Grandstream Networks, Inc.

GWN7600/GWN7600LR

Mid-Tier/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.

WARNING

Please do not use a different power adaptor with devices as it may cause damage to the products and void the 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.
- Consult the dealer or an experienced radio/TV technician for help.

GNU GPL INFORMATION

GWN7600/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 GWN7600/GWN7600LR via Web GUI in standalone mode, with other GWN76XX Access Points 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 "GWN7600/GWN7600LR/GWN7600/GWN7600LR User Manual".

This guide covers following topics:

CHANGE LOG

This section documents significant changes from previous versions of the GWN7600/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 1.0.6.41

- Added date time display on Overview Page. [Overview Page]
- Added new feature scheduling module. [SCHEDULE]
- Added possibility to print/delete multiple vouchers. [VOUCHERS]
- Added expiration period to vouchers. [VOUCHERS]
- Added DHCP Server. [DHCP Sever]
- Added support for GWN.Cloud [GWN.CLOUD]
- Added support for Transfer AP and Transfer Network Group.[Transfer AP – Transfer Network Group]
- Added support for Outdoor/Indoor Scene WiFi channel configuration (Applicable for GWN7600LR Only). [Scene]

Firmware Version 1.0.5.13

- Added support for Sequential Upgrade [Sequential Upgrade]
- Added support for Feature Scheduling [SCHEDULE]
- Added support for Master Transfer [Transfer to Master]
- Added support for Airtime Fairness [Airtime Fairness]
- Added support for Social login/Voucher [VOUCHERS]
- Added support for Mesh Network [MESH NETWORK]

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

- No major changes.

Firmware Version 1.0.3.19

- Added support for captive portal [CAPTIVE PORTAL]
- Added support for 802.11k/r/v [Enable Voice Enterprise]
- Added support for failover master [Failover Master]
- Added support for VLAN assignment via RADIUS [Dynamic Vlan]
- Added support for Select SSID Band [SSID Band]
- Added support for Exact Radio Power Configuration in dBm [Custom Wireless Power]
- Added support for AP Location [AP Location]
- Added support for Per-Client/Per-SSID bandwidth rules [BANDWIDTH RULES]
- Added option to limit clients count per SSID [Wireless Client Limit]
- Added support for WiFi Schedule [SCHEDULE]
- Added support for LED control [LED SCHEDULE]
- Added option to enable/disable DHCP option 66 & 43 override [DHCP options 66 and 43 override]

Firmware Version 1.0.1.31

- This is the initial version.

WELCOME

Thank you for purchasing Grandstream GWN7600/GWN7600LR Enterprise Wireless Access Point. The GWN7600 is a mid-tier Wave-2 802.11ac WiFi access point for small to medium sized businesses, multiple floor offices, commercial locations and branch offices. The GWN7600LR Outdoor Long-range 802.11ac Wave-2 Wi-Fi 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 GWN7600/GWN7600LR come equiped with dual-band, 2x2:2 MU-MIMO with beam-forming technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range for both Indoor (GWN7600) and Outdoor deployement (GWN7600LR).

To ensure easy installation and management, the GWN7600/GWN7600LR uses a controller-less distributed network management design in which the controller is embedded 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. This wireless access point can be paired with any third party routers as well as Grandstream GWN series routers. With support for advanced QoS, low-latency real-time applications, 450+ concurrent client devices per AP and dual Gigabit network ports with PoE, the GWN7600/GWN7600LR is an ideal WiFi access point for medium wireless network deployments with medium-to-high user density.

⚠ **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: GWN7600 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)
Antennas	2x 2.4 GHz, gain 3 dBi, internal antenna 2x 5 GHz, gain 3 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 877 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 300 Mbps; 400 Mbps 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, 2x2:2 5GHz
Coverage Range	Up to 541ft. (165 meters) for GWN7600. *Coverage range can vary based on environment
Maximum TX Power	5G: 22dBm 2.4G: 22dBm *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; 80.11n 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
BSSID	16 SSIDs per radio
Concurrent Clients	450+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x USB 2.0 port, 1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	multi-color LEDs 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 GWN7600 allows it to auto-discover, auto-provision and manage up to 30 GWN76XX in a network
Power and Green Energy Efficiency	DC Input: 24VDC/1A Power over Ethernet (802.3af) compliant Maximum Power Consumption: 13.8W
Temperature & Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3 x 205.3 x 45.9mm; Unit Weight: 526g Unit + Mounting Kits Dimension: 205.3 x 205.3 x 53.9mm; Unit + Mounting Kits Weight : 610g Entire Package Dimension: 228.5*220*79mm; Entire Package Weight: 854g
Package Content	GWN7600 Wave-2 802.11ac Wireless AP, Mounting Kits, Quick Installation Guide
Compliance	FCC, CE, RCM, IC

Table 2: 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	multicolor 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 GWN7600/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 GWN7600/GWN7600LR.

Equipment Packaging

Table 3: GWN7600 Equipment Packaging

Main Case	Yes (1)
Mounting Bracket	Yes (1)
Ceiling Mounting Bracket	Yes (1)
Plastic Expansion Bolt	Yes (3)
M3 NUT	Yes (3)
Screw (PM 3 x 50)	Yes (3)
Screw (PM 3.5 x 20)	Yes (3)
Quick Installation Guide	Yes (1)
GPL License	Yes (1)

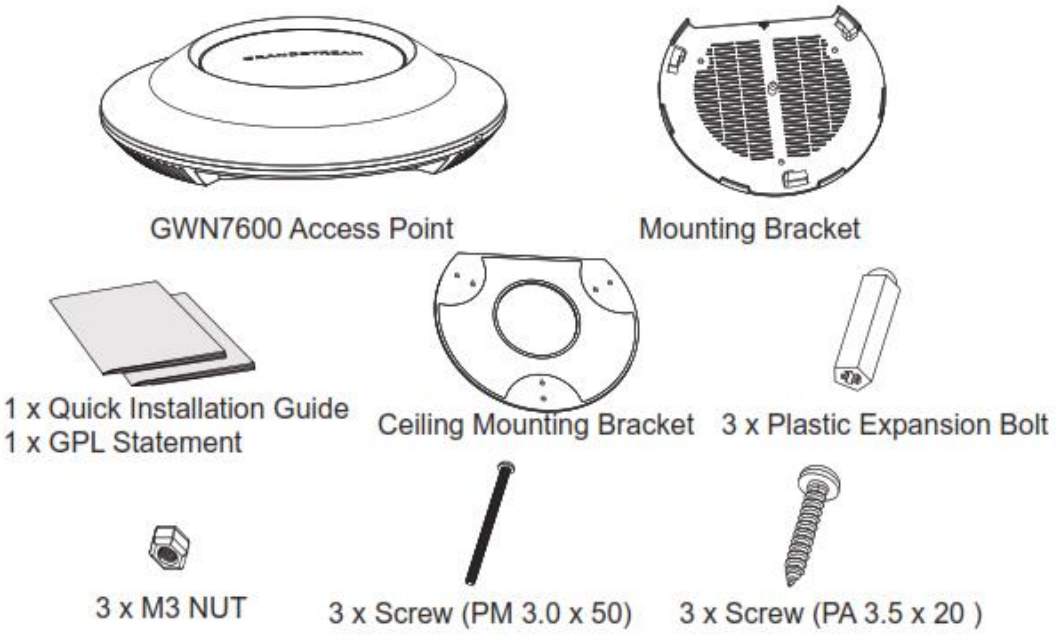


Figure 1: GWN7600 Equipment Package

Below is the equipment packaging for GWN7600LR model.

Table 4: 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)

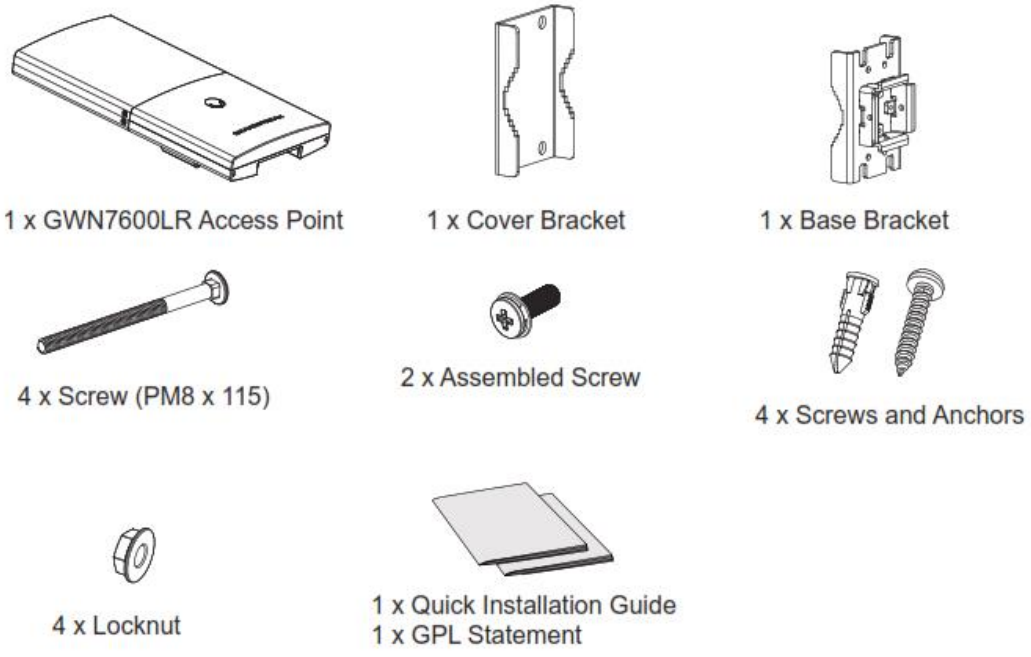


Figure 2: GWN7600LR Equipment Package

GWN7600/GWN7600LR Access Point Ports

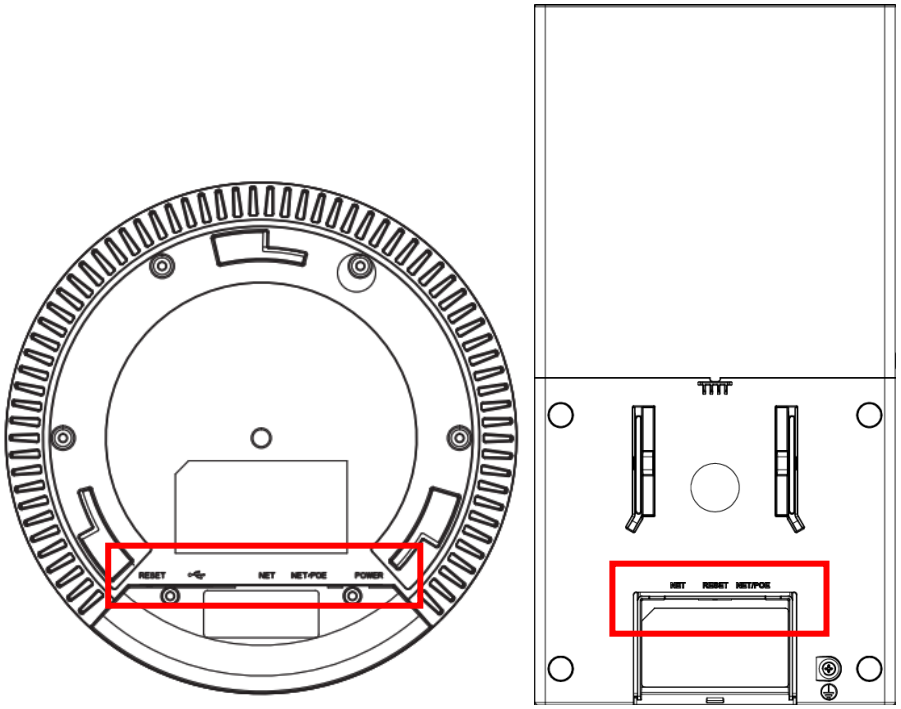


Figure 3: GWN7600 & GWN7600LR Ports

Table 5: GWN7600 Ports Description

Port	Description
Power	Power adapter connector (24V, 1A)
NET/PoE	Ethernet RJ45 port (10/100/1000Mbps) supporting PoE (802.3af).
NET	Ethernet RJ45 port (10/100/1000Mbps) to your router or another GWN76xx series
	USB 2.0 port (for future IOT & location-based applications)
RESET	Factory reset button. Press for 7 seconds to reset factory default settings.

Table 6: 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 GWN7600/GWN7600LR Access Point

Step 1:

Connect one end of a RJ-45 Ethernet cable into the NET or PoE/NET port of the GWN7600/GWN7600LR.

Step 2:

Connect the other end of the Ethernet cable(s) into a LAN port to your Network.

Step 3:

For GWN7600 only, connect the 24V DC power adapter into the power jack on the back of the access point Insert the main plug of the power adapter into a surge-protected power outlet. Otherwise PoE can be used if the switchport does provide PoE power.

Note: GWN7600/GWN7600LR can be powered using PoE (802.3af) switch via PoE/NET port. In this case, both power and network connectivity will be provided over the PoE/NET port.

Step 4:

Wait for the GWN7600/GWN7600LR to boot up and acquire an IP address from the DHCP Server.

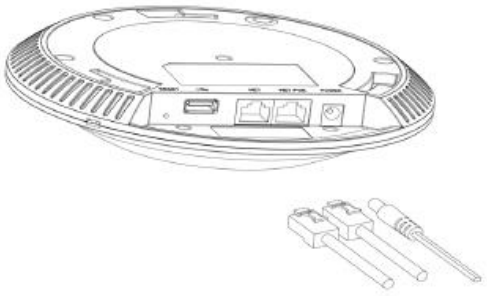


Figure 4: Connecting GWN AP - GWN7600 as example

Warranty

If the GWN7600/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.

Wall and Ceiling Mount Installation for GWN7600

GWN7600 can be mounted on the wall or ceiling, please refer to the following steps for the appropriate installation.

Wall Mount

Step1:

Position the mounting bracket at the desired location on the wall with the arrow pointing up.

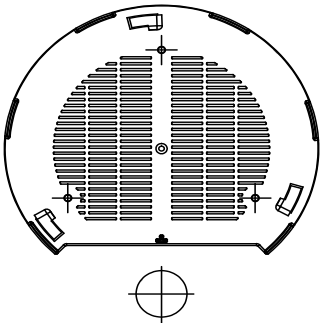


Figure 5: Wall Mount – Steps 1 & 2

Step 2:

Use a pencil to mark the four mounting holes (screw holes DIA 5.5mm, reticle hole DIA 25mm).

Step 3:

Insert screw anchors into the 5.5 mm holes. Attach the mounting bracket to the wall by inserting the screws into the anchors.

Step 4:

Connect the power cable and the Ethernet cable (RJ45) to the correct ports of your GWN7600.

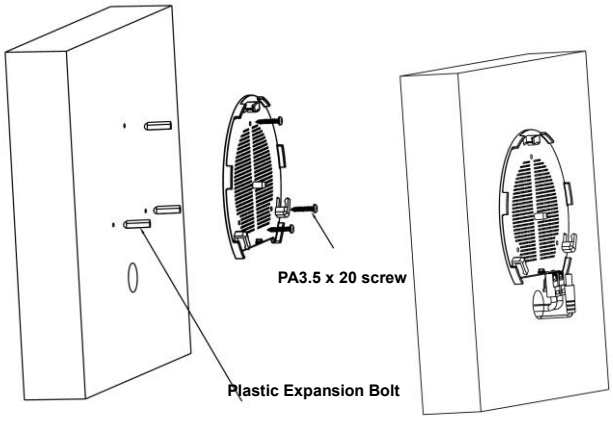


Figure 6: Wall Mount – Steps 3 & 4

Step 5:

Align the arrow on the GWN7600 AP with the arrow on the locking tab of the mounting bracket and ensure that your GWN is firmly seated on the mounting bracket.

Step 6:

Turn the GWN clockwise until it locks into place and fits the locking tab.

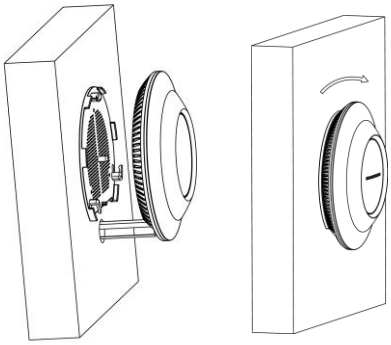


Figure 7: Wall Mount – Steps 5 & 6

Ceiling Mount

Step 1:

Remove the ceiling tile.

Step 2:

Place the ceiling backing plate in the center of the ceiling tile and mark the mounting screw holes (screw holes DIA 5.5mm, reticle hole DIA 25mm).

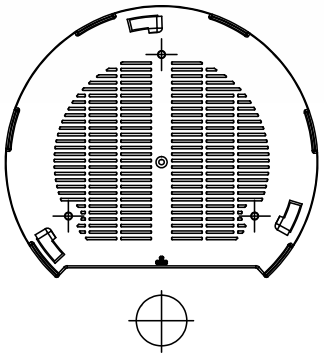


Figure 8: Ceiling Mount – Steps 1 & 2

Step 3:

Insert the screws through the mounting bracket.

Step 4:

Connect the power cable and the Ethernet cable (RJ45) to the correct ports of your GWN7600.

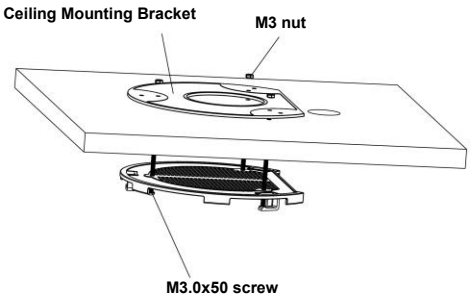


Figure 9: Ceiling Mount – Step 3

Step 5:

Align the arrow on the GWN7600 AP with the arrow on the locking tab of the mounting bracket and ensure that your GWN is firmly seated on the mounting bracket and connect the network and power cables.

Step 6:

Turn the GWN clockwise until it locks into place and fits the locking tab.

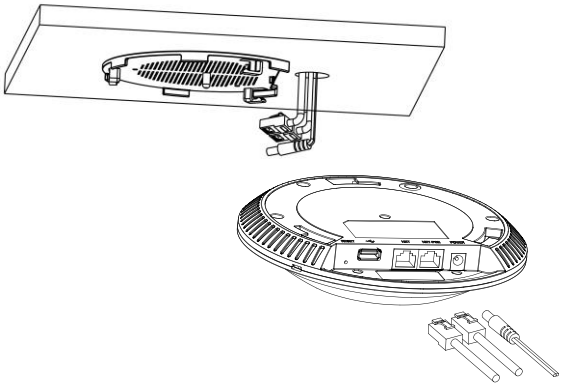


Figure 10: Ceiling Mount – Step 4

⚠ **Note:**

Ceiling mounting is recommended for optimal coverage performance.

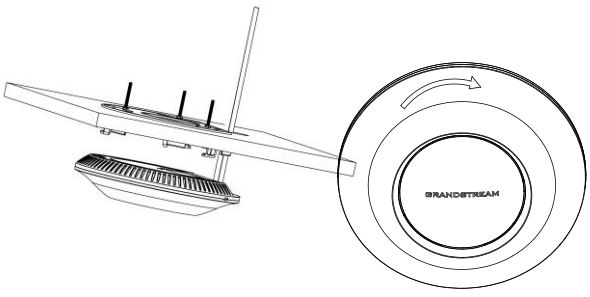


Figure 11: Ceiling Mount – Steps 5 & 6

Mounting Instructions for GWN7600LR

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.

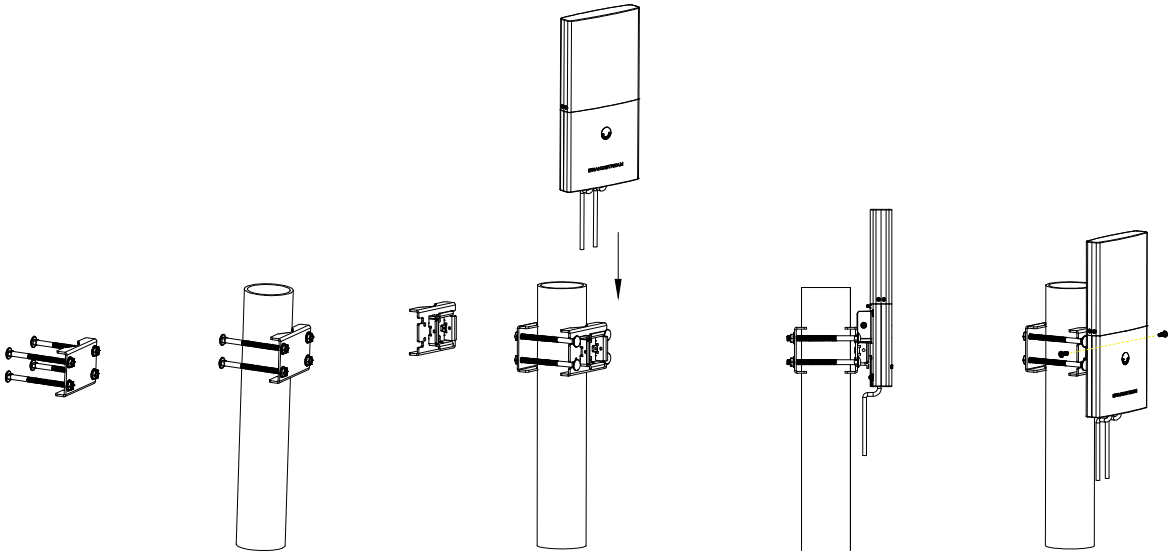


Figure 12: GWN7600LR Vertical Mounting

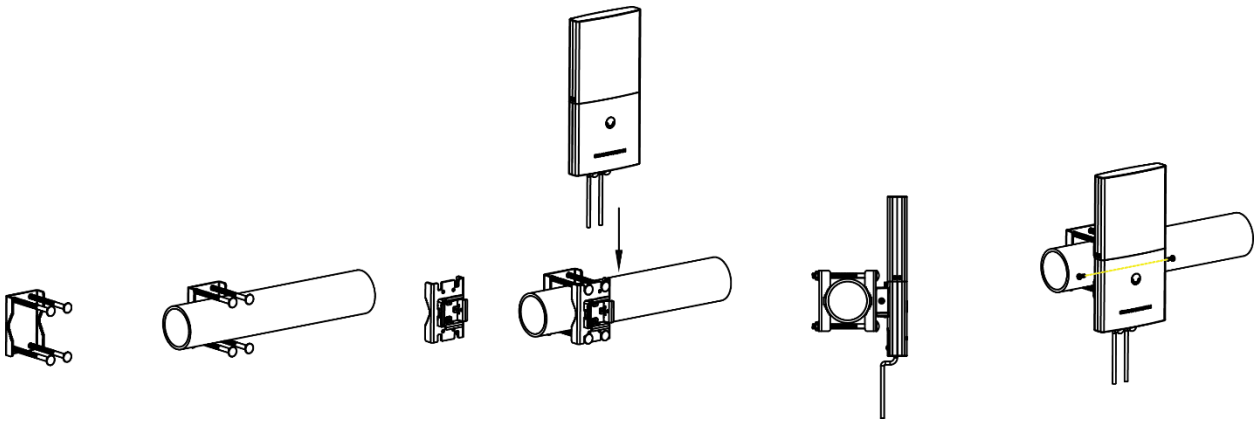


Figure 13: GWN7600LR Horizontal Mounting

GETTING STARTED

The GWN7600/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 GWN7600/GWN7600LR's setup.

This section provides step-by-step instructions on how to read LED patterns, discover the GWN7600/GWN7600LR and use its Web GUI interface.

LED Patterns

The panel of the GWN7600/GWN7600LR has different LED patterns for different activities, to help users read the status of the GWN7600/GWN7600LR whether it's powered up correctly, provisioned, in upgrading process and more, for more details please refer to the below table.

Table 7: LED Patterns

LED Status	Indication
OFF	Unit is powered off or abnormal power supply.
Blinking green	Firmware update in progress.
Solid green	Firmware update successful.
Blinking red	Delete slave paring
Solid red	Firmware update failed.
Blinking pink	Unit not provisioned.
Solid pink	Unit not paired
Blinking blue	Unit provisioning in progress.
Solid blue	Unit is provisioned successfully.
Blinking White	Used for Access Point location feature

Discover the GWN7600/GWN7600LR

Once the GWN7600/GWN7600LR is powered up and connected to the Network correctly, users can discover the GWN7600/GWN7600LR using one of the below methods:

Method1: Discover the GWN7600/GWN7600LR using its MAC address

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. From a computer connected to same Network as the GWN7600/GWN7600LR, type in the following address using the GWN7600/GWN7600LR's MAC address on your browser https://gwn_<mac>.local
   For example, if a GWN7600/GWN7600LR has the MAC address **00:0B:82:8B:58:30**, this unit can be accessed by typing https://gwn_000b828b5830.local/ on the browser.

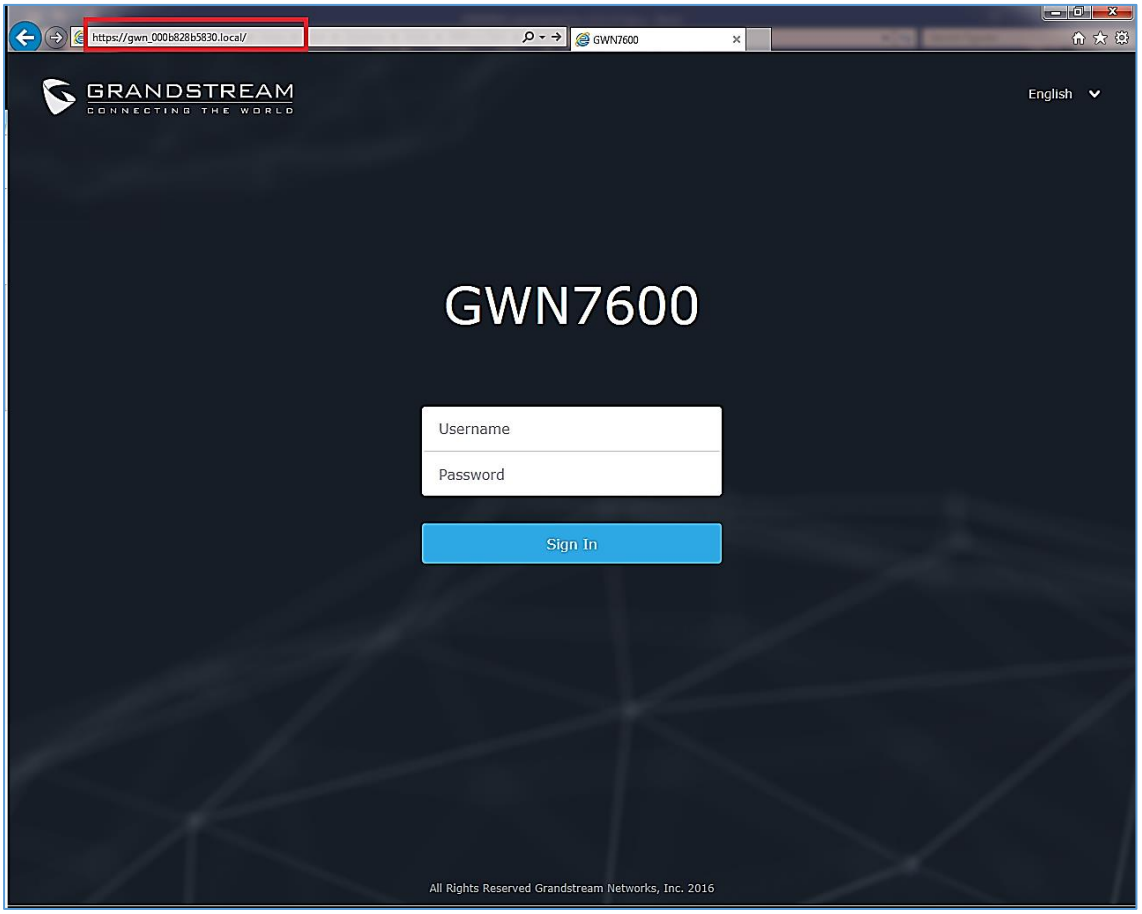


Figure 14: Discover the GWN7600/GWN7600LR using its MAC Address

Method 2: Discover the GWN7600/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, click on **Select** to define the network interface, then click on **Scan**.
3. The tool will discover all GWN7600/GWN7600LR Access Points connected on the network showing their MAC, IP addresses and firmware version.
4. Click on **Manage Device** to be redirected directly to the GWN7600/GWN7600LR's configuration interface, or type in manually the displayed IP address on your browser.

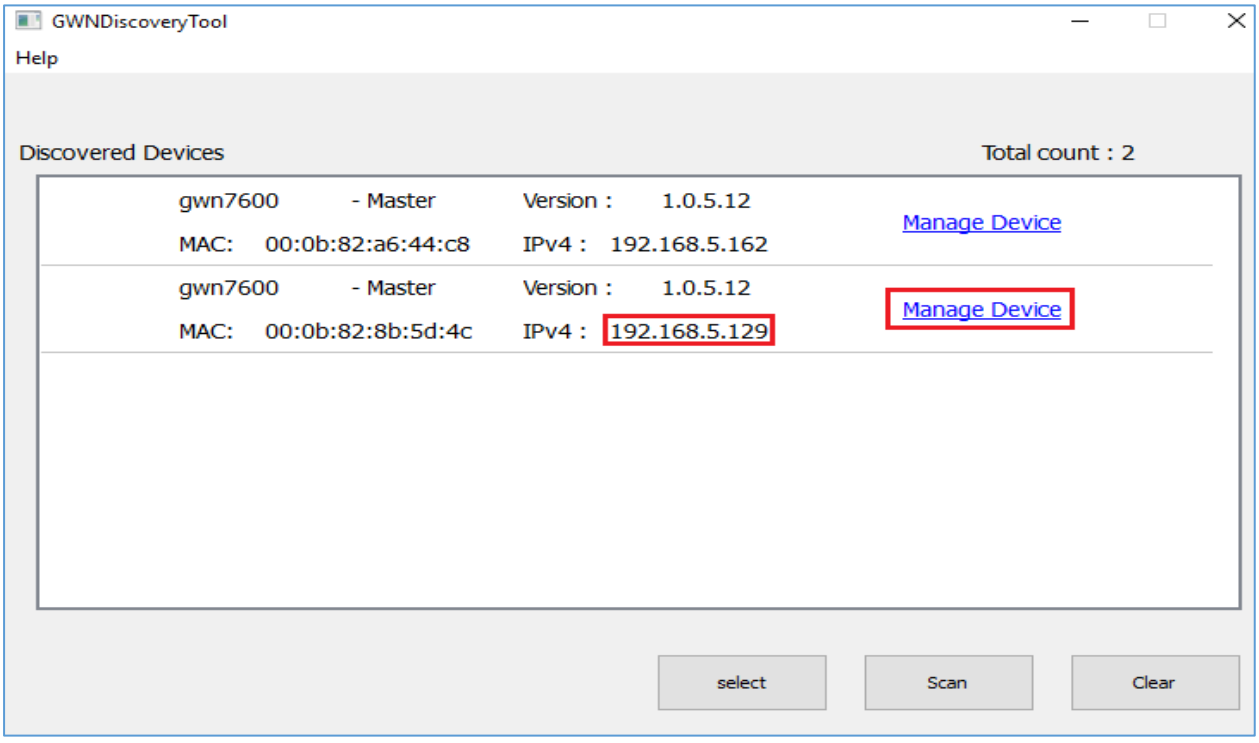


Figure 15: GWN Discovery Tool

Use the Web GUI

Users can access then the GWN7600/GWN7600LR using its WebGUI, the following sections will explain how to access and use the Web Interface.

Access Web GUI

The GWN7600/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 and etc.

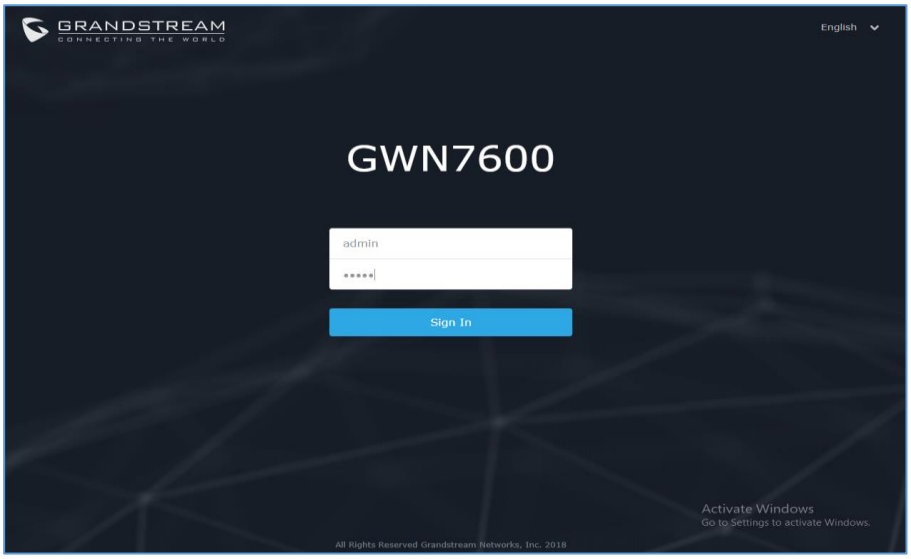


Figure 16: GWN7600/GWN7600LR Web GUI Login Page

To access the Web GUI:

1. Make sure to use a computer connected to the same local Network as the GWN7600/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 GWN7600/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 GWN7600/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 login.

Figure 17: GWN7600/GWN7600LR Web GUI Language (Login page)

Figure 18: GWN7600/GWN7600LR Web GUI Language (Web Interface)

Overview Page

Overview is the first page shown after successful login to the GWN7600/GWN7600LR's Web Interface. Overview page provides an overall view of the GWN7600/GWN7600LR's information presented in a Dashboard style for easy monitoring along with firmware version and date-time information at the top.

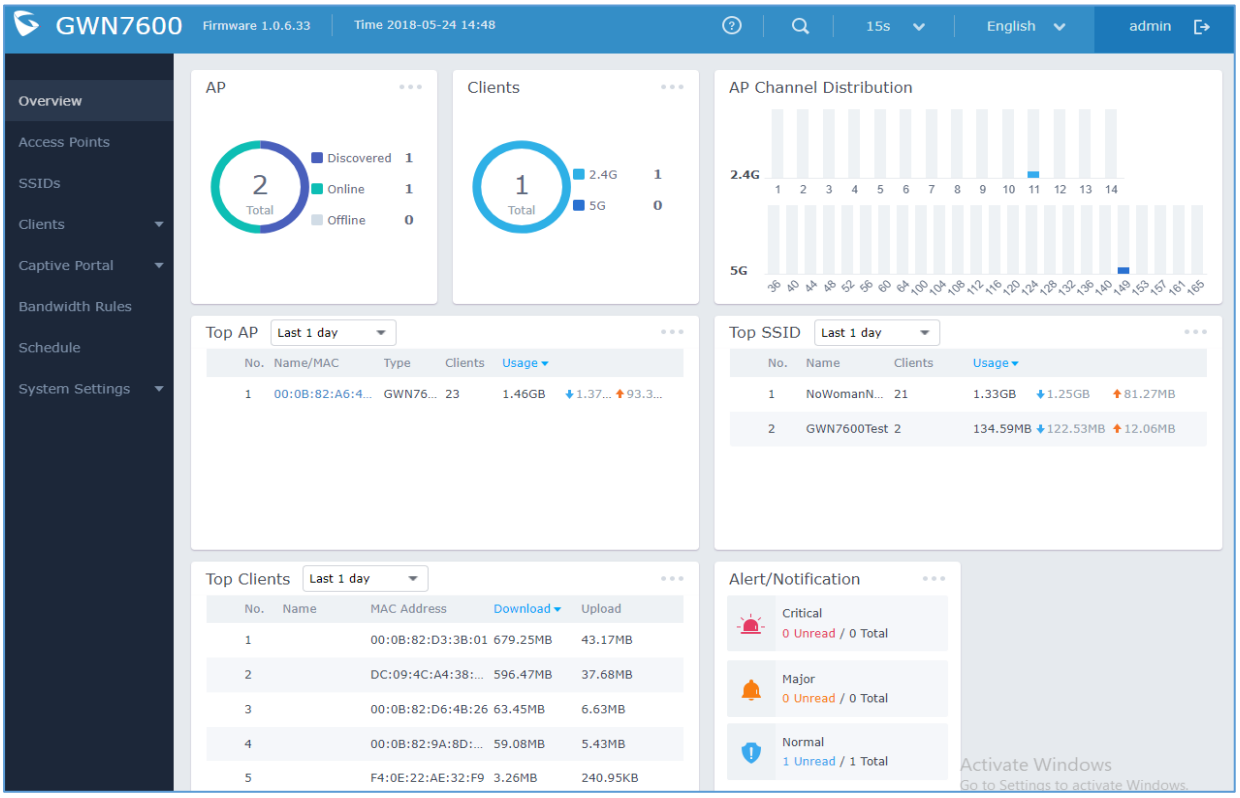


Figure 19: GWN7600/GWN7600LR's Dashboard

Users can quickly see the status of the GWN7600/GWN7600LR for different items, please refer to the following table:

Table 8: Overview

AP	Shows the number of Access Point 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 SSID 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 Overview page in addition to other tabs can be updated each 15s, 1min ,2min and 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 16).

Click on  button to apply changes.

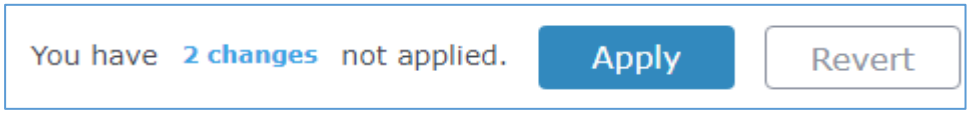


Figure 20: Apply Changes

GWN.CLOUD

Starting from firmware 1.0.6.41, the GWN7600/GWN7600LR can be managed by your **GWN.Cloud** account, **GWN.Cloud** web interface now can be accessed at https://www.gwn.cloud. Please refer to **GWN.Cloud User Guide** for how to add your GWN AP to **GWN.Cloud.**

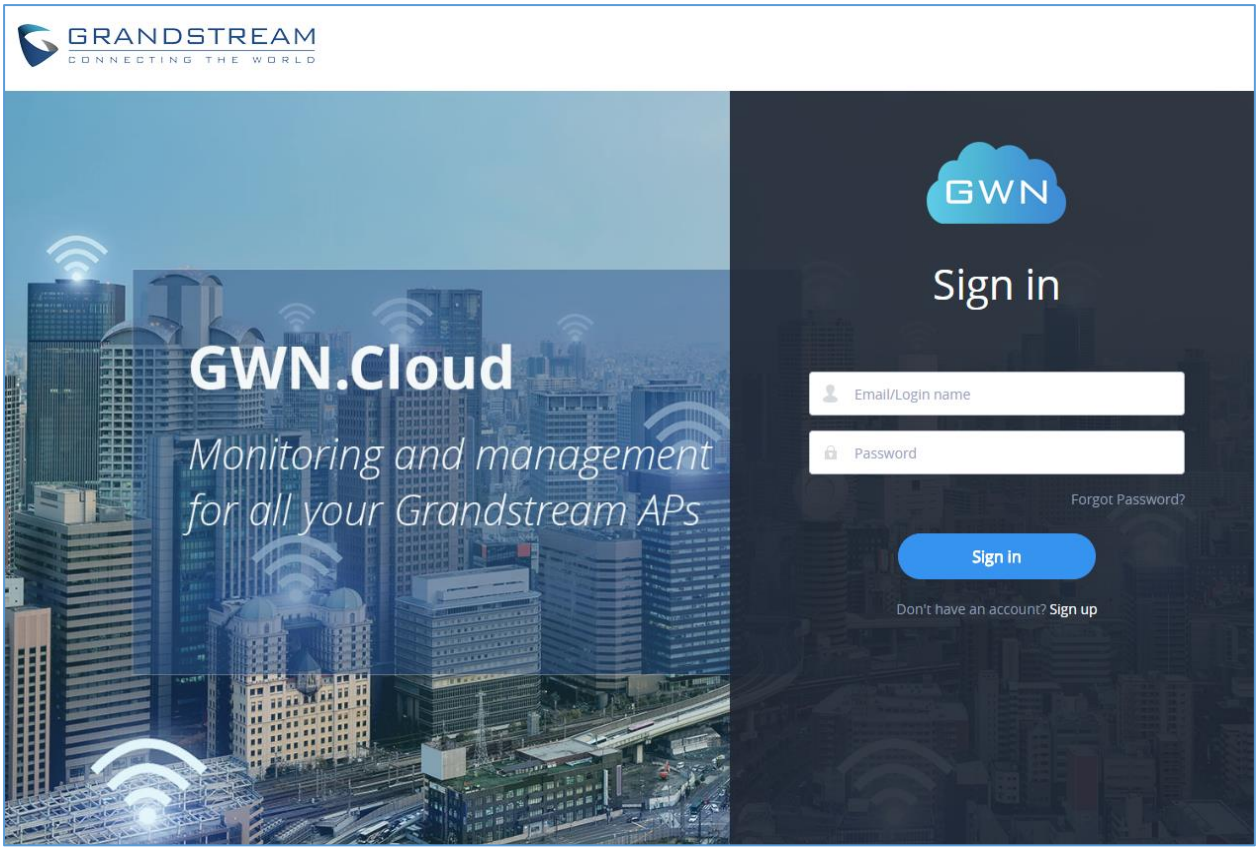


Figure 21: GWN.Cloud Login Page

USING GWN7600/GWN7600LR AS STANDALONE ACCESS POINT

The GWN7600/GWN7600LR can be used in Standalone mode, where it can act as Master Access Point Controller or in Slave mode and managed by another GWN76xx Master.

This section will describe how to use and configure the GWN7600/GWN7600LR in standalone mode.

Connect to GWN7600/GWN7600LR Default Wi-Fi Network

GWN7600/GWN7600LR can be used as standalone access point out of box, or after factory reset with Wi-Fi enabled by default.

After powering the GWN7600/GWN7600LR and connecting it to the network, GWN7600/GWN7600LR will broadcast a default SSID based on its MAC address **GWN [MAC's last 6 digits]** and a random password. Note that GWN7600/GWN7600LR's default SSID and password information are printed on the MAC tag of the unit as shown on the below figure.

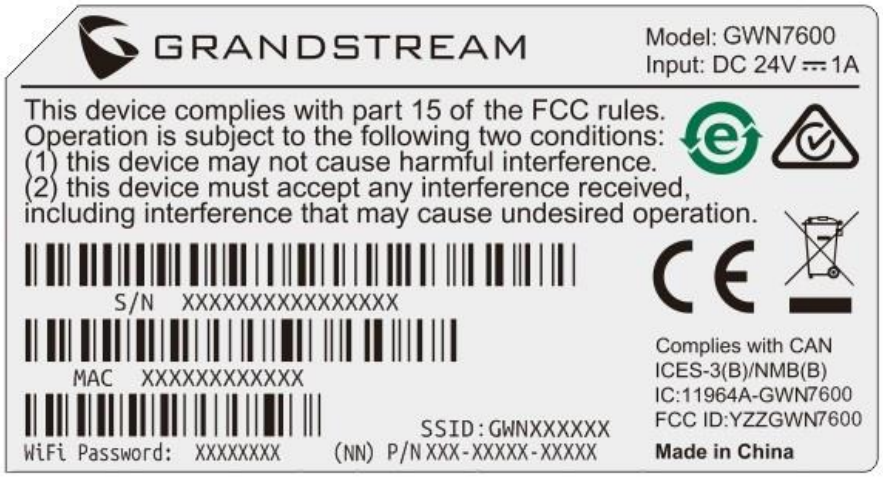


Figure 22: MAC Tag Label

USING GWN7600/GWN7600LR AS MASTER ACCESS POINT CONTROLLER

Master Mode allows a GWN7600/GWN7600LR to act as an Access Point Controller managing other GWN76XX 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.

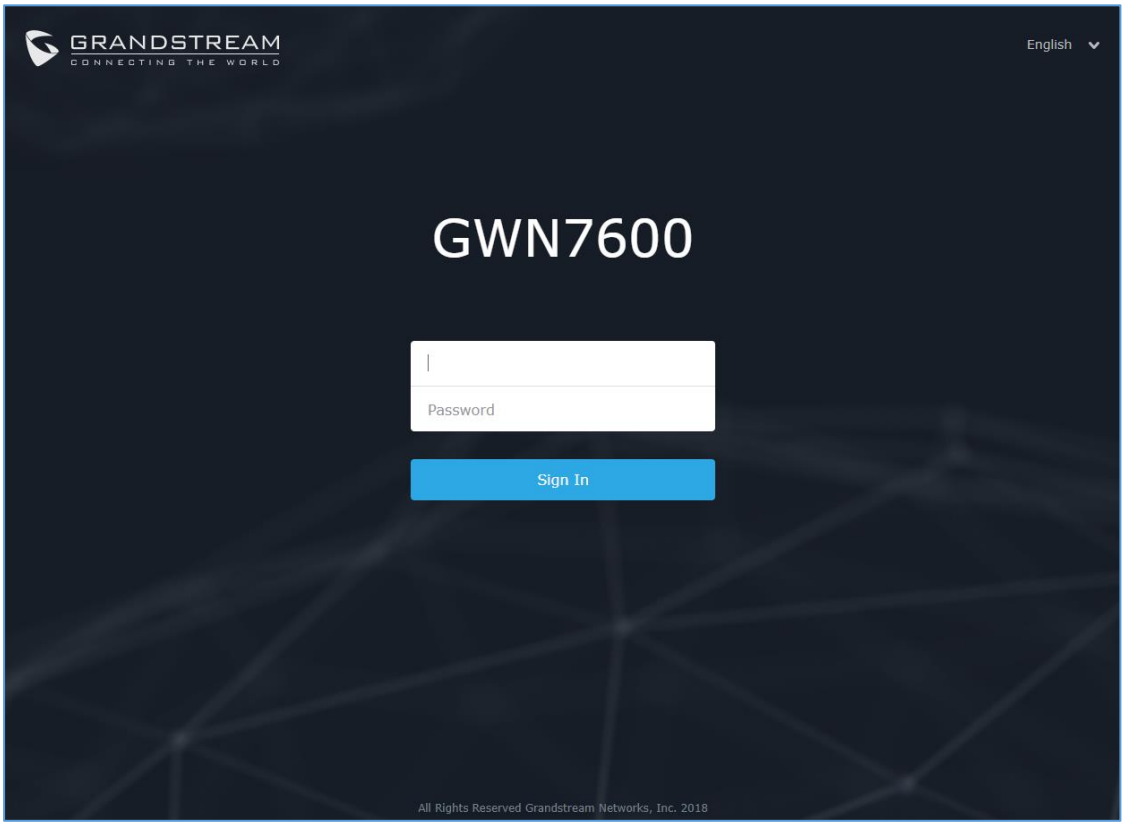


Figure 23: Login Page

⚠ **Warning:**

"**Set unit as Master**" option will forbid the GWN7600/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 GWN7600/GWN7600LR, or unpair it from the initial GWN76XX in order 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.

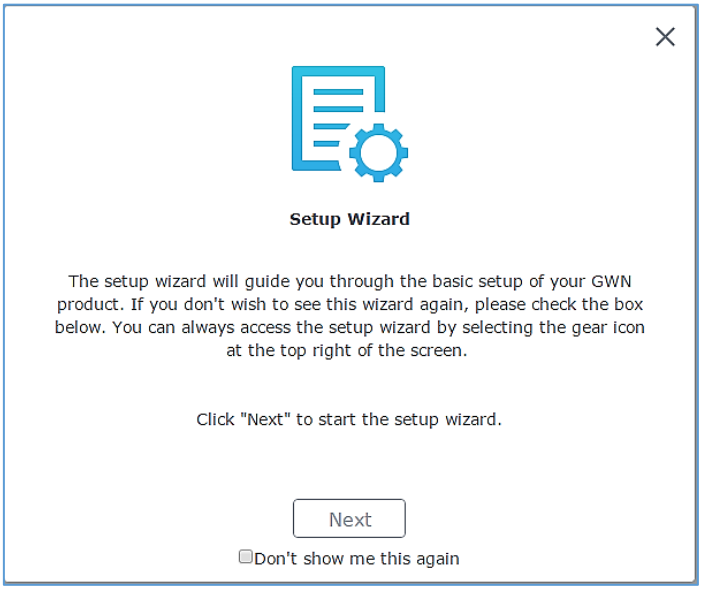


Figure 24: Setup Wizard

Discover and Pair Other GWN7600/GWN7600LR Access Point

To Pair a GWN76XX access point connected to the same Network as the GWN7600/GWN7600LR follows the below steps:

1. Connect to the GWN7600/GWN7600LR Web GUI as Master and go to **Access Points.**

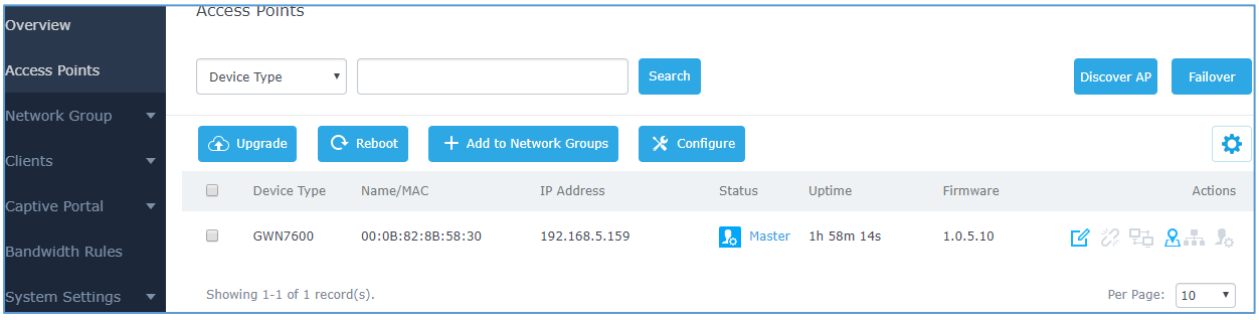


Figure 25: Discover and Pair GWN7600/GWN7600LR

2. Click on Discover AP, in order to discover access points within GWN7600/GWN7600LR's Network, the following page will appear.

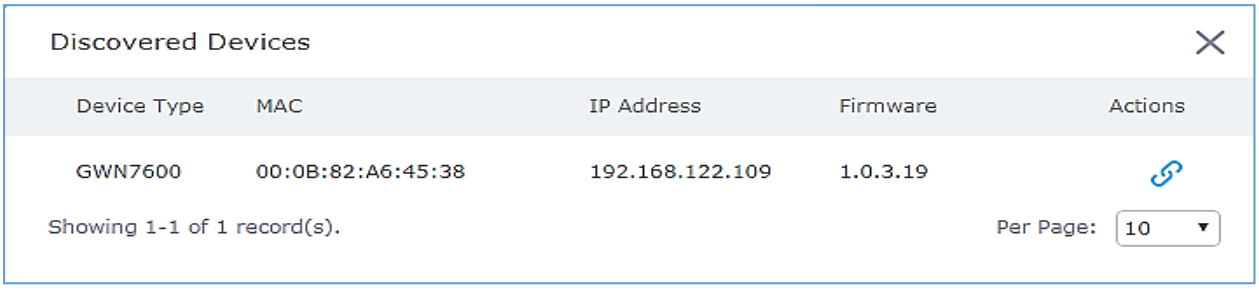


Figure 26: Discovered Devices

3. Click on Pair under Actions, in order to pair the discovered access point as slave with the GWN7600/GWN7600LR acting as Master.

4. The paired GWN7600/GWN7600LR will appear Online, users can click on to unpair it.

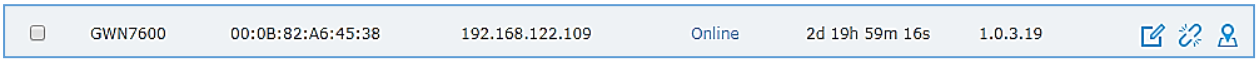


Figure 27: GWN7600/GWN7600LR Online

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.

6. Now an easier way to transfer your master authority from one unit to another available unit is available on Access Point management page. By clicking the "**Transfer to Master**" button the designated slave unit will be upgraded to master and current master will be downgraded to slave accordingly.

Table 9: Device Configuration

Field	Description
Status	Shows the device's status information such as MAC, Product Model, Part Number, Boot Version, Firmware version, IP Address, Link Speed, Uptime, and Users count via different Radio channels.
Clients	Shows the connected Users to the GWN7600/GWN7600LR access point.
Configuration	• **Device Name:** Set GWN7600/GWN7600LR's name to be shown next to MAC address. • **Airtime Fairness:** Allow faster clients to have more airtime than slower clients. • **Fixed IP:** Set a static IP for the GWN7600/GWN7600LR, default is unchecked.

- **Frequency:** Set the GWN7600/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 2.4 GHz.
- **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high-density environment.
- **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be Secondary below Primary, Primary below Secondary or Auto.
- **Channel:** Select Auto, or a specified channel, default is Auto. Note that the proposed channels depend on **Country** Settings under **System Settings→Maintenance**.
- **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, it can be Low, Medium or 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 GWN7600/GWN7600LR is not being discovered or the pair icon is grey color, make sure that it is not being paired with another GWN76XX Access Point acting as Master Controller, if yes users will need to unpair it first, or reset it to factory default settings in order to make it available for pairing by other GWN76XX Access Point Controller

AP Location

GWN supports a handy feature which allows users to locate other Access points by blinking LED. To use the feature, navigate on the master web GUI under "Access Points" page and click on the icon near the desired AP, and it corresponding unit will start blinking the LEDs.

Sequential Upgrade

If you choose multiple slave devices to upgrade their firmware, two options are available: "All-at-Once" and "Sequential". "All-at-Once" will use the default method, all checked slaves will upgrade their firmware at the same time, while using "Sequential" upgrade method, the slaves will upgrade their firmware one by one in order to:

- Avoid entire Wi-Fi service interruption by full system firmware upgrade.
- Reduce network bandwidth consumption caused by firmware downloading.

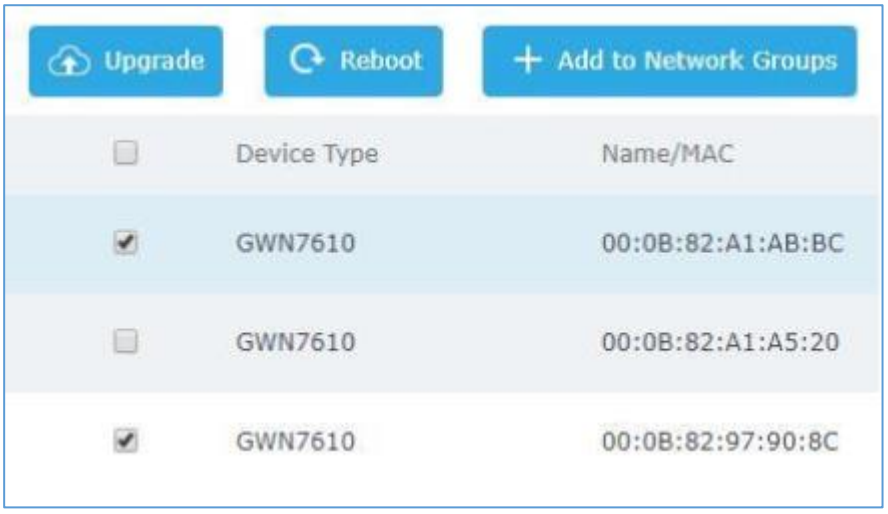


Figure 28: Choosing multiple devices

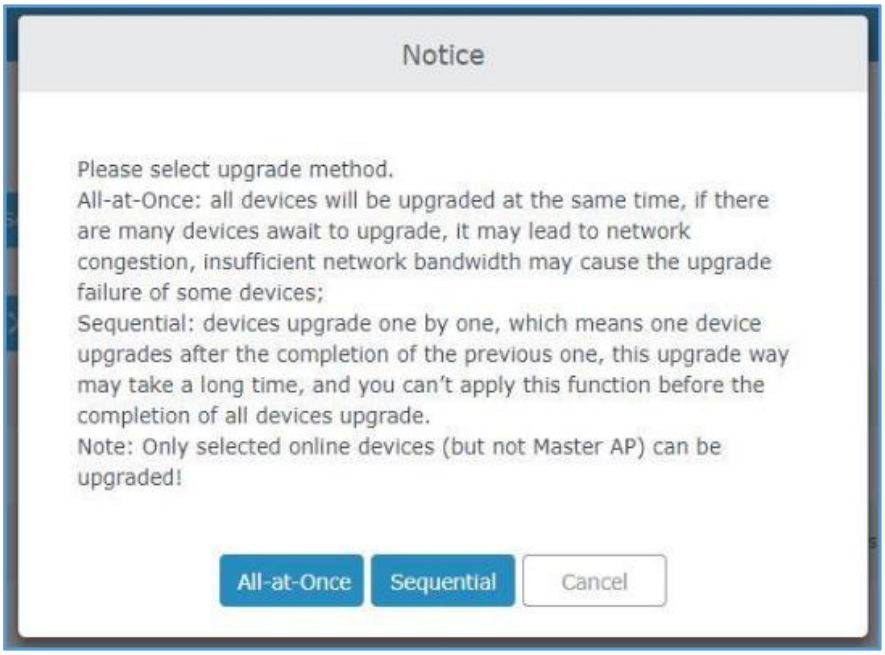
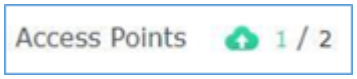


Figure 29: All-at-Once and Sequential Upgrade

Once you choose sequential upgrade, the following icon 

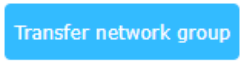
will update you about the number of upgraded slaves out of the selected slaves.

Transfer AP – Transfer Network Group

Users can easily transfer the AP from local master to the ***GWN.CLOUD*** account by clicking on 

. When you already have Network/WIFI configurations on your cloud account, using this feature will let you choose existing Network/SSID to adopt your local AP.

Note: Local configurations will not be transferred.



feature will allow you to transfer your local configurations to your cloud account.

For more details, please refer to **GWN.Cloud User Guide**.

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.

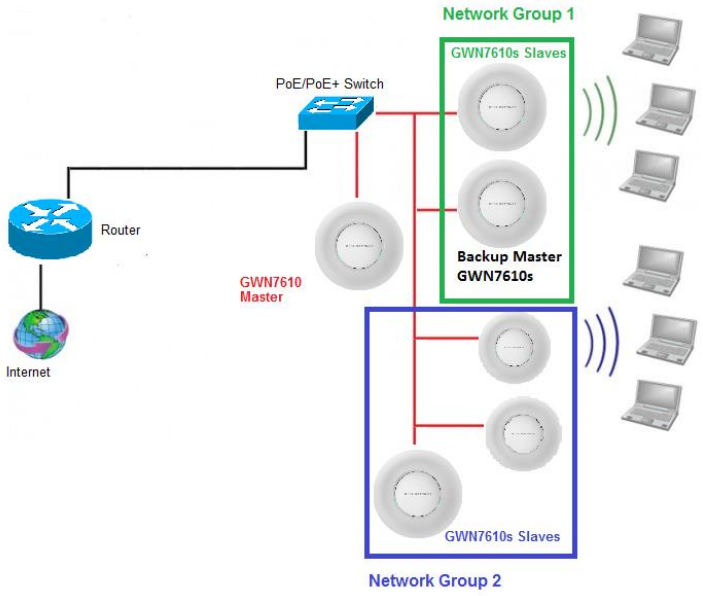


Figure 30: Failover Master

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**

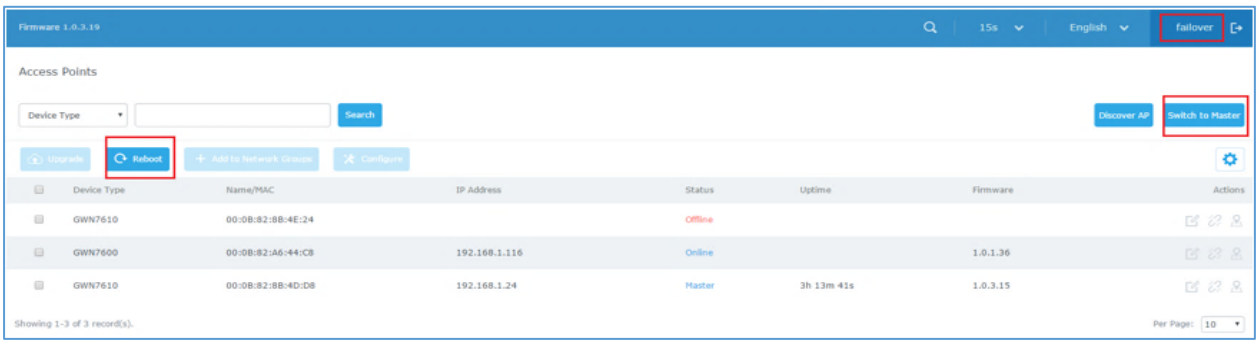


Figure 31: Failover Mode GUI

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 SSID has an Client Bridge Support enabled, the AP adopted in this SSID 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.

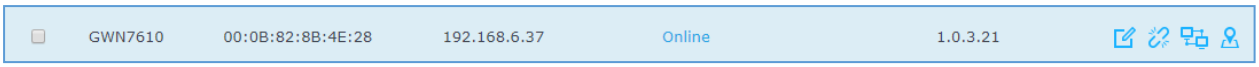


Figure 32: Client Bridge

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 SSID or SSID WiFi settings in order to have it fully functional. See ***[Client Bridge Support]***

SSID

When using GWN7600/GWN7600LR as Master Access Point, users have the ability to create different SSIDs and adding GWN7600/GWN7600LR Slave Access Points.

Log in as Master to the GWN7600/GWN7600LR WebGUI and go to **SSIDs.**

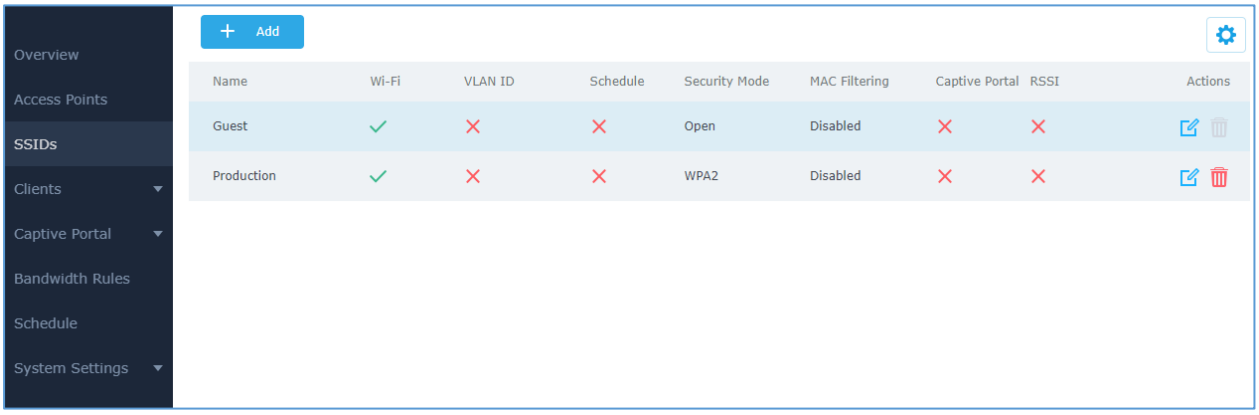


Figure 33: SSID

The GWN7600/GWN7600LR can support up to 16 SSIDs, click on Add to add a new SSID.

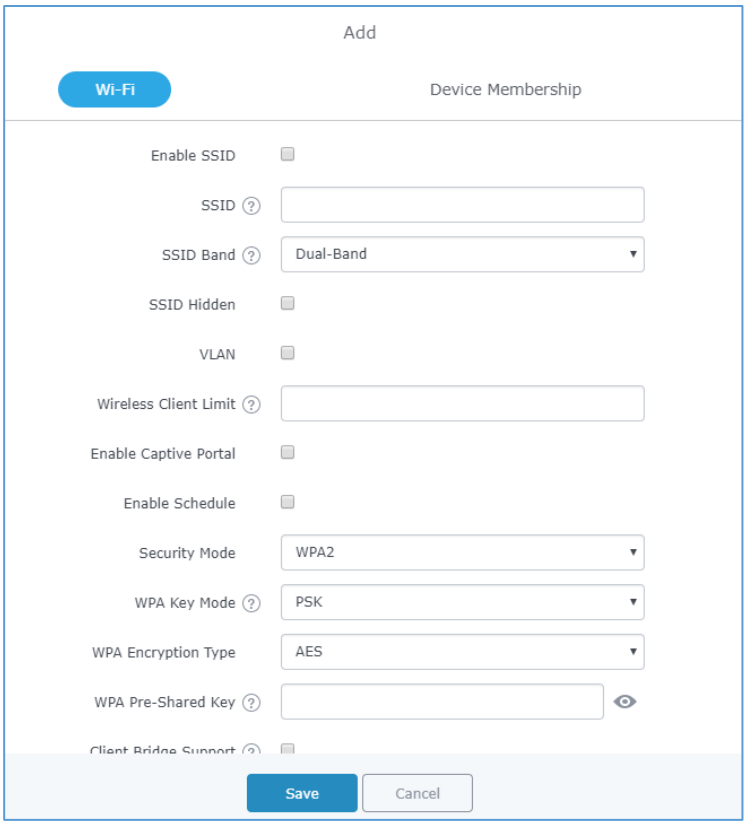


Figure 34: Add a new SSID

When editing or adding a new SSID, users will have two tabs to configure:

- **Wi-Fi:** Please refer to the below table for Wi-Fi tab options

Table 10: Wi-Fi

Field	Description
Enable SSID	Check to enable Wi-Fi for the SSID.
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.
VLAN	Enter the VLAN ID corresponding to the SSID.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a SSID, 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	Click on the checkbox to enable the captive portal feature.
Captive Portal Policy	Select the captive portal policy already created on the "*CAPTIVE PORTAL*" web page to be used in the created SSID.
Enable Schedule	Check the box and choose a schedule to apply for the selected 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.

WEP Key	Enter the password key for WEP protection mode.
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 allow 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 SSID has an Client Bridge Support enabled, the AP adopted in this SSID can be turned in to Bridge Client mode by click the Bridge button.
RADIUS Sever Address	Configures RADIUS authentication server address.
RADIUS Server Port	Configures RADIUS Server Listening port (default is: 1812).
RADIUS Server Secret	Enter the secret password for client authentication with RADIUS server.
RADIUS Accounting Server	Configures the address for the RADIUS accounting server.
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port (defaults to 1813).
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server.
Client Time Policy	Select a time policy to be applied to all clients connected to this SSID.
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.

Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN7600/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 GWN7600/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 GWN7600/GWN7600LR access points. • **Radio Mode:** Wireless clients can access to the internet services, GWN7xxx router and the access points GWN7600/GWN7600LR but they cannot communicate with each other.
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 lower 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 SSID.

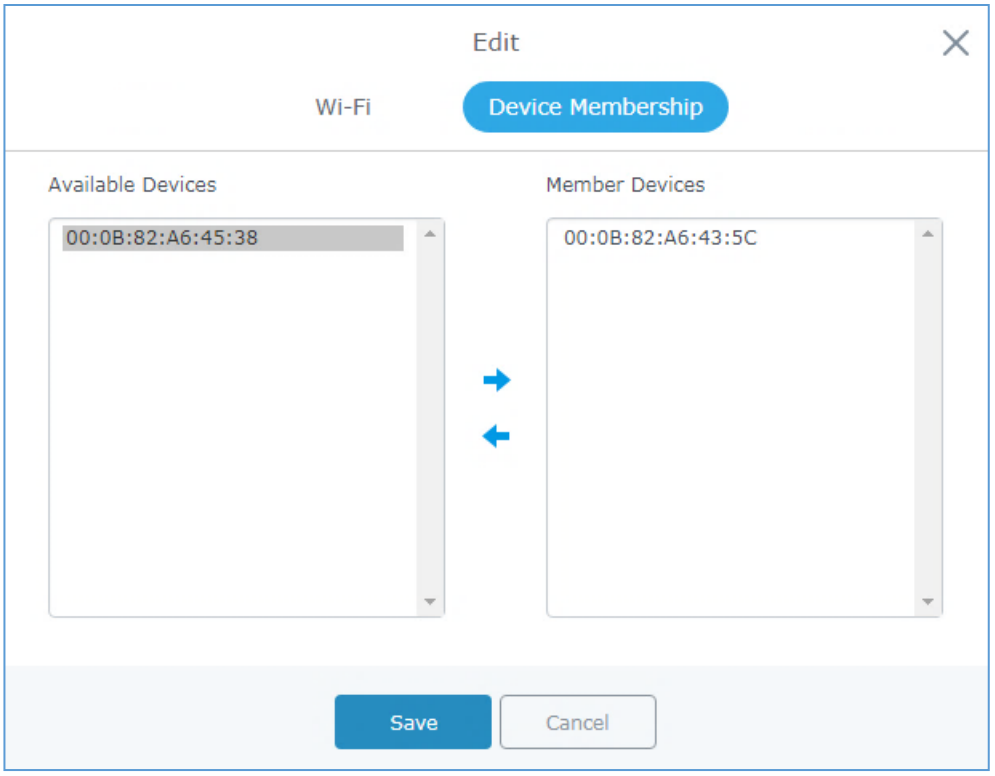


Figure 35: Device Membership

Click on → to add the GWN7600/GWN7600LR to the SSID or click on ← to remove 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 GWN7600/GWN7600LR from **Web GUI→Clients→Clients** to perform different actions to wireless clients.

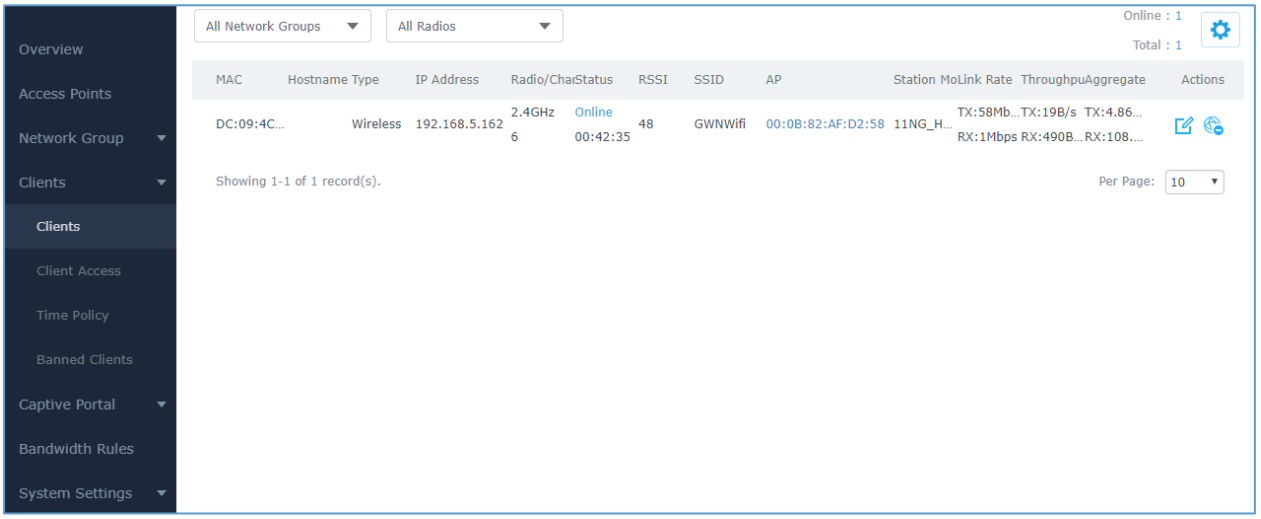


Figure 36: Clients

- 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 SSID.

Clients Access

From this menu, users can manage in global 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.

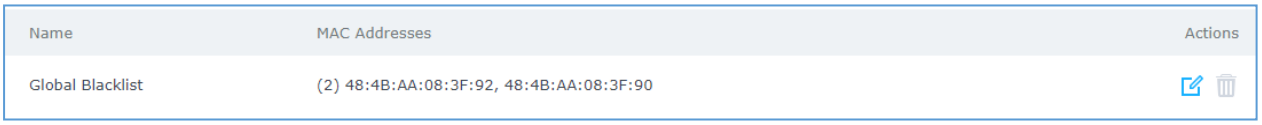


Figure 37: Global Blacklist

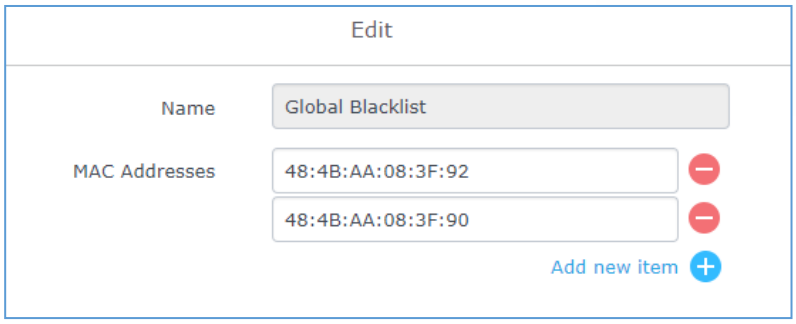


Figure 38: Managing the Global Blacklist

A second option is to add custom access lists that will be used as matching mechanism for MAC address filtering option under 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.

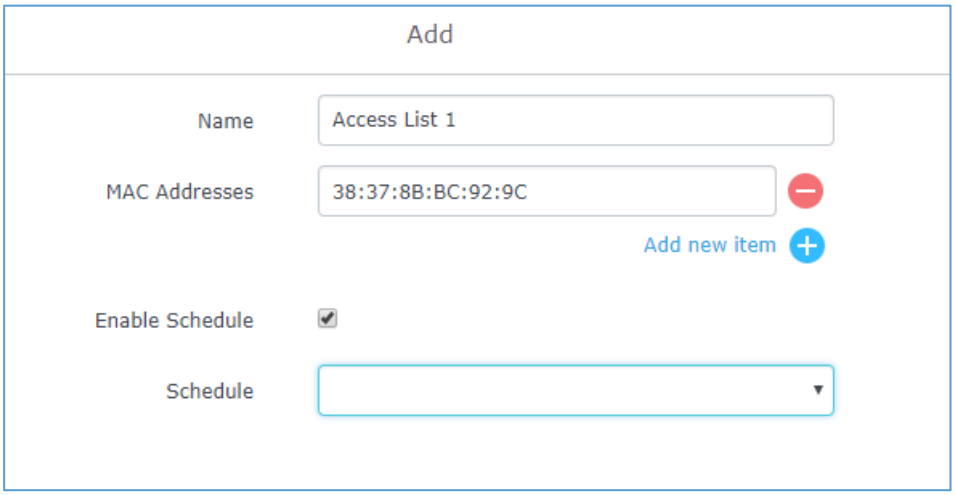


Figure 39: Adding Client Access List

Users can check « Enable Schedule » to assign a schedule for the list when it will take effect.

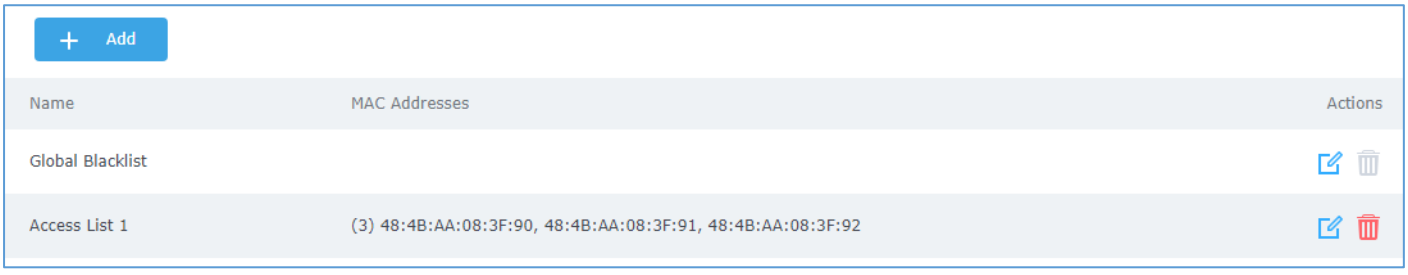


Figure 40: Adding New Access List

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

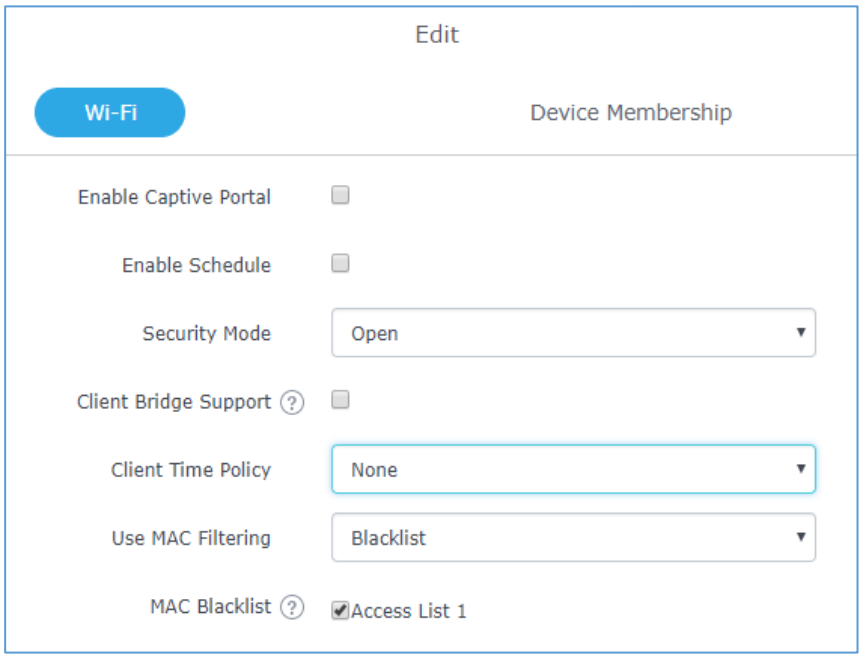


Figure 41: Blacklist Access List

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 11: 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 when the reset will be applied.
Reset Hour	If "Reset Weekly" or "Reset Daily" is selected, this is the hour and day when 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 menu 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 .

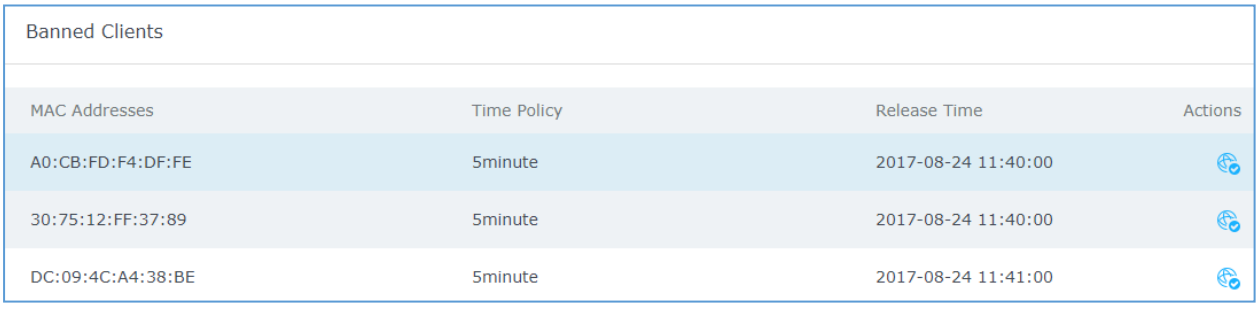


Figure 42: Ban/Unban Client

LED SCHEDULE

GWN7600/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 GWN7600/GWN7600LR WebGUI navigate to "**System Settings→LEDs**".

Following options are available:

Table 12: LEDs

Field	Description
LEDs Always Off	Configure whether to disable the AP LED dictator
Schedule	Please choose a schedule to assign to LEDs, users can configure schedules under the menu *SCHEDULE*

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

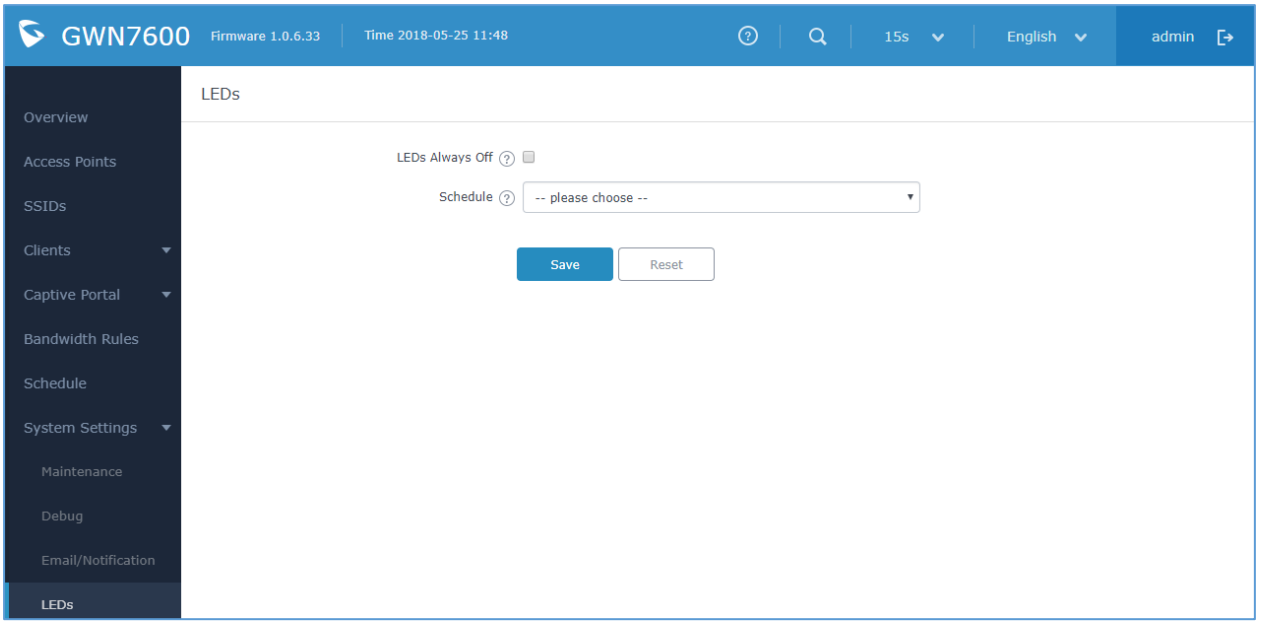


Figure 43: LED Scheduling Sample

CAPTIVE PORTAL

Captive Portal feature on GWN7600/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 GWN7600/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 GWN7600/GWN7600LR Web page under "Captive Portal".

The page contains three tabs: **Policy**, **Files** and **Clients**.

Policy

Users can customize a portal policy in this page.

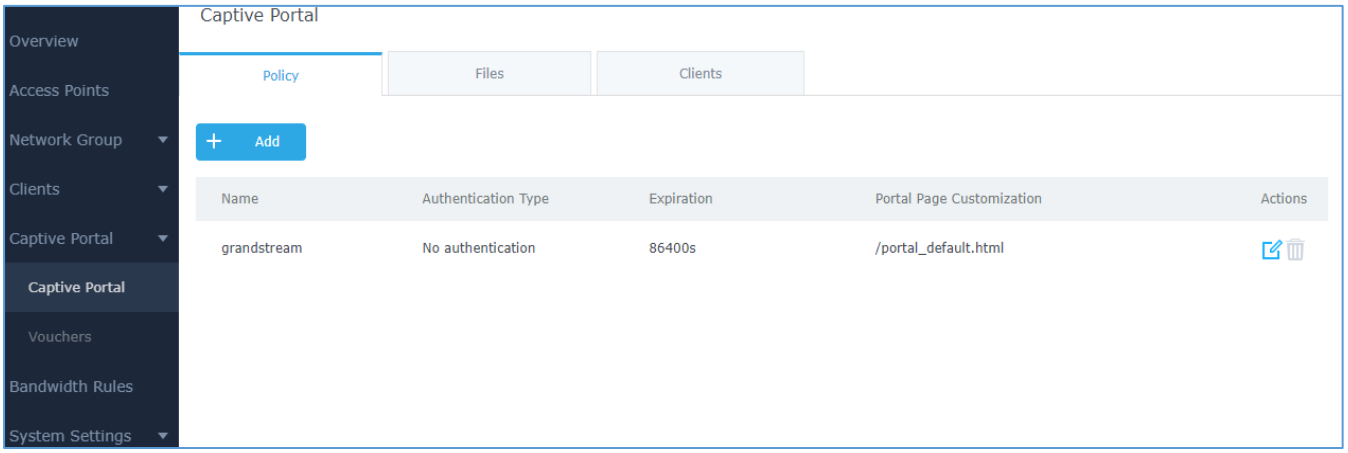
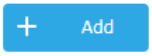


Figure 44: Captive Portal Policy

Click on  to edit the policy.

Click on  to delete the policy.

Click on  to add a policy.

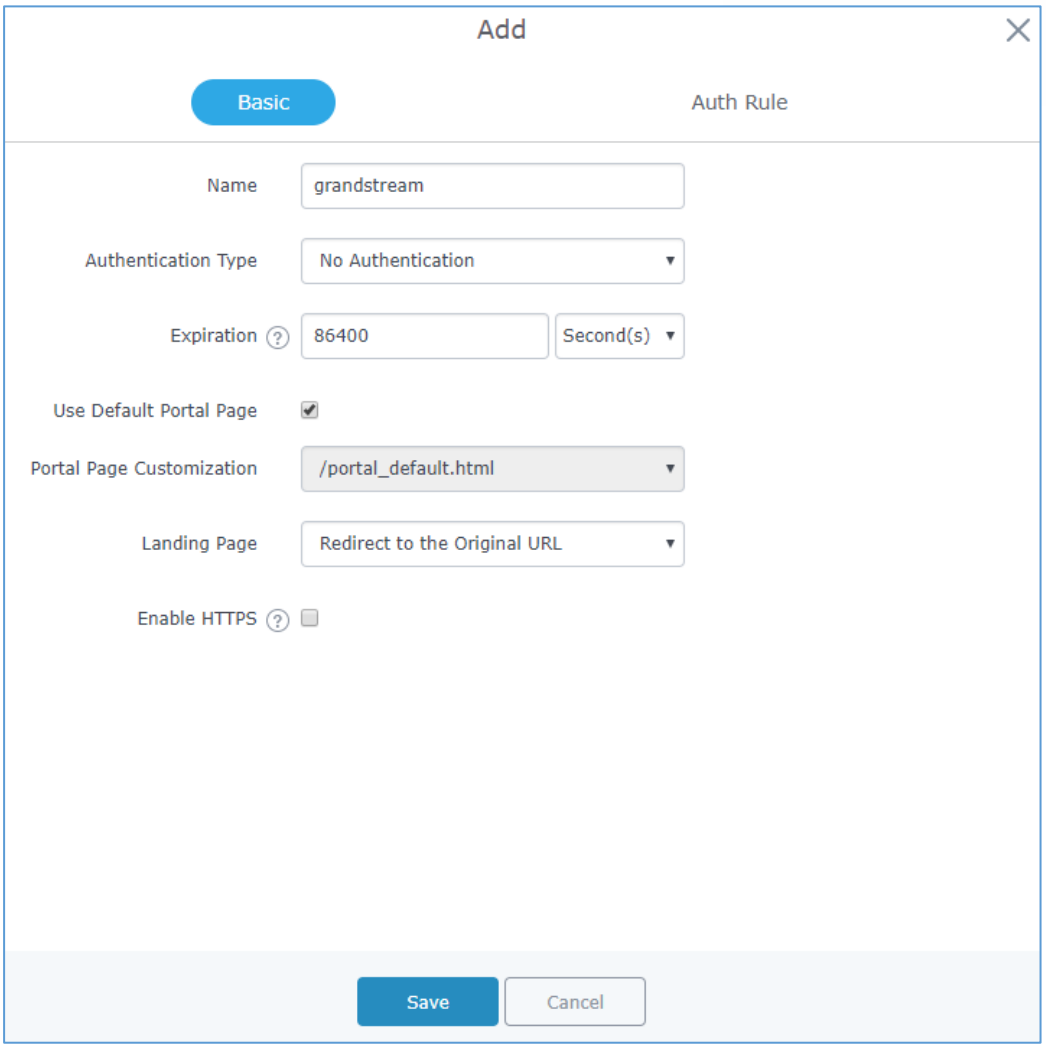


Figure 45: Add a New Policy

Below table lists the items policy add page configures.

Table 13: Policy Parameters

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	Three types of authentication 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. • **Social Login Authentication:** Choosing this option will allow users to enable authentication Facebook or Twitter or WeChat. • **Vouchers:** Choose this page when using authentication via Vouchers. • **Simple Password:** Choose this page when using authentication via Simple password.
RADIUS Server Address	Fill in the IP address of the RADIUS server.
RADIUS Server Port	Set the RADIUS server port, the default value is 1812.
RADIUS Server Key	Fill in the key of the 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
Secret Key	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.
Twitter	Check this box to enable Twitter Authentication.
Owner	Enter the app Owner to use Twitter Login API.
Consumer Key	Enter the app Key to use Twitter Login API.
Consumer Secret	Enter the app secret to use Twitter Login API.
Use Default Portal Page	If checked, the users will be redirected to the default portal page once connected to the GWN.
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 is set to redirect to external page, user should set the URL address for redirecting.
Enable HTTPS	Check to enable/disable HTTPS service.

In case social media authentication is used, the user needs to allow some traffic between the AP and social medial platforms (Facebook API as example) to send authentication credentials and receive reply, this traffic can be allowed using the Authentication rules which are explained below.

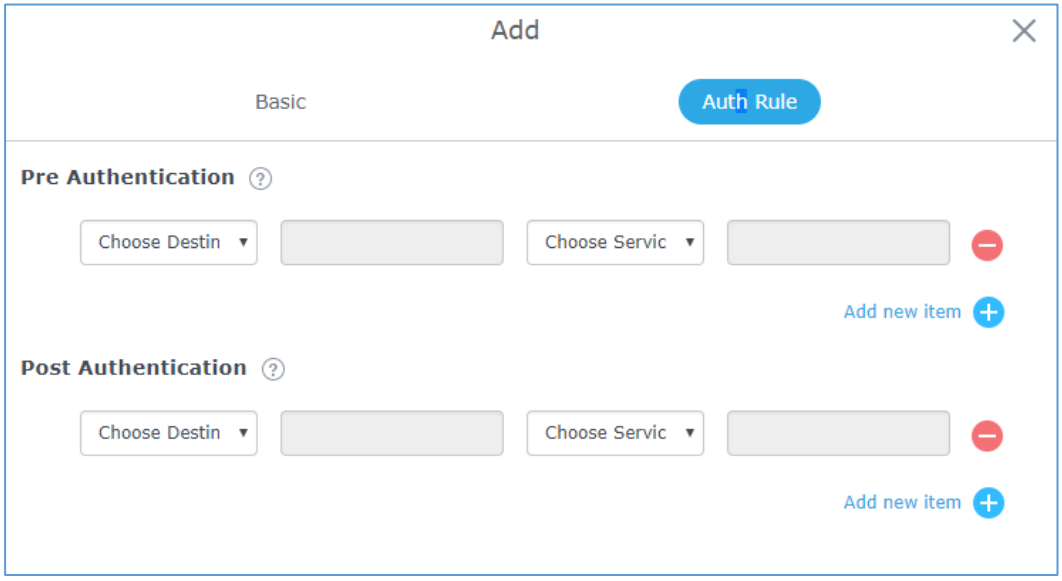


Figure 46: Authentication rules

Pre-Authentication Rules

Using this option, users can set rules to match traffic that will be allowed for connected WiFi users before authentication process. This can be needed for example to setup Facebook authentication where some traffic should be allowed to Facebook server(s) to process the user's authentication. Or simply to be used to allow some type of traffic for unauthenticated users.

Post-Authentication Rules

On the other hand, post authentication rules are used to match traffic that will be banned for WiFi clients after authentication. As an example, if you want to disallow connected WiFi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that traffic and once a connected client passes the authentication process they will be banned from issuing telnet and SSH connections.

Files

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:

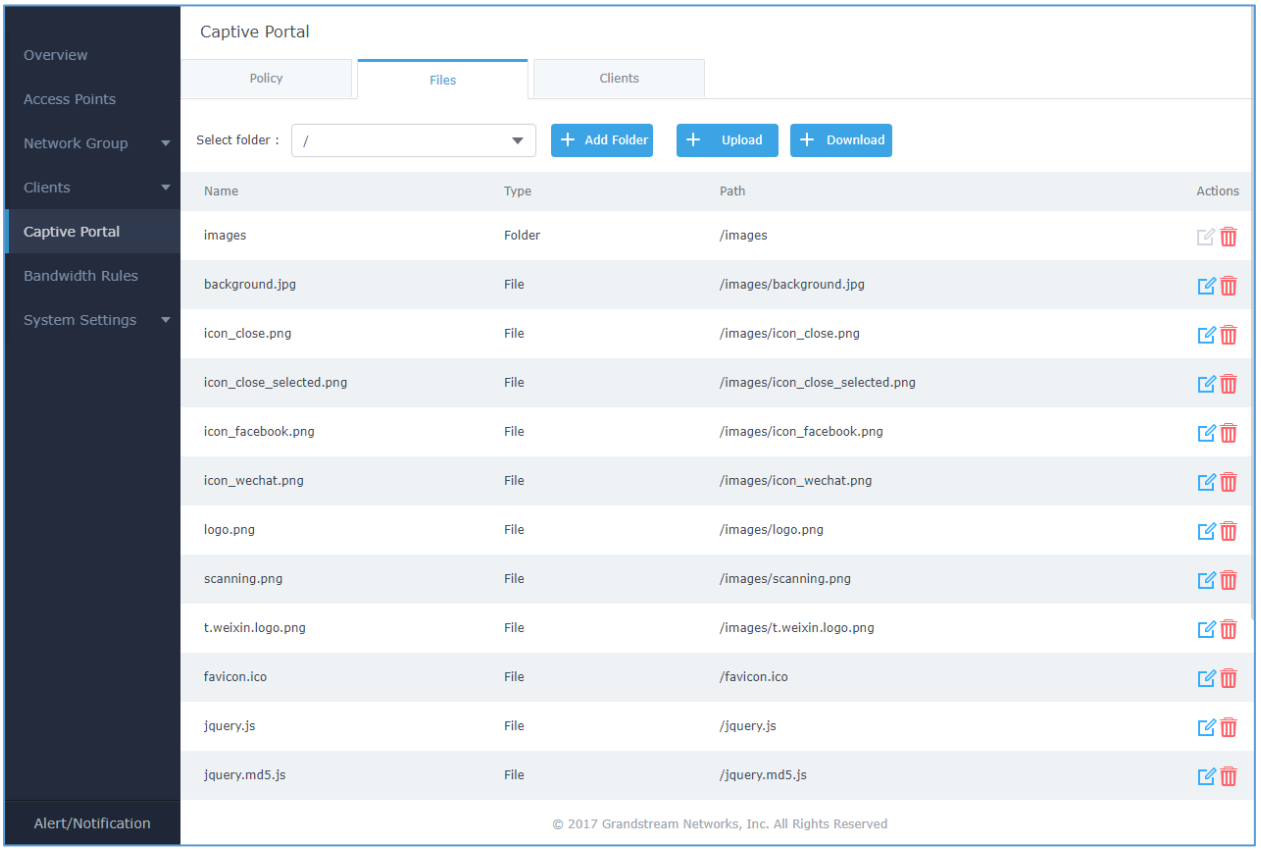


Figure 47: Captive Portal Files

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

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

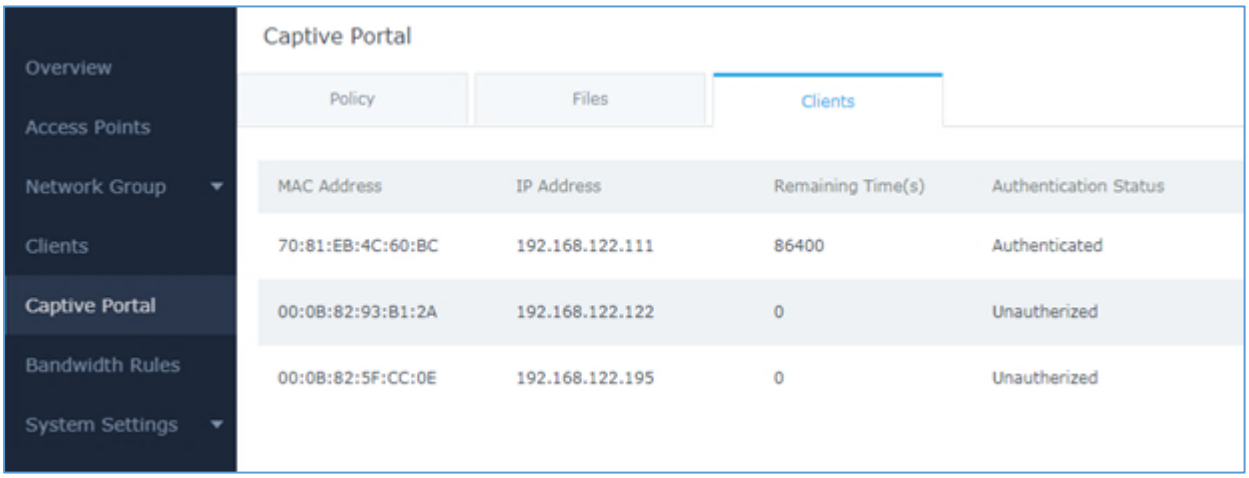


Figure 48: Captive Portal Clients

VOUCHERS

Voucher Feature Description

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

As an example, a coffee shop could offer internet access to customers via WiFi 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.

The usage of voucher feature needs to be combined with captive portal that is explained after this section, in order to have the portal page requesting clients to enter voucher code for authentication.

Voucher Configuration

In order to configure/create vouchers for clients to use, follow below steps:

1. On controller web GUI, navigate under "**Captive Portal → Vouchers**"
2. Click on 

button in order to add a new voucher.
3. Enter voucher details which are explained on the next table.
4. Press save to create the voucher(s).

Notes:

- Users can specify how many vouchers to generate which have the same profile, this way the GWN will generate as many vouchers as needed which do have the same settings avoiding creating them one by one.
- The admin can verify the status of each vocoder on the list (In use, not used, expired …etc).
- Press  to print the voucher, and  to delete it.

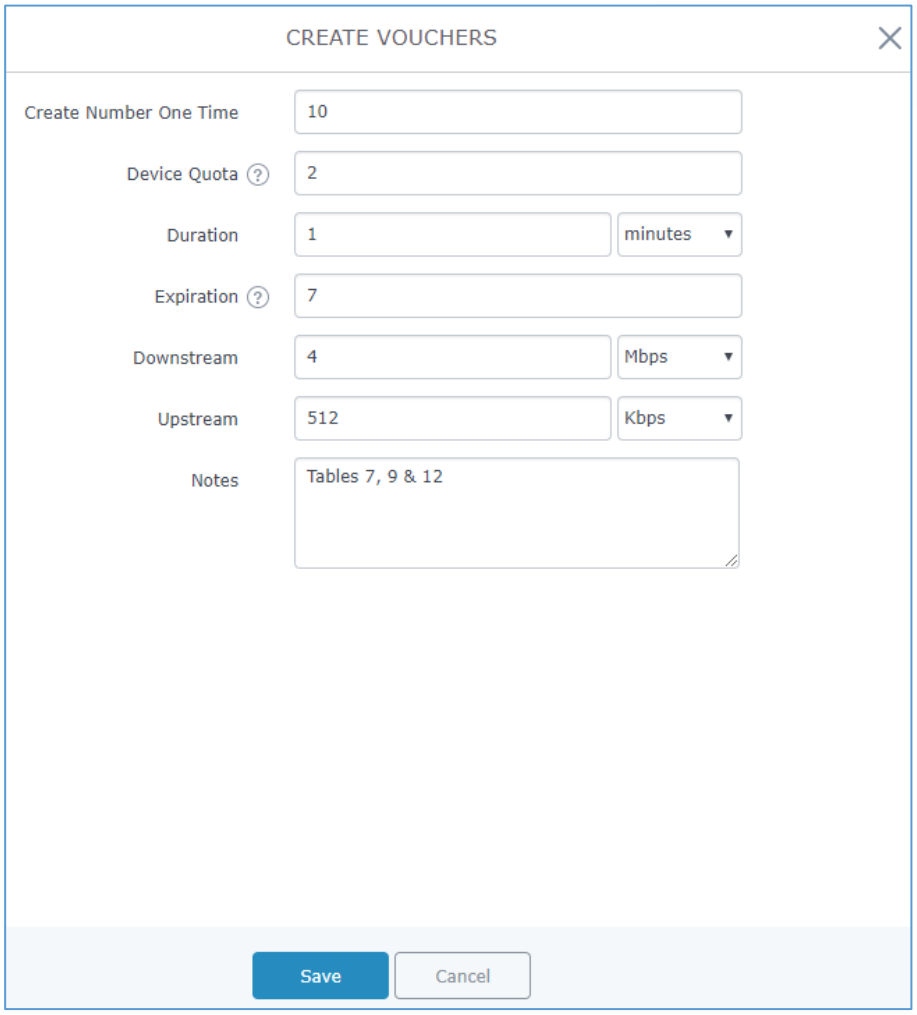


Figure 49: Add Voucher Sample

The below figure shows the status of the vouchers after GWN randomly generates the code for each one.

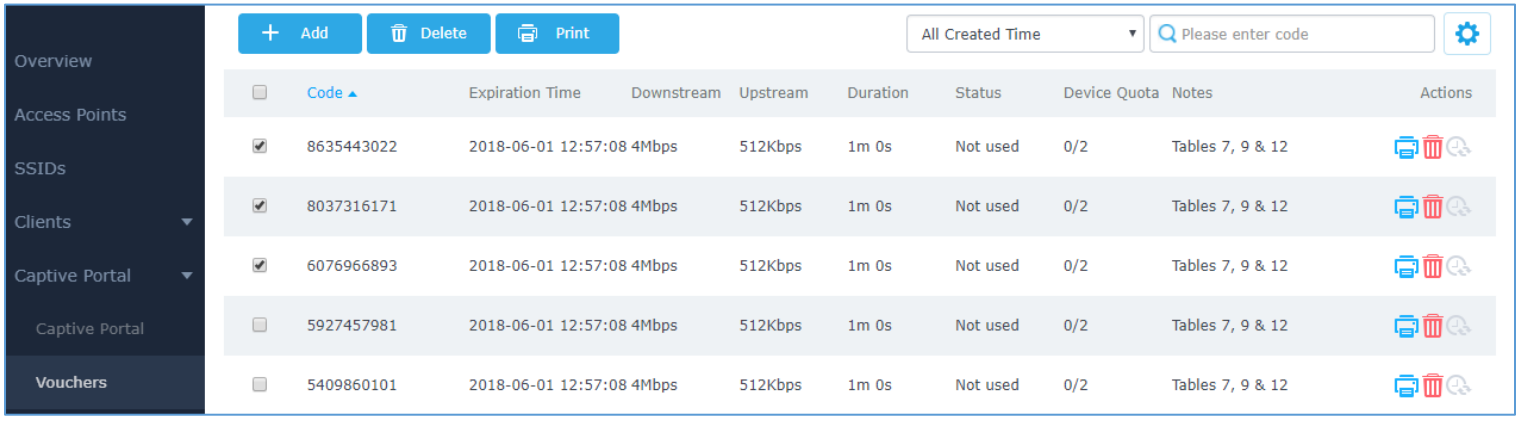
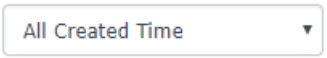


Figure 50: Vouchers List

Users can click on buttons 

and 

to delete and print multiple vouchers.

Also, users can use the drop-down list filter 

to filter the vouchers that where created at specific date-time.

The following table summarizes description for voucher configuration parameters:

Table 14: Voucher Parameters

Field	Description
Create Number One Time	Specify how many vouchers to generate which will have same profile/settings (duration, bandwidth and number of users).
Device Quota	Specify how many users can use the voucher.
Duration	Specify the duration after which the voucher will expire, and clients will be disconnected from internet. **Note:** in case or multiple users, the duration will start counting after first user starts using the voucher.
Expiration	Set the validity period of credentials, limited to 1-365 integer. The unit is day.
Downstream	Set the downstream bandwidth speed limit (in Kbps or Mbps).
Upstream	Set the upstream bandwidth speed limit (in Kbps or Mbps).
Notes	Notes for the admin when checking the list of vouchers.

Using Voucher with GWN captive portal

In order to successfully use the voucher feature, users will need to create a captive portal in order to request voucher authentication codes from users before allowing them access to internet. More details about captive portal will be covered on next section but for voucher configuration please follow below steps.

1. Go under "**Captive Portal → Captive portal**" menu.
2. Press 

in order to add new captive portal policy.
3. Set the following parameters as shown on the screenshot for basic setup then save and apply.

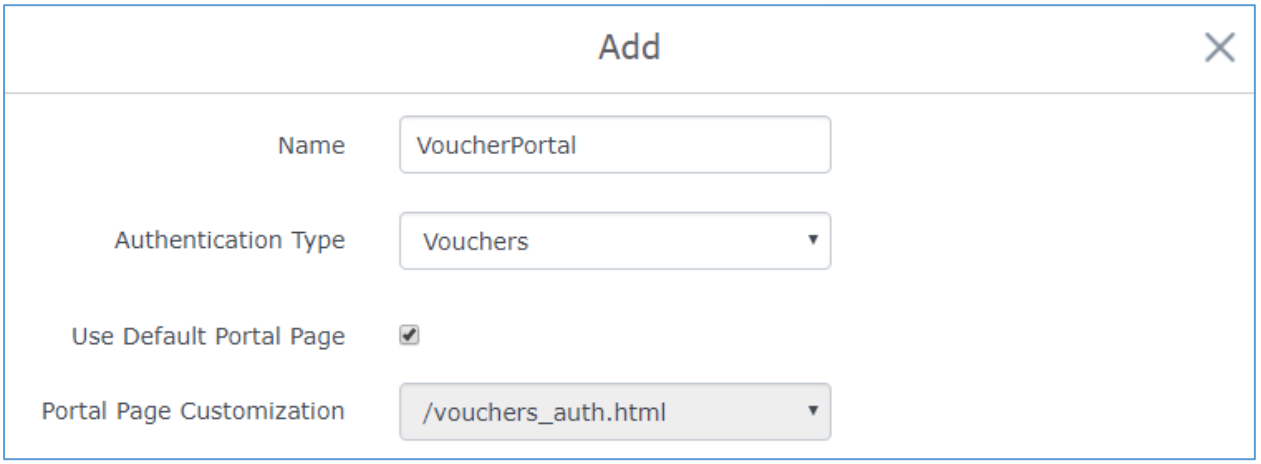


Figure 51: Captive Portal with Voucher authentication

Then go under your SSID configuration page and enable the generated captive portal under WiFi settings tab.

MESH NETWORK

In Mesh Network, wireless connection is established between multiple Aps, which is used to passthrough data traffic rather than client association. Each AP will evaluate the performance of wireless channel based on several factors and choose one or multiple appropriate APs to setup connection.

In a mesh network, access points are categorized to two types:

- **CAP (Central Access Point):** this is an access point that has an uplink connection to the wired network.
- **RE (Range Extender):** This is an access point that participate on the mesh network topology and has a wireless uplink connection to the central network.

In order to deploy mesh access points (RE), users/installers can follow below steps:

1. make sure to have the master and CAP access points already deployed (sometimes the CAP access points can be the master controller of the network).
2. Next, we need to pair the RE access points to the master. This can be done in two ways:
   A. Connect all REs to the same wired LAN as the master then perform the normal process of discovery/pairing process, and after successfully pairing the APs they can be deployed on the field.
   B. REs can also be discovered wirelessly when powered via PSU or PoE Injector, and admin can configure them after discovery. This requires that the REs must be within the range of the Master or CAP Slave's signals coverage.

Note: If there are other GWN APs broadcasting in the same field with different subnet, RE may be wirelessly connected to those networks and cannot be discovered and paired by your Master. Therefore, it is recommended to use the first method of wired pairing and then deploy those REs.

3. After that all slave access points have been deployed and paired to the master, you can directly manage them to operate the mesh network. Mesh service configuration is the same as transitional GWN WLAN.
4. Log into the master page, and under Access Points page you can see the information, for example the AP in the "**Online Wireless**" state **is the RE** (Range Extender) with a wireless uplink to the CAP. The APs showing "**Online**" state are either a wired **master** or **CAP**.

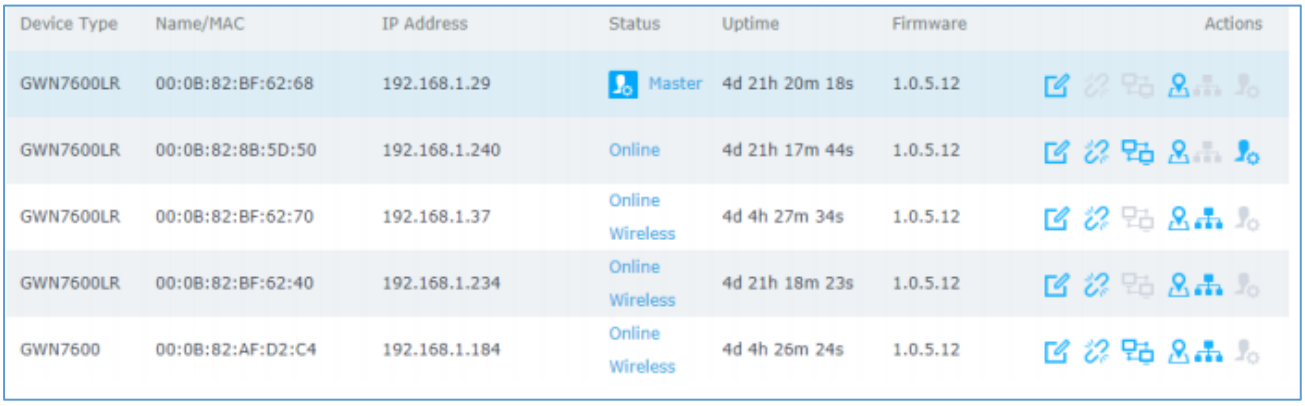


Figure 52: Access Points Status

For Global mesh network settings, navigate to the menu **"System Settings → Mesh"** for setting up the following parameters described below:

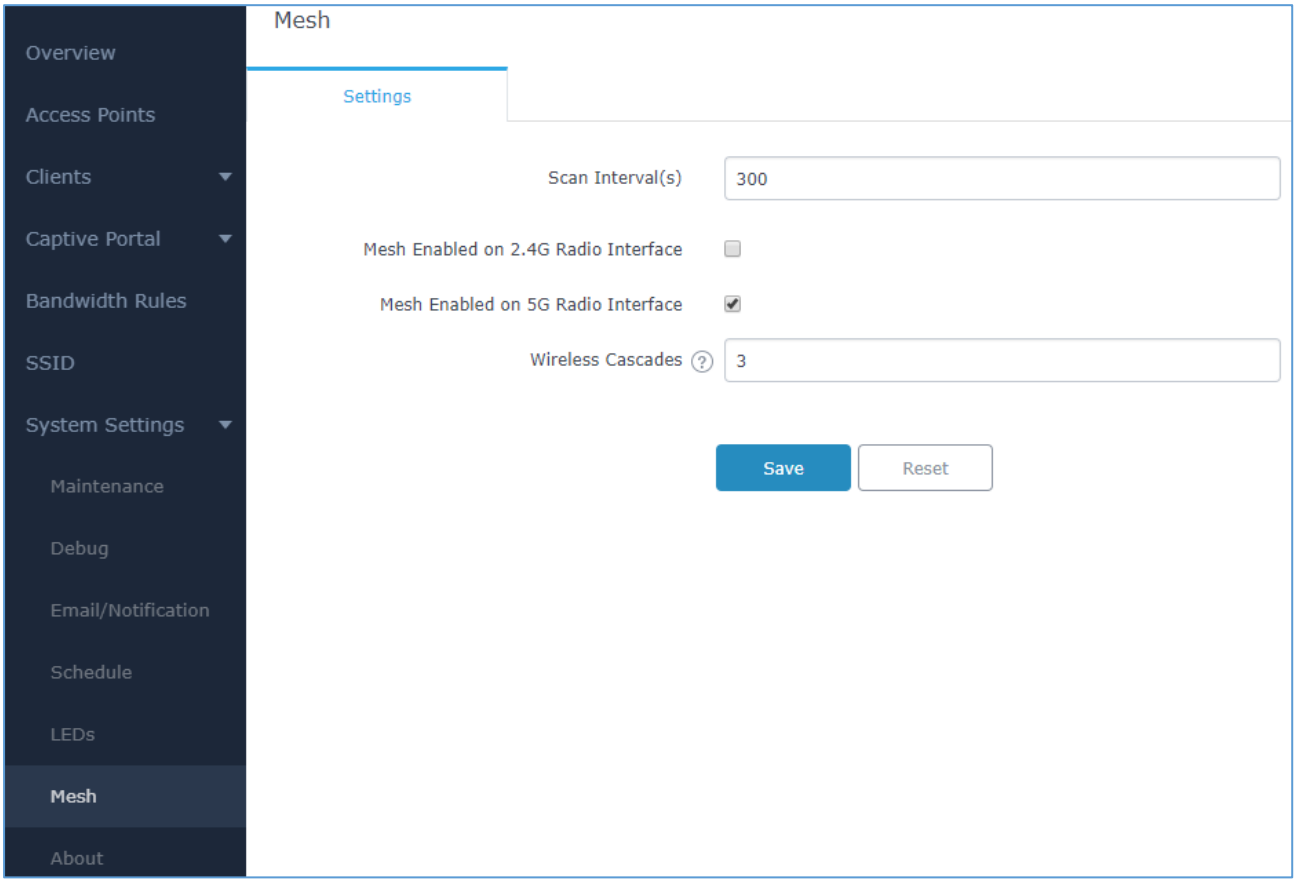


Figure 53: Mesh settings

The following table describes the Mesh configuration settings.

Table 15: Mesh configuration

Filed	Description
Scan Interval	Interval in seconds to scan for available Mesh neighbors.
Mesh Enabled on 2.4G Radio Interface	If checked, Mesh will work on 2.4GHz band.
Mesh Enabled on 5G	If checked, Mesh will work on 5GHz band.
Wireless cascades	Define how many AP can be cascaded wirelessly with the AP. The minimum value is 1 and maximum value is 4.

For more detailed information about GWN Mesh network feature, you may refer to the following technical document: Mesh Network Guide.

BANDWIDTH RULES

The bandwidth rule is a GWN7600/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 GWN7600/GWN7600LR WebGUI under “Bandwidth Rules”.

Click 

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

Table 16: Bandwidth Rules

Field	Description
Enable	Enable/Disable the Bandwidth rule.
SSID	Select which SSID will be affected by the bandwidth rule limitation.
Range Constraint	Choose the type of rule to be applied on bandwidth utilization from the dropdown list, three options are available: • **All:** 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.
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.
Enable Schedule	Enable this option to assign a schedule for the bandwidth rule.
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.

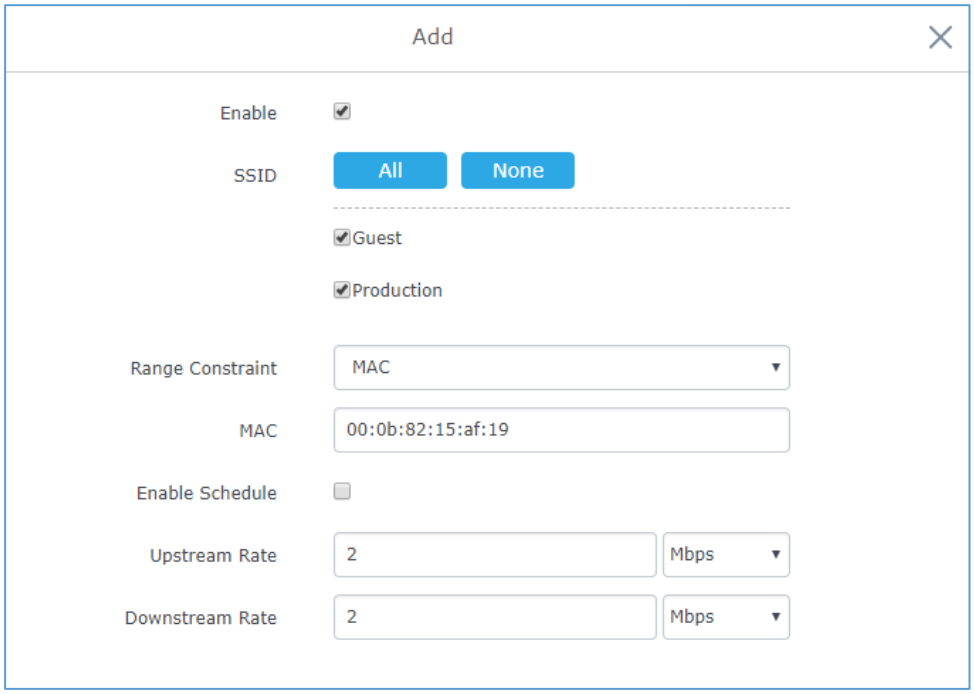


Figure 54: MAC Address Bandwidth Rule

The following figure shows examples of bandwidth rules:

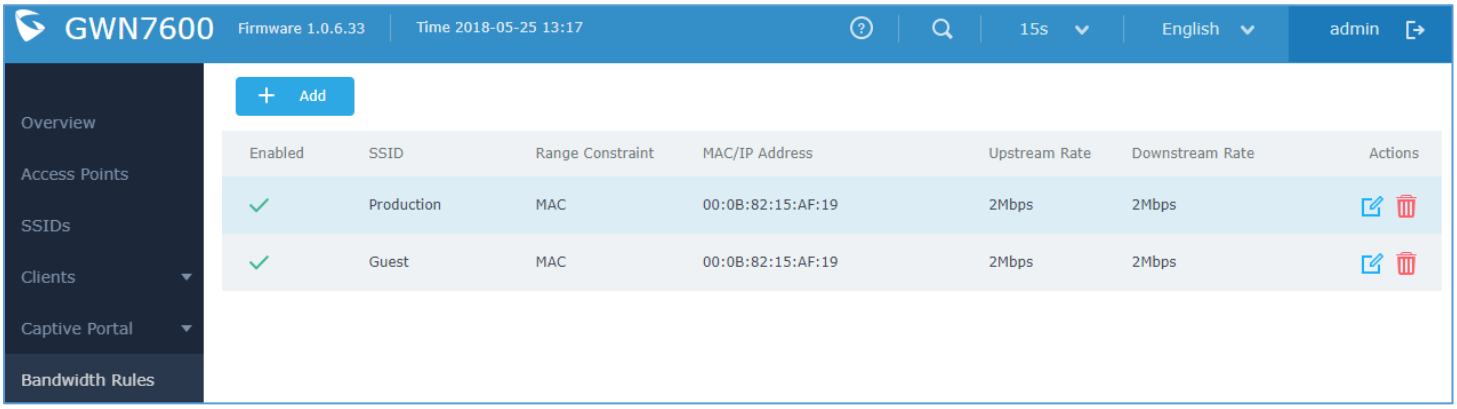


Figure 55: Bandwidth Rules

Note:

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

Per-SSID

Navigate on the web GUI under "SSID→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.

SCHEDULE

Users can use the schedule configuration menu to set specific schedule for GWN features while giving the flexibility to specify the date and time to turn On/Off the selected feature.

The Schedule can be used for settings up specific time for Wi-Fi where the service will be active or for LED schedule or bandwidth rules …etc.

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

1- Go under "**Schedule**" and click on **Create New Schedule**.

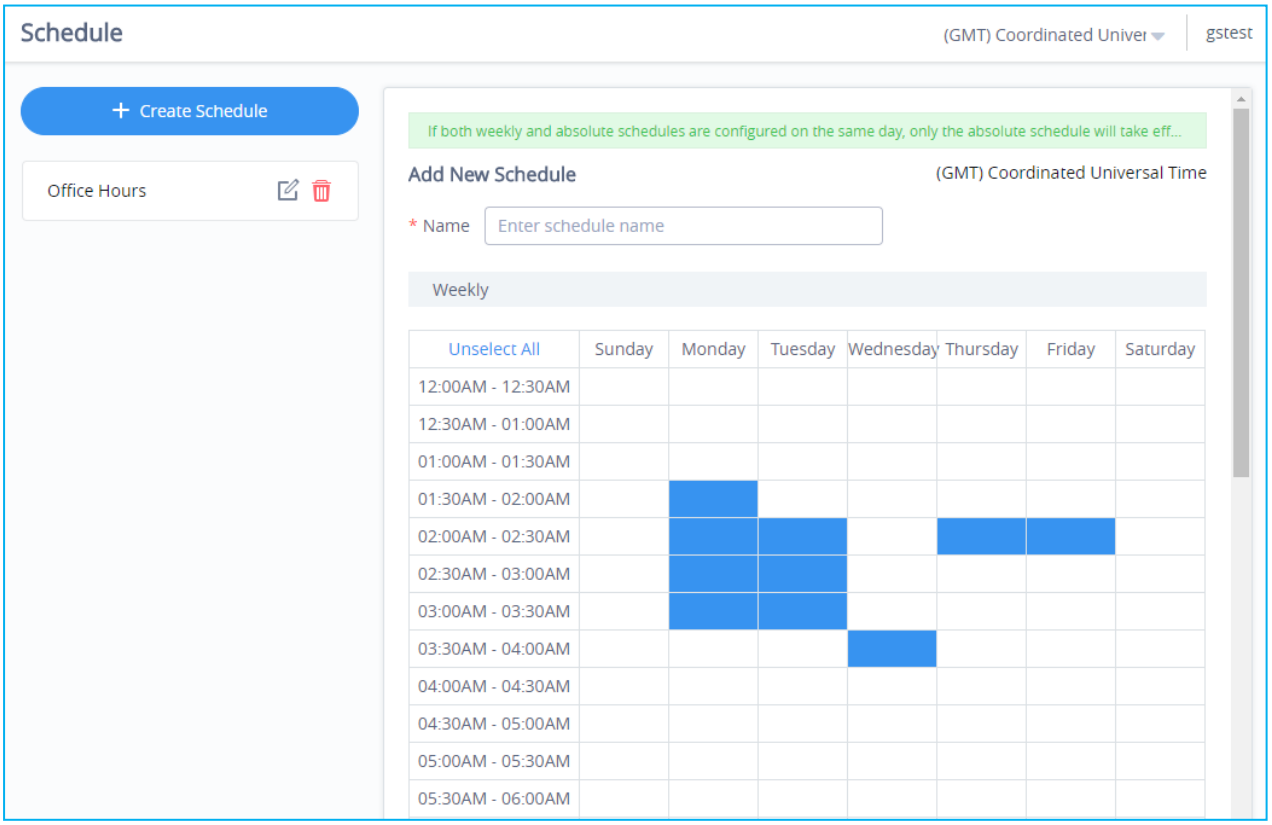


Figure 56: Create New Schedule

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

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.

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

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

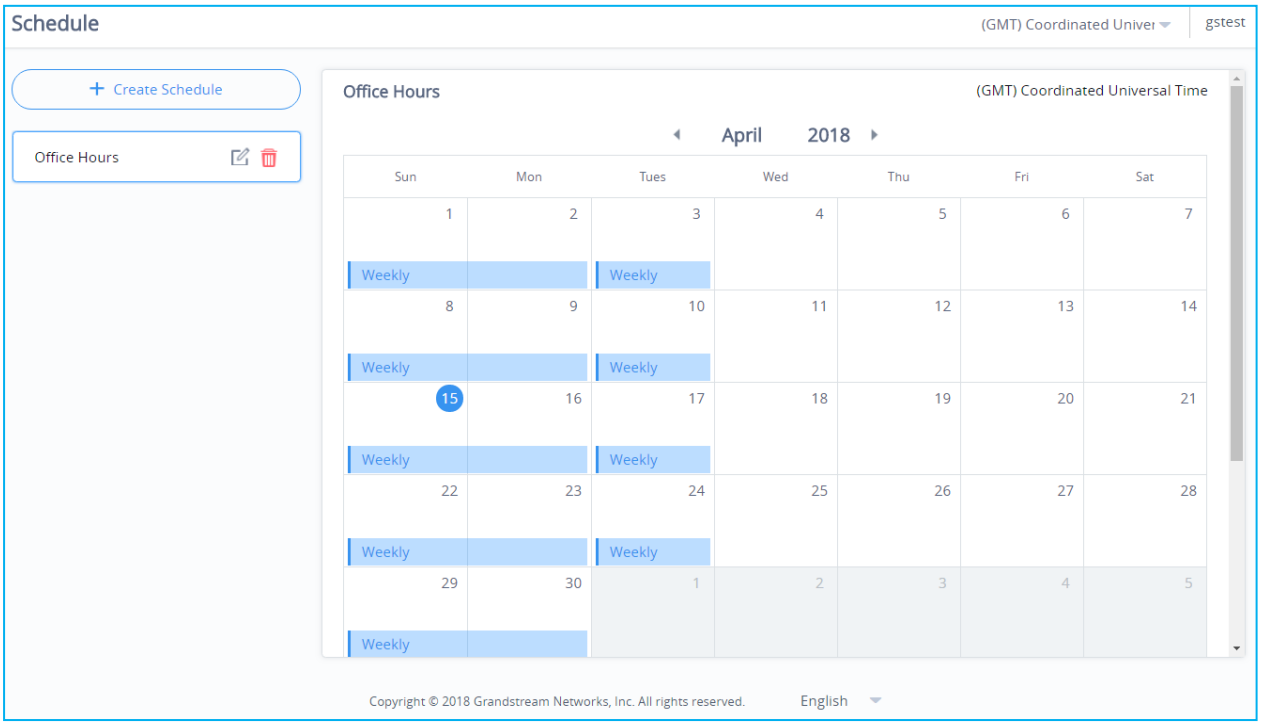


Figure 57: Schedules List

SYSTEM SETTINGS

Maintenance

Users can access Maintenance page from GWN7600/GWN7600LR WebGUI→**System Settings**→ **Maintenance**.

Basic

Basic page allows Country and Time configuration.

Table 17: 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.
Scene	Configure whether to enable/disable 5.150-5.350GHz (channels 36-64) for outdoor usage in order to follow some countries regulations. **Note:** - This option is only available for certain countries and only effective for outdoor type of access points. - This Option is only applicable for **GWN7600LR Only.**
Time Zone	Configure time zone for the GWN7600/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 18: 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 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(m)	Specify the time to check for firmware upgrade (in minutes).
Reboot	Click on Reboot button to reboot the device.
Download Configuration	Click on Download to download the device's configuration file.
Upload Configuration	Click on Upload to upload the device's configuration file.
Upgrade Now	Click on Upgrade, to launch firmware/config file provisioning. Please make sure to Save and Apply changes before clicking on Upgrade.
Factory Reset	Click on Reset to restore the GWN7600/GWN7600LR to factory default settings

Access

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

Table 19: 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.
New User Password	Configure the password for user-level Web GUI access. This field is case sensitive with a maximum length of 32 characters.
Confirm New User Password	Enter the new User password again to confirm.

Syslog

The syslog Web page provides configuration settings for syslog.

Table 20: Syslog Parameters

Field	Description
Syslog Server	Enter the IP address or URL of Syslog server.
Syslog Level	Select the level of Syslog, 5 levels are available: **None, Debug, Info, Warning** and **Error**.
Log DNS Queries	Check to log DNS Queries

Logserver

The logserver page allows the user to configure syslog server on GWN7600/GWN7600LR in order to save log messages on connected external USB drive.

First connect a USB drive to the Access point, then configure the parameters and make sure to start the server in order to collect messages from devices sending syslog to GWN.

Following table gives description for configuration parameters of GWN Logserver:

Option	Description
Logrotate File Size	Select the size of file to trigger rotation, if left empty, then the router will use only the Logrotate frequency rules to trigger rotation. Default is 5 M. Units can be M (Megabytes) or K (Kilobytes).
Logrotate File Count	Select the Maximum number of rotates files to keep. Default is 56 files.
Logrotate Mode	Choose the time rotation frequency mode (default every 3 hours). • Every X Minutes (0-59). • Every X hours (0-23) • X hour of day (0-23). • X day of week (Sunday-Saturday) + X hour of day (0-23).
Hours	Enter the number of hours period after which trigger file rotation.
Minutes	Enter the number of Minutes period after which trigger file rotation.
Hour of the day	Enter the hour of day at which trigger file rotation.
Day of the week	Enter Day of the week + hour of day, at which trigger file rotation.

Devices	Select the path (a USB partition) to store collected logs. Required.
Enable Logserver	Enables the logserver.

After setting up the logserver and saving the settings, users need to connect an USB external storage and press Start button in order to start collecting logs.

All log messages from all devices will be put on one single file, and the router will keep rotating and creating new files based on the configured rotation policy.

- Under **Syslog File List**, users can select a device and press **List** button to list all saved logs on this device.
- Press **Download** button to download a saved log.
- Press **Clear** button to remove logs.

Debug

GWN7600/GWN7600LR offers many features for managing and monitoring connected clients to SSIDs, as well as debugging and troubleshooting

Capture (GWN7600 Only)

This section is used to generate packet trace captures from SSIDs interfaces which will help to sniff packets within the SSID for troubleshooting purpose or monitoring. Users will need to plug a USB device to the USB port on the back of the GWN7600.

To access Capture page, go to **System Settings→Debug→Capture.**

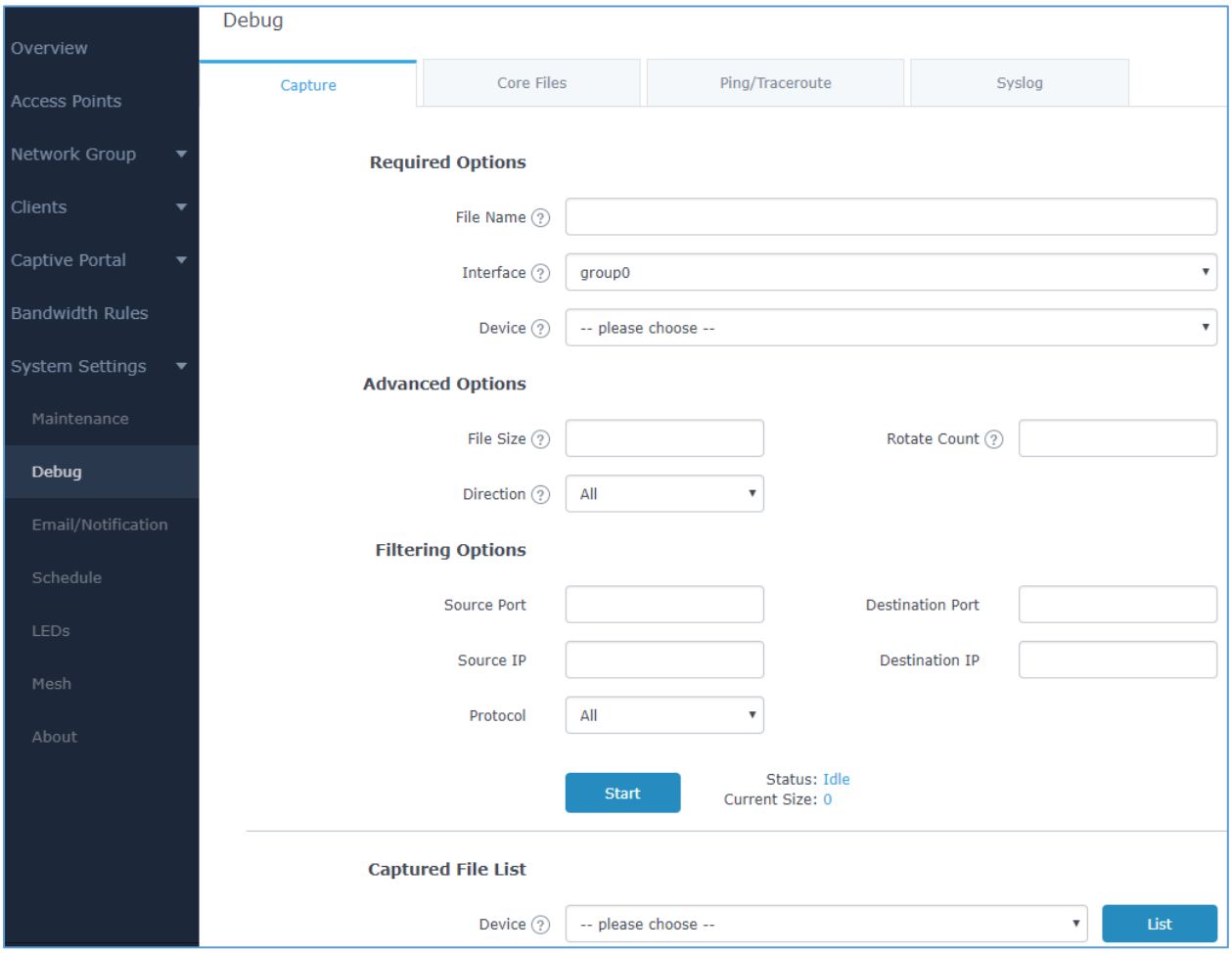


Figure 58: Capture Page

The below table will show different fields used on debug page:

Table 21: Debug

Required Options	
File Name	Enter the name of the capture file that will be generated.
Interface	Choose a SSID as Interface on which the traffic will be captured.
Device	Choose a device plugged to USB port to save the capture once started.
Advanced Options	
File Size	Set a File size that the capture will not exceed.
Rotate Count	Set a value for rotating captures.
Direction	Choose if you want to get all traffic or only outgoing or incoming to the chosen interface.

Filtering Options	
Source Port	Set the Source Port to filter capture traffic coming from the defined source port.
Destination Port	Set the Destination Port to filter capture traffic coming from the defined port.
Source IP	Set the Source IP to filter capture traffic coming from the defined source IP.
Destination IP	Set Destination IP to filter capture traffic coming from the defined destination IP.
Protocol	Choose ALL or a specific protocol to capture (IP, ARP, RARP, TCP, UDP, ICMP, IPv6)

Click on Start to start capturing on a certain device plugged to the USB port.

Click on Stop to stop the capture.

Click on List to show the captured files on a chosen device, users could check the capture files details.

Click on Clear to delete all files.

Click on next to a capture file to download it on a local folder.

Click on to delete the corresponding capture file.

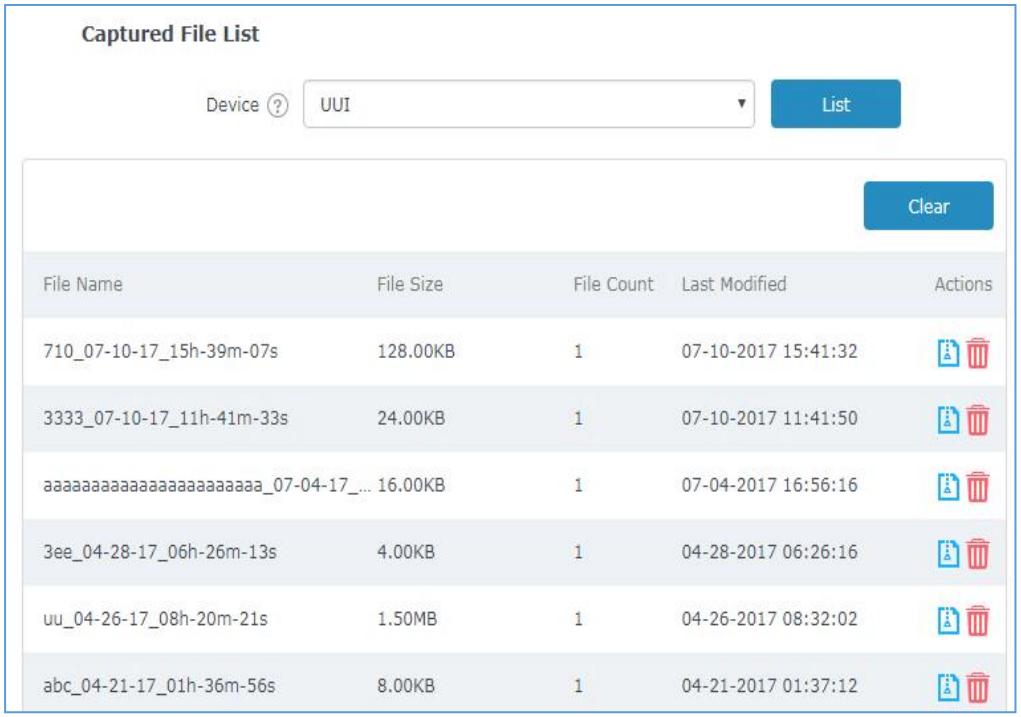


Figure 59: Capture Files

Core Files

The Core Files Web page displays core dumps generated when the GWN7600/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 GWN7600/GWN7600LR offers both Ping and Traceroute tools for IPv4 and IPv6 protocols.

To use these tools, go to GWN7600/GWN7600LR **WebGUI → System Settings → Debug → Ping/Traceroute.**

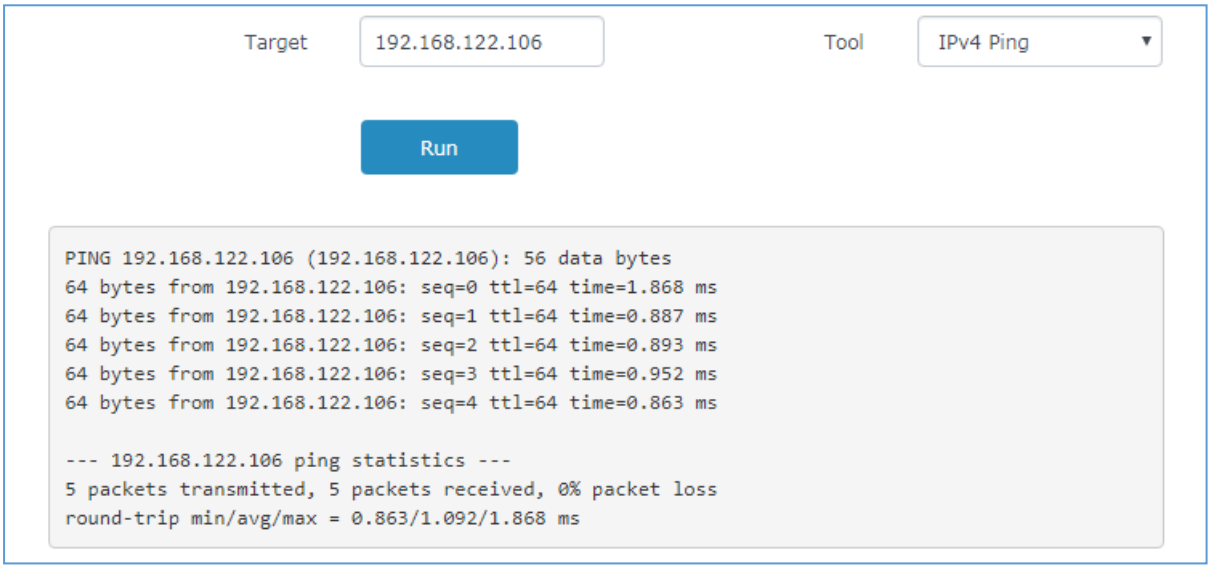


Figure 60: IP Ping

- 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**.

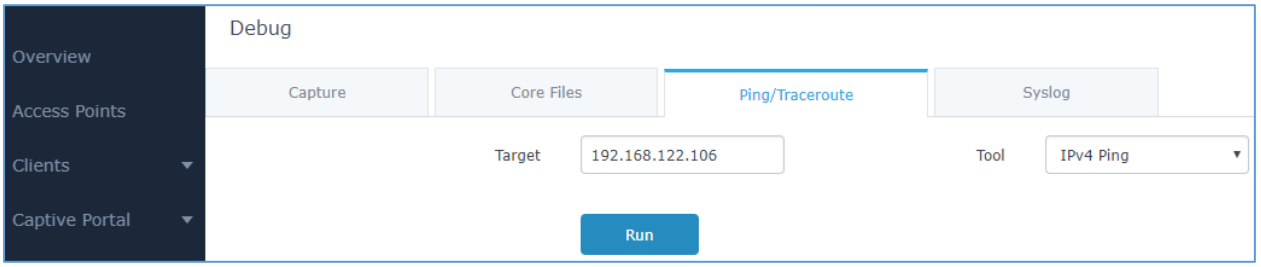


Figure 61: IP Traceroute

Syslog

The syslog Web page displays logs generated by the GWN7600/GWN7600LR for troubleshooting purpose as shown in figure below.

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

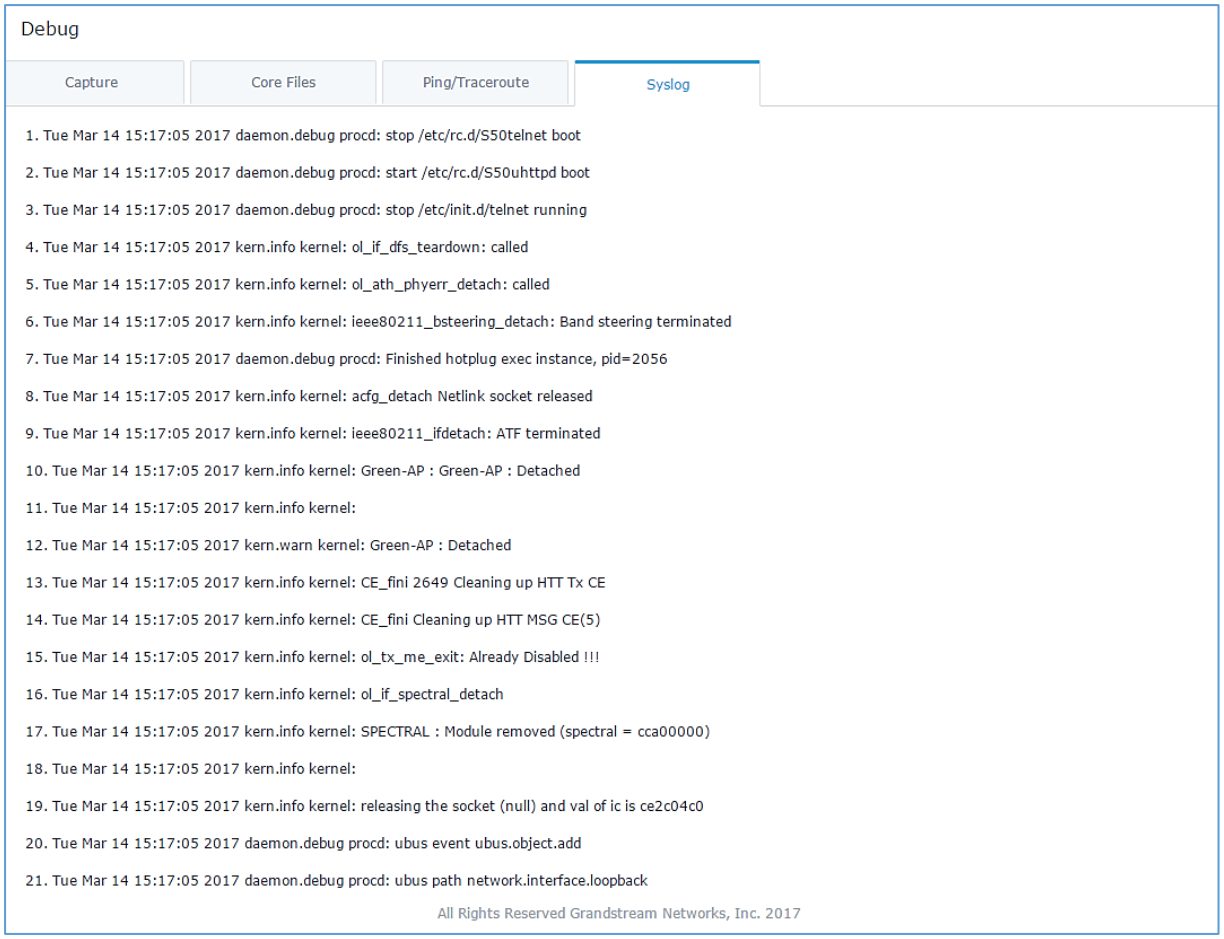


Figure 62: Syslog

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.

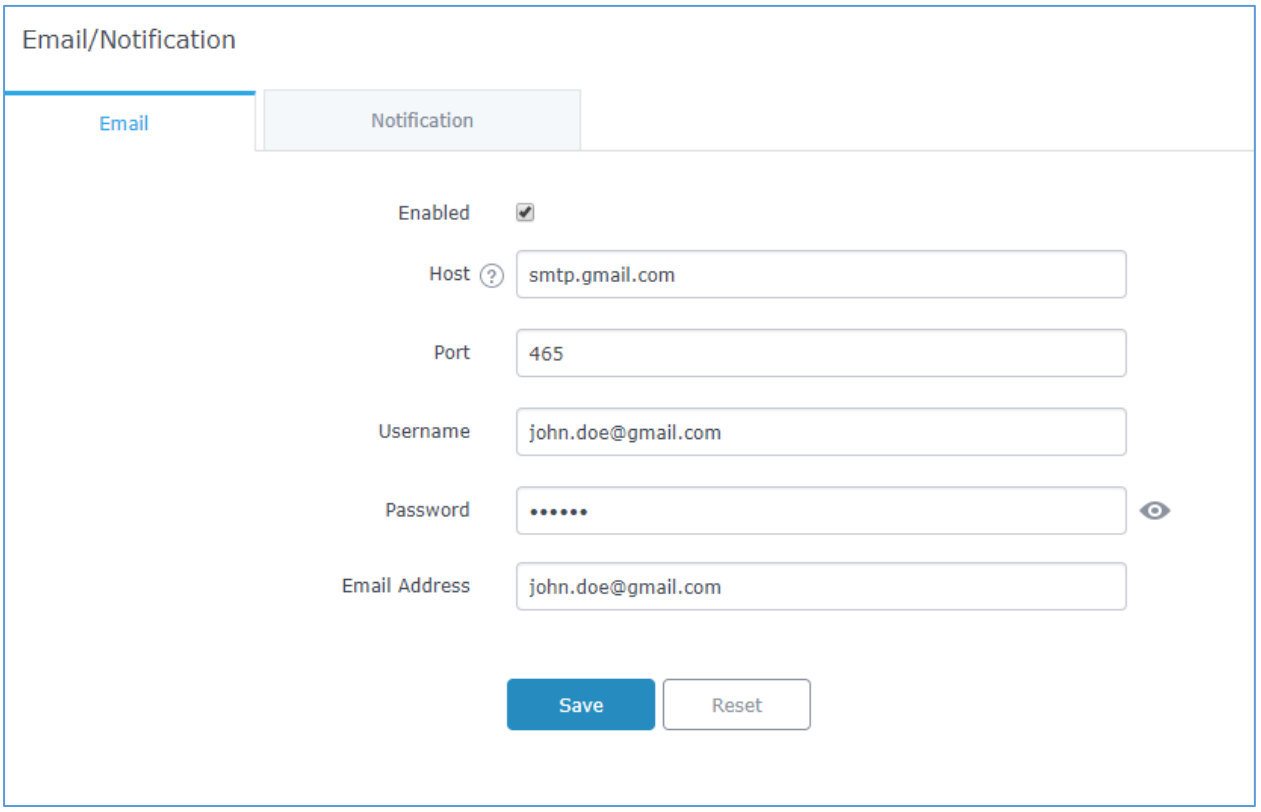


Figure 63: Email

Table 22: 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.

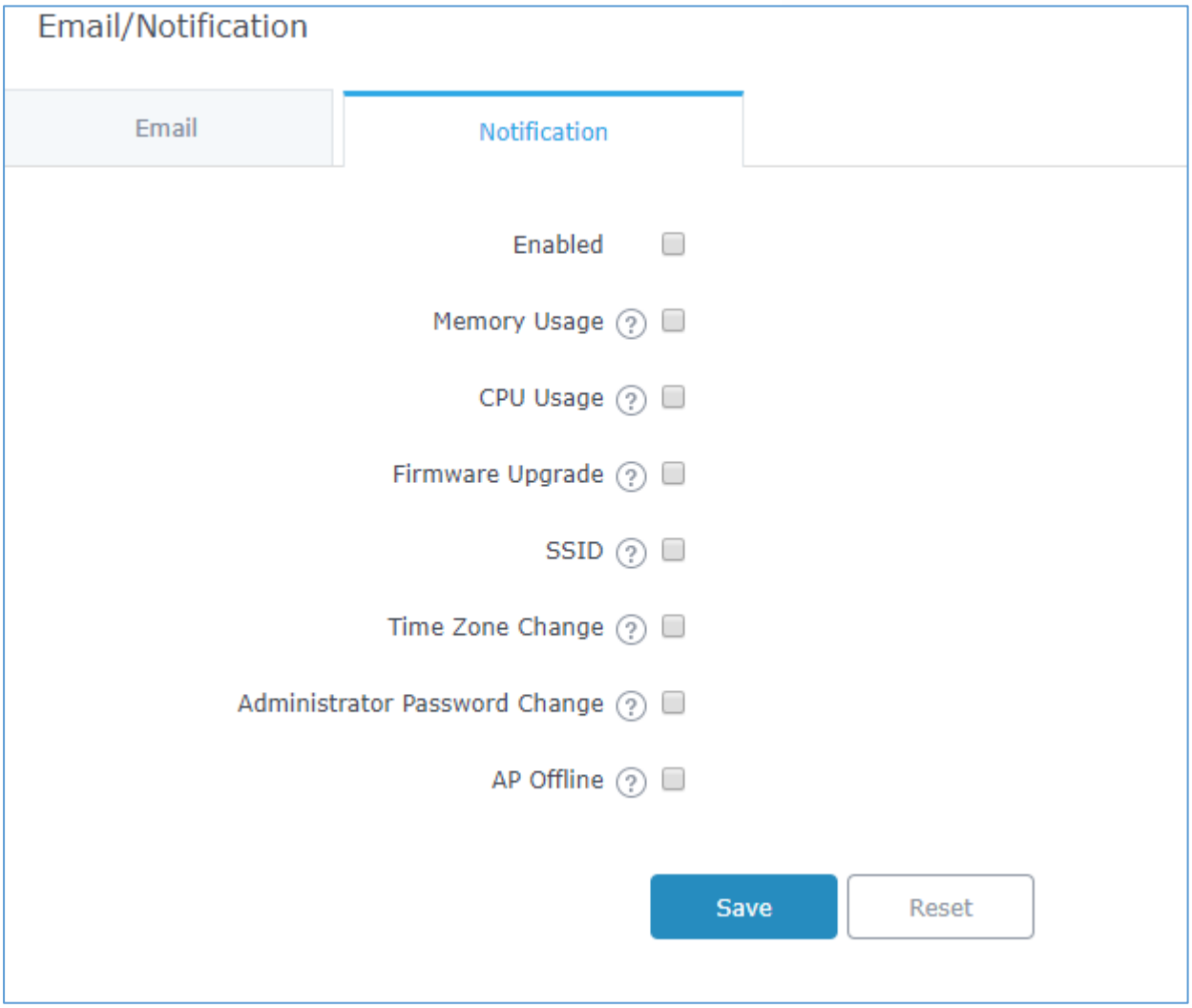


Figure 64: Notification

The following table describes the notifications configuration settings.

Table 23: 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.
SSID	Configures whether to send notification if any 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.

DHCP Sever

By default, GWN has DHCP relay, but users could create and manage multiple DHCP server pools which will be mapped to the SSID using Vlan tag, for example when creating a DHCP pool under "**System Settings → DHCP Server**" users need to set a VLAN ID and same one should be set under SSID in order to map the configured DHCP pool with the SSID. This way users could configure multiple SSIDs mapped to multiple VLANs on the network in which case they are isolated by layer 2 switching.

The table below summarizes the configuration parameters for DHCP server.

Table 24: DHCP Server Parameters

Field	Description
Name	Set the name of the DHCP Pool.
Enabled	Enable/Disable the DHCP pool.
VLAN ID	Set a VLAN ID, same one should be set on SSID settings to map it with the DHCP pool.
DHCP Server Static Address	Configure the static address of the DHCP server (through which GWN Master AP will be accessible).
DHCP Server Subnet Mask	Sets the subnet mask for the DHCP Pool.
DHCP Start Address	Set the start address for DHCP
DHCP End Address	Set the end address for DHCP
DHCP Leases Time	Set the DHCP lease time for the clients (default 12h).
DHCP Options	Add the Option items for DHCP, detailed option contents can be found via: https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq

DHCP Gateway	Set the gateway for DHCP, and it is better to set the gateway, should be different that the static IP of the access point and on the same subnet.
DHCP Preferred DNS	Set the preferred DNS for DHCP
DHCP Alternated DNS	Set the alternated DNS for DHCP

UPGRADING AND PROVISIONING

Upgrading Firmware

The GWN7600/GWN7600LR can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN7600/GWN7600LR.

Upgrading via Web GUI

The GWN7600/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**.

Table 25: Network Upgrade Configuration

Field	Description
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 GWN7600/GWN7600LR is being paired as slave using another GWN7600/GWN7600LR Access Point acting as Controller, users can upgrade their paired access points from the GWN7600/GWN7600LR Master Controller.

To upgrade a slave access point, log in to the GWN7600/GWN7600LR acting as Master Controller and go to **Access Points.**

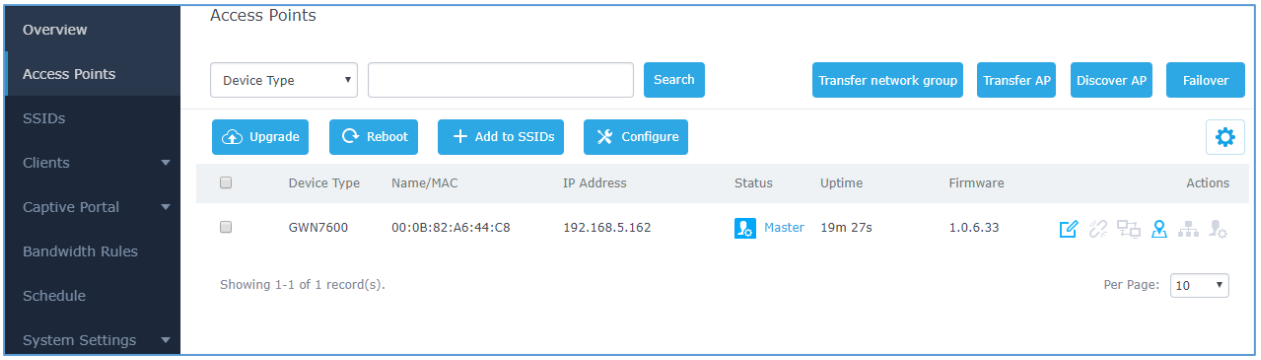


Figure 65: Access Points

Make sure that firmware server path is set correctly under Maintenance, check the desired APs to upgrade, and click on  to upgrade the selected paired access points.

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

⚠ **Notes:**

- Please do not interrupt or power cycle the GWN7600/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 GWN7600/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 GWN7600/GWN7600LR web configuration interface;
5. Configure the Firmware Server to the IP address of the PC;
6. Update the changes and reboot the GWN7600/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 GWN7600/GWN7600LR configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GWN7600/GWN7600LR when necessary.

Download Configuration

Users can download the GWN7600/GWN7600LR configuration for restore purpose under **Web GUI→System Settings→Maintenance→Upgrade**.

Click on Download to download locally the configuration file.

Upload Configuration

Users can upload configuration file to the GWN7600/GWN7600LR under **Web GUI→System Settings→Maintenance→Upgrade**.

Click on Upload to browse for the configuration to upload.

Please note that the GWN7600/GWN7600LR will reboot after the configuration file is restored successfully.

Configuration Server (Pending)

Users can download and provision the GWN7600/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 in order for the GWN7600/GWN7600LR to be provisioned with that config server file.

Reset and reboot

- Users 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 GWN7600/GWN7600LR itself to factory settings.

Syslog

On the GWN7600/GWN7600LR, users could dump the syslog information to a remote server under **Web GUI→System Settings→Maintenance**. Enter the syslog server hostname or IP address and select the level for the syslog information. Five levels of syslog are available: None, Debug, Info, Warning, and Error.

EXPERIENCING THE GWN7600/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 GWN7600/GWN7600LR Wireless Access Point, it will be sure to bring convenience and color to both your business and personal life