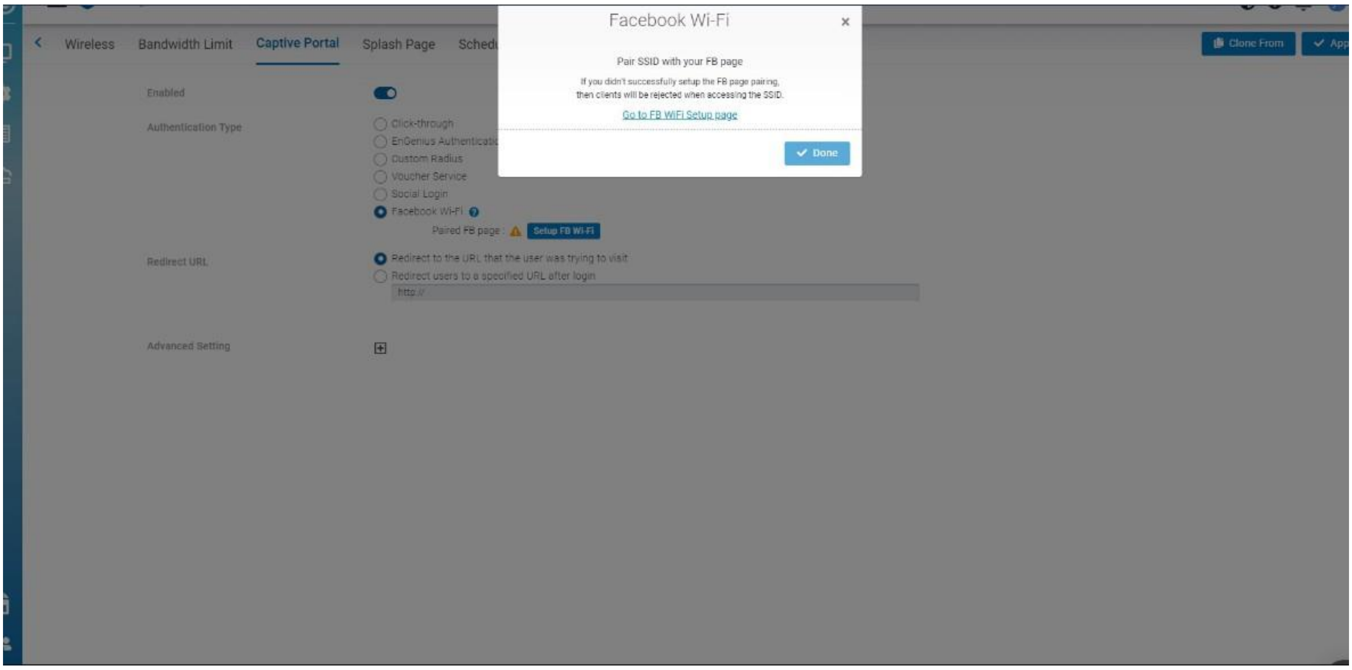
3. You will now see a link ‘**Go to FB Wi-Fi Setup page**’. Clicking on this link will take you to your Facebook Wi-Fi settings page.



Enabled

Authentication Type
○ Click-through
○ EnGenius Authenticati
○ Custom Radius
○ Voucher Service
○ Social Login
● Facebook Wi-Fi
Paired FB page : ⚠ Setup FB 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

Facebook Wi-Fi ×

Pair SSID with your FB page

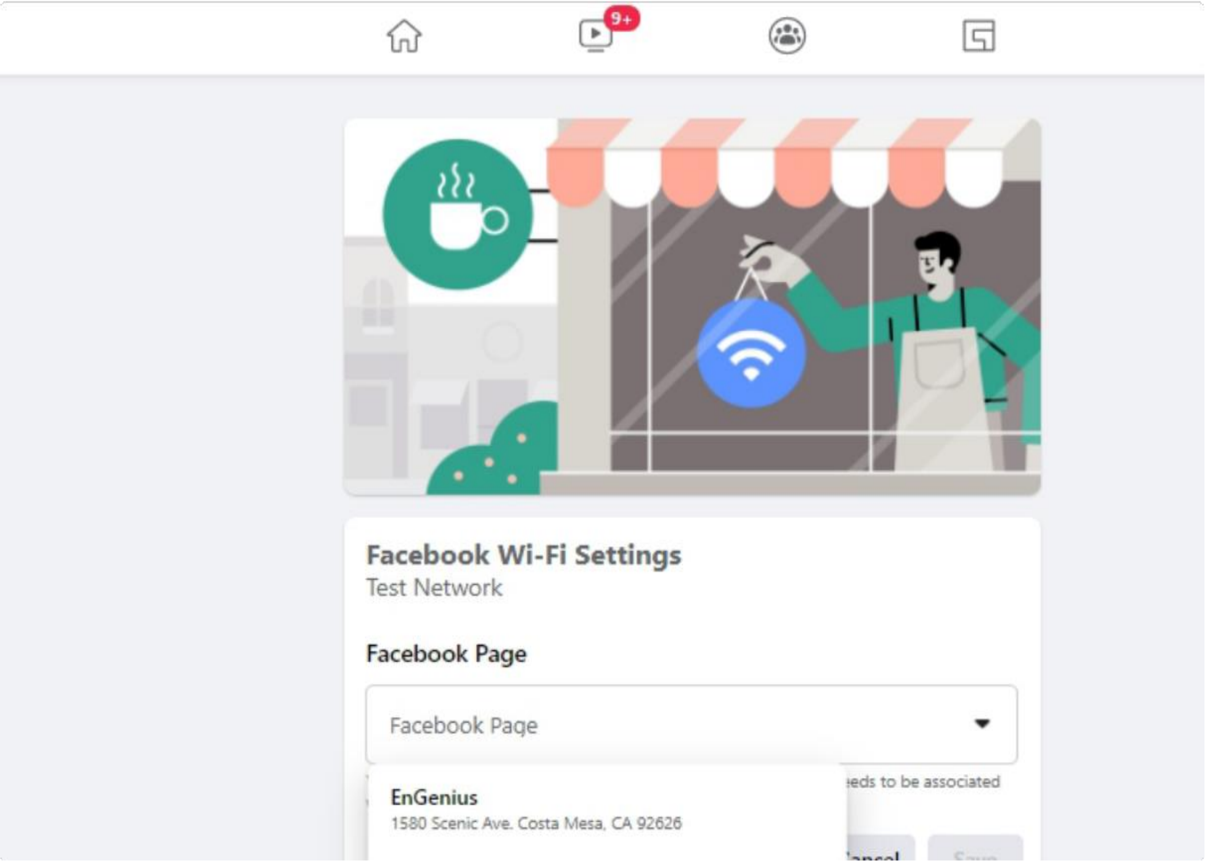
If you didn't successfully setup the FB page pairing, then clients will be rejected when accessing the SSID.

Go to FB WiFi Setup page

✓ Done

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:



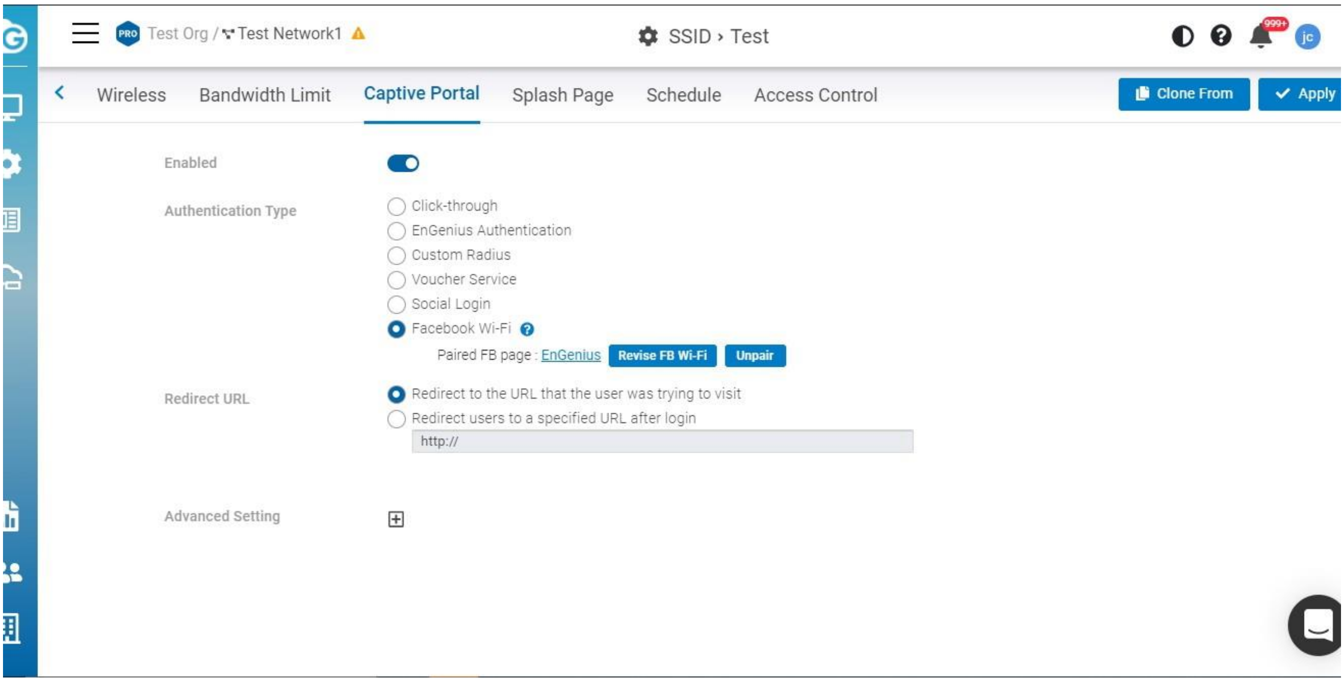
Facebook Wi-Fi Settings
Test Network

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

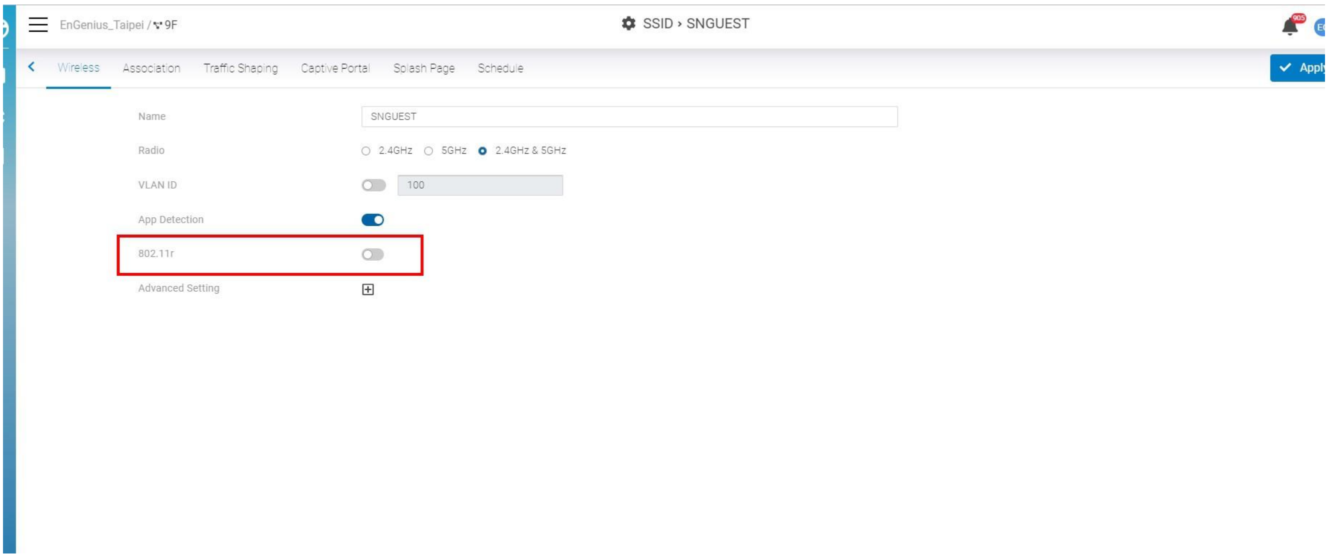
Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login
http://

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

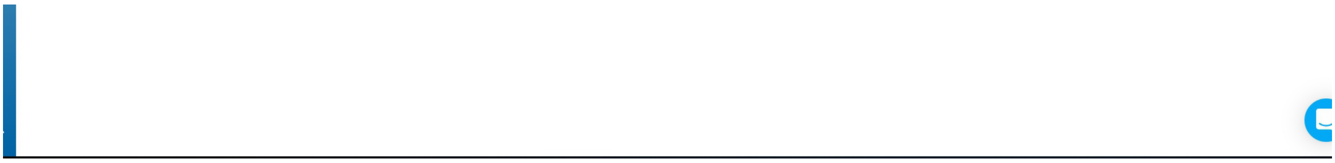
Radio: ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

VLAN ID: 100

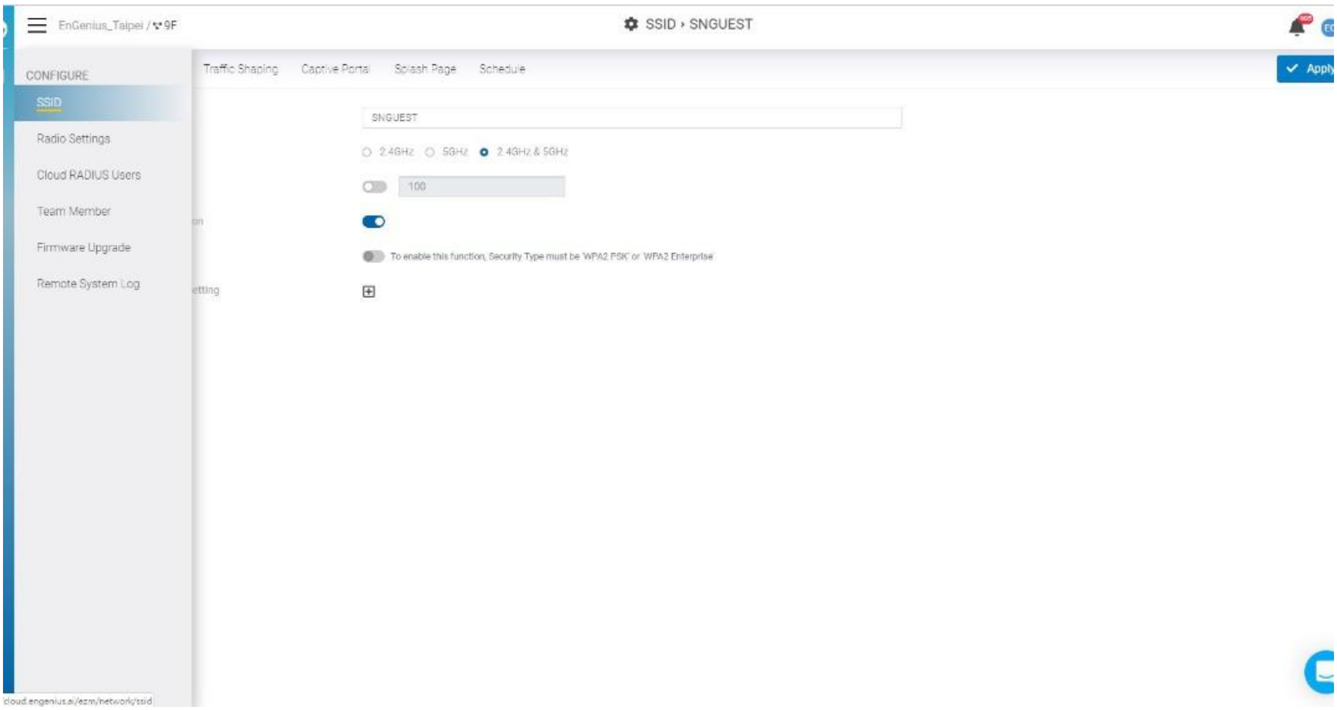
App Detection

802.11r

Advanced Setting ⊞



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



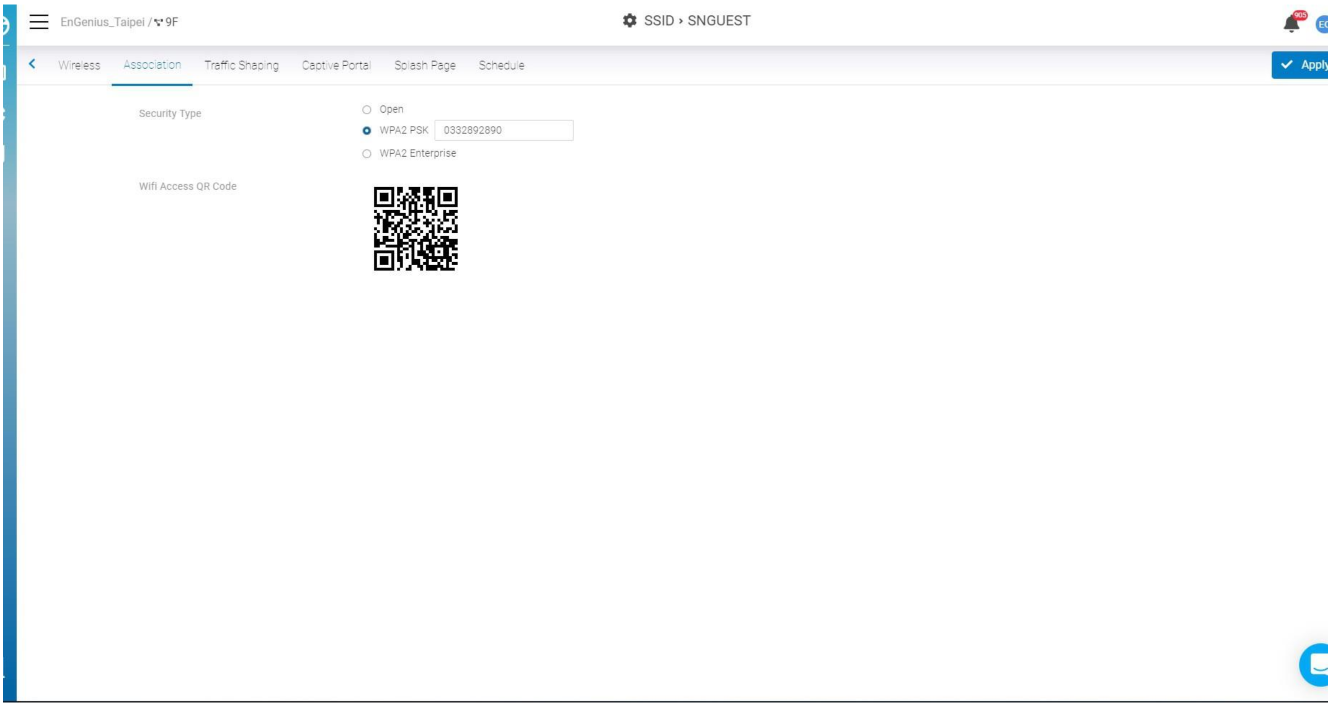
SNGUEST

○ 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.



Security Type
○ Open
● WPA2 PSK 0332892890
○ WPA2 Enterprise

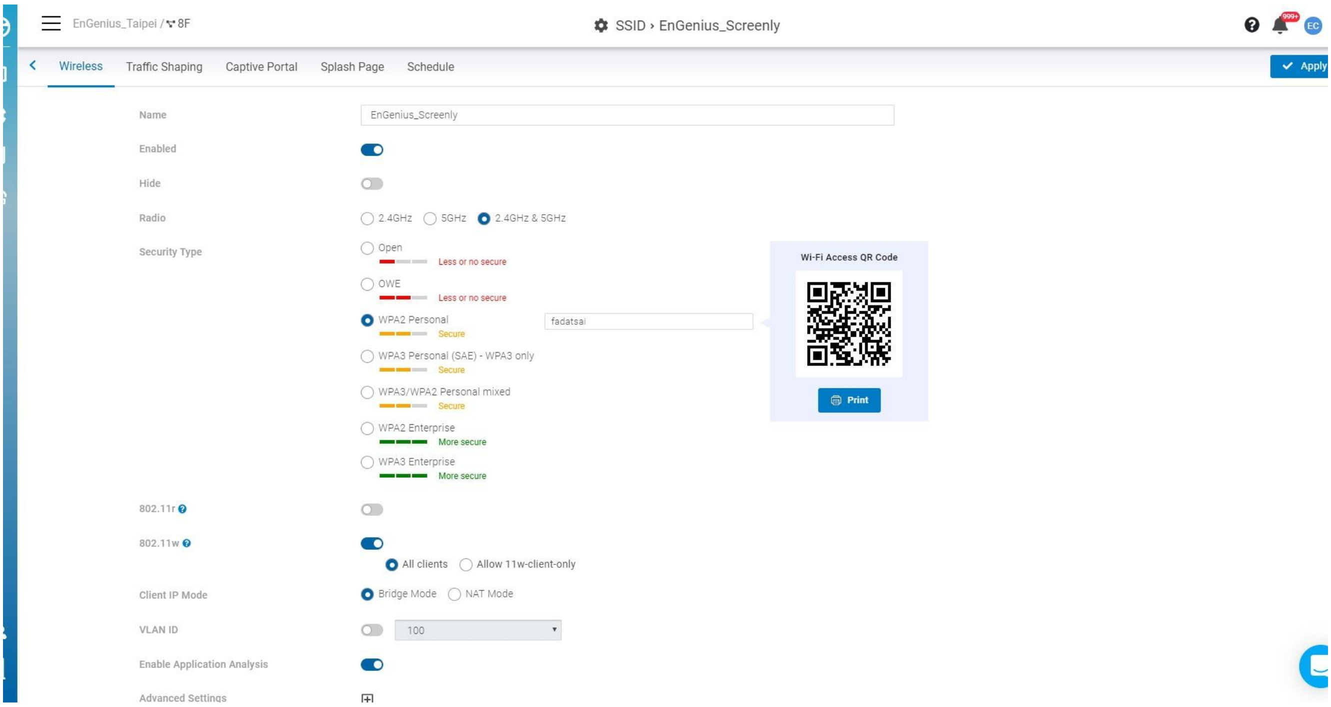
Wifi Access QR Code

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**.**


EnGenius_Taipei / 8F
SSID › EnGenius_Screenly
Wireless | Traffic Shaping | Captive Portal | Splash Page | Schedule

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 — fadatsai
○ 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 ⊞

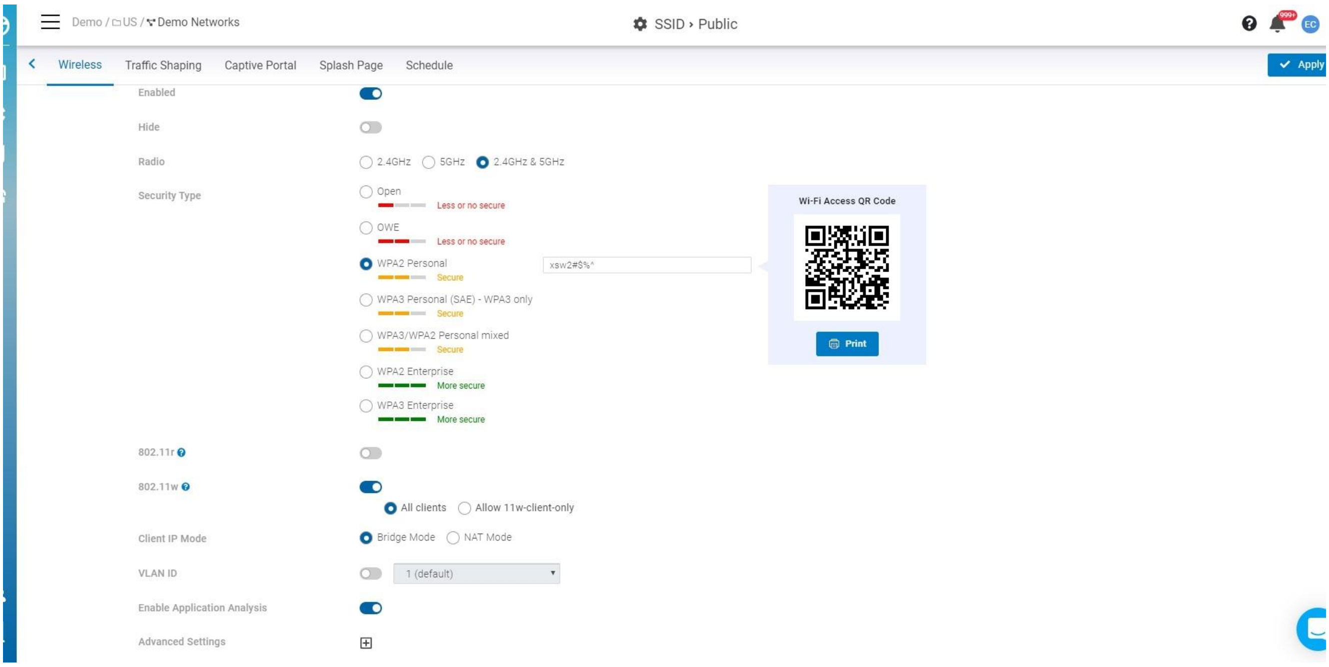
The following describes the authentication types on this screen:

- **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.



Enabled ●

Hide ○

Radio ○ 2.4GHz ○ 5GHz ● 2.4GHz & 5GHz

Security Type
○ Open — Less or no secure
○ OWE — Less or no secure
● WPA2 Personal — Secure — xsw2#$%^
○ WPA3 Personal (SAE) - WPA3 only — Secure
○ WPA3/WPA2 Personal mixed — Secure
○ WPA2 Enterprise — More secure
○ WPA3 Enterprise — More secure

802.11r ○

802.11w ● — ● All clients ○ Allow 11w-client-only

Client IP Mode ● Bridge Mode ○ NAT Mode

VLAN ID ○ 1 (default)

Enable Application Analysis ●

Advanced Settings ⊞

Client IP Addressing

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:

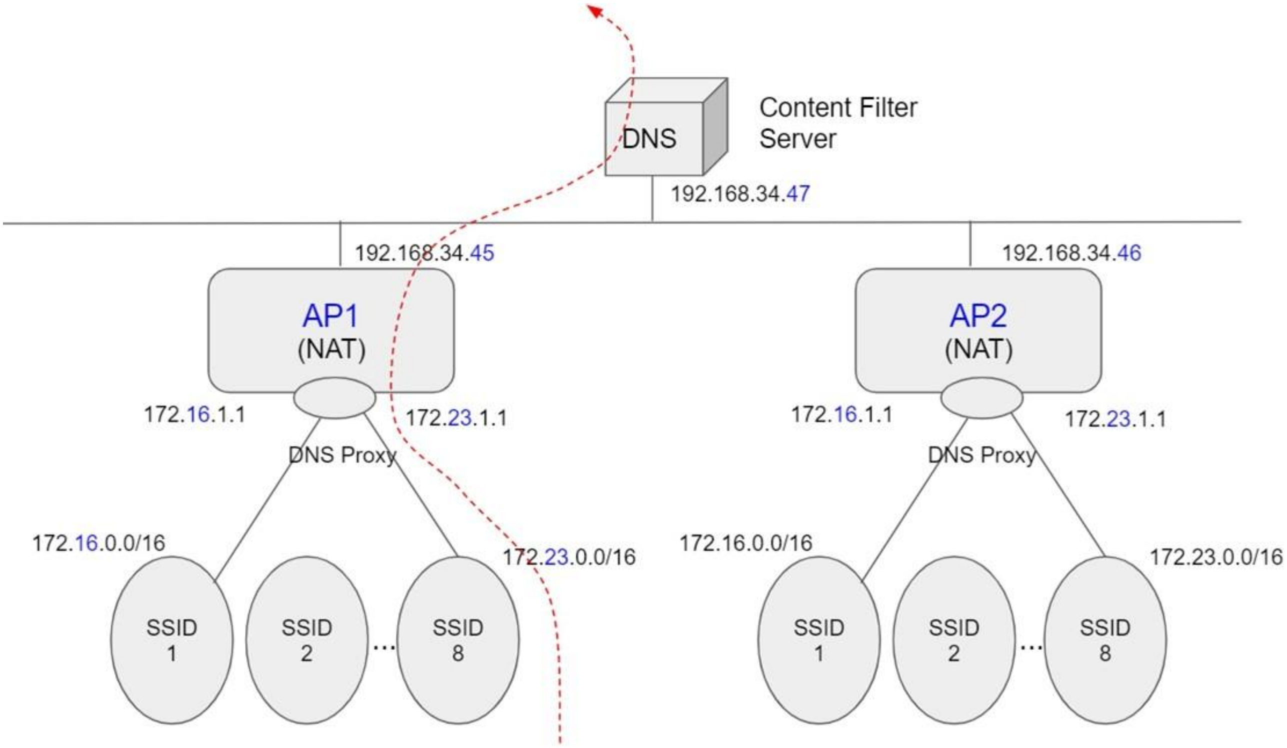
1. No NAT client can be talked to the other NAT client, neither same SSID nor different SSID (client isolation enabled and block internal routing)
2. Change the IP range of CP DNS to be same as AP DNS (172.16-23.0.0/16)

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.



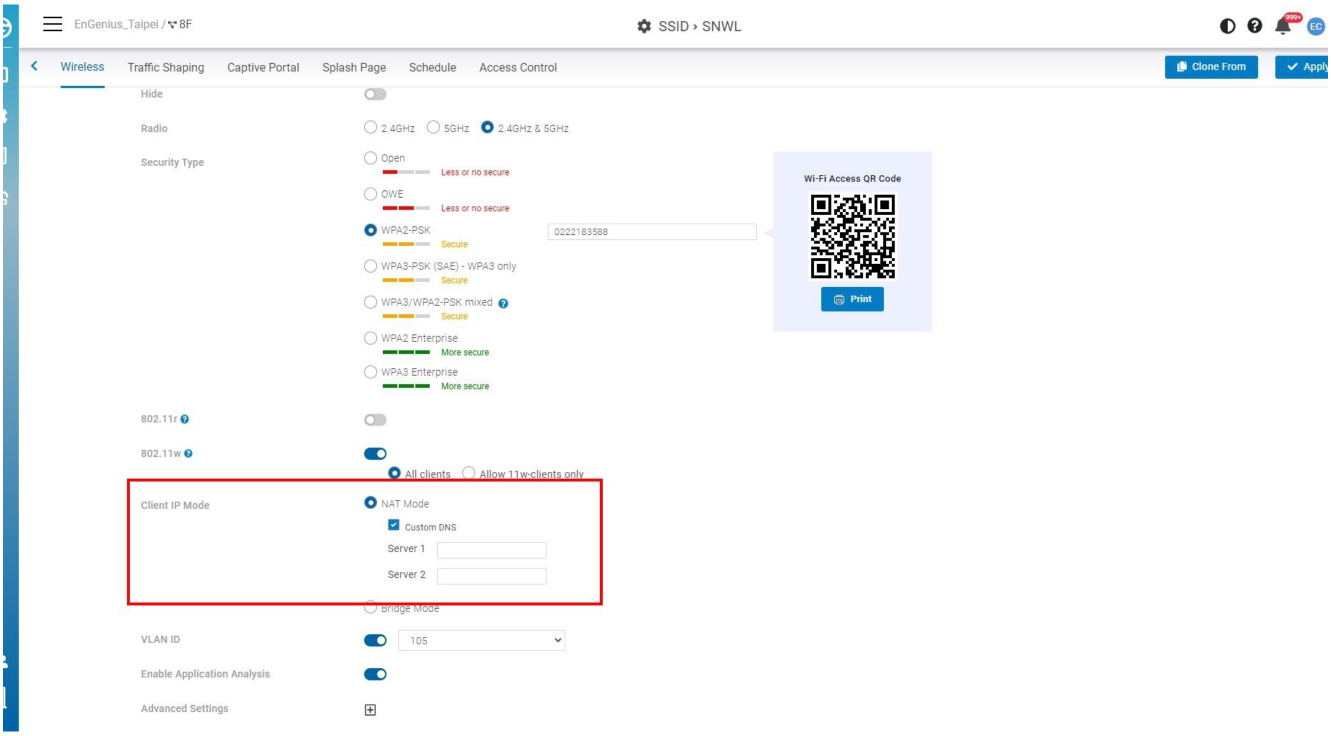
Configuring Custom DNS for an SSID in NAT Mode

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.

Dynamic VLAN Pooling

When Dynamic Client VLAN Pooling is enabled on your WLAN, the clients will be assigned IPs from any of the VLANs listed in the pool, which are randomly selected based on MAC hashing algorithm performed by the cloud/AP.

In a single Instant AP cluster, a large number of clients can be assigned to the same VLAN. Using the same VLAN for multiple clients can lead to a high level of broadcasts in the same subnet. To manage the broadcast traffic, you can partition the network into different subnets and use L3-mobility between those subnets when clients roam. However, if a large number of clients need to be in the same subnet, you can configure dynamic client VLAN pooling, in which each client is randomly assigned a VLAN from a pool of VLANs on the same SSID. Thus, VLAN pooling allows automatic partitioning of a single broadcast domain of clients into multiple VLANs.

> ⓘ Dynamic VLAN pooling usually works with BCMC Suppression to get better experience and reduce network complexity for large scale networks.

Advanced Settings

L2 isolation

L2 isolation is a feature to prevent wireless client from communicating with any other devices in the network except gateway. With this feature enabled, not only clients associating with the same SSID cannot communicate with each other (this is so called **client isolation** conventionally) but also clients cannot access other devices in the same LAN. Another exception is that wired devices added to VIP list are still accessible.

Example Use Cases

- Guest SSID to isolate clients and also stop them accessing corporation LAN resources
- Free WiFi service in which administrator want to keep the authentication simple, e.g., WPA2_PSK, such that customer can access the SSID via QR-code scanning.

> ⓘ L2 isolation works with all types of client IP addressing, i.e., NAT mode and Bridge mode.

Band Steering

Dual band operation with Band Steering detects clients capable of dual band operation and steers them to another frequency which leaves the more crowded band available for communication. This helps improve the end-user experience by reducing channel utilization, especially in high-density environments. **Band Steering** is configured on a per-SSID basis.

RSSI Threshold

This value defines the minimum RSSI required for dual-band wireless clients to associate to 5G band. If the client's RSSI drops below this threshold, it is only allowed to connect to 2.4G band. The recommended value is -60~-80.

BCMC Suppression

BCMC suppression is a feature to drop all the broadcast and multicast frames on a VLAN except for ARP, DHCP, IPv6 router advertisement, and IPv6 neighbor solicitation.

Broadcast-Multicast traffic from APs, remote APs, or distributions terminating on the same VLAN floods all VLAN member ports. This causes critical bandwidth wastage, especially when the APs are connected to an L3 cloud where the available bandwidth is limited or expensive. Suppressing the VLAN broadcast-multicast traffic to prevent flooding can result in loss of client connectivity.

To effectively prevent flooding of broadcast-multicast traffic on all VLAN member ports, use BCMC Suppression to ensure controlled flooding of broadcast-multicast traffic without compromising the client connectivity. This option is disabled by default. You must enable this option for the controlled flooding of broadcast-multicast traffic.

Example Use Cases

- Enterprise network with over 1000 active wired or wireless clients in different VLANs.
- Campus network with over 1000 active wired or wireless clients in different VLANs.

> ⓘ BCMC Suppression usually works with dynamic VLAN pooling to reduce the management complexity for large scale networks.

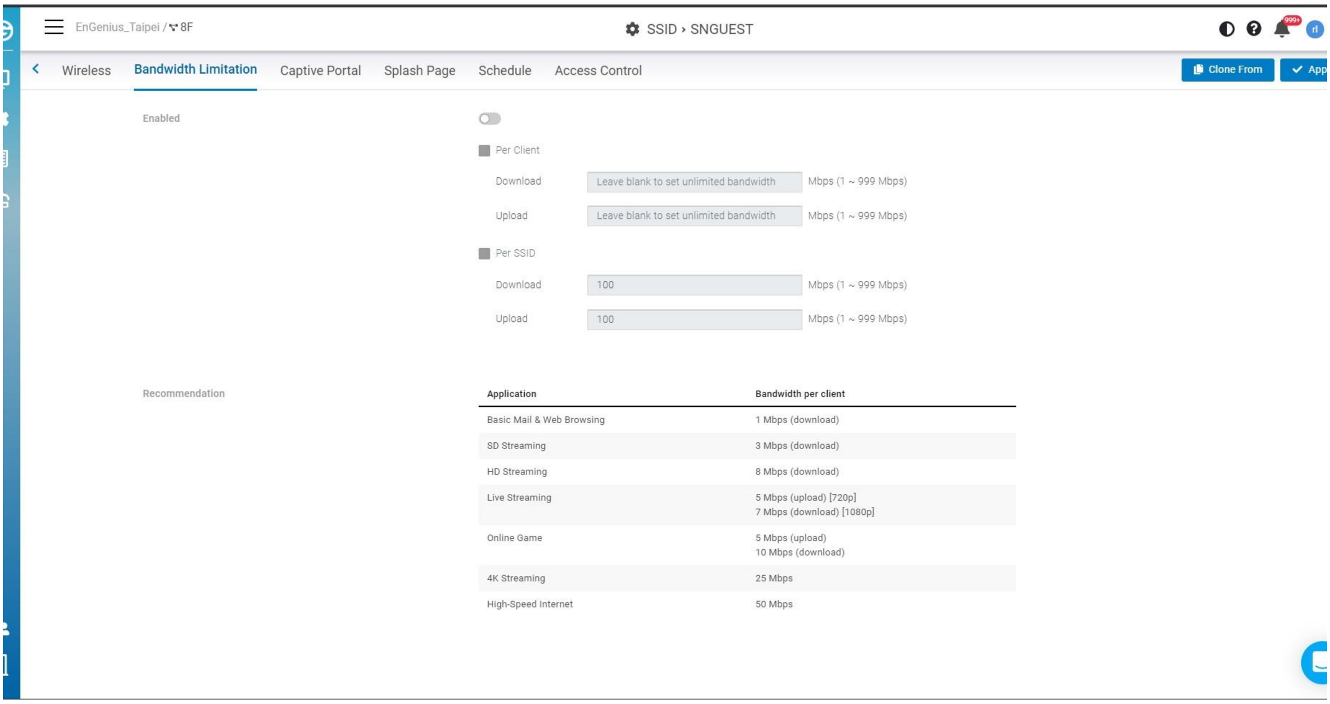
QoS

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 .

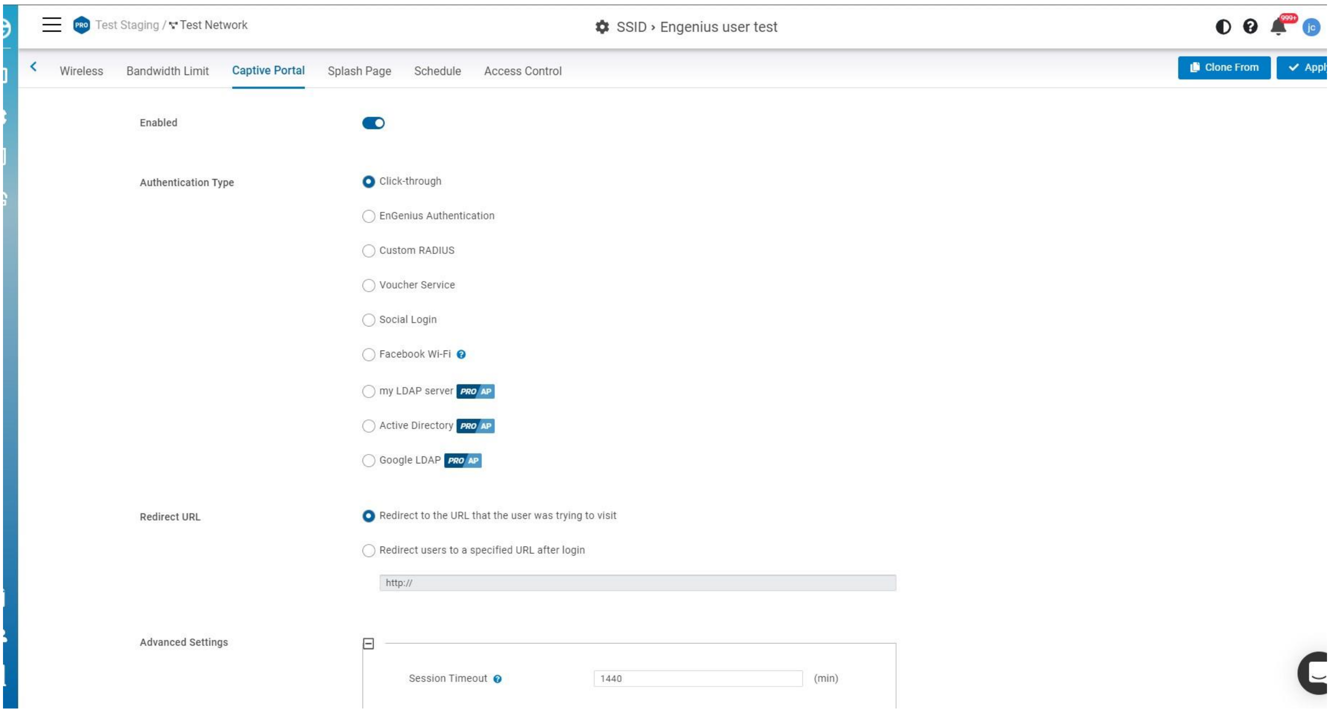
Upload Limit

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
○ Facebook Wi-Fi
○ my LDAP server
○ Active Directory
○ Google LDAP

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

Advanced Settings
Session Timeout 1440 (min)

Authentication Type

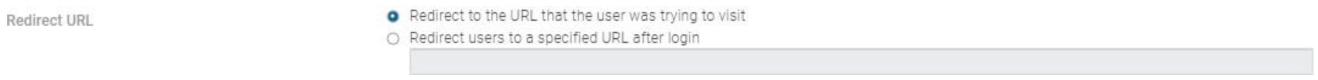
- **Click-through**: Users must view and acknowledge your splash page before being allowed on the network.
- **EnGenius Authentication**: Users must enter a username and password before being allowed on the network. You could edit user settings through **Configure** > **Cloud RADIUS User**.
- **Custom 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.



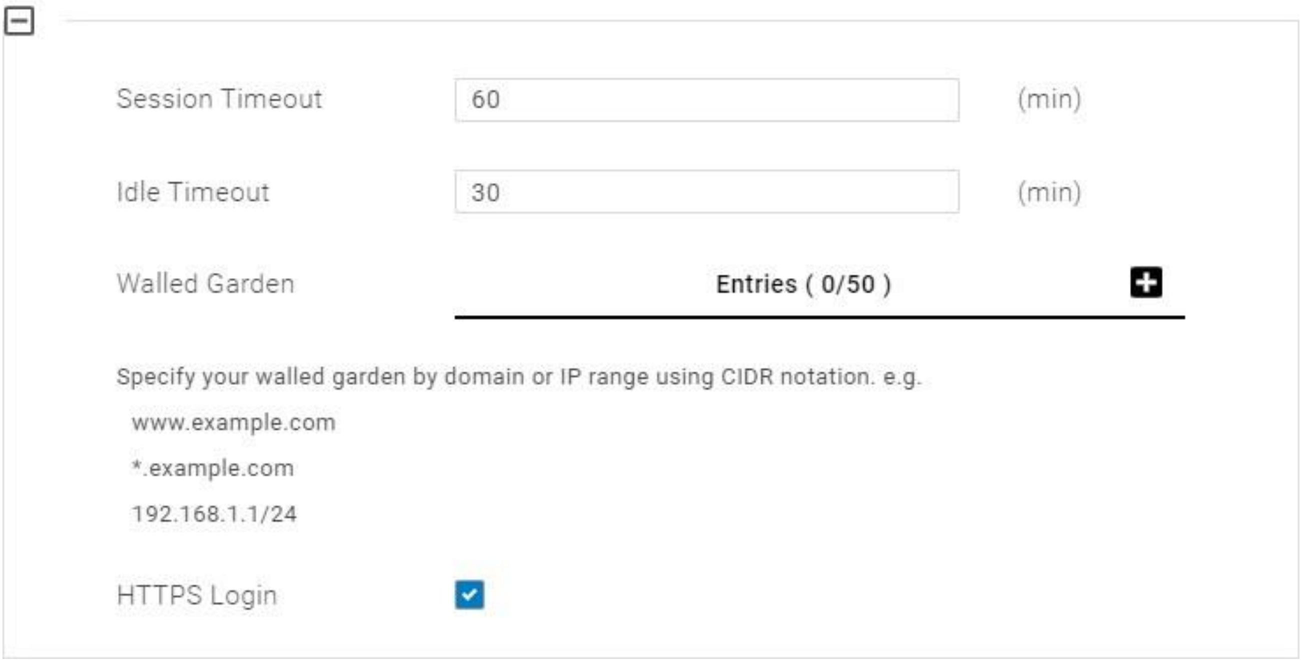
Redirect URL

● 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.

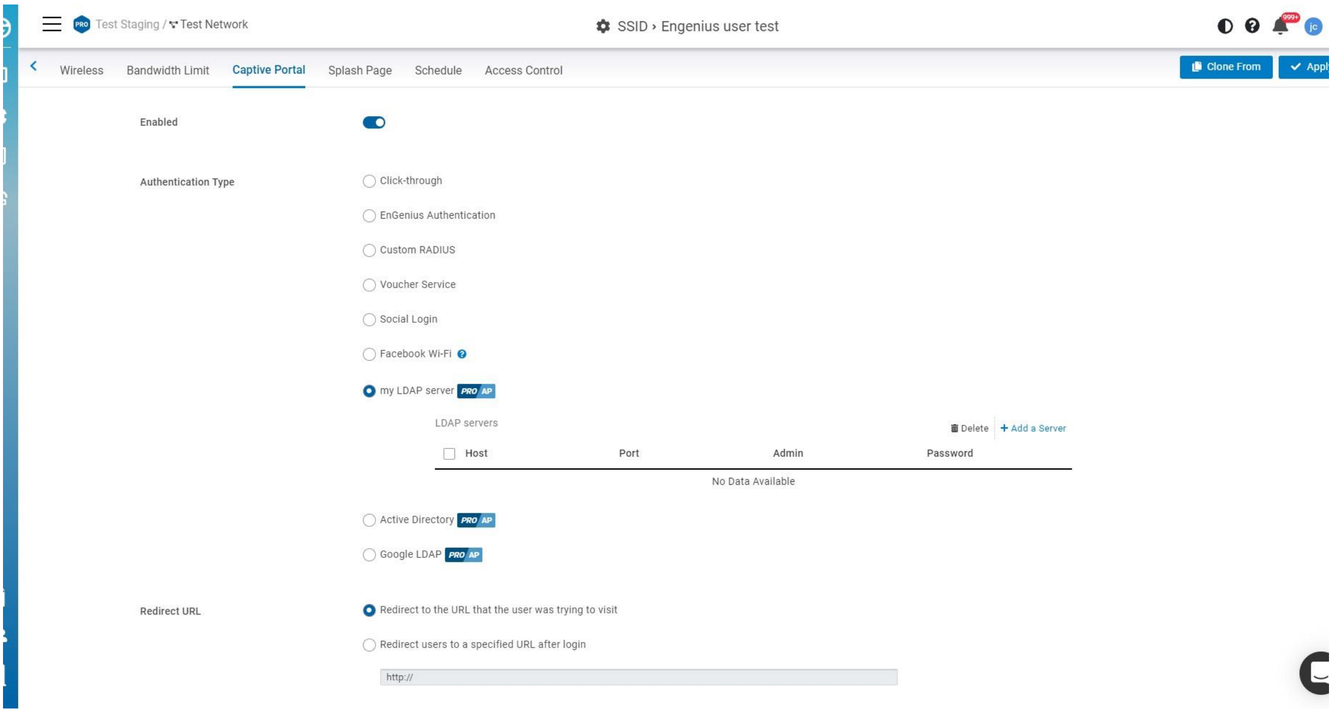
Idle Timeout: Specify a time limit for an idle client after which users will be disconnected and required to log in again.

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.

LDAP server

Captive Portal supports the way to authenticate with an externally hosted LDAP server. The option is available at **Configure > SSID > Captive Portal > my LDAP server**



Enabled

Authentication Type
○ Click-through
○ EnGenius Authentication
○ Custom RADIUS
○ Voucher Service
○ Social Login
○ Facebook Wi-Fi
● my LDAP server

LDAP servers

□ Host	Port	Admin	Password

No Data Available

○ Active Directory
○ Google LDAP

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

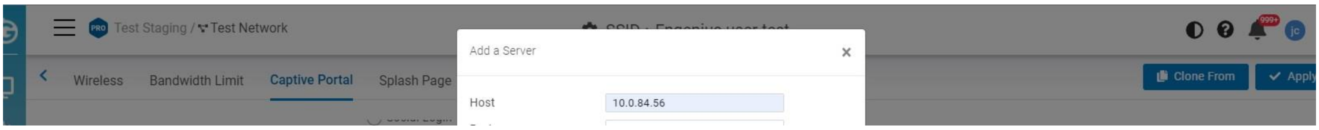
http://

Follow the steps below to configure the LDAP service:

1. Click **Add a server** to add a new LDAP server.

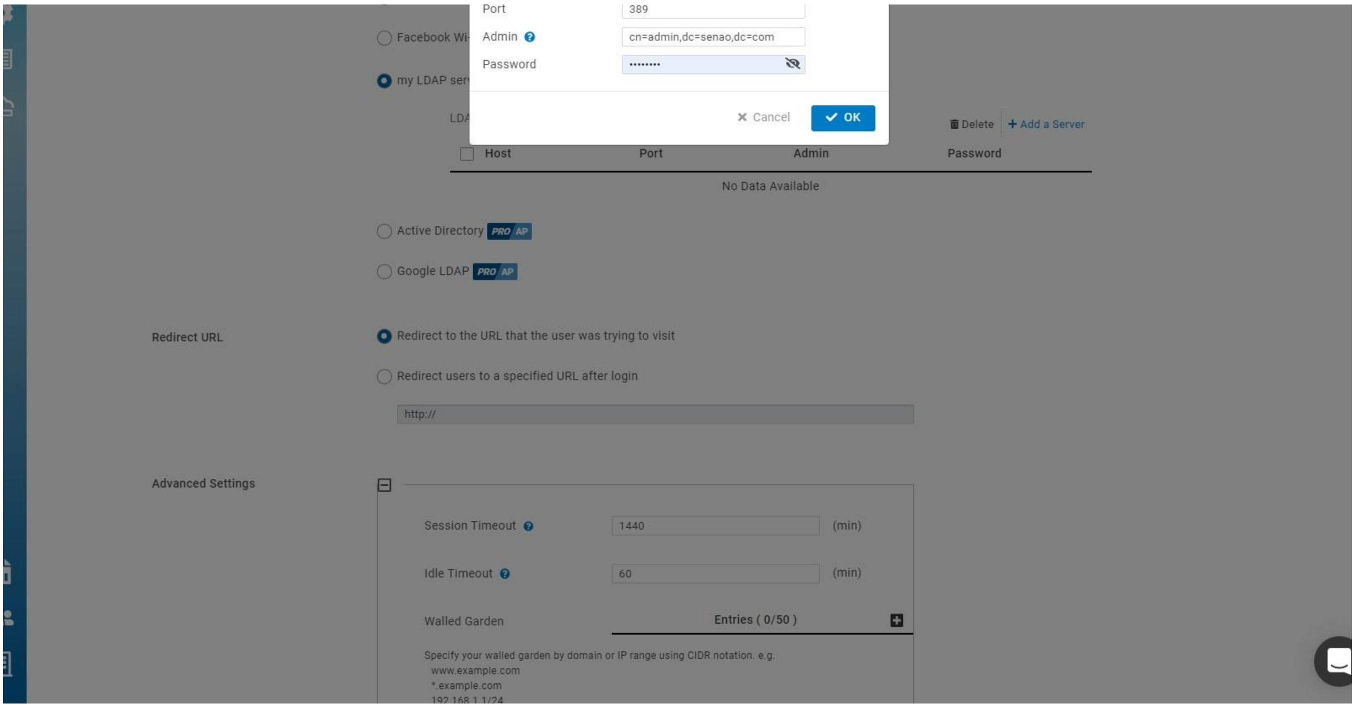
2. Enter the IP address or domain name of your LDAP server in the **Host** field and the LDAP listening port in the **Port** field.

3. For LDAP admin, enter the distinguished name of the administrative account to bind your LDAP server, for example, **cn=admin,dc=example,dc=com**, and the password.



Add a Server

Host 10.0.84.56



Port 389

Admin cn=admin,dc=senao,dc=com

Password ••••••••

✕ Cancel | ✓ OK

○ Facebook Wi-

● my LDAP ser

LDA

🗑 Delete | + Add a Server

□ Host	Port	Admin	Password

No Data Available

○ Active Directory PRO AP

○ Google LDAP PRO AP

Redirect URL

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

○ Redirect users to a specified URL after login

http://

Advanced Settings

Session Timeout 1440 (min)

Idle Timeout 60 (min)

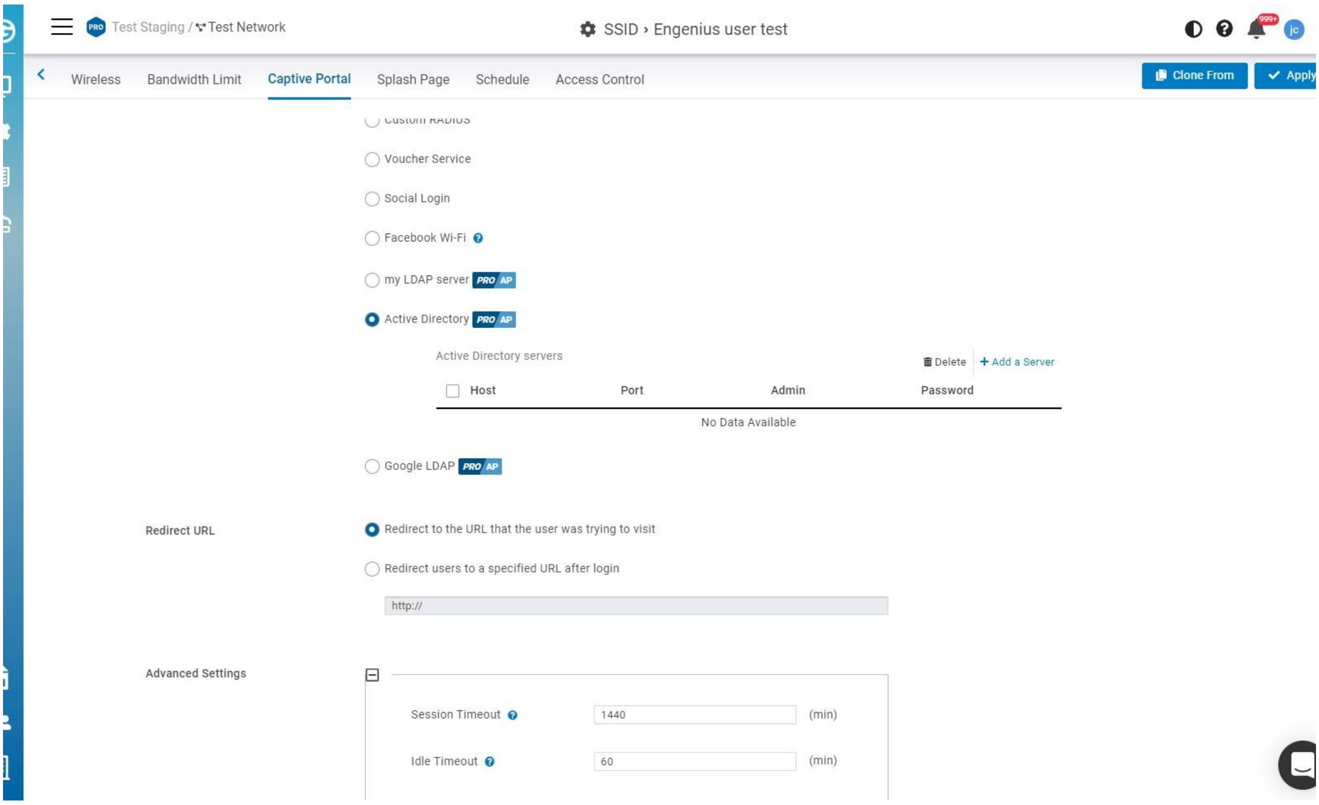
Walled Garden — Entries (0/50)

Specify your walled garden by domain or IP range using CIDR notation. e.g.
www.example.com
*.example.com
192.168.1.1/24

4. Click **OK** and then click **Apply** button.

Active Directory

Captive Portal supports the way to authenticate via an externally hosted AD server. The option is available at **Configure > SSID > Captive Portal > Active Directory.**



○ Custom RADIUS

○ Voucher Service

○ Social Login

○ Facebook Wi-Fi

○ my LDAP server PRO AP

● Active Directory PRO AP

Active Directory servers

🗑 Delete | + Add a Server

□ Host	Port	Admin	Password

No Data Available

○ Google LDAP PRO AP

Redirect URL

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

○ Redirect users to a specified URL after login

http://

Advanced Settings

Session Timeout 1440 (min)

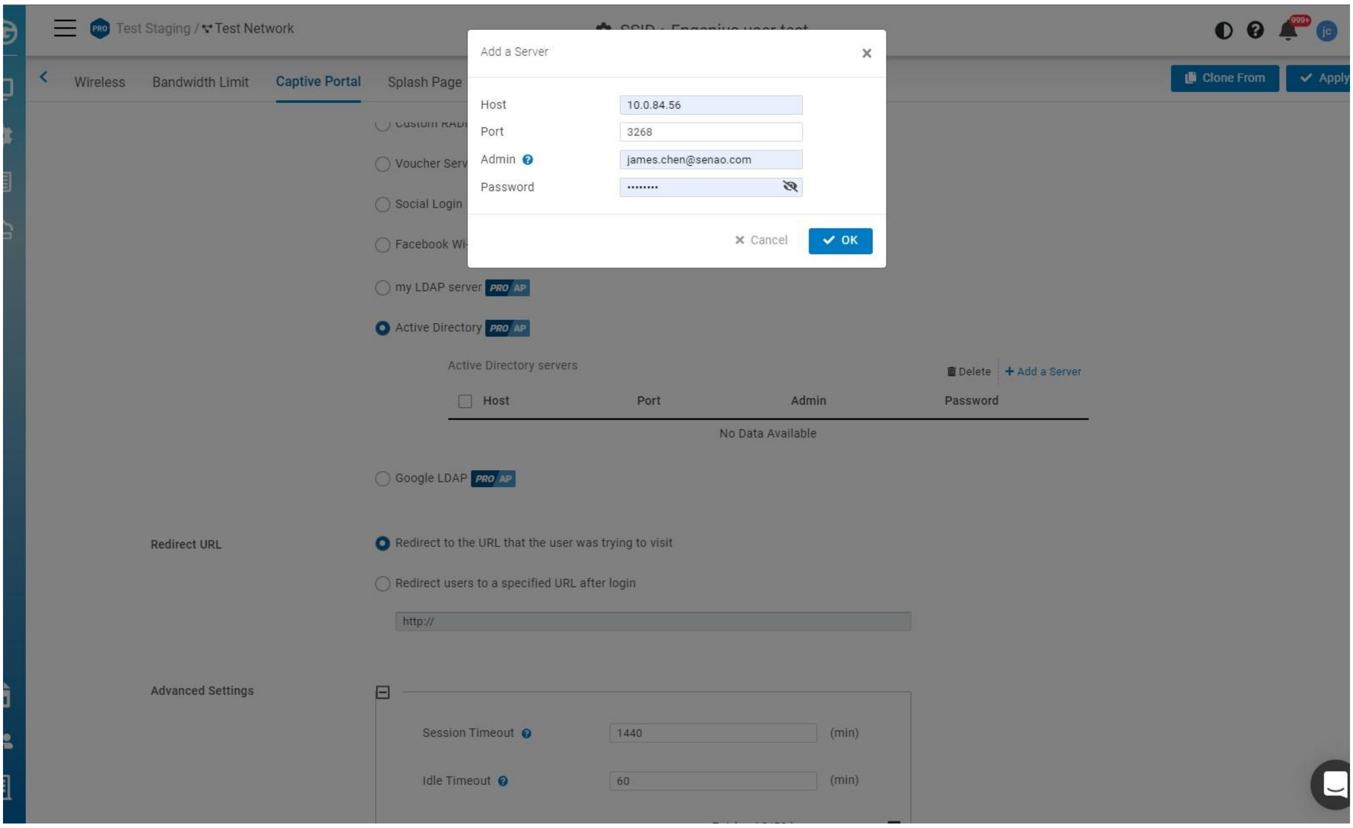
Idle Timeout 60 (min)

Follow the steps below to configure your AD service.

1. Click **Add a server** to add a new AD server in the list.

2. Enter the IP address or domain name of your AD server in the **Host** field and the AD server listening port in the **Port** field.

3. For AD admin, enter the AD format: **admin@example.com**, and the password.



Add a Server

Host: 10.0.84.56

Port: 3268

Admin: james.chen@senao.com

Password: ••••••••

✕ Cancel | ✓ OK

○ Voucher Serv

○ Social Login

○ Facebook Wi-

○ my LDAP server PRO AP

● Active Directory PRO AP

Active Directory servers

□ Host	Port	Admin	Password
No Data Available			

○ Google LDAP PRO AP

Redirect URL

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

○ Redirect users to a specified URL after login

http://

Advanced Settings

Session Timeout: 1440 (min)

Idle Timeout: 60 (min)

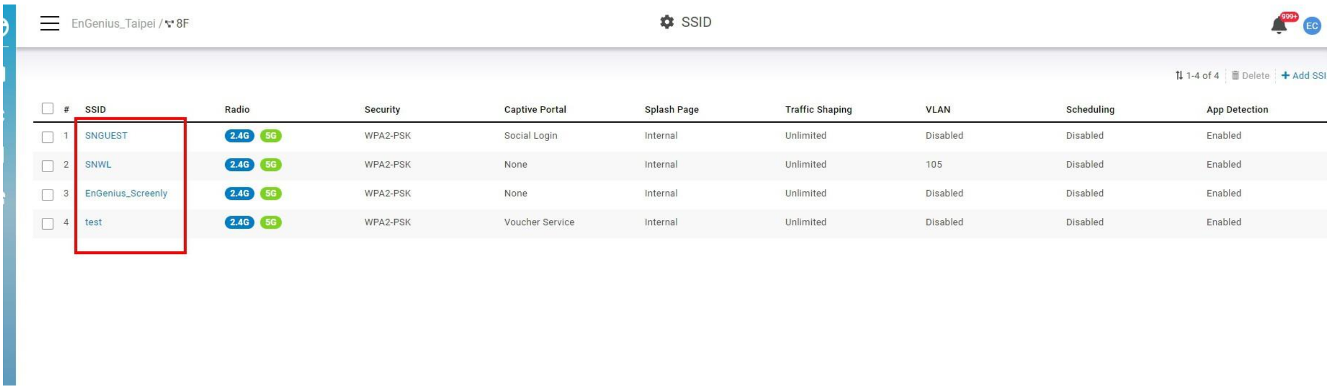
4. Click **OK** and then click **Apply** button.

Social Login

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

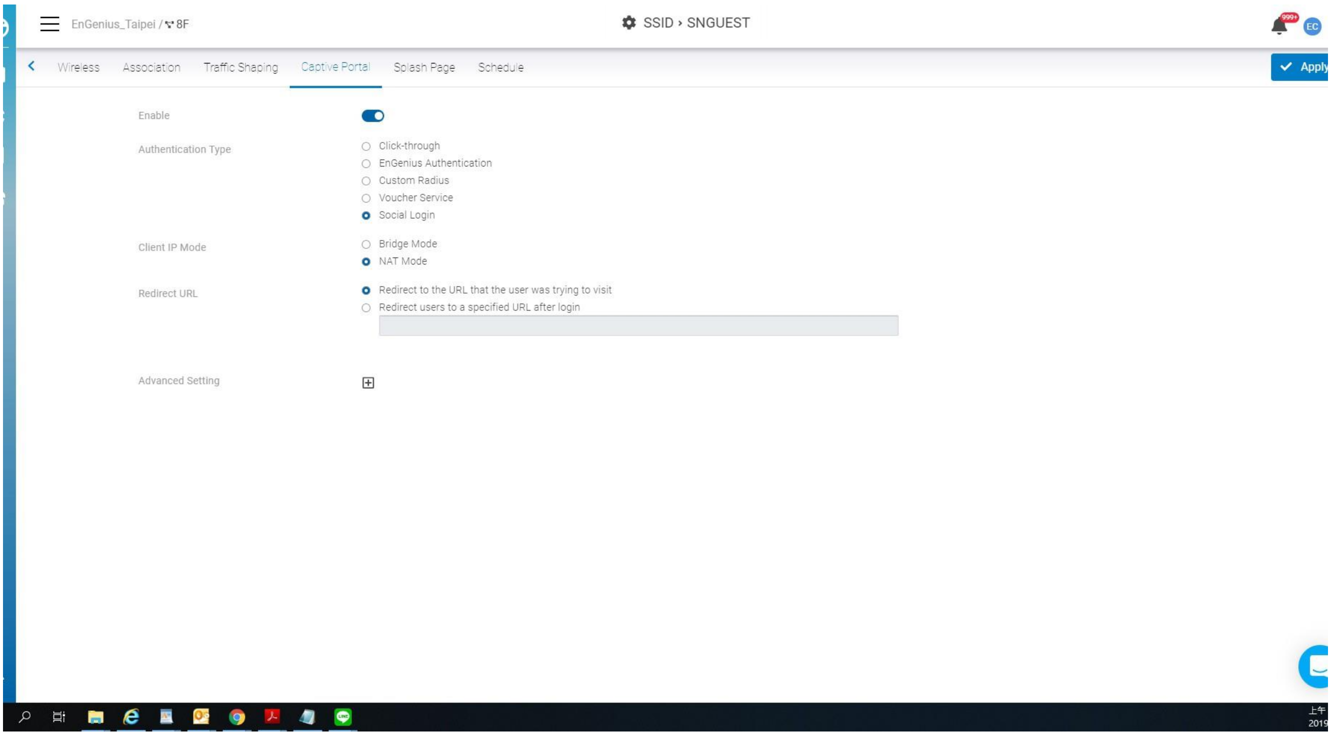
Follow the below steps to configure social login.

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	105	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.**

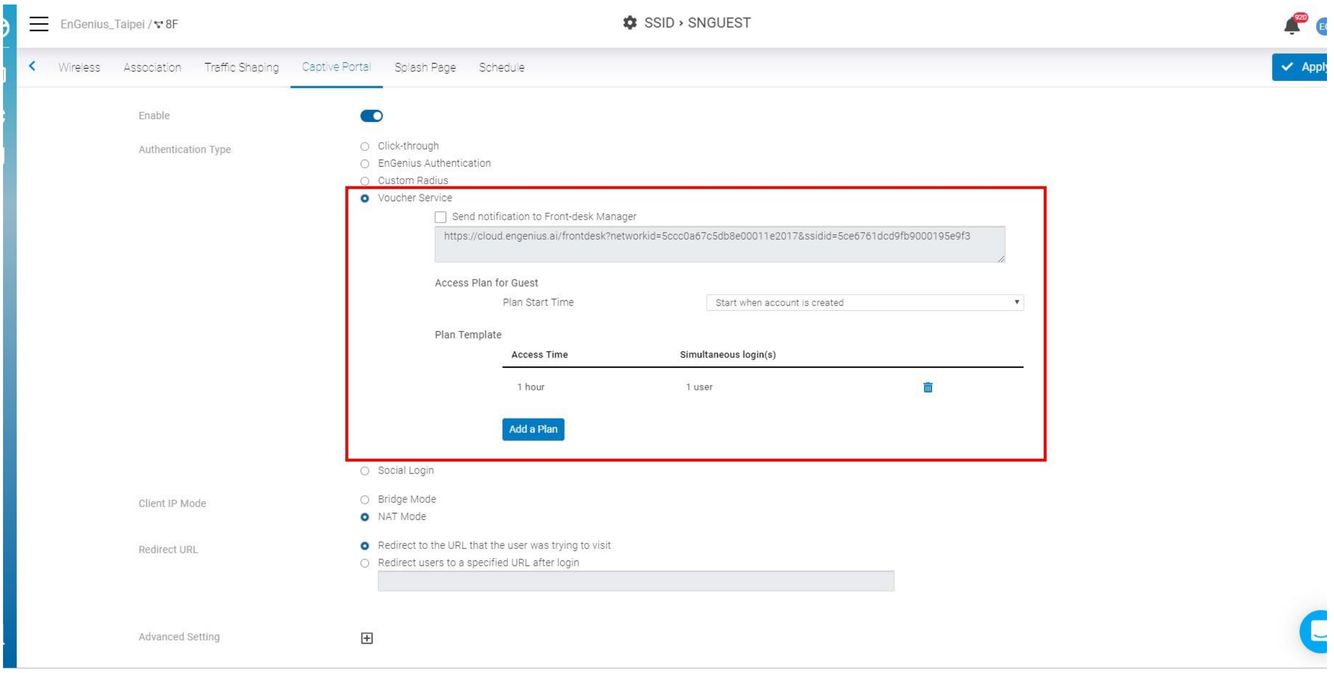
Voucher Service

This guide is intended to help you set up your network to generate and accept vouchers. With vouchers, you

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=5ccc0a67c5db8e00011e2017&ssidid=5ce6761dcd9fb9000195e9f3

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.

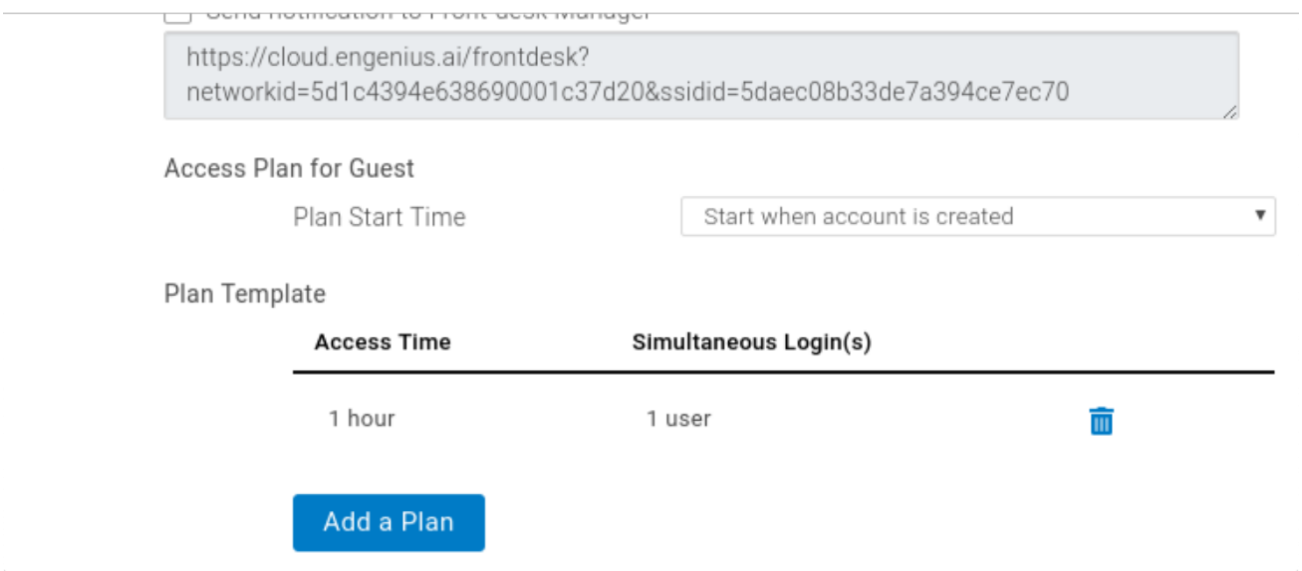
Management URL and Access Plan

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



□ Send notification to Front desk Manager

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

Access Plan for Guest

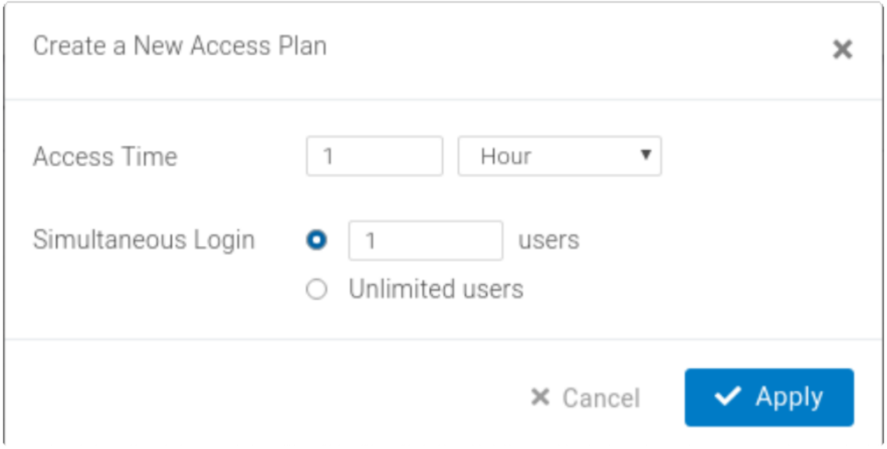
Plan Start Time: Start when account is created

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

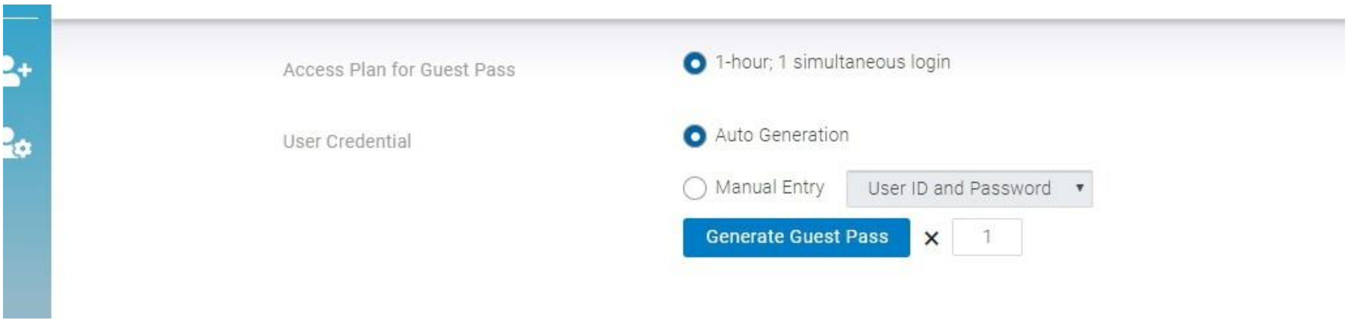
Plan Start Time

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 ▾

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.

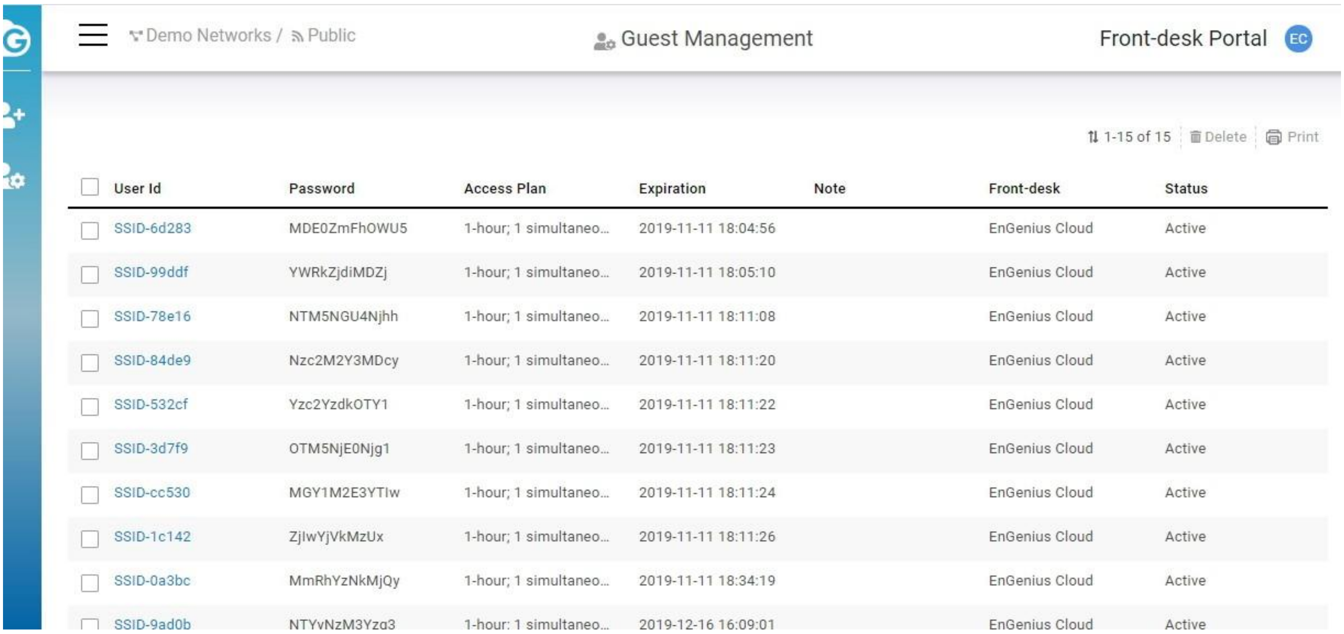
Managing Voucher User

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

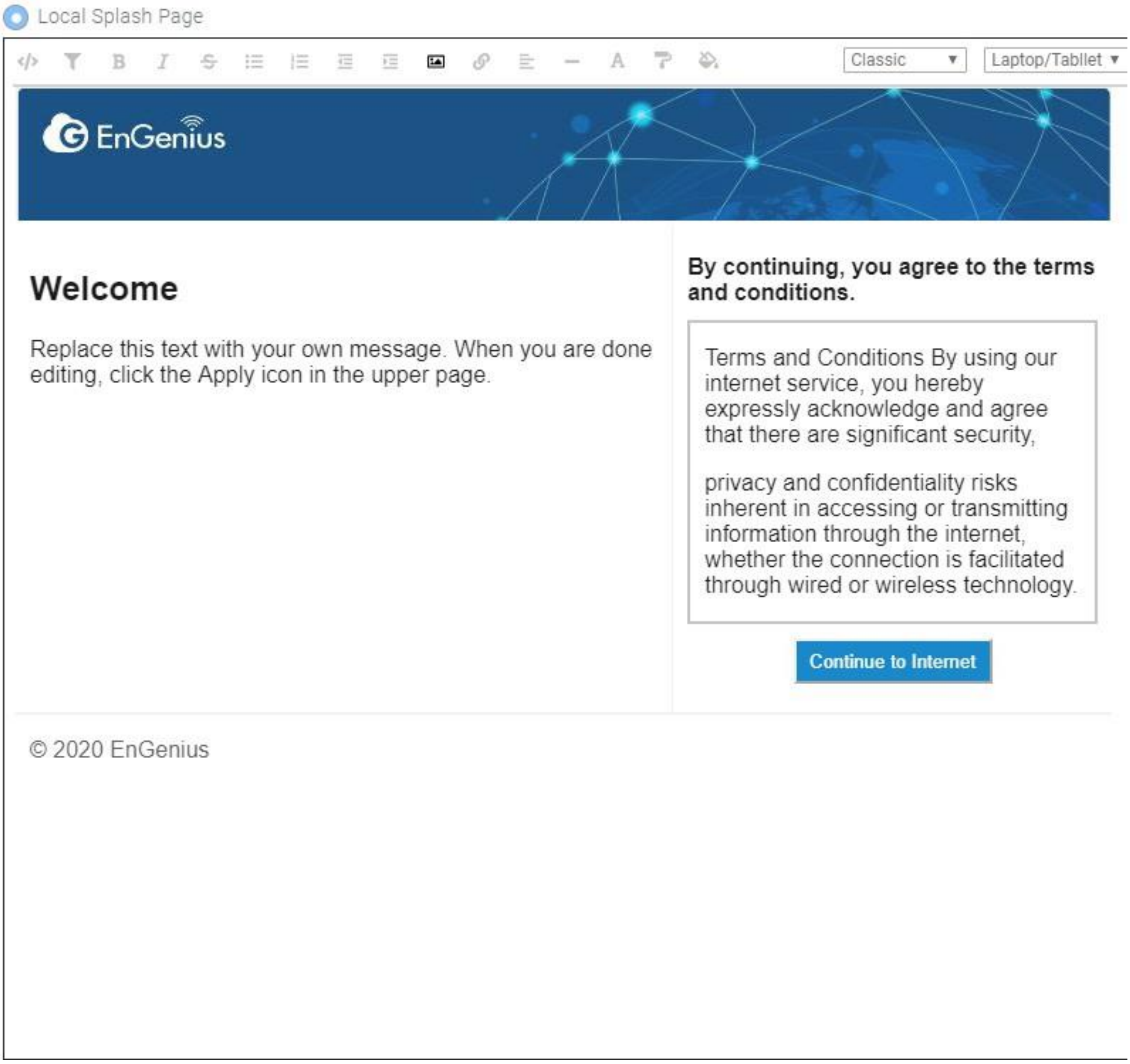
Configuring Splash Page

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

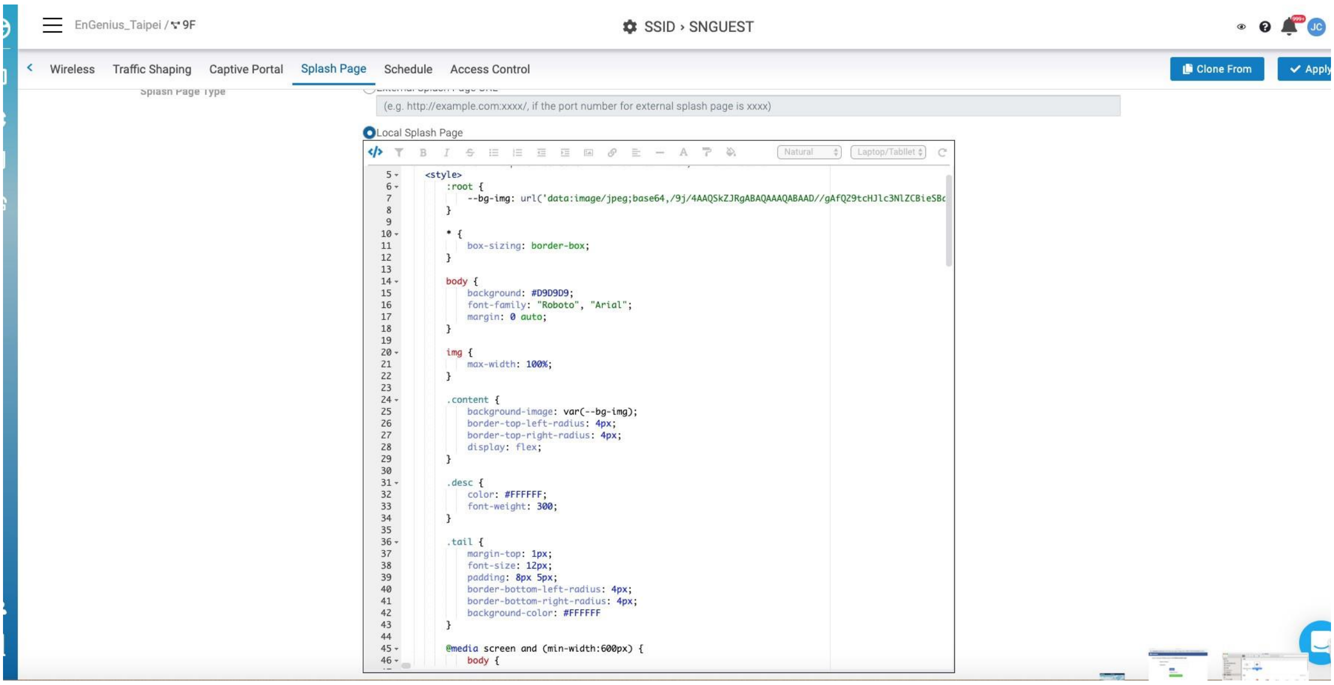
You can choose different template from the drop-down menu at the top of the editor.

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 .

</>



(e.g. http://example.com:xxxx/, if the port number for external splash page is xxxx)

● Local Splash Page

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

      * {
          box-sizing: border-box;
      }

      body {
          background: #D9D9D9;
          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 {
```

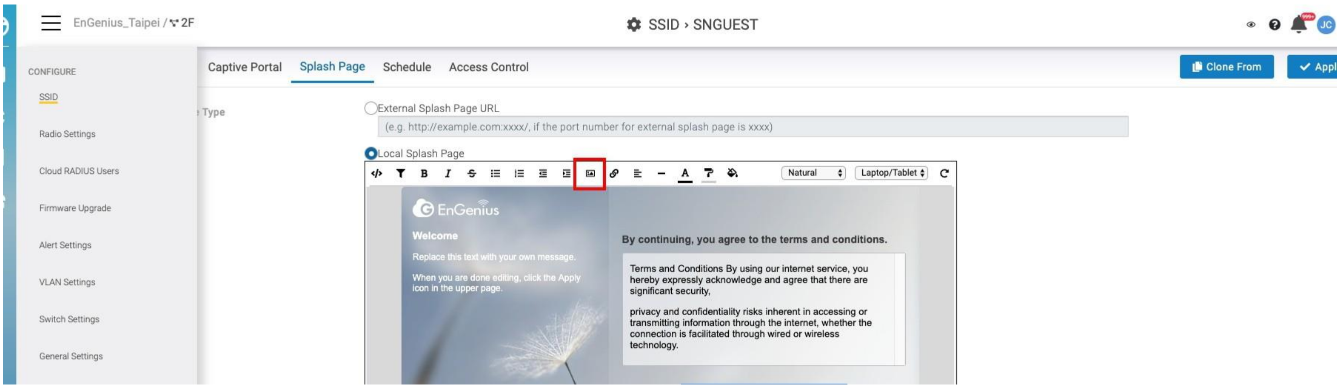
Choosing a starting template

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**.



○ External Splash Page URL

(e.g. http://example.com:xxxx/, if the port number for external splash page is xxxx)

● Local Splash Page

Welcome

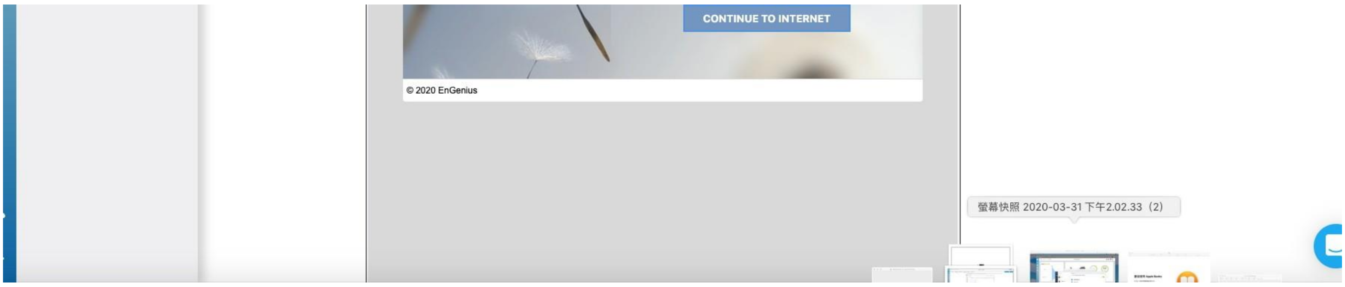
Replace this text with your own message.

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,

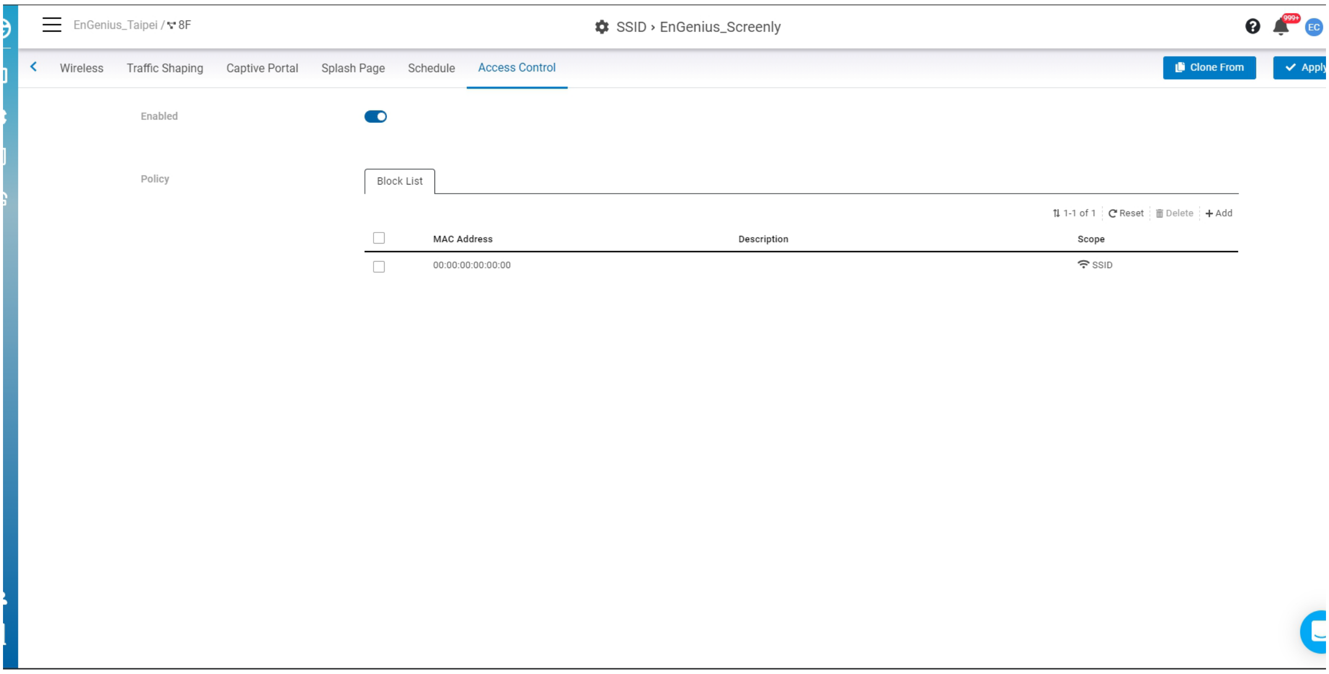
privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology.



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.



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

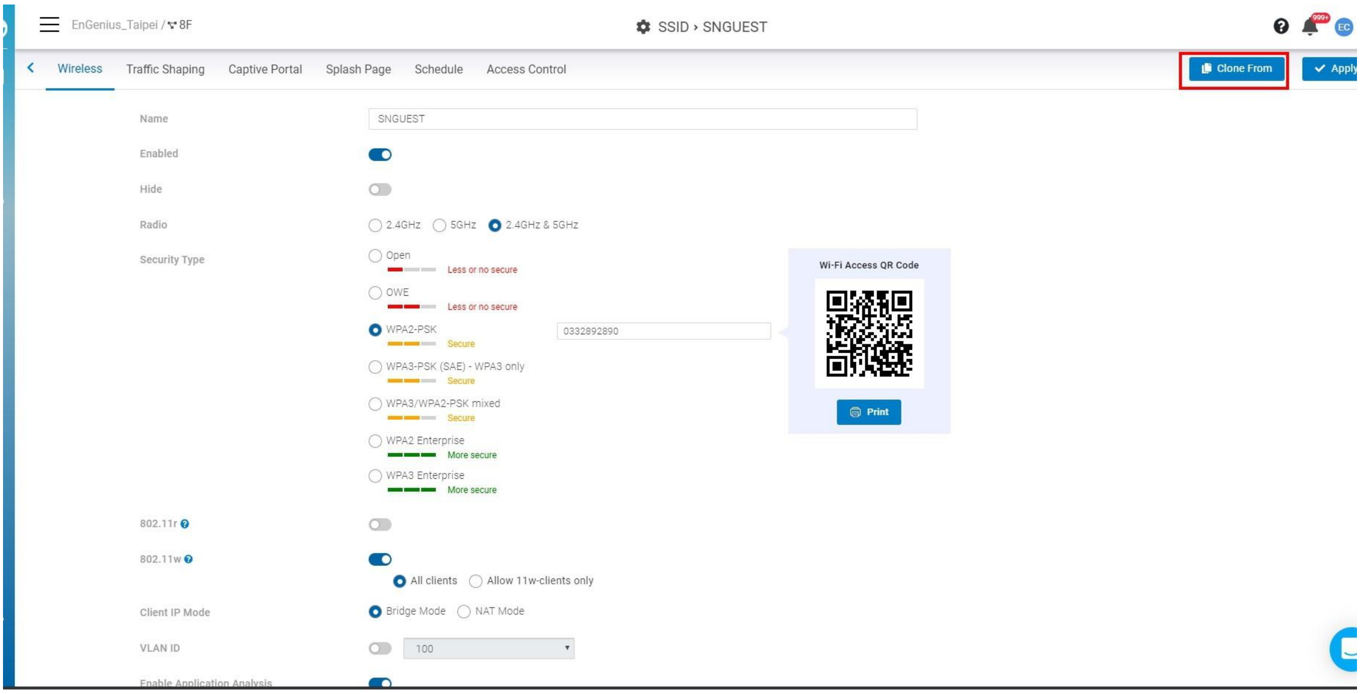
The following describes the functions on this screen:

- **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.



Name: SNGUEST

Enabled: on

Hide: off

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 — Secure
- ○ WPA3/WPA2-PSK mixed — Secure
- ○ WPA2 Enterprise — More secure
- ○ WPA3 Enterprise — More secure

802.11r: off

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

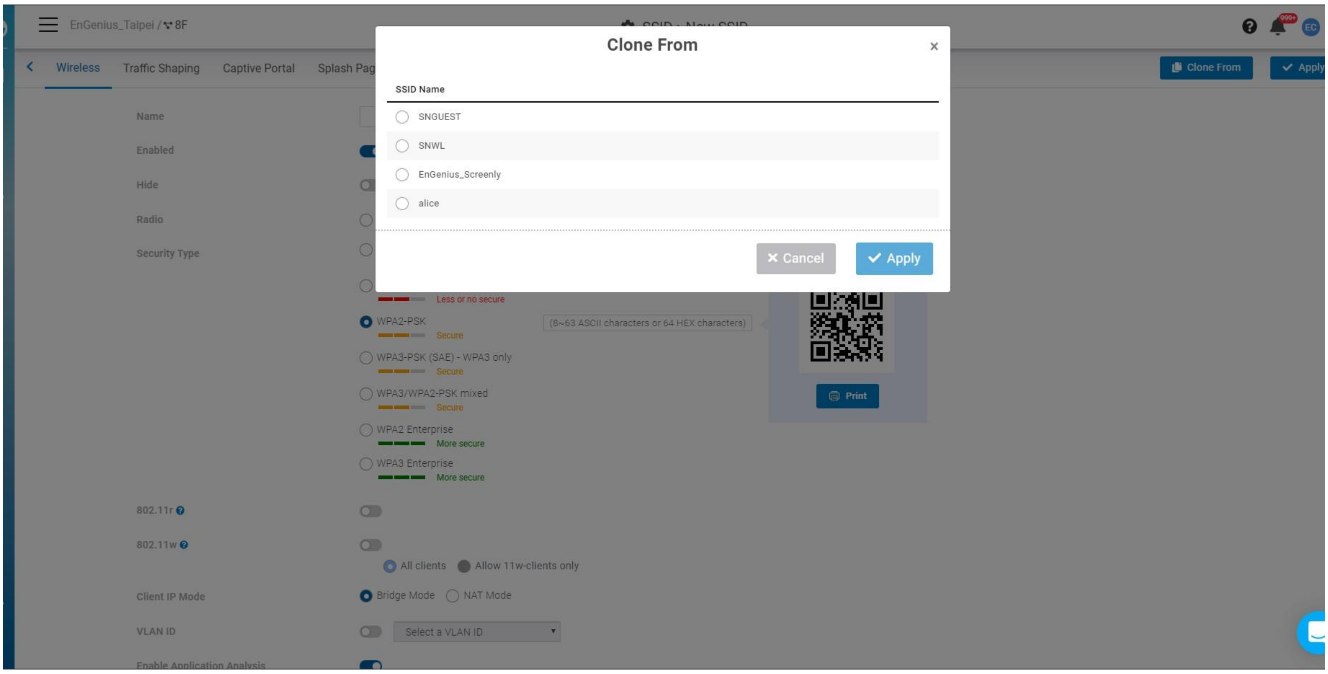
Client IP Mode: ● Bridge Mode ○ NAT Mode

VLAN ID: off — 100

Enable Application Analysis: on

Follow steps to clone SSID

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



Clone From

SSID Name
○ SNGUEST
○ SNWL
○ EnGenius_Screenly
○ alice

✕ Cancel ✓ Apply

WPA2-PSK (8~63 ASCII characters or 64 HEX characters)

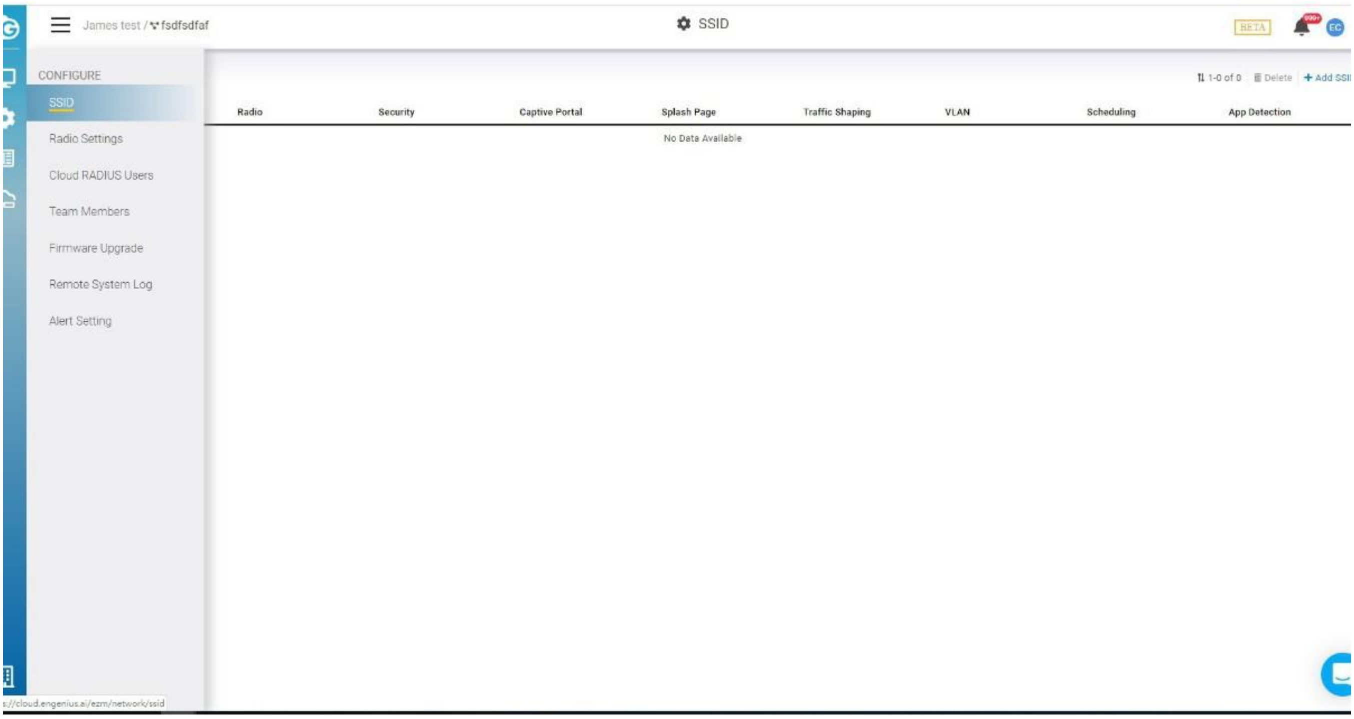
VLAN ID: Select a VLAN ID

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

Examples

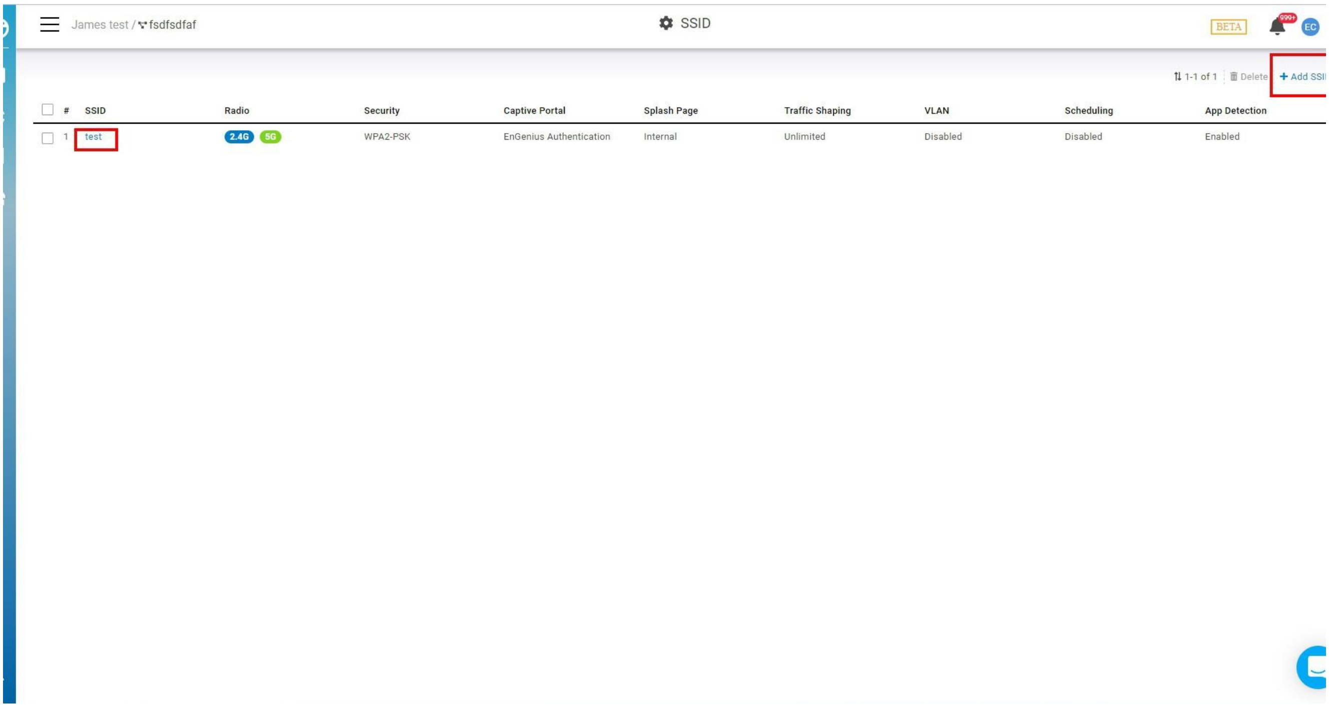
How to Configure Captive Portal

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).



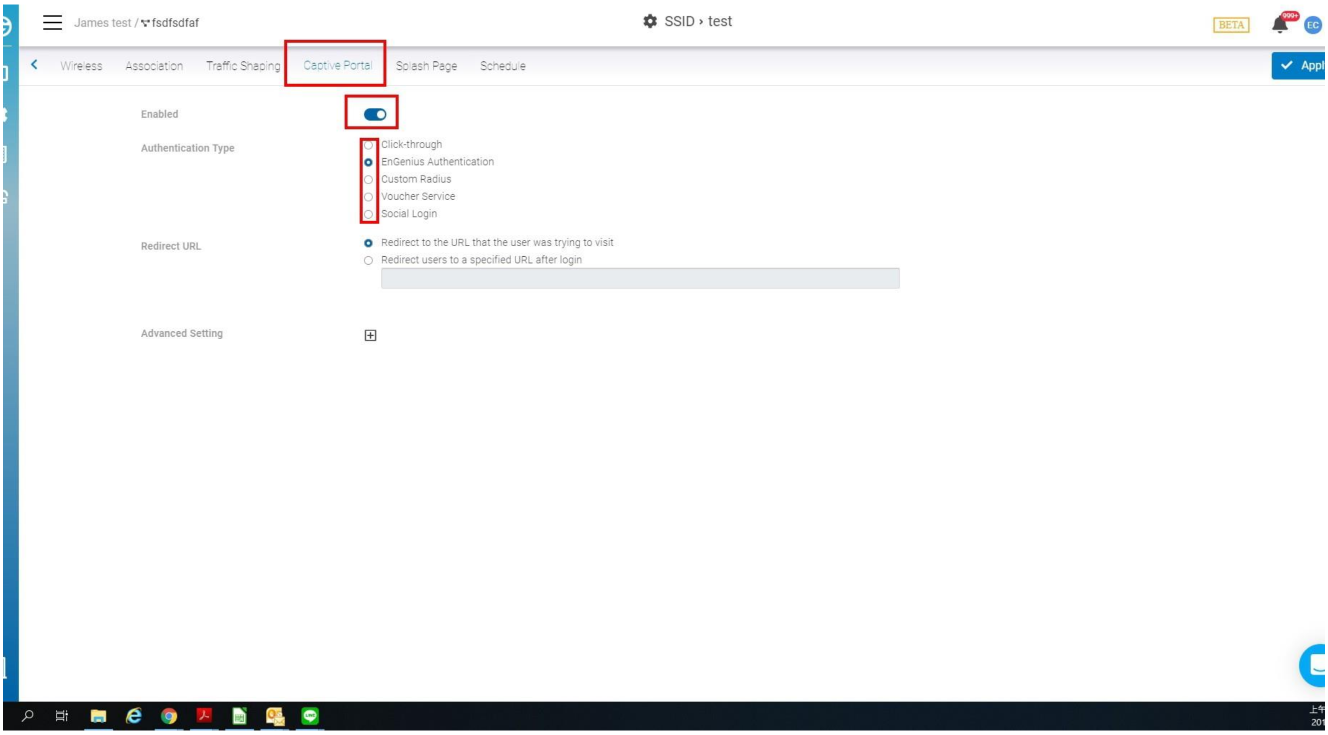
Radio	Security	Captive Portal	Splash Page	Traffic Shaping	VLAN	Scheduling	App Detection
			No Data Available				

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



☐	#	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.



Enabled ●

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

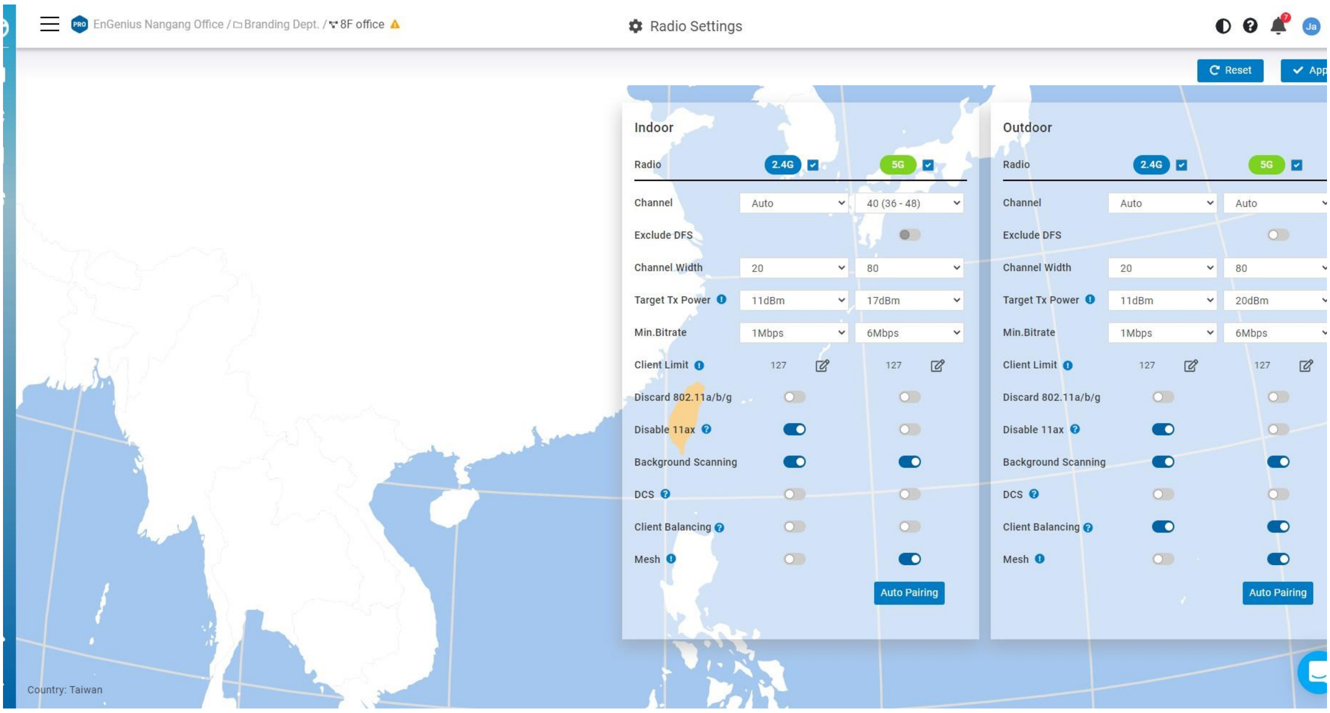
Redirect URL
● Redirect to the URL that the user was trying to visit
○ Redirect users to a specified URL after login

Advanced Setting ⊞

4. Click **Apply.**

Configuring Radio

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



Indoor			Outdoor		
Radio	2.4G ☑	5G ☑	Radio	2.4G ☑	5G ☑
Channel	Auto	40 (36 - 48)	Channel	Auto	Auto
Exclude DFS		○	Exclude DFS		○
Channel Width	20	80	Channel Width	20	80
Target Tx Power	11dBm	17dBm	Target Tx Power	11dBm	20dBm
Min.Bitrate	1Mbps	6Mbps	Min.Bitrate	1Mbps	6Mbps
Client Limit	127	127	Client Limit	127	127
Discard 802.11a/b/g	○	○	Discard 802.11a/b/g	○	○
Disable 11ax	●	○	Disable 11ax	●	○
Background Scanning	●	●	Background Scanning	●	●
DCS	○	○	DCS	○	○
Client Balancing	○	○	Client Balancing	●	●
Mesh	○	●	Mesh	○	●

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.

Exclude DFS

Some use cases may require that Dynamic Frequency Selection (DFS) channels be excluded from the Auto Channel algorithm. DFS channels can be allowed or excluded on the radio settings page.

Since DFS channels can only be used until radar communication is heard, disabling DFS may be useful if the wireless network is in close proximity to a harbor, airport, or weather radar station. Administrators may also want to disable DFS if most local wireless clients do not support DFS channels.

> ⓘ Please notice that Exclude DFS only affected when Channel is Auto on 5G.

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 5 GHz.

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.

The 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 the 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 clients' 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 the impact of performance on other 802.11ac/ax clients.

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

DCS (Dynamic Channel Selection)

Dynamic Channel Selection allows a Wireless Access Point to monitor traffic and noise levels on the channel which is current operating and also keeps watching utilization of other channels with background scanning.

When DCS is enabled and traffic or noise levels of current channel exceed predefined threshold (50%) for a period (15 mins), the AP ceases operating on the current channel and hops to an alternative channel with best utilization in statistics.

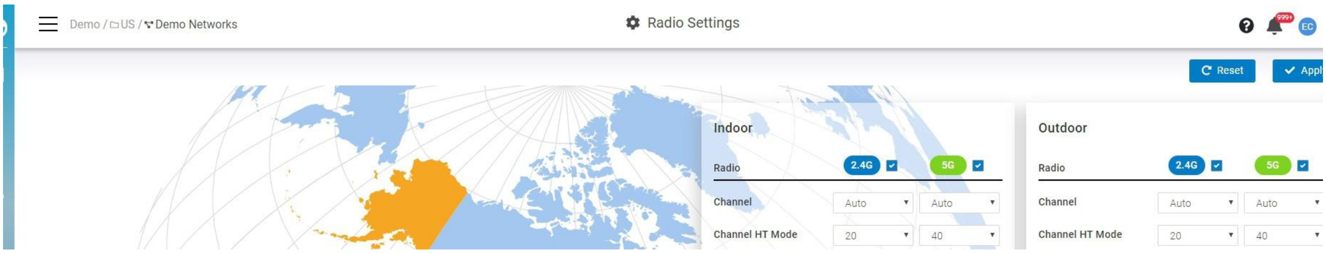
When to use it

DCS is useful for the complex and dynamic wireless environment where numerous APs and travel routers broadcast and transmit packets in the same area. It usually comes with high radio interference and situation changes from time to time. In this case, DCS could be helpful to react for unexpected interference with a short-term mechanism and jump to a cleaner channel to operate.

- When DCS is enabled, the client will be disconnected if the system decides to hop to a new channel. That may affect some real-time applications.
- DCS only takes effect when the channel of Radio is set in "auto".
- This feature requires AP firmware version to be V1.X.35 or above.

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

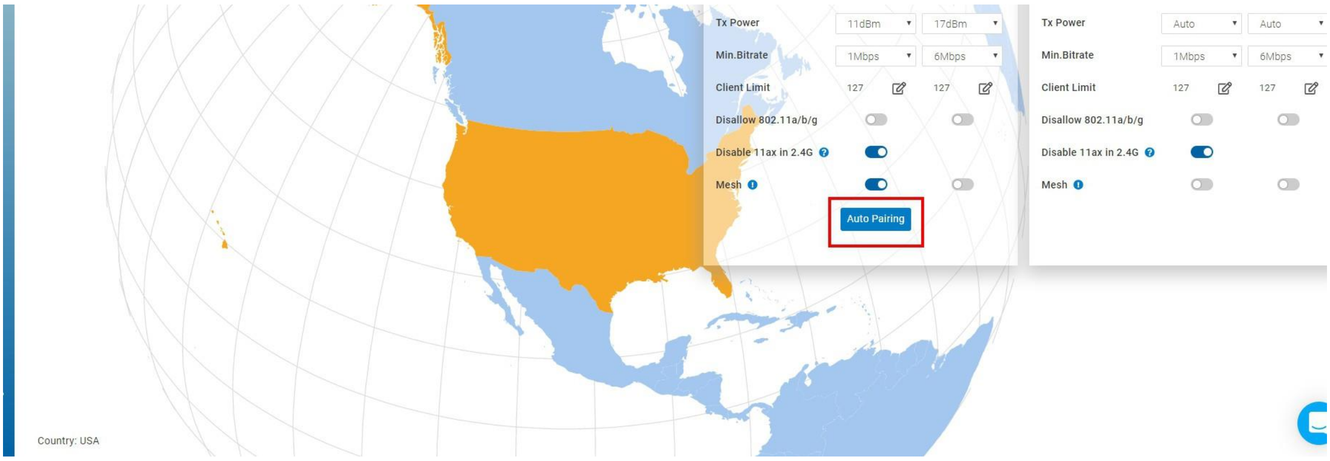
Channel HT Mode 20 40

Outdoor

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

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 is already registered to your Org and be assigned to a Network nearby the cloud-connected AP. (less than 10 meters 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

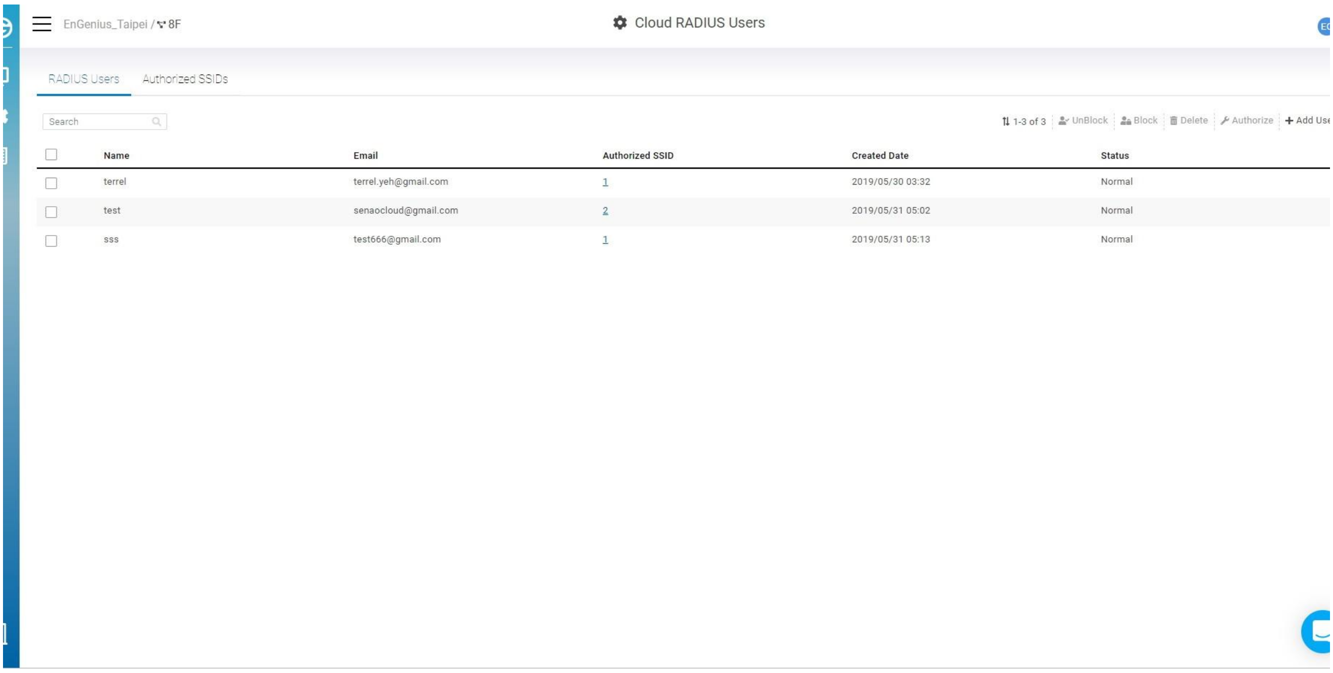
> 1. There must be a Cloud-connected AP nearby try-to-mesh AP to access wirelessly and in the same "Network", so the Mesh configuration can be pushed to 2 AP's to mesh together.
>
> 2. It might take some time since the try-to-mesh AP might need to go through firmware upgrade and reboot (around 4-10 min…).

5. After everything is good, you can find a 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.

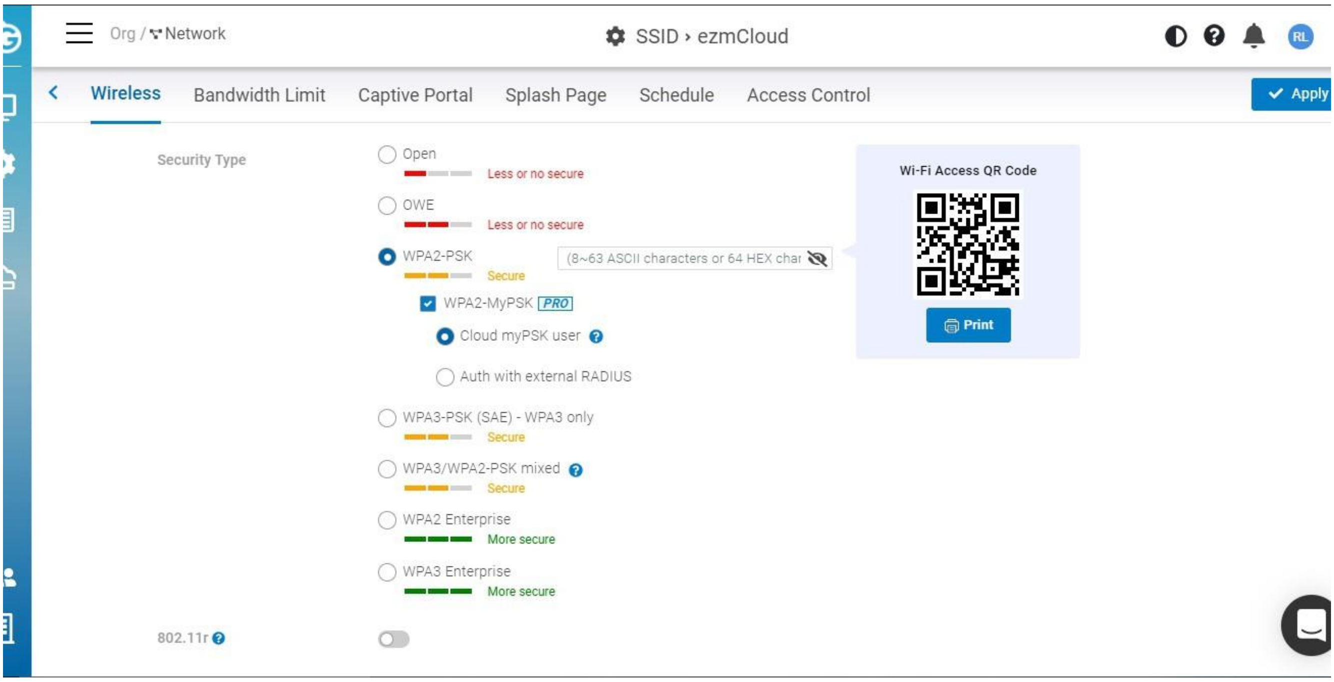
The following describes the functions on this screen:

- **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

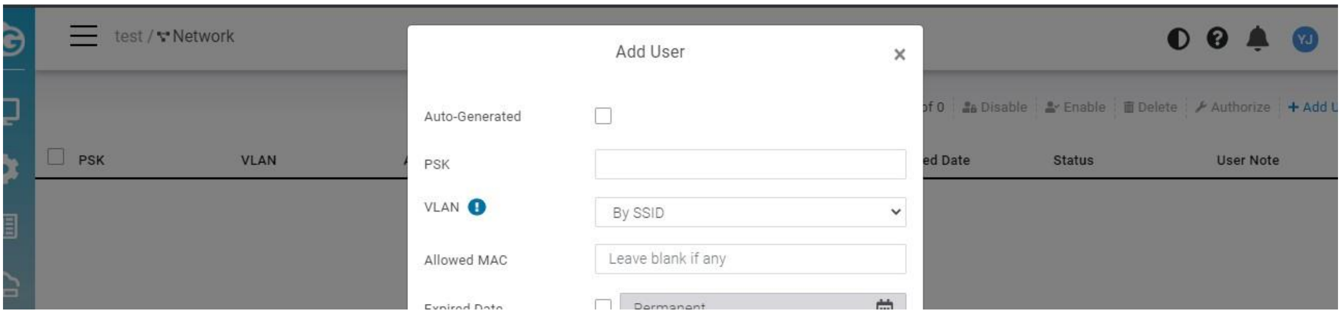
○ WPA2 Enterprise — More secure

○ WPA3 Enterprise — More secure

802.11r

Create my PSK Users

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



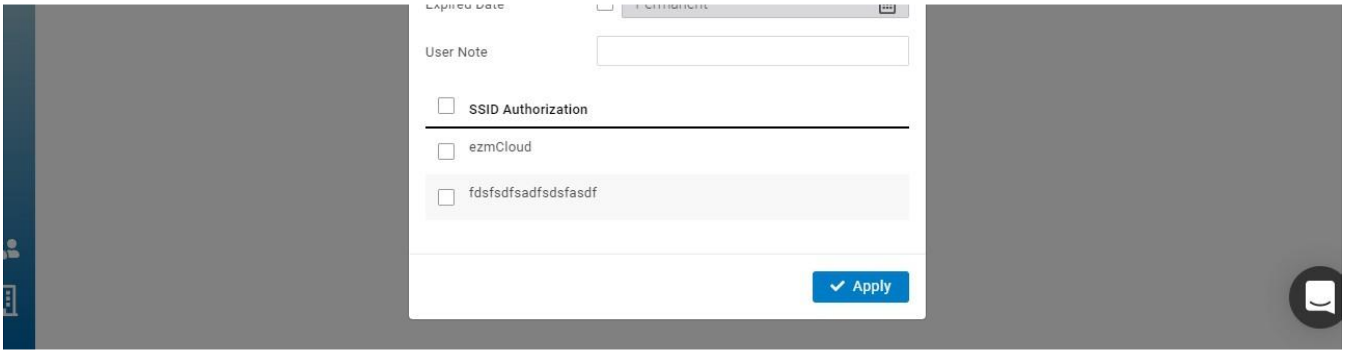
Auto-Generated □

PSK

VLAN By SSID

Allowed MAC Leave blank if any

Expired Date □ Permanent


User Note

□ SSID Authorization

□ ezmCloud

□ fdsfsdfsadfsdsfasdf

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.

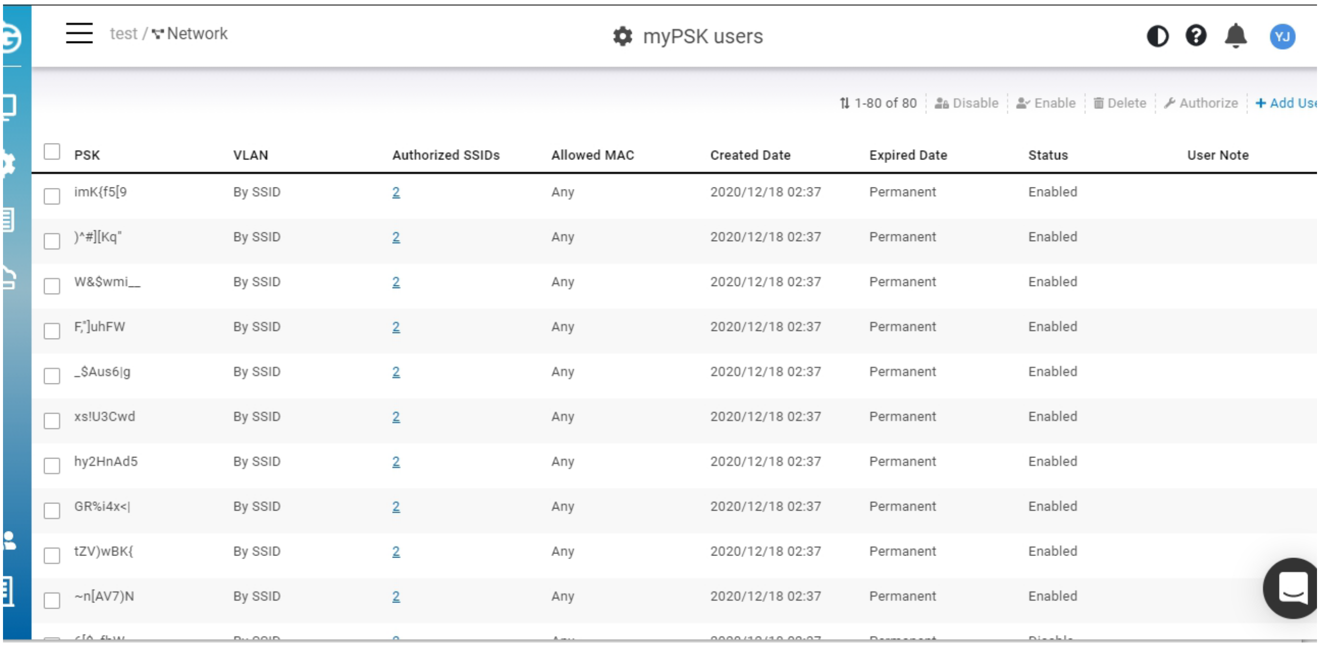
Expired Date: Default is Permanent, click the checkbox to choose the expired date

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

SSID Authorized: The SSIDs you want users to access

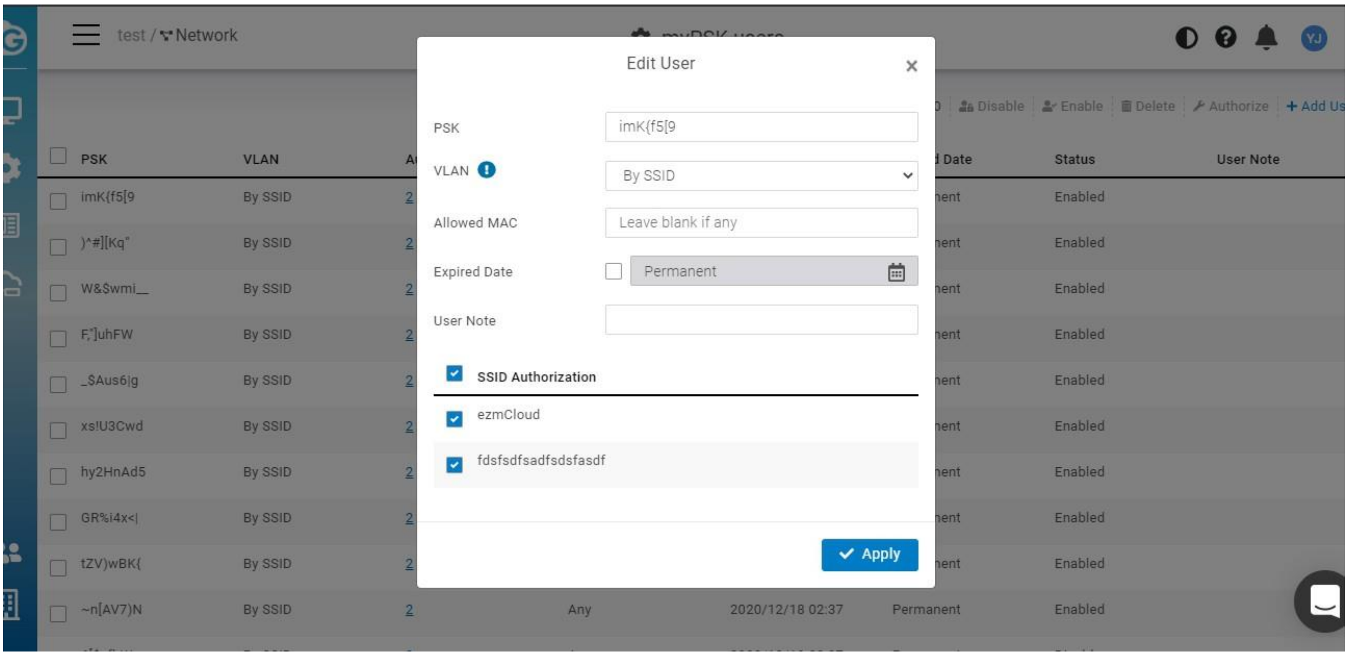
Edit MyPSK Users

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

✓ Apply

PSK	VLAN	A			d Date	Status	User Note
imK{f5[9	By SSID	2			ent	Enabled	
)^#][Kq"	By SSID	2			ent	Enabled	
W&$wmi__	By SSID	2			ent	Enabled	
F,']uhFW	By SSID	2			ent	Enabled	
_$Aus6lg	By SSID	2			ent	Enabled	
xs!U3Cwd	By SSID	2			ent	Enabled	
hy2HnAd5	By SSID	2			ent	Enabled	
GR%i4x<|	By SSID	2			ent	Enabled	
tZV)wBK(	By SSID	2			ent	Enabled	
~n[AV7)N	By SSID	2	Any	2020/12/18 02:37	Permanent	Enabled	

Note

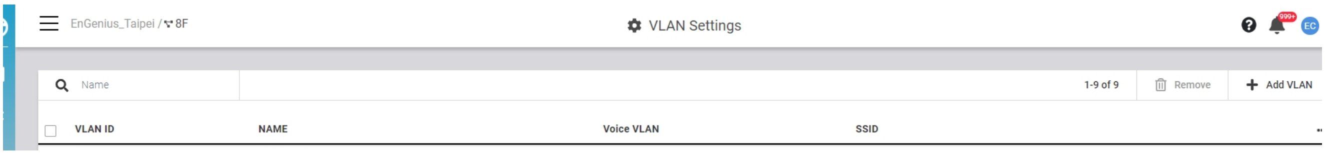
1. Doesn't support Captive portal mode nor NAT mode
2. Each Network has limited to 500 PSK users
3. In the SSID => Wireless => WPA2 myPSK , there is an option "Auth with External RADIUS Server " which is supported with AP v1.X.25 firmware or above. Available models : (ECW220/230/260)

Configuring VLAN

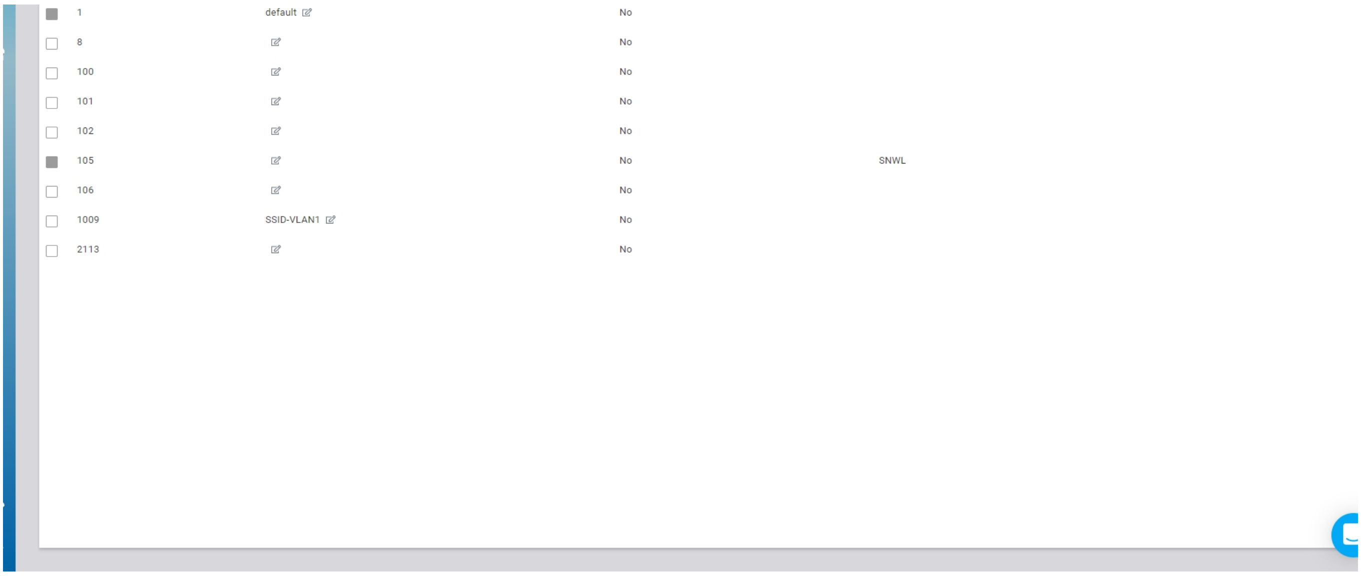
This setting allows you to configure VLAN to all devices in the network at once . Table displays all VLANs have been configure in selected network .

Use this screen to add and delete VLANs for network.

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



VLAN ID	NAME	Voice VLAN	SSID

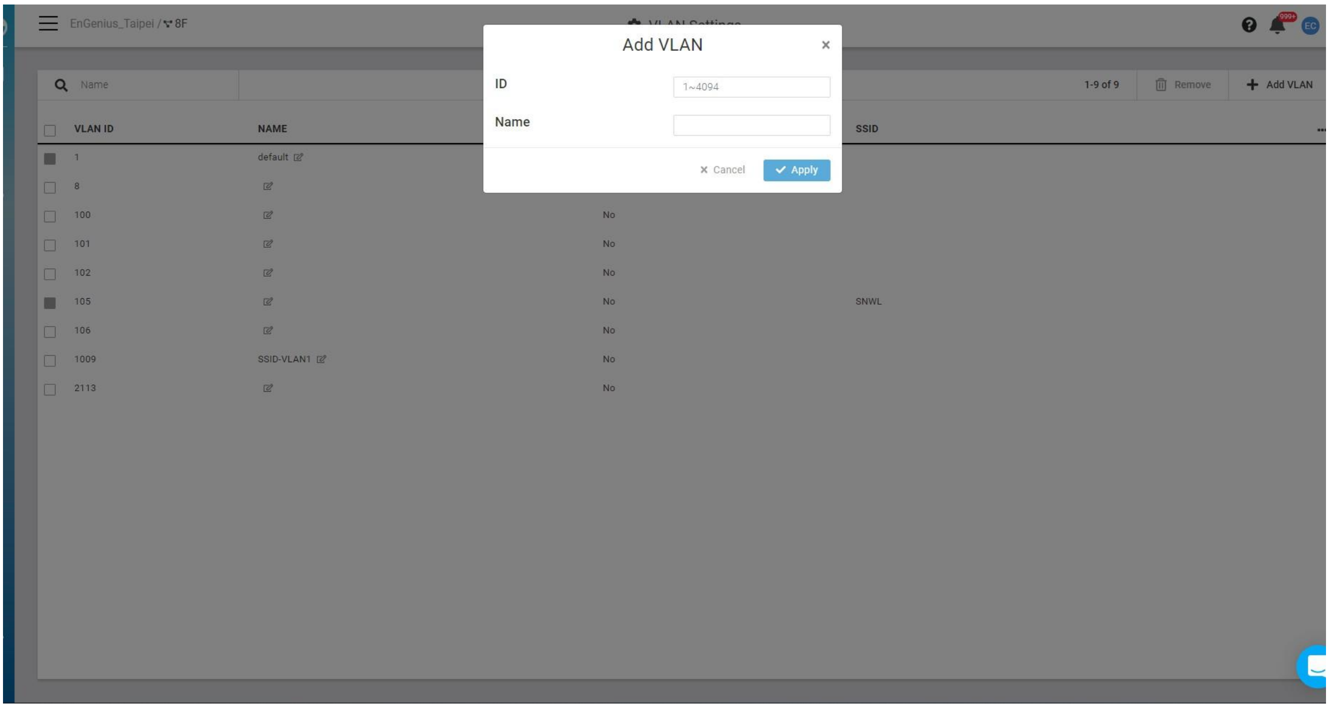


■	1	default	No	
□	8		No	
□	100		No	
□	101		No	
□	102		No	
■	105		No	SNWL
□	106		No	
□	1009	SSID-VLAN1	No	
□	2113		No	

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



Add VLAN

ID: 1~4094

Name:

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

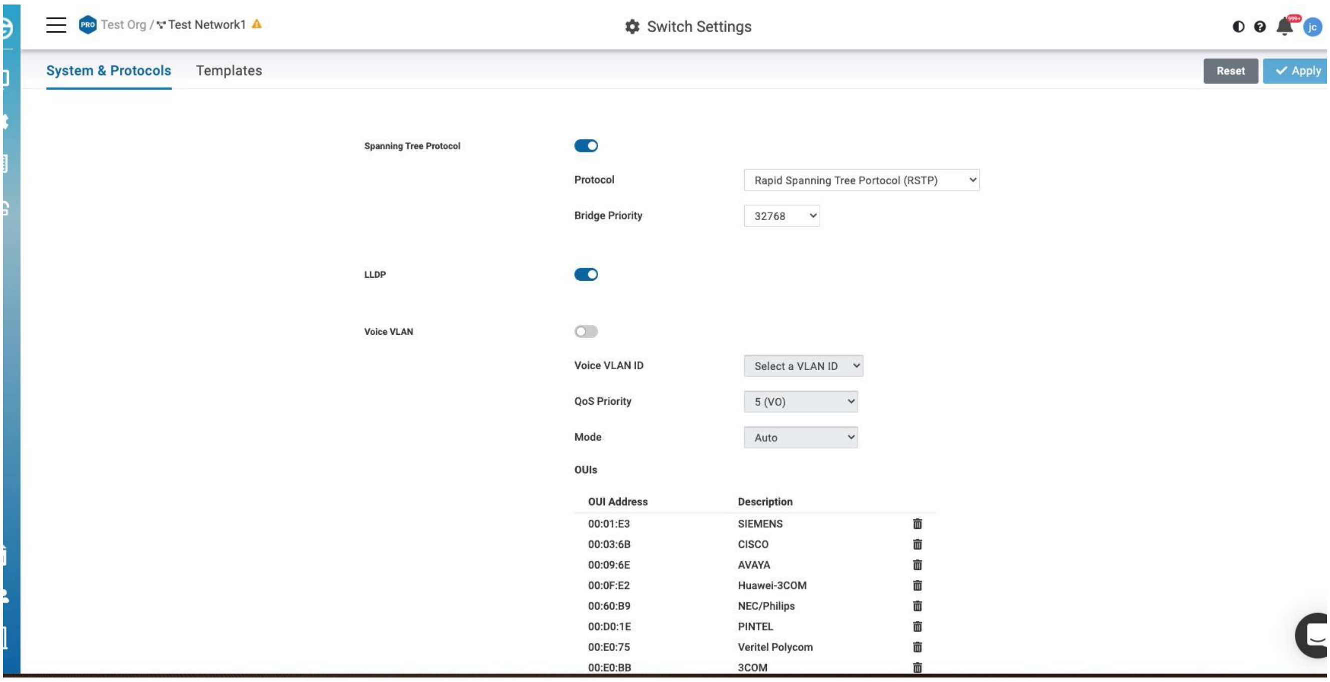
1. Click **Add VLAN** button.
2. Input **VLAN ID** and **VLAN Name.**

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)

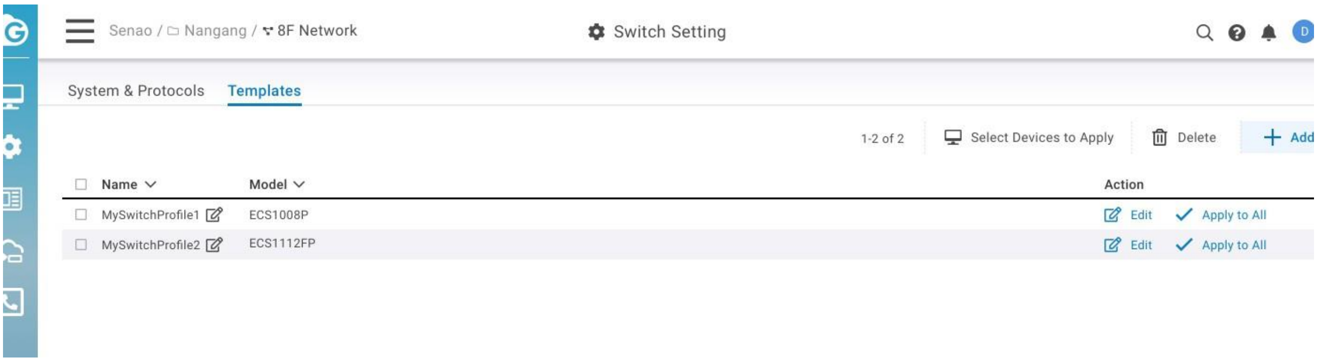
Mode: Auto

OUIs

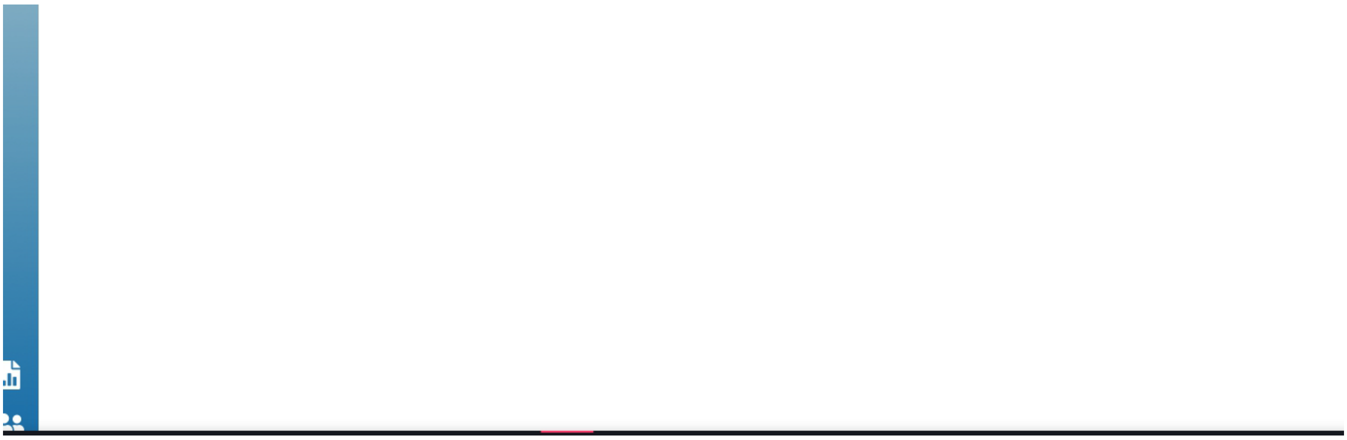
OUI Address	Description
00:01:E3	SIEMENS
00:03:6B	CISCO
00:09:6E	AVAYA
00:0F:E2	Huawei-3COM
00:60:B9	NEC/Philips
00:D0:1E	PINTEL
00:E0:75	Veritel Polycom
00:E0:BB	3COM

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.

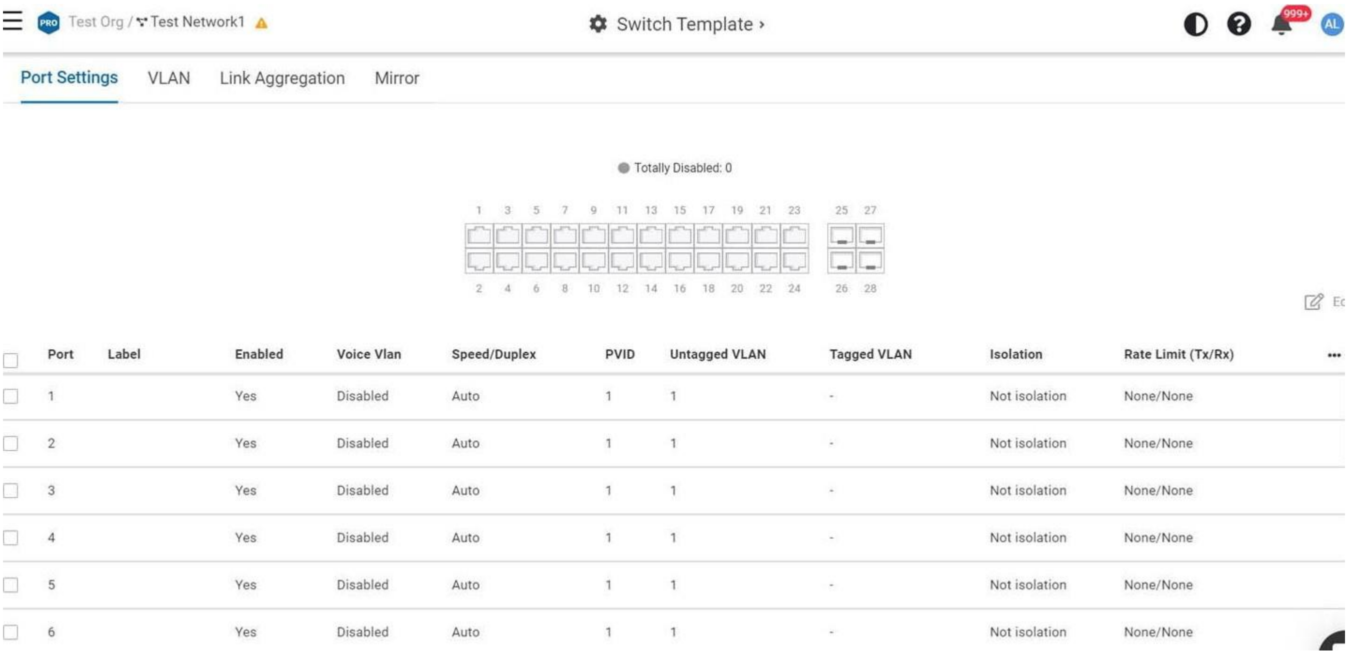
you can access this screen by **Configure** > **Switch Settings** > **Template**



□ 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.



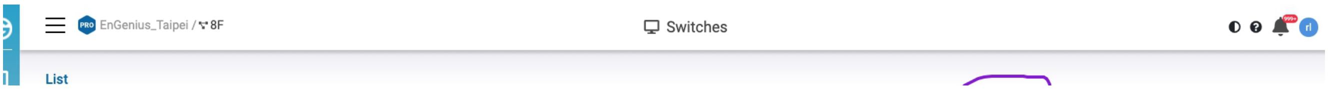
□	Port	Label	Enabled	Voice Vlan	Speed/Duplex	PVID	Untagged VLAN	Tagged VLAN	Isolation	Rate Limit (Tx/Rx)	•••
□	1		Yes	Disabled	Auto	1	1	-	Not isolation	None/None	
□	2		Yes	Disabled	Auto	1	1	-	Not isolation	None/None	
□	3		Yes	Disabled	Auto	1	1	-	Not isolation	None/None	
□	4		Yes	Disabled	Auto	1	1	-	Not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

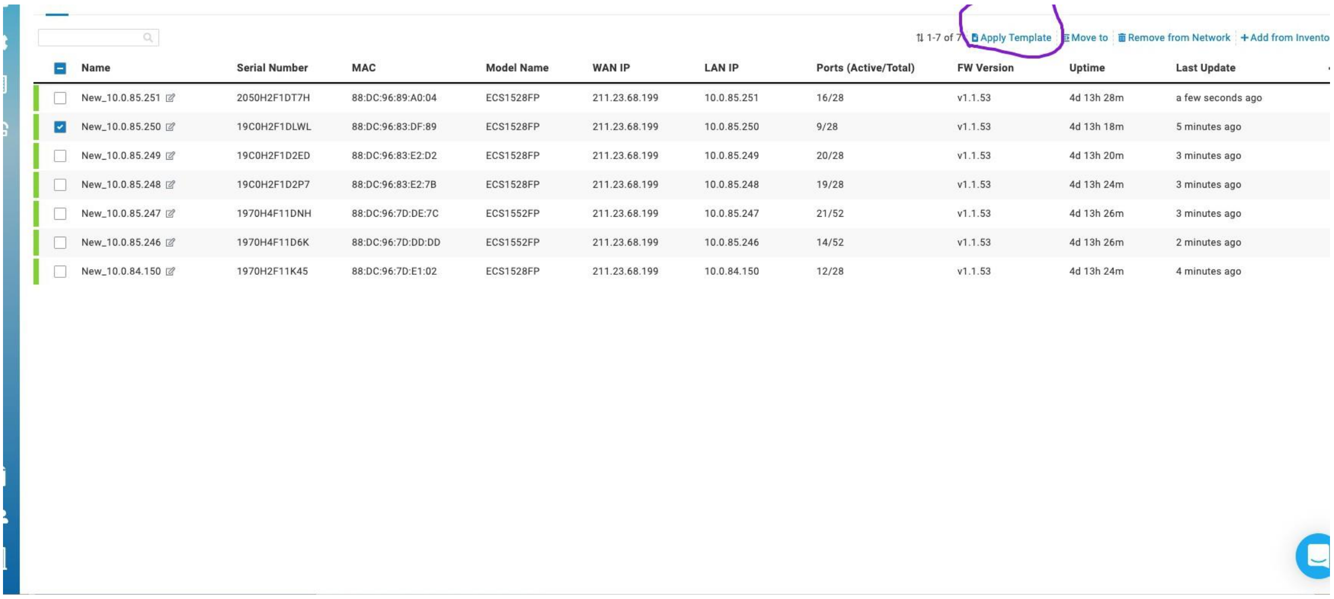
- **Apply to All** will apply the Switch Template to all devices of the same model in the Network.

> **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**





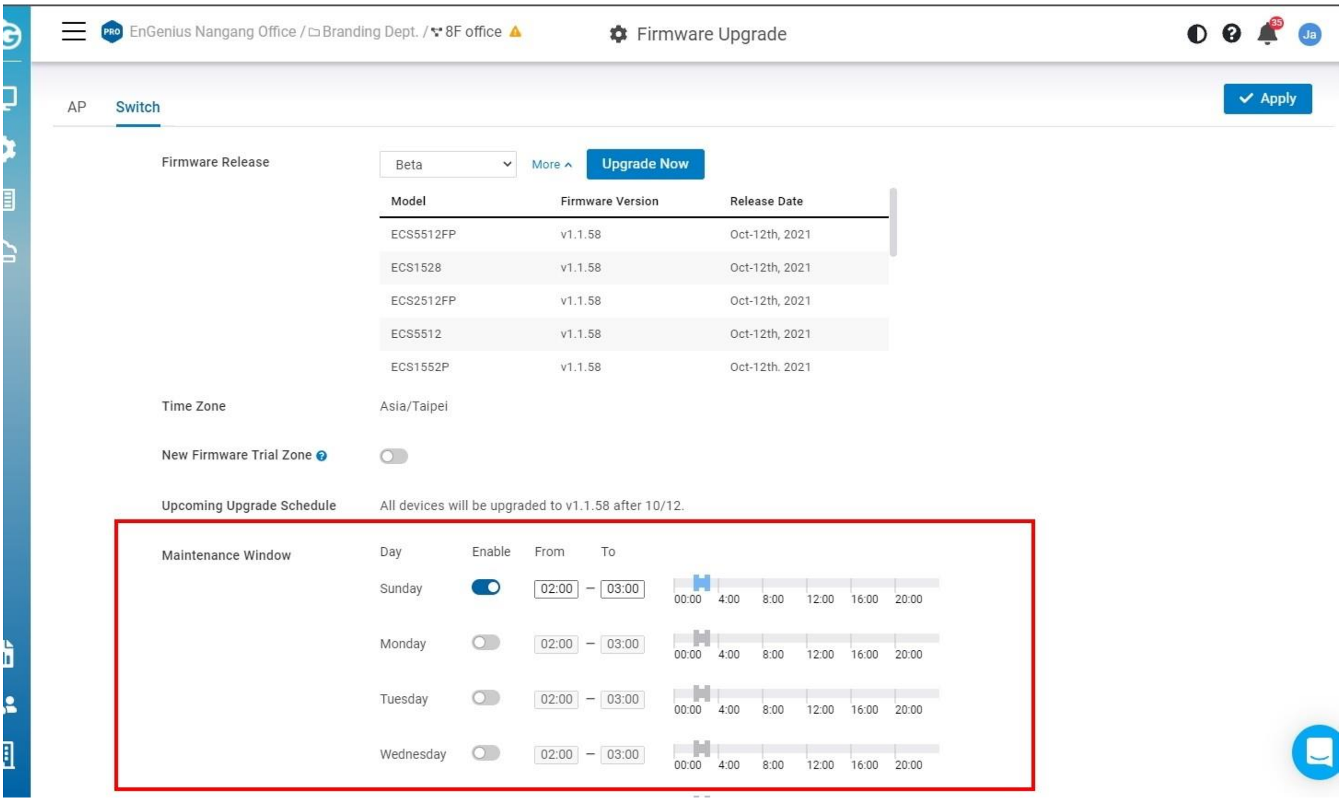
1-7 of 7 Apply Template Move to Remove from Network + Add from Invento

	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.



EnGenius Nangang Office / Branding Dept. / 8F office

Firmware Upgrade

Firmware Release: Beta

Model	Firmware Version	Release Date
ECS5512FP	v1.1.58	Oct-12th, 2021
ECS1528	v1.1.58	Oct-12th, 2021
ECS2512FP	v1.1.58	Oct-12th, 2021
ECS5512	v1.1.58	Oct-12th, 2021
ECS1552P	v1.1.58	Oct-12th, 2021

Time Zone: Asia/Taipei

New Firmware Trial Zone: ○

Upcoming Upgrade Schedule: All devices will be upgraded to v1.1.58 after 10/12.

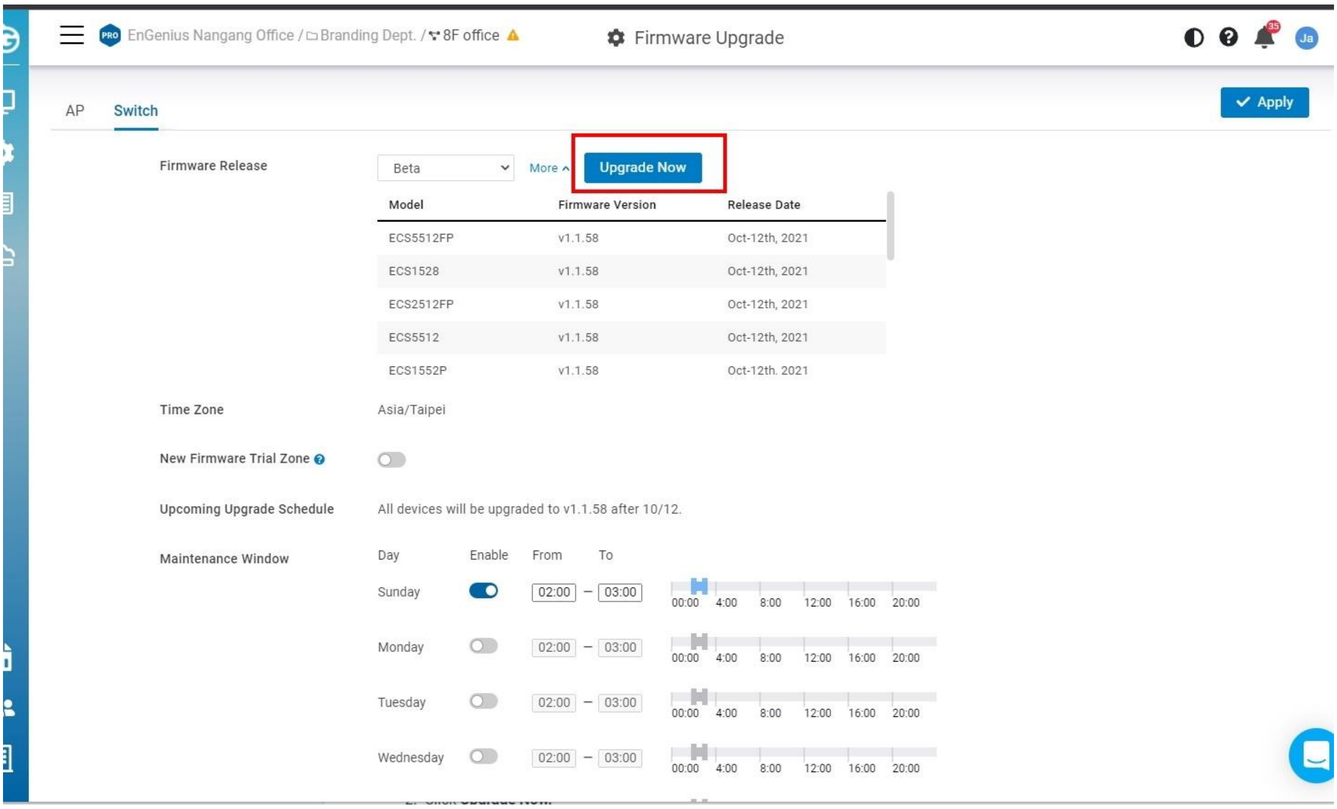
Maintenance Window

Day	Enable	From	To
Sunday	●	02:00	03:00
Monday	○	02:00	03:00
Tuesday	○	02:00	03:00
Wednesday	○	02:00	03:00

Manual Upgrade

To manually update device firmware:

1. Select the firmware you desire to upgrade.
2. Click **Upgrade Now** (If you have the devices in the New Firmware Trial Zone, you will only upgrade the Firmware on these devices.)



Firmware Release: Beta

Model	Firmware Version	Release Date
ECS5512FP	v1.1.58	Oct-12th, 2021
ECS1528	v1.1.58	Oct-12th, 2021
ECS2512FP	v1.1.58	Oct-12th, 2021
ECS5512	v1.1.58	Oct-12th, 2021
ECS1552P	v1.1.58	Oct-12th. 2021

Time Zone: Asia/Taipei

New Firmware Trial Zone

Upcoming Upgrade Schedule: All devices will be upgraded to v1.1.58 after 10/12.

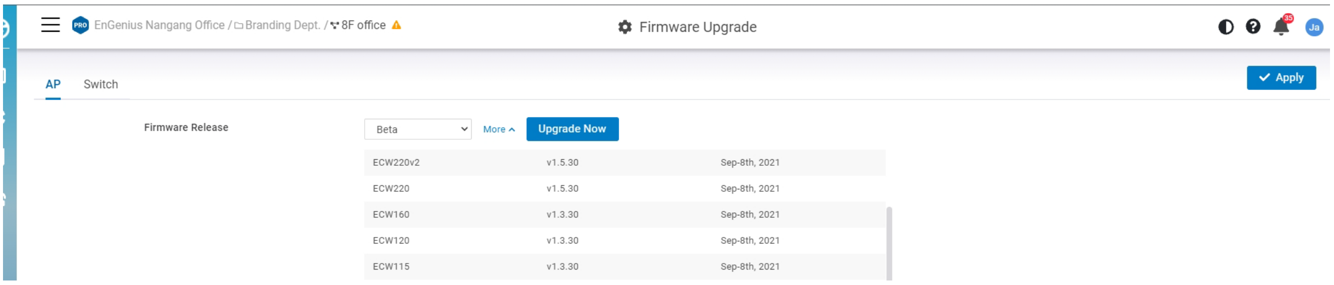
Maintenance Window

Day	Enable	From	To
Sunday	●	02:00	03:00
Monday	○	02:00	03:00
Tuesday	○	02:00	03:00
Wednesday	○	02:00	03:00

3. Click **Apply**.

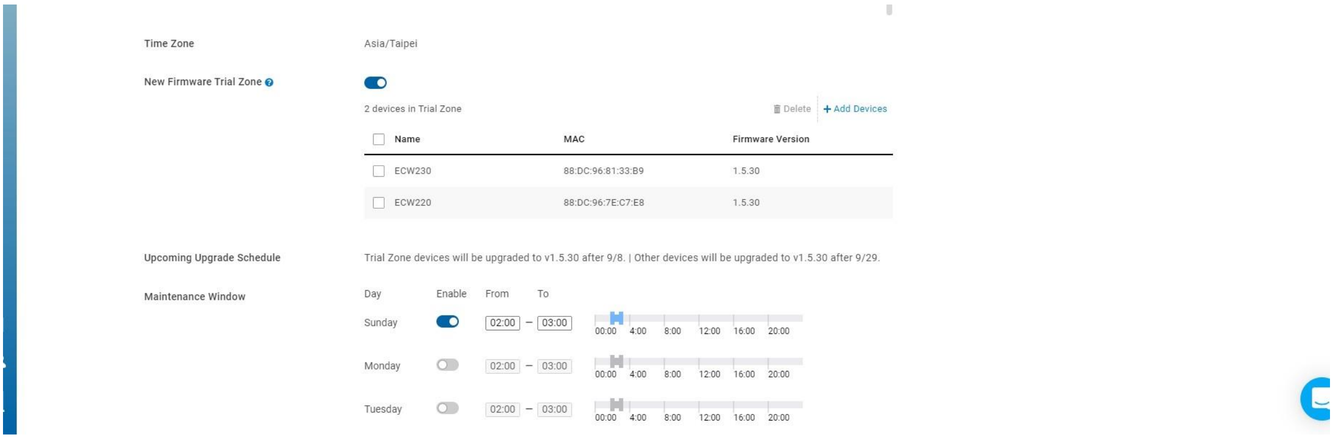
New Firmware Trial Zone

Users can choose cloud devices into a New Firmware Trial Zone, so the devices in Trial Zone will be upgraded first (based on the **Maintenance Window** schedule), the other devices won't be upgraded within 21 days from the firmware release date. So you can prevent from the network going wrong after the firmware upgrade at one time.



Firmware Release: Beta

ECW220v2	v1.5.30	Sep-8th, 2021
ECW220	v1.5.30	Sep-8th, 2021
ECW160	v1.3.30	Sep-8th, 2021
ECW120	v1.3.30	Sep-8th, 2021
ECW115	v1.3.30	Sep-8th, 2021


Time Zone: Asia/Taipei

New Firmware Trial Zone: on

2 devices in Trial Zone

	Name	MAC	Firmware Version
□	ECW230	88:DC:96:81:33:B9	1.5.30
□	ECW220	88:DC:96:7E:C7:E8	1.5.30

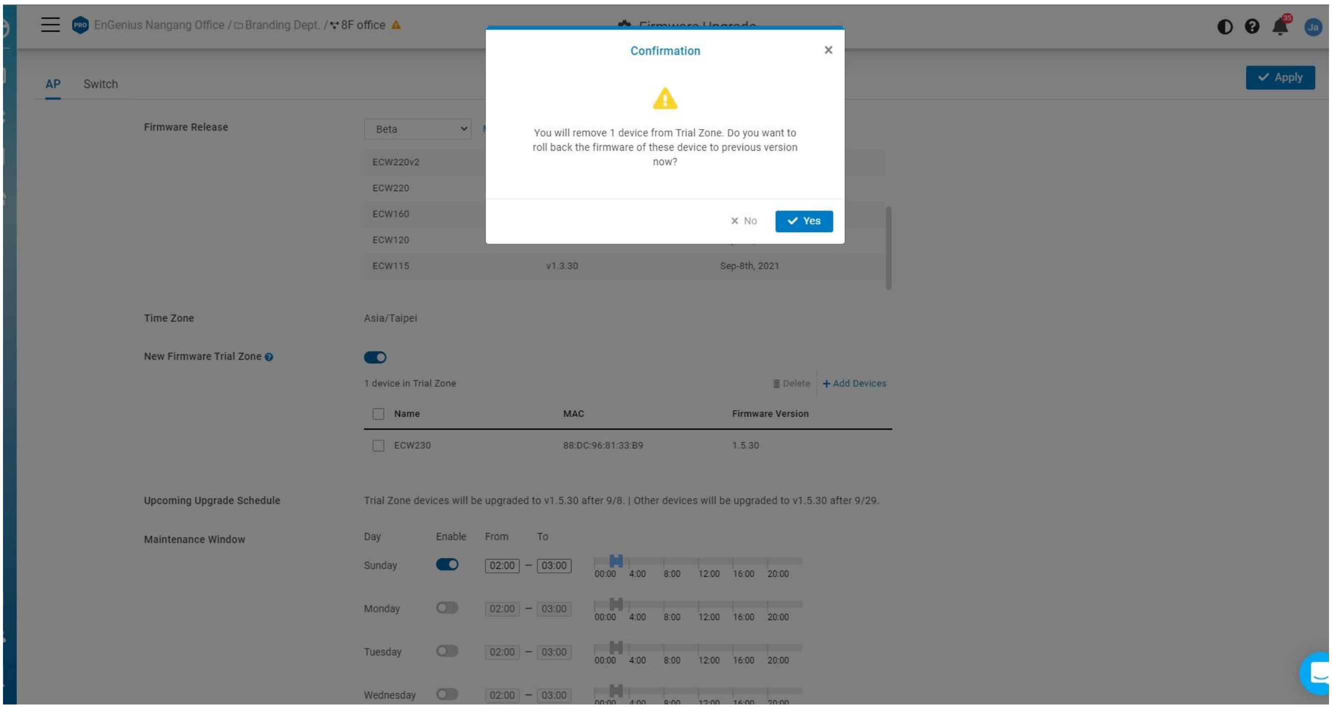
Upcoming Upgrade Schedule: Trial Zone devices will be upgraded to v1.5.30 after 9/8. | Other devices will be upgraded to v1.5.30 after 9/29.

Maintenance Window

Day	Enable	From	To
Sunday	on	02:00	03:00
Monday	off	02:00	03:00
Tuesday	off	02:00	03:00

Rollback to Previous Version

If the firmware has any issue during the trial period, you can call support or roll back to the device's previous firmware version by removing the device from Trial Zone.



Confirmation

You will remove 1 device from Trial Zone. Do you want to roll back the firmware of these device to previous version now?

Firmware Release: Beta

ECW220v2		
ECW220		
ECW160		
ECW120		
ECW115	v1.3.30	Sep-8th, 2021

Time Zone: Asia/Taipei

New Firmware Trial Zone: on

1 device in Trial Zone

	Name	MAC	Firmware Version
□	ECW230	88:DC:96:81:33:B9	1.5.30

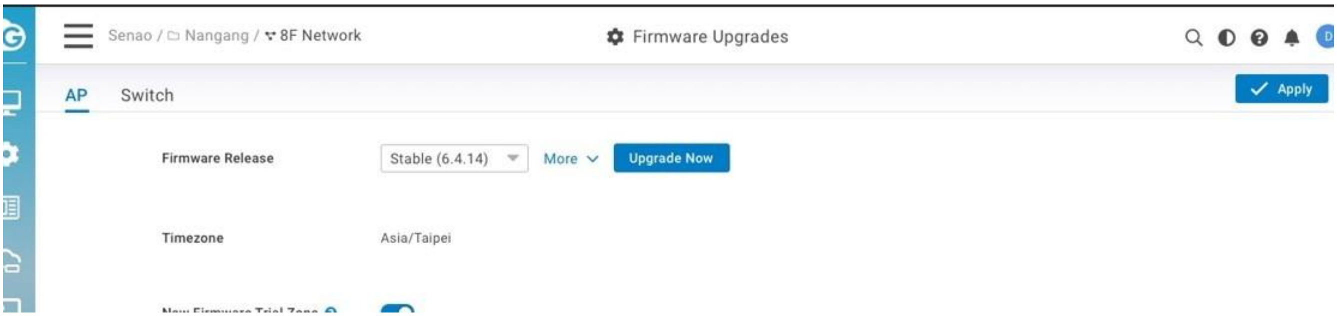
Upcoming Upgrade Schedule: Trial Zone devices will be upgraded to v1.5.30 after 9/8. | Other devices will be upgraded to v1.5.30 after 9/29.

Maintenance Window

Day	Enable	From	To
Sunday	on	02:00	03:00
Monday	off	02:00	03:00
Tuesday	off	02:00	03:00
Wednesday	off	02:00	03:00

Upcoming Upgrade Schedule

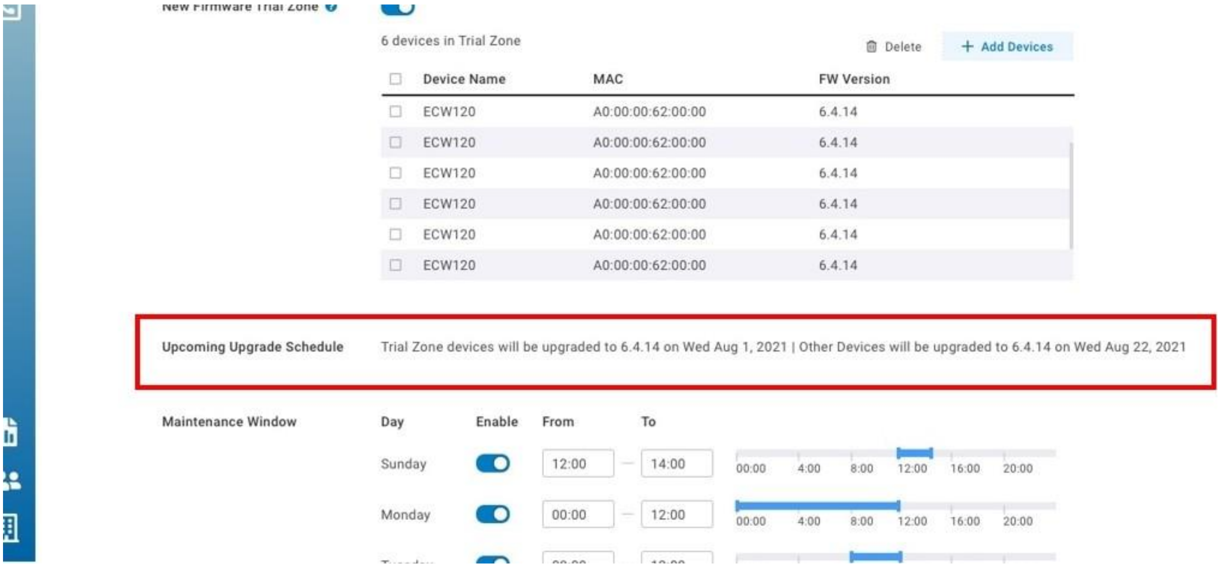
This allows you to know the exact Firmware Upgrade date of Trial Zone devices and other devices. So you will easily know what will be happening next.



Firmware Release: Stable (6.4.14)

Timezone: Asia/Taipei

New Firmware Trial Zone



New Firmware Trial Zone

6 devices in Trial Zone

□	Device Name	MAC	FW Version
□	ECW120	A0:00:00:62:00:00	6.4.14
□	ECW120	A0:00:00:62:00:00	6.4.14
□	ECW120	A0:00:00:62:00:00	6.4.14
□	ECW120	A0:00:00:62:00:00	6.4.14
□	ECW120	A0:00:00:62:00:00	6.4.14
□	ECW120	A0:00:00:62:00:00	6.4.14

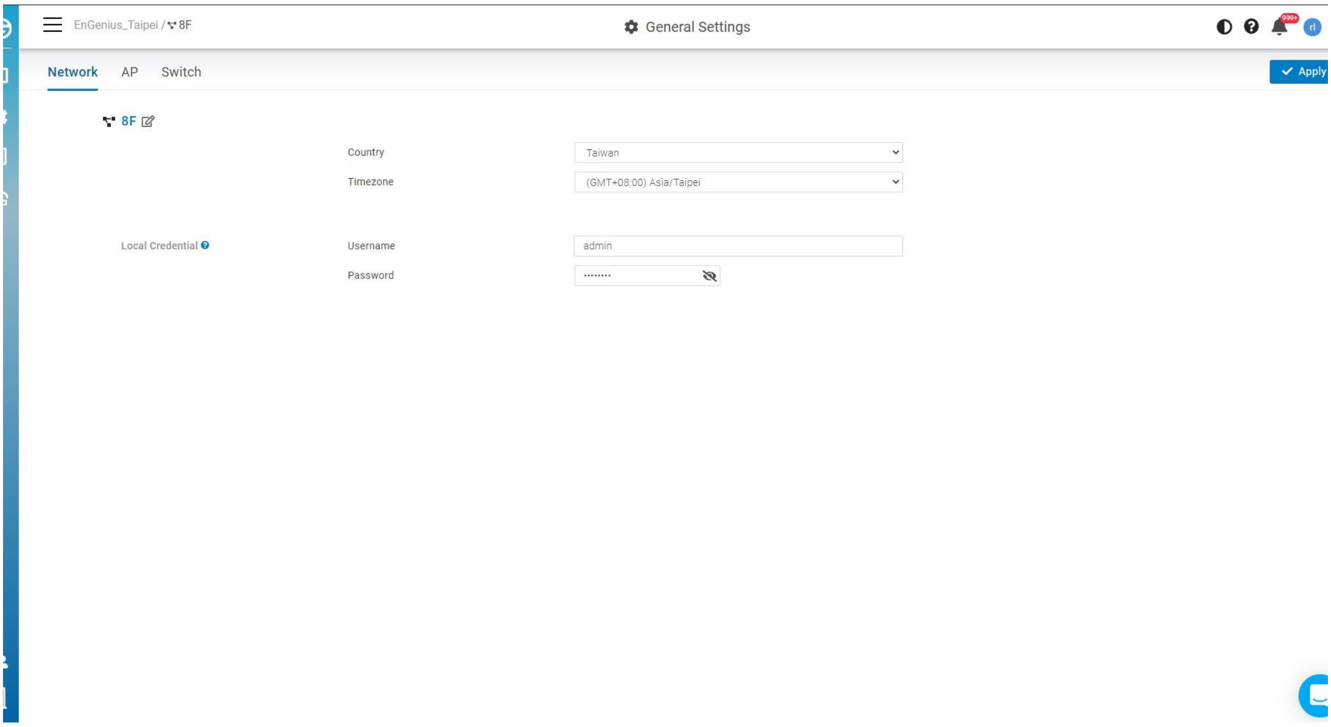
Upcoming Upgrade Schedule: Trial Zone devices will be upgraded to 6.4.14 on Wed Aug 1, 2021 | Other Devices will be upgraded to 6.4.14 on Wed Aug 22, 2021

Maintenance Window

Day	Enable	From	To
Sunday	●	12:00	14:00
Monday	●	00:00	12:00

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.

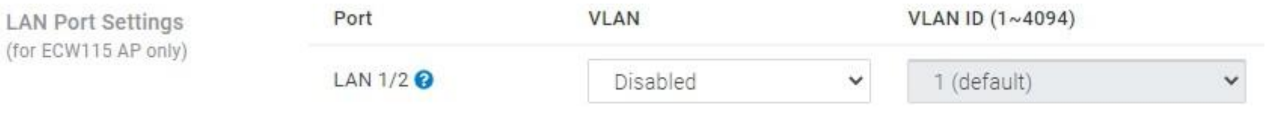
LED Light

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



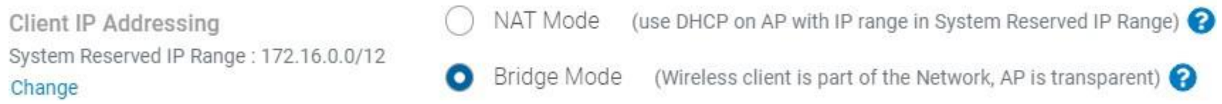
LAN Port Settings (for ECW115 AP only)	Port	VLAN	VLAN ID (1~4094)
	LAN 1/2 ?	Disabled	1 (default)

LAN 3 | Disabled | 1 (default)

System Reserved IP Range

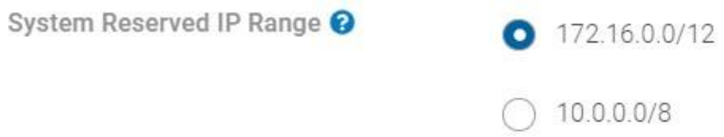
When using NAT (AP DHCP) and captive portal, AP will leverage a range of IP addresses as default. If user unconsciously configures their local Network conflicting with the range, it will cause problems. the user is able to change the System reserved range if they cannot change their local LAN IP address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

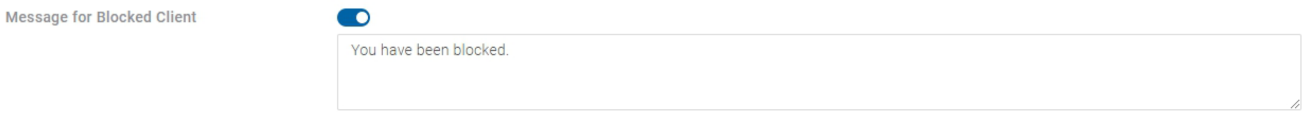
General Settings > **AP** > **System Reserved IP Range**


System Reserved IP Range

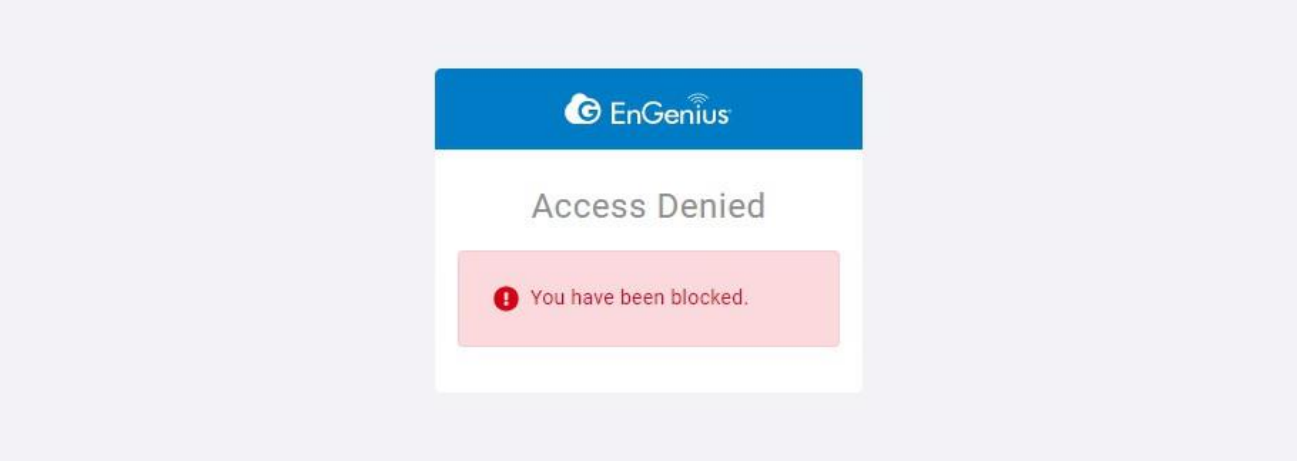
● 172.16.0.0/12
○ 10.0.0.0/8

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

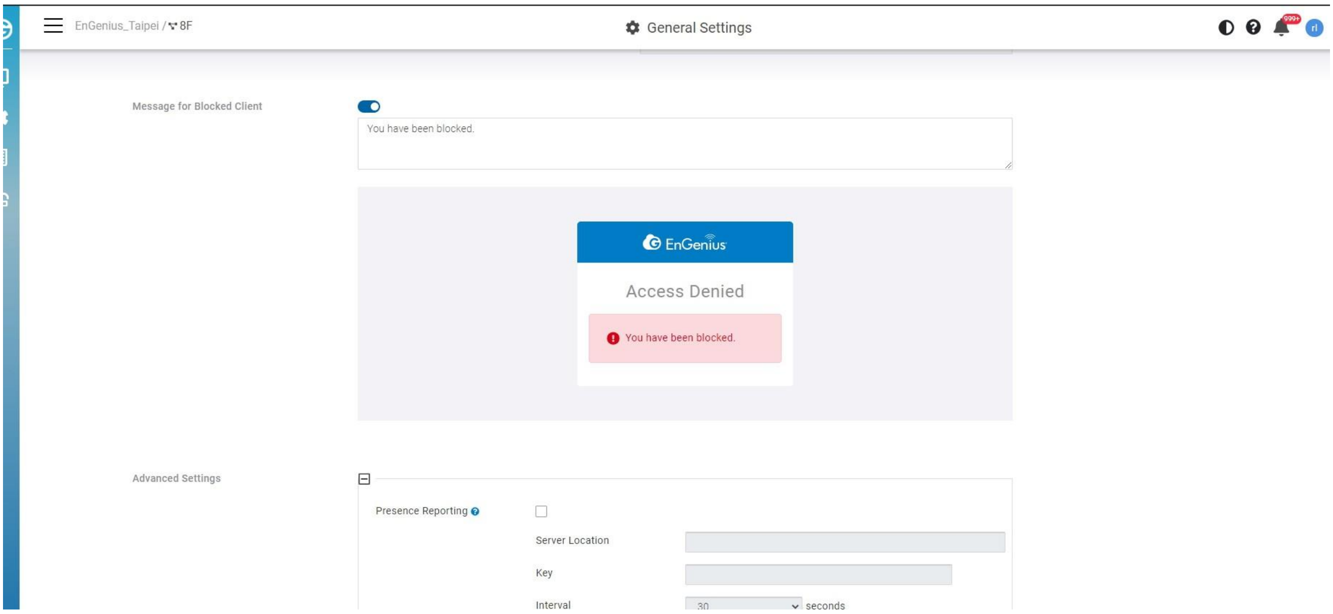
For applications like CRM tools, presence analytics, or location-aware services which need to continuously gather presence data of wireless clients, EnGenius Cloud Acess Points are capable of delivering real-time presence data to fulfill the requirement.

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.

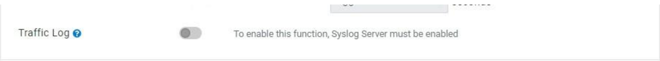
Advanced Settings

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**.

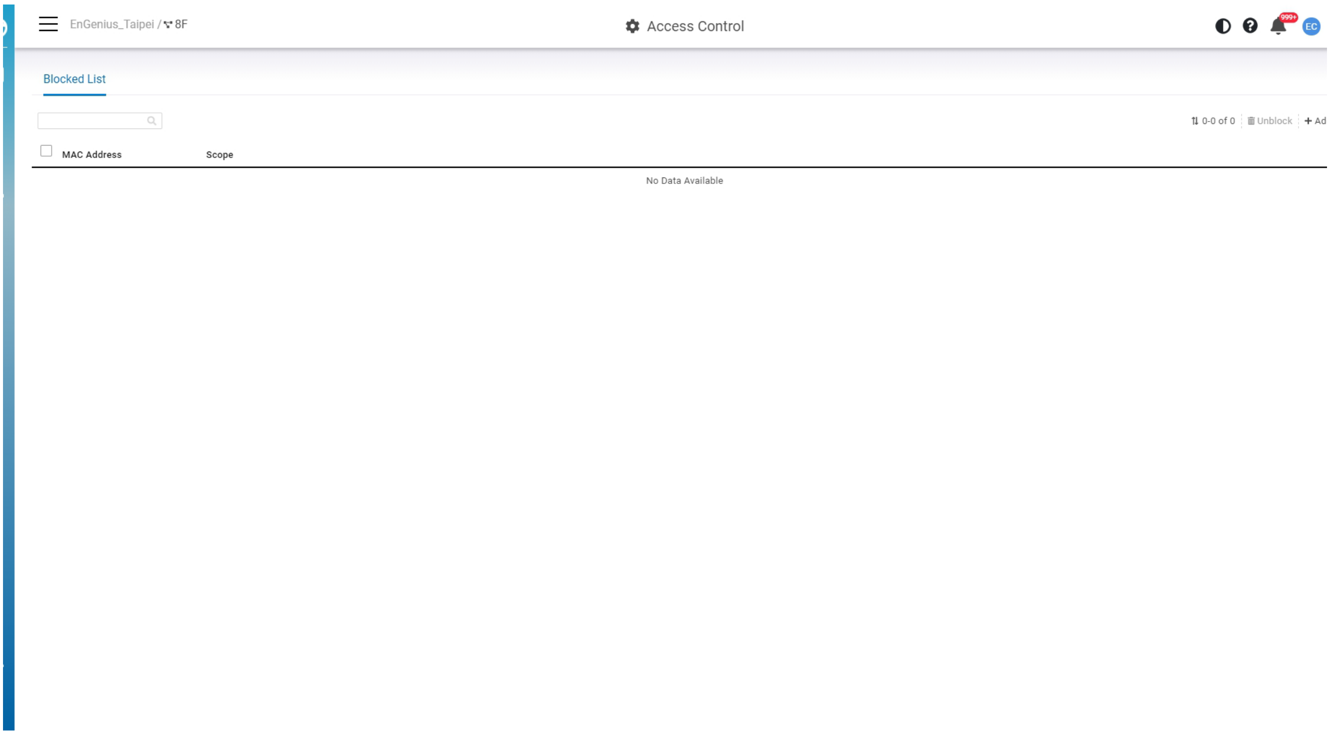
- **Status**: Enable to open the function to the remote system log.
- **Log server address**: Specify the IP address or hostname of the Syslog server.
- **Log server port:** Specify the port of the Syslog server. The default port is 514.

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**

> ⓘ
>
> If L2 isolation is enabled, the whitelist clients will be excluded, which means clients under the subnet can access this client even L2 isolation is on (Only wired client can take effect)
>
> If NAT mode, no whitelist client will be allowed. That means Under NAT mode, “client isolation” will be enabled automatically

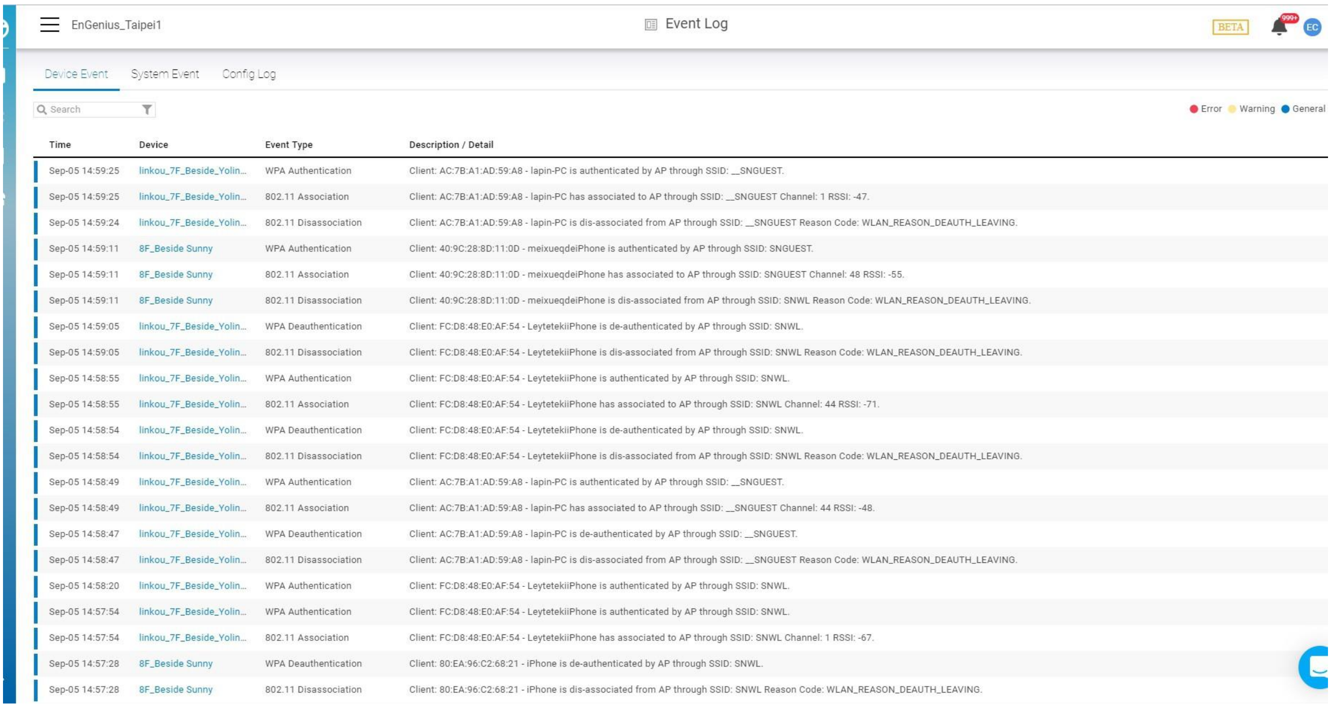
Analytics

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.**

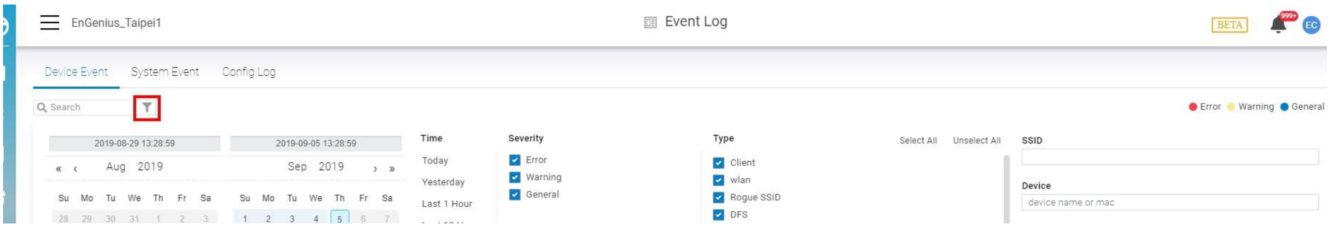
Click **Analyze** > **Event Log** > **Device Event** to access this screen.



Time	Device	Event Type	Description / Detail
Sep-05 14:59:25	linkou_7F_Beside_Yolin...	WPA Authentication	Client: AC:7B:A1:AD:59:A8 - lapin-PC is authenticated by AP through SSID: __SNGUEST.
Sep-05 14:59:25	linkou_7F_Beside_Yolin...	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_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 14:59:11	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_Yolin...	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_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 14:58:55	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.

Searching the Event Log

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



2019-08-29 13:28:59

2019-09-05 13:28:59

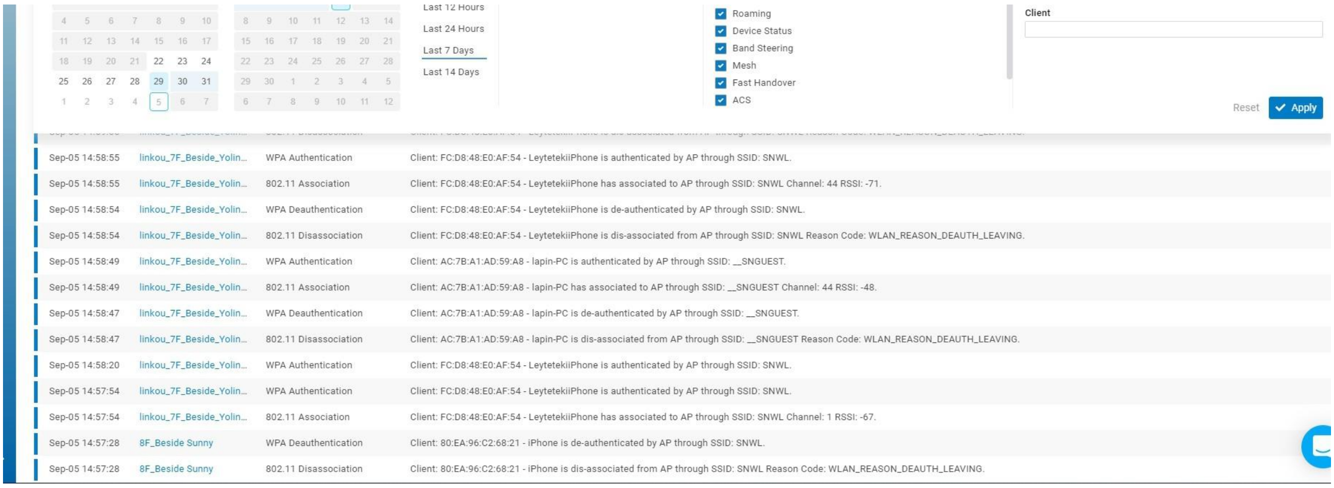
Time: Today, Yesterday, Last 1 Hour

Severity: ☑ Error ☑ Warning ☑ General

Type: ☑ Client ☑ wlan ☑ Rogue SSID ☑ DFS

SSID:

Device: device name or mac



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.

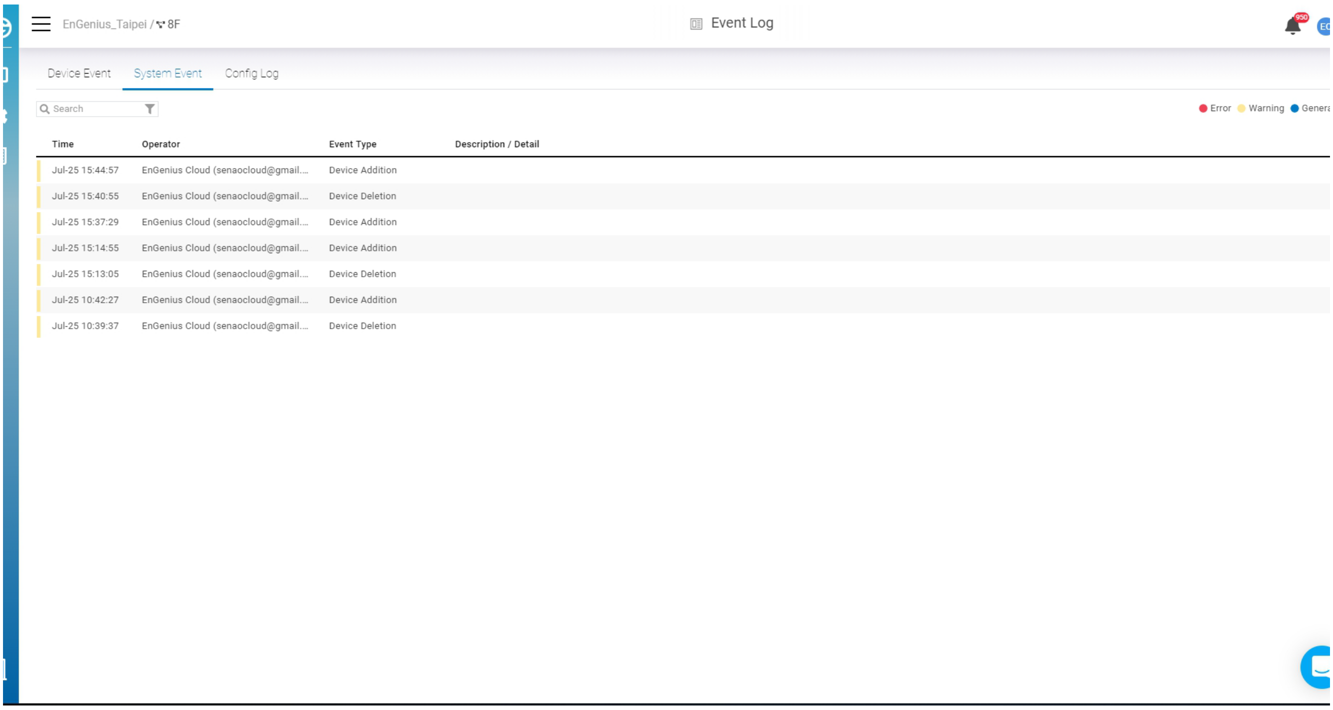
You can specify date/time, severity, and other parameters. Select one or multiple **event types**, then enter the **SSID**, **device name/MAC**, or select **client** to display the log messages related to it. After customizing your search parameters, remember to click **Apply** to perform the search.

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.



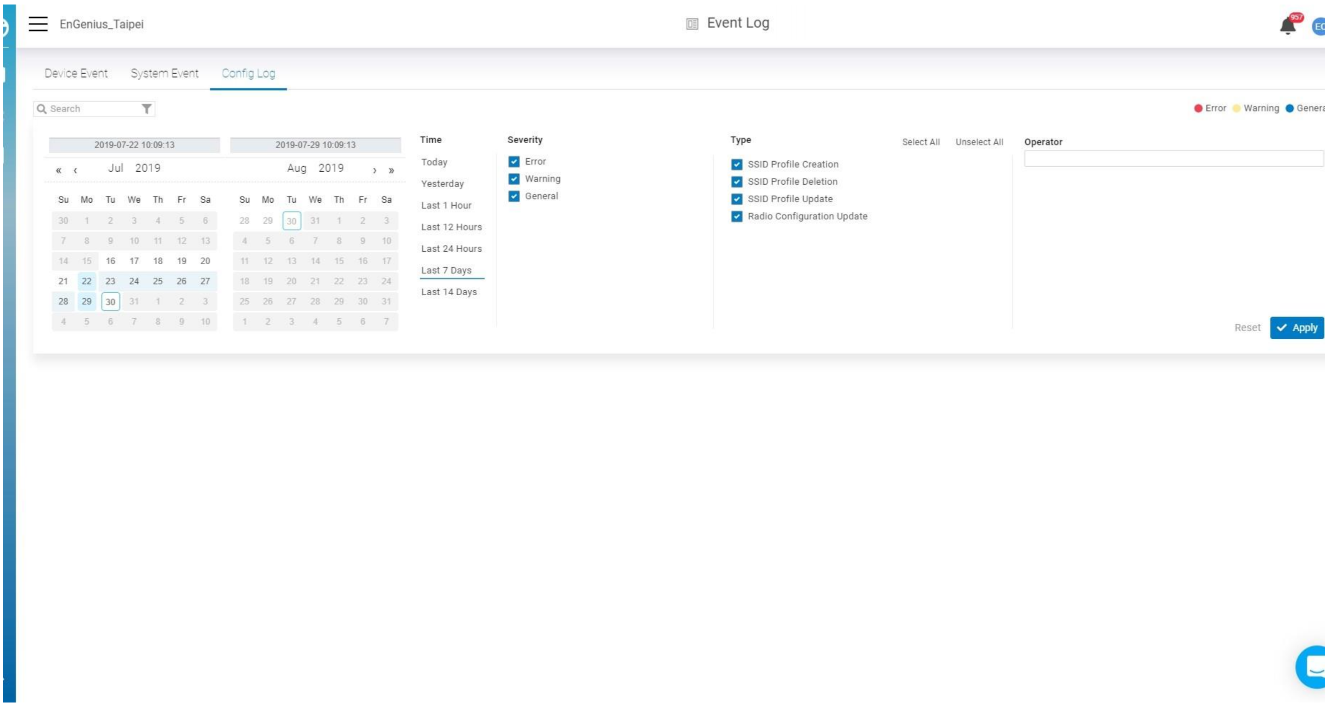
Time	Operator	Event Type	Description / Detail
Jul-25 15:44:57	EnGenius Cloud (senaocloud@gmail....	Device Addition	
Jul-25 15:40:55	EnGenius Cloud (senaocloud@gmail....	Device Deletion	
Jul-25 15:37:29	EnGenius Cloud (senaocloud@gmail....	Device Addition	
Jul-25 15:14:55	EnGenius Cloud (senaocloud@gmail....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

Severity
- ☑ Error
- ☑ Warning
- ☑ General

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

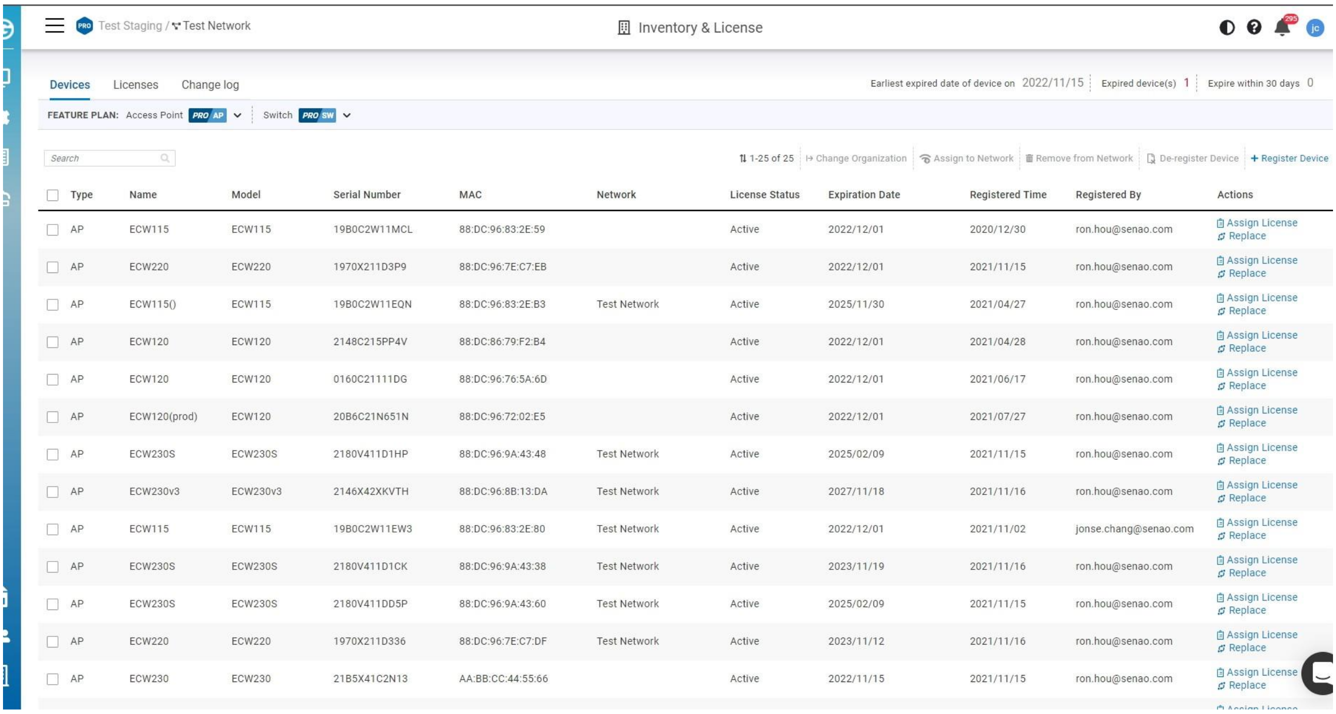
Managing Organizations

Managing Device Inventory and License

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

- **Type**: type of the device.
- **Name**: Device name.
- **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.
- **License Status:** Active, Inactive, Merging, expired, you can see the detailed explanation in the license section.
- **Expiration Date**: The date that the license is expired
- **Register Time**: time of the device's addition to the inventory.
- **Register by**: user responsible for adding the device to the inventory.



Earliest expired date of device on 2022/11/15 | Expired device(s) 1 | Expire within 30 days 0

□	Type	Name	Model	Serial Number	MAC	Network	License Status	Expiration Date	Registered Time	Registered By	Actions
□	AP	ECW115	ECW115	19B0C2W11MCL	88:DC:96:83:2E:59		Active	2022/12/01	2020/12/30	ron.hou@senao.com	Assign License Replace
□	AP	ECW220	ECW220	1970X211D3P9	88:DC:96:7E:C7:EB		Active	2022/12/01	2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW115()	ECW115	19B0C2W11EQN	88:DC:96:83:2E:B3	Test Network	Active	2025/11/30	2021/04/27	ron.hou@senao.com	Assign License Replace
□	AP	ECW120	ECW120	2148C215PP4V	88:DC:86:79:F2:B4		Active	2022/12/01	2021/04/28	ron.hou@senao.com	Assign License Replace
□	AP	ECW120	ECW120	0160C21111DG	88:DC:96:76:5A:6D		Active	2022/12/01	2021/06/17	ron.hou@senao.com	Assign License Replace
□	AP	ECW120(prod)	ECW120	20B6C21N651N	88:DC:96:72:02:E5		Active	2022/12/01	2021/07/27	ron.hou@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411D1HP	88:DC:96:9A:43:48	Test Network	Active	2025/02/09	2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW230v3	ECW230v3	2146X42XKVTH	88:DC:96:8B:13:DA	Test Network	Active	2027/11/18	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW115	ECW115	19B0C2W11EW3	88:DC:96:83:2E:80	Test Network	Active	2022/12/01	2021/11/02	jonse.chang@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411D1CK	88:DC:96:9A:43:38	Test Network	Active	2023/11/19	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411DD5P	88:DC:96:9A:43:60	Test Network	Active	2025/02/09	2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW220	ECW220	1970X211D336	88:DC:96:7E:C7:DF	Test Network	Active	2023/11/12	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW230	ECW230	21B5X41C2N13	AA:BB:CC:44:55:66		Active	2022/11/15	2021/11/15	ron.hou@senao.com	Assign License Replace

On the top of the right corner, you could see below information

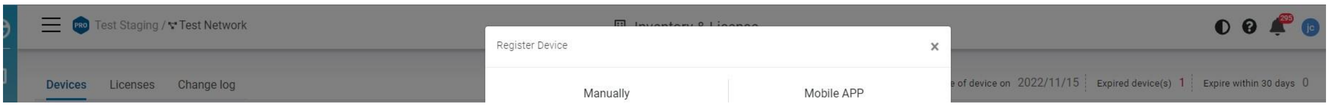
Earliest expired date on of devices on: This will display the earliest expired date of the devices in the organization to remind users to add license by then.

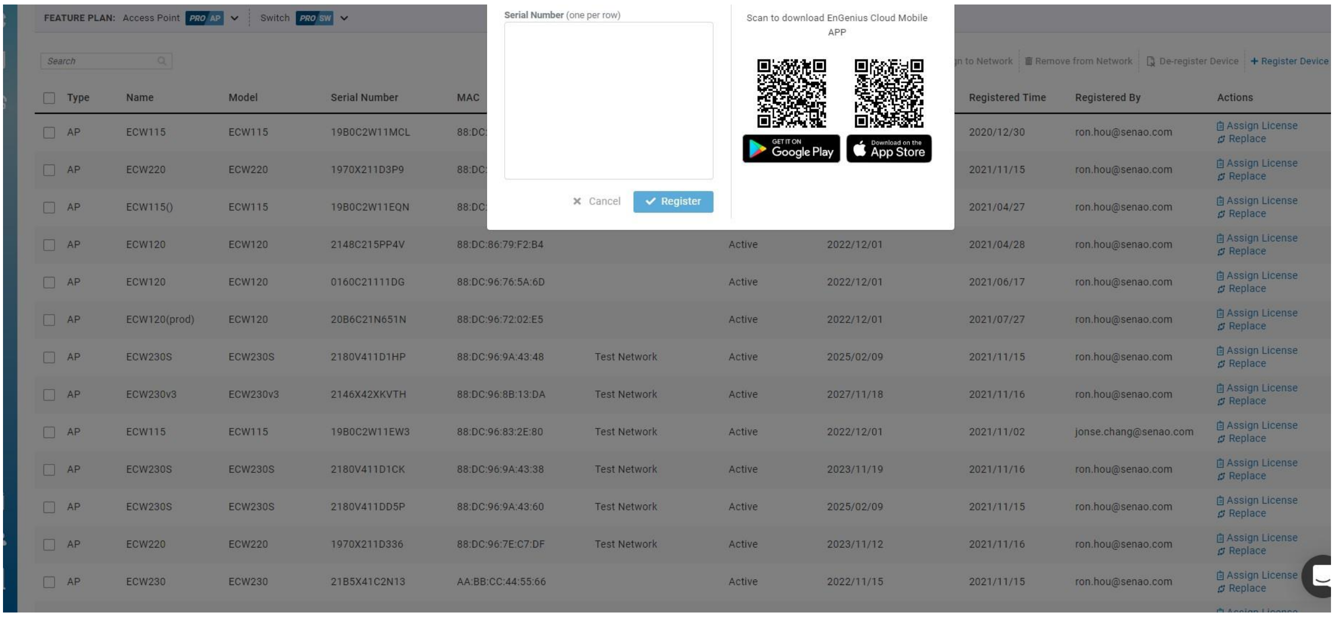
Expired devices: The **n**umber of expired devices in this organization. For example, If it’s AP, and since AP license mode is “Pro”, so those AP cannot be managed by Cloud and show off-line if in Network.

Expire within 30 days: The number of the devices will expire within 30 days in this organization. Furthermore, cloud will send you the notification when there are devices to be expired within 30 days and within 3 days.

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.





Serial Number (one per row)

✕ Cancel ✓ Register

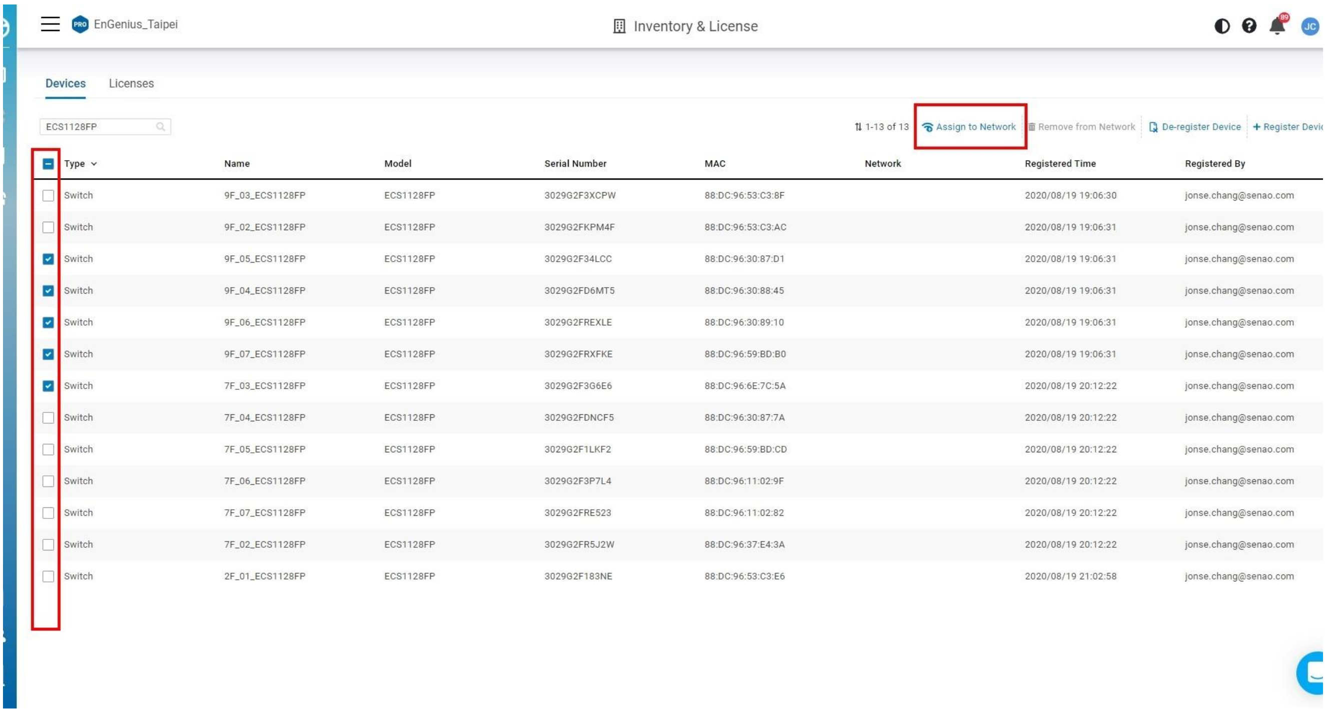
□	Type	Name	Model	Serial Number	MAC				Registered Time	Registered By	Actions
□	AP	ECW115	ECW115	19B0C2W11MCL	88:DC:				2020/12/30	ron.hou@senao.com	Assign License Replace
□	AP	ECW220	ECW220	1970X211D3P9	88:DC:				2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW115()	ECW115	19B0C2W11EQN	88:DC:				2021/04/27	ron.hou@senao.com	Assign License Replace
□	AP	ECW120	ECW120	2148C215PP4V	88:DC:86:79:F2:B4		Active	2022/12/01	2021/04/28	ron.hou@senao.com	Assign License Replace
□	AP	ECW120	ECW120	0160C21111DG	88:DC:96:76:5A:6D		Active	2022/12/01	2021/06/17	ron.hou@senao.com	Assign License Replace
□	AP	ECW120(prod)	ECW120	20B6C21N651N	88:DC:96:72:02:E5		Active	2022/12/01	2021/07/27	ron.hou@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411D1HP	88:DC:96:9A:43:48	Test Network	Active	2025/02/09	2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW230v3	ECW230v3	2146X42XKVTH	88:DC:96:8B:13:DA	Test Network	Active	2027/11/18	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW115	ECW115	19B0C2W11EW3	88:DC:96:83:2E:80	Test Network	Active	2022/12/01	2021/11/02	jonse.chang@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411D1CK	88:DC:96:9A:43:38	Test Network	Active	2023/11/19	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW230S	ECW230S	2180V411DD5P	88:DC:96:9A:43:60	Test Network	Active	2025/02/09	2021/11/15	ron.hou@senao.com	Assign License Replace
□	AP	ECW220	ECW220	1970X211D336	88:DC:96:7E:C7:DF	Test Network	Active	2023/11/12	2021/11/16	ron.hou@senao.com	Assign License Replace
□	AP	ECW230	ECW230	21B5X41C2N13	AA:BB:CC:44:55:66		Active	2022/11/15	2021/11/15	ron.hou@senao.com	Assign License Replace

Assigning Devices to a Network

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

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

3. Click **Assign to Network**.



☐	Type	Name	Model	Serial Number	MAC	Network	Registered Time	Registered By
□	Switch	9F_03_ECS1128FP	ECS1128FP	3029G2F3XCPW	88:DC:96:53:C3:8F		2020/08/19 19:06:30	jonse.chang@senao.com
□	Switch	9F_02_ECS1128FP	ECS1128FP	3029G2FKPM4F	88:DC:96:53:C3:AC		2020/08/19 19:06:31	jonse.chang@senao.com
☑	Switch	9F_05_ECS1128FP	ECS1128FP	3029G2F34LCC	88:DC:96:30:87:D1		2020/08/19 19:06:31	jonse.chang@senao.com
☑	Switch	9F_04_ECS1128FP	ECS1128FP	3029G2FD6MT5	88:DC:96:30:88:45		2020/08/19 19:06:31	jonse.chang@senao.com
☑	Switch	9F_06_ECS1128FP	ECS1128FP	3029G2FREXLE	88:DC:96:30:89:10		2020/08/19 19:06:31	jonse.chang@senao.com
☑	Switch	9F_07_ECS1128FP	ECS1128FP	3029G2FRXFKE	88:DC:96:59:BD:B0		2020/08/19 19:06:31	jonse.chang@senao.com
☑	Switch	7F_03_ECS1128FP	ECS1128FP	3029G2F3G6E6	88:DC:96:6E:7C:5A		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	7F_04_ECS1128FP	ECS1128FP	3029G2FDNCF5	88:DC:96:30:87:7A		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	7F_05_ECS1128FP	ECS1128FP	3029G2F1LKF2	88:DC:96:59:BD:CD		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	7F_06_ECS1128FP	ECS1128FP	3029G2F3P7L4	88:DC:96:11:02:9F		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	7F_07_ECS1128FP	ECS1128FP	3029G2FRE523	88:DC:96:11:02:82		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	7F_02_ECS1128FP	ECS1128FP	3029G2FR5J2W	88:DC:96:37:E4:3A		2020/08/19 20:12:22	jonse.chang@senao.com
□	Switch	2F_01_ECS1128FP	ECS1128FP	3029G2F183NE	88:DC:96:53:C3:E6		2020/08/19 21:02:58	jonse.chang@senao.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 device page.
2. Select one or multiple devices as per your requirements.
3. Click **Remove from Network.**

De-registering a Device from EnGenius Cloud

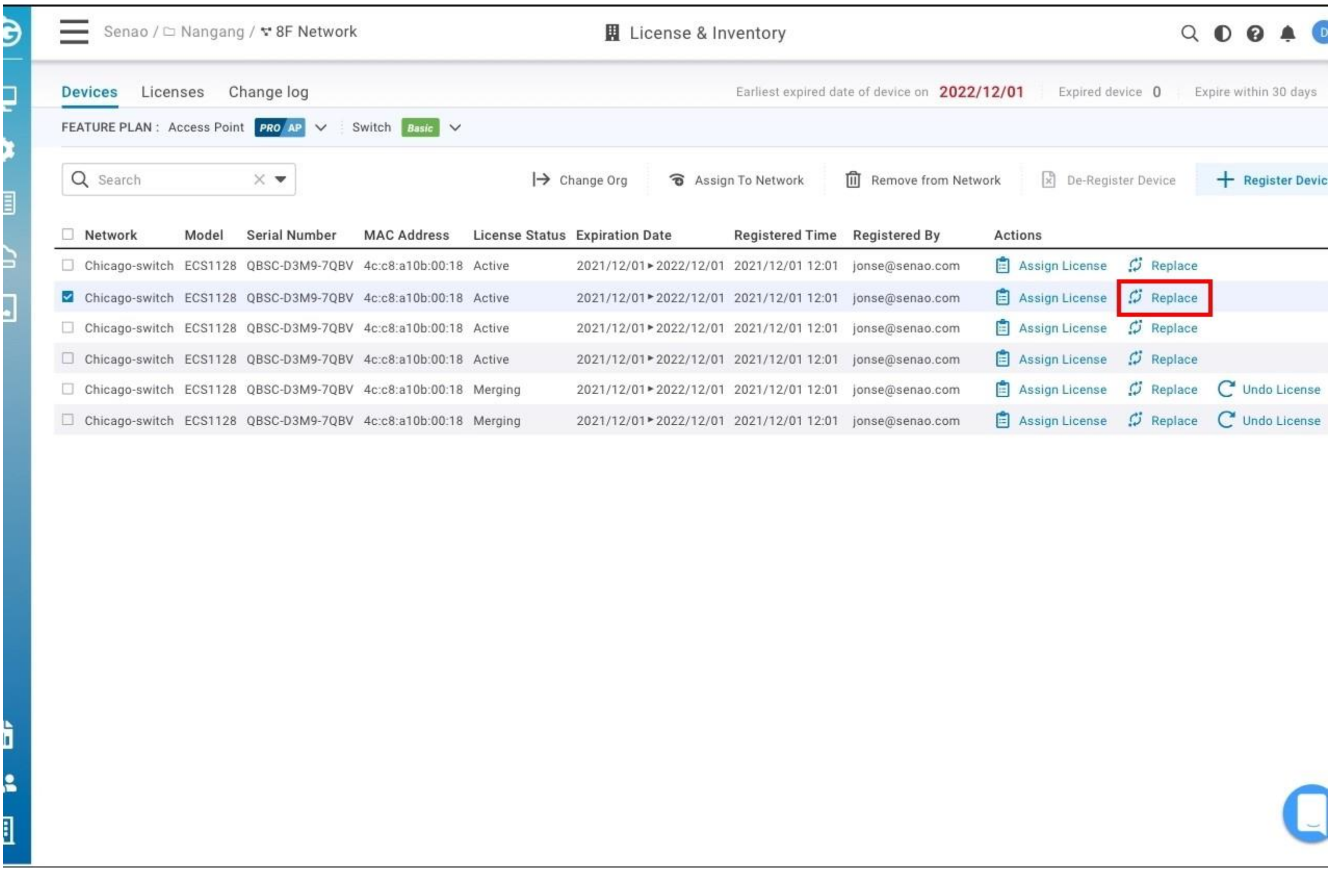
This feature allows you to remove registered devices from EnGenius Cloud inventory.

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

> ⓘ If you de-register the device when the license status is active or merged, the license on the device will be deleted. As for status is merging, the license will be disassociated. This action cannot be undone and all records will be lost.

Replace the device

The device can be replaced with other devices for RMA/DoA purposes. This is the only way the license on the device can be transferred to other devices, so the replaced device's license will be expired after you replace the device successfully and the new device will use the replaced device's license.



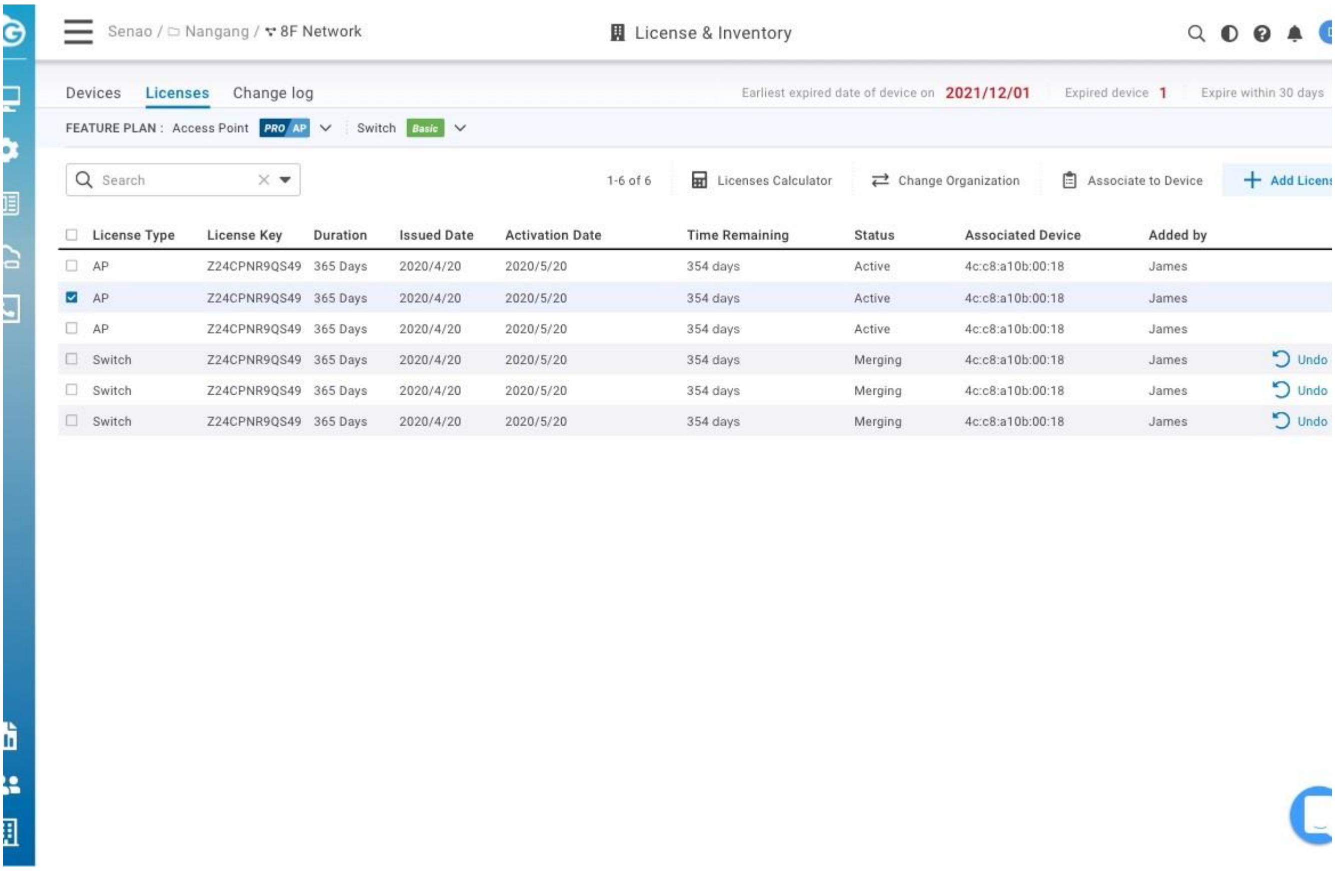
Earliest expired date of device on 2022/12/01 Expired device 0 Expire within 30 days

FEATURE PLAN : Access Point PRO AP Switch Basic

□	Network	Model	Serial Number	MAC Address	License Status	Expiration Date	Registered Time	Registered By	Actions		
□	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Active	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	
☑	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Active	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	
□	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Active	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	
□	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Active	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	
□	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Merging	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	Undo License
□	Chicago-switch	ECS1128	QBSC-D3M9-7QBV	4c:c8:a10b:00:18	Merging	2021/12/01▸2022/12/01	2021/12/01 12:01	jonse@senao.com	Assign License	Replace	Undo License

Per-Device Licensing

The Per-Device licensing model allows users to assign a license directly to a specific device. There are two types of feature plans - BASIC and PRO. (For details, click on "https://www.engenius.ai/cloud/licenses"). You need to buy the AP Pro license to associate with the AP to use the AP Pro feature set and so does Switch. You can navigate to the Organization > Inventory & License > license tab to access this page.



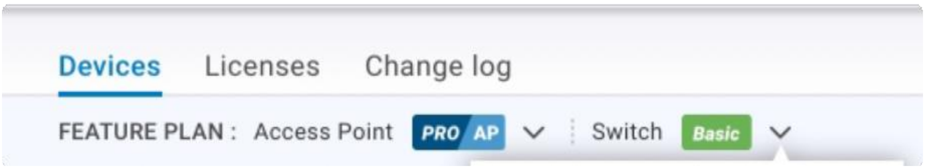
Earliest expired date of device on 2021/12/01 Expired device 1 Expire within 30 days

1-6 of 6

□	License Type	License Key	Duration	Issued Date	Activation Date	Time Remaining	Status	Associated Device	Added by	
□	AP	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Active	4c:c8:a10b:00:18	James	
☑	AP	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Active	4c:c8:a10b:00:18	James	
□	AP	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Active	4c:c8:a10b:00:18	James	
□	Switch	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Merging	4c:c8:a10b:00:18	James	Undo
□	Switch	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Merging	4c:c8:a10b:00:18	James	Undo
□	Switch	Z24CPNR9QS49	365 Days	2020/4/20	2020/5/20	354 days	Merging	4c:c8:a10b:00:18	James	Undo

Feature plan

On the top of the page, you can switch the Feature plan per Device type.



For example, you need the PRO feature and there is a pro icon near the feature name. What you need to do in advance to use the PRO feature is below.

1. Purchase the AP/ SW PRO license to get the License Key
2. Add the License Key on the License page and associate the licenses to Devices (AP/SW)

3. Switch the AP/SW feature plan to PRO, so you can use this feature (https://www.engenius.ai/cloud/licenses) => The AP/SW feature plan details.

Icon	Description
Basic	Device will use basic feature plan. No license is required
PRO AP	AP Professional Plan is required.
PRO SW	Switch Professional Plan is required.

- Note 1: Under the"Pro" feature plan, all devices need to have valid licenses, otherwise the device will not be able to be managed by Cloud.

License status

Inactive: A license has not started to burn.

Active: The license starts to burn which means the license has started to tick and the time remaining starts to decrease.

Merging: There is a 7 days grace period for users to undo the license associated with a device, in case users place the license wrongly. Once “merged”, after 7 days or when the license is activated, the license is bundled with the device and cannot be removed. (the only way is “replacement”)

Expired: The license on the device is expired

Merged: When the license is associated with the device after 7 days grace period but hasn't been used (activated). For example, if a license is added to a device that has a license on it already, the newly-added license will become “merged” and the activation date will be the date after the previous license.

Canceled: When the license order is canceled, the license will be canceled, and the associated device's expired date will be deducted.

1 Year Free License

All existing devices and any newly registered devices will have 1 year free Pro license.

The activation date is the date the device is “registered” to the Org, and the expired date is after 1 year. If the user de-registered the device and register again, The cloud will keep the expired date.

Note: For purchased licenses associated with the device already, once the device is de-registered from the Organization, Cloud cannot associate the licenses with the device anymore, so if the device registers to Organization again, it’s like a brand new one without the license.