# 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



# 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:

# 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 1.0.5.15

- Added support for New Firmware Reminder on Master Web [New Firmware Notification]
- Added support for Sequential Upgrade [Slave AP upgrade Modes]
- Added support for Feature Scheduling [Schedule]
- Added support for Master Direction [Master Direction]
- Added support for Master Transfer [Master Transfer]
- Added support for Airtime Fairness [Airtime Fairness]
- Added support for Social login/Voucher [VOUCHER][CAPTIVE PORTAL]

## Firmware Version 1.0.4.22

- Included patch for WPA2 4-way handshake vulnerability [VU#228519]

## 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.

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

---

# PRODUCT OVERVIEW

## Technical Specifications

**Table 1: GWN7610 Technical Specifications**

| | |
|---|---|
| **Wi-Fi Standards** | IEEE 802.11 a/b/g/n/ac |
| **Antennas** | 3x 2.4 GHz, gain 3 dBi, internal antenna<br>3x 5 GHz, gain 3 dBi, internal antenna |
| **Wi-Fi Data Rates** | IEEE 802.11ac: 6.5 Mbps to 1300 Mbps<br>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps<br>IEEE 802.11n: 6.5 Mbps to 450 Mbps<br>IEEE 802.11b: 1, 2, 5.5, 11 Mbps<br>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps<br>*****_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<br>5GHz radio: 5.150 - 5.250 GHz, 5.725 - 5.850 GHz (FCC, IC, RCM) |
| **Channel Bandwidth** | 2.4G: 20 and 40 MHz<br>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)<br>**coverage range can vary based on environment* |
| **Maximum TX Power** | 5G: 26dBm (FCC) / 20dBm (CE)<br>2.4G: 26dBm (FCC) / 17dBm (CE)<br>**Maximum power varies by country, frequency band and MCS rate* |
| **Receiver Sensitivity** | **2.4G**<br>802.11b:-92dBm@11Mbps; 802.11g:-76dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz:-70dBm@MCS7<br>**5G**<br>802.11a:-94dBm@6Mbps; 801.11a:-77dBm@54Mbps; 802.11ac 20MHz: -69dBm@MCS8; 802.11ac HT40:-65dBm@MCS9; 802.11ac 80MHz: |

| | |
|---|---|
| | 1dBm@MCS9<br>** 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<br>Power over Ethernet 802.3af/802.3at compliant<br>Maximum Power Consumption: 13.8W |
| **Environmental** | Operation: 0°C to 50°C<br>Storage: -10°C to 60°C<br>Humidity: 10% to 90% Non-condensing |
| **Physical** | **Unit Dimension:** 205.3 x 205.3 x 45.9mm; Unit Weight: 540g<br>**Unit + Mounting Kits Dimension:** 205.3 x 205.3 x 50.9mm; **Unit + Mounting Kits Weight:** 600g<br>**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.

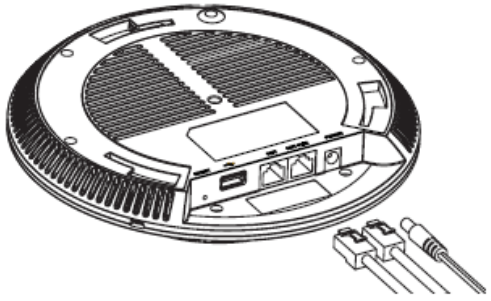


**Figure 2: Connecting GWN7610**

## 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

**Step1:**

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

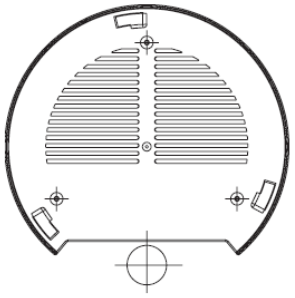


**Figure 3: Wall Mount – Steps 1 & 2**

**Step 2:**

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

**Step 3:**

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

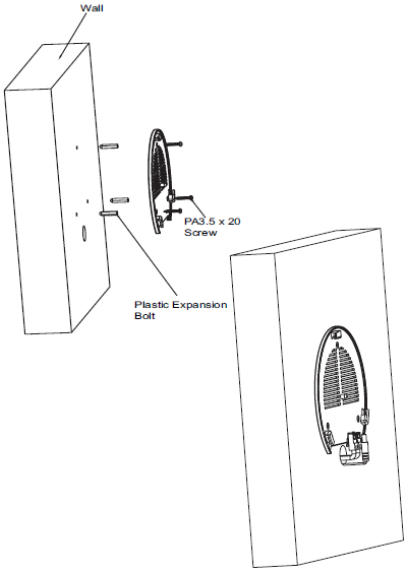



**Figure 4: Wall Mount – Steps 3 & 4**

**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.

**Step 6:**

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

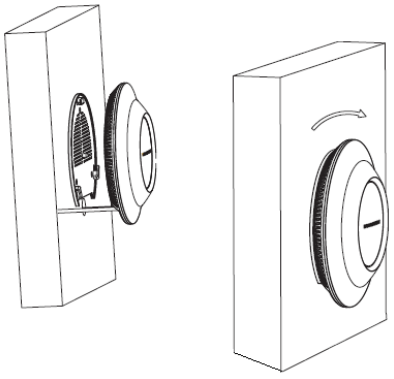


**Figure 5: Wall Mount – Steps 5 & 6**

## Ceiling Mount

**Step 1:**

Remove the ceiling tile.

**Step 2:**

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

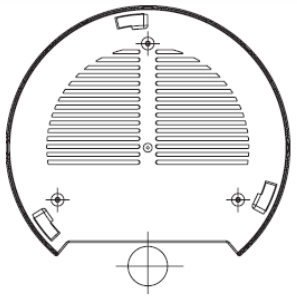


**Figure 6: Ceiling Mount – Steps 1 & 2**

**Step 3:**

Insert the screws through the mounting bracket.

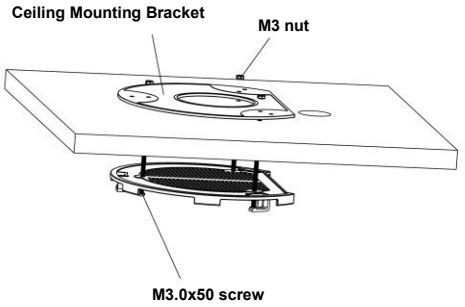



**Figure 7: Ceiling Mount – Step 3**

**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.

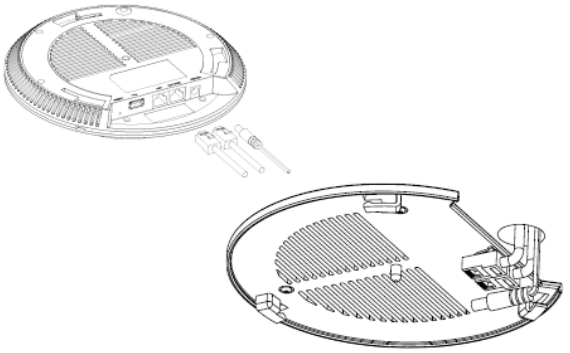


**Figure 8: Ceiling Mount – Step 4**

⚠ **Note:**

Ceiling mounting is recommended for optimal coverage performance.

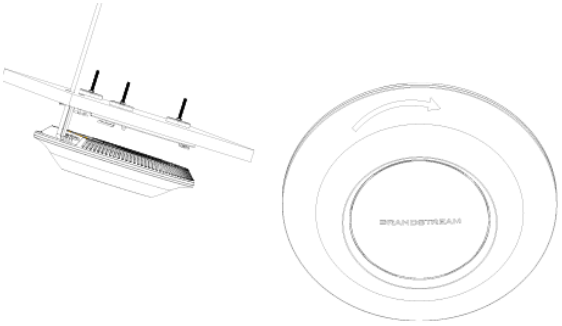


**Figure 9: Ceiling Mount – Steps 5 & 6**

# 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. |
| **Blinking White** | Used for Access Point location feature. |

## 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.

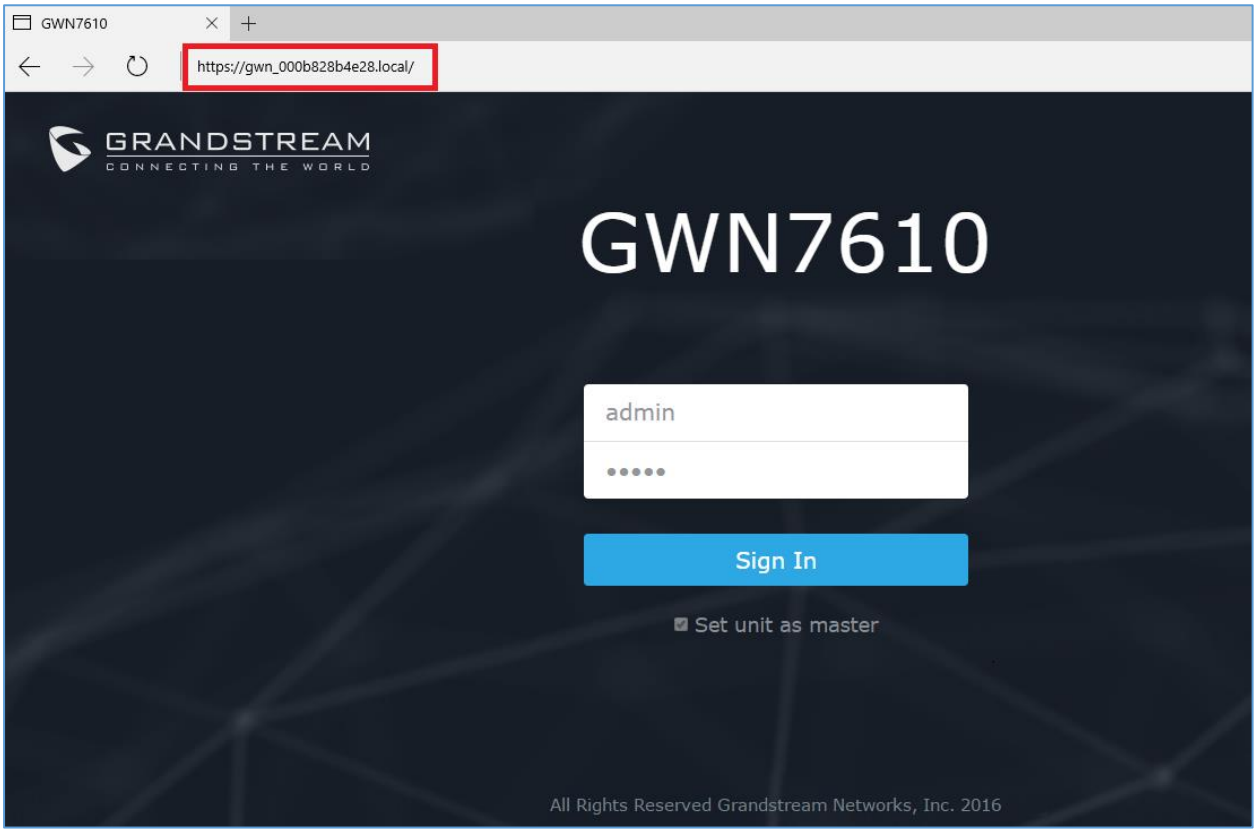



**Figure 10: Discover the GWN7610 using its MAC Address**

### 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.

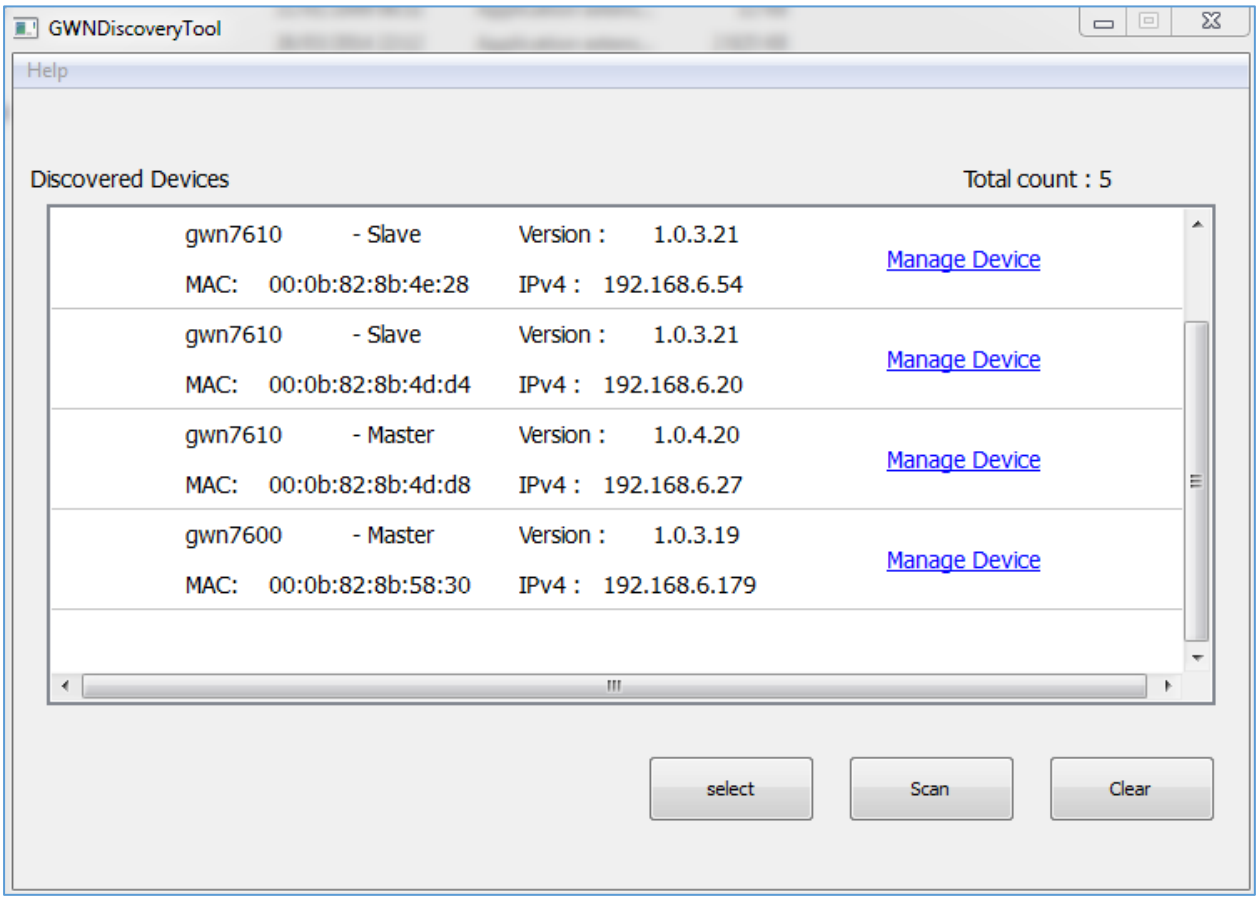



**Figure 11: GWN Discovery Tool**

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.

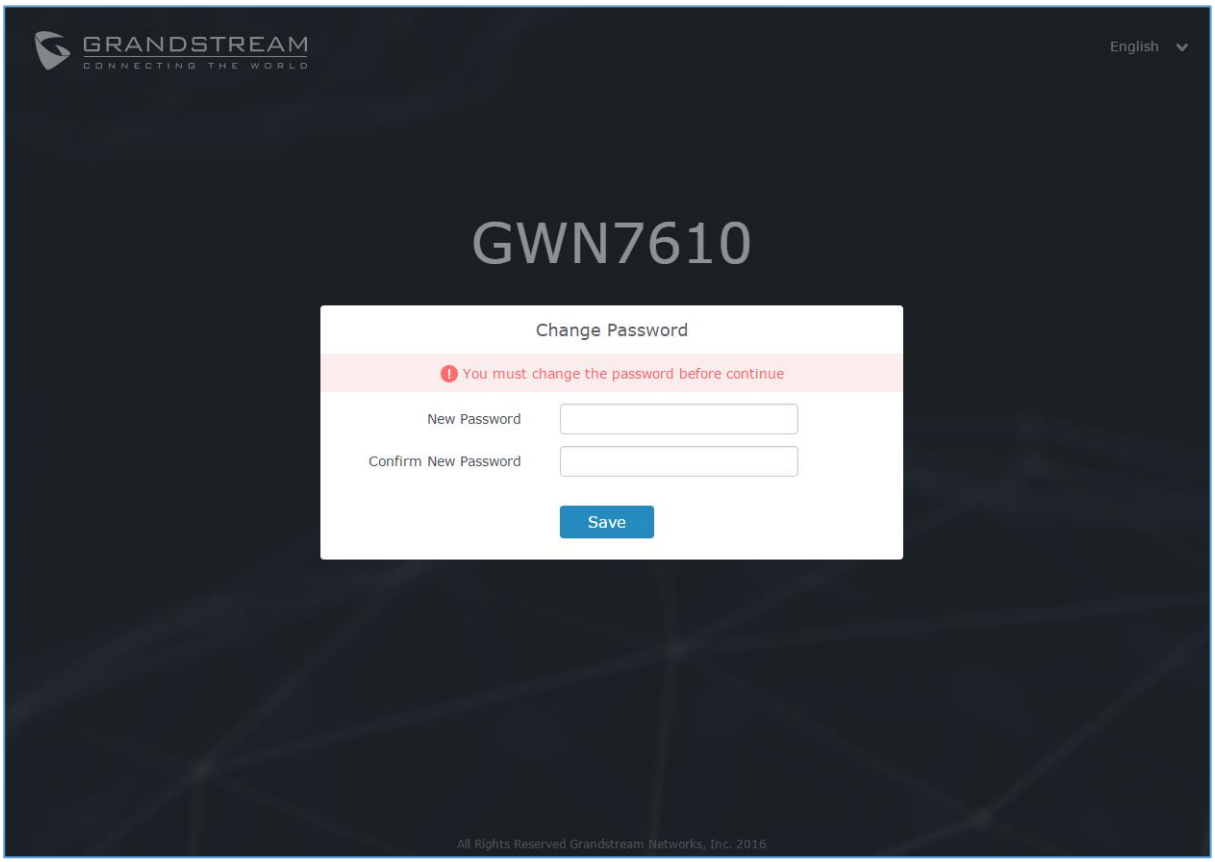



**Figure 13: Change Password on first boot**

## 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**

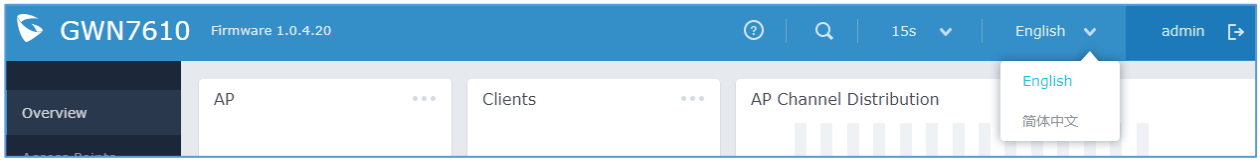



**Figure 15: GWN7610 Web GUI Language**

## 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.

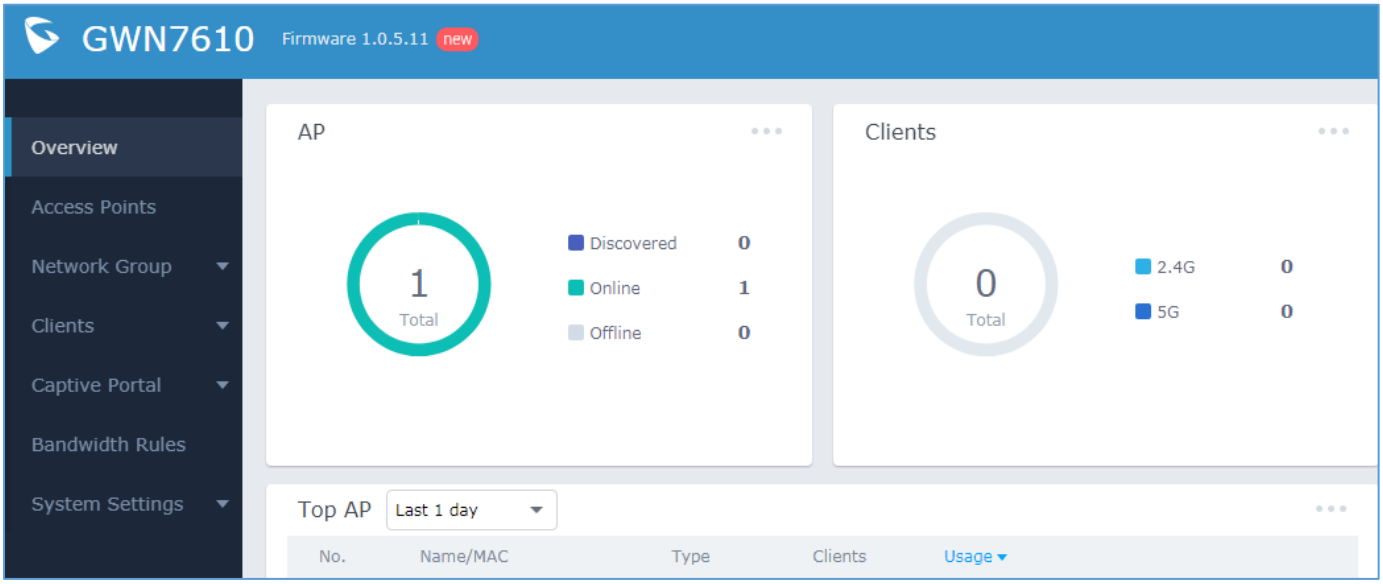



**Figure 16: Overview Page**

Along with the firmware version of the unit, users can quickly see the status of the GWN7610 for different items, please refer to the following table for each item:

**New Firmware Notification**: Starting from firmware version 1.0.5.14, and once a different OFFICIAL firmware is released on Grandstream Networks website, the master AP will popup reminder notification to the administrator in order to upgrade the device. You can click on ***New*** button in order to be redirected to the release note of the new firmware version, for upgrading steps please refer to section [***Upgrading Firmware***].

**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.

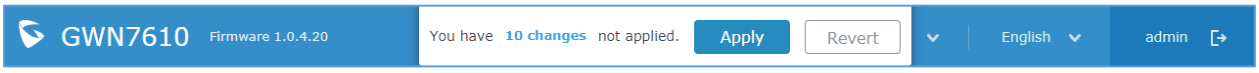



**Figure 17: Apply Changes**

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.

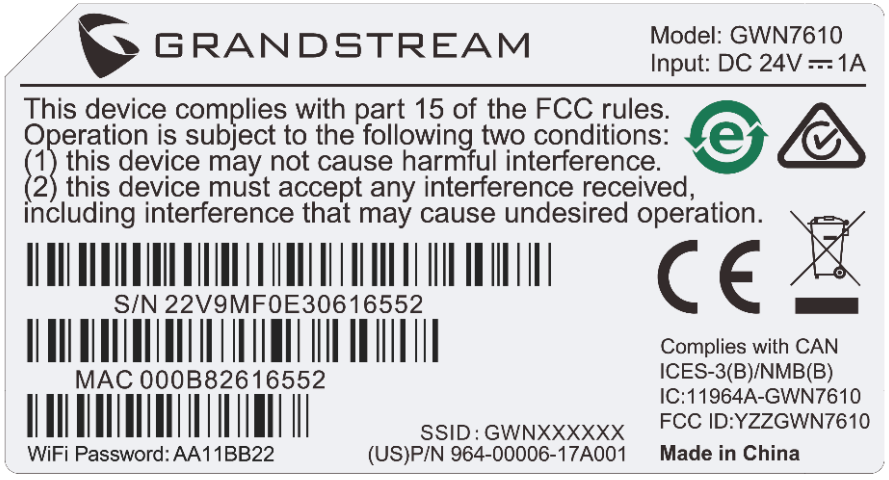



**Figure 18: MAC Tag Label**

# 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.

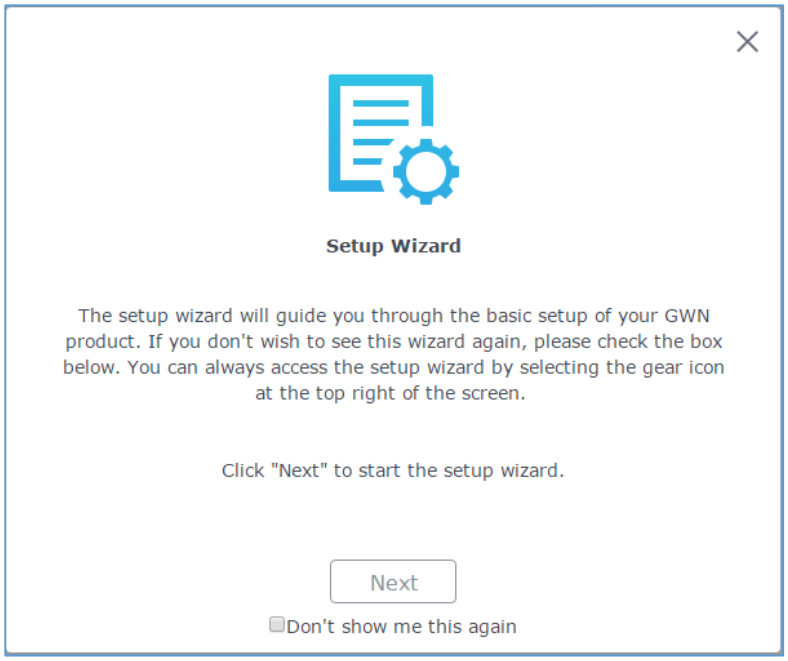



**Figure 20: Setup Wizard**

## Discover and Pair Other GWN7610 Access Point

First, note that by default the GWN controller access point will automatically discover all APs connected to the same LAN (broadcast domain), but starting from firmware 1.0.5.14 a new possibility has been added in order to pair and provision remote APs using DHCP option 43 with master direction explained below.

**Master Direction**

In order to pair and manage access points located on remote networks, the admin needs to configure the IP address of master AP on DHCP option 43 which will be send to the slave access point during booting stage and allow the save/master connection to be established remotely. GWN7610 accepts option 224 encapsulated in option 43, and the syntax is in TLV format. A simple example of DHCP 43 configuration would be: *224(Type)12(Length)10.157.0.234(Value) translated into Hex as e00c31302e3135372e302e323334*

Scenario example: a company has two offices connected via VPN (master AP located on network 192.168.1.0/24 and slave AP located on remote network 192.168.2.0/2). On remote network the admin can set DHCP option 43 using GWN7000 router as following value: **encap:43,224,"192.168.1.100".**

After that the slave AP will be listed on the master AP discovered devices and ready for paring and provisioning process which is described on the next steps.

To Pair a GWN7610 slave access discovered by the GWN7610 master A, follow the steps below:

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

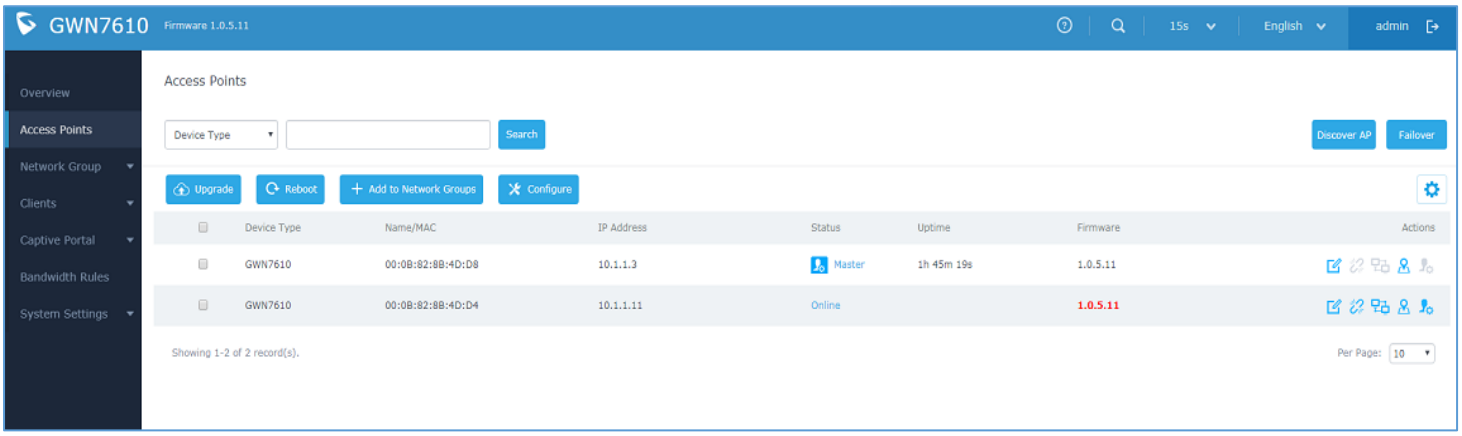



**Figure 21:Discover AP**

2. Click on Discover AP to list discovered access points, the following page will appear.

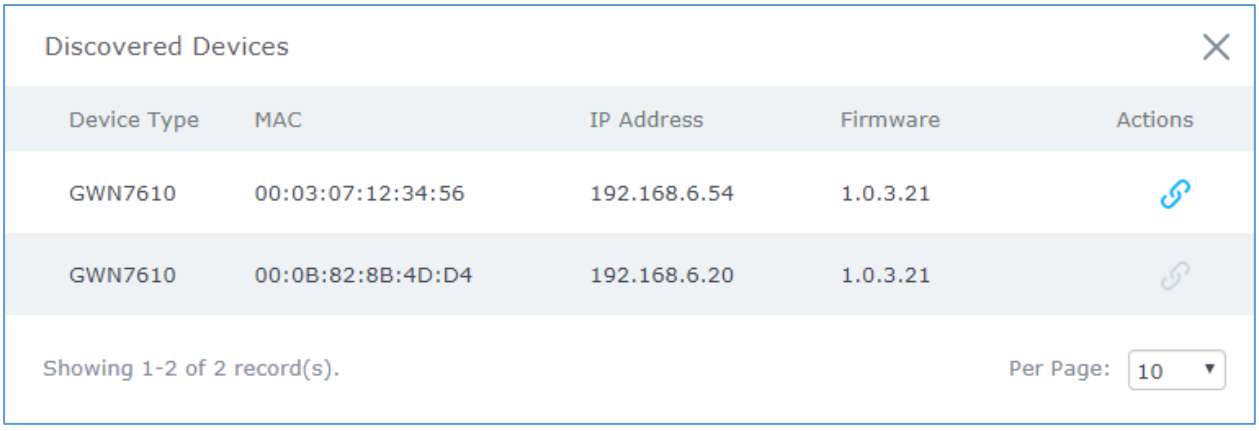



**Figure 22: Discovered Devices**

**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.


**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.<br>• **Fixed IP:** Used to set a static IP for the GWN7610, if checked users will need to set the following:<br>*-IPv4 Address:* Enter the IPv4 address to be set as static for the device<br>*-IPv4 Subnet Mask:* Enter the Subnet Mask.<br>*-IPv4 Gateway:* Enter the Network Gateway's IPv4 Address.<br>*-Preferred IPv4 DNS:* Enter the Primary IPv4 DNS.<br>*-Alternate IPv4 DNS*: Enter the Alternate IPv4 DNS.<br>• **Frequency:** Set the GWN7610's frequency, it can be either 2.4GHz, 5GHz or Dual-band.<br>• **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.<br>• **Airtime Fairness:** Enable/disable airtime fairness on the access point. This is useful on networks with legacy old WiFi client stations in order to avoid them slowing down the network.<br>• **Mode(2.4G):** Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.<br>• **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.

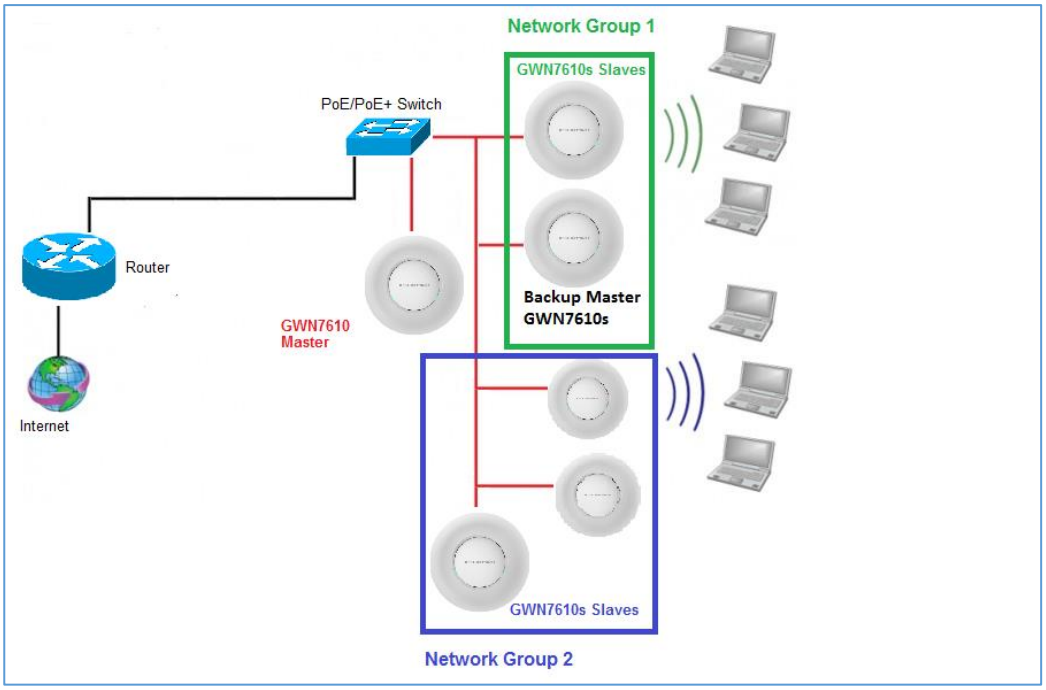



**Figure 24: Failover Master**

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**

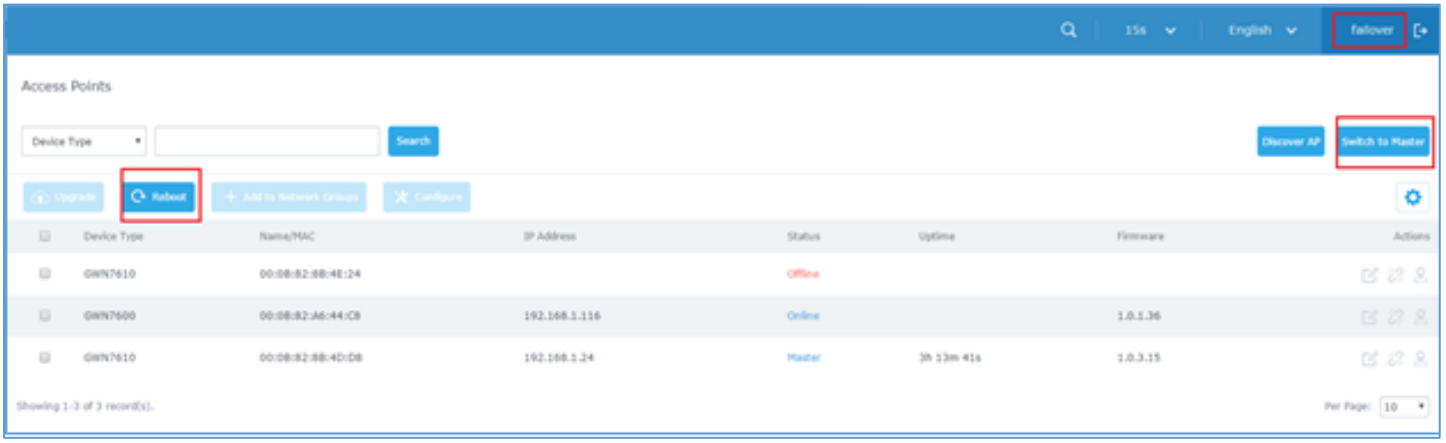



**Figure 25: Failover Mode GUI**

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.

## Master Transfer

Users could easily transfer the master control functionality to one of the slaves by pressing the button  next to the designated slaved access point.
This can be useful for example when the admin wants to do some maintenance or change the original master unit, thus keeping all the configuration and sending all control to a new unit before removing the old one.

During the transfer process the master will send all configuration files to the designated slave while taking into consideration validation between the two devices for more security, once the slave completes copying the files it will send notification to the original master which will become a slave if it is an access point or reset itself if it's a GWN7000 router.

**Note:** the master transfer feature relies on some master failover functions and it is recommended to have all access points on firmware version 1.0.5.14 or higher in order to have the process or transfer working properly.

## 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.

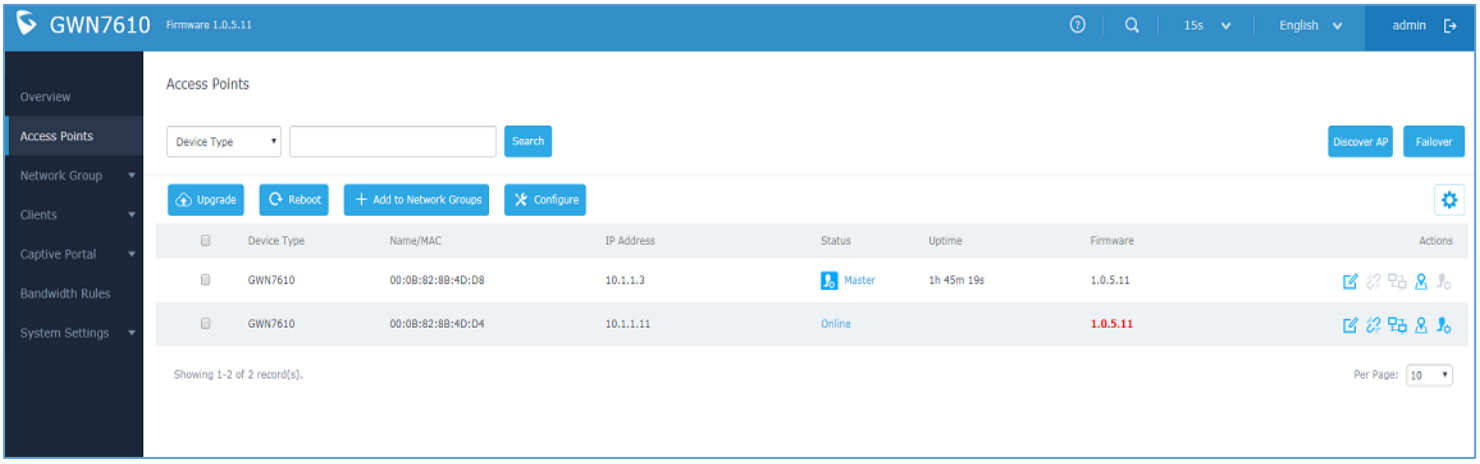



**Figure 26: Controller Protocol Security Enhancement**

## 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.


**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.**

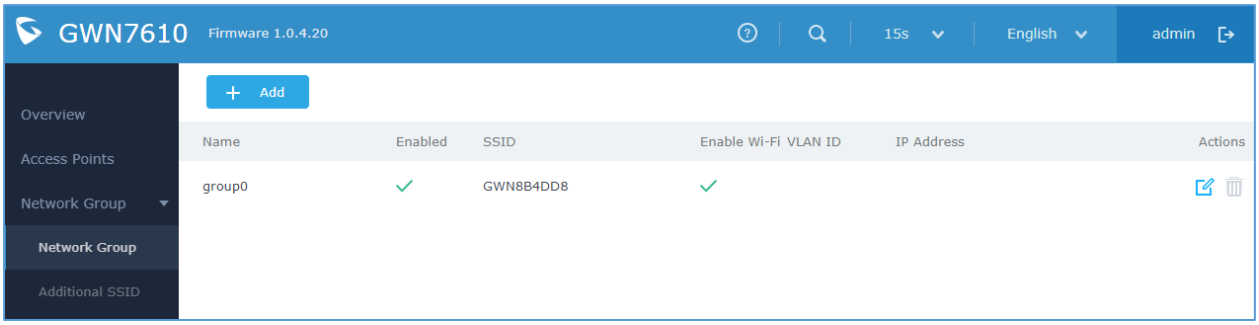



**Figure 28: Network Group**

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



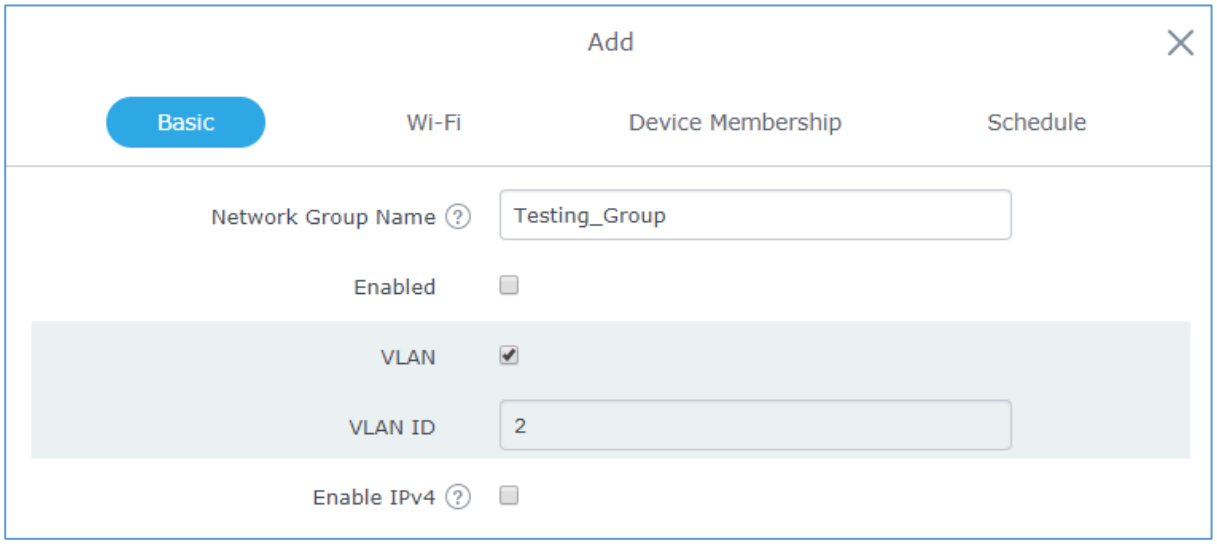



**Figure 29: Add a New Network Group**

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:<br>• **Dual-Band**<br>• **2.4GHz**<br>• **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.<br>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:<br>• **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.<br>• **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.<br>• **WPA/WPA2:** Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type.<br>• **WPA2:** Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. Recommended configuration for authentication.<br>• **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:<br>• **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.<br>• **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.<br>• **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).<br>Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":".<br>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.<br>• 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.<br>• 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.<br>• 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.<br>**Note:** 11R is required for enterprise audio feature, 11V and 11K are optional. |
| **Enable 11R** | Check to enable 802.11r |
| **Enable 11K** | Check to enable 802.11k |

| | |
|---|---|
| **Enable 11V** | Check to enable 802.11v |
| **Upstream Rate** | Set 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.

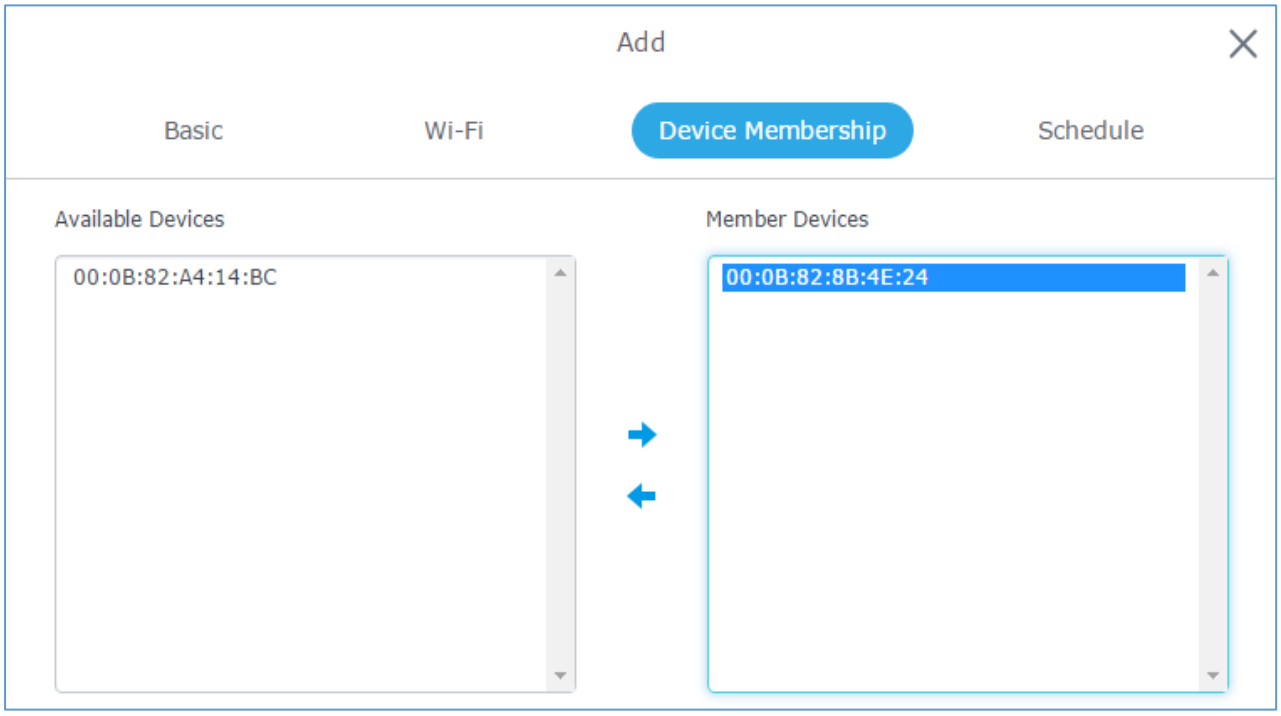



**Figure 30: Device Membership**

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.

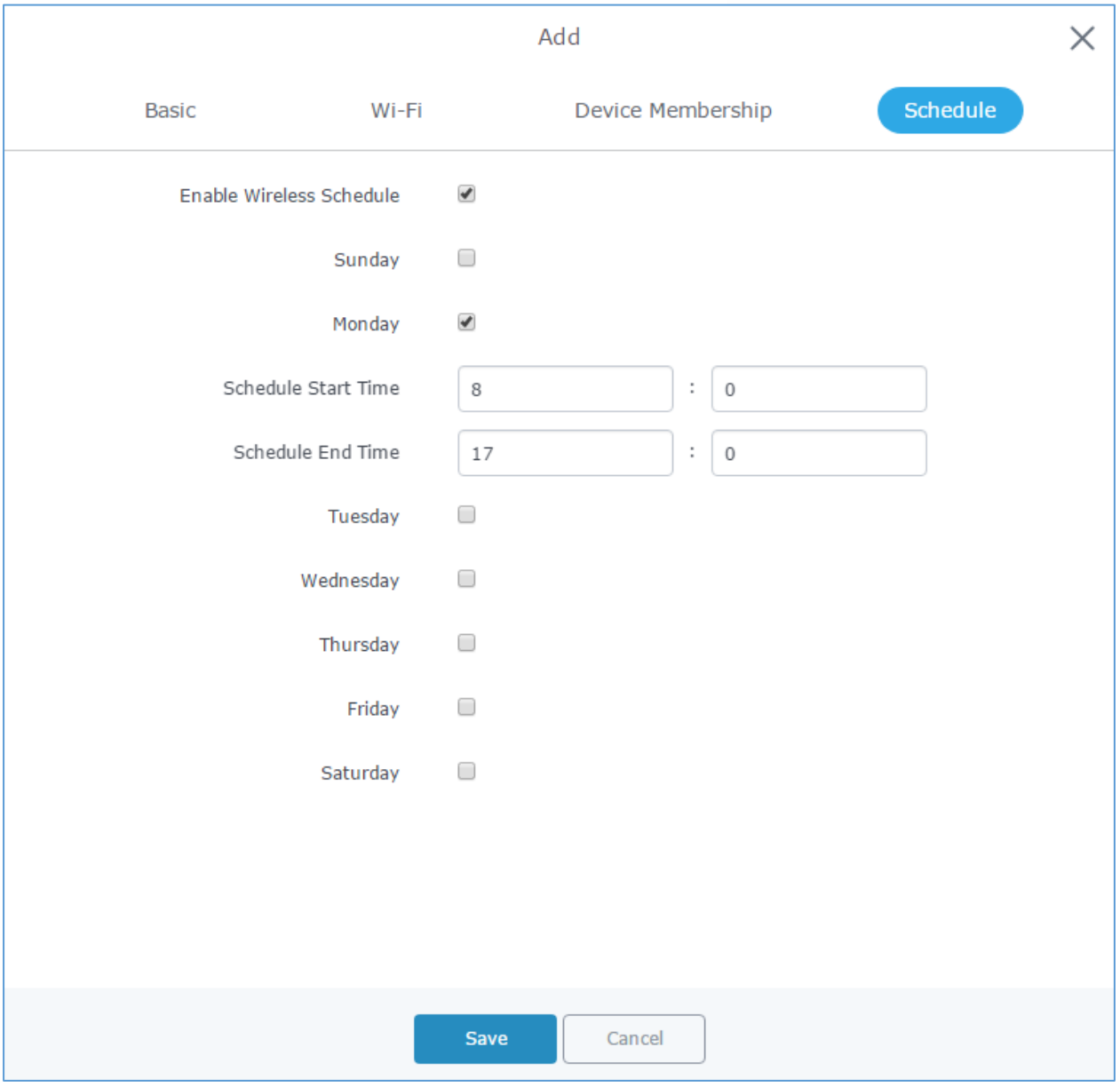



**Figure 31: Wi-Fi Schedule**

**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 

.

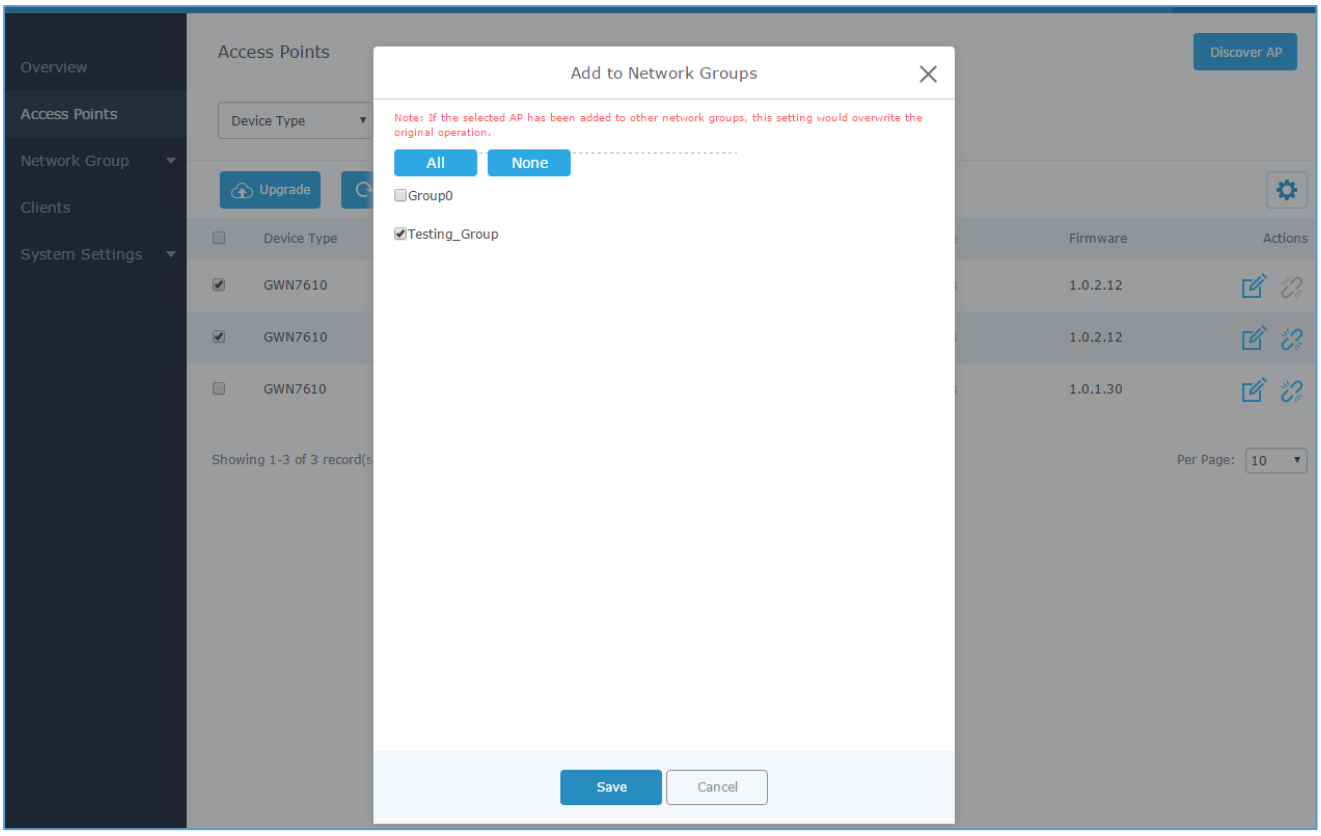



**Figure 32: Add AP to Network Group from Access Points Page**

- 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.

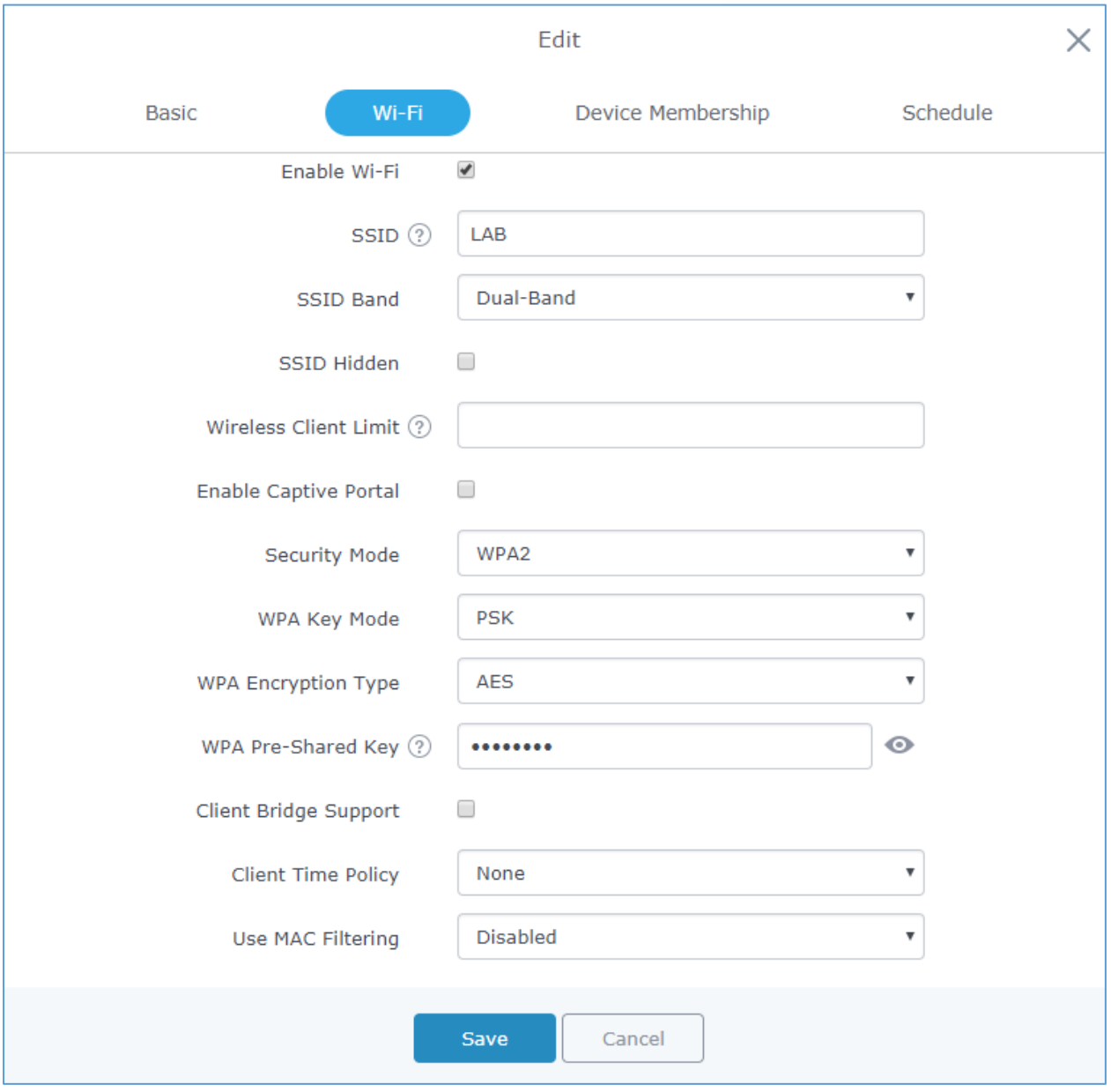



**Figure 33: Create an SSID**

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.**

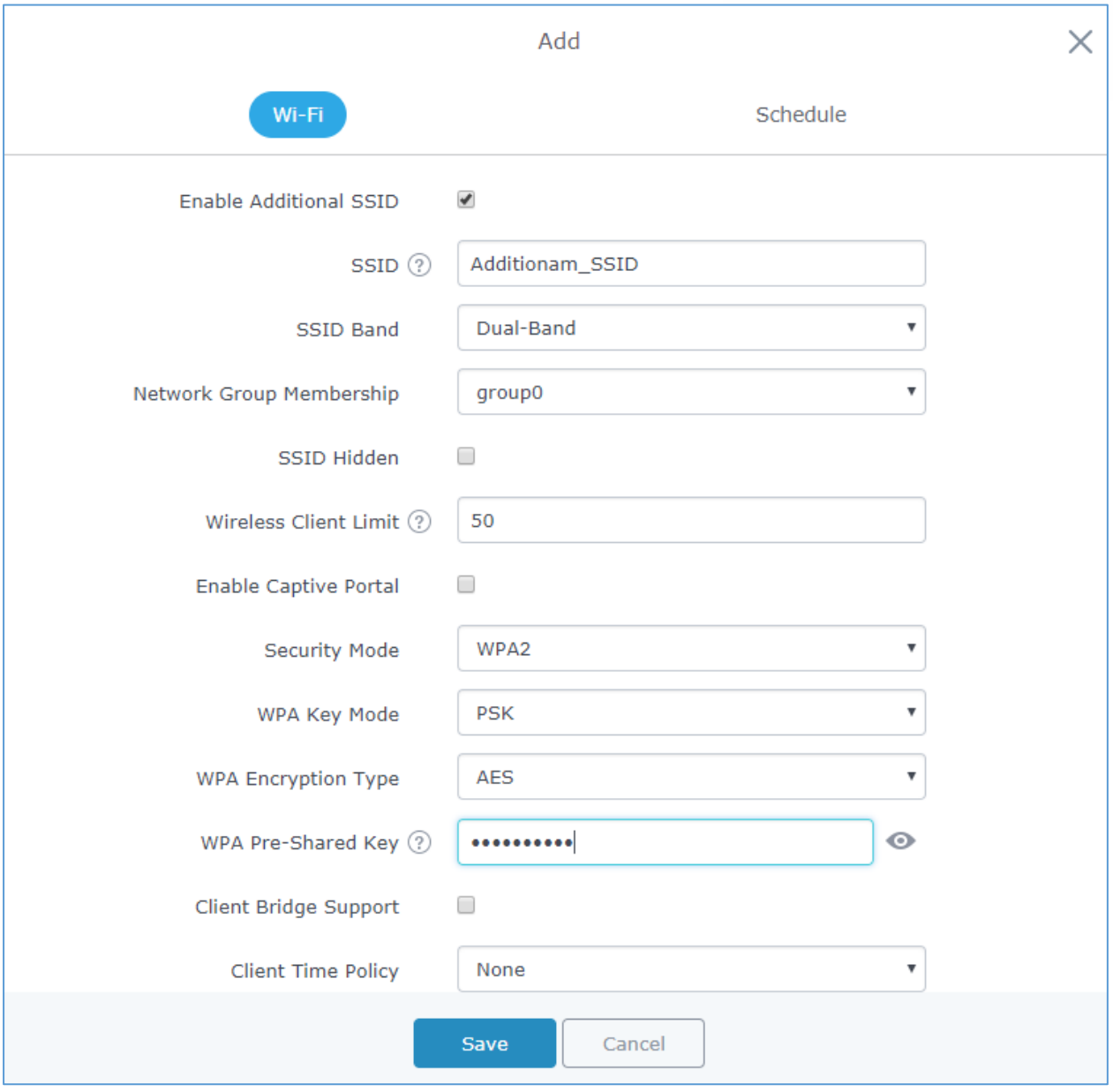



**Figure 34: Additional SSID**

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.

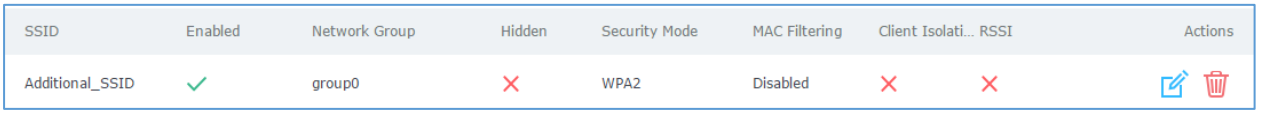



**Figure 35: Additional SSID Created**

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.

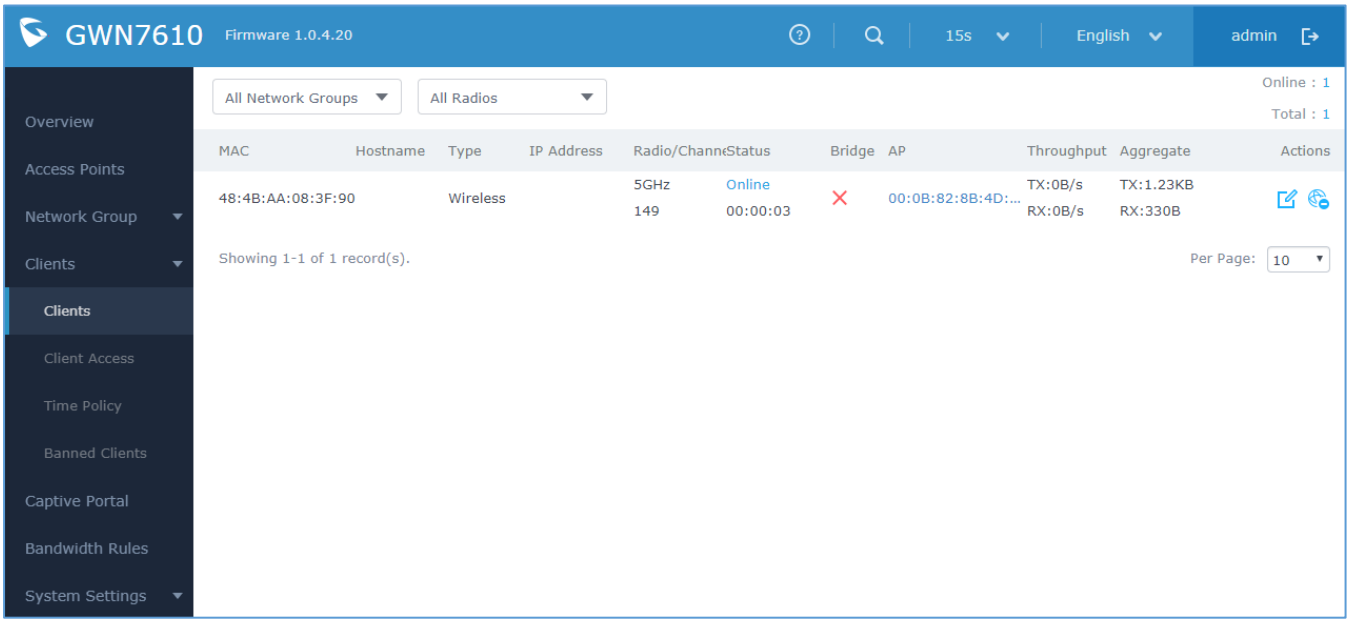



**Figure 36: Clients**

- 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 

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

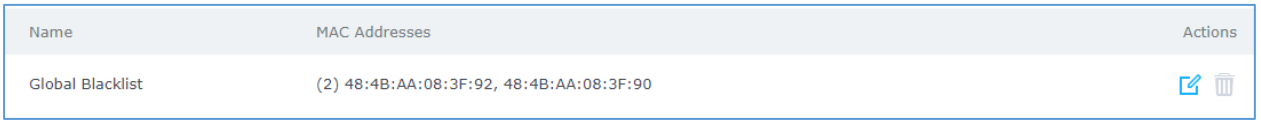



**Figure 37: Global Blacklist**

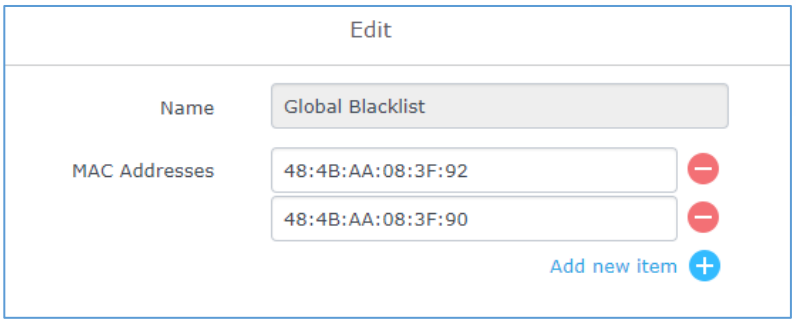



**Figure 38: Managing the Global Blacklist**

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

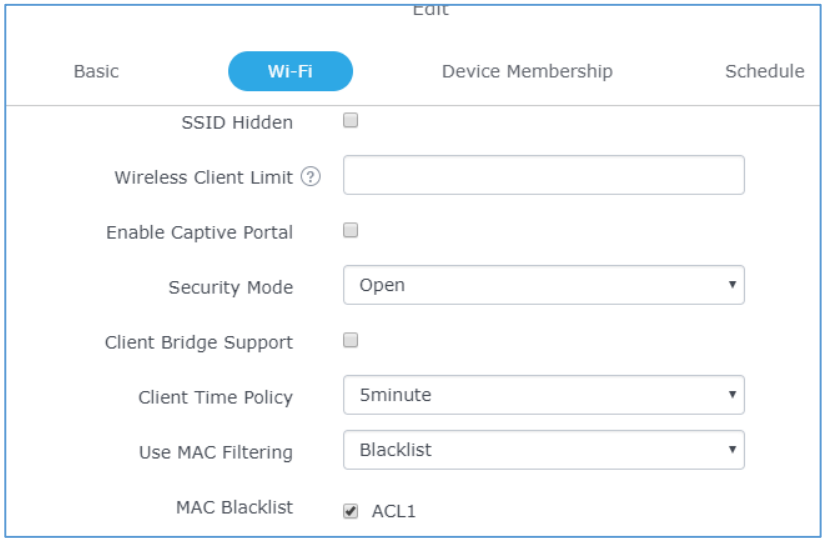



**Figure 39: Blacklist Access List**

Note: Users could set also a schedule on which the access list will be taken into consideration, please check more details under [Schedule] section.

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

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

## Banned Clients

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

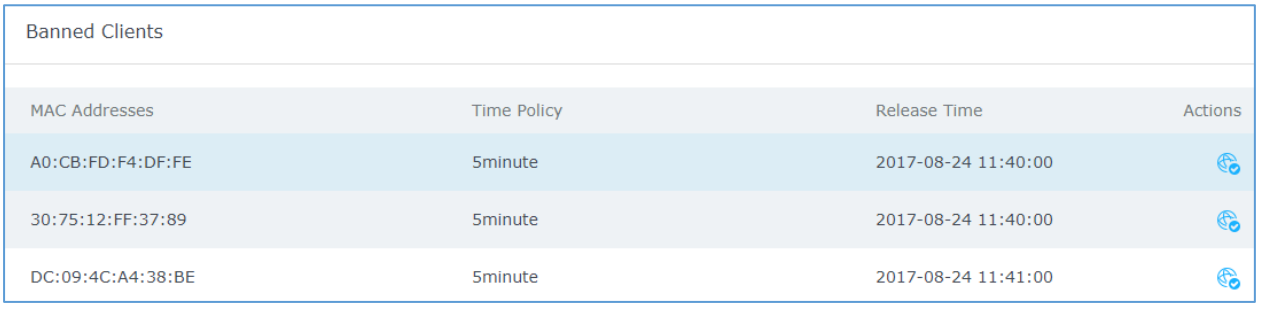



**Figure 40: Ban/Unban Client**

# 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.

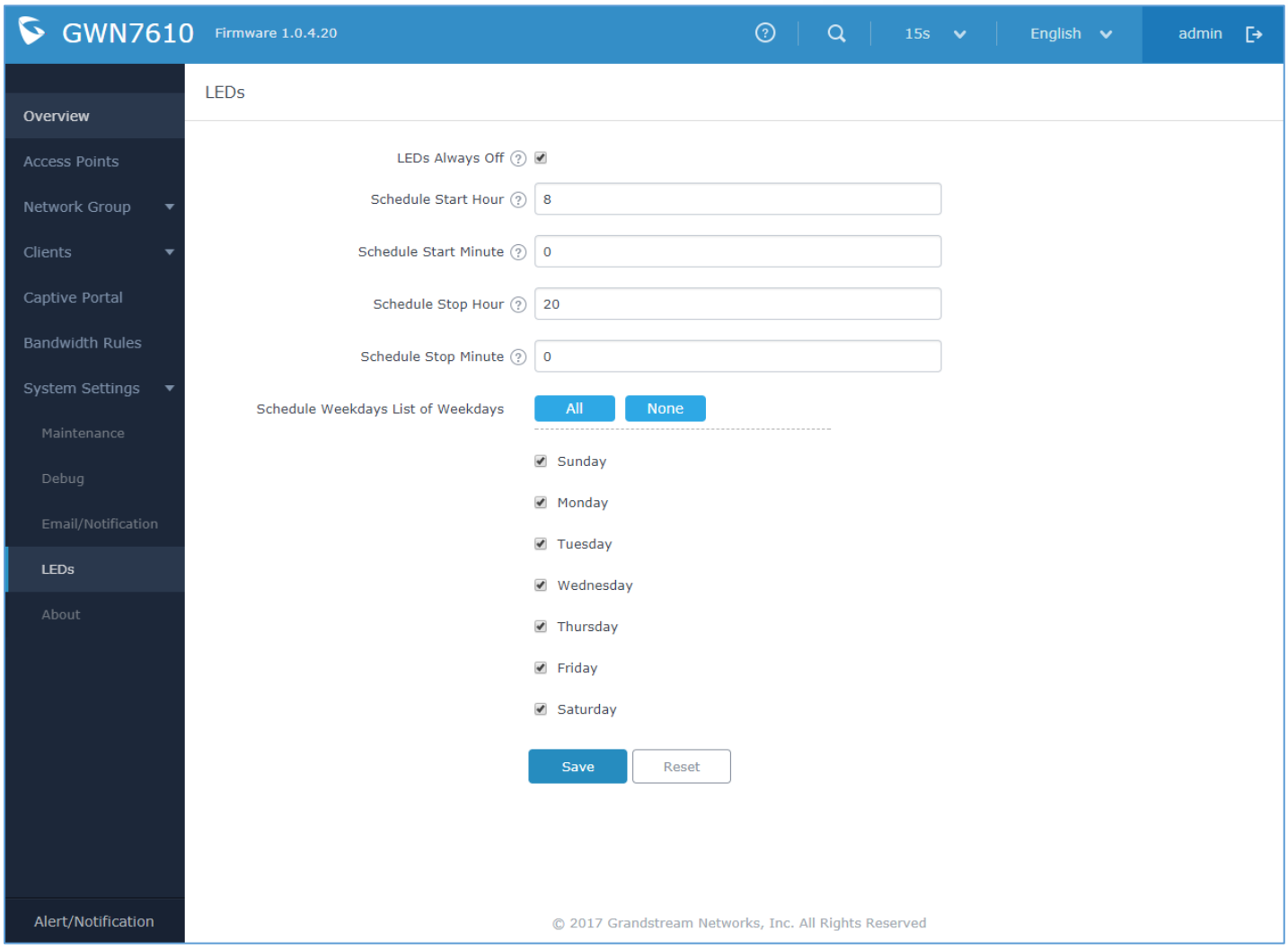



**Figure 41: LEDs Schedule**

# VOUCHER

## Voucher Feature Description

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

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

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

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

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

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

## Voucher Configuration

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

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

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

**Notes:**

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

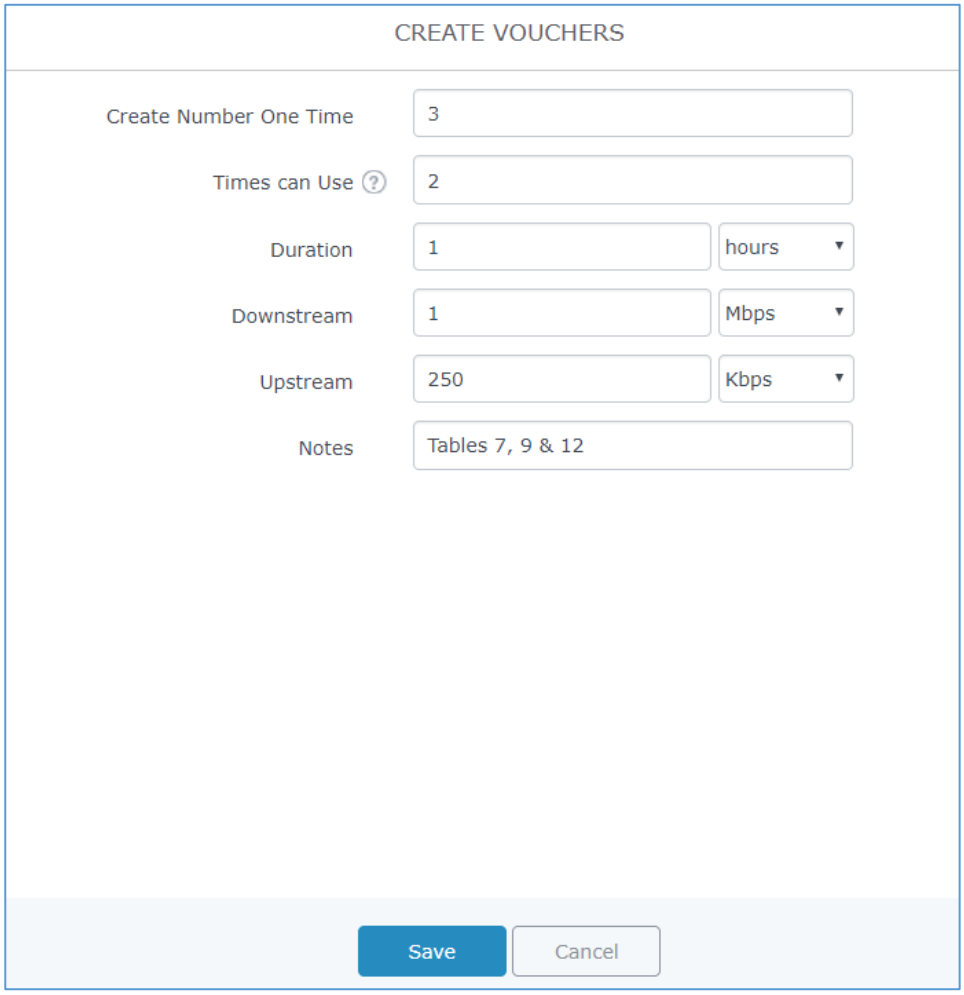



**Figure 42: Add Voucher Sample**

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

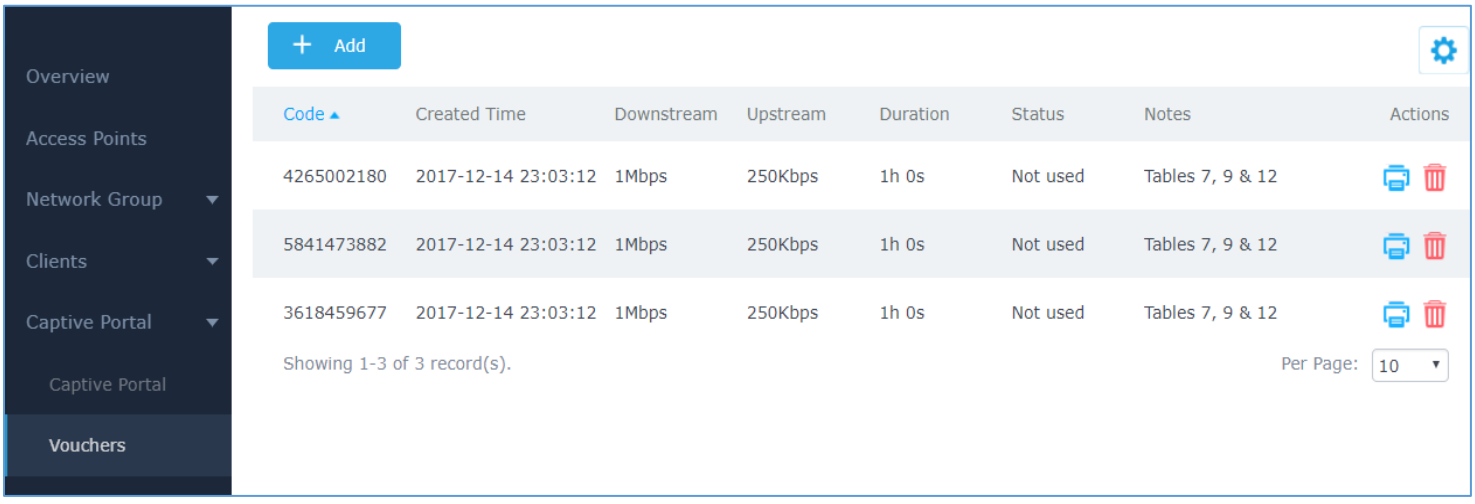



**Figure 43: Vouchers List**

The following table summarizes description for voucher configuration parameters:

**Table 10: 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). |
| **Times can Use** | Specify how many users can use the voucher. |
| **Duration** | Specify the duration after which the voucher will expire, and clients will be disconnected from internet.<br>**Note:** in case or multiple users, the duration will start counting after first user starts using the voucher. |
| **Downstream** | Set the downstream bandwidth speed limit (in Kbps or Mbps). |
| **Upstream** | Set the upstream bandwidth speed limit (in Kbps or Mbps). |
| **Notes** | Notes for the admin when checking the list of vouchers. |

## Using Voucher with GWN captive portal

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

1. Go under "**Captive Portal → Captive portal**" menu.
2. Press + Add in order to add new captive portal policy.
3. Set the following parameters as shown on the screenshot for basic setup then save and apply.

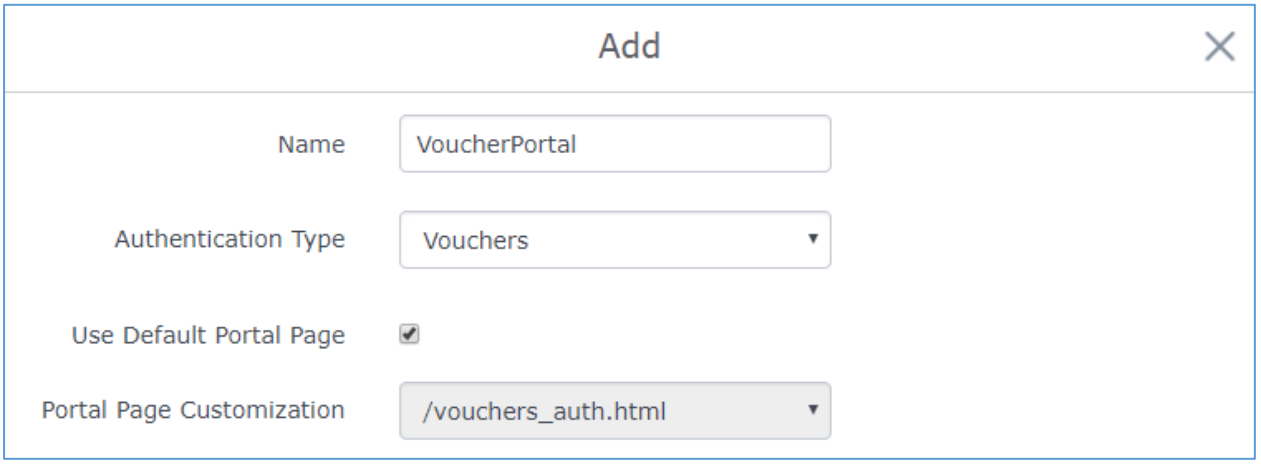



**Figure 44: Captive Portal with Voucher authentication**

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

# 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 11: 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.<br>If this field is set to 0 the landing page will never expire. |
| **Authentication Type** | Three types of authentication are available:<br>• **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.<br>• **RADIUS Server:** Choosing this option will allow users to set a RADIUS server to authenticate connecting clients.<br>• **Social Login Authentication:** Choosing this option will allow users to login using social applications such as Facebook, twitter and WeChat.<br>• **Vouchers:** Choose this option to use voucher codes for authentication.<br>• **Simple Password:** Allow authentication via simple password. |
| **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. |
| **Facebook Authentication** | Check to enable/disable Facebook Authentication |
| **Facebook App ID** | Fill in the Facebook App ID. |
| **Facebook APP Key** | Set the key for the portal, once clients want to connect to the WiFi, they should enter this key. |
| **Owner** | Enter twitter owner. |
| **Consumer Key** | Enter twitter consumer key. |
| **Consumer Secret** | Enter Twitter consumer secret. |
| **Portal Page Customization** | This option allows users to choose the portal page that will be shown once a client tries to connect to the GWN, two pages are available:<br>• **Password_Auth:** This page is used when simple password authentication policy is selected.<br>• **Portal Default:** This page is used when no authentication is specified, users will have only to accept license agreement to gain access to internet.<br>• **Portal Pass:** This option provides authentication textbox when using RADIUS authentication mode, in order to enter username and identity stored in RADIUS database.<br>• **Social_auth.**html: This will give the default portal page based on the social networking application selection (Facebook, twitter and WeChat).<br>• **Vouchers_auth.**html: This is default page to be used when having portal policy based on vouchers, see [VOUCHER].<br>• **Wechat.htm**: page used when selecting portal authentication policy via WeChat app. |
| **Landing page** | Select the landing page where the users will be sent after successful authentication, two options are available:<br>• **Redirect External Page URL Address:** for promotional purposes, admin can this to redirect all authenticated users to the company website. |

| | |
|---|---|
| | • **Redirect to the Original URL Address:** Sent the user to the original requested URL. |
| **Enable HTTPS** | Check to enable/disable HTTPS service over captive portal. |
| **Pre-Authentication Rule(s)** | Set the Pre-Authentication Rules for temporarily release the IP or ports of the devices (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET) |
| **Post Authentication Rule(s)** | Set the Post Authentication Rules (e.g.: subnet:192.168.10.1/12, TCP: TCP src 80 dst 80, UDP: UDP src 80 dst 80, SSH, TELNET, HTTP, HTTPS) |

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

**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:

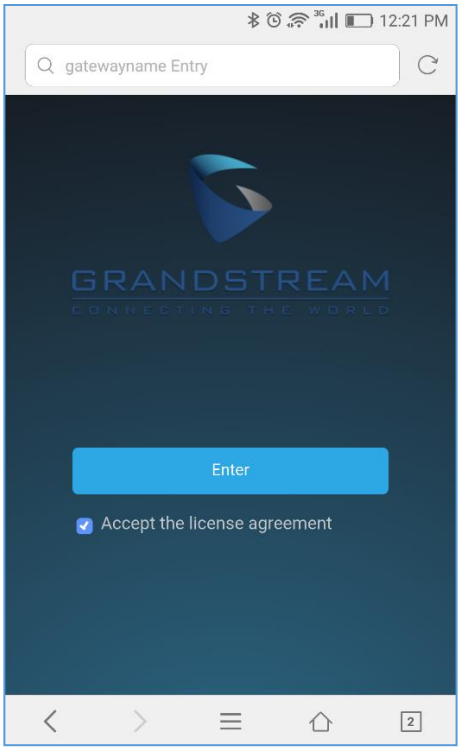



**Figure 45: portal_default.html page**

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

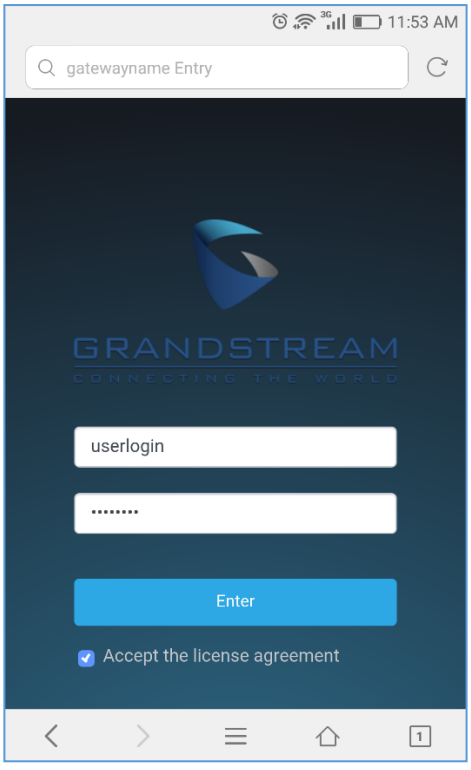



**Figure 46: portal_pass.html page**

The following figure shows default files used for Captive Portal:

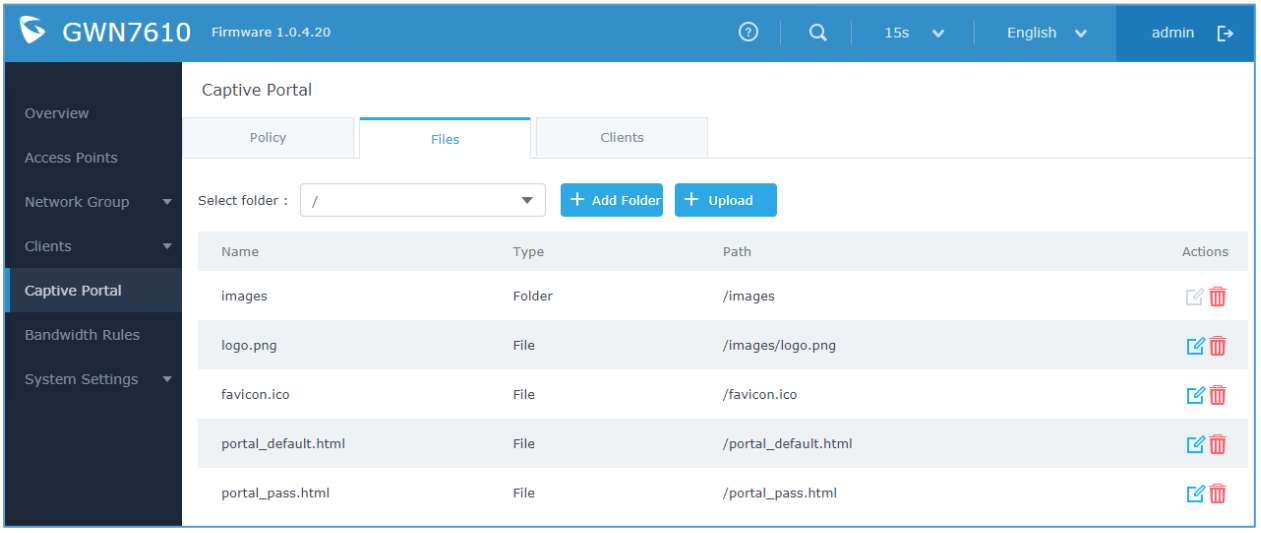
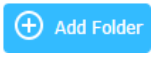
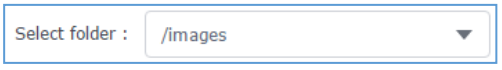



**Figure 47: Files Settings Page**

- Click  to upload a new Web page.
- Click  to add a new folder.
- Click  to upload files to the selected folder.
- Folder can be selected from the dropdown list  .

## Clients Page

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

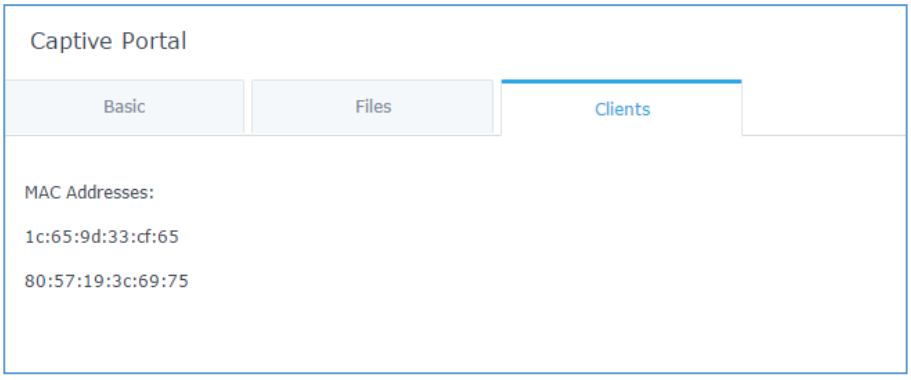



Figure 48: Client Web Page

# 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 

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

**Table 12: Bandwidth Rules**

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

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

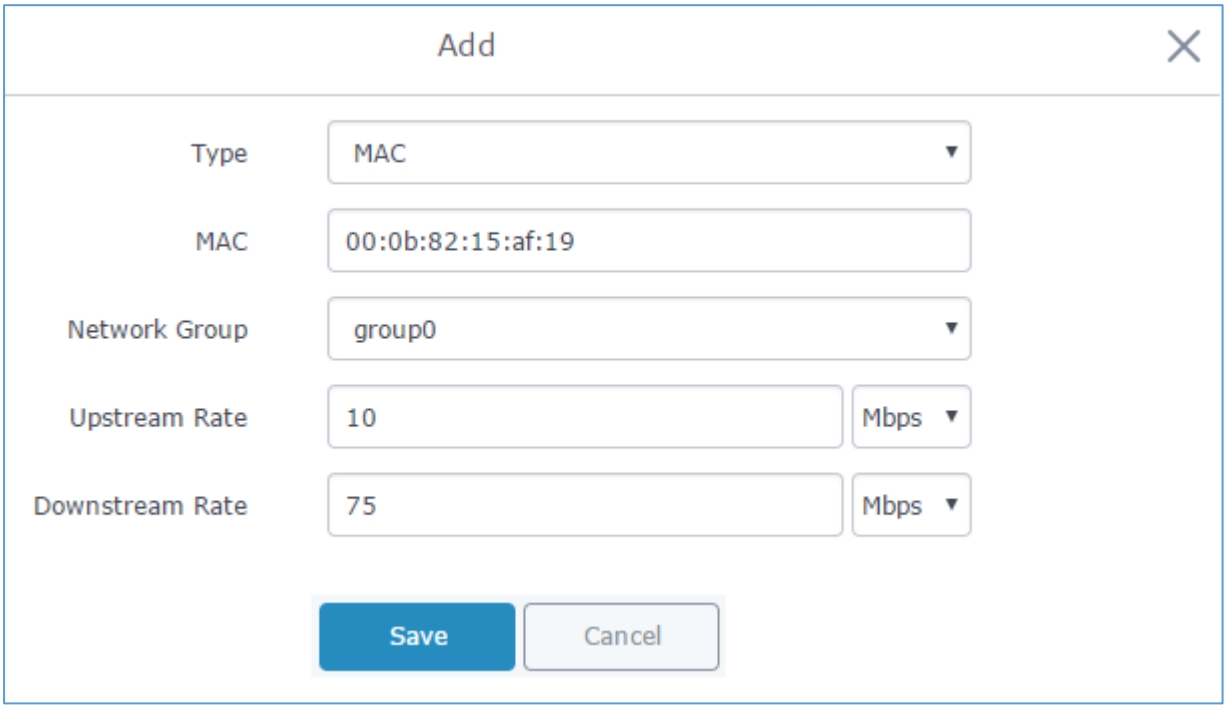



**Figure 49: MAC Address Bandwidth rule**

The following figure shows examples of bandwidth rules:

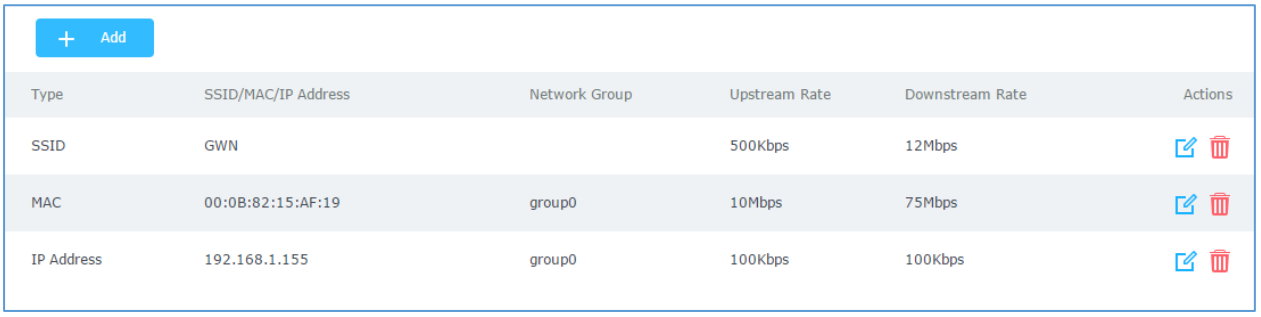



**Figure 50: Bandwidth Rules**

**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 13: 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 14: 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 15: 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 16: 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).<br>• Every X hours (0-23)<br>• Every X Minutes (0-59).<br>• X hour of day (0-23).<br>• 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.

The log files can be seen on the list below after pressing “List” button:

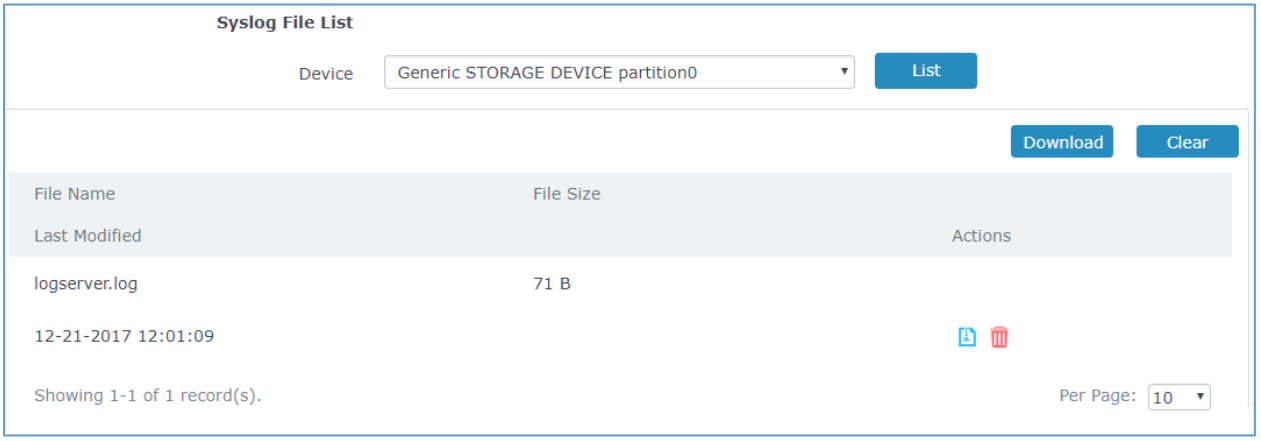



**Figure 51: Log Files List**

## 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.

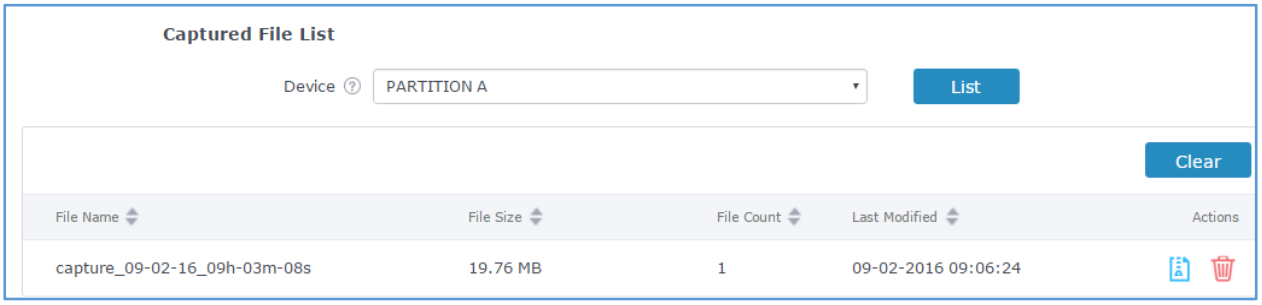



**Figure 52: Capture Files**

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

**Table 17: 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.**

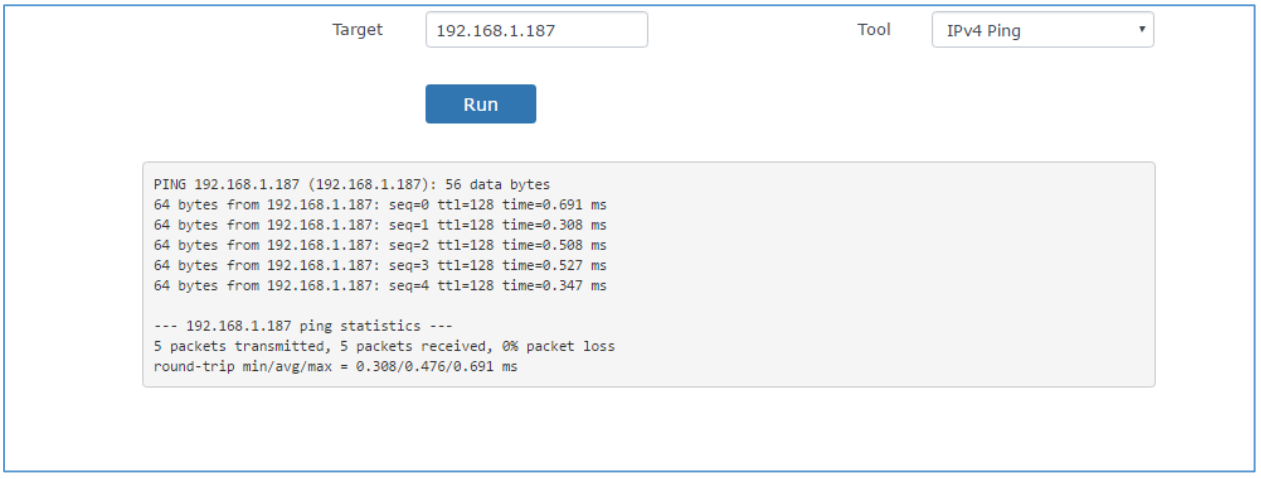



**Figure 53: IP Ping**

- 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**.

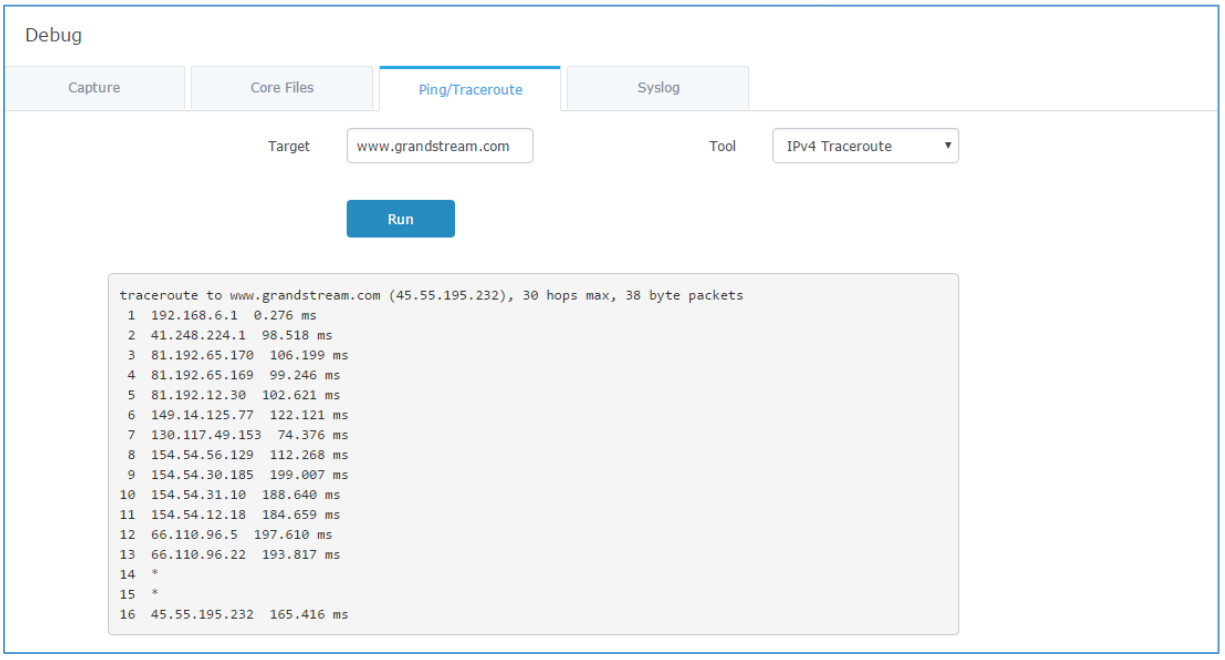



**Figure 54: Traceroute**

## Syslog

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

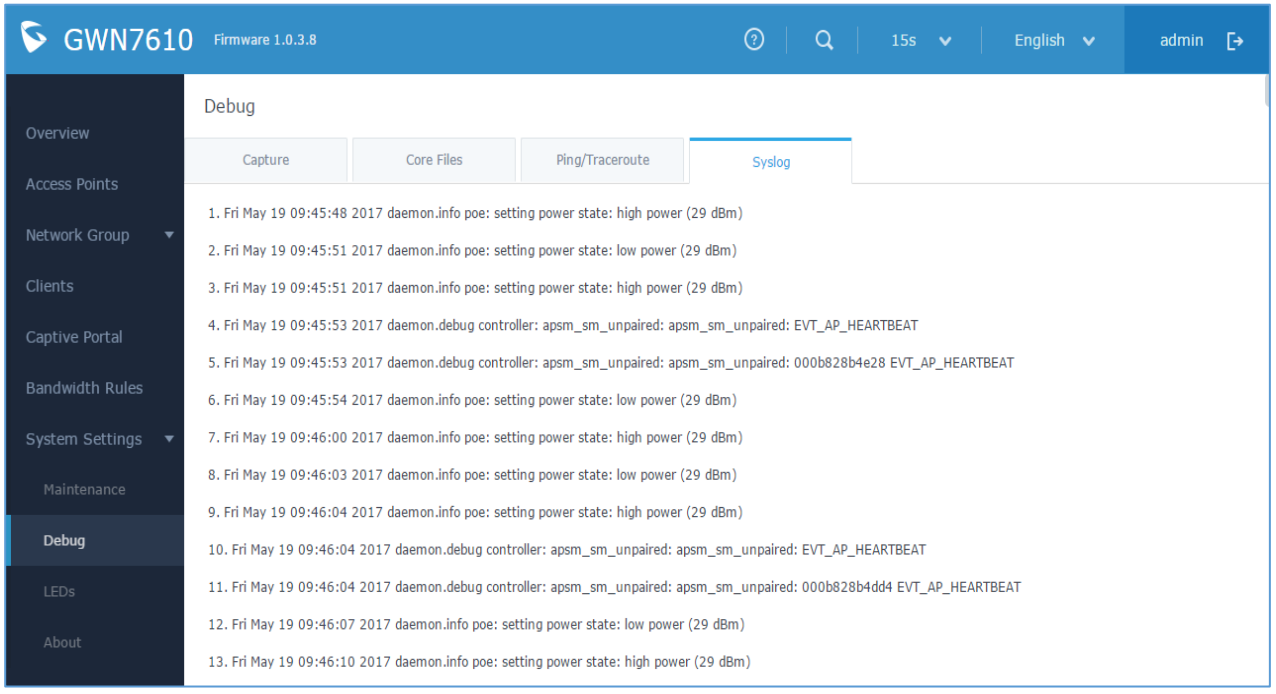



**Figure 55: Syslog**

## Schedule

Users can use the schedule configuration menu to set specific schedule for GWN features (bandwidth rules, access control), while giving the flexibility to specify the date and time to turn On/Off the selected feature.
In order to configure a new schedule, follow below steps:

1. Navigate to “System Settings → Schedule”.
2. Press + Add to add new schedule.
3. Enable the schedule and select associated feature (bandwidth rule or client access).
4. Specify the date and time along with months and days to enable ON and Off the feature.
5. Press save and apply the changes.

After the configuration done, the GWN will check regularly the date and time in order to decide whether to activate or deactivate the associated feature with the schedule.
The figure on next page shows a sample configuration that enabled bandwidth rule limitation during office working hours for WiFi users:

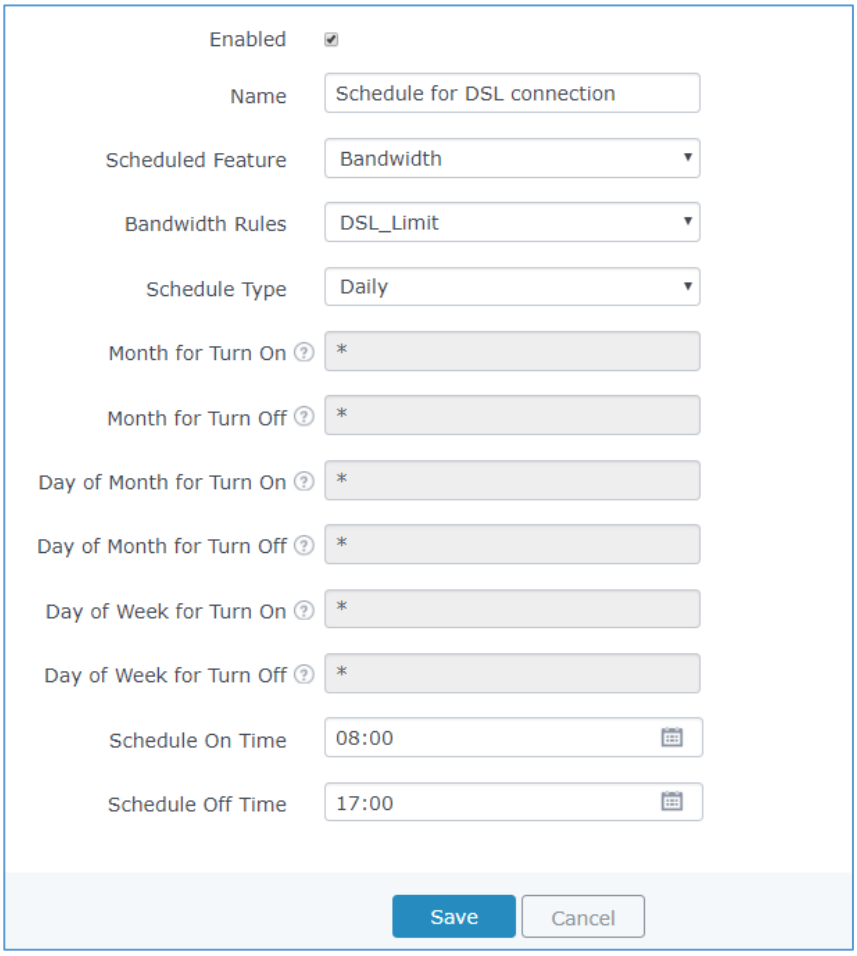



**Figure 56: Schedule Sample**

**Note:**

For date and time settings, user have two options:

1- Either enter the number for the month (1 for January 2 for February …etc) or enter * symbol (default value) to specify all months of the year. Same goes for day of the month and day of the week.

2- Select the schedule Type from the drop-down list (daily, all weekdays, weekends, monthly and annually).

## 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 18: 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 19: 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 Master AP 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 20: 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.**

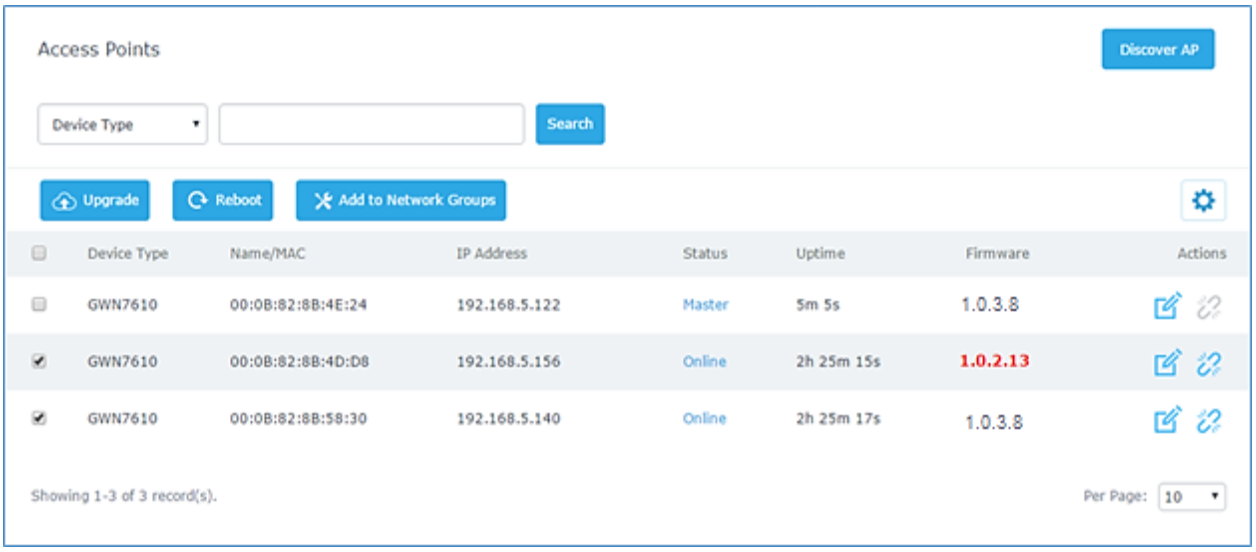
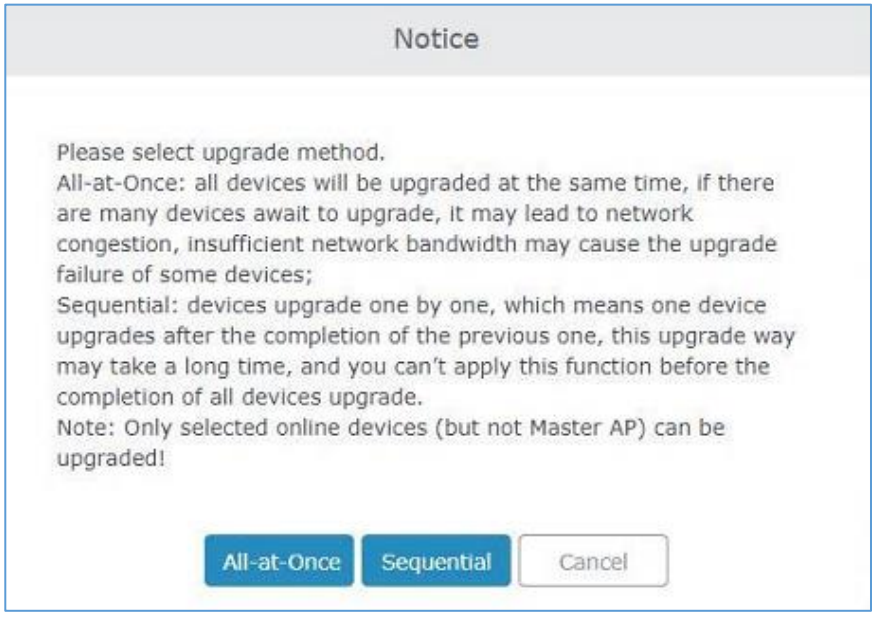



**Figure 57: Access Points**

For multiple devices upgrade, users should make sure that firmware server path is set correctly under maintenance configuration menu then check the desired APs to upgrade, and click on 


### Slave AP upgrade Modes

Once pressed the button, there are two modes for slave firmware upgrade:




1. Simultaneous upgrade: users can press "All-at-once" button in order to launch firmware upgrade process under all selected devices. This could consume lots of bandwidth and will halt the WiFi service during the full process.
2. Sequential upgrade: if sequential mode is selected, the controller will trigger the firmware upgrade process under salve access points on a sequential fashion, thus consuming less bandwidth on the network and not interrupting the full WiFi service during full process.


**Note:** Once you choose sequential upgrade, the number with beside the green upgrading icon will tell you how many slaves have done its upgrading.

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


**Figure 58: 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.