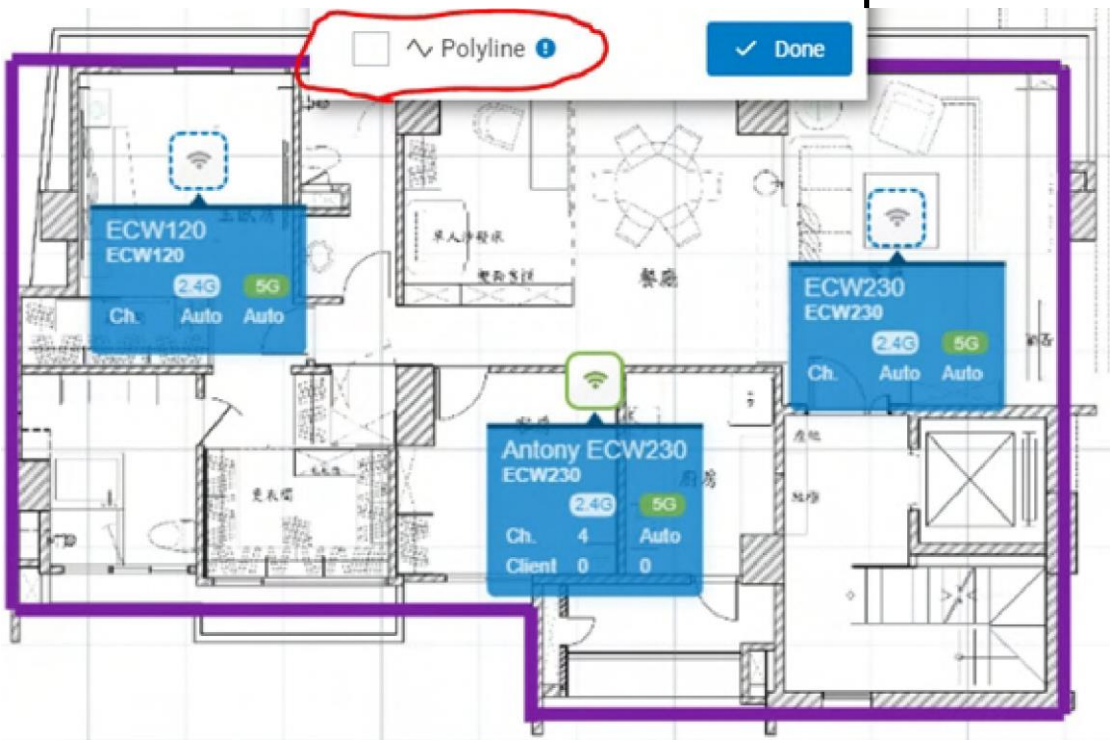
ADD OBSTANCE

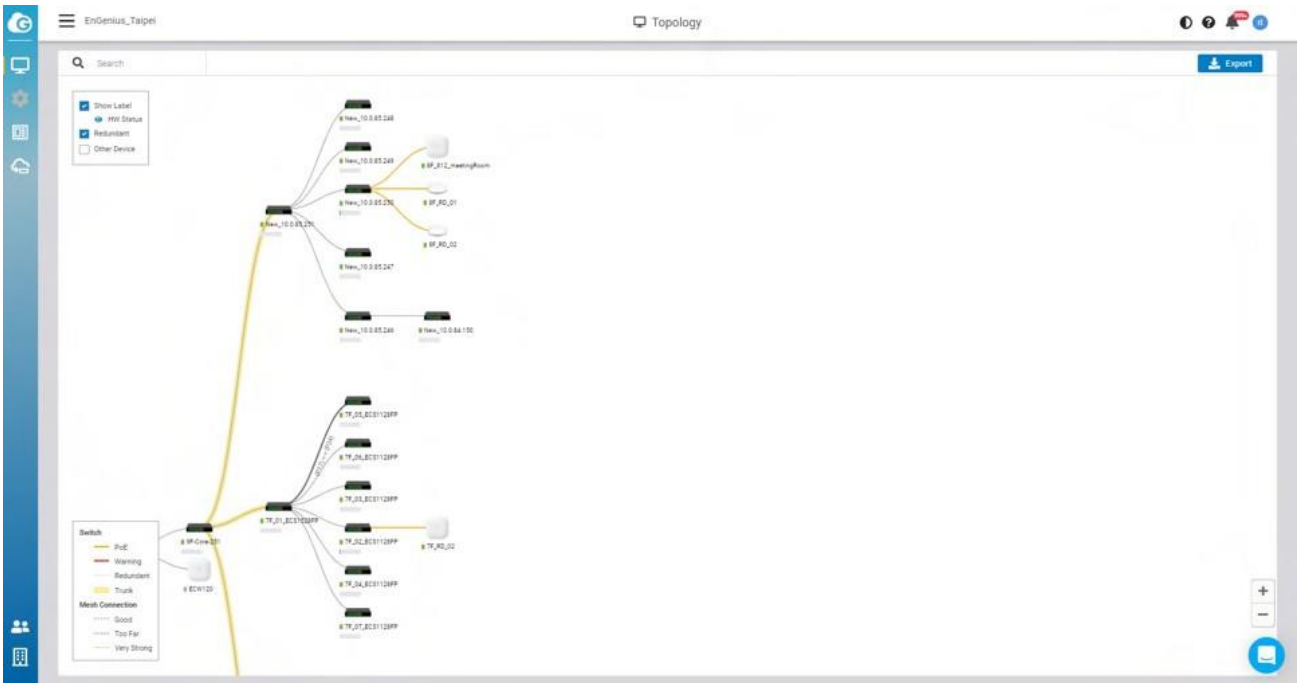
Concrete Wall (12dB)



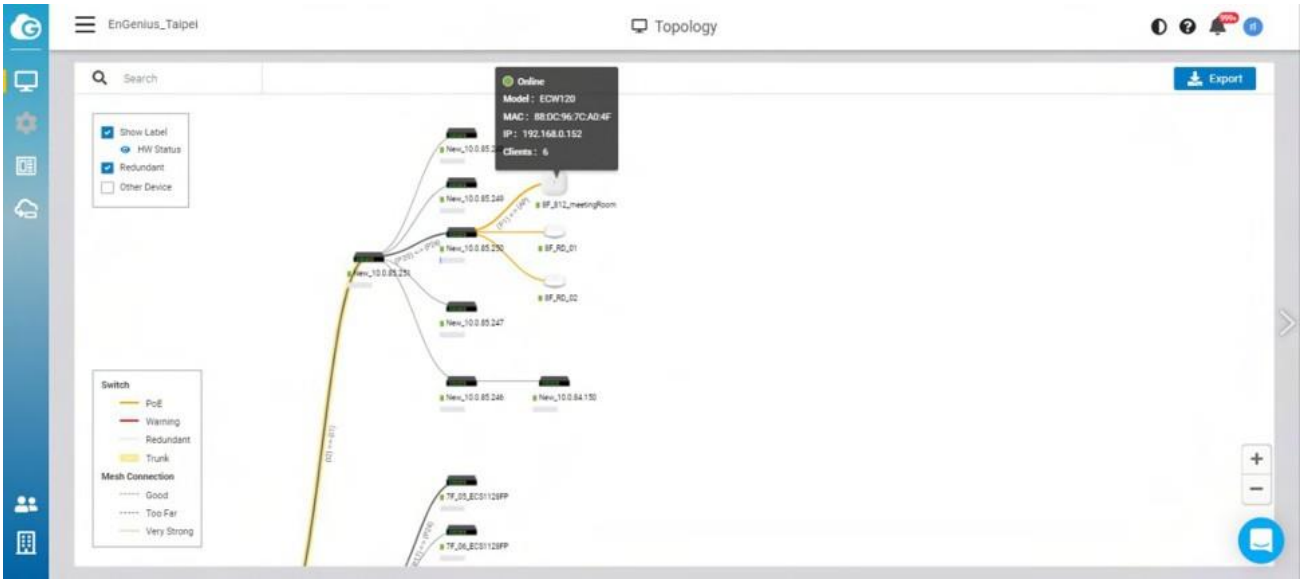
Topology

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

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



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



The following describes the functions on this screen:

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

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

Redundant : Click to display or hide the redundant link .

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

Export : Click to download topology as PDF format .

Configuring Networks

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

Configuring SSIDs

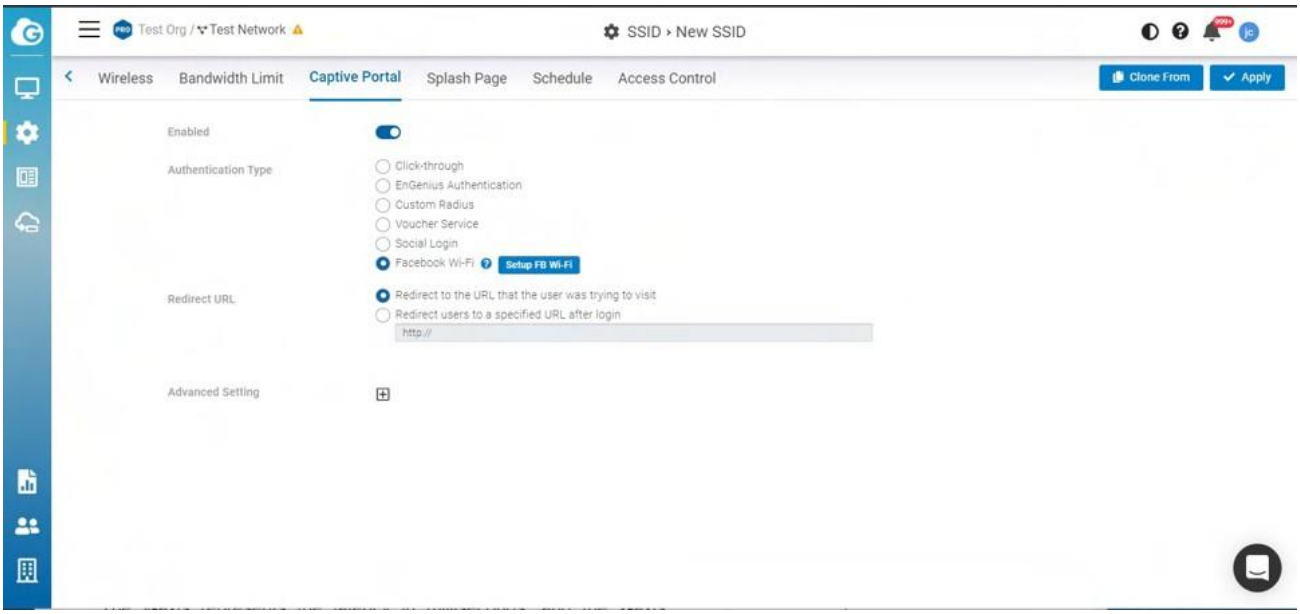
Facebook Wi-Fi

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

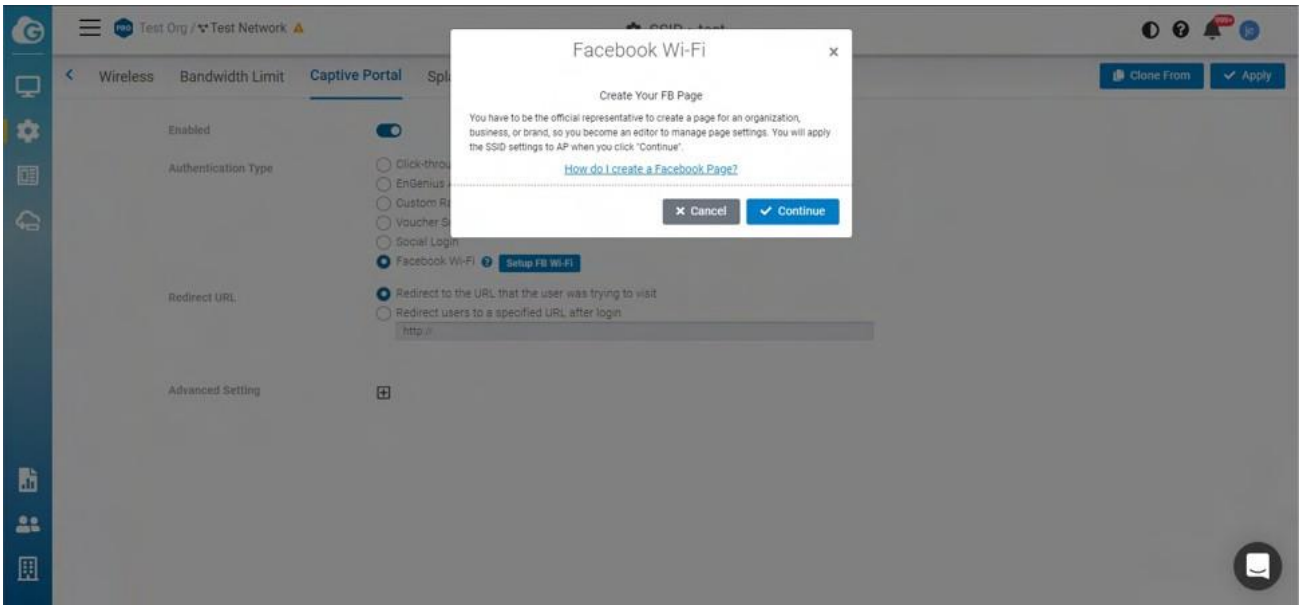
Configuring EnGenius Wi-Fi with Facebook Login

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

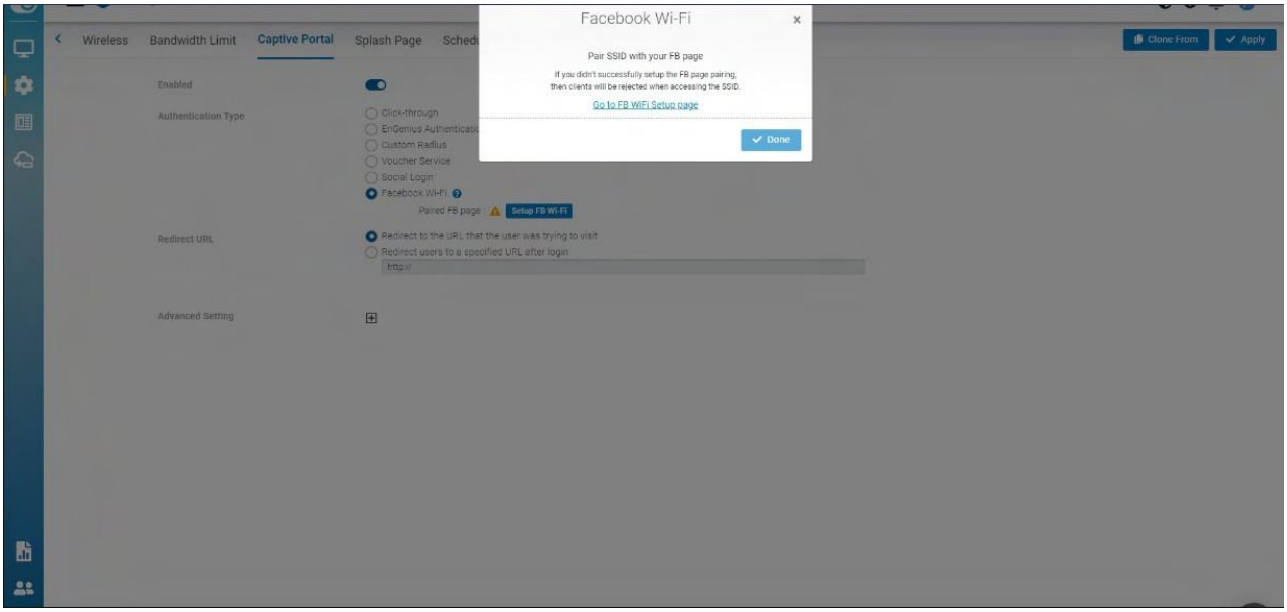
1. Select **Facebook Wi-Fi** under the **Authentication Type** section and click the **Setup Facebook Wi-Fi** button:



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

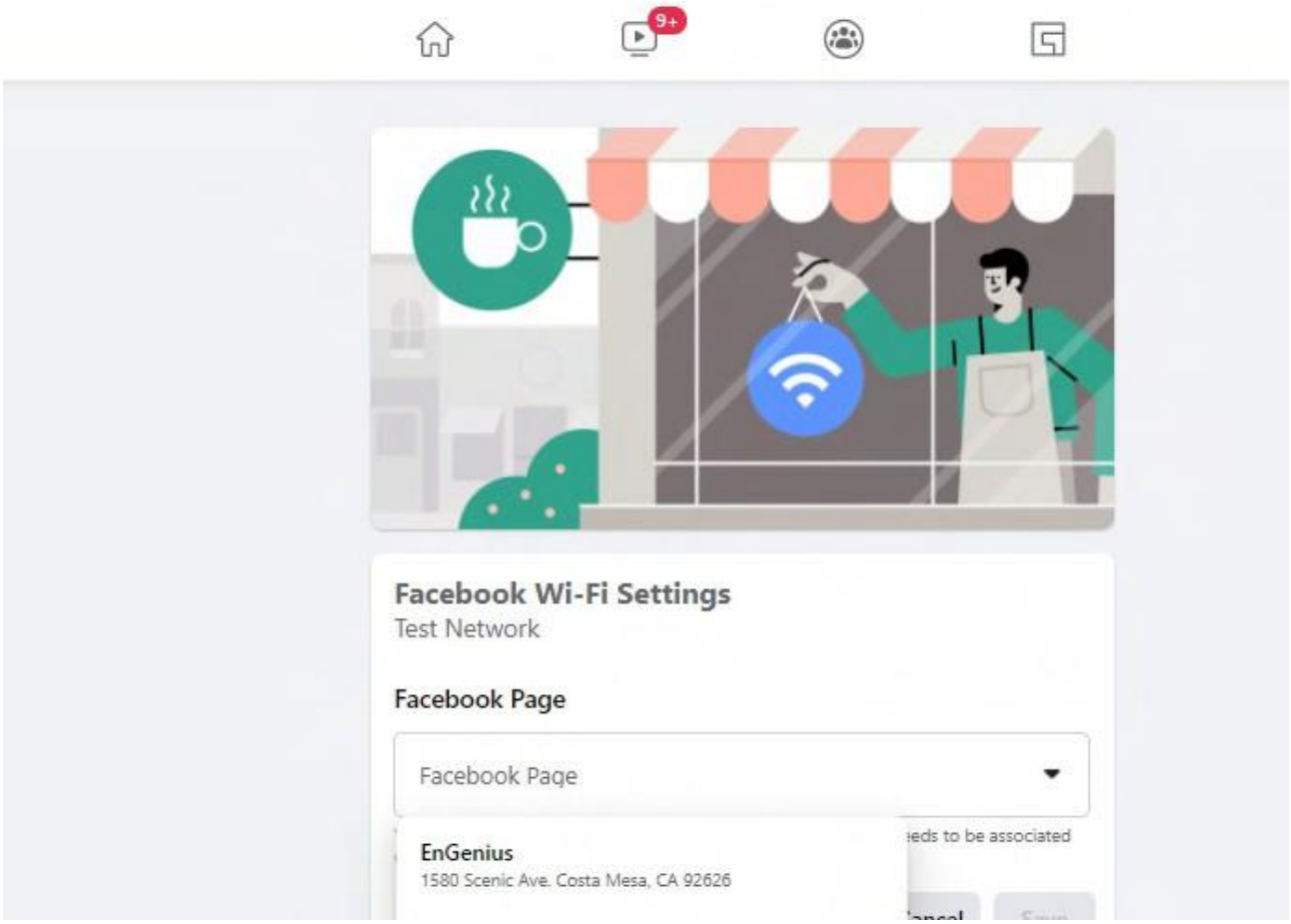


3. You will now see a link '**Go to FB Wi-Fi Setup page**'. Clicking on this link will take you to your Facebook Wi-Fi settings page.

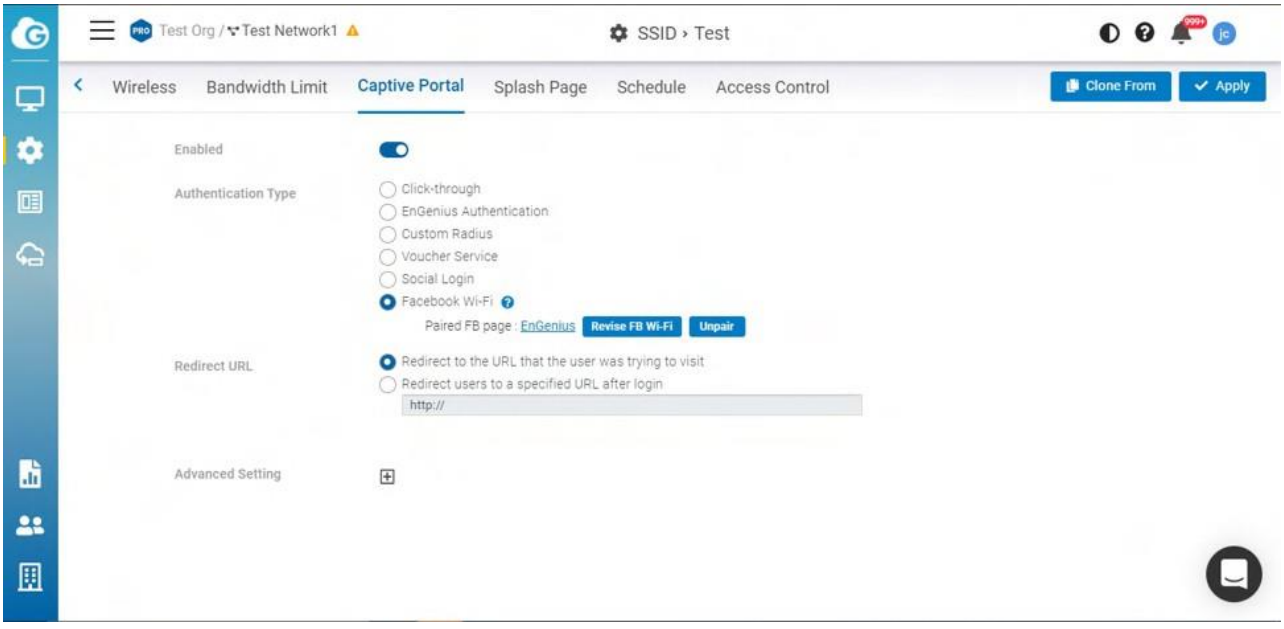


4.

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:



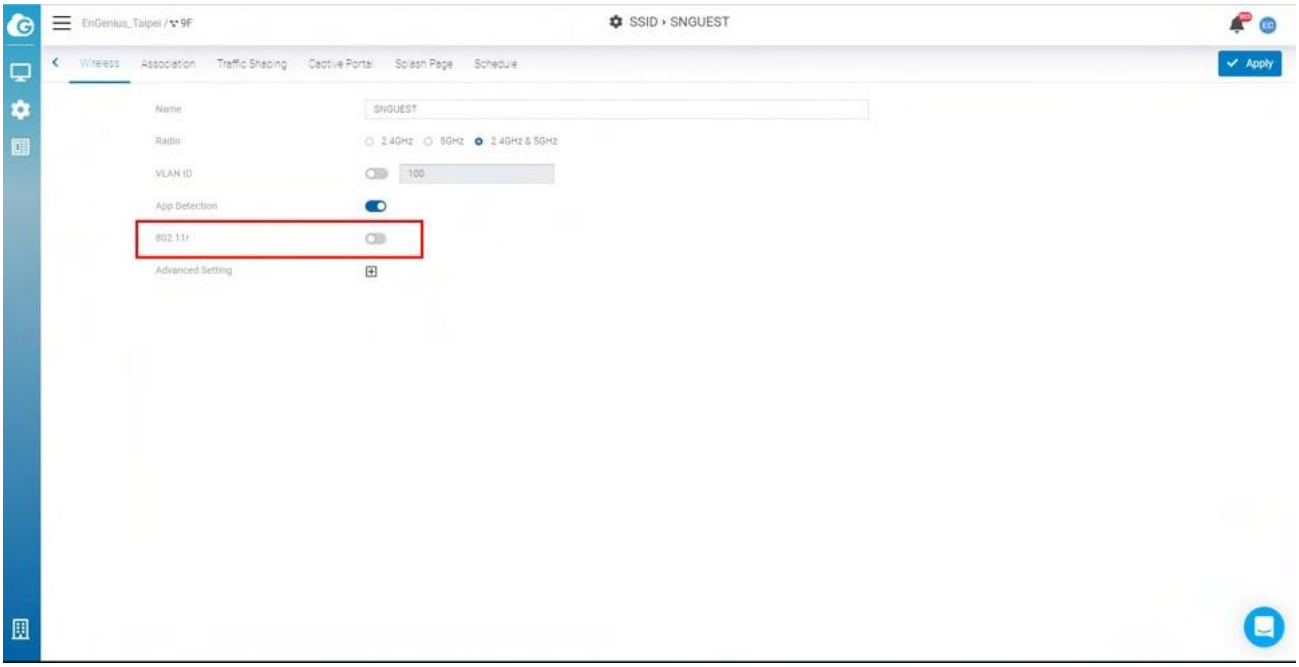
5. Once your Facebook page has been successfully paired with your SSID, the SSID page will update the Facebook Wi-Fi section with information about the paired page, along with an option to **Unpair**.



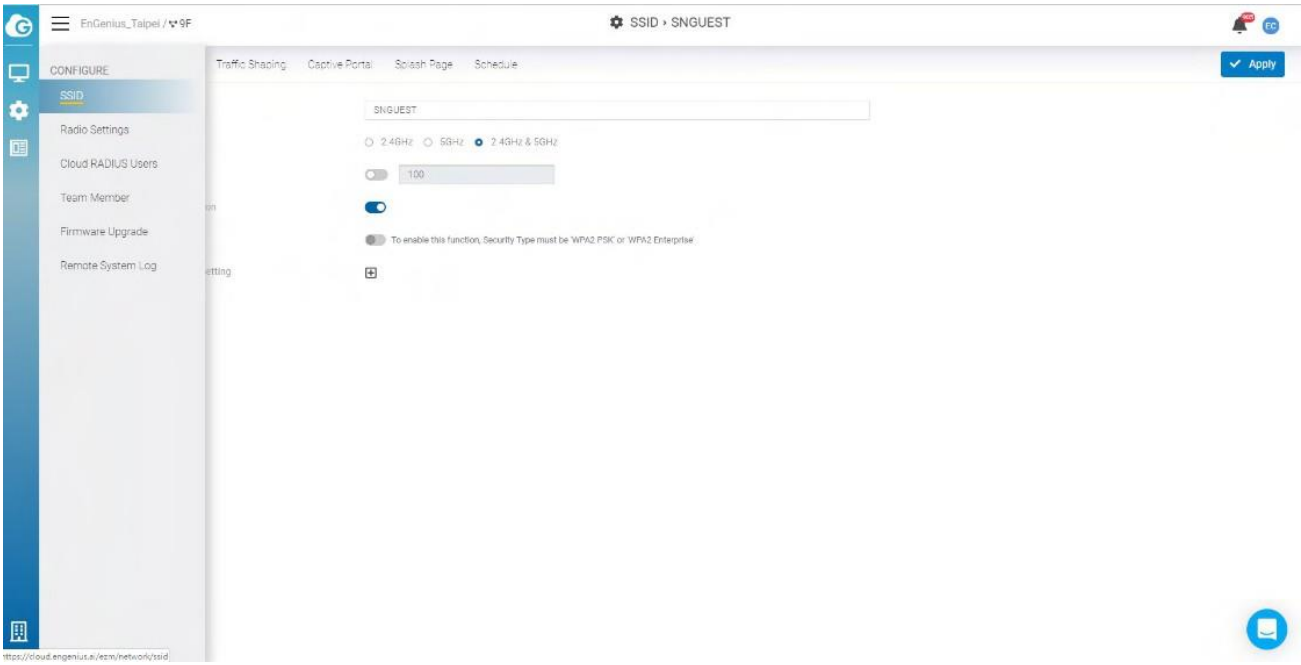
802.11 Settings

802.11r

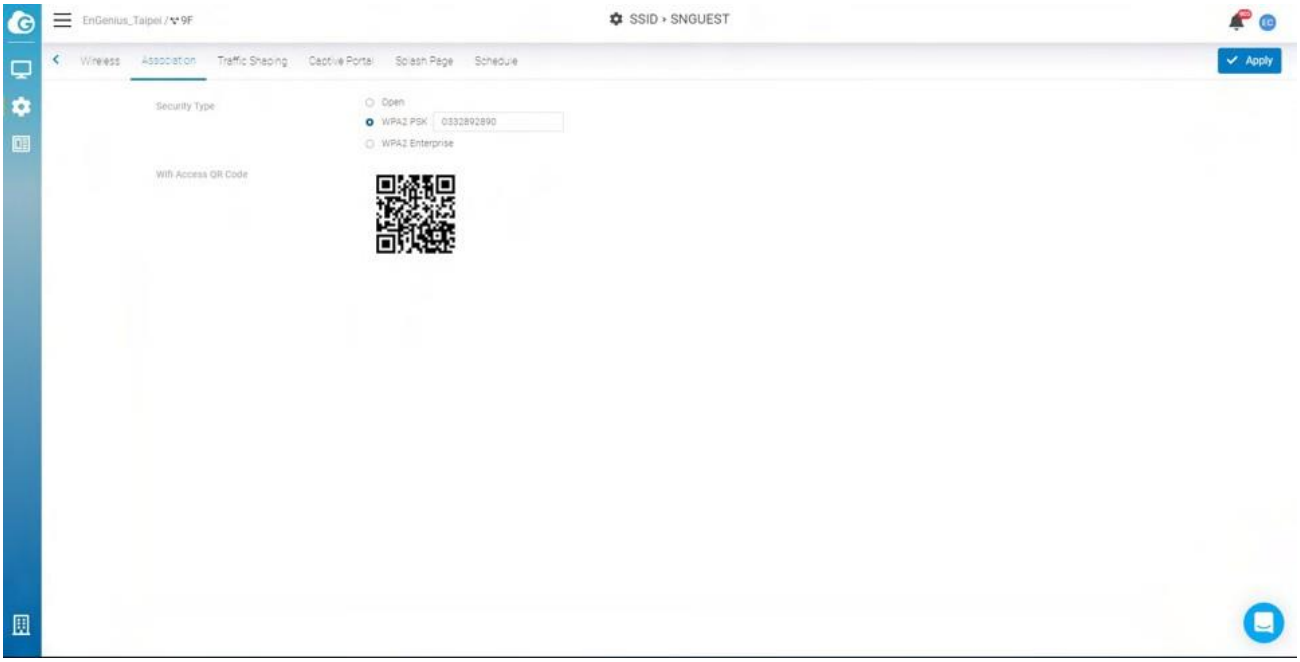
802.11r is a standards-based fast roaming technology that is leveraged when using a secure SSID (WPA2-PSK & WPA2-Enterprise). This option improves client device roaming by reducing the handoff delay in situations where client devices roam from one access point to another. 802.11r is disabled by default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



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



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



802.11w

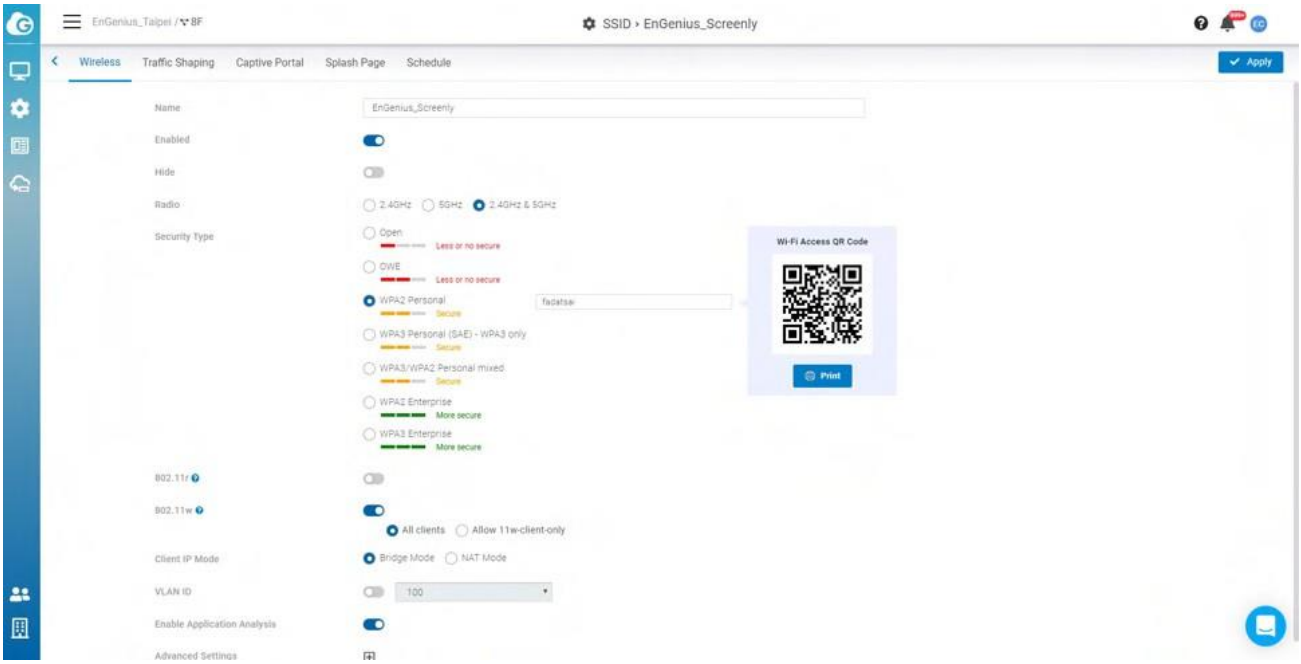
802.11w is enabled when Security Type is **not Open**. **802.11w** enables Protected Management Frames (PMF) for management frames such as authentication, de-

authentication, 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.



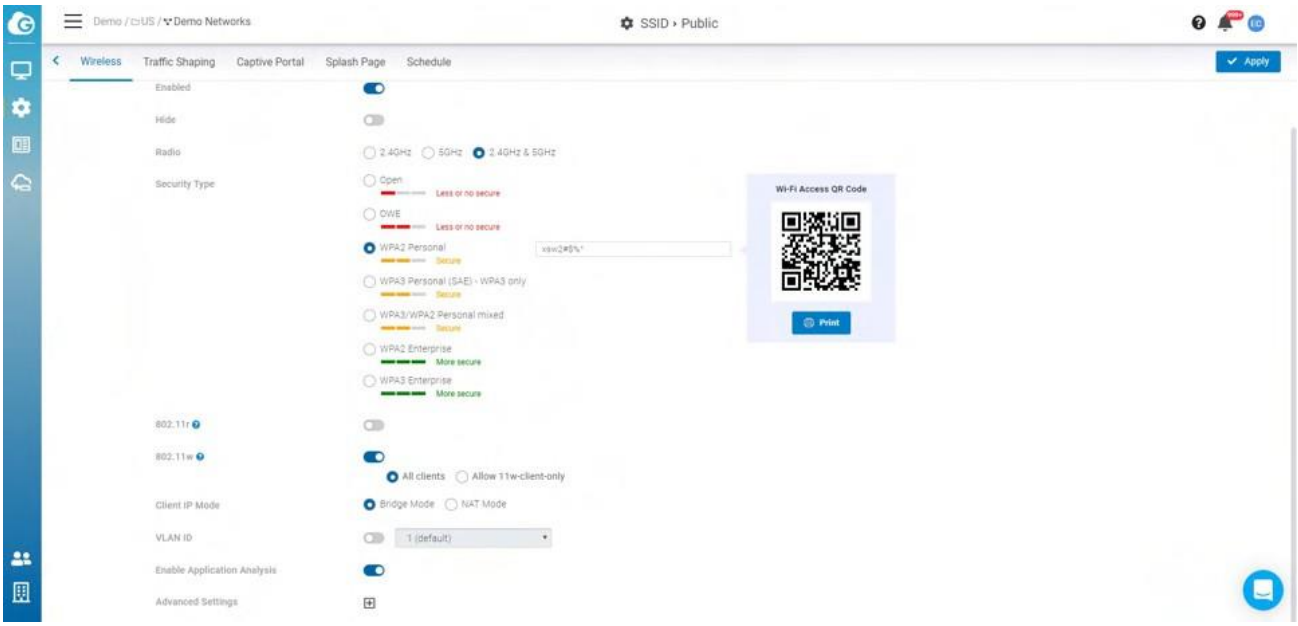
The following describes the authentication types on this screen:

- **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.



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:

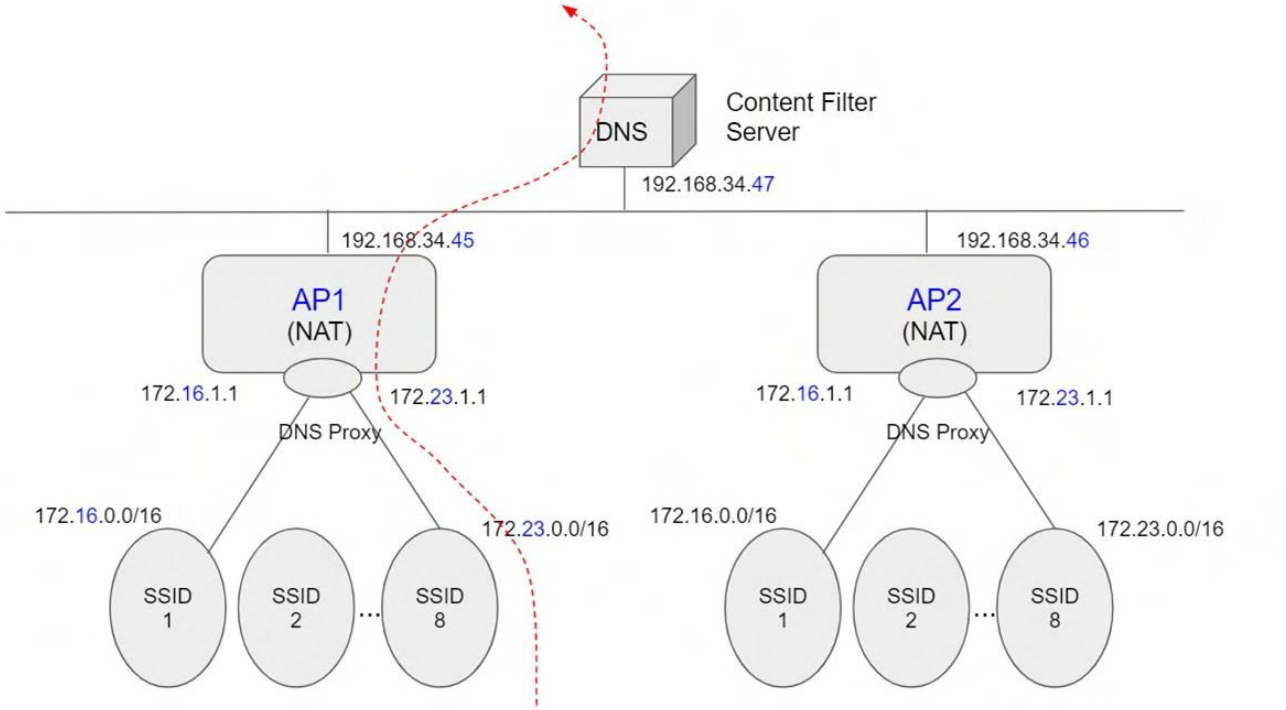
1. No NAT client can be talked to the other NAT client, neither same SSID nor different SSID (client isolation enabled and block internal routing)
2. Change the IP range of CP DNS to be same as AP DNS (172.16-23.0.0/16)

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.



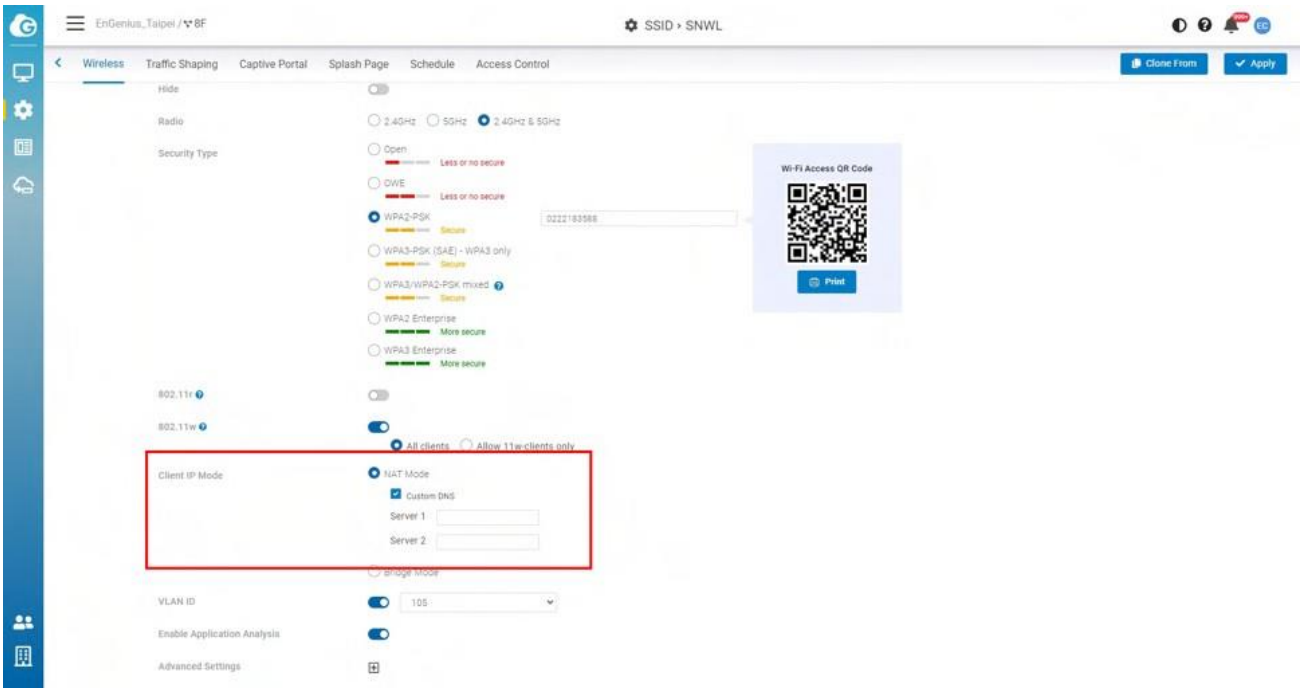
Configuring Custom DNS for an SSID in NAT Mode

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.**



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.

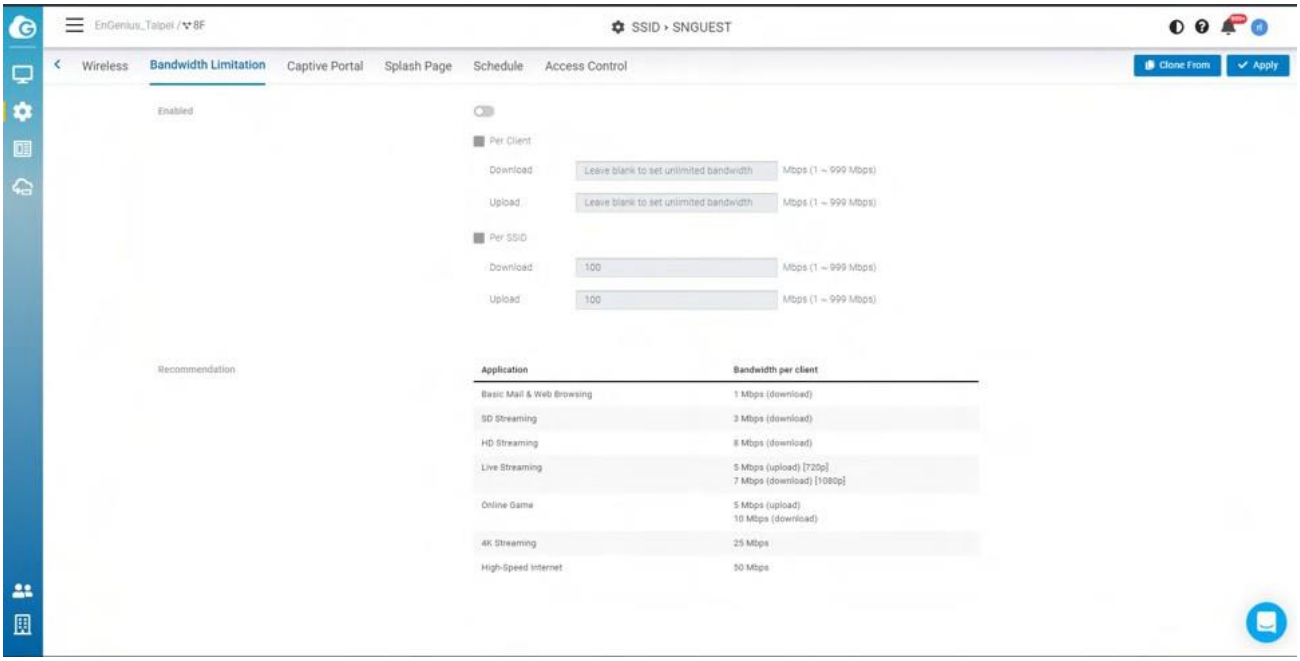
QoS

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.



Download Limit

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

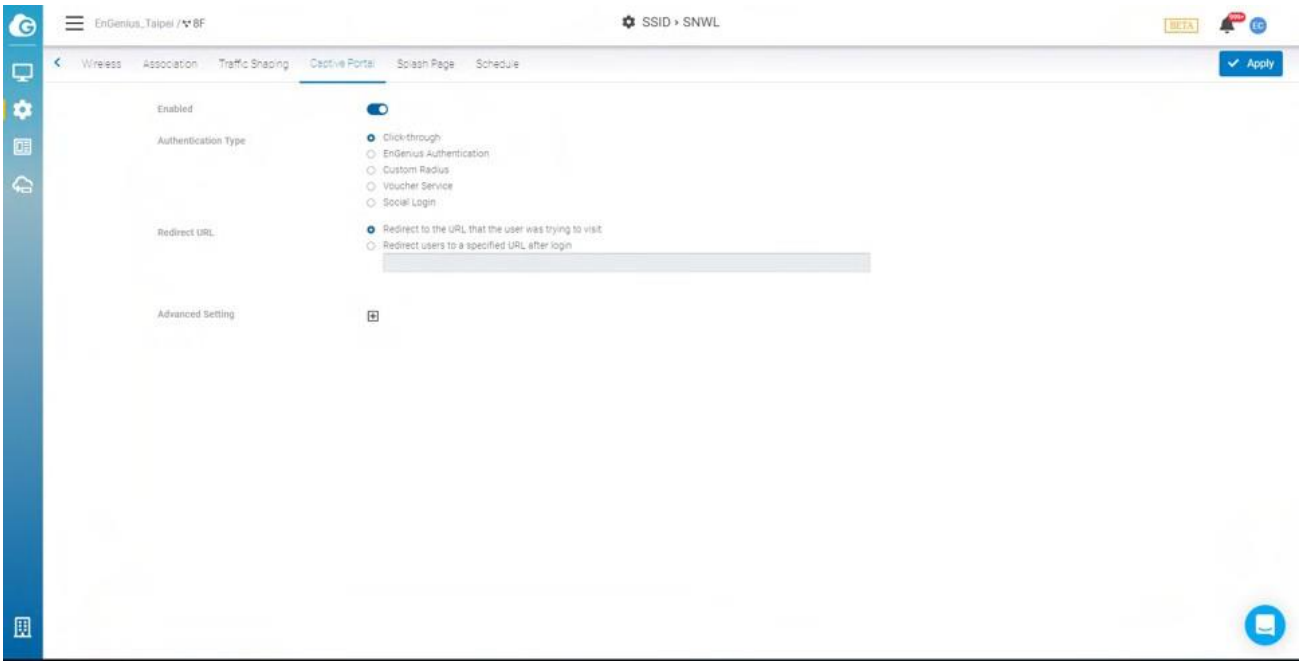
Upload Limit

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.



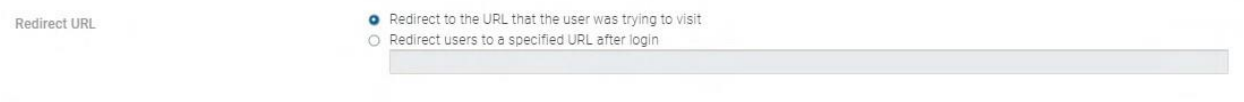
Authentication Type

- **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 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: 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.

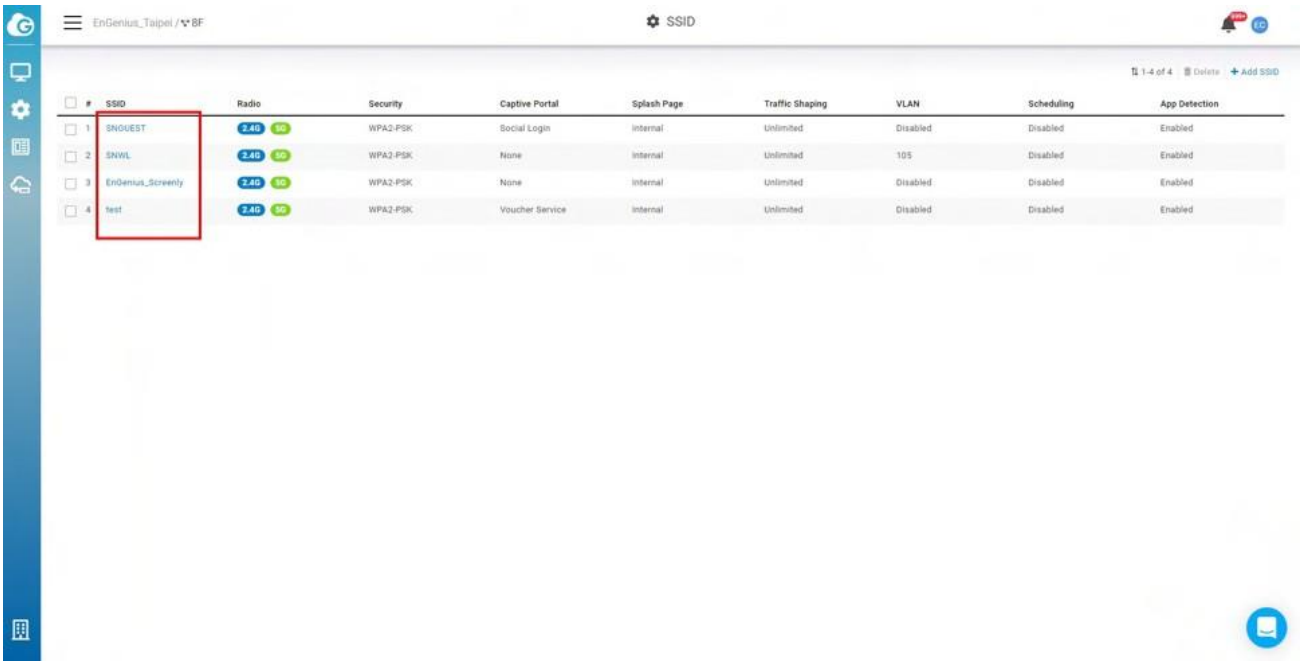
HTTPS Login: This option allows users to log in through HTTPS. When you enable it, your password is encrypted, so others could not retrieve your information.

Social Login

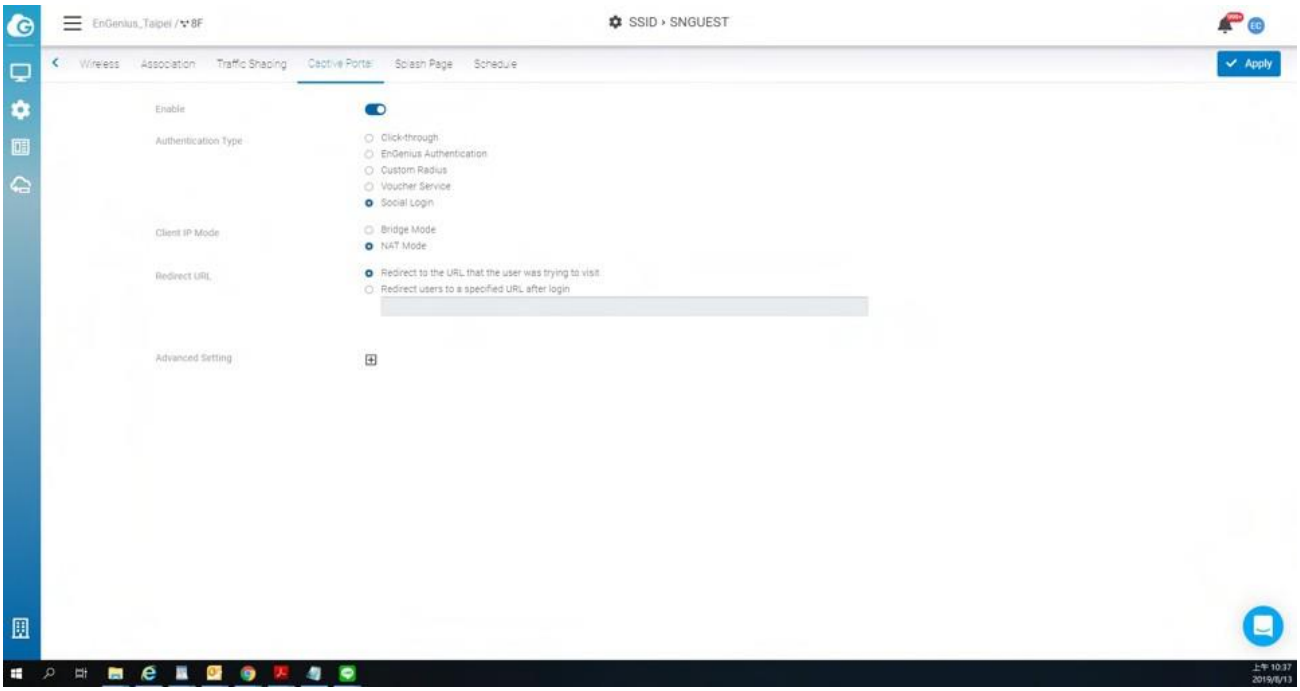
Social login allows you to use your Facebook account to access WiFi.

Follow the below steps to configure social login.

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



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



3. Click **Apply.**

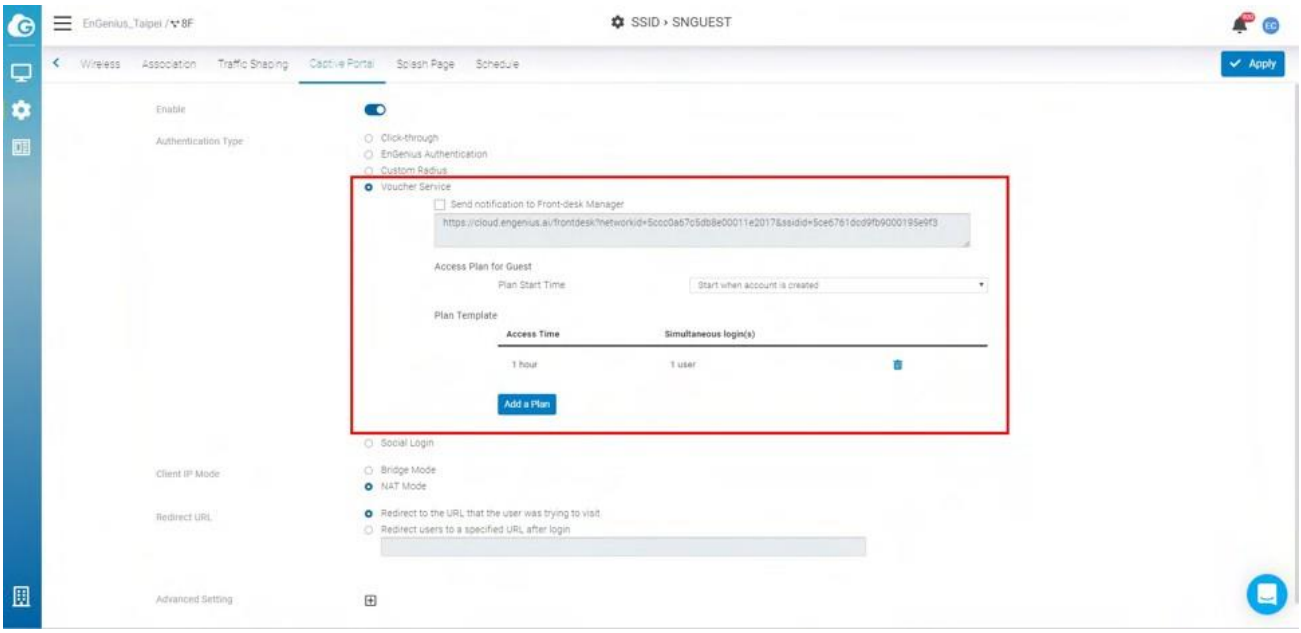
Voucher Service

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**.



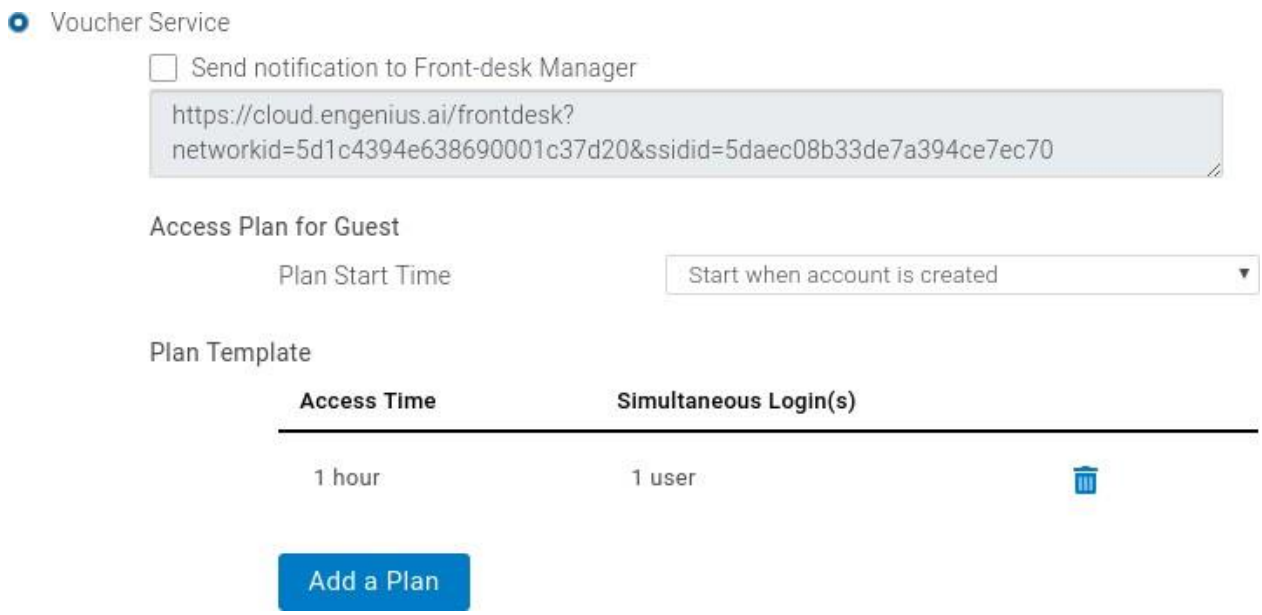
> Note: Please make sure that **Security Type** at **Configure > SSID > Association** has been configured as **open** or **WPA2 PSK** before trying to enable Voucher Service. Since Voucher Service is capable of generating user/password randomly, it can not work with a dedicated WPA2 Enterprise authentication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

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

Management URL and Access Plan

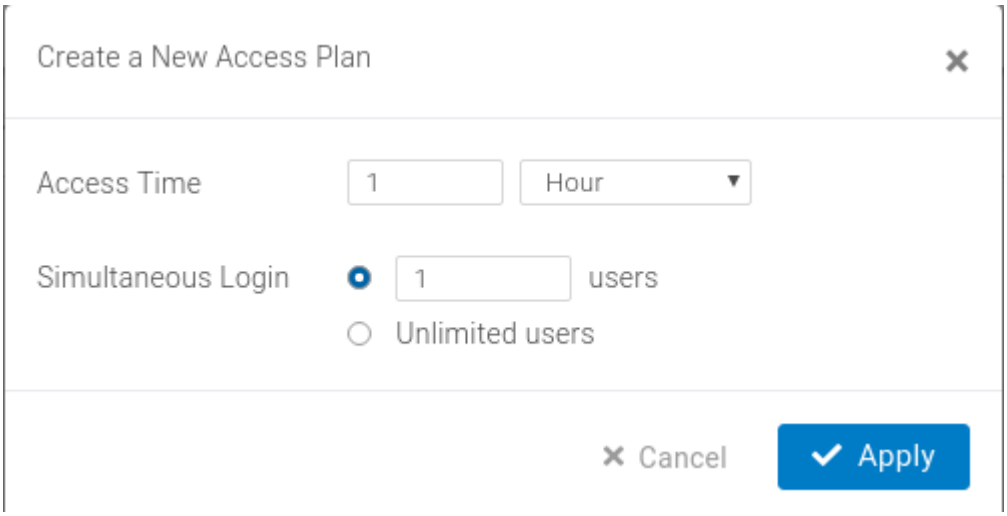
Management URL

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.



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**).



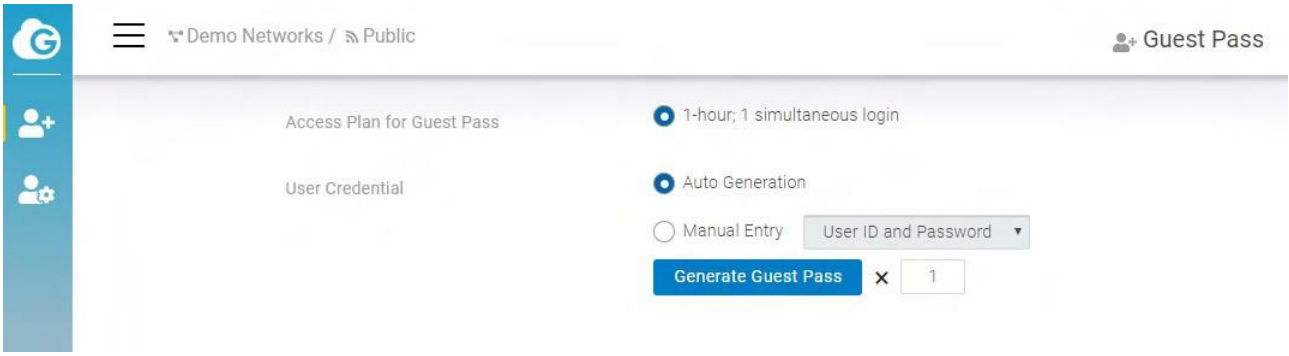
Plan Start Time

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:



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.

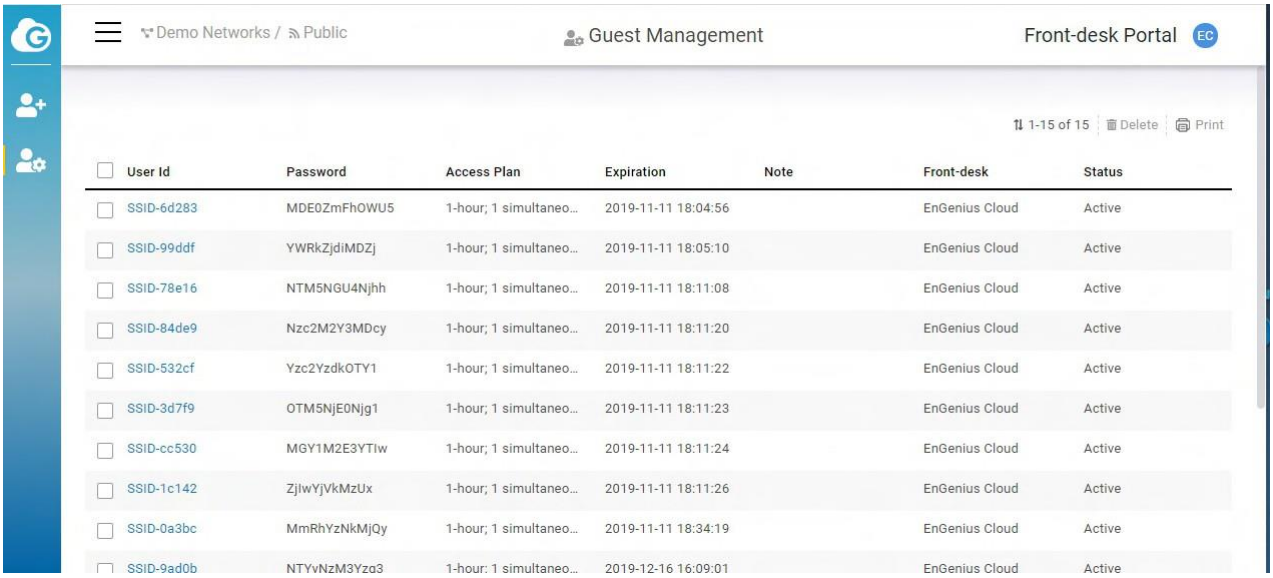
Managing Voucher User

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.



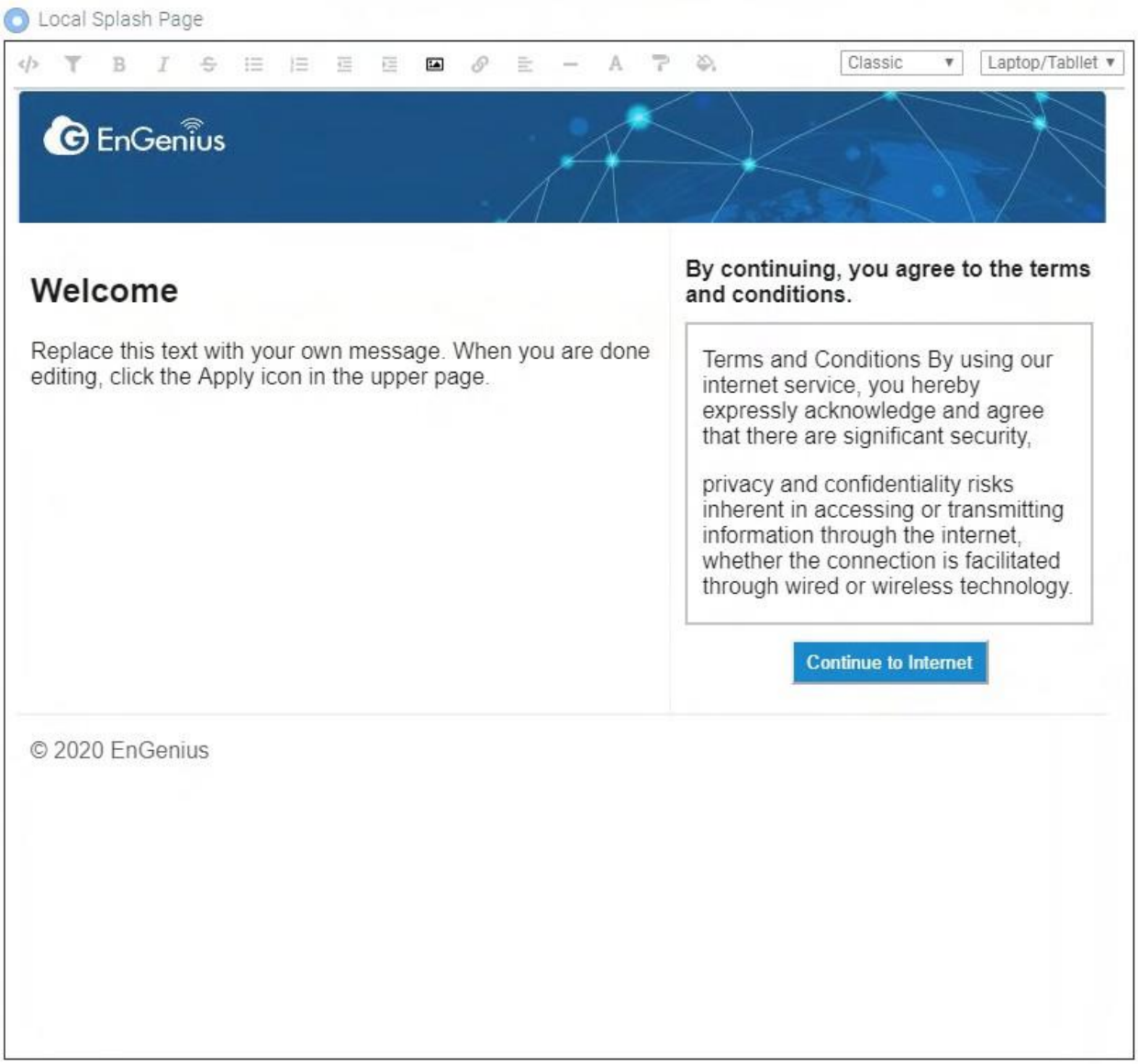
Configuring Splash Page

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.



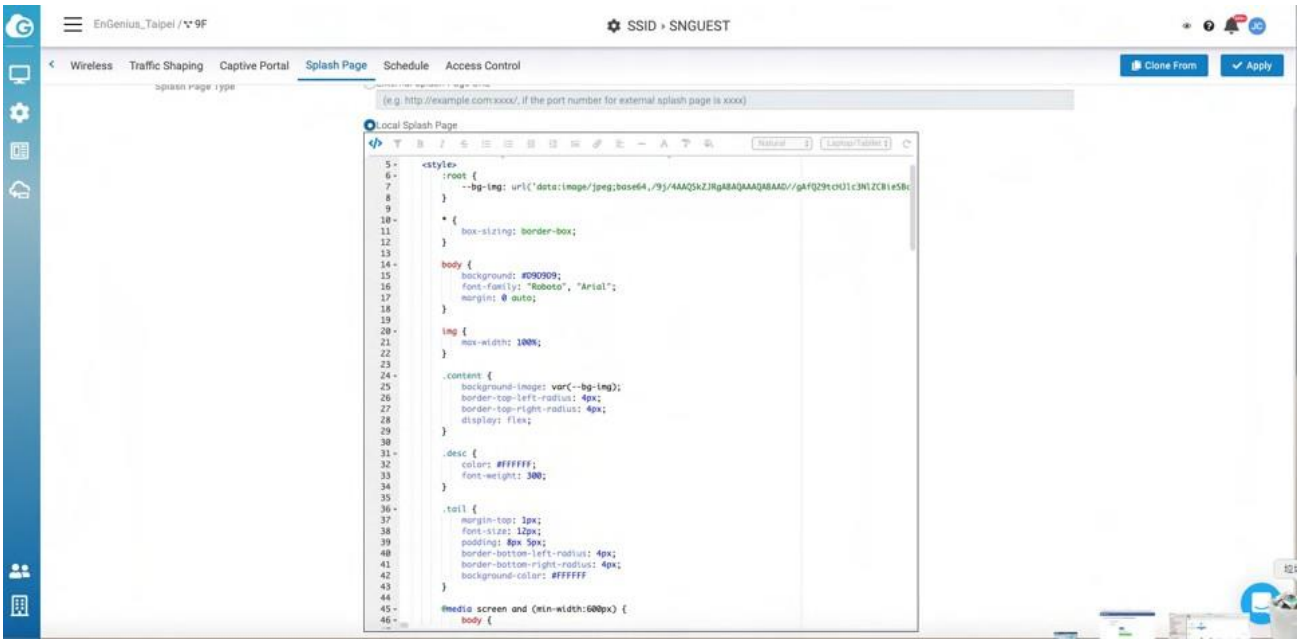
After you complete the splash page, please remember to click **Apply**.

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 .



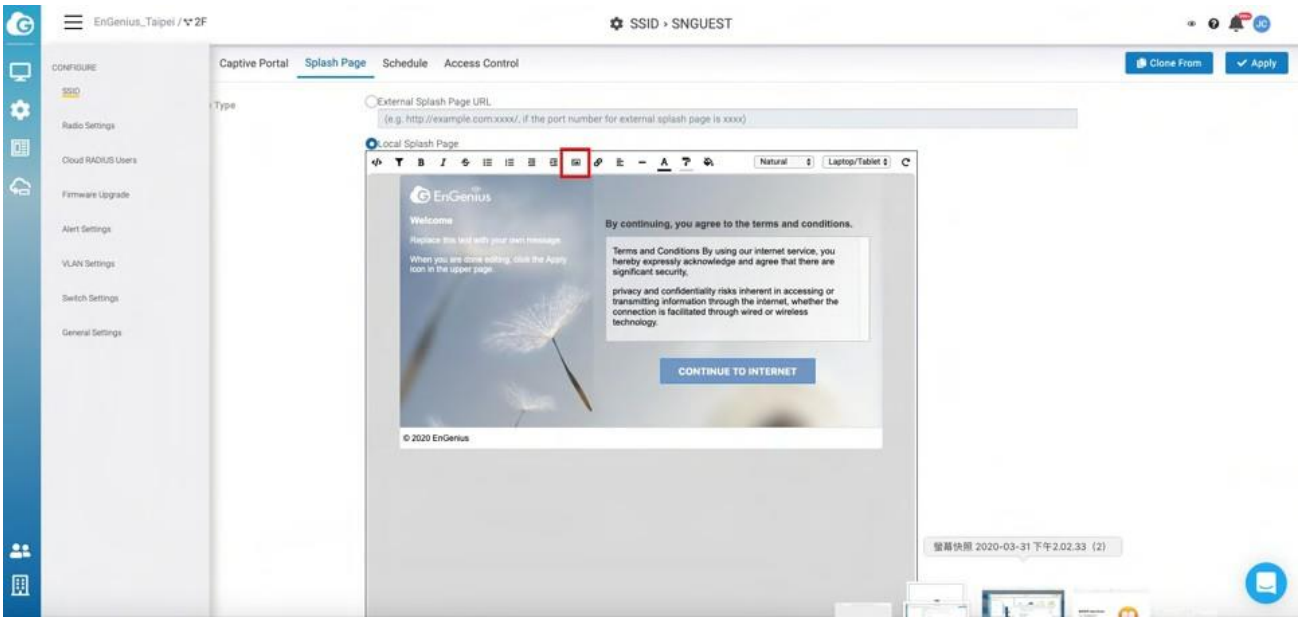
Choosing a starting template

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.

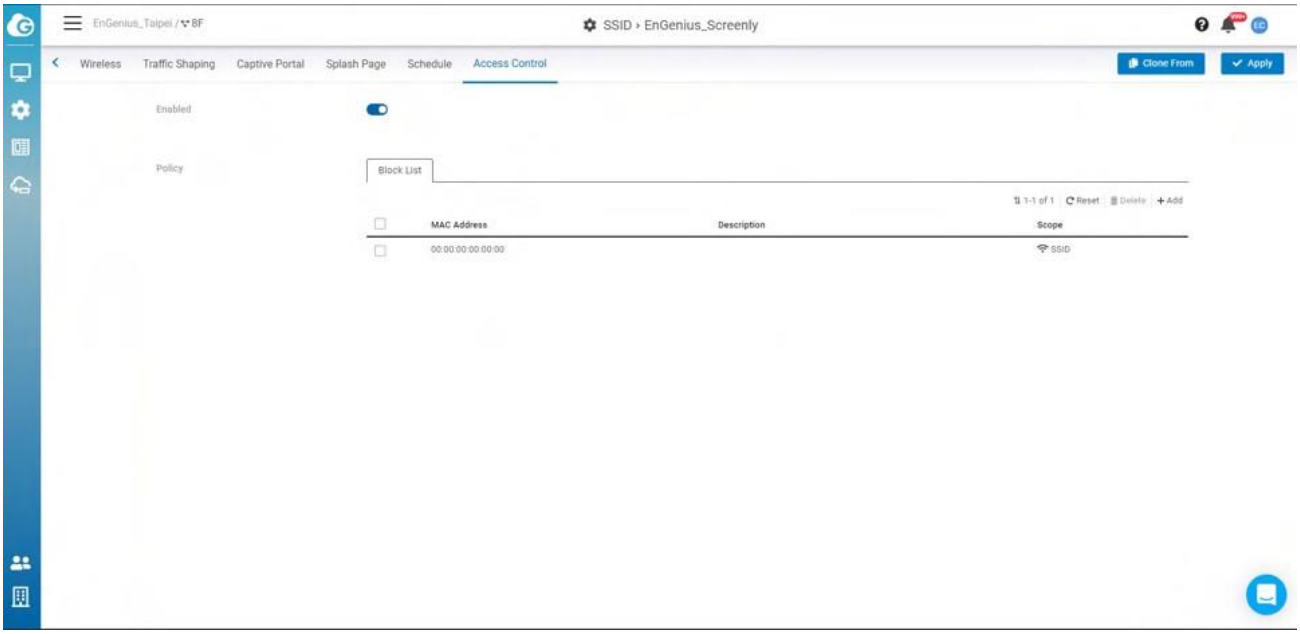
1. Click the **Insert Image** button, then navigate to a file, or drag and drop it into the **upload images**.



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.



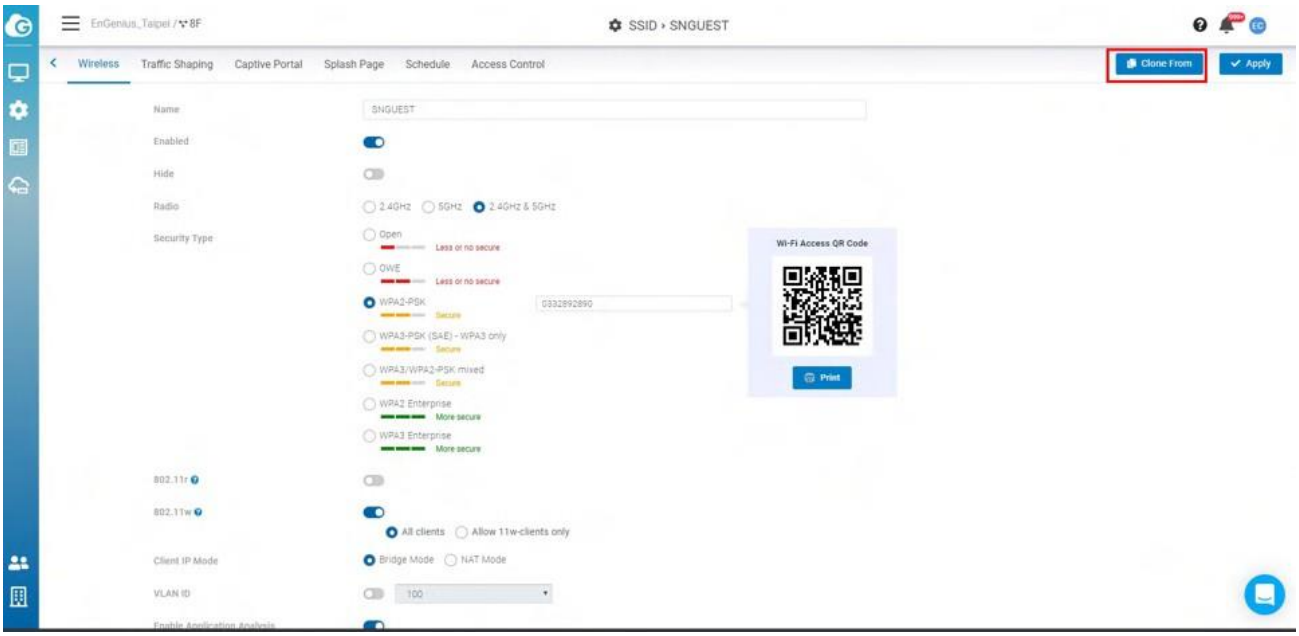
The following describes the functions on this screen:

- **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 .

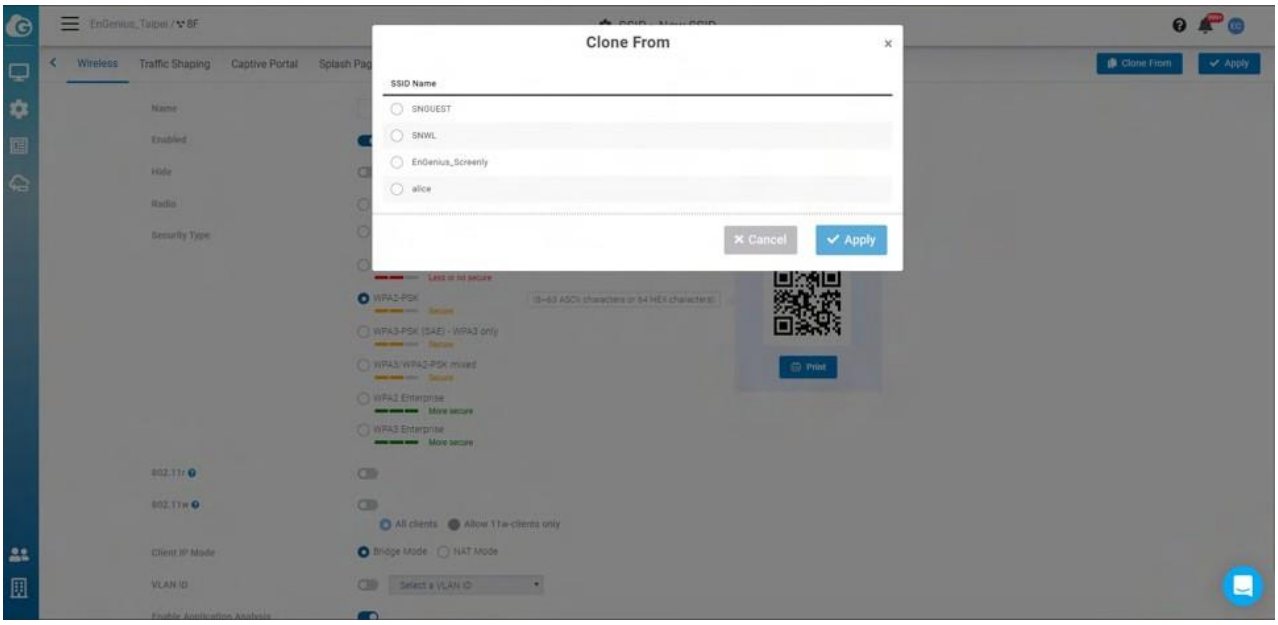
Clone SSID

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



Follow steps to clone SSID

1. Click **Clone From**
2. Select SSID to be cloned => Click **apply** in popup



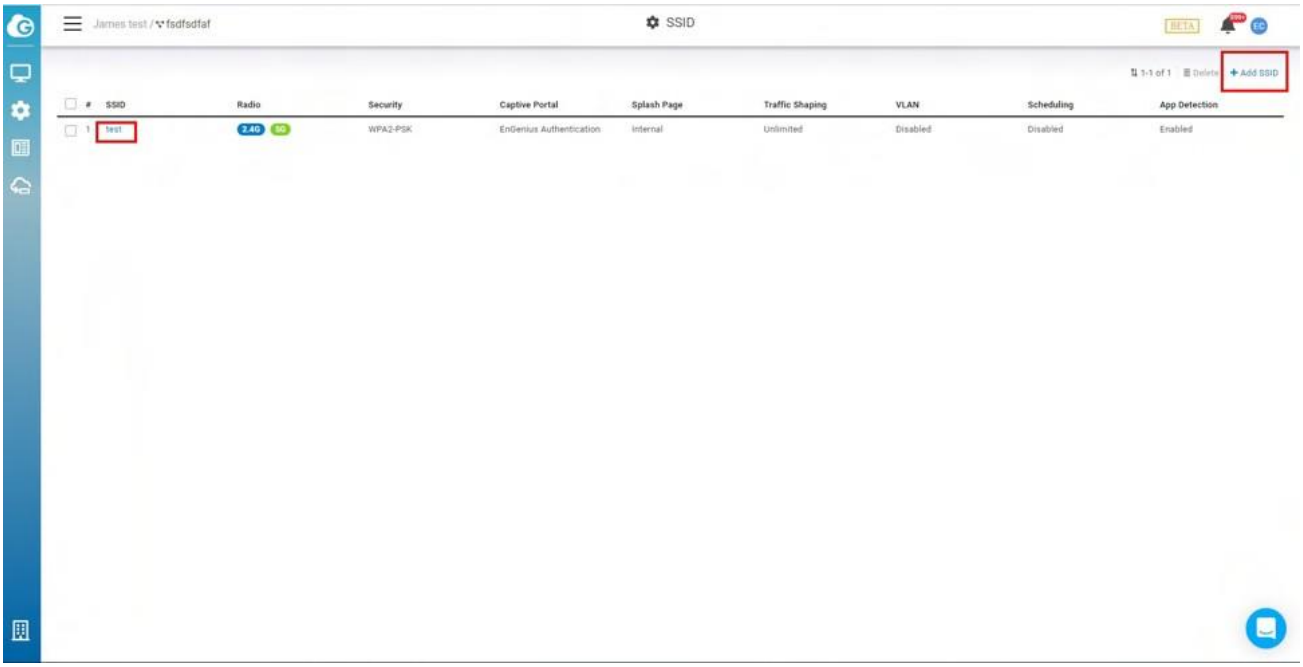
3. Click **Apply on tab bar** to take effect

Examples

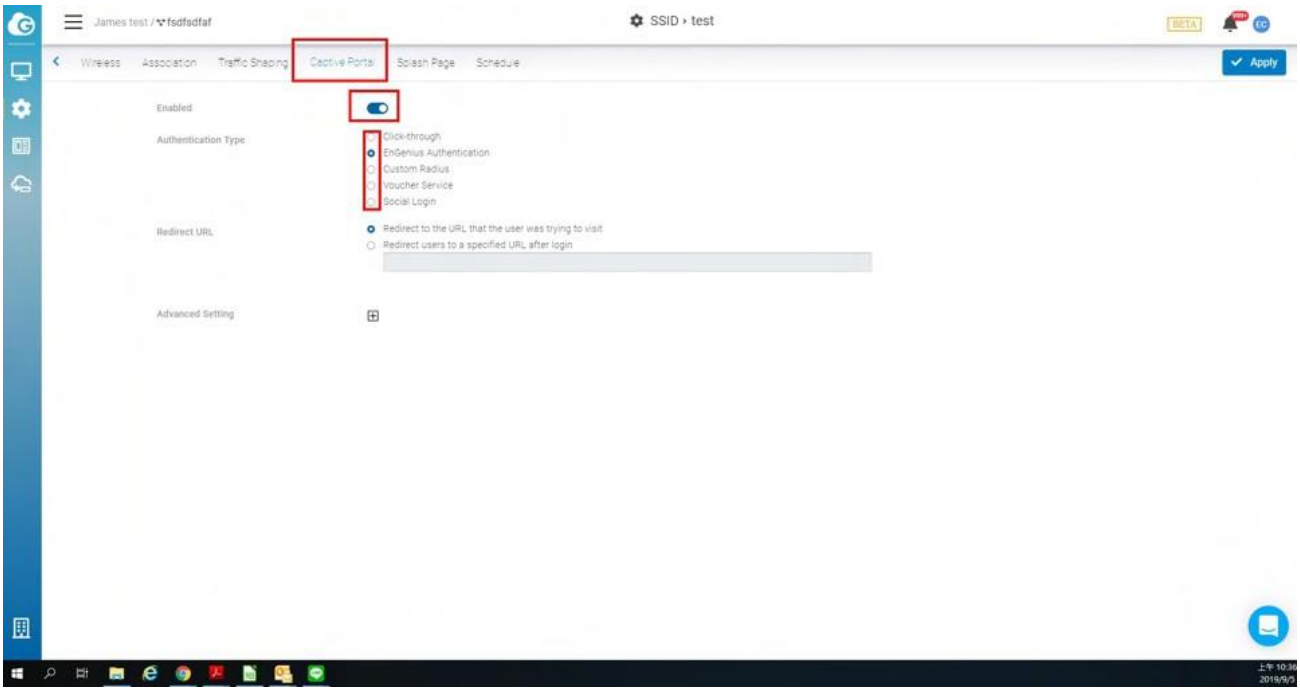
How to Configure Captive Portal

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.



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

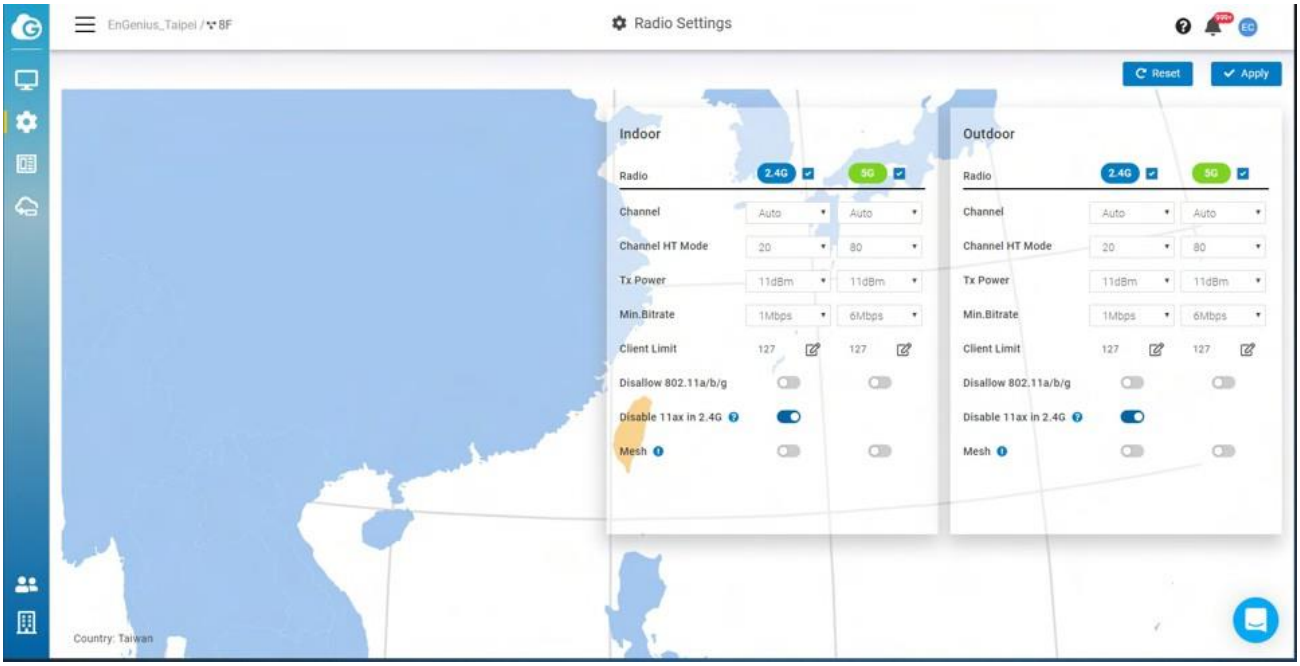


4. Click **Apply.**

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**.



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

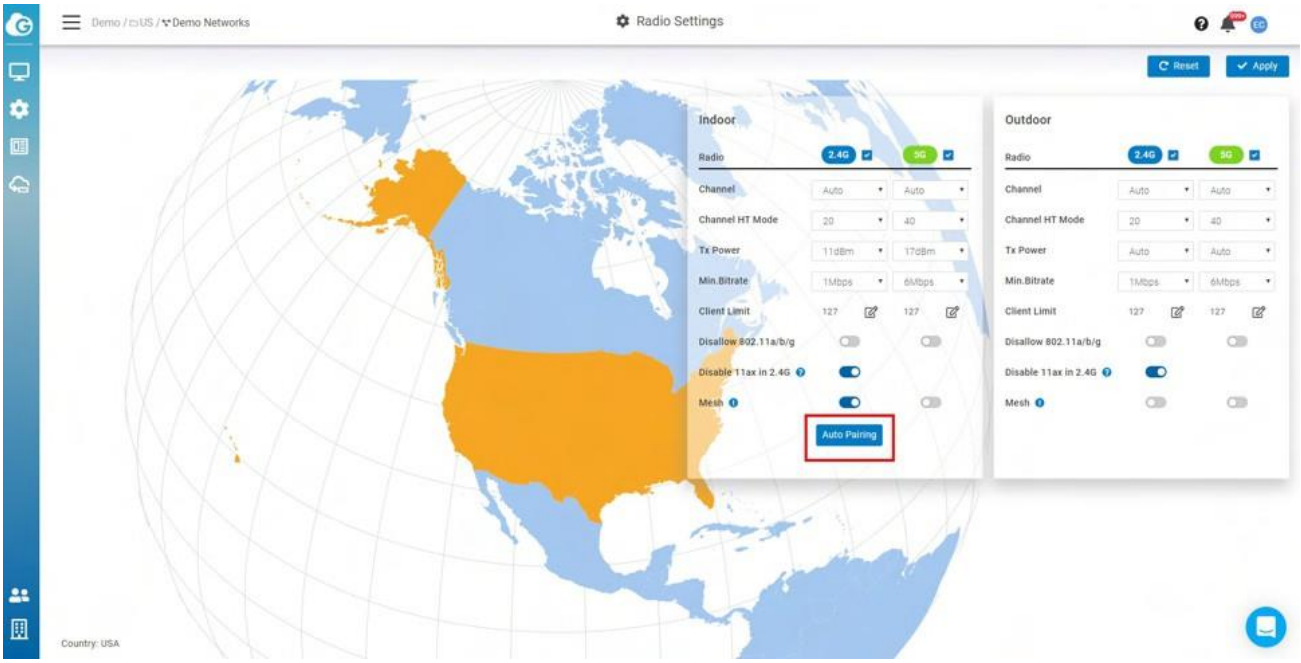
This option allows users to discard 802.11 a/b/g devices to use network to prevent from impact of performance to other 802.11ac/ax clients.

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.



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

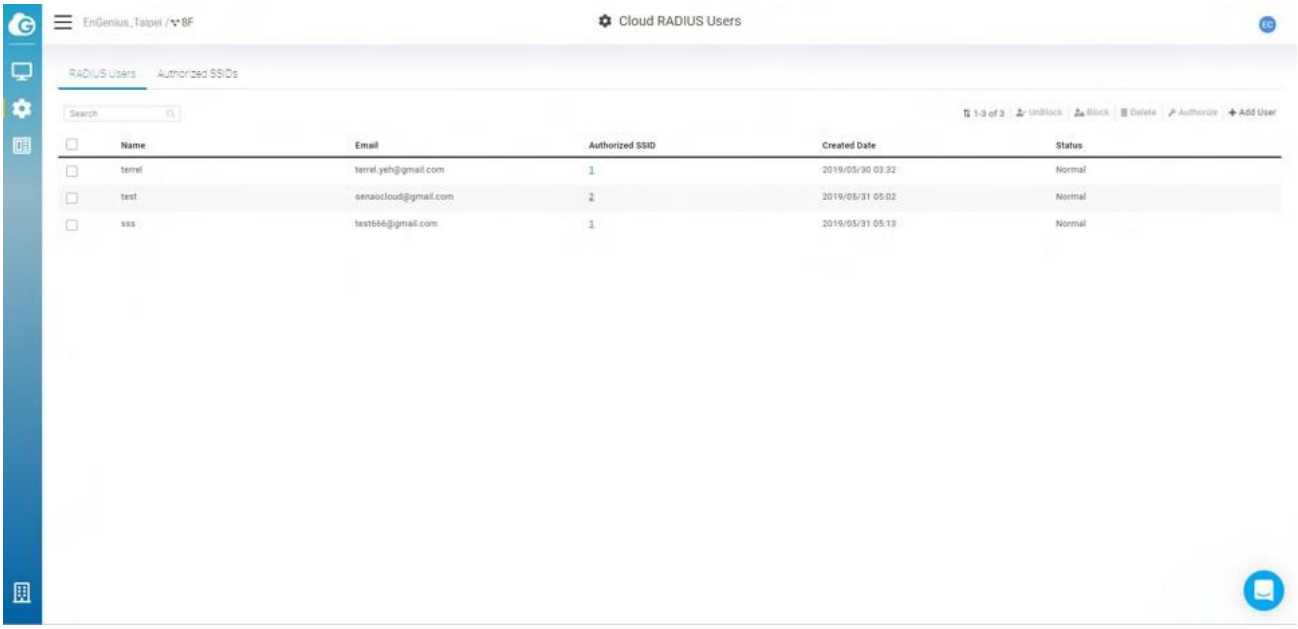
> 1. There must be a Cloud-connected AP nearby try-to-mesh AP to access wirelessly and in the same “Network”, so the Mesh configuration can be pushed to 2 AP's to mesh together.
>
> 2. It might take some time since the try-to-mesh AP might need to go through firmware upgrade and reboot (around 4-10 min…).

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).



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:

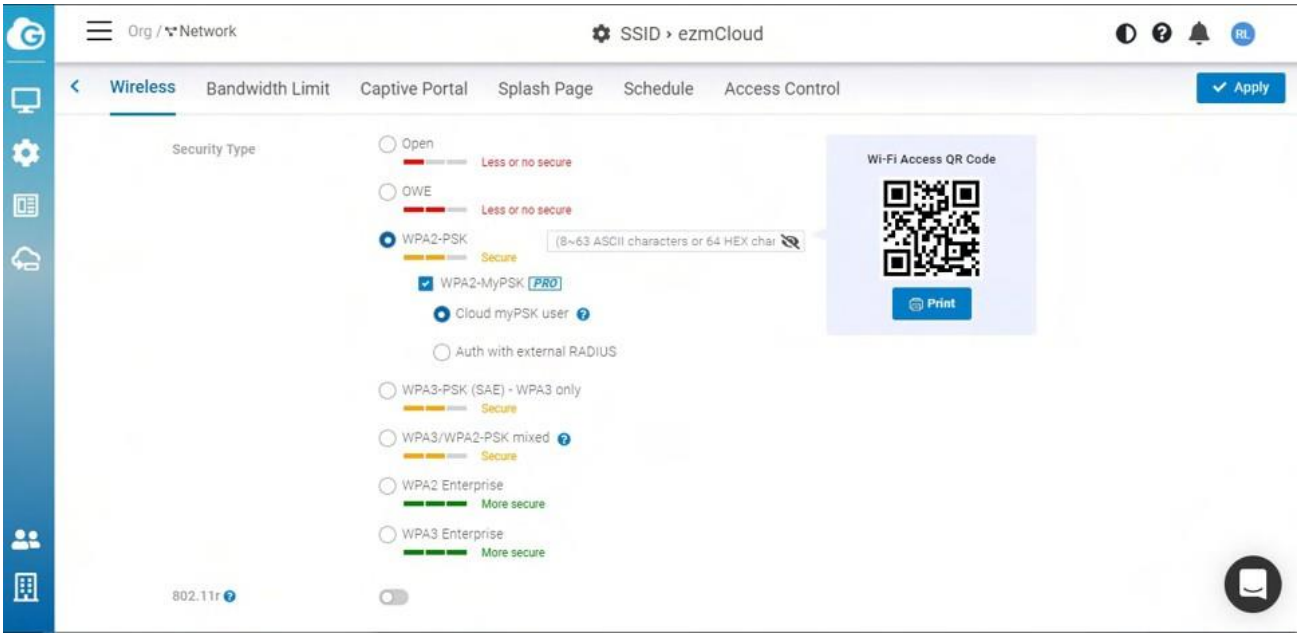
- **Add User:** Add users and authorize users to SSIDs.
- **Authorize:** Allows you to authorize users to SSIDs.
- **Delete:** Delete users.
- **Block:** Block users.

- **Unblock:** Unblock users.

Configuring MyPSK

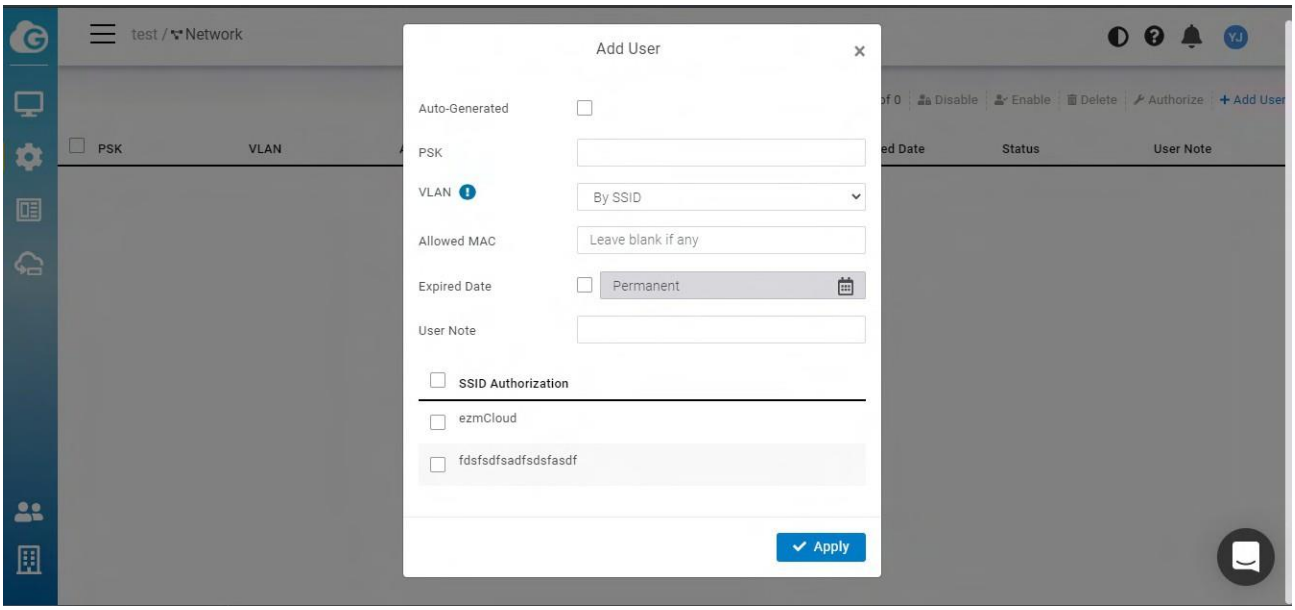
When setting up an enterprise wireless network, it is common to configure WPA2-PSK authentication in order to onboard different users on to the wireless network. However, IT administrators may still encounter some drawbacks with this method of authentication when they need to use different PSKs in order 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**



Create my PSK Users

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



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.

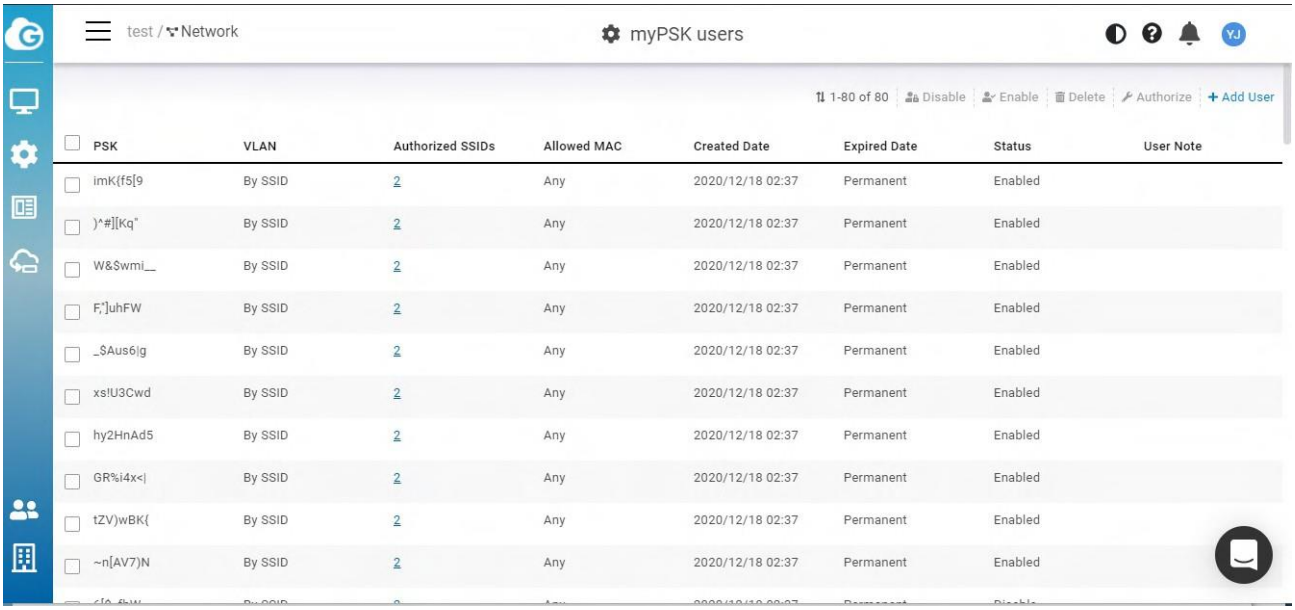
Expired Date: Default is Permanent, click the checkbox to choose the expired date

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

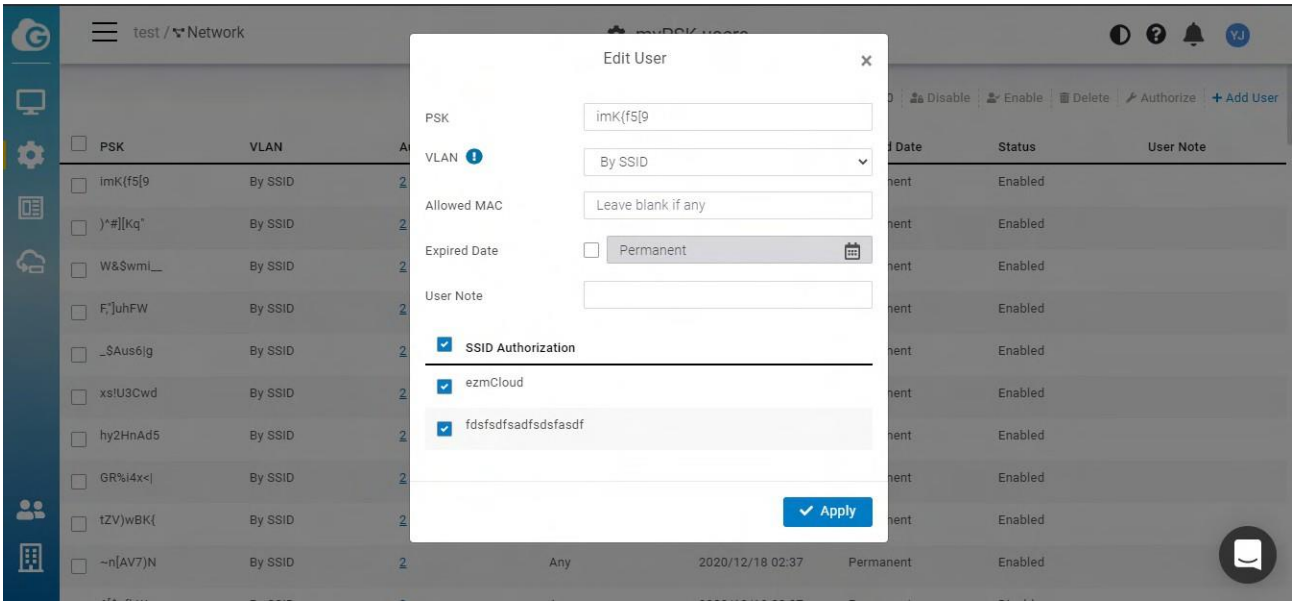
SSID Authorized: The SSIDs you want users to access

Edit MyPSK Users

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



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



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 .

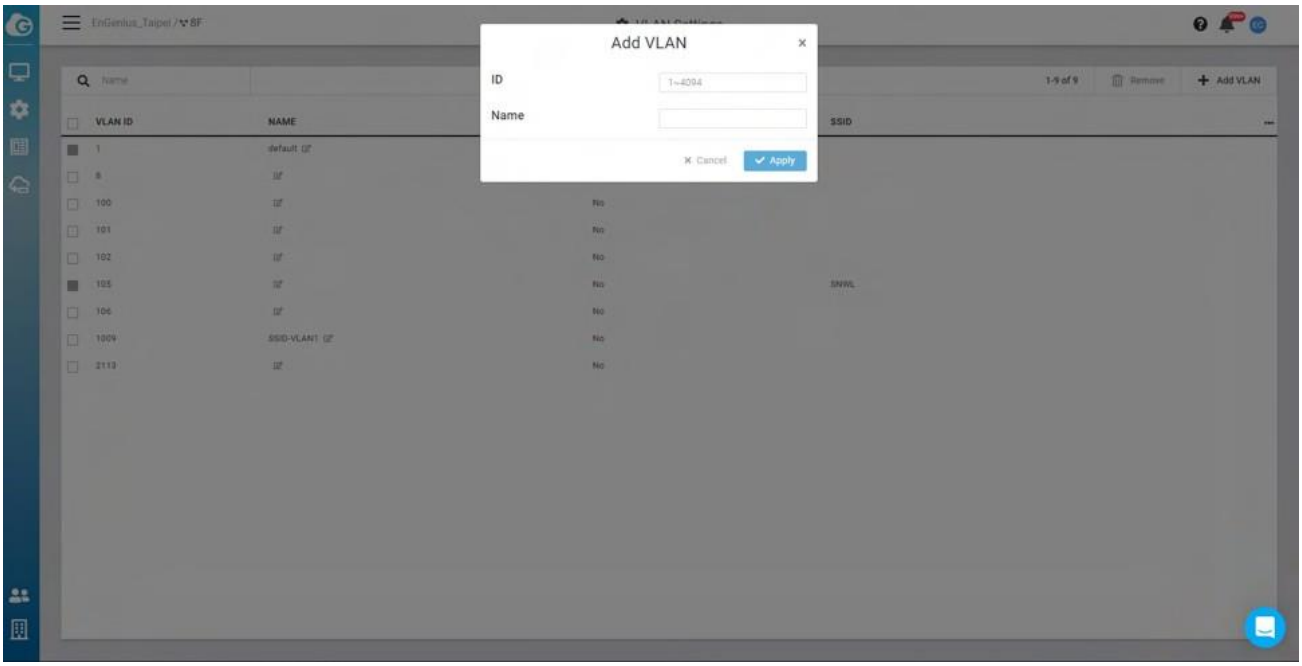
Use this screen to add and delete VLANs for network.

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

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

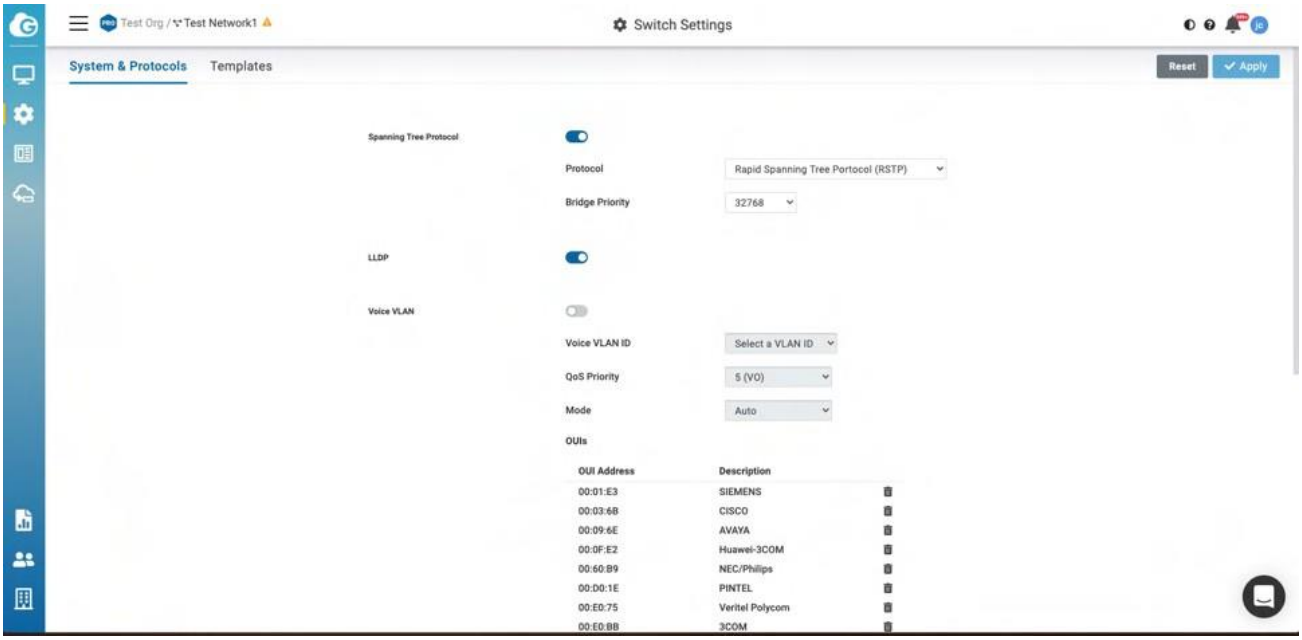


1. Click **Add VLAN** button.
2. Input **VLAN ID** and **VLAN Name.**
3. Click **Apply** to complete the settings.

> 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 .

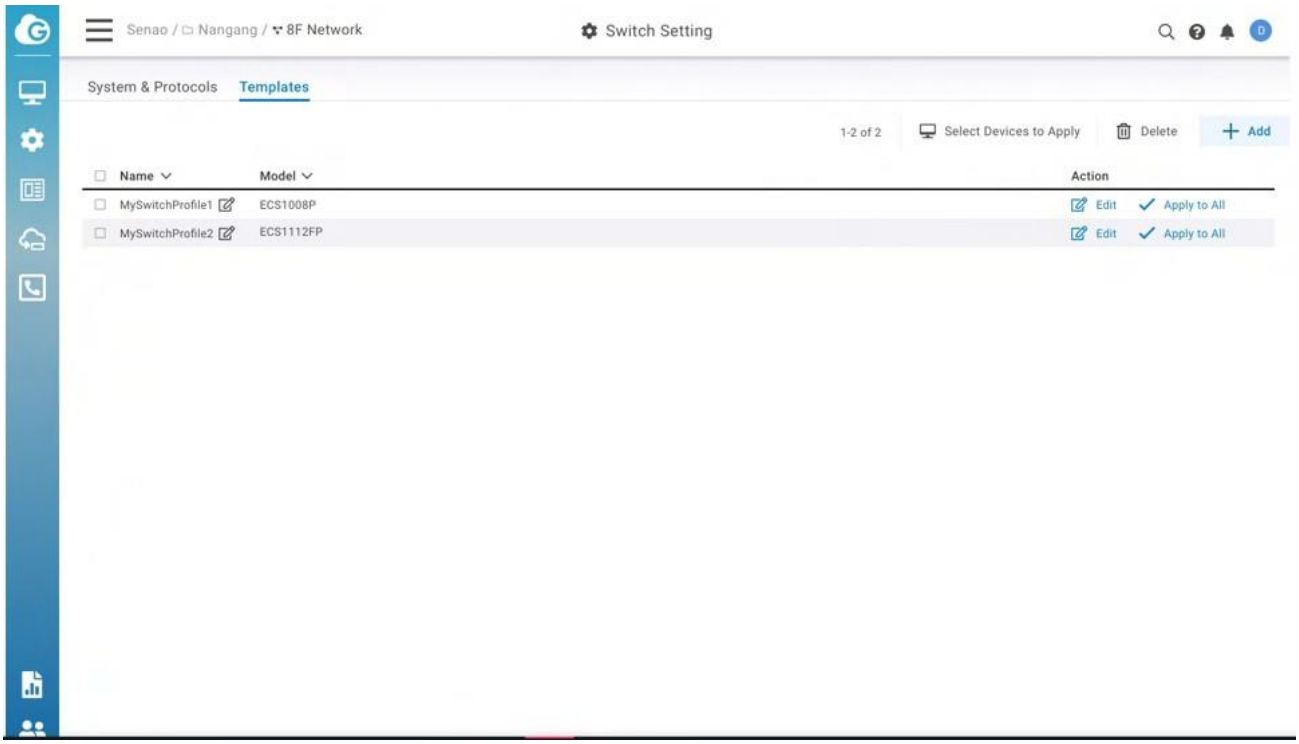
Configuring Switch Settings

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**.

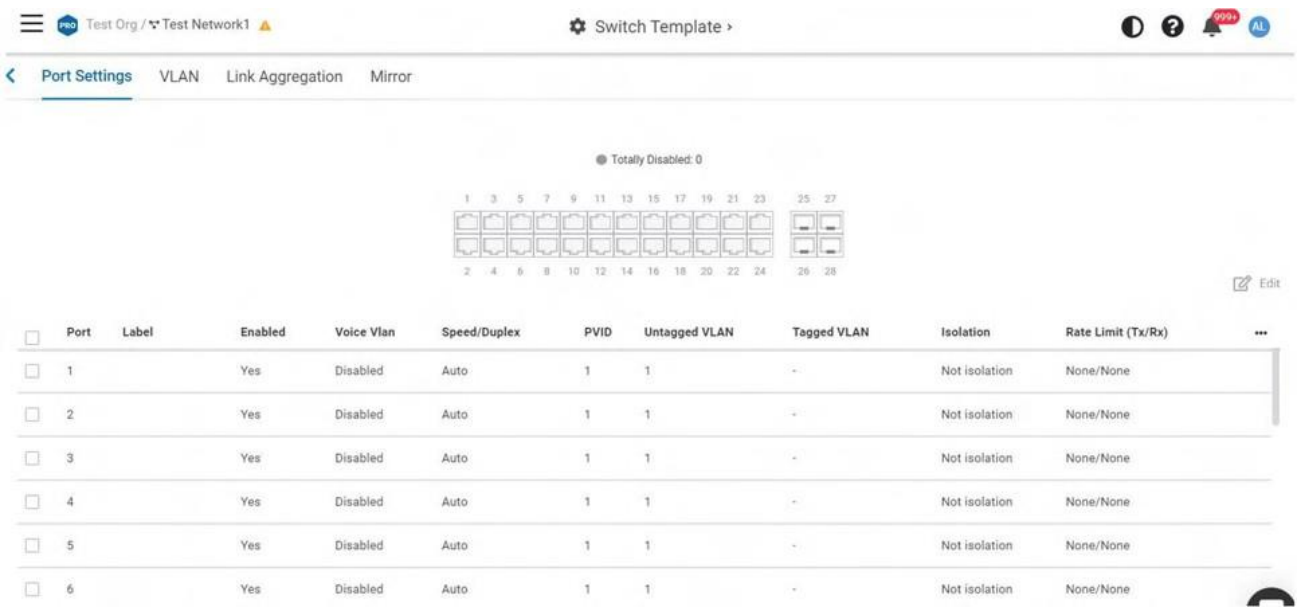


Many MSP or SI would like to be able to “group configure port settings” in the Network. Switch Template feature helps users to apply same port configuration to all switch with same models in the Network to save time of configuration one by one.

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



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



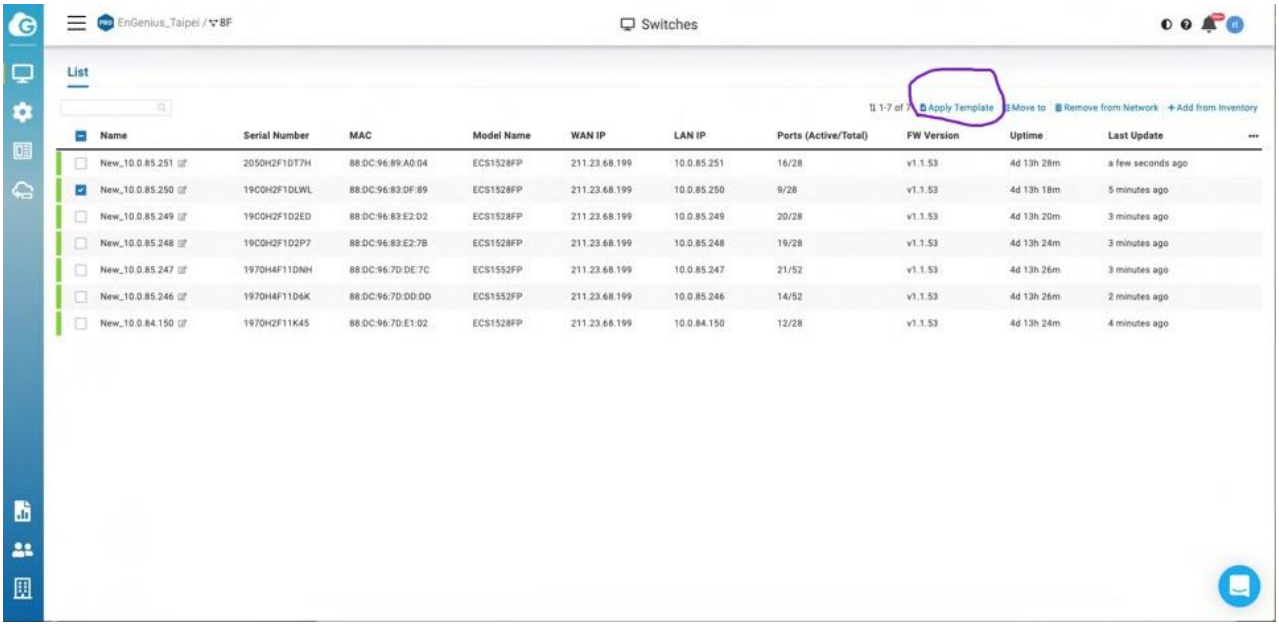
- **Apply to All** will apply the Switch Template to all devices of the same model in the Network.

> **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

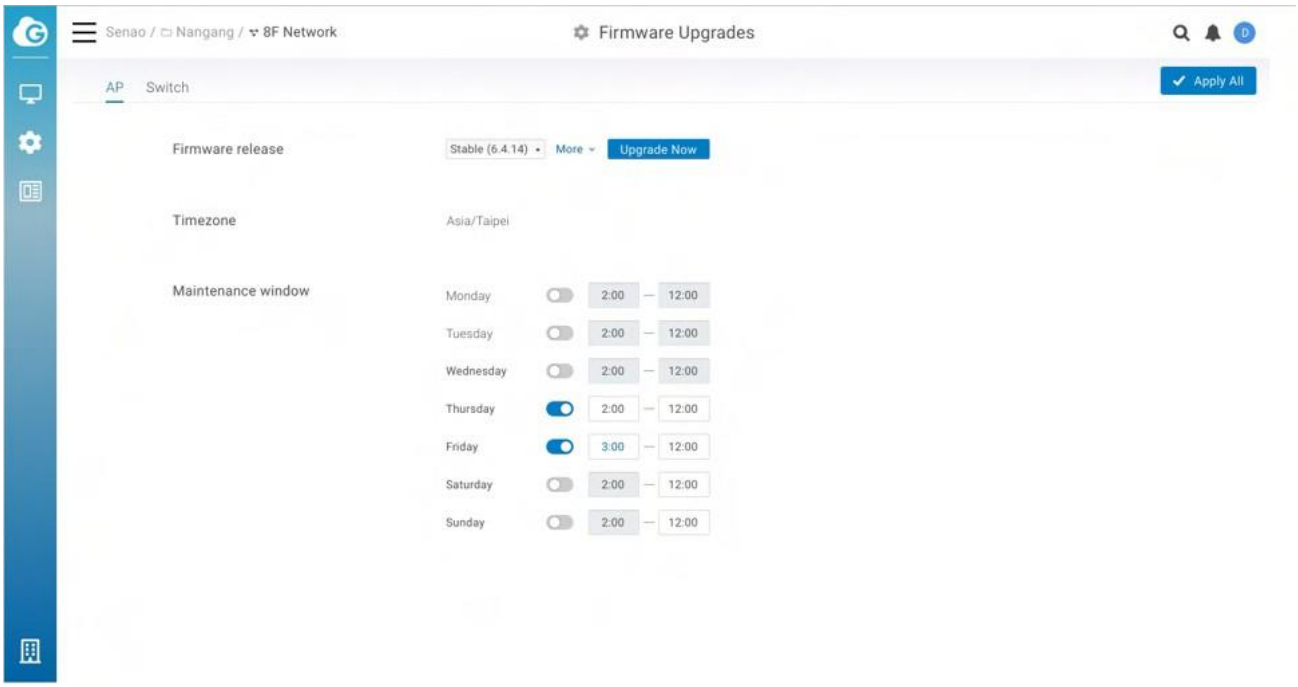
Manage > **Switch List** > **choose the Switches to be applied** > Choose **Apply Template**



Firmware Upgrade

Automatic Upgrades

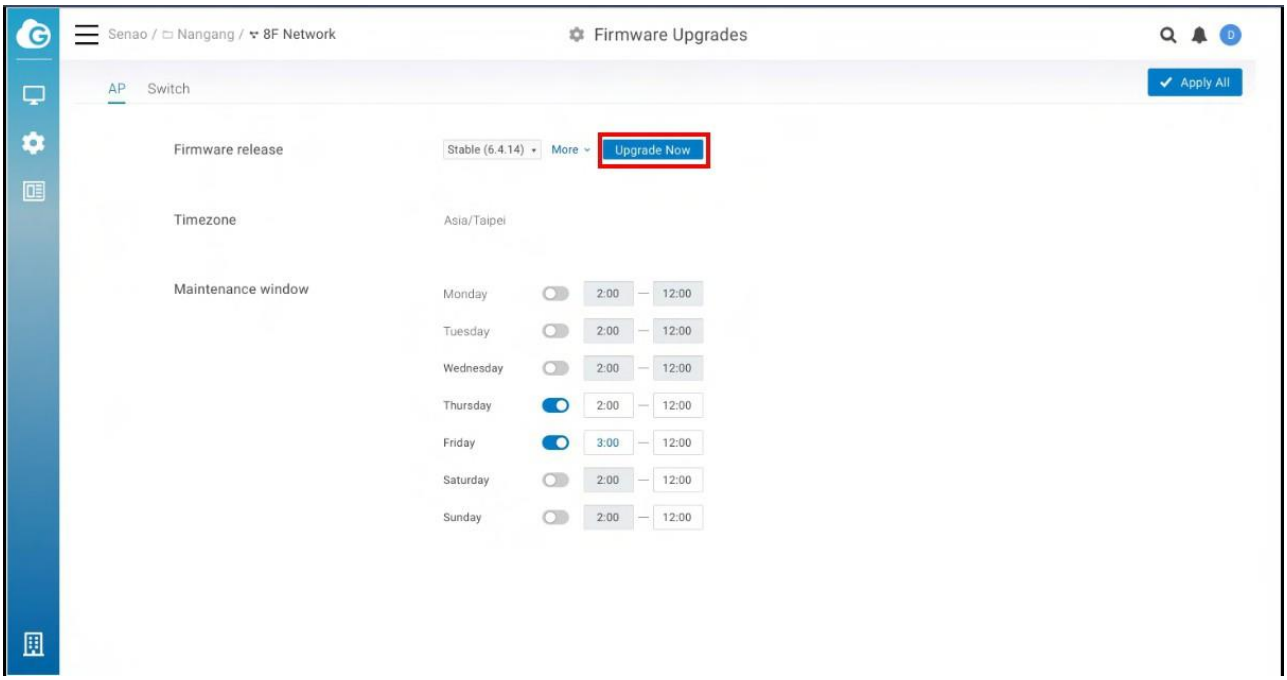
EnGenius Cloud enables automatic upgrades by default and will upgrade firmware according to the **Maintenance Window** time period each week.



Manual Upgrade

To manually update device firmware:

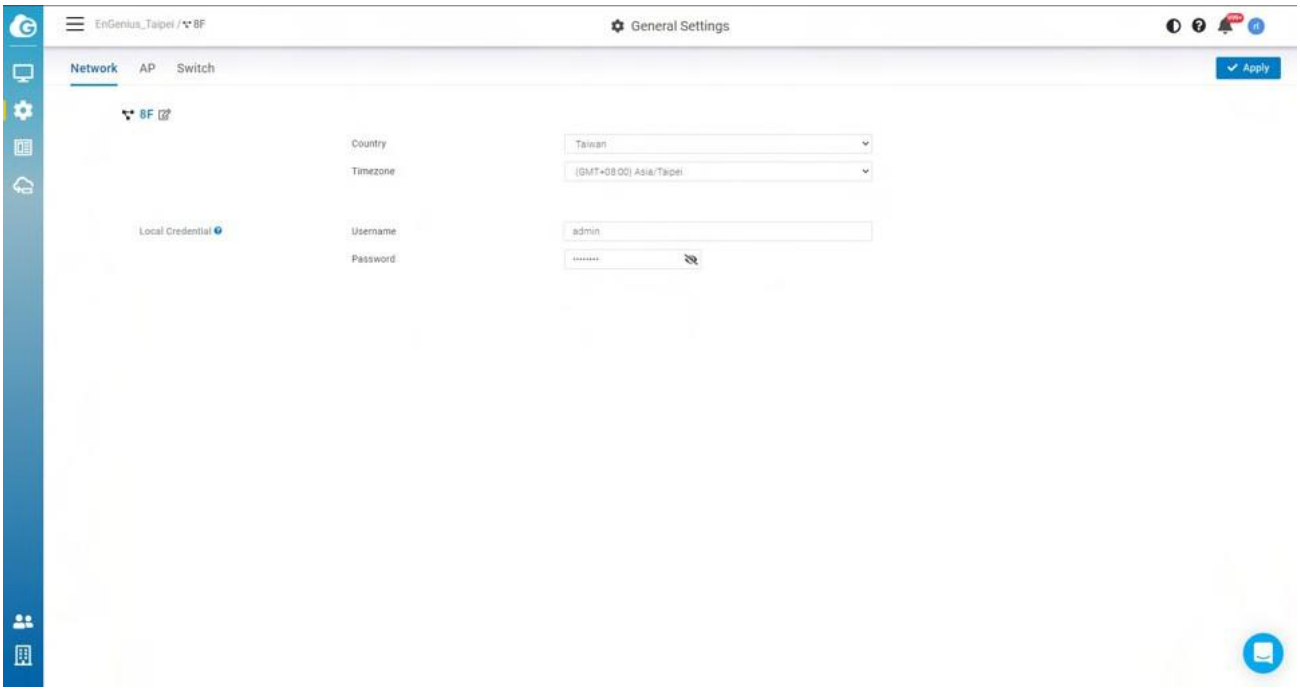
1. Select the firmware you desire to upgrade.
2. Click **Upgrade Now.**



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.



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 .

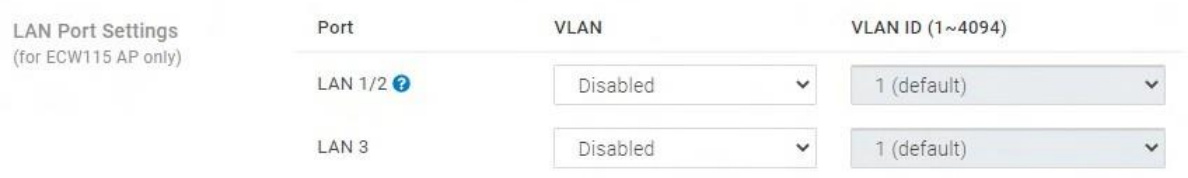
> Note that username and password could be blank if you don't want to change device login account of local web GUI.

LED Light

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

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



System Reserved IP Range

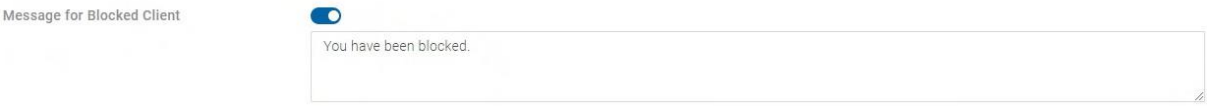
When using NAT (AP DHCP) and captive portal, AP will leverage a range of IP addresses as default. If user unconsciously configures their local Network conflicting with the range, it will cause problems. the user is able to change the System reserved range if they cannot change their local LAN IP address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

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

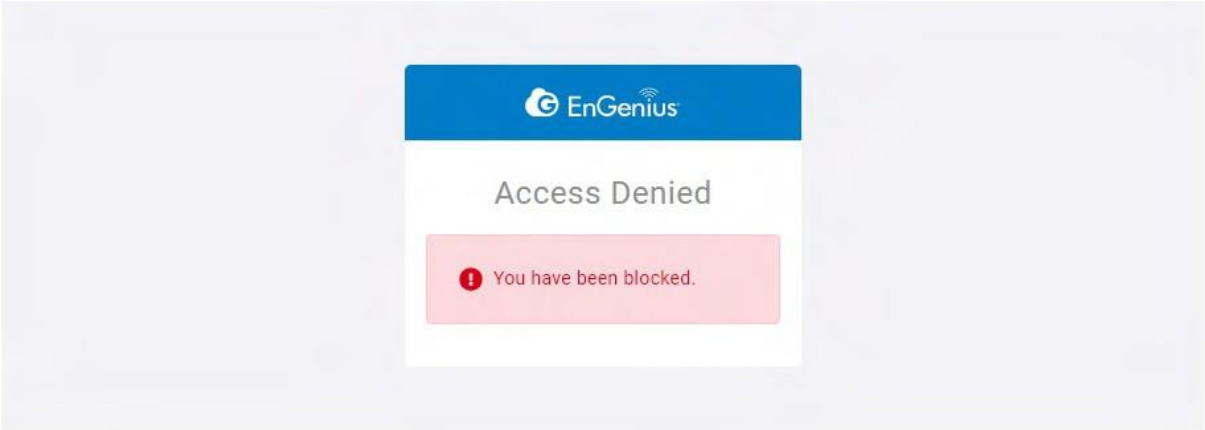
General Settings > **AP** > **System Reserved IP Range**

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.



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



Advanced settings

Presence reporting

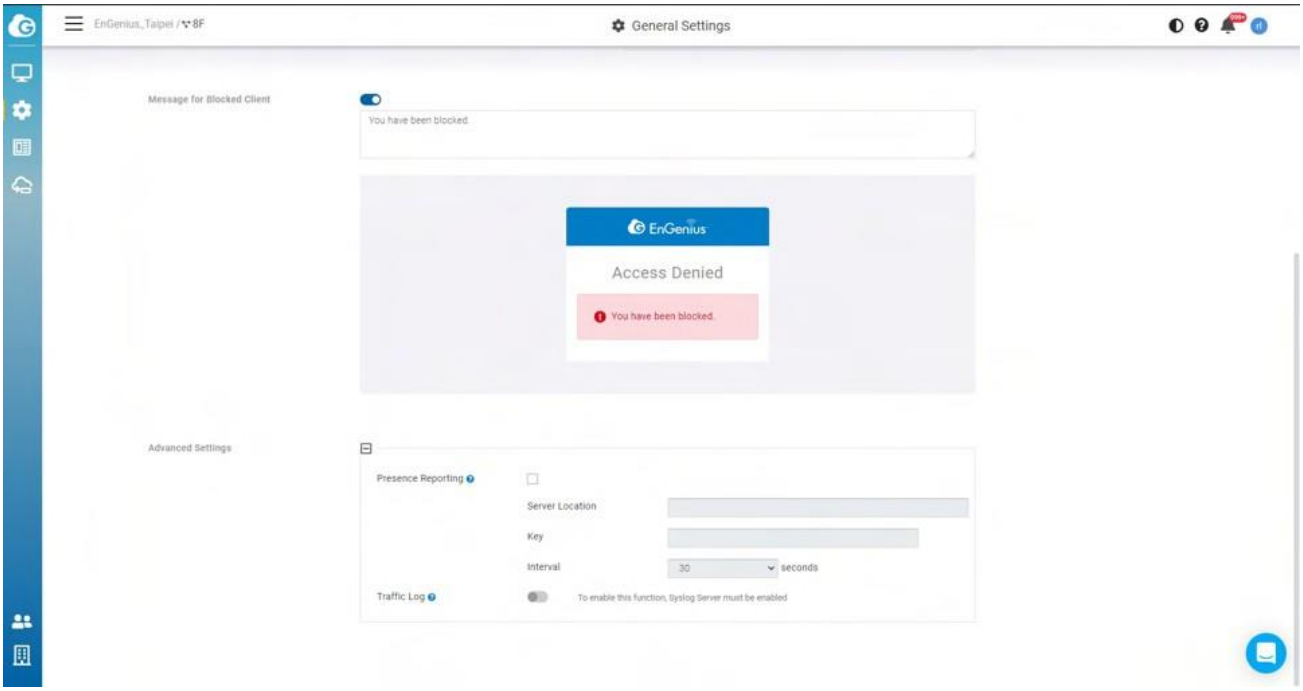
For applications like CRM tools, presence analytics, or location-aware services which need to continuously gather presence data of wireless clients, EnGenius Cloud Acess Points are capable of delivering real-time presence data to fulfill the requirement.

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



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**.

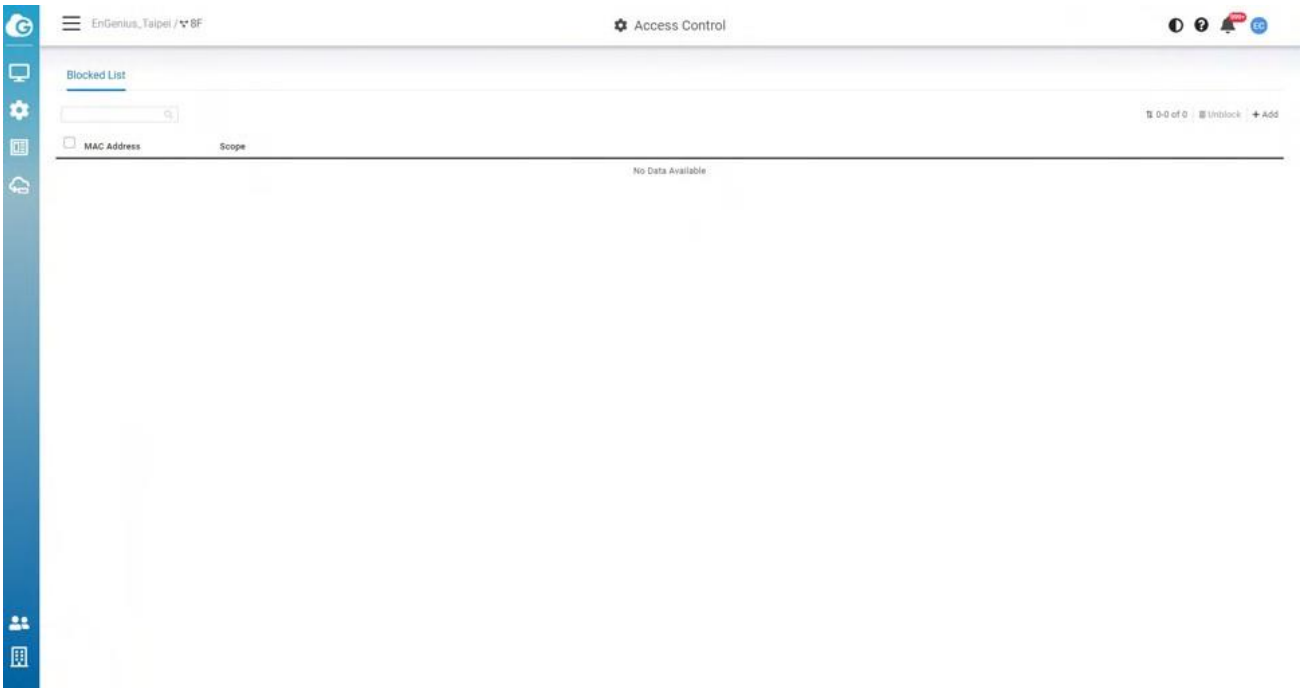
- **Status**: Enable to open the function to the remote system log.
- **Log server address**: Specify the IP address or hostname of the Syslog server.
- **Log server port:** Specify the port of the Syslog server. The default port is 514.

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**

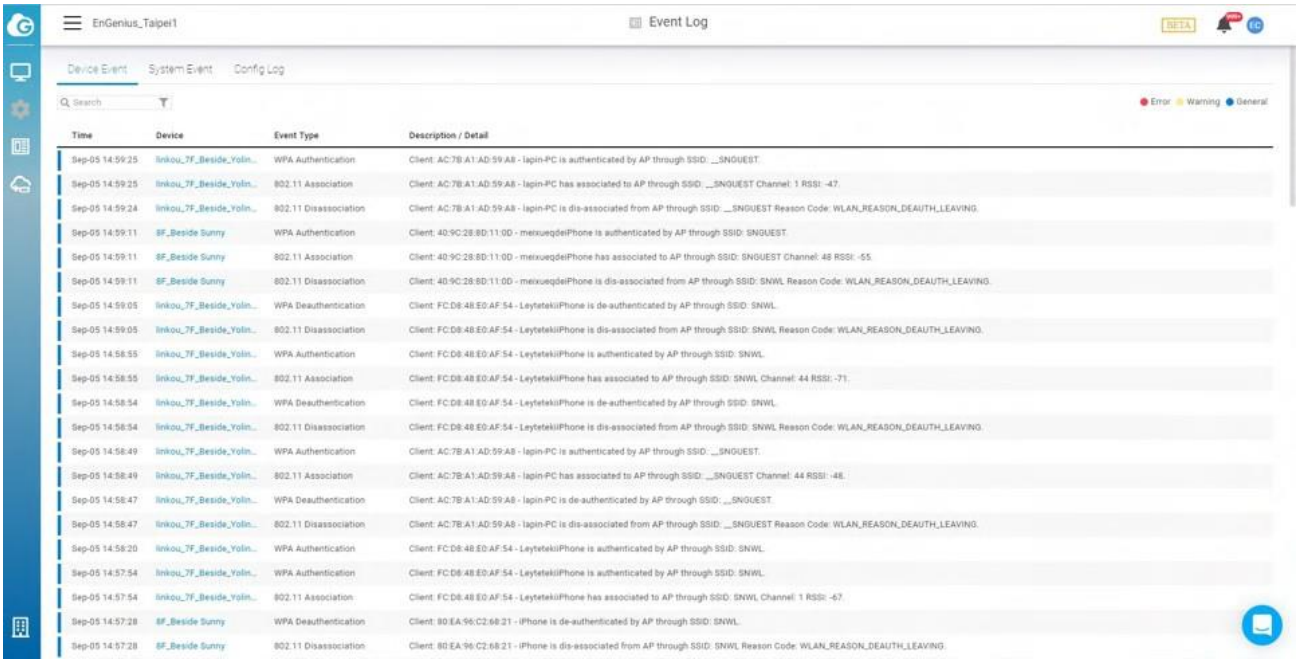
Analytics

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.

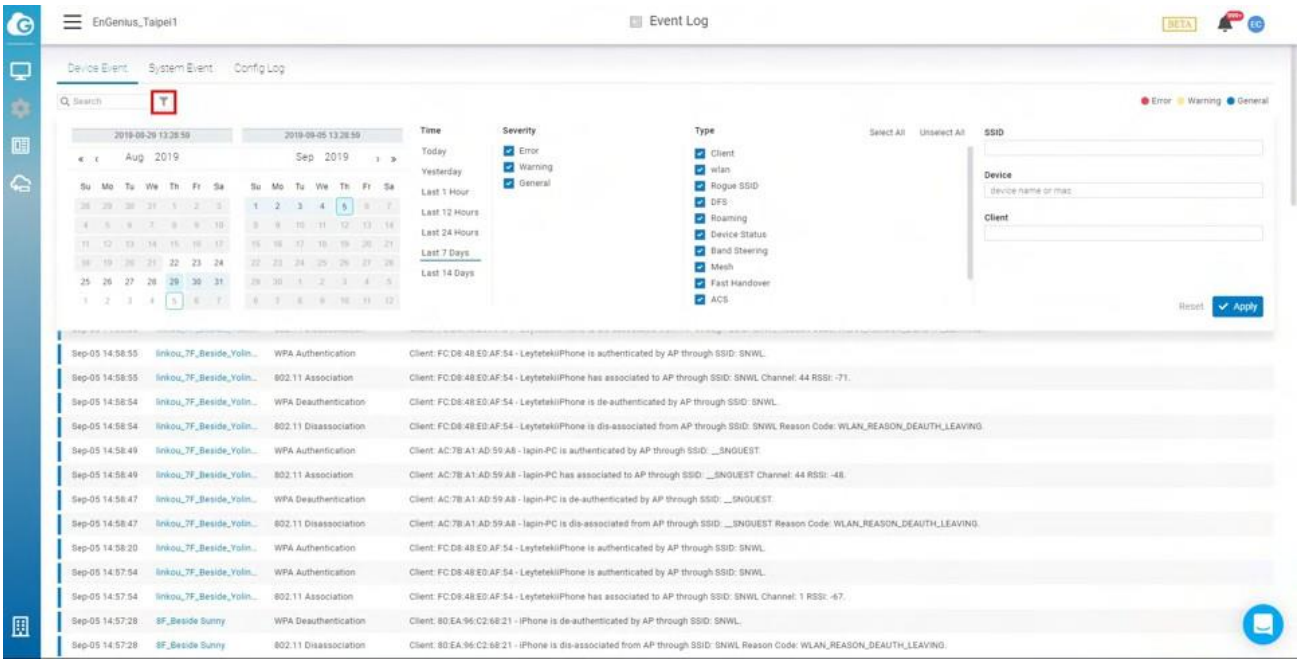
Use this screen to view **Device Events.**

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



Searching the Event Log

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



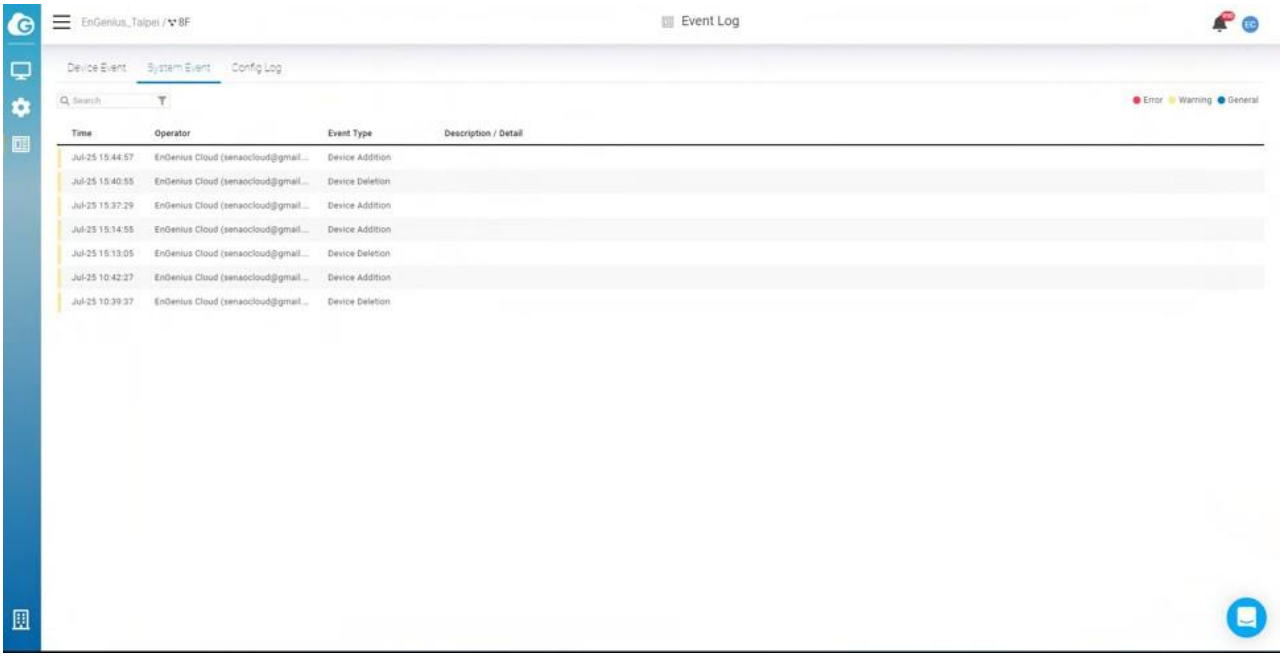
You can specify date/time, severity, and other parameters. Select one or multiple **event types**, then enter the **SSID**, **device name/MAC**, or select **client** to display the log messages related to it. After customizing your search parameters, remember to click **Apply** to perform the search.

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.

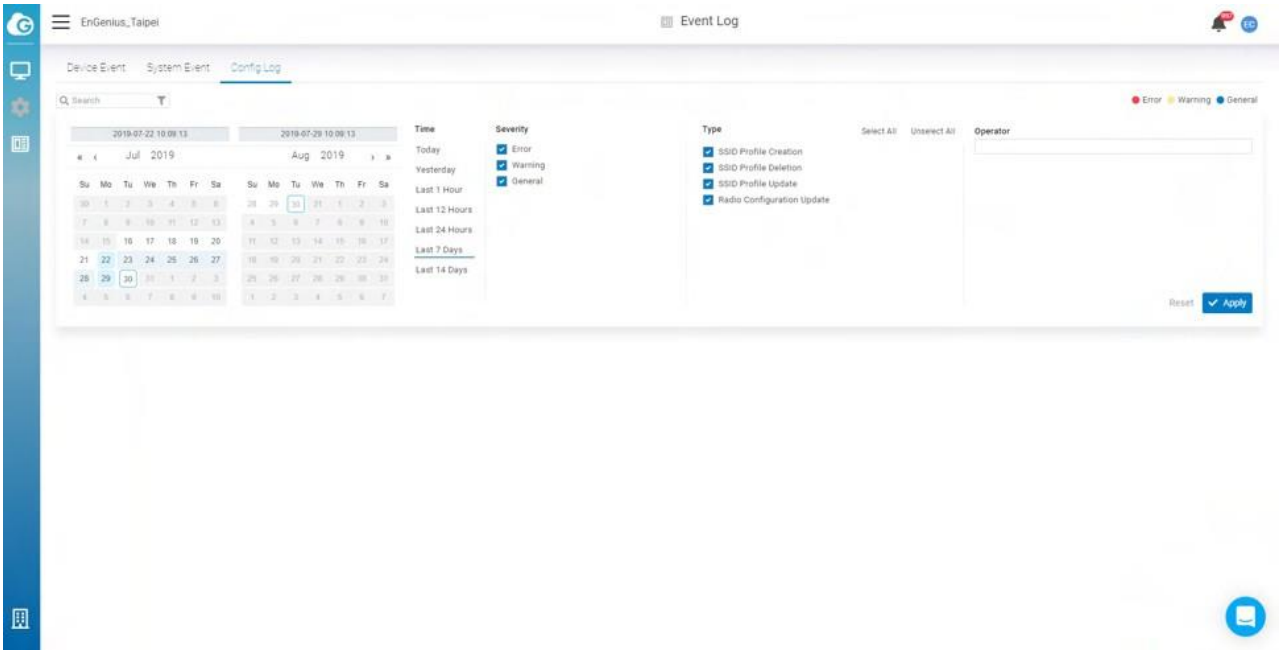


Config Logs

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.

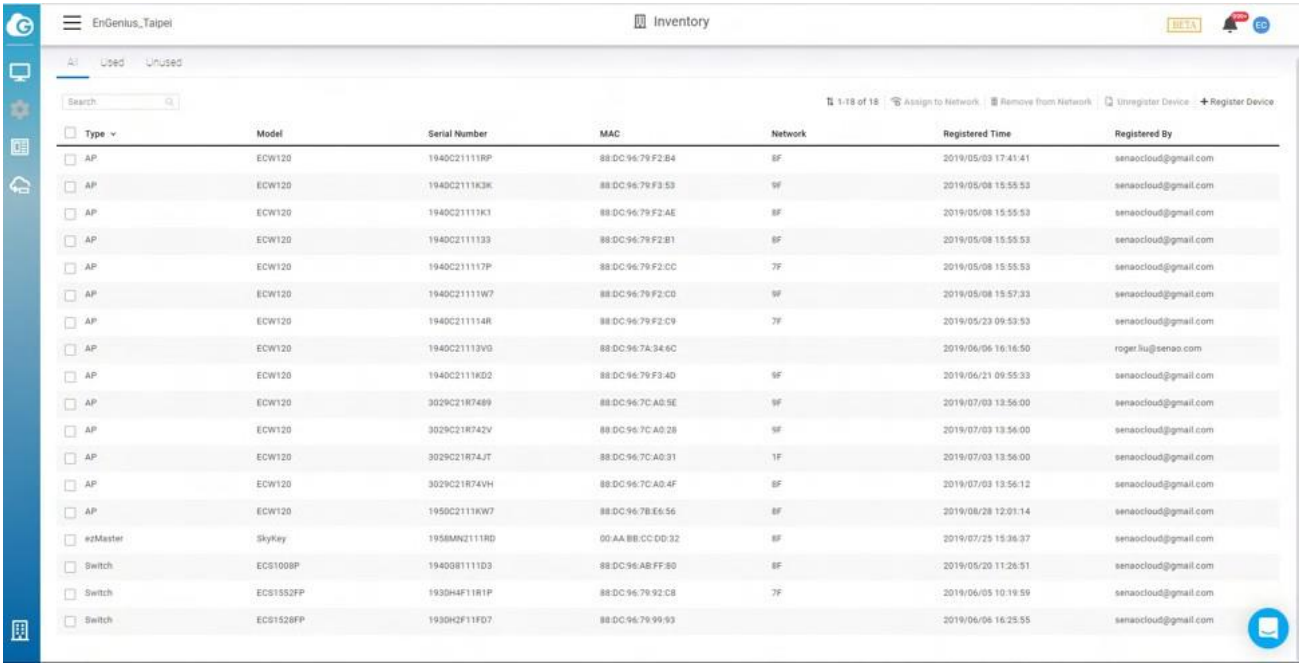


Managing Organizations

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:

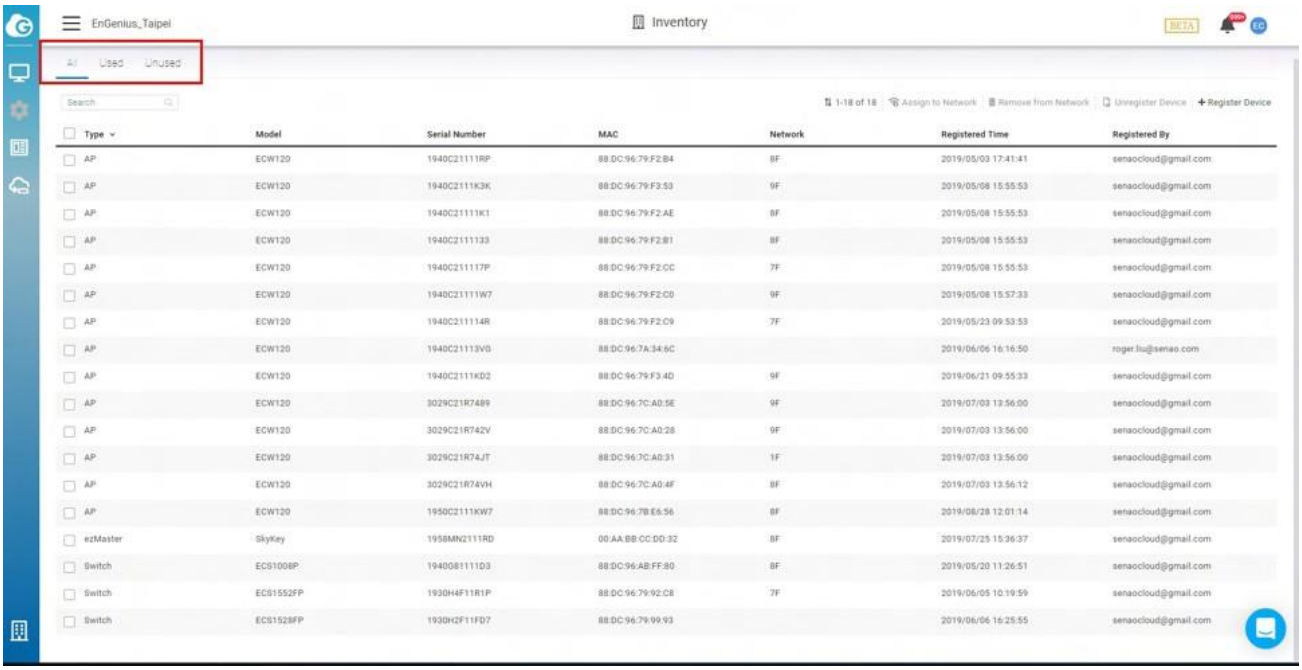
- **Type**: type of the device.
- **Model**: model name of the device.
- **Serial Number**: serial number of the device.
- **MAC**: MAC address of the device.
- **Network**: the network that the device has been added to.
- **Register Time**: time of the device's addition to the inventory.
- **Register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



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.

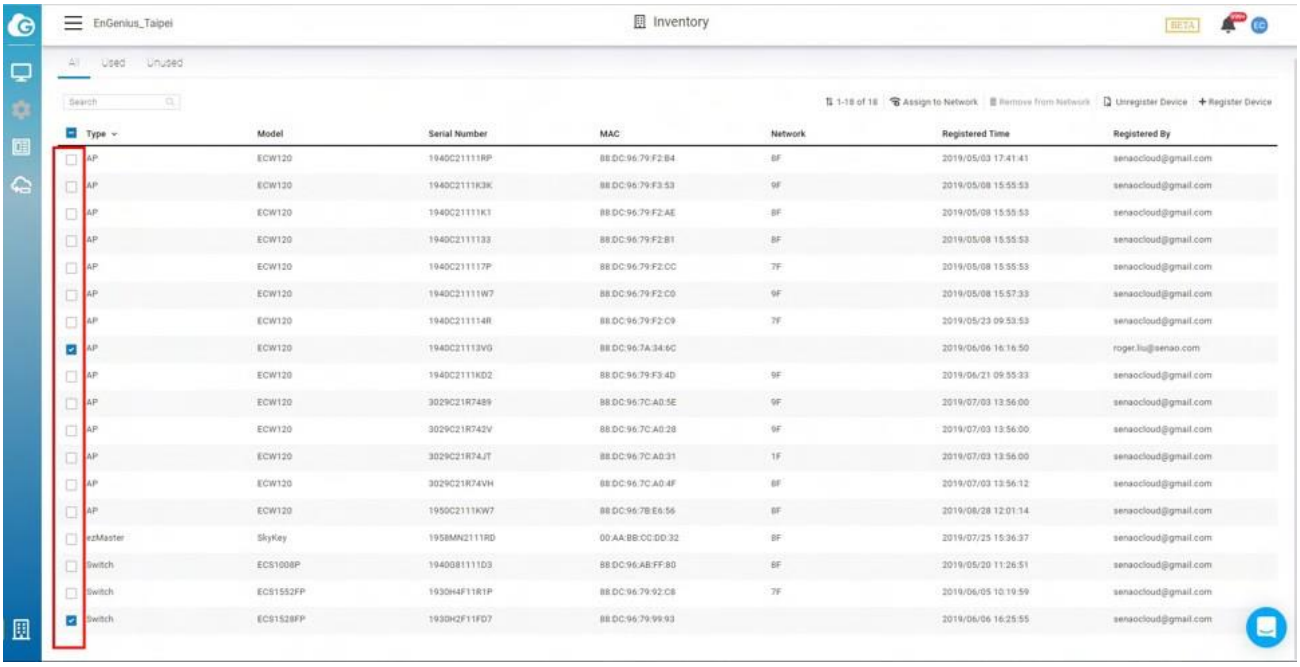
Click **Organization** > **Inventory** to access this screen.



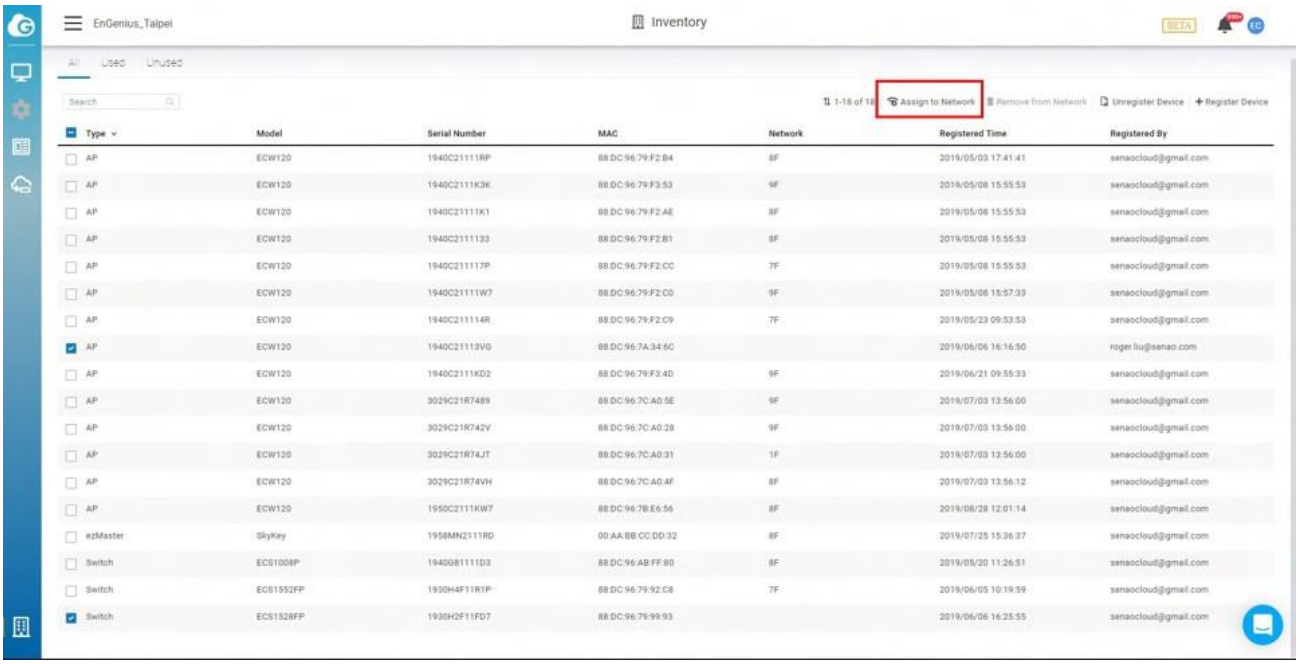
Assigning Devices to a Network

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.



3. Click **Assign to Network.**



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.**

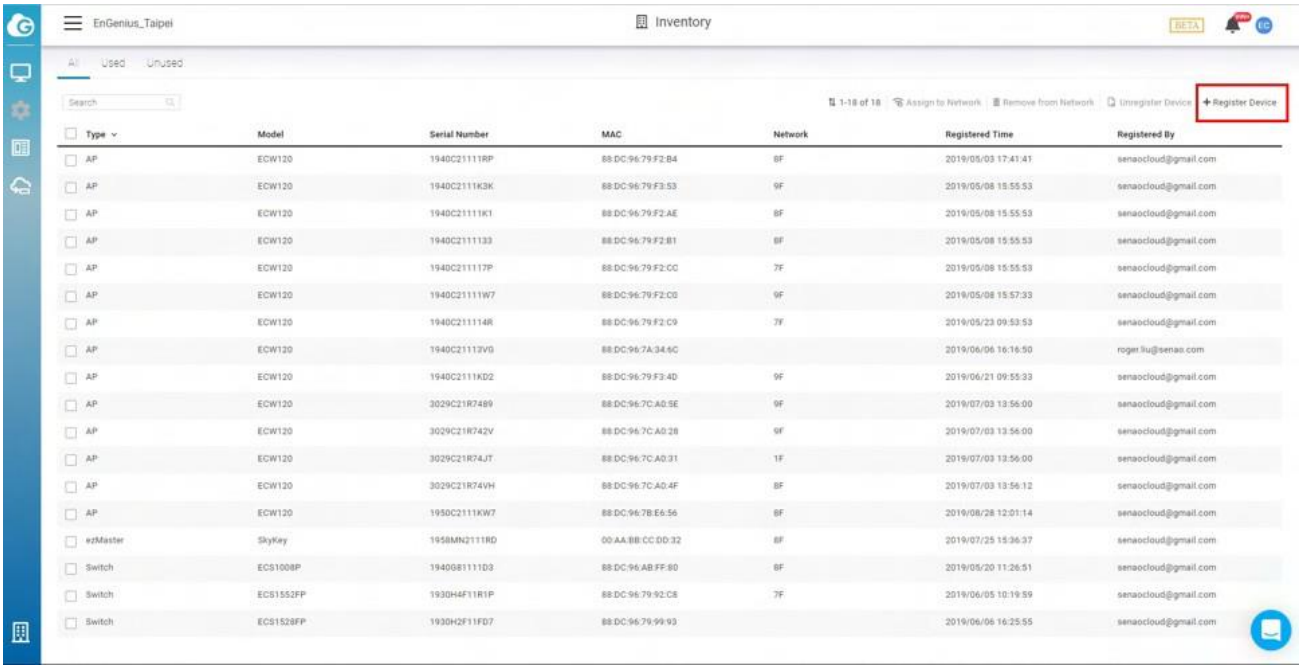
De-registering a Device from EnGenius Cloud

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.**

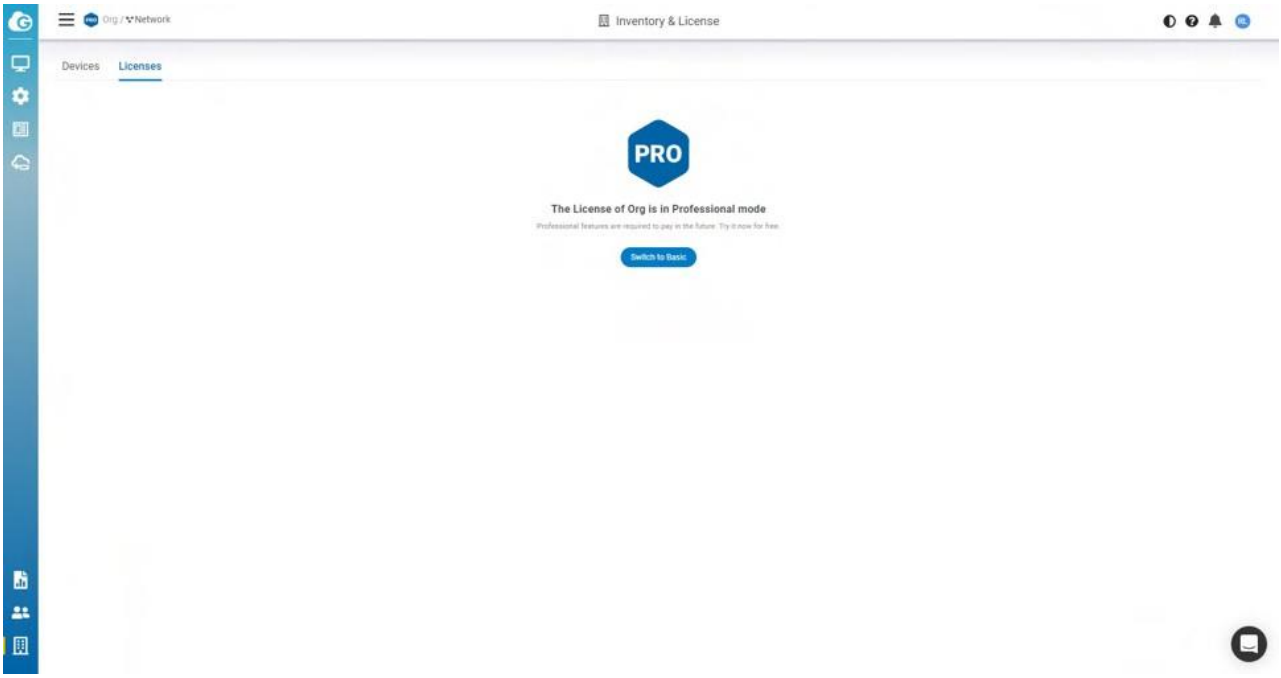
Register a Device

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



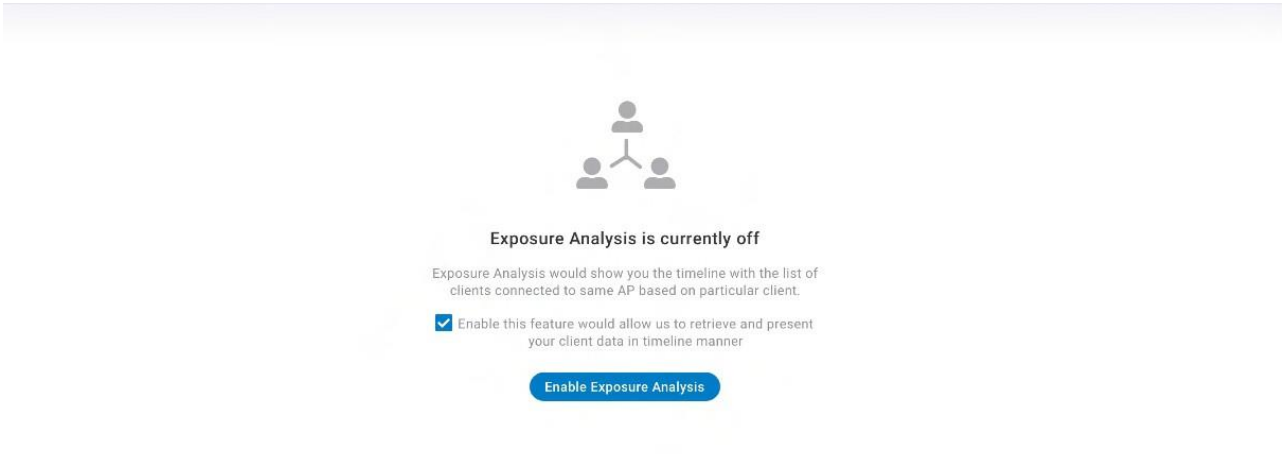
License

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.

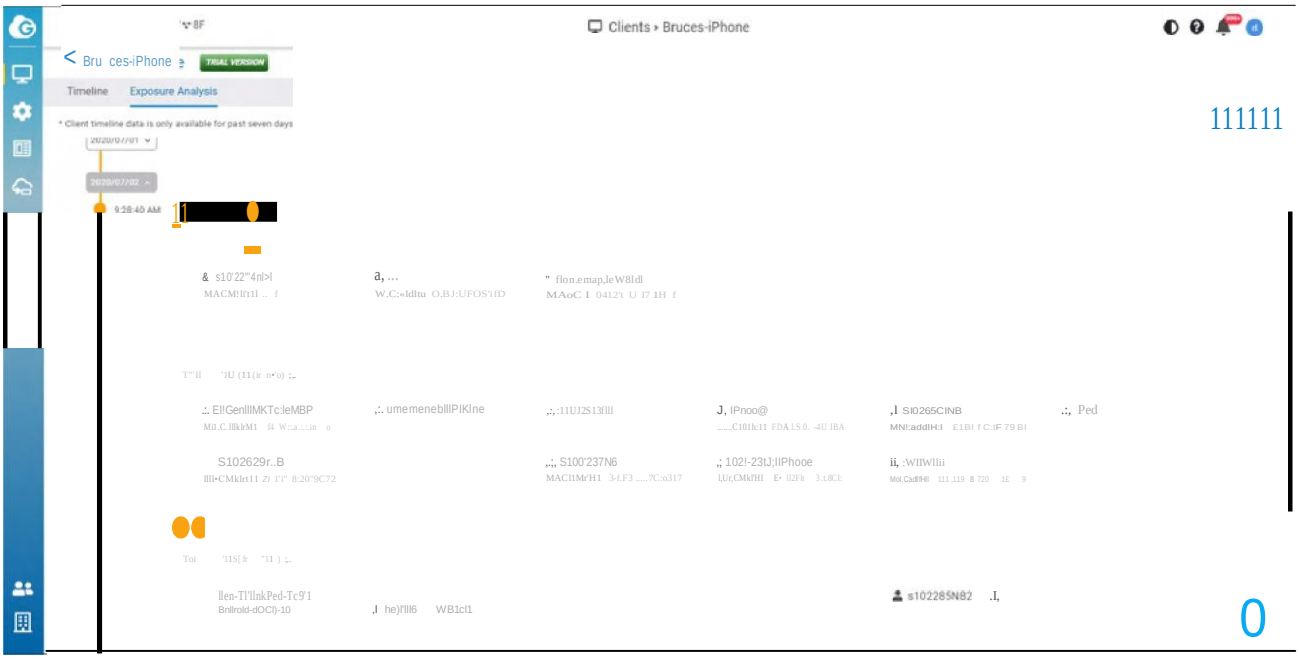


Privacy

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.



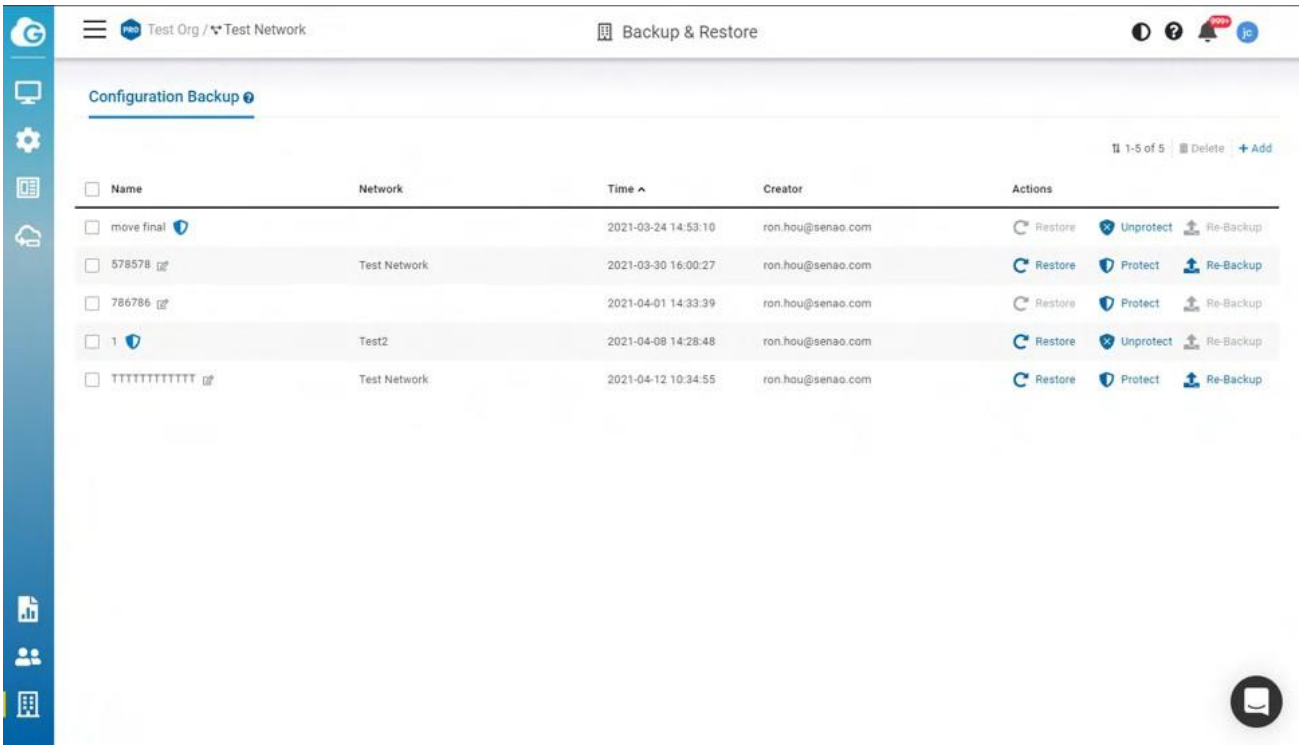
You can click **Manage**=> **Clients** to access this page to see the details after you enable the Exposure Analysis.


Clients ▸ Bruces-iPhone
Bru ces-iPhone
TRIAL VERSION
Timeline
Exposure Analysis
* Client timeline data is only available for past seven days
9:28:40 AM
111111
0

Backup & Restore

Generating a New Backup

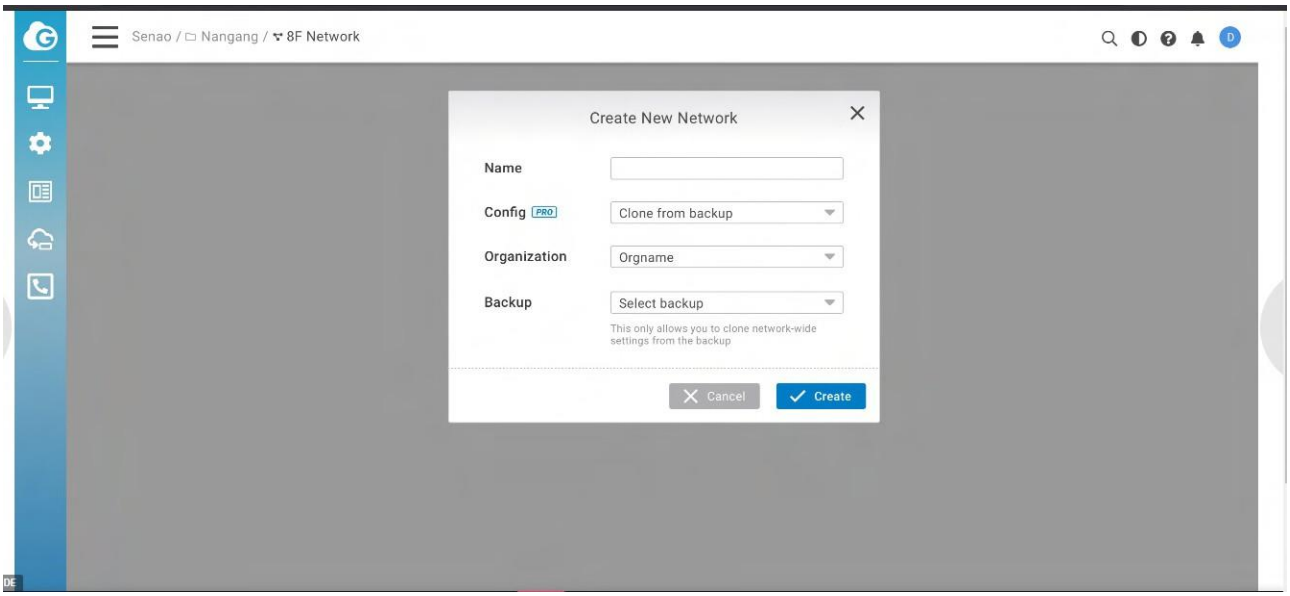
Users can create a new Network-wide setting and device backup by going to **Organizations > Backup & Restore**



- **Restore:** This allows you to restore all settings(Network-wide settings and Device settings) 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

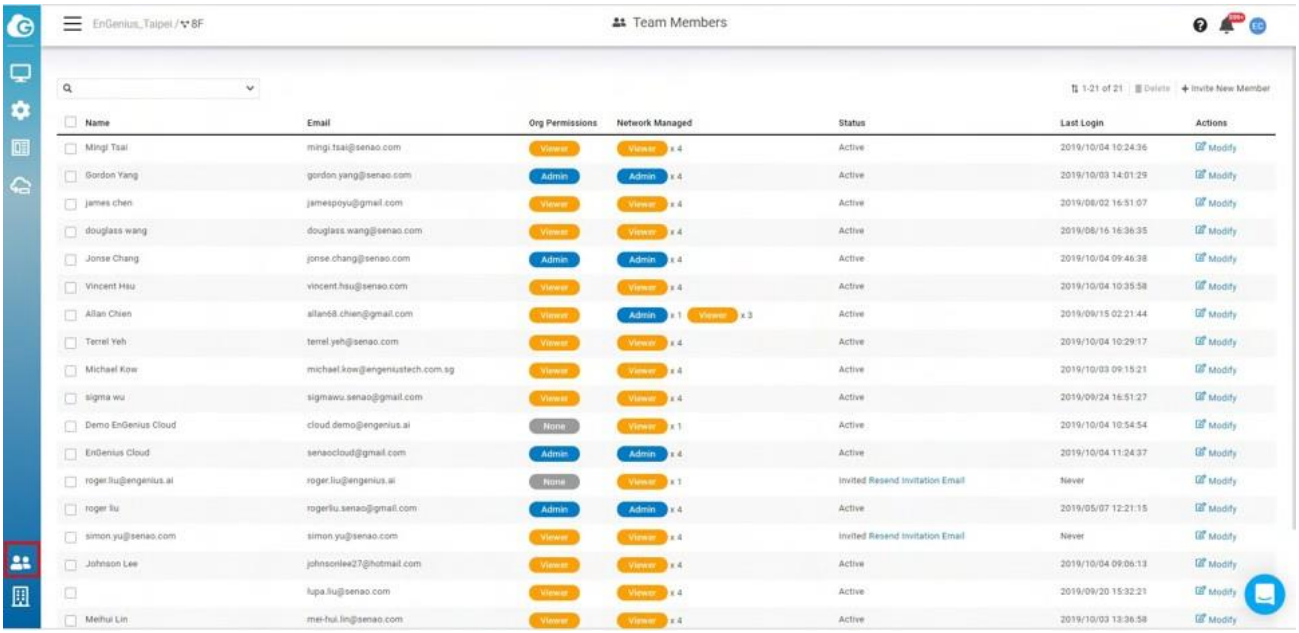
When creating a new network you have the option to clone the configuration from another network. This will copy all network-wide configurations from the existing network with the exception of local device configurations.



Managing Team Members

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

Click **Team Member icon** to access this screen.

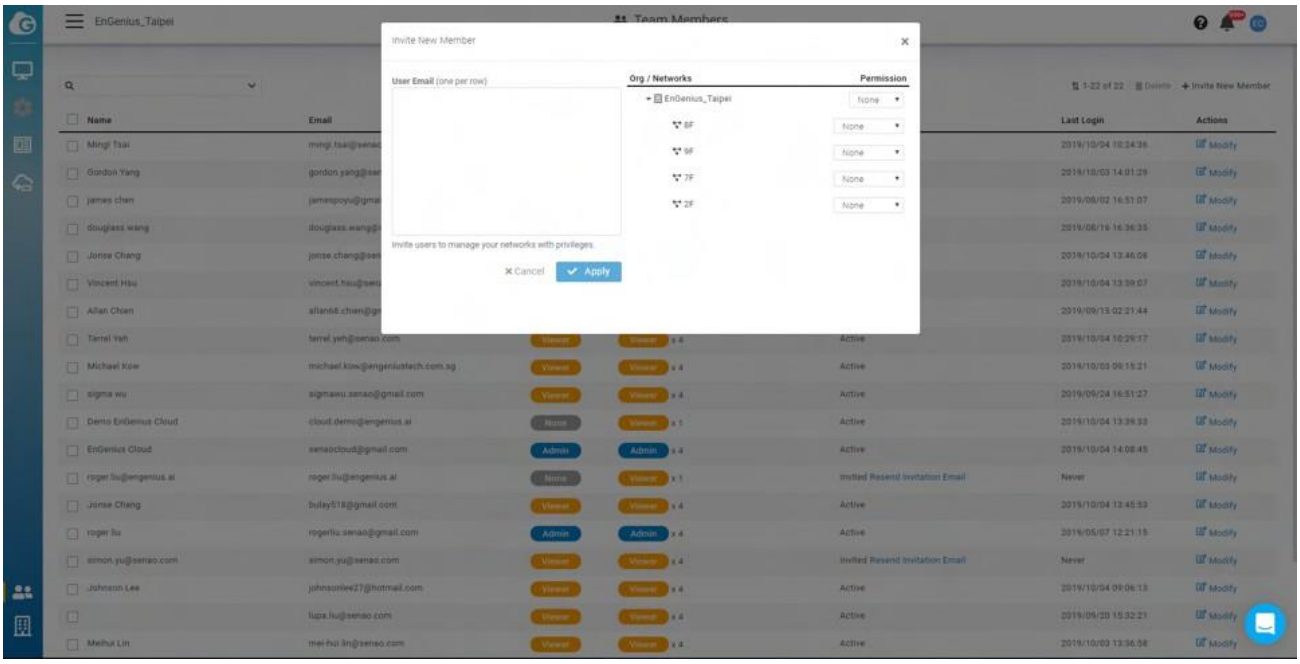


The Team Member page contains the following information about each member:

- **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

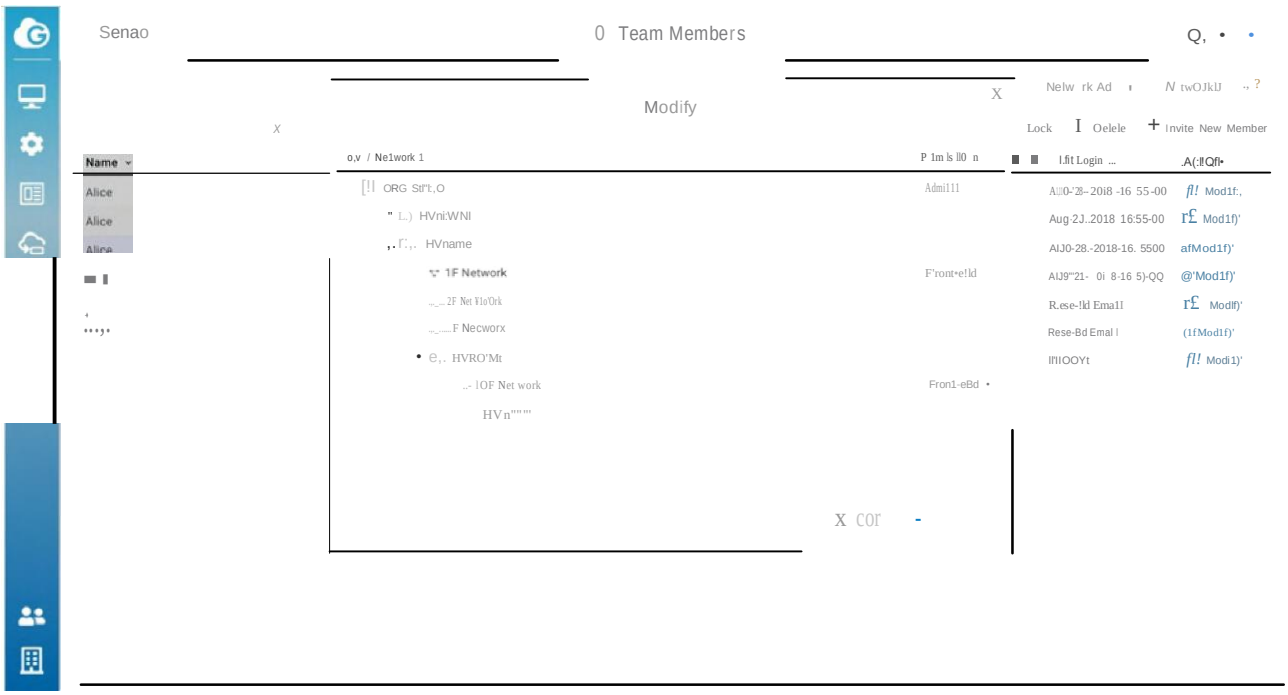
You can invite multiple users and assign them permissions for entire organization trees at once.



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
Nelw rk Ad N twOJkIJ
Lock I Oelele + Invite New Member
Name
Alice
Alice
Alice
o,v / Ne1work 1
P 1m ls ll0 n
ORG Stl"t·,O
Admi111
" L.) HVni:WNI
,. r·:,. HVname
1F Network
F'ront•e!ld
2F Net Flo'Ork
F Necworx
e,. HVRO'Mt
IOF Net work
Fron1-eBd •
HVn""""
l.fit Login ...
A(:lfQfl•
All0-'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 Ema1I
r£ Modlf)'
Rese-Bd Emal I
(1fMod1f)'
lfIIOOYt
fl! Modi1)'
x cor -

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.

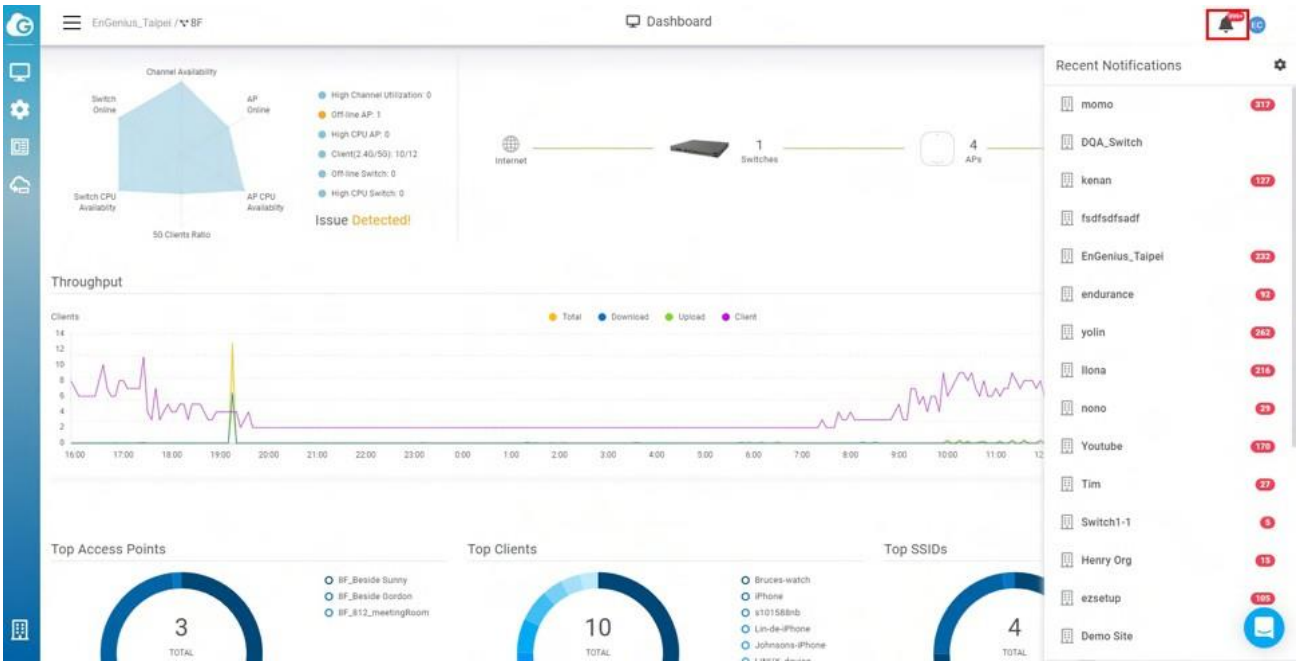
Viewer: user able to access most aspects of a network, including the configuration section, but no changes can be made.

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

Notification & Alerts

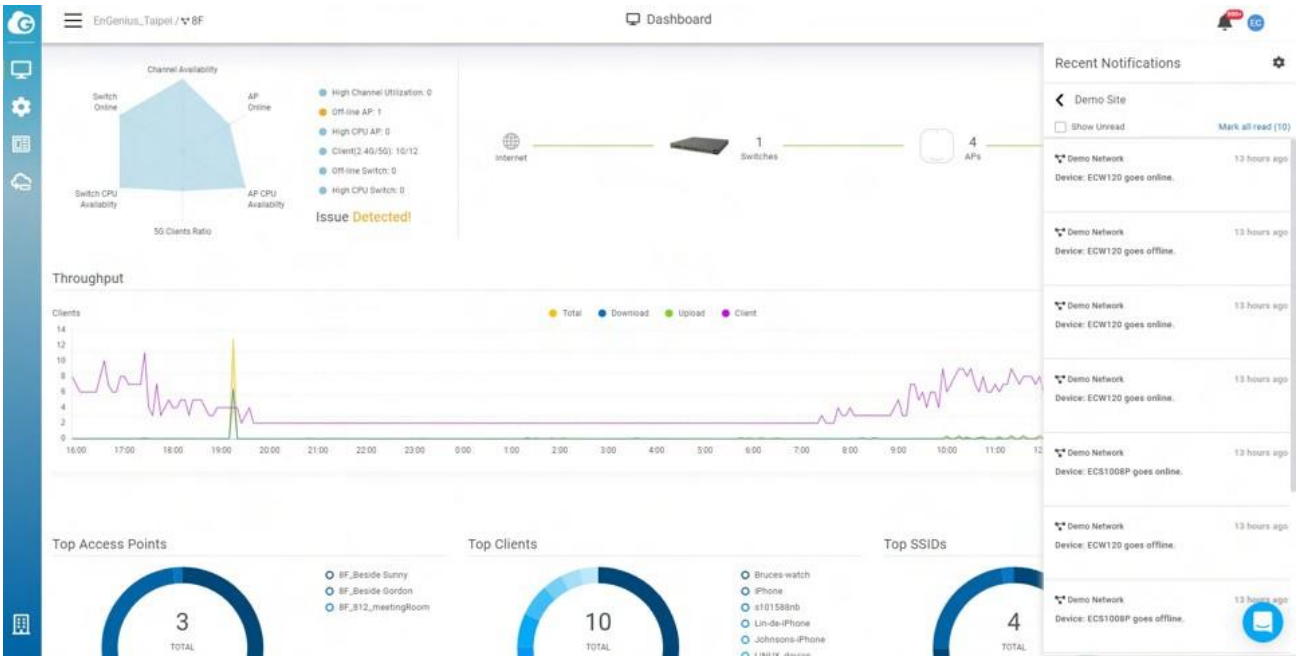
Notification Center

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

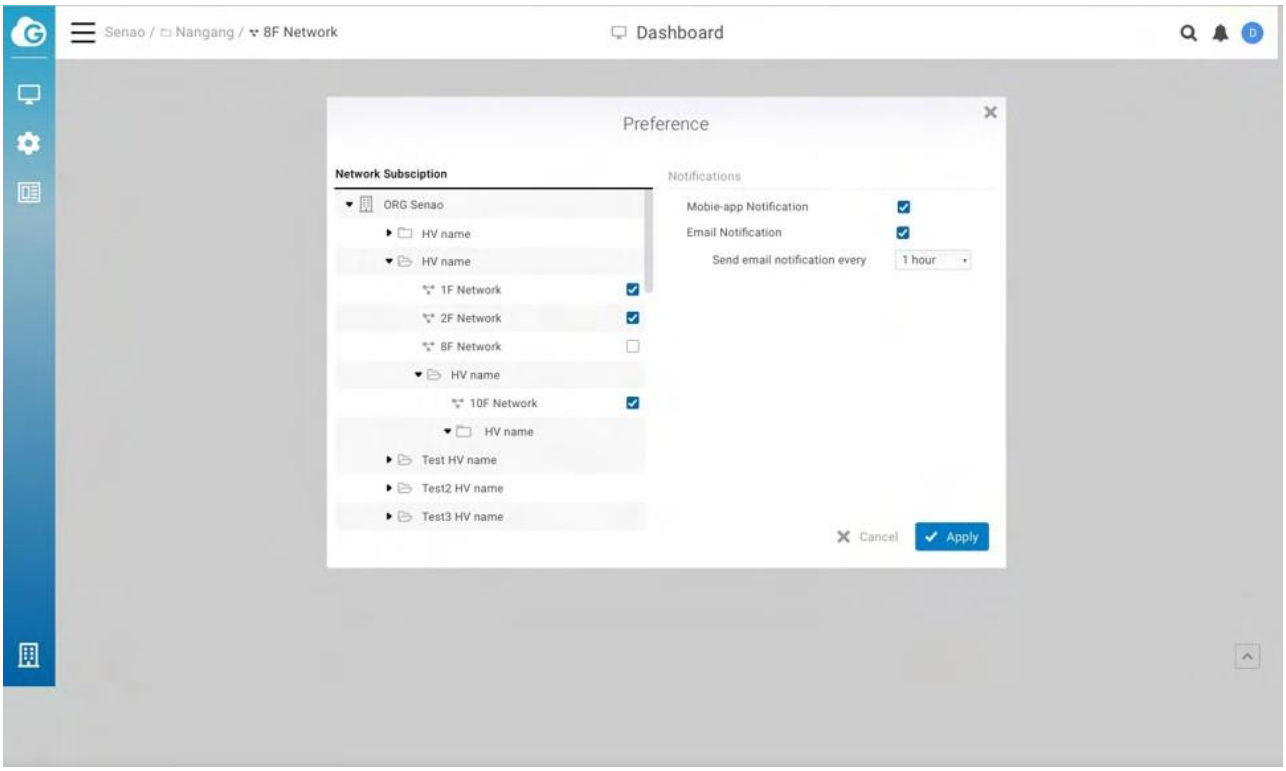
This shows the event numbers that occur and is ordered by organization. You can click one of the organizations in the list to access detailed event information.



Preferences

Network Subscription

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



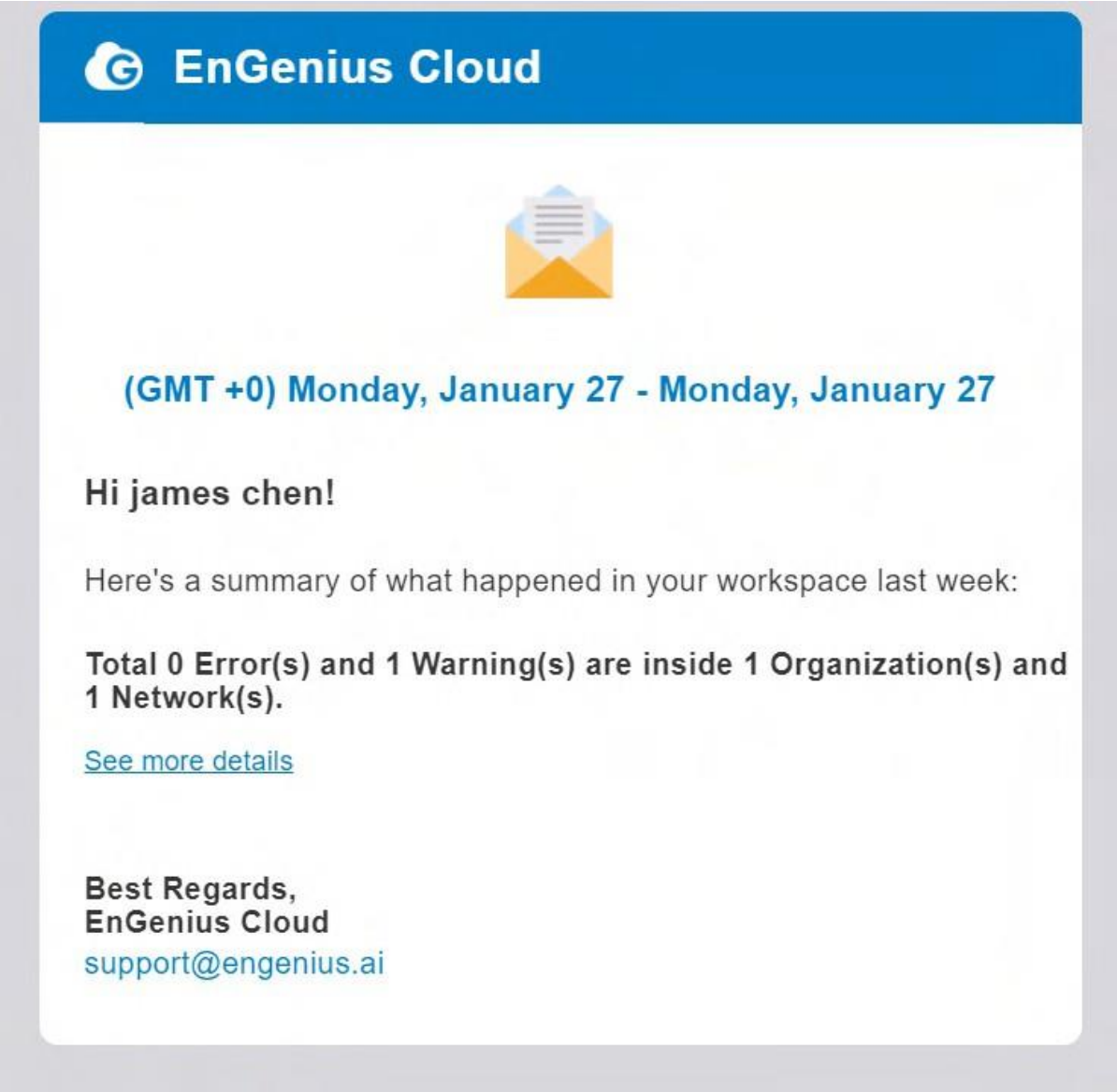
Notifications

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

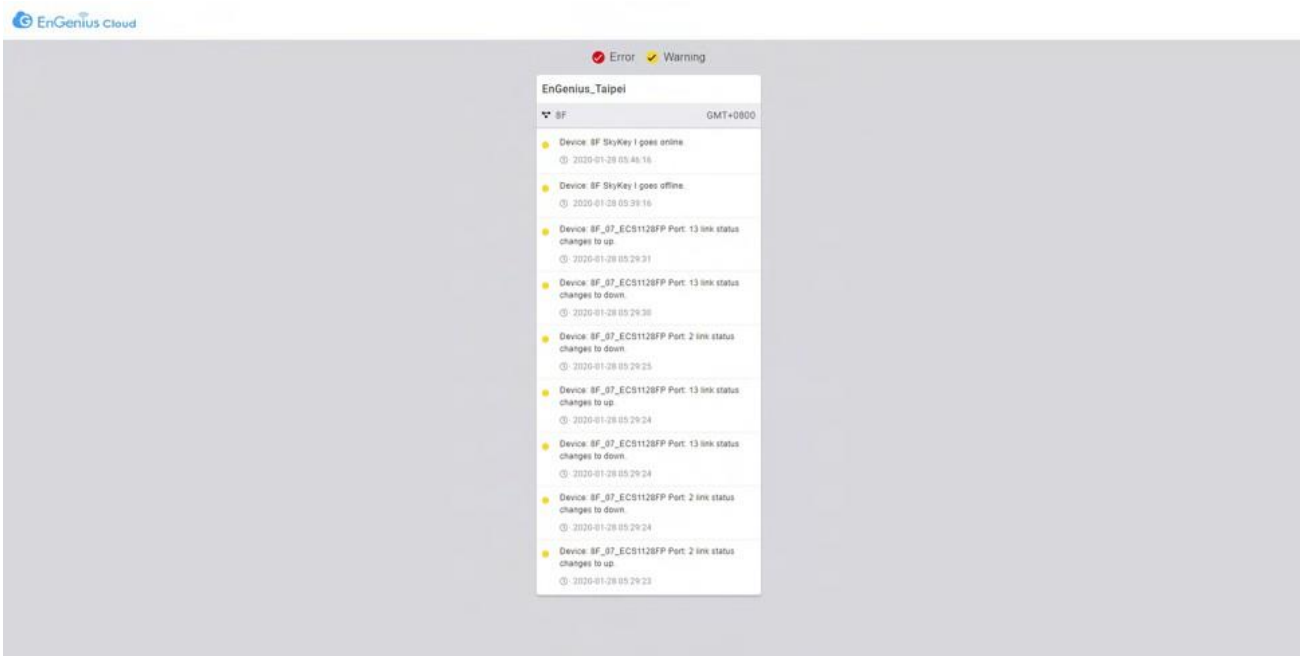
Email Notification: You will receive an email digest of network events at a scheduled time if at least one event has occurred.

Email format

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



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

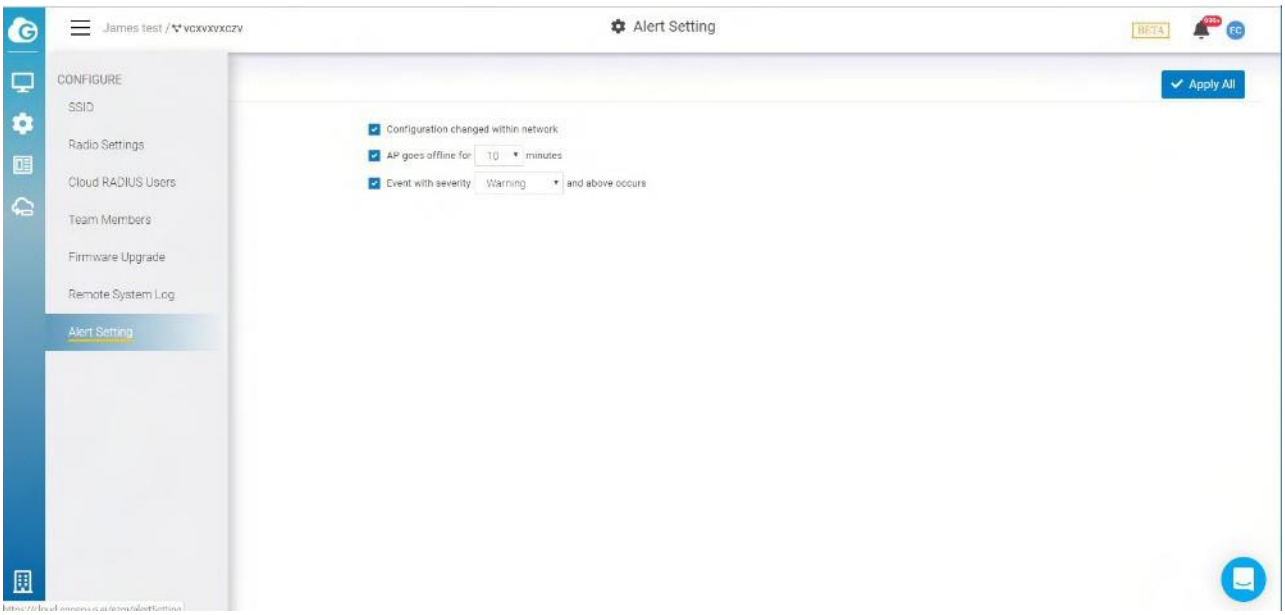


Filter events: On the top of page allows you to filter events. You can check or uncheck the checkbox near error and warning events.

Configuring Alert Settings

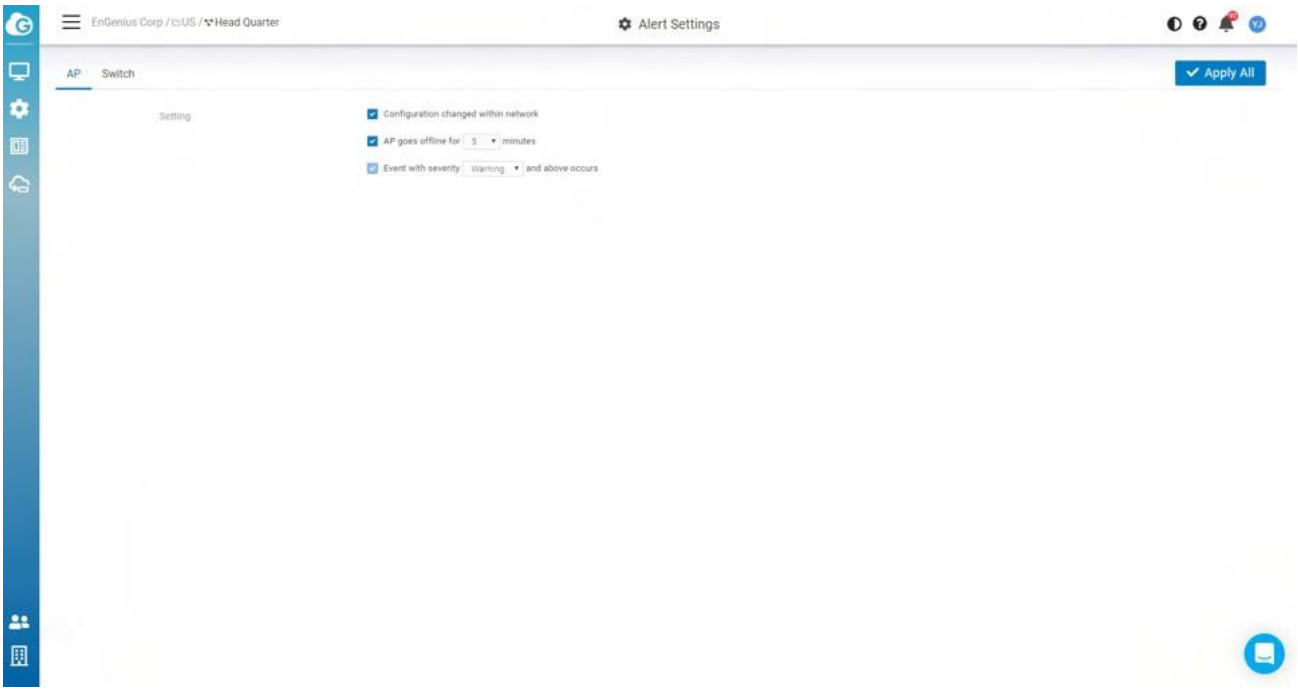
There are a number of options available for email alerts to be sent when certain network or device events occur.

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



Access Point Alerts

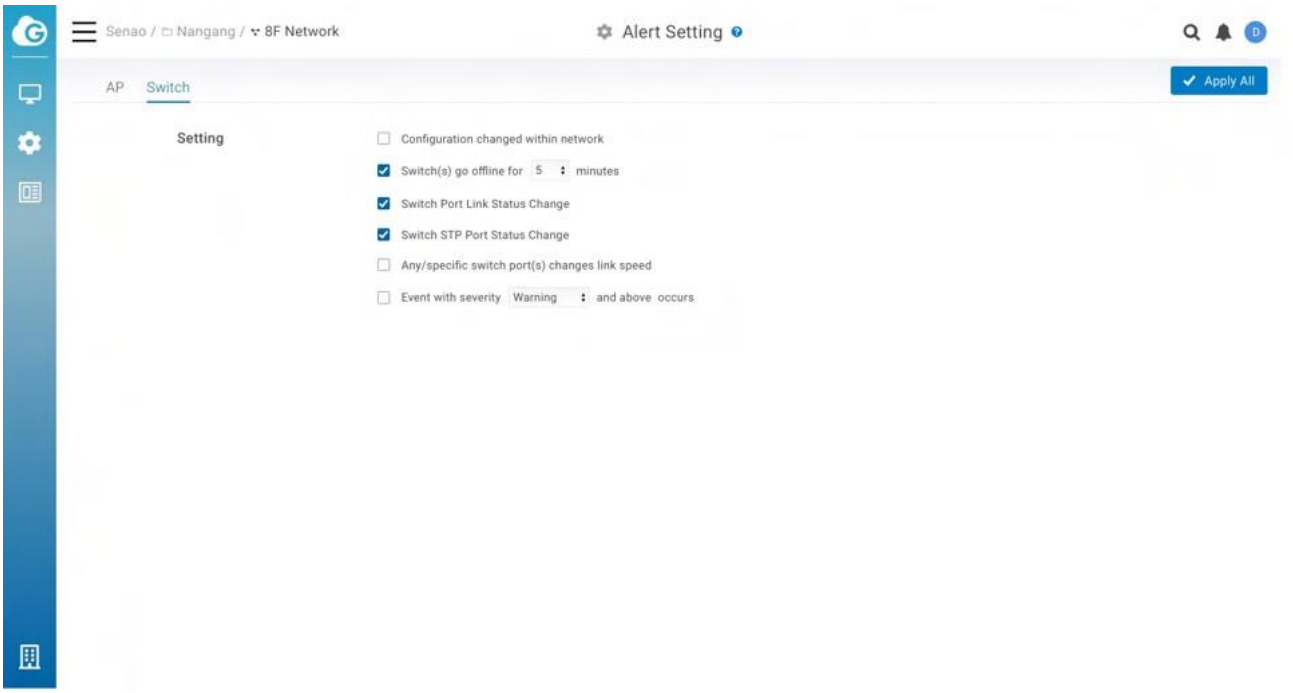
Alerts can be configured for the following access point events:



- **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:



- **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.

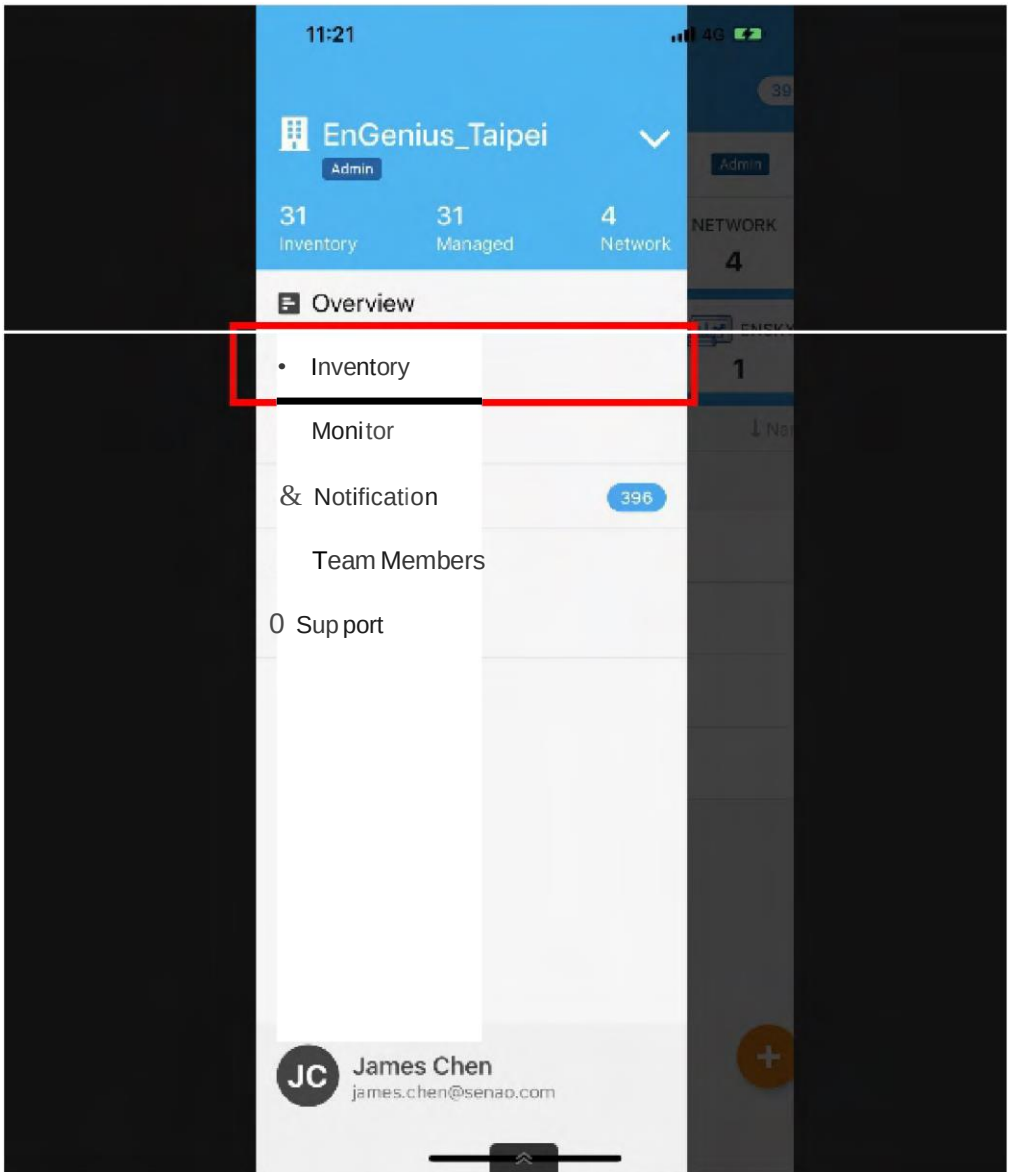
Mobile App

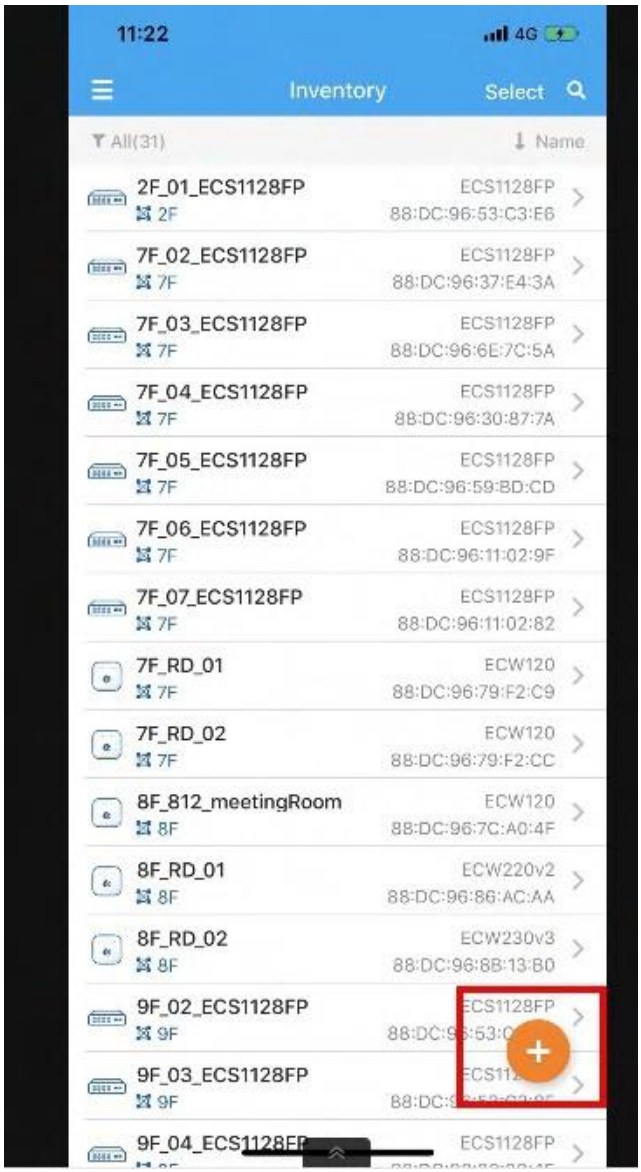
The EnGenius Mobile App is a mobile user interface (UI) for EnGenius Cloud. You can keep an eye on your network when you are on the go. This is a great solution for around the clock network support. Versions are available for Android on Google Play and iOS via the App Store.

Adding a Device

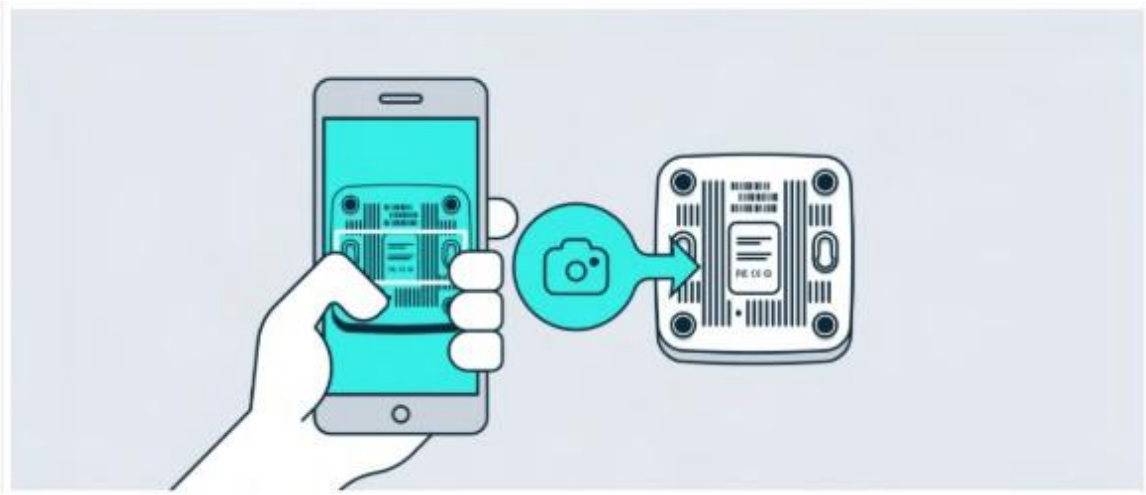
This section explains how to add a networking device to your network using the EnGenius Mobile App.

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


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

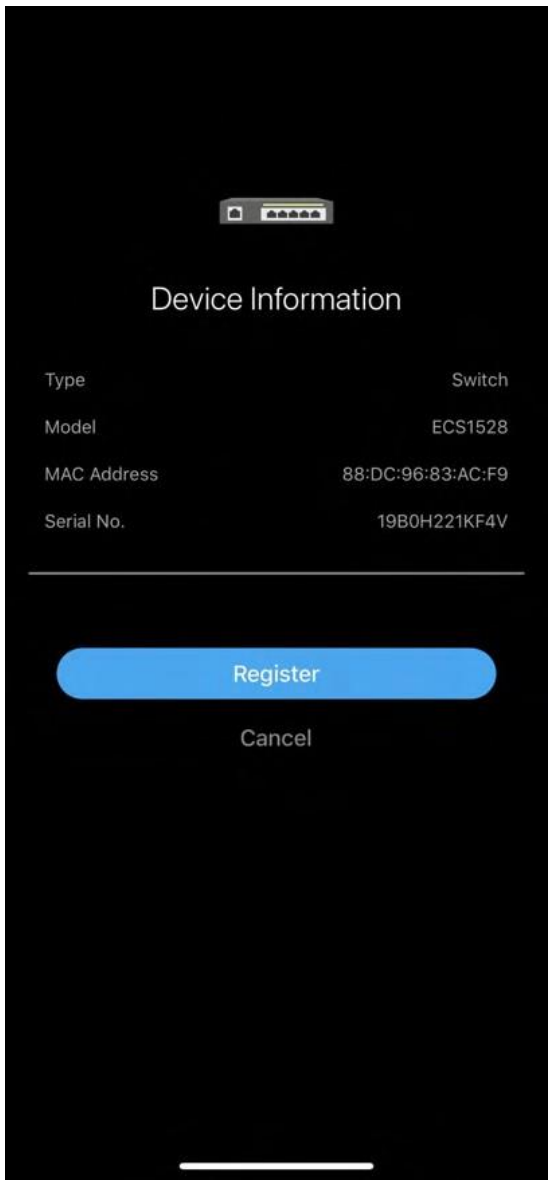


2. Find the QR code at the bottom of the device and scan it.

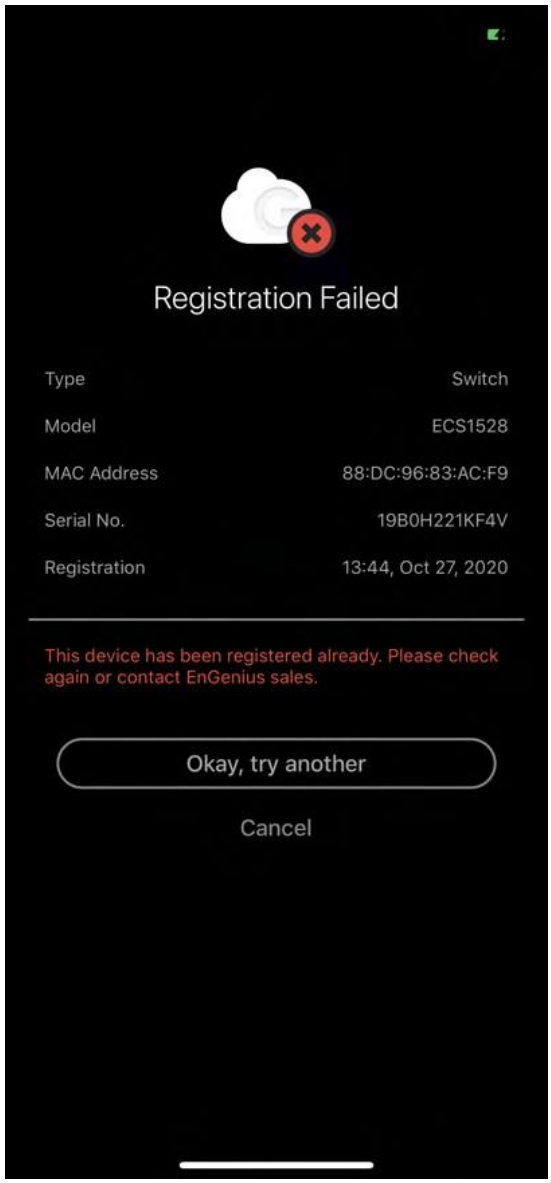


If the camera successfully scanned a QR code, the app will display the Device Information. You could tap

Register to complete the Registration.

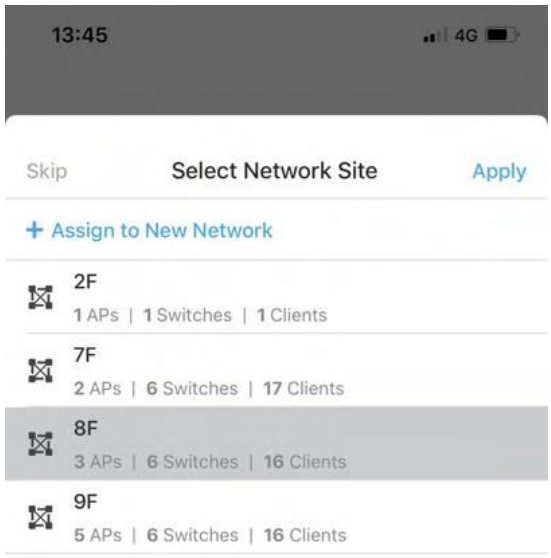


If you failed to scan the QR code successfully, you could tap **Okay, try another**.

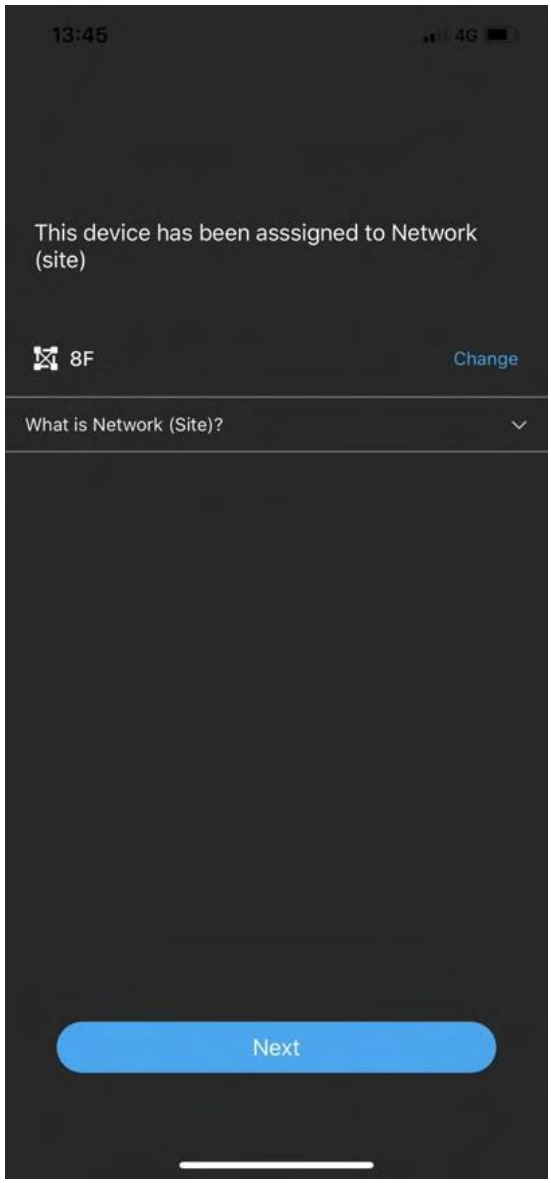


3. Once a device has been successfully registered, you can tap **Assign to Network site now.**

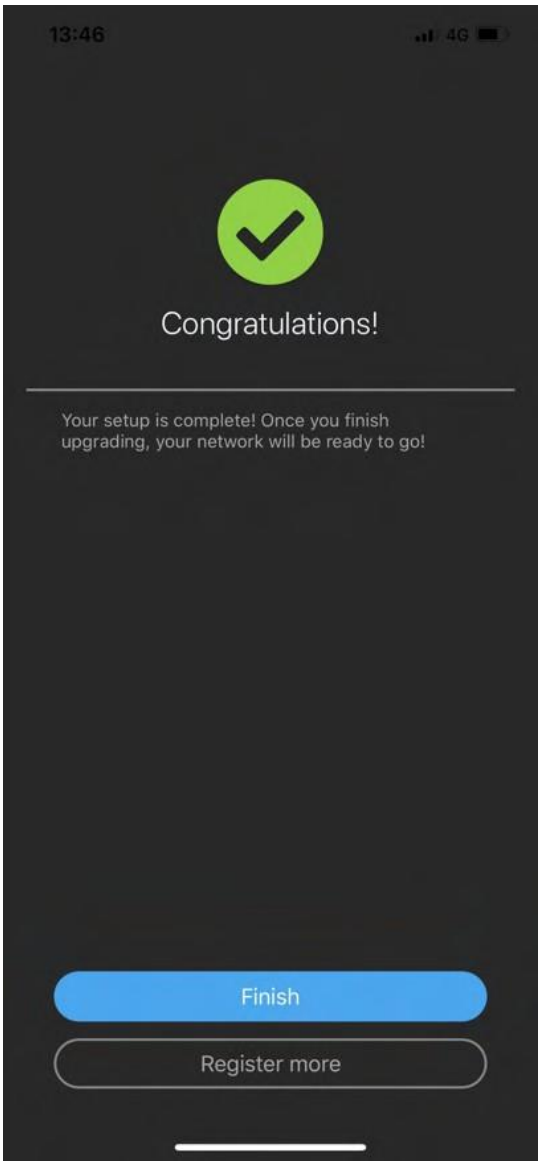
5. Tap the Network and tap **Apply**.



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



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


13:46
4G
Congratulations!
Your setup is complete! Once you finish upgrading, your network will be ready to go!
Finish
Register more

Get Remote Support

LiveChat

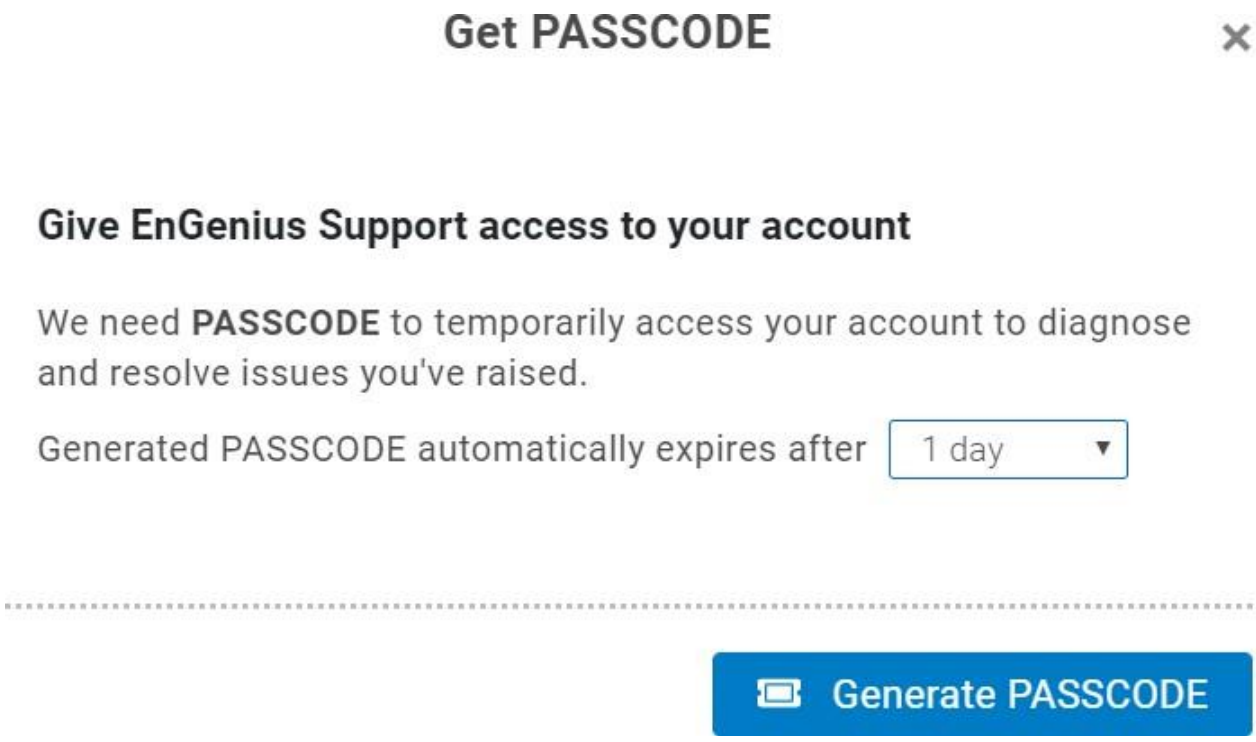
Whenever you login the system, you can always find a `LiveChat` button at bottom-right corner of the page.

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`.



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.

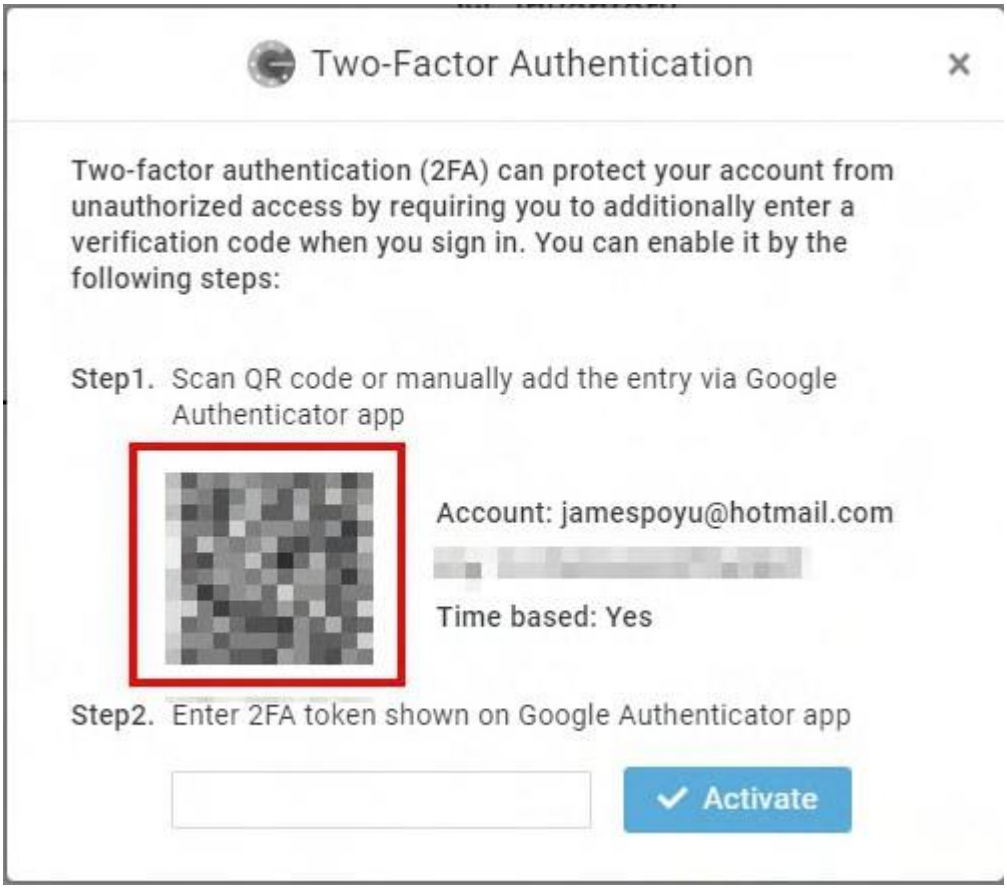
How to Enable 2FA to protect your account

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**.

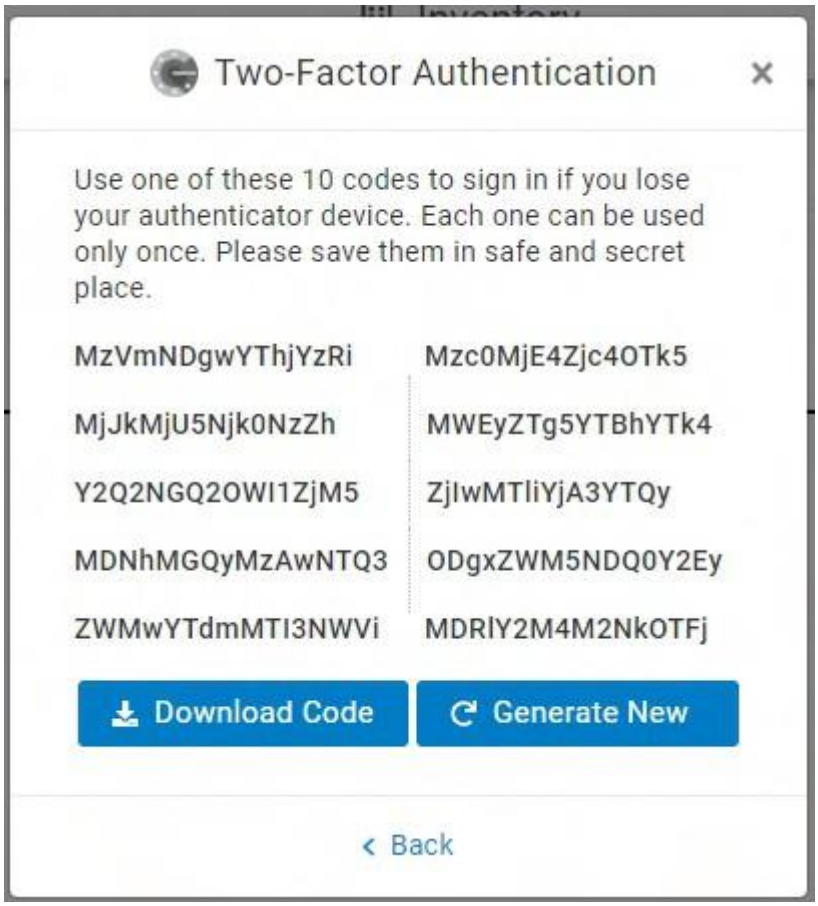
4. Your phone will now be in the "scanning" mode. Go ahead and scan the QR code that appeared in the popup.



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).



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

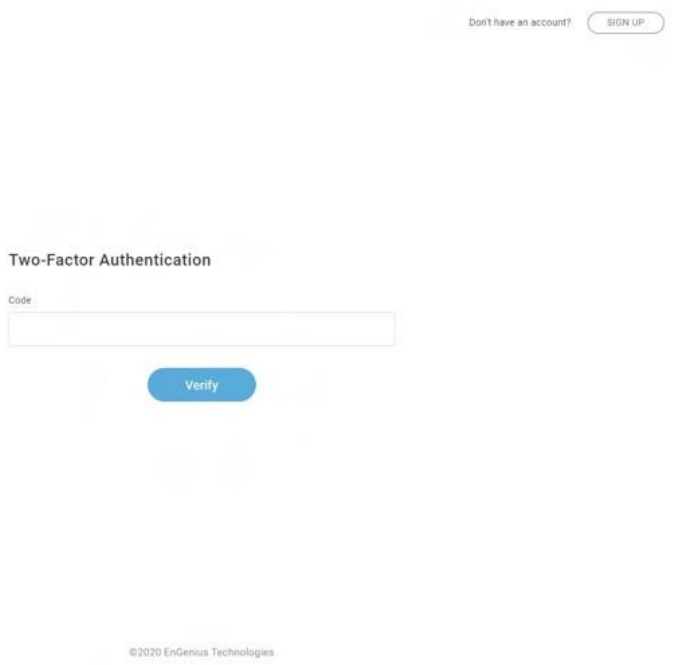
1. Select **Two Factor Authentication** from the top-right menu.
2. Click **Deactivate**

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.



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 .**

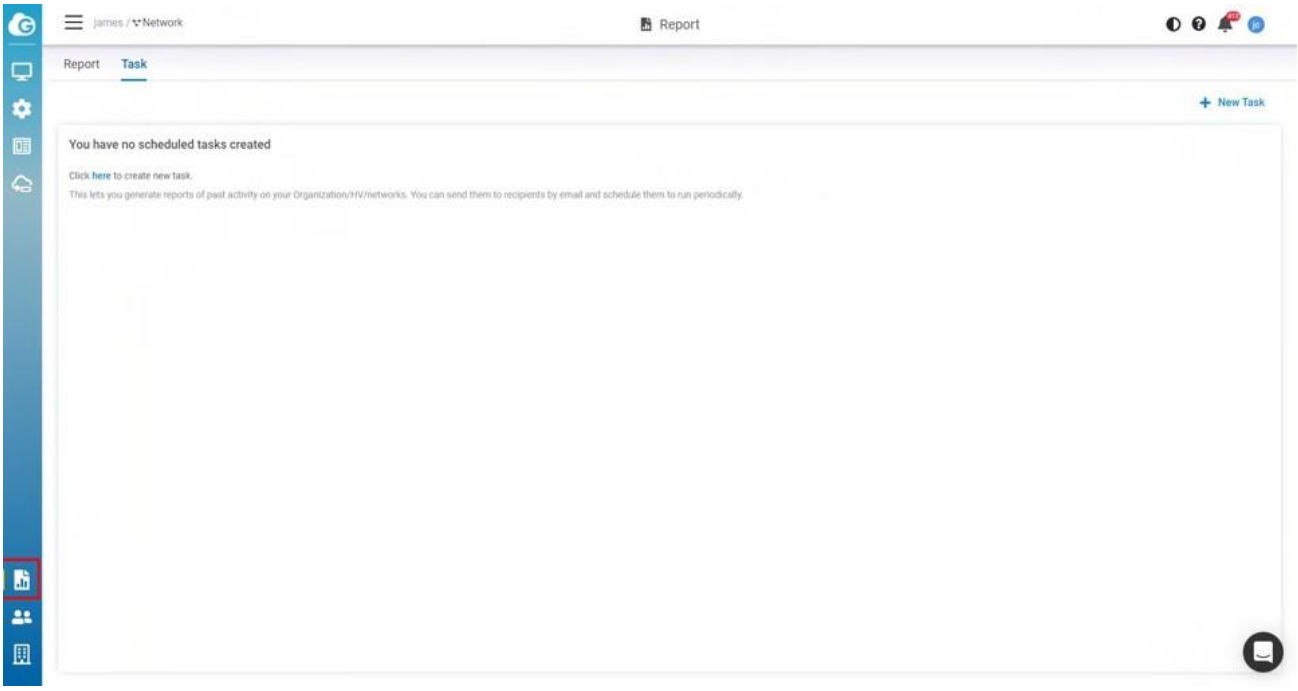
> If the user manages multiple Organizations and does not enable 2FA, he is still able to log in to Cloud. However, he cannot access the Org with 2FA enforcement enabled as a requirement.

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.

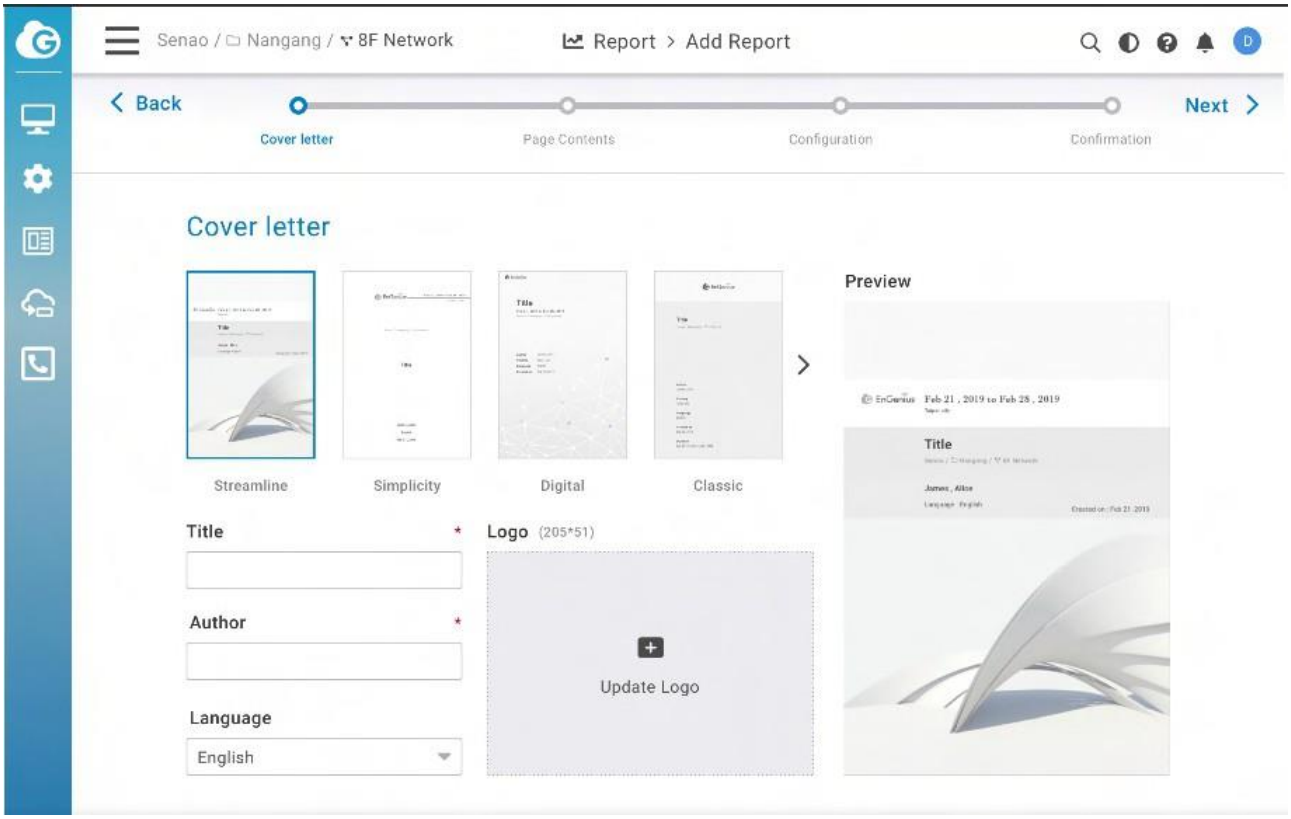


When you click on this button a new wizard will be displayed with the steps to customize report content directly

Cover letter

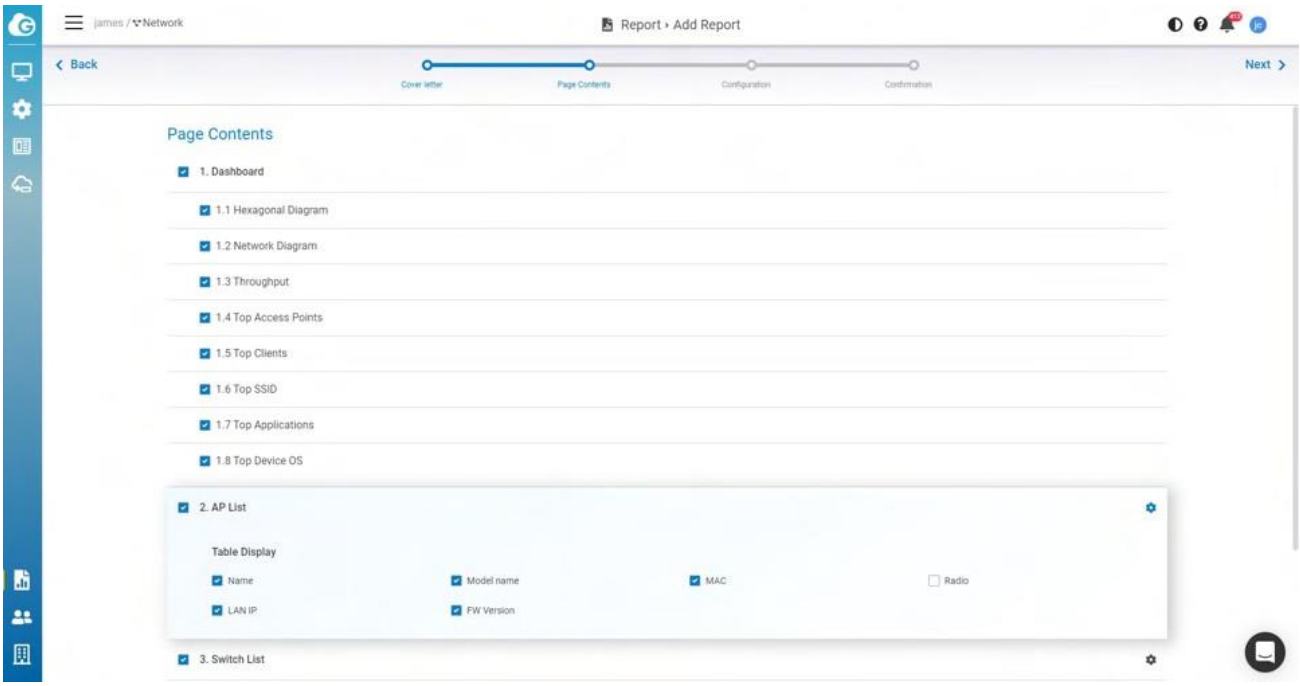
- **Author**: Input Author and will be displayed in report cover letter)

- **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)



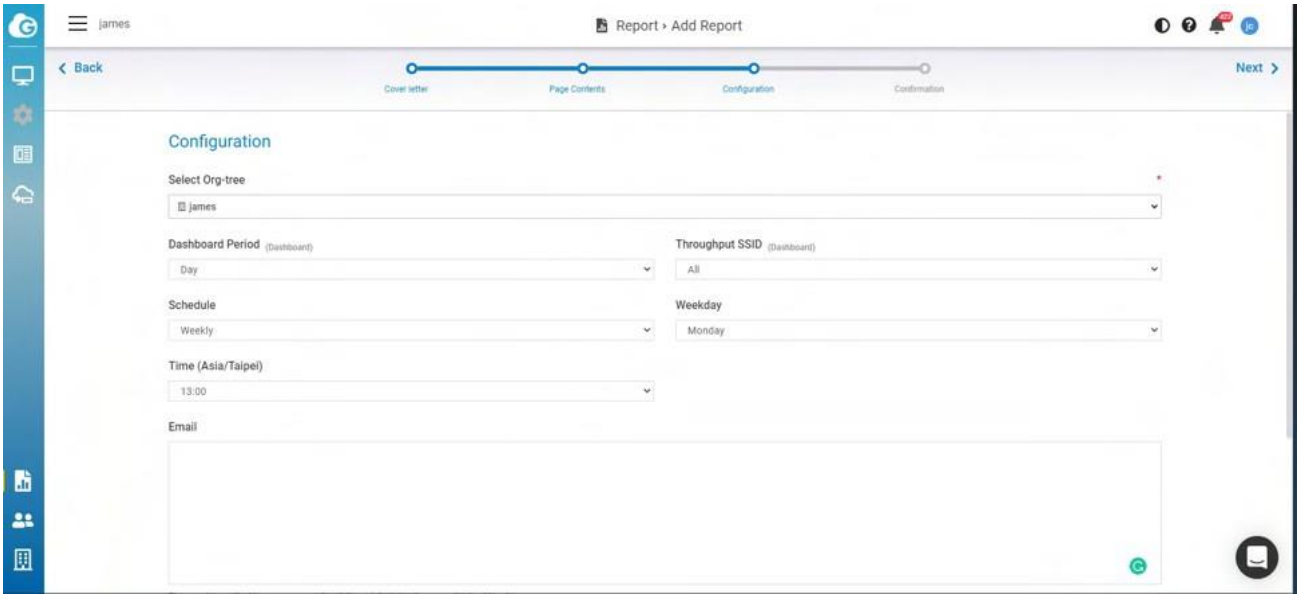
Page Content

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.



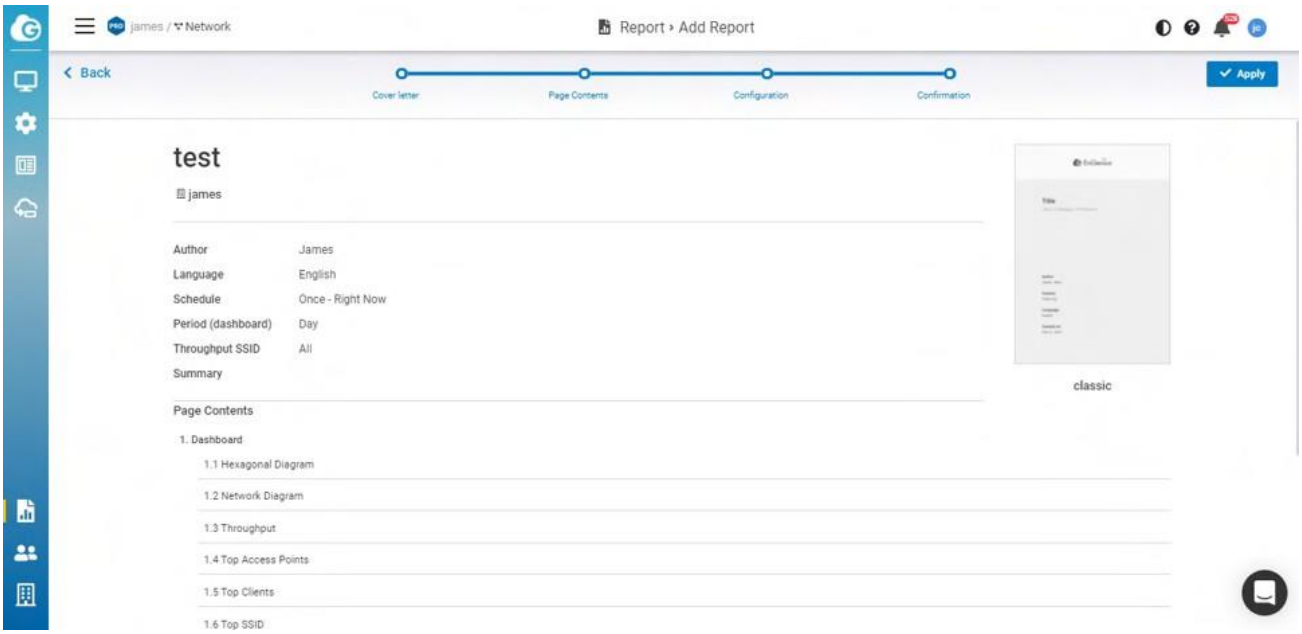
Configuration

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)



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.

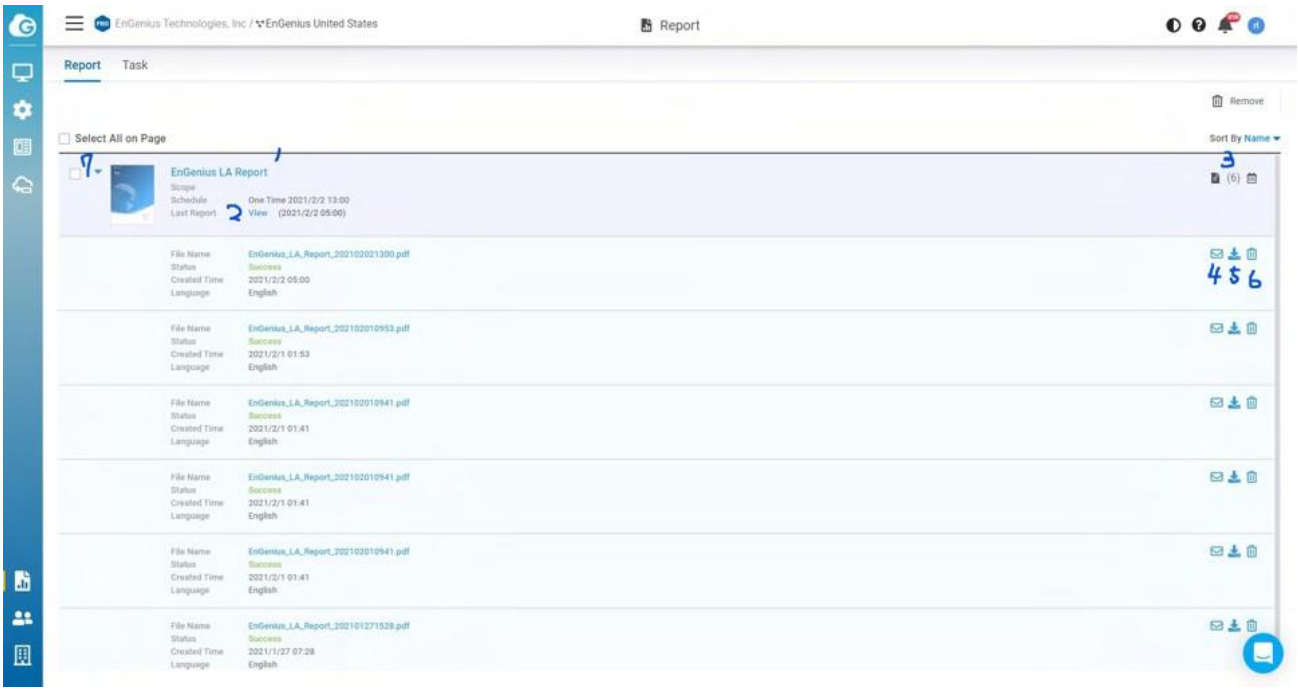


Reports View

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:

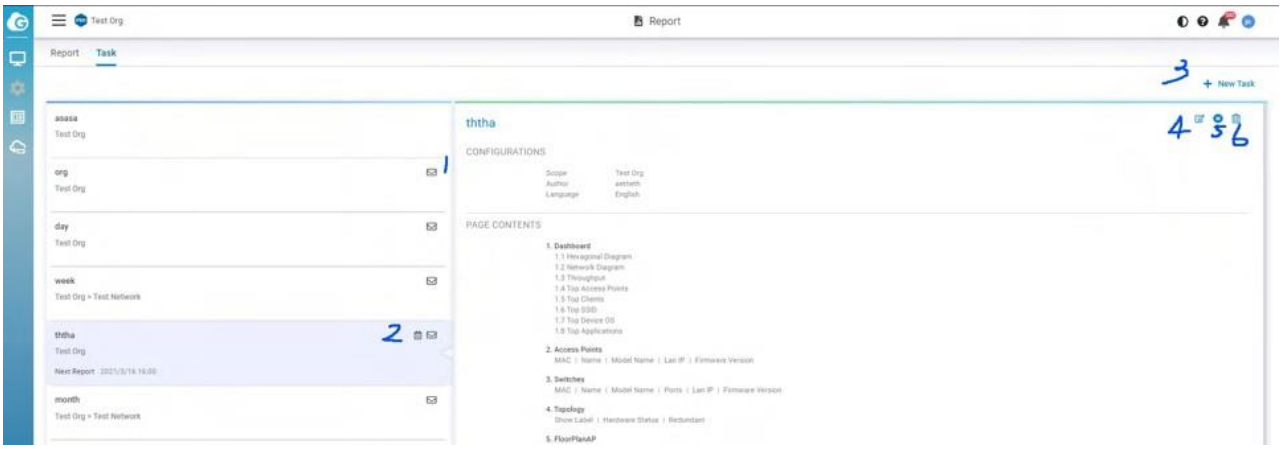
1. **Task name** (same as report name): Click to navigate to corresponding tasks.
2. **Last report:** You can easily download the last generated report by hyperlink.
3. Numbers of reports generated by same tasks.
4. Allows you to email this report to someone.
5. Download report.
6. Delete report.



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.



Appendix

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

Mounting the AP

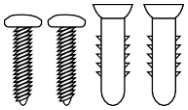
Using the provided hardware, the AP can be attached to a wall or a ceiling.

1. Managed Indoor Access Point

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

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

4. Mounting Screw Kit

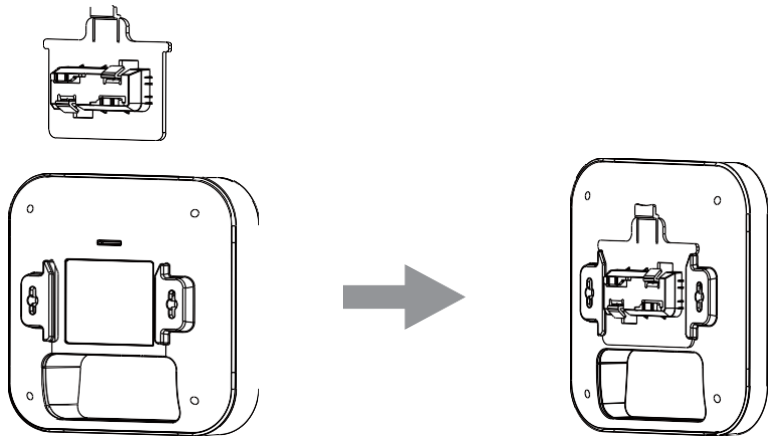


Ceiling Mount an Access Point

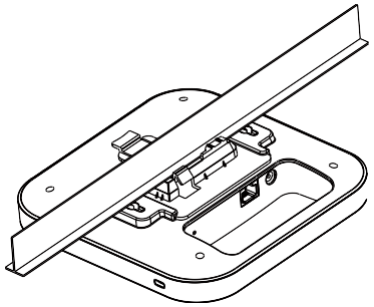
1) Slide the ceiling mount base into the slot of the Access Point.

2) Hold the Access Point with one hand to reach the other hand over the T-Rail sides of the bracket. Then hook the stationary end of the ceiling mount bracket onto the T-Rail.

1



2

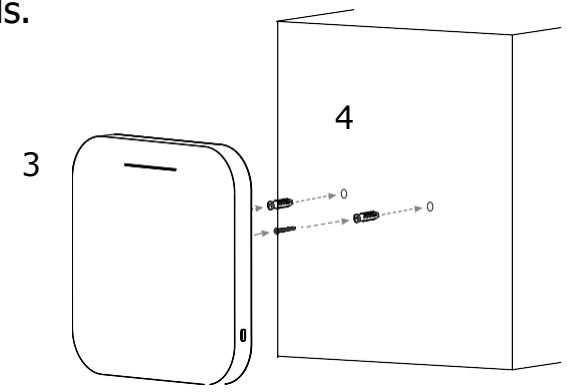


Wall Mount an Access Point

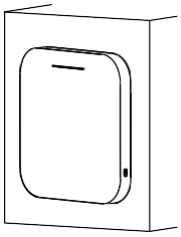
3) Continued from A, determine where the Access Point to be placed and mark location on the surface for the two mounting holes. Use the appropriate drill bit to drill two 8.1mm diagram and 26mm depth holes in the markings and hammer the bolts into the openings.

4) Screw the anchors unto the holes until they are flush with the wall ; screw the included screws into the anchors.h

5) Place the Access Point against wall with the mounting screw heads.



5



FCC 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.

NOTE: 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 or more 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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

ISED Statement:

This device contains licence-exempt transmitter(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) this device may not cause interference,

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) L'appareil ne doit pas produire de brouillage;

(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et un corps humain.

WiFi 5GHz Band 1 indoor use only.
WiFi 5GHz Bande 1 à usage intérieur uniquement.