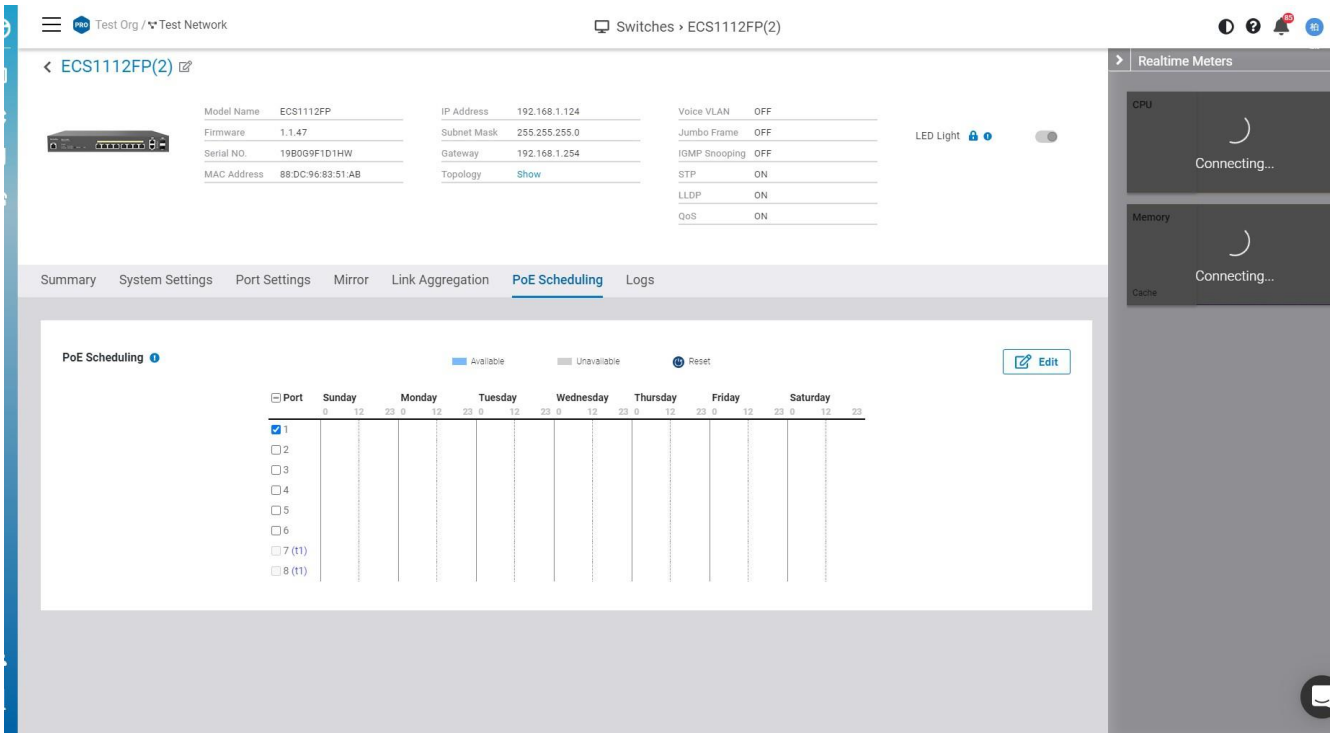
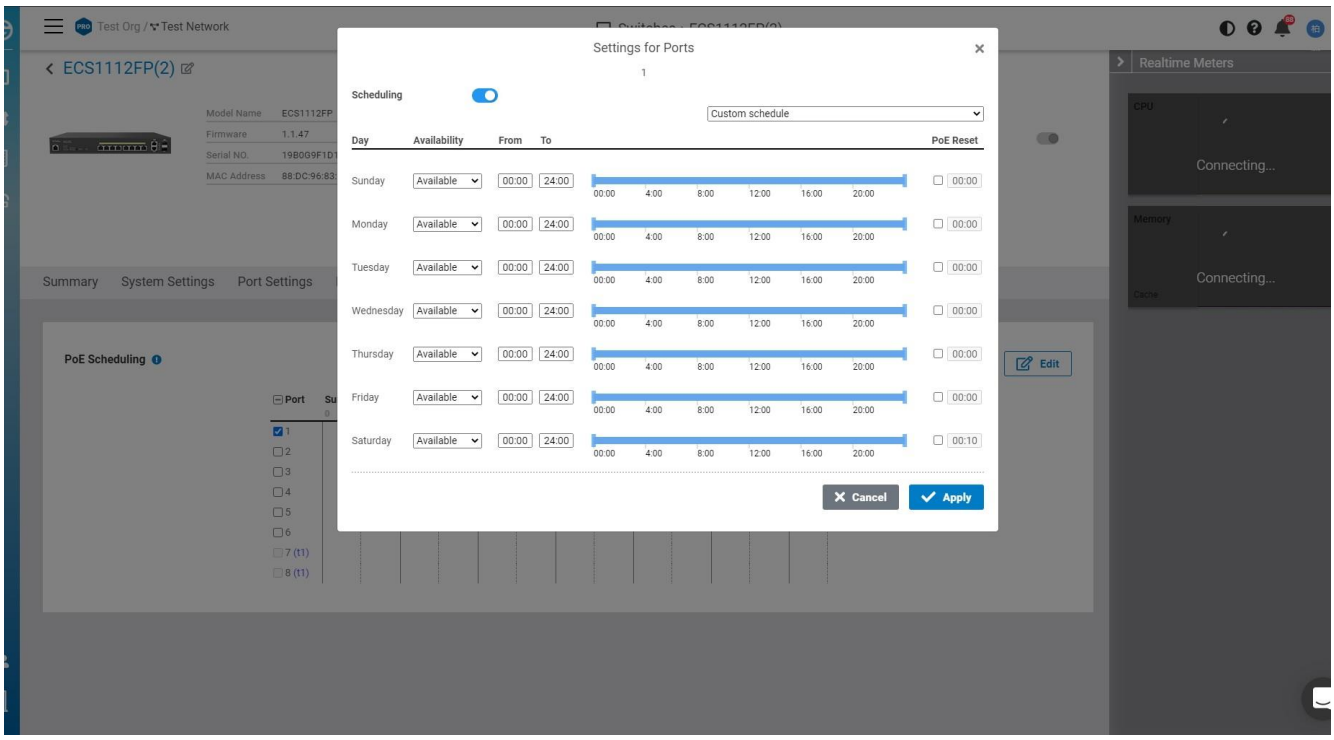
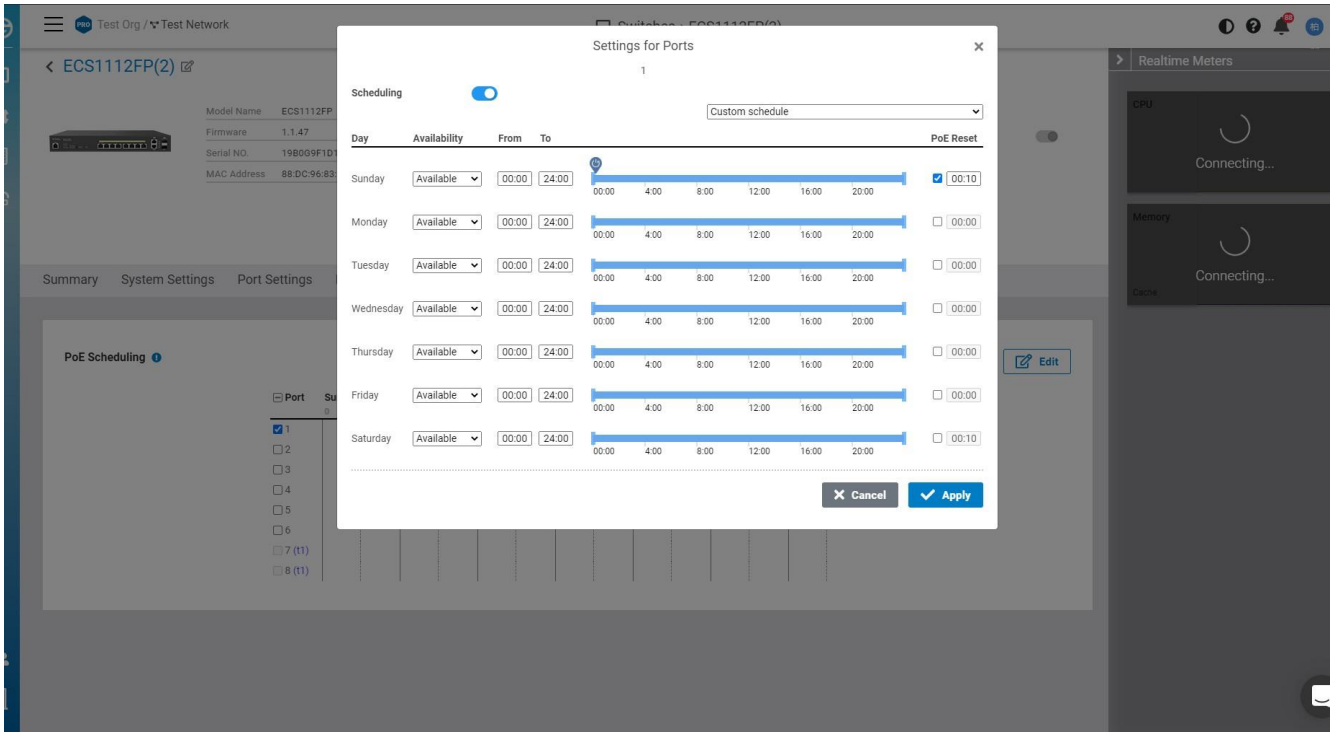
Edit PoE Scheduling

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.

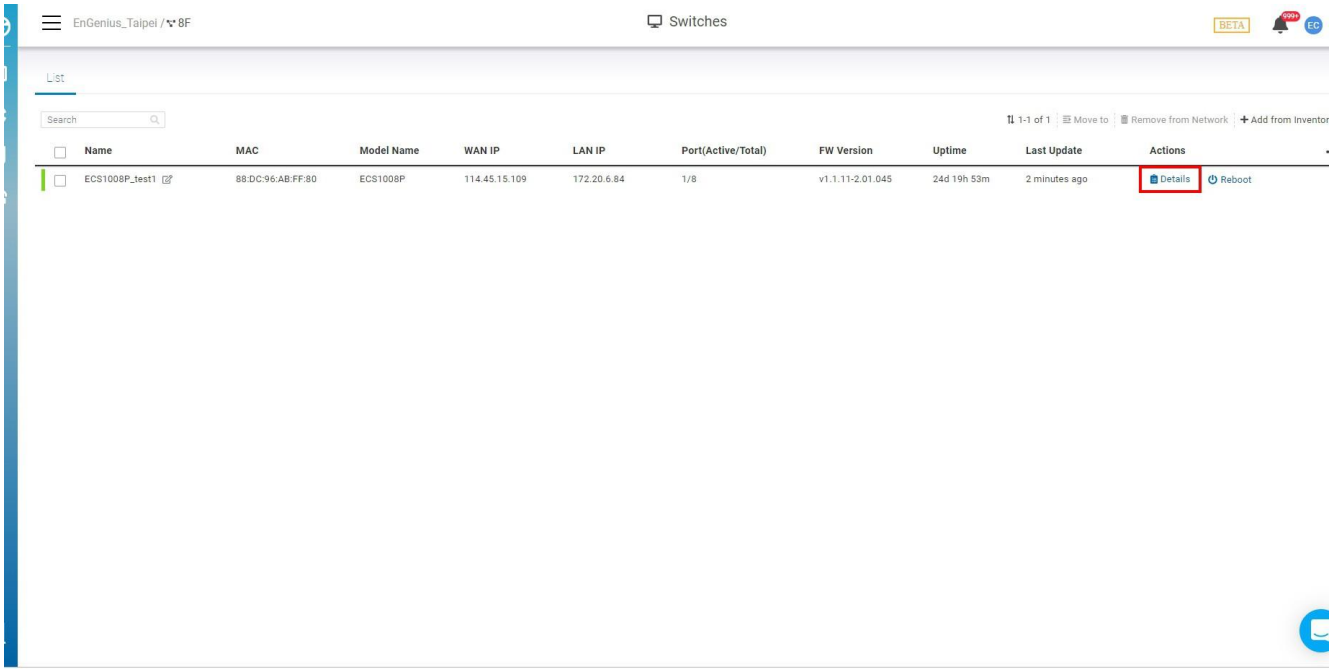




4. Click Apply.

Getting Switch Analytics

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

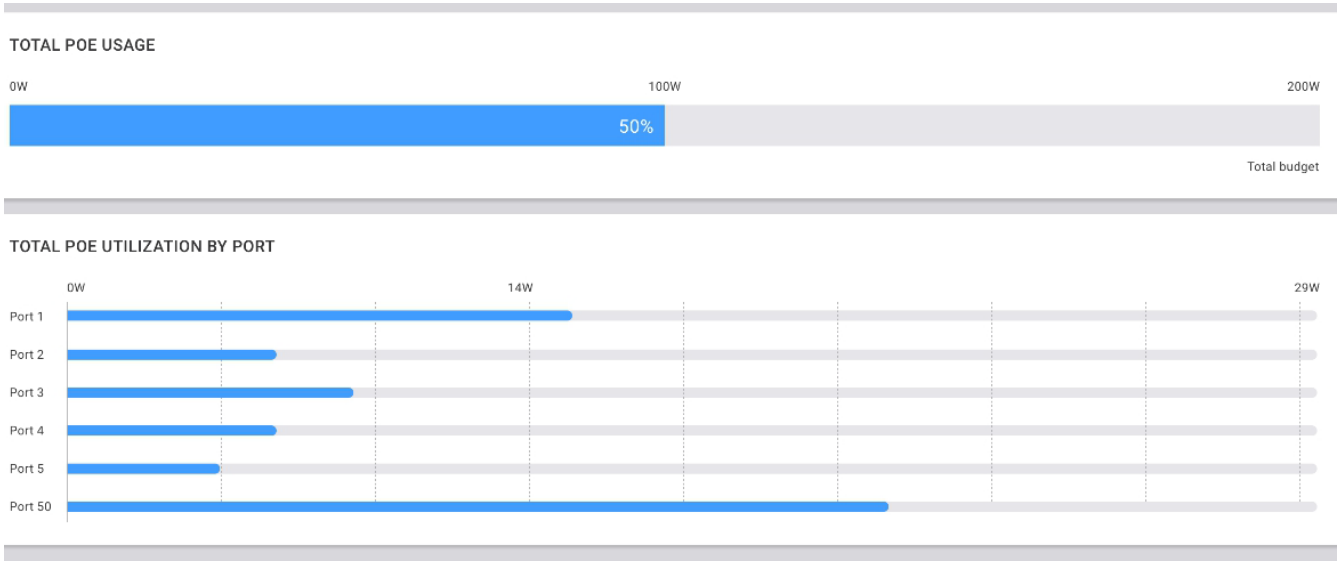


PoE reset from the Switch Panel :

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.

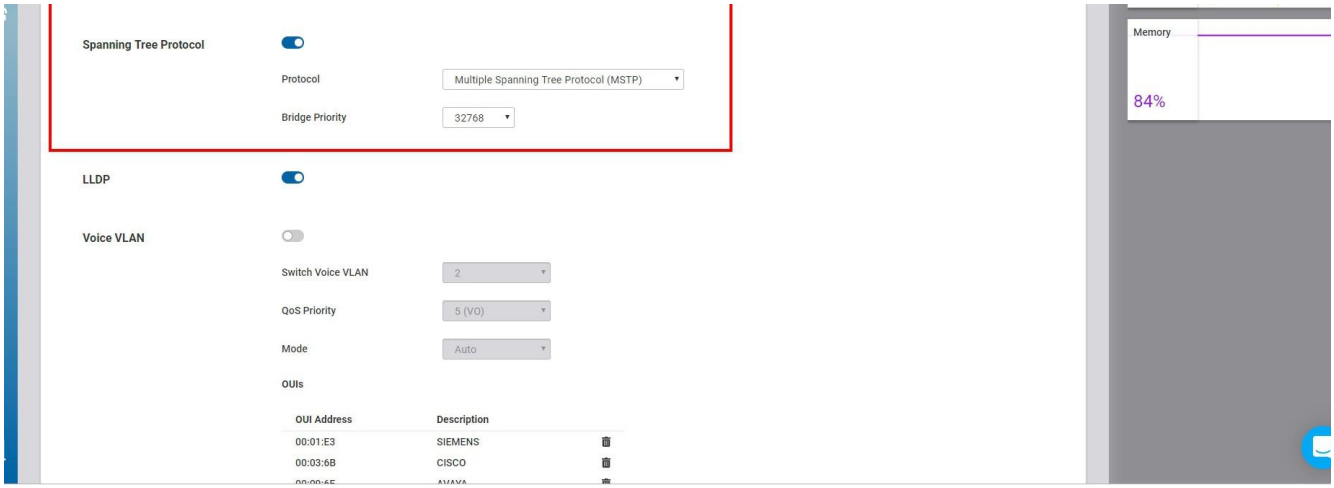


System Setting

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.

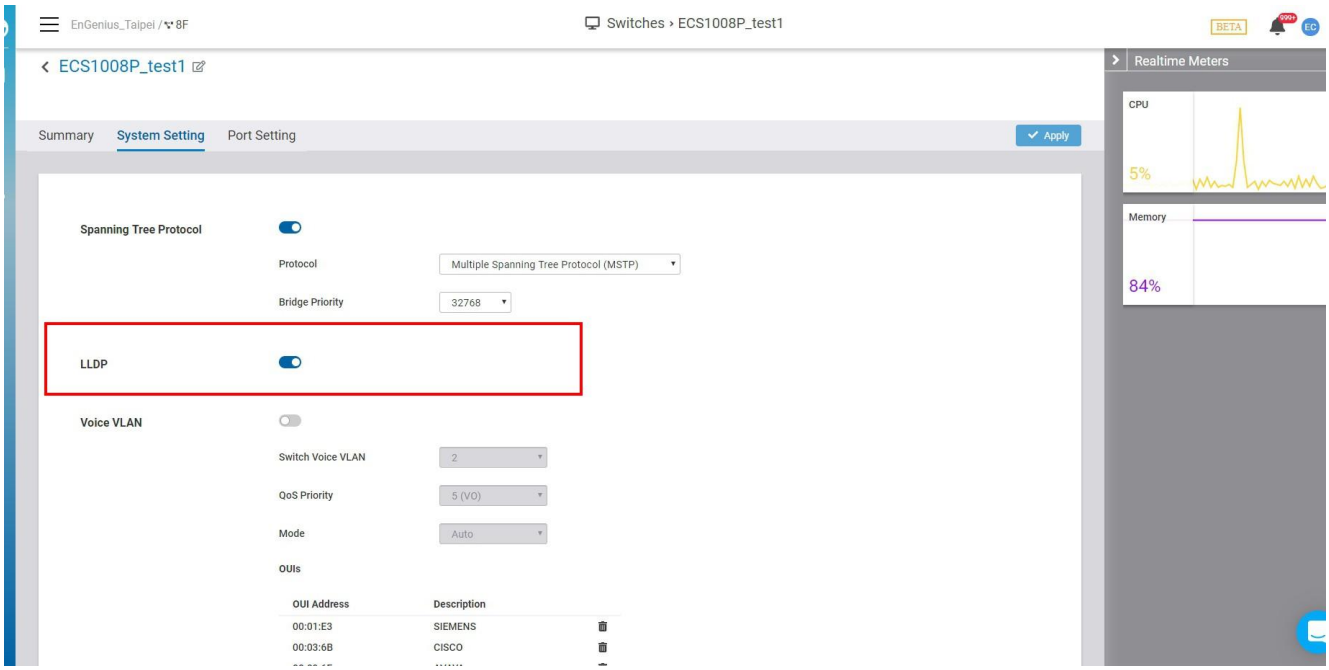


Procedure

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.



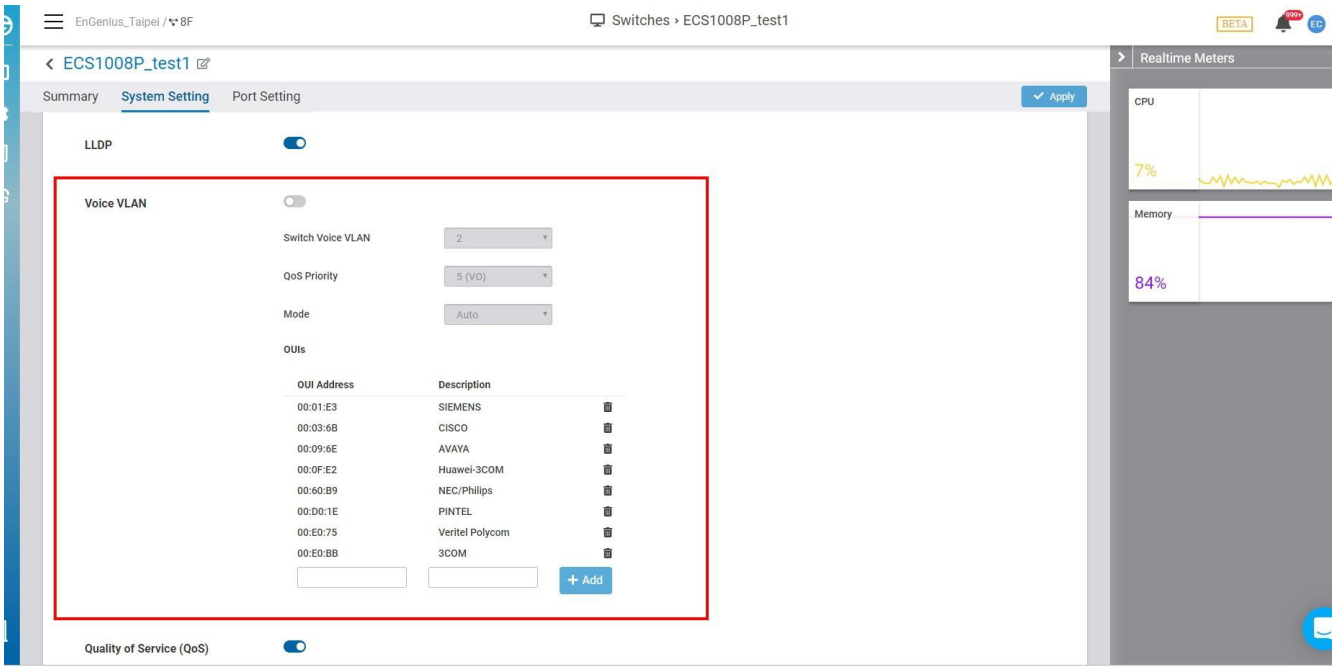
Procedure

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.

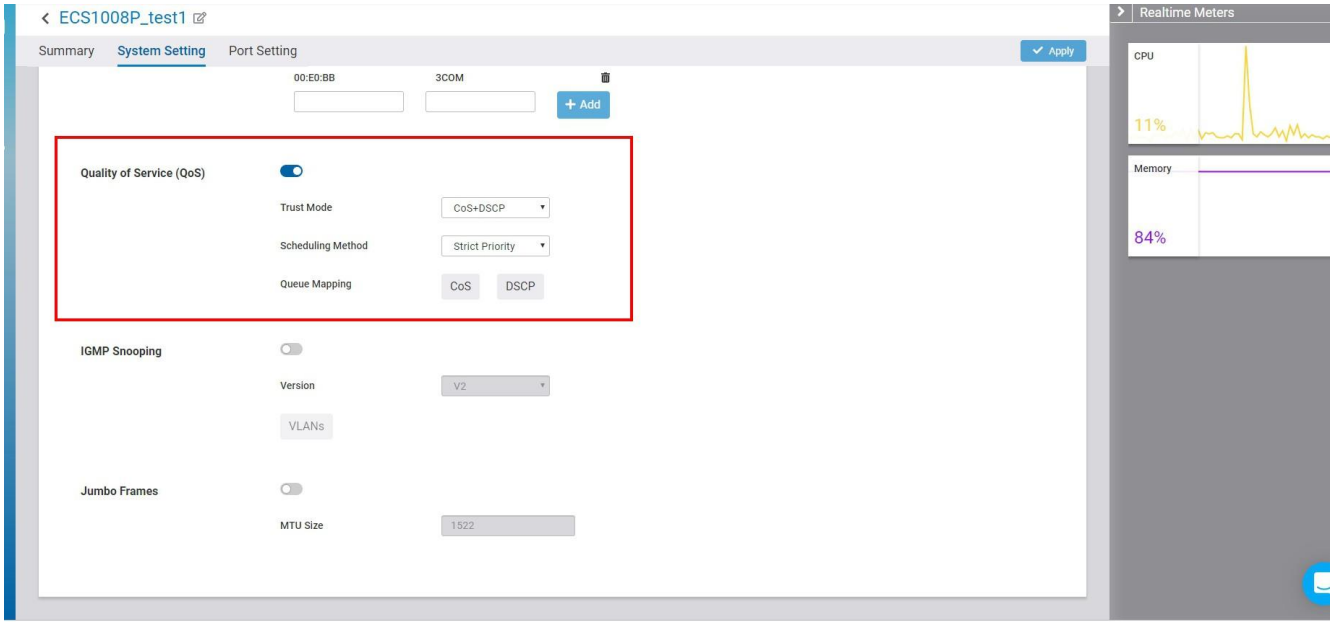
Switch Voice VLAN: Allows you to choose what VLAN is used for Voice VLAN. You can set up VLANs in Port Settings.

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.



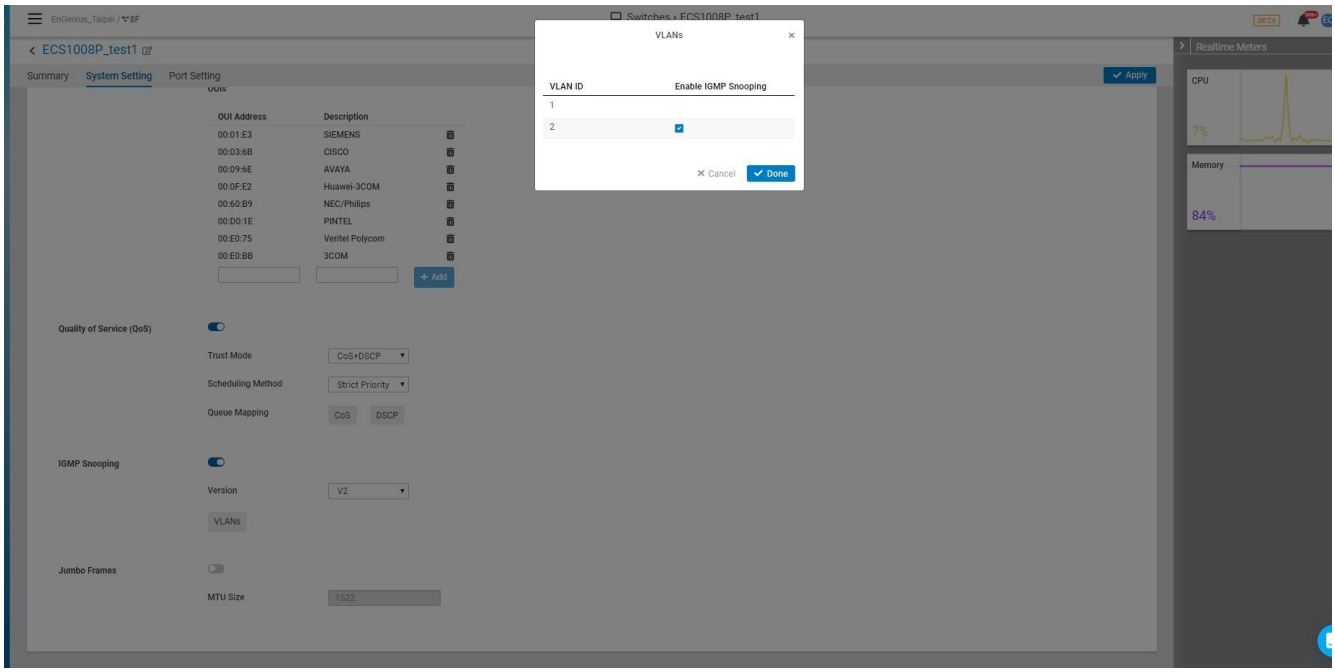
Trust Mode: Allows you to define whether the switch will use CoS, DSCP, or both trust modes for QoS.

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

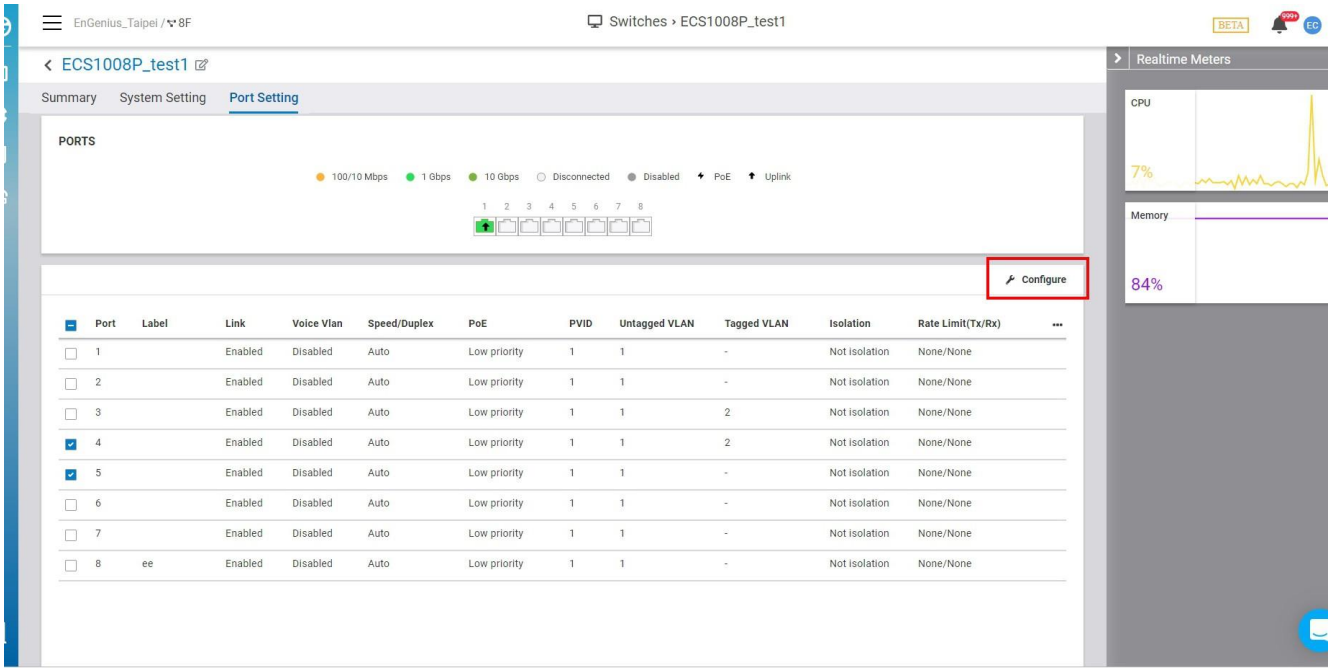
Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application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

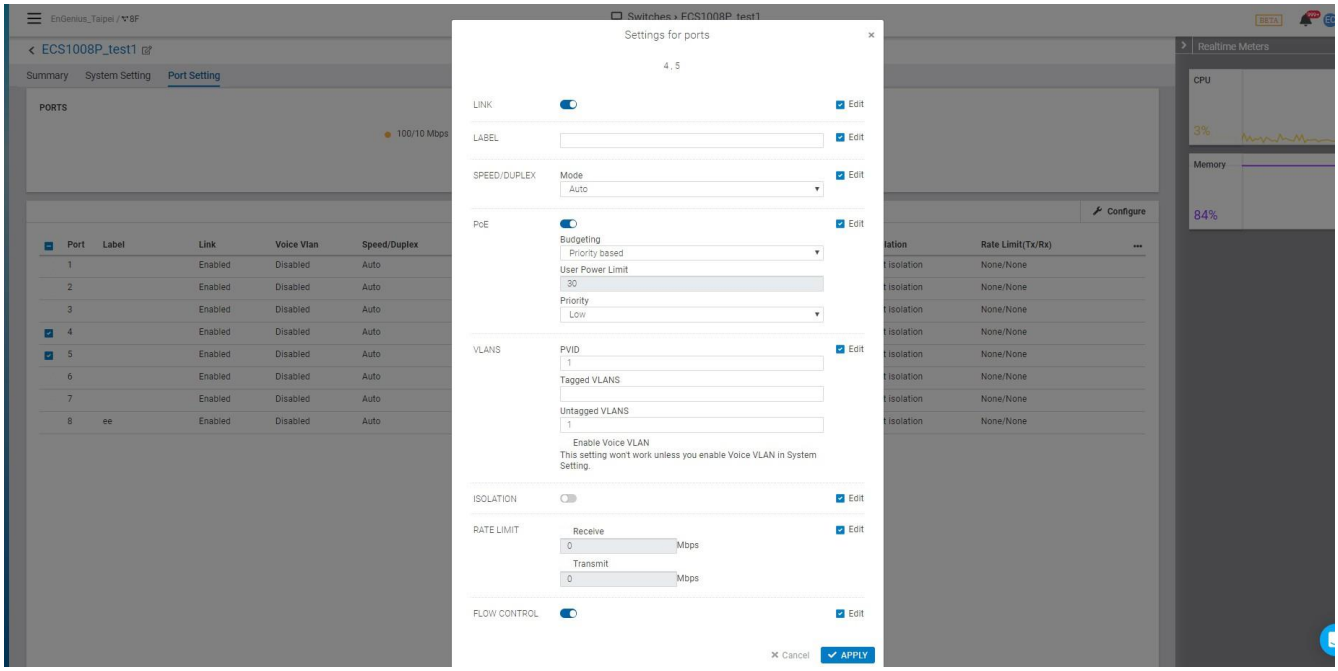
The switch supports a jumbo frame size of up to **9216 bytes**. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important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

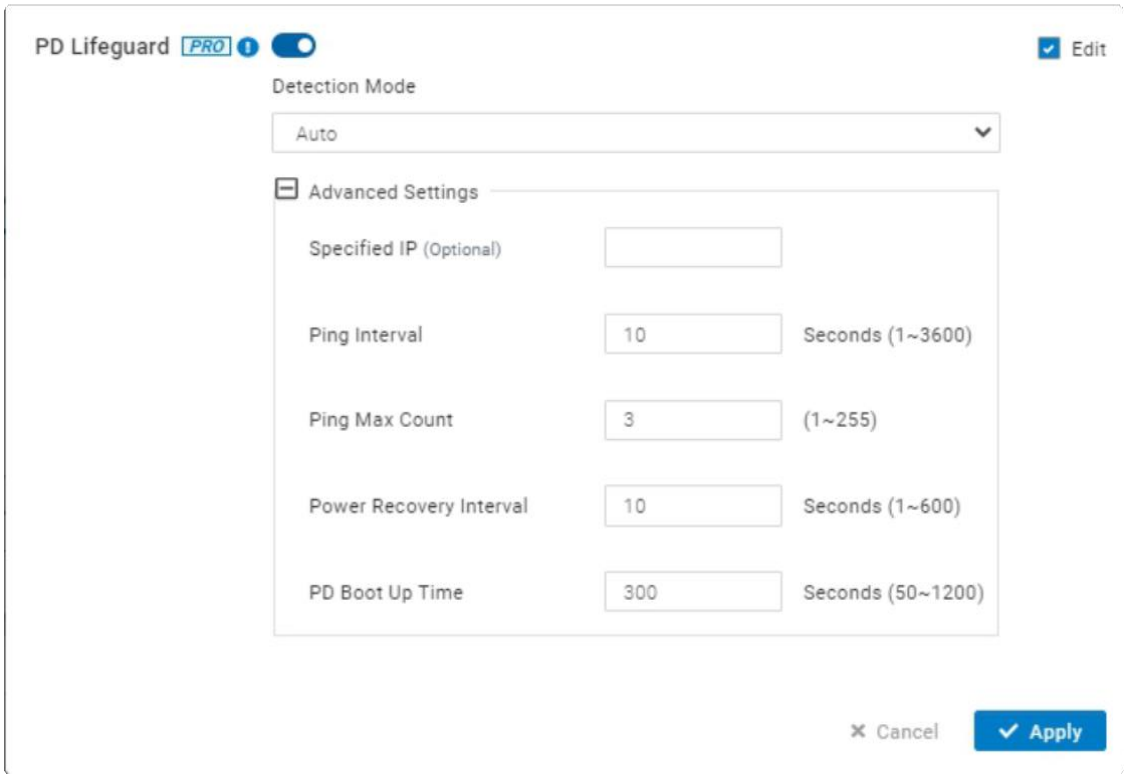
Flow Control: Enabling this will have the switch regulate traffic during times of congestion.

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.

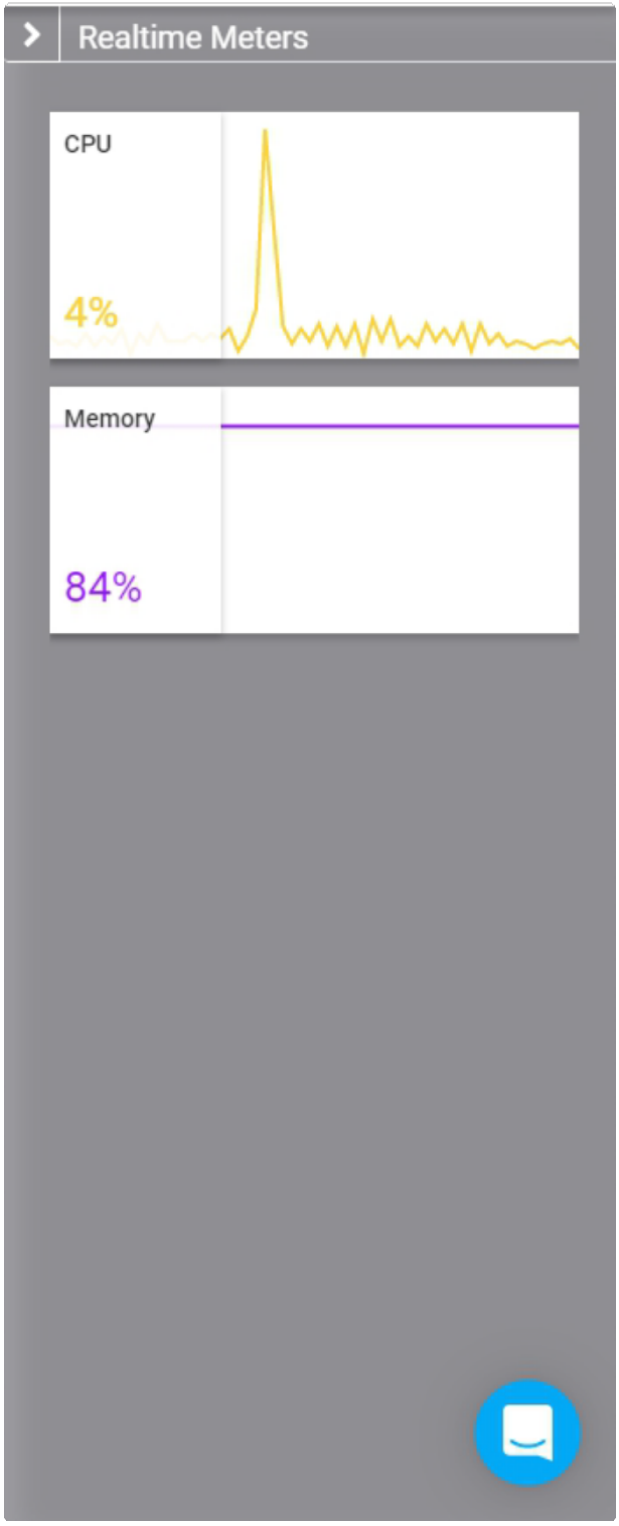


Realtime Meters

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

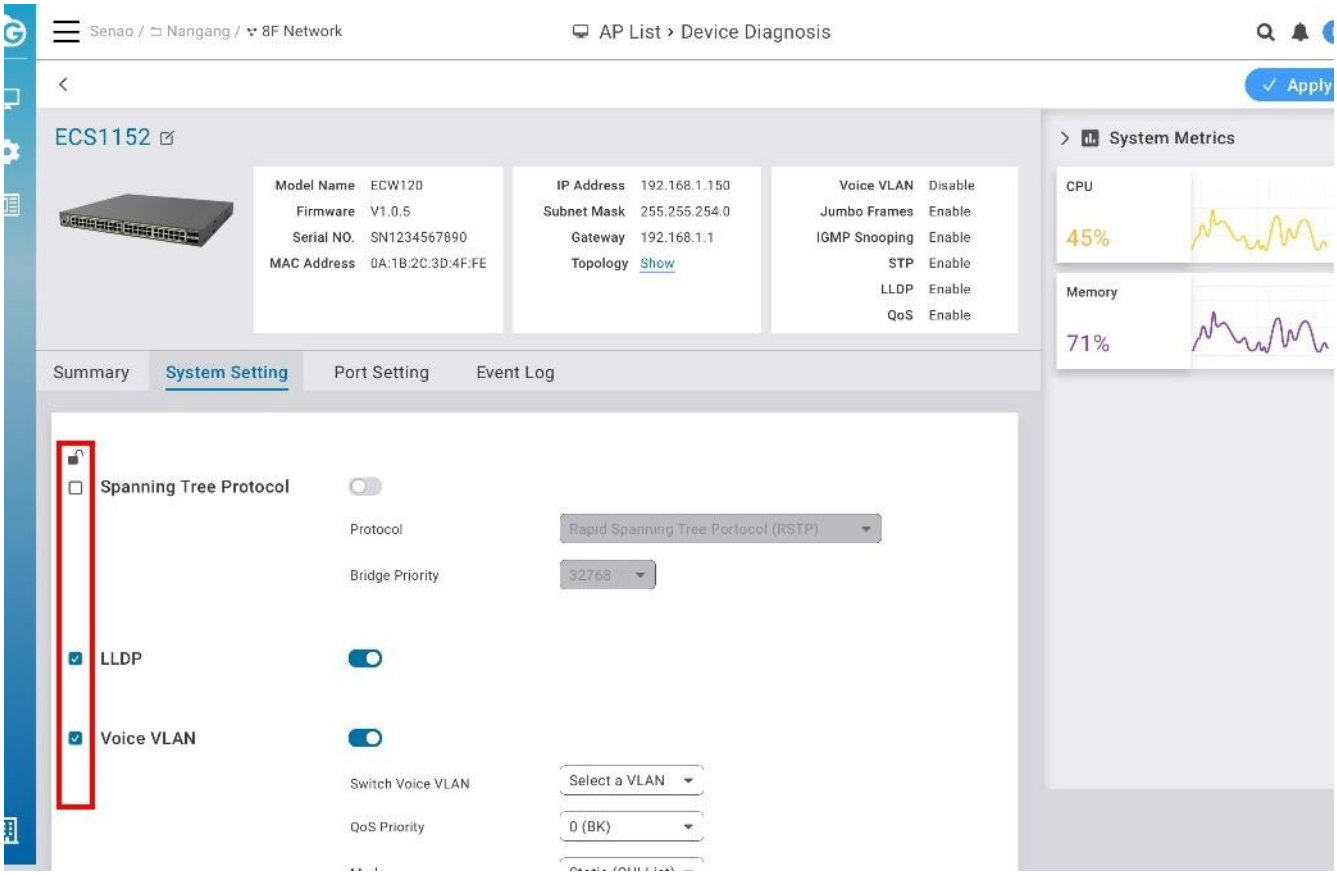
- **CPU**
- **Memory**

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



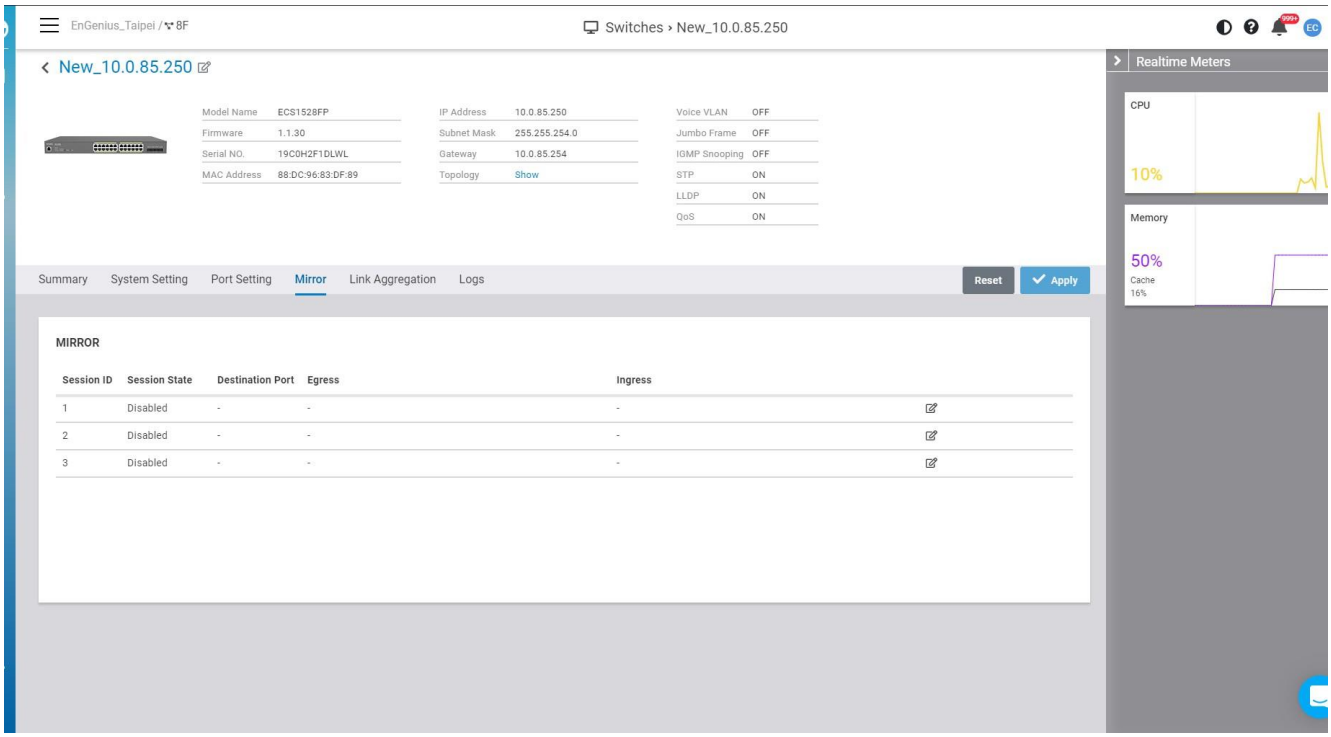
Override System setting on the Switch Network-wide setting

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 .



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**

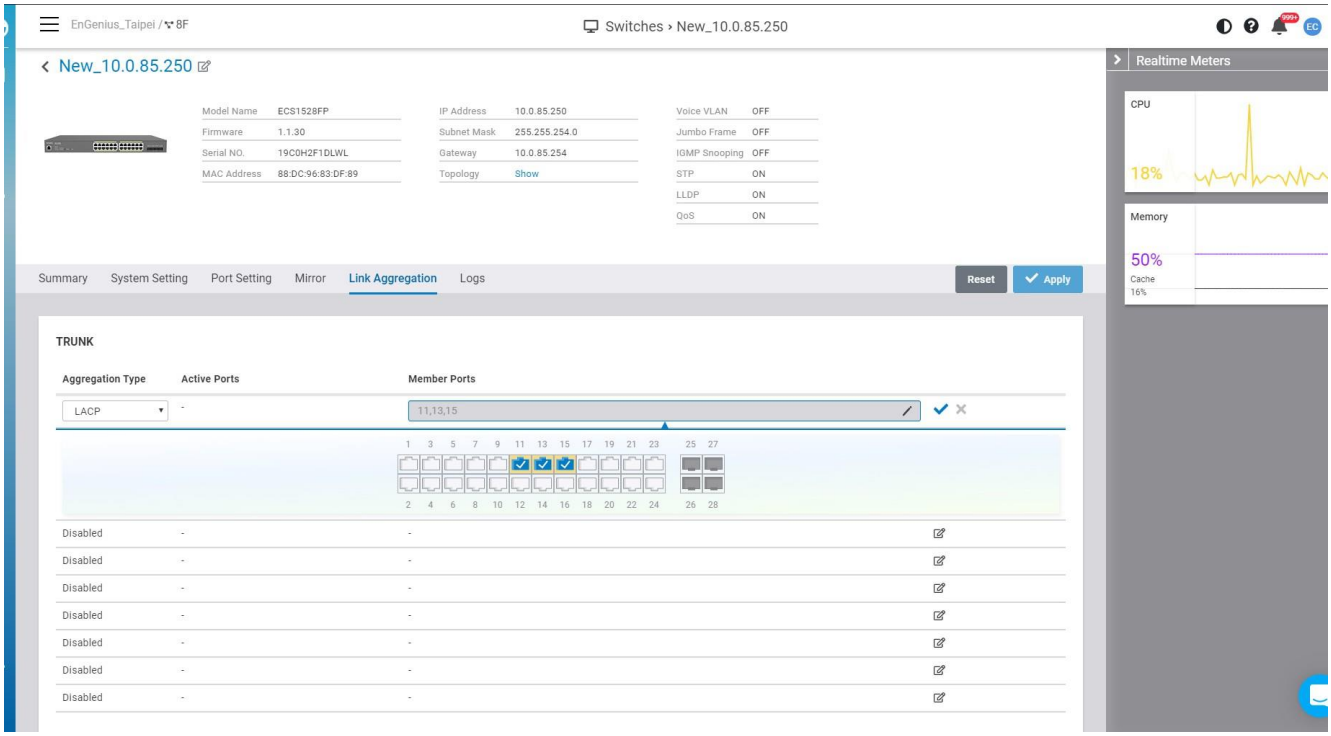
How to Configure

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

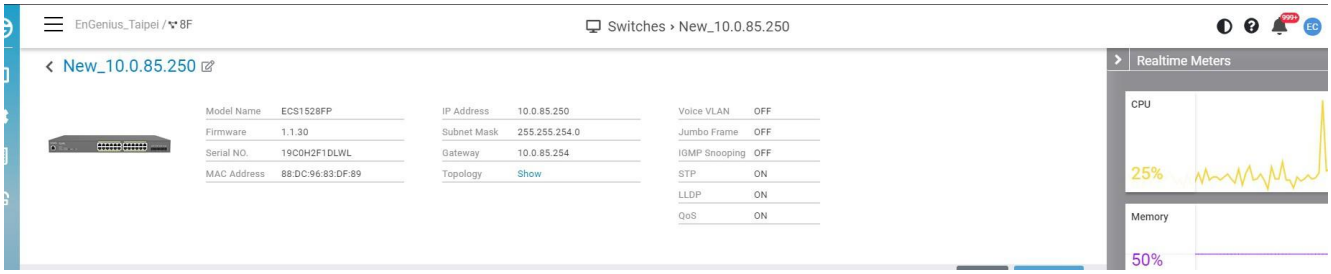
- **LACP**: LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor 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.

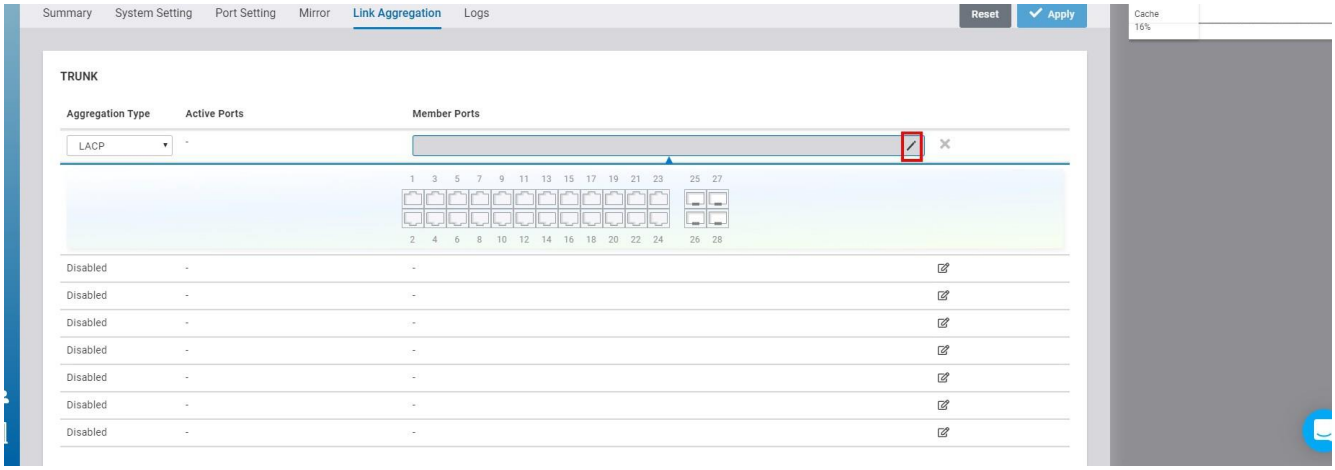
Then select the **Member Ports** to add into the trunk group. There are two ways to select the ports

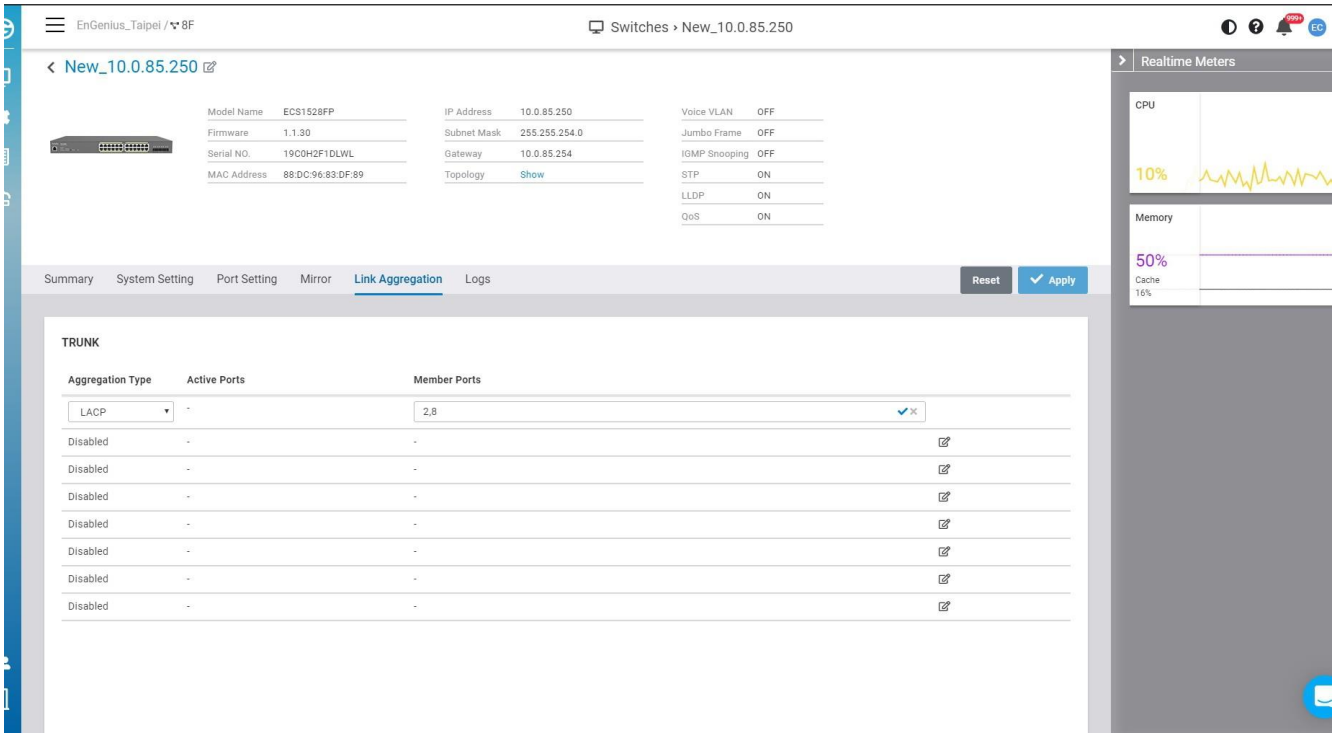
1. Click on the port picker to select multiple ports.



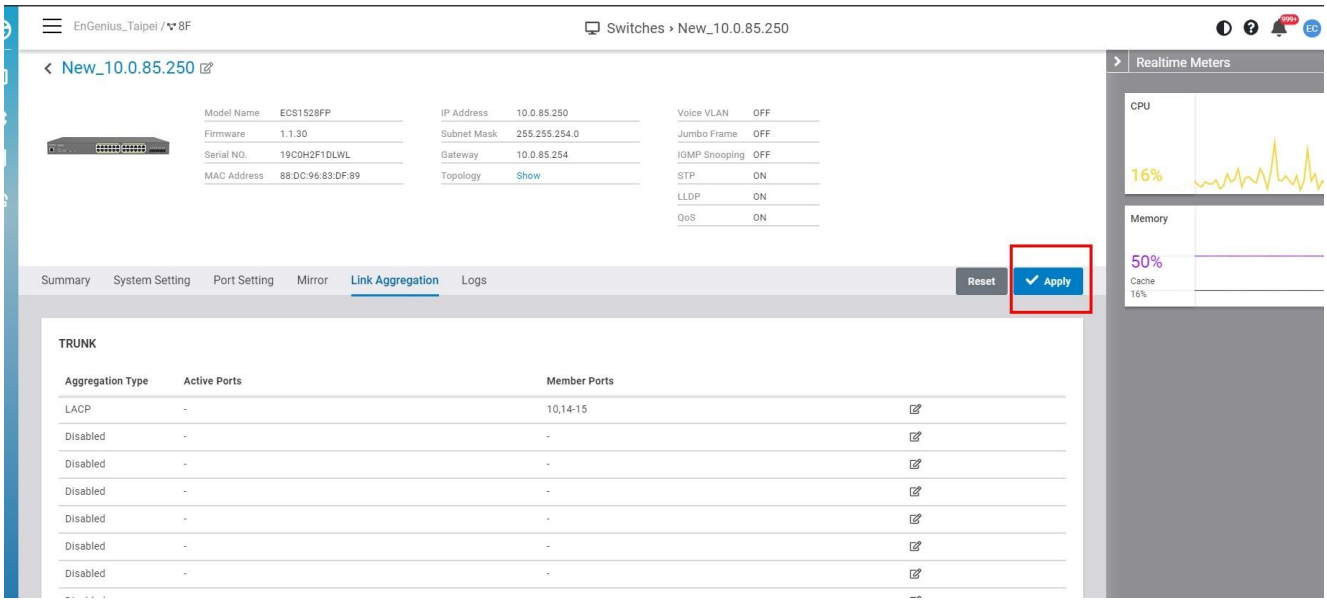
2. Click Pencil icon to input port numbers

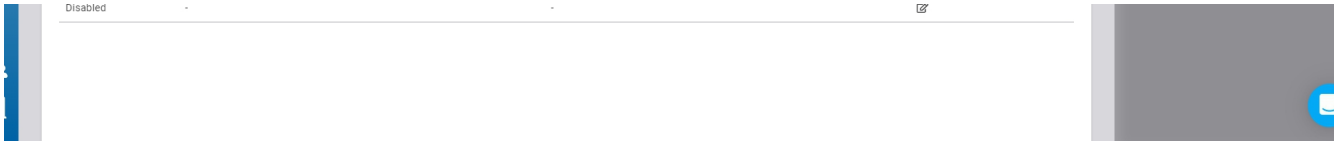






After you complete the trunk settings , remember to click **Apply** to take effect .





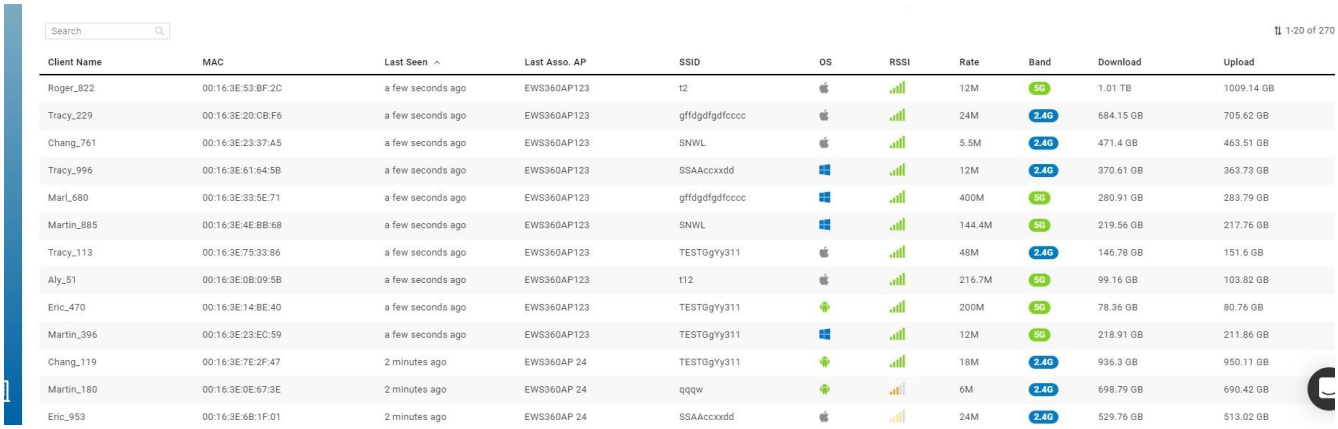
Managing Clients

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.

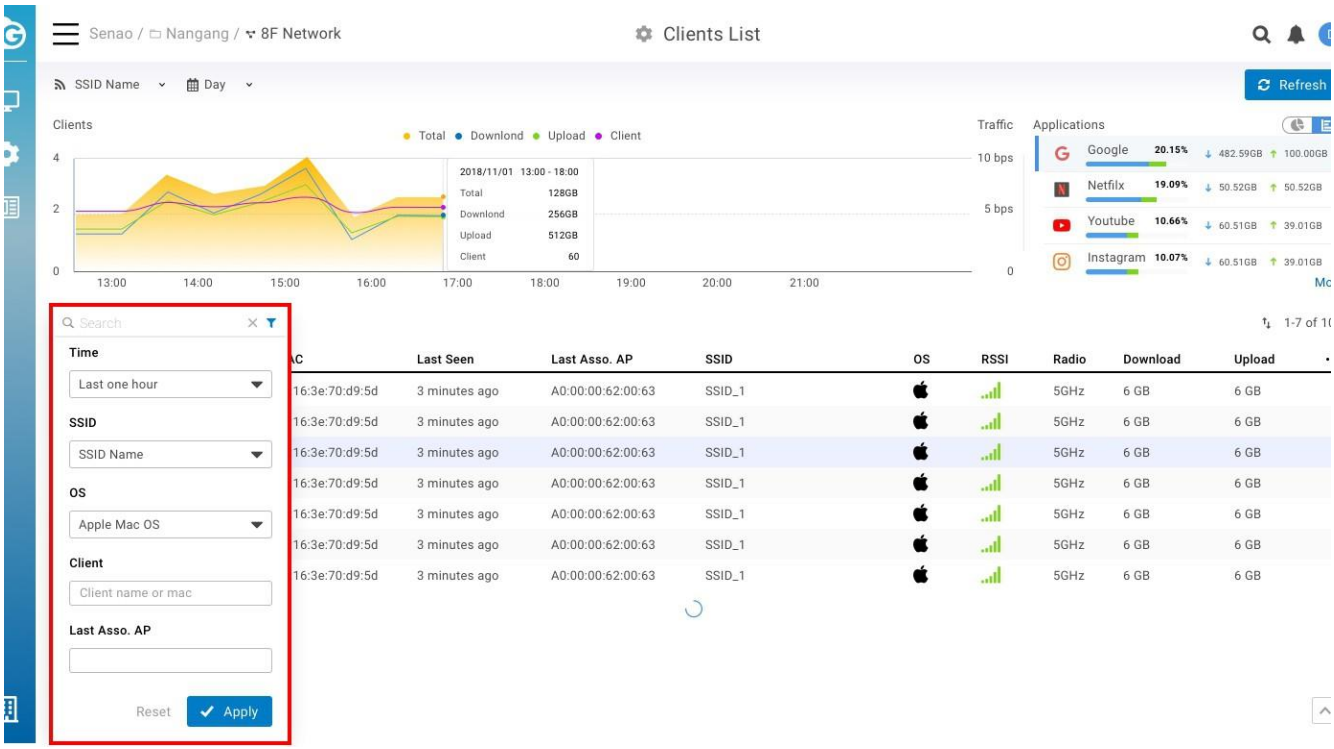
Filtering the Clients List

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.



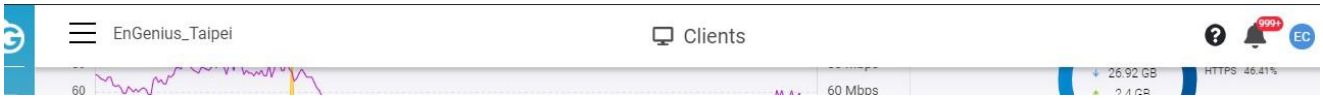
Searching for Clients

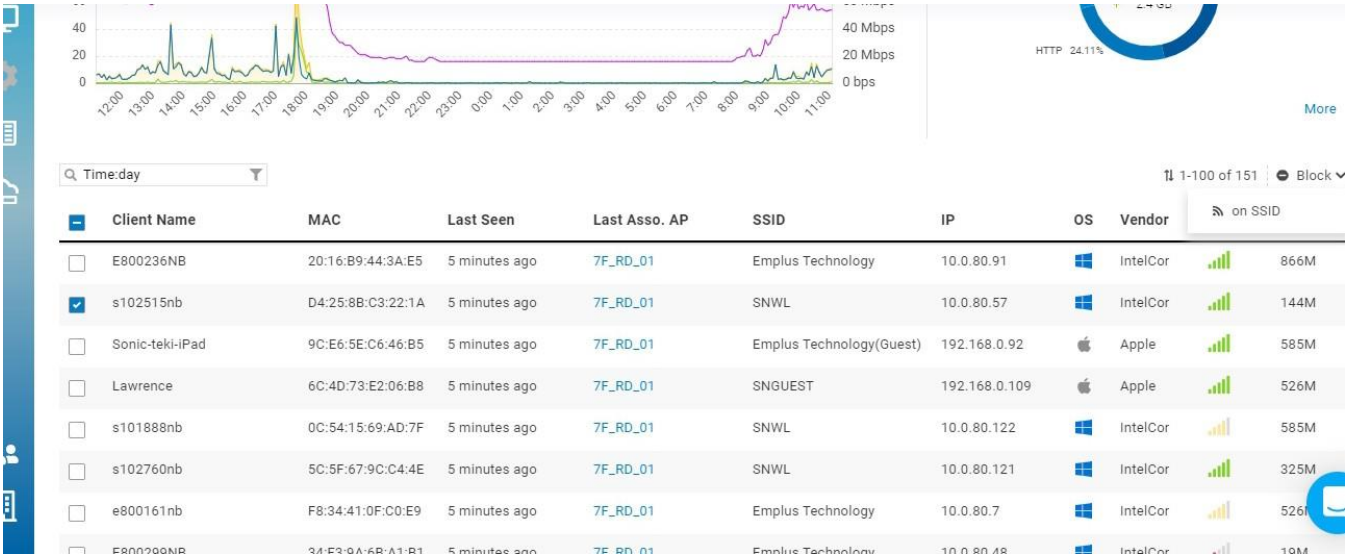
You can search for a client in the current client list by using the search. You can search by any parameter included in the search options, and it will attempt to match your query across all fields. You can also specify multiple parameters by clicking on the icon in the search box, as seen below:



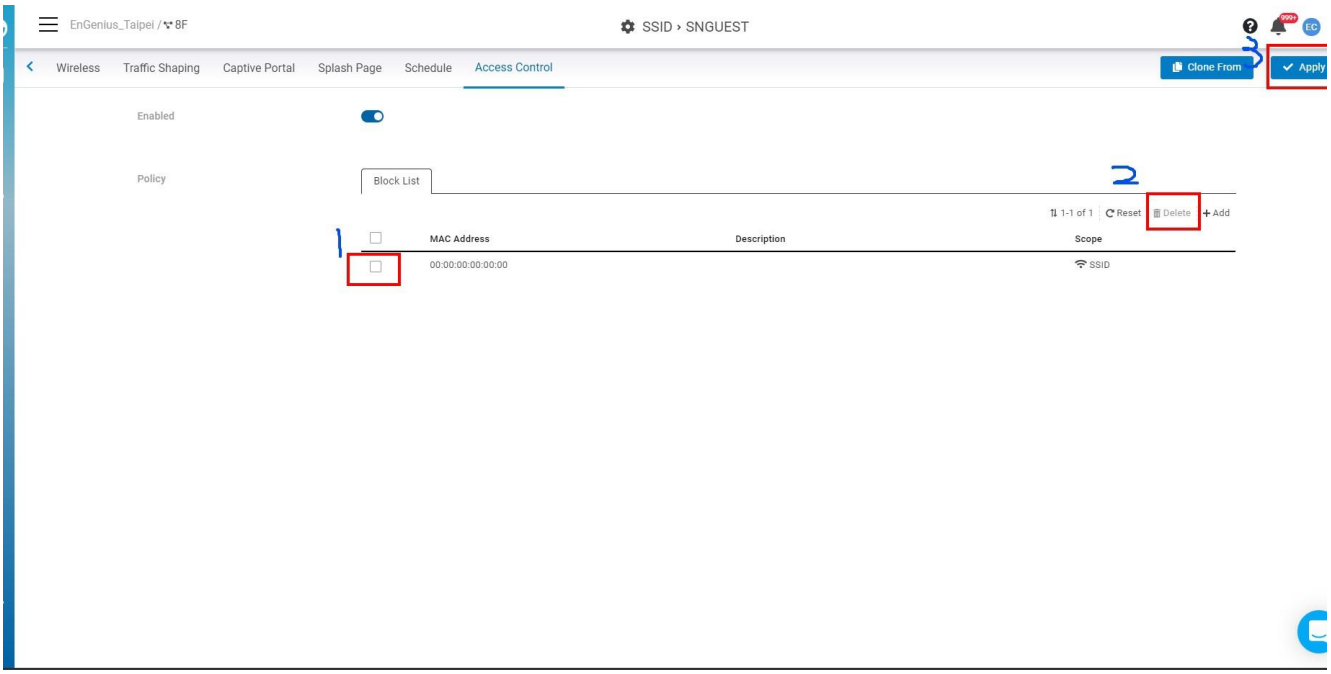
Block Clients

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



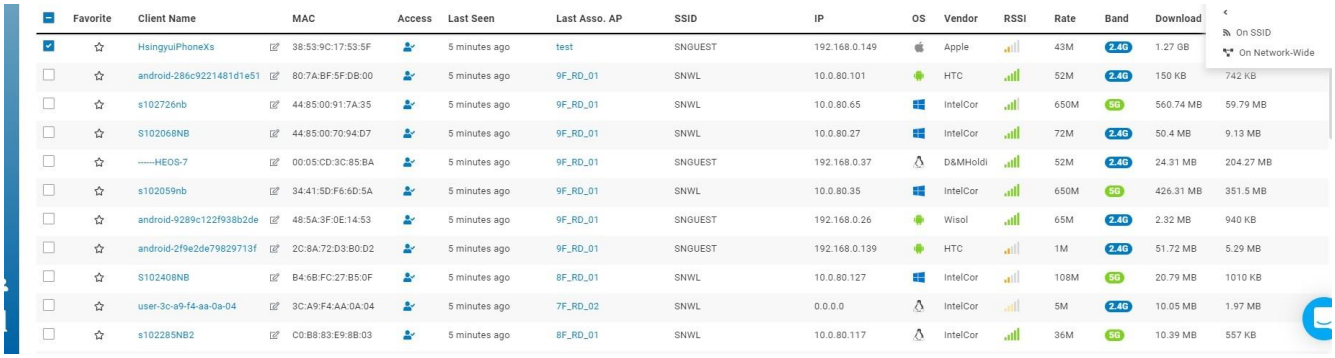


Once you want to unblock clients , please go to **Configure** > **SSID** > **Access control** to delete the Mac Address from the Block list .



VIP Clients

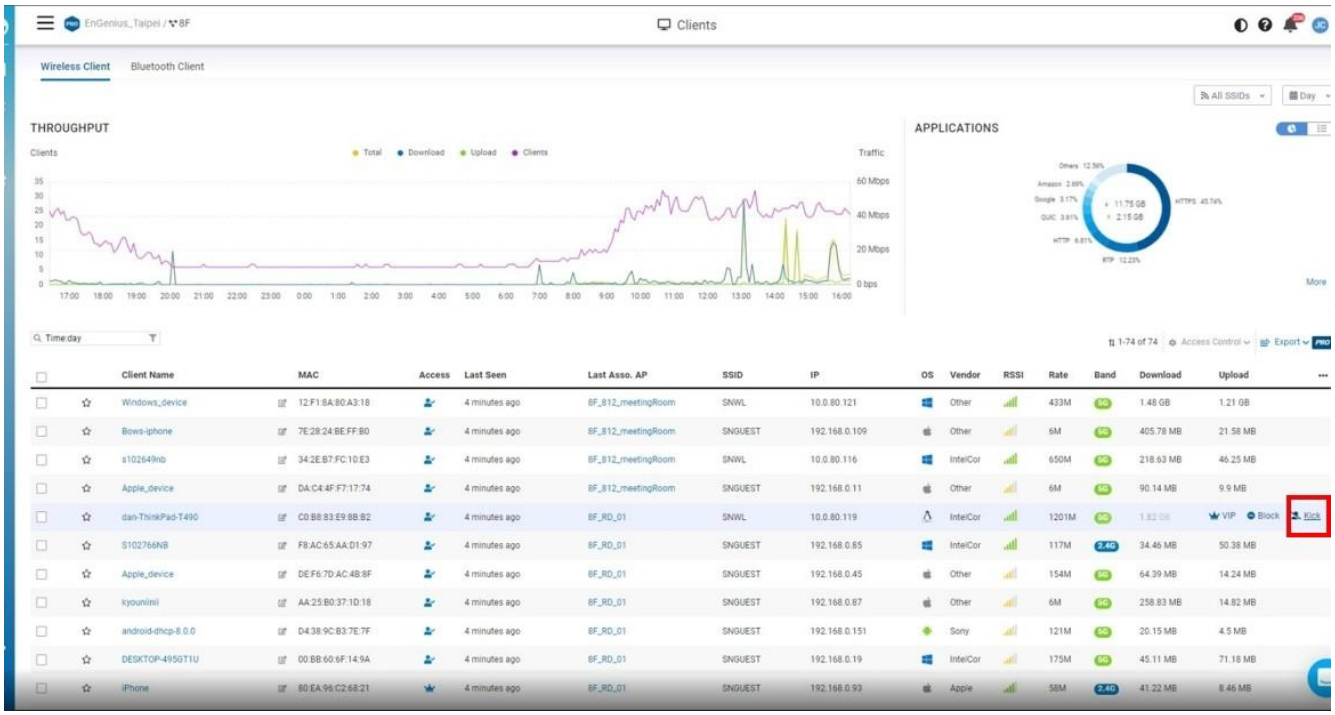
This allows you to make clients as VIP on the current SSID or on Network-wide that clients connected.



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.

Kick Clients

If you don't want to block clients permanently, you could just kick them so that they can connect again if they want to.



Client Timeline

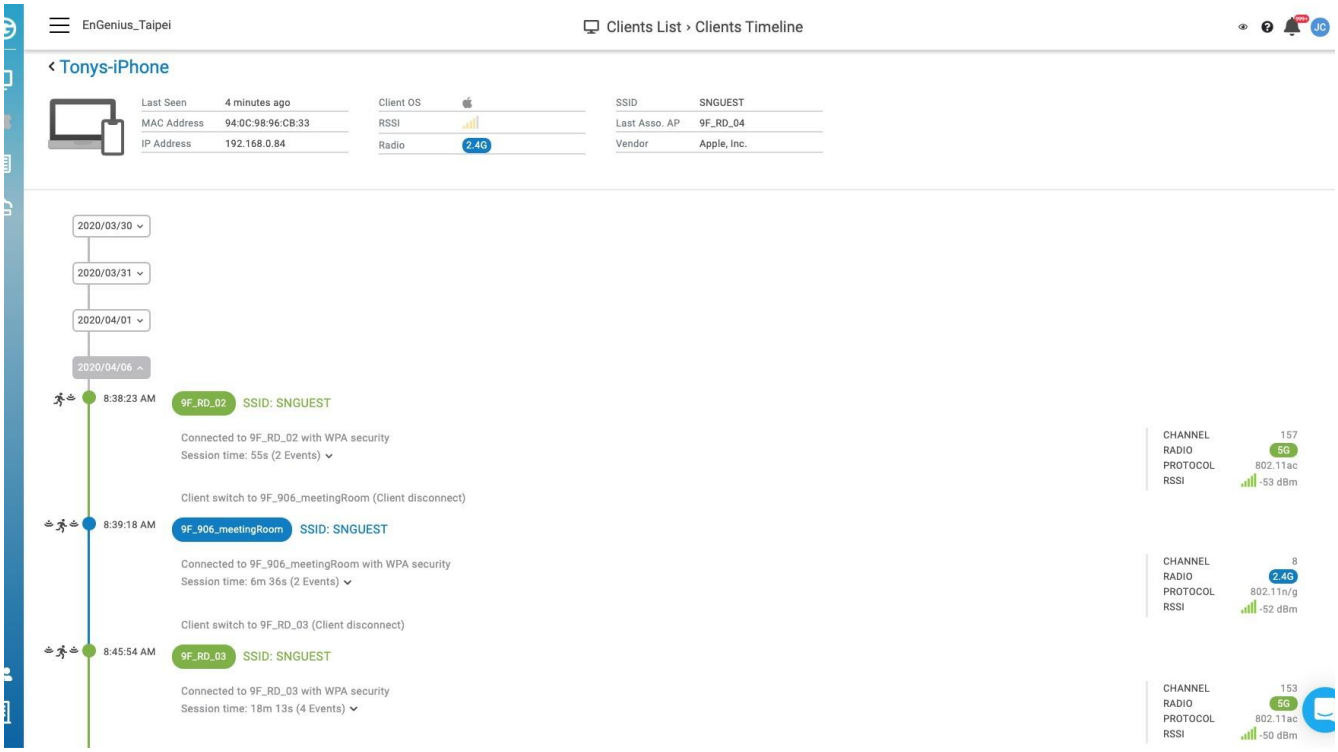
The Client Timeline is a great feature that aggregates and analyzes activities of a specific wireless client to provide an intuitive and historical view. With Client Timeline, user can easily know how clients associate, authenticate, and roam among Access Points. It is extremely useful when you need 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:

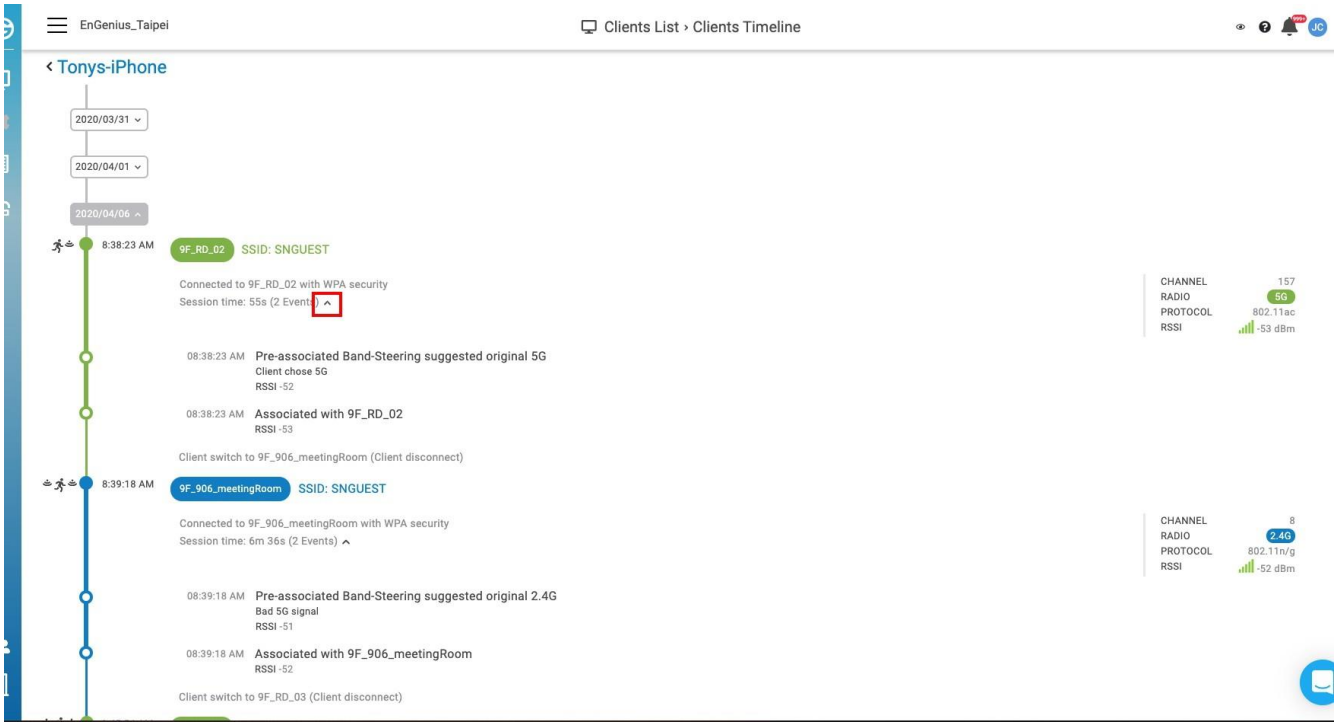


Table below displays client leave patterns when client leaves each connection session.

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.
	The client disconnected from the AP due to band

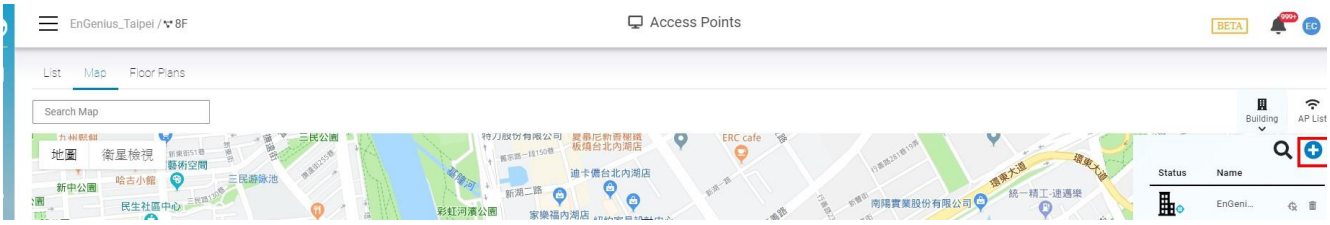
Steer to {radio}	steering protocol. It received the 802.11v trigger and connected to suggested band accordingly.
Disconnected by {device_name}	The client was disconnected by the AP due to ba RSSI signal (fast handover).
AP disconnect	The client was disconnected by the AP due to unknown reason.
Kicked 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 contro
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 disable 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.

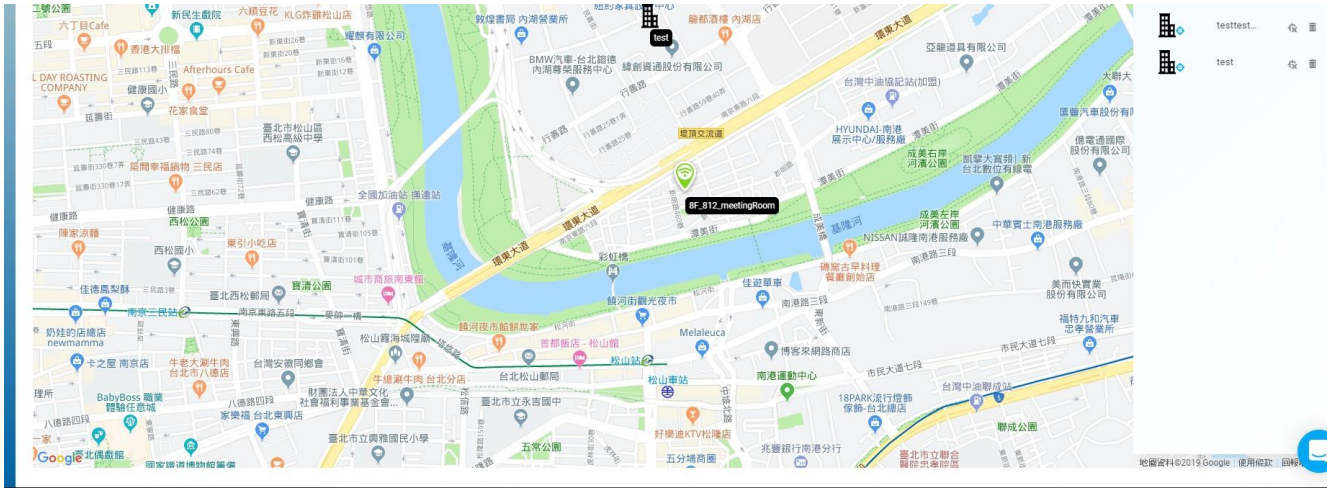
Device Map Location

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.

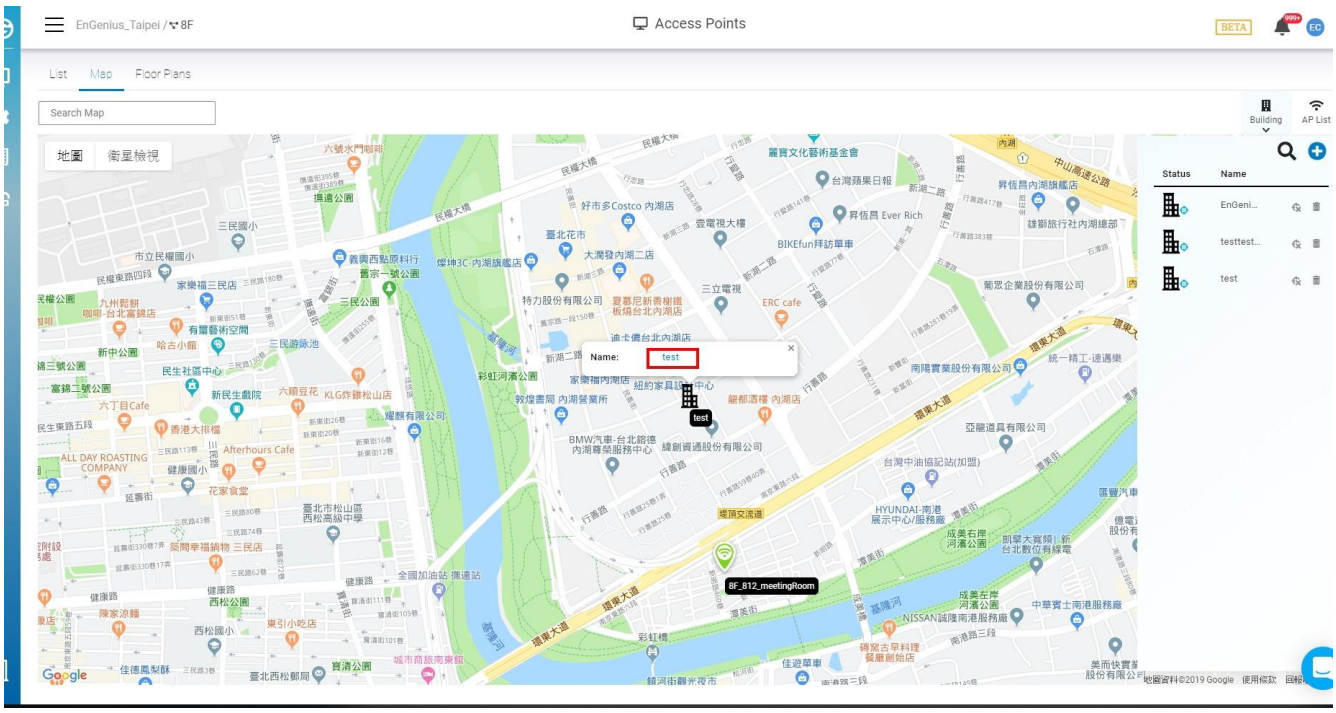
Create Buildings

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



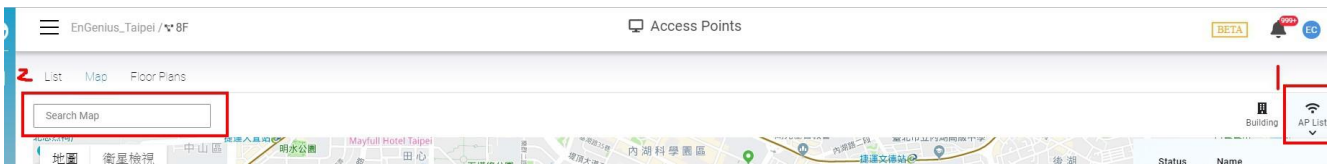


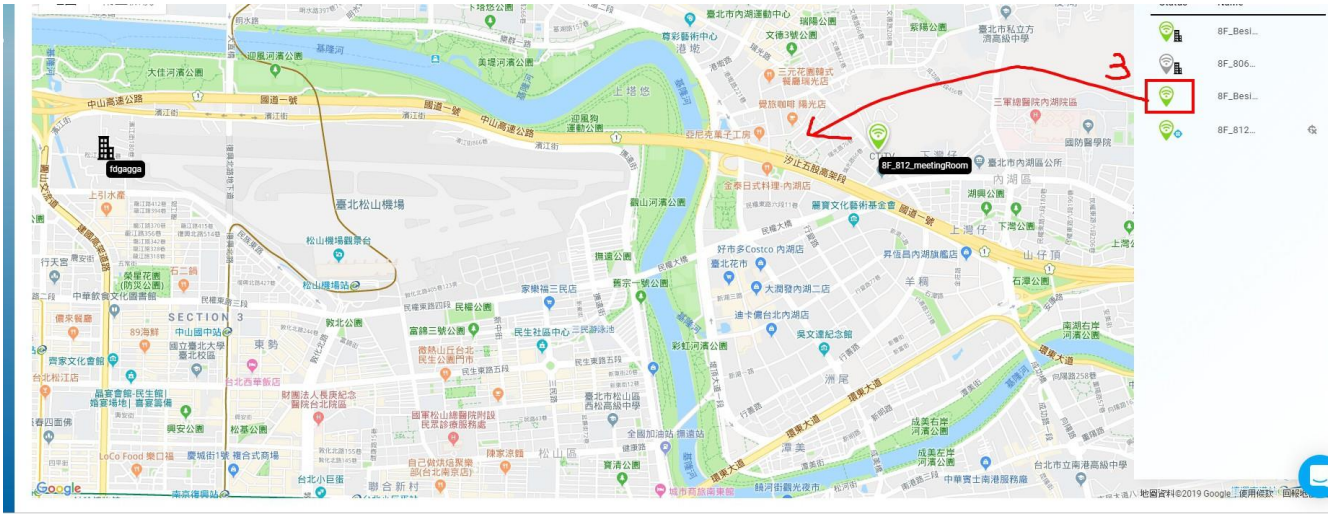
After you create a building, you can drag it to the map. Single-click on the building icon and a hyperlink will appear to allow you to edit floor plans.



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.

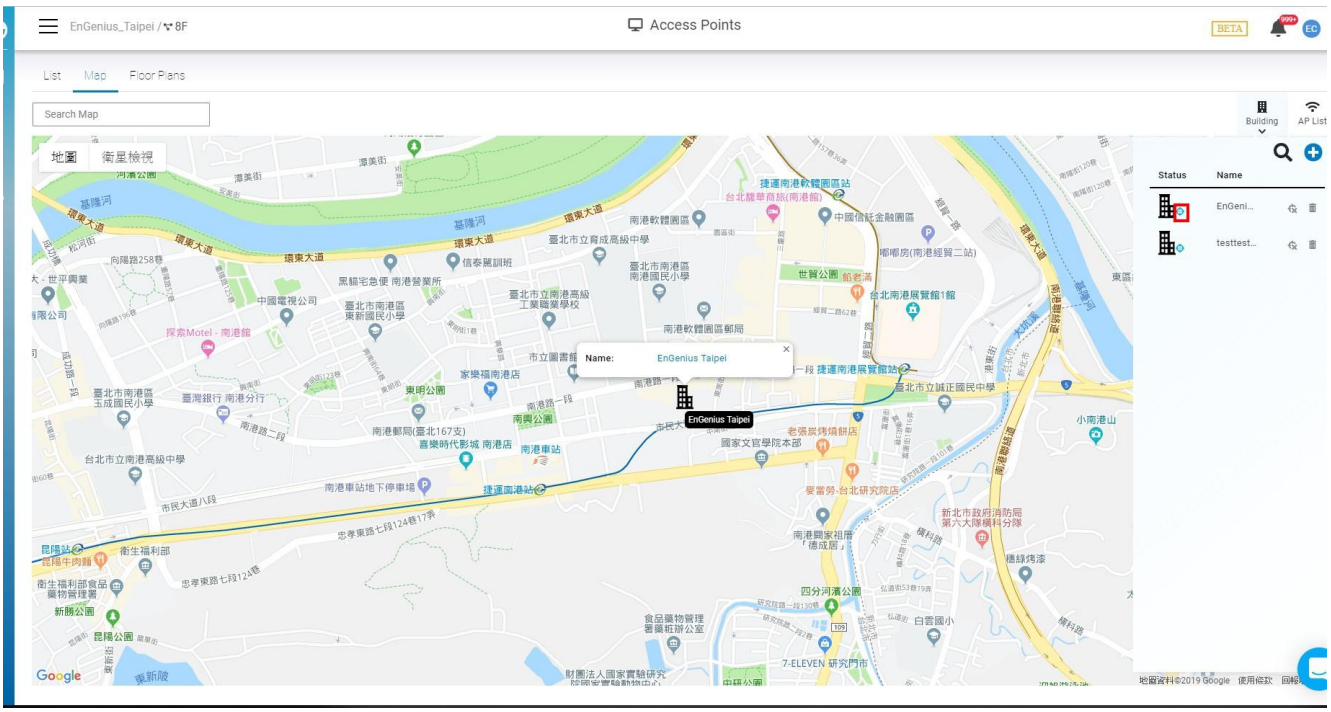




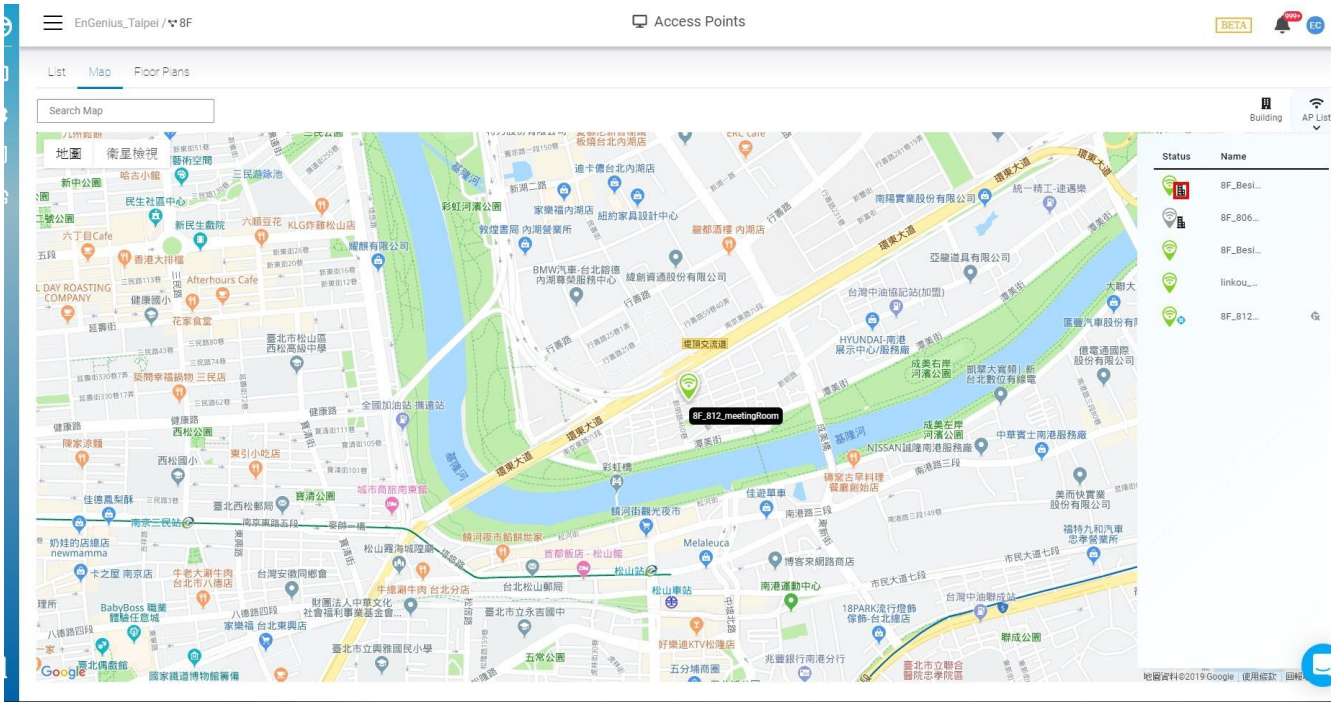
Navigation

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

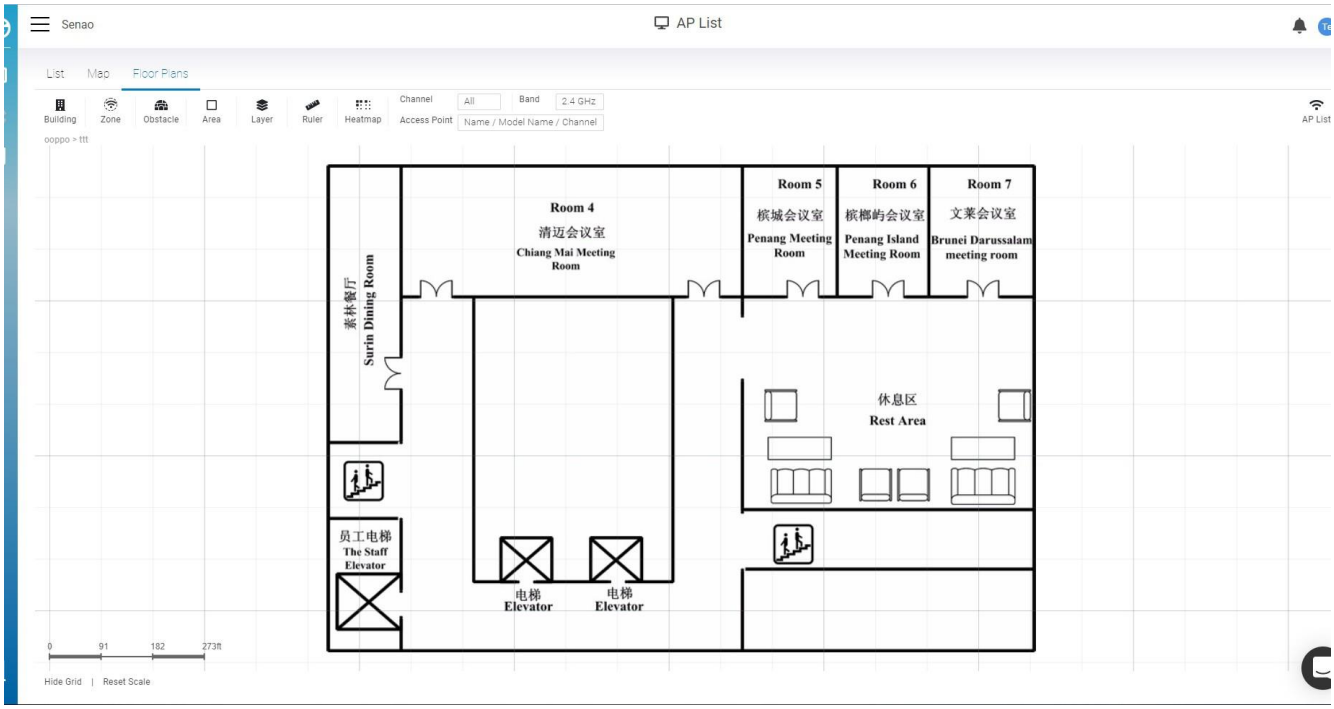
Floor plans allow you to simulate the heatmap. This article will discuss how to upload custom floor plans, pin them on the map, and place devices within these floor plans.

Uploading Floor Plans

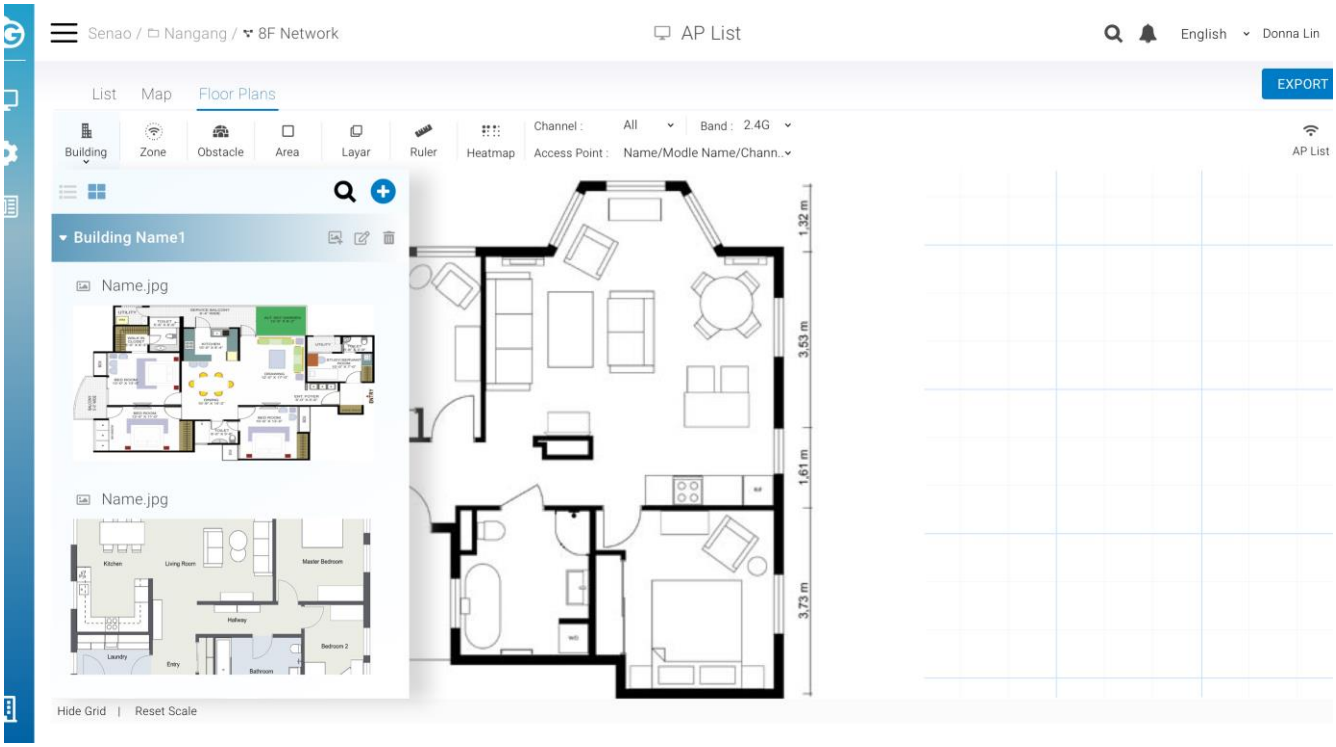
Before uploading floor plans, a building must be created to contain them (see **Managing Devices > Device Map Location** in the user manual).

To upload a custom floor plan/map**:**

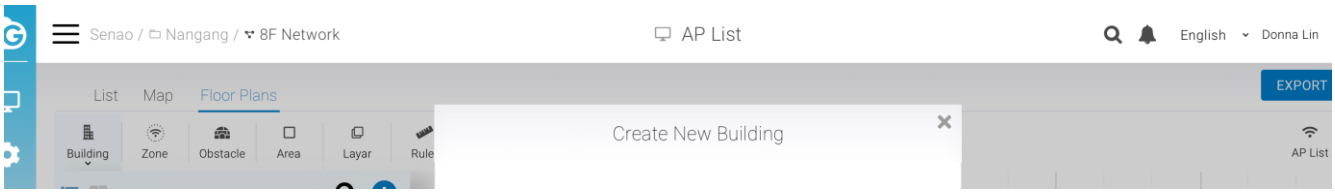
1. Navigate to **Manage > Map & Floor plans**.

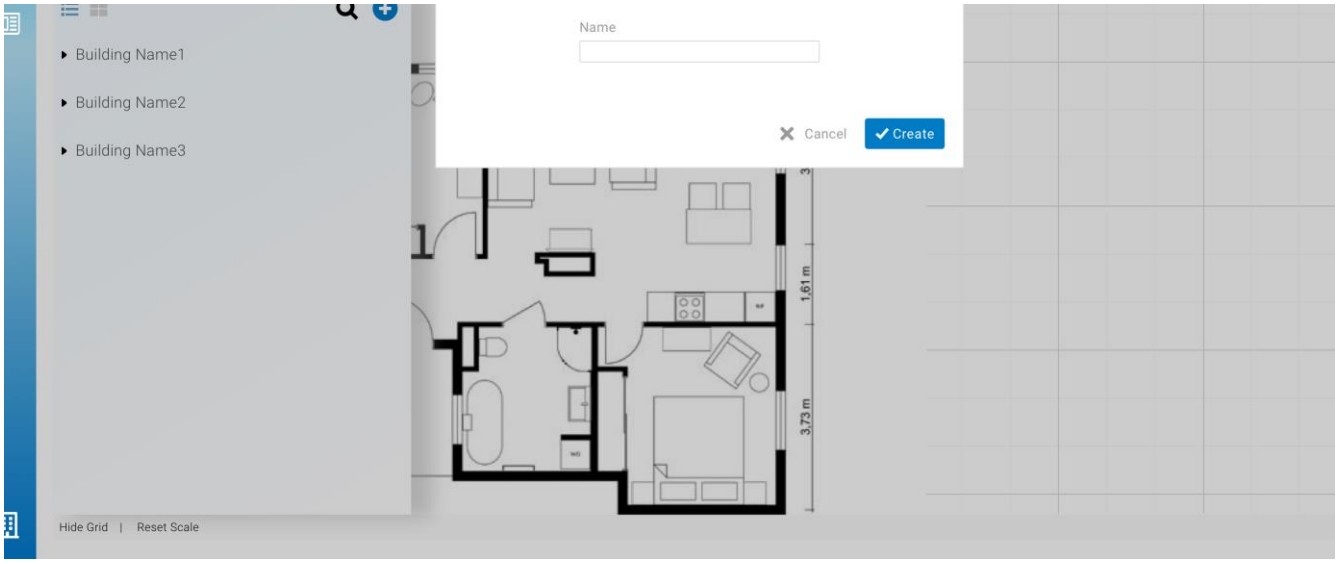


2. Click **Building** and click **Add**.

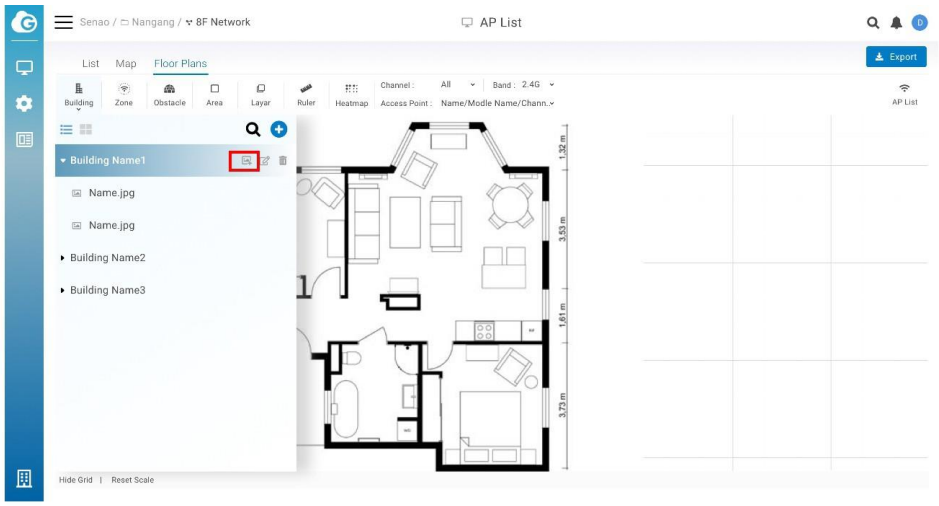


3. Enter a **name** and then click **Create**.

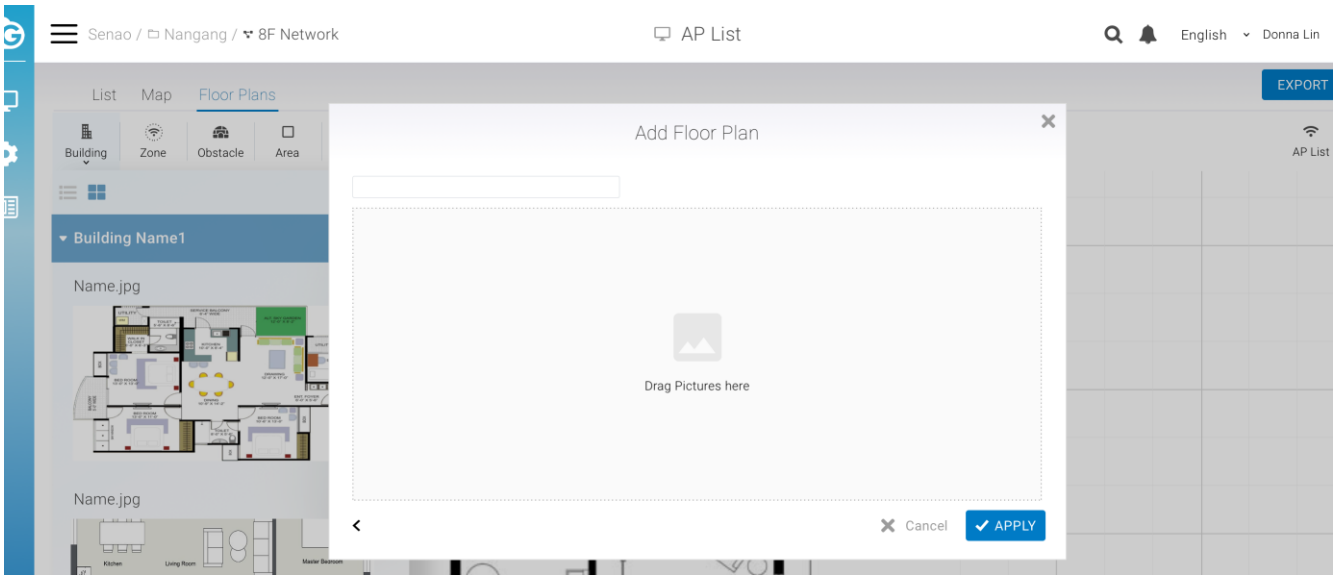




4. Find the building you have just created in the building list and click the picture icon**.**



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

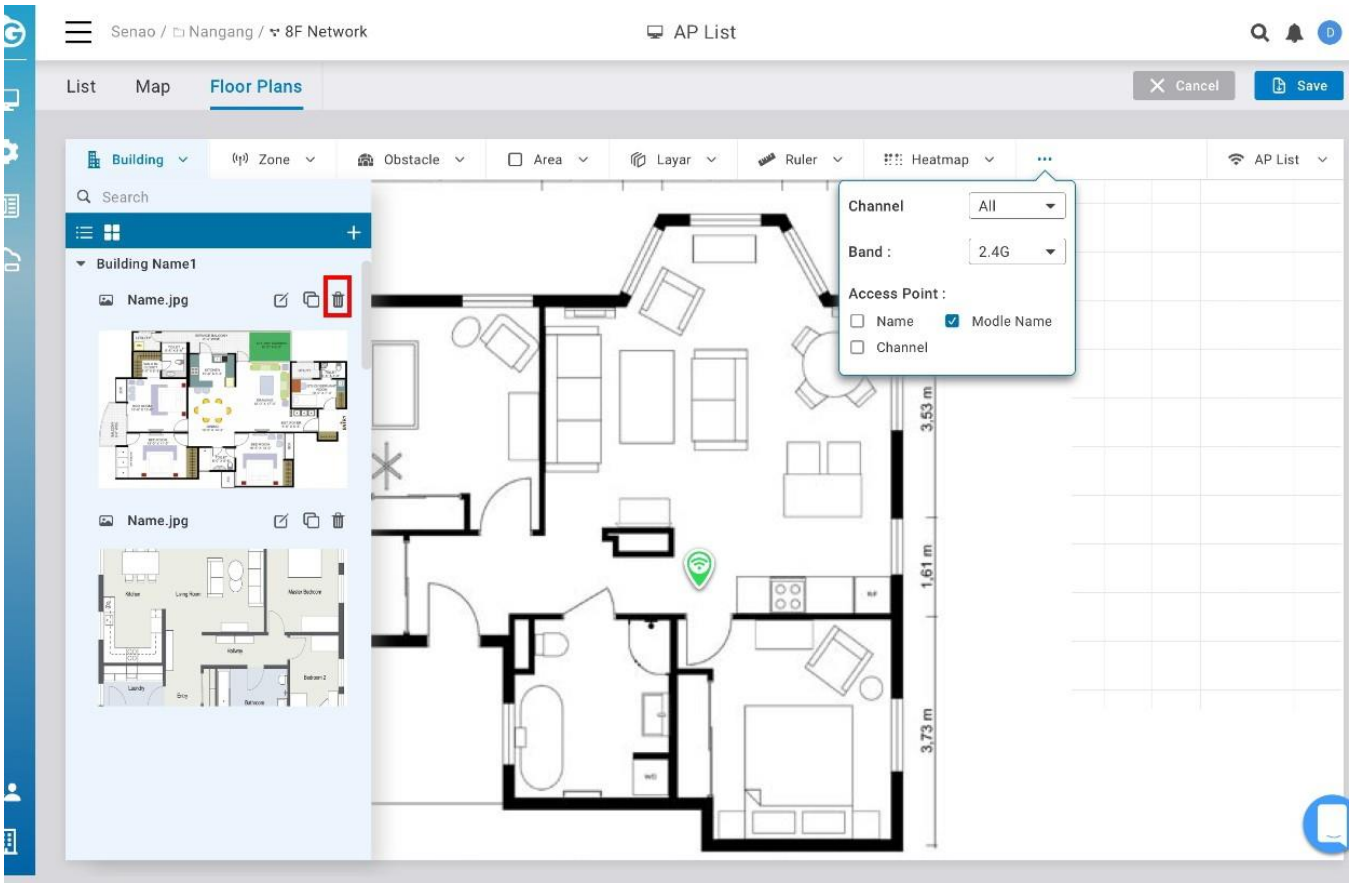


Deleting a Floor Plan

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

Follow these steps to delete a floor plan:

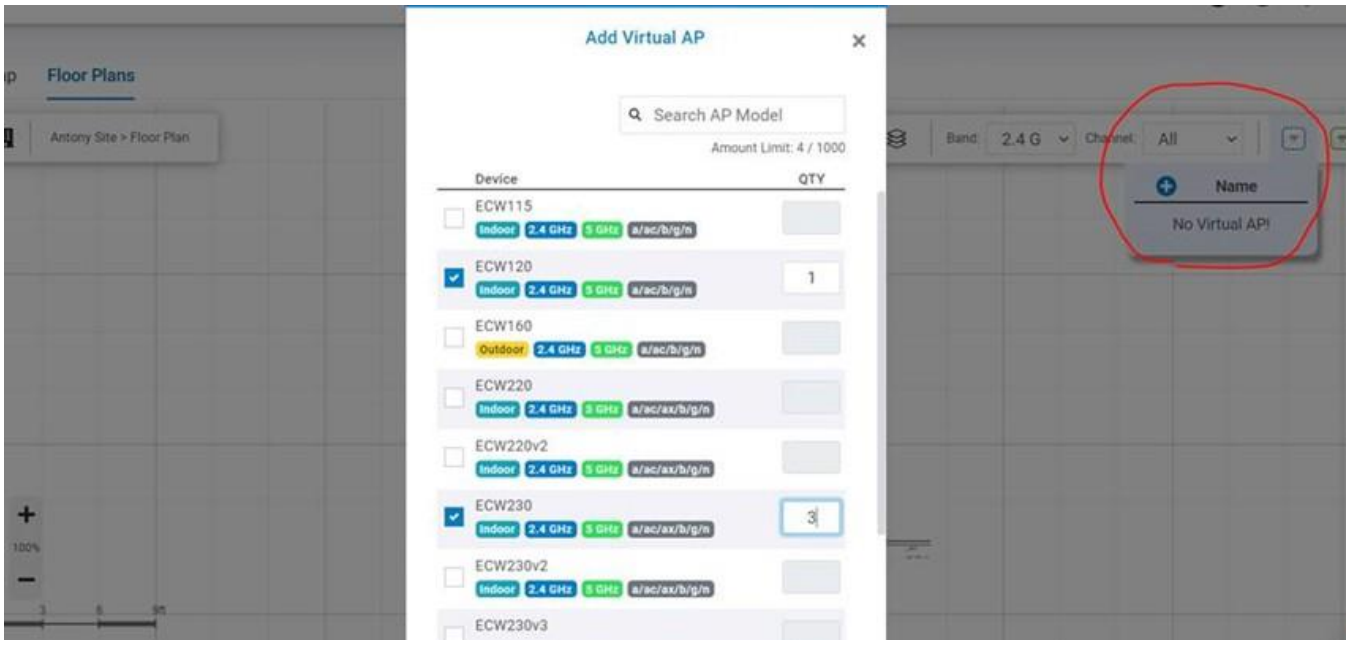
1. Find the building you created in the building list.
2. When the floor plan appears, hover over it and click **Delete**.



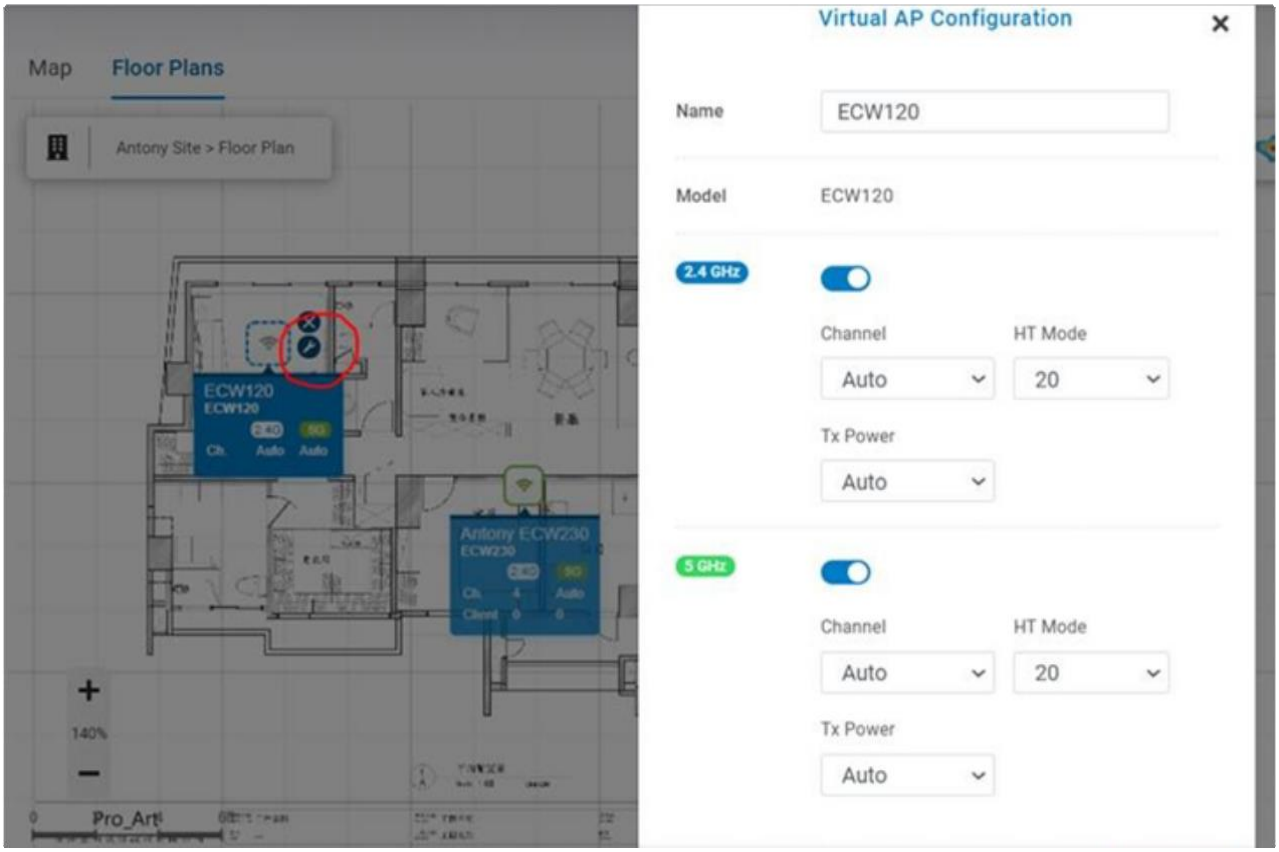
Virtual AP

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

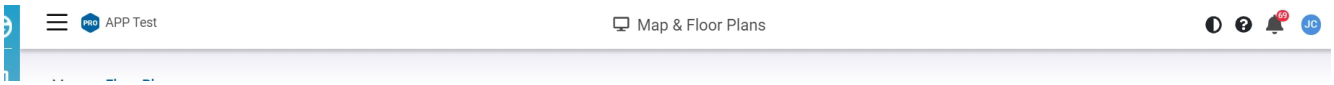
Add Virtual AP and choose units of models to add

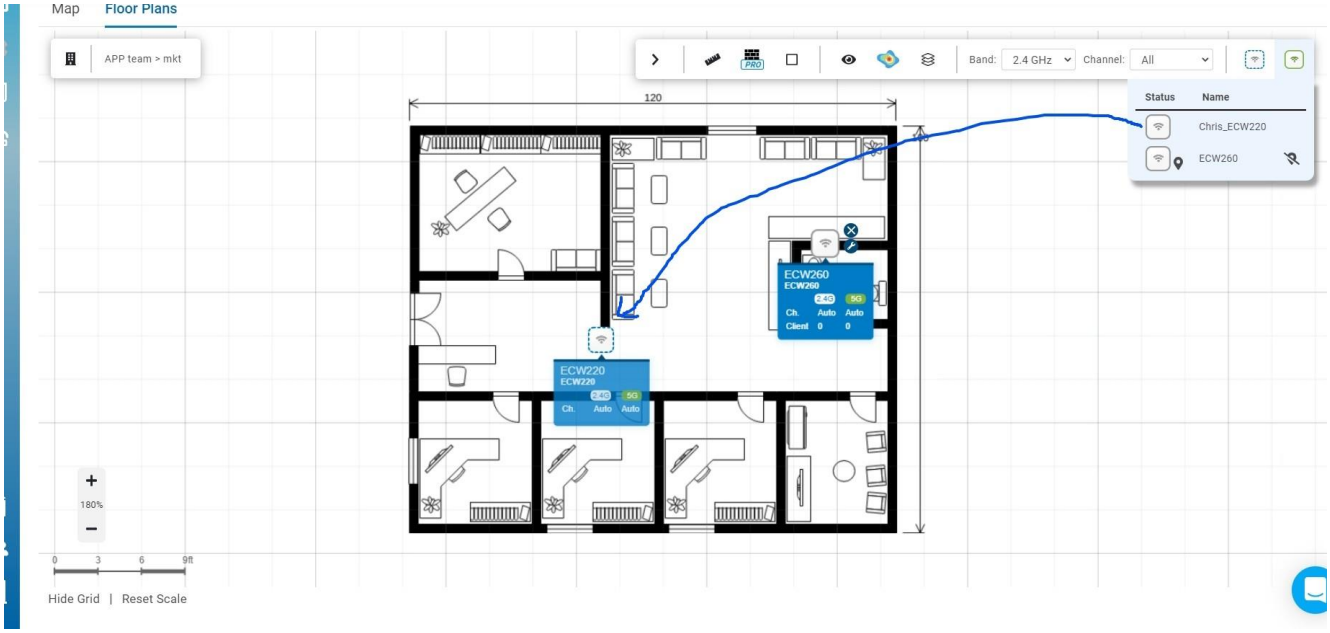


The Tool icon for users to modify the tx power and channel for heat map simulation



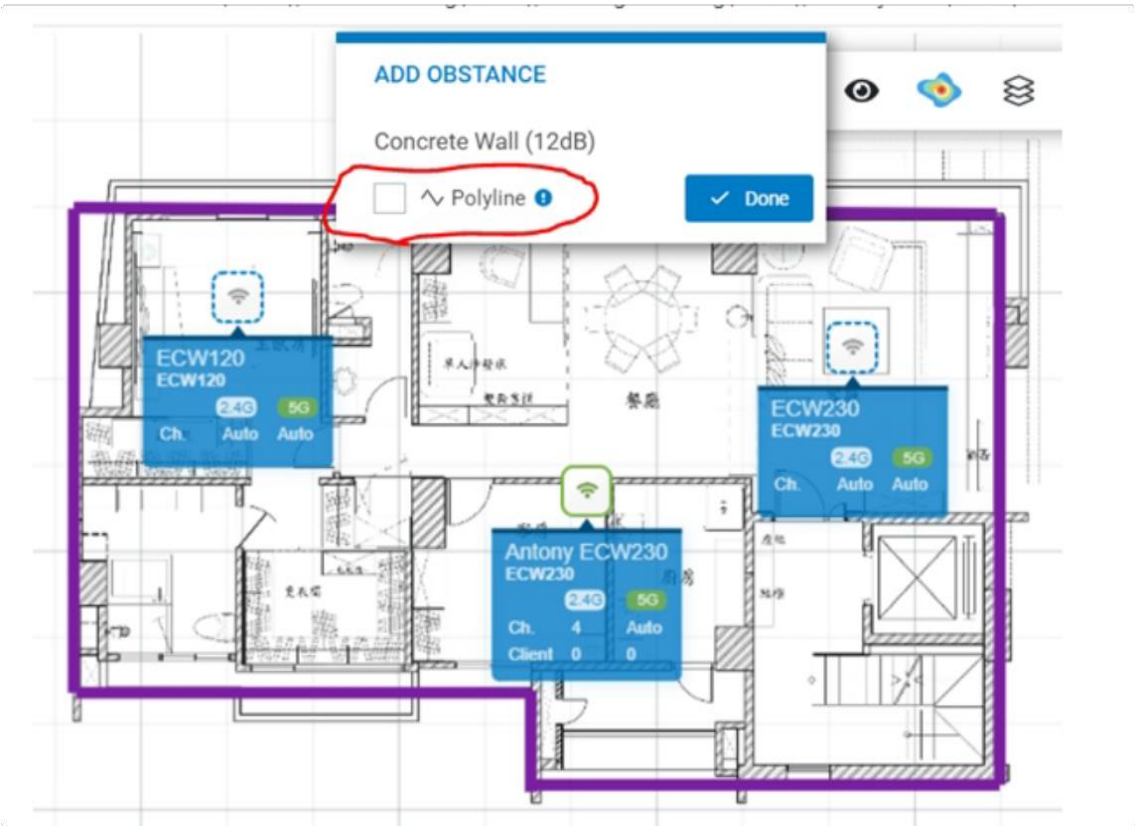
Drag the physical AP to Virtual AP (model needs to be the same) then physical AP could use the Virtual AP configuration.





Polyline in Obstacle

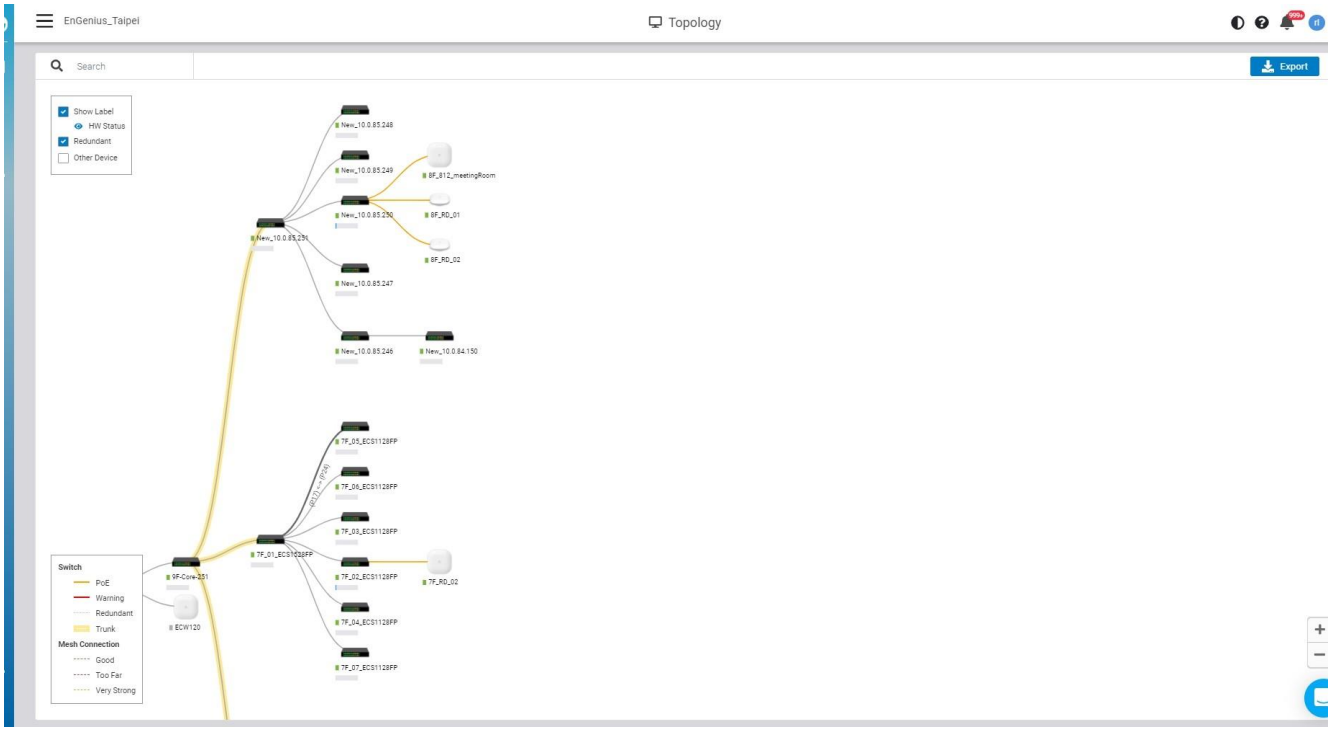
When drawing the walls, users used to draw the line one by one by click “start” and “end” for straight lines, now with the **“Polyline”** option available, users can simply click on the turning point to draw lines quicker.



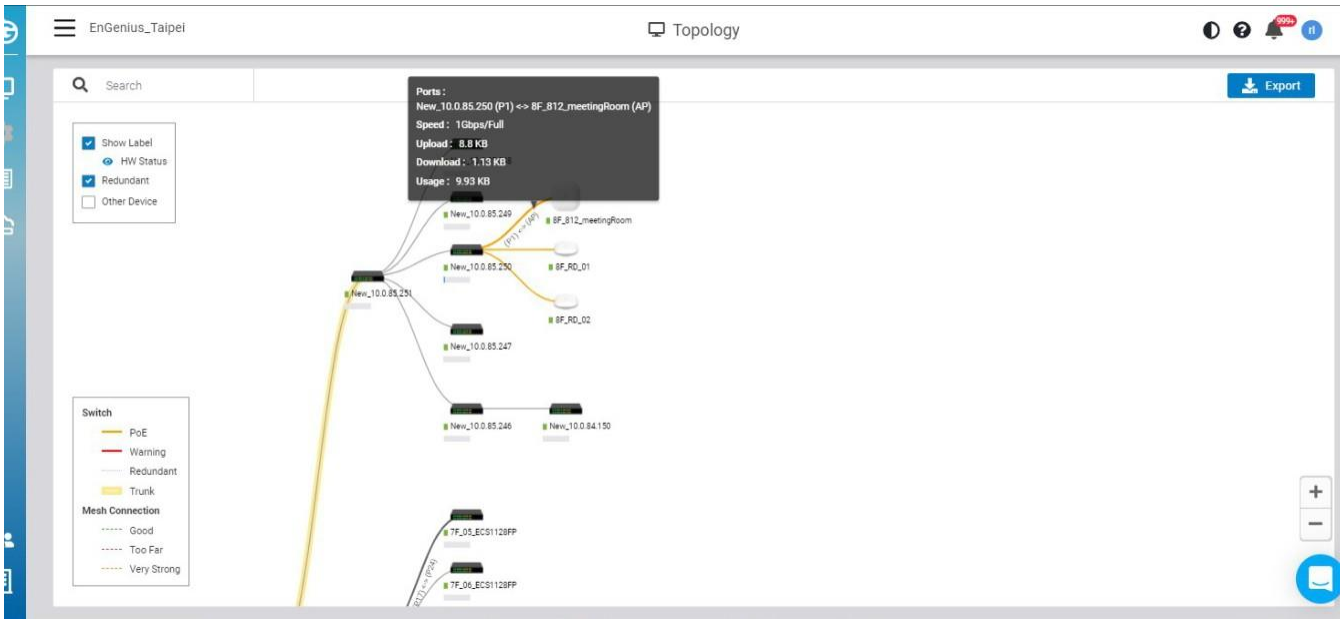
Topology

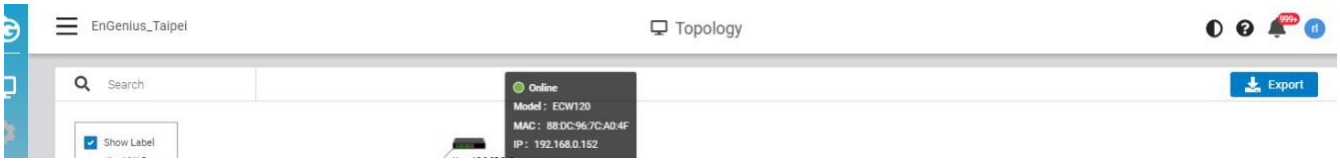
Network topology is a powerful tool to provide administrators a graphic overview of the logical network topology and the status of EnGenius devices.

Use this screen to view the topology of the Org/Network. Click **Manage** > **Topology** to access this screen and double-click the organization/hierarchy view/network on the tree to change the scope.



Learn which physical links in your network are most heavily-trafficked; simply hover over individual network links and devices to learn statistics about that connection's negotiated speed, usage, and a number of directly connected clients using it in the past 5 minutes.





The following describes the functions on this screen:

Show label : Click to display or hide the device name & HW status on each device.

HW status : Click to display or hide the POE Utilization on each switch.

Redundant : Click to display or hide the redundant link .

Other Devices : Click to display the third party devices as well as EWS series devices.

Export : Click to download topology as PDF format .

Configuring Networks

There’s a lot that EnGenius Cloud can do to customize a network to meet your specific needs. We’ll walk you through the most common settings here.

Configuring SSIDs

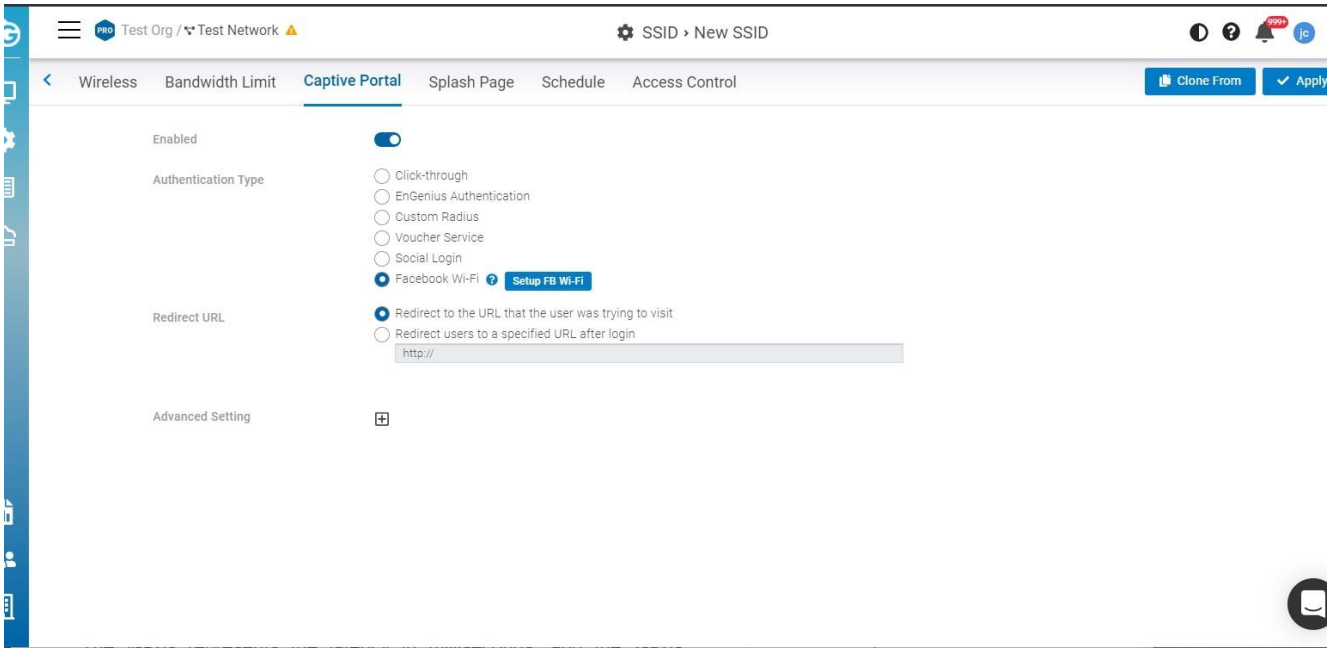
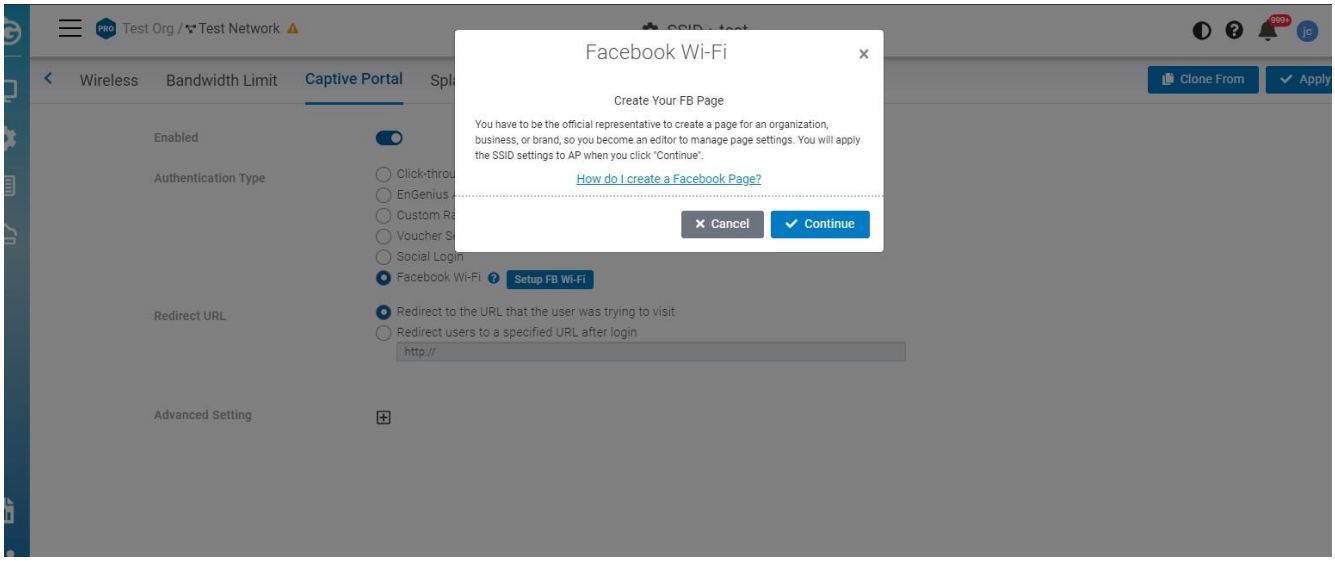
Facebook Wi-Fi

Facebook login provides a social sign-on experience for users logging in to access points. You can use your Facebook page as the sign-in page when they first log in to your network. Users can then check in with their Facebook credentials, update their status, and 'like' the Facebook page.

Configuring EnGenius Wi-Fi with Facebook Login

After creating a Facebook page, Facebook Login is configured on the **Configure** > **SSID** > Click one of the SSID > **Captive Portal** by taking the following step:

1. Select **Facebook Wi-Fi** under the **Authentication Type** section and click the **Setup Facebook Wi-Fi** button**:**



2. Wizard is displayed. Click **Continue** if you have created the Facebook page in advance. If you haven't created it, you could create a Facebook page.