EnGenius Certified Wireless Professional (ECWP)

ECWP training

Visualize Your Network

Engenius Networks EU
www.engeniusnetworks.eu

EnGenius Certified Wireless Professional - topics

- Course overview
- EnGenius Cloud overview
- WLAN fundamentals
- WLAN planning and design
- Initialization
- Management
- Monitoring
- Security
- Diagnostic tools
- Glossary
- ECWP exam

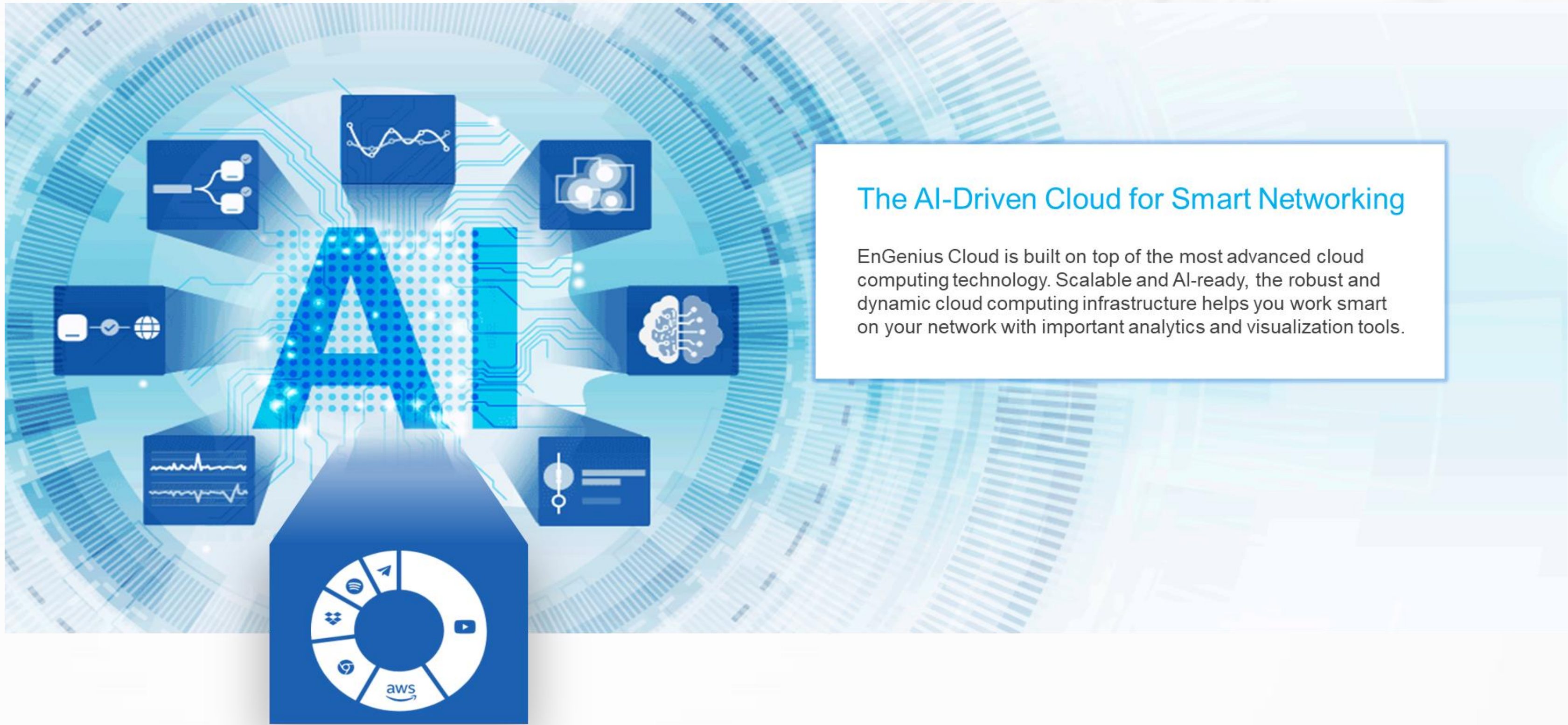
Course overview

The EnGenius Cloud Certified Wireless Professional (ECWP) Course, equips personnel with the knowledge necessary for managing wired and wireless cloud-based networks through EnGenius' product offerings.

EnGenius Cloud overview

EnGenius Cloud, one of the solutions offered by EnGenius, simplifies wireless and wired network management through an AI-Driven cloud platform.

EnGenius Cloud is built on top of the most advanced cloud computing technology. Scalable and AI-ready, the robust and dynamic cloud computing infrastructure helps you work smarter on your network with important analytics and visualization tools.



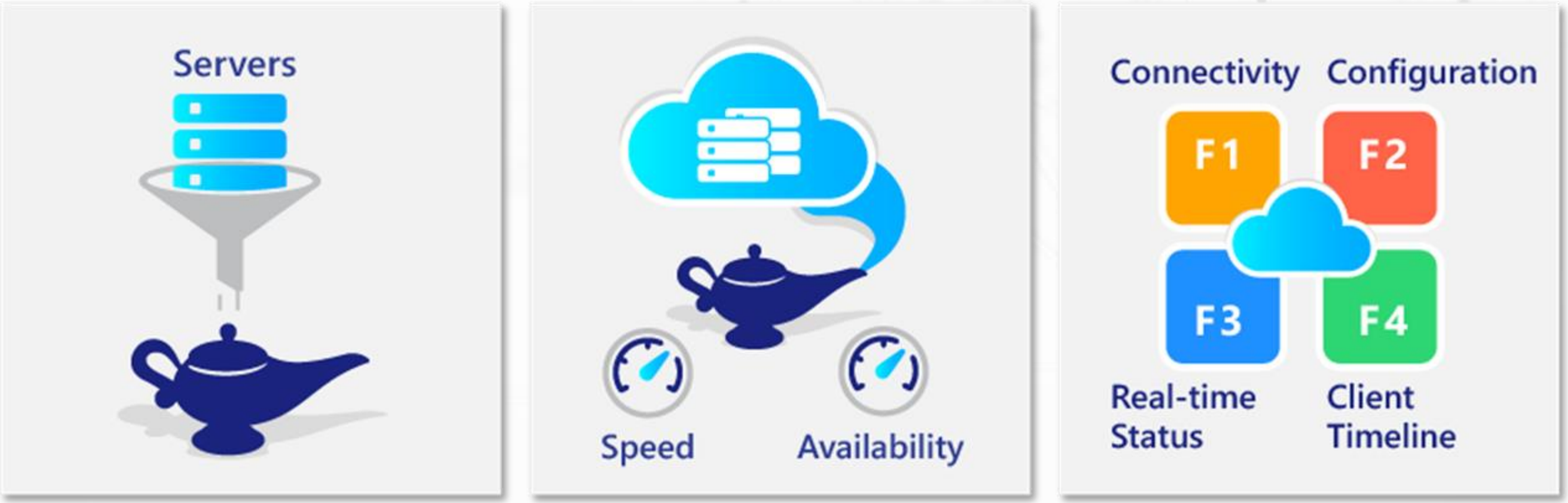
The AI-Driven Cloud for Smart Networking

EnGenius Cloud is built on top of the most advanced cloud computing technology. Scalable and AI-ready, the robust and dynamic cloud computing infrastructure helps you work smart on your network with important analytics and visualization tools.

Next-Gen Infrastructure

EnGenius Cloud utilizes an FaaS architecture which delivers uninterrupted cloud management regardless of platform utilization worldwide. The service-level agreement guarantees 99.99% availability for your network. Portal updates are rolled out in the background so that clients may continue to manage and monitor critical sites.

Serverless Backend of EnGenius Cloud



Servers are abstracted

Scaling is event-driven

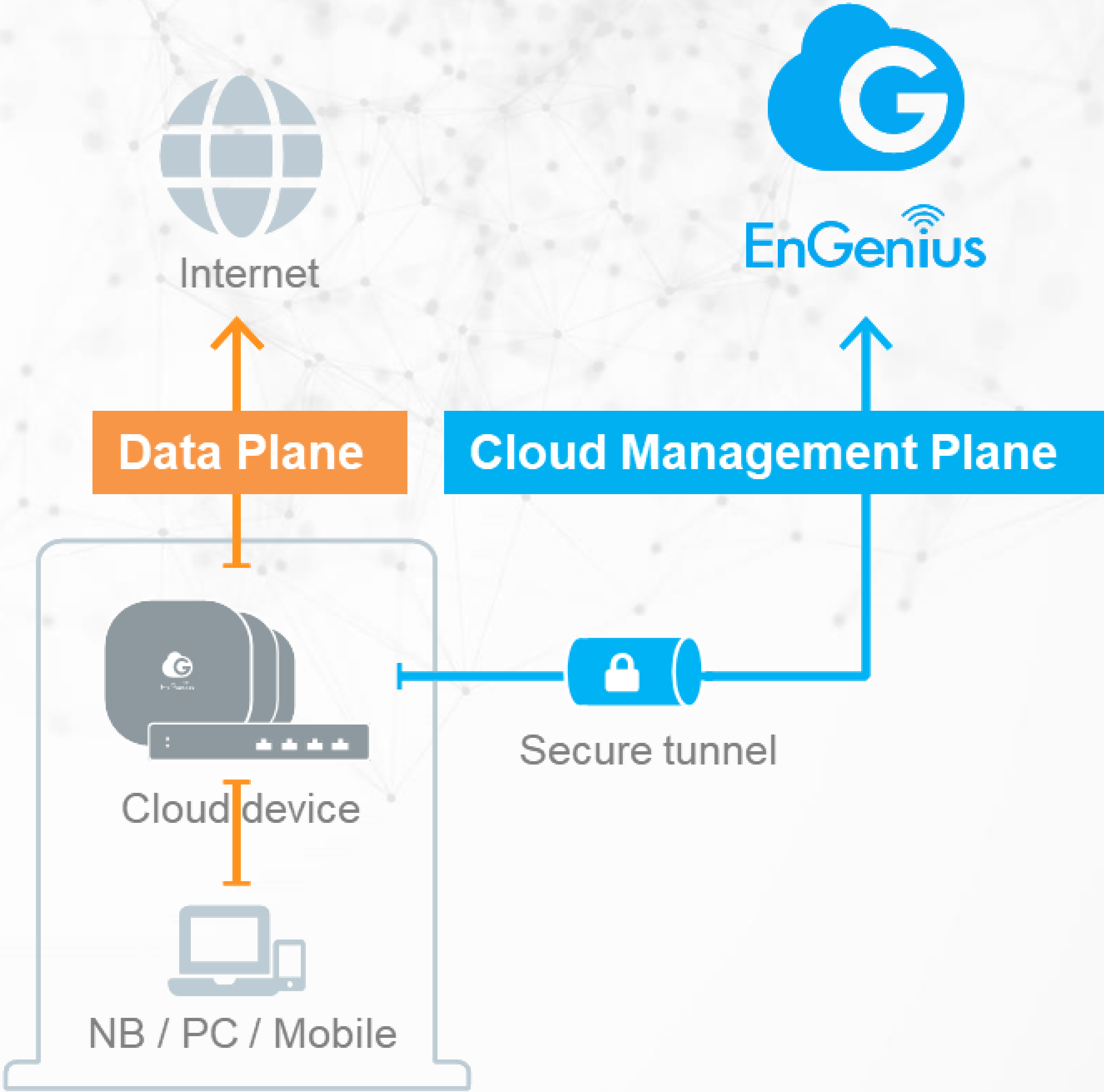
FaaS (Function-as-a-Service)

Secure and Committed to Privacy

EnGenius Cloud utilizes HTTPS for management of cloud devices.

To further increase security, MFA or multi-factor authentication is in place between the cloud devices and the Cloud. Whenever there is an exchange of data, verifications are initiated to prevent hackers getting into your network or to the Cloud.

We value client's privacy. With EnGenius Cloud, the type of information that goes to and from the Cloud portal are management and monitoring information of your hardware. Sensitive client data such as browsing history, passwords, and payment information are all kept on the client's local data plane.

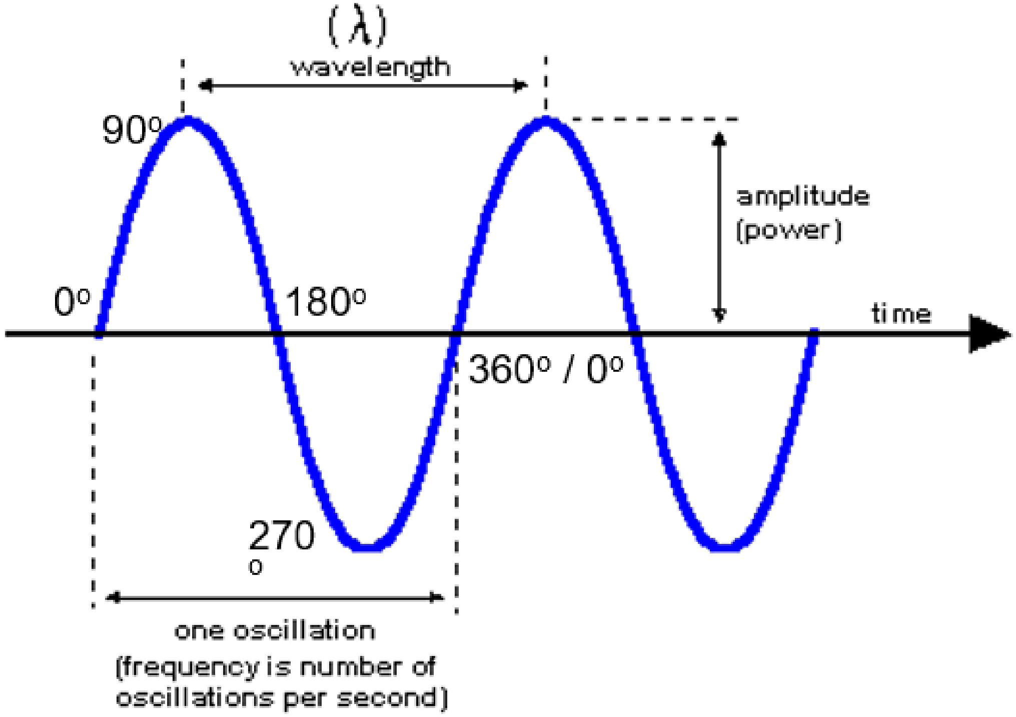


WLAN Fundamentals - topics

- RF Fundamentals
  - Electromagnetic Waves
  - Modulation
  - Unit of Measurement
  - Signal Degradation
  - Link Budget
  - Contention
  - Data Rate
- Wi-Fi technology overview
  - Standards and Regulations
  - Wi-Fi Technology Generations

RF Fundamentals- Electromagnetic Waves

- **Frequency f**: Number of periodic cycles traversed by an electromagnetic wave in one second. Measured in Hz (1/sec).
- **Wavelength λ**: Length of a single oscillation
- Frequency and wavelength have an inverse relationship, relative to the speed of light (c): f= c / λ

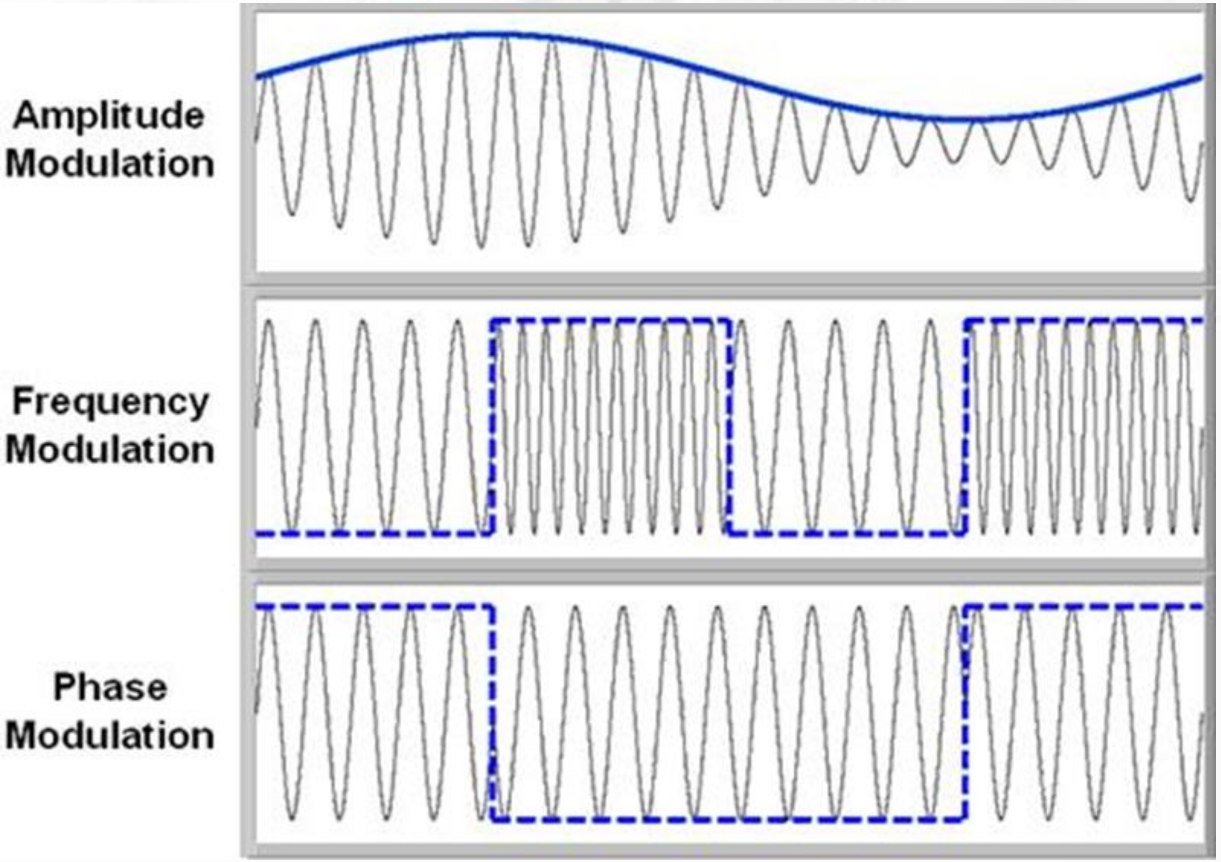


https://victoriastaffordapsychicinvestigation.files.wordpress.com/2012/02/wavelength-amplitude-power-time-oscillations-per-second-line-17m-wow-seti-the-idea-girl-says-youtube.gif

RF Fundamentals- Modulation

- Amplitude Modulation (AM): Change the amplitude (i.e. power) of the signal over time
- Frequency Modulation (FM): Change the frequency (i.e. wavelength) of the signal over time
- Phase Modulation (PM): Change the phase of the signal over time

In Wi-Fi, the list of channel (i.e. range of frequency) is fixed where different countries/regions have their own respective applicable channels. Wi-Fi utilizes both phase and amplitude modulation.



http://www.ni.com/cms/images/devzone/tut/dhall_analog_modulation.JPG

RF Fundamentals- Unit of Measurement - Decibels

Power levels in Wi-Fi: 1000 mW to 10^-9 mW

Convenient to use logarithms to characterize radio frequency power

- Exponents become multiplication
- Multiplication become addition
- Division becomes subtraction

Logarithms turn hard math problems into easy math problems (predate computers by ~400 years)

$$L_{dB} = 10log_{10}(\frac{P_0}{P_1})$$

$$P_1 = 10(\frac{L_{db}}{10})P_0$$

RF Fundamentals- Unit of Measurement - Types of Power Measurement

- dBm: Absolute measure of power in decibels (relative to milliwatts, where 0 dBm = 1 mW)
- dB: Relative comparison of two power values
- dBi: Relative gain of signal strength of an antenna (relative to a theoretical isotropic radiator

Law of 3 dB

- +3 dB = 2x power
- -3 dB = ½ power
- Examples:
  - 17 dBm = 50 mW
  - 20 dBm = 100 mW
  - 23 dBm = 200 mW

Law of 10 dB

- +10 dB = 10x power
- -10 dB = 0.1x power
- Examples:
  - 10 dBm = 10 mW
  - 20 dBm = 100 mW
  - 30 dBm = 1000 mW

RF Fundamentals- Signal Degradation - Thermal Noise

The background noise of the universe, under which no receiver can distinguish a modulated electromagnetic signal

$$N_{dBm} = 10\log_{10}(1000k_BT) + 10\log_{10}(\Delta f)$$

N_{dBm} = Thermal noise in dBm

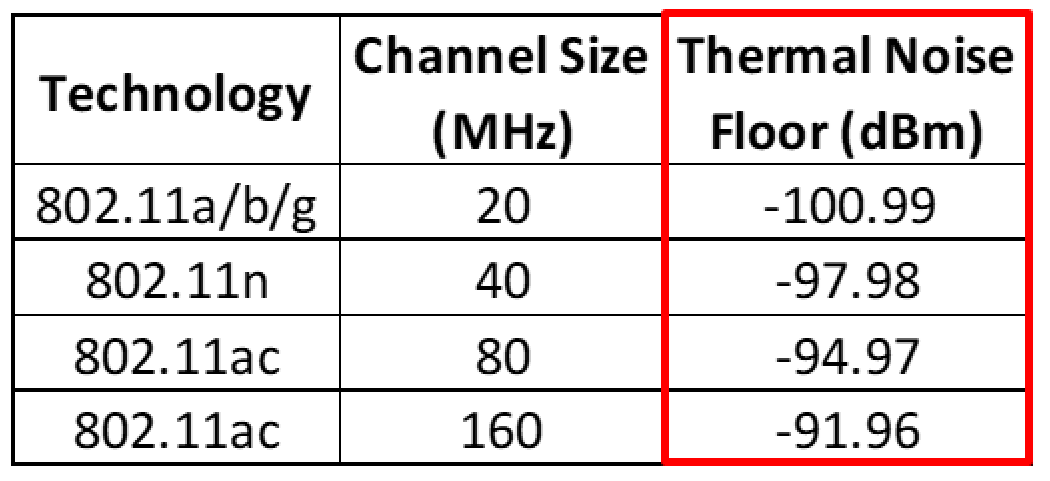
k_BT= Boltzmann constant

T = Temperature

Δf = Channel size

At room temperature:

$$N_{dBm} = 174.0 + 10\log_{10}(\Delta f)$$



Technology	Channel Size (MHz)	Thermal Noise Floor (dBm)
802.11a/b/g	20	-100.99
802.11n	40	-97.98
802.11ac	80	-94.97
802.11ac	160	-91.96

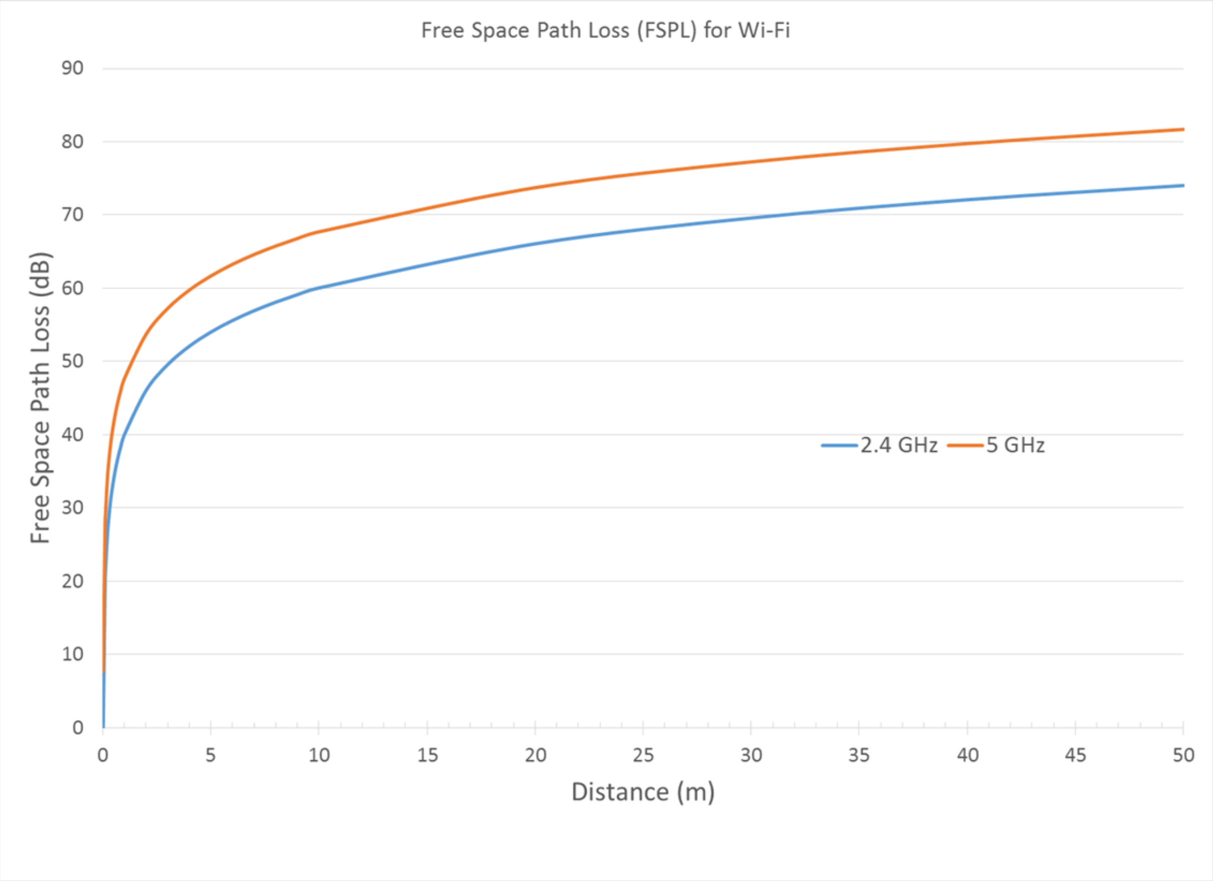
RF Fundamentals- Signal Degradation - Free Space Path Loss (FSPL)

The degradation of signal strength of an electromagnetic wave as it propagates through free space (inverse square law)

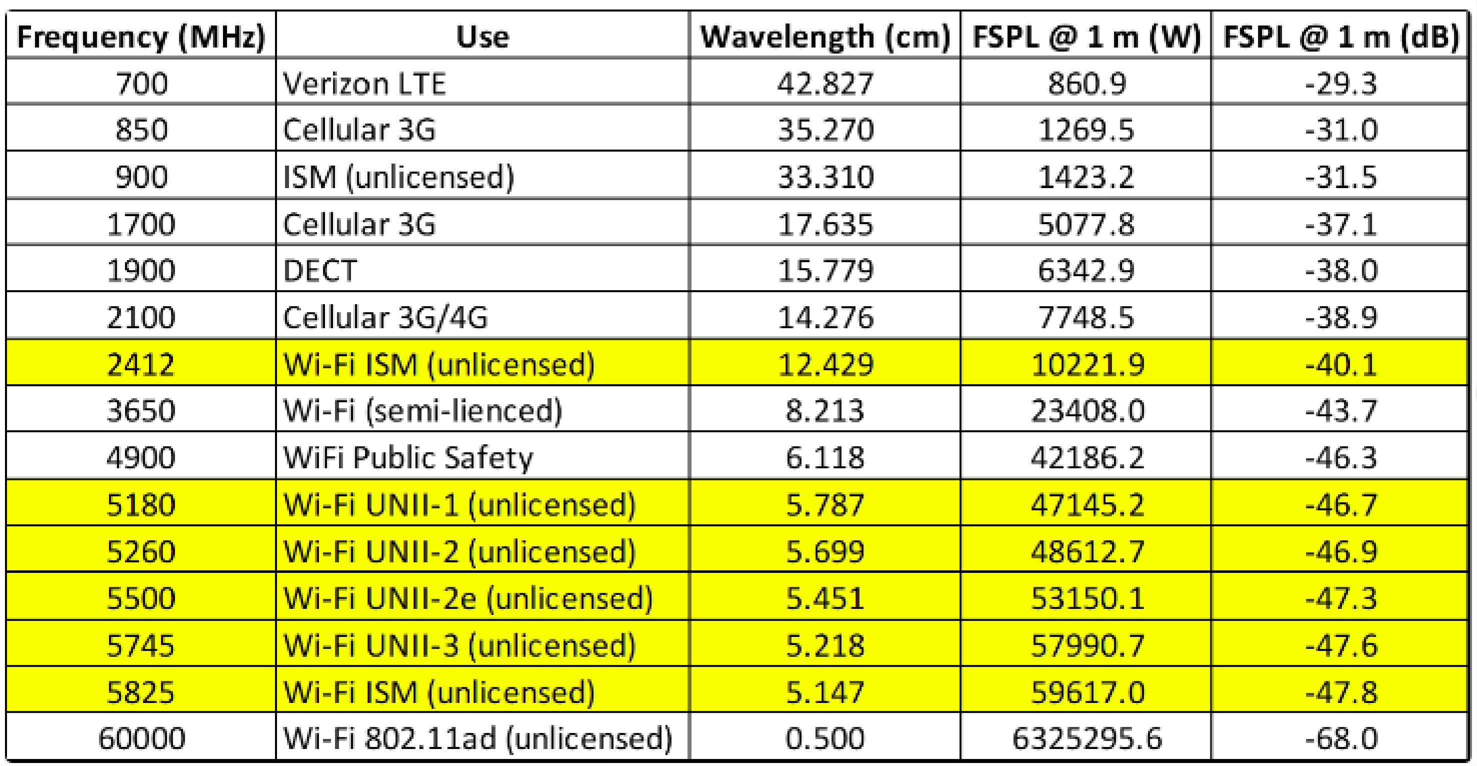
$$\mathrm{FSPL_W}=\left(\frac{4\pi d f}{c}\right)^2$$

$$\mathrm{FSPL_{dB}}= 20\log_{10}(d)+20\log_{10}(f) +20\log_{10}\left(\frac{4\pi}{c}\right)$$

FSPL is defined relative to the distance between a transmitter and receiver where both are using isotropic antennas (i.e. spherical signal patterns)



RF Fundamentals- Signal Degradation - FSPL @ 1 m



Frequency (MHz)	Use	Wavelength (cm)	FSPL @ 1 m (W)	FSPL @ 1 m (dB)
700	Verizon LTE	42.827	860.9	-29.3
850	Cellular 3G	35.270	1269.5	-31.0
900	ISM (unlicensed)	33.310	1423.2	-31.5
1700	Cellular 3G	17.635	5077.8	-37.1
1900	DECT	15.779	6342.9	-38.0
2100	Cellular 3G/4G	14.276	7748.5	-38.9
2412	Wi-Fi ISM (unlicensed)	12.429	10221.9	-40.1
3650	Wi-Fi (semi-lienced)	8.213	23408.0	-43.7
4900	WiFi Public Safety	6.118	42186.2	-46.3
5180	Wi-Fi UNII-1 (unlicensed)	5.787	47145.2	-46.7
5260	Wi-Fi UNII-2 (unlicensed)	5.699	48612.7	-46.9
5500	Wi-Fi UNII-2e (unlicensed)	5.451	53150.1	-47.3
5745	Wi-Fi UNII-3 (unlicensed)	5.218	57990.7	-47.6
5825	Wi-Fi ISM (unlicensed)	5.147	59617.0	-47.8
60000	Wi-Fi 802.11ad (unlicensed)	0.500	6325295.6	-68.0

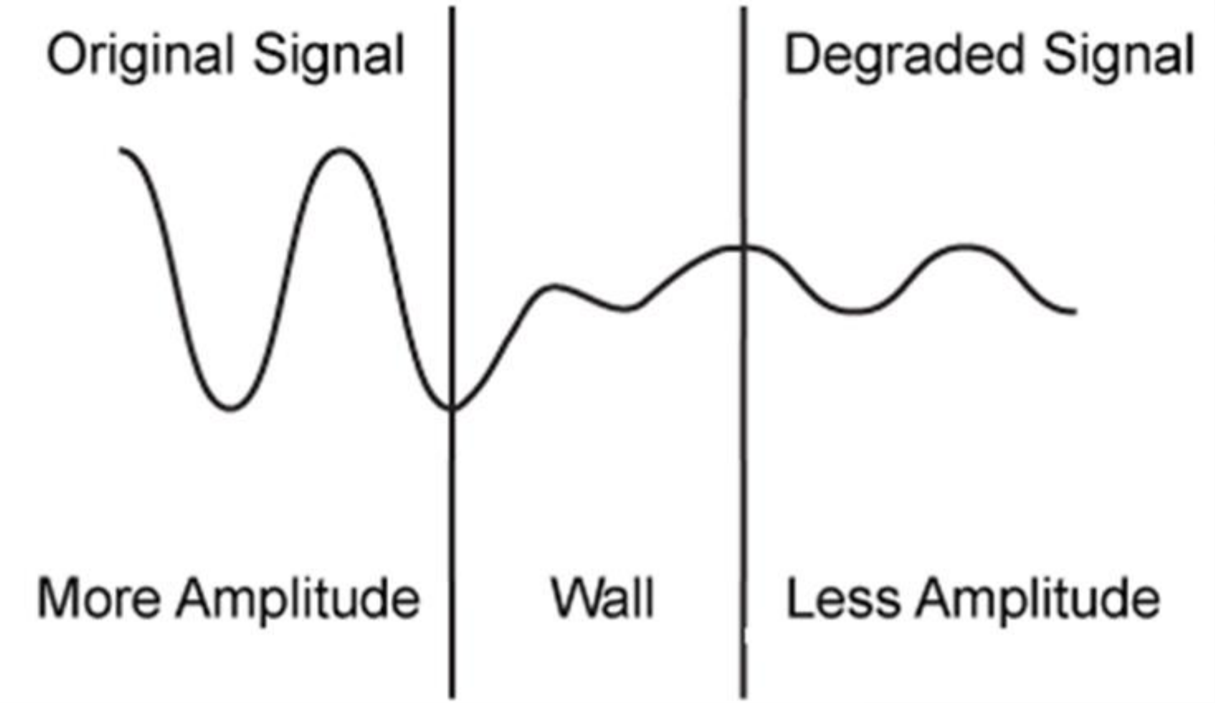
RF Fundamentals- Signal Degradation - Attenuation

Loss of an electromagnetic signal from interaction with objects in the environment

Function of the material type and the wavelength:

- **Absorption**: Energy absorbed by the material
- **Reflection**: Energy reflected by the material (creates multipath signals)

Lower frequency signals propagate through materials more easily (i.e. less loss) than higher frequency signals



RF Fundamentals- Signal Degradation - Typical material absorption and reflection

(!) These values are representative. Actual wall structures can vary dramatically. Where possible, losses through walls should be measured. Moisture content can also impact absorption.

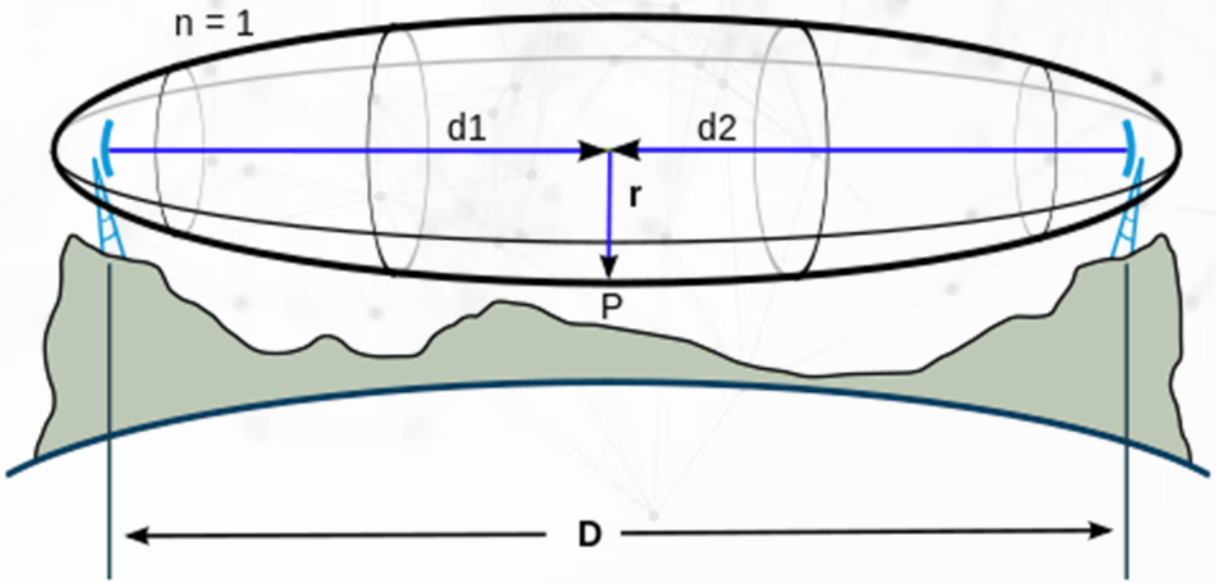
Building Material	2.4 GHz		5 GHz	
	Absorption	Reflection	Absorption	Reflection
Brick 3.5"	6 dB	6%	10 dB	13%
Brick 10"	10 dB	6%	25 dB	13%
Cubicle Divider	1 dB	12%	2 dB	0%
Concrete 8"	10 dB	40%	13 dB	30%
Concrete 18"	18 dB	40%	30 dB	30%
Concrete 27"	30 dB	40%	45 dB	30%
Drywall	3 dB	6%	6 dB	7%
Glass (interior)	3 dB	7%	6 dB	32%
Glass (exterior)	7 dB	7%	6 dB	32%
Glass (exterior coated)	13 dB	7%	20 dB	32%
Steel Fire Door 1.75"	13 dB	90%	25 dB	90%
Steel Fire Door 2.5"	19 dB	90%	32 dB	90%
Wood Door (hollow)	4 dB	12%	7 dB	0%
Wood Door (solid)	6 dB	2%	10 dB	3%

RF Fundamentals- Signal Degradation - Diffraction

Diffraction causes electromagnetic waves passing near an object to bend, even if not in the direct visual path. This effect can degrade the received signal by changing the phase.

Fresnel Zone

Area surrounding the line of sight that must remain clear of obstructions. Effect dictates the height at which each antenna for a point-to-(multi)point link must be mounted. Above 7 miles, earth curvature must also be taken into account.



https://upload.wikimedia.org/wikipedia/commons/thumb/5/5c/FresnelSVG1.svg/500px-FresnelSVG1.svg.png

RF Fundamentals- Signal Degradation - Fresnel Zone Calculation

$$R_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

R_n: Radius of nth Fresnel Zone (higher order Fresnel zones have significantly lower impact on the link – only concerned with 1st order)

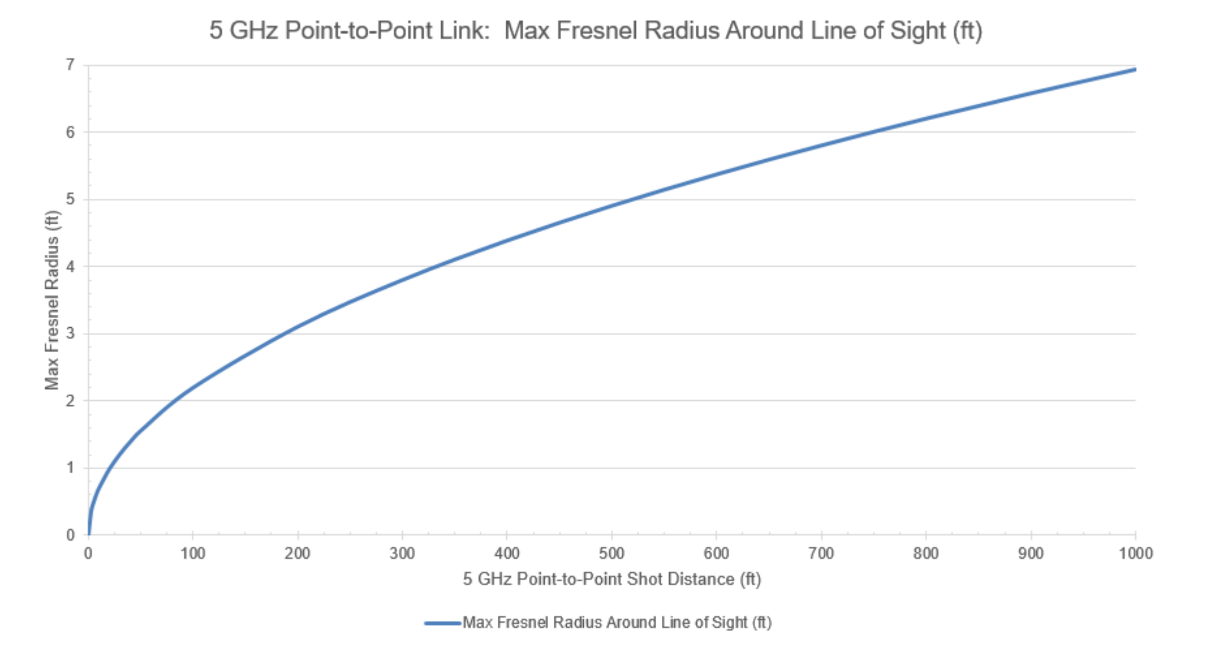
λ: Wavelength

D: Distance between two antennas.

$D=d_1+d_2$

d_1: Distance to given point from radio 1

d_2: Distance to given point from radio 2



$$R_{1max} = \frac{1}{2}\sqrt{\lambda D}$$

RF Fundamentals- Link Budget

The link budget is estimated based on the following factors:

- EIRP: Effective isotropic radiated power
  - (+) Transmitter power
  - (+) Transmitter antenna gain
  - (-) Transmitter antenna cable & connector losses
- Free space path loss
- Attenuation in path (e.g. walls, windows, etc.)
- Receiver antenna gain
- Receiver antenna cable / connector losses

Received Signal Strength Indicator (RSSI)

Measured signal strength at the receiver (client)

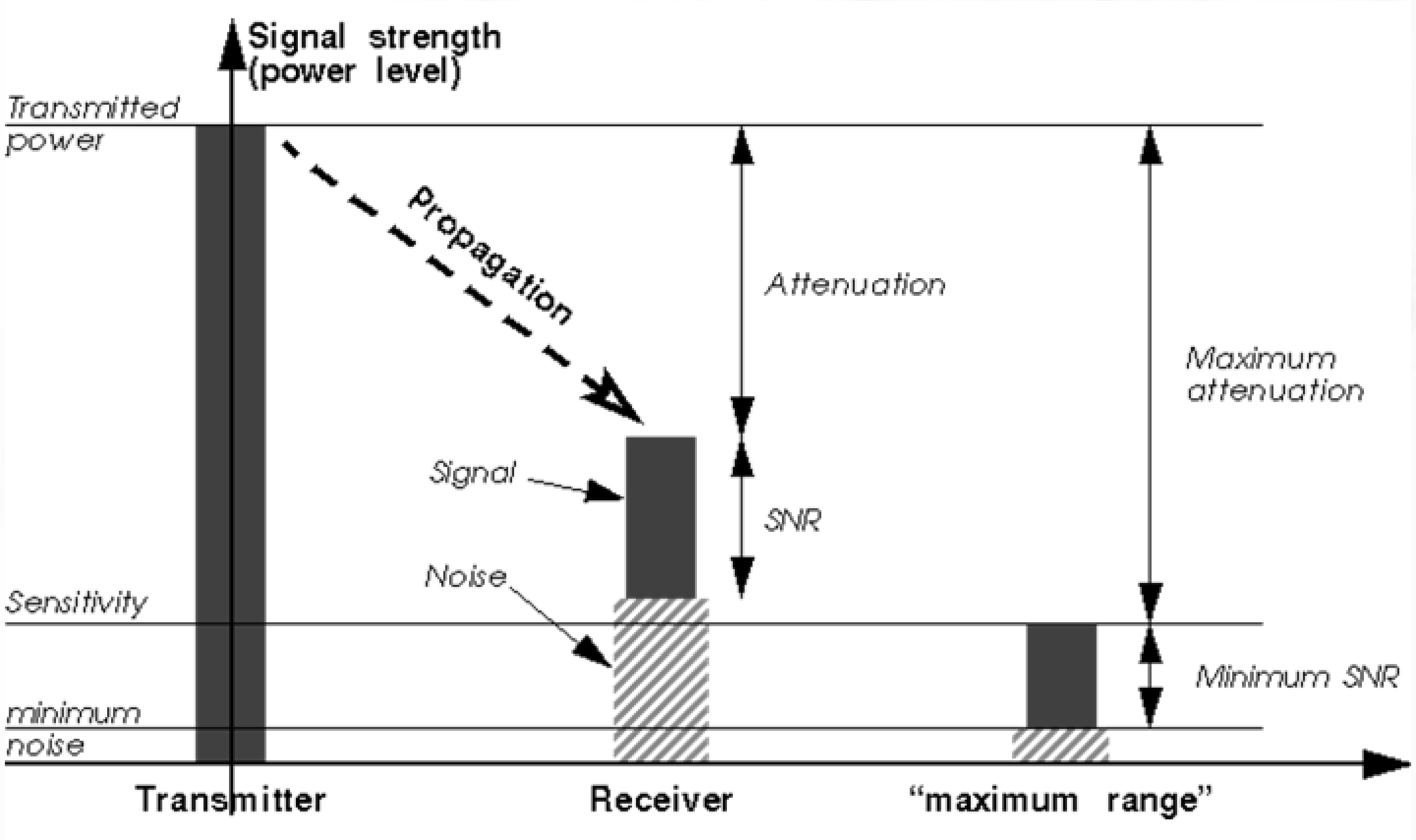
Receive Sensitivity

Minimum signal strength that the receiver can interpret a signal at a particular modulation

RF Fundamentals- Link Budget

Fade Margin / SNR

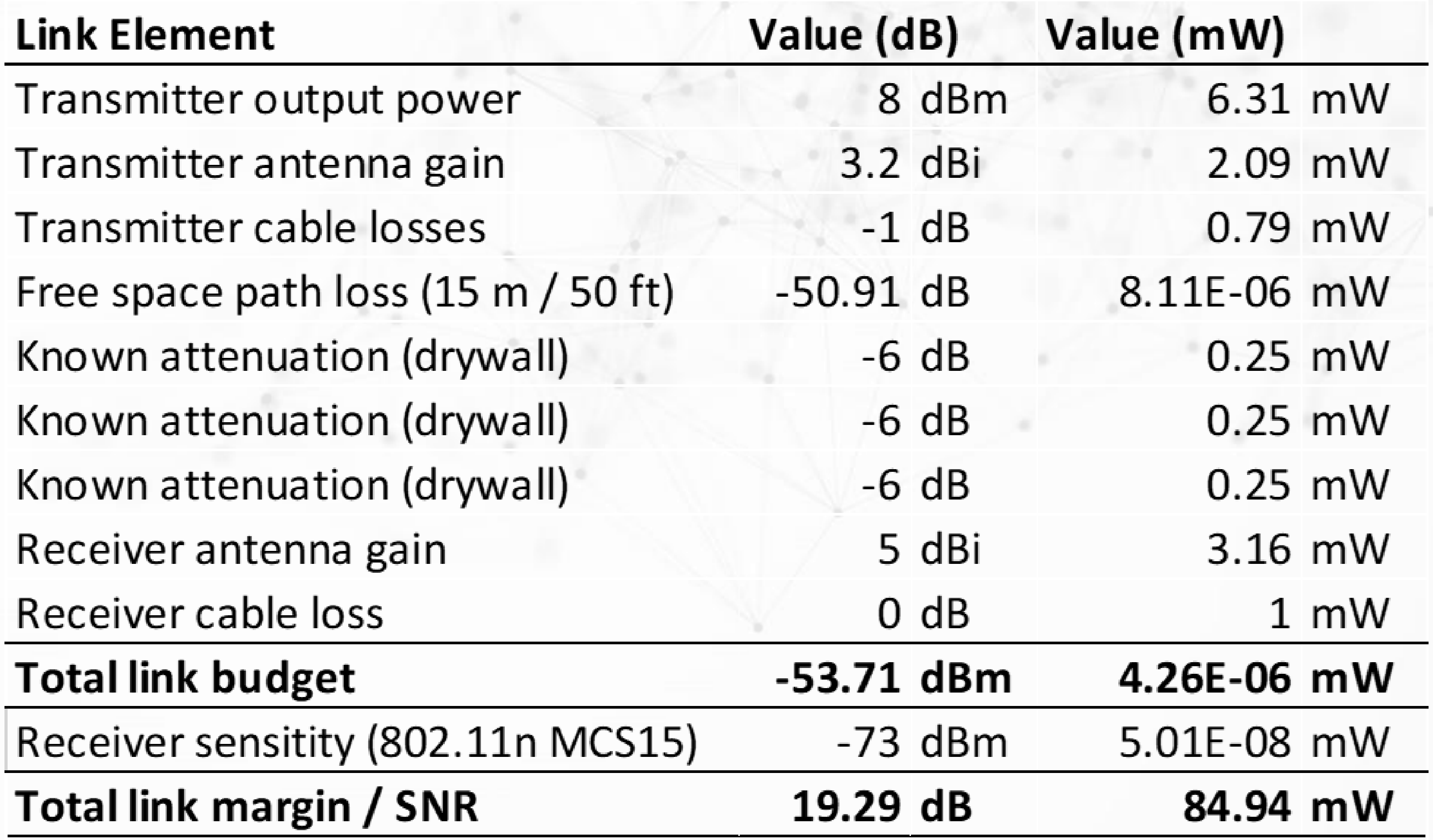
Difference between the link budget and the receive sensitivity (a.k.a. signal to noise ratio)



Signal to Noise Ratio (SNR)

RF Fundamentals- Link Budget example

- An iPhone communicating @ 5 GHz with ECW120 located 50 feet (15 m) away through three walls
- Good performance requires > 15 - 20 dB margin



Link Element	Value (dB)		Value (mW)	
Transmitter output power	8	dBm	6.31	mW
Transmitter antenna gain	3.2	dBi	2.09	mW
Transmitter cable losses	-1	dB	0.79	mW
Free space path loss (15 m / 50 ft)	-50.91	dB	8.11E-06	mW
Known attenuation (drywall)	-6	dB	0.25	mW
Known attenuation (drywall)	-6	dB	0.25	mW
Known attenuation (drywall)	-6	dB	0.25	mW
Receiver antenna gain	5	dBi	3.16	mW
Receiver cable loss	0	dB	1	mW
Total link budget	**-53.71**	**dBm**	**4.26E-06**	**mW**
Receiver sensitivity (802.11n MCS15)	-73	dBm	5.01E-08	mW
Total link margin / SNR	**19.29**	**dB**	**84.94**	**mW**

RF Fundamentals- Contention

Why is wired communication so much faster than wireless communication? Electrons on a wire and radio signals in air travel at the same speed (i.e. speed of light) but wired networks seem to get better throughput results vs wireless connections. The answer? Contention.

In any network, collision may occur when two or more devices transmit data at the same time.

On a wired network, there are separate wire pairs in Ethernet for transmit (Tx) and receive (Rx) communication. Due to this, Full Duplex mode can be used where wired network devices can both talk (Tx) and listed (Rx) simultaneously. When a collision occurs, a device:

- stops talking (Tx)
- waits until the medium is clear (Rx)
- and continues to talk (Tx) where it left off when it's clear

RF Fundamentals- Contention (2)

On wireless networks, the same medium is used for Tx and Rx communication; therefore, Half Duplex mode is used, which means that wireless network devices cannot transmit and receive on the medium at the same time. When collision occurs on the wireless network, the wireless station is unaware. Interference can also occur on the wireless network when the receiver hears more than one transmission on the same channel at the same time.

To avoid collisions on wireless networks:

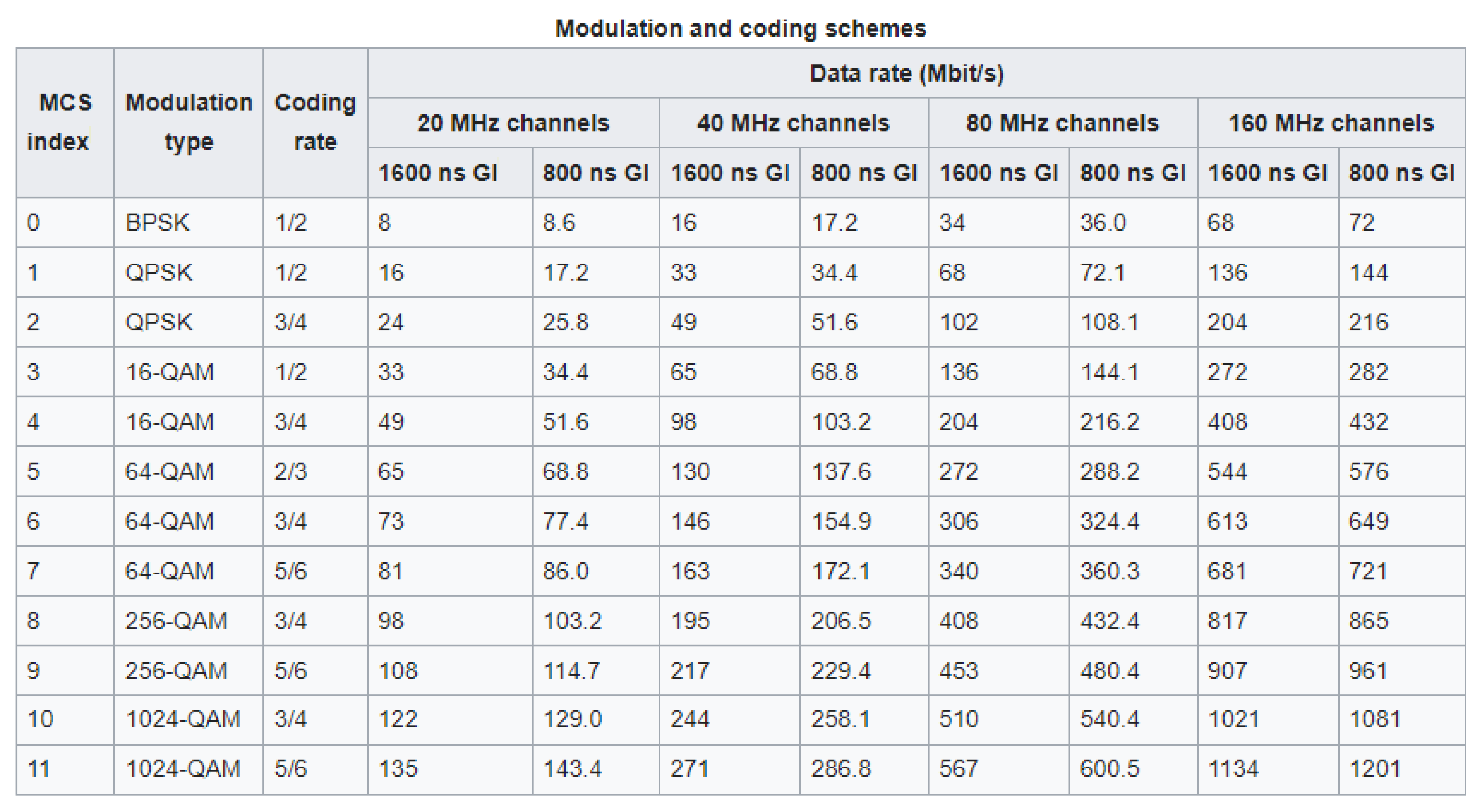
- a device need to contend for/reserve time to use the medium
- transmit information when the medium is yours (Tx)
- receive an acknowledgement (ACK) from the intended receiver that the transmission was successful (Rx)
- repeat the process when no ACK is received

RF Fundamentals- Data rate

The data rate defines the connection or link-speed at a given time. The maximum attainable data rate highly depends on the AP, wireless adapter of connecting device, and RSSI to name a few.

Every wireless generation has its own set of attainable data rates.

(!) A common misconception is that data rates equate to the actual throughput of the wireless connection. Due to the nature of Wi-Fi, data rates tend to provide information of the link-speed rather than the actual throughput.



Modulation and coding schemes

MCS index	Modulation type	Coding rate	Data rate (Mbit/s)							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	8	8.6	16	17.2	34	36.0	68	72
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86.0	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129.0	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

Wi-Fi Standards and Regulations - Regulatory Bodies

Depending on your country/region, your local government may be following regulations from the Federal Communications Commission (FCC) or Conformitè Europëenne (CE) in which both:

- Regulate interstate and international communications by radio, television, wire, satellite, and cable (collaborates with similar agencies in various countries)
- Allocate and enforce rules for use of all radio spectrum
- Spectrum Types:
    - Licensed: A single organization pays to use particular sections of spectrum in a geographic area. Violators can be fined.
    - Unlicensed: Anyone can use the spectrum as long as they meet requirements on maximum power, interference handling, and other usage cautions. Violators can be fined.

Wi-Fi Alliance

A Conglomeration of over 350 access point and client device manufacturers who coined and marketed the term “Wi-Fi”. The Wi-Fi Alliance encourages interoperability of Wi-Fi devices between vendors.

They are also responsible for establishing and conducting standardized testing for critical standards such as:

- Wi-Fi Multimedia (WMM): Quality of Service (QoS) [802.11e]
- Wi-Fi Multimedia Power Save (WMM-PS): Power saving technology for client devices
- Wi-Fi Protected Access (WPA/WPA2): Security [802.11i]
- Wi-Fi Voice Personal / Enterprise: VoWiFi applications [802.11k, 802.11r]

Telecommunication Standards Organizations

The **European Telecommunications Standards Institute** (ETSI) **and Institute of Electrical and Electronics Engineers** (IEEE) set many telecommunication standards.

Many Wi-Fi alliance members joined the IEEE working groups to establish Wi-Fi as an IEEE standard.

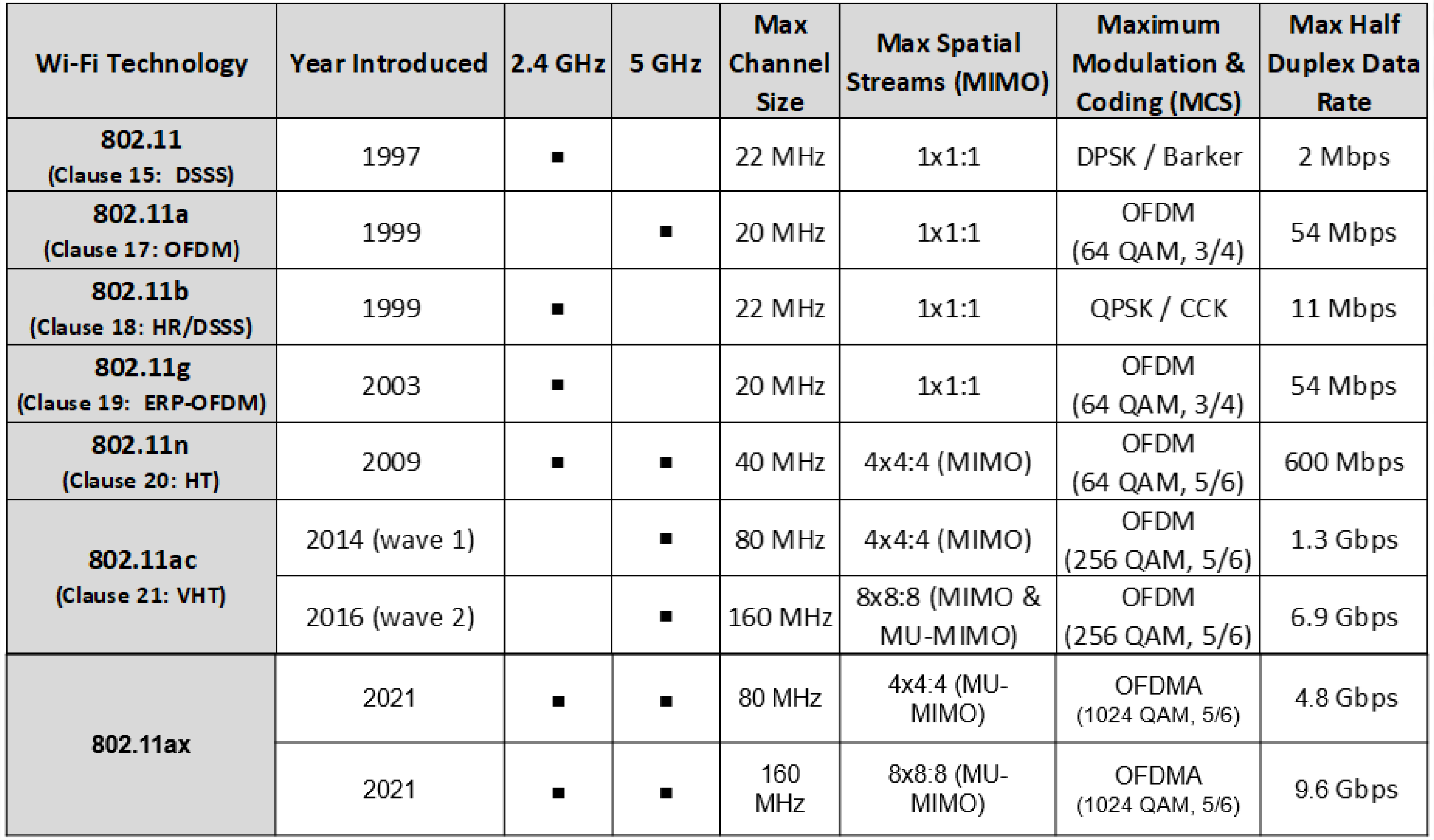
ETSI is a European Standards Organization (ESO). ETSI has special role in Europe. It includes supporting European regulations and legislation through the creation of Harmonized European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

Because of this many Wi-Fi alliance members also joined the ETSI working groups to allow Wi-Fi in Europe.

In some cases, laws and/or rules needed to be changed to allow the use of new standards.

A recent example: The Wi-Fi (6E) use of part of the 6 GHz band was only possible after the regulatory bodies (the CE partially and the FCC fully) opened these bands up for this use by Wi-Fi in Europe and the USA, respectively.

Wi-Fi Technology Generations - History



Wi-Fi Technology	Year Introduced	2.4 GHz	5 GHz	Max Channel Size	Max Spatial Streams (MIMO)	Maximum Modulation & Coding (MCS)	Max Half Duplex Data Rate
802.11 **(Clause 15: DSSS)**	1997	■		22 MHz	1x1:1	DPSK / Barker	2 Mbps
802.11a **(Clause 17: OFDM)**	1999		■	20 MHz	1x1:1	OFDM (64 QAM, 3/4)	54 Mbps
802.11b **(Clause 18: HR/DSSS)**	1999	■		22 MHz	1x1:1	QPSK / CCK	11 Mbps
802.11g **(Clause 19: ERP-OFDM)**	2003	■		20 MHz	1x1:1	OFDM (64 QAM, 3/4)	54 Mbps
802.11n **(Clause 20: HT)**	2009	■	■	40 MHz	4x4:4 (MIMO)	OFDM (64 QAM, 5/6)	600 Mbps
802.11ac **(Clause 21: VHT)**	2014 (wave 1)		■	80 MHz	4x4:4 (MIMO)	OFDM (256 QAM, 5/6)	1.3 Gbps
	2016 (wave 2)		■	160 MHz	8x8:8 (MIMO & MU-MIMO)	OFDM (256 QAM, 5/6)	6.9 Gbps
802.11ax	2021	■	■	80 MHz	4x4:4 (MU-MIMO)	OFDMA (1024 QAM, 5/6)	4.8 Gbps
	2021	■	■	160 MHz	8x8:8 (MU-MIMO)	OFDMA (1024 QAM, 5/6)	9.6 Gbps

Wi-Fi Technology Generations - History

Wi-Fi 4 - 802.11n [2.4 GHz and 5 GHz]

- 40 MHz channels on 5 GHz
- MIMO (2x2, 3x3, or **4x4**)

Wi-Fi 5 - 802.11ac Wave 1 [5 GHz]

- 80 MHz channels on 5 GHz (>2x throughput) Suitable for low / medium density deployments
- New MCS mode: 256 QAM (33% throughput) Requires extremely strong signal / good SNR
- Newer chipsets: better 802.11n device performance: 802.11n 2.4GHz 256-QAM vs 64-QAM (Wi-Fi 4)

Wi-Fi 5 - 802.11ac Wave 2 [5 GHz]

- MU-MIMO (4x4:4) Effective only in high-density environments
- 160 MHz channels on 5 GHz Not suitable for multi-AP deployments

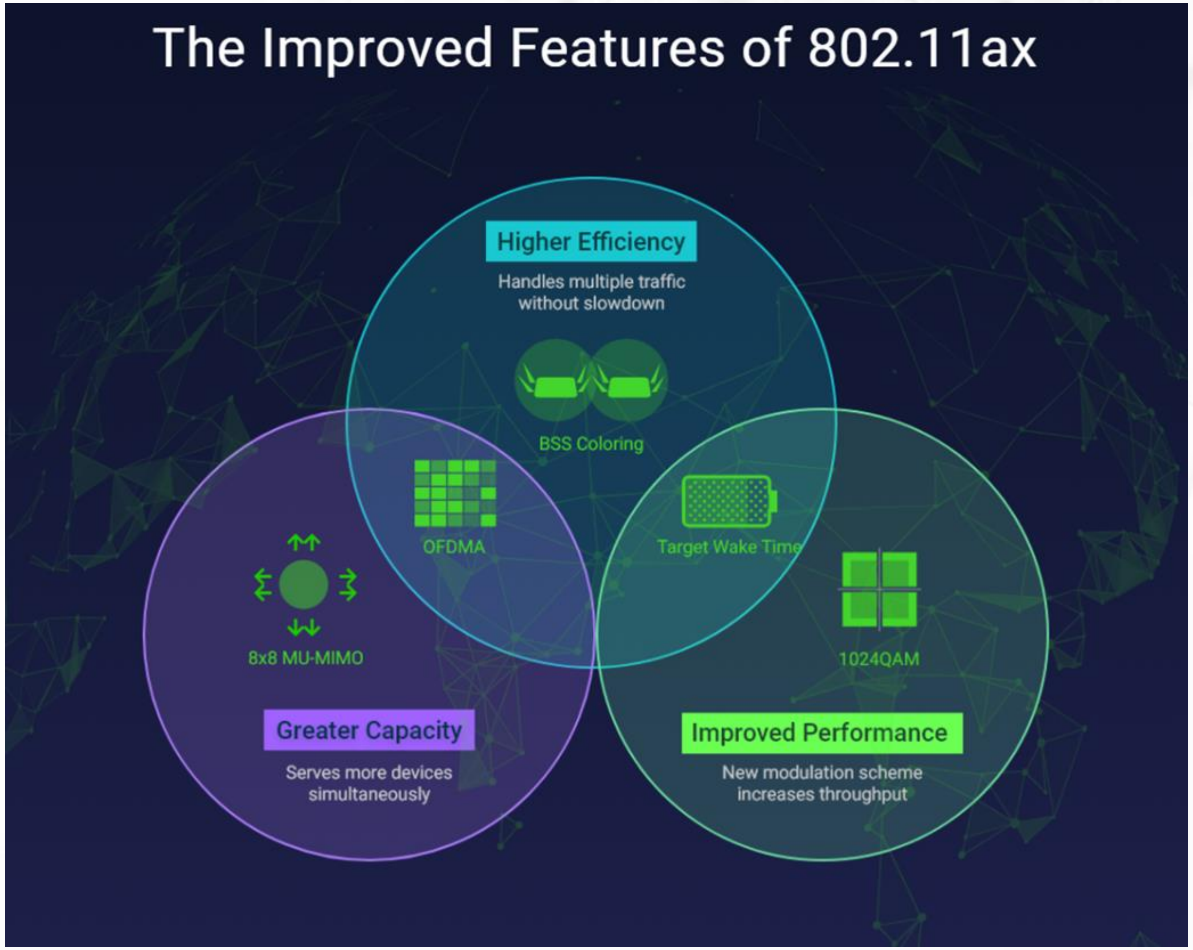
Wi-Fi 6 - 802.11ax [2.4 GHz and 5 GHz]

- MU-MIMO (8x8:8) Effective only in high-density environments
- OFDMA Improves concurrent traffic, reduces latency, and increases efficiency
- New MCS mode: 1024 QAM Increases throughput and capacity by 25%

Wi-Fi 6E [6 GHz]

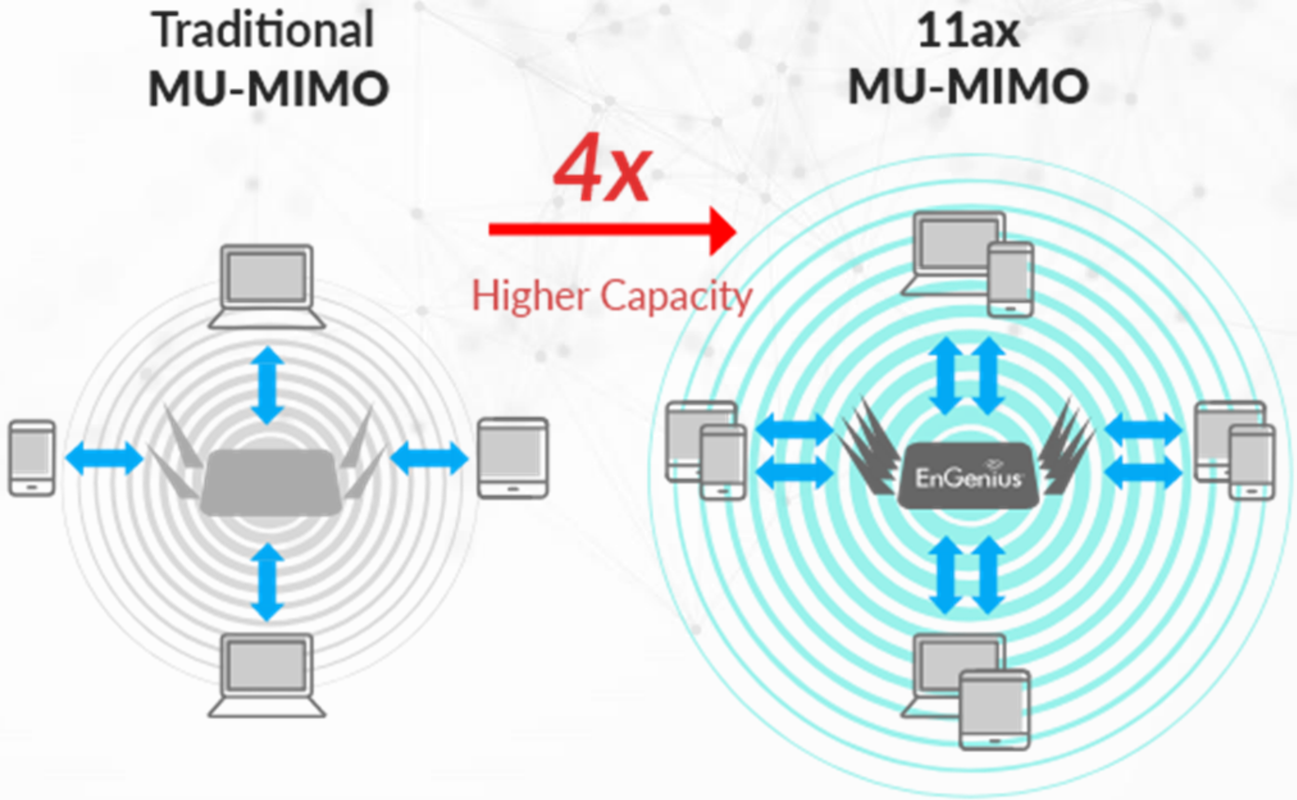
Wi-Fi 6 - 802.11ax

Wi-Fi 6 is a huge leap in WLAN technology as it not only increases the connectivity bandwidth over the previous generation, but also greatly enhances wireless network efficiency.


The Improved Features of 802.11ax
Higher Efficiency
Handles multiple traffic without slowdown
BSS Coloring
OFDMA
Target Wake Time
8x8 MU-MIMO
1024QAM
Greater Capacity
Serves more devices simultaneously
Improved Performance
New modulation scheme increases throughput

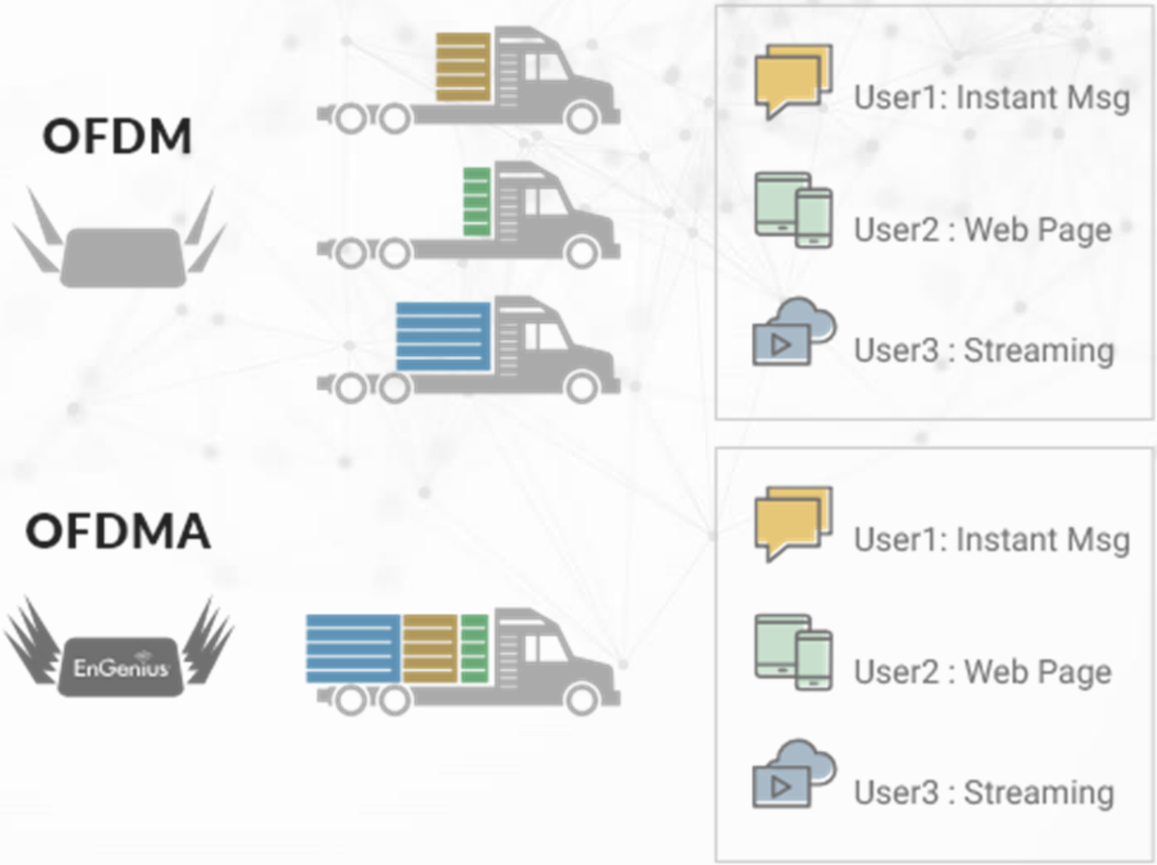
Wi-Fi 6 - 802.11ax - MU-MIMO Built-in for Both Download and Upload Links

11ax access points with 8x8 MU-MIMO in Uplink and downlink increase 4x in median throughputs in dense scenarios compared to traditional MU-MIMO



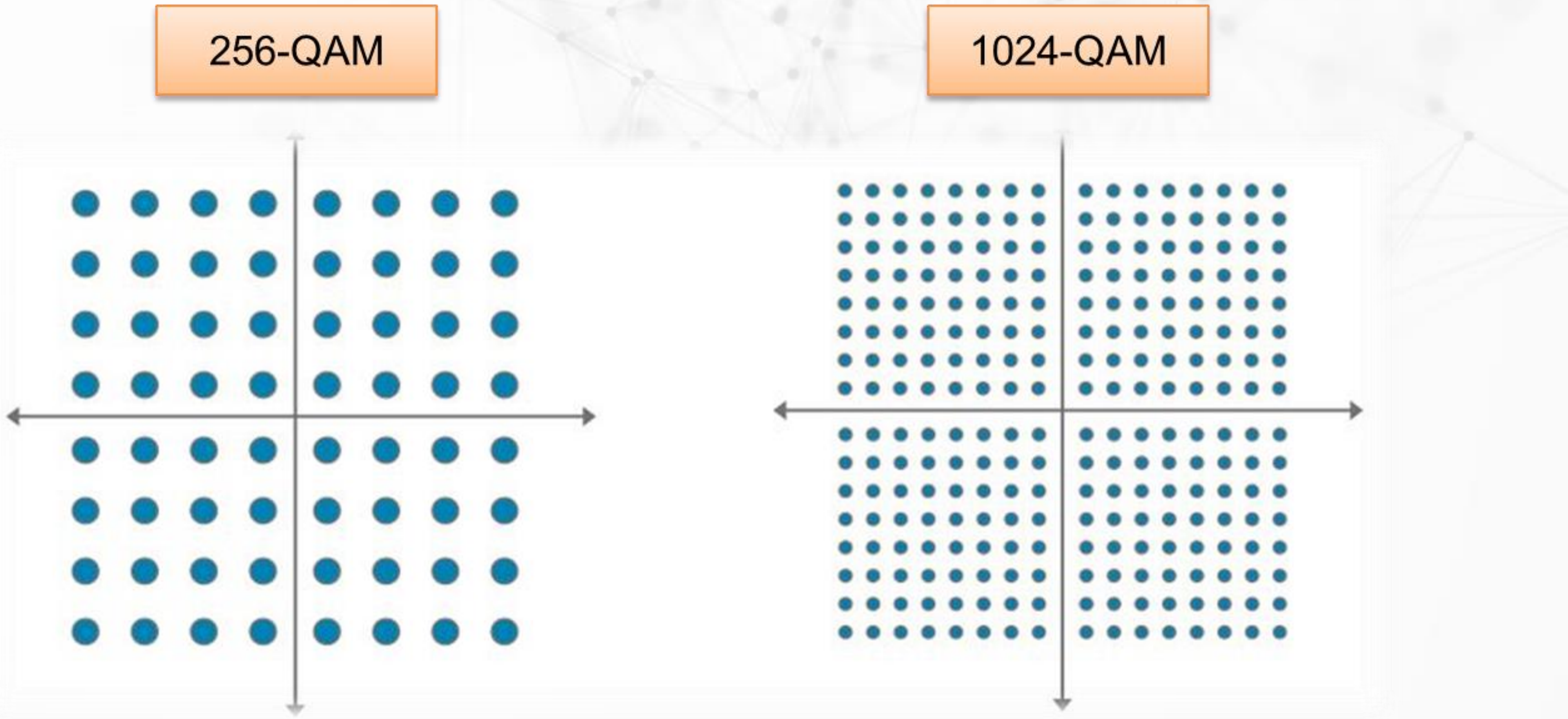
Wi-Fi 6 - 802.11ax - Advance Coding - OFDMA

11ax adopts OFDMA to allows multiple users with varying bandwidth needs to be served simultaneously. It results in fixed overhead payload size, reduced latency, and increased efficiency.



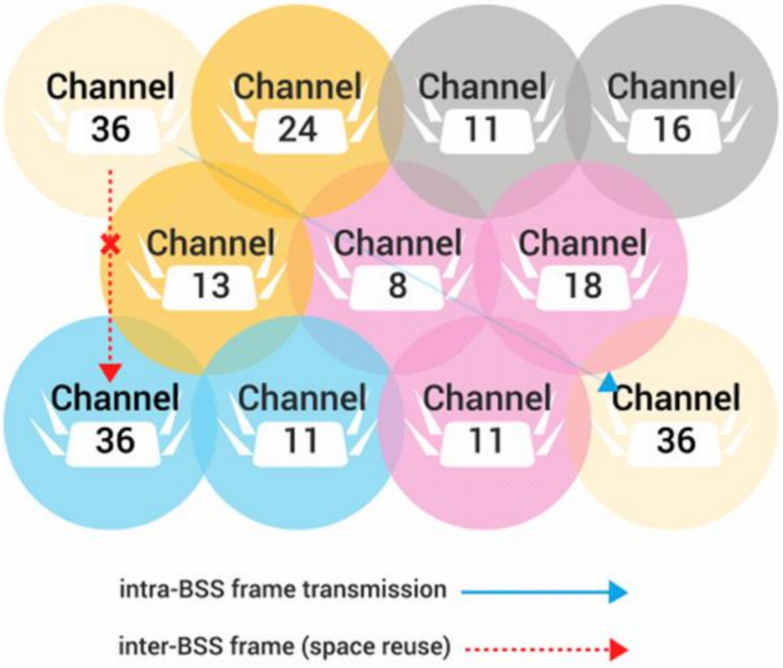
Wi-Fi 6 - 802.11ax - 1024-QAM to Enhance Connection Speed

11ax comes with a higher modulation scheme of 1024 QAM, which translates to better throughput and 25% higher capacity than traditional modulation scheme.



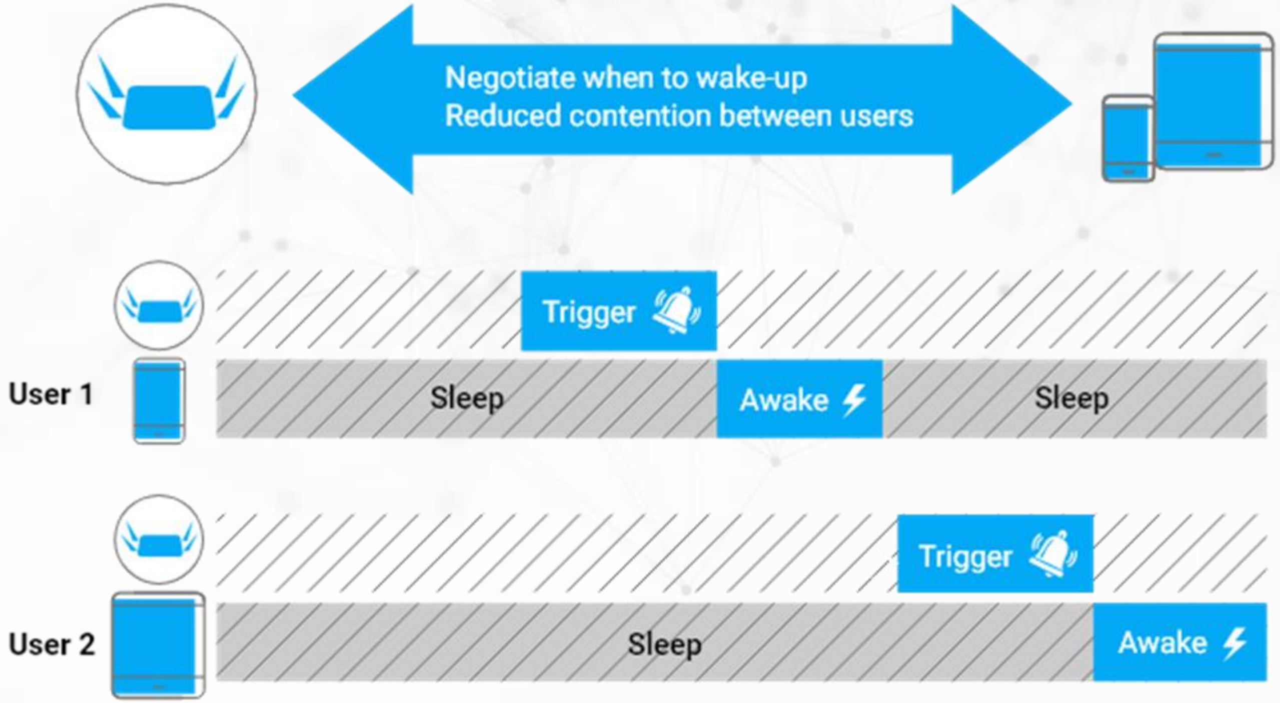
Wi-Fi 6 - 802.11ax - BSS Coloring to Reduce Co-channel Interference

802.11ax features BSS coloring which tags frames with a "color" to differentiate between adjacent basic service sets to reduce waiting time and lessen contention. If they have the same color, this is called an intra-BSS frame transmission. Without BSS coloring, only one radio can transmit at a time, and if clients "hear" transmissions from other clients, this results to co-channel interference.



Wi-Fi 6 - 802.11ax - Target wake time (TWT) saves the battery life of devices

The target wake time feature lets devices keep a radio receiver sleeping and wake it up as needed to receive periodic transmissions from an access point. The result is significant power-saving for battery-powered devices.



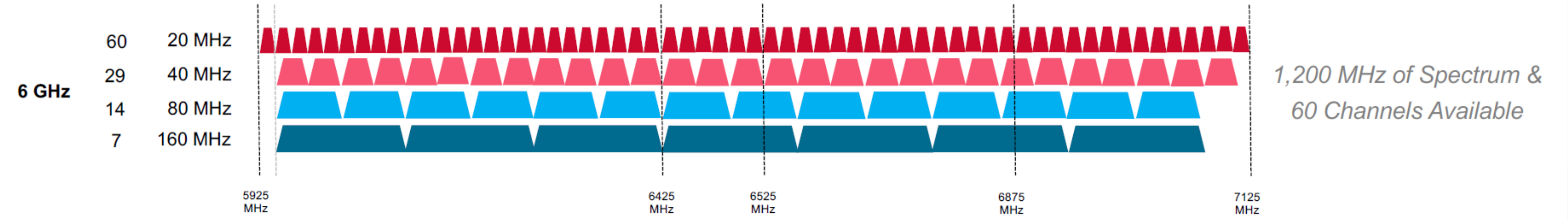
Wi-Fi 6 - 802.11ax - Growth of Wi-Fi Capabilities

How is Wi-Fi able to expand its capabilities from one generation to the next when the law of physics holds it back? The answer is Mathematics.

- Sufficiently complex algorithms running on sufficiently capable computer processors can "bend" physics
- New techniques to squeeze additional performance
    - Multiple streams and beam forming to boost signal strength
    - More sophisticated modulation & coding techniques
- Each generation: increase complexity
    - Increased sensitivity and fragility
    - Wi-Fi design becomes increasingly more important

Wi-Fi 6E – 6 GHz

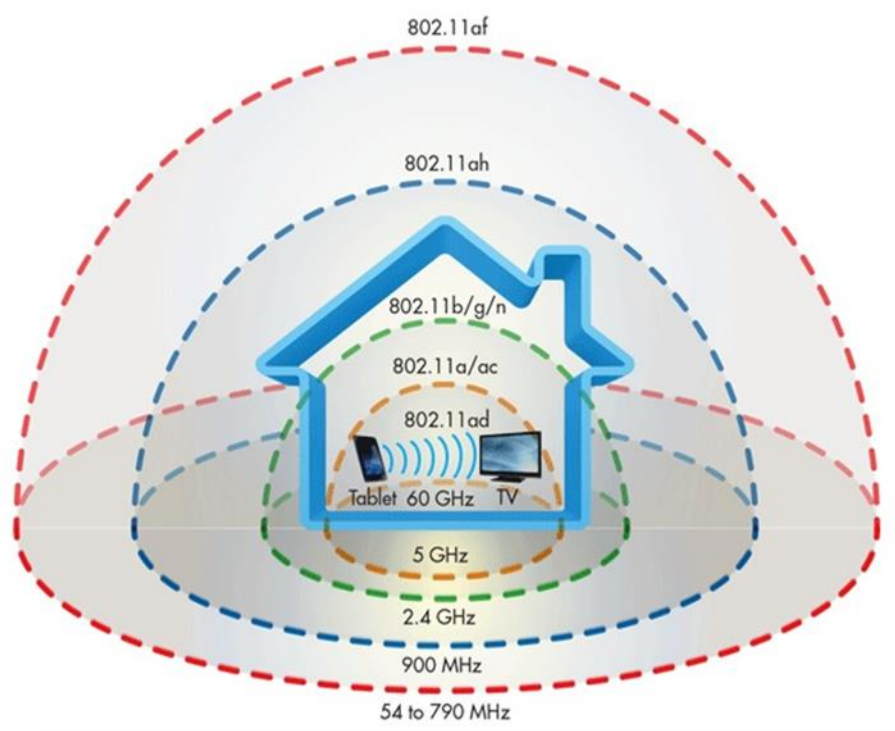
- Expansion of Wi-Fi 6 which runs on 6 GHz frequency
- Available frequencies differ per region



1,200 MHz of Spectrum & 60 Channels Available

Wi-Fi 6 - 802.11ax - What's on the Horizon?

- WiGig: 802.11ad
    - 60 GHz
    - Single room
    - Ultra high bandwidth
    - Target: Media Centers
- HaLow: 802.11ah
    - 900 MHz
    - Good penetration
    - Low bandwidth
    - Target: IoT
- White-Fi: 802.11af
    - 54-790 MHz (VHF/UHF)
    - Good penetration
    - Moderate bandwidth
    - Target: IoT, webcams



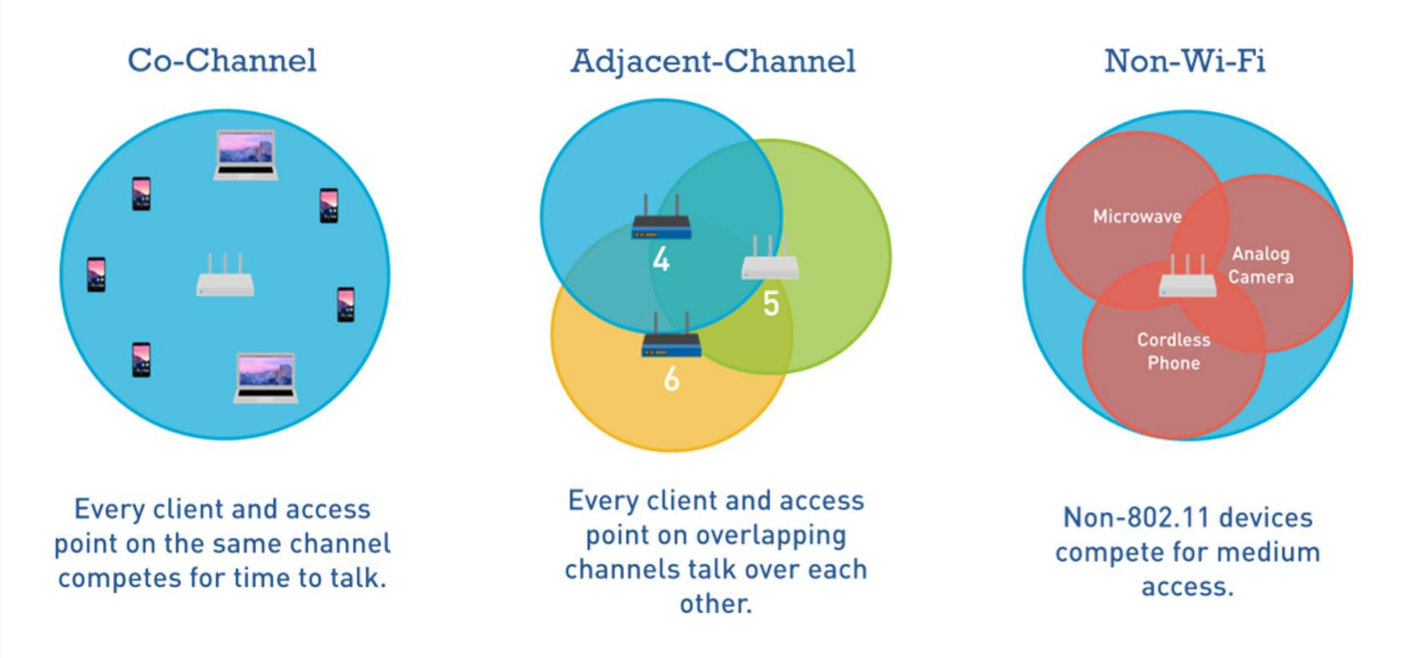
WLAN planning and design - topics

- Wi-Fi interference
- Site survey
- Wi-Fi heat map
- Channel planning

Wi-Fi interference

Interference is one of the most common root cause of wireless issues and yet it is often overlooked.

Interference can come from your own devices or 3rd party devices broadcasting on the same or adjacent channel.



Every client and access point on the same channel competes for time to talk.

Every client and access point on overlapping channels talk over each other.

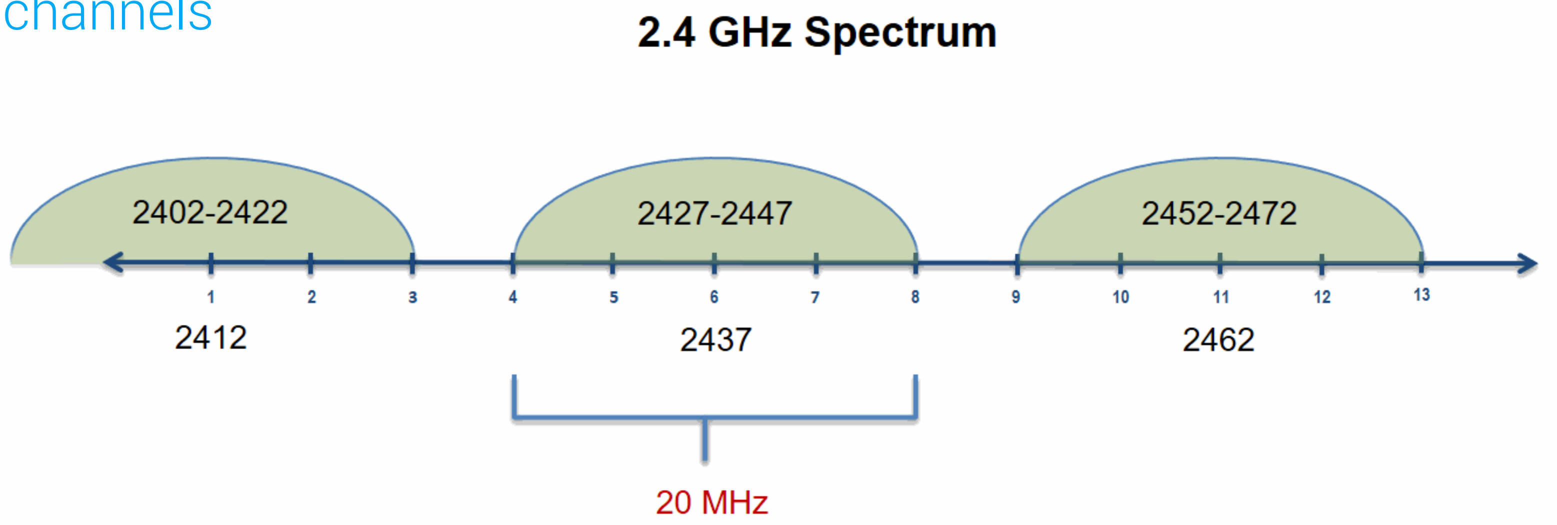
Non-802.11 devices compete for medium access.

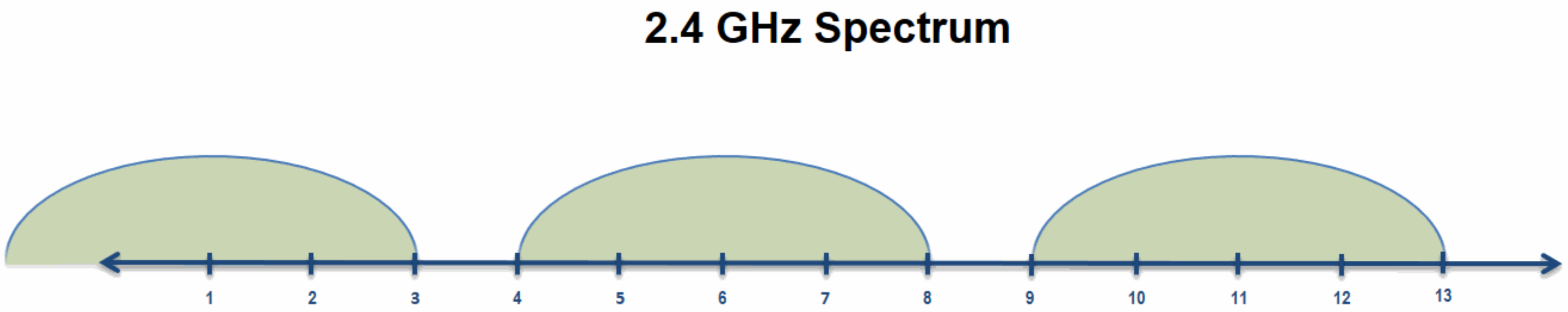
Wi-Fi interference - 2.4 GHz Wi-Fi spectrum

Although there is a channel spacing of 5 MHz in between channels on the 2.4 GHz spectrum, the minimum channel width is generally 20 MHz. This means that each channel spans across multiple frequencies.

Wi-Fi interference – Overlapping channels

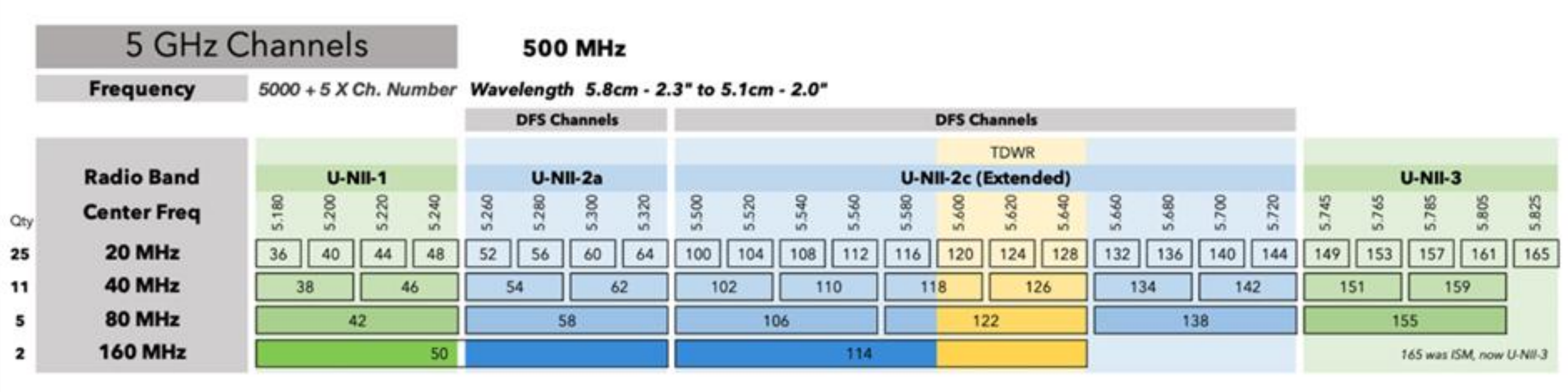
Interference occurs when two or more channels overlap, either on the same channel, or through adjacent channels.





Wi-Fi interference

The 5 GHz spectrum has more channel options. And are spaced apart so that no two channels are overlapping when using 20 MHz channel width. But you have to be aware of DFS channels in your deployment.



5 GHz Channels

500 MHz

Frequency *5000 + 5 X Ch. Number* **Wavelength 5.8cm - 2.3" to 5.1cm - 2.0"**

						DFS Channels				DFS Channels																
															TDWR											
	Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Qty	Center Freq	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
25	20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
11	40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
5	80 MHz	42				58				106				122				138				155				
2	160 MHz	50								114												*165 was ISM, now U-NII-3*				

DFS - Dynamic Frequency Selection

DFS channels prioritize specific channels for radar and weather equipment. These channels will vary per country. When an AP detects a broadcast from these devices, the AP may standby between 1-10 mins and/or switch to a different channel. During this period, client devices will not be able to connect to the AP.

Zero-Wait DFS

To circumvent DFS-incurred downtimes, Zero-Wait DFS will seamlessly change the channel of the AP upon detecting a radar broadcast nearby. This will allow the AP to skip the 1-10 min wait in selecting or switching channels, thus reducing downtime

Site Survey

A proper pre-deployment site survey goes a long way in terms of ensuring good coverage and channel planning to avoid interference amongst your deployed APs. This is usually done during ocular inspection or site visit.

There are a couple of things to take note of in doing a site survey:

- When using a PC/Mac, set aside a buffer for the RSSI to account for lower Tx power devices such as mobile phones and Ultrabook's. I.e. If you get -75 dBm on a PC, target about +5 dBm more.
- -75 dBm is about on the borderline between good and unreliable client connection, environmental factors and the performance of the wireless adapter on the client device will also affect this. -65 dBm is the recommended ceiling target if the environment requires VoIP services.
- In a multi-AP deployment, the distance between APs is determined based on the RSSI reading in between. There needs to be an overlap of wireless coverage to minimize downtime when transitioning to another access point. In Fast Roaming enabled environments, the APs are required to be able to "hear" each other.

The RSSI level can be controlled, by shifting the position of the AP, or by adjusting the APs transmit power. The Tx power of a device is directly proportional to the RSSI level and coverage.

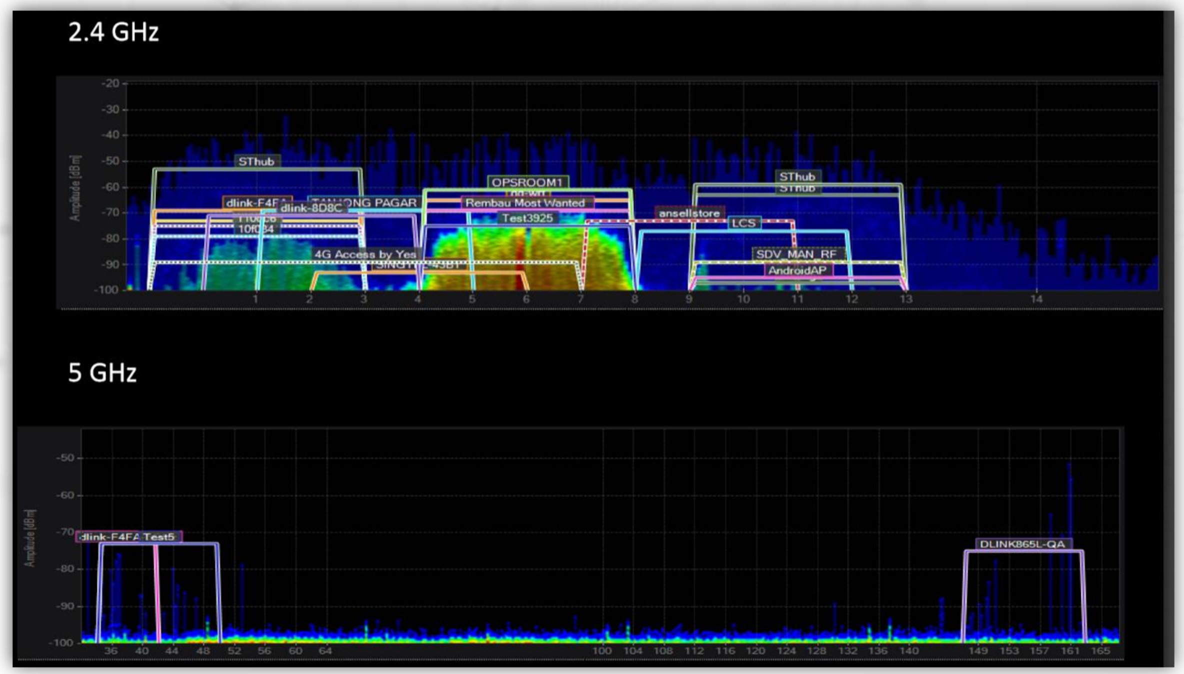
Site Survey Tools

There are many site survey tools available in the market which are both free and licensed, the main difference is the user experience and the amount of data you can gather.

Below are some of the tools available on different platforms:

- inSSIDer by Metageek (PC/Mac)
- Airport Utility (iOS)
- WiFi Analyzer (Android)
- WiFi Scanner (Mac)
- EnGenius Cloud Frequency Spectrum (Security AP)

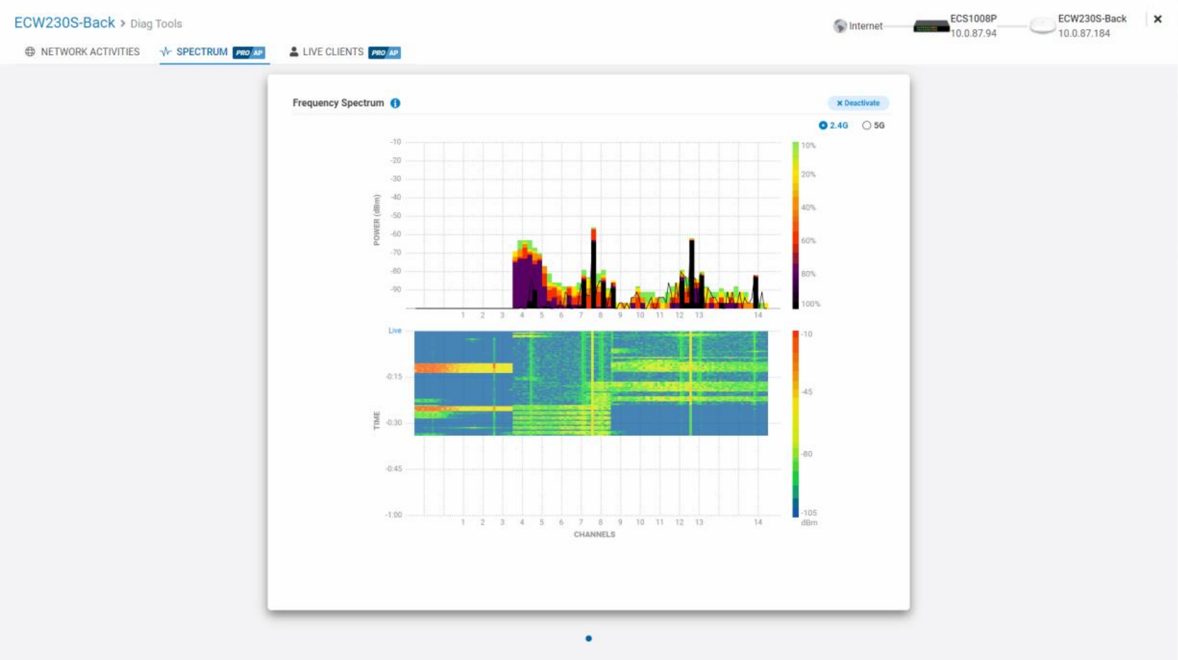
There are hardware-based dedicated tools as well which are compact and handheld. It's a good investment if you foresee doing multiple site surveys in the future.



Courtesy: CWNP Wi-Fi Conference 2014 Presentation: Your Phy Type (MetaGeek)

Spectrum analyzer

EnGenius Cloud is the only wireless brand to offer a built-in real-time spectrum analyzer on an access point.
Available on Security APs with an AP PRO License
This allows the MSP or system integrator to optimize their workflow with minimum equipment as possible as this tool is fully integrated on EnGenius Cloud.



Wi-Fi Heat Map

Wireless heat maps are used for multiple purposes:

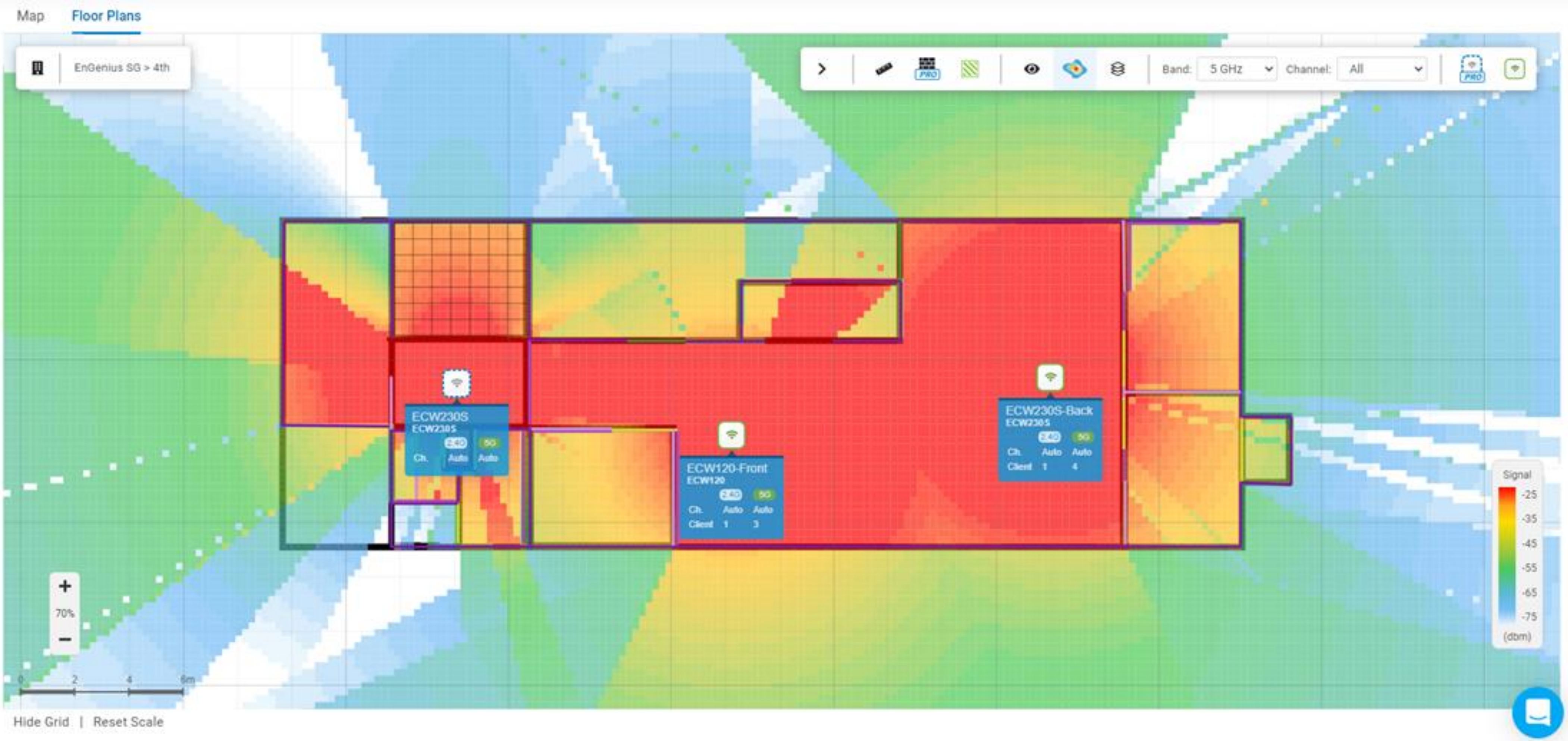
Pre-deployment planning

Post-deployment adjustments

Project proposals

Sometimes, heat maps are also used when there are site survey constraints, or going on-site is just not possible. There are multiple software in the market which can help you generate a heat map but most often than not, it can cost thousands of dollars for subscriptions.

EnGenius Cloud Floor Plan View



Band: 5 GHz
Channel: All

ECW230S
ECW230S

	2.4G	5G
Ch.	Auto	Auto

ECW120-Front
ECW120

	2.4G	5G
Ch.	Auto	Auto
Client	1	3

ECW230S-Back
ECW230S

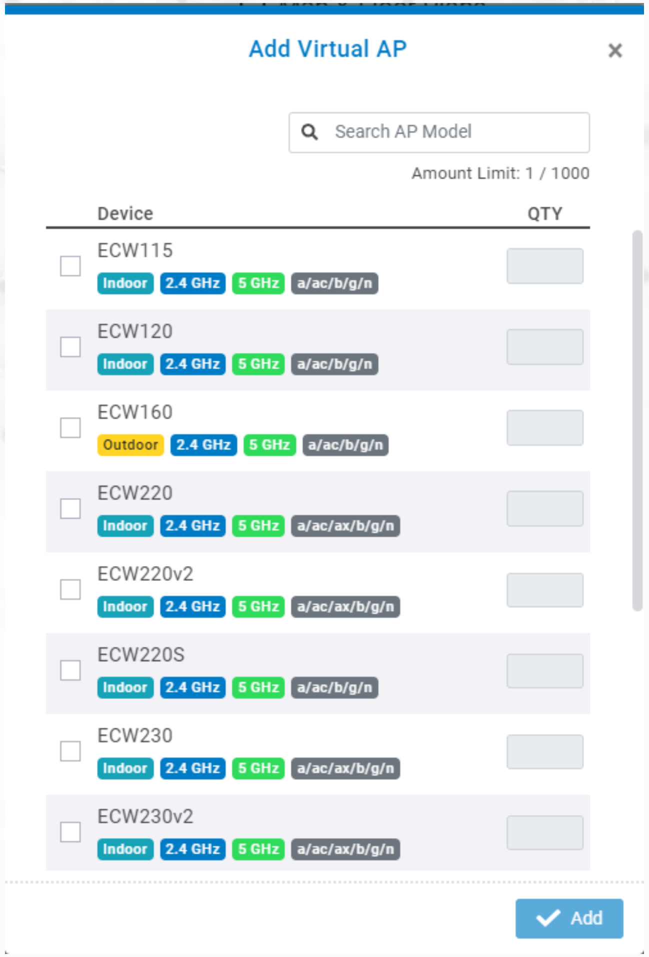
	2.4G	5G
Ch.	Auto	Auto
Client	1	4

EnGenius Cloud Floor Plan View

EnGenius Cloud's Floor Plan View allows you to plot obstacles and generate heat map based on the settings and antenna specs of each model.

Pro feature: If you do not have a physical unit, you can also plot Virtual APs in place for planning or simulation.

The floor plan can be extracted using the Reporting function on EnGenius Cloud.



Add Virtual AP ×

Search AP Model

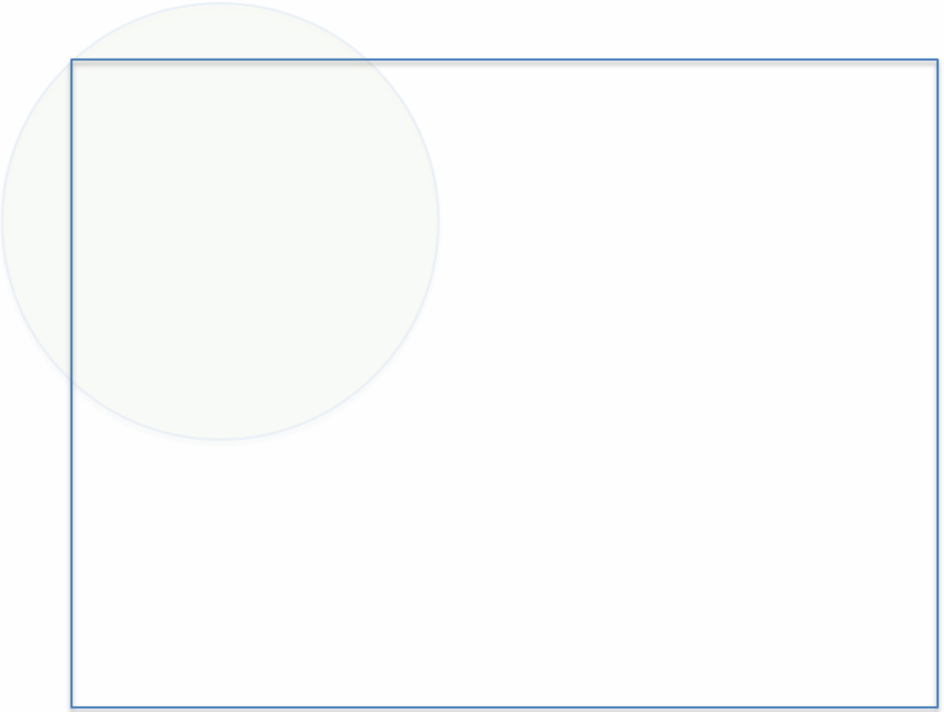
Amount Limit: 1 / 1000

	Device	QTY
□	ECW115 Indoor 2.4 GHz 5 GHz a/ac/b/g/n	
□	ECW120 Indoor 2.4 GHz 5 GHz a/ac/b/g/n	
□	ECW160 Outdoor 2.4 GHz 5 GHz a/ac/b/g/n	
□	ECW220 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
□	ECW220v2 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
□	ECW220S Indoor 2.4 GHz 5 GHz a/ac/b/g/n	
□	ECW230 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	
□	ECW230v2 Indoor 2.4 GHz 5 GHz a/ac/ax/b/g/n	

Channel Planning - 2.4 GHz for 6 APs

Channel planning is one of the most essential steps in designing a Wi-Fi system. How you plan your channels will directly impact the amount of support calls you will have due to wireless interference issues post-deployment.

The main goal in channel planning is to make sure that no two or more APs overlap with the same or adjacent channels which can immediately cause interference.



Channel planning - 2.4 GHz (20 MHz) for a multi-story deployment

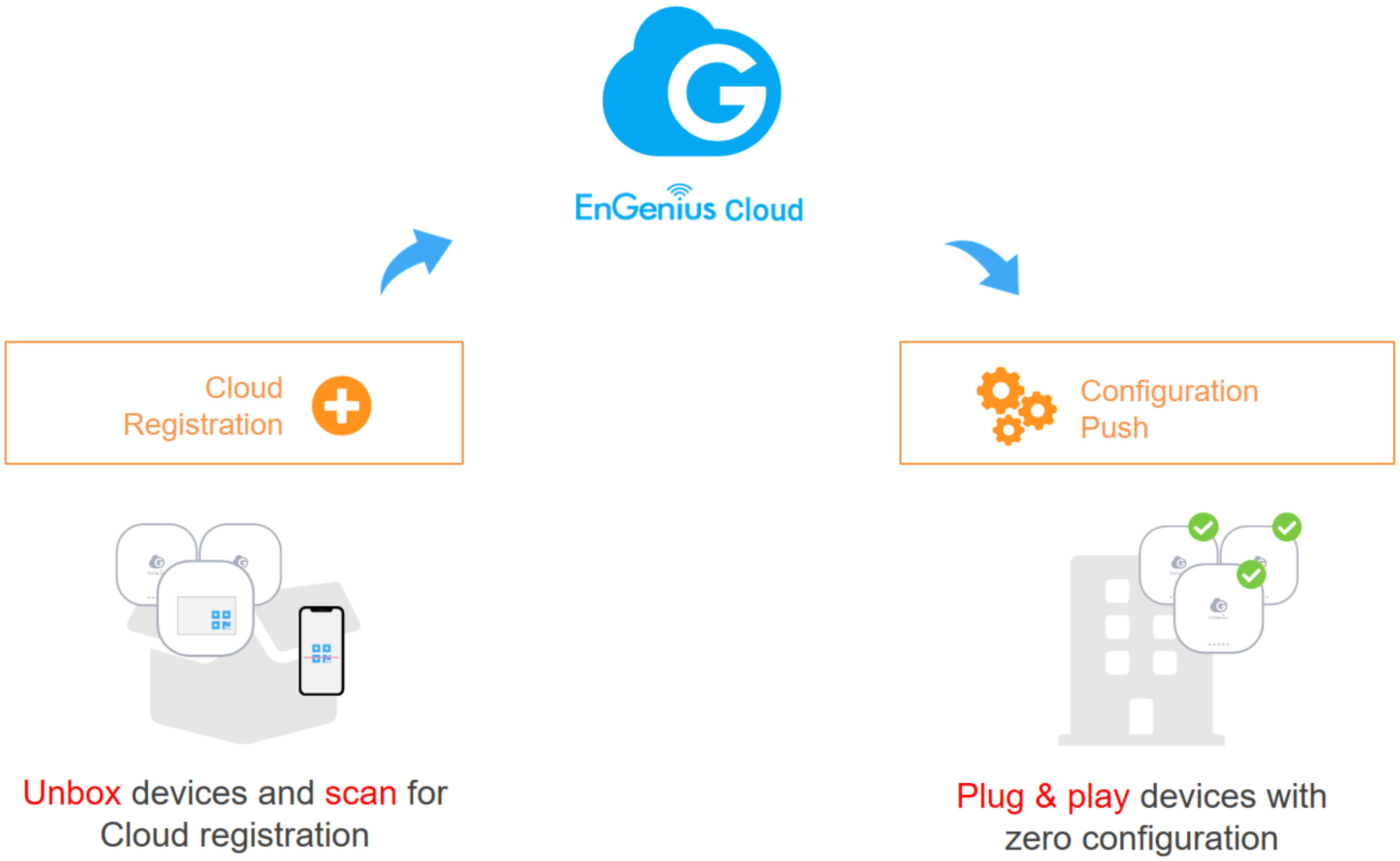
Channel planning gets a bit tougher once you consider verticality in the environment. EnGenius ceiling mount APs have a spherical antenna pattern which can penetrate walls and floors depending on the material. Penetration and coverage of an access point can be determined through site surveys.

Initialization - topics

- Overview
- Firewall requirements
- EnGenius Cloud setup

Overview

- There are a couple of ways to initialize an EnGenius Cloud setup:
    - EnGenius Cloud Portal
    - EnGenius Cloud To-Go App
- When deploying for larger, or controlled networks, we suggest to run the setup using the EnGenius Cloud Portal.
- EnGenius Cloud devices require internet access for management and monitoring. Once registered, settings and configuration will be pushed to the devices and keep them in sync.


EnGenius Cloud
Cloud Registration
Configuration Push
Unbox devices and scan for Cloud registration
Plug & play devices with zero configuration

Firewall Requirements

In a typical network environment, most of the ports used by EnGenius Cloud for device communication are open. However, some networks have tighter security. In such cases, the following ports need to be allowed by the network administrator to ensure that the Cloud devices function accordingly:

Cloud Devices	Cloud Services	Source IP	Destination IP	Ports	Protocol	Direction
AP, Switch, EnSky	Periodical Cloud communication, Firmware Upgrade, Real-Time Meter	Your Network	Any	443	TCP	Outbound
AP, Switch, EnSky	Persistent Cloud communication	Your Network	44.224.197 .174	80	TCP	Outbound
AP	Cloud RADIUS	Your Network	44.225.123 .183	1812/1813	TCP & UDP	Outbound
AP, Switch, EnSky	NTP Synchroniz ation	Your Network	Any	123	UDP	Outbound
AP, Switch, EnSky	Remote Tunnel	Your Network	44.230.110 .152	22	TCP	Outbound
AP	Splash Page	Your Network	Any	80/443	TCP	Outbound

EnGenius Cloud Setup

Initialization of EnGenius Cloud is straightforward:

1. Create an EnGenius Cloud account
2. Register Cloud device
3. Assign the device to a Network

Once the device is plugged into the network and has internet access, it will sync configuration with EnGenius Cloud.

(!) If you're adding a device for the first time, it will check for a newer firmware available on the server and update itself once it connects to the internet. The LEDs will blink simultaneously during this period. The device will proceed to go online once done.

EnGenius Cloud Setup

You don't have to pre-configure a device if you are deploying the units on a DHCP environment.

Deployment Site

Unbox Cloud devices and connect to the network

Headquarters

01 Create Cloud account

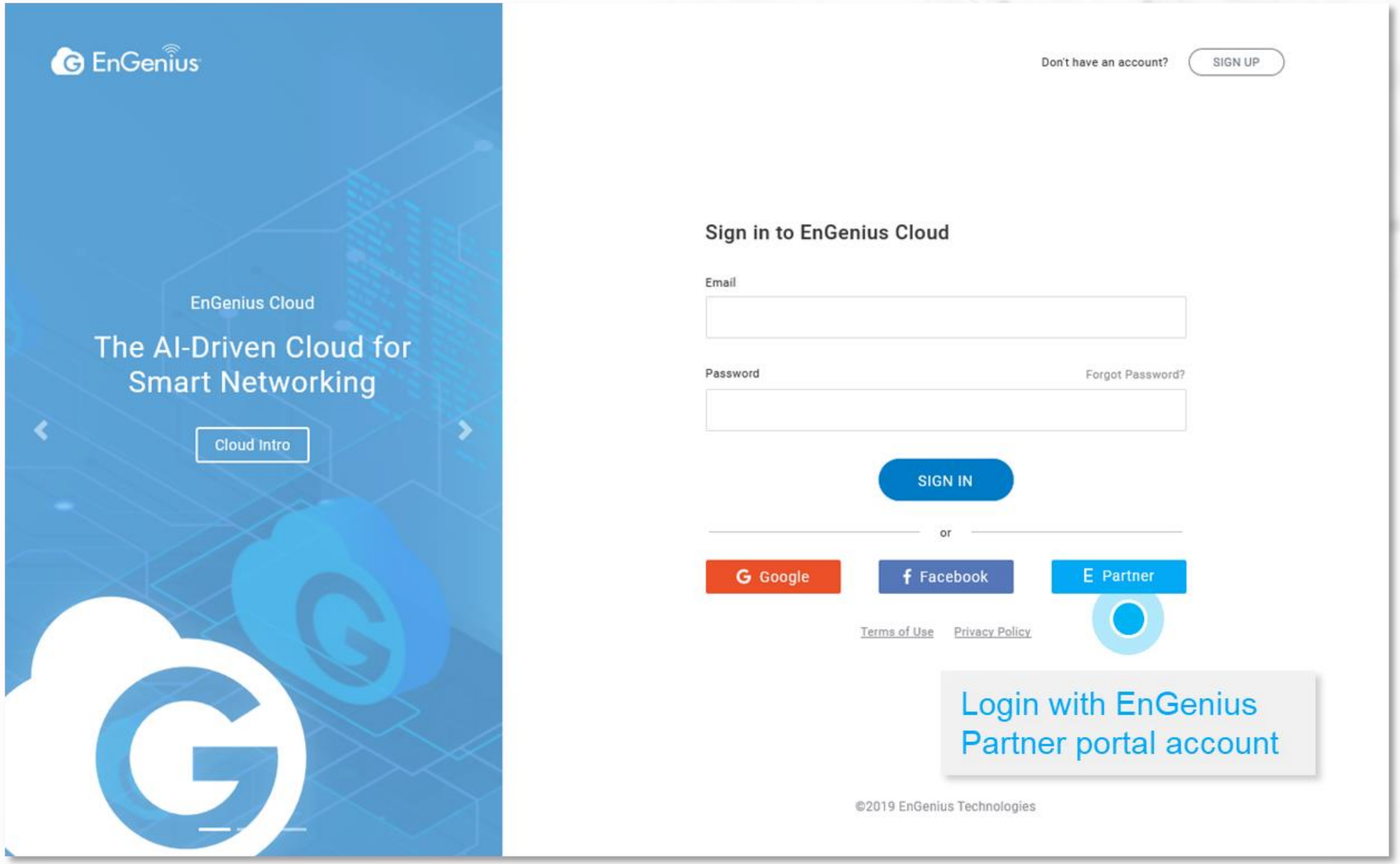
02 Register Cloud device

03 Assign devices to Network (Group configuration)

You're good to Go!

EnGenius Cloud Account

There are multiple options in signing up for an EnGenius Cloud account. If you already have an existing Partner Portal account, you may use that as well for SSO.



EnGenius

Don't have an account? SIGN UP

EnGenius Cloud

The AI-Driven Cloud for Smart Networking

Cloud Intro

Sign in to EnGenius Cloud

Email

Password

Forgot Password?

SIGN IN

or

Google Facebook Partner

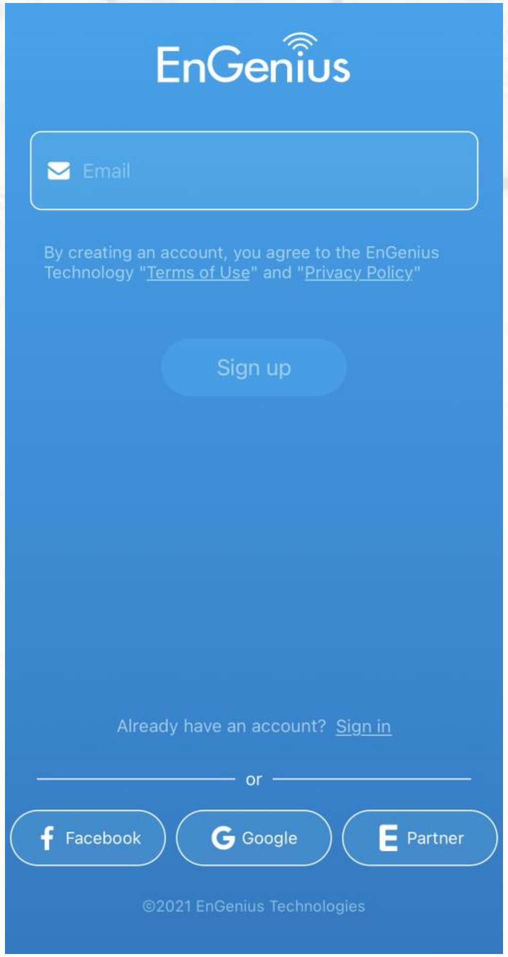
Terms of Use Privacy Policy

Login with EnGenius Partner portal account

©2019 EnGenius Technologies

EnGenius Cloud account – Cloud-to-go

Account registration can also be done via the EnGenius Cloud To-Go app.



EnGenius

Email

By creating an account, you agree to the EnGenius Technology "Terms of Use" and "Privacy Policy"

Sign up

Already have an account? Sign in

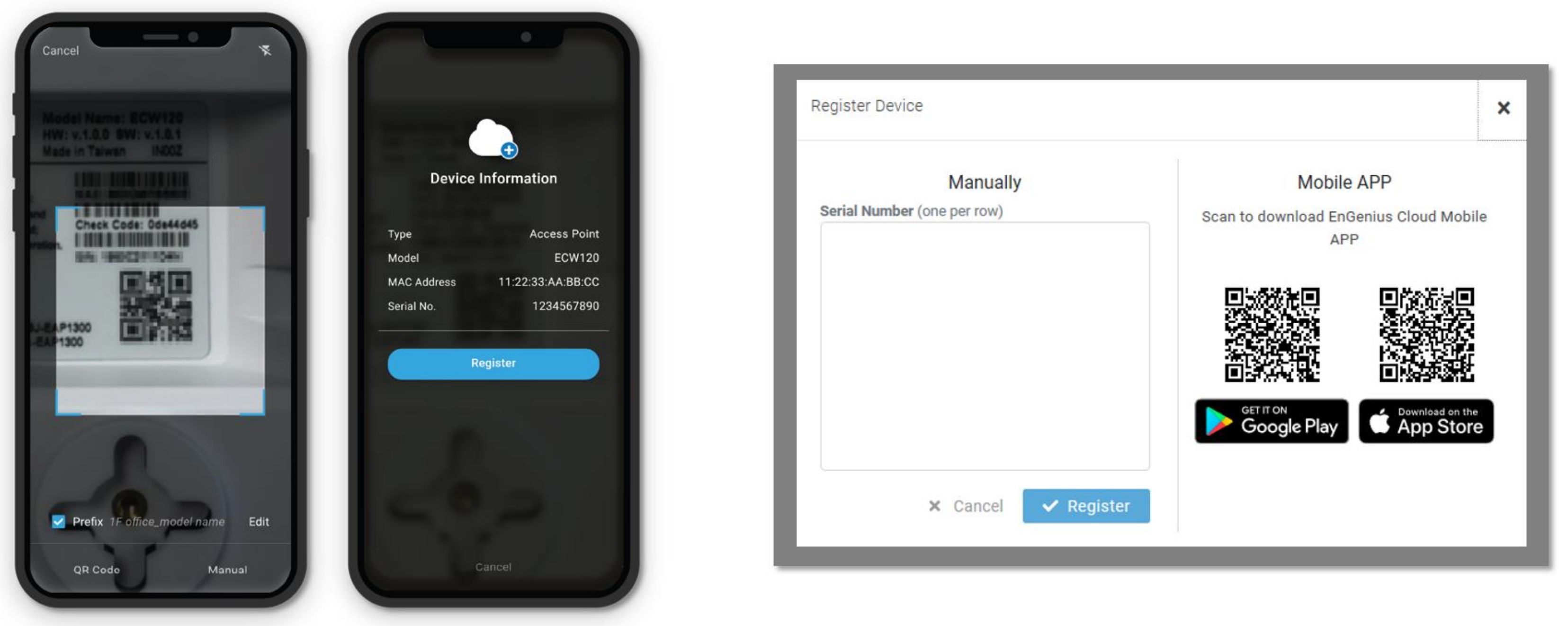
or

Facebook Google Partner

©2021 EnGenius Technologies

Device Registration

To register EnGenius Cloud devices to an Organization, the serial number or QR code is required. Registered Cloud devices are stored in the Organization's Inventory.



Device Information

Type	Access Point
Model	ECW120
MAC Address	11:22:33:AA:BB:CC
Serial No.	1234567890

Register Device

Manually

Serial Number (one per row)

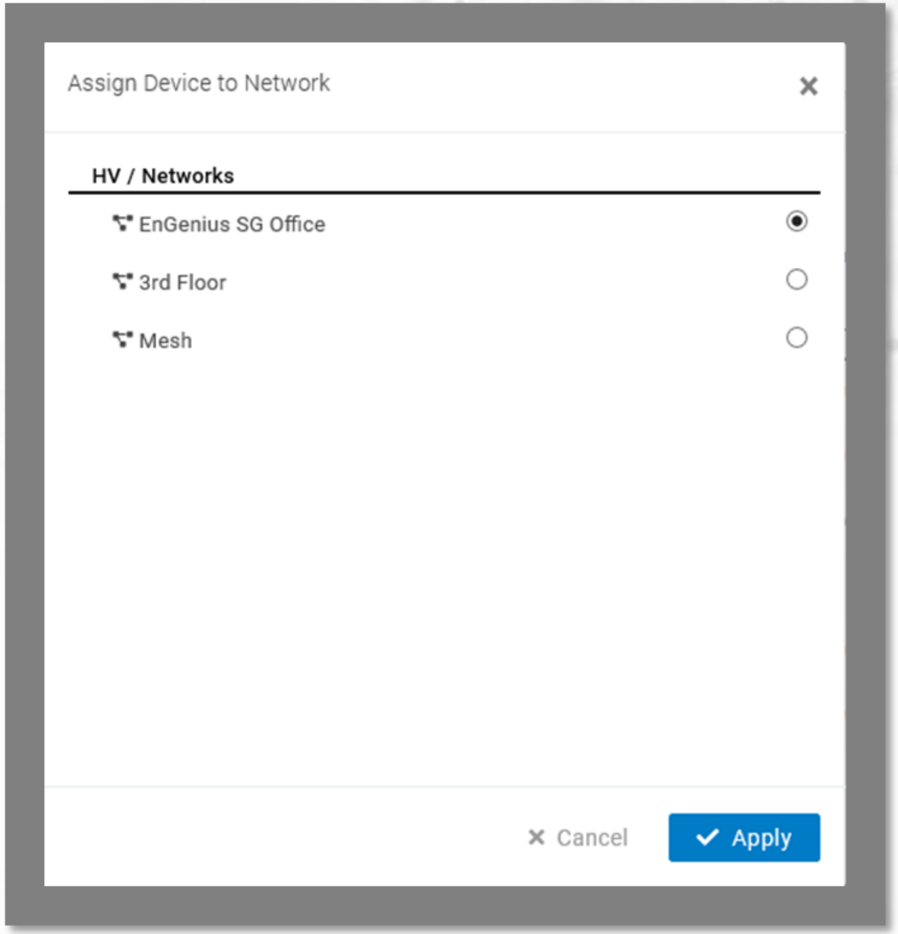
Mobile APP

Scan to download EnGenius Cloud Mobile APP

Network Assignment

Devices in the organization its inventory can be assigned to a network.

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



Assign Device to Network

HV / Networks

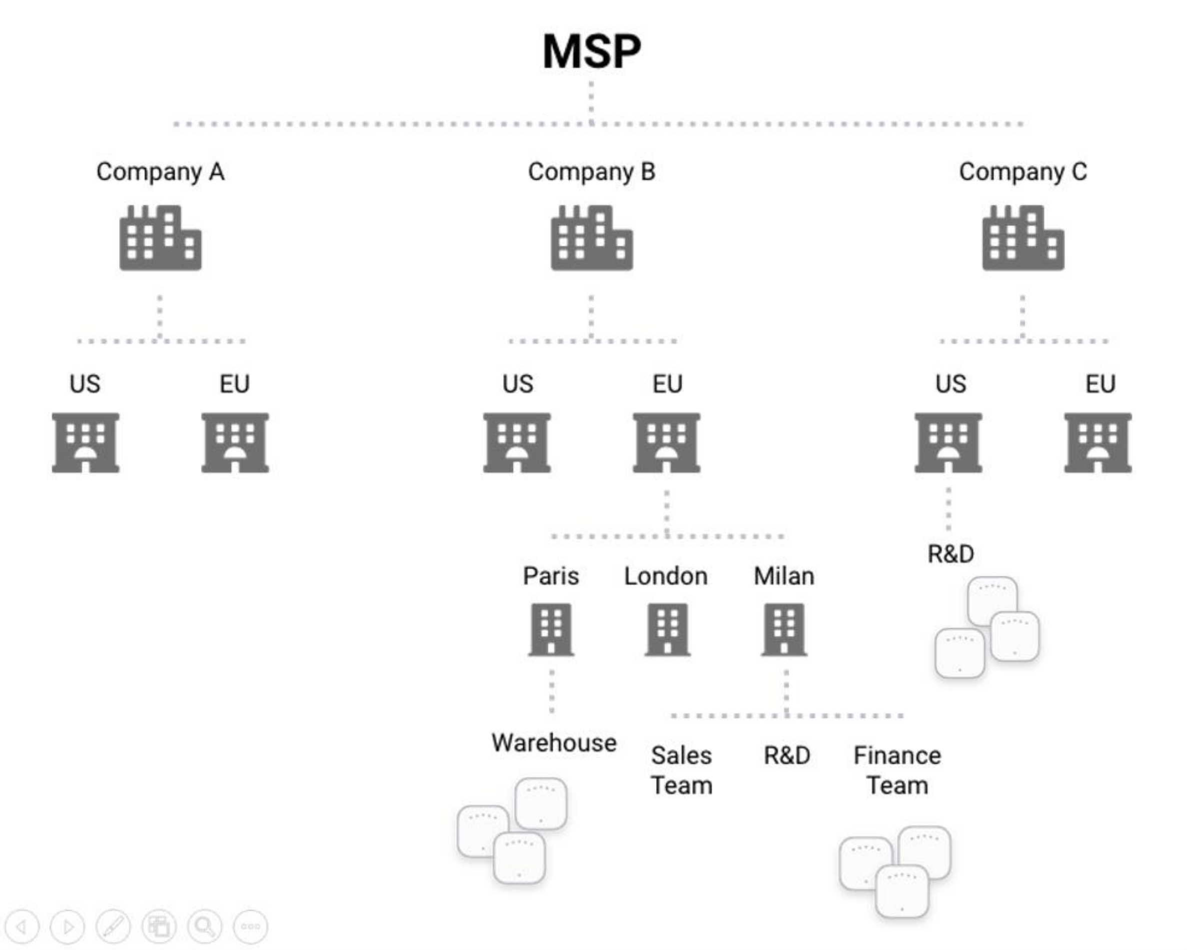
- EnGenius SG Office ●
- 3rd Floor ○
- Mesh ○

Management - topics

- Network management
    - Hierarchy View
        - Organizations
        - Networks
    - Access points
        - Radio settings
        - SSIDs
- Multitenancy
- Inventory & license management

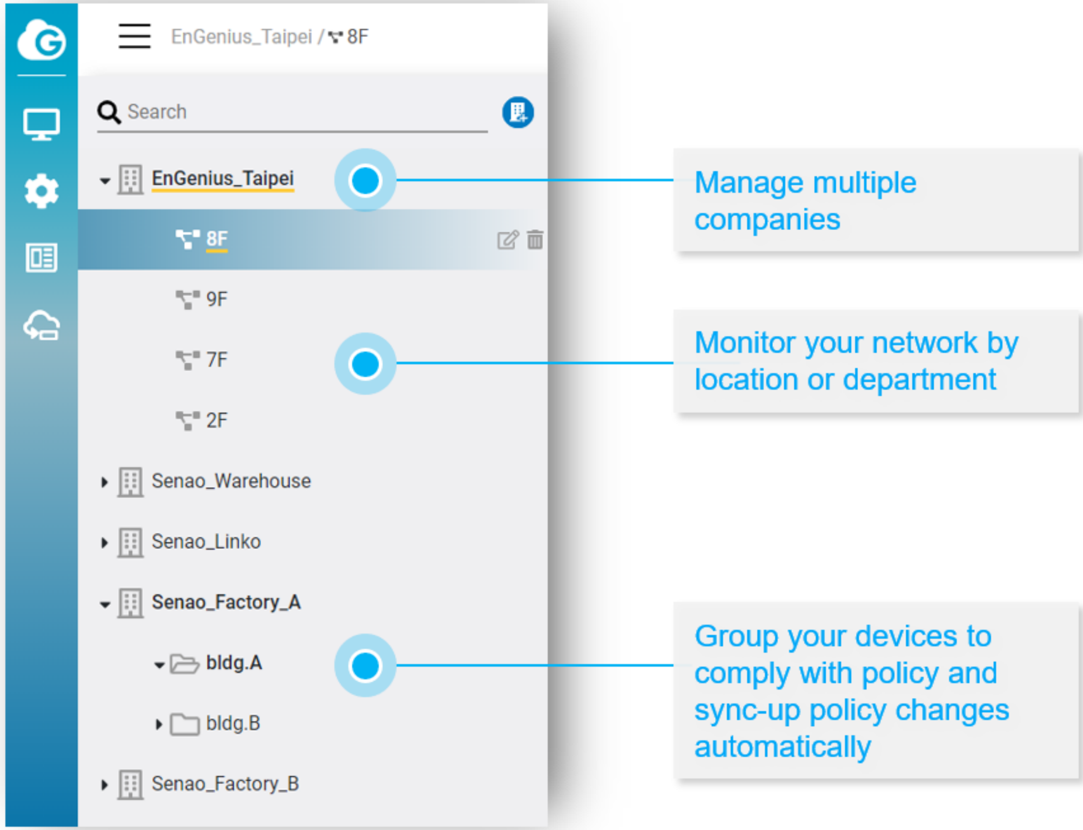
Network management

A managed service provider or system integrator usually juggles between clients when it comes to maintenance and support. When using a traditional system, doing such tasks usually takes great effort: remote access needed in place for each site, multiple accounts required to be setup, or each client required to have their own individual system, and so on.



Network management (2)

With EnGenius Cloud, individual companies can be managed from the same interface. Each company or corporation are separated through Organizations and depending on the structure, Cloud devices can be split into several Networks.



Manage multiple companies

Monitor your network by location or department

Group your devices to comply with policy and sync-up policy changes automatically

Organizations

Organizations are totally independent of each other. Each Org has its own Inventory, License, Team Members, and Networks.

If another administrator has invited you as a Viewer or Admin, their Organization will appear under your Hierarchy View.

Networks

Depending on how the network is segmented, Networks can be branched from the main Org or placed in "sub-folders".

Under the Network, devices follow a general policy setting set by the administrator. Certain parameters may be overridden when running a specific configuration for a device. I.e. Tx Power, Channel, SSID, etc.

Access points

EnGenius Cloud access points are grouped per network.

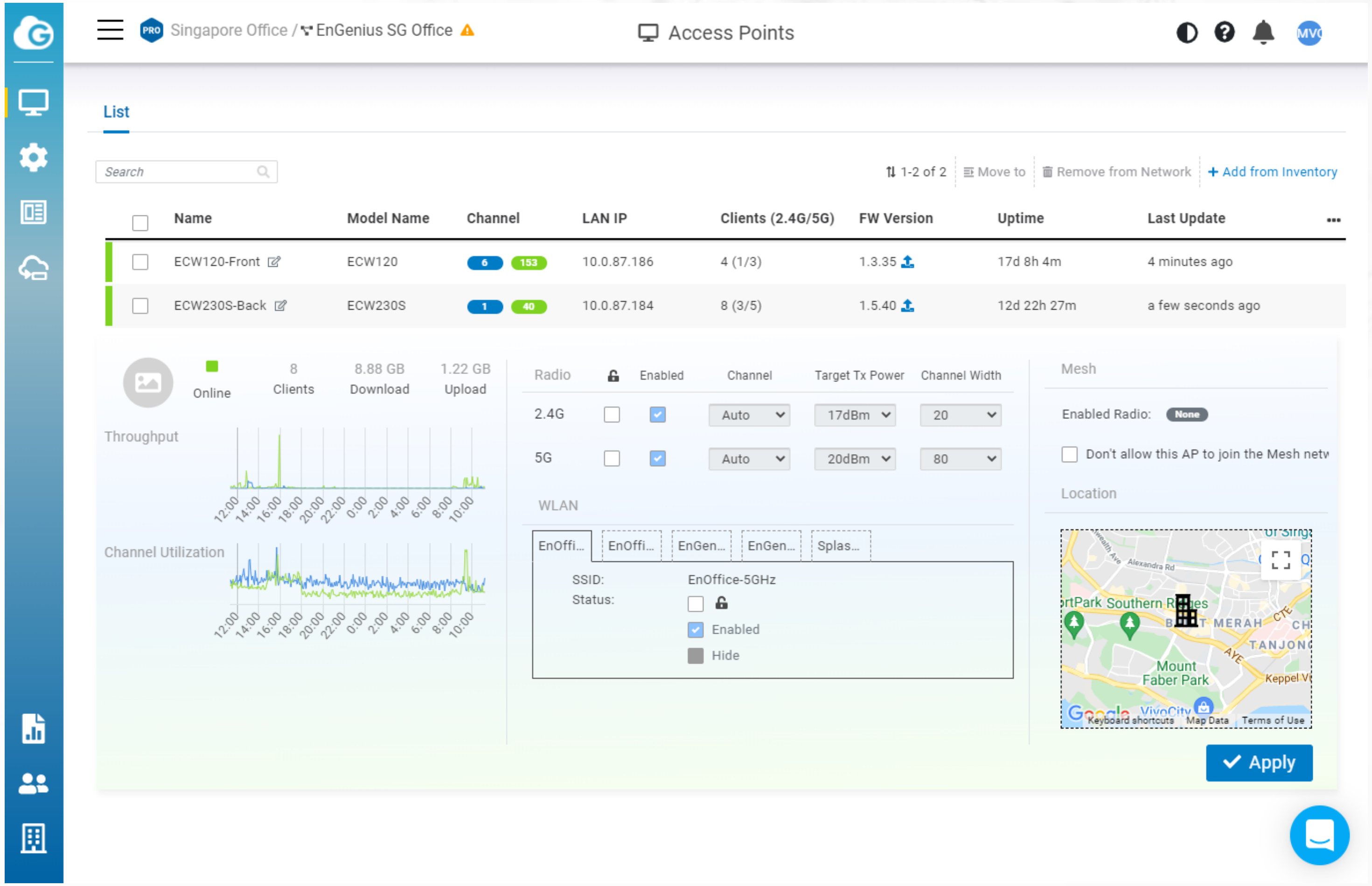
Depending on the network administrator, the network can be setup in multiple ways.

Network segregation can be done per:

- Branch or site - clients with multiple branches or locations, and each site have their own wireless configuration
- Building - hospitality verticals usually have the same setup for all APs in multiple floors, except for a few units in specific areas which can be overridden on the access points page or individual AP details page
- Floor - commercial or leasing establishments may have a different network layout per story
- Department - some clients call for specific network setups per department despite being on the same physical location; in this situation, the Org is split into several Networks for each department.

Access points (2)

Each access point can be configured to override the radio, mesh and SSID settings. This comes in handy for fine tuning APs in specific placement areas.



Singapore Office / EnGenius SG Office ⚠

Access Points

List

Search

1-2 of 2 | Move to | Remove from Network | + Add from Inventory

□	Name	Model Name	Channel	LAN IP	Clients (2.4G/5G)	FW Version	Uptime	Last Update
□	ECW120-Front	ECW120	6 153	10.0.87.186	4 (1/3)	1.3.35	17d 8h 4m	4 minutes ago
□	ECW230S-Back	ECW230S	1 40	10.0.87.184	8 (3/5)	1.5.40	12d 22h 27m	a few seconds ago

Online	8	8.88 GB	1.22 GB
	Clients	Download	Upload

Throughput

Channel Utilization

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

WLAN

EnOffi... | EnOffi... | EnGen... | EnGen... | Splas...

SSID: EnOffice-5GHz

Status: □ 🔓

☑ Enabled

■ Hide

Mesh

Enabled Radio: None

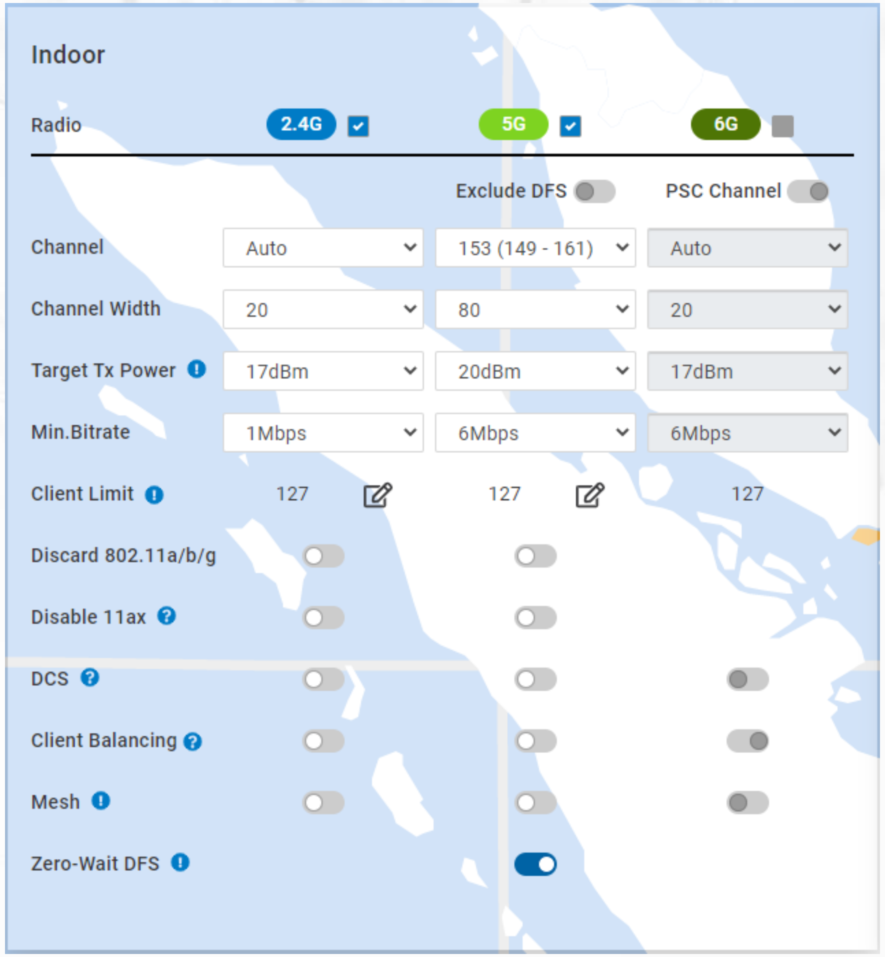
□ Don't allow this AP to join the Mesh netw

Location

✓ Apply

Radio settings

Radio settings can only be configured when viewing a network. These settings applies to all APs within the network unless overridden on the specific device.



Indoor

Radio	2.4G ☑	5G ☑	6G □
		Exclude DFS ○	PSC Channel ○
Channel	Auto	153 (149 - 161)	Auto
Channel Width	20	80	20
Target Tx Power	17dBm	20dBm	17dBm
Min.Bitrate	1Mbps	6Mbps	6Mbps
Client Limit	127	127	127
Discard 802.11a/b/g	○	○	
Disable 11ax	○	○	
DCS	○	○	○
Client Balancing	○	○	●
Mesh	○	○	○
Zero-Wait DFS		●	

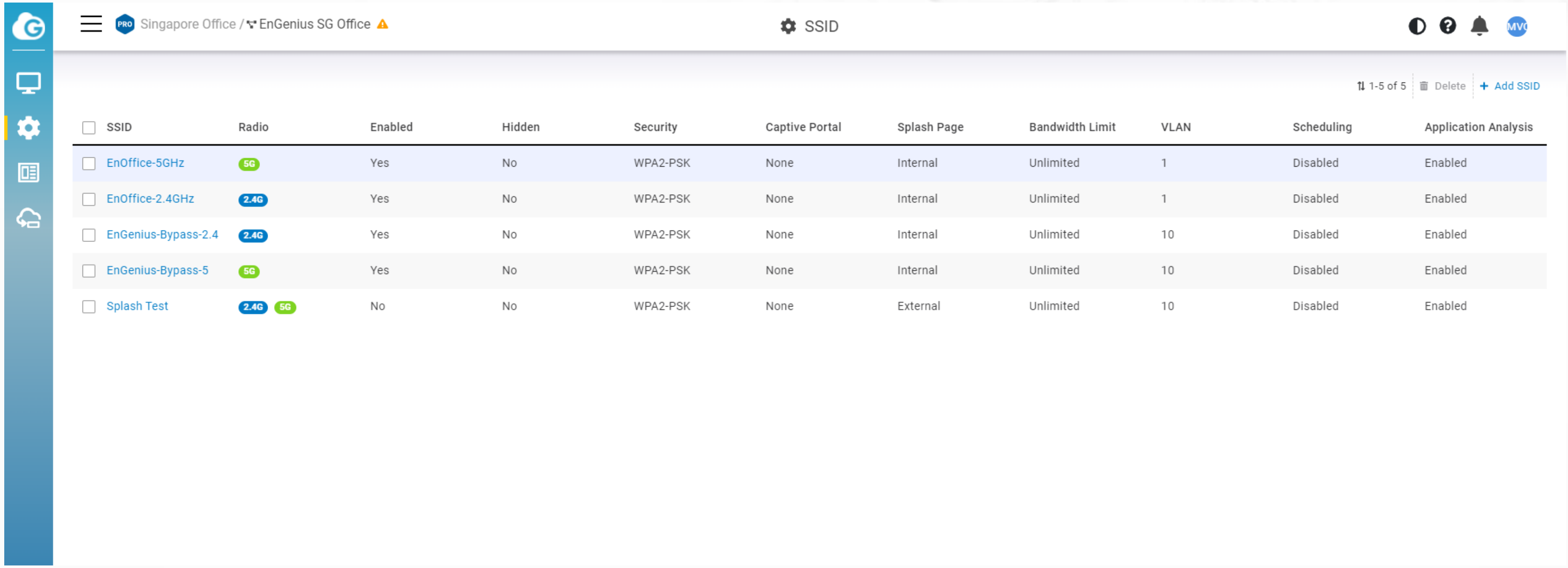
Radio settings descriptions of options

Option	Description
Radio	Enables/Disables 2.4 GHz/5 GHz radios.
Channel	Specifies a frequency or set to auto.
Exclude DFS	When channel selection is set to auto, the device will not scan/select DFS channels.
Channel Width	Sets the channel width from 20, 40, or 80 MHz. The higher channel widths support higher data rates for Wi-Fi 5 and Wi-Fi 6 models, but this subjects the AP to interference. See: Wi-Fi Interference.
Target Tx Power	Sets the target transmit power for the AP which depends on the maximum allowable EIRP per country. The actual Tx power set by the system may be higher or lower than the Target Tx set.
Min. Bitrate	Sets the minimum bitrate for the AP. Adjusting this option will affect clients who have older generation devices or have low RSSI/SNR .
Client Limit	Limits the maximum concurrent clients on the AP per radio. 127 for Wi-Fi 5 and 500 for Wi-Fi 6 models.
Discard 802.11a/b/g	Blocks connections from older generation devices.
Disable 11ax	Disables 802.11ax on Wi-Fi 6 models. This option will force the AP to run in 802.11ac mode, useful for environments where majority of client devices do not support 802.11ax yet.
DCS	When "Dynamic Channel Selection" is selected, the AP scans and changes channels on start-up or upon reboot. DCS allows the AP to scan the environment every 15 mins, and change the channel if the utilization is >50%. During the change, clients momentarily get disconnected. This option is not advisable for use in connection-sensitive applications.
Client Balancing	In a multi-AP deployment, this option allows the AP to steer clients to neighboring units to prevent overloading or to spread clients evenly in a dense AP deployment. This function utilizes 802.11v.
Mesh	Enabling Mesh unlocks Auto Pairing

SSID Profiles

A total of 8 SSID profiles can be created per Network. If all profiles are enabled with all radios selected (2.4 GHz, 5 GHz, and 6 GHz—on supported APs), the APs under the Network will broadcast 24 BSSIDs.

(!) Enabling 5 or more SSIDs may heighten channel utilization due to the increase in overhead.

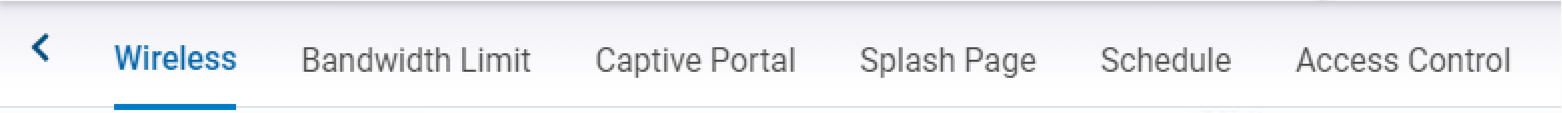


☐ SSID	Radio	Enabled	Hidden	Security	Captive Portal	Splash Page	Bandwidth Limit	VLAN	Scheduling	Application Analysis
☐ EnOffice-5GHz	5G	Yes	No	WPA2-PSK	None	Internal	Unlimited	1	Disabled	Enabled
☐ EnOffice-2.4GHz	2.4G	Yes	No	WPA2-PSK	None	Internal	Unlimited	1	Disabled	Enabled
☐ EnGenius-Bypass-2.4	2.4G	Yes	No	WPA2-PSK	None	Internal	Unlimited	10	Disabled	Enabled
☐ EnGenius-Bypass-5	5G	Yes	No	WPA2-PSK	None	Internal	Unlimited	10	Disabled	Enabled
☐ Splash Test	2.4G 5G	No	No	WPA2-PSK	None	External	Unlimited	10	Disabled	Enabled

SSID tabs

Each SSID can be configured independently and will broadcast through all APs on the Network once enabled. I.e. SSID 1 - WPA2 PSK, SSID 2 - Voucher Service, SSID 3 - Captive Portal AD Authentication, etc.

The SSID page contains several tabs for customization. This applies to all APs unless overridden and disabled on specific devices.



SSID tab - Wireless

These options allows you to customize the main settings for the SSID.

- Name - the SSID name
- Enable - enables the SSID
- Hide - disables SSID broadcast (hidden SSID)
- Radio - select which radio the SSID operates on (2.4 GHz, 5 GHz, 6GHz, none, some or all)
- Security Type
  - Open - no encryption, used for public hotspots
  - WPA2 PSK - basic WPA2 pre-shared key, AES encryption
  - WPA2 MyPSK - configure the SSID with a portable PSK which works with either EnGenius Cloud MyPSK Users or an external RADIUS server used as the user database; respective user's assigned VLAN can be configured in MyPSK Users page or from specified RADIUS server.
    (!) MyPSK user-assigned VLAN allows respective user to be associated to a specific VLAN regardless of the native VLAN assigned to the AP or SSID.

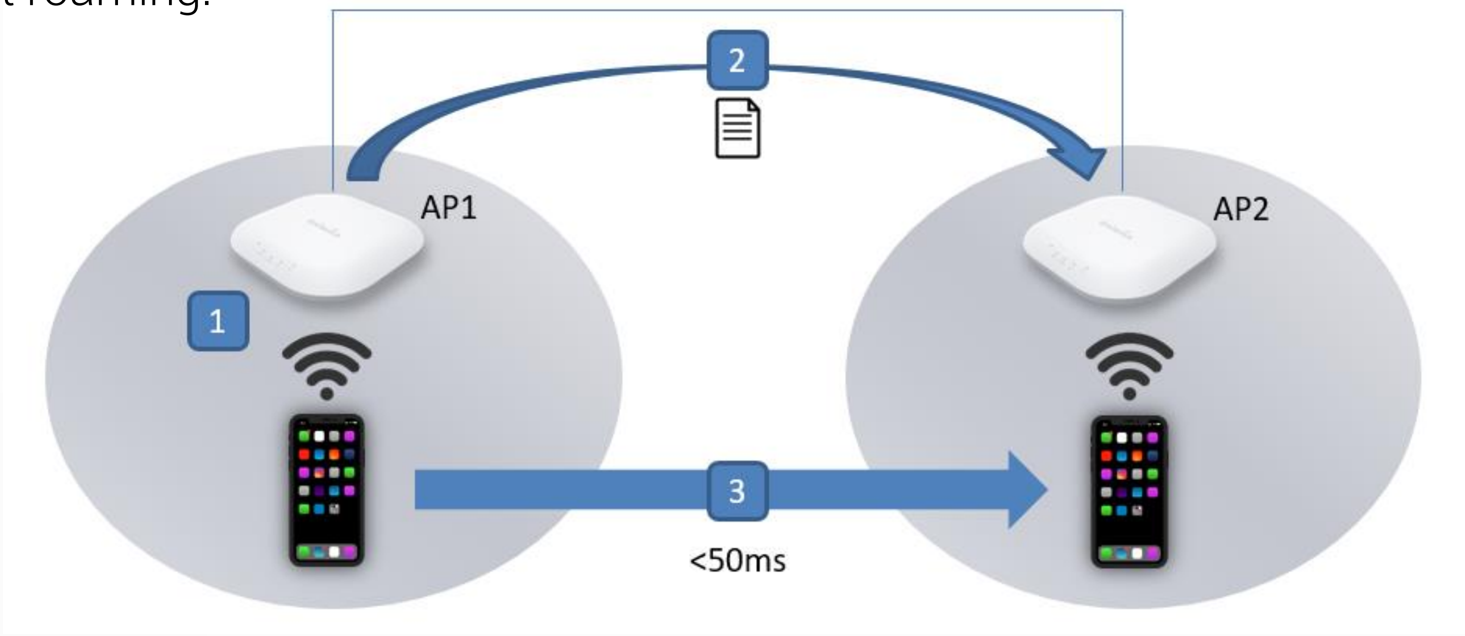
SSID tab – Wireless (2)

- Security Type (continued)
  - WPA3 Personal - robust and utilizes the latest security protocols to-date
  - WPA3 Personal/WPA2 PSK Mixed - not all client devices are compatible with WPA3, to allow connections for non-WPA3 compatible devices, this option should be selected
  - WPA2 and WPA3 Enterprise - WPA2/3 and username/password authentication via specific database
    - EnGenius Cloud RADIUS - Cloud-based RADIUS server
    - Custom RADIUS - external RADIUS server
    - Google LDAP - Google Secure LDAP service
    - my LDAP Server - external LDAP server
    - Active Directory - Windows Active Directory authentication

(!) Within each Network, only 1 SSID profile can be set with either Google LDAP, my LDAP, or Active Directory authentication as the wireless security or its Captive Portal authentication option.

SSID tab – Wireless (3)

- **802.11r** - Fast Roaming, requires AP coverage overlap
  (!) For Fast Roaming to function, there needs to be an overlap in coverage between the APs where the client device also needs to support fast roaming.
  Fast roaming is widely used for seamless transition between APs. The standards supported for Fast Roaming are 802.11r, 802.11k, and 802.11v.
  Fast roaming is supported by most flagship mobile phones and tablets. At the moment, not all laptops support fast roaming.



SSID tab – Wireless (4)

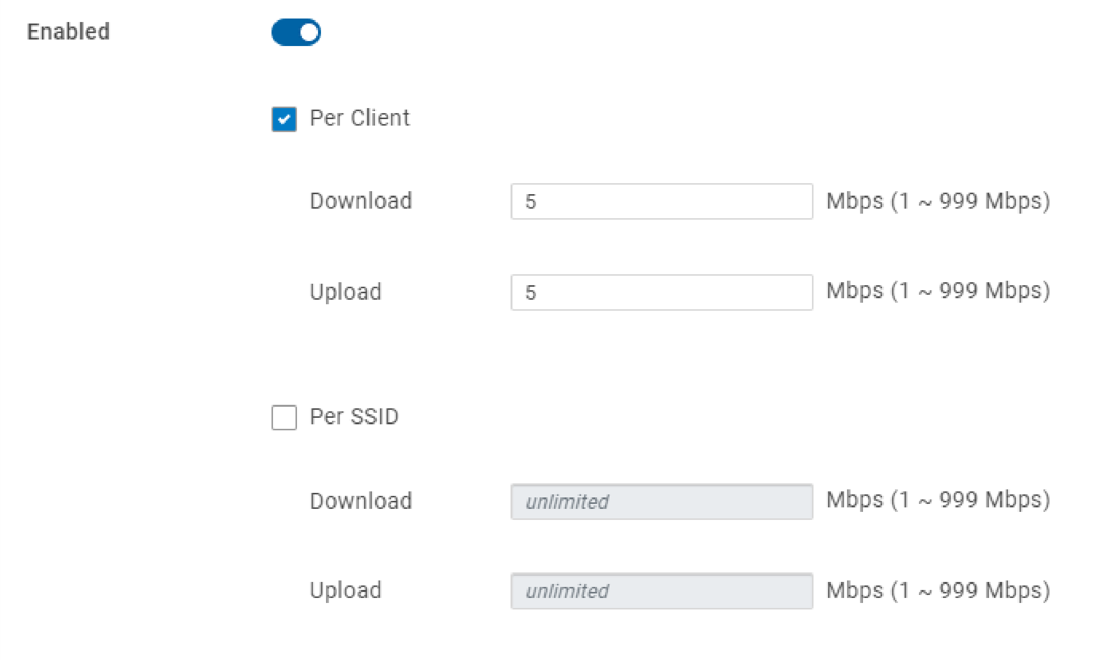
- 802.11w - PMF or Protected Management Frames add a layer of protection to prevent wireless attacks such as deauthentication attacks on connected clients
- Default VLAN - tag a specific VLAN to the SSID; MyPSK's Users' VLAN option overrides this.
- Client IP Addressing
  - Bridge Mode - the default option, wireless clients will obtain an IP address from the external DHCP server
  - NAT Mode - the AP acts as a DHCP server and provides a set range of IPs to wireless clients; in NAT mode, wireless clients are not able to communicate with any other wireless client on the same AP - used for guest networks.
- Dynamic Client VLAN Pooling - assign a VLAN range and randomly assign wireless clients as they connect to the SSID, used to prevent broadcast traffic flooding by splitting the subnet into smaller clusters

SSID tab – Wireless (5)

- Application Analysis - enables Layer-7 awareness for wireless clients, allows you to monitor the bandwidth consumption of the commonly utilized applications on the organization or network
- Advanced Settings
    - L2 Isolation - blocks wireless to wireless and wireless to wired communication
    - Band Steering - prioritizes the 5 GHz radio for wireless connection
    - RSSI Threshold - defines the minimum threshold at which the AP will push the client off from 5 GHz to 2.4 GHz when the RSSI level drops lower than the set value.
    - BCMC Suppression - Broadcast/Multicast traffic is blocked from the LAN to the wireless side, keeping the wireless network healthy. Only DHCP and ARP are allowed for broadcast; it's not advisable for use in environments where applications required to transmit multicast packets on the network.

SSID tab - Bandwidth limit

Bandwidth Limit allows you to throttle the maximum speed of wireless clients to prevent data hogs. This function is most needed in bandwidth limited environments such as public Wi-Fi spaces like cafés or libraries.



Enabled ●

☑ Per Client

Download 5 Mbps (1 ~ 999 Mbps)

Upload 5 Mbps (1 ~ 999 Mbps)

□ Per SSID

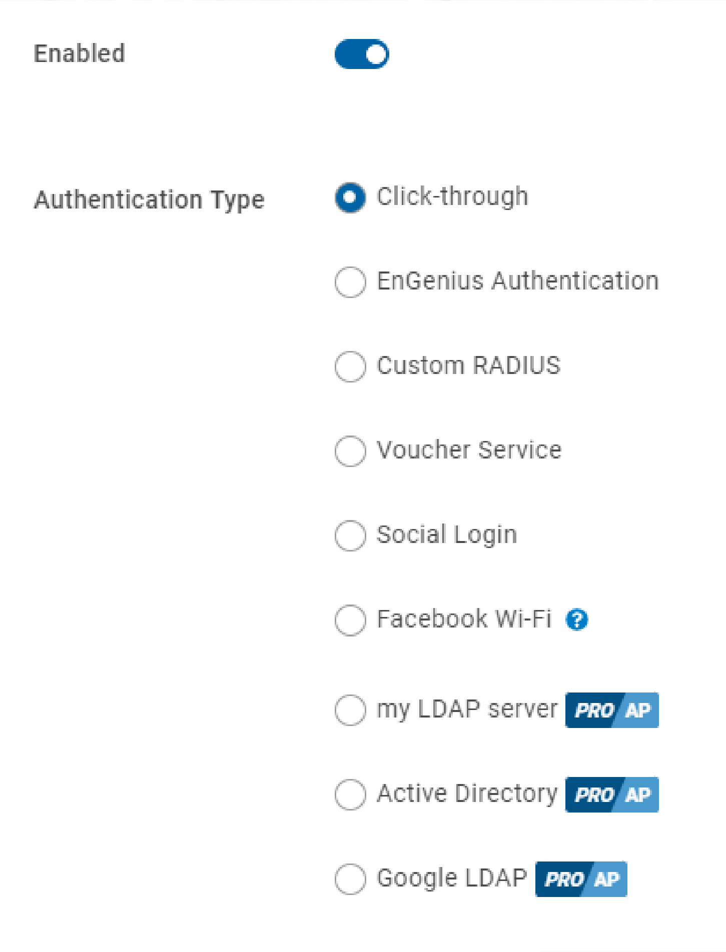
Download *unlimited* Mbps (1 ~ 999 Mbps)

Upload *unlimited* Mbps (1 ~ 999 Mbps)

SSID tab - Captive portal

Certain wireless deployments require a splash page as part of the association process. Splash pages are used to present information, disclaimers, or add additional layer of authentication/registrations prior to bridging the client to the network.

There are several captive portal options available on EnGenius Cloud, some also used as authentication options in the wireless security types.



Enabled ●

Authentication Type

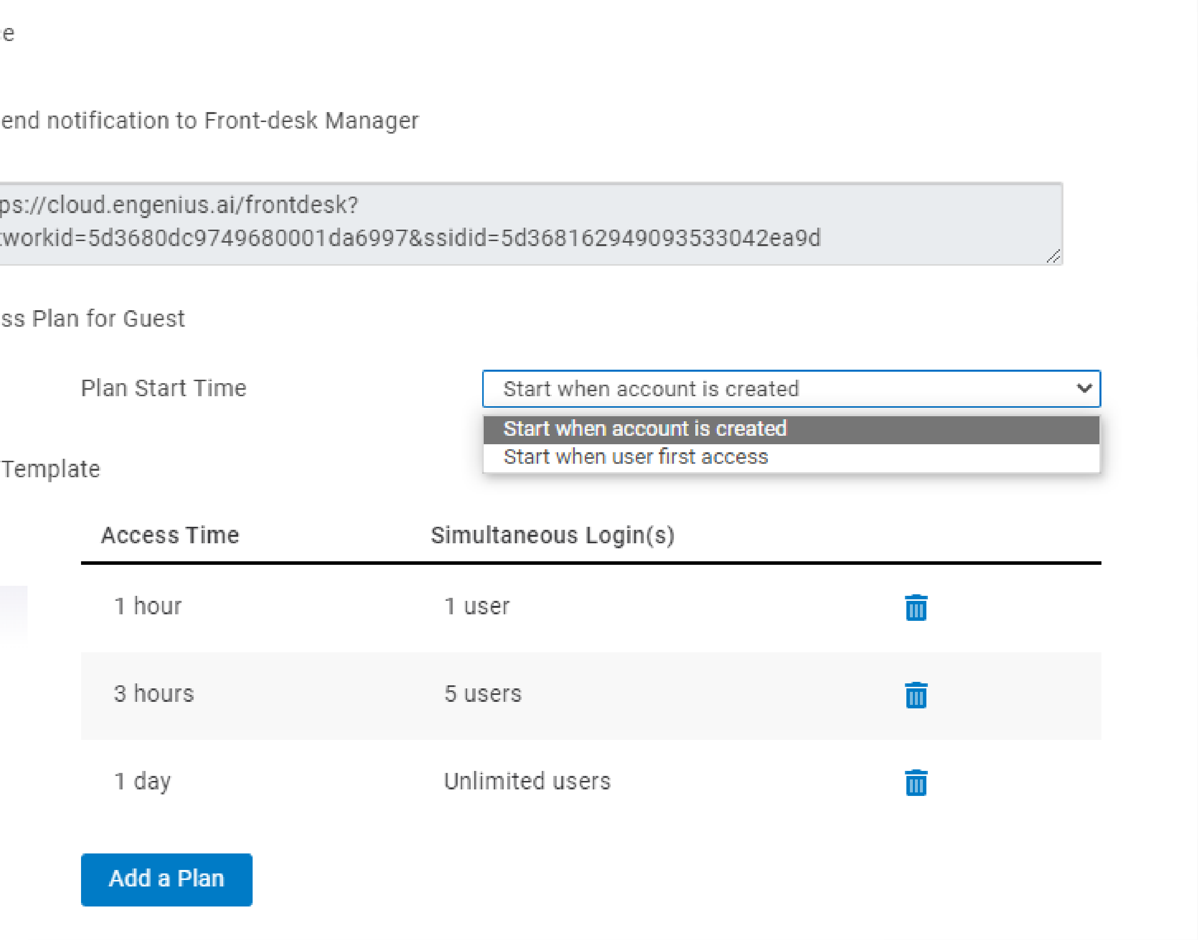
● Click-through
○ EnGenius Authentication
○ Custom RADIUS
○ Voucher Service
○ Social Login
○ Facebook Wi-Fi ?
○ my LDAP server PRO AP
○ Active Directory PRO AP
○ Google LDAP PRO AP

SSID tab - Captive portal – Authentication types

- Click Through - presents a splash page and a button to proceed without authentication, used for advertisements, notices, or disclaimers
- EnGenius Authentication - EnGenius Cloud RADIUS server
- Custom RADIUS - external RADIUS server
    - CoA-RADIUS - CoA process allows you to change user access immediately. If enabled, the AP will respond to the disconnect message sent by the RADIUS server.
    - Bandwidth Limit by RADIUS - overrides the bandwidth limit set on the SSID and allows the RADIUS server to set an individual limit per user or user level
    - RADIUS MAC-Authentication - allows a RADIUS server to whitelist client devices which are authorized to access the network as a secondary security measure. I.e. Person A connects to the wireless network using Person B's credentials, after a successful association, the MAC address of the device is checked for authentication and is verified on the RADIUS server's whitelist

SSID tab - Captive portal – Authentication types (2)

- **Voucher Service** - a voucher service or hotspot service is a quick way to provide wireless access via "tickets". Plans can be set by the administrator, and the vouchers are managed by a designated front-desk staff, or the admins themselves.



● Voucher Service

□ Send notification to Front-desk Manager

https://cloud.engenius.ai/frontdesk?networkid=5d3680dc9749680001da6997&ssidid=5d36816294909353042ea9d

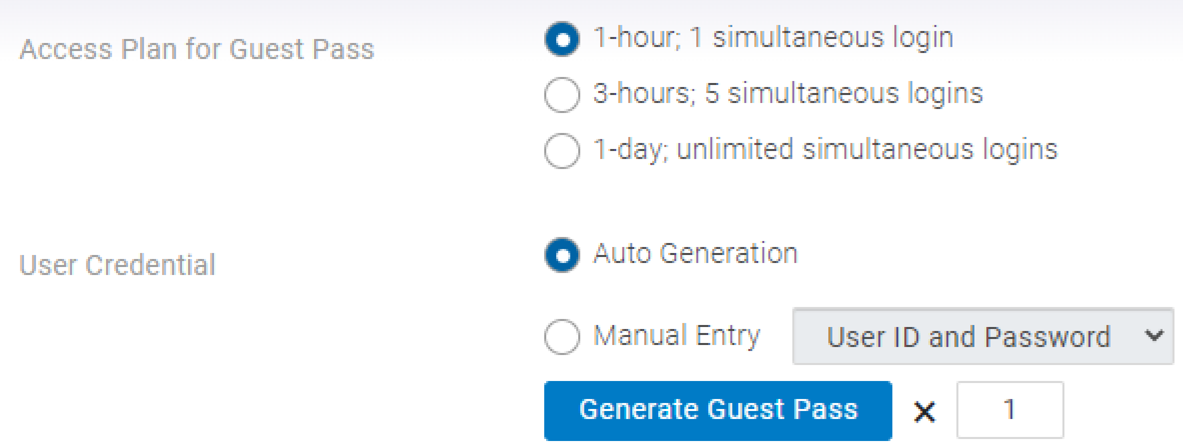
Access Plan for Guest

Plan Start Time: Start when account is created

- Start when account is created
- Start when user first access

Plan Template

Access Time	Simultaneous Login(s)
1 hour	1 user
3 hours	5 users
1 day	Unlimited users



Access Plan for Guest Pass

● 1-hour; 1 simultaneous login
○ 3-hours; 5 simultaneous logins
○ 1-day; unlimited simultaneous logins

User Credential

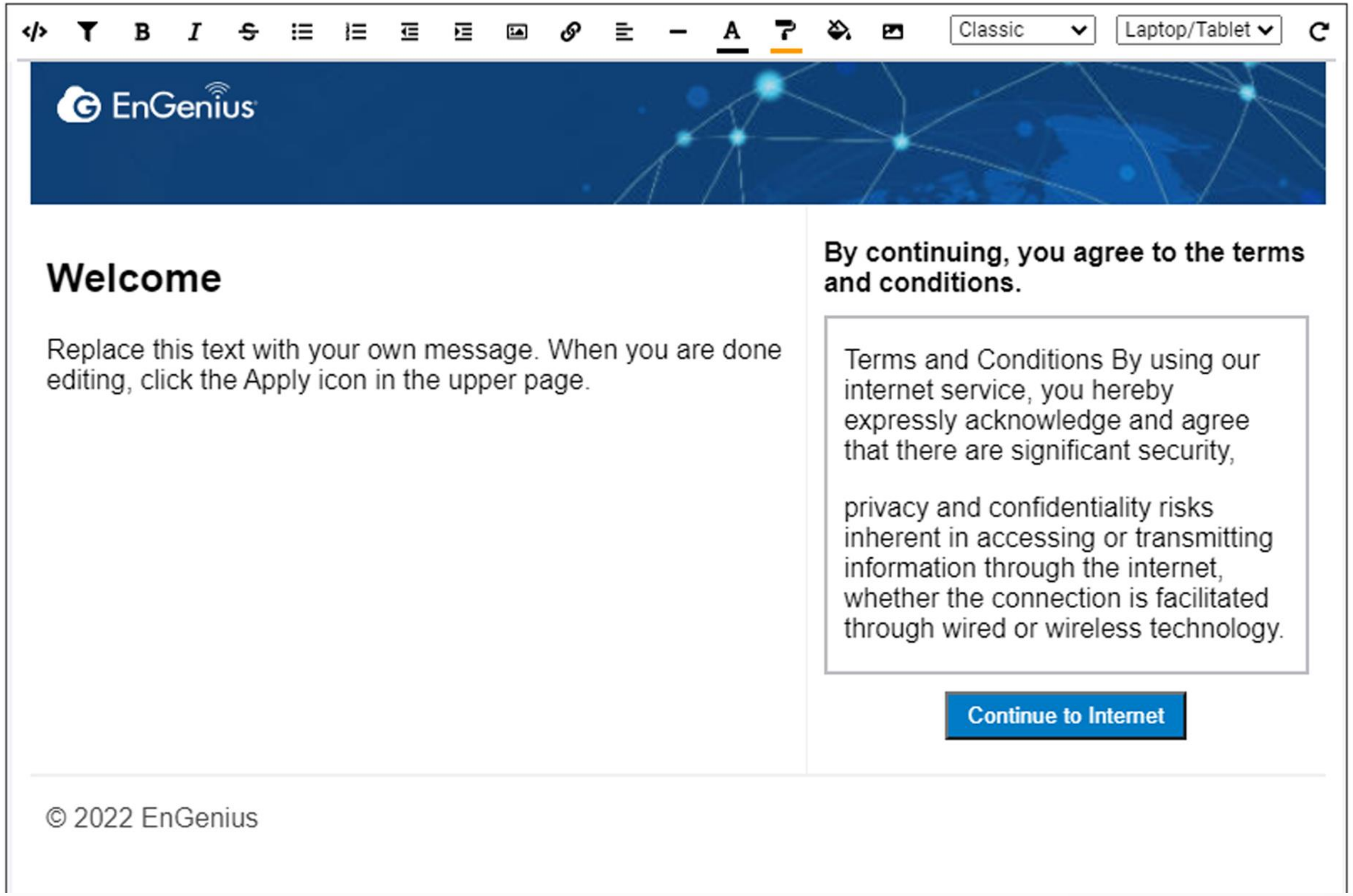
● Auto Generation
○ Manual Entry: User ID and Password

SSID tab - Captive portal – Authentication types (3)

- Social Login - simple authentication option using social media accounts
- Facebook Wi-Fi - full Facebook Wi-Fi integration, including Instagram authentication
- my LDAP server - external LDAP server
- Active Directory - Windows Active Directory authentication
- Google LDAP - Google Secure LDAP service

SSID tab - Splash Page

The EnGenius Splash Page is fully customizable in a WYSIWYG format. Views can be previewed in a mobile or laptop format. For further customization, an HTML editor is also available as well as a redirection for an external splash page useful for 3rd party hotspot gateway portal integrations.



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,

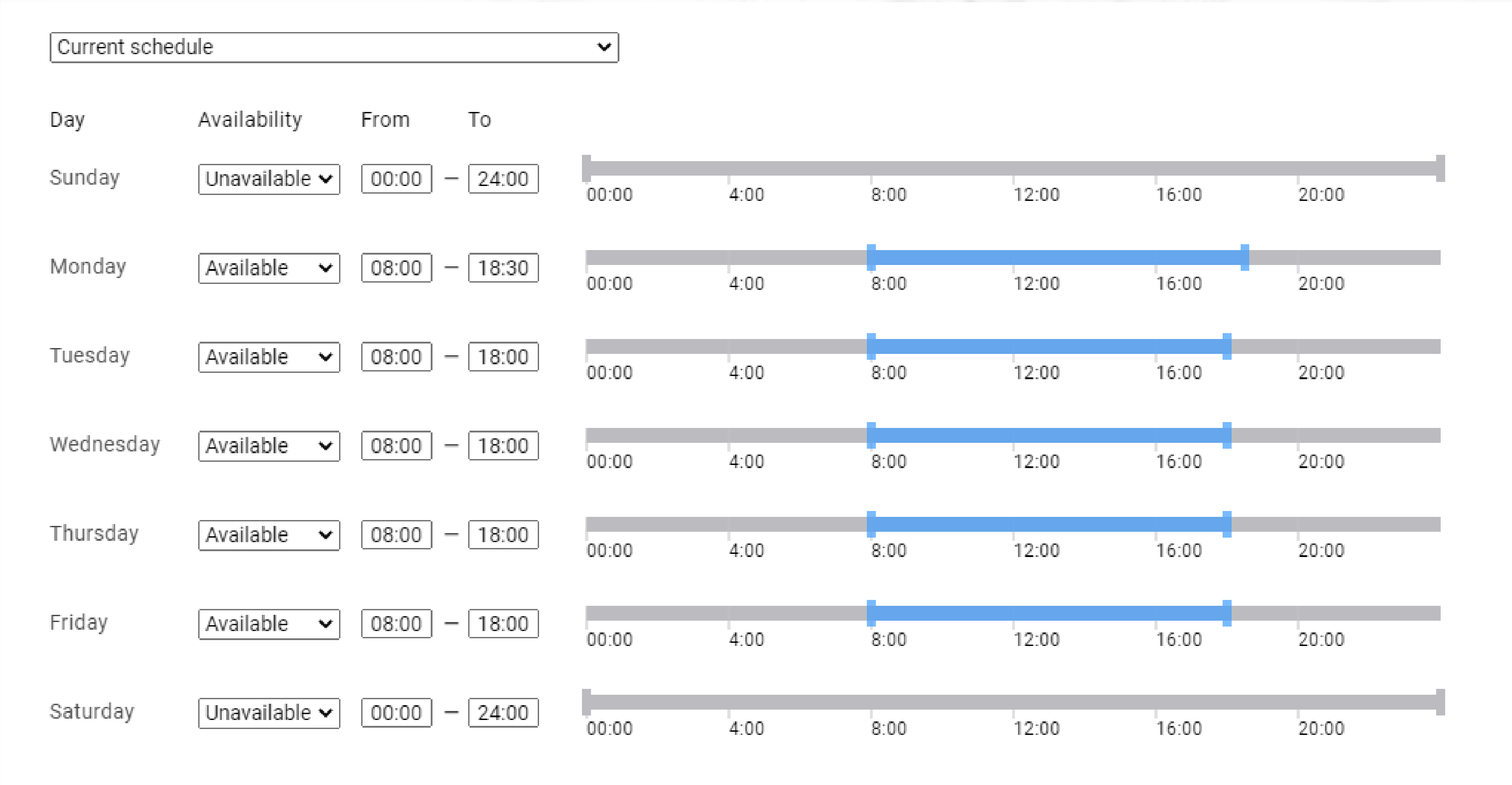
privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology.

© 2022 EnGenius

SSID tab - SSID Scheduler

To prevent unnecessary connections outside operating hours, or for allowing access only on a specific timeslot, scheduling can be done per SSID.

The SSID is disabled, and wireless clients will get disconnected on the offline periods.



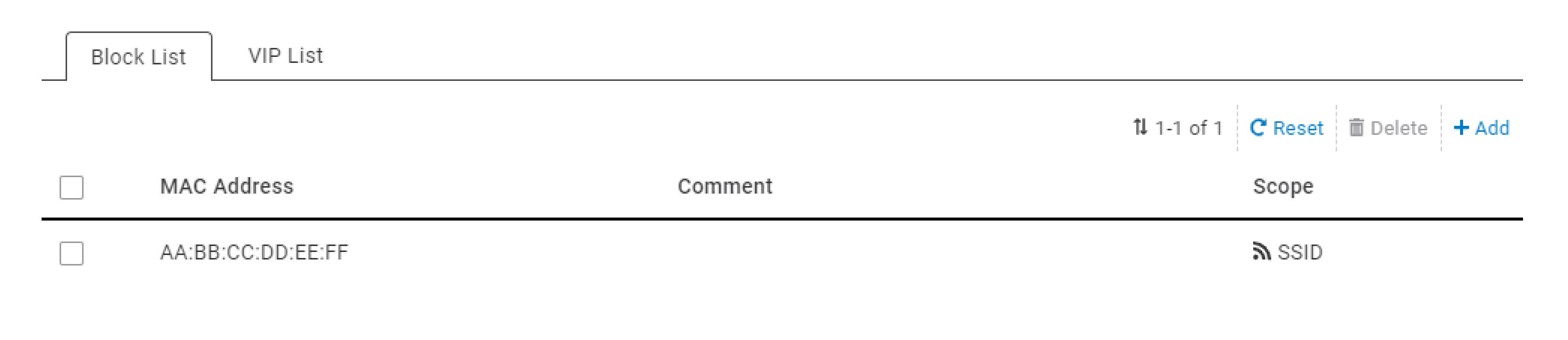
Current schedule

Day	Availability	From		To
Sunday	Unavailable	00:00	–	24:00
Monday	Available	08:00	–	18:30
Tuesday	Available	08:00	–	18:00
Wednesday	Available	08:00	–	18:00
Thursday	Available	08:00	–	18:00
Friday	Available	08:00	–	18:00
Saturday	Unavailable	00:00	–	24:00

SSID tab - Access control

The Access Control serves as two functions, a Block List and VIP List

- Block List - blocks all wireless devices on the list either on the SSID or Network-wide
- VIP List - the VIP List functions in two ways:
    - Wireless devices - such as printers or smart devices which are not able to authenticate on a captive portal will be allowed to bypass the splash page when tagged as VIPs.
    - Wired devices - registered as VIPs will be whitelisted on the network to allow access from wireless clients even when L2 Isolation is enabled.



□	MAC Address	Comment	Scope
□	AA:BB:CC:DD:EE:FF		SSID

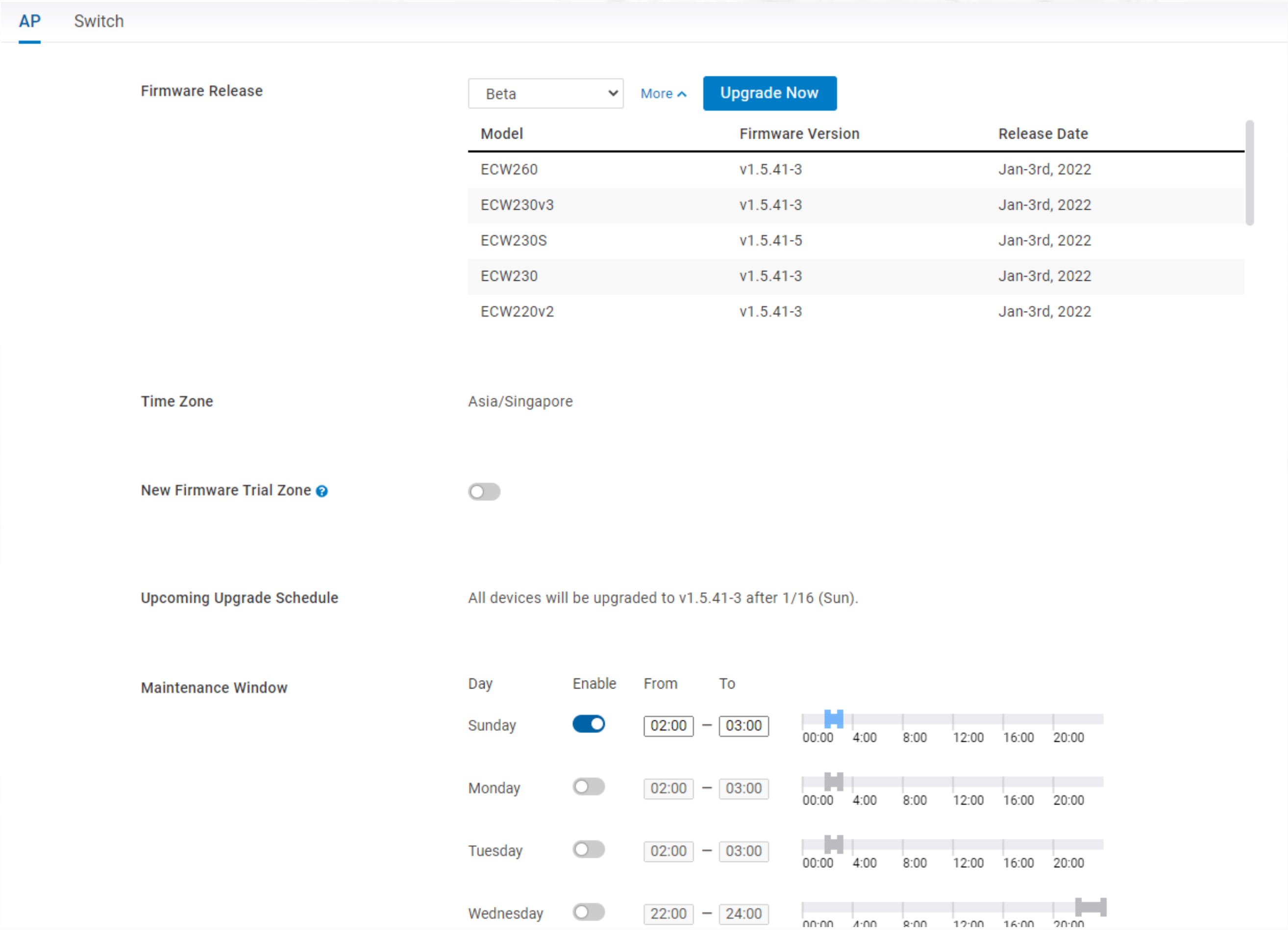
External Splash Page Integration

When integrating with an external splash page, or 3rd party hotspot gateway provider, parameters may need to be customized to match.

See https://docs.engenius.ai/cloud-white-papers/captive-portal/external-splash-page

Firmware management

EnGenius Cloud makes it simple to manage firmware on Cloud devices. When a Cloud device, added on the Network, gains internet access, EnGenius Cloud will push the latest firmware and trigger an auto-update.



Firmware Release: Beta

Model	Firmware Version	Release Date
ECW260	v1.5.41-3	Jan-3rd, 2022
ECW230v3	v1.5.41-3	Jan-3rd, 2022
ECW230S	v1.5.41-5	Jan-3rd, 2022
ECW230	v1.5.41-3	Jan-3rd, 2022
ECW220v2	v1.5.41-3	Jan-3rd, 2022

Time Zone: Asia/Singapore

New Firmware Trial Zone ○

Upcoming Upgrade Schedule: All devices will be upgraded to v1.5.41-3 after 1/16 (Sun).

Maintenance Window

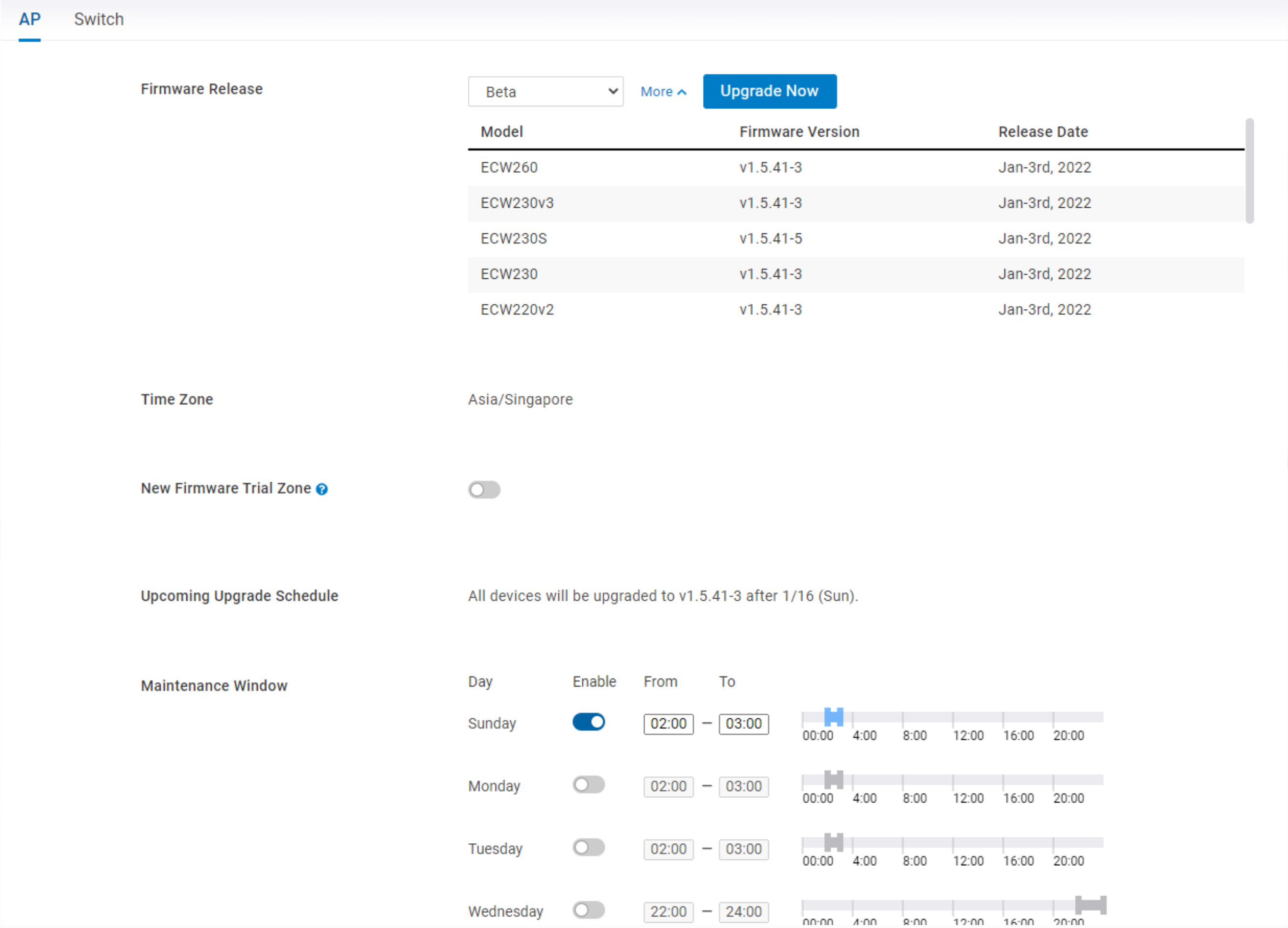
Day	Enable	From	To
Sunday	●	02:00	03:00
Monday	○	02:00	03:00
Tuesday	○	02:00	03:00
Wednesday	○	22:00	24:00

Firmware management (2)

The firmware release selection allows options for the following:

- Stable Release
- Beta Release
- Previous Stable Release

The firmware scheduler has separate tabs for APs and switches, this provides flexibility in running auto-firmware updates. The scheduler follows the Network's time zone.



Firmware Release: Beta

Model	Firmware Version	Release Date
ECW260	v1.5.41-3	Jan-3rd, 2022
ECW230v3	v1.5.41-3	Jan-3rd, 2022
ECW230S	v1.5.41-5	Jan-3rd, 2022
ECW230	v1.5.41-3	Jan-3rd, 2022
ECW220v2	v1.5.41-3	Jan-3rd, 2022

Time Zone: Asia/Singapore

New Firmware Trial Zone ○

Upcoming Upgrade Schedule: All devices will be upgraded to v1.5.41-3 after 1/16 (Sun).

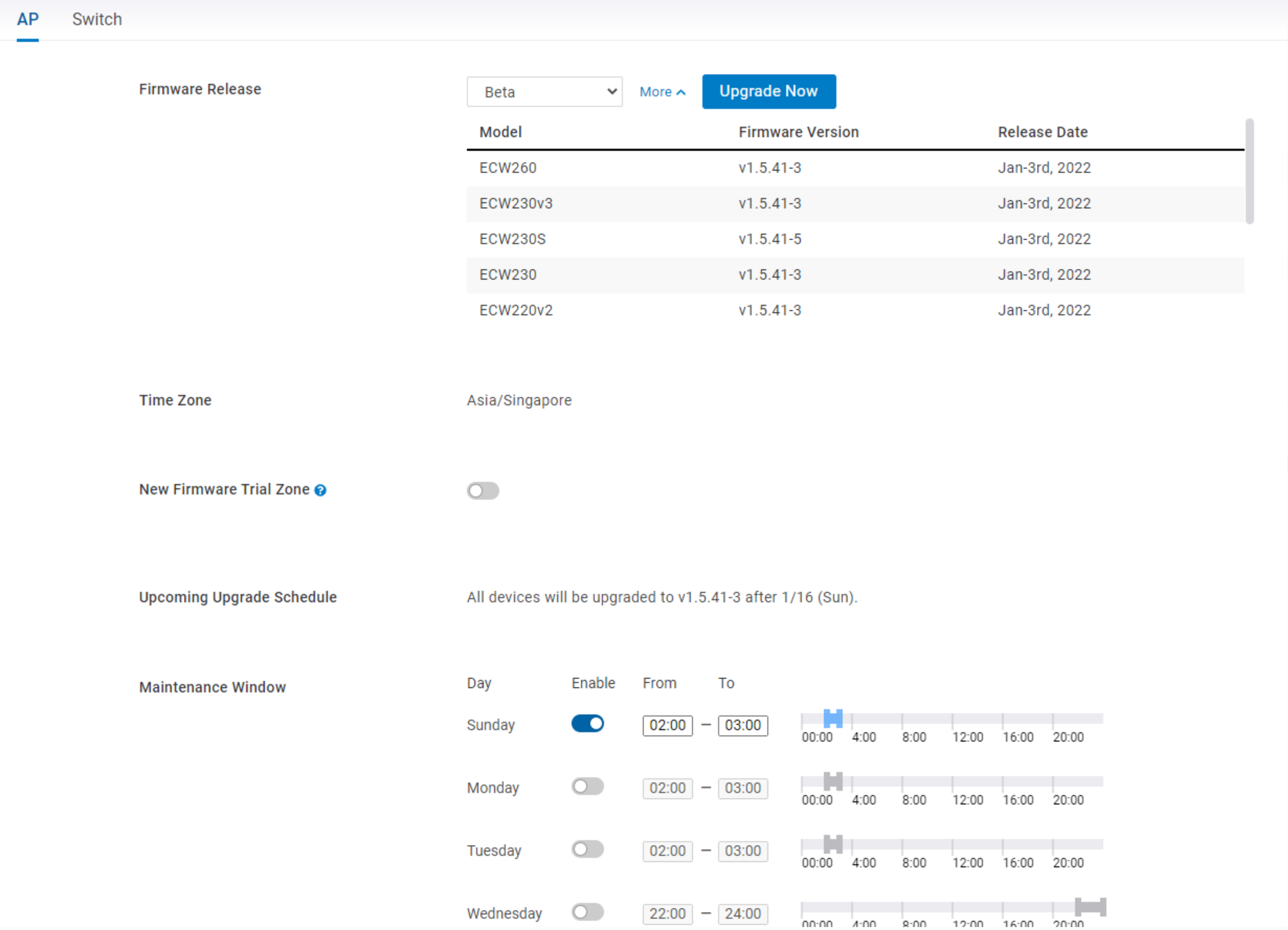
Maintenance Window

Day	Enable	From	To
Sunday	●	02:00	03:00
Monday	○	02:00	03:00
Tuesday	○	02:00	03:00
Wednesday	○	22:00	24:00

Firmware management - New Firmware Trial Zone

This function allows the network administrator to pick the selected devices to upgrade firmware as scheduled, and other will not be upgraded within the first 21 days after the firmware was released.

If the firmware has any issue during the trial period, the admin can roll back to previous version by removing the devices from the Trial Zone.



Firmware Release: Beta

Model	Firmware Version	Release Date
ECW260	v1.5.41-3	Jan-3rd, 2022
ECW230v3	v1.5.41-3	Jan-3rd, 2022
ECW230S	v1.5.41-5	Jan-3rd, 2022
ECW230	v1.5.41-3	Jan-3rd, 2022
ECW220v2	v1.5.41-3	Jan-3rd, 2022

Time Zone: Asia/Singapore

New Firmware Trial Zone: ○

Upcoming Upgrade Schedule: All devices will be upgraded to v1.5.41-3 after 1/16 (Sun).

Maintenance Window

Day	Enable	From	To
Sunday	●	02:00	03:00
Monday	○	02:00	03:00
Tuesday	○	02:00	03:00
Wednesday	○	22:00	24:00

Multitenancy

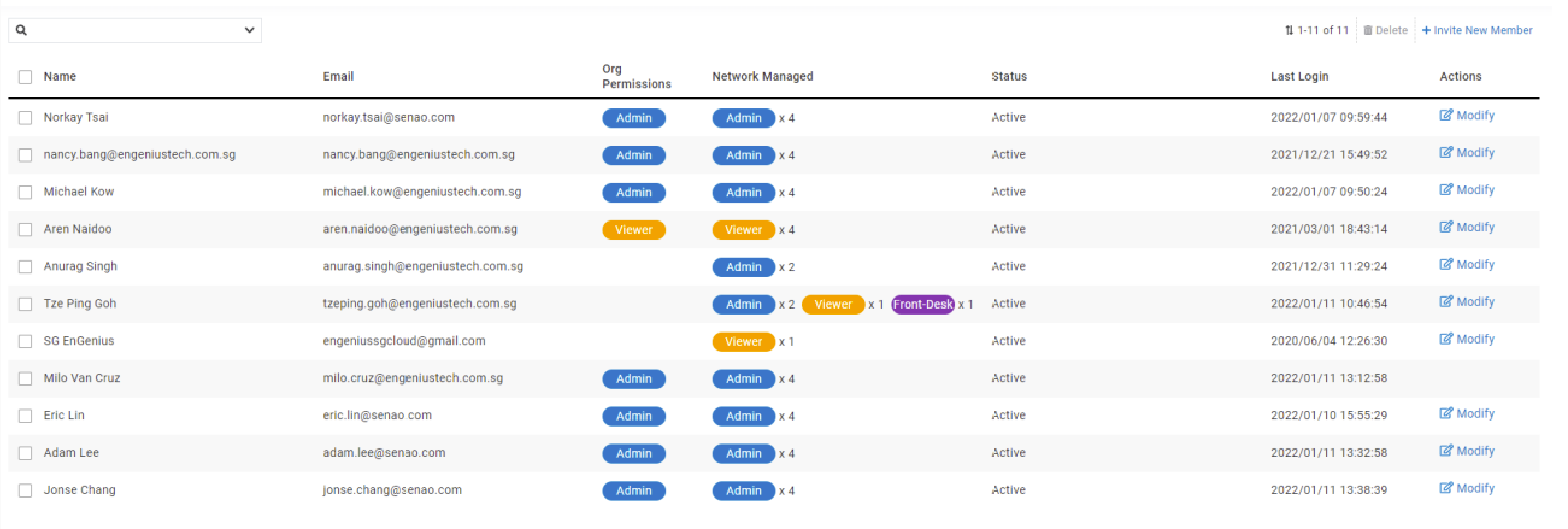
The larger the organization, the more network administrators are required depending on how the network is segregated.

EnGenius Cloud team members page allows for easy management of multitenancy for each organization.

Each member can be set with the following permissions:

- Admin – has full control on the organization, and/or specific networks, and/or the front-desk portal.
- Viewer – can view the organization, and/or specific networks, but will not be able to apply any configuration or run diagnostic tests.
- Front-desk – has access to the front-desk portal for voucher creation and management.

Multitenancy (2)



□	Name	Email	Org Permissions	Network Managed	Status	Last Login	Actions
□	Norkay Tsai	norkay.tsai@senao.com	Admin	Admin x 4	Active	2022/01/07 09:59:44	Modify
□	nancy.bang@engeniustech.com.sg	nancy.bang@engeniustech.com.sg	Admin	Admin x 4	Active	2021/12/21 15:49:52	Modify
□	Michael Kow	michael.kow@engeniustech.com.sg	Admin	Admin x 4	Active	2022/01/07 09:50:24	Modify
□	Aren Naidoo	aren.naidoo@engeniustech.com.sg	Viewer	Viewer x 4	Active	2021/03/01 18:43:14	Modify
□	Anurag Singh	anurag.singh@engeniustech.com.sg		Admin x 2	Active	2021/12/31 11:29:24	Modify
□	Tze Ping Goh	tzeping.goh@engeniustech.com.sg		Admin x 2 Viewer x 1 Front-Desk x 1	Active	2022/01/11 10:46:54	Modify
□	SG EnGenius	engeniussgcloud@gmail.com		Viewer x 1	Active	2020/06/04 12:26:30	Modify
□	Milo Van Cruz	milo.cruz@engeniustech.com.sg	Admin	Admin x 4	Active	2022/01/11 13:12:58	
□	Eric Lin	eric.lin@senao.com	Admin	Admin x 4	Active	2022/01/10 15:55:29	Modify
□	Adam Lee	adam.lee@senao.com	Admin	Admin x 4	Active	2022/01/11 13:32:58	Modify
□	Jonse Chang	jonse.chang@senao.com	Admin	Admin x 4	Active	2022/01/11 13:38:39	Modify

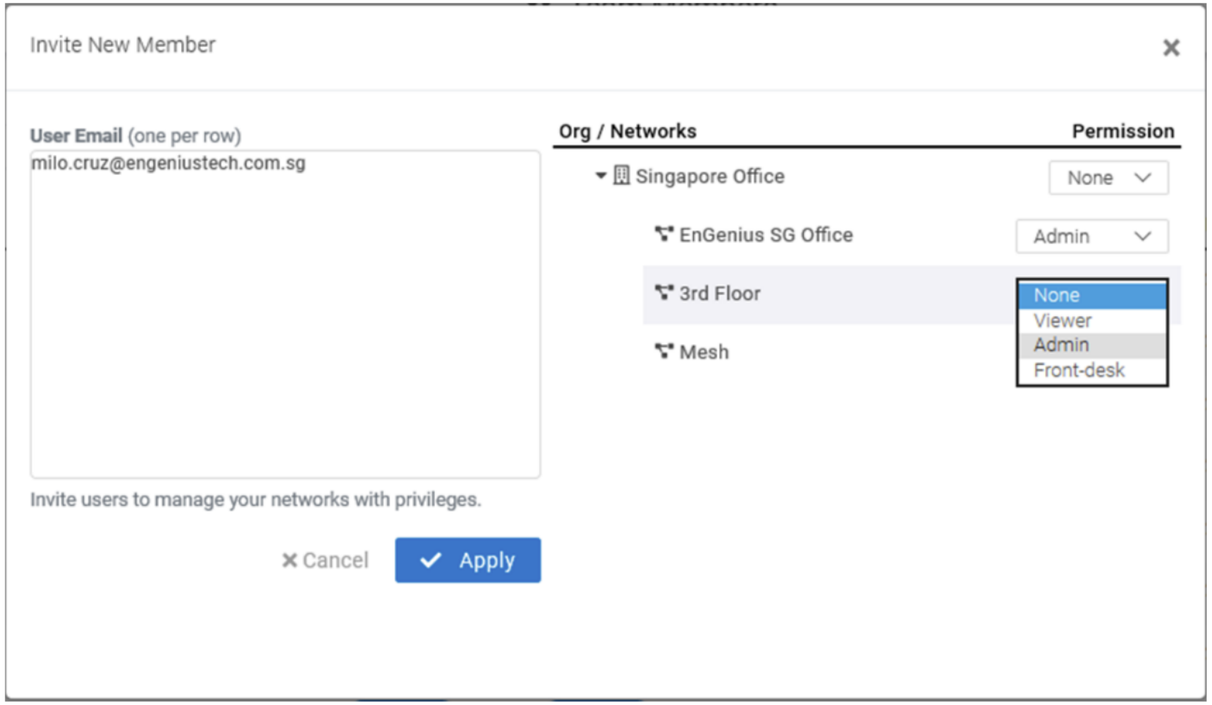
Multitenancy (3)

Team member settings can be modified at anytime.

To add new members, a valid email address must be keyed in. Multiple email addresses may be entered at once. Permissions can be selected and applied to the whole organization, or specific networks.

Once applied, the added individual will receive a confirmation email, with a link to sing-in on the cloud portal.

This will only work if the invited person has an existing Engenius cloud account.



Invite New Member

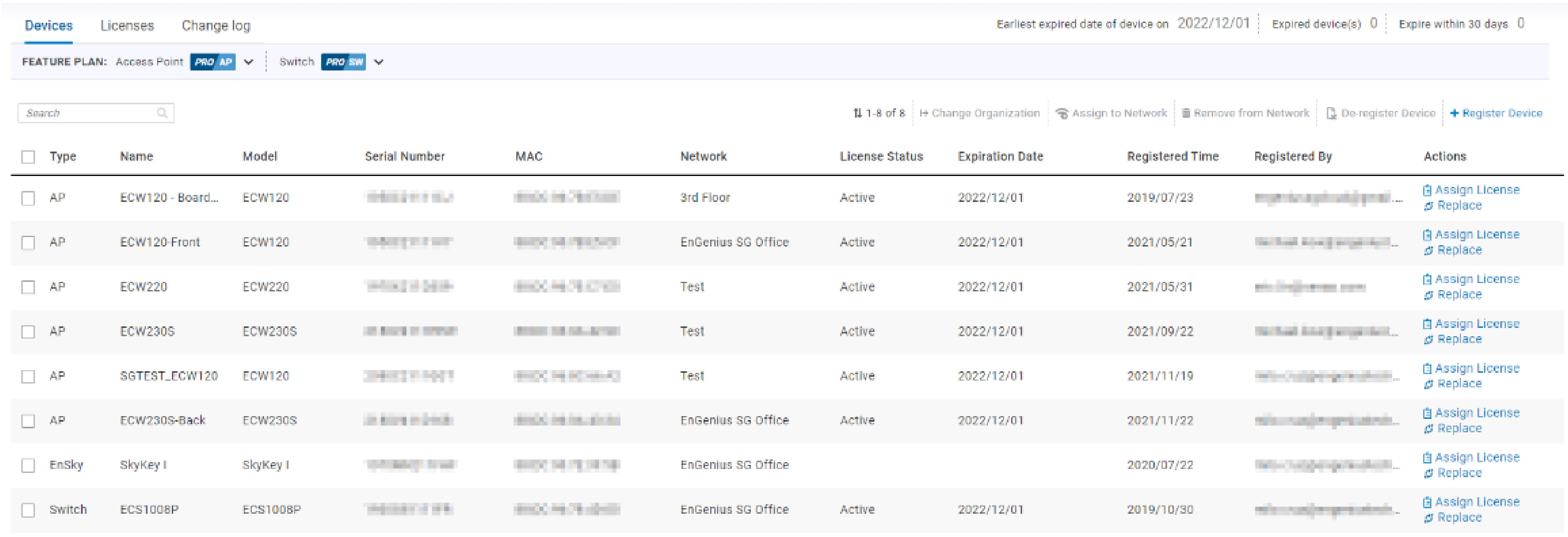
User Email (one per row)
milo.cruz@engeniustech.com.sg

Invite users to manage your networks with privileges.

Org / Networks	Permission
Singapore Office	None
EnGenius SG Office	Admin
3rd Floor	None
Mesh	

Device inventory

Keeping tabs on your devices may be time-consuming and rather difficult with a decentralized system; however, with the EnGenius Cloud, full information is provided online for your reference, if the need arises



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

FEATURE PLAN: Access Point PRO AP | Switch PRO SW

1-8 of 8 | Change Organization | Assign to Network | Remove from Network | De-register Device | + Register Device

□	Type	Name	Model	Serial Number	MAC	Network	License Status	Expiration Date	Registered Time	Registered By	Actions
□	AP	ECW120 - Board...	ECW120	[redacted]	[redacted]	3rd Floor	Active	2022/12/01	2019/07/23	[redacted]	Assign License Replace
□	AP	ECW120-Front	ECW120	[redacted]	[redacted]	EnGenius SG Office	Active	2022/12/01	2021/05/21	[redacted]	Assign License Replace
□	AP	ECW220	ECW220	[redacted]	[redacted]	Test	Active	2022/12/01	2021/05/31	[redacted]	Assign License Replace
□	AP	ECW230S	ECW230S	[redacted]	[redacted]	Test	Active	2022/12/01	2021/09/22	[redacted]	Assign License Replace
□	AP	SGTEST_ECW120	ECW120	[redacted]	[redacted]	Test	Active	2022/12/01	2021/11/19	[redacted]	Assign License Replace
□	AP	ECW230S-Back	ECW230S	[redacted]	[redacted]	EnGenius SG Office	Active	2022/12/01	2021/11/22	[redacted]	Assign License Replace
□	EnSky	SkyKey I	SkyKey I	[redacted]	[redacted]	EnGenius SG Office			2020/07/22	[redacted]	Assign License Replace
□	Switch	ECS1008P	ECS1008P	[redacted]	[redacted]	EnGenius SG Office	Active	2022/12/01	2019/10/30	[redacted]	Assign License Replace

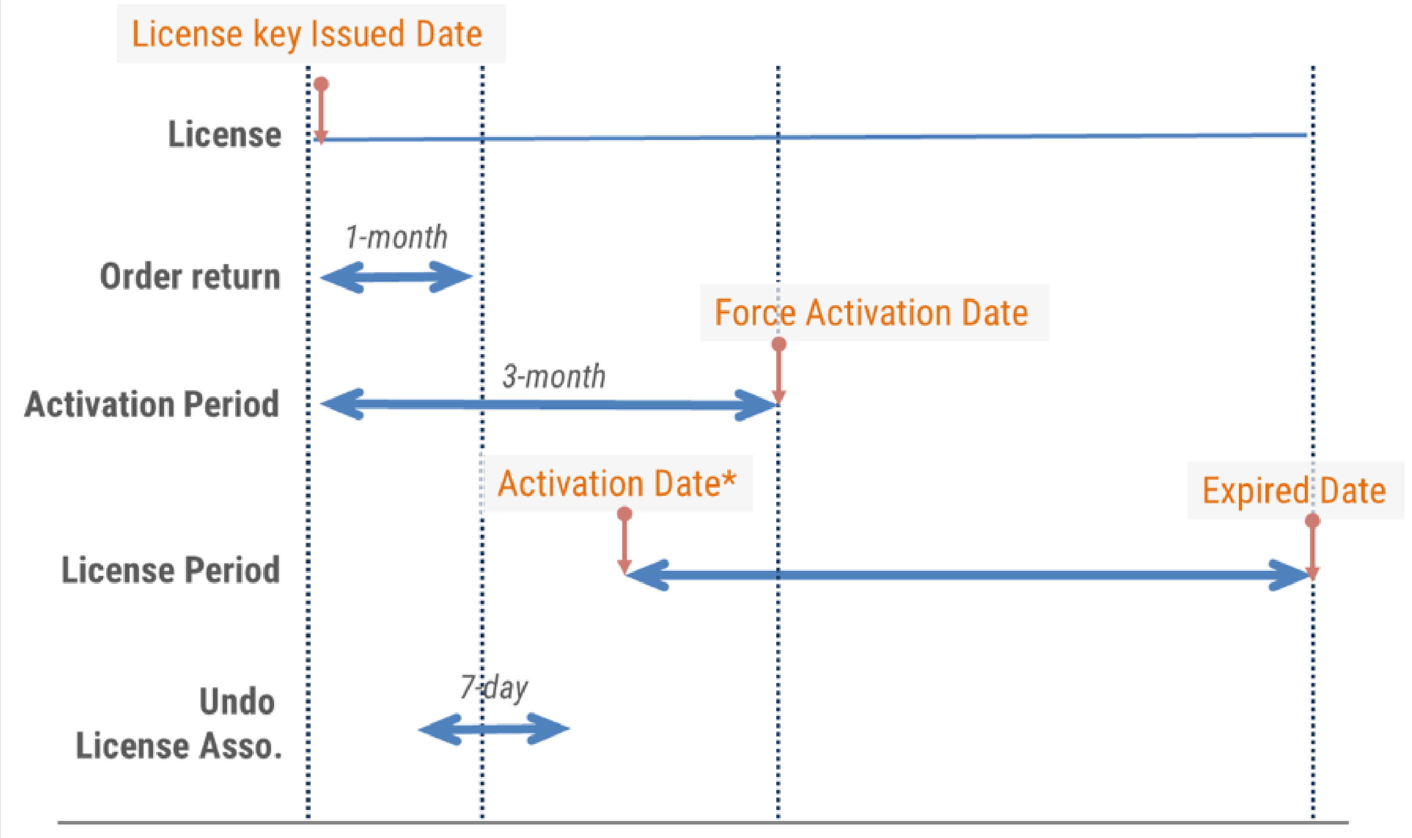
EnGenius Cloud Inventory

License management

Managing EnGenius Cloud Pro licenses is as simple as managing the device inventory.

See https://www.engenius.ai/cloud/licenses/

Here is a summary of the key things to remember when purchasing or associating licenses:



License facts

- All devices have a 1-year trial license, which will only be revoked through RMA or replacement.
- Pro licenses are permanently attached to a device, unless RMA or replacement is processed. In which case the attached Pro license will be transferred to the replacement device.
- De-registering a device will remove and void the Pro-license.
- Devices with licenses associated can be moved to another organization if both organizations are managed by the same administrator.

Terms	Descriptions
License key issue date	The date when the license is issued and emailed
Activation date	The date a license-associated device is assigned to a managed network
Forced-activation date	The date that the license is auto activated because of no activation on any device after 90 days of being issued
Expiration date	For a licensed device, the expired date means the end of the license duration
Order return	The license order can be returned within one month after the license key is issued. (This is subject to the operation of each region. Please contact your local EnGenius office or reseller)
Undo license association	You can disassociate a license from a device within seven days after it was associated

Monitoring - topics

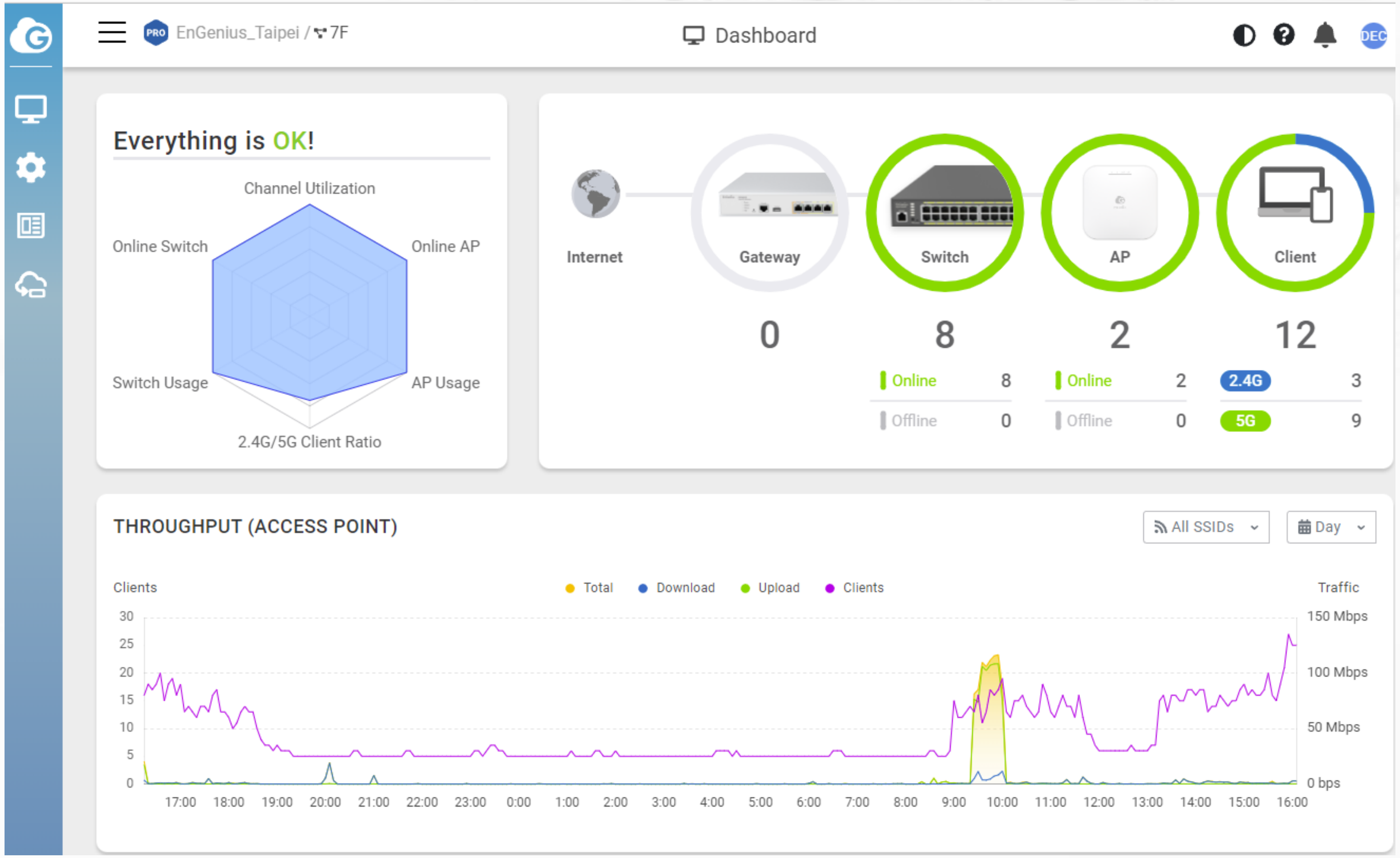
- Dashboard
- Switches
- Topology View
- Client list
- Reports
- Notifications & Alerts
- SNMP Monitoring
- API Integration
- Syslog & Traffic Logs
- Presence reporting

Dashboard

The EnGenius Cloud Dashboard provides quick information on the overall health of your Organization, or specific Networks:

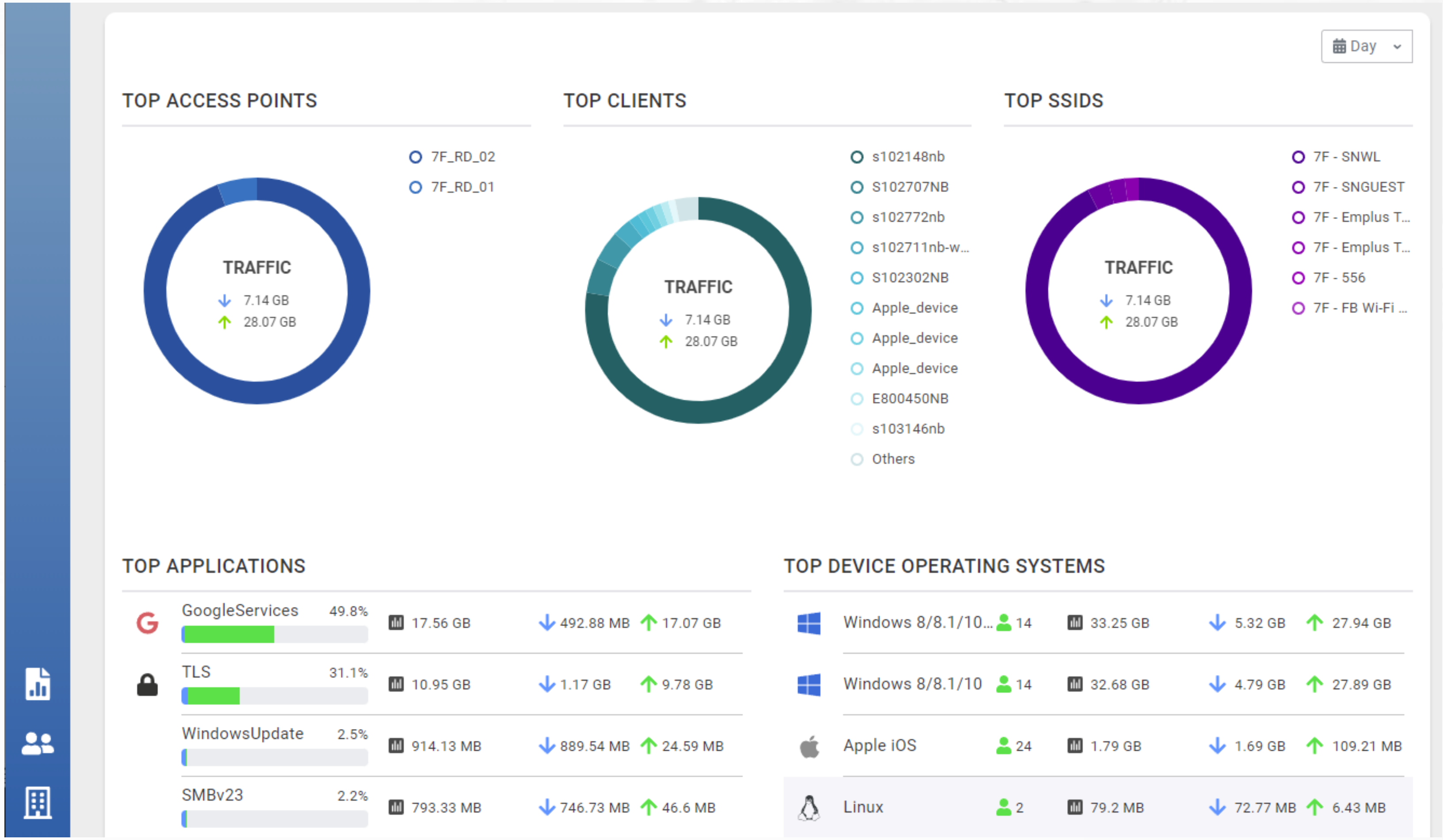
- Device count with online/offline status.
- Client count per radio.

The radar graph highlights immediate issues on the AP and switch status, channel utilization, and CPU usage.



Dashboard (2)

Bandwidth usage is also available on the main page.



TOP ACCESS POINTS

TOP CLIENTS

TOP SSIDS

TOP APPLICATIONS

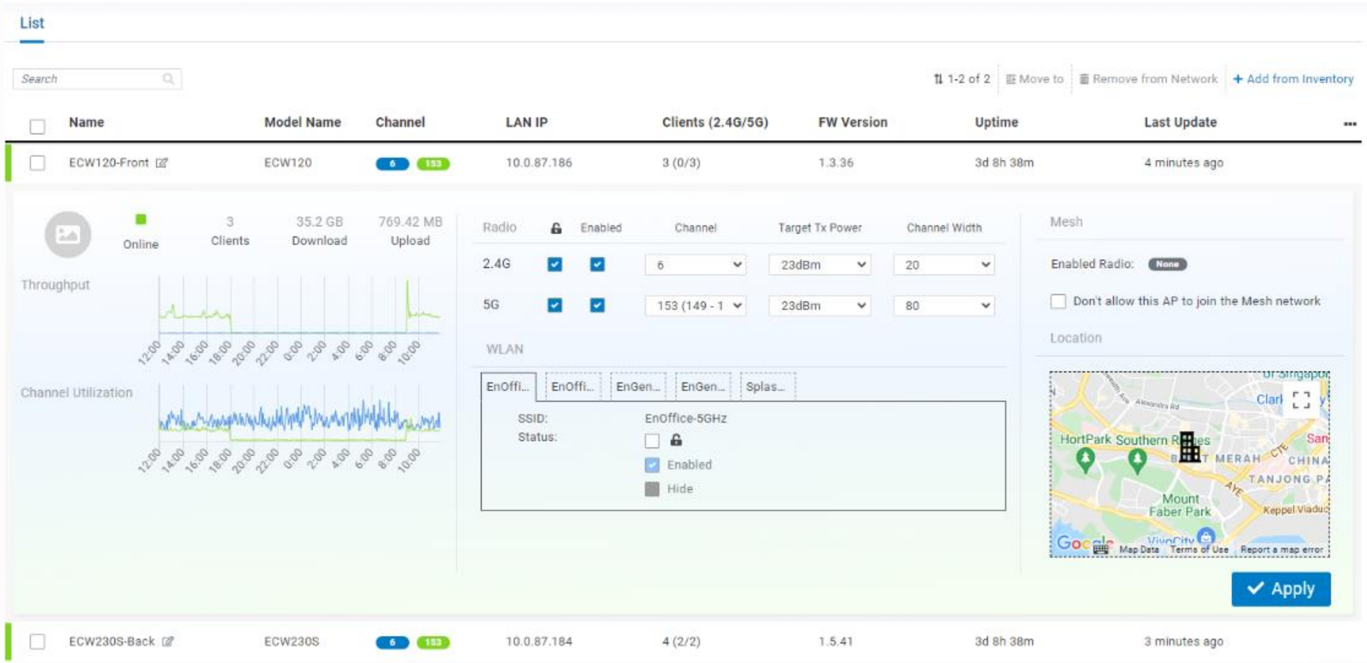
GoogleServices	49.8%	17.56 GB	↓ 492.88 MB	↑ 17.07 GB
TLS	31.1%	10.95 GB	↓ 1.17 GB	↑ 9.78 GB
WindowsUpdate	2.5%	914.13 MB	↓ 889.54 MB	↑ 24.59 MB
SMBv23	2.2%	793.33 MB	↓ 746.73 MB	↑ 46.6 MB

TOP DEVICE OPERATING SYSTEMS

Windows 8/8.1/10...	14	33.25 GB	↓ 5.32 GB	↑ 27.94 GB
Windows 8/8.1/10	14	32.68 GB	↓ 4.79 GB	↑ 27.89 GB
Apple iOS	24	1.79 GB	↓ 1.69 GB	↑ 109.21 MB
Linux	2	79.2 MB	↓ 72.77 MB	↑ 6.43 MB

APs – list and quick view panel

When monitoring devices, a Quickview panel is expandable for checking AP settings, or utilization.



List

Search

⇅ 1-2 of 2 | Move to | Remove from Network | + Add from Inventory

☐	Name	Model Name	Channel	LAN IP	Clients (2.4G/5G)	FW Version	Uptime	Last Update	•••
☐	ECW120-Front	ECW120	6 153	10.0.87.186	3 (0/3)	1.3.36	3d 8h 38m	4 minutes ago	
☐	ECW230S-Back	ECW230S	6 153	10.0.87.184	4 (2/2)	1.5.41	3d 8h 38m	3 minutes ago	

Online | 3 Clients | 35.2 GB Download | 769.42 MB Upload

Radio	🔓	Enabled	Channel	Target Tx Power	Channel Width
2.4G	☑	☑	6	23dBm	20
5G	☑	☑	153 (149 - 1	23dBm	80

WLAN

EnOffi... | EnOffi... | EnGen... | EnGen... | Splas...

SSID: EnOffice-5GHz

Status: ☐ 🔓

☑ Enabled

☐ Hide

Mesh

Enabled Radio: None

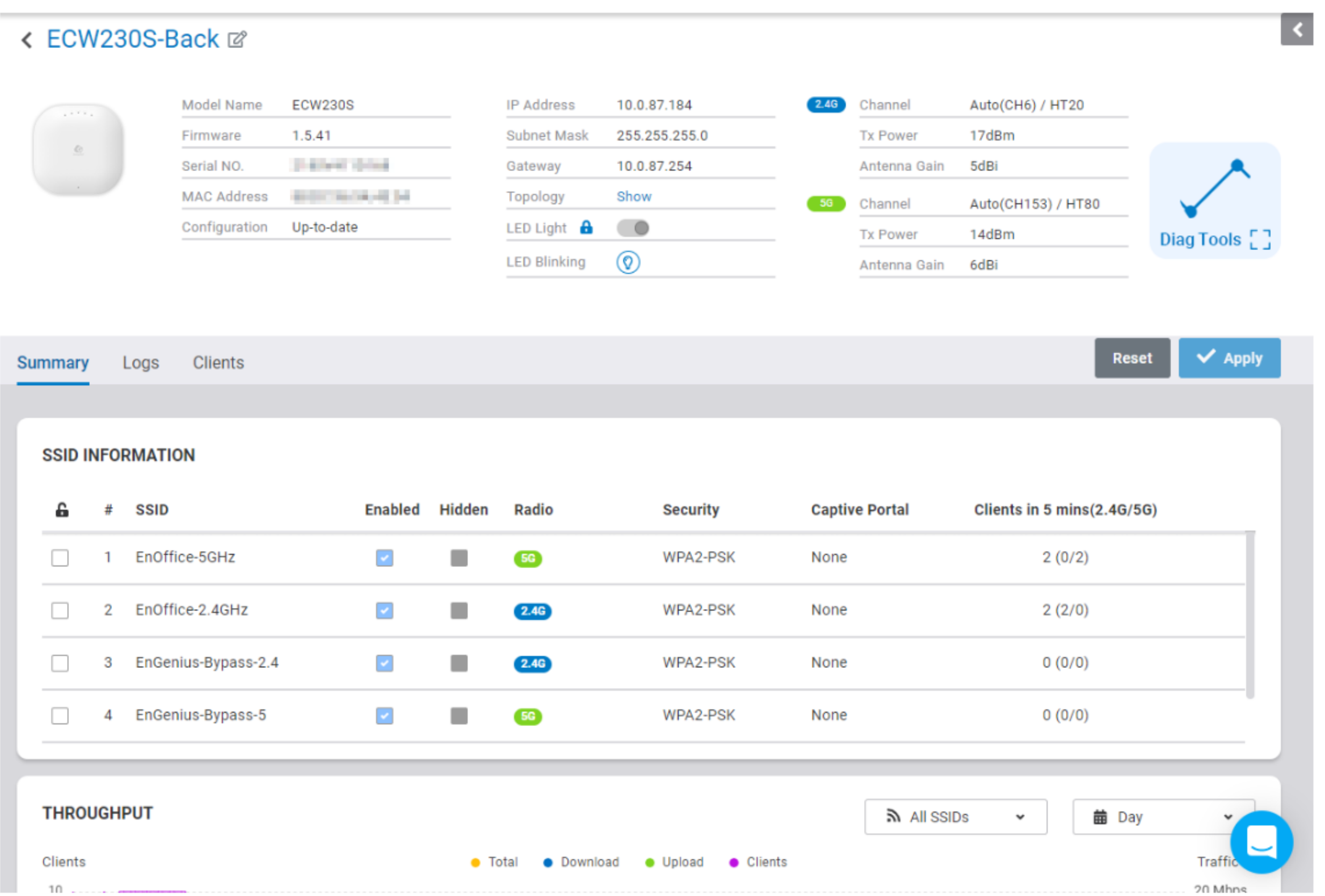
☐ Don't allow this AP to join the Mesh network

Location

✓ Apply

APs - details page

The AP details page provides full information on the unit as well as options to override.



ECW230S-Back

Model Name	ECW230S	IP Address	10.0.87.184	2.4G Channel	Auto(CH6) / HT20
Firmware	1.5.41	Subnet Mask	255.255.255.0	Tx Power	17dBm
Serial NO.	[redacted]	Gateway	10.0.87.254	Antenna Gain	5dBi
MAC Address	[redacted]	Topology	Show	5G Channel	Auto(CH153) / HT80
Configuration	Up-to-date	LED Light		Tx Power	14dBm
		LED Blinking		Antenna Gain	6dBi

SSID INFORMATION

	#	SSID	Enabled	Hidden	Radio	Security	Captive Portal	Clients in 5 mins(2.4G/5G)
☐	1	EnOffice-5GHz	☑	☐	5G	WPA2-PSK	None	2 (0/2)
☐	2	EnOffice-2.4GHz	☑	☐	2.4G	WPA2-PSK	None	2 (2/0)
☐	3	EnGenius-Bypass-2.4	☑	☐	2.4G	WPA2-PSK	None	0 (0/0)
☐	4	EnGenius-Bypass-5	☑	☐	5G	WPA2-PSK	None	0 (0/0)

THROUGHPUT

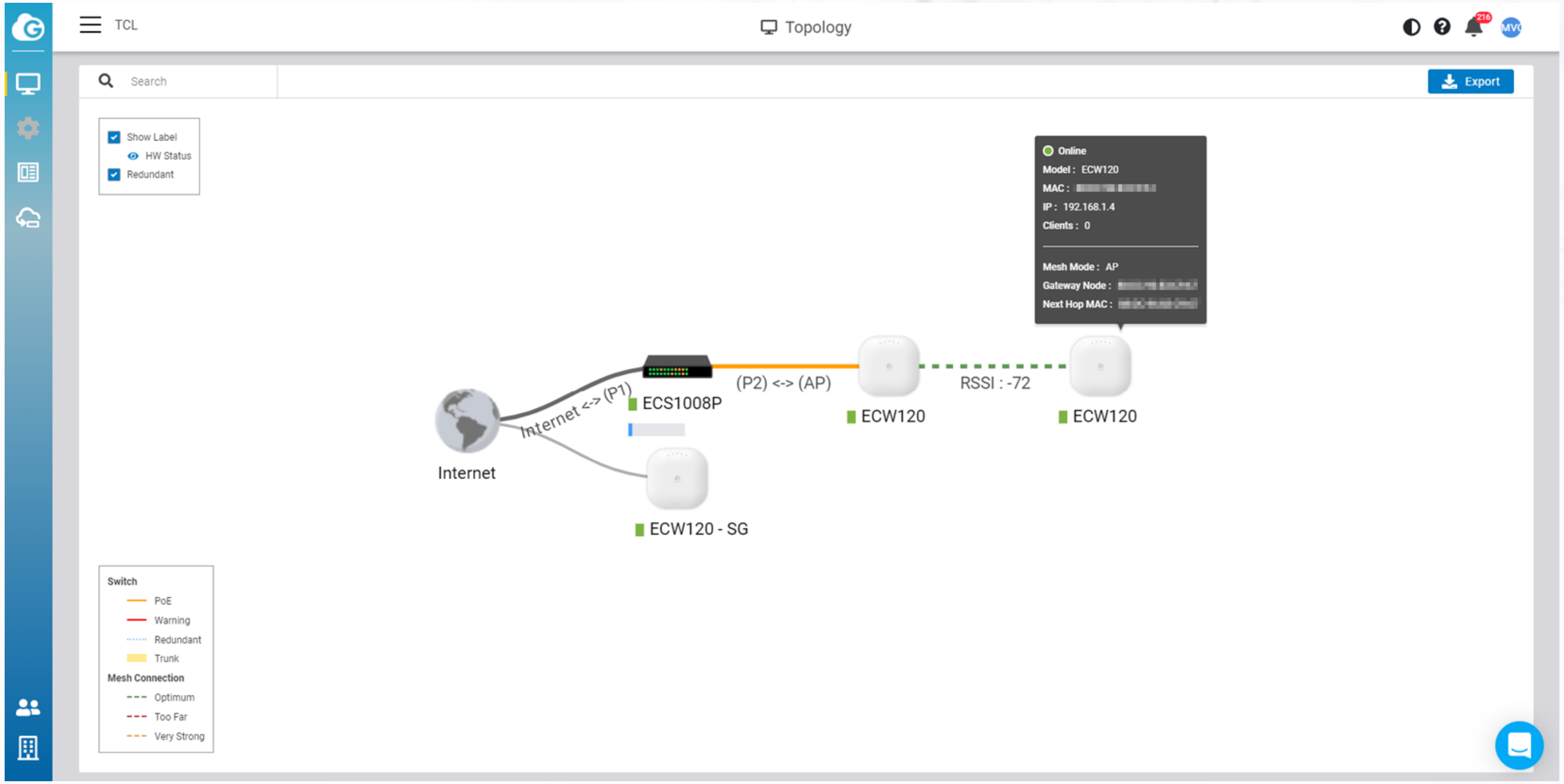
Topology view

EnGenius topology view provides details on the network connection layout of the cloud devices. Information available are:

- Port Connections
- Uplink
- PoE information
- Redundancy links
- Trunks
- Mesh topology
- Device information

With a PRO license, 3rd party devices connected directly on ECS Switches will be displayed.

(!) LLDP should be supported for 3rd party devices to appear on Topology View.



☑ Show Label
HW Status
☑ Redundant

Online
Model : ECW120
MAC : [redacted]
IP : 192.168.1.4
Clients : 0

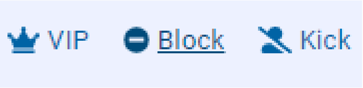
Mesh Mode : AP
Gateway Node : [redacted]
Next Hop MAC : [redacted]

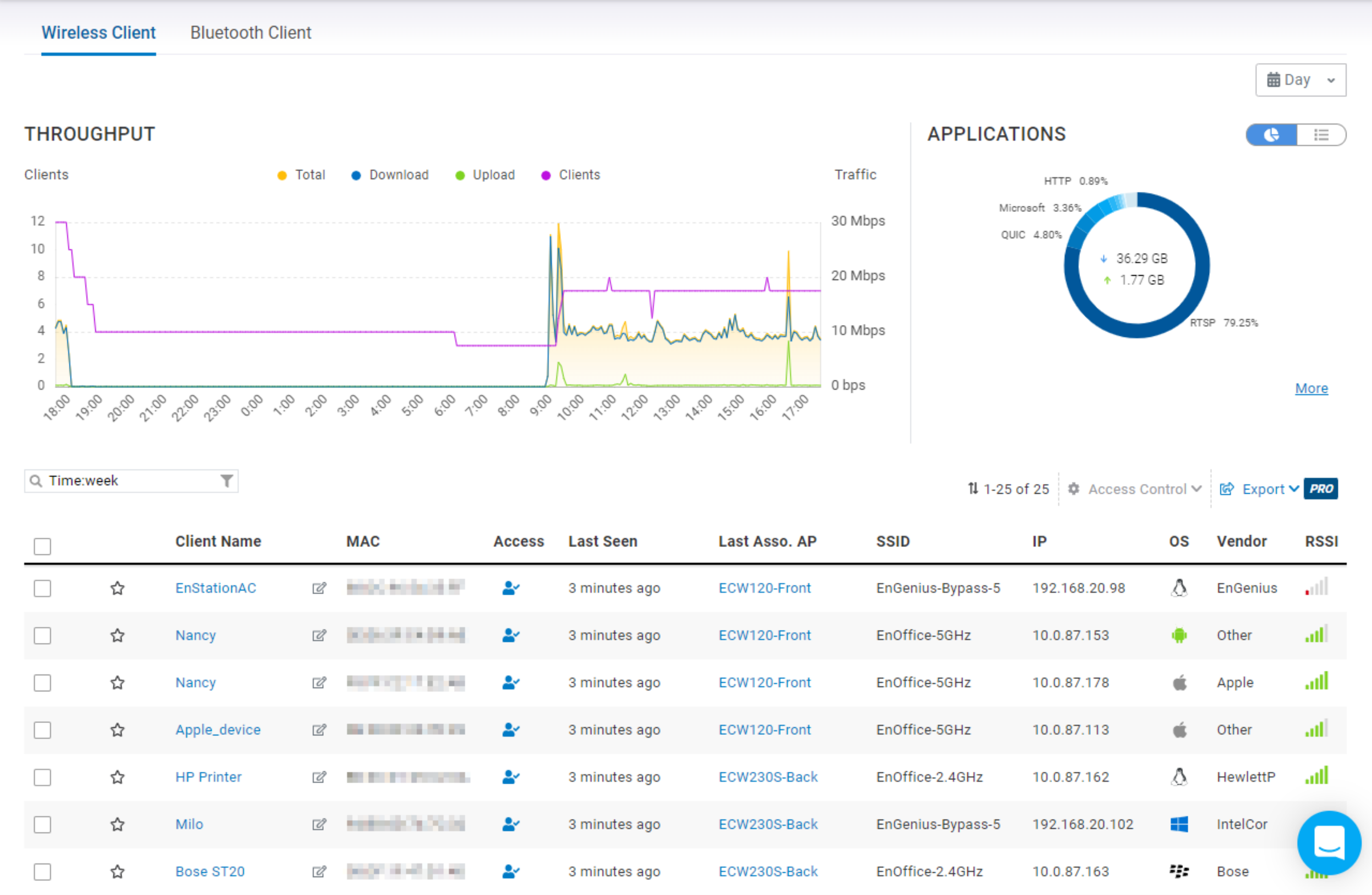
Switch
PoE
Warning
Redundant
Trunk
Mesh Connection
Optimum
Too Far
Very Strong

Client list

The Client List will be populated and stored on the Cloud, regardless of the number of clients on the Org or Network.

Access Control can directly be triggered for individual clients on this page.

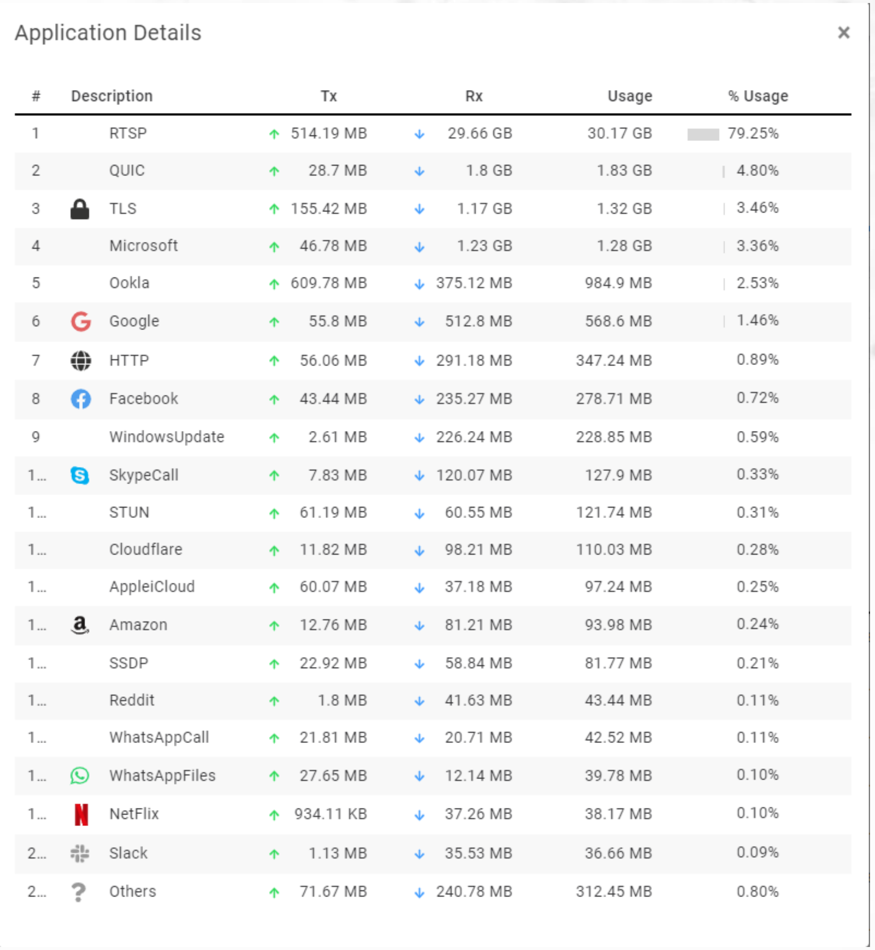




□		Client Name		MAC	Access	Last Seen	Last Asso. AP	SSID	IP	OS	Vendor	RSSI
□	☆	EnStationAC	✎	[redacted]	✓	3 minutes ago	ECW120-Front	EnGenius-Bypass-5	192.168.20.98		EnGenius	
□	☆	Nancy	✎	[redacted]	✓	3 minutes ago	ECW120-Front	EnOffice-5GHz	10.0.87.153		Other	
□	☆	Nancy	✎	[redacted]	✓	3 minutes ago	ECW120-Front	EnOffice-5GHz	10.0.87.178		Apple	
□	☆	Apple_device	✎	[redacted]	✓	3 minutes ago	ECW120-Front	EnOffice-5GHz	10.0.87.113		Other	
□	☆	HP Printer	✎	[redacted]	✓	3 minutes ago	ECW230S-Back	EnOffice-2.4GHz	10.0.87.162		HewlettP	
□	☆	Milo	✎	[redacted]	✓	3 minutes ago	ECW230S-Back	EnGenius-Bypass-5	192.168.20.102		IntelCor	
□	☆	Bose ST20	✎	[redacted]	✓	3 minutes ago	ECW230S-Back	EnOffice-2.4GHz	10.0.87.163		Bose	

Client list - Application Analysis

When Application Analysis is enabled on the SSID, the usage details will be displayed here.



Application Details ×

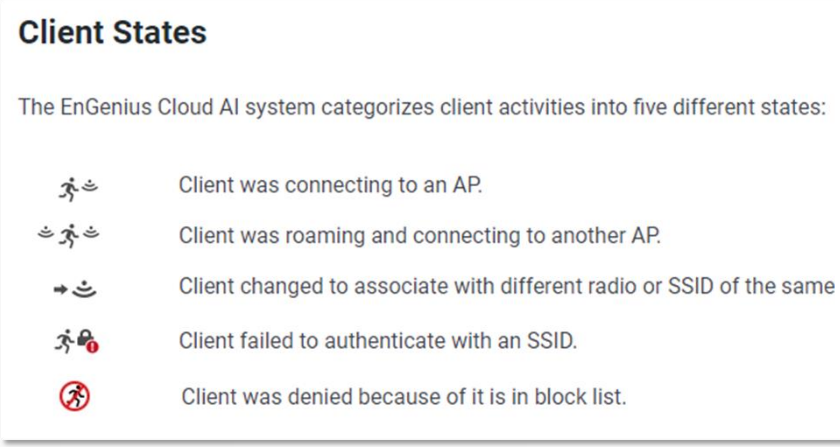
#	Description	Tx	Rx	Usage	% Usage
1	RTSP	↑ 514.19 MB	↓ 29.66 GB	30.17 GB	79.25%
2	QUIC	↑ 28.7 MB	↓ 1.8 GB	1.83 GB	4.80%
3	TLS	↑ 155.42 MB	↓ 1.17 GB	1.32 GB	3.46%
4	Microsoft	↑ 46.78 MB	↓ 1.23 GB	1.28 GB	3.36%
5	Ookla	↑ 609.78 MB	↓ 375.12 MB	984.9 MB	2.53%
6	Google	↑ 55.8 MB	↓ 512.8 MB	568.6 MB	1.46%
7	HTTP	↑ 56.06 MB	↓ 291.18 MB	347.24 MB	0.89%
8	Facebook	↑ 43.44 MB	↓ 235.27 MB	278.71 MB	0.72%
9	WindowsUpdate	↑ 2.61 MB	↓ 226.24 MB	228.85 MB	0.59%
1...	SkypeCall	↑ 7.83 MB	↓ 120.07 MB	127.9 MB	0.33%
1...	STUN	↑ 61.19 MB	↓ 60.55 MB	121.74 MB	0.31%
1...	Cloudflare	↑ 11.82 MB	↓ 98.21 MB	110.03 MB	0.28%
1...	AppleiCloud	↑ 60.07 MB	↓ 37.18 MB	97.24 MB	0.25%
1...	Amazon	↑ 12.76 MB	↓ 81.21 MB	93.98 MB	0.24%
1...	SSDP	↑ 22.92 MB	↓ 58.84 MB	81.77 MB	0.21%
1...	Reddit	↑ 1.8 MB	↓ 41.63 MB	43.44 MB	0.11%
1...	WhatsAppCall	↑ 21.81 MB	↓ 20.71 MB	42.52 MB	0.11%
1...	WhatsAppFiles	↑ 27.65 MB	↓ 12.14 MB	39.78 MB	0.10%
1...	NetFlix	↑ 934.11 KB	↓ 37.26 MB	38.17 MB	0.10%
2...	Slack	↑ 1.13 MB	↓ 35.53 MB	36.66 MB	0.09%
2...	Others	↑ 71.67 MB	↓ 240.78 MB	312.45 MB	0.80%

Client Timeline

Client Timeline is a very useful tool which displays the client journey from the moment a client associating to the SSID, until disconnection.

This tool can greatly reduce probing for wireless client issues.

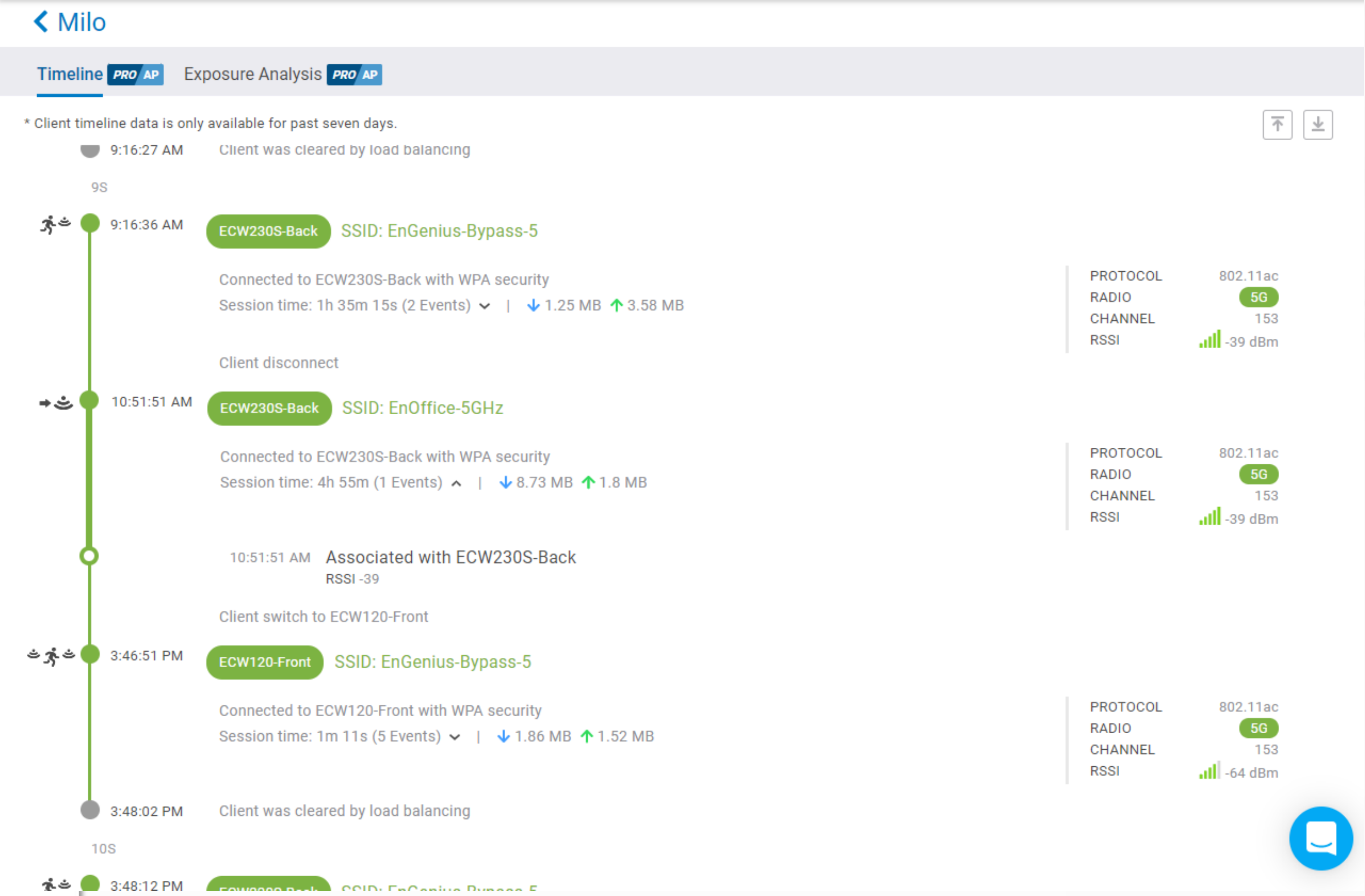
7-days!



Client States

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

- Client was connecting to an AP.
- Client was roaming and connecting to another AP.
- Client changed to associate with different radio or SSID of the same
- Client failed to authenticate with an SSID.
- Client was denied because of it is in block list.



< Milo

* Client timeline data is only available for past seven days.

9:16:27 AM Client was cleared by load balancing

9S

9:16:36 AM ECW230S-Back SSID: EnGenius-Bypass-5

Connected to ECW230S-Back with WPA security
Session time: 1h 35m 15s (2 Events) | ↓ 1.25 MB ↑ 3.58 MB

PROTOCOL	802.11ac
RADIO	5G
CHANNEL	153
RSSI	-39 dBm

Client disconnect

10:51:51 AM ECW230S-Back SSID: EnOffice-5GHz

Connected to ECW230S-Back with WPA security
Session time: 4h 55m (1 Events) | ↓ 8.73 MB ↑ 1.8 MB

PROTOCOL	802.11ac
RADIO	5G
CHANNEL	153
RSSI	-39 dBm

10:51:51 AM Associated with ECW230S-Back
RSSI -39

Client switch to ECW120-Front

3:46:51 PM ECW120-Front SSID: EnGenius-Bypass-5

Connected to ECW120-Front with WPA security
Session time: 1m 11s (5 Events) | ↓ 1.86 MB ↑ 1.52 MB

PROTOCOL	802.11ac
RADIO	5G
CHANNEL	153
RSSI	-64 dBm

3:48:02 PM Client was cleared by load balancing

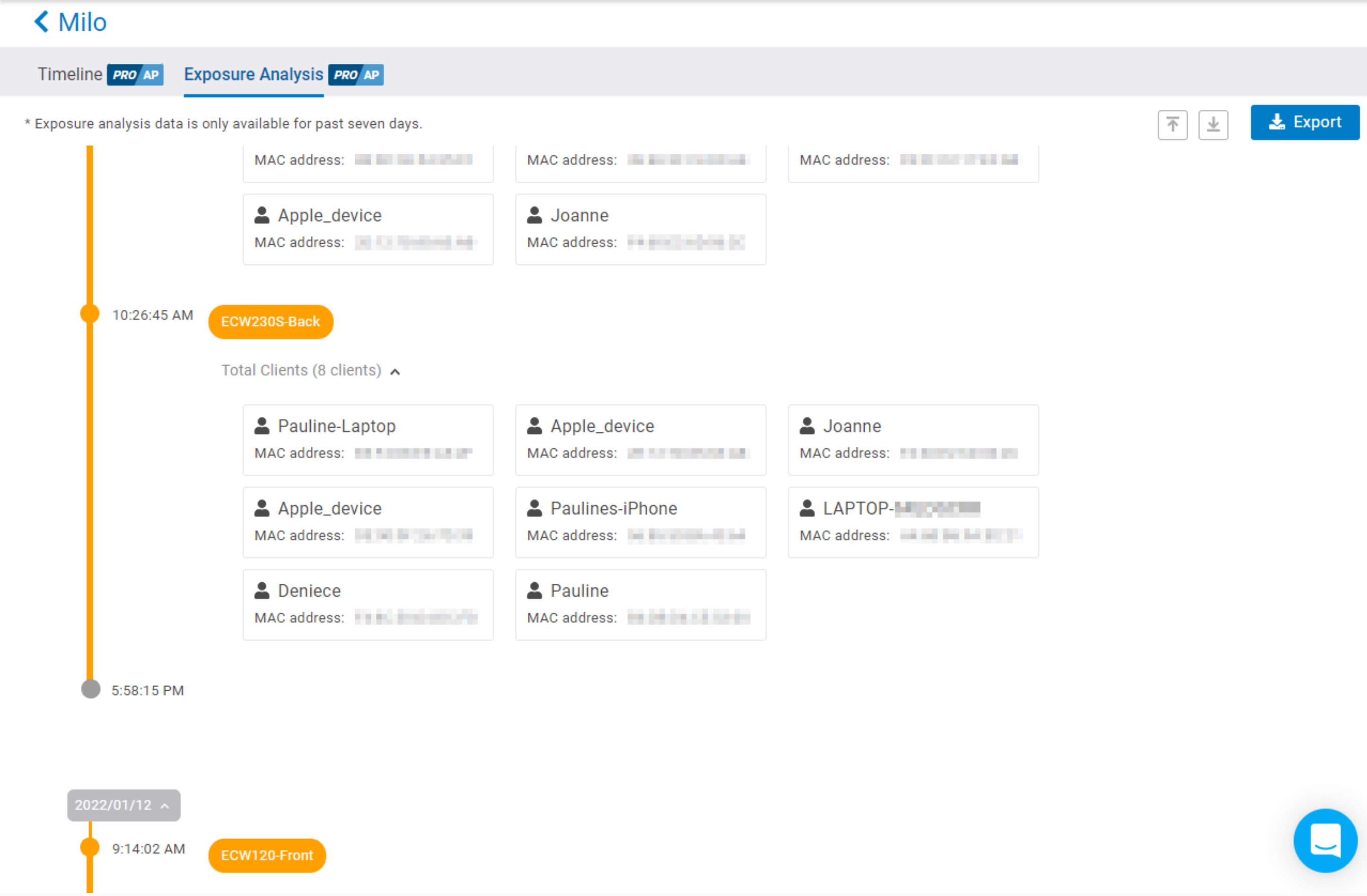
10S

3:48:12 PM ECW230S-Back SSID: EnGenius-Bypass-5

Exposure Analysis

Exposure Analysis allows a quick way to initiate contact tracing when the need arises. This may be used for other functions as well such as attendance checking.

Exposure Analysis can be viewed up to 7 days back. Exposure duration are tabulated in .CSV format when extracted.



< Milo

Timeline PRO AP | Exposure Analysis PRO AP

* Exposure analysis data is only available for past seven days.

Export

MAC address: [redacted] | MAC address: [redacted] | MAC address: [redacted]

Apple_device — MAC address: [redacted]
Joanne — MAC address: [redacted]

10:26:45 AM ECW230S-Back

Total Clients (8 clients)

Pauline-Laptop — MAC address: [redacted]
Apple_device — MAC address: [redacted]
Joanne — MAC address: [redacted]
Apple_device — MAC address: [redacted]
Paulines-iPhone — MAC address: [redacted]
LAPTOP-[redacted] — MAC address: [redacted]
Deniece — MAC address: [redacted]
Pauline — MAC address: [redacted]

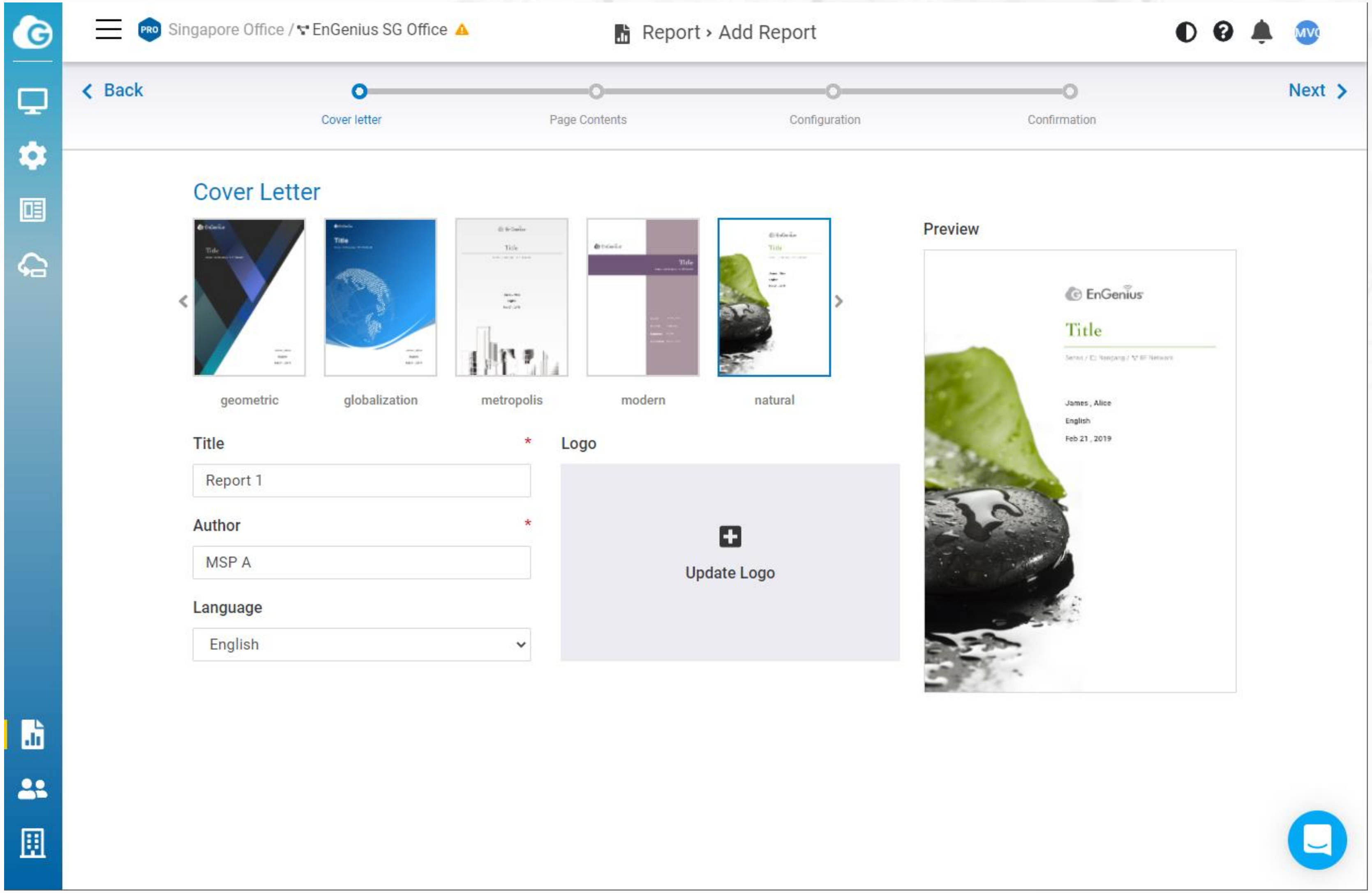
5:58:15 PM

2022/01/12

9:14:02 AM ECW120-Front

Reports

EnGenius Cloud Reports can be generated to provide a summary of customizable parameters. The reports can either be generated at once, or by schedule. The latter requires a PRO license.



PRO Singapore Office / EnGenius SG Office

Report › Add Report

Back — Cover letter — Page Contents — Configuration — Confirmation — Next

Cover Letter

geometric | globalization | metropolis | modern | natural

Title *: Report 1

Author *: MSP A

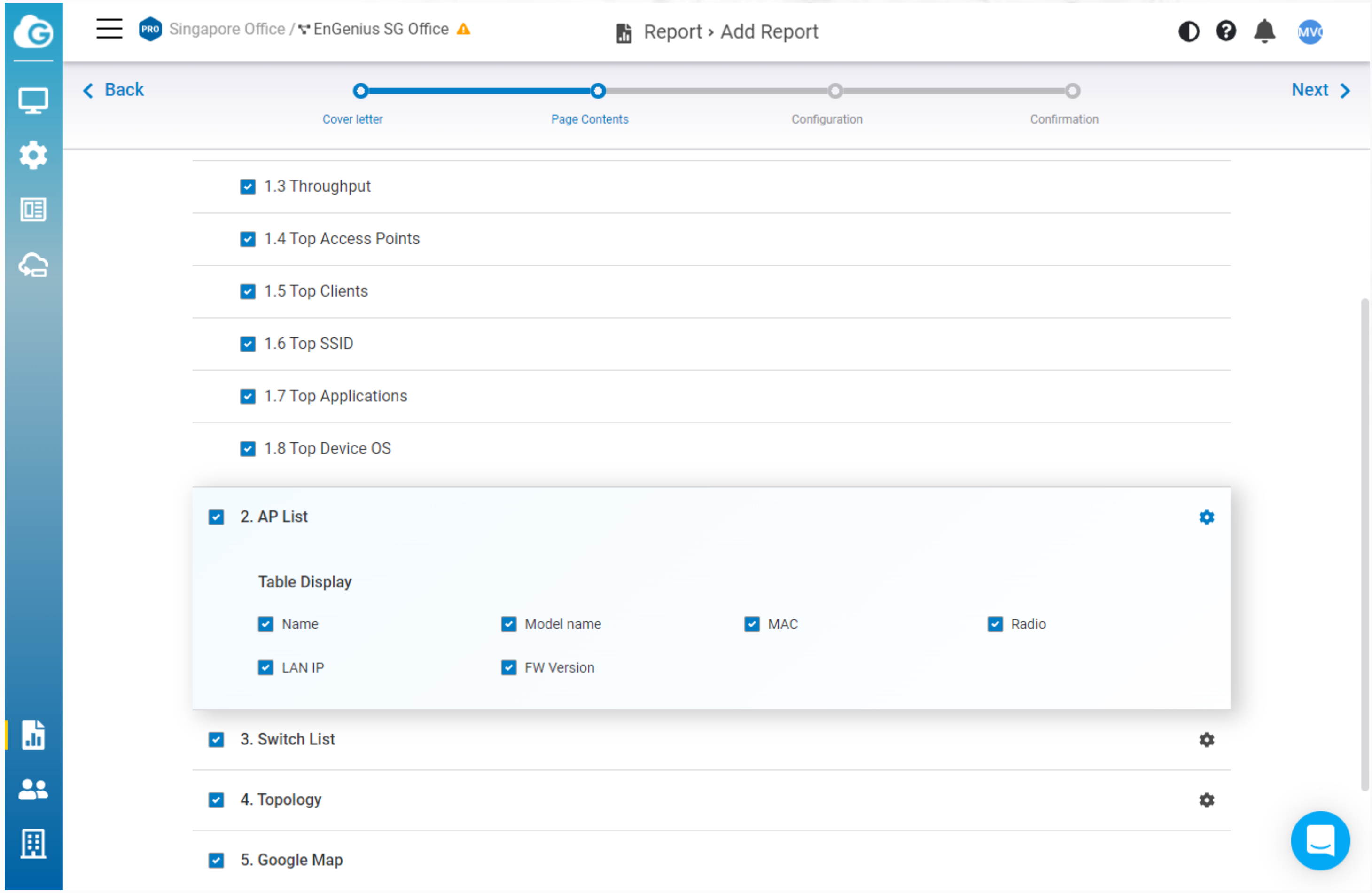
Language: English

Logo: Update Logo

Preview

EnGenius
Title
James , Alice
English
Feb 21 , 2019

Reports (2)



☑ 1.3 Throughput

☑ 1.4 Top Access Points

☑ 1.5 Top Clients

☑ 1.6 Top SSID

☑ 1.7 Top Applications

☑ 1.8 Top Device OS

☑ 2. AP List

Table Display

☑ Name ☑ Model name ☑ MAC ☑ Radio

☑ LAN IP ☑ FW Version

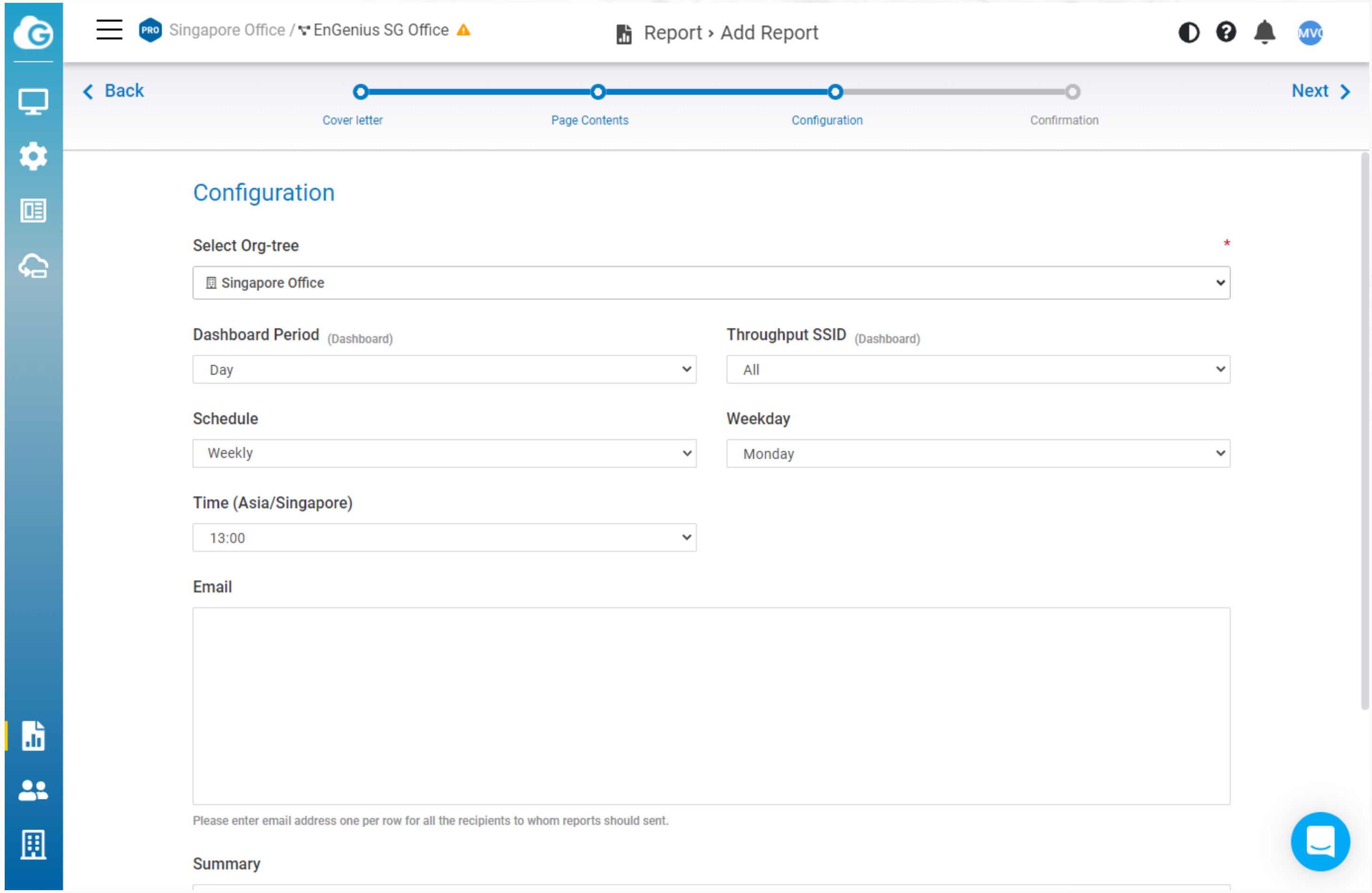
☑ 3. Switch List

☑ 4. Topology

☑ 5. Google Map

Reports (3)

The generated reports are in PDF format and can either be downloaded or sent via email.



Configuration

Select Org-tree *
Singapore Office

Dashboard Period (Dashboard): Day

Throughput SSID (Dashboard): All

Schedule: Weekly

Weekday: Monday

Time (Asia/Singapore): 13:00

Email

Please enter email address one per row for all the recipients to whom reports should sent.

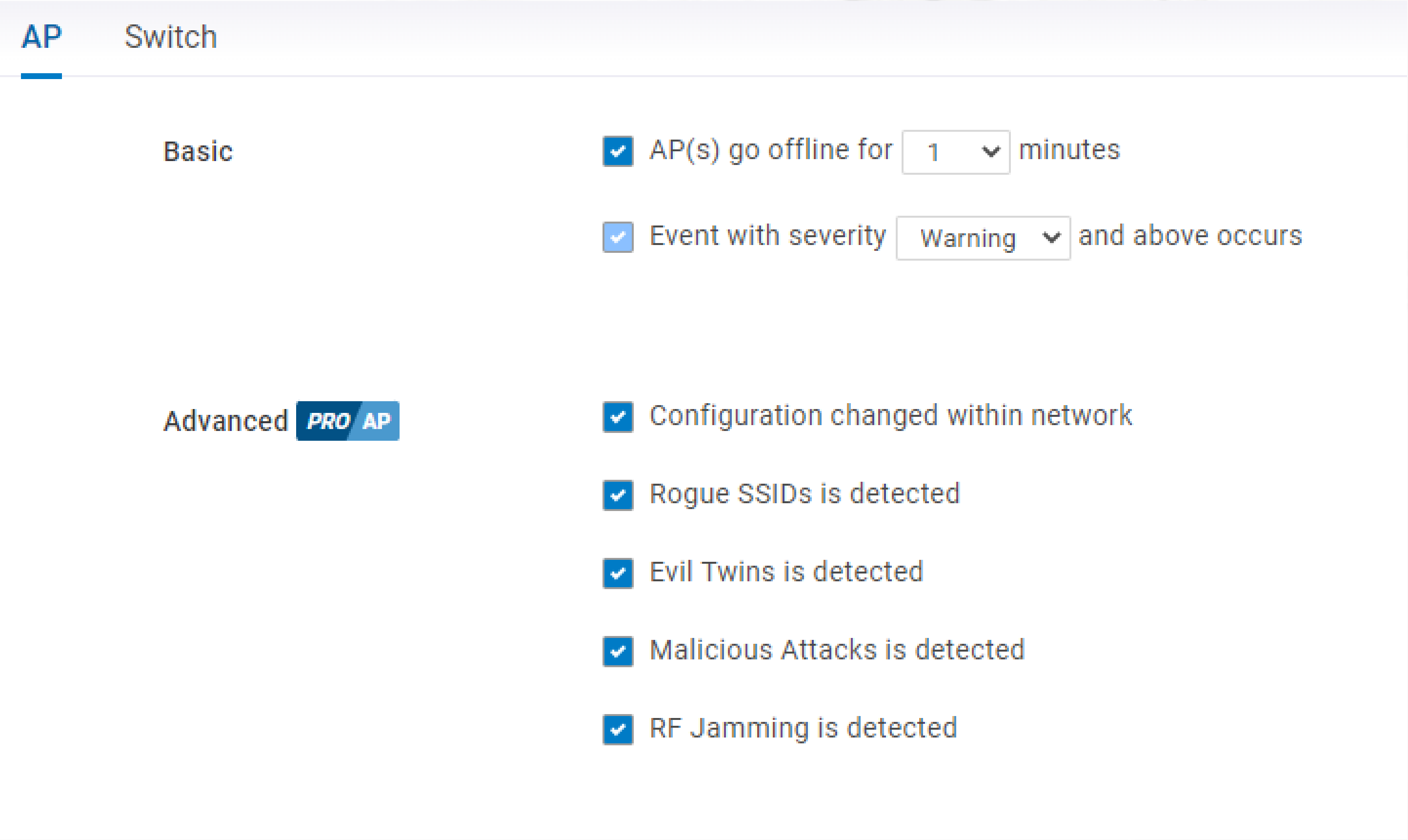
Summary

Notifications & Alerts

Notifications on EnGenius Cloud can be customized, and delivered in a couple of ways:

- Alerts via the Cloud Portal
- Email alerts
- EnGenius Cloud To-Go push notifications

The AP alerts are shown to the right.



Basic

☑ AP(s) go offline for 1 minutes

☑ Event with severity Warning and above occurs

Advanced PRO AP

☑ Configuration changed within network

☑ Rogue SSIDs is detected

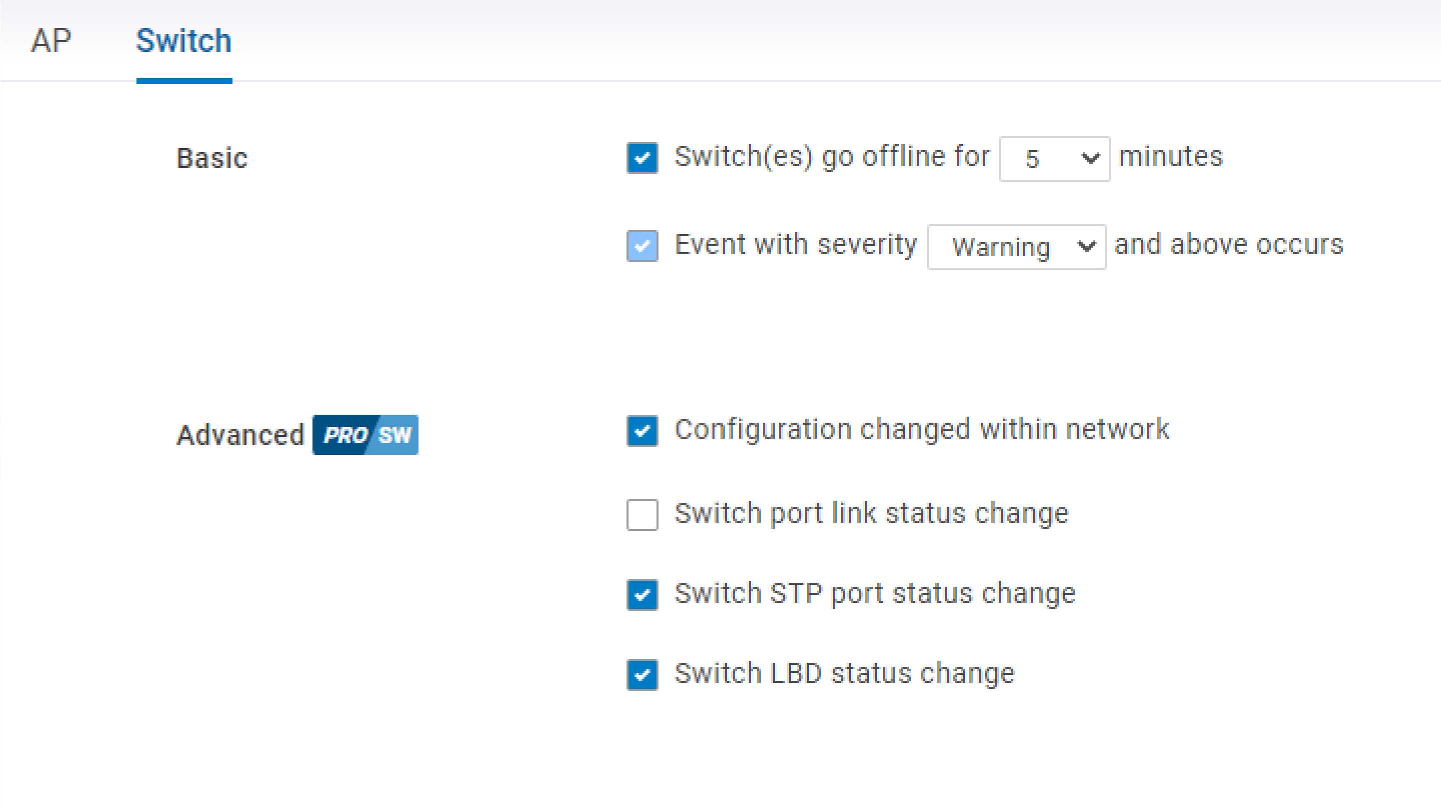
☑ Evil Twins is detected

☑ Malicious Attacks is detected

☑ RF Jamming is detected

Notifications & Alerts - Switch

The switch alerts



AP | **Switch**

Basic

☑ Switch(es) go offline for 5 minutes

☑ Event with severity Warning and above occurs

Advanced PRO SW

☑ Configuration changed within network

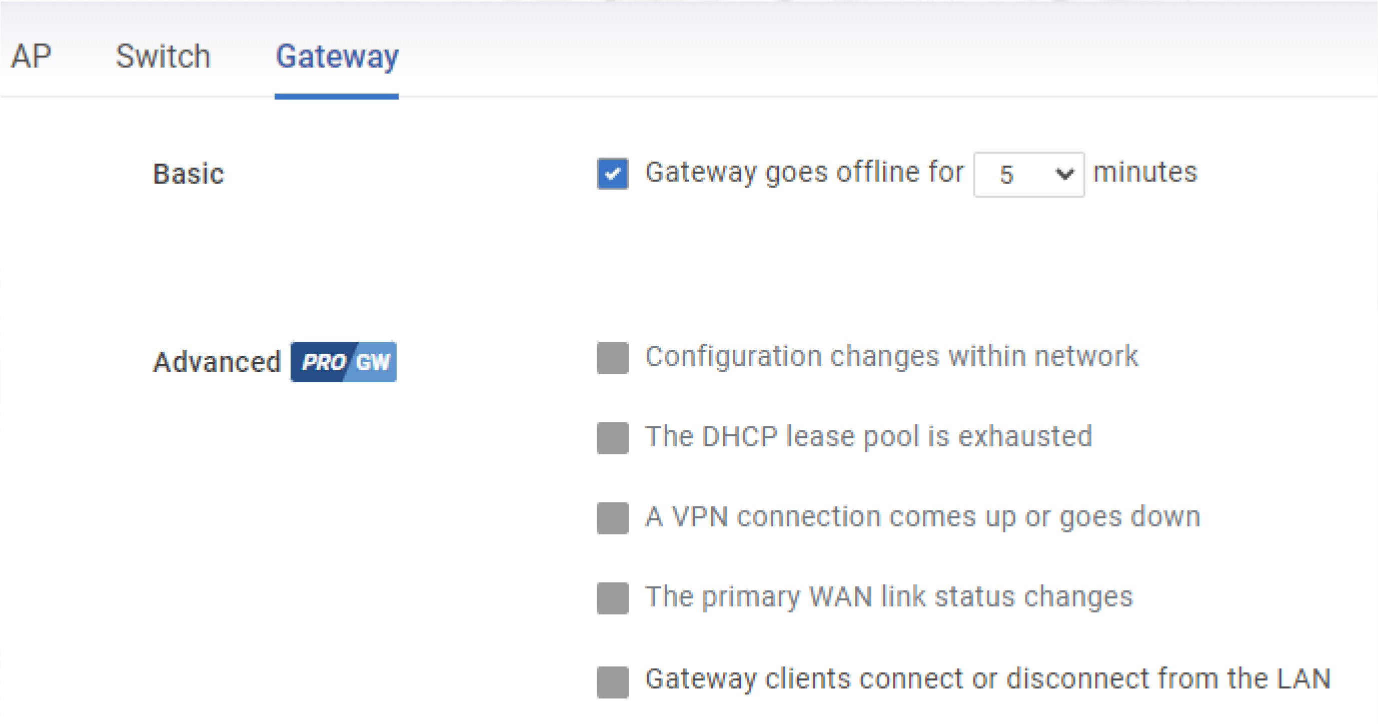
□ Switch port link status change

☑ Switch STP port status change

☑ Switch LBD status change

Notifications & Alerts - Gateway

The gateway alerts



Basic

☑ Gateway goes offline for 5 minutes

Advanced PRO GW

□ Configuration changes within network

□ The DHCP lease pool is exhausted

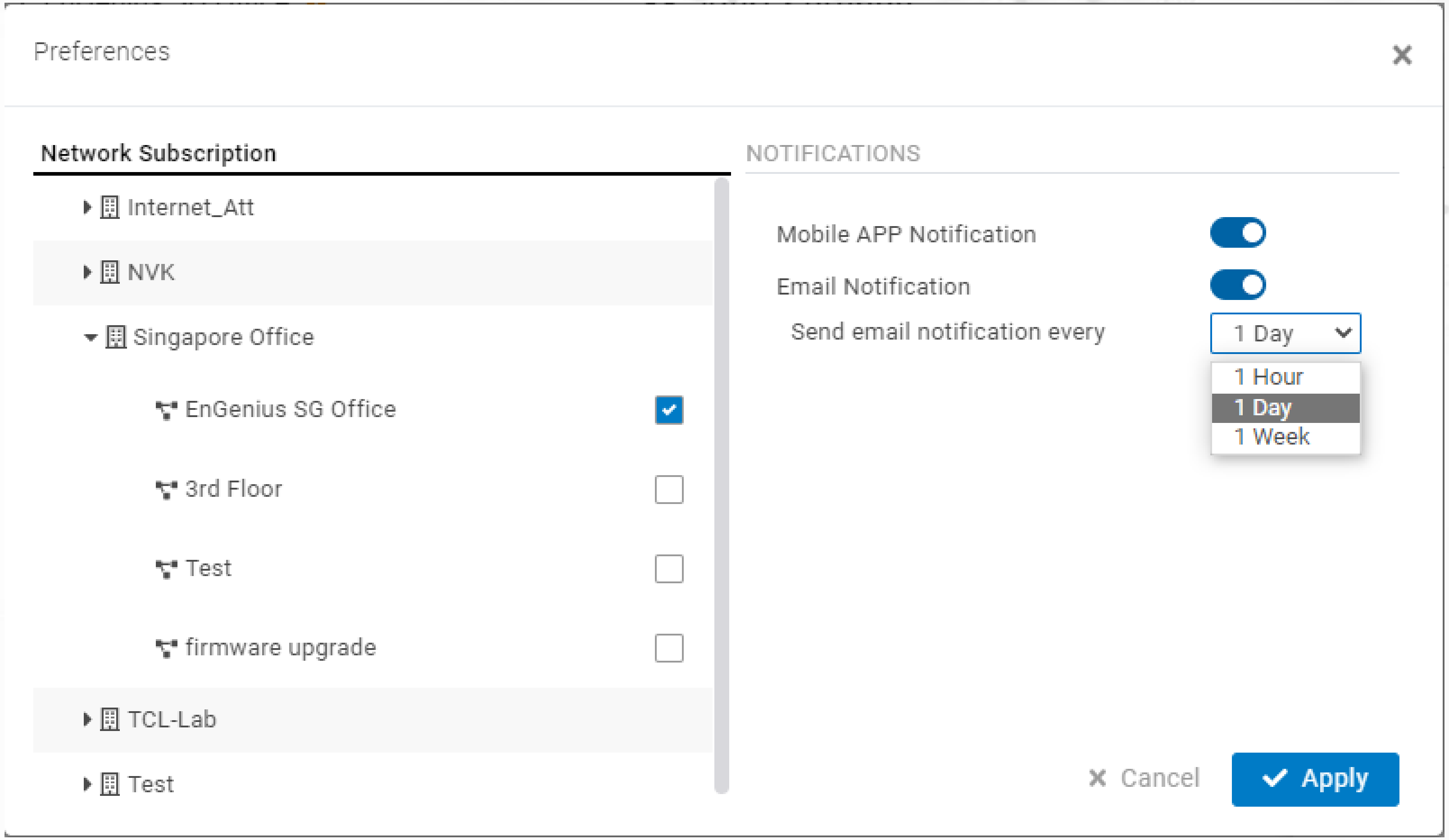
□ A VPN connection comes up or goes down

□ The primary WAN link status changes

□ Gateway clients connect or disconnect from the LAN

Notifications & Alerts

EnGenius Cloud To-Go utilizes push notifications to deliver alerts in real-time.



Preferences

Network Subscription

- Internet_Att
- NVK
- Singapore Office
  - EnGenius SG Office ☑
  - 3rd Floor □
  - Test □
  - firmware upgrade □
- TCL-Lab
- Test

NOTIFICATIONS

Mobile APP Notification: on

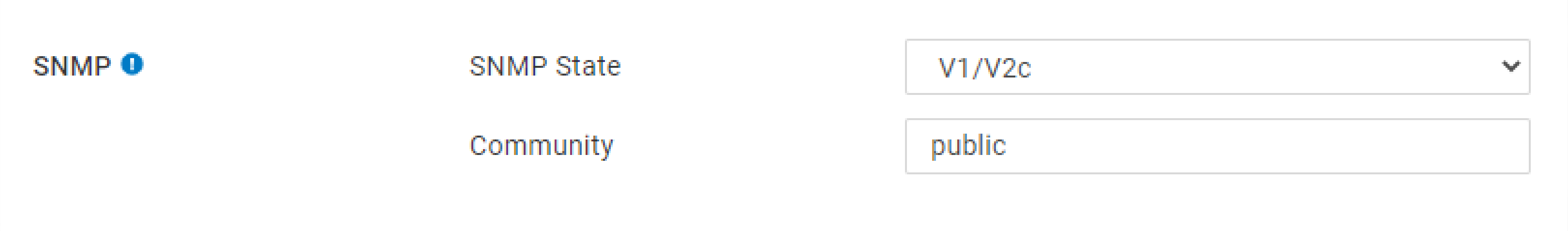
Email Notification: on

Send email notification every: 1 Day

SNMP Monitoring

There are situations where clients may have multiple networking brands on hand. In these situations, the usage of 3rd party monitoring services through APIs or SNMP is common in their NOC.

EnGenius Cloud APs and Switches can be monitored externally through APIs or SNMP.



SNMP

SNMP State: V1/V2c

Community: public

Below are the supported MIBs for SNMP:

Access Points

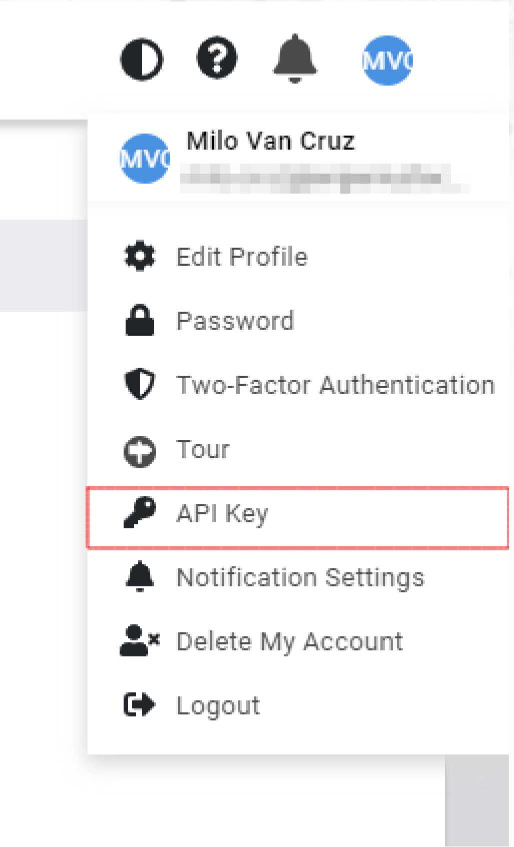
- RFC1213-MiB

Switches

- BRIDGE-MiB
- Q-BRIDGE-MiB
- DNS-RESOLVER-MiB
- RFC1213-MiB
- ENTITY-MiB RMON2-MiB
- EtherLike-MiB
- SNMP-FRAMEWORK-MiB
- IEEE8021-PAE-MiB
- SNMP-NOTIFICATION-MiB
- IF-MiB SNMP-TARGET-MiB
- IF-FORWARD-MiB
- SNMP-USER-BASED-SM-MiB
- IP-MiB SNMPv2-MiB
- LLDP-MiB
- SNMP-VIEW-BASED-ACM-MiB
- MAU-MiB TCP-MiB
- P-BRIDGE-MiB

API Integration

API Keys are required for API Integration. An administrator of a PRO License-enabled Org may generate and manage API Keys.

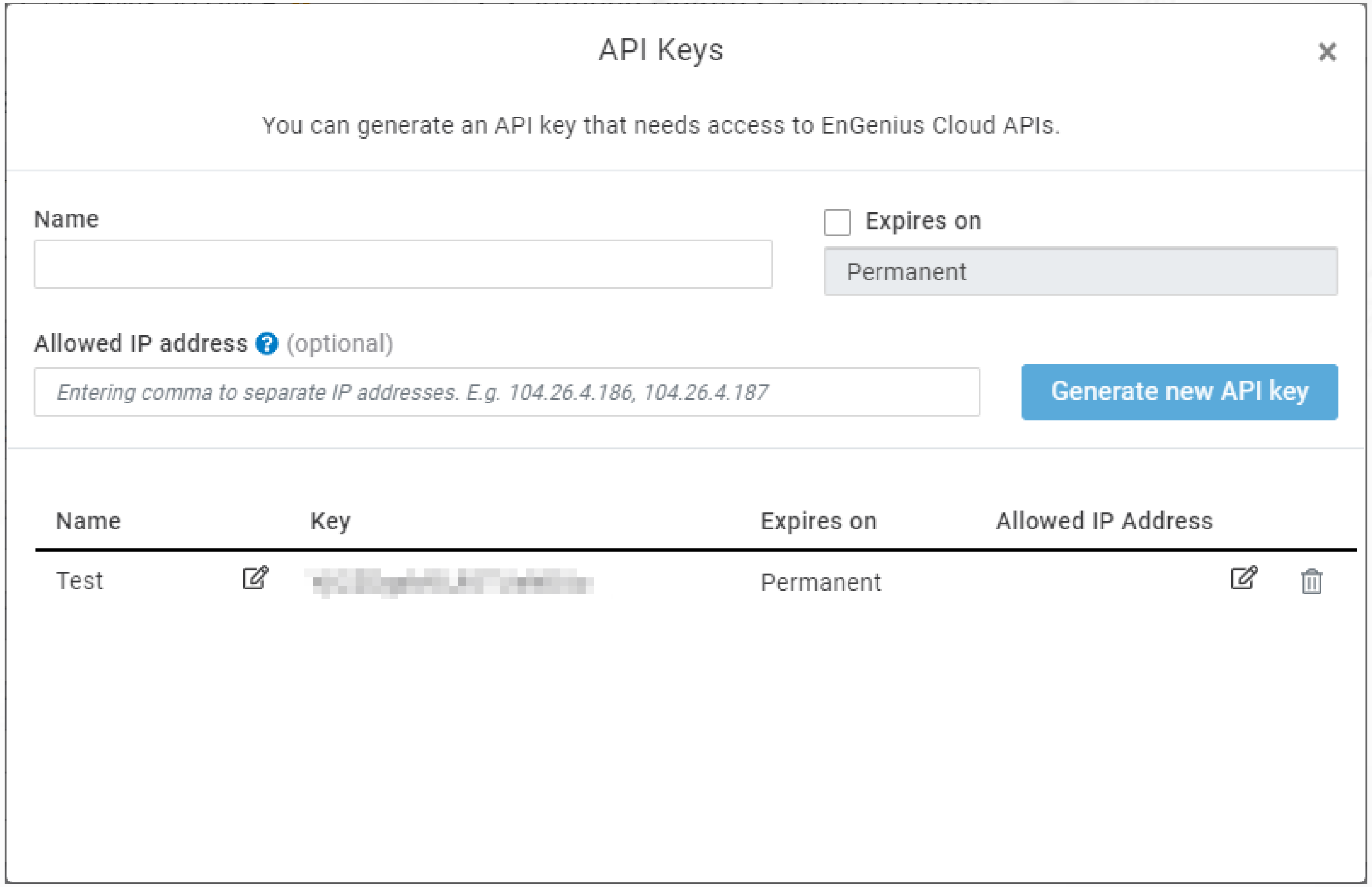


API Integration

API keys can be generated from the profile options. PRO License is required.

API Keys are unique, and grant access to all Orgs managed by the administrator that generated the key.

3rd party integrations such as LBS, BLE, or external voucher service management will require APIs for integration.



API Keys

You can generate an API key that needs access to EnGenius Cloud APIs.

Name

□ Expires on

Permanent

Allowed IP address (optional)

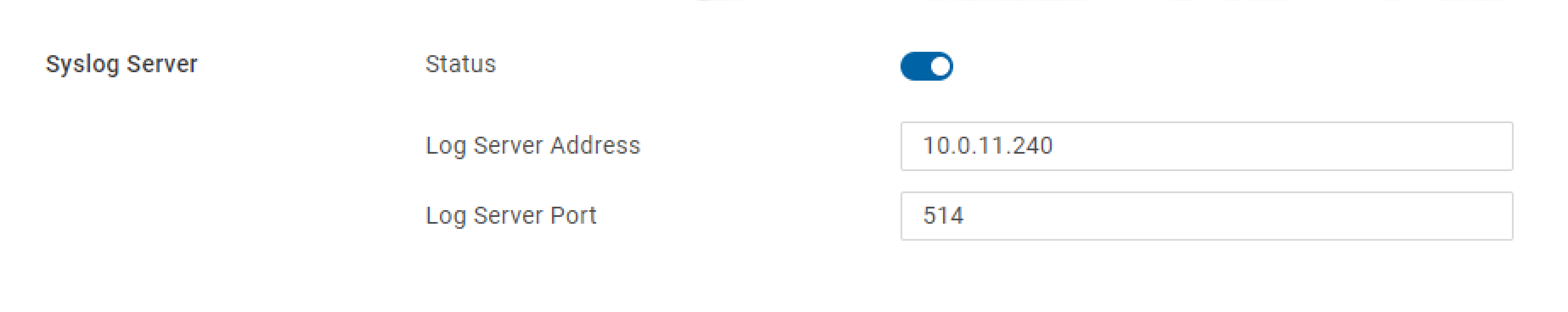
Entering comma to separate IP addresses. E.g. 104.26.4.186, 104.26.4.187

Name	Key	Expires on	Allowed IP Address
Test	[redacted]	Permanent	

Syslog

Some network environments keep an archive of device logs on an external syslog server. Configuring external syslog on the Cloud is as simple as enabling, and keying in the server's IP and port to route all logs to an external server.

APs and Switches can be configured to have separate syslog servers.



Syslog Server

Status ●

Log Server Address 10.0.11.240

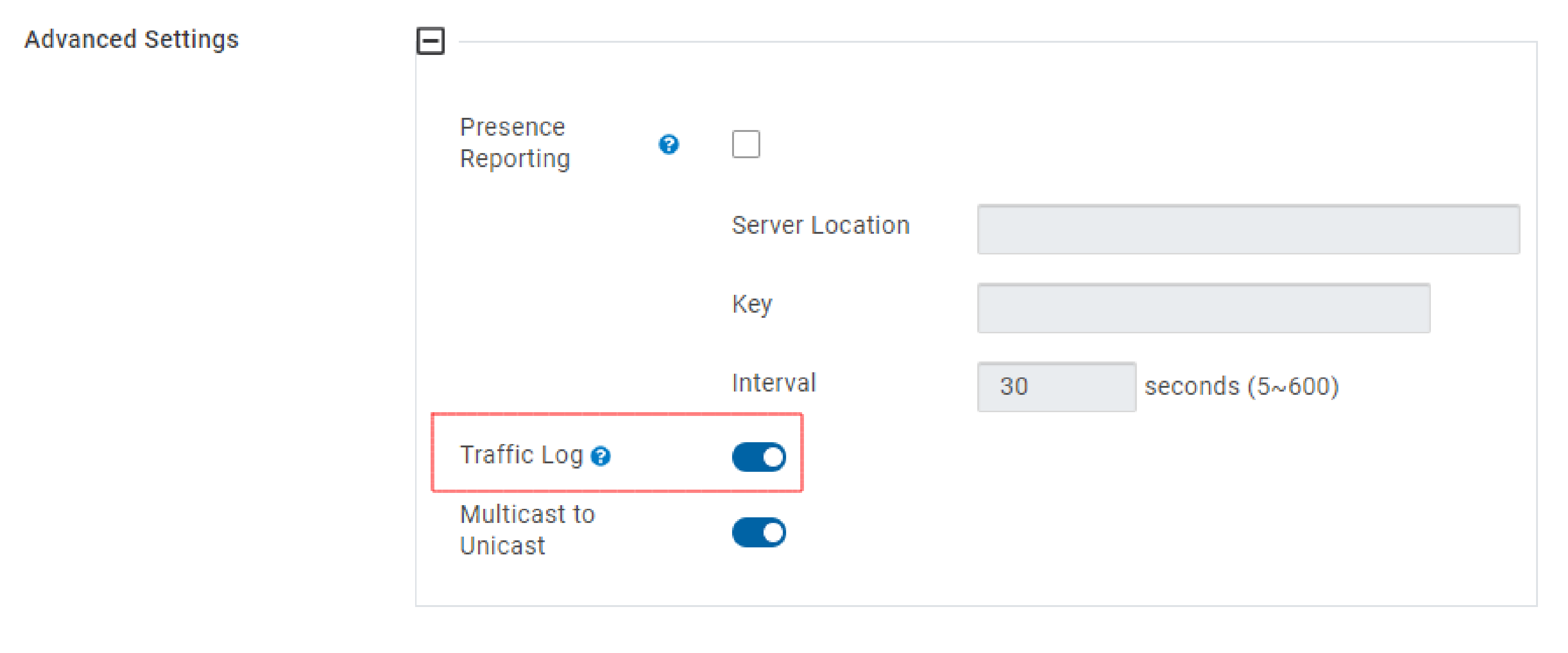
Log Server Port 514

Traffic Logs

Some territories require that all traffic logs are stored, and accessible in time of need by local authorities. This option is disabled on the Cloud by default. When enabled, the APs feed all client information such as Src MAC, Dst MAC, Src IP, Dst IP, and Port, to an external syslog server.

To enable traffic logs, syslog must first be setup.

(!) Enabling Traffic Log will severely degrade the performance of the AP.



Advanced Settings ⊟

Presence Reporting ❓ □

Server Location

Key

Interval 30 seconds (5~600)

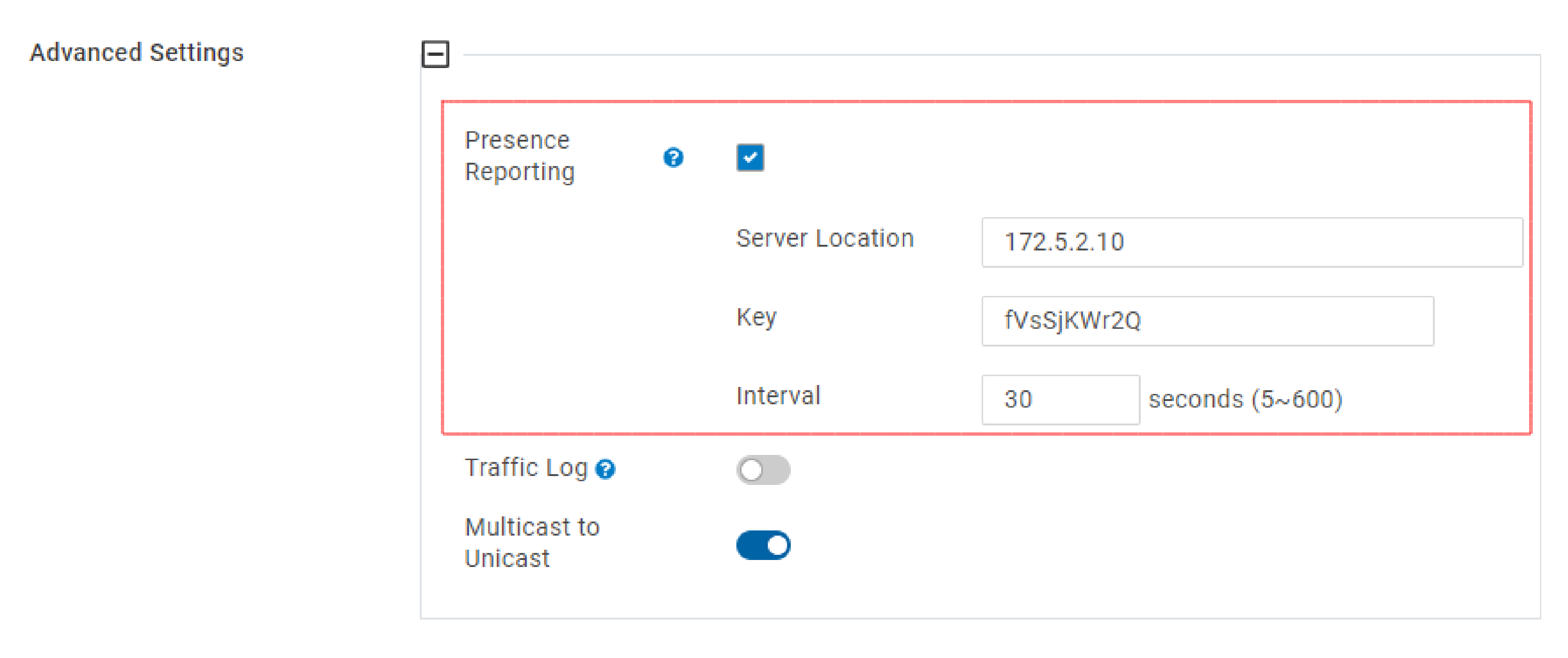
Traffic Log ❓ ●

Multicast to Unicast ●

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 Access 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.



Advanced Settings

Presence Reporting ☑

Server Location: 172.5.2.10

Key: fVsSjKWr2Q

Interval: 30 seconds (5~600)

Traffic Log: ○ (off)

Multicast to Unicast: ● (on)

(!) If you have requirements for location-based services or LBS, please contact EnGenius for integration.

Security - topics

- AirGuard
- Network Security
- Two-Factor Authentication

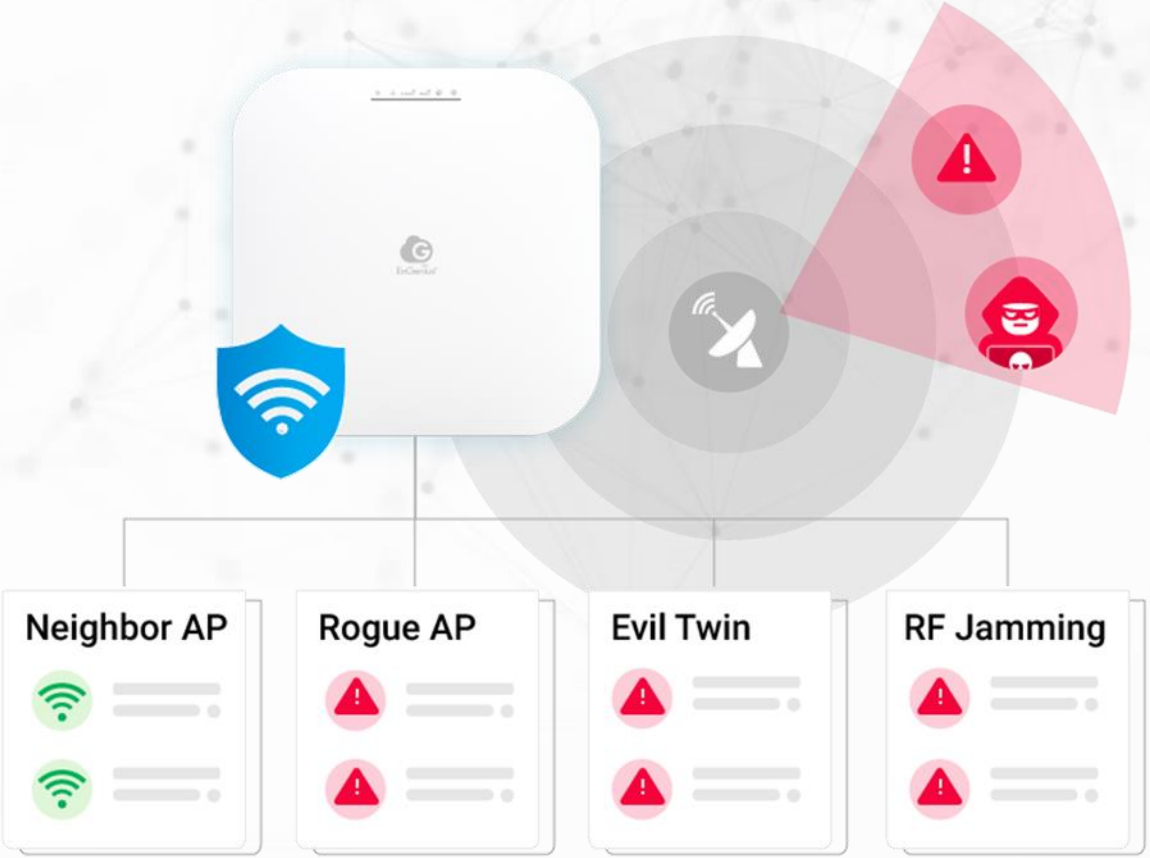
Security Concerns in Wi-Fi

- Data transmitted over wireless may contain sensitive personal or financial data. Nowadays, open-source hacking tools are easy to get and through impersonation of client devices and access points in anytime and everywhere. Once the victim is connected, the attacker can steal credentials, inject malicious codes into the victim's browsers, redirect the victim to a malware site, and so much more…

EnGenius AirGuard™

In response to rising cyber-attacks, EnGenius has expanded its security portfolio to enclose AirGuard™ features in new Wi-Fi 6 cloud-managed security access points (APs); AirGuard™ is designed to assist network administrators for uninterrupted monitoring and protection of information-sensitive, distributed enterprise wireless networks.

AirGuard™ detects, analyzes, and eliminates wireless threats to protect your network from attacks.



EnGenius AirGuard™

WIDS (Wireless intrusion detection system)

The system monitors the radio spectrum used by wireless LANs for the presence of unauthorized, rogue APs and the wireless attack tools, and immediately alerts a systems administrator whenever a rogue AP is detected.

WIPS (Wireless Intrusion Prevention System)

The system monitors the radio spectrum for the presence of unauthorized APs (intrusion detection) and can automatically provide countermeasures (intrusion prevention). It is able to accurately detect and automatically classify a threat for elimination, then prevent the connections between the rogue AP and wireless clients.

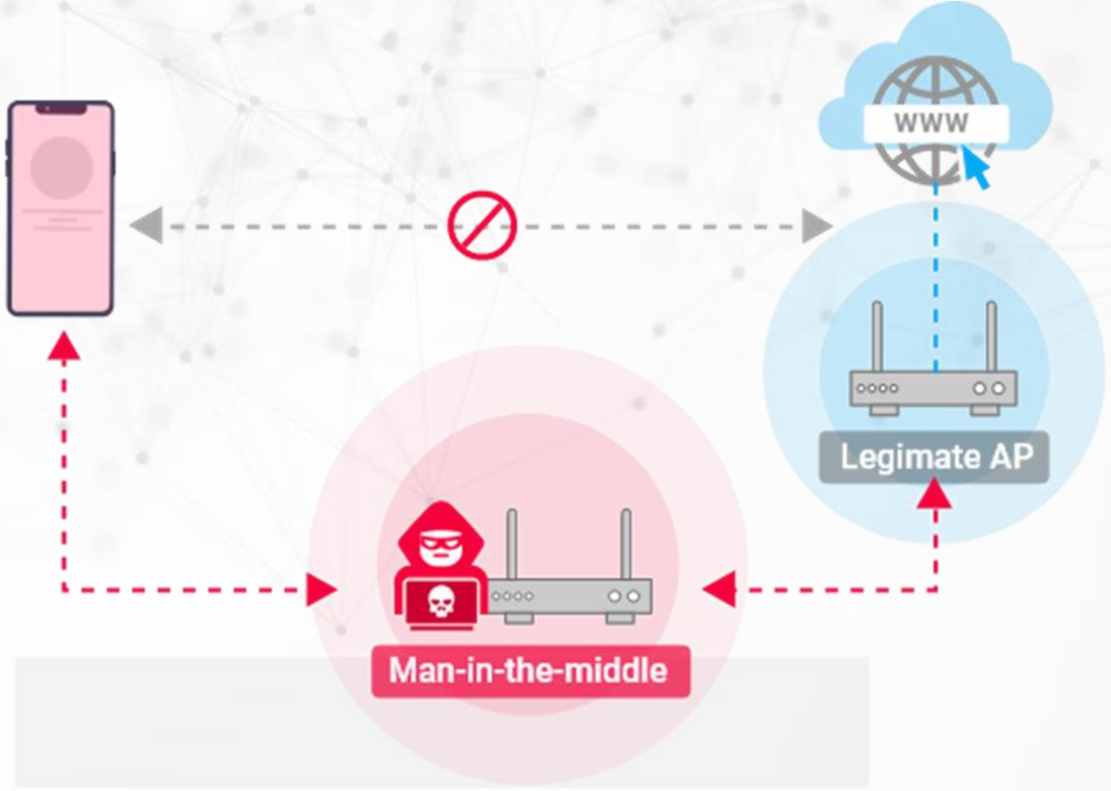
Common wireless attacks that AirGuard™ prevents

Reason for attacks

- Steal information
    - Login credentials
    - Credit card information
    - Database
- Terminate function of wireless IP devices
    - Wireless IP camera
    - Personal hotspot
    - Drone de-authentication
- Pranks

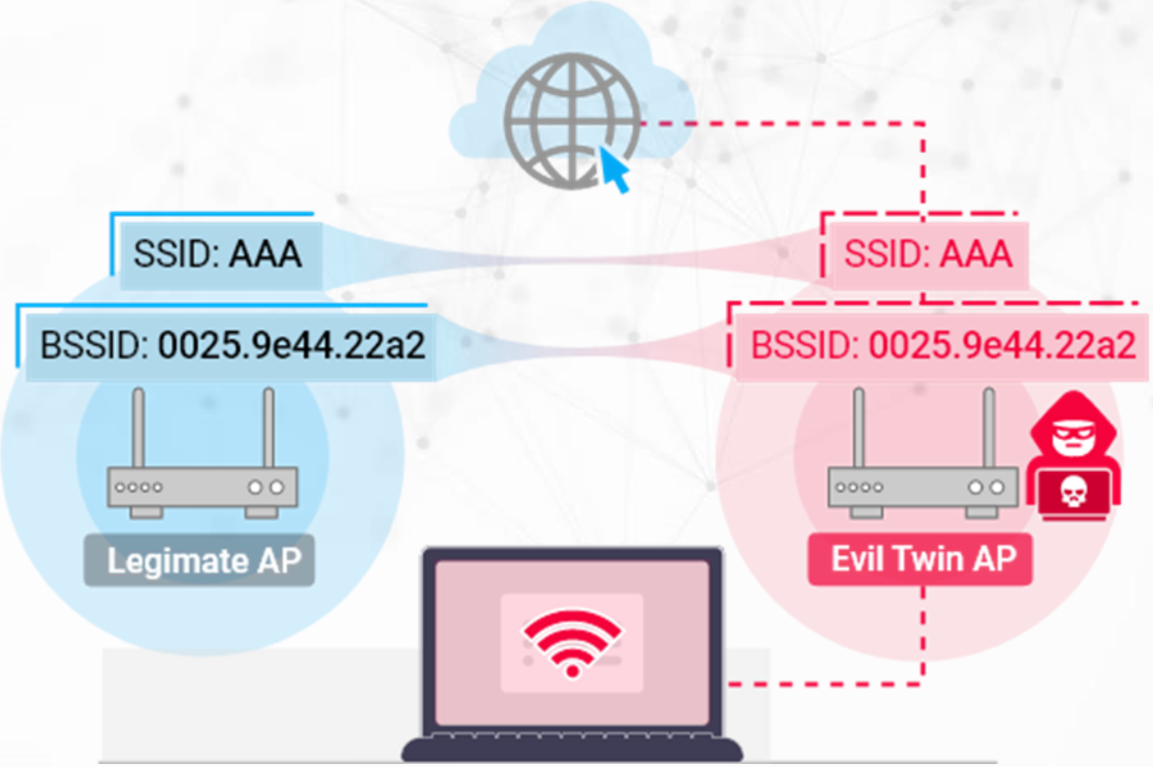
Man-in-the-middle attack (MITM)

When the SSID security type is Open or WPA-Personal, the attacker secretly relays and possibly alters the communications between AP and wireless client who believe that they are directly communicating with each other. Then the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.



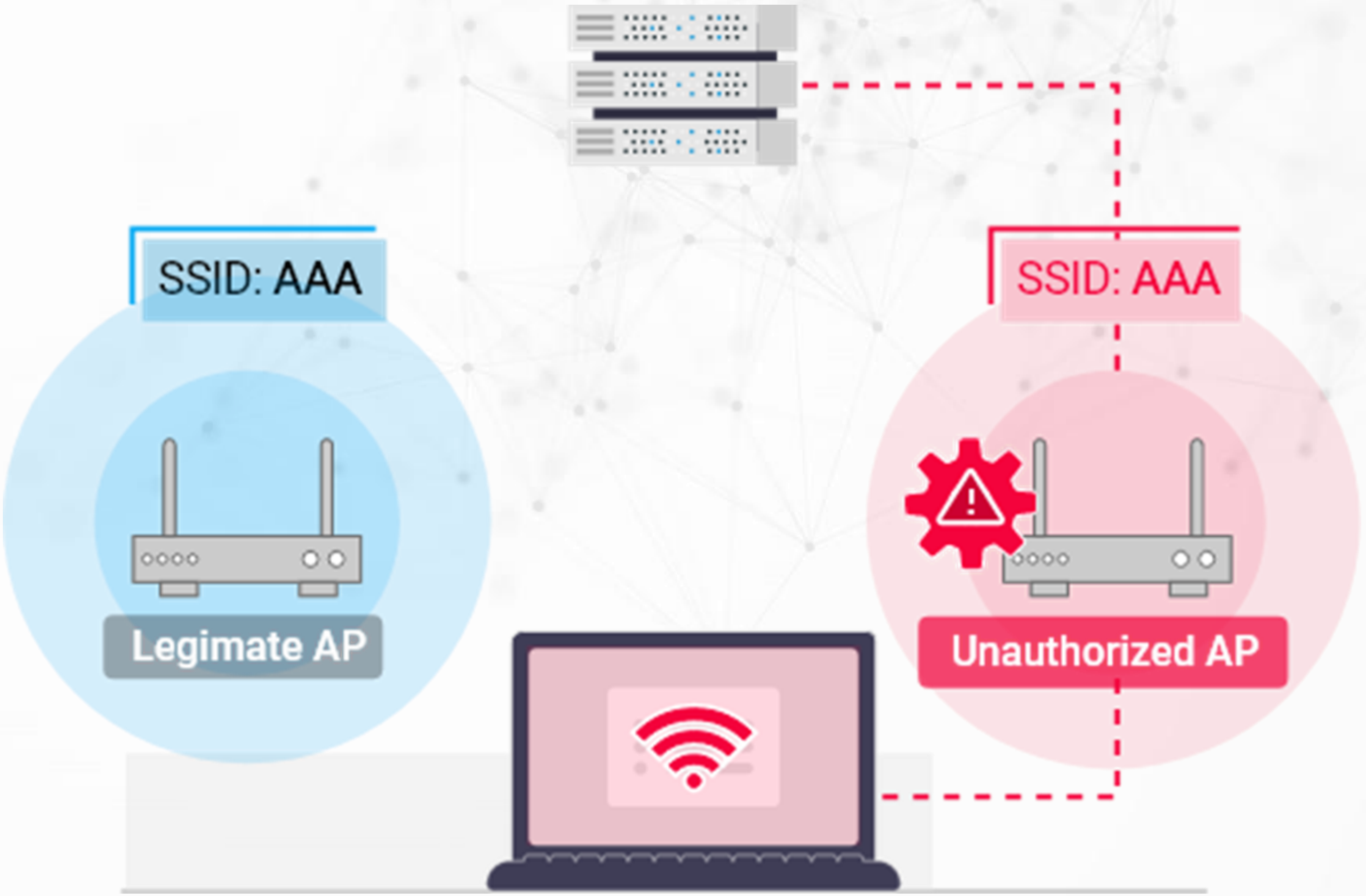
Evil Twin

- AP Impersonation
  As Rogue AP may simulate same SSID and MAC address as official AP, once the victim is connected, the attacker can steal all the data from the victim.
- AP Spoofing
  An AP that spoofs the wireless MAC address of the authorized AP. An attacker can launch an attack through an AP masquerading as a legitimate AP.



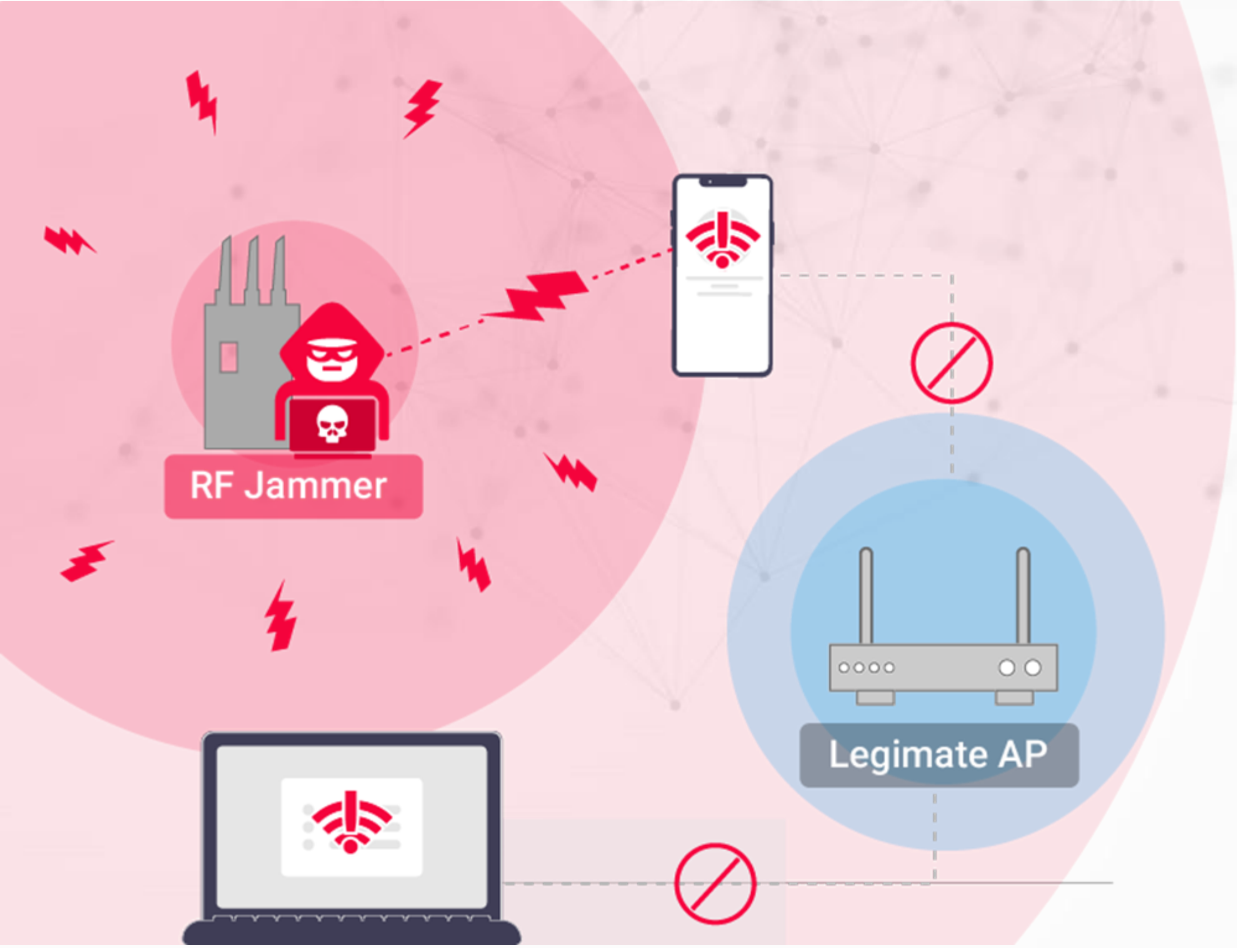
Valid SSID miss-use

- An un-authorized AP uses same SSID as legitimate SSID in authorized Network, so the client might connect to the malicious AP and causes security breach.



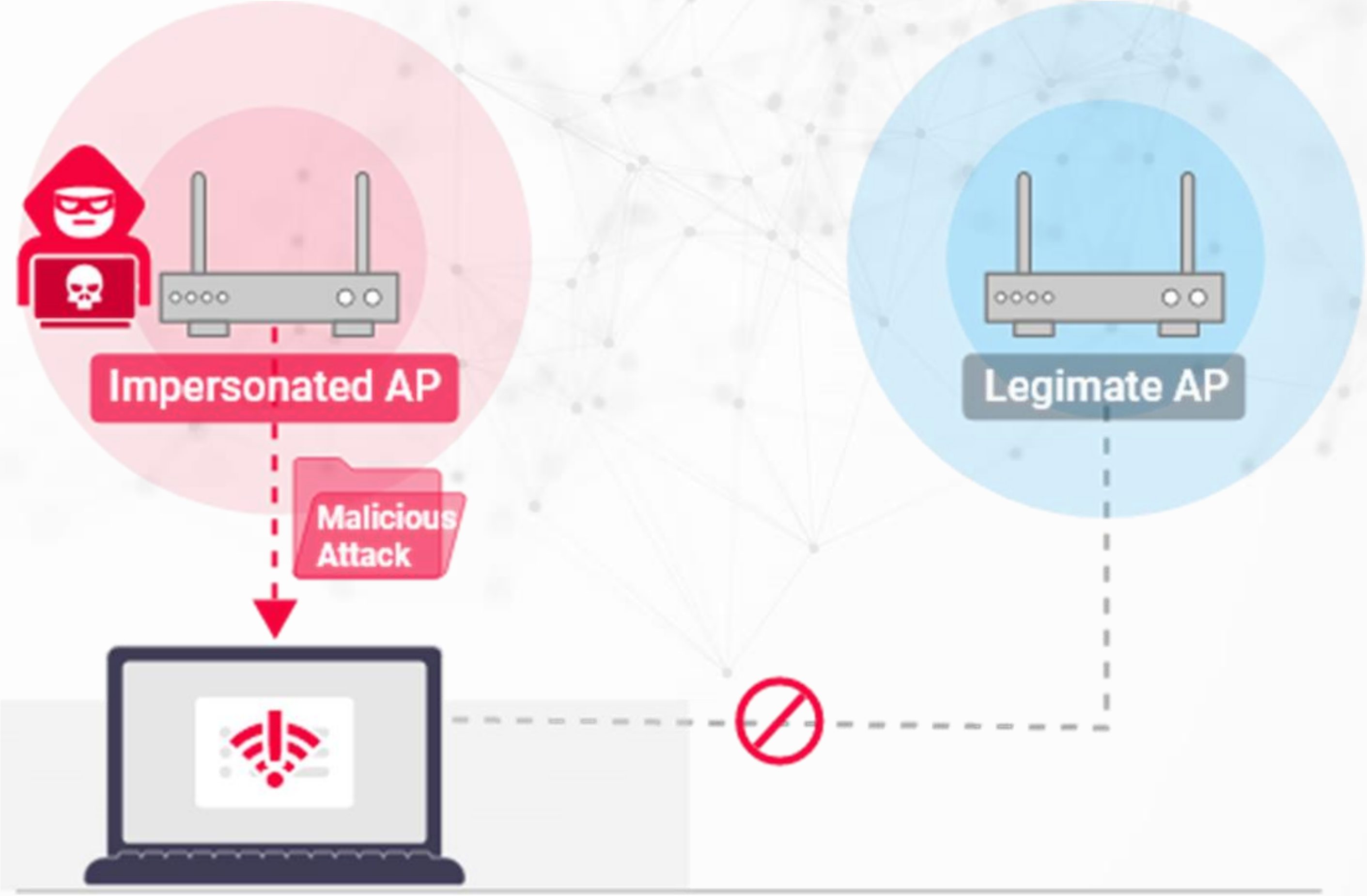
RF Jamming

- The RF jammer device will specify a SSID/Channel to send packets or RF signal continually, thus other clients will be dropped by channel busy.



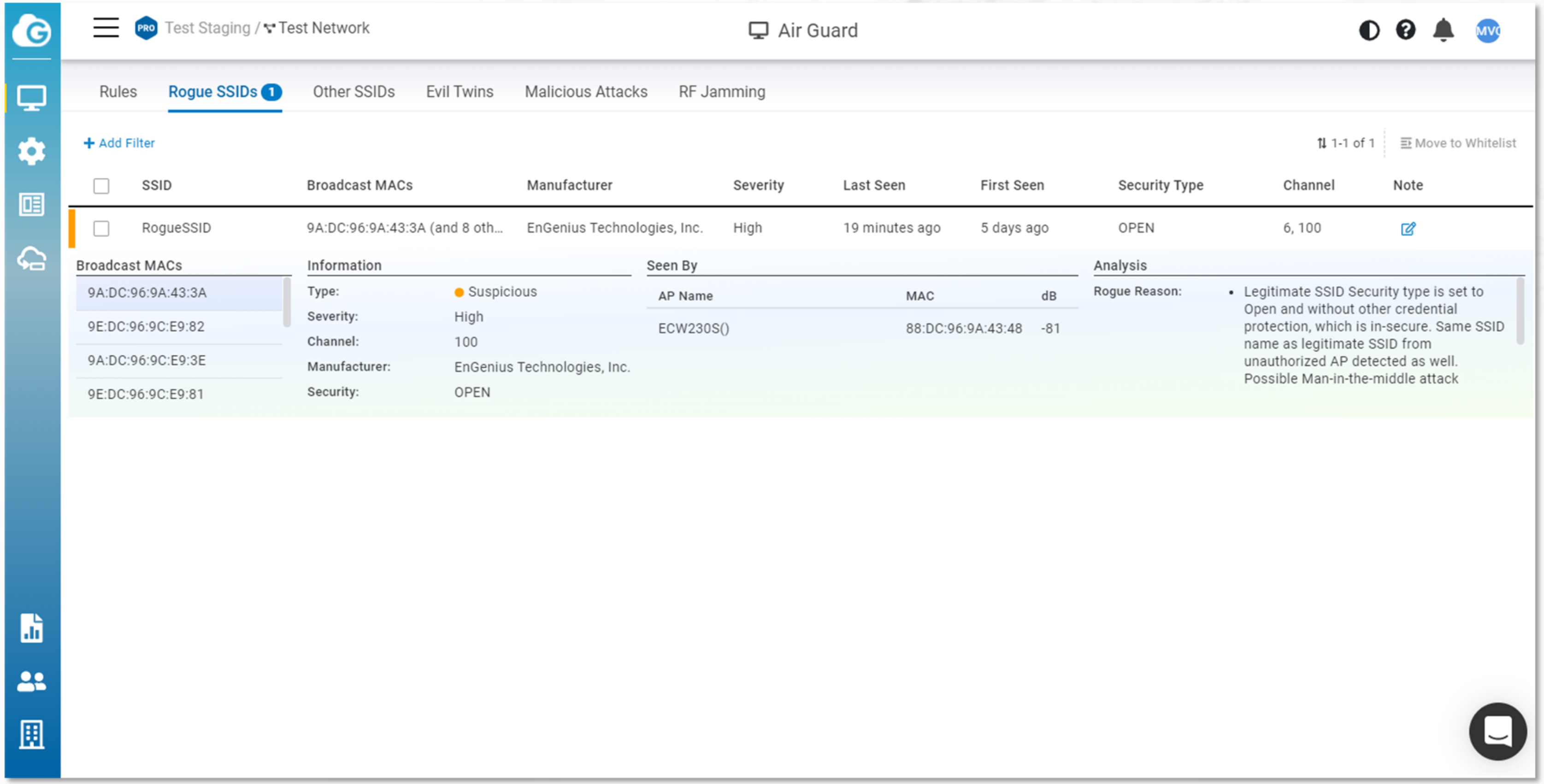
De-authentication Attacks

- A hacker can impersonate a legitimate AP and send a de-auth frame to a client (or vice versa) using the de-authentication feature of the 802.11 Wi-Fi protocol, causing client devices to disconnect from the AP.



AirGuard™ Management

- EnGenius Security APs such as the ECW220S, ECW230S, and future S models are equipped with AirGuard™. An AP PRO License is also required to utilize the feature.
- On the EnGenius Cloud Portal, attacks are automatically detected, and the system provides information if further action is required.



□	SSID	Broadcast MACs	Manufacturer	Severity	Last Seen	First Seen	Security Type	Channel	Note
□	RogueSSID	9A:DC:96:9A:43:3A (and 8 oth...	EnGenius Technologies, Inc.	High	19 minutes ago	5 days ago	OPEN	6, 100	

Broadcast MACs

9A:DC:96:9A:43:3A
9E:DC:96:9C:E9:82
9A:DC:96:9C:E9:3E
9E:DC:96:9C:E9:81

Information

Type:	● Suspicious
Severity:	High
Channel:	100
Manufacturer:	EnGenius Technologies, Inc.
Security:	OPEN

Seen By

AP Name	MAC	dB
ECW230S()	88:DC:96:9A:43:48	-81

Analysis

Rogue Reason:

- Legitimate SSID Security type is set to Open and without other credential protection, which is in-secure. Same SSID name as legitimate SSID from unauthorized AP detected as well. Possible Man-in-the-middle attack

De-authentication Attacks

De-authentication Attacks

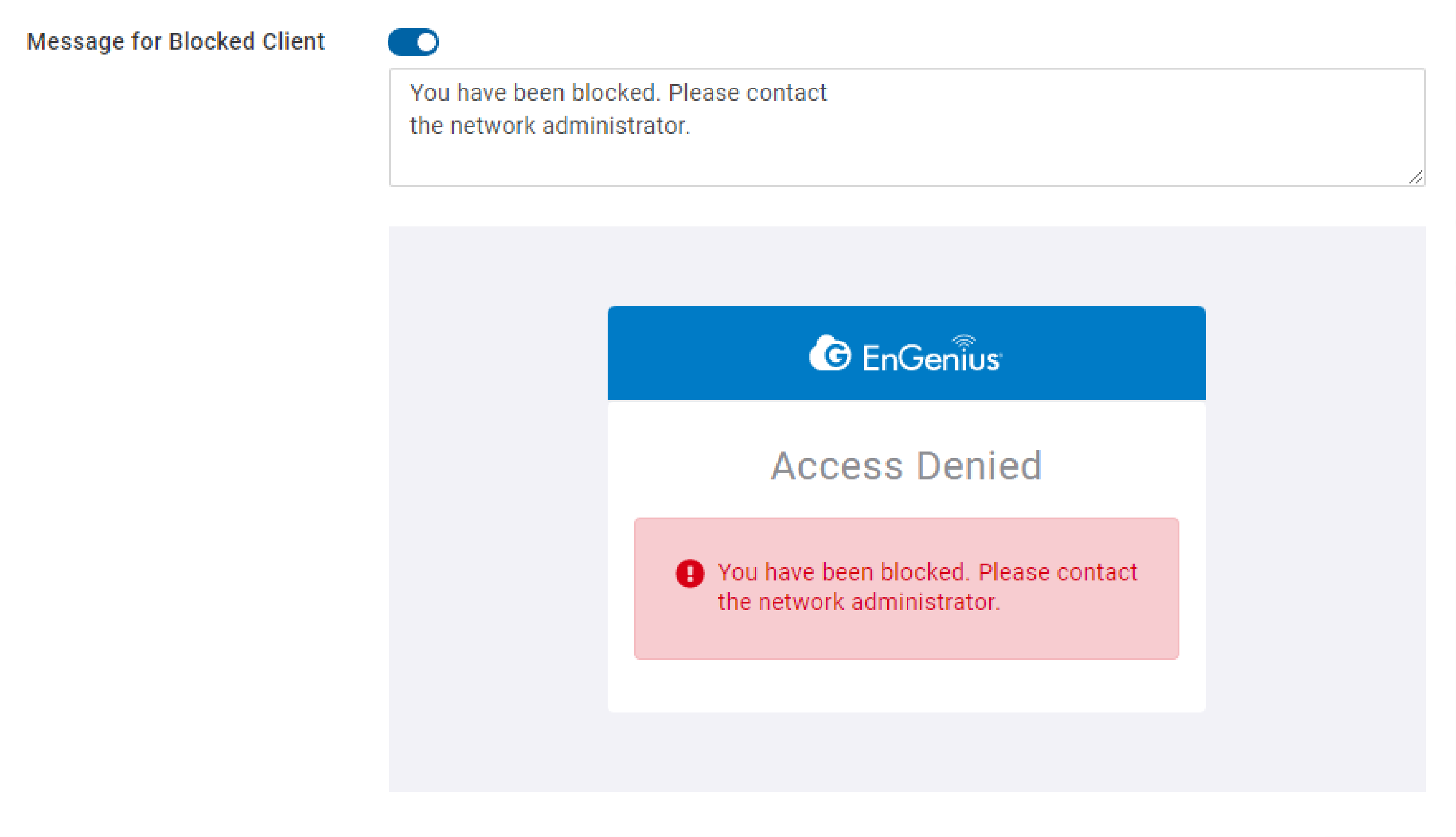
ACL: Access Control List

Blacklist

The Blacklist can hold 1000 MAC addresses per Org.

Splash Page for Blocked Clients

When a client is blocked and attempts to connect to the SSID, a special splash page can be enabled under the General Settings to alert the client that he was banned from accessing the wireless network.



Message for Blocked Client

You have been blocked. Please contact the network administrator.

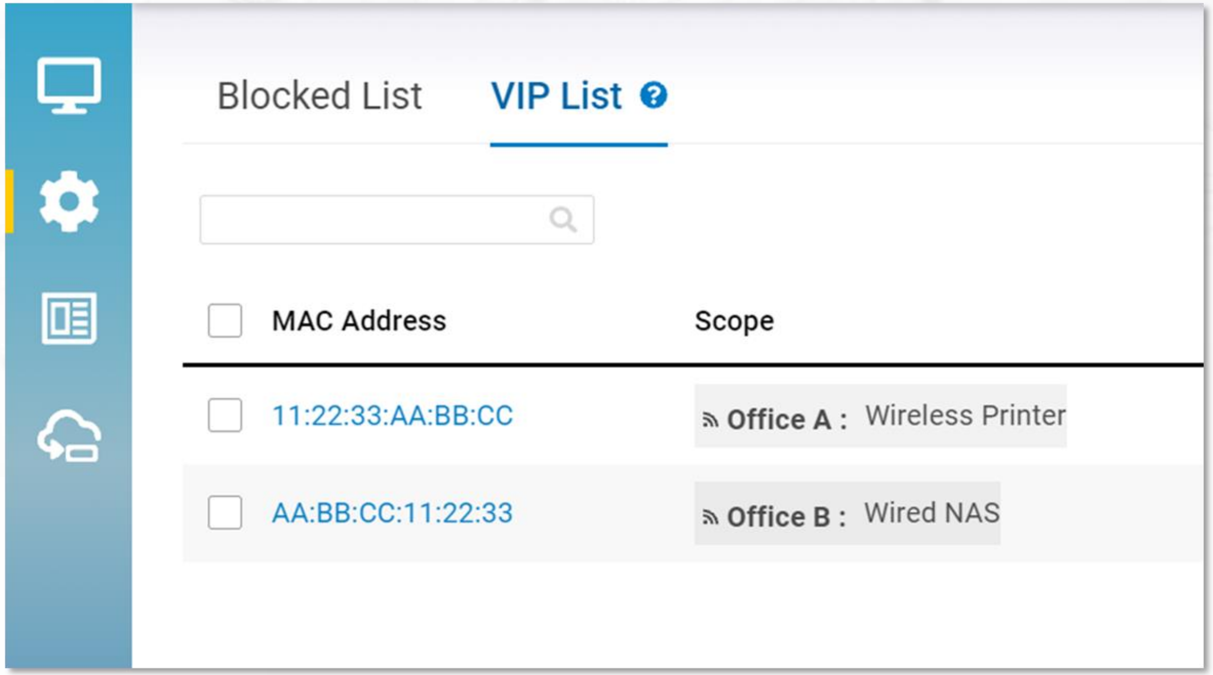
Access Denied

You have been blocked. Please contact the network administrator.

VIP List

The VIP List functions either as a Captive Portal bypass or L2 Isolation Whitelist depending on the interface (wired/wireless MAC address) registered:

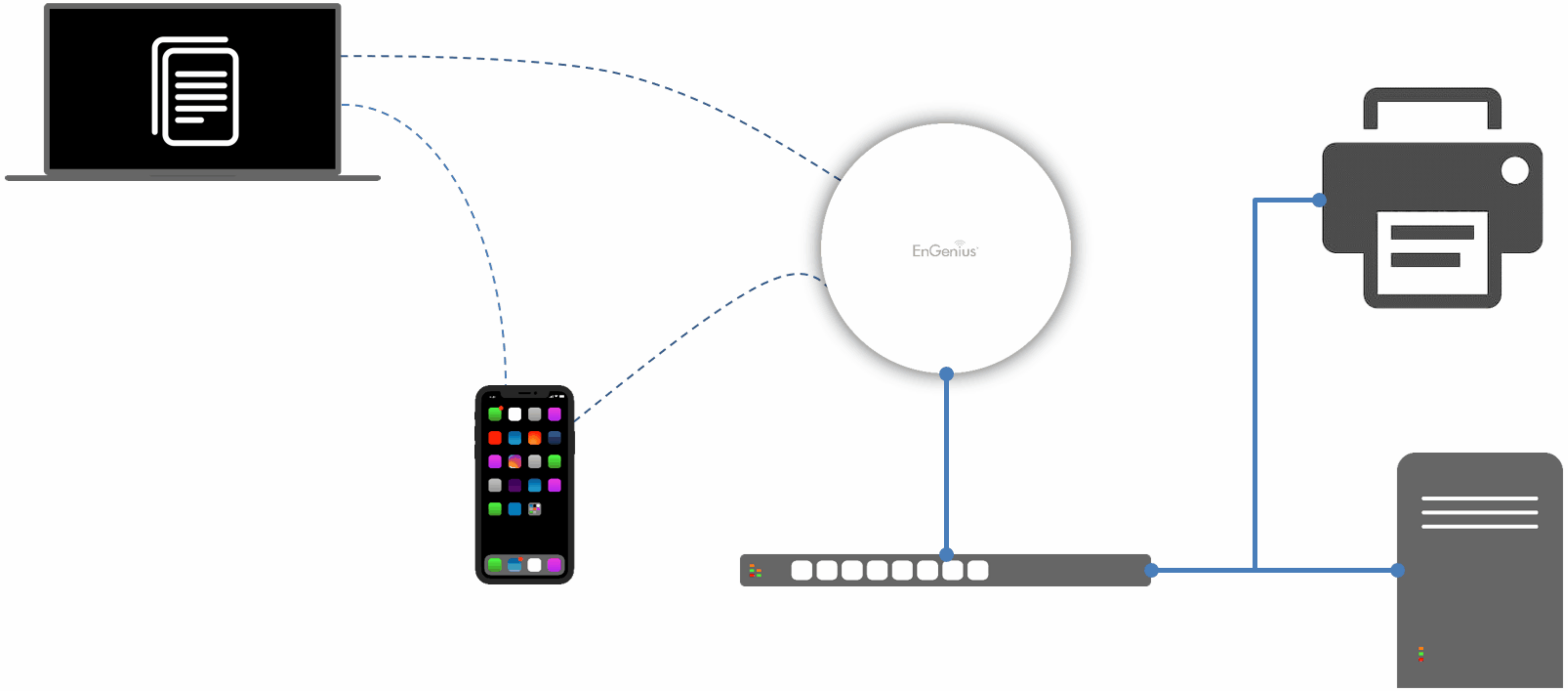
- Wireless devices such as printers or smart devices which are not able to authenticate on a captive portal will be allowed to bypass the splash page when tagged as VIPs.
- Wired devices registered as VIPs will be whitelisted on the network to allow access from wireless clients even when L2 Isolation is enabled.



□	MAC Address	Scope
□	11:22:33:AA:BB:CC	Office A : Wireless Printer
□	AA:BB:CC:11:22:33	Office B : Wired NAS

L2 isolation

L2 isolation prevents wireless to wireless and wireless to wired communication. To allow specific devices to still be accessible even when L2 isolation is enabled, the device such as a wired network printer, can be added as a VIP for access.



Random Wireless MAC Address

Staring iOS 14, and Android 10, a feature to enhance privacy when connecting to Wi-Fi networks was added to mobile devices. Enabled by default, it allows mobile devices to hide the actual hardware MAC address of the wireless adapter. This feature is useful when connecting to public networks; however, when associating to controlled environments such as offices or corporate networks, it may cause issues on the connection, as well as monitoring concerns for the network administrator.

On controlled environments, the MAC address of devices is used to identify the owner of the unit or the staff. When random MAC is activated, this prevents identification.

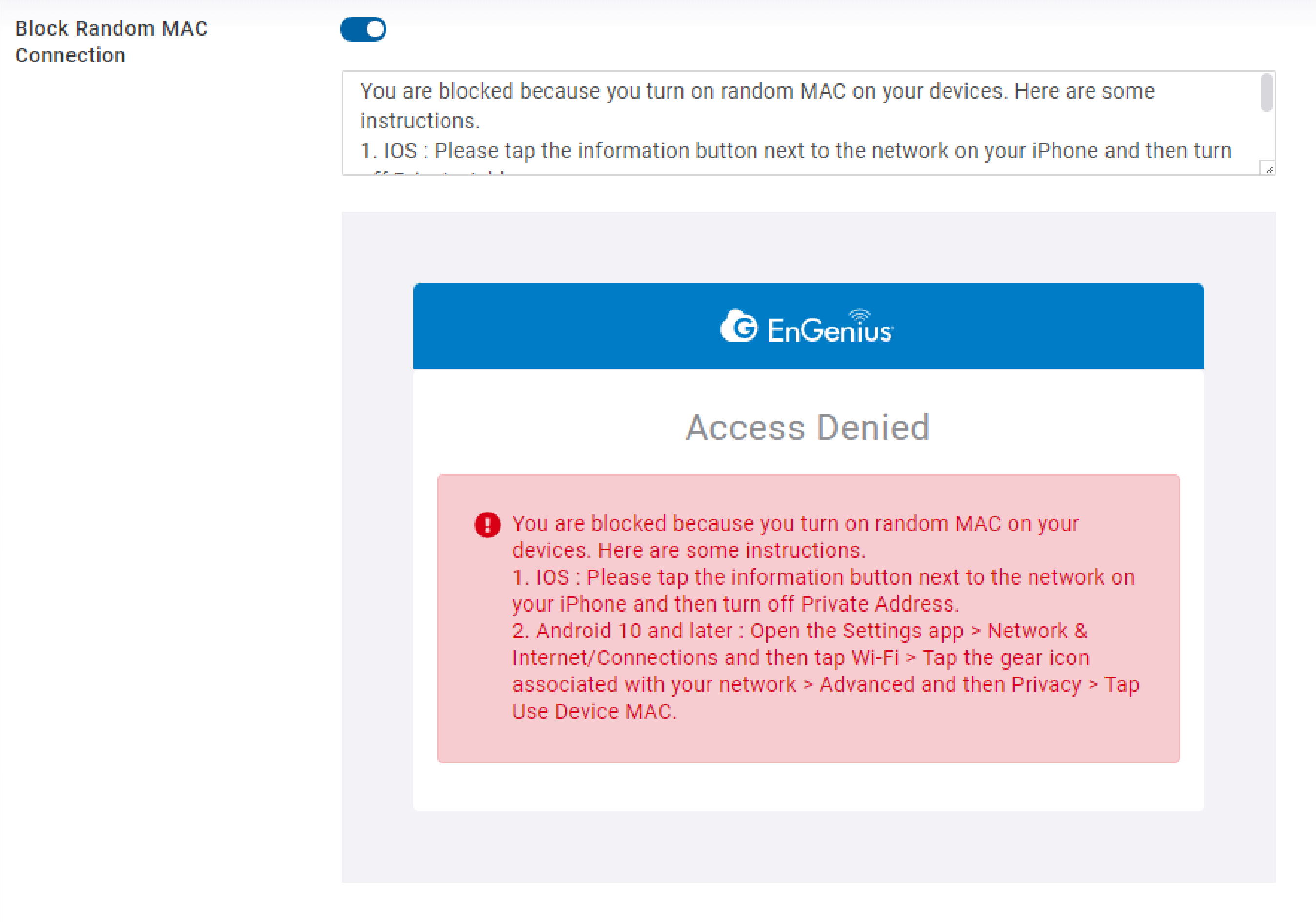
Some corporate networks also utilize MAC authentication especially in BYOD environments. This allows control over devices that connect to a secured network. Random MAC addresses essentially prevents an authorized device from connecting.

Block Random MAC Connection

EnGenius Cloud can prevent random MAC address from connecting on the wireless network by automatically identifying and blocking the device when an attempt to connect to the network is made.

The client will get a special splash page, with instructions on how to disable random MAC from their device. Once the client disables random MAC, they will be able to connect as usual.

(!) Windows 10 and above also has a random MAC address feature but is disabled by default.



Block Random MAC Connection

You are blocked because you turn on random MAC on your devices. Here are some instructions.
1. IOS : Please tap the information button next to the network on your iPhone and then turn

EnGenius

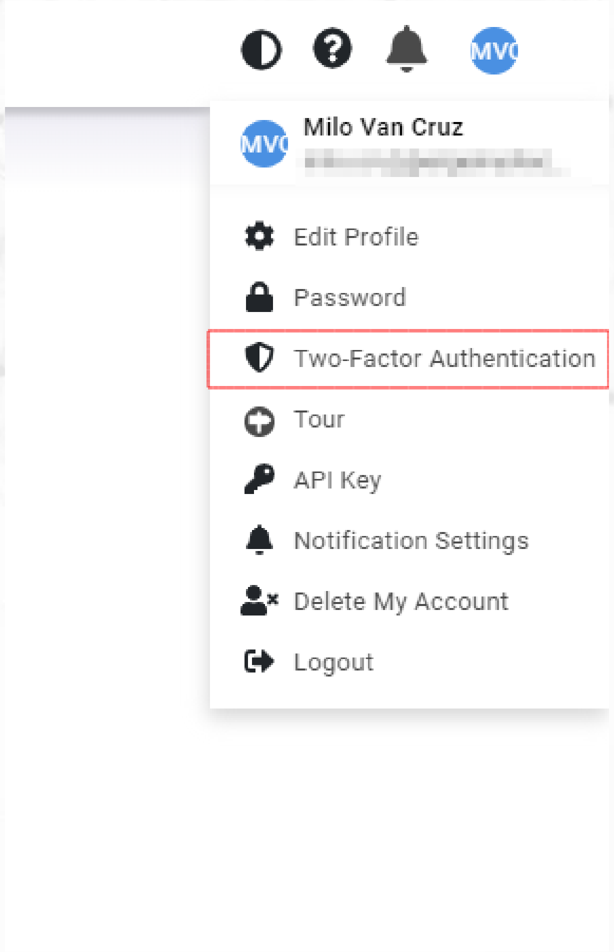
Access Denied

You are blocked because you turn on random MAC on your devices. Here are some instructions.
1. IOS : Please tap the information button next to the network on your iPhone and then turn off Private Address.
2. Android 10 and later : Open the Settings app > Network & Internet/Connections and then tap Wi-Fi > Tap the gear icon associated with your network > Advanced and then Privacy > Tap Use Device MAC.

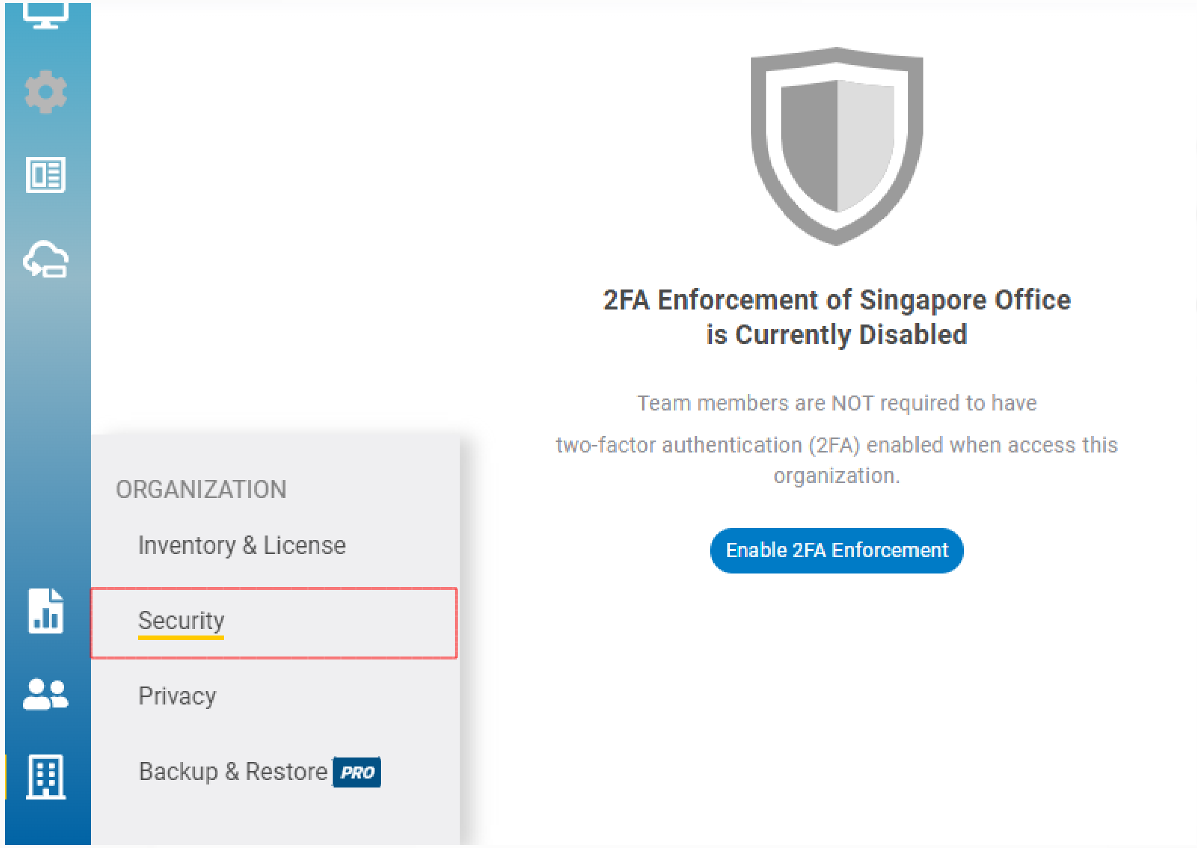
Two-Factor Authentication

2FA can be enabled on EnGenius Cloud, and pair with Google Authenticator. This adds an extra layer of security when logging on the EnGenius Cloud Portal, or when accessing 2FA-enabled Organizations.

(!) When 2FA is enabled, DO NOT delete the Google Authenticator app on your device. Doing so, without the backup keys, will prevent you from accessing your EnGenius Cloud account.

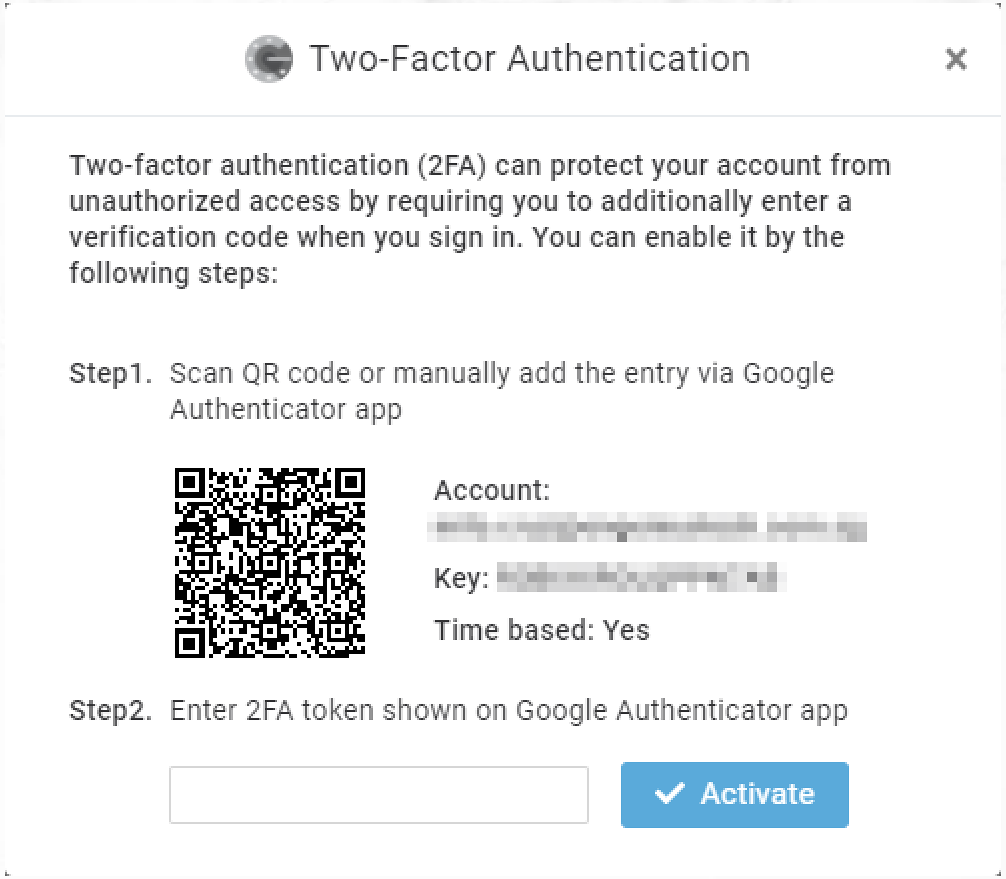


Two-Factor Authentication (2)



2FA Enforcement of Singapore Office is Currently Disabled

Team members are NOT required to have two-factor authentication (2FA) enabled when access this organization.



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

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

Account: [redacted]

Key: [redacted]

Time based: Yes

Step2. Enter 2FA token shown on Google Authenticator app

Diagnostic tools - topics

- Diagnostic SSIDs
- Real-time diagnostic tools

Diagnostic SSIDs

When deploying EnGenius Cloud APs, diagnostic SSIDs will broadcast error information if the AP detects network issues:

EnMGMTxxxx-No_Eth

Cause: AP does not have an Ethernet connection.

Solution: Check if the Ethernet cable is unplugged.

EnMGMTxxxx-No_IP

Cause: AP cannot get an IP address from DHCP server.

Solution: Check the AP's IP address configuration.

EnMGMTxxxx-IP_Conflict

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

Solution: Check the AP's IP address configuration.

.

EnMGMTxxxx-Gateway_ERR

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

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

EnMGMTxxxx-Proxy_ERR

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

Solution: Check the AP's proxy configuration in miscellaneous settings.

EnMGMTxxxx-DNS_ERR

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

Solution: Check the AP's IP address configuration.

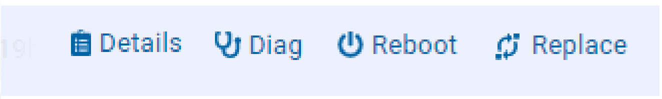
EnMGMTxxxx-Cloud_ERR

Cause: Everything seems to be working, but a connection to EnGenius Cloud cannot be established.

Solution: Check EnGenius Cloud server status from EnGenius support

Real-time diagnostic tools

EnGenius Cloud switches are equipped with diagnostic tools for quick troubleshooting. The diagnostic tools is accessible via the switch page when highlighting a device, or via the switch details page:



(!) These tools are available on both the Basic and PRO Licenses. Under the Basic License, the real-time duration is limited to 1 minute per activation. Real-time diagnostics has an interval of 1 second regardless of license level.

Real-time diagnostic tools

The availability of diagnostic tools on EnGenius Cloud enhances remote troubleshooting, without having to rely on external hardware and software to run these tasks.

The following items can be checked through the diagnostic tools:

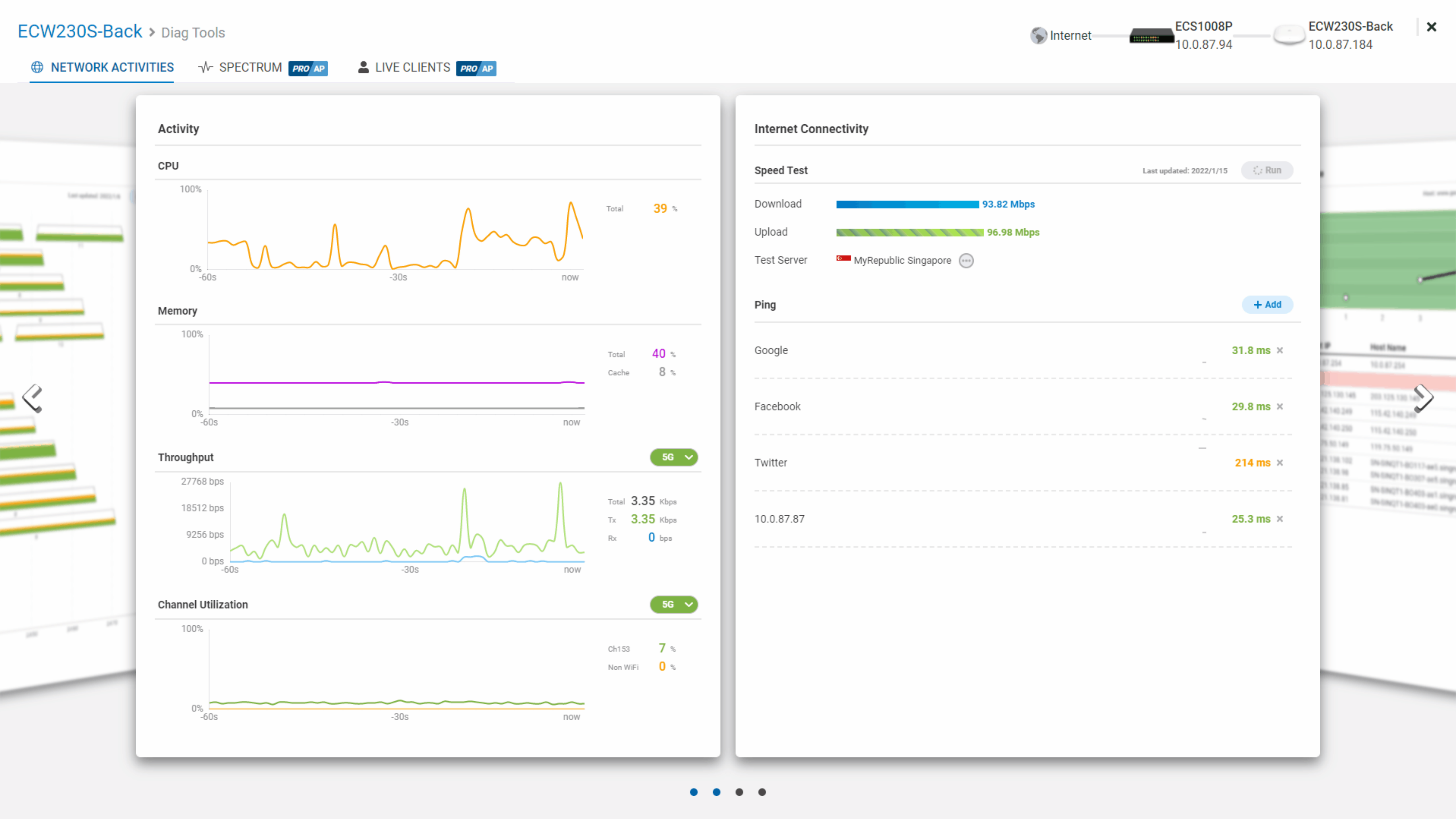
Activity

- CPU
- Memory
- Throughput
- Current-Channel Utilization

Internet Connectivity

- Speed Test
- Ping
- Traceroute

Channel Utilization Table



Activity

CPU

Total 39 %

Memory

Total 40 %
Cache 8 %

Throughput

Total 3.35 Kbps
Tx 3.35 Kbps
Rx 0 bps

Channel Utilization

Ch153 7 %
Non WiFi 0 %

Internet Connectivity

Speed Test

Last updated: 2022/1/15

Download 93.82 Mbps

Upload 96.98 Mbps

Test Server MyRepublic Singapore

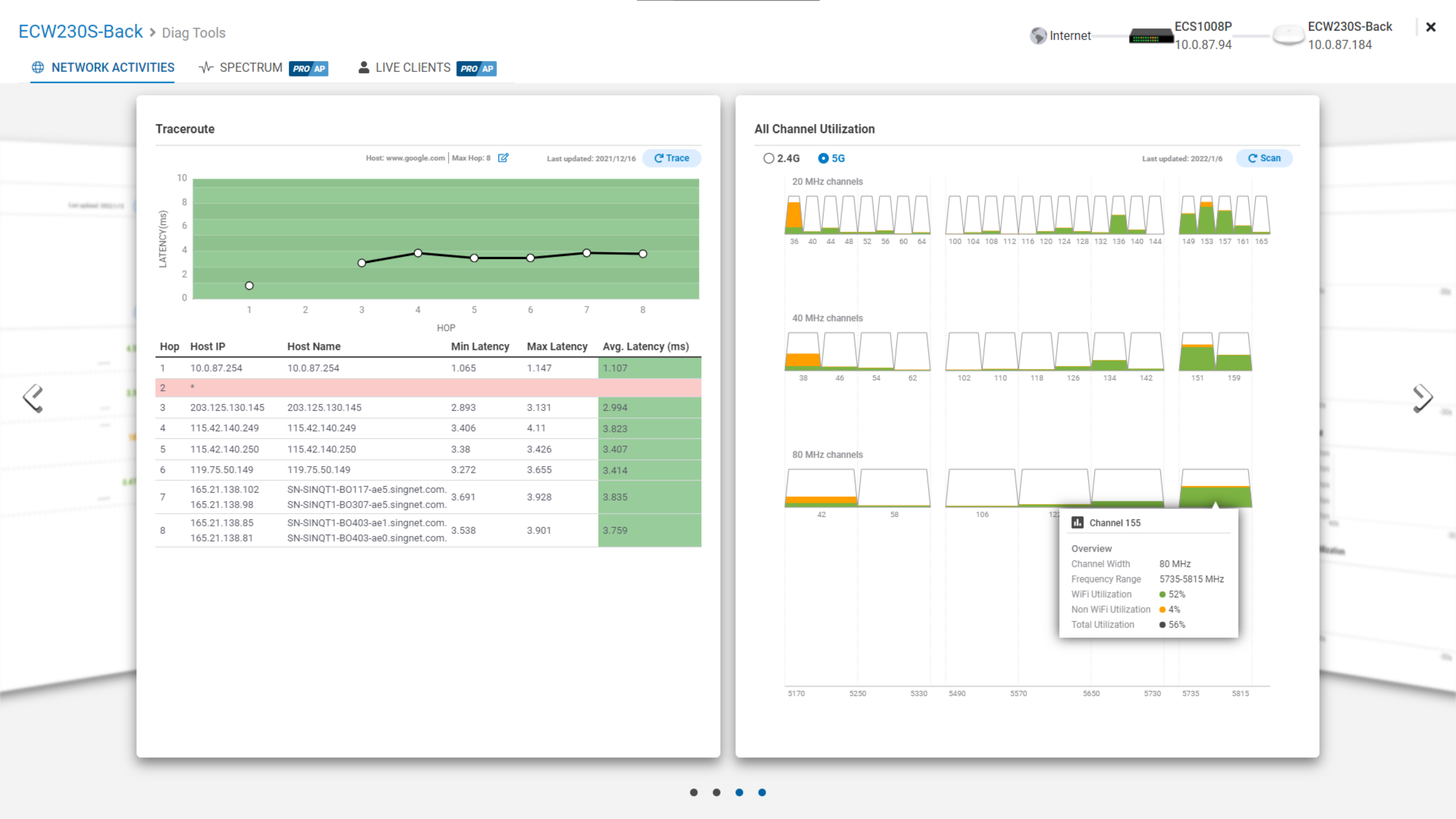
Ping

Google 31.8 ms ×

Facebook 29.8 ms ×

Twitter 214 ms ×

10.0.87.87 25.3 ms ×



Hop	Host IP	Host Name	Min Latency	Max Latency	Avg. Latency (ms)
1	10.0.87.254	10.0.87.254	1.065	1.147	1.107
2	*				
3	203.125.130.145	203.125.130.145	2.893	3.131	2.994
4	115.42.140.249	115.42.140.249	3.406	4.11	3.823
5	115.42.140.250	115.42.140.250	3.38	3.426	3.407
6	119.75.50.149	119.75.50.149	3.272	3.655	3.414
7	165.21.138.102 165.21.138.98	SN-SINQT1-BO117-ae5.singnet.com. SN-SINQT1-BO307-ae5.singnet.com.	3.691	3.928	3.835
8	165.21.138.85 165.21.138.81	SN-SINQT1-BO403-ae1.singnet.com. SN-SINQT1-BO403-ae0.singnet.com.	3.538	3.901	3.759

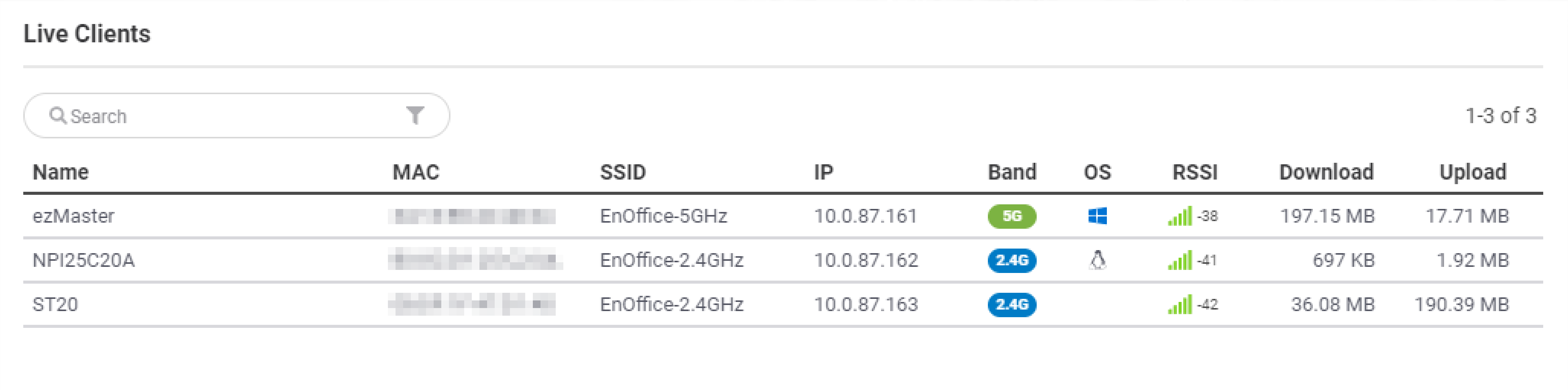
Channel 155

Overview

Channel Width	80 MHz
Frequency Range	5735-5815 MHz
WiFi Utilization	● 52%
Non WiFi Utilization	● 4%
Total Utilization	● 56%

Live clients (Pro)

When the AP is equipped with an AP PRO License, client devices can be viewed in real-time for a quick check on the status of each connected device.



Live Clients

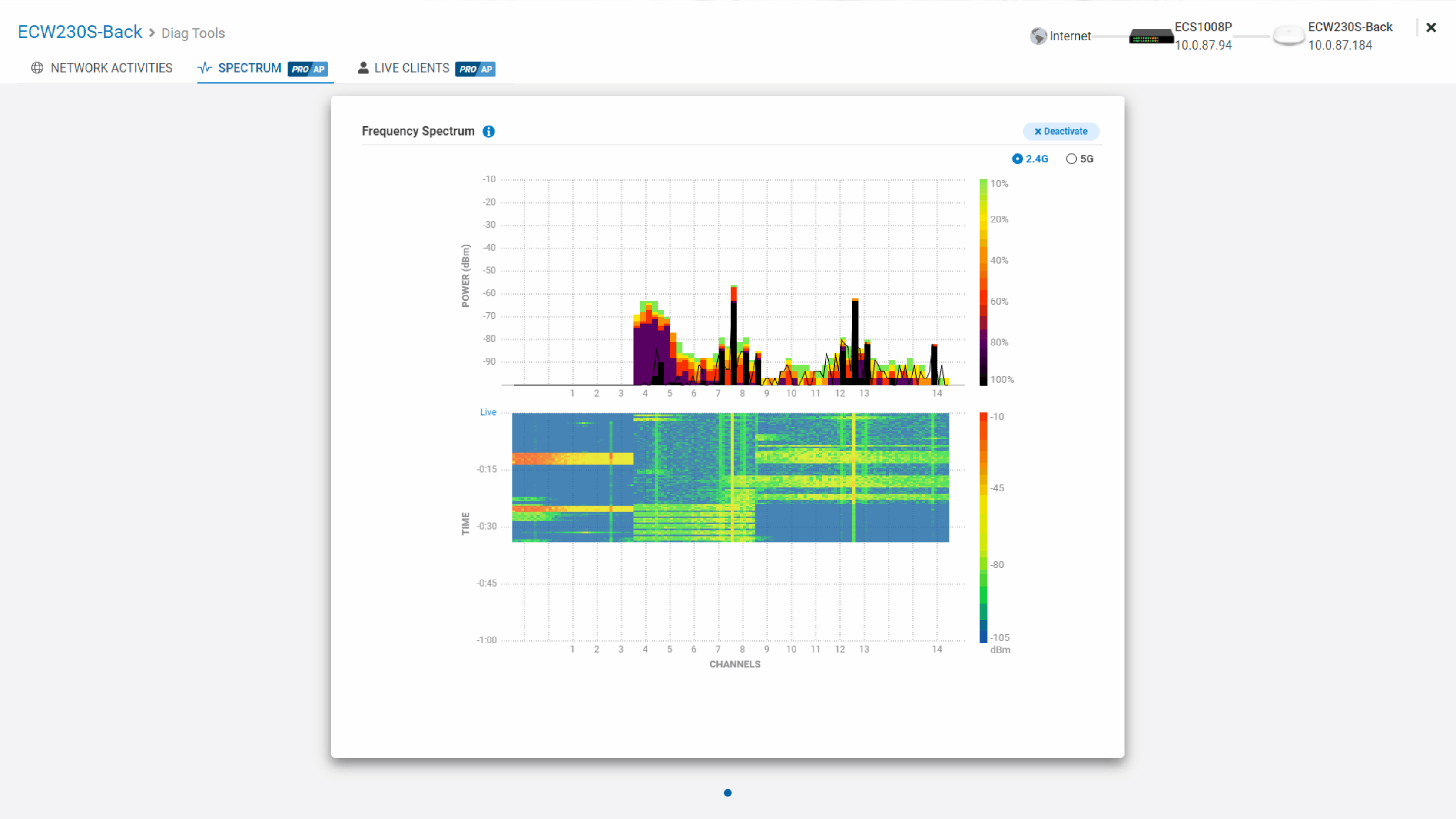
Search

1-3 of 3

Name	MAC	SSID	IP	Band	OS	RSSI	Download	Upload
ezMaster	[redacted]	EnOffice-5GHz	10.0.87.161	5G	⊞	-38	197.15 MB	17.71 MB
NPI25C20A	[redacted]	EnOffice-2.4GHz	10.0.87.162	2.4G	🐧	-41	697 KB	1.92 MB
ST20	[redacted]	EnOffice-2.4GHz	10.0.87.163	2.4G		-42	36.08 MB	190.39 MB

RF Analyzer

EnGenius Security APs are equipped with a full spectrum analyzer for real-time channel utilization and interference diagnostics without the need for additional hardware or software.



Glossary

EnGenius Certified Wireless Professional

Glossary

Access Control List (ACL)

a list of MAC addresses for either Black or white-listing.

Access Point (AP)

hardware device providing connection for a client device to the network over wireless.

Auto Channel

intelligent channel selection based on neighboring APs to avoid wireless interference.

Auto Power

intelligent power management based on neighboring APs to avoid wireless interference.

Band Steering

prioritize the 5GHz radio over 2.4 GHz for client device connections.

Broadcast

data that is being sent out to the entire network.

Channel

specific frequency at which a radio runs.

Channel Width

frequency range or span that directly affects connectivity speed of a radio. also referred to as *channel HT/VHT (high throughput/very high throughput)*.

Glossary

Client

a device with the ability to connect to the network. also referred to as *wired/wireless client*.

dBi (decibel isotropic)

unit of measurement to define the antenna's power gain.

dBm (decibel-milliwatt)

unit of measurement to define the transmit power of an access point.

Dual-Band

an access point with two radios, 2.4GHz and 5GHz.

Encryption

process of encoding wireless data to further secure a network.

Fast Roaming

allow a client to seamlessly transit from one AP to another without disruptions on applications.

L2 Isolation

prevents wireless clients from being able to communicate with any other client (including wired clients) on the network.

LOS (line-of-sight)

a straight line between two devices, free of obstructions.

MAC Address

unique identifier for every network interface.

Glossary

Managed Mode

a device that is operating under a controller or management system.

Multicast

data that is being sent out to multiple destinations.

RSSI (received signal strength indication)

measurement of radio power on the receiver.

RSSI threshold

minimum signal level tolerance setting to allow clients to switch over to other APs or radios with stronger coverage.

SSID (service set identifier)

name of a Wi-Fi network.

TX power (transmit power)

power level of an access point or radio which is proportional to its coverage.

Wireless Mesh

interconnection of access points to form a distributed network through Wi-Fi architecture.

Exam

EnGenius Certified Wireless Professional

Exam

- You need to open all online subject before you can do the exam.
  - 40 questions
  - 40 minutes
  - 3 tries total
    If you fail a third time, please contact us via academy@engenius.ai for additional tries.

Visualize Your Network

EnGenius