Grandstream Networks, Inc.

GWN7602

Mid-Tier 802.11ac Wi-Fi 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 to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with 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

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.
This transmitter must not be co-located or operating in conjunction with any other antenna transmitter.

ISEDC Warning

This device complies with Innovation, Science, and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISEDC Warning

This equipment complies with ISEDC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Cet équipement est conforme aux ISEDC RF limites d'exposition aux radiations dans un environnement non contrôlé. Cet émetteur ne doit pas être situé ou opérant en conjonction avec une autre antenne ou émetteur.

CE Warranty
Frequency;
2.4G Wi-Fi: 2412-2472MHz;
5G Wi-Fi: 5150-5250MHz;
Output power:
2.4G Wi-Fi:
802.11b: 18.23dBm;
802.11g: 18.96dBm;
802.11n20: 18.69dBm;
802.11n40: 18.38dBm.
5G Wi-Fi:
802.11a: 21.24dBm;
802.11n20: 21.27dBm;
802.11n40: 22.13dBm;
802.11ac: 21.19dBm;
802.11ac40: 22.16dBm;
802.11ac80: 22.22dBm.

GNU GPL INFORMATION

GWN7602 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 GWN7602 in standalone mode, Or as a slave with Master GWN76XX Access points. The intended audiences of this document are network administrators. Please visit http://www.grandstream.com/support to download the latest "GWN7602 User Manual".

This guide covers following topics:

- Product Overview
- Installation
- Getting Started
- Using GWN7602 as Standalone Access Point
- Managing GWN7602 from a master GWN76xx
    - SSIDs
    - Clients Configuration
    - Captive Portal
    - Vouchers
    - Mesh Network
    - Bandwidth Rules
    - DHCP Server
    - Schedule
    - LED Schedule
- Upgrading and Provisioning
- Managing GWN7602 From GWN.Cloud
- Experiencing the GWN7602 Wireless Access Point

CHANGE LOG

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

Firmware Version 0.12.25.1

- This is the initial version of GWN7602.

WELCOME

Thank you for purchasing Grandstream GWN7602 Mid-Tier 802.11ac Wi-Fi Access Point.

The GWN7602 is an 802.11ac wireless access point. It offers dual-band 2x2:2 technology and a sophisticated antenna design for ideal network throughput and Wi-Fi coverage range. Three 100M Ports provide IP Phones, IPTV, PC and etc. with Ethernet, and an uplink Gigabit network port with PoE/PoE+. To ensure easy installation and management, the GWN7602 supports to be managed by GWN series APs (except GWN7602) with embedded controller or GWN.Cloud Management System. With support for advanced QoS, low-latency real-time applications, up to 80 client devices, combining with the features of Mesh, Captive Portal, the GWN7602 is an ideal wireless access point for small sized business, coffee shops, restaurants, and hotel deployments.

PRODUCT OVERVIEW

Technical Specifications

Table 1: GWN7602 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac
Antennas	2 dual band internal antennas. Antenna 1 - 2.4GHz: gain 3.0dBi, 5GHz: gain 3.5dBi Antenna 2 - 2.4GHz: gain 3.5dBi, 5GHz: gain 3.0dBi
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 867Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps 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	2.4 GHz Radio: 2412 – 2484 GHz 5 GHz Radio: 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20, 40, 80 MHz
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise.
MIMO	4x4:4 2.4GHz (MIMO) 4x4:4 5GHz (MU-MIMO)
Coverage Range	Up to 100 meters **coverage range can vary based on environment*
Maximum TX Power	2.4G: 21 dBm 5G: 21 dBm **Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b:-96dBm@1Mbps,-88dBm@11Mbps;802.11g:-93dBm@6Mbps, -76dm@54Mbps; 802.11n20MHz:-92dBm@MCS0,-73dBm@MCS7;802.11n40MHz: -88.5dBm@MCS0,-71dBm@MCS7

	5G 802.11a: -91dBm@6Mbps, -73.5dBm@54Mbps; 802.11ac:VHT20: -89.5dbm@MCS0, -71.5dBm@ MCS7, -64dBm@MCS8; VHT40: -87.5dBm@MCS0; -69.5dBm@MCS7, -62dBm@MCS9, VHT80: -83.5dBm@MCS0, -65.5dBm@MCS7, -58.5dBm@MCS9 ** Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	4 SSIDs
Concurrent Clients	Up to 80.
Network Interfaces	1 x 10/100/1000M uplink Ethernet port with POE/POE+ 2 x 10/100M Ethernet port with PSE 1 x 10/100M Ethernet port
Auxiliary Ports	1x Reset Pinhole
Mounting	Wall mountable
LEDs	1x tri-color LEDs for device tracking and status indication
Network Protocols	IPv4/IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
Network Management	GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN.Manager offers premise-based software controller for up to 3,000 GWN APs
Power and Green Energy Efficiency	Support 802.3az; PoE 802.3af/ 802.3at PSE max output per port: 6W; Max Consumption: 20 W
Environmental	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10％ to 90% Non-condensing
Physical	Unit Dimension:135 x 115 x 30mm; Unit Weight: 188g Entire Package Dimension: 171 x 140 x 33mm; Entire Package Weight: 278.5g
Package Content	GWN7602 802.11ac Wireless AP, Quick Start Guide
Compliance	FCC, CE, RCM, IC

INSTALLATION

Before deploying and configuring the GWN7602, 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 GWN7602.

Equipment Packaging

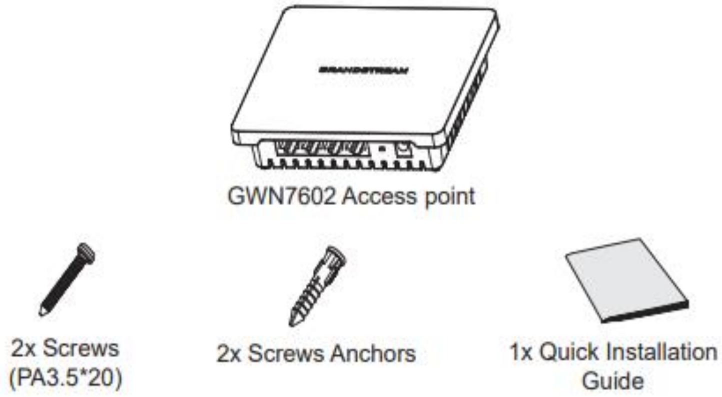


Figure 1: GWN7602 Equipment Packaging

Table 2: GWN7602 AP Ports Description

Port	Description
DC12V	Power adapter connector (12V, 2A)
PoE	Ethernet RJ45 port (10/100/1000Mbps) supporting PoE/PoE+.
LAN1	1x 10/100M Ethernet port.
LAN2/LAN3	2x 10/100M Ethernet ports with PSE.
RESET	Factory reset pinhole. Press for 7 seconds to reset factory default settings.

Power and Connect GWN7602 Access Point

The GWN7602 can be powered either using the right PSU (DC12V, 2A) or using a PoE/PoE+ switch:

- **Option A:** Power Adapter to AC outlet.
- **Option B:** RJ45 Ethernet Cable to PoE/PoE+ switch

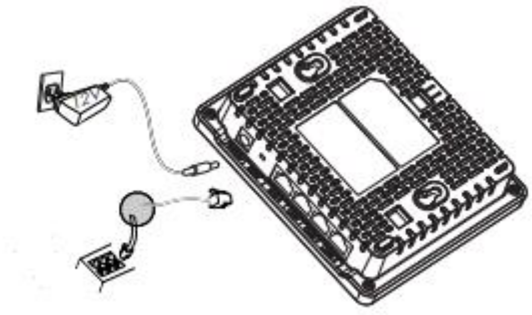


Figure 2: Connecting GWN7602

Warranty

If the GWN7602 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 an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.

Wall Mount Installation

GWN7602 can be mounted on the wall. Please refer to the following steps for the appropriate installation.

Step1:

Use a measuring tape to measure the distance between the two wall mount slots on the back of the GWN7602 access point and use a pencil to mark the mounting screw holes on the wall.

Step 2:
Drill the holes in the spots that you have marked and slide the anchors into the wall. Attach the GWN7602 access point to the wall via the wall mount slots.

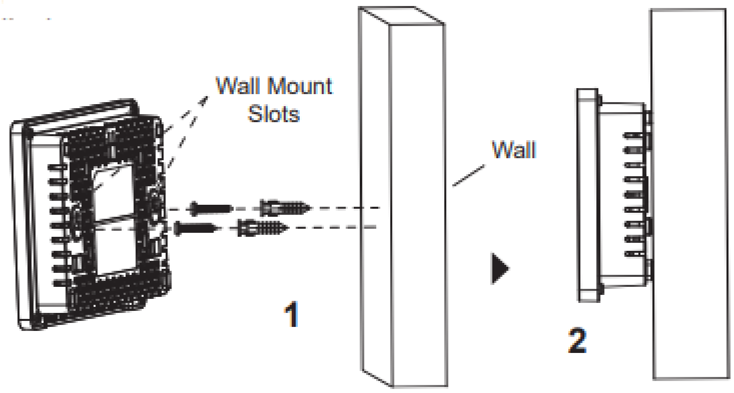


Figure 3: Wall Mount – Steps 1 & 2

GETTING STARTED

The GWN7602 Wi-Fi Access Could only be managed via another GWN76XX Master AP (Except GWN7602), Or through the GWN.Cloud platform for easy management and deployment.

This section provides step-by-step instructions on how to read LED patterns, and discover the GWN7602.

LED Patterns

The panel of the GWN7602 has different LED patterns for different activities, to help users read the status of the GWN76XX whether it is powered up correctly, provisioned, in upgrading process and more, for more details please refer to the below table.

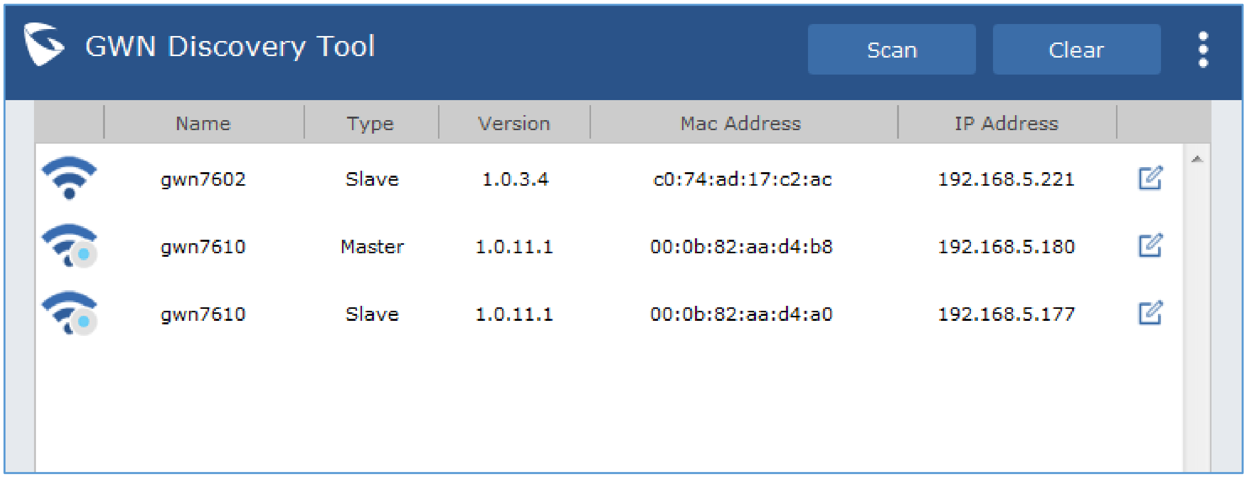
Table 3: LED Patterns

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 paired slave - Factory reset initiated.
Solid red	Firmware update failed.
Solid purple	Unit not provisioned.
Blinking blue	Unit provisioning in progress.
Solid blue	Unit is provisioned successfully.
Blinking White	Used for Access Point location feature

Discovering the GWN7602

Once the GWN7602 is powered up and connected to the Network correctly, users can discover the GWN7602 using GWN Discovery Tool as described in below steps:

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 GWN76XX Access Points connected on the network showing their MAC, IP addresses and firmware version.



Name	Type	Version	Mac Address	IP Address
gwn7602	Slave	1.0.3.4	c0:74:ad:17:c2:ac	192.168.5.221
gwn7610	Master	1.0.11.1	00:0b:82:aa:d4:b8	192.168.5.180
gwn7610	Slave	1.0.11.1	00:0b:82:aa:d4:a0	192.168.5.177

Figure 4: GWN Discovery Tool

USING GWN7602 AS STANDALONE ACCESS POINT

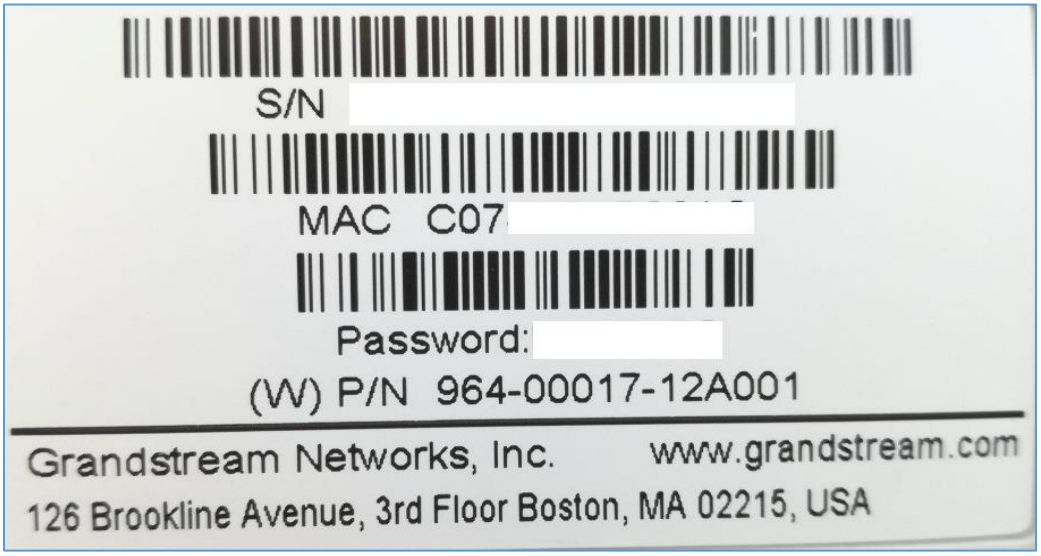
The GWN76XX can be used in Standalone mode, or in Slave mode where managed by another GWN76XX Master, Or GWN Cloud platform.
This section will describe how to use the GWN7602 in standalone mode.

Connect to GWN7602 Default Wi-Fi Network

GWN76XX can be used as standalone access point out of box, or after factory reset with Wi-Fi enabled by default.

After powering the GWN7602 and connecting it to the network, GWN7602 will broadcast a default SSID based on its MAC address **GWN [MAC's last 6 digits]** and a random password.

Note that GWN76XX's default SSID and password information are printed on the MAC tag of the unit as shown on the below figure.



S/N [redacted]

MAC C07[redacted]

Password: [redacted]

(W) P/N 964-00017-12A001

Grandstream Networks, Inc. www.grandstream.com

126 Brookline Avenue, 3rd Floor Boston, MA 02215, USA

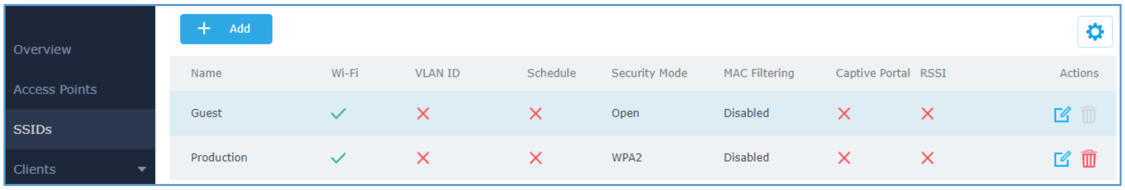
Figure 5: MAC Tag Label

MANAGING GWN7602 FROM A MASTER GWN76XX

SSID

When using GWN7602 as Slave Access Point, users can create different SSIDs from the GWN76XX Master and assign GWN7602 Slave Access Points to them.

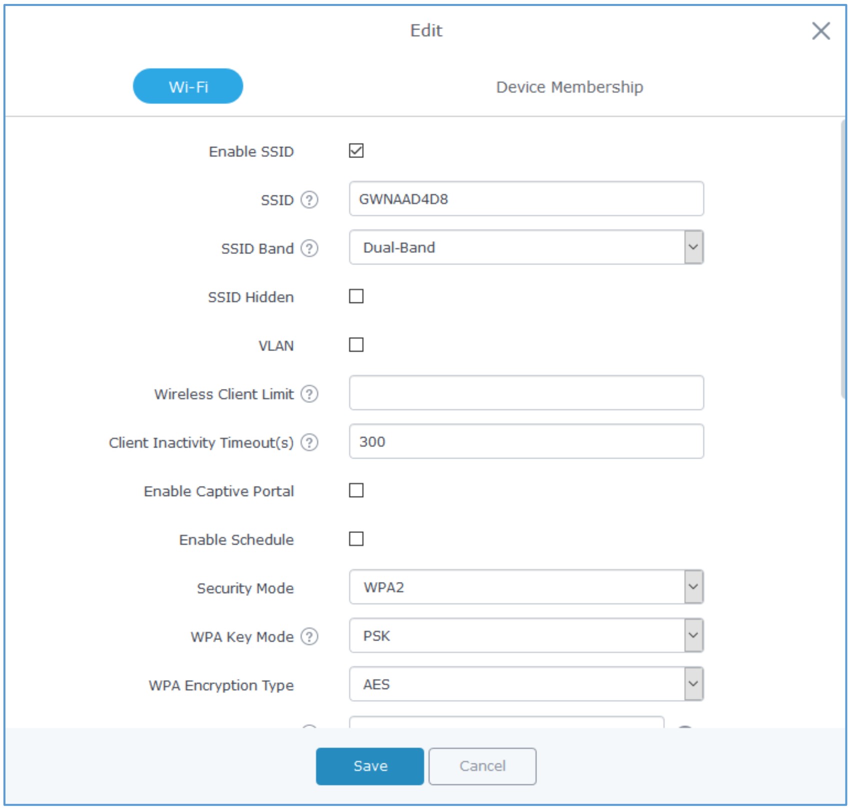
Log in as Master to the GWN76XX WebGUI and go to **SSIDs.**



Name	Wi-Fi	VLAN ID	Schedule	Security Mode	MAC Filtering	Captive Portal	RSSI	Actions
Guest	✓	✗	✗	Open	Disabled	✗	✗	
Production	✓	✗	✗	WPA2	Disabled	✗	✗	

Figure 6: SSID

GWN7602 can support up to 4 SSIDs, click on ⊕ Add to add a new SSID.



Enable SSID	☑
SSID	GWNAAD4D8
SSID Band	Dual-Band
SSID Hidden	☐
VLAN	☐
Wireless Client Limit	
Client Inactivity Timeout(s)	300
Enable Captive Portal	☐
Enable Schedule	☐
Security Mode	WPA2
WPA Key Mode	PSK
WPA Encryption Type	AES

Figure 7: 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 4: 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 is 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.
Client Inactivity Timeout(s)	AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default. Range from 60-3600 seconds.
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.

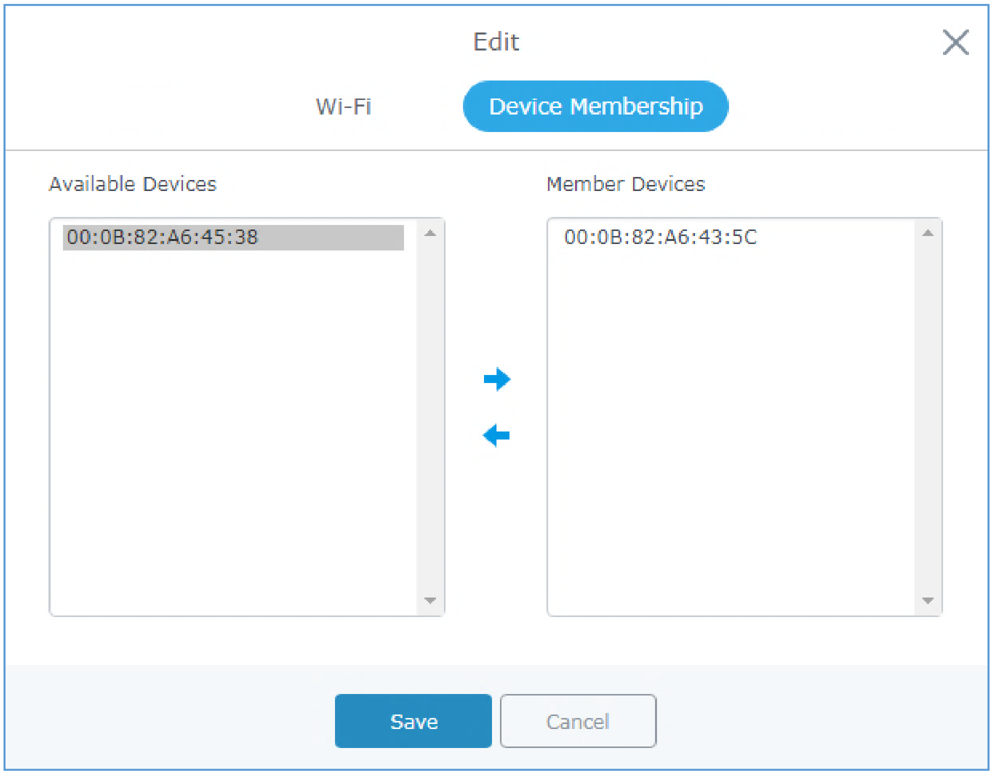
WEP Key	Enter the password key for WEP protection mode. *This field is available only when “Security Mode” is set to “WEP 64-bit” or “WEP 128-bit”.*
WPA Key Mode	Two modes are available: • **PSK:** Use a pre-shared key to authenticate to the Wi-Fi. • **802.1X:** Use a RADIUS server to authenticate to the Wi-Fi. *This field is available only when “Security Mode” is set to “WPA/WPA2” or “WPA2”.*
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. *This field is available only when “Security Mode” is set to “WPA/WPA2” or “WPA2”.*
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. *This field is available only when “Security Mode” is set to “WPA/WPA2” or “WPA2”.*
RADIUS Sever Address	Configures RADIUS authentication server address. *This field is available only when “WPA Key Mode” is set to “802.1x”.*
RADIUS Server Port	Configures RADIUS Server Listening port. Default is: 1812. *This field is available only when “WPA Key Mode” is set to “802.1x”.*
RADIUS Server Secret	Enter the secret password for client authentication with RADIUS server. *This field is available only when “WPA Key Mode” is set to “802.1x”.*
RADIUS Accounting Server	Configures the address for the RADIUS accounting server. *This field is available only when “WPA Key Mode” is set to “802.1x”.*
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port. Defaults to 1813. *This field is available only when “WPA Key Mode” is set to “802.1x”.*
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server. *This field is available only when “WPA Key Mode” is set to “802.1x”.*

RADIUS NAS ID	Enter the RADIUS NAS ID. *This field is available only when "WPA Key Mode" is set to "802.1x".*
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 Wi-Fi connection to the LAN ports transparently. Once a SSID has a Client Bridge Support enabled, the AP adopted in this SSID can be turned in to Bridge Client mode by click the Bridge button.
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.
Enable Dynamic VLAN	When enabled, clients will be assigned IP address from corresponding VLAN configured on the RADIUS user profile. *This field is available only when "WPA Key Mode" is set to "802.1x".*
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76XX's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available: • **Radio Mode:** Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76XX but they cannot communicate with each other. • **Internet Mode:** Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76XX. • **Gateway MAC Mode:** Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76XX access points.
Minimum Access Rate Limit	Specify whether to limit the minimum access rate for clients. When enabled, it will help to eliminate the legacy connection which slow the total performance of the Wi-Fi network. Range from 1 to 54 Mbps.

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".
Beacon Interval	Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp… • **Using High Beacon Interval:** AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save Wi-Fi clients energy consumption. • **Using Low Beacon Interval:** AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by Wi-Fi clients with weak signal. **Notes:** 1. When AP enables several SSIDs with different interval values, the max value will take effect. 2. When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. 3. When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. 4. When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500. 5. Mesh feature will take up a share when it is enabled. Default value is 100ms. Valid range: 40 – 500 ms.

DTIM Period	Configures the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Default value is 1, meaning that AP will have DTIM broadcast every beacon. If set to 10, AP will have DTIM broadcast every 10 beacons. Valid range: 1 – 10.
Multicast to Unicast	Once selected, AP will convert multicast streams into unicast streams over the wireless link. Which helps to enhance the quality and reliability of video/audio stream and preserve the bandwidth available to the non-video/audio clients.
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. *This field is available only when “Security Mode” is set to “WPA/WPA2” or “WPA2”.*
Enable 11R	Check to enable 802.11r. *This field is available only when “Security Mode” is set to “WPA/WPA2” or “WPA2”.*
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
ARP Proxy	This option will enable GWN AP to answer the ARP requests from its LAN for its connected Wi-Fi clients. This is mainly to reduce the airtime consumed by ARP Packets

- **Device Membership**: Used to add or remove paired access points to the SSID.



Available Devices: 00:0B:82:A6:45:38

Member Devices: 00:0B:82:A6:43:5C

Figure 8: Device Membership

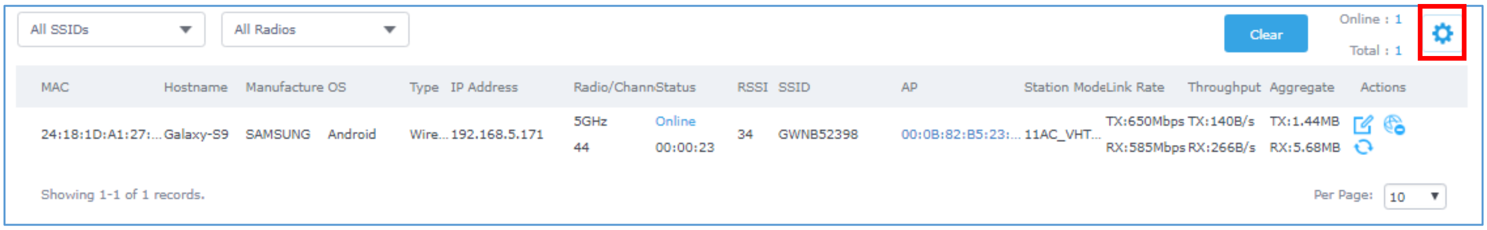
Click on → to add the GWN76XX to the SSID or click on ← to remove it.

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 GWN7602 from the master GWN76XX Web GUI **Clients → Clients** to perform different actions to wireless clients.



MAC	Hostname	Manufacture	OS	Type	IP Address	Radio/Chann	Status	RSSI	SSID	AP	Station Mode	Link Rate	Throughput	Aggregate	Actions
24:18:1D:A1:27:...	Galaxy-S9	SAMSUNG	Android	Wire...	192.168.5.171	5GHz 44	Online 00:00:23	34	GWNB52398	00:0B:82:B5:23:...	11AC_VHT...	TX:650Mbps RX:585Mbps	TX:140B/s RX:266B/s	TX:1.44MB RX:5.68MB	

Showing 1-1 of 1 records.

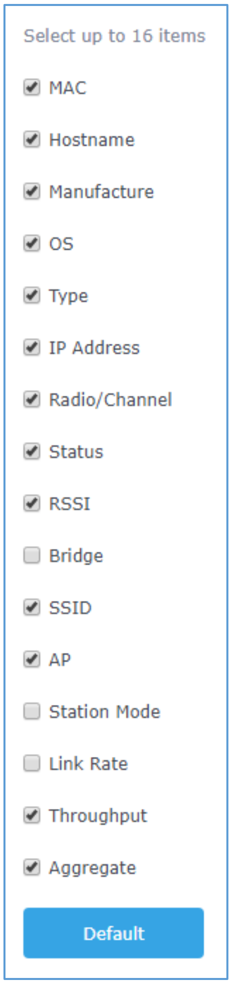
Per Page: 10

Figure 9: 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.
- Click on ⟳ to release Wi-Fi offline client IP lease.

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



Select up to 16 items

☑ MAC

☑ Hostname

☑ Manufacture

☑ OS

☑ Type

☑ IP Address

☑ Radio/Channel

☑ Status

☑ RSSI

☐ Bridge

☑ SSID

☑ AP

☐ Station Mode

☐ Link Rate

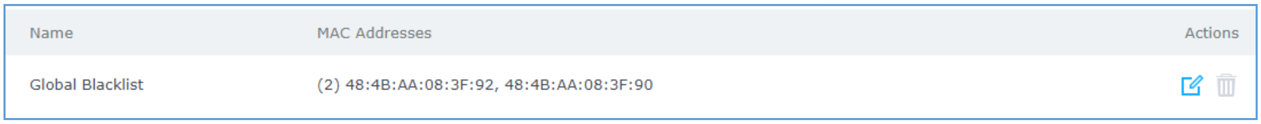
☑ Throughput

☑ Aggregate

Figure 10: Clients - Select Items

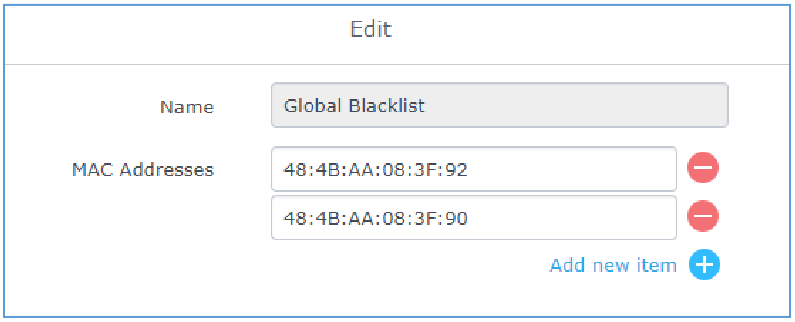
Clients Access

From this menu, users can manage in global way the blacklist of clients that will be blocked from accessing the Wi-Fi network, click on Client Access to add or remove MAC addresses of client from global blacklist.



Name	MAC Addresses	Actions
Global Blacklist	(2) 48:4B:AA:08:3F:92, 48:4B:AA:08:3F:90	✎ 🗑

Figure 11: Global Blacklist



Edit

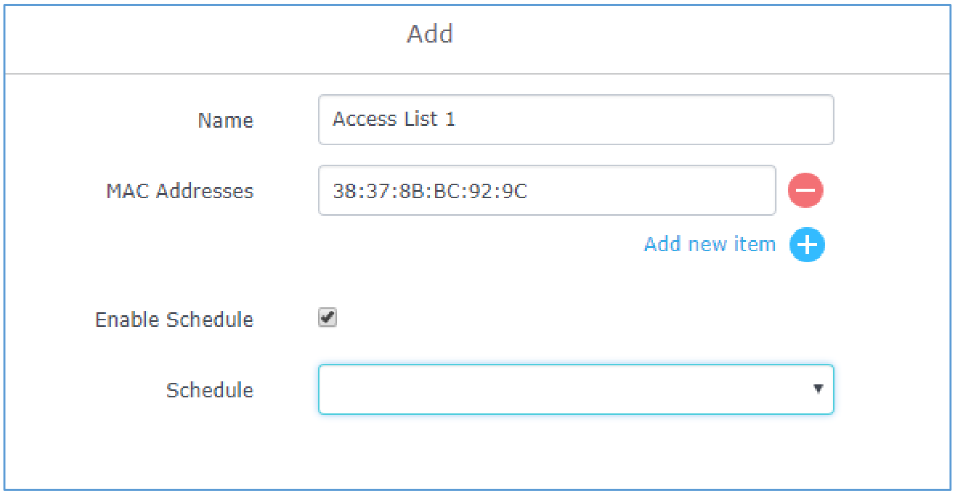
Name: Global Blacklist

MAC Addresses: 48:4B:AA:08:3F:92 ⊖
48:4B:AA:08:3F:90 ⊖

Figure 12: 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 Wi-Fi network.

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



Add

Name: Access List 1

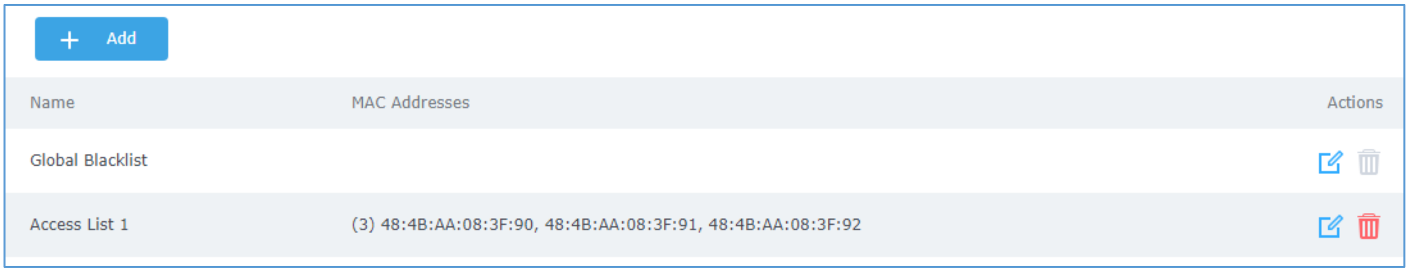
MAC Addresses: 38:37:8B:BC:92:9C ⊖

Enable Schedule ☑

Schedule: ▾

Figure 13: Adding Client Access List

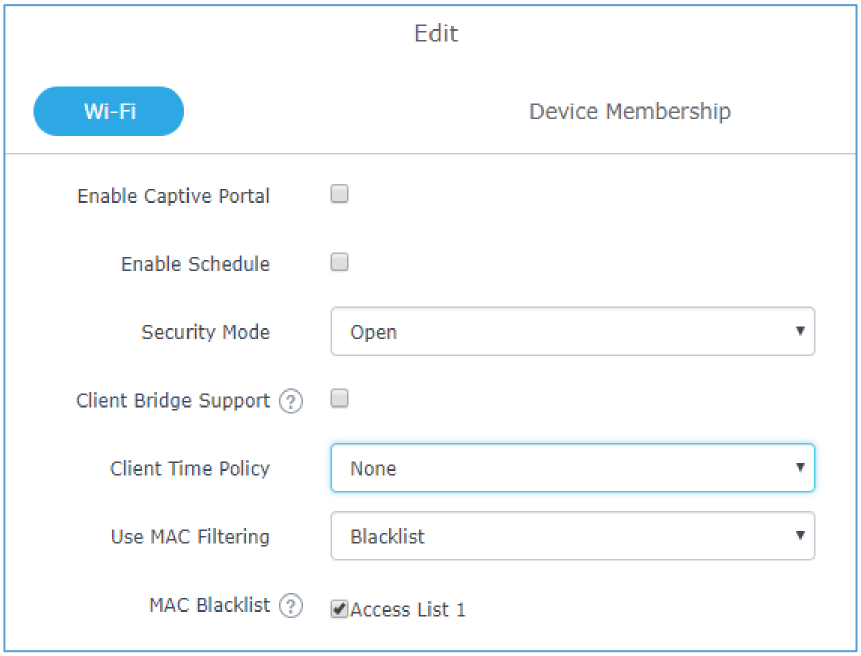
Users can check « Enable Schedule » to assign a schedule for the list when it will take effect.



Name	MAC Addresses	Actions
Global Blacklist		✎ 🗑
Access List 1	(3) 48:4B:AA:08:3F:90, 48:4B:AA:08:3F:91, 48:4B:AA:08:3F:92	✎ 🗑

Figure 14: Adding New Access List

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



Edit

Enable Captive Portal □

Enable Schedule □

Security Mode: Open

Client Bridge Support □

Client Time Policy: None

Use MAC Filtering: Blacklist

MAC Blacklist: ☑ Access List 1

Figure 15: 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 Wi-Fi and reconnect type and value after which they will be allowed to connect back after they have been disconnected.

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

Table 5: Time Policy Parameters

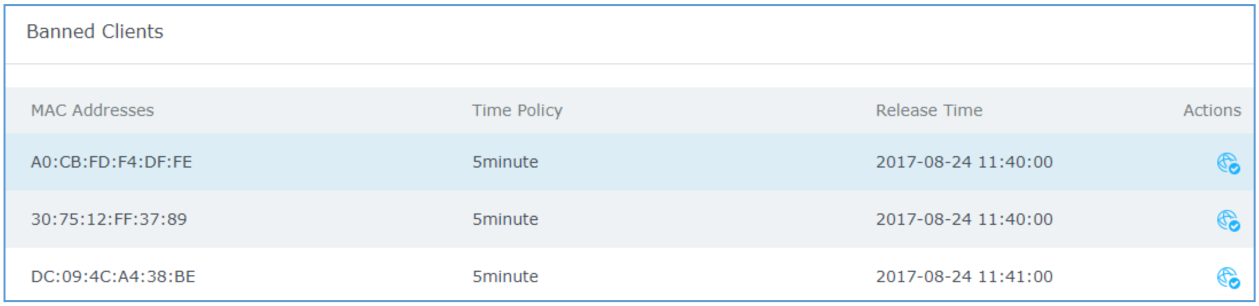
Option	Description
Name	Enter the name of the policy
Enabled	Check the box to enable the policy
Limit Client Connection Time	Sets amount of time a client may be connected.
Client Reconnect Timeout Type	Select the method with which we will reset a client's connection timer so they may reconnect again. 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.
Day of the Week	If "Reset Weekly" is selected, this is the day when the reset will be applied.
Hour of the Day	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 🌐 .



Banned Clients

MAC Addresses	Time Policy	Release Time	Actions
A0:CB:FD:F4:DF:FE	5minute	2017-08-24 11:40:00	🌐
30:75:12:FF:37:89	5minute	2017-08-24 11:40:00	🌐
DC:09:4C:A4:38:BE	5minute	2017-08-24 11:41:00	🌐

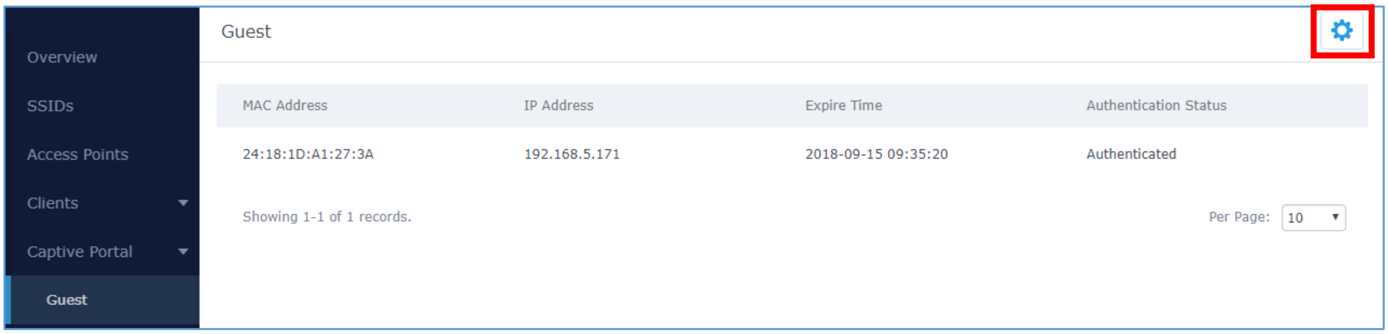
Figure 16: Ban/Unban Client

Captive Portal

Captive Portal feature on GWN7602 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 GWN7602 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 Master GWN76XX Web page under "Captive Portal". The page contains following sub-menus: **Guest**, **Policy List**, **Splash Page** and **Vouchers**.

Guest

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



Guest

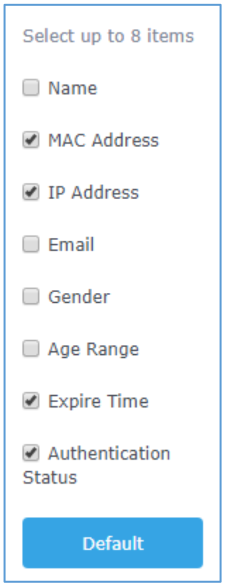
MAC Address	IP Address	Expire Time	Authentication Status
24:18:1D:A1:27:3A	192.168.5.171	2018-09-15 09:35:20	Authenticated

Showing 1-1 of 1 records.

Per Page: 10

Figure 17: Captive Portal – Guest Page

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



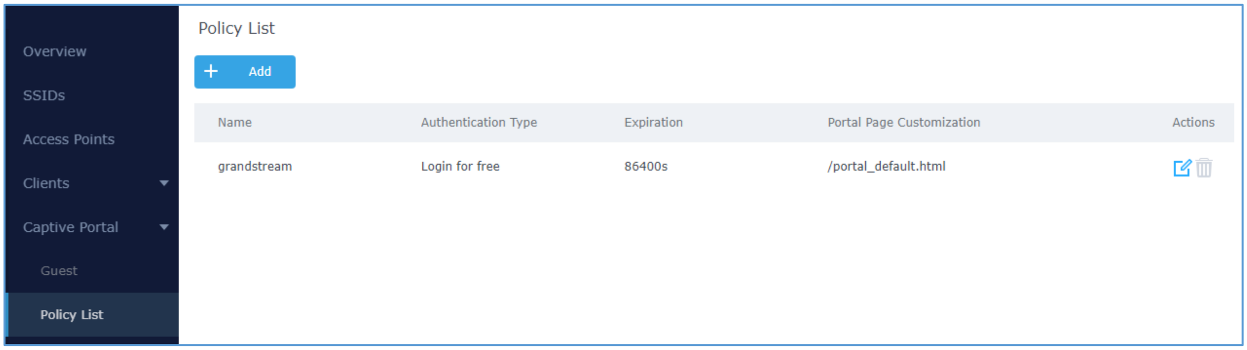
Select up to 8 items

- □ Name
- ☑ MAC Address
- ☑ IP Address
- □ Email
- □ Gender
- □ Age Range
- ☑ Expire Time
- ☑ Authentication Status

Figure 18: Captive Portal - Guest Page - Select Items

Policy List

Users can customize a portal policy in this page.



Policy List

+ Add

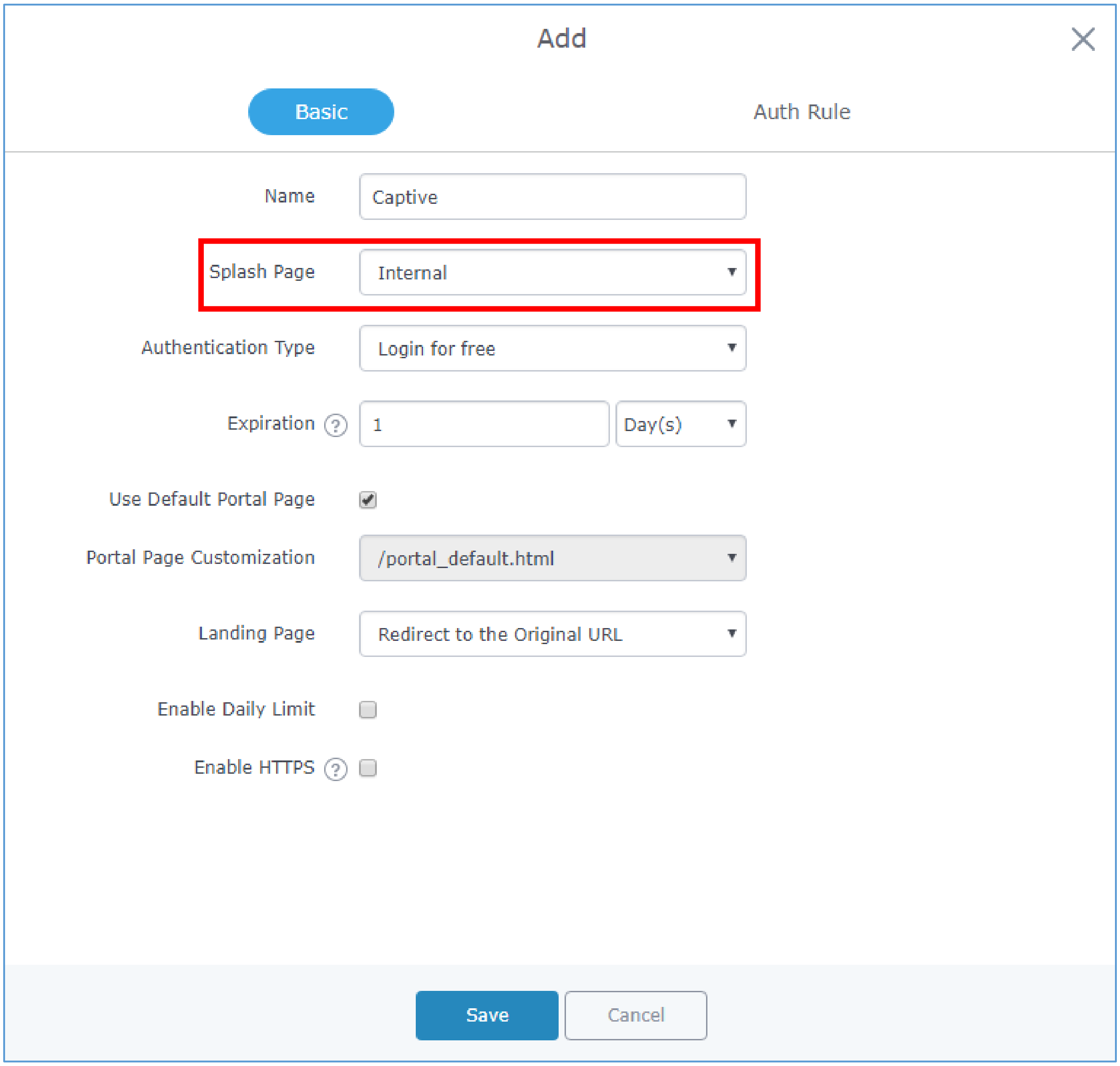
Name	Authentication Type	Expiration	Portal Page Customization	Actions
grandstream	Login for free	86400s	/portal_default.html	✎ 🗑

Figure 19: Captive Portal - Policy List

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

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

Administrator can use an internal or external splash page.



Add

Name: Captive

Splash Page: Internal

Authentication Type: Login for free

Expiration: 1 Day(s)

Use Default Portal Page ☑

Portal Page Customization: /portal_default.html

Landing Page: Redirect to the Original URL

Enable Daily Limit ☐

Enable HTTPS ☐

Figure 20: Add a New Policy

Internal Splash Page

Below table lists the items policy add page configures

Table 6: Captive Portal – Policy List – Splash Page is "Internal"

Field	Description
Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, Internal or External.
Authentication Type	Following types of authentication are available: • **Login for free:** 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. • **Vouchers:** Choose this page when using authentication via Vouchers. • **Login with Password:** Choose this page when using authentication via a password.
Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
If Authentication Type is set to "RADIUS Authentication"	
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 Secret	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.
If Authentication Type is set to "Social Login Authentication"	
Facebook	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 Wi-Fi___33, they should enter this key.
Twitter	Check this box to enable Twitter Authentication.
Force to Follow	If checked, users need to Follow owner before been authenticated.
Owner	Enter the app Owner to use Twitter Login API. *This field appears only when* **Force to Follow** *is checked.*
Consumer Key	Enter the app Key to use Twitter Login API.
Consumer Secret	Enter the app secret to use Twitter Login API.
For all Authentication Types	
Use Default Portal Page	If checked, the users will be redirected to the default portal page once connected to the GWN. If unchecked, users can manually select which Portal Page to use from **Portal Page Customization** drop-down list.
Portal Page Customization	Select the customized portal page (if "Use Default Portal Page" is unchecked). • */facebook.html*

	• */password_auth.html* • */portal_default.html* • */portal_pass.html* • */portal_tip.html* • */social_auth.html* • */status.html* • */twitter.html* • */twitter_website.html* • */vouchers_auth.html*
Landing Page	Choose the landing page, 2 options are available: • **Redirect to the Original URL.** • **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. *This field appears only when* **Landing Page** *is set to "Redirect to an External Page".*
Enable Daily Limit	If enabled, captive portal will limit user connection by times of one day.
Failsafe Mode	If checked, AP will grant access to STA if AP cannot reach to external authentication server. *This option is available only when* **Authentication Type** *is set to "RADIUS Server" or "Vouchers".*
Enable HTTPS	Check to enable/disable HTTPS service.

Notes:

1. If Facebook authentication is configured, you will need to log in your Facebook account of https://developers.facebook.com/apps , and set the OAuth redirect to : https://cwp.gwn.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3
2. If Twitter authentication is configured, you will need to log in your Twitter account of https://apps.twitter.com/app, and set the callback URLs to: http://cwp.gwn.cloud:8080/GsUserAuth.cgi

External Splash Page

Table 7: Captive Portal – Policy List – Splash Page is “External”

Field	Description
Name	Enter the name of the Captive Portal policy
Splash Page	Select to either use **Internal** or **External** Splash Page.
External Splash Page URL	Enter the External Splash Page URL, and make sure to enter the pre-authentication rules request by the external portal platform in the pre-authentication configuration option.
RADIUS Server Address	Fill in the IP address of the RADIUS server.
RADIUS Server Port	Set the RADIUS server port, the default value is 1812.
RADIUS Server Secret	Fill in the key of the RADIUS server.
RADIUS Accounting Server Address	Configures the address for the RADIUS accounting server.
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port (default is 1813).
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server.
Accounting Update Interval	Enter Update Interval for RADIUS Accounting Server. The interval unit can be set by seconds, minutes, hours or days.
RADIUS NAS ID	Enter RADIUS NAS ID. *This field appears only when* **Splash Page** *is set to “External”.*
Redirect URL	Specify URL where to redirect clients after authentication.

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.

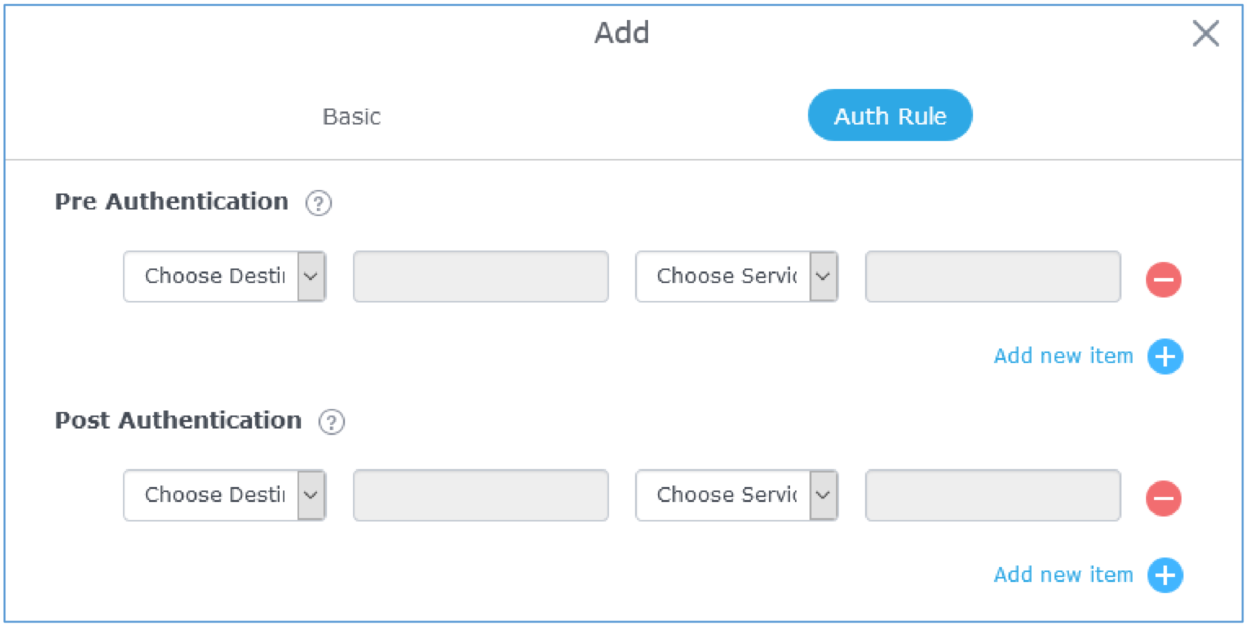


Figure 21: Authentication rules

Pre-Authentication Rules

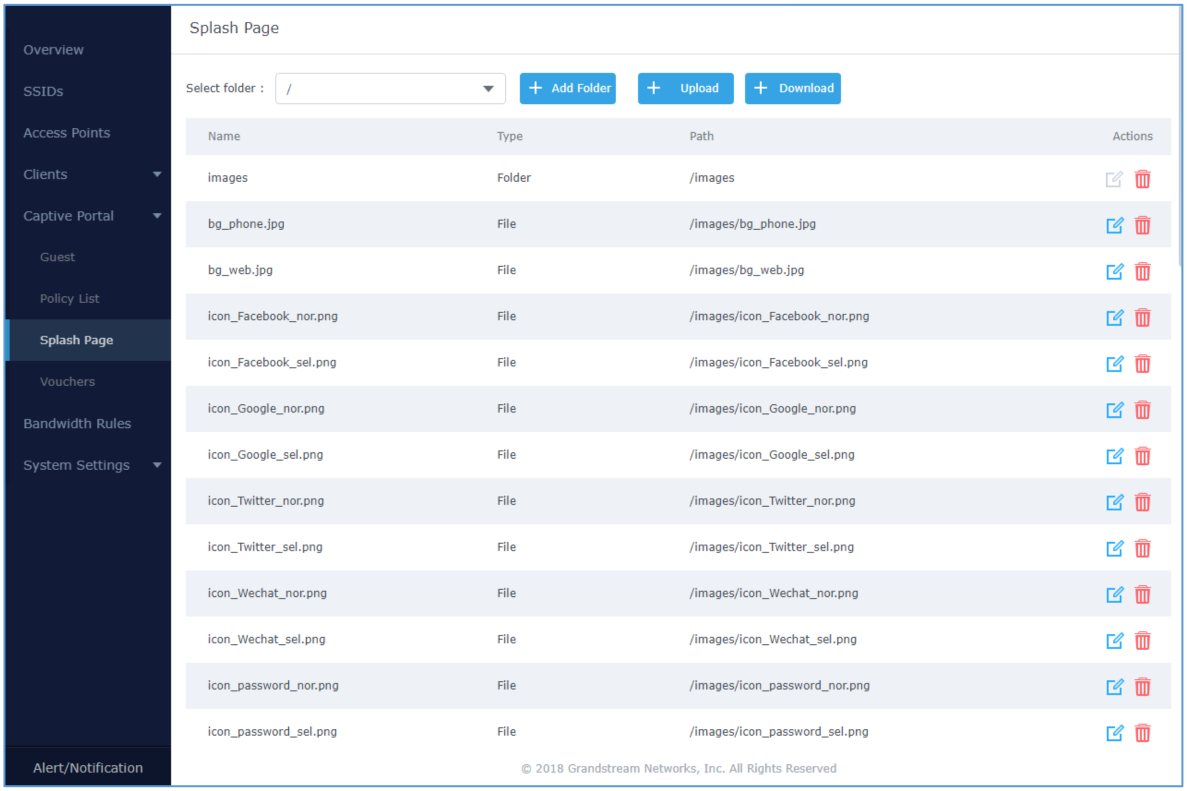
Using this option, users can set rules to match traffic that will be allowed for connected Wi-Fi users before authentication process. This can be needed for example to setup Facebook authentication where some traffic should be allowed to Facebook server(s) to process the user's authentication. Or simply 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 Wi-Fi clients after authentication. As an example, if you want to disallow connected Wi-Fi 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.

Splash Page

Files configuration page allows users to view and upload HTML pages and related files (images…).



Name	Type	Path	Actions
images	Folder	/images	✎ 🗑
bg_phone.jpg	File	/images/bg_phone.jpg	✎ 🗑
bg_web.jpg	File	/images/bg_web.jpg	✎ 🗑
icon_Facebook_nor.png	File	/images/icon_Facebook_nor.png	✎ 🗑
icon_Facebook_sel.png	File	/images/icon_Facebook_sel.png	✎ 🗑
icon_Google_nor.png	File	/images/icon_Google_nor.png	✎ 🗑
icon_Google_sel.png	File	/images/icon_Google_sel.png	✎ 🗑
icon_Twitter_nor.png	File	/images/icon_Twitter_nor.png	✎ 🗑
icon_Twitter_sel.png	File	/images/icon_Twitter_sel.png	✎ 🗑
icon_Wechat_nor.png	File	/images/icon_Wechat_nor.png	✎ 🗑
icon_Wechat_sel.png	File	/images/icon_Wechat_sel.png	✎ 🗑
icon_password_nor.png	File	/images/icon_password_nor.png	✎ 🗑
icon_password_sel.png	File	/images/icon_password_sel.png	✎ 🗑

© 2018 Grandstream Networks, Inc. All Rights Reserved

Figure 22: Captive Portal – Splash Page

User can add folder in corresponding folder by selecting the folder and click on + Add Folder.

- Click on + Upload to upload a file from local device.
- Click on + Download 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.

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 Wi-Fi using voucher codes that can be delivered on each command. Once the voucher expires the client can no longer connect to the internet.

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

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

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

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.

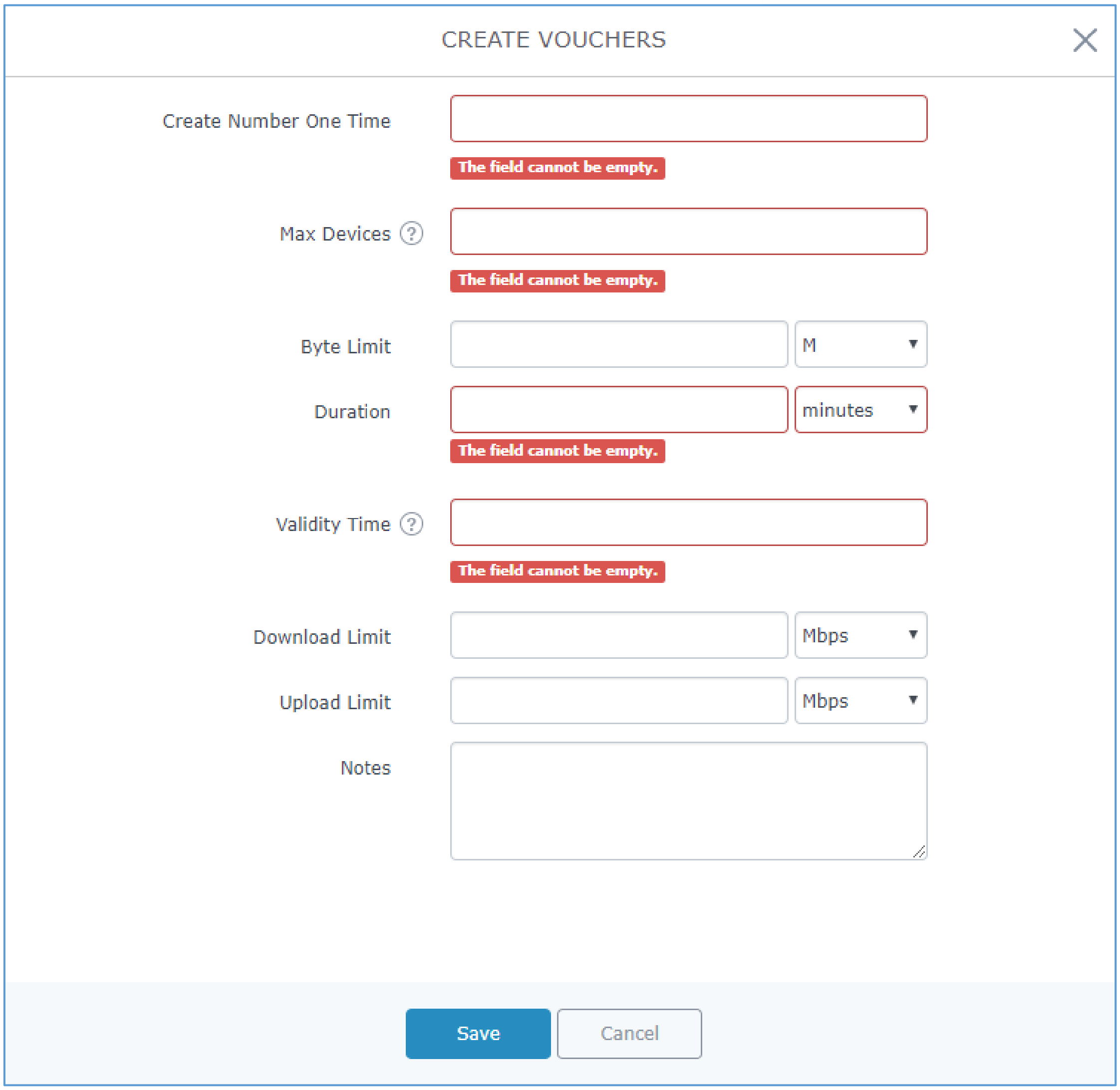
Voucher Configuration

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

1. On controller web GUI, navigate under "**Captive Portal → Vouchers**"
2. Click on **+ Add** 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, 🗑 to delete it or 🔄 to renew the voucher.

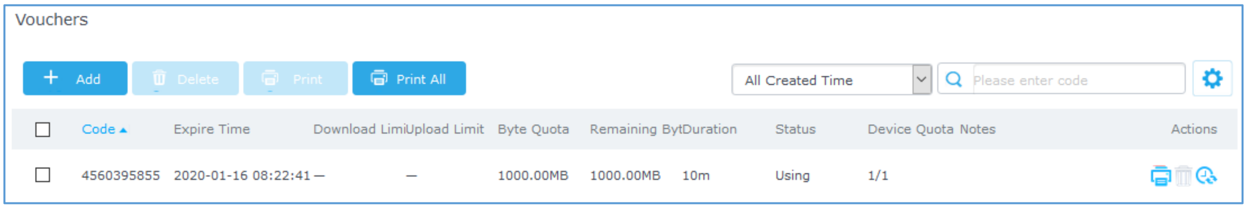


CREATE VOUCHERS

Create Number One Time	The field cannot be empty.
Max Devices ?	The field cannot be empty.
Byte Limit	M
Duration	minutes The field cannot be empty.
Validity Time ?	The field cannot be empty.
Download Limit	Mbps
Upload Limit	Mbps
Notes	

Figure 23: Add Voucher Sample

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



Vouchers

□	Code ▲	Expire Time	Download Limi	Upload Limit	Byte Quota	Remaining Byt	Duration	Status	Device Quota	Notes	Actions
□	4560395855	2020-01-16 08:22:41	—	—	1000.00MB	1000.00MB	10m	Using	1/1		

Figure 24: Vouchers List

Users can click on buttons Delete and Print to delete and print multiple vouchers or click Print All button to print all vouchers at once.

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 8: Voucher Parameters

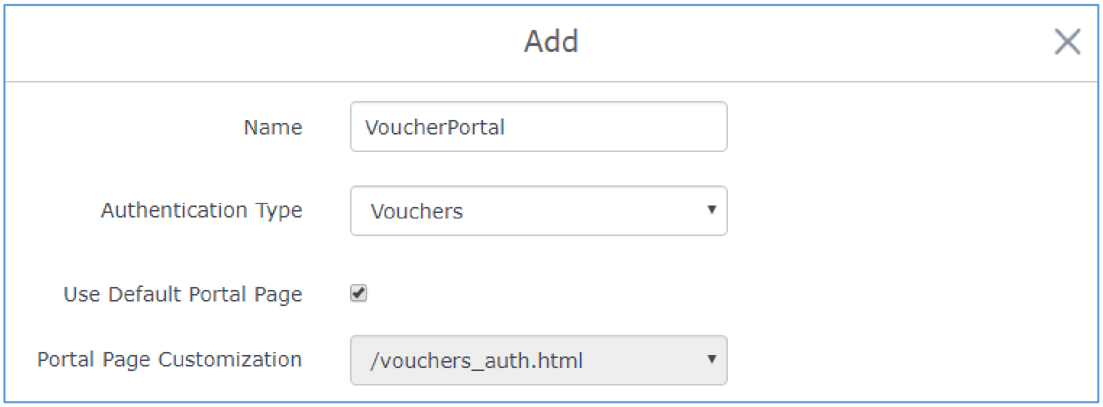
Field	Description
Create Number One Time	Specify how many vouchers to generate which will have same profile/settings (duration, bandwidth and number of users). Valid range: 1 – 1000.
Max Devices	Specify how many users can use same voucher. Valid range: 1 – 5.
Byte Limit	Specify download byte limit for the voucher. The unit can be either **M** (Megabyte) or **G** (Gigabyte). Valid range: 10 – 1048576 (M) 1 – 1024 (G)
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.
Validity Time	Set the validity period of credentials, limited to 1-365 integer. The unit is day.
Download Limit	Set the downstream bandwidth speed limit (in Kbps or Mbps).
Upload Limit	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.



Add

Name: VoucherPortal

Authentication Type: Vouchers

Use Default Portal Page: ☑

Portal Page Customization: /vouchers_auth.html

Figure 25: Captive Portal with Voucher authentication

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

Mesh Network

In Mesh Network, wireless connection is established between multiple Aps, which is used to pass-through 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:

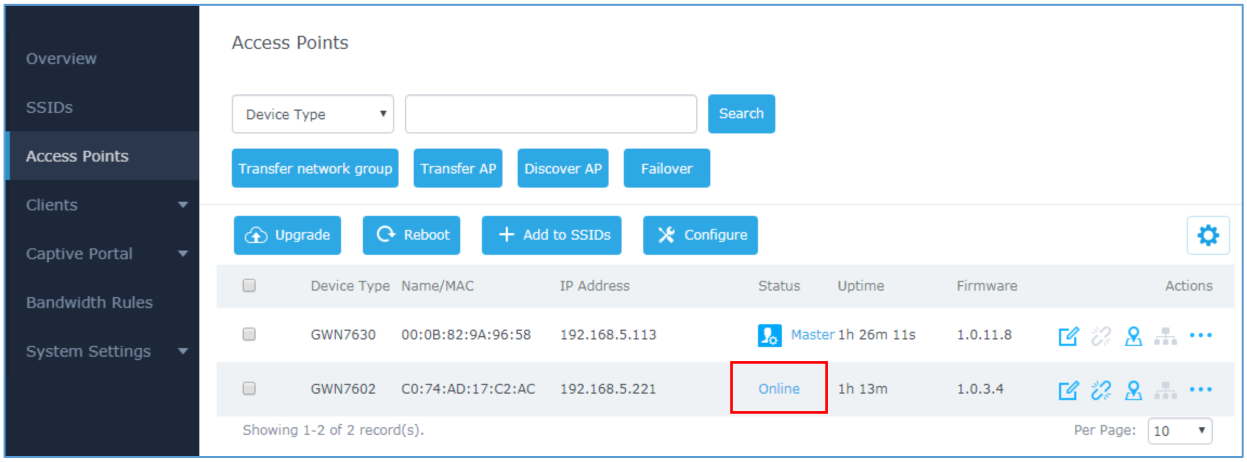
   A. Connect all REs to the same wired LAN as the master then perform the normal process of discovery/pairing process, and after successfully pairing the APs they can be deployed on the field.

   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**.



□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7630	00:0B:82:9A:96:58	192.168.5.113	Master	1h 26m 11s	1.0.11.8	•••
□	GWN7602	C0:74:AD:17:C2:AC	192.168.5.221	Online	1h 13m	1.0.3.4	•••

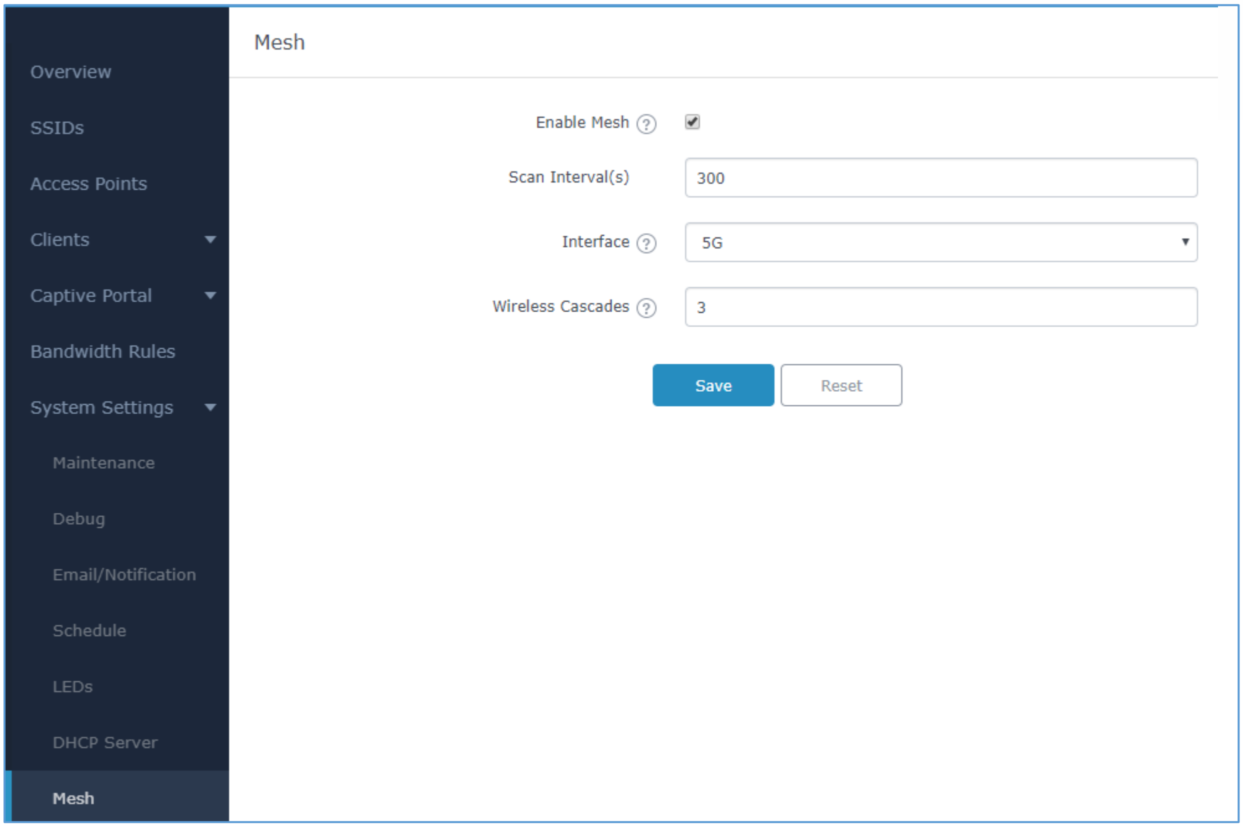
Showing 1-2 of 2 record(s). Per Page: 10

Figure 26: Access Points Status

For Global mesh network settings, on Master GWN76XX, navigate to the menu **"System Settings → Mesh"** for setting up the following parameters described below:

Table 9: Mesh parameters

Filed	Description
Enable Mesh	When checked the Mesh feature will be activated. Default is disabled.
Scan Interval	Interval in seconds to scan for available Mesh neighbors. Must be less than or equal to 300 seconds.
Interface	Select either 2.4GHz or 5GHz band.
Wireless cascades	Define how many AP can be cascaded wirelessly with the AP. The minimum value is 1 and maximum value is 3.



Mesh

Enable Mesh ☑

Scan Interval(s) 300

Interface 5G

Wireless Cascades 3

Figure 27: Mesh settings for GWN7602

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 GWN7602 feature that allows users to limit bandwidth utilization per SSID or client (MAC address or IP address).

This option can be configured from the Master GWN76XX WebGUI under “Bandwidth Rules”.

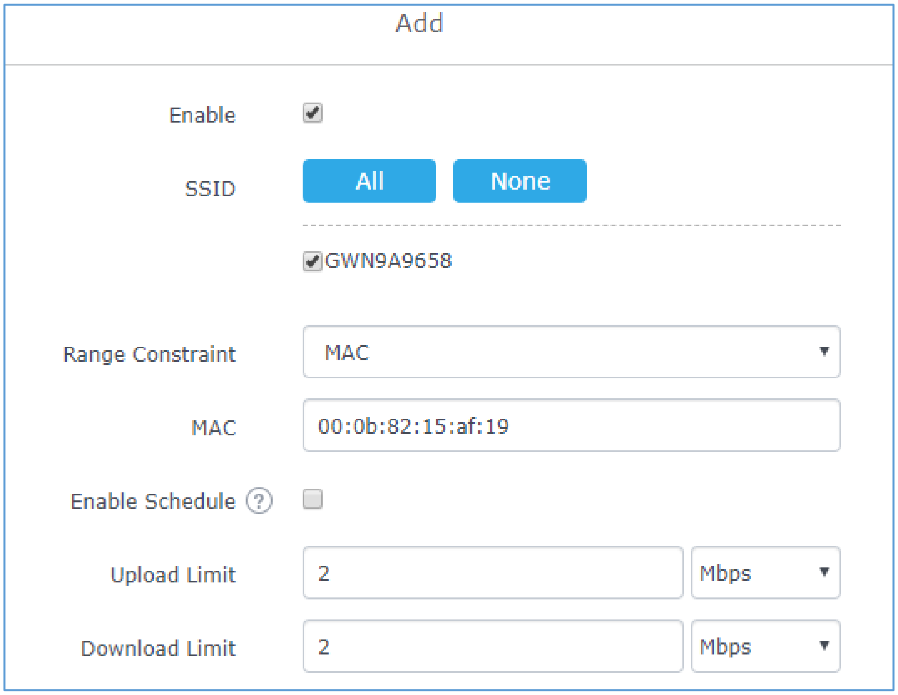
Click + Add to add a new rule, the following table provides an explanation about different options for bandwidth rules.

Table 10: 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: • **Per-SSID:** Set a bandwidth limitation on the SSID level. • **Per-User:** Set a bandwidth limitation per Client. • **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.
Upload Limit	Specify the limit for the upload bandwidth using Kbps or Mbps.
Download Limit	Specify the limit for the download bandwidth using Kbps or Mbps.

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



Add

Enable ☑

SSID

☑ GWN9A9658

Range Constraint: MAC

MAC: 00:0b:82:15:af:19

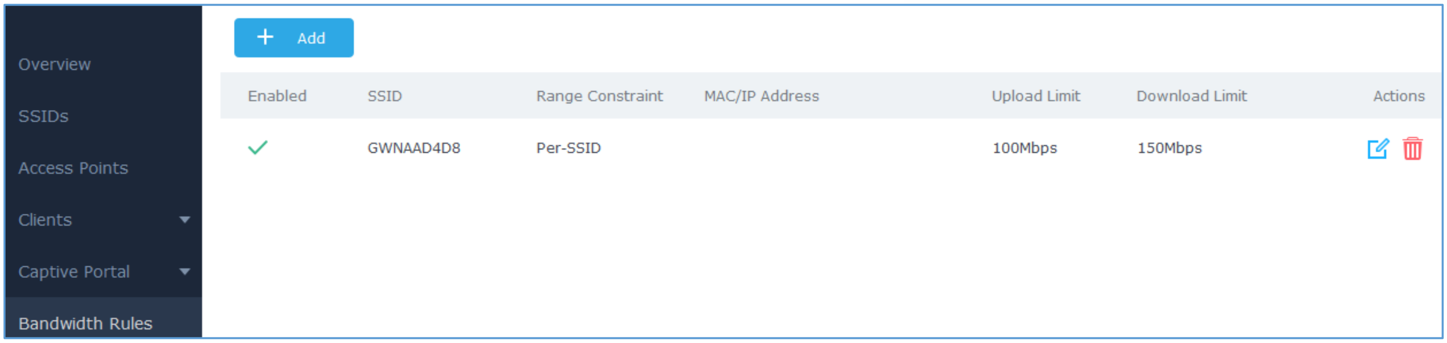
Enable Schedule ? □

Upload Limit: 2 Mbps

Download Limit: 2 Mbps

Figure 28: MAC Address Bandwidth Rule

The following figure shows examples of bandwidth rules:



Enabled	SSID	Range Constraint	MAC/IP Address	Upload Limit	Download Limit	Actions
✓	GWNAAD4D8	Per-SSID		100Mbps	150Mbps	

Figure 29: Bandwidth Rules

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

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

System Settings

Maintenance

Users can access Maintenance page from the master GWN76XX Web GUI under **System Settings→ Maintenance**.

Basic

Basic page allows Country and Time configuration.

Table 11: Basic

Field	Description
Rebind Protection	Anti-domain name hijacking protection. If enabled, when the address returned by the superior DNS is a private LAN address, it will be regarded as a domain name hijacking, thus discarding the analytical result. If disabled, the analytical results will not be discarded.
Web HTTP Access	Enables Web HTTP Access. By default, it is disabled.
Web HTTPS Port	Specifies HTTPS port. By default, is 443.
Country	Select the country from the drop-down list. This can affect the number of channels depending on the country standards.
Time Zone	Configure time zone for the GWN7602. 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.
Reboot Schedule	Select the time schedule when AP will be rebooted. Refer to [**Schedule**] to define time.

Upgrade

The Upgrade Web page allows upgrade related configuration.

Table 12: Upgrade

Field	Description
Authenticate Config File	Authenticates configuration file before acceptance. The default setting is No.
XML Config File Password	The password for encrypting the XML configuration file using OpenSSL. The password is to decrypt the XML configuration file is it is encrypted via OpenSSL
Upgrade Via	Allow users to choose the method to load the firmware and config: TFTP, HTTP or HTTPS.
Firmware Server	Define the IP address or URL for the firmware upgrade server. Make sure all files relevant to the firmware are updated completely
Config Server	Configure the IP address of URL for the file server.
Check/Download New Firmware and Config at Boot	Configure whether to enable/disable automatic upgrade and provisioning when reboot.
Allow DHCP options 66 and 43 override	Enable/Disable DHCP options 66 and 43 to override the upgrade and provisioning settings
Automatic Upgrade	Set automatic upgrade every intervals/day/week. The device will request to upgrade automatically according to the setup time. The default setting is Disabled
X Hours	Select the time period to check for firmware upgrade. *This field is available when select “Check every X Hours” in “Automatic Upgrade”*
Hour of Day (0-23)	Defines the hour of the day (0-23) to check the HTTP/TFTP server for firmware upgrade or configuration file changes.

	This field is available when select "Check at Hour of Day" and "Check at Day of Week" in "Automatic Upgrade"
Day of Week	Defines the day of the week to check the HTTP/TFTP server for firmware upgrade or configuration file changes. *This field is available when select "Check at Day of Week" in "Automatic Upgrade"*
Upgrade Now	Click on Upgrade button to begin the upgrade. Note that the device will reboot after downloading the firmware.
Download Configuration	Click on Download button to download the device configuration file to PC.
Upload Configuration	Click on Upload to select a compressed config file to restore the config; after succeeding, the device will reboot automatically.
Reboot	Click on Reboot button to reboot device.
Factory Reset	Click on Reset to restore the device and all online APs to factory default settings.

Access

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

Table 13: 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 14: 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 Master GWN76XX controllers in order to save log messages for GWN7602 on connected external USB drive.

First connect a USB drive to the Master Access point, then configure the parameters and make sure to start the server in order to collect messages from GWN7602 sending syslog to GWN Master.

Following table gives description for configuration parameters of GWN Logserver:

Table 15: Logserver Parameters

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 hour (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 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.

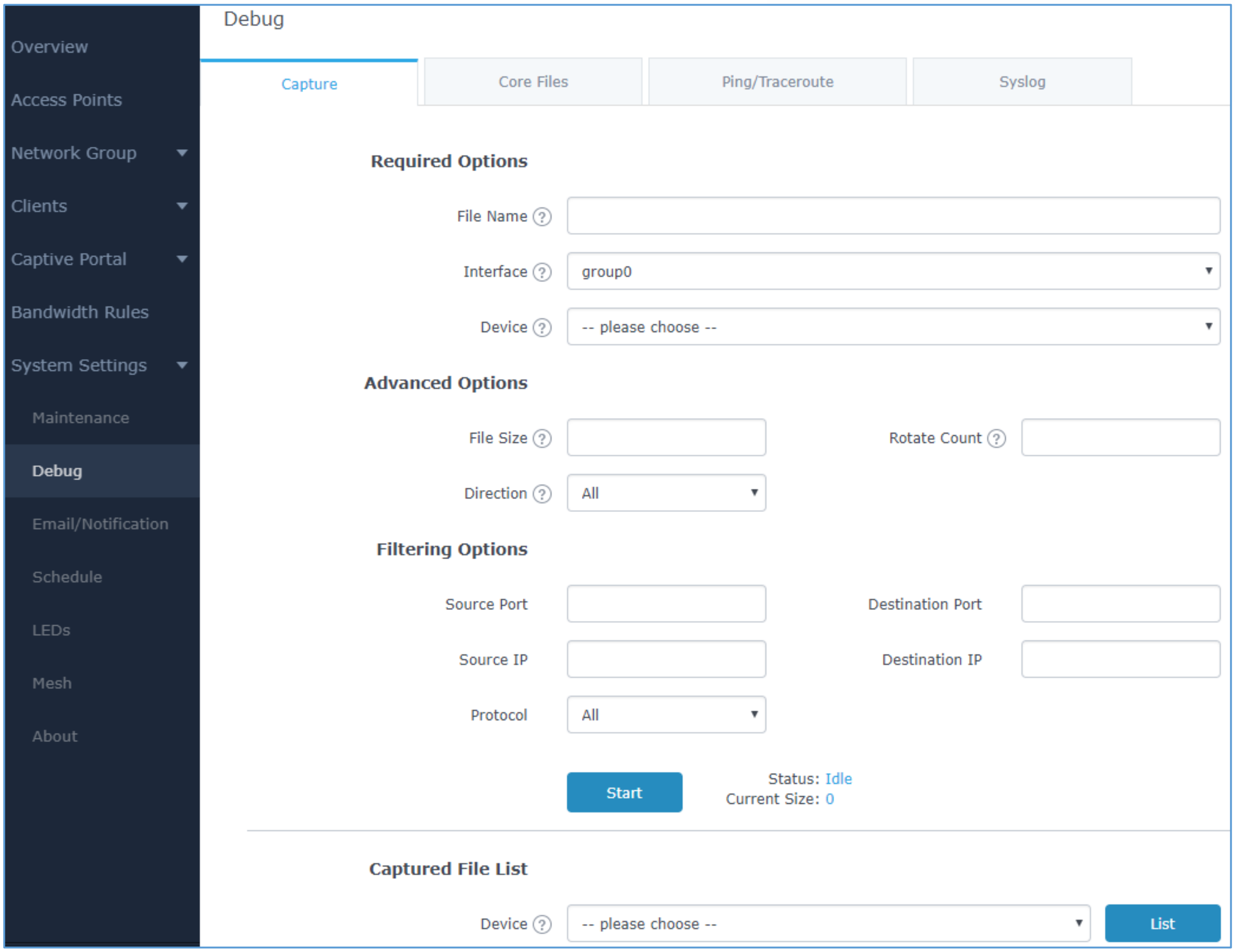
- Under **Syslog File List**, users can select a device and press **List** button to list all saved logs on this device.
- Press **Download** button to download a saved log.
- Press **Clear** button to remove logs.

Debug

GWN7602 offers many features for managing and monitoring connected clients to SSIDs, as well as debugging and troubleshooting.

Capture (Available Only When the Master is GWN7610 OR GWN7600)

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 Master GWN7610/GWN7600. To access Capture page, go to **System Settings→Debug→Capture.**



Debug

Required Options

File Name:

Interface: group0

Device: -- please choose --

Advanced Options

File Size:

Rotate Count:

Direction: All

Filtering Options

Source Port:

Destination Port:

Source IP:

Destination IP:

Protocol: All

Status: Idle
Current Size: 0

Captured File List

Device: -- please choose --

Figure 30: Capture Page

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

Table 16: Debug

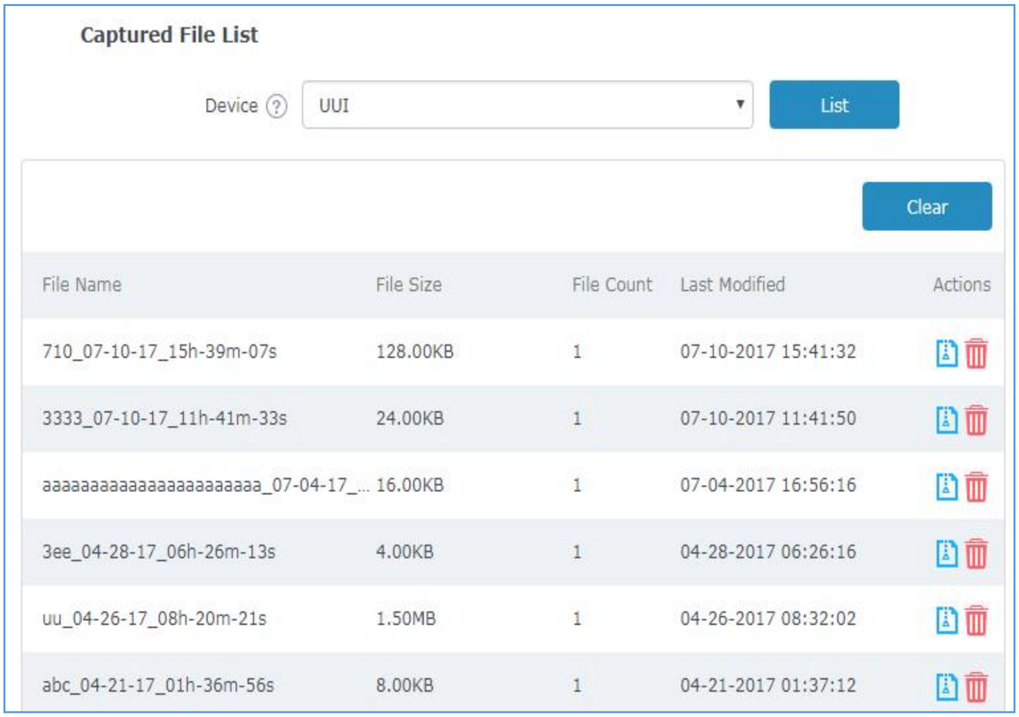
Required Options	
File Name	Enter the name of the capture file that will be generated.
Interface	Choose a SSID as Interface on which the traffic will be captured.
Device	Choose a device plugged to USB port to save the capture once started.
Advanced Options	
File Size	Set a File size that the capture 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	
Custom Filter	Check this option when adding custom filtering rule. When selected, the default filtering options will be hidden (Source Port, Destination Port...etc).
Custom Filtering Rule	Configures a filter expression in which traffic should be captured，for example：icmp and host 8.8.8.8. Once configured, then you need to click on Validate.
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)
Filtering Options Logic	Choose the filtering logic between all filter options to either “And” or “Or” when capturing traffic.
Device	Select the device from which you want to list the captured file.

- 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.



Captured File List

Device UUI

File Name	File Size	File Count	Last Modified	Actions
710_07-10-17_15h-39m-07s	128.00KB	1	07-10-2017 15:41:32	
3333_07-10-17_11h-41m-33s	24.00KB	1	07-10-2017 11:41:50	
aaaaaaaaaaaaaaaaaaaaaa_07-04-17_...	16.00KB	1	07-04-2017 16:56:16	
3ee_04-28-17_06h-26m-13s	4.00KB	1	04-28-2017 06:26:16	
uu_04-26-17_08h-20m-21s	1.50MB	1	04-26-2017 08:32:02	
abc_04-21-17_01h-36m-56s	8.00KB	1	04-21-2017 01:37:12	

Figure 31: Capture Files

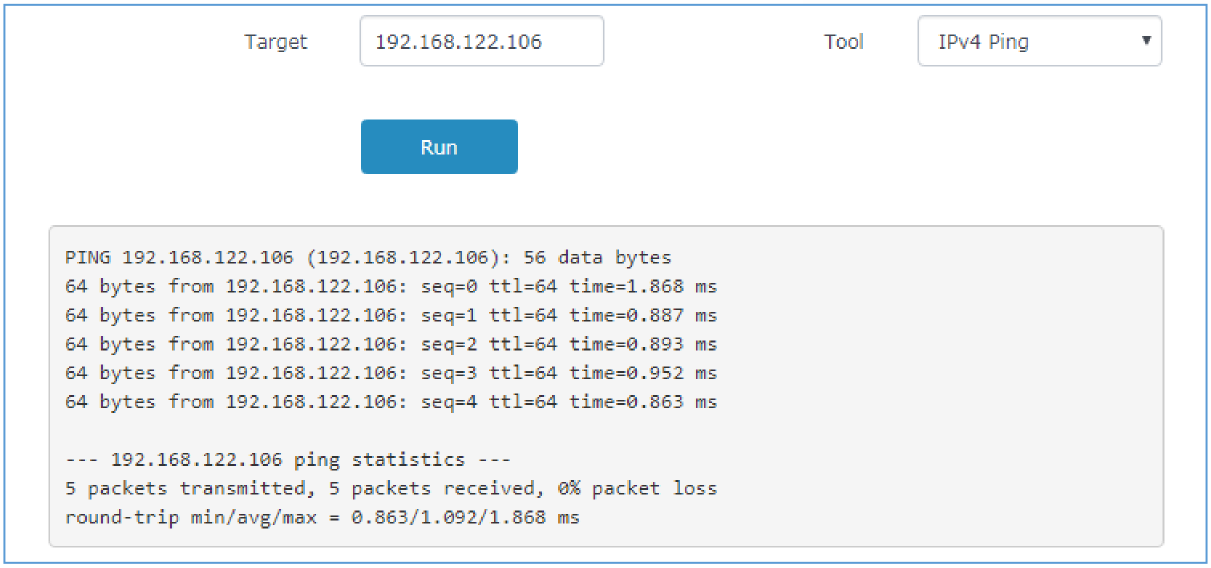
Core Files

The Core Files Web page displays core dumps generated when the GWN7602 crashes. This is helpful for troubleshooting purposes.

Ping/Traceroute

Ping and Traceroute are useful debugging tools to verify reachability with other clients across the network. The master GWN76XX offers both Ping and Traceroute tools for IPv4 protocol.

To use these tools, go to Master GWN76XX Web GUI **System Settings → Debug → Ping/Traceroute.**



Target: 192.168.122.106

Tool: IPv4 Ping

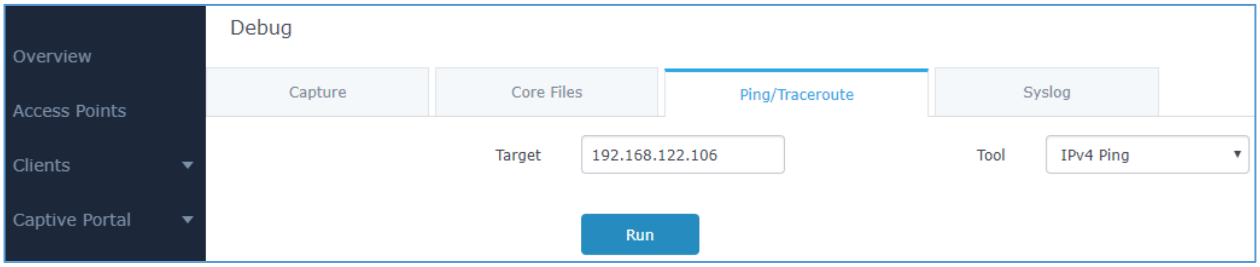
```
PING 192.168.122.106 (192.168.122.106): 56 data bytes
64 bytes from 192.168.122.106: seq=0 ttl=64 time=1.868 ms
64 bytes from 192.168.122.106: seq=1 ttl=64 time=0.887 ms
64 bytes from 192.168.122.106: seq=2 ttl=64 time=0.893 ms
64 bytes from 192.168.122.106: seq=3 ttl=64 time=0.952 ms
64 bytes from 192.168.122.106: seq=4 ttl=64 time=0.863 ms

--- 192.168.122.106 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.863/1.092/1.868 ms
```

Figure 32: IP Ping

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

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



Target: 192.168.122.106

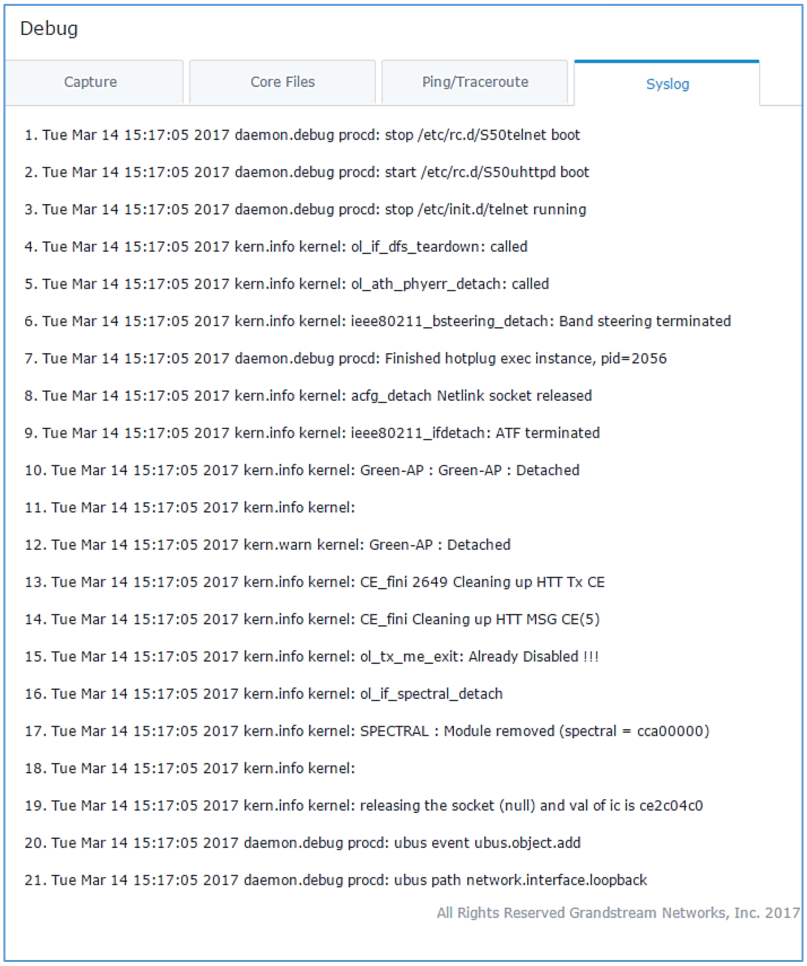
Tool: IPv4 Ping

Figure 33: IP Traceroute

Syslog

The syslog Web page displays logs generated by the GWN7602 for troubleshooting purpose as shown in figure below.

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



```
1. Tue Mar 14 15:17:05 2017 daemon.debug procd: stop /etc/rc.d/S50telnet boot
2. Tue Mar 14 15:17:05 2017 daemon.debug procd: start /etc/rc.d/S50uhttpd boot
3. Tue Mar 14 15:17:05 2017 daemon.debug procd: stop /etc/init.d/telnet running
4. Tue Mar 14 15:17:05 2017 kern.info kernel: ol_if_dfs_teardown: called
5. Tue Mar 14 15:17:05 2017 kern.info kernel: ol_ath_phyerr_detach: called
6. Tue Mar 14 15:17:05 2017 kern.info kernel: ieee80211_bsteering_detach: Band steering terminated
7. Tue Mar 14 15:17:05 2017 daemon.debug procd: Finished hotplug exec instance, pid=2056
8. Tue Mar 14 15:17:05 2017 kern.info kernel: acfg_detach Netlink socket released
9. Tue Mar 14 15:17:05 2017 kern.info kernel: ieee80211_ifdetach: ATF terminated
10. Tue Mar 14 15:17:05 2017 kern.info kernel: Green-AP : Green-AP : Detached
11. Tue Mar 14 15:17:05 2017 kern.info kernel:
12. Tue Mar 14 15:17:05 2017 kern.warn kernel: Green-AP : Detached
13. Tue Mar 14 15:17:05 2017 kern.info kernel: CE_fini 2649 Cleaning up HTT Tx CE
14. Tue Mar 14 15:17:05 2017 kern.info kernel: CE_fini Cleaning up HTT MSG CE(5)
15. Tue Mar 14 15:17:05 2017 kern.info kernel: ol_tx_me_exit: Already Disabled !!!
16. Tue Mar 14 15:17:05 2017 kern.info kernel: ol_if_spectral_detach
17. Tue Mar 14 15:17:05 2017 kern.info kernel: SPECTRAL : Module removed (spectral = cca00000)
18. Tue Mar 14 15:17:05 2017 kern.info kernel:
19. Tue Mar 14 15:17:05 2017 kern.info kernel: releasing the socket (null) and val of ic is ce2c04c0
20. Tue Mar 14 15:17:05 2017 daemon.debug procd: ubus event ubus.object.add
21. Tue Mar 14 15:17:05 2017 daemon.debug procd: ubus path network.interface.loopback
```

Figure 34: Syslog

One Key Debug

This feature is useful when AP is paired, as users can still login to the paired AP using “admin” username and “SSH” password (**System → Settings →SSH Password**).

User will have access to the usual Capture, Ping/Traceroute and Syslog and to One Key Debug feature that allows collecting more information that can be share with support for troubleshooting purposes directly from the Access Points web interface.

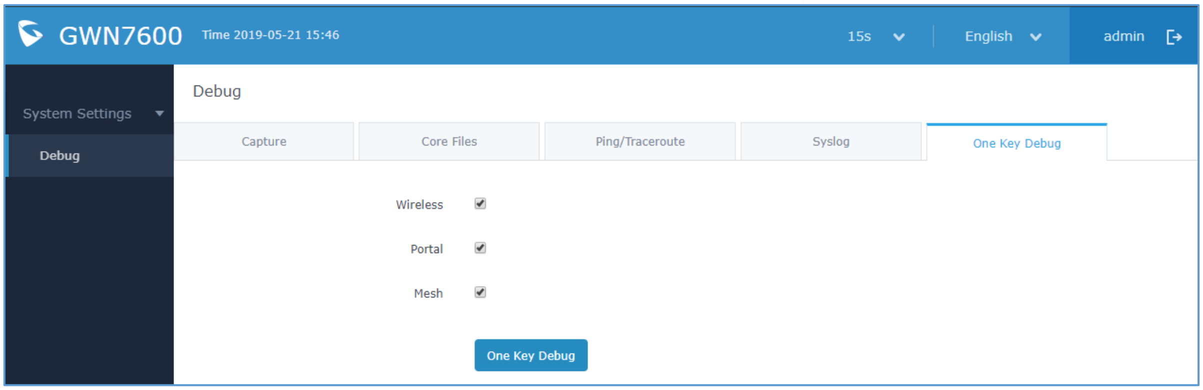
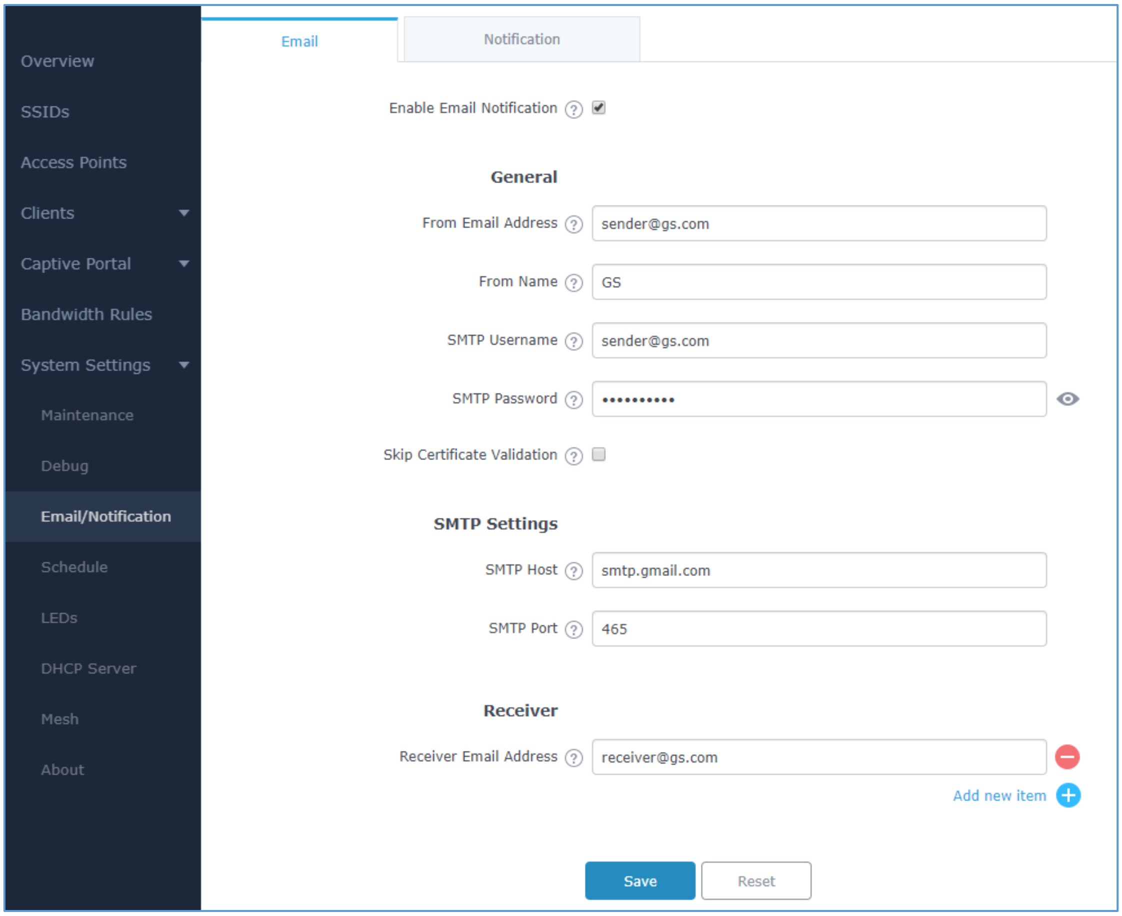


Figure 35: One Key Debug

After selecting the features to debug (Wireless: clients connections, SSIDs.., Captive portal debugging or Mesh network) then you should press the **One Key Debug** button, and after 30 min the debug file will be available under Core file.

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.



Enable Email Notification ☑

General

From Email Address: sender@gs.com

From Name: GS

SMTP Username: sender@gs.com

SMTP Password: ••••••••••

Skip Certificate Validation ☐

SMTP Settings

SMTP Host: smtp.gmail.com

SMTP Port: 465

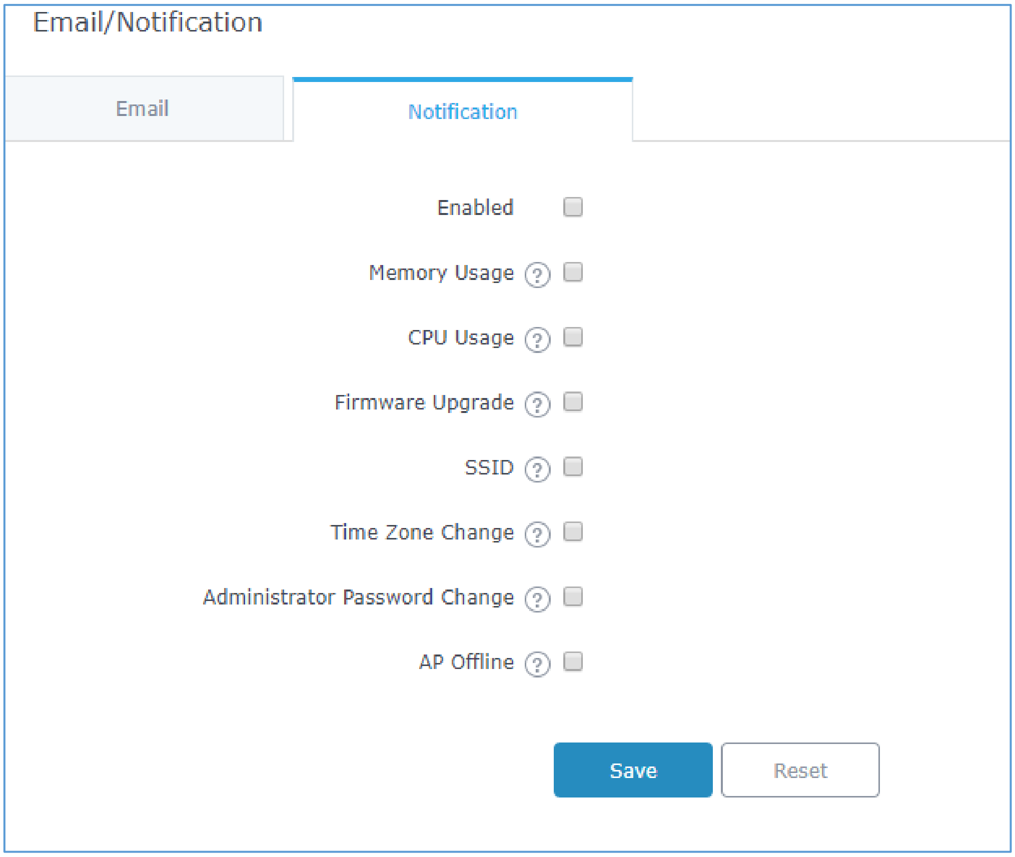
Receiver

Receiver Email Address: receiver@gs.com

Figure 36: Email

Table 17: Email Setting

Filed	Description
Enable Email Notification	Once enabled, AP will send related notification email to the receivers. **Note**: if no event is specified in the Notification page, server will send an empty mail.
General	
From Email Address	Specify the email address of the notification sender. If the address is not specified, AP will use the SMTP username as a sender.
From Name	Specifies the name of the notification sender.
SMTP Username	Specifies the username to login to the mail server
Email Address	Specifies the email address of the administer where to receive notifications.
Skip Certificate Validation	Check this box to skip the certificate validation
SMTP Settings	
SMTP Host	Configures the SMTP Email Server IP or Domain Name.
SMTP Port	Specifies the Port number used by server to send email.
Receiver Email Address	Specifies the email addresses to receive notifications.



Email/Notification

Enabled □

Memory Usage ? □

CPU Usage ? □

Firmware Upgrade ? □

SSID ? □

Time Zone Change ? □

Administrator Password Change ? □

AP Offline ? □

Figure 37: Notification

The following table describes the notifications configuration settings.

Table 18: Email Events

Filed	Description
Enabled	Enable/disable the notification. By default, it is disabled
Memory Usage	Configures whether to send notification if memory usage is greater than the configured threshold. By default, it is 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 is 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 Server

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 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 19: DHCP Server Parameters

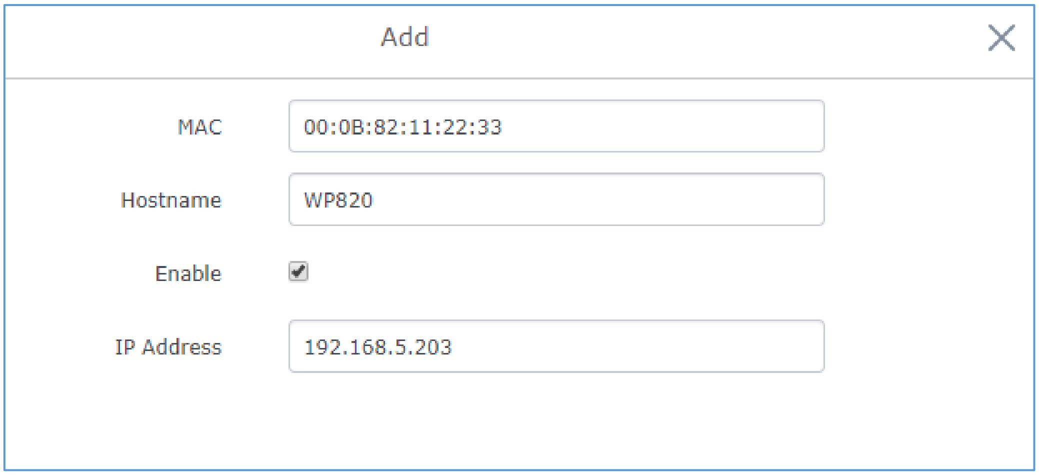
Field	Description
Name	Set the name of the DHCP Pool.
Enable	Enable/Disable the DHCP pool.
VLAN ID	Set a VLAN ID, same one should be set on SSID settings to map it with the DHCP pool.
DHCP Server Static Address	Configure the static address of the DHCP server (through which GWN Master AP will be accessible).
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 Lease 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

Static DHCP

Users can use the feature in order to set static DHCP binding to certain clients, to whom you do not want the IP address to change.

To configure Static DHCP, please follow below steps:

1. Go under the menu "**System Settings ➔ DHCP Server ➔ Static DHCP**".
2. Click + Add button to create a new entry.
3. Enter the name of the device, along with its MAC address and IP address



Add ✕

MAC: 00:0B:82:11:22:33

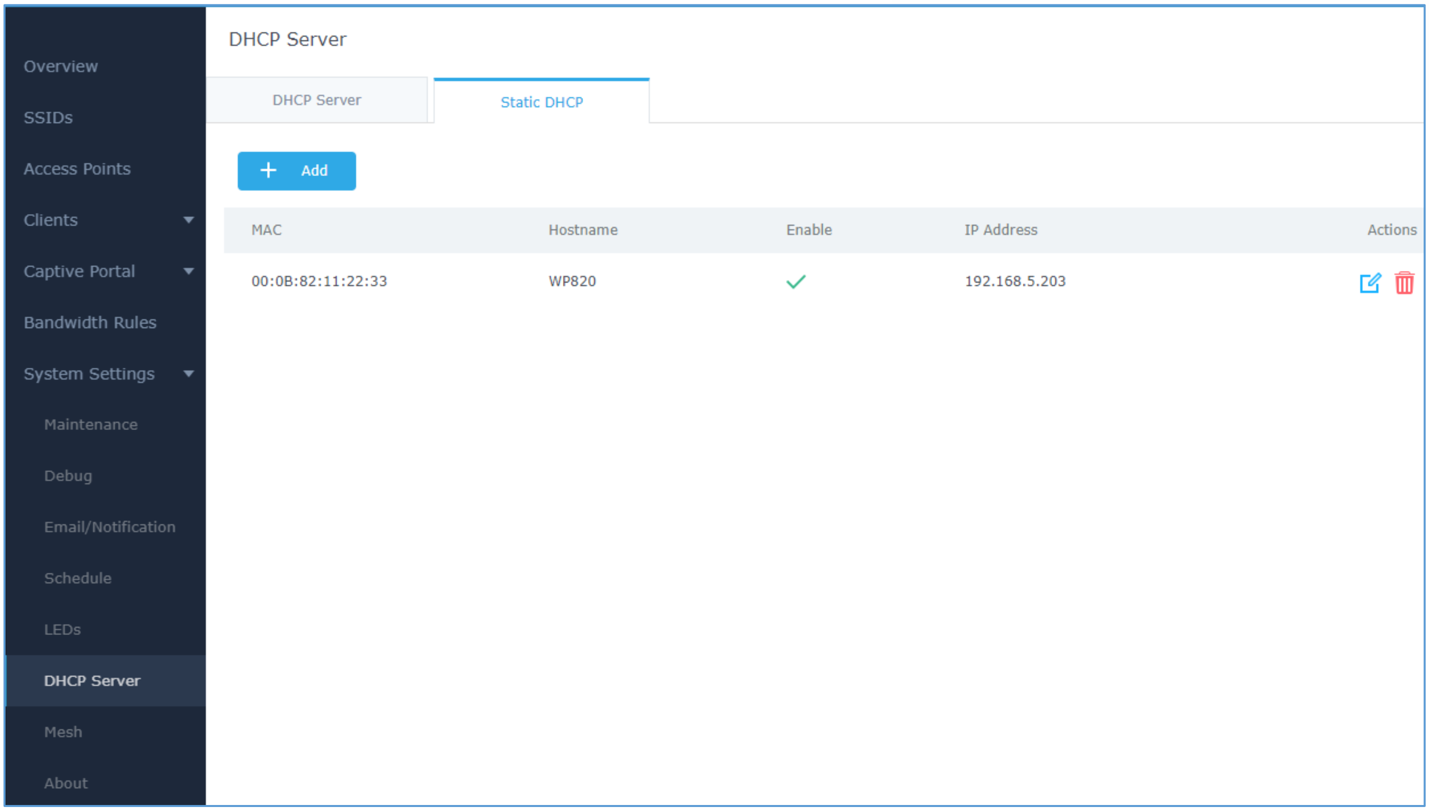
Hostname: WP820

Enable: ☑

IP Address: 192.168.5.203

Figure 38: DHCP Binding

4. Press Save and Apply to submit the changes.



MAC	Hostname	Enable	IP Address	Actions
00:0B:82:11:22:33	WP820	✓	192.168.5.203	

Figure 39: Static DHCP Devices List

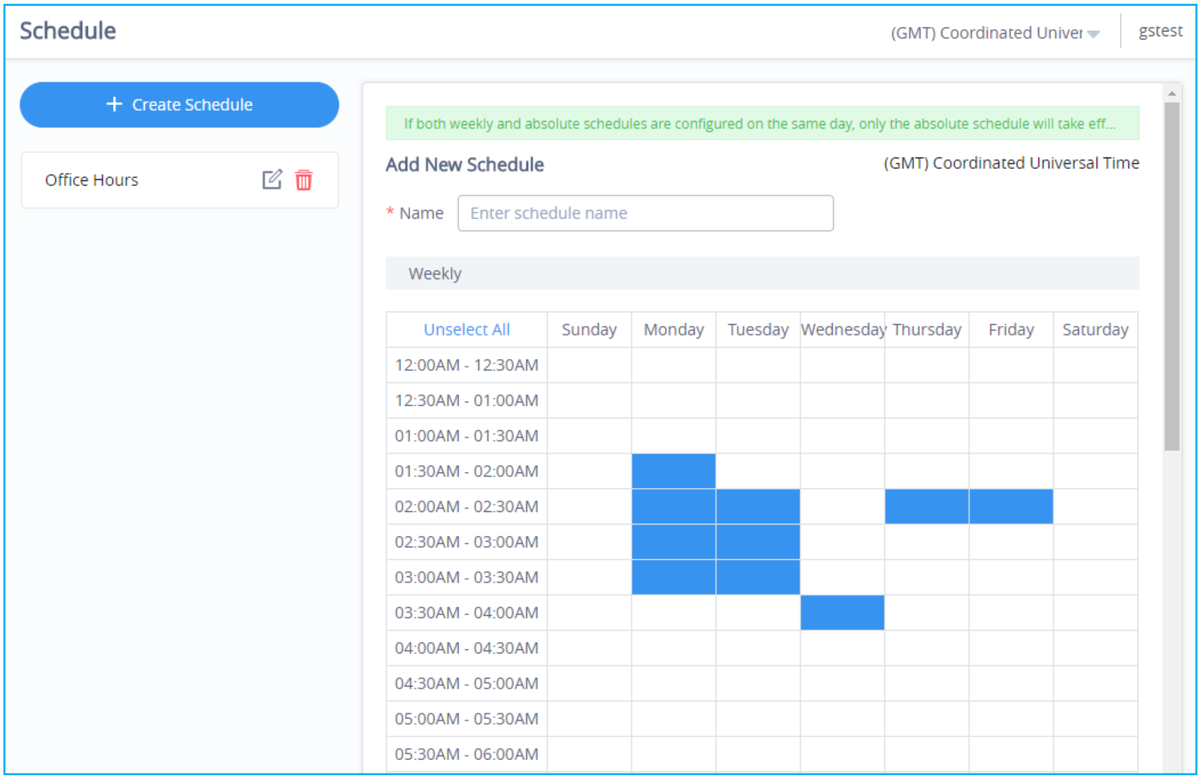
Schedule

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.

To configure a new schedule, follow below steps:

1. Go under “**Schedule**” and click on **Create New Schedule**.



Schedule

(GMT) Coordinated Univer▾ | gstest

+ Create Schedule

Office Hours

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

Add New Schedule

(GMT) Coordinated Universal Time

* Name: Enter schedule name

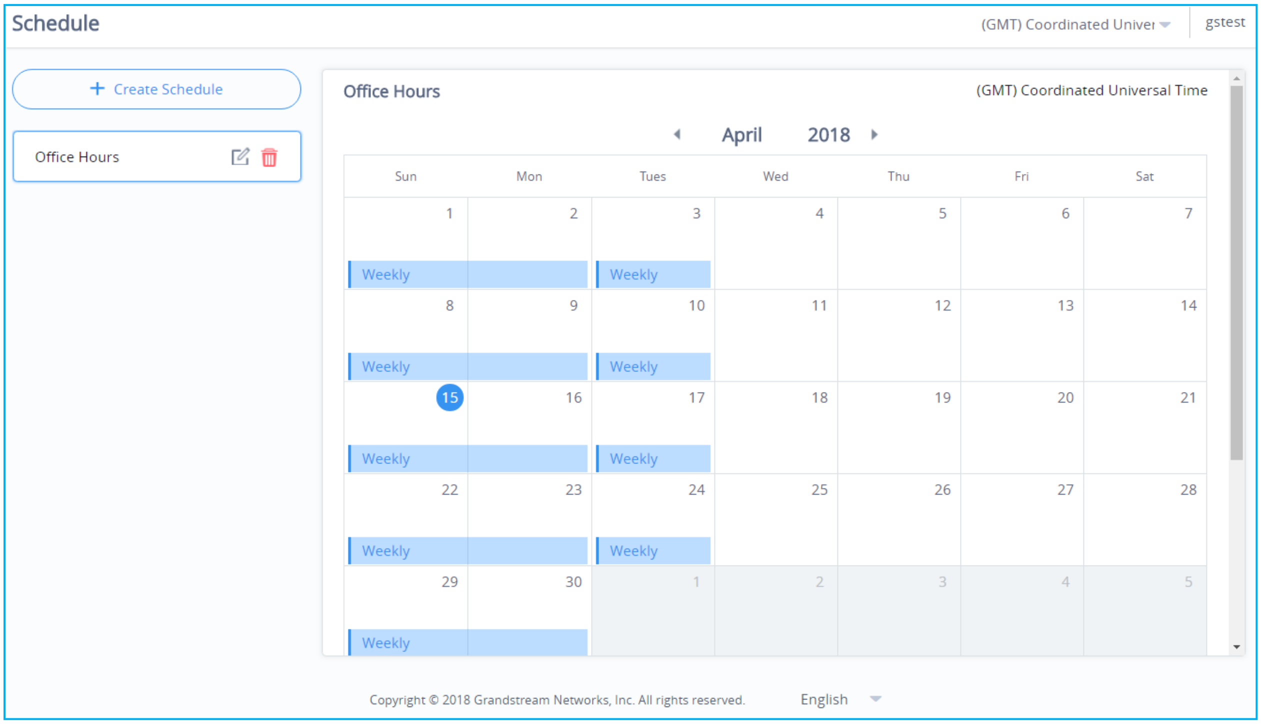
Weekly

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

Figure 40: 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:


Schedule
(GMT) Coordinated Univer
gstest
+ Create Schedule
Office Hours
Office Hours
(GMT) Coordinated Universal Time
April 2018
Copyright © 2018 Grandstream Networks, Inc. All rights reserved.
English

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

Figure 41: Schedules List

LED Schedule

GWN7602 Access Points series also support 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.

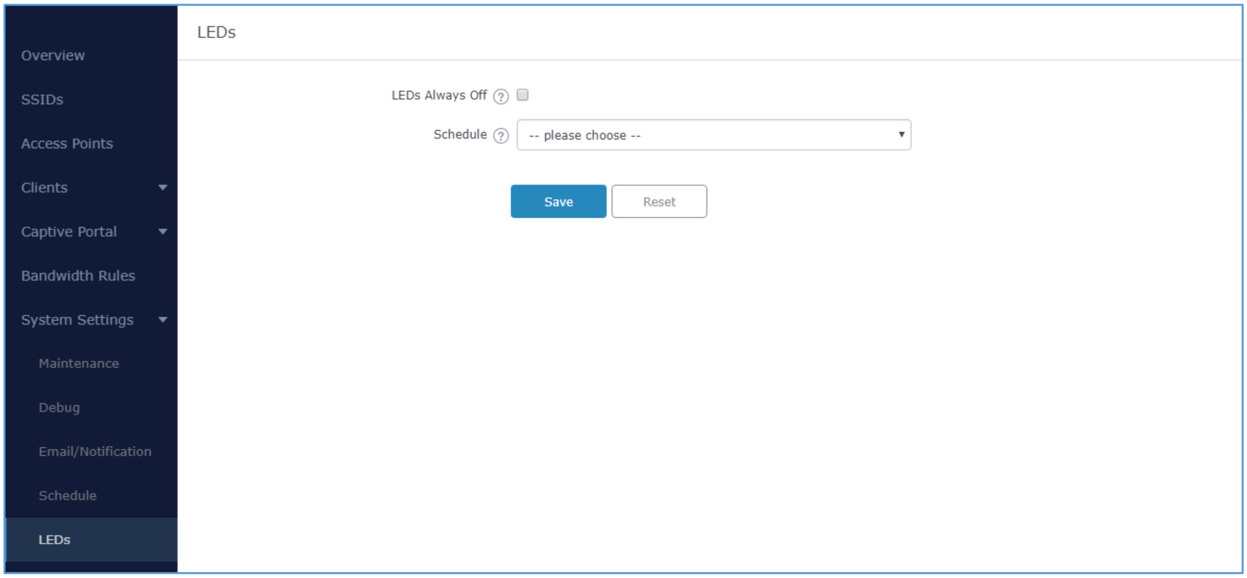
To configure LED schedule, on the Master GWN76XX WebGUI navigate to "**System Settings→LEDs**".

Following options are available:

Table 20: 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.



LEDs

LEDs Always Off ☐

Schedule: -- please choose --

Figure 42: LED Scheduling Sample

UPGRADING AND PROVISIONING

Upgrading Firmware

The GWN7602 can be upgraded to a new firmware version remotely. This section describes how to upgrade your GWN7602 via the Master GWN76XX.

Upgrading via the Master GWN76XX Web GUI

The GWN7602 can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:
firmware.grandstream.com/BETA
192.168.5.87
The upgrading configuration can be accessed via:
Web GUI→System Settings→Maintenance→Upgrade

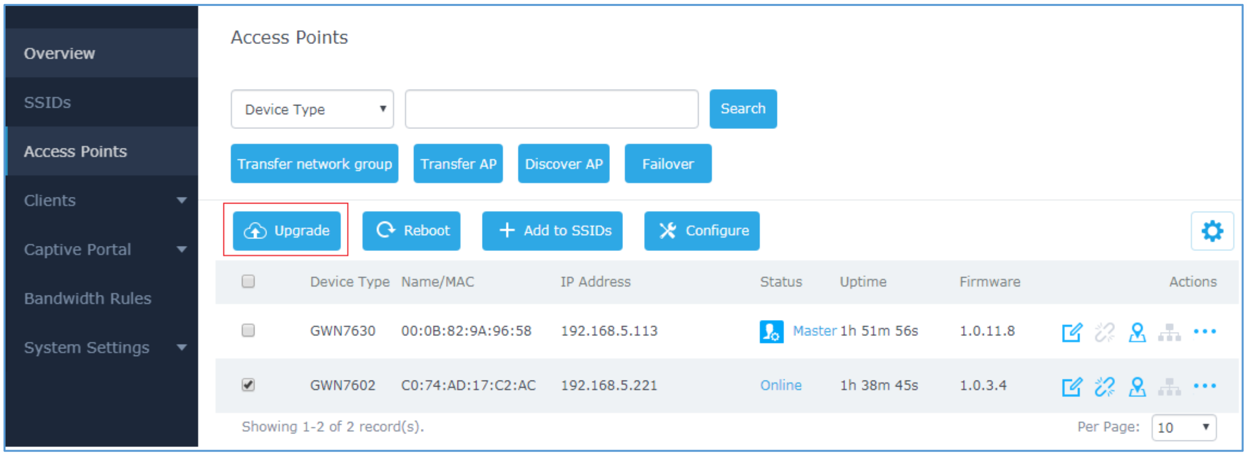
Table 21: Network Upgrade Configuration

Field	Description
Authenticate Config File	Authenticates configuration file before acceptance. The default setting is No.
XML Config File Password	The password for encrypting the XML configuration file using OpenSSL. The password is to decrypt the XML configuration file is it is encrypted via OpenSSL
Upgrade Via	Allow users to choose the method to load the firmware and config: TFTP, HTTP or HTTPS.
Firmware Server	Define the IP address or URL for the firmware upgrade server. Make sure all files relevant to the firmware are updated completely
Config Server	Configure the IP address of URL for the file server.
Check/Download New Firmware and Config at Boot	Configure whether to enable/disable automatic upgrade and provisioning when reboot.
Allow DHCP options 66 and 43 override	Enable/Disable DHCP options 66 and 43 to override the upgrade and provisioning settings

Automatic Upgrade	Set automatic upgrade every intervals/day/week. The device will request to upgrade automatically according to the setup time. The default setting is Disabled
X Hours	Select the time period to check for firmware upgrade. *This field is available when select "Check every X Hours" in "Automatic Upgrade"*
Hour of Day (0-23)	Defines the hour of the day (0-23) to check the HTTP/TFTP server for firmware upgrade or configuration file changes. *This field is available when select "Check at Hour of Day" and "Check at Day of Week" in "Automatic Upgrade"*
Day of Week	Defines the day of the week to check the HTTP/TFTP server for firmware upgrade or configuration file changes. *This field is available when select "Check at Day of Week" in "Automatic Upgrade"*
Upgrade Now	Click on Upgrade button to begin the upgrade. Note that the device will reboot after downloading the firmware. Note: Please save and apply your configuration first if there are any configuration modification.
Download Configuration	Click on Download button to download the device configuration file to PC.
Upload Configuration	Click on Upload to select a compressed config file to restore the config; after succeeding, the device will reboot automatically.
Reboot	Click on Reboot button to reboot device.
Factory Reset	Click on Reset to restore the device and all online APs to factory default settings.

When the GWN7602 is being paired as slave using another GWN76XX Access Point acting as Controller, users can upgrade their paired access points from the GWN76XX Master Controller.

To upgrade the GWN7602, log in to the GWN76XX acting as Master Controller and go to **Access Points.**



□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7630	00:0B:82:9A:96:58	192.168.5.113	Master	1h 51m 56s	1.0.11.8	•••
☑	GWN7602	C0:74:AD:17:C2:AC	192.168.5.221	Online	1h 38m 45s	1.0.3.4	•••

Showing 1-2 of 2 record(s).

Per Page: 10

Figure 43: Upgrading GWN7602

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

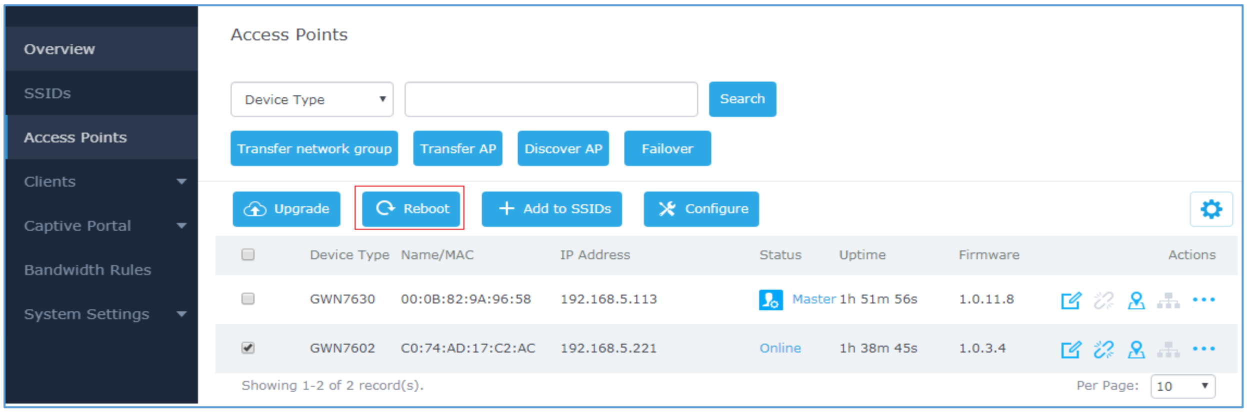
Provisioning

Configuration Server

Users can provision the GWN7602 by putting the config file on a TFTP/HTTP or HTTPS server and set Config Server from the Master GWN76XX to the TFTP/HTTP or HTTPS server used in order for the GWN7602 to be provisioned with that config file

Reboot

Users could perform a reboot under the Master GWN76XX Web GUI **Access Points** page by clicking on Reboot button as shown in below screenshot.



□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7630	00:0B:82:9A:96:58	192.168.5.113	Master	1h 51m 56s	1.0.11.8	•••
☑	GWN7602	C0:74:AD:17:C2:AC	192.168.5.221	Online	1h 38m 45s	1.0.3.4	•••

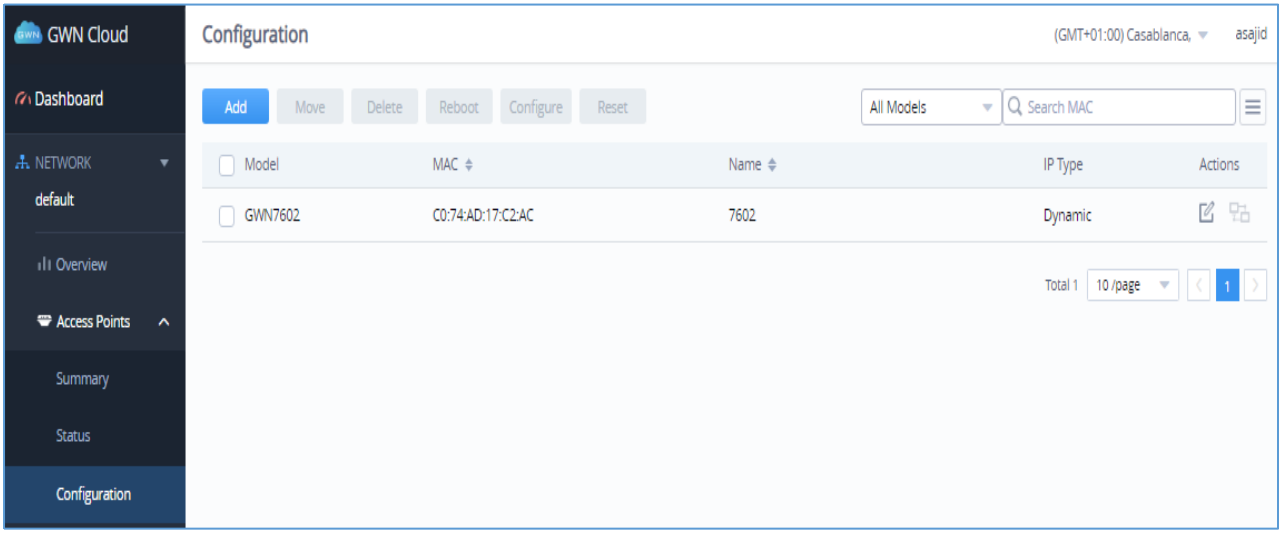
Showing 1-2 of 2 record(s).

Per Page: 10

Figure 44: Reboot GWN7602 from Master AP

MANAGING GWN7602 FROM GWN CLOUD

The GWN7602 can be managed by your **GWN.Cloud** account, **GWN Cloud** web interface now can be accessed at: https://www.gwn.cloud.



Model	MAC	Name	IP Type	Actions
GWN7602	C0:74:AD:17:C2:AC	7602	Dynamic	

Figure 45: GWN Cloud Web GUI

.

For Further information, please refer to the GWN Cloud user guide in below link:

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

EXPERIENCING THE GWN7602 Wi-Fi ACCESS POINTS

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 GWN7602 Wi-Fi Access Point, it will be sure to bring convenience and color to both your business and personal life