

# Grandstream Networks, Inc.

---

## GWN Management Platform

***GWN.Cloud:*** Cloud based Access Points Controller

***GWN Manager:*** On-premise Access Points Controller

## User Guide



## COPYRIGHT

©2020 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

<b>DOCUMENT PURPOSE .....</b>	<b>14</b>
<b>CHANGE LOG .....</b>	<b>15</b>
GWN.Cloud .....	15
<i>Version 1.0.10.9</i> .....	15
<i>Version 1.0.10.7</i> .....	15
<i>Version 1.0.9.8</i> .....	15
<i>Version 1.0.8.17</i> .....	16
<i>Version 1.0.8.7</i> .....	16
<i>Version 1.0.7.18</i> .....	16
<i>Version 1.0.0.37</i> .....	17
GWN Manager .....	17
<i>Version 1.0.0.21</i> .....	17
<b>REQUIREMENTS .....</b>	<b>18</b>
<b>WELCOME .....</b>	<b>19</b>
<b>PRODUCT OVERVIEW .....</b>	<b>20</b>
Features Highlights.....	20
Specifications .....	21
<b>GETTING TO KNOW GWN MANAGEMENT PLATFORM.....</b>	<b>23</b>
GWN.Cloud .....	23
<i>Sign up to GWN.Cloud</i> .....	23
GWN Manager .....	26
<i>Installation Steps</i> .....	26
<i>Configuring GWN Manager</i> .....	28
<i>Upgrading GWN Manager</i> .....	28
<i>Uninstalling GWN Manager</i> .....	28



<i>First Use.....</i>	29
<i>Sign up to GWN Manager.....</i>	30
<b>GETTING STARTED WITH GWN MANAGEMENT PLATFORM .....</b>	<b>32</b>
GWN76xx LED Patterns .....	32
Adding GWN76XX to GWN.Cloud.....	33
<i>Method 1: Adding New AP Manually .....</i>	33
<i>Method 2: Adding New AP using GWN.Cloud Application.....</i>	35
<i>Method 3: Transfer APs from Local Master.....</i>	36
Adopt GWN76XX to GWN Manager.....	39
<i>Discover GWN76XX .....</i>	40
<i>Method 1: Auto Discovery .....</i>	40
<i>Method 2: Manual discovery .....</i>	40
<b>DASHBOARD .....</b>	<b>42</b>
Overview .....	42
Network List.....	43
AP List.....	45
<b>NETWORK.....</b>	<b>47</b>
Create a New Network.....	47
Overview Page .....	48
<b>ACCESS POINTS .....</b>	<b>50</b>
Summary.....	50
Status.....	50
Configuration .....	54
<i>Add New Access Points.....</i>	54
<i>Move Access Points .....</i>	55
<i>Delete Access Points .....</i>	55
<i>Reboot Access Points.....</i>	55



Configure Access Points .....	56
Reset Access Points .....	58
<b>SSID .....</b>	<b>59</b>
Summary .....	59
Configuration .....	59
Wi-Fi Settings .....	60
Device Membership .....	67
<b>CLIENTS .....</b>	<b>68</b>
Summary .....	68
Clients Count .....	68
Bandwidth Usage .....	69
Clients Statistics for Last Day .....	69
Client Manufacturer .....	69
Client OS .....	69
Status Page .....	69
<b>CAPTIVE PORTAL .....</b>	<b>72</b>
Summary .....	72
Guest New Session .....	73
Guest Session by Authentication .....	73
Guest Session by SSID .....	74
Guest .....	74
Guest .....	75
Policy List .....	76
Internal Splash Page .....	77
External Splash Page .....	79
Splash Page .....	80
Page .....	80



<i>Advertisement</i> .....	86
Voucher .....	89
<b>ACCESS CONTROL</b> .....	<b>92</b>
Access List .....	92
Time Policy .....	93
Bandwidth rules .....	94
<b>INSIGHT</b> .....	<b>96</b>
Site Survey .....	96
Known Clients .....	96
<b>SYSTEM</b> .....	<b>98</b>
Settings .....	98
<i>URL Access Log</i> .....	99
<i>Guest Information</i> .....	101
Schedule .....	102
Mesh .....	103
Maintenance .....	106
Alert .....	106
Upgrade .....	109
<b>USER MANAGEMENT</b> .....	<b>112</b>
Add New Users .....	112
User Privilege levels .....	113
<i>Super Administrator</i> .....	113
<i>Platform Administrator</i> .....	115
<i>Network Administrator</i> .....	115
<i>Guest Editor</i> .....	115
Edit User Settings .....	115
<i>Changing Password</i> .....	115



<i>Changing Super Administrator Email</i> .....	116
Delete Users.....	116
Change Log.....	117
Report .....	118
Feedback .....	121
<b>GLOBAL (GWN MANAGER ONLY) .....</b>	<b>123</b>
Manager Settings .....	123
<i>Manager Log</i> .....	123
<i>SMTP Server</i> .....	123
<i>Backup &amp; Restore</i> .....	124
Report .....	125
Change Log.....	125
<b>EXPERIENCING GWN MANAGEMENT PLATFORMS .....</b>	<b>126</b>



## Table of Tables

Table 1: Requirements.....	18
Table 2: GWN Management Platform Specifications .....	21
Table 3: GWN.Cloud Sign up Settings.....	25
Table 4: GWN Manager Setup Wizard .....	29
Table 5: LED Patterns.....	32
Table 6: Dashboard Description .....	43
Table 7: Create a New Network Settings .....	44
Table 8: Create a New Network Settings .....	48
Table 9: Access Points Status Parameters .....	51
Table 10: Access Point Configuration Settings .....	56
Table 11: SSID Wi-Fi Settings .....	61
Table 12: Add new Policy List – Splash Page as “Internal”.....	77
Table 13: Add new Policy List – Splash Page as “External” .....	79
Table 14: Advertisement Settings Configuration .....	87
Table 15: Voucher Configuration Parameters .....	90
Table 16: Time Policy Configuration Parameters .....	93
Table 17: Bandwidth Rules .....	94
Table 18: Settings.....	98
Table 19: Maintenance.....	106
Table 20: Alert.....	106
Table 21: Alert configuration parameters .....	107
Table 22: Super Administrator Account.....	114
Table 23: Report Settings.....	119
Table 24: SMTP server Configuration Details .....	123
Table 25: Backup Configuration Details.....	124





## Table of Figures

Figure 1: GWN.Cloud Architecture .....	23
Figure 2: GWN.Cloud Login Page .....	24
Figure 3: GWN.Cloud Sign up page .....	24
Figure 4: GWN.Cloud Dashboard .....	25
Figure 5: GWN Manager Architecture .....	26
Figure 6: GWN Manager Start page.....	27
Figure 7: GWN Manager Wizard .....	30
Figure 8: GWN Manager Login Page .....	31
Figure 9: GWN Manager Dashboard .....	31
Figure 10: GWN Access Point MAC and Wi-Fi Password .....	33
Figure 11: Adding New Access Point to GWN.Cloud .....	34
Figure 12: Adding Access Points Manually .....	34
Figure 13: Import CSV file for APs .....	35
Figure 14: Upload CSV file .....	35
Figure 15: Adding Access Point to GWN.Cloud using GWN App .....	36
Figure 16: Access Points Status.....	36
Figure 17: Master AP - Access Points .....	37
Figure 18: Transfer AP to Cloud .....	37
Figure 19: Select Network.....	38
Figure 20: Transfer AP to Cloud - Success.....	38
Figure 21: Adding New Access Point to GWN Manager.....	39
Figure 22: Auto detect Access Points .....	39
Figure 23: Select Access Points.....	39
Figure 24: Confirm APs Adoption .....	40
Figure 25: Adopted Access Points.....	40



Figure 26: Manager Settings – SSH.....	41
Figure 27: Manager Settings – Slave WebGUI.....	41
Figure 28: GWN.Cloud Dashboard - Overview.....	42
Figure 29: GWN.Cloud Dashboard - Network List .....	44
Figure 30: Create a New Network .....	44
Figure 31: GWN.Cloud Dashboard – AP List.....	45
Figure 32: Customize AP List Table Fields .....	46
Figure 33: Network List and Network Creation Button .....	47
Figure 34: Create Network.....	48
Figure 35: Overview Page Displays Information related to Specific Network.....	49
Figure 36: Access Points – Summary.....	50
Figure 37: Access Points - Status .....	51
Figure 38: Usage of a Specific AP .....	52
Figure 39: Current Clients - Stats per AP .....	52
Figure 40: Event Log per AP .....	53
Figure 41: AP Info.....	53
Figure 42: Debug Tool Tab.....	54
Figure 43: Access Points Configuration Page.....	54
Figure 44: Moving Access Points between Networks.....	55
Figure 45: Delete Access Point .....	55
Figure 46: Reboot Access Point.....	55
Figure 47: Access Point Configuration Page .....	56
Figure 48: Reset Access Point.....	58
Figure 49: SSIDs - Summary .....	59
Figure 50: SSIDs - Configuration .....	60
Figure 51: SSIDs – Configuration – Wi-Fi Settings .....	60
Figure 52: Device Membership - Available Devices .....	67



Figure 53: Device Membership - Members Devices .....	67
Figure 54: Clients - Summary .....	68
Figure 55: Clients Status.....	69
Figure 56: Client Data Usage Info .....	70
Figure 57: Client Info .....	70
Figure 58: Client Roaming .....	71
Figure 59: Captive Portal Summary .....	72
Figure 60: Guest New Session .....	73
Figure 61: Guest Session by Authentication .....	74
Figure 62: Guest Session by SSID.....	74
Figure 63: Guest Section .....	75
Figure 64: Guest List .....	75
Figure 65: Export Guest Information Period .....	76
Figure 66: Add/Edit Captive Portal Policy .....	77
Figure 67: Create New Splash Page .....	81
Figure 68: Setup Logging Methods - Splash Page.....	82
Figure 69: Upload a logo - Splash Page.....	82
Figure 70: Name - Splash Page.....	83
Figure 71: Setup Social Logging Parameters .....	84
Figure 72: Splash Page Preview .....	85
Figure 73: Splash Pages List .....	85
Figure 74: Enable Captive Portal .....	86
Figure 75: Portal Splash Page .....	86
Figure 76: Advertisement Page.....	87
Figure 77: Add Video - Advertisement .....	88
Figure 78: Adding Vouchers.....	89
Figure 79: Voucher Details.....	91



Figure 80: Voucher Settings.....	91
Figure 81: Access List.....	92
Figure 82: Adding New Clients to Access List.....	92
Figure 83: Add Time Policy List.....	93
Figure 84: MAC Address Bandwidth Rule .....	95
Figure 85: Site Survey - Insight.....	96
Figure 86: Known Clients - Insight .....	97
Figure 87 :System Settings.....	98
Figure 88: URL Access Log Settings.....	100
Figure 89: Export Immediately .....	100
Figure 90: Export Succeed .....	100
Figure 91: URL Access Log- CSV file example.....	101
Figure 92: Guest Information .....	101
Figure 93: Create New Schedule- Weekly.....	102
Figure 94: Create New Schedule- Absolute.....	102
Figure 95: Schedules List .....	103
Figure 96: Mesh Settings.....	104
Figure 97: Mesh Topology.....	104
Figure 98: Neighbor.....	105
Figure 99: Maintenance/Syslog Settings .....	106
Figure 100: Alert Email .....	107
Figure 101: Alert Events List.....	107
Figure 102: Alert Details .....	109
Figure 103: Upgrade.....	109
Figure 104: Firmware - Recommended Version .....	110
Figure 105: Firmware - Customized Version.....	110
Figure 106: Upgrade AP from GWN Manager .....	110



Figure 107: Upgrade Schedule for GWN AP from GWN Manager .....	111
Figure 108: Upgrade - Schedule .....	111
Figure 109 : Users List.....	112
Figure 110 : Add New “Platform Administrator” User .....	113
Figure 111 : Add “New Network Administrator” User .....	113
Figure 112 : Edit Super Administrator Account.....	114
Figure 113 : Edit Super Administrator Password .....	116
Figure 114 : Edit Super Administrator Email .....	116
Figure 115 : Delete Users .....	117
Figure 116: Change Log Records .....	117
Figure 117: Change Log Action .....	118
Figure 118: Generate Report .....	118
Figure 119: Create Report .....	119
Figure 120: Created Report .....	121
Figure 121: Generated Report .....	121
Figure 122: Feedback.....	122
Figure 123: SMTP server.....	123
Figure 124: Backup Settings .....	124
Figure 125: Restore .....	124
Figure 126: Confirm Backup .....	125



## DOCUMENT PURPOSE

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

This guide will cover the below topics:

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

## CHANGE LOG

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

### GWN.Cloud

#### Version 1.0.10.9

- No Major changes.

#### Version 1.0.10.7

- Added Site Survey feature. [Site Survey]
- Added feature of Minimum Rate Control. [Enable Minimum Rate] [Minimum Rate (Mbps)]
- Added feature of SSH Remote Access. [SSH Remote Access]
- Added feature of External Portal support Socifi Platform. [External Splash Page]
- Added feature of Client inactivity timeout. [Client Inactivity Timeout]
- Added feature of Upgrade Regularly. [Upgrade]
- Added feature of Client Steering. [Client Steering]
- Enhanced feature of Voucher: display of remaining bytes. [Figure 79: Voucher Details]
- Enhanced feature of Dynamic VLAN. [Enable Dynamic VLAN]
- Changed LED patterns. [GWN76xx LED Patterns]

#### Version 1.0.9.8

- Added support for collecting user feedback from GWN Cloud page. [Feedback]
- Added support for Voucher Style Customization. [Voucher Settings]
- Added support for video URL. [Advertisement]
- Added support to export Guest Information via Email. [Email Guest Information]
- Added support for client RX/TX Rate display. [Status Page]



- Expanded Max Devices to use the same Voucher. [Voucher]
- Added support to enable/disable client connection/disconnection events.

### **Version 1.0.8.17**

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

### **Version 1.0.8.7**

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

### **Version 1.0.7.18**

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





[Convert IP multicast to unicast].

- Enhanced Captive Portal features. [Failsafe Mode] [Daily Limit] [Byte Quota] [Force To Follow]

### **Version 1.0.0.37**

- This is the initial version for GWN.Cloud.

## **GWN Manager**

### **Version 1.0.0.21**

- This is the initial version for GWN Manager.



## REQUIREMENTS

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

Table 1: Requirements

	Model	GWN.Cloud 1.0.10.9		GWN Manager 1.0.0.21	
		Minimum	Recommended	Minimum	Recommended
Version of AP	GWN7610	1.0.6.37	1.0.11.8	1.0.13.1	1.0.13.1
	GWN7600	1.0.6.33	1.0.11.8	1.0.13.1	1.0.13.1
	GWN7600LR	1.0.6.33	1.0.11.8	1.0.13.1	1.0.13.1
	GWN7630	1.0.9.2	1.0.11.8	1.0.13.1	1.0.13.1
	GWN7630LR	1.0.11.8	1.0.11.10	1.0.13.1	1.0.13.1
	GWN7602	1.0.1.6	1.0.3.4	1.0.3.4	1.0.3.4
Version of APP	iOS™	1.0.2	1.0.5	1.0.6	1.0.6
	Android™	1.0.0.7	1.0.0.14	1.0.0.19	1.0.0.19
System (GWN Manager only)	<b>OS:</b> Linux Redhat7, CentOS 7  <b>Hardware:</b>  <b>For up to 200 APs and 2000 Clients:</b> <ul style="list-style-type: none"> <li>• CPU: Intel® Core™ i3-3240 or above</li> <li>• RAM: 4GB or above</li> <li>• Storage: 250GB (SSD preferred, depend on retained data size)</li> </ul> <b>For up to 3000 APs and 30000 Clients:</b> <ul style="list-style-type: none"> <li>• CPU: Intel® Xeon® Silver 4210</li> <li>• RAM: 16GB or above</li> <li>• Storage: 250GB (SSD preferred, depend on retained data size)</li> </ul>				



## WELCOME

Thank you for using Grandstream GWN Management Platform.

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

## PRODUCT OVERVIEW

### Features Highlights

<b>GWN.Cloud</b>	<ul style="list-style-type: none"> <li>• Software-as-a-Service (SaaS) Solution to manage all your Grandstream Access point, without any additional on-premise infrastructure.</li> <li>• 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.</li> <li>• Easy way to add new access point, either by scanning a barcode from GWN.Cloud App (iOS &amp; Android) or by entering AP MAC and random password.</li> <li>• No limits on number of sites or APs</li> </ul>
<b>GWN Manager</b>	<ul style="list-style-type: none"> <li>• Linux solution to secure manage all your Grandstream Access point</li> <li>• Automatically discover and Adopt Access point in your network</li> <li>• Adopt APs manually using SSH or through Web GUI by setting the Manager address and port.</li> <li>• Up to 3000 APs, with high performance hardware</li> </ul>
<b>Shared</b>	<ul style="list-style-type: none"> <li>• Highly available with no single point of failure across the whole system.</li> <li>• Easy and intuitive dashboard for monitoring.</li> <li>• Network Group creation.</li> <li>• AP and clients Centralized monitoring and management.</li> <li>• Captive portal configuration.</li> <li>• Bandwidth control per SSID, IP, or MAC address.</li> </ul>



## Specifications

**Table 2: GWN Management Platform Specifications**

<b>Function</b>	<ul style="list-style-type: none"> <li>• Network-based AP management</li> <li>• Network/AP/client monitoring</li> </ul>
<b>Security and Authentication</b>	<ul style="list-style-type: none"> <li>• Supports access policies configuration (blacklist, whitelist, time policy)</li> <li>• Multiple security modes including WPA, WPA2, WEP, open, etc.</li> <li>• Bandwidth rules for client access</li> <li>• User and privilege management</li> </ul>
<b>Enterprise Features</b>	<ul style="list-style-type: none"> <li>• No limits on number of sites or APs for GWN.Cloud; Up to 3000 APs for GWN Manager with high performance hardware</li> <li>• Hosted by AWS with 99.99% uptime (GWN.Cloud only)</li> <li>• Bank-grade TLS encryption from end-to-end</li> <li>• X.509 certificate-based authentication</li> <li>• Supports Wi-Fi Alliance Voice-Enterprise</li> <li>• Mobile app for iOS™ and Android™</li> <li>• Real-time Wi-Fi Scan for deployment</li> <li>• URL access log collection</li> <li>• Multiple Wi-Fi performance optimization methods including band steering, Minimum RSSI, ARP Proxy, IP multicast to unicast, etc</li> </ul>
<b>Supported Wi-Fi Access Points</b>	GWN7610, GWN7600, GWN7600LR, GWN7630, GWN7630LR, GWN7602.
<b>Captive Portals</b>	<ul style="list-style-type: none"> <li>• Splash page with built-in WYSIWYG editor</li> <li>• Facebook, Twitter integration</li> <li>• Multiple captive portal authentications including simple password, radius, voucher, custom field etc.</li> <li>• External captive portal integration</li> </ul>



	<ul style="list-style-type: none"> <li>• Real-time guest statistics and monitoring</li> <li>• Advertisement integration with flexible strategies</li> <li>• Export guest info into file and automatically send to email</li> </ul>
<b>Centralized Management</b>	<ul style="list-style-type: none"> <li>• Local data forwarding, no user traffic sent to the controller</li> <li>• Network-based AP management</li> <li>• Network/AP/client monitoring</li> <li>• Layer2 and Layer3 based AP discovery</li> </ul>
<b>Reporting and Monitoring</b>	<ul style="list-style-type: none"> <li>• Real-time Wi-Fi AP and client monitoring</li> <li>• Detailed reports by network, AP, client etc.</li> <li>• Retrieval of historical data for statistical observations</li> <li>• Real-time alerts and event logs</li> </ul>
<b>Maintenance</b>	<ul style="list-style-type: none"> <li>• Ping/traceroute/capture</li> <li>• Both configuration and data backup</li> <li>• Scheduled AP firmware update and LED control</li> <li>• Change log for audit trail</li> </ul>
<b>Languages</b>	English, Chinese, French, German, Portuguese and Spanish



## GETTING TO KNOW GWN MANAGEMENT PLATFORM

### GWN.Cloud



Figure 1: GWN.Cloud Architecture

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

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

### Sign up to GWN.Cloud

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



**Figure 2: GWN.Cloud Login Page**

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



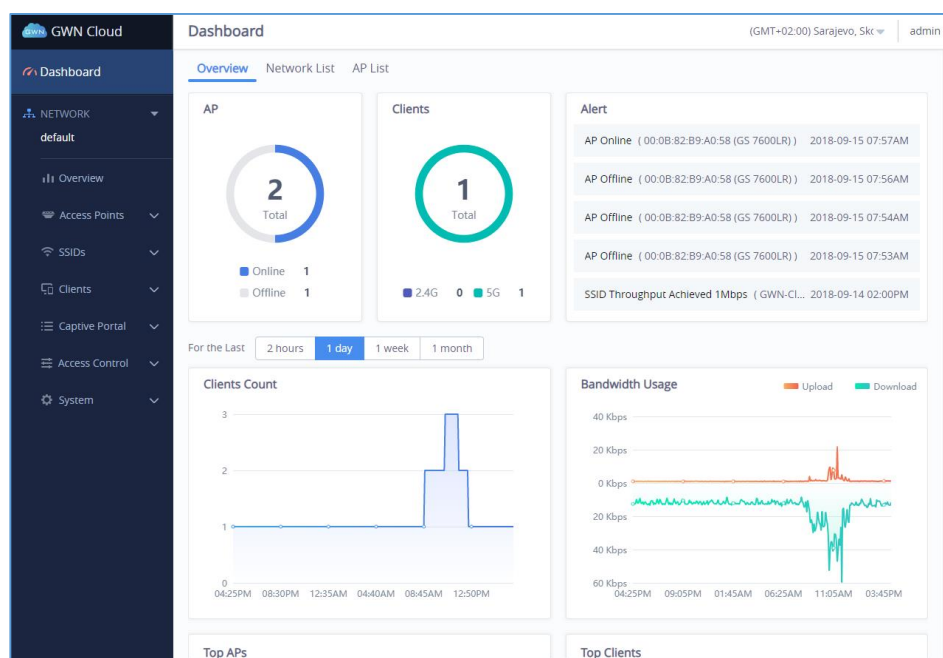
**Figure 3: GWN.Cloud Sign up page**



**Table 3: GWN.Cloud Sign up Settings**

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

## GWN Manager



Figure 5: GWN Manager Architecture

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

### Installation Steps

#### 1. Install dependencies:

- Type in the following commands under CentOS Terminal

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

#### 2. Installing GWN Manager

- Download link: <https://www.grandstream.com/support/firmware>
- After a successful download, browse to the file directory and uncompress it:

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

- Then, Install all packages:

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

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



### 3. Add firewall exceptions:

```
firewall-cmd --zone=public --add-port=8443/tcp --permanent
firewall-cmd --zone=public --add-port=10014/tcp --permanent
firewall-cmd --reload
```

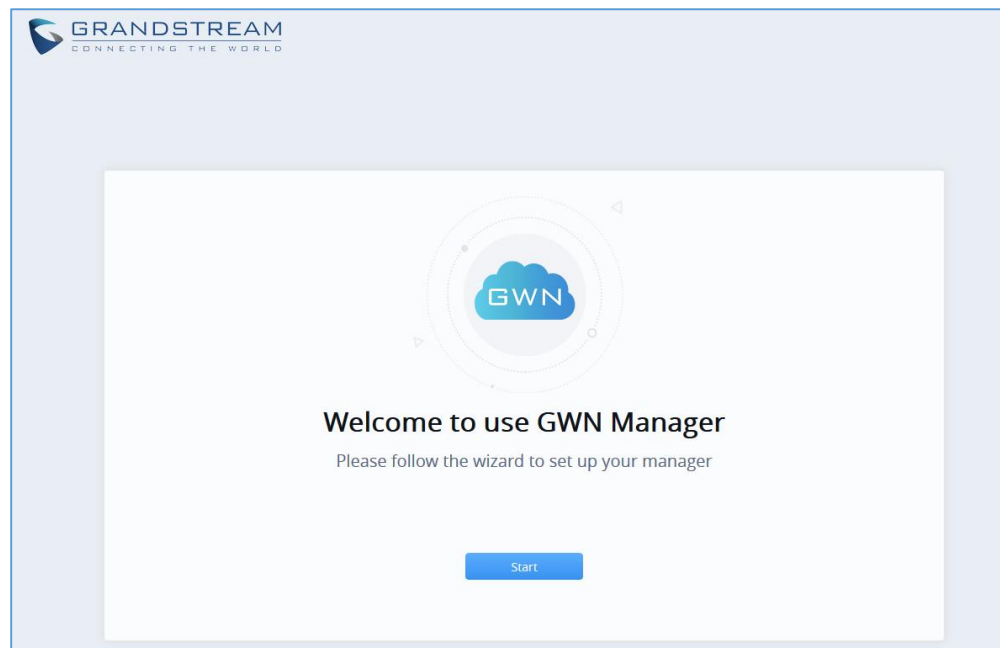
**Note:** By default, GWN Manager use port 8443 for web service (nginx) and port 10014 for gateway communication separately.

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

```
/gwn/gwn start
```

```
[root@02 ~]# /gwn/gwn start
Protocol: https
Nginx listening port(https): 8443
Access URL: https://192.168.5.142:8443
May need a little time, please wait patiently!
Starting redis: [ OK ]
Starting mysql: [ OK ]
Starting nginx: [ OK ]
Starting web: [ OK ]
Starting email: [ OK ]
Starting gateway: [ OK ]
[root@02 ~]# _
```

**Note:** After all services starting up, please go to the Web Portal for further configuration. By default, the Web Portal address is [https://server\\_ipaddress:8443](https://server_ipaddress:8443)



**Figure 6: GWN Manager Start page**

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



## Configuring GWN Manager

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

```
/gwn/gwn config
```

### Warnings:

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

```
/gwn/gwn restart
```

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

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

## Upgrading GWN Manager

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

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

```
/gwn/gwn restart
```

## Uninstalling GWN Manager

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

```
rpm -e gwn gwn-redis gwn-mariadb gwn-nginx
```

```
rm -rf /gwn
```



## Important Notes

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

## First Use

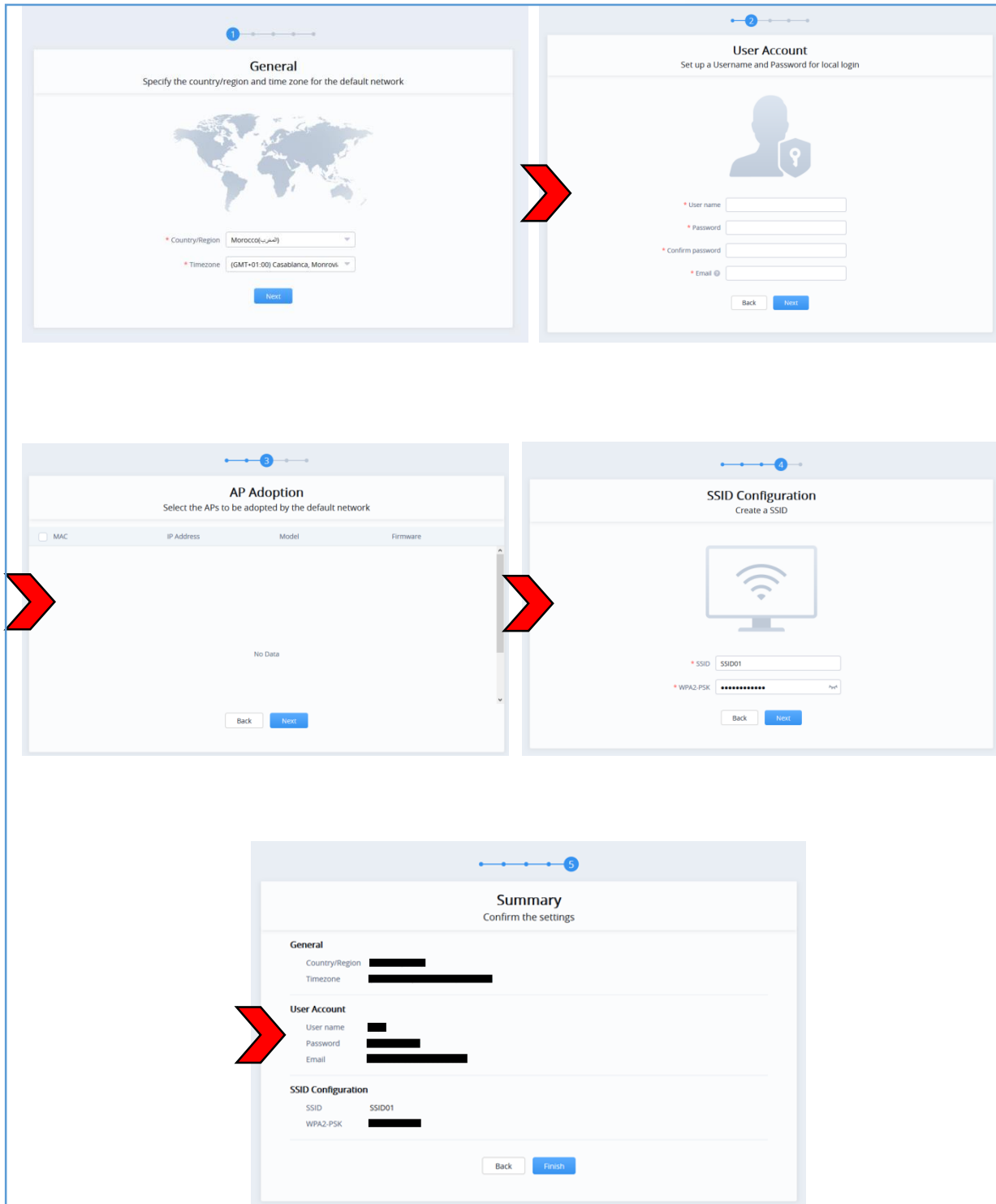
The GWN Manager provides an easy and intuitive Web UI to manage and monitor GWN76xx Access Points, it provides users access to all GWN Access Points settings, without any additional on-premise infrastructure.

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

**Table 4: GWN Manager Setup Wizard**

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





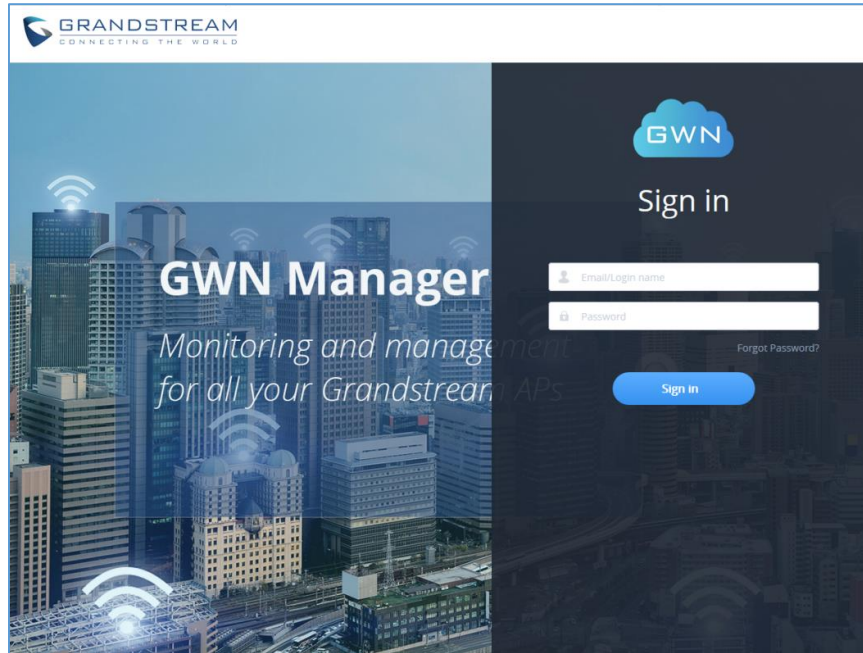
The figure displays five sequential screenshots of the GWN Manager Wizard setup process, connected by red arrows indicating the flow:

- General (Step 1):** "Specify the country/region and time zone for the default network." Includes a world map and dropdowns for Country/Region (Morocco) and Timezone (GMT+01:00 Casablanca, Morocco).
- User Account (Step 2):** "Set up a Username and Password for local login." Includes fields for User name, Password, Confirm password, and Email.
- AP Adoption (Step 3):** "Select the APs to be adopted by the default network." Shows a table with columns: MAC, IP Address, Model, and Firmware. The table is currently empty with "No Data" displayed.
- SSID Configuration (Step 4):** "Create a SSID." Includes fields for SSID (SSID01) and WPA2-PSK.
- Summary (Step 5):** "Confirm the settings." A review screen showing the configured values for General, User Account, and SSID Configuration.

**Figure 7: GWN Manager Wizard**

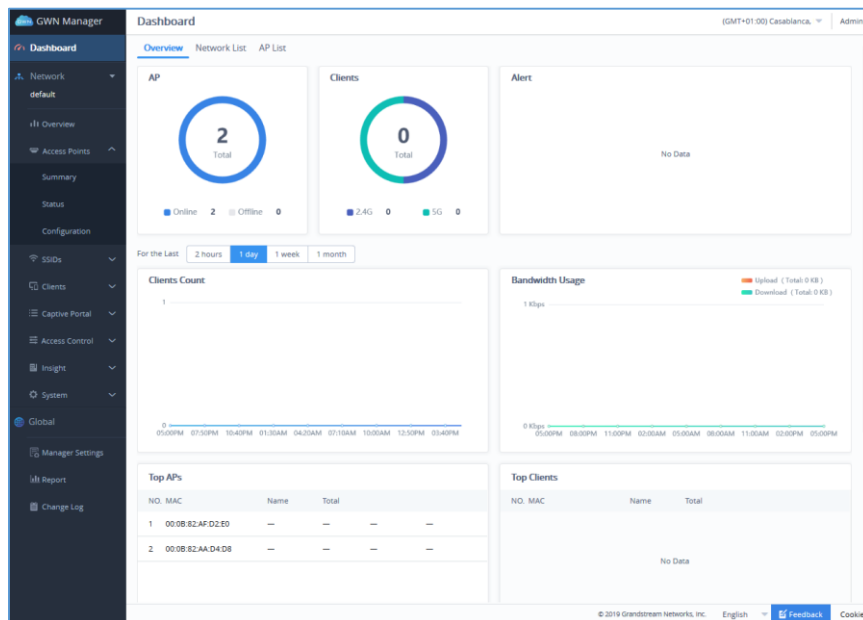
## Sign up to GWN Manager

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



**Figure 8: GWN Manager Login Page**

The following page will be displayed:



**Figure 9: GWN Manager Dashboard**

## GETTING STARTED WITH GWN MANAGEMENT PLATFORM

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

### GWN76xx LED Patterns

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

Table 5: LED Patterns

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

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





## Adding GWN76XX to GWN.Cloud

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

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

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

There are 3 methods to add GWN76xx to the cloud:

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

### Method 1: Adding New AP Manually

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

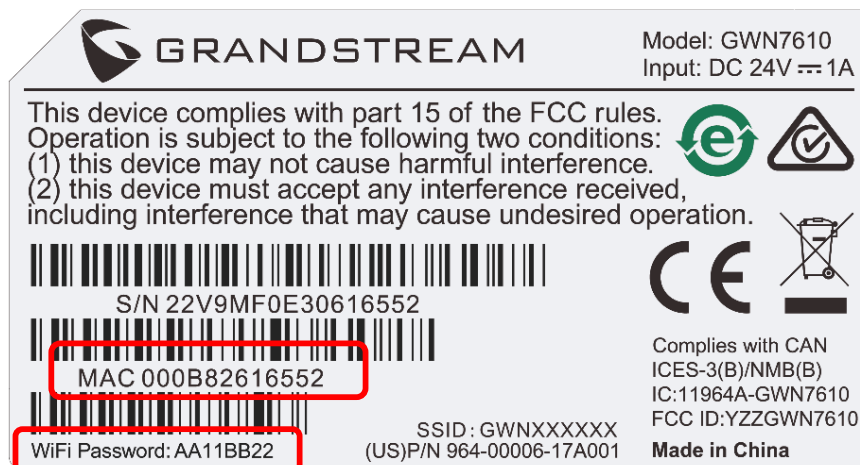
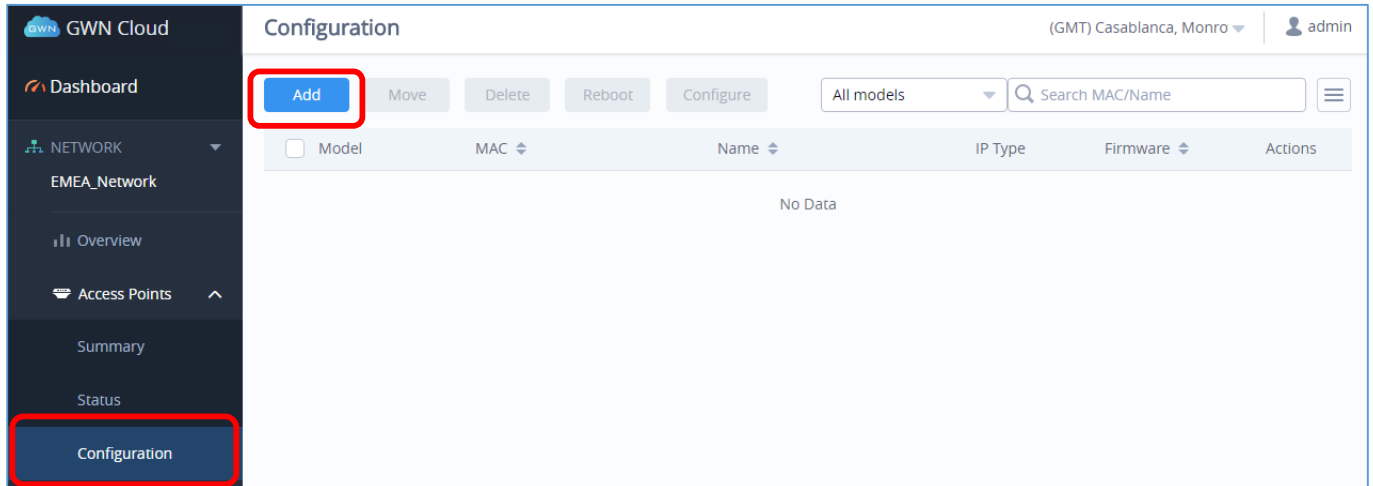


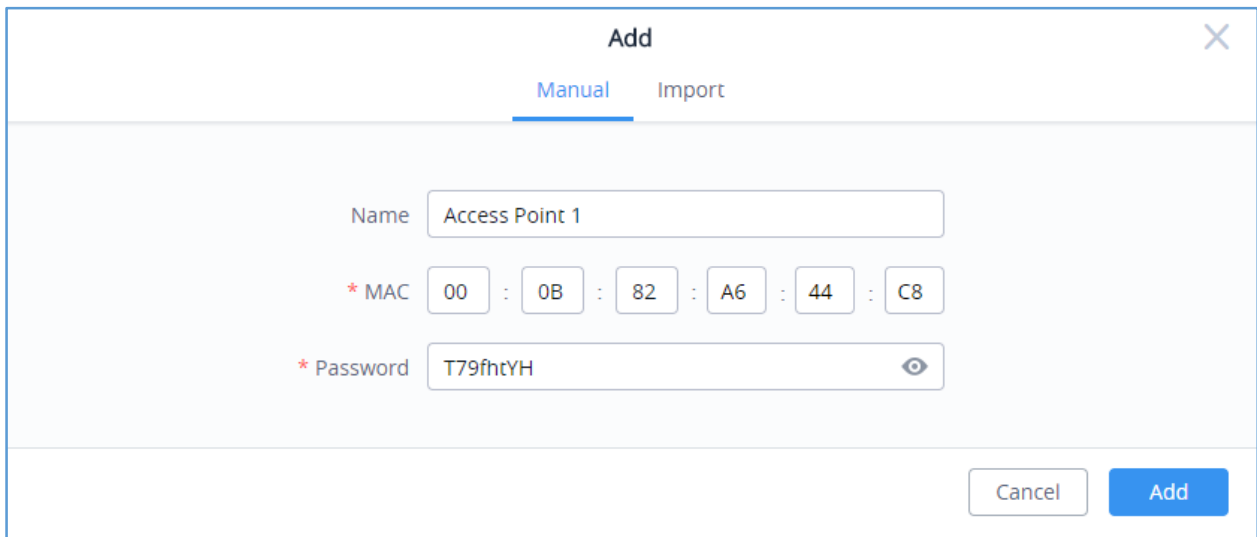
Figure 10: GWN Access Point MAC and Wi-Fi Password

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



**Figure 11: Adding New Access Point to GWN.Cloud**

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



**Figure 12: Adding Access Points Manually**

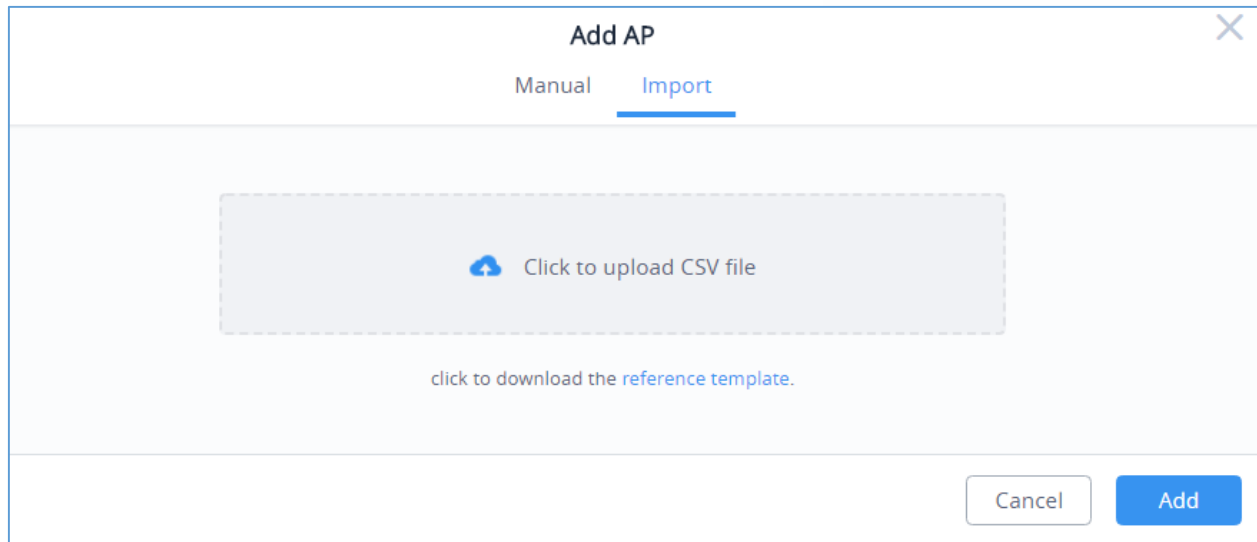
5. Click on **Add** and reset your Access Point. After reset, it will be added automatically to your Cloud account and you will be able to monitor/manage it.

### Bulk-add AP using CSV file import

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

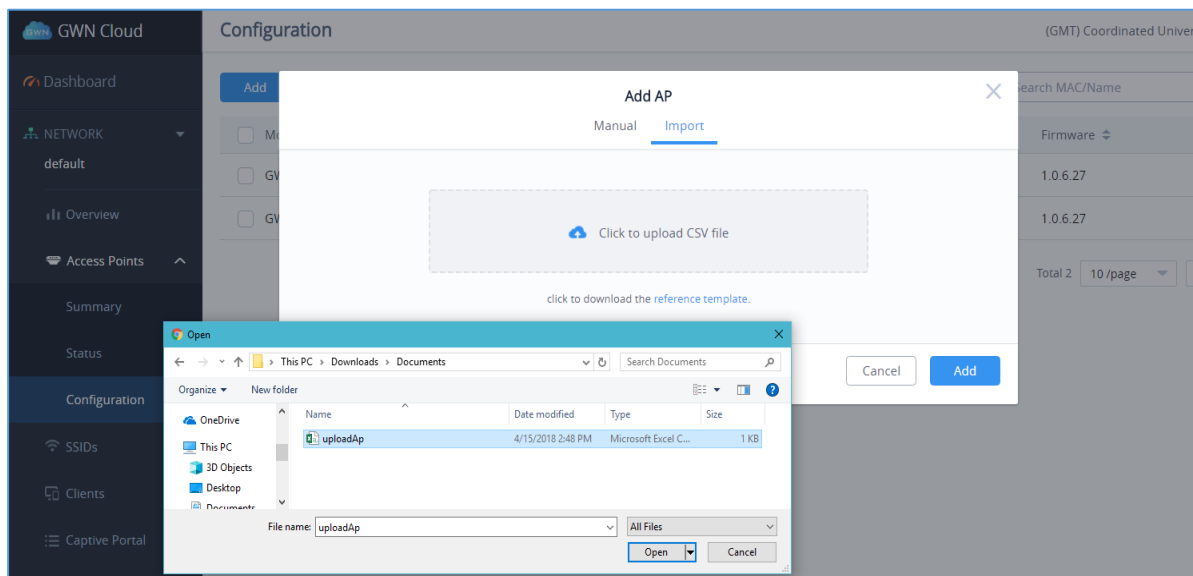
- 1- After clicking on **Add** under the menu **Access Points** → **Configuration**, click on **Import** Tab.





**Figure 13: Import CSV file for APs**

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



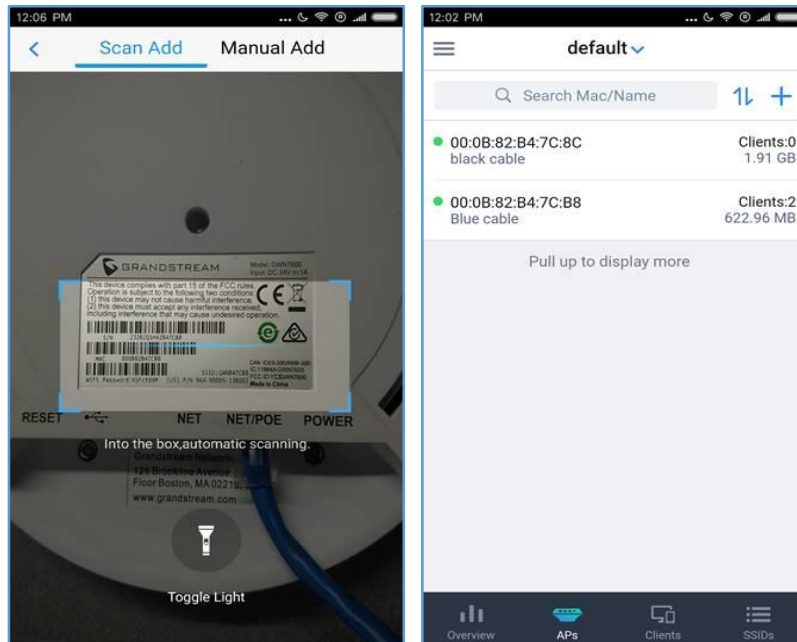
**Figure 14: Upload CSV file**

## Method 2: Adding New AP using GWN.Cloud Application

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







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

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



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

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

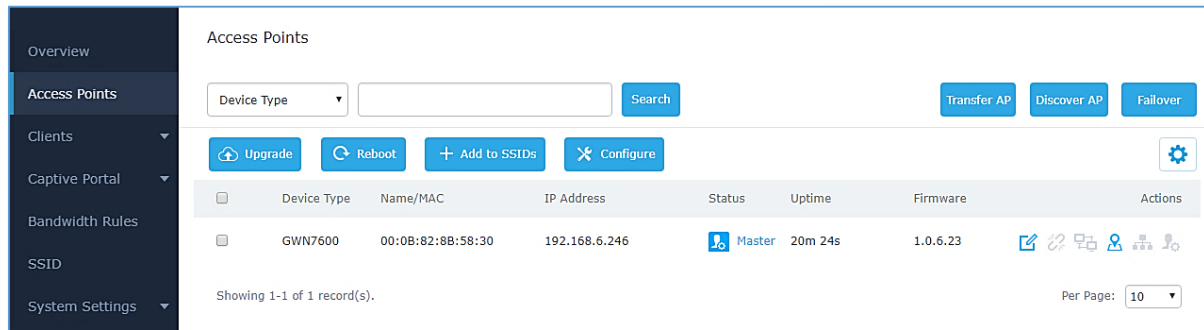
Status							
(GMT) Coordinated Univer   gstest							
● Online: 3							
Model	MAC	Name	IP Address	Uptime	Channel	Clients	Actions
● GWN7600	00:0B:82:A6:44:C8	GWN7600B	192.168.5.191	1h 5m	2.4G 1 5G 40	5	 
● GWN7600	00:0B:82:AF:D2:58	GWN7600A	192.168.5.189	1h 7m	2.4G 11 5G 40	0	 
● GWN7600	00:0B:82:AF:D2:E0	GWN7600C	192.168.5.190	13m	2.4G 1 5G 36	0	 
Total 3 10/page < 1 >							

**Figure 16: Access Points Status**

### Method 3: Transfer APs from Local Master

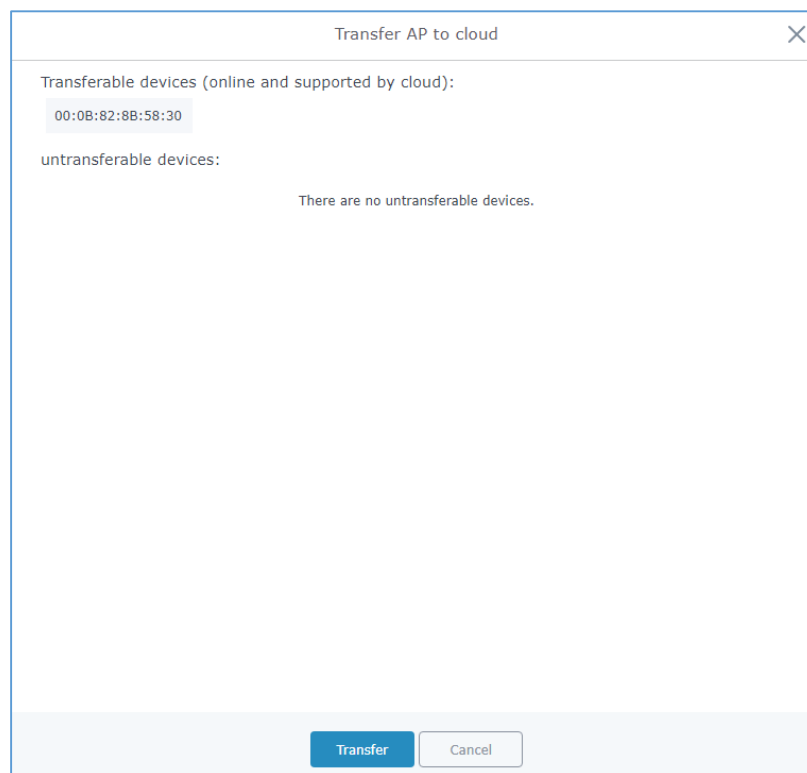
Another method to add GWN APs to the cloud is by transferring them to the cloud from the local Master AP. Follow these steps to achieve this:

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



**Figure 17: Master AP - Access Points**

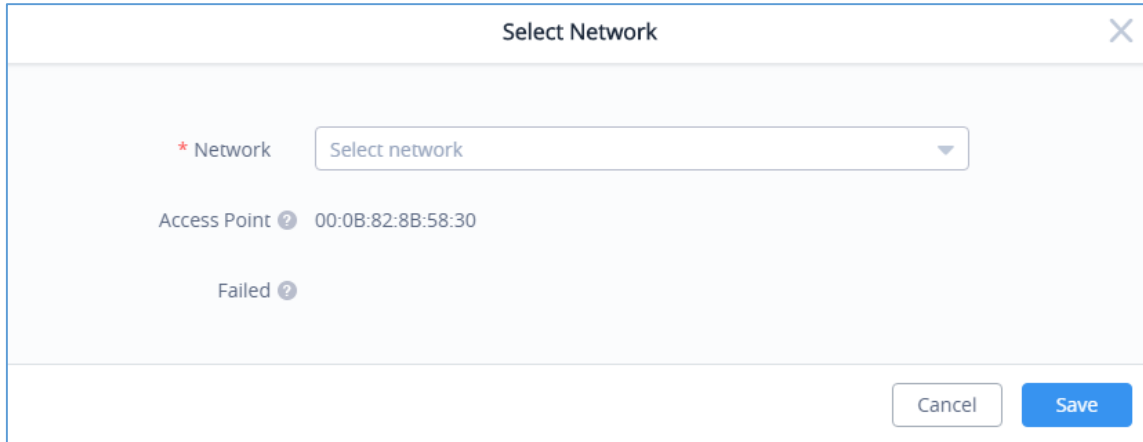
2. Press **Transfer AP** button. A new window will display “Transferable devices” list as shown below.



**Figure 18: Transfer AP to Cloud**

3. Press **Transfer** button. The web browser will redirect to GWN.Cloud login page.
4. Once logged in to the cloud, the configuration page “Select Network” will be displayed:

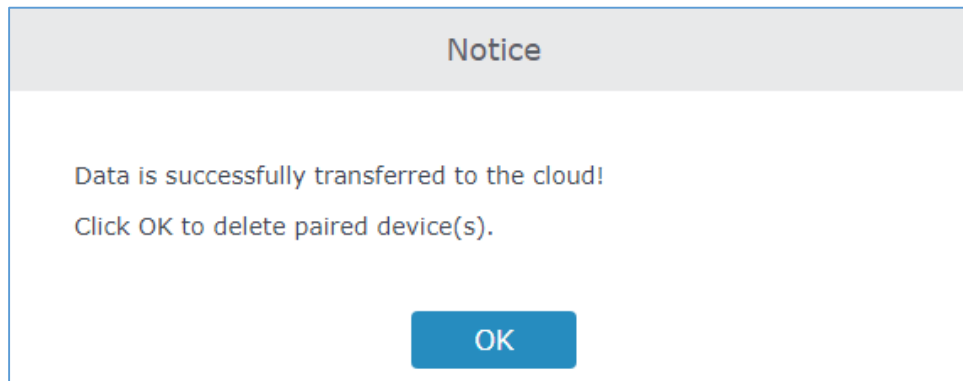




The dialog box titled "Select Network" contains a close button (X) in the top right corner. Inside, there is a label "\* Network" followed by a dropdown menu with the text "Select network". Below this, the text "Access Point ? 00:0B:82:8B:58:30" is displayed. Further down, the text "Failed ?" is shown. At the bottom right, there are two buttons: "Cancel" and "Save".

**Figure 19: Select Network**

- **Access Point:** Shows the MAC address of the passed check device.
  - **Failed:** Shows the MAC address of the authentication failed or added.
5. Select **Network** from the drop-down list to which the AP will be assigned.
  6. Press **Save** button to confirm.
  7. Once added to the cloud, Master AP web UI will display following successful notice.



The dialog box titled "Notice" has a grey header bar with the title "Notice". The main content area contains the text "Data is successfully transferred to the cloud!" followed by "Click OK to delete paired device(s)". At the bottom center, there is a blue button labeled "OK".

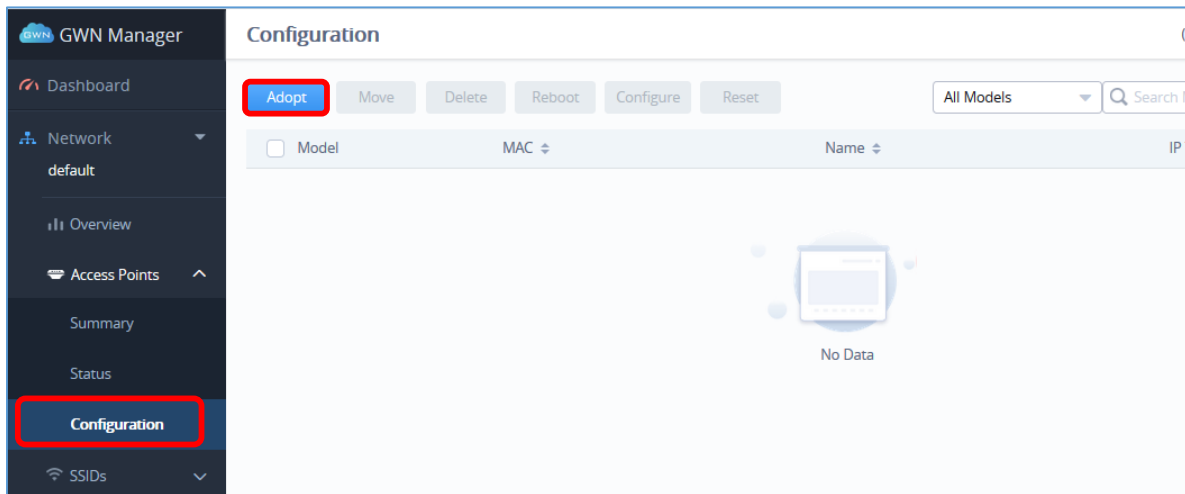
**Figure 20: Transfer AP to Cloud - Success**



## Adopt GWN76XX to GWN Manager

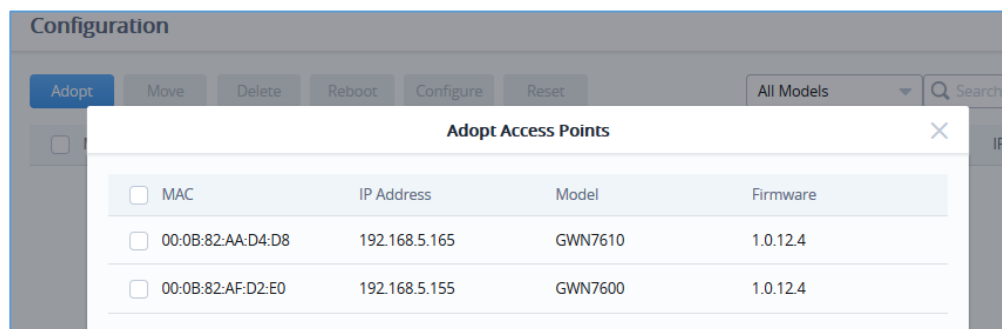
**Note:** Refer to **[REQUIREMENTS]** section of this document to make sure your GWN76xx is using the proper firmware version. If not, please upgrade the units before adding them to GWN Manager.

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



**Figure 21: Adding New Access Point to GWN Manager**

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



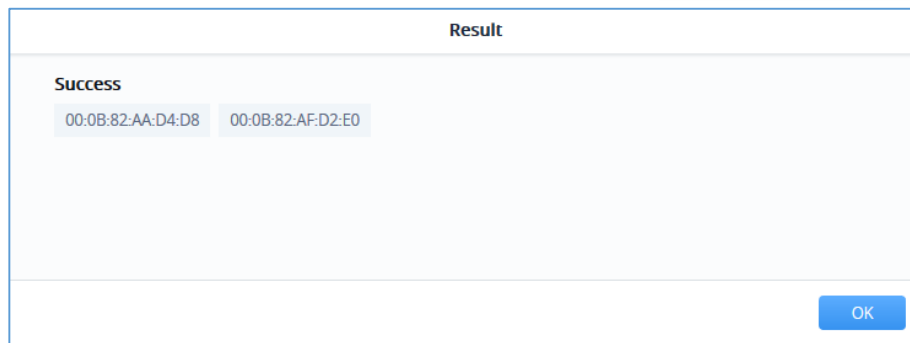
**Figure 22: Auto detect Access Points**

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

<input checked="" type="checkbox"/>	MAC	IP Address	Model	Firmware
<input checked="" type="checkbox"/>	00:0B:82-AA:D4:D8	192.168.5.165	GWN7610	1.0.12.4
<input checked="" type="checkbox"/>	00:0B:82-AF:D2:E0	192.168.5.155	GWN7600	1.0.12.4

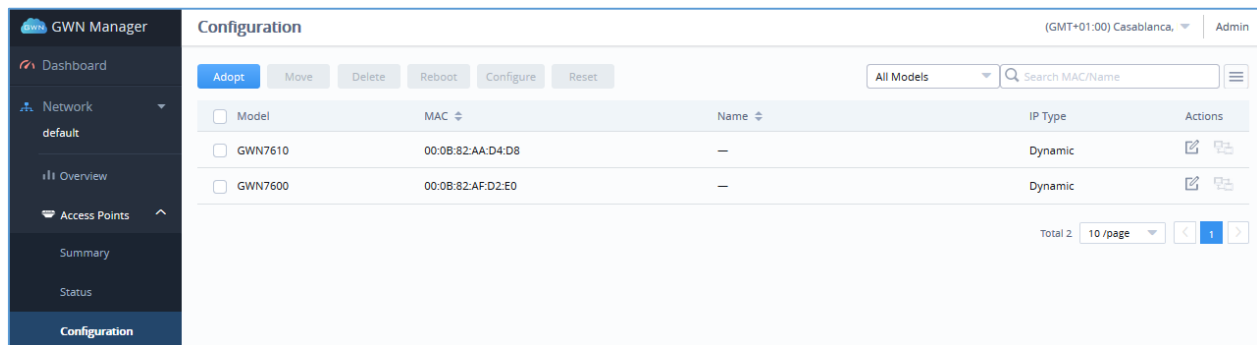
**Figure 23: Select Access Points**

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



**Figure 24: Confirm APs Adoption**

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



**Figure 25: Adopted Access Points**

## Discover GWN76XX

### Method 1: Auto Discovery

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

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

### Method 2: Manual discovery

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



```
Main Menu

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

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

[1] Manager Address: :10014
[x] Back

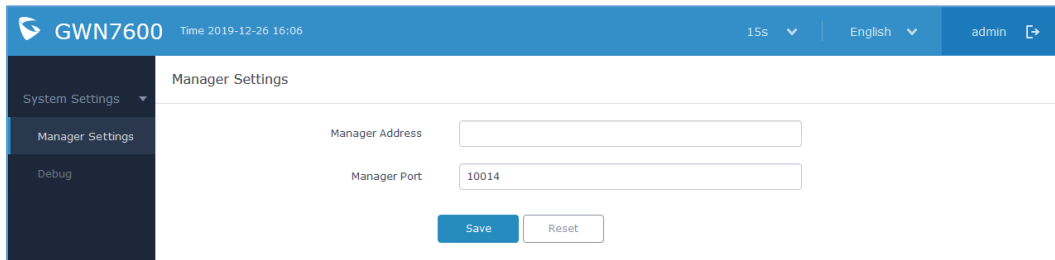
Select by pressing the [number] or [letter] and then ENTER
1
[x] Back

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

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

Figure 26: Manager Settings – SSH

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



The screenshot shows the WebUI of a GWN7600 device. The top bar includes the device name 'GWN7600', the time '2019-12-26 16:06', a refresh button '15s', a language dropdown 'English', and a user profile 'admin'. On the left, a sidebar menu has 'System Settings' (expanded), 'Manager Settings' (selected), and 'Debug'. The main content area is titled 'Manager Settings' and contains two input fields: 'Manager Address' (empty) and 'Manager Port' (containing '10014'). Below these fields are 'Save' and 'Reset' buttons.

Figure 27: Manager Settings – Slave WebGUI



# DASHBOARD

## Overview

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

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

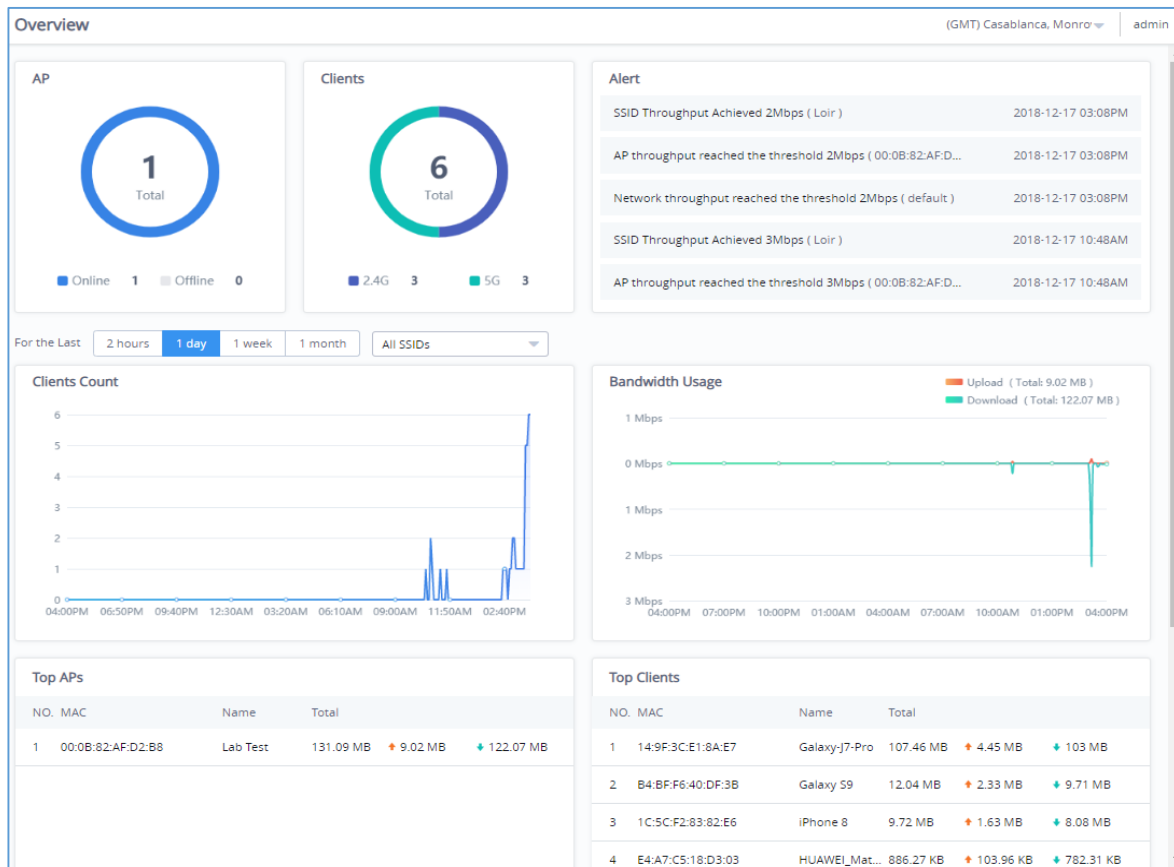


Figure 28: GWN.Cloud Dashboard - Overview

The following table describes each section:

**Table 6: Dashboard Description**

Section	Description
<b>Access Points</b>	Displays the number of Access points monitored as well as their status (Offline/Online)
<b>Clients</b>	Displays the total number of clients connected to the monitored APs, in addition to the band they are connected to 2.4G or 5G.
<b>Alerts</b>	This section shows alerts the administrator about any wrong behavior, based on the configured Alerts. (Refer to Alert section under Settings for more details)
<b>Clients Count</b>	<p>It shows the number of clients connected at a specific period of time; the administrator can toggle between four different periods of time:</p> <ul style="list-style-type: none"> <li>• <b>2 hours:</b> Displays the connected clients graph for the two last hours.</li> <li>• <b>1 day:</b> Displays the connected clients graph for the last day.</li> <li>• <b>1 week:</b> Displays the connected clients graph for the last week.</li> <li>• <b>1 month:</b> Displays the connected clients graph for the last month.</li> </ul>
<b>Bandwidth usage</b>	This section shows the bandwidth usage (Upload/Download) by all the clients, it provides the BW statistics for both Download and upload.
<b>Top APs</b>	Displays the top APs that consumed the max of the bandwidth/data
<b>Top Clients</b>	Lists the clients that downloaded/uploaded the max of data
<b>Top SSIDs</b>	Displays the SSIDs that are mostly used by clients.

## Network List

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



Dashboard

(GMT) Casablanca, Monro

administrator1







Overview

Network List

AP List

Create Network

Search Name

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

Total 3

10 /page

<

1

>

Figure 29: GWN.Cloud Dashboard - Network List

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

Create Network

\* Network Name

Network1

Country/Region

Morocco

Time Zone

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

Network Administrator

admin@grandstream.com

Optional Account

Clone Network

Select a network to clone

Cancel

Save

Figure 30: Create a New Network

Table 7: Create a New Network Settings

Setting	Description
Network Name	Enter the network Name to identify different networks in your environment.
Country/Region	Select the country/Region, this is required to set the Wi-Fi specifications of your

	country on GWN AP.
<b>Time Zone</b>	Select your time zone.
<b>Network Administrator</b>	This field displays the list of administrators that can manage this network.
<b>Clone Network</b>	When you have an existing Network, you can choose to clone the new one with the already existing network.

- Administrator can search for specific Network by name using

## AP List

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

Dashboard(GMT) Coordinated Univergstest

OverviewNetwork ListAP List

All models

Q

Search MAC/Name

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

Total 3

10/page

<

1

>

**Figure 31: GWN.Cloud Dashboard – AP List**

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

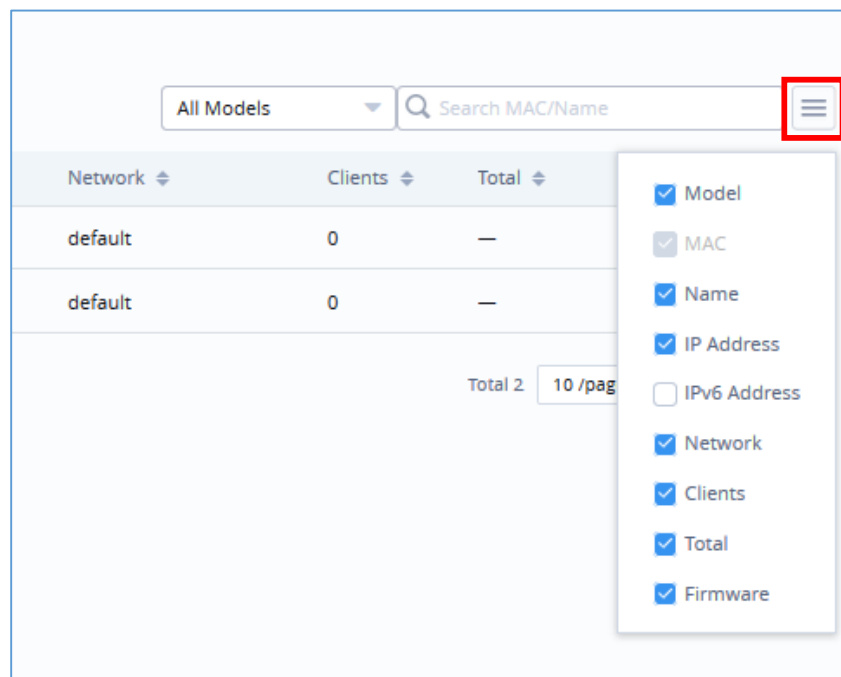
- Access Point Model.
- MAC address of the AP.
- Name of the AP.
- The IP address of the AP.
- The network Group to which the AP is assigned.
- The number of clients connected to the AP.



- Total Data consumed by the AP.
- Firmware.

**Notes:**

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



**Figure 32: Customize AP List Table Fields**

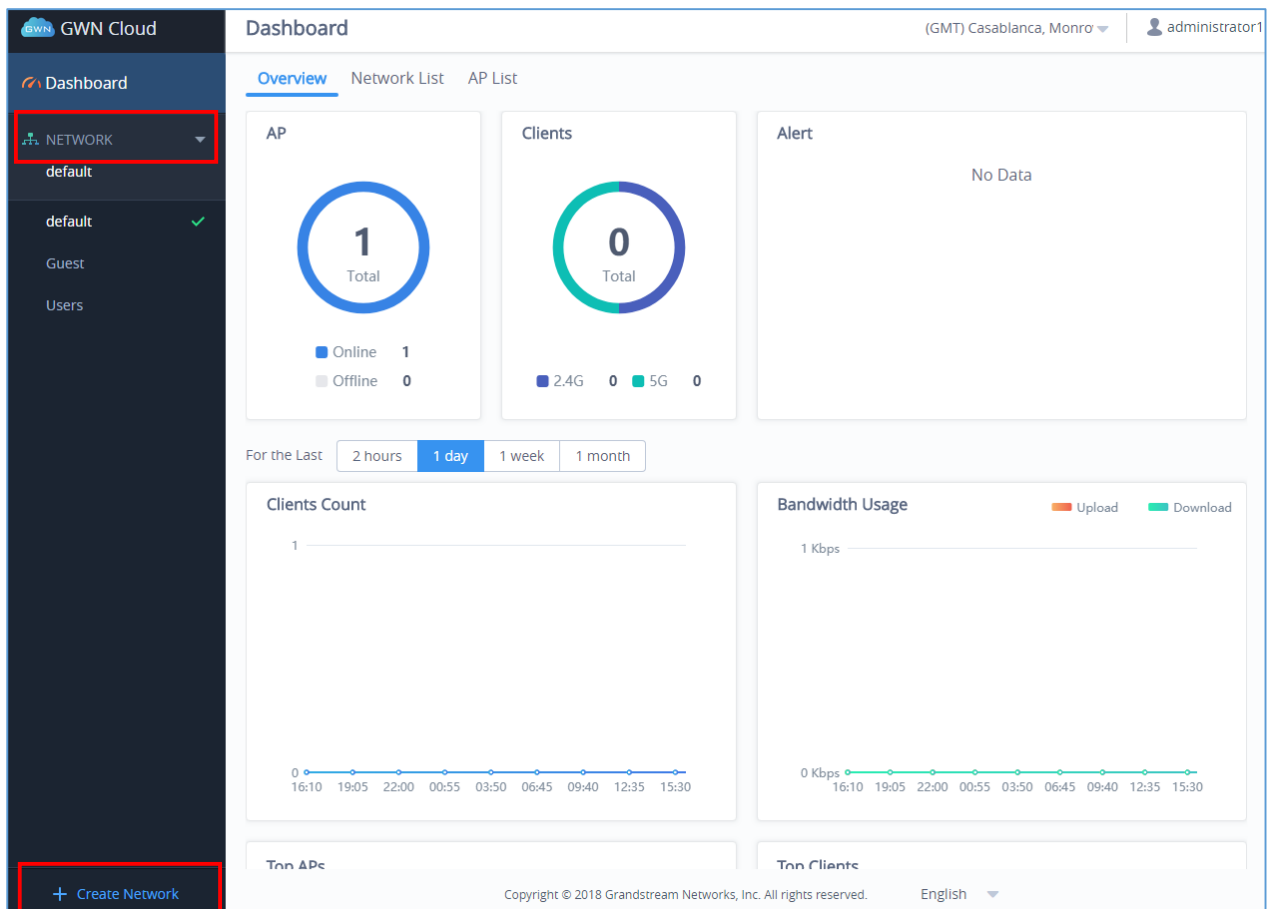


## NETWORK

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

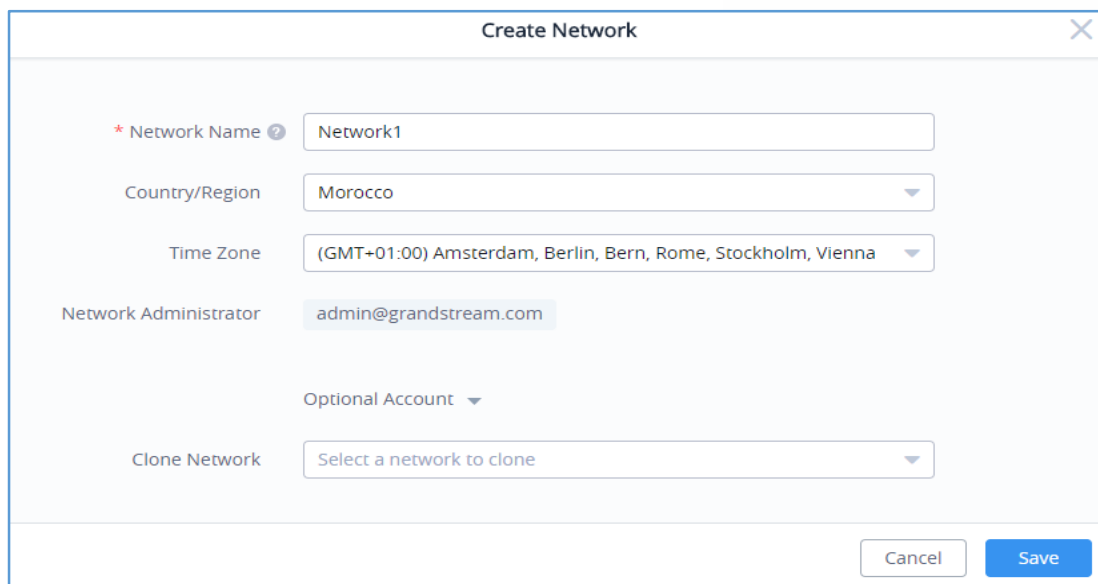
### Create a New Network

1. Click on **Network** and a list of the networks will be displayed.
2. Click on **+ Create Network** to add new network to your Platform Account.



**Figure 33: Network List and Network Creation Button**

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



The 'Create Network' dialog box contains the following fields and controls:

- Network Name:** A text input field with a red asterisk and a help icon, containing the value 'Network1'.
- Country/Region:** A dropdown menu showing 'Morocco'.
- Time Zone:** A dropdown menu showing '(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'.
- Network Administrator:** A text input field containing 'admin@grandstream.com'.
- Optional Account:** A small dropdown arrow.
- Clone Network:** A dropdown menu showing 'Select a network to clone'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

**Figure 34: Create Network**

**Table 8: Create a New Network Settings**

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

## Overview Page

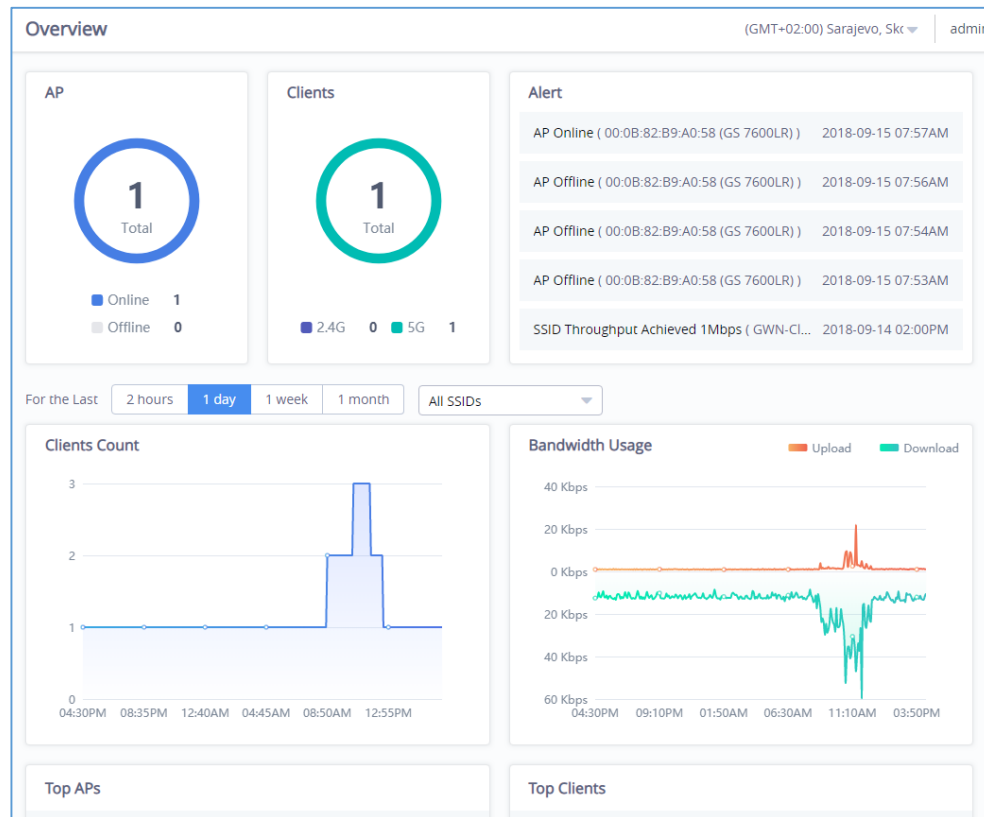
The overview page provides an overall view of the network selected. The administrator must select a network first and click on **Overview** in order to display the network overview including:

- Access Points added to this network
- Clients connected to the network





- Different Alerts
- Clients Count
- Bandwidth usage
- Top APs
- Top Clients
- Top SSIDs



**Figure 35: Overview Page Displays Information related to Specific Network**

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

## ACCESS POINTS

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

1. Summary
2. Status
3. Configuration

### Summary

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

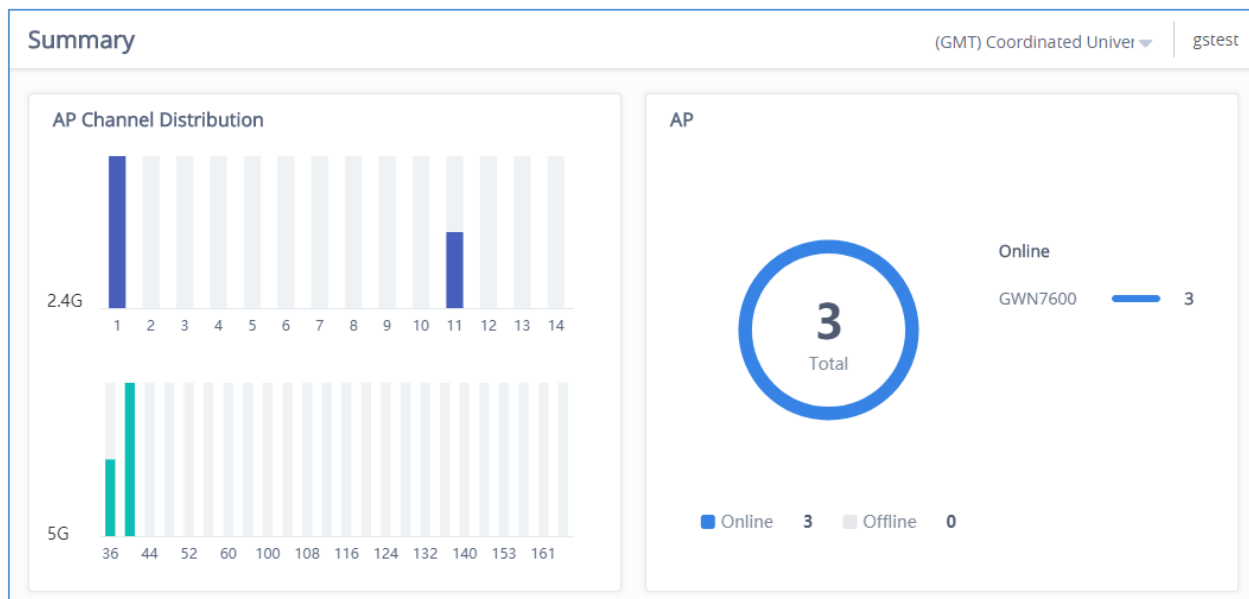








Figure 36: Access Points – Summary

### Status



The Status page lists all the access points assigned to the selected network, along with the possibility to perform some basic operations such as 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.



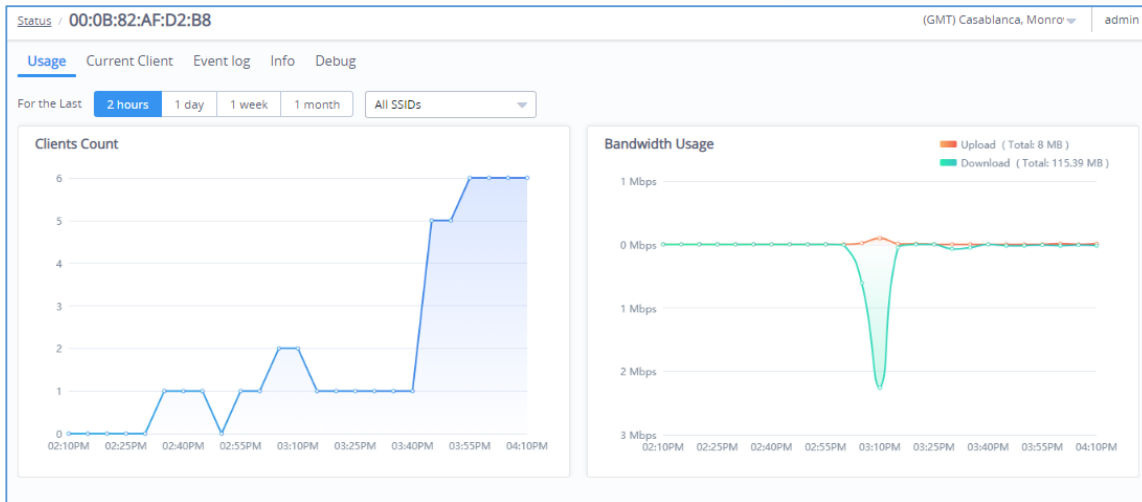
Status							
<div> <span>Online: 3</span> <div> <input type="text" value="Search MAC/Name"/> </div> </div>							
Model	MAC	Name	IP Address	Uptime	Channel	Clients	Actions
<span>●</span> GWN7600	00:0B:82:A6:44:C8	GWN7600B	192.168.5.191	1h 5m	2.4G 1 5G 40	5	 
<span>●</span> GWN7600	00:0B:82:AF:D2:58	GWN7600A	192.168.5.189	1h 7m	2.4G 11 5G 40	0	 
<span>●</span> GWN7600	00:0B:82:AF:D2:E0	GWN7600C	192.168.5.190	13m	2.4G 1 5G 36	0	 
<div> Total 3 <div> 10 /page </div> <div> 1 </div> </div>							

**Figure 37: Access Points - Status**

**Table 9: Access Points Status Parameters**

<b>Model</b>	GWN Access Point Model: GWN7610, GWN7600, GWN7600LR or GWN7630 (Beta)
<b>MAC</b>	MAC Address of the Access Point
<b>Name</b>	Access Point's name
<b>IP Address</b>	IP Address of the Access point
<b>Firmware</b>	Firmware of the Access point
<b>Uptime</b>	Uptime of the Access point
<b>Channel</b>	Channels used by this Access points for both 2G and 5G.
<b>Client</b>	Number of clients connected to the Access Point
<b>Actions</b>	<p>Locate Access point using  button.</p> <p>Press  to clear access point usage.</p>

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



**Figure 38: Usage of a Specific AP**

The first tab will display the data usage for the specified access point and allows the user to filter the traffic graph for the last 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.

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

(GMT+01:00) Casablanca,

Usage

Current Client

Event log

Info

Debug

Search MAC

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

**Figure 39: Current Clients - Stats per AP**

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



Status / 00:0B:82:AF:D2:B8 (GMT) Casablanca, Morocco

Usage Current Client Event log Info Debug

Search MAC

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

**Figure 40: Event Log per AP**

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

**Figure 41: AP Info**

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

- **Ping/Traceroute** tools, such as the **ping** utility, **traceroute** utility and **nslookup** tool.
- **Capture**, to capture traffic for different network groups and filter by IP, TCP 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.
- **SSH Remote Access**: This feature enables SSH access from GWN.cloud to your AP device, and this is mainly for extra troubleshooting method. Remote SSH will be automatically deactivated after 48 hours.



[Status](#) / 00:0B:82:AF:D2:58

[Usage](#)
[Current Client](#)
[Event log](#)
[Info](#)
[Debug](#)

[Ping/Traceroute](#)
[Capture](#)
[Core Files](#)
[SSH Remote Access](#)

\* Target

Tool

IPv4 Ping

Run

Figure 42: Debug Tool Tab

## Configuration

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



Configuration							
(GMT+01:00) Casablanca, ▼							
<div> <div>Add</div> <div>Move</div> <div>Delete</div> <div>Reboot</div> <div>Configure</div> <div>Reset</div> </div> <div> <div>All models</div> <div>Search MAC</div> </div>							
<input type="checkbox"/> Model	MAC ↕	Name ↕	Status ↕	IP Type	Channel	Tx Power	Actions
<input type="checkbox"/> GWN7610	00:0B:82:AA:D4:D8	—	Online	Dynamic	2.4G 1 5G 40	2.4G 20dBm 5G 20dBm	 
<div>Total 1</div> <div>10/page</div> <div>&lt; 1 &gt;</div>							

Figure 43: Access Points Configuration Page

### Add New Access Points

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

## Move Access Points

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

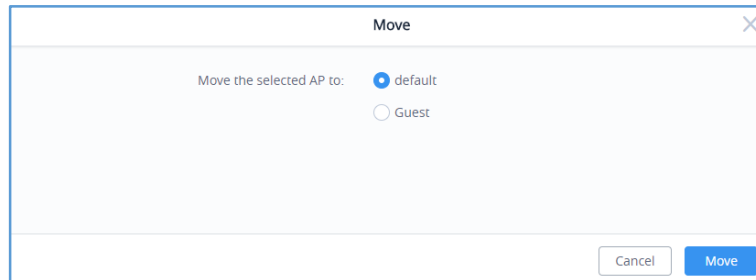


Figure 44: Moving Access Points between Networks

## Delete Access Points

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

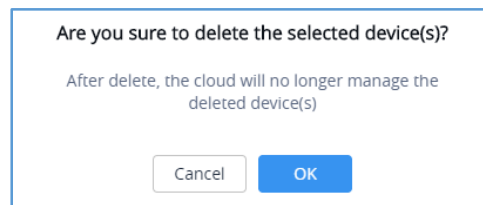


Figure 45: Delete Access Point

## Reboot Access Points

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

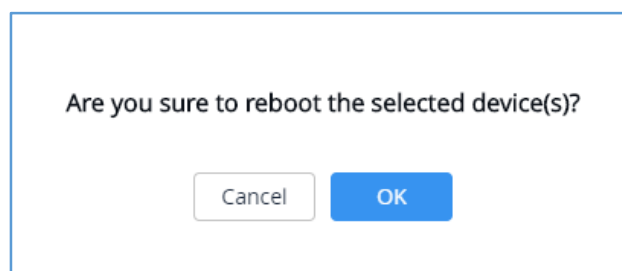
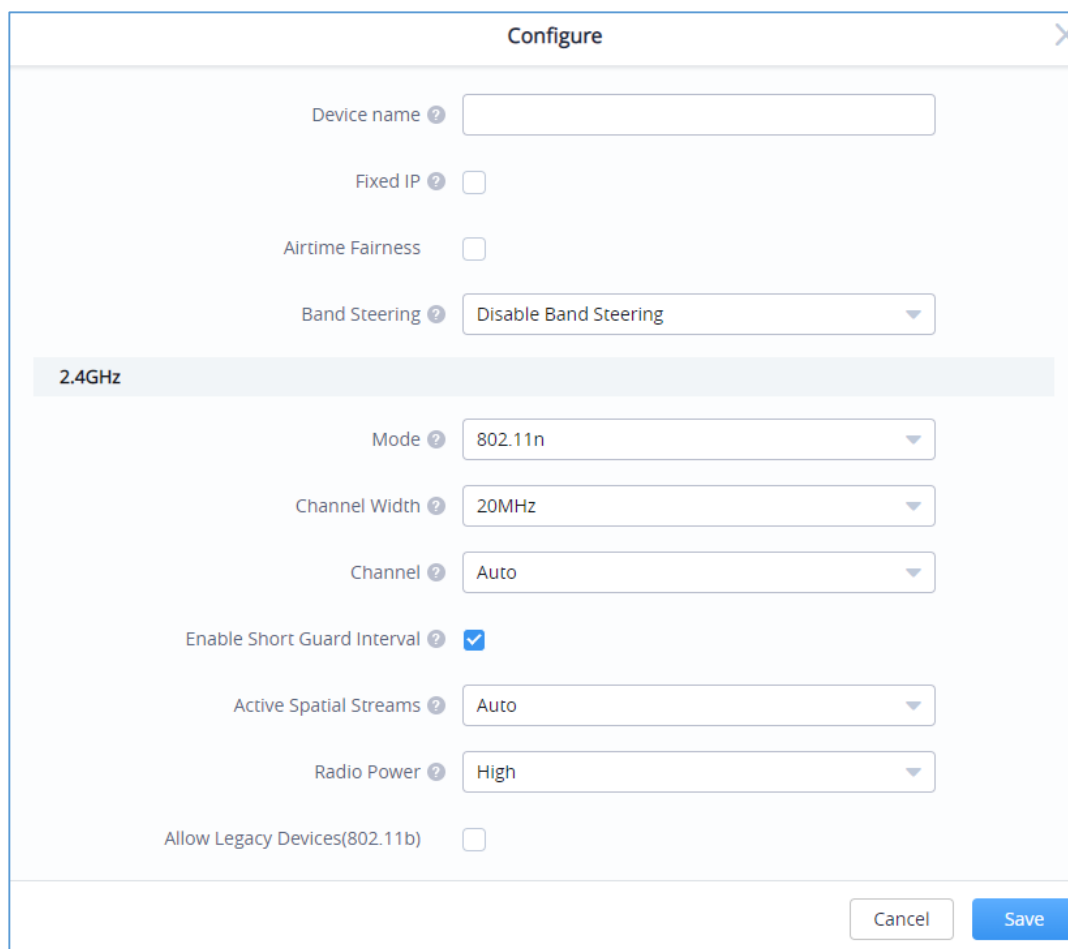


Figure 46: Reboot Access Point



## Configure Access Points

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



The configuration page is titled "Configure" and contains the following settings:

- Device name**: Text input field.
- Fixed IP**: Checkbox.
- Airtime Fairness**: Checkbox.
- Band Steering**: Dropdown menu with "Disable Band Steering" selected.
- 2.4GHz**: Section header for 2.4GHz settings.
- Mode**: Dropdown menu with "802.11n" selected.
- Channel Width**: Dropdown menu with "20MHz" selected.
- Channel**: Dropdown menu with "Auto" selected.
- Enable Short Guard Interval**: Checkbox, checked.
- Active Spatial Streams**: Dropdown menu with "Auto" selected.
- Radio Power**: Dropdown menu with "High" selected.
- Allow Legacy Devices(802.11b)**: Checkbox.

Buttons: Cancel, Save.

**Figure 47: Access Point Configuration Page**

The following settings can be configured from this page:

**Table 10: Access Point Configuration Settings**

<b>Device Name</b>	Set GWN76xx's name to identify it along with its MAC address.
<b>Fixed IP</b>	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.
<b>Airtime Fairness</b>	Allow faster clients to have more airtime than slower clients.



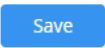


<b>Band Steering</b>	<p>Band Steering will help redirecting clients to a radio band 2.4G or 5G, depend on what's supported by the device, for efficient use and to benefit from the maximum throughput. Four options are allowed by GWN.Cloud:</p> <ul style="list-style-type: none"> <li>• <b>Disable Band steering:</b> This will disable the band steering feature and the access point will accept the band chosen by the client.</li> <li>• <b>2G in Priority:</b> 2G Band will be prioritized over 5G Band</li> <li>• <b>5G in Priority:</b> 2G Band will be prioritized over 5G Band</li> <li>• <b>Balance:</b> GWN will balance between the clients connected to 2G and those connected to 5G.</li> </ul>
<b>Client Steering (Beta)</b>	<p>This feature will help Wi-Fi client to roam to other APs within same Network. Roaming threshold can be configured using RSSI Threshold and Client Access Threshold. Both parameters will show up only when Client Steering is enabled.</p>
<b>RSSI Threshold</b>	<p>GWN76xx will start monitoring the RSSI for the clients in order to redirect them to another GWN AP in the same network. This prevents clients from remaining associated with AP with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients. Default is -75.</p>
<b>Client Access Threshold</b>	<p>GWN76xx will start monitoring the number of clients' connections with the AP, once reaching configured threshold, it will roam to the other. Default is 30.</p>
<b>Mode</b>	<p>Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.</p>
<b>Channel Width</b>	<p>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.</p>
<b>Channel</b>	<p>Select "Auto" or a specific channel. Default is "Auto". Note that the proposed channels depend on Country Settings under <b>System → Settings</b>.</p>

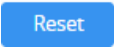



<b>Enable Short Guard interval</b>	Check to activate this option to increase throughput.
<b>Active Spatial streams</b>	Choose active spatial stream. Available options: "Auto", "1 stream" and "2 streams".
<b>Radio Power</b>	Set the Radio Power depending on desired cell size to be broadcasted, four options are available: "Low", "Medium", "High" and "custom" Default is "High".
<b>Custom 2.4GHz/GHz Tx Power (dBm)</b>	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.
<b>Allow Legacy Devices(802.11b)</b>	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.

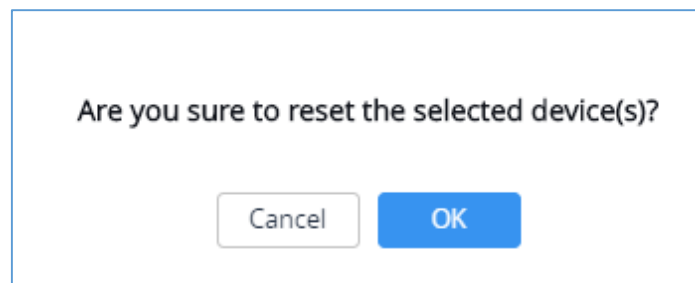


Figure 48: Reset Access Point



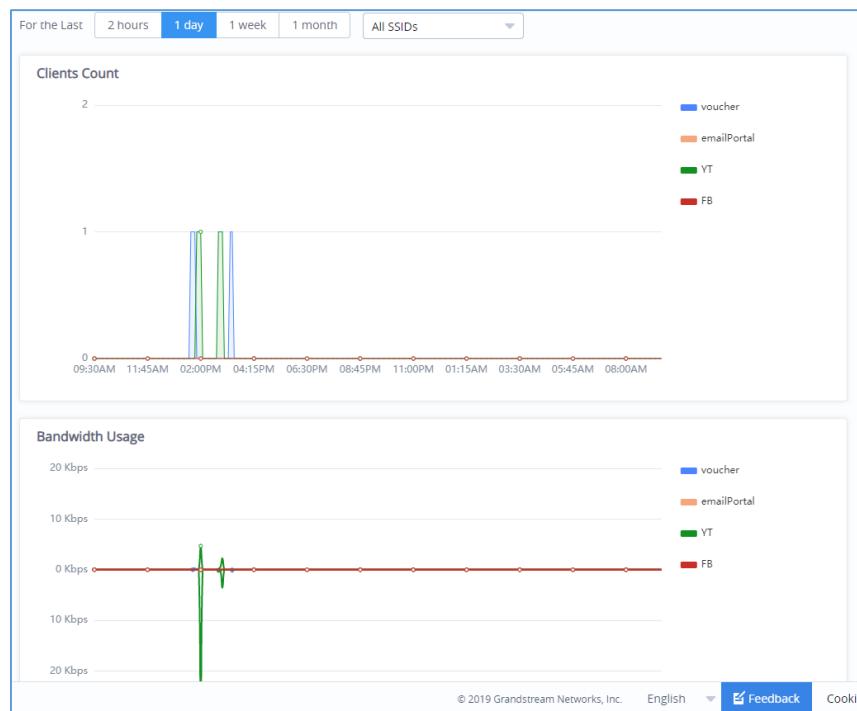
## SSID

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

- Summary
- Configuration

### Summary

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







**Figure 49: SSIDs - Summary**

### Configuration

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



Configuration <span style="float: right;">(GMT) Casablanca, Morocco   admin</span>									
<div> <div>Add</div> <div>(2/16)</div> <div></div> </div>									
Name	Wi-Fi	VLAN ID	Online Devices	Schedule	Security Mode	MAC Filtering	Client Isolation	Portal	Actions
GWN-Cloud	Enabled	—	0	Off	WPA2	Disabled	Off	Off	 
Guest_WiFi	Enabled	—	1	Off	WPA2	Disabled	Off	Off	 

**Figure 50: SSIDs - Configuration**

## Wi-Fi Settings

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

Add SSID

Wi-Fi Settings

Device Membership

Basic

\* SSID ?

Enabled

☐

VLAN

☐

SSID Band

Dual-Band

Access Security

Security Mode

WPA2

WPA Key Mode

PSK

WPA Encryption Type

AES

\* WPA Pre-Shared Key ?

Enable Captive Portal

☐

Cancel

Save

**Figure 51: SSIDs – Configuration – Wi-Fi Settings**

**Table 11: SSID Wi-Fi Settings**

Field	Description
<b>SSID</b>	Set or modify the SSID name.
<b>Enabled</b>	Check to enable Wi-Fi for the SSID
<b>VLAN</b>	Check to Enable VLAN and enter VLAN ID, otherwise, this SSID will be using the default network group.
<b>SSID Band</b>	Select the Wi-Fi band the GWN will use, three options are available: <b>Dual-Band, 2.4GHz or 5GHz</b>
<b>Security Mode</b>	<p>Set the security mode for encryption, 5 options are available:</p> <ul style="list-style-type: none"> <li>• <b>WEP 64-bit:</b> 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.</li> <li>• <b>WEP 128-bit:</b> 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.</li> <li>• <b>WPA/WPA2:</b> Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type.</li> <li>• <b>WPA2:</b> Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. Recommended configuration for authentication.</li> <li>• <b>Open:</b> No password is required. Users will be connected without authentication. Not recommended for security reasons.</li> </ul> <p><b>Note:</b> GWN products support for 802.1x (PEAP-MSCHAPv2 and EAP-TLS) requires external AAA server to permit authentication and centralized access management.</p>
<b>WEP Key</b>	<p>Enter the password key for WEP protection mode.</p> <p>This option is available when selecting <b>WEP64-bit/WEP128-bit</b> as <b>Security Mode</b></p>
<b>WPA Key Mode</b>	Select key mode (Pre-Shared Key or 802.1X Authentication).



<b>WPA Encryption Type</b>	Select Encryption type (AES or AES/TKIP).
<b>WPA Pre-Shared Key</b>	Configures the WPA pre-shared key. The input range: 8-63 ASCII characters or 8-64 hex characters. This option is available when selecting <b>PSK</b> as <b>WPA Key Mode</b> .
<b>RADIUS Sever Address</b>	Configures RADIUS authentication server address. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS Server Port</b>	Configures RADIUS Server Listening port (defaults to 1812). This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS Server Secret</b>	Enter the secret password for client authentication with RADIUS server. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS Accounting Server Address</b>	Configures the address for the RADIUS accounting server. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS Accounting Server Port</b>	Configures RADIUS accounting server listening port (Default is 1813). This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS Accounting Server Secret</b>	Enter the secret password for client authentication with RADIUS accounting server. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>RADIUS NAS ID</b>	Configures the Radius NAS ID used to notify the source of RADIUS access request so that, the RADIUS server can choose policy for that request. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .
<b>Enable Captive Portal</b>	Click on the checkbox to enable the captive portal feature.
<b>Captive Portal Policy</b>	Select the captive portal policy already created on the " <b>CAPTIVE PORTAL</b> " web page to be used in the created SSID.
<b>MAC Filter</b>	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to Wi-Fi. Default is Disabled.
<b>Enable Dynamic VLAN</b>	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile. This option is available when selecting <b>802.1x</b> as <b>WPA Key Mode</b> .



	<p><b>Note:</b> When using 802.1X authentication on your SSID with dynamic VLAN assignment. Admin does not need to create all VLAN SSIDs to match destination VLAN. On 1.0.11.1, AP will trunk its Ethernet with the VLAN assigned to Wi-Fi client through 802.1X</p>
<b>Client Isolation</b>	<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"> <li>• <b>Radio Mode:</b> Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76xx but they cannot communicate with each other.</li> <li>• <b>Internet Mode:</b> 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.</li> <li>• <b>Gateway MAC Mode:</b> 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.</li> </ul>
<b>Gateway MAC Address</b>	<p>This field is required when using <b>Client Isolation</b>, 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><b>Example:</b> 00:0B:82:8B:4D:D8</p>
<b>SSID Hidden</b>	<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>
<b>Beacon Interval</b>	<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"> <li>• <b><u>Using High Beacon Interval:</u></b> 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.</li> </ul>



	<ul style="list-style-type: none"> <li>• <b>Using Low Beacon Interval:</b> 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.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When AP enables several SSIDs with different interval values, the max value will take effect.</li> <li>2. When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500.</li> <li>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.</li> <li>4. When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500.</li> <li>5. Mesh feature will take up a share when it is enabled.</li> </ol> <p>Default value is 100ms. Valid range: 40 – 500 ms.</p>
<b>DTIM Period</b>	<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>
<b>Wireless Client Limit</b>	<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>
<b>Client Inactivity Timeout</b>	<p>AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.</p>





<b>Client Bridge</b>	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.
<b>Client Time Policy</b>	Configures the client time policy. Default is None.
<b>Convert IP multicast to unicast</b>	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.
<b>Schedule</b>	Select a schedule that will be applied to this SSID, schedules can be managed from the menu <b>"System → Schedule"</b> .
<b>Enable Minimum RSSI</b>	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in <b>Minimum RSSI (dBm)</b> .
<b>Minimum RSSI (dBm)</b>	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".
<b>Enable Minimum Rate</b>	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP.
<b>Minimum Rate (Mbps)</b>	Specify the minimum access rate. Once the client access rate is less than the specified value, AP will kick it off. Available values are: 1Mbps, 2Mbps, 5Mbps, 6Mbps, 9Mbps, 11Mbps or 12Mbps.
<b>Enable Voice Enterprise</b>	<p>Enable this feature to help clients connected to the GWN76xx to perform better roaming decision.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>



	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>11R is required for enterprise audio feature, 11V and 11K are optional.</li> <li>Enable Voice Enterprise is only available under “<b>WPA/WPA2</b>” and “<b>WPA2</b>” Security Mode.</li> </ol>
<b>Enable 11R</b>	Check to enable 802.11r
<b>Enable 11K</b>	Check to enable 802.11k
<b>Enable 11V</b>	Check to enable 802.11v
<b>ARP Proxy</b>	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.

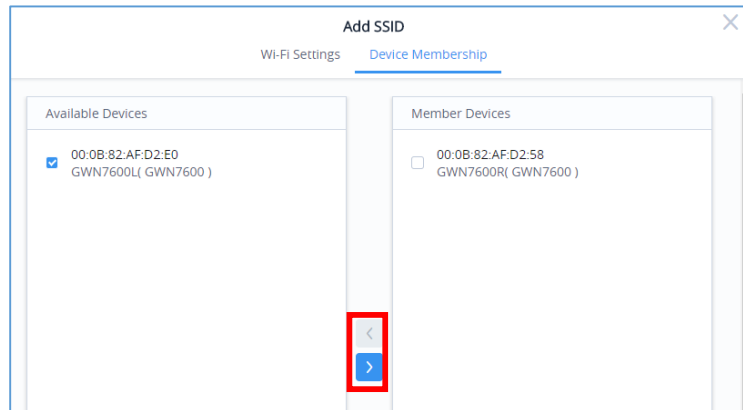



Figure 52: Device Membership - Available Devices

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

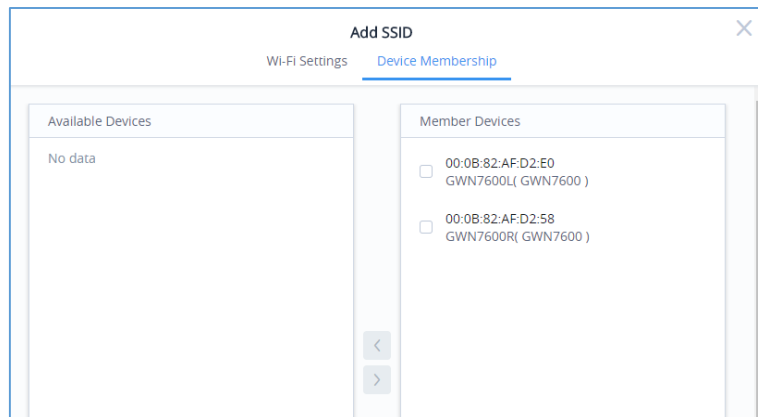


Figure 53: Device Membership - Members Devices

## SSID Limit

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



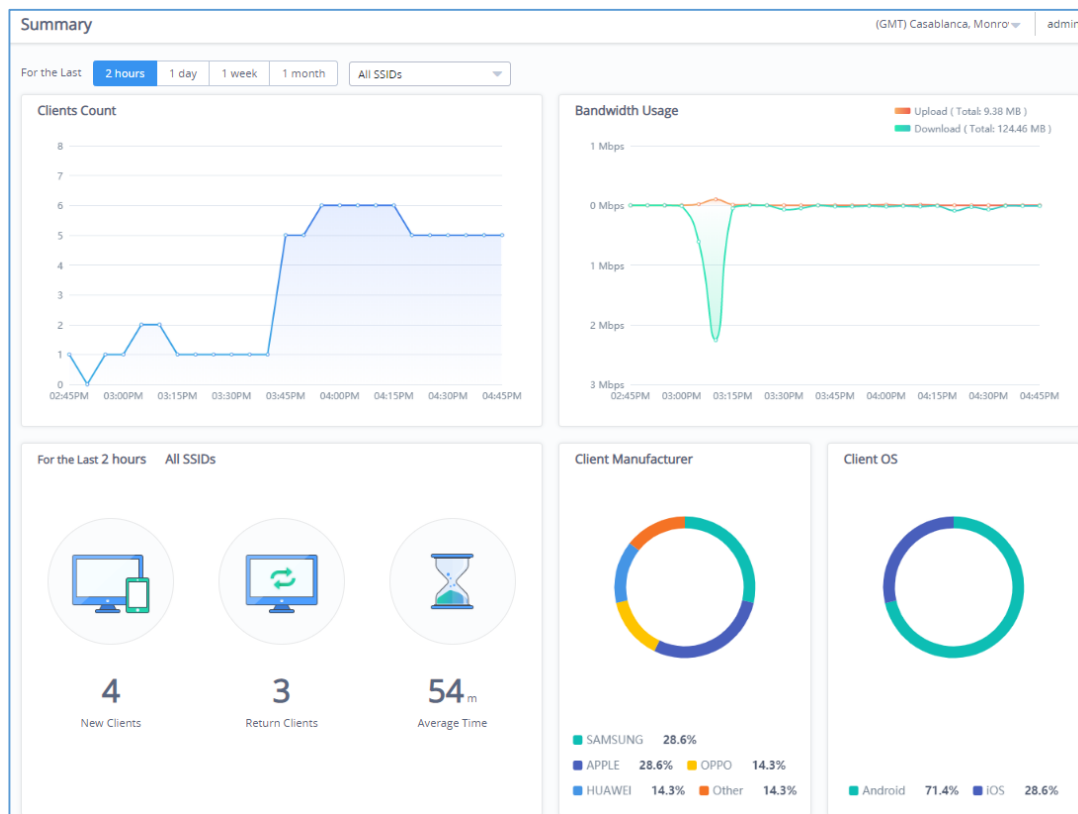
## CLIENTS

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

- Summary
- Status

### Summary

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



**Figure 54: Clients - Summary**

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

### Clients Count

Provides in real time the number of clients connected to the Access points, the administrator can filter select

the period for monitoring, which can be 2 hours, 1 day, 1 week or 1 month, and specify the SSID to monitor.

## Bandwidth Usage

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

## Clients Statistics for Last Day

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

## Client Manufacturer





















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

## Client OS


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




## Status Page

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


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

**Figure 55: Clients Status**

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

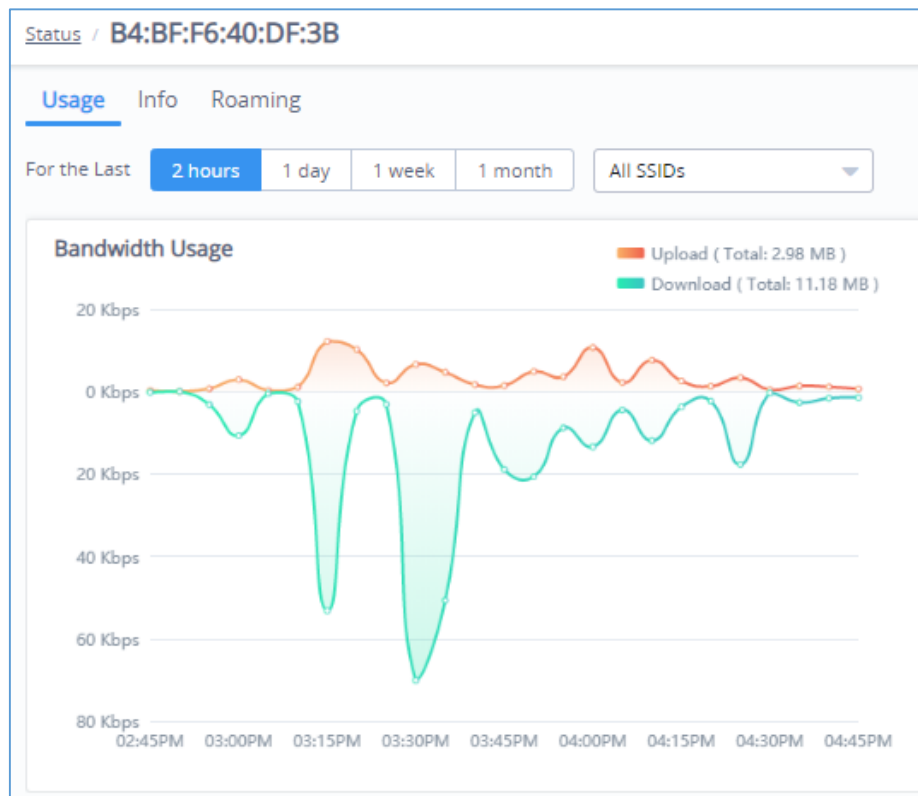
- Click on  under Actions to edit the client's hostname.
- Click on  under Actions to set the bandwidth rules to each client.
- Click on  to block a client's MAC address from connecting to the SSID, Once the client is blocked it will be added to Global blacklist under **Clients → Access List**.



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

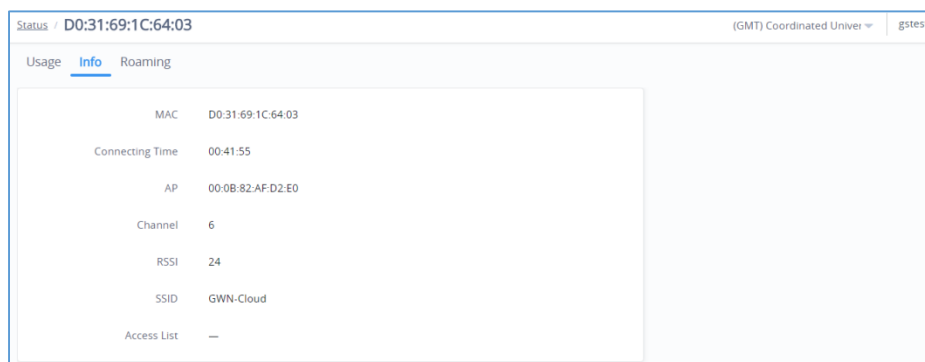
Users can click on a specific client to see detailed information about that client as follow:

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



**Figure 56: Client Data Usage Info**

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



**Figure 57: Client Info**



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

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

(GMT) Coordinated Universal Time | gstest

Usage

Info

Roaming

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

Total 4

10 /page

1

**Figure 58: Client Roaming**

## CAPTIVE PORTAL

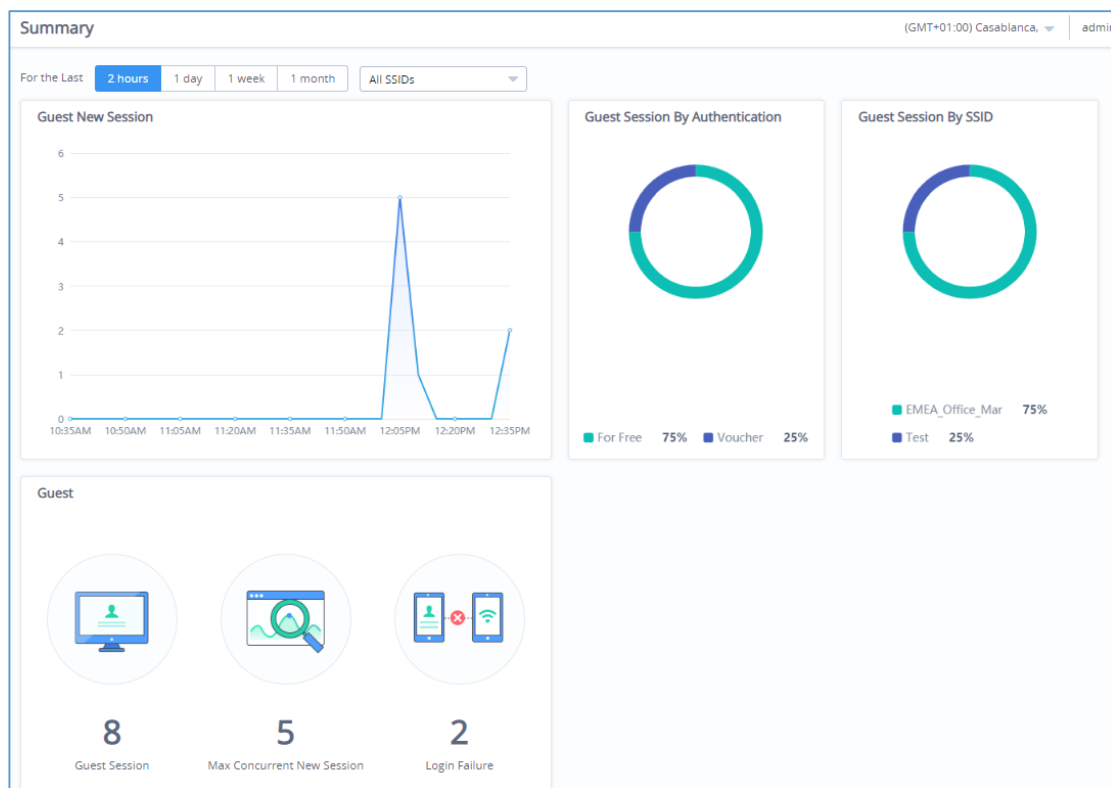
Captive Portal feature helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet. Once connected to a GWN AP, Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

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

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

### Summary

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



**Figure 59: 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.

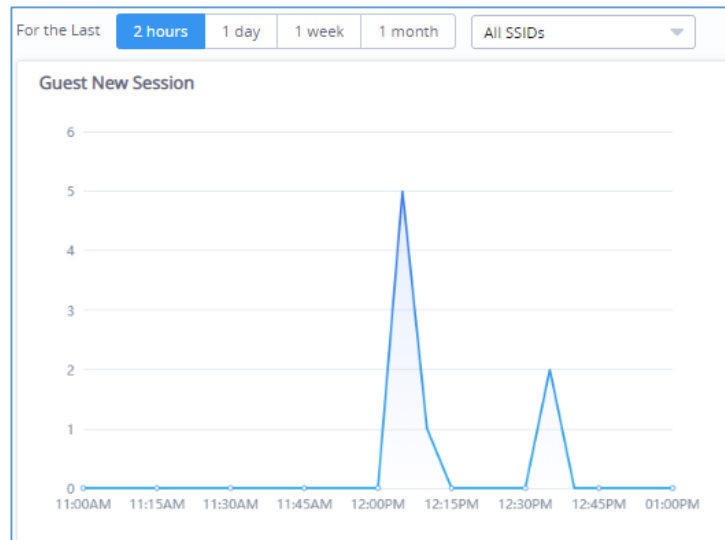
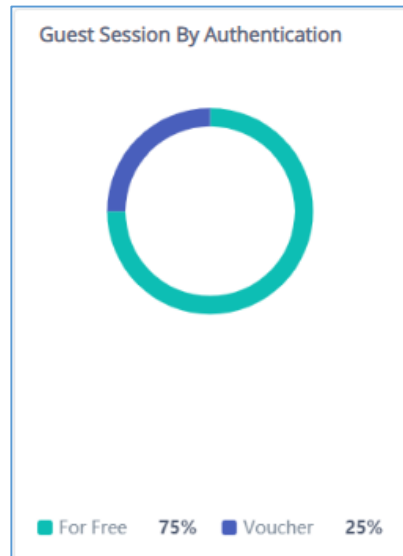


Figure 60: Guest New Session

## 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 61: Guest Session by Authentication**

## Guest Session by SSID

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



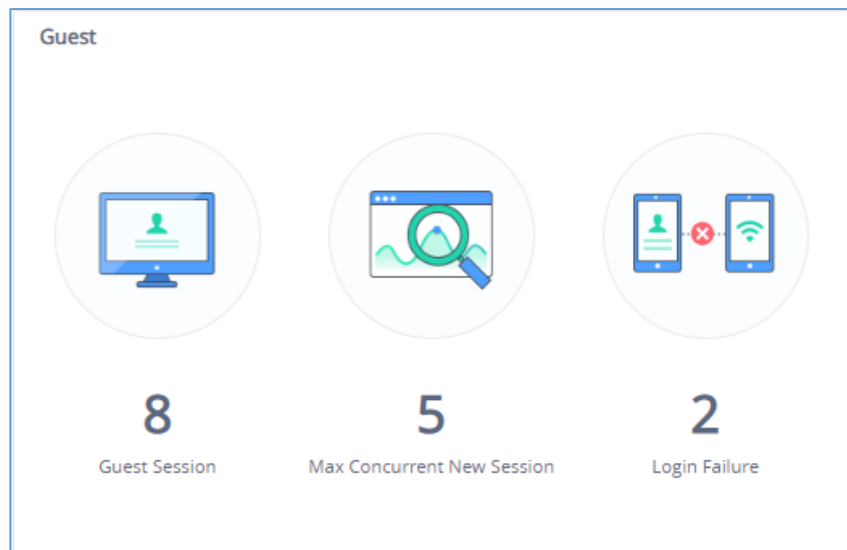
**Figure 62: Guest Session by SSID**

## 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



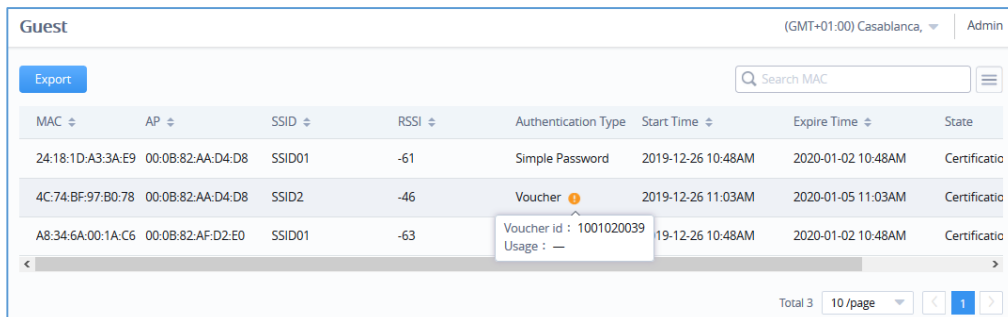
login failure.



**Figure 63: Guest Section**

## Guest

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

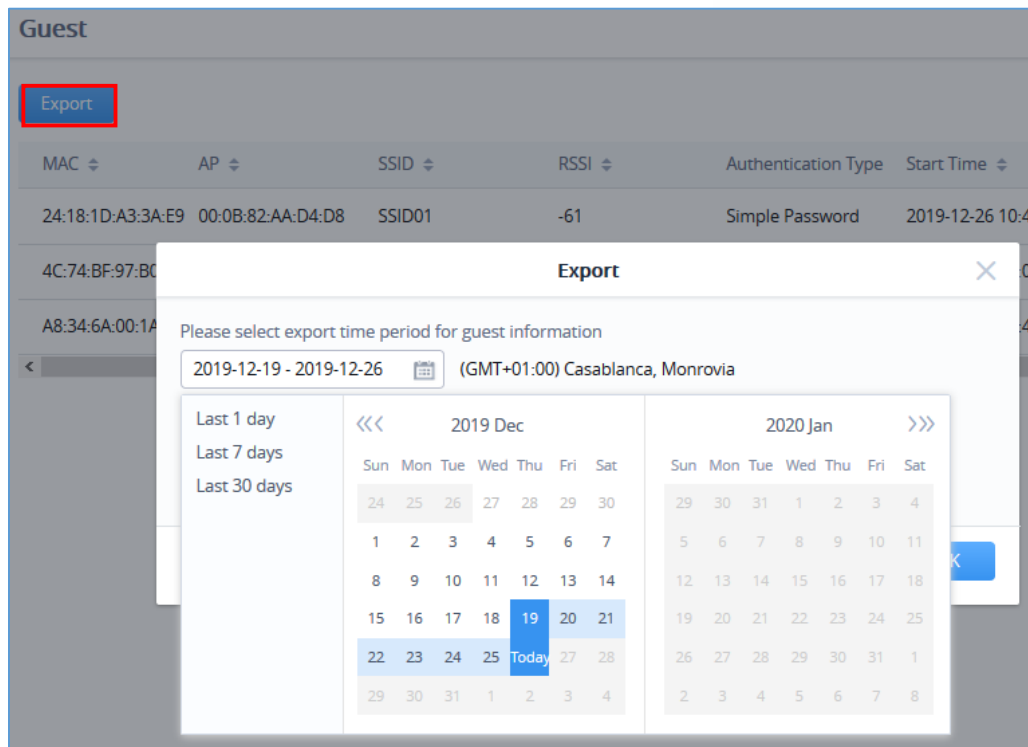


MAC	AP	SSID	RSSI	Authentication Type	Start Time	Expire Time	State
24:18:1D:A3:3A:E9	00:0B:82:AA:D4:D8	SSID01	-61	Simple Password	2019-12-26 10:48AM	2020-01-02 10:48AM	Certificatio
4C:74:BF:97:B0:78	00:0B:82:AA:D4:D8	SSID2	-46	Voucher	2019-12-26 11:03AM	2020-01-05 11:03AM	Certificatio
A8:34:6A:00:1A:C6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


Tooltip for third row:  
 Voucher id : 1001020039  
 Usage : —

**Figure 64: Guest List**

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



**Figure 65: Export Guest Information Period**

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

## Policy List

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

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

**Edit Portal Policy**
✕

\* Name ?

Splash page ? Internal ▼

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

Failsafe Mode ? ☐

Daily Limit ? ☐

\* Splash Page Customization ?  ▼

Landing Page ?  ▼

Enable HTTPS ? ☐

Pre Authentication Rule (s) ?

Select Destina ▼

-

Select Service ▼

-

+ Add New Authentication Rule

Post Authentication Rule (s) ?

Select Destina ▼

-

Select Service ▼

-

+ Add New Authentication Rule

**Figure 66: Add/Edit Captive Portal Policy**

## Internal Splash Page

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

**Table 12: Add new Policy List – Splash Page as “Internal”**

Field	Description
<b>Name</b>	Enter a name to identify the created portal policy.
<b>Splash Page</b>	Select Splash Page type, Internal or External.



<b>Client Expiration</b>	Configures the period of validity, after the valid period, the client will be re-authenticated again.
<b>Failsafe Mode</b>	When enabled; guest can surf on the internet when the authentication server or external portal cannot communicate.
<b>Daily Limit</b>	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.
<b>Splash Page Customization</b>	Configure portal display page.
<b>Landing page</b>	<p>Select the landing page where the users will be sent after successful authentication, two options are available:</p> <ul style="list-style-type: none"> <li>• <b>Redirect External Page URL Address:</b> for promotional purposes, admin can this to redirect all authenticated users to the company website.</li> <li>• <b>Redirect to the Original URL Address:</b> Sent the user to the original requested URL.</li> </ul>
<b>Enable HTTPS</b>	<p>Check to enable/disable HTTPS service over captive portal.</p> <p><b>Note:</b> Once enabled, both HTTP and HTTPS requests sent from stations will be redirected to the splash page by using HTTPS protocol, and in some cases, guests may not be authenticated successfully for the system or browser does not trust our self-signed certificate.</p>



<b>Pre-Authentication Rule(s)</b>	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)
<b>Post Authentication Rule(s)</b>	Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS)

## External Splash Page

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

Field	Description
<b>Name</b>	Enter a name to identify the created portal policy.
<b>Splash Page</b>	Select Splash Page type, <b>Internal</b> or <b>External</b> Splash Page
<b>Platform</b>	Select which external captive portal platform to use: <ul style="list-style-type: none"> <li>• <b>Linkyfi Platform</b> (<a href="https://www.avsystem.com/products/linkyfi">https://www.avsystem.com/products/linkyfi</a>)</li> <li>• <b>Purple Platform</b> (<a href="https://purple.ai/">https://purple.ai/</a>)</li> <li>• <b>Universal Platform</b> (Socifi Platform for instance)</li> </ul>
<b>External Splash Page Address</b>	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.
<b>RADIUS Server Address</b>	Enter the RADIUS Server Address provided by external portal platform.
<b>RADIUS Server Port</b>	Enter the RADIUS Server Port provided by external portal platform, the default value is 1812.
<b>RADIUS Server Secret</b>	Enter the RADIUS Server Secret provided by external portal platform.
<b>RADIUS Accounting Server Address</b>	Enter the Radius Accounting Server Address provided by external portal platform.
<b>RADIUS Accounting Server Port</b>	Enter the Radius Accounting Server Port provided by external portal platform.



<b>RADIUS Accounting Server Secret</b>	Enter the Radius Accounting Server Port provided by external portal platform.
<b>Accounting Update Interval</b>	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.
<b>RADIUS NAS ID</b>	Specify the AP tag, limit to 32 characters. <i>This field appears only when <b>Platform</b> is set to “Linkyfi Platform”.</i>
<b>Redirect URL</b>	Please enter the Redirect URL provided by external portal platform.
<b>Pre-Authentication Rule(s)</b>	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)
<b>Post Authentication Rule(s)</b>	Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS)

**Note:**

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

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

## Splash Page

### Page

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

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

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

Users can set the following:

- **Authentication type:** Add one or more ways from the supported authentication methods (Simple





Password, Facebook, Twitter, Voucher, Radius, No Authentication, WeChat.

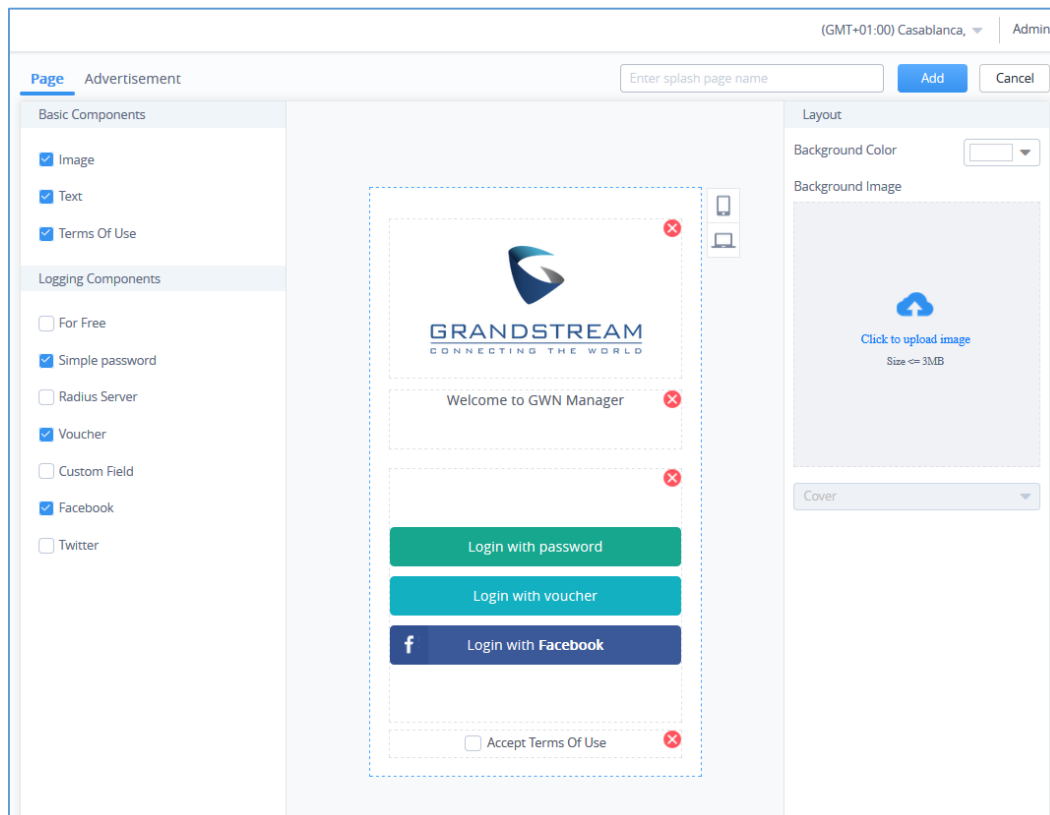
- **Setup a picture (company Logo)** to be displayed on the splash page.
- **Customize** the layout of the page and background colors.
- **Customize the Terms of use text.**
- **Visualize a preview** for both mobile devices and laptops.

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

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

1. First go under “**Captive Portal → Splash Page**” then click on

Create Splash Page

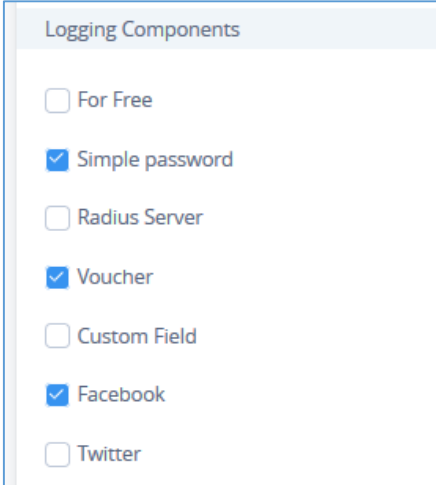


**Figure 67: Create New Splash Page**

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



Server, For Free or Custom Field)

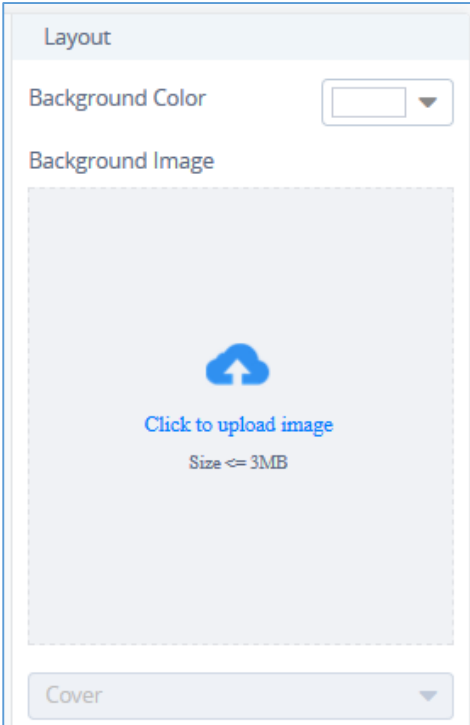


Logging Components

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

**Figure 68: Setup Logging Methods - Splash Page**


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



Layout

Background Color   

Background Image



Click to upload image

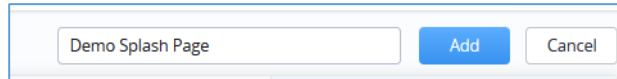
Size <= 3MB

Cover ▼

**Figure 69: Upload a logo - Splash Page**

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





**Figure 70: Name - Splash Page**

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



### Logging Configuration

#### Simple password

\* Simple Password ?

The field should not be empty

Button Text

Login with password

Button Color

Font Color

#### Voucher

Button Text

Login with voucher

Button Color

Font Color

#### Facebook

\* Facebook App Id ?

The field should not be empty

\* Facebook App Secret ?

The field should not be empty

Byte Limit(MB)


1-1048576 integers


Per Day

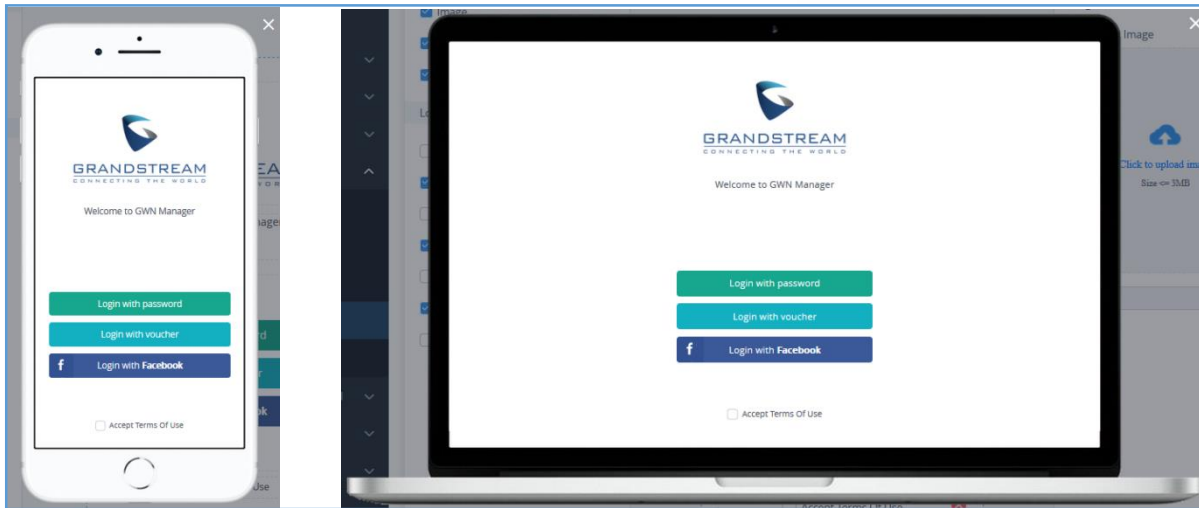
**Figure 71: Setup Social Logging Parameters**

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

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

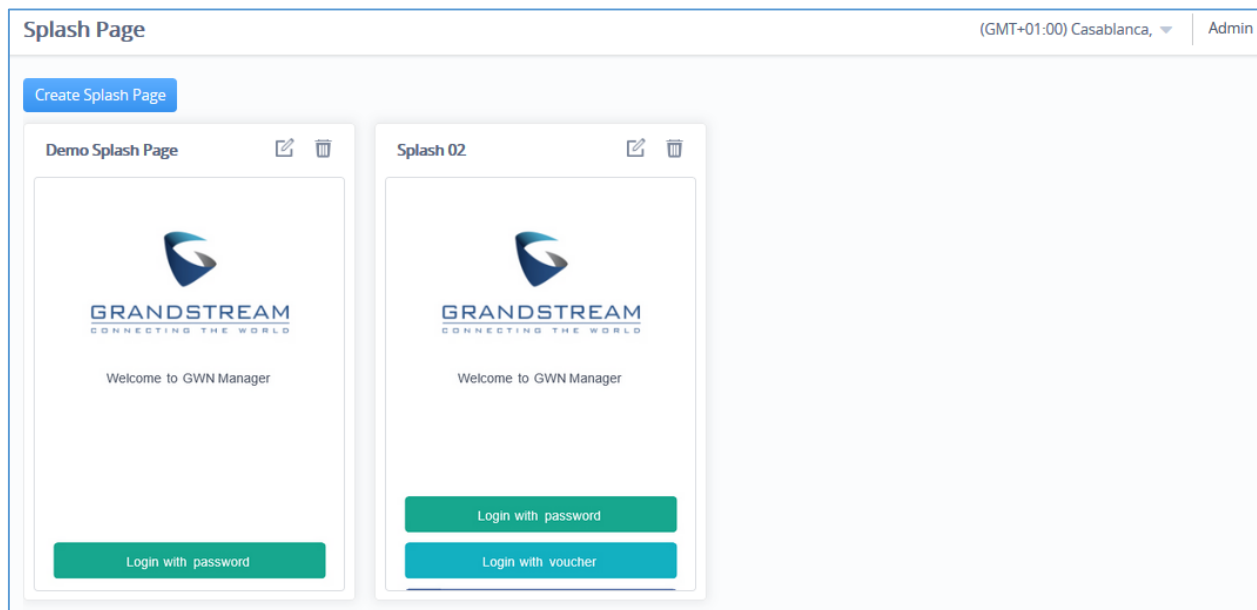
- To see the preview of the page on mobile phones click on  button.

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



**Figure 72: Splash Page Preview**

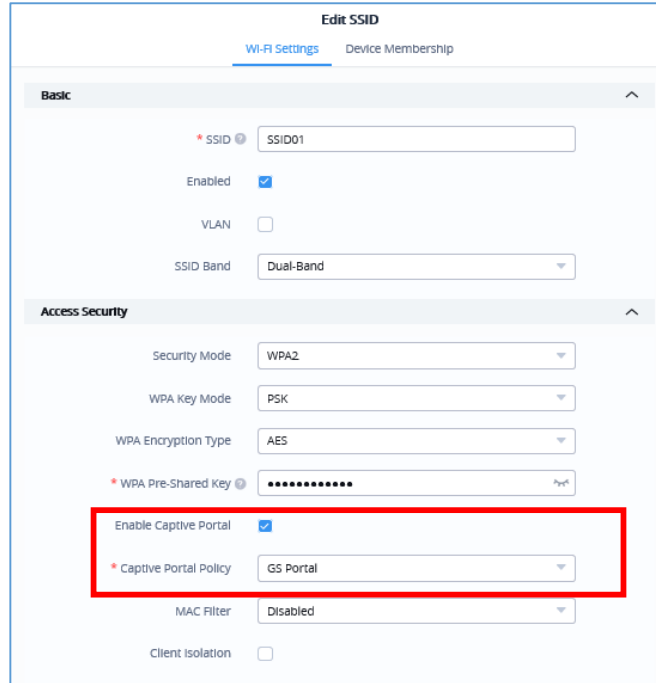
7. If you are satisfied with the final design. Click on **Add** and after the page has been added to it will be displayed along other existing pages with the possibility to either “Edit” or “Delete” it.



**Figure 73: Splash Pages List**

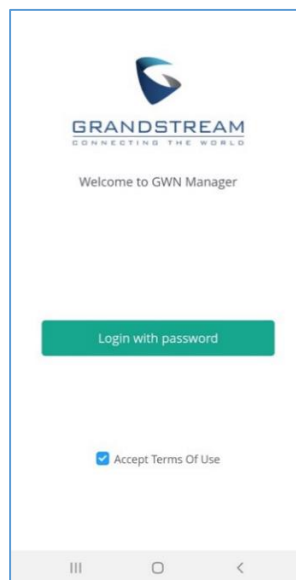
All these pages can be used on different captive portal policies depending on the user’s needs.

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



**Figure 74: Enable Captive Portal**

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



**Figure 75: Portal Splash Page**

## Advertisement

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

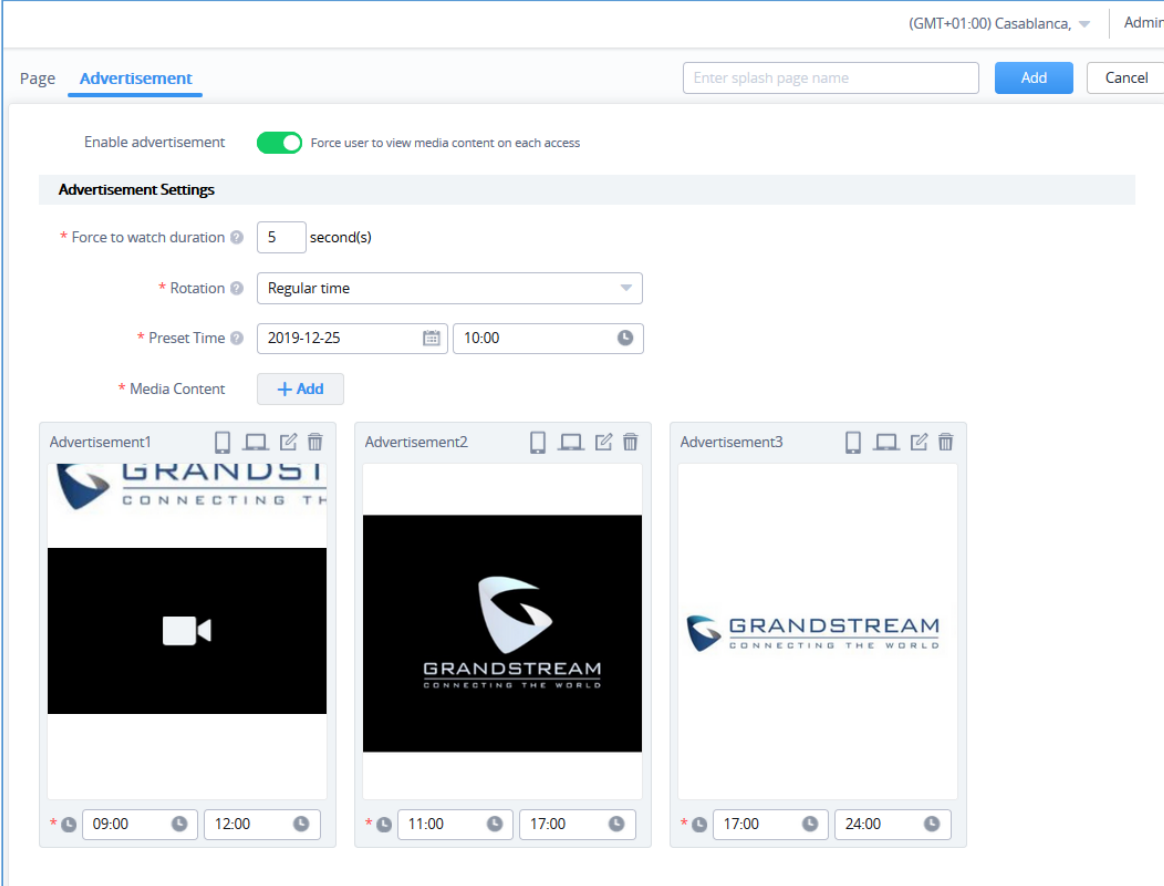
As an example, most companies or stores have free Wi-Fi which they offer to their customers, this is a good place to meet their customers where they are at by using the **Advertisement Splash Page** to connect



advertisers to target customers either by displaying a promoting video or images.

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

1. Go under “**Captive Portal** → **Splash Page** → **Advertisement**”
- Click on **Enable Advertisement**.



The screenshot shows the 'Advertisement' configuration page in the Grandstream management interface. At the top, there's a header with the location '(GMT+01:00) Casablanca' and an 'Admin' link. Below the header, there's a 'Page' tab labeled 'Advertisement' and a search bar 'Enter splash page name' with 'Add' and 'Cancel' buttons. The main content area has a toggle for 'Enable advertisement' which is turned on, and another toggle 'Force user to view media content on each access' which is also turned on. Under 'Advertisement Settings', there are fields for 'Force to watch duration' (set to 5 seconds), 'Rotation' (set to Regular time), and 'Preset Time' (set to 2019-12-25 at 10:00). There's also a '+ Add' button for 'Media Content'. Below these settings, there are three advertisement slots: 'Advertisement1' (a video player showing a black screen with a white play button), 'Advertisement2' (an image of the Grandstream logo on a black background), and 'Advertisement3' (another image of the Grandstream logo). Each slot has a schedule bar at the bottom with time slots and a star icon.


**Figure 76: Advertisement Page**

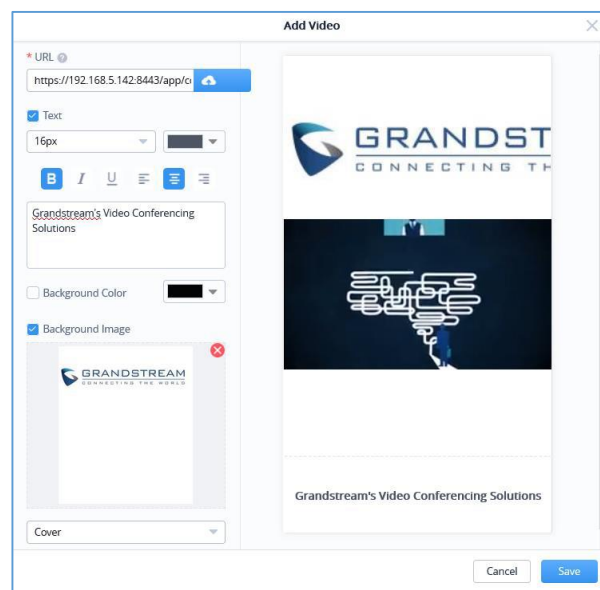
2. Enter the Advertisement Settings, below table gives more details about each option:

**Table 14: Advertisement Settings Configuration**

<b>Force to watch duration</b>	<p>Specify the duration that guests must watch advertisement for.</p> <p>Please enter an integer from 1 to 300.</p>
<b>Rotation</b>	<p>Specify the rotation mode of the ads.</p> <ul style="list-style-type: none"> <li>• <b>Random:</b> the ads will be prompted randomly.</li> <li>• <b>Regular Interval:</b> the created ads should be specified with advertising periods,</li> </ul>





	<p>and the ads will be prompted in turns.</p> <ul style="list-style-type: none"> <li>• <b>Regular Time:</b> the created ads should be specified with start time and end time, and the ads will be prompted at regular time every day.</li> </ul>
<b>Preset Time</b>	Preset the start time of the advertising policy.
<b>Media Content</b>	<p>Click  button to add Image/Video content.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The video file content should not exceed 5 MB</li> <li>• Video format only supports MP4 in H.264 codec</li> <li>• Supports input of YouTube URL.</li> <li>• When playing ads with multiple images, it will automatically switch every 3 seconds.</li> </ul>



**Figure 77: Add Video - Advertisement**

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

- To see the preview of the ads on mobile phones click on  button.
- Or click on  button to see the preview of the ads on computer screens.





## Voucher

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

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

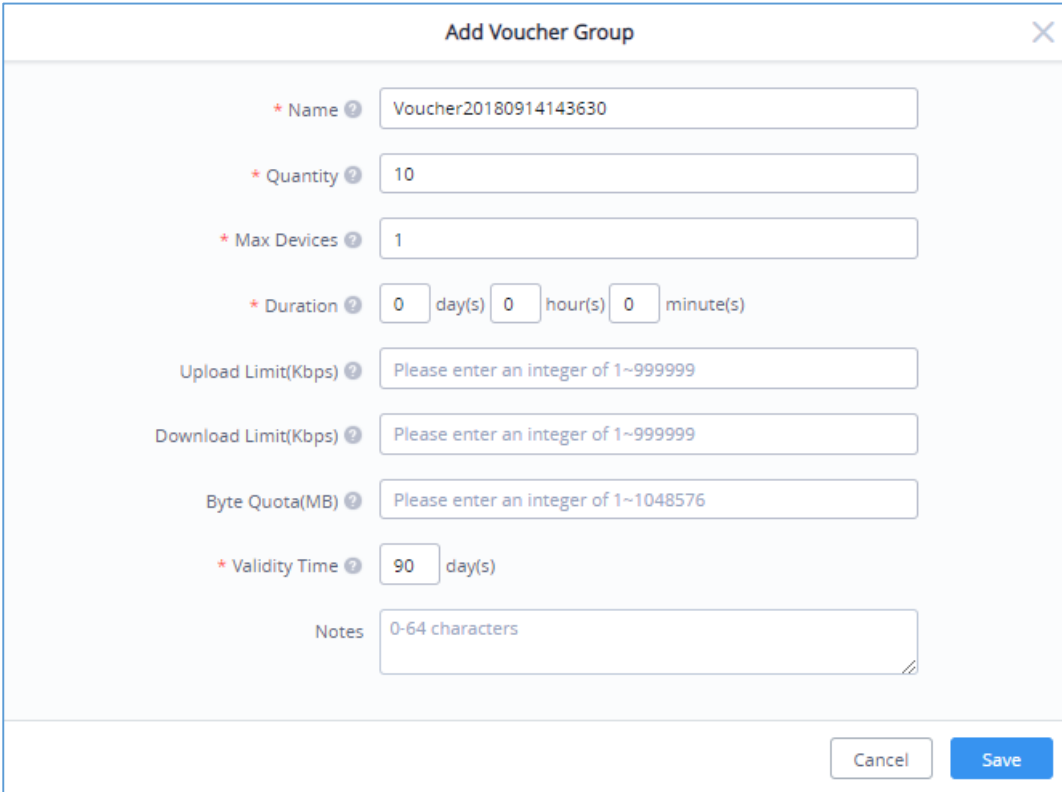
Note that multiple users can use a single voucher for connection with expiration duration of the voucher that starts counting after first successful connection from one of the users that are allowed.

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

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

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

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



Add Voucher Group

\* Name ? Voucher20180914143630

\* Quantity ? 10

\* Max Devices ? 1

\* Duration ? 0 day(s) 0 hour(s) 0 minute(s)

Upload Limit(Kbps) ? Please enter an integer of 1~999999

Download Limit(Kbps) ? Please enter an integer of 1~999999

Byte Quota(MB) ? Please enter an integer of 1~1048576

\* Validity Time ? 90 day(s)

Notes 0-64 characters

Cancel

Save

Figure 78: Adding Vouchers

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

**Table 15: Voucher Configuration Parameters**
















<b>Name</b>	Enter a name to identify the voucher
<b>Quantity</b>	Specify how many voucher codes to create which do follow same settings (bandwidth rates, duration, validity...Etc.). Range from 1~1000.
<b>Max Devices</b>	Specify how many users can connect using the same voucher code. Range is from 1~10000 while 0 means unlimited.
<b>Duration</b>	Configure the voucher duration from 1 minutes to 7 days.
<b>Upload Limit (kbps)</b>	Configured upstream data rate limit for the voucher. 0 means unlimited.
<b>Download Limit (kbps)</b>	Configured downstream data rate limit for the voucher. 0 means unlimited.
<b>Byte Quota (MB)</b>	Configure the total usage of the voucher.
<b>Validity Time</b>	Duration of validity of the voucher. It starts with first authentication.
<b>Notes</b>	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 / **Voucher20191003164151** (GMT+02:00) Amsterdam, ▾ mbouj

All ▾ 🔍 Search Password

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

Total 10 10 /page < 1 >

**Figure 79: Voucher Details**

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

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

Add Settings Details 🔍 Search Group Name/Creator

Kbps ▴ ▾ Byte Limit(MB)


—

—

—

0 /page < 1 >

**Voucher Settings** ✕

Logo ? 

Slogan ?

Cancel Save

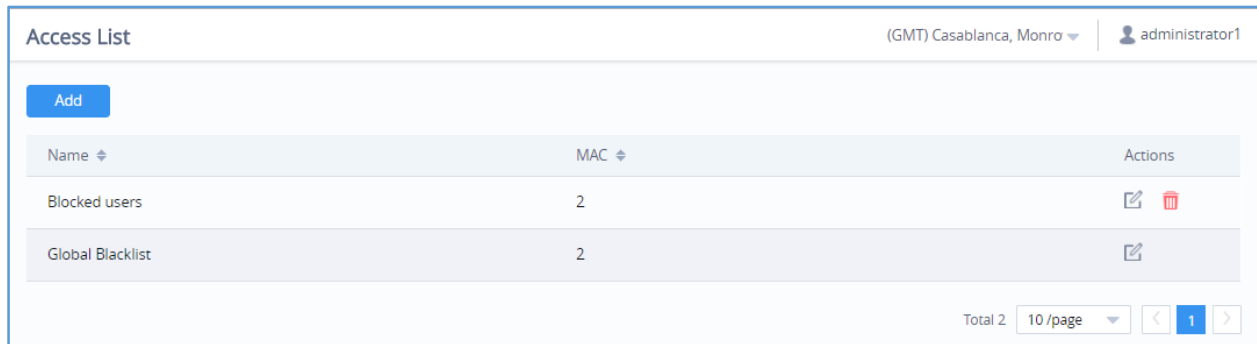
**Figure 80: Voucher Settings**

## ACCESS CONTROL

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

### Access List

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

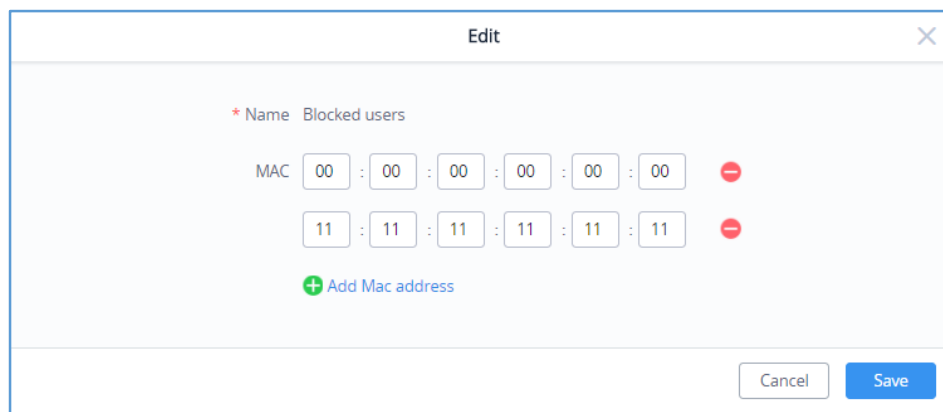


Name	MAC	Actions
Blocked users	2	
Global Blacklist	2	

Total 2 10 /page

Figure 81: 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:



Edit

\* Name Blocked users

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

11 : 11 : 11 : 11 : 11 : 11

Add Mac address

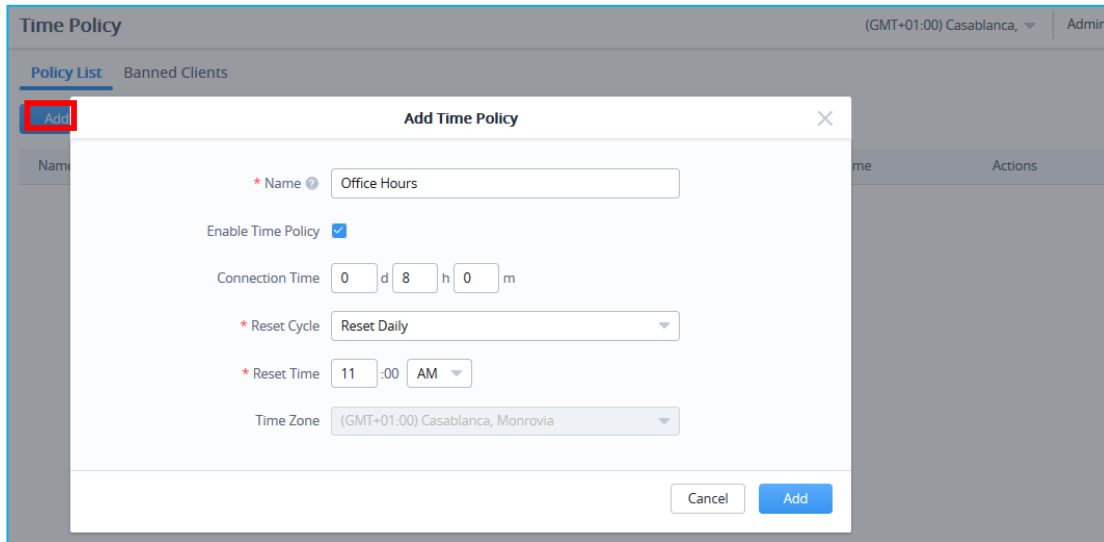
Cancel Save

Figure 82: 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 83: Add Time Policy List**

**Table 16: Time Policy Configuration Parameters**

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



## Bandwidth rules

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

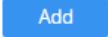
Click  to add a new rule, the following table provides an explanation about different options for bandwidth rules.

Table 17: Bandwidth Rules

Field	Description
Enable Bandwidth Rules	Enable/Disable Bandwidth Rules
SSID	Select the SSID to which the limitation will be applied.
Range Constraint	<ul style="list-style-type: none"> <li>• <b>Per-SSID:</b> means the rule will be shared/applied to all clients connected to the SSID.</li> <li>• <b>Single MAC:</b> This means the rule will be applied only to one client.</li> <li>• <b>Single IP:</b> 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.</li> <li>• <b>Per-Client:</b> 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.</li> </ul>
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 " <b>System → Schedule</b> "
Upstream Rate	Specify the limit for the upload bandwidth using Kbps or Mbps.



("Upload Limit" for GWN Manager)	
<b>Downstream Rate</b> ("Download Limit" for GWN Manager)	Specify the limit for the download bandwidth using Kbps or Mbps.

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

Add Bandwidth Rules

Enabled Bandwidth Rules

\* SSID

☒ GWN-Cloud  
☒ Select All

Range Constraint

Single MAC

Schedule

Office Hours

\* MAC

00

:

0B

:

82

:

10

:

10

:

10

\* Please fill in at least one of the following items

Upstream Rate

10

Mbps

Downstream Rate

75

Mbps

Cancel

Add

**Figure 84: MAC Address Bandwidth Rule**

## INSIGHT

### Site Survey

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

Site Survey										
<a href="#">Detect</a> <a href="#">Refresh</a>		All		2.4G&5G		Q Search				
	SSID	BSSID	Channel	Protocol	BW(MHz)	Security	Manufacture	Detected By	RSSI	Last Seen
1	EMEA_Training	06:0B:82:AA:D4:BA	48	802.11ac	80	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-48	2019-09-26 0...
1	EMEA_Office	00:0B:82:AA:D4:BA	48	802.11ac	80	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-48	2019-09-26 0...
1	EMEA_Office 1	00:0B:82:9A:96:59	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-44	2019-09-26 0...
1	EMEA_Office 2	8C:0C:90:4A:7F:48	1	802.11g	—	WPA	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 3	8C:0C:90:4A:7F:48	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 4	8C:0C:90:4A:7F:48	1	802.11g	—	WPA	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
1	EMEA_Office 5	8C:0C:90:4A:7F:48	1	802.11n/g	20	WPA2	Grandstream Netw...	00:0B:82:AF:D2:E...	-84	2019-09-26 0...
				Total 78		10/page	<a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">...</a> <a href="#">8</a>			

Figure 85: Site Survey - Insight

Users can press [Detect](#) to run the Wi-Fi Scanner or Press [Refresh](#) to refresh the results page.

### Known Clients

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

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



GWN Manager

Dashboard

Network

default

Overview

Access Points

SSIDs

Clients

Captive Portal

Access Control

Insight

Site Survey

Known Clients

System

Known Clients

(GMT+01:00) Casablanca, Admin

All ClientsAll TimeSearch MAC/Hostname/OS/Manufacturer

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

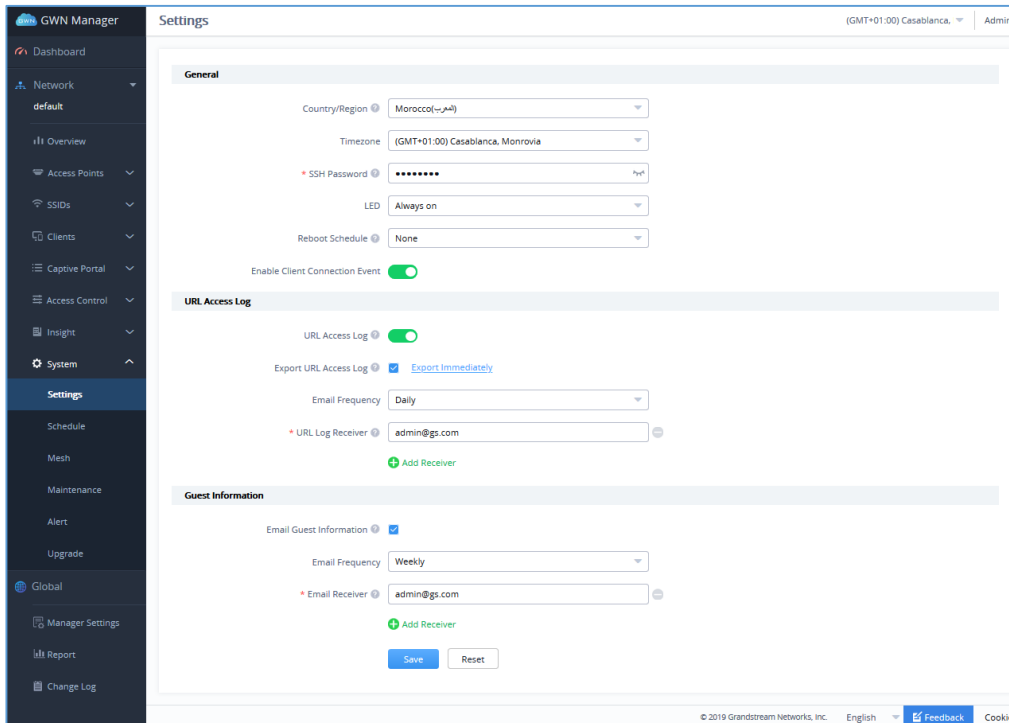
Total 1510/page12

Figure 86: Known Clients - Insight

# SYSTEM

## Settings

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



**Figure 87 :System Settings**

**Table 18: Settings**

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

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

## URL Access Log

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

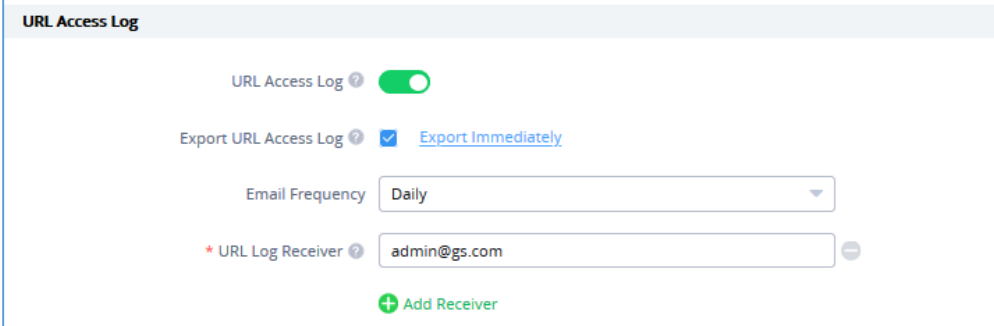
The platform System will send these logs via Email to the configured Log Receiver in a form of downloadable link providing a CSV file format containing all the websites logs visited for each client during the defined period (daily, weekly or monthly basis).

In order to enable this feature, follow below steps:

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



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




**Figure 88: URL Access Log Settings**

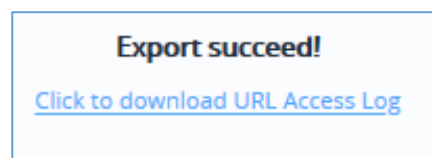
In this example, the administrator will start receiving, on a daily basis, an Email containing a downloadable link providing a CSV file containing the websites visited by the clients during the last day.

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 89: Export Immediately**

- Click  and notice the success confirmation message:



**Figure 90: Export Succeed**

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

Once downloaded, administrators will have a CSV file tracking the Internet activity for all the clients



connected to the paired GWN76xx access points.

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

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

**Figure 91: URL Access Log- CSV file example**

#### Notes:

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

## Guest Information

In order to enable this feature, follow below steps:

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

**Guest Information**

Email Guest Information ☒

Email Frequency Weekly

\* Email Receiver admin@gs.com

+ Add Receiver

Save Reset

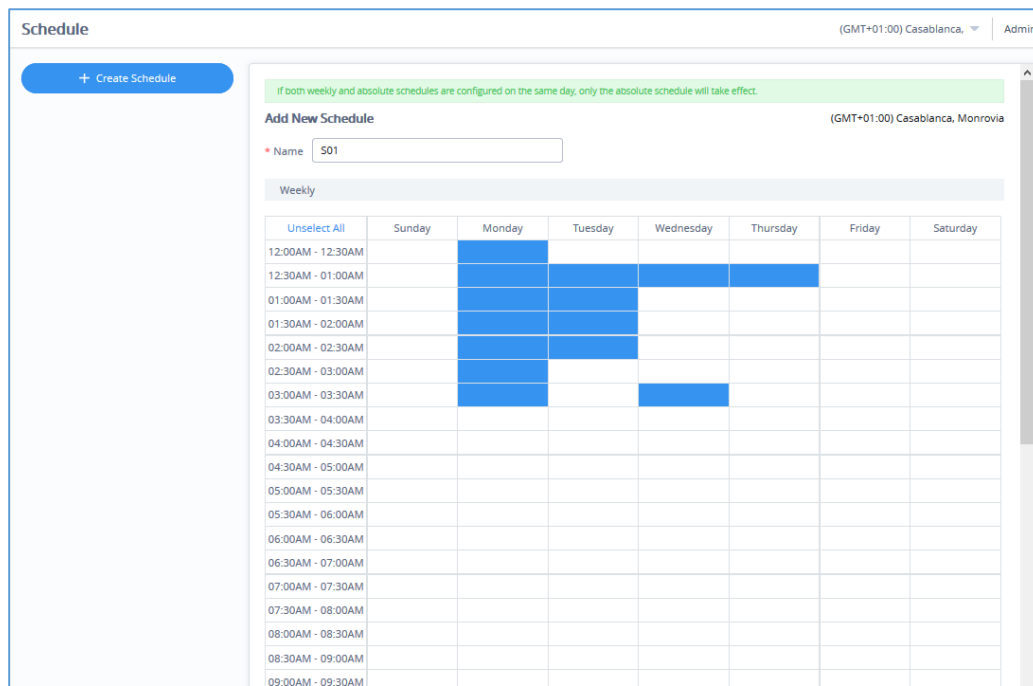
**Figure 92: Guest Information**

## Schedule

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

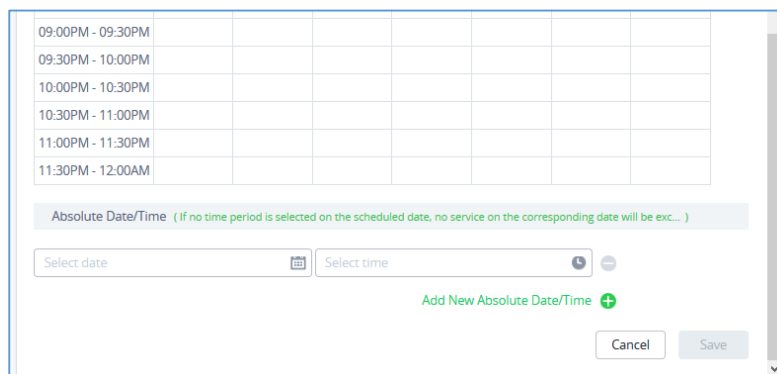
1. Go under “System → Schedule” and click on

+ Create Schedule



**Figure 93: Create New Schedule- Weekly**

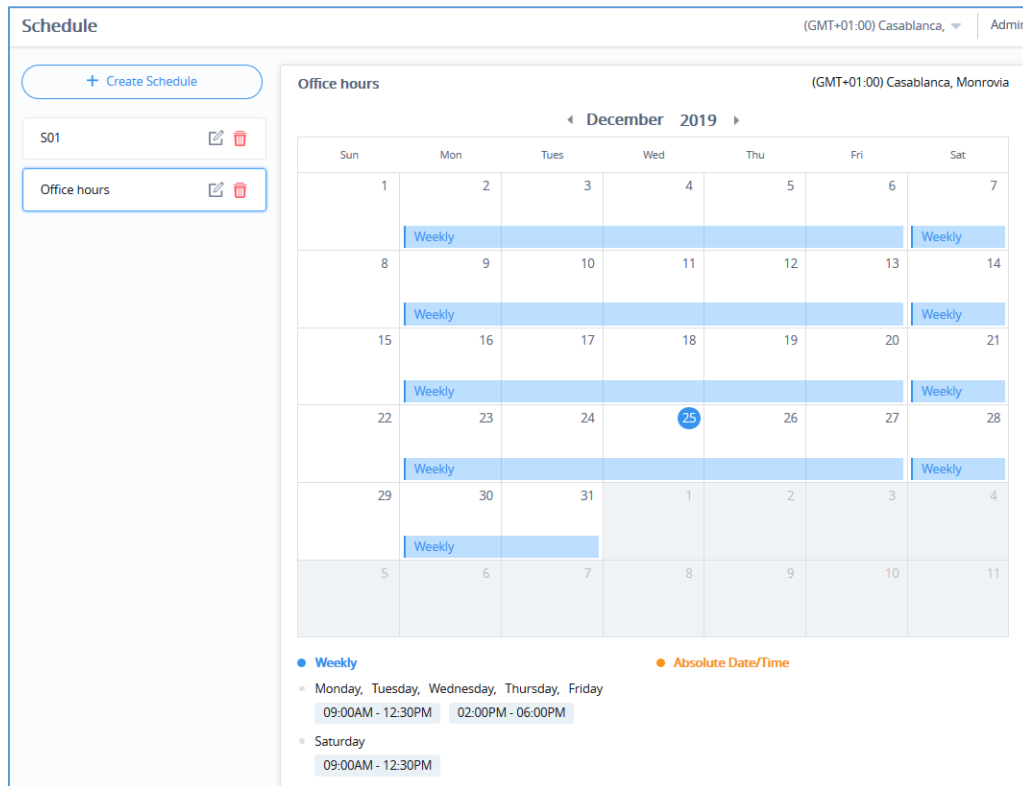
2. Select the periods on each day that will be included on the schedule and enter a name for the schedule (ex: S01).
3. Users can choose to set weekly schedule or absolute schedule (for specific days for example), and if both weekly schedule and absolute schedules are configured on the same day then the absolute schedule will take effect and the weekly program will be cancelled for that specific date.



**Figure 94: Create New Schedule- Absolute**

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

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



**Figure 95: 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.

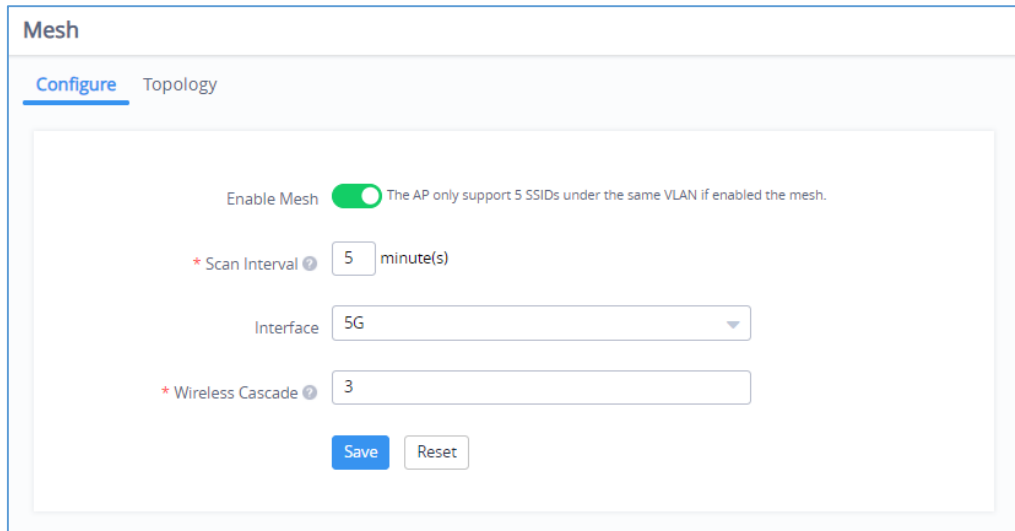
In addition, Mesh networking provides a mechanism for network redundancy. When an abnormality occurs in a wired network, an AP suffering the uplink failure can keep the data service continuity through its Mesh



network.

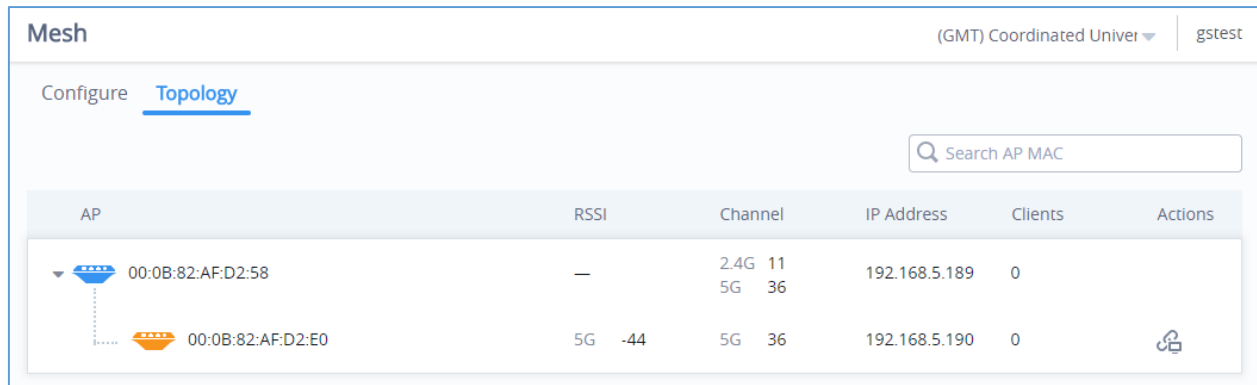
For more details about the GWN Mesh Network feature, please don't hesitate to read the following technical paper: [http://www.grandstream.com/sites/default/files/Resources/GWN76XX\\_Mesh\\_Network.pdf](http://www.grandstream.com/sites/default/files/Resources/GWN76XX_Mesh_Network.pdf)


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




**Figure 96: Mesh Settings**

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



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 97: Mesh Topology**

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



- Click **Refresh Neighbor** to update information

Neighbor

☐ Disable Automatic Uplink ?

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

Refresh Neighbor

2.4G

5G

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

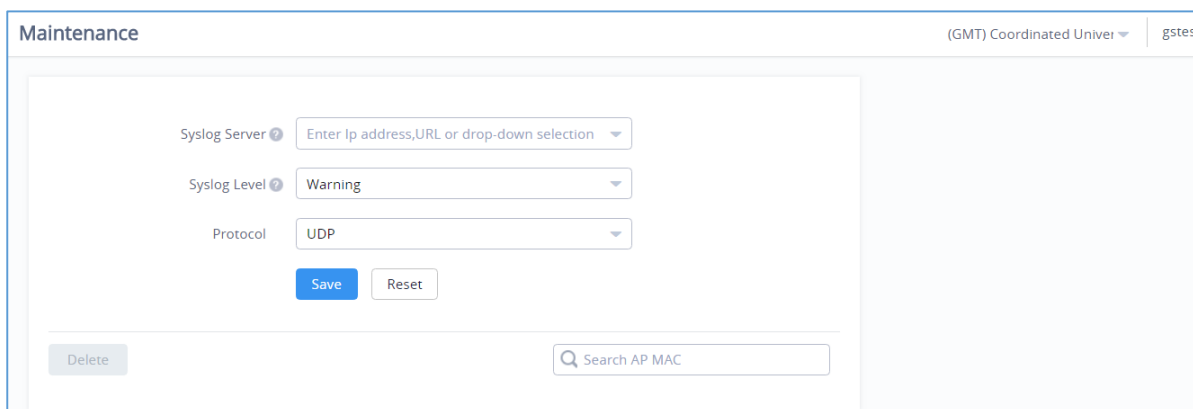
Close

Save

**Figure 98: Neighbor**

## Maintenance

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



**Figure 99: Maintenance/Syslog Settings**

**Table 19: Maintenance**

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

## Alert

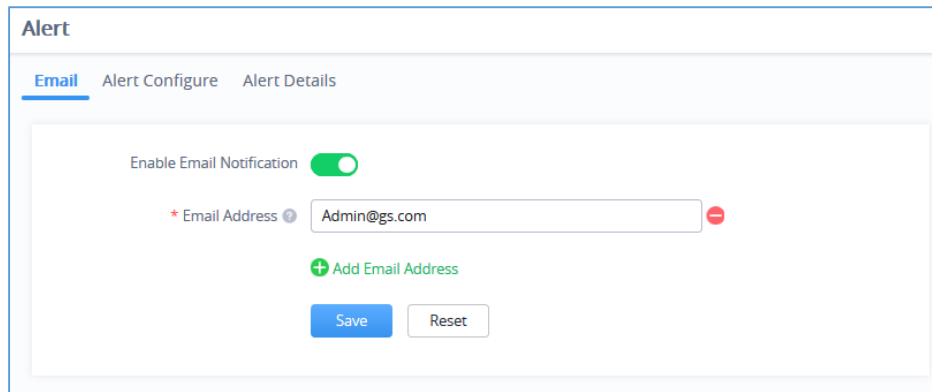
The Alert Web page provides configuration for Alert settings. The first tab is to setup the email address of admin(s) which will be receiving alert events notifications.

**Table 20: Alert**

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

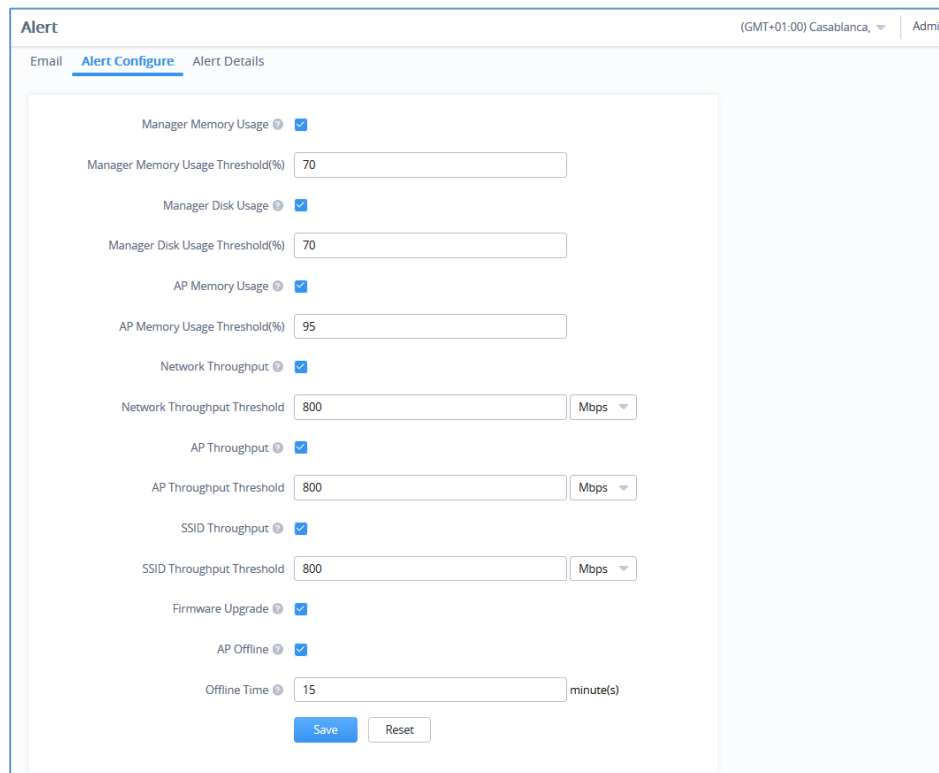


	Firmware Upgrade, AP Offline
<b>Alert details</b>	Displays the alerts in the web UI of GWN Manager.



**Figure 100: Alert Email**

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



**Figure 101: Alert Events List**

The next Table details the Alert configuration parameters:

**Table 21: Alert configuration parameters**

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

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



Alert

(GMT+01:00) Casablanca


Admin

Email


Alert Configure

Alert Details

Select Time




All

 Search MAC

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

Total 8

10/page



1




Figure 102: Alert Details

## Upgrade

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

- **Managing Firmware Files**

1. Go to **Upgrade → Devices**.

Upgrade

(GMT+01:00) Casablanca, ▾

Admin

Devices

Schedule

Firmware

Upgrade

All Models ▾

☰

<input type="checkbox"/> Model ▾	MAC ▾	Firmware ▾	Latest Available Version	Scheduling
<input type="checkbox"/> GWN7610	00:0B:82:AA:D4:D8	1.0.12.4	1.0.12.3	No
<input type="checkbox"/> GWN7600	00:0B:82:AF:D2:E0	1.0.12.4	1.0.12.3	No

Total 2

10 /page ▾

<

1

>











Figure 103: Upgrade

2. Click on **Firmware** button. A new window will be displayed:
  - a. **Recommended Version:** The recommended version tab lists the latest official firmware.

Firmware	
Recommended Version Customized Version	
Model	Firmware
GWN7600	1.0.12.3
GWN7610	1.0.12.3
GWN7600LR	1.0.12.3
GWN7630	1.0.12.3
GWN7630LR	1.0.12.3
GWN7602	1.0.3.0

**Figure 104: Firmware - Recommended Version**

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

Firmware		
Recommended Version Customized Version		
Upload		
 Click to upload the BIN file		
Name	Model	Option
 1.0.12.5	GWN7600	 
 1.0.12.3	GWN7600	 
 1.0.12.4	GWN7600	 

**Figure 105: Firmware - Customized Version**

### • Upgrading Firmware

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

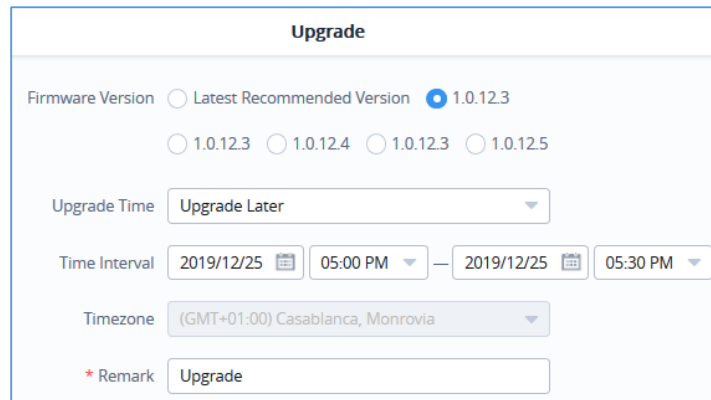
Upgrade	
Firmware Version	<input type="radio"/> Latest Recommended Version <input checked="" type="radio"/> 1.0.12.3 <input type="radio"/> 1.0.12.3 <input type="radio"/> 1.0.12.4 <input type="radio"/> 1.0.12.3 <input type="radio"/> 1.0.12.5
Upgrade Time	<input type="text" value="Upgrade Now"/>
* Remark	<input type="text" value="Upgrade"/>

**Figure 106: Upgrade AP from GWN Manager**

1. Select the firmware version from the list. Both recommended and customized versions will be displayed.

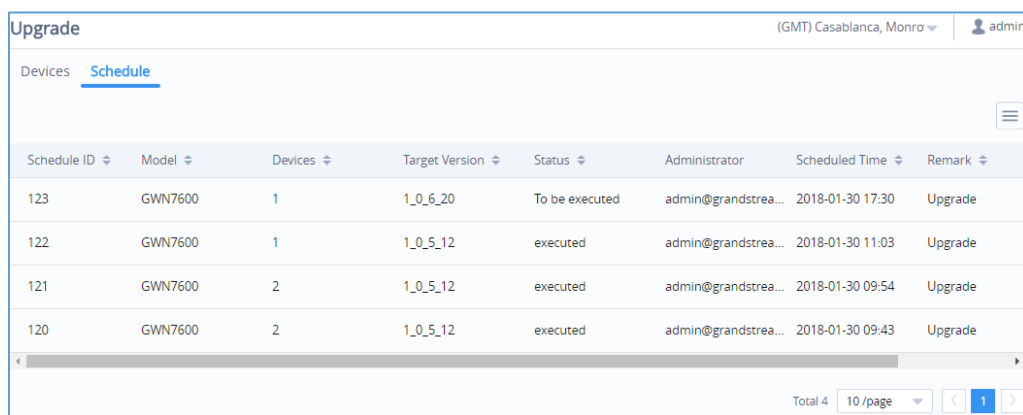


2. In the Upgrade Time list, select:
  - a. **Upgrade Now:** Trigger immediate upgrade for the GWN76XX access points.
  - b. **Upgrade Later:** Schedule upgrade at specific date and time. Administrator must specify time interval.



**Figure 107: Upgrade Schedule for GWN AP from GWN Manager**

The schedule tab lists upcoming and executed upgrade actions:



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

**Figure 108: Upgrade - Schedule**

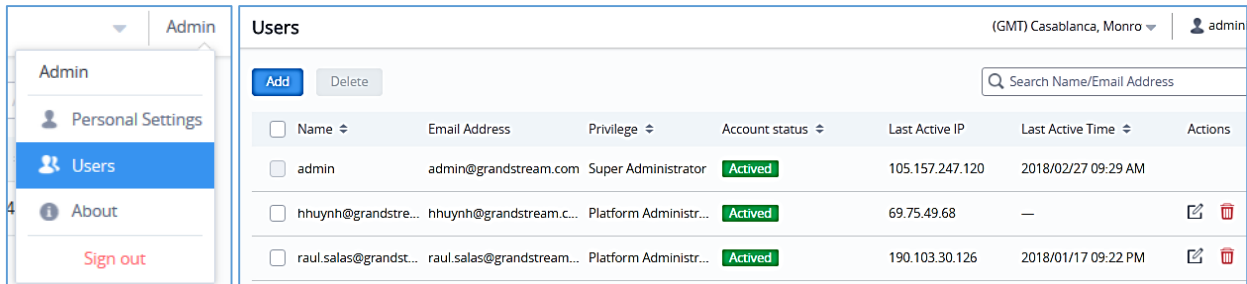
## USER MANAGEMENT





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

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


### Add New Users

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

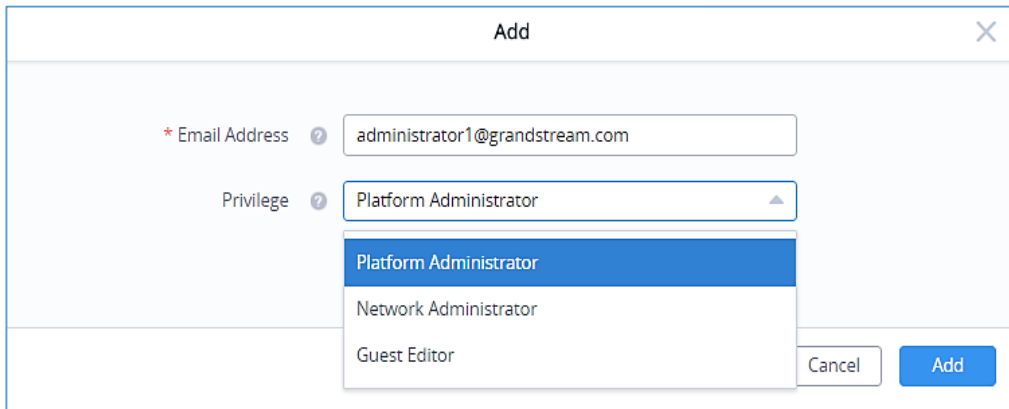


Name	Email Address	Privilege	Account status	Last Active IP	Last Active Time	Actions
admin	admin@grandstream.com	Super Administrator	Activated	105.157.247.120	2018/02/27 09:29 AM	
hhuynh@grandstream.com	hhuynh@grandstream.com	Platform Administrator	Activated	69.75.49.68	—	 
raul.salas@grandstream.com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

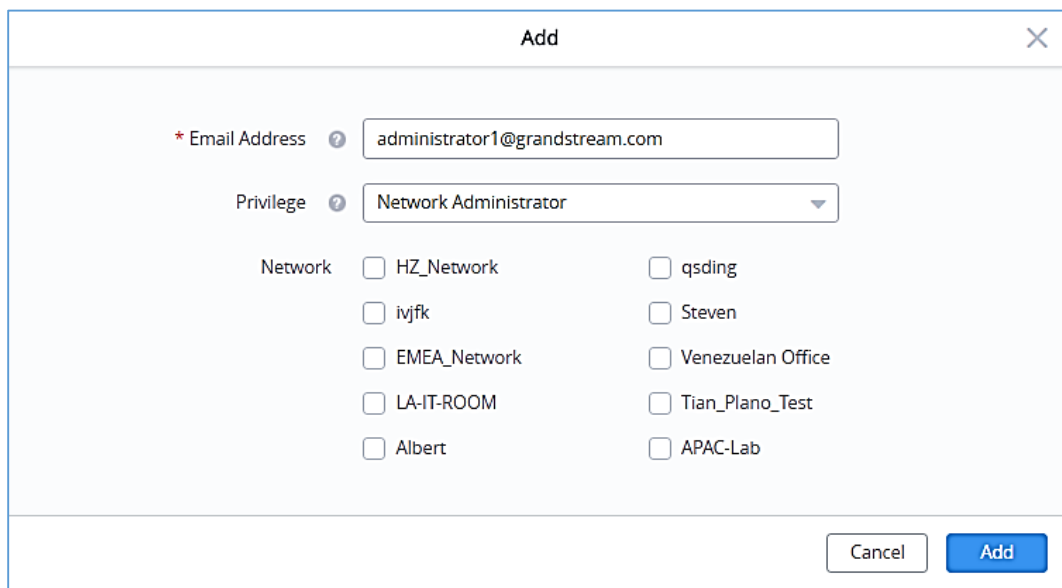
**Figure 109 : Users List**

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





**Figure 110 : Add New “Platform Administrator” User**



**Figure 111 : Add “New Network Administrator” User**

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

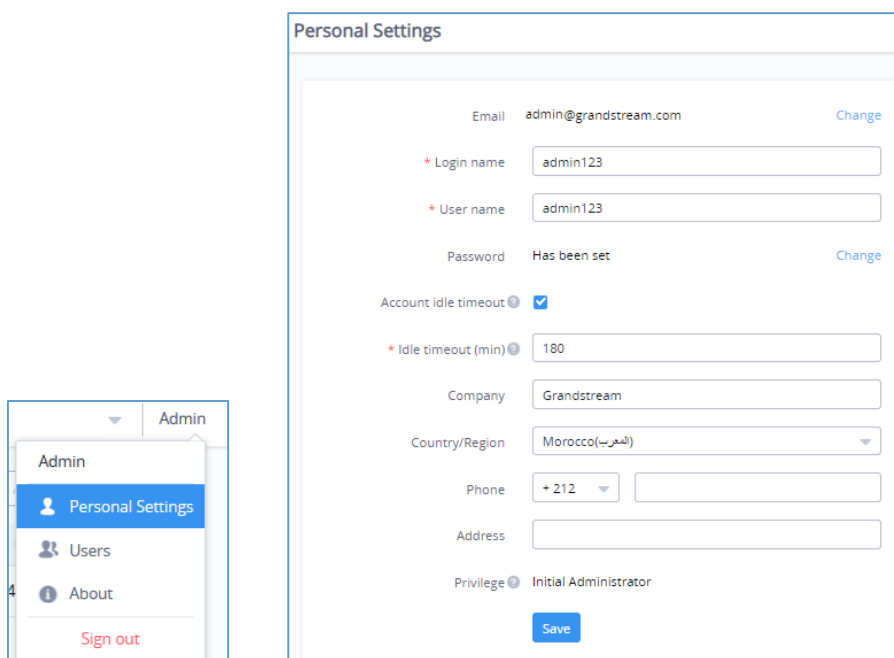
## User Privilege levels

### Super Administrator

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



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



The screenshot shows the 'Personal Settings' page for the Super Administrator account. The page is titled 'Personal Settings' and contains the following fields and options:

- 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)
- Phone:** +212
- Address:**
- Privilege:** Initial Administrator
- Save** button

In the top left navigation bar, the 'Personal Settings' option is highlighted under the 'Admin' menu.

Figure 112 : Edit Super Administrator Account

Table 22: Super Administrator Account

Field	Description
<b>Email</b>	The email address of the Super Administrator. Click on <b>change</b> to change this email address
<b>Login name</b>	Username used for login authentication
<b>Username</b>	This is the name that will be displayed on the top right corner of the web page when login as super administrator
<b>Password</b>	Password used for login authentication
<b>Account Idle timeout</b>	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.
<b>Idle timeout (min)</b>	Specify the idle timeout, please enter an integer from 5 to 1440.
<b>Company</b>	Enter the company name

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

## Platform Administrator

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

## Network Administrator

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

## Guest Editor

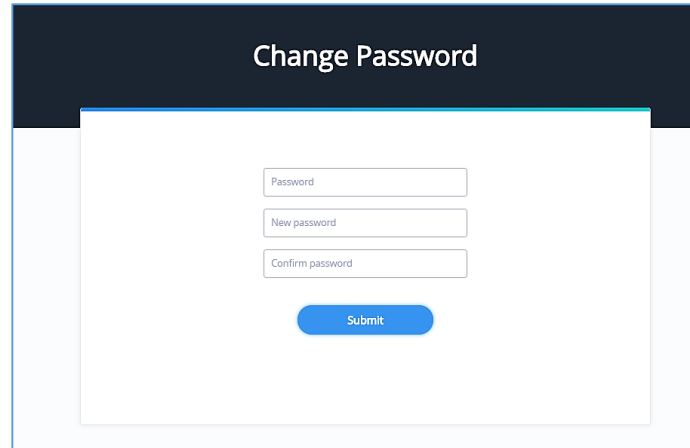
This is the lowest privilege level, a guest editor can only view and edit/monitor captive portal, and voucher page within his network.

## Edit User Settings

### Changing Password

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



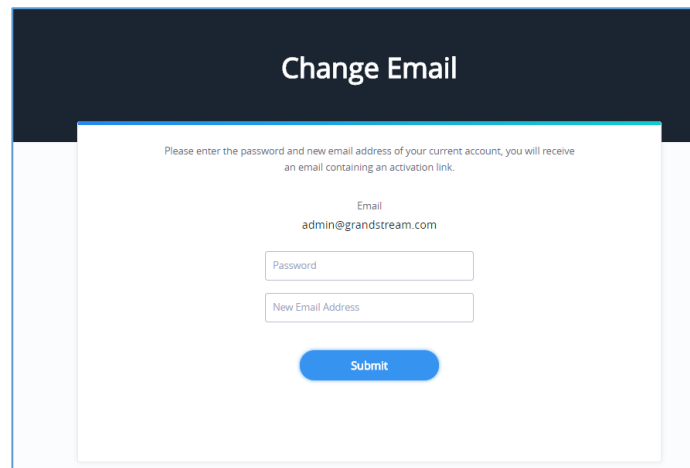


**Figure 113 : Edit Super Administrator Password**

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

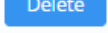
### Changing Super Administrator Email

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

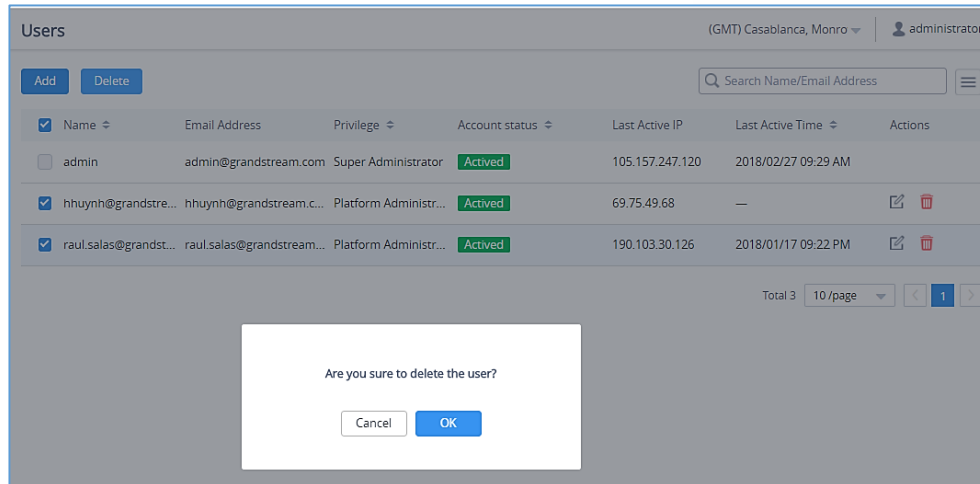


**Figure 114 : Edit Super Administrator Email**

### Delete Users

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






**Figure 115 : Delete Users**

## Change Log

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

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 116: 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.



More Details ✕

Update Account

Old Value

Idle timeout (min) 180

User name admin

New Value

Idle timeout (min) 180

User name administrator

**Figure 117: Change Log Action**

**Note:** This option can be found under [Global section](#) for **GWN Manager**

## Report

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

To generate the report, click on **username** from the top right corner → **Report**, then click on

**Create Report**

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

**Report**
(GMT+01:00) Casablanca, ▼
admin

Schedule
Generated Report

Create Report

Q Search Title

Title ↕	Scheduled Time ↕	Administrator	Report Frequency	Actions
EMEA_Report	2018-09-18 11:42AM	admin@gmail.com	Daily	<span style="font-size: 0.8em; margin-right: 5px;">📄</span> <span style="font-size: 0.8em; color: red;">🗑</span>

Total 1
 

10 /page

<
1
>

**Figure 118: Generate Report**



Create Report

Title

EMEA\_Report

Network

☒ default
 ☒ Casablanca
 ☐ Berlin

Report Contents

☒ Clients Count
 ☒ Bandwidth Usage
 ☒ Client Statistics  
(Client Manufacturer, Client OS, New Clients, Return Clients, Average Duration)
☐ Guest Statistics  
(Guest New Session, Guest Session, Max Concurrent New Session, Login Failure)

☒ Top APs
 

Top 20

☒ Top Clients
 

Top 50

☒ Top SSIDs
 

Top 5

Report Frequency

Daily

Report Generate Time

Now

Email Address

admin@grandstream.com

+

+

Add Email Address

Cancel

OK

**Figure 119: Create Report**

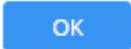
The following table provides an explanation about different options for report settings:

**Table 23: Report Settings**

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





<b>Report Contents</b>	<p>Specify the report contents for the <i>selected network group(s)</i>, the contents can include:</p> <ul style="list-style-type: none"> <li>• <b>Clients Count:</b> reports the number of clients for all the SSIDs under selected network group.</li> <li>• <b>Bandwidth Usage:</b> The download and upload level statistics for all the SSIDs for the selected network group</li> <li>• <b>Clients Statistics:</b> 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.</li> <li>• <b>Guest Statistics:</b> reports statistics about the clients connected via Captive portal including the Guest New session, the Max concurrent New session, the login failure.</li> <li>• <b>Top APs:</b> reports the top 5/20/50 APs that consumed the max of the bandwidth/data.</li> <li>• <b>Top Clients:</b> Lists the top 5/20/50 clients that downloaded/uploaded the max of data</li> <li>• <b>Top SSIDs:</b> reports the top 5/20/50 SSIDs that are mostly used by clients.</li> </ul>
<b>Report Frequency</b>	Specify the report frequency to be generated either on daily basis, weekly, monthly or custom range.
<b>Date</b>	Specify the Start and Date for the report to be generated when selecting “ <i>Custom Range</i> ” as <b>Report Frequency</b> .
<b>Report Generate Time</b>	Select either to generate the report now, or at later time
<b>Time</b>	<p>Specify when you want the report to be generated.</p> <p>This field appear when selecting “<b>Later</b>” in “<b>Report Generate Time</b>”.</p>
<b>Email Address</b>	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 .

Report				
(GMT+01:00) Casablanca, admin				
Schedule Generated Report				
<div>Create Report</div> <div>Search Title</div>				
Title	Scheduled Time	Administrator	Report Frequency	Actions
EMEA_Report	2018-09-18 11:42AM	admin@gmail.com	Daily	 
Total 1 10 /page				

**Figure 120: Created Report**

#### Note:

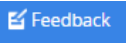
- Once you create a report, it cannot be edited afterwards, you will need to delete it and create a new one.
- Once the report is generated, it will appear under **Generated Report** section, the administrator can view it by clicking on  Action button, download it in PDF format by clicking on , or delete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

Report				
(GMT+01:00) Casablanca, admin				
Schedule <u>Generated Report</u>				
<div>Search Title</div>				
Title	Generated Time	Administrator	Report Frequency	Actions
EMEA_Report-Sep 16 2018-Sep 16 2018	2018-09-17 11:42AM	admin@gmail.com	Daily	  
Total 1 10 /page				

**Figure 121: Generated Report**


- This option can be found under [Global section](#) for **GWN Manager**

## Feedback


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


Feedback
X

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

 Upload Attachment (Up to 5 can be uploaded)  
 ( File type: zip, tar, rar, xls, xlsx, txt, docx, doc, jpeg, jpg, png, pdf, mp4, avi, wav, csv )


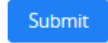
\* Please enter your email address so that we can contact you in time.

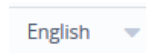
Admin@gs.com


 Add Email

Cancel
Submit

**Figure 122: Feedback**

Users can add multiple emails by click on  before  feedbacks

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



## GLOBAL (GWN MANAGER ONLY)

### Manager Settings

#### Manager Log

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

#### SMTP Server

Set up SMTP server configuration:

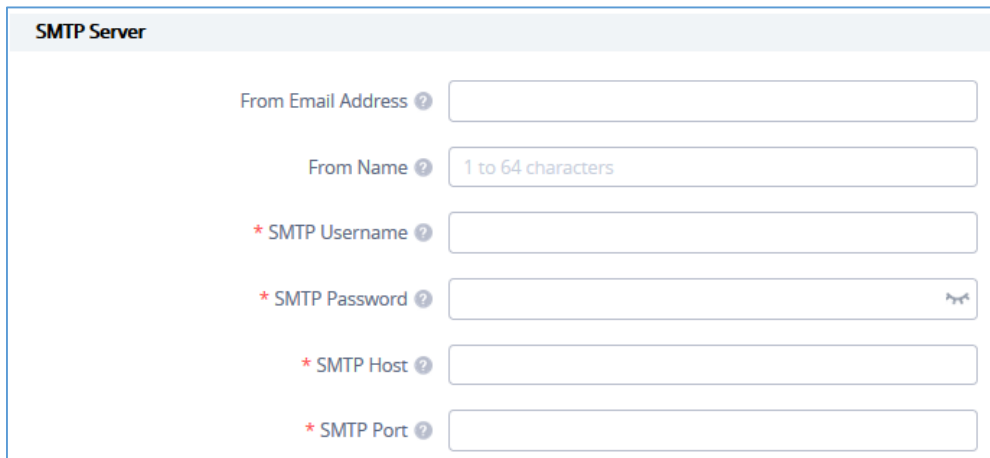


Figure 123: SMTP server

Table 24: SMTP server Configuration Details

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

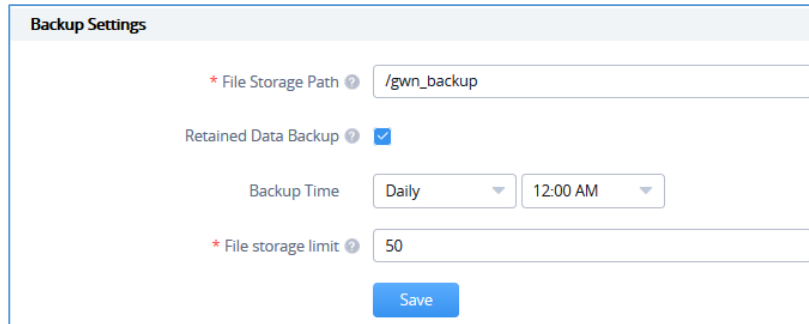


Users may test the configuration using option

Send test email

## Backup & Restore

Users can Backup GWN Manager configuration as shown below:

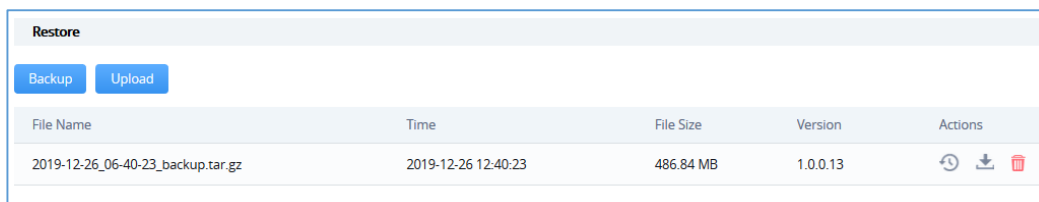


**Figure 124: Backup Settings**

**Table 25: Backup Configuration Details**

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

Restore tab holds the two option “Backup and Upload:



**Figure 125: Restore**

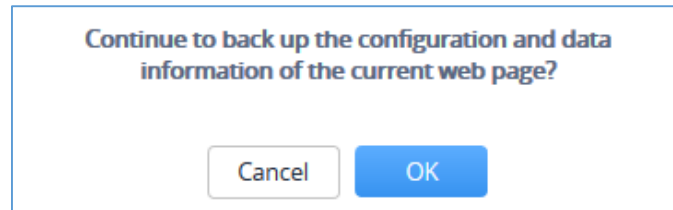
Users can either click 

Upload

 to import backup from the local directory. Or, click 




Backup

 to backup immediately. A pop window will show to confirm the operation:



**Figure 126: Confirm Backup**

A list of available Backup files with their specific Time, File Size and Version is displayed on the bottom

where the user may Restore , Download  or Delete  a File.

## Report

Refer to [Report] section.

## Change Log

Refer to [Change Log] section.



## EXPERIENCING GWN MANAGEMENT PLATFORMS

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

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

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

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