

Grandstream Networks, Inc.

GWN7600LR

Enterprise 802.11ac Wave-2

Outdoor Long Range WiFi Access Point

User Manual



COPYRIGHT

©2017 Grandstream Networks, Inc. <http://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

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.



FCC Caution

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

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

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

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



GNU GPL INFORMATION

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

Grandstream GNU GPL related source code can be downloaded from Grandstream web site:

<http://www.grandstream.com/support/faq/gnu-general-public-license>



Table of Contents

DOCUMENT PURPOSE	11
CHANGE LOG	12
Firmware Version 1.0.3.24	12
Firmware Version 1.0.3.19	12
Firmware Version 1.0.2.52	12
WELCOME	13
PRODUCT OVERVIEW	14
Technical Specifications	14
INSTALLATION	16
Equipment Packaging	16
GWN7600LR Access Point Ports	17
Power and Connect GWN7600LR Access Point	18
Mounting Instructions	18
Warranty	19
GETTING STARTED	20
LED Patterns	20
Discover the GWN7600LR	20
<i>Method 1: Discover GWN7600LR using its MAC address</i>	<i>20</i>
<i>Method 2: Discover GWN7600LR using GWN Discovery Tool</i>	<i>21</i>
Use the Web GUI	22
<i>Access Web GUI</i>	<i>22</i>
<i>Web GUI Languages</i>	<i>23</i>
<i>Overview Page</i>	<i>24</i>
<i>Save And Apply Changes</i>	<i>25</i>
USING GWN7600LR AS STANDALONE ACCESS POINT	26



Connect to GWN7600LR Default Wi-Fi Network	26
USING GWN7600LR AS MASTER ACCESS POINT CONTROLLER	27
Login Page	28
Discover and Pair Other GWN7600LR Access Point	28
Failover Master	31
NETWORK GROUPS	34
CLIENTS CONFIGURATION	42
LED SCHEDULE	43
CAPTIVE PORTAL	45
<i>Policy Configuration Page</i>	45
<i>Files Configuration Page</i>	48
<i>Clients Page</i>	49
BANDWIDTH RULES	50
SYSTEM SETTINGS	52
Maintenance	52
<i>Basic</i>	52
<i>Upgrade</i>	52
<i>Access</i>	53
<i>Syslog</i>	53
Debug	54
<i>Core Files</i>	54
<i>Ping/Traceroute</i>	54
<i>Syslog</i>	55
UPGRADING AND PROVISIONING	56
Upgrading Firmware	56
<i>Upgrading via Web GUI</i>	56
Upgrading Slave Access Points	56



Provisioning and backup.....	58
<i>Download Configuration</i>	58
<i>Configuration Server</i>	58
Reset and reboot	58
EXPERIENCING THE GWN7600LR WIRELESS ACCESS POINT	59



Table of Tables

Table 1: GWN7600LR Technical Specifications	14
Table 2: GWN7600LR Equipment Packaging	16
Table 3: GWN7600LR Ports Description	17
Table 4: LED Patterns	20
Table 5: Overview	25
Table 6: Device Configuration	30
Table 7: Wi-Fi	35
Table 8: LEDs	43
Table 9: Policy Add	46
Table 10: Bandwidth Rules	50
Table 11: Basic	52
Table 12: Upgrade	52
Table 13: Access	53
Table 14: Syslog	53
Table 15: Network Upgrade Configuration	56



Table of Figures

Figure 1: GWN7600LR Equipment Package	16
Figure 2: GWN7600LR Ports	17
Figure 3: GWN7600LR Vertical Mounting	18
Figure 4: GWN7600LR Horizontal Mounting	19
Figure 5: Discover the GWN7600LR using its MAC Address	21
Figure 6: GWN Discovery Tool	22
Figure 7: GWN7600LR Web GUI Login Page	23
Figure 8: GWN7600LR Web GUI Language	23
Figure 9: GWN7600LR Web GUI Language	24
Figure 10: Overview Page	24
Figure 11: Apply Changes	25
Figure 12: Apply Successful	25
Figure 13: MAC Tag Label	26
Figure 14: Login Page	27
Figure 15: Setup Wizard	28
Figure 16: Discover and Pair GWN7600LR	29
Figure 17: Discovered Devices	29
Figure 18: GWN7600LR online	30
Figure 19: Failover Master	32
Figure 20: Failover Mode GUI	33
Figure 21: Network Group	34
Figure 22: Add a New Network Group	35
Figure 23: Device Membership	39
Figure 24: WiFi Schedule	40
Figure 25: Add AP to Network Group	40
Figure 26: Additional SSID	41
Figure 27: Additional SSID Created	41
Figure 28: Clients	42
Figure 29: Ban/Unban Client	42
Figure 30: Paginate between client's list	42
Figure 31: LED Scheduling Sample	44
Figure 32: Captive Portal policy	45
Figure 33: Add a new policy	46
Figure 34: Captive Portal Files	48
Figure 35: Captive Portal Clients	49
Figure 36: MAC Address Bandwidth rule	51
Figure 37: Bandwidth Rules	51
Figure 38: IP Ping	54
Figure 39: IP Traceroute	55



Figure 40: Syslog	55
Figure 41: Access Points.....	57



DOCUMENT PURPOSE

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

This guide covers following topics:

- [Product Overview](#)
- [Installation](#)
- [Getting Started](#)
- [Using GWN7600LR as Standalone Access Point](#)
- [Using GWN7600LR as Master Access Point Controller](#)
- [Network Groups](#)
- [Clients Configuration](#)
- [System Settings](#)
- [Upgrading and Provisioning](#)
- [Experiencing the GWN7600LR Wireless Access Point](#)



CHANGE LOG

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

Firmware Version 1.0.3.24

- No major changes.

Firmware Version 1.0.3.19

- Added support for Captive Portal [CAPTIVE PORTAL]
- Added support for better roaming decision. [Enable Voice Enterprise]
- Added support for Failover. [Failover Master]
- Added support for VLAN assignment via RADIUS. [Enable Dynamic VLAN (beta)]
- Added support for select SSID Band. [SSID Band]
- Added support for Exact Radio Power Configuration in dBm [Custom Wireless Power]
- Added support for AP locating. [AP Locating]
- Added support for Bandwidth Rules. [BANDWIDTH RULES]
- Added option to limit clients count per SSID. [Wireless Client Limit]
- Added support for Wireless Schedule. [Wireless Schedule]
- Added support for LED control [LED SCHEDULE]
- Added option to enable/disable DHCP option 66 & 43 override [Allow DHCP options 66 and 43 override]

Firmware Version 1.0.2.52

- This is the initial version.



WELCOME

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

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

 **Caution:**

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



PRODUCT OVERVIEW

Technical Specifications

Table 1: GWN7600LR Technical Specifications

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



SSIDs	16 SSIDs per access point
Concurrent Clients	450+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole
Mounting	Outdoor base bracket and cover bracket included
LEDs	1 tri-color LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7600LR allows it to auto-discover, auto-provision and manage up to 30 GWN76XXs in a network
Power and Green Energy Efficiency	Power over Ethernet 802.3af and 802.3at compliant Maximum Power Consumption: <ul style="list-style-type: none"> ▪ 12.9 W (PoE supply) ▪ 23.0 W (PoE+ supply)
Temperature & Humidity	Operation: -30°C to 60°C Storage: -30°C to 70°C Humidity: 5% to 95% Non-condensing
Physical	Unit Dimension: 290×150×35mm; Unit Weight: 708g Unit + Mounting Kits Dimension: 290×150×56mm; Unit + Mounting Kits Weight: 1528.2g Entire Package Dimension: 423×187×97mm; Entire Package Weight: 1844g
Package Content	Enterprise 802.11ac Wave-2 Outdoor Long Range WiFi Access Point, Mounting Kits, Quick Installation Guide
Waterproof Grade	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC



INSTALLATION

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

Equipment Packaging

Table 2: GWN7600LR Equipment Packaging

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



Figure 1: GWN7600LR Equipment Package



GWN7600LR Access Point Ports

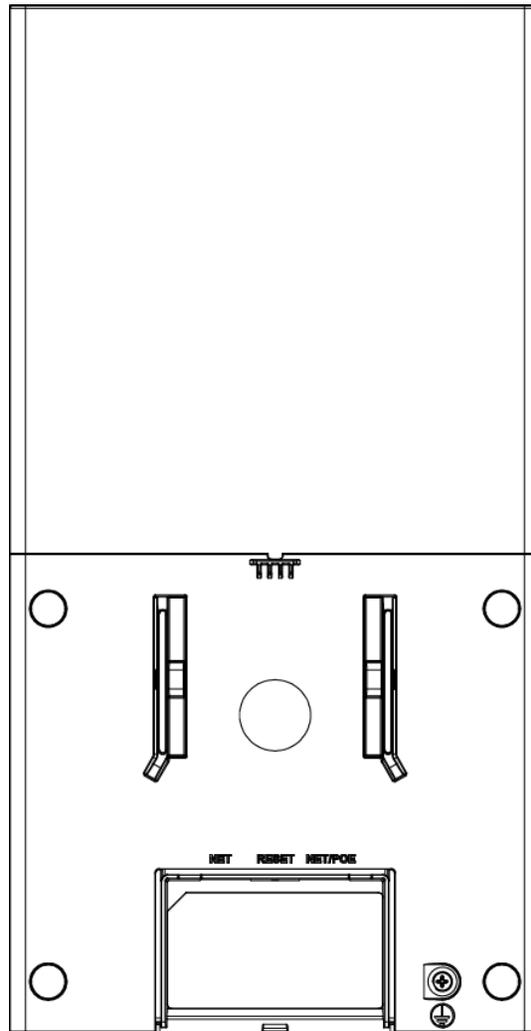


Figure 2: GWN7600LR Ports

Table 3: GWN7600LR Ports Description

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



Power and Connect GWN7600LR Access Point

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

Mounting Instructions

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

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

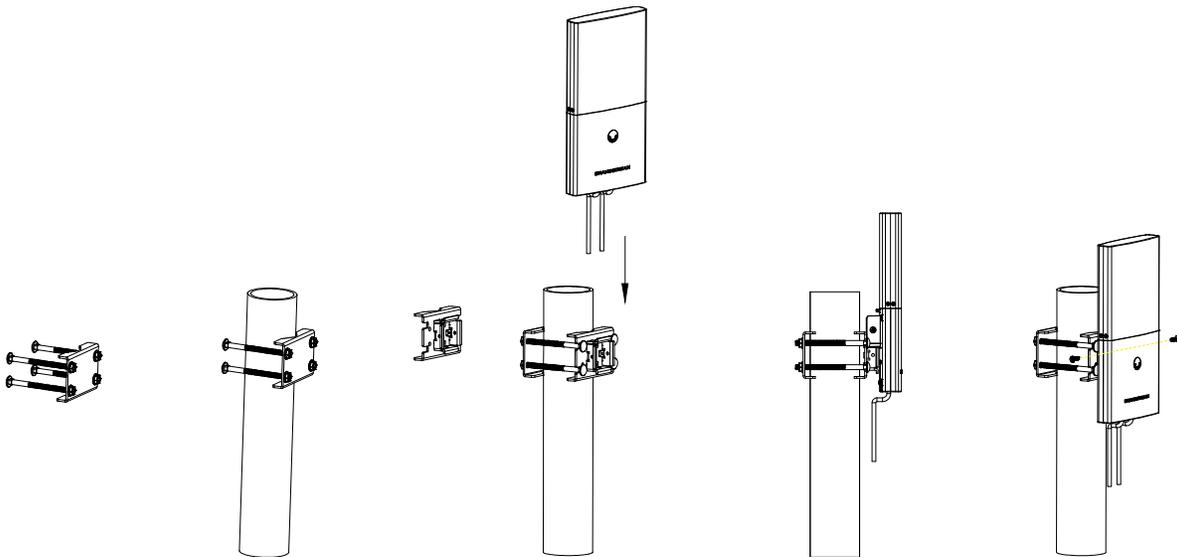


Figure 3: GWN7600LR Vertical Mounting

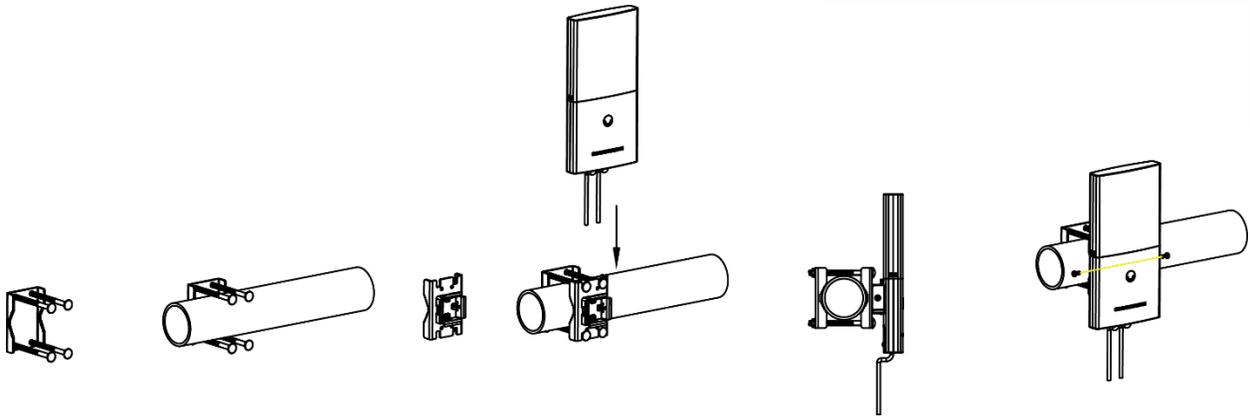


Figure 4: GWN7600LR Horizontal Mounting

Warranty

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



GETTING STARTED

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

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

LED Patterns

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

The table below describes LED patterns available on GWN7600LR.

Table 4: LED Patterns

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

Discover the GWN7600LR

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

Method1: Discover GWN7600LR using its MAC address

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



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

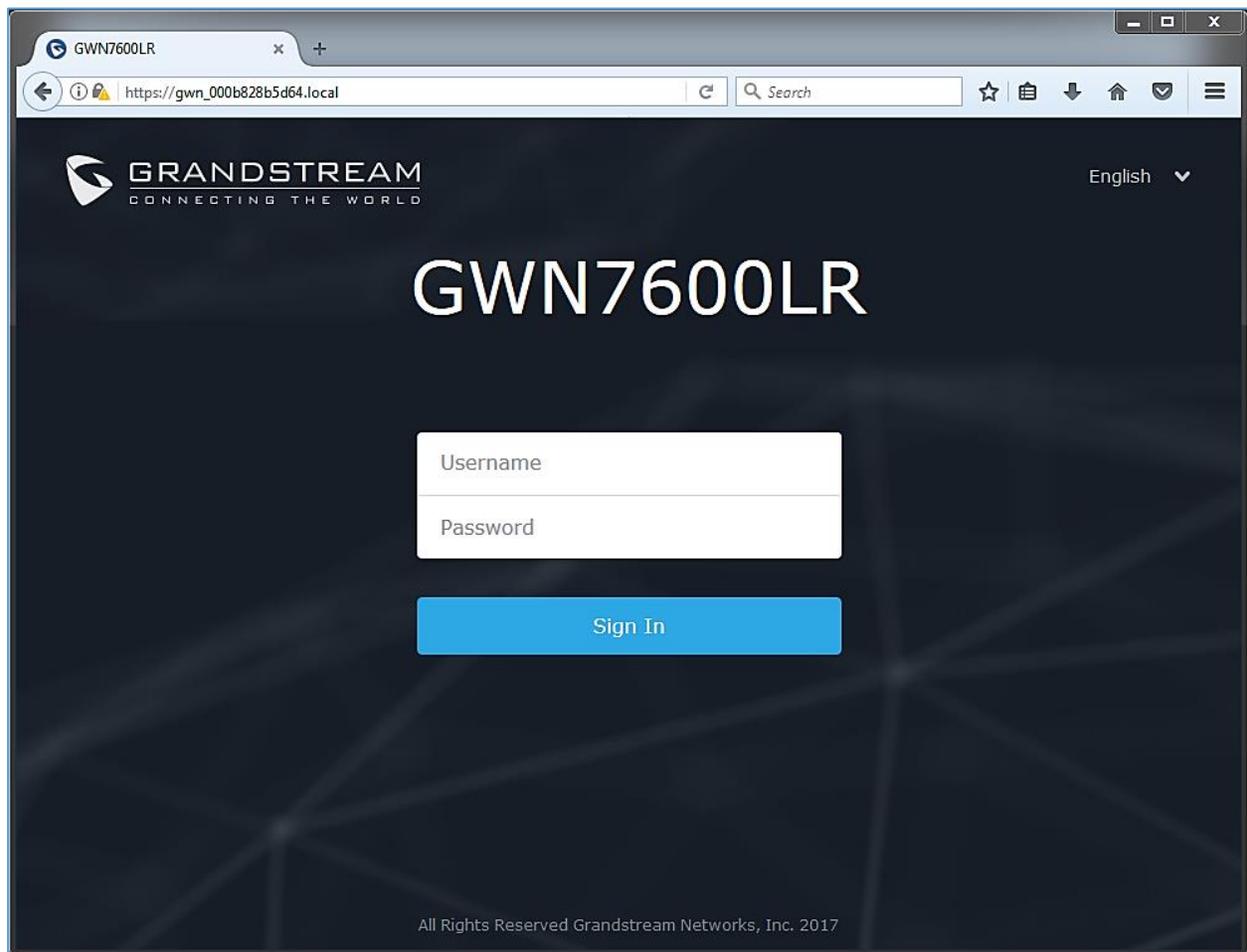


Figure 5: Discover the GWN7600LR using its MAC Address

Method 2: Discover GWN7600LR using GWN Discovery Tool

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



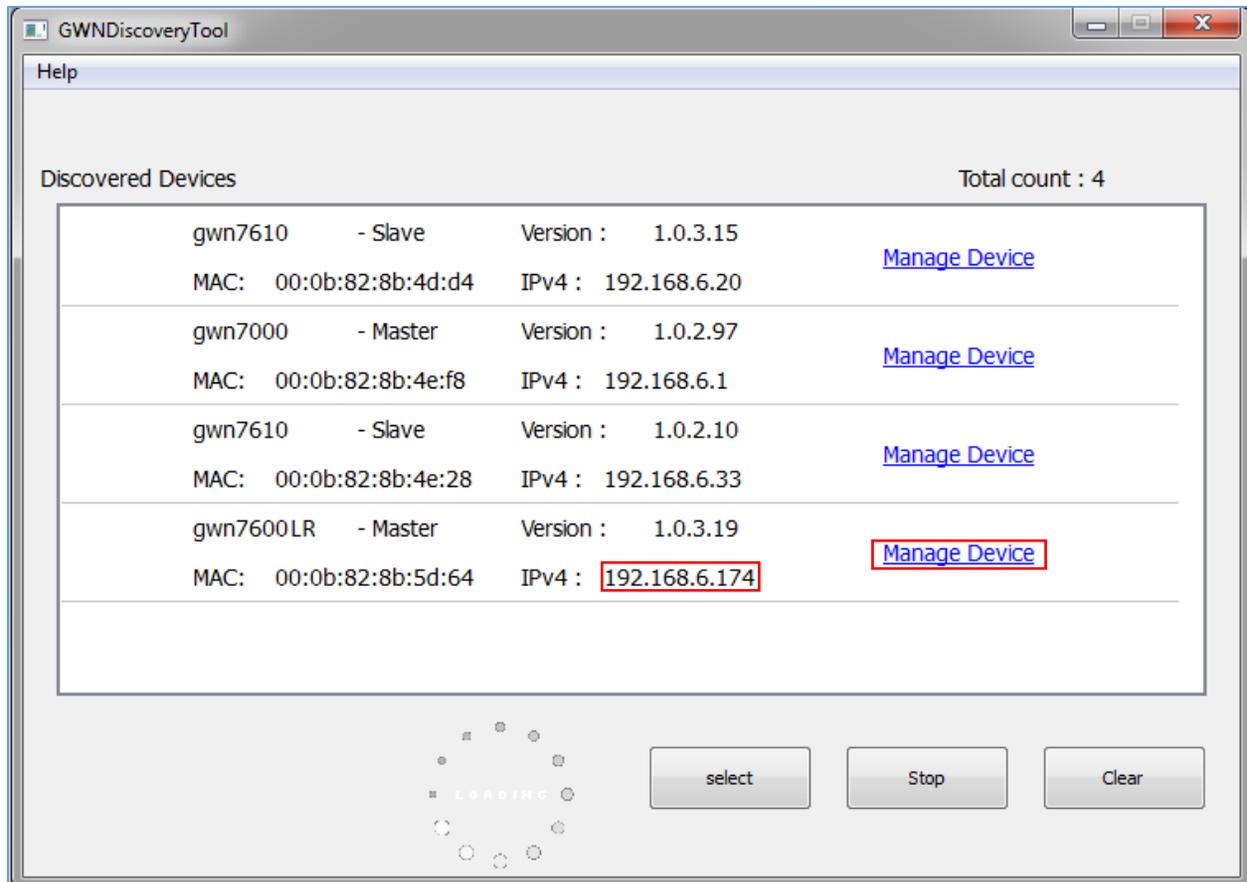


Figure 6: GWN Discovery Tool

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

Use the Web GUI

Access Web GUI

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



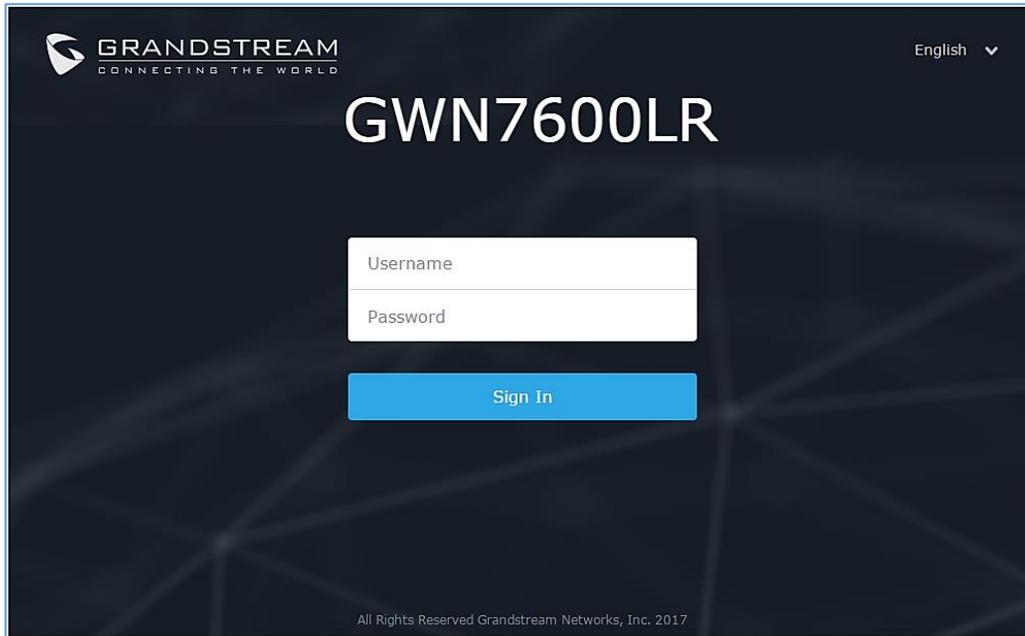


Figure 7: GWN7600LR Web GUI Login Page

To access the Web GUI:

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

https://IP_Address

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

Web GUI Languages

Currently the GWN7600LR series web GUI supports **English** and **Simplified Chinese**.

Users can select the displayed language at the upper right of the web GUI either before or after logging in.

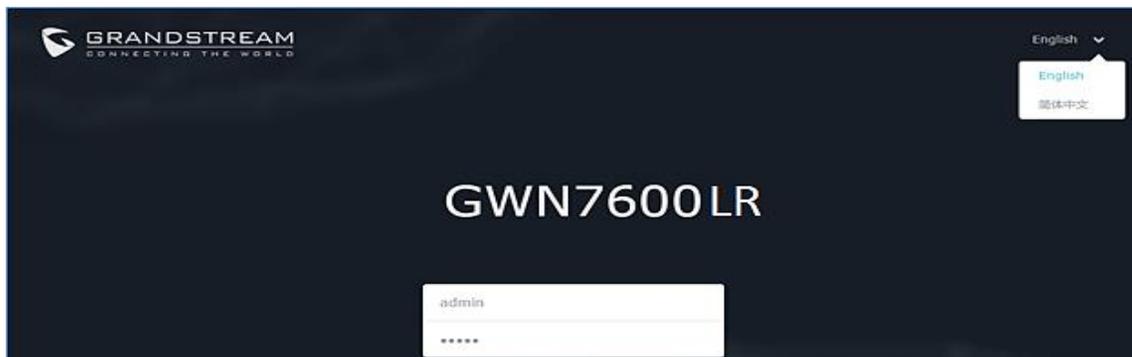


Figure 8: GWN7600LR Web GUI Language





Figure 9: GWN7600LR Web GUI Language

Overview Page

Overview is the first page shown after successful login to the GWN7600LR's Web Interface.

Overview page provides an overall view of the GWN7600LR's information presented in a Dashboard style for easy monitoring.

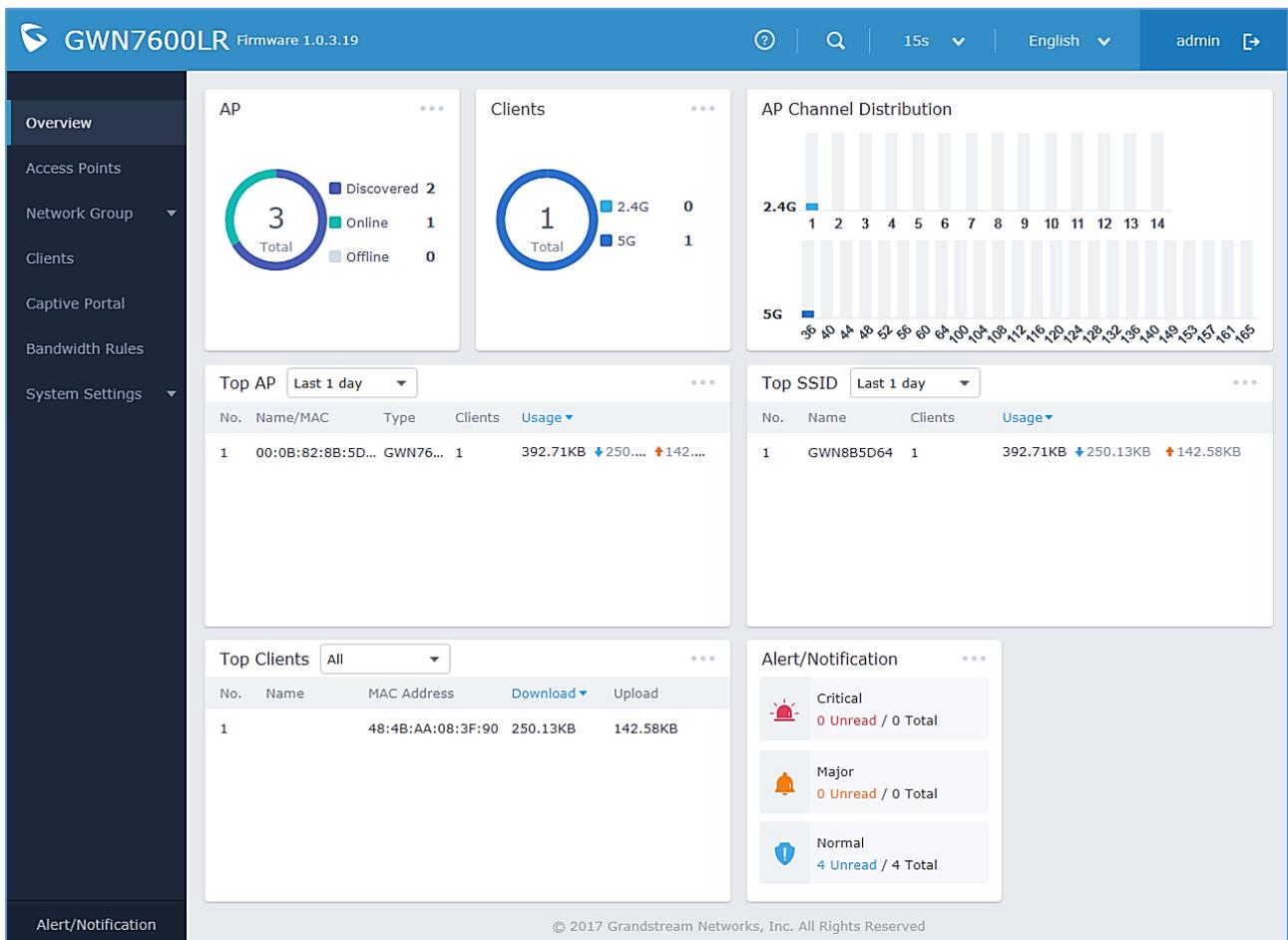


Figure 10: Overview Page

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



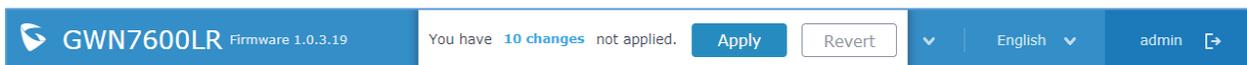
Table 5: Overview

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

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

Save And Apply Changes

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


Figure 11: Apply Changes

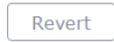
Click on  button to apply changes, or  to undo the changes.


Figure 12: Apply Successful


USING GWN7600LR AS STANDALONE ACCESS POINT

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

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

Connect to GWN7600LR Default Wi-Fi Network

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

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

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



Figure 13: MAC Tag Label

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

USING GWN7600LR AS MASTER ACCESS POINT CONTROLLER

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

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



Figure 14: Login Page

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

 **Warning:**

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

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



Login Page

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

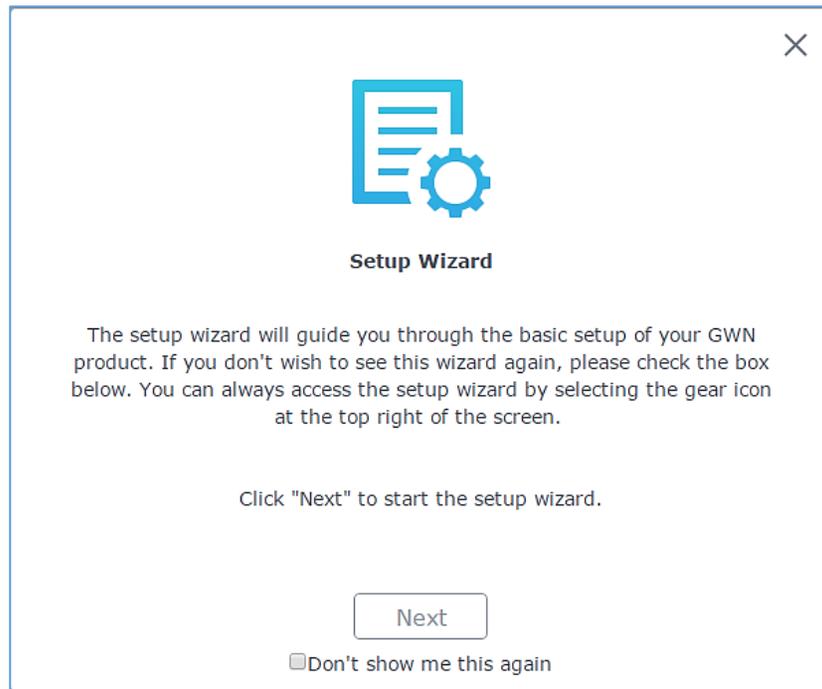


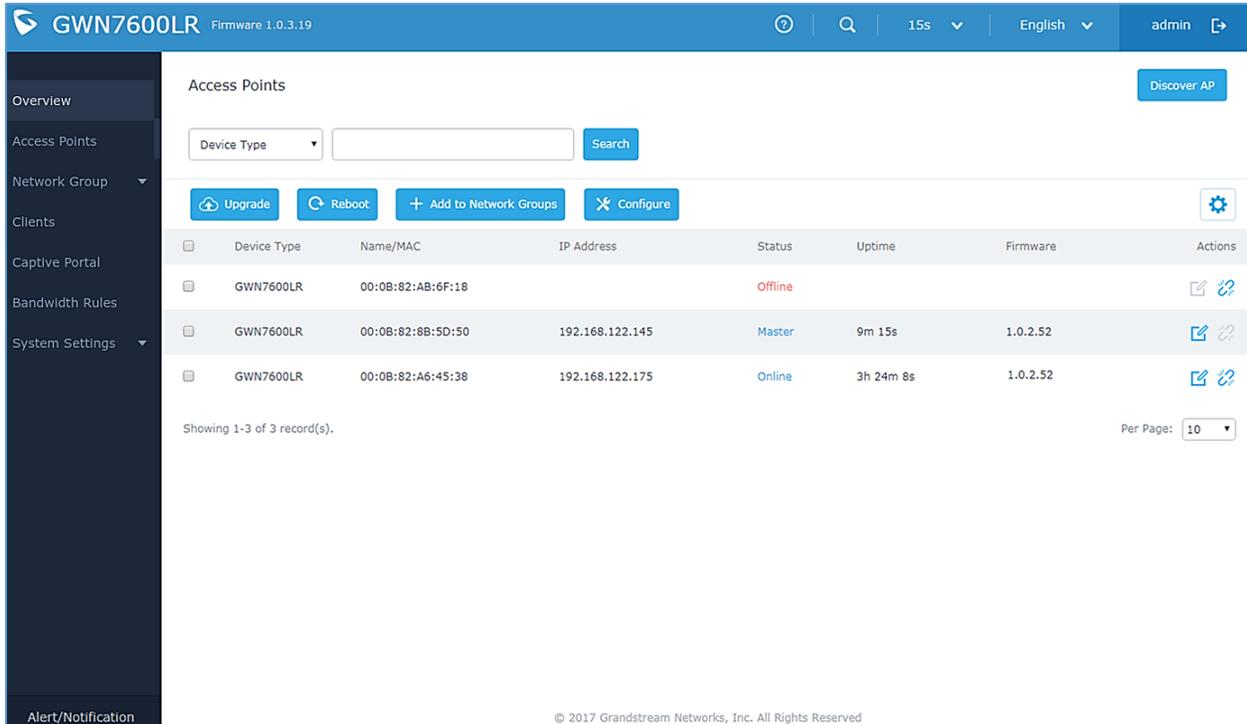
Figure 15: Setup Wizard

Discover and Pair Other GWN7600LR Access Point

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

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





GWN7600LR Firmware 1.0.3.19

Access Points Discover AP

Device Type Search

Upgrade
Reboot
+ Add to Network Groups
Configure
Settings

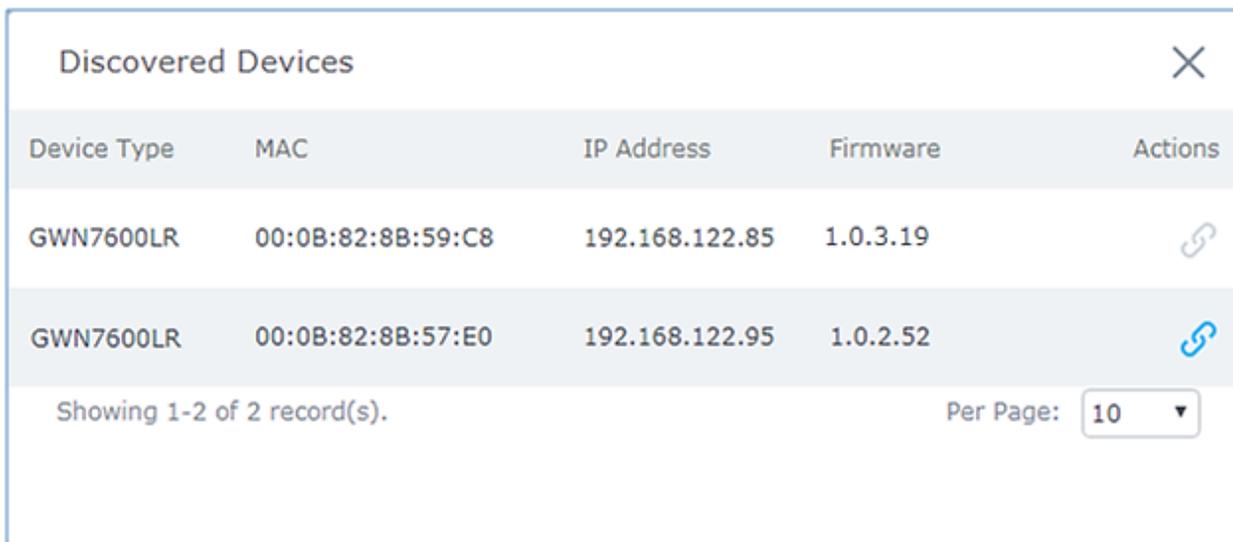
Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7600LR	00:0B:82:AB:6F:18		Offline			
GWN7600LR	00:0B:82:8B:5D:50	192.168.122.145	Master	9m 15s	1.0.2.52	
GWN7600LR	00:0B:82:A6:45:38	192.168.122.175	Online	3h 24m 8s	1.0.2.52	

Showing 1-3 of 3 record(s). Per Page: 10

© 2017 Grandstream Networks, Inc. All Rights Reserved

Figure 16: Discover and Pair GWN7600LR

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



Discovered Devices ✕

Device Type	MAC	IP Address	Firmware	Actions
GWN7600LR	00:0B:82:8B:59:C8	192.168.122.85	1.0.3.19	
GWN7600LR	00:0B:82:8B:57:E0	192.168.122.95	1.0.2.52	

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

Figure 17: Discovered Devices



- Click on Pair  under Actions to pair the discovered access point as slave with the GWN7600LR acting as Master.
- The paired GWN7600LR will appear Online, users can click on  to unpair it.

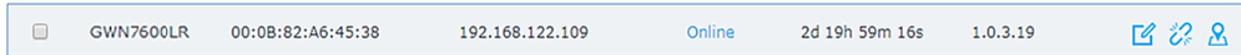


Figure 18: GWN7600LR online

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

Table 6: Device Configuration

Status	Shows the device's status information such as Firmware version, IP Address, Link Speed, Uptime, and Users count via different Radio channels.
Clients	Shows the connected Users to the GWN7600LR access point.
Configuration	<ul style="list-style-type: none"> • Device Name: Set GWN7600LR's name to be shown next to MAC address. • Fixed IP: Used to set a static IP for the GWN7600LR, if checked users will need to set the following: <ul style="list-style-type: none"> ○ IPv4 Address: Enter the IPv4 address to be set as static for the device. ○ IPv4 Subnet Mask: Enter the Subnet Mask. ○ IPv4 Gateway: Enter the Network Gateway's IPv4 Address. ○ Preferred IPv4 DNS: Enter the Primary IPv4 DNS. ○ Alternate IPv4 DNS: Enter the Alternate IPv4 DNS. • Frequency: Set the GWN7600LR's frequency, it can be either 2.4GHz, 5GHz or Dual-band. • Band Steering: When Frequency is set to Dual-Band, users can check this option to enable Band Steering on the Access Point, this will help redirecting clients to a radio band accordingly for efficient use and to benefit from the maximum throughput supported by the client. • Mode: Choose the mode for the frequency band, 802.11n/g/b for 2.4GHz and 802.11ac for 5GHz.



- **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20MHz is suggested in very high-density environment.
- **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be “Secondary Below Primary”, “Primary Below Secondary” or “Auto”.
- **Channel:** Select “Auto” or a specific channel. Default is “Auto”. Note that the proposed channels depend on **Country** Settings under System Settings→Maintenance.
- **Enable Short Guard Interval:** Check to activate this option to increase throughput.
- **Active Spatial Streams:** Choose active spatial stream if Auto, 1 or 2 streams.
- **Radio Power:** Set the Radio Power depending on desired cell size to be broadcasted, three options are available: “Low”, “Medium” or “High”. Default is “High”.
- **Allow Legacy Devices(802.11b):** Check to support 802.11b devices to connect the AP in 802.11n/g mode.
- **Custom Wireless Power(dBm):** allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.

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

AP Locating

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

Failover Master

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



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

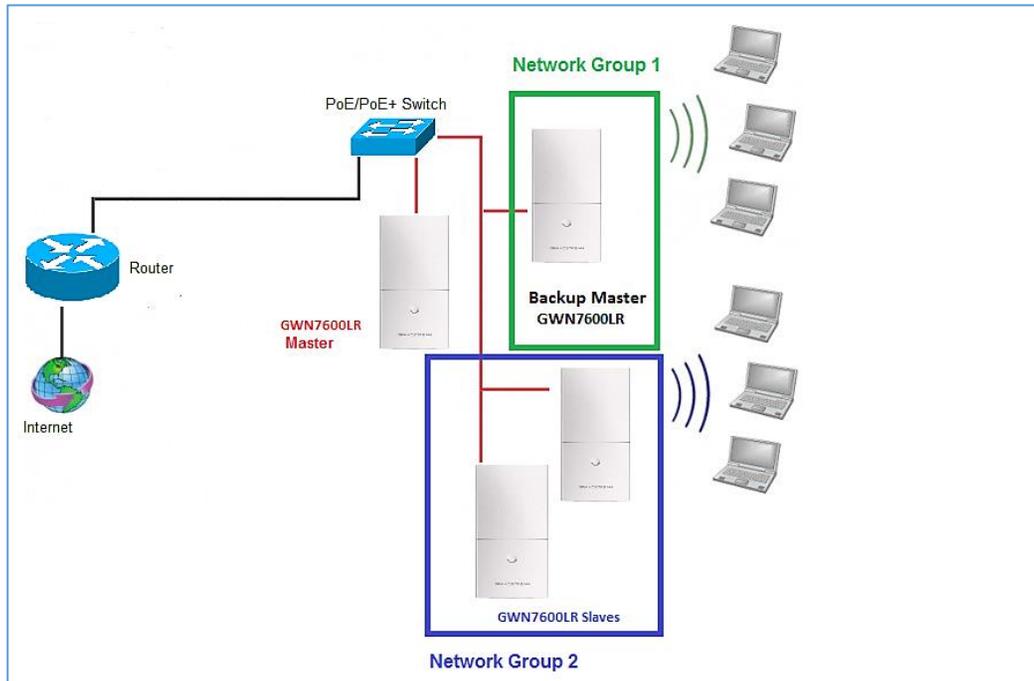


Figure 19: Failover Master

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

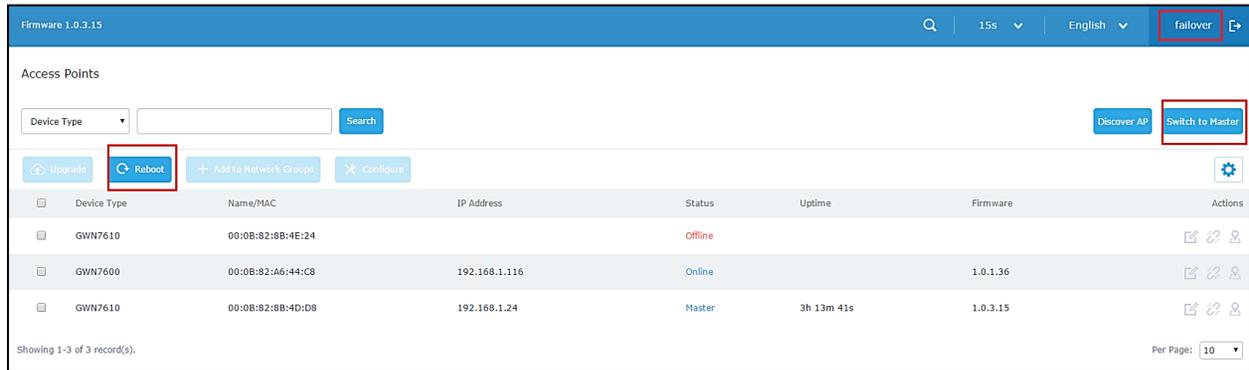
Once failover slave has been selected, the primary master will send the configuration of the network to the failover slave and the slave will start monitoring the status of the primary master to detect any failure for any reason (network connection loss, power outage).

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**





Firmware 1.0.3.15

Access Points

Device Type Search

Discover AP Switch to Master

Upgrade Reboot Add to Network Groups Configure

Device Type	Name/MAC	IP Address	Device Type	Status	Uptime	Firmware	Actions
<input type="checkbox"/>	GWN7610	00:0B:82:8B:4E:24		Offline			
<input type="checkbox"/>	GWN7600	00:0B:82:A6:44:C8	192.168.1.116	Online		1.0.1.36	
<input type="checkbox"/>	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 20: 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.

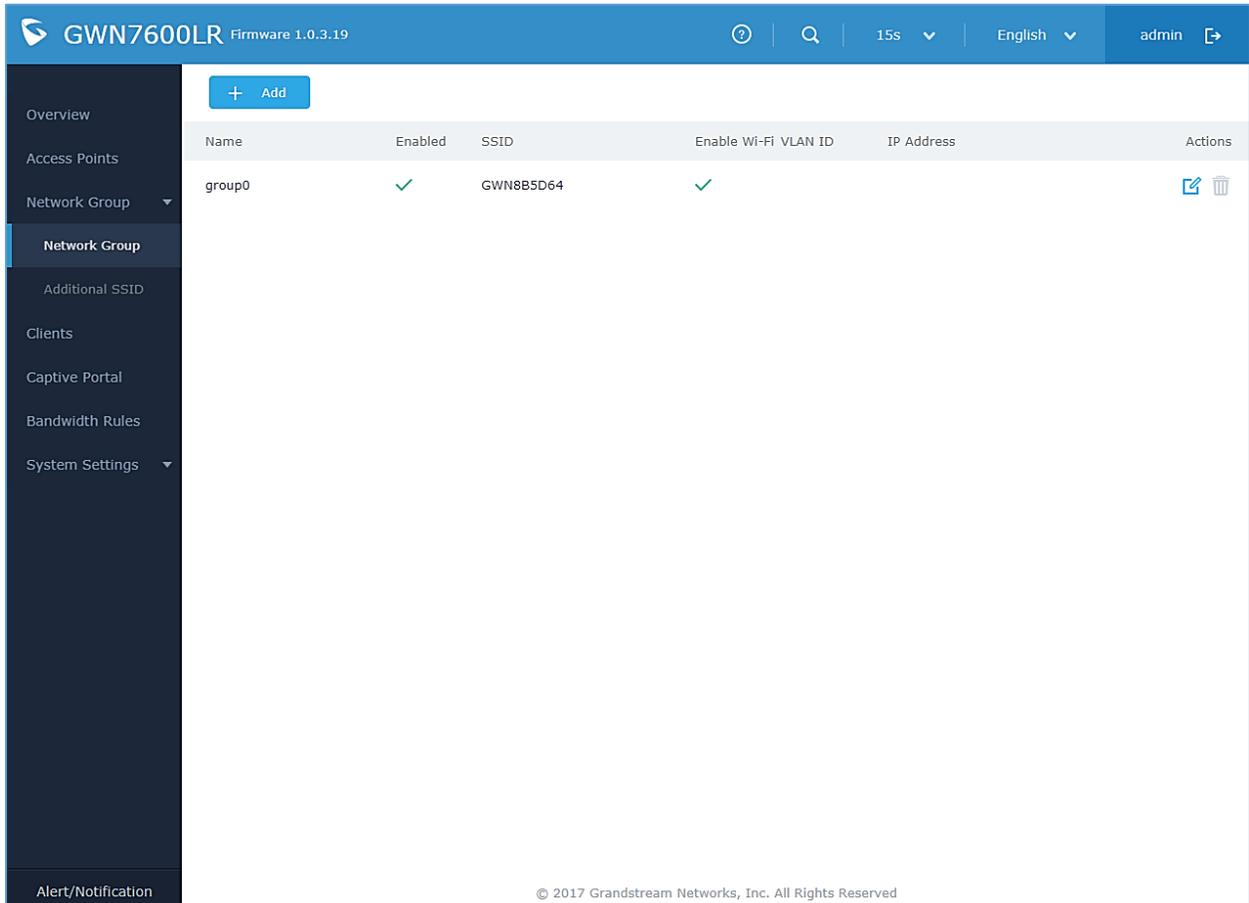
Users also can press on « **Switch to master** » button in order to set the failover slave as the new primary master of the wireless network, once this is done they have full write permission control over the web GUI option as usual.



NETWORK GROUPS

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

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



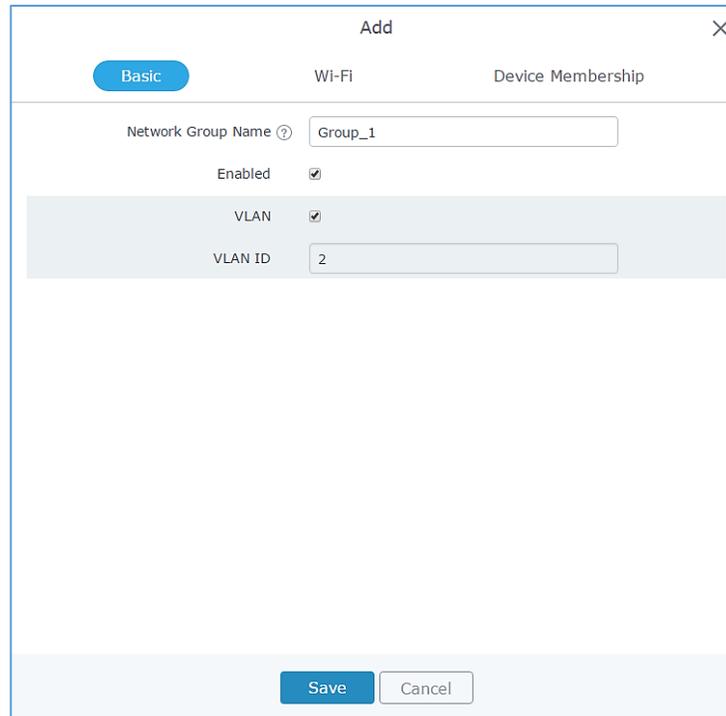
The screenshot shows the GWN7600LR WebGUI interface. The top header displays 'GWN7600LR Firmware 1.0.3.19' and includes a search icon, a timer at '15s', a language dropdown set to 'English', and a user profile for 'admin'. The left sidebar contains navigation links: Overview, Access Points, Network Group (selected), Additional SSID, Clients, Captive Portal, Bandwidth Rules, and System Settings. The main content area features a '+ Add' button and a table with the following data:

Name	Enabled	SSID	Enable Wi-Fi VLAN ID	IP Address	Actions
group0	✓	GWN8B5D64	✓		 

At the bottom of the page, there is a copyright notice: © 2017 Grandstream Networks, Inc. All Rights Reserved.

Figure 21: Network Group

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



Add ×

Basic
Wi-Fi
Device Membership

Network Group Name ?

Enabled

VLAN

VLAN ID

Save
Cancel

Figure 22: Add a New Network Group

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

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

Table 7: Wi-Fi

Field	Description
Enable Wi-Fi	Check to enable Wi-Fi for the network group.
SSID	Set or modify the SSID name.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: <ul style="list-style-type: none"> • Dual-Band • 2.4GHz • 5Ghz
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. If set to 0 the limit is disabled.
Enable Captive Portal	Check to enable/disable captive portal



Captive Portal Policy	Select the captive portal policy already created on the “ CAPTIVE PORTAL ” web page to be used in the created SSID.
Security Mode	<p>Set the security mode for encryption, 5 options are available:</p> <ul style="list-style-type: none"> • WEP 64-bit: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5. • WEP 128-bit: Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13. • WPA/WPA2: Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. • WPA2: Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. Recommended configuration for authentication. • Open: No password is required. Users will be connected without authentication. Not recommended for security reasons
WPA Key Mode	<p>Two modes are available:</p> <ul style="list-style-type: none"> • PSK: Use a pre-shared key to authenticate to the Wi-Fi. • 802.1X: Use a RADIUS server to authenticate to the Wi-Fi.
WPA Encryption Type	<p>Two modes are available:</p> <ul style="list-style-type: none"> • AES: This method changes dynamically the encryption keys making them nearly impossible to circumvent. • AES/TKIP: use both Temporal Key Integrity Protocol and Advanced Encryption Standard for encryption, this provides the most reliable security.
WPA Pre – Shared Key	Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters.
RADIUS Server Address	Enter the RADIUS server IP or FQDN address.
RADIUS Server Port	Enter the RADIUS server port. The default port is 1812.
RADIUS Server Secret	Enter the shared secret between the authenticator and the RADIUS server.
RADIUS Accounting Server Address	Enter the RADIUS Accounting server IP or FQDN address.
RADIUS Accounting Server Port	Enter the RADIUS Accounting server port. The default port is 1813.



RADIUS Accounting Server Secret	Enter the shared secret between the authenticator and the RADIUS Accounting server if configured.
RADIUS NAS ID	Enter the RADIUS NAS ID.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to the zone's Wi-Fi. Default is Disabled.
Enable Dynamic VLAN (beta)	When enabled, clients will be assigned IP address form corresponding VLAN configured on the Radius user profile.
Client Isolation	<p>Client isolation feature blocks any TCP/IP connection between connected clients to GWN7600LR's Wi-Fi access point.</p> <p>Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi.</p> <p>Three modes are available:</p> <ul style="list-style-type: none"> • Internet Mode: Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN7600LR. • Gateway MAC Mode: Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN7600LR access points. • Radio Mode: Wireless clients can access to the internet services, GWN7xxx router and the access points GWN7600LR but they cannot communicate with each other. <p>The default value is "Disabled".</p>
Gateway MAC Address	<p>This field is required when using Client Isolation, so users will not lose access to the Network (usually Internet).</p> <p>Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":".</p> <p>Example: 00:0B:82:8B:4D:D8</p>
RSSI Enabled	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm) .
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is smaller than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1".



Enable Voice Enterprise	<p>Check to enable/disable Voice Enterprise. The roaming time will be reduced once enable voice enterprise.</p> <ul style="list-style-type: none"> • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. <p>Note: 11R is required for enterprise audio feature, 11V and 11K are optional.</p>
Enable 11R	Check to enable 802.11r
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
Upstream Rate	Set the maximum upstream rate
Downstream Rate	Set the maximum downstream rate



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

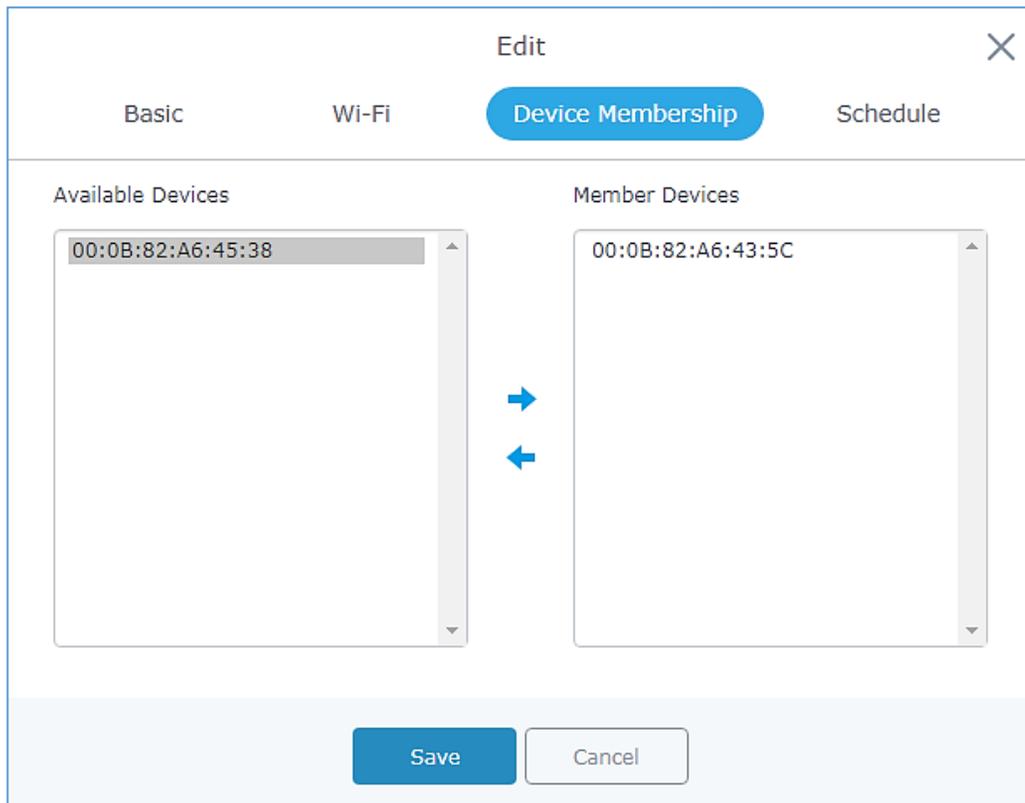


Figure 23: Device Membership

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

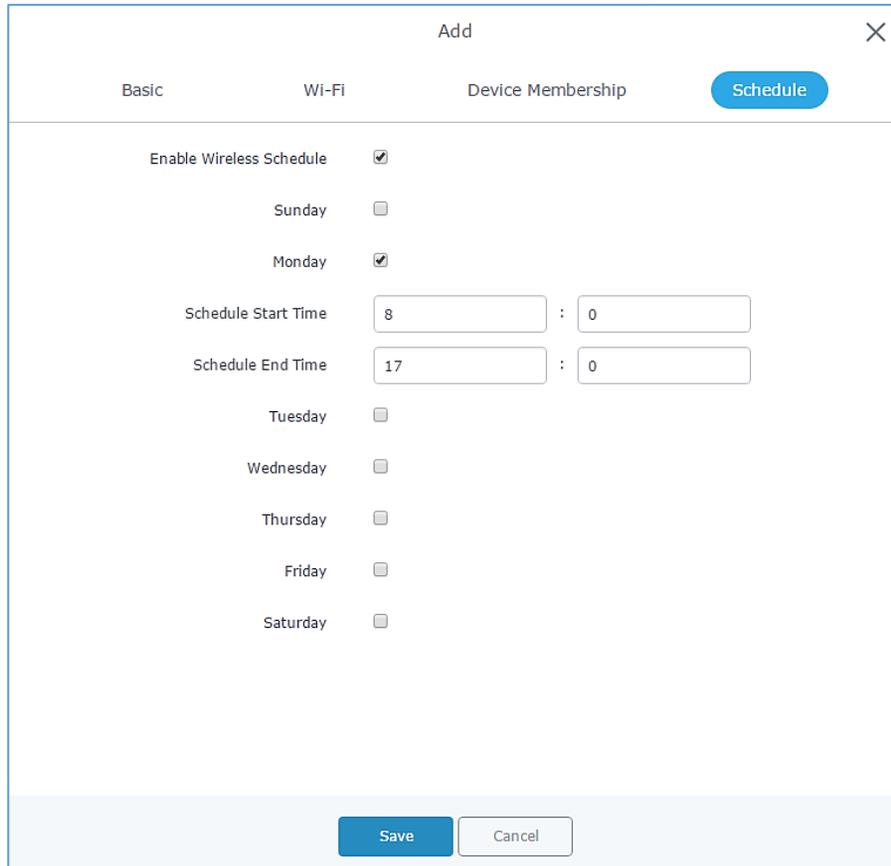
- **Schedule:** Used to schedule the times when the Wi-Fi is ON or OFF.

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

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

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





The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. It has four tabs: "Basic", "Wi-Fi", "Device Membership", and "Schedule". The "Schedule" tab is active and highlighted in blue. The "Schedule" tab contains the following settings:

- Enable Wireless Schedule:
- Sunday:
- Monday:
- Schedule Start Time: 8 : 0
- Schedule End Time: 17 : 0
- Tuesday:
- Wednesday:
- Thursday:
- Friday:
- Saturday:

At the bottom of the dialog are "Save" and "Cancel" buttons.

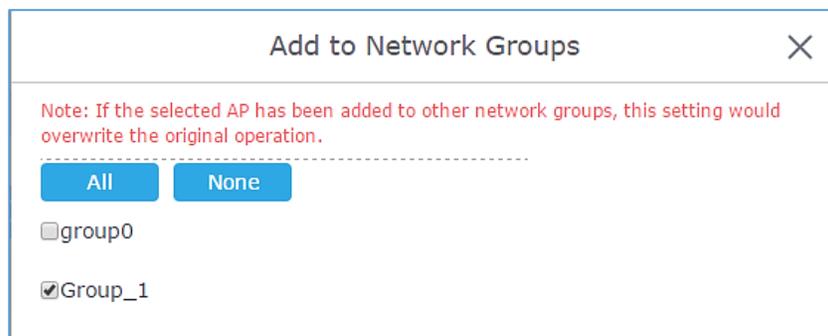
Figure 24: WiFi Schedule

Note:

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

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

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



The screenshot shows a modal window titled "Add to Network Groups" with a close button (X) in the top right corner. It contains a red note: "Note: If the selected AP has been added to other network groups, this setting would overwrite the original operation." Below the note are two buttons: "All" and "None". Underneath, there are two checkboxes: "group0" (unchecked) and "Group_1" (checked).

Figure 25: Add AP to Network Group



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

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

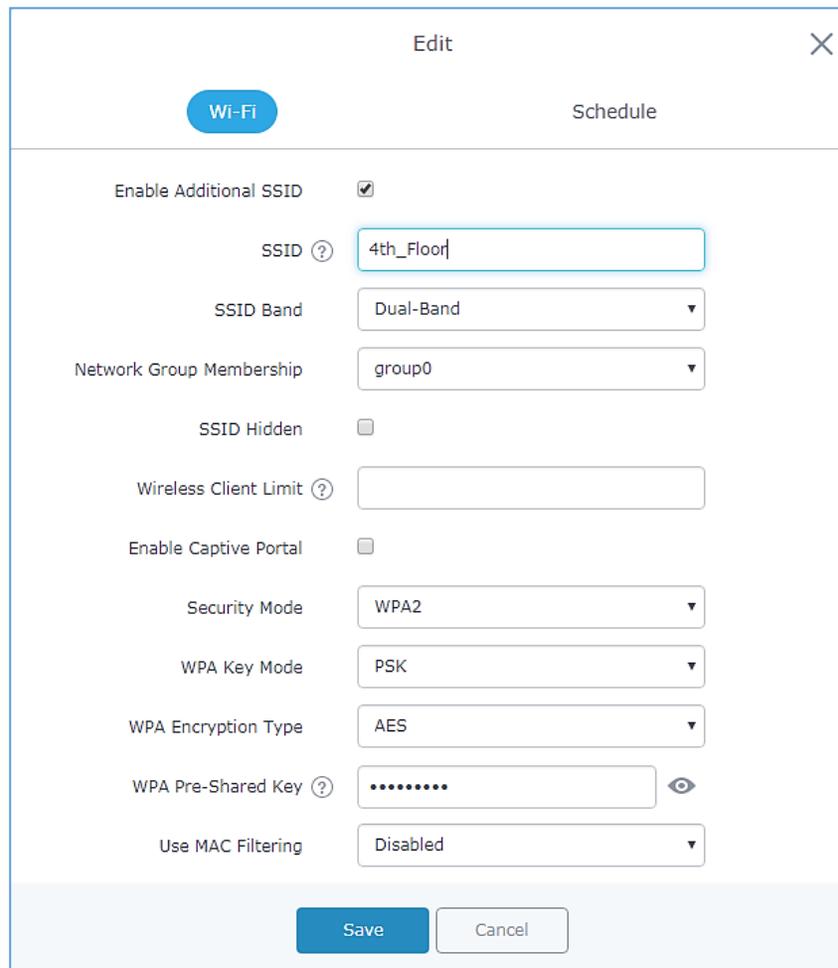


Figure 26: Additional SSID

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

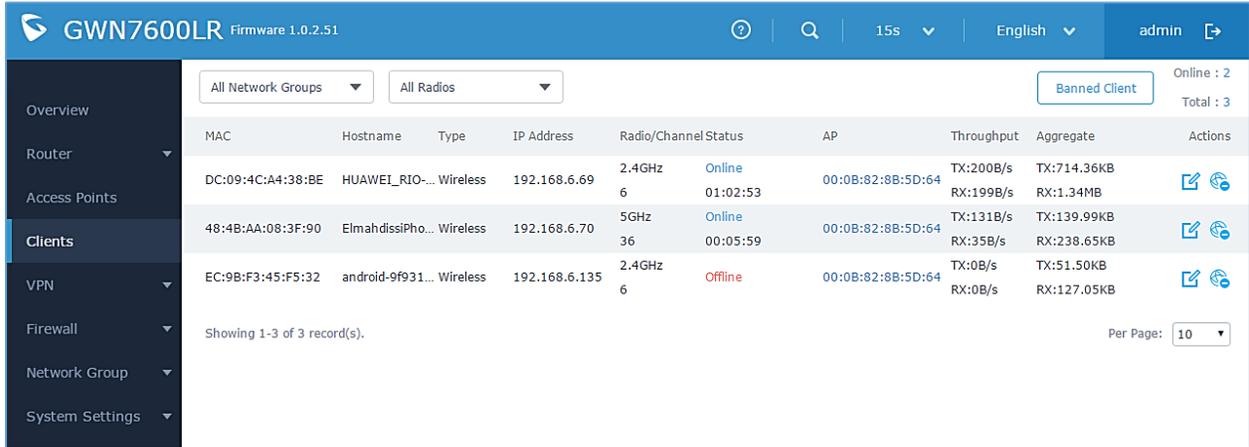
SSID ▲	Enabled	Network Group	Hidden	Security Mode	MAC Filtering	Client Isol...	RSSI	Actions
4th_Floor	✓	group0	✗	WPA/WPA2	Disabled	✗	✗	 

Figure 27: Additional SSID Created

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

CLIENTS CONFIGURATION

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

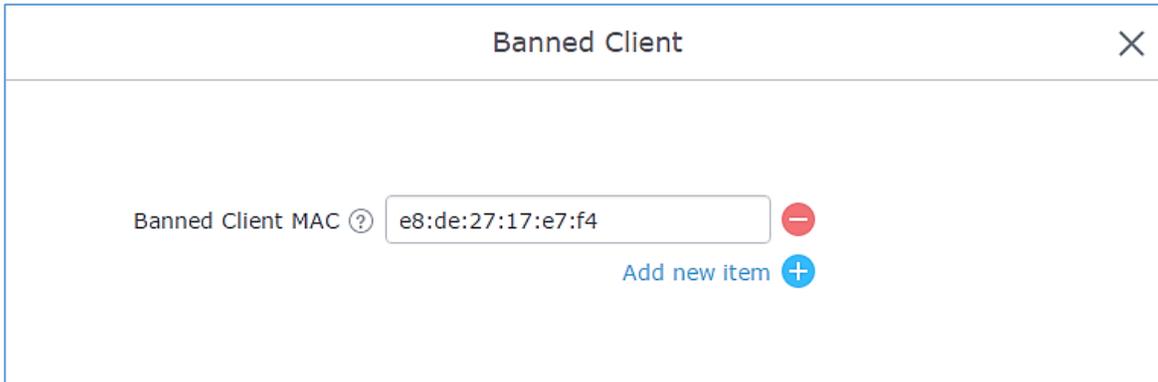


MAC	Hostname	Type	IP Address	Radio/Channel	Status	AP	Throughput	Aggregate	Actions
DC:09:4C:A4:38:BE	HUAWEI_RIO-...	Wireless	192.168.6.69	2.4GHz 6	Online 01:02:53	00:08:82:8B:5D:64	TX:200B/s RX:199B/s	TX:714.36KB RX:1.34MB	
48:4B:AA:08:3F:90	EimahdissiPho...	Wireless	192.168.6.70	5GHz 36	Online 00:05:59	00:08:82:8B:5D:64	TX:131B/s RX:35B/s	TX:139.99KB RX:238.65KB	
EC:9B:F3:45:F5:32	android-9f931...	Wireless	192.168.6.135	2.4GHz 6	Offline	00:08:82:8B:5D:64	TX:0B/s RX:0B/s	TX:51.50KB RX:127.05KB	

Showing 1-3 of 3 record(s). Per Page: 10

Figure 28: Clients

- Click on under Actions to check a client's status and modify basic settings such as Device's Name.
- Click on to block a client's MAC address from connecting to the zone's network group.
- Click on [Banned Client](#) to add or remove a client from banned client list.



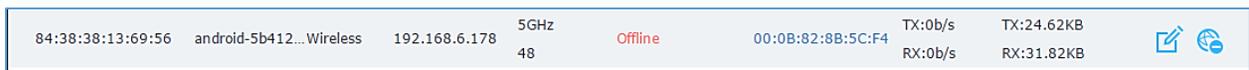
Banned Client

Banned Client MAC

[Add new item](#)

Figure 29: Ban/Unban Client

- Users can scroll down to the down of the client's page to paginate between clients list.



84:38:38:13:69:56	android-5b412...	Wireless	192.168.6.178	5GHz 48	Offline	00:08:82:8B:5C:F4	TX:0b/s RX:0b/s	TX:24.62KB RX:31.82KB	
-------------------	------------------	----------	---------------	------------	---------	-------------------	--------------------	--------------------------	--

Figure 30: Paginate between client's list



LED SCHEDULE

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

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

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

Following options are available:

Table 8: LEDs

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

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



GWN7600 Firmware 1.0.3.19

LEDs

LEDs Always Off

Schedule Start Hour

Schedule Start Minute

Schedule Stop Hour

Schedule Stop Minute

Schedule Weekdays List of Weekdays

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Figure 31: LED Scheduling Sample



CAPTIVE PORTAL

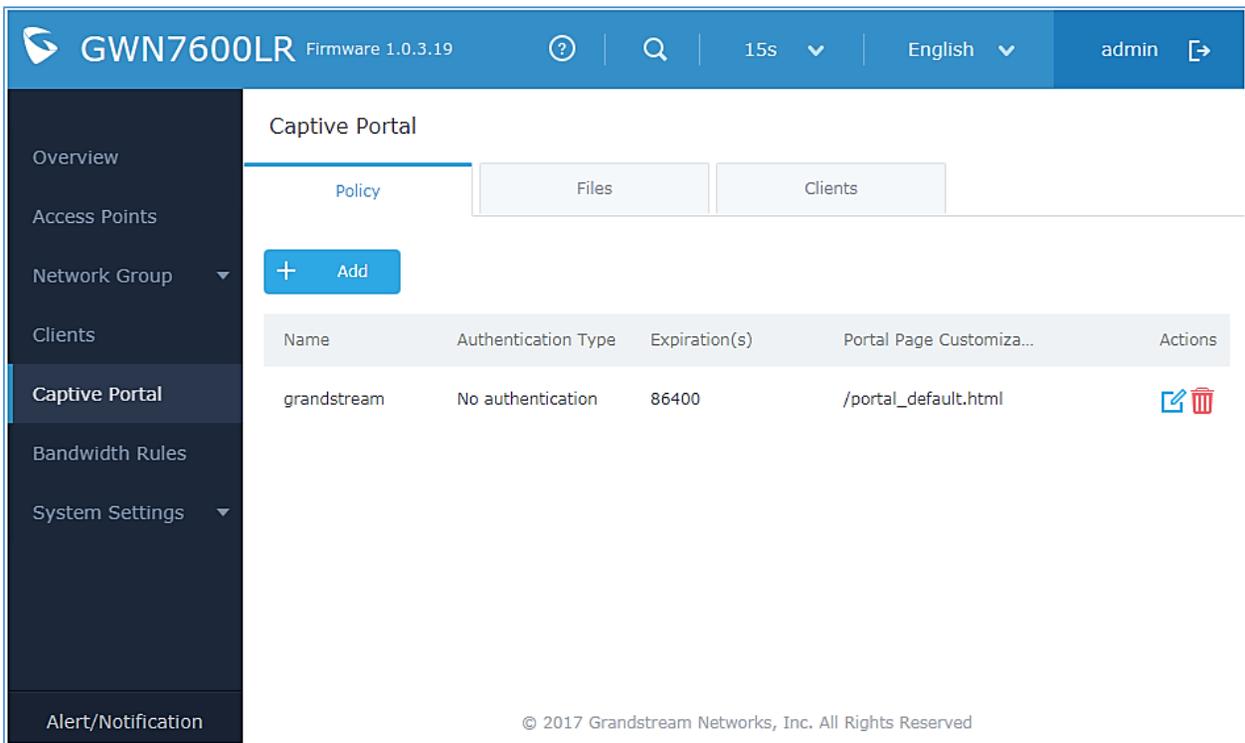
Captive Portal feature on GWN7600LR AP helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet. Once connected to a GWN7600LR AP, Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the GWN7600LR Web page under "Captive Portal".

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

Policy Configuration Page

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



The screenshot shows the 'Captive Portal' configuration page for GWN7600LR. The page has a top navigation bar with 'GWN7600LR Firmware 1.0.3.19', a search icon, '15s', 'English', and 'admin'. A left sidebar contains navigation options: Overview, Access Points, Network Group, Clients, Captive Portal (selected), Bandwidth Rules, System Settings, and Alert/Notification. The main content area has three tabs: Policy (selected), Files, and Clients. Below the tabs is an '+ Add' button. A table lists the policy details:

Name	Authentication Type	Expiration(s)	Portal Page Customiza...	Actions
grandstream	No authentication	86400	/portal_default.html	 

© 2017 Grandstream Networks, Inc. All Rights Reserved

Figure 32: Captive Portal policy

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



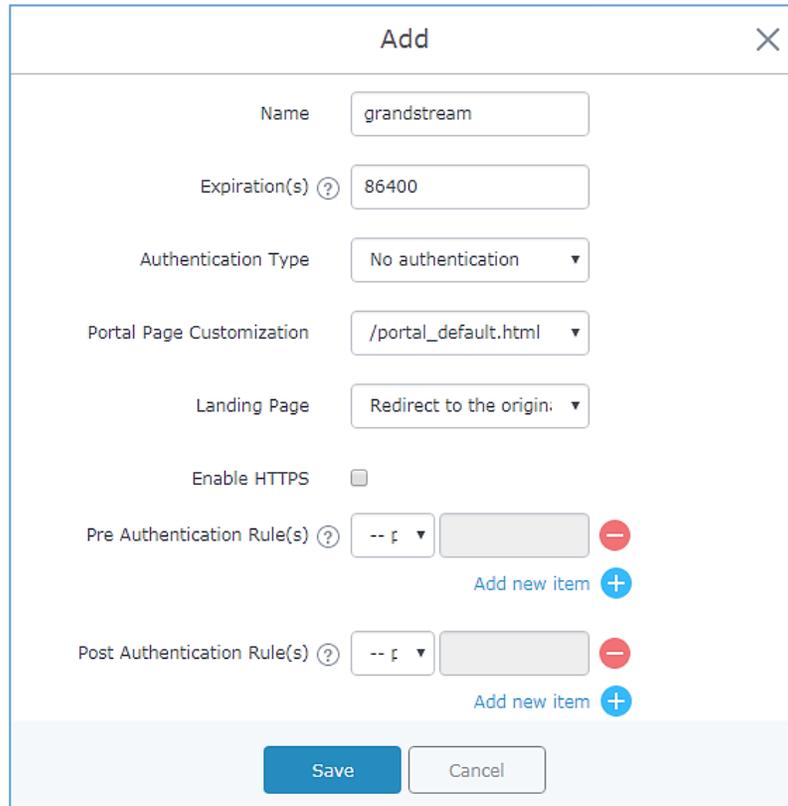


Figure 33: Add a new policy

Below table lists the items policy add page configures.

Table 9: Policy Add

Field	Description
Name	Enter the name of the Captive Portal policy
Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Authentication Type	<p>Select an authentication type for the portal, 3 types are available:</p> <ul style="list-style-type: none"> • No Authentication: When choosing this option, the landing page feature will not provide any type of authentication, instead it will prompt users to accept the license agreement to gain access to internet. • RADIUS Server: Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. • Third party authentication: Allows users to select either the WeChat authentication or Facebook authentication.
Radius Server Address	Enter the IP address or the FQDN of the RADIUS server used to authenticate clients.



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

Note:

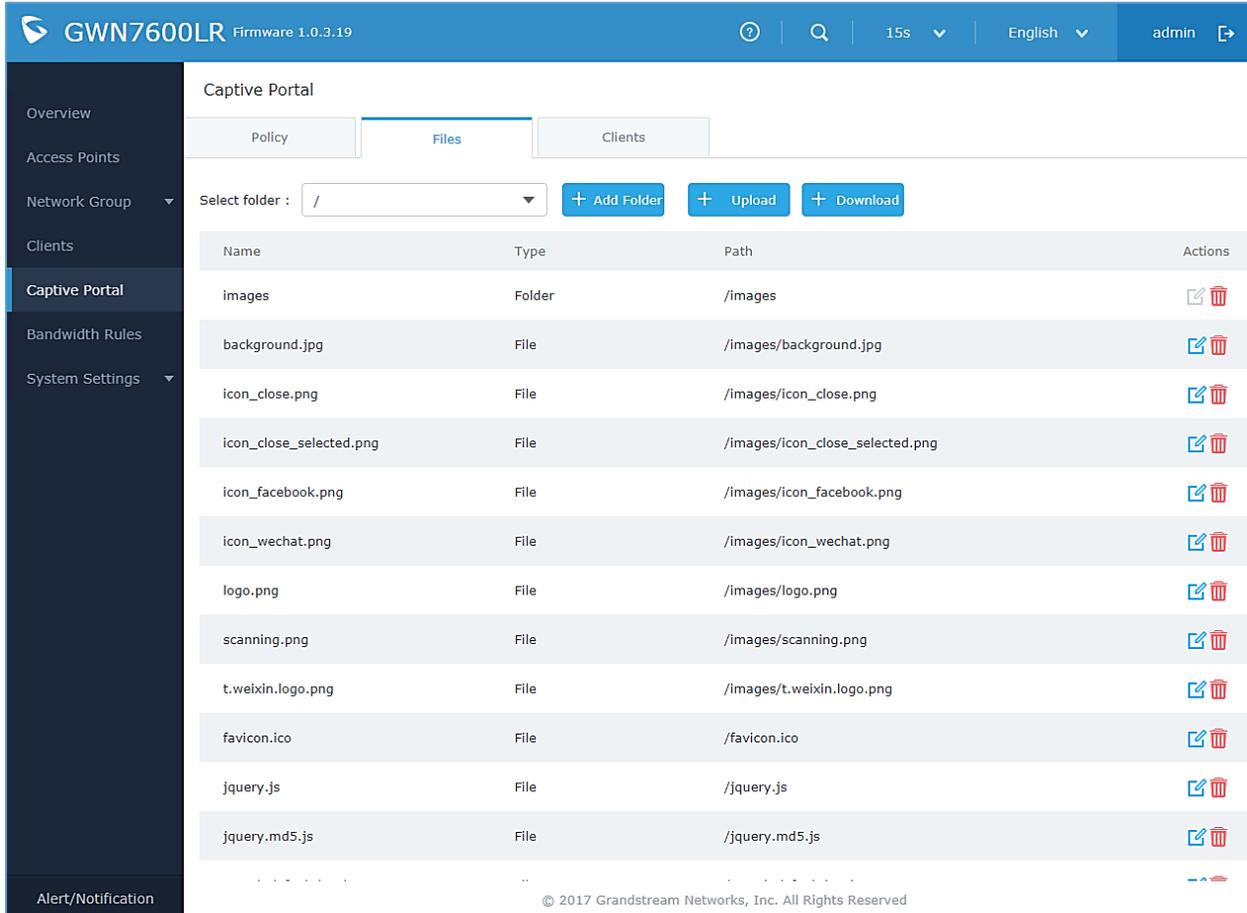
Users could create multiple captive portal instances and assign the desired one for each network Group. As an example, users can create one captive portal for Intranet usage and a second one for public Guest users, after customizing each captive portal separately, you can assign each one to the corresponding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



Files Configuration Page

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

The captive portal uses two HTML pages using authentication scenarios, either **portal_default.html** which doesn't provide authentication, only accepting license agreement, while **portal_pass.html** provides textboxes for authentication, Wired or Wi-Fi clients will be redirected to one of these pages before accessing Internet. The following figure shows **portal_default.html** page:



The screenshot shows the 'Captive Portal' configuration page for 'GWN7600LR' (Firmware 1.0.3.19). The 'Files' tab is active, showing a file manager interface. At the top, there are buttons for '+ Add Folder', '+ Upload', and '+ Download'. Below is a table listing files and folders:

Name	Type	Path	Actions
images	Folder	/images	[Edit] [Delete]
background.jpg	File	/images/background.jpg	[Edit] [Delete]
icon_close.png	File	/images/icon_close.png	[Edit] [Delete]
icon_close_selected.png	File	/images/icon_close_selected.png	[Edit] [Delete]
icon_facebook.png	File	/images/icon_facebook.png	[Edit] [Delete]
icon_wechat.png	File	/images/icon_wechat.png	[Edit] [Delete]
logo.png	File	/images/logo.png	[Edit] [Delete]
scanning.png	File	/images/scanning.png	[Edit] [Delete]
t.weixin.logo.png	File	/images/t.weixin.logo.png	[Edit] [Delete]
favicon.ico	File	/favicon.ico	[Edit] [Delete]
jquery.js	File	/jquery.js	[Edit] [Delete]
jquery.md5.js	File	/jquery.md5.js	[Edit] [Delete]

At the bottom of the page, there is a copyright notice: © 2017 Grandstream Networks, Inc. All Rights Reserved.

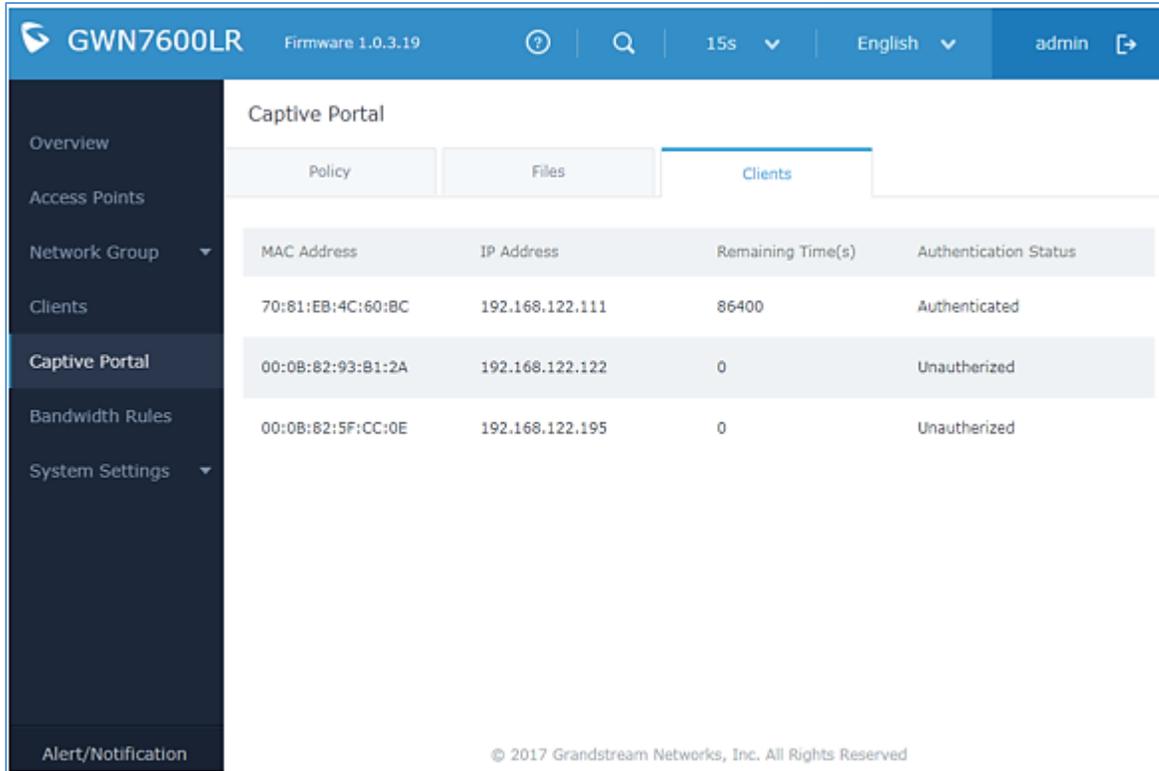
Figure 34: Captive Portal Files

- User can add folder in corresponding folder by selecting the folder and click on .
- Click on  to upload a file from local device.
- Click on  to download the files in Captive Portal folder.
- Click on  to edit the corresponding file, in another word, to replace the file with a new one.
- Click on  to delete the file.



Clients Page

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



The screenshot displays the 'Captive Portal' configuration page for device GWN7600LR. The 'Clients' tab is selected, showing a table of active and unauthorized clients. The table has the following data:

MAC Address	IP Address	Remaining Time(s)	Authentication Status
70:81:EB:4C:60:BC	192.168.122.111	86400	Authenticated
00:0B:82:93:B1:2A	192.168.122.122	0	Unauthorized
00:0B:82:5F:CC:0E	192.168.122.195	0	Unauthorized

© 2017 Grandstream Networks, Inc. All Rights Reserved

Figure 35: Captive Portal Clients

BANDWIDTH RULES

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

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

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

Table 10: Bandwidth Rules

Field	Description
Type	Choose the type of rule to be applied on bandwidth utilization from the dropdown list, three options are available: <ul style="list-style-type: none"> 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	<input type="text" value="MAC"/>	
MAC	<input type="text" value="00:0b:82:15:af:19"/>	
Network Group	<input type="text" value="group0"/>	
Upstream Rate	<input type="text" value="10"/>	<input type="text" value="Mbps"/>
Downstream Rate	<input type="text" value="75"/>	<input type="text" value="Mbps"/>

Figure 36: MAC Address Bandwidth rule

The following figure shows examples of bandwidth rules:

+ Add					
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 37: Bandwidth Rules

Note:

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

Per-SSID

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

Per-Client

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

SYSTEM SETTINGS

Maintenance

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

Basic

Basic page allows Country and Time configuration.

Table 11: Basic

Field	Description
Country	Select the country from the drop-down list. This can affect the number of channels depending on the country standards.
Time Zone	Configure time zone for the GWN7600LR. Make sure to reboot the device to take effect.
NTP Server	Configure the IP address or URL of the NTP server. The device will obtain the date and time from the configured server.
Date Display Format	Change the Date Display Format, three options are possible YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY

Upgrade

The Upgrade Web page allows upgrade related configuration.

Table 12: Upgrade

Field	Description
Authenticate Config File	Authenticate configuration file before acceptance. Default is disabled.
XML Config File Password	Enter the password for encrypting the XML configuration file using OpenSSL. The password is used to decrypt the XML configuration file if it is encrypted via OpenSSL.
Upgrade Via	Specify uploading method for firmware and configuration. 3 options are available: HTTP, HTTPS and TFTP.
Firmware Server	Configure the IP address or URL for the firmware upgrade server.
Config Server	Configure the IP address or URL for the configuration file server.
Check/Download New Firmware and config at Boot	Choose whether to enable or disable automatic upgrade and provisioning after reboot. Default is disabled.
Allow DHCP options 66 and 43 override	Configure whether to allow DHCP options 66 and 63 to override the upgrade and provisioning setting.
Automatic Upgrade	Specify the time to check for firmware upgrade (in minutes).



Upgrade Now	Click on Upgrade, to launch firmware/config file provisioning. Please make sure to Save and Apply changes before clicking on Upgrade.
Download Configuration	Click on Download to download the device's configuration file.
Upload Configuration	Select a compressed config file to restore the device previous configuration, after upload successfully, the device will reboot automatically.
Reboot	Click on Reboot button to reboot the device.
Factory Reset	Click on Reset to restore the GWN7600LR to factory default settings

Access

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

Table 13: Access

Field	Description
Current Administrator Password	Enter the current administrator password
New Administrator Password	Change the current password. This field is case sensitive with a maximum length of 32 characters.
Confirm New Administrator Password	Enter the new administrator password one more time to confirm.
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 14: Syslog

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



Debug

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

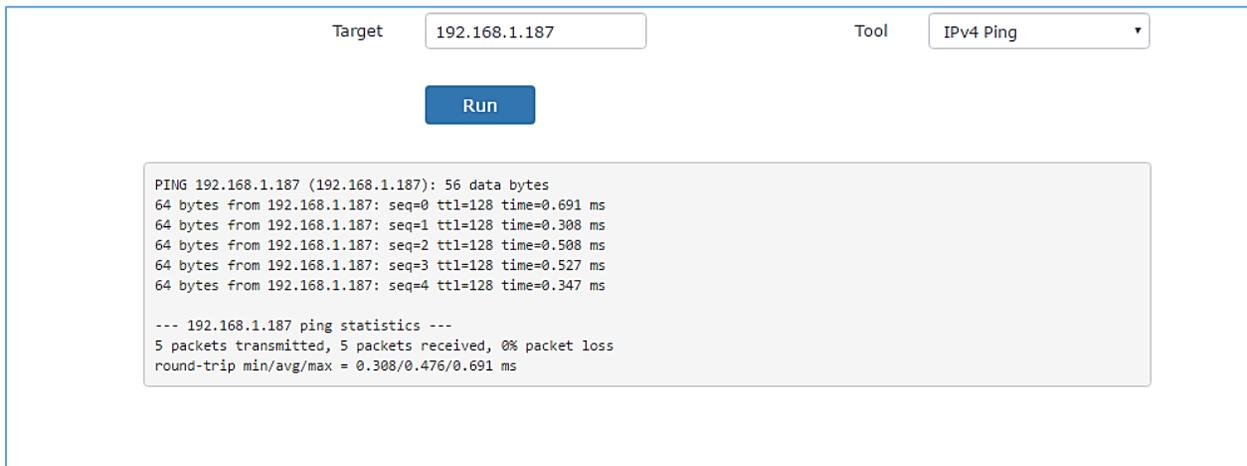
Core Files

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

Ping/Traceroute

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

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



```
Target 192.168.1.187 Tool IPv4 Ping
Run
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 38: IP Ping

- Next to **Tool** choose from the dropdown menu:
 - IPv4 Ping for an IPv4 Ping test to Target
 - IPv6 Ping for an IPv6 Ping test to Target
 - IPv4 Traceroute for an IPv4 Traceroute to Target
 - IPv6 Traceroute for an IPv6 Traceroute to Target
- Type in the destination's IP address in **Target** field.
- Click on **Run**.



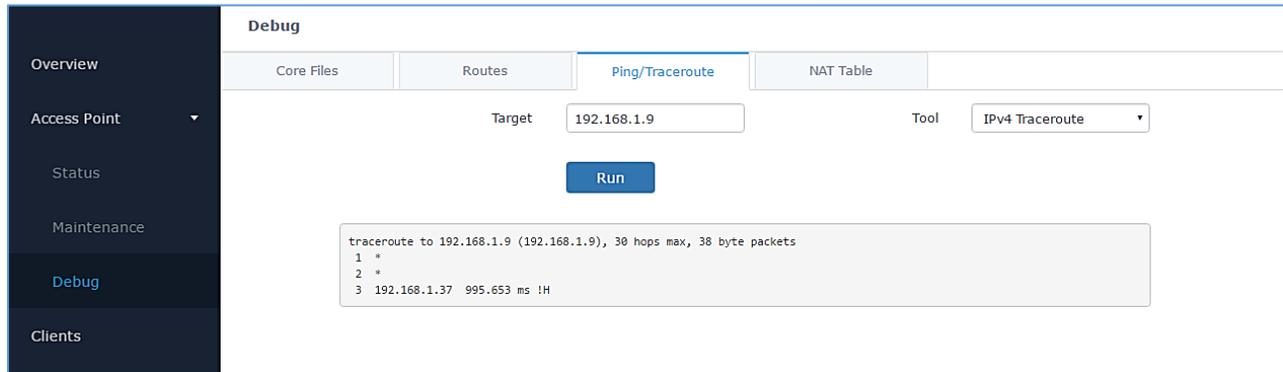


Figure 39: IP Traceroute

Syslog

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

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

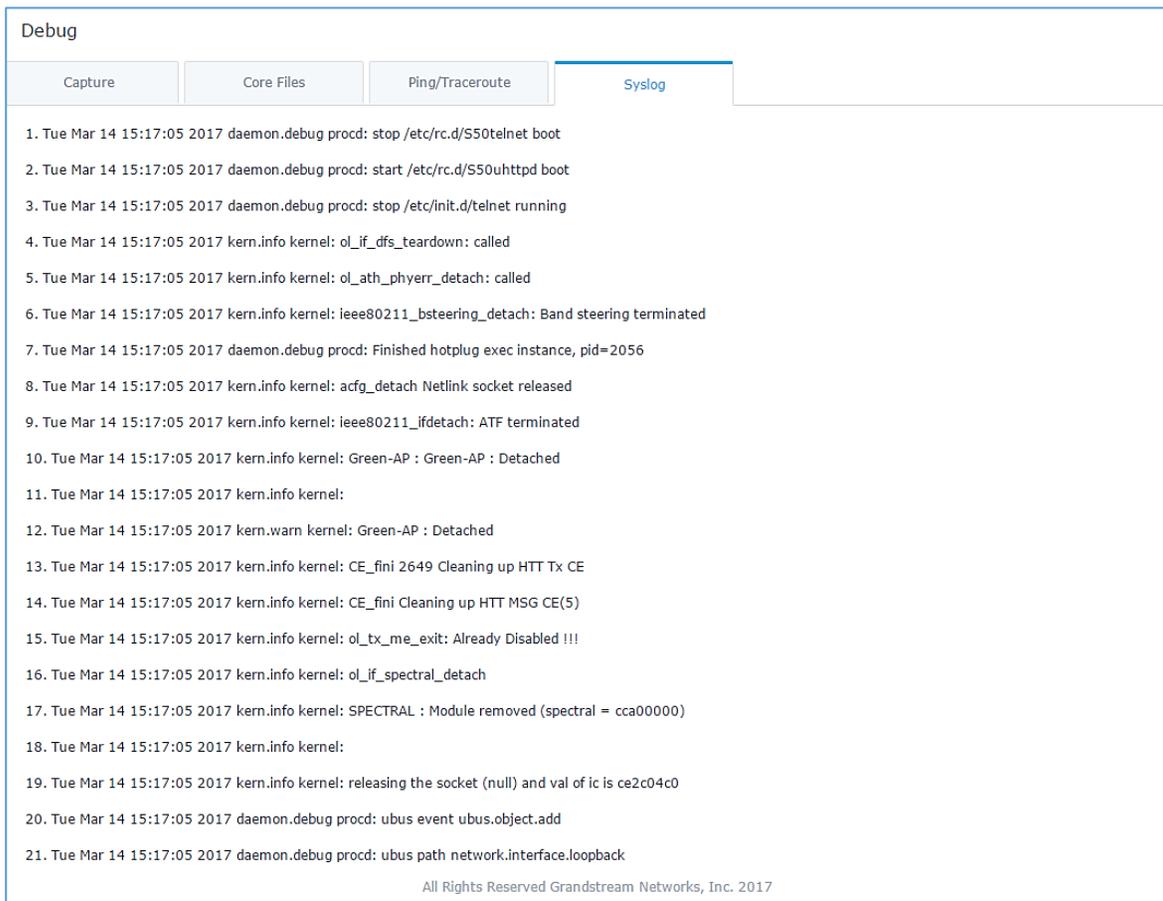


Figure 40: Syslog



UPGRADING AND PROVISIONING

Upgrading Firmware

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

Upgrading via Web GUI

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

Examples of valid URLs:

firmware.grandstream.com/BETA
 192.168.5.87

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

Table 15: Network Upgrade Configuration

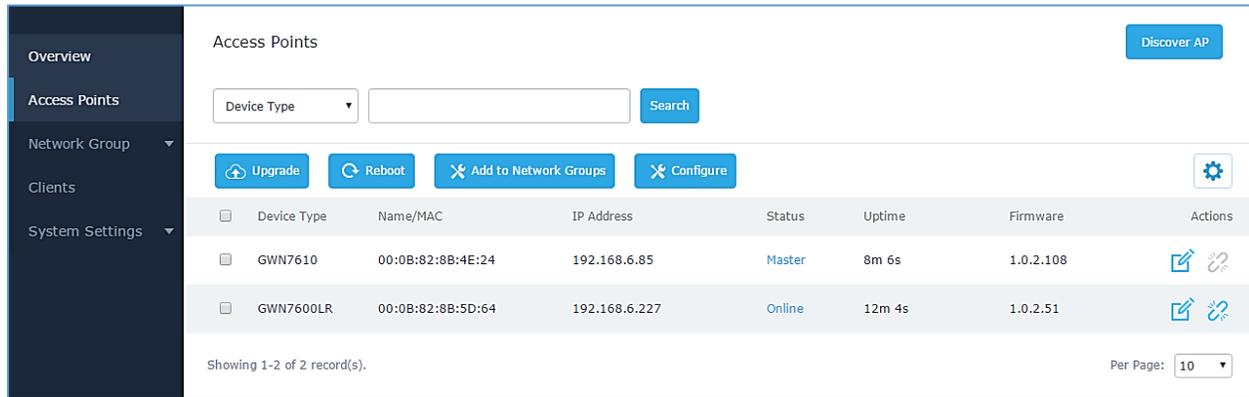
Upgrade Via	Allow users to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
Firmware Server	Define the server path for the firmware server.
Check Update on Boot	Allows the device to check if there is a firmware from the configured firmware server at boot.
Automatic Upgrade check interval(m)	Set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

Upgrading Slave Access Points.

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

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





Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7610	00:0B:82:8B:4E:24	192.168.6.85	Master	8m 6s	1.0.2.108	[Upgrade] [Reboot]
GWN7600LR	00:0B:82:8B:5D:64	192.168.6.227	Online	12m 4s	1.0.2.51	[Upgrade] [Reboot]

Figure 41: Access Points

Make sure that firmware server path is set correctly under Maintenance, and click on  to upgrade all selected access points.

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

 **Note:**

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

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

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

Instructions for local firmware upgrade via TFTP:

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



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

Provisioning and backup

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

Download Configuration

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

Click on  to download locally the configuration file.

Configuration Server

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

Reset and reboot

Administrators could perform a reboot and reset the device to factory functions under **Web GUI→System**

Settings→Maintenance→Upgrade by clicking on  button.

 Will restore all the GWN7600LR itself to factory settings.

EXPERIENCING THE GWN7600LR WIRELESS ACCESS POINT

Please visit our website: <http://www.grandstream.com> to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our [product related documentation](#), [FAQs](#) and [User and Developer Forum](#) for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

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

