Grandstream Networks, Inc.

GWN Management Platforms

GWN.Cloud: *Cloud based Access Points Controller*

GWN Manager: *On-premise Access Points Controller*

User Guide

COPYRIGHT

The latest electronic version of this guide is available for download here:

http://www.grandstream.com/support

Table of Contents

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes the basic concepts and operations necessary to use GWN Management Platforms to manage multiple GWN Access points including GWN7610, GWN7600, GWN7630 and GWN7600LR. The intended audiences of this document are network administrators.

This guide will cover the below topics:

- Product Overview
- Getting To Know GWN Management Platform
- Getting Started With GWN Management Platform
- Dashboard
- Network
- Access Points
- SSID
- Clients
- Captive Portal
- Access Control
- Insight
- System
- User Management
- Global

CHANGE LOG

This section documents significant changes from previous versions of the GWN Management Platform User Manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

GWN.Cloud

Version 1.0.19.7

- Support client name in csv file when import access list. [Access List]
- Added secondary RADIUS server for WLAN 802.1x authentication. [Wi-Fi Settings]
- Added WPA3 options for SSID setting. [Security Mode]
- Moved upgrade feature from Network to Global. [Upgrade]

Version 1.0.19.2

- Added new statistical graphs for top website and guest count. [Overview] [Overview Page]
- Added API feature. [API Developer]
- Added SNMP feature. [SNMP]
- Added Rogue AP feature. [Rogue AP]
- Added Firewall feature. [Firewall]
- Added Hotspot 2.0 feature (Beta). [Hotspot 2.0]
- Added NAT as a new client IP assignment method. [NAT Pool]
- Added support for 802.11w Management Frame Protection. [802.11w]
- Added support to import access list by csv file. [Access List]

Version 1.0.10.7

- Added Site Survey feature. [Site Survey]
- Added feature of Minimum Rate Control. [Enable Minimum Rate] [Minimum Rate (Mbps)]
- Added feature of SSH Remote Access. [SSH Remote Access]
- Added feature of External Portal support Socifi Platform. [External Splash Page]

- Added feature of Client inactivity timeout. [Client Inactivity Timeout]
- Added feature of Upgrade Regularly. [Upgrade]
- Added feature of Client Steering. [RADIO]
- Enhanced feature of Voucher: display of remaining bytes. [Figure 80: Voucher Details]
- Enhanced feature of Dynamic VLAN. [Enable Dynamic VLAN]
- Changed LED patterns. [GWN76xx LED Patterns]

Version 1.0.9.8

- Added support for collecting user feedback from GWN Cloud page. [
- Feedback]
- Added support for Voucher Style Customization. [Voucher Settings]
- Added support for video URL. [Advertisement]
- Added support to export Guest Information via Email. [Email Guest Information]
- Added support for client RX/TX Rate display. [Status]
- Expanded Max Devices to use the same Voucher. [Voucher]
- Added support to enable/disable client connection/disconnection events.

Version 1.0.8.17

- Added support for Advertisement for Captive Portal [Advertisement]
- Added support for Custom Field for Captive Portal Splash Page [Splash Page][Guest]
- Added feature of ARP Proxy. [ARP Proxy]
- Added support of Clear client data. [Status]
- Enhanced Event log by Wi-Fi authentication event. [Event Log per AP]
- Added EU Server support. [Zone]
- Enhanced Bandwidth Rules by adding option to limit bandwidth Per-Client. [Range Constraint]
- Added Total Bandwidth Usage Display [Summary][Overview][Status]
- Added Export Immediately feature for URL Access Logs. [URL Access Log]

Version 1.0.8.7

- Added support for URL logging (Except for GWN7610). [URL Access Log]

Version 1.0.7.18

- Enhanced Client Information. [Summary] [Client Manufacturer] [Client OS]
- Enhanced Access Point status. [Status]
- Added Reset access point button. [Reset Access Points]
- Added External Captive Portal Support. [External Splash Page]
- Added AP Scheduling Reboot. [Reboot Schedule]
- Added Change Log section. [Change Log]
- Added Account idle timeout. [Account Idle timeout]
- Added feature of Wi-Fi Statistic Report. [Report]
- Added feature of Captive Portal Guest Summary. [Summary]
- Changed SSID limit. [SSID Limit]
- Enhanced Wi-Fi Service by adding configurable options. [Beacon Interval] [DTIM Period] [Convert IP multicast to unicast].
- Enhanced Captive Portal features. [Failsafe Mode] [Daily Limit] [Byte Quota] [Force To Follow]

Version 1.0.0.37

- This is the initial version for GWN.Cloud.

GWN Manager

Version 1.0.19.8

- No major changes.

Version 1.0.19.7

- Support client name in csv file when import access list. [Access List]
- Added secondary RADIUS server for WLAN 802.1x authentication. [Wi-Fi Settings]
- Added WPA3 options for SSID setting. [Security Mode]

- Moved upgrade feature from Network to Global. [Upgrade]

Version 1.0.19.2

- Added new statistical graphs for top website and guest count. [Overview] [Overview Page]
- Added API feature. [API Developer]
- Added SNMP feature. [SNMP]
- Added Rogue AP feature. [Rogue AP]
- Added Firewall feature. [Firewall]
- Added Hotspot 2.0 feature (Beta). [Hotspot 2.0]
- Added NAT as a new client IP assignment method. [NAT Pool]
- Added support for 802.11w Management Frame Protection. [802.11w]
- Added support to import access list by csv file. [Access List]

Version 1.0.0.33

- This is the initial version for GWN Manager.

REQUIREMENTS

Following table shows the requirements of Grandstream networking products GWN76xx and version of APP per GWN Management Platform:

Table 1: Requirements

	Model	GWN.Cloud 1.0.19.7		GWN Manager 1.0.19.7	
		Minimum	Recommended	Minimum	Recommended
Version of AP	GWN7610	1.0.6.37	1.0.19.15	1.0.15.20	1.0.19.15
	GWN7600	1.0.8.17			
	GWN7600LR	1.0.8.17			
	GWN7630	1.0.9.2			
	GWN7630LR	1.0.11.8			
	GWN7602	1.0.1.6			
Version of APP	iOS™	1.0.5	1.0.6	1.0.6	1.0.6
	Android™	1.0.0.14	1.0.0.20	1.0.0.19	1.0.0.20
System (GWN Manager only)	**OS:** Linux Redhat7, CentOS 7 **Hardware:** - **For up to 200 APs and 2000 Clients:** • CPU: Intel® Core™ i3-3240 or above • RAM: 4GB or above • Storage: 250GB (SSD preferred, depend on retained data size) - **For up to 3000 APs and 30000 Clients:** • CPU: Intel® Xeon® Silver 4210 • RAM: 16GB or above • Storage: 250GB (SSD preferred, depend on retained data size)				

WELCOME

Thank you for using Grandstream GWN Management Platform.

GWN Management Platforms are enterprise-grade Wi-Fi network management platforms that offer a centralized, streamlined network management and monitoring. This includes GWN.Cloud, the cloud-based platform and the GWN Manager which is a Linux based platform. Both solutions allow business to deploy a secure Wi-Fi network in seconds and manage those networks across multiple locations through a web user interface. Users can keep an eye on the network's performance with real-time monitoring, alerts, statistics and reports that can be viewed using a web browser or the mobile application.

PRODUCT OVERVIEW

Features Highlights

GWN.Cloud	• Software-as-a-Service (SaaS) Solution to manage all your Grandstream Access point, without any additional on-premise infrastructure. • High level security, since all the traffic between GWN AP and cloud is secured, in addition to powerful authentication method required to add new AP. • Easy way to add new access point, either by scanning a barcode from GWN.Cloud App (iOS & Android) or by entering AP MAC and random password. • No limits on number of sites or APs
GWN Manager	• Linux solution to secure manage all your Grandstream Access point • Automatically discover and Adopt Access point in your network • Adopt APs manually using SSH or through Web GUI by setting the Manager address and port. • Up to 3000 APs, with high performance hardware
Shared	• Highly available with no single point of failure across the whole system. • Easy and intuitive dashboard for monitoring. • Network Group creation. • AP and clients Centralized monitoring and management. • Captive portal configuration. • Bandwidth control per SSID, IP, or MAC address.

Specifications

Table 2: GWN Management Platform Specifications

Function	• Network-based AP management • Network/AP/client monitoring
Security and Authentication	• Supports access policies configuration (blacklist, whitelist, time policy) • Multiple security modes including WPA, WPA2, WPA3, WEP, open, etc. • Bandwidth rules for client access • User and privilege management
Enterprise Features	• No limits on number of sites or APs for GWN.Cloud; Up to 3000 APs for GWN Manager with high performance hardware • Hosted by AWS with 99.99% uptime (GWN.Cloud only) • Bank-grade TLS encryption from end-to-end • X.509 certificate-based authentication • Supports Wi-Fi Alliance Voice-Enterprise • Mobile app for iOS^{TM} and Android^{TM} • Real-time Wi-Fi Scan for deployment • URL access log collection • Multiple Wi-Fi performance optimization methods including band steering, Minimum RSSI, ARP Proxy, IP multicast to unicast, etc
Supported Wi-Fi Access Points	GWN7610, GWN7600, GWN7600LR, GWN7630, GWN7630LR, GWN7602, GWN7605, GWN7605LR, GWN7615.
Captive Portals	• Splash page with built-in WYSIWYG editor • Facebook, Twitter integration • Multiple captive portal authentications including simple password, radius, voucher, custom field etc. • External captive portal integration

	- Real-time guest statistics and monitoring - Advertisement integration with flexible strategies - Export guest info into file and automatically send to email
Centralized Management	- Local data forwarding, no user traffic sent to the controller - Network-based AP management - Network/AP/client monitoring - Layer2 and Layer3 based AP discovery
Reporting and Monitoring	- Real-time Wi-Fi AP and client monitoring - Detailed reports by network, AP, client etc. - Retrieval of historical data for statistical observations - Real-time alerts and event logs
Maintenance	- Ping/traceroute/capture - Both configuration and data backup - Scheduled AP firmware update and LED control - Change log for audit trail
Languages	English, Chinese, French, German, Portuguese and Spanish

GETTING TO KNOW GWN MANAGEMENT PLATFORM

GWN.Cloud

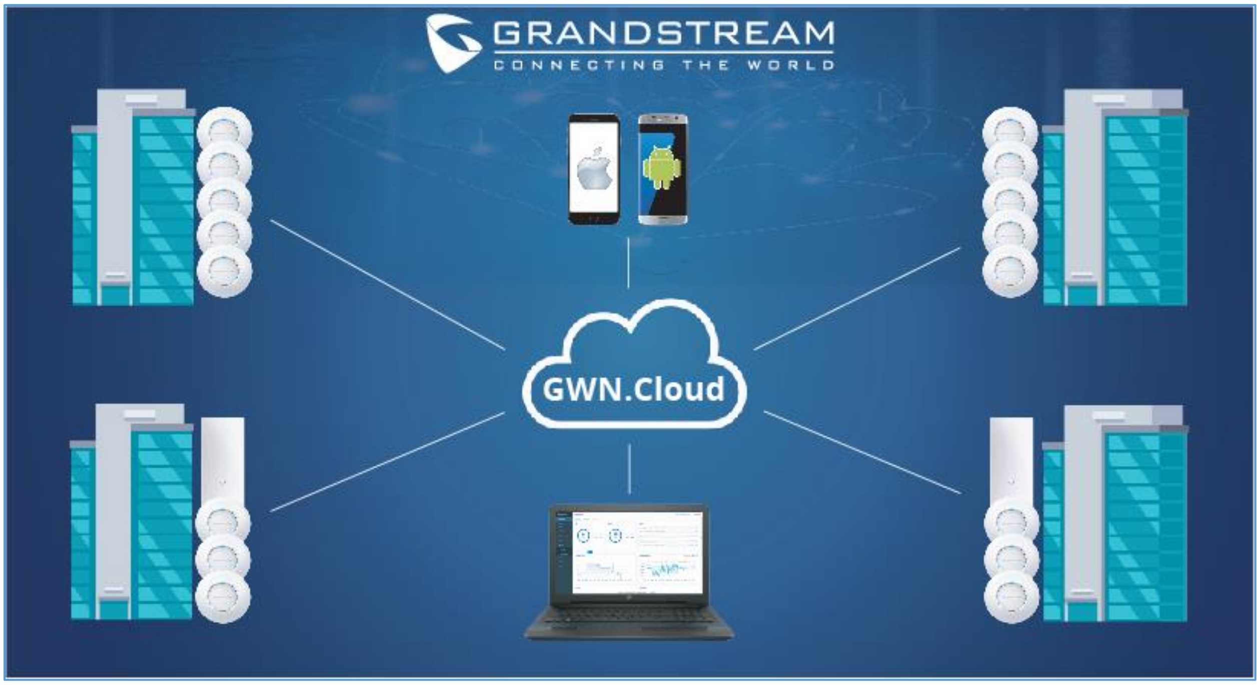


Figure 1: GWN.Cloud Architecture

GWN.Cloud is a cloud-based platform used to manage and monitor GWN Access points wherever they are in Internet. The platform can be accessed using the following link: https://www.gwn.cloud/login

It provides an easy and intuitive web-based configuration interface as well as an Android App.

Sign up to GWN.Cloud

When accessing GWN.Cloud for the first time, users are required to sign up. The following screen will be displayed:

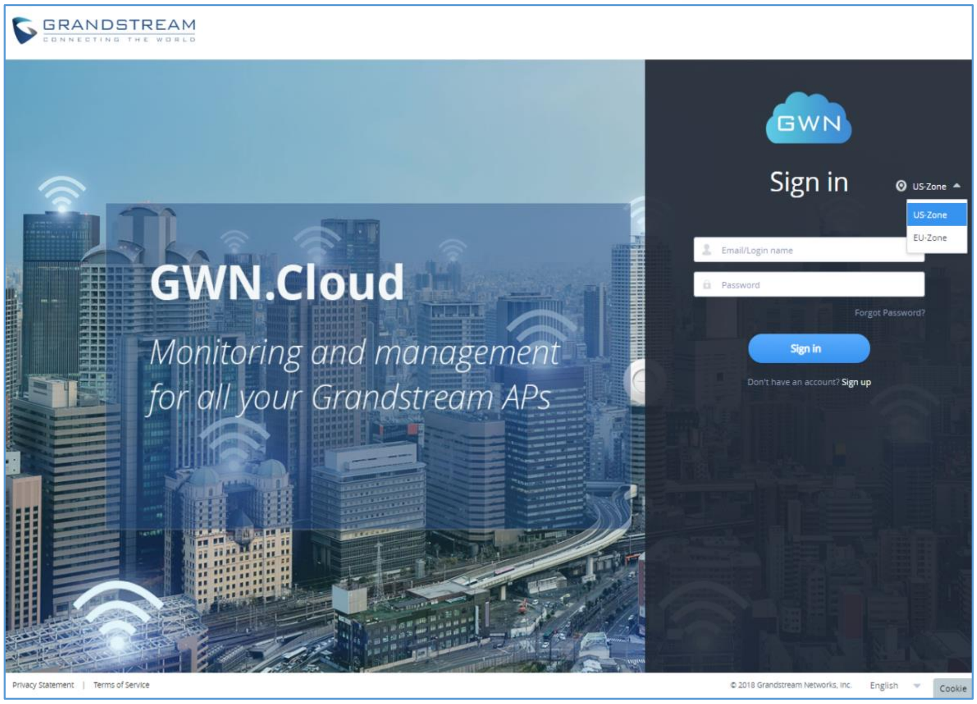

GRANDSTREAM
CONNECTING THE WORLD
GWN.Cloud
Monitoring and management for all your Grandstream APs
GWN
Sign in
US-Zone
US-Zone
EU-Zone
Email/Login name
Password
Forgot Password?
Sign in
Don't have an account? Sign up
Privacy Statement | Terms of Service
© 2018 Grandstream Networks, Inc.
English
Cookie

Figure 2: GWN.Cloud Login Page

1. Click on Sign up to go to the sign-up screen, then enter the required information.

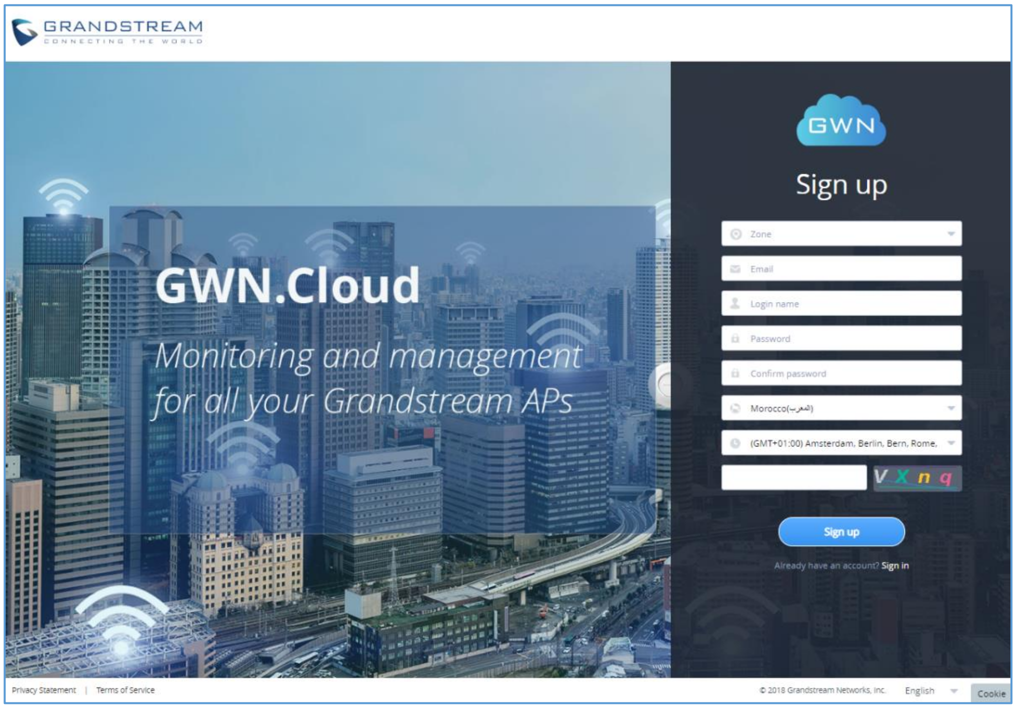
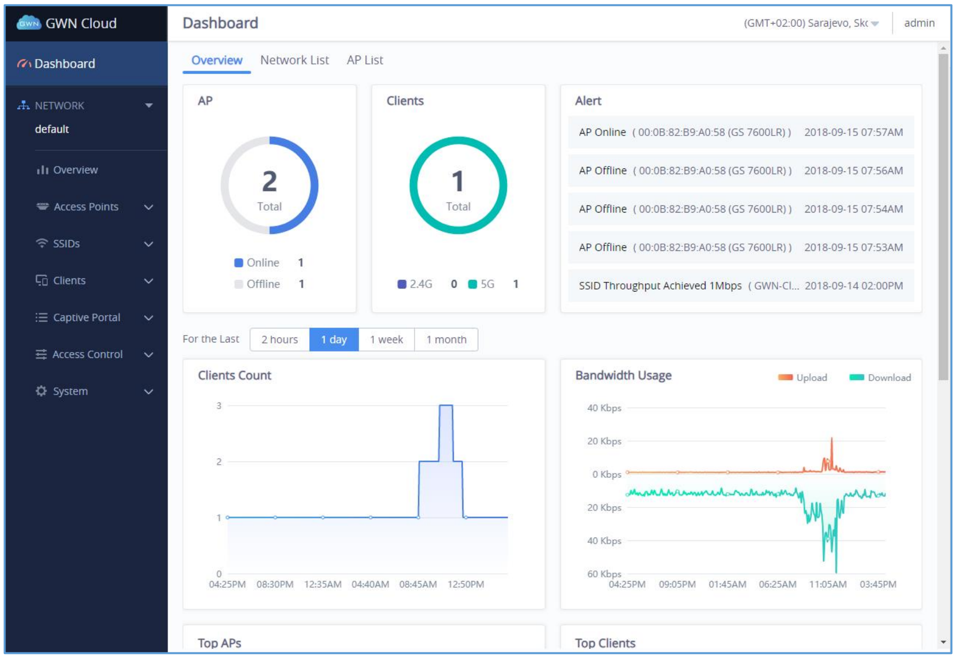

GRANDSTREAM
CONNECTING THE WORLD
GWN.Cloud
Monitoring and management for all your Grandstream APs
GWN
Sign up
Zone
Email
Login name
Password
Confirm password
Morocco(المغرب)
(GMT+01:00) Amsterdam, Berlin, Bern, Rome,
V X n q
Sign up
Already have an account? Sign in
Privacy Statement | Terms of Service
© 2018 Grandstream Networks, Inc.
English
Cookie

Figure 3: GWN.Cloud Sign up page

Table 3: GWN.Cloud Sign up Settings

Zone	Users will need to choose **US server** or **EU server** to store their data at. This is mainly for GDPR regulation compliance.
Email	This email will be used to receive account activation link and also can be used as a username when login to GWN.Cloud.
Login name	Enter the login name that will be used to login to your GWN.Cloud space.
Password	Enter the password for Login authentication
Confirm password	Confirm the previously entered password
Country/Region	Enter the country/region on which applies to your account.
Time zone	Set your time zone.
Confirmation code	Copy the confirmation from the Captcha.

2. Once you create an account, you can access to your GWN.Cloud page for the first time and the following page will be displayed:



AP Online (00:0B:82:B9:A0:58 (GS 7600LR)) 2018-09-15 07:57AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR)) 2018-09-15 07:56AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR)) 2018-09-15 07:54AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR)) 2018-09-15 07:53AM
SSID Throughput Achieved 1Mbps (GWN-Cl... 2018-09-14 02:00PM

Figure 4: GWN.Cloud Dashboard

GWN Manager

Figure 5: GWN Manager Architecture

GWN Manager is an On-premise Access Points Controller used to manage and monitor GWN Access points on your network. The GWN Manager platform can be installed and accessed by following the steps below:

Installation Steps

1. **Install dependencies:**

- Type in the following commands under CentOS Terminal

```
yum install epel-release

yum install jemalloc libaio glibc-devel fontconfig xorg-x11-font-utils freetype
```

2. **Installing GWN Manager**

- Download link: https://www.grandstream.com/support/tools?hsLang=en
- After a successful download, browse to the file directory and uncompress it:

```
tar -zxvf GWN_Manager-1.0.0.21-201912121121.tar.gz
```

- Then, Install all packages:

```
rpm -ivh gwn*1.0.0.21*.rpm
```

Warning: Please use the rpm packages we provided to install mariadb, redis, nginx, or GWN Manager may work abnormally.

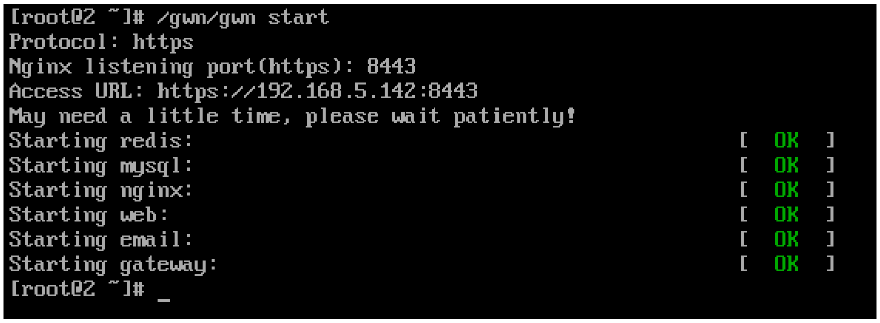
3. **Add firewall exceptions:**

```
firewall-cmd --zone=public --add-port=8443/tcp –permanent

firewall-cmd --zone=public --add-port=10014/tcp –permanent

firewall-cmd --reload
```

Note: By default, GWN Manager use port 8443 for web service (nginx) and port 10014 for gateway communication separately.

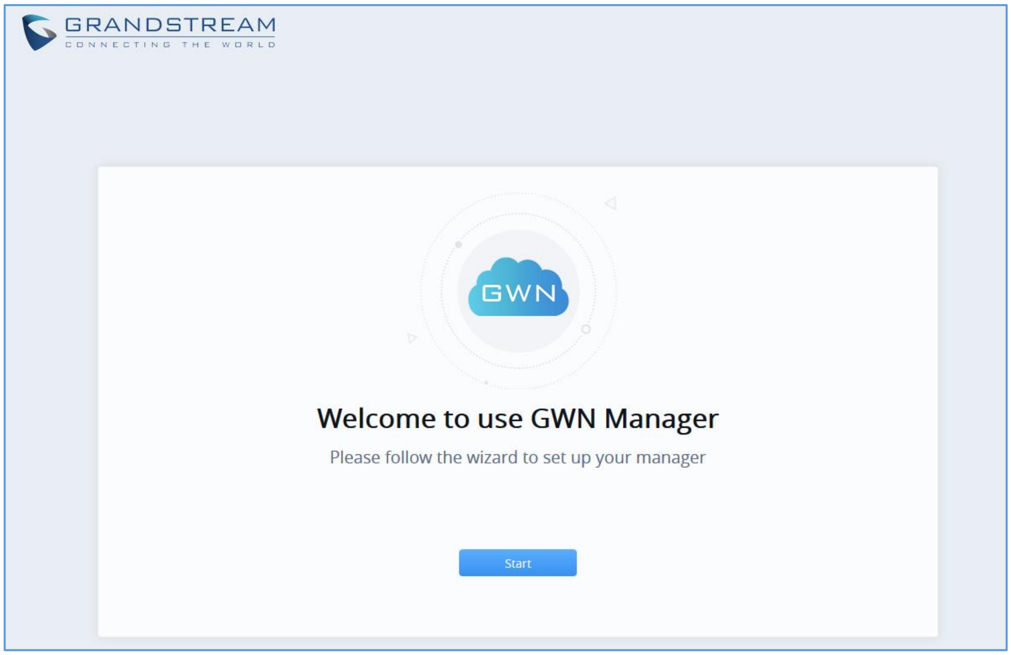
4. **Run the script to start the services:**

```
/gwn/gwn start
```



```
[root@2 ~]# /gwn/gwn start
Protocol: https
Nginx listening port(https): 8443
Access URL: https://192.168.5.142:8443
May need a little time, please wait patiently!
Starting redis:                                       [  OK  ]
Starting mysql:                                       [  OK  ]
Starting nginx:                                       [  OK  ]
Starting web:                                         [  OK  ]
Starting email:                                       [  OK  ]
Starting gateway:                                     [  OK  ]
[root@2 ~]# _
```

Note: After all services starting up, please go to the Web Portal for further configuration. By default, the Web Portal address is *https://server_ipaddress:8443*



Welcome to use GWN Manager

Please follow the wizard to set up your manager

Figure 6: GWN Manager Start page

Note: GWN Manager installation is supported on virtual machines (Tested on **VMware** & **VirtualBox**).

Configuring GWN Manager

Users can change the nginx binding protocol, port as well as access address for communication:

```
/gwn/gwn config
```

Warnings:

- If you change the nginx binding port, do not forget to add a new firewall exception, and if you change the IP address of your machine, don't forget to update the config of access address synchronously. Moreover, for security consideration, GWN Manager runs as a non-root user, so please use a number larger than 1024 as the nginx binding port number, or you may fail to start the service due to denied permission.
- HTTPs is used by default due to its security, and GWN Manager will automatically generate certificate along with private key after installation. You can also apply for a certificate that signed by trusted authority to replace it. Path to replace the ssl certificate and private key:

- certificate: /gwn/conf/nginx/ssl.pem
- private key: /gwn/conf/nginx/ssl.key

- After replacing the two files, restart gwn service to validate it:

```
/gwn/gwn restart
```

- If the login password is forgotten, users can change it using the command below:

```
/gwn/gwn modify-password
```

Upgrading GWN Manager

GWN Manager will check for the new firmware version automatically when you log into web GUI, if a new version is found, a notification will pop-up and you may click to complete upgrade. You can also upgrade manually using the below commands:

```
rpm -Uvh gwn*1.0.0.13*.rpm

/gwn/gwn restart
```

Uninstalling GWN Manager

Run these commands to uninstall GWN packages from your Linux system:

```
rm -e gwn gwn-redis gwn-mariadb gwn-nginx

rm -rf /gwn
```

Important Notes

- GWN Manager only support one access address at present, so if your machine has more than one network interface, you should set the access address to the one (IP address) that you expect to communicate with Access point.
- Please consider setting the right time zone of your machine before running GWN Manager, modifying the time zone may cause data corruption.

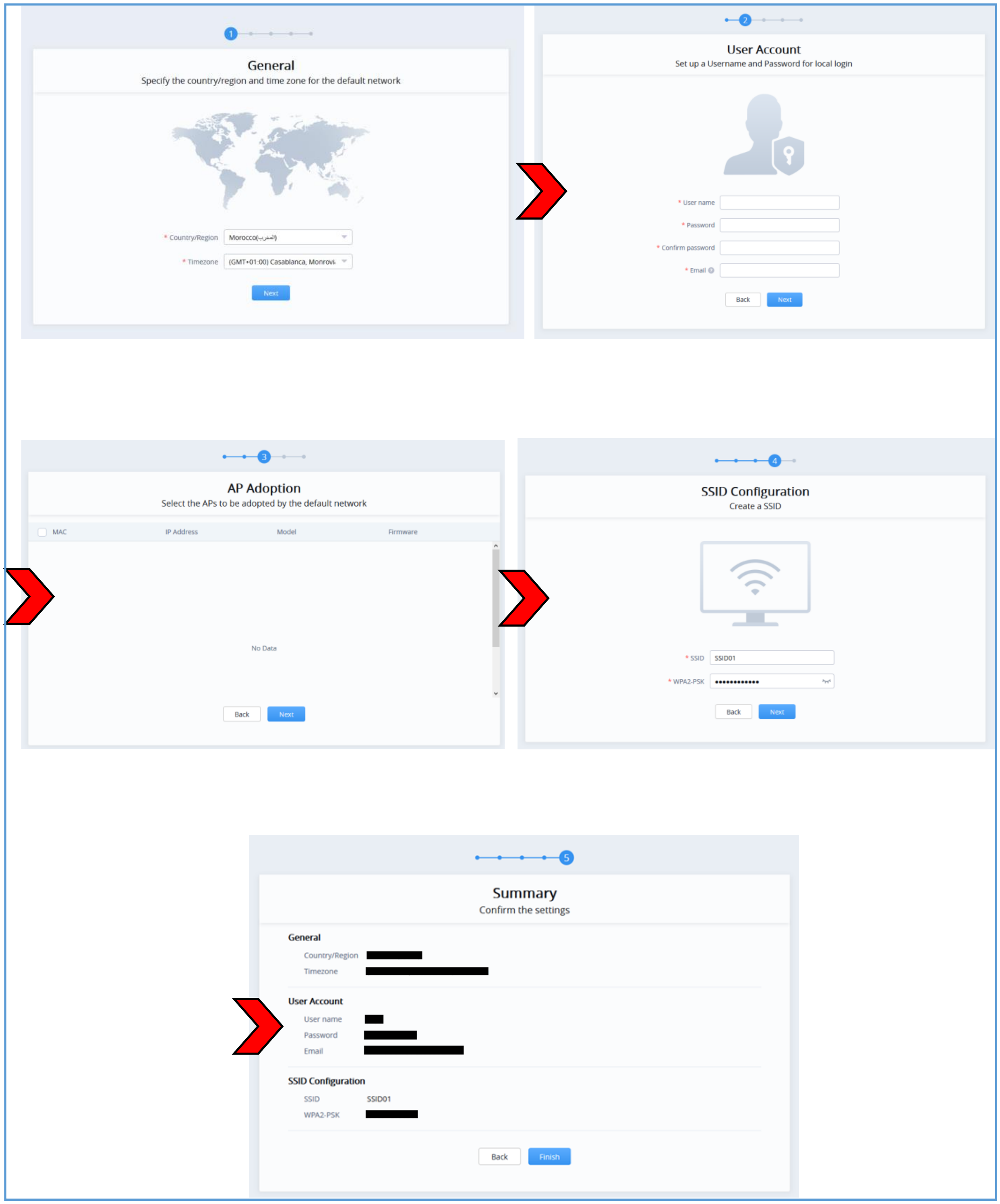
First Use

The GWN Manager provides an easy and intuitive Web UI to manage and monitor GWN76xx Access Points, it provides users access to all GWN Access Points settings, without any additional on-premise infrastructure.

On first use, users need to fill in additional information following the GWN Manager Wizard:

Table 4: GWN Manager Setup Wizard

General	Specify the country/region and time zone for the default network: Country/Region Time zone **Note**: These parameters can be automatically detected by the system
User Account	Set up a Username and Password for local login Username Password Confirm password Email
AP Adoption	Select the APs to be adopted by the default network. **Note:** APs Available on the same LAN will be detected automatically
SSID Configuration	Create a SSID
Summary	Review all the previous settings



1 General
Specify the country/region and time zone for the default network

- * Country/Region: Morocco(المغرب)
- * Timezone: (GMT+01:00) Casablanca, Monrovi

2 User Account
Set up a Username and Password for local login

- * User name
- * Password
- * Confirm password
- * Email

3 AP Adoption
Select the APs to be adopted by the default network

MAC	IP Address	Model	Firmware

No Data

4 SSID Configuration
Create a SSID

- * SSID: SSID01
- * WPA2-PSK: ••••••••••••

5 Summary
Confirm the settings

General

- Country/Region: [redacted]
- Timezone: [redacted]

User Account

- User name: [redacted]
- Password: [redacted]
- Email: [redacted]

SSID Configuration

- SSID: SSID01
- WPA2-PSK: [redacted]

Figure 7: GWN Manager Wizard

Sign up to GWN Manager

Enter the previously configured user credentials to access the GWN Manager GUI:

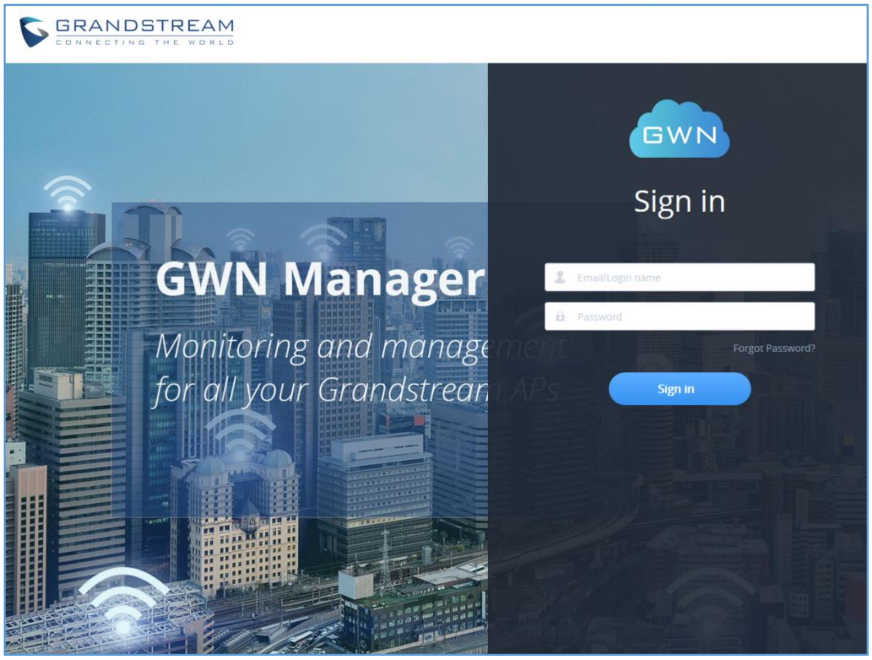
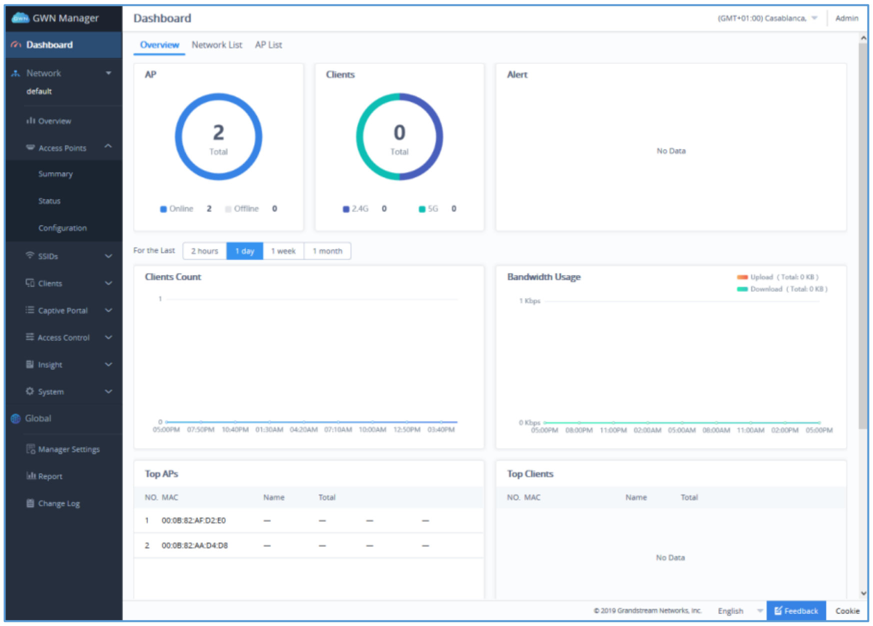


Figure 8: GWN Manager Login Page

The following page will be displayed:



Top APs

NO.	MAC	Name	Total		
1	00:0B:82:AF:D2:E0	—	—	—	—
2	00:0B:82:AA:D4:D8	—	—	—	—

Top Clients

NO.	MAC	Name	Total

No Data

Figure 9: GWN Manager Dashboard

GETTING STARTED WITH GWN MANAGEMENT PLATFORM

The GWN Management Platforms provide an easy and intuitive Web UI or mobile app (both Android & iOS versions) to manage and monitor GWN76xx Access Points, it provides users access to all GWN Access Points settings, without any additional on-premise infrastructure.

GWN76xx LED Patterns

The panel of the GWN76XX has different LED patterns for different activities, to help users read the status of the GWN76XX AP whether it's powered up correctly, provisioned, in upgrading process and more, for more details please refer to the below table.

Table 5: LED Patterns

LED Status	Indication
OFF	Unit is powered off or abnormal power supply.
Solid green	Unit is powered on.
Blinking green	Firmware update in progress.
Solid green	Firmware update successful.
Solid red	Firmware update failed.
Blinking red	Factory reset initiated
Solid purple	Unit not provisioned.
Blinking blue	Unit provisioning in progress.
Solid blue	Unit is provisioned successfully and running normally.
Blinking White	Used for Access Point location feature.

Note: To add GWN76XX AP to a GWN Management platform, either GWN.Cloud or GWN Manager, the status of the LED should be **Solid Purple** (AP not provisioned/uncontrolled).

Adding GWN76XX to GWN.Cloud

To add an Access point to GWN.Cloud, the administrator needs two information:

- MAC address of the Access Point.
- Wi-Fi Password in the back of the unit.

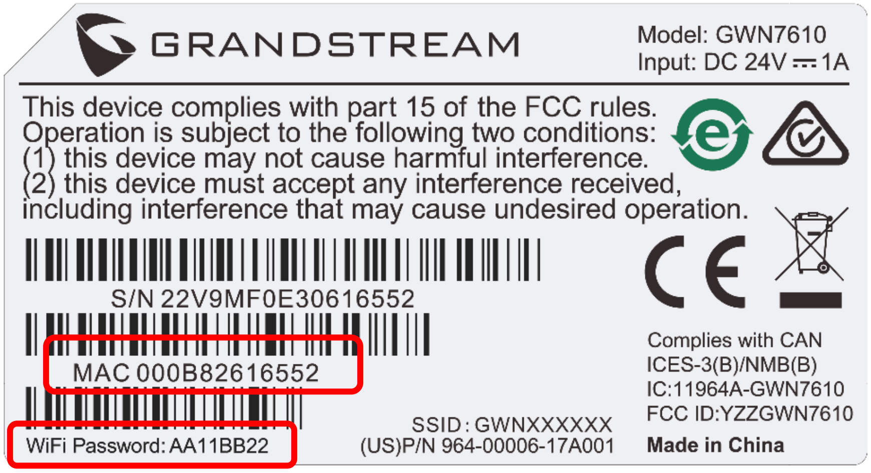
Note: Refer to [***REQUIREMENTS]*** section of this document to make sure your GWN76xx is using the proper firmware version. If not, please upgrade the units before adding them to GWN.Cloud.

There are 3 methods to add GWN76xx to the cloud:

- **Method 1: Adding New AP Manually**
- **Method 2: Adding New AP using GWN Application**
- **Method 3: Transfer APs control from Local Master**

Method 1: Adding New AP Manually

1. Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package.
2. Locate the Wi-Fi Password.



GRANDSTREAM

Model: GWN7610
Input: DC 24V ⎓ 1A

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

S/N 22V9MF0E30616552

MAC 000B82616552

WiFi Password: AA11BB22

SSID : GWNXXXXXX
(US)P/N 964-00006-17A001

Complies with CAN
ICES-3(B)/NMB(B)
IC:11964A-GWN7610
FCC ID:YZZGWN7610
Made in China

Figure 10: GWN Access Point MAC and Wi-Fi Password

3. Navigate to **Access Points → Configuration** → Click on **Add** button.

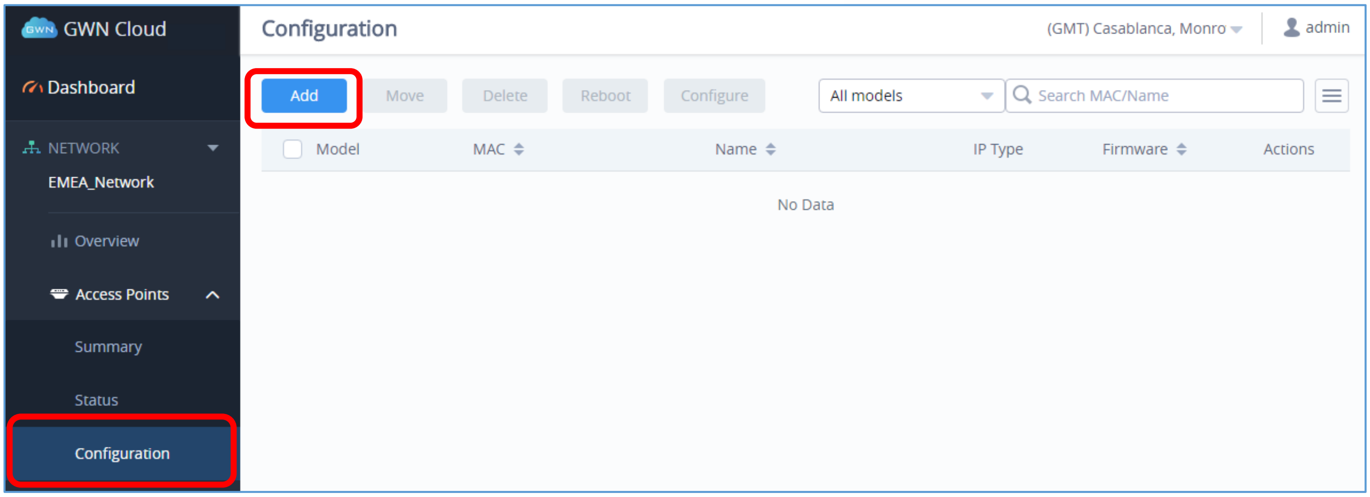
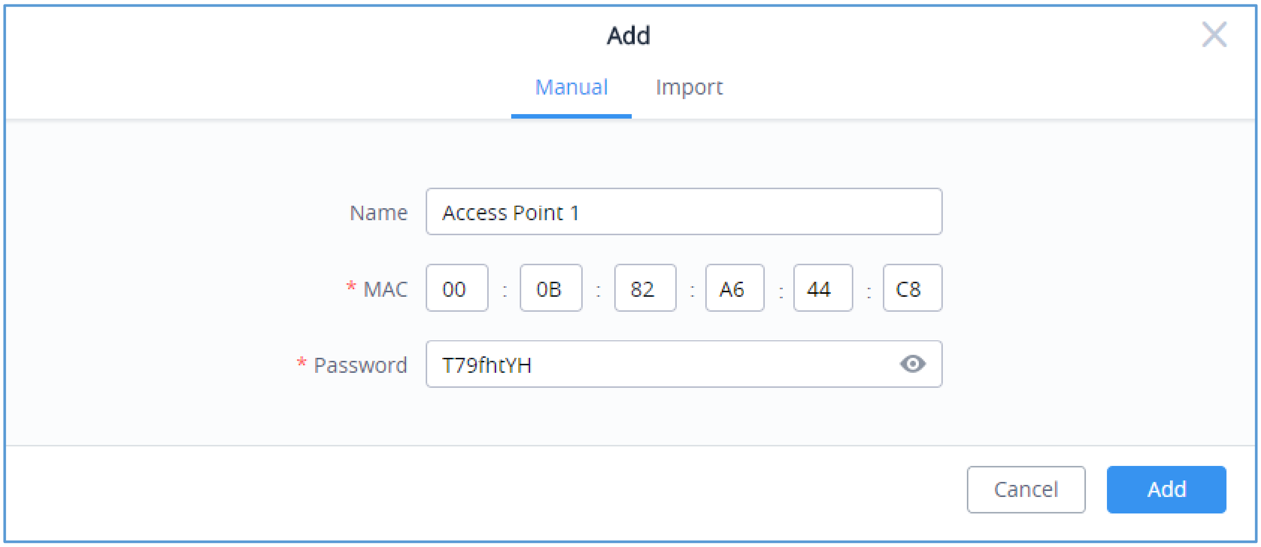


Figure 11: Adding New Access Point to GWN.Cloud

4. Enter the MAC address the Wi-Fi Password of the access point to be added.



Name: Access Point 1

* MAC: 00 : 0B : 82 : A6 : 44 : C8

* Password: T79fhtYH

Figure 12: Adding Access Points Manually

5. Click on **Add** and reset your Access Point. After reset, it will be added automatically to your Cloud account and you will be able to monitor/manage it.

Bulk-add AP using CSV file import

Another option for bulk-add access points is to use CSV file upload, to do that follow below steps:

1- After clicking on **Add** under the menu **Access Points → Configuration,** click on **Import** Tab**.**

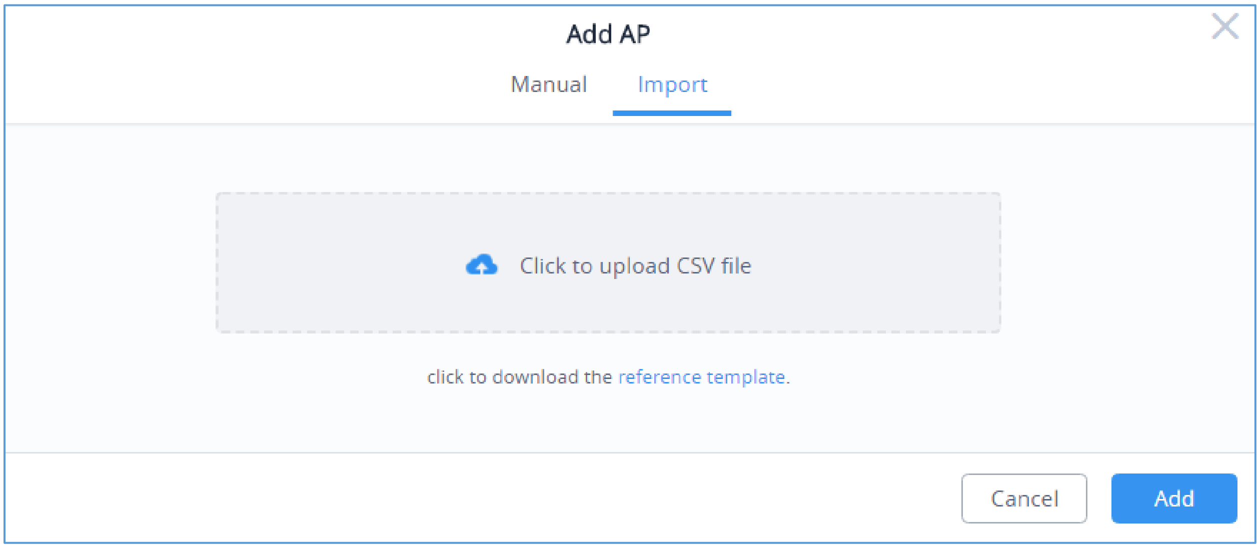


Figure 13: Import CSV file for APs

2- After this select “Click to upload CSV file” in order to import pre-configured CSV file with list of access points (MAC address and Wi-Fi password).

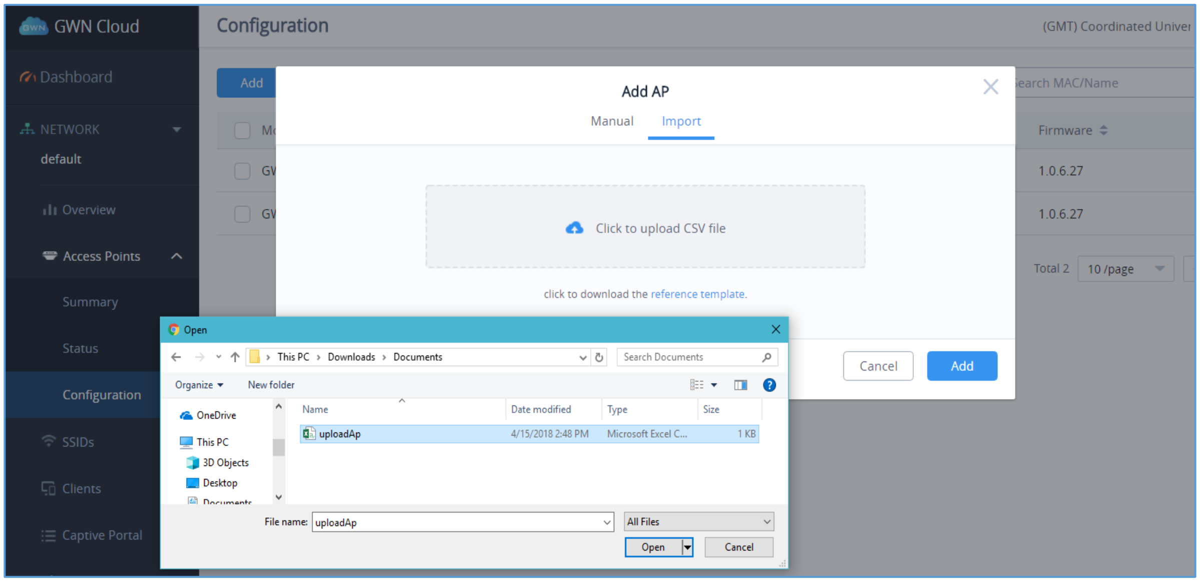


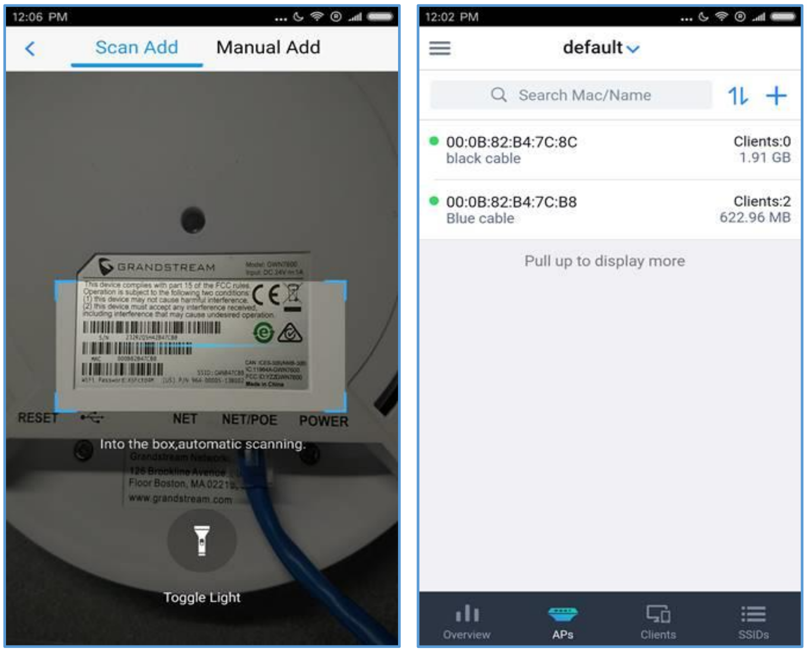
Figure 14: Upload CSV file

Method 2: Adding New AP using GWN.Cloud Application

An easy way to add new Access points to your GWN.Cloud is to use GWN.Cloud Application.

Note: GWN.Cloud Application is available on Google Play for Android^{TM} and App Store for iOS^{TM}.

The operation is done by scanning the barcode from GWN Access Point’s sticker.

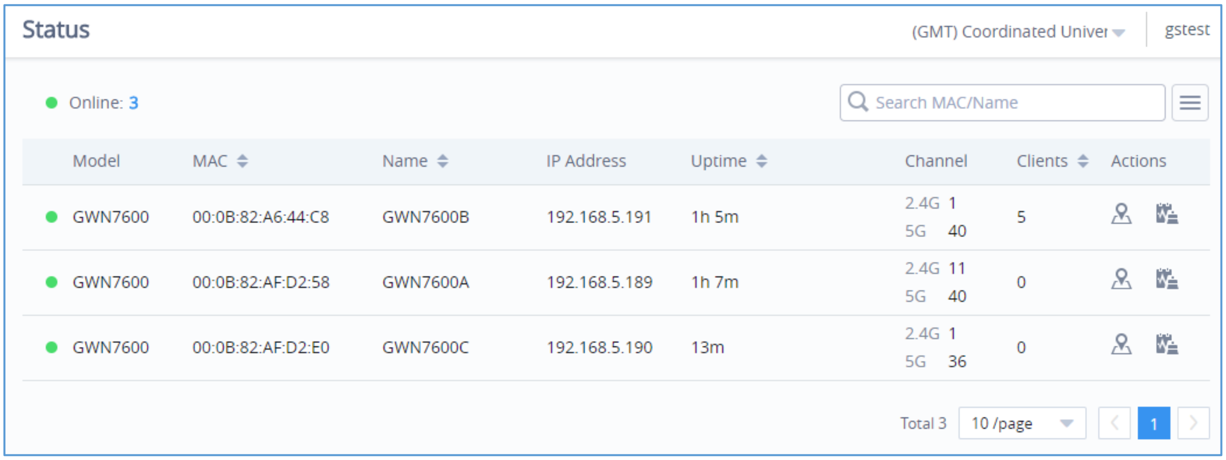


00:0B:82:B4:7C:8C Clients:0
black cable 1.91 GB

00:0B:82:B4:7C:B8 Clients:2
Blue cable 622.96 MB

Figure 15: Adding Access Point to GWN.Cloud using GWN App

Once added, the list of APs will be displayed on GWN.Cloud interface.



● Online: 3

	Model	MAC	Name	IP Address	Uptime	Channel	Clients	Actions
●	GWN7600	00:0B:82:A6:44:C8	GWN7600B	192.168.5.191	1h 5m	2.4G 1 5G 40	5	
●	GWN7600	00:0B:82:AF:D2:58	GWN7600A	192.168.5.189	1h 7m	2.4G 11 5G 40	0	
●	GWN7600	00:0B:82:AF:D2:E0	GWN7600C	192.168.5.190	13m	2.4G 1 5G 36	0	

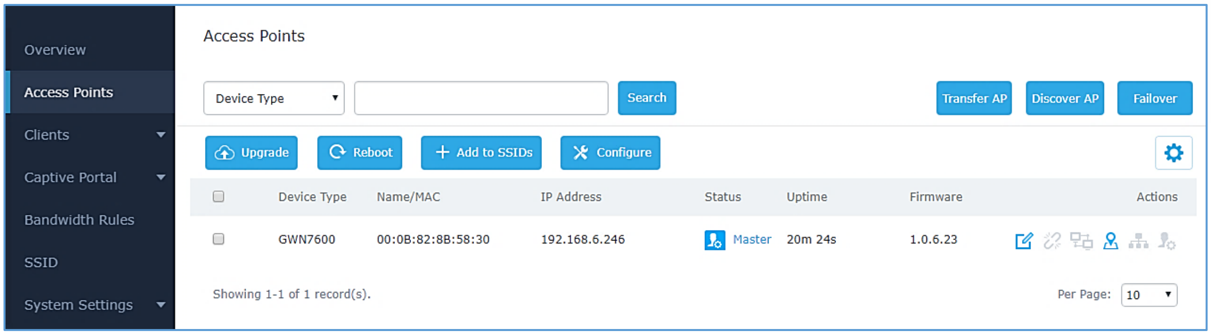
Total 3 10 /page 1

Figure 16: Access Points Status

Method 3: Transfer APs from Local Master

Another method to add GWN APs to the cloud is by transferring them to the cloud from the local Master AP. Follow these steps to achieve this:

1. Access the web UI of the Master AP and go to **Access Points**.

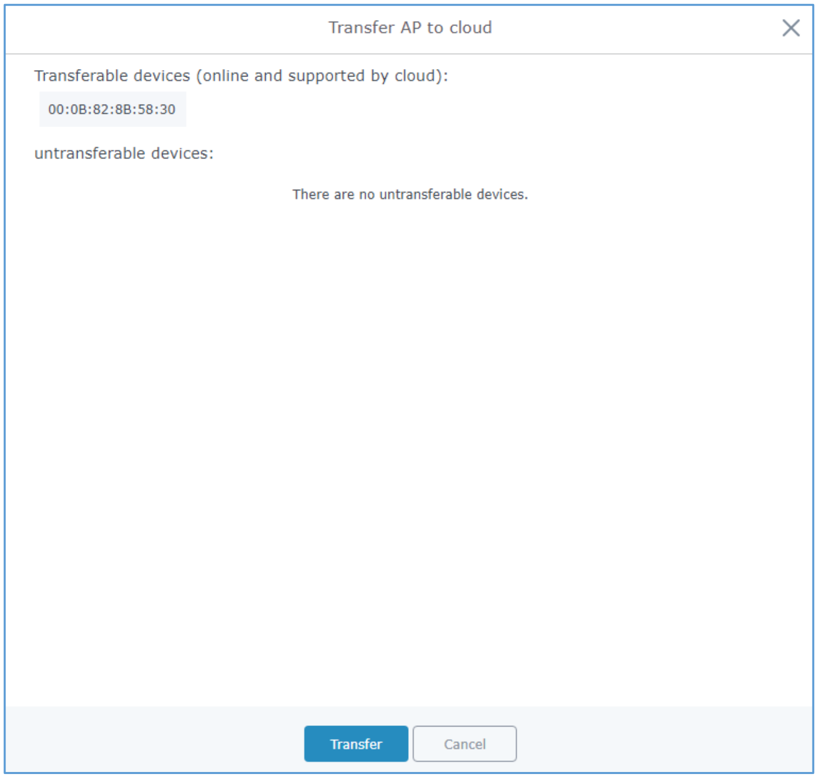


	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware
□	GWN7600	00:0B:82:8B:58:30	192.168.6.246	Master	20m 24s	1.0.6.23

Showing 1-1 of 1 record(s).

Figure 17: Master AP - Access Points

2. Press Transfer AP button. A new window will display “Transferable devices” list as shown below.



Transferable devices (online and supported by cloud):

00:0B:82:8B:58:30

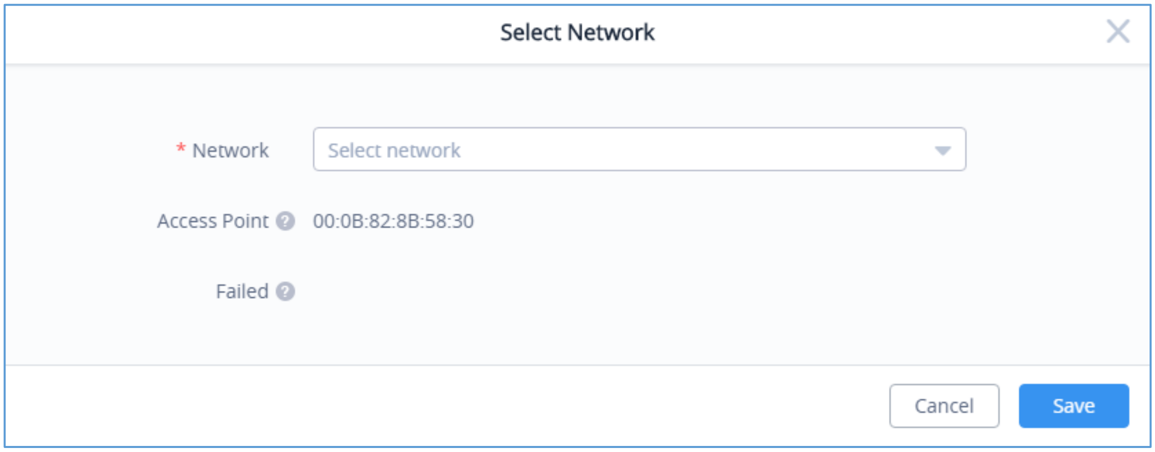
untransferable devices:

There are no untransferable devices.

Figure 18: Transfer AP to Cloud

3. Press Transfer button. The web browser will redirect to GWN.Cloud login page.

4. Once logged in to the cloud, the configuration page “Select Network” will be displayed:



Select Network

* Network: Select network

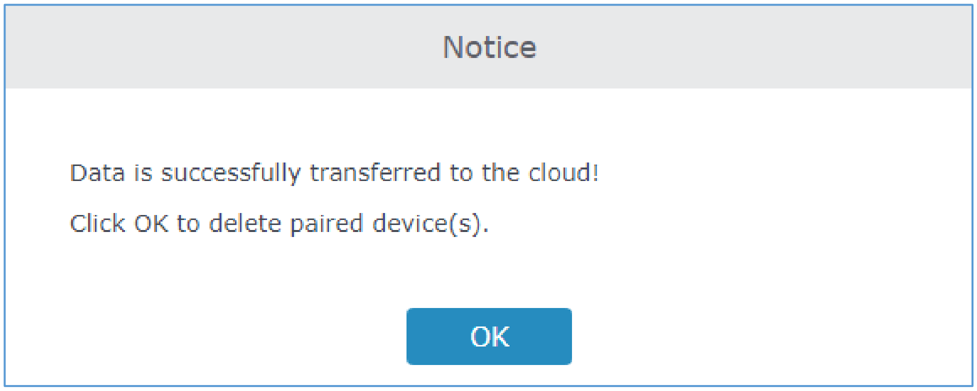
Access Point: 00:0B:82:8B:58:30

Failed

Figure 19: Select Network

- ***Access Point***: Shows the MAC address of the passed check device.
- ***Failed:*** Shows the MAC address of the authentication failed or added.

5. Select **Network** from the drop-down list to which the AP will be assigned.
6. Press **Save** button to confirm.
7. Once added to the cloud, Master AP web UI will display following successful notice.



Notice

Data is successfully transferred to the cloud!

Click OK to delete paired device(s).

Figure 20: Transfer AP to Cloud - Success

Adopt GWN76XX to GWN Manager

Note: Refer to [***REQUIREMENTS]*** section of this document to make sure your GWN76xx is using the proper firmware version. If not, please upgrade the units before adding them to GWN Manager.

1. Navigate to **Access Points → Configuration**
2. Click on **Adopt** button.

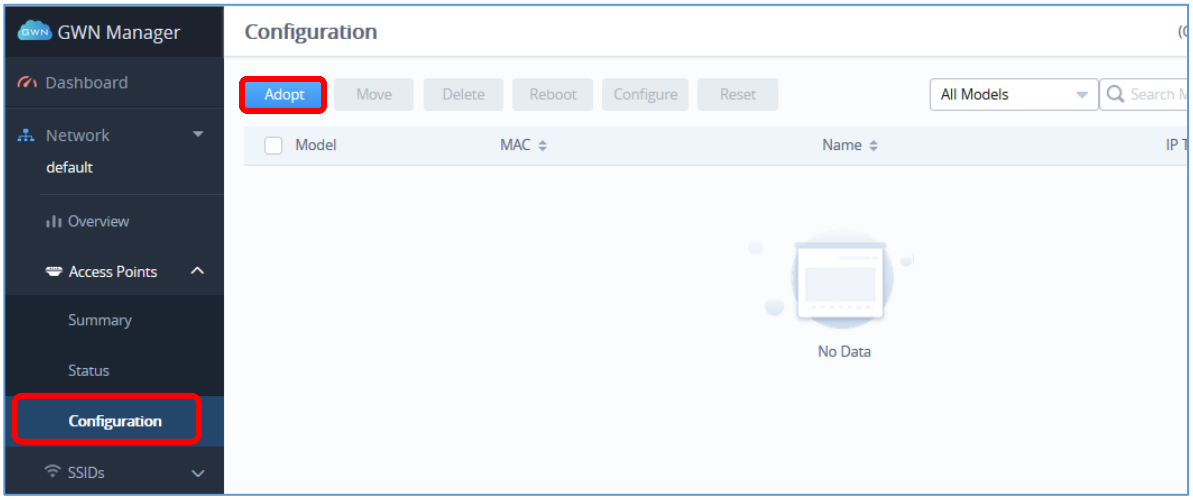
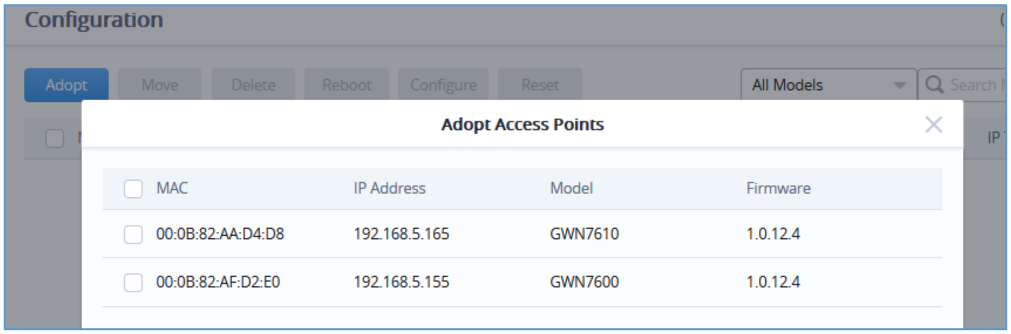


Figure 21: Adding New Access Point to GWN Manager

3. The GWN Manager will scan and detect the available APs on your Network

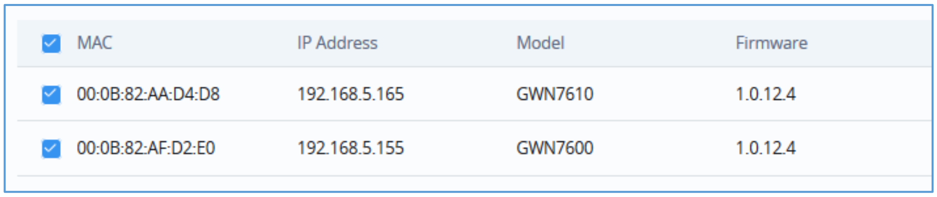


Adopt Access Points

□ MAC	IP Address	Model	Firmware
□ 00:0B:82:AA:D4:D8	192.168.5.165	GWN7610	1.0.12.4
□ 00:0B:82:AF:D2:E0	192.168.5.155	GWN7600	1.0.12.4

Figure 22: Auto detect Access Points

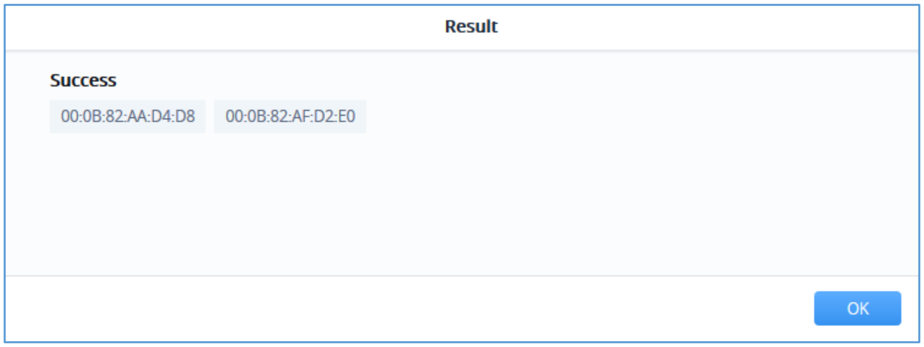
4. Select an AP by checking the box on its left. Or select all by checking the top box.



☑ MAC	IP Address	Model	Firmware
☑ 00:0B:82:AA:D4:D8	192.168.5.165	GWN7610	1.0.12.4
☑ 00:0B:82:AF:D2:E0	192.168.5.155	GWN7600	1.0.12.4

Figure 23: Select Access Points

5. A new window will pop up to confirm the success of the operation:
   Notice the MAC addresses of the new added units. Then, click **OK** to confirm.



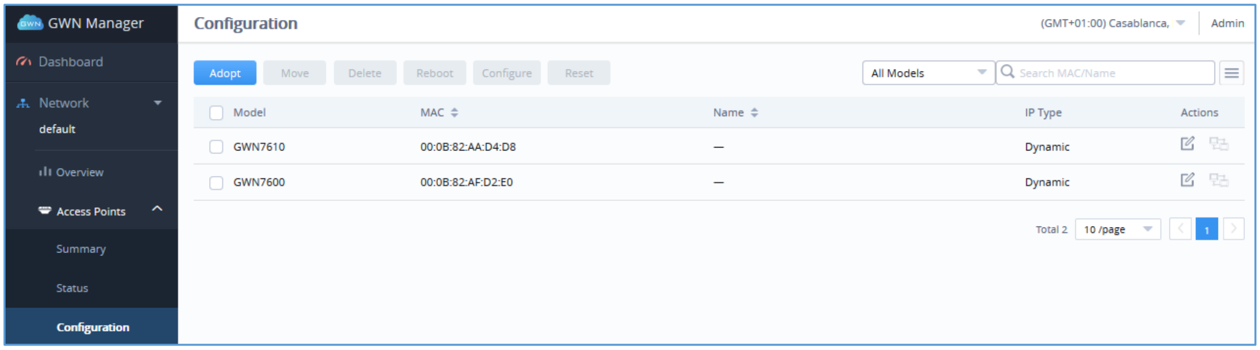
Result

Success

00:0B:82:AA:D4:D8 00:0B:82:AF:D2:E0

Figure 24: Confirm APs Adoption

6. The newly added APs should now be available under **Access Points → Configuration**



Model	MAC	Name	IP Type	Actions
GWN7610	00:0B:82:AA:D4:D8	—	Dynamic	
GWN7600	00:0B:82:AF:D2:E0	—	Dynamic	

Figure 25: Adopted Access Points

Discover GWN76XX

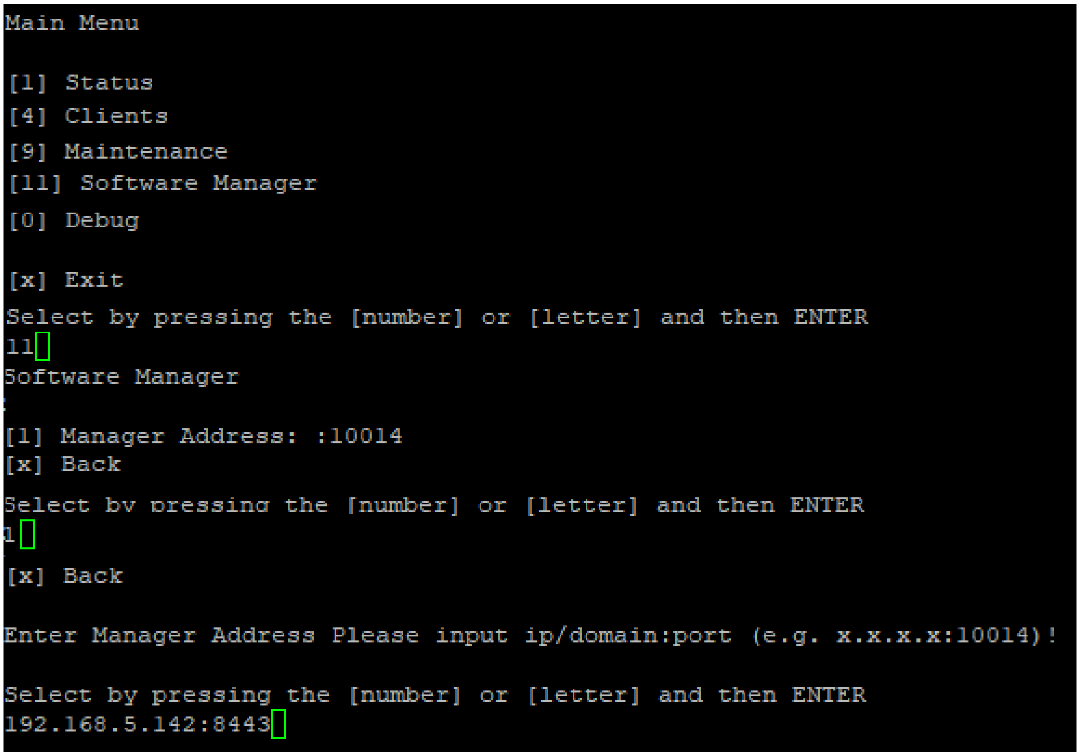
Method 1: Auto Discovery

- If GWN Manager connects to the same local subnet as GWN APs, it can discover the APs automatically via layer 2 broadcast.
- GWN APs accept DHCP option 224 encapsulated in option 43 to direct the controller. An example of DHCP option 43 configuration would be:

```
224(type)18(length)172.16.1.124:10014(value) translated into Hex as
e0123137322e31362e312e3132343a3130303134
```

Method 2: Manual discovery

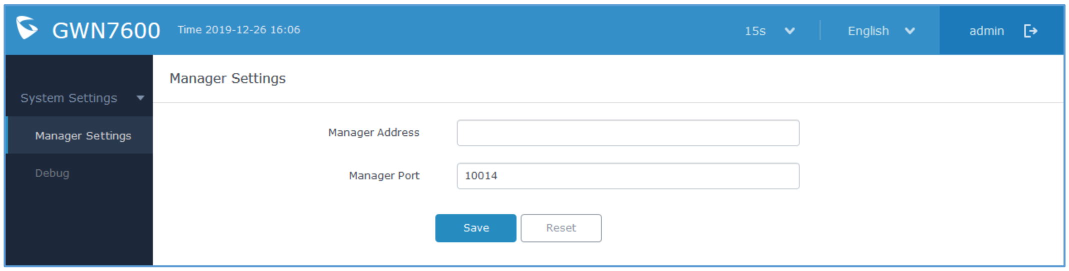
- You can SSH to slave AP and use GWN menu to set the Manager address and port (10014).



```
Main Menu

[1] Status
[4] Clients
[9] Maintenance
[11] Software Manager
[0] Debug

[x] Exit
Select by pressing the [number] or [letter] and then ENTER
11
Software Manager

[1] Manager Address: :10014
[x] Back
Select by pressing the [number] or [letter] and then ENTER
1
[x] Back

Enter Manager Address Please input ip/domain:port (e.g. x.x.x.x:10014)!

Select by pressing the [number] or [letter] and then ENTER
192.168.5.142:8443
```

Figure 26: Manager Settings – SSH

- You can log into WebUI of slave AP or an unpaired AP to set the Manager address and port.



Manager Settings

Manager Address

Manager Port 10014

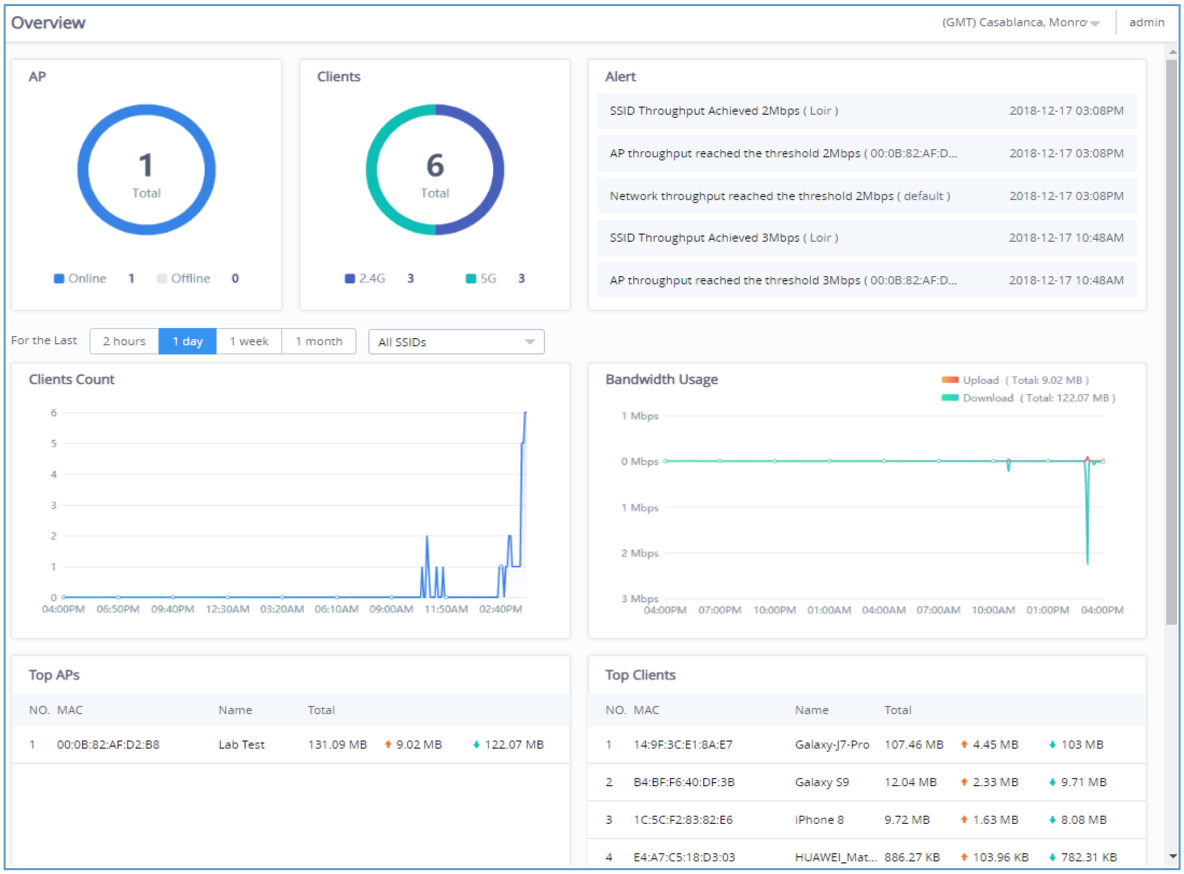
Figure 27: Manager Settings – Slave WebGUI

DASHBOARD

Overview

The Overview page provides general information that can be used to monitor both access points and clients connected to them, it's separated into seven sections:

- Access Points
- Clients
- Alerts
- Clients Count
- Bandwidth usage
- Top APs
- Top Clients
- Top SSIDs
- Tope Websites



Alert

SSID Throughput Achieved 2Mbps (Loir)	2018-12-17 03:08PM
AP throughput reached the threshold 2Mbps (00:0B:82:AF:D...	2018-12-17 03:08PM
Network throughput reached the threshold 2Mbps (default)	2018-12-17 03:08PM
SSID Throughput Achieved 3Mbps (Loir)	2018-12-17 10:48AM
AP throughput reached the threshold 3Mbps (00:0B:82:AF:D...	2018-12-17 10:48AM

Top APs

NO.	MAC	Name	Total		
1	00:0B:82:AF:D2:B8	Lab Test	131.09 MB	↑ 9.02 MB	↓ 122.07 MB

Top Clients

NO.	MAC	Name	Total		
1	14:9F:3C:E1:8A:E7	Galaxy-J7-Pro	107.46 MB	↑ 4.45 MB	↓ 103 MB
2	B4:BF:F6:40:DF:3B	Galaxy S9	12.04 MB	↑ 2.33 MB	↓ 9.71 MB
3	1C:5C:F2:83:82:E6	iPhone 8	9.72 MB	↑ 1.63 MB	↓ 8.08 MB
4	E4:A7:C5:18:D3:03	HUAWEI_Mat...	886.27 KB	↑ 103.96 KB	↓ 782.31 KB

Figure 28: GWN.Cloud Dashboard - Overview

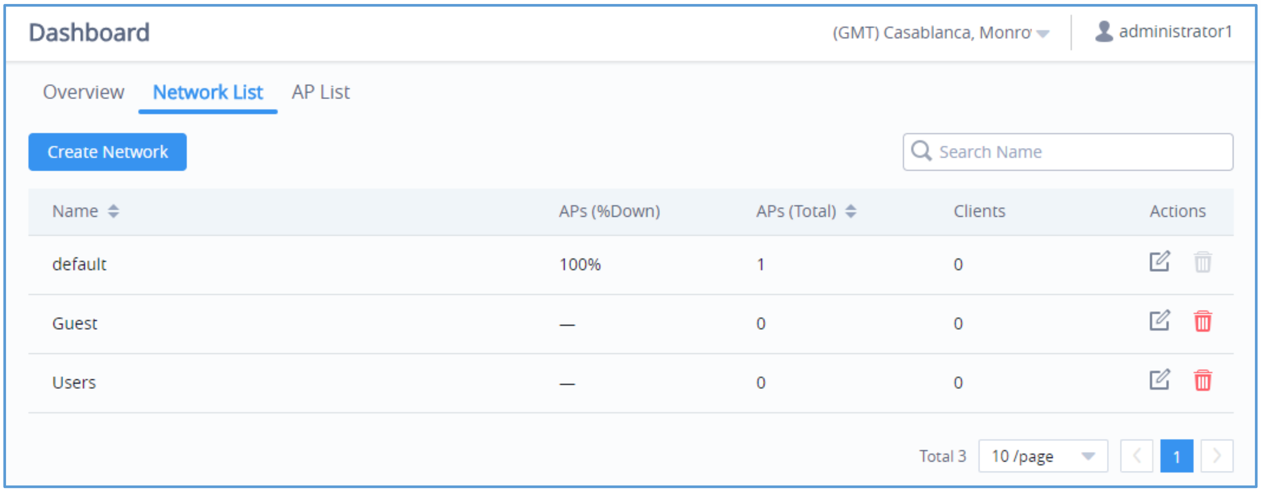
The following table describes each section:

Table 6: Dashboard Description

Section	Description
Access Points	Displays the number of Access points monitored as well as their status (Offline/Online)
Clients	Displays the total number of clients connected to the monitored APs, in addition to the band they are connected to 2.4G or 5G.
Alerts	This section shows alerts the administrator about any wrong behavior, based on the configured Alerts. (Refer to Alert section under Settings for more details)
Clients Count	It shows the number of clients connected at a specific period of time; the administrator can toggle between four different periods of time: • **2 hours:** Displays the connected clients graph for the two last hours. • **1 day:** Displays the connected clients graph for the last day. • **1 week:** Displays the connected clients graph for the last week. • **1 month:** Displays the connected clients graph for the last month.
Bandwidth usage	This section shows the bandwidth usage (Upload/Download) by all the clients, it provides the BW statistics for both Download and upload.
Top APs	Displays the top APs that consumed the max of the bandwidth/data
Top Clients	Lists the clients that downloaded/uploaded the max of data
Top SSIDs	Displays the SSIDs that are mostly used by clients.

Network List

The Network List page displays different Network Groups created on your account:



Dashboard

(GMT) Casablanca, Monro

administrator1

Overview | Network List | AP List

Create Network

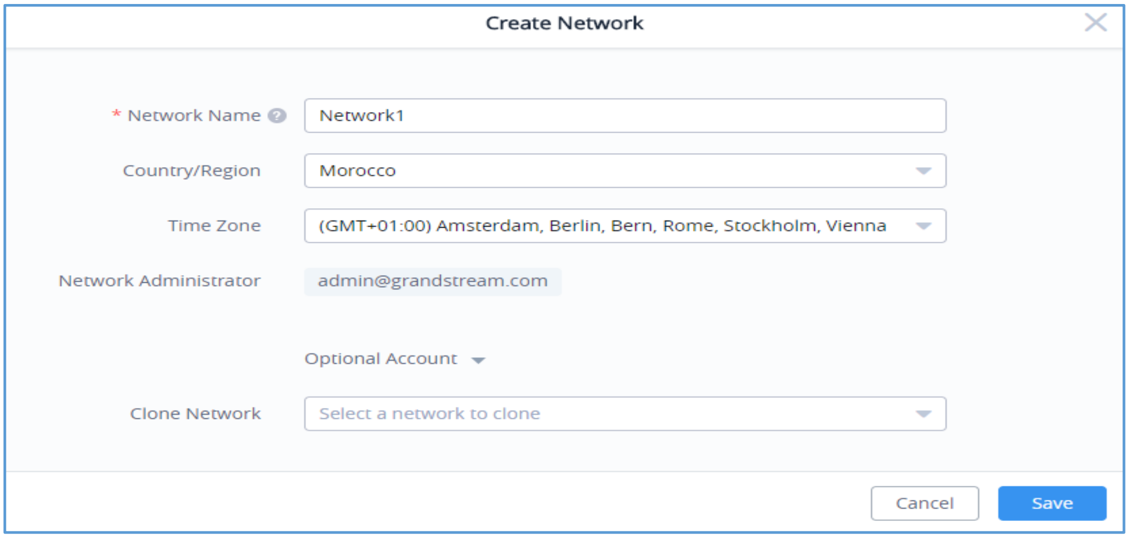
Search Name

Name	APs (%Down)	APs (Total)	Clients	Actions
default	100%	1	0	
Guest	—	0	0	
Users	—	0	0	

Total 3 | 10 /page | 1

Figure 29: GWN.Cloud Dashboard - Network List

- From Network list pages the administrator can monitor the number of Access points connected to each AP as well as the total APs, in addition to the number of clients on each network group.
- From this page New Network Groups can be also added by clicking on Create Network button. A new page will popup, fill in the fields as show in previous figure to create a new network.



Create Network

* Network Name	Network1
Country/Region	Morocco
Time Zone	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Network Administrator	admin@grandstream.com
	Optional Account
Clone Network	Select a network to clone

Cancel | Save

Figure 30: Create a New Network

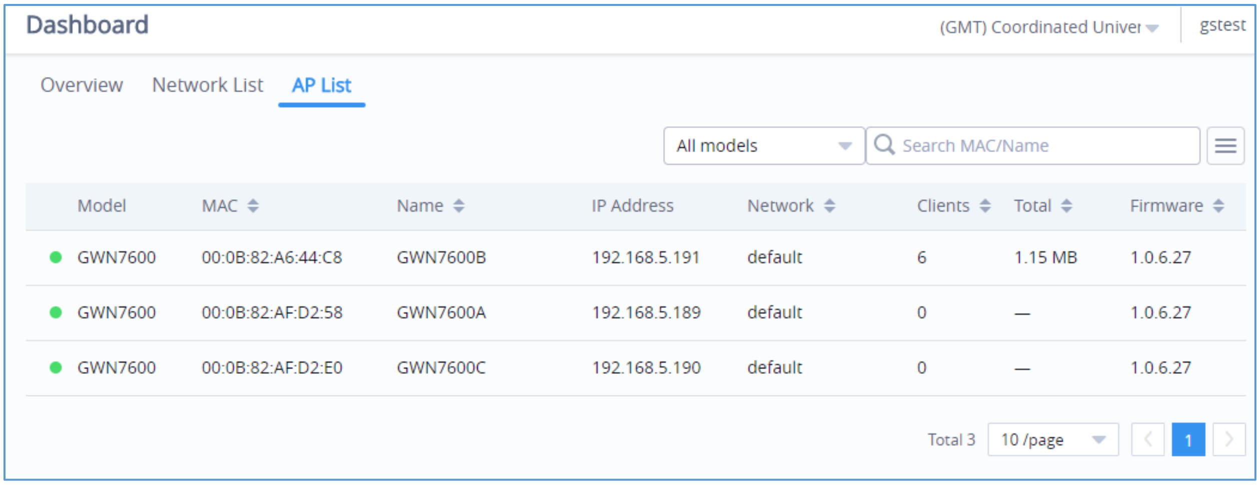
Table 7: Create a New Network Settings

Setting	Description
Network Name	Enter the network Name to identify different networks in your environment.
Country/Region	Select the country/Region, this is required to set the Wi-Fi specifications of your country on GWN AP.
Time Zone	Select your time zone.
Network Administrator	This field displays the list of administrators that can manage this network.
Clone Network	When you have an existing Network, you can choose to clone the new one with the already existing network.

- Administrator can search for specific Network by name using .

AP List

The AP List page displays the list of APs connected to your Account.



	Model	MAC	Name	IP Address	Network	Clients	Total	Firmware
●	GWN7600	00:0B:82:A6:44:C8	GWN7600B	192.168.5.191	default	6	1.15 MB	1.0.6.27
●	GWN7600	00:0B:82:AF:D2:58	GWN7600A	192.168.5.189	default	0	—	1.0.6.27
●	GWN7600	00:0B:82:AF:D2:E0	GWN7600C	192.168.5.190	default	0	—	1.0.6.27

Total 3 10 /page 1

Figure 31: GWN.Cloud Dashboard – AP List

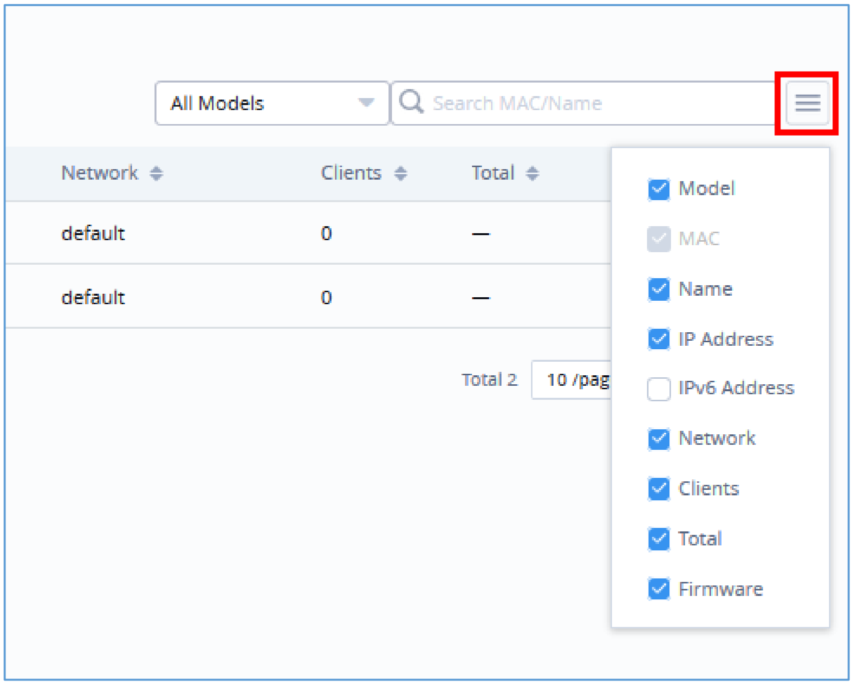
The AP List page provides also the following information regarding the Access point:

- Access Point Model.
- MAC address of the AP.

- Name of the AP.
- The IP address of the AP.
- The network Group to which the AP is assigned.
- The number of clients connected to the AP.
- Total Data consumed by the AP.
- Firmware.

Notes:

- The administrator can search access points from this list by Model, by name or also by MAC address.
- The list of information to display can be customized, by selecting which fields to display, as shown in the following figure:



All Models

Search MAC/Name

Network	Clients	Total
default	0	—
default	0	—

Total 2 10 /pag

☑ Model
☑ MAC
☑ Name
☑ IP Address
□ IPv6 Address
☑ Network
☑ Clients
☑ Total
☑ Firmware

Figure 32: Customize AP List Table Fields

NETWORK

The network page provides an information regarding all the network groups created under your account, once the administrator selects one network all the other configuration pages will change to reflect the information related to the selected network.

Create a New Network

1. Click on **Network** and a list of the networks will be displayed.

2. Click on + Create Network to add new network to your Platform Account.

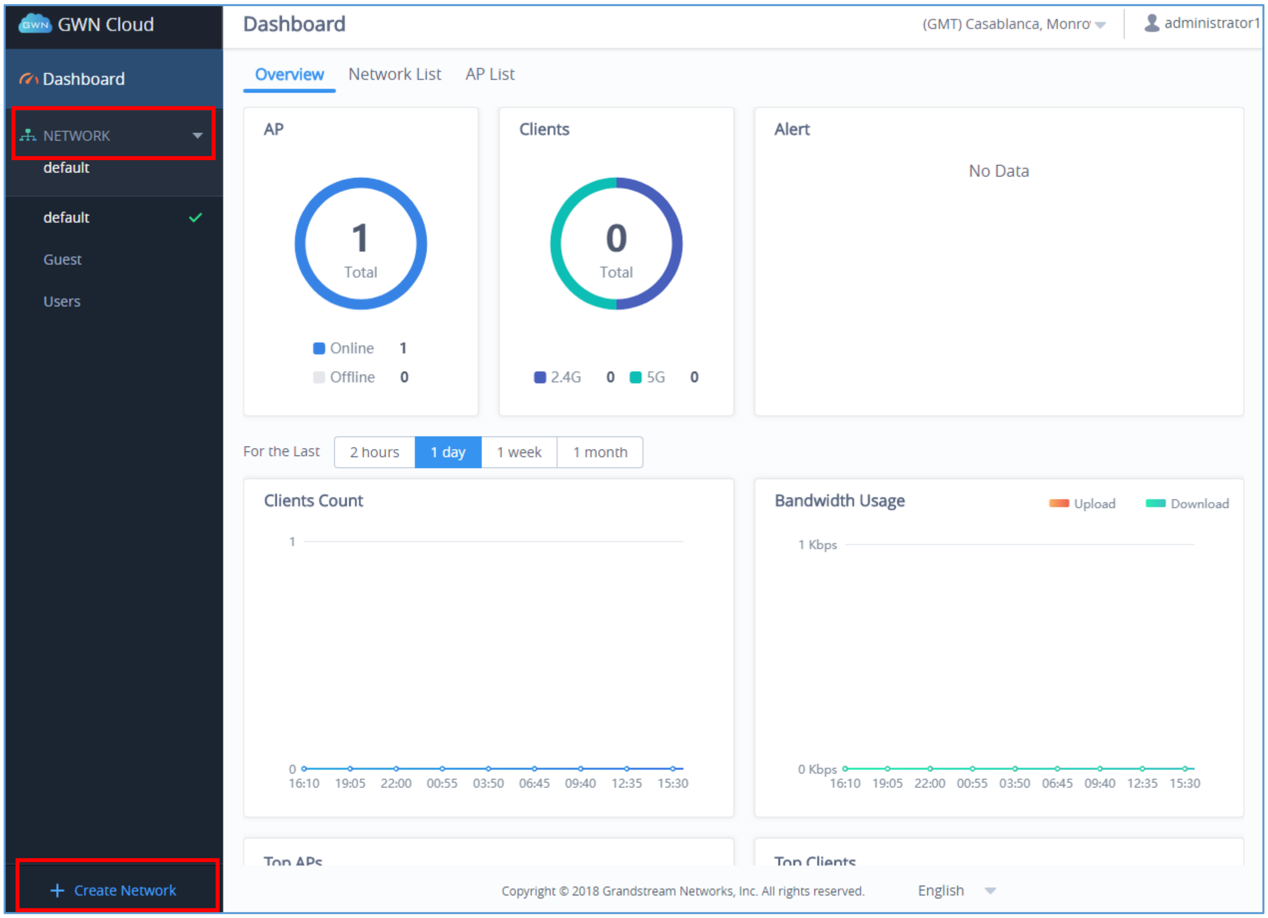
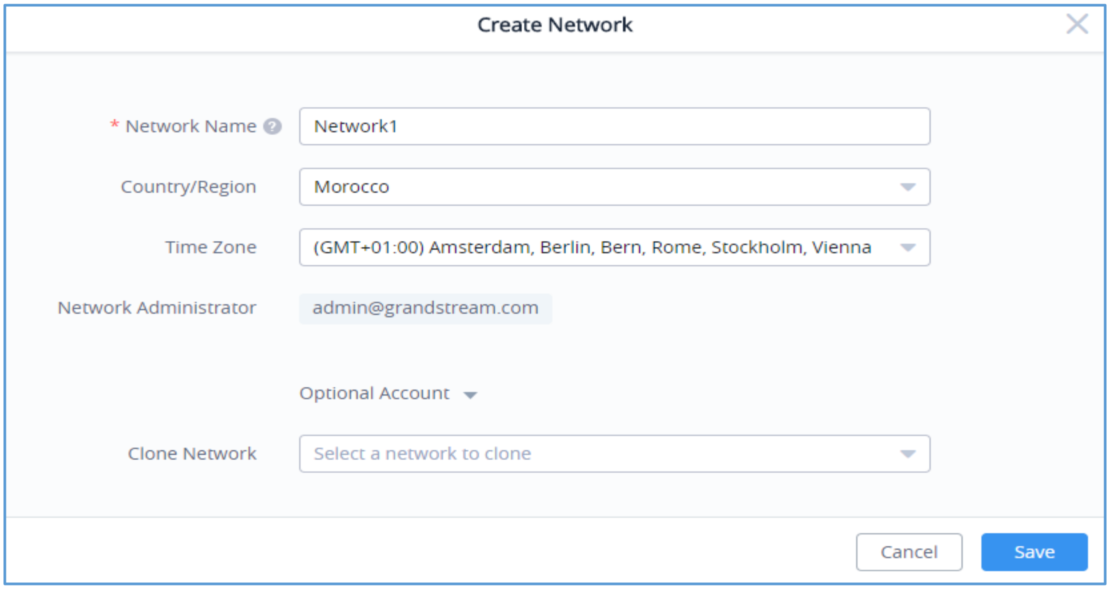


Figure 33: Network List and Network Creation Button

3. Fill the information as shown in the figure below.



Create Network

* Network Name: Network1

Country/Region: Morocco

Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Network Administrator: admin@grandstream.com

Figure 34: Create Network

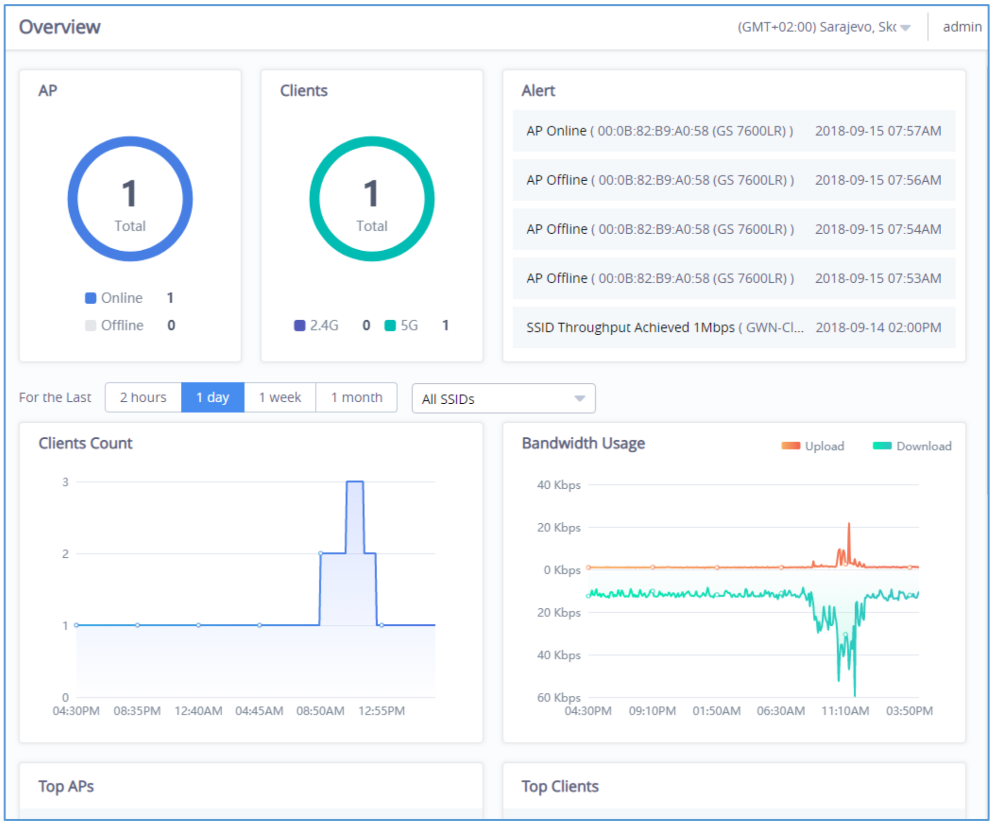
Table 8: Create a New Network Settings

Setting	Description
Network Name	Enter the network Name to identify different networks in your environment.
Country/Region	Select the country/Region, this is required to set the Wi-Fi specifications of your country on GWN AP.
Time Zone	Select your time zone.
Network Administrator	This field displays the list of administrators that can manage this network.
Clone network	When you have an existing Network, you can choose to clone the new one with the already existing network.

Overview Page

The overview page provides an overall view of the network selected. The administrator must select a network first and click on **Overview** in order to displays the network overview including:

- Access Points added to this network
- Clients connected to the network
- Different Alerts
- Clients Count
- Bandwidth usage
- Top APs
- Top Clients
- Top SSIDs
- Top Websites



Overview

(GMT+02:00) Sarajevo, Sk | admin

AP

1 Total

Online 1
Offline 0

Clients

1 Total

2.4G 0 5G 1

Alert

AP Online (00:0B:82:B9:A0:58 (GS 7600LR))	2018-09-15 07:57AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR))	2018-09-15 07:56AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR))	2018-09-15 07:54AM
AP Offline (00:0B:82:B9:A0:58 (GS 7600LR))	2018-09-15 07:53AM
SSID Throughput Achieved 1Mbps (GWN-Cl...	2018-09-14 02:00PM

For the Last: 2 hours | 1 day | 1 week | 1 month — All SSIDs

Clients Count

Bandwidth Usage

Top APs

Top Clients

Figure 35: Overview Page Displays Information related to Specific Network

Note: The overview page is related to specific network, while Dashboard is general overview page that shows information related to all the network monitored by the administrator.

ACCESS POINTS

From the access points page, the administrator can monitor different information regarding the access points of the selected network, this section is separated into 3 sub-sections:

1. Summary
2. Status
3. Configuration

Summary

The summary page displays information about the monitored access points, including Channel usage as well as the total access points and their status Online/Offline.

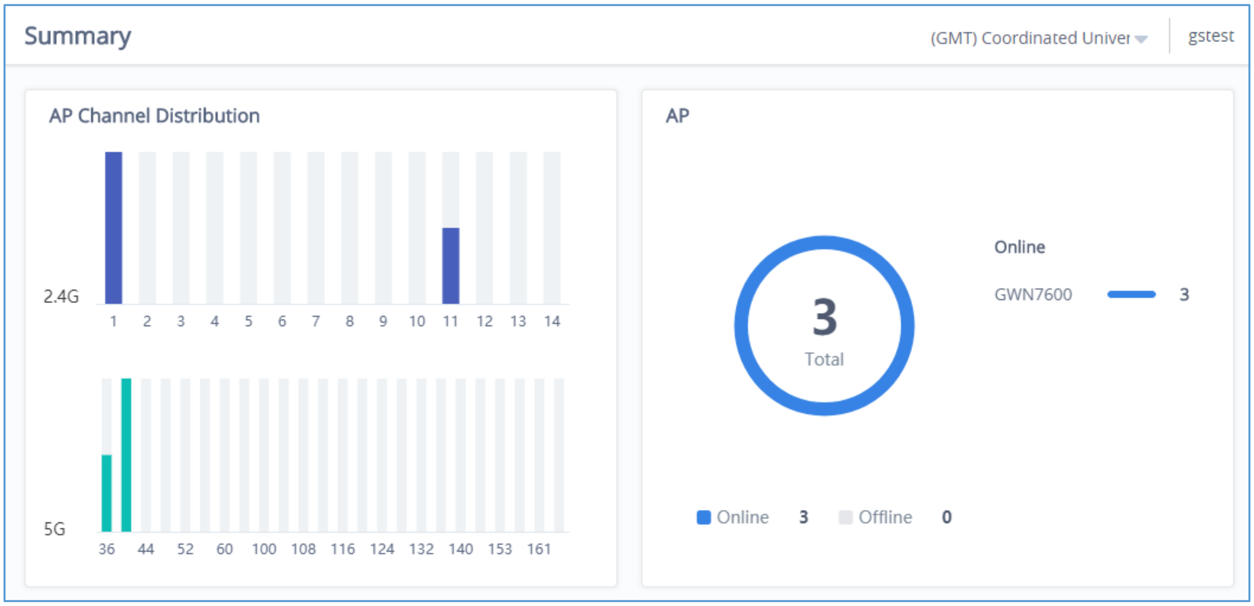
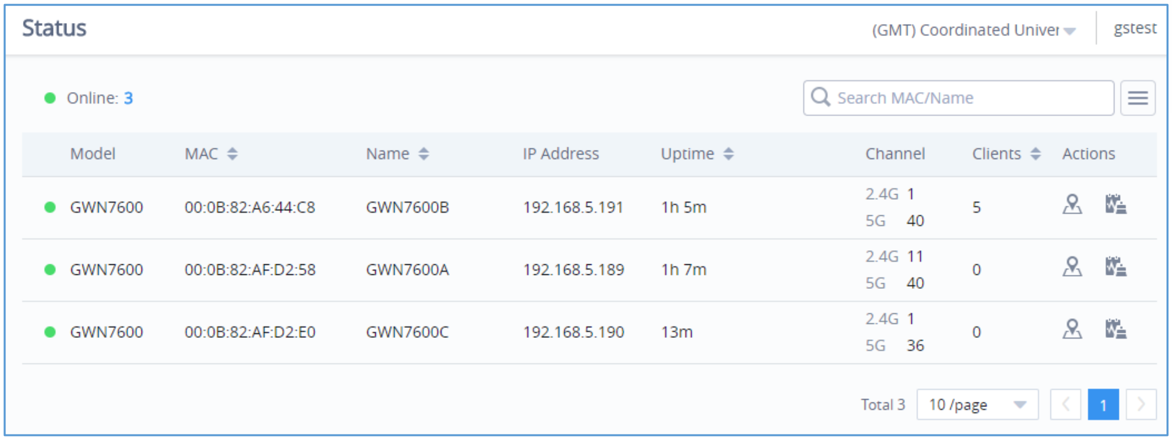


Figure 36: Access Points – Summary

Status

The Status page lists all the access points assigned to the selected network, along with the possibility to perform some basic operations such locating the device (LEDs start blinking in White) or clear the usage data, also users can check more detailed information about each access point and benefit from useful debugging tools which can help diagnose issue when they appear.



Status

(GMT) Coordinated Univer | gstest

Online: 3

Search MAC/Name

Model	MAC	Name	IP Address	Uptime	Channel	Clients	Actions
GWN7600	00:0B:82:A6:44:C8	GWN7600B	192.168.5.191	1h 5m	2.4G 1 5G 40	5	
GWN7600	00:0B:82:AF:D2:58	GWN7600A	192.168.5.189	1h 7m	2.4G 11 5G 40	0	
GWN7600	00:0B:82:AF:D2:E0	GWN7600C	192.168.5.190	13m	2.4G 1 5G 36	0	

Total 3 | 10 /page | 1

Figure 37: Access Points - Status

Table 9: Access Points Status Parameters

Model	GWN Access Point Model
MAC	MAC Address of the Access Point
Name	Access Point’s name
IP Address	IP Address of the Access point
Firmware	Firmware of the Access point
Uptime	Uptime of the Access point
Channel	Channels used by this Access points for both 2G and 5G.
Client	Number of clients connected to the Access Point
Actions	Locate Access point using button. Press to clear access point usage.

To get more detailed information about the status of a specific access point, users can click on the desired AP then a page similar to the following will show up:

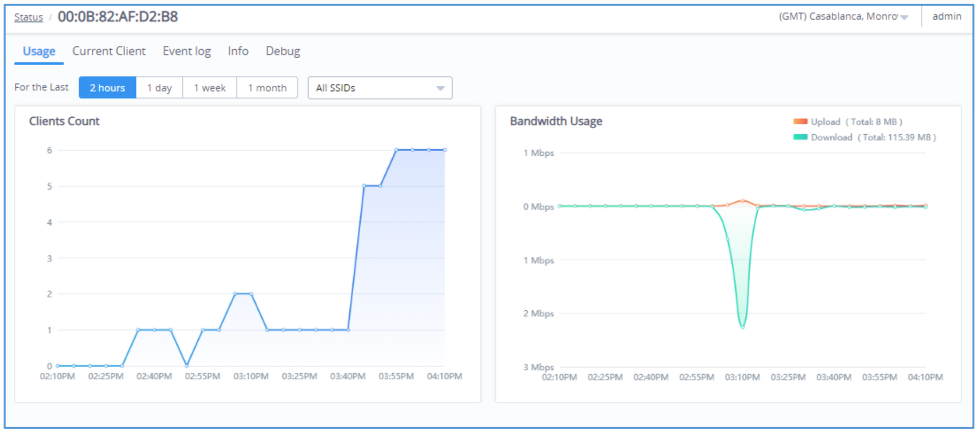
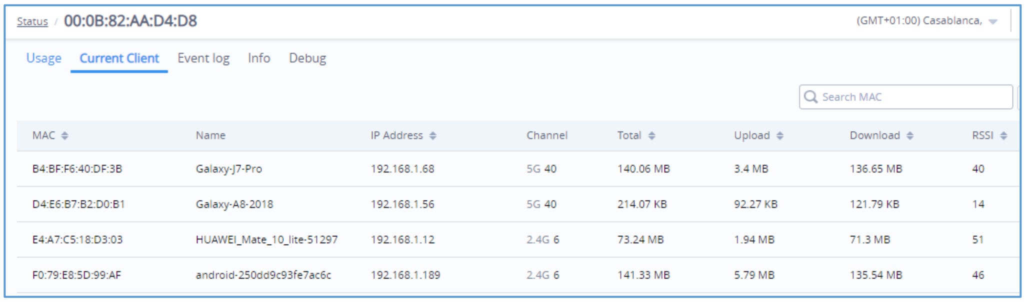


Figure 38: Usage of a Specific AP

The first tab will display the data usage for the specified access point and allows the user to filter the traffic graph for the last 2hours, 1day, 1week or 1 month. Also, the user has the ability to visualize the data usage (Upload/Download) for all SSIDs broadcasted by the AP or select a specific SSID from the drop-down list.

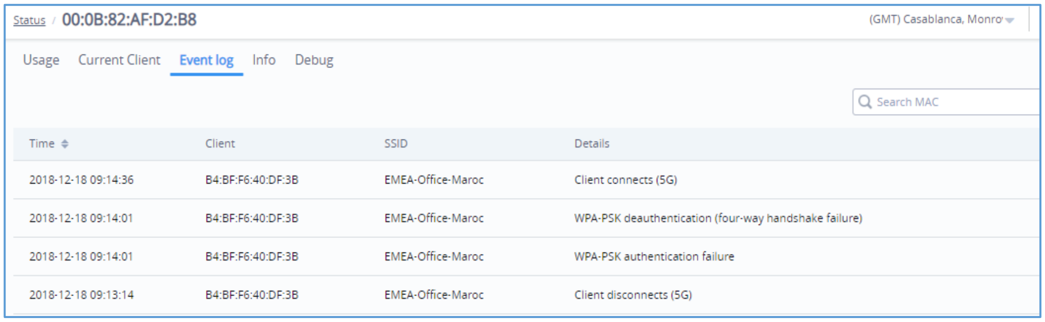
Click on Current clients to see the currently connected clients to the select AP as shown on the figure below.



MAC	Name	IP Address	Channel	Total	Upload	Download	RSSI
B4:BF:F6:40:DF:3B	Galaxy-J7-Pro	192.168.1.68	5G 40	140.06 MB	3.4 MB	136.65 MB	40
D4:E6:B7:B2:D0:B1	Galaxy-A8-2018	192.168.1.56	5G 40	214.07 KB	92.27 KB	121.79 KB	14
E4:A7:C5:18:D3:03	HUAWEI_Mate_10_lite-51297	192.168.1.12	2.4G 6	73.24 MB	1.94 MB	71.3 MB	51
F0:79:E8:5D:99:AF	android-250dd9c93fe7ac6c	192.168.1.189	2.4G 6	141.33 MB	5.79 MB	135.54 MB	46

Figure 39: Current Clients - Stats per AP

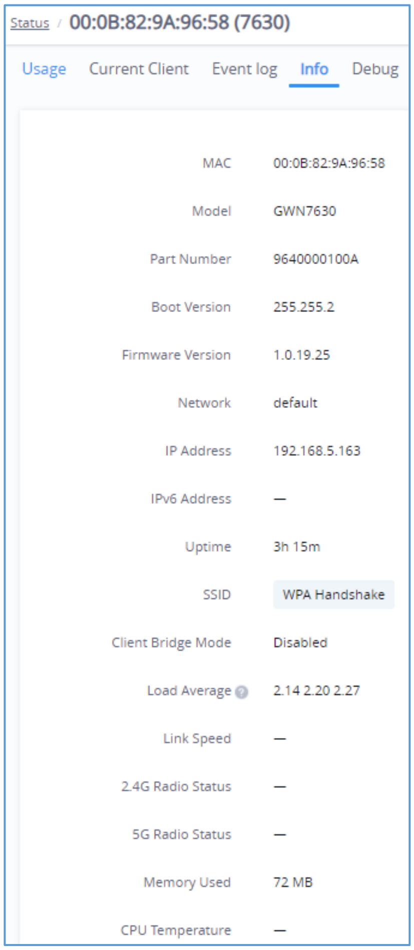
Click on Event log tab to see the log of all events that have occurred on the select access point, some events can help diagnosing Wi-Fi problems as shown on the figure below, the client has been disconnected due to four-way handshake failure, which is most likely because of wrong Wi-Fi password secret entered on client device.



Time	Client	SSID	Details
2018-12-18 09:14:36	B4:BF:F6:40:DF:3B	EMEA-Office-Maroc	Client connects (5G)
2018-12-18 09:14:01	B4:BF:F6:40:DF:3B	EMEA-Office-Maroc	WPA-PSK deauthentication (four-way handshake failure)
2018-12-18 09:14:01	B4:BF:F6:40:DF:3B	EMEA-Office-Maroc	WPA-PSK authentication failure
2018-12-18 09:13:14	B4:BF:F6:40:DF:3B	EMEA-Office-Maroc	Client disconnects (5G)

Figure 40: Event Log per AP

The next tab “Info” shows detailed information about the select AP, such as the model, name, firmware version, memory used and which SSID is being broadcasted by this AP and more.



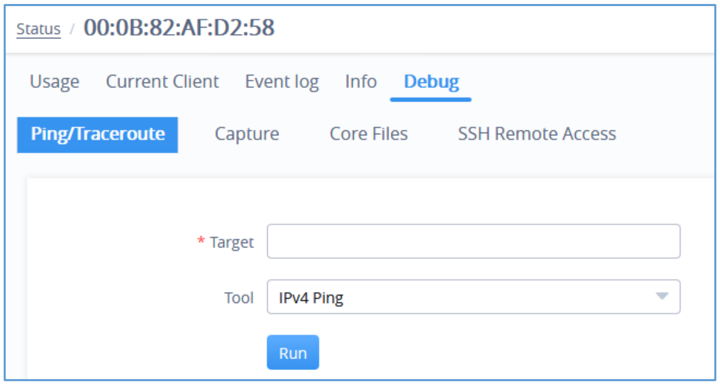
Status / 00:0B:82:9A:96:58 (7630)

MAC	00:0B:82:9A:96:58
Model	GWN7630
Part Number	9640000100A
Boot Version	255.255.2
Firmware Version	1.0.19.25
Network	default
IP Address	192.168.5.163
IPv6 Address	—
Uptime	3h 15m
SSID	WPA Handshake
Client Bridge Mode	Disabled
Load Average	2.14 2.20 2.27
Link Speed	—
2.4G Radio Status	—
5G Radio Status	—
Memory Used	72 MB
CPU Temperature	—

Figure 41: AP Info

The last Tab is used by administrator for debugging purposes and provides the following tools:

- **Ping/Traceroute** tools, such as the **ping** utility, **traceroute** utility and **nslookup** tool.
- **Capture,** to capture traffic for different network groups and filter by IP, TCP of UDP traffic. Mostly this will be used by engineering team for debugging purposes.
- **Core Files,** when a crash event happens on the unit, it will automatically generate a coredump file that can used by engineering team for debugging purposes.
- **SSH Remote Access:** This feature enables SSH access from GWN.cloud to your AP device, and this is mainly for extra troubleshooting method. Remote SSH will be automatically deactivated after 48 hours.



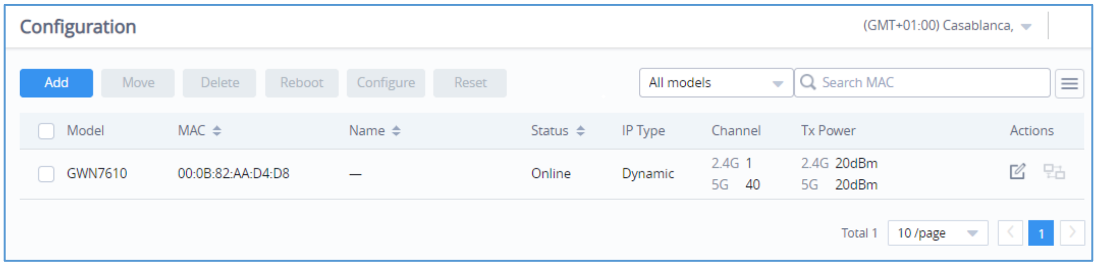
* Target

Tool: IPv4 Ping

Figure 42: Debug Tool Tab

Configuration

The configuration page allows the administrator to add, move, delete, reboot, configure or reset access points.



Model	MAC	Name	Status	IP Type	Channel	Tx Power	Actions
GWN7610	00:0B:82:AA:D4:D8	—	Online	Dynamic	2.4G 1 5G 40	2.4G 20dBm 5G 20dBm	

Total 1 10 /page 1

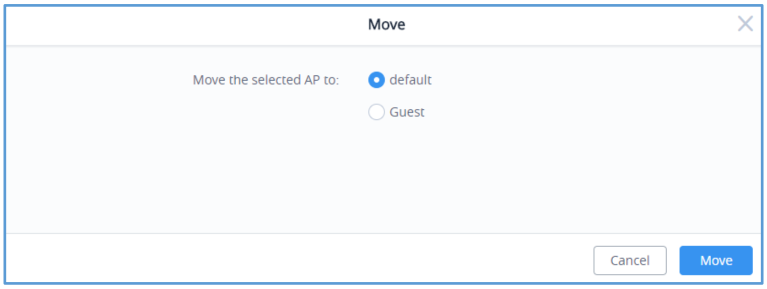
Figure 43: Access Points Configuration Page

Add New Access Points

- There are two methods to add new access points, either manually or using GWN Cloud App. Please refer to *[Adding GWN76XX to GWN.Cloud]* section in this manual.
- Please refer to [*Adopt GWN76XX to GWN Manager]* section in this manual.

Move Access Points

The administrator can move GWN Access points from one network to another. Click on Move button and the following window will popup, select the network where to move the access point and click on move.



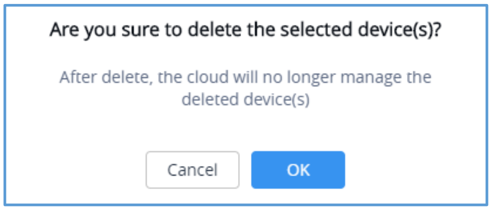
Move

Move the selected AP to: ● default ○ Guest

Figure 44: Moving Access Points between Networks

Delete Access Points

To delete an access point, select it, then click on reboot button, the following confirmation message will be displayed:



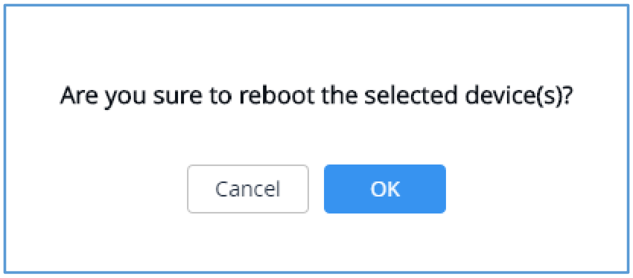
Are you sure to delete the selected device(s)?

After delete, the cloud will no longer manage the deleted device(s)

Figure 45: Delete Access Point

Reboot Access Points

To reboot an Access point, select it then click on Reboot button, the below confirmation message will be displayed:

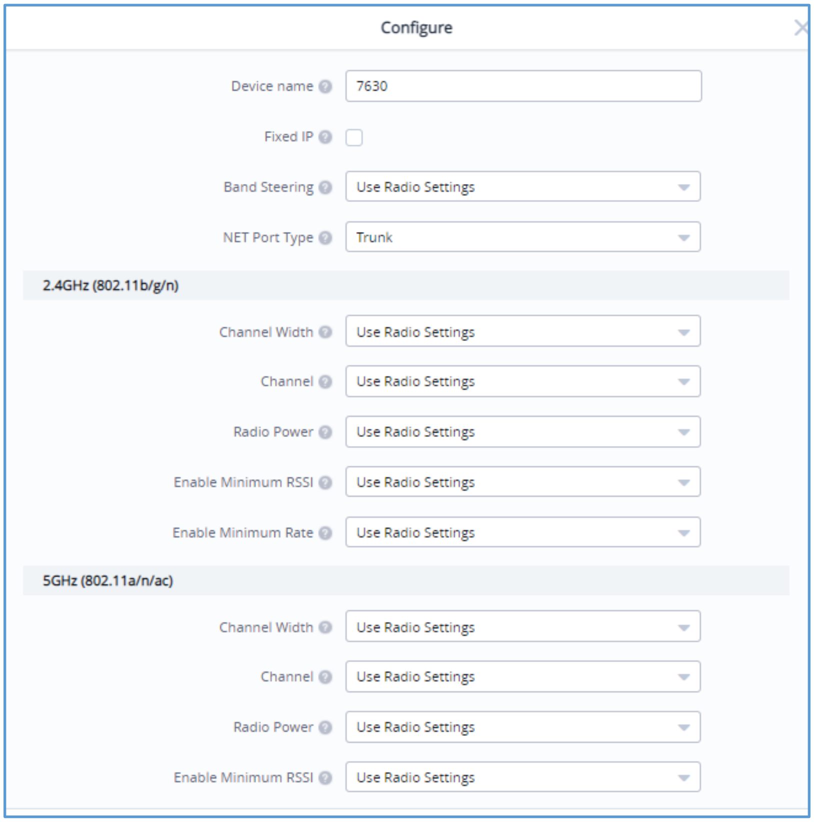


Are you sure to reboot the selected device(s)?

Figure 46: Reboot Access Point

Configure Access Points

To configure an access point, select and click on Configure button. A new config page will popup:



Configure

Device name	7630
Fixed IP	□
Band Steering	Use Radio Settings
NET Port Type	Trunk
2.4GHz (802.11b/g/n)	
Channel Width	Use Radio Settings
Channel	Use Radio Settings
Radio Power	Use Radio Settings
Enable Minimum RSSI	Use Radio Settings
Enable Minimum Rate	Use Radio Settings
5GHz (802.11a/n/ac)	
Channel Width	Use Radio Settings
Channel	Use Radio Settings
Radio Power	Use Radio Settings
Enable Minimum RSSI	Use Radio Settings

Figure 47: Access Point Configuration Page

The following settings can be configured from this page:

Table 10: Access Point Configuration Settings

Device Name	Set GWN76xx's name to identify it along with its MAC address.
Fixed IP	Check this option to configure the device with a static IP configuration; it must be in the same subnet with the default Network Group; Once enabled, these fields will show up: IPv4 Address/IPv4 Subnet Mask/IPv4 Gateway/Preferred IPv4 DNS/Alternate IPv4 DNS.
Band Steering	Band Steering will help redirecting clients to a radio band 2.4G or 5G, depend on what's supported by the device, for efficient use and to benefit from the maximum throughput. Four options are allowed by GWN.Cloud: • **Disable Band steering**: This will disable the band steering feature and the access point will accept the band chosen by the client.

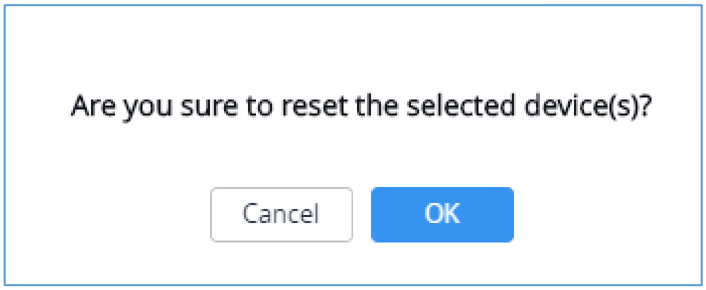
	• **2G in Priority:** 2G Band will be prioritized over 5G Band • **5G in Priority:** 5G Band will be prioritized over 2G Band • **Balance:** GWN will balance between the clients connected to 2G and those connected to 5G.
Net Port Type	You can configure Trunk port or Access port. When it's set to *Access*, you also need to specify the VLAN ID. For example, if you have multiple SSIDs on different VLANs, then the port need to be set to Trunk in order to negotiate trunk with the switch port where the AP is plugged. Otherwise if there is only one SSID/VLAN the port type is set to Access. *This feature is not supported in GWN7600/7600LR/GWN7610.*
Radio Power	Set the Radio Power depending on desired cell size to be broadcasted, four options are available: "Low", "Medium", "High" and "custom" Default is "High".
Custom 2.4GHz/5GHz Tx Power (dBm)	Allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.
Enable Minimum RSSI	Configures whether to enable/disable Minimum RSSI function. This option can be either Disabled, or Enabled and set manually or set to Use Radio Settings.
Minimum Access Rate Limit	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP. This option can be either Disabled, or Enabled and set manually or set to Use Radio Settings.

Notes:

- The administrator can filter access points by Model or search by name/MAC of the device.
- Click on Save Button to save the changes and apply them to the AP.

Reset Access Points

To reset an access point, select and click on Reset button, a confirmation message will be displayed, click on OK to confirm the operation.



Are you sure to reset the selected device(s)?

Figure 48: Reset Access Point

SSID

SSIDs page is used to monitor and manage network SSIDs, it's divided into two different sections:

- Summary
- Configuration

Summary

The summary page displays statistics about different SSIDs, including the number of clients connected to them as well as the bandwidth usage per period of time.

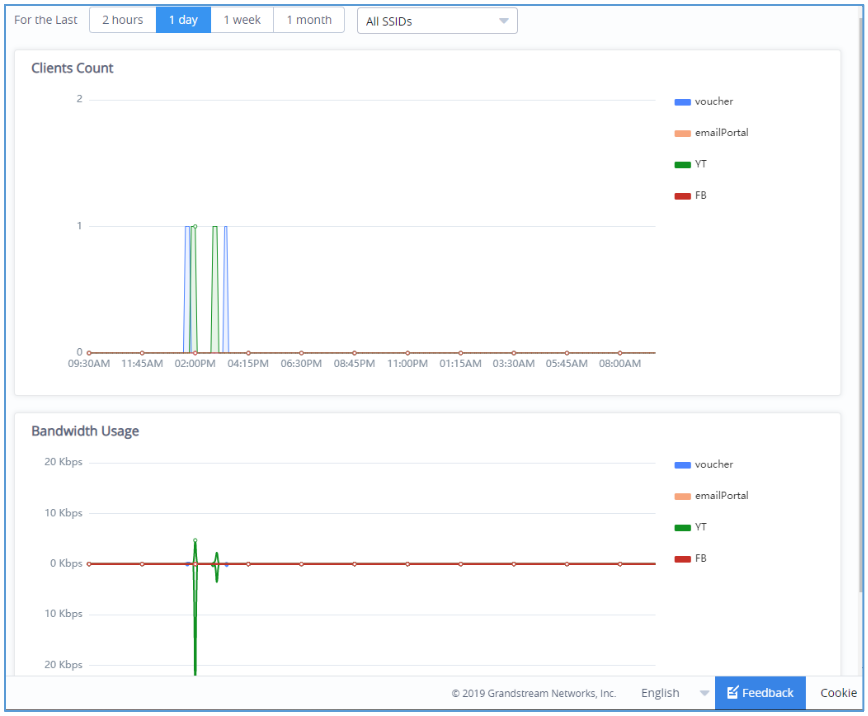
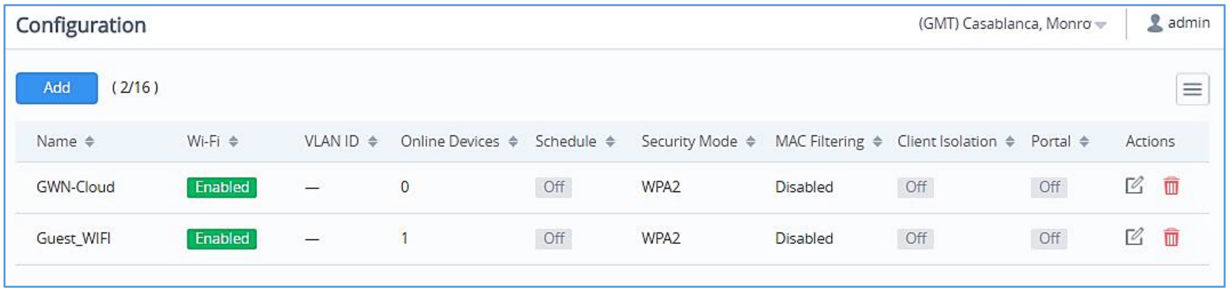


Figure 49: SSIDs - Summary

Configuration

From the Configuration page, users can create new SSIDs or configure an existing SSID.



Configuration

(GMT) Casablanca, Monro admin

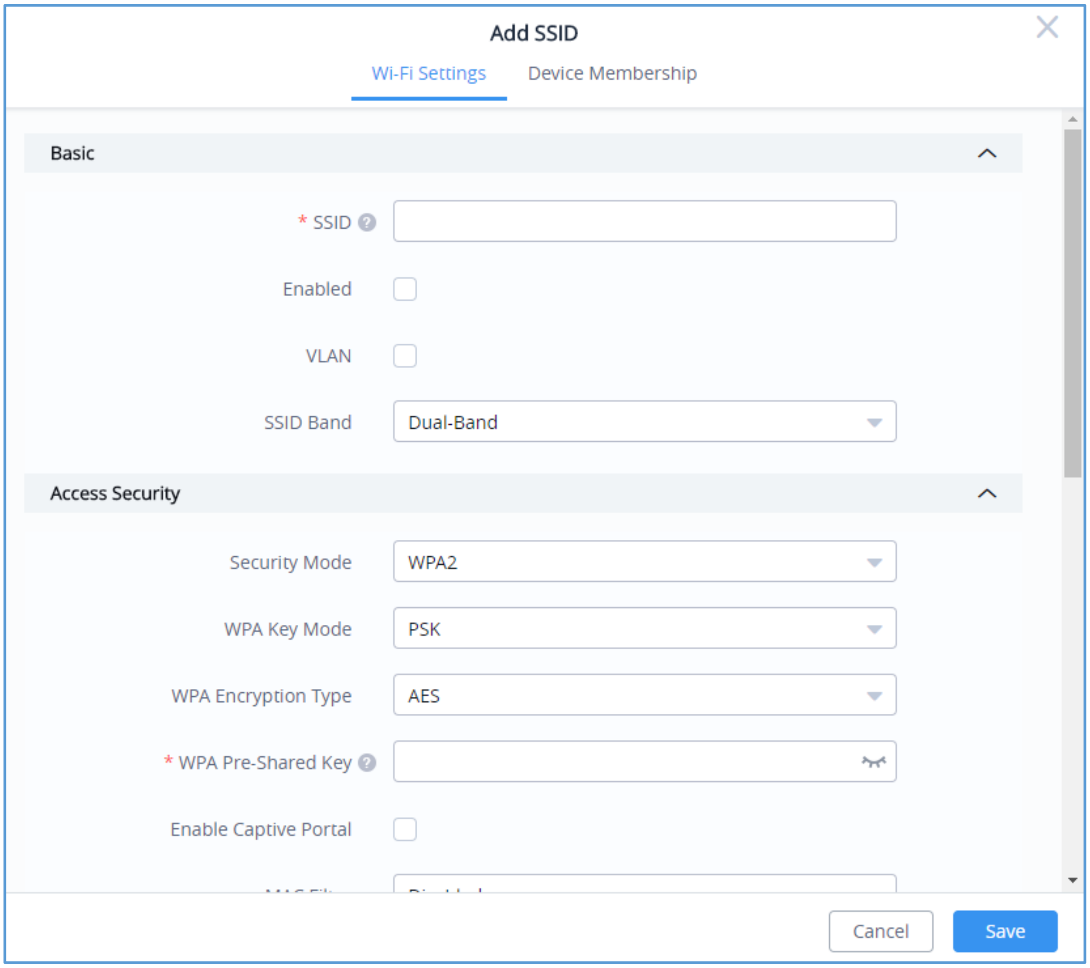
Add (2/16)

Name	Wi-Fi	VLAN ID	Online Devices	Schedule	Security Mode	MAC Filtering	Client Isolation	Portal	Actions
GWN-Cloud	Enabled	—	0	Off	WPA2	Disabled	Off	Off	
Guest_WIFI	Enabled	—	1	Off	WPA2	Disabled	Off	Off	

Figure 50: SSIDs - Configuration

Wi-Fi Settings

To add new SSID, navigate to **SSIDs → Configuration → Add**. A new page will popup, enter different settings to add new SSID.



Add SSID

Wi-Fi Settings | Device Membership

Basic

* SSID	
Enabled	□
VLAN	□
SSID Band	Dual-Band

Access Security

Security Mode	WPA2
WPA Key Mode	PSK
WPA Encryption Type	AES
* WPA Pre-Shared Key	
Enable Captive Portal	□

Figure 51: SSIDs – Configuration – Wi-Fi Settings

Table 11: SSID Wi-Fi Settings

Field	Description
SSID	Set or modify the SSID name.
Enabled	Check to enable Wi-Fi for the SSID
VLAN	Check to Enable VLAN and enter VLAN ID, otherwise, this SSID will be using the default network group.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: **Dual-Band**, **2.4GHz** or **5GHz**
Security Mode	Set the security mode for encryption, 8 options are available: • **WEP 64-bit:** Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5. • **WEP 128-bit:** Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13. • **WPA/WPA2:** Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. • **WPA2:** Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. Recommended configuration for authentication. • **WPA2/WPA3:** Using "802.1x" as WPA Key Mode, with "GCMP-256" or "GCMP-128" Encryption Type. • **WPA3-192:** Using "SAE-PSK" or "802.1x" as WPA Key Mode, with "GCMP-256" or "CCMP-256" Encryption Type. • **Open:** No password is required. Users will be connected without authentication. Not recommended for security reasons. **Note:** GWN products support for 802.1x (PEAP-MSCHAPv2 and EAP-TLS) requires external AAA server to permit authentication and centralized access management.

WEP Key	Enter the password key for WEP protection mode. This option is available when selecting **WEP64-bit/WEP128-bit** as **Security Mode**
WPA Key Mode	Select key mode (Pre-Shared Key or 802.1X Authentication).
WPA Encryption Type	Select Encryption type (AES or AES/TKIP).
WPA Pre-Shared Key	Configures the WPA pre-shared key. The input range: 8-63 ASCII characters or 8-64 hex characters. This option is available when selecting **PSK** as **WPA Key Mode.**
RADIUS Sever Address	Configures RADIUS authentication server address. This option is available when selecting **802.1x** as **WPA Key Mode.**
RADIUS Server Port	Configures RADIUS Server Listening port (defaults to 1812). This option is available when selecting **802.1x** as **WPA Key Mode.**
RADIUS Server Secret	Enter the secret password for client authentication with RADIUS server. This option is available when selecting **802.1x** as **WPA Key Mode.**
Secondary RADIUS Server	Enable the configuration of secondary RADIUS authentication server address
RADIUS Accounting Server Address	Configures the address for the RADIUS accounting server. This option is available when selecting **802.1x** as **WPA Key Mode.**
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port (Default is 1813). This option is available when selecting **802.1x** as **WPA Key Mode.**
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server. This option is available when selecting **802.1x** as **WPA Key Mode.**
RADIUS NAS ID	Configures the Radius NAS ID used to notify the source of RADIUS access request so that, the RADIUS server can choose policy for that request. This option is available when selecting **802.1x** as **WPA Key Mode.**
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.

Captive Portal Policy	Select the captive portal policy already created on the "***CAPTIVE PORTAL***" web page to be used in the created SSID.
MAC Filter	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to Wi-Fi. Default is Disabled.
Enable Dynamic VLAN	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile. This option is available when selecting **802.1x** as **WPA Key Mode.** **Note:** When using 802.1X authentication on your SSID with dynamic VLAN assignment. Admin does not need to create all VLAN SSIDs to match destination VLAN. On 1.0.11.1, AP will trunk its Ethernet with the VLAN assigned to Wi-Fi client through 802.1X
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76xx's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Available modes are: • **Radio Mode:** Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76xx but they cannot communicate with each other. • **Internet Mode:** Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76xx. • **Gateway MAC Mode:** Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76xx access points.
Gateway MAC Address	This field is required when using **Client Isolation,** so users will not lose access to the Network (usually Internet). Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":". **Example:** 00:0B:82:8B:4D:D8

802.11w	Management Frame Protection 802.11w applies to a set of management frames, these include Disassociation, Deauthentication, and Robust Action frames. 3 modes are available: - **Disabled**：Disable 802.11w; - **Optional:** Either 802.11w supported or unsupported clients can access the network; - **Required:** Only the clients that support 802.11w can access the network.
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
Beacon Interval	Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp… - **Using High Beacon Interval:** AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save WiFi clients energy consumption. - **Using Low Beacon Interval:** AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by WiFi clients with weak signal. **Notes:** 1. When AP enables several SSIDs with different interval values, the max value will take effect. 2. When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. 3. When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. 4. When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500.

	5. Mesh feature will take up a share when it is enabled. Default value is 100ms. Valid range: 40 – 500 ms.
DTIM Period	Configures the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Default value is 1, meaning that AP will have DTIM broadcast every beacon. If set to 10, AP will have DTIM broadcast every 10 beacons. Valid range: 1 – 10.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. 0 means limit is disabled.
Client Inactivity Timeout	AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.
Client Bridge	Configures the client bridge support to allows the access point to be configured as a client for bridging wired only clients wirelessly to the network. When an access point is configured in this way, it will share the Wi-Fi connection to the LAN ports transparently. Once a Network Group has a Client Bridge Support enabled, the AP adopted in this Network Group can be turned into Bridge Client mode by click the Bridge button.
Client Time Policy	Configures the client time policy. Default is None.
Convert IP multicast to unicast	Once selected, AP will convert multicast streams into unicast streams over the wireless link. Which helps to enhance the quality and reliability of video/audio stream and preserve the bandwidth available to the non-video/audio clients.
Schedule	Select a schedule that will be applied to this SSID, schedules can be managed from the menu "**System → Schedule**".
Enable Minimum RSSI	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in **Minimum RSSI (dBm).**
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected.

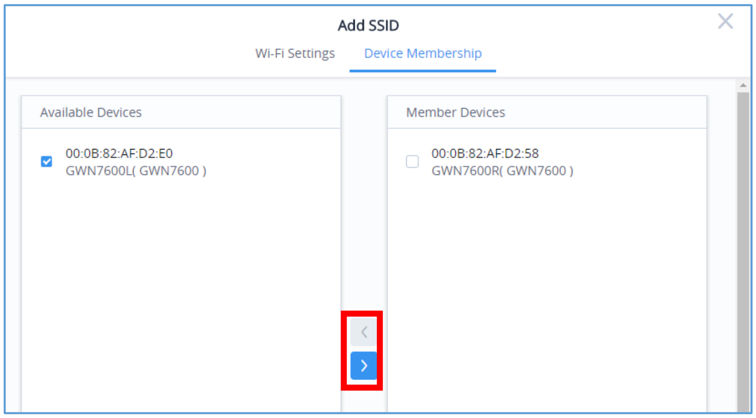
	The input range is from "-94" or "-1".
Enable Minimum Rate	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP.
Minimum Rate (Mbps)	Specify the minimum access rate. Once the client access rate is less than the specified value, AP will kick it off. Available values are: 1Mbps, 2Mbps, 5Mbps, 6Mbps, 9Mbps, 11Mbps or 12Mbps.
Enable Voice Enterprise	Enable this feature to help clients connected to the GWN76xx to perform better roaming decision. • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. **Notes:** 1. 11R is required for enterprise audio feature, 11V and 11K are optional. 2. Enable Voice Enterprise is only available under **"WPA/WPA2"** and **"WPA2"** Security Mode.
Enable 11R	Check to enable 802.11r
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
ARP Proxy	Once enabled, AP will avoid transferring the ARP messages to Stations, while initiatively answer the ARP requests in the LAN.

Device Membership

After adding new SSID the administrator needs to select the GWN76XX access points to be assigned to it.

To add a GWN76xx to a SSID, follow below steps:

1. Check the access points to add from "Available Devices" list.

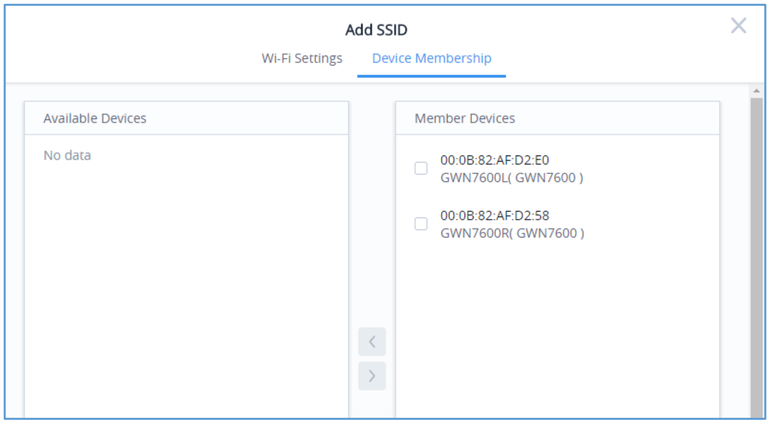


☑ 00:0B:82:AF:D2:E0 GWN7600L(GWN7600)

□ 00:0B:82:AF:D2:58 GWN7600R(GWN7600)

Figure 52: Device Membership - Available Devices

2. Press › to move GWN76xx Access Points to "Member Devices".
3. Once done, press **Save** button.



□ 00:0B:82:AF:D2:E0 GWN7600L(GWN7600)

□ 00:0B:82:AF:D2:58 GWN7600R(GWN7600)

Figure 53: Device Membership - Members Devices

SSID Limit

Users have not limit on number of SSID which can be created per Network; however, when any AP has reached a limit of 16 SSID, it will be shown in grey in the new SSID's available devices and cannot be added to new SSID anymore.

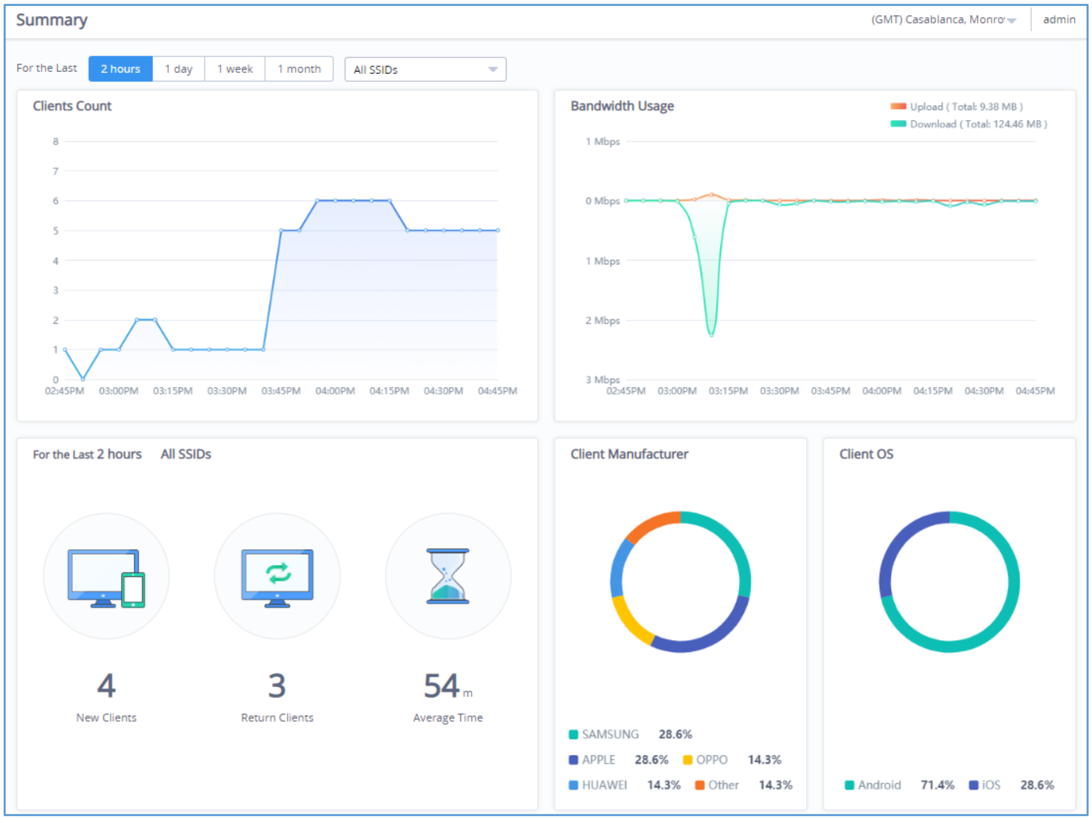
CLIENTS

From The client's page, the administrator can monitor and manage all the clients connected to his networks/access points, this configuration page is divided to 2 sections:

- Summary
- Status

Summary

The summary page provides real time information about the number of clients connected to different SSIDs, the bandwidth usage as well as the client Manufacturer and Client OS.



Summary | (GMT) Casablanca, Monro | admin

For the Last: 2 hours | 1 day | 1 week | 1 month — All SSIDs

Clients Count

Bandwidth Usage — Upload (Total: 9.38 MB) — Download (Total: 124.46 MB)

For the Last 2 hours All SSIDs

4 New Clients

3 Return Clients

54 m Average Time

Client Manufacturer

SAMSUNG	28.6%
APPLE	28.6%
OPPO	14.3%
HUAWEI	14.3%
Other	14.3%

Client OS

Android	71.4%
iOS	28.6%

Figure 54: Clients - Summary

The summary page is divided into 5 different sections: Clients count, Bandwidth usage, Clients statistics for last day, Client Manufacturer as well as Client OS.

Clients Count

Provides in real time the number of clients connected to the Access points, the administrator can filter select the period for monitoring, which can be 2 hours, 1 day, 1 week or 1 month, and specify the SSID to monitor.

Bandwidth Usage

This section shows the download and upload level per time, based on this information the administrator can decide to reduce the bandwidth for specific user and increase it for others.

Clients Statistics for Last Day

From this section, the administrator can monitor the number of new clients for the last day as well as the return clients and the average time spent in the network.

Client Manufacturer

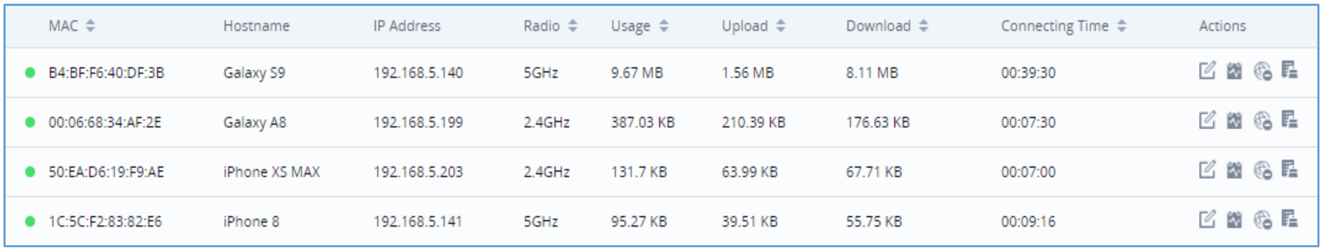
This section shows the statistics of the different client's manufacturer connected to the Access points based on their vendor name.

Client OS

This section shows the statistics of the client's *Operating System* connected to the APs; for example: Android, iOS...

Status

The status page allows the administrator to monitor all the wireless clients connected to his network:



	MAC	Hostname	IP Address	Radio	Usage	Upload	Download	Connecting Time	Actions
●	B4:BF:F6:40:DF:3B	Galaxy S9	192.168.5.140	5GHz	9.67 MB	1.56 MB	8.11 MB	00:39:30	✎ ▨ ◍ ▤
●	00:06:68:34:AF:2E	Galaxy A8	192.168.5.199	2.4GHz	387.03 KB	210.39 KB	176.63 KB	00:07:30	✎ ▨ ◍ ▤
●	50:EA:D6:19:F9:AE	iPhone XS MAX	192.168.5.203	2.4GHz	131.7 KB	63.99 KB	67.71 KB	00:07:00	✎ ▨ ◍ ▤
●	1C:5C:F2:83:82:E6	iPhone 8	192.168.5.141	5GHz	95.27 KB	39.51 KB	55.75 KB	00:09:16	✎ ▨ ◍ ▤

Figure 55: Clients Status

By clicking on the ☰ icon, user can display other information's such as TX and RX Rate, SSID etc.

- Click on ✎ under Actions to edit the client's hostname.

- Click on ▨ under Actions to set the bandwidth rules to each client.

- Click on to block a client's MAC address from connecting to the SSID, Once the client is blocked it will be added to Global blacklist under **Clients → Access List.**

- Click on to clear collected data from Wi-Fi clients. This is mainly for certain data security regulation compliance.

Users can click on a specific client to see detailed information about that client as follow:

First tab is for **data usage** (Upload/Download) for the selected client as shown on the figure below:

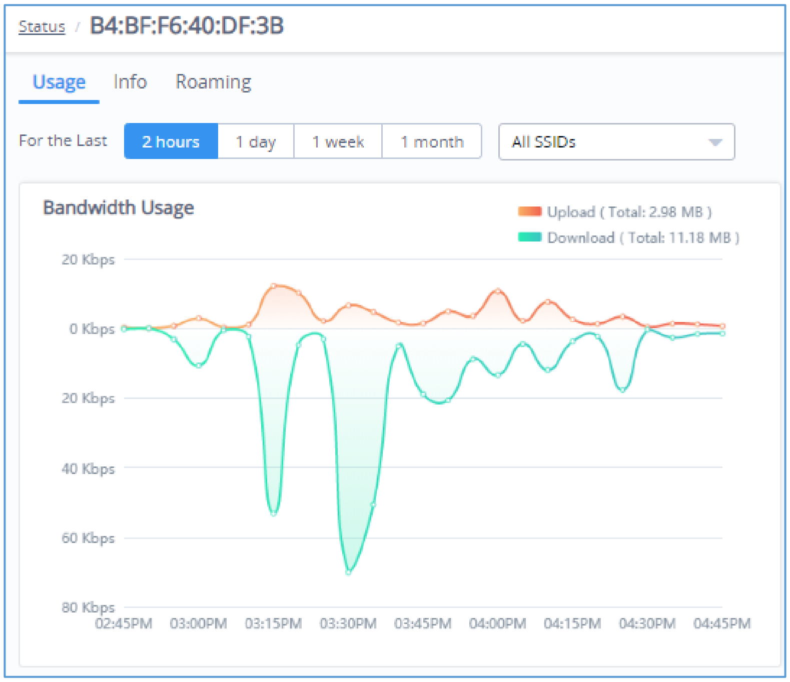
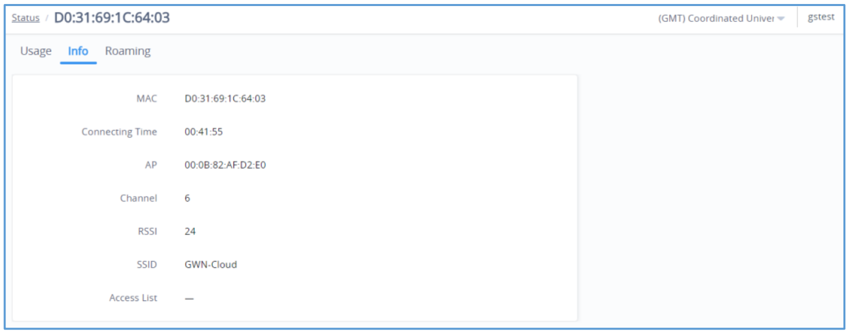


Figure 56: Client Data Usage Info

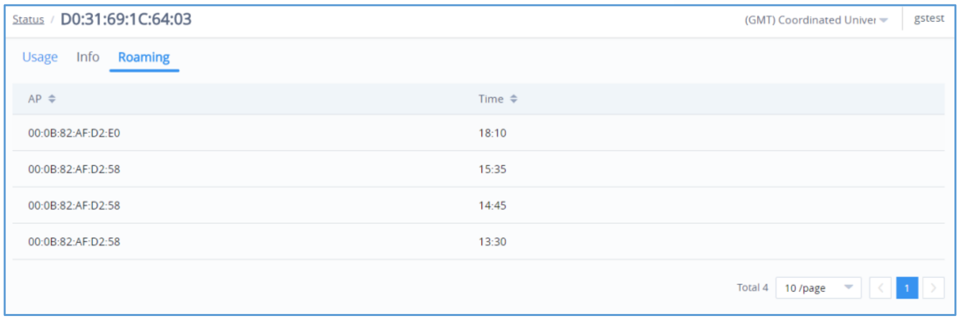
The second tab has some information about the client device itself, such as the MAC address, IP address, UP time…etc.



MAC	D0:31:69:1C:64:03
Connecting Time	00:41:55
AP	00:0B:82:AF:D2:E0
Channel	6
RSSI	24
SSID	GWN-Cloud
Access List	—

Figure 57: Client Info

The last tab is to check roaming status of the client between the different APs as shown on the sample figure below, which do include the Time of roaming.



Status / D0:31:69:1C:64:03

(GMT) Coordinated Univer gstest

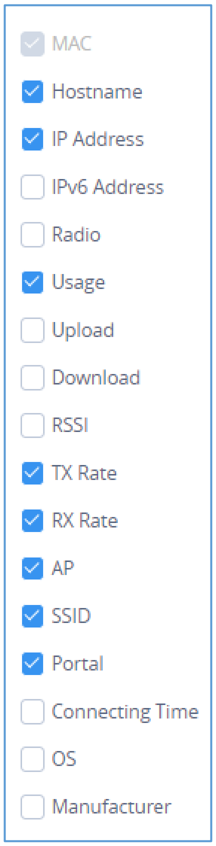
Usage Info **Roaming**

AP	Time
00:0B:82:AF:D2:E0	18:10
00:0B:82:AF:D2:58	15:35
00:0B:82:AF:D2:58	14:45
00:0B:82:AF:D2:58	13:30

Total 4 10 /page 1

Figure 58: Client Roaming

Users can press ☰ button to customize items to display on the page. Following items are supported:



☑ MAC
☑ Hostname
☑ IP Address
☐ IPv6 Address
☐ Radio
☑ Usage
☐ Upload
☐ Download
☐ RSSI
☑ TX Rate
☑ RX Rate
☑ AP
☑ SSID
☑ Portal
☐ Connecting Time
☐ OS
☐ Manufacturer

Figure 59: Clients - Select Items

CAPTIVE PORTAL

Captive Portal feature helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet. Once connected to a GWN AP, Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the platform Web page under "Captive Portal".

The page contains five tabs: **Summary, Guest, Policy List, Splash page and Vouchers.**

Summary

The summary page provides real time information about the clients connected via Captive portal to different SSIDs, including statistics showing the authentication type, the guest session by SSID as well as the max concurrent new session and login failure, the administrator can filter select the period for monitoring, which can be 2 hours, 1 day, 1 week or 1 month, He can also specify the SSID to monitor.

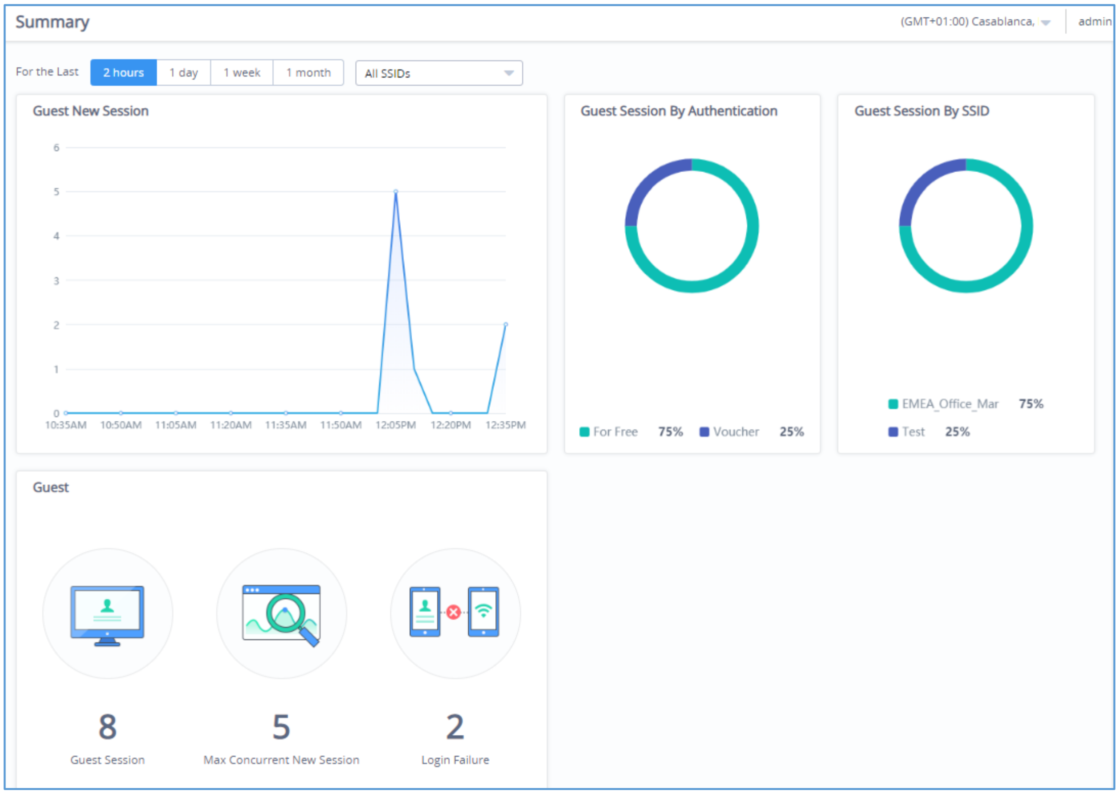


Figure 60: Captive Portal Summary

The summary page is divided into 4 different sections: Guest New Session, Guest Session By Authentication, Guest Session By SSID, Guest section.

Guest New Session

Provides in real time the number of clients connected via Captive Portal, the administrator can filter select the period for monitoring, which can be 2 hours, 1 day, 1 week or 1 month, He can also specify the SSID to monitor.

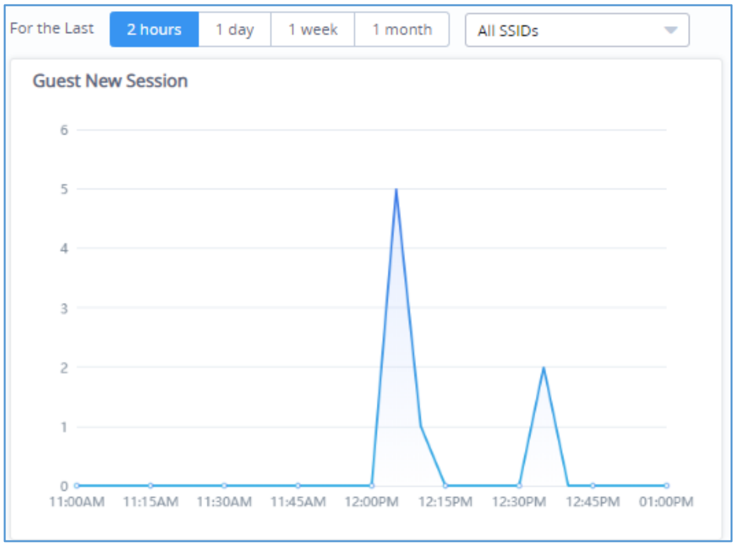


Figure 61: Guest New Session

Guest Session by Authentication

Displays a statistical graphic showing the authentication type used by clients to gain access to internet, it can include all the authentication methods deployed by the captive portal (Free login, Simple password, Facebook Authentication, Twitter Authentication…).

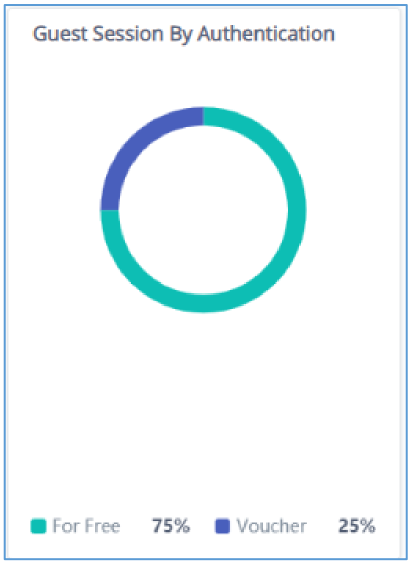


Figure 62: Guest Session by Authentication

Guest Session by SSID

This section displays count of authenticated guests on captive portals per SSID.

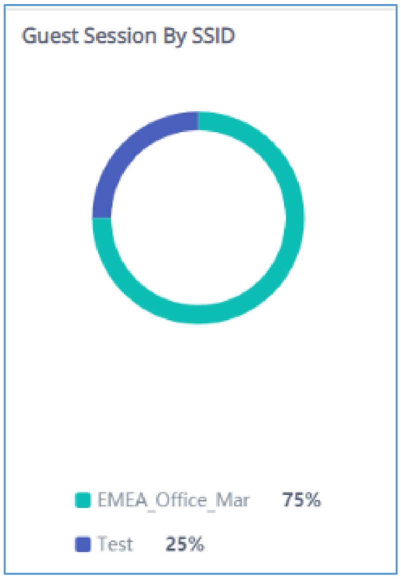


Figure 63: Guest Session by SSID

Guest

This section provides the number of authenticated clients connected on captive portal according to the period selected: 2hours, 1day, 1 week or 1 month, as well as the maximum concurrent new session and login failure.

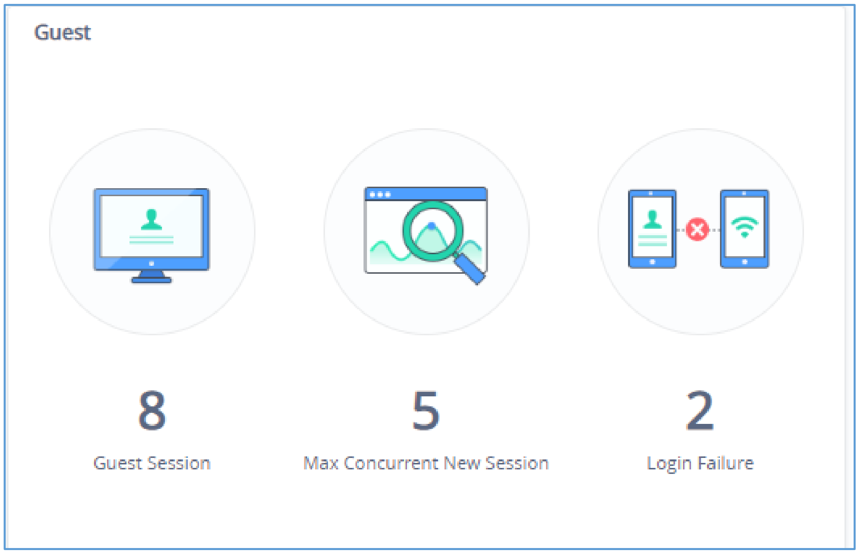
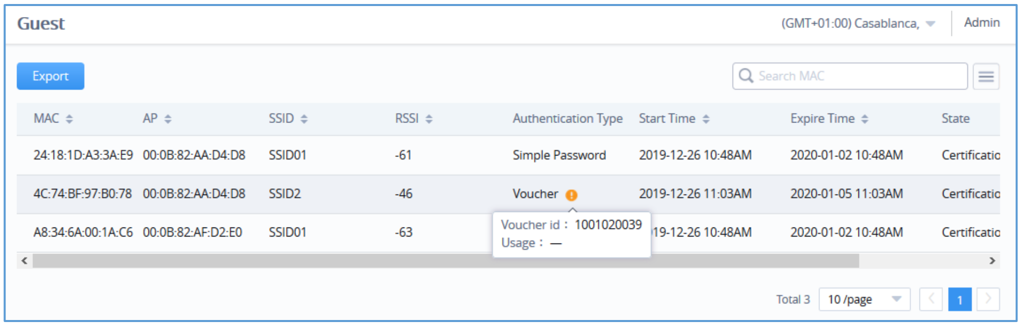


Figure 64: Guest Section

Guest

The guest page displays information about the clients connected via Captive portal including the MAC address, Hostname, Authentication Type, the Access point they are connected to, Certification state, SSID as well as the RSSI and Data usage. The following figure shows an example of the connected client via captive portal.

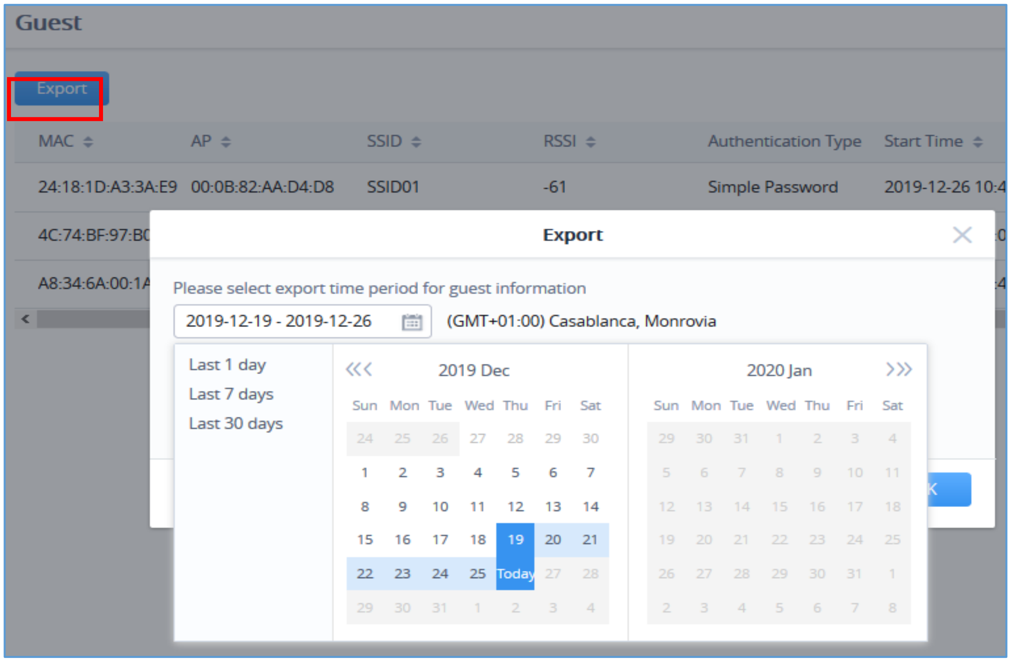


MAC	AP	SSID	RSSI	Authentication Type	Start Time	Expire Time	State
24:18:1D:A3:3A:E9	00:0B:82:AA:D4:D8	SSID01	-61	Simple Password	2019-12-26 10:48AM	2020-01-02 10:48AM	Certificatio
4C:74:BF:97:B0:78	00:0B:82:AA:D4:D8	SSID2	-46	Voucher	2019-12-26 11:03AM	2020-01-05 11:03AM	Certificatio
A8:34:6A:00:1A:C6	00:0B:82:AF:D2:E0	SSID01	-63		19-12-26 10:48AM	2020-01-02 10:48AM	Certificatio

Voucher id : 1001020039
Usage : —

Figure 65: Guest List

Administrator can also export a *.csv* file containing all the guest information (Client MAC address; Authentication Form when choosing Custom Field, Last Visit...etc.) by clicking on Export button, and selecting the export time period for all users which connected to the captive portal during that period



MAC	AP	SSID	RSSI	Authentication Type	Start Time
24:18:1D:A3:3A:E9	00:0B:82:AA:D4:D8	SSID01	-61	Simple Password	2019-12-26 10:4
4C:74:BF:97:B0					
A8:34:6A:00:1A					

Export

Please select export time period for guest information

2019-12-19 - 2019-12-26 (GMT+01:00) Casablanca, Monrovia

2019 Dec

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	Today	27	28
29	30	31	1	2	3	4

2020 Jan

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

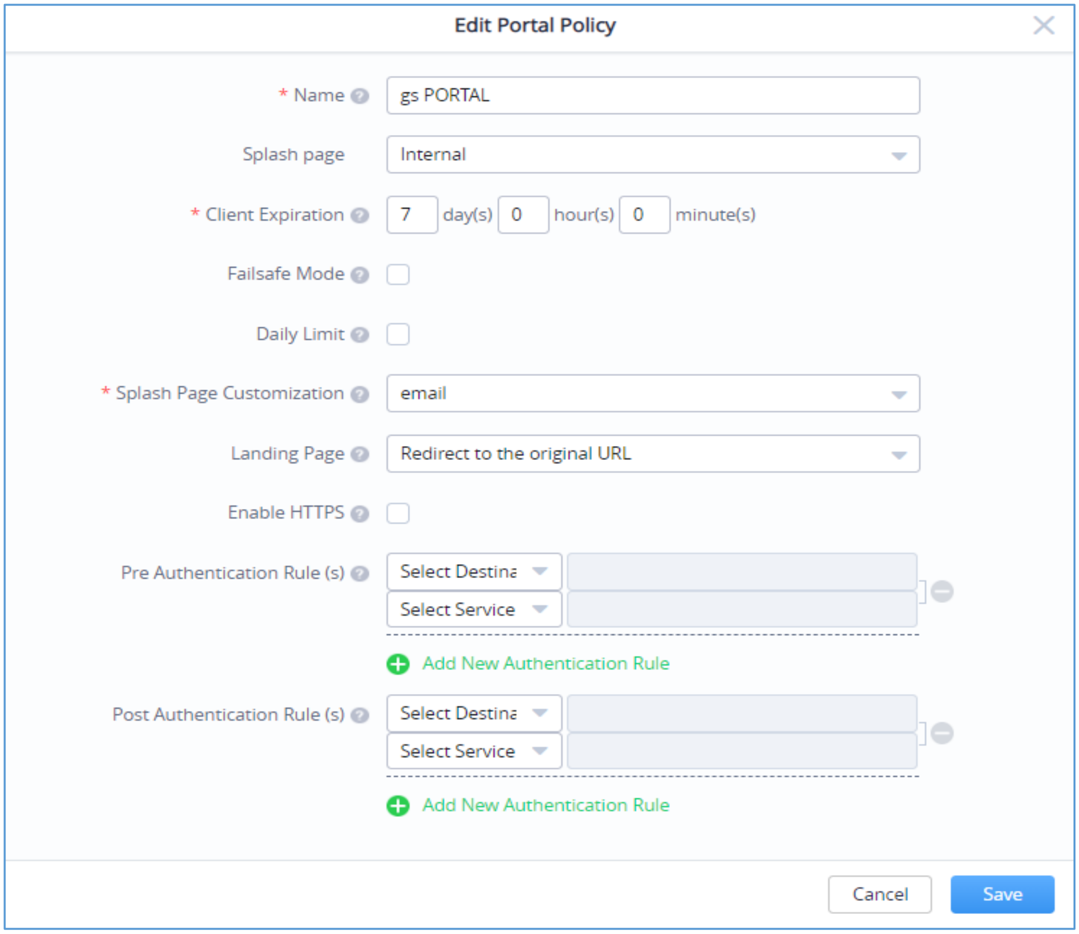
Figure 66: Export Guest Information Period

Note: When authenticating using either “Voucher” or “Custom Field” method, an ! icon will prompt under “Authentication Type” column, when scrolling mouse over it, it will display the actual voucher number/Authentication form filled by users before gaining access to internet.

Policy List

The policy configuration page allows adding multiple captive portal policies which will be applied to SSIDs and contains options for different authentication types a splash page that can be easily configured as shown on the next section.

Each SSID can be assigned a different captive portal policy, for example company ABC could have a specified Wi-Fi for staff people who can access via a portal policy requiring user name and password for authentication, and another SSID for guest people who can sign in via their Facebook account; also, they could assign either an internal or external Splash page.



Edit Portal Policy

* Name	gs PORTAL
Splash page	Internal
* Client Expiration	7 day(s) 0 hour(s) 0 minute(s)
Failsafe Mode	□
Daily Limit	□
* Splash Page Customization	email
Landing Page	Redirect to the original URL
Enable HTTPS	□
Pre Authentication Rule (s)	Select Destina Select Service Add New Authentication Rule
Post Authentication Rule (s)	Select Destina Select Service Add New Authentication Rule

Figure 67: Add/Edit Captive Portal Policy

Internal Splash Page

The following table describes all the settings when creating new internal captive portal policies:

Table 12: Add new Policy List – Splash Page as "Internal"

Field	Description
Name	Enter a name to identify the created portal policy.
Splash Page	Select Splash Page type, Internal or External.
Client Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Failsafe Mode	When enabled; guest can surf on the internet when the authentication server or external portal cannot communicate.
Daily Limit	Once enabled, guest can authenticate once every day, and he cannot re-authenticate after the first authentication expired. The authentication will reset every 0 o'clock.
Splash Page Customization	Configure portal display page.
Landing page	Select the landing page where the users will be sent after successful authentication, two options are available: • **Redirect External Page URL Address:** for promotional purposes, admin can this to redirect all authenticated users to the company website. • **Redirect to the Original URL Address:** Sent the user to the original requested URL.
Enable HTTPS	Check to Enable/disable HTTPS service over captive portal. **Note:** If enabled, both HTTP and HTTPS requests sent from stations will be redirected to the splash page by using HTTPS protocol, and in some cases, guests may not be authenticated successfully for the system or browser does not trust our self-signed certificate.

Pre-Authentication Rule(s)	Set the Pre-Authentication Rules for temporarily release the IP or ports of the devices (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET)
Post Authentication Rule(s)	Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS)

External Splash Page

Table 13: Add new Policy List – Splash Page as "External"

Field	Description
Name	Enter a name to identify the created portal policy.
Splash Page	Select Splash Page type, **Internal** or **External** Splash Page
Platform	Select which external captive portal platform to use: • **Linkyfi Platform** (https://www.avsystem.com/products/linkyfi) • **Purple Platform** (https://purple.ai/) • **Universal Platform** (Socifi Platform for instance)
External Splash Page Address	Enter the External Splash Page URL, and make sure to enter the pre-authentication rules request by the external portal platform in the pre-authentication configuration option.
RADIUS Server Address	Enter the RADIUS Server Address provided by external portal platform.
RADIUS Server Port	Enter the RADIUS Server Port provided by external portal platform, the default value is 1812.
RADIUS Server Secret	Enter the RADIUS Server Secret provided by external portal platform.
RADIUS Accounting Server Address	Enter the Radius Accounting Server Address provided by external portal platform.
RADIUS Accounting Server Port	Enter the Radius Accounting Server Port provided by external portal platform.

RADIUS Accounting Server Secret	Enter the Radius Accounting Server Port provided by external portal platform.
Accounting Update Interval	Enter the Accounting Update Interval, an integer from 30 to 604800. Once the external splash page has configured the parameter, this value will be invalid.
RADIUS NAS ID	Specify the AP tag, limit to 32 characters. *This field appears only when* **Platform** *is set to "**Linkyfi Platform**".*
Redirect URL	Please enter the Redirect URL provided by external portal platform.
Pre-Authentication Rule(s)	Set the Pre-Authentication Rules for temporarily release the IP or ports of the devices (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET)
Post Authentication Rule(s)	Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS)

Note:

Users could create multiple captive portal instances and assign the desired one for each SSID.

As an example, users can create one captive portal for Intranet usage and a second one for public Guest users, after customizing each captive portal separately, you can assign each one to the corresponding SSID.

Splash Page

Page

Splash page allows users with an easy to configure menu to generate a customized splash page that will be displayed to the users when trying to connect to the Wi-Fi.

On this menu, users can create multiple splash pages and assign each one of them on a separate captive portal policy to enforce the select authentication type.

The generation tool provides an intuitive "WYSIWYG" method to customize a captive portal with very rich manipulation tool.

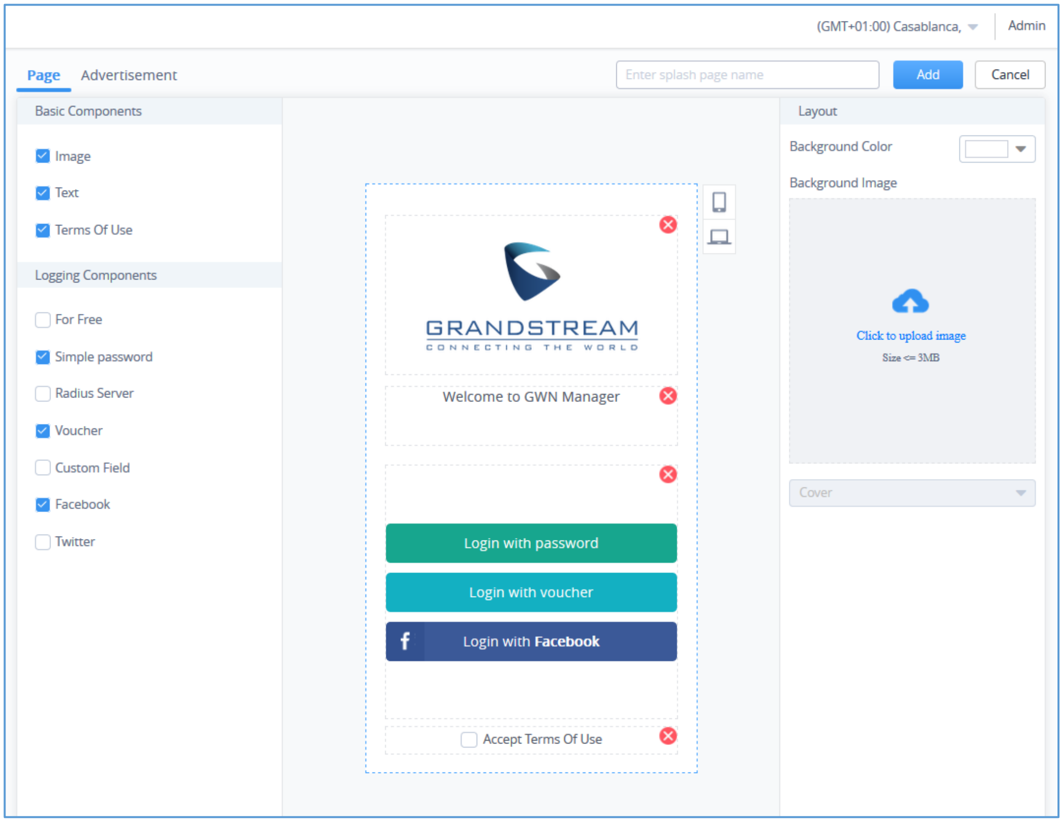
Users can set the following:

- **Authentication type**: Add one or more ways from the supported authentication methods (Simple Password, Facebook, Twitter, Voucher, Radius, No Authentication, WeChat.
- **Setup a picture (company Logo**) to be displayed on the splash page.
- **Customize** the layout of the page and background colors.
- **Customize the Terms of use text.**
- **Visualize a preview** for both mobile devices and laptops.

Note: On each splash page, the maximum number of authentication methods is 5 methods.

Let's create a simple splash page as demonstration, the steps below can be followed to reproduce the same image.

1. First go under "**Captive Portal → Splash Page**" then click on Create Splash Page .



Basic Components

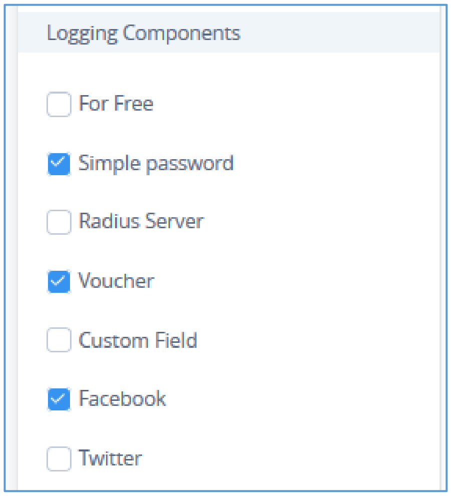
☑ Image
☑ Text
☑ Terms Of Use

Logging Components

☐ For Free
☑ Simple password
☐ Radius Server
☑ Voucher
☐ Custom Field
☑ Facebook
☐ Twitter

Figure 68: Create New Splash Page

2. Next, under “Logging Components” tab we check the methods that will be displayed to the users as a choice to logging. (Users can choose logging either via Facebook, Twitter, Vouchers, Radius Server, For Free or Custom Field)



Logging Components

☐ For Free

☑ Simple password

☐ Radius Server

☑ Voucher

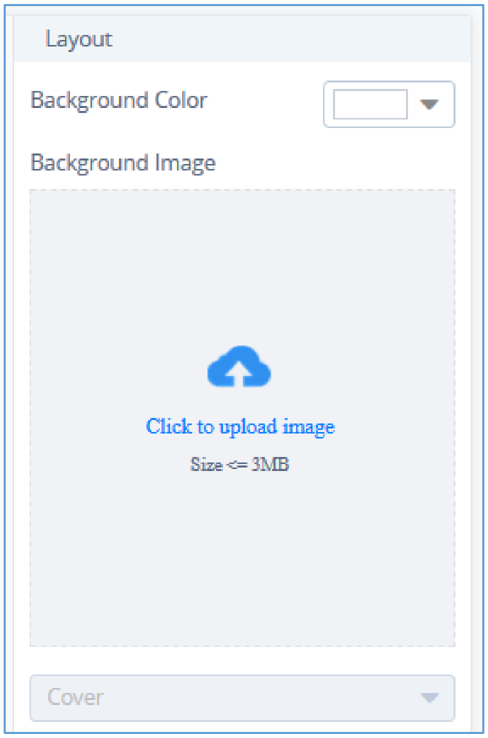
☐ Custom Field

☑ Facebook

☐ Twitter

Figure 69: Setup Logging Methods - Splash Page

3. Under “Layout”, users can upload a logo picture using “Click to Upload Image” which will be used on the splash page. and select a background color if desired (we will skip this step as we demo).



Layout

Background Color

Background Image

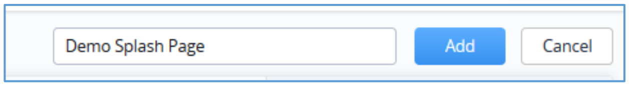
Click to upload image

Size <= 3MB

Cover

Figure 70: Upload a logo - Splash Page

4. Give the page a name at the top of the screen and click on **Add**.

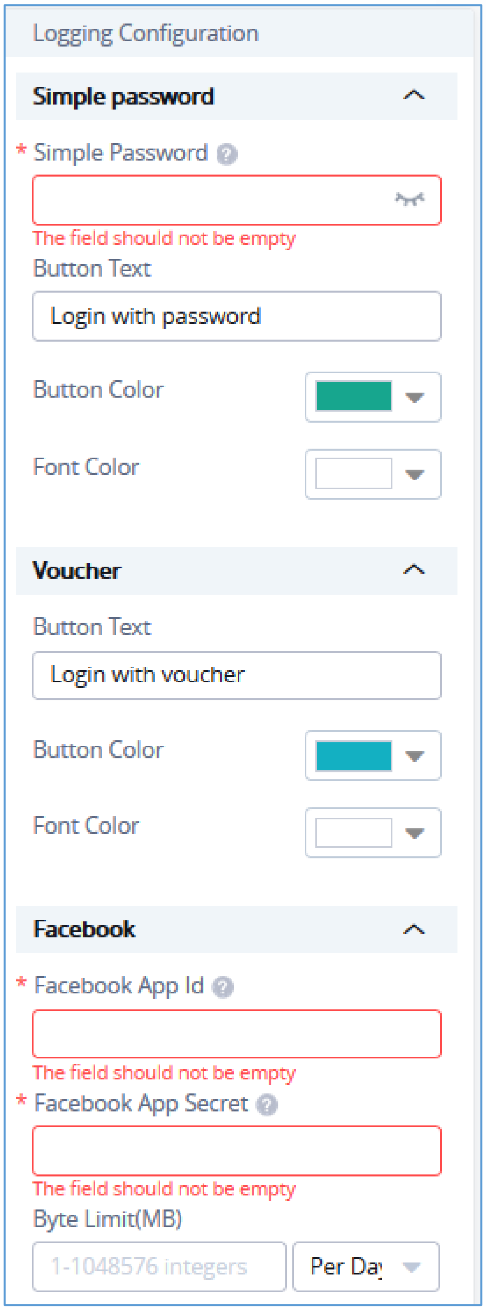


Demo Splash Page

Figure 71: Name - Splash Page

5. Once you click on **Add,** you will be prompted to enter some necessary information that are required when using social logging (Facebook API codes, Twitter...Etc.) for more details about these concepts, please refer to the following How-to Guides:

   - ✓ Captive Portal - RADIUS Authentication
   - ✓ Captive Portal - Facebook Authentication
   - ✓ Captive Portal - Twitter Authentication
   - ✓ Captive Portal - Voucher Authentication



Logging Configuration

Simple password

* Simple Password

The field should not be empty

Button Text: Login with password

Button Color

Font Color

Voucher

Button Text: Login with voucher

Button Color

Font Color

Facebook

* Facebook App Id

The field should not be empty

* Facebook App Secret

The field should not be empty

Byte Limit(MB): 1-1048576 integers, Per Day

Figure 72: Setup Social Logging Parameters

Note: When choosing "Twitter Authentication" method; a **"Force To Follow"** button will be added; by enabling it, admin can request guest Wi-Fi clients to follow his Twitter account when getting authenticated.

6. Once done, users can have a preview of the look of the page on either mobile phones or laptops.

   ○ To see the preview of the page on mobile phones click on 📱 button.

- Or click on 💻 button to see the preview of the page on computer screens.

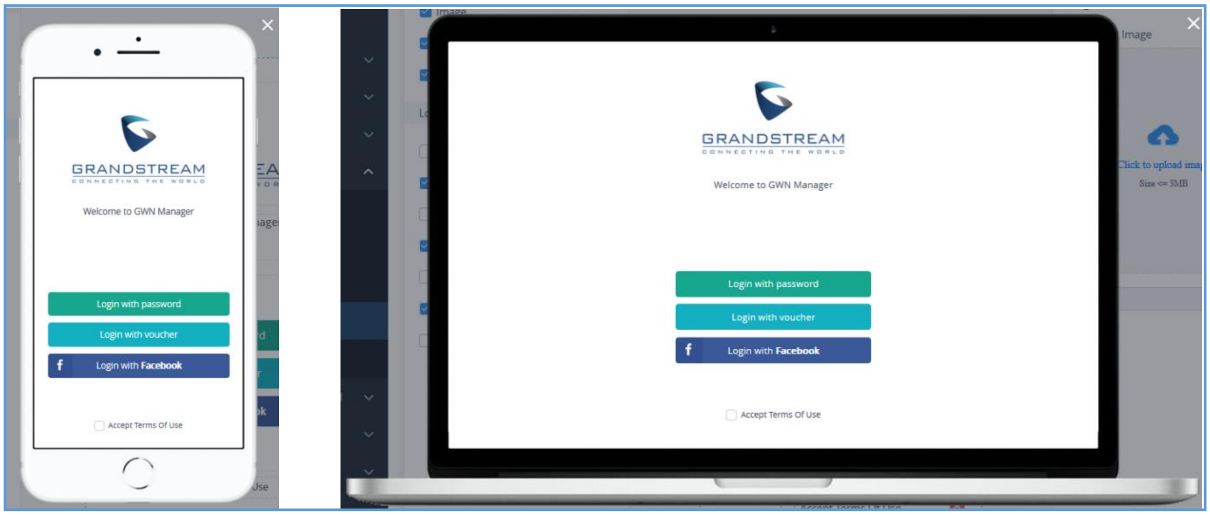


Figure 73: Splash Page Preview

7. If you are satisfied with the final design. Click on **Add** and after the page has been added to it will be displayed along other existing pages with the possibility to either "Edit" or "Delete" it.

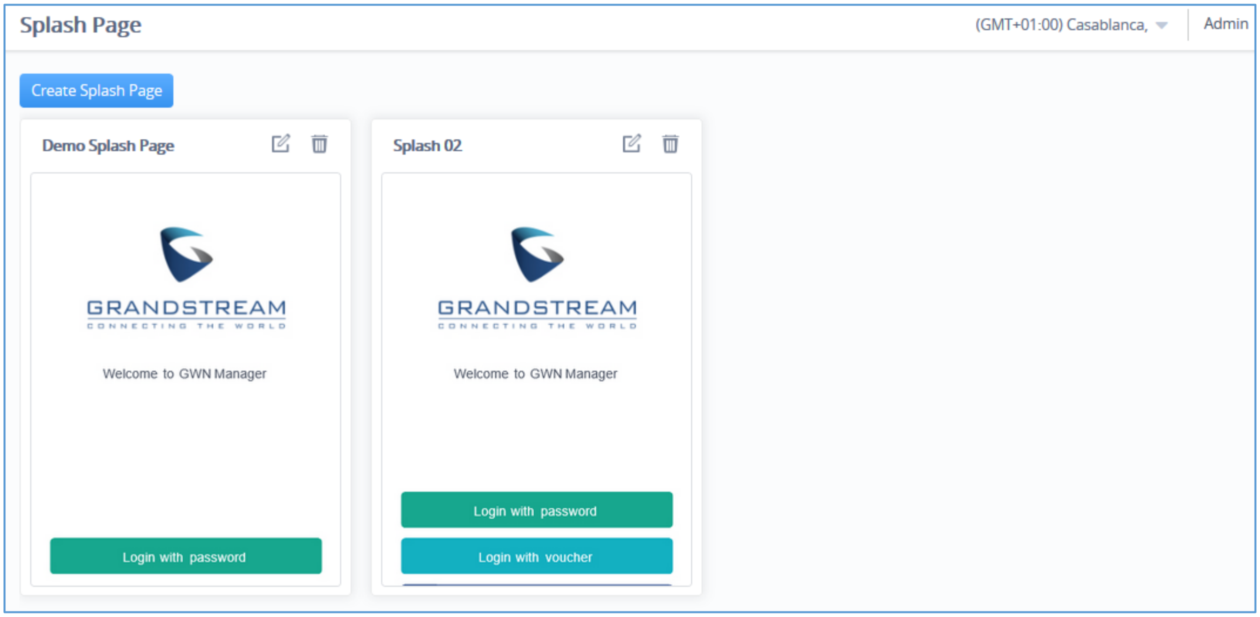
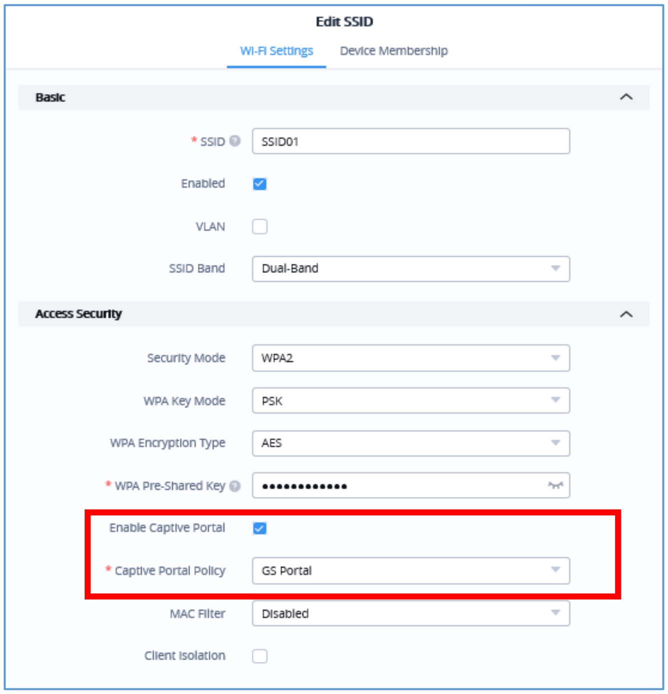


Figure 74: Splash Pages List

All these pages can be used on different captive portal policies depending on the user's needs.

8. Go back to SSIDs ➔ Configuration ➔ Actions: "Edit" ➔ Wi-Fi Settings ➔ Access Security, to "Enable" Captive Portal and "Select" the preferred Captive Portal Policy:



Edit SSID

Wi-Fi Settings | Device Membership

Basic

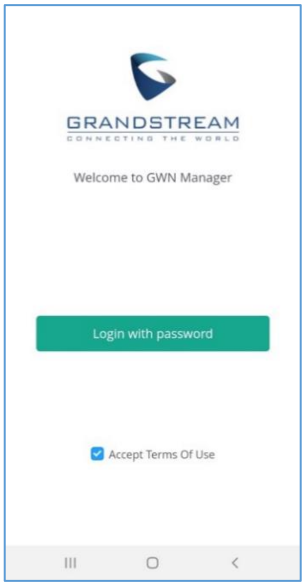
* SSID	SSID01
Enabled	☑
VLAN	☐
SSID Band	Dual-Band

Access Security

Security Mode	WPA2
WPA Key Mode	PSK
WPA Encryption Type	AES
* WPA Pre-Shared Key	••••••••••••
Enable Captive Portal	☑
* Captive Portal Policy	GS Portal
MAC Filter	Disabled
Client Isolation	☐

Figure 75: Enable Captive Portal

9. Clients will get the below display when trying to connect to the Wi-Fi:



GRANDSTREAM
CONNECTING THE WORLD

Welcome to GWN Manager

☑ Accept Terms Of Use

Figure 76: Portal Splash Page

Advertisement

Advertisement page is a Marketing feature which will allow to play advertisement upon Captive Portal login for Wi-Fi users.

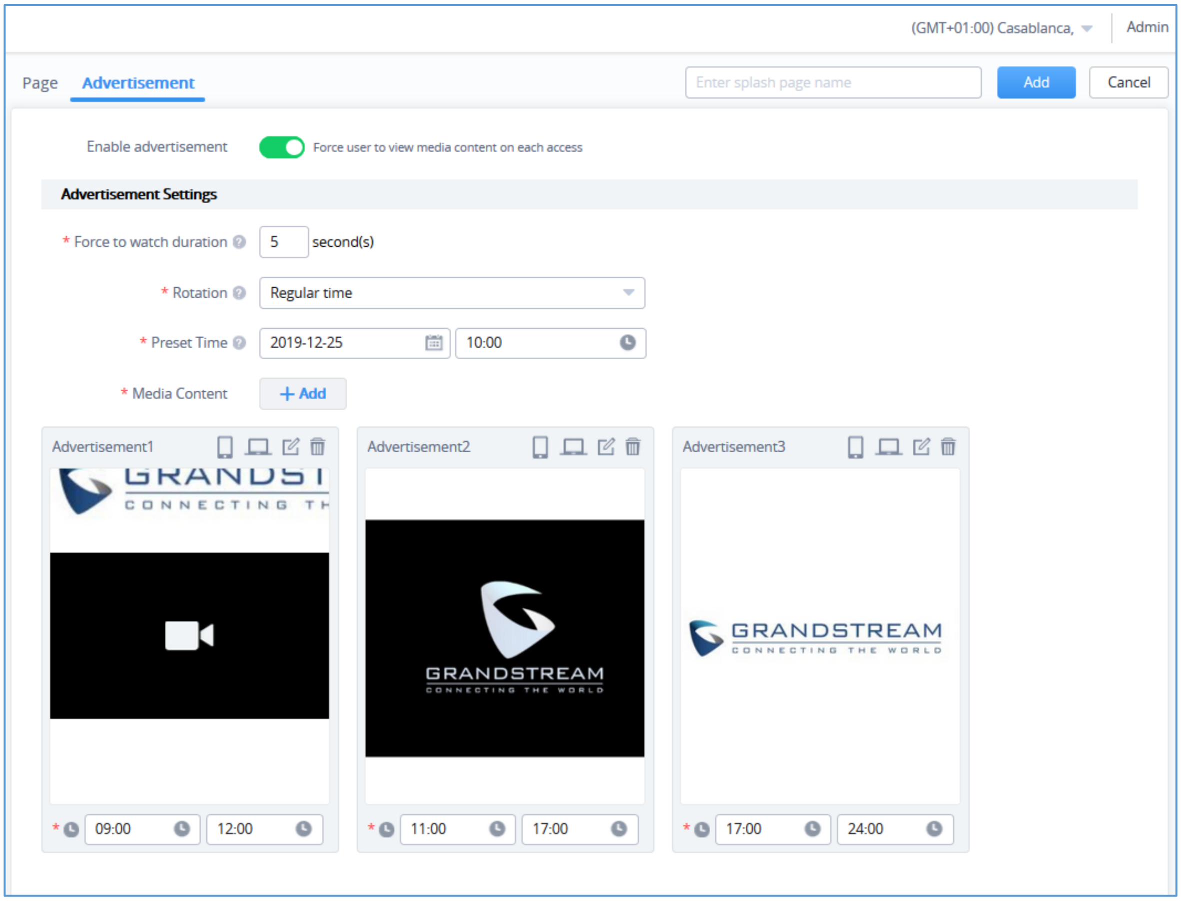
As an example, most companies or stores have free Wi-Fi which they offer to their customers.

This is a good place to meet their customers where they are at by using the **Advertisement Splash Page** to connect advertisers to target customers either by displaying a promoting video or images.

To configure or enable advertisement, following steps must be configured:

1. Go under "**Captive Portal → Splash Page → Advertisement**"

- Click on **Enable Advertisement.**



(GMT+01:00) Casablanca, Admin

Page Advertisement

Enter splash page name Add Cancel

Enable advertisement: on. Force user to view media content on each access

Advertisement Settings

* Force to watch duration: 5 second(s)

* Rotation: Regular time

* Preset Time: 2019-12-25 10:00

* Media Content: + Add

Advertisement1: 09:00 – 12:00

Advertisement2: 11:00 – 17:00

Advertisement3: 17:00 – 24:00

Figure 77: Advertisement Page

2. Enter the Advertisement Settings, below table gives more details about each option:

Table 14: Advertisement Settings Configuration

Force to watch duration	Specify the duration that guests must watch advertisement for. Please enter an integer from 1 to 300.
Rotation	Specify the rotation mode of the ads. • **Random:** the ads will be prompted randomly.

	• **Regular Interval:** the created ads should be specified with advertising periods, and the ads will be prompted in turns. • **Regular Time:** the created ads should be specified with start time and end time, and the ads will be prompted at regular time every day.
Preset Time	Preset the start time of the advertising policy.
Media Content	Click + Add button to add Image/Video content. **Notes:** • The video file content should not exceed 5 MB • Video format only supports MP4 in H.264 codec • Supports input of YouTube URL. • When playing ads with multiple images, it will automatically switch every 3 seconds.

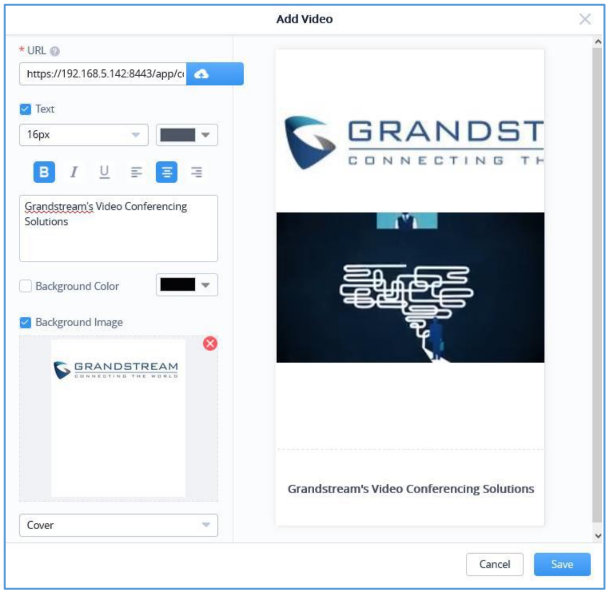

Add Video
* URL
https://192.168.5.142:8443/app/c
☑ Text
16px
B I U
Grandstream's Video Conferencing Solutions
□ Background Color
☑ Background Image
Cover
Grandstream's Video Conferencing Solutions
Cancel
Save

Figure 78: Add Video - Advertisement

3. Once done, users can have a preview of the advertisement on either mobile phones or laptops.

    - To see the preview of the ads on mobile phones click on 📱 button.

    - Or click on 💻 button to see the preview of the ads on computer screens.

Voucher

Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from platform controller.

As an example, a coffee shop could offer internet access to customers via Wi-Fi using voucher codes that can be delivered on each command. Once the voucher expires the client can no longer connect to the internet.

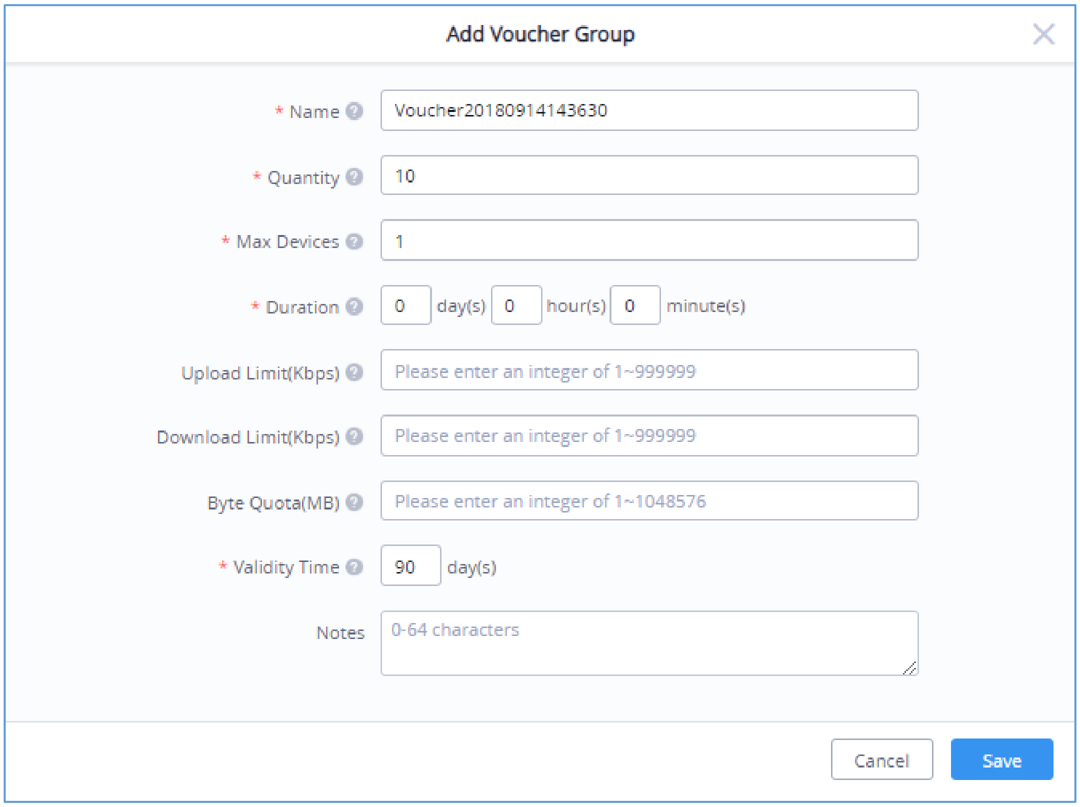
Note that multiple users can use a single voucher for connection with expiration duration of the voucher that starts counting after first successful connection from one of the users that are allowed.

Another interesting feature is that the admin can set data bandwidth limitation on each created voucher depending on the current load on the network, users' profile (VIP customers get more speed than regular ones etc.…) and the internet connection available (fiber, DSL or cable etc.…) to avoid connection congestion and slowness of the service.

Each created voucher can be printed and served to the customers for usage, and the limit is 1000 vouchers.

To configure or add vouchers, following steps must be followed:

4. Go under "**Captive Portal → Voucher**" then click on **Add**.



Add Voucher Group

* Name	Voucher20180914143630
* Quantity	10
* Max Devices	1
* Duration	0 day(s) 0 hour(s) 0 minute(s)
Upload Limit(Kbps)	Please enter an integer of 1~999999
Download Limit(Kbps)	Please enter an integer of 1~999999
Byte Quota(MB)	Please enter an integer of 1~1048576
* Validity Time	90 day(s)
Notes	0-64 characters

Figure 79: Adding Vouchers

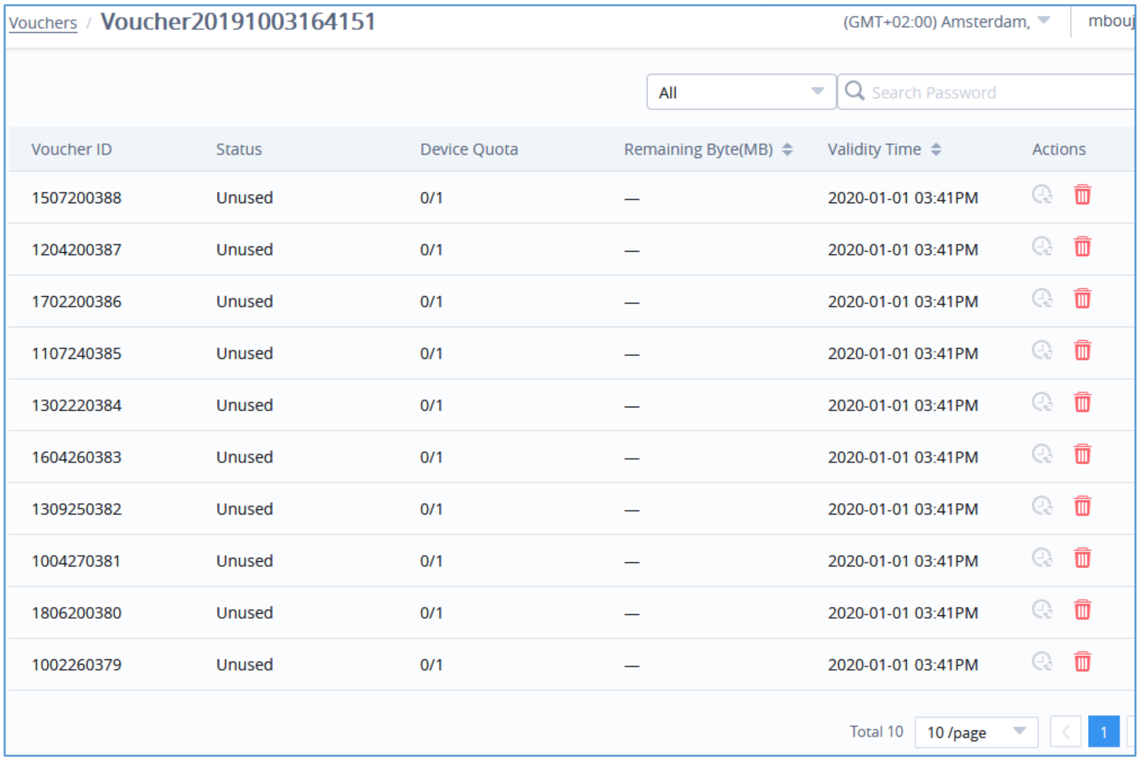
5. Enter the parameters to create a voucher, below table give more details about each option.

Table 15: Voucher Configuration Parameters

Name	Enter a name to identify the voucher
Quantity	Specify how many voucher codes to create which do follow same settings (bandwidth rates, duration, validity...Etc.). Range from 1~1000.
Max Devices	Specify how many users can connect using the same voucher code. Range is from 1~10000 while 0 means unlimited.
Duration	Configure the voucher duration from 1 minutes to 7 days.
Upload Limit (kbps)	Configured upstream data rate limit for the voucher. 0 means unlimited.
Download Limit (kbps)	Configured downstream data rate limit for the voucher. 0 means unlimited.
Byte Quota (MB)	Configure the total usage of the voucher.
Validity Time	Duration of validity of the voucher. It starts with first authentication.
Notes	Notes entered during configuration. Used by admin for documentation purpose.

6. Click on Save to generate the Vouchers.

7. Once done, the voucher status will be displayed with related information and users can click on the voucher to see more details about the generated codes.

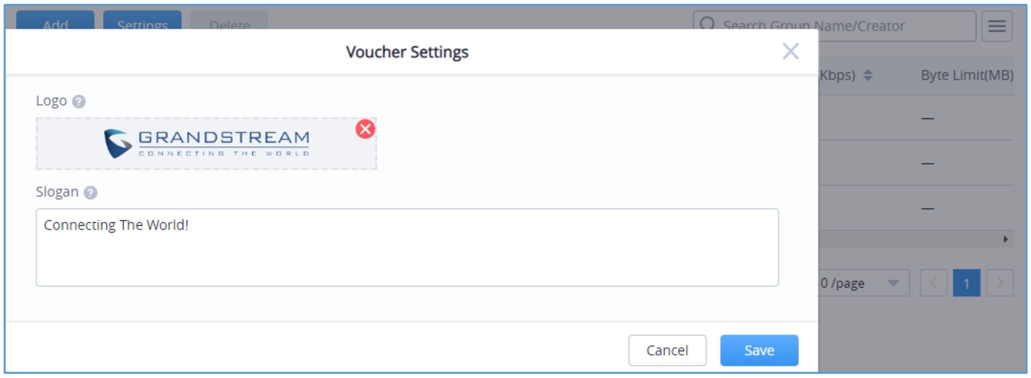


Voucher ID	Status	Device Quota	Remaining Byte(MB)	Validity Time	Actions
1507200388	Unused	0/1	—	2020-01-01 03:41PM	
1204200387	Unused	0/1	—	2020-01-01 03:41PM	
1702200386	Unused	0/1	—	2020-01-01 03:41PM	
1107240385	Unused	0/1	—	2020-01-01 03:41PM	
1302220384	Unused	0/1	—	2020-01-01 03:41PM	
1604260383	Unused	0/1	—	2020-01-01 03:41PM	
1309250382	Unused	0/1	—	2020-01-01 03:41PM	
1004270381	Unused	0/1	—	2020-01-01 03:41PM	
1806200380	Unused	0/1	—	2020-01-01 03:41PM	
1002260379	Unused	0/1	—	2020-01-01 03:41PM	

Figure 80: Voucher Details

This page displays the vouchers status as used/unused, remaining Bytes, the validity time and how many devices used the voucher if multi-user is enabled (quota) when setting the voucher parameters.

With Voucher Settings, users can customize the voucher layout by clicking on Settings and can add logo (Size <=1MB, pixel: 368*30) and slogan (maximum character length is 120).



Logo

Slogan

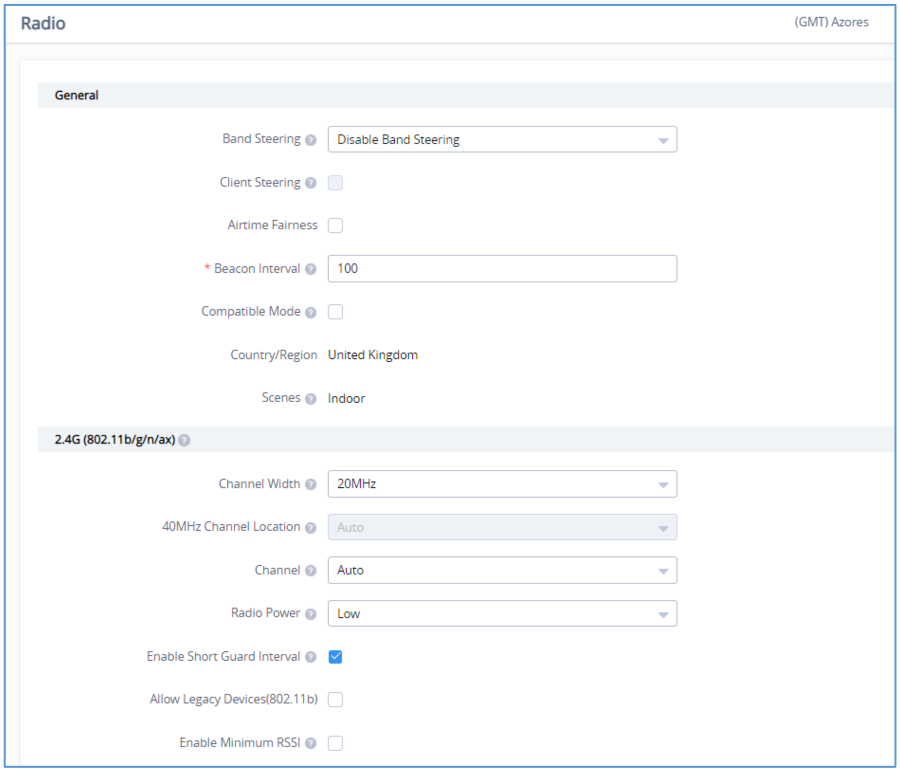
Connecting The World!

Figure 81: Voucher Settings

RADIO

When using GWN76XX as Master Access Point, users can edit the frequency band used by the AP and channel used along with the Transmission power for each band.

Log in as Master to the GWN76XX Web GUI and go to **Radio.**



Radio (GMT) Azores

General

Band Steering: Disable Band Steering

Client Steering: □

Airtime Fairness: □

* Beacon Interval: 100

Compatible Mode: □

Country/Region: United Kingdom

Scenes: Indoor

2.4G (802.11b/g/n/ax)

Channel Width: 20MHz

40MHz Channel Location: Auto

Channel: Auto

Radio Power: Low

Enable Short Guard Interval: ☑

Allow Legacy Devices(802.11b): □

Enable Minimum RSSI: □

Figure 82: Radio-General

Table 16: Radio Settings

General	
Field	**Description**
Band Steering	When Frequency is set to Dual-Band, users can check this option to enable Band Steering on the Access Point, this will help redirecting clients to a radio band accordingly for efficient use and to benefit from the maximum throughput supported by the client.
Client Steering	This feature will help Wi-Fi client to roam to other APs within same Network. Parameters of RSSI Threshold and Client Access Threshold parameters will show up only when Client Steering is enabled.

	Supported only by GWN7600/7600LR/ GWN7630/7630LR /GWN7605/ 7605LR.
Airtime Fairness	Allow faster clients to have more airtime than slower clients. *This feature is not supported on GWN7600/GWN7600LR/GWN7610.*
Beacon Interval	Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp… • **Using High Beacon Interval:** AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save Wi-Fi clients energy consumption. • **Using Low Beacon Interval:** AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by Wi-Fi clients with weak signal. **Notes:** 1. When AP enables several SSIDs with different interval values, the max value will take effect. 2. When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. 3. When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. 4. When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500. 5. Mesh feature will take up a share when enabled.
Scene	Depending deployment type (Indoor or Outdoor) then additional 5Ghz channels (DFS Channels) will be available to be used. Please refer to table DFS Channels supported by Model.
2.4G & 5G Configuration	• **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high-density environment.

	• **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be Secondary below Primary, Primary below Secondary or Auto. • **Channel:** Select Auto, or a specified channel, default is Auto. Note that the proposed channels depend on **Country** Settings under **System Settings→Maintenance**. • **Radio Power:** Set the Radio Power, it can be Low, Medium or High, or Dynamically assigned by RRM (AP will actively change TX power depending on RRM settings). • **Enable Short Guard Interval:** Check to activate this option to increase throughput. • **Custom Wireless Power(dBm):** allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31. • **Allow Legacy Devices(802.11b):** Check to support 802.11b devices to connect the AP in 802.11n/g mode. (2.4GHz setting) • **Dynamic Channel Assignment:** Once enabled, AP will try to allocate and move the best channel during operation, unlike Auto Channel Selection (ACS) which scan and assign channel when Wi-Fi interface goes up for one time. *This feature is not supported on GWN7602.* • **Transmit Power Control:** TPC algorithm runs every 10 minutes. AP acquires the RSSI information of the neighbor by wireless scanning and establishes the neighbor table. The algorithm requires that there must be at least 3 neighbor APs with RSSI larger than -70dbm. Otherwise, power will not be adjusted. *This feature is not supported on GWN7602.* **Coverage Hole Detection:** CHD enables AP to decide whether to increase the AP power by the current SNR and SNR threshold of the connected clients. *This feature is not supported on GWN7602.* • **Enable Minimum RSSI:** Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm). • **Minimum RSSI:** Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from “-94” or “-1”.

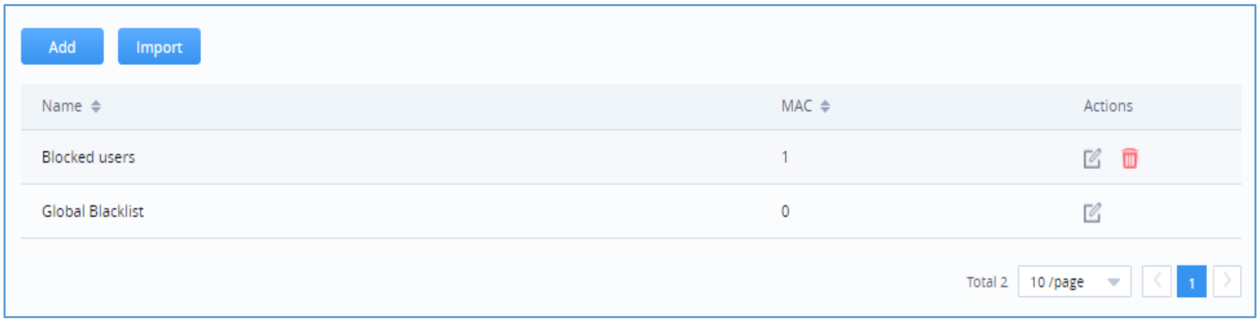
	• **Minimum Access Rate Limit:** Specify whether to limit the minimum access rate for clients. When enabled, it will help to eliminate the legacy connection which slow the total performance of the Wi-Fi network. Range from 1 to 54 Mbps.

ACCESS CONTROL

Access control menu is used in order to set different access control policy such as blocking specific clients from accessing the wireless network using access list of MAC addresses, or setting up time policies which specified how much time are clients allowed to connect to a specific network/SSID and finally administrator can even setup bandwidth rules to control the data rate usage for a specific MAC, IP address or even the whole SSID/Network Group.

Access List

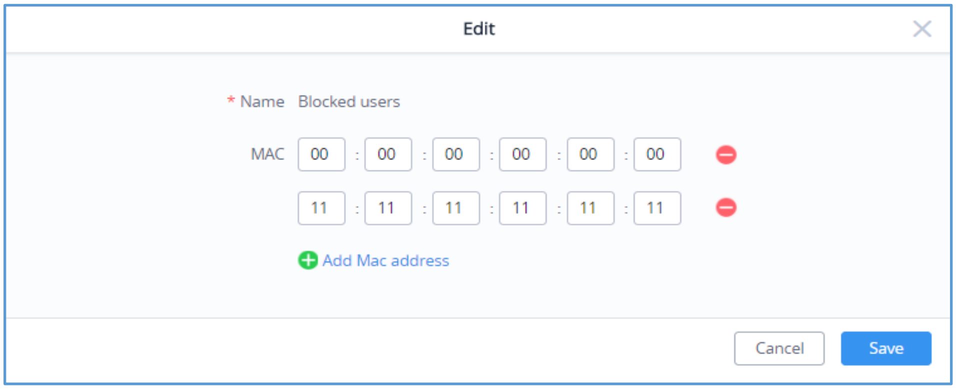
Access List configuration page is used to block specific clients by their address MAC, the administrator can create several access Lists and apply them to specific SSIDs.



Name	MAC	Actions
Blocked users	1	✎ 🗑
Global Blacklist	0	✎

Figure 83: Access List

To add a client to access list go under **Clients → Access List → Add,** a new page will popup, enter the MAC addresses of the clients to block and click on save:



* Name: Blocked users

MAC: 00 : 00 : 00 : 00 : 00 : 00

11 : 11 : 11 : 11 : 11 : 11

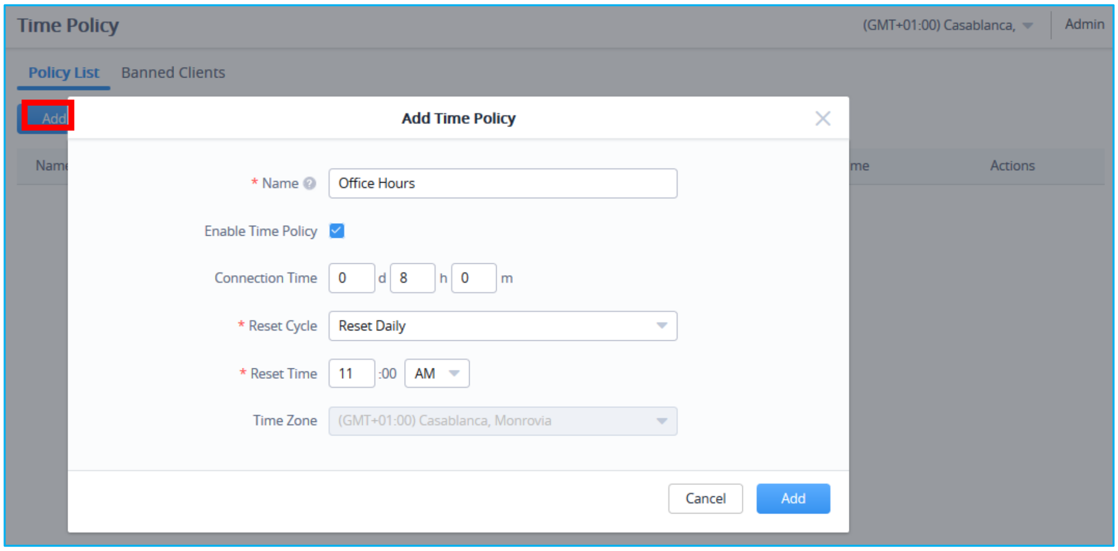
Figure 84: Adding New Clients to Access List

Note: It is also possible to import an access list in CSV format by clicking on Import.

Template is available for download from the same page

Time Policy

The administrator can configure a Time policy which will dictate for how much a client connect to the Wi-Fi if this policy is applied for the SSID.



Add Time Policy

* Name: Office Hours

Enable Time Policy: ☑

Connection Time: 0 d 8 h 0 m

* Reset Cycle: Reset Daily

* Reset Time: 11 :00 AM

Time Zone: (GMT+01:00) Casablanca, Monrovia

Figure 85: Add Time Policy List

Table 17: Time Policy Configuration Parameters

Name	Enter a name to identify the Policy. Supports 1 to 32 characters, including numbers, letters and special characters.
Enable Time Policy	Check/Uncheck to Enable/Disable Policy
Connection Time	Configure the policy duration from 1 minutes to 365 days.
Reset Cycle	Set up a Reset mode: Daily, Weekly or Periodically
Reset Time	When Reset Cycle is Daily: configure the time of the day When Reset Cycle is Weekly: configure the time and the day of the week When Reset Cycle is Periodically: configure the period (d//h/m)
Time Zone	Detected Automatically. This parameter can be changed under System → Settings

Bandwidth rules

The bandwidth rule is a platform feature that allows users to limit bandwidth utilization per SSID, per Client or client (MAC address or IP address).

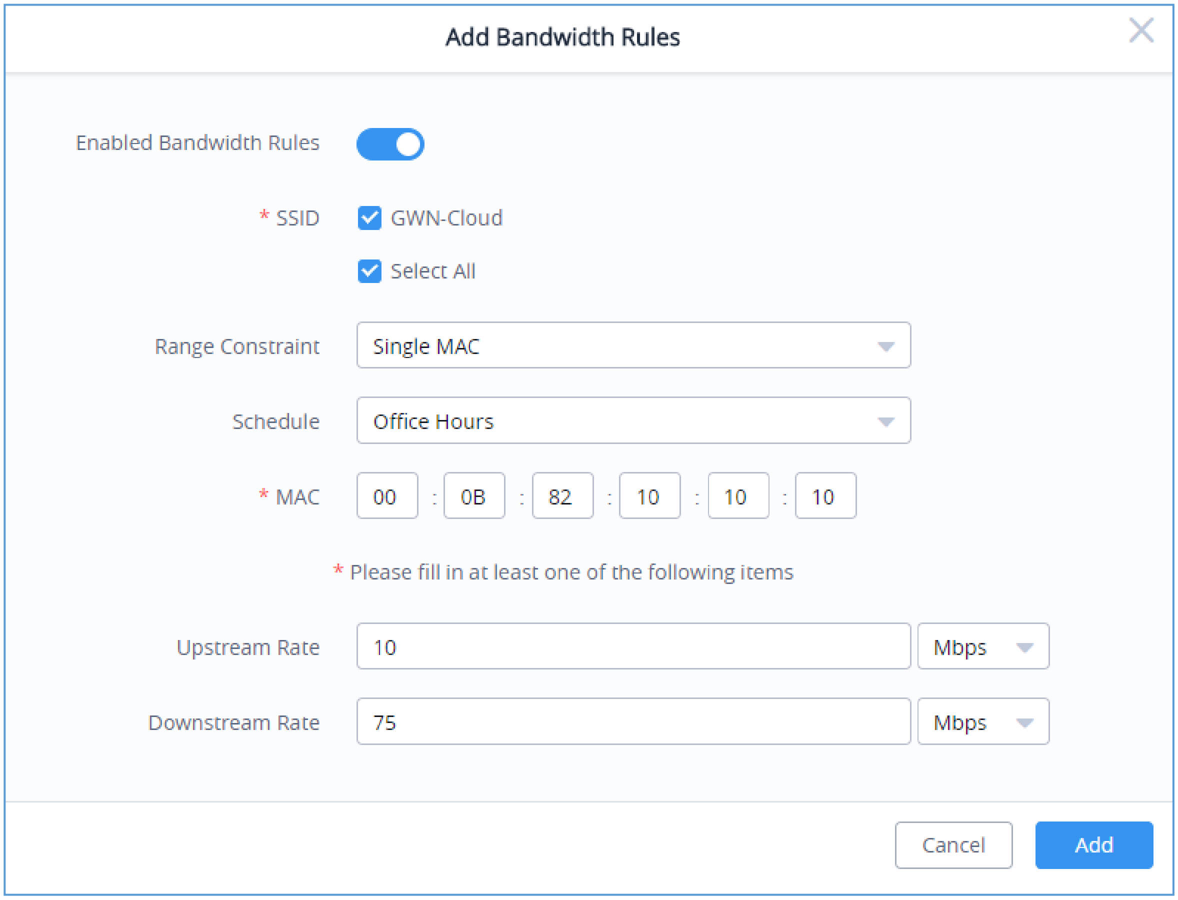
Click Add to add a new rule, the following table provides an explanation about different options for bandwidth rules.

Table 18: Bandwidth Rules

Field	Description
Enable Bandwidth Rules	Enable/Disable Bandwidth Rules
SSID	Select the SSID to which the limitation will be applied.
Range Constraint	• **Per-SSID:** means the rule will be shared/applied to all clients connected to the SSID. • **Single MAC**: This means the rule will be applied only to one client. • **Single IP**: This means the rule will be applied to the specified IP or shared among subnet, for example if we set a Downstream Rate of 20 Mbps on 192.168.10.0/24; all members of that subnet will share the 20Mbps Downstream Rate. • **Per-Client:** This means the rule will be applied to each client connected to the specific SSID, for example if we set a rule of 5Mbps Downstream Rate, each client will have a maximum downstream rate of 5Mbps.
MAC	Enter the MAC address of the device to which the limitation will be applied, this option appears only when MAC type is selected.
IP address	Enter the IP address of the device to which the limitation will be applied, this option appears only when IP Address type is selected.
Schedule	Select a specific schedule where this bandwidth rule will be active, the schedule can be created under the menu "**System → Schedule**"
Upstream Rate	Specify the limit for the upload bandwidth using Kbps or Mbps.

Downstream Rate	Specify the limit for the download bandwidth using Kbps or Mbps.

The following figure shows an example of MAC address rule limitation.



Add Bandwidth Rules

Enabled Bandwidth Rules: ●

* SSID: ☑ GWN-Cloud

☑ Select All

Range Constraint: Single MAC

Schedule: Office Hours

* MAC: 00 : 0B : 82 : 10 : 10 : 10

* Please fill in at least one of the following items

Upstream Rate: 10 Mbps

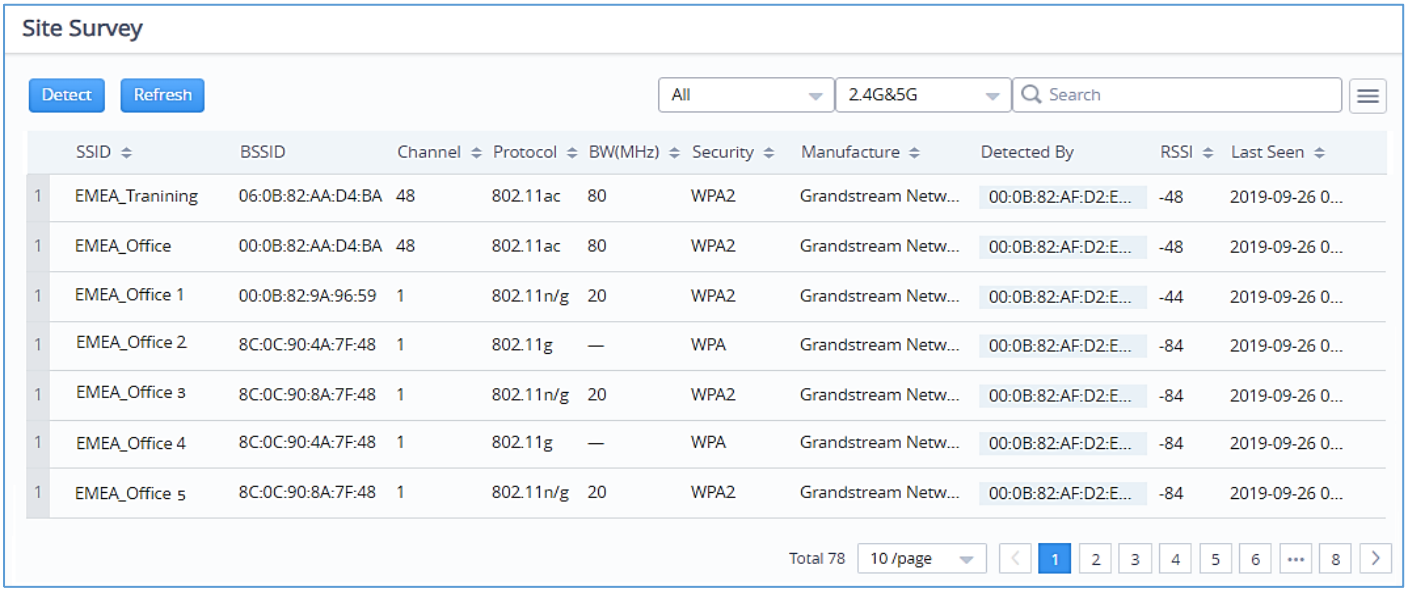
Downstream Rate: 75 Mbps

Figure 86: MAC Address Bandwidth Rule

INSIGHT

Site Survey

An integrated Wi-Fi Scanner is supported on GWN Management Platforms helps the administrator to scan the wireless networks in the area and to display extensive information including: SSID's name, AP's MAC address, Channel used, Wi-Fi Standard, Bandwidth, security standard used, Manufacturer, RSSI, … and more.



Site Survey

	SSID	BSSID	Channel	Protocol	BW(MHz)	Security	Manufacture	Detected By	RSSI	Last Seen
1	EMEA_Tranining	06:0B:82:AA:D4:BA	48	802.11ac	80	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-48	2019-09-26 0...
1	EMEA_Office	00:0B:82:AA:D4:BA	48	802.11ac	80	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-48	2019-09-26 0...
1	EMEA_Office 1	00:0B:82:9A:96:59	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-44	2019-09-26 0...
1	EMEA_Office 2	8C:0C:90:4A:7F:48	1	802.11g	—	WPA	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 3	8C:0C:90:8A:7F:48	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 4	8C:0C:90:4A:7F:48	1	802.11g	—	WPA	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 5	8C:0C:90:8A:7F:48	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...

Total 78 10 /page < 1 2 3 4 5 6 ••• 8 >

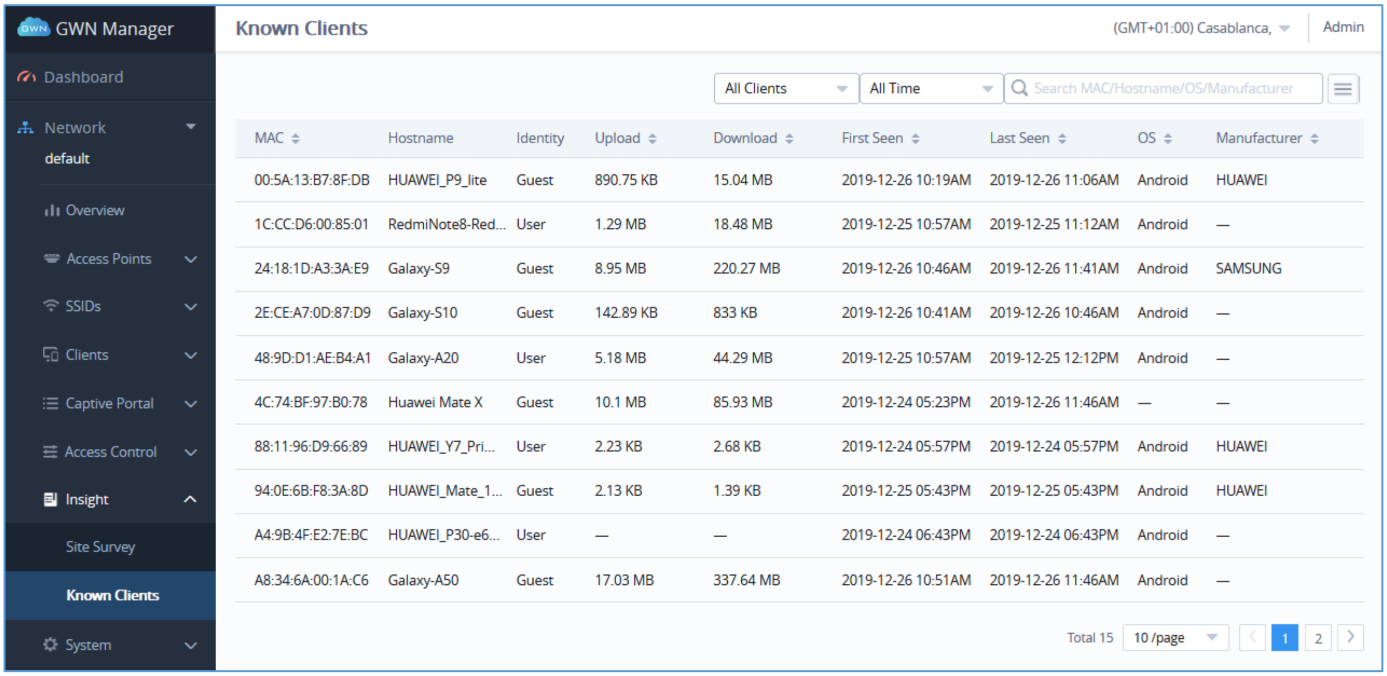
Figure 87: Site Survey - Insight

Users can press Detect to run the Wi-Fi Scanner or Press Refresh to refresh the results page.

Known Clients

This option is only available on **GWN Manager**.

It displays extensive information about all the previously connected clients including: MAC address, Hostname, Identity (Network), Upload/Download stream, OS … and more.



Known Clients

(GMT+01:00) Casablanca, | Admin

All Clients | All Time | Search MAC/Hostname/OS/Manufacturer

MAC	Hostname	Identity	Upload	Download	First Seen	Last Seen	OS	Manufacturer
00:5A:13:B7:8F:DB	HUAWEI_P9_lite	Guest	890.75 KB	15.04 MB	2019-12-26 10:19AM	2019-12-26 11:06AM	Android	HUAWEI
1C:CC:D6:00:85:01	RedmiNote8-Red...	User	1.29 MB	18.48 MB	2019-12-25 10:57AM	2019-12-25 11:12AM	Android	—
24:18:1D:A3:3A:E9	Galaxy-S9	Guest	8.95 MB	220.27 MB	2019-12-26 10:46AM	2019-12-26 11:41AM	Android	SAMSUNG
2E:CE:A7:0D:87:D9	Galaxy-S10	Guest	142.89 KB	833 KB	2019-12-26 10:41AM	2019-12-26 10:46AM	Android	—
48:9D:D1:AE:B4:A1	Galaxy-A20	User	5.18 MB	44.29 MB	2019-12-25 10:57AM	2019-12-25 12:12PM	Android	—
4C:74:BF:97:B0:78	Huawei Mate X	Guest	10.1 MB	85.93 MB	2019-12-24 05:23PM	2019-12-26 11:46AM	—	—
88:11:96:D9:66:89	HUAWEI_Y7_Pri...	User	2.23 KB	2.68 KB	2019-12-24 05:57PM	2019-12-24 05:57PM	Android	HUAWEI
94:0E:6B:F8:3A:8D	HUAWEI_Mate_1...	Guest	2.13 KB	1.39 KB	2019-12-25 05:43PM	2019-12-25 05:43PM	Android	HUAWEI
A4:9B:4F:E2:7E:BC	HUAWEI_P30-e6...	User	—	—	2019-12-24 06:43PM	2019-12-24 06:43PM	Android	—
A8:34:6A:00:1A:C6	Galaxy-A50	Guest	17.03 MB	337.64 MB	2019-12-26 10:51AM	2019-12-26 11:46AM	Android	—

Total 15 | 10 /page | 1 | 2

Figure 88: Known Clients - Insight

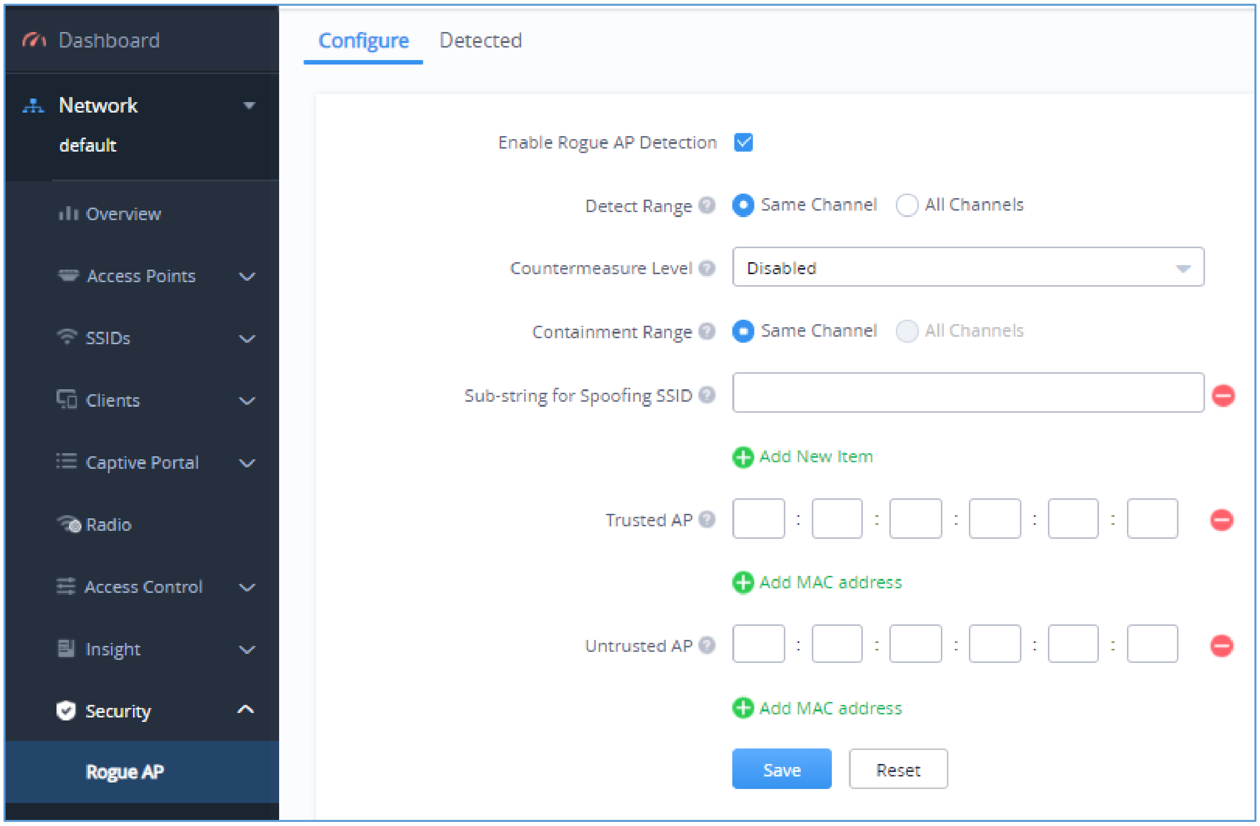
SECURITY

Rogue AP

GWN Cloud and GWN Manager offer the ability to prevent malicious intrusion to the network and increases the wireless security access of clients when introducing Rogue AP detection feature to the adopted / paired GWN76xx Wi-Fi access points. The detected APs will be listed with all the details under “Detected” section for further intervention.

Note: This feature is not supported in GWN7610/GWN7602.

Navigate to **Security ➔ Rogue AP** , The below figure shows the configuration page in order to enable Rogue AP detection.



Enable Rogue AP Detection ☑

Detect Range ● Same Channel ○ All Channels

Countermeasure Level: Disabled

Containment Range ● Same Channel ○ All Channels

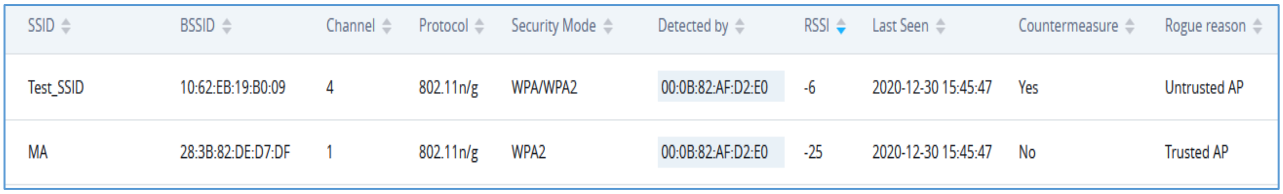
Sub-string for Spoofing SSID

Trusted AP

Untrusted AP

Figure 89: Rogue AP configuration page

The “**Detected**” page shows all the SSIDs within the Wi-Fi coverage of the adopted / paired, GWN76xx, including the APs that have been set as Trusted or Untrusted.



SSID	BSSID	Channel	Protocol	Security Mode	Detected by	RSSI	Last Seen	Countermeasure	Rogue reason
Test_SSID	10:62:EB:19:B0:09	4	802.11n/g	WPA/WPA2	00:0B:82:AF:D2:E0	-6	2020-12-30 15:45:47	Yes	Untrusted AP
MA	28:3B:82:DE:D7:DF	1	802.11n/g	WPA2	00:0B:82:AF:D2:E0	-25	2020-12-30 15:45:47	No	Trusted AP

Figure 90: Detected Trusted and Untrusted APs

Table 19: Rogue AP parameters description

Field	Description
Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect range	Specify the rogue AP detect range. • **Same channel:** AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication. • **All channels:** AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt. Default is Same Channel.
Countermeasure level	Countermeasures level specifies the type of attacks which will be suspected by the AP. Select different levels: • **High:** Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. • **Medium:** Untrusted BSSID, Illegal access without authentication, Illegal access. • **Low:** Untrusted BSSID, Illegal access without authentication. Default is Disabled.

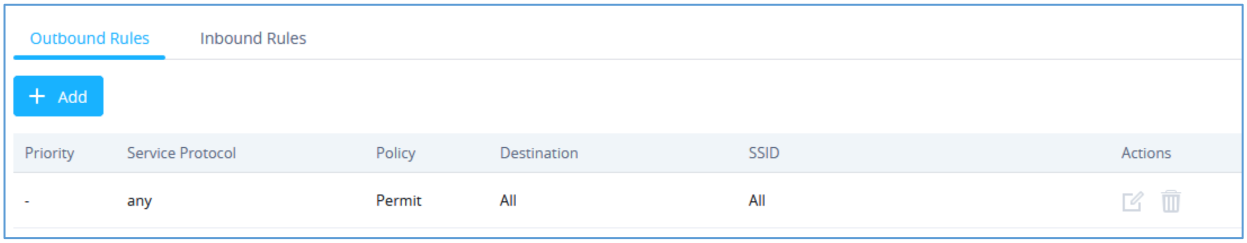
Containment Range	Specify the containment range: - **Same channel:** detect AP will countermeasure the APs in the same channel. - **All channels:** detect AP will countermeasure the APs in all channels at the cost of consuming of much AP performance. Default is Same Channel.
Sub-string for Spoofing SSID	The AP broadcasting SSID with the specified string will be classified as a Spoofing SSID.
Trusted AP	You can specify MAC address of the trusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as trusted AP, no countermeasures will be executed on it.
Untrusted AP	You can specify MAC address of the untrusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

Firewall

This section is located under to **Security ➔ Firewall** , it does allow users to control the outgoing and incoming traffic from clients connected to the adopted / paired GWN76xx Wi-Fi access points by manually setting up policies to either deny or permit the traffic based on protocol type and by specifying SSIDs and destinations.

Outbound Rules

Below figure shows the Outbound Rules configuration page, Click on Add to add outbound rules based on the parameters as described in the table.



Priority	Service Protocol	Policy	Destination	SSID	Actions
-	any	Permit	All	All	

Figure 91: Firewall Outbound Rules

Table 20: Firewall Outbound Rules parameters

Field	Description
Service Protocol	Select type of traffic to be affected by the outbound rule like ICMP, HTTP, HTTPS… or you may add another type of traffic when selecting Custom. When set to Custom, user could enter the following: **Protocol:** TCP or UDP **Port:** define the port used by this protocol.
Policy	Either select to Permit or Deny Outbound traffic.
Destination	Select either: • **Particular Domain:** enter FQDN of a destination. • **Particular IP:** IP address of destination. • **Particular Network:** Network IP address. • **All:** the rule will apply on all destinations.
SSID	Select one or multiple SSIDs to apply the rule on.

Inbound Rules

Click on Add to add inbound rules based on the parameters as described in the table.

Table 21: Firewall Inbound Rules parameters

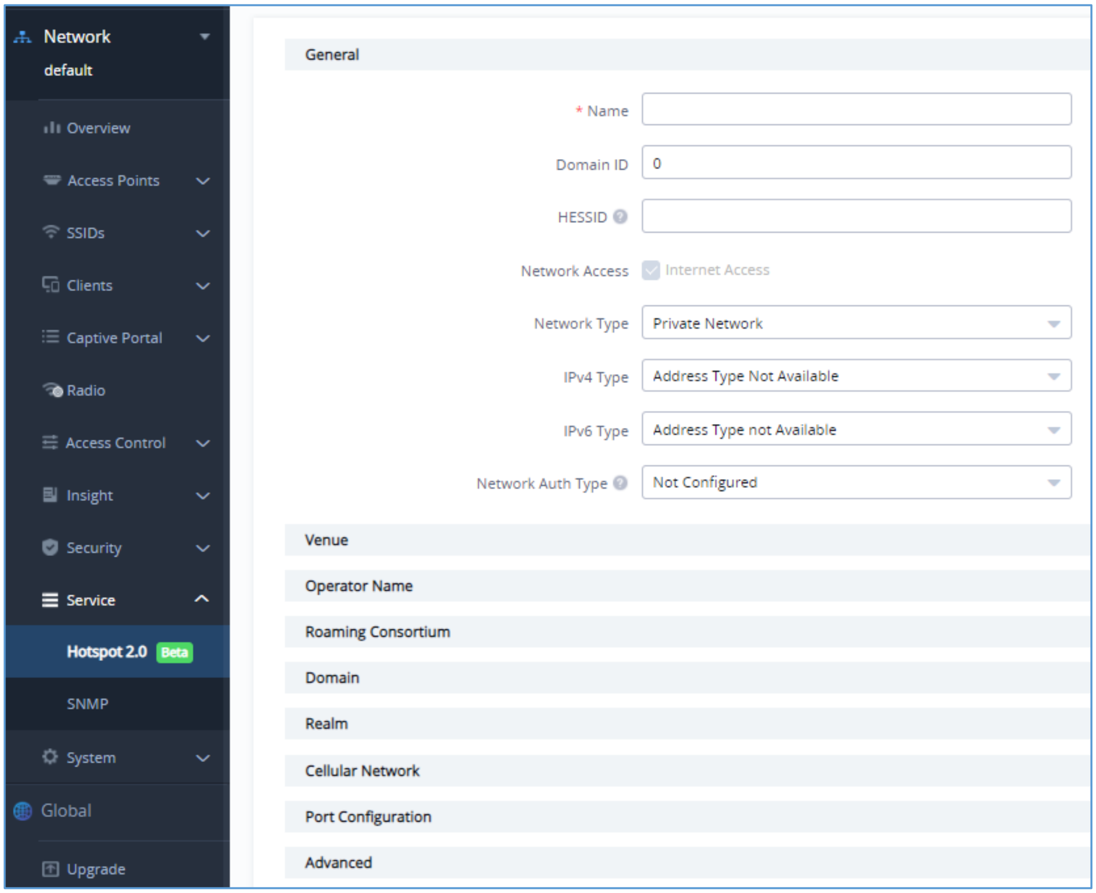
Field	Description
Service Protocol	Select type of traffic to be affected by the inbound rule like ICMP, HTTP, HTTPS… or you may add another type of traffic when selecting Custom. When set to Custom, user could enter the following: **Protocol:** TCP or UDP **Port:** define the port used by this protocol.
Policy	Either select to Permit or Deny inbound traffic.
Source	Select either: • **Particular IP:** IP address of source. • **Particular Network:** Network IP address. • **All:** the rule will apply on all destinations.

SERVICE

Hotspot 2.0

This section lists the configuration page for Hotspot 2.0. This technology allows mobile devices to automatically connect to available Passpoint-certified WiFi hotspots. This gives the device liberty to hop from one hotspot on a network to another without the need log in to each hotspot. This feature is currently a Beta.

Note: This is not supported in GWN7610/GWN7602.



General

* Name:
Domain ID: 0
HESSID:
Network Access: ☑ Internet Access
Network Type: Private Network
IPv4 Type: Address Type Not Available
IPv6 Type: Address Type not Available
Network Auth Type: Not Configured

Venue
Operator Name
Roaming Consortium
Domain
Realm
Cellular Network
Port Configuration
Advanced

Figure 92: Hotspot 2.0

Table 22: Hotspot 2.0 parameters description

General	
Field	**Description**

Name	Set name of the hotspot.
Domain ID	Set the Domain ID.
HESSID	Configure the Homogenous Extended Service Set Identifier information for Hotspot2.0. This value must be consistent with the BSSID of an AP to identify the AP set that provides the same network access service. The format is H:H:H:H:H:H, where H is a 2-digit hexadecimal number.
Network Access	Enabled or disable internet access.
Network Type	Select network type: • Private network • Private network with guest access • Chargeable public network • Free public network • Personal device network • Emergency services only network • Test or experimental • Wildcard
IPv4 Type	Select IPv4 Type: • Address type not available • Public IPv4 address available • Port-restricted IPv4 address available • Single NATed private IPv4 address available • Double NATed private IPv4 address available • Port-restricted IPv4 address and single NATed IPv4 address available • Port-restricted IPv4 address and double NATed IPv4 address available • Availability of the address type not known
IPv6 Type	Select IPv4 Type: • Address type not available • Address type available • Availability of the address type not known
Network Auth Type	Configure the Network authentication type to help users find and select the right network. Select either: • Acceptance of terms and conditions

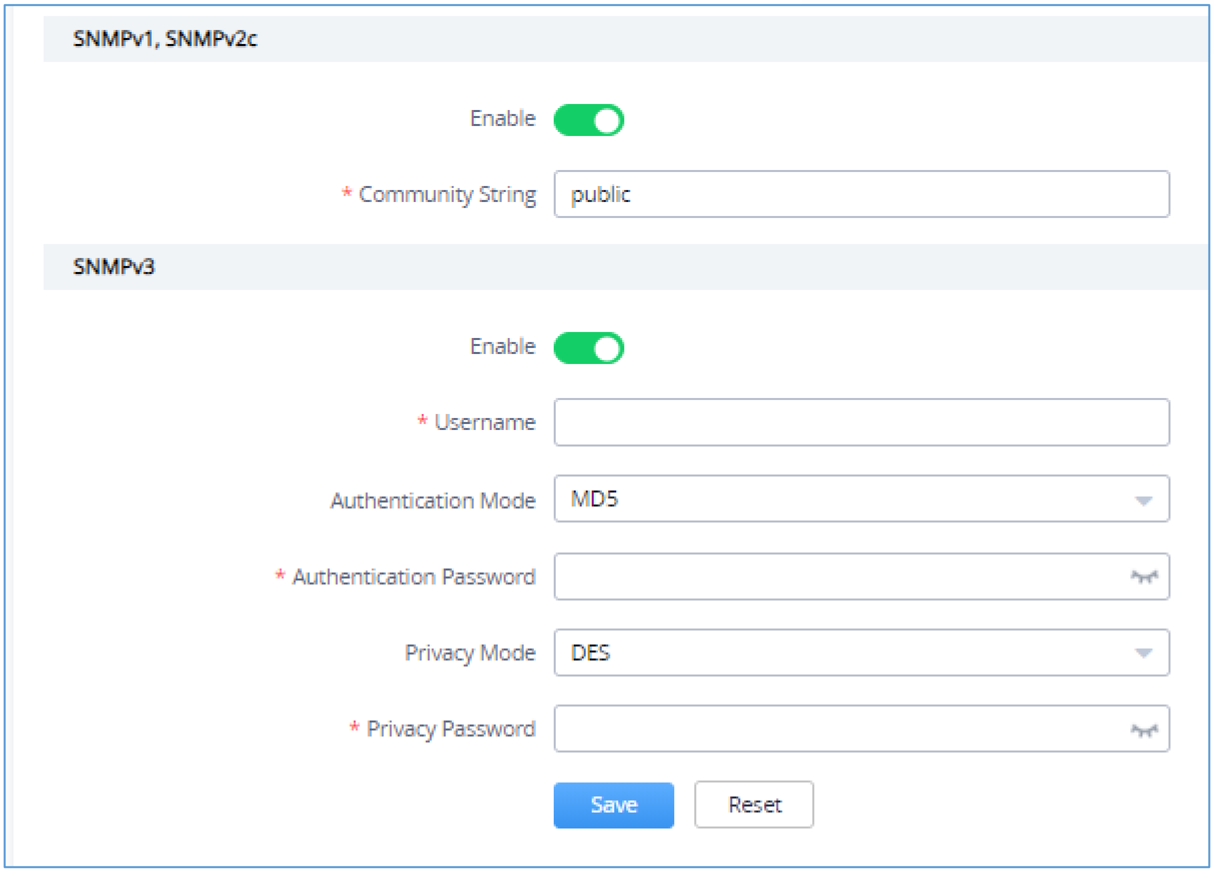
	• On-line enrollment supported • http/https redirection • DNS redirection • Not configured
Venue	
Venue Group	Select the Venue Group type: • Unspecified • Assembly • Business • Educational • Factory • Institutional • Mercantile • Residential • Storage • Utility • Vehicular • Outdoor
Venue Type	Select the Venue type, which will depend on the Venue Group.
Language Code	Select the language.
Venue Name	Set the Venue name.
Operator Name	
Language Code	Select the language.
Operator Name	Set the Operator name.
Roaming Consortium	
Roaming Consortium Name	Configure the Roaming Consortium Name to identify network operators. The format is H-H-H or H-H-H-H-H, where H is a 2-digit hexadecimal number.
Domain	
Domain	Enter the domain name.
Realm	

Realm	Select the EAP Method: EAP-TLS, EAP-SIM, EAP-TTLS, EAP-AKA and EAP-AKA'.
Cellular Network Information	
Cellular Network Information	Enter the Name, Country Code and Network Code.
Port Configuration	
IP Protocol	Configure the protocol type: ICMP, TCP, UDP or ESP.
Port Number	Set the protocol port.
Port Status	Set the port status to either: Open, Close or Unknown.
Advanced	
WAN Link Status	Set the WAN Link Status to either: Not configured, Link-up, Link-down or Link-test.
WAN Downlink Speed	Set Download speed.
WAN Uplink Speed	Set Upload speed.
GAS Fragmentation Limit	Set GAS fragmentation limit. Default is 1400.
GAS Comeback Delay	Set GAS comeback delay. Default is 0.
Disable Downstream Group-Addressed Forwarding	When this option is disabled, it means the DGAF is enabled, the AP will forward all downlink broadcast ARP messages and wireless group broadcasts. When this option is anabled, the DGAF function is disabled, the AP will discard all downlink broadcast ARP messages and wireless group broadcasts. Disable DGAF function to prevent attackers from using the vulnerability of all clients in the same BSS using the same Group Temporal Key (GTK) to forge Group address frames and then attack the clients.

SNMP

This section lists the SNMPv1, SNMPv2c, and SNMPv3 options available to integrate the adopted / paired GWN76xx Wi-Fi access points with enterprise monitoring systems.

Users can enable SNMP feature under **Service ➔ SNMP**



SNMPv1, SNMPv2c

Enable: on

* Community String: public

SNMPv3

Enable: on

* Username:

Authentication Mode: MD5

* Authentication Password:

Privacy Mode: DES

* Privacy Password:

Figure 93: SNMP configuration page

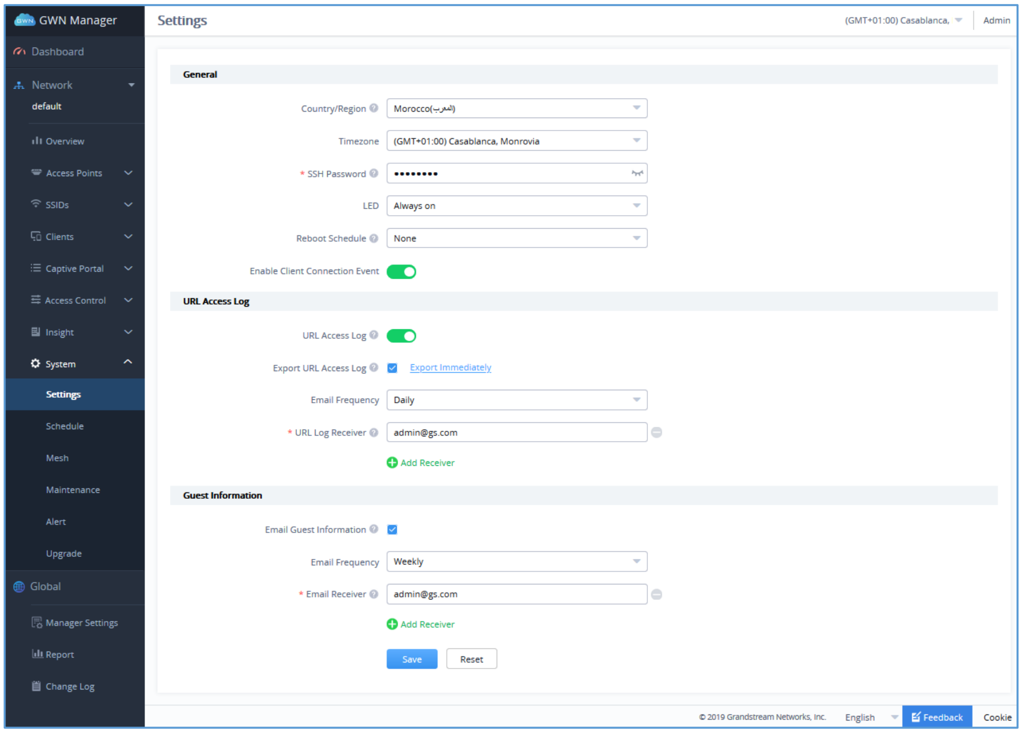
Table 23: SNMP parameters description

Field	Description
Enable	Enable SNMPv1/SNMPv2c.
Community String	Enter the SNMP Community string.
Enable	Enable SNMPv3.
Username	Enter the SNMPv3 username.
Authentication Mode	Set the Authentication mode to: either MD5 or SHA.
Authentication password	Enter the SNMPv3 authentication password.
Privacy Mode	Set the Privacy mode to: either AES128 or DES.
Privacy password	Enter the privacy password.

SYSTEM

Settings

Settings page allows Country and Time configuration, reboot schedule and enabling URL log activity.



Settings

General

Country/Region: Morocco(المغرب)

Timezone: (GMT+01:00) Casablanca, Monrovia

* SSH Password: ••••••••

LED: Always on

Reboot Schedule: None

Enable Client Connection Event: ON

URL Access Log

URL Access Log: ON

Export URL Access Log: ☑ Export Immediately

Email Frequency: Daily

* URL Log Receiver: admin@gs.com

Guest Information

Email Guest Information: ☑

Email Frequency: Weekly

* Email Receiver: admin@gs.com

© 2019 Grandstream Networks, Inc.

Figure 94 :System Settings

Table 24: Settings

Field	Description
Country/Region	Select the country or region from the drop-down list. This can affect the number of channels depending on the country standards.
Time Zone	Configure time zone for GWN APs. Please reboot the device to take effect.
SSH Password	Set SSH Password for GWN APs.
LED	Select whether to always turn ON or OFF the LEDs on the APs or apply a schedule for this function.
LED Schedule	Select a schedule that will be applying to LEDs, dictating when they will be ON and OFF.

Reboot Schedule	Once scheduled, the current network will not work for a while during the scheduled period.
Enable client connection event	When enabled, then Client connects/disconnects events are listed under Access Points→Status→AP details page.
URL Access Log	Once enabled, the GWN Cloud will record the URL access log from the clients. **Note:** GWN7610 does not support this feature.
Export URL Access Log	Once enabled, the Cloud Server will periodically send out the log download link to the configured URL Log Received email. Users can click on "Export Immediately" and then specify the time range of the URL Access Log to be exported; range is 1 to 30 last days.
Email Frequency	Specify the Email frequency to be generated either on daily basis, weekly or monthly.
URL Log Receiver	Configure the Email address of the URL Log Receiver.
Email Guest Information	Once enabled, cloud server will periodically send out the guest information download link as configured.
Email Frequency	Specify the Email frequency to be generated either on daily basis, weekly or monthly.
URL Log Receiver	Configure the Email address of the URL Log Receiver.

URL Access Log

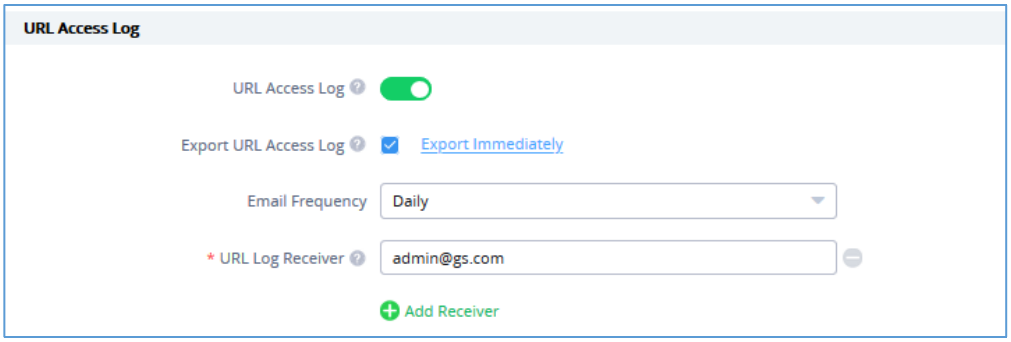
Administrators can easily configure the platform to record, monitor and maintain a log of all the websites visited by the clients connected to the paired GWN76xx access points.

The platform System will send these logs via Email to the configured Log Receiver in a form of downloadable link providing a CSV file format containing all the websites logs visited for each client during the defined period (daily, weekly or monthly basis).

In order to enable this feature, follow below steps:

1. Go under **"System → Settings"** and enable URL Access Log field, this will configure the GWN Manager System to start recording the websites logs visited by the clients.
2. Enable Export URL Access Log.

3. Administrators can choose to set the Email Frequency to be generated either on a daily, weekly or monthly basis.
4. Configure the URL Log Receiver Email.



URL Access Log

URL Access Log: on

Export URL Access Log: ☑ Export Immediately

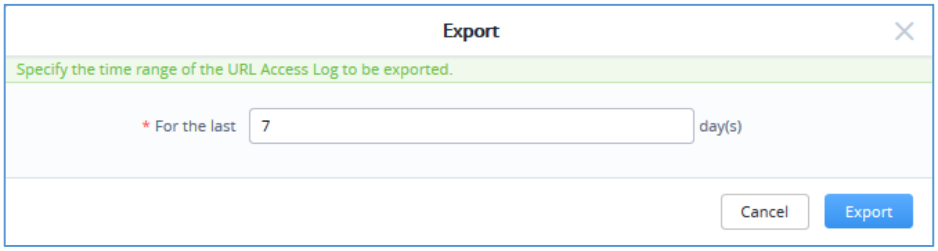
Email Frequency: Daily

* URL Log Receiver: admin@gs.com

Figure 95: URL Access Log Settings

In this example, the administrator will start receiving, on a daily basis, an Email containing a downloadable link providing a CSV file containing the websites visited by the clients during the last day.

Users can click on Export Immediately , and then specify the time range of the URL Access Log during the last (1 – 30) days to be exported immediately.



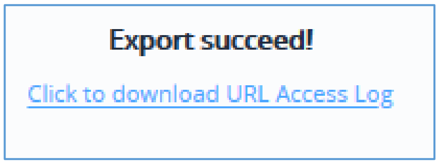
Export

Specify the time range of the URL Access Log to be exported.

* For the last 7 day(s)

Figure 96: Export Immediately

5. Click Export and notice the success confirmation message:



Export succeed!

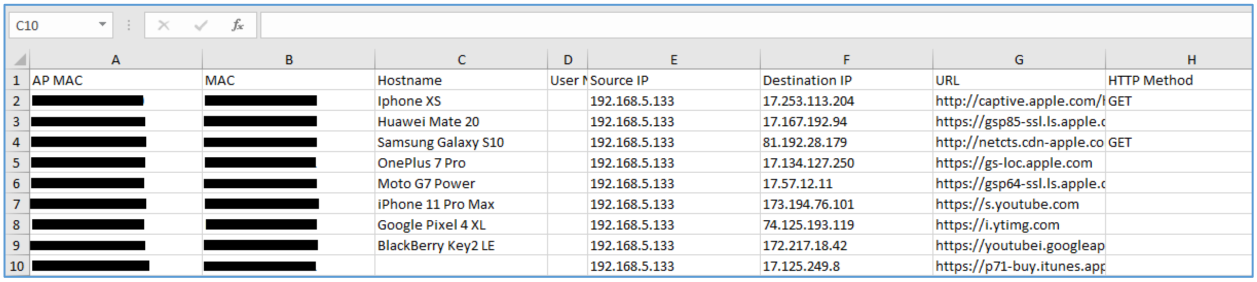
Click to download URL Access Log

Figure 97: Export Succeed

6. Click the highlighted link to Download the log file and save it locally.

Once downloaded, administrators will have a CSV file tracking the Internet activity for all the clients connected to the paired GWN76xx access points.

The CSV file will contain columns displaying the AP MAC address, client's hostname as well the device MAC address, the Source and Destination IP, the URL logs, the HTTP Method (GET/POST) and the time of request.



C10

	A	B	C	D	E	F	G	H
1	AP MAC	MAC	Hostname	User N	Source IP	Destination IP	URL	HTTP Method
2	[redacted]	[redacted]	Iphone XS		192.168.5.133	17.253.113.204	http://captive.apple.com/l	GET
3	[redacted]	[redacted]	Huawei Mate 20		192.168.5.133	17.167.192.94	https://gsp85-ssl.ls.apple.c	
4	[redacted]	[redacted]	Samsung Galaxy S10		192.168.5.133	81.192.28.179	http://netcts.cdn-apple.co	GET
5	[redacted]	[redacted]	OnePlus 7 Pro		192.168.5.133	17.134.127.250	https://gs-loc.apple.com	
6	[redacted]	[redacted]	Moto G7 Power		192.168.5.133	17.57.12.11	https://gsp64-ssl.ls.apple.c	
7	[redacted]	[redacted]	iPhone 11 Pro Max		192.168.5.133	173.194.76.101	https://s.youtube.com	
8	[redacted]	[redacted]	Google Pixel 4 XL		192.168.5.133	74.125.193.119	https://i.ytimg.com	
9	[redacted]	[redacted]	BlackBerry Key2 LE		192.168.5.133	172.217.18.42	https://youtubei.googleap	
10	[redacted]	[redacted]			192.168.5.133	17.125.249.8	https://p71-buy.itunes.app	

Figure 98: URL Access Log- CSV file example

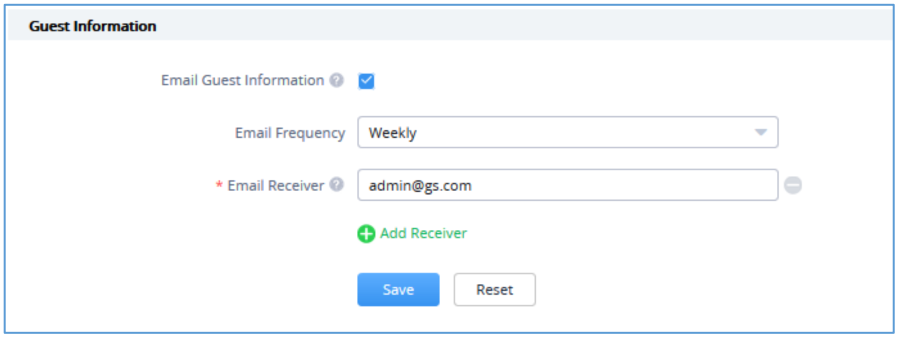
Notes:

- Currently, GWN7610 doesn't support this feature.
- The Platform Database will keep storage of reports for 30 days, after that, they will be automatically erased from the system.

Guest Information

In order to enable this feature, follow below steps:

1. Go under **"System → Settings"** and enable Guest Information field.
2. Choose to set the Email Frequency to be generated either on a daily, weekly or monthly basis.
3. Configure the Email Receiver.



Guest Information

Email Guest Information ☑

Email Frequency: Weekly

* Email Receiver: admin@gs.com

Figure 99: Guest Information

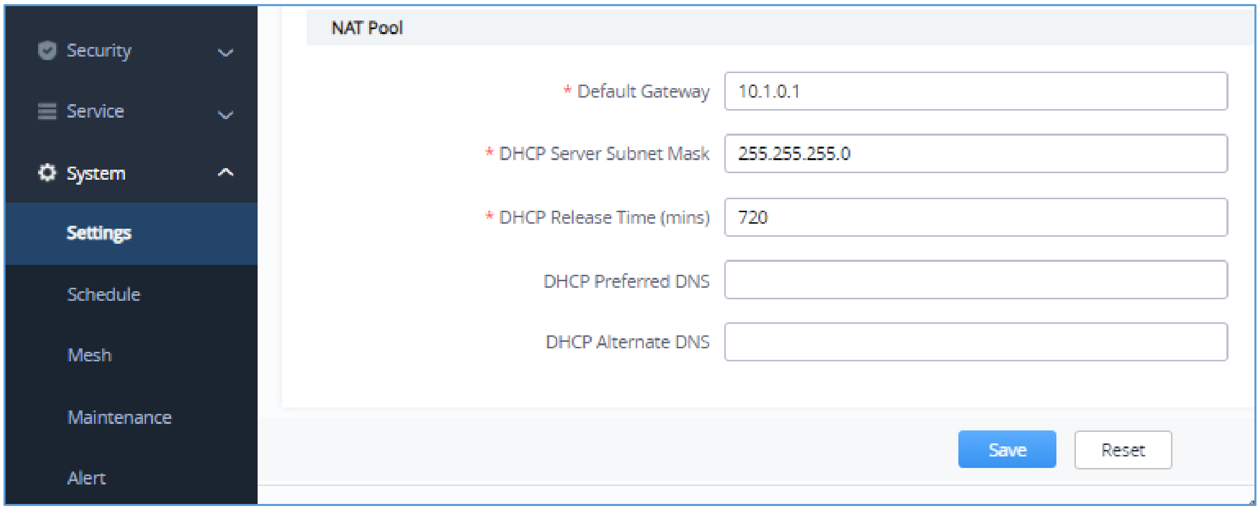
NAT Pool

Users can use this feature in order to set an address Pool from which the clients that are connected to the adopted / paired GWN76xx will acquire their IP address in that way the access point will act as a light weight router.

Notes:

- This option cannot be enabled when **Client Assignment IP** *is set to Bridge mode.*
- This option is not supported in GWN7610.

Navigate to **System → Settings → NAT Pool**, in order to configure the Gateway, DHCP Server Subnet Mask, DHCP Lease Time and DHCP Preferred/Alternate DNS



NAT Pool

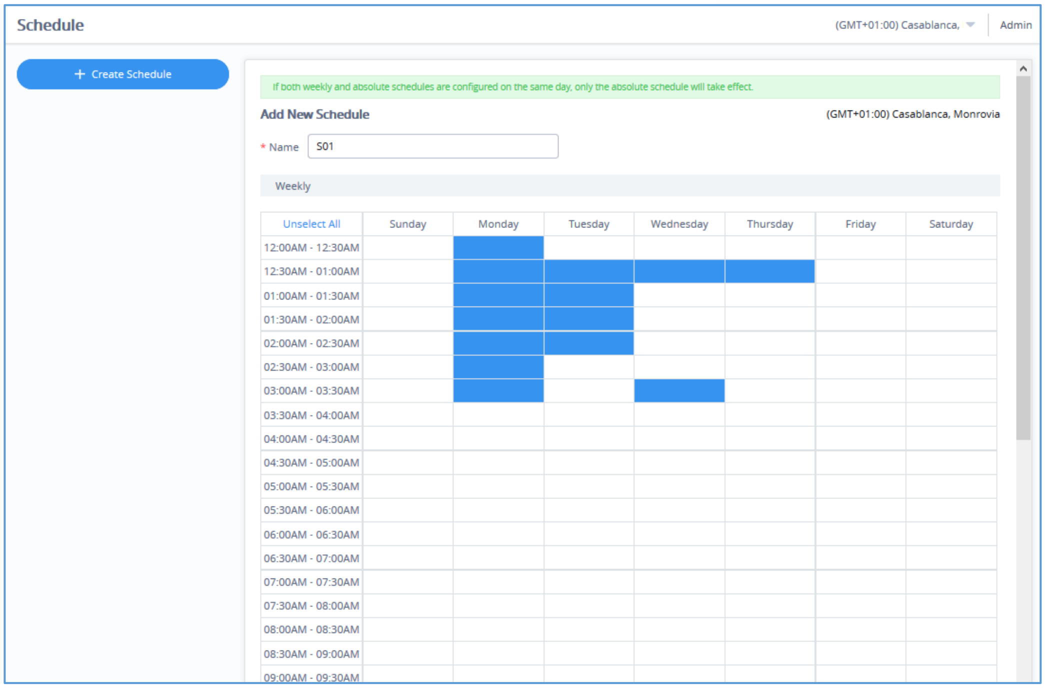
* Default Gateway	10.1.0.1
* DHCP Server Subnet Mask	255.255.255.0
* DHCP Release Time (mins)	720
DHCP Preferred DNS	
DHCP Alternate DNS	

Figure 100: NAT Pool configuration

Schedule

In order to configure a new schedule, follow below steps:

1. Go under "System → Schedule" and click on



Schedule

(GMT+01:00) Casablanca, | Admin

If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.

Add New Schedule

(GMT+01:00) Casablanca, Monrovia

* Name: S01

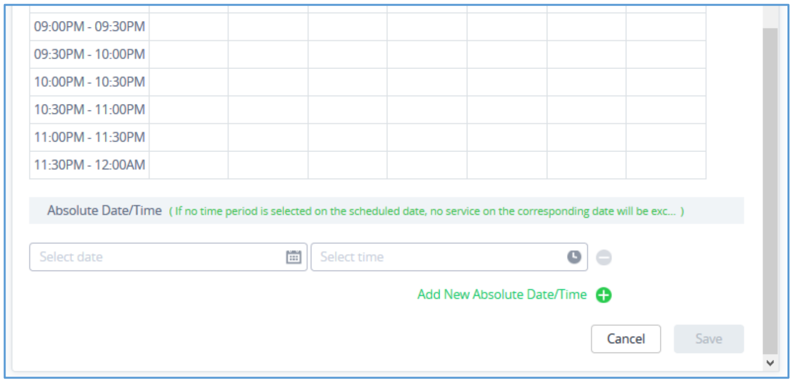
Weekly

Unselect All	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
12:00AM - 12:30AM		■					
12:30AM - 01:00AM		■	■	■	■		
01:00AM - 01:30AM		■	■				
01:30AM - 02:00AM		■	■				
02:00AM - 02:30AM		■	■				
02:30AM - 03:00AM		■					
03:00AM - 03:30AM		■		■			
03:30AM - 04:00AM							
04:00AM - 04:30AM							
04:30AM - 05:00AM							
05:00AM - 05:30AM							
05:30AM - 06:00AM							
06:00AM - 06:30AM							
06:30AM - 07:00AM							
07:00AM - 07:30AM							
07:30AM - 08:00AM							
08:00AM - 08:30AM							
08:30AM - 09:00AM							
09:00AM - 09:30AM							

Figure 101: Create New Schedule- Weekly

2. Select the periods on each day that will be included on the schedule and enter a name for the schedule (ex: S01).

3. Users can choose to set weekly schedule or absolute schedule (for specific days for example), and if both weekly schedule and absolute schedules are configured on the same day then the absolute schedule will take effect and the weekly program will be cancelled for that specific date.



09:00PM - 09:30PM							
09:30PM - 10:00PM							
10:00PM - 10:30PM							
10:30PM - 11:00PM							
11:00PM - 11:30PM							
11:30PM - 12:00AM							

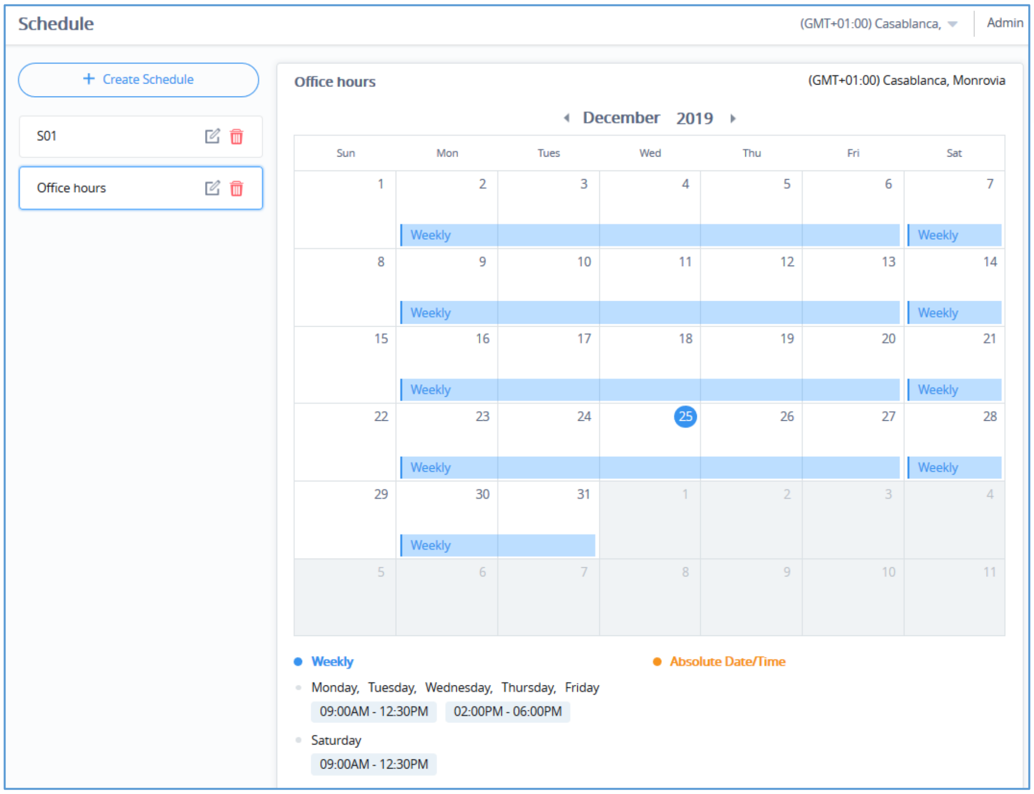
Absolute Date/Time (If no time period is selected on the scheduled date, no service on the corresponding date will be exc...)

Select date | Select time

Figure 102: Create New Schedule- Absolute

4. Once the schedule periods are selected, click on Save to save the schedule.

The list of created schedules will be displayed as shown on the figure below. With the possibility to edit or delete each schedule:



Schedule (GMT+01:00) Casablanca, Admin

S01

Office hours

Office hours (GMT+01:00) Casablanca, Monrovia

December 2019

Sun	Mon	Tues	Wed	Thu	Fri	Sat
1	2 Weekly	3	4	5	6	7 Weekly
8	9 Weekly	10	11	12	13	14 Weekly
15	16 Weekly	17	18	19	20	21 Weekly
22	23 Weekly	24	25	26	27	28 Weekly
29	30 Weekly	31	1	2	3	4
5	6	7	8	9	10	11

● Weekly ● Absolute Date/Time

Monday, Tuesday, Wednesday, Thursday, Friday
09:00AM - 12:30PM 02:00PM - 06:00PM

Saturday
09:00AM - 12:30PM

Figure 103: Schedules List

Mesh

Wireless Mesh Network is a wireless extension of the traditional wired network using multiple access points connected through wireless links to areas where wired access is not an option while also expanding the coverage of the WLAN network.

In the traditional WLAN network, the uplink of the AP is a wired network (usually an Ethernet Link):

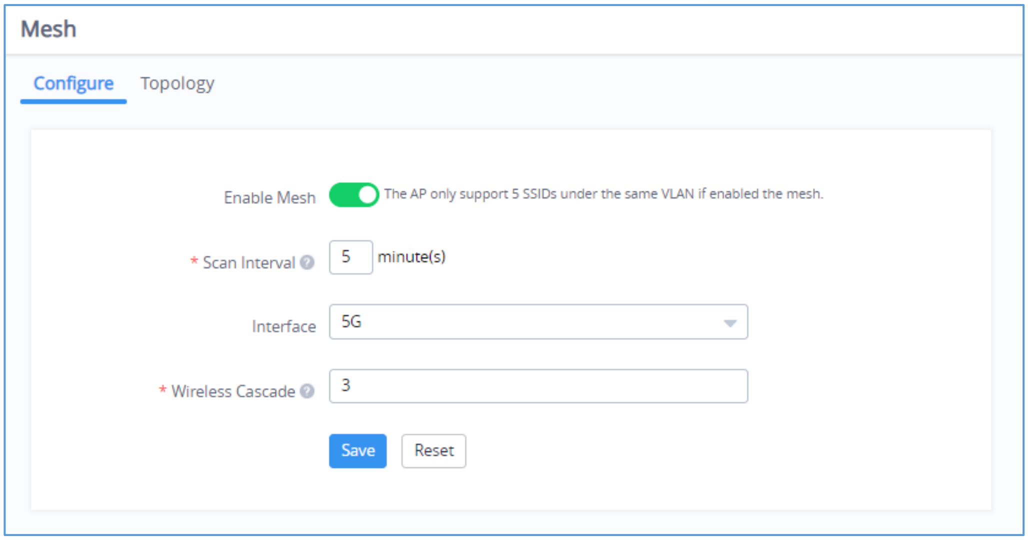
- The advantages of a wired network are security, anti-interference and stable bandwidth.
- The disadvantages are high construction cost, long period of planning and deployment, and difficulty of change in case a modification is needed.

However, these are precisely the advantages of wireless networks. As a result, Wireless Mesh Network is an effective complement of wired network.

In addition, Mesh networking provides a mechanism for network redundancy. When an abnormality occurs in a wired network, an AP suffering the uplink failure can keep the data service continuity through its Mesh network.

For more details about the GWN Mesh Network feature, please Check the document from below link: *http://www.grandstream.com/sites/default/files/Resources/GWN76XX_Mesh_Network.pdf*

Users can setup some Mesh Network parameters under the menu "**System → Mesh**", as shown on the figure below:


Mesh

Enable Mesh ● The AP only support 5 SSIDs under the same VLAN if enabled the mesh.

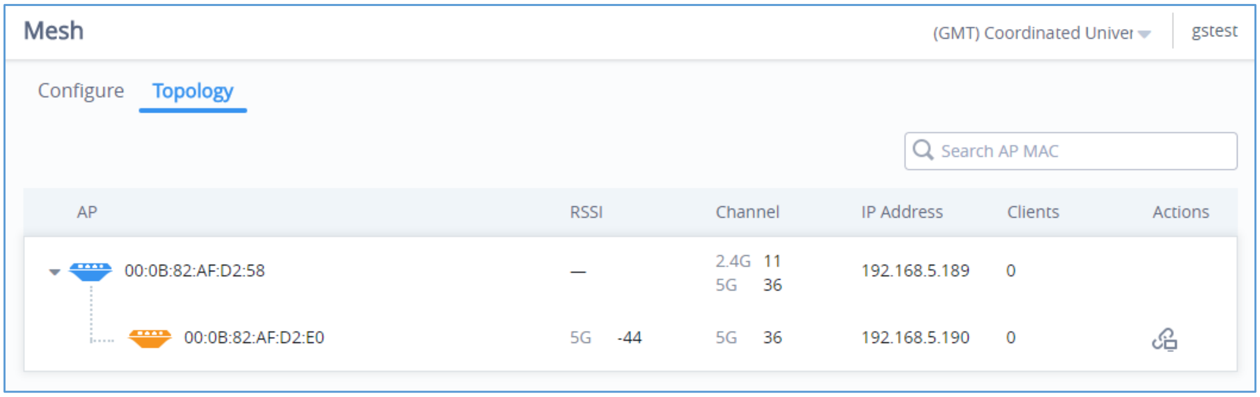
* Scan Interval: 5 minute(s)

Interface: 5G

* Wireless Cascade: 3

Figure 104: Mesh Settings

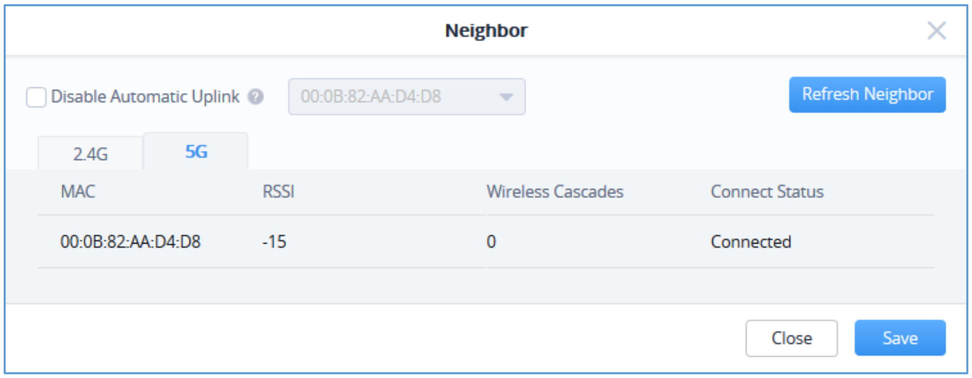
Also, it's possible to visualize the Mesh topology by going under the **Topology** Tab.


Mesh

AP	RSSI	Channel	IP Address	Clients	Actions
00:0B:82:AF:D2:58	—	2.4G 11 5G 36	192.168.5.189	0	
00:0B:82:AF:D2:E0	5G -44	5G 36	192.168.5.190	0	

Figure 105: Mesh Topology

- Click To check the AP Neighbors:
- By checking option **"Disable Automatic Uplink",** the uplink of this AP will need to be assigned manually.
- Select 2.4G or 5G to display the AP Neighbors information by frequency band. Available information: MAC, RSSI, Wireless Cascades and Connect Status.
- Click Refresh Neighbor to update information



MAC	RSSI	Wireless Cascades	Connect Status
00:0B:82:AA:D4:D8	-15	0	Connected

Figure 106: Neighbor

Maintenance

The Maintenance Web page allows to configure Syslog settings in order to have APs sending log messages to your debugging syslog server.

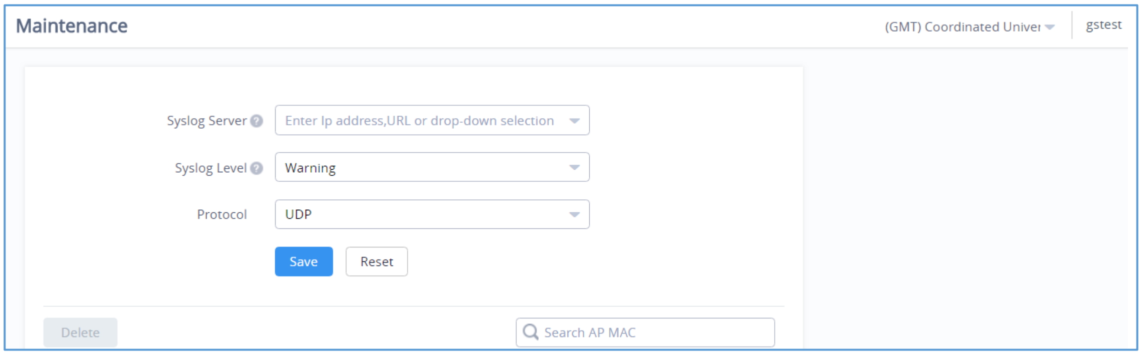


Figure 107: Maintenance/Syslog Settings

Table 25: Maintenance

Field	Description
Syslog Server	Enter the IP address or URL of Syslog server.
Syslog Level	Select the level of Syslog, 5 levels are available: **None, Emergency, Alert, Critical, Error, Warning** and **Notice**.
Protocol	Select which protocol will be used for transport (UDP or TCP).

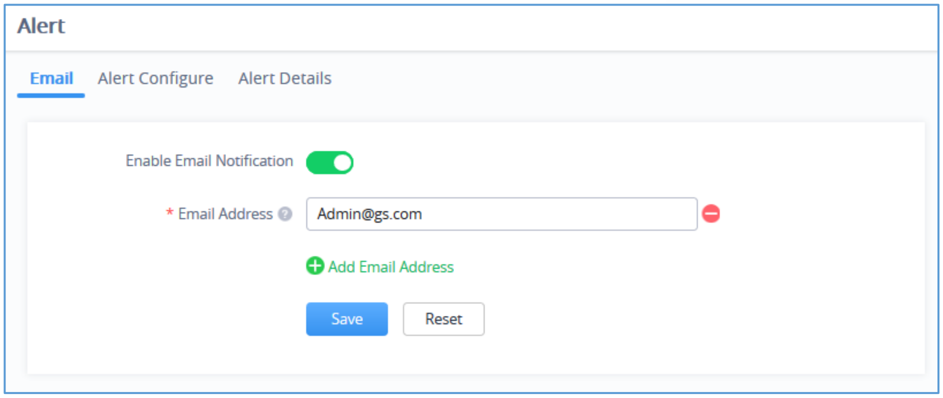
Alert

The Alert Web page provides configuration for Alert settings. The first tab is to setup the email address of admin(s) which will be receiving alert events notifications.

Table 26: Alert

Field	Description
Email	Enable this feature to receive alerts via email
Alert configure	Specify the modules to monitor, there are seven modules: Memory Usage, CPU Usage, Network Throughput, AP Throughput, SSID Throughput, Firmware Upgrade, AP Offline

Alert details	Displays the alerts in the web UI of GWN Manager.



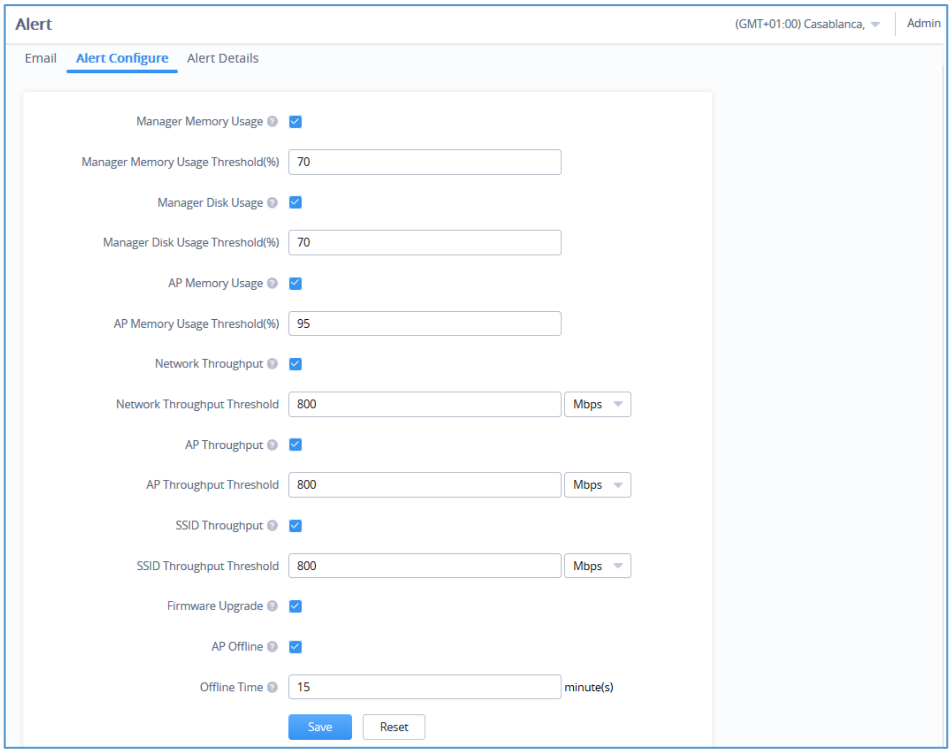
Alert

Enable Email Notification: on

* Email Address: Admin@gs.com

Figure 108: Alert Email

Next Tab is to enabled/disable specific alert events as shown on the figure below:



Alert

Manager Memory Usage ☑

Manager Memory Usage Threshold(%): 70

Manager Disk Usage ☑

Manager Disk Usage Threshold(%): 70

AP Memory Usage ☑

AP Memory Usage Threshold(%): 95

Network Throughput ☑

Network Throughput Threshold: 800 Mbps

AP Throughput ☑

AP Throughput Threshold: 800 Mbps

SSID Throughput ☑

SSID Throughput Threshold: 800 Mbps

Firmware Upgrade ☑

AP Offline ☑

Offline Time: 15 minute(s)

Figure 109: Alert Events List

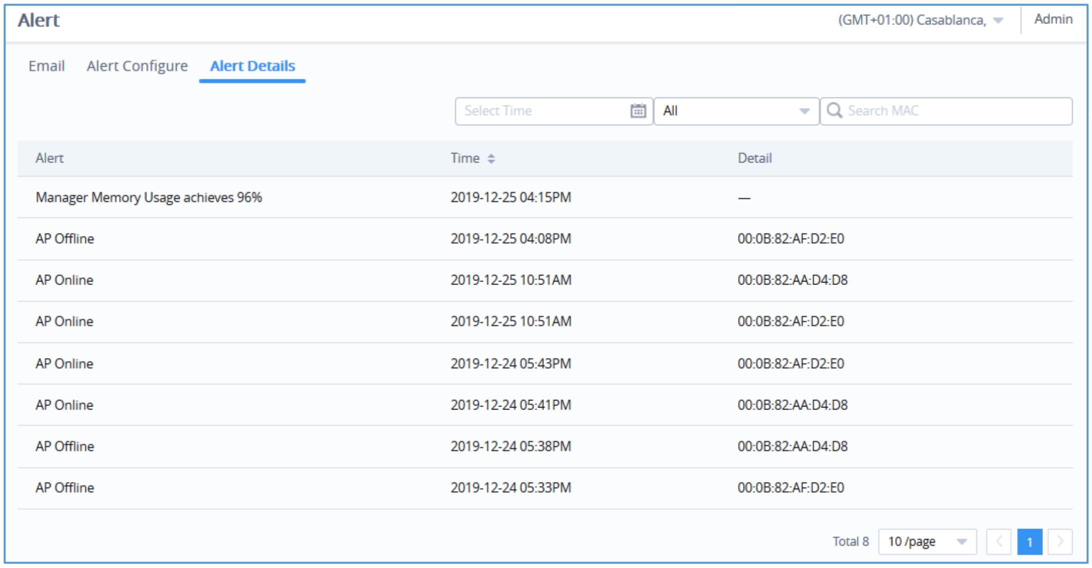
The next Table details the Alert configuration parameters:

Table 27: Alert configuration parameters

Manager Memory Usage Threshold(%)	**(GWN Manager** only**)** Once enabled, system will generate an Alert when Manager Memory Usage reaches the configured threshold [1-100].

Manager Disk Usage Threshold(%)	**(GWN Manager** only**)** Once enabled, system will generate an Alert when Manager Disk Usage reaches the configured threshold [1-100].
AP Memory Usage Threshold(%)	Once enabled, system will generate an Alert when AP memory usage reaches the configured threshold [1-100].
Network Throughput Threshold	Once enabled, system will generate an Alert when network throughput reaches the configured threshold [1-999].
AP Throughput Threshold	Once enabled, system will generate an Alert when AP throughput reaches the configured threshold [1-999].
SSID Throughput Threshold	Once enabled, system will generate an Alert when SSID throughput reaches the configured threshold [1-999].
Firmware Upgrade	Once enabled, system will generate an Alert when AP starts or finishes upgrade.
AP Offline	Once enabled, system will generate an Alert when the AP goes online or offline.
Offline Time	Specify the tolerance time of AP offline alert, manager will generate an alert if the AP keeps offline for the specified time period.

The last tab is to display the alert events that have occurred on the managed system as shown below:



Alert	Time	Detail
Manager Memory Usage achieves 96%	2019-12-25 04:15PM	—
AP Offline	2019-12-25 04:08PM	00:0B:82:AF:D2:E0
AP Online	2019-12-25 10:51AM	00:0B:82:AA:D4:D8
AP Online	2019-12-25 10:51AM	00:0B:82:AF:D2:E0
AP Online	2019-12-24 05:43PM	00:0B:82:AF:D2:E0
AP Online	2019-12-24 05:41PM	00:0B:82:AA:D4:D8
AP Offline	2019-12-24 05:38PM	00:0B:82:AA:D4:D8
AP Offline	2019-12-24 05:33PM	00:0B:82:AF:D2:E0

Figure 110: Alert Details

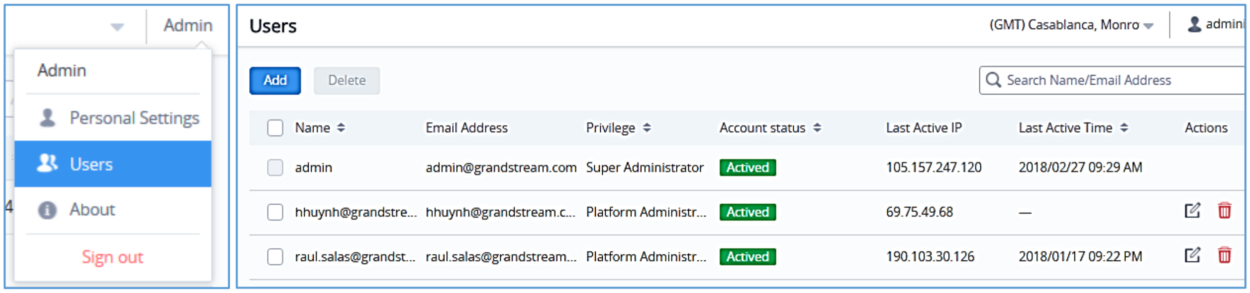
USER MANAGEMENT

User Management allows the administrator to create multiple accounts for different administrators or users to login to the platform. There are four different access levels to monitor and manage GWN Management Platforms:

- Super administrator
- Platform administrator
- Network administrator
- Guest editor

Add New Users

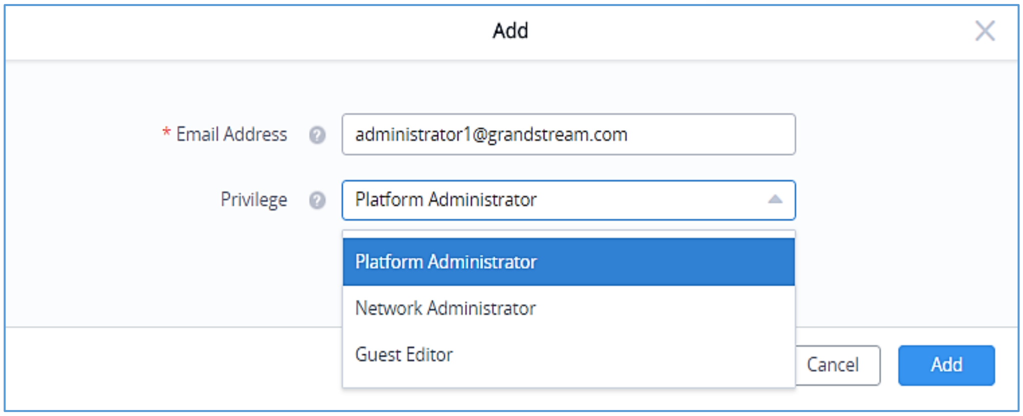
To list all the users managing an account, Click on **username** from the top right corner → **Users**



□	Name	Email Address	Privilege	Account status	Last Active IP	Last Active Time	Actions
□	admin	admin@grandstream.com	Super Administrator	Actived	105.157.247.120	2018/02/27 09:29 AM	
□	hhuynh@grandstre...	hhuynh@grandstream.c...	Platform Administr...	Actived	69.75.49.68	—	✎ 🗑
□	raul.salas@grandst...	raul.salas@grandstream...	Platform Administr...	Actived	190.103.30.126	2018/01/17 09:22 PM	✎ 🗑

Figure 111 : Users List

To add a new user, click on Add button then enter the email address and select the privilege to assign to the new user.

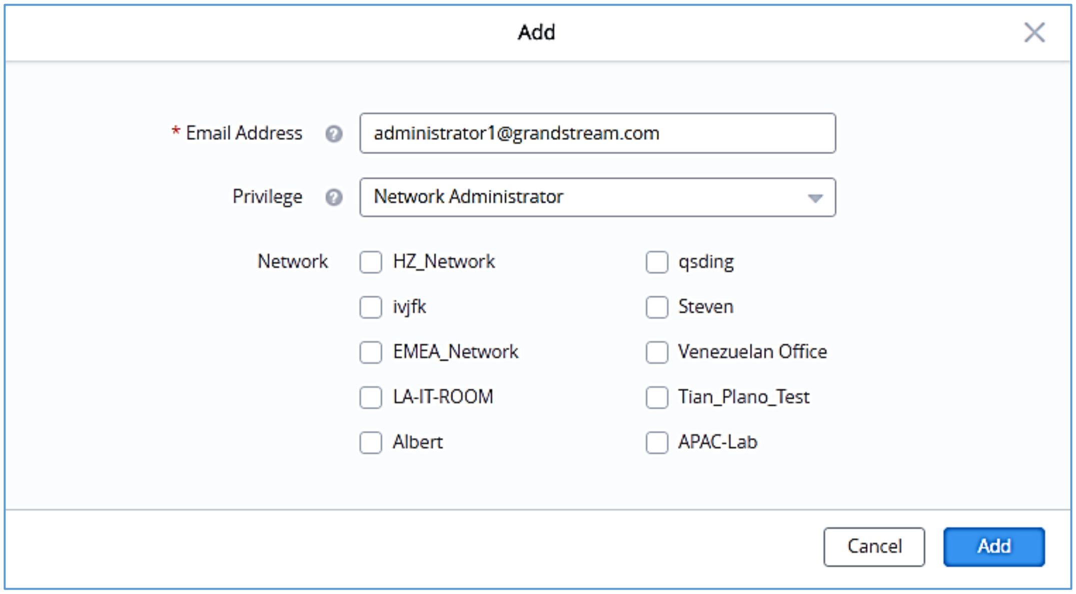


Add

* Email Address: administrator1@grandstream.com

Privilege: Platform Administrator

Figure 112 : Add New "Platform Administrator" User



Add

* Email Address: administrator1@grandstream.com

Privilege: Network Administrator

Network:
□ HZ_Network
□ qsding
□ ivjfk
□ Steven
□ EMEA_Network
□ Venezuelan Office
□ LA-IT-ROOM
□ Tian_Plano_Test
□ Albert
□ APAC-Lab

Figure 113 : Add "New Network Administrator" User

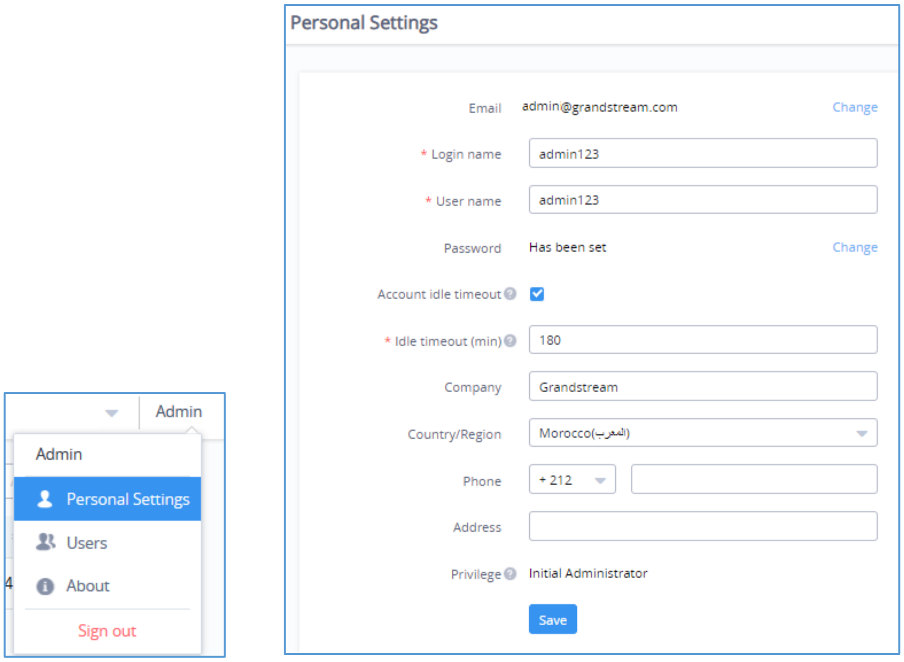
Note: When selecting privilege "Network Administrator" or "Guest Editor", the networks that will be monitored by this user should be selected, the new user will have access to those networks only.

User Privilege levels

Super Administrator

The Super administrator is an admin with top authority, using this privilege users can create/delete accounts with any privilege level. Each account has a unique Super Administrator which is created automatically when signing in.

To edit Super Administrator account, click on its name from the top right corner → Click on **Personal Settings** a new page displaying the administrator details will be displayed.



Personal Settings

Email admin@grandstream.com Change

* Login name admin123

* User name admin123

Password Has been set Change

Account idle timeout ☑

* Idle timeout (min) 180

Company Grandstream

Country/Region Morocco(المغرب)

Phone + 212

Address

Privilege Initial Administrator

Save

Figure 114 : Edit Super Administrator Account

Table 28: Super Administrator Account

Field	Description
Email	The email address of the Super Administrator. Click on **change** to change this email address
Login name	Username used for login authentication
Username	This is the name that will be displayed on the top right corner of the web page when login as super administrator
Password	Password used for login authentication
Account Idle timeout	Once enabled, the administrators will be logged out automatically after being idle for the specified time. This parameter will not take effect until the account login at the next time.
Idle timeout (min)	Specify the idle timeout, please enter an integer from 5 to 1440.
Company	Enter the company name

Country/Region	Select the country/region from the list
Phone	Enter the phone number
Address	Enter the address
Multi-Factor Safety Authentication	**(GWN Manager** only**)** Enable/Disable Multi-Factor Safety Authentication.
Privilege	Displays the type of privileges that the user has

Platform Administrator

Platform administrator is the second highest level, users with this privilege can create, delete all users with the same privilege or lower, in other words a platform administrator can create, delete, or edit other platform administrators, network administrators and guest editors.

Network Administrator

A network administrator is the third user privilege level, he can edit the networks assigned to him, and create or delete Guest editor belonging to the network he owns.

Guest Editor

This is the lowest privilege level, a guest editor can only view and edit/monitor captive portal, and voucher page within his network.

Edit User Settings

Changing Password

To Edit the user password, access the user account settings by clicking on his username from the top right corner of the page, then click on **Change** next to the password field, a new web page will be displayed, enter the old password, then the new one, confirm it, and finally submit the changes.

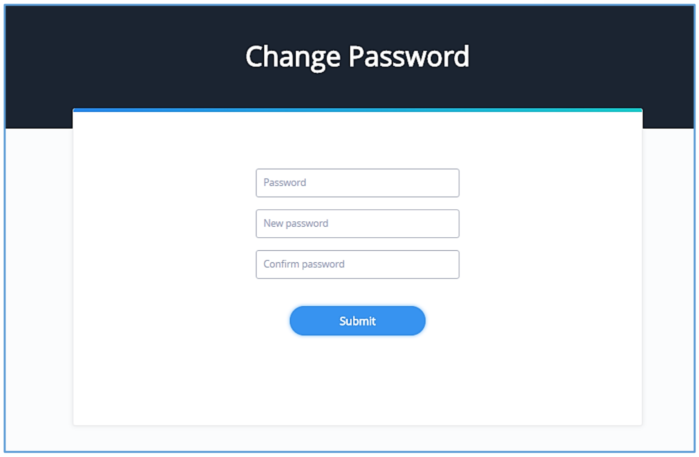
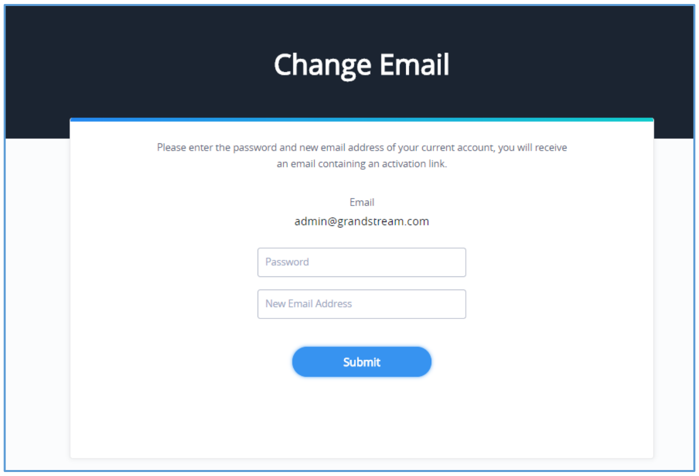


Figure 115 : Edit Super Administrator Password

Note: User passwords registered for authentication through the web portal are stored in an encrypted form

Changing Super Administrator Email

To edit super admin’s email address, click on **Change** and a new web page will be displayed, enter the **password** of the super admin account as well as the **new email address** then click on **Submit.**



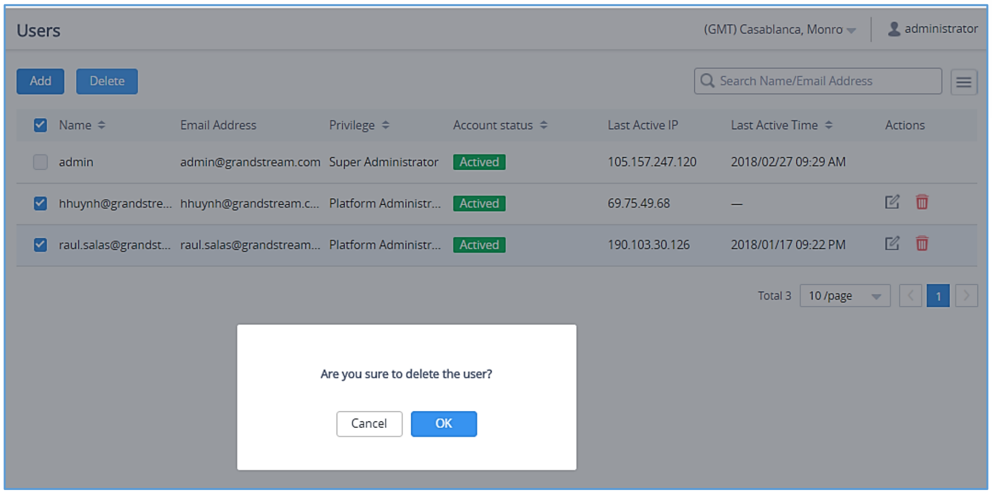
Please enter the password and new email address of your current account, you will receive an email containing an activation link.

Email
admin@grandstream.com

Figure 116 : Edit Super Administrator Email

Delete Users

To delete users, select one or multiple users, click on Delete button, then accept the confirmation message.



Users (GMT) Casablanca, Monro administrator

☑ Name	Email Address	Privilege	Account status	Last Active IP	Last Active Time	Actions
□ admin	admin@grandstream.com	Super Administrator	Actived	105.157.247.120	2018/02/27 09:29 AM	
☑ hhuynh@grandstre...	hhuynh@grandstream.c...	Platform Administr...	Actived	69.75.49.68	—	
☑ raul.salas@grandst...	raul.salas@grandstream...	Platform Administr...	Actived	190.103.30.126	2018/01/17 09:22 PM	

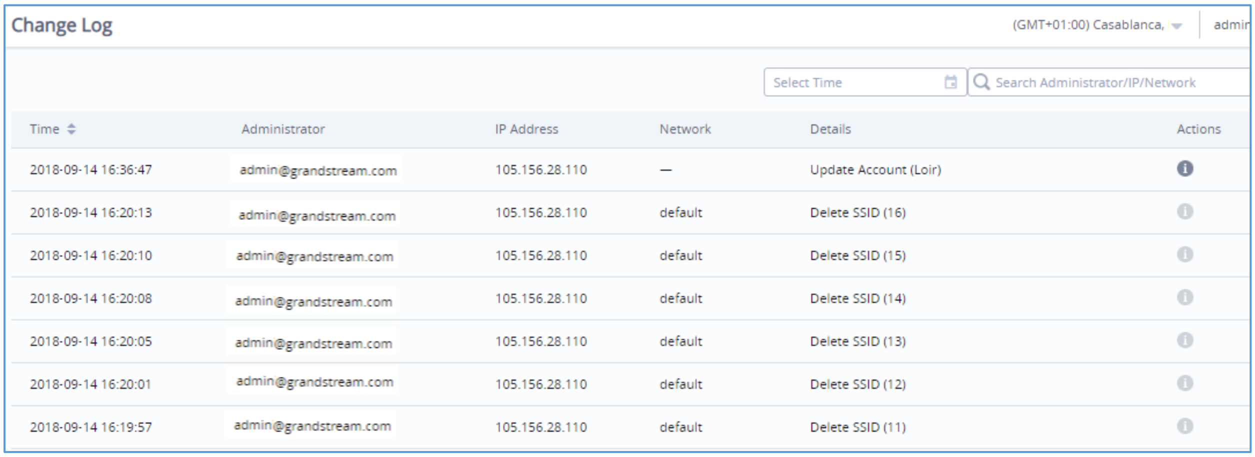
Total 3 10 /page 1

Are you sure to delete the user?

Figure 117 : Delete Users

Change Log

To list all the event logs recorded on the platform, Click on **username** from the top right corner ➔ **Change Log**

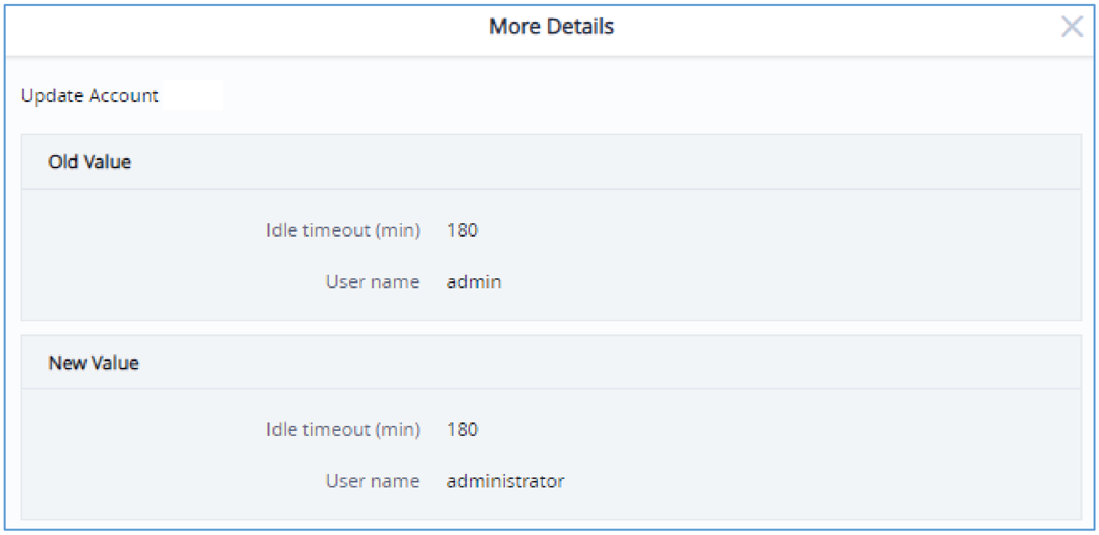


Change Log (GMT+01:00) Casablanca, admin

Time	Administrator	IP Address	Network	Details	Actions
2018-09-14 16:36:47	admin@grandstream.com	105.156.28.110	—	Update Account (Loir)	ⓘ
2018-09-14 16:20:13	admin@grandstream.com	105.156.28.110	default	Delete SSID (16)	ⓘ
2018-09-14 16:20:10	admin@grandstream.com	105.156.28.110	default	Delete SSID (15)	ⓘ
2018-09-14 16:20:08	admin@grandstream.com	105.156.28.110	default	Delete SSID (14)	ⓘ
2018-09-14 16:20:05	admin@grandstream.com	105.156.28.110	default	Delete SSID (13)	ⓘ
2018-09-14 16:20:01	admin@grandstream.com	105.156.28.110	default	Delete SSID (12)	ⓘ
2018-09-14 16:19:57	admin@grandstream.com	105.156.28.110	default	Delete SSID (11)	ⓘ

Figure 118: Change Log Records

- For some records including a value update, users can click on ⓘ under **Actions** section to list the actual change by showing both: The **Old** and **New** value.



Update Account

Old Value

Idle timeout (min) 180

User name admin

New Value

Idle timeout (min) 180

User name administrator

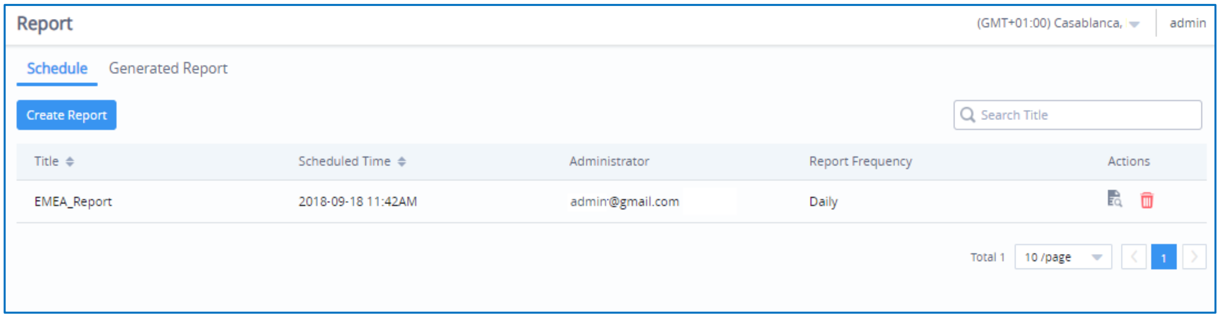
Figure 119: Change Log Action

Note: This option can be found under Global section for **GWN Manager** and **GWN Manager**

Report

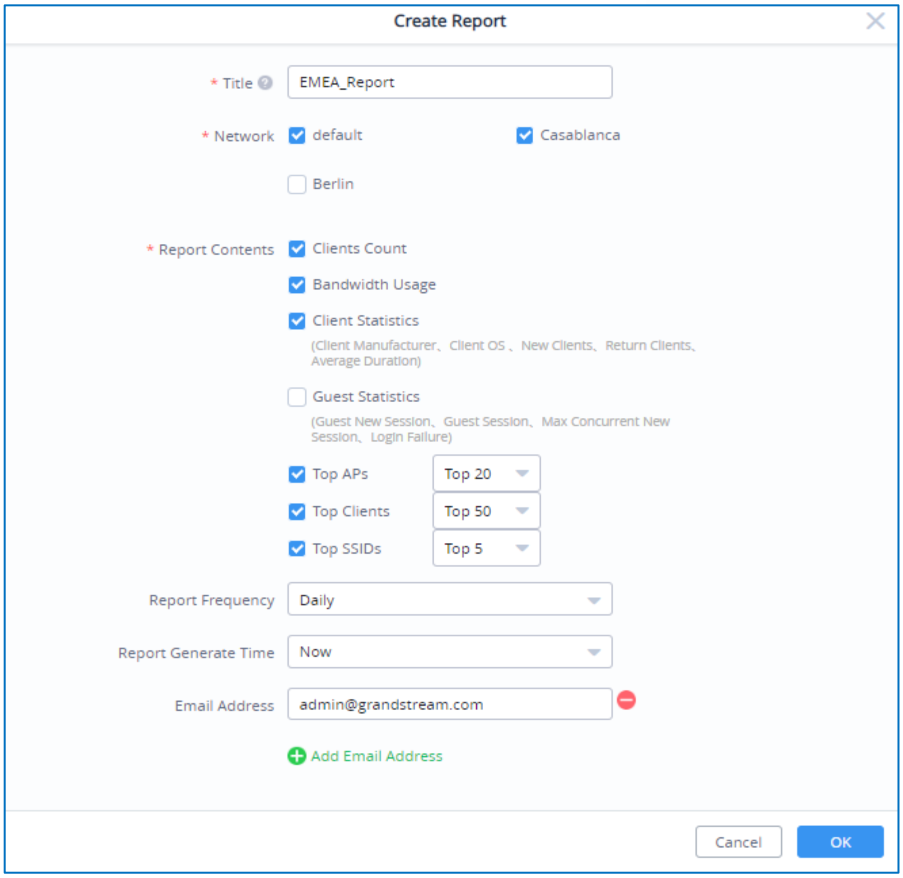
Administrators can generate and configure the platform to send reports periodically to the configured email addresses. Each report can be related to one or more different Network groups, providing Wi-Fi statistics (clients count, bandwidth usage, client and guest statistics…etc.)

To generate the report, click on **username** from the top right corner → **Report,** then click on Create Report button, a new page displaying the report details will be displayed.



Title	Scheduled Time	Administrator	Report Frequency	Actions
EMEA_Report	2018-09-18 11:42AM	admin@gmail.com	Daily	

Figure 120: Generate Report



Create Report

* Title: EMEA_Report

* Network: ☑ default ☑ Casablanca ☐ Berlin

* Report Contents:

- ☑ Clients Count
- ☑ Bandwidth Usage
- ☑ Client Statistics (Client Manufacturer、Client OS 、New Clients、Return Clients、Average Duration)
- ☐ Guest Statistics (Guest New Session、Guest Session、Max Concurrent New Session、Login Failure)
- ☑ Top APs: Top 20
- ☑ Top Clients: Top 50
- ☑ Top SSIDs: Top 5

Report Frequency: Daily

Report Generate Time: Now

Email Address: admin@grandstream.com

Figure 121: Create Report

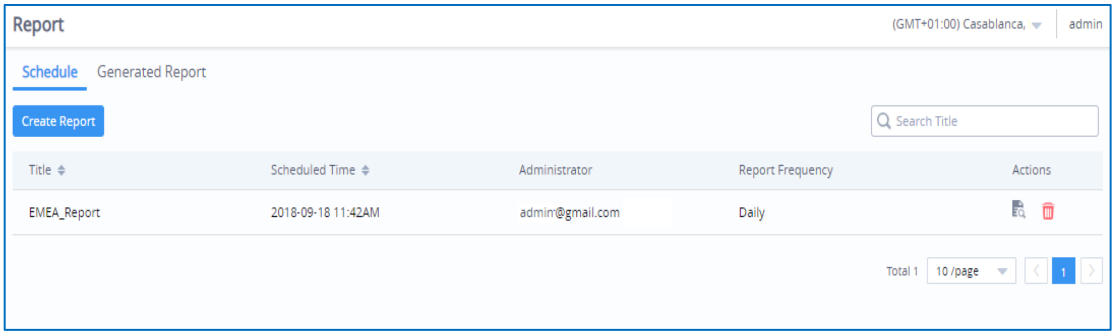
The following table provides an explanation about different options for report settings:

Table 29: Report Settings

Field	Description
Title	Specify the report title. The maximum length is 32 alphabet characters.
Network	Specify the Network Group to be included in the generated report.

Report Contents	Specify the report contents for the *selected network group(s)*, the contents can include: • **Clients Count:** reports the number of clients for all the SSIDs under selected network group. • **Bandwidth Usage:** The download and upload level statistics for all the SSIDs for the selected network group • **Clients Statistics:** reports the statistics for the different client manufacturer, client OS, the number for new clients as well as the return clients and the average duration. • **Guest Statistics:** reports statistics about the clients connected via Captive portal including the Guest New session, the Max concurrent New session, the login failure. • **Top APs:** reports the top 5/20/50 APs that consumed the max of the bandwidth/data. • **Top Clients:** Lists the top 5/20/50 clients that downloaded/uploaded the max of data • **Top SSIDs:** reports the top 5/20/50 SSIDs that are mostly used by clients.
Report Frequency	Specify the report frequency to be generated either on daily basis, weekly, monthly or custom range.
Date	Specify the Start and Date for the report to be generated when selecting "*Custom Range*" as **Report Frequency**.
Report Generate Time	Select either to generate the report now, or at later time
Time	Specify when you want the report to be generated. This field appear when selecting **"Later"** in **"Report Generate Time".**
Email Address	Enter the mail address(es) to which the report will be sent.

Once you press OK , a report schedule will be generated under **Schedule** section which you can preview by clicking on 🔍 Action button, or delete it using 🗑 .



Report (GMT+01:00) Casablanca, admin

Schedule Generated Report

Create Report Search Title

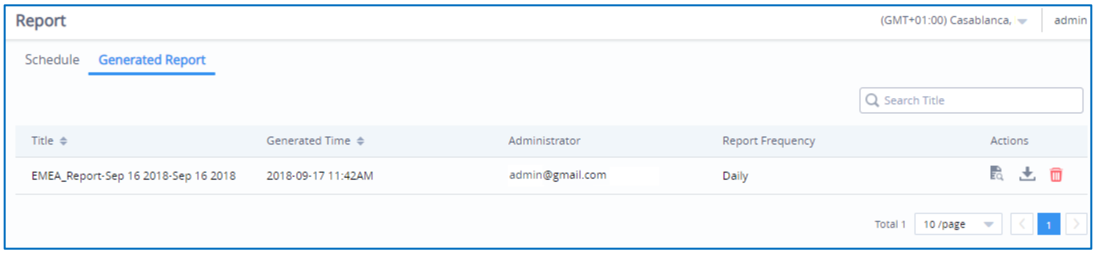
Title	Scheduled Time	Administrator	Report Frequency	Actions
EMEA_Report	2018-09-18 11:42AM	admin@gmail.com	Daily	🔍 🗑

Total 1 10 /page 1

Figure 122: Created Report

Note:

- Once you create a report, it cannot be edited afterwards, you will need to delete it and create a new one.
- Once the report is generated, it will appear under **Generated Report** section, the administrator can view it by clicking on 🔍 Action button, download it in PDF format by clicking on ⤓ , or delete it using 🗑 .



Report (GMT+01:00) Casablanca, admin

Schedule Generated Report

Search Title

Title	Generated Time	Administrator	Report Frequency	Actions
EMEA_Report-Sep 16 2018-Sep 16 2018	2018-09-17 11:42AM	admin@gmail.com	Daily	🔍 ⤓ 🗑

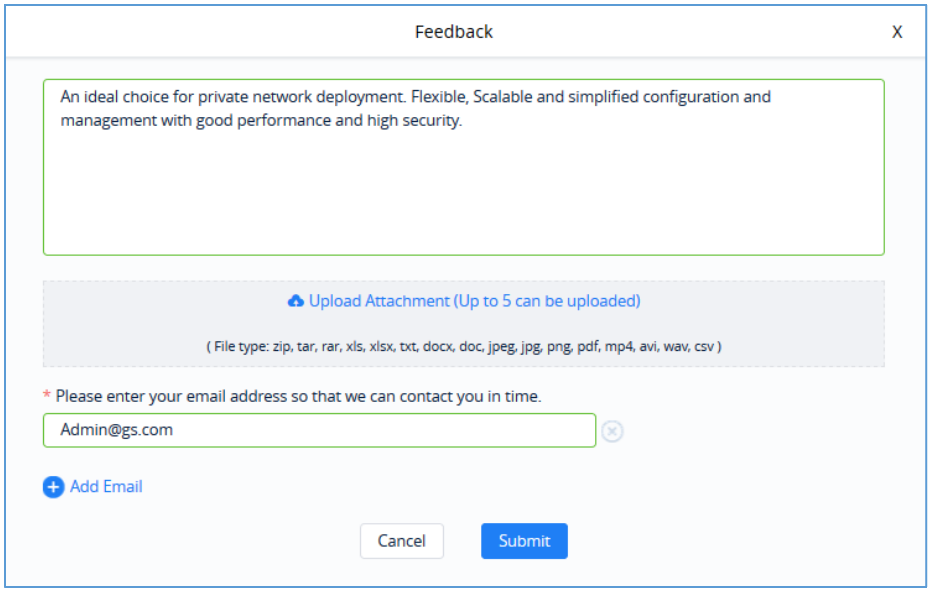
Total 1 10 /page 1

Figure 123: Generated Report

- This option can be found under Global section for **GWN Manager** and **GWN Cloud**

Feedback

Users can now send their feedback by clicking on Feedback the icon on the bottom of the page (maximum allowed character input is 2000) and they can file in different format (tar, jpg, pdf…etc) along with screenshot of the GWN Cloud page if needed.



Feedback

An ideal choice for private network deployment. Flexible, Scalable and simplified configuration and management with good performance and high security.

Upload Attachment (Up to 5 can be uploaded)

(File type: zip, tar, rar, xls, xlsx, txt, docx, doc, jpeg, jpg, png, pdf, mp4, avi, wav, csv)

* Please enter your email address so that we can contact you in time.

Admin@gs.com

Figure 124: Feedback

Users can add multiple emails by click on Add Email before Submit feedbacks

Change the display language by clicking on English then selecting an input from the dropdown list

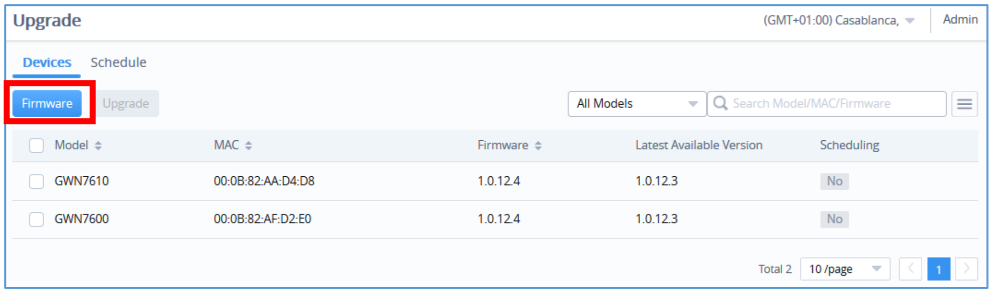
GLOBAL

Upgrade

This feature allows upgrading access points. Under “Upgrade” menu allows administrator to manage GWN APs firmware, trigger immediate upgrade or schedule an upgrade for GWN76xx.

- **Managing Firmware Files**

1. Go to **Upgrade → Devices.**



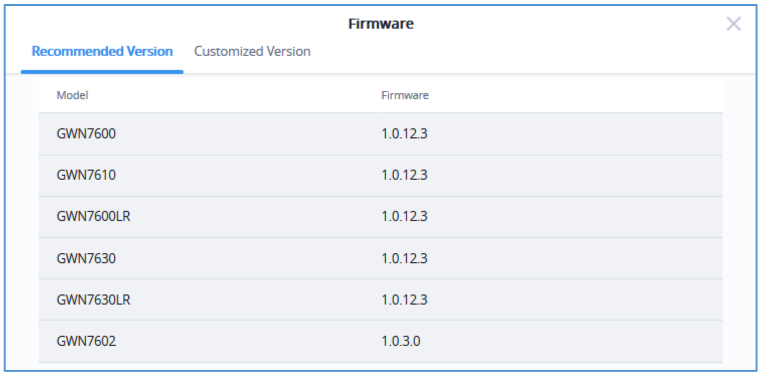
Model	MAC	Firmware	Latest Available Version	Scheduling
☐ GWN7610	00:0B:82:AA:D4:D8	1.0.12.4	1.0.12.3	No
☐ GWN7600	00:0B:82:AF:D2:E0	1.0.12.4	1.0.12.3	No

Total 2 10 /page 1

Figure 125: Upgrade

2. Click on Firmware button. A new window will be displayed:

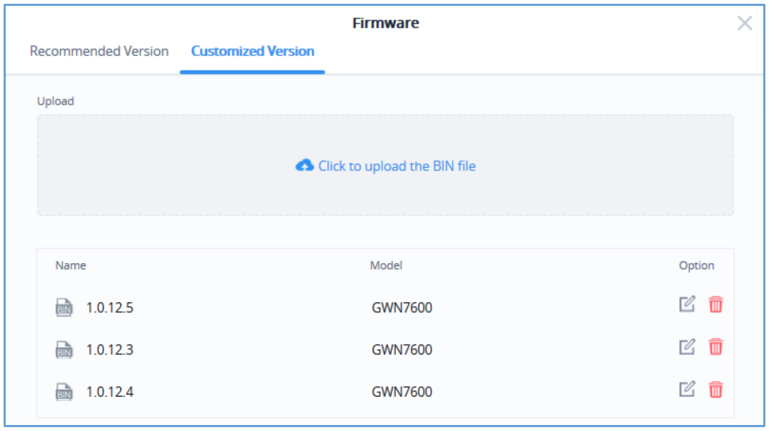
a. **Recommended Version:** The recommended version tab lists the latest official firmware.



Model	Firmware
GWN7600	1.0.12.3
GWN7610	1.0.12.3
GWN7600LR	1.0.12.3
GWN7630	1.0.12.3
GWN7630LR	1.0.12.3
GWN7602	1.0.3.0

Figure 126: Firmware - Recommended Version

b. **Customized Version:** From the customized version tab, users can upload a custom firmware to GWN Manager server to use it for access point upgrade.



Firmware

Recommended Version | Customized Version

Upload

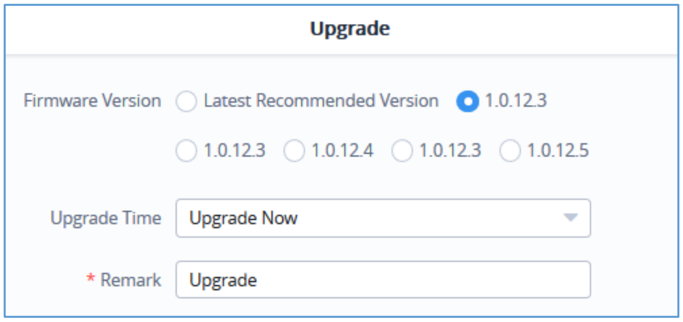
Click to upload the BIN file

Name	Model	Option
1.0.12.5	GWN7600	
1.0.12.3	GWN7600	
1.0.12.4	GWN7600	

Figure 127: Firmware - Customized Version

- **Upgrading Firmware**

To upgrade access points, select one or more from the list, then click on upgrade button, a new web page will popup:



Upgrade

Firmware Version ○ Latest Recommended Version ● 1.0.12.3
○ 1.0.12.3 ○ 1.0.12.4 ○ 1.0.12.3 ○ 1.0.12.5

Upgrade Time: Upgrade Now

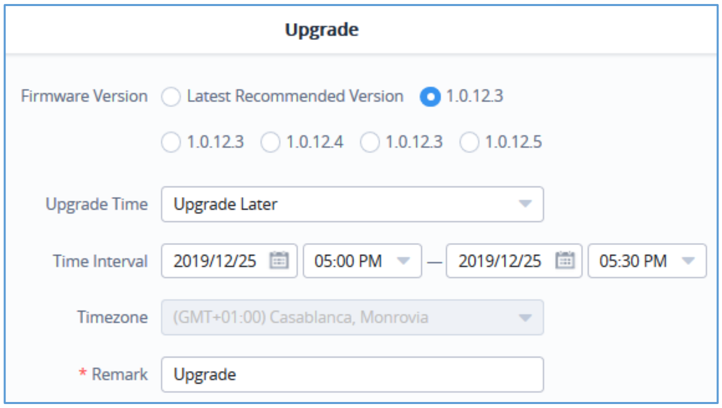
* Remark: Upgrade

Figure 128: Upgrade AP from GWN Manager

1. Select the firmware version from the list. Both recommended and customized versions will be displayed.
2. In the Upgrade Time list, select:

a. **Upgrade Now:** Trigger immediate upgrade for the GWN76XX access points.

b. **Upgrade Later:** Schedule upgrade at specific date and time. Administrator must specify time interval.

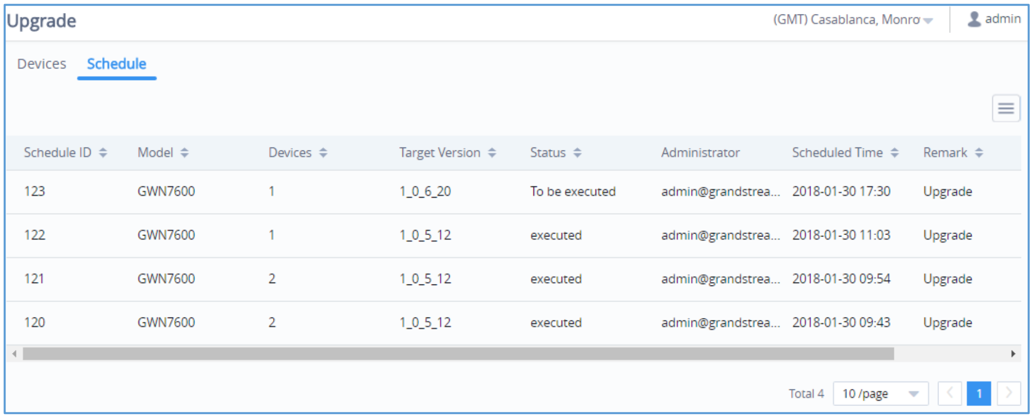


Upgrade

Firmware Version	○ Latest Recommended Version ● 1.0.12.3 ○ 1.0.12.3 ○ 1.0.12.4 ○ 1.0.12.3 ○ 1.0.12.5
Upgrade Time	Upgrade Later
Time Interval	2019/12/25 05:00 PM — 2019/12/25 05:30 PM
Timezone	(GMT+01:00) Casablanca, Monrovia
* Remark	Upgrade

Figure 129: Upgrade Schedule for GWN AP from GWN Manager

The schedule tab lists upcoming and executed upgrade actions:



Upgrade (GMT) Casablanca, Monro admin

Devices Schedule

Schedule ID	Model	Devices	Target Version	Status	Administrator	Scheduled Time	Remark
123	GWN7600	1	1_0_6_20	To be executed	admin@grandstrea...	2018-01-30 17:30	Upgrade
122	GWN7600	1	1_0_5_12	executed	admin@grandstrea...	2018-01-30 11:03	Upgrade
121	GWN7600	2	1_0_5_12	executed	admin@grandstrea...	2018-01-30 09:54	Upgrade
120	GWN7600	2	1_0_5_12	executed	admin@grandstrea...	2018-01-30 09:43	Upgrade

Total 4 10 /page 1

Figure 130: Upgrade - Schedule

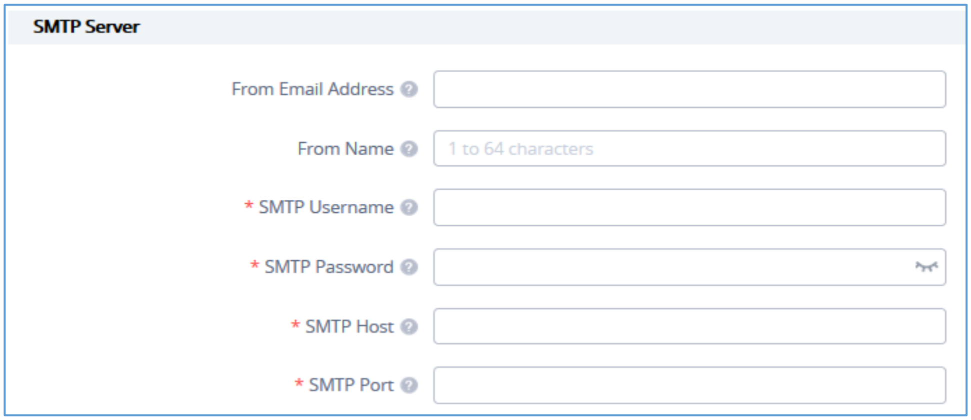
Manager Settings (GWN Manager Only)

Manager Log

Click on Export to download all the manager Log to your local directory (Including Redis, Nginx, MySQL and GWN logs).

SMTP Server

Set up SMTP server configuration:



SMTP Server

From Email Address

From Name: 1 to 64 characters

* SMTP Username

* SMTP Password

* SMTP Host

* SMTP Port

Figure 131: SMTP server

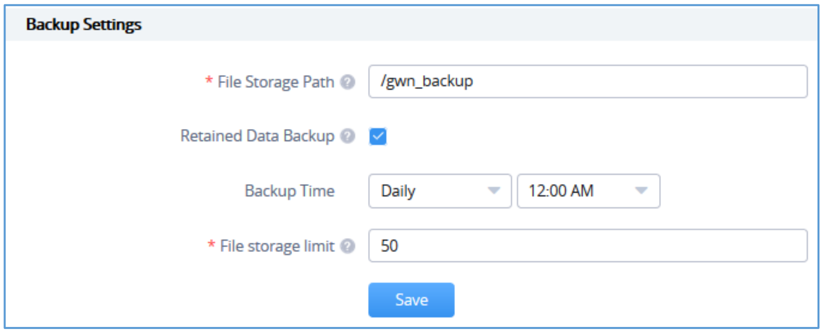
Table 30: SMTP server Configuration Details

From Email Address	Specify the email address of the notification sender. If the address is not specified, AP will use the SMTP username as a sender.
From Name	Specify the Name of the notification sender.
SMTP Username	Enter the username to login the mail server.
SMTP Password	Enter the password to login the mail server.
SMTP Host	Specify the mail server URL.
SMTP Port	Specify the mail server port.

Users may test the configuration using option Send test email .

Backup & Restore

Users can Backup GWN Manager configuration as shown below:



Backup Settings

* File Storage Path: /gwn_backup

Retained Data Backup: ☑

Backup Time: Daily 12:00 AM

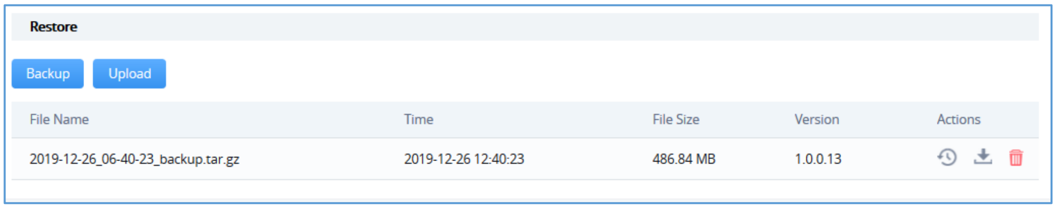
* File storage limit: 50

Figure 132: Backup Settings

Table 31: Backup Configuration Details

File Storage Path	Specify the path the backup files will be stored.
Retained Data Backup	Specify the contents of retained data backup. Settings only will not backup any data. The other options will back up the settings and the data recorded in the specified period.
Backup Time	Enter the backup time period (Daily, Weekly or Monthly)
File storage limit	Specify the maximum file number manager will store. Once the backup files reached limit, the old ones will be replaced with the new ones.

Restore tab holds the two option “Backup and Upload:



File Name	Time	File Size	Version	Actions
2019-12-26_06-40-23_backup.tar.gz	2019-12-26 12:40:23	486.84 MB	1.0.0.13	⟲ ⬇ 🗑

Figure 133: Restore

Users can either click Upload to import backup from the local directory. Or, click Backup to backup immediately. A pop window will show to confirm the operation:

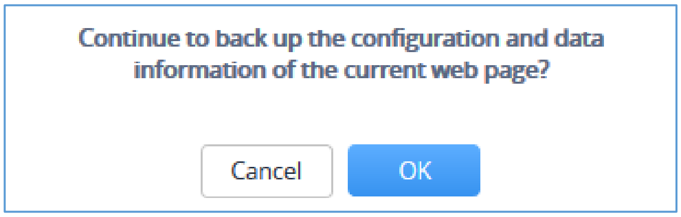

Continue to back up the configuration and data information of the current web page?

Figure 134: Confirm Backup

A list of available Backup files with their specific Time, File Size and Version is displayed on the bottom where the user may Restore ⟲ , Download ⬇ or Delete 🗑 a File.

Report

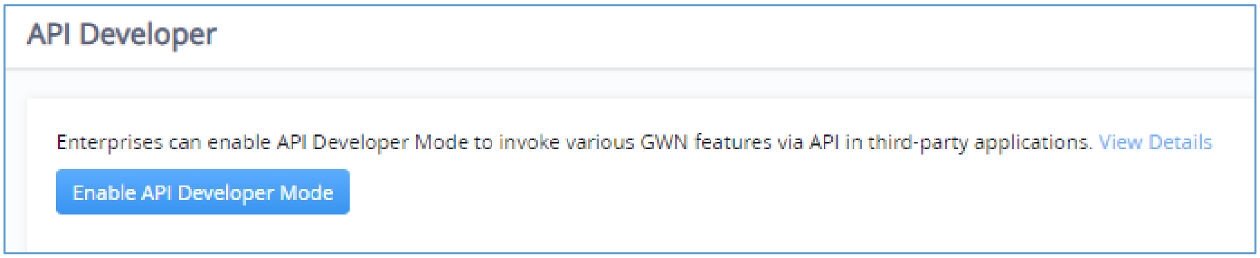
Refer to [Report] section.

Change Log

Refer to [Change Log] section.

API Developer

Enterprises can enable API Developer Mode to invoke various GWN features via API in third-party applications.



API Developer

Enterprises can enable API Developer Mode to invoke various GWN features via API in third-party applications. View Details

Figure 135: Enable API Developer Mode

For further details, please refer to the GWN API Developer Guide

EXPERIENCING GWN MANAGEMENT PLATFORMS

Please visit our Website: http://www.grandstream.com to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for using Grandstream GWN Management Platforms, it will be sure to bring convenience to both your business and personal life.