Grandstream Networks, Inc.

GWN7600LR

Outdoor Long Range 802.11ac Wave-2 WiFi Access Point

User Manual

COPYRIGHT

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

http://www.grandstream.com/support

CAUTION

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this guide, could void your manufacturer warranty.

FCC Caution

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

GNU GPL INFORMATION

GWN7600LR firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site:
http://www.grandstream.com/support/faq/gnu-general-public-license

Table of Contents

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes how to configure the GWN7600LR via Web GUI in standalone mode, with other GWN7600LR as Master/Slave architecture and more. The intended audiences of this document are network administrators. Please visit http://www.grandstream.com/support to download the latest "GWN7600LR User Manual".

This guide covers following topics:

CHANGE LOG

This section documents significant changes from previous versions of the GWN7600LR user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.4.12

- Added support for Timed Client Disconnect and Enhanced Client Blocking [CLIENTS CONFIGURATION]
- Added support for Client Bridge [Client Bridge]
- Added support for Syslog server [Syslog]
- Added support for Configurable web UI access port [Web HTTP Access]
- Added support for E-mail notifications [Email/Notification]
- Included patch for WPA2 4-way handshake vulnerability [VU#228519]

Firmware Version 1.0.3.25

- This is the initial official release of GWN7600LR.

WELCOME

Thank you for purchasing Grandstream GWN7600LR Outdoor Long-range 802.11ac Wave-2 Wi-Fi Access Point. This Wi-Fi long range access point is designed to provide extended coverage support. Ideal for outdoor Wi-Fi solutions thanks to its waterproof casing and heat resistant technology. The GWN7600LR comes equipped with dual-band 2x2:2 MU-MIMO with beam-forming technology and a sophisticated antenna design for maximum network throughput and extended Wi-Fi coverage range of up to 300 meters.

To ensure easy installation and management, the GWN7600LR uses a controller-less distributed network management design and an embedded controller within the product's web user interface. This allows each access point to manage a network of up to 30 GWN76xx series APs independently without needing separate controller hardware/software and without a single point-of-failure. Its easy installation and management features packed with extra coverage support and advanced performance features make the GWN7600LR an ideal enterprise AP for mid-size wireless network deployments.

⚠ **Caution:**

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Note (VU#228519): "Out of the box" Grandstream Access Points are not affected by this issue. APs with old firmware are only affected after changing into client-bridge mode. Please refer to our white paper of "WPA Security Vulnerability" here.

PRODUCT OVERVIEW

Technical Specifications

Table 1: GWN7600LR Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)
Antennas	2x 2.4 GHz, gain 4 dBi, internal antenna 2x 5 GHz, gain 5 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 300 Mbps; 400Mbps with 256-QAM on 2.4GHz IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz radio: 2.400 - 2.4835 GHz 5GHz radio: 5.150 - 5.250 GHz, 5.725 - 5.850 GHz
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20,40 and 80 MHz
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2x2:2 2.4GHz (MIMO), 2x2:2 5GHz (MU-MIMO)
Coverage Range	Up to 984ft. (300 meters) *Coverage range can vary based on environment
Maximum TX Power	5G: 22dBm (FCC) / 20dBm (CE) 2.4G: 22dBm (FCC) / 17dBm (CE) *Maximum power varies by country, frequency band and MCS rate
Receiver Sensitivity	**2.4G** 802.11b: -99dBm@1Mbps, -91dBm@11Mbps; 802.11g:-93dBm@6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -72dBm@MCS7; 802.11n 40MHz: -69dBm @MCS7 **5G** 802.11a: -91dBm@6Mbps, -74dBm@54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac; HT40: -63dBm@MCS9; 802.11ac 80MHz: -60dBm@MCS9

SSIDs	16 SSIDs per access point
Concurrent Clients	450+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole
Mounting	Outdoor base bracket and cover bracket included
LEDs	1 tri-color LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7600LR allows it to auto-discover, auto-provision and manage up to 30 GWN76XXs in a network
Power and Green Energy Efficiency	Power over Ethernet 802.3af and 802.3at compliant Maximum Power Consumption: ▪ 12.9 W (PoE supply) ▪ 23.0 W (PoE+ supply)
Temperature & Humidity	Operation: -30°C to 60°C Storage: -30°C to 70°C Humidity: 5% to 95% Non-condensing
Physical	Unit Dimension: 290×150×35mm; Unit Weight: 708g Unit + Mounting Kits Dimension: 290×150×56mm; Unit + Mounting Kits Weight: 1528.2g Entire Package Dimension: 423×187×97mm; Entire Package Weight: 1844g
Package Content	Enterprise 802.11ac Wave-2 Outdoor Long Range WiFi Access Point, Mounting Kits, Quick Installation Guide
Waterproof Grade	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC

INSTALLATION

Before deploying and configuring the GWN7600LR, the device needs to be properly powered up and connected to the network. This section describes detailed information on installation, connection and warranty policy of the GWN7600LR.

Equipment Packaging

Table 2: GWN7600LR Equipment Packaging

Main Case	Yes (1)
Cover Interface	Yes (1)
Base Bracket	Yes (1)
Cover Bracket	Yes (1)
Assembled Screw	Yes (4)
Locknut	Yes (4)
Anchors + Screws	Yes (4)
Screw (PM8 x 115)	Yes (4)
Quick Installation Guide	Yes (1)
GPL License	Yes (1)

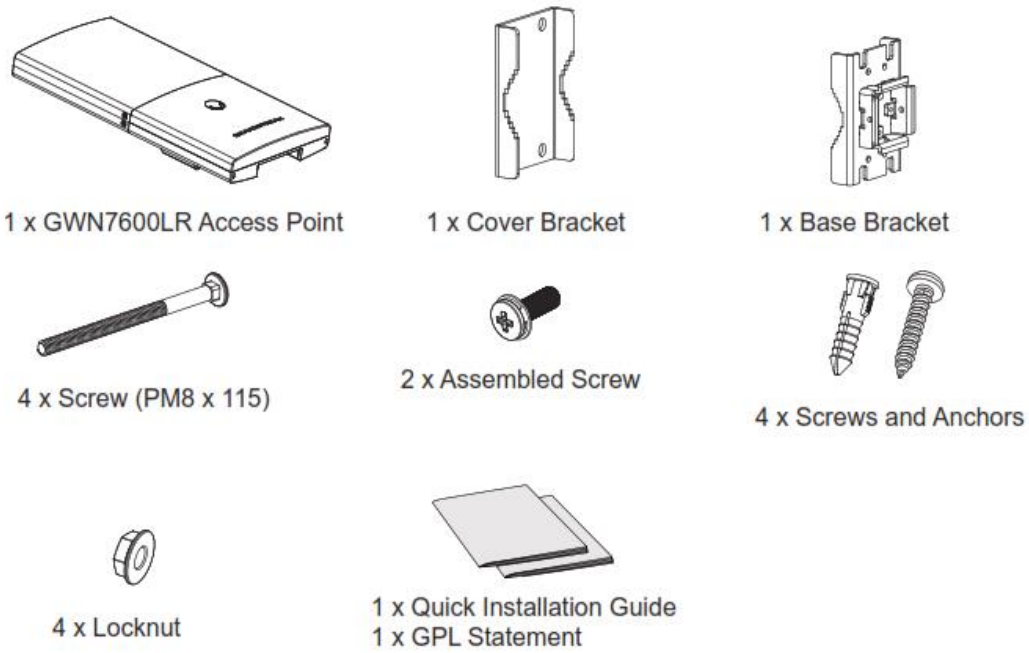

Figure 1: GWN7600LR Equipment Package

GWN7600LR Access Point Ports

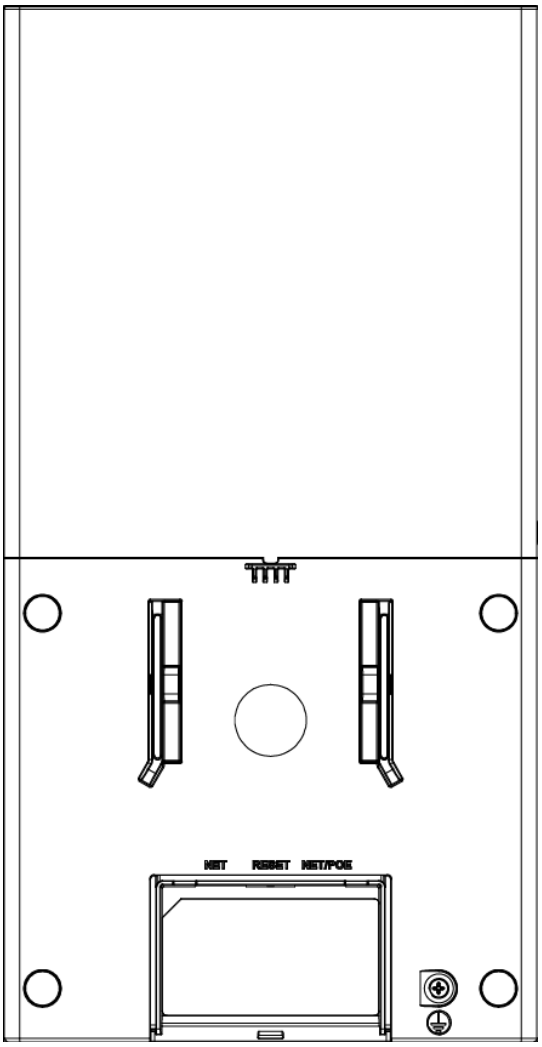

Figure 2: GWN7600LR Ports

Table 3: GWN7600LR Ports Description

Port	Description
NET/PoE	Ethernet RJ45 port (10/100/1000Mbps) supporting PoE.
NET	Ethernet RJ45 port (10/100/1000Mbps) to your router or another GWN76xx series.
RESET	Factory reset button. Press for 7 seconds to reset factory default settings.

Power and Connect GWN7600LR Access Point

1. Connect one end of a RJ-45 Ethernet cable into the PoE/NET port of the GWN7600LR.
2. Connect the other end of the Ethernet cable(s) to a PoE switch connected to your LAN network.
3. Wait for the GWN7600LR to boot up and acquire an IP address from the DHCP Server.

Mounting Instructions

Please refer to the following steps for the mounting your GWN7600LR correctly.

1. Prepare the Cover Bracket by inserting the 4 screws (PM8) into corresponding holes.
2. Attach the Cover Bracket with screws on the vertical/horizontal Mounting Bolt were GWN7600LR will be installed.
3. Assemble the Base Bracket with the Cover Bracket using provided locknuts and screws (PM8).
4. Connect the Ethernet cable (RJ45) to the correct ports of your GWN7600LR.
5. Align the GWN7600LR with the Base Bracket and pull it down to the right position.
6. Install the 2x Assembled screws to fix GWN7600LR on the Mounting Bolt.

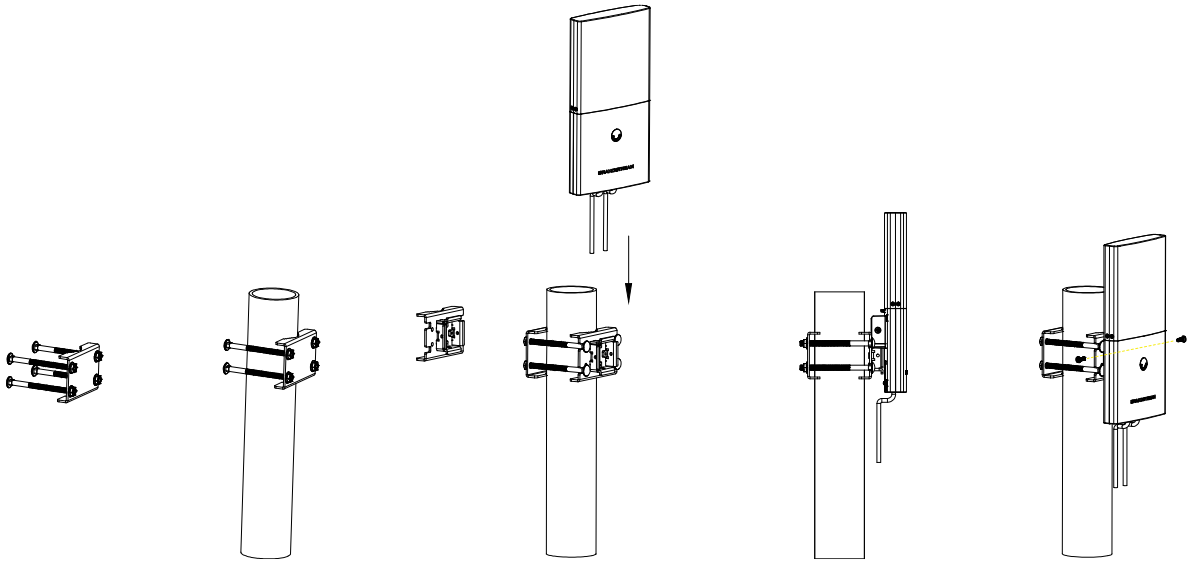

Figure 3: GWN7600LR Vertical Mounting

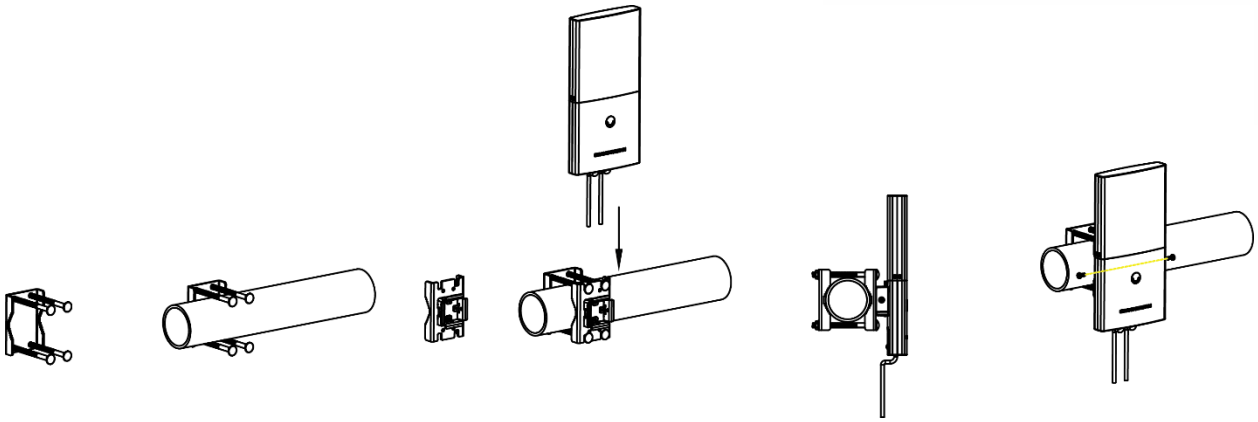

Figure 4: GWN7600LR Horizontal Mounting

Warranty

If the GWN7600LR Wireless Access Point was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for a RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.

GETTING STARTED

The GWN7600LR Wireless Access Point provides an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN7600LR's setup.

This section provides step-by-step instructions on how to read LED patterns, discover the GWN7600LR and use its Web GUI interface.

LED Patterns

The panel of the GWN7600LR has different LED patterns for different activities, to help users read the status of the GWN7600LR whether it's powered up correctly, provisioned, in upgrading process and more.

The table below describes LED patterns available on GWN7600LR.

Table 4: LED Patterns

LED Status	Indication
OFF	GWN7600LR is powered off or abnormal power supply.
Solid green	GWN7600LR is powered on.
Blinking green	GWN7600LR's firmware update in progress.
Solid green	GWN7600LR's firmware update successful.
Solid red	GWN7600LR's update failed.
Blinking purple	GWN7600LR not provisioned.
Blinking blue	GWN7600LR provisioning in progress.
Solid blue	GWN7600LR is provisioned successfully.

Discover the GWN7600LR

Once the GWN7600LR is powered up and connected to the Network correctly, users can discover the GWN7600LR using one of the below methods:

Method 1: Discover GWN7600LR using its MAC address

1. Locate the MAC address of the GWN7600LR from the package box.
2. From a computer connected to same Network as the GWN7600LR, type in the following address using the GWN7600LR's MAC address on your browser https://gwn_<mac>.local

For example, if a GWN7600LR has the MAC address **00:B8:8B:7E:7E:7E**, this unit can be accessed by typing https://gwn_00b88b7e7e7e.local/ on the browser.

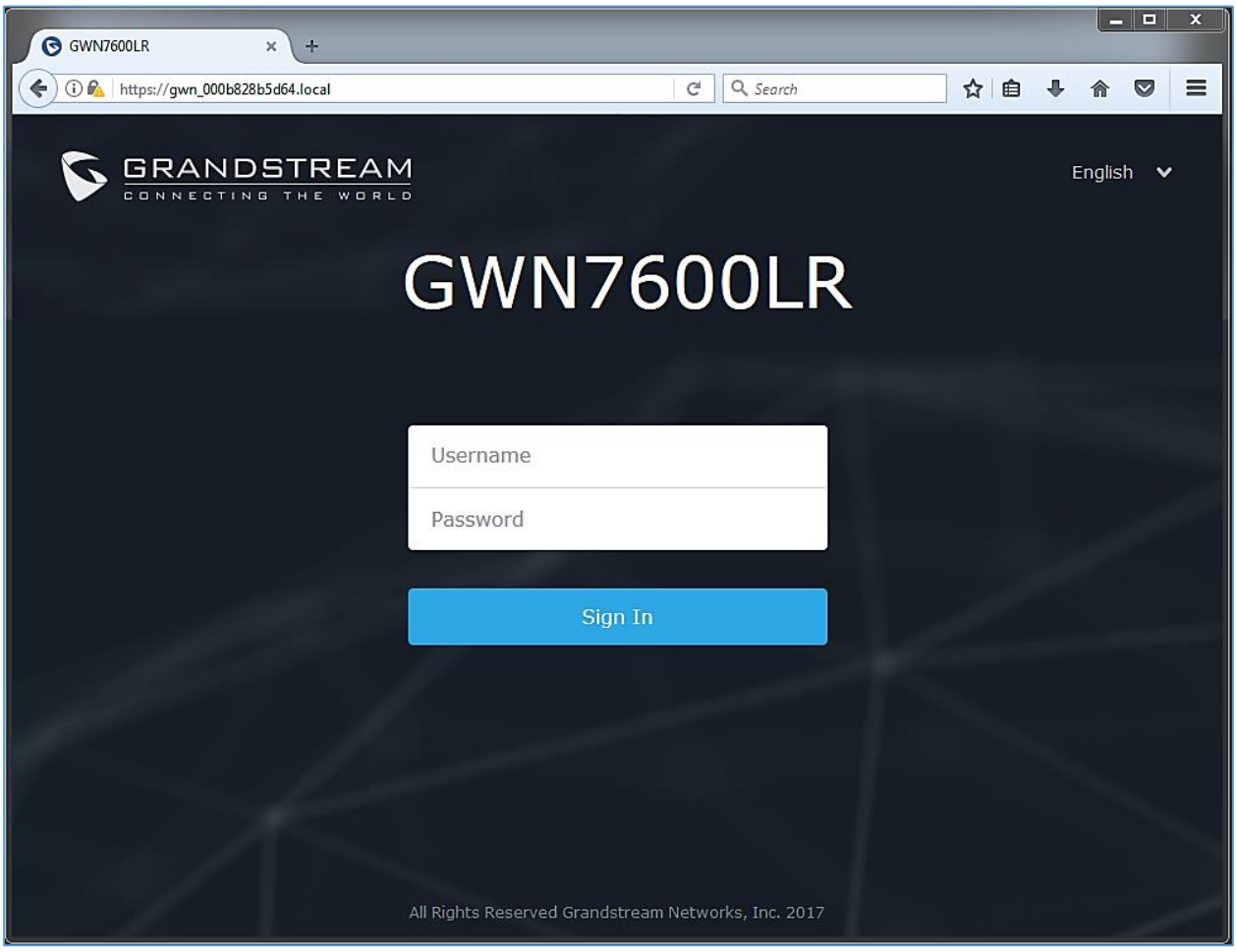

Figure 5: Discover the GWN7600LR using its MAC Address

Method 2: Discover GWN7600LR using GWN Discovery Tool

1. Download and install **GWN Discovery Tool** from the following link: http://www.grandstream.com/support/tools
2. Open the GWNDiscoveryTool, and click on **Scan**.
3. The tool will discover all GWN76xx Access Points, including GWN7600LR, connected to the network showing their MAC and IP addresses.
4. Click on **Manage Device** to be redirected directly to the GWN7600LR's configuration interface, or type in manually the displayed IP address on your browser.

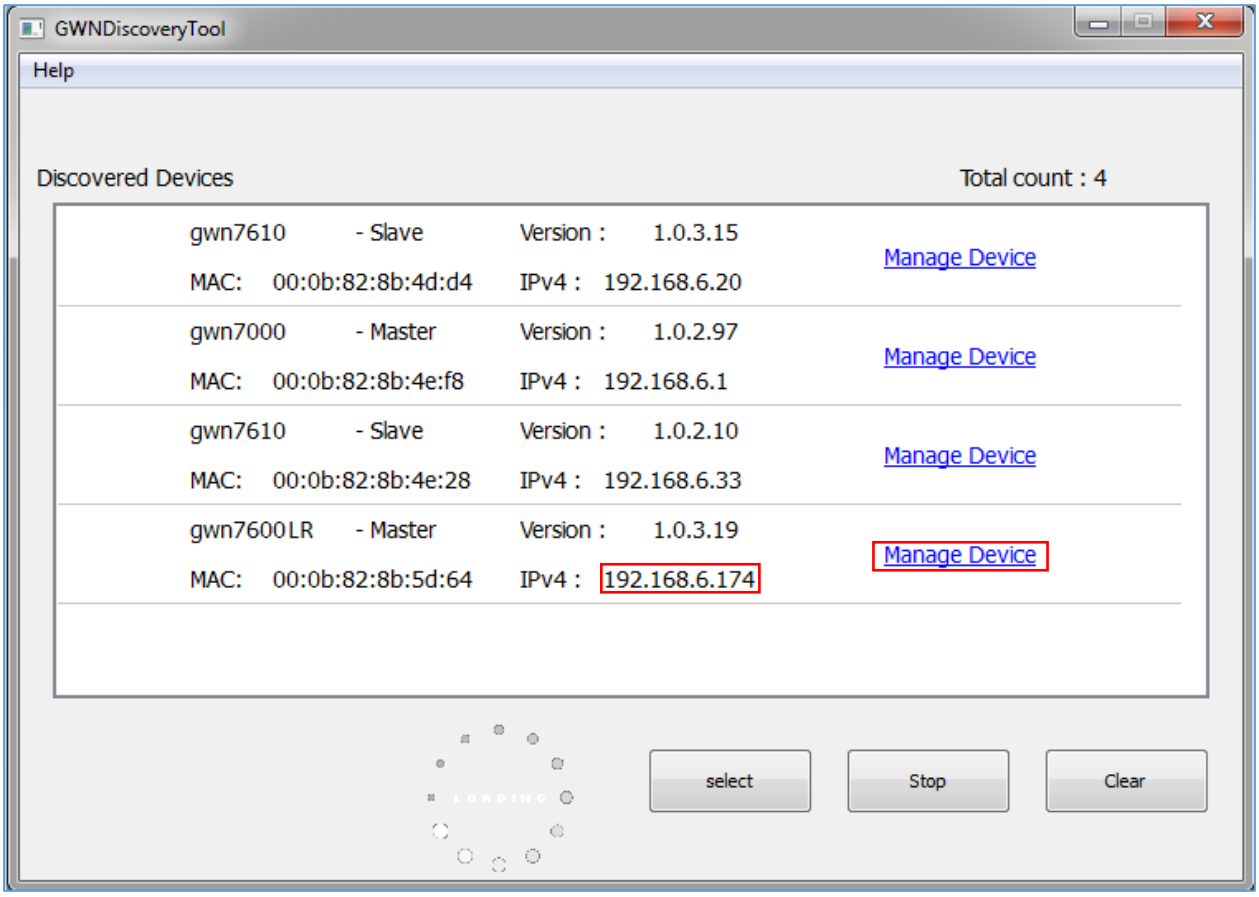

Figure 6: GWN Discovery Tool

Users can access then the GWN7600LR using its Web GUI, the following sections will explain how to access and use the Web Interface.

Use the Web GUI

Access Web GUI

The GWN7600LR embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome etc.

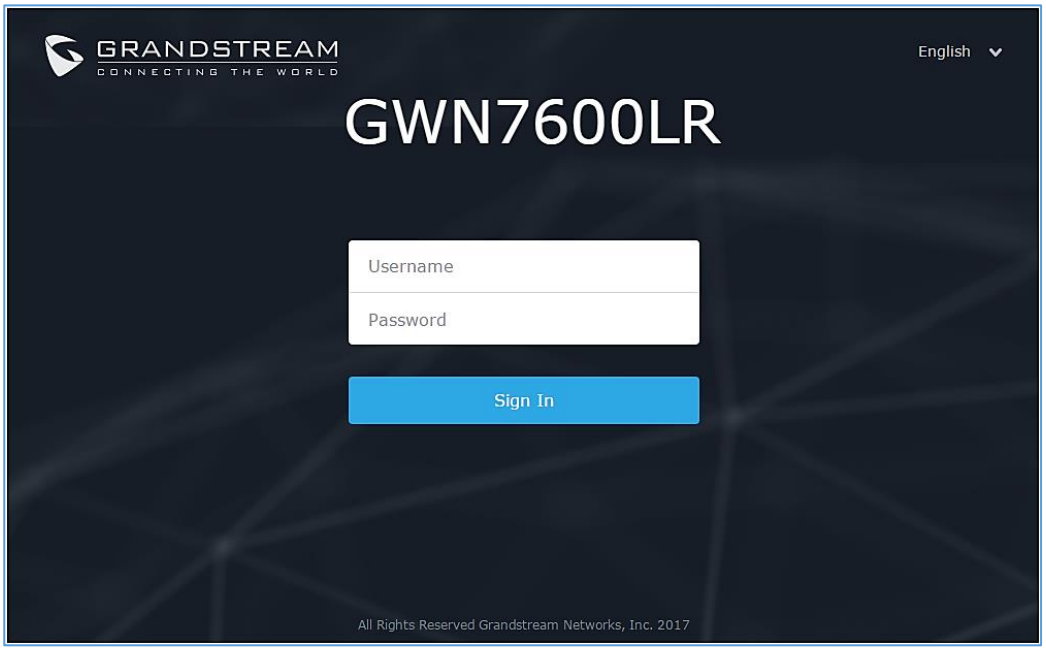

Figure 7: GWN7600LR Web GUI Login Page

To access the Web GUI:

1. Make sure to use a computer connected to the same local Network as the GWN7600LR.
2. Ensure the device is properly powered up.
3. Open a Web browser on the computer and type in the URL using the MAC address as shown in Discover the GWN7600LR or the IP address using the following format:

   https://IP_Address

4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username and password are "admin" and "admin".

Web GUI Languages

Currently the GWN7600LR series web GUI supports ***English*** and ***Simplified Chinese.***
Users can select the displayed language at the upper right of the web GUI either before or after logging in.

Figure 8: GWN7600LR Web GUI Language

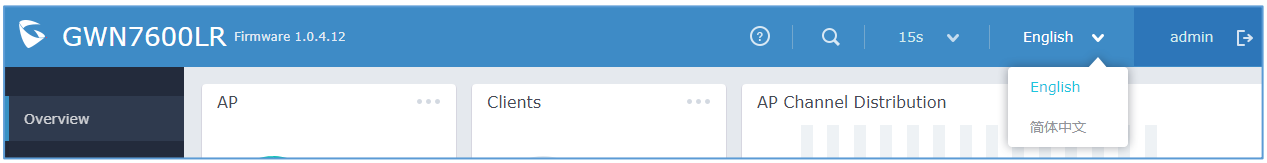

Figure 9: GWN7600LR Web GUI Language

Overview Page

Overview is the first page shown after successful login to the GWN7600LR's Web Interface. Overview page provides an overall view of the GWN7600LR's information presented in a Dashboard style for easy monitoring.

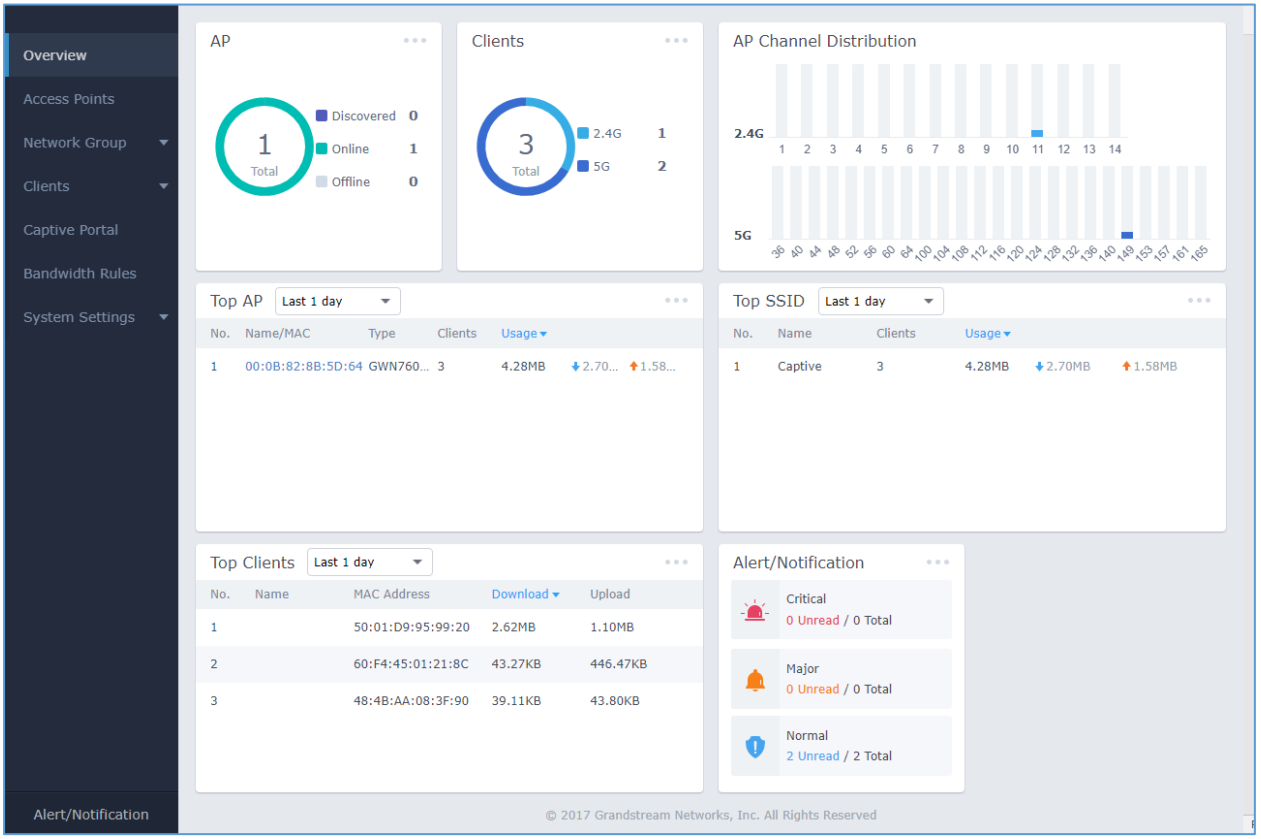

Figure 10: Overview Page

Users can quickly see the status of the GWN7600LR for different items, please refer to the following table for each item:

Table 5: Overview

AP	Shows the number of Access Points that are Discovered, Paired(Online) and Offline. Users may click on ••• to go to Access Points page for basic and advanced configuration options for the APs
Clients	Shows the total number of connected clients, and a count for clients connected to each Channel. Users may click on ••• to go to Clients page for more options.
AP Channel Distribution	Shows the Channel used for all APs that are paired with this Access Point.
Top AP	Shows the Top APs list, users may assort the list by number of clients connected to each AP or data usage combining upload and download. Users may click on ••• to go to Access Points page for basic and advanced configuration options for the APs.
Top SSID	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on ••• to go to Network Group page for more options.
Top Clients	Shows the Top Clients list, users may assort the list of clients by their upload or download. Users may click on ••• to go to Clients page for more options.
Alert/Notification	Shows 3 types of Alert/Notifications: Critical, Major and Normal. Users can click ••• to pop up the list of Alert and Notifications.

Note that status icons can be updated each 15s, 1min, 2min, 5min or Never by clicking in the upper bar menu (Default is 15s).

Save And Apply Changes

When clicking on "Save" button after configuring or changing any option on the web GUI pages. A message mentioning the number of changes will appear on the upper menu (See Figure 11).

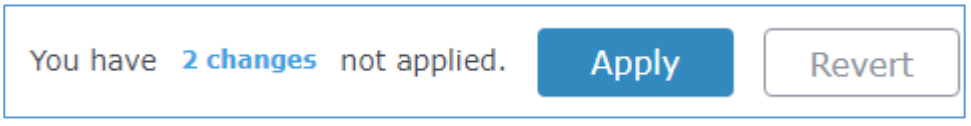

Figure 11: Apply Changes

Click on Apply button to apply changes, or Revert to undo the changes.

USING GWN7600LR AS STANDALONE ACCESS POINT

The GWN7600LR can be used in Standalone mode, where it can act as Master Access Point Controller or in Slave mode and managed by another GWN7600LR Master.

This section will describe how to use and configure the GWN7600LR in standalone mode.

Connect to GWN7600LR Default Wi-Fi Network

GWN7600LR can be used as standalone access point out of box, or after factory reset with Wi-Fi enabled by default.

After powering the GWN7600LR and connecting it to the network, GWN7600LR will broadcast a default SSID based on its MAC address **GWN[MAC's last 6 digits]** and a random password.

Note that GWN7600LR's default SSID and password information are printed on the MAC tag of the unit as shown on the below figure.

Figure 12: MAC Tag Label

Note : Label's content is for reference only, subject to actual production.

USING GWN7600LR AS MASTER ACCESS POINT CONTROLLER

Master Mode allows a GWN7600LR to act as an Access Point Controller managing other GWN7600LR access points. This will allow users adding other access points under one controller and managing them in an easy and a centralized way.

Master/Slave mode is helpful with large installations that needs more coverage area zones with the same controller.

Figure 13: Login Page

At factory reset, "**Login as Master**" will be checked by default, click on "**Sign In**" after typing the admin's username and password.

⚠ **Warning:**

"**Login as Master**" option will forbid the GWN7600LR Access Point from being paired by other Master GWN76xx, and can only act as a Master Access point controller.

Users will need to perform a factory reset to the GWN7600LR, or unpair it from the initial GWN76xx to make it open to Master Access Point mode again.

Login Page

After login, users can use the Setup Wizard tool to go through the configuration setup, or exit and configure it manually. Setup Wizard can be accessed anytime by clicking on while on the web interface.

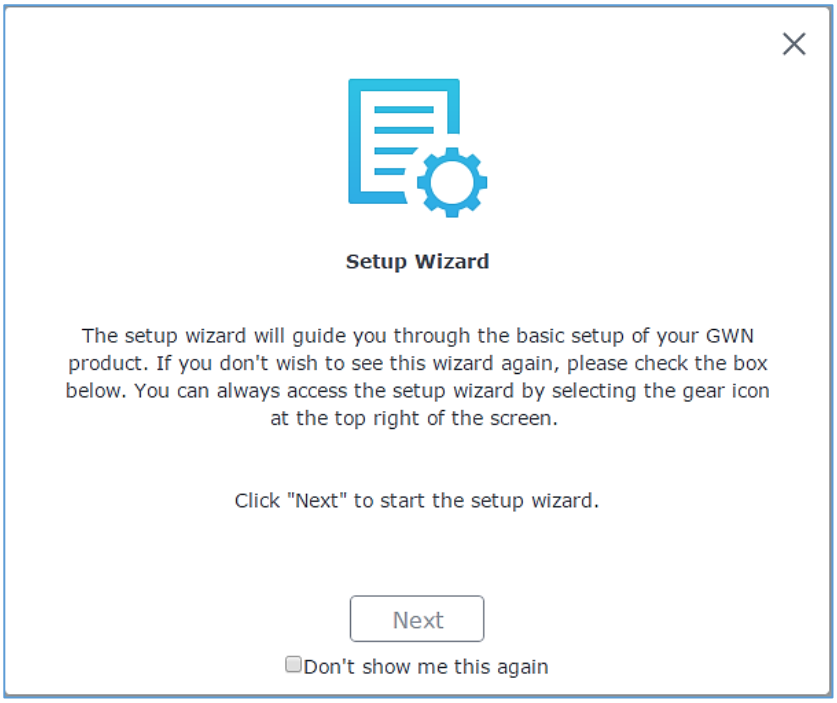

Figure 14: Setup Wizard

Discover and Pair Other GWN7600LR Access Point

To Pair a GWN7600LR access point connected to the same Network as the GWN7600LR follow the below steps:

1. Connect to the GWN7600LR Web GUI as Master and go to **Access Points.**

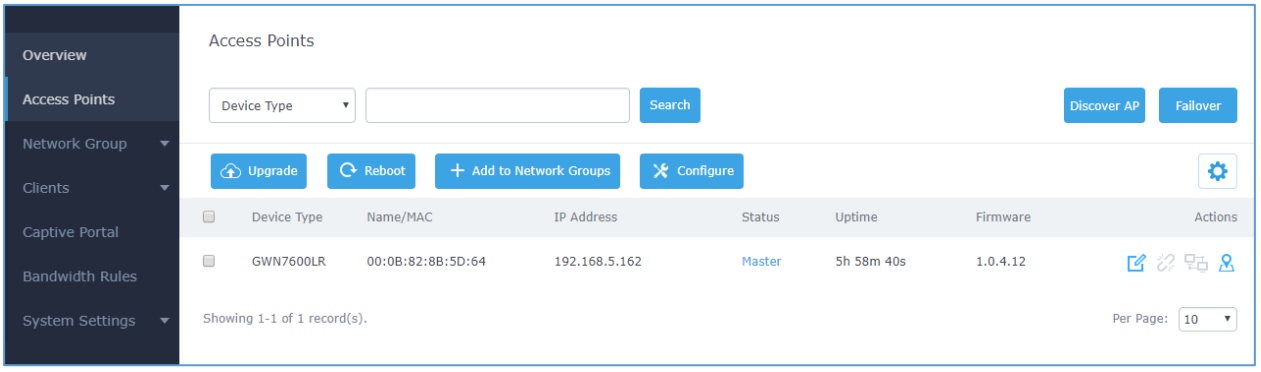

Figure 15: Discover and Pair GWN7600LR

2. Click on Discover AP to discover access points within GWN7600LR's Network, the following page will appear.

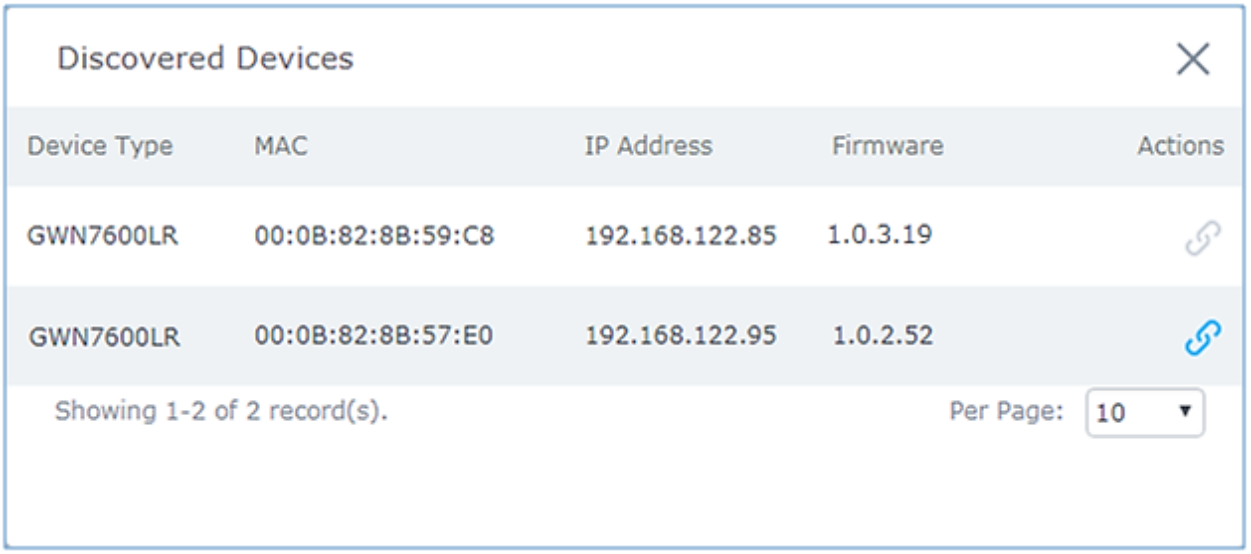

Figure 16: Discovered Devices

3. Click on Pair under Actions to pair the discovered access point as slave with the GWN7600LR acting as Master.

4. The paired GWN7600LR will appear Online, users can click on to unpair it.

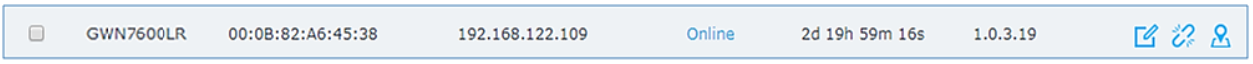

Figure 17: GWN7600LR online

5. Users can click on next to Master or paired access point to check device configuration for its status, users connected to it and configuration. Refer to below table for Device Configuration tabs.

Table 6: Device Configuration

Status	Shows the device's status information such as Firmware version, IP Address, Link Speed, Uptime, and Users count via different Radio channels.
Clients	Shows the connected Users to the GWN7600LR access point.
Configuration	• **Device Name:** Set GWN7600LR's name to be shown next to MAC address. • **Fixed IP:** Used to set a static IP for the GWN7600LR, if checked users will need to set the following:

- IPv4 Address: Enter the IPv4 address to be set as static for the device.
- IPv4 Subnet Mask: Enter the Subnet Mask.
- IPv4 Gateway: Enter the Network Gateway's IPv4 Address.
- Preferred IPv4 DNS: Enter the Primary IPv4 DNS.
- Alternate IPv4 DNS: Enter the Alternate IPv4 DNS.

- **Frequency:** Set the GWN7600LR's frequency, it can be either 2.4GHz, 5GHz or Dual-band.
- **Band Steering:** When Frequency is set to Dual-Band, users can check this option to enable Band Steering on the Access Point, this will help redirecting clients to a radio band accordingly for efficient use and to benefit from the maximum throughput supported by the client.
- **Mode:** Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.

- **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20MHz is suggested in very high-density environment.
- **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be "Secondary Below Primary", "Primary Below Secondary" or "Auto".
- **Channel:** Select "Auto" or a specific channel. Default is "Auto". Note that the proposed channels depend on **Country** Settings under System Settings–>Maintenance.
- **Enable Short Guard Interval:** Check to activate this option to increase throughput.
- **Active Spatial Streams:** Choose active spatial stream if Auto, 1 or 2 streams.
- **Radio Power:** Set the Radio Power depending on desired cell size to be broadcasted, three options are available: "Low", "Medium" or "High". Default is "High".
- **Allow Legacy Devices(802.11b):** Check to support 802.11b devices to connect the AP in 802.11n/g mode.

	• **Custom Wireless Power(dBm):** allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.

Note: If a GWN7600LR is not being paired or the pair icon is grey color, make sure that it is not being paired with another GWN76xx acting as Master Access Point Controller, if yes users will need to unpair it first, or reset it to factory default settings to make it available for pairing by other GWN76xx Access Point Controller

AP Locating

Click on , the LED of the correlated AP will be blinking for 10 times, which may help to locate where the AP is.

Failover Master

In a Master-Slave architecture, having a backup Master is critical for redundancy and failover function, thus, and in order to avoid a single point of failure in your wireless network, you can specify a slave AP as failover master.

Whenever it detects the master is down, it will promote itself as failover master within a time frame of around 20~30 minutes by entering failover mode. After then, if the master AP comes back, failover master will automatically go back to slave mode, or if the master doesn't come back to alive, Administrator can login using "failover" account to turn the failover master as true master and take over all controls.

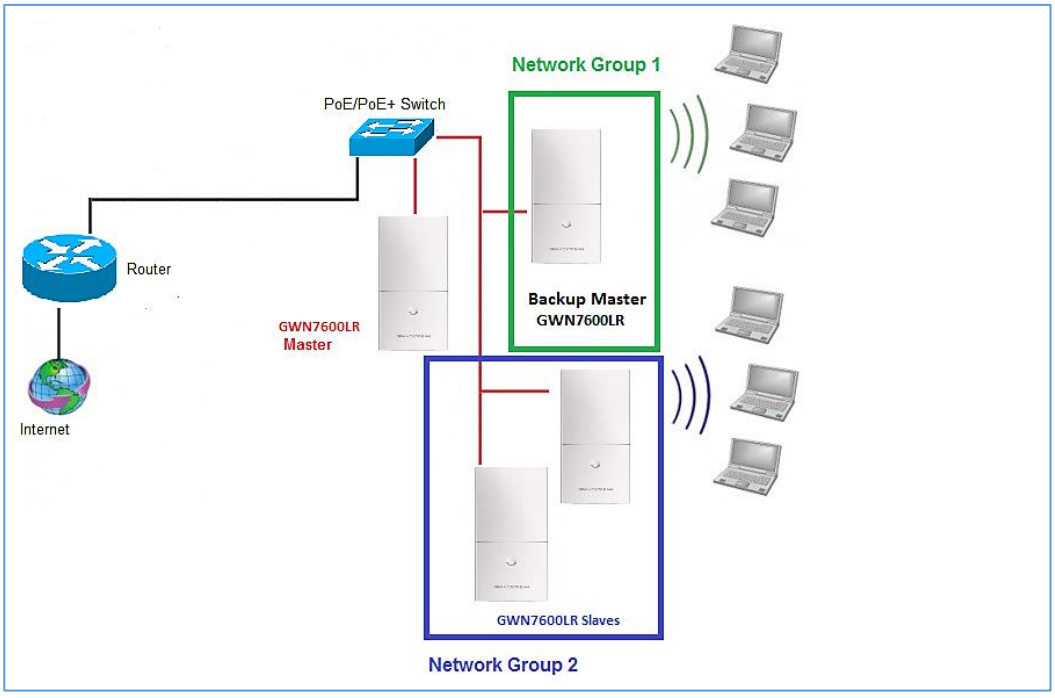

Figure 18: Failover Master

Users could select the failover Master by following below steps:

- Log into web GUI of the master GWN.
- Go to Access Points page.
- Press Failover
- Select from the available paired Slave Aps the candidate to become a failover Master.
- Save and Apply the settings.

Failover Mode

Once failover slave has been selected, the primary master will send the configuration of the network to the failover slave and the slave will start monitoring the status of the primary master to detect any failure for any reason (network connection loss, power outage).
In case of failure, the failover slave will promote itself to a temporary backup master while waiting for the primary master to come back.
During the failover mode users could access the web GUI of the failover slave using a special failover account with same admin password.

- **Username = failover**
- **Password = admin password**

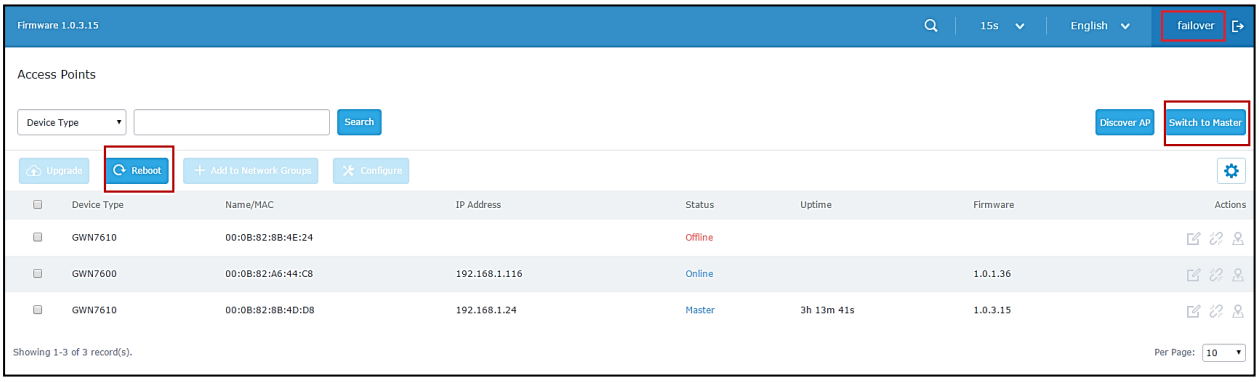

Figure 19: Failover Mode GUI

The failover mode has only read permission on the configuration and very limited options, users still can reboot other slave Access points in case it is needed.

Users also can press on **« Switch to master »** button in order to set the failover slave as the new primary master of the wireless network, once this is done they have full write permission control over the web GUI option as usual.

Client Bridge

The Client Bridge feature allows an 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 WiFi connection to the LAN ports transparently. This is not to be confused with a mesh setup. The client will not accept wireless clients in this mode.

Once a Network Group has an Client Bridge Support enabled, the AP adopted in this Network Group can be turned in to Bridge Client mode by click the Bridge button .

Please be noted that once an AP it turned into Client Bridge mode, it cannot be controlled by a Master anymore, and a factory reset is required to turn it back into normal AP mode.

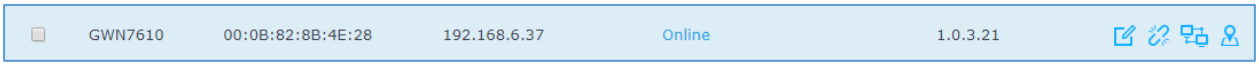

Figure 20: Client Bridge

Important Notes:

- The access point that will be operating on bridge mode, must be set with a fixed IP address before activating the bridge mode on the access point.
- Users must enable client bridge support option under network group or SSID WiFi settings in order to have it fully functional. See ***[Client Bridge Support]***

NETWORK GROUPS

When using GWN7600LR as Master Access Point, users can create different Network groups and adding GWN7600LR Slave Access Points.

Log in as Master to the GWN7600LR WebGUI and navigate to **Network Group→Network Group.**

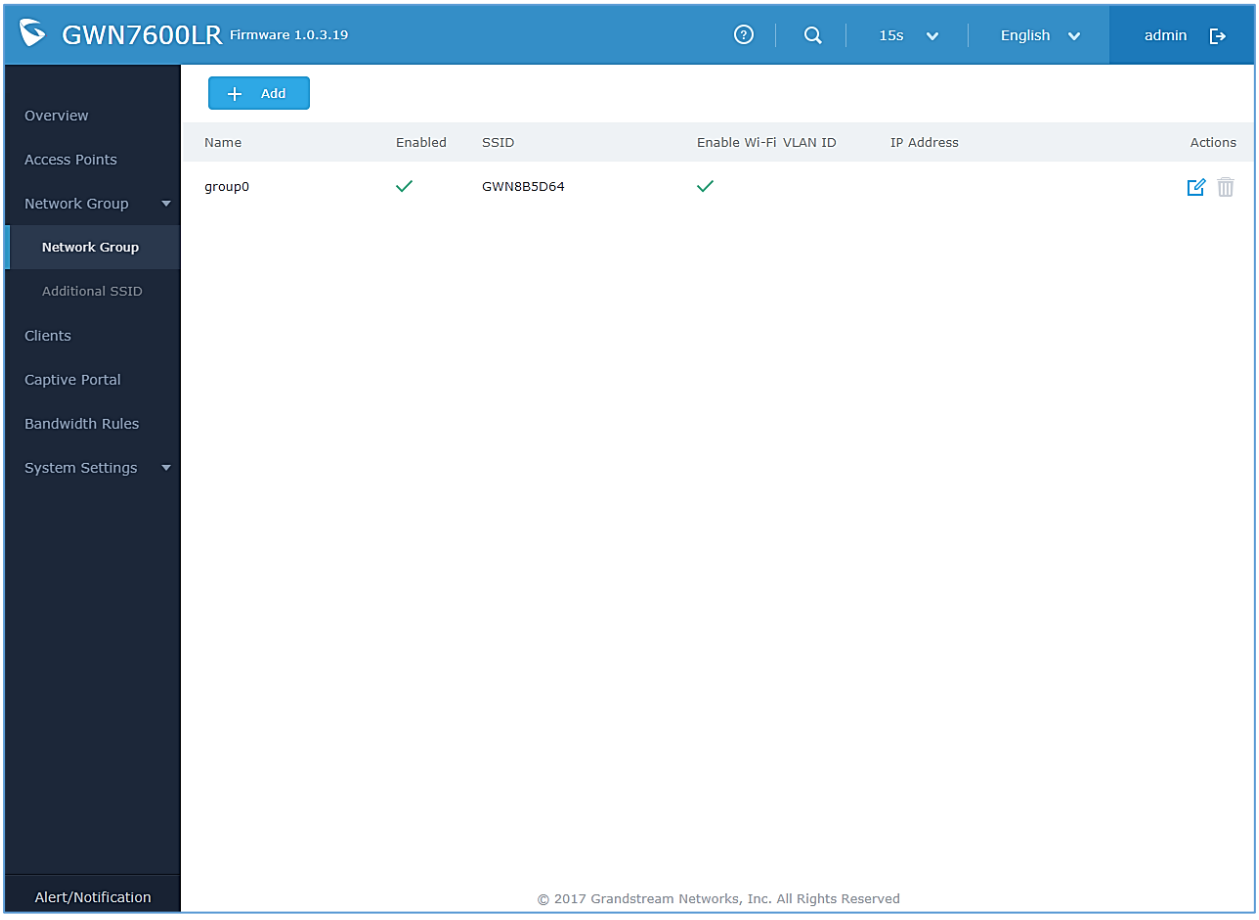

Figure 21: Network Group

The GWN7600LR will have a default network group named group0, click on to edit it, or click on Add to add a new network group.

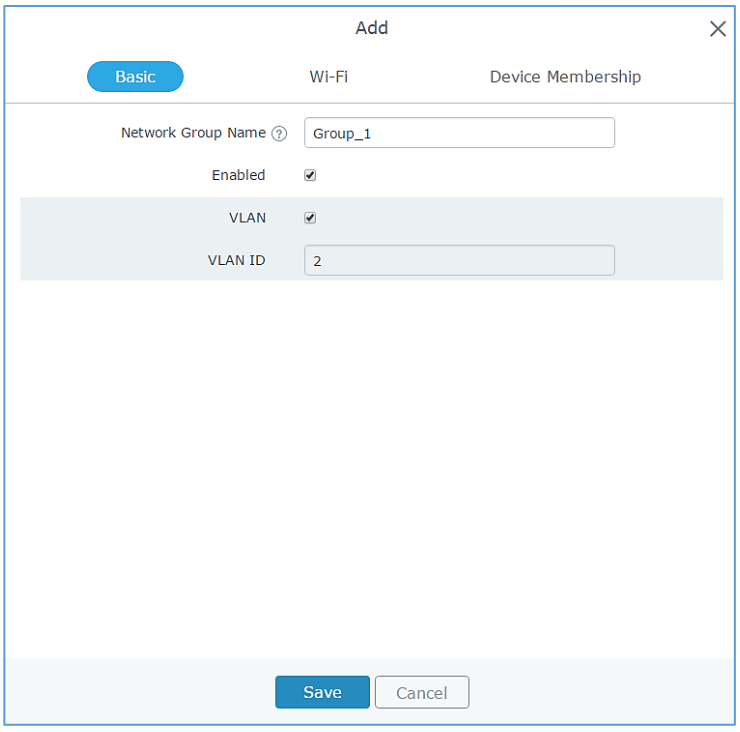

Figure 22: Add a New Network Group

When editing or adding a new network group, users will have three tabs to configure:

- **Basic:** Used to name the network group, and set a VLAN ID if adding a new network group
- **Wi-Fi:** Please refer to the below table for Wi-Fi tab options

Table 7: Wi-Fi

Field	Description
Enable Wi-Fi	Check to enable Wi-Fi for the network group.
SSID	Set or modify the SSID name.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: • **Dual-Band** • **2.4GHz** • **5Ghz**
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. If set to 0, the limit is disabled.
Enable Captive Portal	Check to enable/disable captive portal

Captive Portal Policy	Select the captive portal policy already created on the "***CAPTIVE PORTAL***" web page to be used in the created SSID.
Security Mode	Set the security mode for encryption, 5 options are available: • **WEP 64-bit**: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5. • **WEP 128-bit**: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13. • **WPA/WPA2**: Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. • **WPA2**: Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. Recommended configuration for authentication. • **Open**: No password is required. Users will be connected without authentication. Not recommended for security reasons
WPA Key Mode	Two modes are available: • **PSK:** Use a pre-shared key to authenticate to the Wi-Fi. • **802.1X:** Use a RADIUS server to authenticate to the Wi-Fi.
WPA Encryption Type	Two modes are available: • **AES:** This method changes dynamically the encryption keys making them nearly impossible to circumvent. • **AES/TKIP:** use both Temporal Key Integrity Protocol and Advanced Encryption Standard for encryption, this provides the most reliable security.
WPA Pre – Shared Key	Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters.
Client Bridge Support	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 WiFi connection to the LAN ports transparently. Once a Network Group has an Client Bridge Support enabled, the AP adopted in this Network Group can be turned in to Bridge Client mode by click the Bridge button.
RADIUS Server Address	Enter the RADIUS server IP or FQDN address.
RADIUS Server Port	Enter the RADIUS server port. The default port is 1812.

RADIUS Server Secret	Enter the shared secret between the authenticator and the RADIUS server.
RADIUS Accounting Server Address	Enter the RADIUS Accounting server IP or FQDN address.
RADIUS Accounting Server Port	Enter the RADIUS Accounting server port. The default port is 1813.
RADIUS Accounting Server Secret	Enter the shared secret between the authenticator and the RADIUS Accounting server if configured.
RADIUS NAS ID	Enter the RADIUS NAS ID.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to the zone's Wi-Fi. Default is Disabled.
Enable Dynamic VLAN (beta)	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile.
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN7600LR's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available: • **Internet Mode**: Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN7600LR. • **Gateway MAC Mode**: Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN7600LR access points. • **Radio Mode**: Wireless clients can access to the internet services, GWN7xxx router and the access points GWN7600LR but they cannot communicate with each other. The default value is "Disabled".

Gateway MAC Address	This field is required when using **Client Isolation,** so users will not lose access to the Network (usually Internet). Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":". Example: 00:0B:82:8B:4D:D8
RSSI Enabled	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in **Minimum RSSI (dBm).**
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is smaller than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1".
Enable Voice Enterprise	Check to enable/disable Voice Enterprise. The roaming time will be reduced once enable voice enterprise. • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. **Note:** 11R is required for enterprise audio feature, 11V and 11K are optional.
Enable 11R	Check to enable 802.11r
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
Upstream Rate	Set the maximum upstream rate
Downstream Rate	Set the maximum downstream rate

- **Device Membership:** Used to add or remove paired access points to the network group

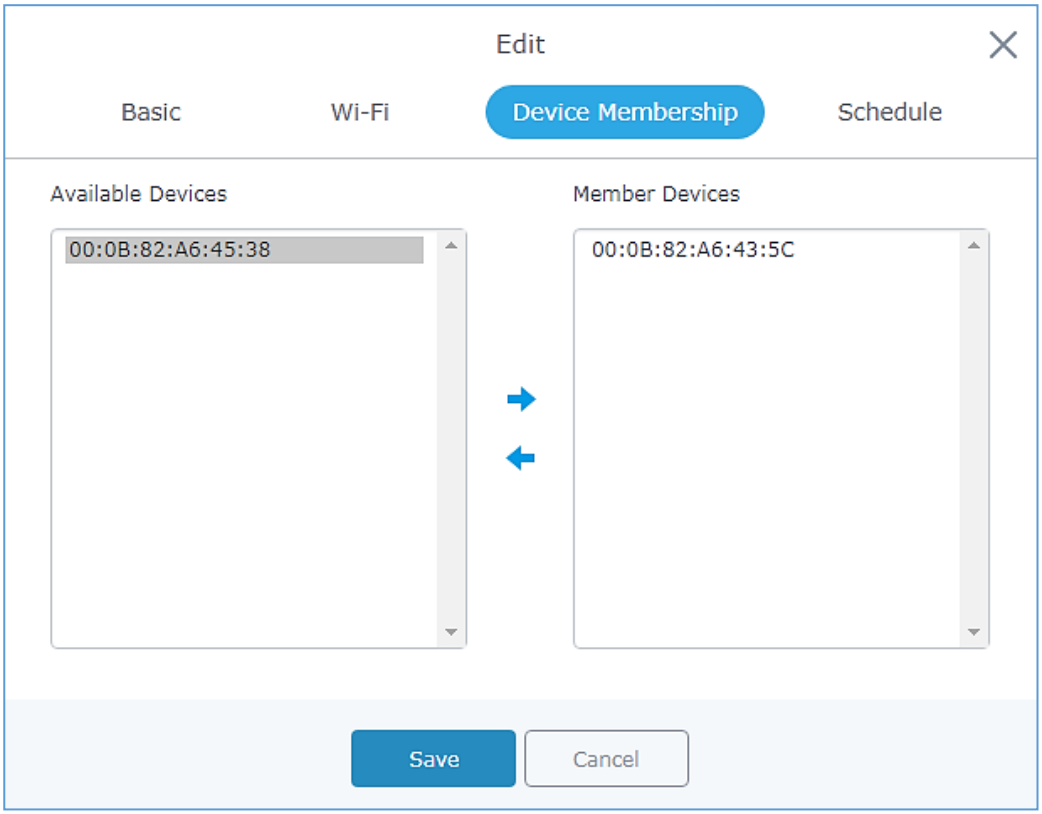

Figure 23: Device Membership

Click on → to add the GWN7600LR to the network group, or click on ← to remove it.

- **Schedule**: Used to schedule the times when the Wi-Fi is ON or OFF.

If users want to schedule the AP operation time, “Enable Wireless Schedule” should be selected first, and then, choose the days the AP needs to work, at last, click on “Save” to save configuration.

In the example below the Wi-Fi is scheduled to be active Monday starting from 8:00 AM until 5:00 PM.

Note: The hour field is in 24 format (from 0 to 23). Valid range for minutes is 0-59.

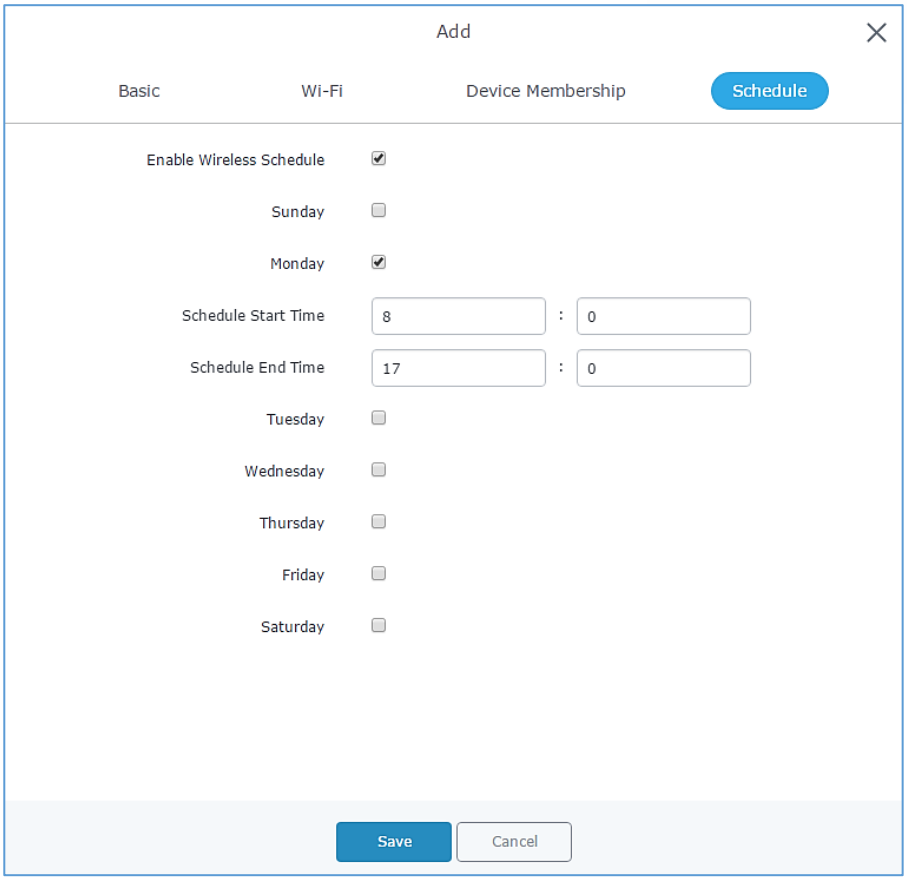

Figure 24: WiFi Schedule

Note:

The schedule feature is based on SSID and not network group, meaning that you can schedule the broadcasting of different SSID on different periods of the day.

- Users can also add a device to a Network Group from Access Points Page:

  Select the desired AP to add to a Network Group and click on 

.

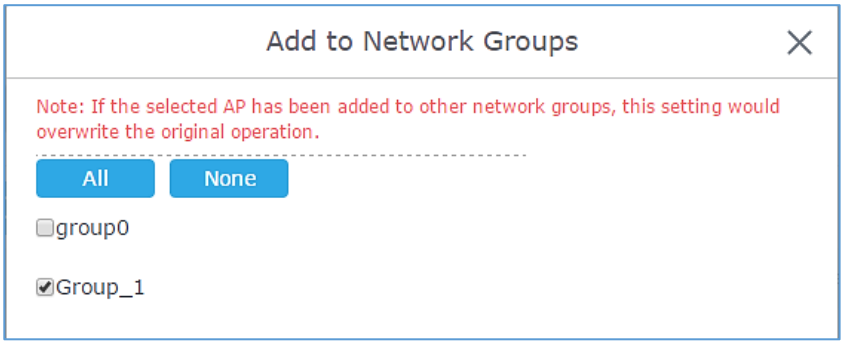

Figure 25: Add AP to Network Group

- Users can also create an additional SSID under the same group.

1. To create an additional SSID go to **Network Group→Additional SSID.**

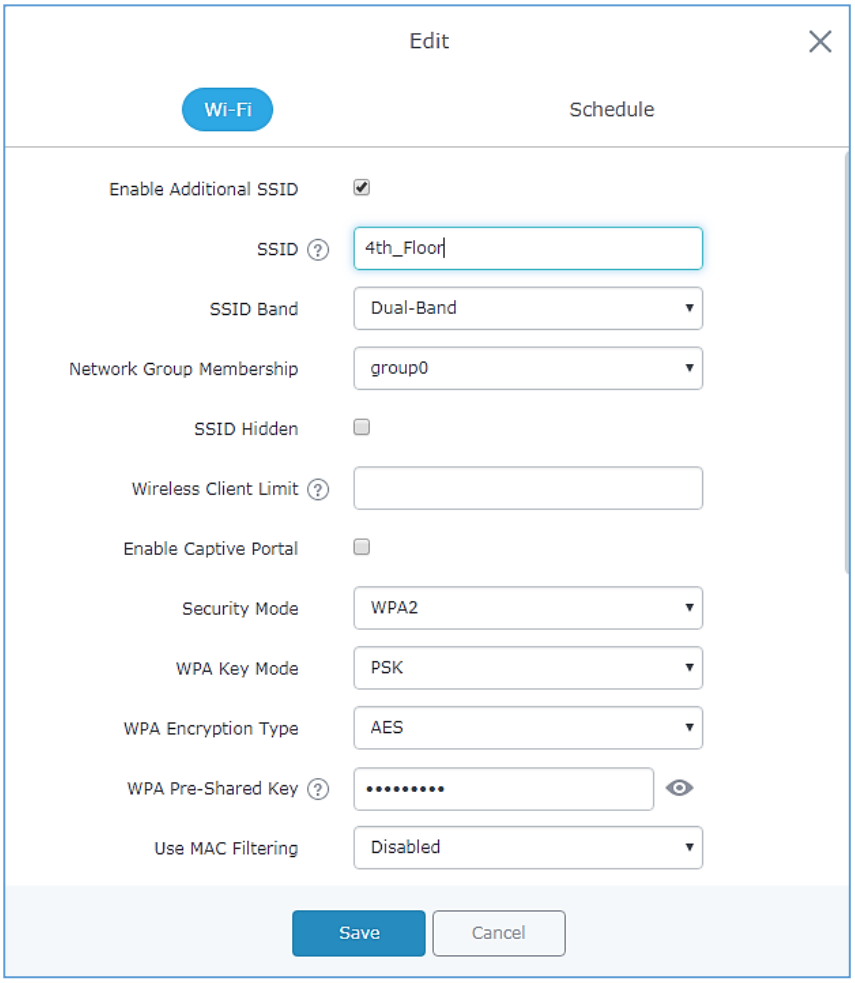

Figure 26: Additional SSID

2. Select one of the available network groups from **Network Group Membership** dropdown menu, this will create an additional SSID with the same Device Membership configured when creating the main network group.

Figure 27: Additional SSID Created

3. Click on to delete the additional SSID, or to edit it.

CLIENTS CONFIGURATION

Users can configure clients' parameters, time policy and also check the list of the clients that has been banned after time disconnect policy has been enabled. Below we discuss each section of this menu:

Clients

Users can access clients list connected to GWN7600LR from **Web GUI→Clients→Clients** to perform different actions to wireless clients.

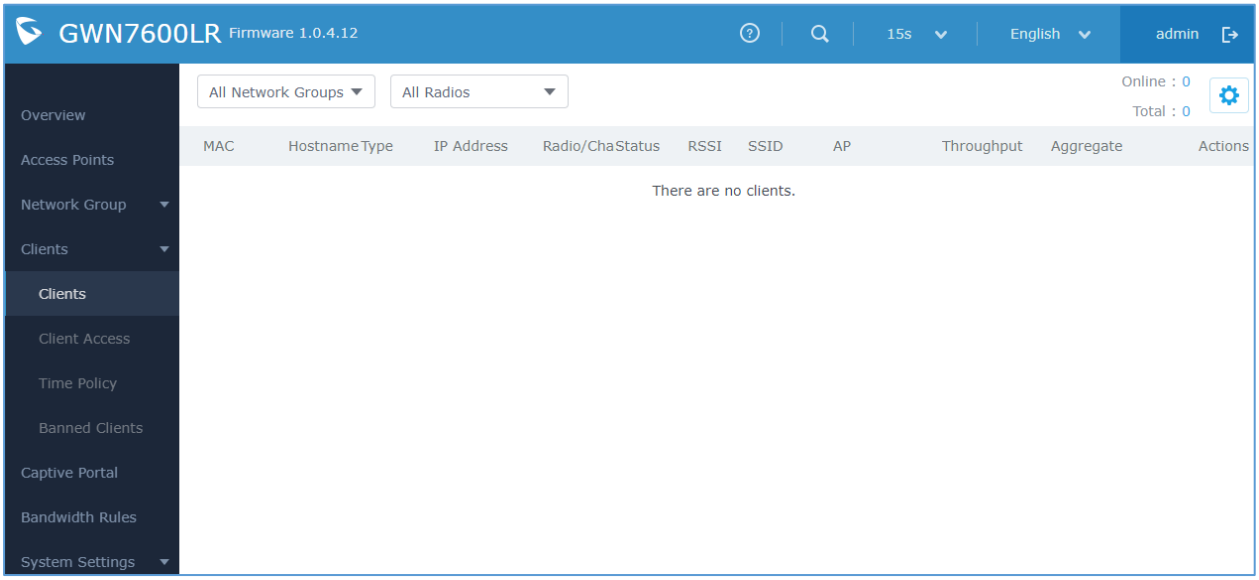

Figure 28: Clients

- Click on  under Actions to check client's status and modify basic settings such Device's Name.
- Click on  to block a client's MAC address from connecting to the zone's network group.

Clients Access

From this menu, users can manage in global and way the blacklist of clients that will be blocked from accessing the WiFi network, click on 

to add or remove MAC addresses of client from global blacklist.

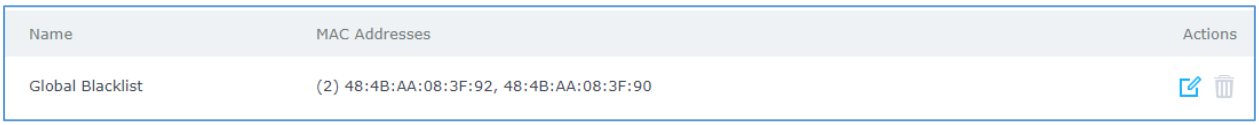

Figure 29: Global Blacklist

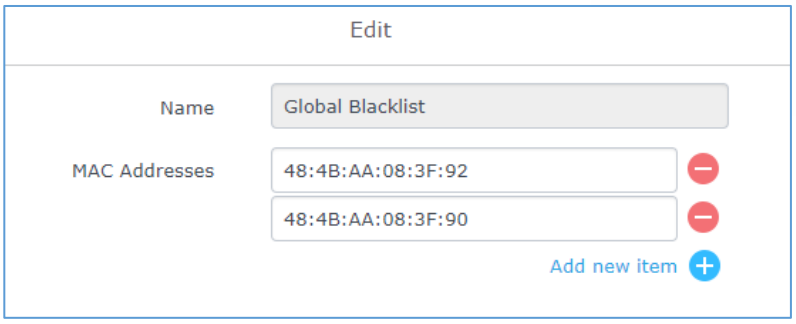

Figure 30: Managing the Global Blacklist

A second option, is to add custom access lists that will be used as matching mechanism for MAC address filtering option under network groups and SSIDs to allow (whitelist) or disallow (blacklist) clients access to the WiFi network.

Click on + Add in order to create new access list, then fill it with all MAC addresses to be matched.

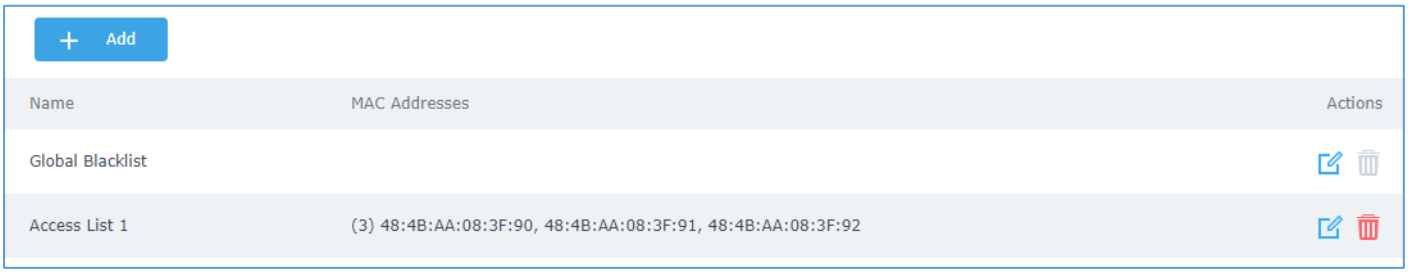

Figure 31: Adding New Access List

Once this is done, this access list can be used under network group or SSID WiFi settings to filter clients either using whitelist or blacklist mode.

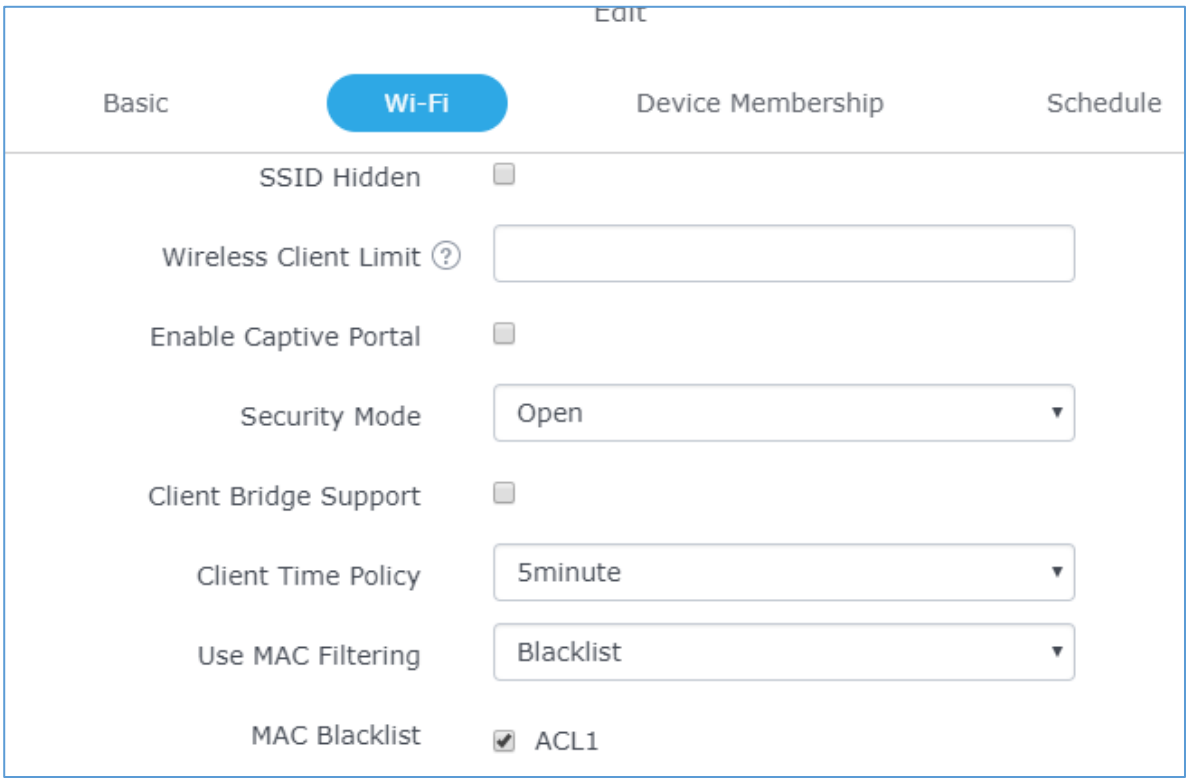

Figure 32: Blacklist Access List

Time Policy

The timed client disconnect feature allows the system administrator to set a fixed time for which clients should be allowed to connect to the access point, after which the client will no longer be allowed to connect for a user configurable cool-down period.

The configuration is based on a policy where the administrator can set the amount of time for which clients are allowed to connect to the WiFi and reconnect type and value after which they will be allowed to connect back after they have been disconnected.

In order to create a new policy, go under **Clients→Time Policy** and add new one., then the following parameters:

Table 8: Time Policy Parameters

Option	Description
Name	Enter the name of the policy
Enabled	Check the box to enable the policy
Limit Client Connection Time	Sets amount of time a client may be connected.
Client Reconnect Timeout Type	Select the method with which we will reset a client's connection timer so they may reconnect again. Options are:

	• Reset Daily. • Reset Weekly. • Reset Hourly. • Timed Reset.
Client Reconnect Timeout	If 'Timed Reset' is selected, this is the period for which the client will have to wait before reconnecting.
Reset Day	If Reset Weekly is selected, this is the day the reset will be applied.
Reset Hour	If Reset Weekly or Reset Daily is select, this is the hour and day the reset will be applied.

Note: Time tracking shall be accounted for on a per-policy basis, such that a client connected to any SSID assigned the time tracking policy will accrue a common counter, regardless of which SSID they are connected to (as long as those SSIDs all share the same time tracking policy).

Banned Clients

Click on Banned Clients to view the list of the clients that have been banned after time disconnect feature has taken effect, these clients will not be allowed to connect back until timeout reset or you can unblock a client by clicking on the icon

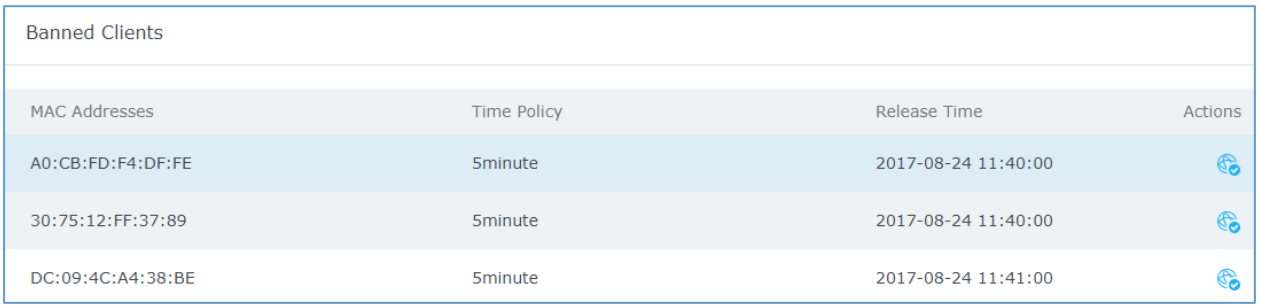

Figure 33: Ban/Unban Client

LED SCHEDULE

GWN7600LR Access Points series support also the LED schedule feature. This feature is used to set the timing when the LEDs are ON and when they will go OFF at customer's convenience.

This can be useful for example when the LEDs become disturbing during some periods of the day, this way with the LED scheduler, you can set the timing so that the LEDs are off at night after specific hours and maintain the Wi-Fi service for other clients without shutting down the AP.

To configure LED schedule, on the GWN7600LR WebGUI navigate to "**System Settings→LEDs**".

Following options are available:

Table 9: LEDs

Field	Description
LEDs Always Off	Configure whether to disable the AP LED dictator
Schedule Stop Hour	Configure the hour the AP LED dictator is disabled. The valid range is from 0 to 23. And the value cannot be empty.
Schedule Start Hour	Configure the minute the AP LED dictator is disabled. The valid range is from 0 to 59.
Schedule Stop Minute	Configure the hour the AP LED dictator is enabled. The valid range is from 0 to 23. And the value cannot be empty.
Schedule Start Minute	Configure the minute the AP LED dictator is enabled. The valid range is from 0 to 59.
Schedule Weekdays list of schedule days	Select the days the AP LED is desired to be disabled or enabled.

Following example on the next page sets the LEDs to be turned on from 8am till 8pm every day.

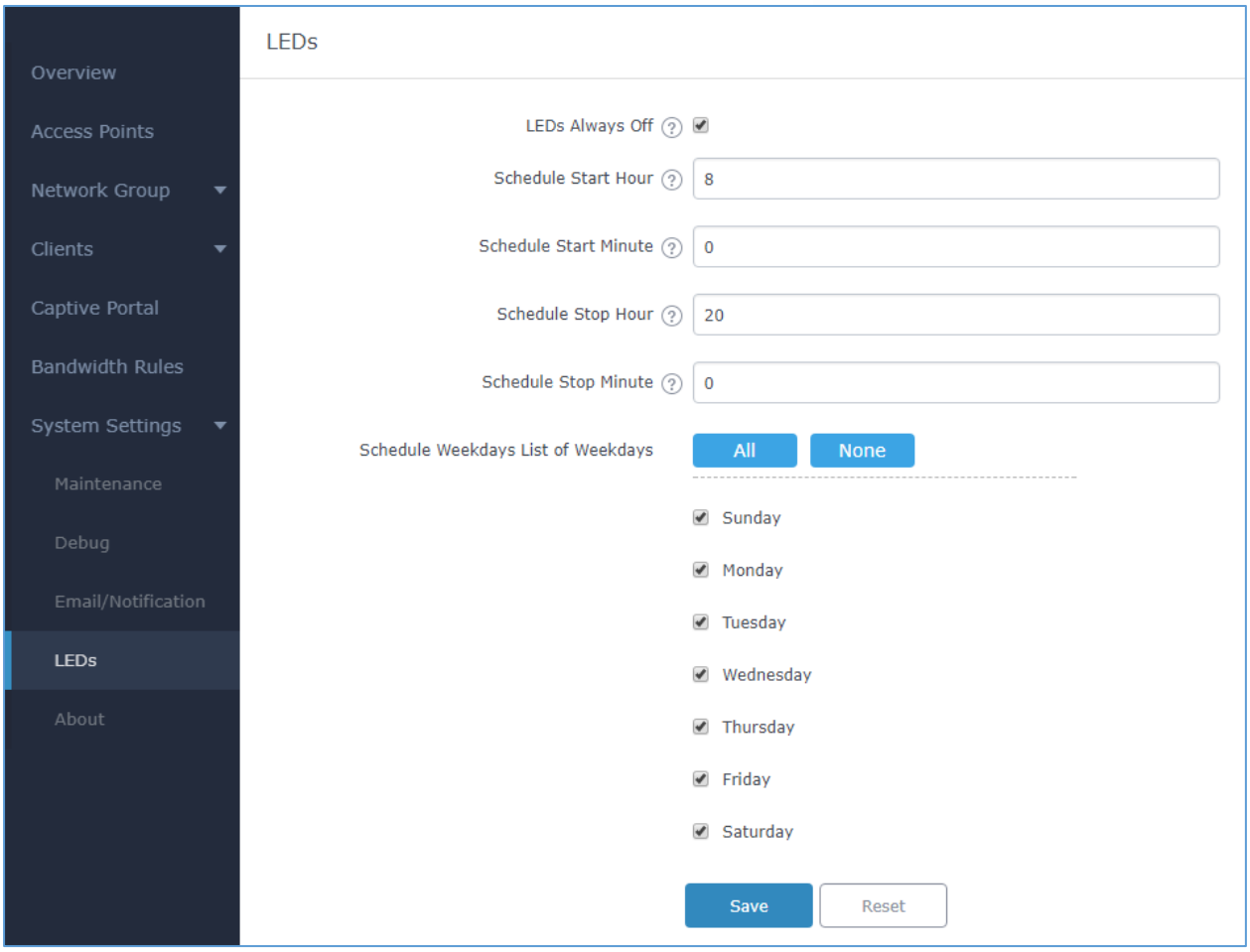

Figure 34: LED Scheduling Sample

CAPTIVE PORTAL

Captive Portal feature on GWN7600LR AP 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 GWN7600LR 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 GWN7600LR Web page under "Captive Portal". The page contains three tabs: **Policy**, **Files** and **Clients**.

Policy Configuration Page

The policy configuration page contains options for authentication type used when enabling the captive portal feature. The following table describes all the settings on this page:

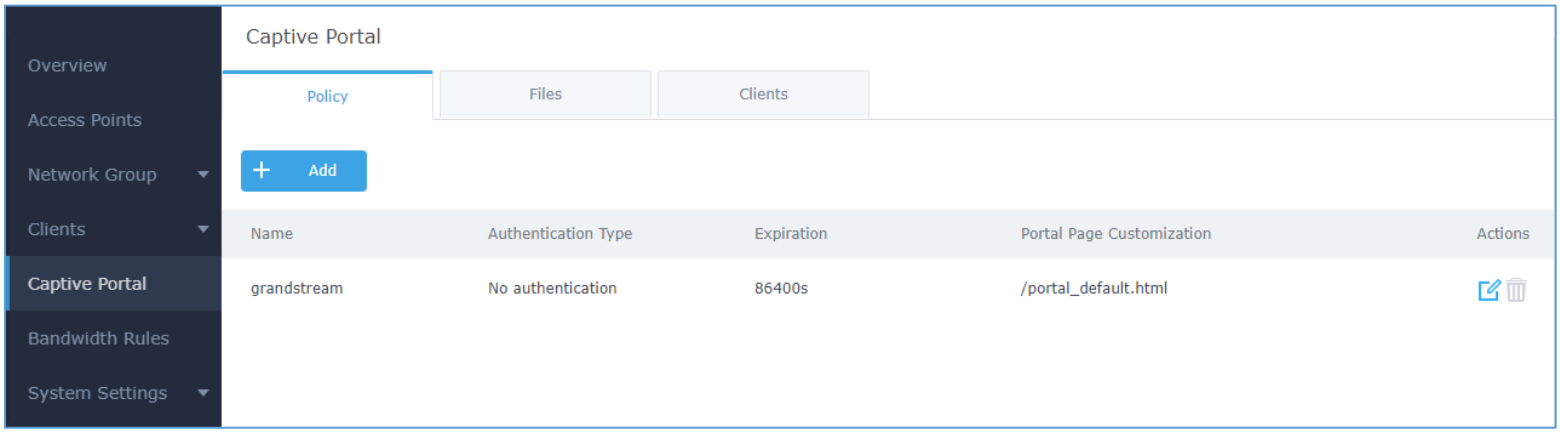

Figure 35: Captive Portal policy

- Click on to edit the policy.
- Click on to delete the policy.
- Click on Add to add a policy.

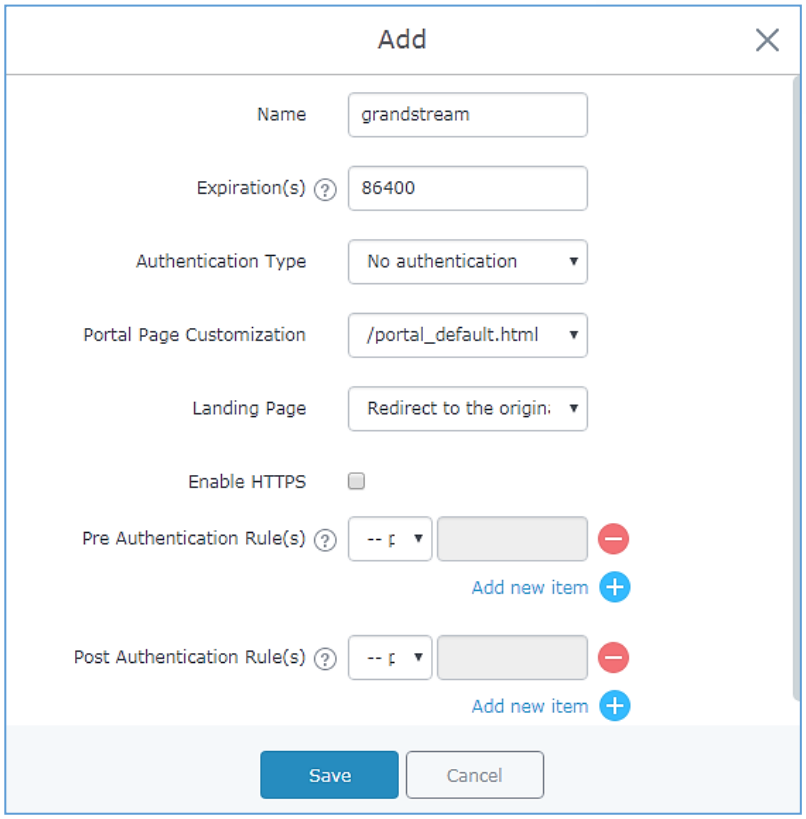

Figure 36: Add a new policy

Below table lists the items policy add page configures.

Table 10: Policy Add

Field	Description
Name	Enter the name of the Captive Portal policy
Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Authentication Type	Select an authentication type for the portal, 3 types are available: • **No Authentication:** When choosing this option, the landing page feature will not provide any type of authentication, instead it will prompt users to accept the license agreement to gain access to internet. • **RADIUS Server:** Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. • **Third party authentication:** Allows users to select either the WeChat authentication or Facebook authentication.
Radius Server Address	Enter the IP address or the FQDN of the RADIUS server used to authenticate clients.

Radius Server Port	Set the RADIUS server port, by default value is 1812.
Radius Server Secret	Enter the shared key between authenticator and RADIUS server.
Radius Authentication Method	Select the radius authentication method, 3 methods are available: PAP, CHAP and MS-CHAP.
WeChat Authentication	Check to enable/disable WeChat Authentication
Shop ID	Fill in the Shop ID that offers WeChat Authentication.
APP ID	Fill in the APP ID provided by the WeChat in its web registration page
SecretKey	Set the key for the portal, once clients want to connect to the WiFi, they should enter this key.
Facebook Authentication	Check to enable/disable Facebook Authentication
Facebook App ID	Fill in the Facebook App ID.
Facebook APP Key	Set the key for the portal, once clients want to connect to the WiFi, they should enter this key.
Portal Page Customization	Select the customized portal page.
Landing Page	Choose the landing page, 2 options are available: redirect to the origin and redirect to external page
Redirect External Page URL Address	Once the landing page redirects to external page, user should set the URL address for redirecting.
Enable HTTPS	Check to enable/disable HTTPS service.
Pre-Authentication Rule(s)	Set the Pre-Authentication Rules for temporarily release the IP or ports of the devices (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET)
Post Authentication Rule(s)	Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS)

Note:

Users could create multiple captive portal instances and assign the desired one for each network Group. 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 network group.

Files Configuration Page

Files configuration page allows users to view and upload HTML pages and related files (images…).
The captive portal uses two HTML pages using authentication scenarios, either **portal_default.html** which doesn't provide authentication, only accepting license agreement, while **portal_pass.html** provides textboxes for authentication, Wired or Wi-Fi clients will be redirected to one of these pages before accessing Internet. The following figure shows **portal_default.html** page:

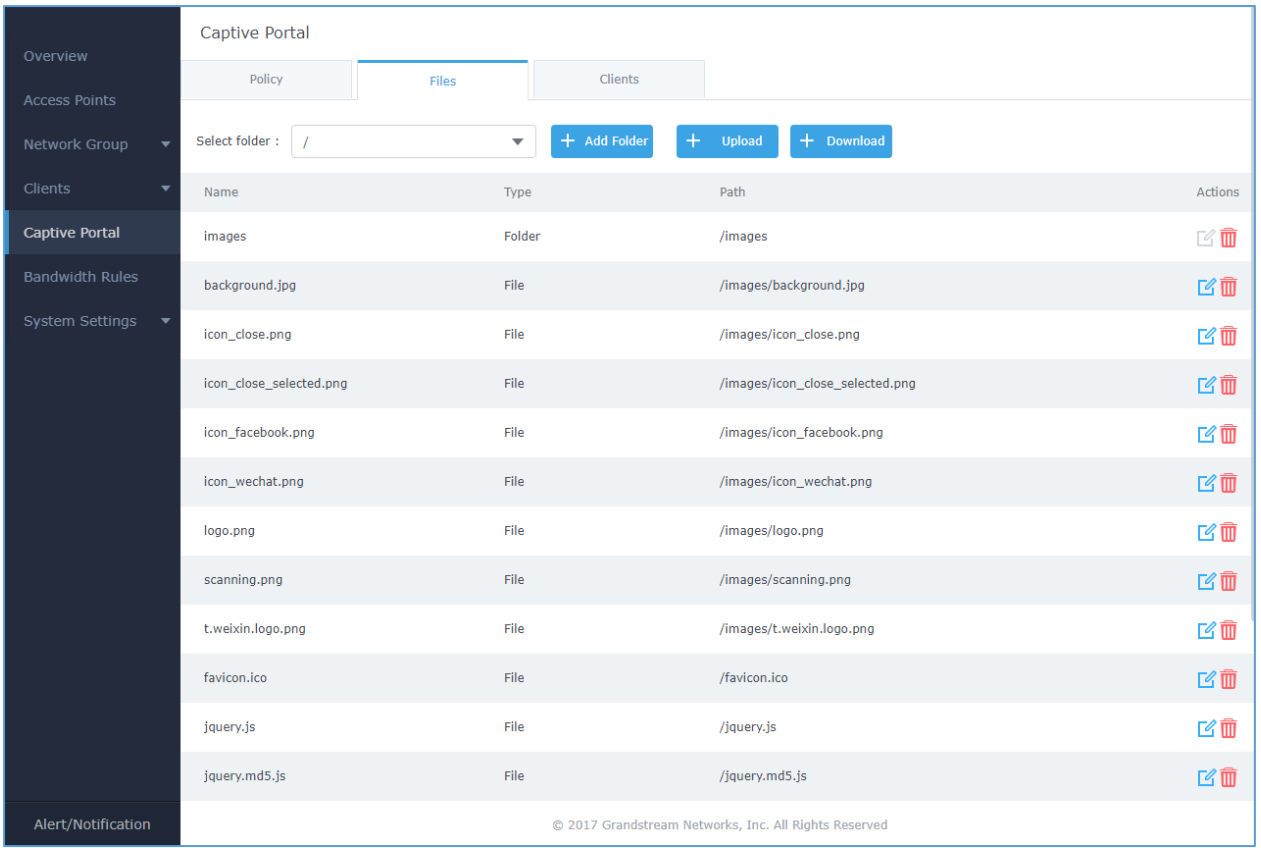

Figure 37: Captive Portal Files

- User can add folder in corresponding folder by selecting the folder and click on 

.
- Click on 

to upload a file from local device.
- Click on 

to download the files in Captive Portal folder.
- Click on  to edit the corresponding file, in another word, to replace the file with a new one.
- Click on  to delete the file.

Clients Page

This section lists the clients connected or trying to connect to Wi-Fi.

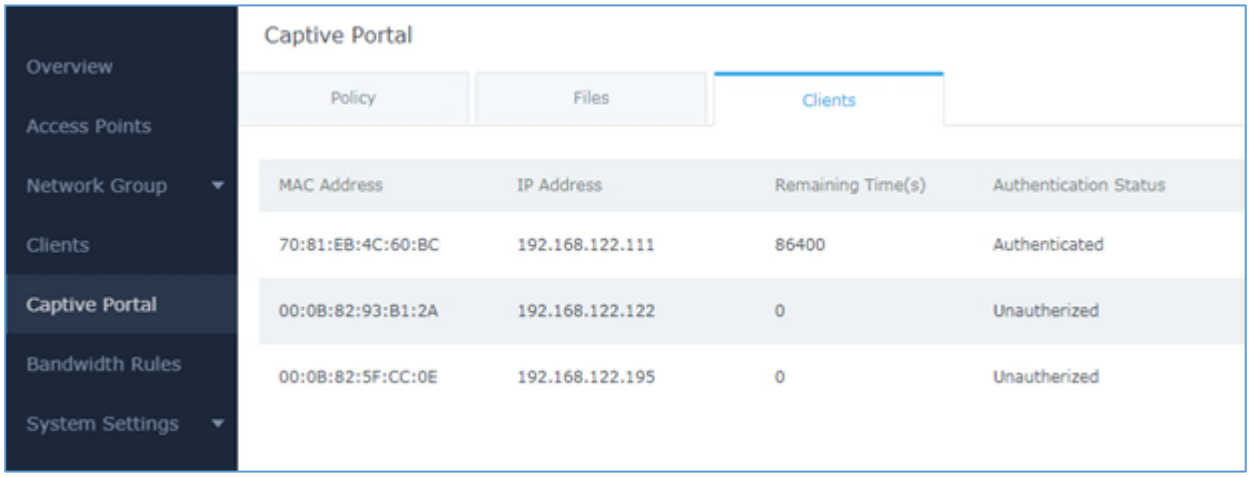

Figure 38: Captive Portal Clients

BANDWIDTH RULES

The bandwidth rule is a GWN7600LR feature that allows users to limit bandwidth utilization per SSID or client (MAC address or IP address).

This option can be configured from the GWN7600LR WebGUI under “Bandwidth Rules”.

Click 

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

Table 11: Bandwidth Rules

Field	Description
Type	Choose the type of rule to be applied on bandwidth utilization from the dropdown list, three options are available: • **SSID:** Set a bandwidth limitation on the SSID level. • **MAC:** Set a bandwidth limitation per MAC address. • **IP Address:** Set a bandwidth limitation per IP address.
SSID	Select the SSID to which the limitation will be applied, this option appears only when SSID type is selected.
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.
Network Group	Choose the network group to which belongs the device, this option is available when choosing either MAC or IP address type.
Upstream Rate	Specify the limit for the upload bandwidth using Kbps or Mbps.
Downstream Rate	Specify the limit for the download bandwidth using Kbps or Mbps.

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

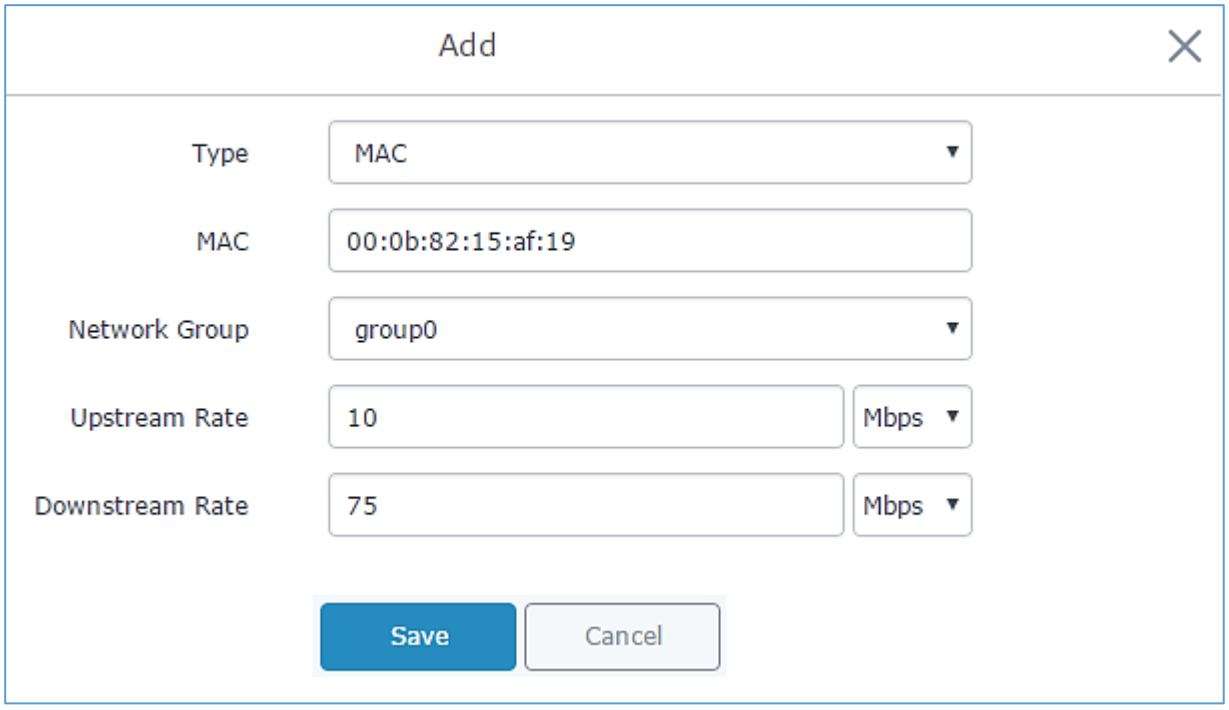

Figure 39: MAC Address Bandwidth rule

The following figure shows examples of bandwidth rules:

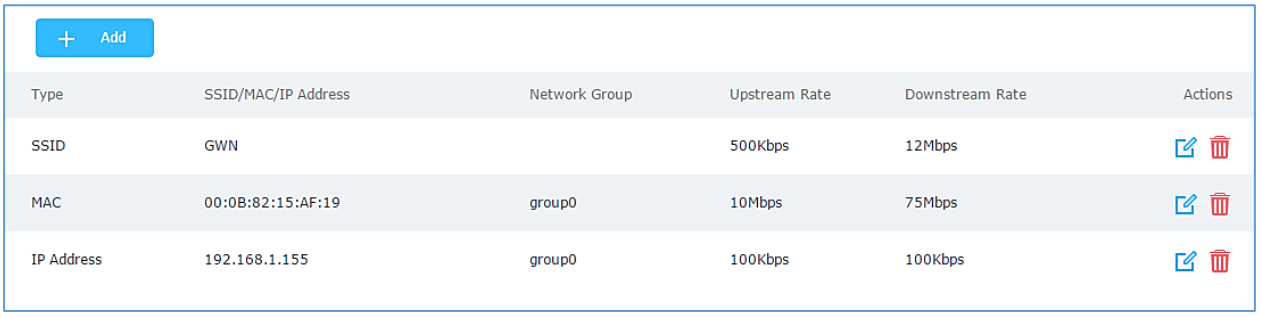

Figure 40: Bandwidth Rules

Note:

The same settings for bandwidth management are available from the following menus:

Per-SSID

Navigate on the web GUI under "Network Group→Add /Edit→WiFi" and you can set the Upstream and Downstream rate in Mbps.

Per-Client

Navigate on the web GUI under "Clients→Edit→Bandwidth Rules" where you can set the Upstream and Downstream rate in Mbps

SYSTEM SETTINGS

Maintenance

Users can access Maintenance page from GWN7600LR WebGUI→**System Settings→Maintenance**.

Basic

Basic page allows Country and Time configuration.

Table 12: Basic

Field	Description
Web HTTP Access	Enables Web HTTP Access. By default, it's disabled.
Web HTTPS Port	Specifies HTTPS port. By default, is 443.
Country	Select the country from the drop-down list. This can affect the number of channels depending on the country standards.
Time Zone	Configure time zone for the GWN7600LR. Make sure to reboot the device to take effect.
NTP Server	Configure the IP address or URL of the NTP server. The device will obtain the date and time from the configured server.
Date Display Format	Change the Date Display Format, three options are possible YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY

Upgrade

The Upgrade Web page allows upgrade related configuration.

Table 13: Upgrade

Field	Description
Authenticate Config File	Authenticate configuration file before acceptance. Default is disabled.
XML Config File Password	Enter the password for encrypting the XML configuration file using OpenSSL. The password is used to decrypt the XML configuration file if it is encrypted via OpenSSL.
Upgrade Via	Specify uploading method for firmware and configuration. 3 options are available: HTTP, HTTPS and TFTP.
Firmware Server	Configure the IP address or URL for the firmware upgrade server.
Config Server	Configure the IP address or URL for the configuration file server.
Check/Download New Firmware and config at Boot	Choose whether to enable or disable automatic upgrade and provisioning after reboot. Default is disabled.

Allow DHCP options 66 and 43 override	Configure whether to allow DHCP options 66 and 63 to override the upgrade and provisioning setting.
Automatic Upgrade	Specify the time to check for firmware upgrade (in minutes).
Upgrade Now	Click on Upgrade, to launch firmware/config file provisioning. Please make sure to Save and Apply changes before clicking on Upgrade.
Download Configuration	Click on Download to download the device's configuration file.
Upload Configuration	Select a compressed config file to restore the device previous configuration, after upload successfully, the device will reboot automatically.
Reboot	Click on Reboot button to reboot the device.
Factory Reset	Click on Reset to restore the GWN7600LR to factory default settings

Access

The access Web page provide configuration for admin and user password.

Table 14: Access

Field	Description
Current Administrator Password	Enter the current administrator password
New Administrator Password	Change the current password. This field is case sensitive with a maximum length of 32 characters.
Confirm New Administrator Password	Enter the new administrator password one more time to confirm.
User Password	Configure the password for user-level Web GUI access. This field is case sensitive with a maximum length of 32 characters.
User Password Confirmation	Enter the new User password again to confirm.

Syslog

The syslog Web page provides configuration settings for syslog.

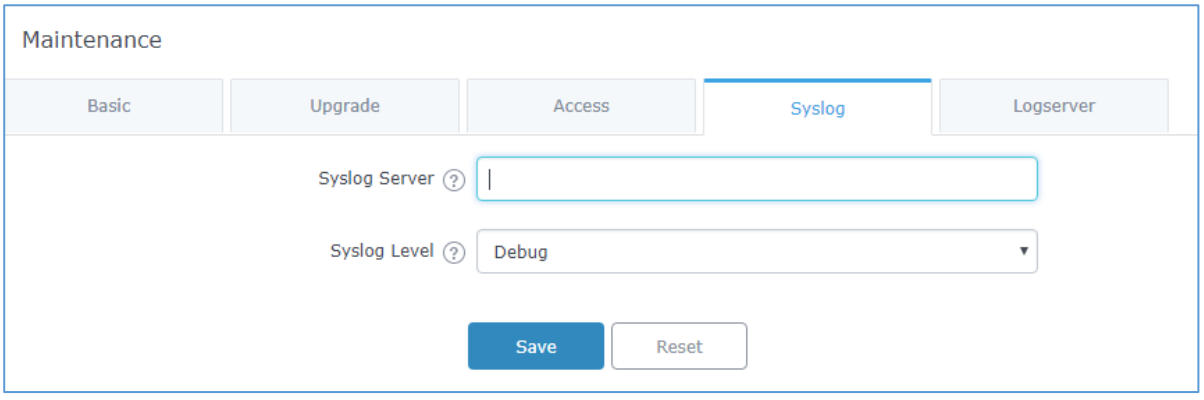

Figure 41: Syslog Server Page

Table 15: Syslog

Field	Description
Syslog Server	Enter the IP address or URL of Syslog server. Please reboot the GWN7600LR to take effect.
Syslog Level	Select the level of Syslog, 5 levels are available: **None, Debug, Info, Warning** and **Error**. Please reboot the GWN7600LR to take effect.

Debug

GWN7600LR offers many features for managing and monitoring connected clients to network groups, as well as debugging and troubleshooting

Core Files

The Core Files Web page displays core dumps generated when the GWN7600LR crashes. This is helpful for troubleshooting purposes, if any core dump found on this page please help to contact our support team for further investigation using following link: https://helpdesk.grandstream.com/

Ping/Traceroute

Ping and Traceroute are useful debugging tools to verify reachability with other clients across the network. The GWN7600LR offers both Ping and Traceroute tools for IPv4 and IPv6 protocols.

To use these tools, go to GWN7600LR WebGUI→**System Settings**→**Debug** and click on **Ping/Traceroute.**

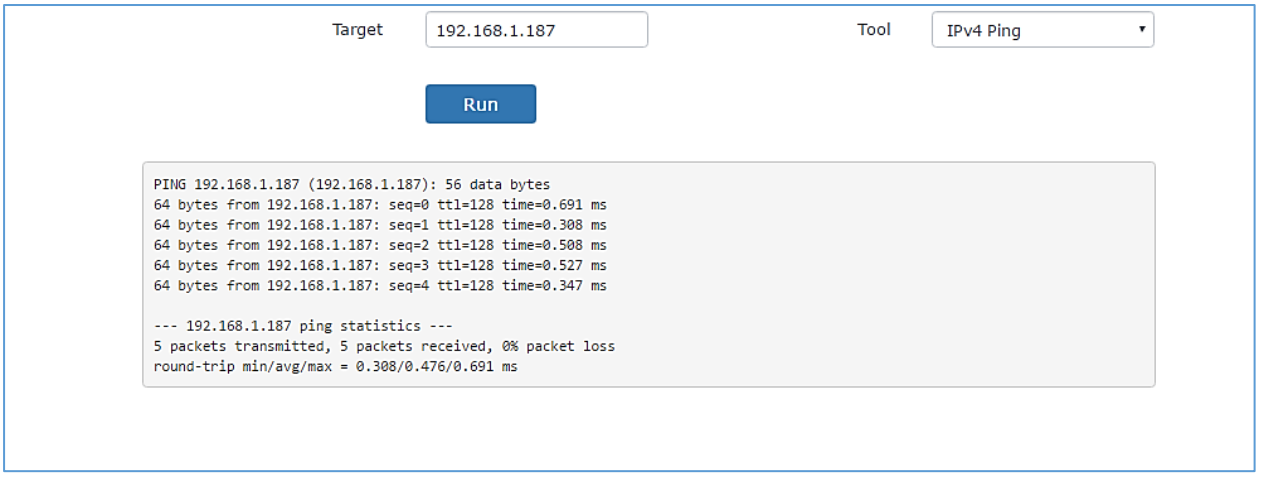

Figure 42: IP Ping

- Next to **Tool** choose from the dropdown menu:
  - IPv4 Ping for an IPv4 Ping test to Target
  - IPv6 Ping for an IPv6 Ping test to Target
  - IPv4 Traceroute for an IPv4 Traceroute to Target
  - IPv6 Traceroute for an IPv6 Traceroute to Target

- Type in the destination's IP address in **Target** field.
- Click on **Run**.

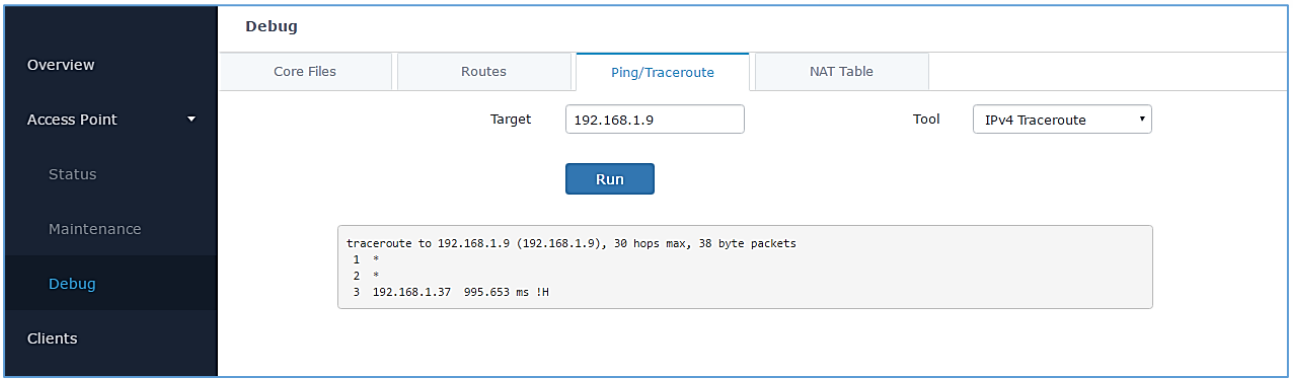

Figure 43: IP Traceroute

Syslog

The syslog Web page displays logs generated by the GWN7600LR for troubleshooting purpose as shown in figure below.

Syslog messages are also displayed in real time under Web GUI→**System Settings→Debug→Syslog.**

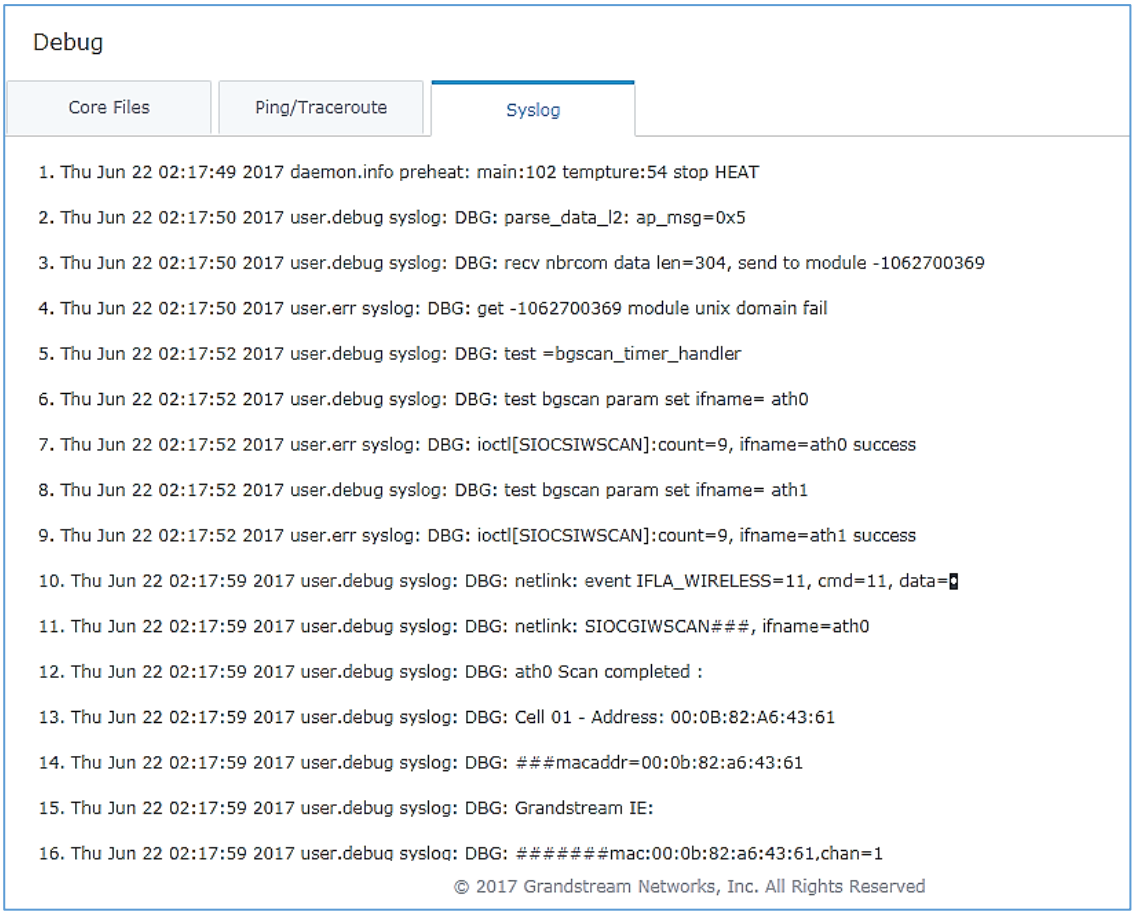

Figure 44: Syslog

Email/Notification

The Email/Notification page allows the administrator to select a predefined set of system events and to send notifications upon the change of the set events.

Note:
A reboot is required in order to activate email notification feature.

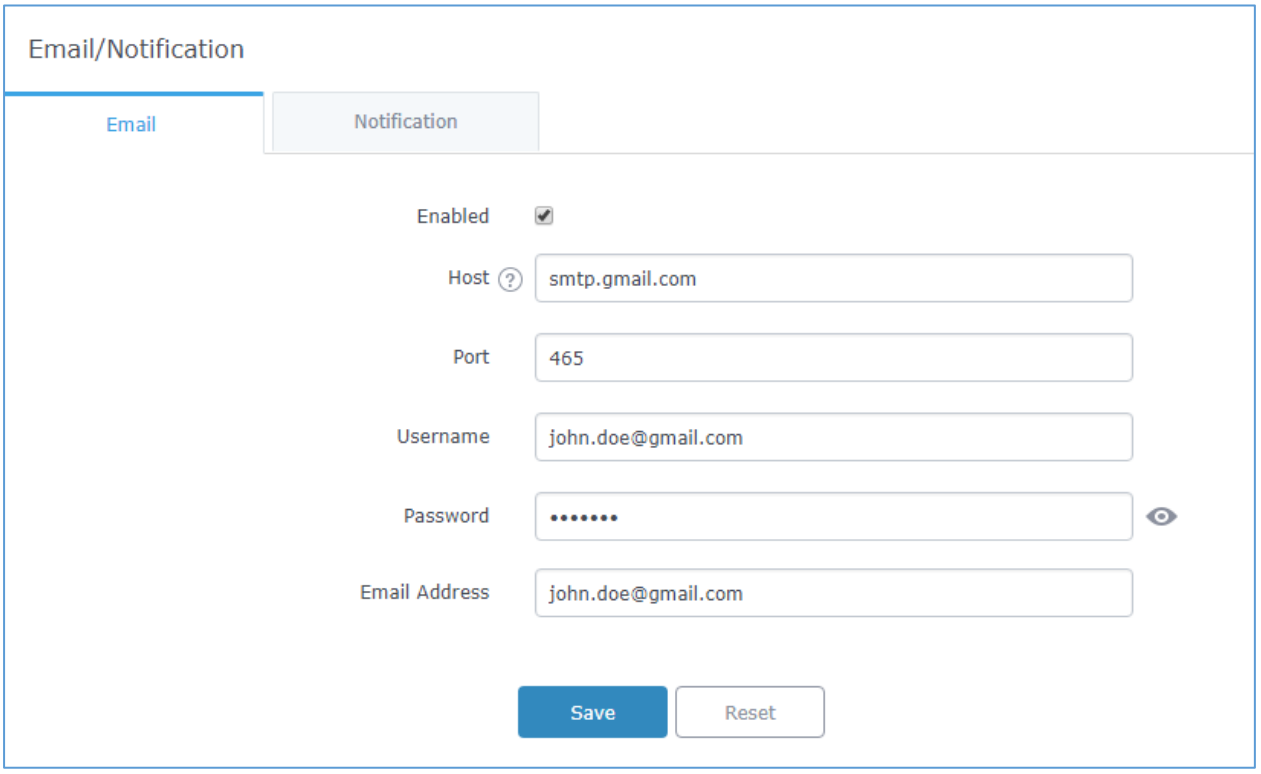

Figure 45: Email

Table 16: Email Setting

Filed	Description
Enabled	Enable/disable the email settings. By default, it's disabled
Host	Configures the SMTP Email Server IP or Domain Name.
Port	Specifies the Port number used by server to send email.
Username	Specifies sender's User ID or account ID in the email system used.
Password	Specifies sender's password of the email account.
Email Address	Specifies the email address of the administer where to receive notifications.

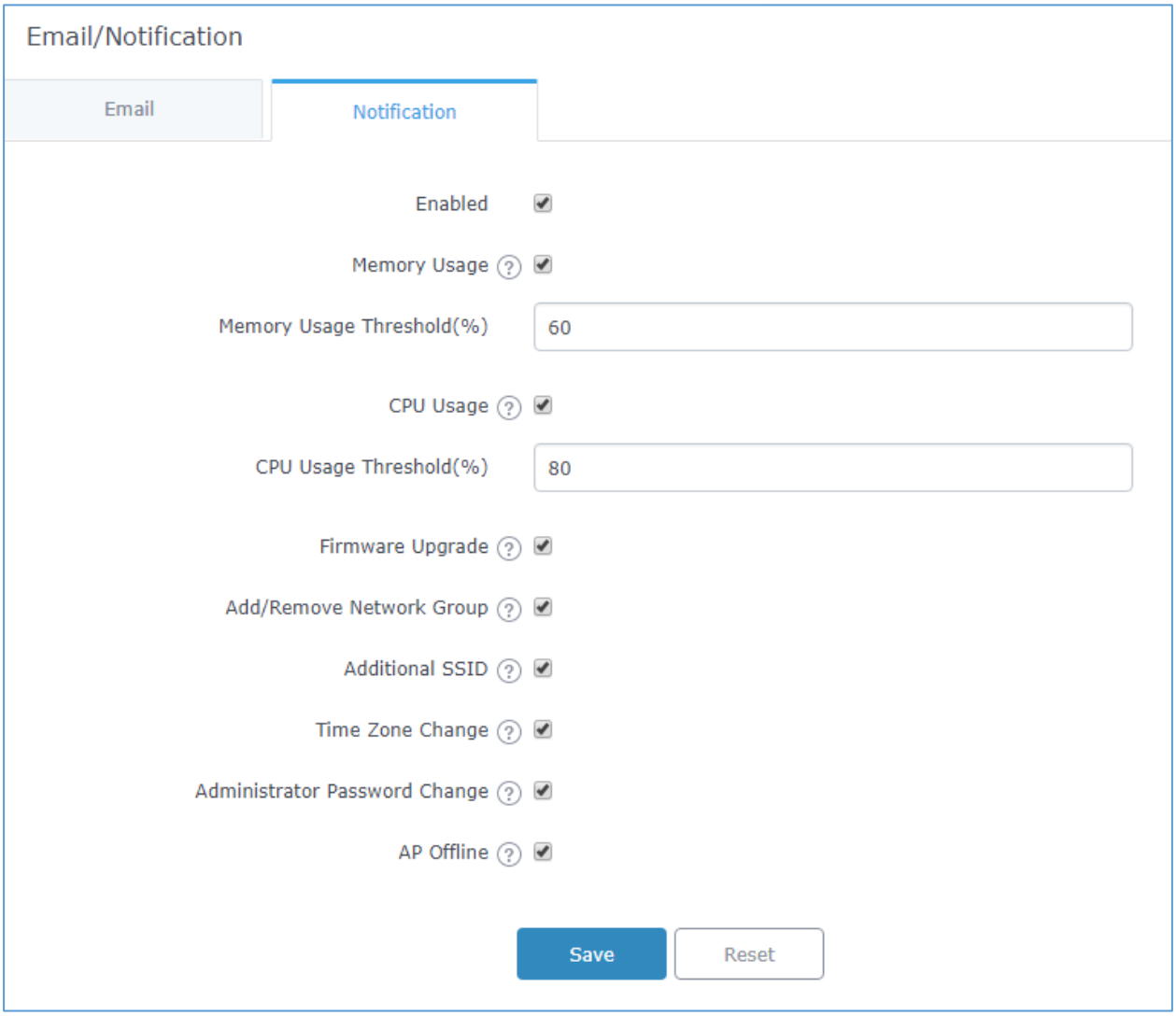

Figure 46: Notification

The following table describe the notifications configuration settings.

Table 17: Email Events

Filed	Description
Enabled	Enable/disable the notification. By default, it's disabled
Memory Usage	Configures whether to send notification if memory usage is greater than the configured threshold. By default, it's disabled.
Memory Usage Threshold (%)	Specifies the Memory Usage Threshold (%). Must be integer between 1 and 100.
CPU Usage	Configures whether to send notification if CPU usage is greater than the configured threshold. By default, it's disabled.

CPU Usage Threshold (%)	Specifies the CPU Usage Threshold (%). Must be integer between 1 and 100.
Firmware upgrade	Configures whether to send notification on firmware upgrade. Default is disabled.
Add/Remove Network Group	Configures whether to send notification when network groups has been added/removed.
Additional SSID	Configures whether to send notification if any additional SSID is enabled. Default is disabled.
Time Zone Change	Configures whether to send notification on time zone change. Default is disabled.
Administrator Password Change	Configures whether to send notification on admin password change. Default is disabled.
AP Offline	Configures whether to send notification when AP going offline. Default is disabled.

UPGRADING AND PROVISIONING

Upgrading Firmware

The GWN7600LR can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN7600LR.

Upgrading via Web GUI

The GWN7600LR can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:
firmware.grandstream.com/BETA
192.168.5.87

The upgrading configuration can be accessed via **Web GUI→System Settings→Maintenance→Upgrade**.

Table 18: Network Upgrade Configuration

Upgrade Via	Allow users to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
Firmware Server	Define the server path for the firmware server.
Check Update on Boot	Allows the device to check if there is a firmware from the configured firmware server at boot.
Automatic Upgrade check interval(m)	Set the value for automatic upgrade check in minutes.
Upgrade Now	Click on Upgrade button to begin the upgrade. Note that the device will reboot after downloading the firmware.

Upgrading Slave Access Points

When the GWN7600LR is being paired as slave using another GWN7600LR acting as Master Access Point Controller, users can upgrade their paired access points from the GWN7600LR acting as Master Access Point Controller.

To upgrade a slave access point, log in to the GWN7600LR Controller and go to **Access Points.**

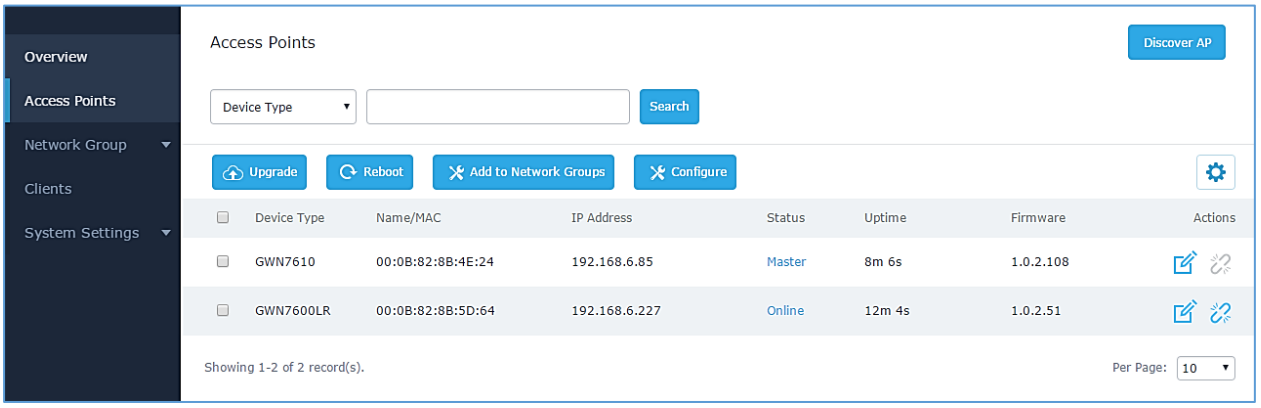

Figure 47: Access Points

Make sure that firmware server path is set correctly under Maintenance, and click on 

to upgrade all selected access points.

The status of the device will show Upgrading, wait until it finishes and reboots, then it will appear online again.

Note:

- Please do not interrupt or power cycle the GWN7600LR during upgrading process.
- The Master Access Point needs to be upgraded from **Web GUI→System Settings→Maintenance.** It cannot be upgraded from Access Points page like the Paired Access Points.

Service providers should maintain their own firmware upgrade servers. For users who do not have TFTP/HTTP/HTTPS server, some free windows version TFTP servers are available for download from
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
http://tftpd32.jounin.net

Please check our website at http://www.grandstream.com/support/firmware for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the GWN7600LR to the same LAN segment;
3. Launch the TFTP server and go to the File menu→**Configure→Security** to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the GWN7600LR web configuration interface;
5. Configure the Firmware Server to the IP address of the PC;
6. Update the changes and reboot the GWN7600LR.

End users can also choose to download a free HTTP server from http://httpd.apache.org/ or use Microsoft IIS web server.

Provisioning and backup

The GWN7600LR configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GWN7600LR when necessary.

Download Configuration

Users can download the GWN7600LR configurations for restore purpose under **Web GUI→System Settings→Maintenance→Upgrade**

Click on Download to download locally the configuration file.

Configuration Server

Administrators can download and provision the GWN7600LR by putting the config file on a TFTP/HTTP or HTTPS server, and set Config Server to the TFTP/HTTP or HTTPS server used for the GWN7600LR to be provisioned with that config server file.

Reset and reboot

Administrators could perform a reboot and reset the device to factory functions under **Web GUI→System Settings→Maintenance→Upgrade** by clicking on Reboot button.

Reset Will restore all the GWN7600LR itself to factory settings.

EXPERIENCING THE GWN7600LR WIRELESS ACCESS POINT

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 purchasing Grandstream GWN7600LR Wireless Access Point, it will be sure to bring convenience and color to both your business and personal life