# ECW230S

## User Manual

# What is EnGenius Cloud?

Other Languages: 日本語

## Before You Begin

To start using the EnGenius Cloud service, you must prepare the following:

- At least one supported EnGenius Cloud wireless access point or switch.
- An existing network with an Internet connection including DHCP and DNS configuration.

> You can also install the "EnGenius Cloud" mobile app (available for both iOS and Android) for easier device registration and monitoring.

## Supported Web Browsers

The EnGenius Cloud is primarily accessible with a web browser. Before signing up for the EnGenius Cloud service or logging on to the web interface to manage your network, first verify that you are using a supported browser.

The following table lists the web browsers that EnGenius Cloud supports:

| Browser | Release |
| --- | --- |
| Google Chrome | 57.0.2987.110 and later |
| Apple Safari | 10.0.3 (12602.4.8) and later |
| Mozilla Firefox | 52.0 and later |
| Microsoft Edge | 80.0.361.103 and later |

If you use an unsupported web browser, you may experience issues displaying elements on the web interface.

# Getting Started

This session will assist you in setting up a new network on the EnGenius Cloud web application. For easier, faster setup, use the EnGenius Cloud for iOS or EnGenius Cloud for Android mobile apps. No matter which version you start with, you can always switch seamlessly between the web and mobile.

> This article is not meant to be a comprehensive list of everything EnGenius Cloud, but rather a stepping stone to get started in the most informed way possible.

# Signing Up

Before you start to manage EnGenius devices, you must first sign up for the service.

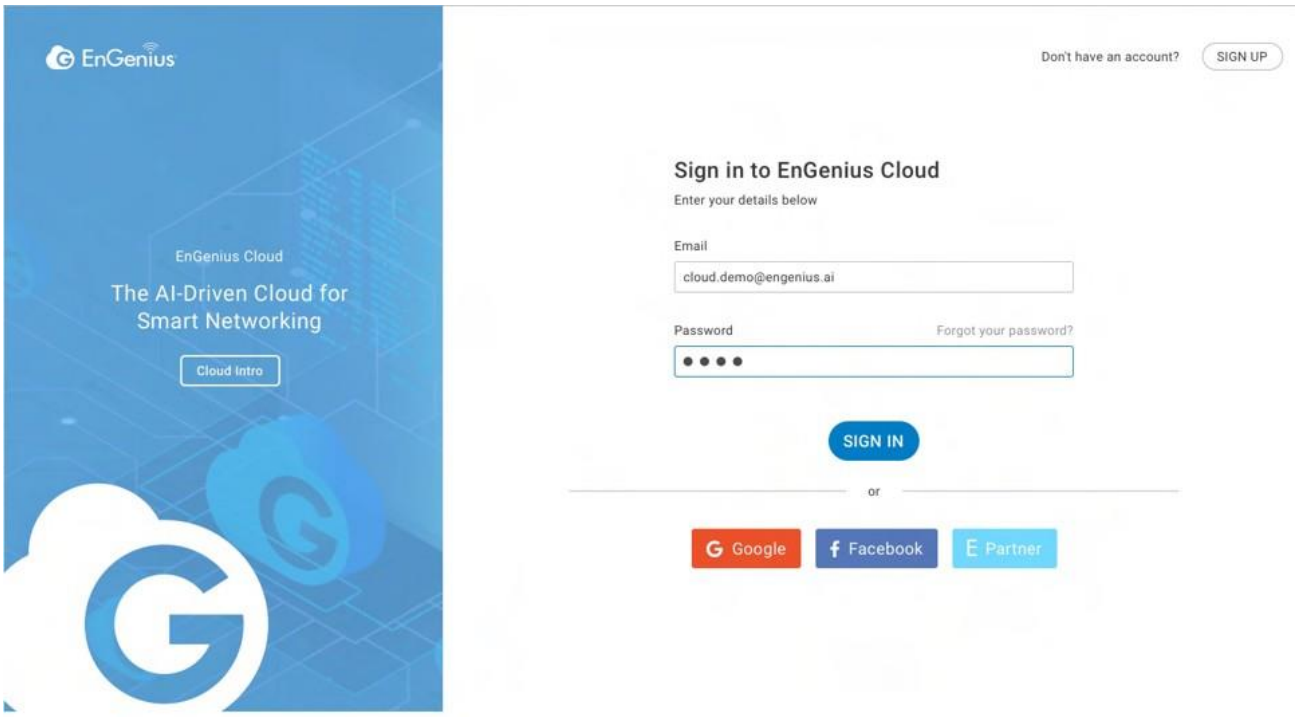
Registering EnGenius Cloud is similar to other web-based platforms and can be done either with a social media account (e.g. Google or Facebook) or by creating an account from scratch. You will need to provide your email address, company name, physical address, and phone number. Furthermore, you must determine the country in which your account will be hosted. That is, all relative device information, user configurations, and client statistics will be kept in the corresponding region of servers (**Oregon** for US and **Frankfurt** for other countries). This enables EnGenius Cloud to protect customer data and comply with requirements like **GDPR** for customers within the European Union.

> Support for signing up with EnGenius Partner Portal will be available soon.

# Logging On

Once your account has been created, you can login to EnGenius Cloud in the following steps:

1. Open a web browser to https://cloud.engenius.ai/ . This will bring up the main login page.




2. Enter your EnGenius Cloud email address and password and click the **Sign in** button.

3. For EnGenius Partner who has account on EnGenius Partner Portal already, you can simply click on "E Partner" button, and EnGenius Partner Portal will pop up login page for you to use Single-Sign-On capability of Partner Portal to log on to EnGenius Cloud

4. For Google and Facebook users, you can also click on "Google" or "Facebook" button to use your account on Google and Facebook to log on to EnGenius Cloud

5. EnGenius Cloud will create a new default Organization and Network for every new account based on the email address as unique user identification. (note: If someone is invited to an Organization or Network, this account won't have default Organization and Network.) If you have multiple accounts created on EnGenius Cloud, EnGenius Cloud will

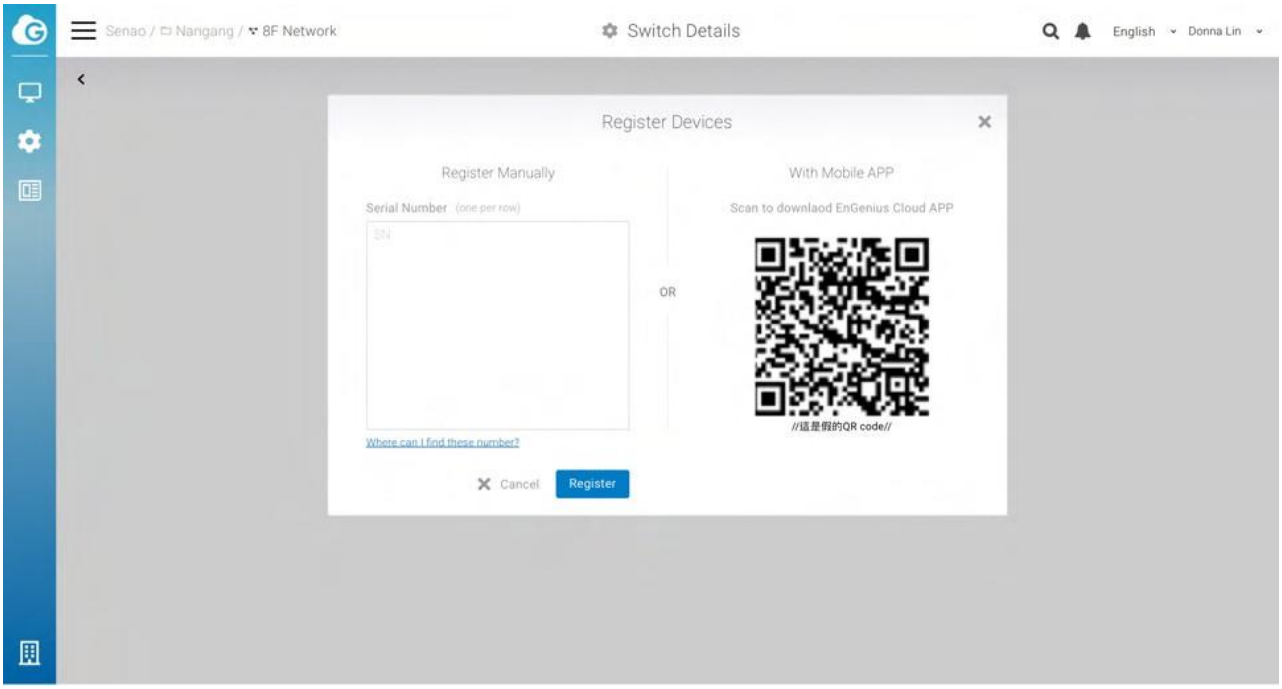
merge your accounts based on the "email address" of the account. For example, if you have created a new account on EnGenius Cloud using the same email address as your google account, then you're able to login to this email account either through Google account authentication with Google account password, or through EnGenius Cloud Login with the password while you created the EnGenius Cloud account.

# Registering Devices to Organization

Register a device to EnGenius Cloud inventory by using the serial number located on the device.

## Registering a device

Registering devices with a serial number is easy. Just enter the serial numbers of your devices, one per line, then click the **Register** button.

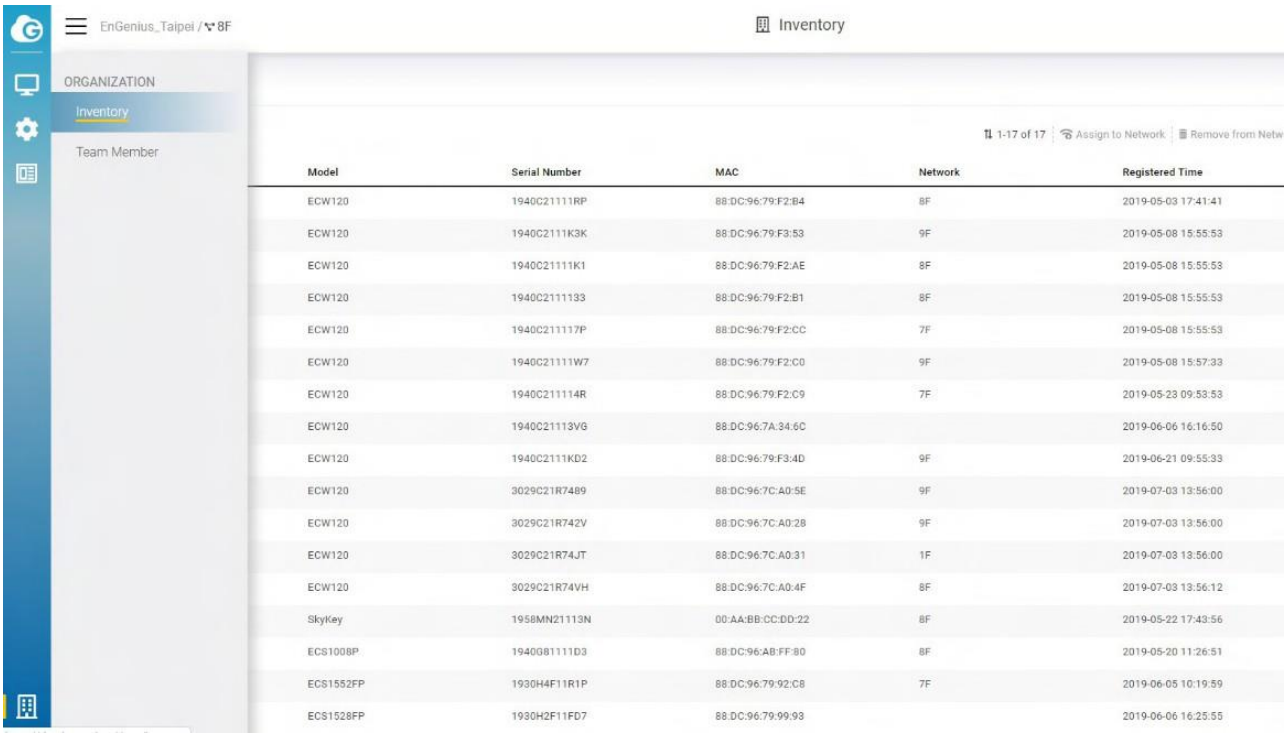


# Assigning Devices to Network

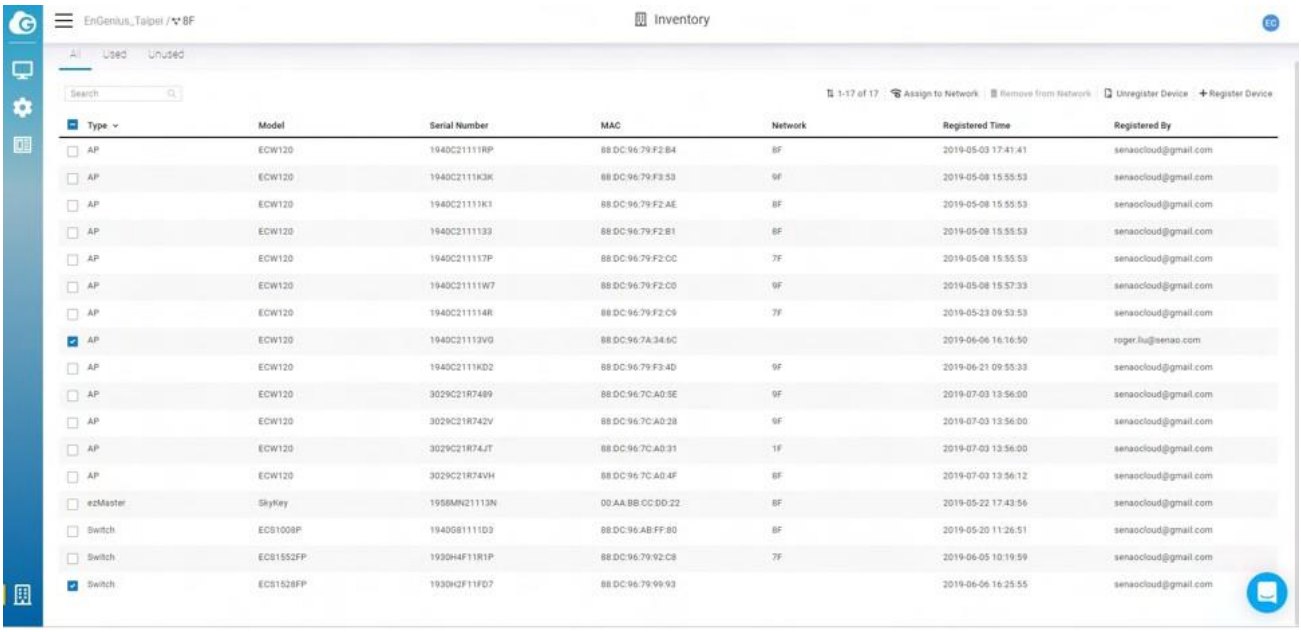
Before devices on EnGenius Cloud can be managed and configured, they must first be added to a network that you have created.

## Adding Devices to a Network

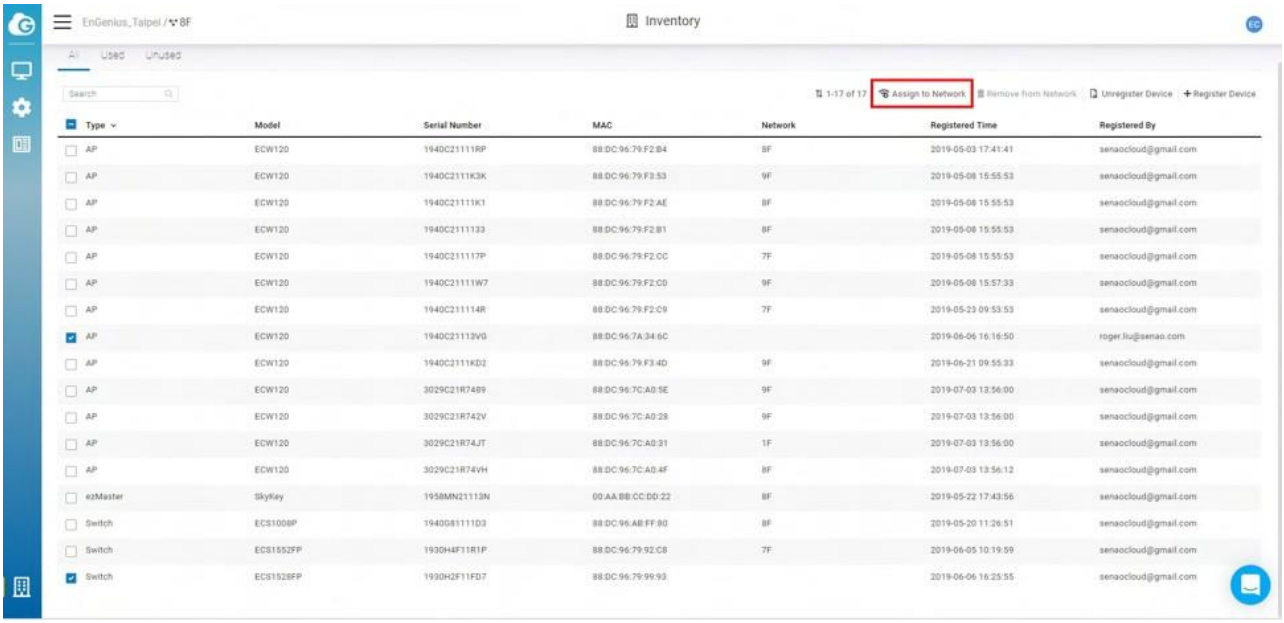
1. Navigate to **Organization** > **Inventory**.




2. Select one or multiple devices as required.




3. Click **Assign to Network.**

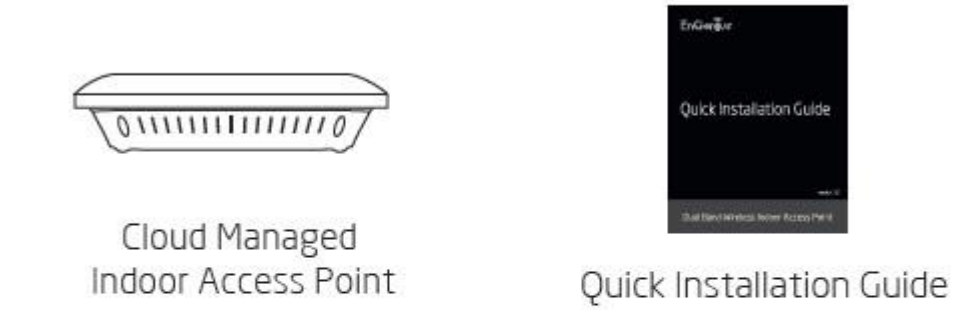


# Device Setup

## ECW AP Installation

### ECW AP Package Contents

-ECW120



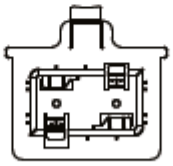

ECW120 Package Contents

-ECW220
-ECW230

Cloud Managed
Indoor Access Point


Quick Installation Guide

Ceiling Mount Base
(9/16" T-Rail)



Ceiling Mount Base
(15/16" T-Rail)

Mounting kit

ECW220/230 Package Contents

**-ECW115**

Cloud Managed
Indoor Access Point


Quick Installation Guide

Junction plate(short)

Junction plate(tall)

Mounting Screw Kit

ECW115 Package Contents

## Minimum Access Requirement

**Power source option** - An ECW AP device can be powered by an 802.3af/at-compliant PoE device or by DC12V input

> Do not use both power sources at the same time.

**Ethernet port:**

- LAN (PoE): Uplink port accepts an 802.3af/at power source.
- LAN2: Data link if this port is built on a device.

**Connect the AP to Internet:**

You need to find a way to let the Cloud AP be able to access internet, so it can be managed by EnGenius Cloud.

- **Connect the uplink LAN port to a switch port or port of router**: This is the most common way to let AP be able to access Internet. (Note: please make sure the port is internet accessible by connecting a notebook to the port and browse the internet)
- **Use your existing Cloud-managed ECW AP to mesh the new AP**: Sometimes the place the AP installed is not accessible with Ethernet cable, then you can leverage EnGenius Mesh technology to mesh the new AP to your existing cloud-managed ECW AP.
- After internet connected, you will see Power LED blinking until the AP is able to communicate with EnGenius Cloud and the LED becomes steady lid. Usually it will take about 8 mins if there is new firmware available to upgrade.
- If the LED keeps blinking, then there could be some issues like no IP address, or local proxy server setting required...etc. To set static IP or Proxy, or managed VLAN, you can login to Local Access Page through Managed SSID of the AP.

---

# ECS Switch Installation

## ECS Switch Package Contents

- For 13" and 19" 1U ECS series model (ECS1xxx/ECS2xxx/ECS5xxx series)

+ ECS Managed Switch
+ Power Cord
+ RJ-45 Console Cable
+ Rack Mount Kit
+ Quick Installation Guide

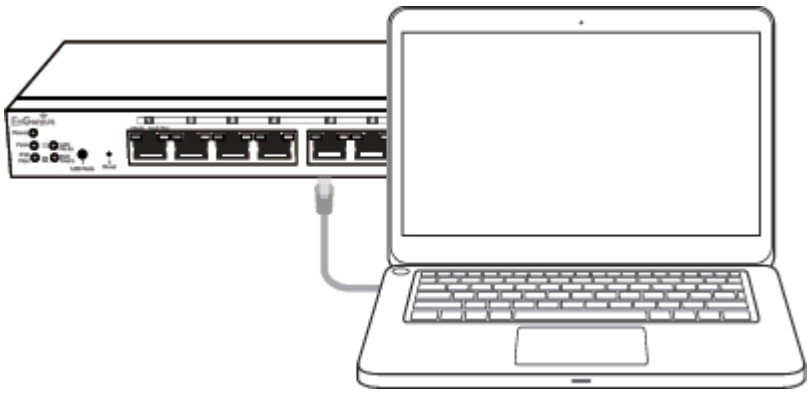
- For Desktop type ECS series model (ECS1008P)

+ ECS Managed Switch
+ Power Adapter
+ Power Cord
+ Ground Screw Kit
+ Rubber Footpads
+ Wall Mount Kit
+ Quick Installation Guide

## Connecting to ECS Switch

**A)** Connect the supplied power adapter (or power cord) to the switch and plug the other end into an electrical outlet. Verify the power LED indicator is lit on the switch. Wait for the switch to complete boot up. It might take few minutes to complete the process.

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



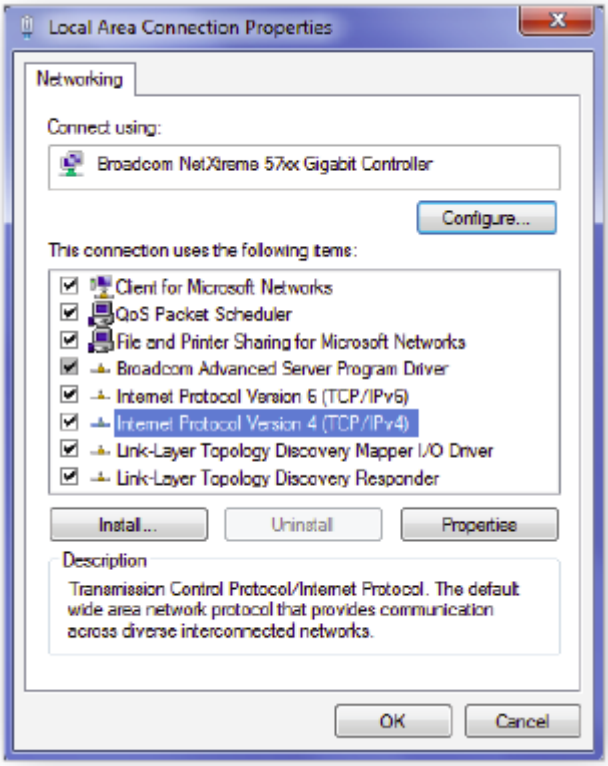
## Login to the ECS Switch Local Access Page

The switch's default IP address setting is DHCP client mode, which will get an IP address from the DHCP server. It will automatically change to static IP address assignment if the switch cannot get an IP address from the DHCP server within two minutes of booting up.

If your switch cannot get an IP address from local DHCP server, or you would like to use static IP address assignment, you may follow the below procedures to manage your computer connection to the switch via a static IP address.

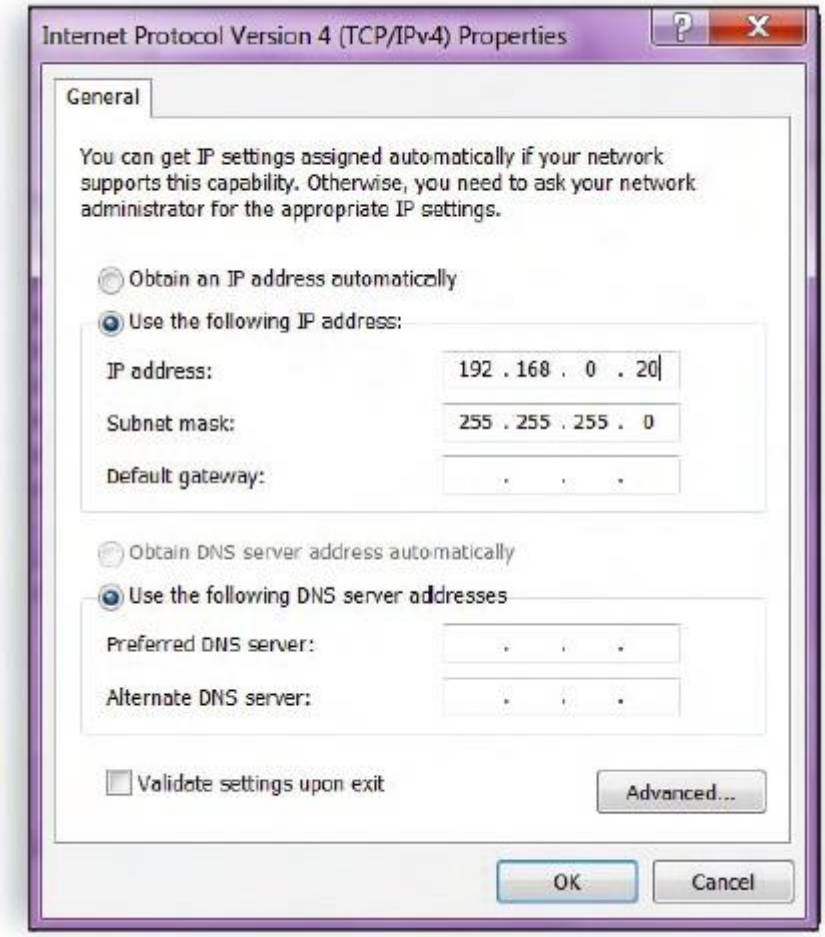
**IP address configuration on your computer:**

A) Once your computer is on, configure the settings of your network adapter. Open Network Connections > Local Area Connection > Internet Protocol Version 4 (TCP/IPv4) > Properties




B) Select **Use the following IP address** and make the following entries:

- **IP Address:** 192.168.0.10 (or any address in the 192.168.0.x network)
- **Subnet mask:** 255.255.255.0

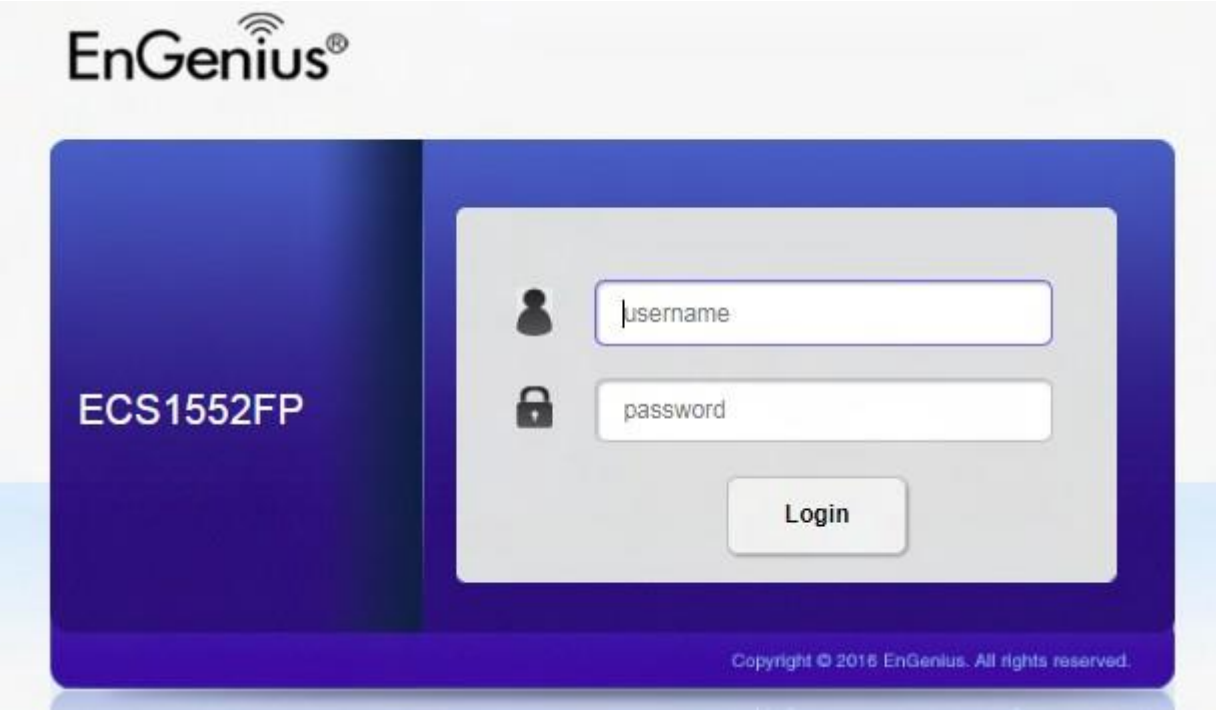



**Login to ECS Switch**

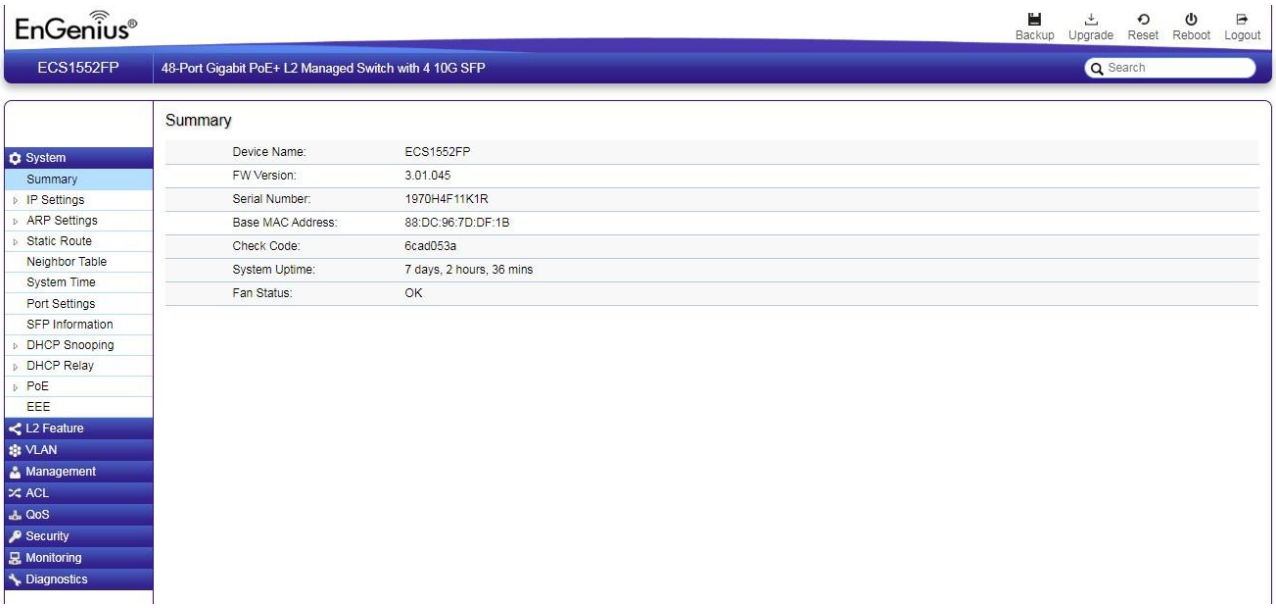
**A)** Open a web browser on your computer. In the address bar of the web browser, enter the ECS switch IP address and hit enter.

**B)** The default username is **admin** and the password is **password**. **We strongly recommend that you change these as soon as possible.** Enter the username and password of the switch and then click Login.

*Your model number may be different in the web browser interface.




**C)** ECS Switch local access page will appear.




Instead of default DHCP settings on ECS switch, users may choose a static IP address setting for their deployed network. Remember to open **System** > **Static Route** to setup the static IP address/gateway settings on the switch in this case.

# QIG

## ECW AP

| | |
|---|---|
| ECW120_ECW220_ECW230_QIG | QIG_ECW120_ECW220_ECW230.pdf - 2MB |
| ECW115_QIG | QIG_ECW115.pdf - 2MB |
| ECW160_QIG | QIG_ECW160.pdf - 2MB |

## ECS Switch

| | |
|---|---|
| ECS_Switch_QIG | ECS_QIG.pdf - 2MB |

# Troubleshooting ECW AP

1. Check the LED Status to see if any problem encountered. If Power LED keeps flashing for over 10 minutes, then there could be Cloud connection issues.
2. Use your mobile phone to scan if Default SSID of the AP found. (you have to be around the AP location) From the Default SSID, you can also identify which stage the AP is stuck on. See details of Default SSID.
3. To troubleshoot the connection issue, you may login to Local page:
    1. Use your client device (e.g., a laptop, mobile device, or tablet) to find the SSID: "EnMGMTxxxx" (xxxx is the last four digits of LAN MAC which can be found on the back of the device) and connect to it.
    2. Enter the URL in web browser: http://EnGenius.local or the IP 192.168.1.1 to access the device's user interface. You can review device status after logging into the AP with the default account/password ( default admin account/ password : admin/ admin.)

***Issue: Cannot find Default SSID***

1. Check for available wireless networks (Check if a known default SSID is being broadcast).

2. If a default SSID is being broadcast, connect your device to it.

3. If no known default SSIDs are present, set up a manual wireless network connection. For the SSID name, use 'EnMGMT', e.g. 'EnMGMTxxxx', where the x's are replaced with the last four digits of the LAN MAC address.

4. After connecting, open a web browser and connect to one of the local access page addresses.

# LED Status


ECW120 LED

| Status | LED / Color | State |
|---|---|---|
| Cloud Connected | Power LED<br>Orange | Solid On |
| Connecting to Cloud | Power LED<br>Orange | Flash |
| No LAN Physical Connection | LAN LED<br>Blue | Off |
| LAN Connected | LAN LED<br>Blue | Solid On |
| LAN Transmitting | LAN LED<br>Blue | Flash |
| Wi-Fi Interface On | 2.4G / 5G<br>Blue/Green | Solid On |
| Wi-Fi Transmitting | 2.4G / 5G<br>Blue/Green | Flash |
| Firmware Upgrade | All LED's | Flash |

| | | |
|---|---|---|
| Mesh Enabled | Mesh LED<br>Blue | Flash |

ECW115 LED

| Status | LED Color | State |
|---|---|---|
| Power Up AP | Orange | Static |
| Waiting Period (before being added to Cloud) | Orange | Flash (slow) |
| Connected to Cloud | Blue | Static |
| Reset to Default | Blue | Flash (quick) |
| Error or Disconnected | Orange | Flash (quick) |
| Firmware Upgrading | Orange/Blue | Flash |

# Default SSIDs

**Default SSIDs (only available before ECW AP is managed by EnGenius Cloud)**

Potential known default SSID names along with potential causes/solutions:

**EnMGMTxxxx-Initializing**

Cause: AP is in bootup sequence.

**EnMGMTxxxx-SSID_name>-No_Eth**

Cause: AP does not have an Ethernet connection.

Solution: Check if the Ethernet cable is unplugged.

**EnMGMTxxxx-No_IP**

Cause: AP cannot get an IP address from the DHCP server. Solution: Check the AP's IP address configuration.

**EnMGMTxxxx-IP_Conflict**

Cause: AP's IP address conflicts with another device's IP in the same network. Solution:

Check the AP's IP address configuration.

**EnMGMTxxxx-Gateway_ERR**

Cause: AP is unable to connect to its default gateway.

Solution: Check the AP's IP address configuration and connectivity to its default gateway.

**EnMGMTxxxx-Proxy_ERR**

Cause: AP could not access Internet through an HTTP/HTTPS proxy.

Solution: Check the AP's proxy configuration in Miscellaneous Settings.

**EnMGMTxxxx-DNS_ERR**

Cause: AP could not resolve the domain name from the DNS server.

Solution: Check the AP's IP address configuration.

**EnMGMTxxxx-Cloud_ERR**

Cause: Everything appears to work normally, but device is unable to connect to cloud server.

Solution: Check cloud server status with EnGenius.

**EnMGMTxxxx-No_Cloud_Configure**

Cause: AP's S/N has not been added to any network.

Solution: Check whether the AP has been added in the inventory and has been added to a network.

**EnMGMTxxxx-Cloud_Configured**

Everything is working as it should!

**EnMGMTxxxx**

Cause: An AP has never connected to the EnGenius cloud or has been factory reset.

# Login to Local Access Page

1. Use your client device (e.g., a laptop, mobile device, or tablet) to find the SSID: “EnMGMTxxxx” (xxxx is the last four digits of the MAC address, found on the back of the device) and connect to it.
2. Under your web browser, enter the URL http:// EnGenius.local or the localhost IP address (192.168.1.1) to access the device's user interface. You can review device status after logging into the AP with the default admin account/password (default account & password: **admin**/**admin**)

By default, EnGenius cloud access points (ECW series) are assigned an IP address dynamically by the DHCP server. If you encounter issues with IP address assignment, please double check that the IP settings include IP address, subnet mask, gateway, proxy, and management VLAN. If any issues still exist, you may change your IP assignment from "DHCP mode" to "Static IP" via the following procedure:


ECW AP's Local Access Page

By default, EnGenius cloud access points (ECW series) are assigned an IP address dynamically by the DHCP server. If you encounter issues with IP address assignment, please double check that the IP settings including IP address, subnet mask, gateway, proxy, and management VLAN. If any issues still exist, you may change your IP assignment from "DHCP mode" to "Static IP" via the following procedure:

a) Select “Local Setting” on this page.

b) Change IPv4 setting from “AS DHCP client” to “Use Static IP”

> c) Configure the IP address, gateway, net mask, and proxy policy as required.
>
> d) Reconnect this device to the LAN again if necessary.

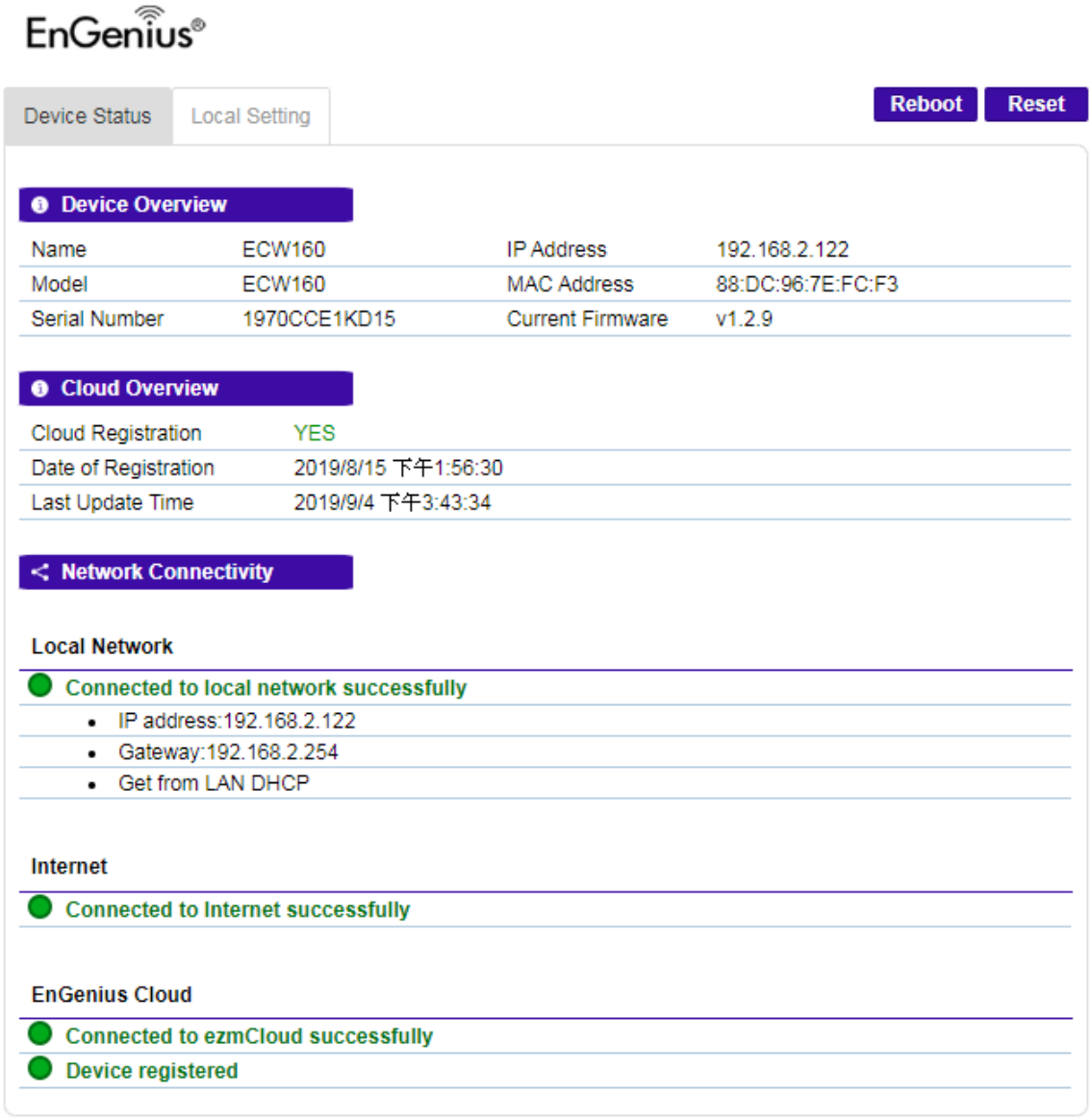
## Local Access Page Options

Every device's status page includes useful information about the status of the device, basic configuration options (such as setting a static IP), and other tools. The following section will explain the items available on the device status page.

ECW Access Points provide the following information and configuration options on their local status page:

**Device Status Section**

Contains information regarding the device overview, EnGenius Cloud overview, and network connectivity information.




Device Status on Local Access Page

**Device Overview**

Provides information regarding the name, model, serial number, IP address, MAC address, and current firmware.

**Cloud Overview**

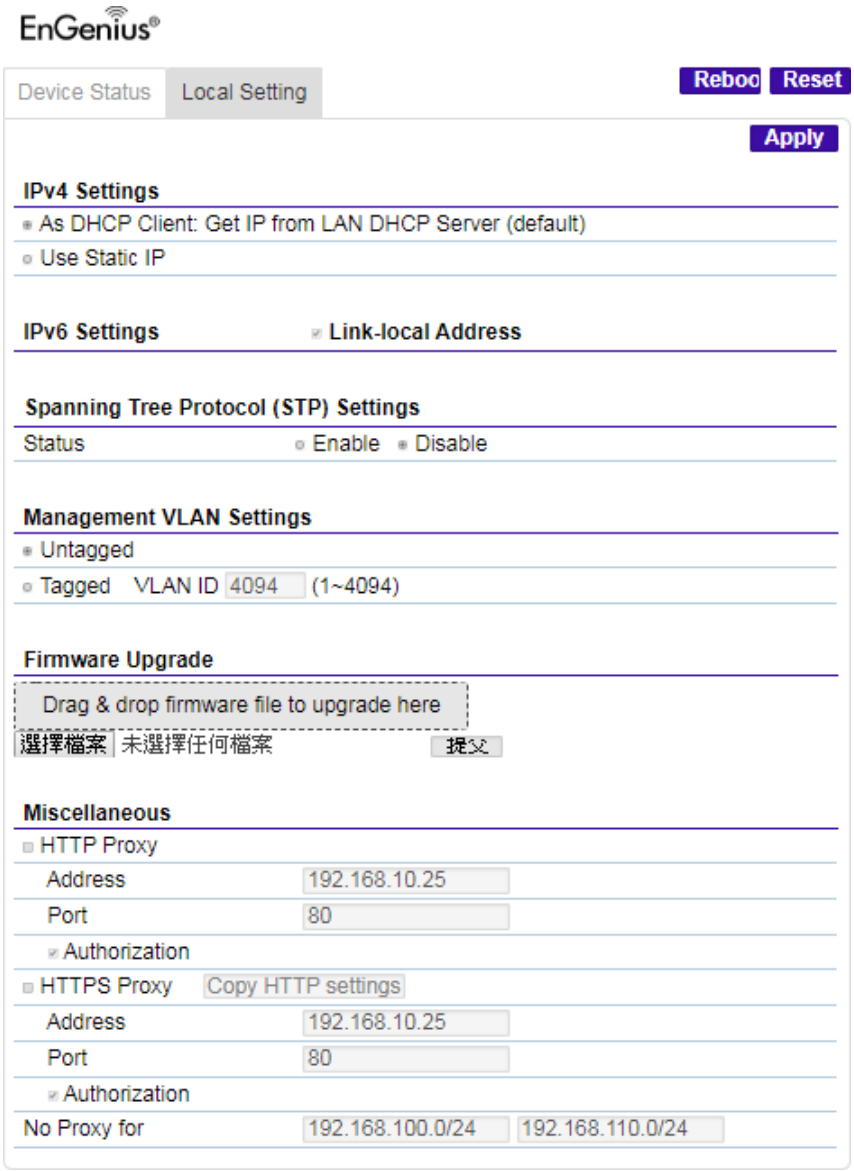
Provides information about the Cloud registration status, date of registration, and time of last update.

**Network Connectivity**

Provides connectivity information to local network, Internet, and EnGenius Cloud.

### Local Setting Section

Provides settings for IPv4 / IPv6 address, management VLAN, firmware upgrade, and other miscellaneous configuration items (such as HTTP/HTTPS Proxy). Users can also reboot the device or reset the device to factory default settings from here.




Local Setting on Local Access page

> The HTTP proxy only allows all default management traffic from the EnGenius ECW device to be sent through a proxy.

# Label information

## ECW AP's

The first step is to get the serial numbers of the Cloud equipment you want to add to your cloud account. The serial number can be found on the box of the Cloud AP (ECW) or Cloud switch (ECS). An example of each is below:


Fig 1: ECW Serial number on box

1. Model number of ECW AP
2. Serial Number of ECW AP (This string of information that is added in the Cloud GUI)
3. Hardware version on ECW AP

The serial number for an ECW AP can also be found on the sticker on the back on the unit (check where you plug in the Ethernet cords into the ECW AP)

Fig 2: Back of AP

Below is an example of the sticker on the back on an ECW220 AP.


Fig 3: Sticker on back of ECW AP

As you can see the sticker on the back of the AP has the MAC address of the AP as well. It has the following items:

1. Model of AP

2. Serial number of ECW AP (This string of information that is added in the Cloud GUI)

You can also find the serial number of the ECW AP In the GUI of the ECW AP, when you login into the unit.

Highlighted below is the information needed to add the AP to the Cloud GUI, if the information is obtained via login to the ECW AP locally in the web GUI.

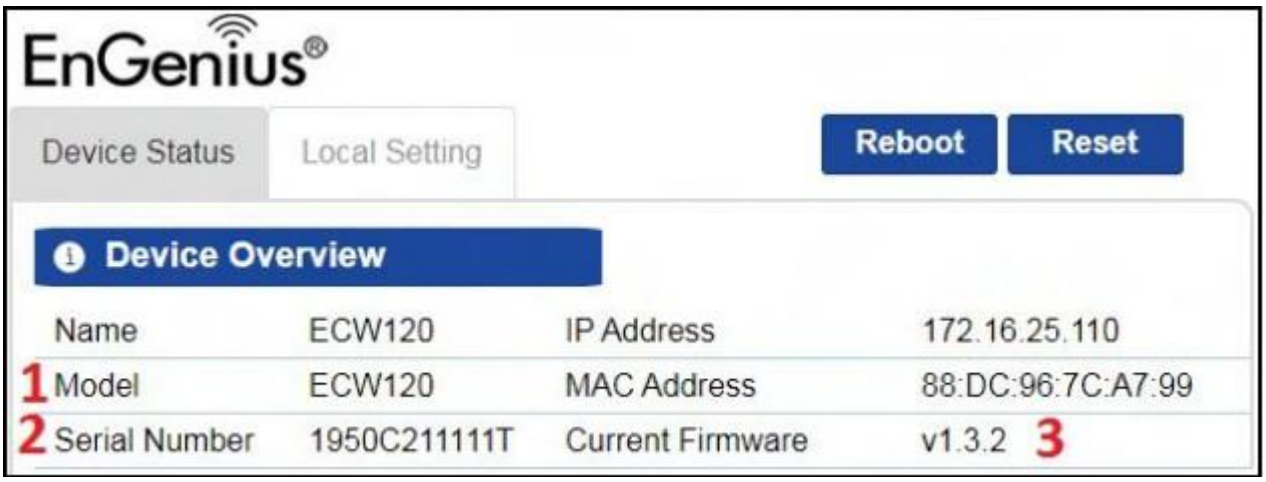



Fig 4: Local Login information

1. Model of the AP

2. Serial Number of ECW AP (This string of information that is added in the Cloud GUI)

3. Firmware version the AP is currently running

---

## ECS Switches

Below is the sticker that is on the box of the ECS switch

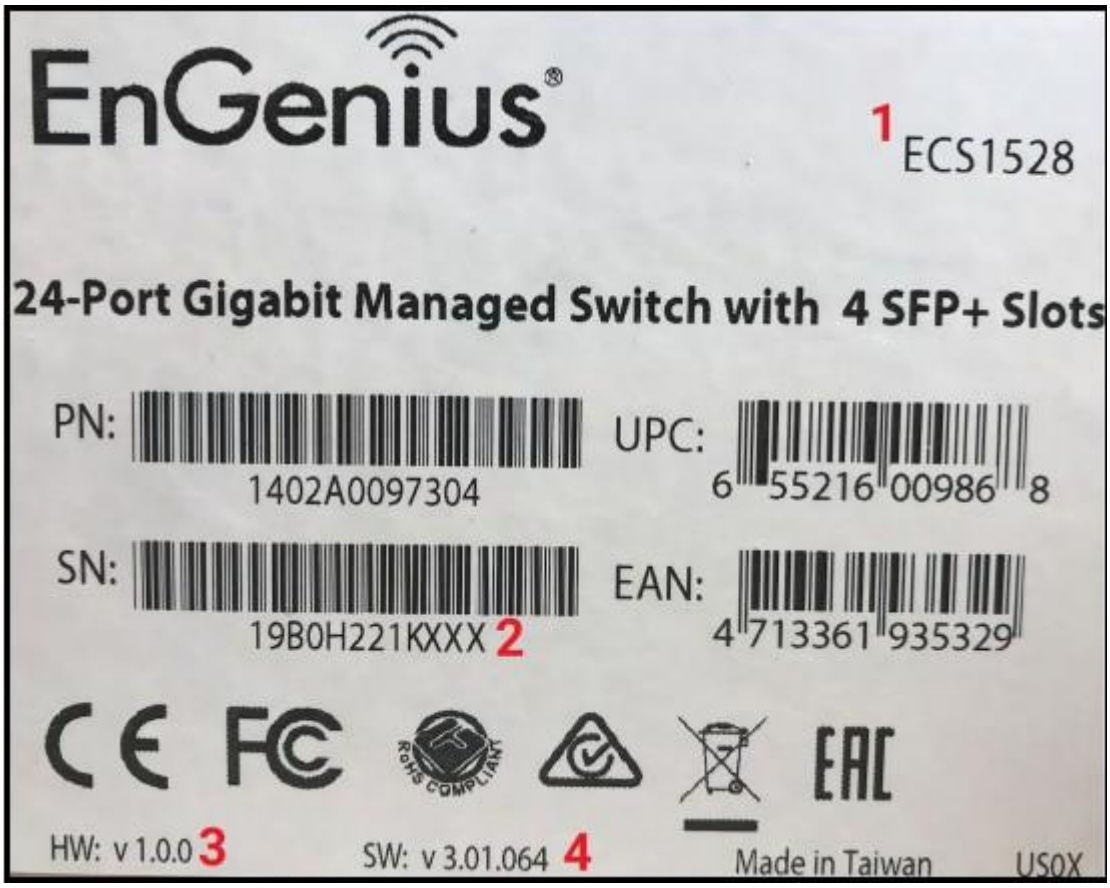



Fig 5: Sticker on the ECS box

1. Model of the ECS switch
2. Serial Number of ECW AP (This string of information that is added in the Gloud GUI)
3. Hardware version of the ECS switch
4. Firmware version that the switch came shipped with

Below is the information you find when you login to the ECS switch locally and go to **System** > **Summary** from the left hand column.

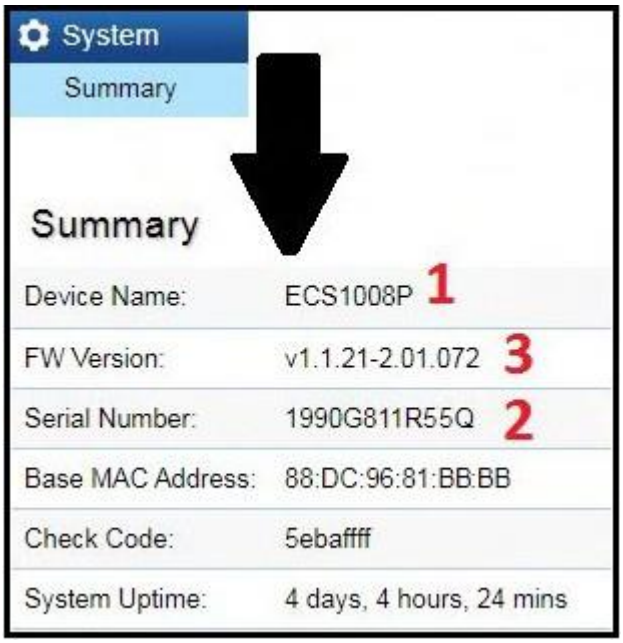



Fig 7: ECS Switch local login screen

1. Model of ECS Switch

2. Serial Number of ECW AP (This string of information that is added in the Gloud GUI)

3. Firmware version the switch is currently running

# Working with Organization Trees

EnGenius Cloud adopts an organization tree structure to let user define the scope of their managed networks. All device managing or monitoring functions can be applied to different scopes as laid out in the user's tree. That gives VAR or MSP users great flexibility in managing their networks.

The current organization tree structure consists of three levels, from largest to smallest:

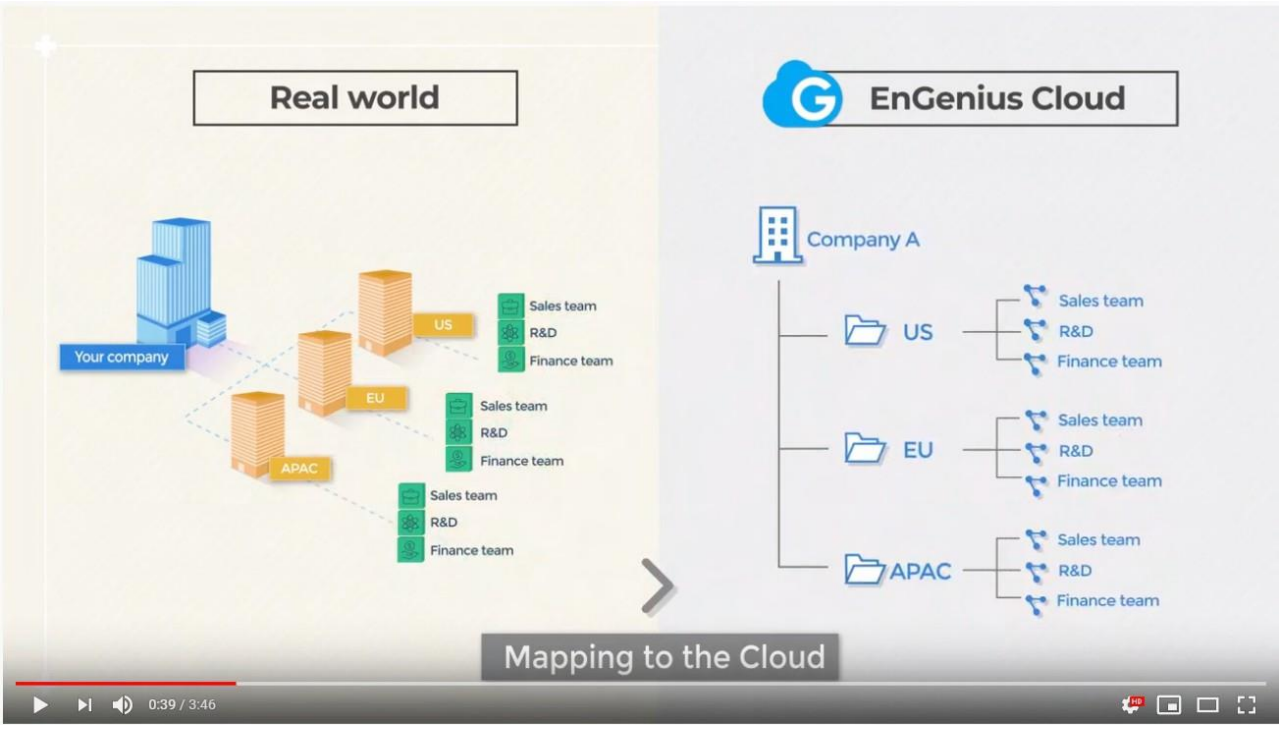
- Organization - A grouping of one or more hierarchies under the umbrella of a single license.
- Hierarchy View - A cluster of networks, which may be geographically concentrated or spread out.
- Network - A set of network devices united by a single configuration set.

The organization tree definition is shown on the top left corner of the web GUI as follows:


---

## How-to Videos

### How to build your company networks in EnGenius Cloud




https://www.youtube.com/watch?v=sN2y44Yzi7s&feature=youtu.be&t=5

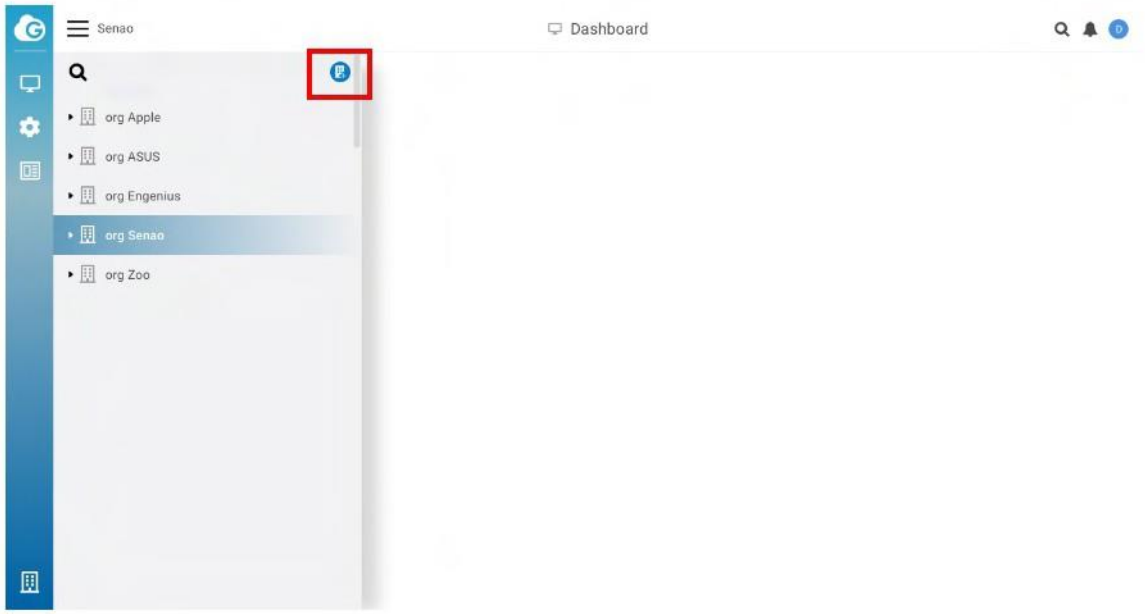
# Organization

A collection of hierarchy views and networks that are part of a single organizational entity, such as a company or school district. Each organization is the owner of a single license.

---

## Adding an organization

Click **Menu > Create Organization** button to create organization



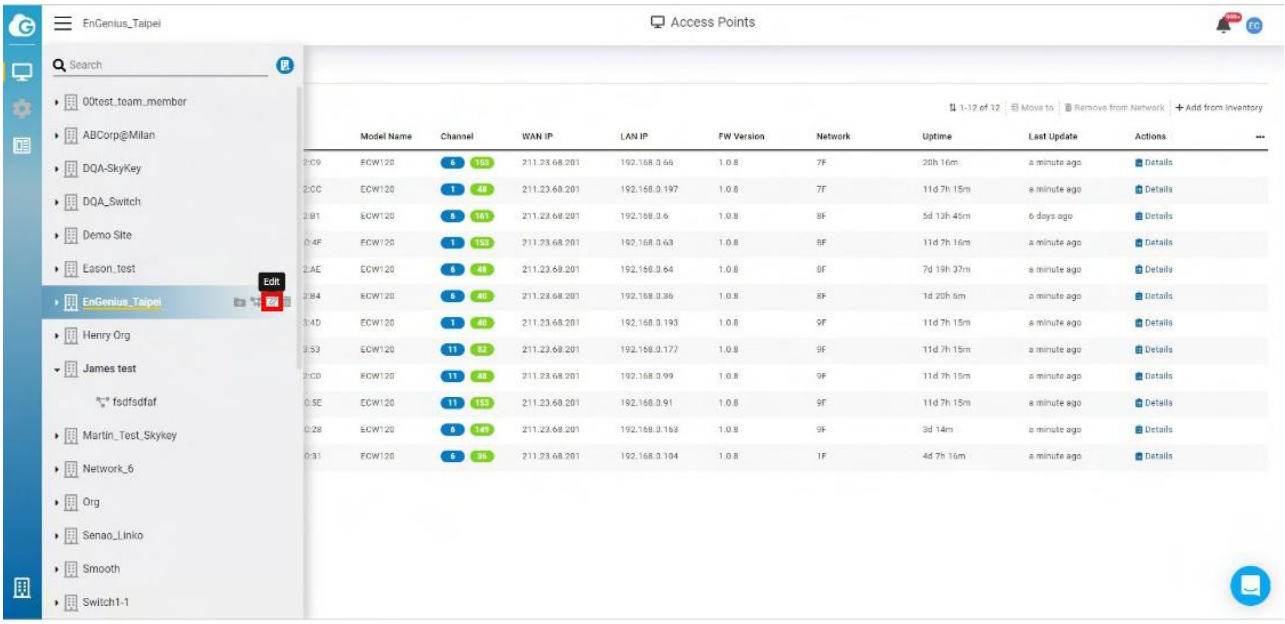

---

## Edit Organization

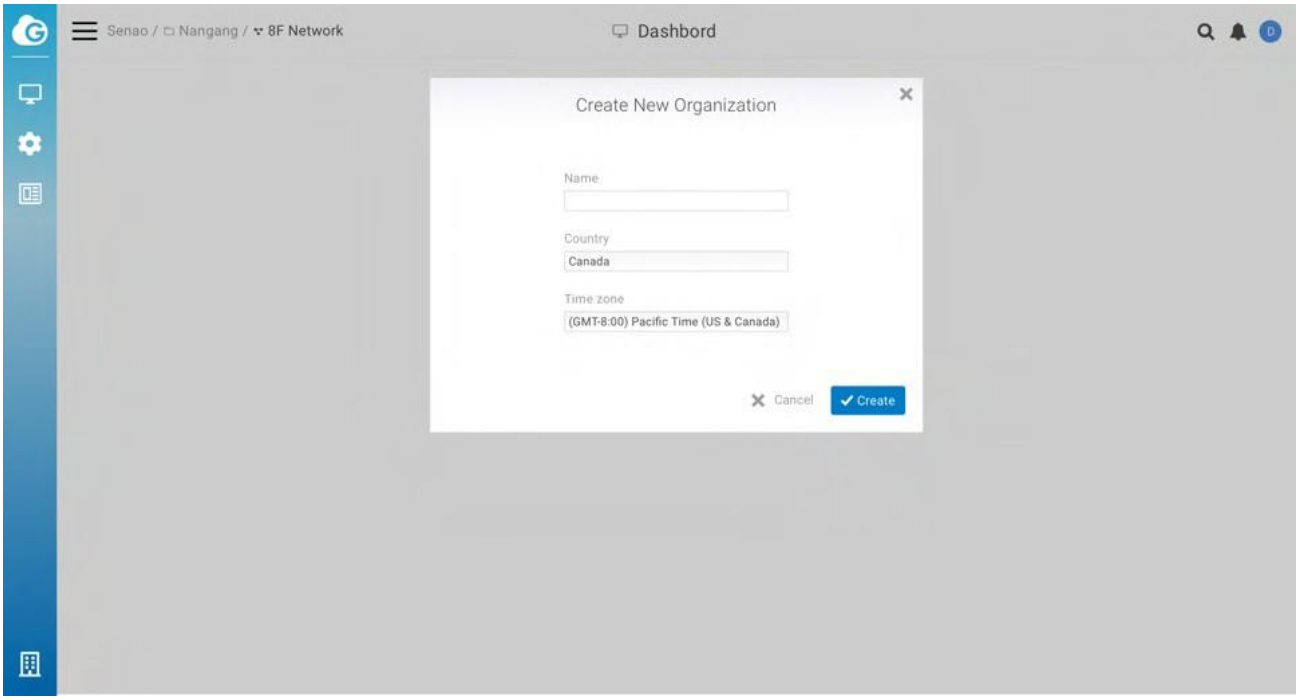
Edit a organization if you need to update any its current settings (for example, if you want to change the Organization name, Country, TimeZone.)

Follow these steps to edit a Organization.

1. Click **Menu > Find the Organization you want to edit > Edit**




2. Update Network Settings as required




3. Click **Apply**

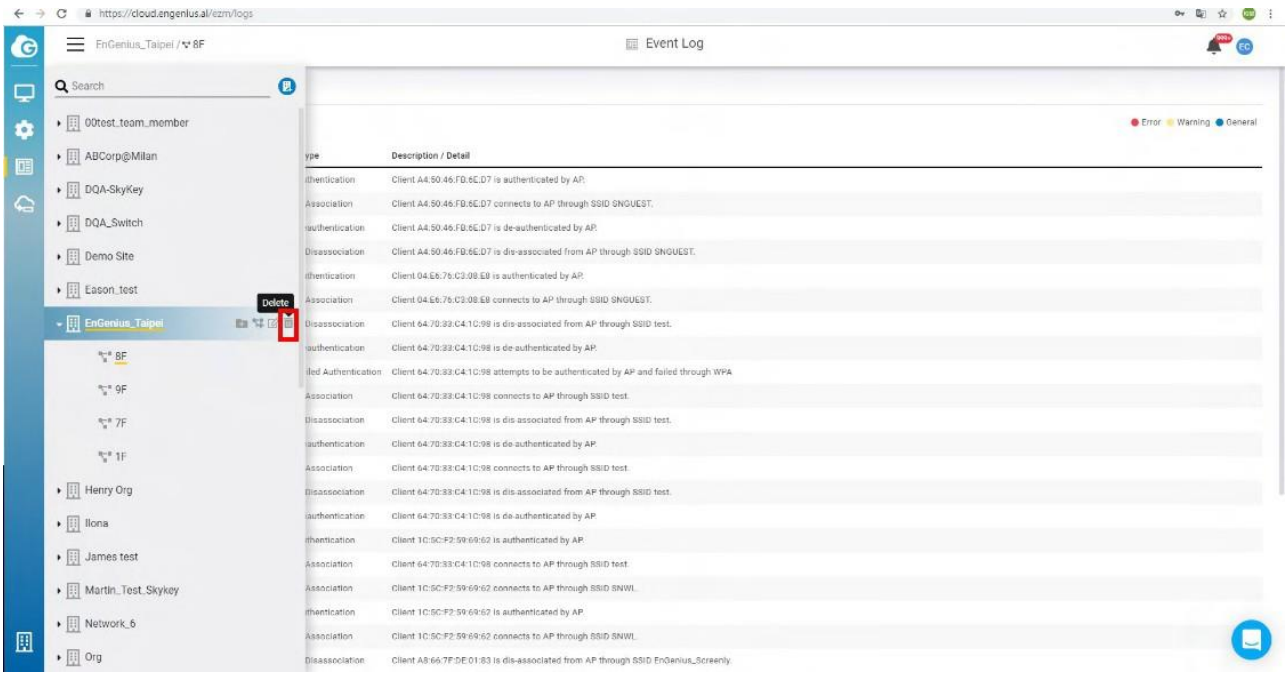
---

# Delete Organization

If you no longer need a Organization that you previously created, you can delete it.

Follow these steps to delete a organization

1. Click **Menu > Find the Organization you want to edit > Delete**




2. Popup is displayed and click **Confirm**

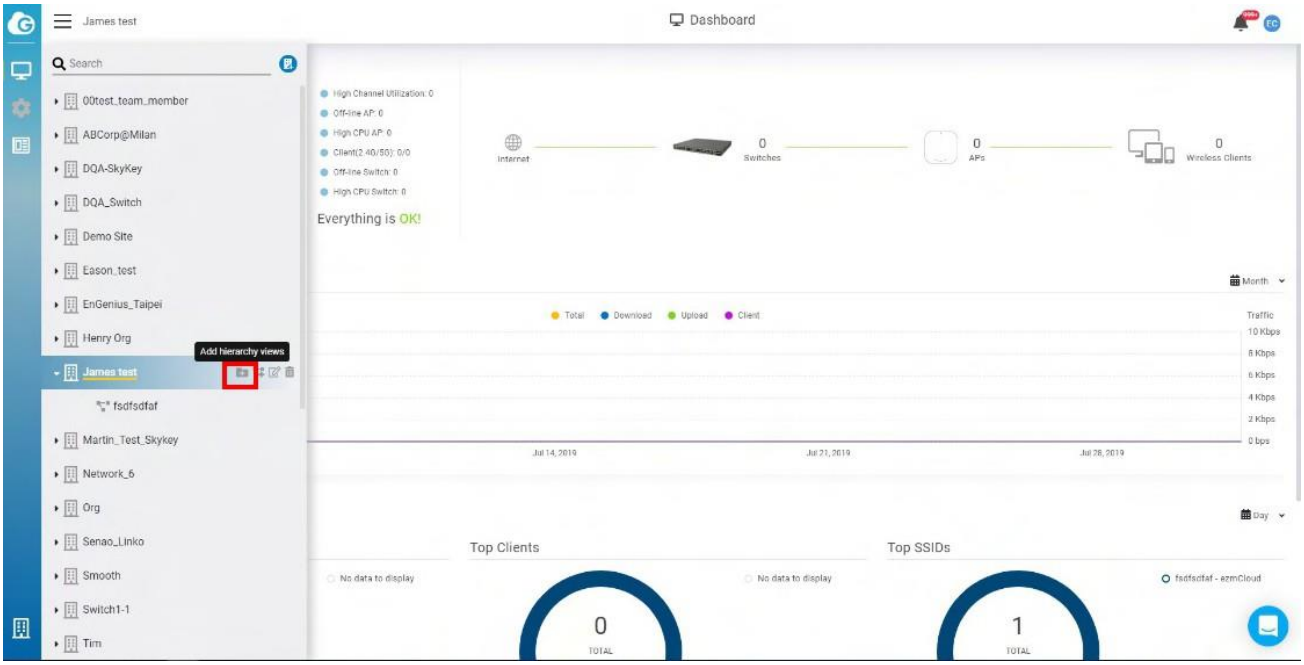
# Hierarchy View

A hierarchy view is a group of networks and/or nested hierarchy views. It follows a tree-like structure much like folders on your computer's operating system.

---

## Adding a hierarchy view

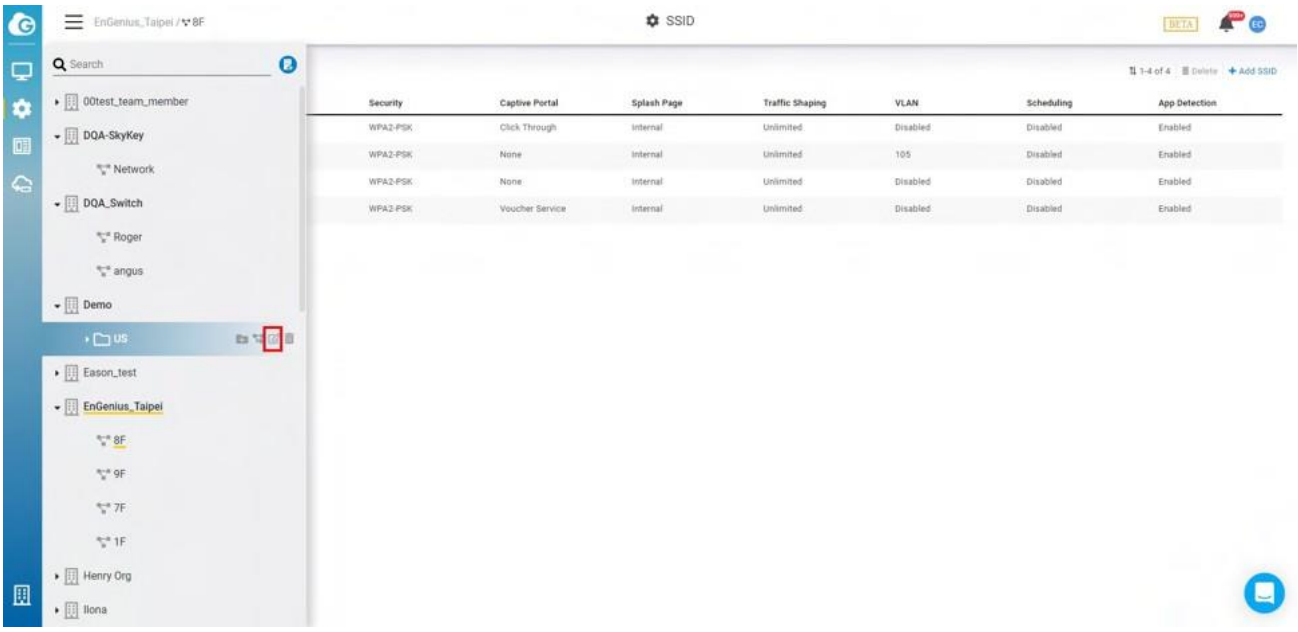
You can create hierarchy views for a new organization or an existing organization, or even within an existing hierarchy view. Click **Menu** > **Choose organization or hierarchy view > Add hierarchy view**



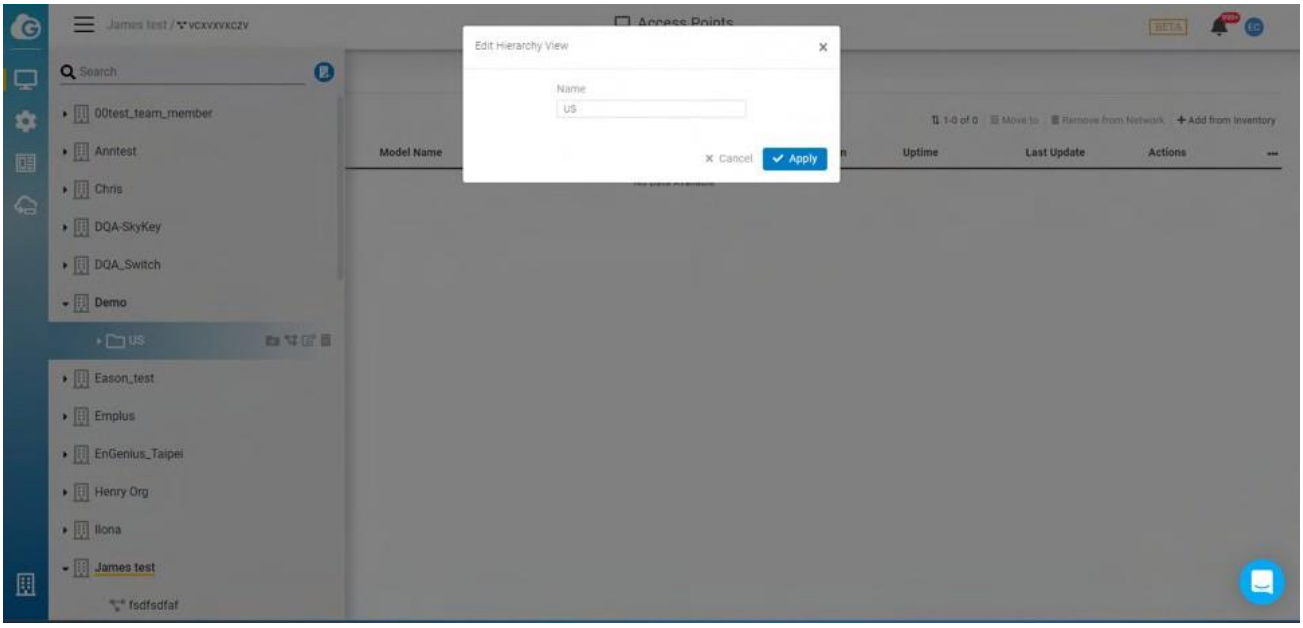

---

## Edit hierarchy views

1. You can edit the name of a hierarchy view name by clicking **Menu** > **Choose hierarchy view > Edit**




2. Change the **Hierarchy View** name and click **Apply.**




---

## Delete Hierarchy View

You can delete hierarchy views by clicking **Menu** > **Choose hierarchy view** and then clicking on the garbage icon.


Cl Access Points
BETA
Q.se.rch
81 Ea..._t.. t
@I Emplus
() EnGerilus:_Talpel
81 sonryOrg
81 James tes t
isd fs dfef
vcxvxvxczv
test
test
Martin_Test_Skykey
Network_6
Or
81 enII0-1.InICO
+ Add from Inventory
Model Name
Channel
WA N IP
No Data Available
0

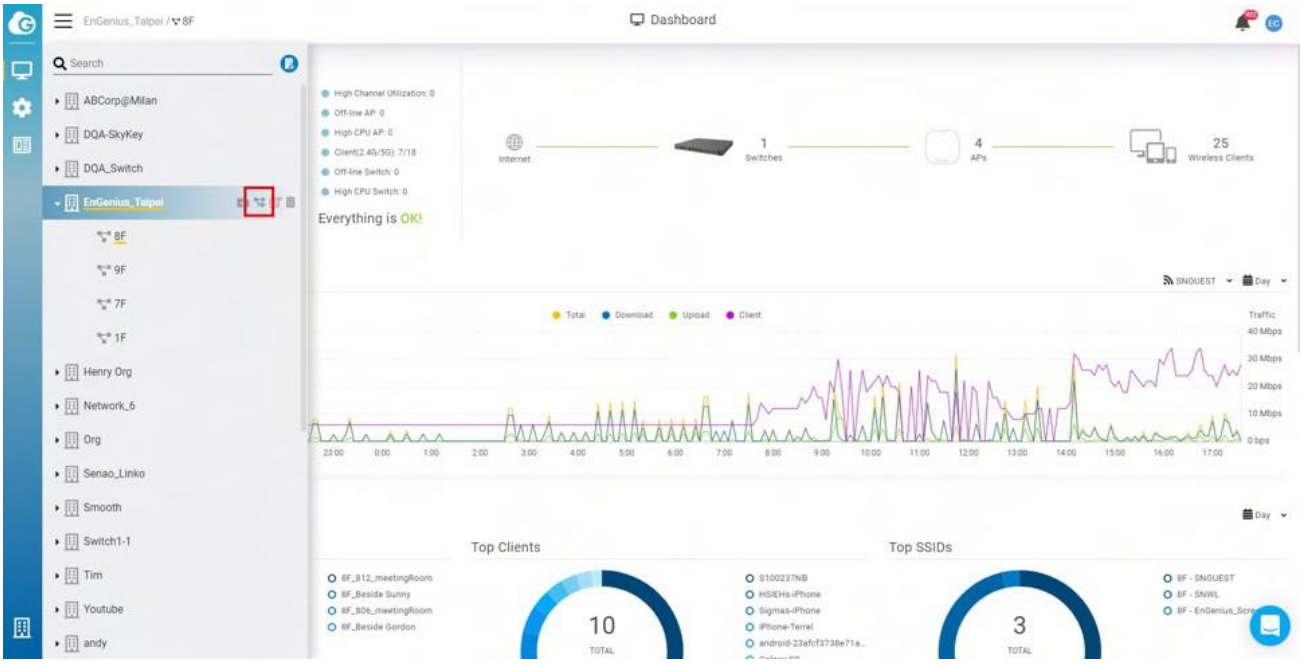
# Network

A network contains a list of devices and relevant information, such as configuration, SSID, radio settings, and firmware upgrade history. Each network contains a single configuration set for its devices, so if you have multiple configurations for devices, you can create a separate network to handle that.

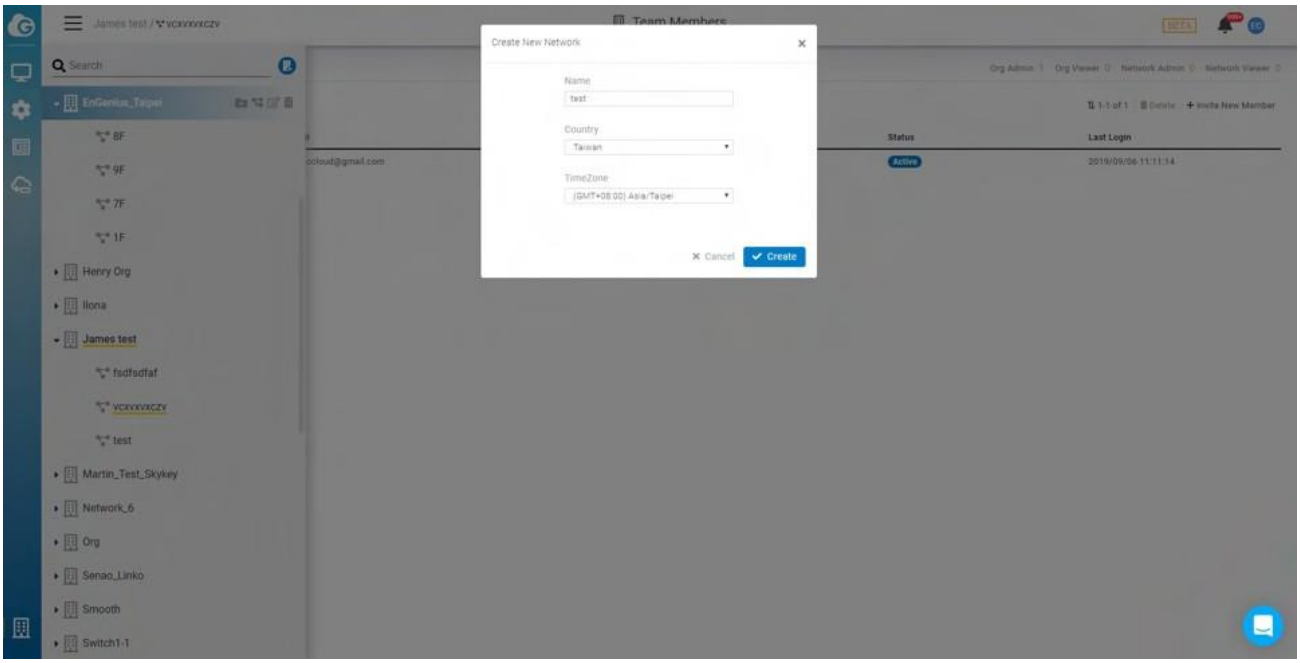
---

## Adding a network

1. Click **Menu > Choose organization or hierarchy > Create network**



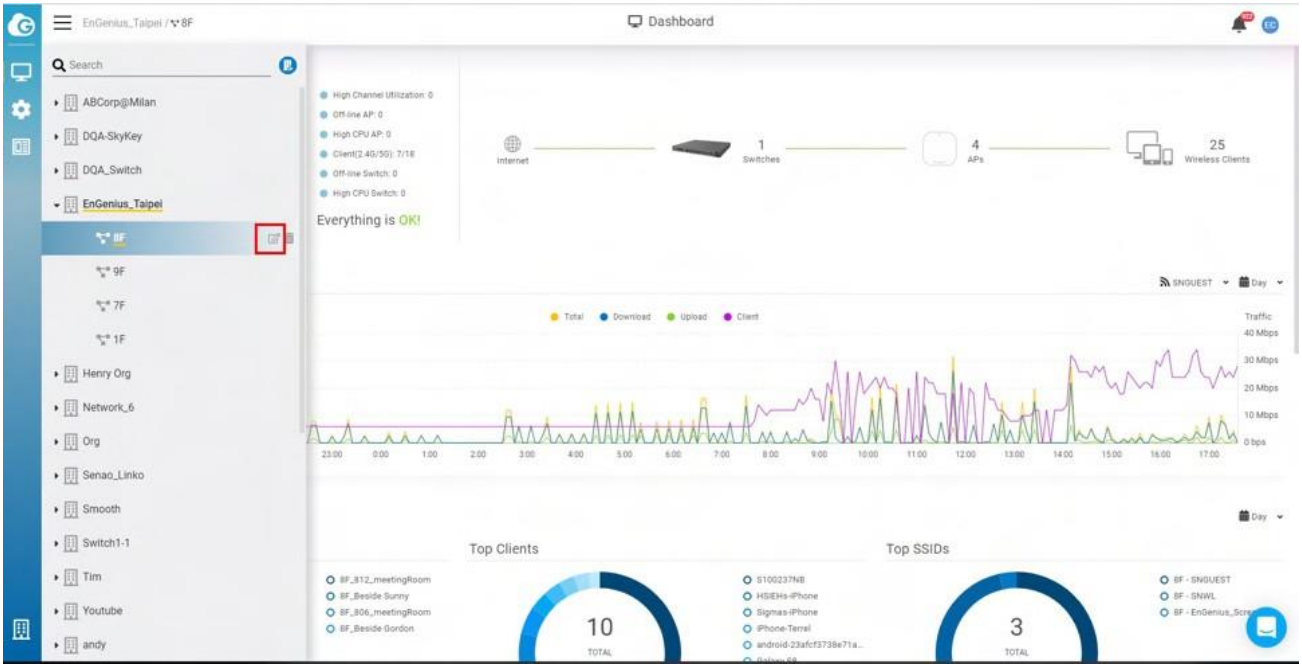

2. Enter a **name** for the network, select the **country**, **time zone,** and then click **Create.**




## Edit Network

**Network name**, **country**, and **timezone** can be edited as needed. Follow the steps below to edit a network.

**Choose network > Edit**

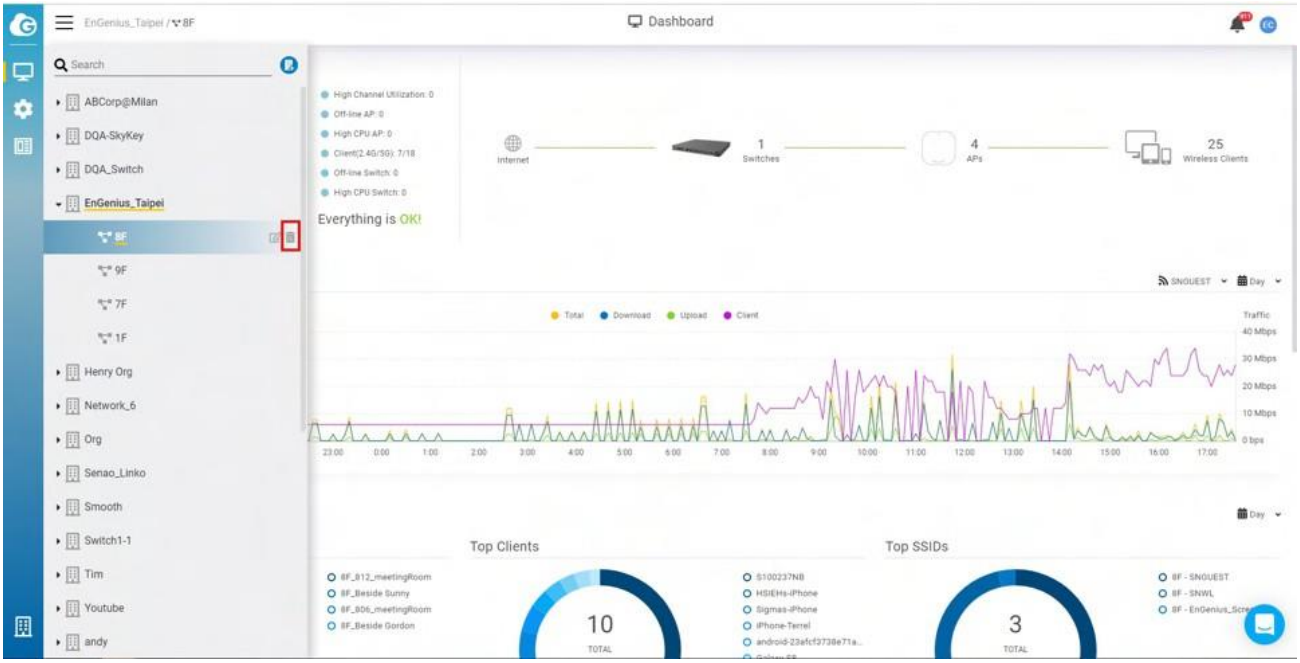


# Delete Network

If you no longer need a network that you previously created, you can delete it.

Follow these steps to delete a network.

1. Click **Menu > Choose network > Delete**



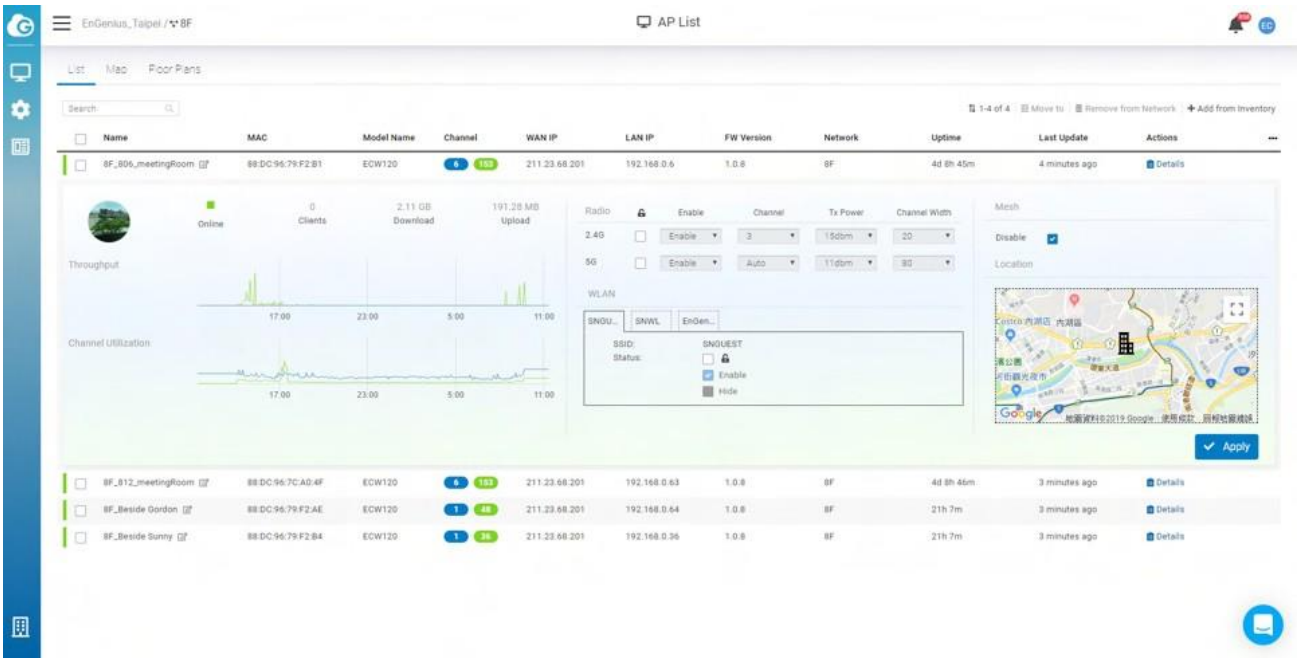

2. Popup is displayed. Click **Confirm.**

# Managing Devices

# Managing Access Points

This screen allows you to view the detailed information about your access points in the selected scope.

Click **Manage > Access Points** to visit the page, and double-click the organization/hierarchy view/network on the tree to change the current scope.




The following describes the functions on this screen:

**Move**: Select one or multiple access points and click to move the AP(s) to another hierarchy view/network.

**Remove From Networks:** Select one or multiple access points and click to remove from the current org/hierarchy view/network.

**Add From Inventory:** Click to add access points from your inventory

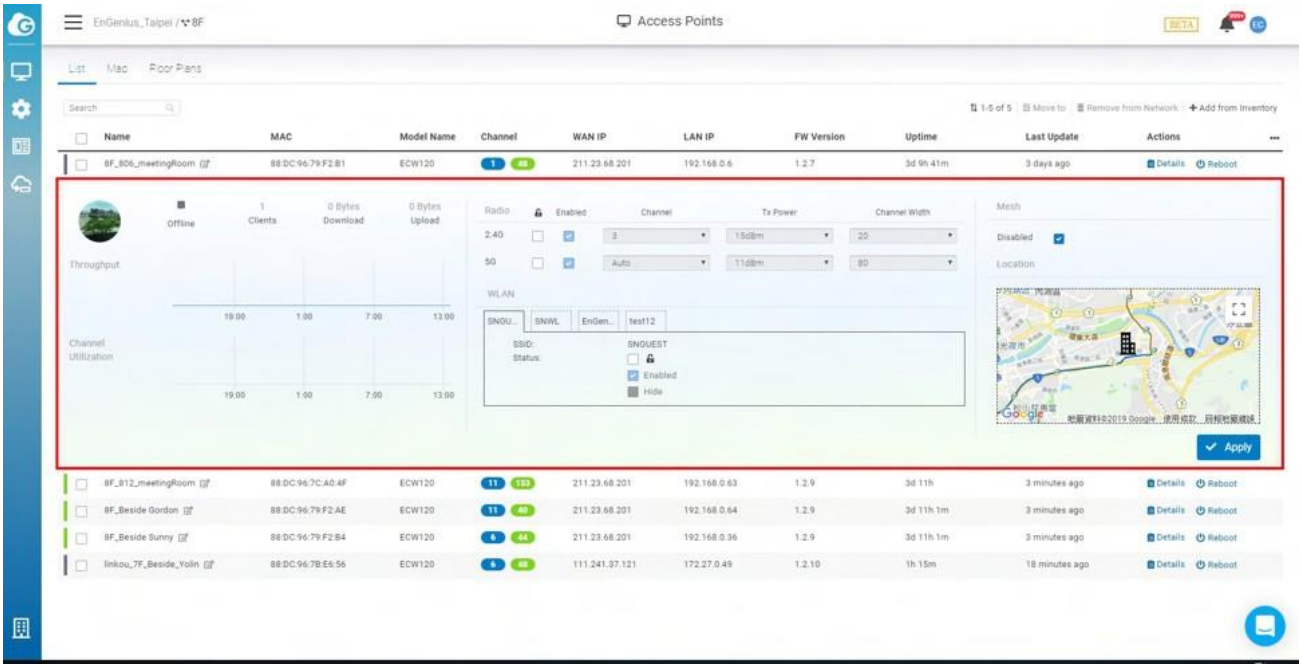
**Detail:** Click to display individual access point details

# Customizing Access Point Radio Settings

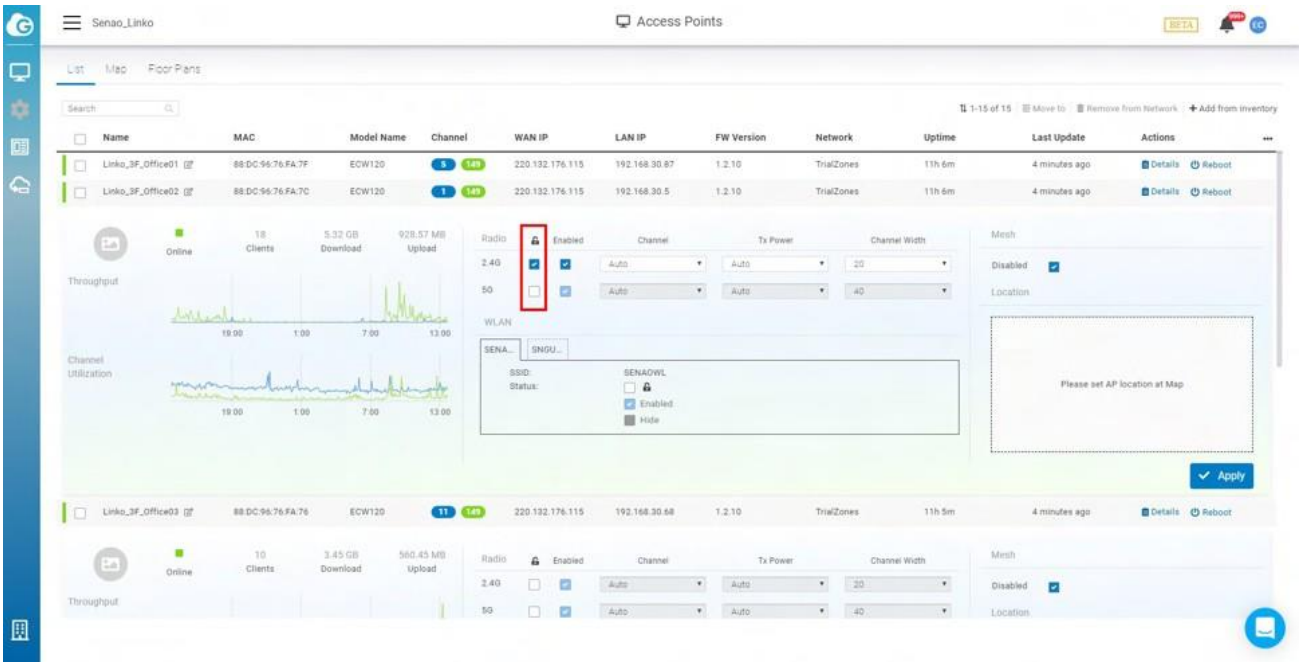
You can override the network's default radio settings of an individual access point if needed.

Follow these steps to customize the radio settings of a network.

1. Choose an access point from the list to show its expanded settings.

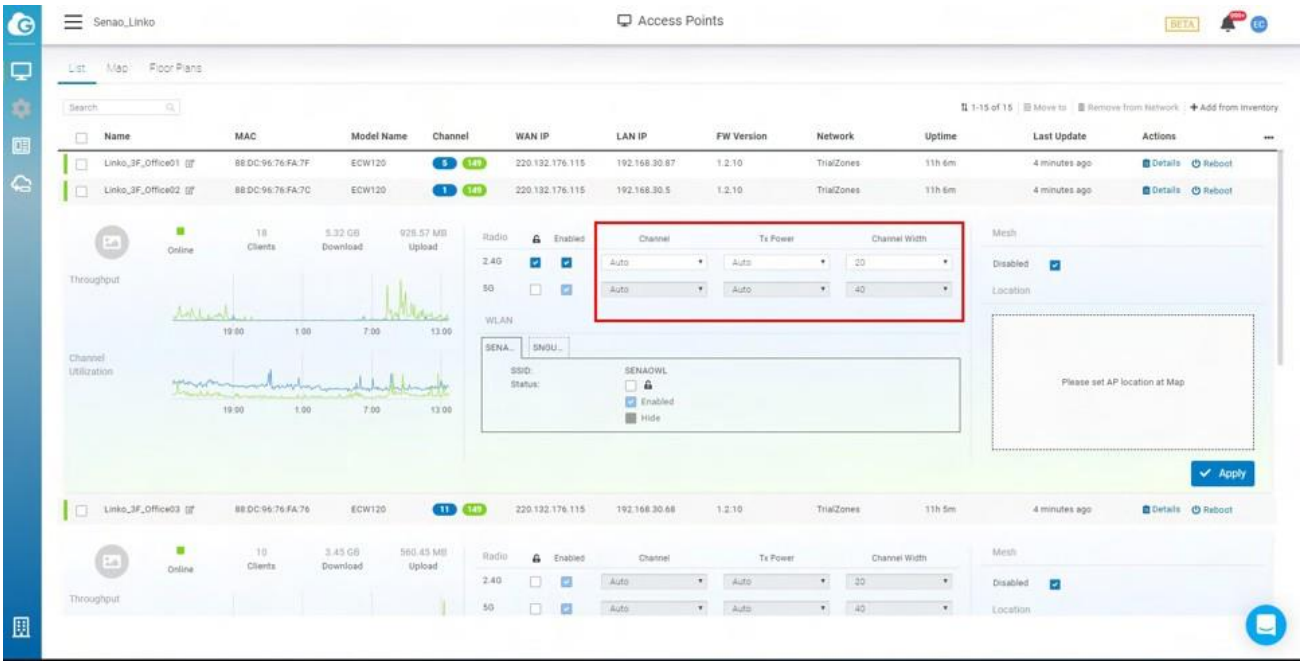



2. In the **Radio** section, click the checkbox below the lock icon to override default settings.

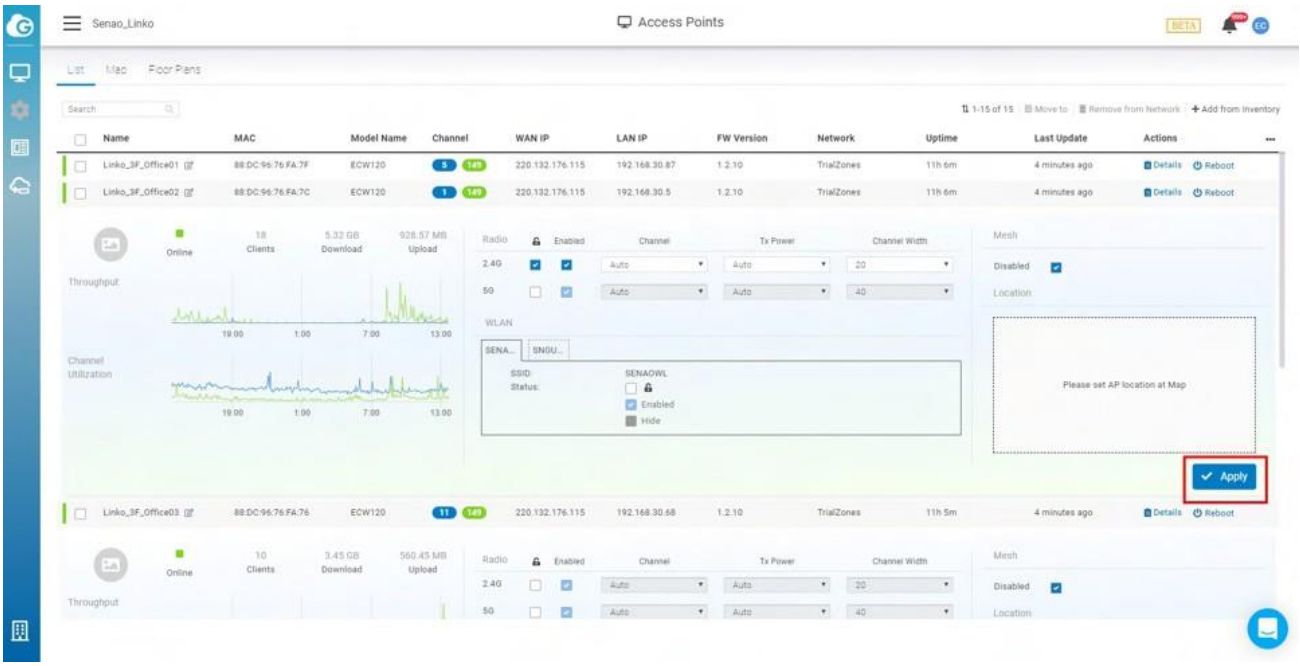



3. Configure the following settings for both the 2.4GHz and 5GHz radio band:

- Channel
- Tx Power
- Channel Width




4. Click **Apply.**

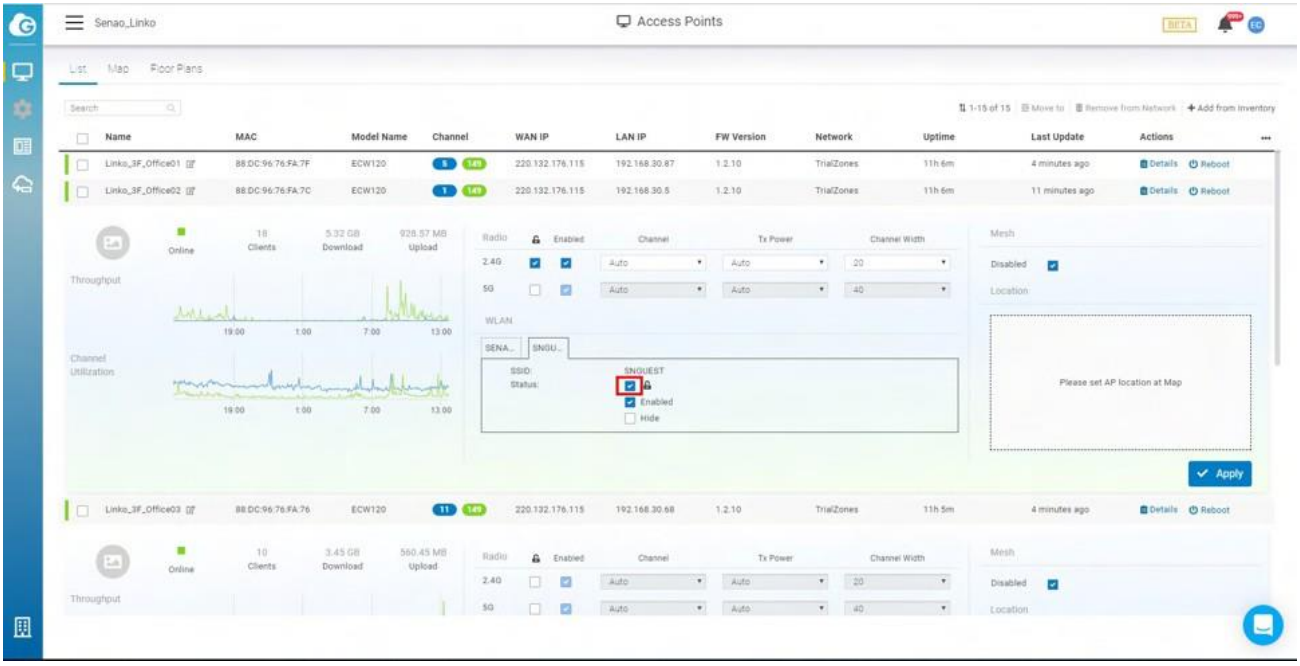



## Customizing the WLAN Settings of an Access Point

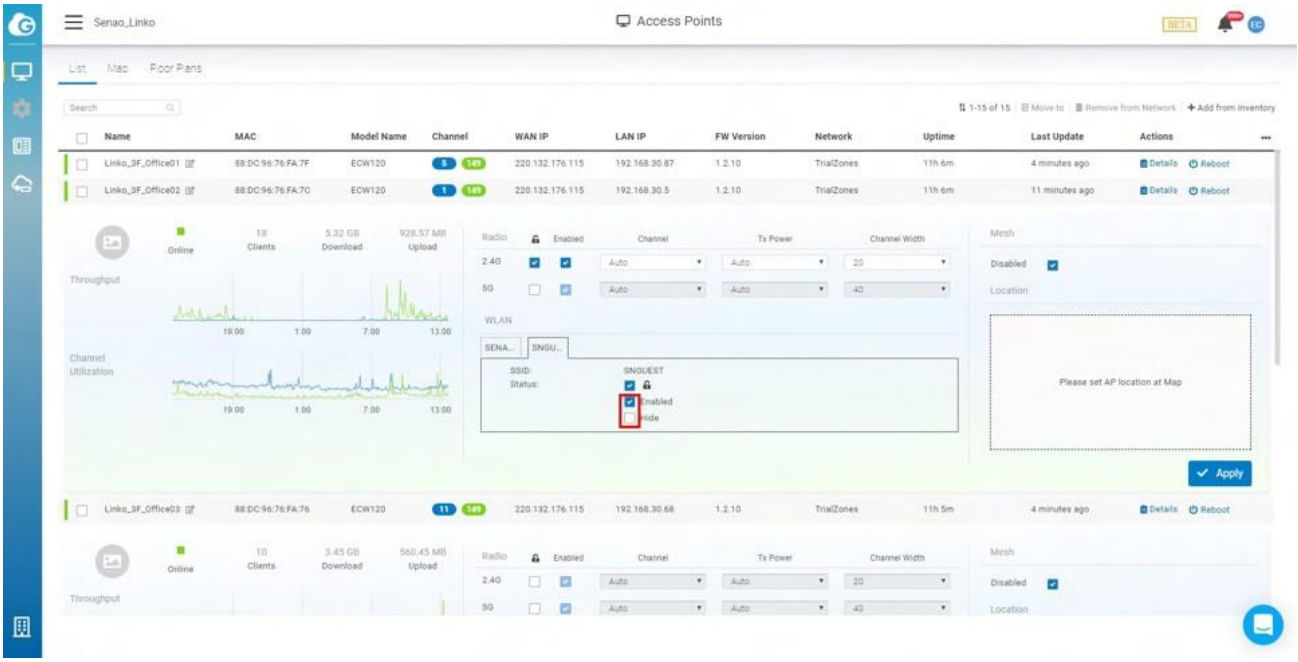
This shows SSIDs and allows you to override the default SSID setting.

Follow these steps to configure to enable the SSID, or hide the SSID of a network.

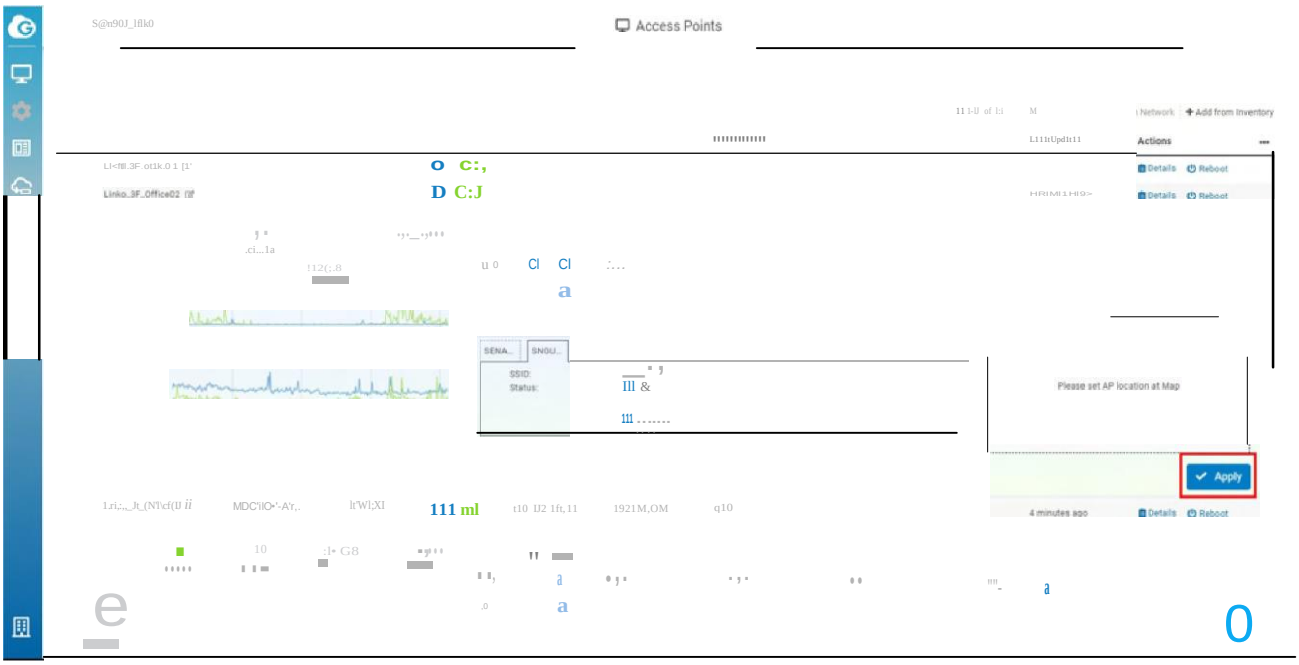
1. In the **WLAN** section, click checkbox near lock icon to override default settings.




2. Configure SSID to be enabled or hidden per your request.

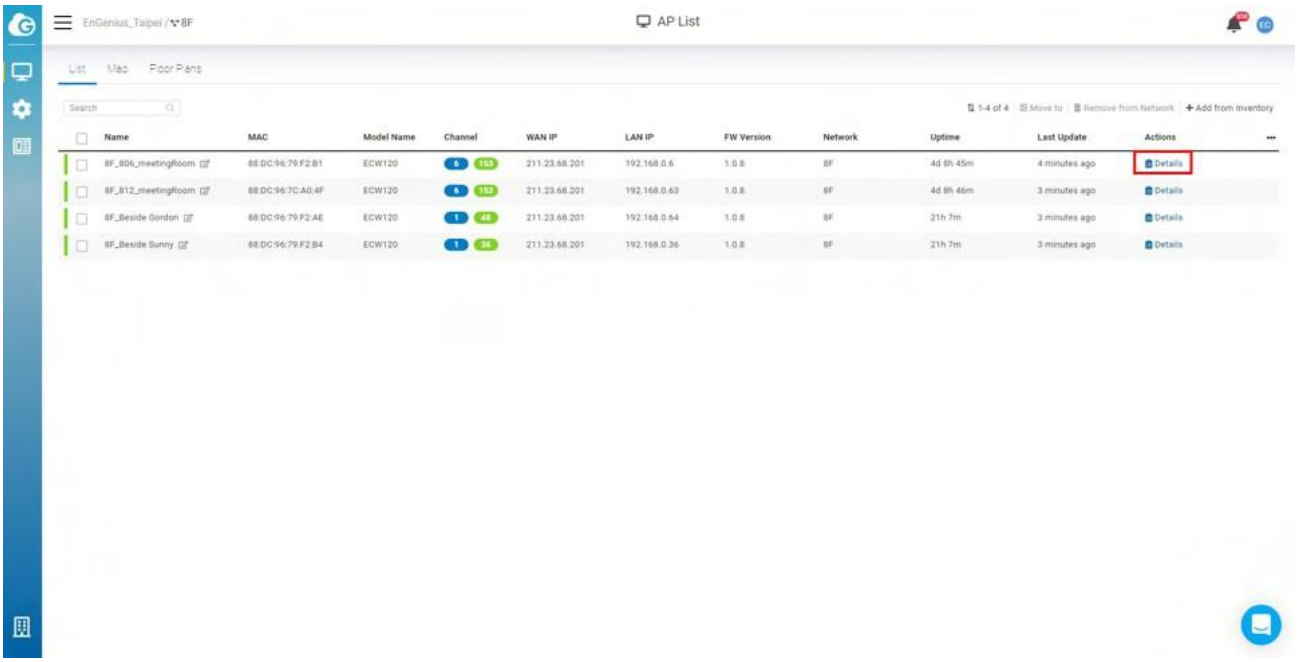



3. Click **Apply.**


Access Points
Add from Inventory
Actions
Details
Reboot
Please set AP location at Map
Apply
4 minutes ago

# Getting Access Point Analytics

From the **access point list** page, you can click **Details** to get detailed information about an individual access point.



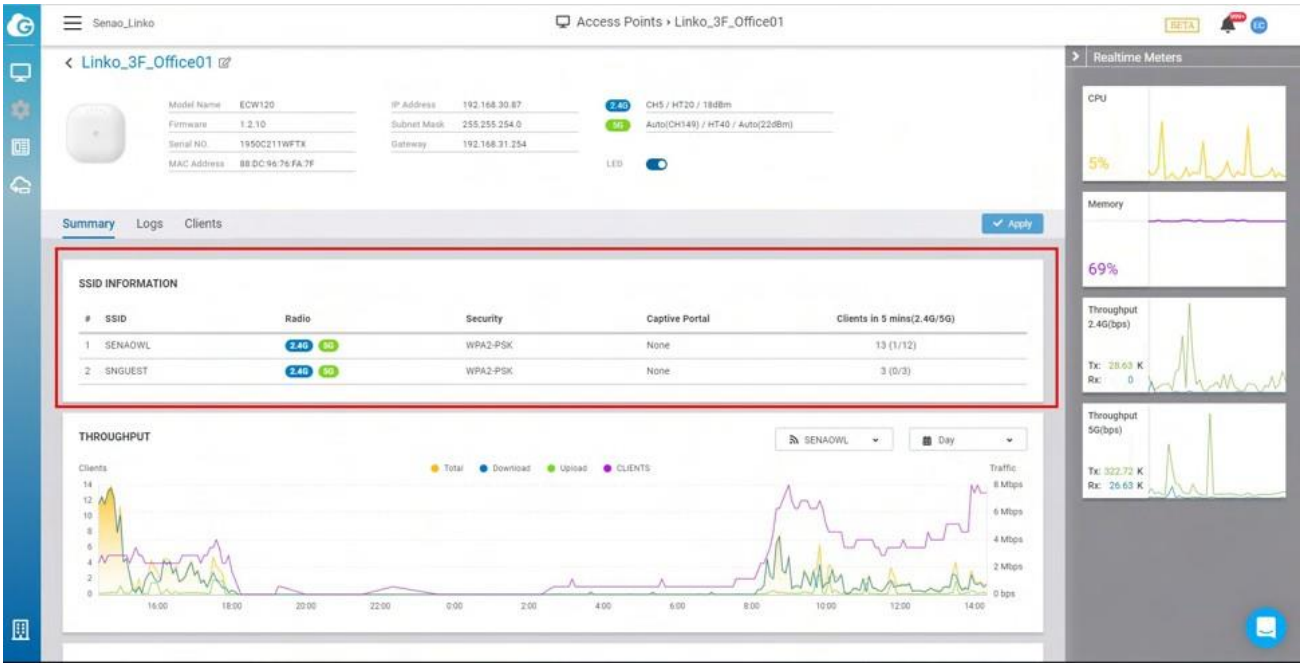

---

## Summary

### SSID

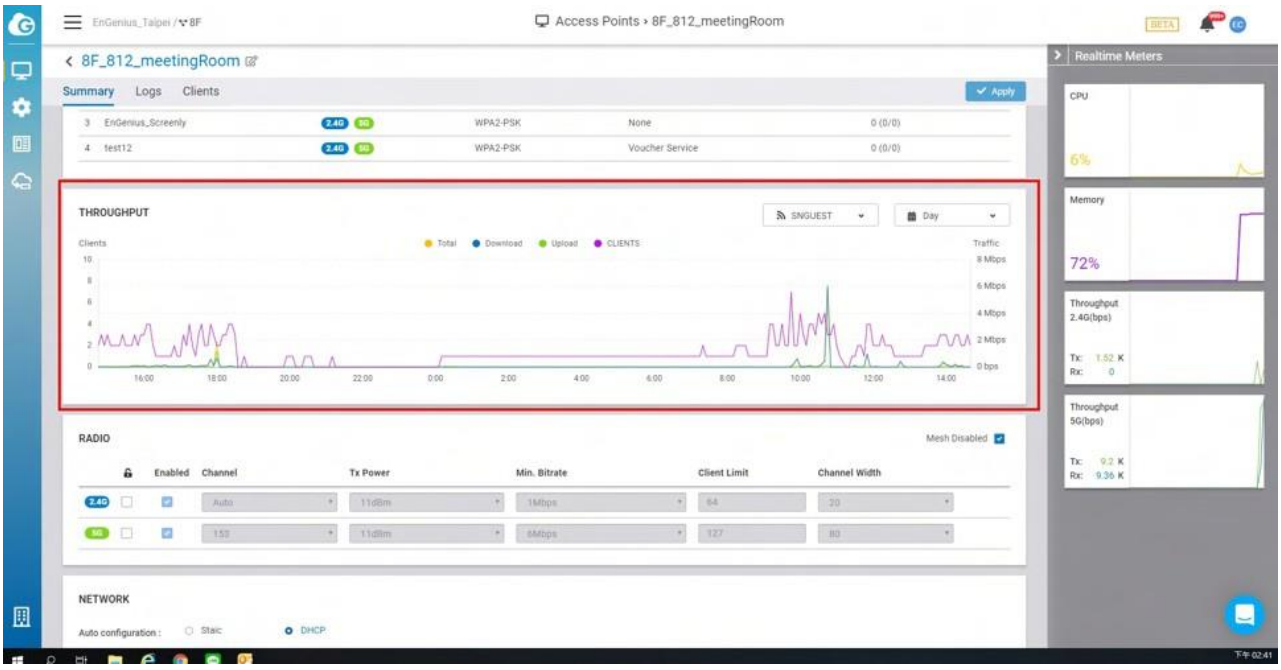
This screen allows you to monitor SSID for your access point.

- **SSID**: Shows the SSID name.
- **Radio**: Shows the SSID use for the 2.4GHz or 5GHz bands.
- **Security**: Authenticate users with Open or WPA-PSK or WPA-Enterprise when they connect to the SSID.
- **Captive portal**: Shows captive portal authentication type.




## Throughput

This screen allows you to monitor Throughput for your access point.

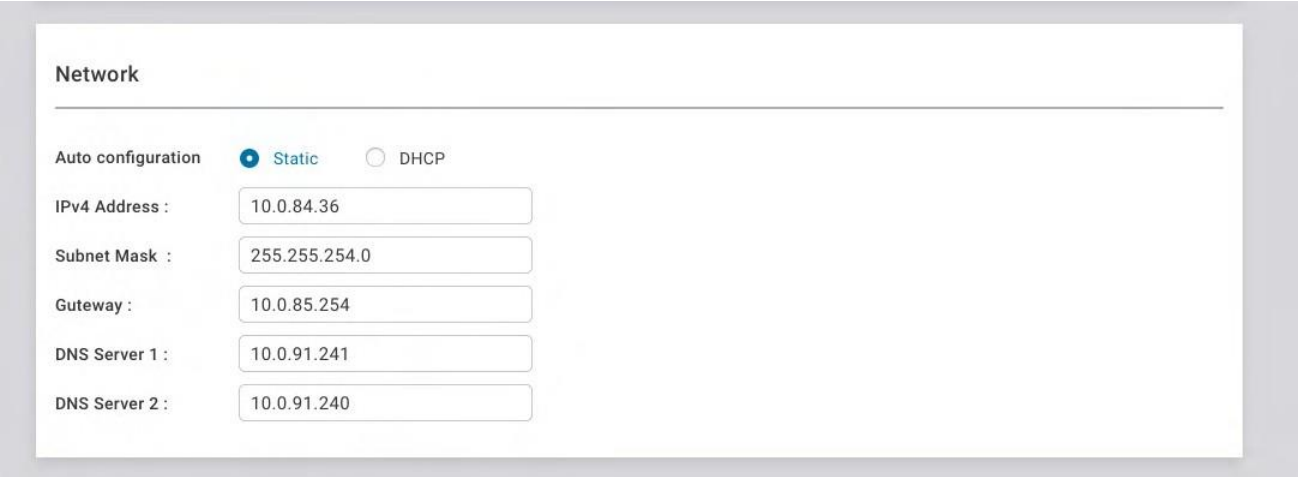


## Radio

This allows you to configure individual radio settings. The default radio setting will be followed by the network radio setting. If you want the radio settings of an access point to be different from the default, you can override them with custom values.


## Network

This allows you to configure individual access point network settings.



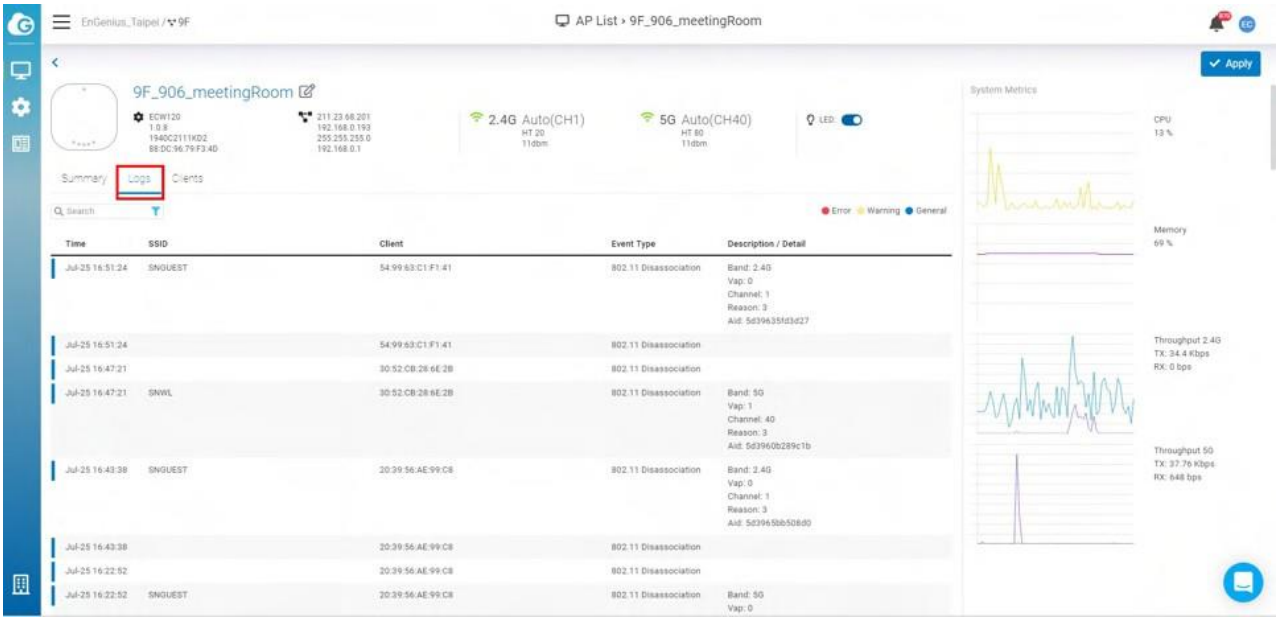

- **DHCP**: You can choose to auto assign IP addresses if there is a **DHCP** server in the network.
- **Static:** Allows you to manually assign an IP address.

Enter the IP address you wish to assign to the access point and fill in the subnet mask, default gateway, and DNS server address.

- **IPV4 Address**: Enter the IP address for the access point.
- **Subnet Mask**: Enter the subnet mask for the access point.
- **Gateway**: Enter the default gateway for the access point.
- **DNS Server 1**: Enter the primary DNS server name.
- **DNS Server 2:** Enter the secondary DNS server name.

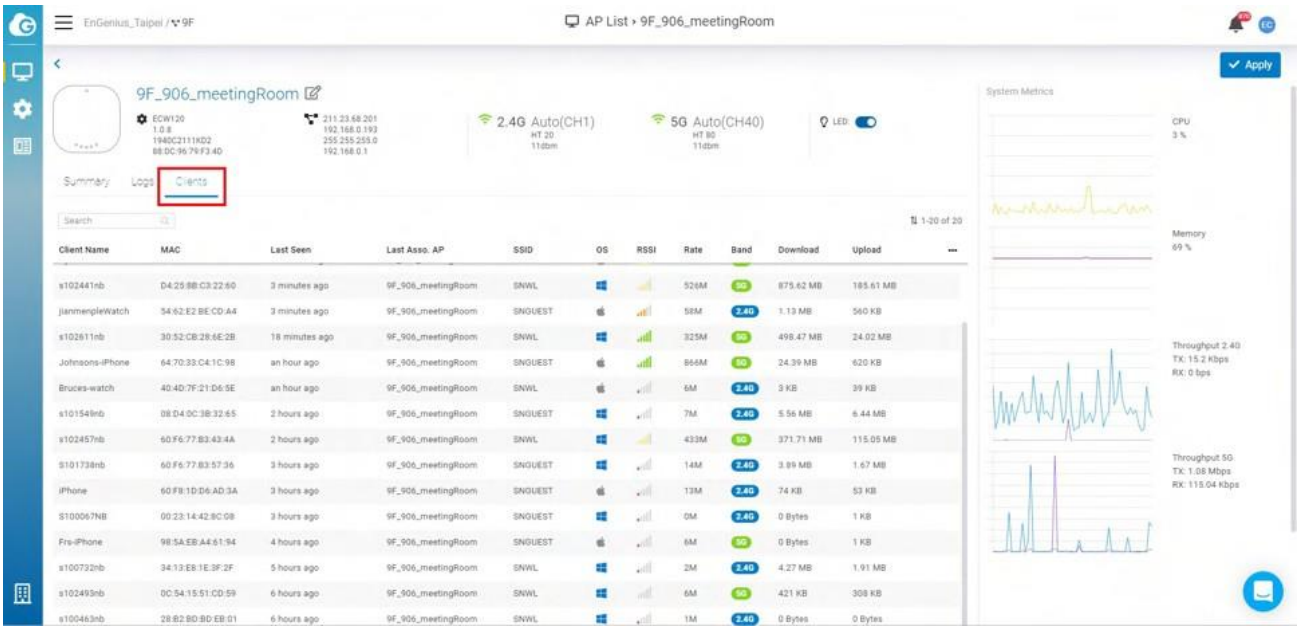
## Logs

Periodically viewing events that have occurred on an access point (or on clients associated with the access point) can help alert you to potential issues. The Logs tab appears and displays the latest events that have occurred in the last 24 hours.



## Clients

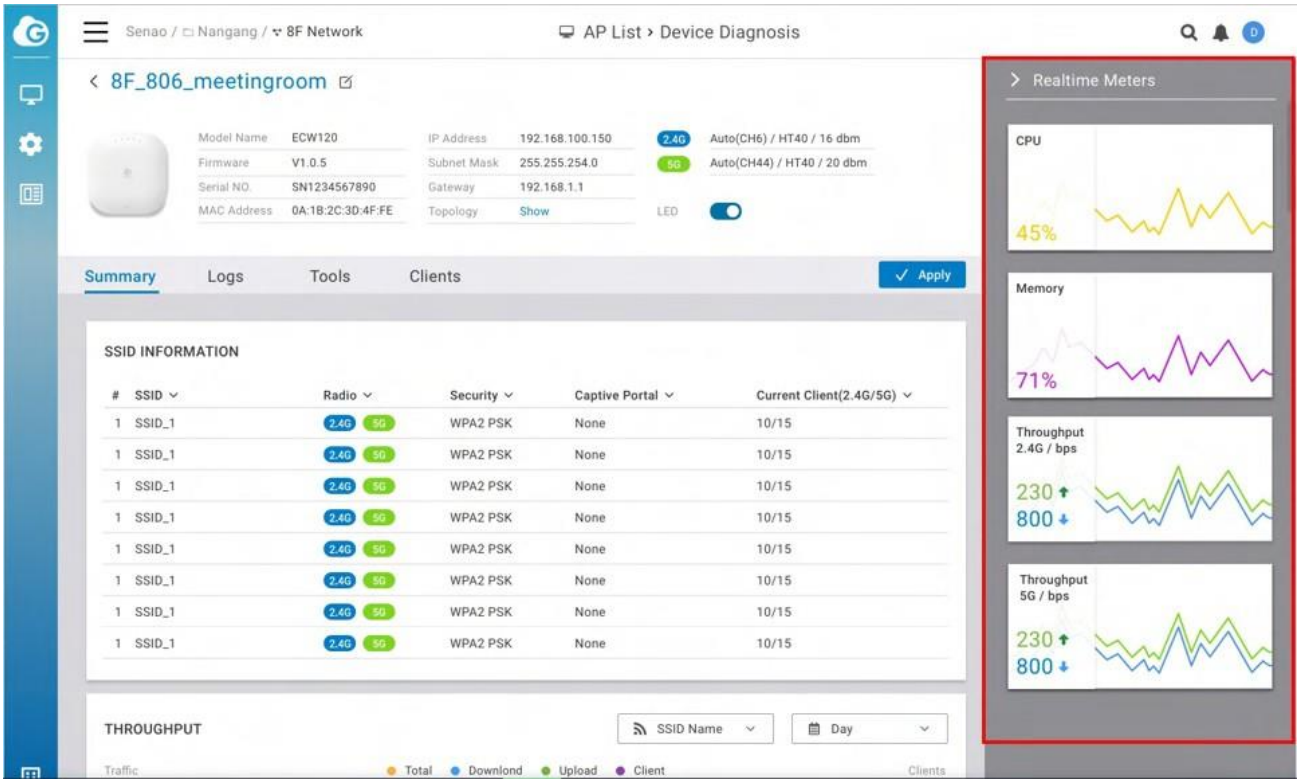
Use the Clients tab on the access point list page to view information about wireless clients that have  associated with a particular access point.




## Realtime Meters

Realtime Meters is primarily for viewing real time statistics. By default, there are four types of data:

- CPU
- Memory
- Throughput 2.4G
- Throughput 5G

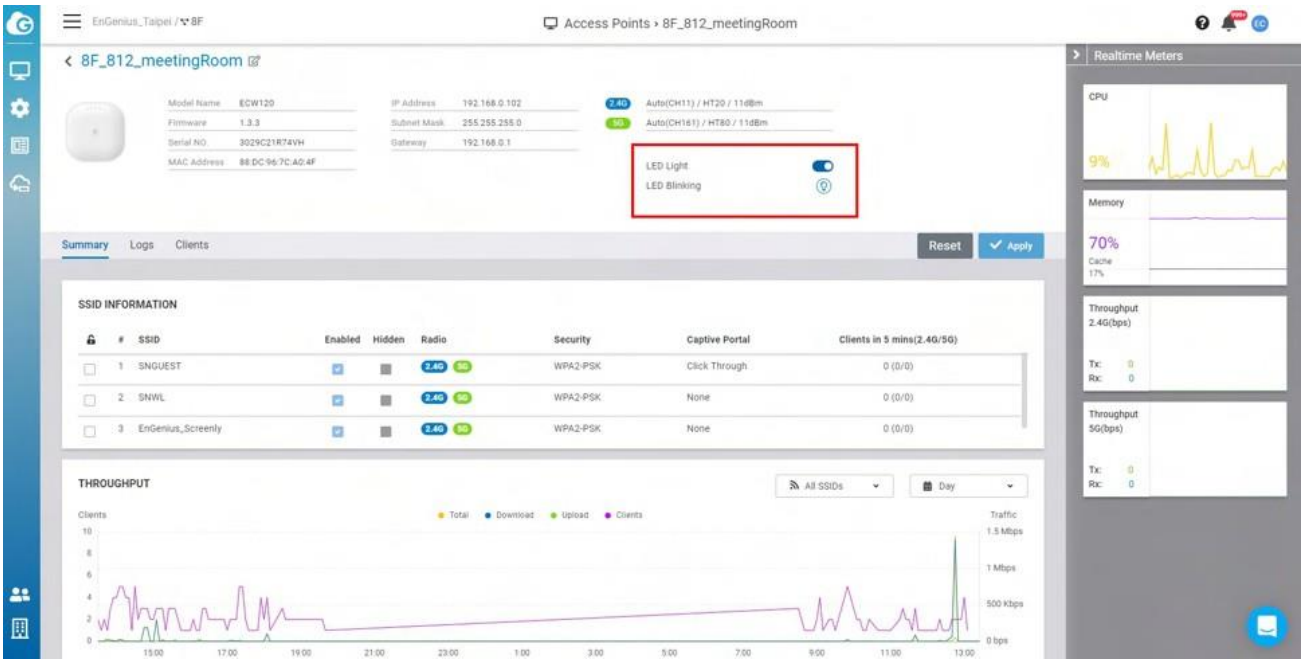



Capturing data over a period of time allows you to see trends most useful for determining the overall performance of your access point.

---

# LED

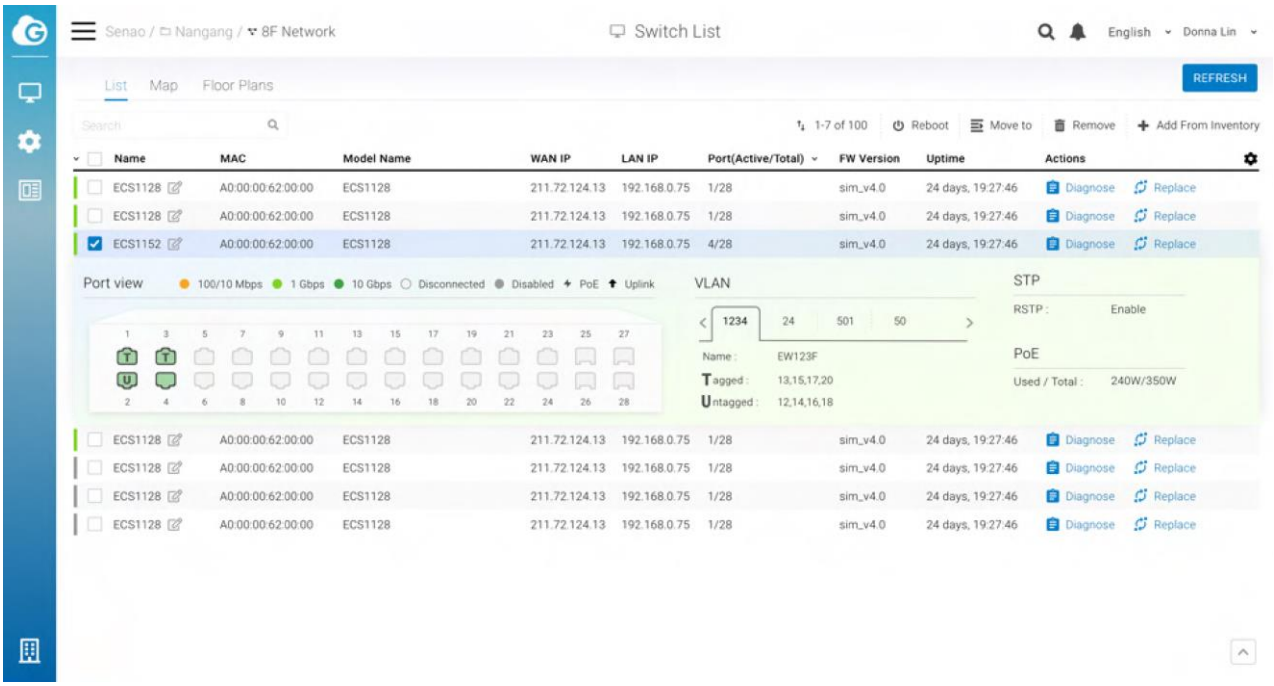
Use this screen to control LED lights and enable LED Blinking .




- **LED Light**: This allows you to enable or disable the LED Lights.
- **LED Blinking:** This feature is useful in situations where user could not find the specific AP properly. Click light bulbs to start blinking .

# Managing Switches

Click **Manage > Switches** to access this screen and double-click the organization/hierarchy view/network on the tree to change the scope.




The **Switch List** page lists all switches within your organization/hierarchy view/network, and allows you to choose each switch to view the port status, VLAN , STP and PoE.

The following describes the functions in this screen:

**Move to**: Select one or multiple switches and click to move the switches to another hierarchy view/network.

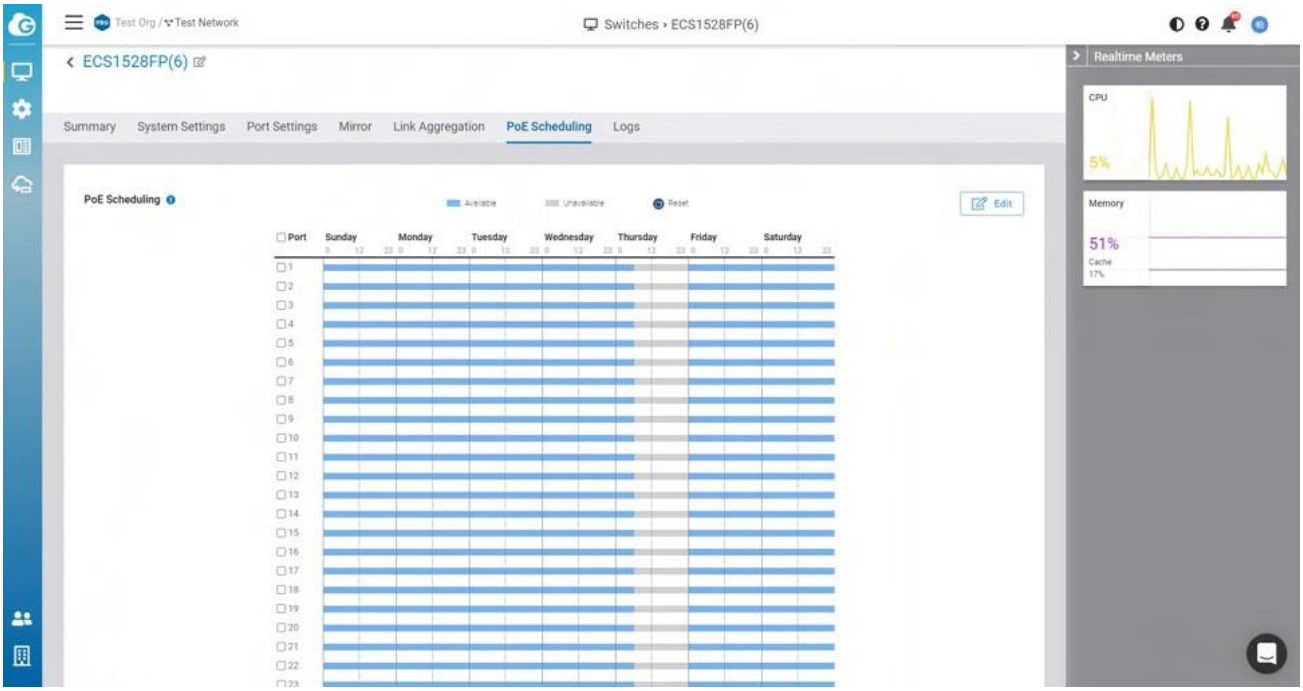
**Remove From Networks:** Select one or multiple switches and click to remove the switches from the current organization/hierarchy view/network.

**Add From Inventory:** Click this button to add switches from your existing inventory.

**Detail:** Click to display the individual switch details.

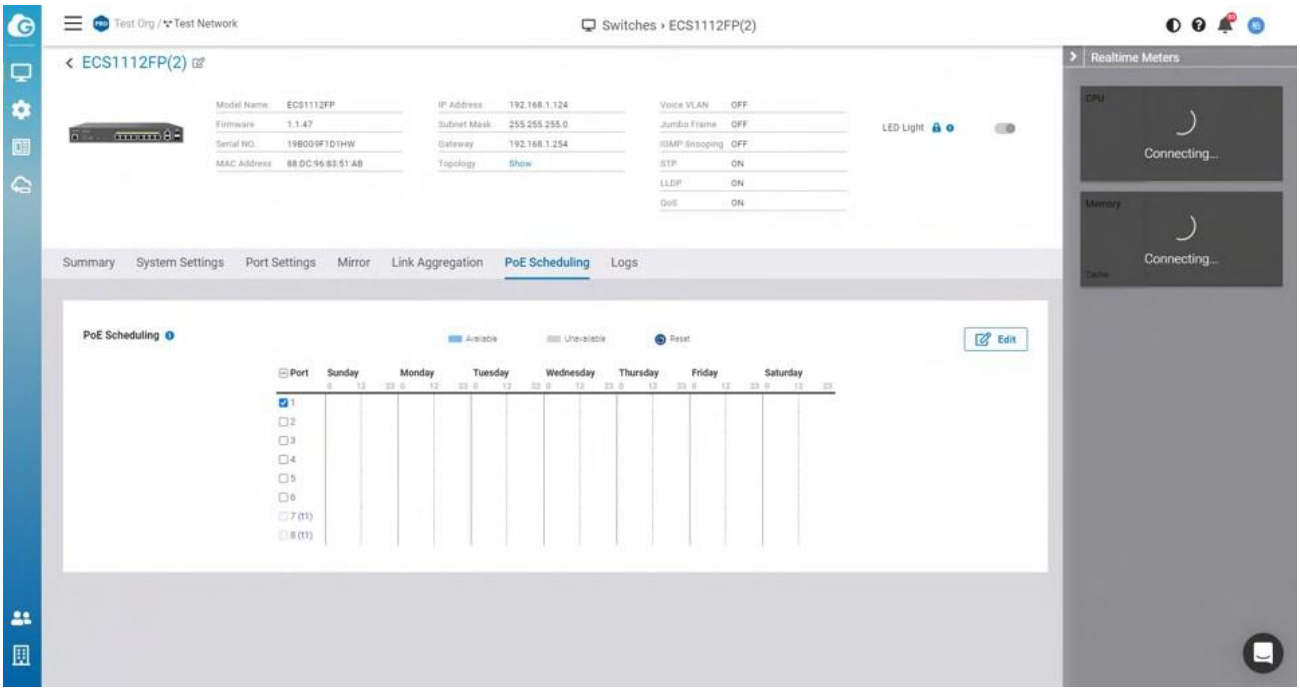
# PoE scheduling

This allows you to view and configure PoE schedules that can be applied to the ports. Below screens display the existing schedules visually. Click **Manage > Switch lists > detail > PoE scheduling** to access this screen

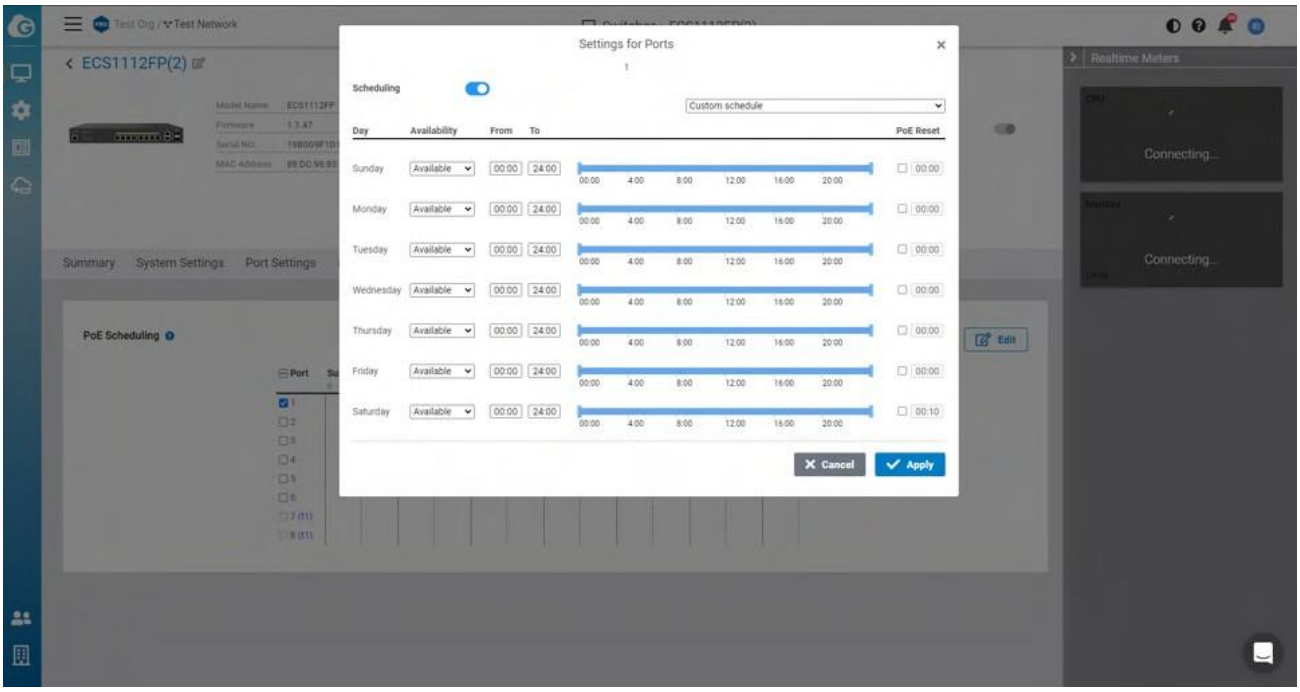



## Edit PoE Scheduling

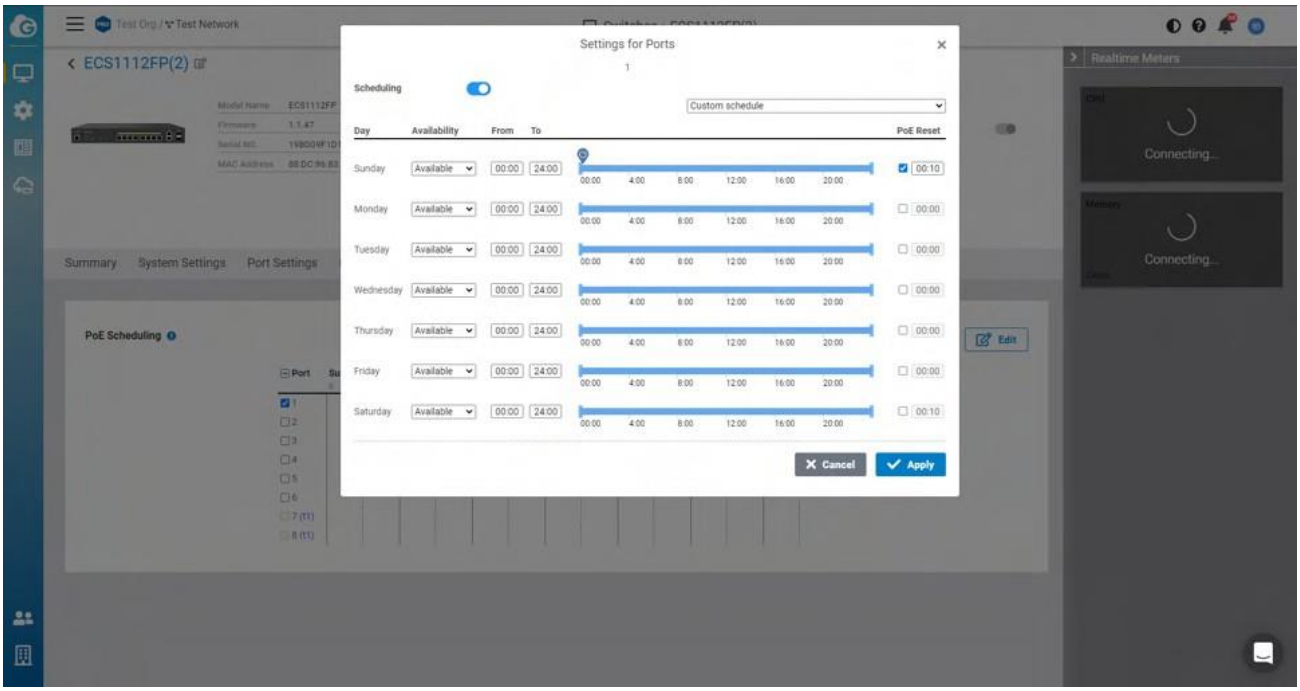
1. Select the ports to be set the PoE scheduling then click Edit




2. Enable scheduling and then customize the PoE on or Off by dragging the bar. This behavior is the same when you configure the SSID scheduling.



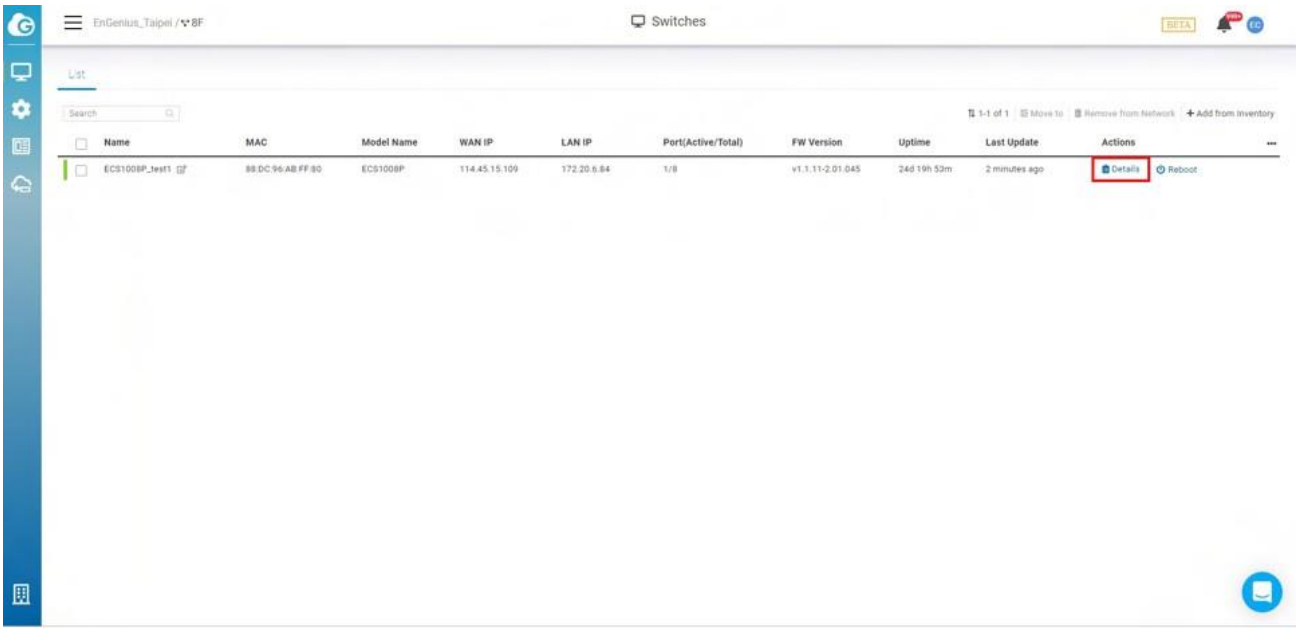

3. If you want to do the PoE reset, you can simply click PoE rest and then drag the icon to the specific time.




4. Click Apply.

# Getting Switch Analytics

From the **Switches** page, you can click **Details** on the web interface to display detailed information about a switch.




## Summary

**PoE reset from the Switch Panel :**

User can mouse-over to the PoE port of the switch port panel and power-cycle the port, so the device attached to the port will be rebooted


**Total PoE Usage:** This bar graph displays the consumed, remaining, and total wattage utilized by Power over Ethernet.

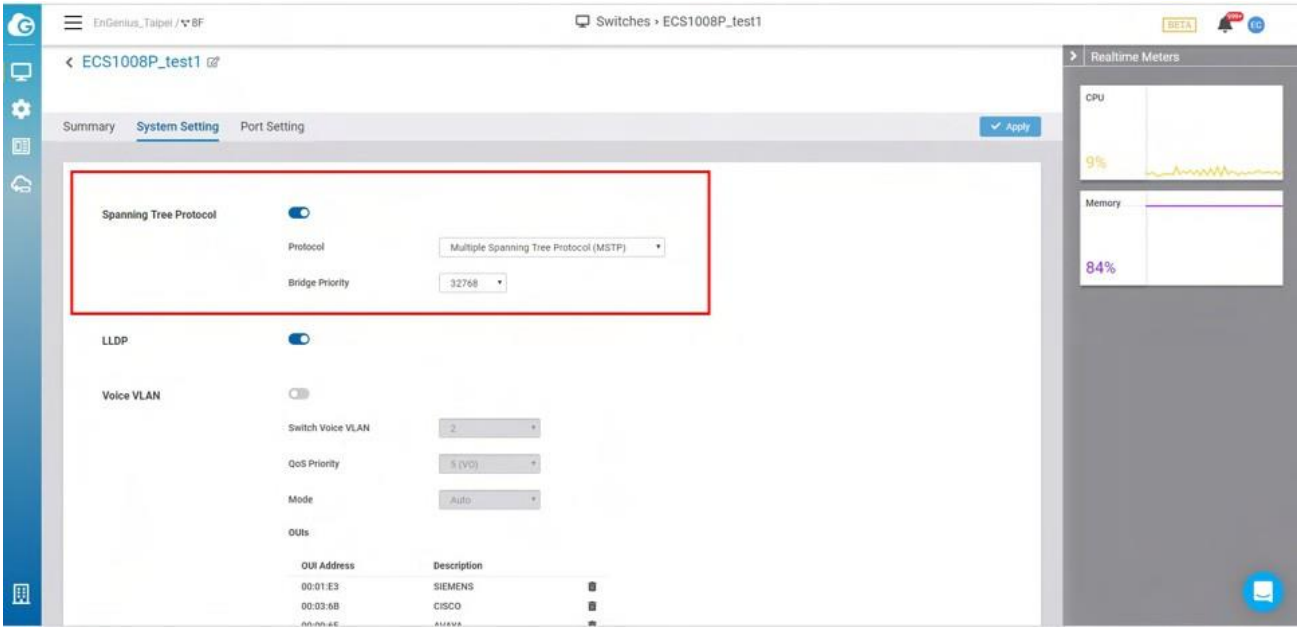
**Total PoE Utilization by Port:** Displays the current PoE utilization by each port, in watts.


# System Setting

The System Settings section allows you to configure all primary networking options for your switch.

## Spanning Tree Protocol

A **Spanning Tree Protocol** is a Layer 2 protocol that prevents loops in a network with redundant paths created by multiple switches. We recommend using this feature if your environment incorporates multiple switches.

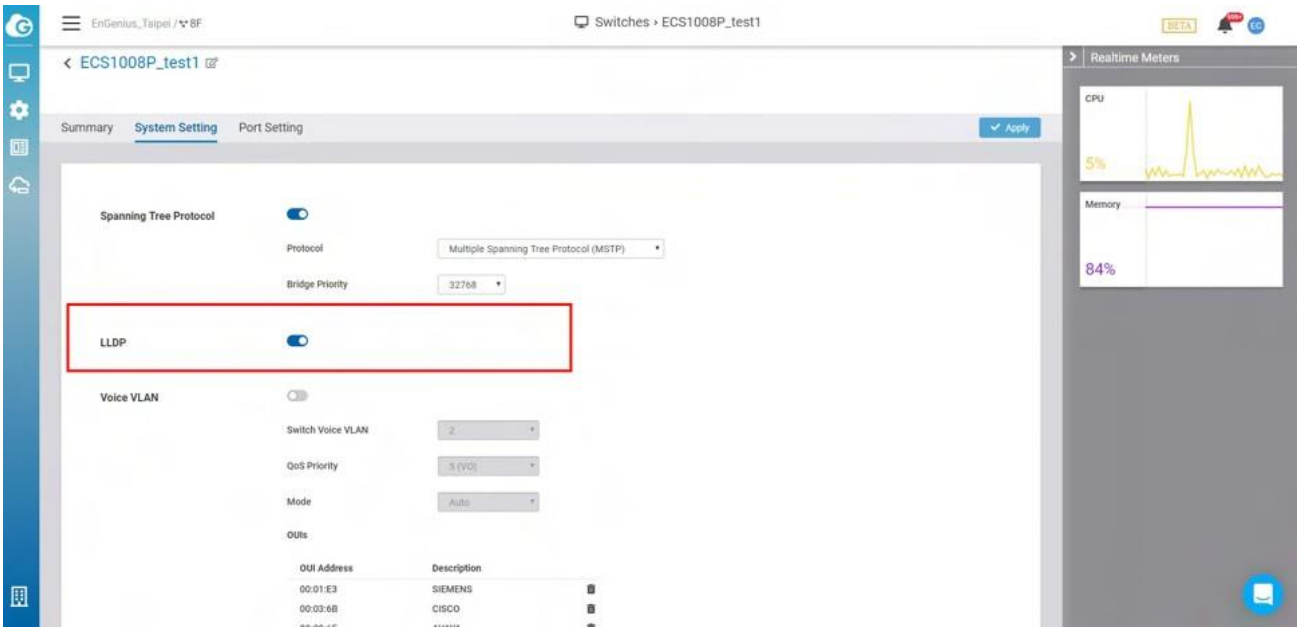



**Procedure**

1. **Enable** the **STP** option
2. Select a **Protocol**
3. Select a **Bridge Priority** value
4. Click **Apply**

## LLDP

The **Link Layer Discovery Protocol (LLDP)** is a Layer 2, vendor-neutral protocol that allows network devices to advertise capabilities, identity, and other information. This data can potentially be queried by SNMP.

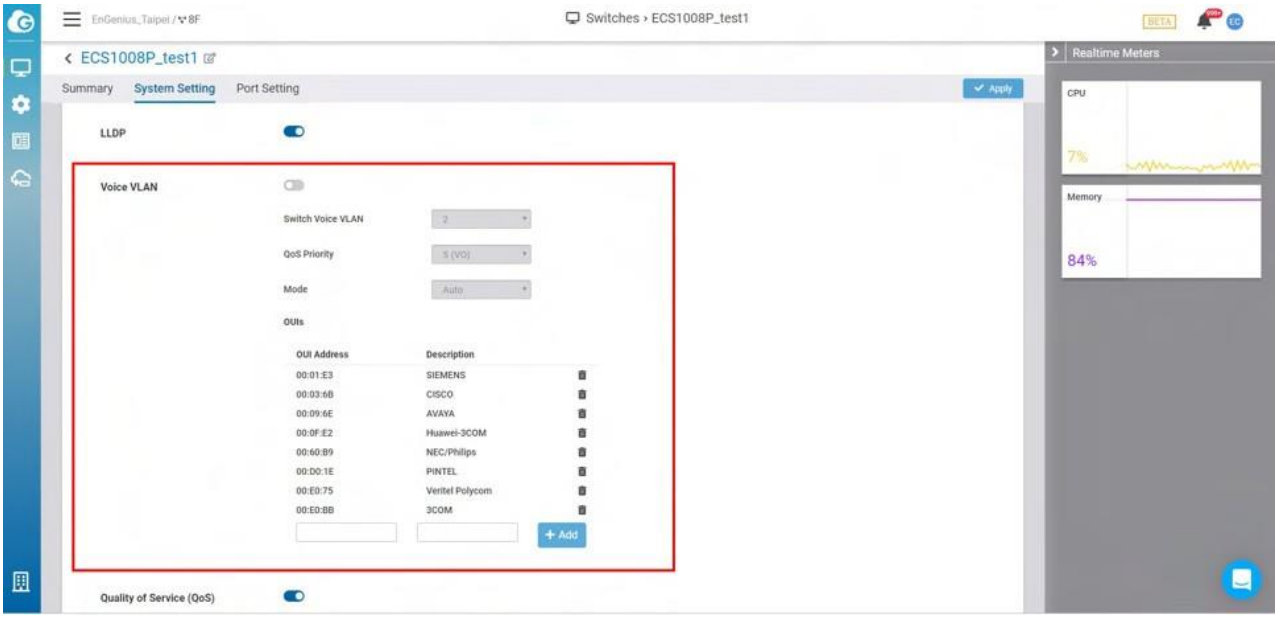



**Procedure**

1. **Enable** the **LLDP** option
2. Click **Apply**

## Voice VLAN

The **Voice VLAN** feature configures switches to automatically allow and prioritize voice traffic over a designated VLAN. This keeps voice traffic separate and prioritized over other traffic types.



**Mode:** Allows you to define the Voice VLAN mode.

- **Auto**: Automatically advertises the Voice VLAN to connected devices via the LLDP-MED protocol.
- **OUIs**: Determines whether a received packet is a voice packet by checking its source MAC address.

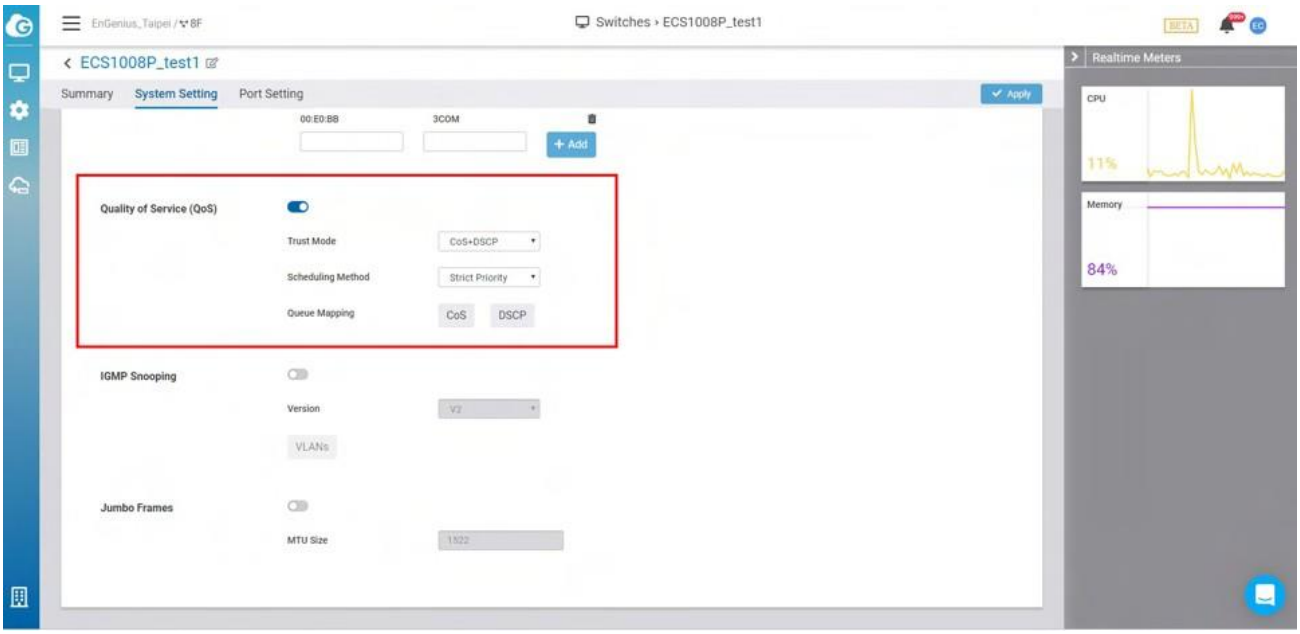
**Switch Voice VLAN**: Allows you to choose what VLAN is used for Voice VLAN. You can set up VLANs in Port Settings.

**QoS Priority:** Lets you define whether the switch will use the Quality of Service CoS value of the incoming packet, or tag the packet with a CoS value between 1-7.

**OUIs:** VoIP traffic has a pre-configured Organizationally Unique Identifier (OUI) prefix in the source MAC address. You can manually add a specific manufacturer's MAC address 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.

## QoS

Quality of service (QoS) allows operators to prioritize application traffic to ensure that latency-affected data, such as VoIP and video conferencing, is uninterrupted during periods of network congestion. Switches implement this by reading tagged packets and prioritizing them accordingly. Packets are classified using **Class of Service (CoS)** on the data link layer, and **Differentiated Services Code Points (DSCP)** on the network layer, mapped to a queue, then sent out accordingly as per QoS.



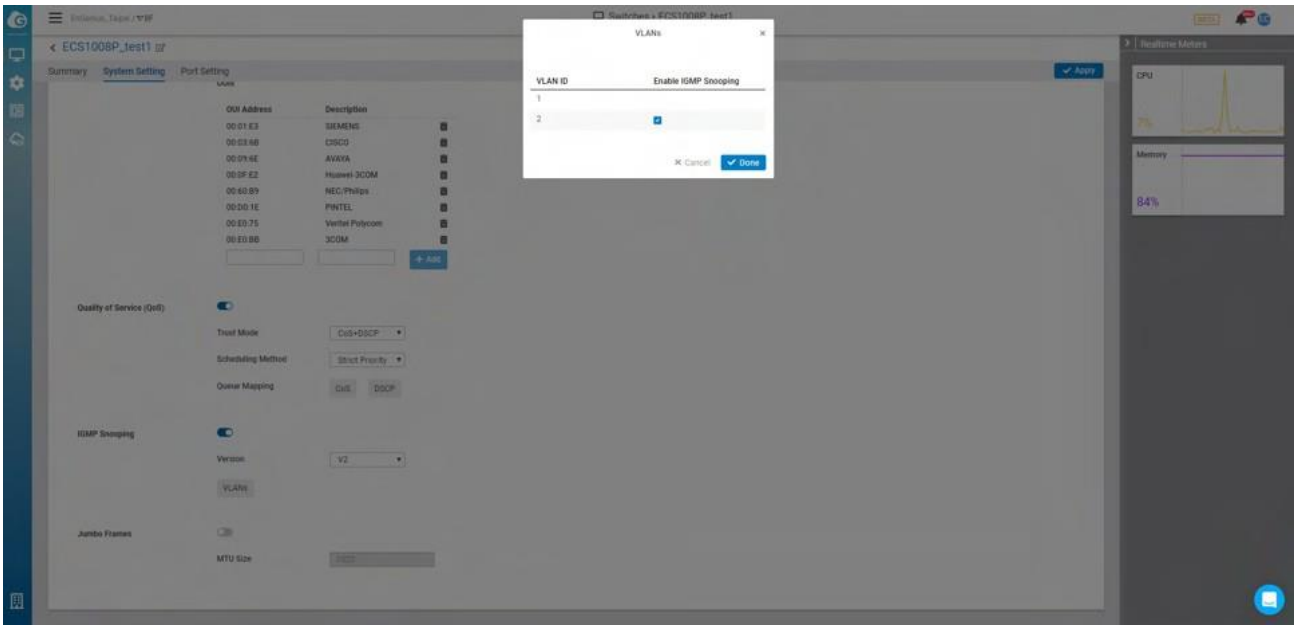

**Trust Mode**: Allows you to define whether the switch will use CoS, DSCP, or both trust modes for QoS.

**Scheduling Method:** Allows you to define what method the switch will use when assessing transmitting incoming packets in queues. **Strict priority** always prioritizes queues with a higher priority, while **Weighted Round Robin (WRR)** weights each queue by priority, then applies a round-robin policy when choosing packets for transmission.

**Queue Mapping:** Tagged packets are sent to queues defined in this setting. For each CoS or DSCP value, you can choose the queue to which tagged packets are mapped.

## IGMP

**IGMP Snooping** is used for controlling multicast traffic. It listens to IGMP messages being processed by the switch and prevents these messages from being sent to hosts not part of the respective multicast.




**Version:** The available IGMP Snooping versions are v2 and v3. You can select either/or in the **Version** dropdown.

**VLANS:** You can enable IGMP Snooping for any VLAN by selecting the corresponding checkbox next to the VLAN ID.

## Jumbo Frame

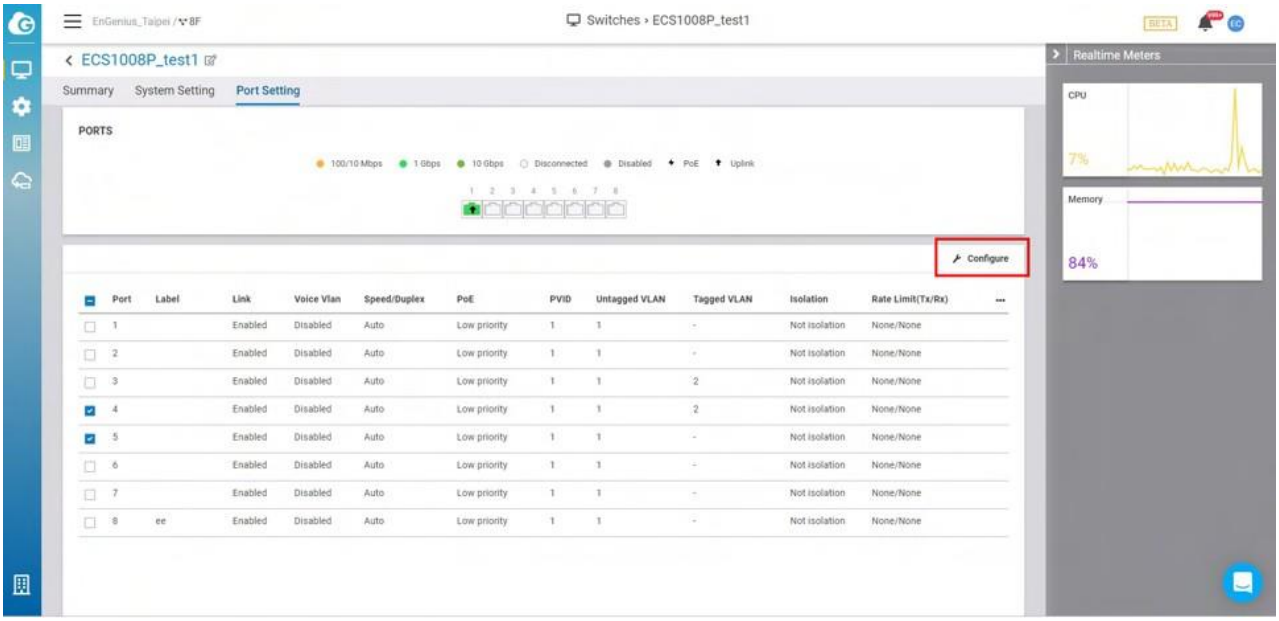
Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application 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.

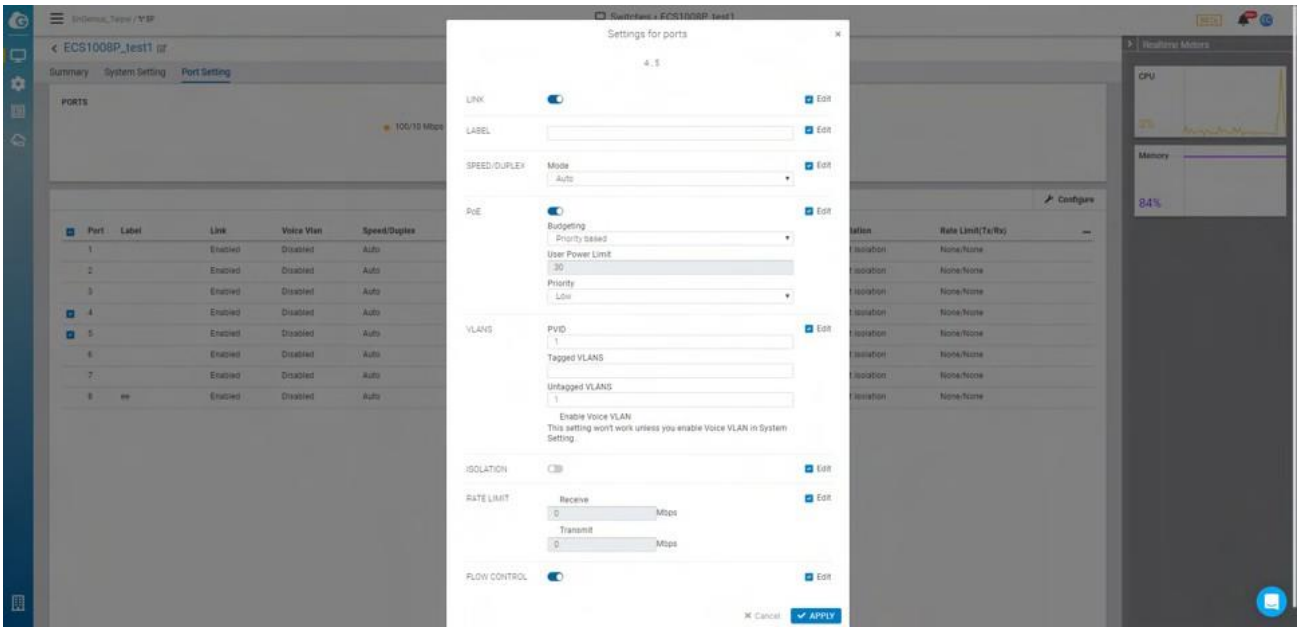
The switch supports a jumbo frame size of up to **9216 bytes**. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important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

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


## Port Settings

Selecting one or more ports and clicking **Configure** will display the following settings:






**Link:** Allows you to enable or disable the connection for this port.

**Label:** Allows you to add a descriptor for this port.

**Speed/Duplex:** Allows you to define the following speed/duplex communication settings for this port:

- Auto: Speed/Duplex will auto-negotiate based on the connected node.
- 1Gbps / Full Duplex
- 100 Mbps / Full Duplex
- 100 Mbps / Half Duplex
- 10 Mbps / Full Duplex
- 10 Mbps / Half Duplex

**Power over Ethernet (PoE):** Allows you to power a connected device through an Ethernet cable using your switch.

**VLANs:** Allows you to group devices to create a partitioned network on the same LAN.

**Isolation**: Allows you to configure a port to transmit traffic only to its connected node.

**Rate Limit**: Allows you to limit the amount of incoming and outgoing traffic in Mbps.

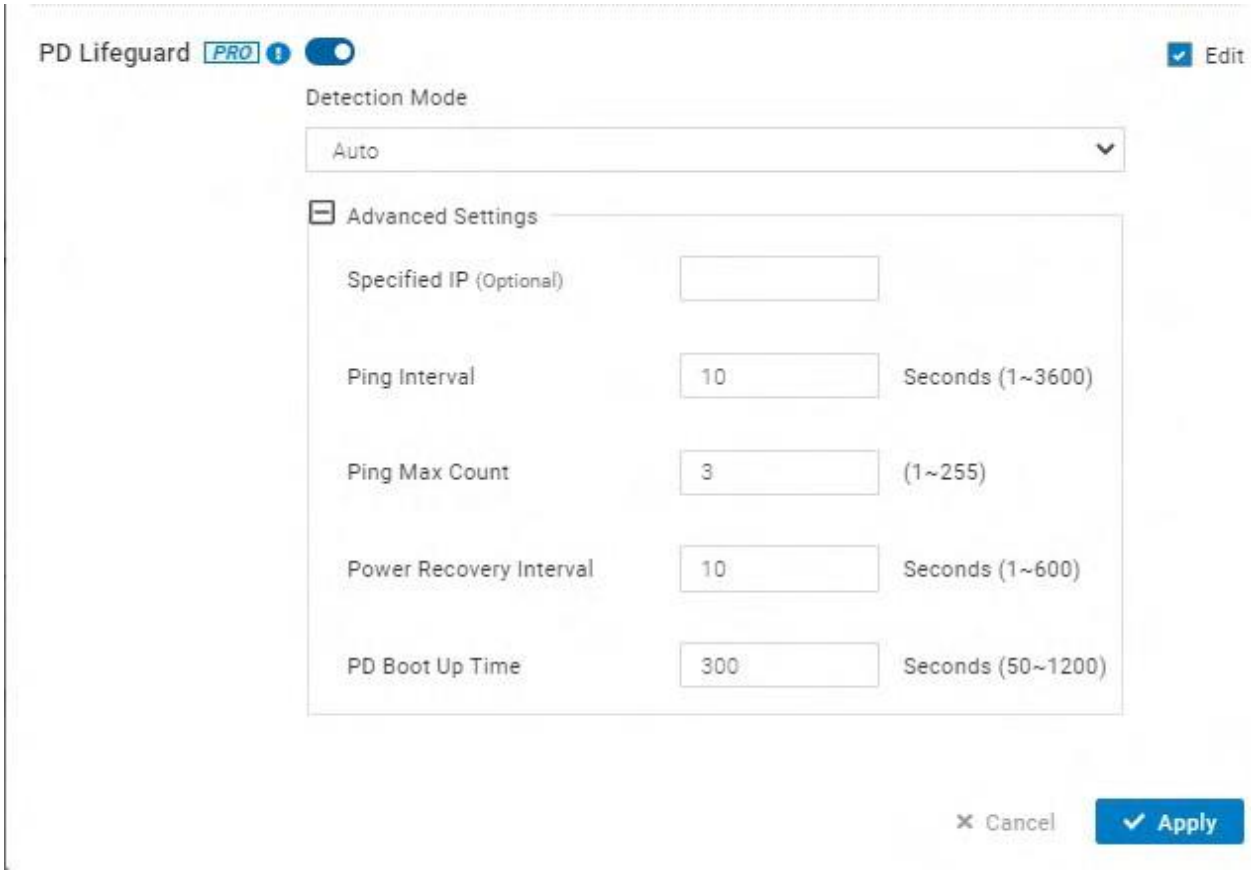
**Flow Control:** Enabling this will have the switch regulate traffic during times of congestion.

**QoS:** If QoS is enabled in **Switch Settings**, you can configure additional settings per port.

- **CoS Value:** All incoming packets that lack a CoS value will use the one set in this dropdown.
- **Trust CoS:** If checked, the switch will queue packets tagged with CoS into their designated queues. If unchecked, all packets will leave the same queue.

**PD lifeguard**: When abnormal events happen on Powered Devices, they might require reboot in order to return to normal operation. PD Lifeguard can be used to judge if the PD is still reachable and turn the unreachable devices off and on.

- **Specified IP**: Setting specified IP on a specific port.
- **Ping Interval:** Setting ping IP interval on a specific port.
- **Ping Max Count**: Setting ping max count on a specific port.
- **Power Recovery Interval:** The waiting time between power off and power on a specific port.
- **PD BootUp Time:** Setting Powered Device boot-up time on a specific port.

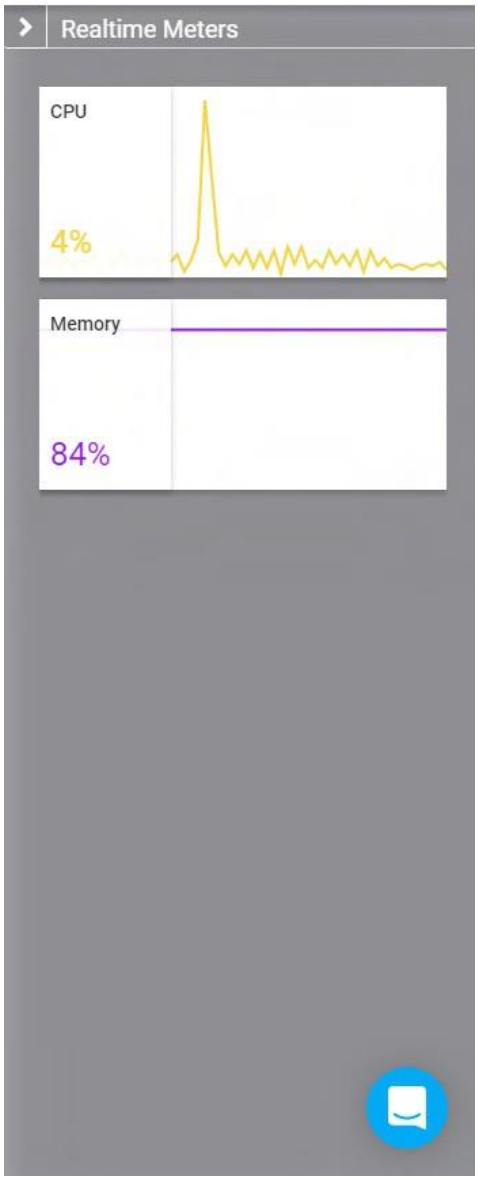


## Realtime Meters

**System Metrics** is primarily for viewing real time statistics . By default there are two types of data:

- **CPU**
- **Memory**

Capturing data over a period of time allows you to see trends useful for determining the overall performance of your switch.




## Override System setting on the Switch Network-wide setting

System setting is followed by Switch setting from the **Configure** > **Switch settings** as default settings. If you want individual AP System settings to be different from the Switch Network- wide setting , you can click below part in the screen to override the setting .

Sen.m / ::i N.:ing,mg / •,;- 8F Network

l;I AP List > Device Diagno sis

ECS1152

Madel Name ECW1 2D
Firmware V1,0. S
Serial NO. SN1 234567 8-90
MAC Addr ess 0A:1B:2C.3D:4F:FE

IP Addn:!ss 192 .1 6B.1 .15□
Sub'1-et M:c1sk 255.255 .2 54.0
Gatewa'.,' 192 16B.1 1
Topology Show

Voice VLAN 0s c1b l !!
J1.1mb0 Fri.im,e5 Enable
IGMP Snooping Enable
STP Enuble
LLDP Enable
QoS Enable

) I!! System Metrics

CPU

45'1o

Memor y

71%

Summary System Sett ing Port Setting Event Log

Spanning Tree Protocol

Prot ocol id Spanning Tree Portocol

Bridg e Priority 68

LLDP

Voice VLAN

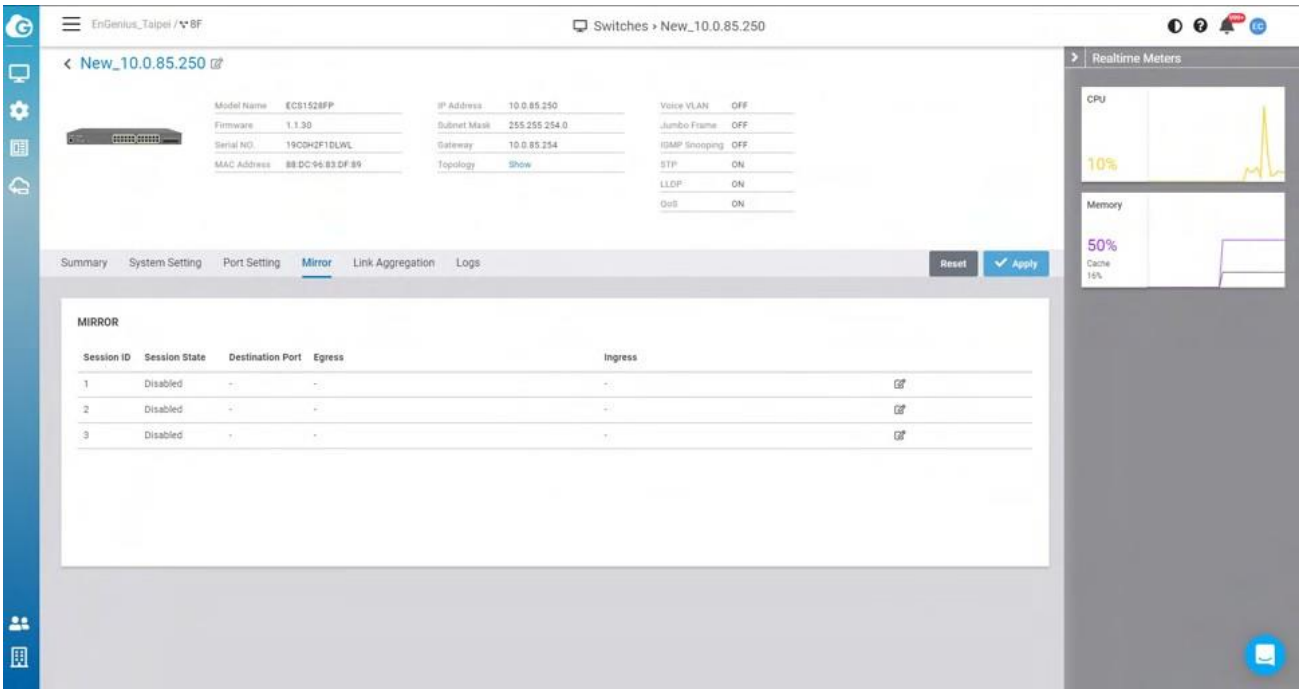
C)

Swit ch Voice VLAN Sf!.lec t a VLAN ..

DoS Prm n !y D (B K)

# Mirror

Port Mirroring allows you to copy packets on one or more ports to a mirroring destination port. You can attach a monitoring device to the mirroring destination port to view details about the packets passing through the copied ports. This is useful for network monitoring and troubleshooting purposes. The feature is available is at **Manage** > **Switch** < **Details** > **Mirror**




The following describe the labels on this screen :

**Session id** : A number identifying the mirror session. Switch supports up to 3 mirror sessions.

**Session State** : Select whether to enable or disable port mirroring.

**Destination Port :** The port which all mirrored data is sent to **.**

**Ingress** : indicates that only data being received will be mirrored.

**Egress** : indicates that only data being sent will be mirrored

## How to configure

1. Click the edit icon towards the right .
2. Enable the **Session state.**
3. Select the **Destination port**
4. Select the **Ingress** and **Egress** port
5. Click **Apply**

---

## Port state

There are four types of port that you configured .

Port was assigned to a destination port .

Port was assigned only data being sent will be mirrored .

Port was assigned only data being received will be mirrored .

Port was assigned both directions of data are being mirrored to the destination port.

# Link Aggregation

Link aggregation groups multiple ports together in parallel to act as a single logical link. Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Member ports in an aggregation group share egress/ingress traffic load, delivering a bandwidth that is multiple of a single physical link. The feature is available is at **Manage** > **Switch** < **Details** > **Link Aggregation**

---

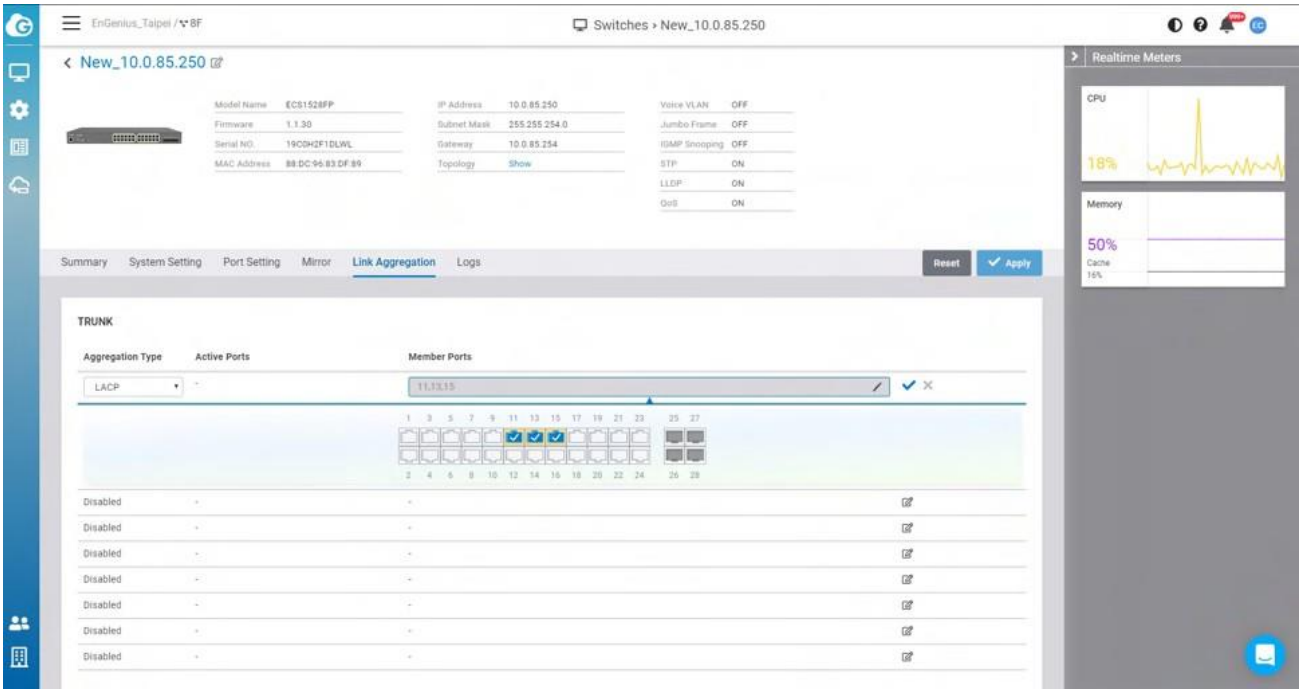
## How to Configure

To Configure trunk , you must select **aggregation type** . Select from the following options:

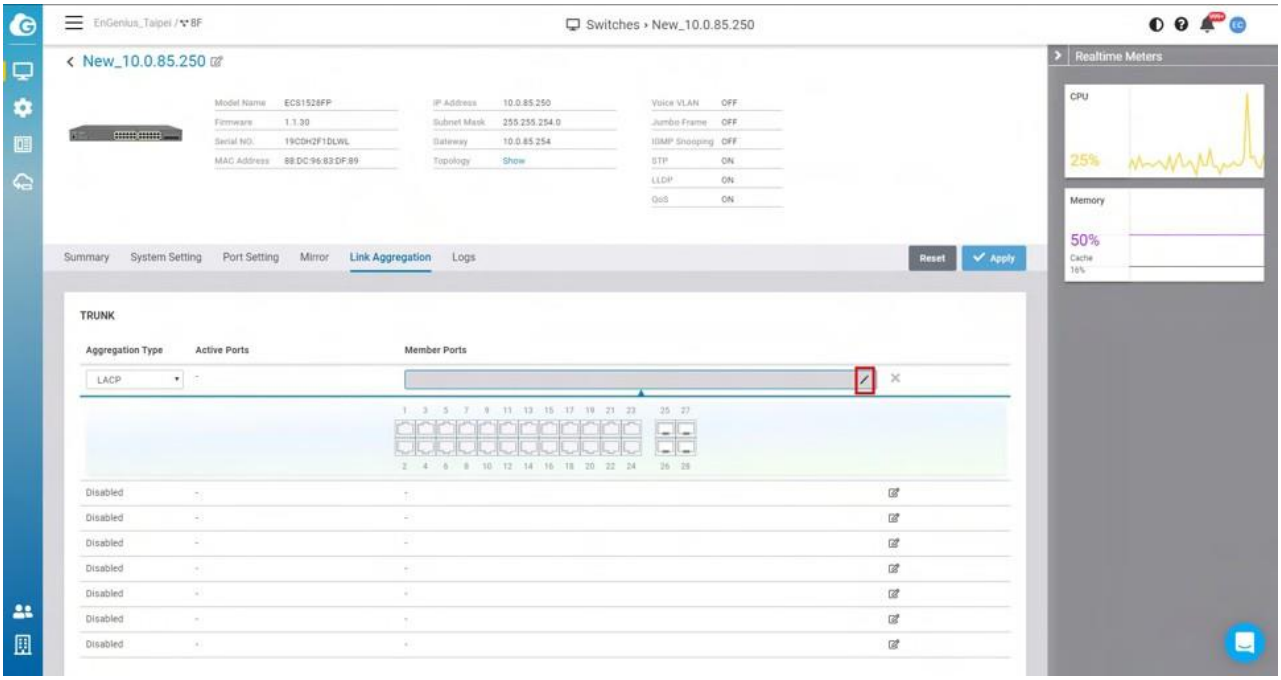
- **LACP**: LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor 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.
- **Static:** Static configuration is used when connecting to a switch that doesn't support LACP.
- **Disable** : Disable the trunk that you configured previously.

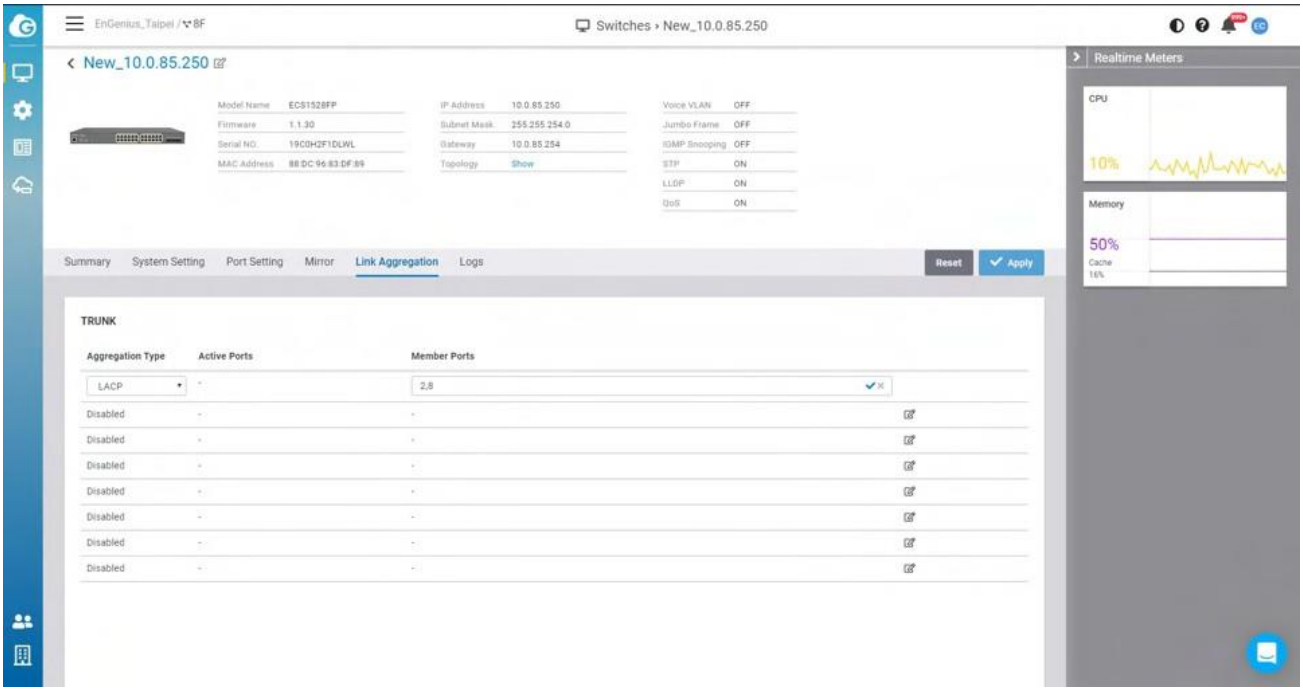
Then select the **Member Ports** to add into the trunk group. There are two ways to select the ports

1. Click on the port  picker to select multiple ports.

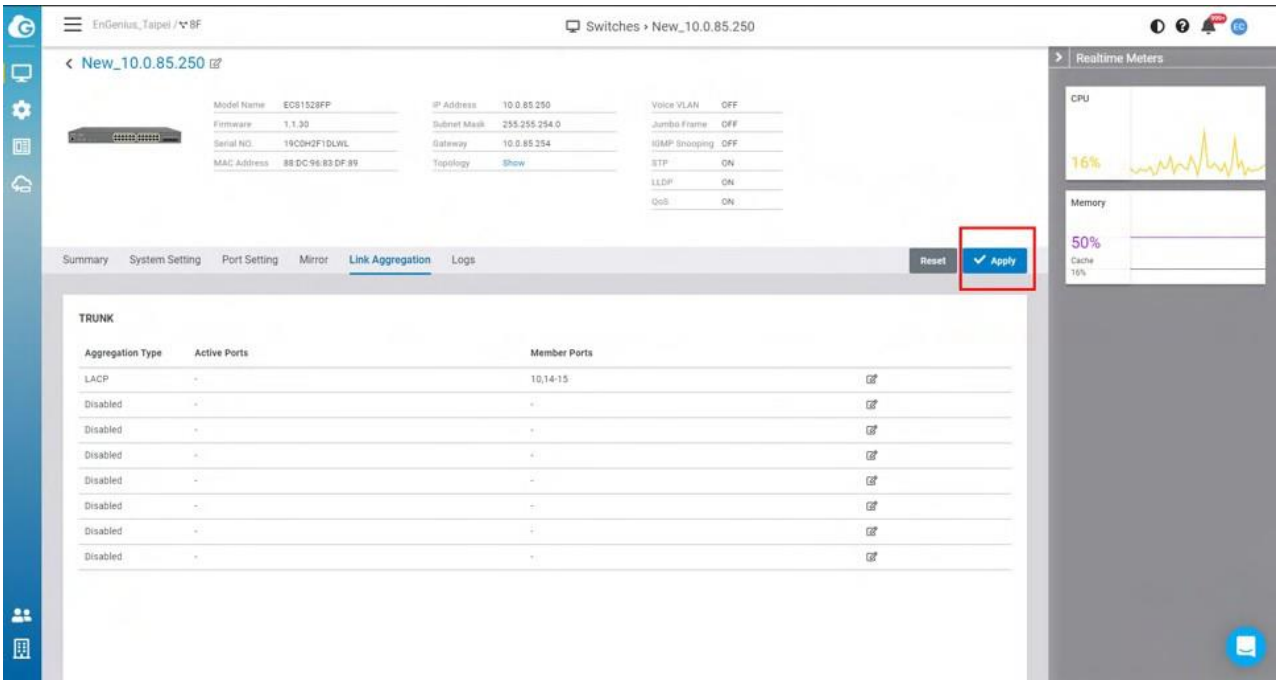



2. Click Pencil icon to input port numbers





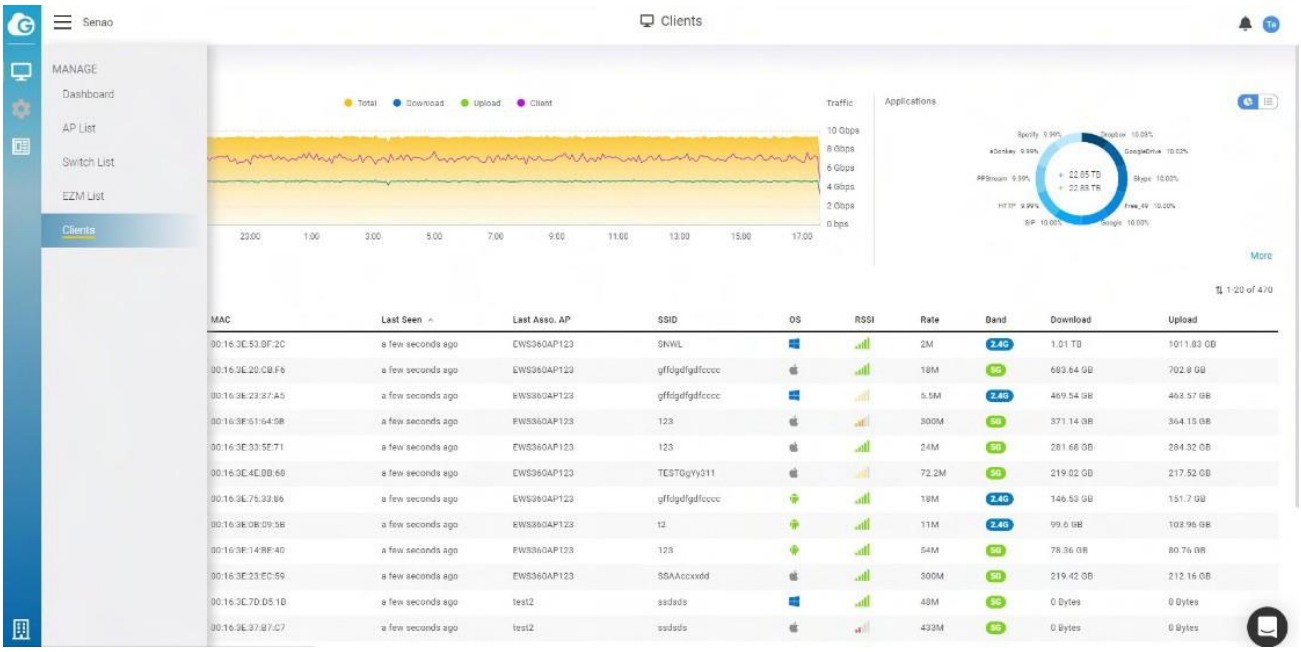

After you complete the trunk settings , remember to click **Apply** to take effect .



# Managing Clients

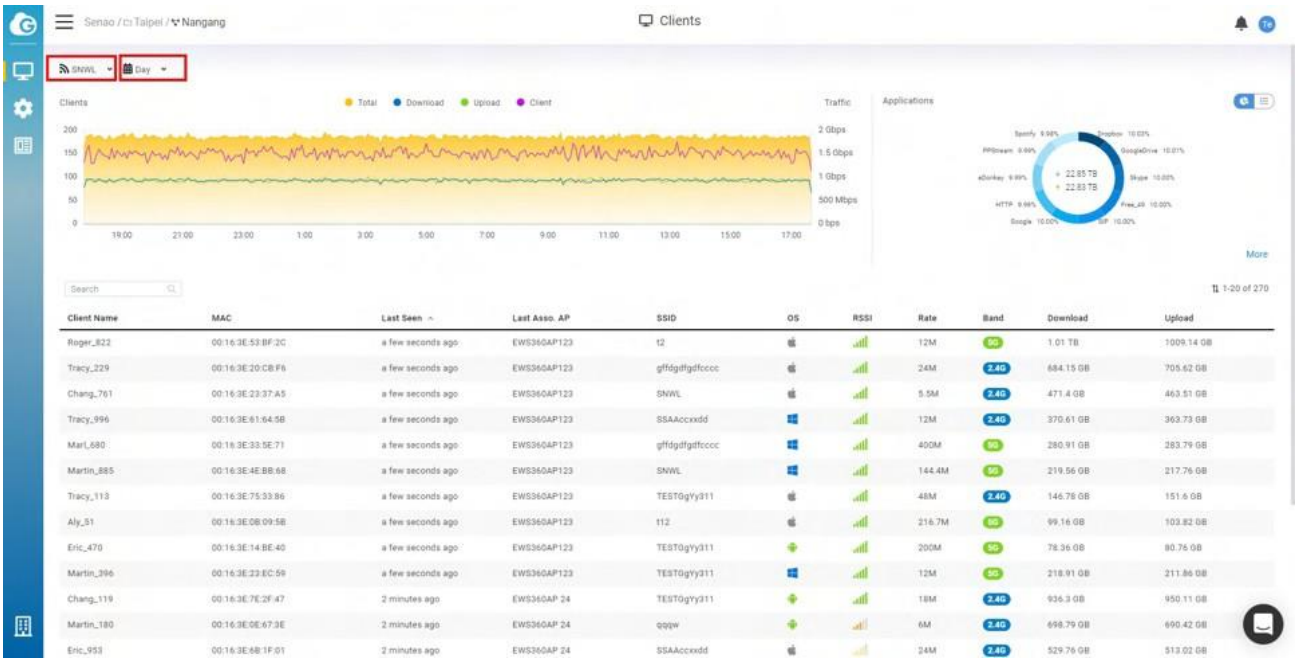
EnGenius Cloud provides management views that collect information about connected clients in your organization/hierarchy view/network.

Click **Manage** -> **Clients** to access this screen and double-click the organization/hierarchy view/network on the tree to change the scope.



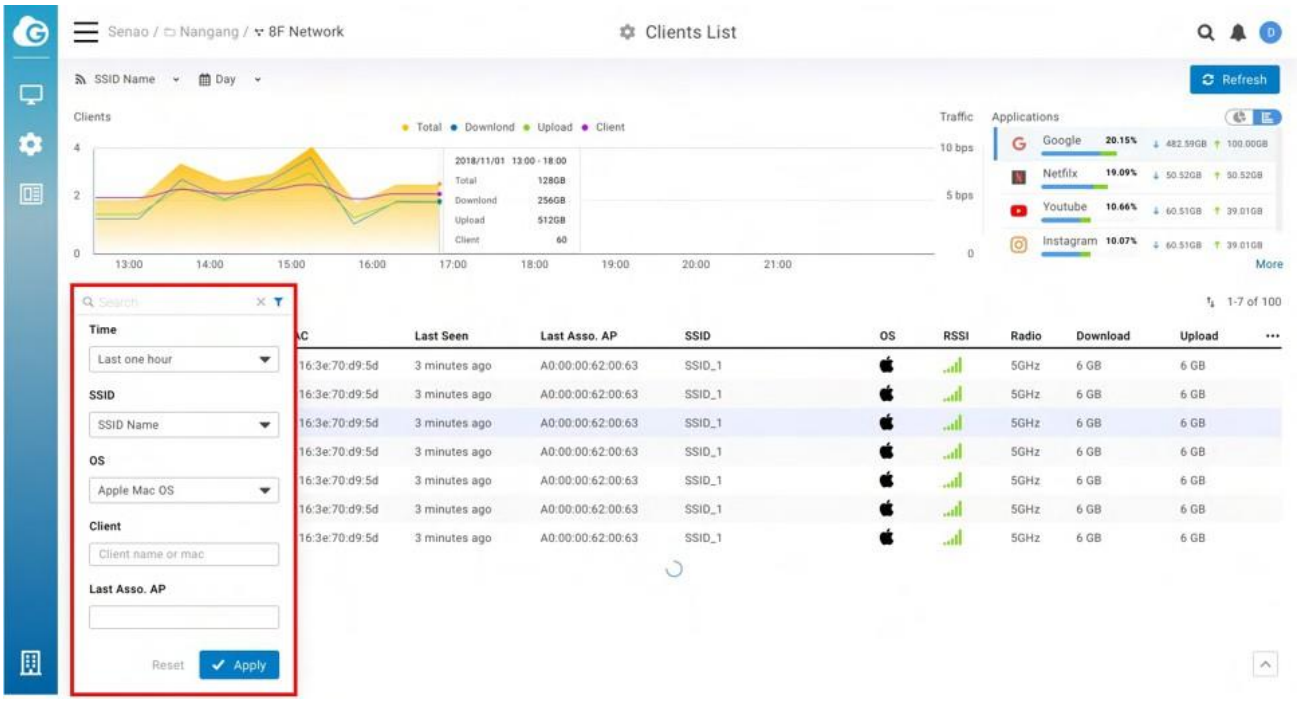

## Filtering the Clients List

The list of clients can be customized based on time intervals, and the chart can be customized based on time intervals and SSIDs. To change these parameters, use the appropriate dropdown menu at the top of the screen.



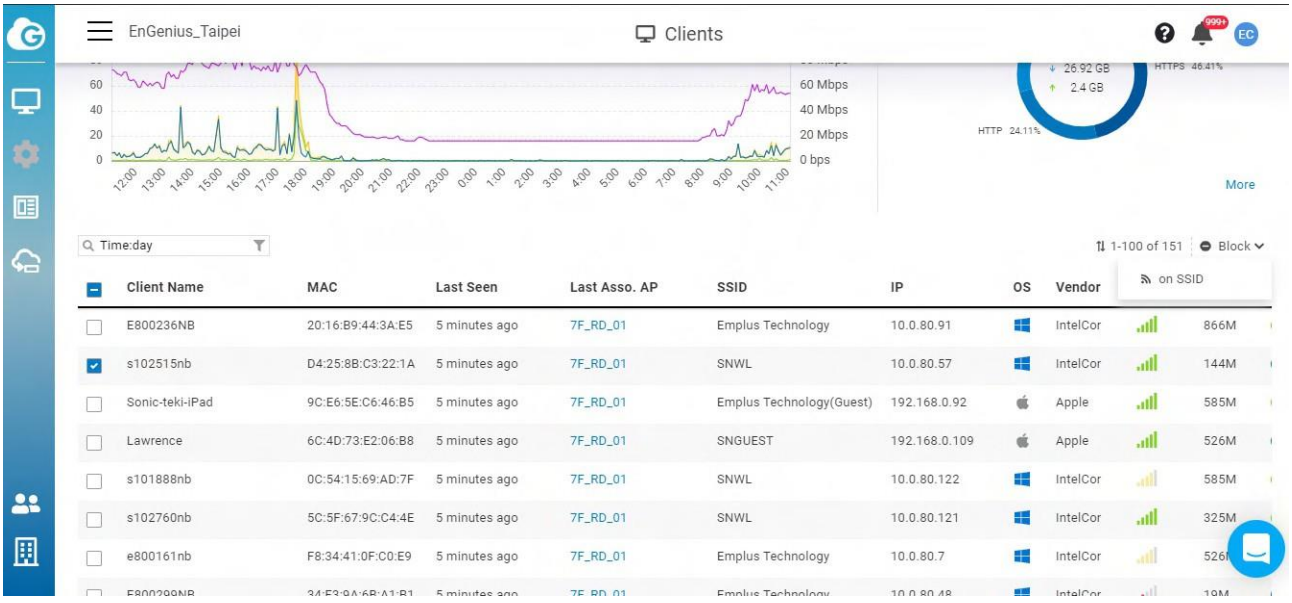

## Searching for Clients

You can search for a client in the current client list by using the search. You can search by any parameter included in the search options, and it will attempt to match your query across all fields. You can also specify multiple parameters by clicking on the icon in the search box, as seen below:

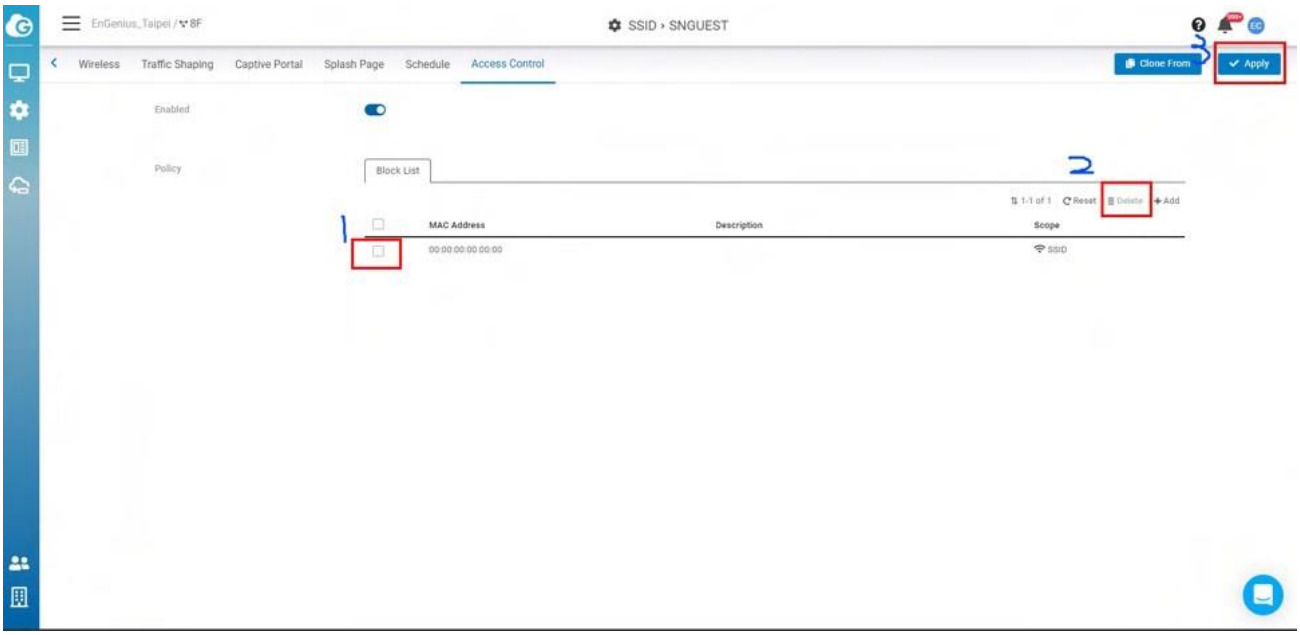



## Block Clients

This allows you to block clients on the current SSID that clients connected .

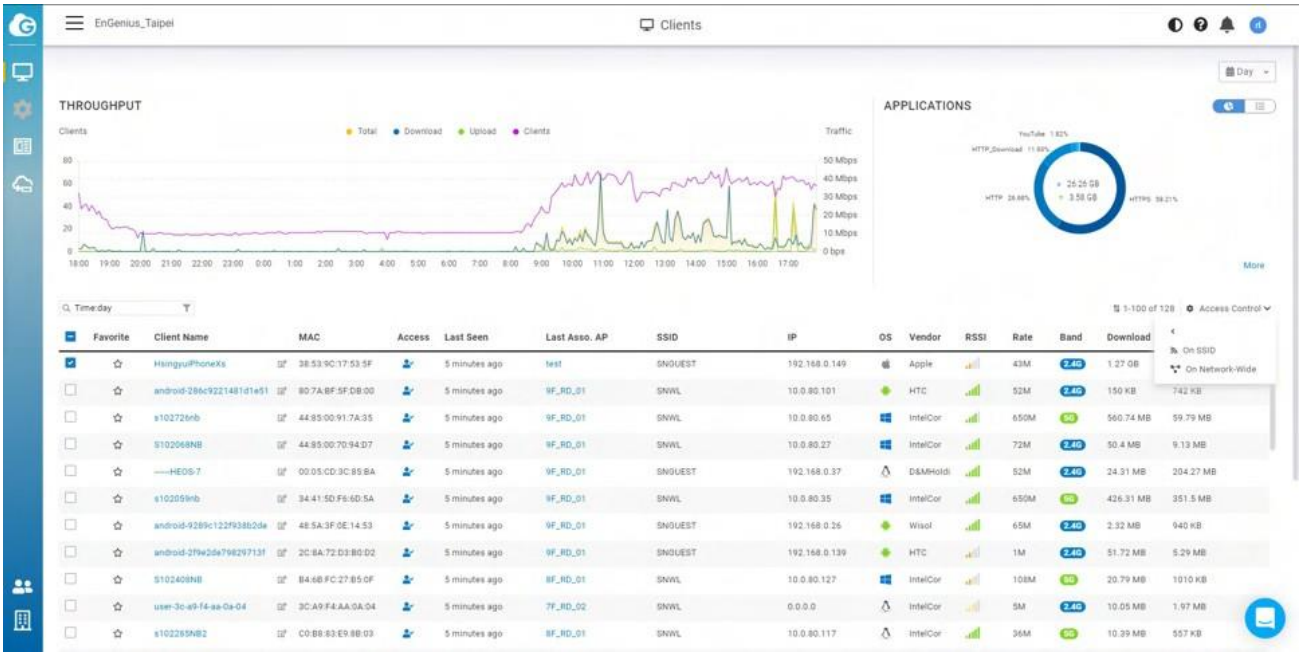



Once you want to unblock clients , please go to **Configure** > **SSID** > **Access control** to delete the Mac Address from the Block list .




## VIP Clients

This allows you to make clients as VIP on the current SSID or on Network wide that clients connected .




Once you want to delete clients from the VIP list , please go to **Configure** > **Access control** to delete the Mac Address from the VIP list .

# Client Timeline

The Client Timeline is a great feature that aggregates and analyzes activities of a specific wireless client to provide an intuitive and historical view. With Client Timeline, user can easily know how clients associate, authenticate, and roam among Access Points. It is extremely useful when you need to debug or trace your wireless network. The feature is available at **Manage** > **Client** > **Client name**.

---

## Client States

The EnGenius Cloud AI system categorizes client activities into five different states:


Client was connecting to an AP.

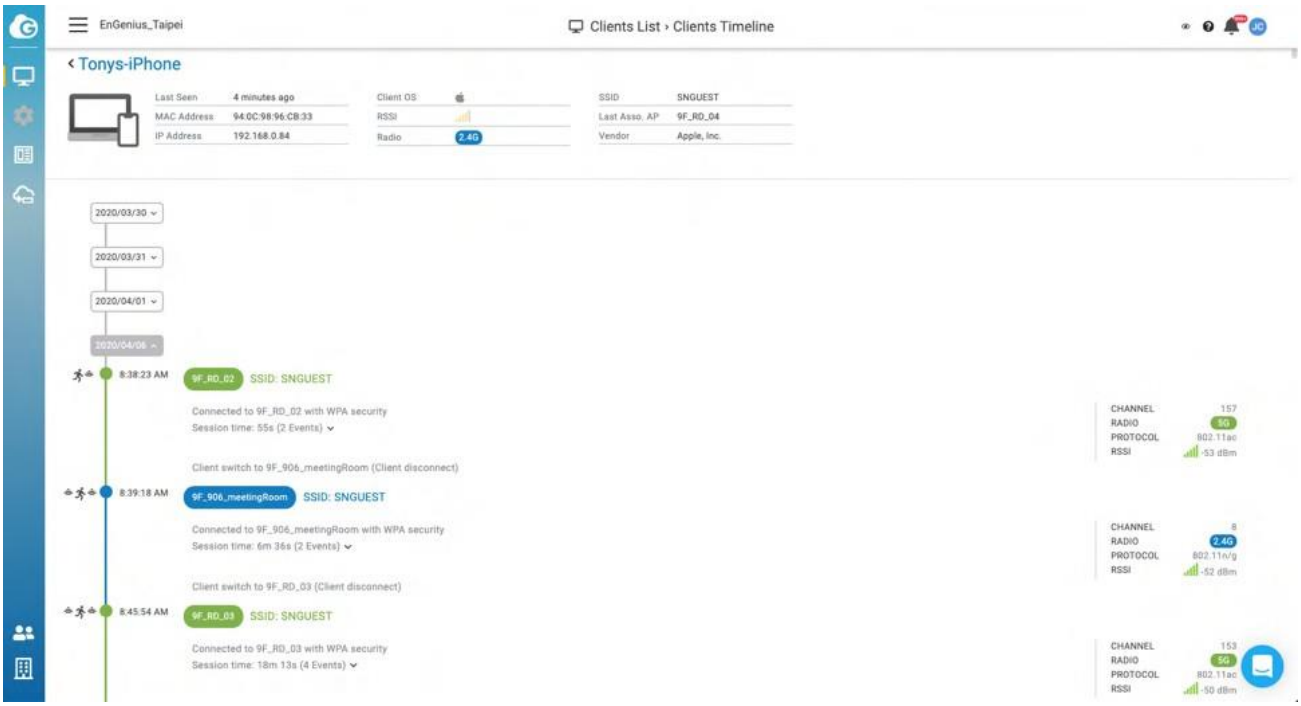

Client was roaming and connecting to another AP.


Client changed to associate with different radio or SSID of the same AP.


Client failed to authenticate with an SSID.


Client was denied because of it is in block list.

The states are displayed at the left hand side of timeline. User can easily see how a client transited its states among APs.




## Radio Color Conventions

The drawing and content of client timeline follows the color conventions as below:

- Green: represent a 5G session.
- Blue: represent a 2.4G session.

> In the right hand side of each session, the system shows the channel, band, protocol, and signal strength of client detected at the beginning of that session.

## Transition Details

The communication between wireless client and AP could be very complicated. Different clients with different wifi chips and wireless drivers can behave very differently while communicating with the same AP. The intelligent engine behind Client Timeline is capable

of analyzing communication packets effectively and performs clean and human readable transition details for the user.

User can click on the event summary inside a connection session to expand the sequence of transition details:

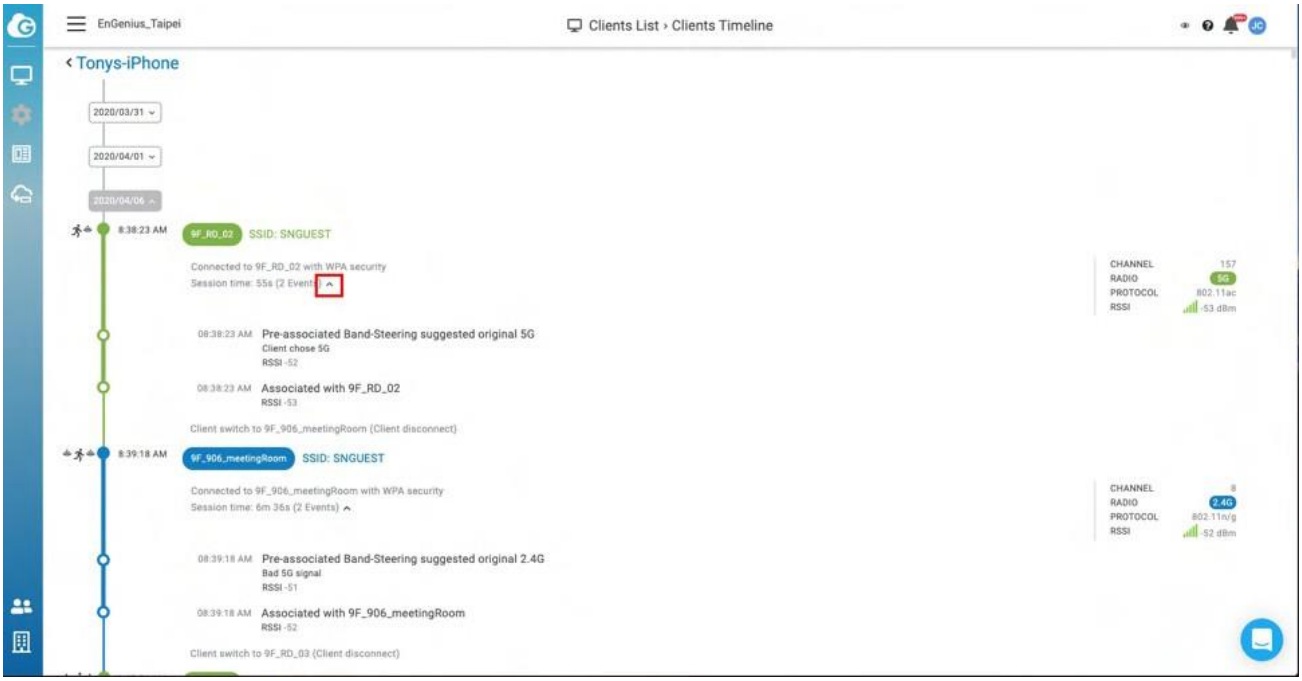



Table below displays client leave patterns when client leaves each connection session.

| Leaving reason | Description |
| --- | --- |
| **Incorrect password** | Client entered the incorrect password for WPA or wrong authentication information for EAP |
| **Client switch to {device_name}/{radio}** | When the RSSI signal is not good enough, the client did not disassociated from the AP and it connected to new AP directly with regular authentication procedure. |
| **Roam out to {device_name}** | When the RSSI signal is not good enough. The client disconnected from the original AP and connected to the new AP by 802.11r fast roaming protocol. |
| **Steer to {radio}** | The client disconnected from the AP due to band steering protocol. It received the 802.11v trigger and connected to suggested band accordingly. |

| | |
|---|---|
| **Disconnected by {device_name}** | The client was disconnected by the AP due to bad RSSI signal (fast handover). |
| **AP disconnect** | The client was disconnected by the AP due to unknown reason. |
| **Kicked by Cloud** | The client was kicked by the cloud administrator. |
| **Denied by ACL** | The connection was refused by AP because the client was on the blocked list under access control. |
| **Exceed client limit** | The connection was refused because the client count has exceeded the maximum 2.4G/5G client limit. |
| **Client inactive** | The client was inactive because it was on power saving mode or far away from the AP. |
| **Client disconnect** | The client disconnected because the user disabled the Wi-Fi or choose to connect to other AP. |
| **Disconnected due to SSID configuration change** | The clients was disconnected due to SSID configuration change. Some configuration change took effect only after recycled (down&up) the NIC (network interface controller). When the NIC is down, all connection are disconnected. |

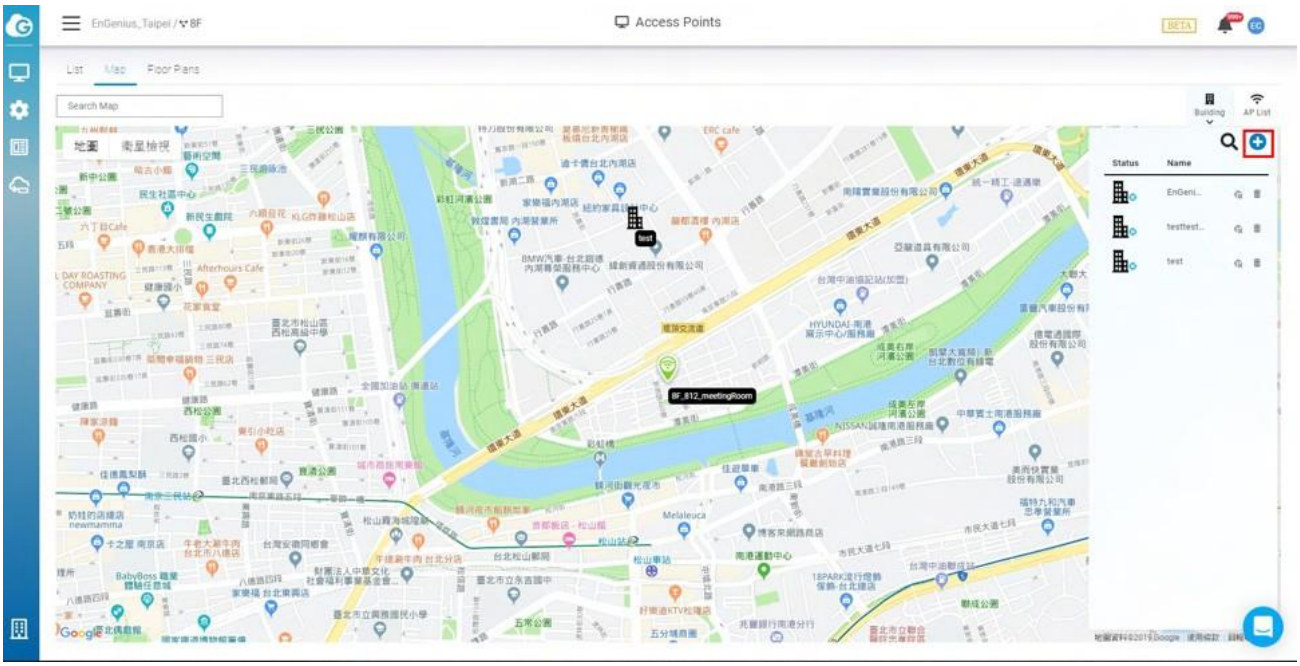
# Device Map Location

This screen allows you to locate a device on the world map to show the relationship between the space and EnGenius Devices. Maps provide a visualization for buildings and access points.

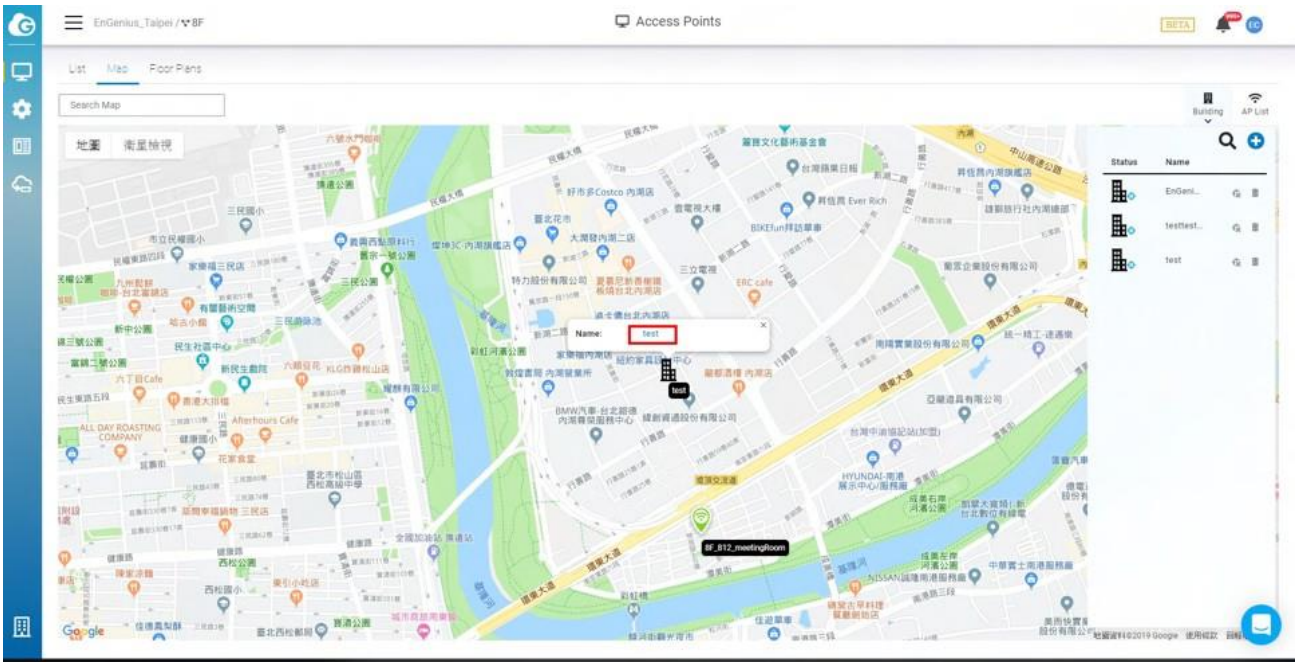
---

## Create Buildings

A **building** means a group of floor plans. You can create a new building with the + button.

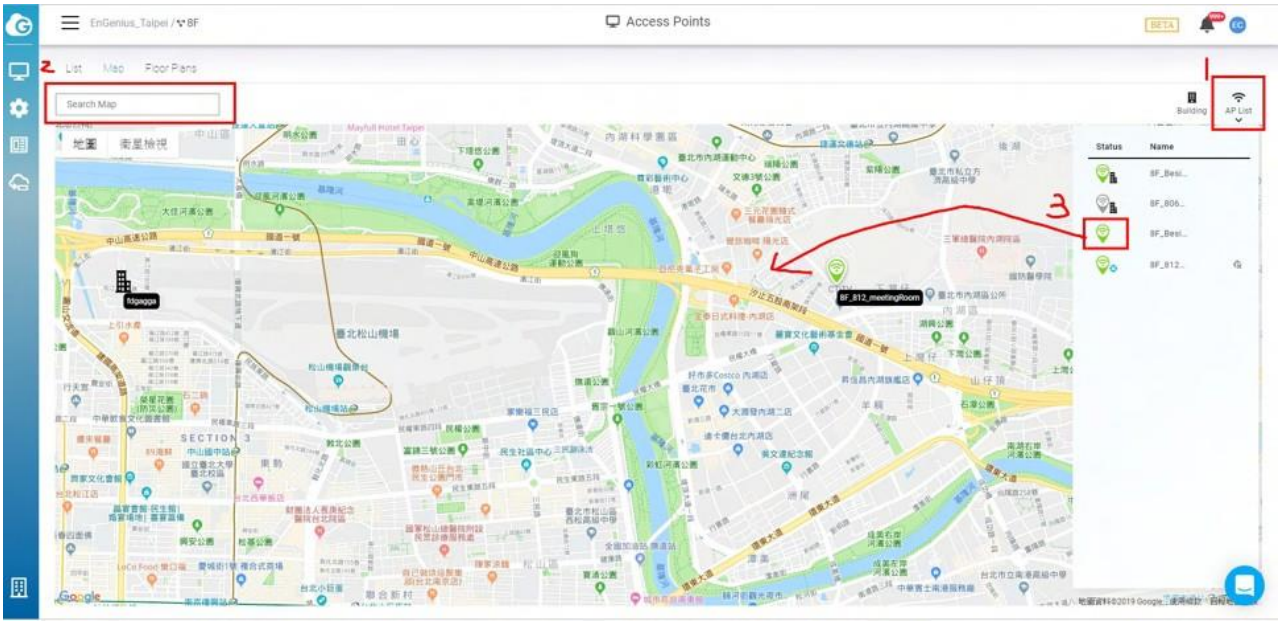



After you create a building, you can drag it to the map. Single-click on the building icon and a hyperlink will appear to allow you to edit floor plans.




## How to Place Access Points or Buildings on the Map

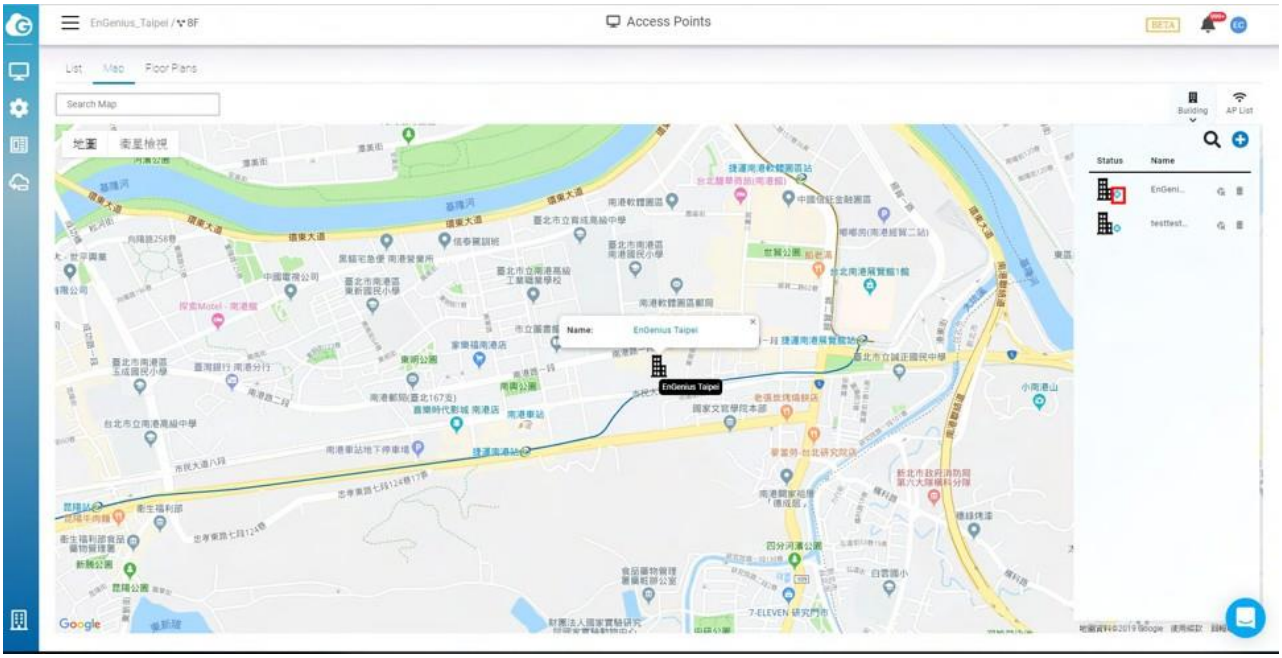
1. Click access point list or buildings list.
2. Enter the street address in the address field.
3. Drag the access point/building onto the map.

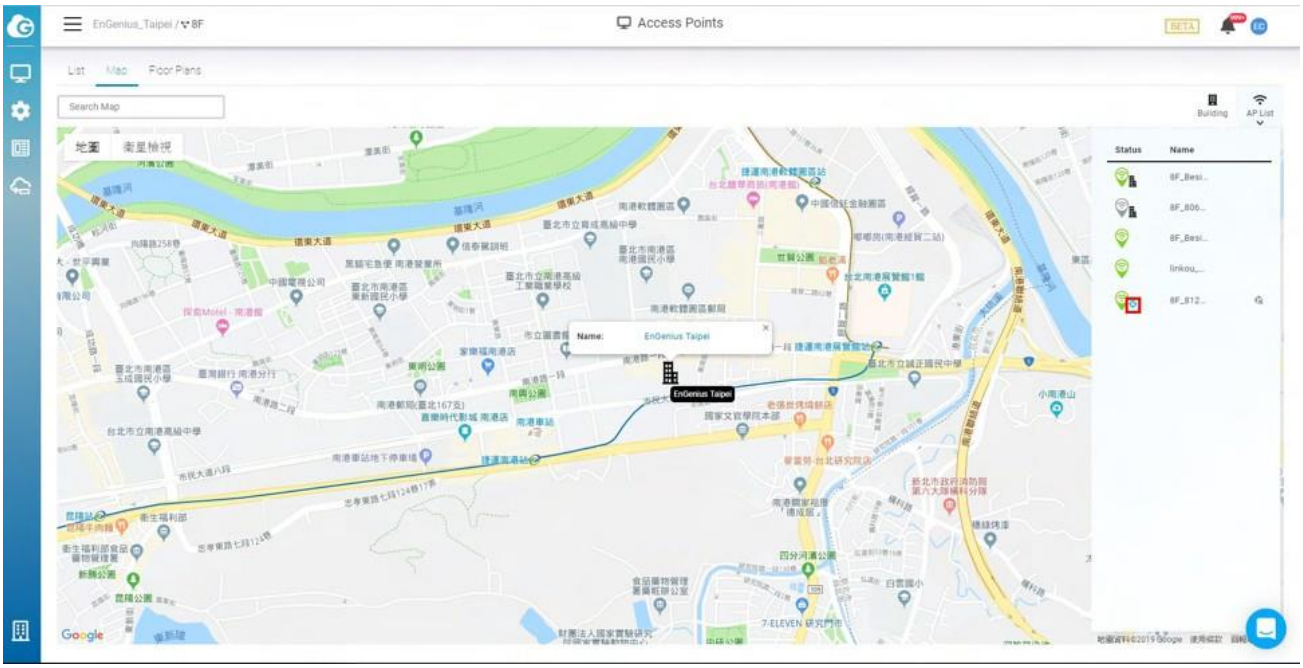


## Navigation

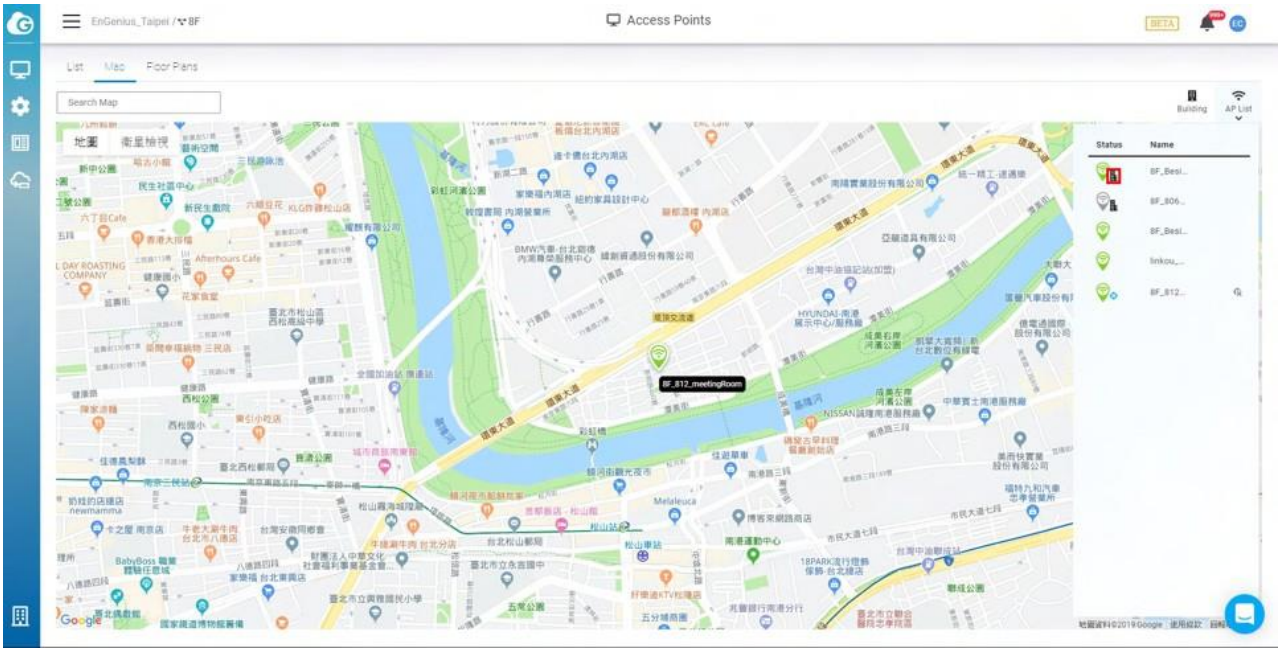
There are a number of ways to navigate through the map display.

**Single Click**: If the user single-clicks on the focus icon on the access point or building lists, it will auto-locate the same item in the map.






**Double Click**: If the user double-clicks on the building icon in the access point list, the UI will auto-navigate to the floor plans of that building.



# Floor Plans

Floor plans allow you to simulate the heatmap. This article will discuss how to upload custom floor plans, pin them on the map, and place devices within these floor plans.

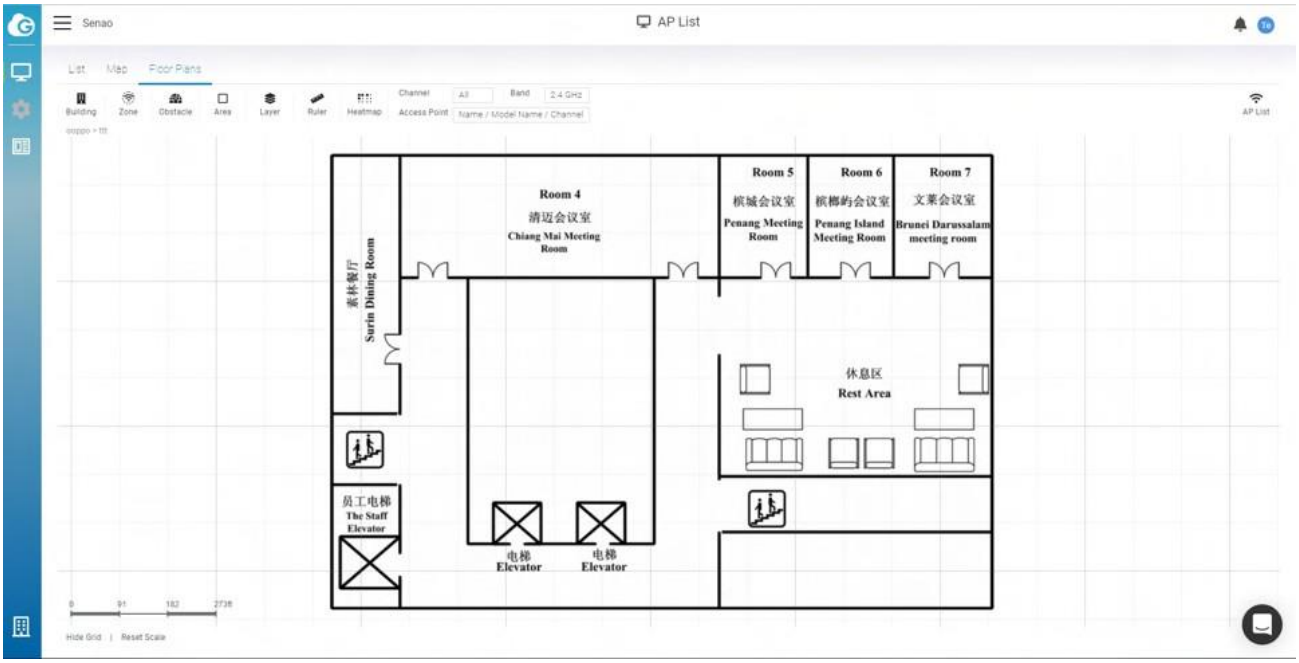
---

## Uploading Floor Plans

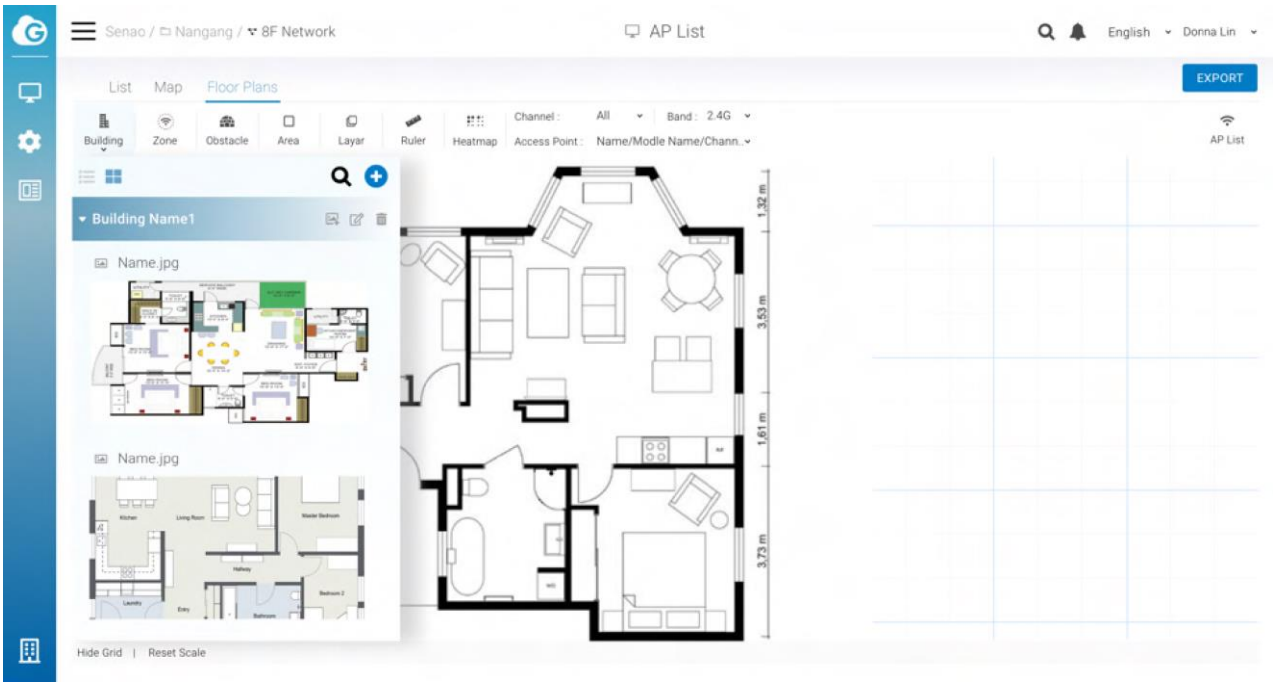
Before uploading floor plans, a building must be created to contain them (see **Managing Devices > Device Map Location** in the user manual).

To upload a custom floor plan/map:

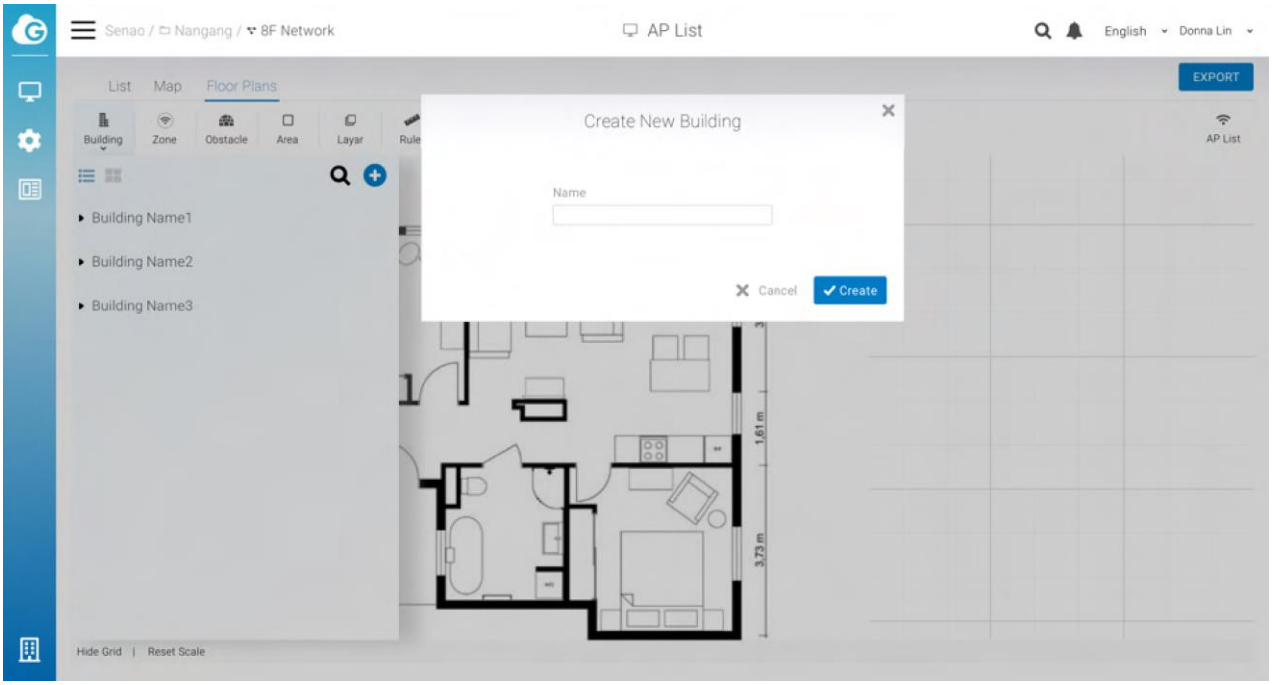
1. Navigate to **Manage > Map & Floor plans**.



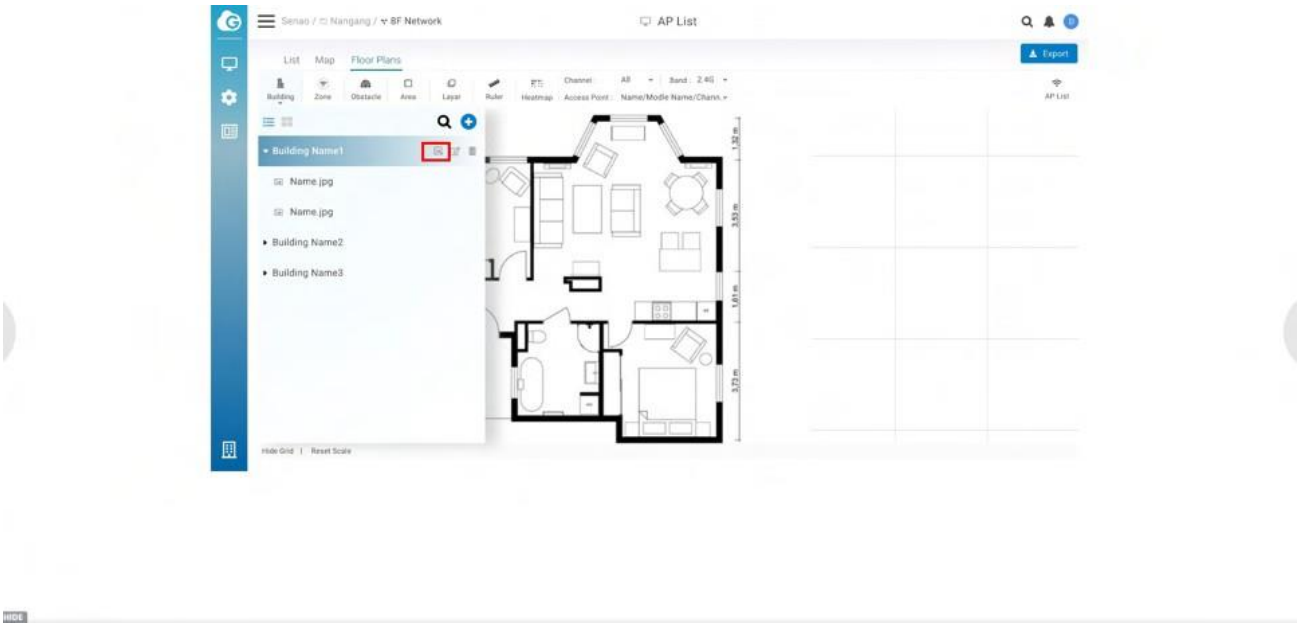

2. Click **Building** and click **Add**.



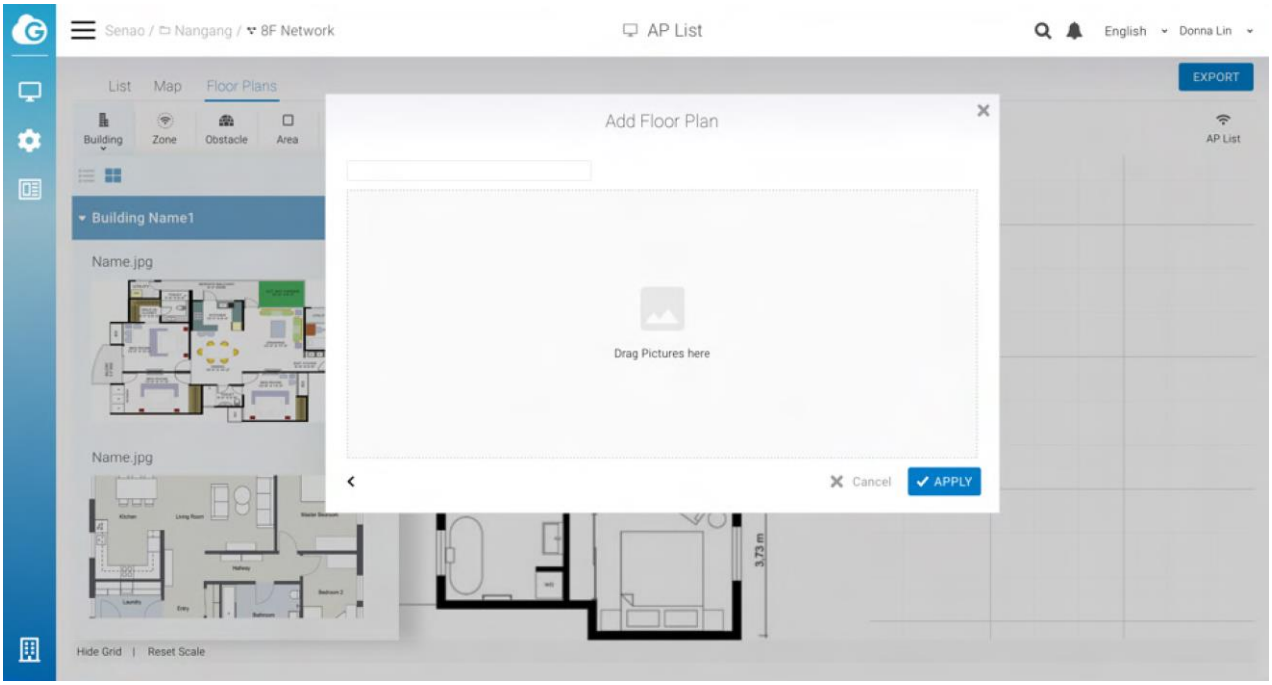

3. Enter a **name** and then click **Create**.




4. Find the building you have just created in the building list and click the picture icon.




5. Enter a **name** and upload the floor plan, then click **Apply**.

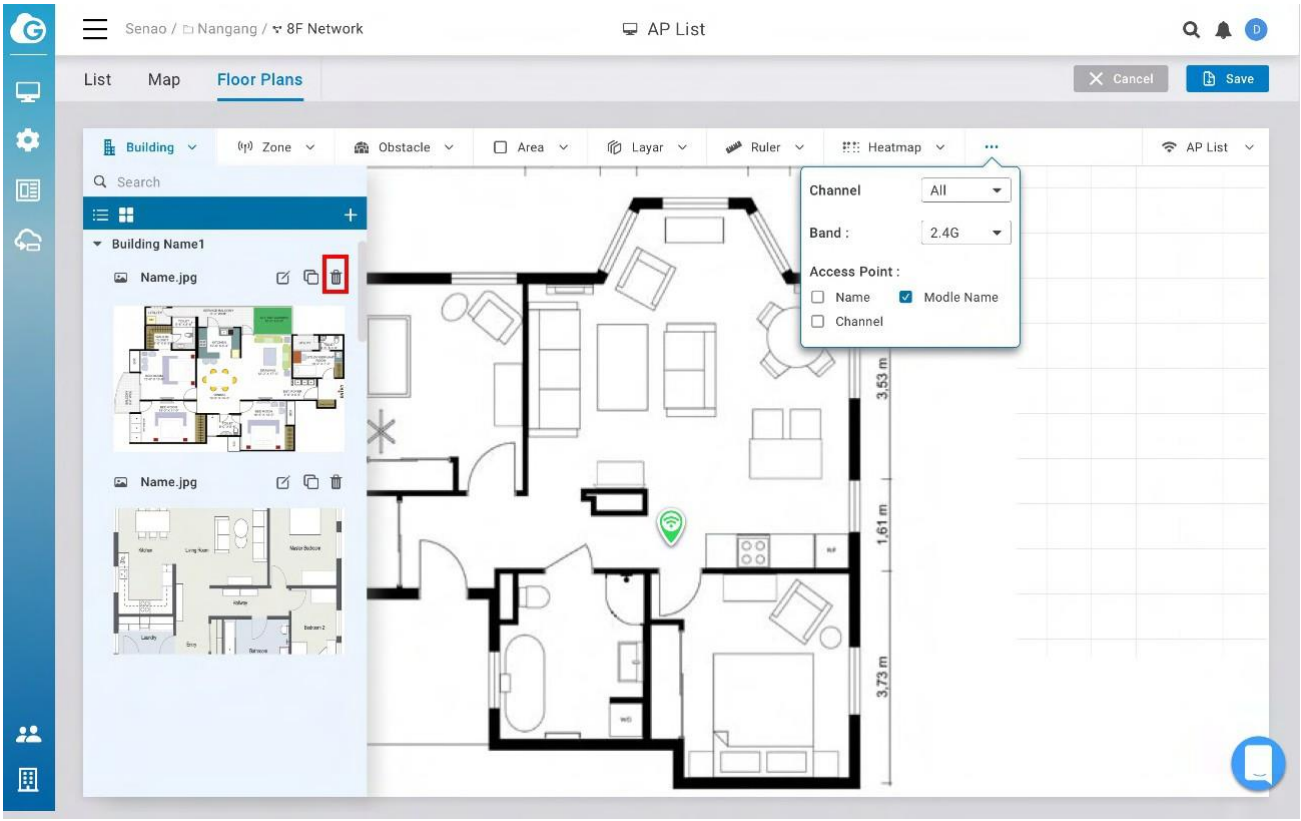



## Deleting a Floor Plan

If you no longer use a floor plan that you previously imported, you can delete it.

Follow these steps to delete a floor plan:

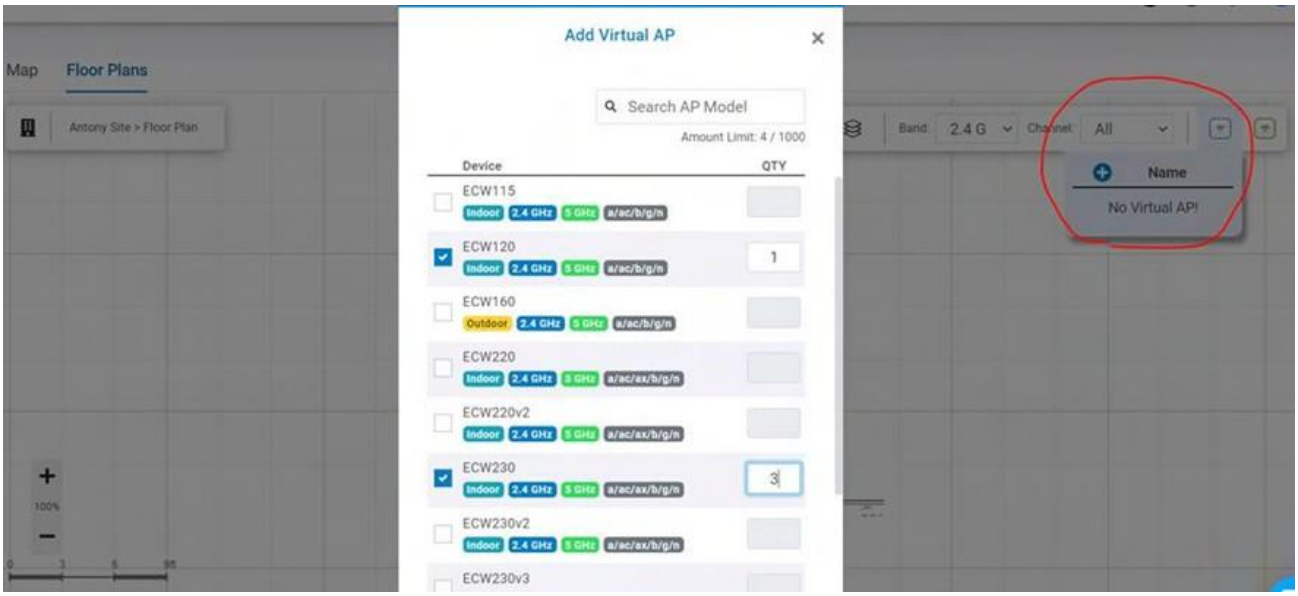
1. Find the building you created in the building list.
2. When the floor plan appears, hover over it and click **Delete**.



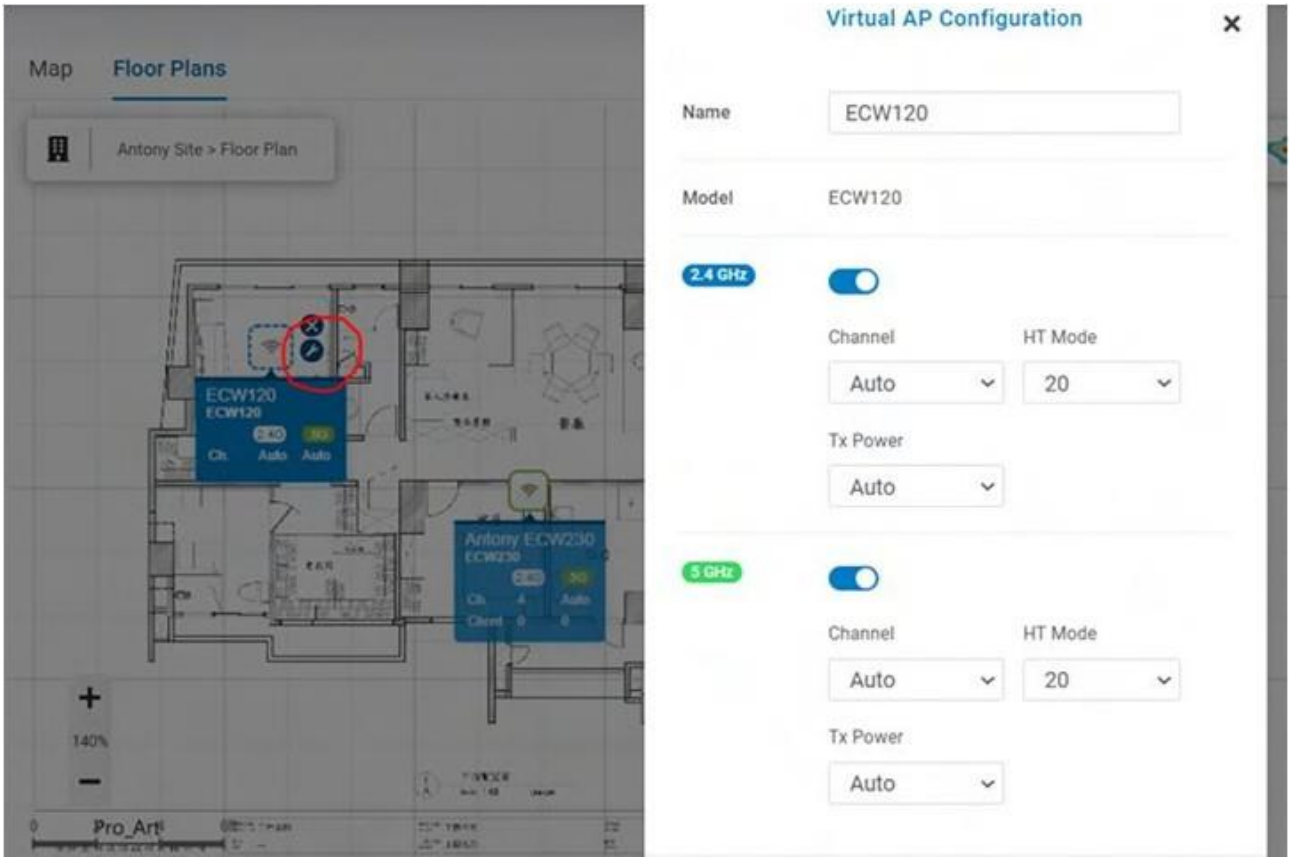

## Virtual AP

Virtual AP" is now available for users to add virtual AP together with "physical AP", so users can simulate the heat map if he adds more AP to increase the coverage

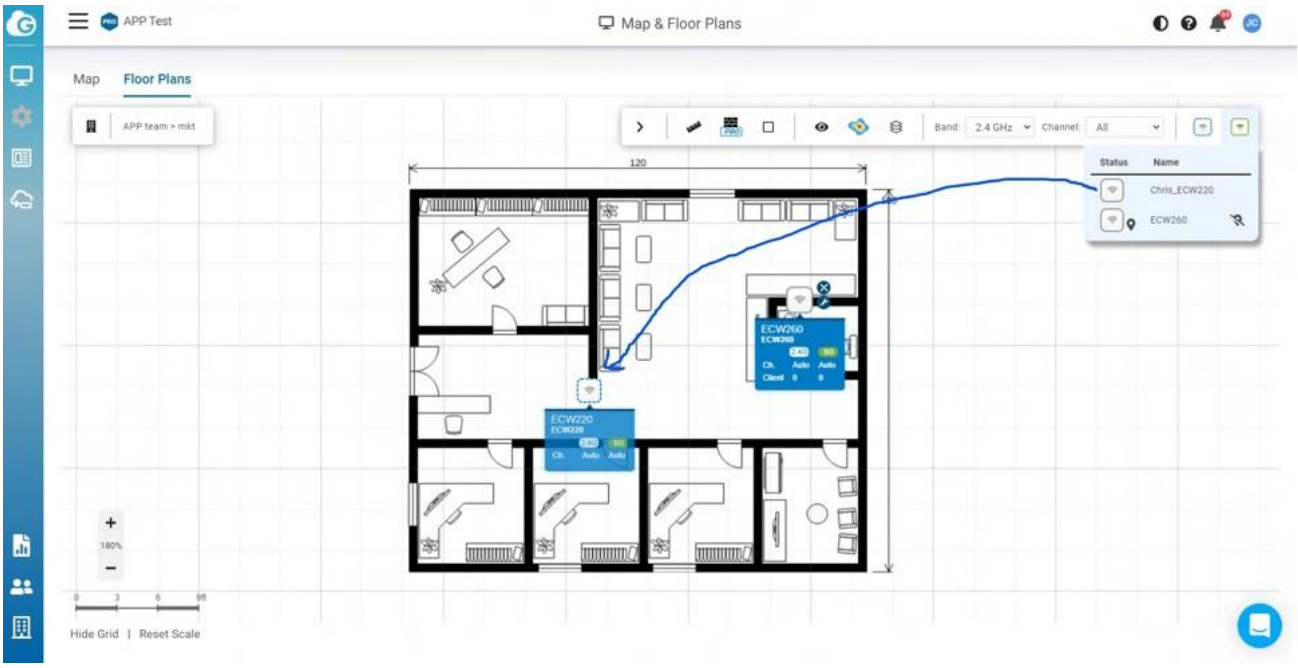
Add Virtual AP and choose units of models to add




The Tool icon for users to modify the tx power and channel for heat map simulation




Drag the physical AP to Virtual AP (model needs to be the same) then physical AP could use the Virtual AP configuration.




## Polyline in Obstacle

When drawing the walls, users used to draw the line one by one by click “start” and “end” for straight lines, now with the “**Polyline**” option available, users can simply click on the turning point to draw lines quicker.