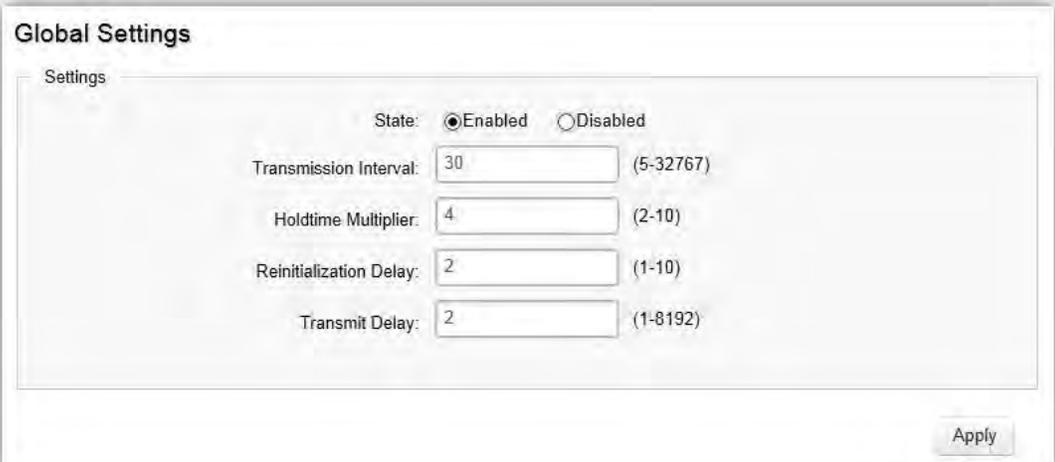
Index	Displays the index for the dynamic MAC address table.
Port	Select the port to which the entry refers.
VID	Displays the VLAN ID corresponding to the MAC address.
MAC Address	Displays the MAC addresses that the Switch learned from a specific port.

LLDP

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to view the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flows in one direction only; from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDPDU is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.

Global Settings



The screenshot shows a 'Global Settings' window with a 'Settings' tab. The 'State' is set to 'Enabled' (radio button selected). Below this are four input fields with their respective values and ranges:

Parameter	Value	Range
Transmission Interval	30	(5-32767)
Holdtime Multiplier	4	(2-10)
Reinitialization Delay	2	(1-10)
Transmit Delay	2	(1-8192)

An 'Apply' button is located at the bottom right of the window.

Select whether to enable or disable the LLDP feature on the Switch. Next, enter the Transmission Interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click Apply to update the system settings.

State	Select Enabled or Disabled to activate LLDP for the Switch.
Transmission Interval	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5 to 32768.
Holdtime Multiplier	Enter the amount of time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2 to 10.
Reinitialization Delay	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1 to 10.
Transmit Delay	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is from 1 to 8191 seconds.

Local Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the Switch.

The screenshot shows a web interface titled "Local Device" with an "Information" section. It contains several fields with their corresponding values:

- Chassis ID Subtype: MAC Address
- Chassis ID: 00:13:64:00:15:00
- System Name: Neihu-7F-EWS5912FP
- System Description: EnGenius EWS5912FP
- Capabilities Supported: Bridge
- Capabilities Enabled: Bridge
- Port ID Subtype: Local

Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device transmitting the LLDP frame.
System Name	Displays the administratively assigned device name.
System Description	Describes the device.

Capabilities Supported	Describes the device functions.
Capabilities Enabled	Describes the device functions.
Port ID Subtype	Displays the port ID type.

Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can viewing detailed LLDP Information for the remote device.

Remote Device														
Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Remote ID	System Name	Time To Live	Auto-Negotiation Supported	Auto-Negotiation Enabled	Auto-Negotiation Advertised Capabilities	Operational MAU Type	802.3 Maximum Frame Size	802.3 Link Aggregation Capability	802.3 Link Aggregation Status	802.3 Link Aggregation Port ID
2	MAC address	00 02 6F FE 94 46	eth0	Janus_test_EWS210AP	72	Disabled	Disabled				0			0
10	MAC address	88 DC 96 1D 0A 05	Locally assigned	g3	EGS7252FP	114	Enabled	Enabled	10GBASE-T half duplex, 10GBASE-T full duplex, 100BASE-TX half duplex, 100BASE-TX full duplex, 1000BASE-T full duplex	1000BASE-T full duplex mode	1522	Capable of being aggregated	Not currently in aggregation	0

Port	Displays the port.
Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype	Displays the port ID type.
Remote ID	Displays the remote ID.
System Name	Displays the administratively assigned device name.
Time to Live	Displays the time to live.
Auto-Negotiation Supported	Displays state for the auto-negotiation supported.
Auto-Negotiation Enabled	Displays state for the auto-negotiation enabled.
Auto-Negotiation Advertised Capabilities	Displays the type of auto-negotiation advertised capabilities.
Operational MAU Type	Displays the type of MAU.
802.3 Maximum Frame Size	Displays the maximum size of 802.3 maximum frame.
802.3 Link Aggregation Capabilities	Displays the 802.3 Link Aggregation capabilities.

802.3 Link Aggregation Status	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID	Displays the port ID of 802.3 Link Aggregation.

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast registers with their local multicast Switch.

A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the Switch from the port.

A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures multicasting accordingly. Based on the IGMP query and report messages, the Switch forwards traffic only to the ports that request the multicast traffic. It enables the Switch to forward packets of multicast groups to those ports that have validated host nodes. The Switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your Switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a broadcast transmission, which forwards packets to all ports on the network.

IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group.

Global Settings

Click to enable or disable the IGMP Snooping feature for the Switch. Next, select whether you wish to use V2 or V3. Finally, select whether you wish to enable or disable the Report Suppression feature for the Switch.

Global Settings

Settings

Status: Enabled Disabled

Version: V2 V3

Report Suppression: Enabled Disabled

Apply

Status	Select to enable or disable IGMP Snooping on the Switch. The Switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled. The default setting is: Disabled.
Version	Select the IGMP version you wish to use. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.
Report Suppression	Select whether Report Suppression is Enabled or Disabled for IGMP Snooping. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Click **Apply** to update the system settings.

VLAN Settings

Use the IGMP Snooping VLAN Settings to configure IGMP Snooping settings for VLANs on the system. The Switch performs IGMP Snooping on VLANs that send IGMP packets. You can specify the VLANs that IGMP Snooping should be performed on. Choose from the drop down box whether to enable or disable IGMP Snooping. Next, choose to enable or disable Fast Leave for the VLAN ID.



VLAN ID	IGMP Snooping Status	Fast Leave
1	Disabled	Disabled

VLAN ID	Displays the VLAN ID.
IGMP Snooping Status	Enables or disables the IGMP Snooping feature for the specified VLAN ID.
Fast Leave	Enables or disables the IGMP Snooping Fast Leave for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an IGMP leave message without first sending out IGMPgroup-specific (GS) queries to the port.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

If Fast Leave is not used, a multicast querier will send a GS-query message when an IGMPv2/v3 group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one IGMP-enabled device.

Fast Leave is supported only with IGMPv2 or IGMPv3 Snooping when IGMP Snooping is enabled. Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

Querier Settings

IGMP Snooping requires that one central Switch to periodically query all end devices on the network to announce their multicast memberships and this central device is the IGMP querier. The snooping Switch sends out periodic queries with a time interval equal to the configured querier query interval. The IGMP query keeps the Switch updated with the current multicast group membership information. If the Switch does not received the updated membership information, then it will stop forwarding multicasts to specified VLANs.

VLAN ID	Querier State	Querier Version	Querier Status	Querier IP	Robustness	Interval	Oper Interval	Max Response Interval	Oper Max Response Interval	Last Member Query Counter	Oper Last Member Query Counter	Last Member Query Interval	Oper Last Member Query Interval
1	Disabled	v2	Non-Querier	—	2	125	125	10	10	2	2	1	1

VLAN ID	Displays the VLAN ID.
Querier State	Select whether to enable or disable the IGMP querier state for the specified VLAN ID. A querier can periodically ask their hosts if they wish to receive multicast traffic. The querier feature will check whether hosts wish to receive multicast traffic when enabled. An elected querier will assume the role of querying the LAN for group members, and then propagates the service requests on to any upstream multicast Switch to ensure that it will continue to receive the multicast service. This feature is only supported for IGMPv1 and v2 snooping.
Querier Version	Enter the version of IGMP packet that will be sent by this port. If an IGMP packet received by the port has a version higher than the specified version, this packet will be dropped.
Robustness	Provides fine-tuning to allow for expected packet loss on a subnet. It is used in calculating the following IGMP message intervals. The default is 2.
Interval	Enter the amount of time in seconds between general query transmissions. The default is 125 seconds.
Oper Interval	Displays the IGMP Interval of the operational querier.
Max Response Interval	Enter the maximum response time used in the queries that are sent by the snooping querier. The default is 10 seconds.
Oper Max Response Interval	Display the maximum response time which used in the queries that are sent by the snooping querier.
Last Member Query	Enter the number of the operational last member querier.

Counter	
Oper Last Member Query Counter	Enter the number of IGMP group-specific queries sent before the switch assumes there are no local members.
Last Member Query Interval	Enter the time between two consecutive group-specific queries that are sent by the querier, including those sent in response to leave group messages. You might lower this interval to reduce the amount of time it takes a querier to detect the loss of the last member of a group.
Oper Last Member Query Interval	Displays the operational last member query interval sent by the elected querier.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Group List

The Group List displays VLAN ID, group IP address, and members port in the IGMP Snooping list.

Group List		
VLAN ID	Group IP Address	Member Ports

Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the Switch will be forwarded to the multicast router reachable from the port.

VLAN ID	Router Ports Auto-Learned	Dynamic Port List	Static Port List	Forbidden Port List
1	Enabled			

VLAN ID	Displays the VLAN ID.
Router Ports Auto-Learned	The Switch will auto detect the presence of a multicast router and forward IGMP packets accordingly.
Dynamic Port List	Displays router ports that have been dynamically configured.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.
Static Port list	Designates a range of ports as being connected to multicast-enabled routers. Ensures that all the packets will reach the multicast-enabled router.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time.

Global Settings

Global Settings

Settings

MLD Snooping Status: Enabled Disabled

MLD Snooping Version: v1 v2

MLD Snooping Report Suppression: Enabled Disabled

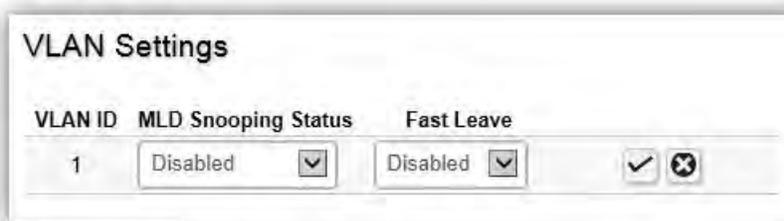
Apply

VLAN ID	Displays the VLAN ID.
Router Ports Auto-Learned	The Switch will auto detect the presence of a multicast router and forward IGMP packets accordingly.
Dynamic Port List	Displays router ports that have been dynamically configured.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.
Static Port list	Designates a range of ports as being connected to multicast-enabled routers. Ensures that all the packets will reach the multicast-enabled router.

Click **Apply** to update the system settings.

VLAN Settings

If the Fast Leave feature is not used, a multicast querier will send a GS-query message when an MLD group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one MLD-enabled device.



VLAN ID	MLD Snooping Status	Fast Leave
1	Disabled	Disabled

Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it. Fast Leave can improve bandwidth usage for a network which frequently experiences many MLD host add and leave requests.

VLAN ID	Displays the VLAN ID.
MLD Snooping Status	Select to enable or disable the MLD snooping feature for the specified VLAN ID.
Fast Leave	Enables or disables the MLD snooping Fast Leave feature for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an MLD leave message without first sending out an MLD group-specific (GS) query to the port.

Select from the drop down list whether to enable or disable MLD Snooping. Next, select to enable or disable Fast Leave for the specified VLAN ID.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Group List

The Group List displays the VLAN ID, IPv6 address, and members port in the MLD Snooping List.



VLAN ID	IPv6 Address	Member Ports
---------	--------------	--------------

Router Settings

The Router Settings feature shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the static and forbidden ports for the specified VLAN IDs that are utilizing MLD Snooping. All MLD packets snooped by the Switch will be forwarded to the multicast router reachable from the port.



VLAN ID	Router Ports Auto-Learned	Dynamic Port List	Static Port List	Forbidden Port List
1	Enabled			<input checked="" type="checkbox"/> <input type="checkbox"/>

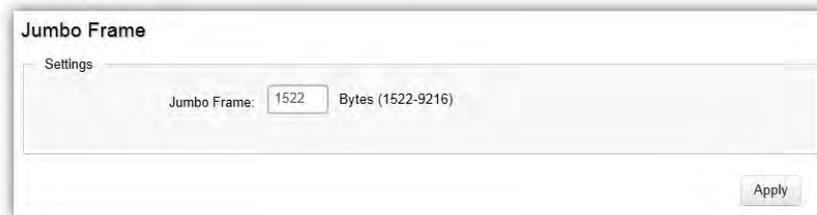
VLAN ID	Displays the VLAN ID.
Router Ports Auto-Learned	The Switch will automatically detect the presence of a multicast router and forward MLD packets accordingly.
Dynamic Port List	Displays router ports that have been dynamically configured.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensure that the forbidden router port will not propagate routing packets out.
Static Port List	Designates a range of ports as being connected to multicast-enabled routers. Ensure that all the packets will reach the multicast-enabled router.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Jumbo Frame

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The switch supports a jumbo frame size of up to **9216 bytes**. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.



Jumbo Frame

Settings

Jumbo Frame: Bytes (1522-9216)

Apply

Jumbo Frame	Enter the size of jumbo frame. The range is from 1522 to 9216 bytes.
--------------------	---

Click **Apply** to update the system settings.

VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same Switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE 802.1Q to perform its functions is in its tags. 802.1Q-compliant Switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.

802.1Q

For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.

VID	Name	Tagged Port	Untagged Port	
1	default		1-12,t1-t8	<input type="button" value="+ Add"/> <input type="button" value="✎"/>

Enabled	Enables 802.1Q VLANs. This feature is enabled by default.
VID	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
Name	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port	Frames transmitted from this port are untagged.



NOTE

The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.

PVID

When an untagged packet enters a Switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address. If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet. Within the Switch, different PVIDs mean different VLANs, so VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1.

PVID

For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.

	Port	PVID	Accept Type		Ingress Filtering
<input type="checkbox"/>		1 ~ 4094	ALL	<input type="checkbox"/>	Enabled <input type="checkbox"/>
<input type="checkbox"/>	1	1	ALL		Enabled
<input type="checkbox"/>	2	1	ALL		Enabled
<input type="checkbox"/>	3	1	ALL		Enabled
<input type="checkbox"/>	4	1	ALL		Enabled
<input type="checkbox"/>	5	1	ALL		Enabled
<input type="checkbox"/>	6	1	ALL		Enabled
<input type="checkbox"/>	7	1	ALL		Enabled
<input type="checkbox"/>	8	1	ALL		Enabled
<input type="checkbox"/>	9	1	ALL		Enabled
<input type="checkbox"/>	10	1	ALL		Enabled
<input type="checkbox"/>	11	1	ALL		Enabled
<input type="checkbox"/>	12	1	ALL		Enabled
<input type="checkbox"/>	trunk1	1	ALL		Enabled
<input type="checkbox"/>	trunk2	1	ALL		Enabled

Port	Displays the VLAN ID to which the PVID tag is assigned. Configure the PVID to assign untagged or tagged frames received on the selected port.
PVID	Enter the PVID value. The range is from 1 to 4094.
Accept Type	Select Tagged Only and Untagged Only from the list. Tagged Only: The port discards any untagged frames it receives. The port only

	<p>accepts tagged frames.</p> <p>Untagged Only: Only untagged frames received on the port are accepted.</p> <p>All: The port accepts both tagged and untagged frames.</p>
Ingress Filtering	<p>Specify how you wish the port to handle tagged frames. Select Enabled or Disabled from the list.</p> <p>Enabled: Tagged frames are discarded if VID does not match the PVID of the port.</p> <p>Disabled: All frames are forwarded in accordance with the IEEE 802.1Q VLAN.</p>



NOTE

To enable PVID functionality, the following requirements must be met:

- > All ports must have a defined PVID.
- > If no other value is specified, the default VLAN PVID is used.
- > If you wish to change the port's default PVID, you must first create a VLAN that includes the port as a member.

Click **Apply** to update the system settings.

Management VLAN

The Management VLAN allows users to transfer the authority of the Switch from the default VLAN to other VLAN IDs. By default, the active management VLAN ID is 1, which allows an IP connection to be established through any port. When the management VLAN is set to a different VLAN, connectivity through the existing management VLAN is lost and an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID.

Management VLAN

For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.

Settings

Management VLAN ID:

Apply

Click **Apply** to update the system settings.

Voice VLAN

Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

Global Settings

Global Settings

Settings

Voice VLAN State: Enabled Disabled

Voice VLAN ID: None

802.1p Remark: Disabled

Remark CoS/802.1p: 6

Aging Time: 1440 (30~65535)min

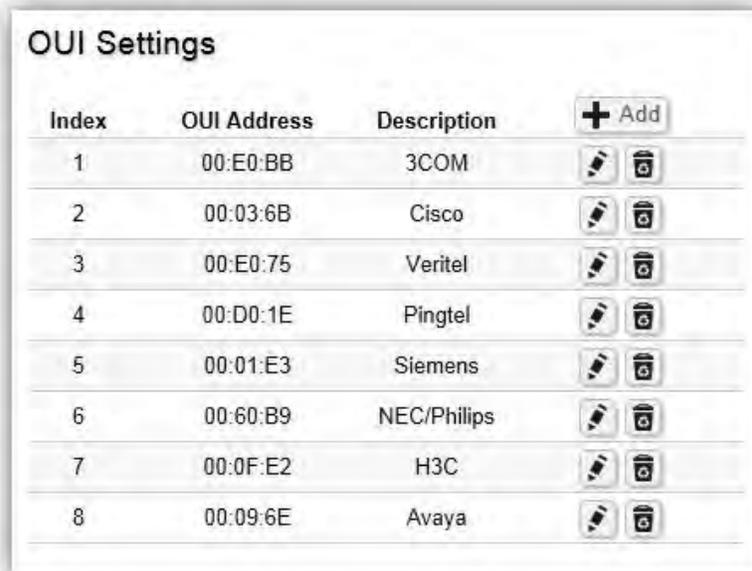
Apply

Voice VLAN State	Select Enabled or Disabled for Voice VLAN on the Switch.
Voice VLAN ID	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the Switch.
802.1p Remark	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p	Defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port. (Range: 0 to 7; Default: 6)
Aging Time	The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 1 to 65535 minutes. The default is 1440 minutes.

Click **Apply** to update the system settings.

OUI Settings

The Switches determines whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a pre-configured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.



Index	OUI Address	Description	+ Add
1	00:E0:BB	3COM	 
2	00:03:6B	Cisco	 
3	00:E0:75	Veritel	 
4	00:D0:1E	Pingtel	 
5	00:01:E3	Siemens	 
6	00:60:B9	NEC/Philips	 
7	00:0F:E2	H3C	 
8	00:09:6E	Avaya	 

Index	Displays the VoIP sequence ID.
OUI Address	This is the globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description	Displays the ID of the VoIP equipment vendor.

To configure the OUI settings, click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specific entry and click the **Add** button to create a new OUI entry.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Port Settings

Enhance your VoIP service further by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.

Port Settings				
	Port	State	CoS Mode	Operate Status
<input type="checkbox"/>		Disabled	Src	
<input type="checkbox"/>	1	Disabled	Src	--
<input type="checkbox"/>	2	Disabled	Src	--
<input type="checkbox"/>	3	Disabled	Src	--
<input type="checkbox"/>	4	Disabled	Src	--
<input type="checkbox"/>	5	Disabled	Src	--
<input type="checkbox"/>	6	Disabled	Src	--
<input type="checkbox"/>	7	Disabled	Src	--
<input type="checkbox"/>	8	Disabled	Src	--
<input type="checkbox"/>	9	Disabled	Src	--
<input type="checkbox"/>	10	Disabled	Src	--
<input type="checkbox"/>	11	Disabled	Src	--
<input type="checkbox"/>	12	Disabled	Src	--
<input type="checkbox"/>	trunk1	Disabled	Src	--
<input type="checkbox"/>	trunk2	Disabled	Src	--
<input type="checkbox"/>	trunk3	Disabled	Src	--
<input type="checkbox"/>	trunk4	Disabled	Src	--

Port	Displays the port to which the Voice VLAN settings are applied.
State	Select Enabled to enhance VoIP quality on the selected port. The default is Disabled.
CoS Mode	Select Src or All from the list. Src: Src QoS attributes are applied to packets with OUIs in the source MAC address. All: All QoS attributes are applied to packets that are classified to the Voice VLAN.
Operate Status	Displays the operating status for the Voice VLAN on the selected port.

Click **Apply** to update the system settings.

Management

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

System Information

Information

System Name: (char : 1 ~ 255)

System Location: (char : 0 ~ 255)

System Contact: (char : 0 ~ 255)

Apply

System Name	Enter the name you wish to use to identify the Switch. You can use up to 255 alphanumeric characters.
System Location	Enter the location of the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.
System Contact	Enter the contact person for the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.

Click **Apply** to update the system settings.

User Management

Use the User Management page to control management access to the Switch based on manually configured user names and passwords. A User account can only view settings without the right to configure the Switch, and an Admin account can configure all the functions of the Switch. Click the Add button to add an account or the Edit button to edit an existing account.

User Name	Password Type	Password	Password Retype	Privilege Type	
admin	Encrypted			Admin	

User Name	Enter a username. You can use up to 18 alphanumeric characters.
Password Type	Select Clear Text or Encrypted from the list.
Password	Enter a new password for accessing the Switch.
Password Retype	Repeat the new password used to access the Switch.
Privilege Type	Select Admin or User from the list to regulate access rights.



Important:

Note that Admin users have full access rights to the Switch when determining the authority of the user account.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Dual Image

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Active	Flash Partition	Status	Image Name	Image Size(Byte)	Created Time
<input type="radio"/>	Partition 0	Backup	IMG-1.05.16-c1.5.3	8273849	2015-07-07 21:50:12
<input checked="" type="radio"/>	Partition 1	Active	IMG-1.05.26-c1.6.24	7320132	2015-11-13 13:38:03

Apply

Active	Selects the partition you wish to be active.
Flash Partition	Displays the number of the partition.
Status	Displays the partition which is currently active on the Switch.
Image Name	Displays the name/version number of the image
Image Size	Displays the size of the image file.
Created Time	Displays the time the image was created.

Click **Apply** to update the system settings.

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as; servers, printers, hubs, Switches, and routers on an Internet Protocol (IP) network. SNMP is used to exchange management information between a network management system (NMS) and a network device. A manager station can manage and monitor the Switch through their network via SNMPv1, v2c and v3. An SNMP managed network consists of two components; agents and a manager.

An agent translates the local management information from the managed Switch into a form that is compatible with SNMP. SNMP allows a manager and agents to communicate with each other for the purpose of accessing Management Information Bases (MIBs). SNMP uses an extensible design, where the available information is defined by MIBs. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

The manager is the console through which network administrators perform network management functions.

Several versions of SNMP are supported. They are v1, v2c, and v3. SNMPv1, which is defined in RFC 1157 "A Simple Network Management Protocol (SNMP)", is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it's required to support older hardware. SNMPv2c, which is defined in RFC 1901 "Introduction to Community-Based SNMPv2", RFC 1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", and RFC 1906 "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)". SNMPv2c updates protocol operations by introducing a GetBulk request and authentication based on community names. Version 2c adds several enhancements to the protocol, such as support for "Informs". Because of this, v2c has become the most widely used version. Unfortunately, a major weakness of v1 and v2c is security. To combat this, SNMP v3 adds a security features that overcome the weaknesses in v1 and v2c. If possible, it is recommended that you use v3 — especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex.

In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment. The SNMPv3 protocol uses different terminology

than SNMPv1 and SNMPv2c as well. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. In the SNMPv3 protocol, agents and managers are renamed to entities. With the SNMPv3 protocol, you create users and determine the protocol used for message authentication as well as if data transmitted between two SNMP entities is encrypted.

The SNMPv3 protocol supports two authentication protocols - HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password to provide even more security.

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. Users can assign views to Community Strings that specify which MIB objects can be accessed by a remote SNMP manager.

The default Community Strings for the Switch used for SNMPv1 and SNMPv2c management access for the Switch are public, which allows authorized management stations to retrieve MIB objects, and private, which allow authorized management stations to retrieve and modify MIB objects.

Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. The SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.

Global Settings

Settings

SNMP State: Enabled Disabled

Engine ID:

Default

(10~64 hex letters, the length of the Engine ID should be even.)

Apply

SNMP State	Enables or disables the SNMP function. The default SNMP global state is: Enabled.
Local Engine ID (10-64 hex characters)	Enter the Switch's Engine ID for the remote clients. A SNMPv3 engine is an independent SNMP agent that resides on the Switch. This engine protects against message replay, delay, and redirection issues. The engine ID is also used in combination with user passwords to generate security keys for authenticating and encrypting SNMPv3 packets. Normally, a local engine ID is automatically generated that is unique to the Switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all local SNMP users will be cleared and you will need to reconfigure all existing users.

Click **Apply** to update the system settings.

View List

SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID) to organize themselves. Each OID identifies a variable that can be read or set via SNMP. The SNMP View List is created for the SNMP management station to manage MIB objects.

Click the **Add** button to create a new entry.

View List

View Name	Subtree OID	Subtree Mask	View Type
all	.1	all	Included

char: 1 ~ 30 max level: 20 char: 1 ~ 20 Included

* If user want to exclude some OID that the parent node included rule must be existed.

View Name	Enter the view name. The view name can contain up to 30 alphanumeric characters.
Subtree OID	Enter the Object Identifier (OID) Subtree. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using a period (.).
Subtree Mask	Select 0 or 1 for Subtree mask. The mask of the Subtree OID 1 means this object number "is concerned", and 0 means "do not concern".
View Type	Select whether the defined OID branch within MIB tree will be Included or Excluded from the selected SNMP view. Generally, if the view type of an entry is Excluded , another entry of view type Included should exist and its OID subtree should overlap the Excluded view entry.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Group List

Configure SNMP Groups to control network access on the Switch by providing users in various groups with different management rights via the Read View, Write View, and Notify View options.



Group List

Group Name	Security Mode	Security Level	Read View	Write View	Notify View
char:1 ~ 30	v1	No Auth	all	None	None

Group Name	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Security Mode	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Level	Select the security level for the group. Security levels apply to SNMPv3 only. No Auth: Neither authentication nor the privacy security levels are assigned to the group. Auth: Authenticates SNMP messages. Priv: Encrypts SNMP messages.
Read View	Management access is restricted to read-only.
Write View	Select a SNMP to allow SNMP write privileges to the Switch's SNMP agent.
Notify View	Select a SNMP group to receive SNMP trap messages generated by the Switch's SNMP agent.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Community List

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. It is important to note that the community name can limit access to the SNMP agent from the SNMP network management station, functioning as a password.

Click **Add** to add a community list to the Switch. Next, name the community and choose the level of access that will be granted to the specified list from the drop down boxes.



Community Name	Community Mode	Group Name	View Name	Access Rights
private	Basic		all	Read Write
public	Basic		all	Read Only

char : 1 ~ 20 Basic Group Name all Read Only

Community Name	Enter the name of SNMP community string.
Community Mode	Selected Basic or Advance from the list. Select the Advance attached to the SNMP group.
Group Name	Select the SNMP group from a list.
View Name	Select the view name from a list.
Access Rights	Specify the level of permission for the MIB objects accessible to the SNMP. Your choices are Read/Write or Read-only .

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

User List

Use the User List page to create SNMP users for authentication with managers using SNMP v3 to associate them to SNMP groups. Click **Add** to add a new user.



Privilege Mode	Select No Auth , Auth , or Priv security level from the list. No auth: Neither authentication nor the privacy security levels are assigned to the group. Auth: Authenticates and ensures that the origin of the SNMP message is authenticated. Priv: Encrypts SNMP messages.
Authentication Protocol	Select the method used to authenticate users. MD5: Using the HMAC-MD5 algorithm. SHA: Using the HMAC-SHA-96 authentication level. Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Authentication Password	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Encryption Protocol	Select the method used to authenticate users. None: No user authentication is used. DES: Using the Data Encryption Standard algorithm.
Encryption Key	Enter the Data Encryption Standard key.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Trap Settings

A trap is a type of SNMP message. The Switch can send traps to an SNMP manager when an event occurs.

You can restrict user privileges by specifying which portions of the MIBs that a user can view. In this way, you restrict which MIBs a user can display and modify for better security. In addition, you can restrict the types of traps users can send as well. You can do this by determining where messages are sent and what types of messages can be sent per user. Traps indicating status changes can be issued by the Switch to the specified trap manager by sending authentication failure messages and other trap messages.

Server IP/Hostname	Enter the server IP or Hostname. The Hostname can contain up to 128 alphanumeric characters.
SNMP Version	Select the SNMP version from the list.
Notify Type	<p>Select the type of notification to be sent.</p> <p>Traps: Traps are sent.</p> <p>Informs: Informes are sent ONLY when v2c is enabled.</p> <p> NOTE: The recipient of a trap message does not send a response to the Switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgment of receipt. Inform messages can be used to ensure that critical information is received by the host. However, please note that informs consume more system resources because they must be kept in memory until a response is received. Informes also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.</p>
Community Name	Select the Community Name from the list.
UDP	Enter the UDP port used to send notifications.
Timeout	Configurable only if the notify type is Informes . Enter the amount of time the device waits before re-sending. The default is 15 seconds.
Retry	Configurable only if the notify type is Informes . Enter the amount of time the

	device waits before re-sending an inform request. The default is 3 seconds.
--	---

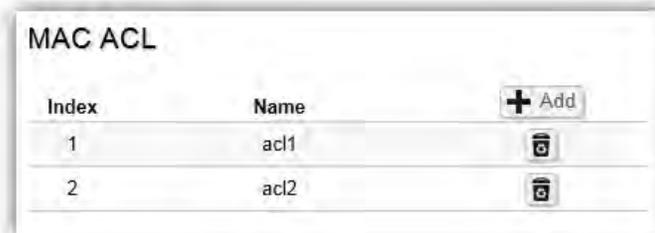
Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

ACL

An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols. Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is considered as a single rule, and up to 256 rules may be defined on each ACL, with up to 3000 rules globally. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

MAC ACL

This page displays the currently-defined MAC-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.



Index	Profile identifier.
Name	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MAC ACE

Use this page to view and add rules to MAC-based ACLs.

Mac-Based ACE

Mac-Based ACE

ACL Name: (Range: 1 - 2147483647, 1 is first processed)

Sequence:

Action:

Destination MAC Address:

Source MAC Address:

VLAN ID: (Range: 1 - 4094)

802.1p Value: (Range: 0 - 7)

Ethertype Value (Hex): (Range: 0600~FFFF)

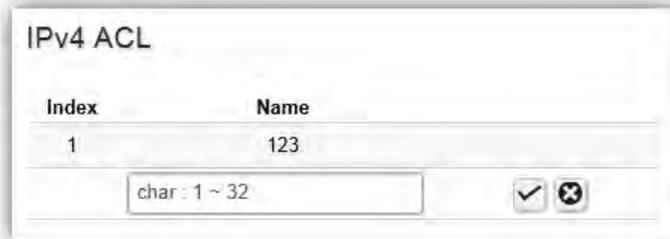
ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action taken if a packet matches the criteria. Permit: Forward packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Destination MAC Value	Enter the destination MAC address.
Destination MAC Wildcard Mask	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Source MAC Value	Enter the source MAC address.
Source MAC Wildcard Mask	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
VLAN ID	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1 to 4094 .

802.1p Value	Enter the 802.1p value. The range is from 0 to 7 .
Ethertype Value	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).

Click **Apply** to update the system settings.

IPv4 ACL

This page displays the currently-defined IPv4-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.



Index	Name
1	123

char: 1 ~ 32

Index	Displays the current number of ACLs.
Name	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv4 ACE

Use this page to view and add rules to IPv4-based ACLs.

The screenshot shows a configuration window titled "IPv4-Based ACE". It contains several input fields: "ACL Name" with the value "123", "Sequence" which is empty, "Action" set to "Permit", "Protocol" set to "Any", "Source IP Address" set to "Any", "Destination IP Address" set to "Any", and "Type of Service" set to "Any". A small note next to the "Sequence" field says "(Range: 1 - 2147483647. 1 is first processed)". An "Apply" button is located at the bottom left of the window.

ACL Name	Select the ACL from the list for which a rule is being created.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action to take if a packet matches the criteria. Permit: Forwards packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Protocol	Select Any , Protocol ID , or Select from a List in the drop down menu. Any: Check Any to use any protocol. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Selects the protocol from the list in the provided field. <ul style="list-style-type: none"> • ICMP: Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host. • IPinIP: IP in IP encapsulates IP packets to create tunnels between two routers. This ensures that IP in IP tunnel appears as a single interface, rather than several separate interfaces. • TCP: Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent. EGP Exterior Gateway Protocol (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network. • IGP: Interior Gateway Protocol (IGP). Enables a routing information exchange between gateways within an autonomous network. • UDP: User Datagram Protocol (UDP). UDP is a communication protocol that

	<p>transmits packets but does not guarantee their delivery.</p> <ul style="list-style-type: none"> • HMP: The Host Mapping Protocol (HMP) collects network information from various networks hosts. HMP monitors hosts spread over the Internet as well as hosts in a single network. • RDP: Reliable Data Protocol (RDP). Provides a reliable data transport service for packet-based applications. • IPv6: Matches the packet to the IPV6 protocol. • IPv6: Rout: Routing Header for IPv6. • IPv6: Frag: Fragment Header for IPv6. • RVSP: Matches the packet to the ReSerVation Protocol(RSVP). • IPv6: ICMP: The Internet Control Message Protocol (ICMP) allows the gateway or destination host to communicate with the source host. • OSPF: The Open Shortest Path First (OSPF) protocol is a link-state hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocols. It is an extension to the PPP protocol • that enables ISPs to operate Virtual Private Networks (VPNs). • PIM: Matches the packet to Protocol Independent Multicast (PIM). • L2TP: Matches the packet to Internet Protocol (L2IP).
Source IP Address Value	Enter the source IP address.
Source IP Mask	Enter the mask of the new source IP address.
Destination IP Address Value	Enter the destination IP address.
Destination IP Mask	Enter the mask of the new source IP address.
Type of Service	Select Any or DSCP to match from drop down list. When DSCP to match is selected, enter the DSCP. The range is from 0 to 63.
ICMP Type	Select Any , Protocol ID , or Select from List from drop down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. The range is from 0 to 255. Select from List: Select the ICMP from the list in the provided field.
ICMP Code	Select Any or User Defined from drop down menu. When User Defined is selected, enter the ICMP code value. The range is from 0 to 255.

Click **Apply** to update the system settings.

IPv6 ACL

This page displays the currently-defined IPv6-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.



The screenshot shows a dialog box titled "IPv6 ACL". It contains two columns: "Index" and "Name". Below the "Name" column, there is a text input field with the placeholder text "char : 1 ~ 32". To the right of the input field are two buttons: a checkmark icon (Apply) and a close icon (Cancel).

Index	Displays the current number of ACLs.
Name	Enter the IPv6 based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

IPv6 ACE

Allows IPv6 Based Access Control Entry (ACE) to be defined within a configured ACL.

ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action taken if a packet matches the criteria. Permit: Forward packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Protocol	Select the Any, Protocol ID, or Select from List from drop down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Select the protocol from the list in the provided field.
Source IP Address Value	Enter the source IP address.
Source IP Prefix Length	Enter the prefix length of the new source IP address. The range is from 0 to 128.
Destination IP Address Value	Enter the destination IP address.
Destination IP Prefix Length	Enter the prefix length of the new source IP address. The range is from 0 to 128.
Source Port	Select Single or Range from the list. Enter the source port that is

	matched to packets. The range is from 0 to 65535.
Destination Port	Select Single or Range from the list. Enter the destination port that is matched to packets. The range is from 0 to 65535.
TCP Flags	Select whether to handle each six TCP control flags; URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), and FIN (Fin) from drop down menu. Don't Care: The ACE do not treat the TCP control flag. Set: The packet with the TCP control flag being set matches the criteria. Unset: The packet with the TCP control flag being unset matches the criteria.
Type of Service	Select Any or DSCP to match from drop down list. When DSCP to match is selected, enter the DSCP. The range is from 0 to 63.

Click **Apply** to update the system settings.

ACL Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.

Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	(none) ▼	(none) ▼	(none) ▼
<input type="checkbox"/> 1			
<input type="checkbox"/> 2			
<input type="checkbox"/> 3			
<input type="checkbox"/> 4			
<input type="checkbox"/> 5			

Port	Select the port for which the ACLs are bound to.
MAC ACL	Select the MAC ACL rule to apply to the port.
IPv4 ACL	Select the IPv4 ACL rule to apply to the port.
IPv6 ACL	Select the IPv6 ACL rule to apply to the port.

Click **Apply** to update the system settings.

QoS

Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS is a means of providing consistent and predictable data delivery to the Switch by distinguishing between packets that have stricter timing requirements from those that are more tolerant of delays. QoS enables traffic to be prioritized while avoiding excessive broadcast and multicast traffic. Traffic such as Voice and Video streaming which require minimal delays can be assigned to a high priority queue, while other traffic can be assigned to a lower priority queue, resulting in uninterrupted actions. Without QoS, all traffic data is as likely to be dropped when the network is congested. This can result in reductions in network performance and hinder the network in time-critical situations.

In a Switch, multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission within a port, the rate at which it is processed depends on how the queue is configured and the amount of traffic present within other queues on the port. If a delay is necessary, packets are held in the queue until they are authorized for transmission.

Global Settings

There are two options for applying QoS information onto packets: the 802.1p Class of Service (CoS) priority field within the VLAN tag of tagged Ethernet frames, and Differentiated Services (DiffServ) Code Point (DSCP). Each port on the Switch can be configured to trust one of the packet fields (802.1p, DSCP or DSCP+802.1p). Packets that enter the Switch's port may carry no QoS information as well. If so, the Switch places such information into the packets before transmitting them to the next node. Thus, QoS information is preserved between nodes within the network and the nodes know which label to give each packet. A trusted field must exist in the packet for the mapping table to be of any use. When a port is configured as untrusted, it does not trust any incoming packet priority designations and uses the port default priority value instead to process the packet.

Global Settings

Qos Global

State: Enabled Disabled

Scheduling Method: Strict Priority

Trust Mode: 802.1p

Apply

State	Select whether QoS is enabled or disabled on the switch.
Scheduling Method	Selects the Strict Priority or WRR to specify the traffic scheduling method. Strict Priority: Specifies traffic scheduling based strictly on the queue priority. WRR: Use the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.
Trust Mode	Select which packet fields to use for classifying packets entering the Switch. DSCP: Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. 802.1p: Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE 802.1p are from 1 to 8.

Click **Apply** to update the system settings.

CoS Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

	CoS	Queue
<input checked="" type="checkbox"/>	1	1
<input type="checkbox"/>	0	2
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	3
<input type="checkbox"/>	3	4
<input type="checkbox"/>	4	5
<input type="checkbox"/>	5	6
<input type="checkbox"/>	6	7
<input type="checkbox"/>	7	8

Apply

CoS	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to update the system settings.

DSCP Mapping

Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.

	DSCP	Queue
<input type="checkbox"/>		1
<input type="checkbox"/>	0	1
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	1
<input type="checkbox"/>	3	1
<input type="checkbox"/>	4	1
<input type="checkbox"/>	5	1
<input type="checkbox"/>	6	1
<input type="checkbox"/>	7	1
<input type="checkbox"/>	8	2
<input type="checkbox"/>	9	2
<input type="checkbox"/>	10	2
<input type="checkbox"/>	11	2
<input type="checkbox"/>	12	2

DSCP	Displays the packet's DSCP values, where 0 is the lowest and 10 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to update the system settings.

Port Settings

From here, you can configure the QoS port settings for the Switch. Select a port you wish to set and choose a CoS value from the drop down box. Next, Select to enable or disable the Trust setting to let any CoS packet be marked at ingress.

Port Settings			
<input type="checkbox"/>	Port	CoS Value	Trust
<input type="checkbox"/>		0	Enabled
<input type="checkbox"/>	1	1	Enabled
<input type="checkbox"/>	2	0	Enabled
<input type="checkbox"/>	3	0	Enabled
<input type="checkbox"/>	4	0	Enabled
<input type="checkbox"/>	5	0	Enabled
<input type="checkbox"/>	6	0	Enabled
<input type="checkbox"/>	7	0	Enabled
<input type="checkbox"/>	8	0	Enabled
<input type="checkbox"/>	9	0	Enabled
<input type="checkbox"/>	10	0	Enabled
<input type="checkbox"/>	11	0	Enabled
<input type="checkbox"/>	12	0	Enabled
<input type="checkbox"/>	trunk1	0	Enabled
<input type="checkbox"/>	trunk2	0	Enabled
<input type="checkbox"/>	trunk3	0	Enabled
<input type="checkbox"/>	trunk4	0	Enabled
<input type="checkbox"/>	trunk5	0	Enabled
<input type="checkbox"/>	trunk6	0	Enabled
<input type="checkbox"/>	trunk7	0	Enabled
<input type="checkbox"/>	trunk8	0	Enabled

Port	Displays the ports for which the CoS parameters are defined.
CoS Value	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust	Select Enabled to trust any CoS packet marking at ingress. Select Disabled to not trust any CoS packet marking at ingress.

Click **Apply** to update the system settings.

Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port's Ingress Rate Limit and Egress Rate.

Bandwidth Control

	Port	Ingress	Ingress Rate (kbps)	Egress	Egress Rate (kbps)
<input type="checkbox"/>		Disabled ▾	1000000	Disabled ▾	1000000
<input type="checkbox"/>	1	Disabled	Off	Disabled	Off
<input type="checkbox"/>	2	Disabled	Off	Disabled	Off
<input type="checkbox"/>	3	Disabled	Off	Disabled	Off
<input type="checkbox"/>	4	Disabled	Off	Disabled	Off
<input type="checkbox"/>	5	Disabled	Off	Disabled	Off
<input type="checkbox"/>	6	Disabled	Off	Disabled	Off
<input type="checkbox"/>	7	Disabled	Off	Disabled	Off
<input type="checkbox"/>	8	Disabled	Off	Disabled	Off
<input type="checkbox"/>	9	Disabled	Off	Disabled	Off
<input type="checkbox"/>	10	Disabled	Off	Disabled	Off
<input type="checkbox"/>	11	Disabled	Off	Disabled	Off
<input type="checkbox"/>	12	Disabled	Off	Disabled	Off

Port	Displays the ports for which the bandwidth settings are displayed.
Ingress	Select enable or disable ingress on the interface.
Ingress Rate	Enter the ingress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress	Select from the drop down box to Enable or Disable egress on the interface.
Egress Rate	Enter the egress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.

Click **Apply** to update the system settings.

Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The Switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

Storm Control

Port	Status	Broadcast (kbps)	Unknown Multicast (kbps)	Unknown Unicast (kbps)
<input type="checkbox"/>	Disabled <input type="checkbox"/>	<input type="checkbox"/> 15-1000000, Enter 15'	<input type="checkbox"/> 15-1000000, Enter 15'	<input type="checkbox"/> 15-1000000, Enter 15'
<input type="checkbox"/>	1 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	2 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	3 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	4 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	5 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	6 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	7 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	8 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	9 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	10 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	11 Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	12 Disabled	Off (10000)	Off (10000)	Off (10000)

Port	Displays the ports for which the Storm Control information is displayed.
Status	Select whether Storm Control is Enabled or Disabled ingress on the interface.
Broadcast	Enter the broadcast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

Unknown Multicast	Enter the Unknown Multicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast	Enter the Unknown Unicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

Click **Apply** to update the system settings.

Security

802.1x

The IEEE 802.1X standard authentication uses the RADIUS (Remote Authentication Dial In User Service) protocol to validate users and provide a security standard for network access control. The user that wishes to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. The mediating device, such as a Switch, is called the authenticator. Clients connected to a port on the Switch must be authenticated by the Authentication server (RADIUS) before accessing any services offered by the Switch on the LAN. Use a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the client and server. This establishes the requirements needed for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

Global Settings

When a supplicant is connected to a Switch port, the port issues an 802.1X authentication request to the attached the 802.1X supplicant. The supplicant replies with the given username and password and an authentication request is then passed to a configured RADIUS server. The authentication server's user database supports Extended Authentication Protocol (EAP), which allows particular guest VLAN memberships to be defined based on each individual user. After authorization, the port connected to the authenticated supplicant then becomes a member of the specified guest VLAN. When the supplicant is successfully authenticated, traffic is automatically assigned to the guest VLAN. The EAP authentication methods supported by the Switch are: EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Global Settings

802.1x Global

State: Enabled Disabled

Guest VLAN: Enabled ▼

Guest VLAN ID: 1 ▼

Apply

State	Select whether authentication is Enabled or Disabled on the Switch.
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the Switch. The default is Disabled.
Guest VLAN ID	Select the guest VLAN ID from the list of currently defined VLANs.

Click **Apply** to update the system settings.

Port Settings

The IEEE 802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides the required credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification to the guest VLAN. If the authentication server determines the credentials are valid, the supplicant is allowed to access resources located on the protected side of the network.

From here, you can configure the port settings as they relate to 802.1X. First, select the mode from you wish to utilize from the drop down box. Next, choose whether to enable or disable re-authentication for the port. Enter the time span that you wish to elapse for the re-authentication Period, Quiet Period, and Supplicant Period. After this, enter the max number of times you wish for the Switch to retransmit the EAP request. Finally, choose whether you wish to enable or disable the VLAN ID.

Port Settings										
Port	Mode	Reauthentication	Reauthentication period	Quiet Period	Supplicant Period	Max Retry	Authorized Status	Guest VLAN		
<input type="checkbox"/>	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled		
<input type="checkbox"/>	1	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	2	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	3	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	4	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	5	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	6	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	7	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	8	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	9	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	10	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	11	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	
<input type="checkbox"/>	12	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled	

Apply

Port	Displays the ports for which the 802.1X information is displayed.
Mode	Select Auto or Force_UnAuthorized or Force_Authorized mode from the list.
Re-Authentication	Select whether port re-authentication is Enabled or Disabled.
Re-authentication period	Enter the time span in which the selected port is re-authenticated. The default is 3600 seconds.
Quiet Period	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.
Supplicant Period	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Max Retry	Enter the maximum number of times that the Switch retransmits an EAP request to the client before it times out the authentication session. The default is 2 times.
Guest VLAN ID	Select whether guest VLAN ID is Enabled or Disabled.

Click **Apply** to update the system settings.

Authenticated Host

The Authenticated Host section displays the Authenticated User Name, Port, Session Time, Authenticated Method, and Mac Address.

Authenticated Host				
User Name	Port	Session Time	Authenticate Method	MAC Address

RADIUS Server

RADIUS proxy servers are used for centralized administration. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service for greater convenience. RADIUS is a server protocol that runs in the application layer, using UDP as transport. The Network Switch with port-based authentication and all have a RADIUS client component that communicates with the RADIUS server. Clients connected to a port on the Switch must be authenticated by the Authentication server before accessing services offered by the Switch on the LAN. Use a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the client and server. The RADIUS server maintains a user database, which contains authentication information. The Switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network.

Index	Server IP	Authorized Port	Key String	Timeout Reply	Retry	Server Priority	Dead Timeout
	x.x.x.x	1812	char:	3	3	1	0

Index	Displays the index for which RADIUS server is displayed.
Server IP	Enter the RADIUS server IP address.
Authorized Port	Enter the authorized port number. The default port is 1812.
Accounting Port	Enter the name you wish to use to identify this Switch.
Key String	Enter the key string used for encrypting all RADIUS communication between the device and the RADIUS server.
Timeout Reply	Enter the amount of time the device waits for an answer from the RADIUS server before switching to the next server. The default value is 3.
Retry	Enter the number of transmitted requests sent to the RADIUS server before a failure occurs. The default is 3.
Server Priority	Enter the priority for the RADIUS server.
Dead Timeout	Enter the amount of time that the RADIUS server is bypassed for service requests. The default value is 0.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Access

HTTP(S) Settings

The EnGenius Switch provides a built-in browser interface that enables you to configure and manage the Switch via Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) requests selectively to help prevent security breaches on the network. You can manage your HTTP and HTTPS settings for the Switch further by choosing the length of session timeouts for HTTP and HTTPS requests. Select whether to enable or disable the HTTP service and enter the HTTP Timeout session. Next, select whether to enable or disable the HTTPS service and enter the HTTPS timeout session for the Switch.

Http & Https Settings

Settings

HTTP Service: Enabled Disabled

HTTP Session Timeout: 0~86400 minutes (0 : no limit)

HTTPS Service: Enabled Disabled

HTTPS Session Timeout: 0~86400 minutes (0 : no limit)

Apply

HTTP Service	Select whether HTTP service for the Switch is Enabled or Disabled. This is enabled by default.
HTTP Session Timeout	Enter the amount of time that elapses before HTTP is timed out. The default is 5 minutes. The range is from 0 to 86400 minutes.
HTTPS Service	Select whether the HTTP service is Enabled or Disabled. This is disabled by default.
HTTPS Session Timeout	Enter the amount of time that elapses before HTTPS is timed out. The default is 5 minutes. The range is from 0 to 86400 minutes.

Click **Apply** to update the system settings.

Telnet Settings

From here, you can configure and manage the Switch's Telnet protocol settings. The Telnet protocol is a standard Internet protocol which enables terminals and applications to interface over the Internet with remote hosts by providing Command Line Interface (CLI) communication using a virtual terminal connection. This protocol provides the basic rules for making it possible to link a client to a command interpreter. The Telnet service for the Switch is enabled by default. Please note that for secure communication, it is better to use SSH over Telnet. To enable and configure SSH Settings, please refer to SSH Settings on the next page.

Telnet Settings

Settings

Telnet Service: Enabled Disabled

Session Timeout: (0-65535) minutes

History Count: (0-256) (0 is disabled)

Password Retry Count: (0-120)

Silent Time: (0-65535) seconds

Apply

Telnet Service	Select whether the Telnet service is Enabled or Disabled. It is enabled by default.
Session Timeout	Enter the amount of time that elapses before the Telnet service is timed out. The default is 5 minutes. The range is from 0 to 65535 minutes.
History Count	Enter the entry number for history of Telnet service. The default is 128. The range is from 0 to 256.
Password Retry Count	Enter the number of password request send to Telnet service. The default is 3. The range is from 0 to 120.
Silent Time	Enter the silent time for Telnet service. The range is from 0 to 65535 seconds.

Click **Apply** to update the system settings.

SSH Settings

Secure Shell (SSH) is a cryptographic network protocol for secure data communication network services. SSH is a way of accessing the command line interface on the network Switch. The traffic is encrypted, so it is difficult to eavesdrop on as it creates a secure connection within an insecure network such as the Internet. Even if an attacker was able to view the traffic, the data would be incomprehensible without the correct encryption key to decode it.

To configure SSH settings for the Switch, first select whether you wish to enable or disable the SSH service for the Switch. Note that SSH is more secure than the Telnet service when

deciding between which service to use. Enter the session timeout you wish to implement for SSH. Next, enter the History Count number you wish. The default count is: 128. Enter the number of passwords requests to be sent across SSH. The default attempts is: 3. Finally, enter the silent time you wish to implement for the SSH service.

SSH Settings

Settings

SSH Service: Enabled Disabled

Session Timeout: (0-65535) minutes

History Count: (0-256) (0 is disabled)

Password Retry Count: (0-120)

Silent Time: (0-65535) seconds

Apply

Telnet Service	Select whether the Telnet service is Enabled or Disabled. It is enabled by default.
Session Timeout	Enter the amount of time that elapses before the Telnet service is timed out. The default is 5 minutes. The range is from 0 to 65535 minutes.
History Count	Enter the entry number for history of Telnet service. The default is 128. The range is from 0 to 256.
Password Retry Count	Enter the number of password request send to Telnet service. The default is 3. The range is from 0 to 120.

Silent Time	Enter the silent time for Telnet service. The range is from 0 to 65535 seconds.
--------------------	---

Click **Apply** to update the system settings.

Console Settings

From here, you can configure the Console service settings for the Switch.

Session Timeout	Enter the amount of time that elapses before Console service is timed out. The default is 5 minutes. The range is from 0 to 65535 minutes.
History Count	Enter the entry number for history of Console service. The default is 128. The range is from 0 to 256.
Password Retry Count	Enter the number of password requests to send to the Console service. The default is 3. The range is from 0 to 120.
Silent Time	Enter the silent time for Console service. The range is from 0 to 65535 seconds.

Click **Apply** to update the system settings.

Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.

	Port	State	Max MAC Address
<input type="checkbox"/>		Disabled <input type="button" value="v"/>	<input type="text" value="256"/>
<input type="checkbox"/>	1	Disabled	256
<input type="checkbox"/>	2	Disabled	256
<input type="checkbox"/>	3	Disabled	256
<input type="checkbox"/>	4	Disabled	256
<input type="checkbox"/>	5	Disabled	256
<input type="checkbox"/>	6	Disabled	256
<input type="checkbox"/>	7	Disabled	256
<input type="checkbox"/>	8	Disabled	256
<input type="checkbox"/>	9	Disabled	256
<input type="checkbox"/>	10	Disabled	256
<input type="checkbox"/>	11	Disabled	256
<input type="checkbox"/>	12	Disabled	256

Max MAC Address	Enter the maximum number of MAC addresses that can be learned on the port. The range is from 1 to 256.
Port	Displays the port for which the port security is defined.
State	Select Enabled or Disabled for the port security feature for the selected port.

Click **Apply** to update the system settings.

Port Isolation

Port Isolation feature provides L2 isolation between ports within the same broadcast domain. When enabled, **Isolated ports** can forward traffic to **Not Isolated ports**, but not to other **Isolated ports**. **Not Isolated ports** can send traffic to any port; whether **Isolated** or **Not Isolated**. The default setting is **Not Isolated**.

Port Isolation		
	Port	Status
<input type="checkbox"/>		Not Isolated <input type="button" value="v"/>
<input type="checkbox"/>	1	Not Isolated
<input type="checkbox"/>	2	Not Isolated
<input type="checkbox"/>	3	Not Isolated
<input type="checkbox"/>	4	Not Isolated
<input type="checkbox"/>	5	Not Isolated
<input type="checkbox"/>	6	Not Isolated
<input type="checkbox"/>	7	Not Isolated
<input type="checkbox"/>	8	Not Isolated
<input type="checkbox"/>	9	Not Isolated
<input type="checkbox"/>	10	Not Isolated

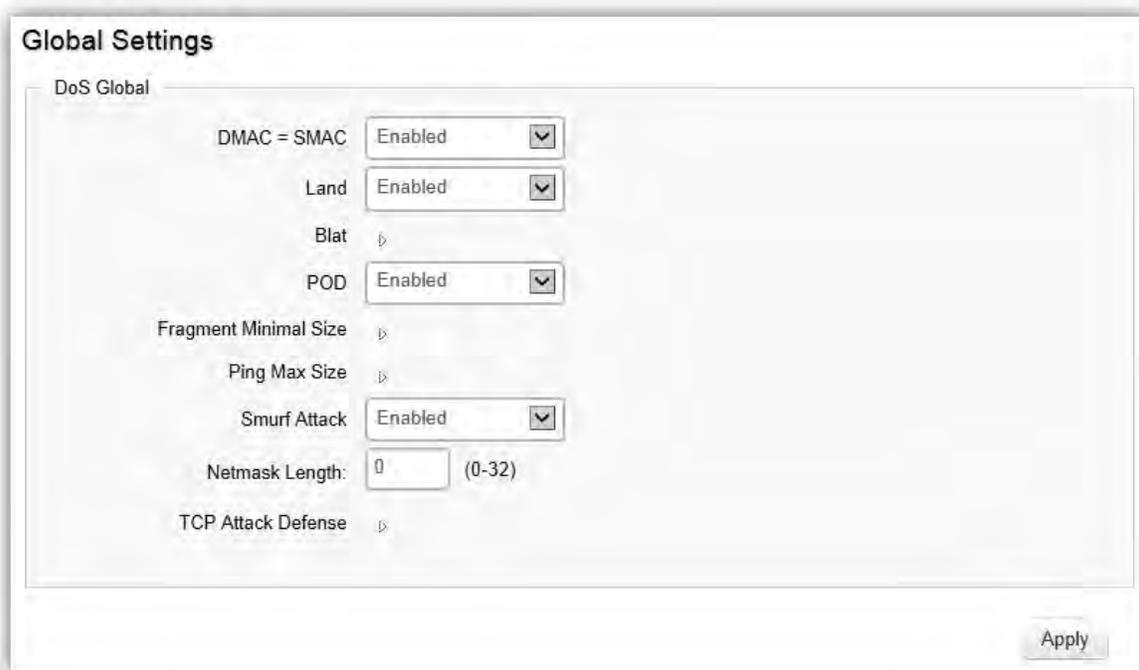
Click **Apply** to update the system settings.

DoS

DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the Switch to monitor and block different types of attacks.

Global Settings

On this page, the user can enable or disable the prevention of different types of DoS attacks. When enabled, the switch will drop the packets matching the types of DoS attack detected.



The screenshot shows a web interface titled "Global Settings" with a sub-section "DoS Global". The settings are as follows:

Setting	Value
DMAC = SMAC	Enabled
Land	Enabled
Blat	⌵
POD	Enabled
Fragment Minimal Size	⌵
Ping Max Size	⌵
Smurf Attack	Enabled
Netmask Length:	0 (0-32)
TCP Attack Defense	⌵

An "Apply" button is located at the bottom right of the settings area.

Click **Apply** to update the system settings.

Port Settings

From here you can configure the Port Settings for DoS for the Switch. Select from the drop down list whether you wish to enable or disable DoS protection for the Switch.

Port Settings		
	Port	DoS Protection
<input type="checkbox"/>		Disabled <input type="button" value="v"/>
<input type="checkbox"/>	1	Disabled
<input type="checkbox"/>	2	Disabled
<input type="checkbox"/>	3	Disabled
<input type="checkbox"/>	4	Disabled
<input type="checkbox"/>	5	Disabled
<input type="checkbox"/>	6	Disabled
<input type="checkbox"/>	7	Disabled
<input type="checkbox"/>	8	Disabled
<input type="checkbox"/>	9	Disabled

Port	Displays the port for which the DoS protection is defined.
DoS Protection	Select Enabled or Disabled for the DoS protection feature for the selected port.

Click **Apply** to update the system settings.

Monitoring

Port Statistics

The Port Statistics page displays a summary of all port traffic statistics.

Port Statistics													
	Port	RXByte	RXUcast	RXNUcast	RXDiscard	TXByte	TXUcast	TXNUcast	TXDiscard	RXMcast	RXBcast	TXMcast	TXBcast
<input type="checkbox"/>													
<input type="checkbox"/>	1	68425444	256869	39943	0	1608175557	384133	11968890	0	32978	6965	3299502	8669388
<input type="checkbox"/>	2	1183982561	4423669	591931	0	1202944962	6789468	64236755	0	218709	373222	17637471	46599284
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	14543	0	113	0	652787142	740821	4367228	10	51	62	1022949	3344279
<input type="checkbox"/>	7	1422341998	5321905	17279	0	3721828038	5893463	82980852	0	4190	13089	21025720	61955132
<input type="checkbox"/>	8	1258800280	5333578	69426	0	1916129700	6792252	82929143	0	63296	6130	20966739	61962404
<input type="checkbox"/>	9	395175390	5716714	237502	0	355120309	5674469	82760755	0	111212	126290	20918692	61842063
<input type="checkbox"/>	10	1579406332	28707090	82155864	0	769244081	26430416	963478	0	20738436	61417428	412219	551259

Port	Displays the port for which statistics are displayed.
RXByte	Displays the number of all packets received on the port.
RXUcast	Displays the number of unicast packets received on the port.
RXNUcast	Displays the number of unicast packets received on the port.
RXDiscard	Displays the number of received packets discarded on the port.
TXByte	Displays the number of all packets transmitted on the port.
TXUcast	Displays the number of unicast packets transmitted on port.
TXNUcast	Displays the number of unicast packets transmitted on the port.
TXDiscard	Displays the number of transmitted packets discarded on the port.
RXMcast	Displays the number of multicast packets received on the port.
RXBcast	Displays the number of broadcast packets received on the port.
TXMcast	Displays the number of multicast packets transmitted on the port.
TXBcast	Displays the number of broadcast packets transmitted on the port.

RMON

Remote Network Monitoring, or RMON is used for support monitoring and protocol analysis of LANs by enabling various network monitors and console systems to exchange network monitoring data through the Switch.

Event List

The Event List defines RMON events on the Switch.



Index	Event Type	Community	Description	Last Time Sent	Owner
1 ~ 65535	Log	private	char: 0 ~ 127		char: 0 ~ 32

Index	Enter the entry number for event.
Event Type	Select the event type. Log: The event is a log entry. SNMP Trap: The event is a trap. Log & Trap: The event is both a log entry and a trap.
Community	Enter the community to which the event belongs.
Description	Displays the number of good broadcast packets received on the interface.
Last Time Sent	Displays the time that event occurred.
Owner	Enter the switch that defined the event.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Event Log Table

From here, you can view specific event logs for the Switch. Choose an event log you wish to view from the drop down list.



The 'Event Log Table' interface features a title bar, a 'Select Event Index:' label, a dropdown menu currently set to 'none', and a 'Refresh' button.

Alarm List

You can configure network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop down boxes.



The 'Alarm List' form contains several fields: Index (1), Sample Port (1), Sample Variable (DropEvents), Sample Interval (1), Sample Type (Absolute), Rising Threshold (0-214), Falling Threshold (0-214), Rising Event (empty), Falling Event (empty), and Owner (chi). Each field has a dropdown arrow, and there are checkmark and cancel icons at the bottom right.

Index	Enter the entry number for the Alarm List.
Sample Port	Select the port from which the alarm samples were taken.
Sample Variable	Select the variable of samples for the specified alarm sample.
Sample Interval	Enter the alarm interval time.
Sample Type	Select the sampling method for the selected variable and comparing the value against the thresholds. Absolute: Compares the values with the thresholds at the end of the sampling interval. Delta: Subtracts the last sampled value from the current value.
Rising Threshold	Enter the rising number that triggers the rising threshold alarm.
Falling Threshold	Enter the falling number that triggers the falling threshold alarm.
Rising Event	Enter the event number by the falling alarm are reported.
Falling Event	Enter the event number by the falling alarms are reported.
Owner	Enter the Switch that defined the alarm.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

History List

History List

Index	Sample Port	Bucket Requested	Interval	Owner	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1 ~ 65535	1	1 ~ 50	1 ~ 3600	char: 0 ~ 32		

Index	Enter the entry number for the History List.
Sample Port	Select the port from which the history samples were taken.
Bucket Requested	Enter the number of samples to be saved. The range is from 1 to 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1 to 3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0 to 32 characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

History Log Table

From here, you can view the History Index for history logs on the Switch. Select a history index to view from the drop down box.

History Log Table

Select History Index: none ▼ Refresh

Statistics

From here, you can view all the RMON statistics of the Switch.

Statistics																		
	Port	Drop Events	Octets	Pkts	Broadcast Pkts	Multicast Pkts	CRC Align Errors	Under Size Pkts	Over Size Pkts	Fragments	Jabbers	Collisions	Pkts 64 Octets	Pkts 65 to 127 Octets	Pkts 128 to 255 Octets	Pkts 256 to 511 Octets	Pkts 512 to 1023 Octets	Pkts 1024 to 1518 Octets
<input type="checkbox"/>																		
<input type="checkbox"/>	1	0	68425444	296812	6965	32978	0	0	0	0	0	0	119763	82197	32811	13992	40047	8002
<input type="checkbox"/>	2	0	1183991729	5015632	373236	218717	0	0	0	0	0	0	457631	3352136	389564	147102	303989	365210
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	0	14543	113	62	51	0	199	0	0	0	195	20	60	28	5	0	0
<input type="checkbox"/>	7	0	1422354322	5339283	13089	4190	42	4	0	0	5	0	1546901	2153386	412948	577706	86773	561560
<input type="checkbox"/>	8	0	1258810916	5403047	6130	63299	0	0	0	0	0	0	1630174	2170577	344589	454008	486857	316842
<input type="checkbox"/>	9	0	395187668	5954372	126364	111212	0	0	0	0	0	0	355586	2207222	259740	116842	75385	2939597
<input type="checkbox"/>	10	0	1579921264	110868964	61419749	20739682	0	0	0	0	0	0	34970962	47545335	14504915	5037080	1427176	7381496
<input type="checkbox"/>	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Port	Indicates the specific port for which RMON statistics are displayed.
Drop Events	Displays the number of dropped events that have occurred on the port.
Octets	Displays the number of octets received on the port.

Pkts	Displays the number of packets received on the port.
Broadcast Pkts	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts	Displays the number of good Multicast packets received on the port.
CRC & Align Errors	Displays the number of CRC and Align errors that have occurred on the port.
Undersize Pkts	Displays the number of undersized packets (less than 64 octets) received on the port.
Oversize Pkts	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments	Displays the number of fragments received on the port.
Jabbers	Displays the total number of received packets that were longer than 1518 octets.
Collisions	Displays the number of collisions received on the port.
Pkts of 64 Octets	Displays the number of 64-byte frames received on the port.
Pkts of 65 to 127 Octets	Displays the number of 65 to 127 byte packets received on the port.
Pkts of 128 to 255 Octets	Displays the number of 128 to 255 byte packets received on the port.
Pkts of 256 to 511 Octets	Displays the number of 256 to 511 byte packets received on the port.
Pkts of 512 to 1023 Octets	Displays the number of 512 to 1023 byte packets received on the port.
Pkts of 1024 to 1518 Octets	Displays the number of 1024 to 1518 byte packets received on port.

Log

The Syslog protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operation and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.

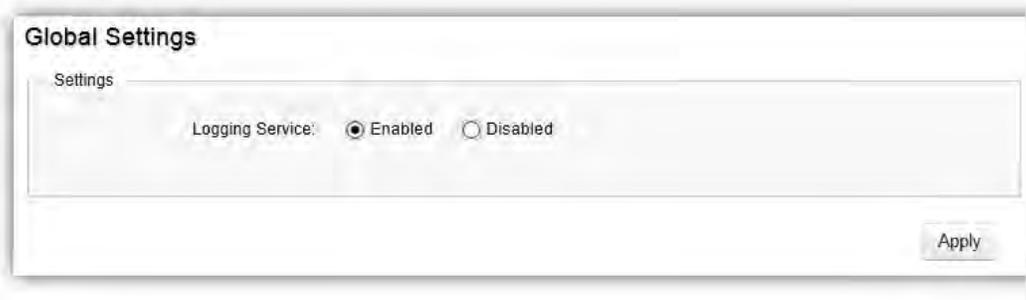
Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details. The following table describes the Syslog 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.
---	------	------------------------	--

Global Settings

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



Click **Apply** to update the system settings.

Local Logging

The System Log is designed to monitor the operation of the 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 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.

Target	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG	
RAM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Flash	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Remote Logging

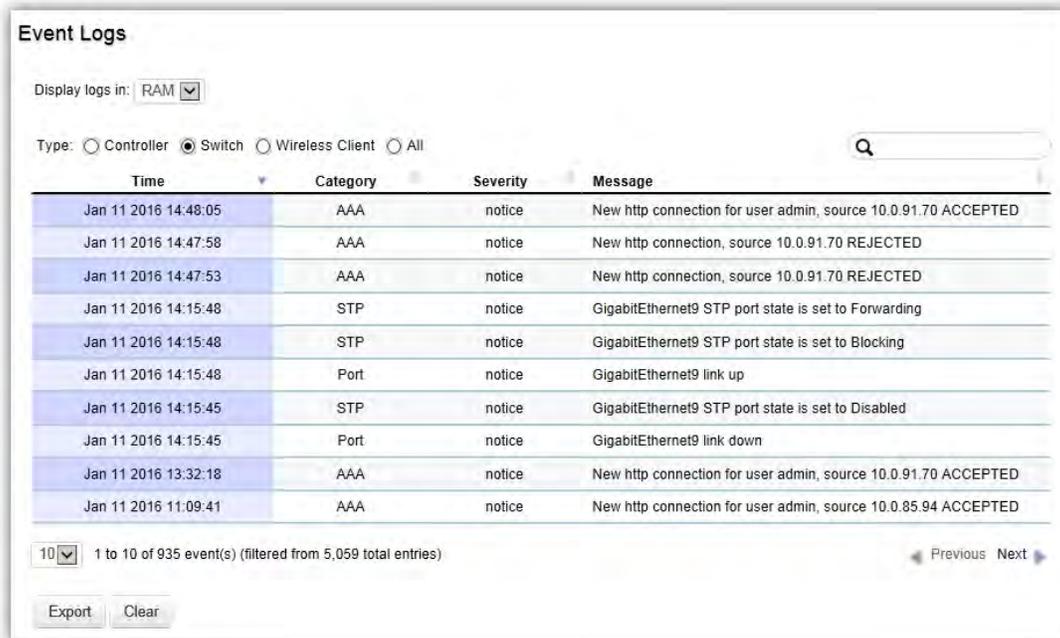
The internal log of the EWS Switch has a fixed capacity; at a certain level, the EWS Switch will start deleting the oldest entries to make room for the newest. If you want a permanent record of all logging activities, you can set up your syslog server to receive log contents from the EWS Switch. Use 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.

IP/Hostname	Server Port	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG	Facility	
char: 1-63	514	No	No	No	No	No	No	No	No	local0	<input checked="" type="checkbox"/> <input type="checkbox"/>

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Event Logs

This page displays the most recent records in the 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.



The screenshot shows the 'Event Logs' interface. At the top, there is a dropdown menu for 'Display logs in:' set to 'RAM'. Below it are radio buttons for 'Type': 'Controller', 'Switch' (selected), 'Wireless Client', and 'All'. A search bar is located to the right of the type selection. The main part of the interface is a table with the following columns: 'Time', 'Category', 'Severity', and 'Message'. The table contains 10 entries, with the most recent at the top. Below the table, there is a pagination control showing '10' entries per page, '1 to 10 of 935 event(s) (filtered from 5,059 total entries)', and 'Previous' and 'Next' buttons. At the bottom, there are 'Export' and 'Clear' buttons.

Time	Category	Severity	Message
Jan 11 2016 14:48:05	AAA	notice	New http connection for user admin, source 10.0.91.70 ACCEPTED
Jan 11 2016 14:47:58	AAA	notice	New http connection, source 10.0.91.70 REJECTED
Jan 11 2016 14:47:53	AAA	notice	New http connection, source 10.0.91.70 REJECTED
Jan 11 2016 14:15:48	STP	notice	GigabitEthernet9 STP port state is set to Forwarding
Jan 11 2016 14:15:48	STP	notice	GigabitEthernet9 STP port state is set to Blocking
Jan 11 2016 14:15:48	Port	notice	GigabitEthernet9 link up
Jan 11 2016 14:15:45	STP	notice	GigabitEthernet9 STP port state is set to Disabled
Jan 11 2016 14:15:45	Port	notice	GigabitEthernet9 link down
Jan 11 2016 13:32:18	AAA	notice	New http connection for user admin, source 10.0.91.70 ACCEPTED
Jan 11 2016 11:09:41	AAA	notice	New http connection for user admin, source 10.0.85.94 ACCEPTED

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

- **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.

Diagnostics

Cable Diagnostics

Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.

Cable Diagnostics
Note: Cable length is only for reference and may be inaccurate when 'OK' is indicated.

Port	Pair A	Cable Length A (meter)	Pair B	Cable Length B (meter)	Pair C	Cable Length C (meter)	Pair D	Cable Length D (meter)
Port 2 <input checked="" type="checkbox"/>	OK	8	OK	8	OK	8	OK	8

To verify accuracy of the test, it is recommended that you run multiple tests in case of test fault or user error.

Click **Test** to perform the cable tests for the selected port.

Ping Test

The Packet Internet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss. Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.

Ping Test

Ping Test Settings

IP Address: 192.168.1.100 (x.x.x.x or hostname)

Count: 4 (1 - 5 | Default : 4)

Interval (in sec): 1 (1 - 5 | Default : 1)

Size (in bytes): 56 (8 - 5120 | Default : 56)

Result:

Test

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IP address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the Switch can communicate with a particular network host before testing.

IPv6 Ping Test

Ping Test Settings

IP Address: (xxxx:xx:xx)

Count: (1 - 5 | Default : 4)

Interval (in sec): (1 - 5 | Default : 1)

Size (in bytes): (8 - 5120 | Default : 56)

Result:

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IPv6 address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

Trace Route

Trace Route Settings

IP Address: (x.x.x.x or hostname)

Max Hop: (2 - 255 | Default : 30)

Result:

```

traceroute to google.com (64.233.187.101), 30 hops max, 40 byte packets
 1 118.163.20.254 (118.163.20.254) 48 bytes to 10.0.85.245  20 ms  20 ms  10 ms
 2 168.95.228.42 (168.95.228.42) 36 bytes to 10.0.85.245  20 ms  30 ms  20 ms
 3 220.128.2.158 (220.128.2.158) 148 bytes to 10.0.85.245  20 ms 220.128.3.102
(220.128.3.102) 148 bytes to 10.0.85.245  20 ms 220.128.1.70 (220.128.1.70) 148 bytes to
10.0.85.245  20 ms
 4 220.128.9.81 (220.128.9.81) 148 bytes to 10.0.85.245  20 ms  20 ms 220.128.8.81
(220.128.8.81) 148 bytes to 10.0.85.245  20 ms
 5 220.128.9.173 (220.128.9.173) 36 bytes to 10.0.85.245  20 ms 220.128.8.173
(220.128.8.173) 36 bytes to 10.0.85.245  20 ms 220.128.9.173 (220.128.9.173) 36 bytes to
10.0.85.245  20 ms
 6 72.14.196.3 (72.14.196.3) 36 bytes to 10.0.85.245  20 ms 74.125.49.158 (74.125.49.158)
36 bytes to 10.0.85.245  20 ms  20 ms
 7 209.85.243.30 (209.85.243.30) 36 bytes to 10.0.85.245  30 ms  30 ms  20 ms
 8 216.239.46.223 (216.239.46.223) 148 bytes to 10.0.85.245  30 ms 209.85.250.229
(209.85.250.229) 148 bytes to 10.0.85.245  20 ms 209.85.252.213 (209.85.252.213) 148
bytes to 10.0.85.245  30 ms
 9 216.239.43.101 (216.239.43.101) 36 bytes to 10.0.85.245  20 ms 66.249.94.131
(66.249.94.131) 36 bytes to 10.0.85.245  20 ms 216.239.50.45 (216.239.50.45) 36 bytes to
10.0.85.245  30 ms

```

IP Address	Enter the IP address or the host name of the station you wish the Switch to ping to.
Max Hop	Enter the maximum number of hops. The range is from 2 to 255 and the default is 30.
Result	Displays the trace route results.

Click **Test** to initiate the trace route.

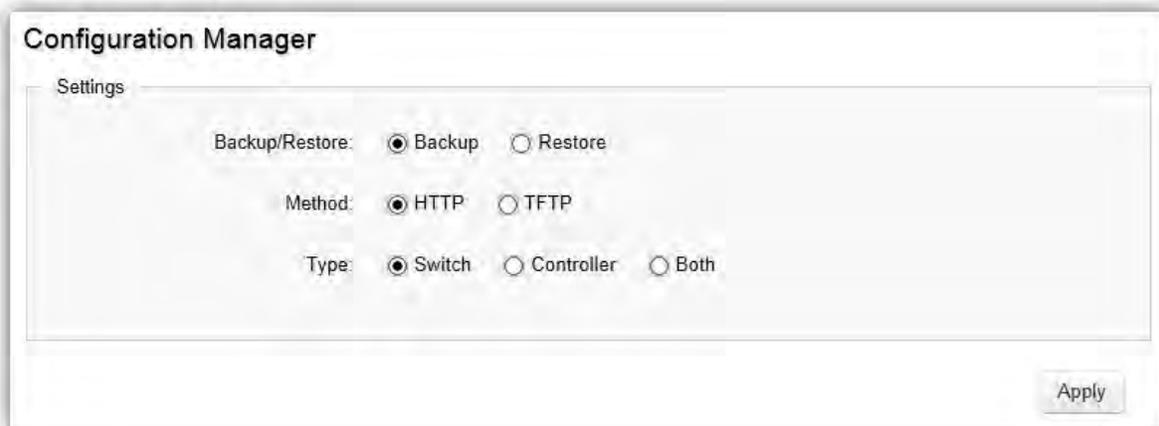
Maintenance

Maintenance functions are available from the maintenance bar located on the upper right corner of the user interface. Maintenance functions include: saving configuration settings, upgrading firmware, resetting the configuration to factory default standards, rebooting the device, and logging out of the interface. The following represents the Maintenance menu bar.



Configuration Manager

The File Management feature is used for saving your current configuration to a file on your computer or a TFTP server, or to restore previously saved configuration settings to the Switch using a configuration file from your local drive or TFTP server.

A dialog box titled "Configuration Manager" with a "Settings" section. It contains three rows of radio button options: "Backup/Restore" with "Backup" selected and "Restore" unselected; "Method" with "HTTP" selected and "TFTP" unselected; and "Type" with "Switch" selected, "Controller" unselected, and "Both" unselected. An "Apply" button is located at the bottom right of the dialog box.

Click **Apply** to download configuration settings to your computer or a TFTP server, or to upload previously saved configuration file to the system.

Firmware Upgrade



The screenshot shows a window titled "Firmware Upgrade" with a "Settings" section. Inside the settings section, there are three fields: "Upgrade Method:" with a dropdown menu set to "HTTP", "Partition:" with a dropdown menu set to "Partition 1(Active)", and "File:" with an empty text box and a "瀏覽..." (Browse...) button. An "Apply" button is located at the bottom right of the window.



WARNING

Backup your configuration before upgrading to prevent loss of settings information.



NOTE: The upgrade process may require a few minutes to complete. It is advised to clear your browser cache after upgrading your firmware.

Appendix

Appendix A - Federal Communications Commission (FCC)

EMC Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operations.



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 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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, 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 own expense.

Appendix B - IC Interference Statement

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-003 (Issue 6)

Appendix C - EU Declaration of Conformity

The following information applies if you use the product within European Union.

CE EMC statement

This device complies with the essential requirements and other relevant provisions of the directives 2004/108 / EC (EMC); 2014 / 30 / EU (EMC); 2006/95 / EC (LVD); 2014/35 / EU (LVD). The following test methods have been applied in order to prove presumption of conformity with the essential requirements:

EN 55032:2015+AC: 2016 (Class A)

EN 55024:2010+A1:2015

EN60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

NOTICE:

Operation of this equipment in a residential environment may cause radio interference.

AVISO:

la operación de este equipo en un entorno residencial puede causar interferencias de radio.