ECW270

User Manual

“This equipment is not suitable for use in locations where children are likely to be present.”

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.

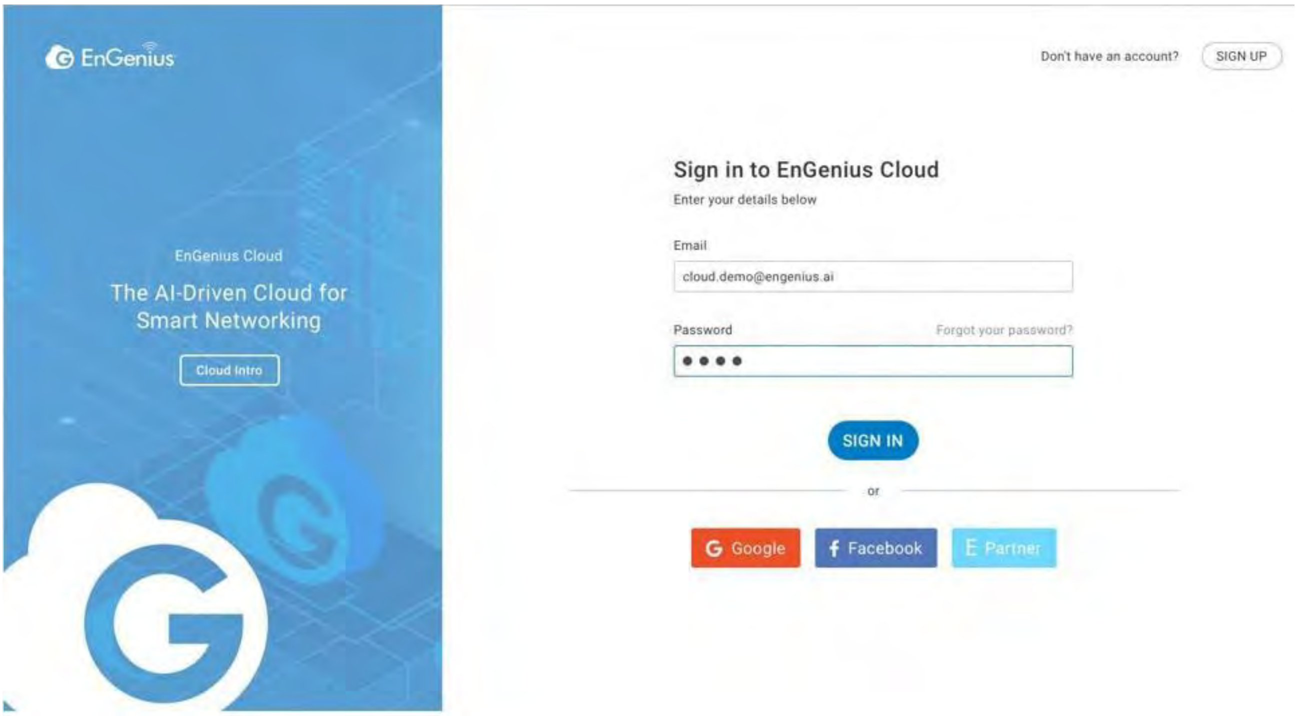
Registering EnGenius Cloud is similar to other web-based platforms and can be done either with a social media account (e.g. Google or Facebook) or by creating an account from scratch. You will need to provide your email address, company name, physical address, and phone number. Furthermore, you must 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 followingsteps:

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



Sign in to EnGenius Cloud

Enter your details below

Email: cloud.demo@engenius.ai

Password: ●●●●

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

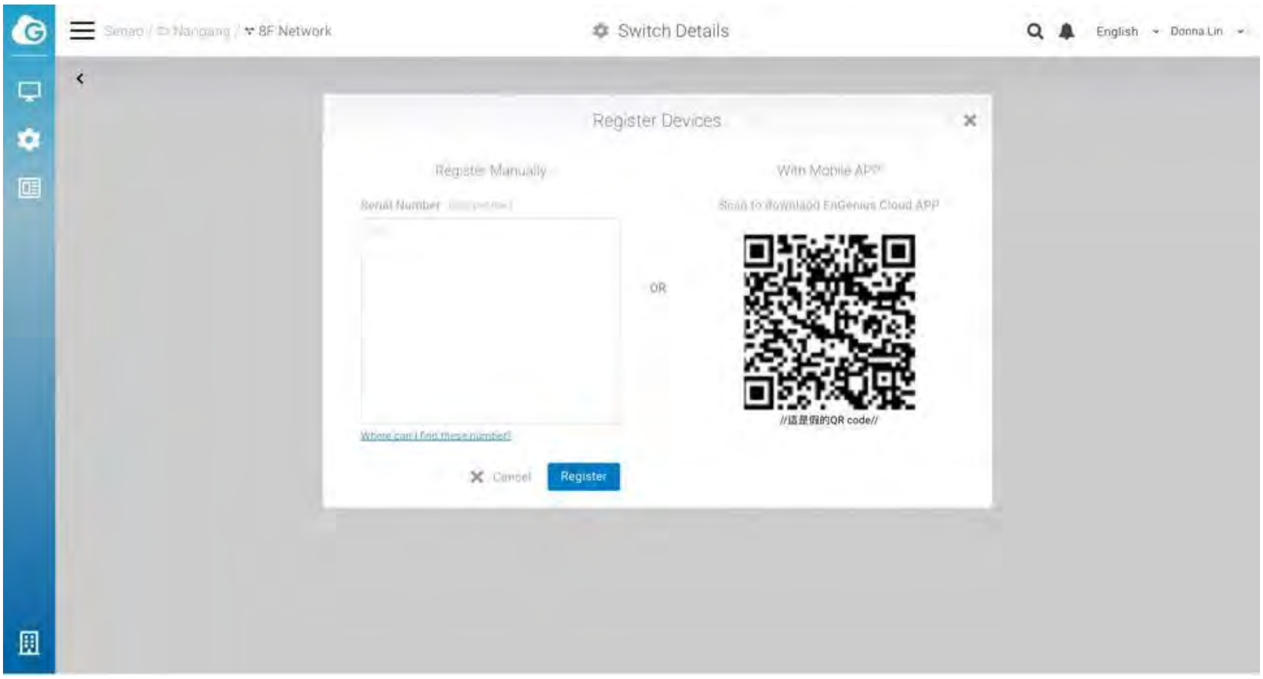
merge your accounts based on the "email address" of the account. For example, if you have created a new account on EnGenius Cloud using the same email address as your google account, then you're able to login to this email account either through Google account authentication with Google account password,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

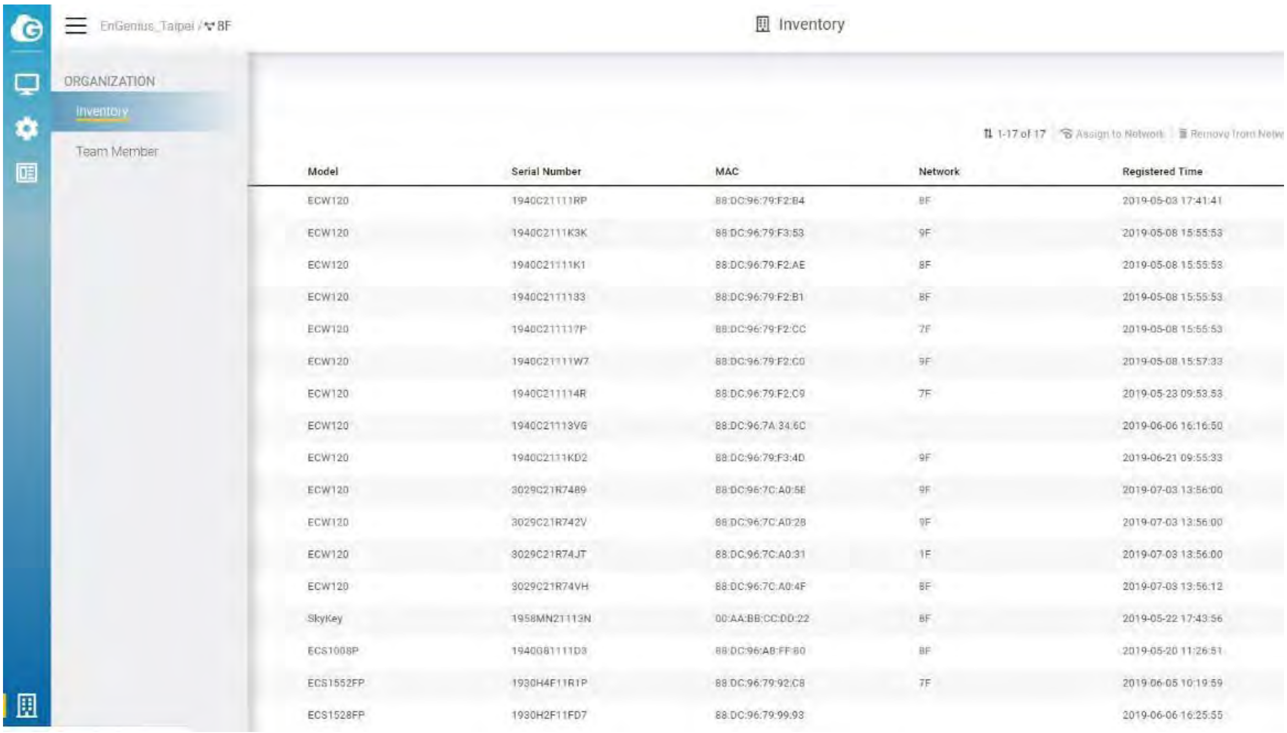


Assigning Devices to Network

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

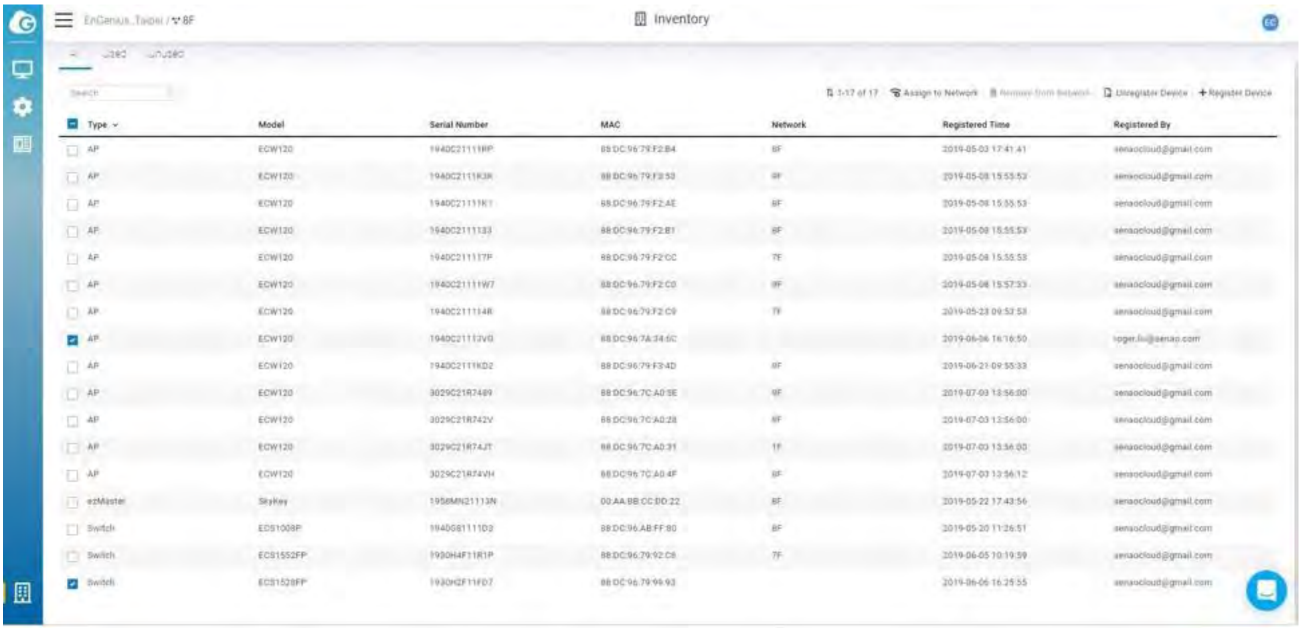
Adding Devices to a Network

1. Navigate to Organization > Inventory.



Model	Serial Number	MAC	Network	Registered Time
ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019-05-03 17:41:41
ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019-05-08 15:55:53
ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019-05-08 15:55:53
ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019-05-08 15:55:53
ECW120	1940C211117P	88:DC:96:79:F2:CC	7F	2019-05-08 15:55:53
ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019-05-08 15:57:33
ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019-05-23 09:53:53
ECW120	1940C21113VG	88:DC:96:7A:34:6C		2019-06-06 16:16:50
ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019-06-21 09:55:33
ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019-07-03 13:56:00
ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019-07-03 13:56:00
ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019-07-03 13:56:00
ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019-07-03 13:56:12
SkyKey	1958MN21113N	00:AA:BB:CC:DD:22	8F	2019-05-22 17:43:56
ECS1008P	1940G81111D3	88:DC:96:AB:FF:60	8F	2019-05-20 11:26:51
ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019-06-05 10:19:59
ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019-06-06 16:25:55

2. Select one or multiple devices as required.



EnGenius_Taipei / 8F

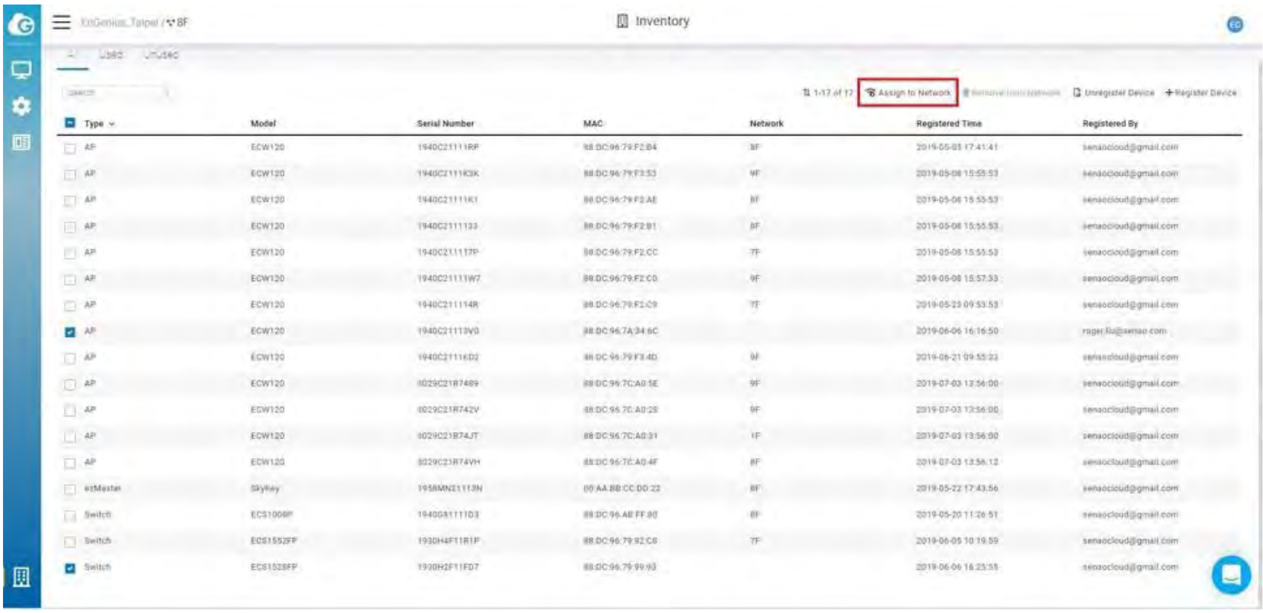
Inventory

All Used Unused

1-17 of 17 | Assign to Network | Remove from Network | Unregister Device | + Register Device

	Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
□	AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019-05-03 17:41:41	senaocloud@gmail.com
□	AP	ECW120	1940C2111K3R	88:DC:96:79:F3:53	9F	2019-05-08 15:53:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C211117P	88:DC:96:79:F2:CC	7F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019-05-08 15:57:33	senaocloud@gmail.com
□	AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019-05-23 09:53:53	senaocloud@gmail.com
☑	AP	ECW120	1940C21113VG	88:DC:96:7A:34:6C		2019-06-06 16:16:50	roger.liu@senao.com
□	AP	ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019-06-21 09:55:33	senaocloud@gmail.com
□	AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019-07-03 13:56:12	senaocloud@gmail.com
□	ezMaster	SkyKey	1958MN21113N	00:AA:BB:CC:DD:22	8F	2019-05-22 17:43:56	senaocloud@gmail.com
□	Switch	ECS1008P	1940G81111D3	88:DC:96:AB:FF:80	8F	2019-05-20 11:26:51	senaocloud@gmail.com
□	Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019-06-05 10:19:59	senaocloud@gmail.com
☑	Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019-06-06 16:25:55	senaocloud@gmail.com

3. Click Assign to Network.



EnGenius_Taipei / 8F

Inventory

All Used Unused

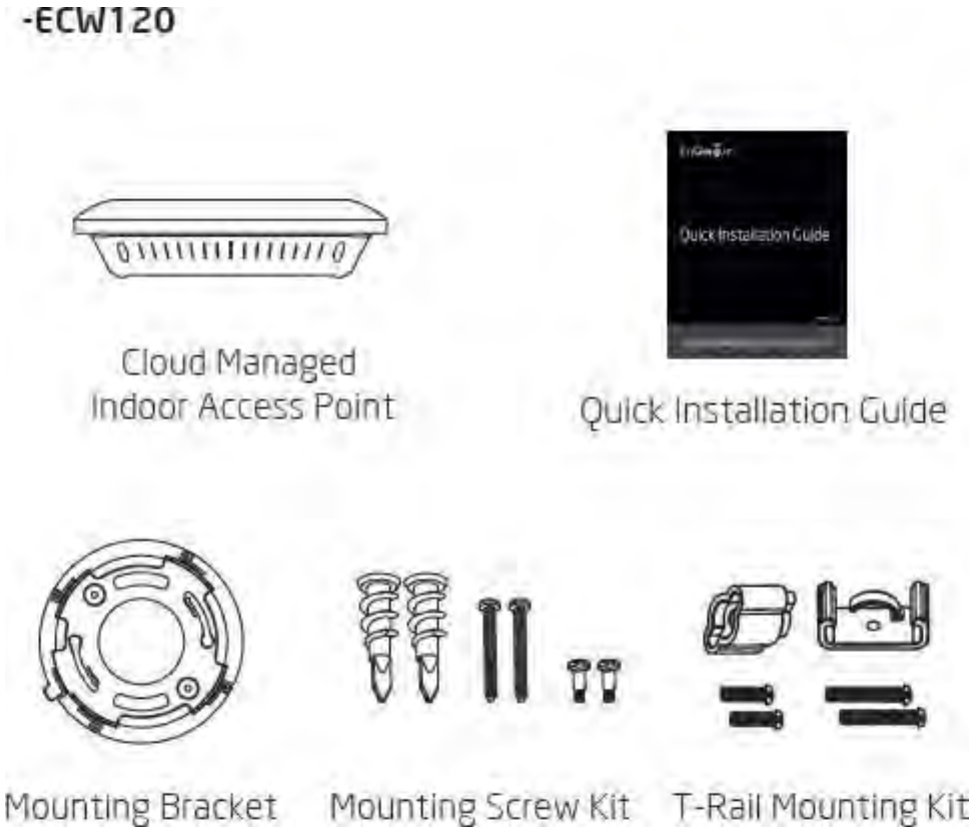
1-17 of 17 | Assign to Network | Remove from Network | Unregister Device | + Register Device

	Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
□	AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019-05-03 17:41:41	senaocloud@gmail.com
□	AP	ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C211117P	88:DC:96:79:F2:CC	7F	2019-05-08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019-05-08 15:57:33	senaocloud@gmail.com
□	AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019-05-23 09:53:53	senaocloud@gmail.com
☑	AP	ECW120	1940C21113VG	88:DC:96:7A:34:6C		2019-06-06 16:16:50	roger.liu@senao.com
□	AP	ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019-06-21 09:55:33	senaocloud@gmail.com
□	AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019-07-03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019-07-03 13:56:12	senaocloud@gmail.com
□	ezMaster	SkyKey	1958MN21113N	00:AA:BB:CC:DD:22	8F	2019-05-22 17:43:56	senaocloud@gmail.com
□	Switch	ECS1008P	1940G81111D3	88:DC:96:AB:FF:80	8F	2019-05-20 11:26:51	senaocloud@gmail.com
□	Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019-06-05 10:19:59	senaocloud@gmail.com
☑	Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019-06-06 16:25:55	senaocloud@gmail.com

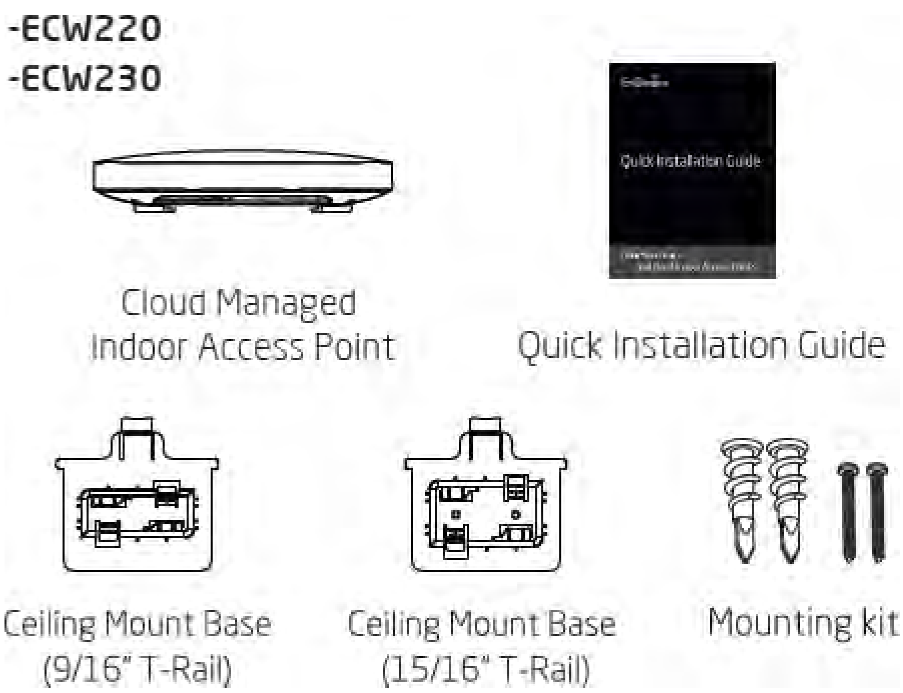
Device Setup

ECW AP Installation

ECW AP Package Contents

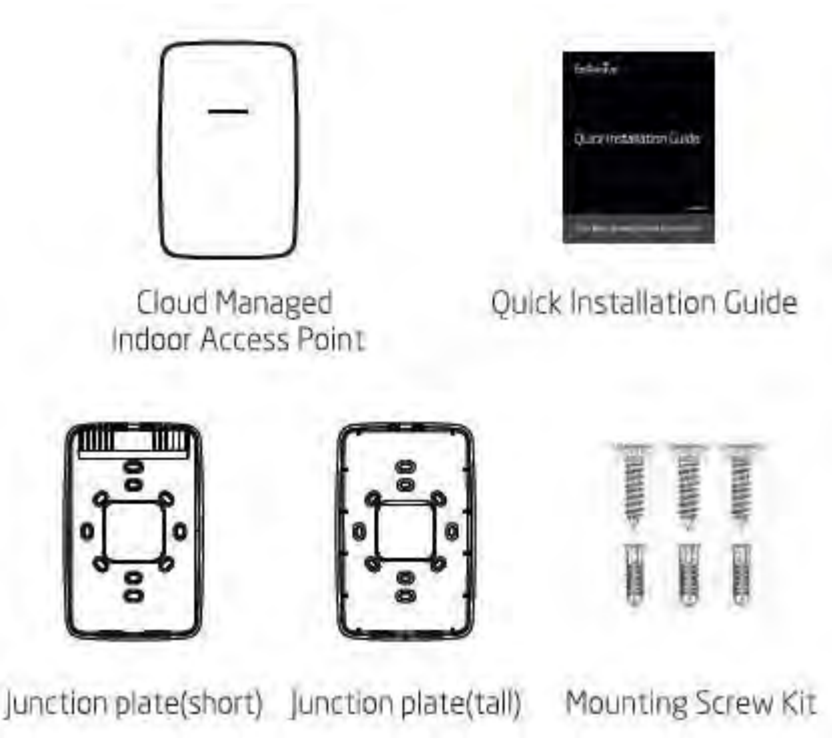


ECW120 Package Contents


-ECW220
-ECW230
Quick Installation Guide
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

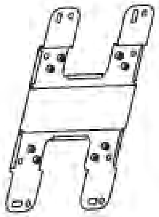


ECW115 Package Contents

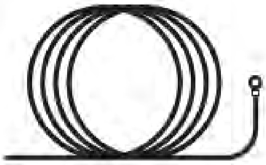
-ECW270

Access Point

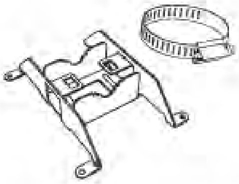
Quick Installation Guide



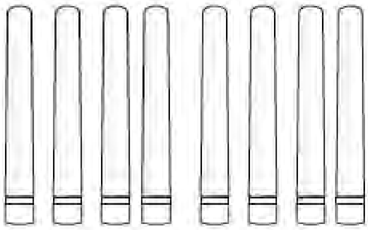
Wall Mounting Kit



Ground Cable



Pole Mounting Kit



2.4 GHz Detachable Antennas **x 4**
5 GHz Detachable Antennas **x 4**

Minimum Access Requirement

Power source option - An ECW AP device can be powered by an 802.3af/at/bt-compliant PoE device or by DC12V /54V input

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

Ethernet port:

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

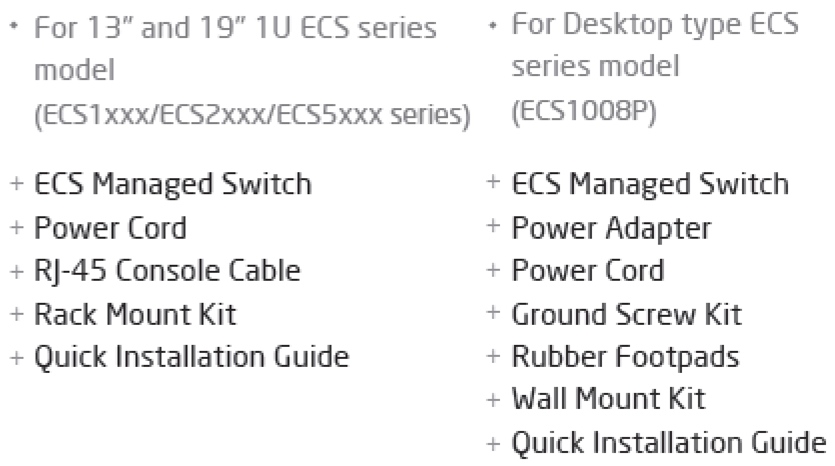
Connect the AP to Internet:

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)

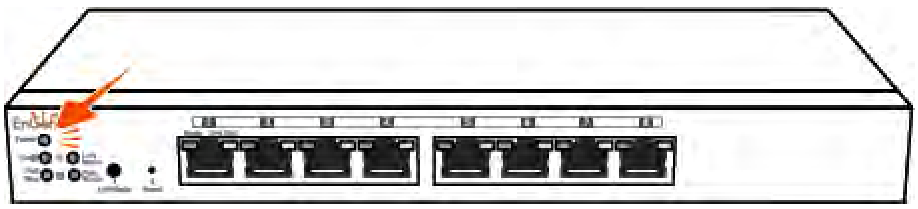
+ ECS Managed Switch
+ Power Cord
+ RJ-45 Console Cable
+ Rack Mount Kit
+ Quick Installation Guide

- For Desktop type ECS series model (ECS1008P)

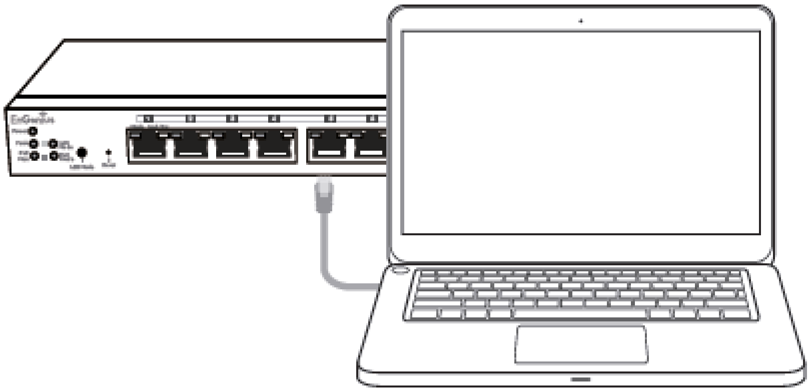
+ ECS Managed Switch
+ Power Adapter
+ Power Cord
+ Ground Screw Kit
+ Rubber Footpads
+ Wall Mount Kit
+ Quick Installation Guide

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.



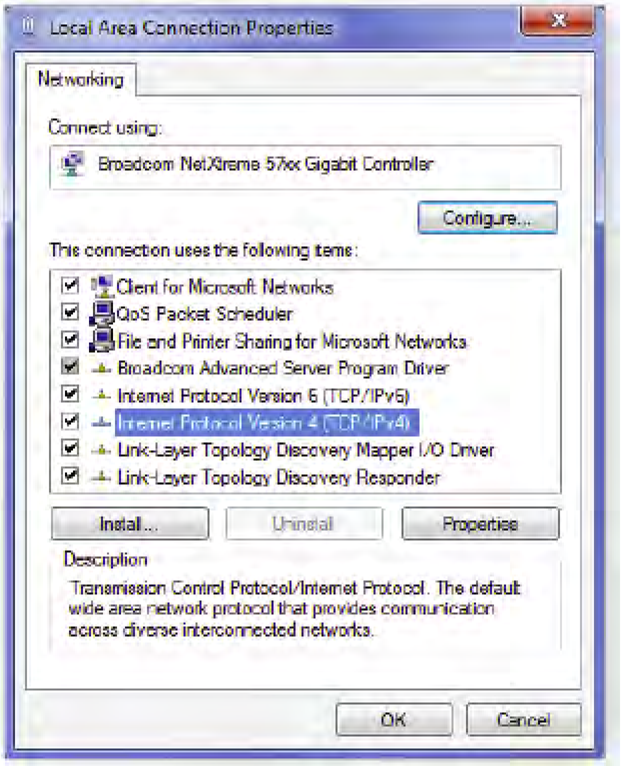
Login to the ECS Switch Local Access Page

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



Local Area Connection Properties

Networking

Connect using:

Broadcom NetXtreme 57xx Gigabit Controller

This connection uses the following items:

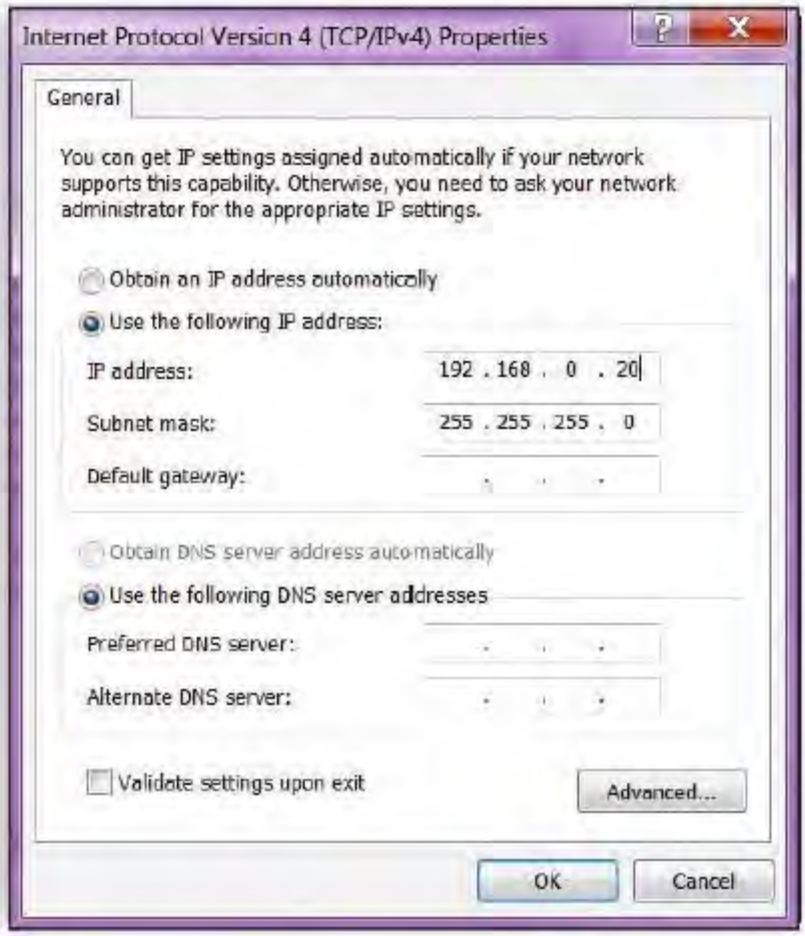
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Broadcom Advanced Server Program Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer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

Description

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

B) 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



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

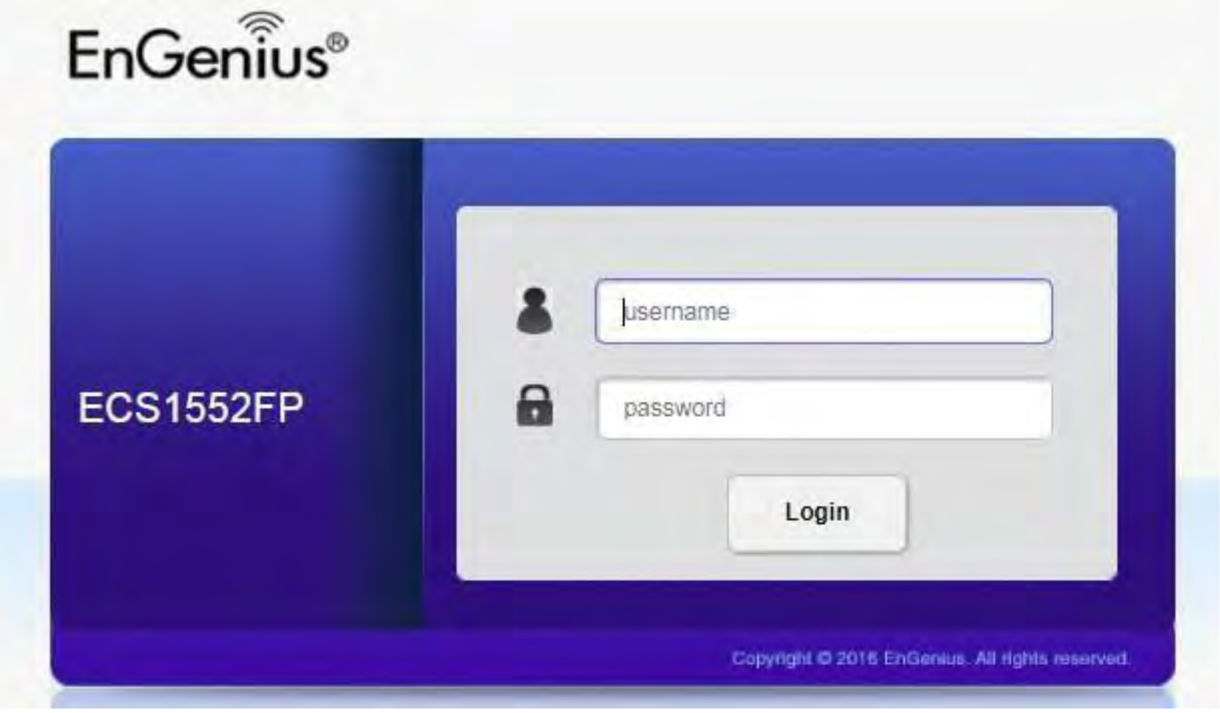
□ Validate settings upon exit

Login to ECS Switch

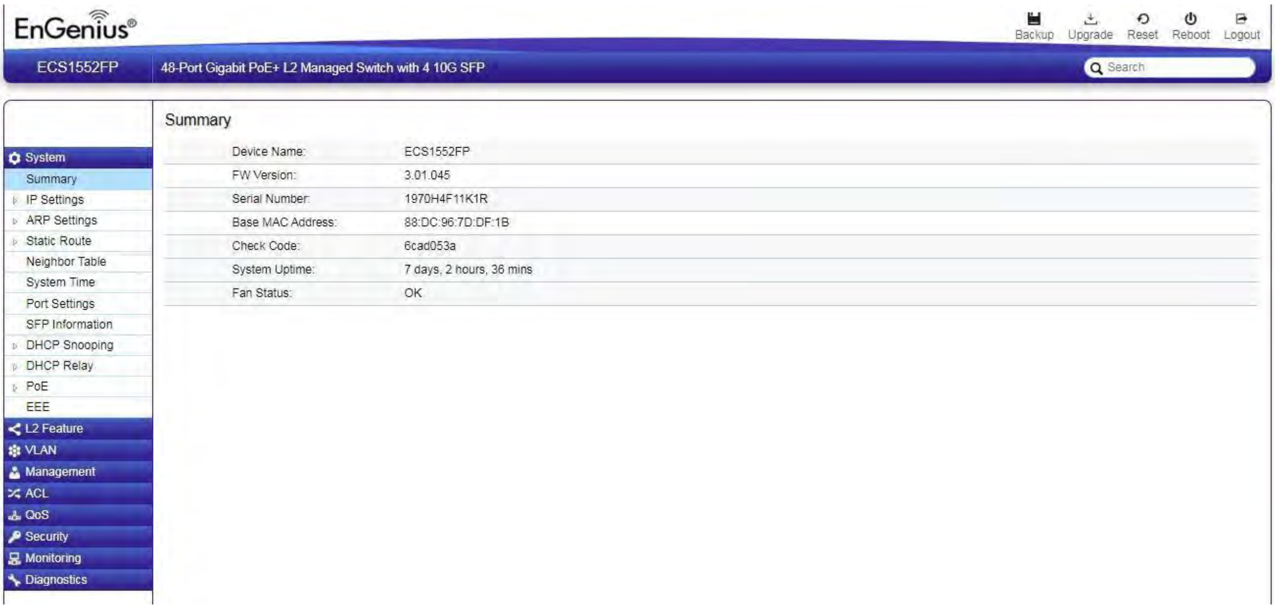
A) Open a web browser on your computer. In the address bar of the web browser, enter the ECS switch IP address and hit enter.

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.



Summary

Device Name:	ECS1552FP
FW Version:	3.01.045
Serial Number:	1970H4F11K1R
Base MAC Address:	88:DC:96:7D:DF:1B
Check Code:	6cad053a
System Uptime:	7 days, 2 hours, 36 mins
Fan Status:	OK

> ⓘ 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

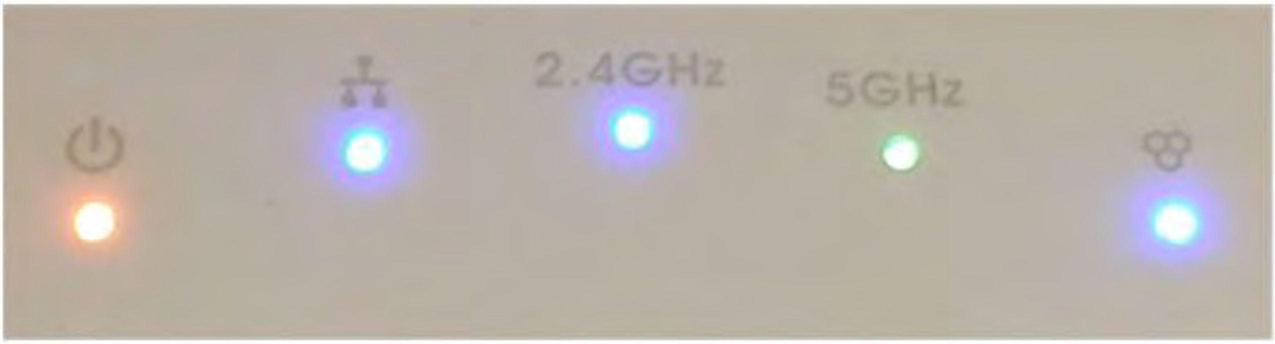
1. Check for available wireless networks (Check if a known default SSID is being broadcast).

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

Mesh Enabled	Mesh LED 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!

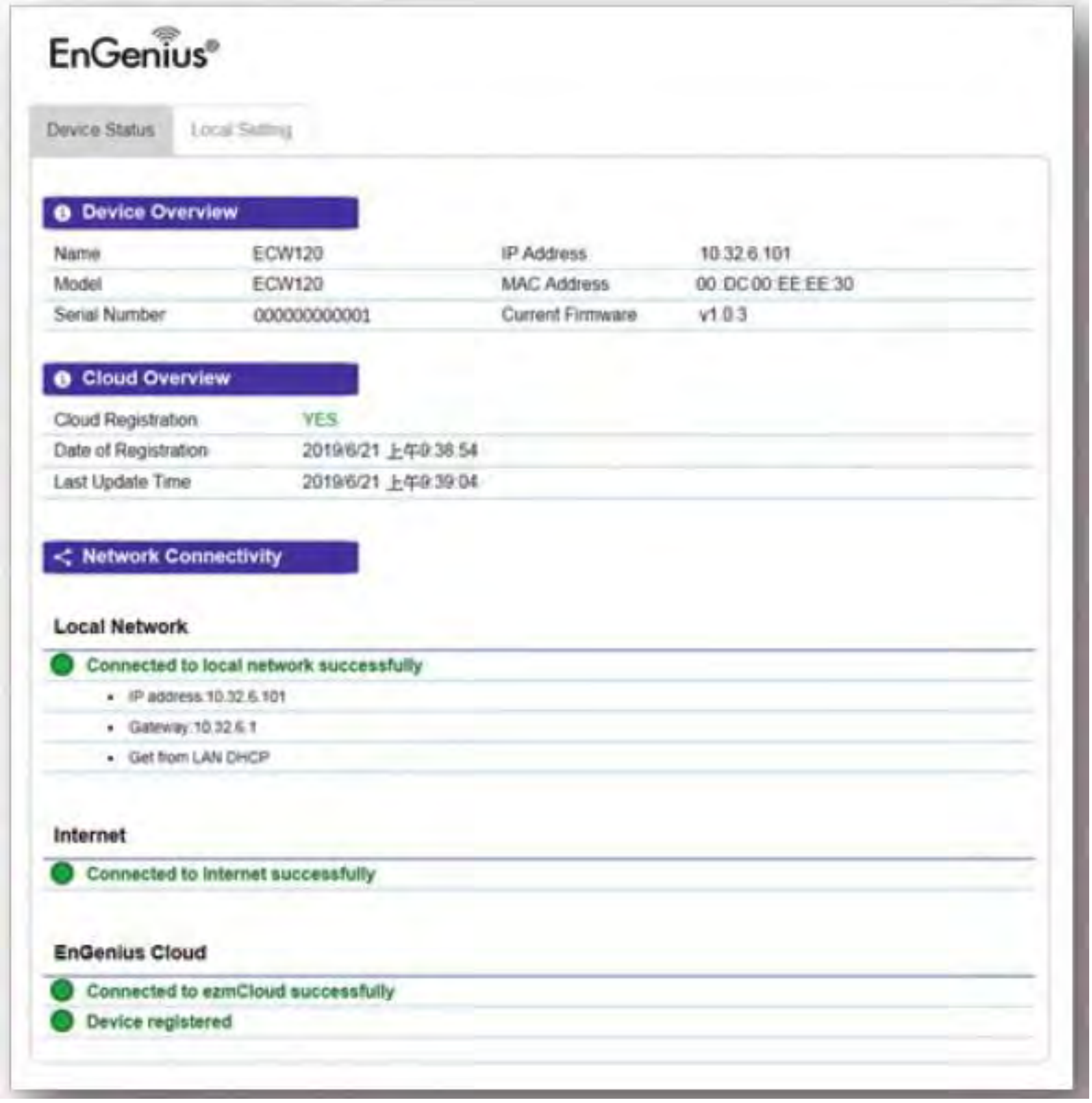
EnMGMTxxxx

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:



Device Overview

Name	ECW120	IP Address	10.32.6.101
Model	ECW120	MAC Address	00:DC:00:EE:EE:30
Serial Number	000000000001	Current Firmware	v1.0.3

Cloud Overview

Cloud Registration	YES
Date of Registration	2019/6/21 上午9:38:54
Last Update Time	2019/6/21 上午9:39:04

Network Connectivity

Local Network

● Connected to local network successfully

- IP address:10.32.6.101
- Gateway:10.32.6.1
- Get from LAN DHCP

Internet

● Connected to Internet successfully

EnGenius Cloud

● Connected to ezmCloud successfully

● Device registered

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.

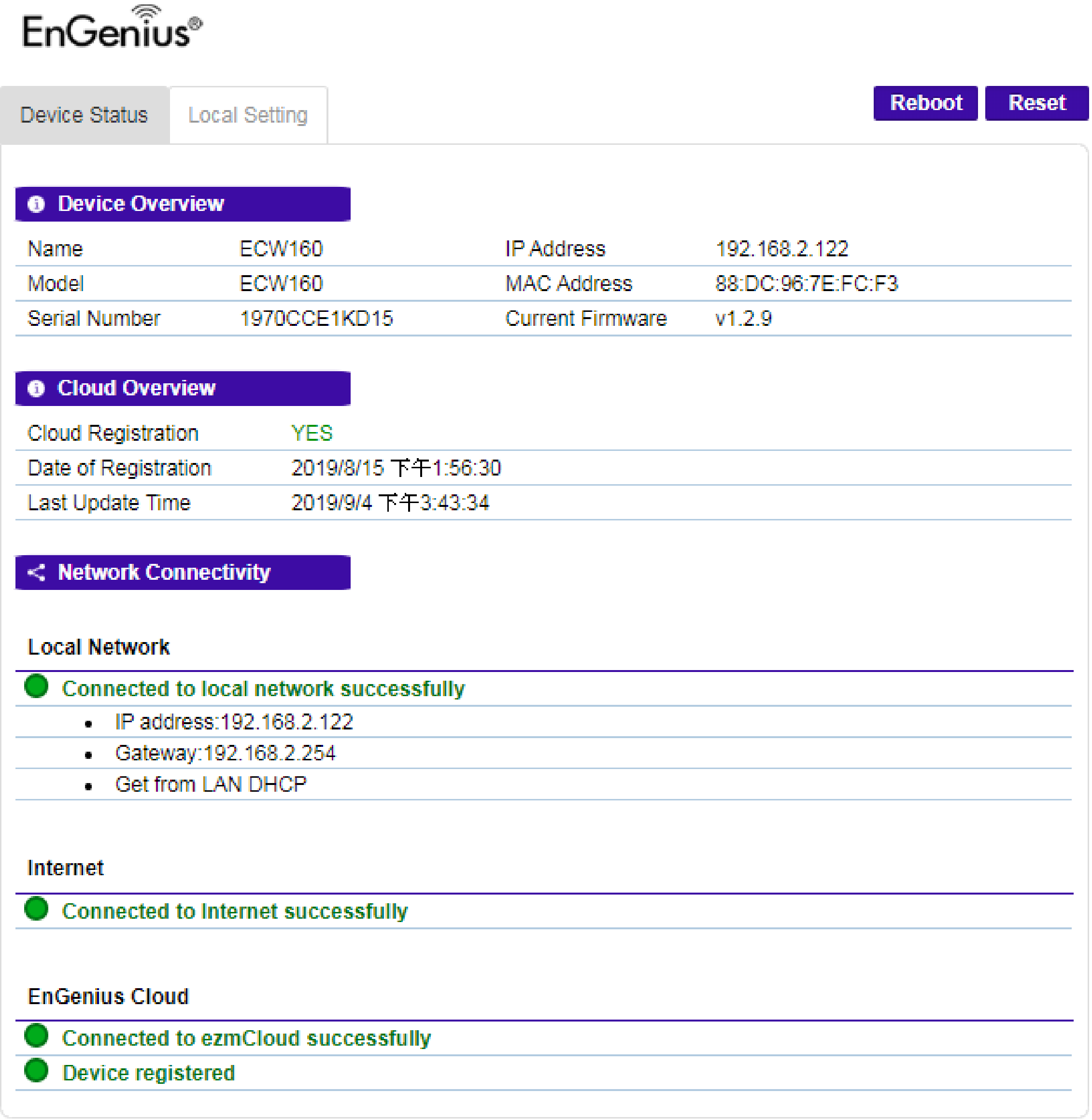
Local Access Page Options

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 Overview

Name	ECW160	IP Address	192.168.2.122
Model	ECW160	MAC Address	88:DC:96:7E:FC:F3
Serial Number	1970CCE1KD15	Current Firmware	v1.2.9

Cloud Overview

Cloud Registration	YES
Date of Registration	2019/8/15 下午1:56:30
Last Update Time	2019/9/4 下午3:43:34

Network Connectivity

Local Network

● Connected to local network successfully

- IP address:192.168.2.122
- Gateway:192.168.2.254
- Get from LAN DHCP

Internet

● Connected to Internet successfully

EnGenius Cloud

● Connected to ezmCloud successfully

● Device registered

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

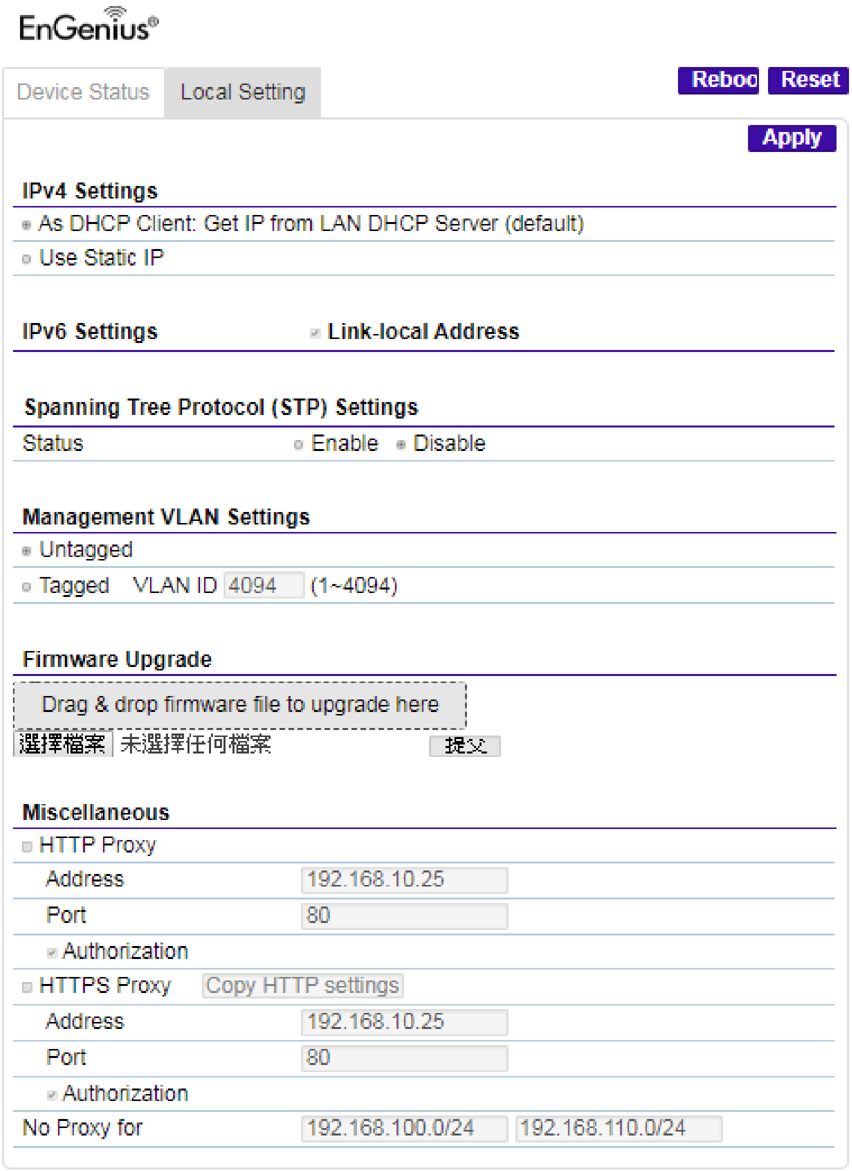
Provides information about the Cloud registration status, date of registration, and time of last update.

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.



IPv4 Settings

● As DHCP Client: Get IP from LAN DHCP Server (default)

○ Use Static IP

IPv6 Settings ☑ **Link-local Address**

Spanning Tree Protocol (STP) Settings

Status ○ Enable ● Disable

Management VLAN Settings

● Untagged

○ Tagged VLAN ID 4094 (1~4094)

Firmware Upgrade

Drag & drop firmware file to upgrade here

選擇檔案 未選擇任何檔案 提交

Miscellaneous

□ HTTP Proxy

Address	192.168.10.25
Port	80
☑ Authorization	

□ HTTPS Proxy Copy HTTP settings

Address	192.168.10.25
Port	80
☑ Authorization	
No Proxy for	192.168.100.0/24 192.168.110.0/24

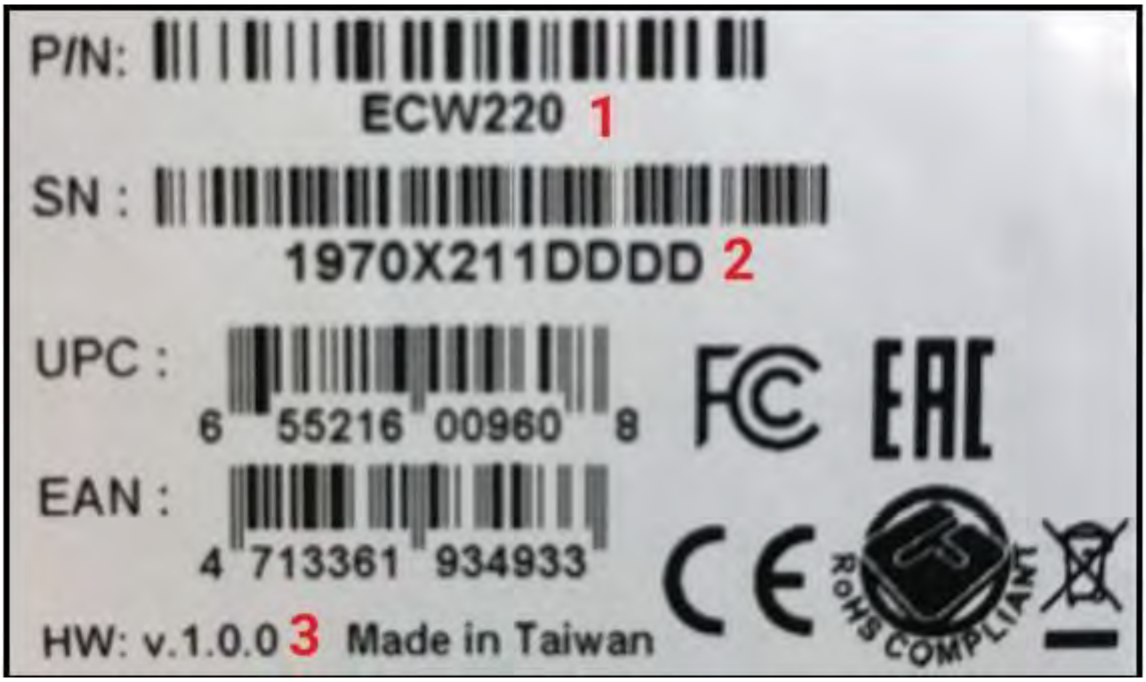
Local Setting on Local Access page

ⓘ 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:



P/N: ECW220

SN : 1970X211DDDD

UPC : 6 55216 00960 8

EAN : 4 713361 934933

HW: v.1.0.0 Made in Taiwan

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)

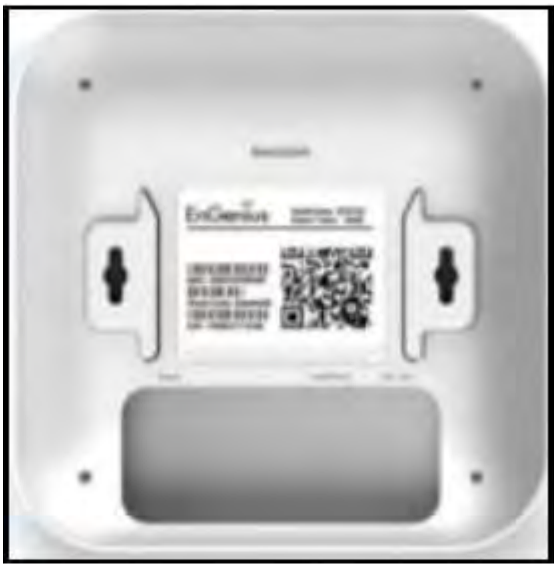
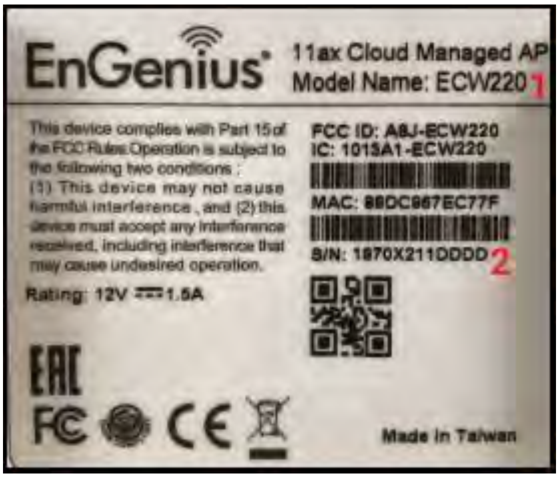


Fig 2: Back of AP

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



EnGenius

11ax Cloud Managed AP
Model Name: ECW220

This device complies with Part 15 of the FCC Rules.Operation is subject to the following two conditions : (1) This device may not cause harmful interference , and (2) this device must accept any interference received, including interference that may cause undesired operation.

Rating: 12V ⎓ 1.5A

FCC ID: A8J-ECW220
IC: 1013A1-ECW220
MAC: 88DC967EC77F
S/N: 1970X211DDDD

Made in Taiwan

Fig 3: Sticker on back of ECW AP

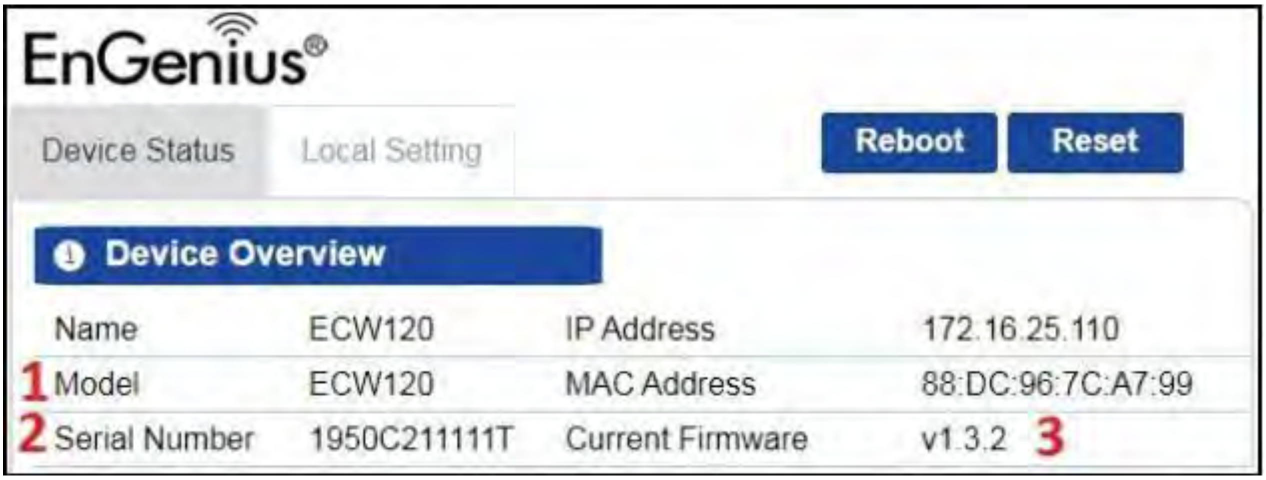
As you can see the sticker on the back of the AP has the MAC address of the AP as well. It has the following items:

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.



Name	ECW120	IP Address	172.16.25.110
Model	ECW120	MAC Address	88:DC:96:7C:A7:99
Serial Number	1950C211111T	Current Firmware	v1.3.2

Fig 4: Local Login information

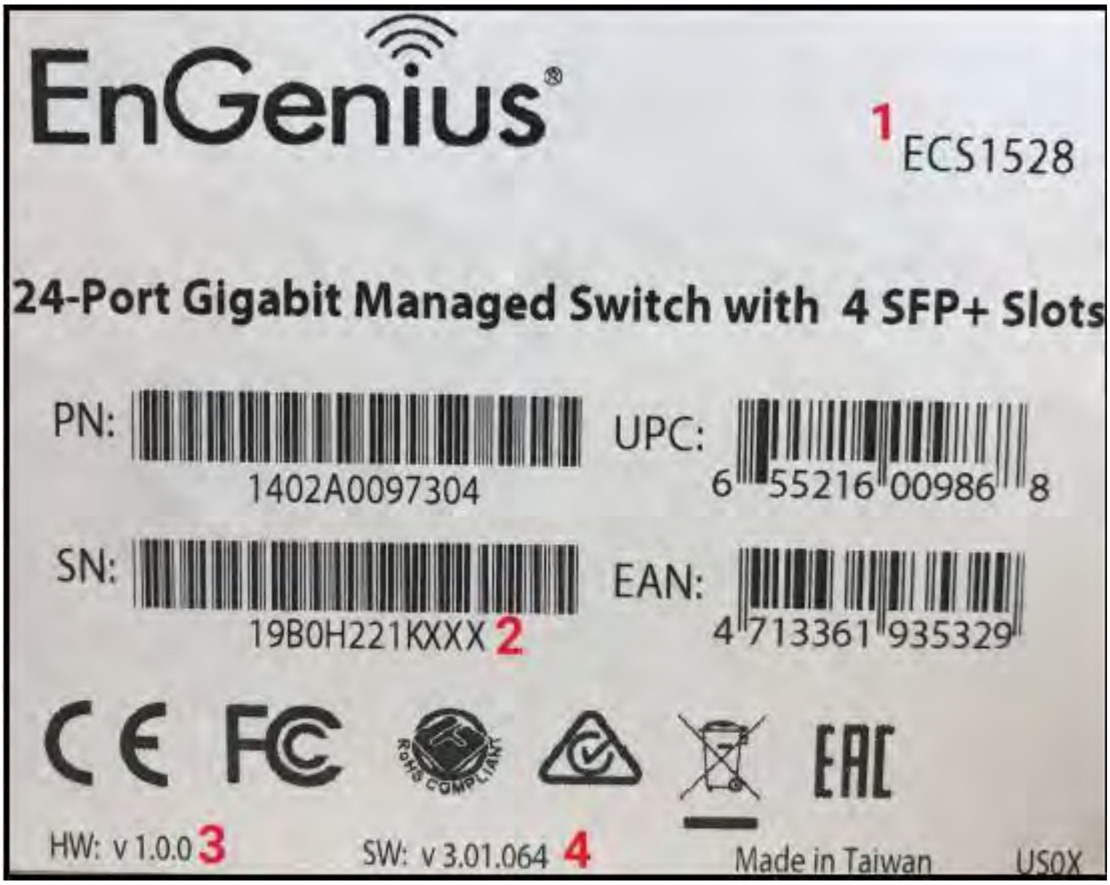
1. Model of the AP

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



EnGenius®

1 ECS1528

24-Port Gigabit Managed Switch with 4 SFP+ Slots

PN: 1402A0097304

UPC: 6 55216 00986 8

SN: 19B0H221KXXX 2

EAN: 4 713361 935329

HW: v 1.0.0 3

SW: v 3.01.064 4

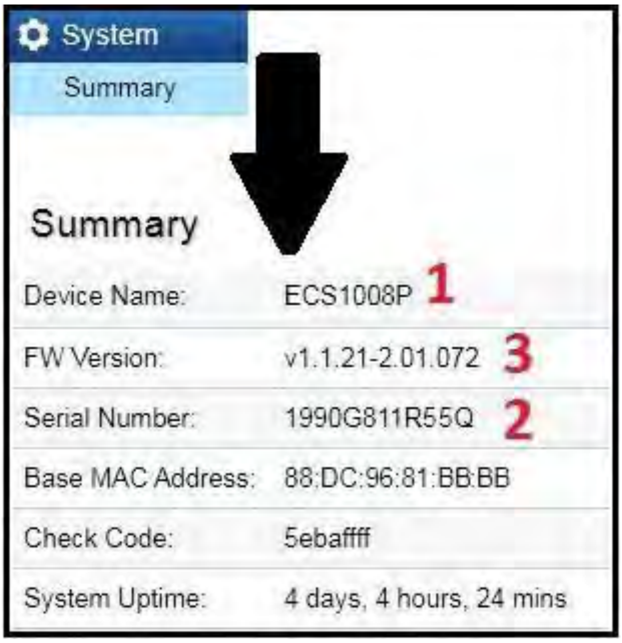
Made in Taiwan

US0X

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.



Summary

Device Name:	ECS1008P
FW Version:	v1.1.21-2.01.072
Serial Number:	1990G811R55Q
Base MAC Address:	88:DC:96:81:BB:BB
Check Code:	5ebaffff
System Uptime:	4 days, 4 hours, 24 mins

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

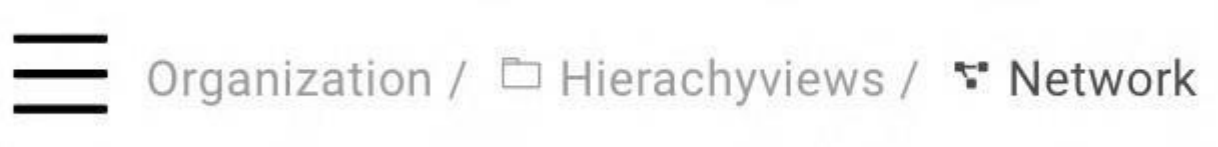
Working with Organization Trees

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:

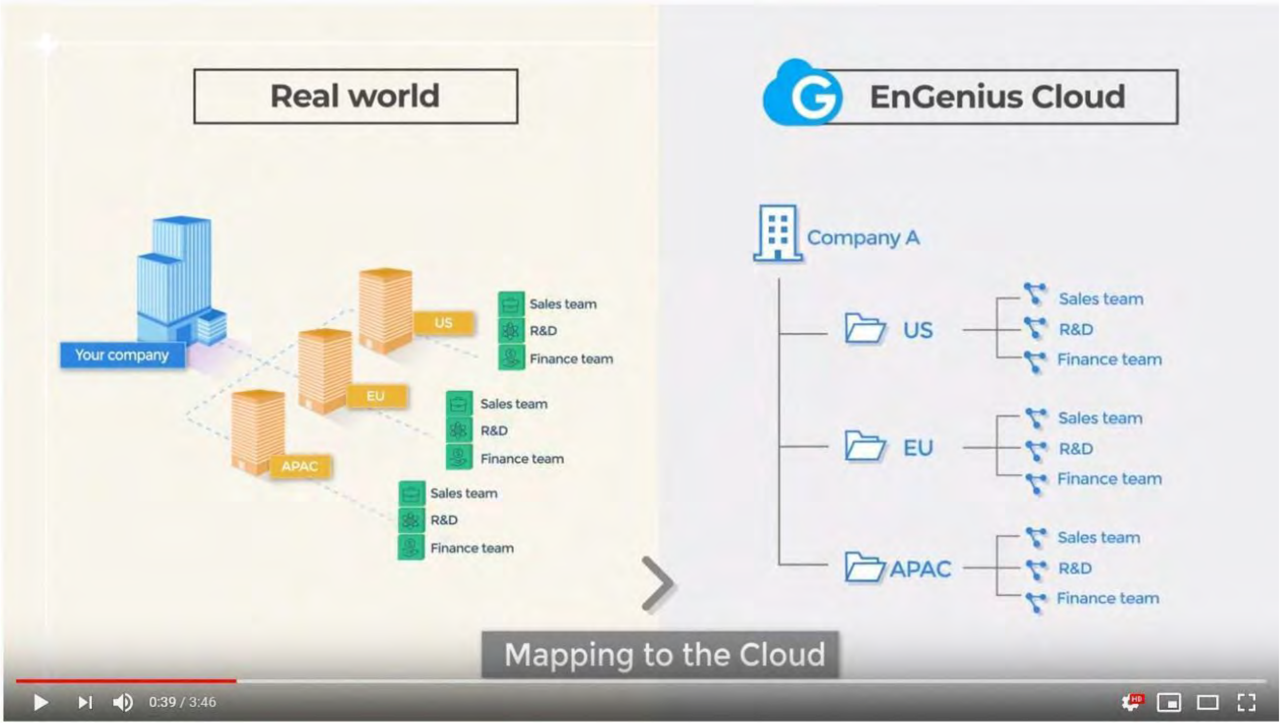
- Organization - A grouping of one or more hierarchies under the umbrella of a single license.
- Hierarchy View - A cluster of networks, which may be geographically concentrated or spread out.
- Network - A set of network devices united by a single configuration set.

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



Real world

EnGenius Cloud

Mapping to the Cloud

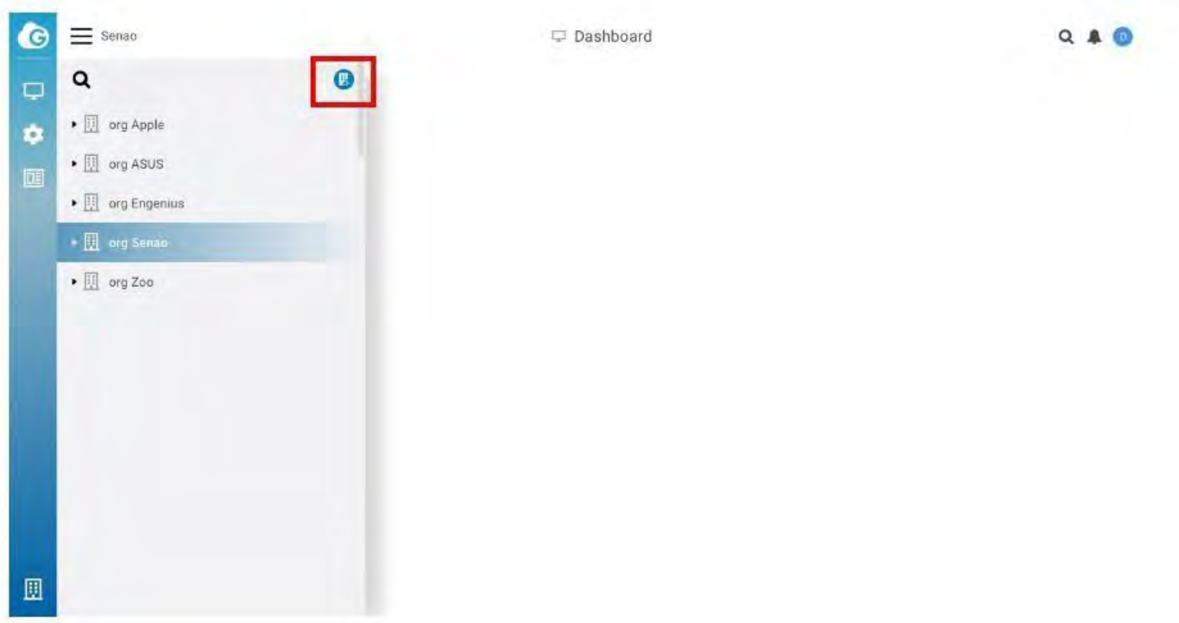
https:/ www.youtube.com/watch?v=sN2y44Yzi7s&feature=youtu.be&t=5

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

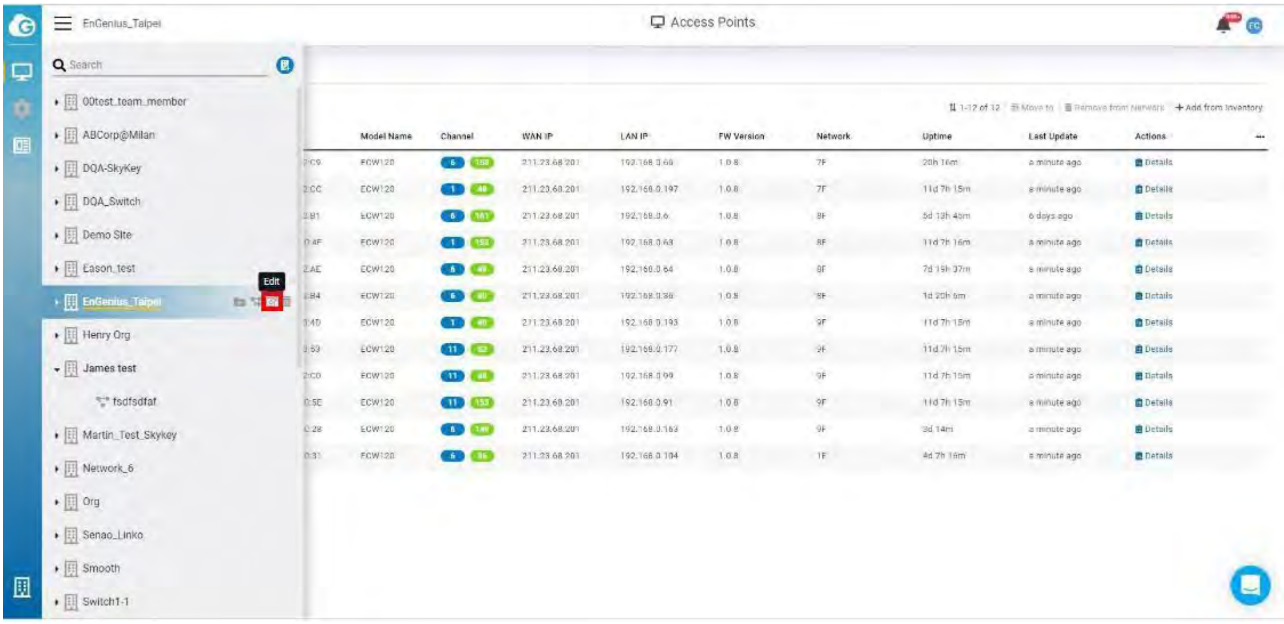


Edit Organization

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



EnGenius_Taipei

Access Points

Search

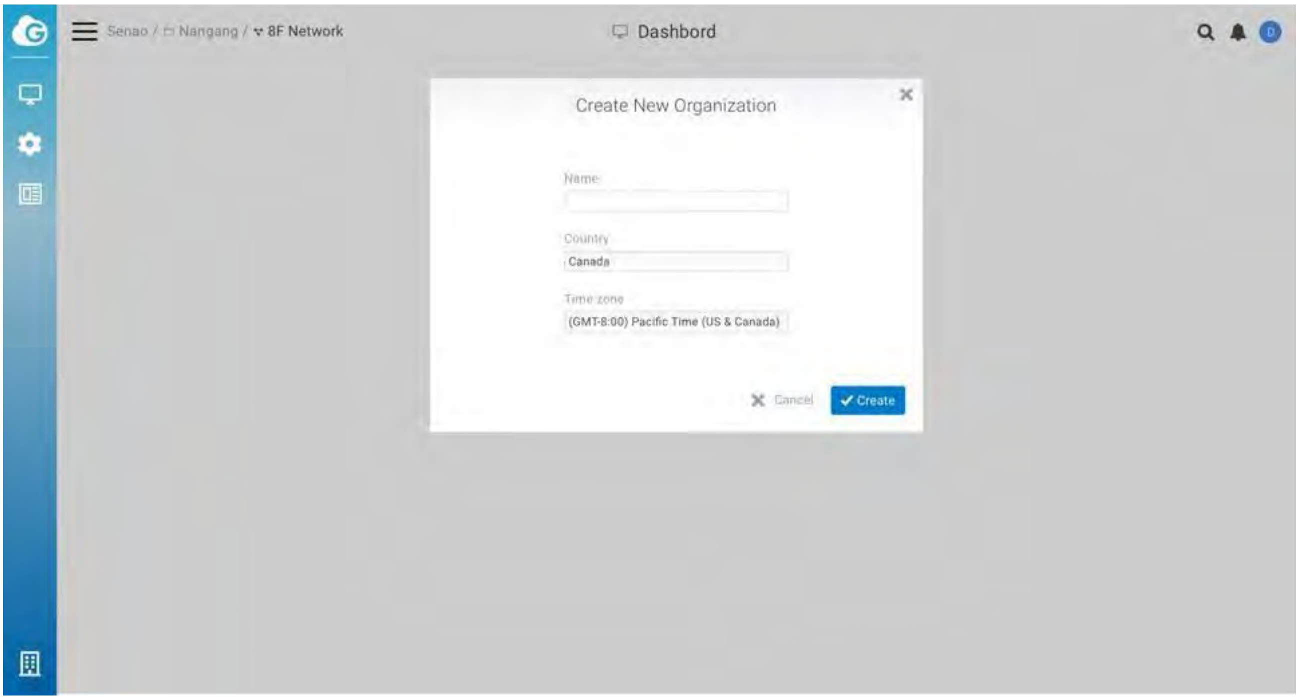
- 00test_team_member
- ABCorp@Milan
- DQA-SkyKey
- DQA_Switch
- Demo Site
- Eason_test
- EnGenius_Taipei
- Henry Org
- James test
  - fsdfsdfaf
- Martin_Test_Skykey
- Network_6
- Org
- Senao_Linko
- Smooth
- Switch1-1

Edit

1-12 of 12 Move to Remove from Network + Add from Inventory

	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
:C9	ECW120	6 153	211.23.68.201	192.168.0.60	1.0.8	7F	20h 16m	a minute ago	Details
:CC	ECW120	1 48	211.23.68.201	192.168.0.197	1.0.8	7F	11d 7h 15m	a minute ago	Details
:B1	ECW120	6 161	211.23.68.201	192.168.0.6	1.0.8	8F	5d 13h 45m	6 days ago	Details
:4F	ECW120	1 153	211.23.68.201	192.168.0.63	1.0.8	8F	11d 7h 16m	a minute ago	Details
:AE	ECW120	6 48	211.23.68.201	192.168.0.64	1.0.8	8F	7d 19h 37m	a minute ago	Details
:B4	ECW120	6 40	211.23.68.201	192.168.0.36	1.0.8	8F	1d 20h 6m	a minute ago	Details
:4D	ECW120	1 40	211.23.68.201	192.168.0.193	1.0.8	9F	11d 7h 15m	a minute ago	Details
:53	ECW120	11 52	211.23.68.201	192.168.0.177	1.0.8	9F	11d 7h 15m	a minute ago	Details
:C0	ECW120	11 48	211.23.68.201	192.168.0.99	1.0.8	9F	11d 7h 15m	a minute ago	Details
:5E	ECW120	11 153	211.23.68.201	192.168.0.91	1.0.8	9F	11d 7h 15m	a minute ago	Details
:28	ECW120	6 149	211.23.68.201	192.168.0.163	1.0.8	9F	3d 14m	a minute ago	Details
:31	ECW120	6 36	211.23.68.201	192.168.0.104	1.0.8	1F	4d 7h 16m	a minute ago	Details

2. Update Network Settings as required



Senao / Nangang / 8F Network

Dashbord

Create New Organization

Name:

Country: Canada

Time zone: (GMT-8:00) Pacific Time (US & Canada)

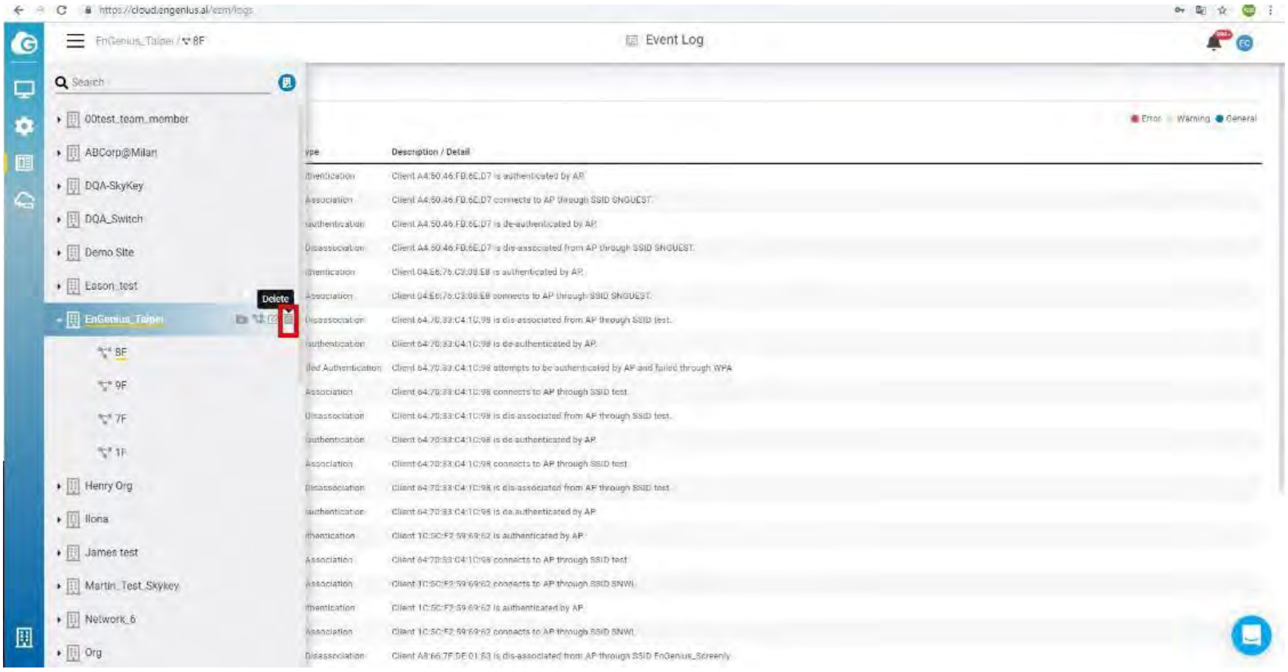
3. Click Apply

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



ype	Description / Detail
thentication	Client A4:50:46:FB:6E:D7 is authenticated by AP.
Association	Client A4:50:46:FB:6E:D7 connects to AP through SSID SNGUEST.
authentication	Client A4:50:46:FB:6E:D7 is de-authenticated by AP.
Disassociation	Client A4:50:46:FB:6E:D7 is dis-associated from AP through SSID SNGUEST.
thentication	Client 04:E6:76:C3:08:E8 is authenticated by AP.
Association	Client 04:E6:76:C3:08:E8 connects to AP through SSID SNGUEST.
Disassociation	Client 64:70:33:C4:10:98 is dis-associated from AP through SSID test.
authentication	Client 64:70:33:C4:10:98 is de-authenticated by AP.
iled Authentication	Client 64:70:33:C4:10:98 attempts to be authenticated by AP and failed through WPA
Association	Client 64:70:33:C4:10:98 connects to AP through SSID test.
Disassociation	Client 64:70:33:C4:10:98 is dis-associated from AP through SSID test.
authentication	Client 64:70:33:C4:10:98 is de-authenticated by AP.
Association	Client 64:70:33:C4:10:98 connects to AP through SSID test
Disassociation	Client 64:70:33:C4:10:98 is dis-associated from AP through SSID test
authentication	Client 64:70:33:C4:10:98 is de-authenticated by AP
thentication	Client 10:5C:F2:59:69:62 is authenticated by AP
Association	Client 64:70:33:C4:10:98 connects to AP through SSID test
Association	Client 10:5C:F2:59:69:62 connects to AP through SSID SNWL
thentication	Client 10:5C:F2:59:69:62 is authenticated by AP
Association	Client 10:5C:F2:59:69:62 connects to AP through SSID SNWL
Disassociation	Client A8:66:7F:DE:01:63 is dis-associated from AP through SSID EnGenius_Screenly

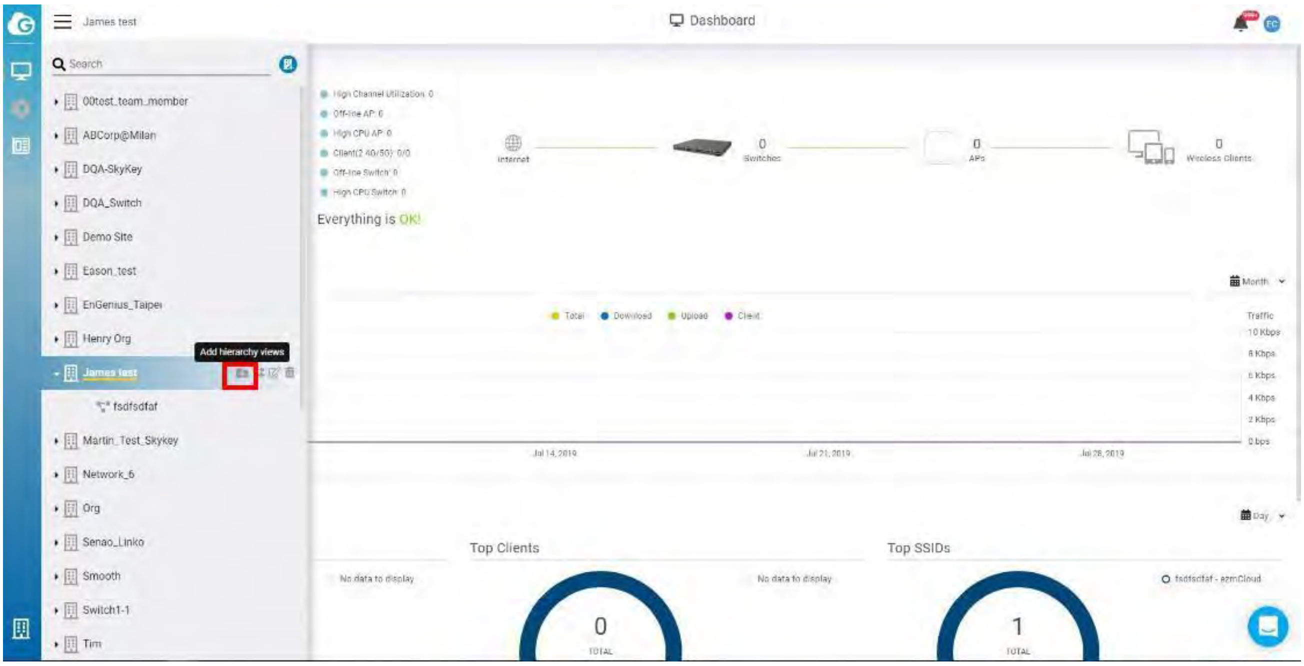
2. Popup is displayed and click **Confirm**

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.

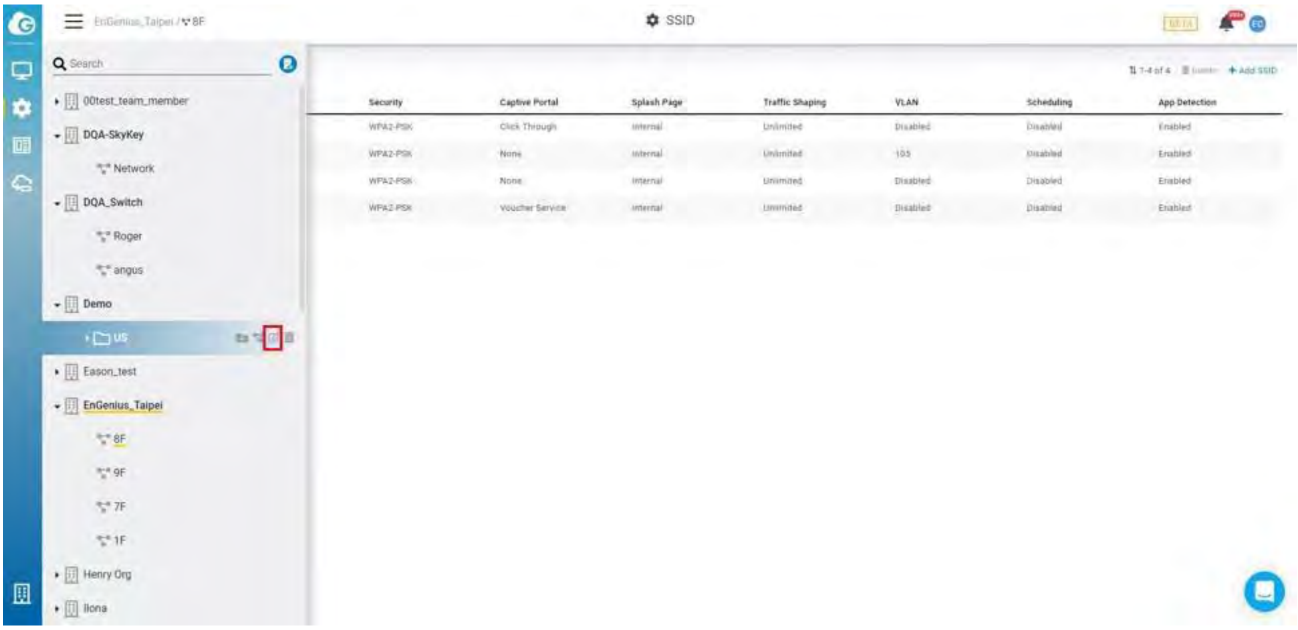
Adding a hierarchy view

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



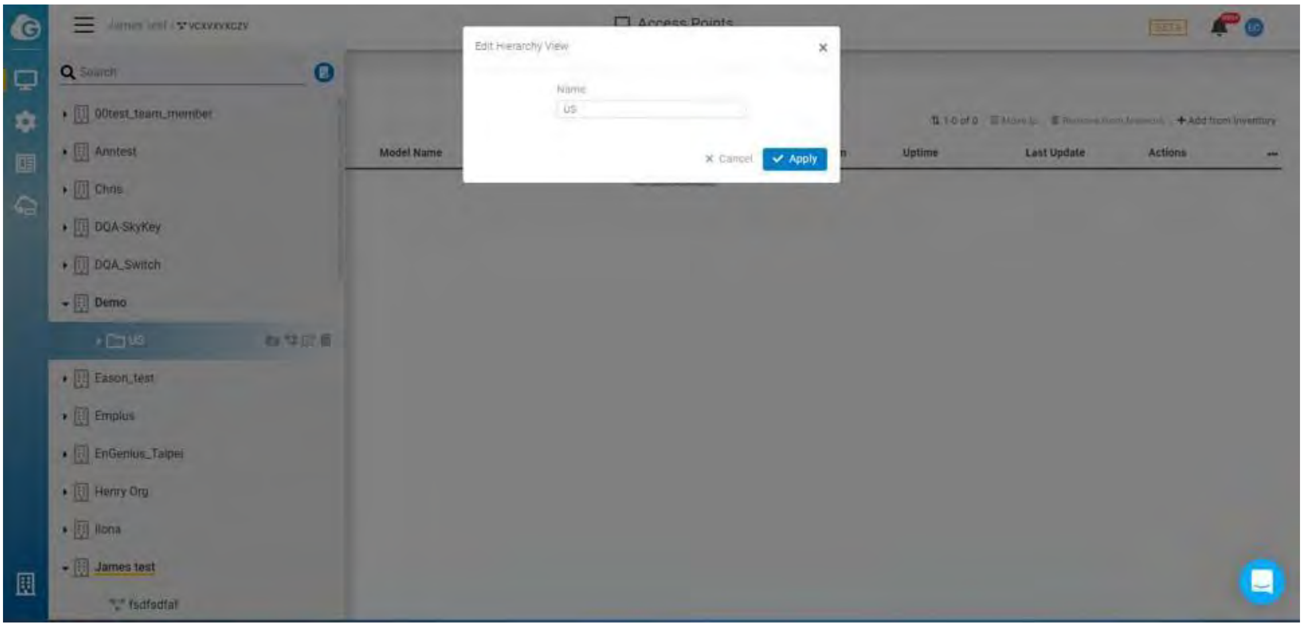
Edit hierarchy views

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



Security	Captive Portal	Splash Page	Traffic Shaping	VLAN	Scheduling	App Detection
WPA2-PSK	Click Through	Internal	Unlimited	Disabled	Disabled	Enabled
WPA2-PSK	None	Internal	Unlimited	105	Disabled	Enabled
WPA2-PSK	None	Internal	Unlimited	Disabled	Disabled	Enabled
WPA2-PSK	Voucher Service	Internal	Unlimited	Disabled	Disabled	Enabled

2. Change the Hierarchy View name and click Apply.

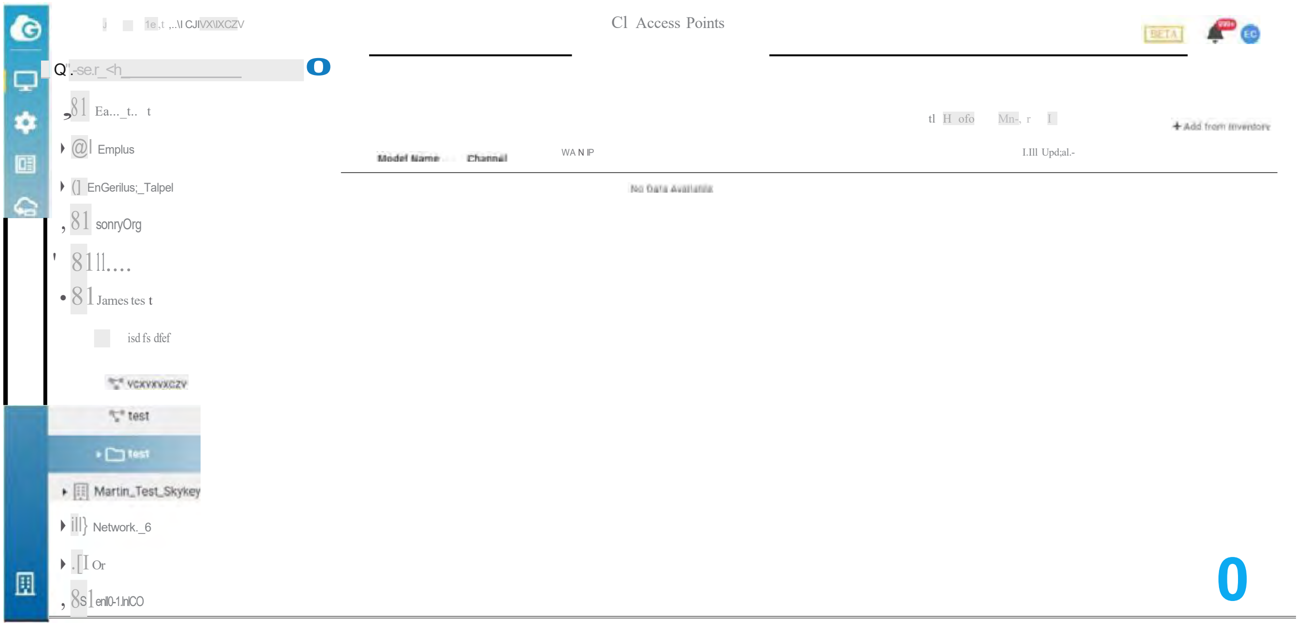


Edit Hierarchy View

Name: US

Delete Hierarchy View

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



1e.t ,..\I CJIVX\IXCZV

Cl Access Points

BETA

Q'.-se.r_<h

Ea..._t.. t

Emplus

EnGerilus;_Talpel

sonryOrg

81ll....

James tes t

isd fs dfef

VCXVXVXCZV

test

test

Martin_Test_Skykey

Network._6

Or

enl0-1.lnCO

tl H ofo Mn-, r I

+ Add from Inventory

Model Name Channel WA N IP I.Ill Upd;al.-

No Data Available

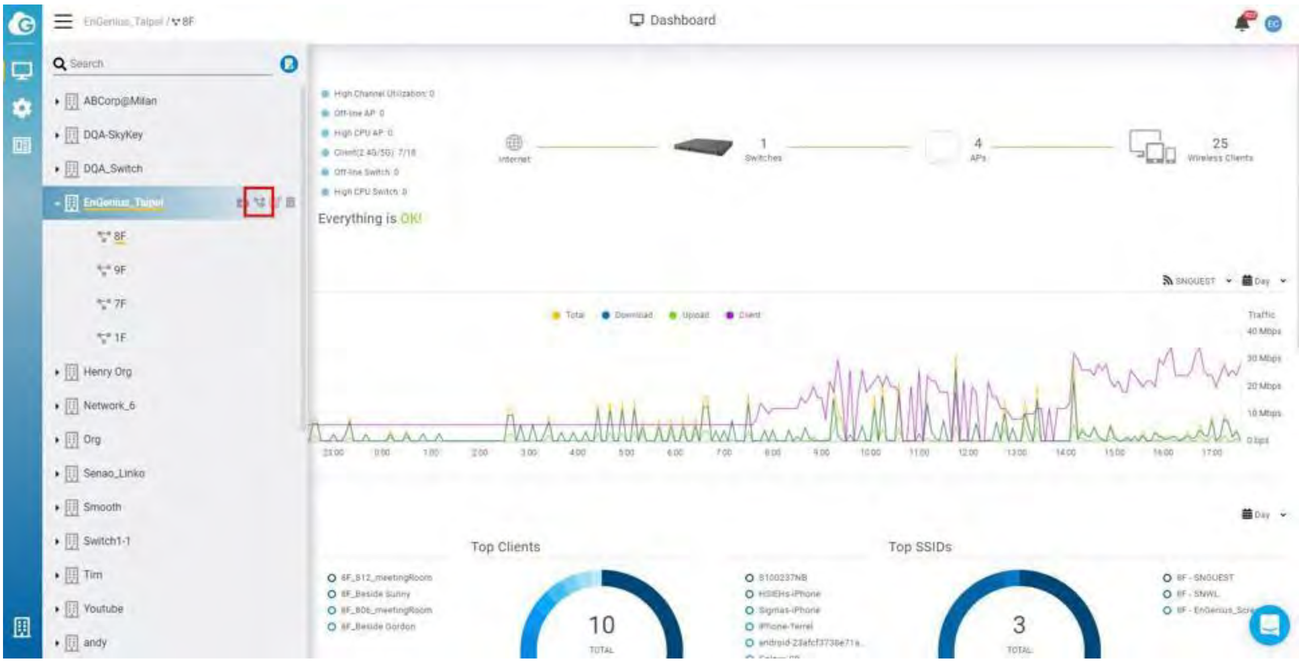
0

Network

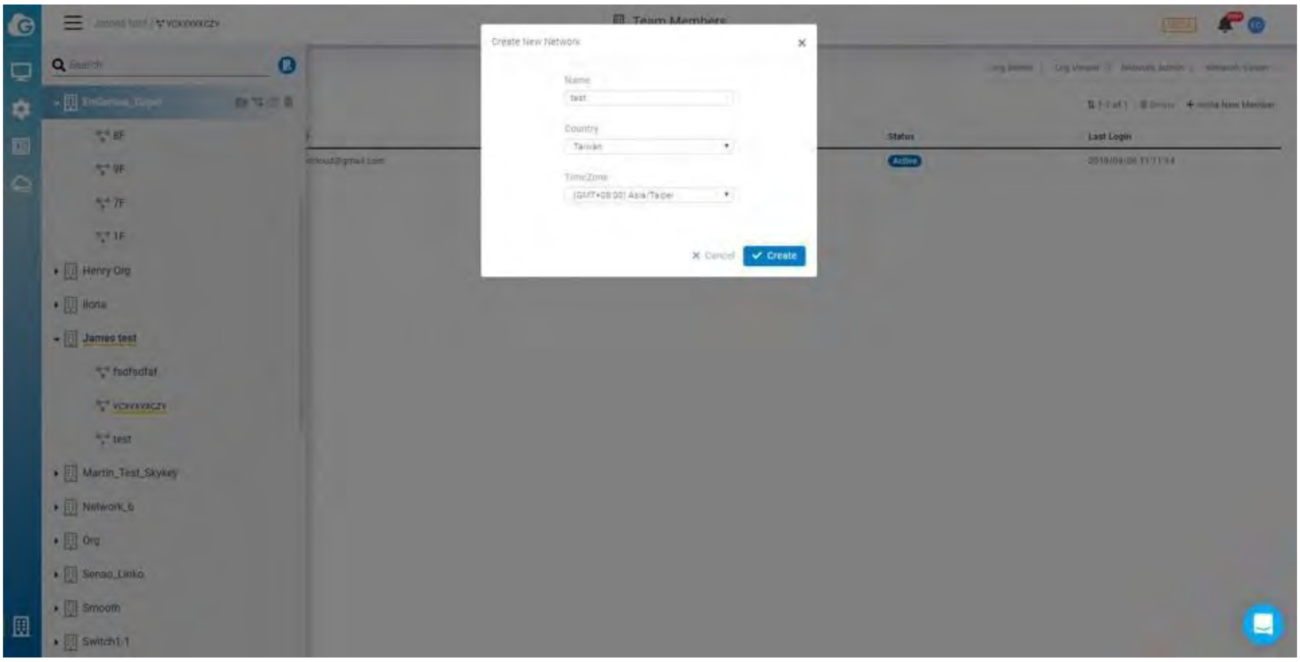
A network contains a list of devices and relevant information, such as configuration, SSID, radio settings, and firmware upgrade history. Each network contains a single configuration set for its devices, so if you have multiple configurations for devices, you can create a separate network to handle that.

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.


Create New Network

Name: test

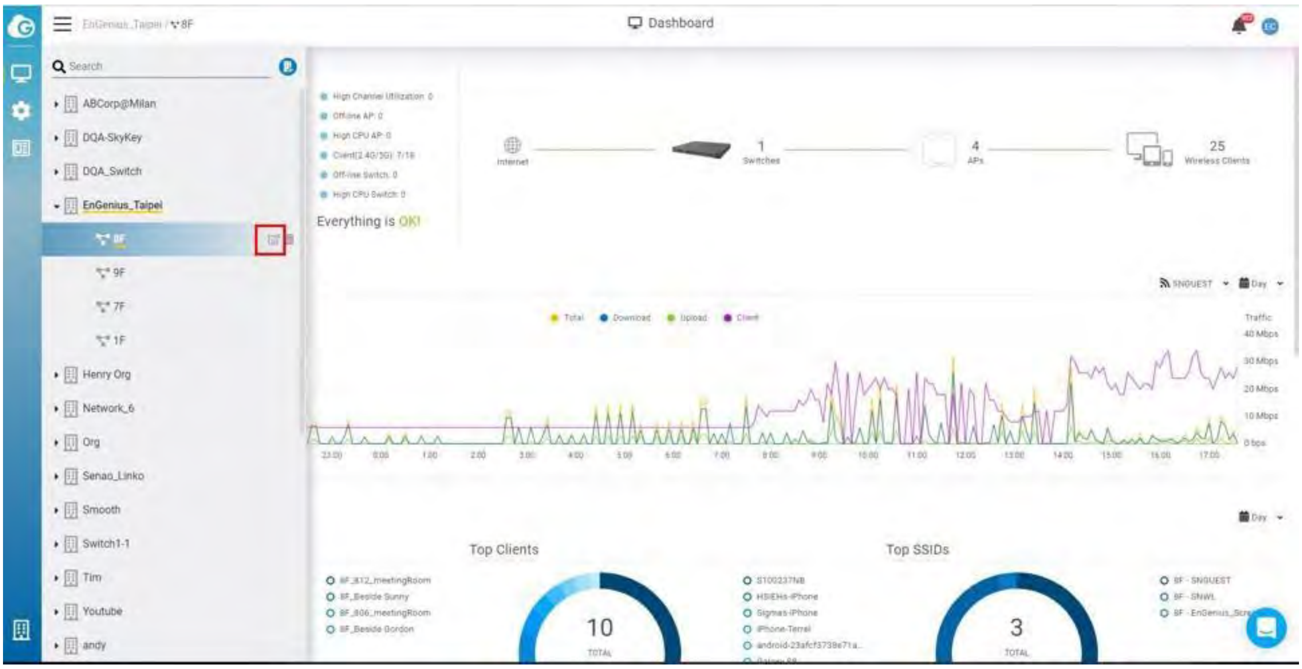
Country: Taiwan

TimeZone: (GMT+08:00) Asia/Taipei

Edit Network

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

Choose network > Edit

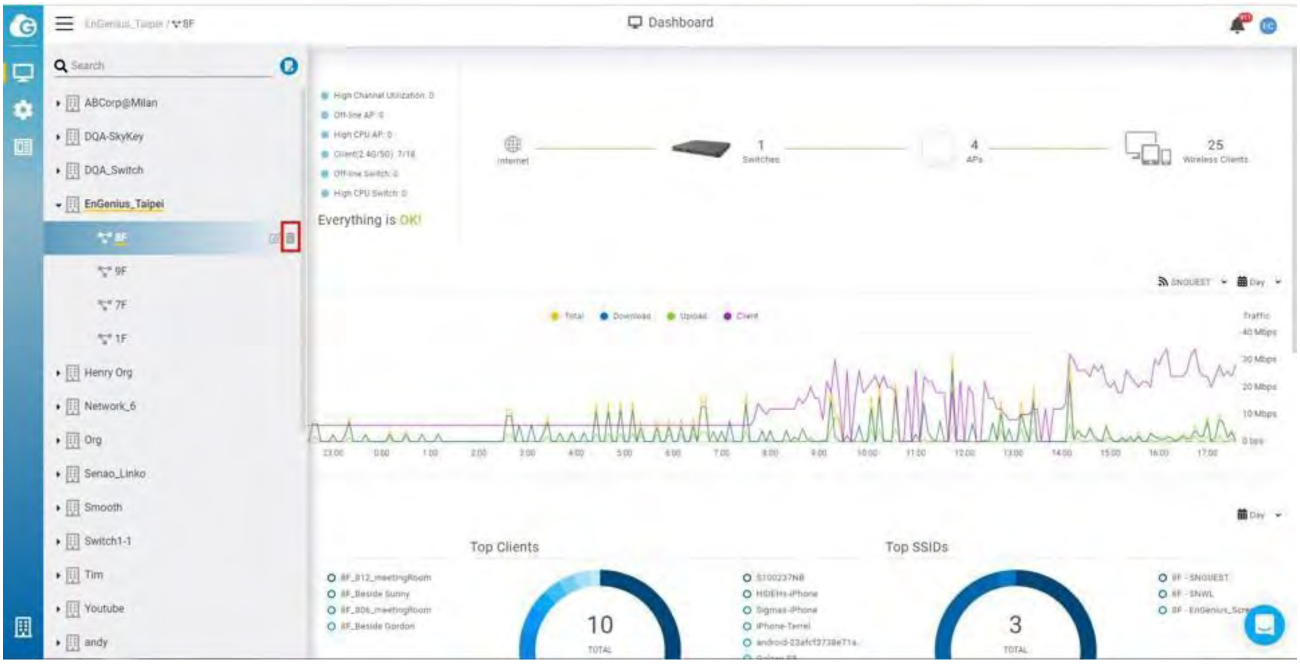


Delete Network

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

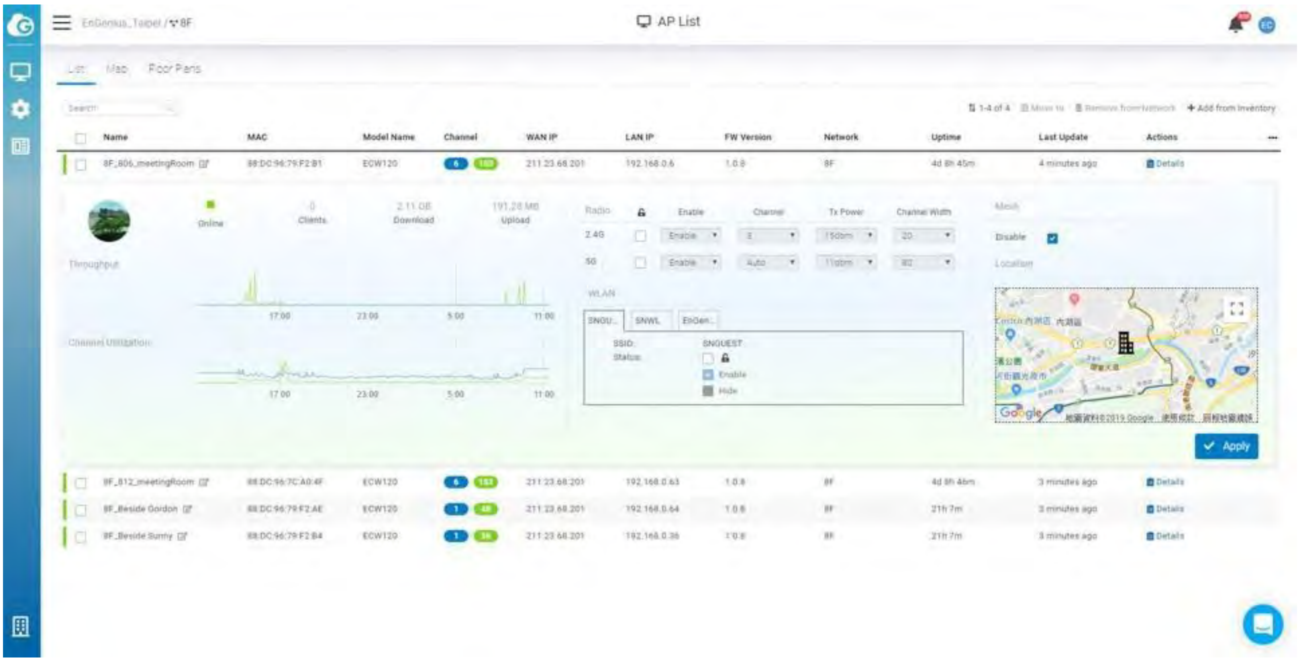


2. Popup is displayed. Click **Confirm.**

Managing 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.



Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
8F_806_meetingRoom	88:DC:96:79:F2:B1	ECW120	6 153	211.23.68.201	192.168.0.6	1.0.8	8F	4d 8h 45m	4 minutes ago	Details
8F_812_meetingRoom	88:DC:96:7C:A0:4F	ECW120	6 153	211.23.68.201	192.168.0.63	1.0.8	8F	4d 8h 46m	3 minutes ago	Details
8F_Beside Gordon	88:DC:96:79:F2:AE	ECW120	1 48	211.23.68.201	192.168.0.64	1.0.8	8F	21h 7m	3 minutes ago	Details
8F_Beside Sunny	88:DC:96:79:F2:B4	ECW120	1 36	211.23.68.201	192.168.0.36	1.0.8	8F	21h 7m	3 minutes ago	Details

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

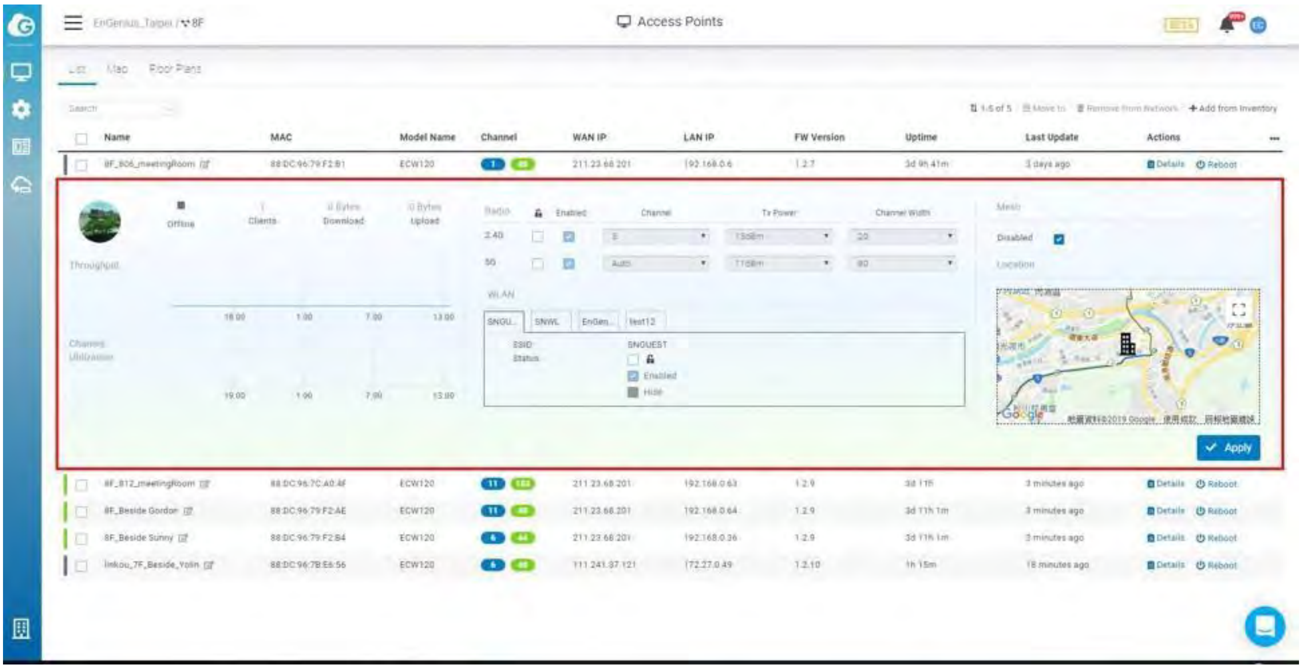
Detail: Click to display individual access point details

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.



EnGenius_Taipei / 8F — Access Points

List | Map | Floor Plans

1-5 of 5 | Move to | Remove from Network | + Add from Inventory

Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Uptime	Last Update	Actions
8F_806_meetingRoom	88:DC:96:79:F2:B1	ECW120	1 48	211.23.68.201	192.168.0.6	1.2.7	3d 9h 41m	3 days ago	Details Reboot
8F_812_meetingRoom	88:DC:96:7C:A0:4F	ECW120	11 153	211.23.68.201	192.168.0.63	1.2.9	3d 11h	3 minutes ago	Details Reboot
8F_Beside Gordon	88:DC:96:79:F2:AE	ECW120	11 48	211.23.68.201	192.168.0.64	1.2.9	3d 11h 1m	3 minutes ago	Details Reboot
8F_Beside Sunny	88:DC:96:79:F2:B4	ECW120	6 44	211.23.68.201	192.168.0.36	1.2.9	3d 11h 1m	3 minutes ago	Details Reboot
linkou_7F_Beside_Yolin	88:DC:96:7B:E6:56	ECW120	6 48	111.241.37.121	172.27.0.49	1.2.10	1h 15m	18 minutes ago	Details Reboot

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	□	☑	5	15dBm	20
5G	□	☑	Auto	17dBm	80

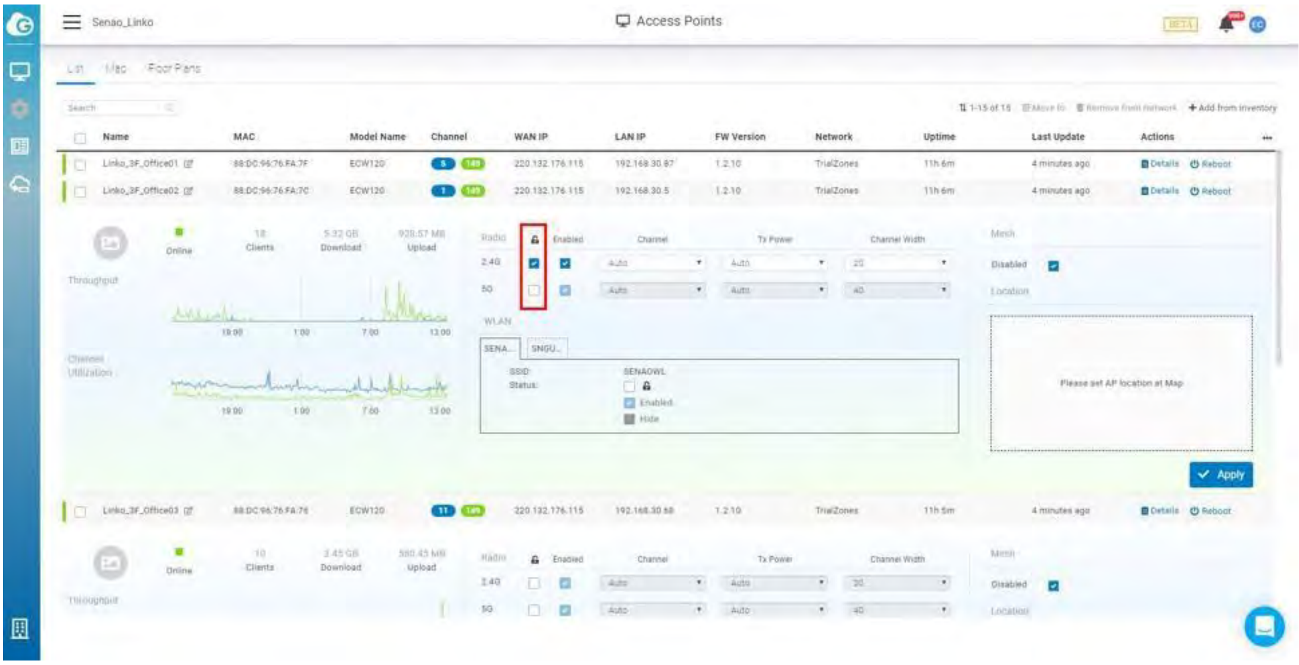
WLAN: SNGU... | SNWL | EnGen... | test12

ESSID: SNGUEST

Status: □ 🔒 ☑ Enabled ■ Hide

Mesh: Disabled ☑

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



Senao_Linko

Access Points

List Map Floor Plans

1-15 of 15 Move to Remove from Network + Add from inventory

Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
Linko_3F_Office01	88:DC:96:76:FA:7F	ECW120	5 149	220.132.176.115	192.168.30.87	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office02	88:DC:96:76:FA:7C	ECW120	1 149	220.132.176.115	192.168.30.5	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office03	88:DC:96:76:FA:76	ECW120	11 149	220.132.176.115	192.168.30.68	1.2.10	TrialZones	11h 5m	4 minutes ago	Details Reboot

Online 18 Clients 5.32 GB Download 928.57 MB Upload

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	☑	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

Mesh: Disabled ☑

Location: Please set AP location at Map

WLAN: SENA... SNGU...

SSID: SENAOWL

Status: □ 🔒 ☑ Enabled ▨ Hide

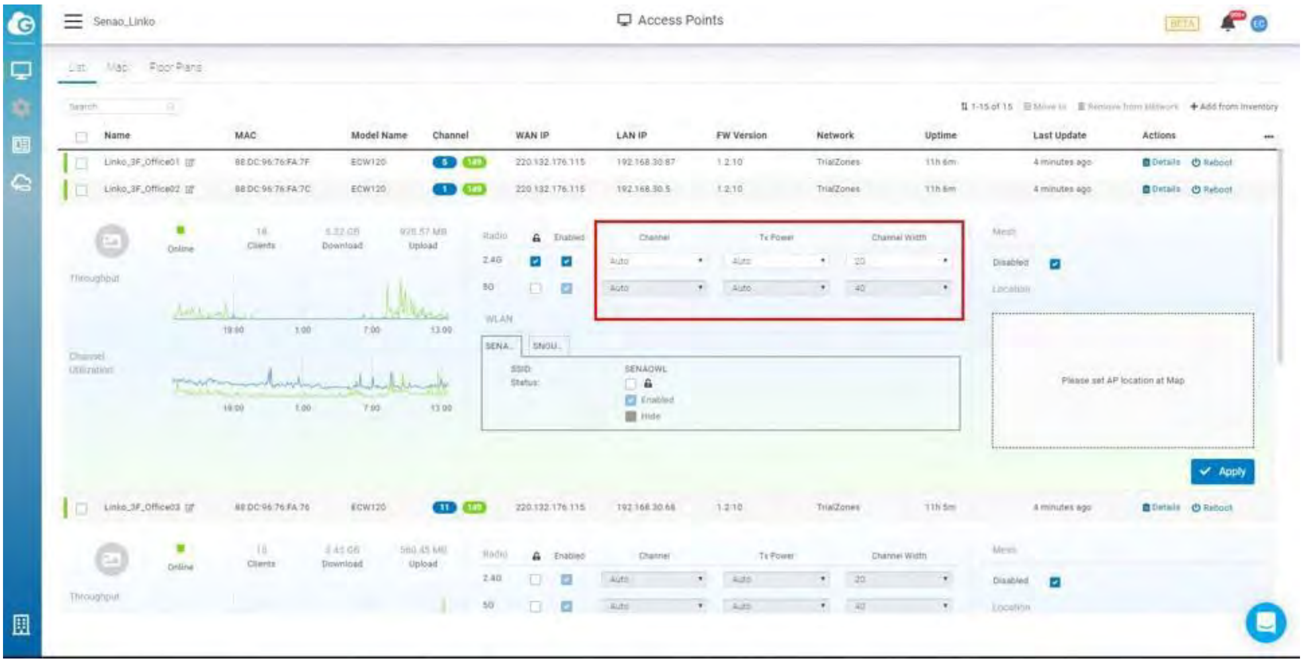
Apply

Online 10 Clients 3.45 GB Download 580.45 MB Upload

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	□	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

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

- Channel
- Tx Power
- Channel Width



Senao_Linko

Access Points

List Map Floor Plans

Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
Linko_3F_Office01	88:DC:96:76:FA:7F	ECW120	5 149	220.132.176.115	192.168.30.87	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office02	88:DC:96:76:FA:7C	ECW120	1 149	220.132.176.115	192.168.30.5	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office03	88:DC:96:76:FA:76	ECW120	11 149	220.132.176.115	192.168.30.68	1.2.10	TrialZones	11h 5m	4 minutes ago	Details Reboot

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	☑	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

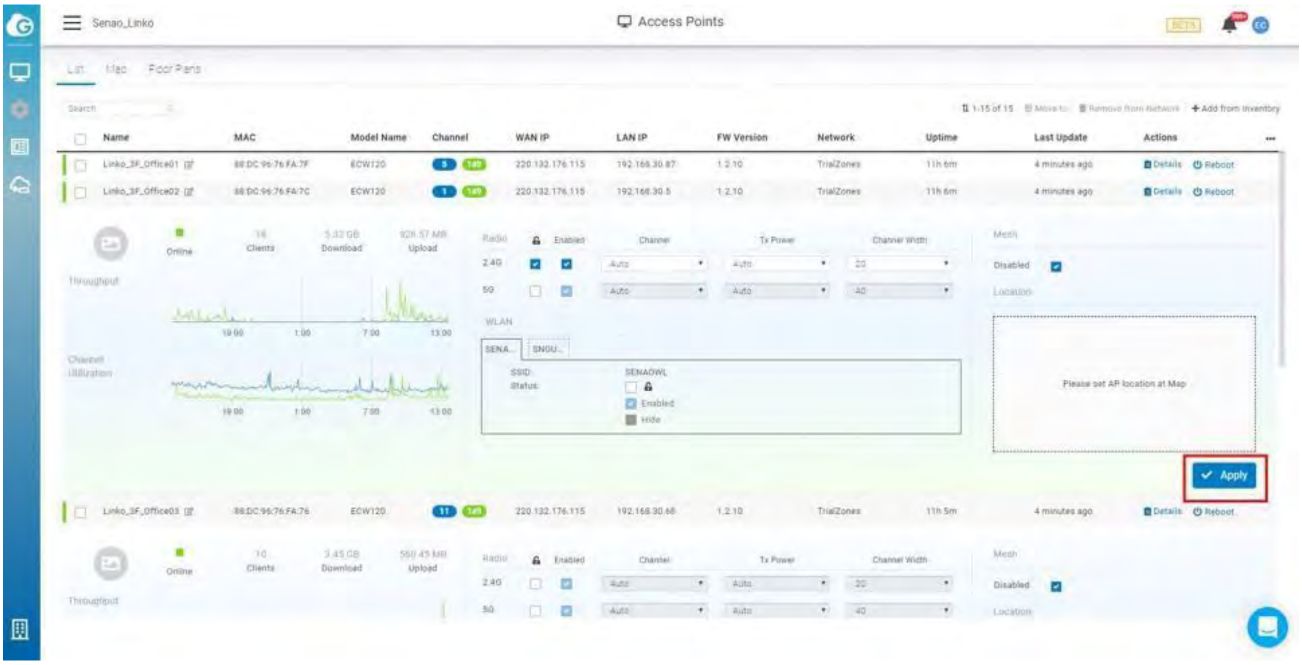
Mesh: Disabled ☑

Please set AP location at Map

SSID: SENAOWL

Apply

4. Click Apply.



Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
Linko_3F_Office01	88:DC:96:76:FA:7F	ECW120	5 149	220.132.176.115	192.168.30.87	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office02	88:DC:96:76:FA:7C	ECW120	1 149	220.132.176.115	192.168.30.5	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
Linko_3F_Office03	88:DC:96:76:FA:76	ECW120	11 149	220.132.176.115	192.168.30.68	1.2.10	TrialZones	11h 5m	4 minutes ago	Details Reboot

Online 16 Clients 5.32 GB Download 926.57 MB Upload

Throughput

Channel Utilization

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	☑	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

Mesh

Disabled ☑

Location

Please set AP location at Map

WLAN

SENA... SNGU...

SSID: SENAOWL

Status: □ 🔒 ☑ Enabled ▨ Hide

✓ Apply

Online 10 Clients 3.45 GB Download 560.45 MB Upload

Throughput

Radio	🔒	Enabled	Channel	Tx Power	Channel Width
2.4G	□	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

Mesh

Disabled ☑

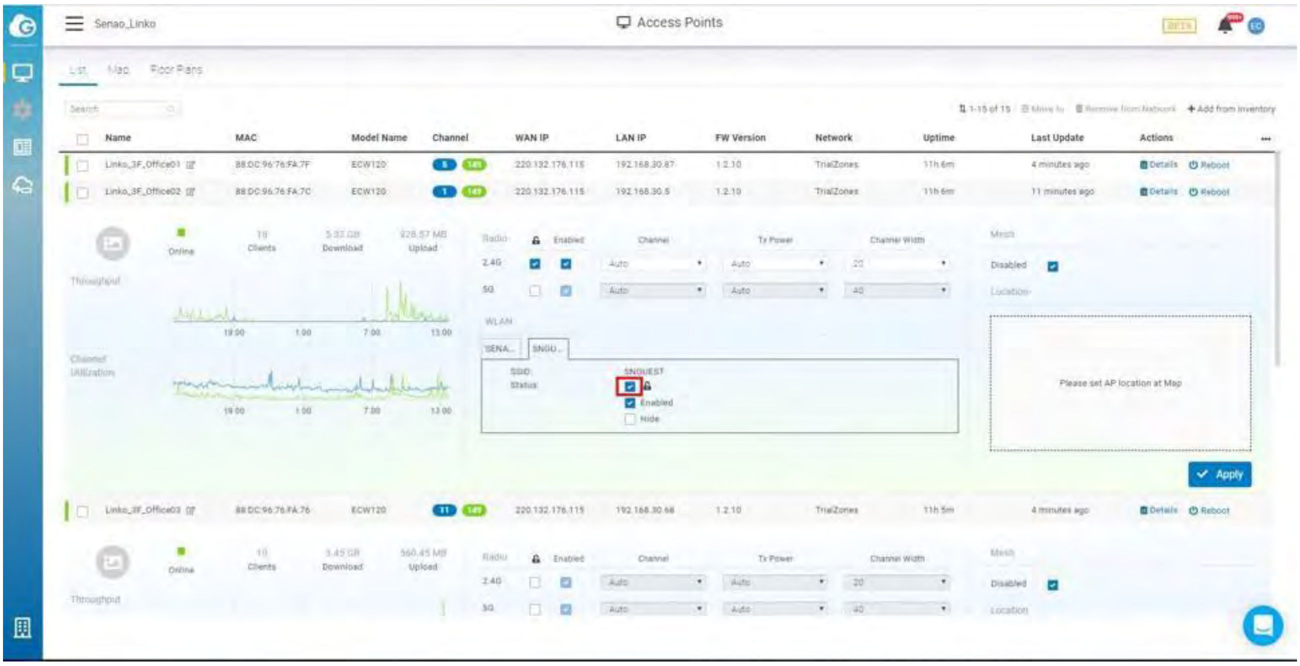
Location

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.



Senao_Linko

Access Points

List Map Floor Plans

1-15 of 15 Move to Remove from Network + Add from inventory

	Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
□	Linko_3F_Office01	88:DC:96:76:FA:7F	ECW120	5 149	220.132.176.115	192.168.30.87	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
□	Linko_3F_Office02	88:DC:96:76:FA:7C	ECW120	1 149	220.132.176.115	192.168.30.5	1.2.10	TrialZones	11h 6m	11 minutes ago	Details Reboot
□	Linko_3F_Office03	88:DC:96:76:FA:76	ECW120	11 149	220.132.176.115	192.168.30.68	1.2.10	TrialZones	11h 5m	4 minutes ago	Details Reboot

Radio		Enabled	Channel	Tx Power	Channel Width
2.4G	☑	☑	Auto	Auto	20
5G	□	☑	Auto	Auto	40

Mesh: Disabled ☑

WLAN: SENA... SNGU...

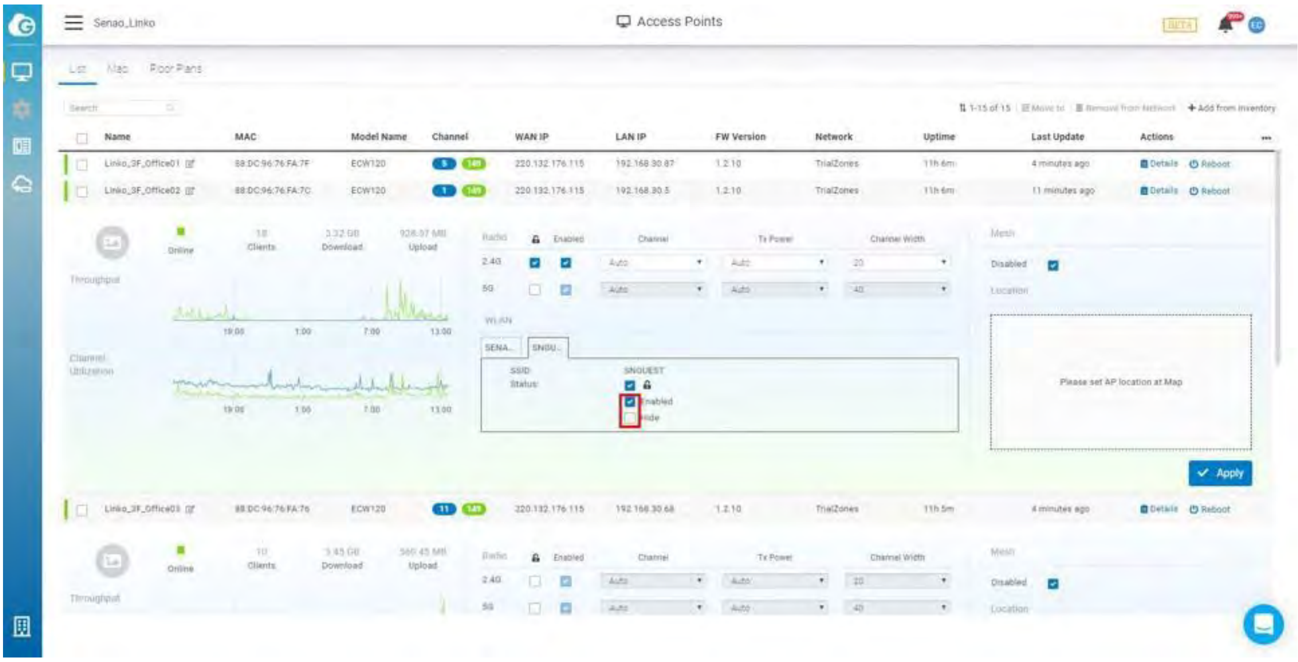
SSID: SNGUEST

Status: ☑ ☑ Enabled □ Hide

Please set AP location at Map

✓ Apply

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



Senao_Linko

Access Points

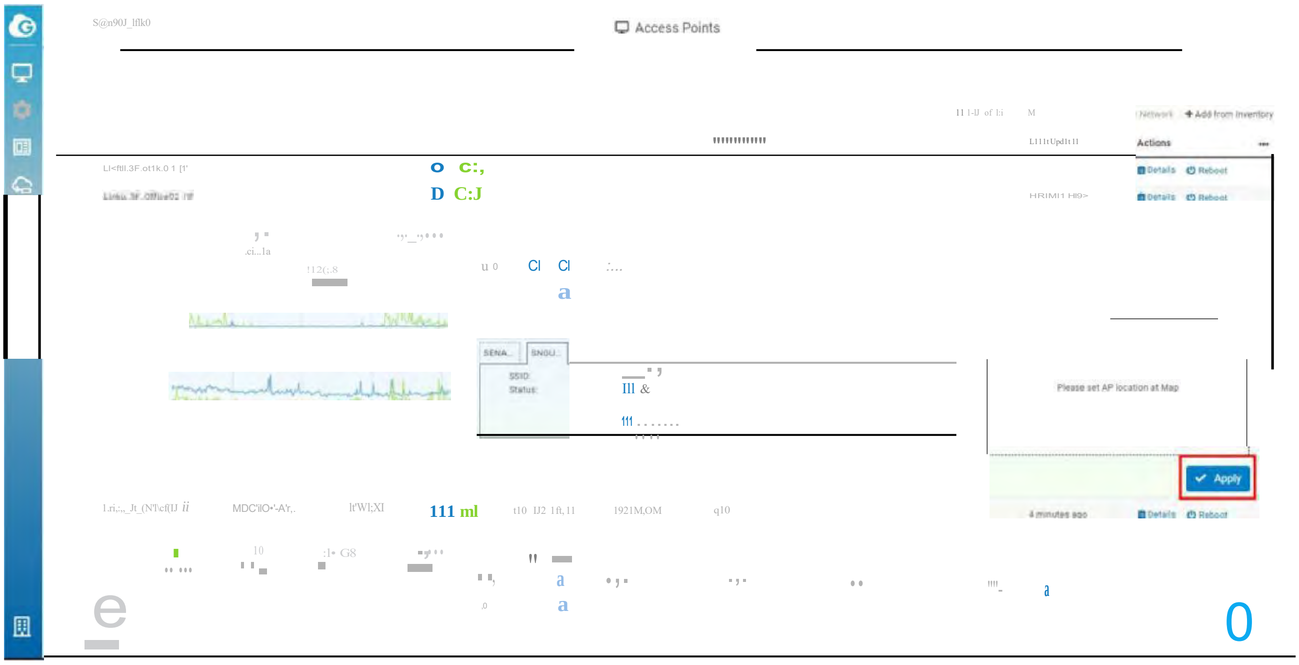
	Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
□	Linko_3F_Office01	88:DC:96:76:FA:7F	ECW120	5 149	220.132.176.115	192.168.30.87	1.2.10	TrialZones	11h 6m	4 minutes ago	Details Reboot
□	Linko_3F_Office02	88:DC:96:76:FA:7C	ECW120	1 149	220.132.176.115	192.168.30.5	1.2.10	TrialZones	11h 6m	11 minutes ago	Details Reboot
□	Linko_3F_Office03	88:DC:96:76:FA:76	ECW120	11 149	220.132.176.115	192.168.30.68	1.2.10	TrialZones	11h 5m	4 minutes ago	Details Reboot

SSID: SNGUEST

Status: ☑ ☑ Enabled □ Hide

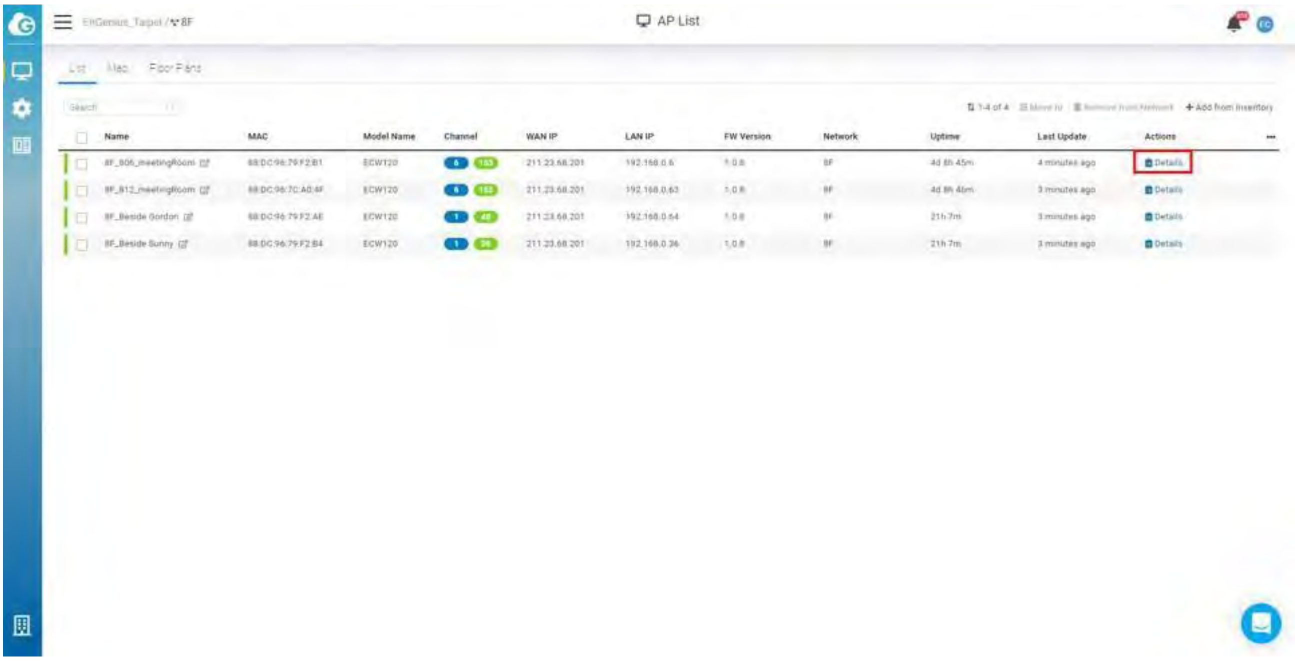
✓ Apply

3. Click Apply.


Access Points
Network
+ Add from inventory
Actions
Details
Reboot
Details
Reboot
SSID:
Status:
Please set AP location at Map
✓ Apply
4 minutes ago
Details
Reboot

Getting Access Point Analytics

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



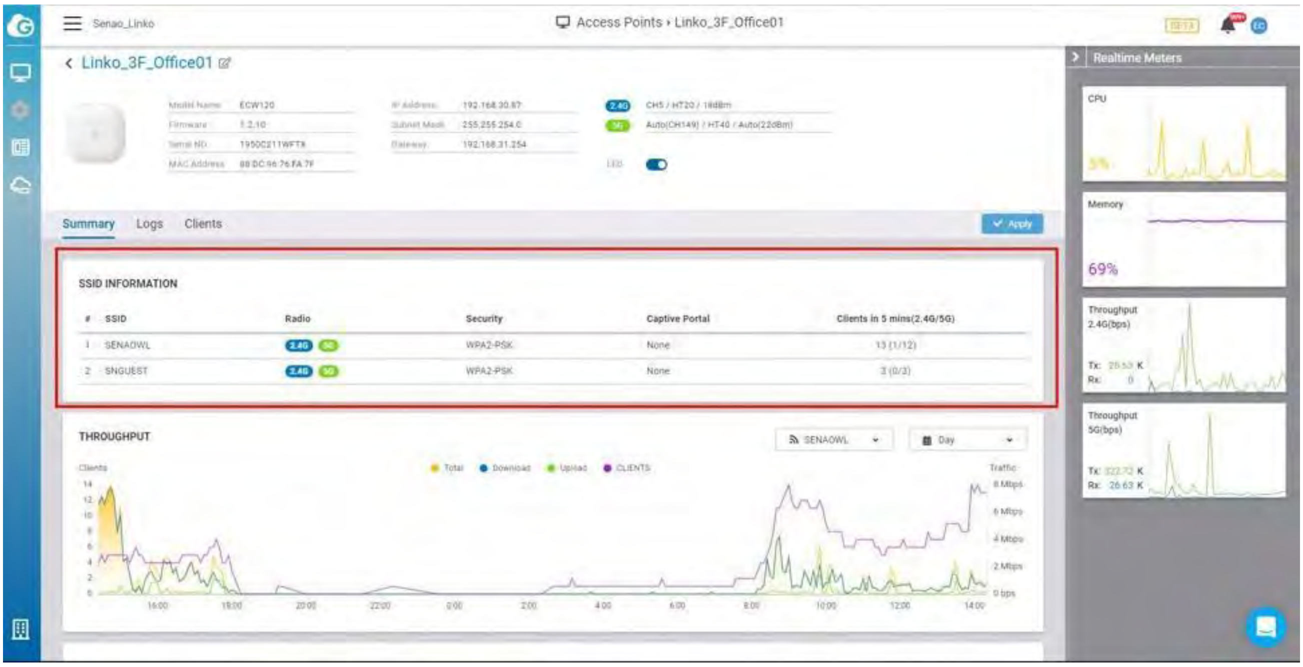
Name	MAC	Model Name	Channel	WAN IP	LAN IP	FW Version	Network	Uptime	Last Update	Actions
8F_806_meetingRoom	88:DC:96:79:F2:B1	ECW120	6 153	211.23.68.201	192.168.0.6	1.0.8	8F	4d 8h 45m	4 minutes ago	Details
8F_812_meetingRoom	88:DC:96:7C:A0:4F	ECW120	6 153	211.23.68.201	192.168.0.63	1.0.8	8F	4d 8h 46m	3 minutes ago	Details
8F_Beside Gordon	88:DC:96:79:F2:AE	ECW120	1 48	211.23.68.201	192.168.0.64	1.0.8	8F	21h 7m	3 minutes ago	Details
8F_Beside Sunny	88:DC:96:79:F2:B4	ECW120	1 36	211.23.68.201	192.168.0.36	1.0.8	8F	21h 7m	3 minutes ago	Details

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.



Linko_3F_Office01

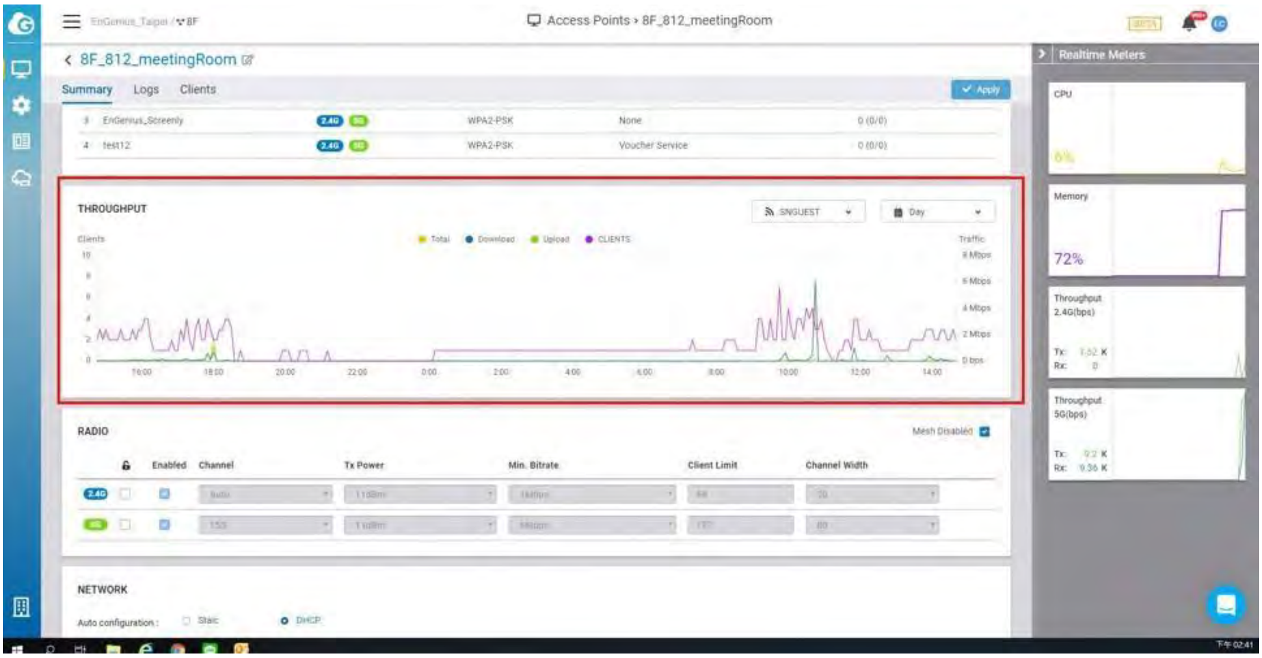
Model Name	ECW120	IP Address	192.168.30.87	2.4G	CH5 / HT20 / 18dBm
Firmware	1.2.10	Subnet Mask	255.255.254.0	5G	Auto(CH149) / HT40 / Auto(22dBm)
Serial NO	19500211WFTX	Gateway	192.168.31.254		
MAC Address	88:DC:96:76:FA:7F				

SSID INFORMATION

#	SSID	Radio	Security	Captive Portal	Clients in 5 mins(2.4G/5G)
1	SENAOWL	2.4G 5G	WPA2-PSK	None	13 (1/12)
2	SNGUEST	2.4G 5G	WPA2-PSK	None	3 (0/3)

Throughput

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



8F_812_meetingRoom

3	EnGenius_Screenly	2.4G 5G	WPA2-PSK	None	0 (0/0)
4	test12	2.4G 5G	WPA2-PSK	Voucher Service	0 (0/0)

RADIO

Mesh Disabled ☑

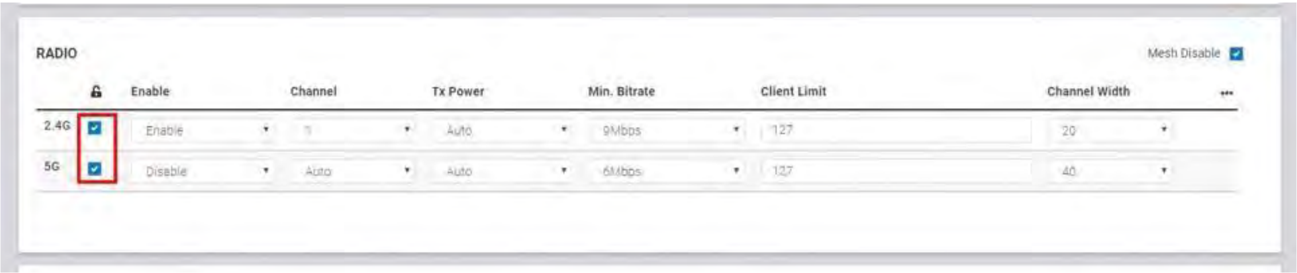
	🔓	Enabled	Channel	Tx Power	Min. Bitrate	Client Limit	Channel Width
2.4G	□	☑	Auto	11dBm	1Mbps	64	20
5G	□	☑	153	11dBm	6Mbps	127	80

NETWORK

Auto configuration : ○ Static ● DHCP

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.



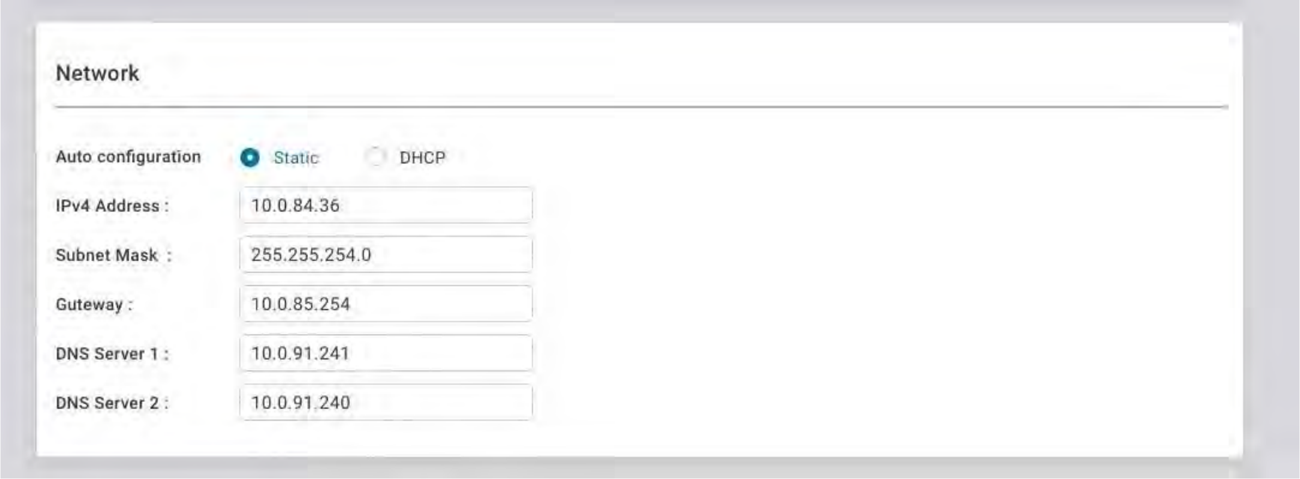
RADIO

Mesh Disable ☑

		Enable	Channel	Tx Power	Min. Bitrate	Client Limit	Channel Width
2.4G	☑	Enable	1	Auto	9Mbps	127	20
5G	☑	Disable	Auto	Auto	6Mbps	127	40

Network

This allows you to configure individual access point network settings.



Network

Auto configuration ● Static ○ DHCP

IPv4 Address :	10.0.84.36
Subnet Mask :	255.255.254.0
Guteway :	10.0.85.254
DNS Server 1 :	10.0.91.241
DNS Server 2 :	10.0.91.240

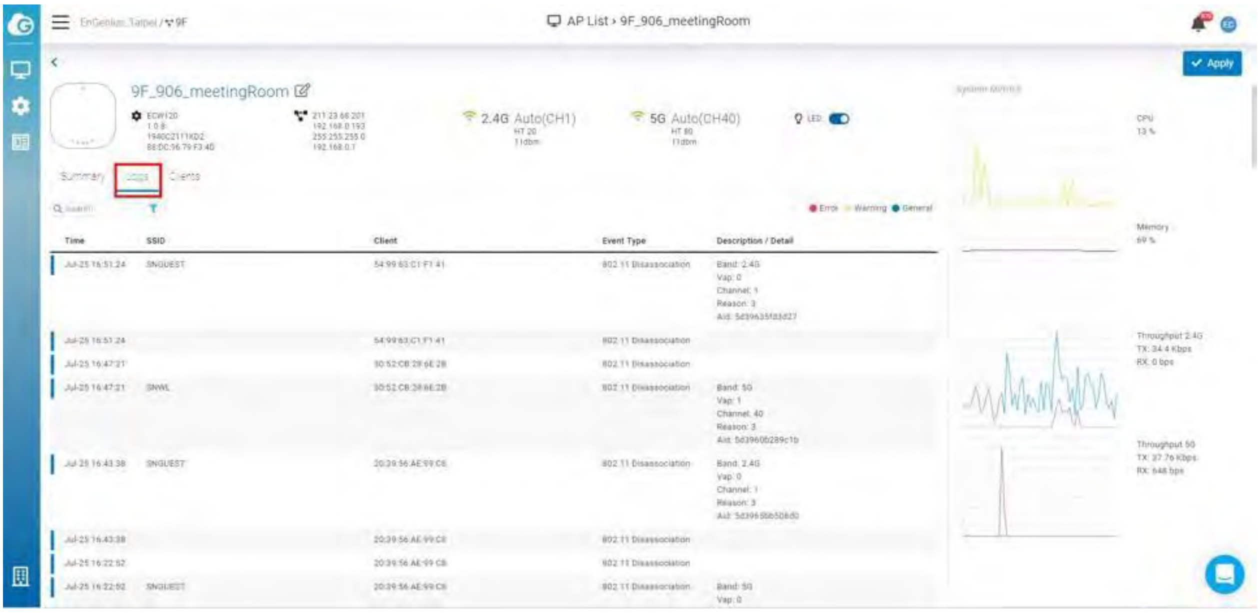
- DHCP: You can choose to auto assign IP addresses if there is a DHCP server in the network.
- Static: Allows you to manually assign an IP address.

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

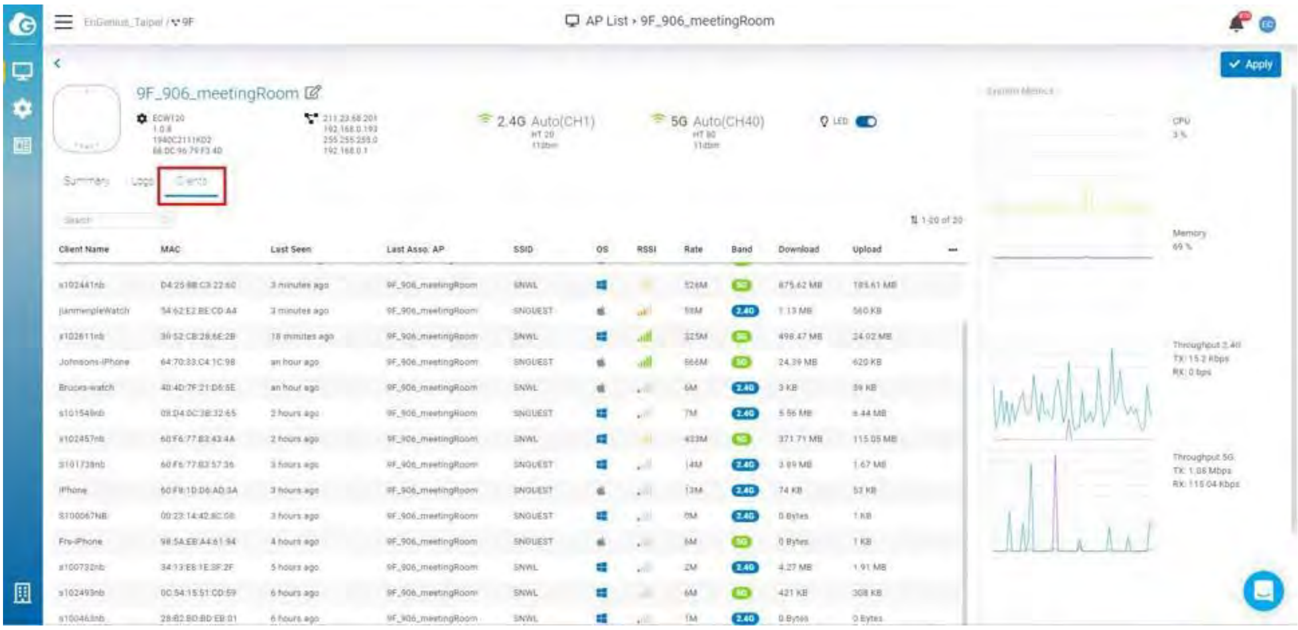
Periodically viewing events that have occurred on an access point (or on clients associated with the access point) can help alert you to potential issues. The Logs tab appears and displays the latest events that have occurred in the last 24 hours.



Time	SSID	Client	Event Type	Description / Detail
Jul-25 16:51:24	SNGUEST	54:99:63:C1:F1:41	802.11 Disassociation	Band: 2.4G Vap: 0 Channel: 1 Reason: 3 Aid: 5d39635f83d27
Jul-25 16:51:24		54:99:63:C1:F1:41	802.11 Disassociation	
Jul-25 16:47:21		30:52:CB:28:6E:2B	802.11 Disassociation	
Jul-25 16:47:21	SNWL	30:52:CB:28:6E:2B	802.11 Disassociation	Band: 5G Vap: 1 Channel: 40 Reason: 3 Aid: 5d3960b289c1b
Jul-25 16:43:38	SNGUEST	20:39:56:AE:99:C8	802.11 Disassociation	Band: 2.4G Vap: 0 Channel: 1 Reason: 3 Aid: 5d3965bb50bd0
Jul-25 16:43:38		20:39:56:AE:99:C8	802.11 Disassociation	
Jul-25 16:22:52		20:39:56:AE:99:C8	802.11 Disassociation	
Jul-25 16:22:52	SNGUEST	20:39:56:AE:99:C8	802.11 Disassociation	Band: 5G Vap: 0

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.

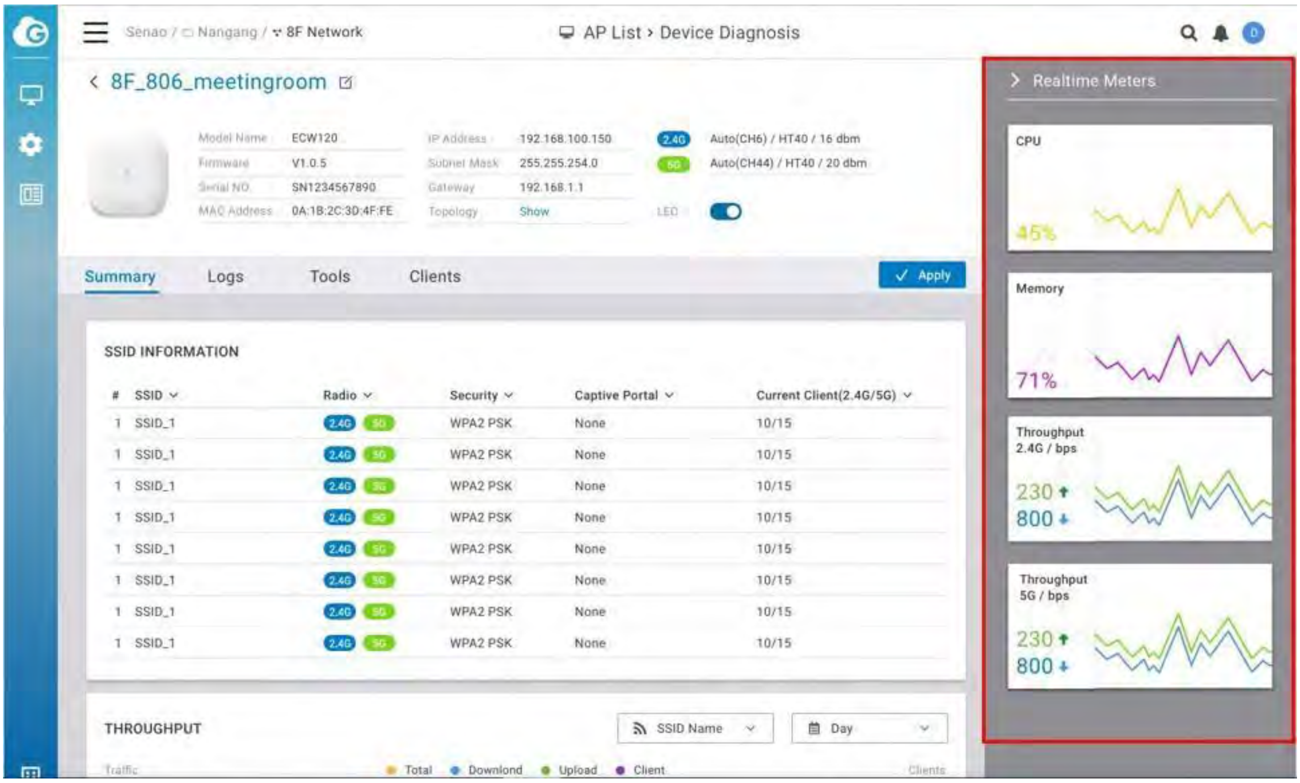


Client Name	MAC	Last Seen	Last Asso. AP	SSID	OS	RSSI	Rate	Band	Download	Upload
s102441nb	D4:25:8B:C3:22:60	3 minutes ago	9F_906_meetingRoom	SNWL	⊞		526M	5G	875.62 MB	185.61 MB
jianmenpleWatch	54:62:E2:BE:CD:A4	3 minutes ago	9F_906_meetingRoom	SNGUEST			58M	2.4G	1.13 MB	560 KB
s102811nb	30:52:CB:28:6E:2B	18 minutes ago	9F_906_meetingRoom	SNWL	⊞		325M	5G	498.47 MB	24.02 MB
Johnsons-iPhone	64:70:33:C4:1C:98	an hour ago	9F_906_meetingRoom	SNGUEST			866M	5G	24.39 MB	620 KB
Brucxs-watch	40:4D:7F:21:D6:5E	an hour ago	9F_906_meetingRoom	SNWL			6M	2.4G	3 KB	39 KB
s101549nb	08:D4:0C:38:32:65	2 hours ago	9F_906_meetingRoom	SNGUEST	⊞		7M	2.4G	5.56 MB	6.44 MB
s102457nb	60:F6:77:B3:43:4A	2 hours ago	9F_906_meetingRoom	SNWL	⊞		433M	5G	371.71 MB	115.05 MB
S101738nb	60:F6:77:B3:57:36	3 hours ago	9F_906_meetingRoom	SNGUEST	⊞		14M	2.4G	3.89 MB	1.67 MB
iPhone	60:F8:1D:D6:AD:3A	3 hours ago	9F_906_meetingRoom	SNGUEST			13M	2.4G	74 KB	53 KB
S100067NB	00:23:14:42:8C:08	3 hours ago	9F_906_meetingRoom	SNGUEST	⊞		0M	2.4G	0 Bytes	1 KB
Frs-iPhone	98:5A:EB:A4:61:94	4 hours ago	9F_906_meetingRoom	SNGUEST			6M	5G	0 Bytes	1 KB
s100732nb	34:13:E8:1E:3F:2F	5 hours ago	9F_906_meetingRoom	SNWL	⊞		2M	2.4G	4.27 MB	1.91 MB
s102493nb	0C:54:15:51:CD:59	6 hours ago	9F_906_meetingRoom	SNWL	⊞		6M	5G	421 KB	308 KB
s100463nb	28:B2:BD:BD:EB:01	6 hours ago	9F_906_meetingRoom	SNWL	⊞		1M	2.4G	0 Bytes	0 Bytes

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



Model Name	ECW120	IP Address	192.168.100.150
Firmware	V1.0.5	Subnet Mask	255.255.254.0
Serial NO.	SN1234567890	Gateway	192.168.1.1
MAC Address	0A:1B:2C:3D:4F:FE	Topology	Show

2.4G Auto(CH6) / HT40 / 16 dbm
5G Auto(CH44) / HT40 / 20 dbm
LED ●

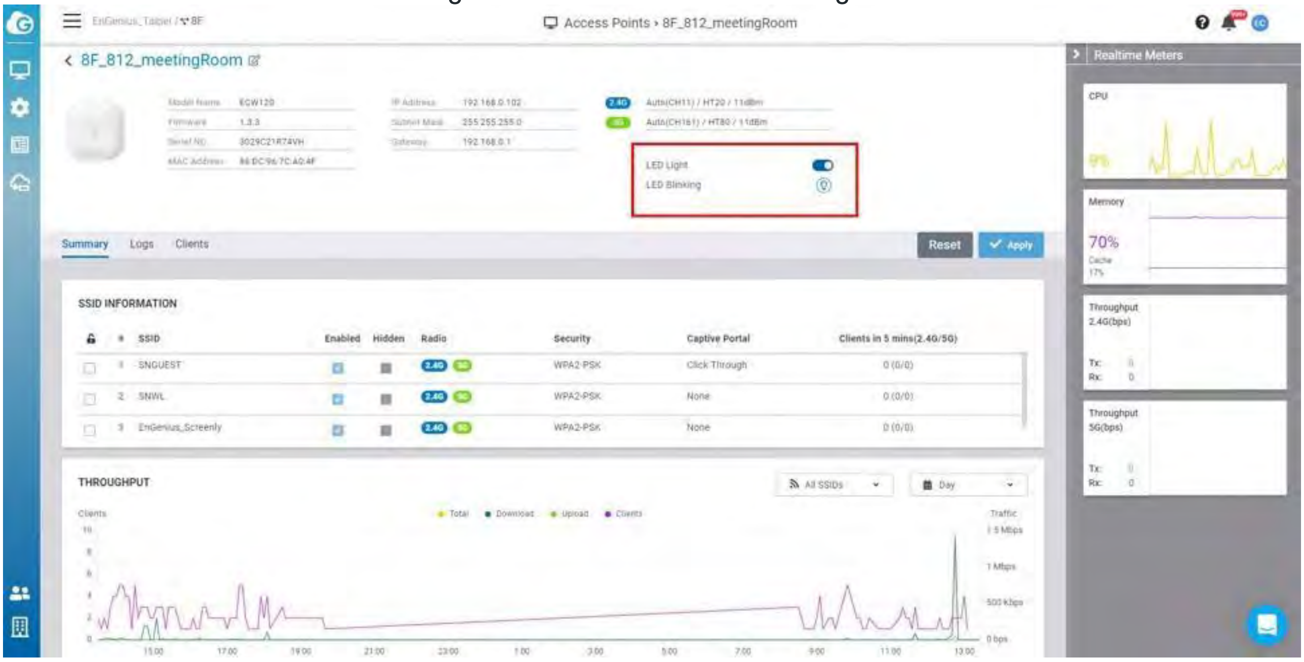
SSID INFORMATION

#	SSID	Radio	Security	Captive Portal	Current Client(2.4G/5G)
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15
1	SSID_1	2.4G 5G	WPA2 PSK	None	10/15

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 .



8F_812_meetingRoom

Model Name	ECW120
Firmware	1.3.3
Serial NO	3029C21R74VH
MAC Address	86:DC:96:7C:A0:4F
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
2.4G	Auto(CH11) / HT20 / 11dBm
5G	Auto(CH161) / HT80 / 11dBm

LED Light

LED Blinking

SSID INFORMATION

	#	SSID	Enabled	Hidden	Radio	Security	Captive Portal	Clients in 5 mins(2.4G/5G)
□	1	SNGUEST	☑	■	2.4G 5G	WPA2-PSK	Click Through	0 (0/0)
□	2	SNWL	☑	■	2.4G 5G	WPA2-PSK	None	0 (0/0)
□	3	EnGenius_Screenly	☑	■	2.4G 5G	WPA2-PSK	None	0 (0/0)

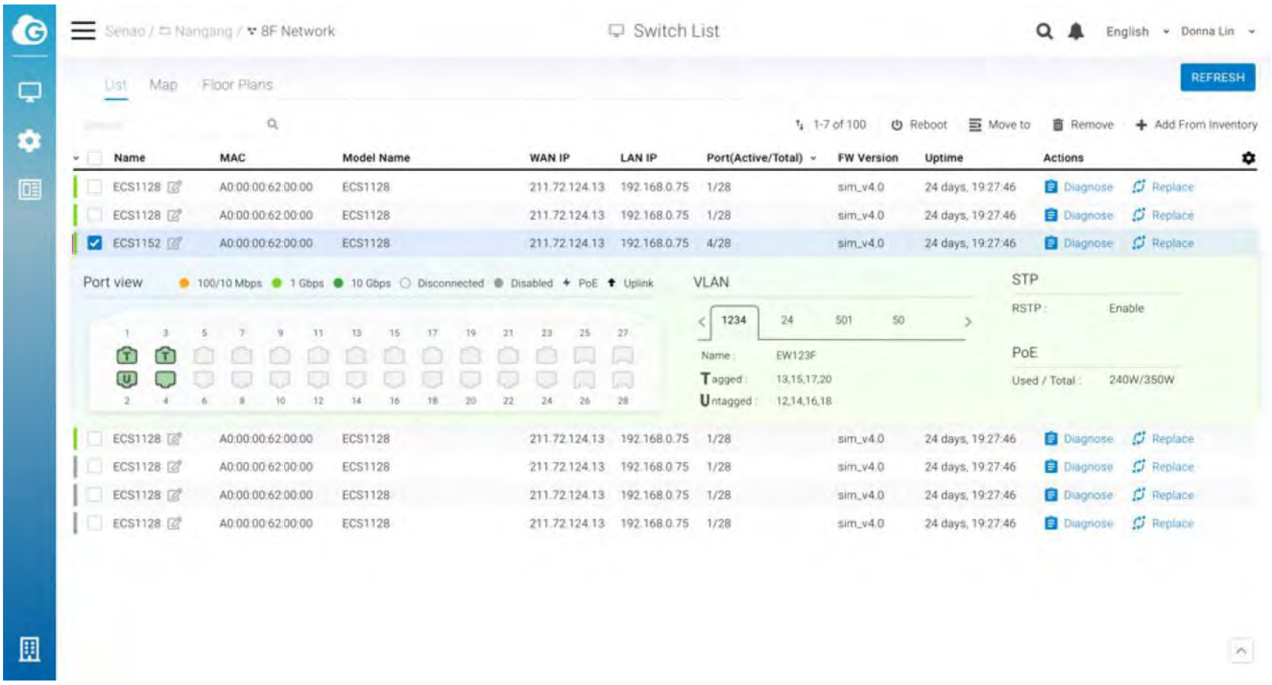
Throughput 2.4G(bps) Tx: 0 Rx: 0

Throughput 5G(bps) Tx: 0 Rx: 0

- 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.



	Name	MAC	Model Name	WAN IP	LAN IP	Port(Active/Total)	FW Version	Uptime	Actions
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace
☑	ECS1152	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	4/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace

VLAN

1234 | 24 | 501 | 50

Name : EW123F

Tagged : 13,15,17,20

Untagged : 12,14,16,18

STP

RSTP : Enable

PoE

Used / Total : 240W/350W

	Name	MAC	Model Name	WAN IP	LAN IP	Port(Active/Total)	FW Version	Uptime	Actions
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace
□	ECS1128	A0:00:00:62:00:00	ECS1128	211.72.124.13	192.168.0.75	1/28	sim_v4.0	24 days, 19:27:46	Diagnose Replace

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.

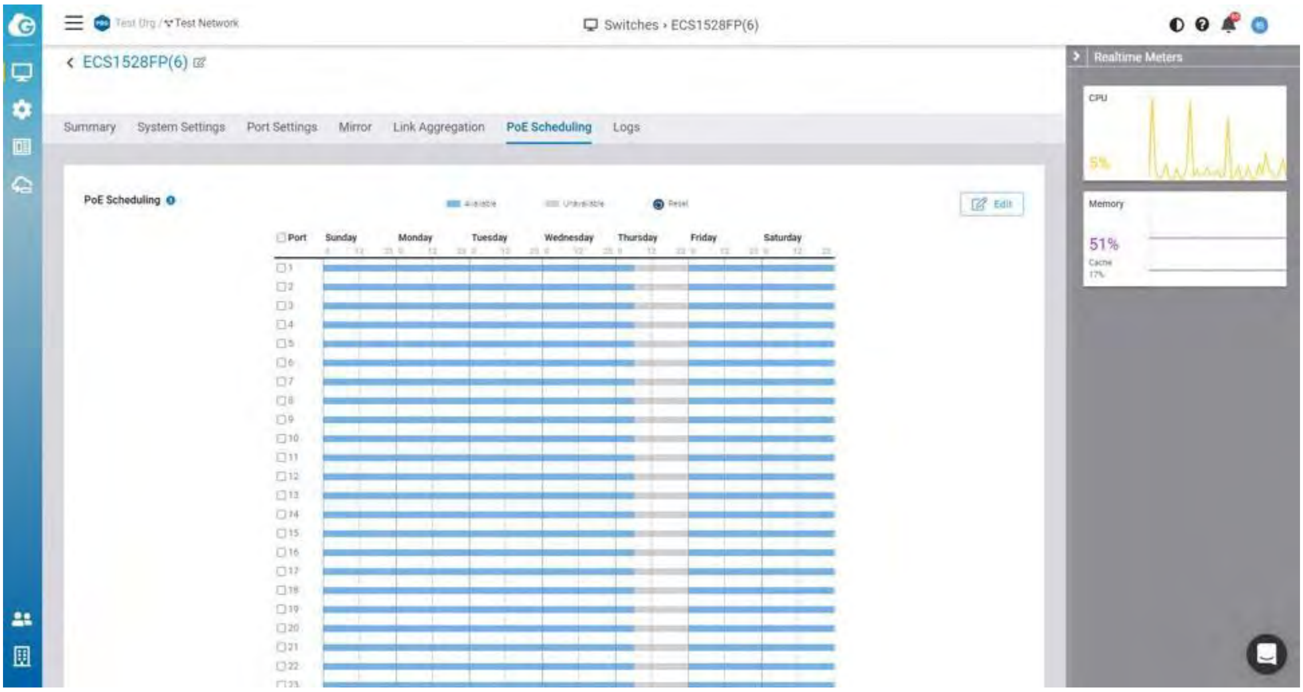
Remove From Networks: Select one or multiple switches and click to remove the switches from the current organization/hierarchy view/network.

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

Detail: Click to display the individual switch details.

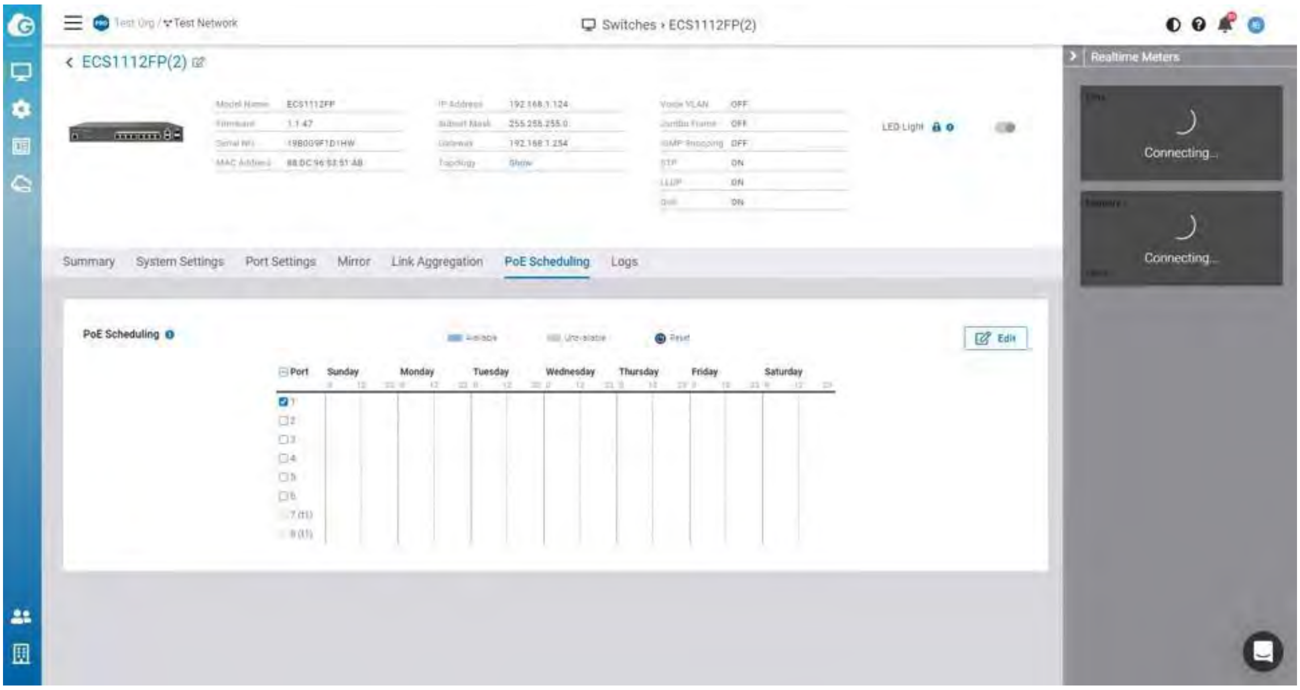
PoE scheduling

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

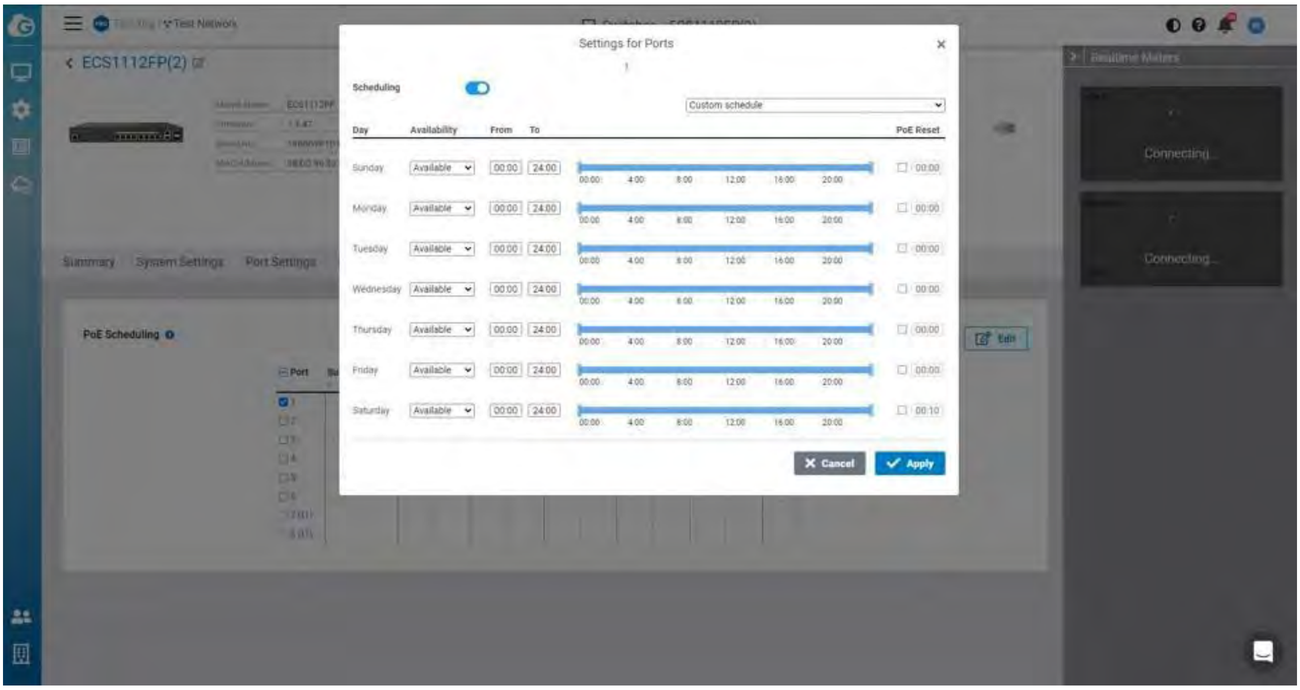


Edit PoE Scheduling

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.

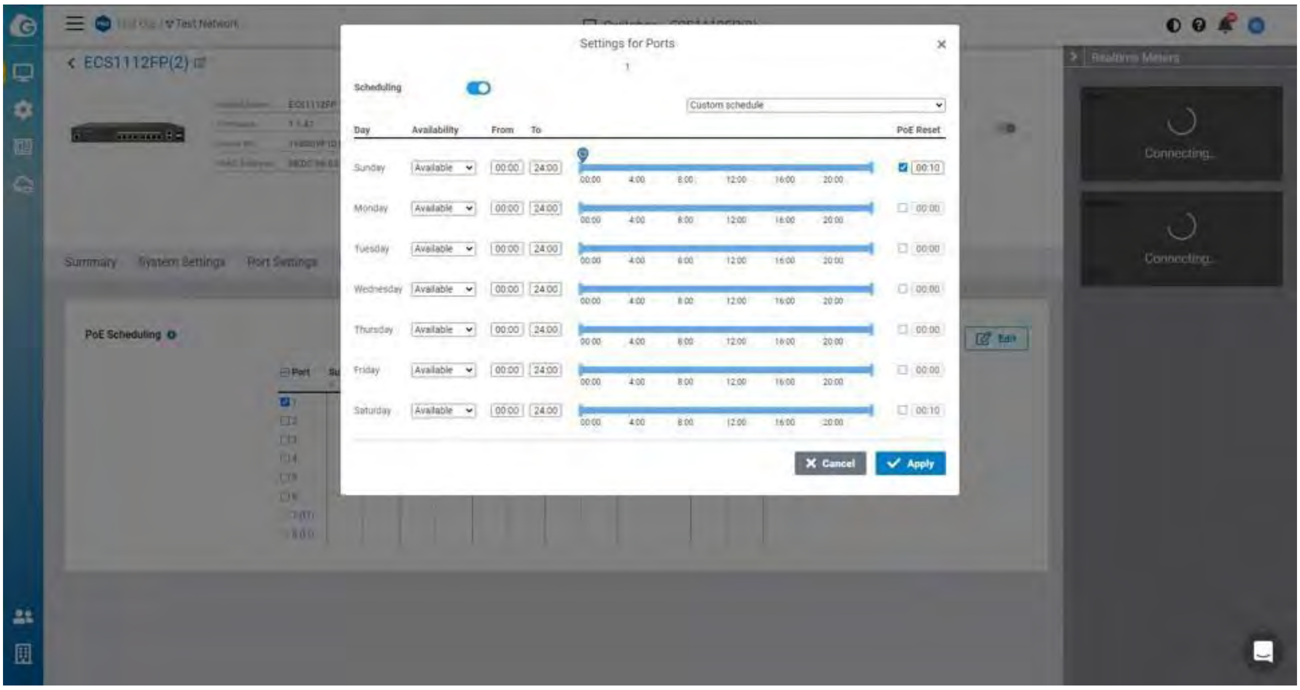


Scheduling: on

Custom schedule

Day	Availability	From	To	PoE Reset
Sunday	Available	00:00	24:00	□ 00:00
Monday	Available	00:00	24:00	□ 00:00
Tuesday	Available	00:00	24:00	□ 00:00
Wednesday	Available	00:00	24:00	□ 00:00
Thursday	Available	00:00	24:00	□ 00:00
Friday	Available	00:00	24:00	□ 00:00
Saturday	Available	00:00	24:00	□ 00:10

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



Settings for Ports

1

Scheduling

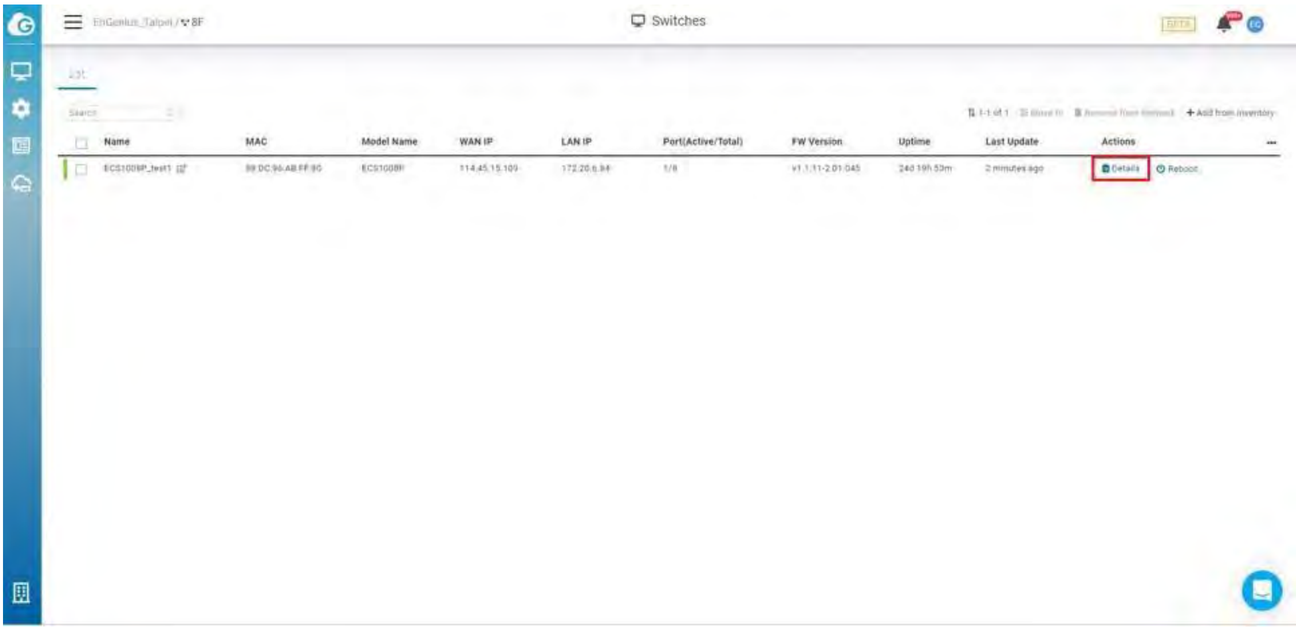
Custom schedule

Day	Availability	From	To	PoE Reset
Sunday	Available	00:00	24:00	☑ 00:10
Monday	Available	00:00	24:00	□ 00:00
Tuesday	Available	00:00	24:00	□ 00:00
Wednesday	Available	00:00	24:00	□ 00:00
Thursday	Available	00:00	24:00	□ 00:00
Friday	Available	00:00	24:00	□ 00:00
Saturday	Available	00:00	24:00	□ 00:10

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.



EnGenius_Taipei / 8F

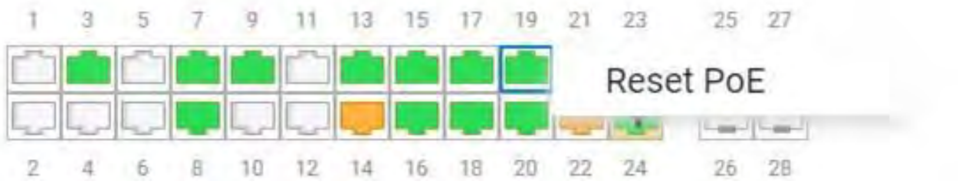
Switches

Name	MAC	Model Name	WAN IP	LAN IP	Port(Active/Total)	FW Version	Uptime	Last Update	Actions
ECS1008P_test1	88:DC:96:AB:FF:90	ECS1008P	114.45.15.109	172.20.6.84	1/8	v1.1.11-2.01.045	24d 19h 53m	2 minutes ago	Details Reboot

Summary

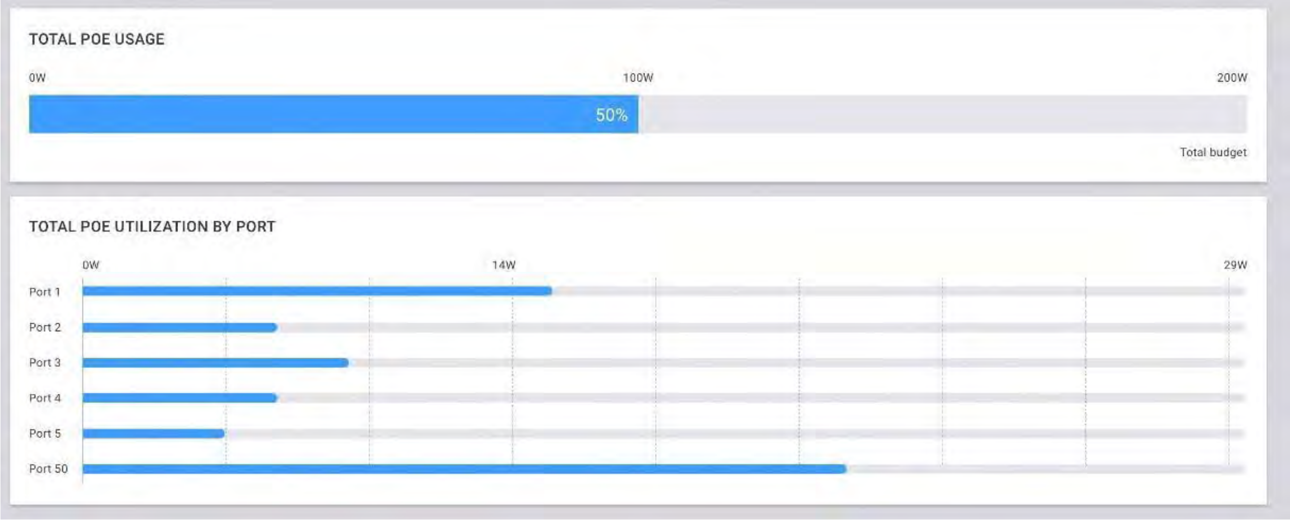
PoE reset from the Switch Panel :

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.

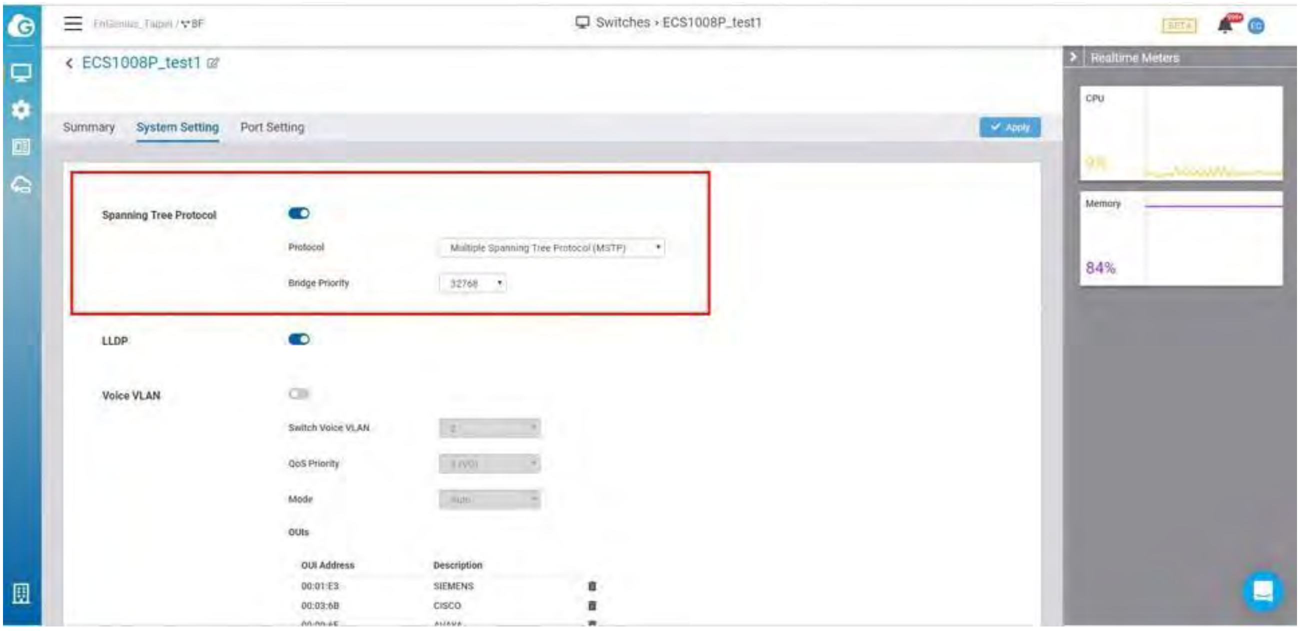


System Setting

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.



Spanning Tree Protocol ●

Protocol: Multiple Spanning Tree Protocol (MSTP)

Bridge Priority: 32768

LLDP ●

Voice VLAN ○

Switch Voice VLAN: 2

QoS Priority: 5 (VO)

Mode: Auto

OUIs

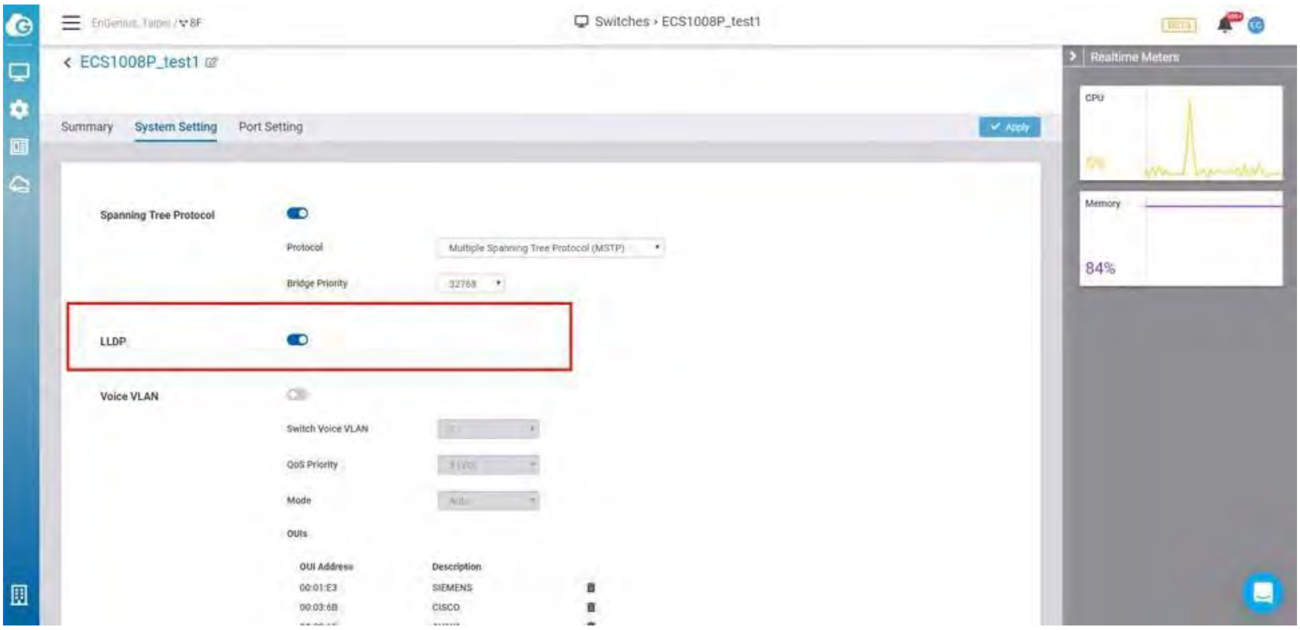
OUI Address	Description
00:01:E3	SIEMENS
00:03:6B	CISCO

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.



Spanning Tree Protocol ●

Protocol: Multiple Spanning Tree Protocol (MSTP)

Bridge Priority: 32768

LLDP ●

Voice VLAN ○

Switch Voice VLAN

QoS Priority

Mode

OUIs

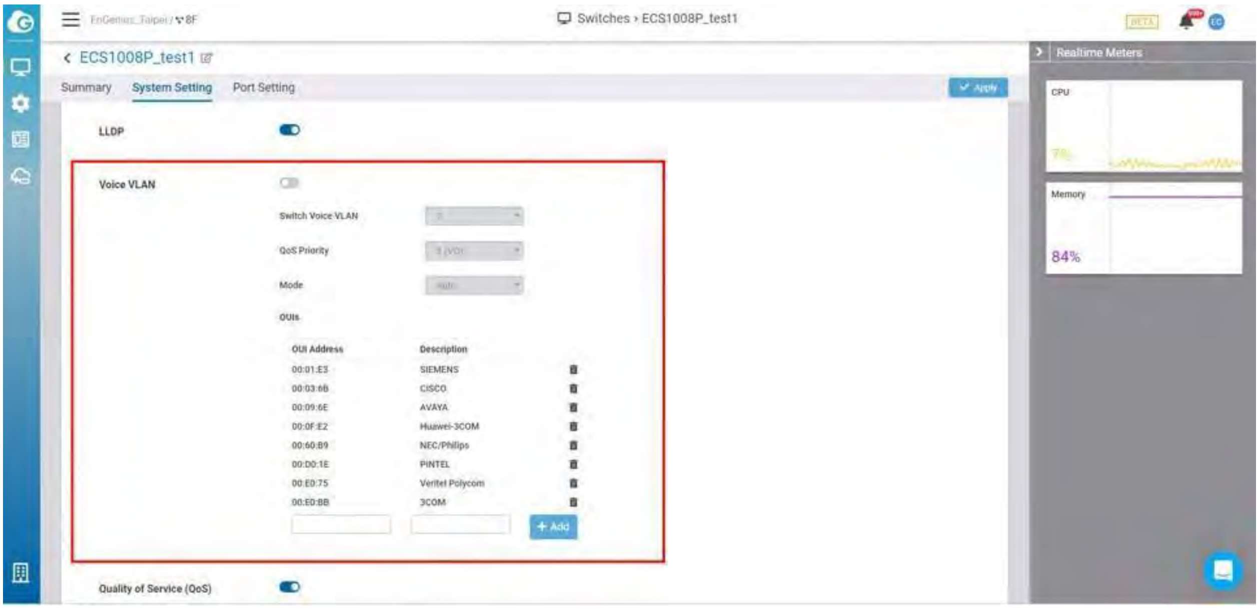
OUI Address	Description
00:01:E3	SIEMENS
00:03:6B	CISCO

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.



LLDP ●

Voice VLAN ○

Switch Voice VLAN

QoS Priority: 3 (VO)

Mode: Auto

OUIs

OUI Address	Description
00:01:E3	SIEMENS
00:03:6B	CISCO
00:09:6E	AVAYA
00:0F:E2	Huawei-3COM
00:60:B9	NEC/Philips
00:D0:1E	PINTEL
00:E0:75	Veritel Polycom
00:E0:BB	3COM

Quality of Service (QoS) ●

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.

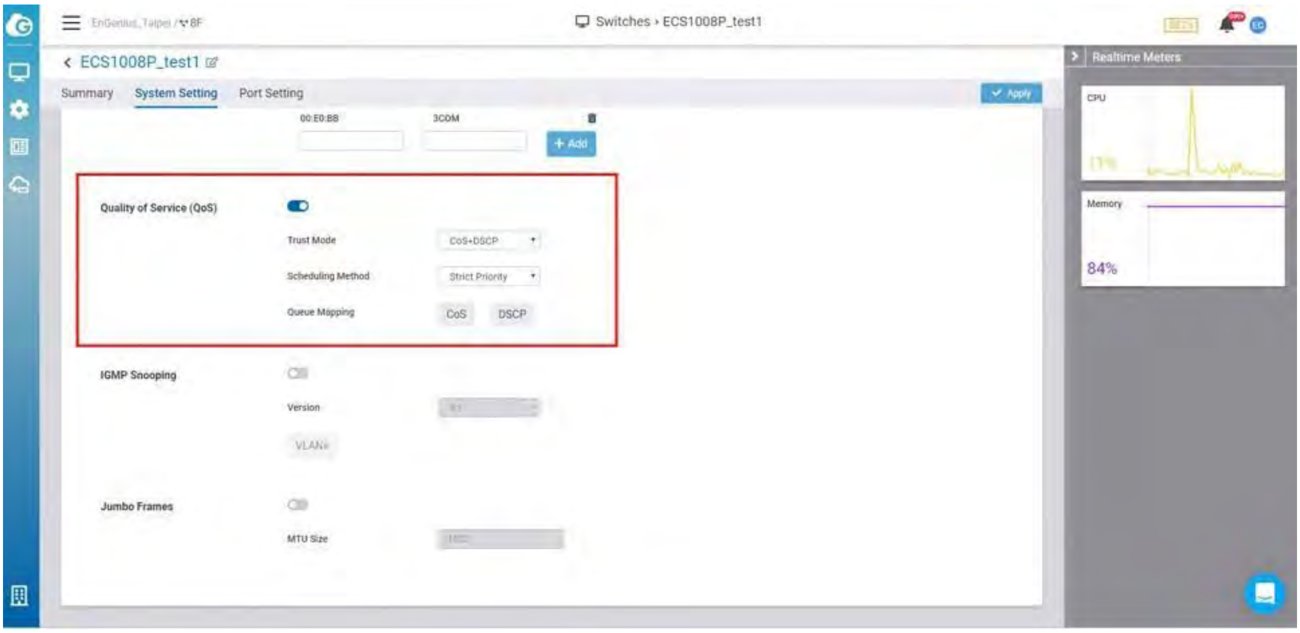
Switch Voice VLAN: Allows you to choose what VLAN is used for Voice VLAN. You can set up VLANs in Port Settings.

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.



00:E0:BB 3COM

Quality of Service (QoS)

Trust Mode: CoS+DSCP

Scheduling Method: Strict Priority

Queue Mapping: CoS DSCP

IGMP Snooping

Version

VLANs

Jumbo Frames

MTU Size

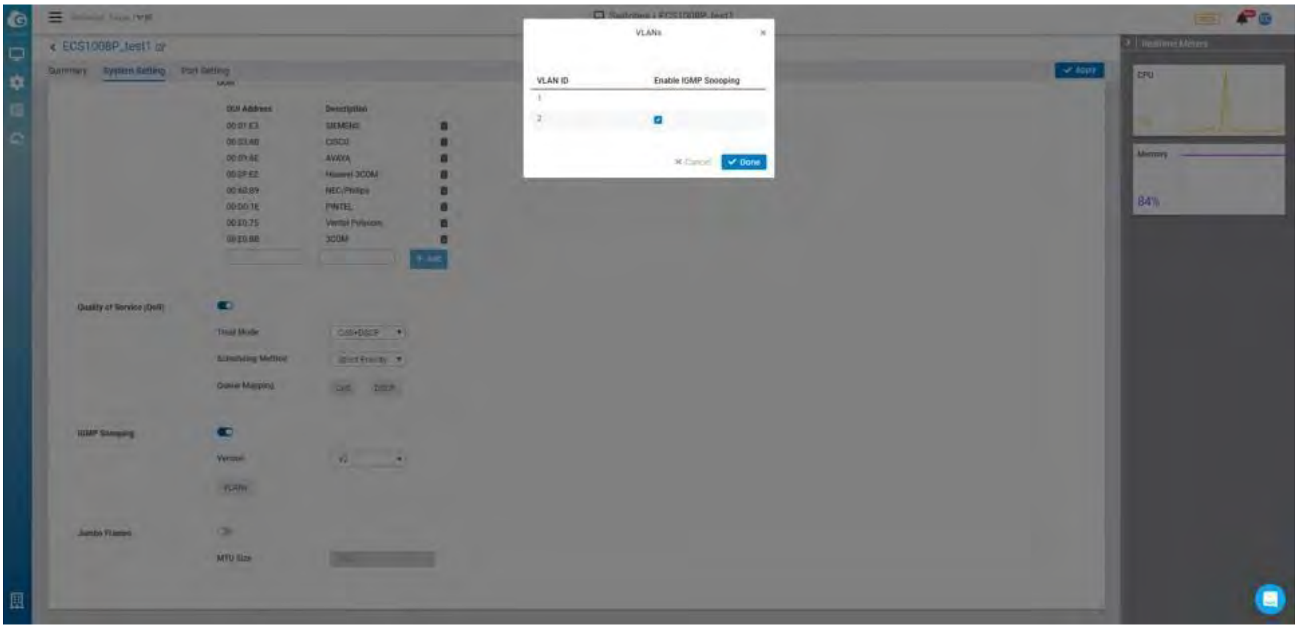
Trust Mode: Allows you to define whether the switch will use CoS, DSCP, or both trust modes for QoS.

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.



VLANs

VLAN ID	Enable IGMP Snooping
1	
2	☑

✕ Cancel ✓ Done

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

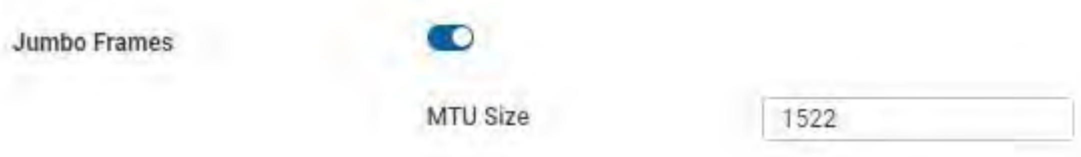
VLANS: You can enable IGMP Snooping for any VLAN by selecting the corresponding checkbox next to the VLAN ID.

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.

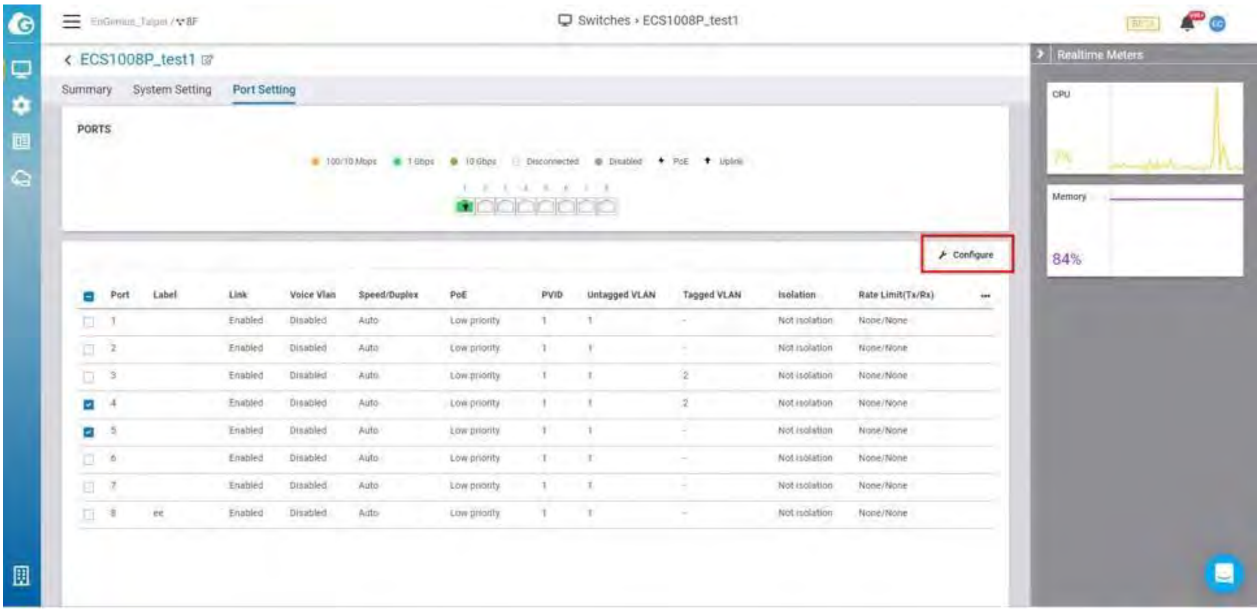


Jumbo Frames

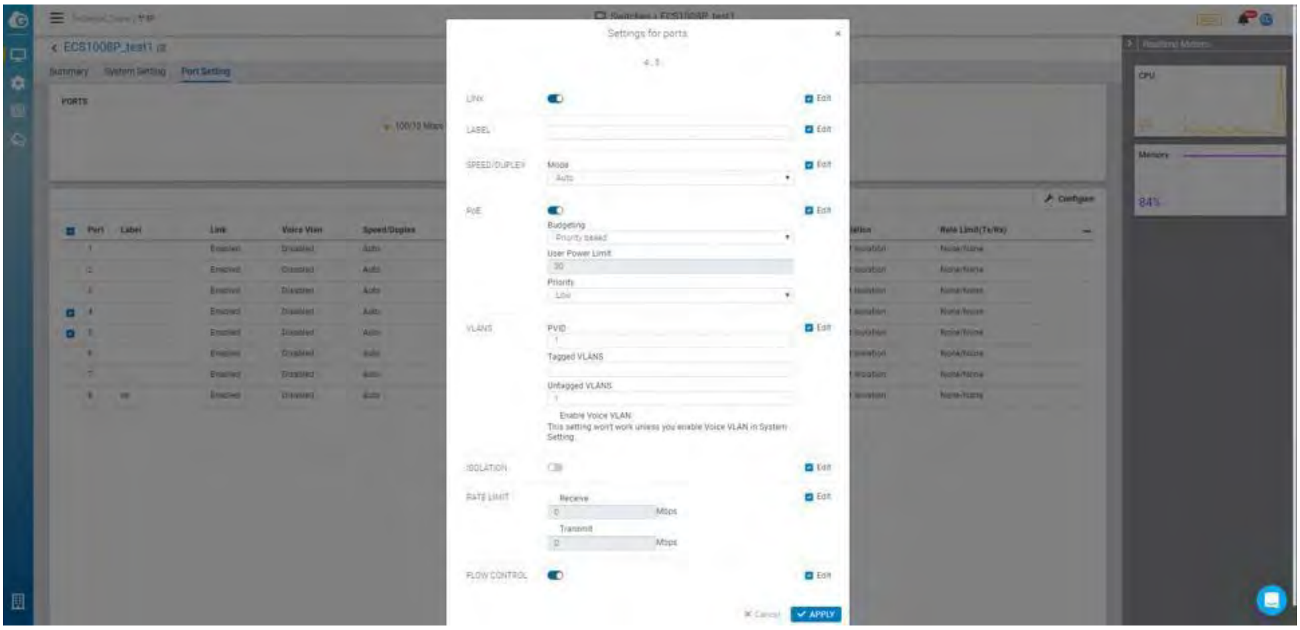
MTU Size 1522

Port Settings

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



	Port	Label	Link	Voice Vlan	Speed/Duplex	PoE	PVID	Untagged VLAN	Tagged VLAN	Isolation	Rate Limit(Tx/Rx)
□	1		Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None
□	2		Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None
□	3		Enabled	Disabled	Auto	Low priority	1	1	2	Not isolation	None/None
☑	4		Enabled	Disabled	Auto	Low priority	1	1	2	Not isolation	None/None
☑	5		Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None
□	6		Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None
□	7		Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None
□	8	ee	Enabled	Disabled	Auto	Low priority	1	1	-	Not isolation	None/None



Settings for ports

4, 5

LINK ● ☑ Edit

LABEL ☑ Edit

SPEED/DUPLEX Mode: Auto ☑ Edit

PoE ● ☑ Edit
Budgeting: Priority based
User Power Limit: 30
Priority: Low

VLANS ☑ Edit
PVID: 1
Tagged VLANS
Untagged VLANS: 1
Enable Voice VLAN
This setting won't work unless you enable Voice VLAN in System Setting

ISOLATION ○ ☑ Edit

RATE LIMIT ☑ Edit
Receive: 0 Mbps
Transmit: 0 Mbps

FLOW CONTROL ● ☑ Edit

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.

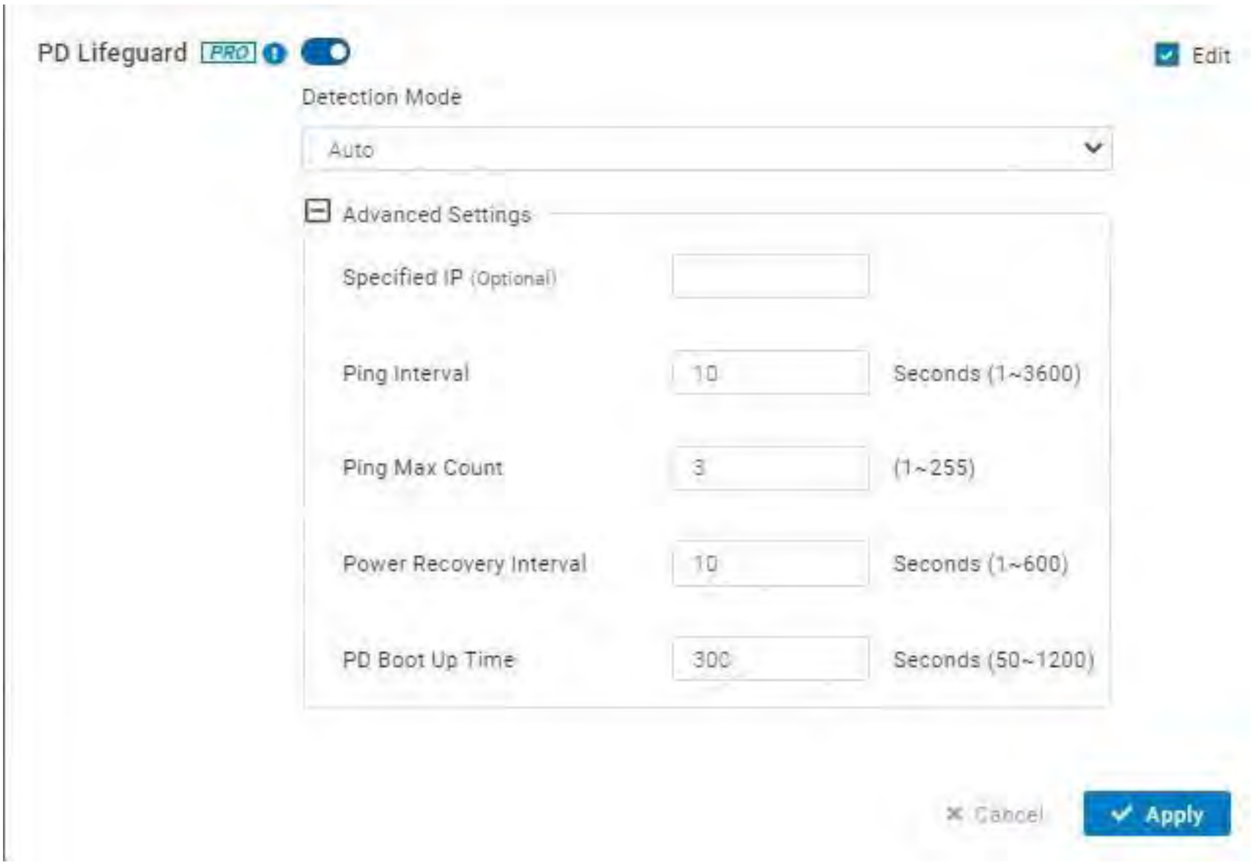
Flow Control: Enabling this will have the switch regulate traffic during times of congestion.

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.



Detection Mode: Auto

Advanced Settings

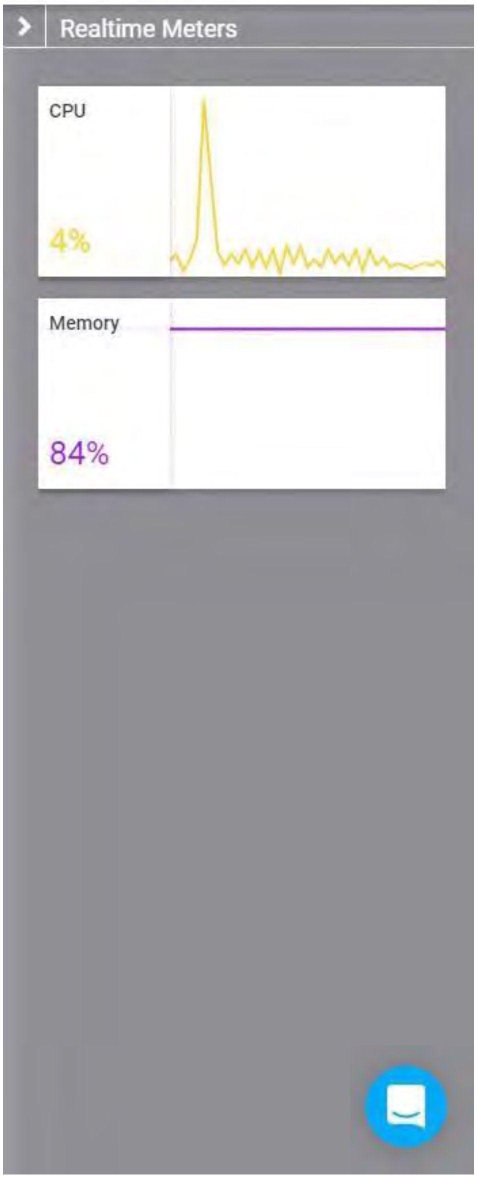
Specified IP (Optional)		
Ping Interval	10	Seconds (1~3600)
Ping Max Count	3	(1~255)
Power Recovery Interval	10	Seconds (1~600)
PD Boot Up Time	300	Seconds (50~1200)

Realtime Meters

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

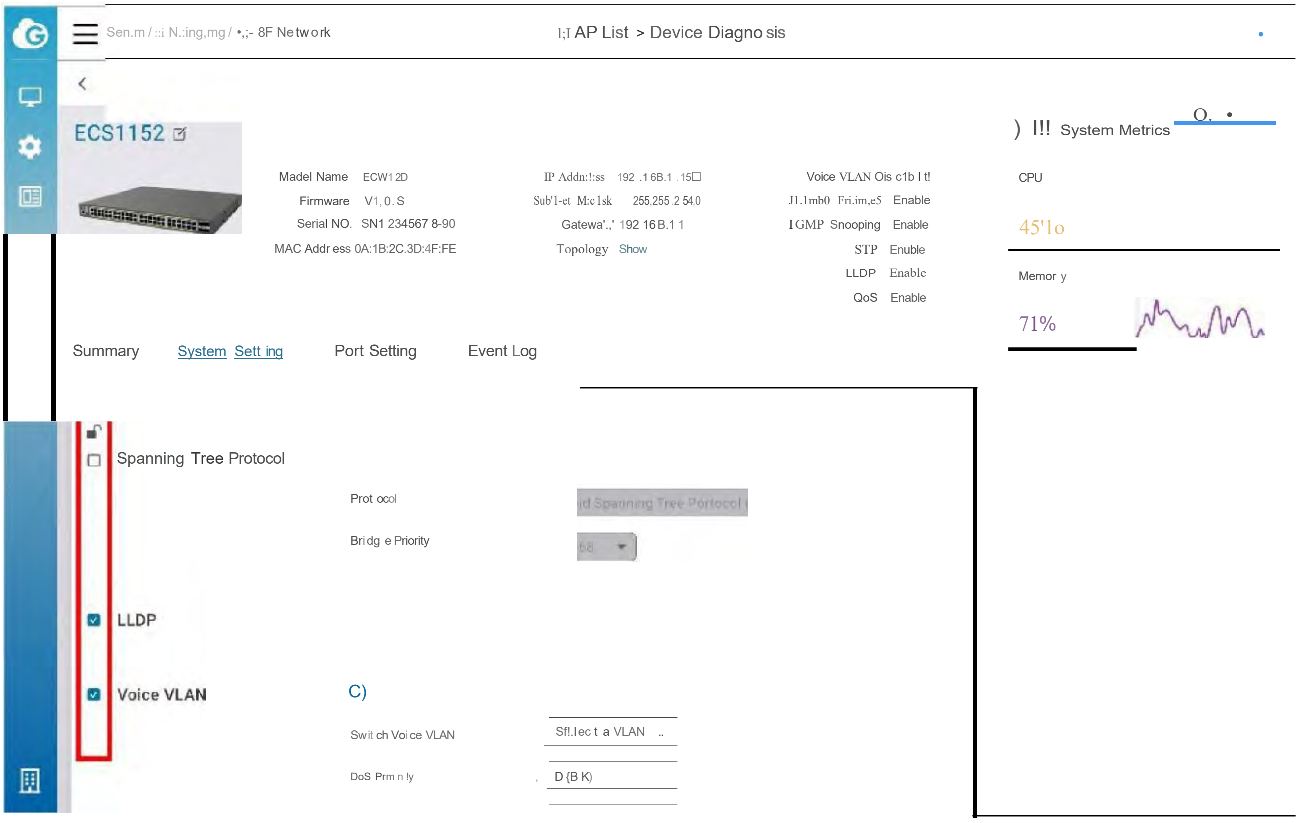
- CPU
- Memory

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

I;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 Ois c1b I t!

J1.1mb0 Fri.im,e5 Enable

IGMP Snooping Enable

STP Enuble

LLDP Enable

QoS Enable

) !!! System Metrics

CPU

45'1o

Memor y

71%

Summary System Sett ing Port Setting Event Log

□ Spanning Tree Protocol

Prot ocol: d Spanning Tree Portocol

Brid g e Priority: 68

☑ LLDP

☑ Voice VLAN

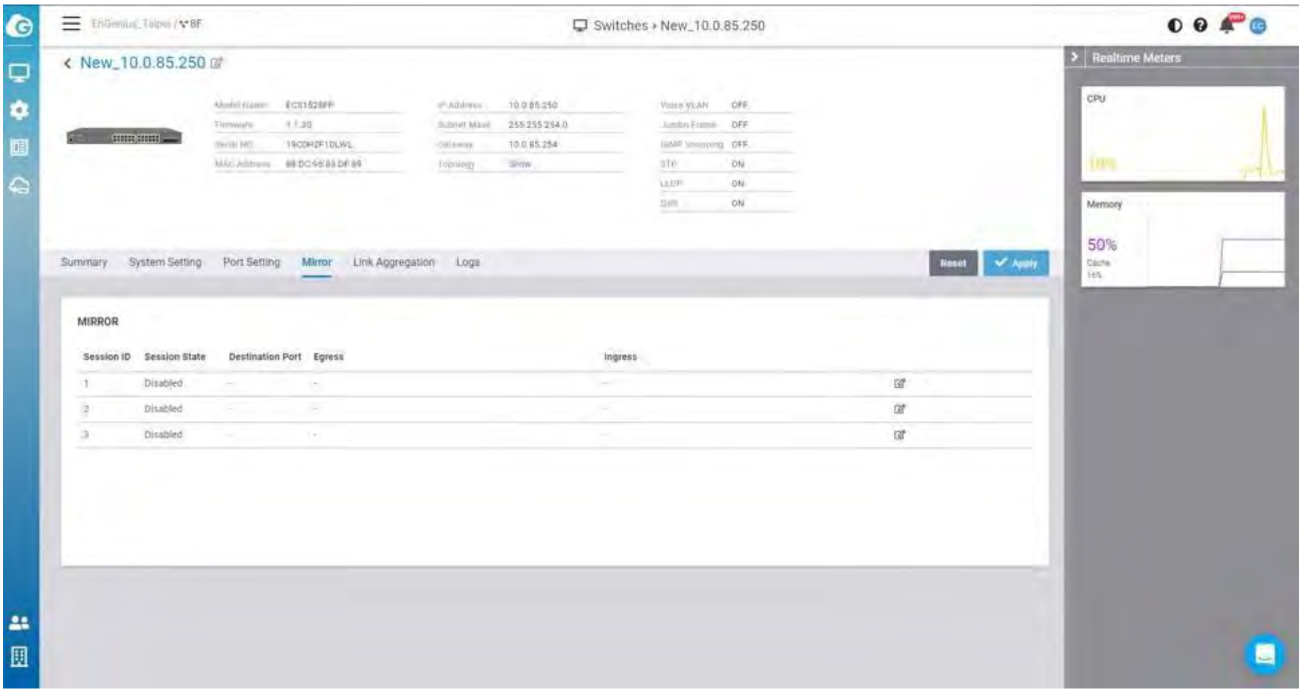
C)

Swit ch Voi ce VLAN: Sf!.lec t a VLAN ..

DoS Prm n ly: 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



Model name	ECS1528FP	IP Address	10.0.85.250	Voice VLAN	OFF
Firmware	1.1.30	Subnet Mask	255.255.254.0	Jumbo Frame	OFF
Serial NO	19C0H2F10LWL	Gateway	10.0.85.254	IGMP Snooping	OFF
MAC Address	88:DC:96:83:DF:89	Topology	Show	STP	ON
				LLDP	ON
				[illegible]	ON

MIRROR

Session ID	Session State	Destination Port	Egress	Ingress
1	Disabled	–	–	–
2	Disabled	–	–	–
3	Disabled	–	–	–

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 .

D Port was assigned to a destination port .

E Port was assigned only data being sent will be mirrored .

I Port was assigned only data being received will be mirrored .

EI 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

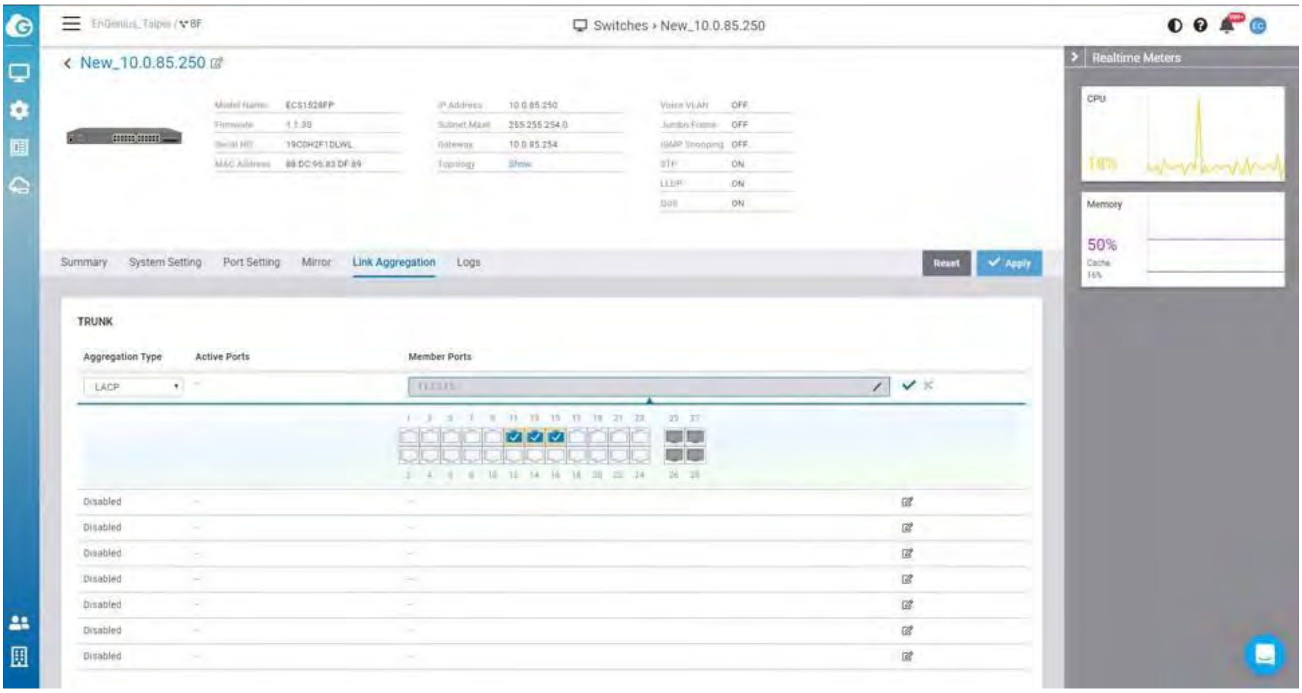
How to **Configure**

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.



EnGenius_Taipei / 8F

Switches › New_10.0.85.250

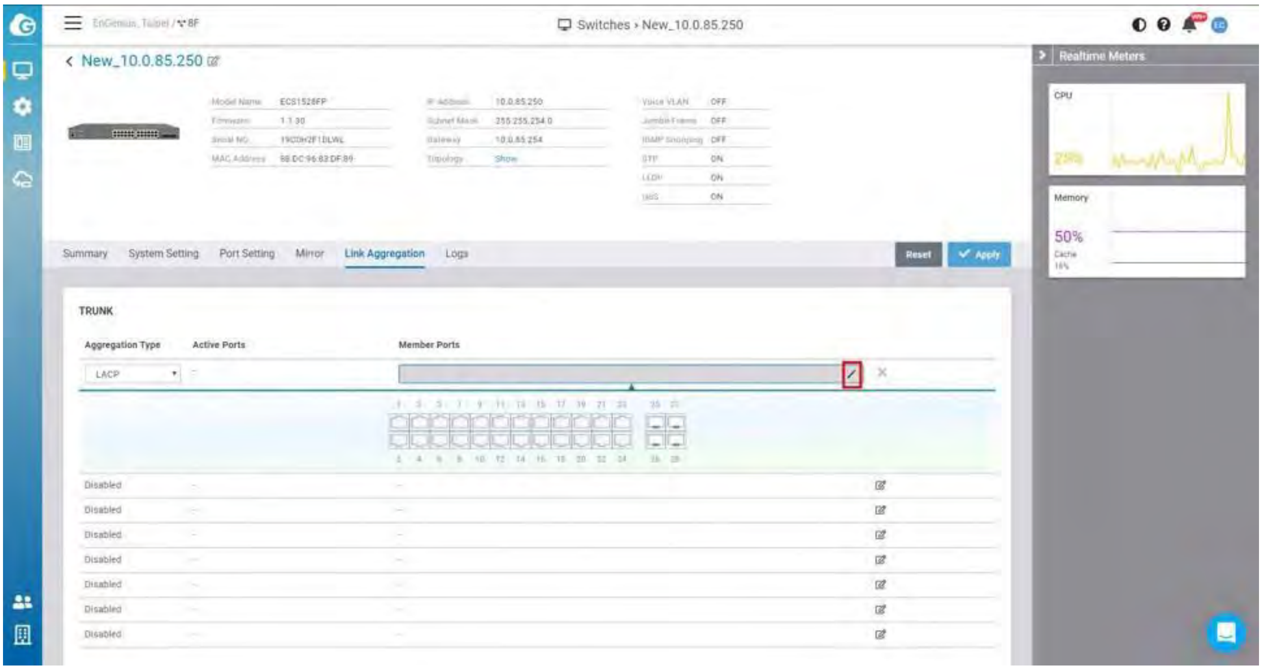
New_10.0.85.250

Model Name	ECS1528FP	IP Address	10.0.85.250	Voice VLAN	OFF
Firmware	1.1.30	Subnet Mask	255.255.254.0	Jumbo Frame	OFF
Serial NO	19C0H2F1DLWL	Gateway	10.0.85.254	IGMP Snooping	OFF
MAC Address	88:DC:96:83:DF:89	Topology	Show	STP	ON
				LLDP	ON
				QoS	ON

TRUNK

Aggregation Type	Active Ports	Member Ports
LACP	–	11,13,15
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–

2. Click Pencil icon to input port numbers



EnGenius_Taipei / 8F

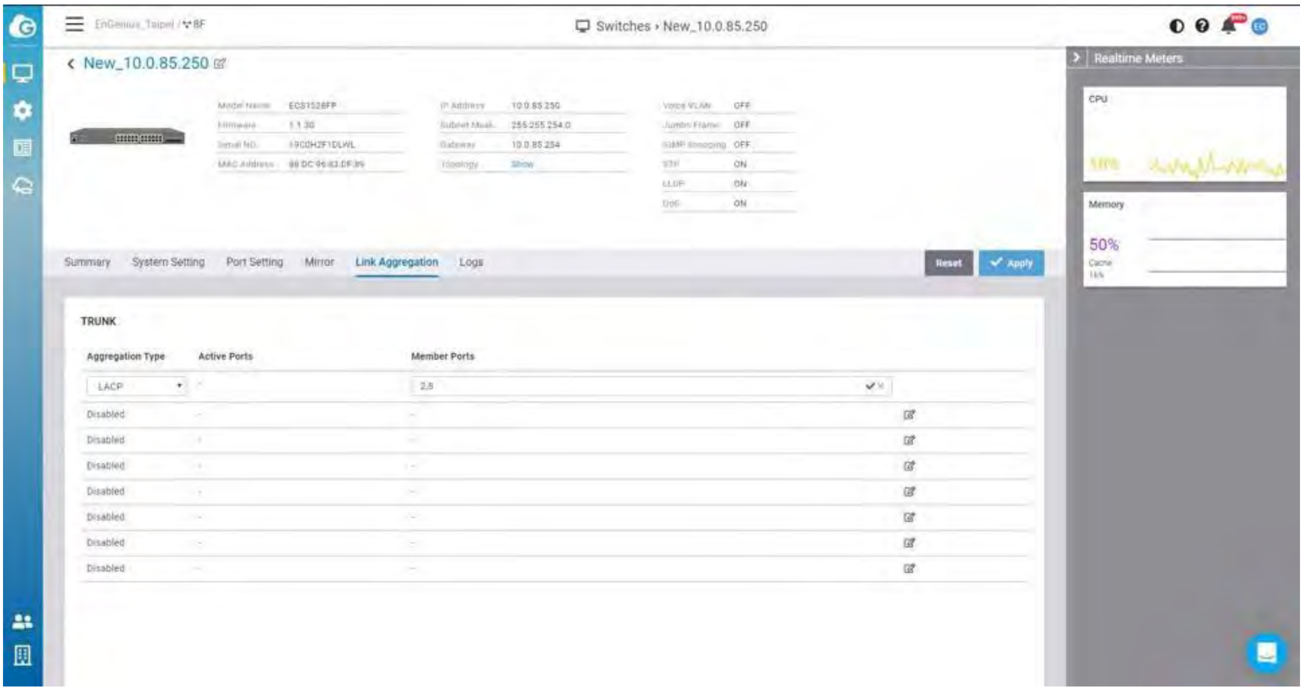
Switches › New_10.0.85.250

New_10.0.85.250

Model Name	ECS1528FP	IP Address	10.0.85.250	Voice VLAN	OFF
Firmware	1.1.30	Subnet Mask	255.255.254.0	Jumbo Frame	OFF
Serial NO	19C0H2F1DLWL	Gateway	10.0.85.254	IGMP Snooping	OFF
MAC Address	88:DC:96:83:DF:89	Topology	Show	STP	ON
				LLDP	ON
				QoS	ON

TRUNK

Aggregation Type	Active Ports	Member Ports
LACP	–	
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–
Disabled	–	–



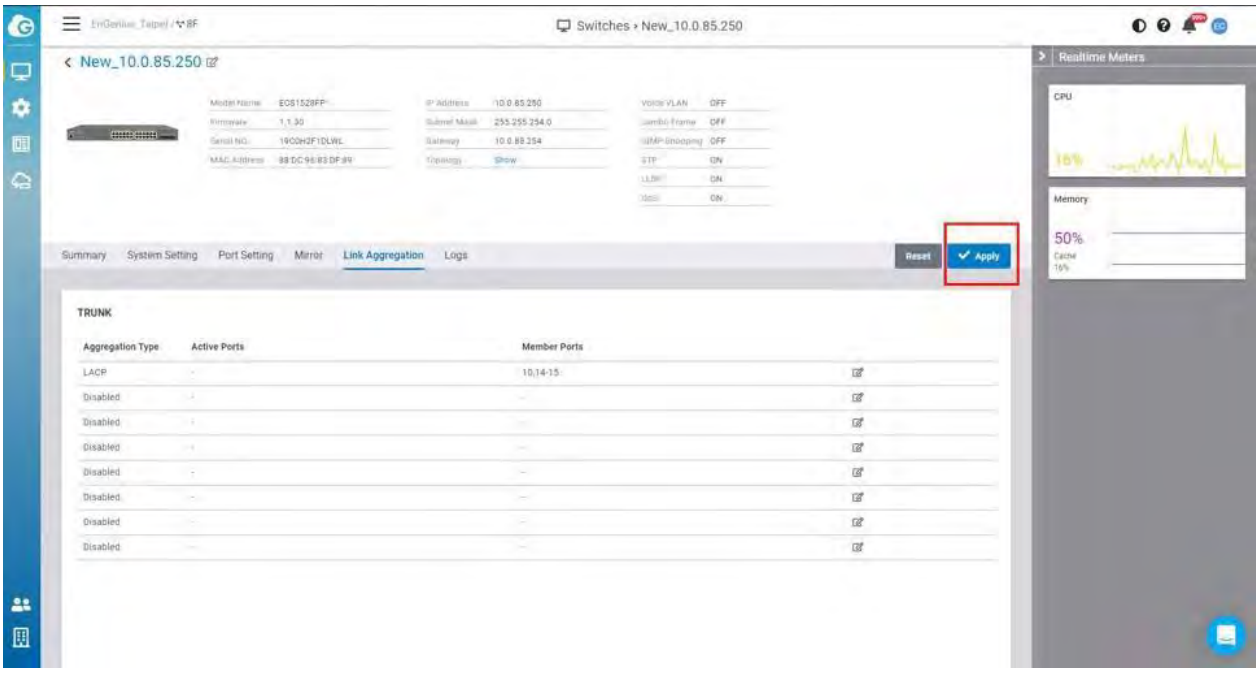
New_10.0.85.250

Model Name	ECS1528FP	IP Address	10.0.85.250	Voice VLAN	OFF
Firmware	1.1.30	Subnet Mask	255.255.254.0	Jumbo Frame	OFF
Serial NO.	19C0H2F1DLWL	Gateway	10.0.85.254	IGMP Snooping	OFF
MAC Address	88:DC:96:83:DF:39	Topology	Show	STP	ON
				LLDP	ON
				QoS	ON

TRUNK

Aggregation Type	Active Ports	Member Ports
LACP	-	2,8
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-

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



New_10.0.85.250

Model Name	ECS1528FP	IP Address	10.0.85.250	Voice VLAN	OFF
Firmware	1.1.30	Subnet Mask	255.255.254.0	Jumbo Frame	OFF
Serial NO.	19C0H2F1DLWL	Gateway	10.0.85.254	IGMP Snooping	OFF
MAC Address	88:DC:96:83:DF:39	Topology	Show	STP	ON
				LLDP	ON
				QoS	ON

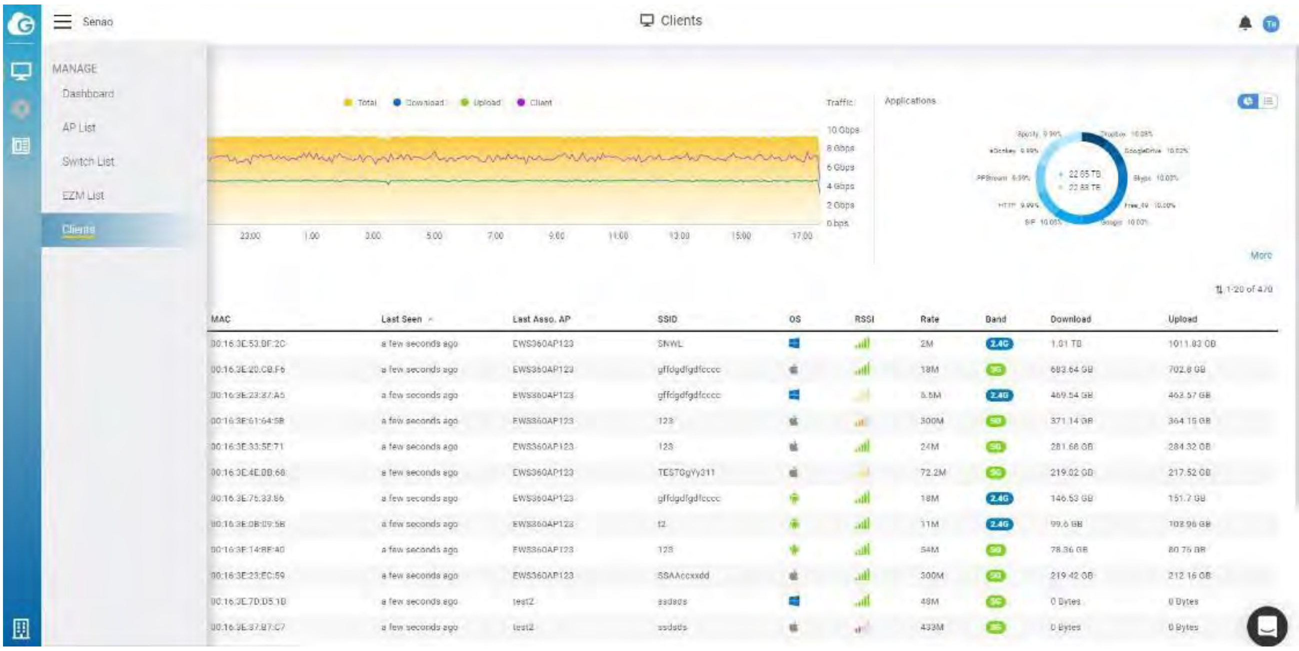
TRUNK

Aggregation Type	Active Ports	Member Ports
LACP	-	10,14-15
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-
Disabled	-	-

Managing Clients

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

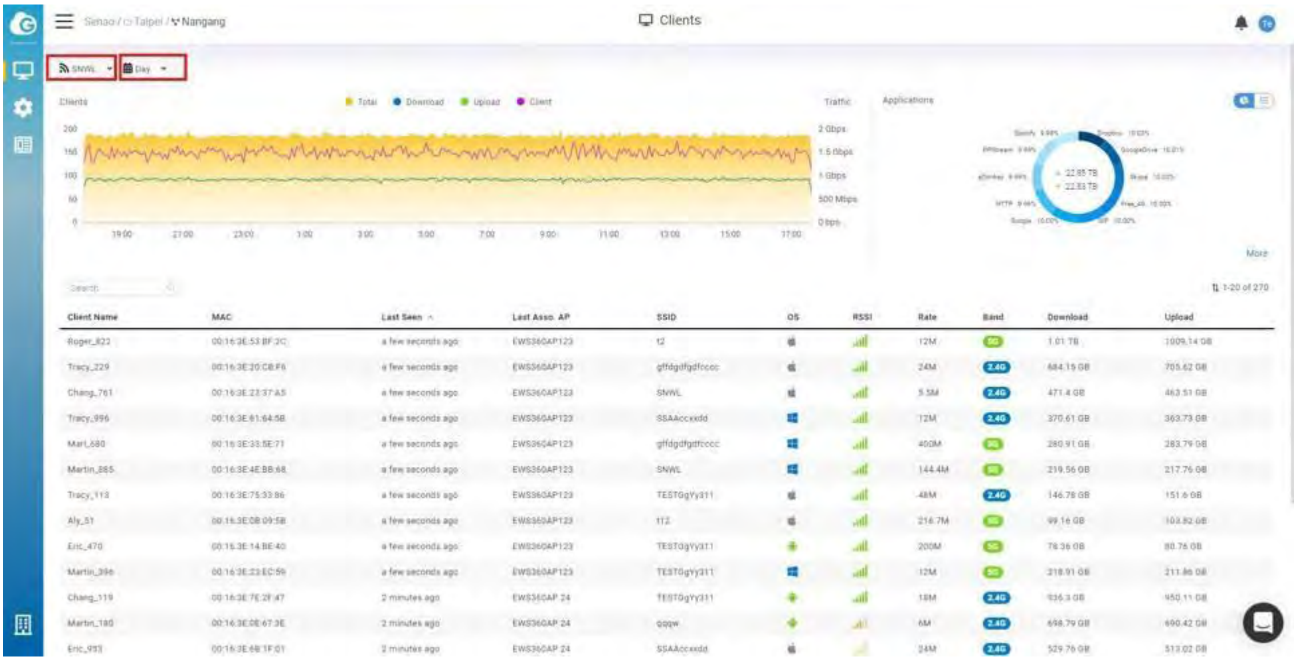
Click Manage -> Clients to access this screen and double-click the organization/hierarchy view/network on the tree to change the scope.



MAC	Last Seen	Last Asso. AP	SSID	OS	RSSI	Rate	Band	Download	Upload
00:16:3E:53:BF:2C	a few seconds ago	EWS360AP123	SNWL			2M	2.4G	1.01 TB	1011.83 GB
00:16:3E:20:CB:F6	a few seconds ago	EWS360AP123	gffdgdfgdfcccc			18M	5G	683.64 GB	702.8 GB
00:16:3E:23:87:A5	a few seconds ago	EWS360AP123	gffdgdfgdfcccc			5.5M	2.4G	469.54 GB	463.57 GB
00:16:3E:61:64:5B	a few seconds ago	EWS360AP123	123			300M	5G	371.14 GB	364.15 GB
00:16:3E:33:5E:71	a few seconds ago	EWS360AP123	123			24M	5G	281.68 GB	284.32 GB
00:16:3E:4E:DD:68	a few seconds ago	EWS360AP123	TESTGgYy311			72.2M	5G	219.02 GB	217.52 GB
00:16:3E:76:33:86	a few seconds ago	EWS360AP123	gffdgdfgdfcccc			18M	2.4G	146.53 GB	151.7 GB
00:16:3E:0B:09:5B	a few seconds ago	EWS360AP123	t2			11M	2.4G	99.6 GB	102.96 GB
00:16:3E:14:BE:40	a few seconds ago	EWS360AP123	123			54M	5G	78.36 GB	80.75 GB
00:16:3E:23:EC:59	a few seconds ago	EWS360AP123	SSAAccxxdd			300M	5G	219.42 GB	212.16 GB
00:16:3E:7D:D5:1B	a few seconds ago	test2	ssdsds			48M	5G	0 Bytes	0 Bytes
00:16:3E:37:B7:C7	a few seconds ago	test2	ssdsds			433M	5G	0 Bytes	0 Bytes

Filtering the Clients List

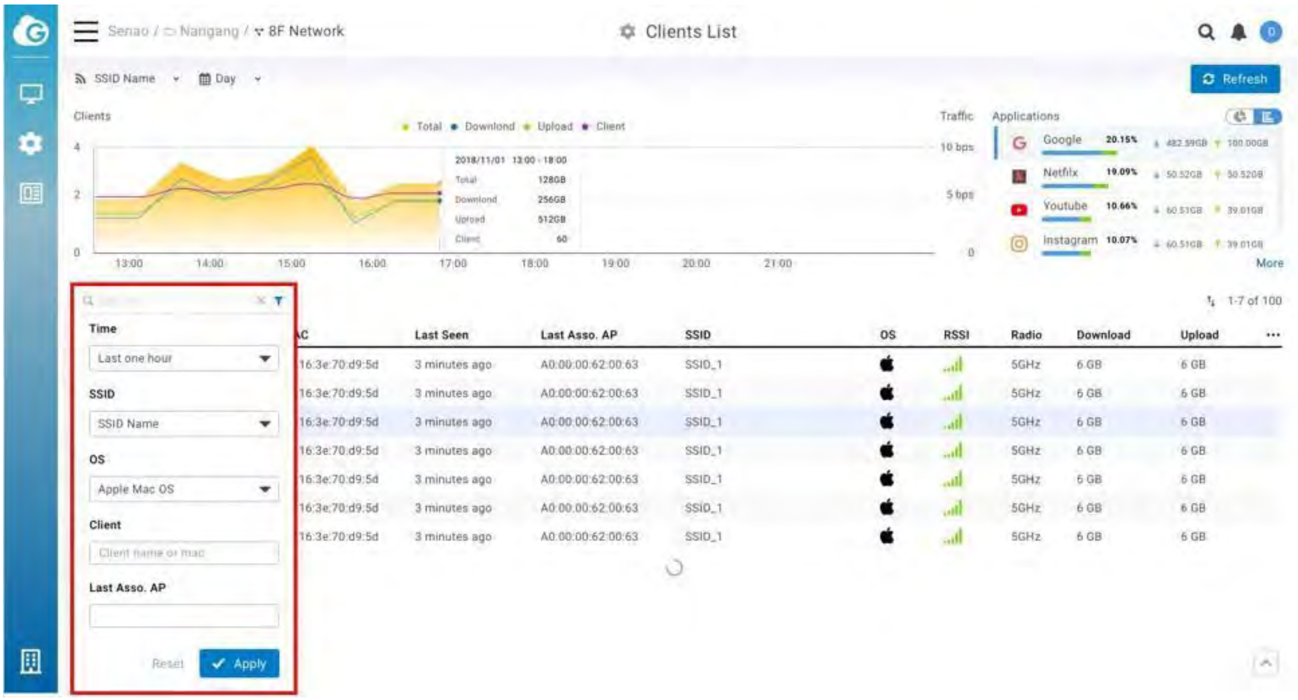
The list of clients can be customized based on time intervals, and the chart can be customized based on time intervals and SSIDs. To change these parameters, use the appropriate dropdown menu at the top of the screen.



Client Name	MAC	Last Seen	Last Asso. AP	SSID	OS	RSSI	Rate	Band	Download	Upload
Roger_822	00:16:3E:53:BF:2C	a few seconds ago	EWS360AP123	t2		📶	12M	5G	1.01 TB	1009.14 GB
Tracy_229	00:16:3E:20:CB:F6	a few seconds ago	EWS360AP123	gffdgdfgdfcccc		📶	24M	2.4G	684.15 GB	705.62 GB
Chang_761	00:16:3E:22:37:A5	a few seconds ago	EWS360AP123	SNWL		📶	5.5M	2.4G	471.4 GB	463.51 GB
Tracy_996	00:16:3E:61:64:5B	a few seconds ago	EWS360AP123	SSAAccxxdd	⊞	📶	12M	2.4G	370.61 GB	363.73 GB
Mari_680	00:16:3E:33:5E:71	a few seconds ago	EWS360AP123	gffdgdfgdfcccc	⊞	📶	400M	5G	280.91 GB	283.79 GB
Martin_885	00:16:3E:4E:BB:68	a few seconds ago	EWS360AP123	SNWL	⊞	📶	144.4M	5G	219.56 GB	217.76 GB
Tracy_113	00:16:3E:75:33:86	a few seconds ago	EWS360AP123	TESTGgYy311		📶	48M	2.4G	146.78 GB	151.6 GB
Aly_51	00:16:3E:08:09:5B	a few seconds ago	EWS360AP123	t12		📶	216.7M	5G	99.16 GB	103.82 GB
Eric_470	00:16:3E:14:BE:40	a few seconds ago	EWS360AP123	TESTGgYy311	🤖	📶	200M	5G	78.36 GB	80.76 GB
Martin_396	00:16:3E:23:EC:59	a few seconds ago	EWS360AP123	TESTGgYy311	⊞	📶	12M	5G	218.91 GB	211.86 GB
Chang_119	00:16:3E:7E:2F:47	2 minutes ago	EWS360AP 24	TESTGgYy311	🤖	📶	18M	2.4G	936.3 GB	950.11 GB
Martin_180	00:16:3E:0E:67:3E	2 minutes ago	EWS360AP 24	qqqw	🤖	📶	6M	2.4G	698.79 GB	690.42 GB
Eric_933	00:16:3E:6B:1F:01	2 minutes ago	EWS360AP 24	SSAAccxxdd		📶	24M	2.4G	529.76 GB	513.02 GB

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:



Time: Last one hour

SSID: SSID Name

OS: Apple Mac OS

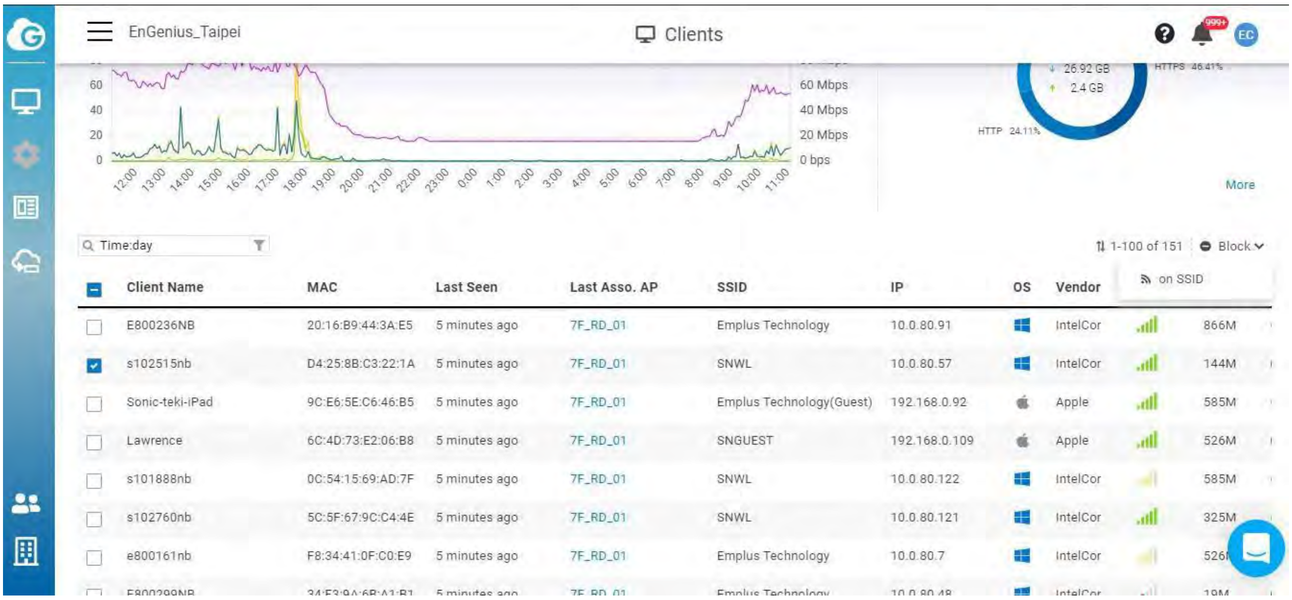
Client: Client name or mac

Last Asso. AP:

AC	Last Seen	Last Asso. AP	SSID	OS	RSSI	Radio	Download	Upload
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB
16:3e:70:d9:5d	3 minutes ago	A0:00:00:62:00:63	SSID_1			5GHz	6 GB	6 GB

Block Clients

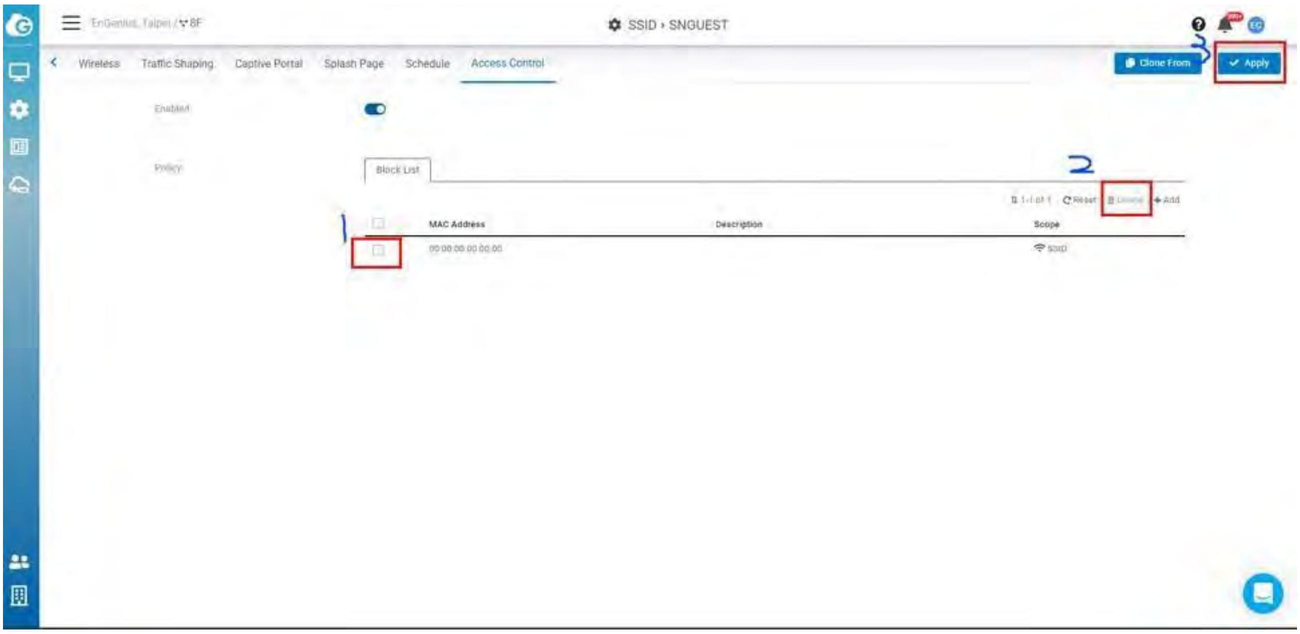
This allows you to block clients on the current SSID that clients connected .



Time:day

☐	Client Name	MAC	Last Seen	Last Asso. AP	SSID	IP	OS	Vendor		
☐	E800236NB	20:16:B9:44:3A:E5	5 minutes ago	7F_RD_01	Emplus Technology	10.0.80.91		IntelCor		866M
☑	s102515nb	D4:25:8B:C3:22:1A	5 minutes ago	7F_RD_01	SNWL	10.0.80.57		IntelCor		144M
☐	Sonic-teki-iPad	9C:E6:5E:C6:46:B5	5 minutes ago	7F_RD_01	Emplus Technology(Guest)	192.168.0.92		Apple		585M
☐	Lawrence	6C:4D:73:E2:06:B8	5 minutes ago	7F_RD_01	SNGUEST	192.168.0.109		Apple		526M
☐	s101888nb	0C:54:15:69:AD:7F	5 minutes ago	7F_RD_01	SNWL	10.0.80.122		IntelCor		585M
☐	s102760nb	5C:5F:67:9C:C4:4E	5 minutes ago	7F_RD_01	SNWL	10.0.80.121		IntelCor		325M
☐	e800161nb	F8:34:41:0F:C0:E9	5 minutes ago	7F_RD_01	Emplus Technology	10.0.80.7		IntelCor		526M
☐	E800299NB	34:F3:9A:6B:A1:B1	5 minutes ago	7F_RD_01	Emplus Technology	10.0.80.48		IntelCor		19M

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



EnGenius_Taipei / 8F

SSID › SNGUEST

Wireless | Traffic Shaping | Captive Portal | Splash Page | Schedule | Access Control

Clone From | ✓ Apply

Enabled ●

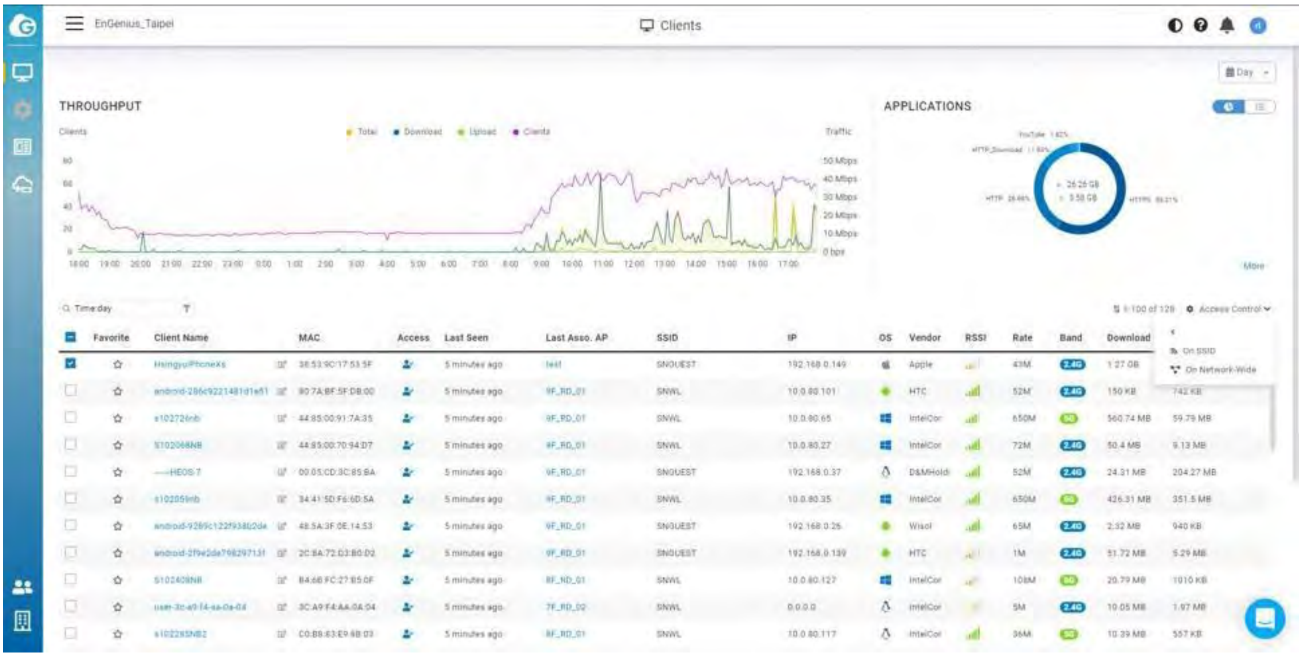
Policy: Block List

1-1 of 1 | Reset | Delete | + Add

□	MAC Address	Description	Scope
□	00:00:00:00:00:00		SSID

VIP Clients

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



EnGenius_Taipei

Clients

Day

Time:day

1-100 of 128 | Access Control ▾ | On SSID | On Network-Wide

☑	Favorite	Client Name	MAC	Access	Last Seen	Last Asso. AP	SSID	IP	OS	Vendor	RSSI	Rate	Band	Download	
☑	☆	HsingyuiPhoneXs	38:53:9C:17:53:5F		5 minutes ago	test	SNGUEST	192.168.0.149		Apple		43M	2.4G	1.27 GB	
□	☆	android-286c9221481d1e51	90:7A:BF:5F:DB:00		5 minutes ago	9F_RD_01	SNWL	10.0.80.101		HTC		52M	2.4G	150 KB	742 KB
□	☆	s102726nb	44:85:00:91:7A:35		5 minutes ago	9F_RD_01	SNWL	10.0.80.65		IntelCor		650M	5G	560.74 MB	59.79 MB
□	☆	S102068NB	44:85:00:70:94:D7		5 minutes ago	9F_RD_01	SNWL	10.0.80.27		IntelCor		72M	2.4G	50.4 MB	9.13 MB
□	☆	----HEOS 7	00:05:CD:3C:85:BA		5 minutes ago	9F_RD_01	SNGUEST	192.168.0.37		D&MHoldi		52M	2.4G	24.31 MB	204.27 MB
□	☆	s102059nb	34:41:5D:F6:6D:5A		5 minutes ago	9F_RD_01	SNWL	10.0.80.35		IntelCor		650M	5G	426.31 MB	351.5 MB
□	☆	android-9289c122f938b2de	48:5A:3F:0E:14:53		5 minutes ago	9F_RD_01	SNGUEST	192.168.0.26		Wisol		65M	2.4G	2.32 MB	940 KB
□	☆	android-2f9e2de798297131	2C:8A:72:D3:B0:D2		5 minutes ago	9F_RD_01	SNGUEST	192.168.0.139		HTC		1M	2.4G	51.72 MB	5.29 MB
□	☆	S102408NB	B4:6B:FC:27:B5:0F		5 minutes ago	8F_RD_01	SNWL	10.0.80.127		IntelCor		108M	5G	20.79 MB	1010 KB
□	☆	user-3c-a9-f4-aa-0a-04	3C:A9:F4:AA:0A:04		5 minutes ago	7F_RD_02	SNWL	0.0.0.0		IntelCor		5M	2.4G	10.05 MB	1.97 MB
□	☆	s102285NB2	C0:B8:83:E9:6B:03		5 minutes ago	8F_RD_01	SNWL	10.0.80.117		IntelCor		36M	5G	10.39 MB	557 KB

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.

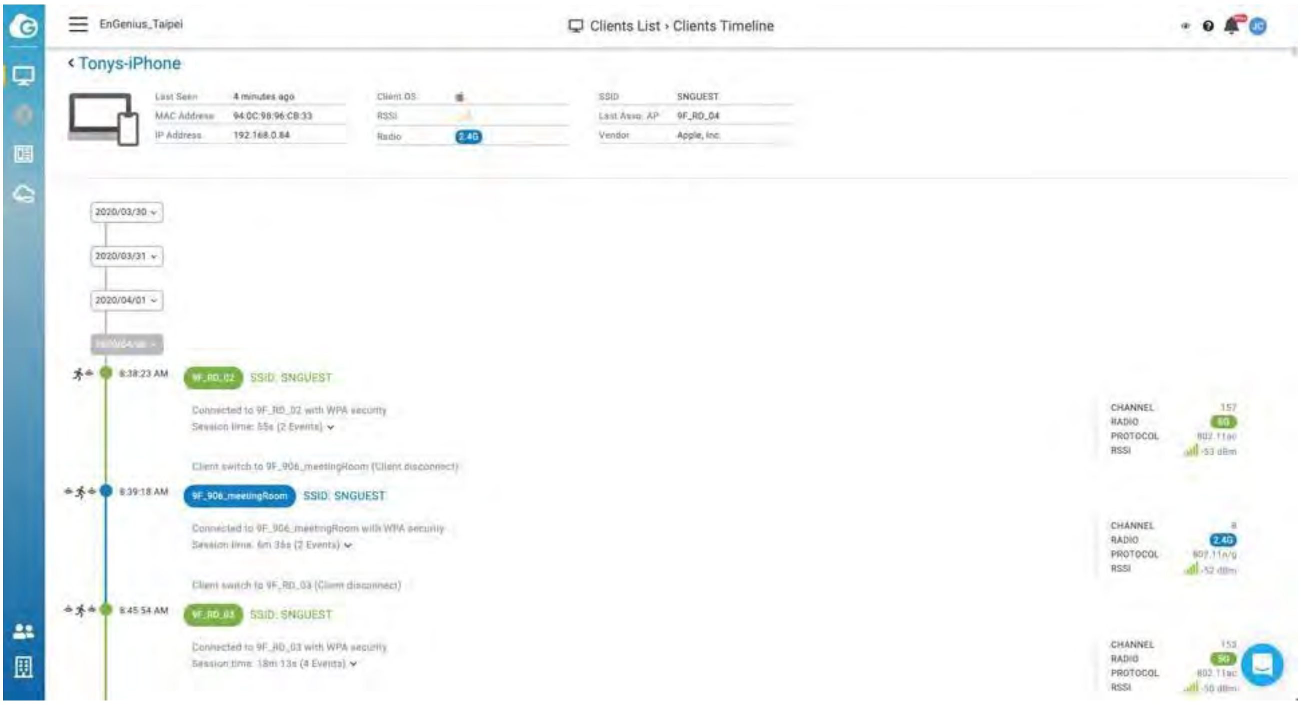
Client was roaming and connecting to another AP.

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.



‹ Tonys-iPhone

Last Seen 4 minutes ago
MAC Address 94:0C:98:96:CB:33
IP Address 192.168.0.84
Client OS
RSSI
Radio 2.4G
SSID SNGUEST
Last Asso. AP 9F_RD_04
Vendor Apple, Inc.

2020/03/30
2020/03/31
2020/04/01

8:38:23 AM 9F_RD_02 SSID: SNGUEST
Connected to 9F_RD_02 with WPA security
Session time: 55s (2 Events)
CHANNEL 157
RADIO 5G
PROTOCOL 802.11ac
RSSI -53 dBm

Client switch to 9F_906_meetingRoom (Client disconnect)

8:39:18 AM 9F_906_meetingRoom SSID: SNGUEST
Connected to 9F_906_meetingRoom with WPA security
Session time: 6m 36s (2 Events)
CHANNEL 8
RADIO 2.4G
PROTOCOL 802.11n/g
RSSI -52 dBm

Client switch to 9F_RD_03 (Client disconnect)

8:45:54 AM 9F_RD_03 SSID: SNGUEST
Connected to 9F_RD_03 with WPA security
Session time: 18m 13s (4 Events)
CHANNEL 153
RADIO 5G
PROTOCOL 802.11ac
RSSI -50 dBm

Radio Color Conventions

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

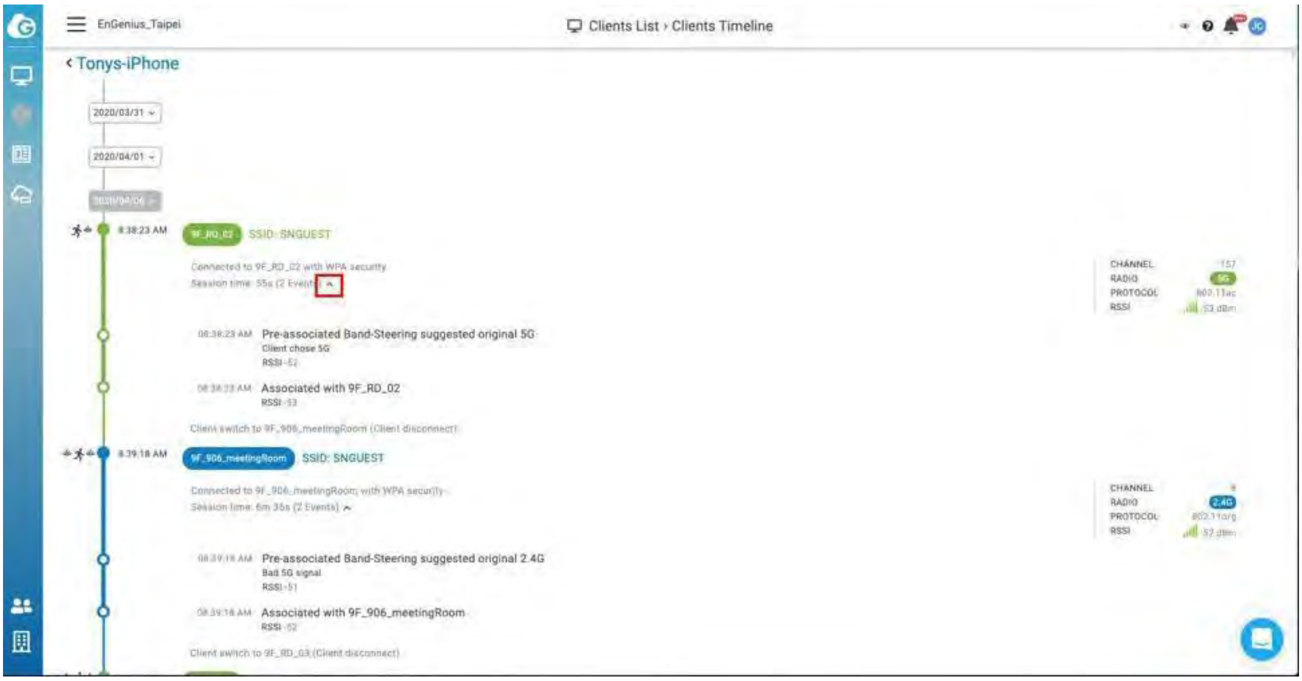
- Green: represent a 5G session.
- Blue: represent a 2.4G session.

> ⓘ 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:



8:38:23 AM 9F_RD_02 SSID: SNGUEST

Connected to 9F_RD_02 with WPA security
Session time: 55s (2 Events)

CHANNEL	157
RADIO	5G
PROTOCOL	802.11ac
RSSI	53 dBm

08:38:23 AM Pre-associated Band-Steering suggested original 5G
Client chose 5G
RSSI -52

08:38:23 AM Associated with 9F_RD_02
RSSI -53

Client switch to 9F_906_meetingRoom (Client disconnect)

8:39:18 AM 9F_906_meetingRoom SSID: SNGUEST

Connected to 9F_906_meetingRoom with WPA security
Session time: 6m 35s (2 Events)

CHANNEL	6
RADIO	2.4G
PROTOCOL	802.11b/g
RSSI	52 dBm

08:39:18 AM Pre-associated Band-Steering suggested original 2.4G
Bad 5G signal
RSSI -51

08:39:18 AM Associated with 9F_906_meetingRoom
RSSI -52

Client switch to 9F_RD_03 (Client disconnect)

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.

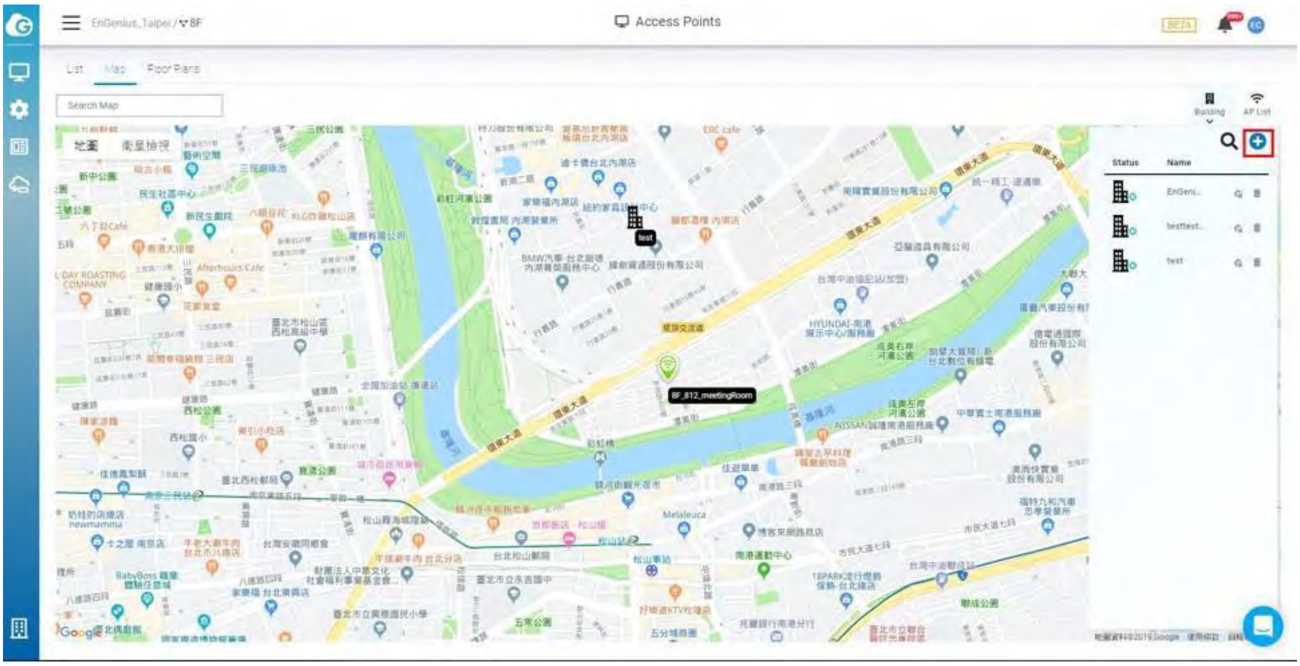
Disconnected by {device_name}	The client was disconnected by the AP due to bad RSSI signal (fast handover).
AP disconnect	The client was disconnected by the AP due to unknown reason.
Kicked by Cloud	The client was kicked by the cloud administrator.
Denied by ACL	The connection was refused by AP because 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

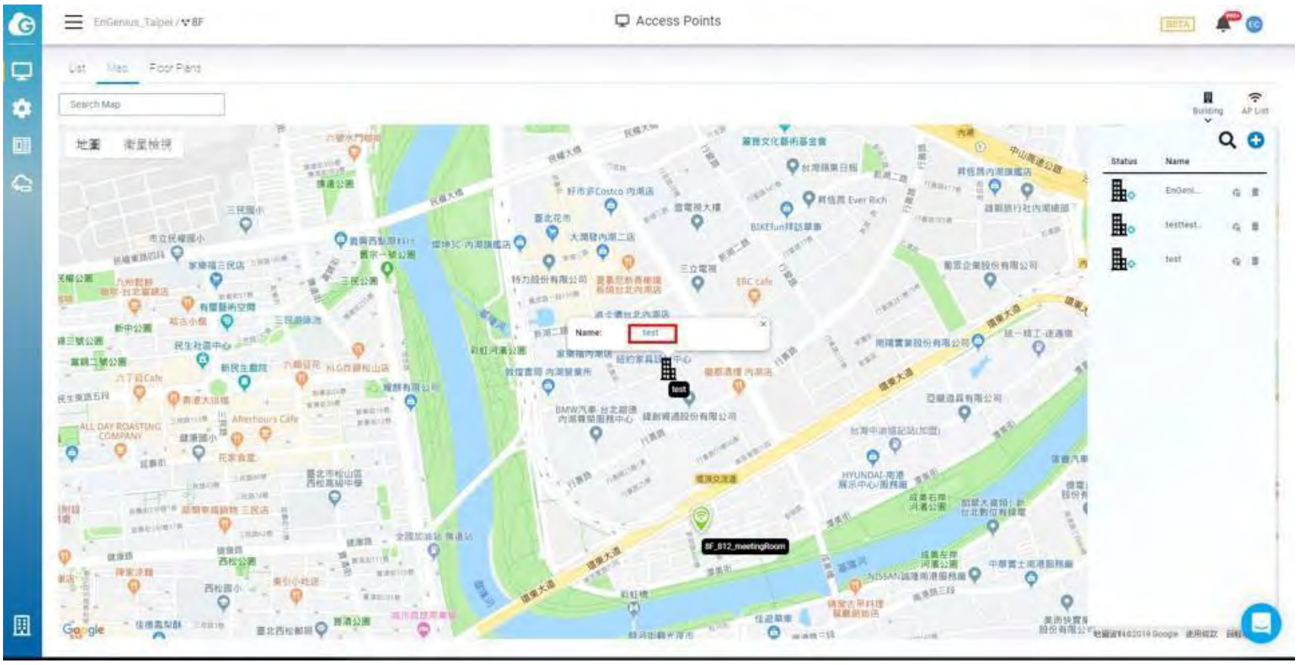
This screen allows you to locate a device on the world map to show the relationship between the space and EnGenius Devices. Maps provide a visualization for buildings and access points.

Create Buildings

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

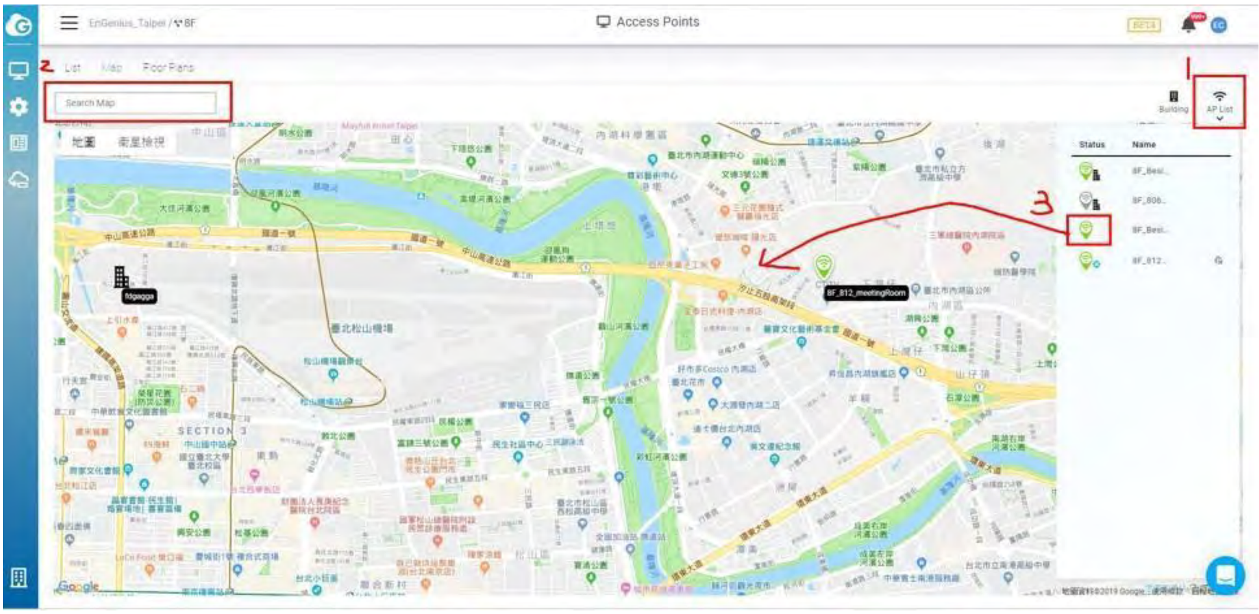


After you create a building, you can drag it to the map. Single-click on the building icon and a hyperlink will appear to allow you to edit floor plans.



How to Place Access Points or Buildings on the Map

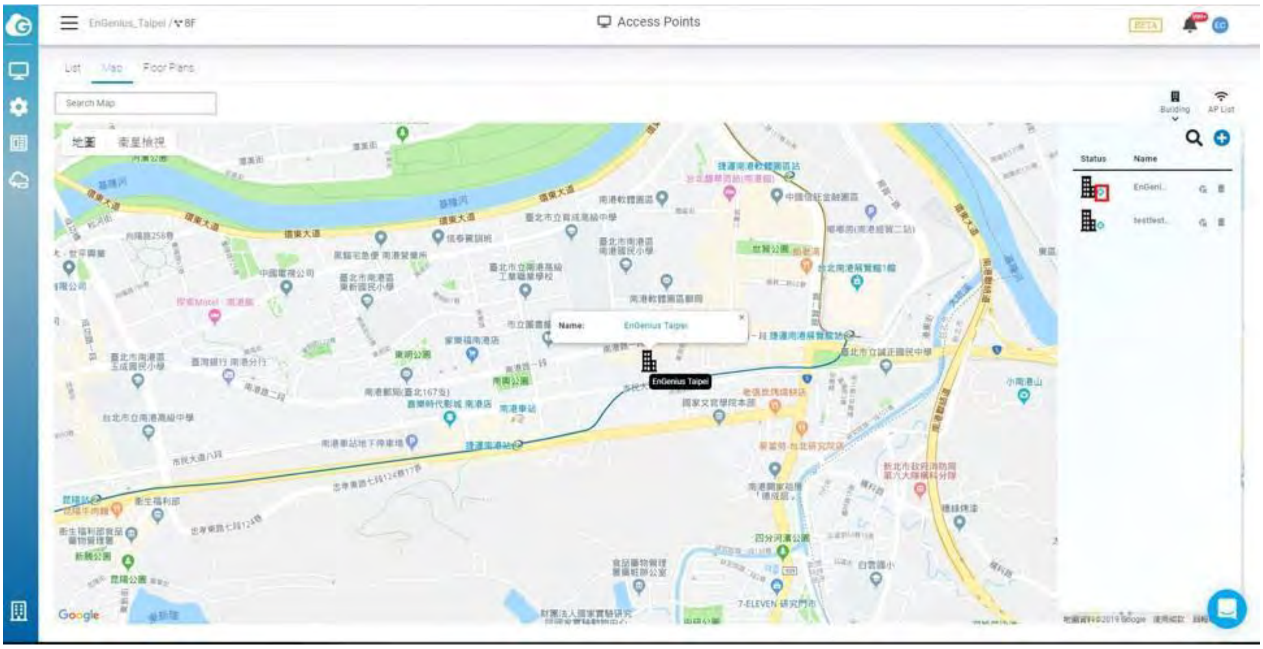
1. Click access point list or buildings list.
2. Enter the street address in the address field.
3. Drag the access point/building onto the map.

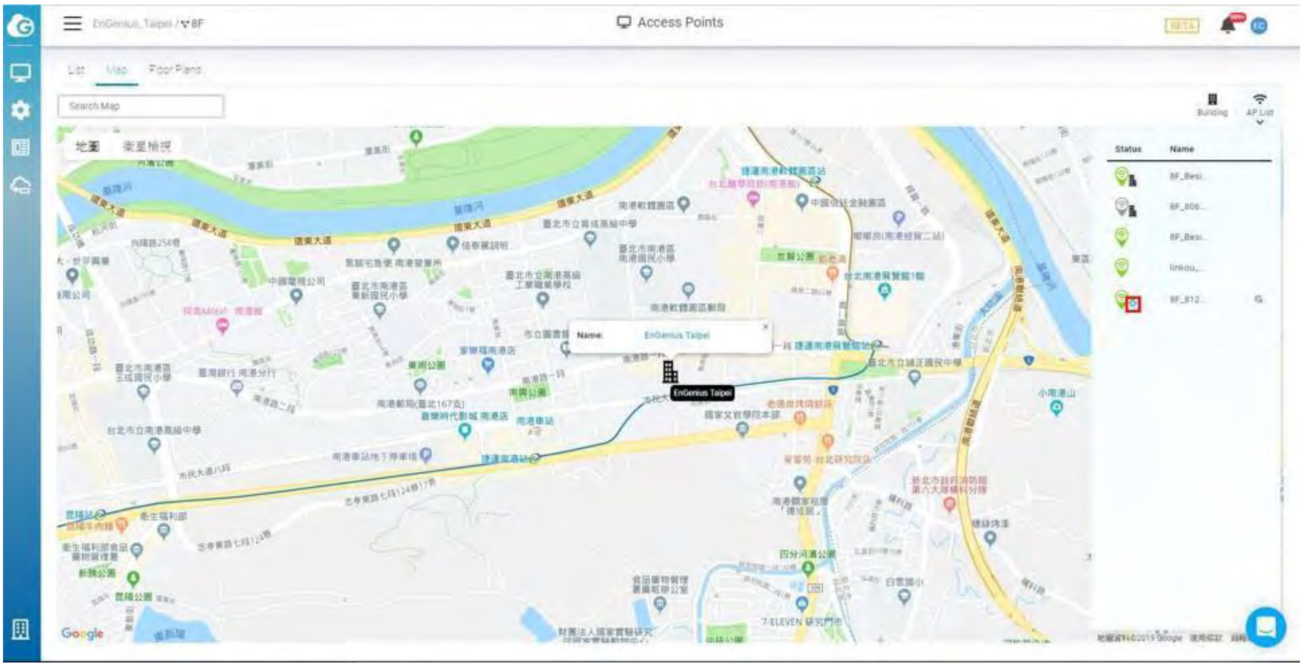


Navigation

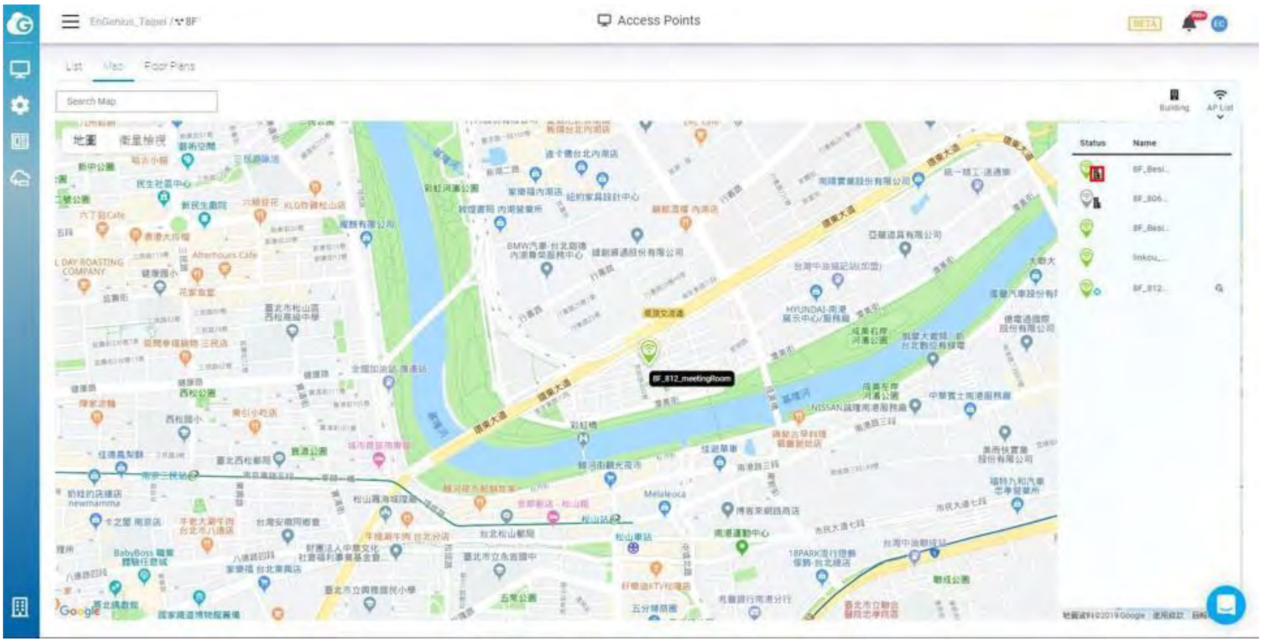
There are a number of ways to navigate through the map display.

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

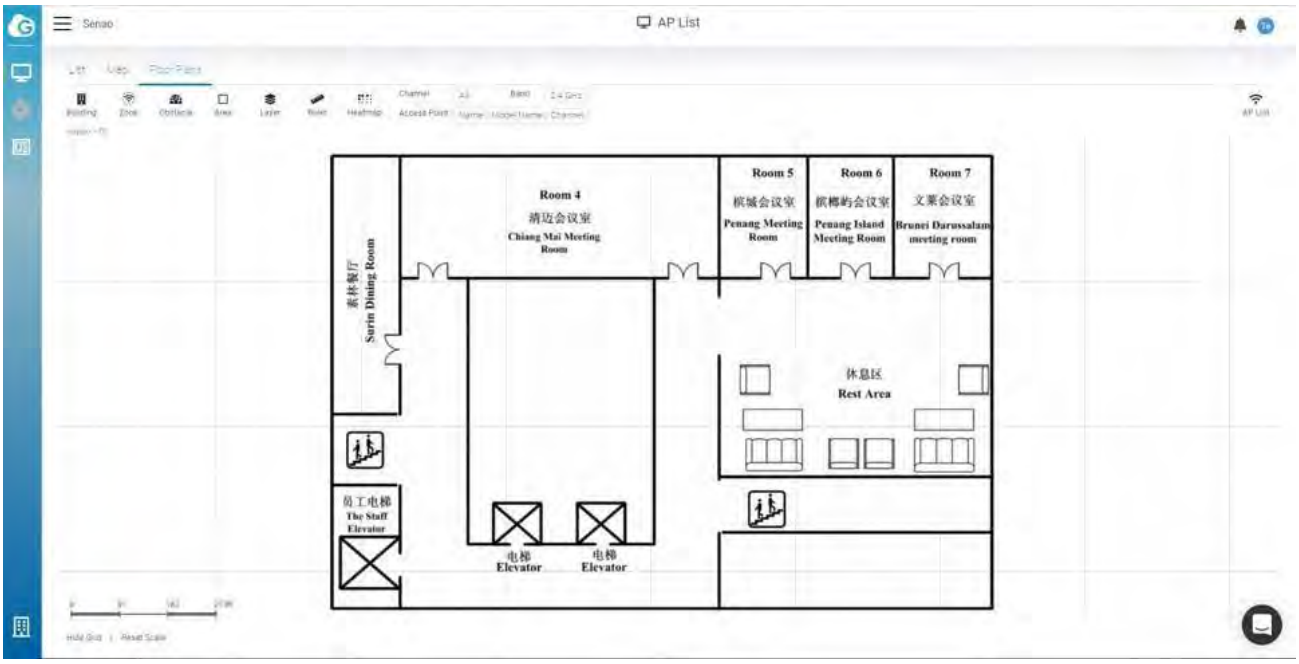
Floor plans allow you to simulate the heatmap. This article will discuss how to upload custom floor plans, pin them on the map, and place devices within these floor plans.

Uploading Floor Plans

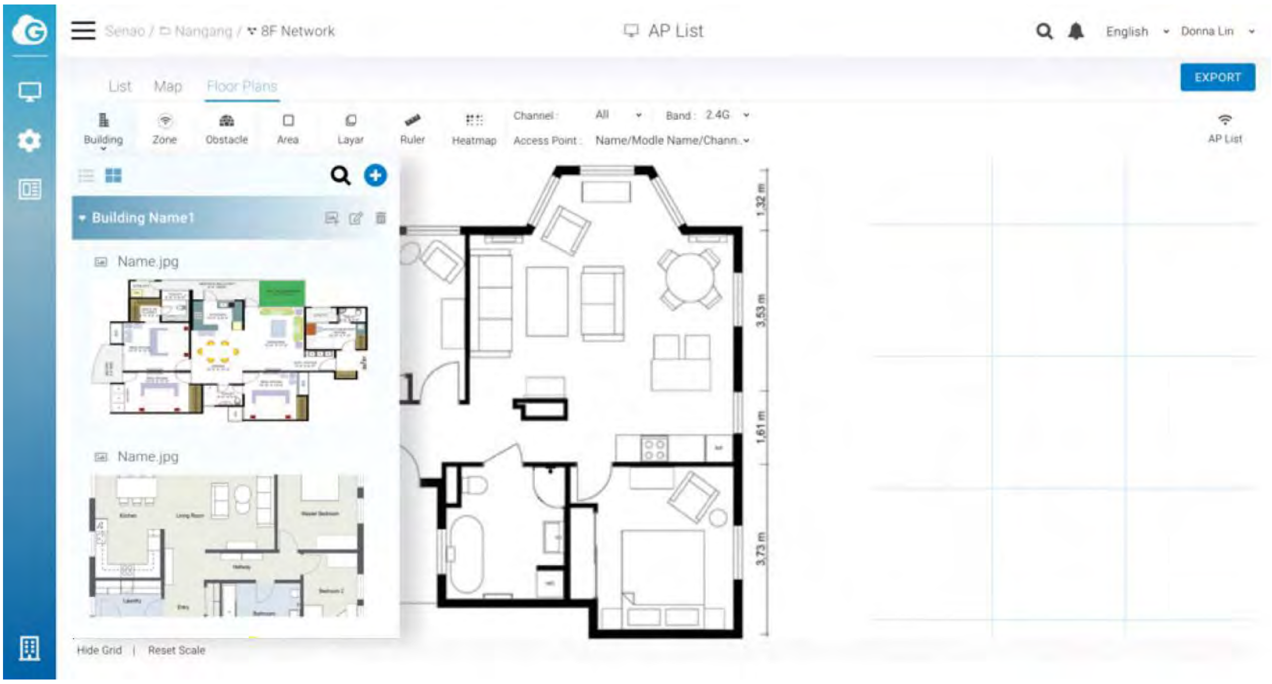
Before uploading floor plans, a building must be created to contain them (see Managing Devices > Device Map Location in the user manual).

To upload a custom floor plan/map:

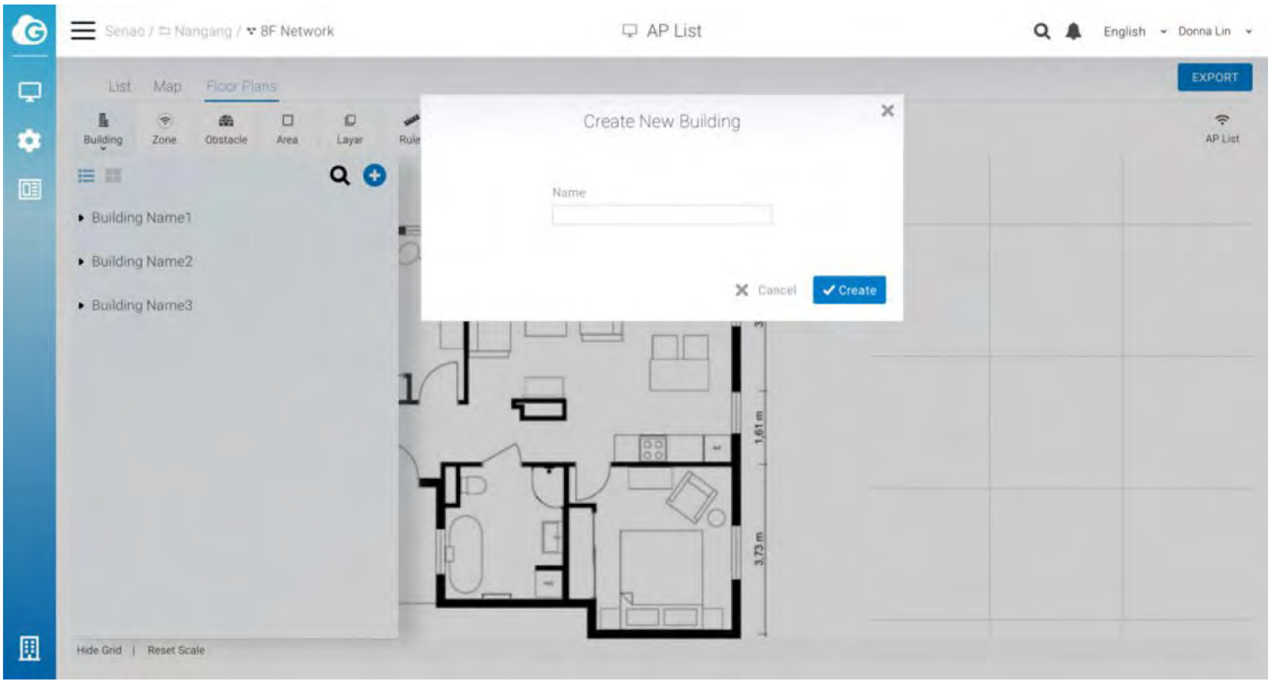
1. Navigate to Manage > Map & Floor plans.



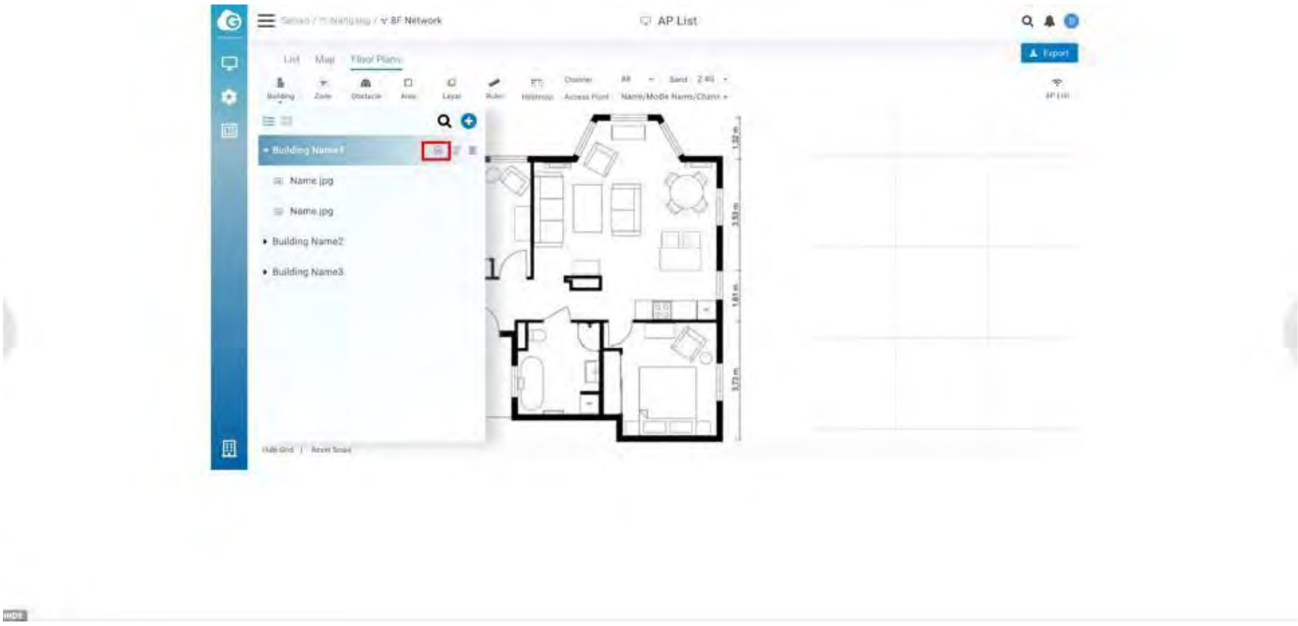
2. Click Building and click Add.



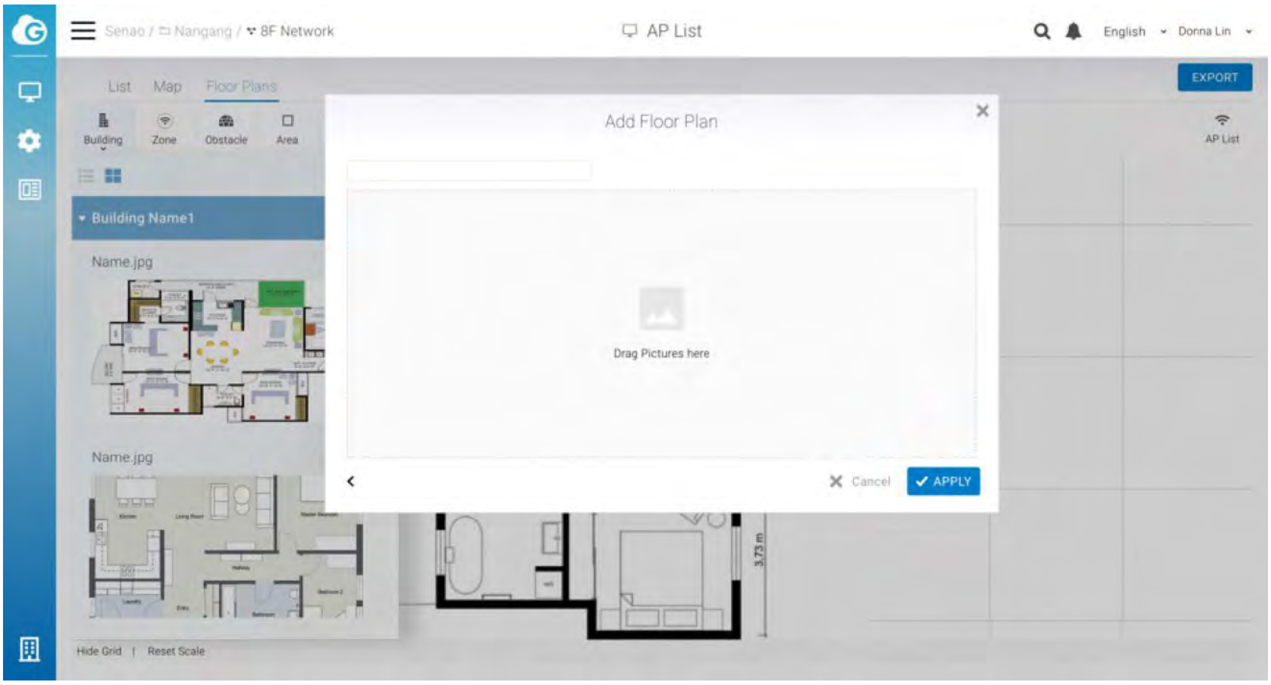
3. Enter a name and then click Create.



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.

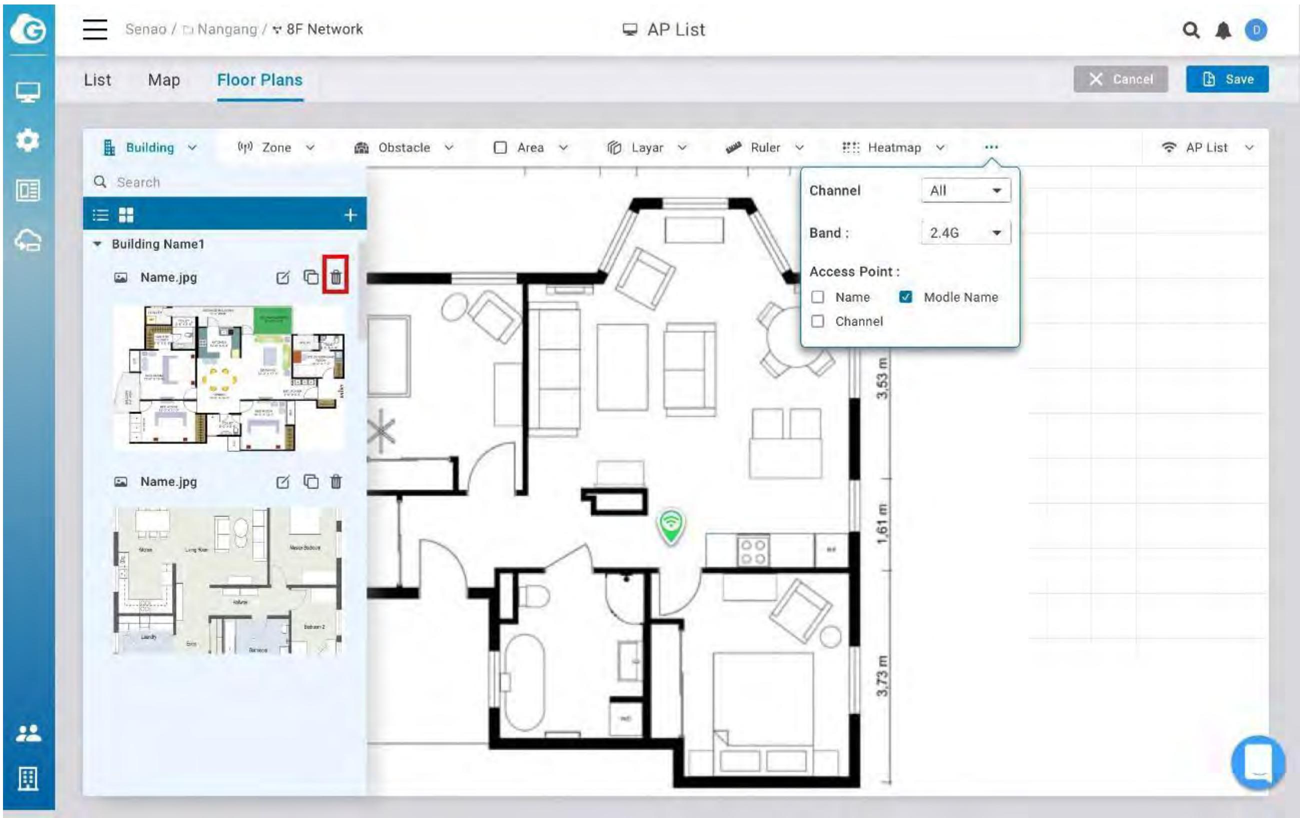


Deleting a Floor Plan

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.

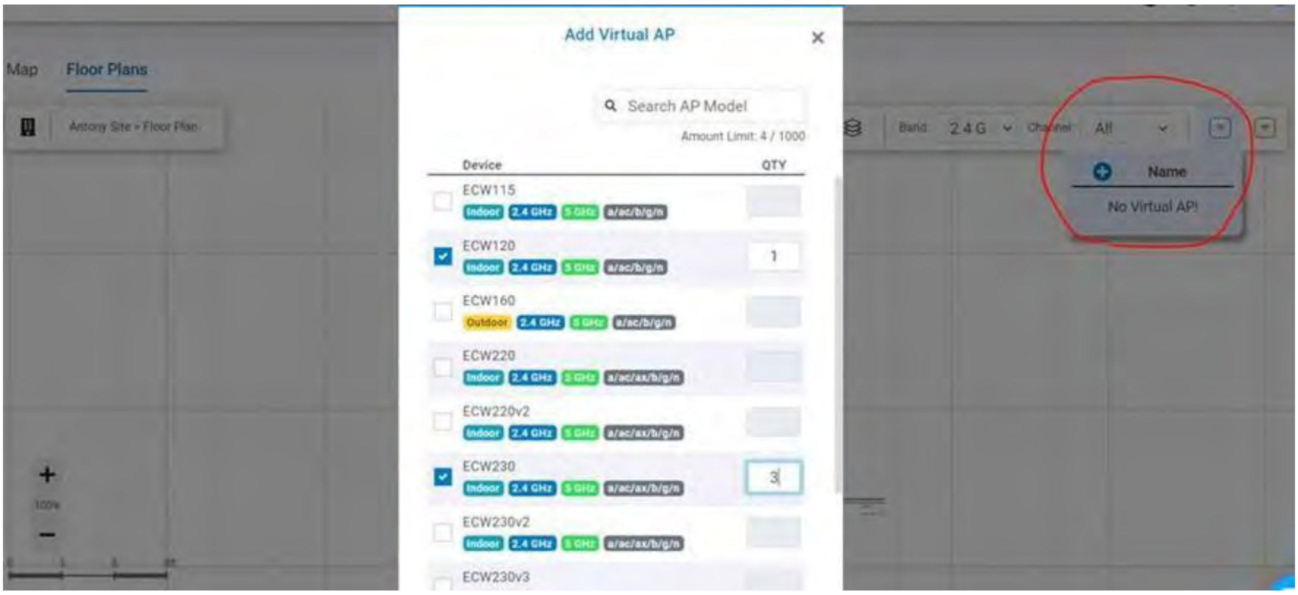


Channel: All
Band : 2.4G
Access Point :
□ Name ☑ Modle Name
□ Channel

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



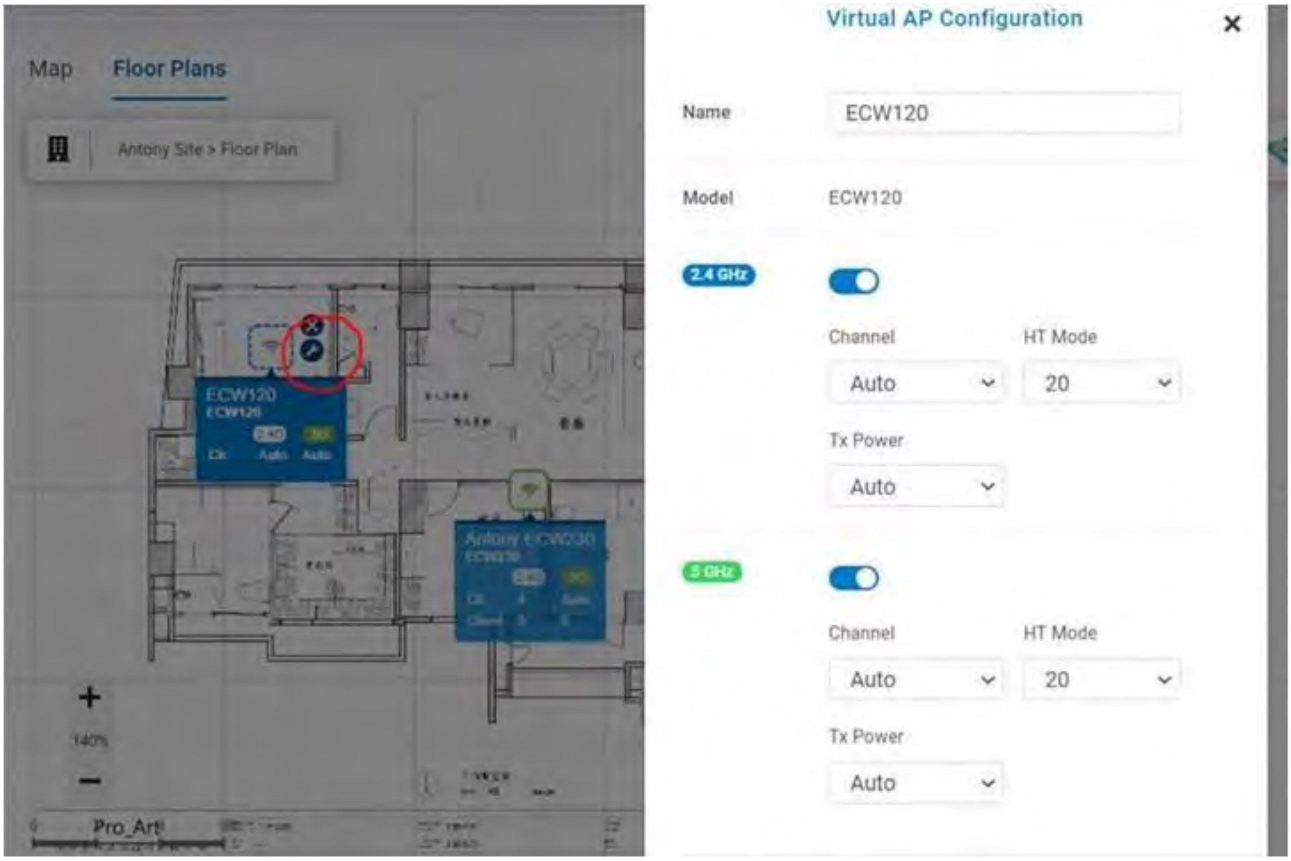
Add Virtual AP

Search AP Model

Amount Limit: 4 / 1000

	Device	QTY
□	ECW115 Indoor 2.4 GHz 5 GHz a/ac/b/g/n	
☑	ECW120 Indoor 2.4 GHz 5 GHz a/ac/b/g/n	1
□	ECW160 Outdoor 2.4 GHz 5 GHz a/ac/b/g/n	
□	ECW220 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
□	ECW220v2 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
☑	ECW230 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	3
□	ECW230v2 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
□	ECW230v3	

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



Virtual AP Configuration

Name: ECW120

Model: ECW120

2.4 GHz

Channel: Auto

HT Mode: 20

Tx Power: Auto

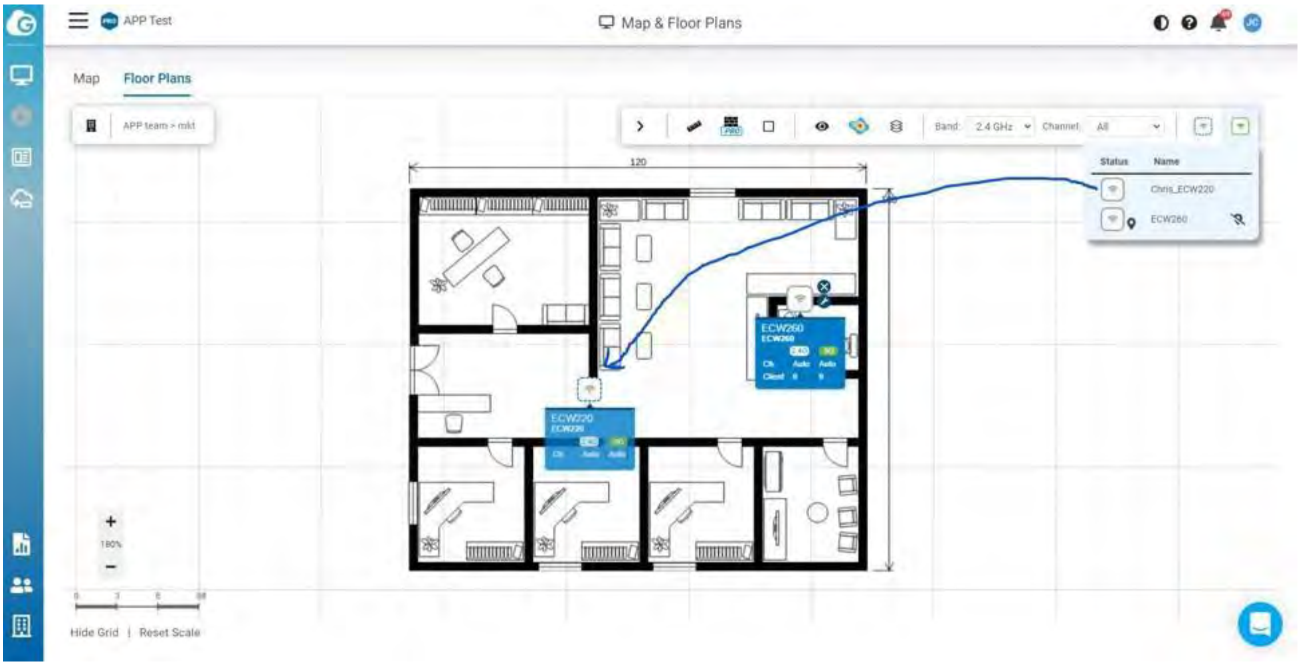
5 GHz

Channel: Auto

HT Mode: 20

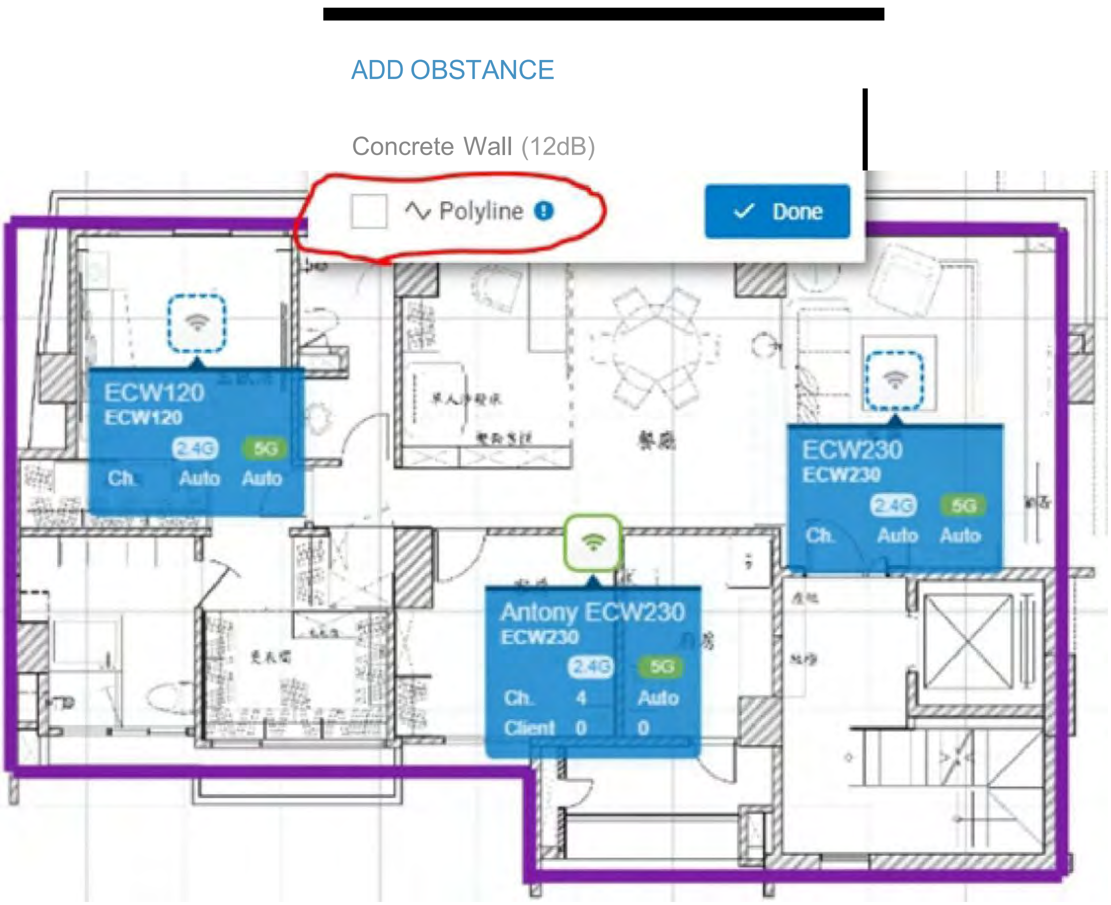
Tx Power: Auto

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.



ADD OBSTANCE

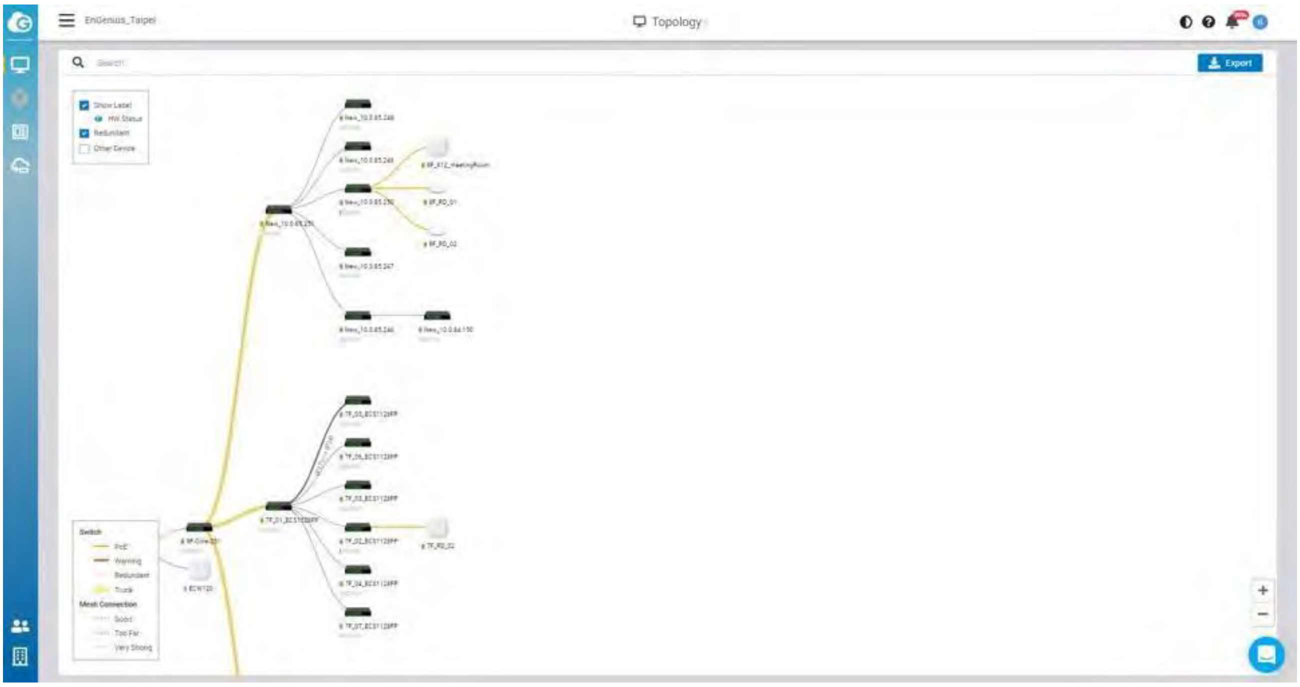
Concrete Wall (12dB)

□ Polyline

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.



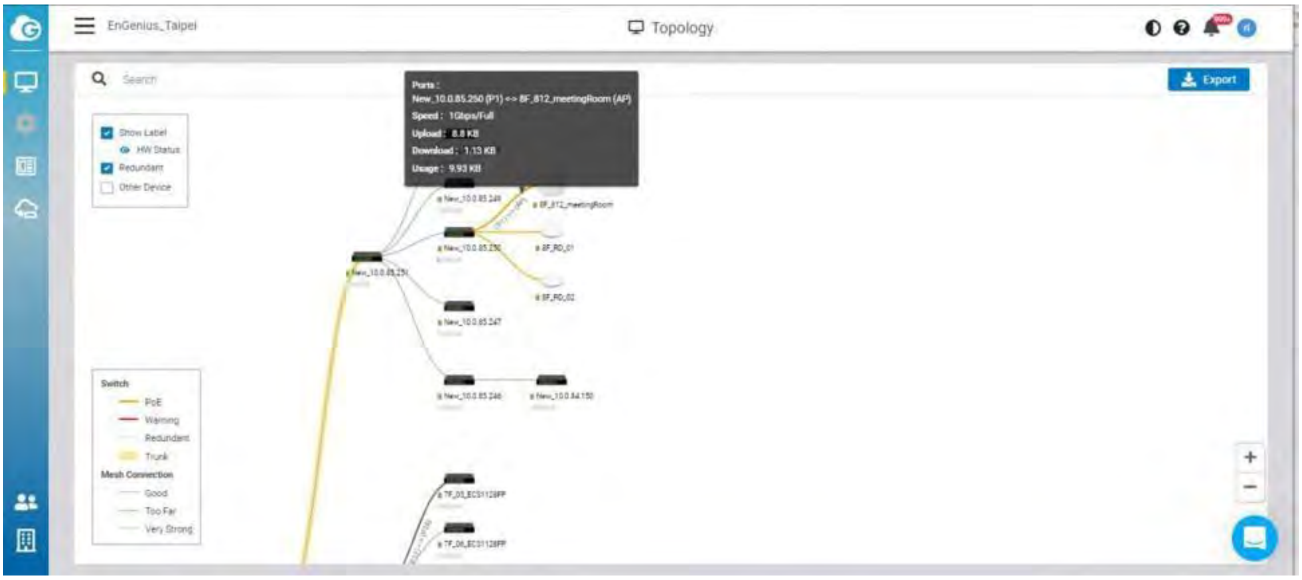
☑ Show Label

HW Status

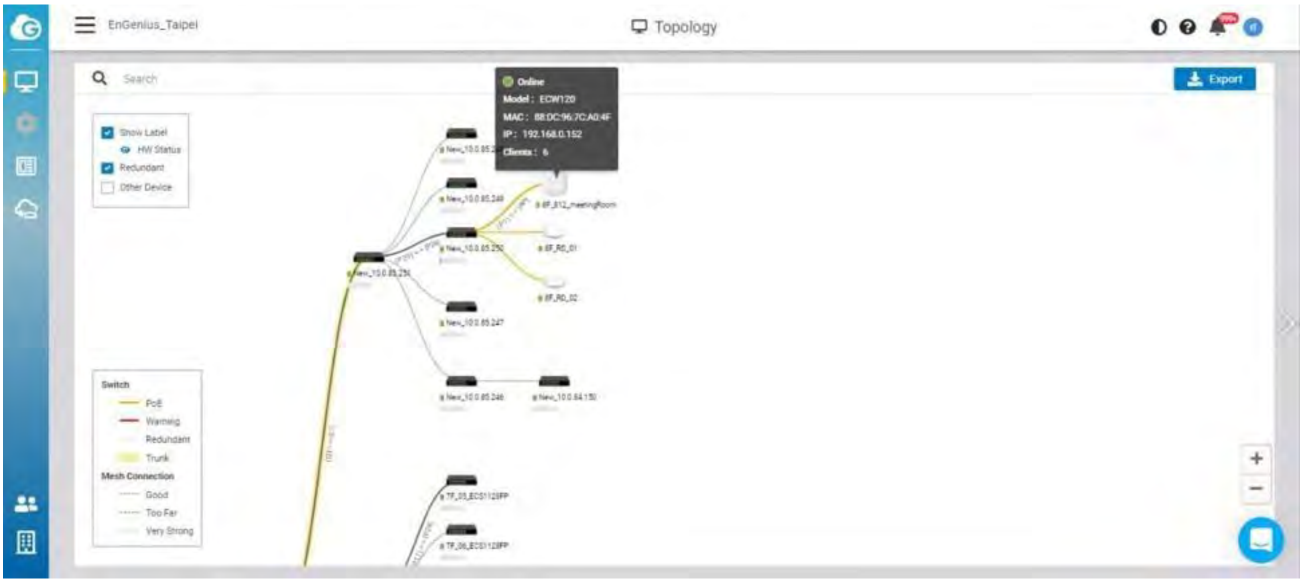
☑ Redundant

☐ Other Device

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.



Ports :
New_10.0.85.250 (P1) <-> 8F_812_meetingRoom (AP)
Speed : 1Gbps/Full
Upload : 8.8 KB
Download : 1.13 KB
Usage : 9.93 KB



Online
Model : ECW120
MAC : 88:DC:96:7C:A0:4F
IP : 192.168.0.152
Clients : 6

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

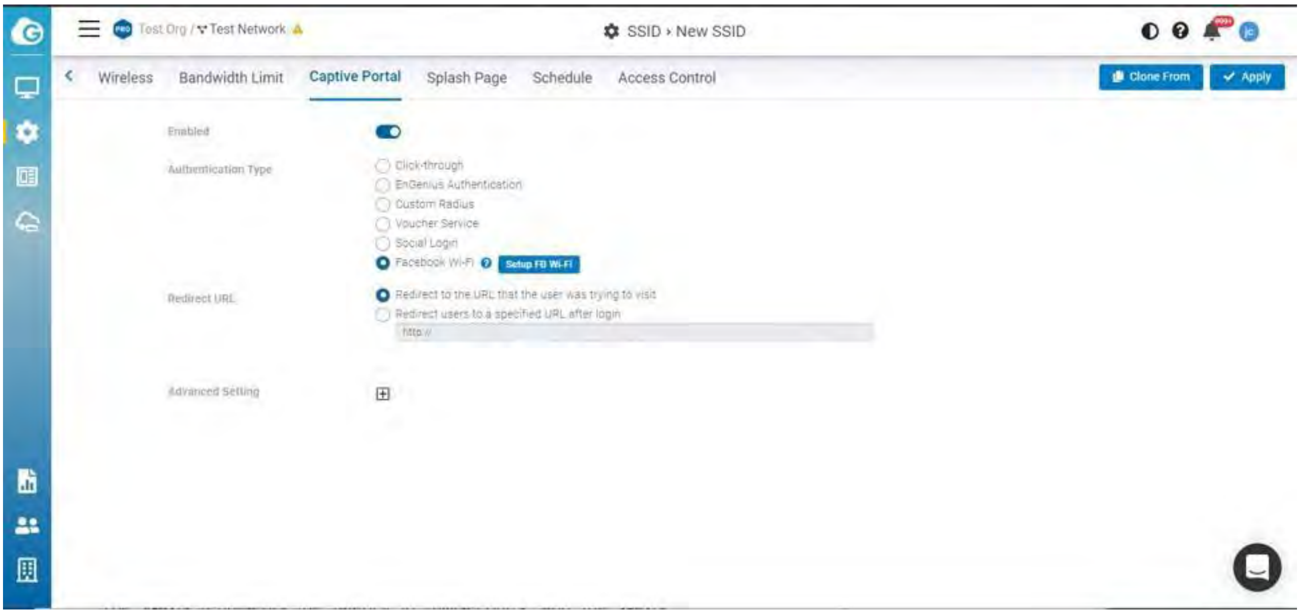
Facebook Wi-Fi

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:



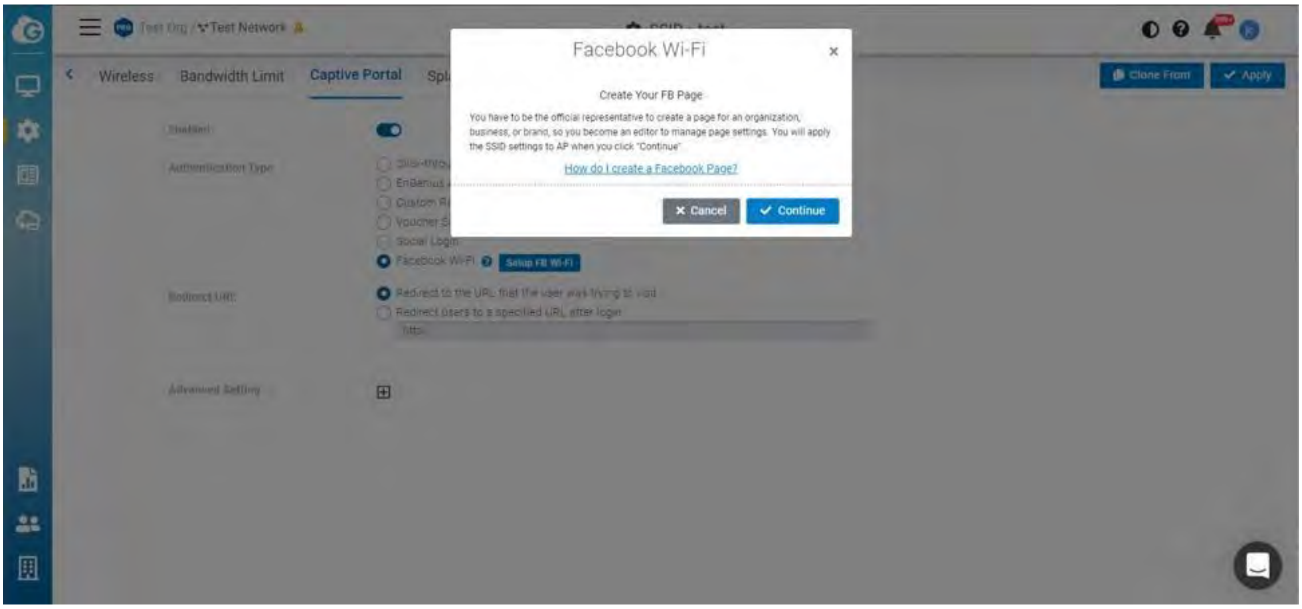
Enabled ●

Authentication Type
○ Click-through
○ EnGenius Authentication
○ Custom Radius
○ Voucher Service
○ Social Login
● Facebook Wi-Fi

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login
http://

Advanced Setting ⊞

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.



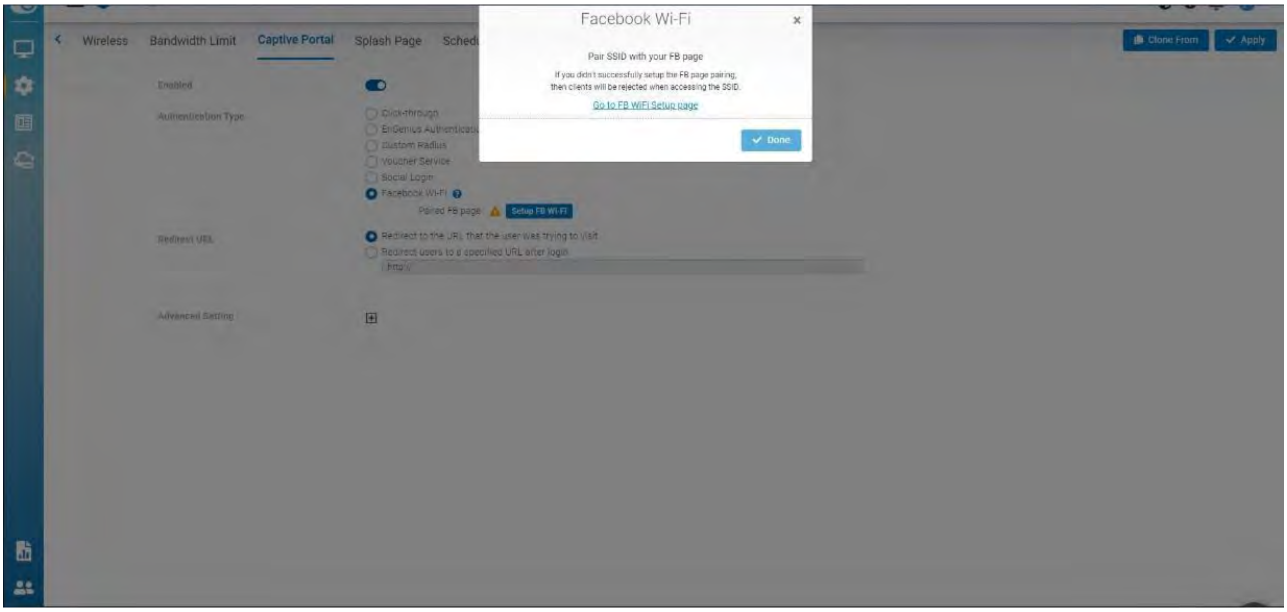
Facebook Wi-Fi

Create Your FB Page

You have to be the official representative to create a page for an organization, business, or brand, so you become an editor to manage page settings. You will apply the SSID settings to AP when you click "Continue"

How do I create a Facebook Page?

3. You will now see a link ‘Go to FB Wi-Fi Setup page’. Clicking on this link will take you to your Facebook Wi-Fi settings page.



Facebook Wi-Fi

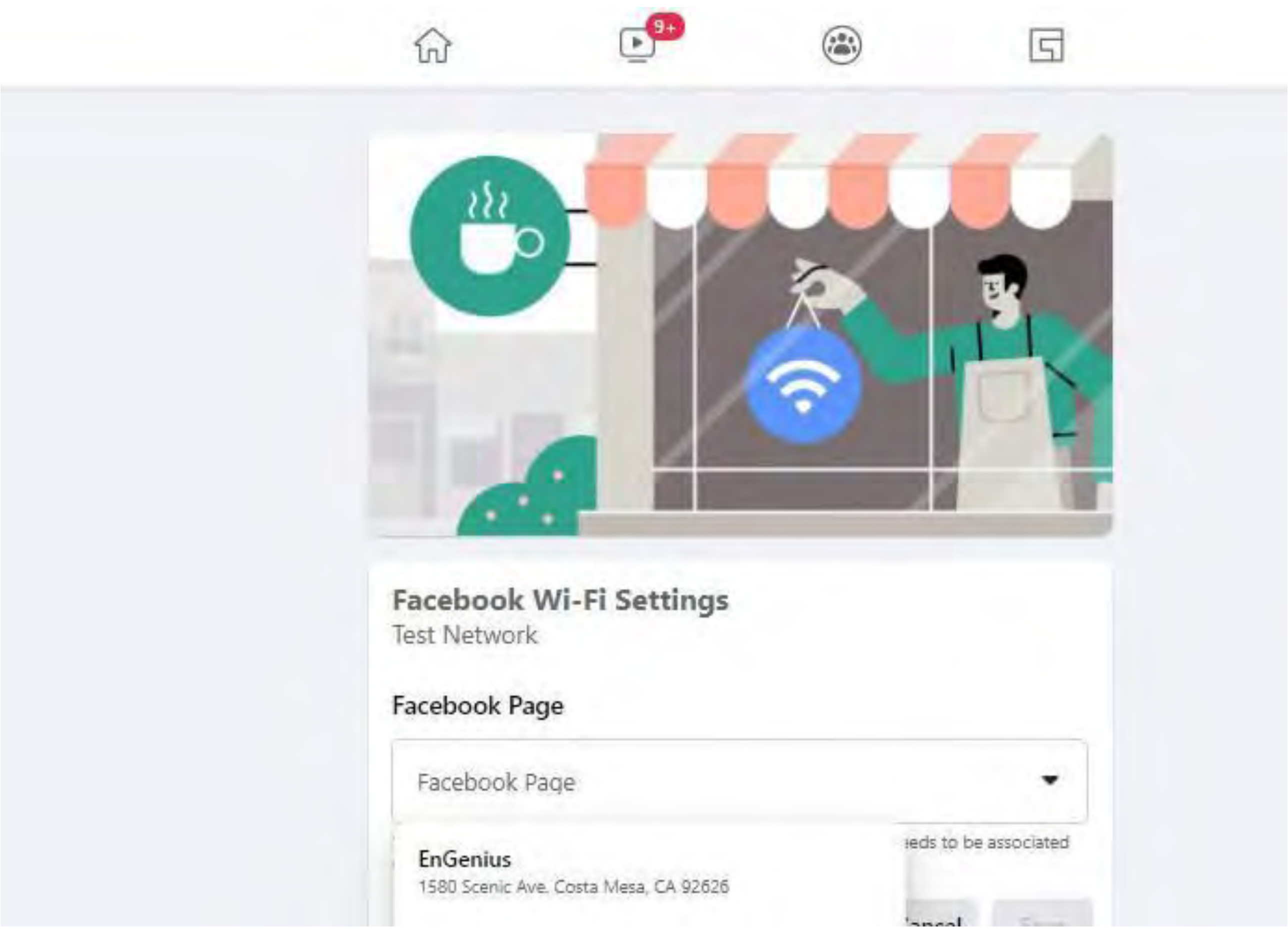
Pair SSID with your FB page

If you didn't successfully setup the FB page pairing, then clients will be rejected when accessing the SSID.

Go to FB WiFi Setup page

4.

If you are not logged into Facebook, you will be prompted to log into Facebook. Once you have logged in, you will see the following settings that will let you pair your SSID with your Facebook Page:



Facebook Wi-Fi Settings

Test Network

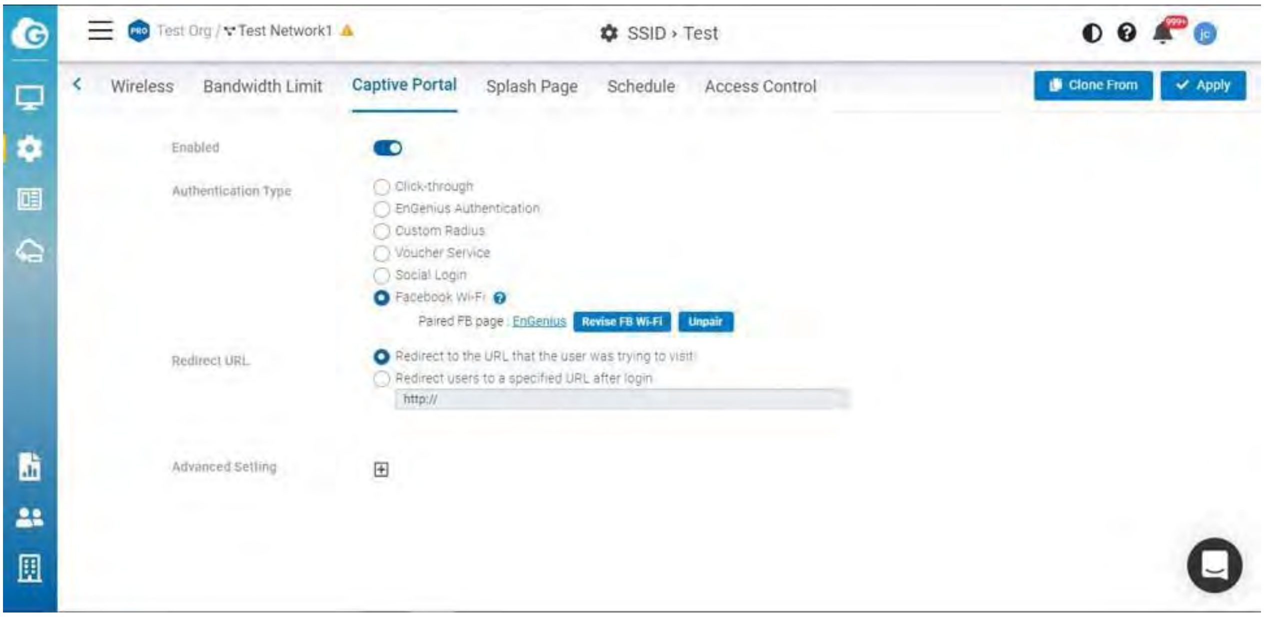
Facebook Page

Facebook Page ▾

EnGenius

1580 Scenic Ave. Costa Mesa, CA 92626

5. Once your Facebook page has been successfully paired with your SSID, the SSID page will update the Facebook Wi-Fi section with information about the paired page, along with an option to Unpair.



Enabled: ●

Authentication Type:
- ○ Click-through
- ○ EnGenius Authentication
- ○ Custom Radius
- ○ Voucher Service
- ○ Social Login
- ● Facebook Wi-Fi

Paired FB page : EnGenius Revise FB Wi-Fi Unpair

Redirect URL:
- ● Redirect to the URL that the user was trying to visit
- ○ Redirect users to a specified URL after login

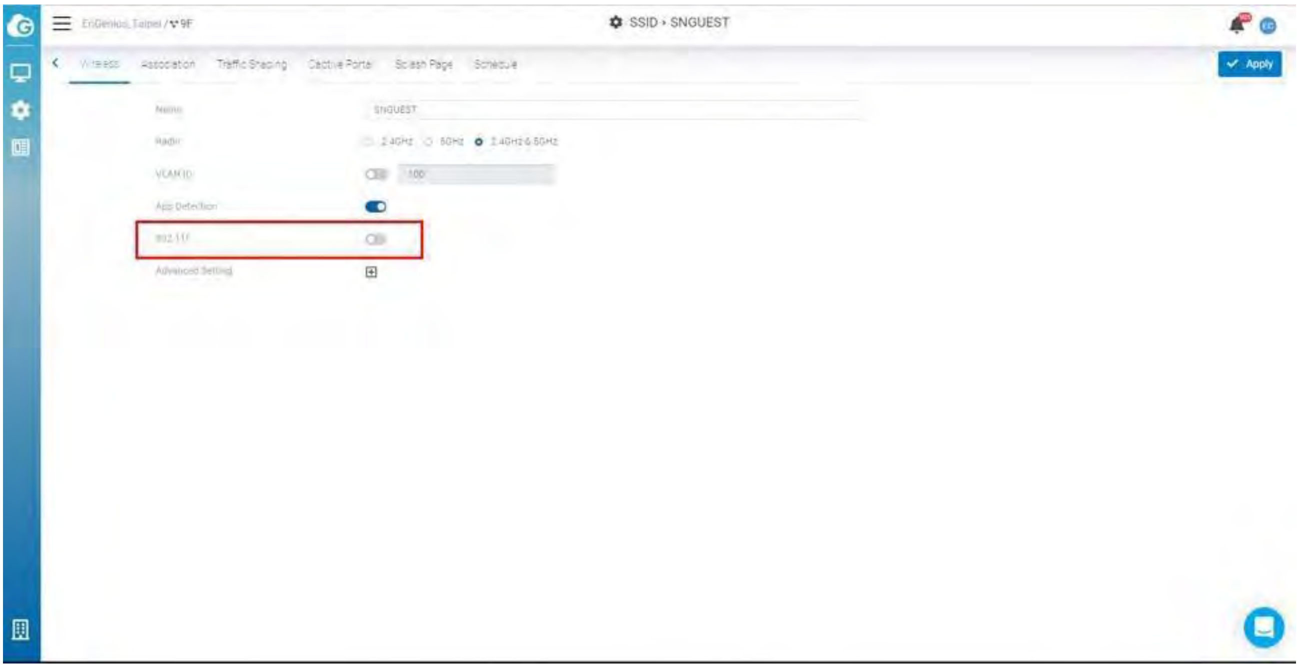
http://

Advanced Setting ⊞

802.11 Settings

802.11r

802.11r is a standards-based fast roaming technology that is leveraged when using a secure SSID (WPA2-PSK & WPA2-Enterprise). This option improves client device roaming by reducing the handoff delay in situations where client devices roam from one access point to another. 802.11r is disabled by default on EnGenius Cloud.



Name: SNGUEST

Radio: ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

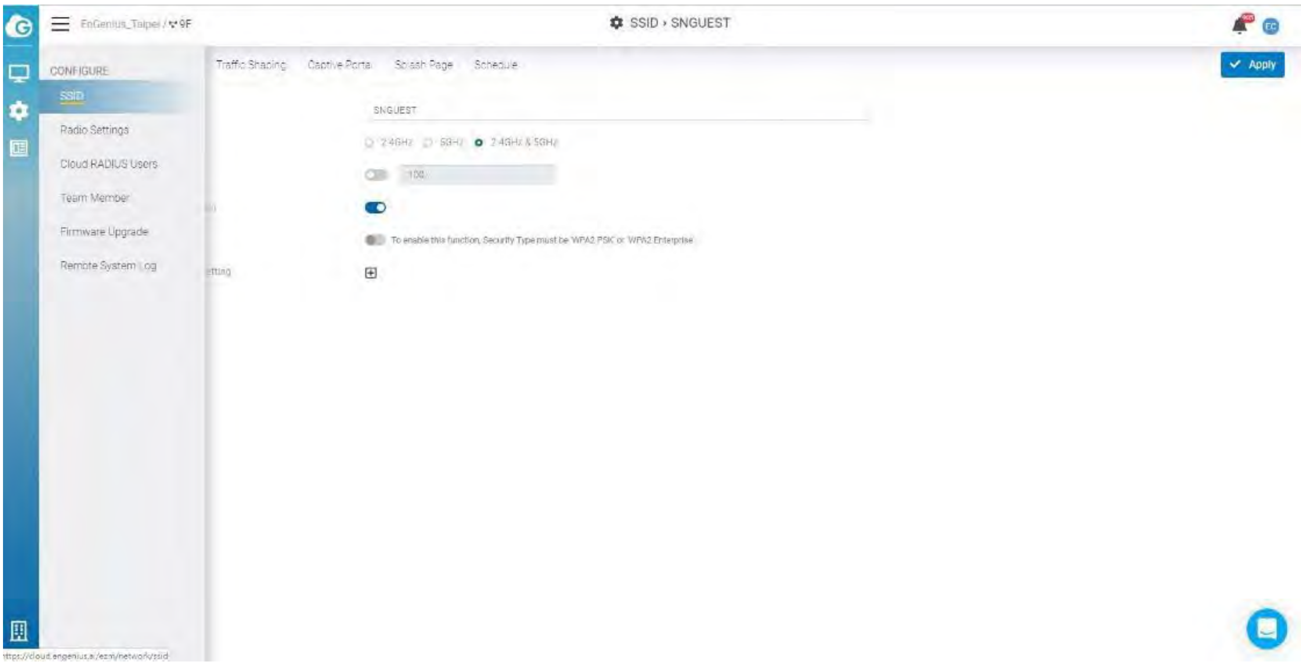
VLAN ID: 100

App Detection

802.11r

Advanced Setting ⊞

This feature can be enabled from the **Configure** > SSID page under Network Scope.



EnGenius_Taipei / 9F

SSID › SNGUEST

CONFIGURE

- SSID
- Radio Settings
- Cloud RADIUS Users
- Team Member
- Firmware Upgrade
- Remote System Log

Traffic Shaping · Captive Portal · Splash Page · Schedule

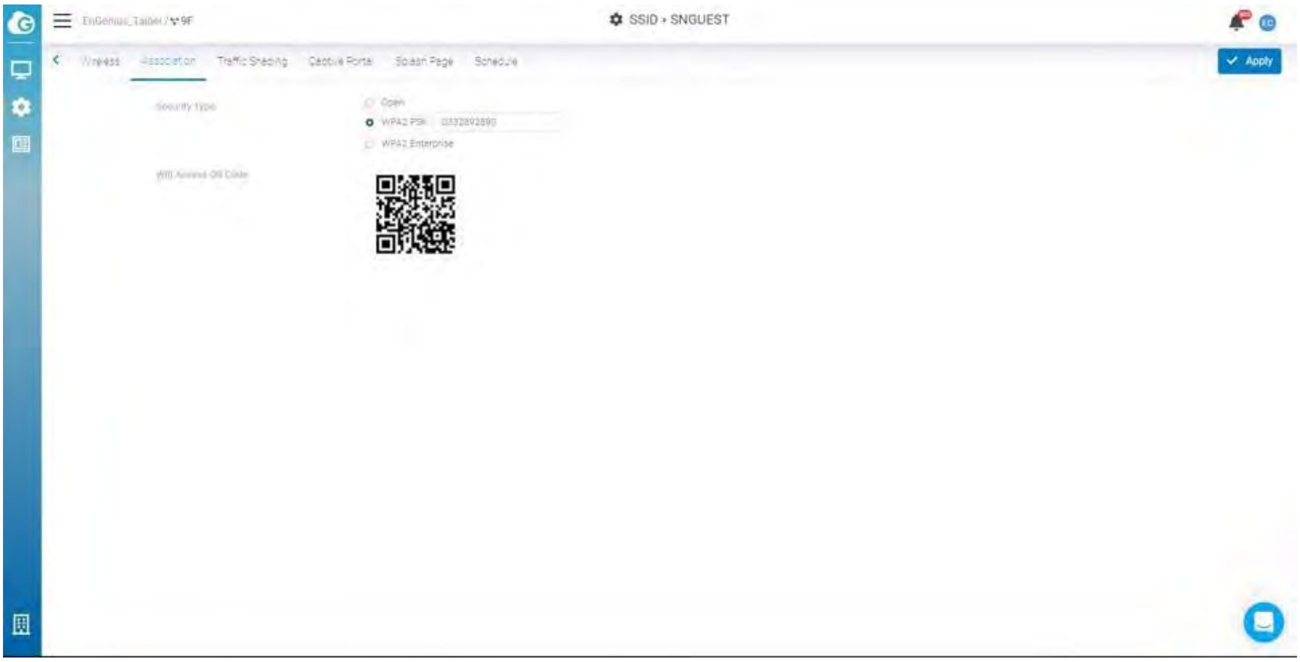
SNGUEST

○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

100

To enable this function, Security Type must be WPA2 PSK or WPA2 Enterprise

If this option cannot be enabled, please go to Wireless > Security Type to select WPA2 PSK or WPA2 Enterprise in advance.



EnGenius_Taipei / 9F

SSID › SNGUEST

Wireless · Association · Traffic Shaping · Captive Portal · Splash Page · Schedule

Security Type: ○ Open ● WPA2 PSK 0332892890 ○ WPA2 Enterprise

Wifi Access QR Code

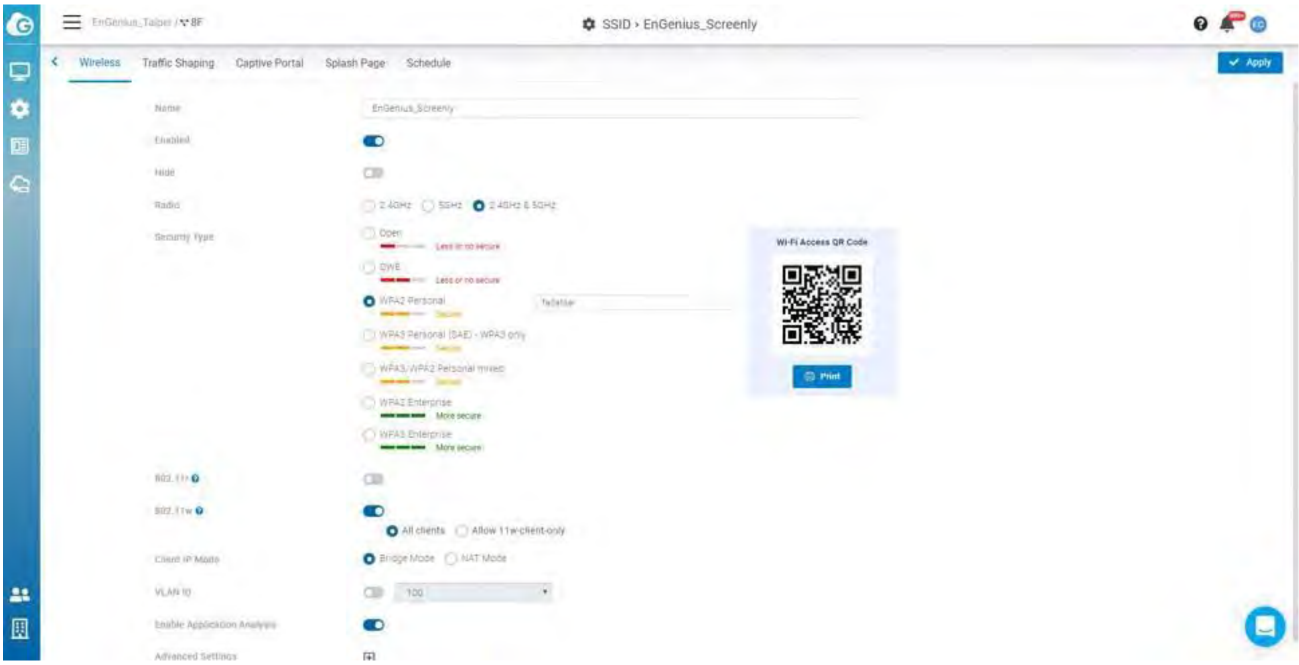
802.11w

802.11w is enabled when Security Type is not Open. 802.11w enables Protected Management Frames (PMF) for management frames such as authentication, deauthentication, association, disassociation, beacon, and probe traffic. This enables APs to help prevent rogue devices from spoofing management frames from APs. Enable 802.11r will allow APs to begin utilizing Protected Management Frames for any clients that support 802.11w.

Configuring Security

Security Type

Click **Configure** > SSID > Click one of SSID > Wireless to access this screen.



Name: EnGenius_Screenly

Enabled: on

Hide: off

Radio: ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

Security Type:
○ Open – Less or no secure
○ OWE – Less or no secure
● WPA2 Personal – Secure – Tafattar
○ WPA3 Personal (SAE) - WPA3 only – Secure
○ WPA3/WPA2 Personal mixed – Secure
○ WPA2 Enterprise – More secure
○ WPA3 Enterprise – More secure

802.11r: off

802.11w: on
● All clients ○ Allow 11w-client-only

Client IP Mode: ● Bridge Mode ○ NAT Mode

VLAN ID: off – 100

Enable Application Analysis: on

Advanced Settings ⊞

The following describes the authentication types on this screen:

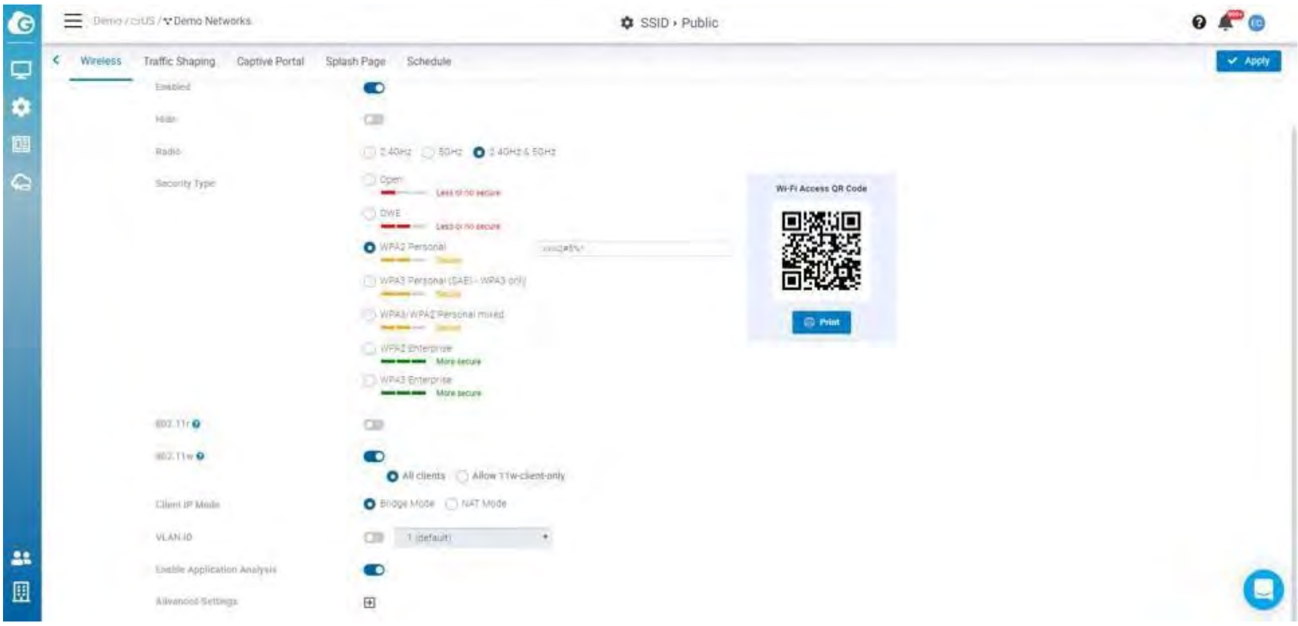
- Open: Allows any client to associate with this network without any data encryption or authentication.
- WPA2 PSK: Enter a pre-shared key of 8-64 case-sensitive characters to enable WPA2-PSK data encryption.
- WPA2 Enterprise: Select Custom Radius to use an external Radius server or select the EnGenius Cloud Radius to use the EnGenius Cloud for 802.1X authentication.
- OWE: When using hotspots in public, users are given better protection through the Wi-Fi Enhanced Open that provides unauthenticated encryption.
- WPA3 Personal (SAE) - WPA3 only: This type features easier password selection for users to easily remember. It also feats a higher level of security wherein data stored and data traffic in the network will not be compromised even if the password was hacked and data was already transmitted. The upgrade also enabled the Simultaneous

Authentication of Equals (SAE) which replaced the Pre-shared Keys (PSK) in WPA2-Personal.

- WPA3/WPA2 Personal mixed: WPA2/WPA3 mixed mode allows for the coexistence of WPA2 and WPA3 clients on a common SSID. The passphrase for both WPA2 and WPA3 clients remains the same, the AP just advertises the different encryption cyphers available to be selected for use by the client. Clients choose which cypher to use for the wireless connection.
- WPA3 Enterprise: This type was mainly built for tighter and consistent application of security protocols across networks of governments, establishments, enterprises, and financial institutions. Offering optional 192-bit minimum security, the WPA3 will make cryptographic tools better. Hence, better protection for sensitive data.

WiFi Access QR code

This QR code allows you to use your mobile device to connect to the specific SSID.



Demo / ciUS / Demo Networks

SSID › Public

Wireless | Traffic Shaping | Captive Portal | Splash Page | Schedule

Enabled: on

Hide: off

Radio: ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

Security Type:
○ Open — Less or no secure
○ OWE — Less or no secure
● WPA2 Personal — Secure
○ WPA3 Personal (SAE) - WPA3 only — Secure
○ WPA3/WPA2 Personal mixed — Secure
○ WPA2 Enterprise — More secure
○ WPA3 Enterprise — More secure

802.11r: off

802.11w: on
● All clients ○ Allow 11w-client-only

Client IP Mode: ● Bridge Mode ○ NAT Mode

VLAN ID: off, 1 (default)

Enable Application Analysis: on

Advanced Settings: ⊞

Client IP Addressing

NAT Mode

In NAT mode, the EnGenius APs run as DHCP servers to assign IP addresses to wireless clients out of a private 172.x.x.x IP address pool behind a NAT.

NAT mode should be enabled when any of the following is true:

- Wireless clients associated to the SSID only require Internet access, not access to local wired or wireless resources.
- There is no DHCP server on the LAN that can assign IP addresses to the wireless clients.
- There is a DHCP server on the LAN, but it does not have enough IP addresses to assign to wireless clients

The implications of enabling NAT mode are as follows:

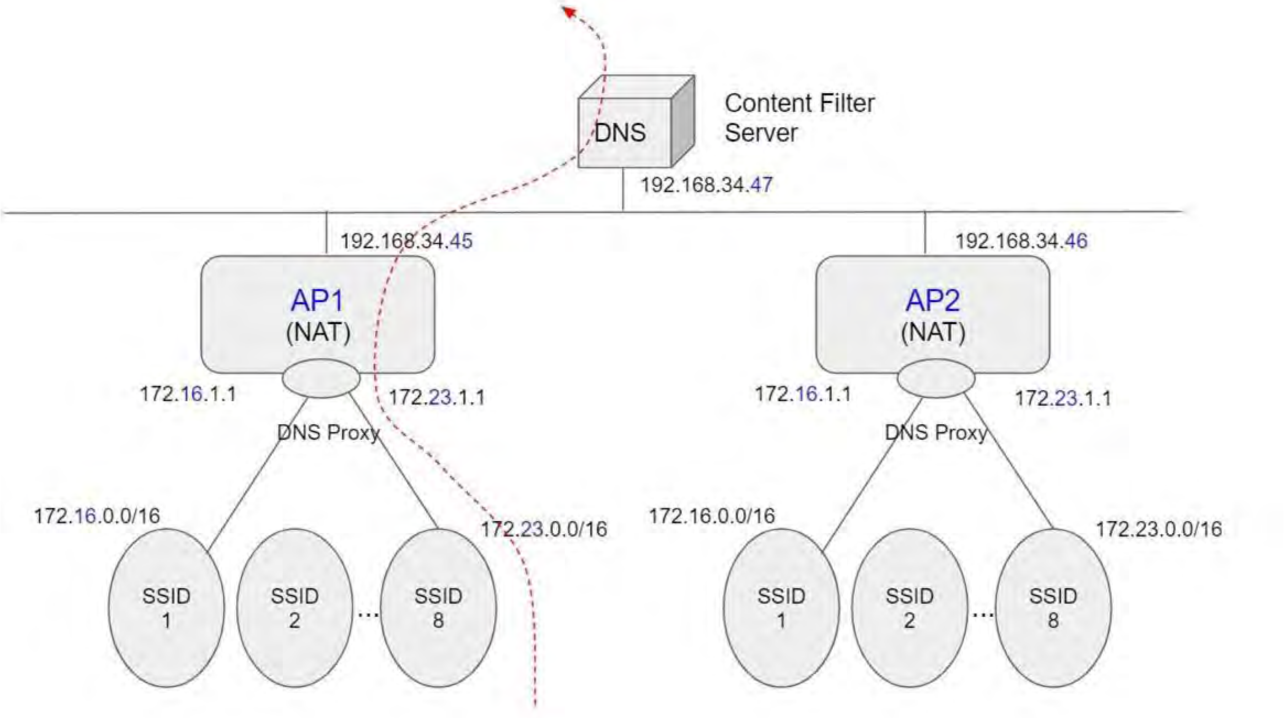
1. No NAT client can be talked to the other NAT client, neither same SSID nor different SSID (client isolation enabled and block internal routing)
2. Change the IP range of CP DNS to be same as AP DNS (172.16-23.0.0/16)

Use Cases

NAT mode works well for providing a wireless guest network since it puts clients on a private wireless network with automatic addressing.

Diagram

When an SSID is configured in NAT Mode, wireless clients will point to the access point as their DNS server. The AP then acts as a DNS proxy and will forward clients' DNS queries to its configured DNS server.



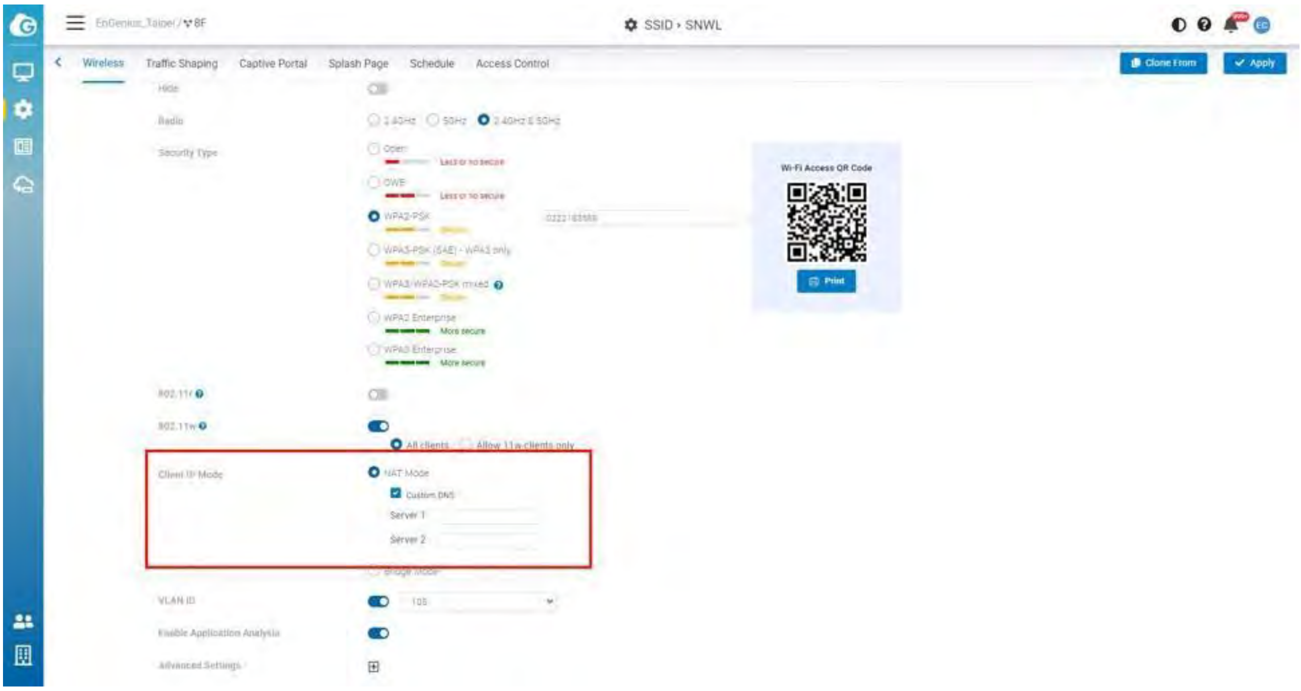
Configuring Custom DNS for an SSID in NAT Mode

This allows you to set custom DNS servers for a NAT SSID, instead of using the AP's DNS server. This is typically used to forward NAT SSID clients to a DNS server with custom content filtering.

Configuration

1. Navigate to **Configure** > SSID, then choose one SSID to customize the DNS settings.

2. Locate the Client IP mode and choose NAT mode then click Custom DNS.



Hide
Radio ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz
Security Type ○ Open Less or no secure
○ OWE Less or no secure
● WPA2-PSK Secure 0222183588
○ WPA3-PSK (SAE) - WPA3 only Secure
○ WPA3/WPA2-PSK mixed Secure
○ WPA2 Enterprise More secure
○ WPA3 Enterprise More secure
802.11r
802.11w ● All clients ○ Allow 11w-clients only
Client IP Mode ● NAT Mode
☑ Custom DNS
Server 1
Server 2
○ Bridge Mode
VLAN ID 105
Enable Application Analysis
Advanced Settings ⊞

3. Enter the preferred Custom DNS IP addresses.

4. Click Apply.

Bridge Mode

In bridge mode, the APs act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server.

Bridge mode should be enabled when the following is true:

- Wired and wireless clients in the network need to reach each other (e.g., a wireless laptop needs to discover the IP address of a network printer, or wired desktop needs to connect to a wireless surveillance camera).

The implications of enabling Bridge mode are as follows:

- Wired and wireless clients have IP addresses in the same subnet

User Cases

Bridge mode works well in most circumstances, particularly for Roaming. and is the simplest option to put wireless clients on the LAN.

Configuration

1. Navigate to **Configure** > SSID , then choose one SSID .

2. Locate the Client IP mode and choose Bridge mode then click Apply.

> ⓘ If you configure Bridge mode on two or more SSIDs in the same network , it means that these Clients have IP addresses in the same subnet.

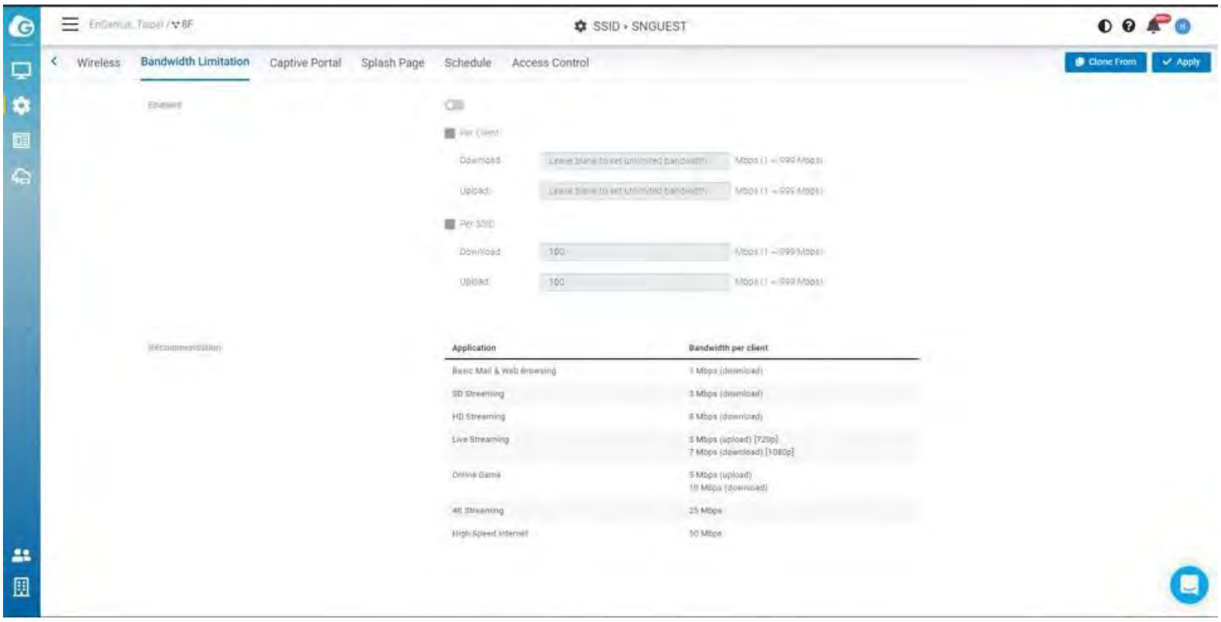
QoS

Bandwidth Limit

Bandwidth Limitation ensures that users do not consume more bandwidth than they should. We integrated bandwidth Limitation that enforces upload and download limits. Bandwidth Limitation can be applied per SSID or per user or both. When both SSID and Per Client bandwidth limit are set, that means when the total sum of client bandwidth is less than SSID bandwidth limit, per client can have a maximum of “per client bandwidth limit”. If the total sum is over the SSID limit, then all users will share the upper limit of SSID bandwidth.

Use this screen to configure maximum bandwidth.

Click **Configure** > SSID > Bandwidth Limit to access this screen.



Enabled

Per Client

Download: Leave blank to set unlimited bandwidth Mbps (1 ~ 999 Mbps)

Upload: Leave blank to set unlimited bandwidth Mbps (1 ~ 999 Mbps)

Per SSID

Download: 100 Mbps (1 ~ 999 Mbps)

Upload: 100 Mbps (1 ~ 999 Mbps)

Recommendation

Application	Bandwidth per client
Basic Mail & Web Browsing	1 Mbps (download)
SD Streaming	3 Mbps (download)
HD Streaming	8 Mbps (download)
Live Streaming	5 Mbps (upload) [720p] 7 Mbps (download) [1080p]
Online Game	5 Mbps (upload) 10 Mbps (download)
4K Streaming	25 Mbps
High-Speed Internet	50 Mbps

Download Limit

Set the maximum download stream limit for traffic from the SSID or Per user .

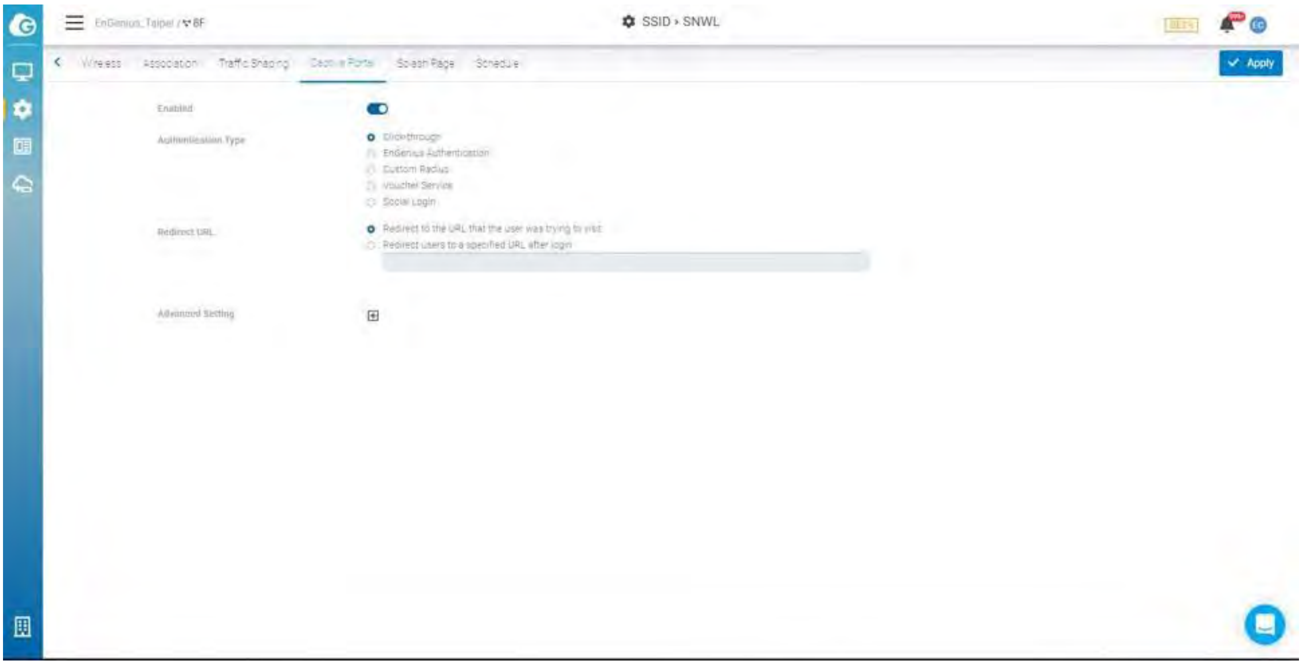
Upload Limit

Set the maximum upload stream limit for traffic from the SSID or Per user .

Captive Portal

A captive portal can intercept network traffic until a user authenticates his/her connection, usually through a specifically designated login page.

Click **Configure** > SSID > Captive Portal to access this screen.



Enabled

Authentication Type
● Click-through
○ EnGenius Authentication
○ Custom Radius
○ Voucher Service
○ Social Login

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login

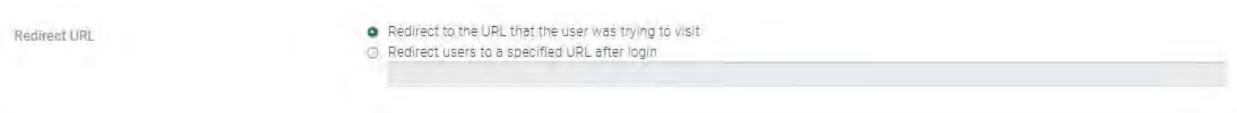
Advanced Setting ⊞

Authentication Type

- Click-through: User must view and acknowledge your splash page before being allowed on the network.
- EnGenius Authentication: User must enter a username and password before being allowed on the network. You could edit user settings through **Configure** > Cloud RADIUS User.
- Custom RADIUS: Enter the host (IP address of your RADIUS server, reachable from the access points), port (UDP port the RADIUS server listens on for access requests, 1812 by default), and secret (RADIUS client shared secret). Optionally, the Accounting Server can be enabled on an SSID that's using WPA2-Enterprise with RADIUS authentication.
- Voucher Service: Edit the access plan for guests for the front-desk manager.
- Social Login: Allows users to use a Facebook account to access WiFi.

Redirect URL

Configure the URL to which users will be redirected after successful login.



Redirect URL

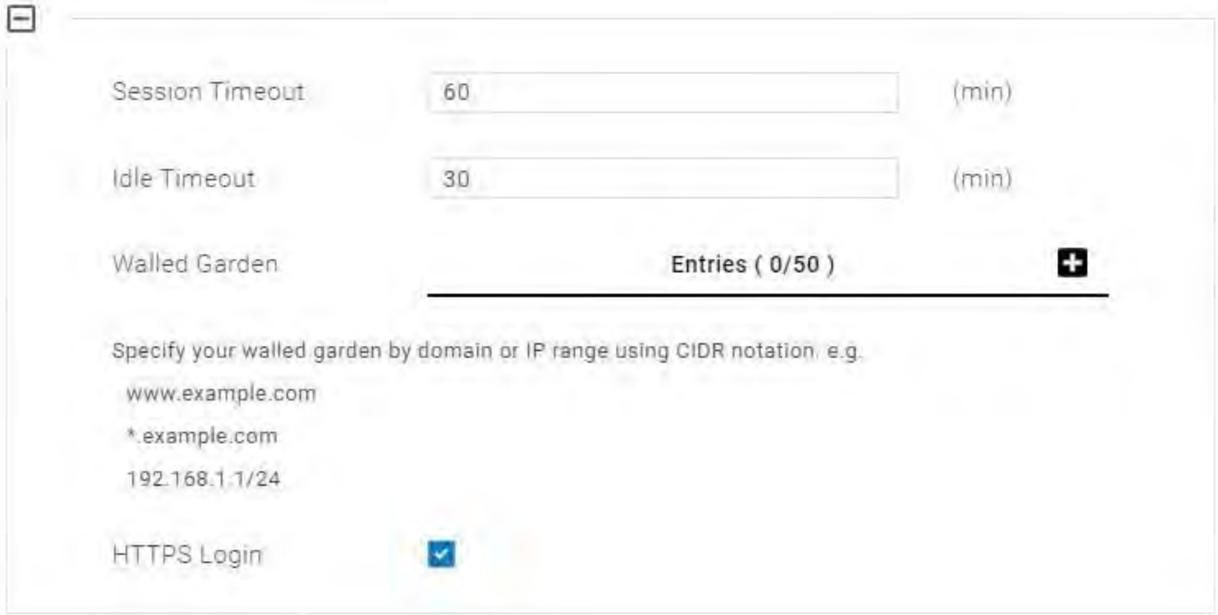
● Redirect to the URL that the user was trying to visit

○ Redirect users to a specified URL after login

Redirect to the original URL: Select this option to cache the initial website from the client during the authentication process and then forward it to the originally targeted web server after the user successfully authenticates.

Redirect users to a new URL: Select this option to redirect users to a pre-designated URL after the user successfully authenticates.

Advanced Setting



Session Timeout 60 (min)

Idle Timeout 30 (min)

Walled Garden Entries (0/50)

Specify your walled garden by domain or IP range using CIDR notation. e.g.

www.example.com

*.example.com

192.168.1.1/24

HTTPS Login ☑

Session Timeout: Specify a time limit after which users will be disconnected and required to log in again.

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

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

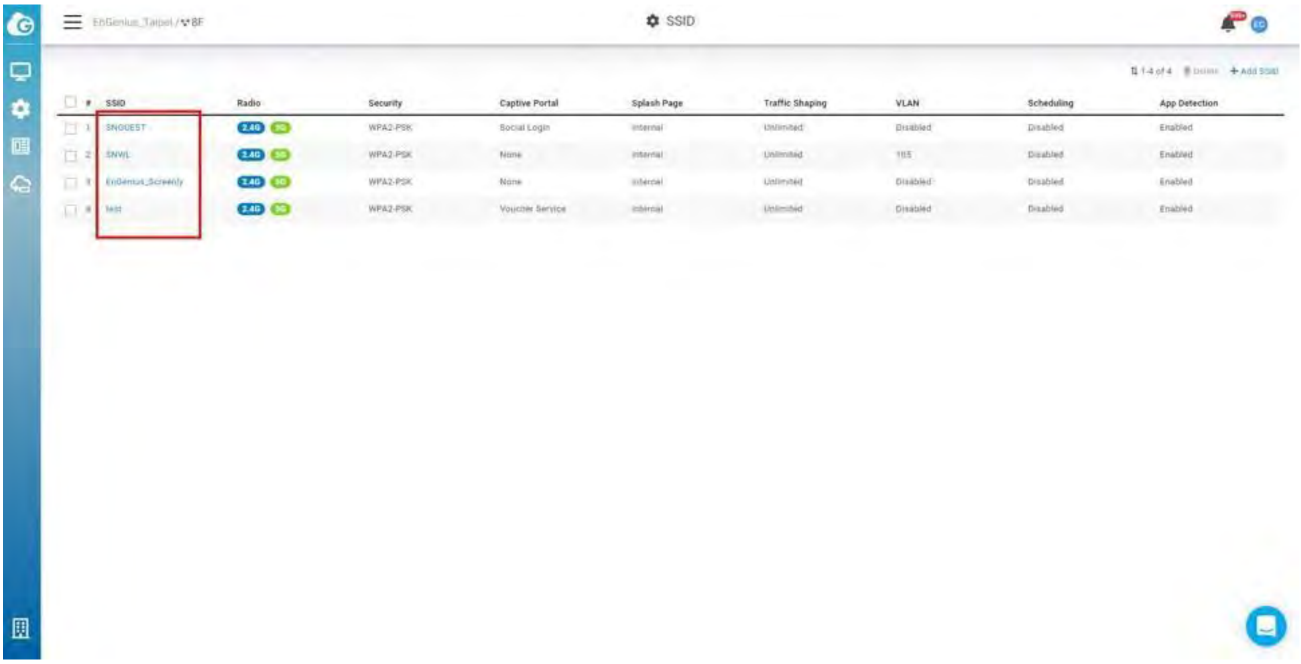
HTTPS Login: This option allows users to log in through HTTPS. When you enable it, your password is encrypted, so others could not retrieve your information.

Social Login

Social login allows you to use your Facebook account to access WiFi.

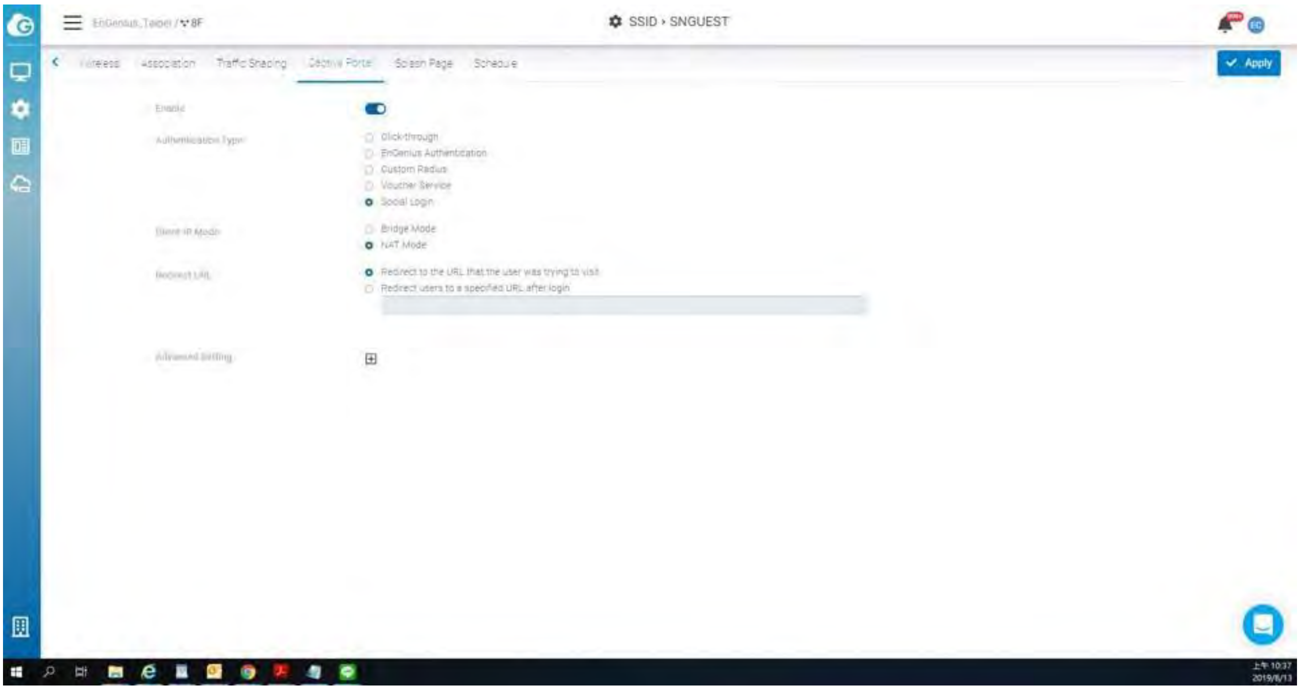
Follow the below steps to configure social login.

1. Click **Configure** > SSID > Select a SSID



□	#	SSID	Radio	Security	Captive Portal	Splash Page	Traffic Shaping	VLAN	Scheduling	App Detection
□	1	SNGUEST	2.4G 5G	WPA2-PSK	Social Login	Internal	Unlimited	Disabled	Disabled	Enabled
□	2	SNWL	2.4G 5G	WPA2-PSK	None	Internal	Unlimited	165	Disabled	Enabled
□	3	EnGenius_Screenly	2.4G 5G	WPA2-PSK	None	Internal	Unlimited	Disabled	Disabled	Enabled
□	4	test	2.4G 5G	WPA2-PSK	Voucher Service	Internal	Unlimited	Disabled	Disabled	Enabled

2. Click Captive portal > go to Authentication Type > select Social login.



Enable

Authentication Type
○ Click-through
○ EnGenius Authentication
○ Custom Radius
○ Voucher Service
● Social Login

Client IP Mode
○ Bridge Mode
● NAT Mode

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login

Advanced Setting ⊞

3. Click Apply.

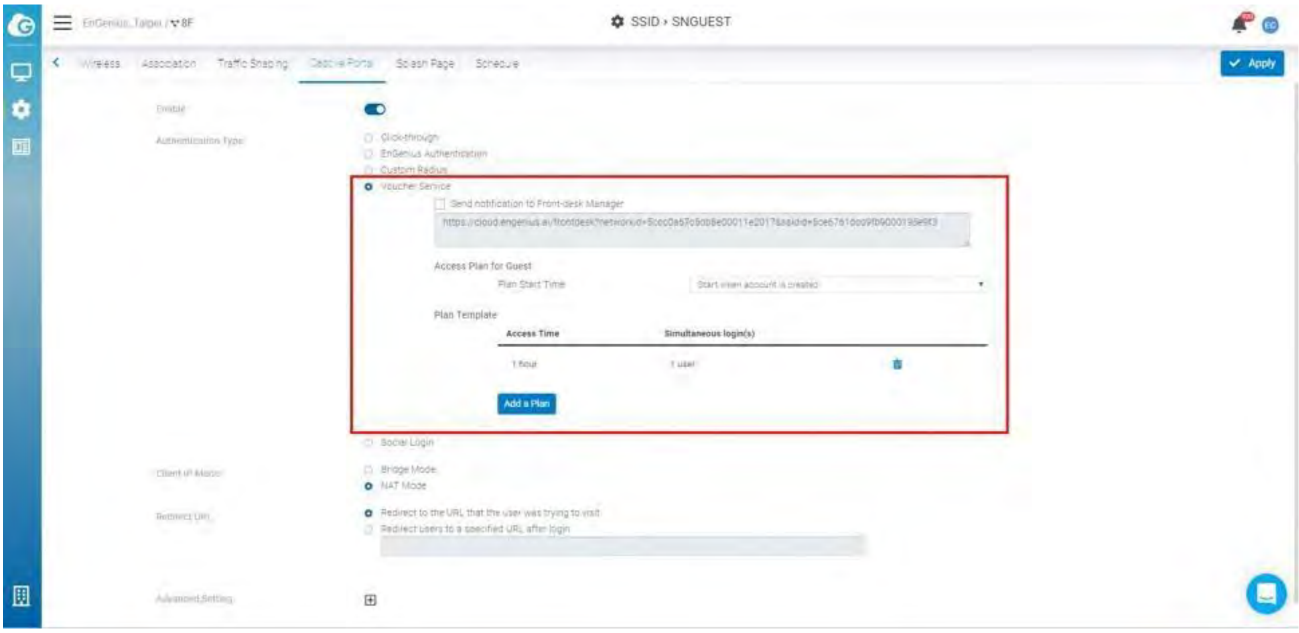
Voucher Service

This guide is intended to help you set up your network to generate and accept vouchers. With vouchers, you control access on a per-user basis by generating guest passes you can provide to users.

Vouchers can be set to specific time increments and are ideal for hotels, coffee shops, apartments, etc. where you want to limit network access to users for a specific period of time.

Enable Voucher Service

Enable the voucher service by clicking **Configure** > SSID > Captive portal > Voucher Service.



Enable: on

Authentication Type:
○ Click-through
○ EnGenius Authentication
○ Custom Radius
● Voucher Service
□ Send notification to Front-desk Manager
https://cloud.engenius.ai/frontdesk?networkId=5cec0a57c5db8e00011e2017&ssidId=5ce6761dc09fb90001[illegible]

Access Plan for Guest
Plan Start Time: Start when account is created

Plan Template

Access Time	Simultaneous login(s)
1 hour	1 user

○ Social Login

Client IP Mode:
○ Bridge Mode
● NAT Mode

Redirect URL:
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login

Advanced Setting ⊞

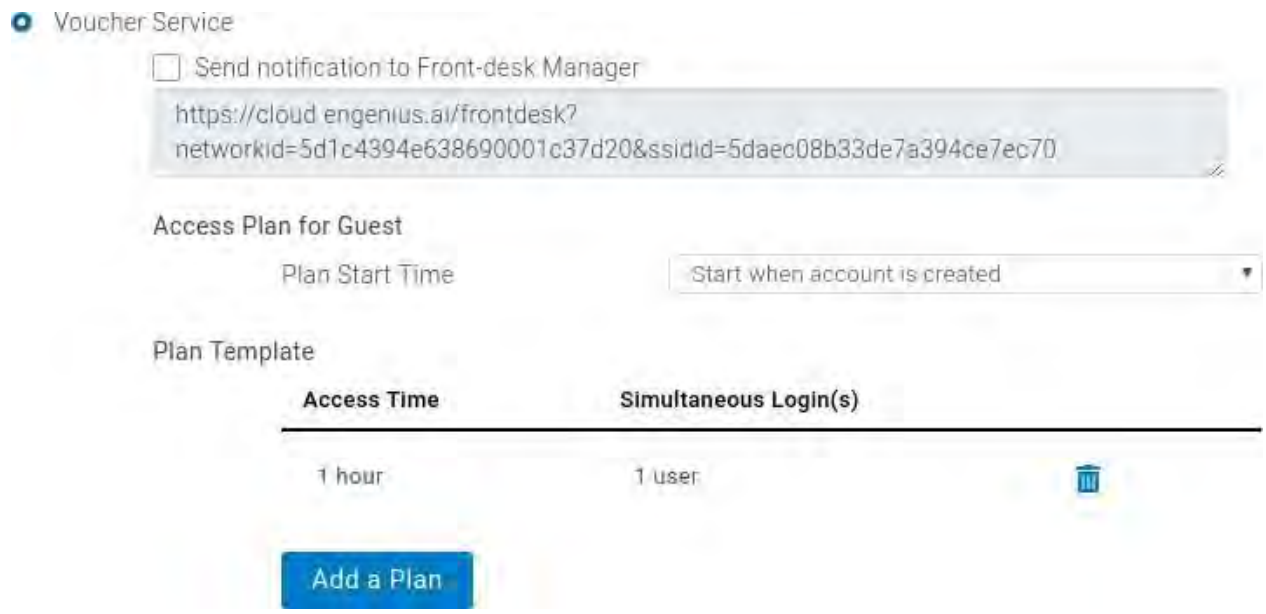
Note: Please make sure that Security Type at **Configure > SSID > Association** has been configured as open or WPA2 PSK before trying to enable Voucher Service. Since Voucher Service is capable of generating user/password randomly, it can not work with a dedicated WPA2 Enterprise authentication server.

Remember click on the `Apply` button at top-right corner to confirm your change on SSID settings.

Management URL and Access Plan

Management URL

For each enabled voucher service, a dedicated Management URL is created. Any team members who have permissions of `Front-desk Manager` or `Administrator` can log in that specific URL and manage Voucher Users there.



● Voucher Service

□ Send notification to Front-desk Manager

https://cloud.engenius.ai/frontdesk?networkid=5d1c4394e638690001c37d20&ssidid=5daec08b33de7a394ce7ec70

Access Plan for Guest

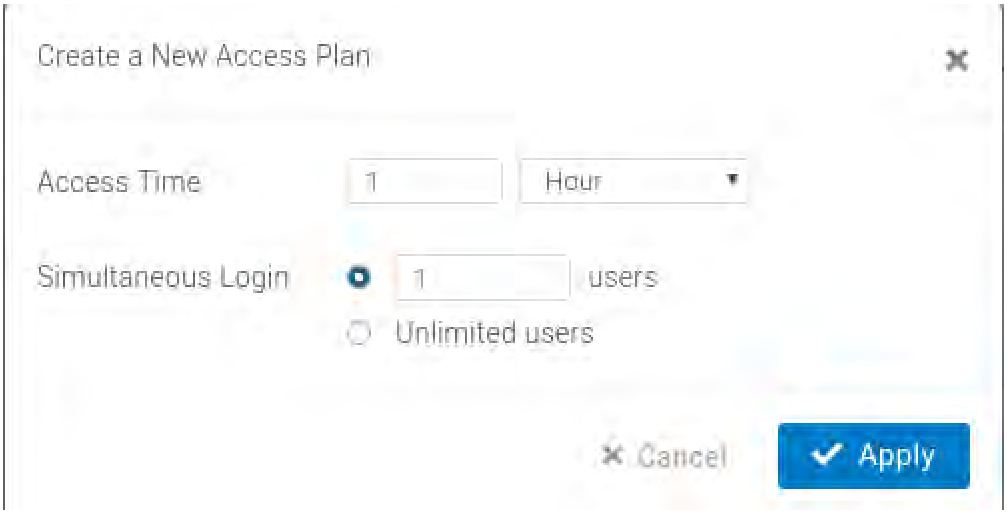
Plan Start Time: Start when account is created

Plan Template

Access Time	Simultaneous Login(s)
1 hour	1 user

Access Plan

In addition, you can create different Plans for voucher user to identify how long a voucher user can access the network (Access Time) and how many simultaneous login are allowed for that user (Simultaneous Login).



Create a New Access Plan ✖

Access Time 1 Hour ▾

Simultaneous Login ● 1 users

○ Unlimited users

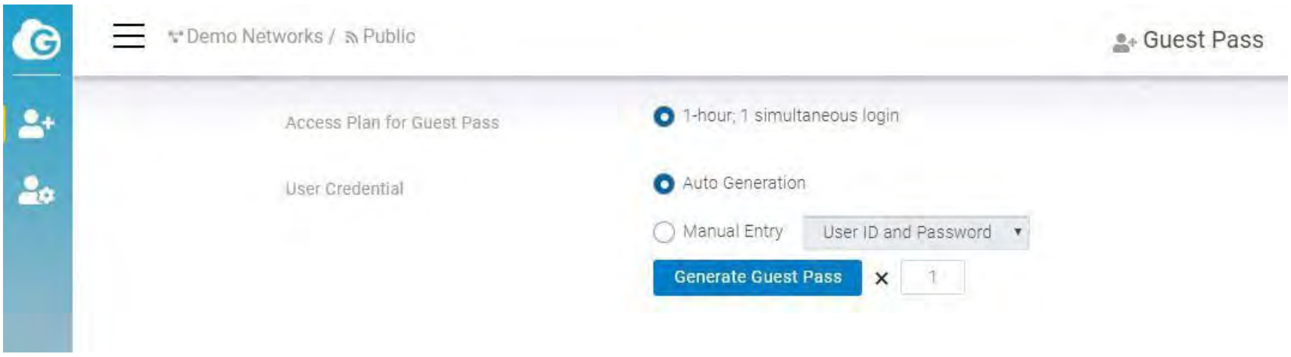
Plan Start Time

The plan start time is an option that defines the plan of voucher service is activated when an account is created or after the account's first login.

Managing Voucher Users

Generating Guest Pass

The first page after you login the Management URL of Voucher Service allows you to generate guest account/password with different manners:



Access Plan for Guest Pass ● 1-hour, 1 simultaneous login

User Credential ● Auto Generation

○ Manual Entry User ID and Password ▾

× 1

A network Administrator or Front-desk Manager can firstly select a access plan and then select to generate account/password of voucher user automatically or manually. Auto

Generation allows you to generate Guest pass in batch , you can fill in the number of the Guest Pass you want to create. Each network supports total 100 Guest Passes.

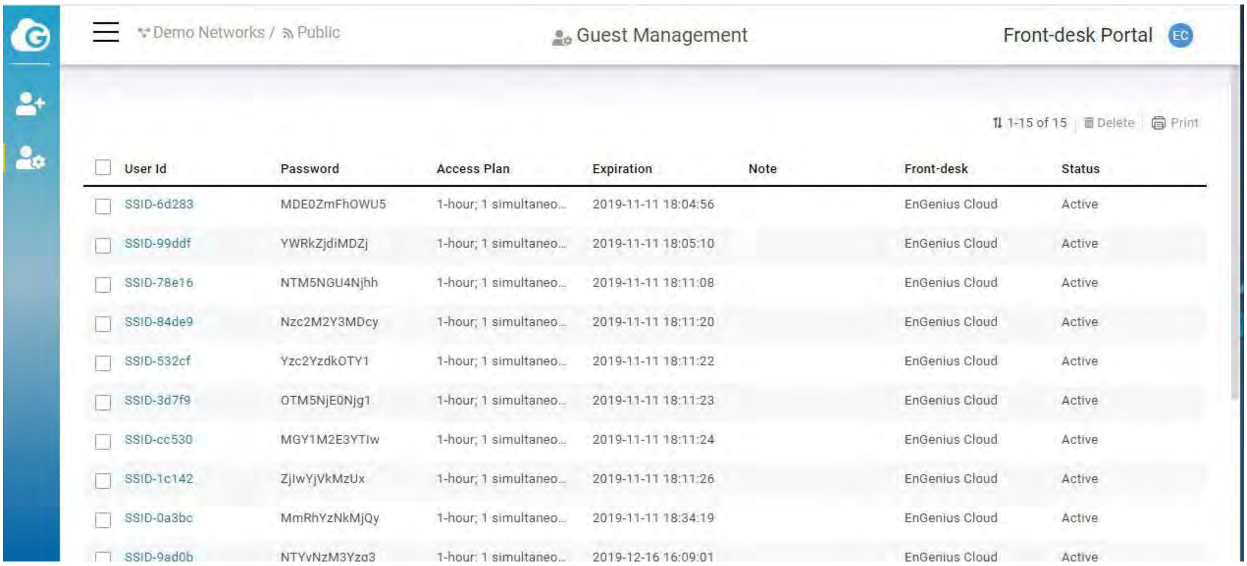
Managing Voucher User

Click on the User Management Button in the toolbar.

A Guest Management Page is performed to list all generated voucher user. You can edit the properties of a voucher user by clicking the user_id of that user or pick the users in that list to delete.

Print the Voucher User Info

In the Guest Management Page, you can also select the users and click on the print button to print the voucher info for end-user. This feature allows you to print voucher users in batch.



□	User Id	Password	Access Plan	Expiration	Note	Front-desk	Status
□	SSID-6d283	MDE0ZmFhOWU5	1-hour; 1 simultaneo...	2019-11-11 18:04:56		EnGenius Cloud	Active
□	SSID-99ddf	YWRkZjdiMDZj	1-hour; 1 simultaneo...	2019-11-11 18:05:10		EnGenius Cloud	Active
□	SSID-78e16	NTM5NGU4Njhh	1-hour; 1 simultaneo...	2019-11-11 18:11:08		EnGenius Cloud	Active
□	SSID-84de9	Nzc2M2Y3MDcy	1-hour; 1 simultaneo...	2019-11-11 18:11:20		EnGenius Cloud	Active
□	SSID-532cf	Yzc2YzdkOTY1	1-hour; 1 simultaneo...	2019-11-11 18:11:22		EnGenius Cloud	Active
□	SSID-3d7f9	OTM5NjE0Njg1	1-hour; 1 simultaneo...	2019-11-11 18:11:23		EnGenius Cloud	Active
□	SSID-cc530	MGY1M2E3YTIw	1-hour; 1 simultaneo...	2019-11-11 18:11:24		EnGenius Cloud	Active
□	SSID-1c142	ZjIwYjVkMzUx	1-hour; 1 simultaneo...	2019-11-11 18:11:26		EnGenius Cloud	Active
□	SSID-0a3bc	MmRhYzNkMjQy	1-hour; 1 simultaneo...	2019-11-11 18:34:19		EnGenius Cloud	Active
□	SSID-9ad0b	NTYyNzM3Yzg3	1-hour; 1 simultaneo...	2019-12-16 16:09:01		EnGenius Cloud	Active

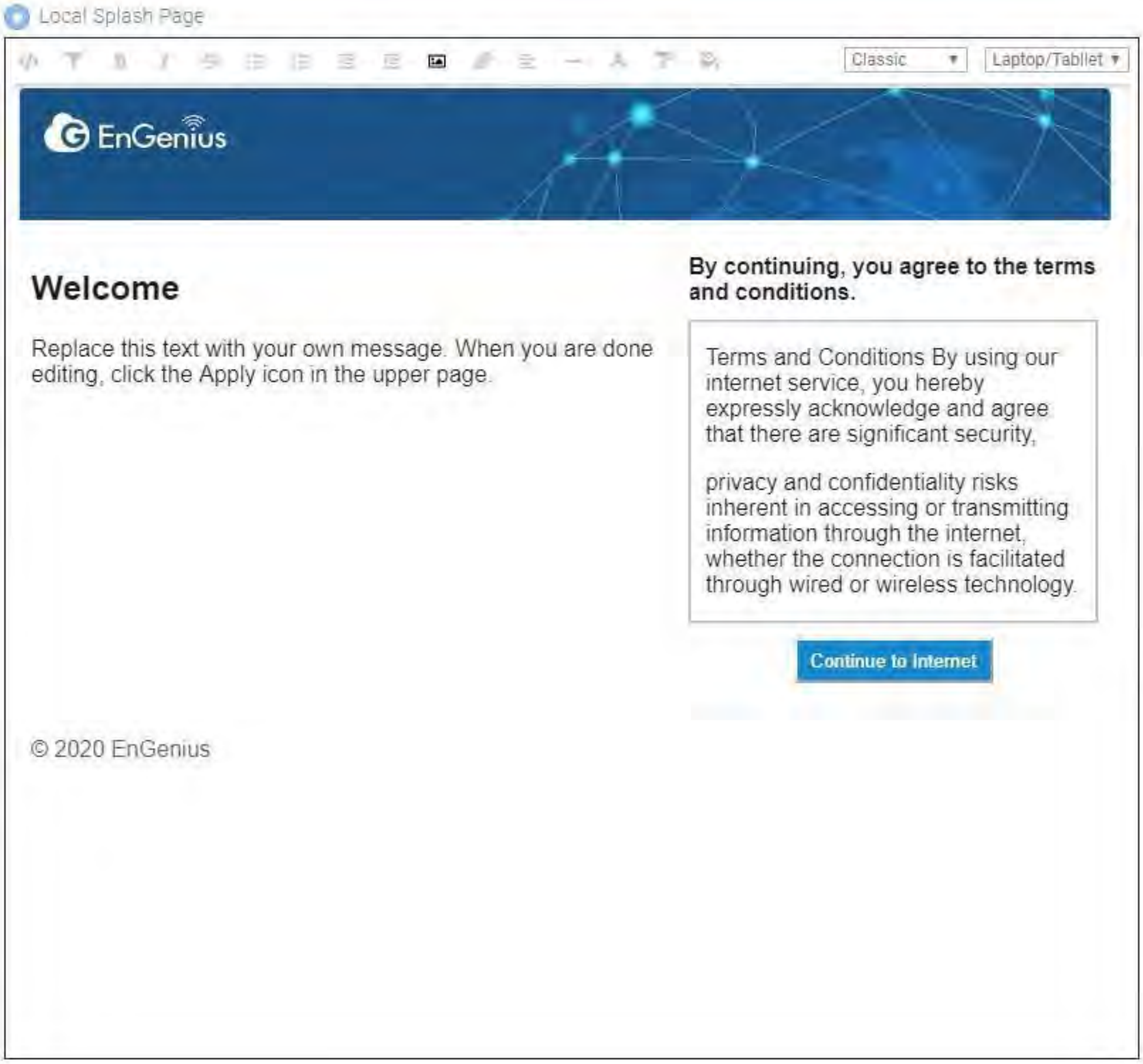
Configuring Splash Page

This guide is intended to help you set up your splash page. With a splash page, you can channel network users to see a custom page before they can access the Internet.

Before you start configuring a splash page, please make sure the captive portal is enabled in advance.

External Splash Page URL: The external splash page enables the administrator to host their own splash page web server, rather than having it hosted by EnGenius Cloud.

Local Splash page : Local Splash page provides the HTML for a splash page that will be hosted internally on the Access Point . For example , allows you to customize your splash page.



Welcome

Replace this text with your own message. When you are done editing, click the Apply icon in the upper page.

By continuing, you agree to the terms and conditions.

Terms and Conditions By using our internet service, you hereby expressly acknowledge and agree that there are significant security,

privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology.

© 2020 EnGenius

After you complete the splash page, please remember to click Apply.

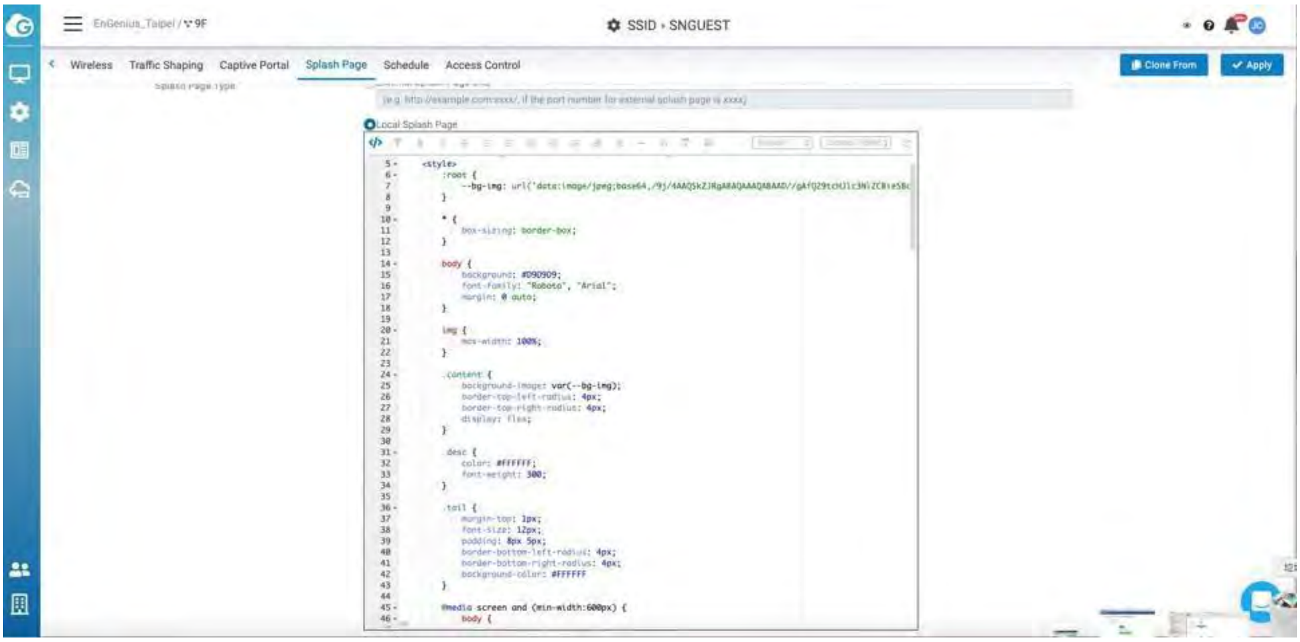
Using the WYSIWYG editor

You can choose different template from the drop-down menu at the top of the editor.

Once you select your starting template, you can customize it with your message, colors, fonts, and images. EnGenius uses a WYSIWYG (what-you-see-is-what-you-get) editor that also supports HTML editing.

In addition to the standard editing tools along the top toolbar , you can click HTML icon to start editing .

</>



```
<style>
    :root {
        --bg-img: url('data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD//gAfQ29tcHJlc3NlZCBieSBc
    }

    * {
        box-sizing: border-box;
    }

    body {
        background: #090909;
        font-family: "Roboto", "Arial";
        margin: 0 auto;
    }

    img {
        max-width: 100%;
    }

    .content {
        background-image: var(--bg-img);
        border-top-left-radius: 4px;
        border-top-right-radius: 4px;
        display: flex;
    }

    .desc {
        color: #FFFFFF;
        font-weight: 300;
    }

    .tail {
        margin-top: 1px;
        font-size: 12px;
        padding: 8px 5px;
        border-bottom-left-radius: 4px;
        border-bottom-right-radius: 4px;
        background-color: #FFFFFF
    }

    @media screen and (min-width:600px) {
        body {
```

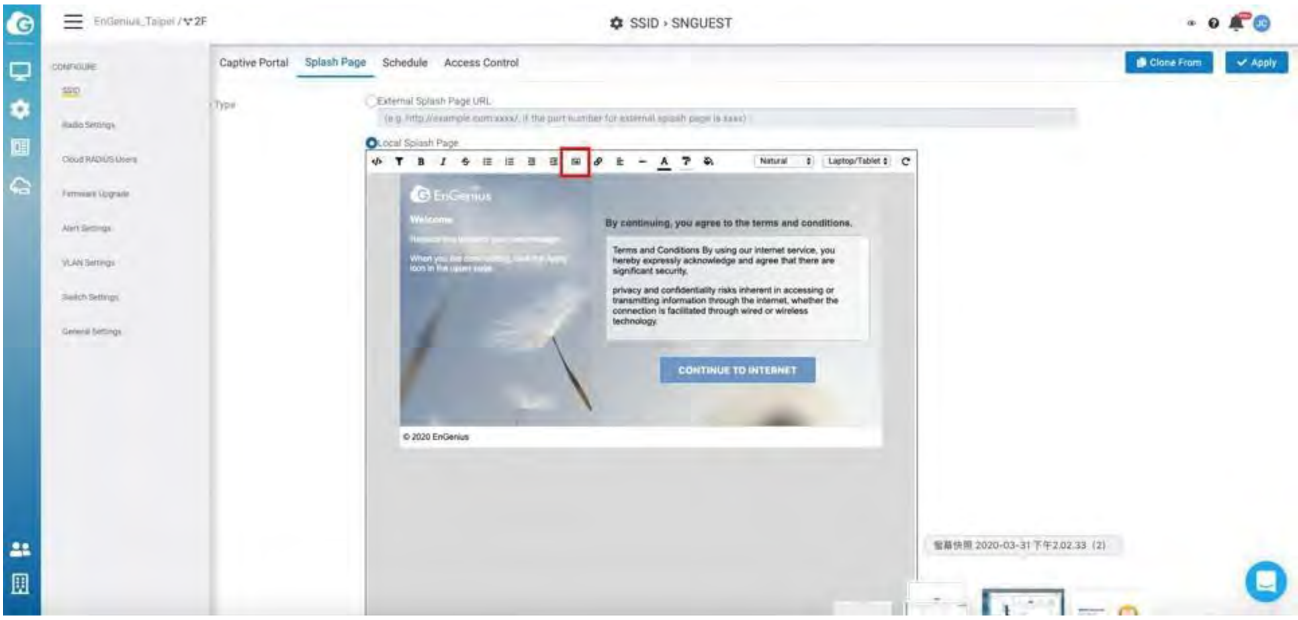
Choosing a starting template

Choose a template from the drop-down menu at the top of the editor. You can customize the content and presentation of these templates to suit your needs . Any edits you make will be a copy of the template, you can go back to the default at any time.

Adding and modifying images

Each splash page template comes with a library of stock images. You can also use the Insert Image tool to add your images and logos.

1. Click the Insert Image button, then navigate to a file, or drag and drop it into the upload images.



By continuing, you agree to the terms and conditions.

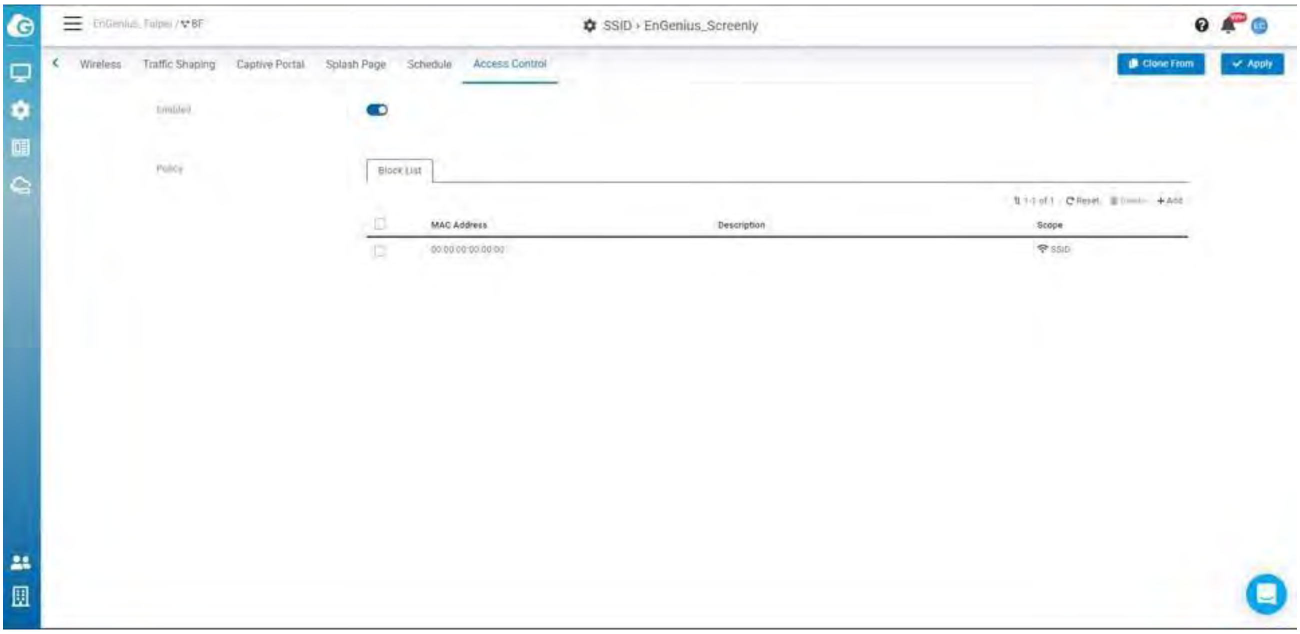
Terms and Conditions By using our internet service, you hereby expressly acknowledge and agree that there are significant security.

privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology.

2. Double-Click on the image or click insert icon to add the image.

Access control

This page allows you to block clients in mac based on current SSID.



Enabled

Policy

□	MAC Address	Description	Scope
□	00:00:00:00:00:00		SSID

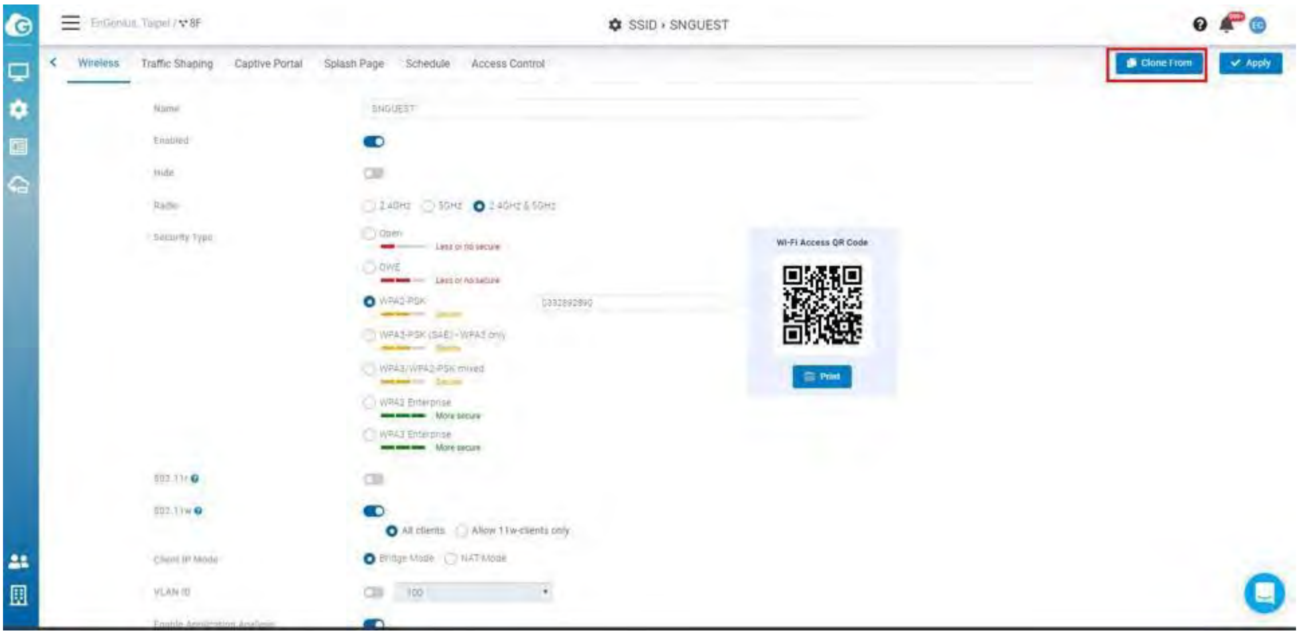
The following describes the functions on this screen:

- Add : The entry for you to add the Mac address to be blocked.
- Reset : Clean all the Block list .
- Delete : Delete the list that you selected .

After you add the block list , remember to click Apply to take effect .

Clone SSID

This allows you to clone SSID configuration which you created previously. So you can create Multiple SSID with same configuration easily.



EnGenius, Taipei / 8F

SSID › SNGUEST

Name: SNGUEST

Enabled: ●

Hide: ○

Radio: ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

Security Type:
○ Open — Less or no secure
○ OWE — Less or no secure
● WPA2-PSK — Secure — 0332892890
○ WPA3-PSK (SAE) - WPA3 only — Strong
○ WPA3/WPA2-PSK mixed — Secure
○ WPA2 Enterprise — More secure
○ WPA3 Enterprise — More secure

802.11r: ○

802.11w: ●
● All clients ○ Allow 11w-clients only

Client IP Mode: ● Bridge Mode ○ NAT Mode

VLAN ID: ○ 100

Enable Application Analysis: ●

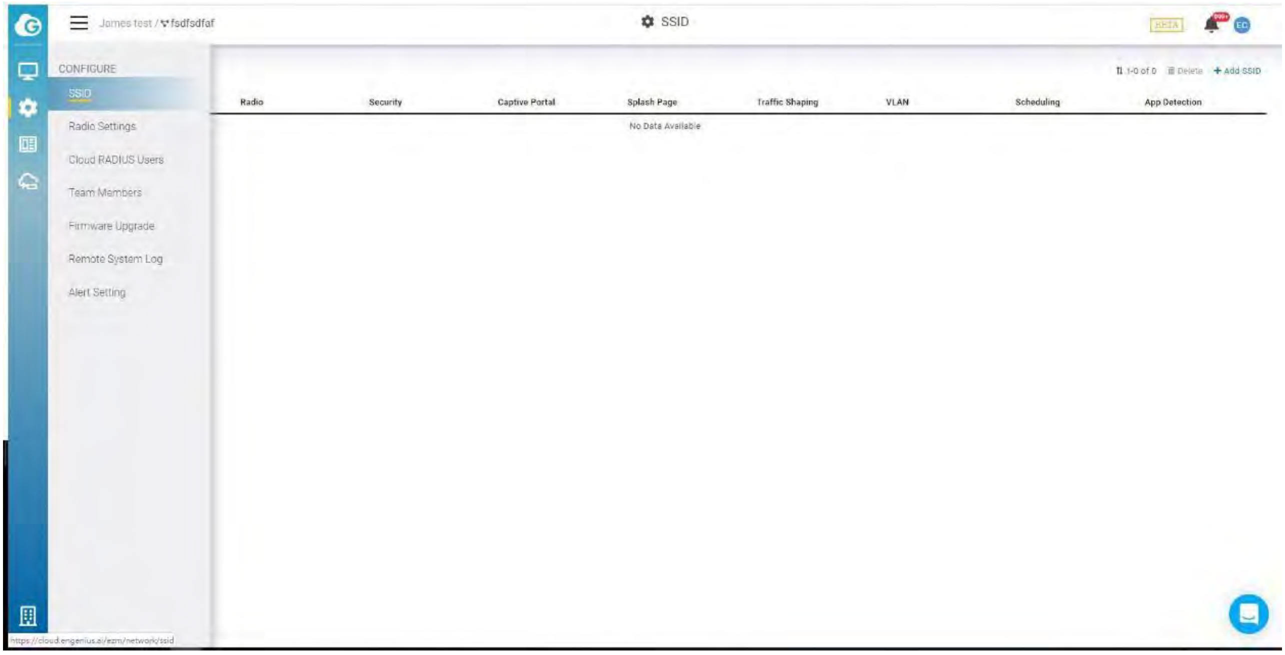
Follow steps to clone SSID

1. Click Clone From
2. Select SSID to be cloned => Click apply in popup
3. Click Apply on tab bar to take effect

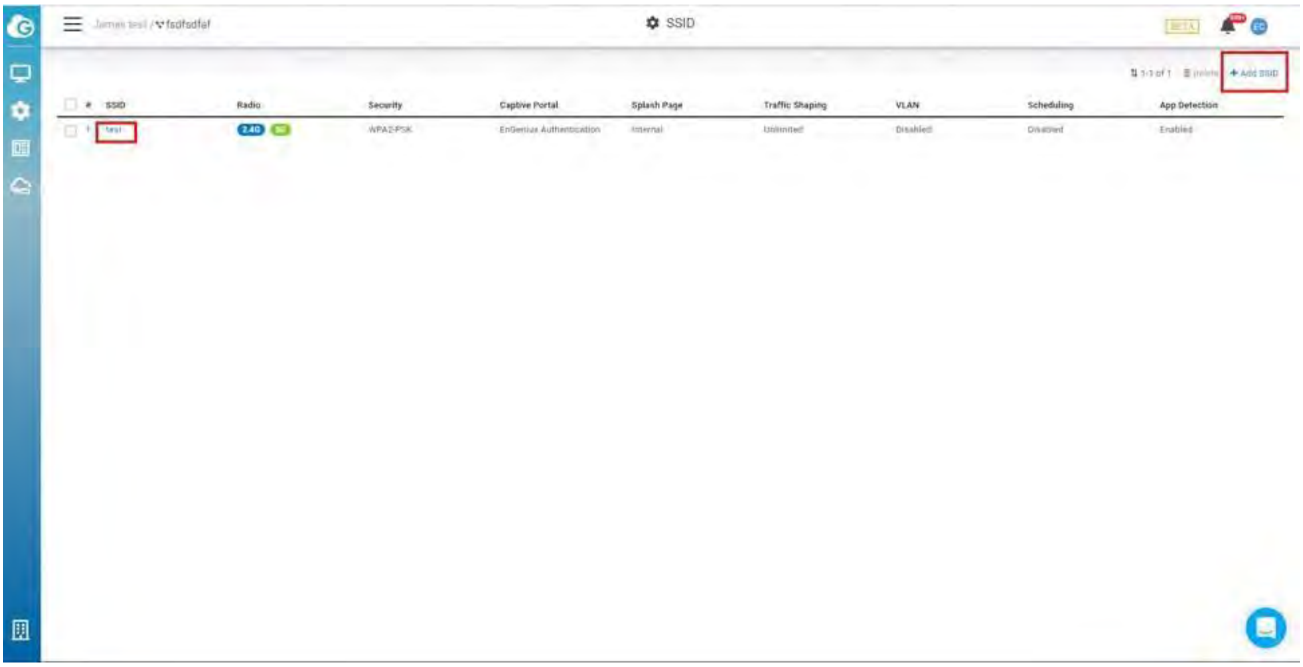
Examples

How to **Configure** Captive Portal

1. Before you begin configuring a captive portal, you need to create a SSID. Navigate to **Configure** > SSID (If you can't click configure, please make sure you are on network scope).



2. Select one of the SSIDs from the list. If one is not available, please click Add SSID to create one.



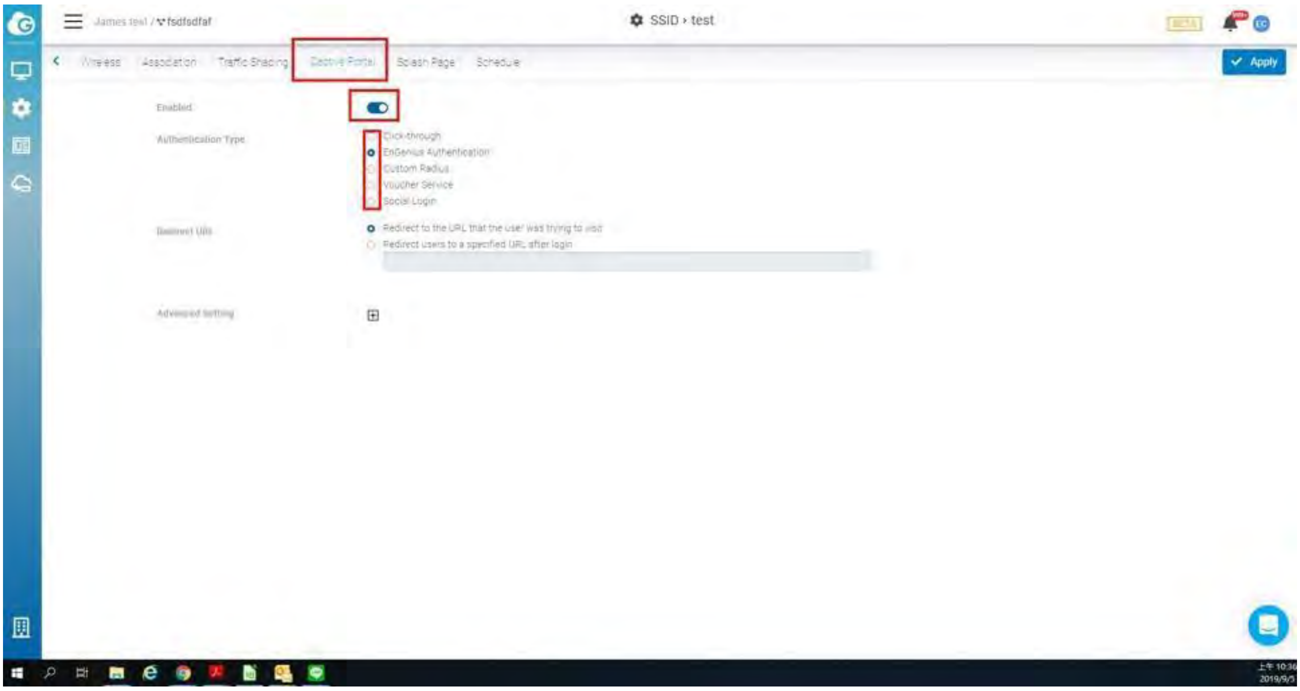
James test / fsdfsdfaf

SSID

1-1 of 1 · Delete · + Add SSID

#	SSID	Radio	Security	Captive Portal	Splash Page	Traffic Shaping	VLAN	Scheduling	App Detection
1	test	2.4G 5G	WPA2-PSK	EnGenius Authentication	Internal	Unlimited	Disabled	Disabled	Enabled

3. Navigate to the captive portal and click Enabled and then select the authentication type.



James test / fsdfsdfaf

SSID › test

Wireless · Association · Traffic Shaping · Captive Portal · Splash Page · Schedule · ✓ Apply

Enabled ●

Authentication Type
○ Click-through
● EnGenius Authentication
○ Custom Radius
○ Voucher Service
○ Social Login

Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login

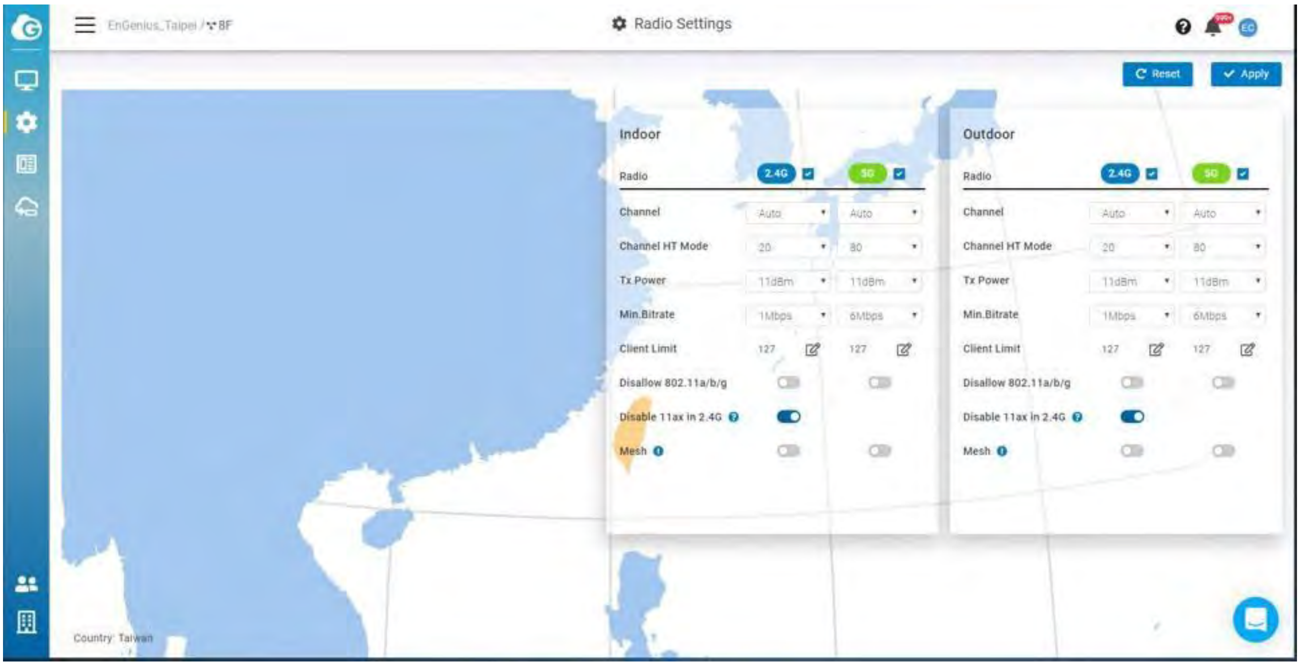
Advanced Setting ⊞

4. Click Apply.

Configuring Radio

Use this screen to configure radio settings for all access points in the network.

Double-click one of the networks on Org-**Trees** > **Configure** > **Radio Settings**.



Indoor

Radio	2.4G ☑	5G ☑
Channel	Auto	Auto
Channel HT Mode	20	80
Tx Power	11dBm	11dBm
Min.Bitrate	1Mbps	6Mbps
Client Limit	127	127
Disallow 802.11a/b/g	○	○
Disable 11ax in 2.4G	●	
Mesh	○	○

Outdoor

Radio	2.4G ☑	5G ☑
Channel	Auto	Auto
Channel HT Mode	20	80
Tx Power	11dBm	11dBm
Min.Bitrate	1Mbps	6Mbps
Client Limit	127	127
Disallow 802.11a/b/g	○	○
Disable 11ax in 2.4G	●	
Mesh	○	○

The settings and options in the Radio Setting page apply to all access points in a network, and you can configure the following settings:

Channel

This option allows users to customize the channels. On the Auto setting, EnGenius access points automatically adjust the channels of their radios to avoid RF interference.

Channel HT Mode

The use of 40 MHz channels on the 2.4 GHz band does not provide for multiple independent channels in multi-AP deployments for 2.4GHz. The recommended setting is

20MHz. To maximize throughput, use 40 MHz for 802.11n and 80 MHz for 802.11ac for 5GHz. Note that higher density deployments should use 20 MHz or 40 MHz channels on 5GHz.

Tx Power

Using this option, users can set a custom range for Tx power.

The higher the transmission power (Tx power) of the access point, the bigger the coverage of the WiFi signal, so usually maximum power is set for an access point to connect to another access point for WDS or mesh purposes.

However, it might not be the best practice if the access point serves the purpose of being a client access point because usually client devices (notebooks, mobile phones, etc.) might not have the same transmission power to be able to communicate back.

Current device's transmission power can be referenced here, where most notebooks and mobile phone transmission power range from 15dBm - 25dBm. Some WiFi devices, like Amazon Echo, are in the smaller range of 10-11dBm.

If your enterprise environment is comprised mainly of notebooks and mobile phones, then it is better to turn down your access point transmission power to 15-17dBm on 5G, and 10-12dBm for 2.4G (so the coverage area of 5G and 2.4G is about the same). If you keep the same transmission power of 5G and 2.4G, it also means the signal strength of 2.4G is about 6 dB higher than 5G at the same location. Then the client device might roam from 5G to 2.4G because it detects better signal strength. It is highly recommended to leverage EnGenius ezWiFiPlanner tool to simulate coverage with different transmission power settings.

Minimum Bit Rate

EnGenius access points can adjust the minimum bit rate for each radio (2.4G and 5G separately). When the minimum bitrate is set, an access point will send out beacons based on the minimum bit rate.

For example, if the bit rate is set to 6Mbps, then those clients with slower than 6Mbps bit rate will not be able to connect to the WiFi and will not slow down other client's performance. 802.11b max bit rate is 11Mbps, so if 12Mbps is set per radio, then 802.11b clients will not be able to connect to the network.

The other benefit is to help better roaming, because when a client roams to a weaker RSSI signal and causes slower performance, then the access point will be kicked out, and the client will search the available SSIDs again to connect to a stronger signal SSID.

If the value is set too high, then it also means a greater density of access points are required to cover the area with the minimum bit rate. This may potentially cause more channel conflict because the transmission power of the access point remains the same, so the RF coverage area is the same and more RF areas overlap.

Client Limit

This is a hardware limitation, commonly applied to most access points in the market. There can be 254 clients connected to an access point at a maximum (127 clients to each 2.4G and 5G band). To serve more than 127 2.4/5G clients in a space, a higher density of access points must be deployed.

Discard 802.11 a/b/g

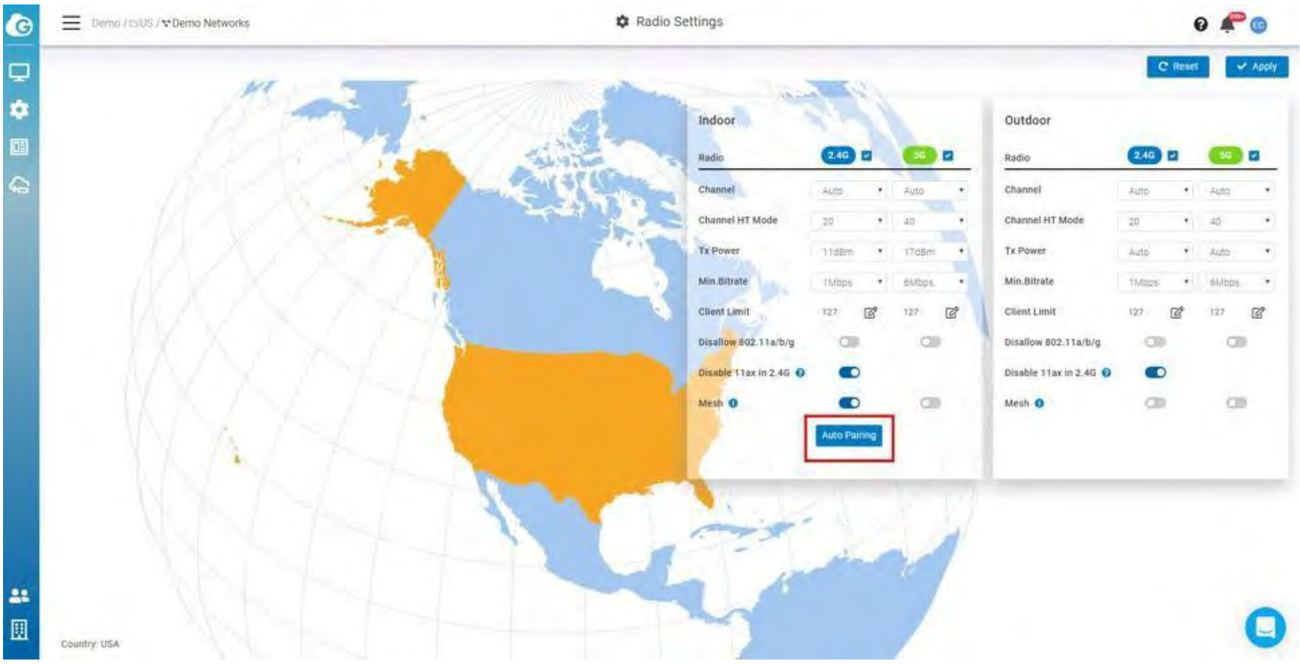
This option allows users to discard 802.11 a/b/g devices to use network to prevent from impact of performance to other 802.11ac/ax clients.

Disable 11ax in 2.4G

Some legacy wireless clients are not compatible with 11ax . This option allows legacy equipment to connect with your network as usual, we suggest you disabling 11ax in 2.4G of your Radio settings. In this way, you can have equipments working in 5G with better performance and get legacy devices served well in 2.4G.

Mesh

This option allows users to enable mesh on 2.4GHz or 5GHz. After you enable mesh, there is an Auto Pairing button. After you click Auto Pairing , access points that haven't linked to the Internet are able to be scanned by neighborhood APs to run the mesh.



Indoor

Radio	2.4G ☑	5G ☑
Channel	Auto	Auto
Channel HT Mode	20	40
Tx Power	11dBm	17dBm
Min.Bitrate	1Mbps	6Mbps
Client Limit	127	127
Disallow 802.11a/b/g	○	○
Disable 11ax in 2.4G	●	
Mesh	●	○

Auto Pairing

Outdoor

Radio	2.4G ☑	5G ☑
Channel	Auto	Auto
Channel HT Mode	20	40
Tx Power	Auto	Auto
Min.Bitrate	1Mbps	6Mbps
Client Limit	127	127
Disallow 802.11a/b/g	○	○
Disable 11ax in 2.4G	●	
Mesh	○	○

How to enable mesh node

1. Find an AP which is wired and working fine (connecting to Cloud successfully that Power LED is steady orange)
2. Place your new try-to-mesh AP which already registered to your Org and be assigned to

a Network nearby the cloud-connected AP. (less than 10 meter depends on the transmission power set of 2 AP's)

3. Power on try-to-mesh AP until "mesh" LED keep flashing
4. Click Auto Pairing and it starts to count down on our Cloud Web UI. That means the Cloud-connected AP is trying to find the try-to-mesh AP and help it to join Cloud

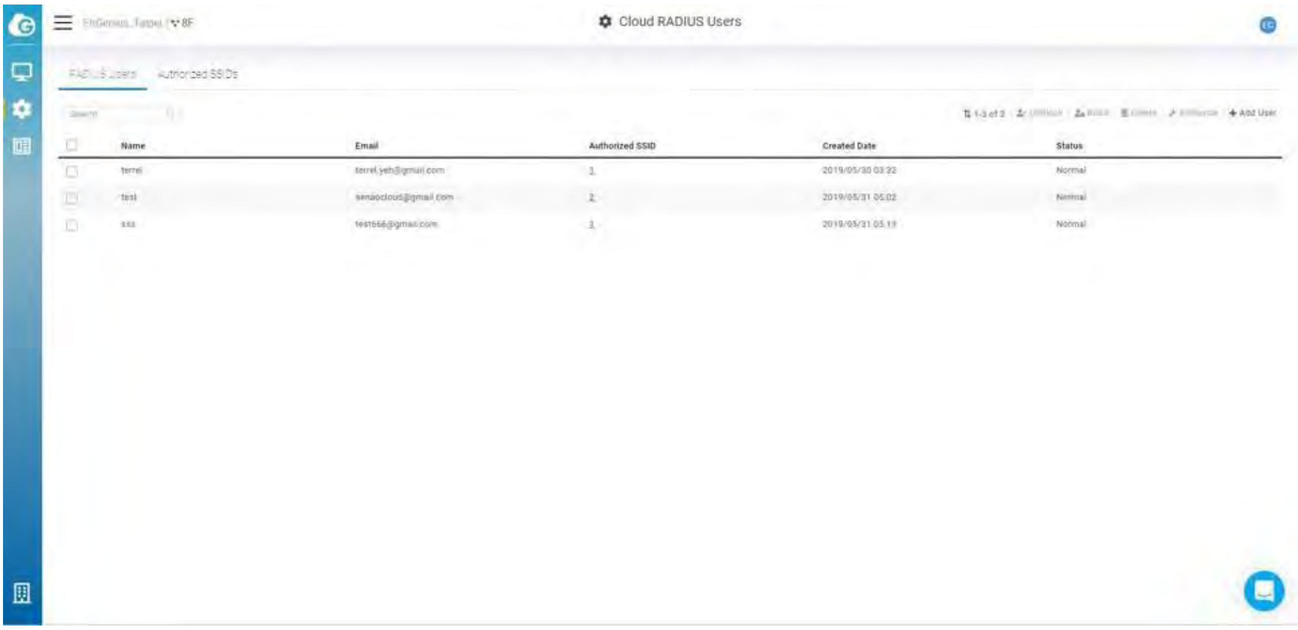
> 1. There must be a Cloud-connected AP nearby try-to-mesh AP to access wirelessly and in the same "Network", so the Mesh configuration can be pushed to 2 AP's to mesh together.
>
> 2. It might take some time since the try-to-mesh AP might need to go through firmware upgrade and reboot (around 4-10 min...).

5. After everything is good, you can find try-to-mesh AP (only ECW120) mesh LED is on, and Power LED is blue.

After you complete each configuration above, you can click Apply, or click Reset to revert back to the original settings.

Configuring Cloud RADIUS

Use this screen to view and manage user accounts authenticated using EnGenius Authentication , you can choose EnGenius authentication from **Configure** > SSID > Captive portal, then select EnGenius Authentication from Authentication Type section).



□	Name	Email	Authorized SSID	Created Date	Status
□	terrel	terrel.yeh@gmail.com	1	2019/05/30 03:32	Normal
□	test	senaocloud@gmail.com	2	2019/05/31 05:02	Normal
□	sss	test666@gmail.com	1	2019/05/31 05:13	Normal

Double-click one of the networks on Org-**Trees > Configure > Cloud RADIUS Users** to access this screen.

The following describes the labels on this screen:

1. Name: Shows the descriptive name of the user account.
2. Email: Shows the type of the user account.
3. Authorized SSID: Shows the SSID numbers that the user has authorized.
4. Create Date: Shows the date and time that the user was created.
5. Status: Shows whether the user has been blocked or not.

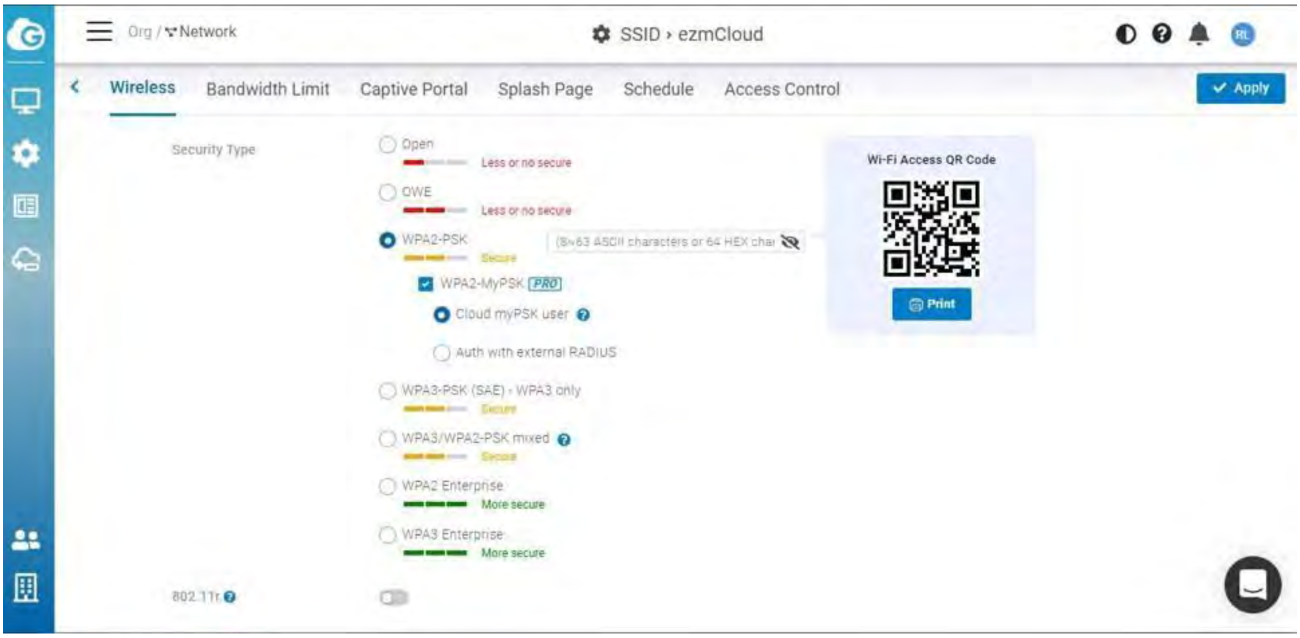
The following describes the functions on this screen:

- Add User: Add users and authorize users to SSIDs.
- Authorize: Allows you to authorize users to SSIDs.
- Delete: Delete users.
- Block: Block users.
- Unblock: Unblock users.

Configuring MyPSK

When setting up an enterprise wireless network, it is common to configure WPA2-PSK authentication in order to onboard different users on to the wireless network. However, IT administrators may still encounter some drawbacks with this method of authentication when they need to use different PSKs in order to assign different VLANs. MyPSK allows a network administrator to use multiple PSKs and assigned different VLANs per SSID.

Before Configuring the MyPSK Users, please make sure you have chosen the Cloud myPSK user From **Configure** > SSID > Wireless > Security Type > WPA2-MyPSK

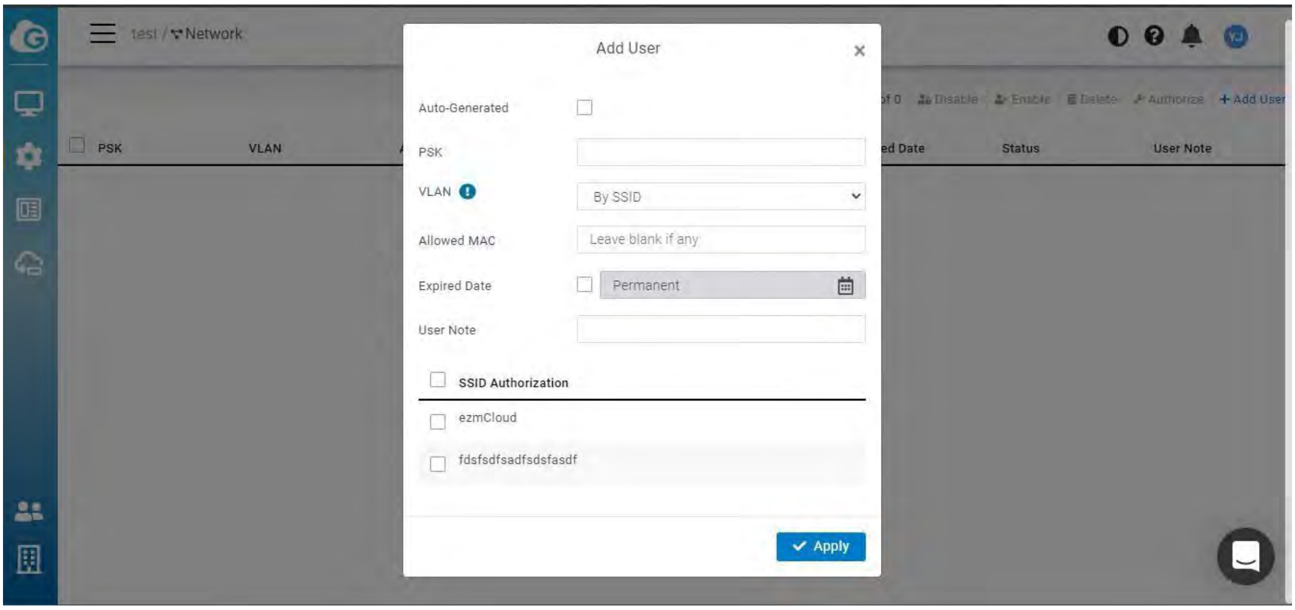


Security Type
○ Open — Less or no secure
○ OWE — Less or no secure
● WPA2-PSK — Secure (8~63 ASCII characters or 64 HEX char
☑ WPA2-MyPSK PRO
● Cloud myPSK user
○ Auth with external RADIUS
○ WPA3-PSK (SAE) - WPA3 only — Secure
○ WPA3/WPA2-PSK mixed — Secure
○ WPA2 Enterprise — More secure
○ WPA3 Enterprise — More secure

802.11r

Create my PSK Users

You can access this screen from **Configure** > MyPSK Users > Add Users



Add User ×

Auto-Generated □

PSK

VLAN By SSID

Allowed MAC Leave blank if any

Expired Date □ Permanent

User Note

□ SSID Authorization

□ ezmCloud

□ fdsfsdfsadfsdsfasdf

Apply

The following describes the labels on the popup.

Auto-Generated: Click the checkbox and then input the number of the users you want to create. Auto-Generated Users are limited to 50 per time.

PSK: Input the password for the user to log in, Auto-Generated Users will have PSK automatically.

VLAN: By SSID means the user is assigned the VLAN from the SSID which you choose to authorize. If you see the VLAN you wanted is not displayed, you could add the VLAN from **Configure > VLAN Settings,** then you could select from the dropdown list.

Allowed MAC: Only the User with this Mac Address could access the SSID, leave it blank if you don't want to restrict it.

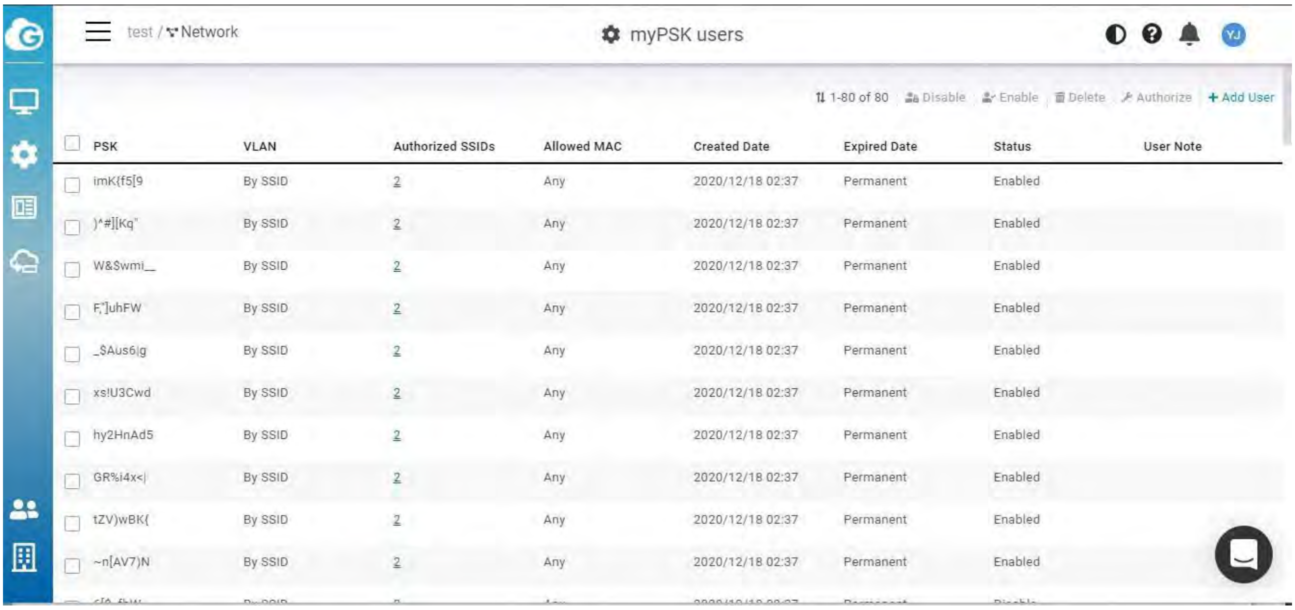
Expired Date: Default is Permanent, click the checkbox to choose the expired date

User note: Add note to map “the user” to the “PSK” to “identify” the person

SSID Authorized: The SSIDs you want users to access

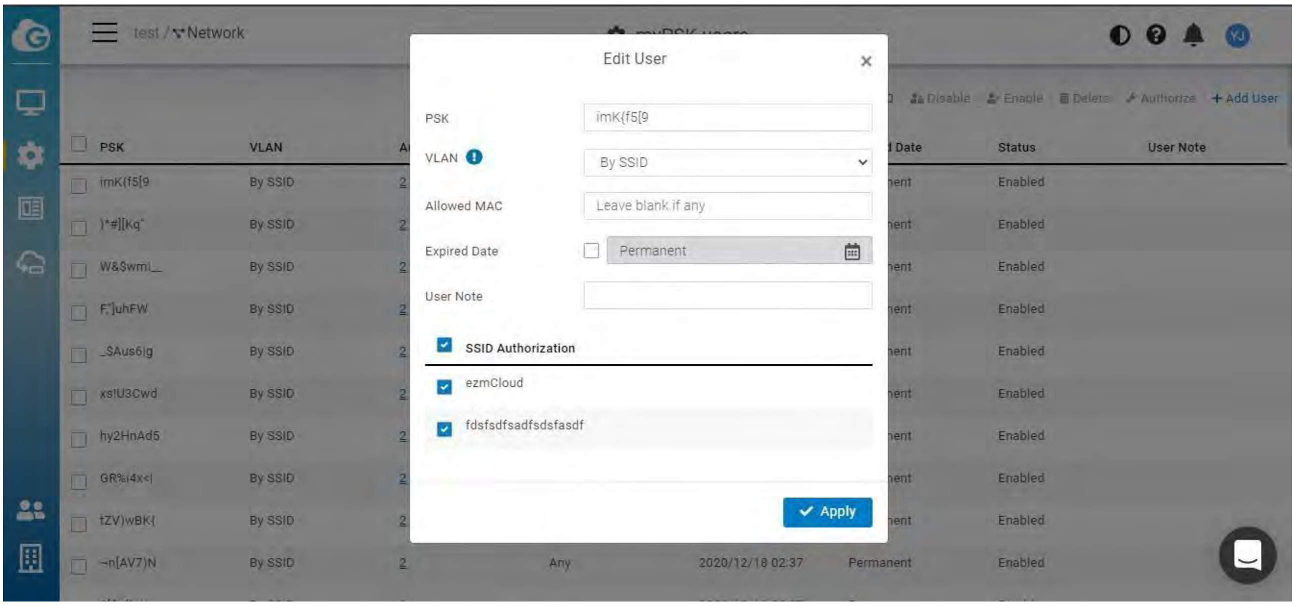
Edit MyPSK Users

1. Click the number on the Authorized SSIDs or each PSK



PSK	VLAN	Authorized SSIDs	Allowed MAC	Created Date	Expired Date	Status	User Note
imK{f5[9	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
)^#][Kq"	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
W&$wmi__	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
F,"]uhFW	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
_$Aus6|g	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
xs!U3Cwd	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
hy2HnAd5	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
GR%i4x<|	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
tZV)wBK{	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	
~n[AV7)N	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	

2. Allows you to edit the details of each user.



Edit User

PSK: imK{f5[9

VLAN: By SSID

Allowed MAC: Leave blank if any

Expired Date: □ Permanent

User Note:

☑ SSID Authorization

☑ ezmCloud

☑ fdsfsdfsadfsdsfasdf

Note

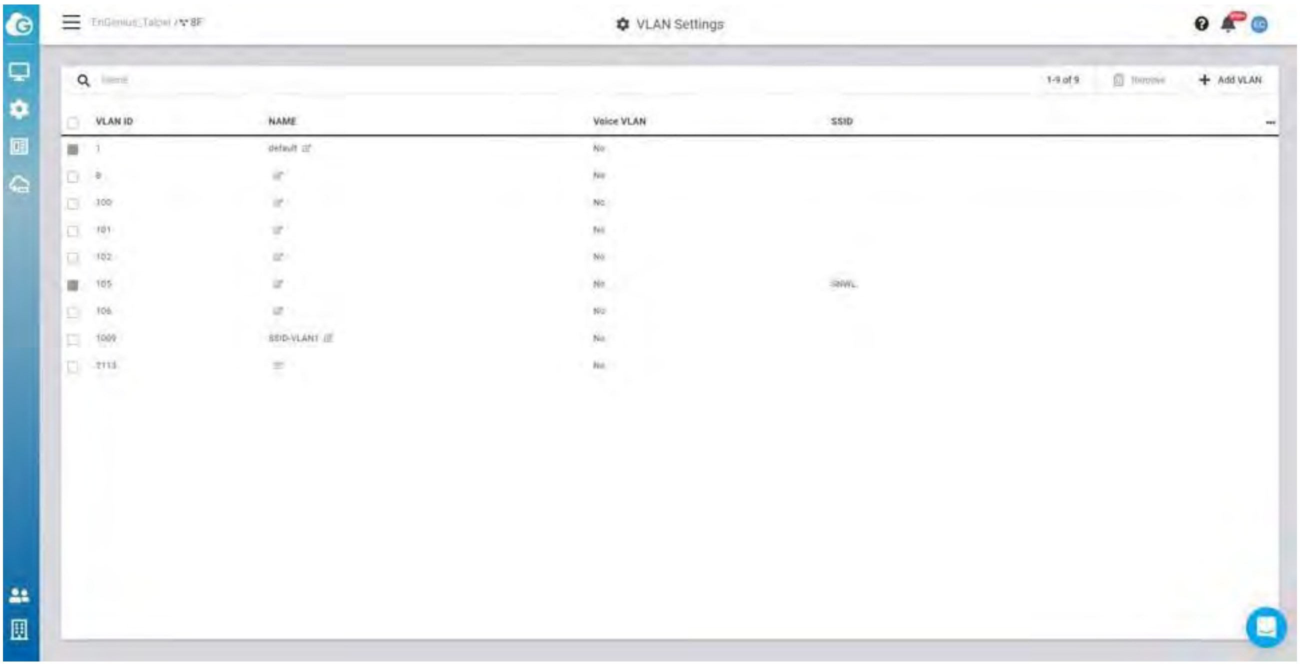
> 1. Doesn't support Captive portal mode nor NAT mode
> 2. Each Network has limited to 500 PSK users
> 3. In the SSID => Wireless => WPA2 myPSK , there is an option "Auth with External RADIUS Server " which is supported with AP v1.X.25 firmware or above. Available models : (ECW220/230/260)

Configuring VLAN

This setting allows you to configure VLAN to all devices in the network at once . Table displays all VLANs have been configure in selected network .

Use this screen to add and delete VLANs for network.

Click **Configure** > VLAN Settings to access this screen.

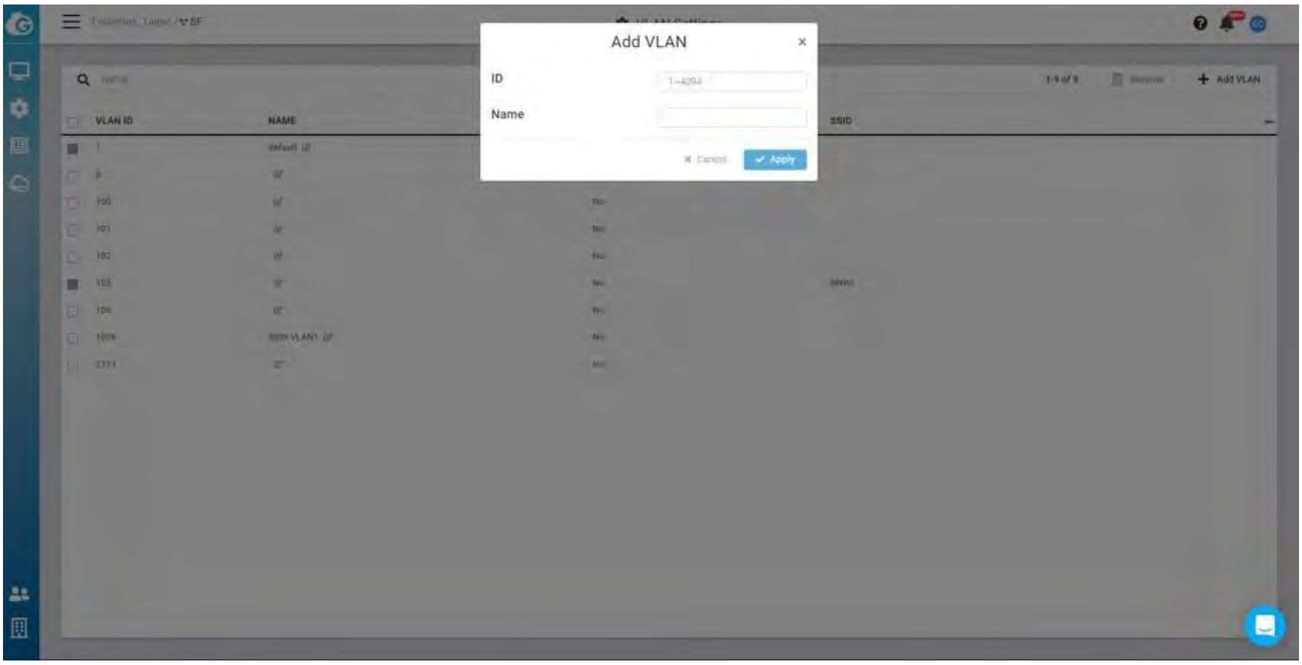


☐	VLAN ID	NAME	Voice VLAN	SSID
■	1	default	No	
☐	8		No	
☐	100		No	
☐	101		No	
☐	102		No	
■	105		No	SNWL
☐	106		No	
☐	1009	SSID-VLAN1	No	
☐	2113		No	

The VLAN Settings page contains the following information :

- VLAN ID : VLAN ID.
- NAME : VLAN name.
- Voice VLAN : This shows if VLAN has been assigned to Voice VLAN or not.
- SSID : the SSID that has been assigned the VLAN.

Add VLAN



ID: 1~4094

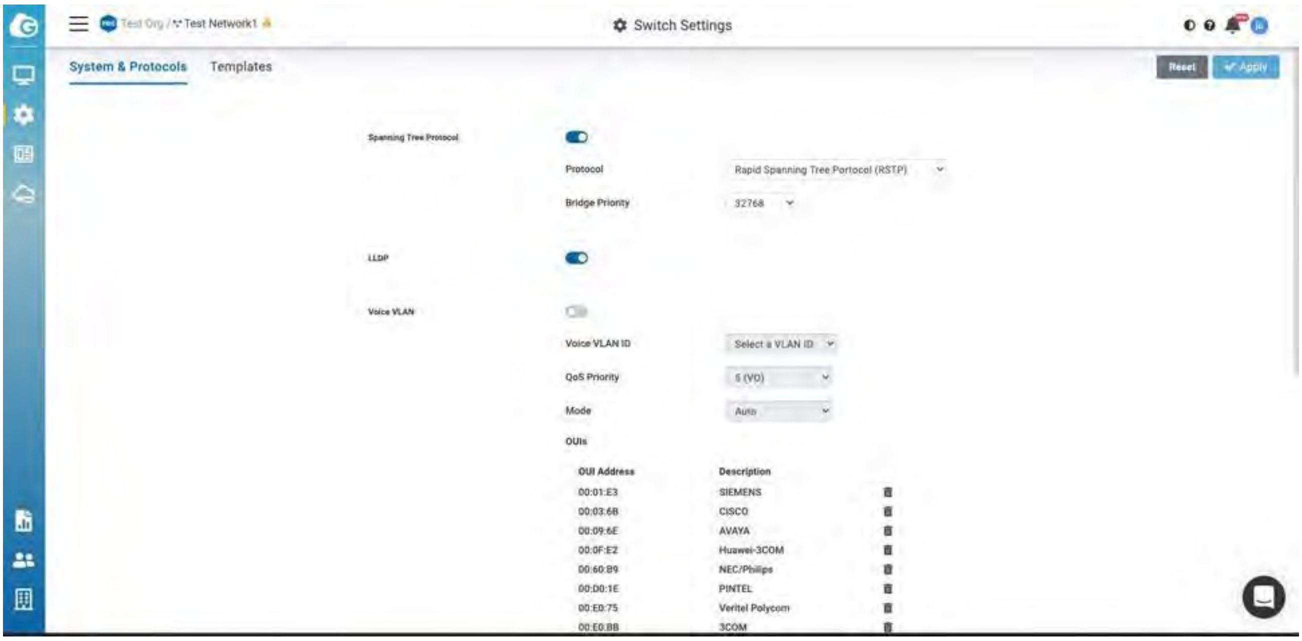
Name:

1. Click Add VLAN button.
2. Input VLAN ID and VLAN Name.
3. Click Apply to complete the settings.

ⓘ After you create the Network wide VLAN , you need to go to Switch detail page to assign ports or go to SSID page to assign the VLAN to specific SSID .

Configuring Switch Settings

This setting allows you to configure Systems & Protocols in the network at once. This gives you to configure the System setting and apply it to whole Switches in the network. you can access this screen by **Configure** > Switch settings.



Spanning Tree Protocol ●

Protocol: Rapid Spanning Tree Portocol (RSTP)

Bridge Priority: 32768

LLDP ●

Voice VLAN ○

Voice VLAN ID: Select a VLAN ID

QoS Priority: 5 (VO)

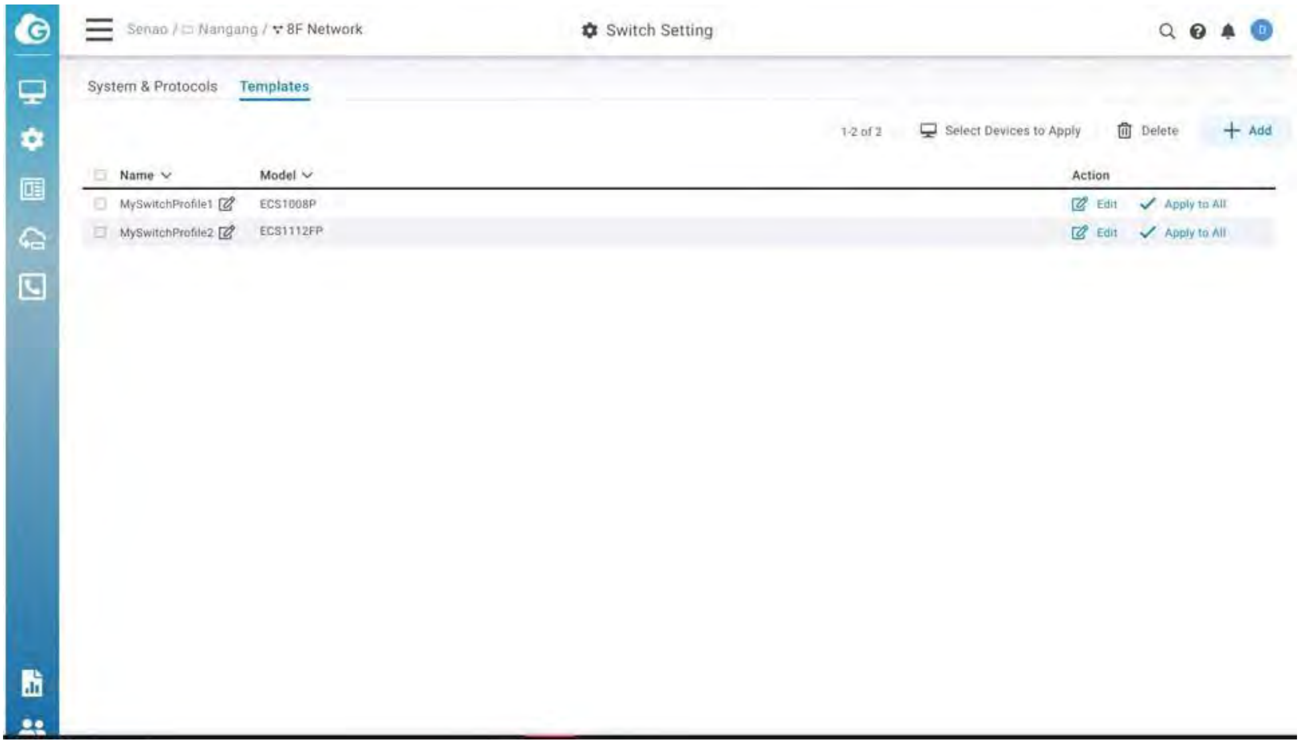
Mode: Auto

OUIs

OUI Address	Description
00:01:E3	SIEMENS
00:03:6B	CISCO
00:09:6E	AVAYA
00:0F:E2	Huawei-3COM
00:60:B9	NEC/Philips
00:D0:1E	PINTEL
00:E0:75	Veritel Polycom
00:E0:BB	3COM

Many MSP or SI would like to be able to “group configure port settings” in the Network. Switch Template feature helps users to apply same port configuration to all switch with same models in the Network to save time of configuration one by one.

you can access this screen by **Configure** > Switch Settings > Template



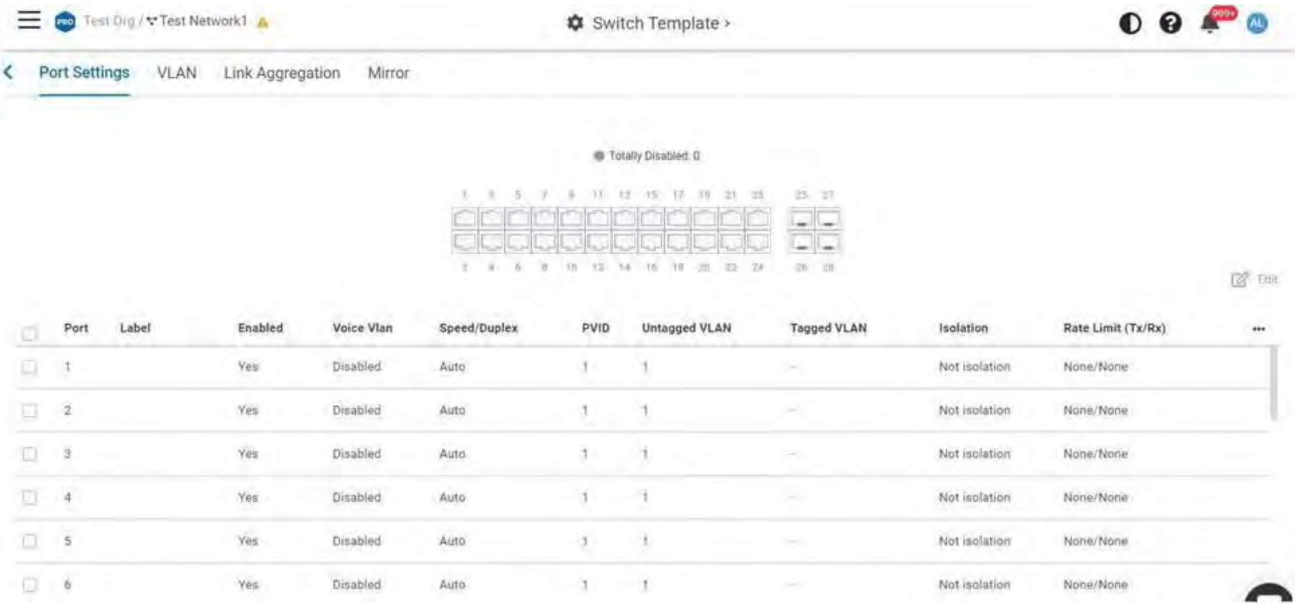
Senao / Nangang / 8F Network — Switch Setting

System & Protocols | Templates

1-2 of 2 | Select Devices to Apply | Delete | + Add

☐	Name	Model	Action
☐	MySwitchProfile1	ECS1008P	Edit ✓ Apply to All
☐	MySwitchProfile2	ECS1112FP	Edit ✓ Apply to All

- You can create any template by Model type (or click on “Edit” of the template). The setting is similar to Individual Switch port settings.



Test Org / Test Network1 — Switch Template ›

Port Settings | VLAN | Link Aggregation | Mirror

● Totally Disabled: 0

Edit

☐	Port	Label	Enabled	Voice Vlan	Speed/Duplex	PVID	Untagged VLAN	Tagged VLAN	Isolation	Rate Limit (Tx/Rx)
☐	1		Yes	Disabled	Auto	1	1	-	Not isolation	None/None
☐	2		Yes	Disabled	Auto	1	1	-	Not isolation	None/None
☐	3		Yes	Disabled	Auto	1	1	-	Not isolation	None/None
☐	4		Yes	Disabled	Auto	1	1	-	Not isolation	None/None
☐	5		Yes	Disabled	Auto	1	1	-	Not isolation	None/None
☐	6		Yes	Disabled	Auto	1	1	-	Not isolation	None/None

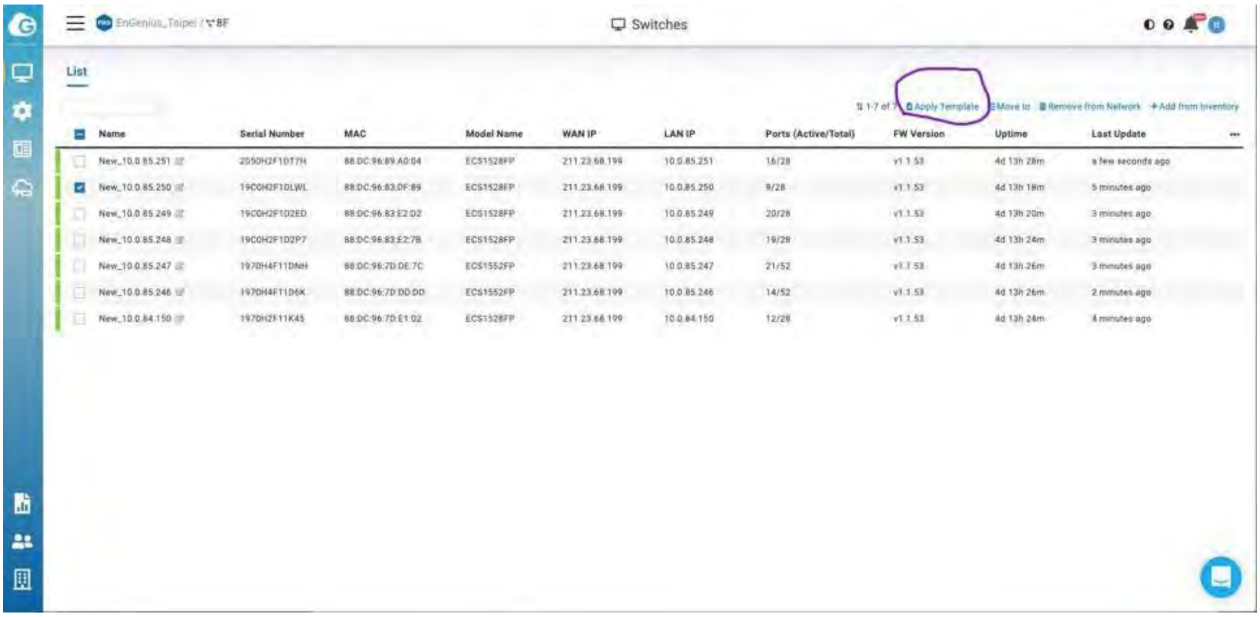
- Apply to All will apply the Switch Template to all devices of the same model in the Network.

ⓘ Note

> - The uplink port will not be overridden by the template to prevent losing connection.
> - Uplink port couldn't be the Mirror destination port
> - PoE on the ports should be enabled when the ports are configured the PoE schedule on the devices.

You can apply the switch template to the same model of the switches from

Manage > Switch List > choose the Switches to be applied > Choose Apply Template

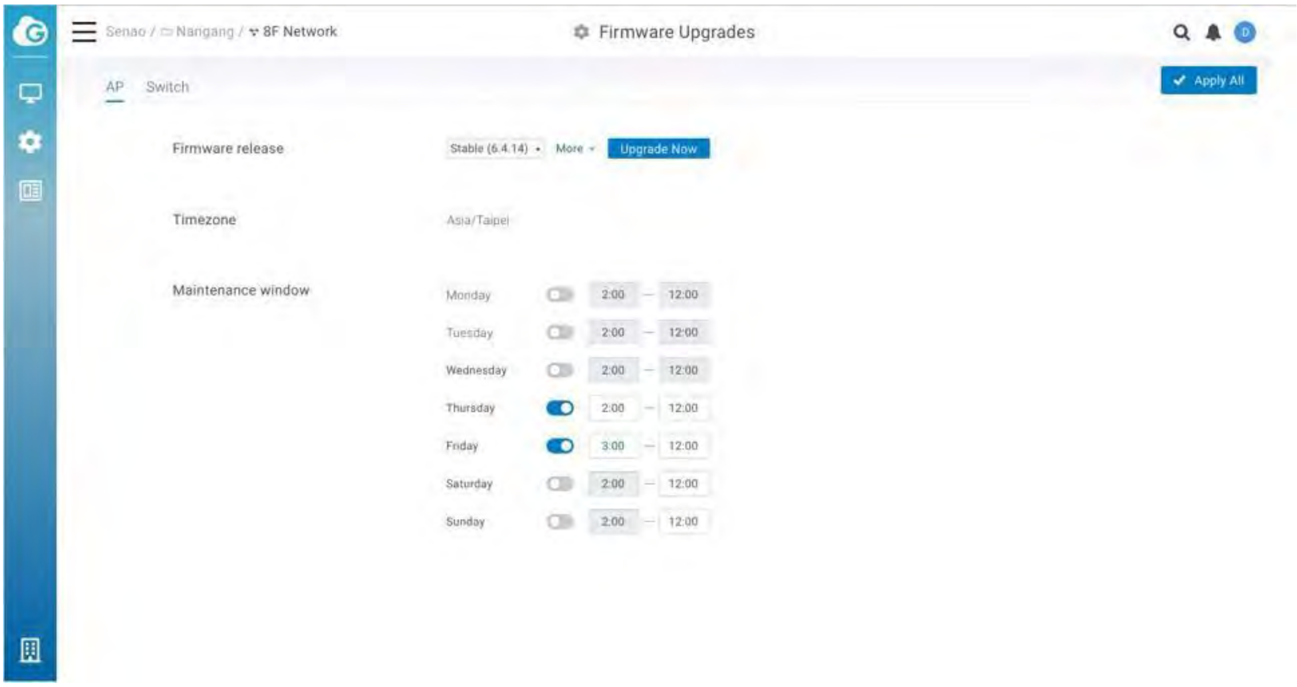


☐	Name	Serial Number	MAC	Model Name	WAN IP	LAN IP	Ports (Active/Total)	FW Version	Uptime	Last Update
☐	New_10.0.85.251	2050H2F1DT7H	88:DC:96:89:A0:04	ECS1528FP	211.23.68.199	10.0.85.251	16/28	v1.1.53	4d 13h 28m	a few seconds ago
☑	New_10.0.85.250	19C0H2F1DLWL	88:DC:96:83:DF:89	ECS1528FP	211.23.68.199	10.0.85.250	9/28	v1.1.53	4d 13h 18m	5 minutes ago
☐	New_10.0.85.249	19C0H2F1D2ED	88:DC:96:83:E2:D2	ECS1528FP	211.23.68.199	10.0.85.249	20/28	v1.1.53	4d 13h 20m	3 minutes ago
☐	New_10.0.85.248	19C0H2F1D2P7	88:DC:96:83:E2:7B	ECS1528FP	211.23.68.199	10.0.85.248	19/28	v1.1.53	4d 13h 24m	3 minutes ago
☐	New_10.0.85.247	1970H4F11DNH	88:DC:96:7D:DE:7C	ECS1552FP	211.23.68.199	10.0.85.247	21/52	v1.1.53	4d 13h 26m	3 minutes ago
☐	New_10.0.85.246	1970H4F11D6K	88:DC:96:7D:DD:DD	ECS1552FP	211.23.68.199	10.0.85.246	14/52	v1.1.53	4d 13h 26m	2 minutes ago
☐	New_10.0.84.150	1970H2F11K45	88:DC:96:7D:E1:02	ECS1528FP	211.23.68.199	10.0.84.150	12/28	v1.1.53	4d 13h 24m	4 minutes ago

Firmware Upgrade

Automatic Upgrades

EnGenius Cloud enables automatic upgrades by default and will upgrade firmware according to the Maintenance Window time period each week.



Firmware release: Stable (6.4.14)

Timezone: Asia/Taipei

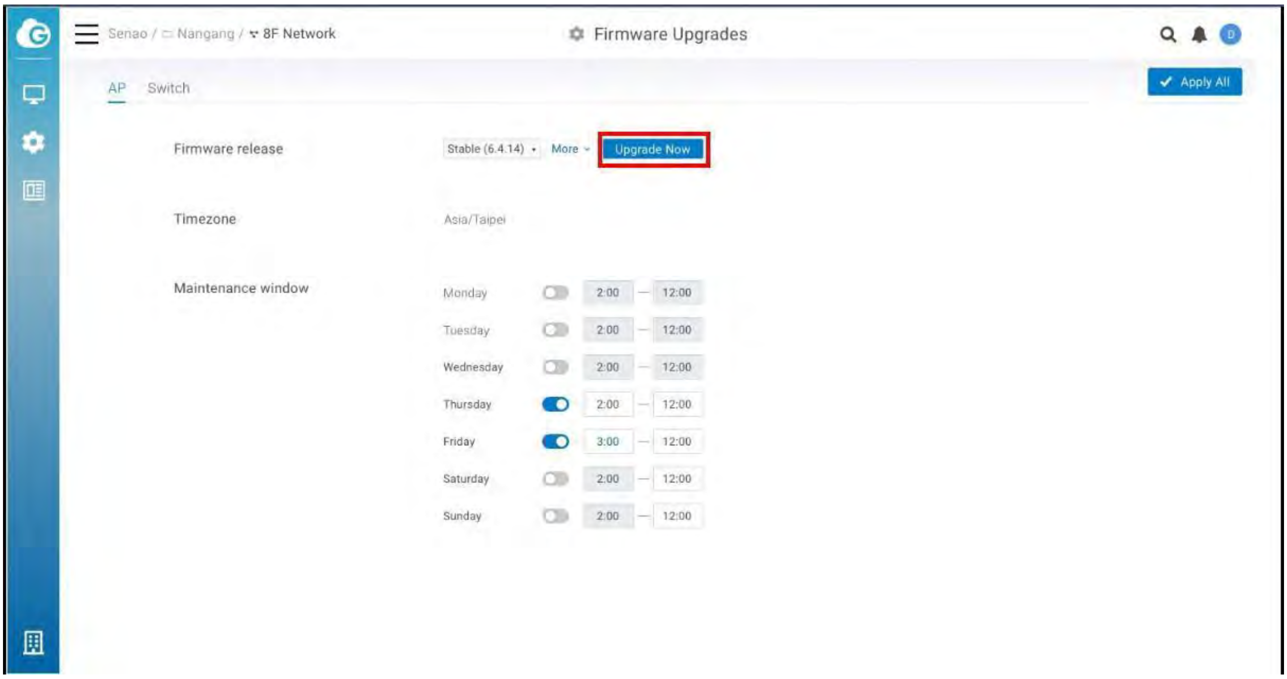
Maintenance window

Monday	○	2:00	12:00
Tuesday	○	2:00	12:00
Wednesday	○	2:00	12:00
Thursday	●	2:00	12:00
Friday	●	3:00	12:00
Saturday	○	2:00	12:00
Sunday	○	2:00	12:00

Manual Upgrade

To manually update device firmware:

1. Select the firmware you desire to upgrade.
2. Click Upgrade Now.



Firmware release: Stable (6.4.14)

Timezone: Asia/Taipei

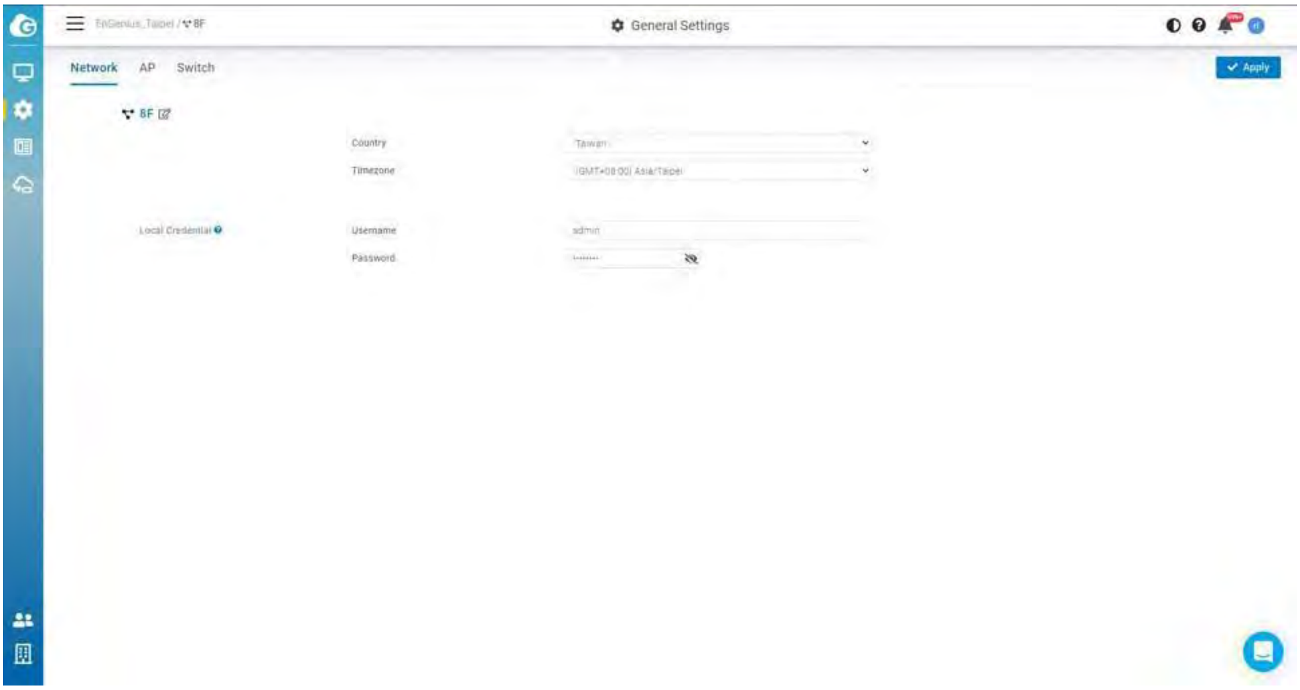
Maintenance window

Monday	○	2:00	12:00
Tuesday	○	2:00	12:00
Wednesday	○	2:00	12:00
Thursday	●	2:00	12:00
Friday	●	3:00	12:00
Saturday	○	2:00	12:00
Sunday	○	2:00	12:00

3. Click Apply.

General Settings

General settings allow you to configure Network settings, AP network-wide settings and so do Switches. Click **Configure** > General Setting to access this screen.



Country: Taiwan

Timezone: (GMT+08:00) Asia/Taipei

Local Credential

Username: admin

Password: ••••••••

Edit Network

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

1. Click edit button to change network name
2. Select Country, Timezone, and then click Apply

Local Credential

This feature allows you to configure the login account of local web GUI for devices. The settings here apply to all APs and Switches in this Network .

> ⓘ Note that username and password could be blank if you don't want to change device login account of local web GUI.

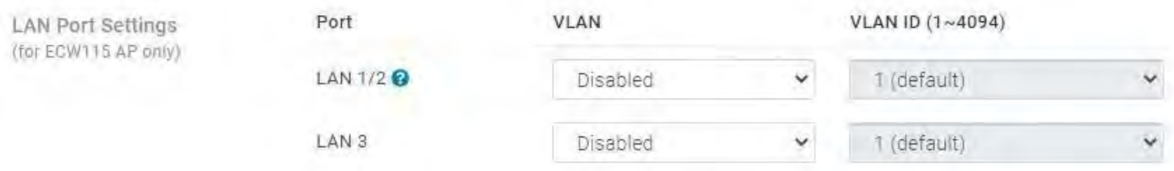
LED Light

This allows you to enable all AP's LED lights in the current network.

LED Light ●

LAN Port settings (for ECW115AP only)

This allows you to configure Lan port settings on ECW115. Noticed that either LAN1 Lan2 can be used for the uplink port. This setting will be applied to the one which is not uplink port



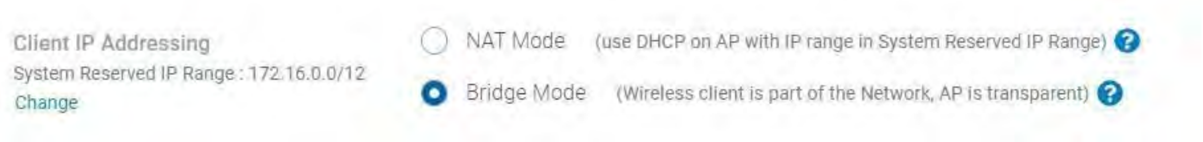
LAN Port Settings
(for ECW115 AP only)

Port	VLAN	VLAN ID (1~4094)
LAN 1/2 ?	Disabled	1 (default)
LAN 3	Disabled	1 (default)

System Reserved IP Range

When using NAT (AP DHCP) and captive portal, AP will leverage a range of IP addresses as default. If user unconsciously configures their local Network conflicting with the range, it will cause problems. the user is able to change the System reserved range if they cannot change their local LAN IP address range.

SSID > Wireless > IP Addressing (NAT/Bridge). Click "Change" will redirect to Network-wide setting

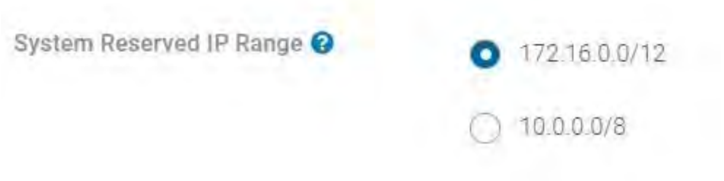


Client IP Addressing
System Reserved IP Range : 172.16.0.0/12
Change

○ NAT Mode (use DHCP on AP with IP range in System Reserved IP Range)

● Bridge Mode (Wireless client is part of the Network, AP is transparent)

General Settings > AP > System Reserved IP Range



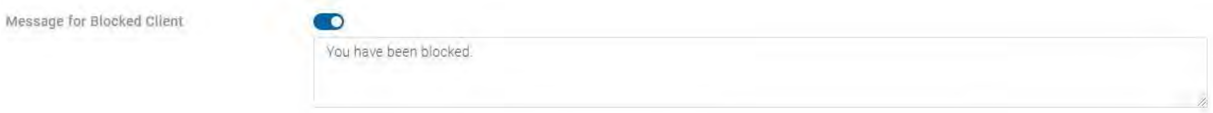
System Reserved IP Range

● 172.16.0.0/12

○ 10.0.0.0/8

Message for blocked Clients

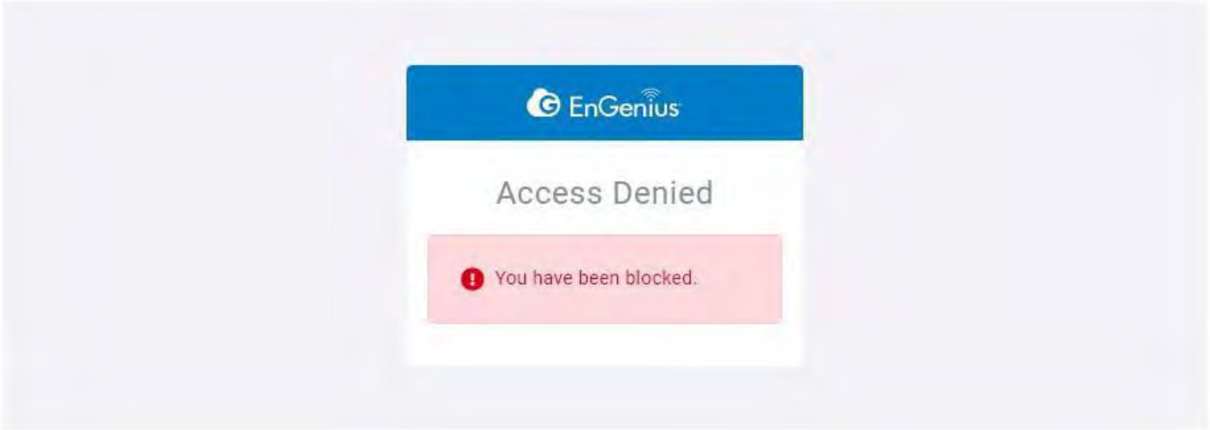
Clients can be blocked from accessing the network. When these clients attempt to connect to the network and open a web browser, they will be redirected to a blocked message. The Network-wide Default block message is configured on a per-network basis. The message is set in the Network-wide > General Settings > AP page.



Message for Blocked Client

You have been blocked.

The blocked splash page below will be presented below to the blocked clients.



Access Denied

You have been blocked.

Advanced settings

Presence reporting

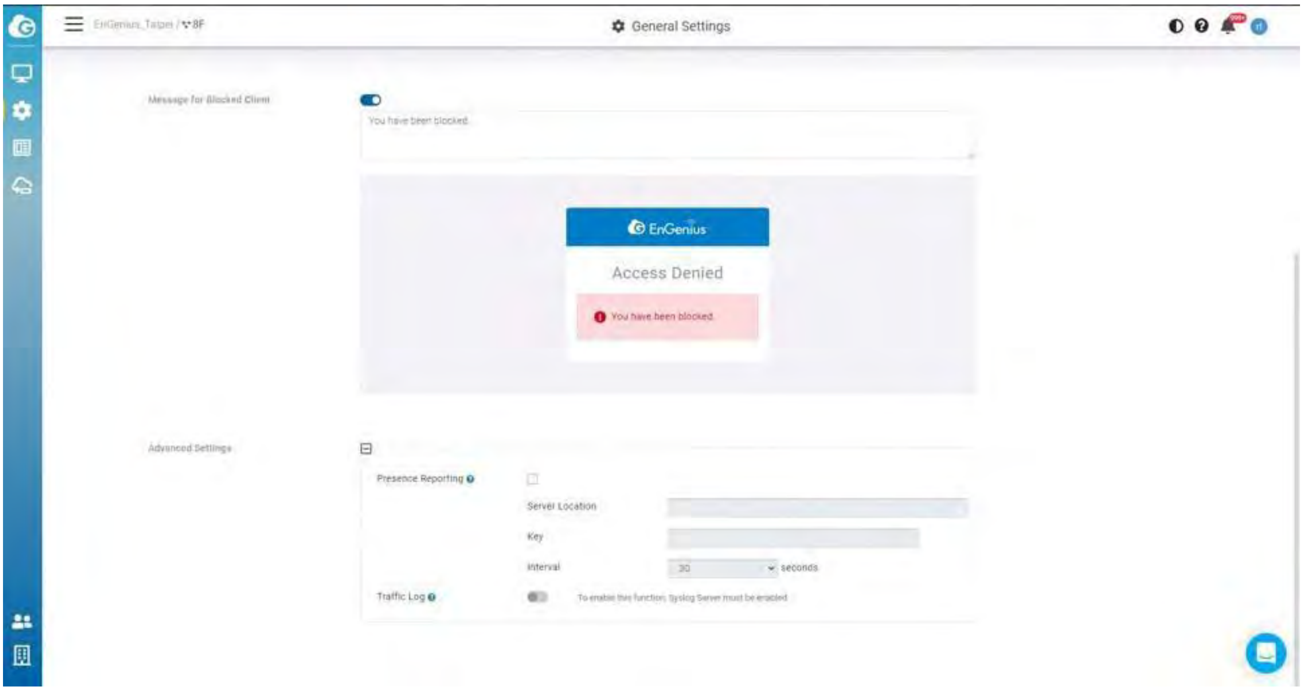
For applications like CRM tools, presence analytics, or location-aware services which need to continuously gather presence data of wireless clients, EnGenius Cloud Acess Points are capable of delivering real-time presence data to fulfill the requirement.

EnGenius Presence Service can have cloud-managed APs continuously gathering 802.11 probe request frames sent by wireless clients and then sending the data to 3rd party servers configured in EnGenius Cloud.

Configuration

In EnGeniusCloud, the configuration of presence service is at

> General Settings > AP > Advanced Settings



Message for Blocked Client

You have been blocked

Access Denied

You have been blocked

Advanced Settings

Presence Reporting □

Server Location

Key

Interval 30 seconds

Traffic Log

To enable this function, Syslog Server must be enabled

the following parameters can be configured on the page:

Parameters	Description
Server Location	3rd party server address
Key	Secret used to generate a SHA256 HMAC signature, over the payload (the JSON message). The signature is then added to a custom HTTP header ("Signature") in the POST message.
Interval	The Interval between two consecutive messages has been sent.

Traffic log

Traffic log feeds wireless client info to remote Syslog server. Note that enabling this setting will severely degrade AP performance. To enable this function, the syslog server must be enabled.

Remote System Log

The Remote System Log gives you the capability to remotely log Syslog events from a device on EnGenius Cloud to your external logging server.

You can enable and configure the remote logging feature from **Configure** → General setting→ Syslog server.

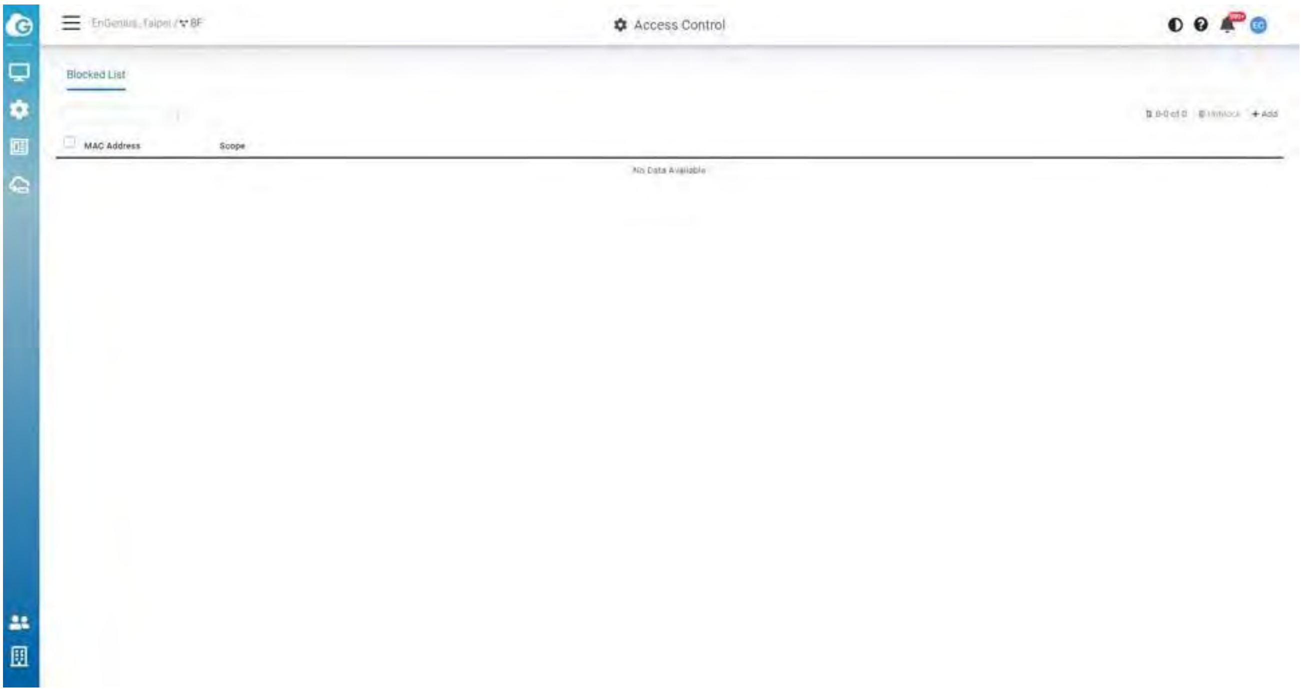
- Status: Enable to open the function to the remote system log.
- Log server address: Specify the IP address or hostname of the Syslog server.
- Log server port: Specify the port of the Syslog server. The default port is 514.

Access Control

In some cases, it is necessary to block a specific client on a network. This configuration will apply to the whole network and will affect the client immediately.

Blocked List

Navigate to **Configure** > Access Control to access this screen.



You could block clients in the current network or on SSID basis depending on your requirement. This blocked list displays which you added the blocked clients in SSID > Access Control and Manage > Clients . So you could manage whole blocked clients easily in single lists. Noted that there is a limit of 1000 clients for blocking.

How to block clients

1. Click Add in the top-right corner .

2. Enter the Mac Address , select the Scope (Current Network or SSID basis) , then click Apply

How to Unblock clients

1. Select the clients on the lists

2. Click Unblock

VIP Lists

All VIP clients can bypass Captive portal. Wired VIP client can bypass L2 isolation .

If wireless printer/scanner/IoT to be accessible, pls make sure the wireless printer/scanner/IoT devices are under SSID of

- Bridge mode
- L2 Isolation is disabled
- Optional: If captive portal is enabled on the SSID, the “VIP” can let the IoT skip captive portal entry

If wired printer / scanner / IoT device to be accessible, then

- Make the devices be “VIP” to all SSID’s (or to the SSID’s for the wireless clients to be able to access)
- Any wireless client can access. No matter if NAT/Bridge mode. L2 Isolation can be enabled / disabled

You could add the VIP clients in the current network or on SSID basis depending on your requirement. This VIP list displays which you added the VIP clients in SSID > Access Control and Manage > Clients . So you could manage whole VIP clients easily in single lists. Noted that there is a limit of 50 clients for VIP.

How to Add VIP clients

1. Click Add in the top-right corner .

2. Enter the Mac Address , select the Scope (Current Network or SSID basis) , then click Apply

How to remove VIP clients

1. Select the clients on the lists

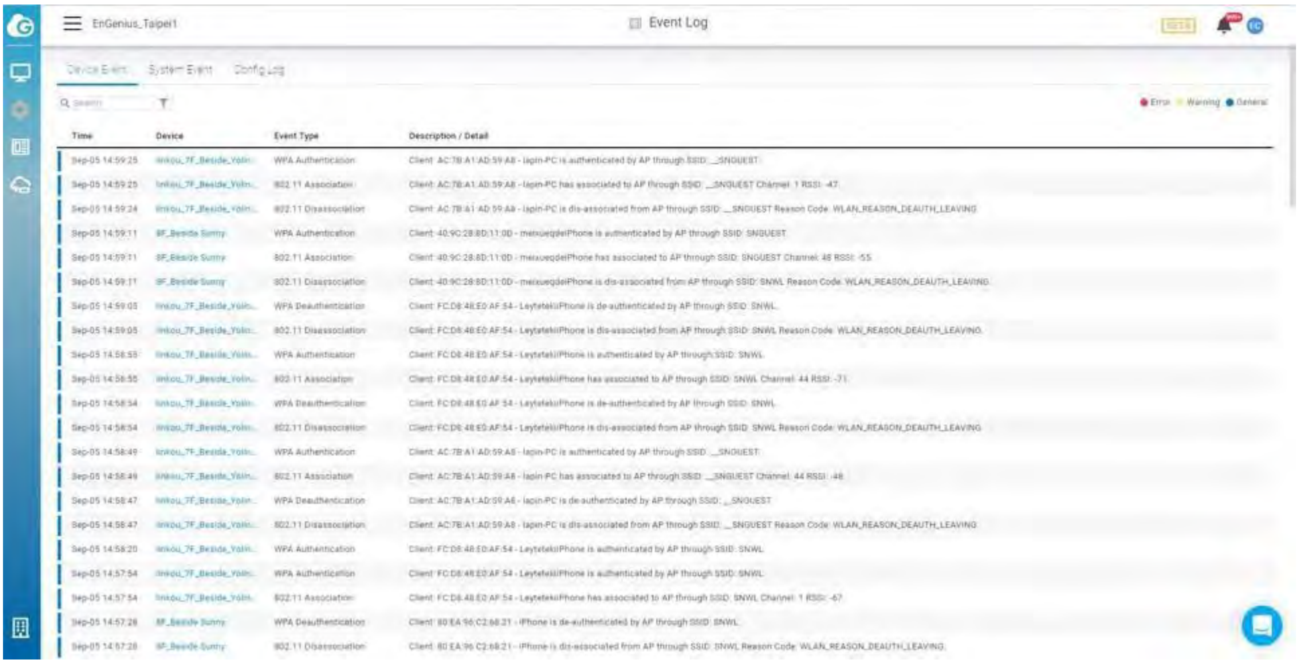
2. Click Delete

Device Events

Device events are events that are specific to individual devices, and are logged to EnGenius Cloud. Examples of events would include the specific time that a device comes online or goes offline.

Use this screen to view Device Events.

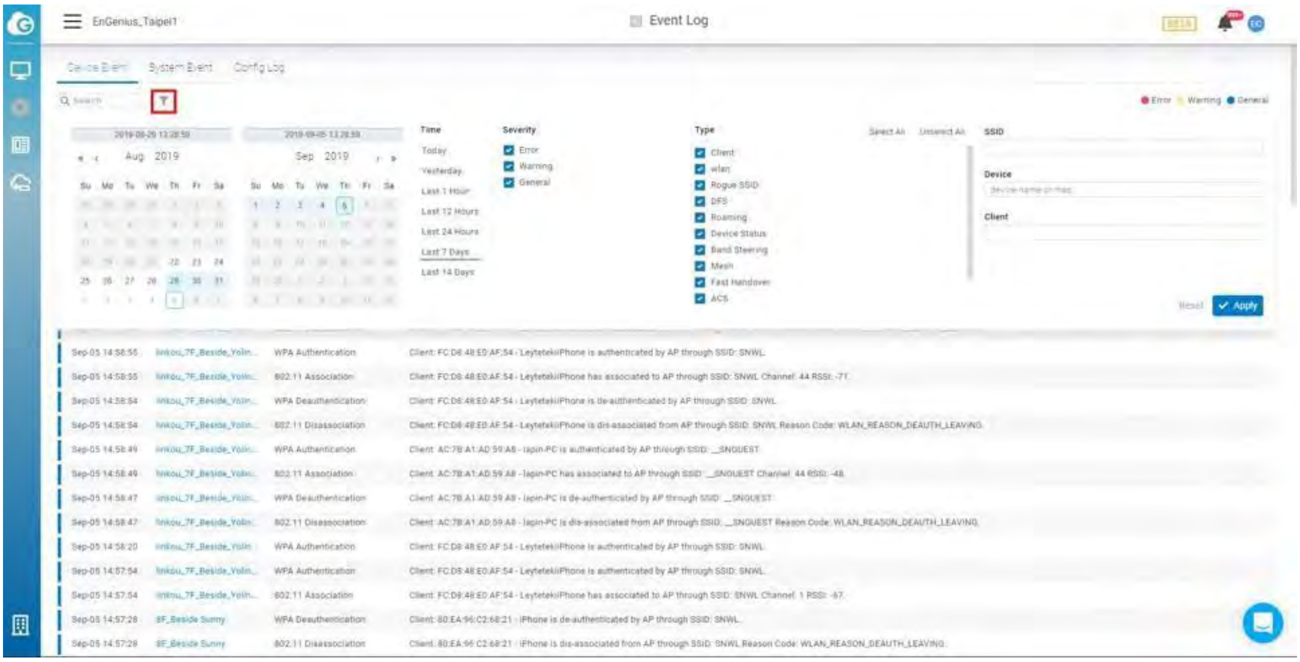
Click Analyze > Event Log > Device Event to access this screen.



Time	Device	Event Type	Description / Detail
Sep-05 14:59:25	linkou_7F_Beside_Yoln...	WPA Authentication	Client: AC:7B:A1:AD:59:A8 - lapin-PC is authenticated by AP through SSID: __SNGUEST
Sep-05 14:59:25	linkou_7F_Beside_Yoln...	802.11 Association	Client: AC:7B:A1:AD:59:A8 - lapin-PC has associated to AP through SSID: __SNGUEST Channel: 1 RSSI: -47
Sep-05 14:59:24	linkou_7F_Beside_Yoln...	802.11 Disassociation	Client: AC:7B:A1:AD:59:A8 - lapin-PC is dis-associated from AP through SSID: __SNGUEST Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:59:11	8F_Beside Sunny	WPA Authentication	Client: 40:9C:28:8D:11:0D - meixueqdeiPhone is authenticated by AP through SSID: SNGUEST
Sep-05 14:59:11	8F_Beside Sunny	802.11 Association	Client: 40:9C:28:8D:11:0D - meixueqdeiPhone has associated to AP through SSID: SNGUEST Channel: 48 RSSI: -55
Sep-05 14:59:11	8F_Beside Sunny	802.11 Disassociation	Client: 40:9C:28:8D:11:0D - meixueqdeiPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:59:05	linkou_7F_Beside_Yoln...	WPA Deauthentication	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is de-authenticated by AP through SSID: SNWL
Sep-05 14:59:05	linkou_7F_Beside_Yoln...	802.11 Disassociation	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:58:55	linkou_7F_Beside_Yoln...	WPA Authentication	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:58:55	linkou_7F_Beside_Yoln...	802.11 Association	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone has associated to AP through SSID: SNWL Channel: 44 RSSI: -71
Sep-05 14:58:54	linkou_7F_Beside_Yoln...	WPA Deauthentication	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is de-authenticated by AP through SSID: SNWL
Sep-05 14:58:54	linkou_7F_Beside_Yoln...	802.11 Disassociation	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:58:49	linkou_7F_Beside_Yoln...	WPA Authentication	Client: AC:7B:A1:AD:59:A8 - lapin-PC is authenticated by AP through SSID: __SNGUEST
Sep-05 14:58:49	linkou_7F_Beside_Yoln...	802.11 Association	Client: AC:7B:A1:AD:59:A8 - lapin-PC has associated to AP through SSID: __SNGUEST Channel: 44 RSSI: -48
Sep-05 14:58:47	linkou_7F_Beside_Yoln...	WPA Deauthentication	Client: AC:7B:A1:AD:59:A8 - lapin-PC is de-authenticated by AP through SSID: __SNGUEST
Sep-05 14:58:47	linkou_7F_Beside_Yoln...	802.11 Disassociation	Client: AC:7B:A1:AD:59:A8 - lapin-PC is dis-associated from AP through SSID: __SNGUEST Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:58:20	linkou_7F_Beside_Yoln...	WPA Authentication	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:57:54	linkou_7F_Beside_Yoln...	WPA Authentication	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:57:54	linkou_7F_Beside_Yoln...	802.11 Association	Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone has associated to AP through SSID: SNWL Channel: 1 RSSI: -67
Sep-05 14:57:28	8F_Beside Sunny	WPA Deauthentication	Client: 80:EA:96:C2:68:21 - iPhone is de-authenticated by AP through SSID: SNWL
Sep-05 14:57:28	8F_Beside Sunny	802.11 Disassociation	Client: 80:EA:96:C2:68:21 - iPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING

Searching the Event Log

EnGenius Cloud allows to search device events based on a number of desired parameters.



```
Sep-05 14:58:55   linkou_7F_Beside_Yolin...   WPA Authentication        Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:58:55   linkou_7F_Beside_Yolin...   802.11 Association        Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone has associated to AP through SSID: SNWL Channel: 44 RSSI: -71
Sep-05 14:58:54   linkou_7F_Beside_Yolin...   WPA Deauthentication      Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is de-authenticated by AP through SSID: SNWL
Sep-05 14:58:54   linkou_7F_Beside_Yolin...   802.11 Disassociation     Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:58:49   linkou_7F_Beside_Yolin...   WPA Authentication        Client: AC:7B:A1:AD:59:A8 - lapin-PC is authenticated by AP through SSID: __SNGUEST
Sep-05 14:58:49   linkou_7F_Beside_Yolin...   802.11 Association        Client: AC:7B:A1:AD:59:A8 - lapin-PC has associated to AP through SSID: __SNGUEST Channel: 44 RSSI: -48
Sep-05 14:58:47   linkou_7F_Beside_Yolin...   WPA Deauthentication      Client: AC:7B:A1:AD:59:A8 - lapin-PC is de-authenticated by AP through SSID: __SNGUEST
Sep-05 14:58:47   linkou_7F_Beside_Yolin...   802.11 Disassociation     Client: AC:7B:A1:AD:59:A8 - lapin-PC is dis-associated from AP through SSID: __SNGUEST Reason Code: WLAN_REASON_DEAUTH_LEAVING
Sep-05 14:58:20   linkou_7F_Beside_Yolin      WPA Authentication        Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:57:54   linkou_7F_Beside_Yolin...   WPA Authentication        Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone is authenticated by AP through SSID: SNWL
Sep-05 14:57:54   linkou_7F_Beside_Yolin...   802.11 Association        Client: FC:D8:48:E0:AF:54 - LeytetekiiPhone has associated to AP through SSID: SNWL Channel: 1 RSSI: -67
Sep-05 14:57:28   8F_Beside Sunny             WPA Deauthentication      Client: 80:EA:96:C2:68:21 - iPhone is de-authenticated by AP through SSID: SNWL
Sep-05 14:57:28   8F_Beside Sunny             802.11 Disassociation     Client: 80:EA:96:C2:68:21 - iPhone is dis-associated from AP through SSID: SNWL Reason Code: WLAN_REASON_DEAUTH_LEAVING
```

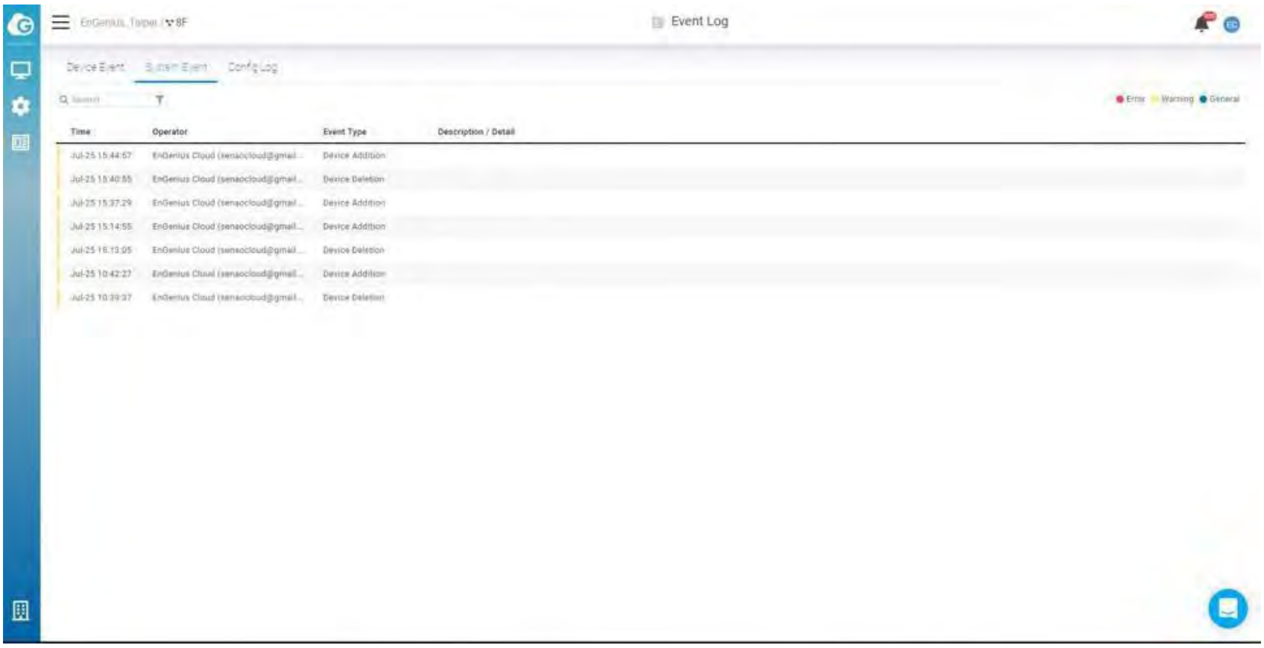
You can specify date/time, severity, and other parameters. Select one or multiple event types, then enter the SSID, device name/MAC, or select client to display the log messages related to it. After customizing your search parameters, remember to click Apply to perform the search.

System Events

System events are events related to EnGenius Cloud itself, such as device management or user management.

Use this screen to view system events. You can specify date/time and severity, then select one or multiple event types. Enter the operator name to display the log messages related to it.

Click Analyze > Event Log > System Events to access this screen.



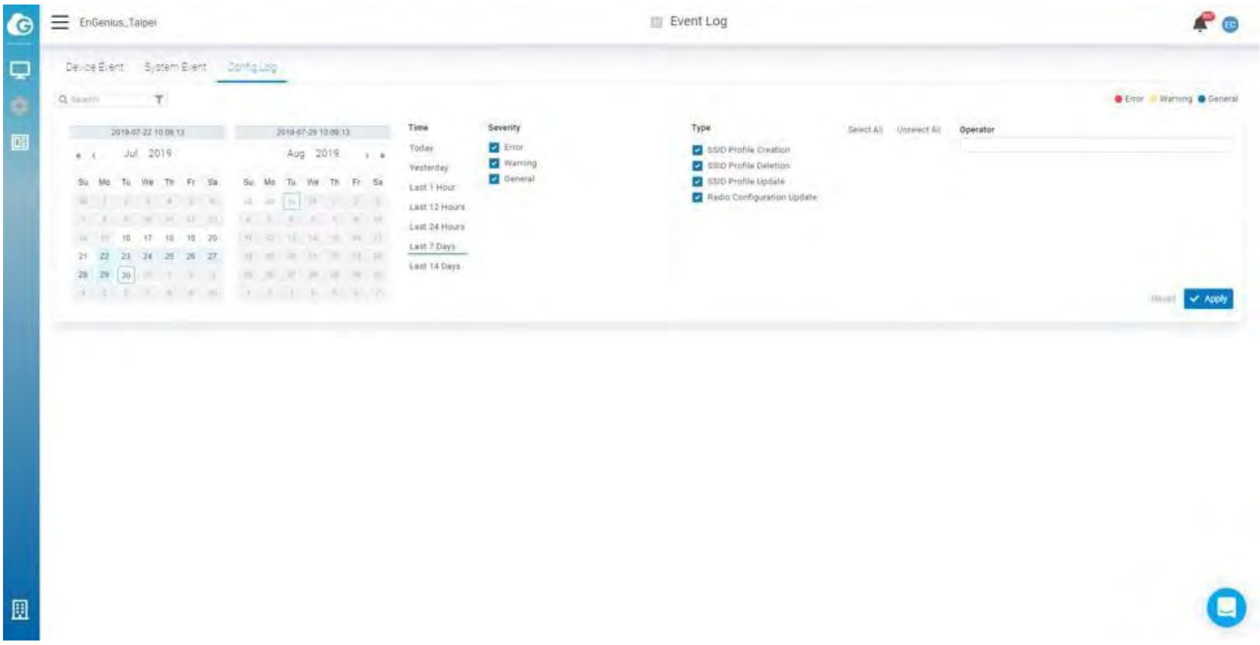
Time	Operator	Event Type	Description / Detail
Jul-25 15:44:57	EnGenius Cloud (senaocloud@gmail...	Device Addition	
Jul-25 15:40:55	EnGenius Cloud (senaocloud@gmail...	Device Deletion	
Jul-25 15:37:29	EnGenius Cloud (senaocloud@gmail...	Device Addition	
Jul-25 15:14:55	EnGenius Cloud (senaocloud@gmail...	Device Addition	
Jul-25 15:13:05	EnGenius Cloud (senaocloud@gmail...	Device Deletion	
Jul-25 10:42:27	EnGenius Cloud (senaocloud@gmail...	Device Addition	
Jul-25 10:39:37	EnGenius Cloud (senaocloud@gmail...	Device Deletion	

Config Logs

Config logs capture events based on your configuration changes, such as changes to SSID settings, radio settings, or network updates.

Use this screen to view config logs. you can specify date/time, severity, select one or multiple event types, and enter the operator name to display the log messages related to it.

Click Analyze > Event Log > **Config** Log to access this screen.



2019-07-22 10:09:13 – 2019-07-29 10:09:13

Time: Today, Yesterday, Last 1 Hour, Last 12 Hours, Last 24 Hours, Last 7 Days, Last 14 Days

Severity: ☑ Error ☑ Warning ☑ General

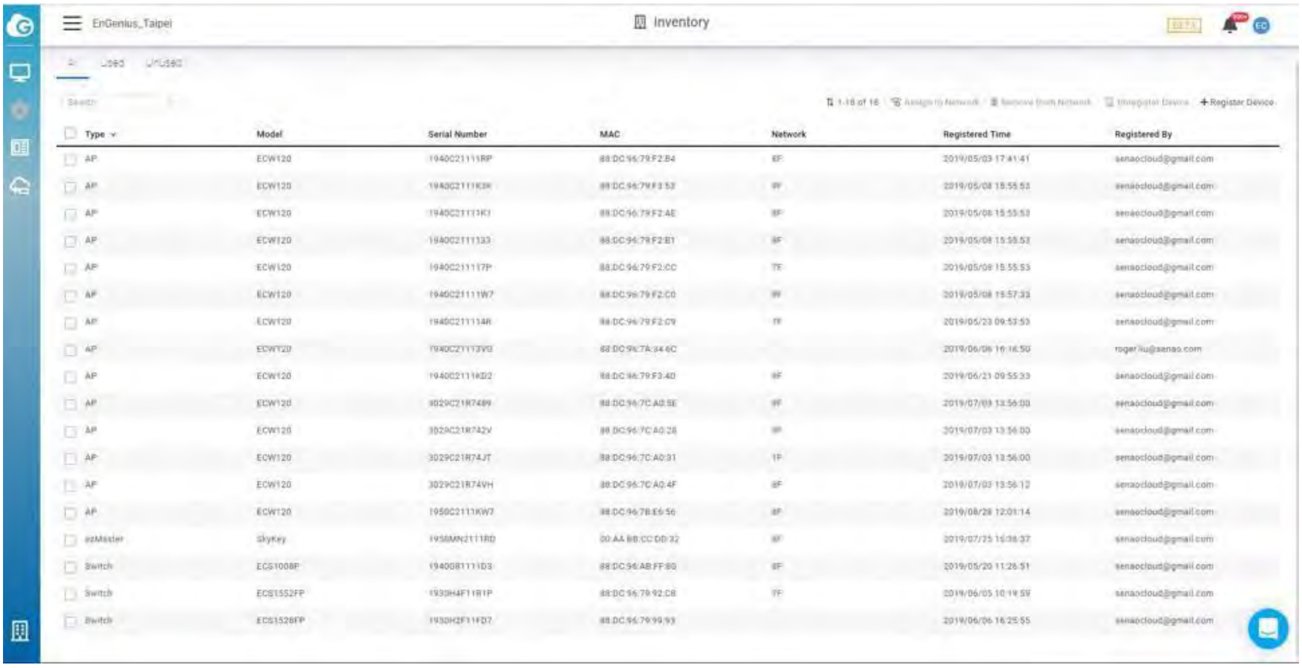
Type: ☑ SSID Profile Creation ☑ SSID Profile Deletion ☑ SSID Profile Update ☑ Radio Configuration Update

Operator:

Managing Device Inventory and Licence

The Inventory page lists all devices currently found in the inventory or added to a network within the current organization. The Inventory page contains the following information about each device:

- Type: type of the device.
- Model: model name of the device.
- Serial Number: serial number of the device.
- MAC: MAC address of the device.
- Network: the network that the device has been added to.
- Register Time: time of the device's addition to the inventory.
- Register by: user responsible for adding the device to the inventory.

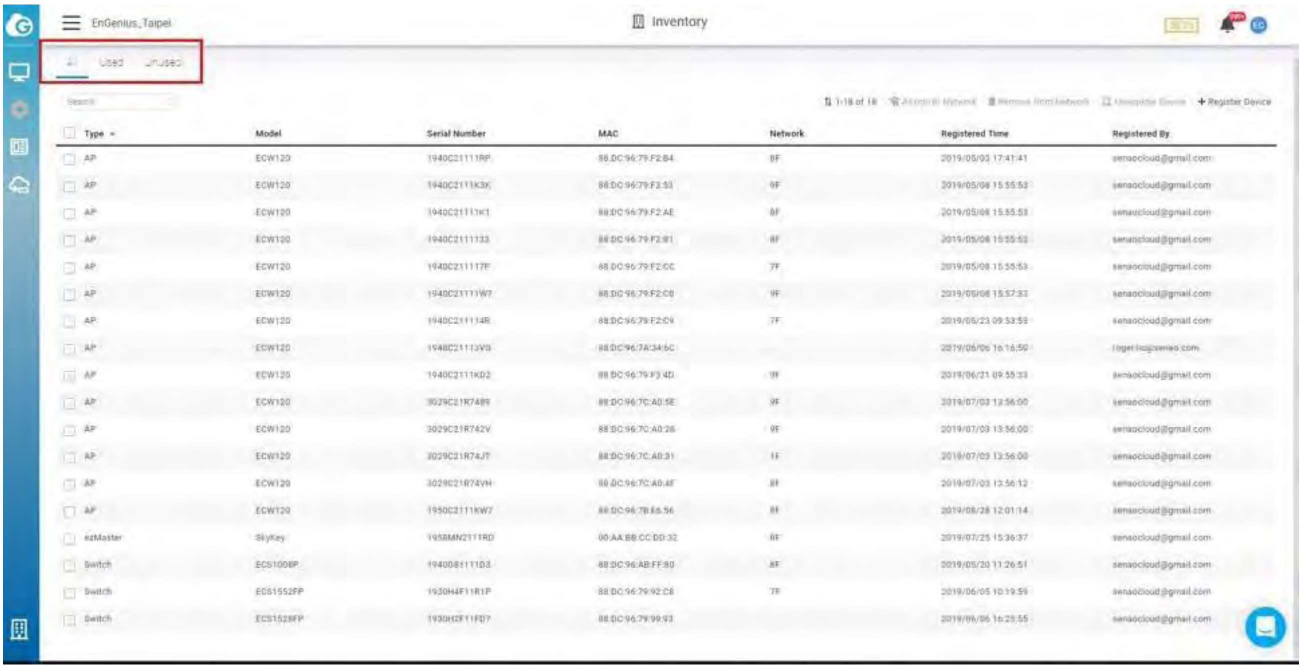


□ Type ▾	Model	Serial Number	MAC	Network	Registered Time	Registered By
□ AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	6F	2019/05/03 17:41:41	senaocloud@gmail.com
□ AP	ECW120	1940C2111K3R	88:DC:96:79:F3:53	9F	2019/05/08 15:55:53	senaocloud@gmail.com
□ AP	ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019/05/08 15:55:53	senaocloud@gmail.com
□ AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019/05/08 15:55:53	senaocloud@gmail.com
□ AP	ECW120	1940C211117P	88:DC:96:79:F2:CC	7F	2019/05/08 15:55:53	senaocloud@gmail.com
□ AP	ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019/05/08 15:57:33	senaocloud@gmail.com
□ AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019/05/23 09:53:53	senaocloud@gmail.com
□ AP	ECW120	1940C21113VG	68:DC:96:7A:34:6C		2019/06/06 16:16:50	roger.liu@senao.com
□ AP	ECW120	1940C2111KD2	88:DC:96:79:F3:40	8F	2019/06/21 09:55:33	senaocloud@gmail.com
□ AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019/07/03 13:56:00	senaocloud@gmail.com
□ AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019/07/03 13:56:00	senaocloud@gmail.com
□ AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019/07/03 13:56:00	senaocloud@gmail.com
□ AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019/07/03 13:56:12	senaocloud@gmail.com
□ AP	ECW120	1950C2111KW7	88:DC:96:7B:E6:56	8F	2019/08/28 12:01:14	senaocloud@gmail.com
□ ezMaster	SkyKey	1958MN2111RD	00:AA:BB:CC:DD:32	8F	2019/07/25 15:38:37	senaocloud@gmail.com
□ Switch	ECS1008P	1940G81111D3	88:DC:96:AB:FF:80	8F	2019/05/20 11:26:51	senaocloud@gmail.com
□ Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019/06/05 10:19:59	senaocloud@gmail.com
□ Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019/06/06 16:25:55	senaocloud@gmail.com

There are also tabs to filter the list based on whether devices are:

- Used: Currently added to a network.
- Unused: Registered, but not in a network.
- All: Lists all registered devices, regardless of whether they are in a network.

Click Organization > Inventory to access this screen.



EnGenius_Taipei

Inventory

All | Used | Unused

Search

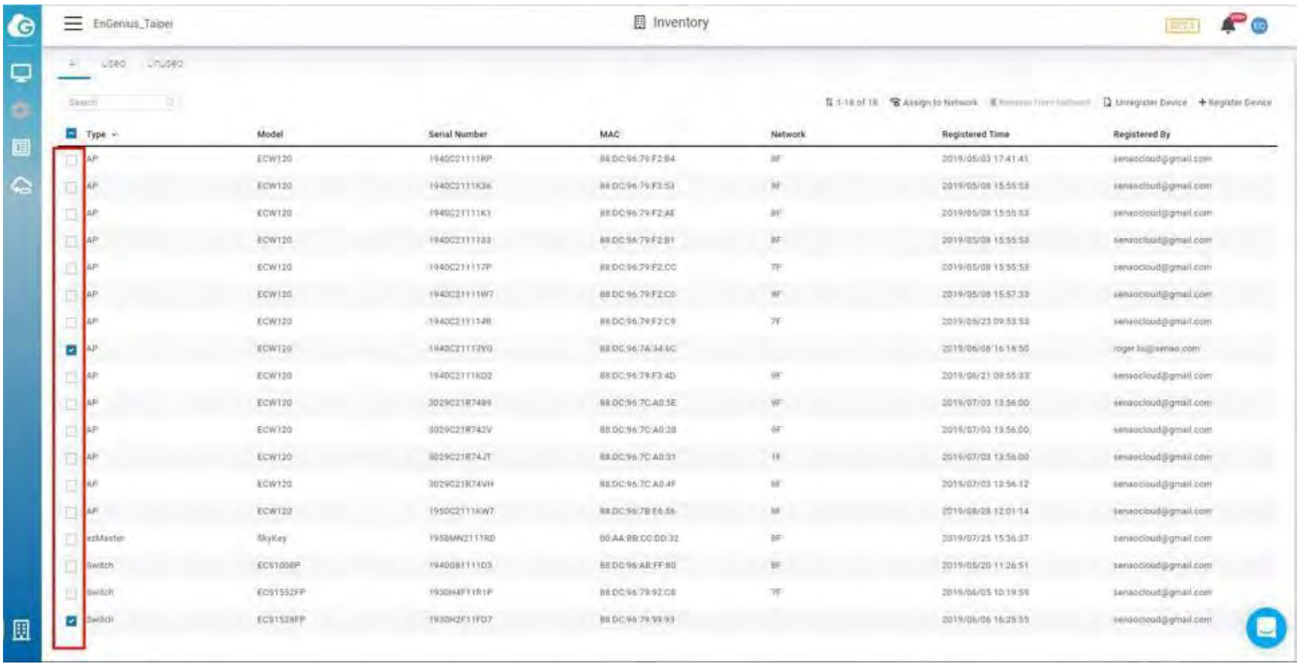
1-18 of 18 | Assign to Network | Remove from Network | Unregister Device | + Register Device

☐ Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
☐ AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019/05/03 17:41:41	senaocloud@gmail.com
☐ AP	ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C211117F	88:DC:96:79:F2:CC	7F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C21111W7	88:DC:96:79:F2:C8	9F	2019/05/08 15:57:33	senaocloud@gmail.com
☐ AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019/05/23 09:53:59	senaocloud@gmail.com
☐ AP	ECW120	1940C21113VG	88:DC:96:7A:34:6C		2019/06/06 16:16:50	roger.lio@senao.com
☐ AP	ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019/06/21 09:55:33	senaocloud@gmail.com
☐ AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019/07/03 13:56:12	senaocloud@gmail.com
☐ AP	ECW120	1950C2111KW7	88:DC:96:7B:E6:56	8F	2019/08/28 12:01:14	senaocloud@gmail.com
☐ ezMaster	SkyKey	1958MN2111RD	00:AA:BB:CC:DD:32	8F	2019/07/25 15:36:37	senaocloud@gmail.com
☐ Switch	ECS1008P	1940081111D3	88:DC:96:AB:FF:80	8F	2019/05/20 11:26:51	senaocloud@gmail.com
☐ Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019/06/05 10:19:59	senaocloud@gmail.com
☐ Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019/06/06 16:25:55	senaocloud@gmail.com

Assigning Devices to a Network

This feature helps the users in assigning devices to a network.

1. Navigate to the inventory page.
2. Select one or multiple devices as per your requirements.



EnGenius_Taipei

Inventory

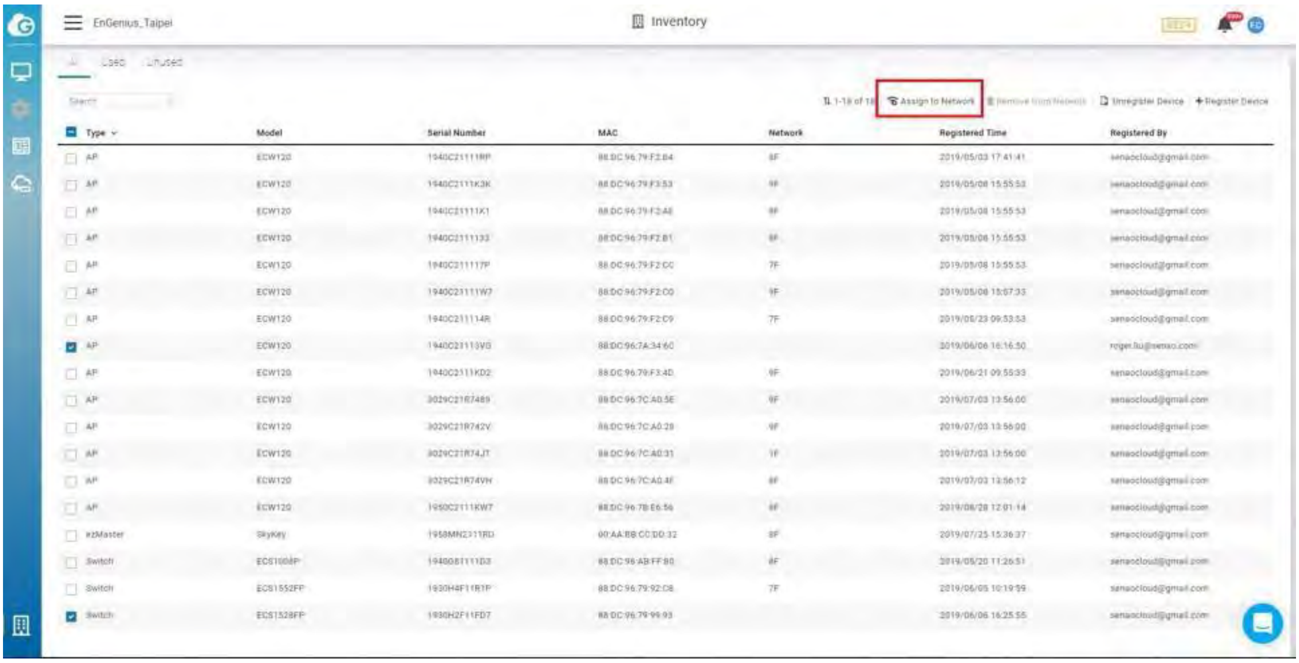
All | Used | Unused

Search

1-18 of 18 | Assign to Network | Remove from Network | Unregister Device | + Register Device

☐ Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
☐ AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019/05/03 17:41:41	senaocloud@gmail.com
☐ AP	ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C21111K1	88:DC:96:79:F2:AE	8F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C211117F	88:DC:96:79:F2:CC	7F	2019/05/08 15:55:53	senaocloud@gmail.com
☐ AP	ECW120	1940C21111W7	88:DC:96:79:F2:C8	9F	2019/05/08 15:57:33	senaocloud@gmail.com
☐ AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019/05/23 09:53:59	senaocloud@gmail.com
☑ AP	ECW120	1940C21113VG	88:DC:96:7A:34:6C		2019/06/06 16:16:50	roger.lio@senao.com
☐ AP	ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019/06/21 09:55:33	senaocloud@gmail.com
☐ AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019/07/03 13:56:00	senaocloud@gmail.com
☐ AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019/07/03 13:56:12	senaocloud@gmail.com
☐ AP	ECW120	1950C2111KW7	88:DC:96:7B:E6:56	8F	2019/08/28 12:01:14	senaocloud@gmail.com
☐ ezMaster	SkyKey	1958MN2111RD	00:AA:BB:CC:DD:32	8F	2019/07/25 15:36:37	senaocloud@gmail.com
☐ Switch	ECS1008P	1940081111D3	88:DC:96:AB:FF:80	8F	2019/05/20 11:26:51	senaocloud@gmail.com
☐ Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019/06/05 10:19:59	senaocloud@gmail.com
☑ Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019/06/06 16:25:55	senaocloud@gmail.com

3. Click Assign to Network.



	Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
□	AP	ECW120	1940C21111RP	88:DC:96:79:F2:84	8F	2019/05/03 17:41:41	senaocloud@gmail.com
□	AP	ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019/05/08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111K1	88:DC:96:79:F2:A8	9F	2019/05/08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019/05/08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C211117P	88:DC:96:79:F2:CC	7F	2019/05/08 15:55:53	senaocloud@gmail.com
□	AP	ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019/05/08 15:57:33	senaocloud@gmail.com
□	AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019/05/23 09:53:53	senaocloud@gmail.com
☑	AP	ECW120	1940C21113VG	88:DC:96:7A:34:60		2019/06/06 16:16:50	roger.liu@senao.com
□	AP	ECW120	1940C2111KD2	88:DC:96:79:F3:4D	9F	2019/06/21 09:55:33	senaocloud@gmail.com
□	AP	ECW120	3029C21R7489	88:DC:96:7C:A0:5E	9F	2019/07/03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R742V	88:DC:96:7C:A0:28	9F	2019/07/03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74JT	88:DC:96:7C:A0:31	1F	2019/07/03 13:56:00	senaocloud@gmail.com
□	AP	ECW120	3029C21R74VH	88:DC:96:7C:A0:4F	8F	2019/07/03 13:56:12	senaocloud@gmail.com
□	AP	ECW120	1950C2111KW7	88:DC:96:7B:E6:56	8F	2019/06/28 12:01:14	senaocloud@gmail.com
□	ezMaster	SkyKey	1958MN2311RD	00:AA:BB:CC:DD:32	8F	2019/07/25 15:36:37	senaocloud@gmail.com
□	Switch	ECS1008P	1948G81111D3	88:DC:96:AB:FF:80	8F	2019/05/20 11:26:51	senaocloud@gmail.com
□	Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019/06/05 10:19:59	senaocloud@gmail.com
☑	Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019/06/06 16:25:55	senaocloud@gmail.com

Removing Devices from a Network

This feature allows for devices to be deleted in bulk from a network.

To delete devices using bulk delete:

1. Navigate to the inventory page.
2. Select one or multiple devices as per your requirements.
3. Click Remove from Network.

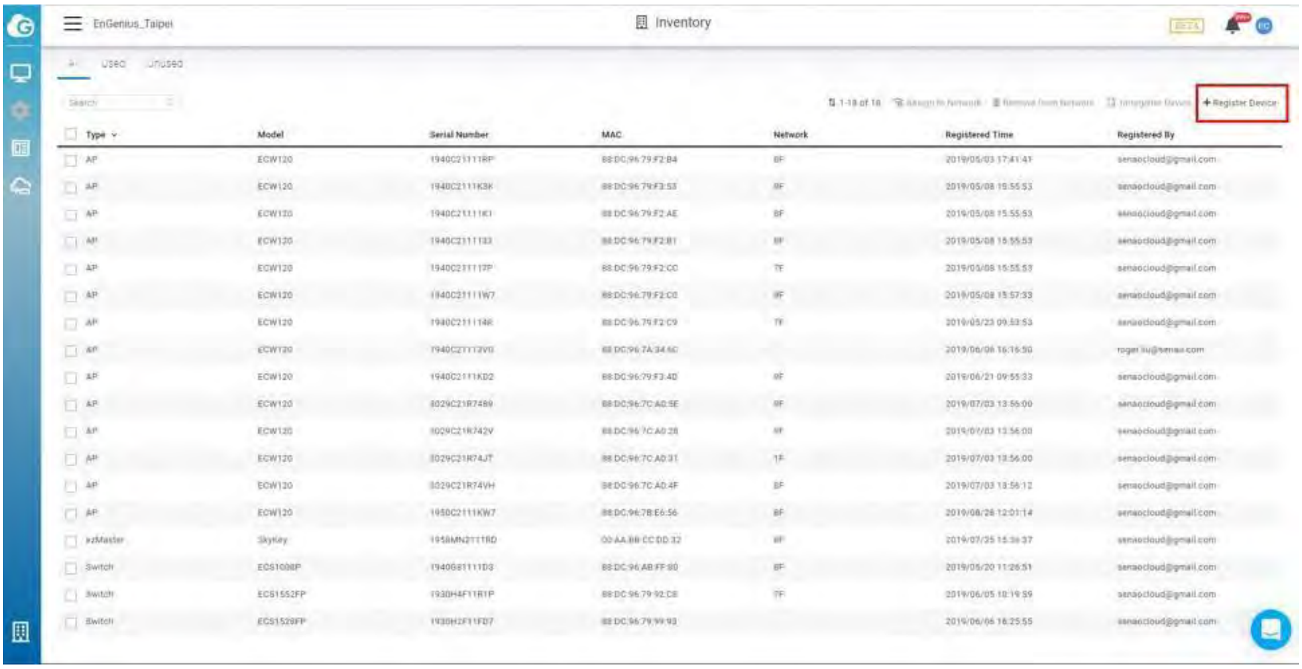
De-registering a Device from EnGenius Cloud

This feature allows you to remove registered devices from EnGenius Cloud inventory.

1. Navigate to the inventory page.
2. Select one or multiple devices as per your requirements.
3. Click De-Register Device.

Register a Device

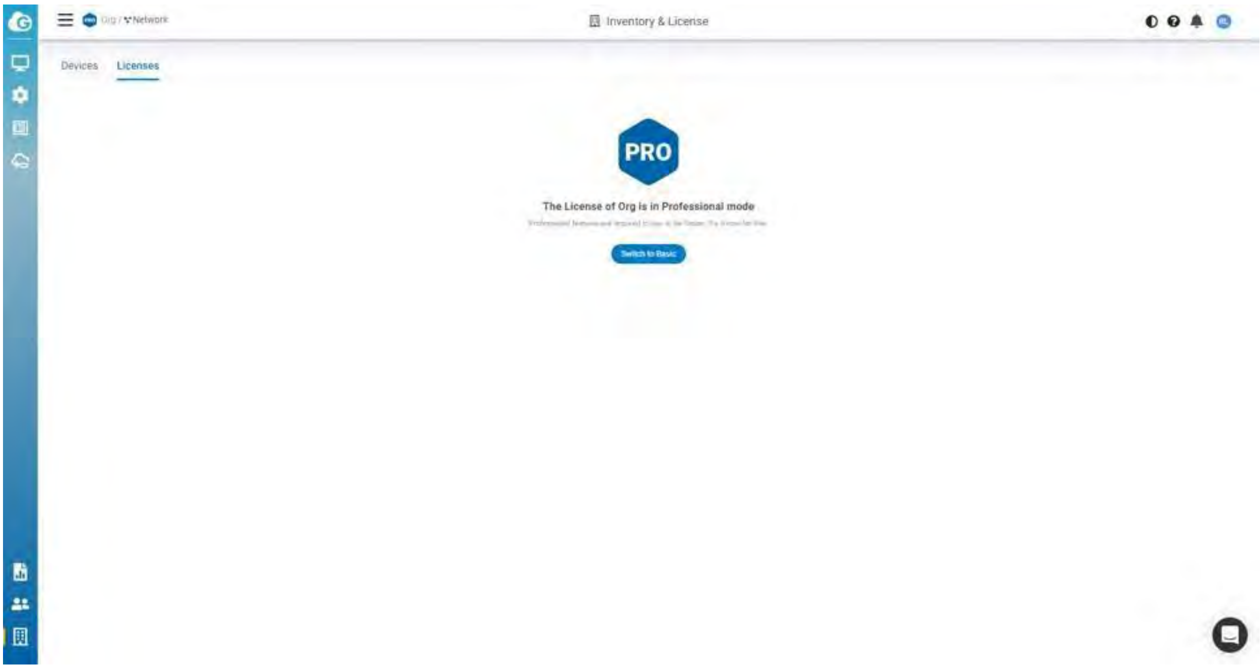
Registering devices onto EnGenius Cloud inventory is easy. Enter devices by their serial number, one per line, and click the Register button.



Type	Model	Serial Number	MAC	Network	Registered Time	Registered By
AP	ECW120	1940C21111RP	88:DC:96:79:F2:B4	8F	2019/05/03 17:41:41	senaocloud@gmail.com
AP	ECW120	1940C2111K3K	88:DC:96:79:F3:53	9F	2019/05/08 15:55:53	senaocloud@gmail.com
AP	ECW120	1940C21111KI	88:DC:96:79:F2:AE	8F	2019/05/08 15:55:53	senaocloud@gmail.com
AP	ECW120	1940C2111133	88:DC:96:79:F2:B1	8F	2019/05/08 15:55:53	senaocloud@gmail.com
AP	ECW120	1940C211117P	88:DC:96:79:F2:C0	7F	2019/05/08 15:55:53	senaocloud@gmail.com
AP	ECW120	1940C21111W7	88:DC:96:79:F2:C0	9F	2019/05/08 15:57:33	senaocloud@gmail.com
AP	ECW120	1940C211114R	88:DC:96:79:F2:C9	7F	2019/05/23 09:53:53	senaocloud@gmail.com
AP	ECW120	1940C21113V0	88:DC:96:7A:34:6C		2019/06/06 16:16:50	roger.liu@senao.com
AP	ECW120	1940C2111KD2	88:DC:96:79:F3:40	9F	2019/06/21 09:55:33	senaocloud@gmail.com
AP	ECW120	8029C21R7489	88:DC:96:7C:A0:5E	9F	2019/07/03 13:56:00	senaocloud@gmail.com
AP	ECW120	8029C21R742V	88:DC:96:7C:A0:28	9F	2019/07/03 13:56:00	senaocloud@gmail.com
AP	ECW120	8029C21R74JT	88:DC:96:7C:A0:31	1F	2019/07/03 13:56:00	senaocloud@gmail.com
AP	ECW120	8029C21R74VH	88:DC:96:7C:A0:4F	8F	2019/07/03 13:56:12	senaocloud@gmail.com
AP	ECW120	1950C2111KW7	88:DC:96:7B:E6:56	8F	2019/08/28 12:01:14	senaocloud@gmail.com
ezMaster	SkyKey	1958MN2111RD	00:AA:BB:CC:DD:32	8F	2019/07/25 15:39:37	senaocloud@gmail.com
Switch	ECS1008P	1940G81111D3	88:DC:96:AB:FF:80	8F	2019/05/20 11:26:51	senaocloud@gmail.com
Switch	ECS1552FP	1930H4F11R1P	88:DC:96:79:92:C8	7F	2019/06/05 10:19:59	senaocloud@gmail.com
Switch	ECS1528FP	1930H2F11FD7	88:DC:96:79:99:93		2019/06/06 16:25:55	senaocloud@gmail.com

License

Click "Switch to Pro" allows you to use the pro features . Professional features are required to pay in the future. Currently, there are free to use.

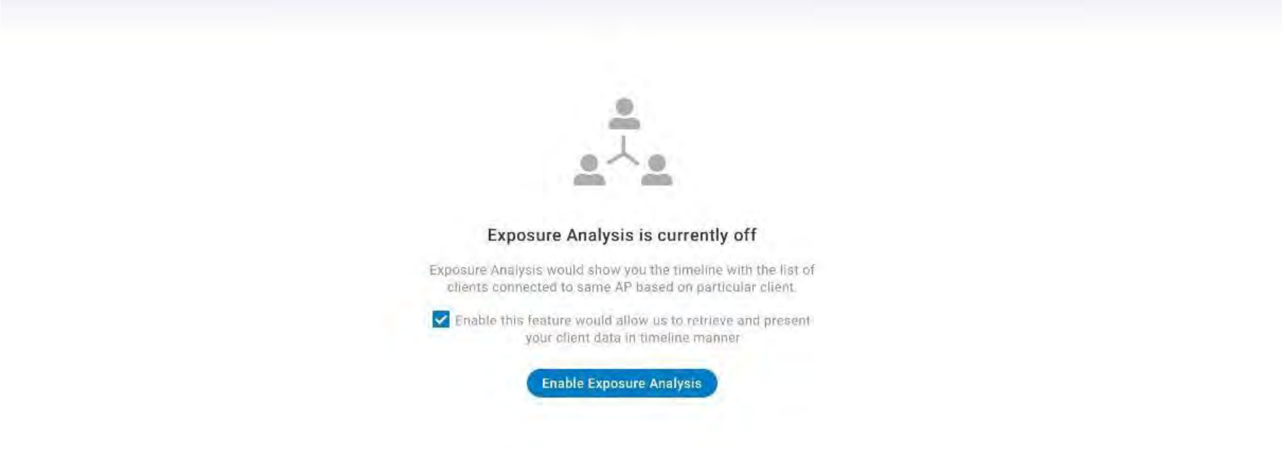


The License of Org is in Professional mode

[illegible]

Privacy

Exposure Analysis would show you the timeline with the list of clients connected to the same AP based on a particular client. If you enable this feature would allow us to retrieve and present your client data in a timeline manner. Click Organization > Privacy to access this screen.

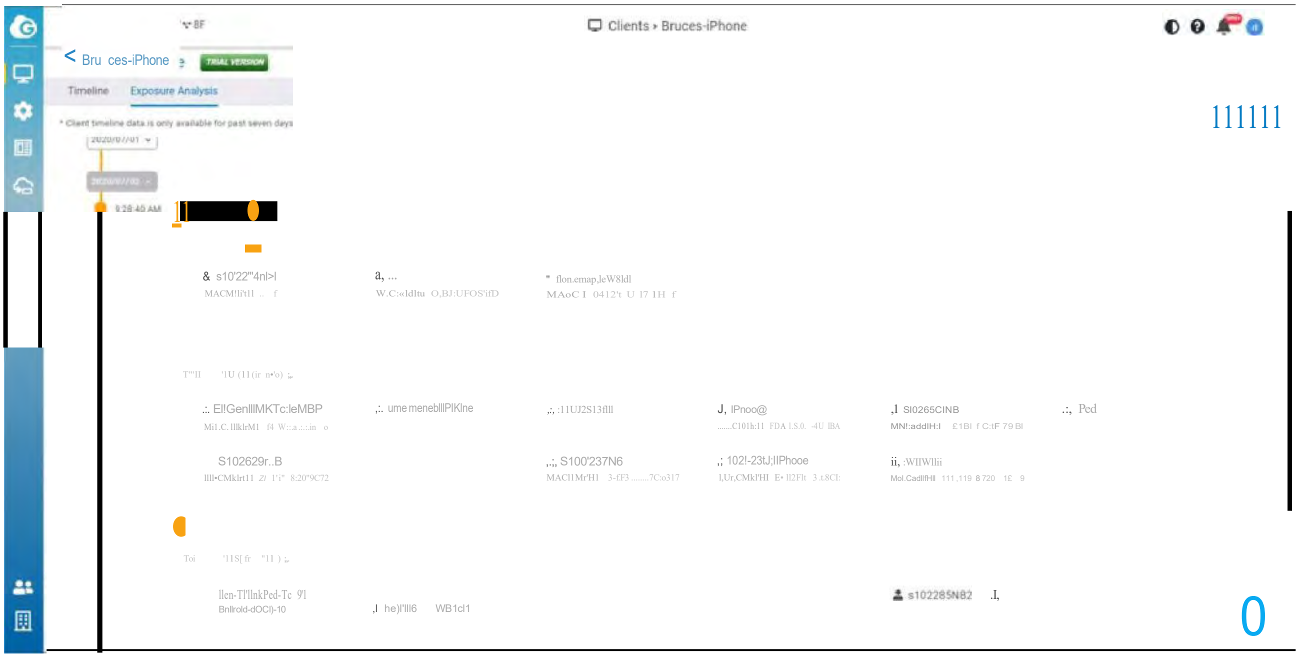


Exposure Analysis is currently off

Exposure Analysis would show you the timeline with the list of clients connected to same AP based on particular client

☑ Enable this feature would allow us to retrieve and present your client data in timeline manner

You can click Manage=> Clients to access this page to see the details after you enable the Exposure Analysis.



* Client timeline data is only available for past seven days

2020/07/01

2020/07/30

9:28:40 AM [redacted]

& s10'22"'4nl>l
MACM!li't11 .. f

a, ...
W.C:«ldltu O,BJ:UFOS'ifD

" flon.emap,leW8ldl
MAoC I 0412't U 17 1H f

T"'II '1U (11(ir n•'o) ;,

.:. El!GenlllMKTc:leMBP
Mi1.C. lllklrM1 f4 W::.a.:.:.in o

,:. ume menebllIPIKlne

,:, :11UJ2S13flll

J, IPnoo@
.......C101h:11 FDA l.S.0. -4U IBA

,l SI0265CINB
MN!:addIH:I £1BI f C:tF 79 BI

.:, Ped

S102629r..B
llll•CMklrt11 Zl 1'i" 8:20"9C72

,.:, S100'237N6
MACl1Mr'H1 3-£F3 ....7C:o317

,; 102!-23tJ;lIPhooe
l,Ur,CMkl'HI E• ll2Flt 3 .t.8CI:

ii, :WIIWllii
Mol.CadllfHll 111 ,119 8 720 1£ 9

Toi '11S[fr "11) ;,

llen-Tl'llnkPed-Tc 9'l
Bnllrold-dOCl)-10

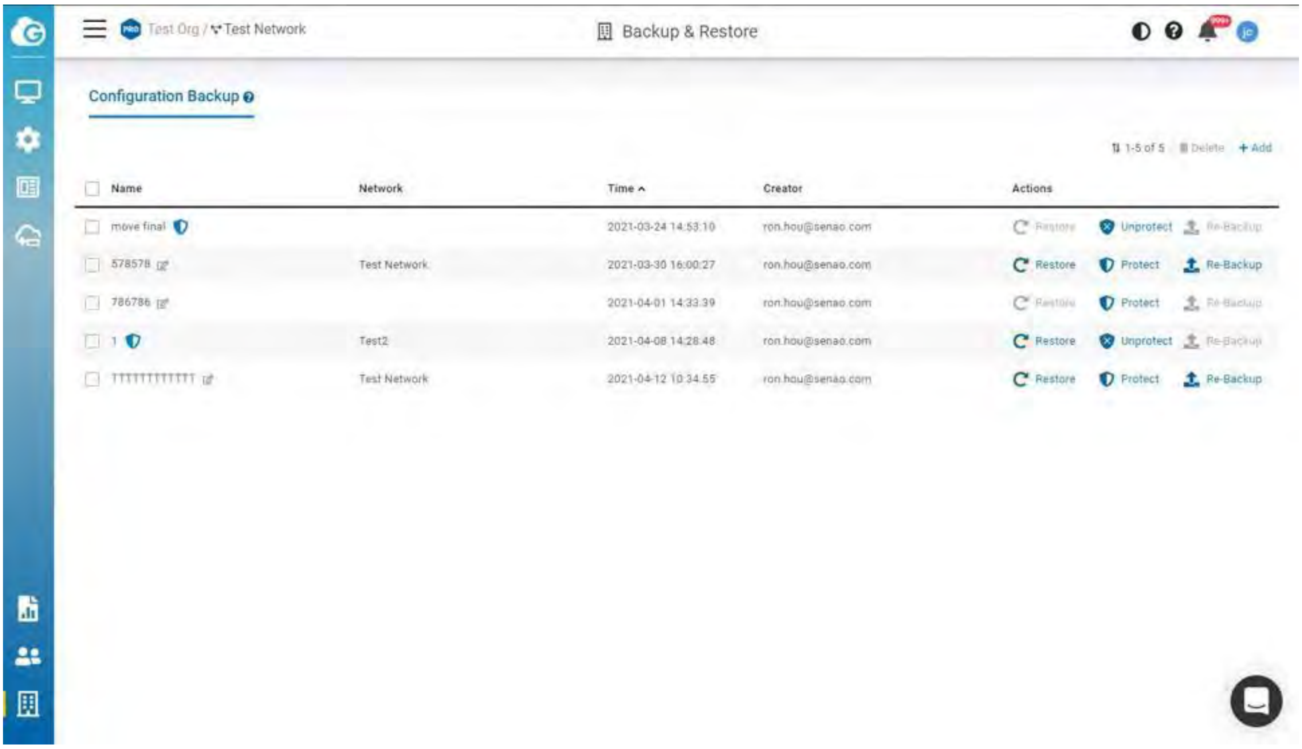
,l he)l'lll6 WB1cl1

s102285N82 .I,

Backup & Restore

Generating a New Backup

Users can create a new Network-wide setting and device backup by going to Organizations > Backup & Restore

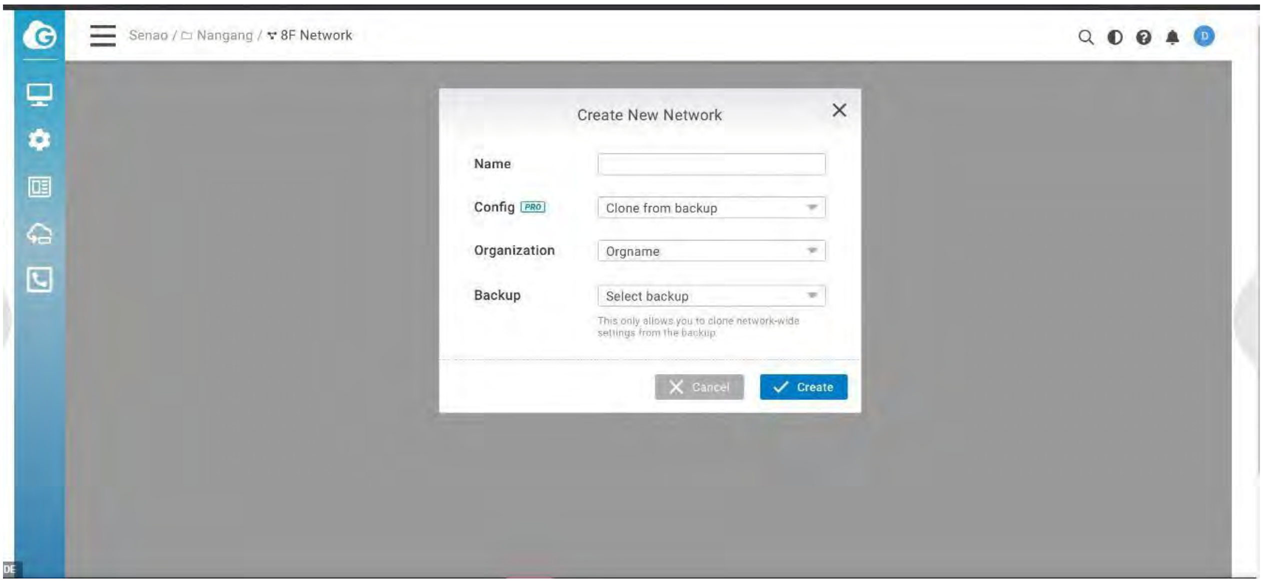


Name	Network	Time	Creator	Actions
move final		2021-03-24 14:53:10	ron.hou@senao.com	Restore Unprotect Re-Backup
578578	Test Network	2021-03-30 16:00:27	ron.hou@senao.com	Restore Protect Re-Backup
786786		2021-04-01 14:33:39	ron.hou@senao.com	Restore Protect Re-Backup
1	Test2	2021-04-08 14:28:48	ron.hou@senao.com	Restore Unprotect Re-Backup
TTTTTTTTTTTT	Test Network	2021-04-12 10:34:55	ron.hou@senao.com	Restore Protect Re-Backup

- Restore: This allows you to restore all settings(Network-wide settings and Devicesettings) to the corresponding network.
- Protect: This allows you to protect the backup, so the backup will not be rotated when you exceed 2 backups of the network.
- Re-Backup: This allows you to update the current settings to the backup of the corresponding network.

Clone Network

When creating a new network you have the option to clone the configuration from another network. This will copy all network-wide configurations from the existing network with the exception of local device configurations.



Create New Network

Name

Config PRO: Clone from backup

Organization: Orgname

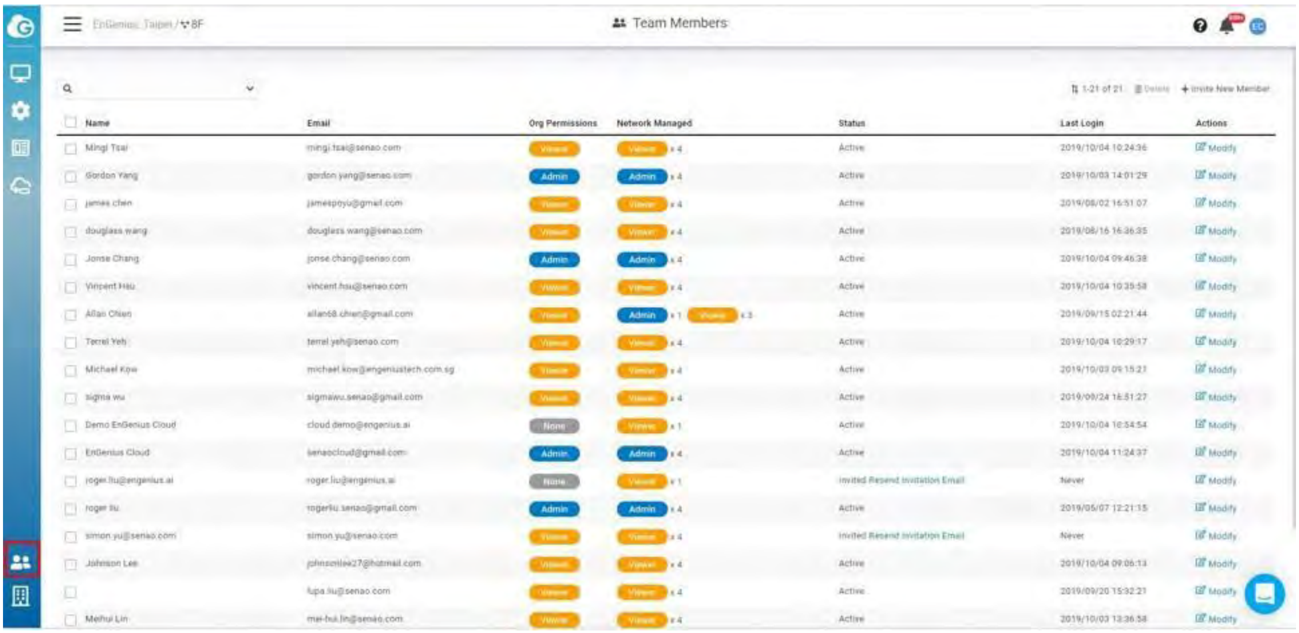
Backup: Select backup

This only allows you to clone network-wide settings from the backup

Managing Team Members

Use this screen to view, manage, and create user accounts for organization/network.

Click Team Member icon to access this screen.



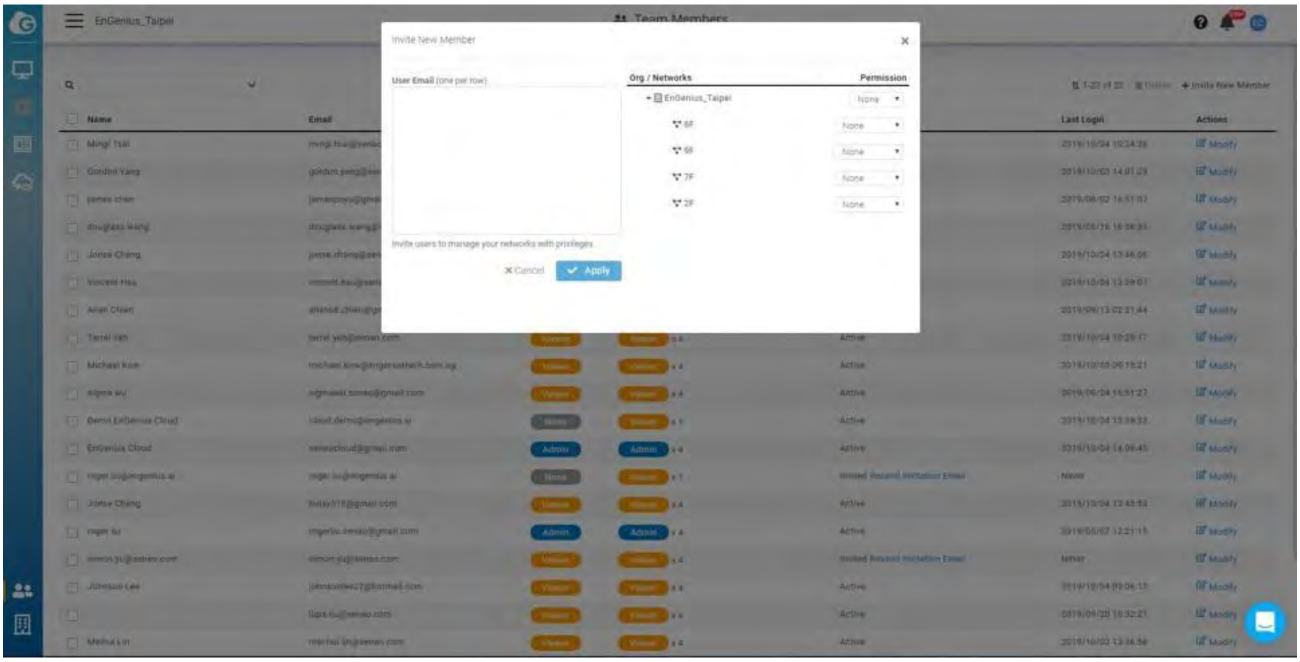
□	Name	Email	Org Permissions	Network Managed	Status	Last Login	Actions
□	Mingi Tsai	mingi.tsai@senao.com	Viewer	Viewer x 4	Active	2019/10/04 10:24:36	Modify
□	Gordon Yang	gordon.yang@senao.com	Admin	Admin x 4	Active	2019/10/03 14:01:29	Modify
□	james chen	jamespoyu@gmail.com	Viewer	Viewer x 4	Active	2019/08/02 16:51:07	Modify
□	douglass wang	douglass.wang@senao.com	Viewer	Viewer x 4	Active	2019/08/16 16:36:35	Modify
□	Jonse Chang	jonse.chang@senao.com	Admin	Admin x 4	Active	2019/10/04 09:46:38	Modify
□	Vincent Hsu	vincent.hsu@senao.com	Viewer	Viewer x 4	Active	2019/10/04 10:35:58	Modify
□	Allan Chien	allan68.chien@gmail.com	Viewer	Admin x 1 Viewer x 3	Active	2019/09/15 02:21:44	Modify
□	Terrel Yeh	terrel.yeh@senao.com	Viewer	Viewer x 4	Active	2019/10/04 10:29:17	Modify
□	Michael Kow	michael.kow@engeniustech.com.sg	Viewer	Viewer x 4	Active	2019/10/03 09:15:21	Modify
□	sigma wu	sigmawu.senao@gmail.com	Viewer	Viewer x 4	Active	2019/09/24 16:51:27	Modify
□	Demo EnGenius Cloud	cloud.demo@engenius.ai	None	Viewer x 1	Active	2019/10/04 10:54:54	Modify
□	EnGenius Cloud	senaocloud@gmail.com	Admin	Admin x 4	Active	2019/10/04 11:24:37	Modify
□	roger.liu@engenius.ai	roger.liu@engenius.ai	None	Viewer x 1	Invited Resend Invitation Email	Never	Modify
□	roger liu	rogerliu.senao@gmail.com	Admin	Admin x 4	Active	2019/05/07 12:21:15	Modify
□	simon.yu@senao.com	simon.yu@senao.com	Viewer	Viewer x 4	Invited Resend Invitation Email	Never	Modify
□	Johnson Lee	johnsonlee27@hotmail.com	Viewer	Viewer x 4	Active	2019/10/04 09:06:13	Modify
□		lupa.liu@senao.com	Viewer	Viewer x 4	Active	2019/09/20 15:32:21	Modify
□	Meihui Lin	mei-hui.lin@senao.com	Viewer	Viewer x 4	Active	2019/10/03 13:36:58	Modify

The Team Member page contains the following information about each member:

- Name : member name .
- Email : member email .
- Org Permissions : member's org permissions .
- Network Managed : Displayed numbers of member's network permissions , hovering on the permission badge will display the network .
- Status : Member account status . Active means member has completed the signup . Invited means invitation mail had been sent but member hasn't complete the signup .
- Last login : time that user last logged in .
- Modify : click to modify the member permissions .

Invite New Members

You can invite multiple users and assign them permissions for entire organization trees at once.



Invite New Member

User Email (one per row)

Org / Networks	Permission
EnGenius_Taipei	None
8F	None
6B	None
7F	None
2F	None

Invite users to manage your networks with privileges

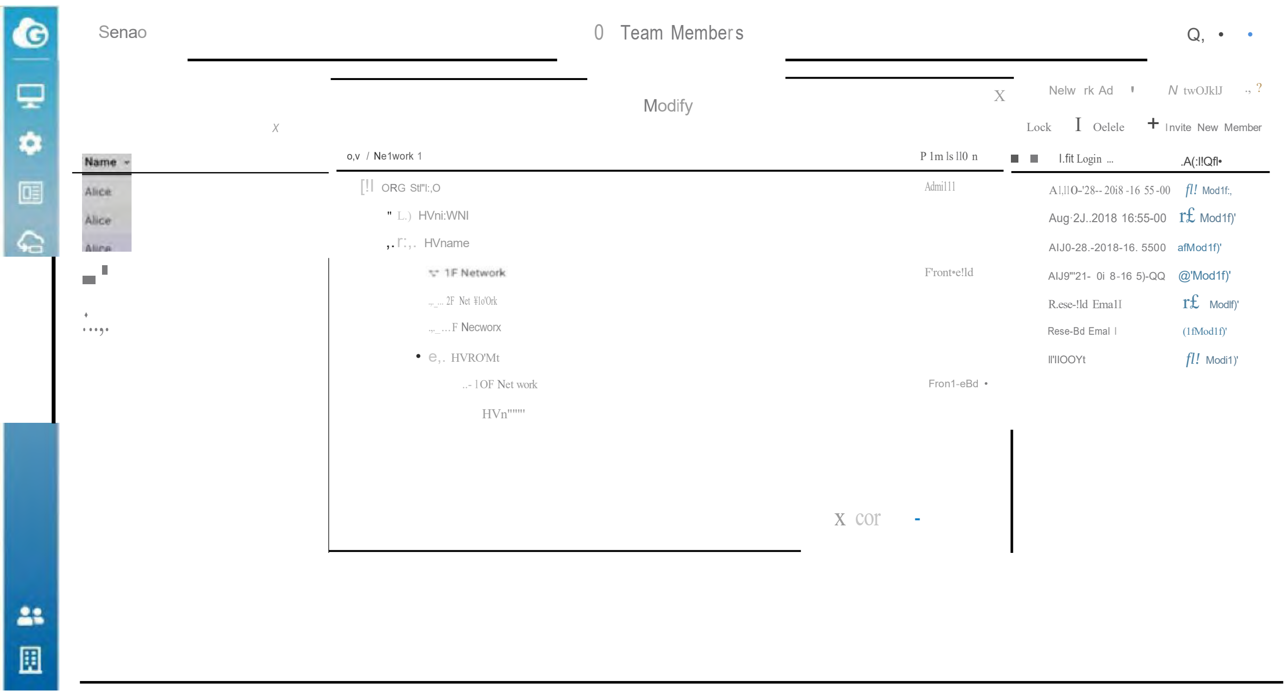
1. Input the user email, one per row.

2. Assign member privileges for a network or organization.

3. Click Apply to save changes.

Modify Member Permissions

1. Click Modify.
2. Change the Permission based on the organization trees.
3. Click Apply.



Senao

0 Team Members

Q, • •

Modify

X

x

Nelw rk Ad ' N twOJklJ ., ?

Lock I Oelele + Invite New Member

Name

Alice

Alice

Alice

o,v / Ne1work 1 P 1m ls ll0 n

[!! ORG Stl"l:,O Admi111

" L.) HVni:WNI

,.r:,. HVname

1F Network F'ront•e!ld

.,_... 2F Net ¥lo'Ork

.,_...F Necworx

• e,. HVRO'Mt

..- 1OF Net work Fron1-eBd •

HVn"""

x cor -

		I.fit Login ...	.A(:!!Qfl•
■	■		
		A1,l1O-'28-- 20i8 -16 55-00	fl! Mod1f:,
		Aug·2J..2018 16:55-00	r£ Mod1f)'
		AIJ0-28.-2018-16. 5500	afMod1f)'
		AIJ9'"21- 0i 8-16 5)-QQ	@'Mod1f)'
		R.ese-!ld Emal1	r£ Modlf)'
		Rese-Bd Emal I	(1fMod1f)'
		Il'IlOOYt	fl! Modi1)'

Roles and Permissions

Organization Permission Types

Admin: user has full administrative access to all networks and organization-wide settings. This is the highest level of access available.

Viewer: user is able to access most aspects of network and organization-wide settings, but unable to make any changes.

Network Permission Types

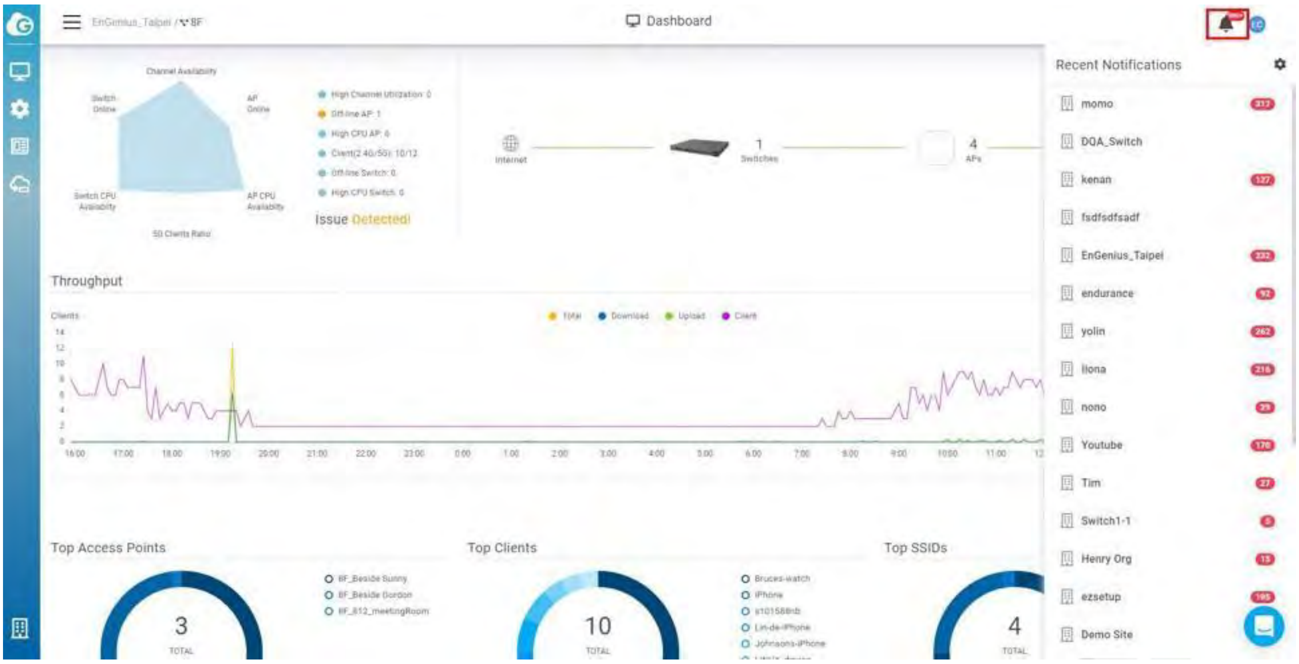
Admin: user has access to view all aspects of a network and makes any changes to it.

Viewer: user able to access most aspects of a network, including the configuration section, but no changes can be made.

Front desk: user is able to access the front desk portal to generate guess passes and manage guest passes only.

Notification Center

EnGenius Cloud provides a notification mechanism for alerting you to important events that occurred. You can click the bell icon to access this screen.

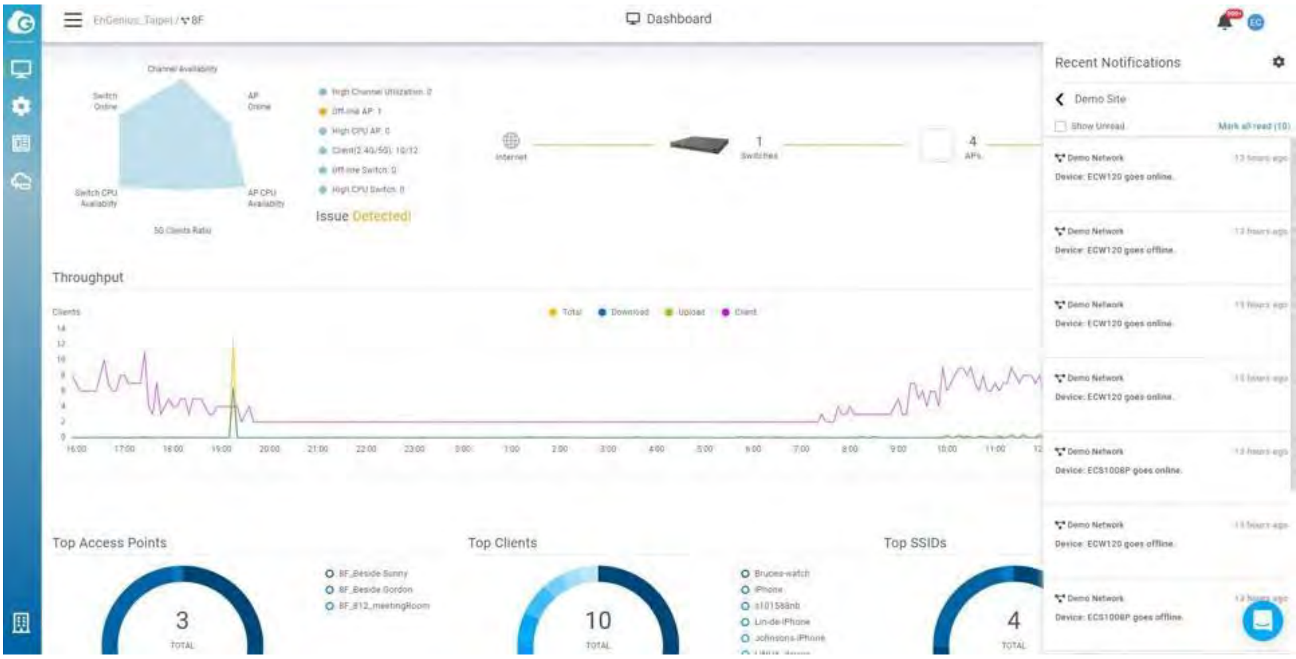


Recent Notifications

momo	312
DQA_Switch	
kenan	127
fsdfsdfsadf	
EnGenius_Taipei	232
endurance	92
yolin	262
ilona	216
nono	29
Youtube	170
Tim	27
Switch1-1	5
Henry Org	15
ezsetup	195
Demo Site	

Recent Notifications

This shows the event numbers that occur and is ordered by organization. You can click one of the organizations in the list to access detailed event information.



Recent Notifications

Demo Site

□ Show Unread Mark all read (10)

Demo Network 13 hours ago
Device: ECW120 goes online.

Demo Network 13 hours ago
Device: ECW120 goes offline.

Demo Network 13 hours ago
Device: ECW120 goes online.

Demo Network 13 hours ago
Device: ECW120 goes online.

Demo Network 13 hours ago
Device: ECS1008P goes online.

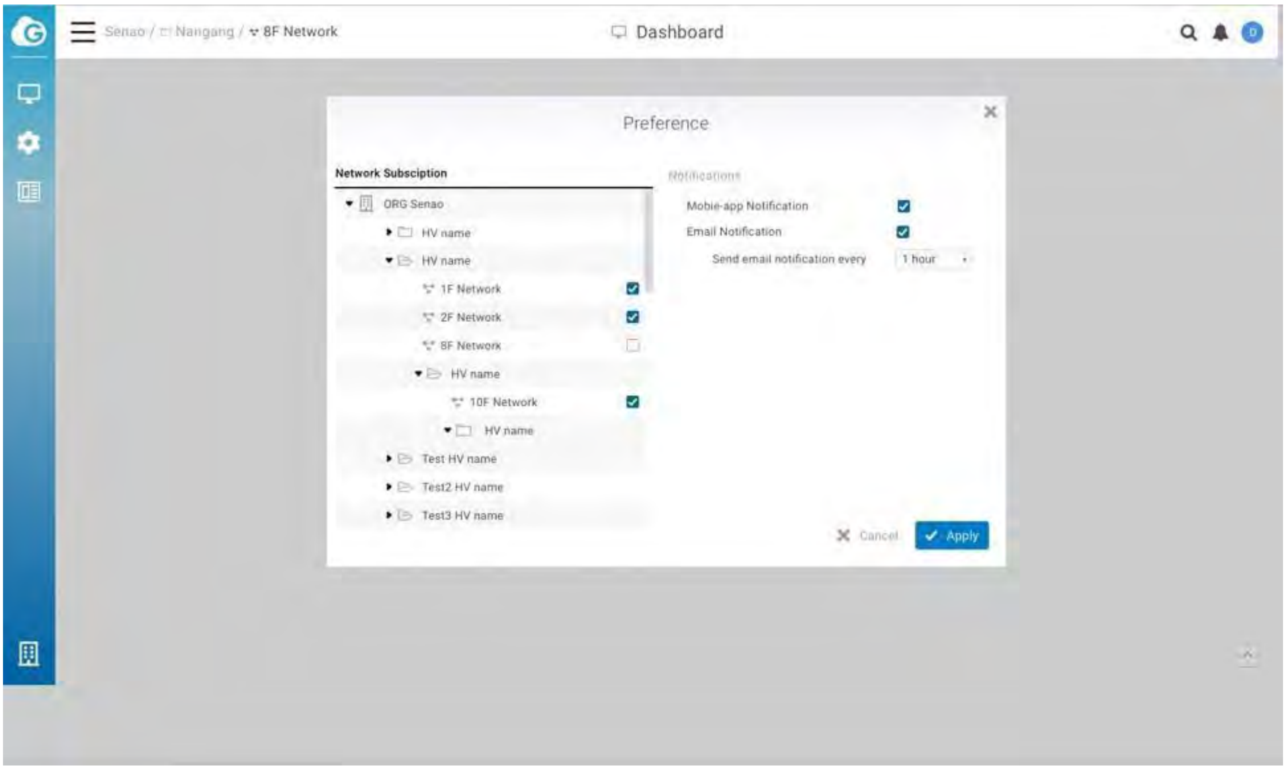
Demo Network 13 hours ago
Device: ECW120 goes offline.

Demo Network 13 hours ago
Device: ECS1008P goes offline.

Preferences

Network Subscription

This allows you to subscribe or unsubscribe to network events. When subscribed, you will receive that network's notifications.



Network Subsciption

- ORG Senao
  - HV name
  - HV name
    - 1F Network ☑
    - 2F Network ☑
    - 8F Network □
    - HV name
      - 10F Network ☑
      - HV name
  - Test HV name
  - Test2 HV name
  - Test3 HV name

Notifications

Mobie-app Notification ☑

Email Notification ☑

Send email notification every 1 hour

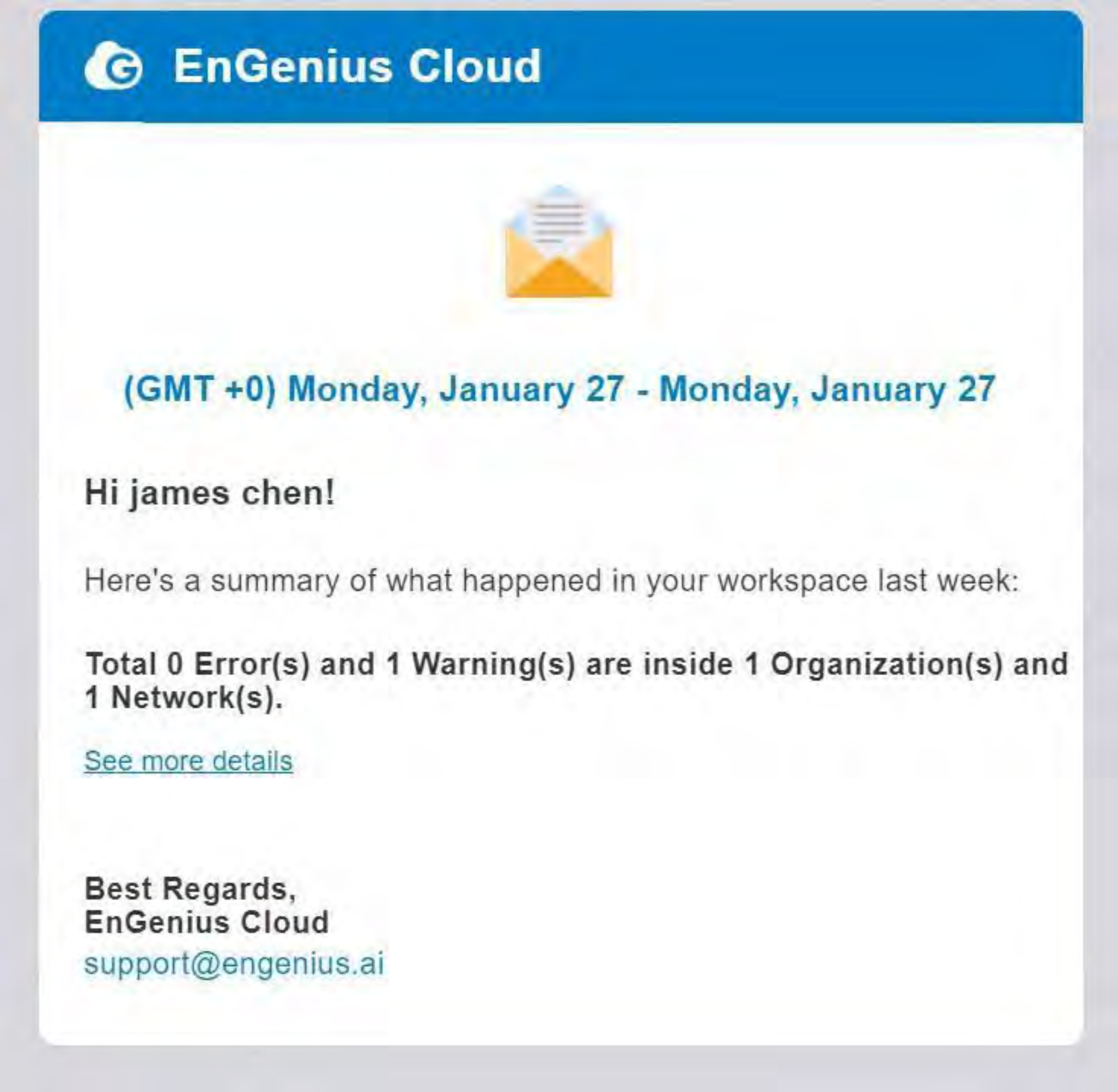
Notifications

Mobile App **Notifications:** You can turn on/off **notifications** on the EnGenius Cloud Mobile App.

Email **Notification**: You will receive an email digest of network events at a scheduled time if at least one event has occurred.

Email format

You will receive email formats like below if you enable the Email **Notification**



EnGenius Cloud

(GMT +0) Monday, January 27 - Monday, January 27

Hi james chen!

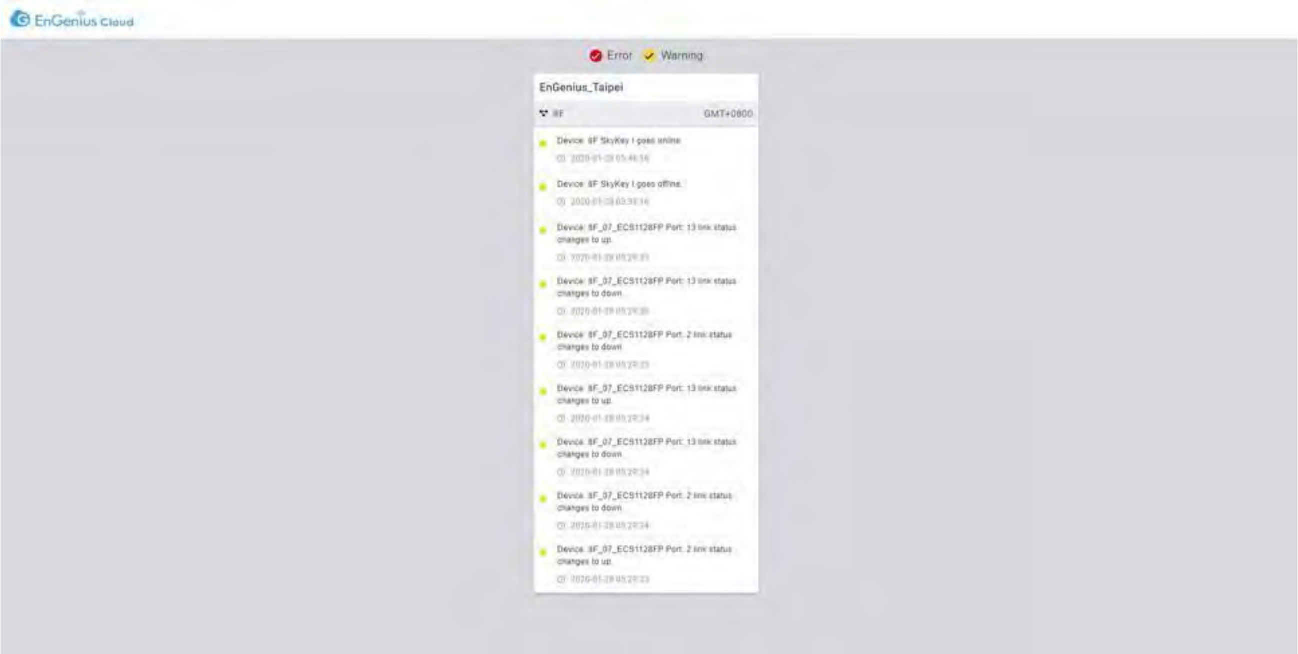
Here's a summary of what happened in your workspace last week:

Total 0 Error(s) and 1 Warning(s) are inside 1 Organization(s) and 1 Network(s).

See more details

Best Regards,
EnGenius Cloud
support@engenius.ai

Click See more details to see Network events. Each card represents an individual organization and each divider inside cards represents different networks.



☑ Error ☑ Warning

EnGenius_Taipei

8F GMT+0800

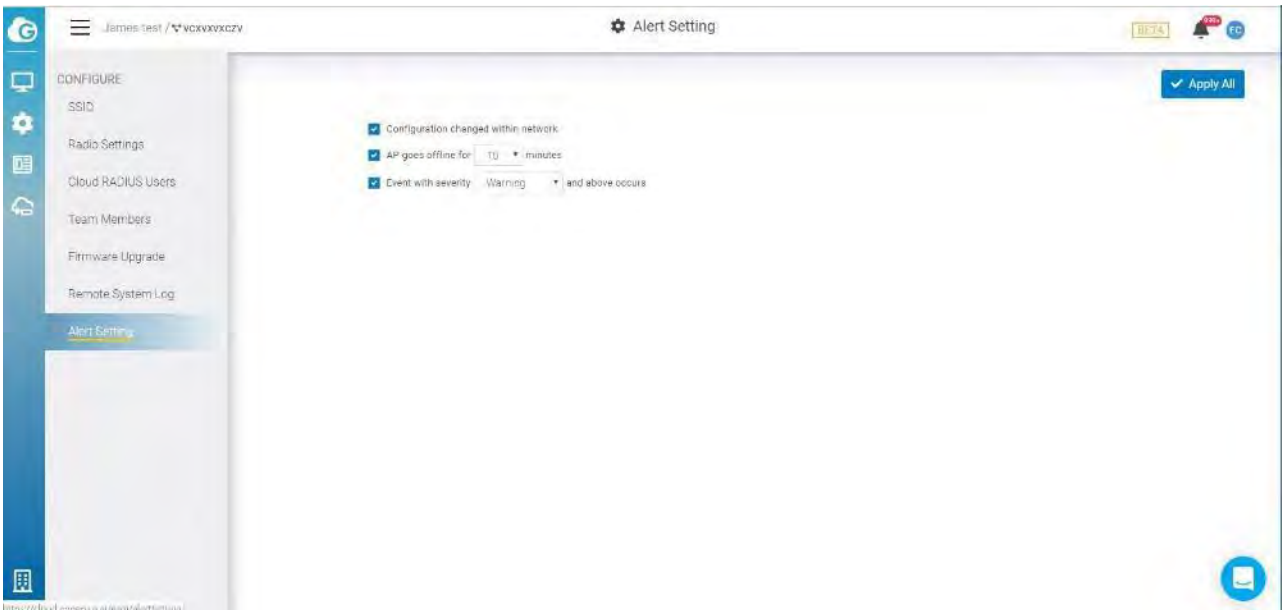
- Device: 8F SkyKey I goes online.
  2020-01-29 05:46:16
- Device: 8F SkyKey I goes offline.
  2020-01-28 03:39:16
- Device: 8F_07_ECS1128FP Port: 13 link status changes to up.
  2020-01-28 05:29:31
- Device: 8F_07_ECS1128FP Port: 13 link status changes to down.
  2020-01-29 05:29:30
- Device: 8F_07_ECS1128FP Port: 2 link status changes to down.
  2020-01-28 05:29:23
- Device: 8F_07_ECS1128FP Port: 13 link status changes to up.
  2020-01-28 05:29:34
- Device: 8F_07_ECS1128FP Port: 13 link status changes to down.
  2020-01-28 05:29:34
- Device: 8F_07_ECS1128FP Port: 2 link status changes to down.
  2020-01-28 05:29:34
- Device: 8F_07_ECS1128FP Port: 2 link status changes to up.
  2020-01-29 05:29:23

Filter events: On the top of page allows you to filter events. You can check or uncheck the checkbox near error and warning events.

Configuring Alert Settings

There are a number of options available for email alerts to be sent when certain network or device events occur.

Alerts can be configured under **Configure** > Alerts.



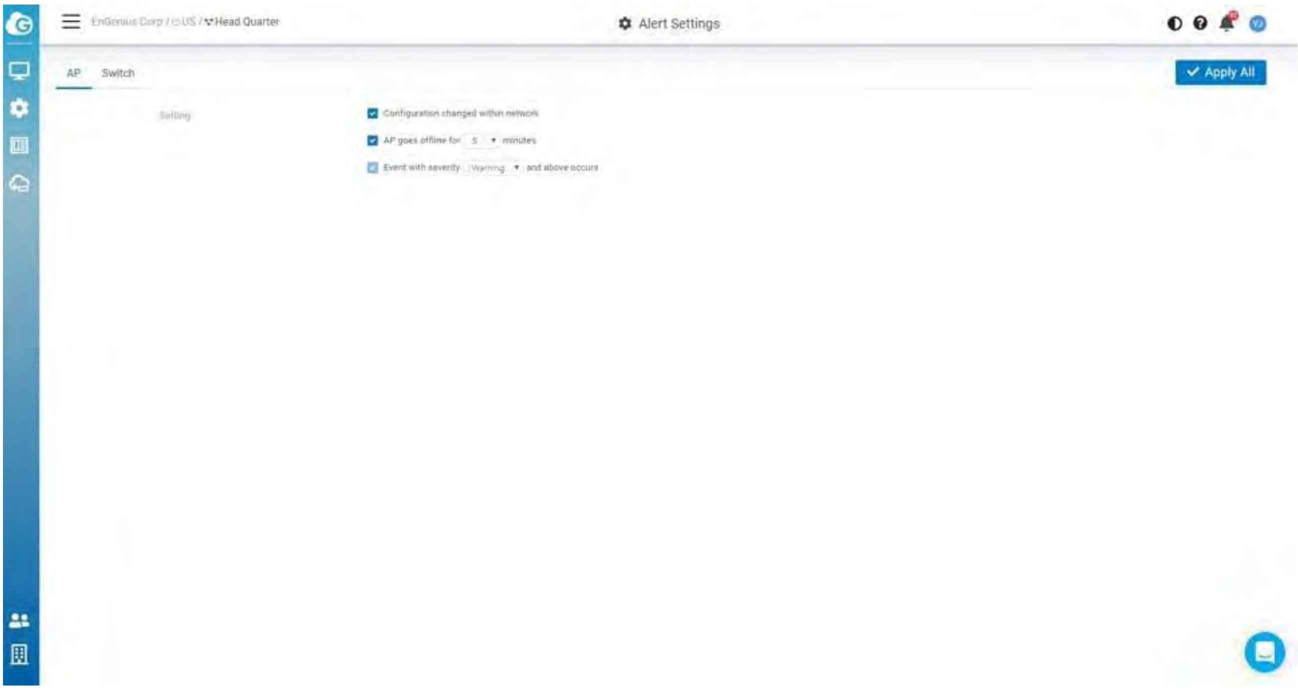
☑ Configuration changed within network

☑ AP goes offline for 10 minutes

☑ Event with severity Warning and above occurs

Access Point Alerts

Alerts can be configured for the following access point events:



Setting

☑ Configuration changed within network

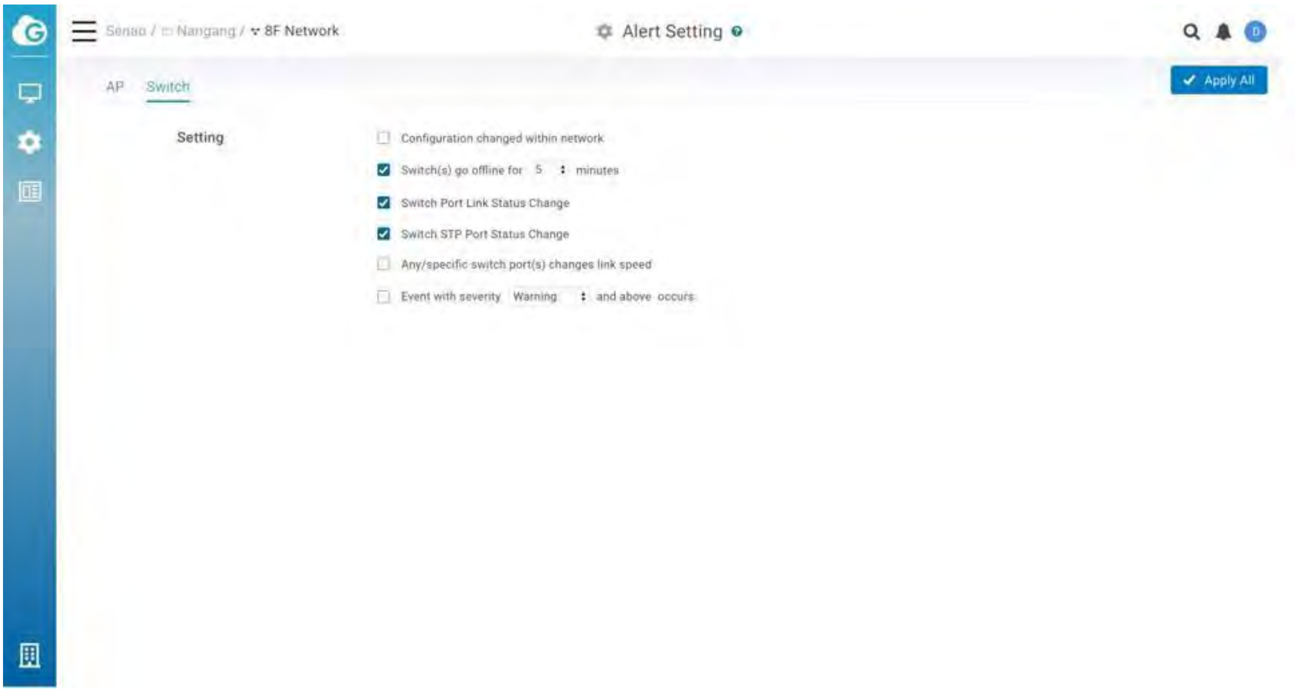
☑ AP goes offline for 5 ▾ minutes

☑ Event with severity Warning ▾ and above occurs

- AP(s) go **offline** for XXX minutes: sends an email if one or more access points go offline for a preset (and customizable) amount of time.
- **Configuration changed** within network: sends an email if SSID, radio settings, firmware upgrade, or individual device settings override the default settings.
- Event with severity XXXX and above occurs: sends an email if event severity meeting a minimum severity threshold occurs.

Switch Alerts

Alerts can be configured for the following switch events:



Setting

☐ Configuration changed within network

☑ Switch(s) go offline for 5 minutes

☑ Switch Port Link Status Change

☑ Switch STP Port Status Change

☐ Any/specific switch port(s) changes link speed

☐ Event with severity Warning and above occurs

- **Configuration changed** within network: sends an email if SSID, radio settings, firmware upgrades, or individual device settings override the default settings.
- Switch port link status change: sends an email when device port link status is changed.
- Switch STP Port status change: sends an email when device port STP status is changed.
- Switch LBD Port status change: sends an email when device LBD status is changed.
- Switch(s) go **offline** for XX minutes: sends an email when switches go offline for a preset number of minutes.
- **Any/specific switch port(s) changed link speed:** sends an email when a switch port link speed changes.
- Event with severity XXX and above occurs: sends an email if an event occurs with a severity equal to or higher than a preset value.

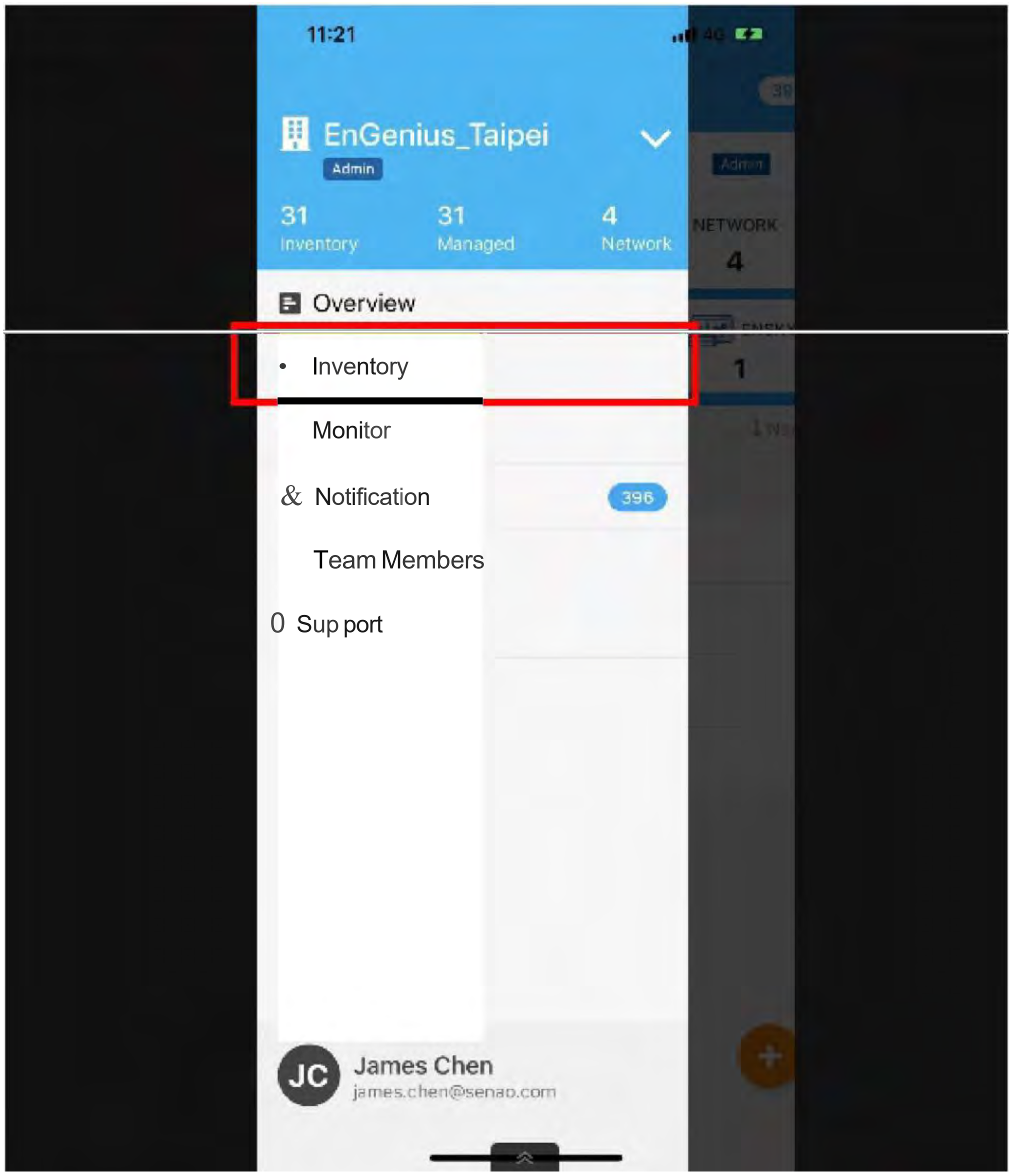
Mobile App

The EnGenius Mobile App is a mobile user interface (UI) for EnGenius Cloud. You can keep an eye on your network when you are on the go. This is a great solution for around the clock network support. Versions are available for Android on Google Play and iOS via the App Store.

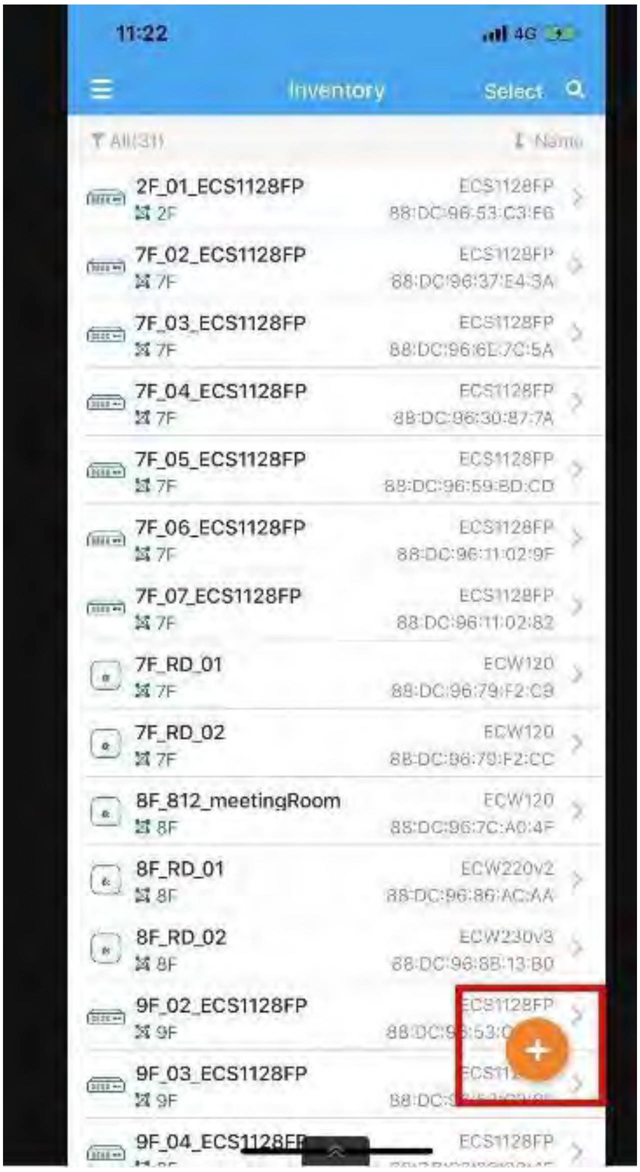
Adding a Device

This section explains how to add a networking device to your network using the EnGenius Mobile App.

1. Navigate to the Inventory tab and tap the + symbol on the bottom-right of the screen.



11:21
EnGenius_Taipei
Admin
31
Inventory
31
Managed
4
Network
Overview
Inventory
Monitor
Notification
396
Team Members
Sup port
JC
James Chen
james.chen@senao.com
NETWORK
4
1



11:22 4G

Inventory Select

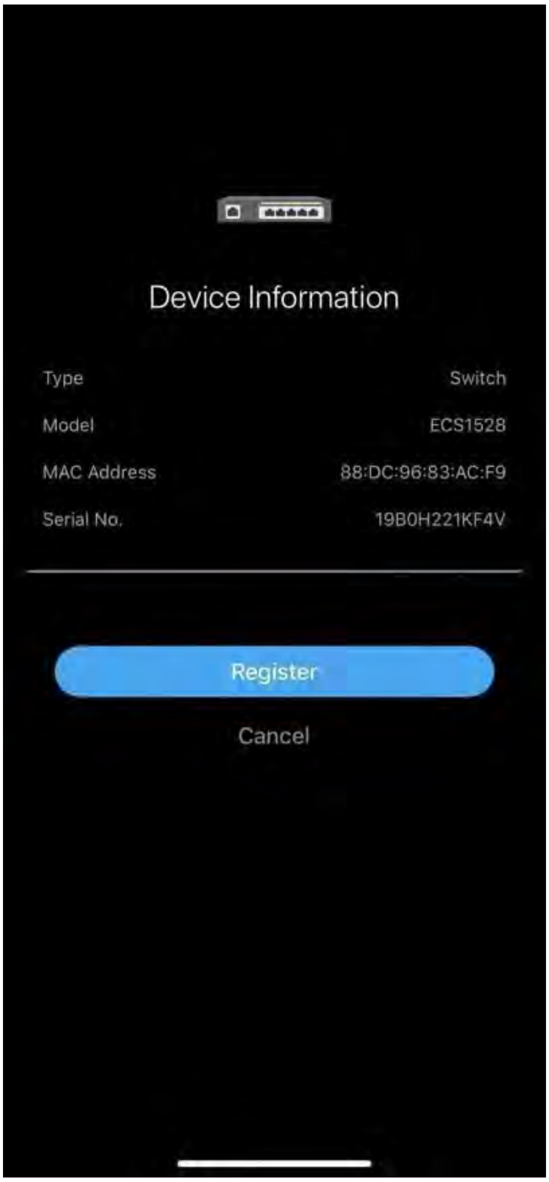
All(31) Name

2F_01_ECS1128FP 2F	ECS1128FP 88:DC:96:53:C3:E6
7F_02_ECS1128FP 7F	ECS1128FP 88:DC:96:37:E4:3A
7F_03_ECS1128FP 7F	ECS1128FP 88:DC:96:6E:7C:5A
7F_04_ECS1128FP 7F	ECS1128FP 88:DC:96:30:87:7A
7F_05_ECS1128FP 7F	ECS1128FP 88:DC:96:59:8D:CD
7F_06_ECS1128FP 7F	ECS1128FP 88:DC:96:11:02:9F
7F_07_ECS1128FP 7F	ECS1128FP 88:DC:96:11:02:82
7F_RD_01 7F	ECW120 88:DC:96:79:F2:C9
7F_RD_02 7F	ECW120 88:DC:96:79:F2:CC
8F_812_meetingRoom 8F	ECW120 88:DC:96:7C:A0:4F
8F_RD_01 8F	ECW220v2 88:DC:96:86:AC:AA
8F_RD_02 8F	ECW230v3 88:DC:96:88:13:B0
9F_02_ECS1128FP 9F	ECS1128FP 88:DC:9 :53:
9F_03_ECS1128FP 9F	ECS11 88:DC:
9F_04_ECS1128FP	ECS1128FP

2. Find the QR code at the bottom of the device and scan it.

If the camera successfully scanned a QR code, the app will display the Device Information. You could tap

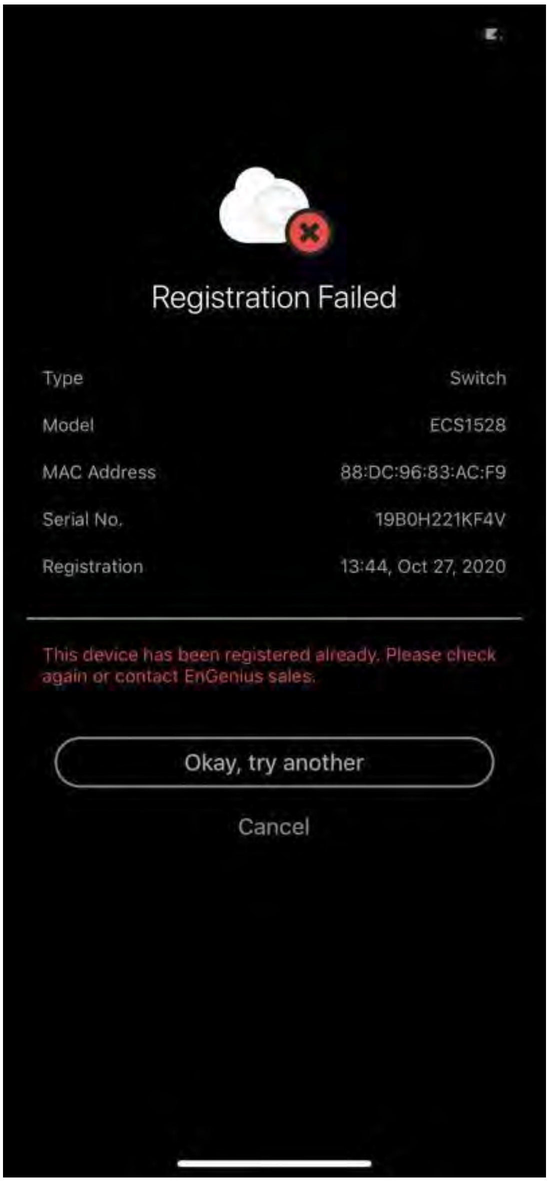
Register to complete the Registration.



Device Information

Type	Switch
Model	ECS1528
MAC Address	88:DC:96:83:AC:F9
Serial No.	19B0H221KF4V

If you failed to scan the QR code successfully, you could tap Okay, try another.



Registration Failed

Type Switch

Model ECS1528

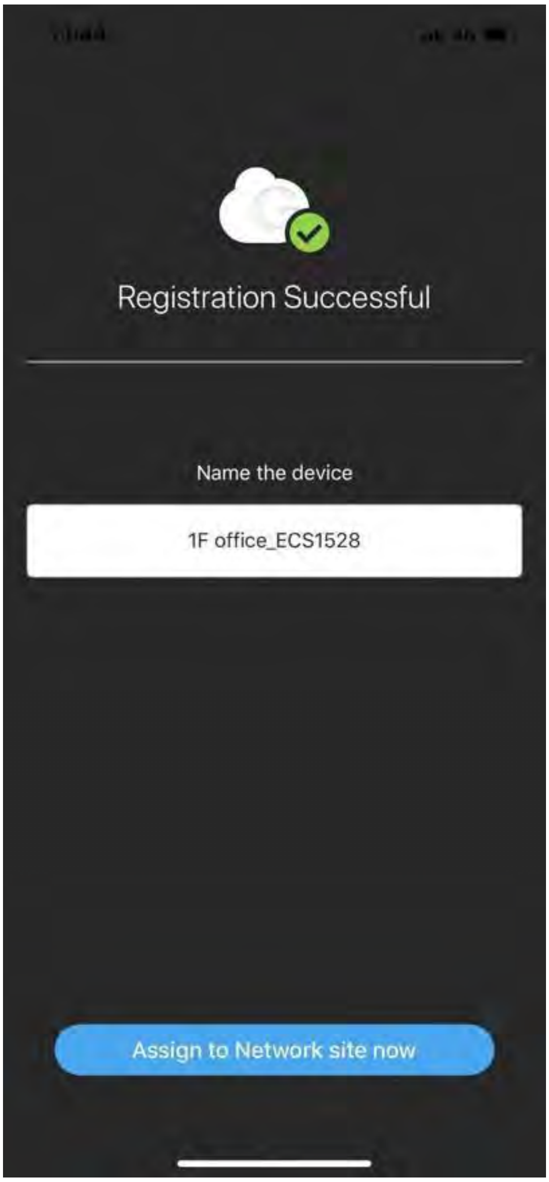
MAC Address 88:DC:96:83:AC:F9

Serial No. 19B0H221KF4V

Registration 13:44, Oct 27, 2020

This device has been registered already. Please check again or contact EnGenius sales.

3. Once a device has been successfully registered, you can tap Assign to Network site now.

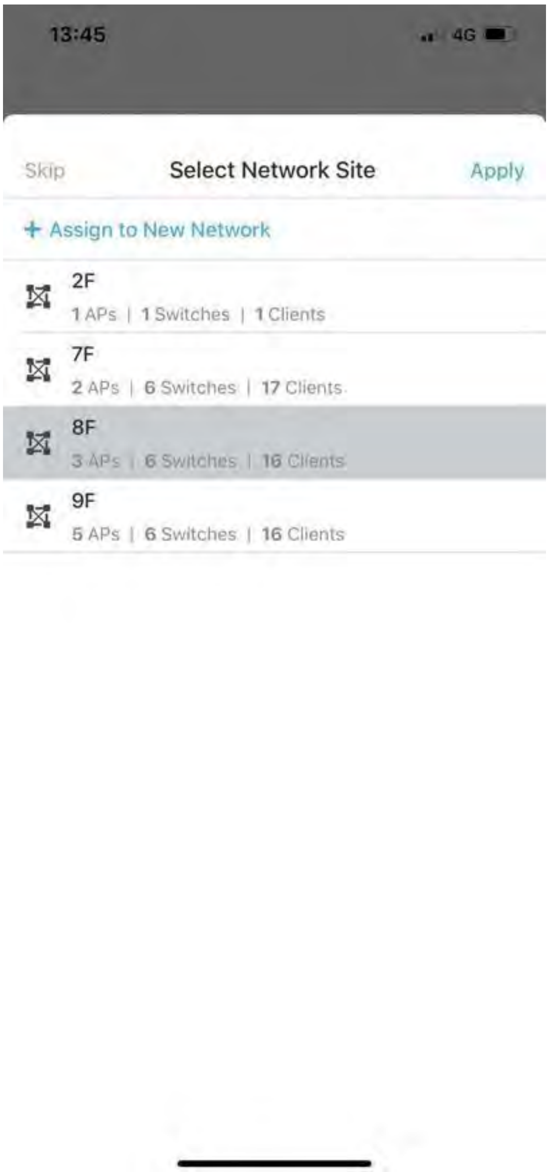


Registration Successful

Name the device

1F office_ECS1528

5. Tap the Network and tap Apply.



13:45

Skip Select Network Site Apply

+ Assign to New Network

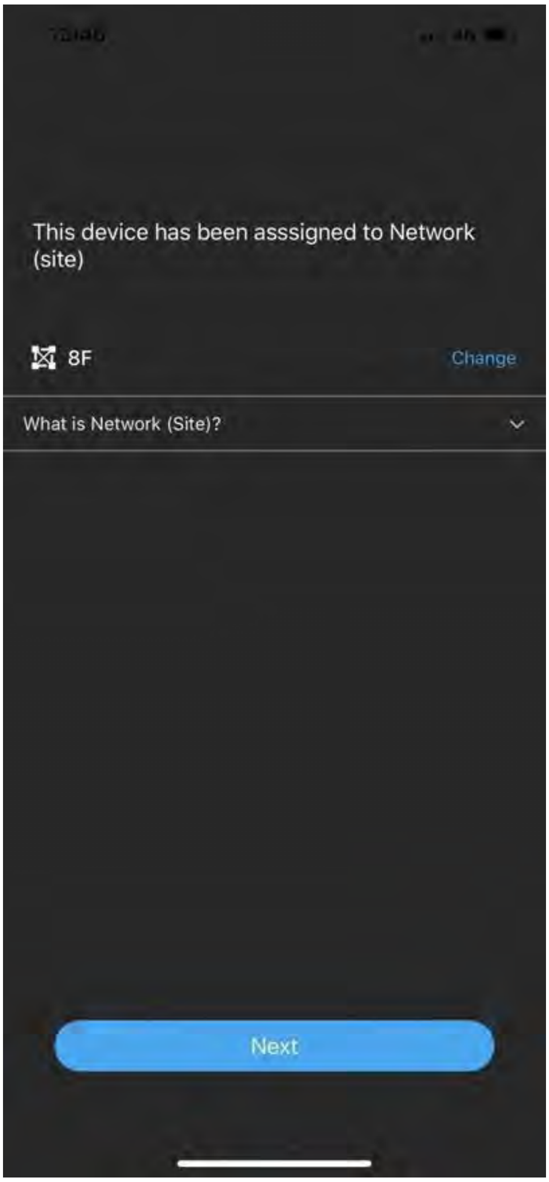
2F
1 APs | 1 Switches | 1 Clients

7F
2 APs | 6 Switches | 17 Clients

8F
3 APs | 6 Switches | 16 Clients

9F
5 APs | 6 Switches | 16 Clients

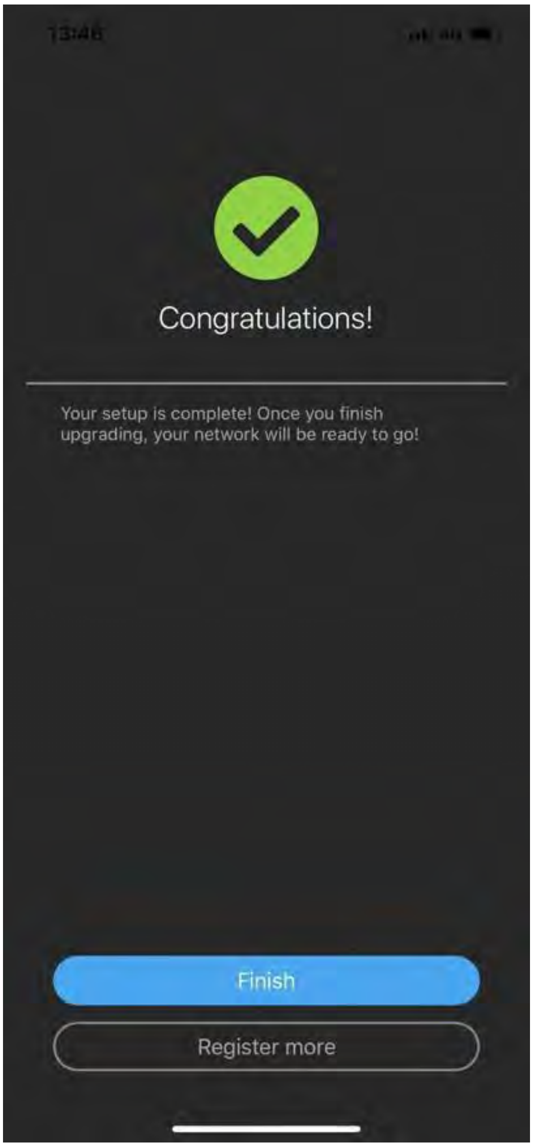
6. Once you select the wrong network, you could tap Change to select the correct network. If the network is correct , tap Next .



This device has been asssigned to Network (site)

8F

7. You could tap Finish to complete the whole process or tap Register more to register other devices .



Congratulations!

Your setup is complete! Once you finish upgrading, your network will be ready to go!

Get Remote Support

LiveChat

Whenever you login the system, you can always find a `LiveChat` button at bottom-right corner of the page.

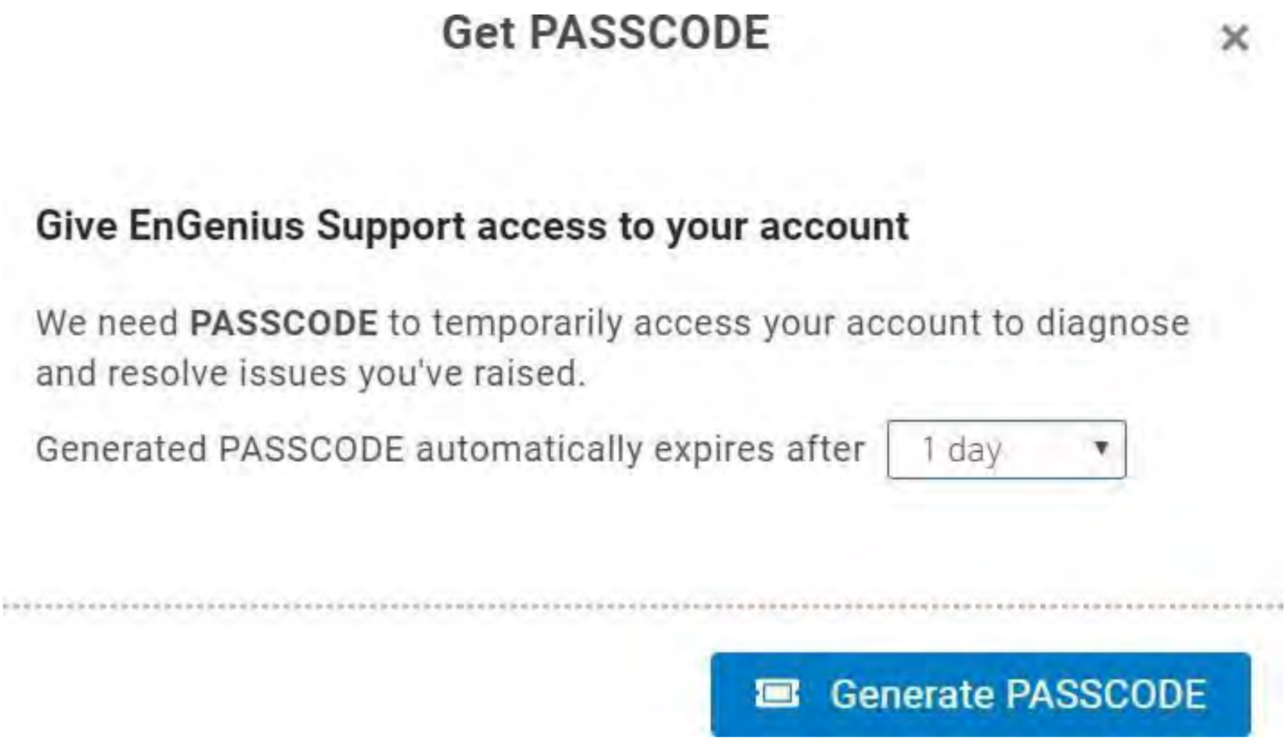
You can leave a message with this chat system. EnGenius support team will usually feed back in minutes.

Remote Support Passcode

The EnGenius Support Passcode is used to verify users' identities for security purposes. When you get trouble on configuring your networks or operating your cloud configurations, you can click on the `Help` button on the top-right corner of menu.

Choose Remote Support and click on `Generate PASSCODE` .

Remote Support



Get PASSCODE

Give EnGenius Support access to your account

We need **PASSCODE** to temporarily access your account to diagnose and resolve issues you've raised.

Generated PASSCODE automatically expires after 1 day

There is an option here that you can decide how long the generated passcode is valid (from 1 hour to 7 days). By sending the generated passcode to EnGenius support team on LiveChat, support team can access your account temporarily to diagnose and resolve issues you've raised.

> ⓘ Note that the generated PASSCODE will automatically expire after a period of time. Support team won't be able to access your resource once the PASSCODE is expired.

Security

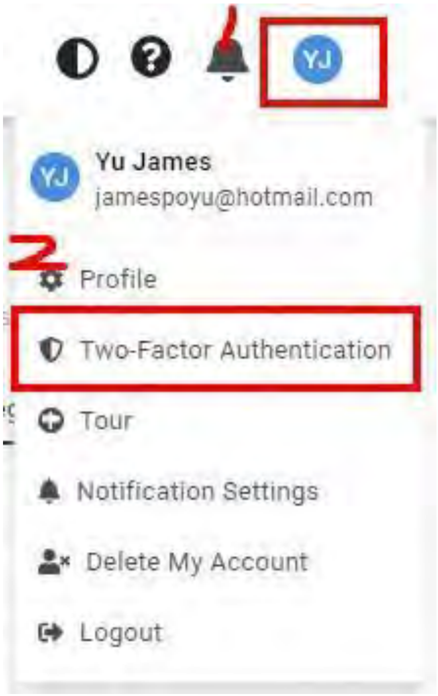
Two Factor Authentication

Two Factor Authentication, also known as 2FA or TFA, is a two-step verification process that requires more information in addition to the usual username and password. This extra piece of information is something only the user will know or have physically with them, like a token sent to a mobile app, for example. It is very important to create backup codes the moment you enable 2FA on your account in case your phone is lost and cannot access the 2FA code.

How to Enable 2FA to protect your account

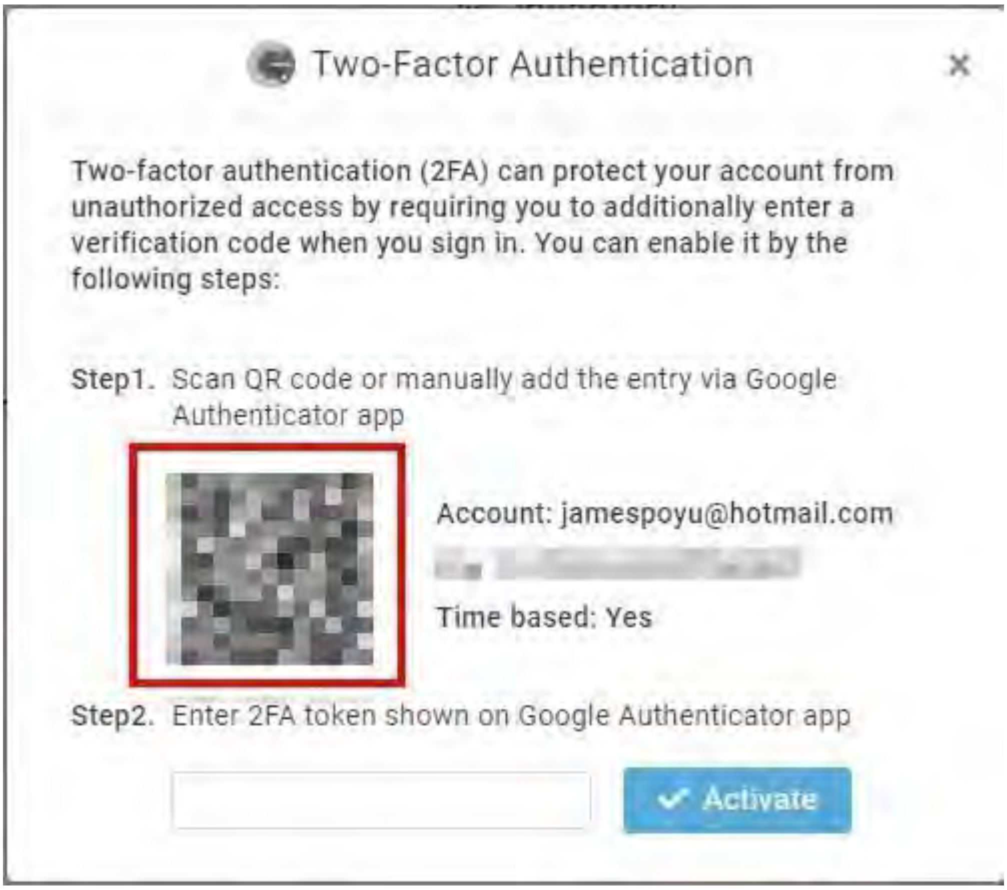
1. Download and install the "Google Authenticator" APP on your mobile phone. https:/ apps.apple.com/us/app/google-authenticator/id388497605 . Google Authenticator will generate OTP (One-time passcode) for your account on EnGenius Cloud by following below steps. Please be reminded that if you have multiple accounts, then you need to generate corresponding entries to each account in Google Authenticator.

2. Select Two Factor Authentication from the top-right menu.



3. Open your chosen authenticator app on your smartphone. Since the following is using Google Authenticator as an example, the steps might vary slightly. Open the Google Authenticator app on your phone, tap Menu, then tap Begin Setup > Scan barcode. If you already have other accounts, you would click the plus sign (+) on the upper right and then Scan barcode.

4. Your phone will now be in the "scanning" mode. Go ahead and scan the QR code that appeared in the popup.



Two-factor authentication (2FA) can protect your account from unauthorized access by requiring you to additionally enter a verification code when you sign in. You can enable it by the following steps:

Step1. Scan QR code or manually add the entry via Google Authenticator app

Account: jamespoyu@hotmail.com

[redacted]

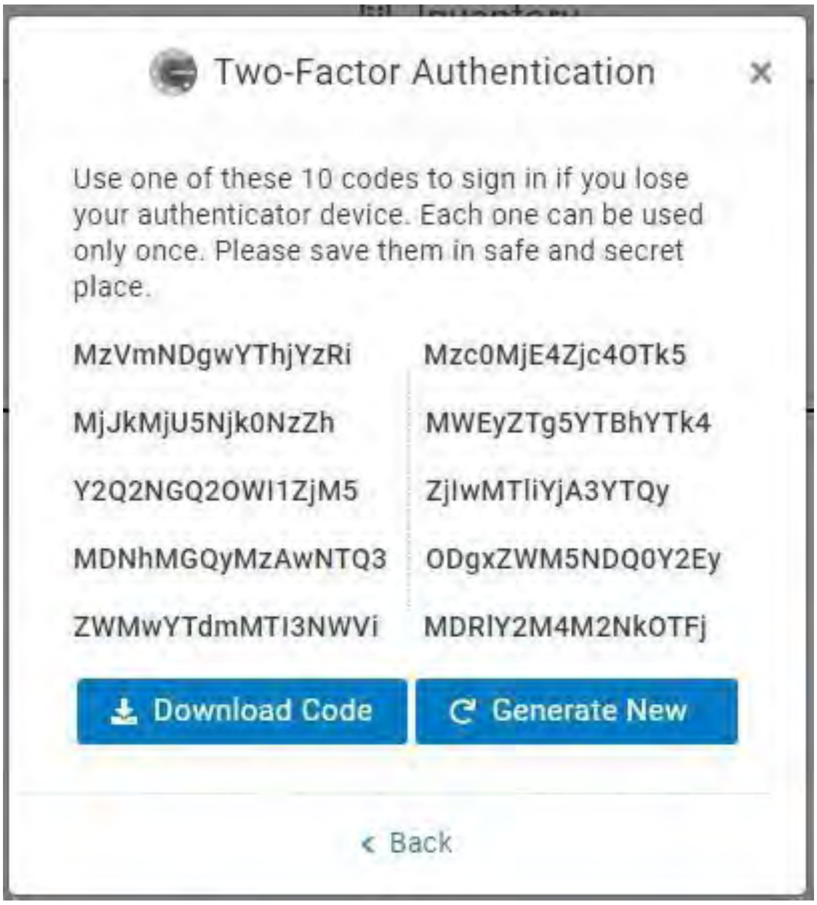
Time based: Yes

Step2. Enter 2FA token shown on Google Authenticator app

5. Enter the 6-digit authentication token provided by Google Authenticator into the popup, then click Activate .

Recovery codes

It is extremely important to back up a set of Recovery codes the moment two-factor authentication is enabled. These codes will allow you to unlock your account to disable 2FA if you somehow lose access to your authenticator app (if say you lost your mobile).



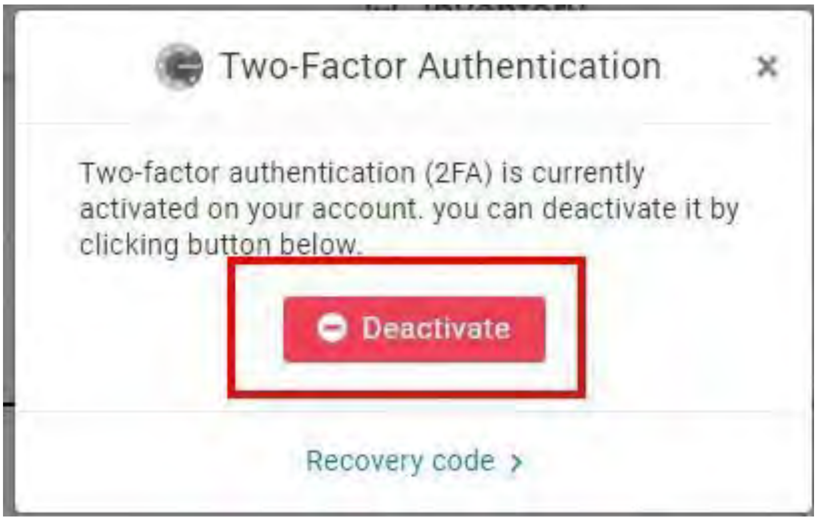
Use one of these 10 codes to sign in if you lose your authenticator device. Each one can be used only once. Please save them in safe and secret place.

MzVmNDgwYThjYzRi	Mzc0MjE4Zjc4OTk5
MjJkMjU5Njk0NzZh	MWEyZTg5YTBhYTk4
Y2Q2NGQ2OWI1ZjM5	ZjlwMTliYjA3YTQy
MDNhMGQyMzAwNTQ3	ODgxZWM5NDQ0Y2Ey
ZWMwYTdmMTI3NWVi	MDRlY2M4M2NkOTFj

You can access Recovery code after you enabled 2FA. You will be given a list of 10 backup codes, copy them somewhere safe. If there's a possibility someone has gained access to your codes, generate new ones to make those compromised ones obsolete.

How to Deactivate 2FA

1. Select Two Factor Authentication from the top-right menu.
2. Click Deactivate



Two-Factor Authentication

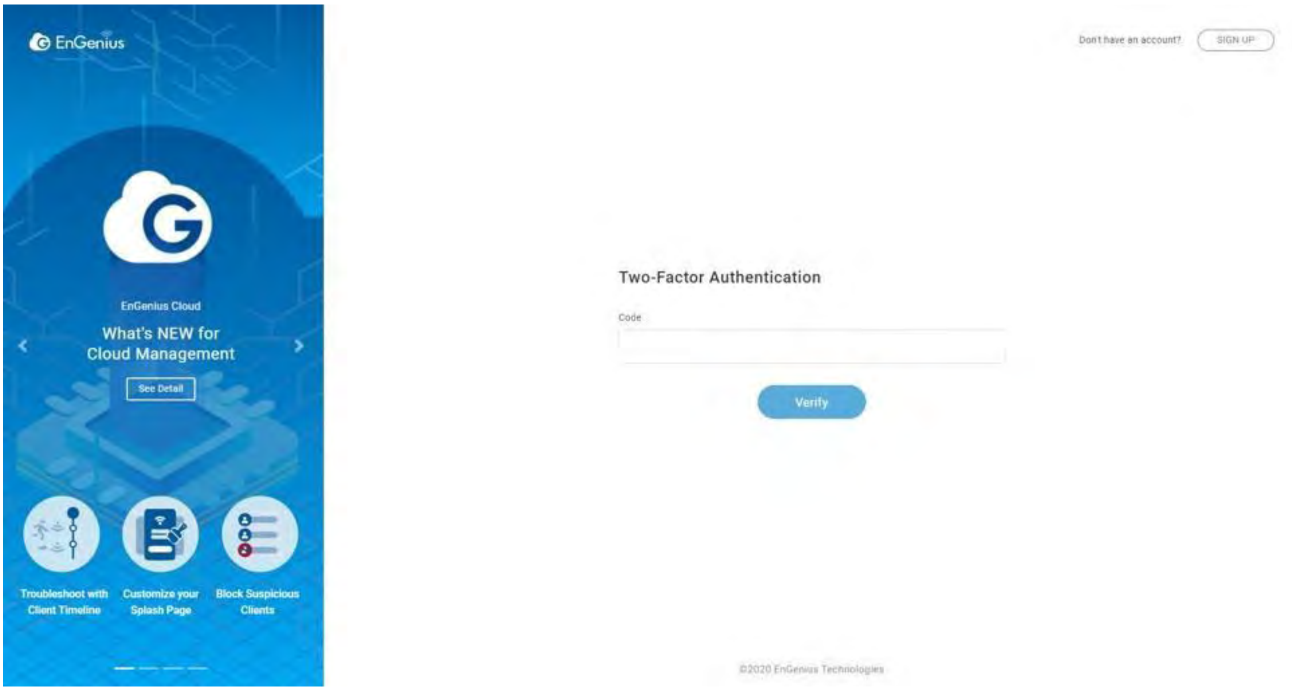
Two-factor authentication (2FA) is currently activated on your account. you can deactivate it by clicking button below.

How to Access a Locked Out Account

If you are locked out of your account because you changed mobiles, deleted the authenticator app by mistake or lost your phone, you can get access to your account once more with the below method.

Login Cloud using recovery codes

1. Go to cloud.engenius.ai enter your username and password as usual, and prompted for the screen for you to enter code.


EnGenius
EnGenius Cloud
What's NEW for Cloud Management
See Detail
Troubleshoot with Client Timeline
Customize your Splash Page
Block Suspicious Clients
Don't have an account?
SIGN UP
Two-Factor Authentication
Code
Verify
©2020 EnGenius Technologies

2. Now just paste one of the backup codes you previously saved and click Verify.

3. Follow the How to Deactivate 2FA and How to Enable 2FA to protect your account procedure again. Remember to click Download code to save a new set of backup codes.

> ⓘ Other possible issues and solutions are discussed in this Google 2-Step Verification Help article.

2FA Enforcement to your Organization

This feature helps the Organization administrator to enforce all Cloud users to have more secure to access the organization. If you enable 2FA Enforcement , your team members are required to have two-factor authentication (2FA) enabled when access this organization. If team members don't activate 2FA, they are not allowed to access this organization . You can access this feature by clicking Organization > Security .

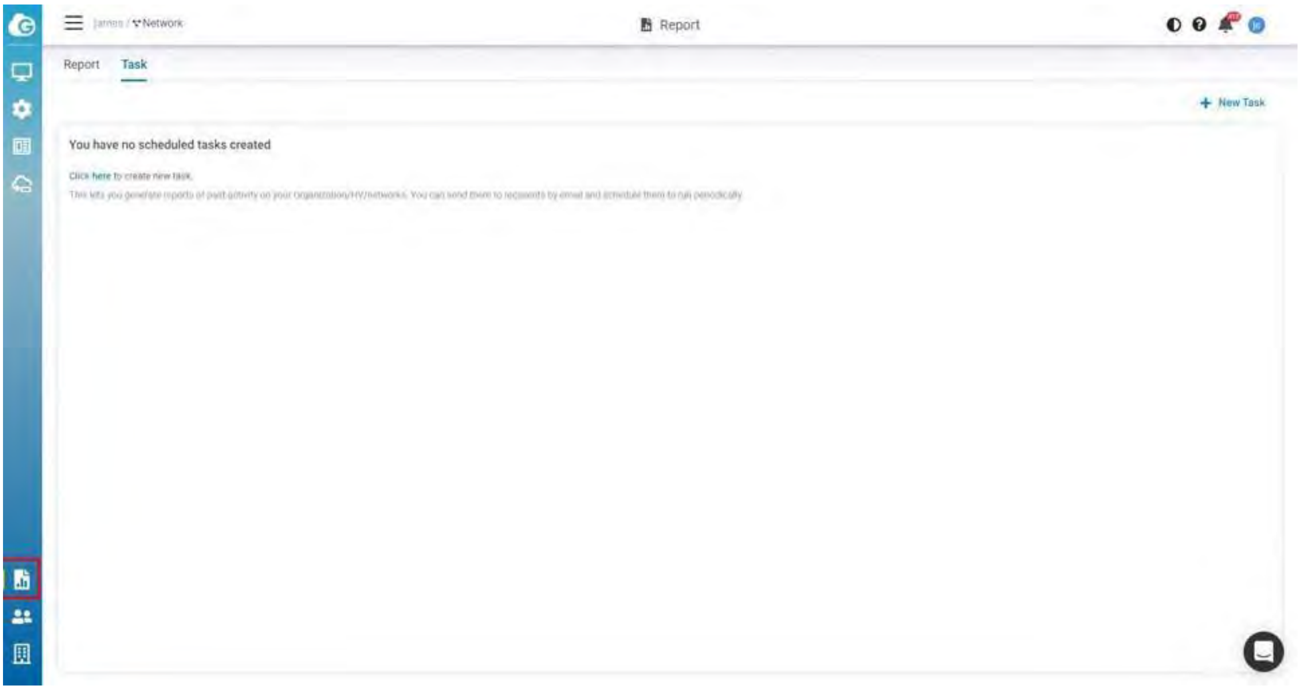
> If the user manages multiple Organizations and does not enable 2FA, he is still able to log in to Cloud. However, he cannot access the Org with 2FA enforcement enabled as a requirement.

Report

Report lets you compile reports of past activity on your Organization/HV/networks. These reports can be filtered to only include certain organizations, HV, or networks. You can send them to recipients by email and schedule them to run periodically.

How can I create Reports?

To create your reports, you need to go to the Reports located on the left panel. Under the tab 'Task' you will find the button 'New Task' and click it.



You have no scheduled tasks created

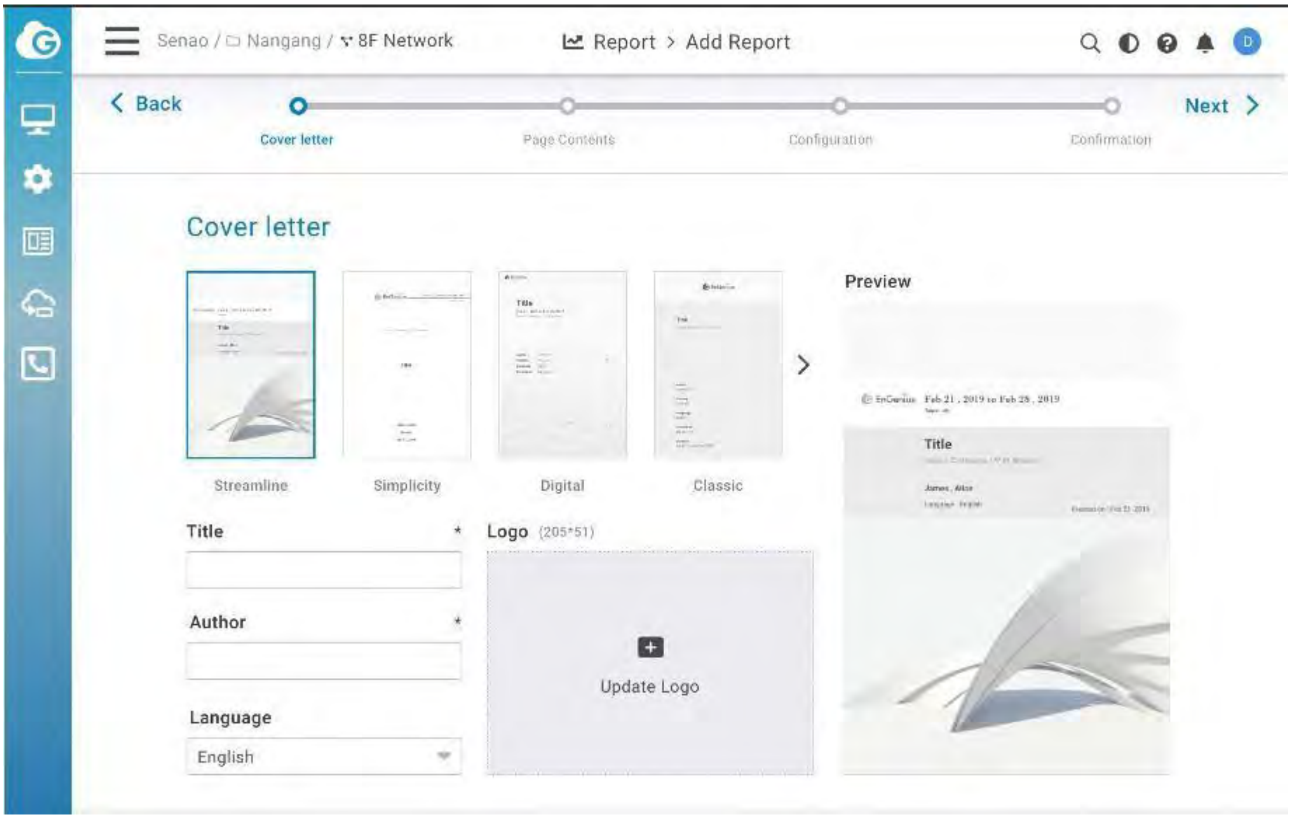
Click here to create new task.

This lets you generate reports of past activity on your Organization/HV/networks. You can send them to recipients by email and schedule them to run periodically

When you click on this button a new wizard will be displayed with the steps to customize report content directly

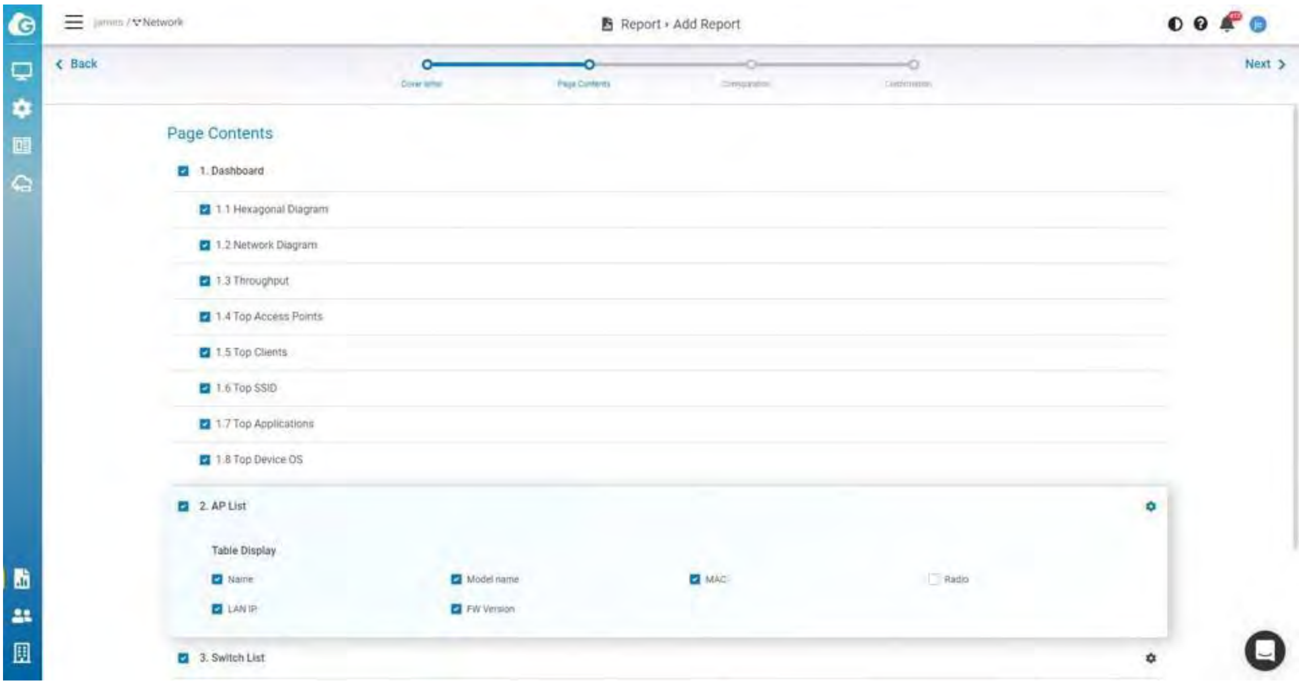
Cover letter

- Author: Input Author and will be displayed in report cover letter)
- Cover letter: Select the style and will be displayed in the cover letter)
- Language: Support English only currently)
- Logo: Upload the logo you want to display on the cover letter)



Page Content

This allows you to select page contents that will be displayed on your report. You can click the gear icon to show or hide the table data.



Page Contents

☑ 1. Dashboard
- ☑ 1.1 Hexagonal Diagram
- ☑ 1.2 Network Diagram
- ☑ 1.3 Throughput
- ☑ 1.4 Top Access Points
- ☑ 1.5 Top Clients
- ☑ 1.6 Top SSID
- ☑ 1.7 Top Applications
- ☑ 1.8 Top Device OS

☑ 2. AP List

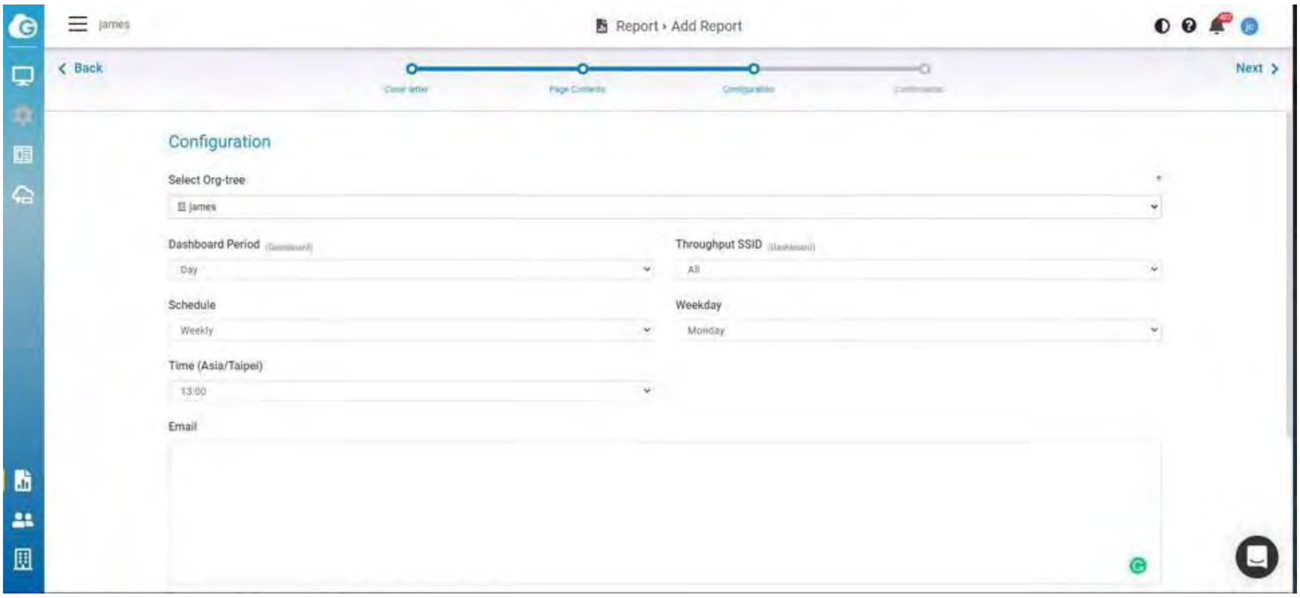
Table Display

☑ Name ☑ Model name ☑ MAC □ Radio
☑ LAN IP ☑ FW Version

☑ 3. Switch List

Configuration

1. Select Org-tree: this is the report data to collect from).
2. Dashboard Period: Select the day, week, or month data you want to display on the dashboard Data. eg: Throughput. Top series .)
3. Throughput SSID: Select the SSID you want to collect on throughput data)
4. Schedule: Select the report to be generated right now or Specific time or weekly)
5. Email: Enter the recipient's email address that you want to send the report)



Configuration

Select Org-tree: james

Dashboard Period (Dashboard): Day

Throughput SSID (Dashboard): All

Schedule: Weekly

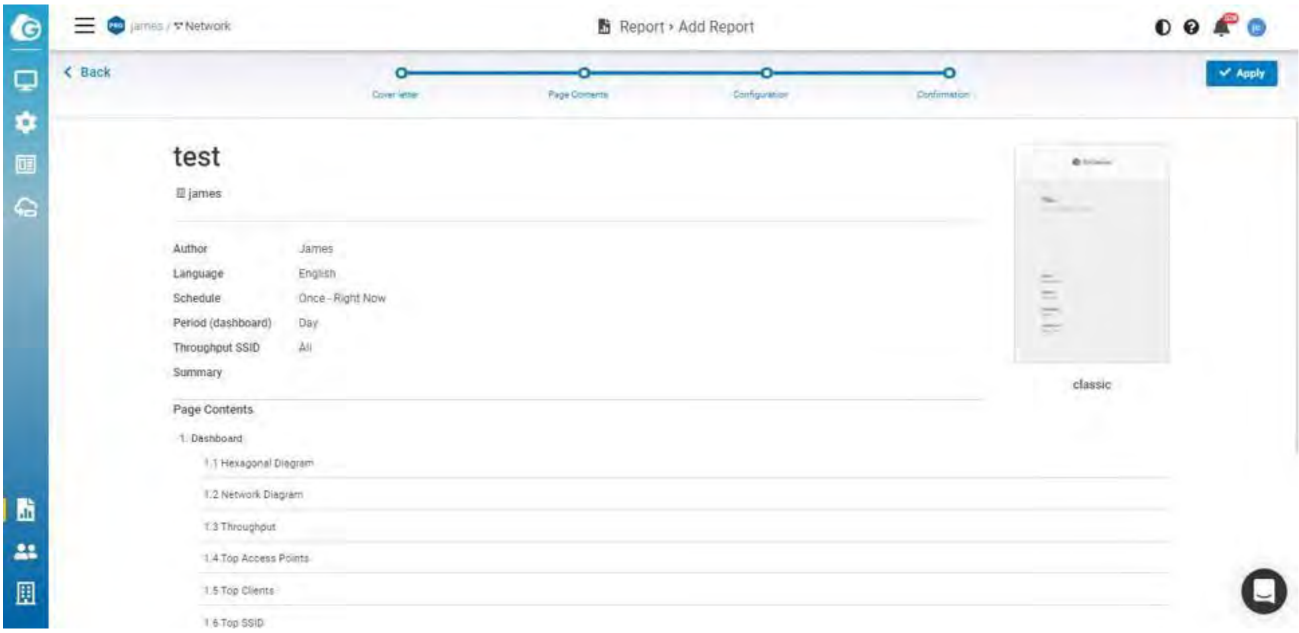
Weekday: Monday

Time (Asia/Taipei): 13:00

Email

Confirmation

This allows you to review all the page contents and settings on a single page. If you want to change the settings, you could click back to change. If all the settings are OK, click Apply to create a task.



test

james

Author James
Language English
Schedule Once - Right Now
Period (dashboard) Day
Throughput SSID All
Summary

Page Contents

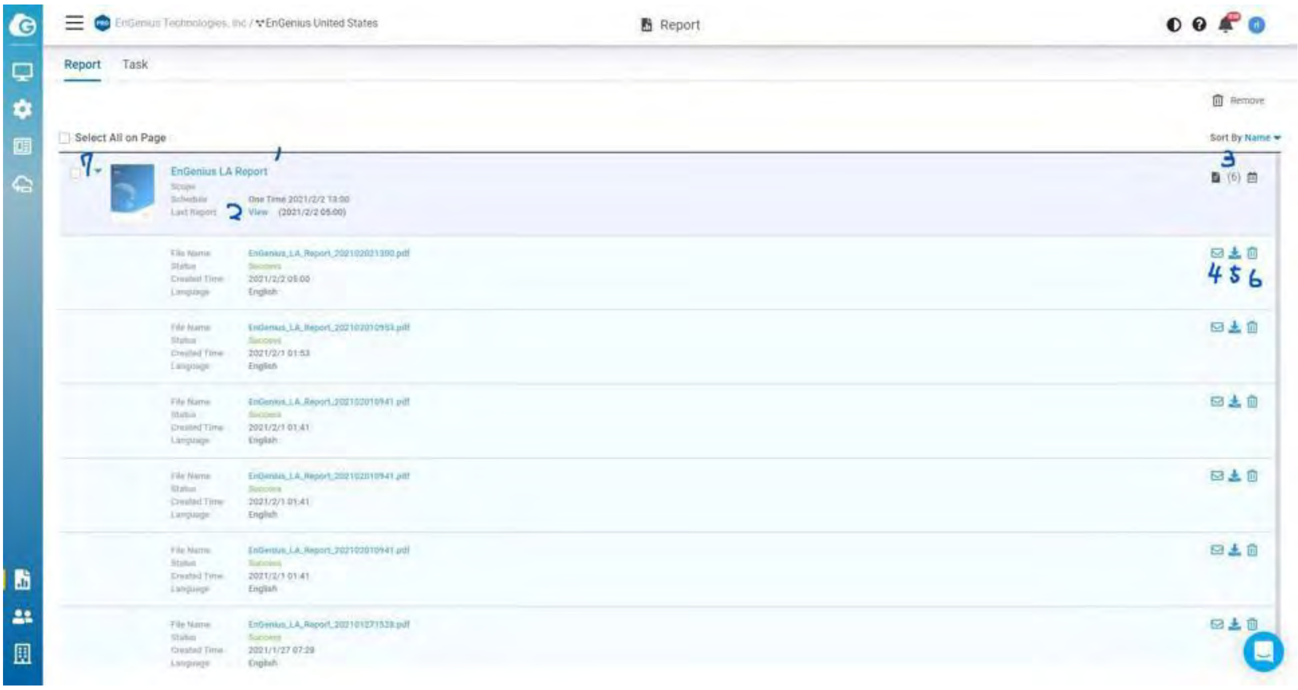
1. Dashboard
1.1 Hexagonal Diagram
1.2 Network Diagram
1.3 Throughput
1.4 Top Access Points
1.5 Top Clients
1.6 Top SSID

Reports View

The Report Tab displayed the lists of reports that the system has generated based on your task.

When you open a saved report from Report Tab, Insightly will run the report and display:

1. Task name (same as report name): Click to navigate to corresponding tasks.
2. Last report: You can easily download the last generated report by hyperlink.
3. Numbers of reports generated by same tasks.
4. Allows you to email this report to someone.
5. Download report.
6. Delete report.



EnGenius LA Report
Scope
Schedule One Time 2021/2/2 13:00
Last Report View (2021/2/2 05:00)

File Name EnGenius_LA_Report_202102021300.pdf
Status Success
Created Time 2021/2/2 05:00
Language English

File Name EnGenius_LA_Report_202102010953.pdf
Status Success
Created Time 2021/2/1 01:53
Language English

File Name EnGenius_LA_Report_202102010941.pdf
Status Success
Created Time 2021/2/1 01:41
Language English

File Name EnGenius_LA_Report_202102010941.pdf
Status Success
Created Time 2021/2/1 01:41
Language English

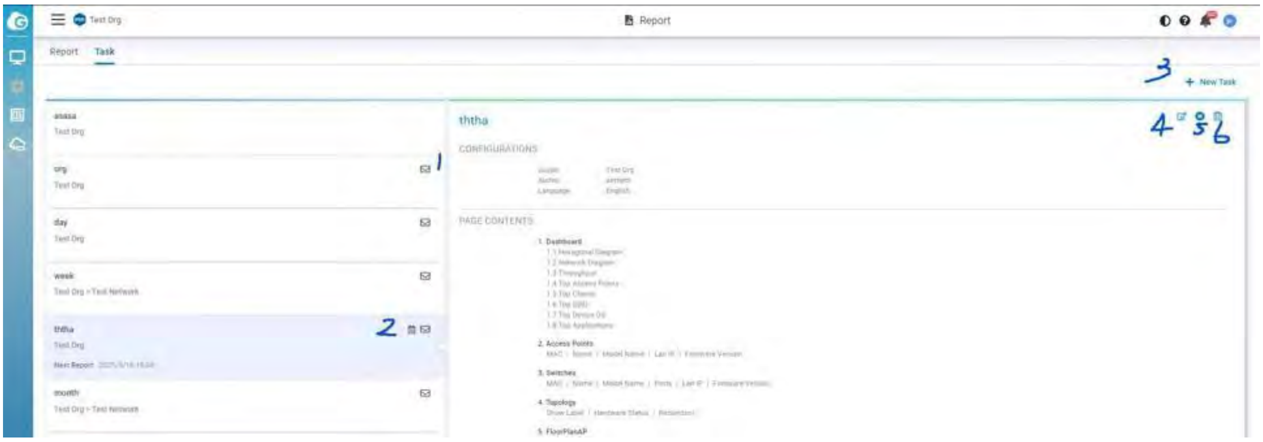
File Name EnGenius_LA_Report_202102010941.pdf
Status Success
Created Time 2021/2/1 01:41
Language English

File Name EnGenius_LA_Report_202101271528.pdf
Status Success
Created Time 2021/1/27 07:29
Language English

Edit Task

After you created the Tasks, this page allows you to monitor the data that you have selected. There are some icons for you to know the task status and do further editing.

1. Mail icon: This task has some email recipients that have been configured.
2. Calendar icon: This task has been scheduled to generate a report continuously.
3. New Task: This allows you to create another task. The basic mode only allowing you to create a single task and only have one report recorded.
4. Edit icon: This allows you to edit the task settings.
5. Pause icon: This allows you to temporarily stop the scheduled task.



asasa
Test Org

org
Test Org

day
Test Org

week
Test Org > Test Network

ththa
Test Org
Next Report

month
Test Org > Test Network

ththa

Scope Test Org
Author
Language English

1. Dashboard
2. Access Points
3. Switches
4. Topology
5. FloorPlanAP

Access Point LED Behavior

Access Point LEDs and what they mean

The table below describes the LEDs on the access point, their flashing patterns, and what those mean for its function.

LED	Static	Flash	Off
Power	Power is on	Cloud is connecting	Power is off
LAN	Connected to LAN	Data is transmitting between AP and the Internet.	No connections to LAN
2.4G	AP is not transmitting data, Radio is on	AP is transmitting data between AP and client	Radio is off
5G	AP is not transmitting data, Radio is on	AP is transmitting data between AP and client	Radio is off

ⓘ If four LEDs are flashing, it means that AP is performing a firmware upgrade.

SSID Troubleshooting Naming Rules

There is a management SSID that lets users know the current status when an access point connects to EnGenius Cloud. If an access point has lost its connection to the Internet but still receives power, it will broadcast a management service set identifier (SSID) that can be connected to for administrative tasks.

Connect to the default SSID by completing the following steps:

1. Physically check that the access point has power.
2. Check if a known default SSID is being broadcast.
3. If a management SSID is being broadcast, connect your device to it.
4. After connecting, check your gateway IP address to connect to the local status page. If you can't find the gateway IP, please make sure the access point is in NAT mode.

Management SSIDS

<EnMGMTxxxx>-SSID_name>-No_Eth

Cause: AP does not have Ethernet connection.

Solution: Check if the Ethernet cable is unplugged.

<EnMGMTxxxx>-No_IP

Cause: AP cannot get an IP address from 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 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 seems to be working, but a connection to EnGenius Cloud cannot be established.

Solution: Check EnGenius Cloud server status with EnGenius.

Firewall rules

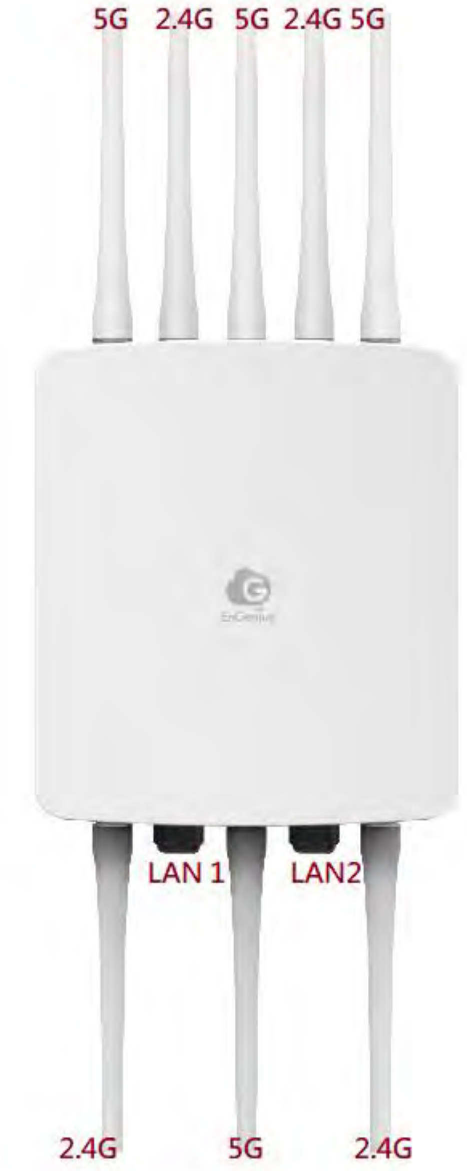
Below is the Firewall rules which is needed to access EnGenius Cloud.

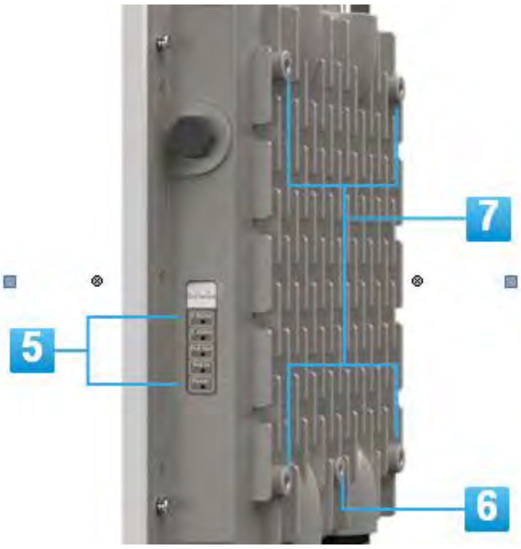
Cloud Devices	Cloud Services	Source IP	Destination IP	Ports	Protocol (TCP/UD
AP, SW , Ensky	Periodical Cloud communication,Firmware Upgrade,Real-Time Meter	Your Networks	any	443	TCP
AP, SW , Ensky	Persistent Cloud communication	Your Networks	44.224.197.174	80	TCP
AP	Cloud Radius	Your Networks	44.225.123.183	1812/1813	TCP & UD
AP, SW , Ensky	NTP time sychronization	Your Networks	any	123	UDP
AP, SW , Ensky	Remote Tunnel	Your Networks	44.230.110.152	22	TCP
AP	Splash Page	Your Networks	any	80/443	TCP

Physical Interface

1 2.4 GHz Antennas: Detachable 5 dBi 2.4 GHz Omni-directional
2 5 GHz Antennas Detachable 7 dBi 5 GHz Omni-directional
3 LAN Port 1 (802.3bt PoE Input): Ethernet port for RJ-45 cable.
4 LAN Port 2 (802.3af PSE Output): Ethernet port for RJ-45 cable.

5 LED Indicators: LED lights for Power, LAN Port 1, LAN Port 2,2.4 GHz Connection and 5 GHz Connection.
6 Ground
7 Mounting Holes: Using the provided hardware, the ECW270 can be attached to a wall or pole.



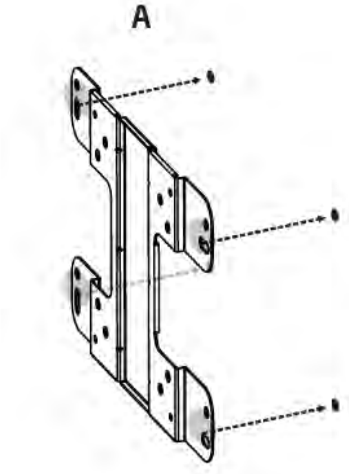


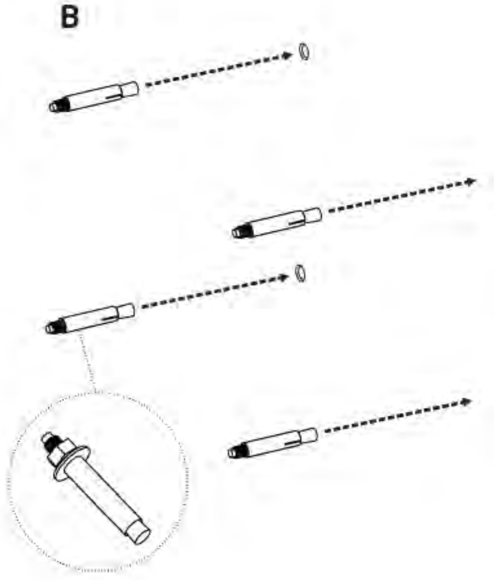
Wall Mounting the Outdoor Device

Using the provided hardware, the AP can be attached to a wall

(A) Determine where the AP is to be placed and mark location on the surface for the four mounting holes. You may adjust the position with a level.

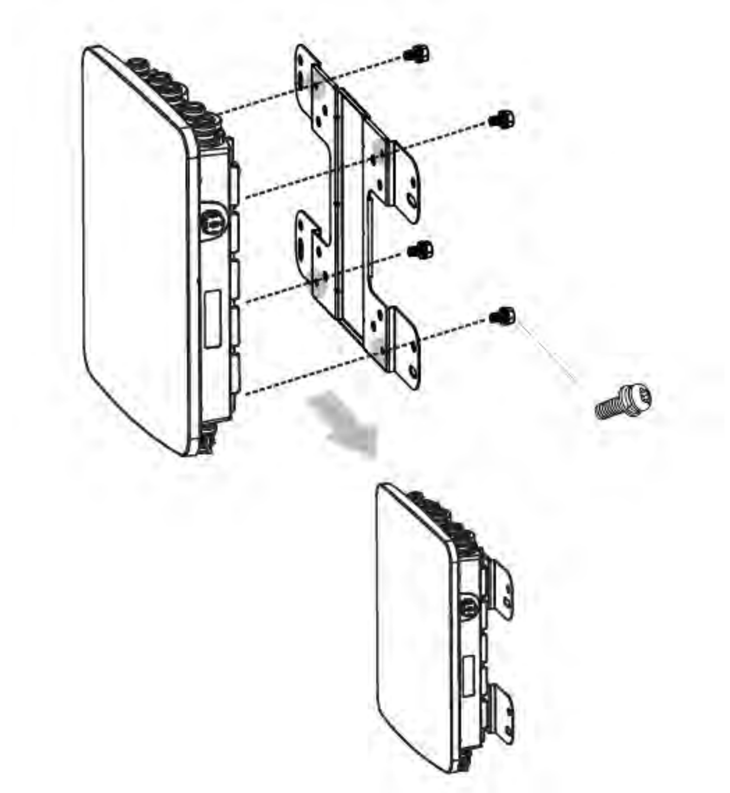
(B) Use the appropriate drill bit to drill four 8mm diagram and 37mm depth holes in the markings and hammer the bolts into the openings.





SCREW P4*8(ISO)(SW)(SUS)

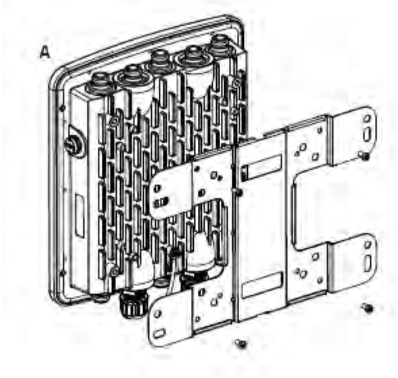
(C) Place the lock and flat washer on the round head screws and drive the screws to attach mounting base to the back of the Access Point.



Pole Mounting the Outdoor Device

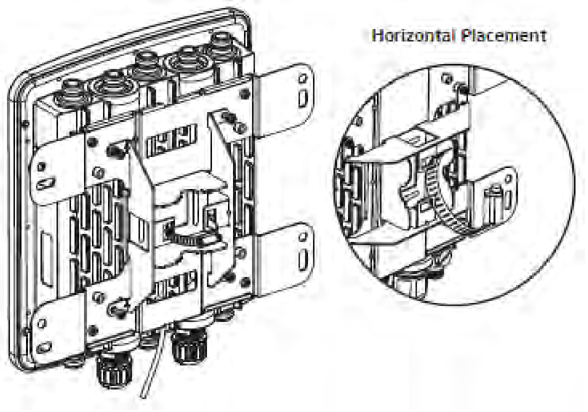
A) Place the lock and flat washer on the cap screws and drive the

screws to attach the mounting base to the back of the Access Point.



C) Thread the open end of the Pole Strap through the two tabs on

the Pole Mount Bracket.



SCREW

P4*8(ISO)(SW)(SUS)18

Housing dimension 249.6*217.7*53.7mm

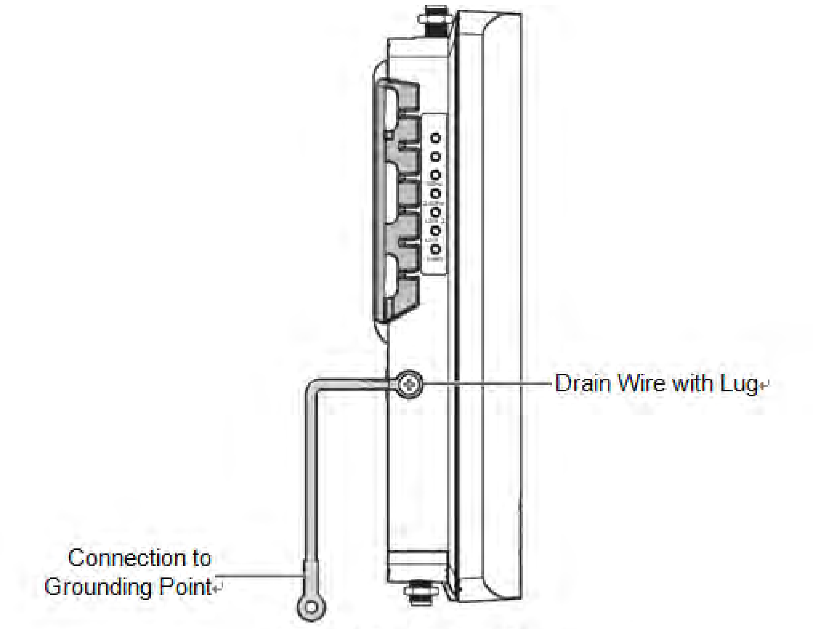
Grounding Connection

The following information provides installation and recommendations for grounding of the device. Before starting the installation procedure, read the following information:

■ The Yellow Green cable is not recommended for use in grounding.

■ Ensure the cable with a core diameter of 2 mm exceeds a length of 50 cm from connection point to ground.

Electromagnetic Interference (EMI) affects the transmission performance of a device. By properly grounding the device to earth ground through a drain wire, you can setup the best possible noise immunity and emissions.



Grounding Connection

Appendix A - FCC Interference Statement

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.Section 15.204(b) states that an approved "transmission system" must always be marketed as a complete system including the antenna.

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

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

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR MOBILE DEVICE USAGE (>20cm/low power)

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Appendix B - Professional Installation Instruction (FCC)

Professional installation instruction

1. Installation personal
   This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.
2. Installation location
   The product shall be installed at a location where the radiating antenna can be kept 20cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.
3. External antenna
   Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.
4. Installation procedure
   Please refer to user’s manual for the detail.
5. Warning
   Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.

Warning:

In order to make sure that the final output power does not exceed the limit set force in relevant rules, please carefully select the installation position and the installation angle of antenna must be vertical to the ground. The violation of the rule could lead to serious federal penalty.

Appendix C - IC Interference Statement

Industry Canada statement

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

FOR MOBILE DEVICE USAGE (>20cm/low power)
Radiation Exposure Statement:
This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:
Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 20 cm entre le radiateur et votre corps.

Caution:

(ii) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; (detachable antenna only)

Avertissement:

(ii) pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas; (detachable antenna only)

Appendix D

Professional installation instruction

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

2. Installation location
   The product shall be installed at a location where the radiating antenna can be kept 20cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna
   Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of ISED limit and is prohibited.

4. Installation procedure
   Please refer to user’s manual for the detail.

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

Instructions d'installation professionnelle

1. Installation

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

2. Emplacement d'installation

En usage normal, afin de respecter les exigences reglementaires concernant l'exposition aux radiofrequences, ce produit doit etre installe de facon a respecter une distance de 20 cm entre l'antenne emettrice et les personnes.

3. Antenn externe.

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

4. Procedure d'installation

Consulter le manuel d'utilisation.

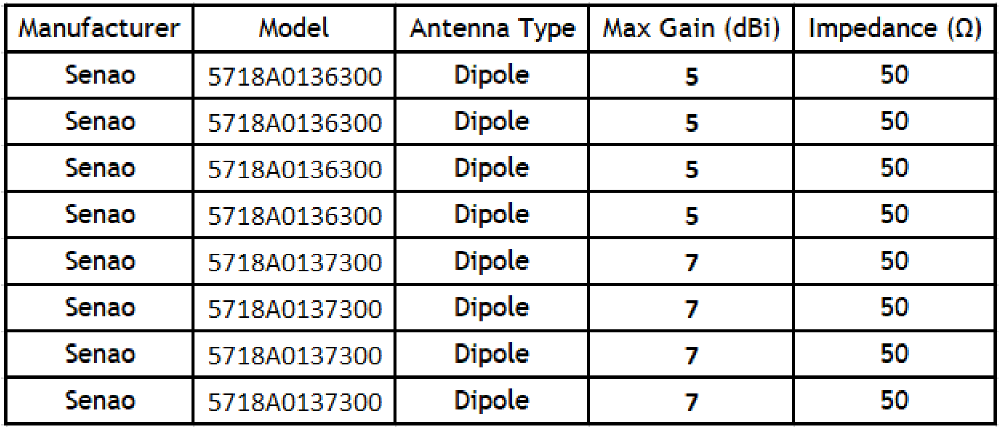
5. Avertissement

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

DETACHABLE ANTENNA USAGE

This radio transmitter [IC: 10103A-ECW270] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 10103A-ECW270] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.



Manufacturer	Model	Antenna Type	Max Gain (dBi)	Impedance (Ω)
Senao	5718A0136300	Dipole	5	50
Senao	5718A0136300	Dipole	5	50
Senao	5718A0136300	Dipole	5	50
Senao	5718A0136300	Dipole	5	50
Senao	5718A0137300	Dipole	7	50
Senao	5718A0137300	Dipole	7	50
Senao	5718A0137300	Dipole	7	50
Senao	5718A0137300	Dipole	7	50