Grandstream Networks, Inc.

GWN7610

Enterprise 802.11ac WiFi Access Point

User Manual

COPYRIGHT

The latest electronic version of this guide is available for download here:
http://www.grandstream.com/support
Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.

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

GWN7610 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 GWN7610 via Web GUI in standalone mode, with other GWN7610 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 “GWN7610 User Manual”.

This guide covers following topics:

- Product Overview
- Installation
- Getting Started
- Using GWN7610 as Standalone Access Point
- Using GWN7610 as Master Access Point Controller
- Network Groups
- Client Configuration
- System Settings
- LED Schedule
- Captive Portal
- Bandwidth Rules
- Upgrading and Provisioning
- Experiencing the GWN7610 Wireless Access Point

CHANGE LOG

This section documents significant changes from previous versions of the GWN7610 user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.4.20

- Enhanced Client Blocking and management features. [CLIENTS CONFIGURATION]
- Added support for Client Bridge. [Client Bridge]
- Added support for Syslog Server. [Logserver]
- Added support for Configurable web UI access port. [Web HTTPS Port]
- Added support for E-mail notifications. [Email/Notification]

Firmware Version 1.0.3.21

- No major changes.

Firmware Version 1.0.3.19

- Added support for Bandwidth Rules [BANDWIDTH RULES]
- Added support for legacy 802.11b [Allow Legacy Device]
- Added support for custom wireless power [Custom Wireless Power]
- Added support for better roaming decision [Enable Voice Enterprise]
- Added support for failover master [Failover Master]
- Added options to select band per SSID [SSID Band]
- Added support for VLAN assignment via Radius [Enable Dynamic VLAN]
- Added option to selectively enable different Wi-Fi norms (802.11b/g/n) [Mode(2.4G)]
- Added option to limit clients count per SSID [Wireless Client Limit]
- Added option to enable/disable DHCP option 66 & 43 override [Allow DHCP options 66 and 43 override]

Firmware Version 1.0.2.108

- Added Controller protocol security enhancement [Controller Protocol Security Enhancement]
- Added support for LED control [LED SCHEDULE]
- Added support for Captive Portal [CAPTIVE PORTAL]
- Added support for Additional SSID [Additional SSID under Same Network Group]
- Added support for Wi-Fi schedule [Schedule]
- Added Client Isolation enhancement [Client Isolation]
- Added support to store Syslog locally on the unit and display it on Web GUI [Syslog]

Firmware Version 1.0.2.15

- Added New Overview Page

- Added Web UI enhancement
- Added support for Password change on first boot [Change Password on first boot]
- Added Country code selection into setup wizard

Firmware Version 1.0.1.27

- This is the initial version

WELCOME

Thank you for purchasing Grandstream GWN7610 Enterprise Wireless Access Point. The GWN7610 is a high-performance 802.11ac wireless access point for small to medium sized businesses, multiple floor offices, commercial locations and branch offices. It offers dual-band 3x3:3 MIMO technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range. To ensure easy installation and management, the GWN7610 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 50 GWN7610s independently without needing seperate controller hardware/software and without a single point-of-failure.

This wireless access point can be paired with any third party routers. With support for advanced QoS, low-latency real-time applications, 250+ client devices per AP and dual Gigabit network ports with PoE/PoE+, the GWN7610 is an ideal wireless access point for large and small wireless network deployments.

⚠ **Caution:**

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

PRODUCT OVERVIEW

Technical Specifications

Table 1: GWN7610 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac
Antennas	3x 2.4 GHz, gain 3 dBi, internal antenna 3x 5 GHz, gain 3 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 1300 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 450 Mbps 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 (FCC, IC, RCM)
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	3x3:3 2.4GHz, 3x3:3 5GHz
Coverage Range	575ft. (175 meters) **coverage range can vary based on environment*
Maximum TX Power	5G: 26dBm (FCC) / 20dBm (CE) 2.4G: 26dBm (FCC) / 17dBm (CE) **Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b:-92dBm@11Mbps; 802.11g:-76dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz:-70dBm@MCS7 **5G** 802.11a:-94dBm@6Mbps; 801.11a:-77dBm@54Mbps; 802.11ac 20MHz: -69dBm@MCS8; 802.11ac HT40:-65dBm@MCS9; 802.11ac 80MHz:

	1dBm@MCS9 ** Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	16 SSIDs per access point
Concurrent Clients	250+
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	3 tri-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 GWN7610 allows it to auto-discover, auto-provision and manage up to 50 GWN7610s in a network
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	DC Input: 24VDC/1A Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 13.8W
Environmental	Operation: 0°C to 50°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: 540g **Unit + Mounting Kits Dimension:** 205.3 x 205.3 x 50.9mm; **Unit + Mounting Kits Weight:** 600g **Entire Package Dimension:** 258 x 247 x 86mm; **Entire Package Weight**: 900g
Package Content	GWN7610 802.11ac Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

INSTALLATION

Before deploying and configuring the GWN7610, 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 GWN7610.

Equipment Packaging

Table 2: GWN7610 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)

GWN7610 Access Point Ports

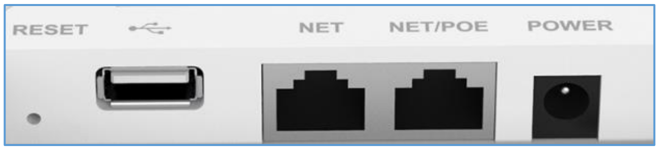


Figure 1: GWN7610 Ports

Table 3: GWN7610 Ports Description

Port	Description
Power	Power adapter connector (24V, 1A)
NET/PoE	Ethernet RJ45 port (10/100/1000Mbps) supporting PoE/PoE+ (802.3af/802.3at).
NET	Ethernet RJ45 port (10/100/1000Mbps) to your router or another GWN7610 series
	USB 2.0 port (for future IOT & location based applications)
RESET	Factory reset button. Press for 7 seconds to reset factory default settings.

Power and Connect GWN7610 Access Point

Step 1:

Connect one end of a RJ-45 Ethernet cable into the NET or PoE/NET port of the GWN7610.

Step 2:

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

Step 3:

Connect the 24V DC power adapter into the power jack on the back of the GWN7610. Insert the main plug of the power adapter into a surge-protected power outlet.

Notes:

- GWN7610 can be powered using PoE(802.3af)/PoE+(802.3at) switch via PoE/NET port. In this scenario, GWN7610 should be connected to the Router using NET port.
- GWN7610 has a PoE detection daemon that will monitor the status and update maximum allowable power for USB ports in real time.

Step 4:

Wait for the GWN7610 to boot up and acquire an IP address from the DHCP Server.

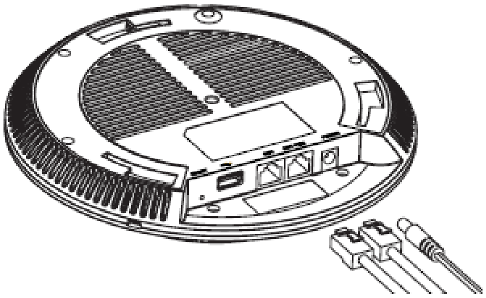


Figure 2: Connecting GWN7610

Warranty

If the GWN7610 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

GWN7610 can be mounted on the wall or ceiling, please refer to the following steps for the appropriate installation.

Wall Mount

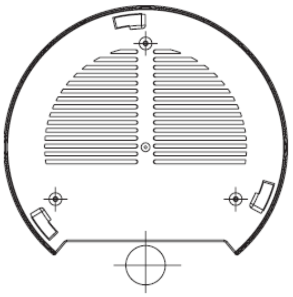


Figure 3: Wall Mount – Steps 1 & 2

Step1:

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

Step 2:

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

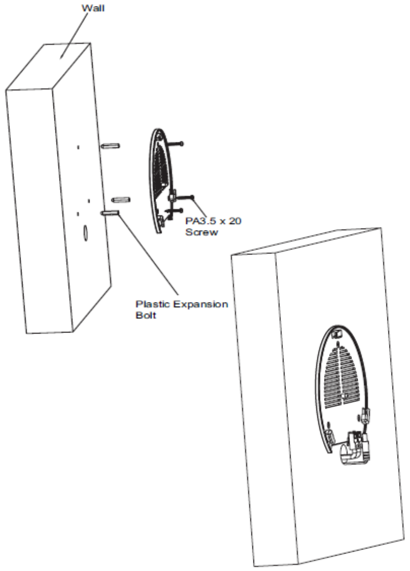


Figure 4: Wall Mount – Steps 3 & 4

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 GWN7610.

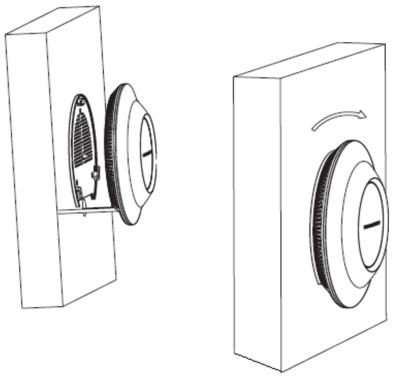


Figure 5: Wall Mount – Steps 5 & 6

Step 5:

Align the arrow on the GWN7610AP 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.

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).

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 GWN7610.

Step 5:

Align the arrow on the GWN7610AP 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.

⚠ **Note:**

Ceiling mounting is recommended for optimal coverage performance.

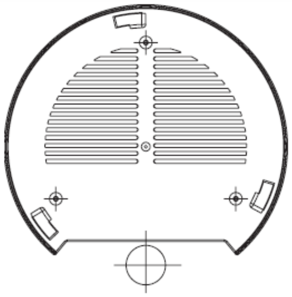


Figure 6: Ceiling Mount – Steps 1 & 2

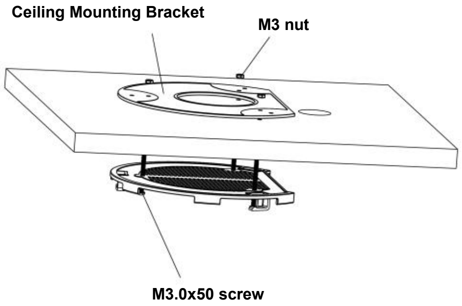


Figure 7: Ceiling Mount – Step 3

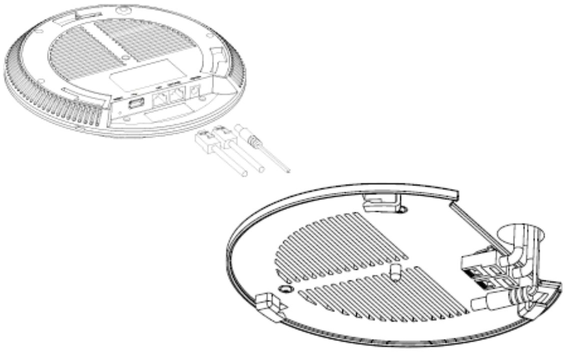


Figure 8: Ceiling Mount – Step 4

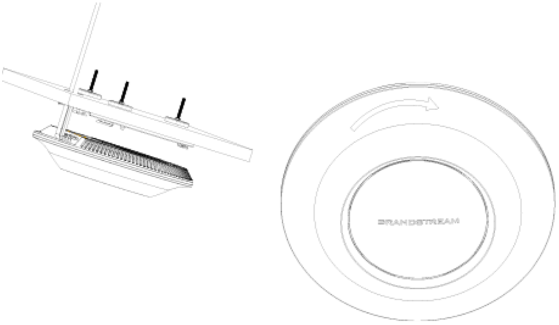


Figure 9: Ceiling Mount – Steps 5 & 6

GETTING STARTED

The GWN7610 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 GWN7610's setup.

This section provides step-by-step instructions on how to read LED patterns, discover the GWN7610 and use its Web GUI interface.

LED Patterns

The panel of the GWN7610 has different LED patterns for different activities, to help users read the status of the GWN7610 whether it's powered up correctly, provisioned, in upgrading process and more, for more details please refer to the below table.

Table 4: LED Patterns

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

Discover the GWN7610

Once the GWN7610 is powered up and connected to the Network correctly, users can discover the GWN7610 using one of the below methods:

Method 1: Discover the GWN7610 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 GWN7610, type in the following address using the GWN7610's MAC address on your browser.

For example, if a GWN7610 has the MAC address **00:0B:82:8B:4E:28**, this unit can be accessed by typing https://gwn_000b828b4e28.local/ on the browser.

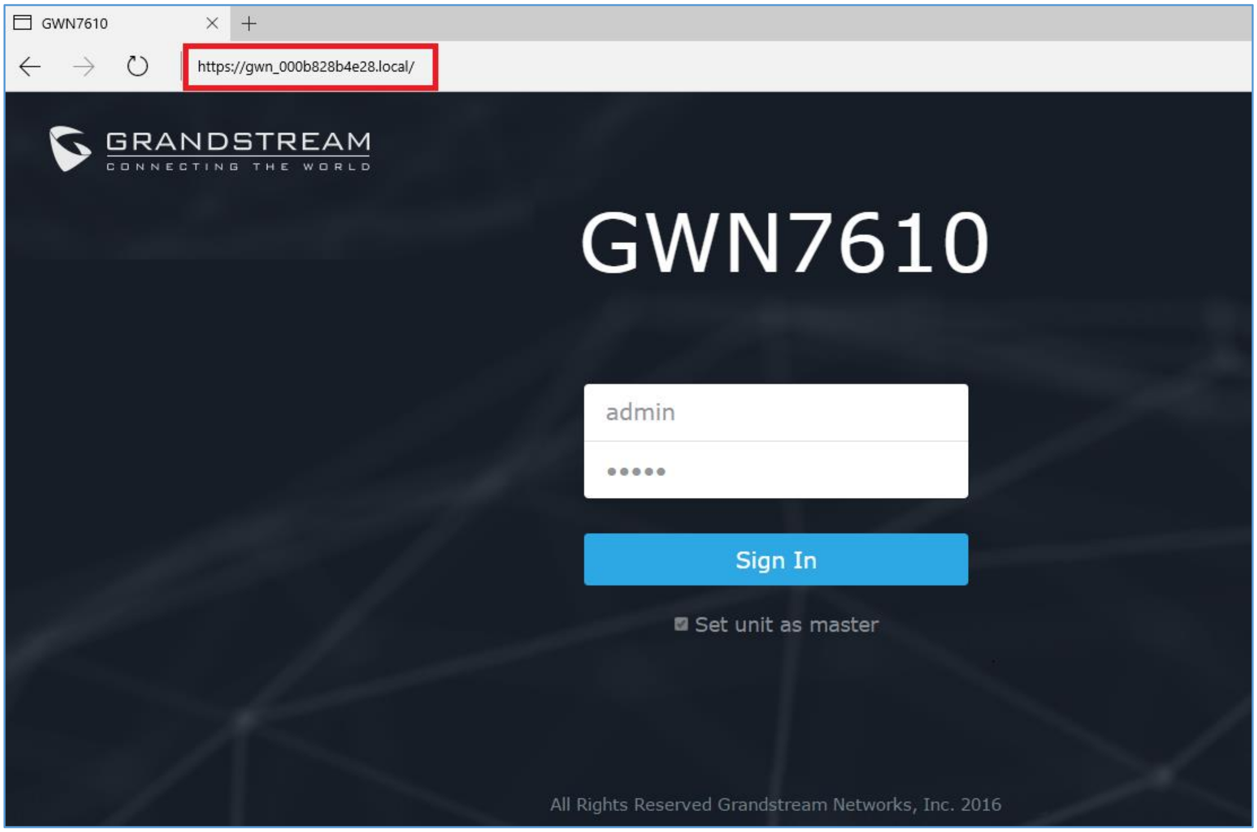
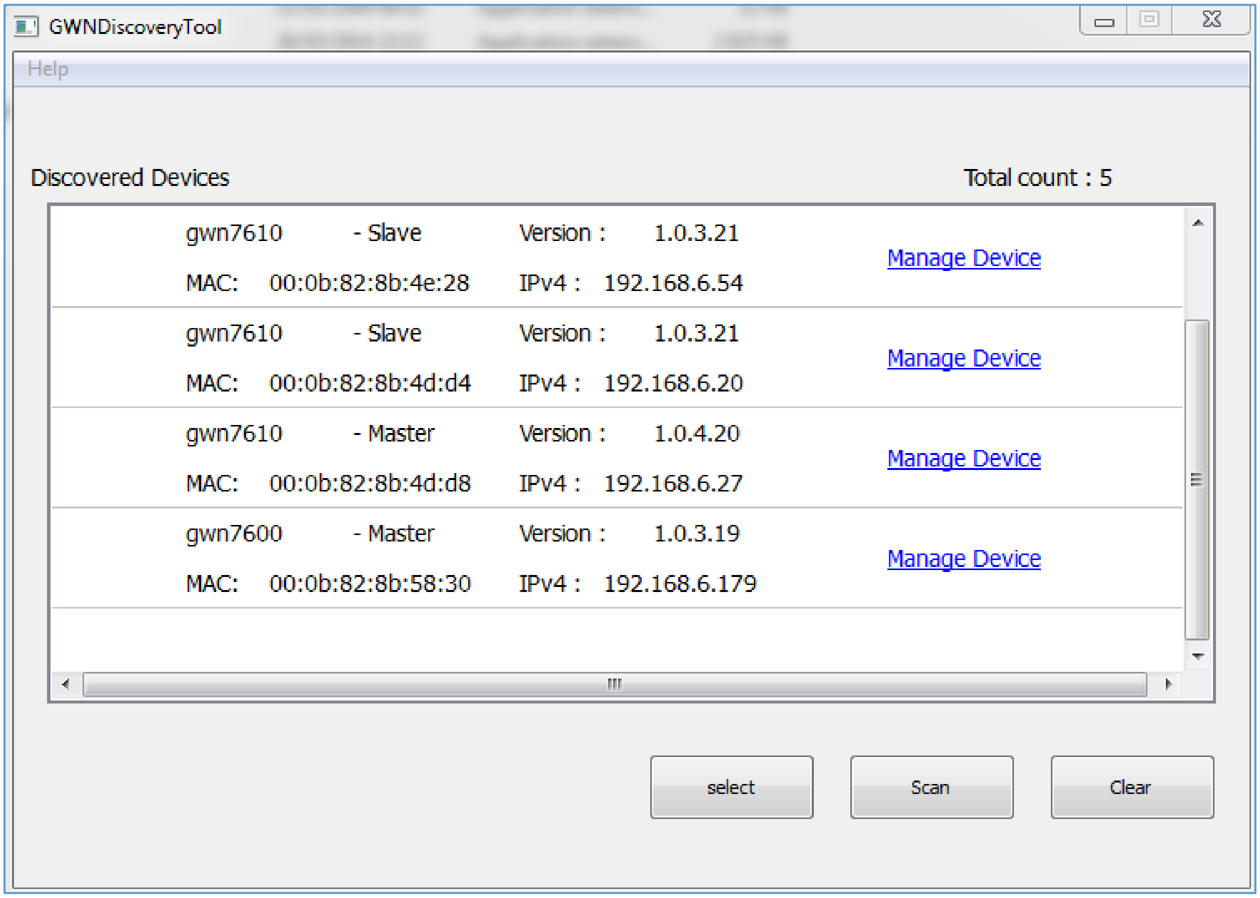

GWN7610
https://gwn_000b828b4e28.local/
GRANDSTREAM
CONNECTING THE WORLD
GWN7610
admin
•••••
Sign In
☑ Set unit as master
All Rights Reserved Grandstream Networks, Inc. 2016

Figure 10: Discover the GWN7610 using its MAC Address

Method 2: Discover the GWN7610 using GWNDiscoveryTool

1. Download and install **GWNDiscoveryTool** from the following link: http://www.grandstream.com/sites/default/files/Resources/GWNDiscoveryTool.zip
2. Open the GWNDiscoveryTool, click on **Select** to define the network interface, then click on **Scan**.
3. The tool will discover all GWN7610 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 GWN7610's configuration interface, or type in manually the displayed IP address on your browser.



Discovered Devices Total count : 5

gwn7610 - Slave Version : 1.0.3.21
MAC: 00:0b:82:8b:4e:28 IPv4 : 192.168.6.54 Manage Device

gwn7610 - Slave Version : 1.0.3.21
MAC: 00:0b:82:8b:4d:d4 IPv4 : 192.168.6.20 Manage Device

gwn7610 - Master Version : 1.0.4.20
MAC: 00:0b:82:8b:4d:d8 IPv4 : 192.168.6.27 Manage Device

gwn7600 - Master Version : 1.0.3.19
MAC: 00:0b:82:8b:58:30 IPv4 : 192.168.6.179 Manage Device

Figure 11: GWN Discovery Tool

Users can access then the GWN7610 using its Web GUI, the following sections will explain how to access and use the Web Interface.

Use the Web GUI

Access Web GUI

The GWN7610 embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome etc.

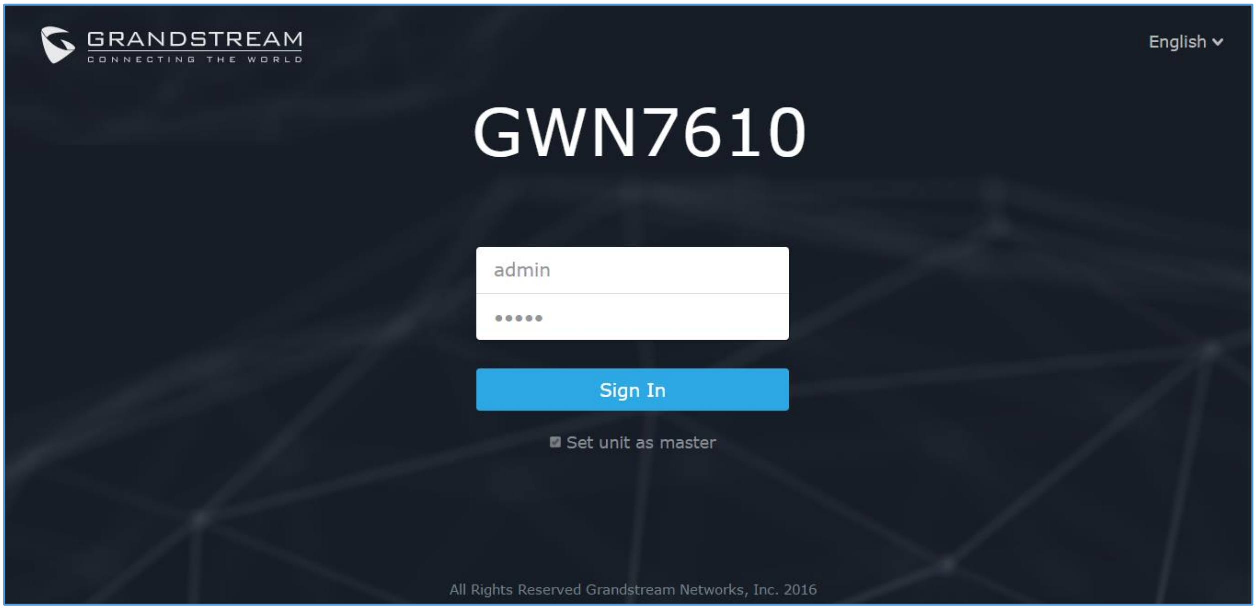


Figure 12: GWN7610 Web GUI Login Page

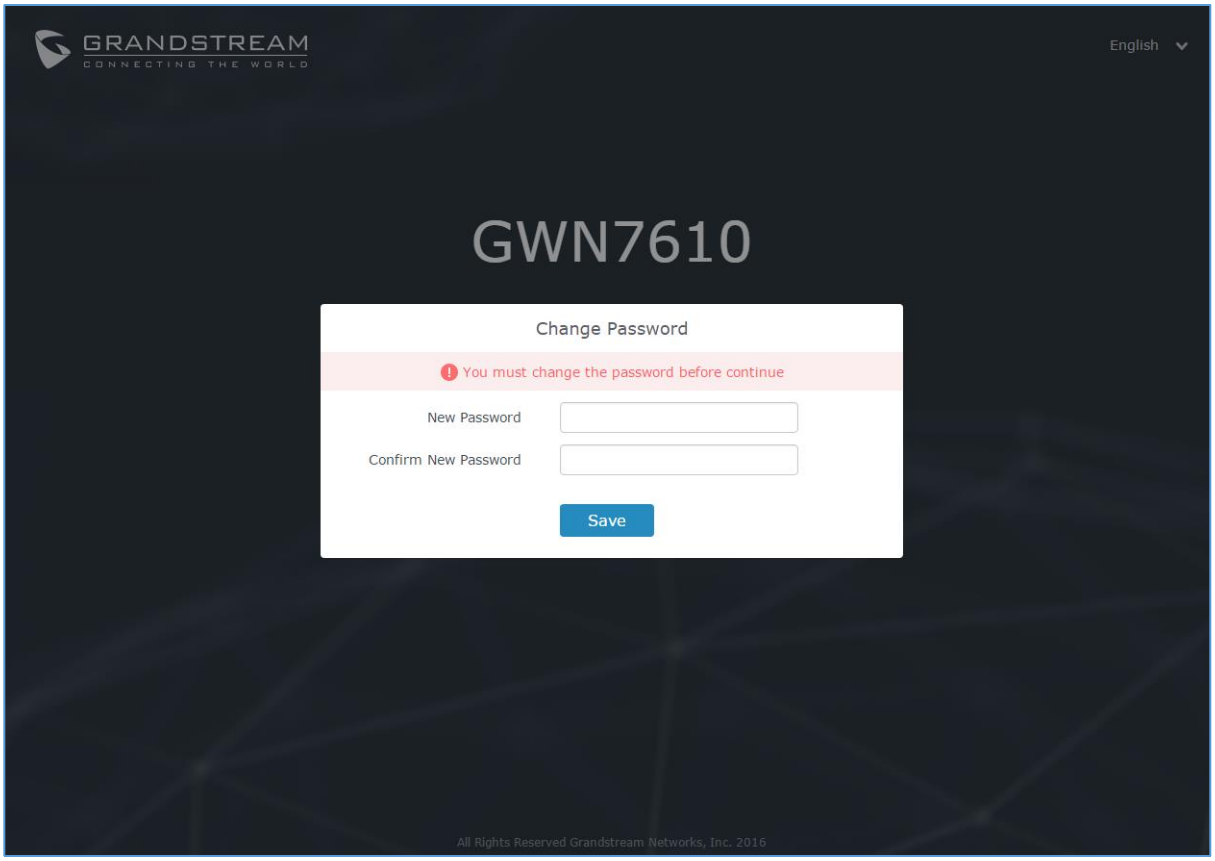
To access the Web GUI:

1. Make sure to use a computer connected to the same local network as the GWN7610.
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 GWN7610*** 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".

Note: At first boot or after factory reset, users will be asked to change the default administrator password before accessing GWN7610 Web interface.

The new password field is case sensitive with a maximum length of 32 characters. Using strong password including letters, digits and special characters is recommended for better security.



Change Password

You must change the password before continue

New Password

Confirm New Password

Figure 13: Change Password on first boot

Web GUI Languages

Currently the GWN7610 series Web GUI supports ***English*** and ***Simplified Chinese.***
Users can select the displayed language at the upper right of the Web GUI either before or after logging in.

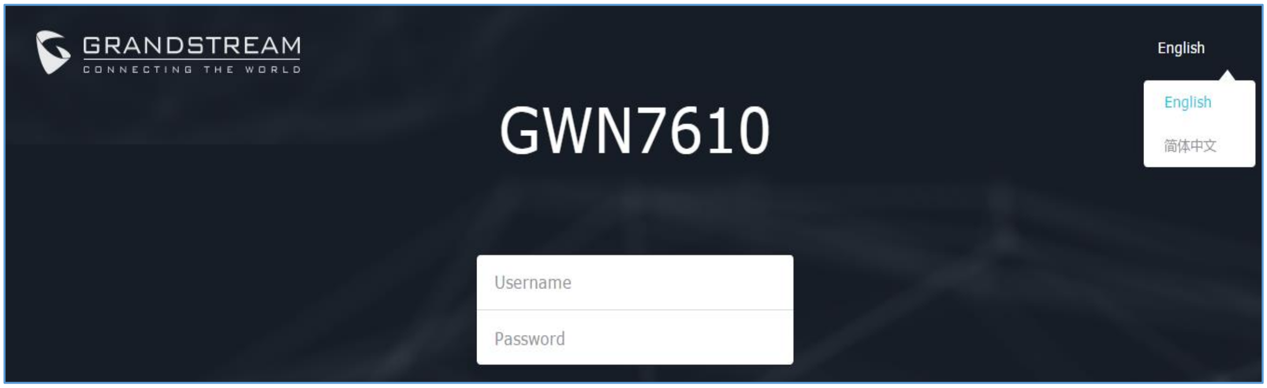


Figure 14: GWN7610 Web GUI Language – Login page

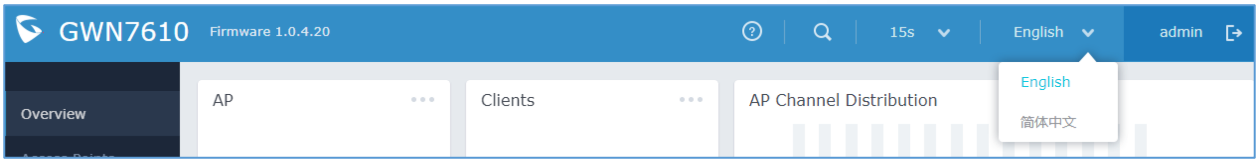
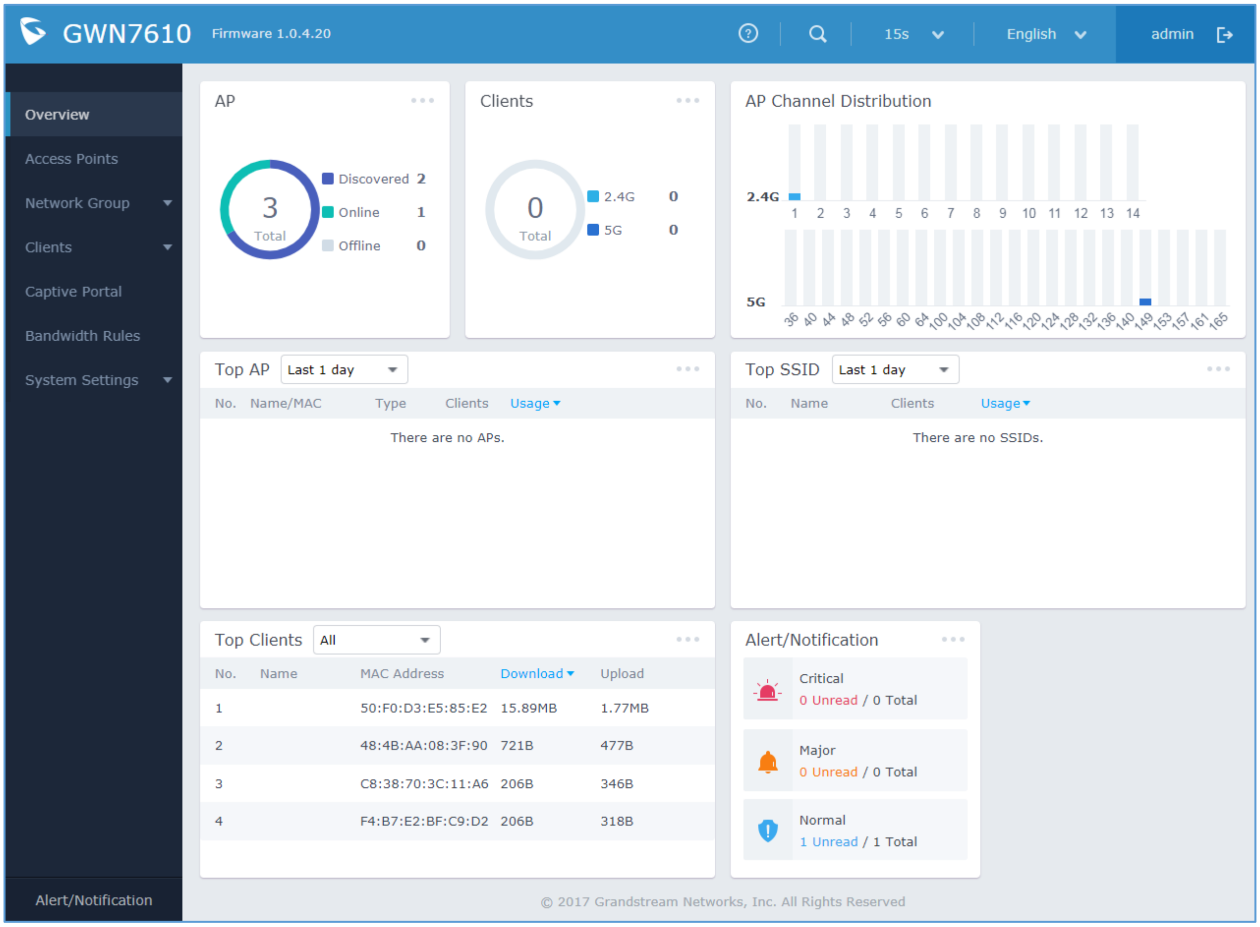


Figure 15: GWN7610 Web GUI Language

Overview Page

Overview is the first page shown after successful login to the GWN7610's Web Interface. Overview page provides an overall view of the GWN7610's information presented in a Dashboard style for easy monitoring.



No.	Name/MAC	Type	Clients	Usage

There are no APs.

No.	Name	Clients	Usage

There are no SSIDs.

No.	Name	MAC Address	Download	Upload
1		50:F0:D3:E5:85:E2	15.89MB	1.77MB
2		48:4B:AA:08:3F:90	721B	477B
3		C8:38:70:3C:11:A6	206B	346B
4		F4:B7:E2:BF:C9:D2	206B	318B

Figure 16: Overview Page

Users can quickly see the status of the GWN7610 for different items, please refer to the following table for each item:

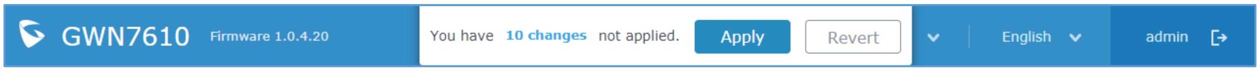
Table 5: Overview

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

Note that 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.



You have 10 changes not applied.

Figure 17: Apply Changes

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

USING GWN7610 AS STANDALONE ACCESS POINT

The GWN7610 can be used in Standalone mode, where it can act as Master Access Point Controller or in Slave mode and managed by another GWN7610 Master.

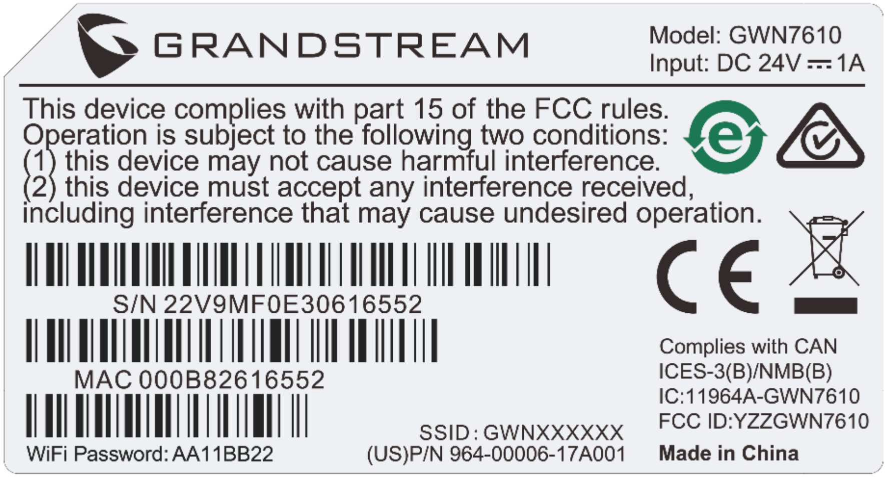
This section will describe how to use and configure the GWN7610 in standalone mode.

Connect to GWN7610 Default Wi-Fi Network

GWN7610 can be used as standalone access point out of box, or after factory reset with Wi-Fi enabled by default.

After powering the GWN7610 and connecting it to the network, GWN7610 will broadcast a default SSID based on its MAC address **GWN[MAC's last 6 digits]** and a random password.

Note that GWN7610's default SSID and password information are printed on the MAC tag of the unit as shown on the below figure.



GRANDSTREAM

Model: GWN7610
Input: DC 24V ⎓ 1A

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

S/N 22V9MF0E30616552

MAC 000B82616552

WiFi Password: AA11BB22

SSID: GWNXXXXXX

(US)P/N 964-00006-17A001

Complies with CAN
ICES-3(B)/NMB(B)
IC:11964A-GWN7610
FCC ID:YZZGWN7610
Made in China

Figure 18: MAC Tag Label

USING GWN7610 AS MASTER ACCESS POINT CONTROLLER

Master Mode allows a GWN7610 to act as an Access Point Controller managing other GWN7610 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 need more coverage area zones with the same controller.

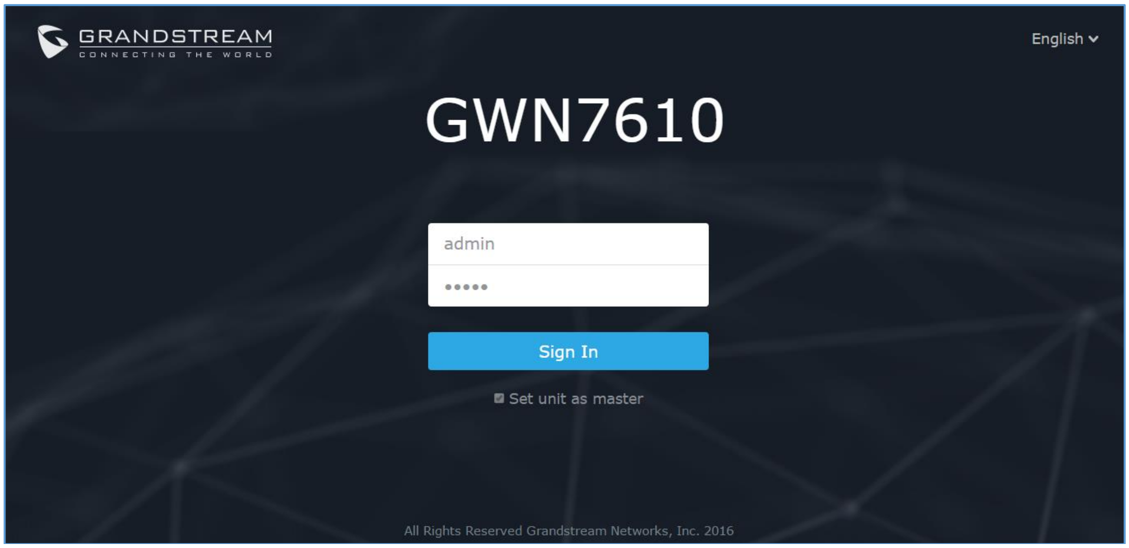


Figure 19: Login Page

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

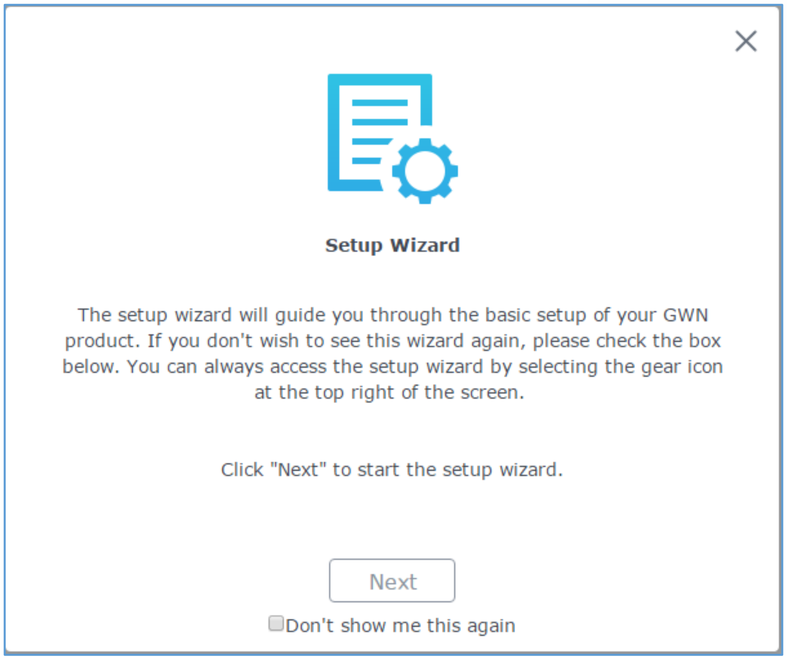
⚠ **Warning:**

"**Set unit as Master**" option will forbid the GWN7610 Access Point from being paired by other Master GWN7610, and can only act as a Master Access point controller.

Users will need to perform a factory reset to the GWN7610, or unpair it from the initial GWN7610 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.



Setup Wizard

The setup wizard will guide you through the basic setup of your GWN product. If you don't wish to see this wizard again, please check the box below. You can always access the setup wizard by selecting the gear icon at the top right of the screen.

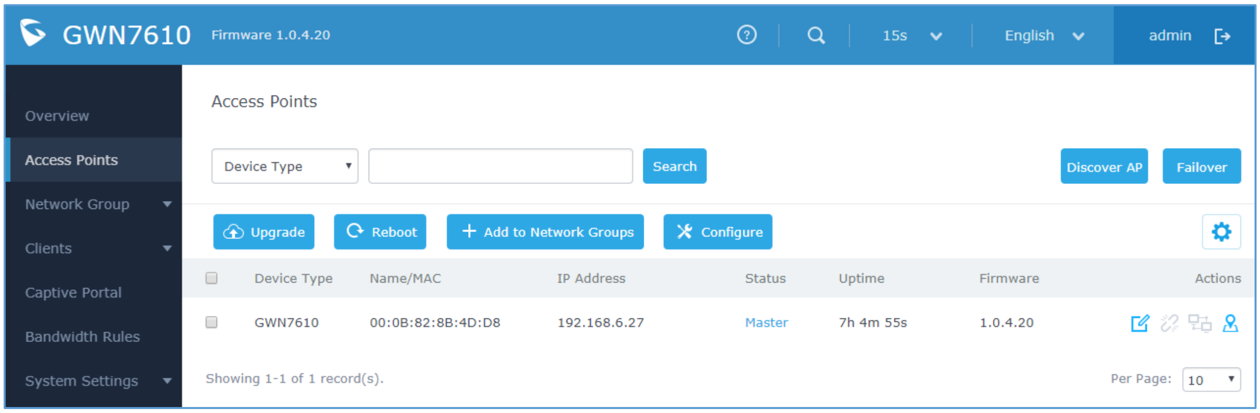
Click "Next" to start the setup wizard.

Figure 20: Setup Wizard

Discover and Pair Other GWN7610 Access Point

To Pair a GWN7610 access point connected to the same Network as the GWN7610 follow the below steps:

1. Connect to the GWN7610 Web GUI as Master and go to **Access Points.**



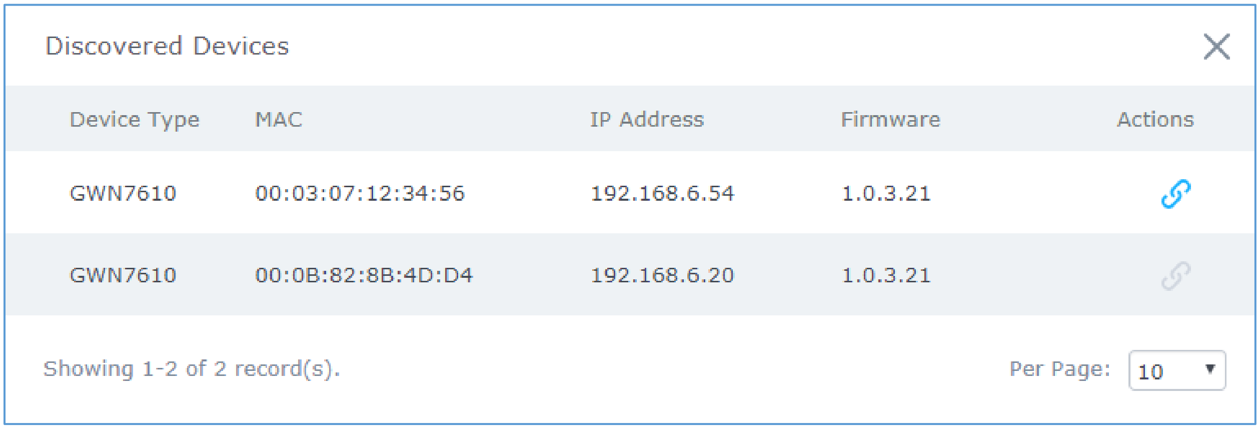
Access Points

□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7610	00:0B:82:8B:4D:D8	192.168.6.27	Master	7h 4m 55s	1.0.4.20	

Showing 1-1 of 1 record(s).

Figure 21:Discover AP

2. Click on Discover AP discover access points within GWN7610's Network, the following page will appear.



Discovered Devices

Device Type	MAC	IP Address	Firmware	Actions
GWN7610	00:03:07:12:34:56	192.168.6.54	1.0.3.21	🔗
GWN7610	00:0B:82:8B:4D:D4	192.168.6.20	1.0.3.21	🔗

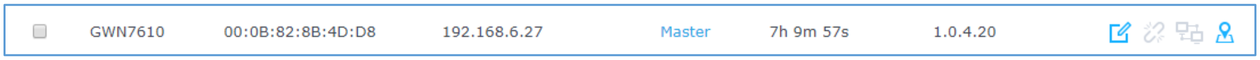
Showing 1-2 of 2 record(s).

Per Page: 10

Figure 22: Discovered Devices

Note: Discovered Slave Aps with lower firmware than the master AP will be highlighted in red bold to remind the users to upgrade their AP, more details refer to [Controller Protocol Security Enhancement]

3. Click on Pair 🔗 under Actions, to pair the discovered Access Point as Slave with the GWN7610 acting as Master
4. The paired GWN7610 will appear Online, users can click on to unpair it.



□	GWN7610	00:0B:82:8B:4D:D8	192.168.6.27	Master	7h 9m 57s	1.0.4.20

Figure 23: GWN7610 online

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

Table 6: Device Configuration

Field	Description
Status	Shows the device's status information such as Firmware version, IP Address, Link Speed, Uptime, and Users count via different Radio channels.
Clients	Shows the users connected to the GWN7610 access point.
Configuration	• **Device Name:** Set GWN7610's name to identify it along with its MAC address. • **Fixed IP:** Used to set a static IP for the GWN7610, if checked users will need to set the following: *-IPv4 Address:* Enter the IPv4 address to be set as static for the device

-IPv4 Subnet Mask: Enter the Subnet Mask.

-IPv4 Gateway: Enter the Network Gateway's IPv4 Address.

-Preferred IPv4 DNS: Enter the Primary IPv4 DNS.

-Alternate IPv4 DNS: Enter the Alternate IPv4 DNS.

- **Frequency:** Set the GWN7610's frequency, it can be either 2.4GHz, 5GHz or Dual-band.
- **Enable 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(2.4G):** Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.
- **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20MHz is suggested in very high density environment.
- **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be "Secondary Below Primary", "Primary Below Secondary" or "Auto".
- **Channel:** Select "Auto" or a specific channel. Default is "Auto". Note that the proposed channels depend on **Country** Settings under **System Settings–>Maintenance**.
- **Enable Short Guard Interval:** Check to activate this option to increase throughput.
- **Active Spatial Streams:** Choose active spatial stream. Available options: "Auto", "1 stream", "2 streams" and "3 streams".
- **Radio Power:** Set the Radio Power depending on desired cell size to be broadcasted, three options are available: "Low", "Medium" or "High". Default is "High".
- **Allow Legacy Device(802.11b):** This feature appears when "Mode" option is set to "802.11g" or "802.11n", it allows legacy devices not supporting "802.11g/n" mode to connect using the "802.11b" mode.

	• **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 GWN7610 is not being paired or the pair icon is grey color, make sure that it is not being paired with another GWN7610 Access Point acting as Master Controller, if yes, users will need to unpair it first, or reset it to factory default settings to make it available for pairing by other GWN7610 Access Point Controller.

Locate Other Access Points by Blinking LED

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.

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.

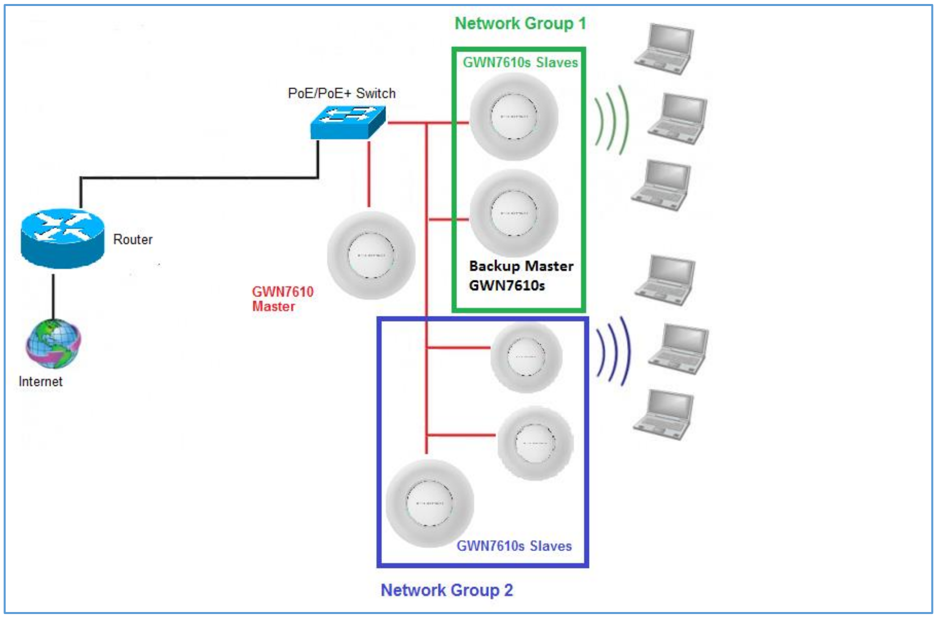


Figure 24: Failover Master

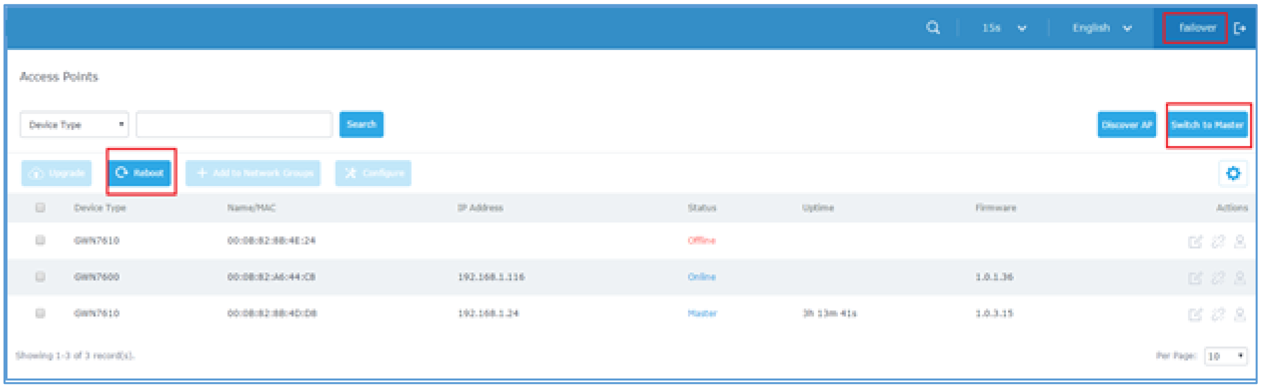
Users could select the failover Master by following below steps:

- 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**



	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7610	00:0B:82:8B:4E:24		Offline			
□	GWN7600	00:0B:82:A6:44:C8	192.168.1.116	Online		1.0.1.36	
□	GWN7610	00:0B:82:8B:4D:D8	192.168.1.24	Master	3h 13m 41s	1.0.3.15	

Showing 1-3 of 3 record(s).

Per Page: 10

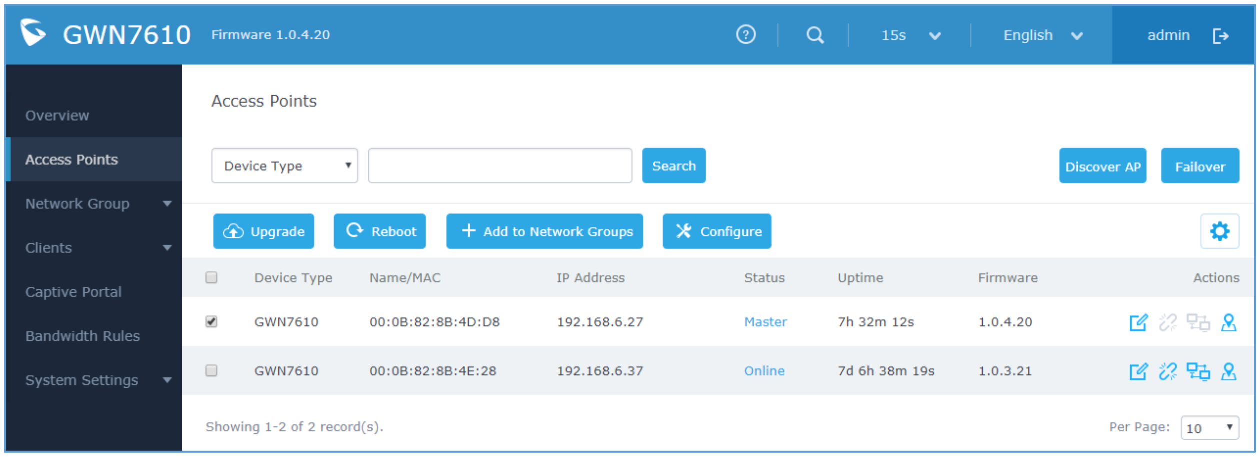
Figure 25: Failover Mode GUI

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.

Controller Protocol Security Enhancement

Controller protocol security enhancement is important for secured provision from Master to Slave. So once a master with 1.0.2.108 found a slave with an older firmware, it will disable the slave’s Wi-Fi and show the slave’s firmware version in RED BOLD to remind user to upgrade the slave as shown on figure below.



GWN7610 Firmware 1.0.4.20 | 15s | English | admin

- Overview
- Access Points
- Network Group
- Clients
- Captive Portal
- Bandwidth Rules
- System Settings

Access Points

Device Type | Search | Discover AP | Failover

Upgrade | Reboot | Add to Network Groups | Configure

□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
☑	GWN7610	00:0B:82:8B:4D:D8	192.168.6.27	Master	7h 32m 12s	1.0.4.20	
□	GWN7610	00:0B:82:8B:4E:28	192.168.6.37	Online	7d 6h 38m 19s	1.0.3.21	

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

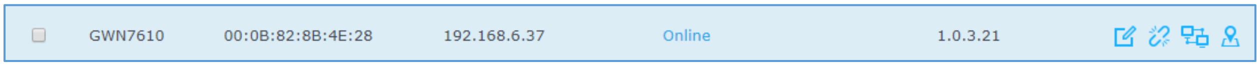
Figure 26: Controller Protocol Security Enhancement

Client Bridge

The Client Bridge feature allows an access point to be configured as a client for bridging wired only clients wirelessly to the network. When an access point is configured in this way, it will share the WiFi connection to the LAN ports transparently. This is not to be confused with a mesh setup. The client will not accept wireless clients in this mode.

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

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



□	GWN7610	00:0B:82:8B:4E:28	192.168.6.37	Online	1.0.3.21

Figure 27: Client Bridge

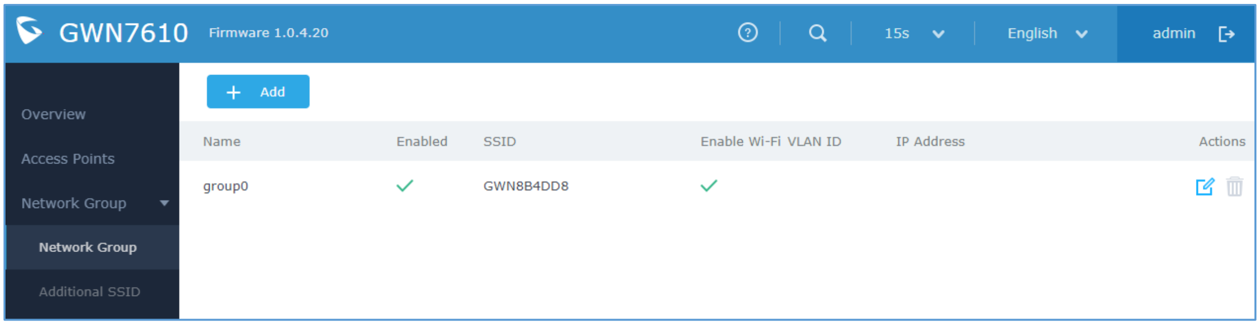
Important Notes:

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

NETWORK GROUPS

When using GWN7610 as Master Access Point, users can create different Network groups and adding GWN7610 Slave Access Points.

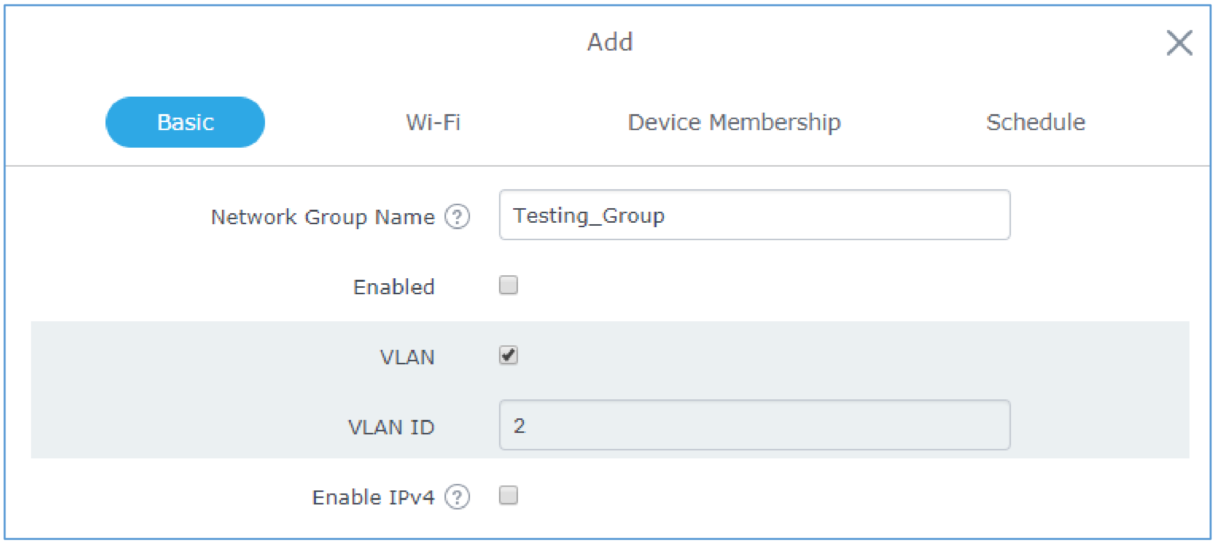
Log in as Master to the GWN7610 WebGUI and go to **Network Group→Network Group.**



Name	Enabled	SSID	Enable Wi-Fi	VLAN ID	IP Address	Actions
group0	✓	GWN8B4DD8	✓			

Figure 28: Network Group

The GWN7610 will have a default network group named group0, click on ✎ to edit it, or click on ⊕ Add to add a new network group.



Network Group Name	Testing_Group
Enabled	☐
VLAN	☑
VLAN ID	2
Enable IPv4	☐

Figure 29: Add a New Network Group

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

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

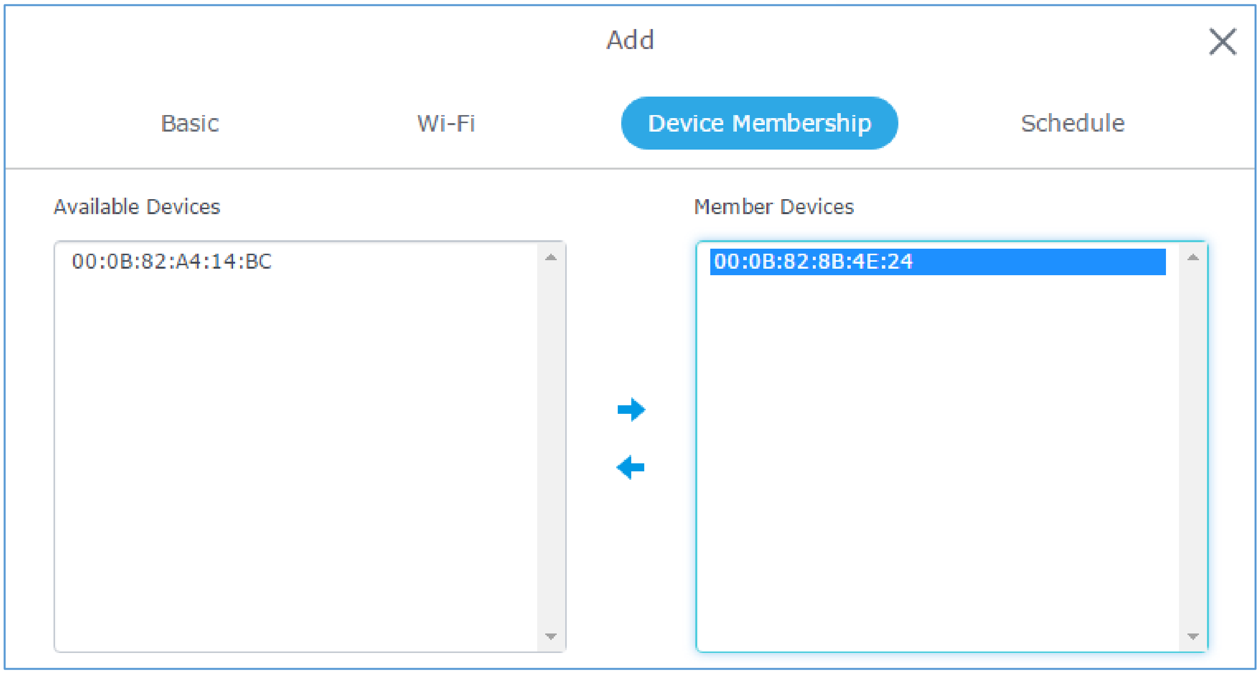
Table 7: Wi-Fi

Field	Description
Enable Wi-Fi	Check to enable Wi-Fi for the network group.
SSID	Set or modify the SSID name.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: • **Dual-Band** • **2.4GHz** • **5Ghz**
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. If set to 0 the limit is disabled.
Enable Captive Portal	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.
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	Select key mode (Pre-Shared Key or 802.1X Authentication).
WPA Encryption Type	Select Encryption type (AES or AES/TKIP).

WPA Pre-Shared Key	Configures the WPA pre-shared key. The input range: 8-63 ASCII characters or 8-64 hex characters.
Client Bridge Support	Configures the client bridge support to allows the access point to be configured as a client for bridging wired only clients wirelessly to the network. When an access point is configured in this way, it will share the WiFi connection to the LAN ports transparently. Once a Network Group has an Client Bridge Support enabled, the AP adopted in this Network Group can be turned in to Bridge Client mode by click the Bridge button.
RADIUS Sever Address	Configures RADIUS authentication server address.
RADIUS Server Port	Configures RADIUS Server Listening port (defaults to 1812).
RADIUS Server Secret	Enter the secret password for client authentication with 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.
RADIUS NAS ID	Configures the Radius NAS ID used to notify the source of RADIUS access request so that, the RADIUS server can choose policy for that request.
Client Time Policy	Configures the client time policy. Default is None.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to the zone’s WiFi. Default is Disabled.
Enable Dynamic VLAN	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile.
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN7610’s Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public WiFi. The available modes are: • **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 GWN7610. • **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 GWN7610 access points.

	• **Radio Mode:** *Wireless clients can access to the internet services*, GWN7xxx router and the access points GWN7610 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	Enable this feature to help clients connected to the GWN7610 to perform better roaming decision. • 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.
Upstream Rate	Set a limitation of upload speed on the SSID.
Downstream Rate	Set a limitation of download speed on the SSID.

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



Available Devices

00:0B:82:A4:14:BC

Member Devices

00:0B:82:8B:4E:24

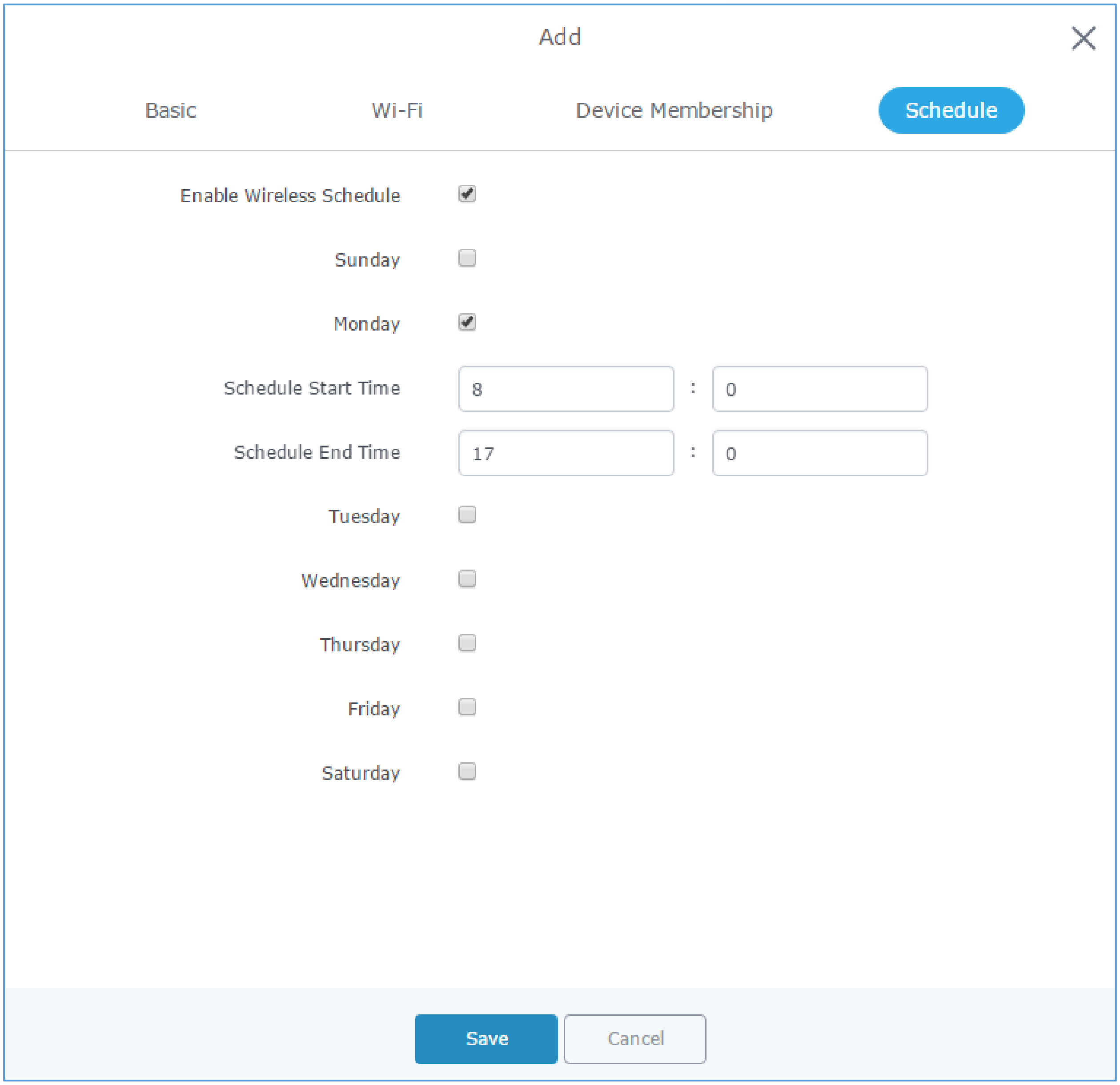
Figure 30: Device Membership

Click on → to add the GWN7610 to the network group, or click on ← to remove it.

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

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

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



Enable Wireless Schedule ☑

Sunday □

Monday ☑

Schedule Start Time 8 : 0

Schedule End Time 17 : 0

Tuesday □

Wednesday □

Thursday □

Friday □

Saturday □

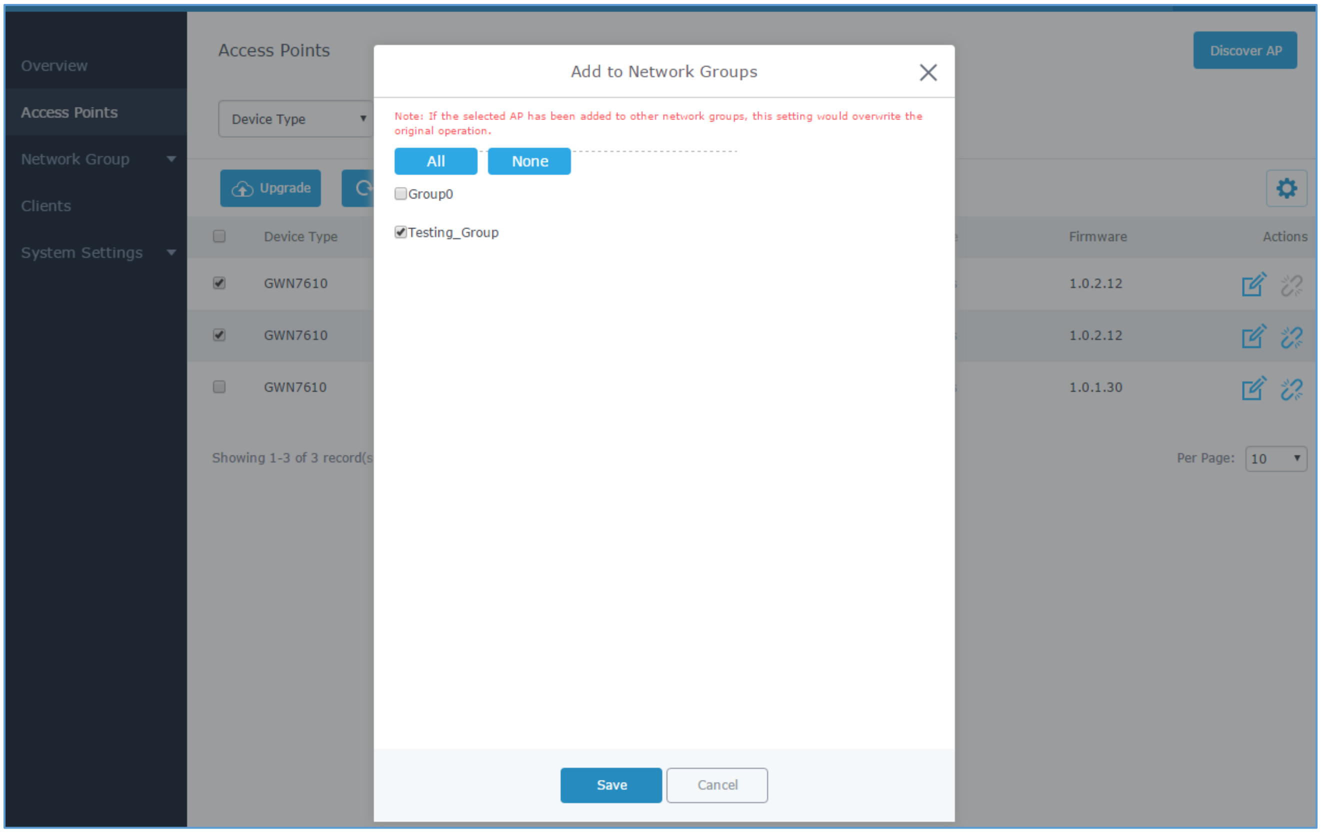
Figure 31: Wi-Fi Schedule

Note:

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

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

- Select the desired AP to add to a Network Group and click on **Add to Network Groups** .



Note: If the selected AP has been added to other network groups, this setting would overwrite the original operation.

☐Group0

☑Testing_Group

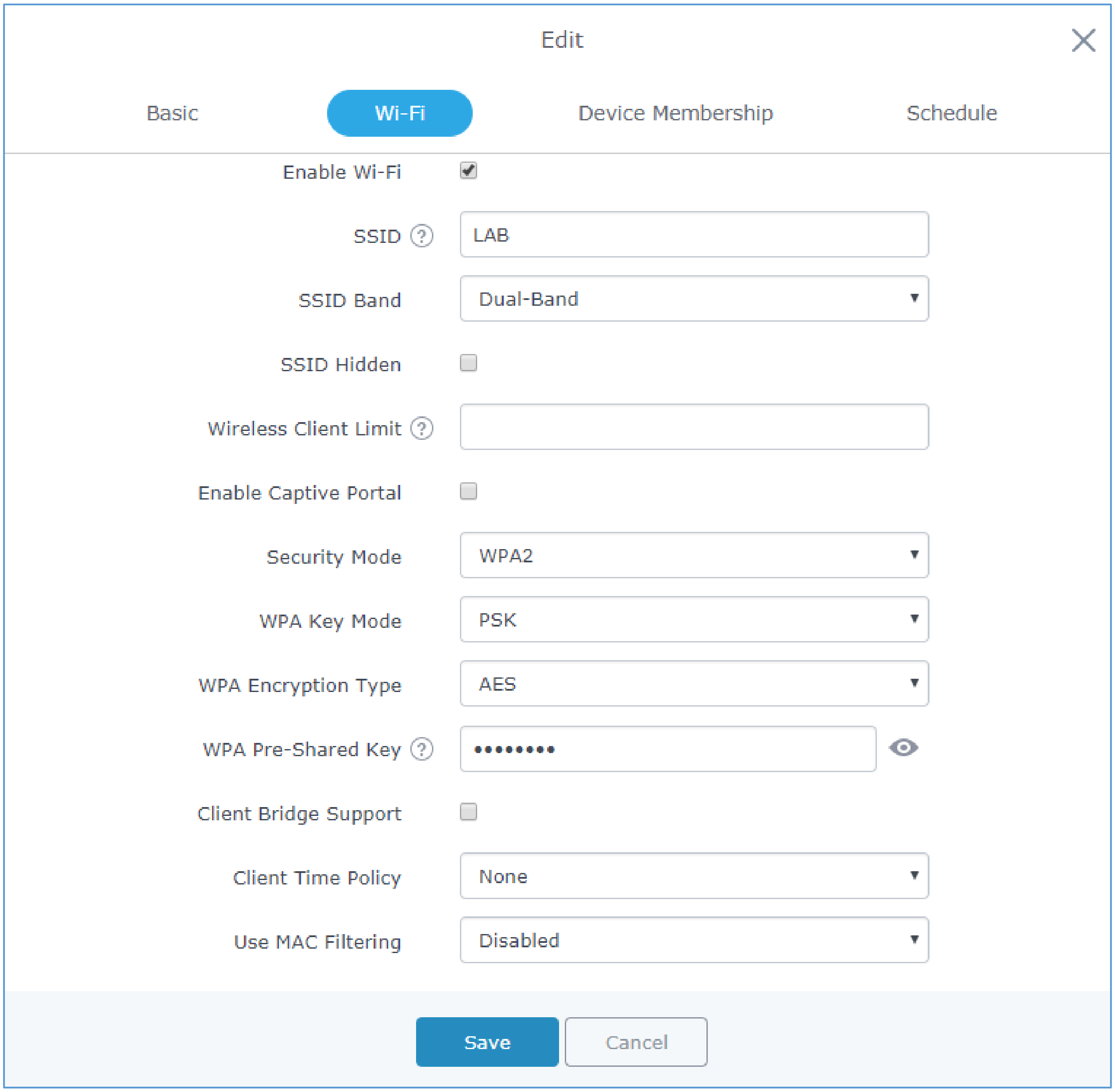
	Device Type	Firmware	Actions
☑	GWN7610	1.0.2.12	
☑	GWN7610	1.0.2.12	
☐	GWN7610	1.0.1.30	

Figure 32: Add AP to Network Group from Access Points Page

- Check to select the desired Network, on which the selected APs will be added, as shown in the above figure.

Create an SSID under a Network Group

Under Network Group Page, click to edit a network group or create a new network group and go to Wi-Fi tab.



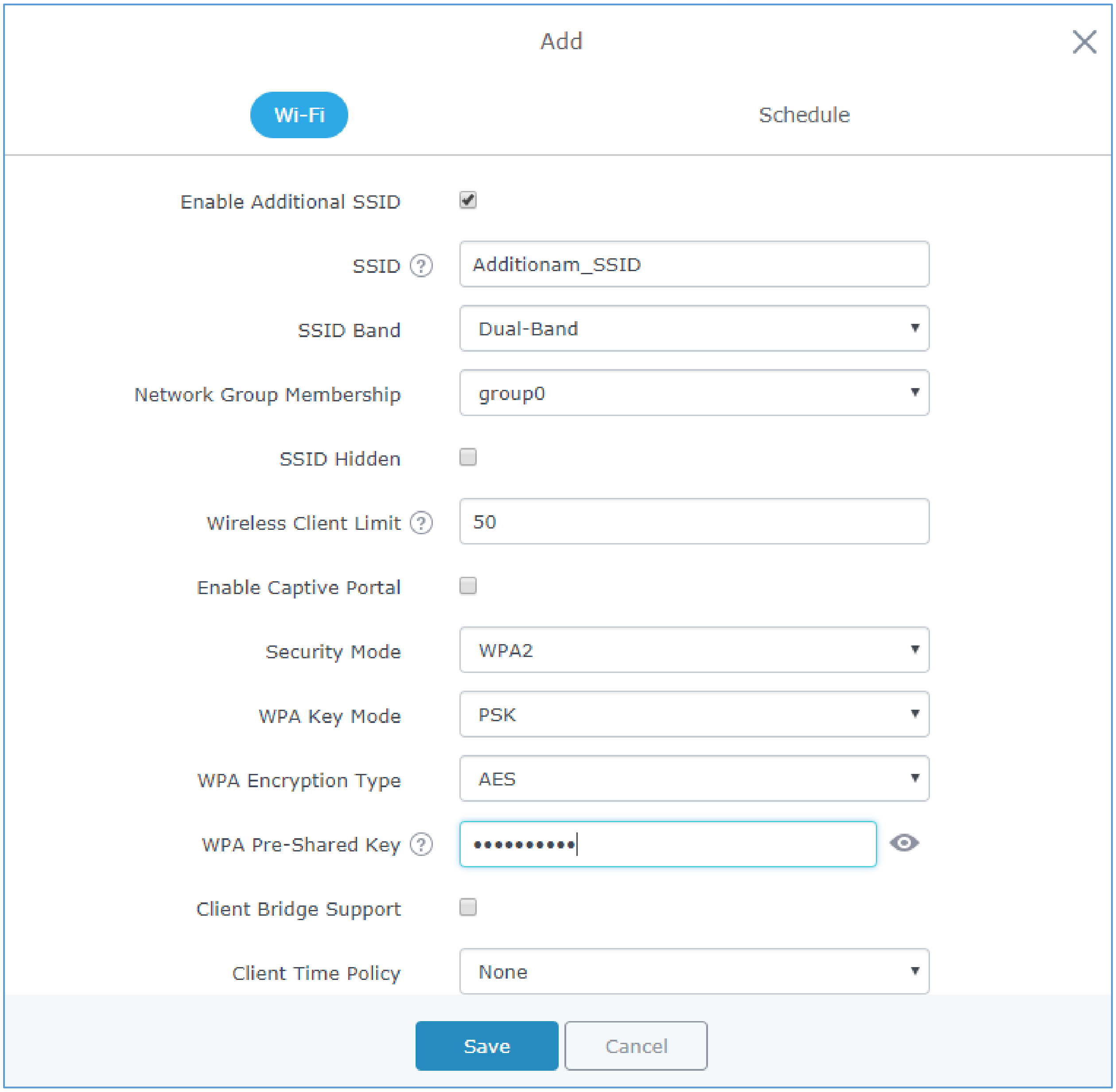
Enable Wi-Fi	☑
SSID	LAB
SSID Band	Dual-Band
SSID Hidden	□
Wireless Client Limit	
Enable Captive Portal	□
Security Mode	WPA2
WPA Key Mode	PSK
WPA Encryption Type	AES
WPA Pre-Shared Key	••••••••
Client Bridge Support	□
Client Time Policy	None
Use MAC Filtering	Disabled

Figure 33: Create an SSID

Refer to [**Table 7: Wi-Fi**] for Wi-Fi options.

Additional SSID under Same Network Group

Users can also create an additional SSID under the same group. To create an additional SSID go to **Network Group→Additional SSID.**

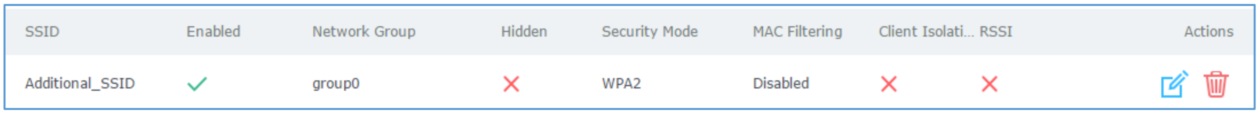


Add

Enable Additional SSID	☑
SSID	Additionam_SSID
SSID Band	Dual-Band
Network Group Membership	group0
SSID Hidden	□
Wireless Client Limit	50
Enable Captive Portal	□
Security Mode	WPA2
WPA Key Mode	PSK
WPA Encryption Type	AES
WPA Pre-Shared Key	••••••••••
Client Bridge Support	□
Client Time Policy	None

Figure 34: Additional SSID

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



SSID	Enabled	Network Group	Hidden	Security Mode	MAC Filtering	Client Isolati...	RSSI	Actions
Additional_SSID	✓	group0	✗	WPA2	Disabled	✗	✗	✎ 🗑

Figure 35: Additional SSID Created

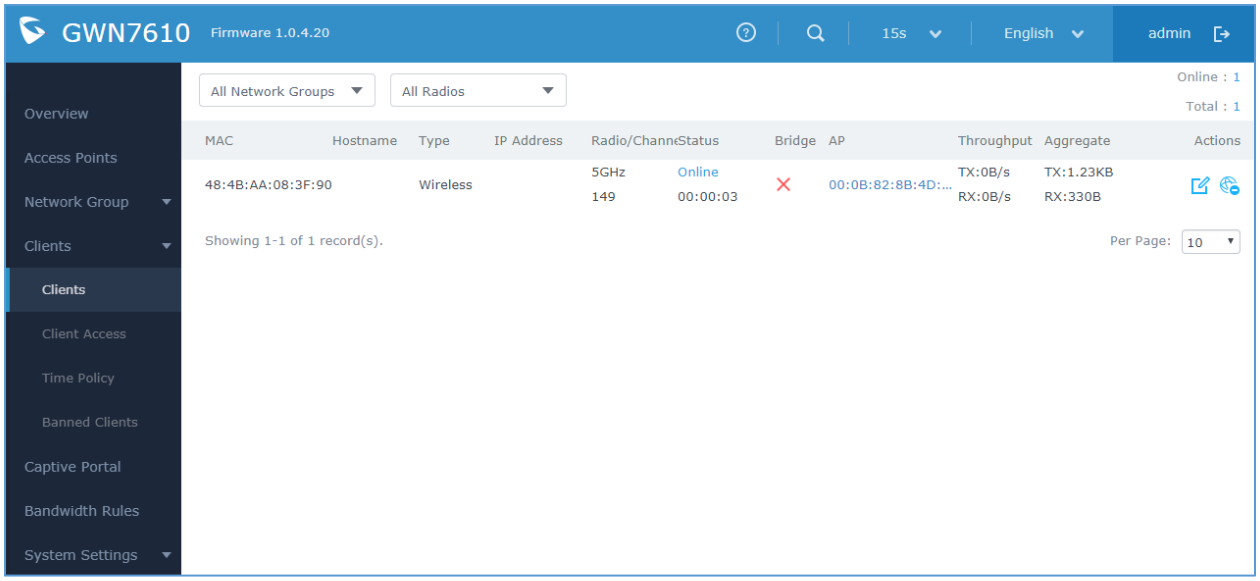
Click on 🗑 to delete the additional SSID, or ✎ to edit it.

CLIENTS CONFIGURATION

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

Clients

Users can access clients list connected to GWN7610 from **Web GUI→Clients→Clients** to perform different actions to wireless clients.



Online : 1
Total : 1

MAC	Hostname	Type	IP Address	Radio/Channe	Status	Bridge	AP	Throughput	Aggregate	Actions
48:4B:AA:08:3F:90		Wireless		5GHz 149	Online 00:00:03	✕	00:0B:82:8B:4D:...	TX:0B/s RX:0B/s	TX:1.23KB RX:330B	✎ ⊖

Showing 1-1 of 1 record(s).

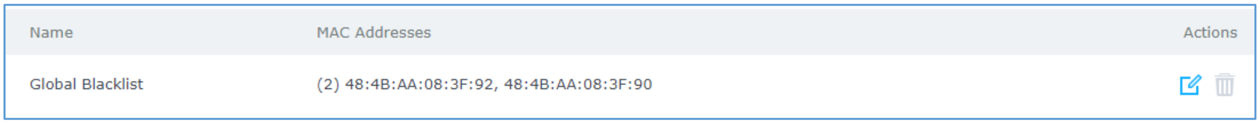
Per Page: 10

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 network group.

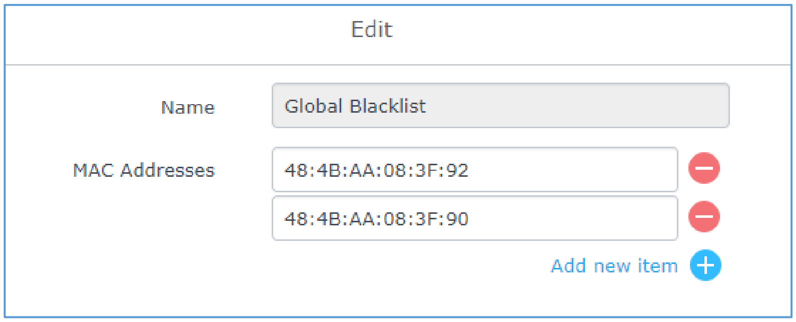
Clients Access

From this menu, users can manage in global and way the blacklist of clients that will be blocked from accessing the WiFi network, click on 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 37: Global Blacklist



Edit

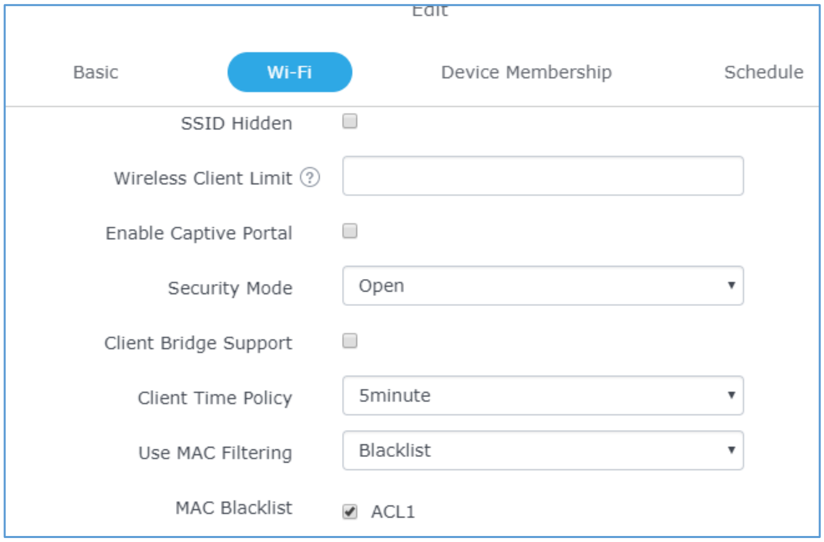
Name	Global Blacklist
MAC Addresses	48:4B:AA:08:3F:92
	48:4B:AA:08:3F:90

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 network groups and SSIDs to allow (whitelist) or disallow (blacklist) clients access to the WiFi network.

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

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



Edit

SSID Hidden	□
Wireless Client Limit	
Enable Captive Portal	□
Security Mode	Open
Client Bridge Support	□
Client Time Policy	5minute
Use MAC Filtering	Blacklist
MAC Blacklist	☑ ACL1

Figure 39: Blacklist Access List

Time Policy

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

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

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

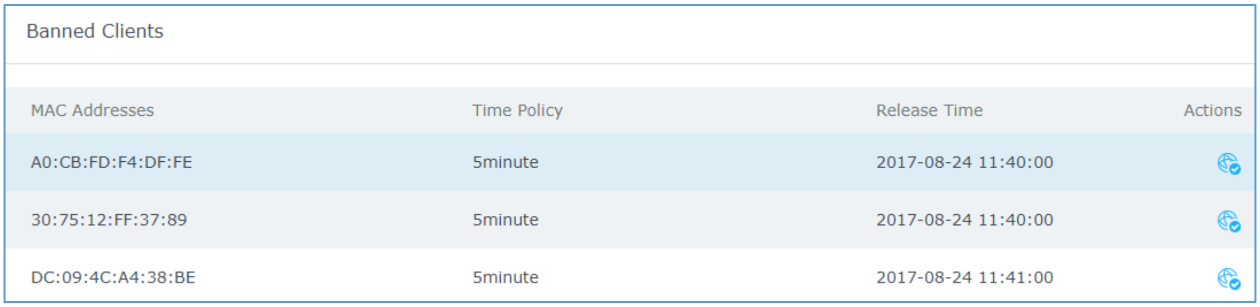
Table 8: Time Policy Parameters

Option	Description
Name	Enter the name of the policy
Enabled	Check the box to enable the policy
Limit Client Connection Time	Sets amount of time a client may be connected.
Client Reconnect Timeout Type	Select the method with which we will reset a client's connection timer so they may reconnect again. Options are: • Reset Daily. • Reset Weekly. • Reset Hourly. • Timed Reset.
Client Reconnect Timeout	If 'Timed Reset' is selected, this is the period for which the client will have to wait before reconnecting.
Reset Day	If Reset Weekly is selected, this is the day the reset will be applied.
Reset Hour	If Reset Weekly or Reset Daily is select, this is the hour and day the reset will be applied.

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

Banned Clients

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



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 40: Ban/Unban Client

LED SCHEDULE

GWN7610 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.

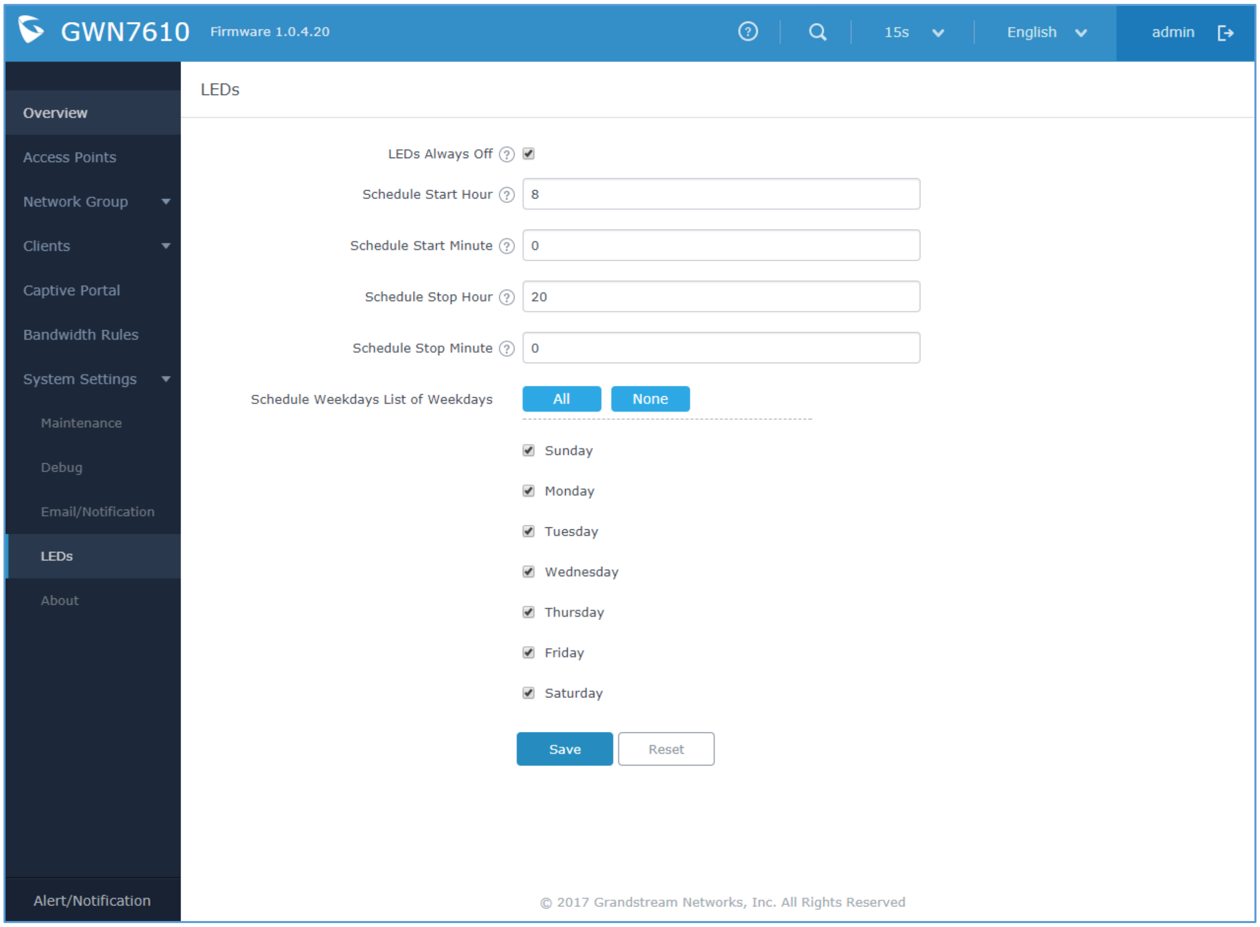
To configure LED schedule, on the GWN7610 WebGUI navigate to "System Settings → LEDs".

Following options are available:

Table 9: LED Schedule settings

Option	Description
LEDs Always off	Turn off completely the LEDs.
Schedule Start Hour	Configure the hour when LEDs will be automatically turned on.
Schedule Start Minute	Configure the minute when LEDs will be automatically turned on.
Schedule Stop Hour	Configure the hour when LEDs will be automatically turned off.
Schedule Stop Minute	Configure the minute when LEDs will be automatically turned off.
Schedule weekdays list	Choose the days for which you want to schedule the LEDs.

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



LEDs

LEDs Always Off ☑

Schedule Start Hour: 8

Schedule Start Minute: 0

Schedule Stop Hour: 20

Schedule Stop Minute: 0

Schedule Weekdays List of Weekdays

☑ Sunday

☑ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday

☑ Saturday

© 2017 Grandstream Networks, Inc. All Rights Reserved

Figure 41: LEDs Schedule

CAPTIVE PORTAL

Captive Portal feature on GWN7610 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 GWN7610 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 GWN7610 Web page under "Captive Portal".
The page contains three tabs: **Policy**, **Files** and **Clients**.

Policy Configuration Page

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

Table 10: Basic Configuration Page

Field	Description
Name	Enter a name to identify the created landing page.
Expiration	Enter the expiration time for the landing page, this field must contain an integer between 60 or 604800 in minutes. If this field is set to 0 the landing page will never expire.
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. • **WeChat:** Choosing this option will allow users to log in using WeChat app.
RADIUS Server Address	Enter the IP address or the FQDN of the RADIUS server used to authenticate clients.
RADIUS Server Port	Enter the RADIUS server port, by default value is 1812.
RADIUS Server Secret	Enter the shared key between authenticator and RADIUS server.
ShopId	Enter the ShopId for WeChat.
AppId	Enter the AppId for WeChat.
SecretKey	Enter the SecretKey for WeChat authentication.

Portal Page Customization	This option allows users to choose the customizable landing page that will be shown once a client tries to connect to the GWN, two pages are available: • **Portal Default:** This page is used when no authentication is specified, users will have only to accept license agreement to gain access to internet. • **Portal Pass:** This option provides authentication textbox when using RADIUS authentication mode, in order to enter username and identity stored in RADIUS database.

Note:
Users could create multiple captive portal instances and assign the desired one for each network Group. As an example, users can create one captive portal for Intranet usage and a second one for public Guest users, after customizing each captive portal separately, you can assign each one to the corresponding network group.

WeChat Authentication

WeChat authentication is a solution for free business WiFi connection, this is mainly designed to help enterprises create personalized captive portal for marketing purposes.

With a rich commercial value, it can greatly help businesses provide better customer experience for free WiFi usage.

You can use WeChat authentication in any scenario, but considering that users use social media

For example, once a visiting customer to the coffee shop wants to access the Internet, they can scan and select the SSID for the shop WiFi, which will pop-up the portal for authentication.

Files Configuration Page

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

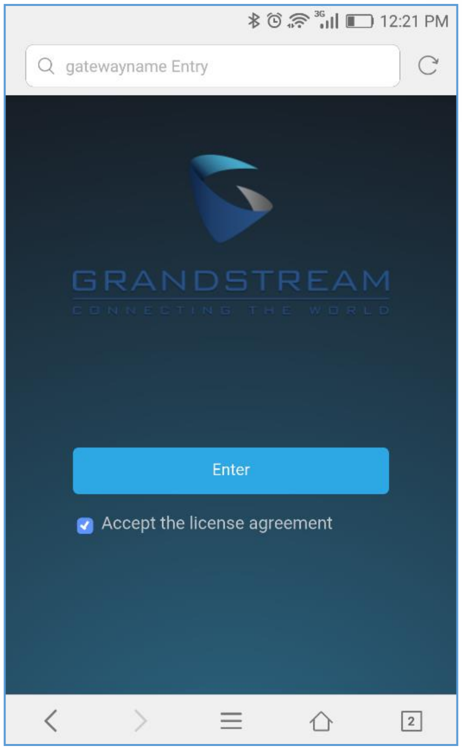


Figure 42: portal_default.html page

The following figure shows **portal_pass.html** page:

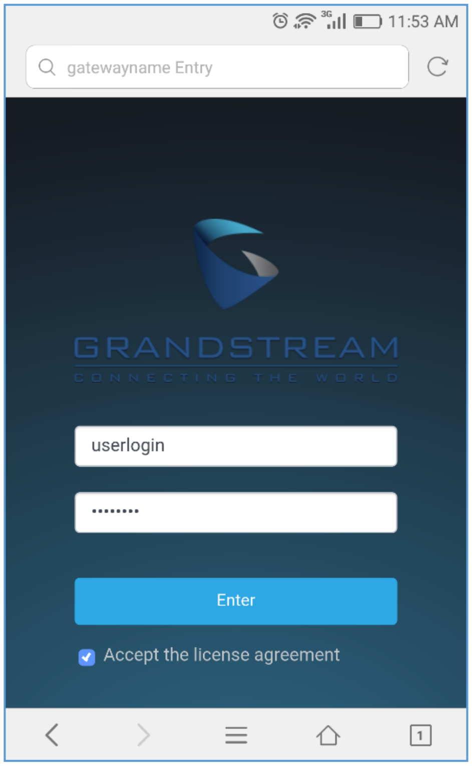
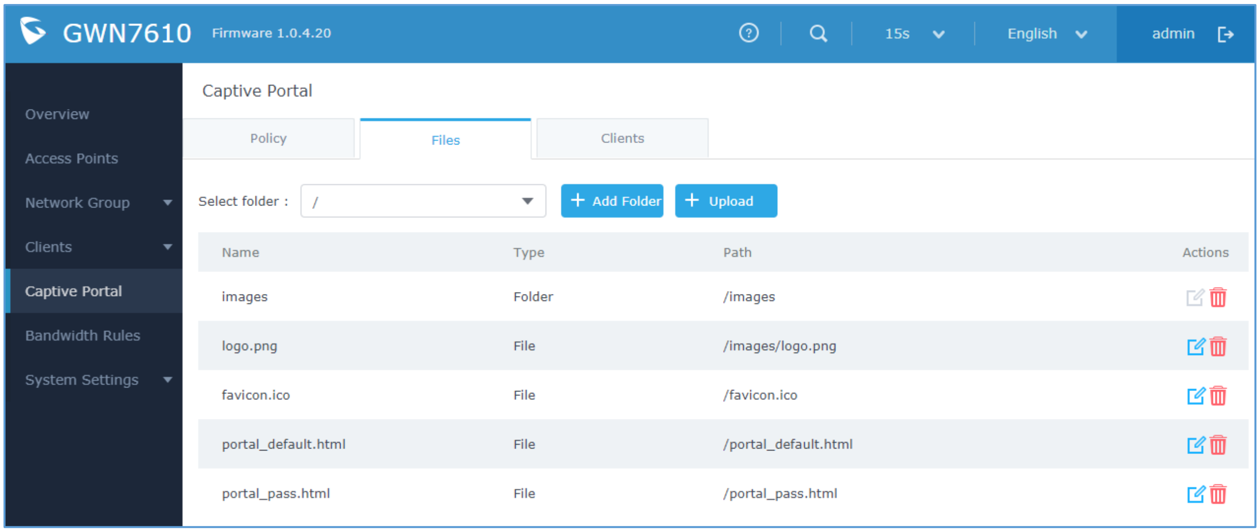


Figure 43: portal_pass.html page

The following figure shows default files used for Captive Portal:



Select folder : /

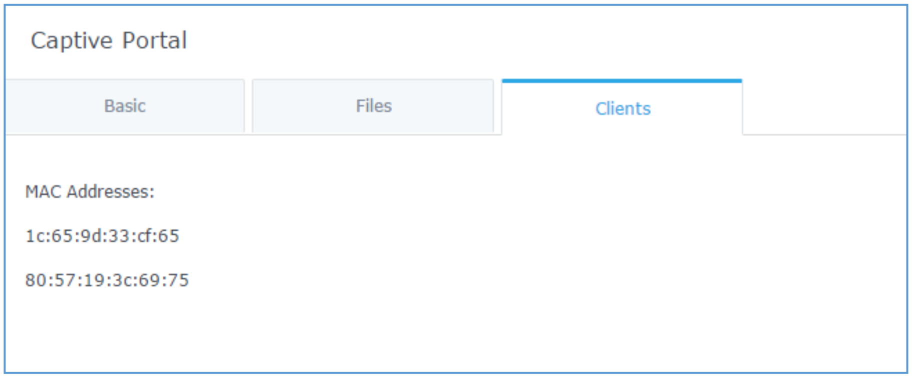
Name	Type	Path	Actions
images	Folder	/images	✎ 🗑
logo.png	File	/images/logo.png	✎ 🗑
favicon.ico	File	/favicon.ico	✎ 🗑
portal_default.html	File	/portal_default.html	✎ 🗑
portal_pass.html	File	/portal_pass.html	✎ 🗑

Figure 44: Files Settings Page

- Click ✎ to upload a new Web page.
- Click ⊕ Add Folder to add a new folder.
- Click ⊕ Upload to upload files to the selected folder.
- Folder can be selected from the dropdown list Select folder : /images ▼ .

Clients Page

Clients page lists MAC addresses of authenticated devices using captive portal.



MAC Addresses:

1c:65:9d:33:cf:65

80:57:19:3c:69:75

Figure 45: Client Web Page

BANDWIDTH RULES

The bandwidth rule is a GWN7610 feature that allows users to limit bandwidth utilization per SSID or client (MAC address or IP address).

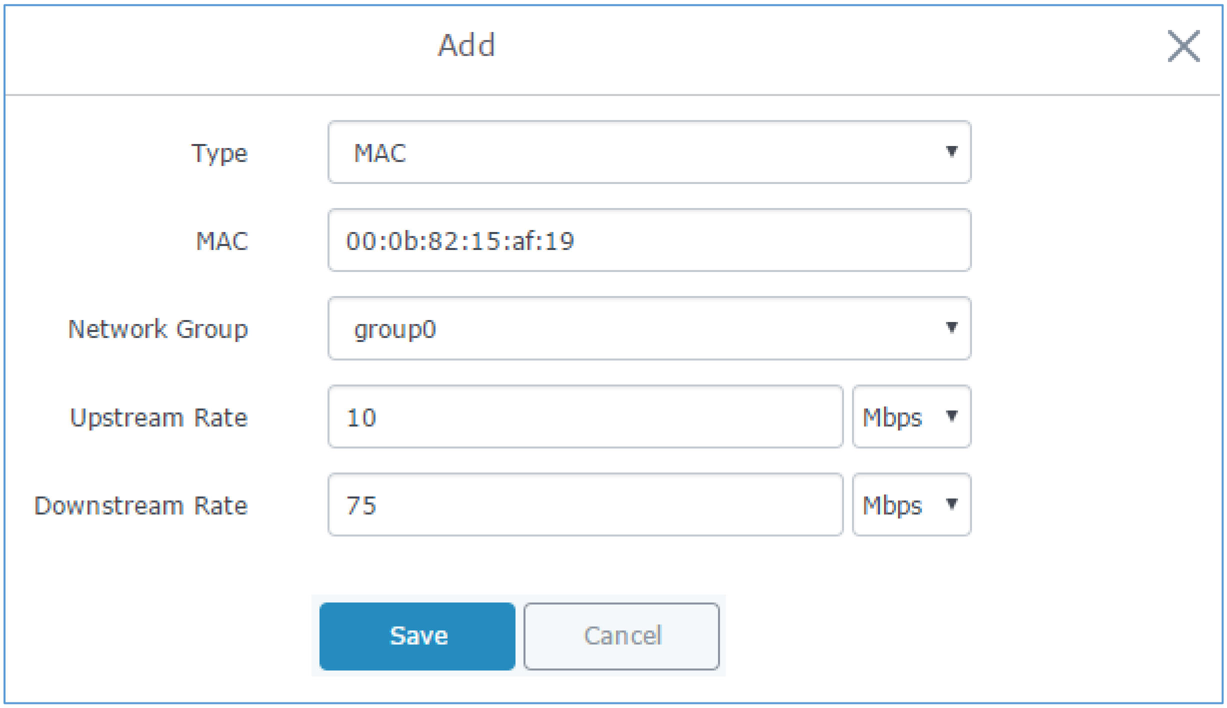
This option can be configured from the GWN7610 WebGUI under “Bandwidth Rules”.

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

Table 11: Bandwidth Rules

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

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

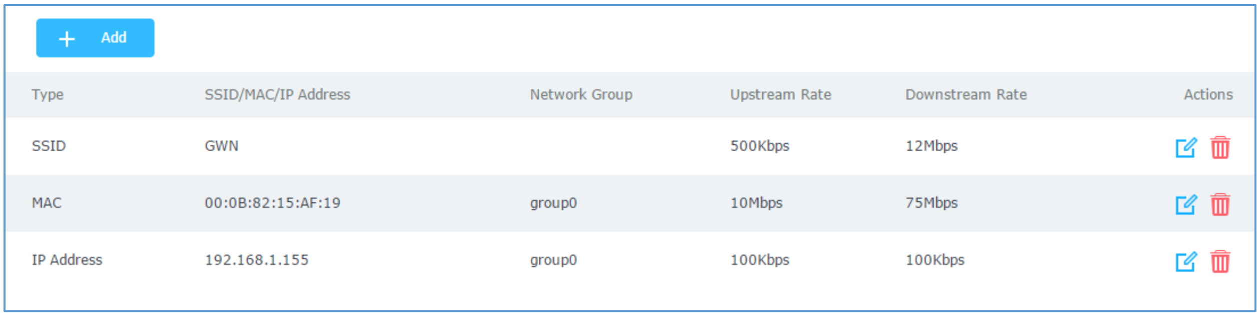


Add

Type	MAC
MAC	00:0b:82:15:af:19
Network Group	group0
Upstream Rate	10 Mbps
Downstream Rate	75 Mbps

Figure 46: MAC Address Bandwidth rule

The following figure shows examples of bandwidth rules:



Type	SSID/MAC/IP Address	Network Group	Upstream Rate	Downstream Rate	Actions
SSID	GWN		500Kbps	12Mbps	
MAC	00:0B:82:15:AF:19	group0	10Mbps	75Mbps	
IP Address	192.168.1.155	group0	100Kbps	100Kbps	

Figure 47: Bandwidth Rules

Note:

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

Per-SSID

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

Per-Client

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

SYSTEM SETTINGS

Maintenance

Refer to the following tables for Maintenance page options.

Basic

Basic page allows Country and Time configuration.

Table 12: Basic

Field	Description
Web HTTP Access	Enable the web HTTP Access. By default, it's disabled.
Web HTTPS Port	Specifies the 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 GWN7610. Please reboot the device to take effect.
NTP Server	Configure the IP address or URL of the NTP server, the device will obtain the date and time from the configured server.
Date Display Format	Change the Date Display Format, three options are possible YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY

Upgrade

The Upgrade Web page allows upgrade related configuration.

Table 13: Upgrade

Field	Description
Authenticate Config File	Authenticate configuration file before acceptance. Default is disabled.
XML Config File Password	Enter the password for encrypting the XML configuration file using OpenSSL. The password is used to decrypt the XML configuration file if it is encrypted via OpenSSL.
Upgrade Via	Specify uploading method for firmware and configuration. 3 options are available: HTTP, HTTPS and TFTP.
Firmware Server	Configure the IP address or URL for the firmware upgrade server.
Config Server	Configure the IP address or URL for the configuration file server.
Check/Download New Firmware at Boot Update on 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 43 to override upgrade and provisioning settings.
Automatic Upgrade	Specify the time to check for firmware upgrade.

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 a 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 GWN7610 to factory default settings

Access

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

Table 14: Access

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

Syslog

The syslog Web page provides configuration settings for syslog.

Table 15: Syslog

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**. Please reboot the GWN7610 to take effect.

Logserver

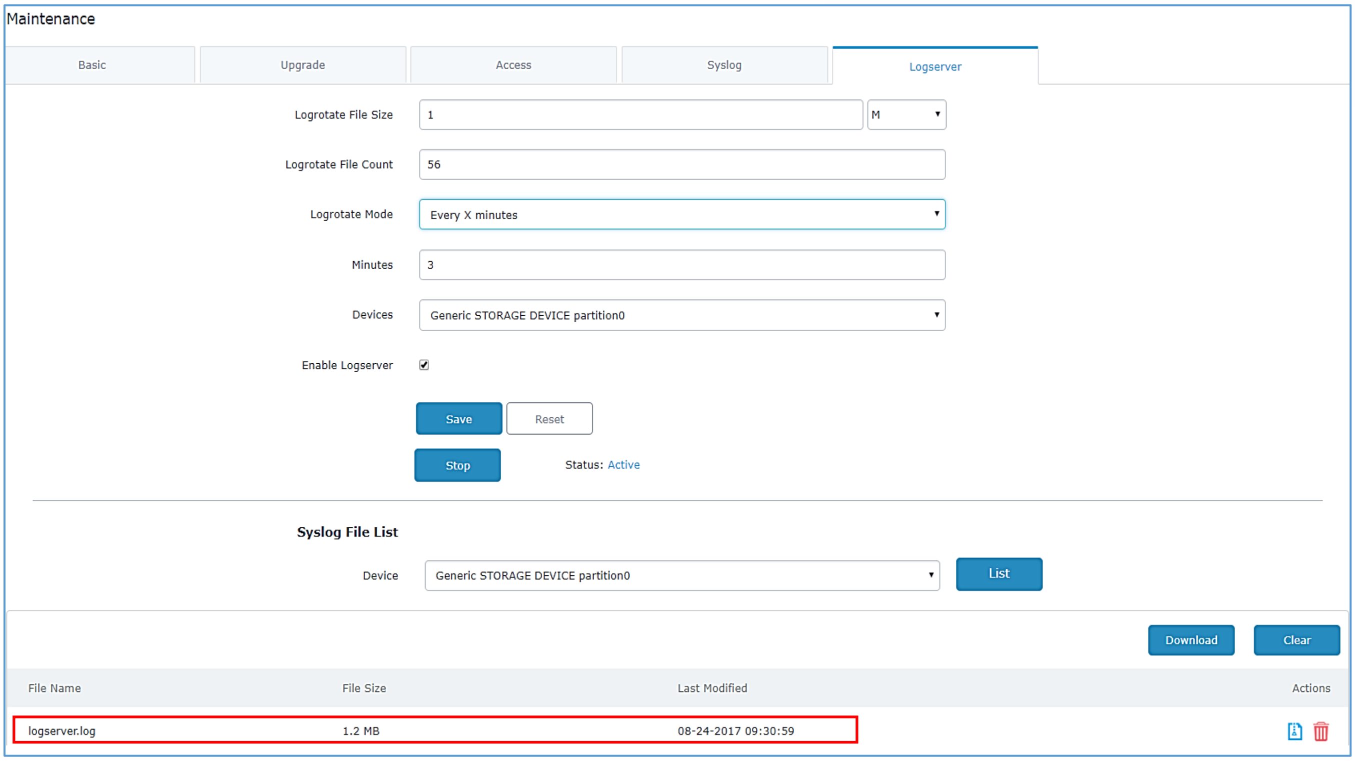
The logserver page allows the user to configure syslog server on GWN7610 in order to save log messages on connected external USB drive.

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.
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 hours (0-23) • Every X Minutes (0-59). • 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 settings up the logserver and saving the settings, users need to connect a 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.



Maintenance

Basic | Upgrade | Access | Syslog | Logserver

Logrotate File Size	1 M
Logrotate File Count	56
Logrotate Mode	Every X minutes
Minutes	3
Devices	Generic STORAGE DEVICE partition0
Enable Logserver	☑

Save Reset

Stop Status: Active

Syslog File List

Device Generic STORAGE DEVICE partition0 List

Download Clear

File Name	File Size	Last Modified	Actions
logserver.log	1.2 MB	08-24-2017 09:30:59	🗎 🗑

Figure 48: Logserver Web Page

Debug

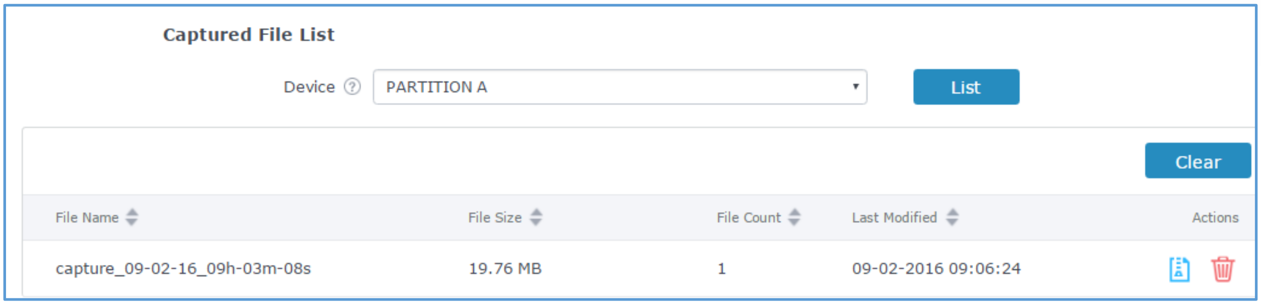
GWN7610 offers many features for managing and monitoring connected clients to network groups, as well as debugging and troubleshooting.

Capture

This section is used to generate packet trace captures from network groups interfaces which will help to sniff packets within the network group for troubleshooting purpose or monitoring...

Users will need to plug a USB device to one of the USB ports on the backside of the GWN7610.
To access Capture page, go to **Maintenance→Debug→Capture**

- 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, or click on 🗑 to delete it.



Captured File List

Device: PARTITION A

File Name	File Size	File Count	Last Modified	Actions
capture_09-02-16_09h-03m-08s	19.76 MB	1	09-02-2016 09:06:24	

Figure 49: Capture Files

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

Table 16: Debug

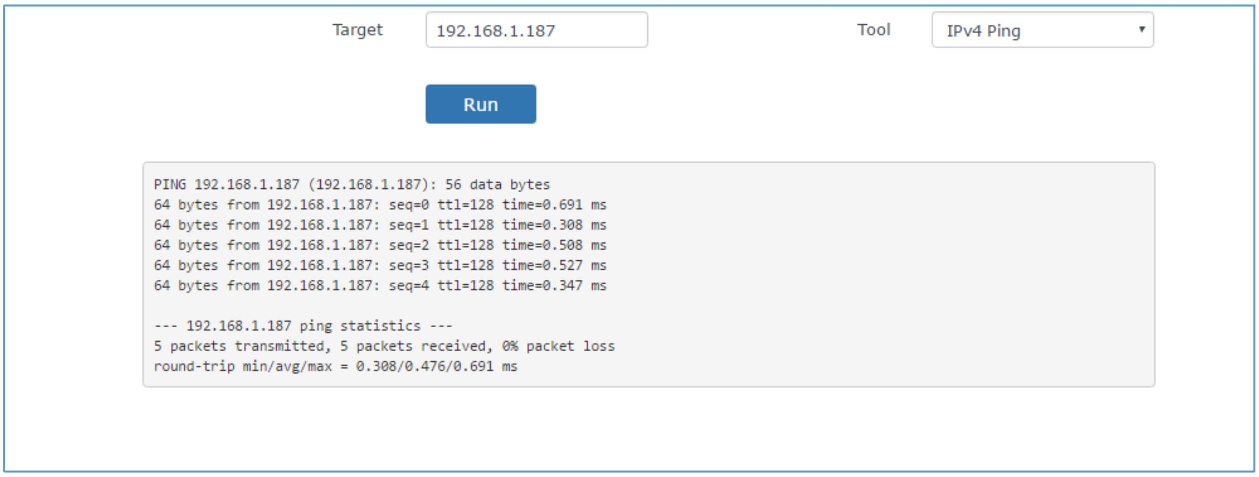
Filed	Description
File Name	Enter the name of the capture file that will be generated.
Interface	Choose a network group as Interface.
Device	Choose a device plugged to USB port to save the capture once started.
File Size	Set a File size that the capture will not exceed (Optional field)
Rotate Count	Set a value for rotating captures (Optional Field)
Direction	Choose if you want to get all traffic or only outgoing or incoming to the choses interface.
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 the Destination IP to filter capture traffic coming from the defined destination IP.
Protocol	Choose ALL or a specific protocol to capture (IP, ARP, TCP, UDP, ICMP, IPv6)

Core Files

The Core Files Web page displays core dumps generated when the GWN7610 crash, 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 GWN7610 offers both Ping and Traceroute tools for IPv4 and IPv6 protocols. To use these tools, go to GWN7610 **WebGUI→System Settings→Debug** and click on **Ping/Traceroute.**



Target 192.168.1.187

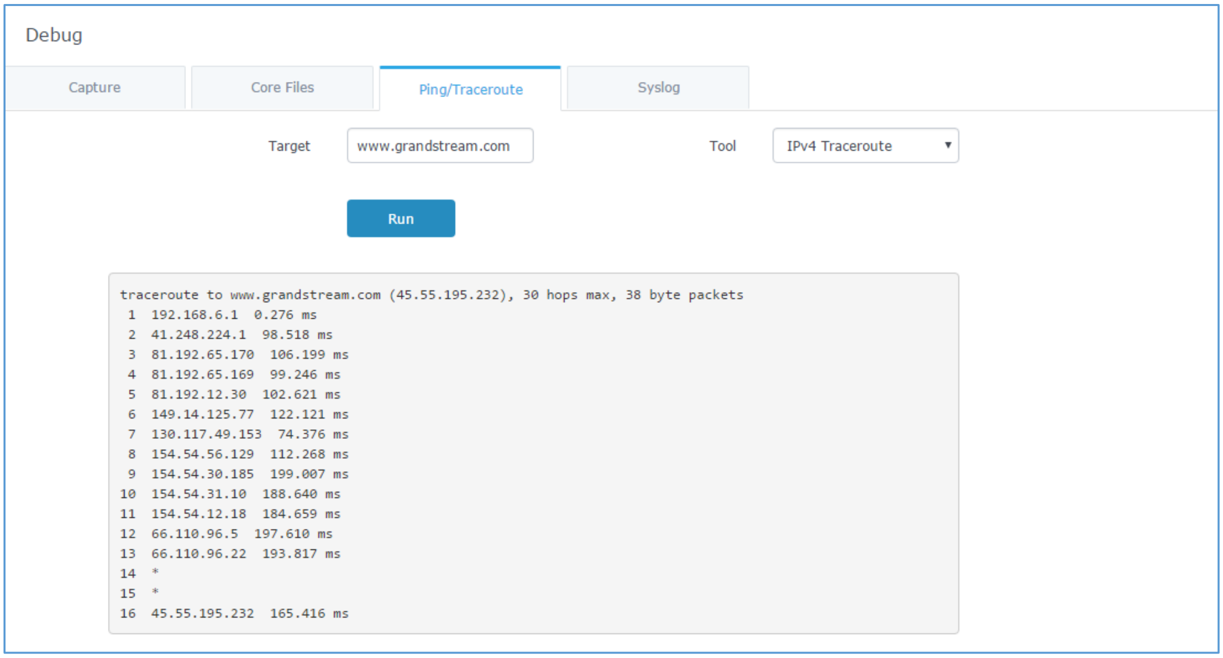
Tool IPv4 Ping

```
PING 192.168.1.187 (192.168.1.187): 56 data bytes
64 bytes from 192.168.1.187: seq=0 ttl=128 time=0.691 ms
64 bytes from 192.168.1.187: seq=1 ttl=128 time=0.308 ms
64 bytes from 192.168.1.187: seq=2 ttl=128 time=0.508 ms
64 bytes from 192.168.1.187: seq=3 ttl=128 time=0.527 ms
64 bytes from 192.168.1.187: seq=4 ttl=128 time=0.347 ms

--- 192.168.1.187 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.308/0.476/0.691 ms
```

Figure 50: 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/domain name in **Target** field.
- Click on **Run**.



Target www.grandstream.com

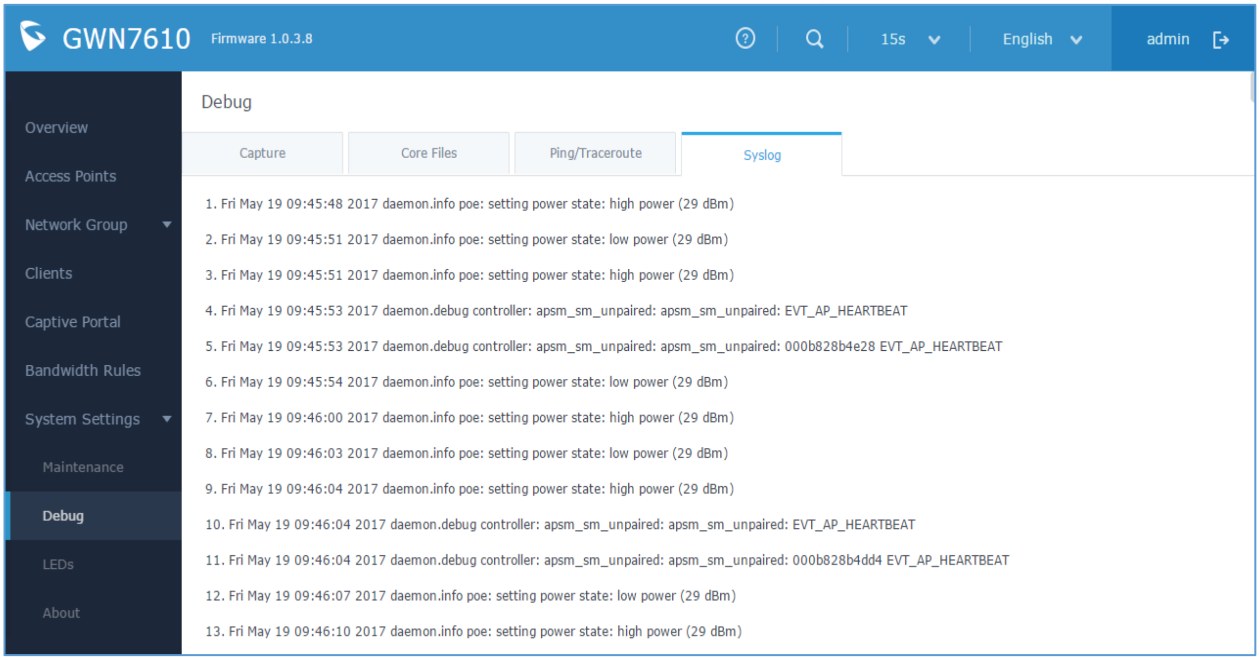
Tool IPv4 Traceroute

```
traceroute to www.grandstream.com (45.55.195.232), 30 hops max, 38 byte packets
 1  192.168.6.1  0.276 ms
 2  41.248.224.1  98.518 ms
 3  81.192.65.170  106.199 ms
 4  81.192.65.169  99.246 ms
 5  81.192.12.30  102.621 ms
 6  149.14.125.77  122.121 ms
 7  130.117.49.153  74.376 ms
 8  154.54.56.129  112.268 ms
 9  154.54.30.185  199.007 ms
10  154.54.31.10  188.640 ms
11  154.54.12.18  184.659 ms
12  66.110.96.5  197.610 ms
13  66.110.96.22  193.817 ms
14  *
15  *
16  45.55.195.232  165.416 ms
```

Figure 51: Traceroute

Syslog

The syslog Web page displays logs generated by the GWN7610 for troubleshooting purpose as shown in figure below.



```
1. Fri May 19 09:45:48 2017 daemon.info poe: setting power state: high power (29 dBm)
2. Fri May 19 09:45:51 2017 daemon.info poe: setting power state: low power (29 dBm)
3. Fri May 19 09:45:51 2017 daemon.info poe: setting power state: high power (29 dBm)
4. Fri May 19 09:45:53 2017 daemon.debug controller: apsm_sm_unpaired: apsm_sm_unpaired: EVT_AP_HEARTBEAT
5. Fri May 19 09:45:53 2017 daemon.debug controller: apsm_sm_unpaired: apsm_sm_unpaired: 000b828b4e28 EVT_AP_HEARTBEAT
6. Fri May 19 09:45:54 2017 daemon.info poe: setting power state: low power (29 dBm)
7. Fri May 19 09:46:00 2017 daemon.info poe: setting power state: high power (29 dBm)
8. Fri May 19 09:46:03 2017 daemon.info poe: setting power state: low power (29 dBm)
9. Fri May 19 09:46:04 2017 daemon.info poe: setting power state: high power (29 dBm)
10. Fri May 19 09:46:04 2017 daemon.debug controller: apsm_sm_unpaired: apsm_sm_unpaired: EVT_AP_HEARTBEAT
11. Fri May 19 09:46:04 2017 daemon.debug controller: apsm_sm_unpaired: apsm_sm_unpaired: 000b828b4dd4 EVT_AP_HEARTBEAT
12. Fri May 19 09:46:07 2017 daemon.info poe: setting power state: low power (29 dBm)
13. Fri May 19 09:46:10 2017 daemon.info poe: setting power state: high power (29 dBm)
```

Figure 52: 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.

Table 17: 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.

The following table describe the notifications configuration settings.

Table 18: Email Events

Filed	Description
Enabled	Enable/disable the notification. By default, it's disabled

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

UPGRADING AND PROVISIONING

Upgrading Firmware

The GWN7610 can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN7610.

Upgrading via WEB GUI

The GWN7610 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

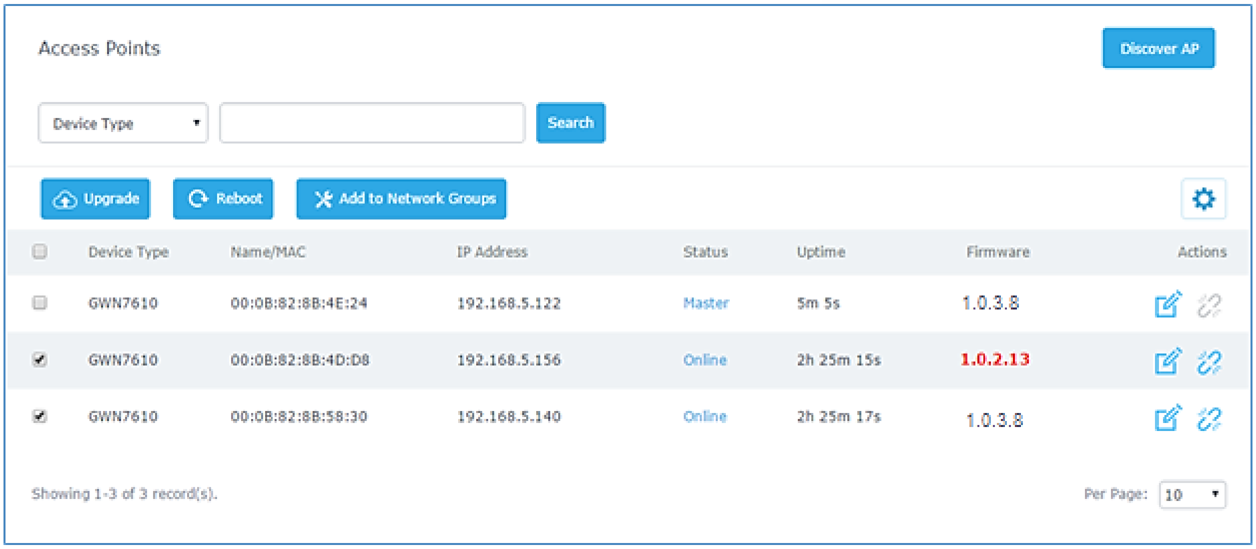
The upgrading configuration can be accessed via **Web GUI→System Settings→Maintenance →Upgrade**.

Table 19: 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 GWN7610 is being paired as slave using another GWN7610 Access Point acting as Controller, users can upgrade their paired access points from the GWN7610 Master Controller.
To upgrade a slave access point, log in to the GWN7610 acting as Master Controller and go to **Access Points.**



Access Points

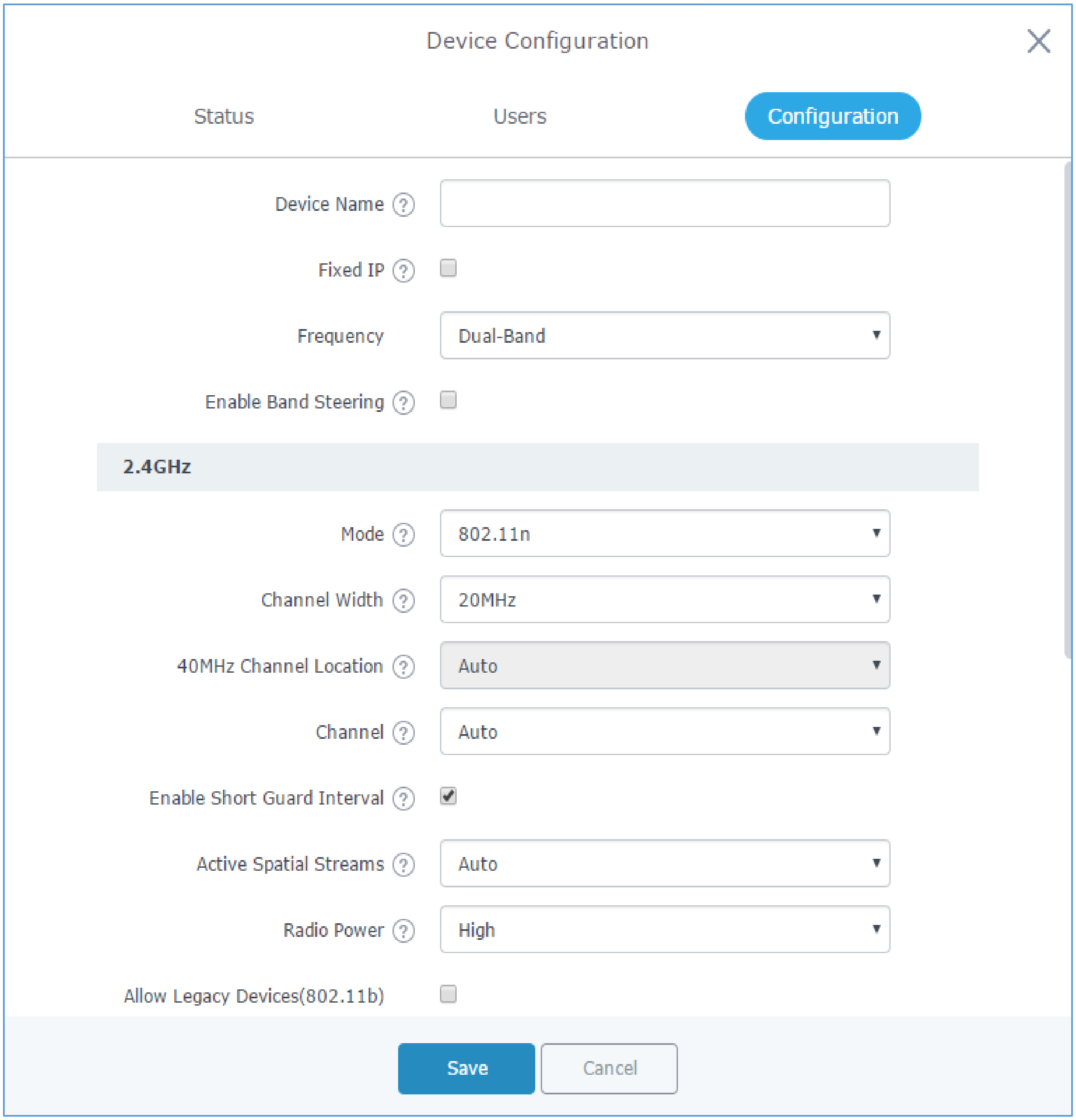
□	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
□	GWN7610	00:0B:82:8B:4E:24	192.168.5.122	Master	5m 5s	1.0.3.8	✎ 🔗
☑	GWN7610	00:0B:82:8B:4D:D8	192.168.5.156	Online	2h 25m 15s	1.0.2.13	✎ 🔗
☑	GWN7610	00:0B:82:8B:58:30	192.168.5.140	Online	2h 25m 17s	1.0.3.8	✎ 🔗

Showing 1-3 of 3 record(s).

Per Page: 10

Figure 53: Access Points

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, or click on ✎ next to the paired device to access its configuration page, and click on Upgrade to upgrade the device.



Device Name ⓘ

Fixed IP ⓘ □

Frequency: Dual-Band

Enable Band Steering ⓘ □

2.4GHz

Mode ⓘ: 802.11n

Channel Width ⓘ: 20MHz

40MHz Channel Location ⓘ: Auto

Channel ⓘ: Auto

Enable Short Guard Interval ⓘ ☑

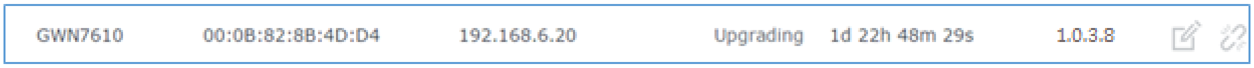
Active Spatial Streams ⓘ: Auto

Radio Power ⓘ: High

Allow Legacy Devices(802.11b) □

Figure 54: Device Configuration

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



GWN7610	00:0B:82:8B:4D:D4	192.168.6.20	Upgrading	1d 22h 48m 29s	1.0.3.8

Figure 55: GWN7610 Upgrading

⚠ **Notes:**

- Please do not interrupt or power cycle the GWN7610 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 GWN7610 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 GWN7610 Web configuration interface;
5. Configure the Firmware Server to the IP address of the PC;
6. Update the changes and reboot the GWN7610.

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 GWN7610 configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GWN7610 when necessary.

Download Configuration

Users can download the GWN7610 configuration for restore purpose under **Web GUI→System Settings→Maintenance**.

Click on [Download] to download locally the configuration file.

Upload Configuration

Users can upload configuration file to the GWN7610 under **Web GUI→System Settings→Maintenance**

Click on Upload to browse for the configuration to upload.

Please note that the GWN7610 will reboot after the configuration file is restored successfully.

Configuration Server (Pending)

Users can download and provision the GWN7610 by putting the config file on a TFTP/HTTP or HTTPS server, and set Config Server to the TFTP/HTTP or HTTPS server used for the GWN7610 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** by clicking on Reboot button.

Reset Will restore all the GWN7610 itself to factory settings.

EXPERIENCING THE GWN7610 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 GWN7610 Wireless Access Point, it will be sure to bring convenience and color to both your business and personal life.