

Grandstream Networks, Inc.

GWN.Cloud

Cloud based Access Points Controller

User Guide



COPYRIGHT

©2018 Grandstream Networks, Inc. <http://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

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

<http://www.grandstream.com/support>

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.



Table of Contents

DOCUMENT PURPOSE	10
CHANGE LOG	11
GWN.Cloud Version 1.0.8.17	11
GWN.Cloud Version 1.0.8.7.....	11
GWN.Cloud Version 1.0.7.18.....	11
GWN.Cloud Version 1.0.0.37	12
REQUIREMENTS	13
WELCOME	14
PRODUCT OVERVIEW	15
Features Highlights.....	15
Specifications	15
GETTING TO KNOW GWN.CLOUD	17
Sign up to GWN.Cloud.....	17
GETTING STARTED	21
GWN76xx LED Patterns	21
Adding GWN76XX to GWN.Cloud.....	22
<i>Method 1: Adding New AP Manually</i>	22
<i>Method 2: Adding New AP using GWN.Cloud Application</i>	25
<i>Method 3: Transfer APs from Local Master</i>	26
GWN.CLOUD DASHBOARD	28
Overview	28
Network List.....	30
AP List.....	31
NETWORK	33
Create a New Network.....	33
Overview Page	35



ACCESS POINTS	36
Summary.....	36
Status.....	36
Configuration.....	42
<i>Add New Access Points</i>	42
<i>Move Access Points</i>	42
<i>Delete Access Points</i>	43
<i>Reboot Access Points</i>	43
<i>Configure Access Points</i>	44
<i>Reset Access Points</i>	46
SSID.....	47
Summary.....	47
Configuration.....	47
<i>Wi-Fi Settings</i>	48
<i>Device Membership</i>	53
CLIENTS.....	56
Summary.....	56
<i>Clients Count</i>	57
<i>Bandwidth Usage</i>	57
<i>Clients Statistics for Last Day</i>	57
<i>Client Manufacturer</i>	57
<i>Client OS</i>	57
Status Page.....	57
CAPTIVE PORTAL	60
Summary.....	60
<i>Guest New Session</i>	61
<i>Guest Session by Authentication</i>	61
<i>Guest Session by SSID</i>	62
<i>Guest</i>	62
Guest.....	63
Policy List.....	64
<i>Internal Splash Page</i>	65
<i>External Splash Page</i>	66
Splash Page.....	67



Page.....	67
Advertisement	73
Voucher	75
ACCESS CONTROL.....	78
Access List	78
Time Policy.....	79
Bandwidth rules.....	79
SYSTEM	82
Settings	82
<i>URL Access Log</i>	83
Schedule	86
Mesh	87
Maintenance.....	89
Alert	89
Upgrade	91
USER MANAGEMENT	95
Add New Users.....	95
User Privilege levels	97
<i>Super Administrator</i>	97
<i>Platform Administrator</i>	98
<i>Network Administrator</i>	98
<i>Guest Editor</i>	98
Edit User Settings.....	98
<i>Changing Password</i>	98
<i>Changing Super Administrator Email</i>	99
Delete Users.....	100
Change Log.....	100
Report	101
EXPERIENCING GWN.CLOUD.....	105



Table of Tables

Table 1: Requirements.....	13
Table 2: GWN.Cloud Specifications.....	15
Table 3: GWN.Cloud Sign up Settings.....	19
Table 4: LED Patterns.....	21
Table 5: Dashboard Description	29
Table 6: Create a New Network Settings	31
Table 7: Create a New Network Settings	34
Table 8: Access Point Configuration Settings	44
Table 9: SSID Wi-Fi Settings.....	48
Table 10: Add new Policy List – Splash Page as “Internal”	65
Table 11: Add new Policy List – Splash Page as “External”	66
Table 12: Advertisement Settings Configuration	74
Table 13: Voucher Configuration Parameters	76
Table 14: Bandwidth Rules	79
Table 15: Settings.....	82
Table 16: Maintenance.....	89
Table 17: Alert.....	90
Table 18: Super Administrator Account.....	97
Table 19: Report Settings.....	102



Table of Figures

Figure 1: GWN.Cloud Architecture	17
Figure 2: GWN.Cloud Login Page.....	18
Figure 3: GWN.Cloud Sign up page.....	19
Figure 4: GWN.Cloud Dashboard	20
Figure 5: GWN Access Point MAC and Wi-Fi Password.....	22
Figure 6: Adding New Access Point to GWN.Cloud	23
Figure 7: Adding Access Points Manually.....	23
Figure 8: Import CSV file for APs	24
Figure 9: Upload CSV file	24
Figure 10: Adding Access Point to GWN.Cloud using GWN App	25
Figure 11: Access Points Status.....	25
Figure 12: Master AP - Access Points	26
Figure 13: Transfer AP to Cloud.....	26
Figure 14: Select Network.....	27
Figure 15: Transfer AP to Cloud - Success.....	27
Figure 16: GWN.Cloud Dashboard - Overview.....	28
Figure 17: GWN.Cloud Dashboard - Network List	30
Figure 18: Create a New Network	30
Figure 19: GWN.Cloud Dashboard – AP List.....	31
Figure 20: Customize AP List Table Fields	32
Figure 21: Network List and Network Creation Button	33
Figure 22: Create Network.....	34
Figure 23: Overview Page Displays Information related to Specific Network.....	35
Figure 24: Access Points - Summary	36
Figure 25: Access Points - Status	37
Figure 26: Access Points Status.....	37
Figure 27: Usage of a Specific AP.....	38
Figure 28: Current Clients - Stats per AP	38
Figure 29: Event Log per AP.....	39
Figure 30: AP Info.....	40
Figure 31: Debug Tool Tab.....	41
Figure 32: Access Points Configuration Page.....	42
Figure 33: Moving Access Points between Networks.....	42
Figure 34: Delete Access Point	43
Figure 35: Reboot Access Point.....	43
Figure 36: Access Point Configuration Page	44
Figure 37: Reset Access Point	46
Figure 38: SSIDs - Summary	47
Figure 39: SSIDs - Configuration	47



Figure 40: SSIDs – Configuration – Wi-Fi Settings	48
Figure 41: Device Membership - Available Devices	54
Figure 42: Device Membership - Members Devices	55
Figure 43: Clients - Summary	56
Figure 44: Clients Status.....	57
Figure 45: Client Data Usage Info	58
Figure 46: Client Info	59
Figure 47: Client Roaming	59
Figure 48: Captive Portal Summary	60
Figure 49: Guest New Session	61
Figure 50: Guest Session by Authentication.....	62
Figure 51: Guest Session by SSID.....	62
Figure 52: Guest Section	63
Figure 53: Captive Portal Status	63
Figure 54: Export Guest Information Period	64
Figure 55: Add/Edit Captive Portal Policy	65
Figure 56: Create New Splash Page	69
Figure 57: Setup Logging Methods - Splash Page.....	70
Figure 58: Setup Social Logging Parameters	71
Figure 59: Splash Page Preview	72
Figure 60: Splash Pages List	72
Figure 61: Portal Splash Page	73
Figure 62: Advertisement Page.....	74
Figure 63: Adding Vouchers.....	76
Figure 64: Voucher Details.....	77
Figure 65: Access List.....	78
Figure 66: Adding New Clients to Access List.....	78
Figure 67: Add Time Policy List.....	79
Figure 68: MAC Address Bandwidth Rule	81
Figure 69 :System Settings.....	82
Figure 70: URL Access Log Settings.....	84
Figure 71: Export Immediately	84
Figure 72: URL Access Log Email.....	85
Figure 73: URL Access Log- CSV file example.....	85
Figure 74: Create New Schedule	86
Figure 75: Schedules List	87
Figure 76: Mesh Settings.....	88
Figure 77: Mesh Topology.....	88
Figure 78: Maintenance/Syslog Settings	89
Figure 79: Alert Email	89
Figure 80: Alert Events List.....	90
Figure 81: Upgrade.....	91



Figure 82: Firmware - Recommended Version	91
Figure 83: Firmware - Customized Version.....	92
Figure 84: Upgrade GWN AP from Cloud.....	93
Figure 85: Upgrade Schedule for GWN AP from Cloud	93
Figure 86: Upgrade - Schedule.....	94
Figure 87 : Users List.....	95
Figure 88 : Add New “Platform Administrator” User	96
Figure 89 : Add “New Network Administrator” User.....	96
Figure 90 : Edit Super Administrator Account	97
Figure 91 : Edit Super Administrator Password	99
Figure 92 : Edit Super Administrator Email.....	99
Figure 93 : Delete Users	100
Figure 94: Change Log Records	100
Figure 95: Change Log Action.....	101
Figure 96: Generate Report	101
Figure 97: Create Report	102
Figure 98: Created Report	104
Figure 99: Generated Report	104

DOCUMENT PURPOSE

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

This guide covers following topics:

- [Product Overview](#)
- [Getting to Know GWN.Cloud](#)
- [Getting Started](#)
- [Adding GWN76xx to GWN.Cloud](#)
- [Networks Management](#)
- [Access Points Management](#)
- [Clients Management](#)
- [SSIDs Management](#)
- [Captive Portal](#)
- [Access Control](#)
- [System Maintenance](#)
- [User Management](#)



CHANGE LOG

This section documents significant changes from previous versions of the GWN.Cloud 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 1.0.8.17

- 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 Page]
- Enhanced Event log by WiFi 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][data usage]
- Added Export Immediately feature for URL Access Logs. [URL Access Log]

GWN.Cloud Version 1.0.8.7

- Added support for URL logging (Only GWN7600/GWN7600LR) [URL Access Log]

GWN.Cloud 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 WiFi Statistic Report. [Report]
- Added feature of Captive Portal Guest Summary. [Summary]
- Changed SSID limit. [SSID Limit]
- Enhanced WiFi 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]



GWN.Cloud Version 1.0.0.37

- This is the initial version for GWN.Cloud.



REQUIREMENTS

Following table shows the requirements of Grandstream networking products and version of APP supporting GWN.Cloud version 1.0.8.:

Table 1: Requirements

	Model	Minimum	Recommended
Version of AP	GWN7610	1.0.6.37	1.0.8.7
	GWN7600	1.0.6.33	1.0.8.7
	GWN7600LR	1.0.6.33	1.0.8.7
Version of APP	iOS	1.0.2	1.0.3
	Android	1.0.0.7	1.0.0.12

WELCOME

Thank you for using Grandstream GWN.Cloud Wireless Access Point Controller.

GWN.Cloud is an enterprise-grade Wi-Fi network management platform that offers a centralized, streamlined network management and monitoring platform. This cloud-based platform allows business to deploy a secure Wi-Fi network in seconds and manage those networks across multiple locations through a web user interface and mobile apps for Android and iOS devices. GWN.Cloud offers a streamlined network configuration process, real-time Wi-Fi access point and client monitoring, as well as a variety of statistics, reports and alerts.



PRODUCT OVERVIEW

Features Highlights

- 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.
- Highly available with no single point of failure across the whole system.
- Easy way to add new access point, either by scanning a barcode from GWN.Cloud app or by entering AP MAC and random password.
- 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.Cloud 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, WEP, open, etc. Bandwidth rules for client access User and privilege management
Enterprise Features	No limits on number of sites or APs Hosted by AWS with 99.99% uptime Bank-grade TLS encryption from end-to-end X.509 certificate-based authentication Supports up to 16 SSIDs per access point Supports Wi-Fi Alliance Voice-Enterprise Mobile app for iOS and Android
Supported Wi-Fi Access Points	GWN7610, GWN7600, GWN7600LR



Captive Portals	Splash page with built-in WYSIWYG editor Facebook, Twitter, WeChat integration Multiple captive portal authentications including simple password, social login authentication, RADIUS Server, etc. Customizable online splash pages
Reporting and Monitoring	Real-time Wi-Fi AP and client monitoring Detailed real-time reports by network, AP, client etc. Maintains 30 days of historical data No user traffic sent to the cloud Real-time alerts
Troubleshooting	Ping Traceroute
Languages	English, Spanish, French, German, Portuguese and Chinese



GETTING TO KNOW 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, The GWN.Cloud can control up to 1000 GWN access points, from different models.

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:



Figure 2: GWN.Cloud Login Page

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

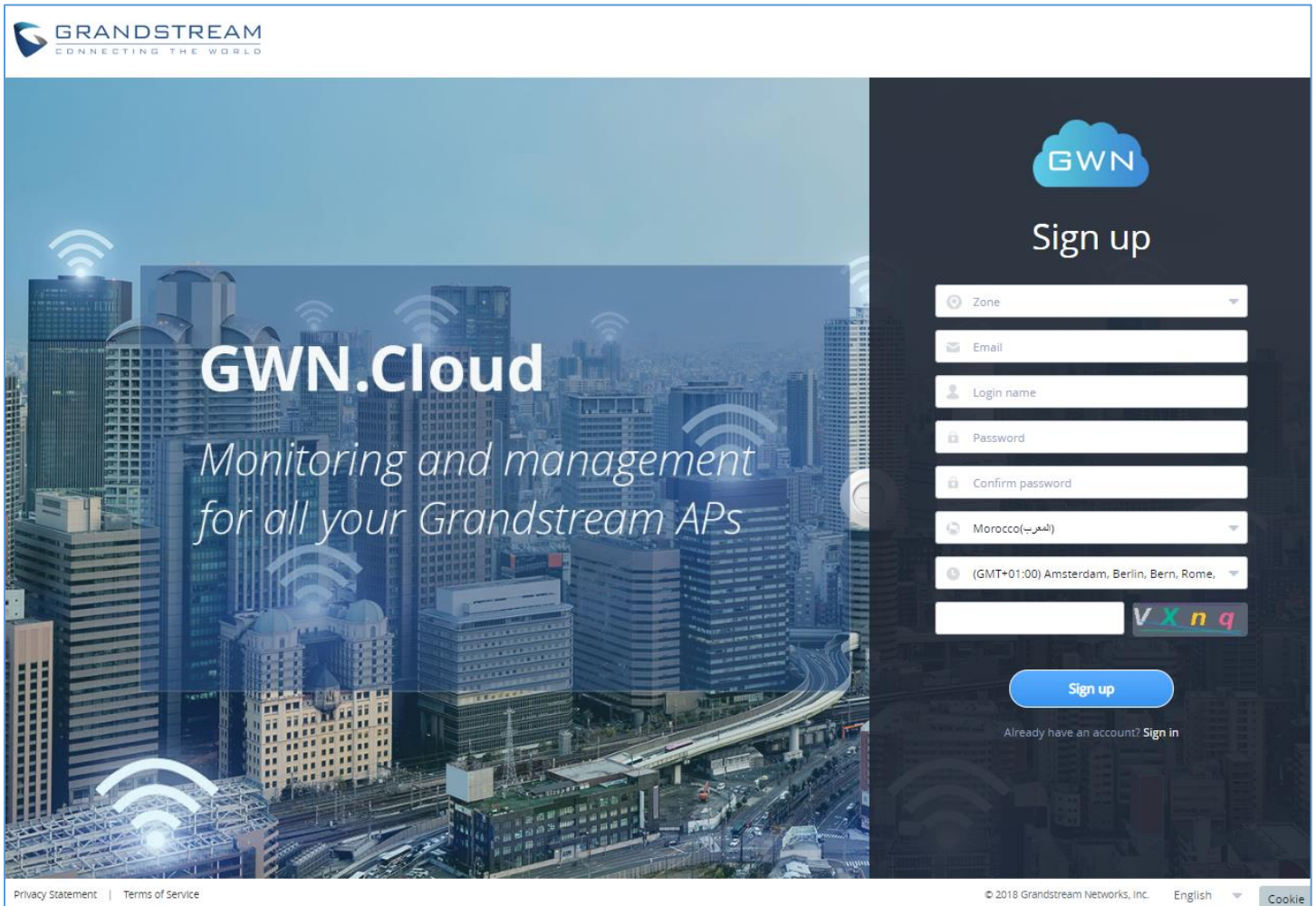


Figure 3: GWN.Cloud Sign up page

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.

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

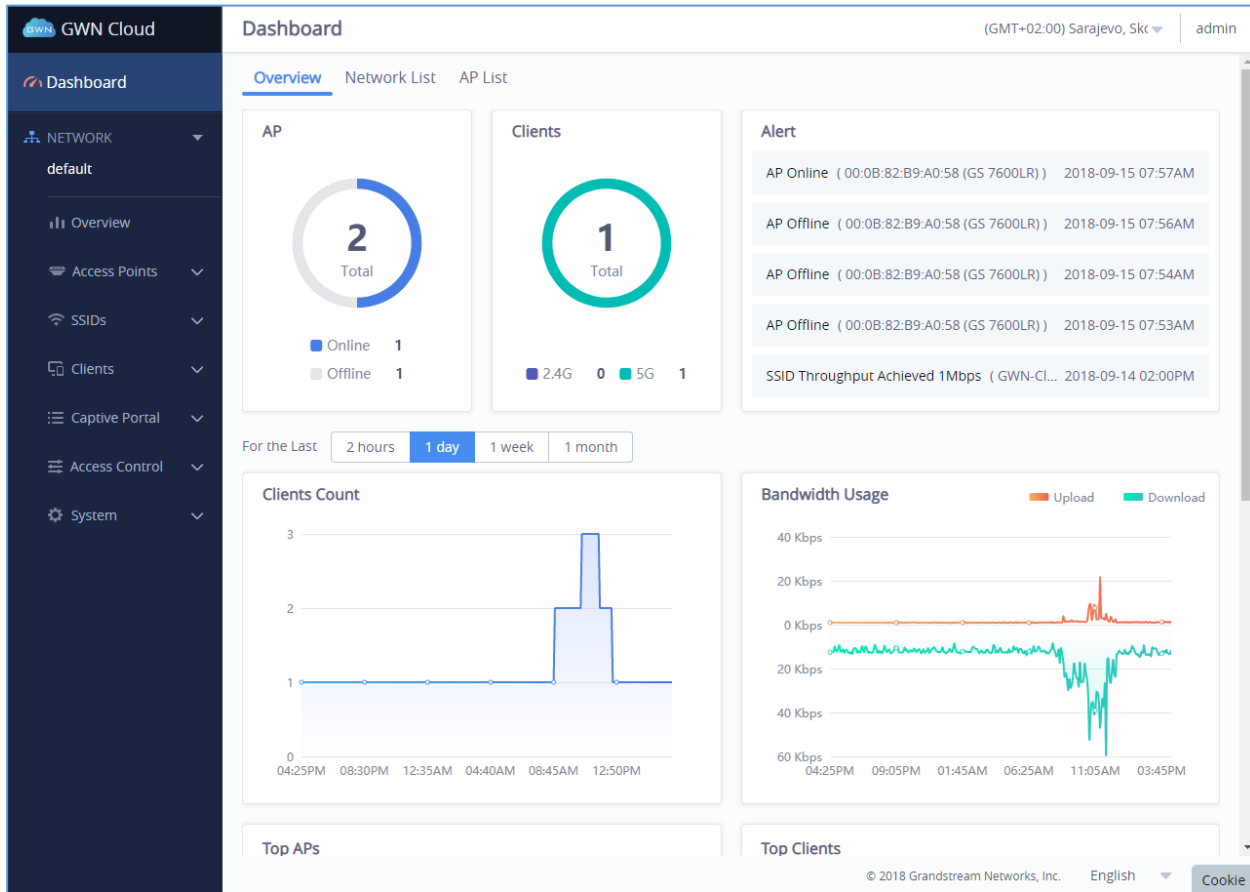


Figure 4: GWN.Cloud Dashboard

GETTING STARTED

The GWN.Cloud provides 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

This section provides steps to discover/add GWN76XX to the cloud for management and monitoring.

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 4: 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
Blinking 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 GWN.Cloud, the status of the LED should be **Blinking 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: GWN76xx Access Points need to be using firmware 1.0.6.23 or higher. If GWN76xx is using older firmware, make sure to upgrade them 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 Android 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.

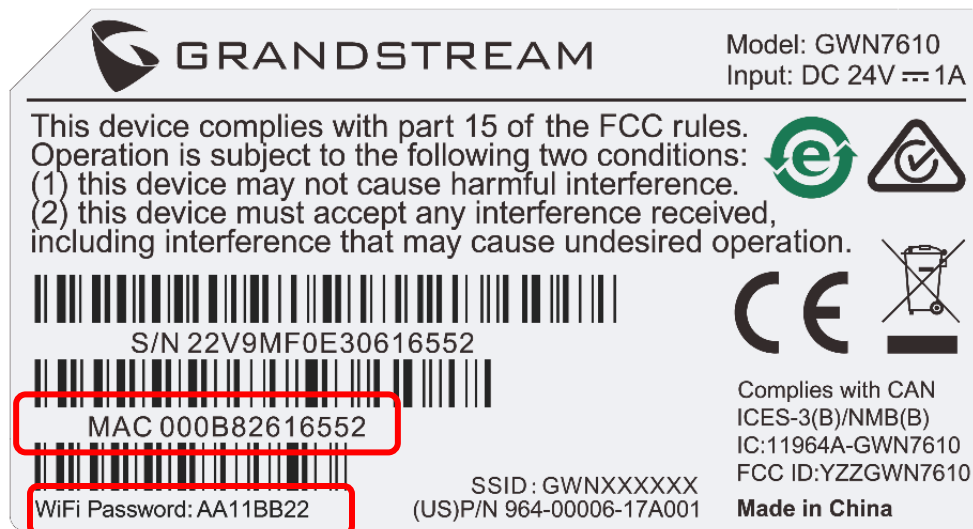


Figure 5: GWN Access Point MAC and Wi-Fi Password

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

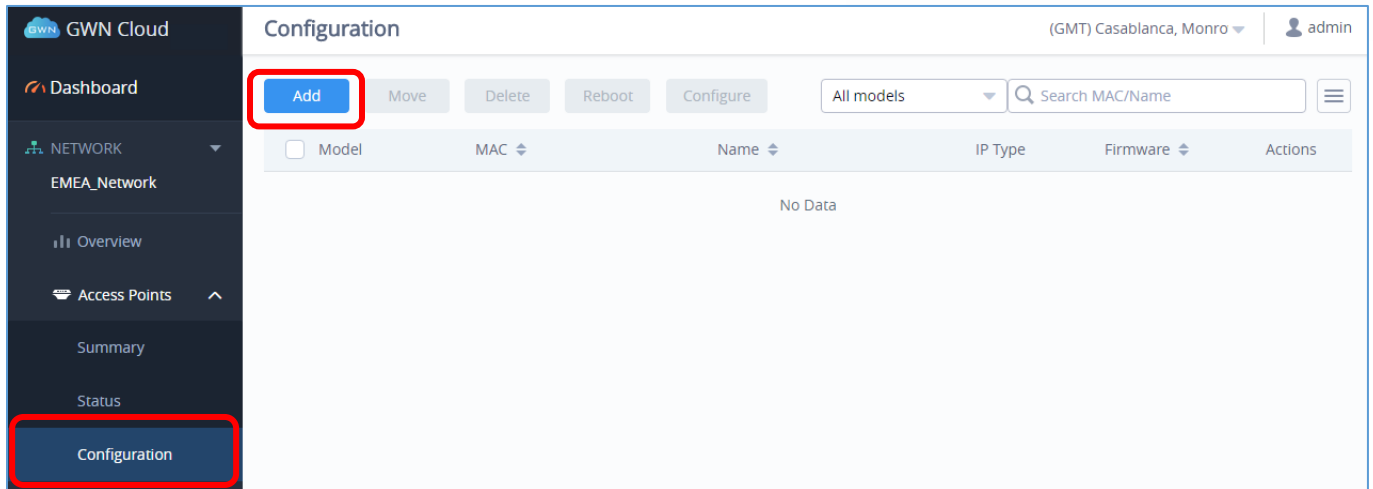


Figure 6: Adding New Access Point to GWN.Cloud

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

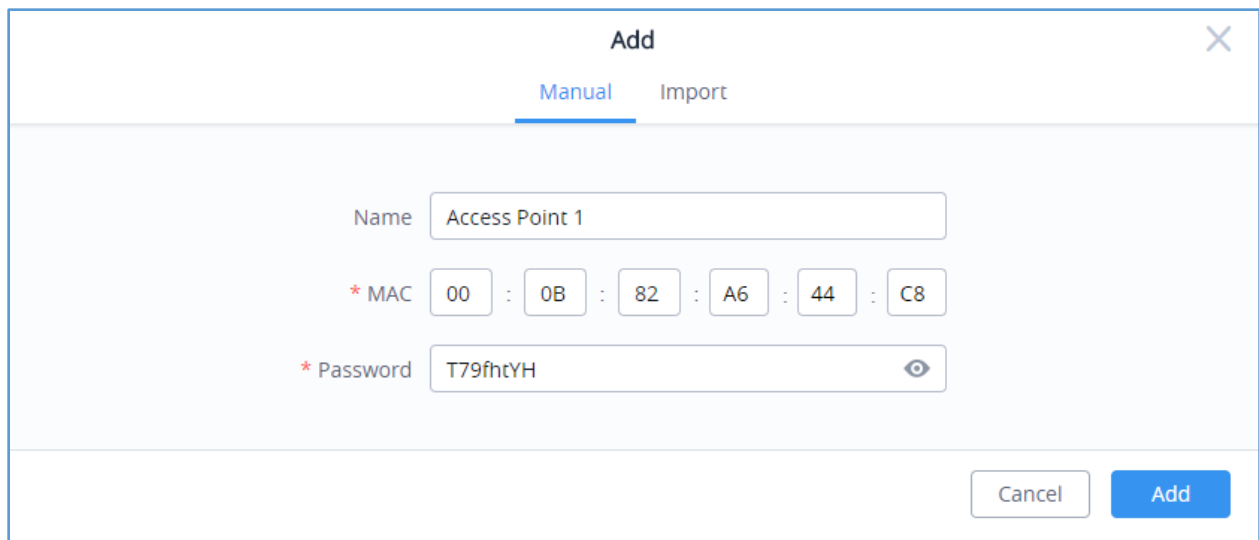


Figure 7: Adding Access Points Manually

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.

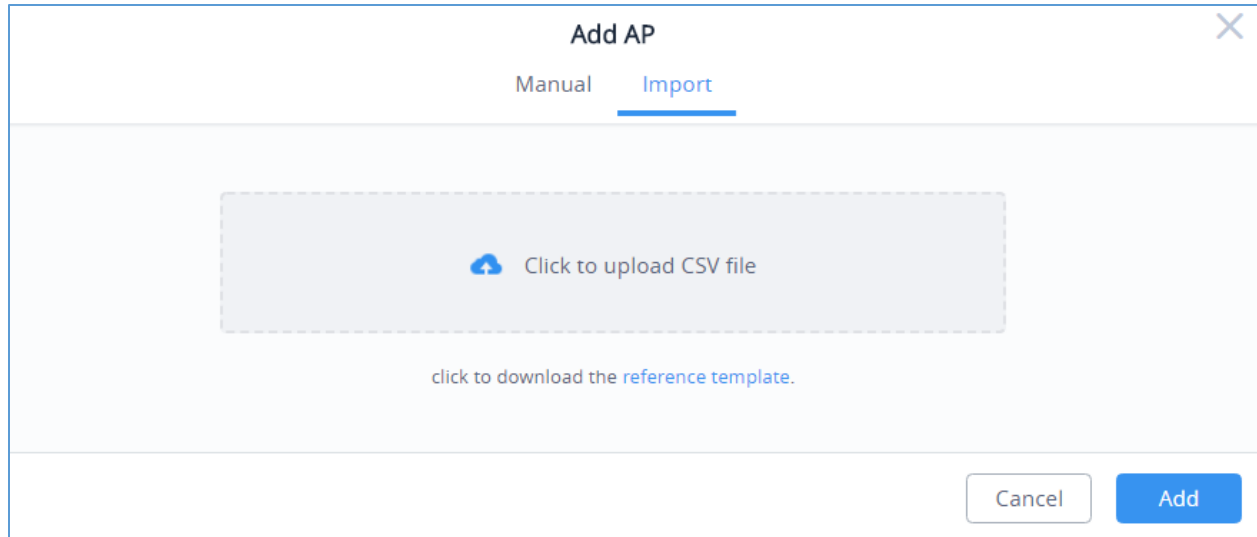


Figure 8: Import CSV file for APs

- 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).

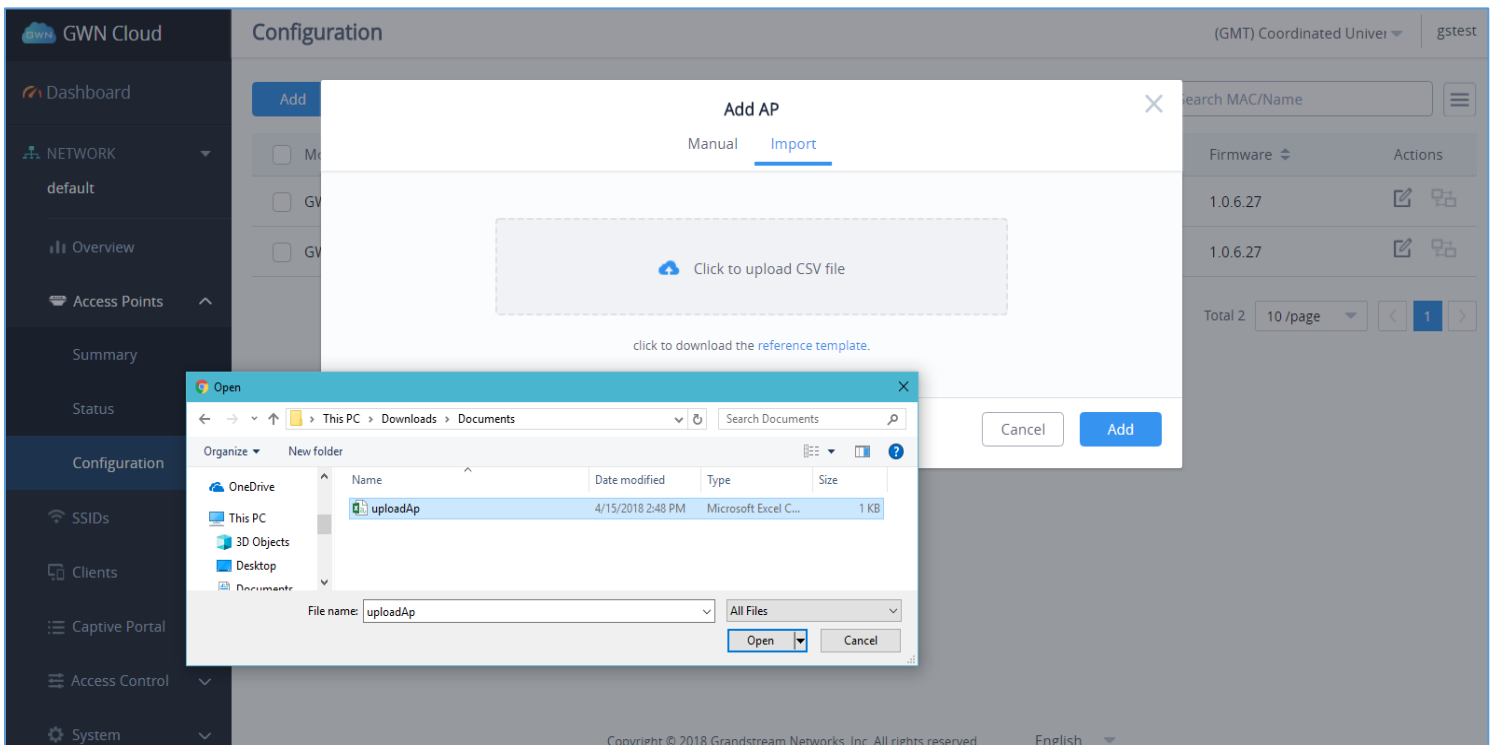


Figure 9: Upload CSV file



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™ and App Store for iOS™.

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

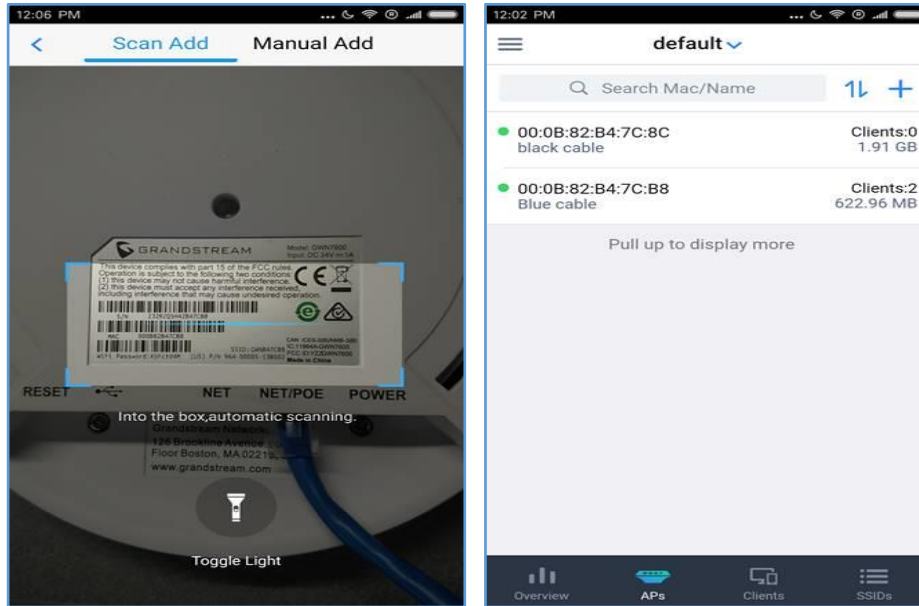


Figure 10: Adding Access Point to GWN.Cloud using GWN App

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

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 11: 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**.

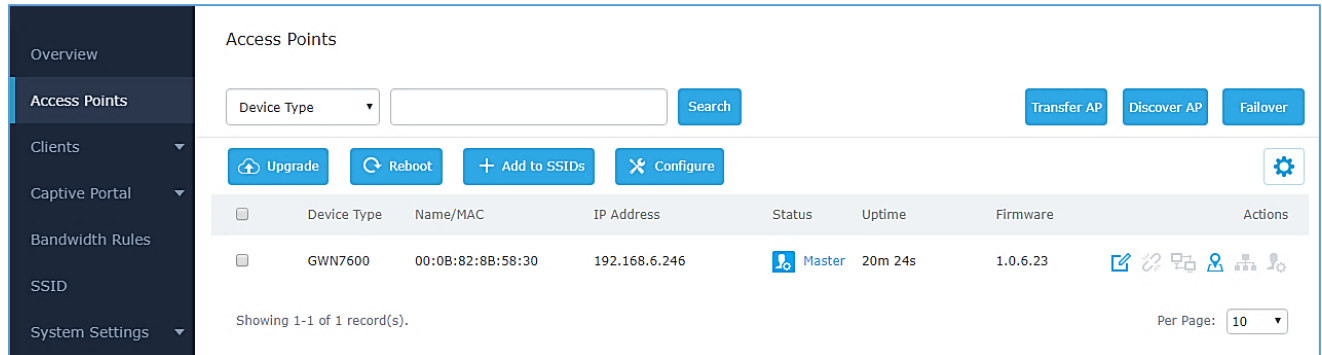


Figure 12: Master AP - Access Points

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

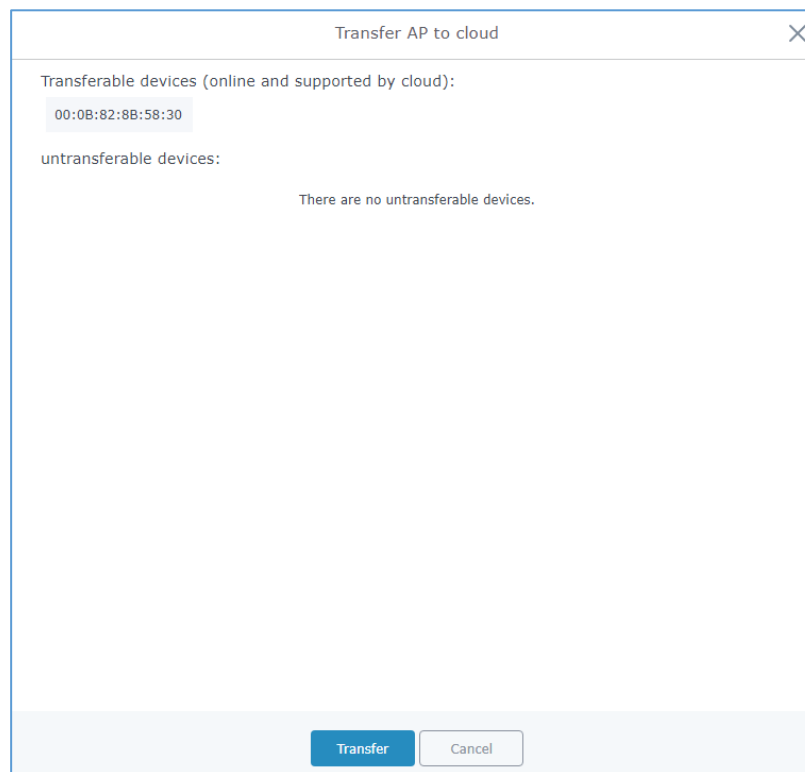
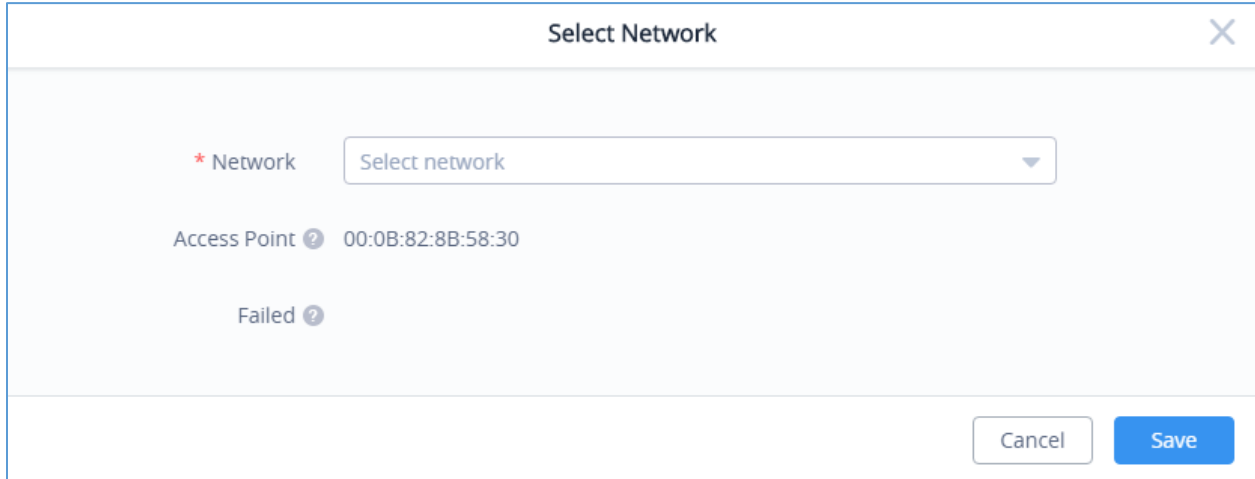


Figure 13: Transfer AP to Cloud

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:



The image shows a 'Select Network' dialog box with a close button (X) in the top right corner. It contains a red asterisk followed by the label '* Network' and a dropdown menu with the text 'Select network'. Below this is the label 'Access Point' followed by a question mark icon and the MAC address '00:0B:82:8B:58:30'. Further down is the label 'Failed' followed by a question mark icon. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 14: 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.

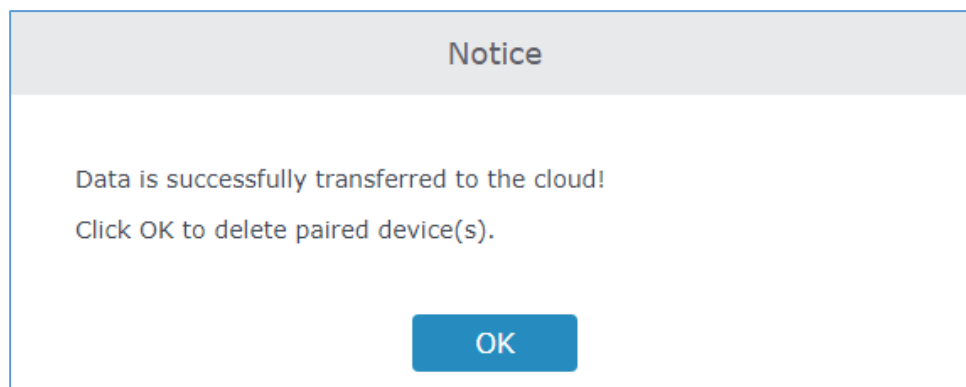


Figure 15: Transfer AP to Cloud - Success

GWN.CLOUD 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

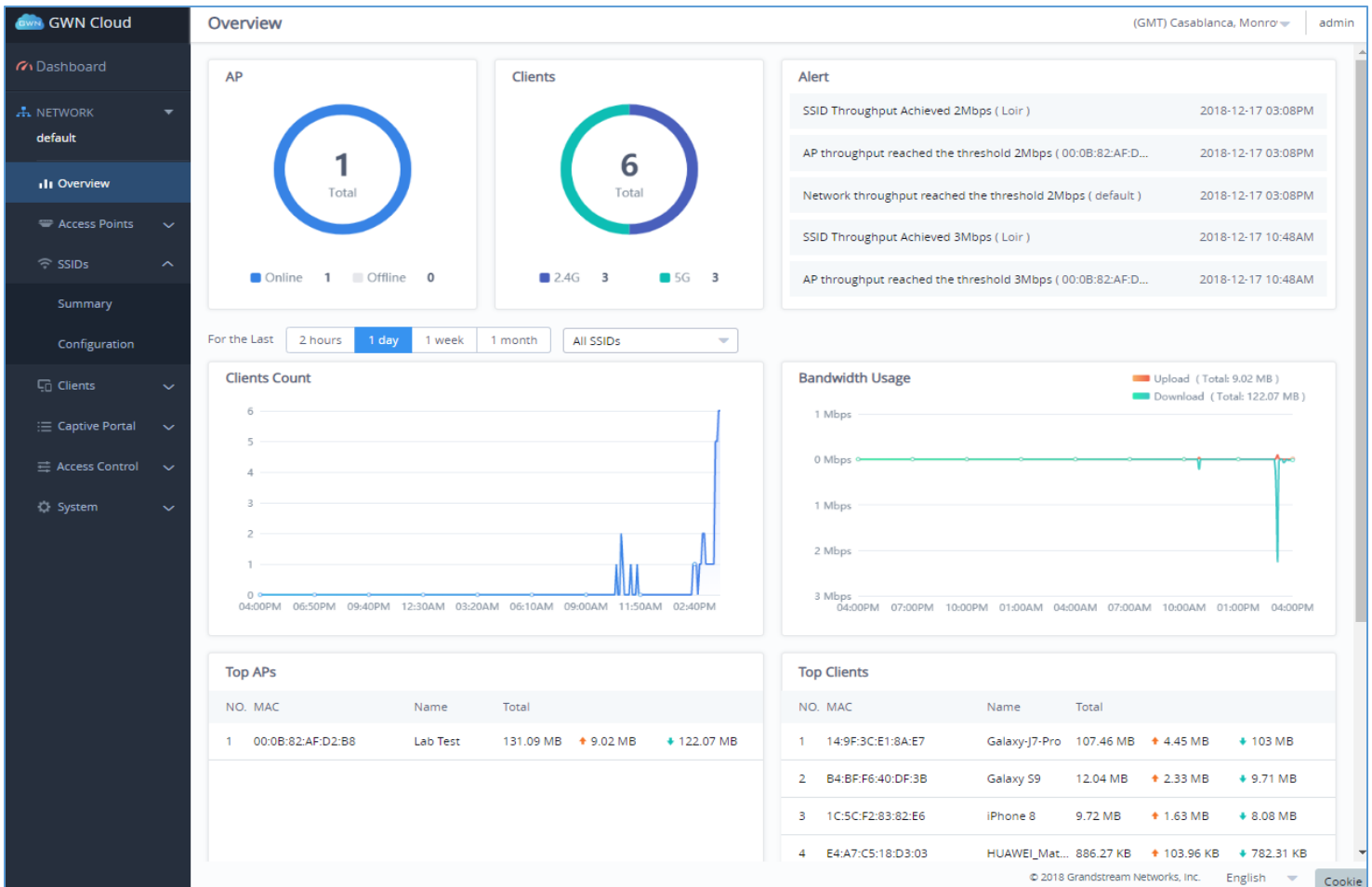


Figure 16: GWN.Cloud Dashboard - Overview

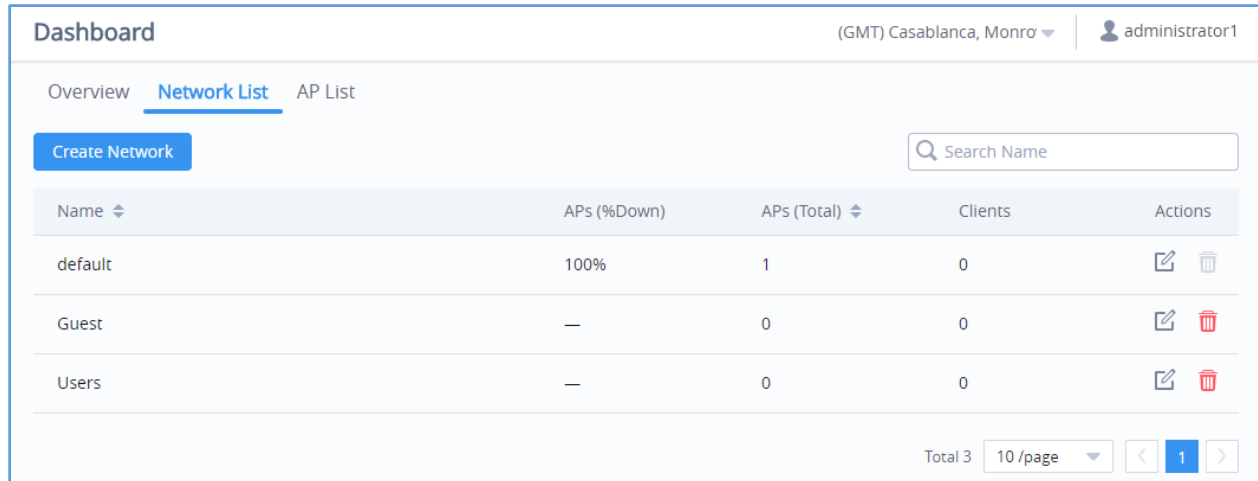
The following table describes each section:

Table 5: 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: <ul style="list-style-type: none"> • 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.

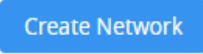
Network List

The Network List page displays different Network Groups created on your GWN.Cloud:



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

Figure 17: 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  button. A new page will popup, fill in the fields as show in previous figure to create a new network.

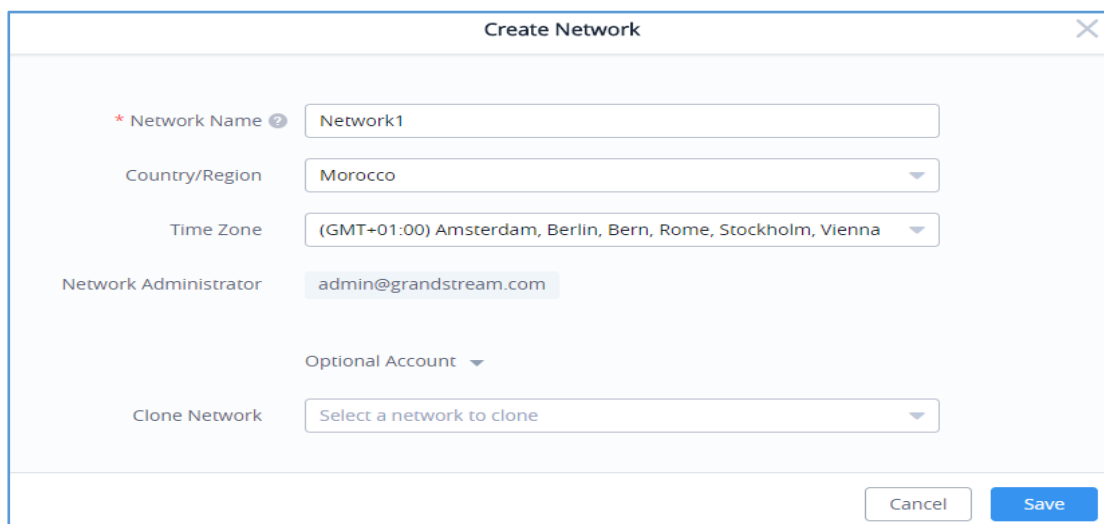


Figure 18: Create a New Network

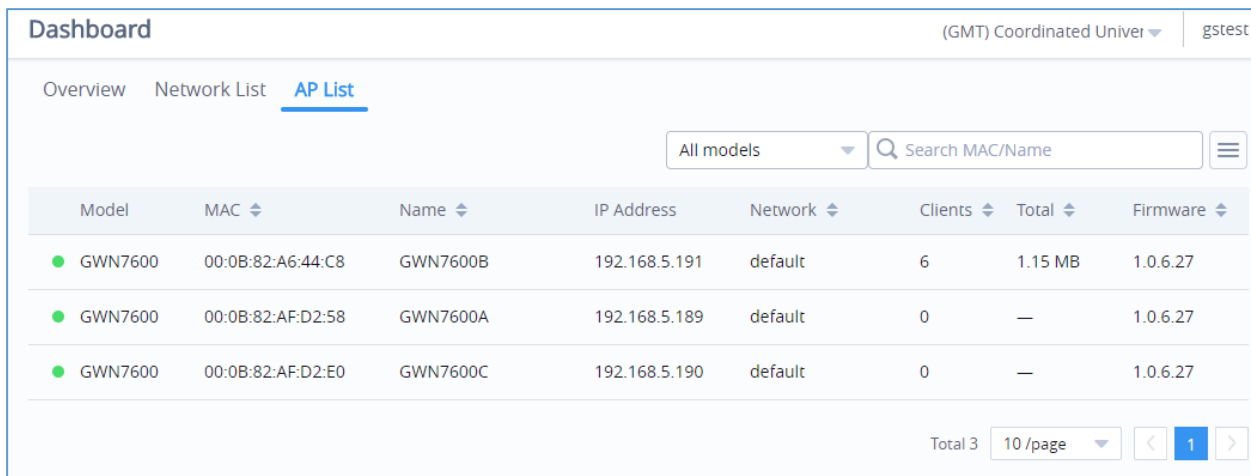
Table 6: Create a New Network Settings

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 GWN.Cloud Account.



The screenshot shows the GWN.Cloud Dashboard with the 'AP List' tab selected. The page header includes 'Dashboard', '(GMT) Coordinated Univer', and 'gstest'. The navigation menu shows 'Overview', 'Network List', and 'AP List'. A search bar is present with 'All models' and 'Search MAC/Name'. The main table lists three APs with columns for Model, MAC, Name, IP Address, Network, Clients, Total, and Firmware. The footer shows 'Total 3' and '10/page'.

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

Figure 19: GWN.Cloud Dashboard – AP List

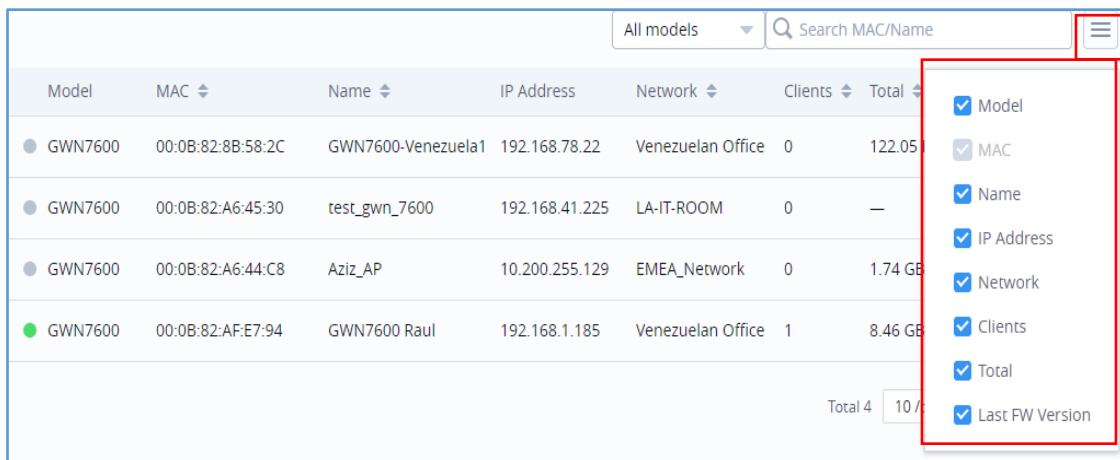
The AP List page provides also the following information regarding the Access point:

- 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:



Model	MAC	Name	IP Address	Network	Clients	Total
GWN7600	00:0B:82:8B:58:2C	GWN7600-Venezuela1	192.168.78.22	Venezuelan Office	0	122.05
GWN7600	00:0B:82:A6:45:30	test_gwn_7600	192.168.41.225	LA-IT-ROOM	0	—
GWN7600	00:0B:82:A6:44:C8	Aziz_AP	10.200.255.129	EMEA_Network	0	1.74 GB
GWN7600	00:0B:82:AF:E7:94	GWN7600 Raul	192.168.1.185	Venezuelan Office	1	8.46 GB
Total 4					10 /	

Figure 20: Customize AP List Table Fields

NETWORK

The network page provides an information regarding all the network groups created under your GWN.Cloud 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 GWN.Cloud account.

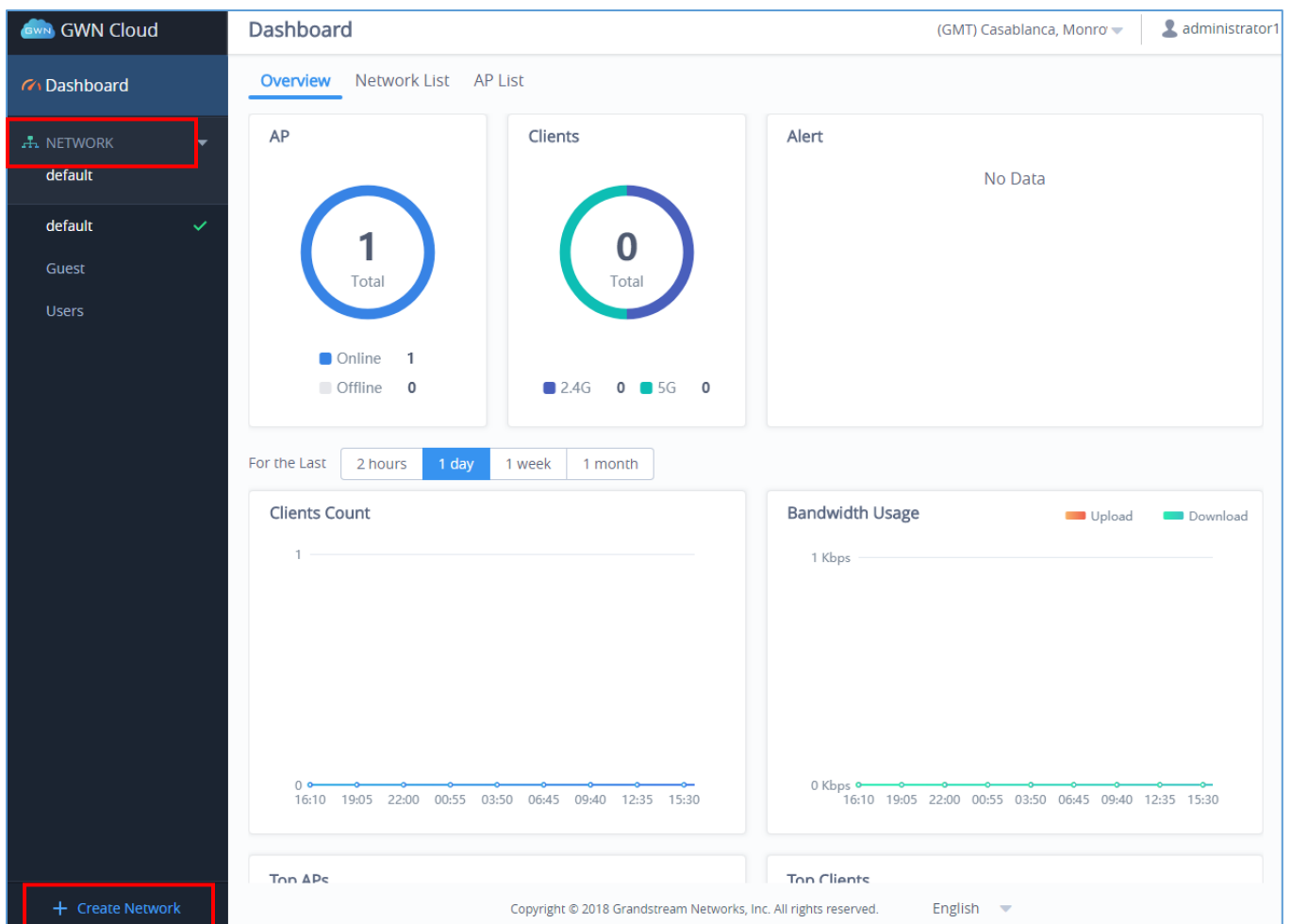


Figure 21: Network List and Network Creation Button

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

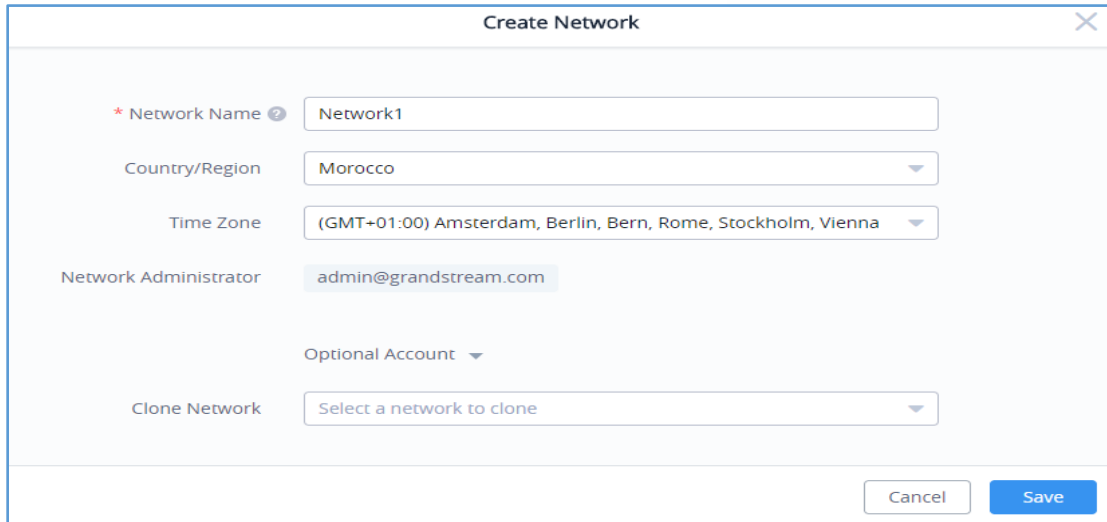


Figure 22: Create Network

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.

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 display 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

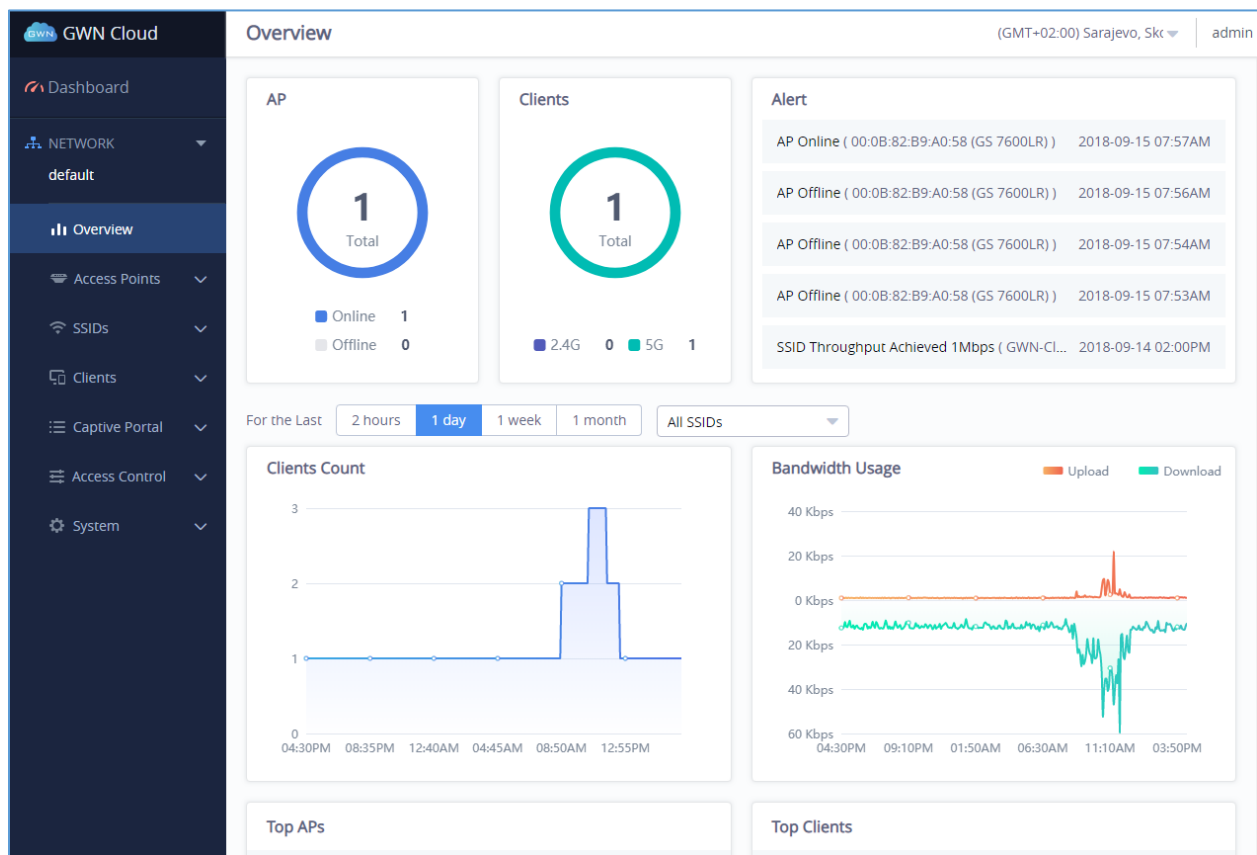


Figure 23: Overview Page Displays Information related to Specific Network

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.

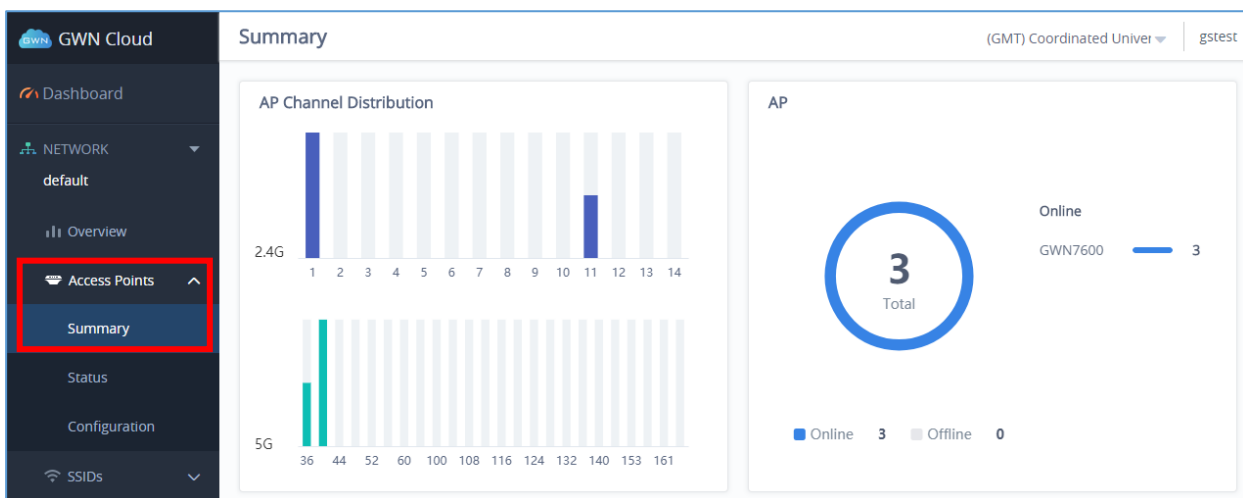


Figure 24: Access Points - Summary

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		<input type="text" value="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	  		

Figure 25: Access Points - Status

Figure 26: Access Points Status

Model	GWN Access Point Model (GWN7610, GWN7600 or GWN7600LR)
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:

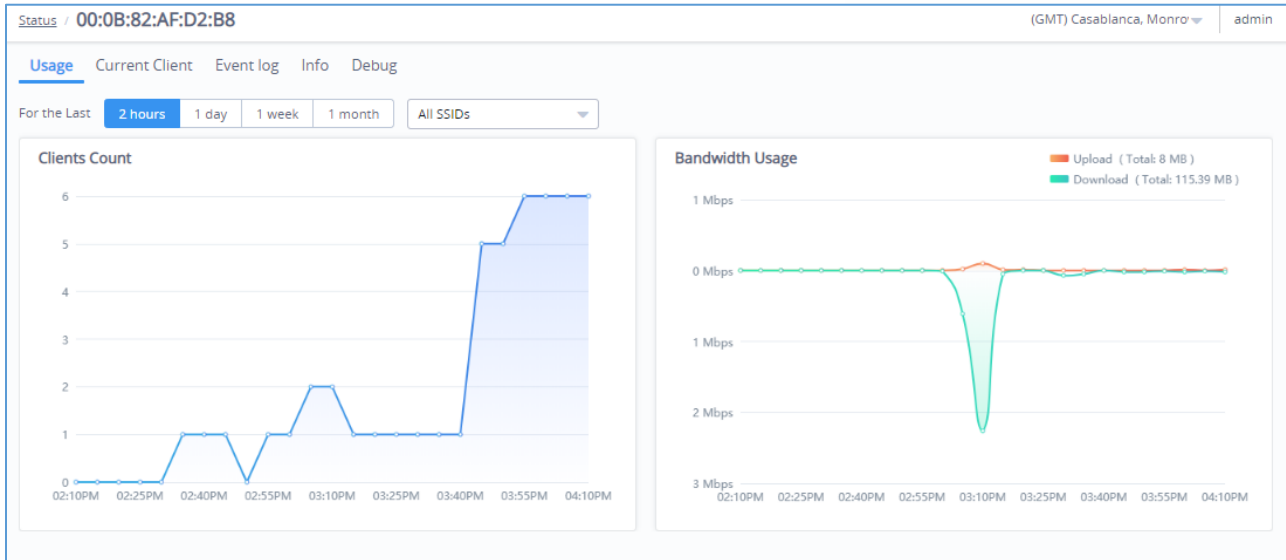
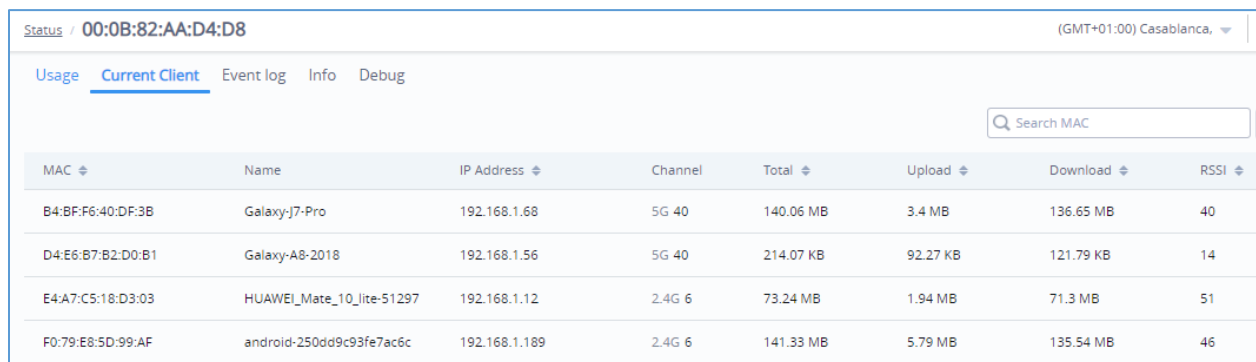


Figure 27: Usage of a Specific AP

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 2 hours, 1 day, 1 week 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 28: 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 WiFi password secret entered on client device.

Status / 00:0B:82:AF:D2:B8 (GMT) Casablanca, Monro ▼ | admin

Usage Current Client Event log Info Debug

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 29: Event Log per AP

The next tab “Info” shows detailed information about the select AP, such as the model, name, firmware version, memory used...etc.

Status / 00:0B:82:AA:D4:D8

Usage Current Client Event log **Info** Debug

MAC	00:0B:82:AA:D4:D8
Model	GWN7610
Part Number	9640000618A
Boot Version	1.0.0.1
Firmware Version	1.0.7.12
Network	default
IP Address	192.168.1.47
Uptime	2h 12m
SSID	LAB_EMEA
Client Bridge Mode	Disabled
Load Average	2.17 2.19 2.18
Link Speed	NET/POE 100 M/FD NET Disconnected
2.4G Radio Status	Channel 6 Clients Count 1 Tx Power (dBm) 20
5G Radio Status	Channel 40 Clients Count 0 Tx Power (dBm) 20
Memory Used	67 MB
CPU Temperature	—

Figure 30: 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 or 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 be used by engineering team for debugging purposes.

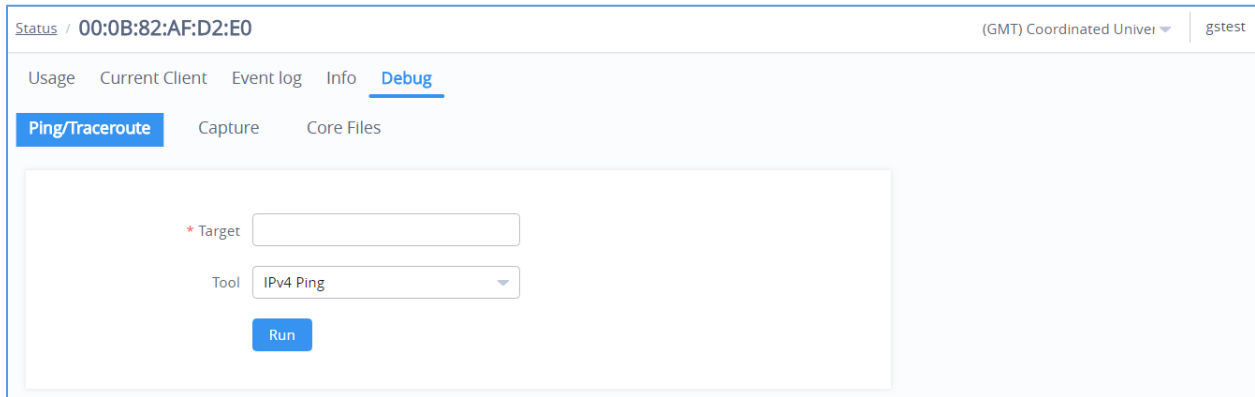
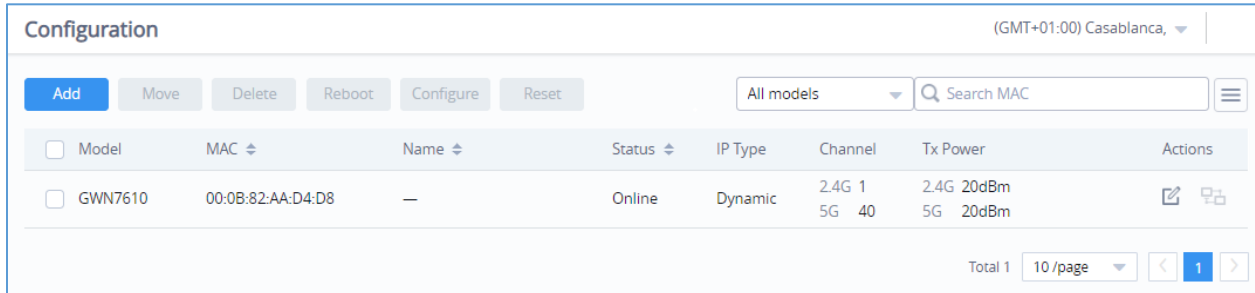


Figure 31: Debug Tool Tab

Configuration

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



The screenshot shows the 'Configuration' page for a network device. At the top right, it indicates '(GMT+01:00) Casablanca'. Below the title, there are several action buttons: 'Add', 'Move', 'Delete', 'Reboot', 'Configure', and 'Reset'. To the right of these buttons is a dropdown menu set to 'All models' and a search bar labeled 'Search MAC'. Below this is a table with the following columns: Model, MAC, Name, Status, IP Type, Channel, Tx Power, and Actions. One row is visible with the following data: Model: GWN7610, MAC: 00:0B:82-AA:D4:D8, Name: —, Status: Online, IP Type: Dynamic, Channel: 2.4G 1 / 5G 40, Tx Power: 2.4G 20dBm / 5G 20dBm. At the bottom right of the table, there is a pagination control showing 'Total 1' and '10/page'.

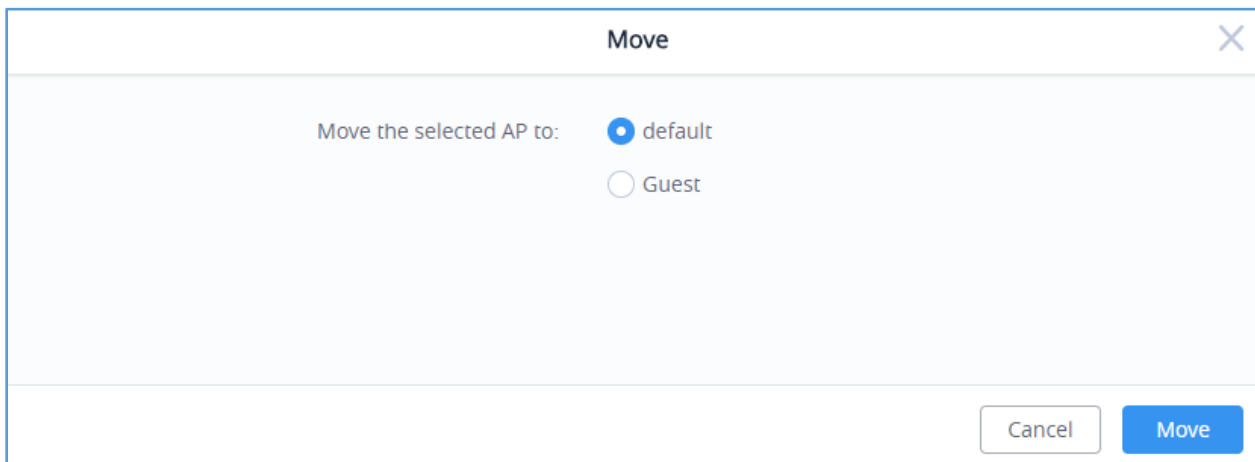
Figure 32: Access Points Configuration Page

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.

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.



The screenshot shows a 'Move' dialog box with a close button (X) in the top right corner. The text inside reads 'Move the selected AP to:'. Below this text are two radio button options: 'default' (which is selected) and 'Guest'. At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Move'.

Figure 33: 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:

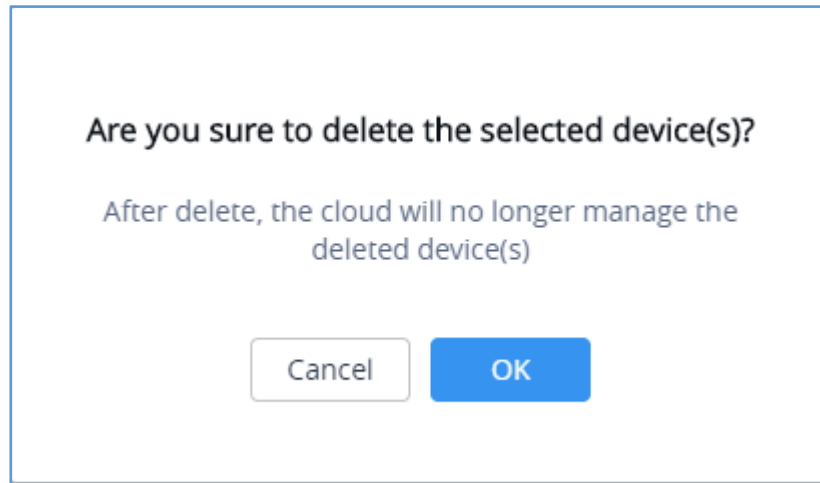




Figure 34: Delete Access Point

Click on  to confirm the operation, and the AP will be deleted.

Reboot Access Points

To reboot an Access point, select it then click on Reboot button, a confirmation message will be displayed, click on  to confirm the operation.

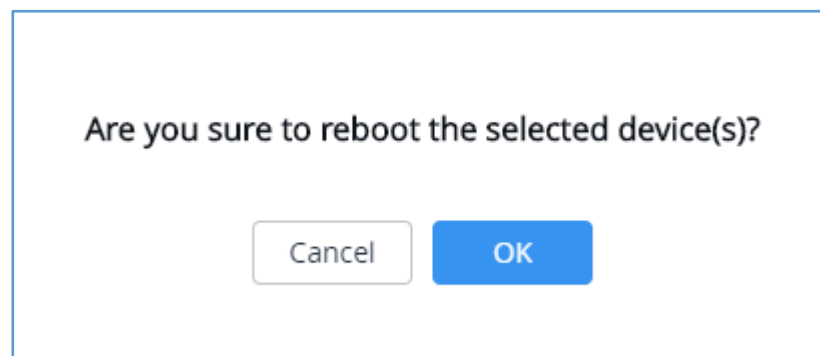


Figure 35: Reboot Access Point

Configure Access Points

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

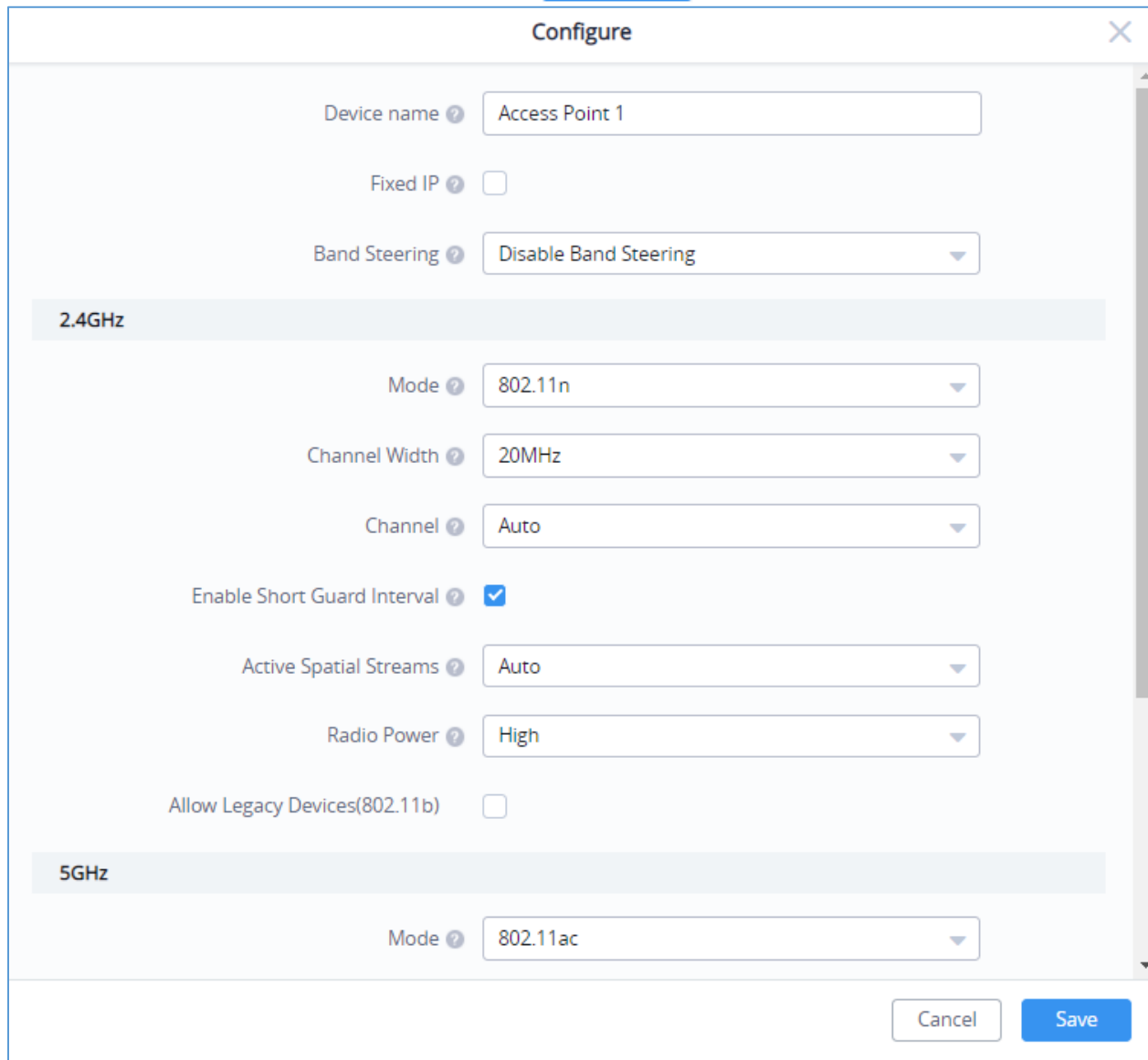


Figure 36: Access Point Configuration Page

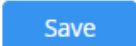
The following settings can be configured from this page:

Table 8: 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.

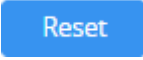

Band Steering	<p>Band Steering will help redirecting clients to a radio band 2.4G or 5G, depend on what's supported by the device, for efficient use and to benefit from the maximum throughput. Four options are allowed by GWN.Cloud:</p> <ul style="list-style-type: none"> • Disable Band steering: This 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: 2G Band will be prioritized over 5G Band • Balance: GWN will balance between the clients connected to 2G and those connected to 5G.
Mode	Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.
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.
Channel	Select "Auto" or a specific channel. Default is "Auto". Note that the proposed channels depend on Country Settings under System → Settings .
Enable Short Guard interval	Check to activate this option to increase throughput.
Active Spatial streams	Choose active spatial stream. Available options: "Auto", "1 stream" and "2 streams".
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/GHz 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.
Allow Legacy Devices(802.11b)	This feature appears when "Mode" option is set to "802.11g" or "802.11n", it allows legacy devices not supporting "802.11g/n" mode to connect using the "802.11b" mode.

Notes:

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



Reset Access Points

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

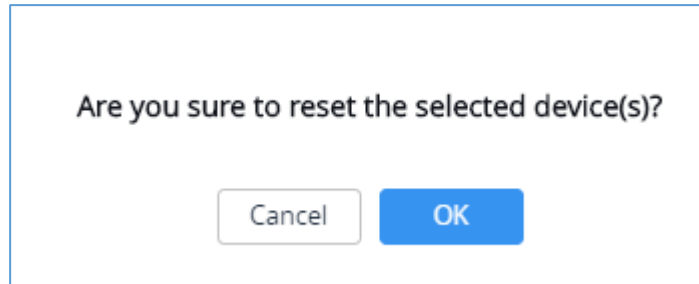


Figure 37: Reset Access Point

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.

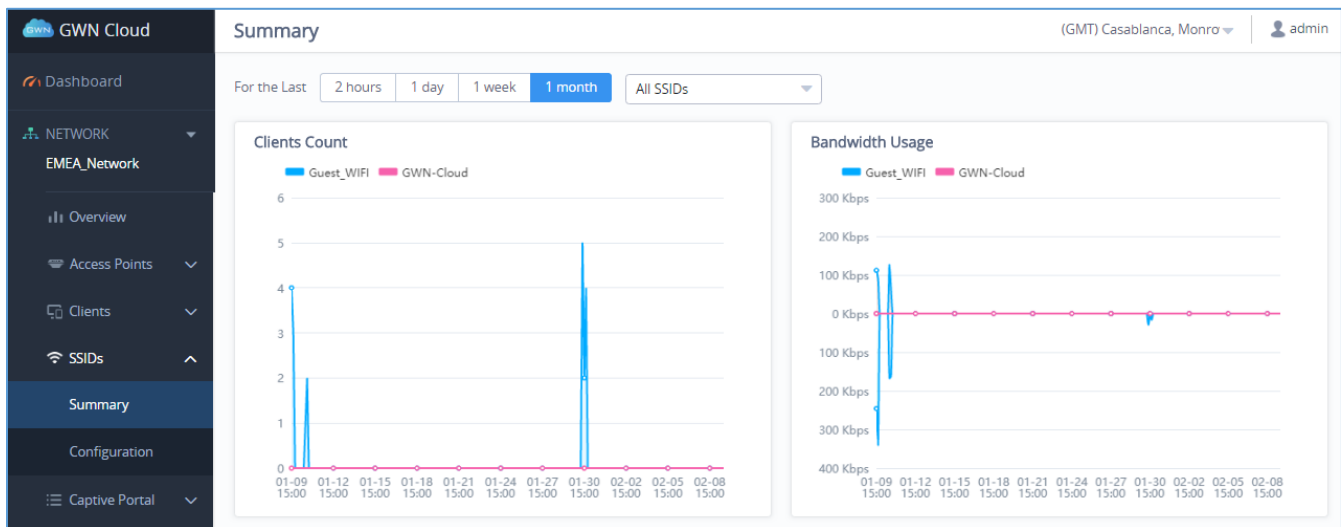
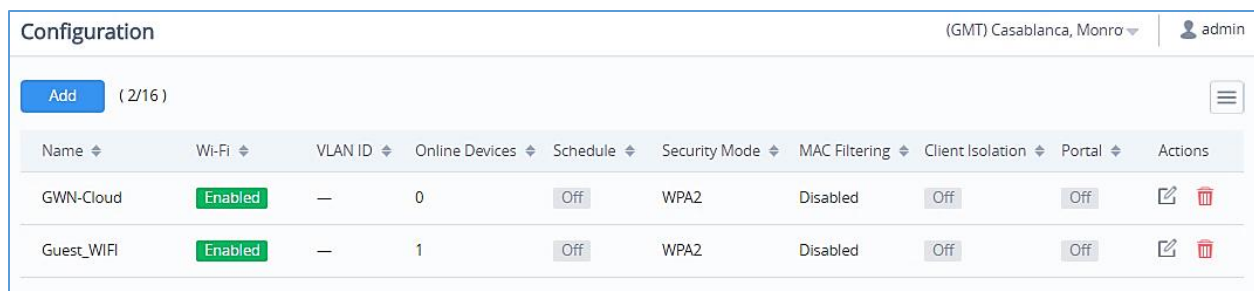


Figure 38: SSIDs - Summary

Configuration

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







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 39: 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.

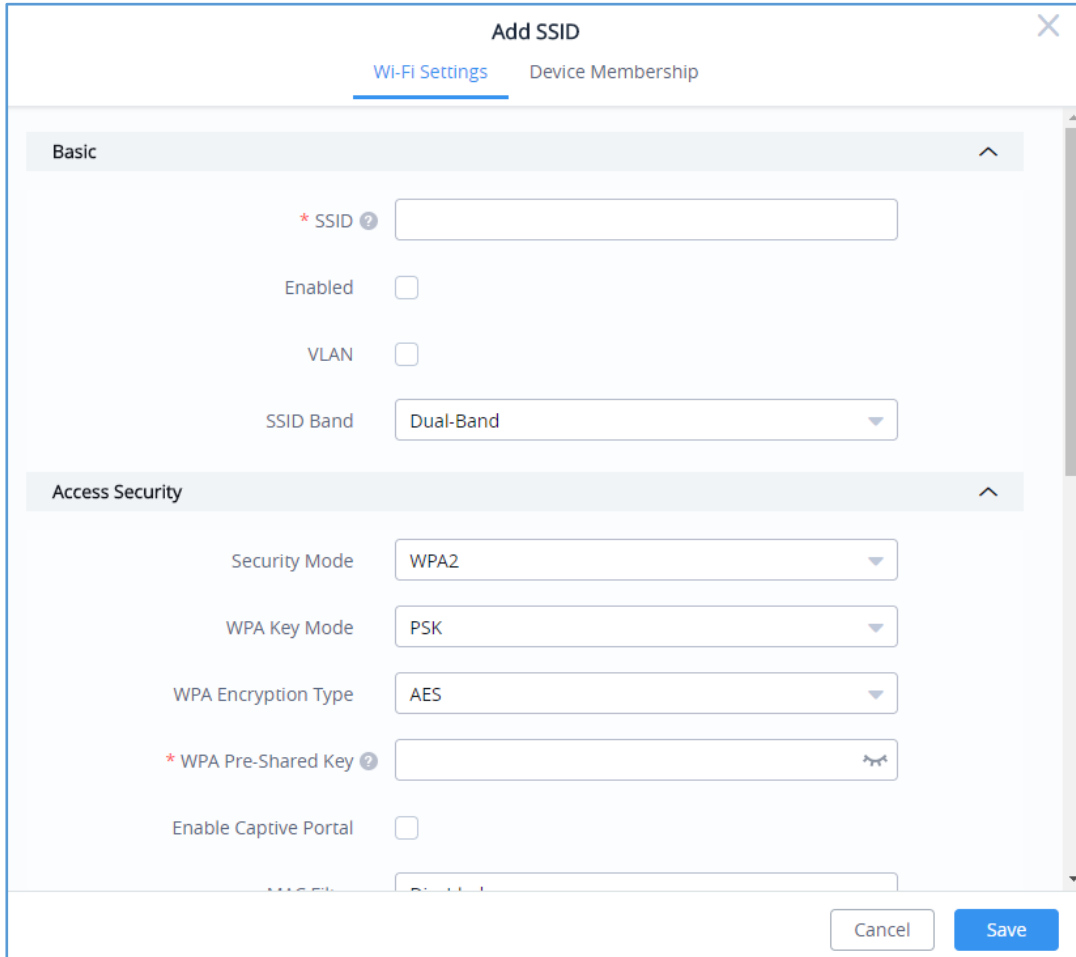


Figure 40: SSIDs – Configuration – Wi-Fi Settings

Table 9: 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: <ul style="list-style-type: none"> • Dual-Band • 2.4GHz • 5GHz

Security Mode	<p>Set the security mode for encryption, 5 options are available:</p> <ul style="list-style-type: none"> • 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. • Open: No password is required. Users will be connected without authentication. Not recommended for security reasons.
WEP Key	<p>Enter the password key for WEP protection mode.</p> <p>This option is available when selecting WEP64-bit/WEP128-bit as Security Mode</p>
WPA Key Mode	<p>Select key mode (Pre-Shared Key or 802.1X Authentication).</p>
WPA Encryption Type	<p>Select Encryption type (AES or AES/TKIP).</p>
WPA Pre-Shared Key	<p>Configures the WPA pre-shared key. The input range: 8-63 ASCII characters or 8-64 hex characters.</p> <p>This option is available when selecting PSK as WPA Key Mode.</p>
RADIUS Sever Address	<p>Configures RADIUS authentication server address.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
RADIUS Server Port	<p>Configures RADIUS Server Listening port (defaults to 1812).</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
RADIUS Server Secret	<p>Enter the secret password for client authentication with RADIUS server.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
RADIUS Accounting Server Address	<p>Configures the address for the RADIUS accounting server.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
RADIUS Accounting Server Port	<p>Configures RADIUS accounting server listening port (Default is 1813).</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>



RADIUS Accounting Server Secret	<p>Enter the secret password for client authentication with RADIUS accounting server.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
RADIUS NAS ID	<p>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.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
Enable Captive Portal	<p>Click on the checkbox to enable the captive portal feature.</p>
Captive Portal Policy	<p>Select the captive portal policy already created on the “CAPTIVE PORTAL” web page to be used in the created SSID.</p>
MAC Filter	<p>Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to Wi-Fi. Default is Disabled.</p>
Enable Dynamic VLAN	<p>When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile.</p> <p>This option is available when selecting 802.1x as WPA Key Mode.</p>
Client Isolation	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>This field is required when using Client Isolation, so users will not lose access to the Network (usually Internet).</p> <p>Type in the default LAN Gateway’s MAC address (router’s MAC address for instance) in hexadecimal separated by “:”.</p> <p>Example: 00:0B:82:8B:4D:D8</p>



SSID Hidden	<p>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.</p>
Beacon Interval	<p>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...</p> <ul style="list-style-type: none"> • 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. <p>Notes:</p> <ol style="list-style-type: none"> 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. <p>Default value is 100ms. Valid range: 40 – 500 ms.</p>
DTIM Period	<p>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.</p> <p>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.</p> <p>Valid range: 1 – 10.</p>
Wireless Client Limit	<p>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.</p>



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 in to 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 Voice Enterprise	<p>Enable this feature to help clients connected to the GWN76xx to perform better roaming decision.</p> <ul style="list-style-type: none"> • 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.



	<p>Note: 11R is required for enterprise audio feature, 11V and 11K are optional.</p> <p>Enable Voice Enterprise is only available under “WPA/WPA2” and “WPA2” Security Mode.</p>
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.

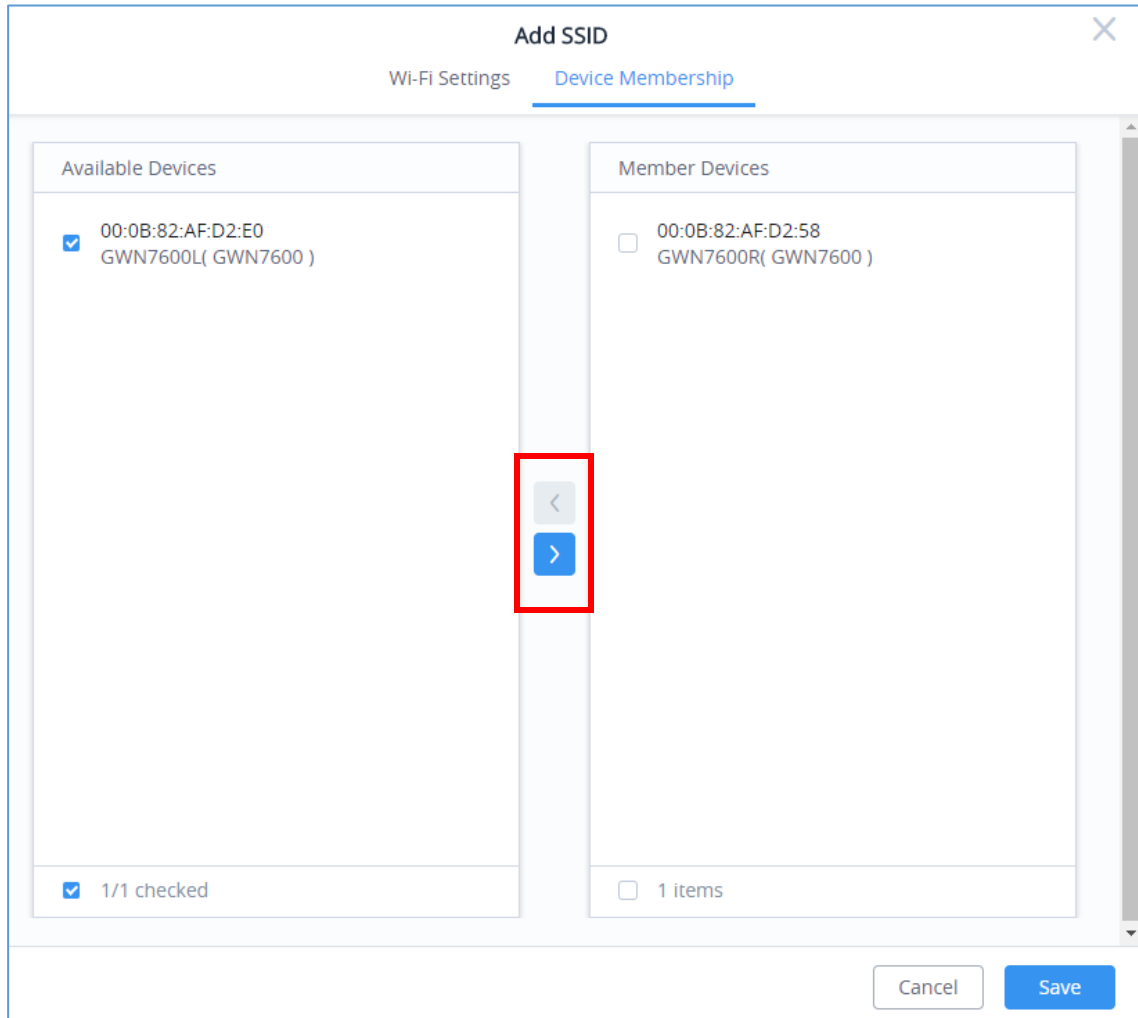



Figure 41: Device Membership - Available Devices

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

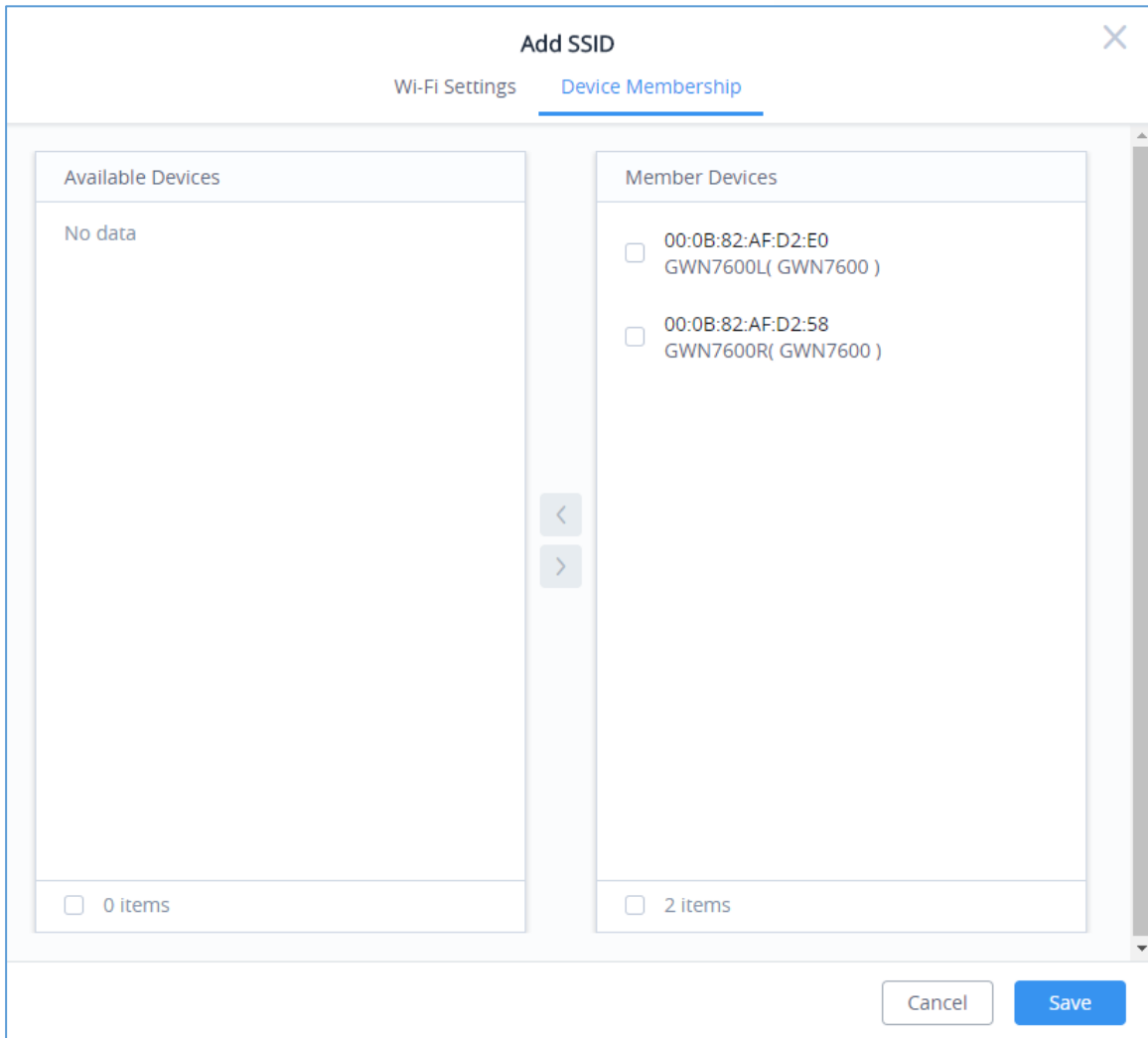


Figure 42: Device Membership - Members Devices

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, GWN.Cloud 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.

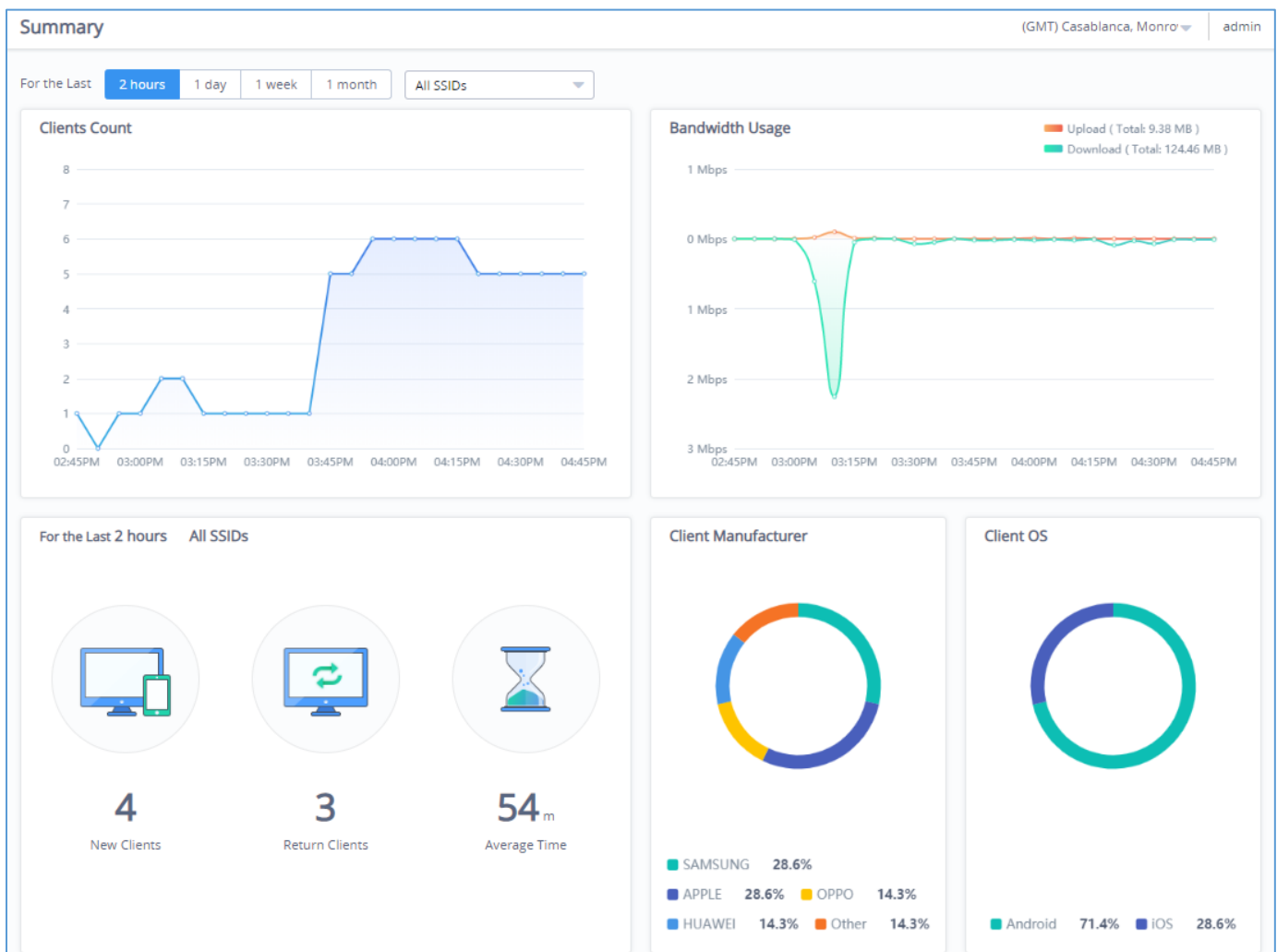


Figure 43: Clients - Summary

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 Page

The status page allows GWN.Cloud 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 44: Clients Status

- 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 black list 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:

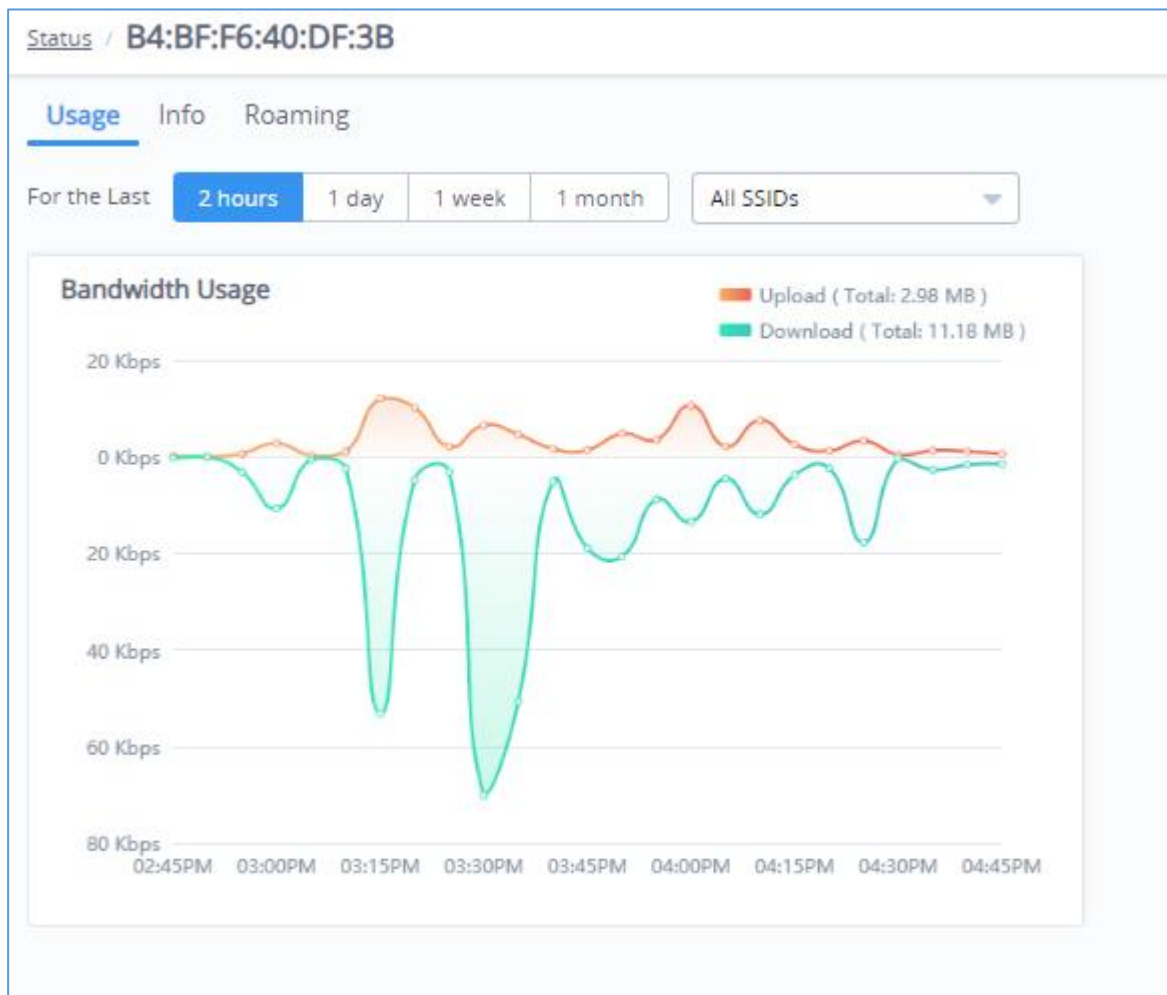


Figure 45: Client Data Usage Info

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

Status / D0:31:69:1C:64:03 (GMT) Coordinated Univer ▼ gstest

Usage **Info** Roaming

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 46: 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 47: Client Roaming

CAPTIVE PORTAL

Captive Portal feature on GWN.Cloud 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 GWN.Cloud 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.

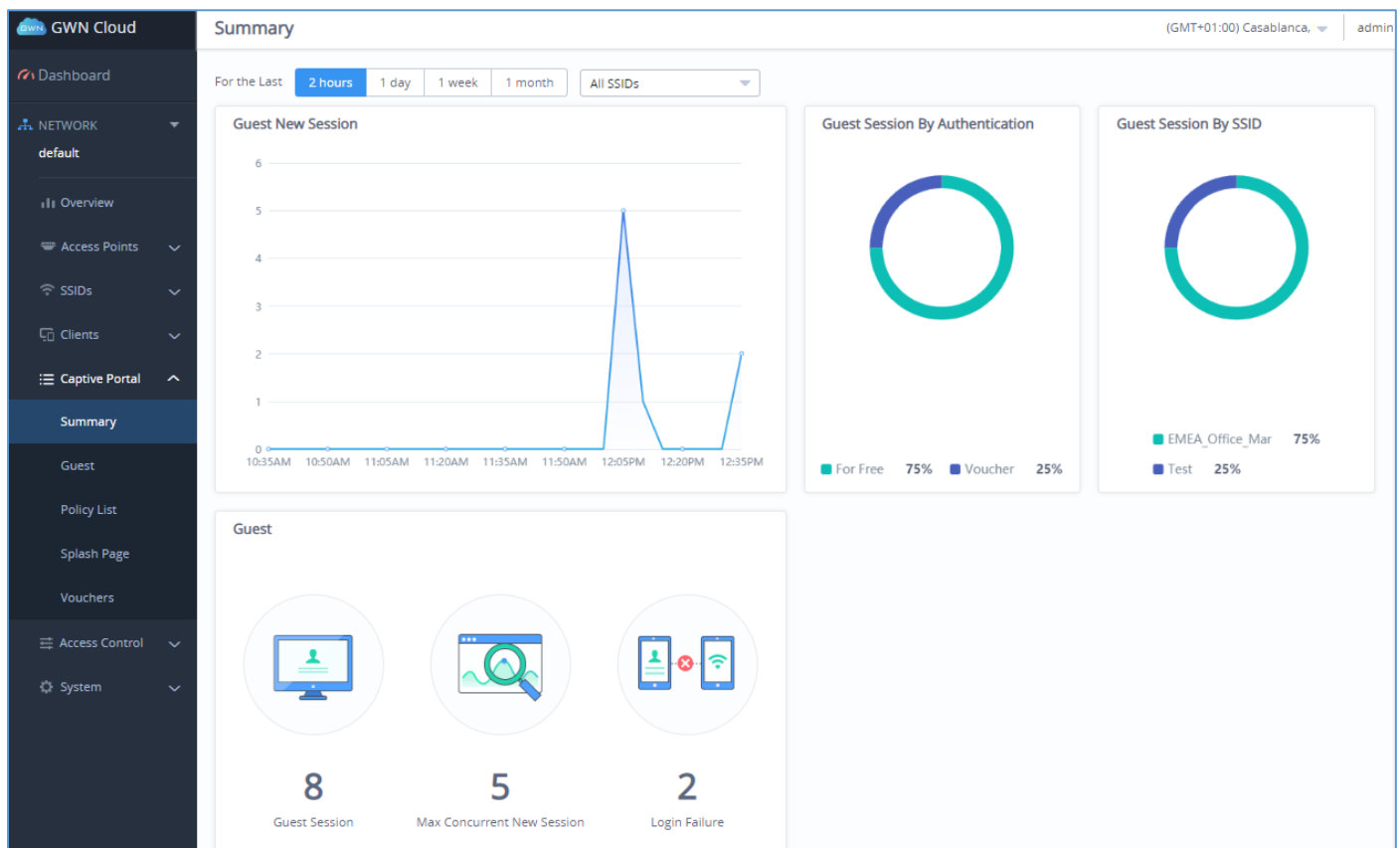


Figure 48: Captive Portal Summary

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.

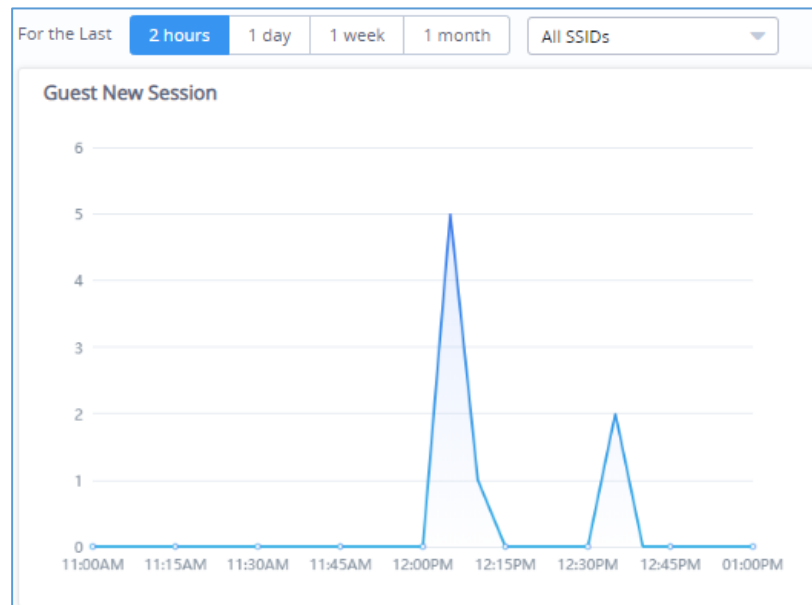


Figure 49: Guest New Session

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...).

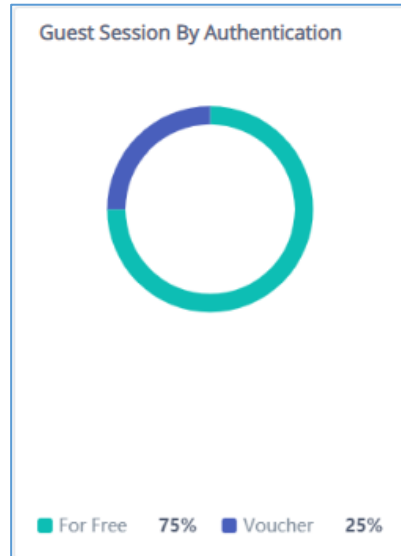


Figure 50: Guest Session by Authentication

Guest Session by SSID

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



Figure 51: 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.

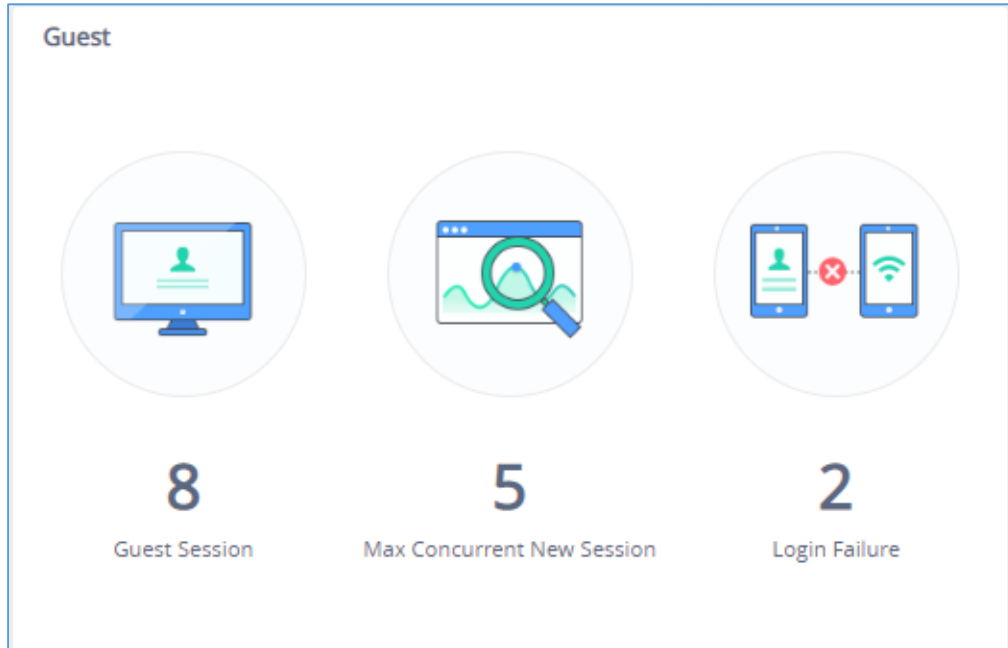
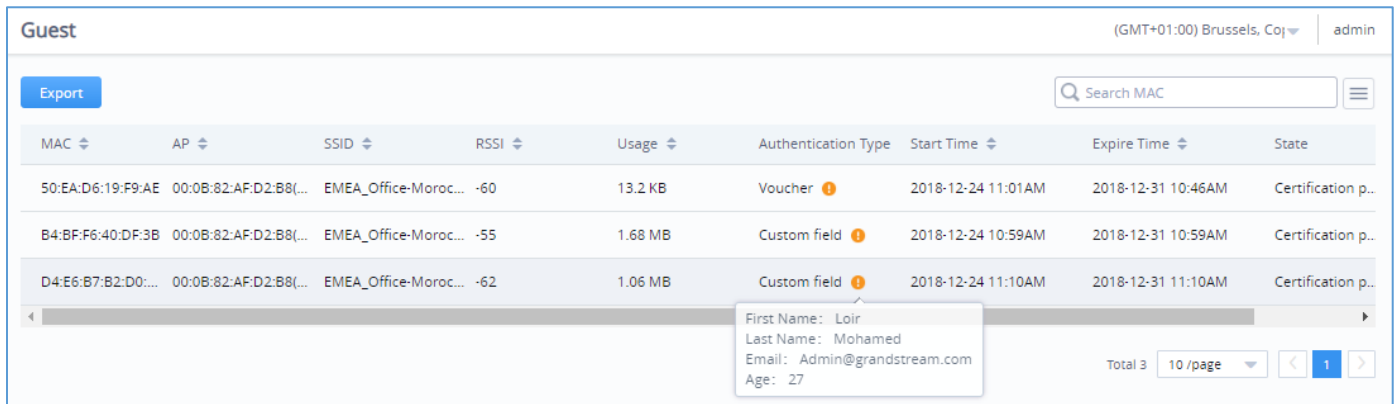


Figure 52: Guest Section

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	Usage	Authentication Type	Start Time	Expire Time	State
50:EA:D6:19:F9:AE	00:08:82:AF:D2:B8(...)	EMEA_Office-Moroc...	-60	13.2 KB	Voucher	2018-12-24 11:01AM	2018-12-31 10:46AM	Certification p..
B4:BF:F6:40:DF:3B	00:08:82:AF:D2:B8(...)	EMEA_Office-Moroc...	-55	1.68 MB	Custom field	2018-12-24 10:59AM	2018-12-31 10:59AM	Certification p..
D4:E6:B7:B2:D0:...	00:08:82:AF:D2:B8(...)	EMEA_Office-Moroc...	-62	1.06 MB	Custom field	2018-12-24 11:10AM	2018-12-31 11:10AM	Certification p..

Figure 53: Captive Portal Status

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

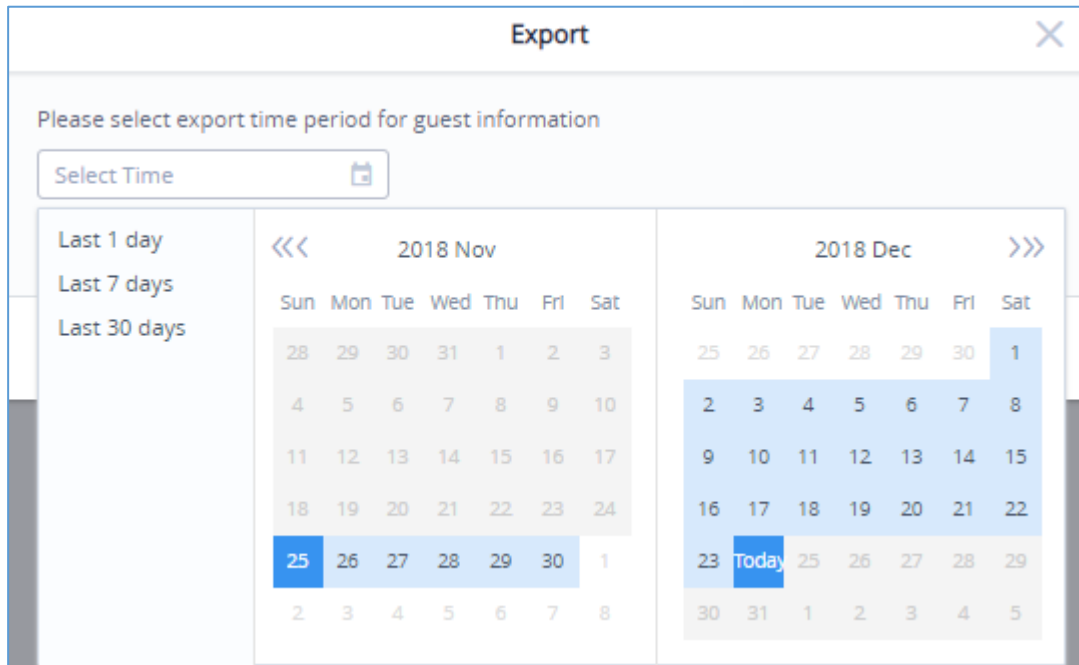



Figure 54: Export Guest Information Period

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.

✕
Add Portal Policy

* Name ?

Splash page

* Expiration ? day(s) hour(s) minute(s)

Failsafe Mode ?

Daily Limit ?

* Splash Page Customization ?

Landing Page ?

Enable HTTPS ?

Pre Authentication Rule (s) ?

+ Add New Authentication Rule

Post Authentication Rule (s) ?

+ Add New Authentication Rule

Figure 55: Add/Edit Captive Portal Policy

Internal Splash Page

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

Table 10: 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.

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: <ul style="list-style-type: none"> • 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.
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 11: 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: <ul style="list-style-type: none"> • Linkyfi Platform(https://www.avsystem.com/products/linkyfi) • Purple Platform (https://purple.ai/)



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. <i>This field appears only when Platform is set to "Linkyfi Platform".</i>
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 New Page.

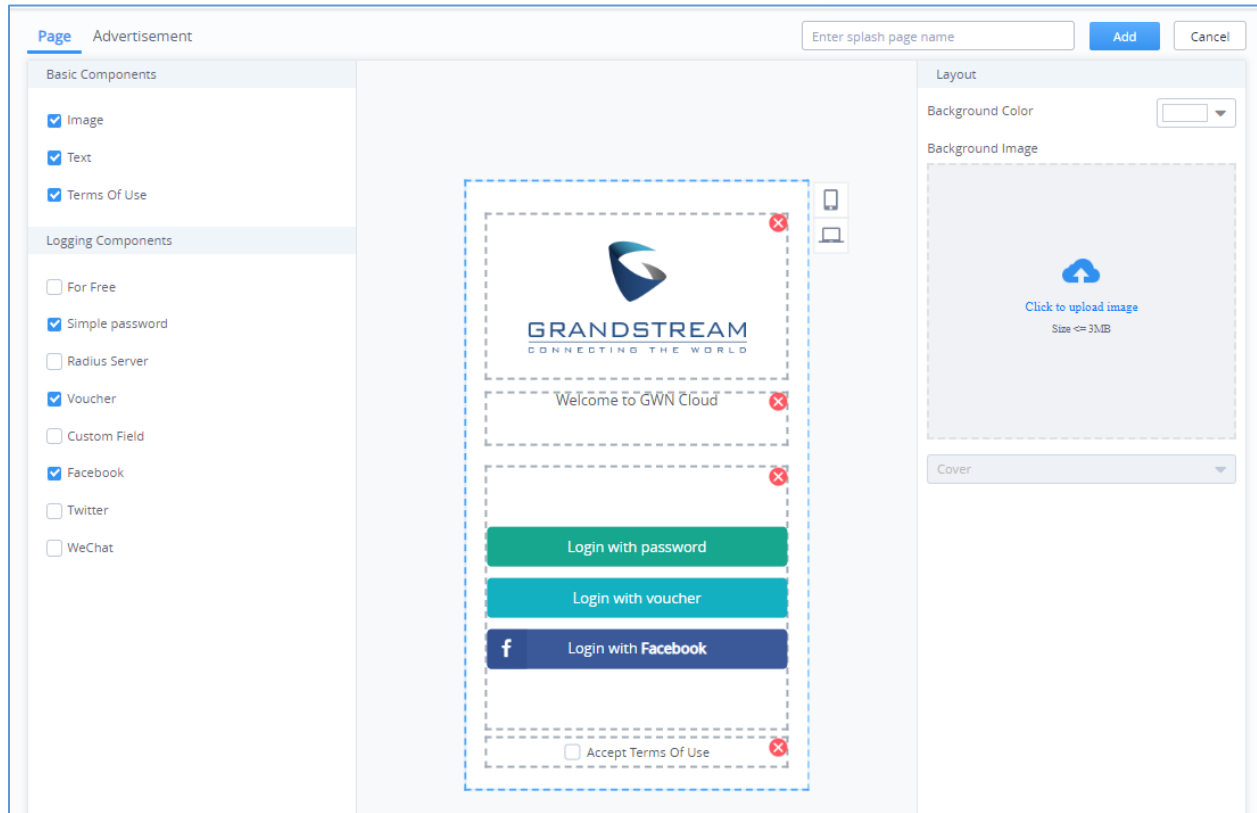


Figure 56: Create New Splash Page

2. Next, under “Logging” 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, WeChat, Radius Server, For Free or Custom Field)

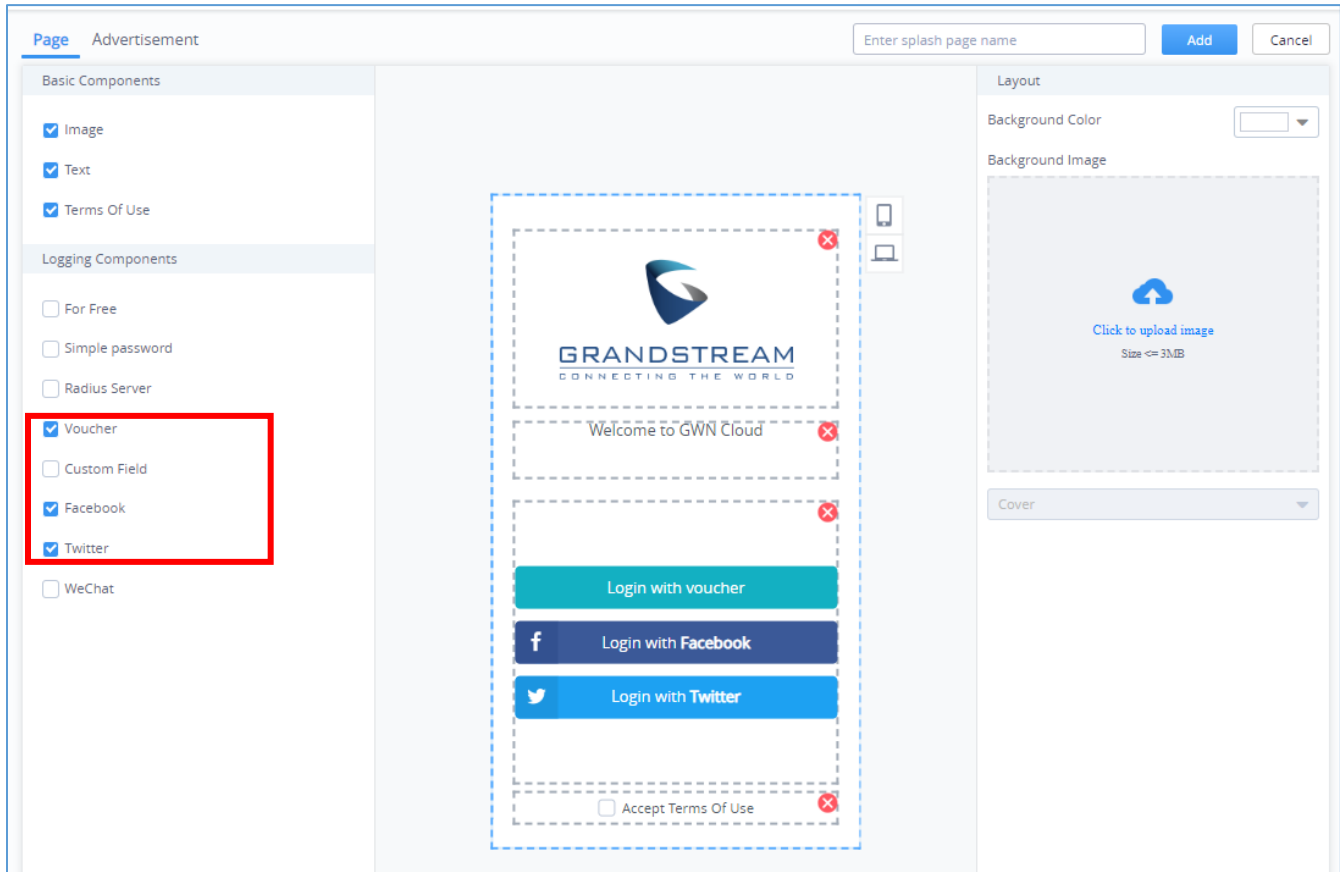
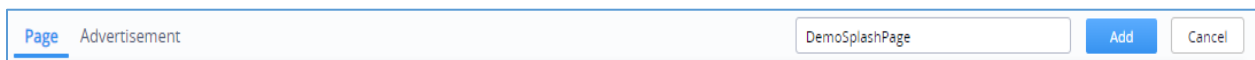


Figure 57: Setup Logging Methods - Splash Page

3. At this stage, 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).
4. Give the page a name at the top of the screen and click on **Add**.



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](#)

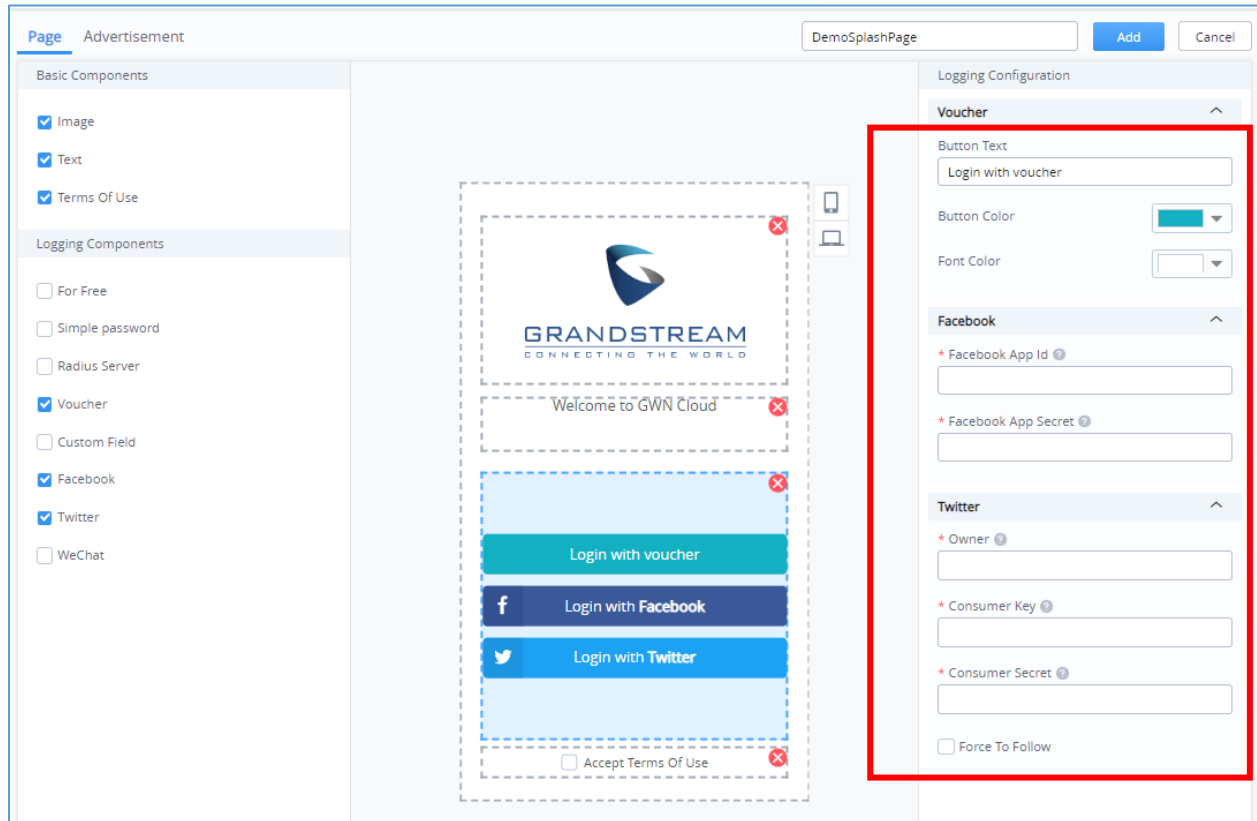




Figure 58: Setup Social Logging Parameters

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, click 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.

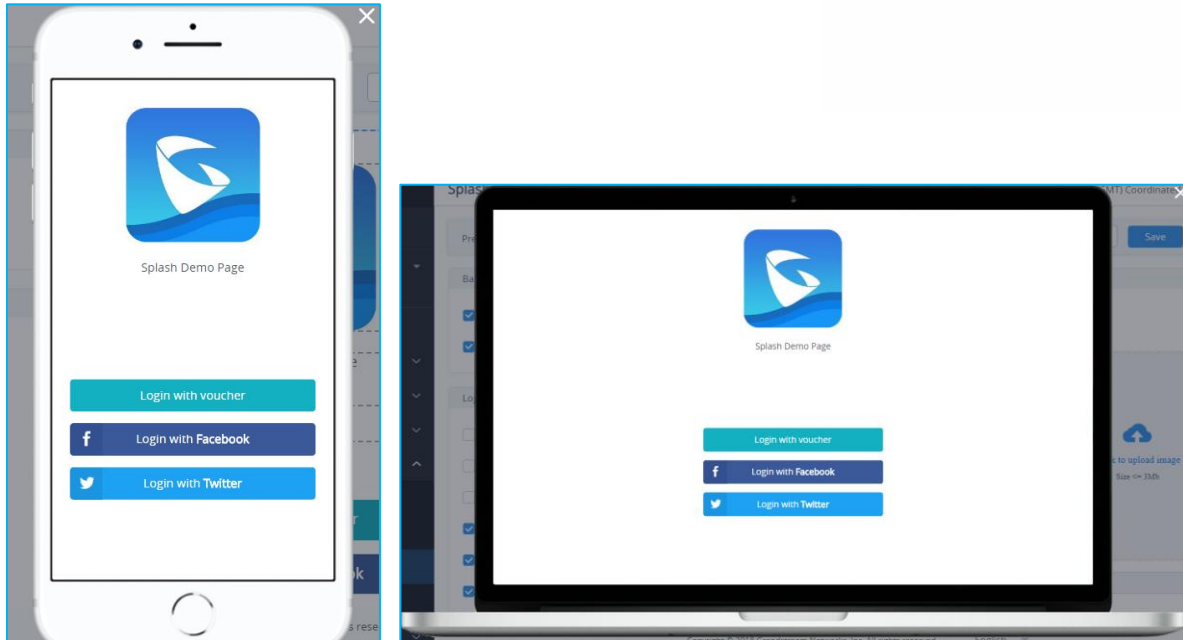


Figure 59: Splash Page Preview

7. If you are satisfied with the final product, then click on **Add** and after the page has been added to it will be displayed along other existing pages, and it's possible to edit it or delete it.

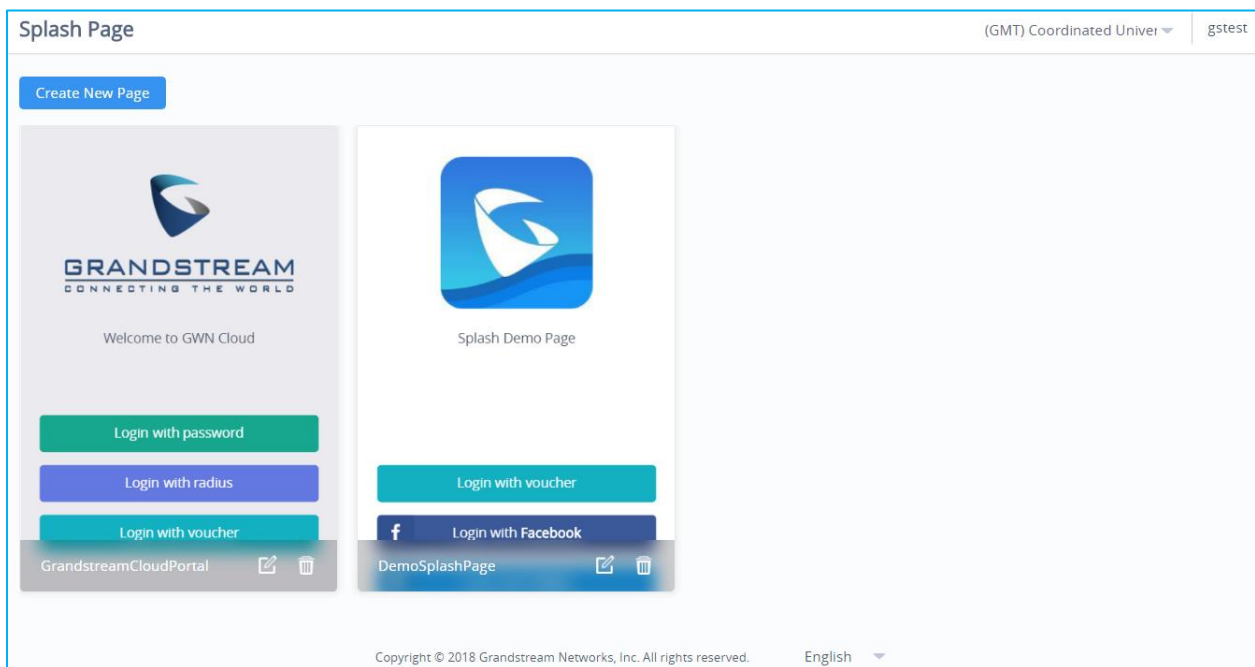


Figure 60: Splash Pages List

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

Below is a sample splash page that the user got when trying to connect to the Wi-Fi:

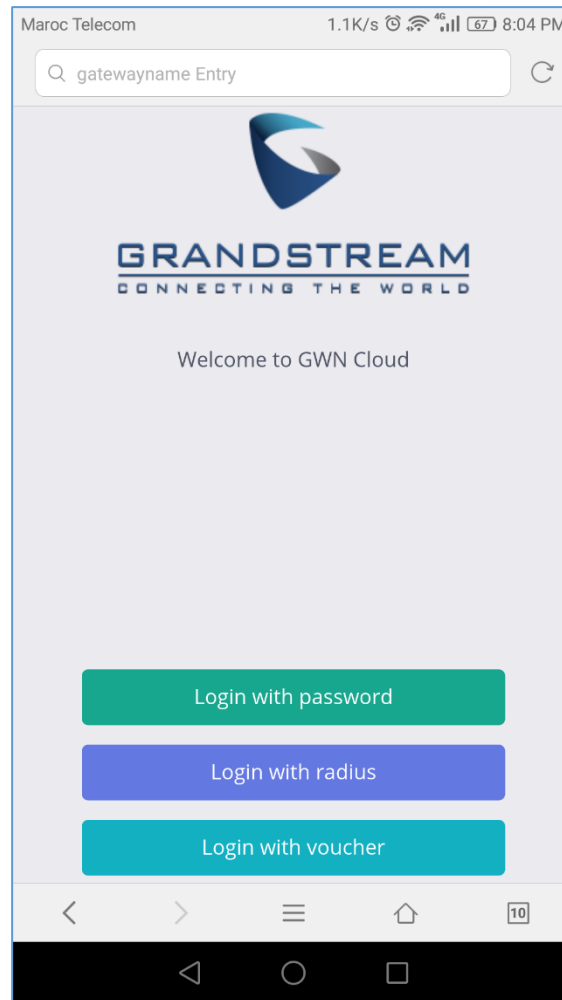


Figure 61: Portal Splash Page

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**” then click on **Enable Advertisement**.



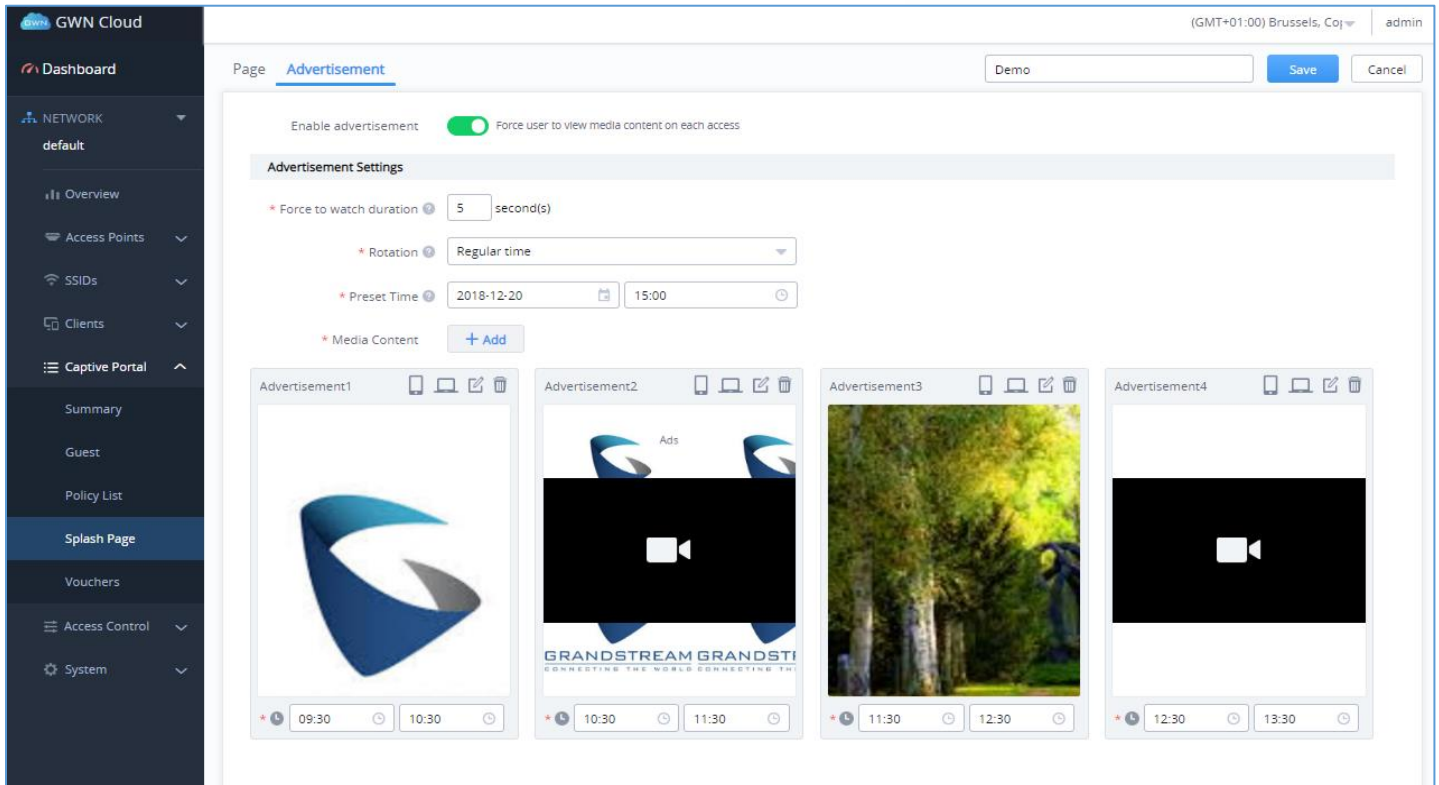
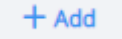


Figure 62: Advertisement Page



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

Table 12: 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. <ul style="list-style-type: none"> • 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  button to add Image/Video content Notes: <ul style="list-style-type: none"> The video content should not exceed 5 MB Video format only supports MP4 in H.264 codec When playing ads with multiple images, it will automatically switch every 3 seconds.
----------------------	--

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 GWN.Cloud 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 ?

* Quantity ?

* Max Devices ?

* Duration ? day(s) hour(s) minute(s)

Upload Limit(Kbps) ?

Download Limit(Kbps) ?

Byte Quota(MB) ?

* Validity Time ? day(s)

Notes ?

Figure 63: Adding Vouchers

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

Table 13: 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.)
Max Devices	Specify how many users can connect using the same voucher code.
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.

- Click on Save to generate the Vouchers.
- 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.

Vouchers / Voucher20180914153655 (GMT+01:00) Casablanca, ▾

All ▾

Password	Status	Validity Time ↕	Device Quota	Actions
1204000220	Unused	2018-12-13 02:37PM	0/1	 
1805010219	Unused	2018-12-13 02:37PM	0/1	 
1801090218	Unused	2018-12-13 02:37PM	0/1	 
1206040217	Unused	2018-12-13 02:37PM	0/1	 
1804030216	Unused	2018-12-13 02:37PM	0/1	 
1405000215	Unused	2018-12-13 02:37PM	0/1	 
1206030214	Unused	2018-12-13 02:37PM	0/1	 
1503000213	Unused	2018-12-13 02:37PM	0/1	 
1802080212	Unused	2018-12-13 02:37PM	0/1	 
1404090211	Unused	2018-12-13 02:37PM	0/1	 



Total 10   1

Figure 64: Voucher Details

This page displays the vouchers status as used/unused, the date of expiry and how many devices used the voucher if multi-user is enabled when setting the voucher parameters.

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.

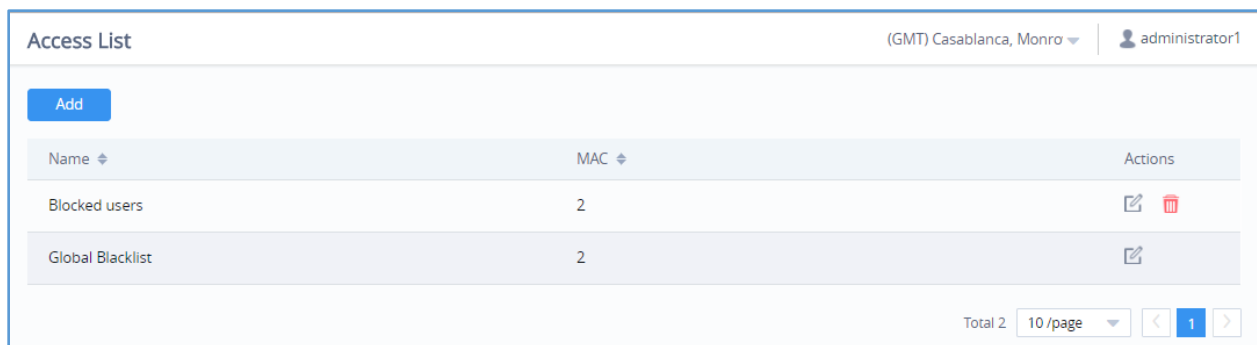


Figure 65: Access List

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:

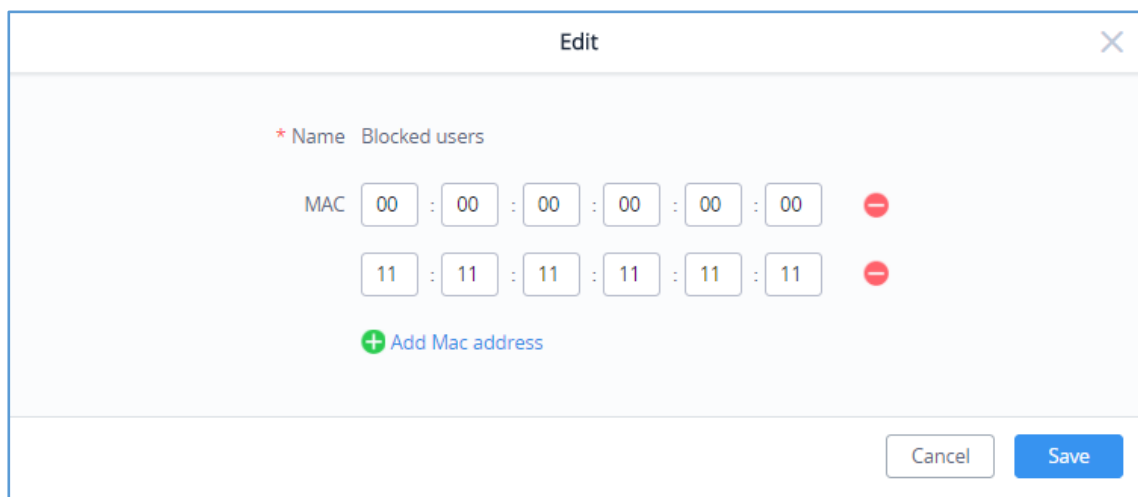


Figure 66: Adding New Clients to Access List

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.

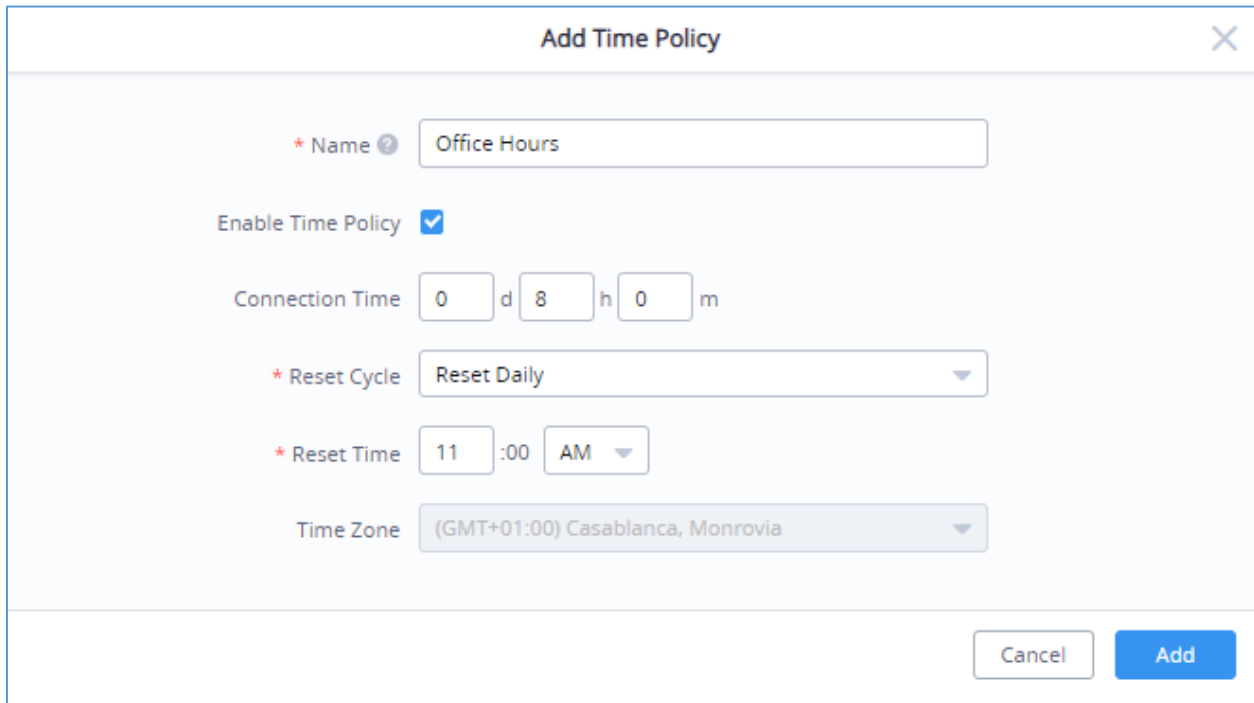


Figure 67: Add Time Policy List

Bandwidth rules

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

This option can be configured from the GWN.Cloud under “Bandwidth Rules”.


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

Table 14: Bandwidth Rules

Field	Description
SSID	Select the SSID to which the limitation will be applied.

Range Constraint	<ul style="list-style-type: none"> • 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

Schedule

* MAC : : : : :

* Please fill in at least one of the following items

Upstream Rate

Downstream Rate

Figure 68: MAC Address Bandwidth Rule

SYSTEM

Refer to the following tables for system page options.

Settings

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

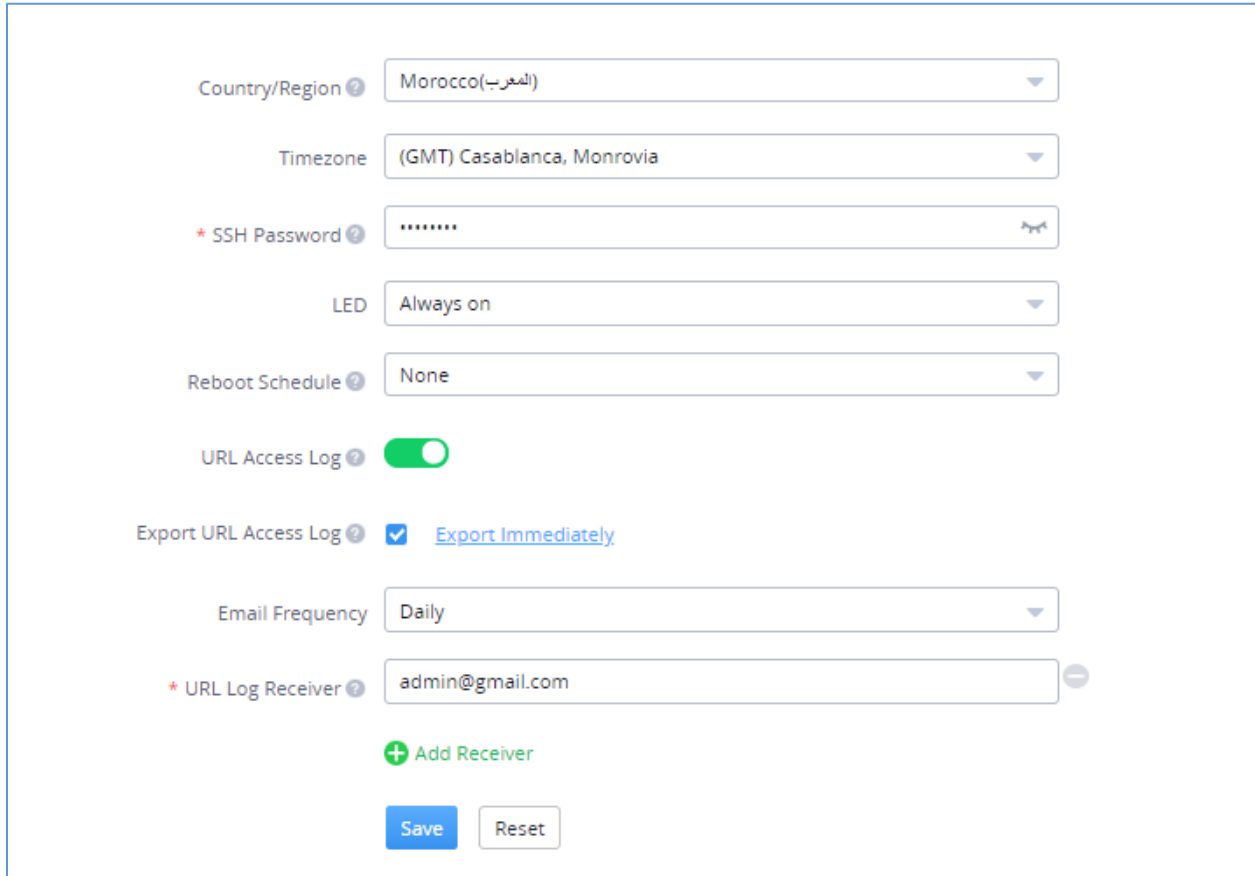


Figure 69 :System Settings

Table 15: Settings

Field	Description
Country	Select the country 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.
URL Access Log	Once enabled, the GWN Cloud will record the URL access log from the clients. Note: Currently, it is only supported with paired GWN7600/GWN7600LR access points.
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.

URL Access Log

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

The GWN.Cloud 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.Cloud 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**.



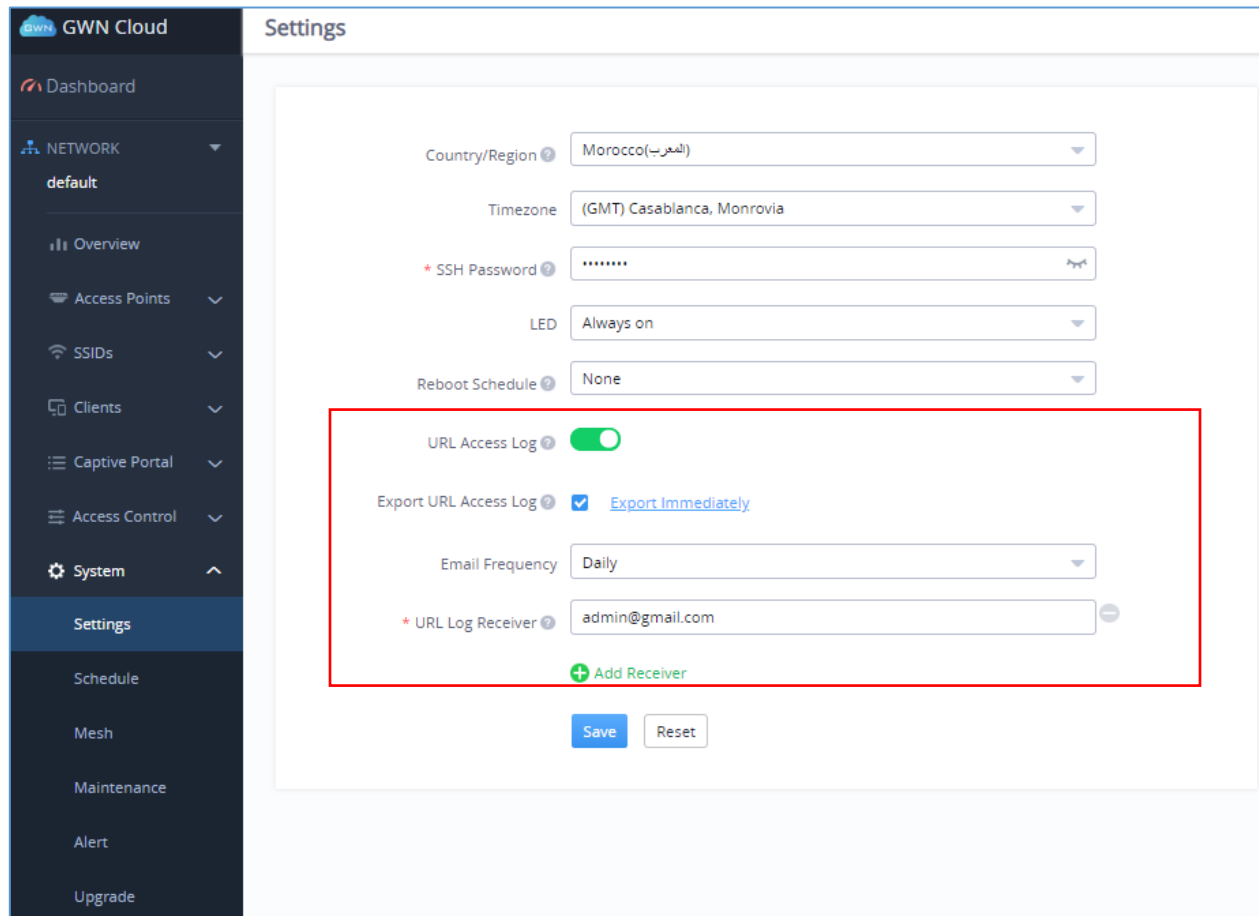


Figure 70: URL Access Log Settings

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.

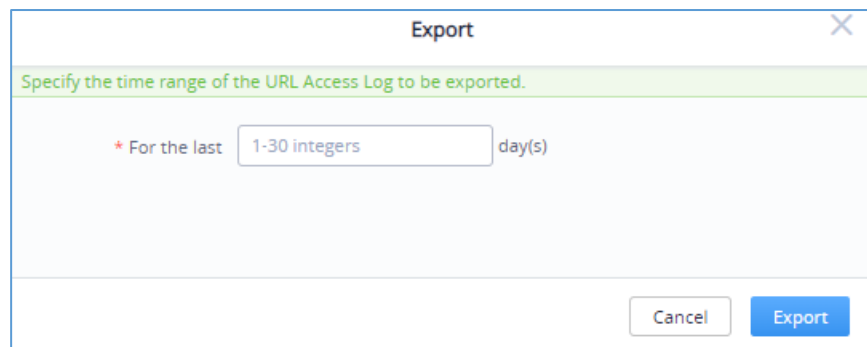


Figure 71: Export Immediately

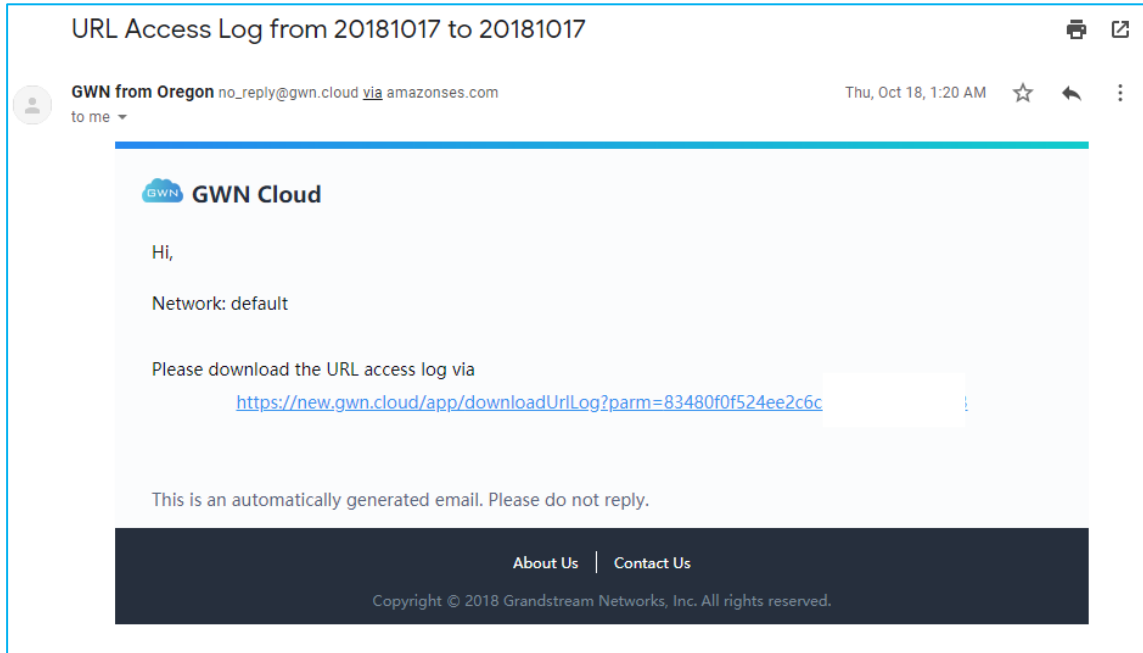


Figure 72: URL Access Log Email

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

This 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.

	A	B	C	D	E	F	G	H	I	J
1	AP MAC	MAC	hostname	User	Source IP	Destination IP	URL	HTTP	Hit Time	
2	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	172.217.18.238	http://clients3.google.com/generate	GET	2018-10-16 10:12AM	
3	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	52.49.102.93	https://api.samsungcloud.com		2018-10-16 10:12AM	
4	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	52.49.102.93	https://api.samsungcloud.com		2018-10-16 10:12AM	
5	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	52.49.102.93	https://api.samsungcloud.com		2018-10-16 10:12AM	
6	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	52.49.102.93	https://api.samsungcloud.com		2018-10-16 10:12AM	
7	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	172.217.21.74	https://play.googleapis.com		2018-10-16 10:12AM	
8	00:08:82:...	B4:BF:...	Galaxy-J7-Pro		192.168.5.144	172.217.21.74	https://play.googleapis.com		2018-10-16 10:12AM	

Figure 73: URL Access Log- CSV file example

Notes:

- This is, currently, only supported for paired GWN7600/GWN7600LR.
- The GWN.Cloud Database will keep storage of reports for **30 DAYS**, after that, they will be automatically erased from the system.

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

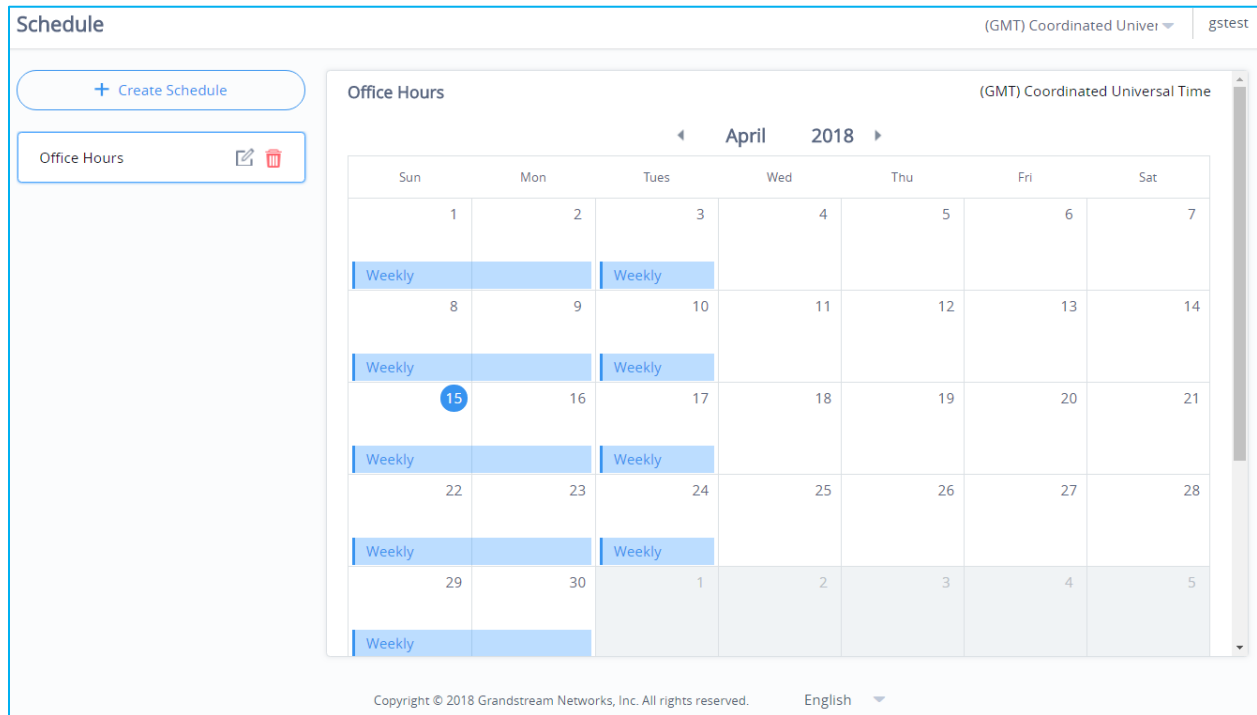


Figure 75: Schedules List

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.

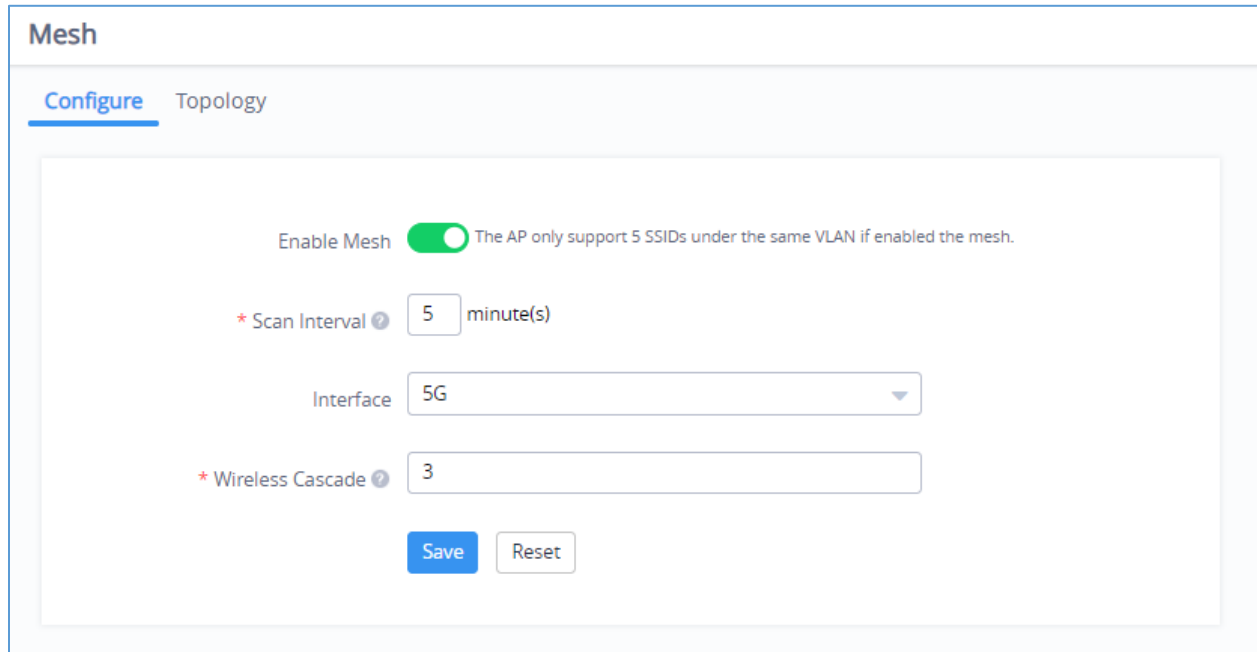
However, these are precisely the advantages of wireless networks. As a result, Wireless Mesh Network is an effective complement of wired network.

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 don't hesitate to read the following technical paper:

http://www.grandstream.com/sites/default/files/Resources/GWN76XX_Mesh_Network.pdf

In GWN.Cloud, users can setup some Mesh Network parameters under the menu “**System → Mesh**”, as shown on the figure below:



Mesh

Configure Topology

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

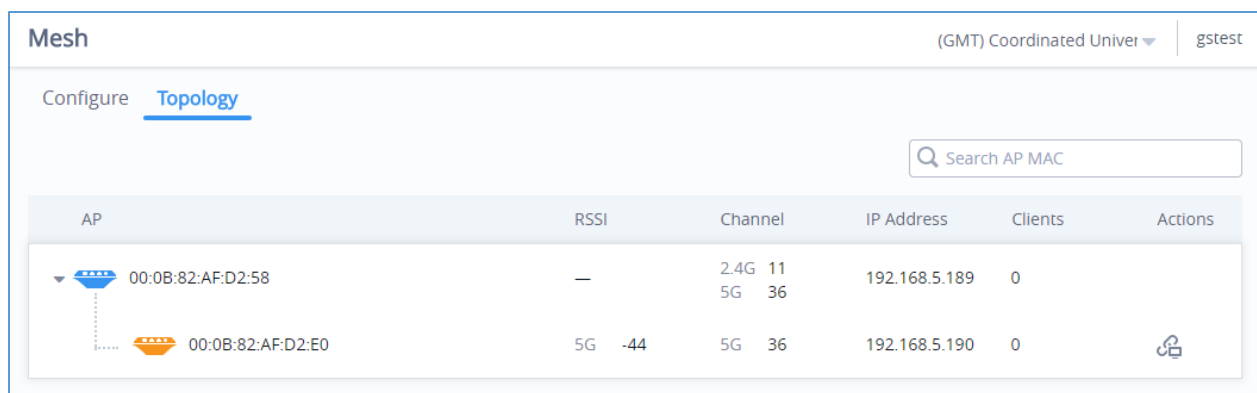
* Scan Interval minute(s)

Interface

* Wireless Cascade

Figure 76: Mesh Settings

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



Mesh (GMT) Coordinated Univer | gstest

Configure **Topology**




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 77: Mesh Topology

Maintenance

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

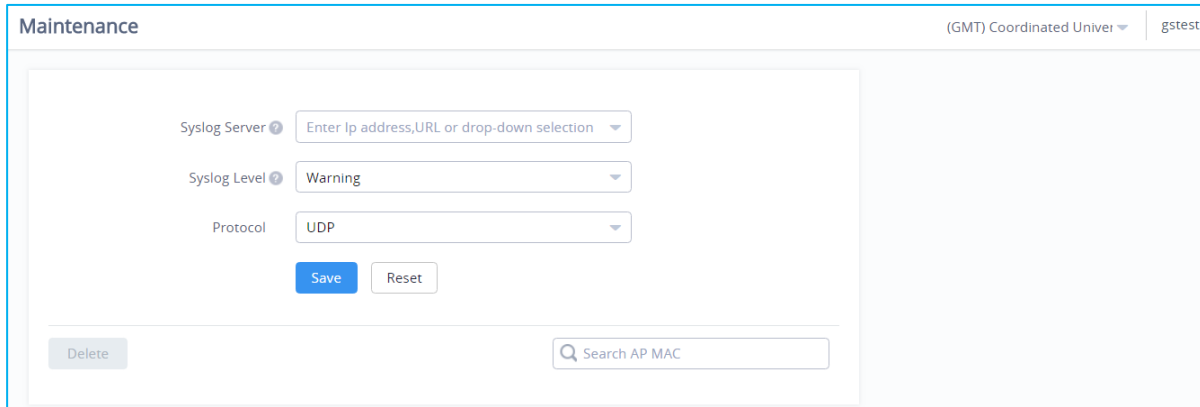


Figure 78: Maintenance/Syslog Settings

Table 16: 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.

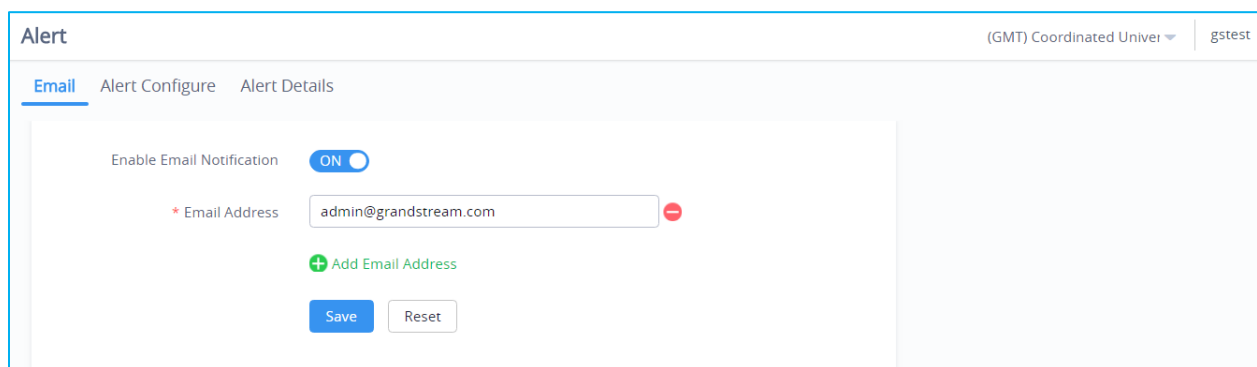


Figure 79: Alert Email

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

Alert

Email
Alert Configure
Alert Details

Memory Usage ?

Network Throughput ?

Network Throughput Threshold Mbps ▼

AP Throughput ?

SSID Throughput ?

Firmware Upgrade ?

AP Offline ?

Save
Reset

Figure 80: Alert Events List

The last tab is to display the alert events that have occurred on the managed system, and finally the table below summarizes the configuration parameters for alert events and notifications.

Table 17: Alert

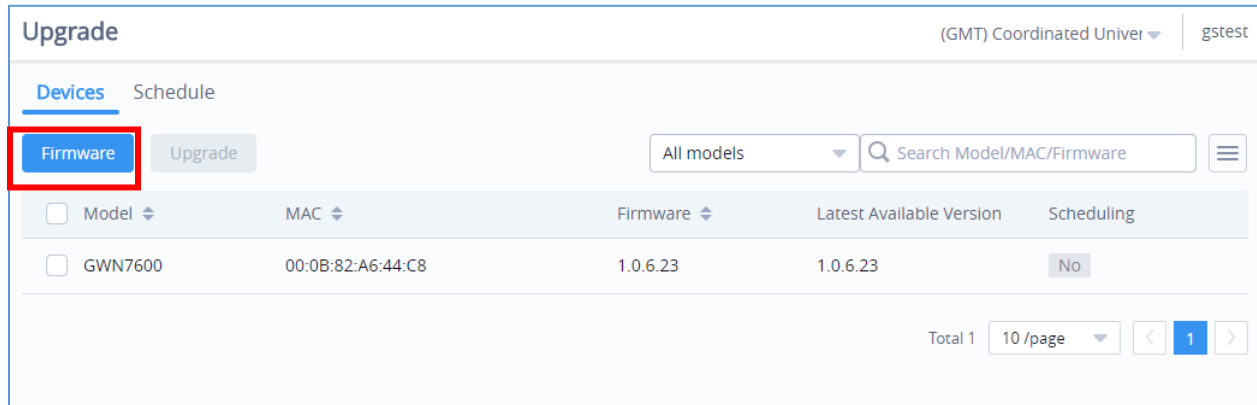
Field	Description
Email	Enable this feature to receive alerts via email
Email Address	Enter the email address to receive alerts via email
Alert configure	Specify the modules to monitor, there are seven modules: Memory Usage, CPU Usage, Network Throughput, AP Throughput, SSID Throughput, Firmware Upgrade, AP Offline
Alert details	Displays the alerts in the web UI of GWN.Cloud.

Upgrade

This feature allows upgrading access points from GWN.Cloud. “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
<input type="checkbox"/> GWN7600	00:0B:82:A6:44:C8	1.0.6.23	1.0.6.23	No

Figure 81: 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	1.0.6.14
GWN7610	
GWN7600LR	

Figure 82: Firmware - Recommended Version

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

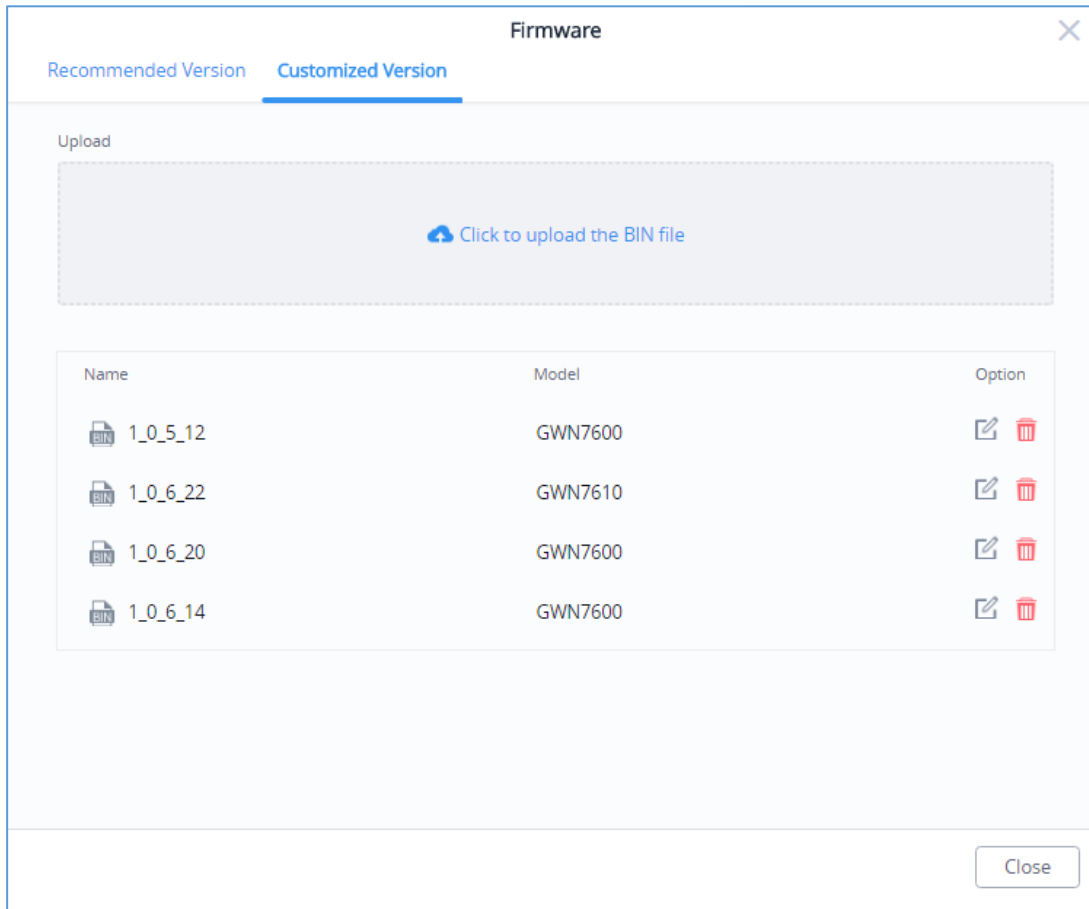


Figure 83: Firmware - Customized Version

- **Upgrading Firmware**

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

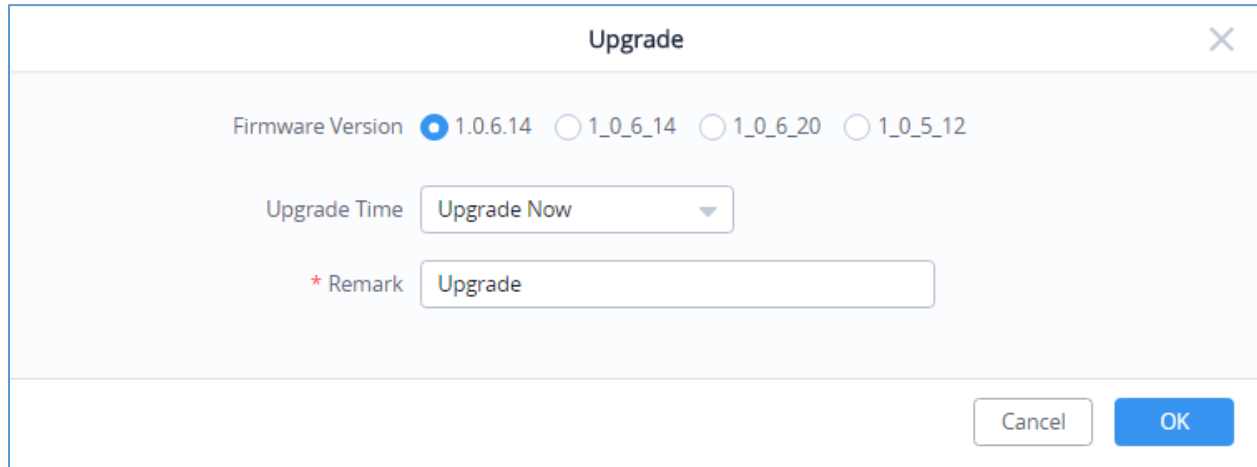


Figure 84: Upgrade GWN AP from Cloud

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.

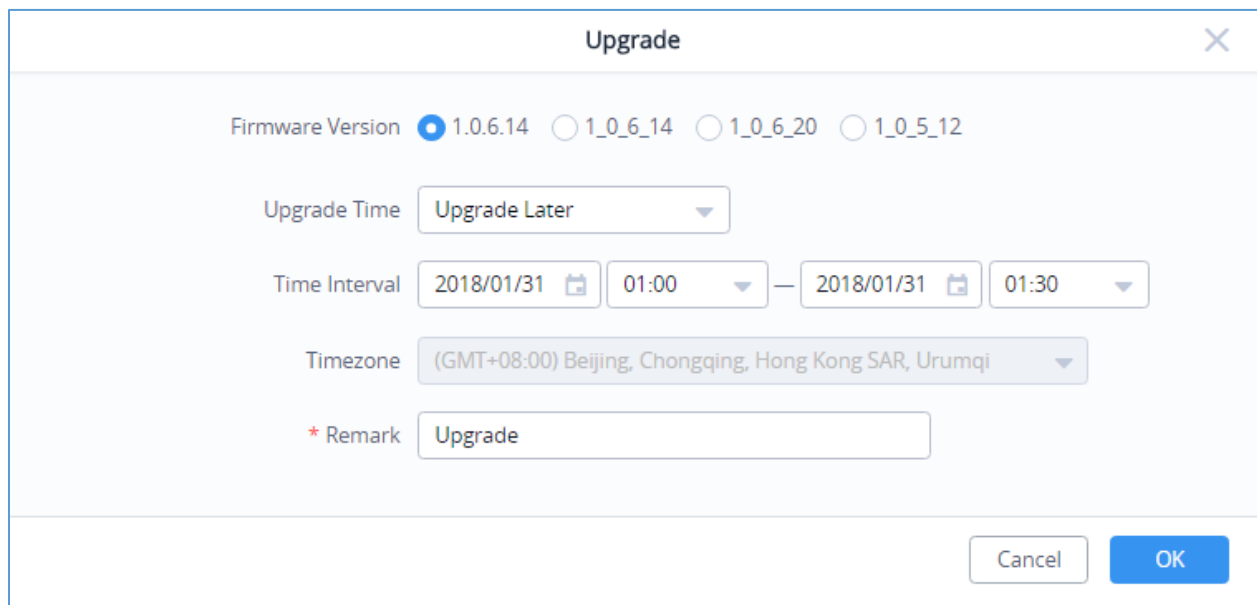












Figure 85: Upgrade Schedule for GWN AP from Cloud

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 86: Upgrade - Schedule

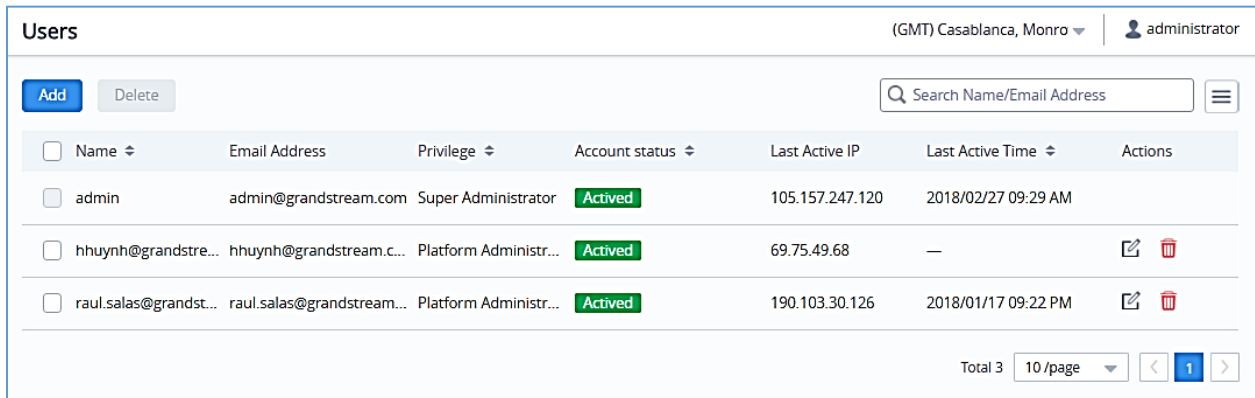
USER MANAGEMENT

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

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

Add New Users


To list all the users managing a GWN.Cloud account, Click on **user name** from the top right corner → **Users**

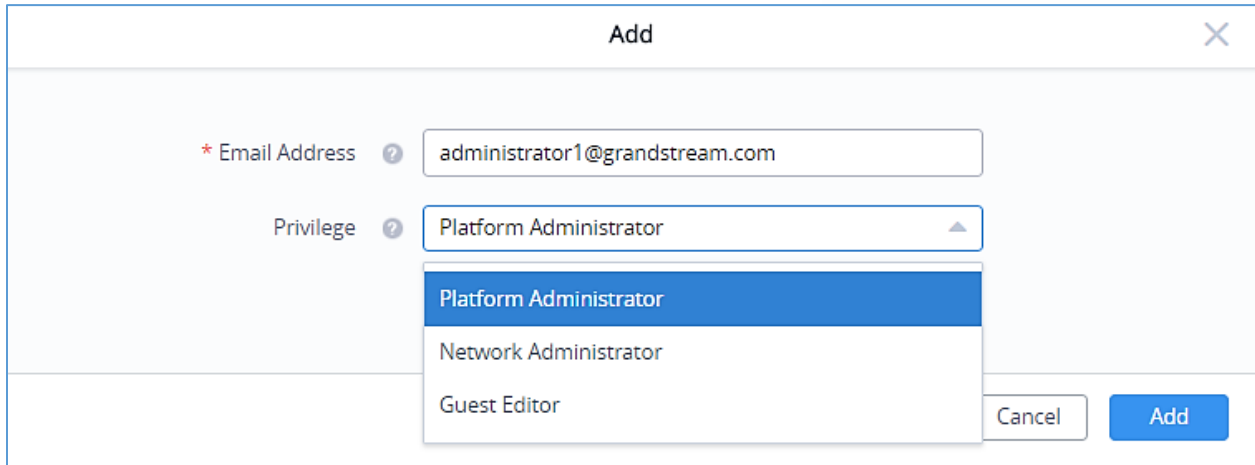


<input type="checkbox"/>	Name ↕	Email Address	Privilege ↕	Account status ↕	Last Active IP	Last Active Time ↕	Actions
<input type="checkbox"/>	admin	admin@grandstream.com	Super Administrator	Activated	105.157.247.120	2018/02/27 09:29 AM	
<input type="checkbox"/>	hhuynh@grandstre...	hhuynh@grandstream.c...	Platform Administr...	Activated	69.75.49.68	—	
<input type="checkbox"/>	raul.salas@grandst...	raul.salas@grandstream...	Platform Administr...	Activated	190.103.30.126	2018/01/17 09:22 PM	

Total 3 | 10/page | 1

Figure 87 : Users List

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

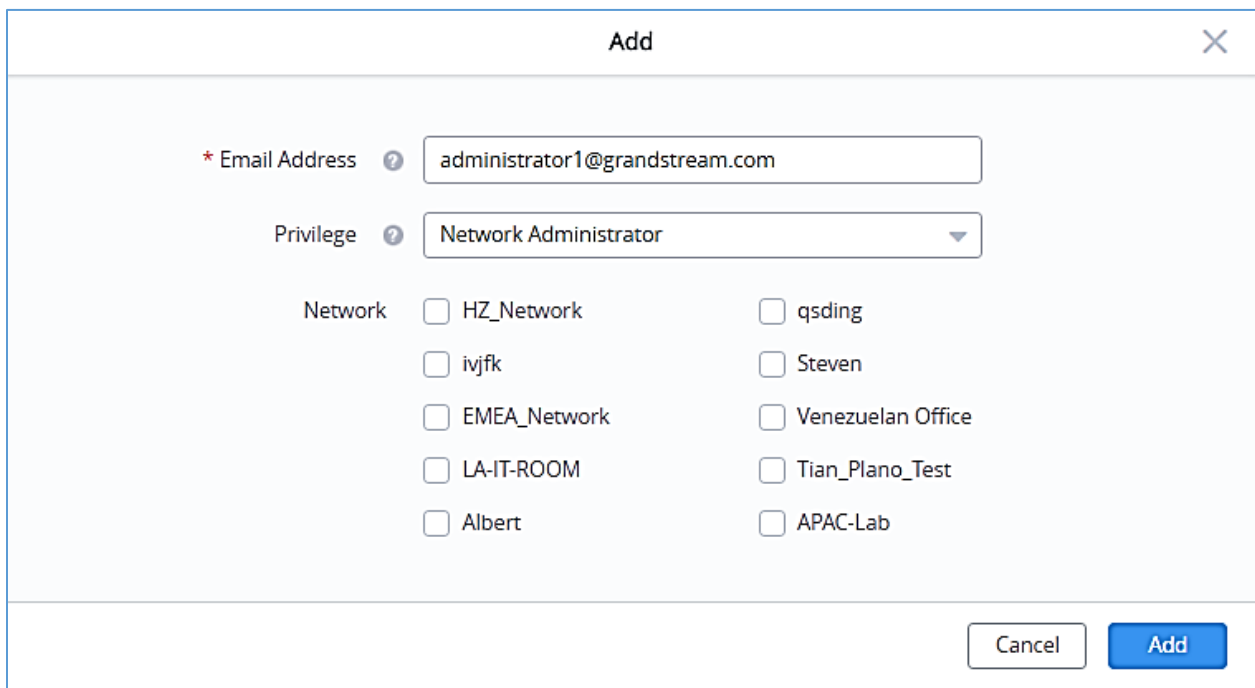


The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains two main input fields:

- * Email Address**: A text input field containing "administrator1@grandstream.com".
- Privilege**: A dropdown menu currently showing "Platform Administrator". A dropdown list is open below it, showing three options: "Platform Administrator" (highlighted in blue), "Network Administrator", and "Guest Editor".

 At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

Figure 88 : Add New "Platform Administrator" User



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following elements:

- * Email Address**: A text input field containing "administrator1@grandstream.com".
- Privilege**: A dropdown menu currently showing "Network Administrator".
- Network**: A section with a label "Network" followed by two columns of checkboxes and network names:

<input type="checkbox"/> HZ_Network	<input type="checkbox"/> qsdng
<input type="checkbox"/> ivjfk	<input type="checkbox"/> Steven
<input type="checkbox"/> EMEA_Network	<input type="checkbox"/> Venezuelan Office
<input type="checkbox"/> LA-IT-ROOM	<input type="checkbox"/> Tian_Plano_Test
<input type="checkbox"/> Albert	<input type="checkbox"/> APAC-Lab

 At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

Figure 89 : Add "New Network Administrator" User

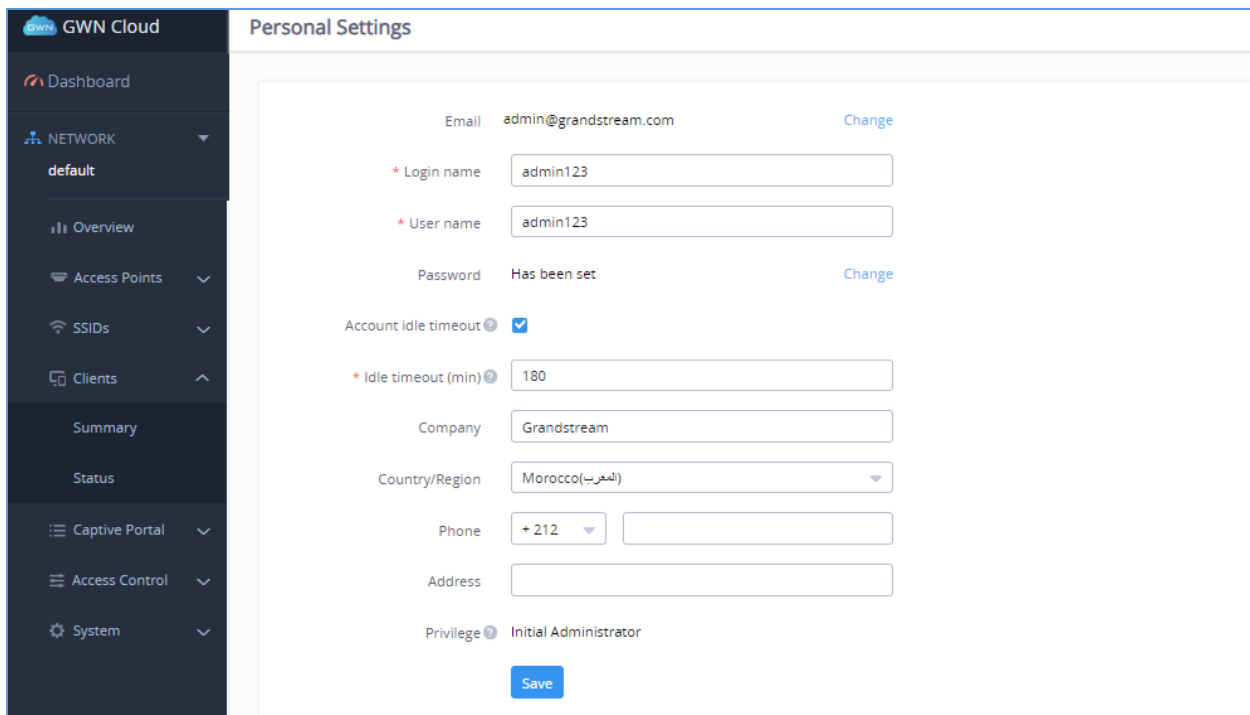
Note: When selecting privilege "Network Administrator" or "Guest Editor", the networks that will be monitored by this user should be selected, the new user will have access to those networks only.

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 GWN.Cloud 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.



The screenshot shows the 'Personal Settings' page for the Super Administrator account. The left sidebar contains navigation options: Dashboard, NETWORK (default), Overview, Access Points, SSIDs, Clients, Summary, Status, Captive Portal, Access Control, and System. The main content area displays the following fields:

- Email: admin@grandstream.com (with a 'Change' link)
- * Login name: admin123
- * User name: admin123
- Password: Has been set (with a 'Change' link)
- Account idle timeout:
- * Idle timeout (min): 180
- Company: Grandstream
- Country/Region: Morocco(المغرب) (dropdown menu)
- Phone: +212 (dropdown menu) and an empty input field
- Address: empty input field
- Privilege: Initial Administrator

A 'Save' button is located at the bottom of the form.

Figure 90 : Edit Super Administrator Account

Table 18: Super Administrator Account

Field	Description
Email	The email address of the Super Administrator. Click on change to change this email address
Login name	User name used for login authentication
User name	This is the name that will be displayed on the top right corner of the GWN.Cloud 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
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

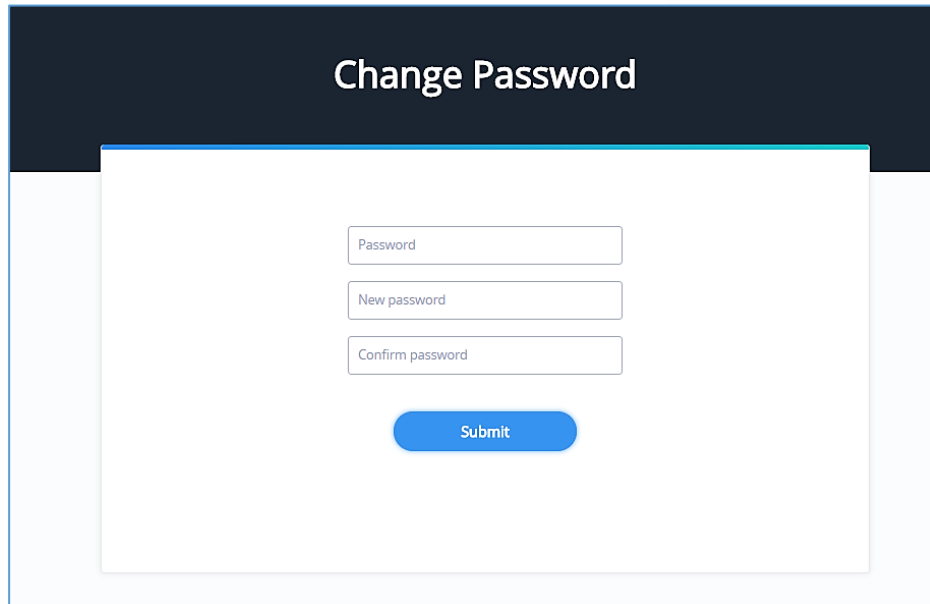
This is the lowest privilege level, a guest editor can only view and edit/monitor captive portal, and voucher page within his network.

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.



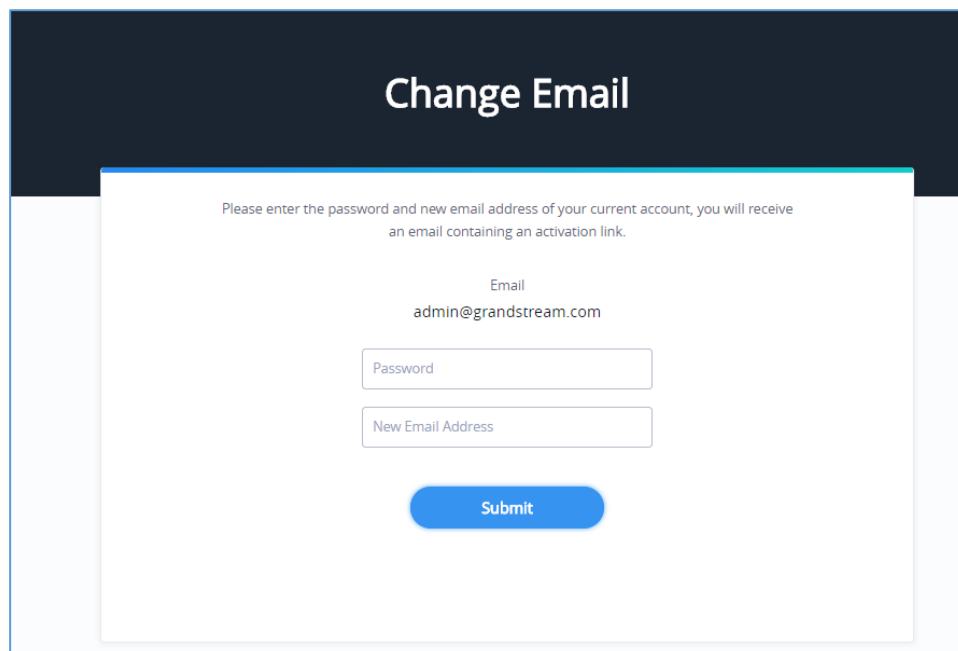


The screenshot shows a web interface with a dark blue header containing the text "Change Password" in white. Below the header is a white form box with a blue border. Inside the form, there are three input fields: "Password", "New password", and "Confirm password". Below these fields is a blue "Submit" button.

Figure 91 : Edit Super Administrator Password

Changing Super Administrator Email

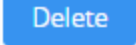
To edit super admin's email address, click on **Change** and a new web page will be displayed, enter the **password** of the super admin account as well as the **new email address** then click on **Submit**.



The screenshot shows a web interface with a dark blue header containing the text "Change Email" in white. Below the header is a white form box with a blue border. At the top of the form, there is a message: "Please enter the password and new email address of your current account, you will receive an email containing an activation link." Below this message, the word "Email" is displayed above the text "admin@grandstream.com". There are two input fields: "Password" and "New Email Address". Below these fields is a blue "Submit" button.

Figure 92 : Edit Super Administrator Email

Delete Users

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

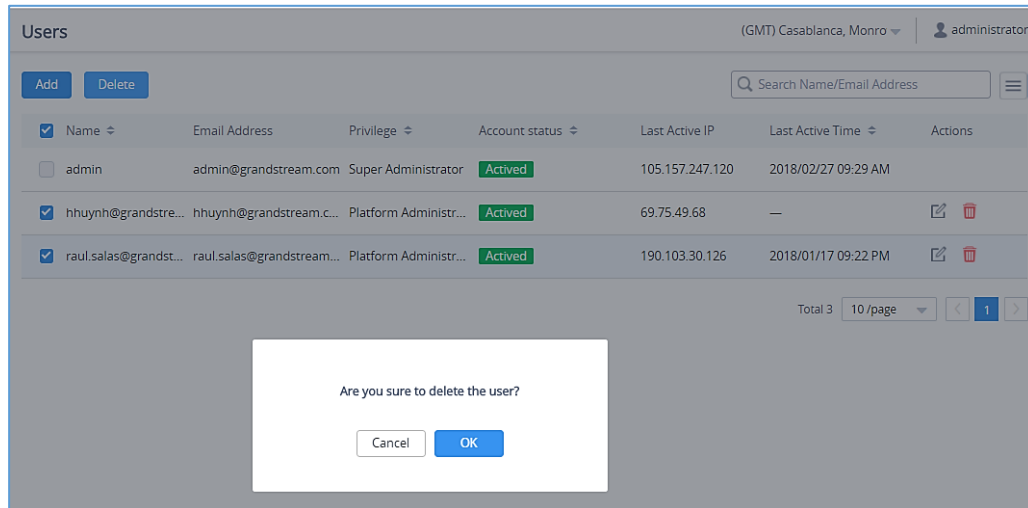
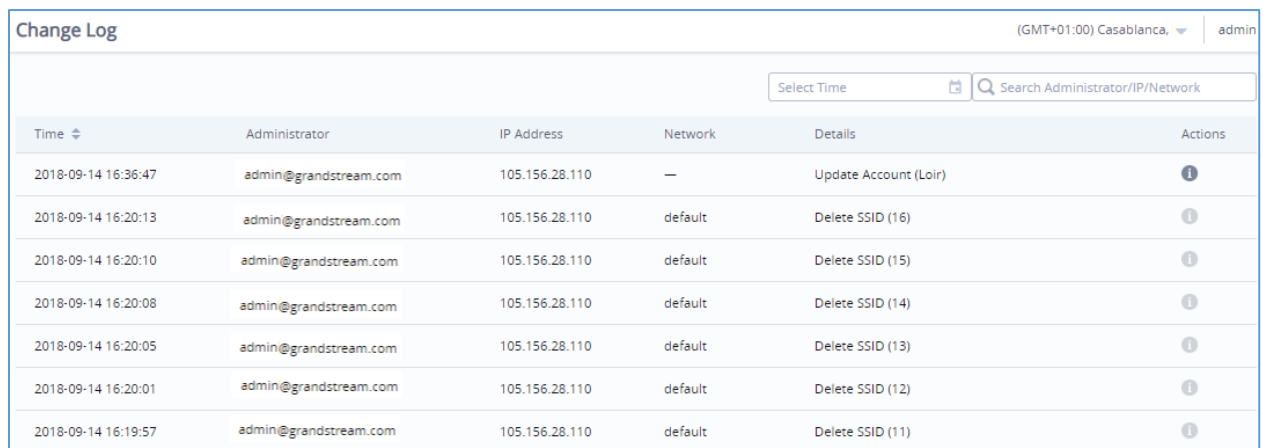


Figure 93 : Delete Users

Change Log

To list all the event logs recorded on the GWN.Cloud, Click on **user name** from the top right corner →


Change Log



The screenshot shows the 'Change Log' page. It features a search bar for 'Administrator/IP/Network' and a table of log entries. The table columns are Time, Administrator, IP Address, Network, Details, and Actions.

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 94: 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.

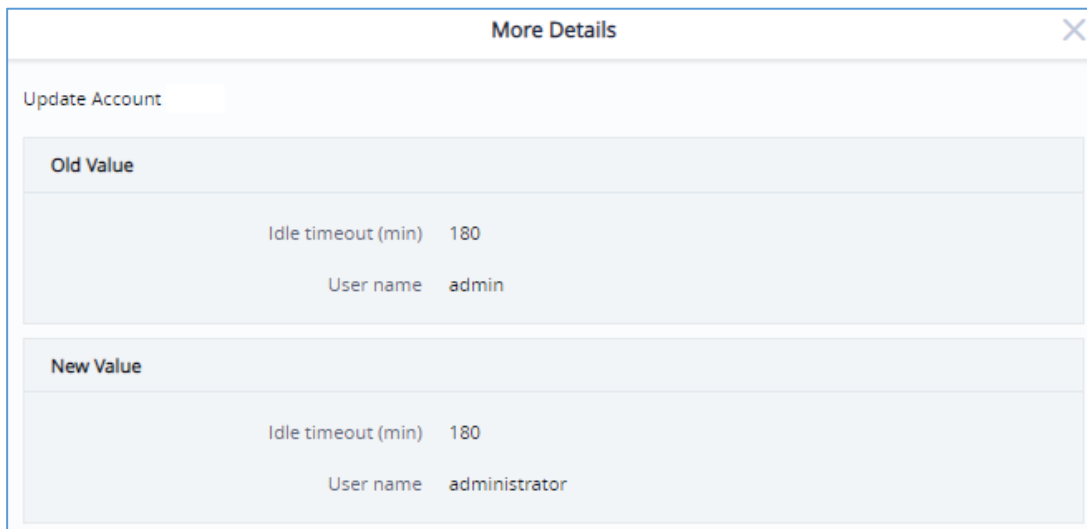
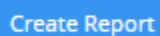


Figure 95: Change Log Action

Report

Administrators can generate and configure the GWN.Cloud 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



button, a new page displaying the report details will be displayed.

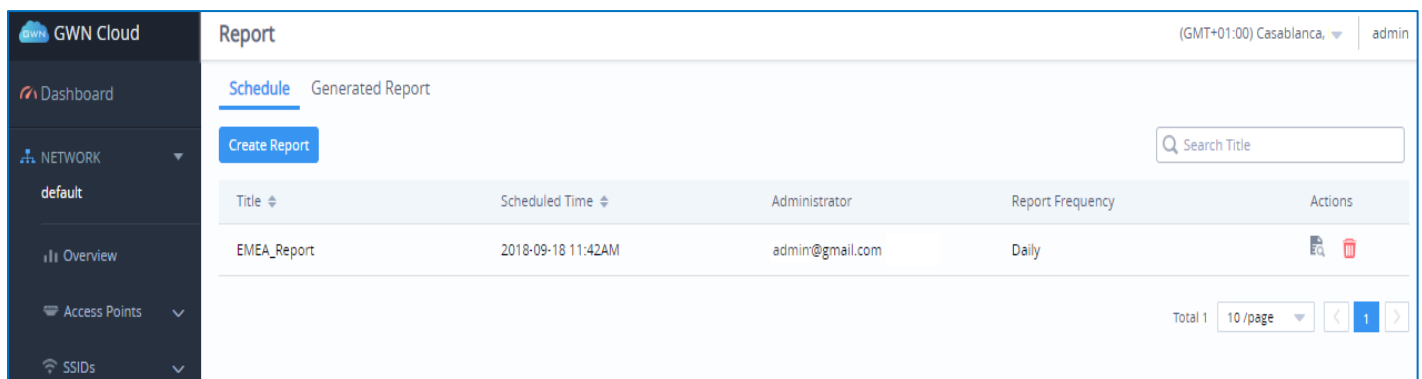


Figure 96: Generate Report

X
Create Report

* Title ?

* 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 Clients

Top SSIDs

Report Frequency

Report Generate Time

Email Address -

+ Add Email Address

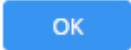


Figure 97: Create Report

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

Table 19: 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	<p>Specify the report contents for the <i>selected network group(s)</i>, the contents can include:</p> <ul style="list-style-type: none"> • 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 “ <i>Custom Range</i> ” 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  , a report schedule will be generated under **Schedule** section which you can preview by clicking on  Action button, or delete it using  .

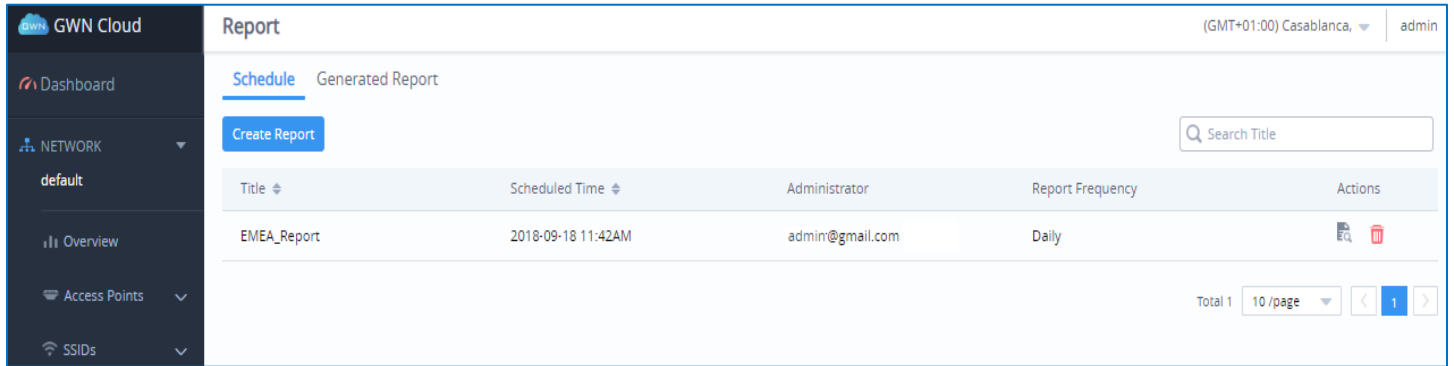


Figure 98: Created Report

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 .

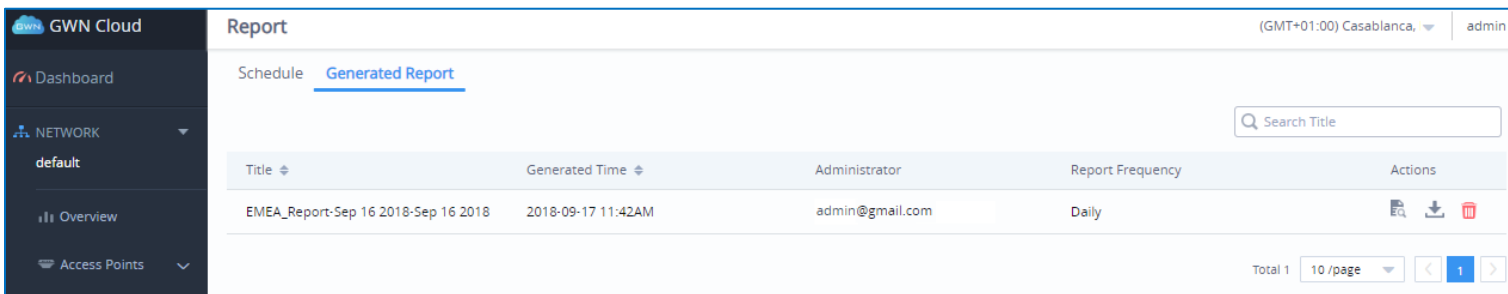


Figure 99: Generated Report

EXPERIENCING GWN.CLOUD

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.Cloud, it will be sure to bring convenience to both your business and personal life.

