# GWN7000 Firmware Release Note

## IMPORTANT UPGRADING NOTE

- **Important security fix on 1.0.6.32. Please upgrade to this or newer version.**
- **If your GWN7000 has firmware version lower than 1.0.2.62 (1.0.2.62 not included), please refer to the beta forum upgrade guide or contact tech support for upgrading assistance.**
- **Downgrading behavior from 1.0.6.28 to 1.0.4.23 or previous firmware will lead to an auto factory reset of GWN7000.**

# Table of Content

# FIRMWARE VERSION 1.0.9.6

## PRODUCT NAME

GWN7000

## DATE

7/6/2020

## FIRMWARE FILE INFORMATION

- GWN7000 Firmware file name: gwn7000fw.bin

  MD5 checksum: 3f2f152bec5ca86d256ff769ce86baf2

## ENHANCEMENT/CHANGES

- Fixed PPPoE WAN slowness issue.
- Fixed an issue of admin to get root shell access by remote command injection.

# FIRMWARE VERSION 1.0.9.5

## PRODUCT NAME

GWN7000

## DATE

3/30/2020

## FIRMWARE FILE INFORMATION

- GWN7000 Firmware file name: gwn7000fw.bin

  MD5 checksum: a6bf16b9596b4f34b854b5291c06a43c

## ENHANCEMENT/CHANGES

- Added support for TLS 1.2

# FIRMWARE VERSION 1.0.9.4

## PRODUCT NAME

GWN7000

## DATE

7/24/2019

## FIRMWARE FILE INFORMATION

- GWN7000 Firmware file name: gwn7000fw.bin

  MD5 checksum: 9b996ed14fcf7171f75c238d363db1da

## ENHANCEMENT/CHANGES

- Added configuration support of **Mesh** for all GWN AP models
- Added configuration support of **External Captive Portal Support** as **Linkyfi**, **Purple**, and **Universal Platform**.
- Enhanced **WiFi Service** by adding configurable options of **Beacon Interval**, **DTIM Period**, and **Convert IP multicast to unicast**.
- Enhanced **Captive Portal features** by adding configurations as **Failsafe mode**, **Byte limit**, **Daily limit**, and **Force To Follow** in Twitter authentication.
- Added configuration support of **ARP Proxy**
- Enhanced **Bandwidth Rules** by adding option to **limit bandwidth Per-Client**
- Added feature of **Client Negotiate Speed Display**
- Added feature of **Slave AP Transfer**

## NEW FEATURES OVERVIEW

All new features and enhancement added in this version matches the local AP master features released from 1.0.7.x to 1.0.9.x. For NEW FEATURE OVERVIEW, please refer to any GWN AP model's release journal as Release_Note_*model_version*.pdf at http://www.grandstream.com/support/firmware. For example, Release_Note_GWN7600_1.0.9.13.pdf.

# FIRMWARE VERSION 1.0.6.32

## PRODUCT NAME

GWN7000

## DATE

2/27/2019

## FIRMWARE FILE INFORMATION

- GWN7000 Firmware file name: gwn7000fw.bin

  MD5 checksum:    66aff44f0ca87b10a615e07510b64d3a

## IMPORTANT UPGRADING NOTE

- Same upgrade notes for upgrading from 1.0.4.x to 1.0.6.28 applies to 1.0.6.32.
- Important security fix applied on 1.0.6.32. Please upgrade.

## ENHANCEMENT/CHANGES

- Fixed security vulnerability to remote code execution by exploiting a POST AUTH Command
- Improved PPPoE WAN speed upon 1.0.6.28

# FIRMWARE VERSION 1.0.6.28

## PRODUCT NAME

GWN7000

## DATE

8/22/2018

## IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.71 or higher.
- Downgrading behavior from 1.0.6.28 to 1.0.4.23 or previous firmware will lead to an auto factory reset of GWN7000.
- Please only use GWN Access Point firmware version 1.0.6.x with this 1.0.6.28 GWN7000 firmware for master and slave pairing.

## ENHANCEMENT/CHANGES

- **Enhanced QoS** features
- Added feature of **Policy Routing**
- Added support of **GRE Tunnels**
- Added support of **IPsec Tunnels**
- Added feature of **Website Blocking**
- Added **WAN interfaces** options for Static Route
- Added feature of **Feature Scheduling**
- Added **NET port as WAN** feature
- Added **WAN/LAN interfaces status on Overview page** on Overview page.
- **Network group** (pre-1.0.4.23 and 1.0.4.23 fw configuration) is split into **LAN** and **SSID** configuration.
- Added feature of **Switch Port LAN Mapping**

- Added feature of **Static DHCP**
- Added **Alert/Email notification of WAN Internet access interruption**
- Added **interface option** in **Ping/Trace Route**
- Changed WAN port VLAN Tag range from 5-4093 to **2-4093**
- Added **System Date and Time** on page header
- Added **Static IP reservation on OpenVPN client**
- Added option to enable/disable **DNS Rebind Attack Protection**
- Added feature of Access Point firmware **Sequential Upgrade**

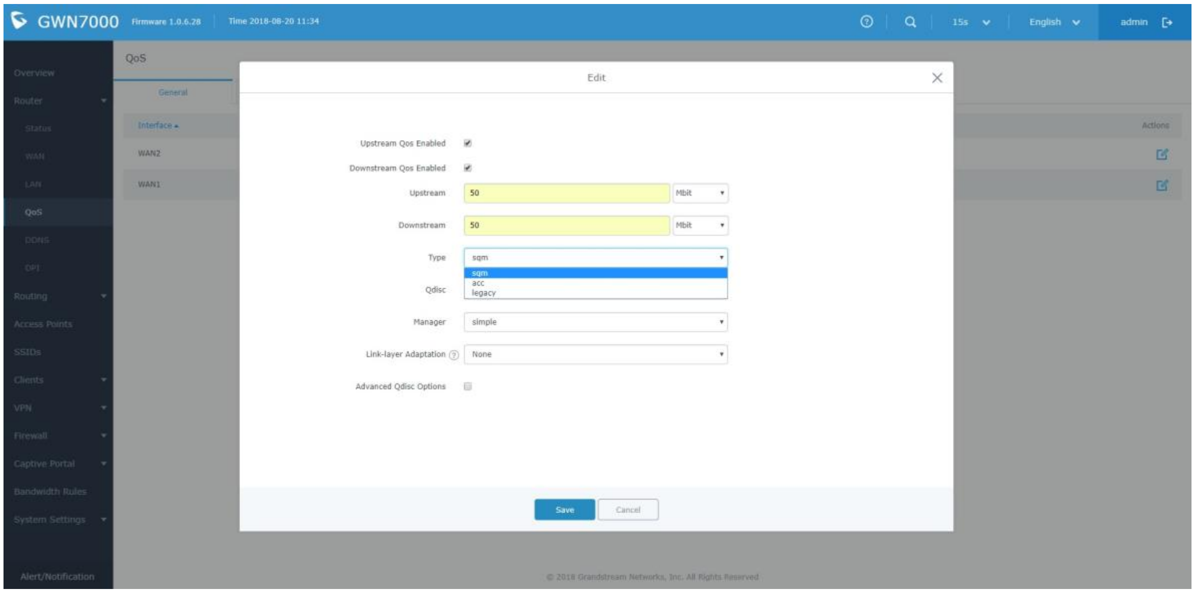
## KNOWN ISSUE

- After upgraded from 1.0.4.23 to 1.0.6.23, the old static route does not take effect in routing table.
- When WAN interfaces, including regular WAN and NET port as WAN, are configured with same VLAN Tag, IP routing will be abnormal.
- After blocking wireless client, blocked client will be displayed as wired in the clients list instead of showing in the Blocked client list.
- OpenVPN Server mode doesn’t push route in PSK mode
- Unrecognized traffic may be classified as HTTPS in Application Traffic.
- Client's name does not display in list of top clients of overview page.

# NEW FEATURES OVERVIEW

- **Enhanced QoS**

QoS Enhancement includes 2 new types of QoS:



Upstream Qos Enabled ☑

Downstream Qos Enabled ☑

Upstream: 50 Mbit

Downstream: 50 Mbit

Type: sqm

Qdisc

Manager: simple

Link-layer Adaptation: None

Advanced Qdisc Options ☐

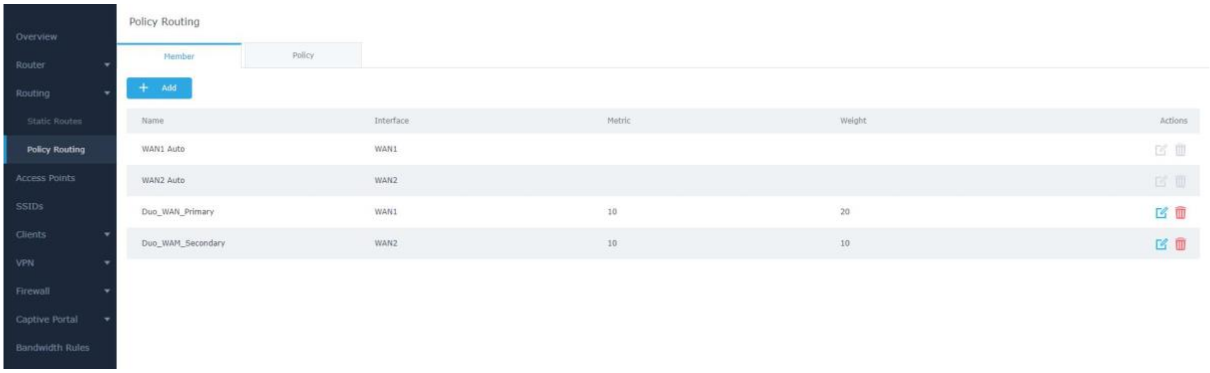
**Adaptive Congestion Control (acc)**: ACC feature combines the power of our original class based QoS, while adding true ingress shaping, and reducing the configuration difficulty. Traditional QoS systems rely on the actual bandwidth provided by your ISP to remain constant; they also require you to set the link rate below what the ISP provisions your link, which leaves the link underutilized. The ACC QoS solves this problem. The ACC QoS also features the anti-bufferbloat and flow fairness of our Smart Queue QoS. Beyond that, the new QoS allows for defining classes so that flows that are latency sensitive and/or need a minimum amount of bandwidth can be placed into; this is extremely useful for VoIP traffic.

**Smart Queue Management (sqm)**: SQM will add multiple simple to configure, but extremely effective forms of QoS that reduces Buffer Bloat and keeps latency at acceptable levels.

- **Policy Routing**

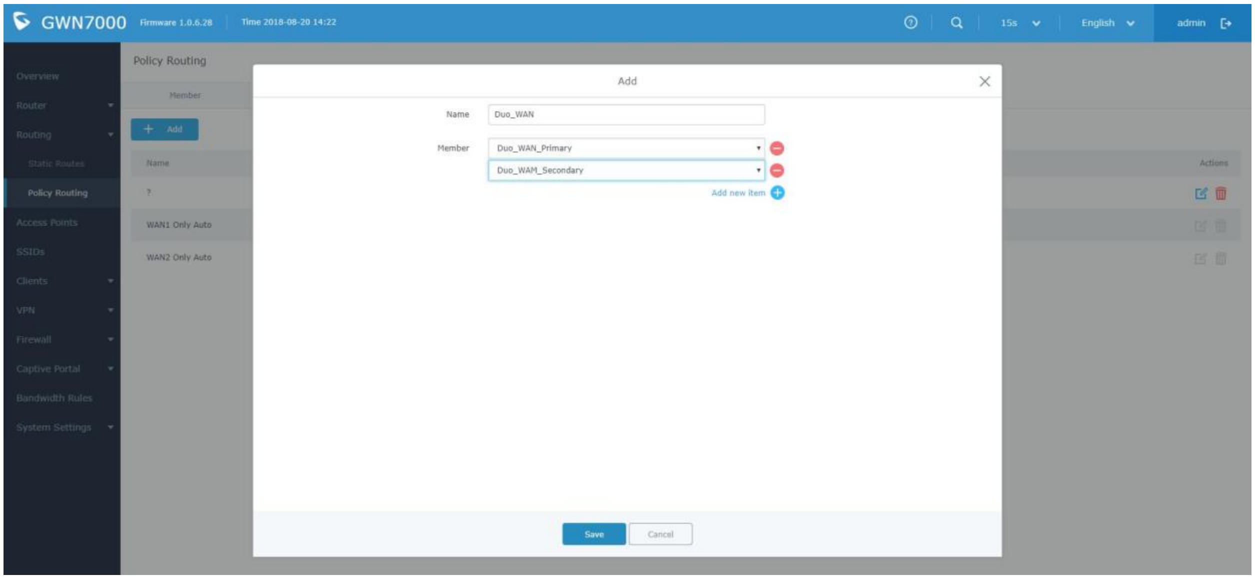
This feature configuration is located at left side menu bar **Routing→Policy Routing.**

To use policy routing. You can create members with interface metric and weight.



| Name | Interface | Metric | Weight | Actions |
|---|---|---|---|---|
| WAN1 Auto | WAN1 | | | |
| WAN2 Auto | WAN2 | | | |
| Duo_WAN_Primary | WAN1 | 10 | 20 | |
| Duo_WAM_Secondary | WAN2 | 10 | 10 | |

Then you can create policies with members added in.



Name: Duo_WAN

Member: Duo_WAN_Primary
Duo_WAM_Secondary

Members within one policy with a lower metric have precedence over higher metric members. Members with same metric will distribute load based on this weight value.

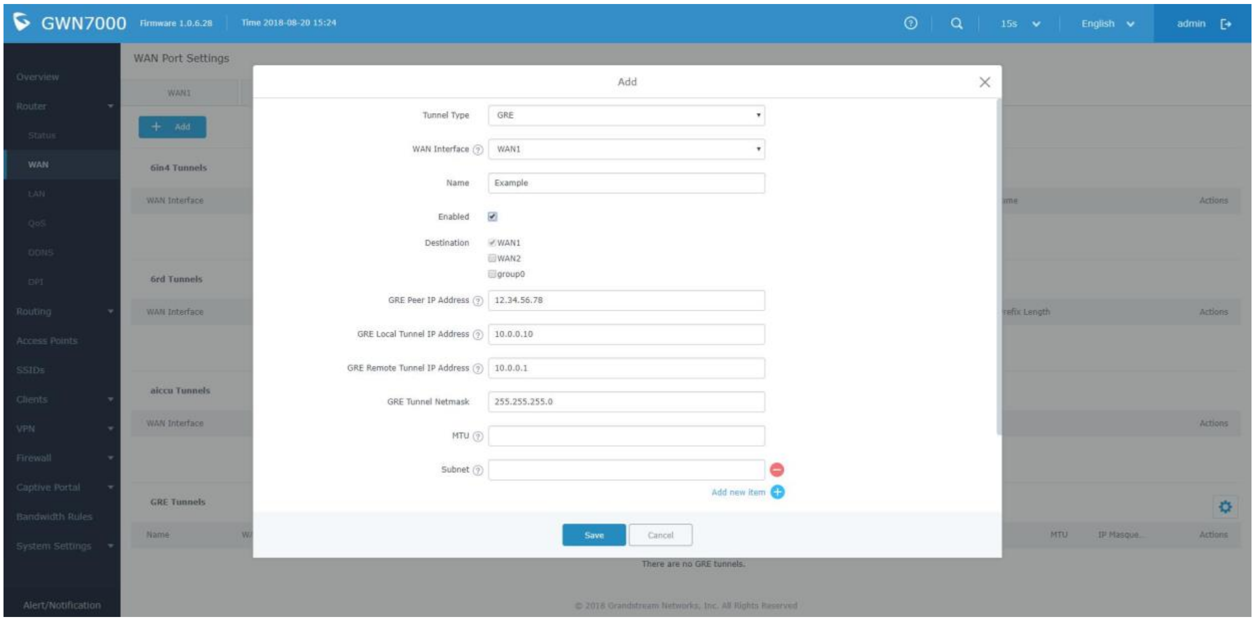
- **Website Blocking**

The Blackhole DNS feature allows the system administrator to download filter lists or create their own filter lists to block DNS queries to URLs or domains. These lists can be used to block adware sites, malware sites, and can be used to block popular social media websites. The administrator can apply this feature to any combination of zones or clients.

Feature configurations are available at **System Settings→Website Blocking**.

- **GRE Tunnels**

**GRE Tunnels'** configuration is located at leftside menu bar **Router→WAN→Tunnel.**



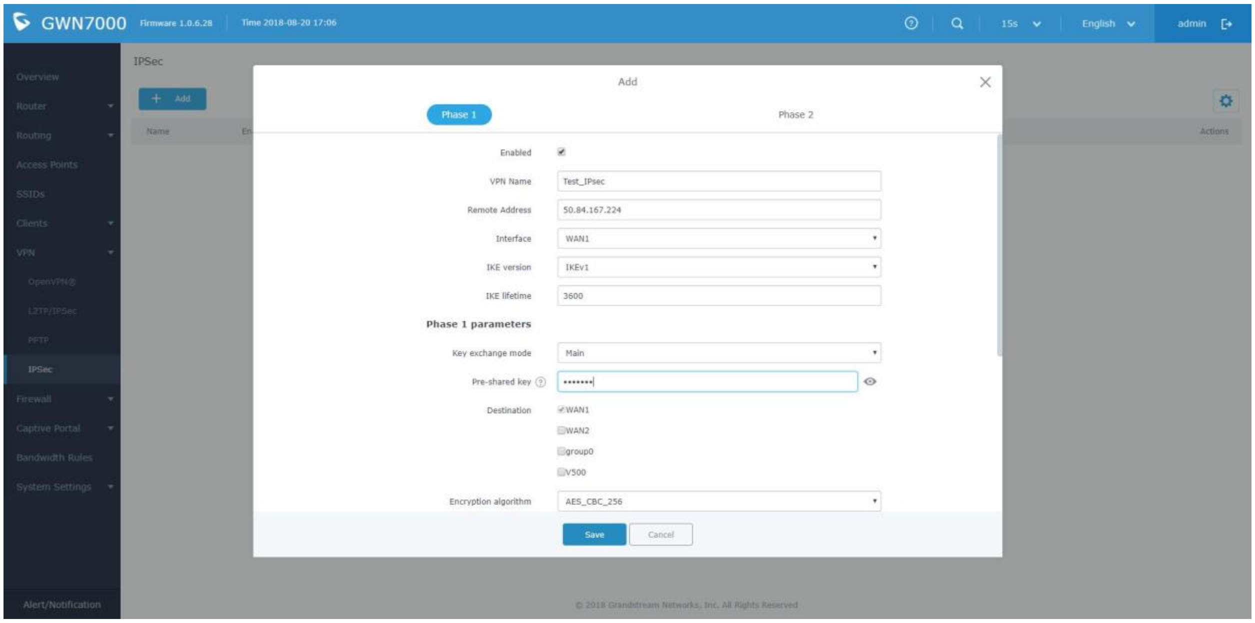
Add

|  |  |
|---|---|
| Tunnel Type | GRE |
| WAN Interface | WAN1 |
| Name | Example |
| Enabled | ☑ |
| Destination | ☑ WAN1<br>□ WAN2<br>□ group0 |
| GRE Peer IP Address | 12.34.56.78 |
| GRE Local Tunnel IP Address | 10.0.0.10 |
| GRE Remote Tunnel IP Address | 10.0.0.1 |
| GRE Tunnel Netmask | 255.255.255.0 |
| MTU |  |
| Subnet |  |

There are no GRE tunnels.

- **IPsec Tunnels**

Configuration is available at **VPN→IPSec**. Phase 1 and 2 configurations are required to build a connection with remote end.

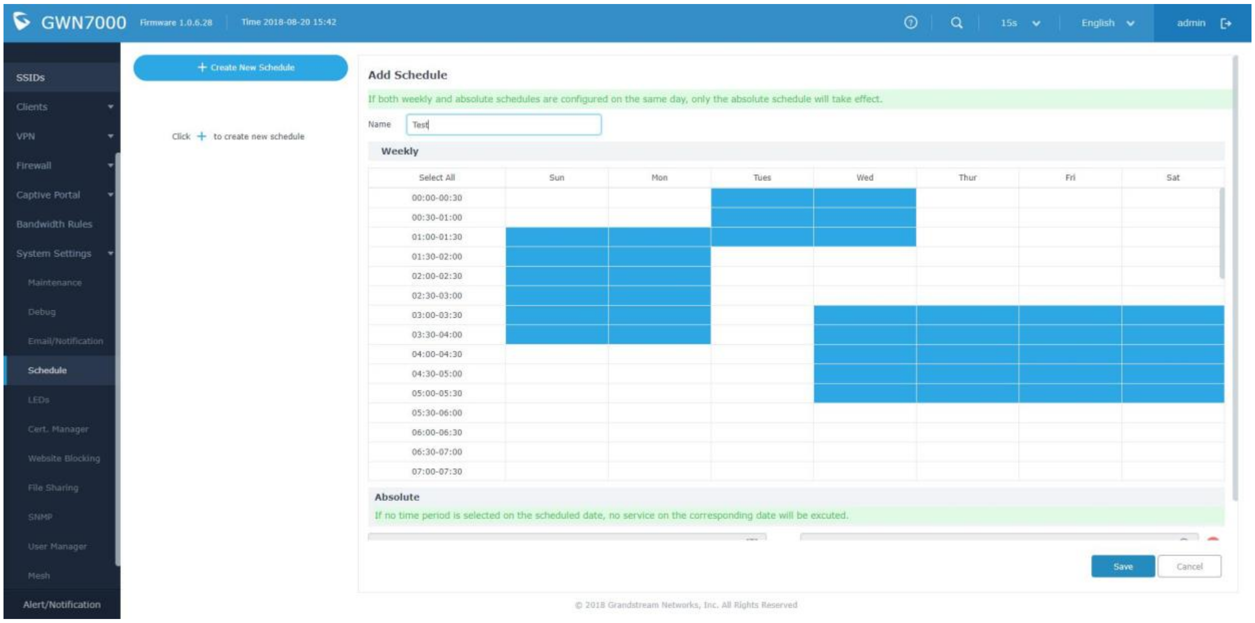


Add

|  |  |
|---|---|
| Enabled | ☑ |
| VPN Name | Test_IPsec |
| Remote Address | 50.84.167.224 |
| Interface | WAN1 |
| IKE version | IKEv1 |
| IKE lifetime | 3600 |
| **Phase 1 parameters** |  |
| Key exchange mode | Main |
| Pre-shared key | ••••••• |
| Destination | ☑ WAN1<br>□ WAN2<br>□ group0<br>□ V500 |
| Encryption algorithm | AES_CBC_256 |

- **Feature Scheduling**

  Feature scheduling allows user to create and manipulate a set of times/days/dates when specific features of the system are to be enabled and disabled. Its configurations are available at **System Settings→Schedule.**



Add Schedule

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

Name: Test

Weekly

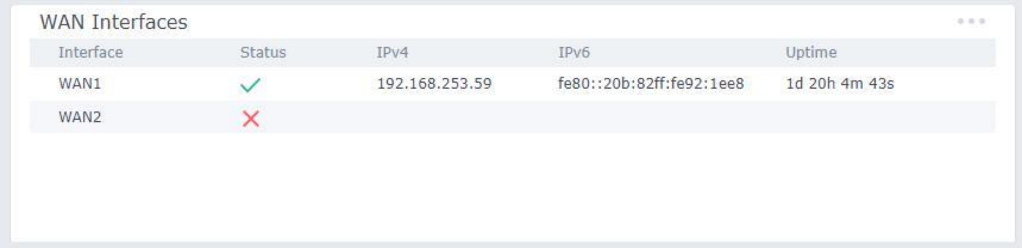
| Select All | Sun | Mon | Tues | Wed | Thur | Fri | Sat |
|---|---|---|---|---|---|---|---|
| 00:00-00:30 | | | ■ | ■ | | | |
| 00:30-01:00 | | | ■ | ■ | | | |
| 01:00-01:30 | ■ | ■ | ■ | ■ | | | |
| 01:30-02:00 | ■ | ■ | | | | | |
| 02:00-02:30 | ■ | ■ | | | | | |
| 02:30-03:00 | ■ | ■ | | | | | |
| 03:00-03:30 | ■ | ■ | | ■ | ■ | ■ | ■ |
| 03:30-04:00 | ■ | ■ | | ■ | ■ | ■ | ■ |
| 04:00-04:30 | | | | ■ | ■ | ■ | ■ |
| 04:30-05:00 | | | | ■ | ■ | ■ | ■ |
| 05:00-05:30 | | | | ■ | ■ | ■ | ■ |
| 05:30-06:00 | | | | | | | |
| 06:00-06:30 | | | | | | | |
| 06:30-07:00 | | | | | | | |
| 07:00-07:30 | | | | | | | |

Absolute

If no time period is selected on the scheduled date, no service on the corresponding date will be excuted.

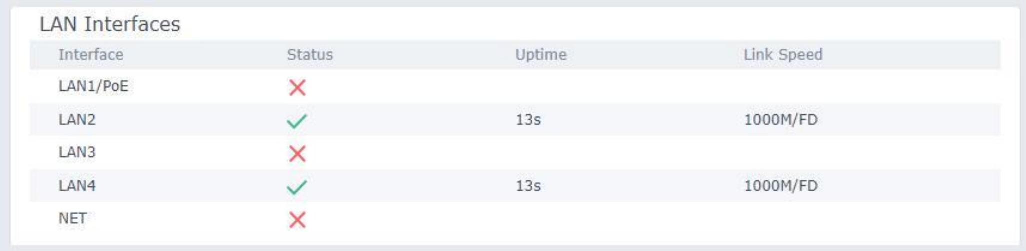
© 2018 Grandstream Networks, Inc. All Rights Reserved

- **WAN/LAN interfaces status on Overview page**



WAN Interfaces

| Interface | Status | IPv4 | IPv6 | Uptime |
|---|---|---|---|---|
| WAN1 | ✓ | 192.168.253.59 | fe80::20b:82ff:fe92:1ee8 | 1d 20h 4m 43s |
| WAN2 | ✗ | | | |



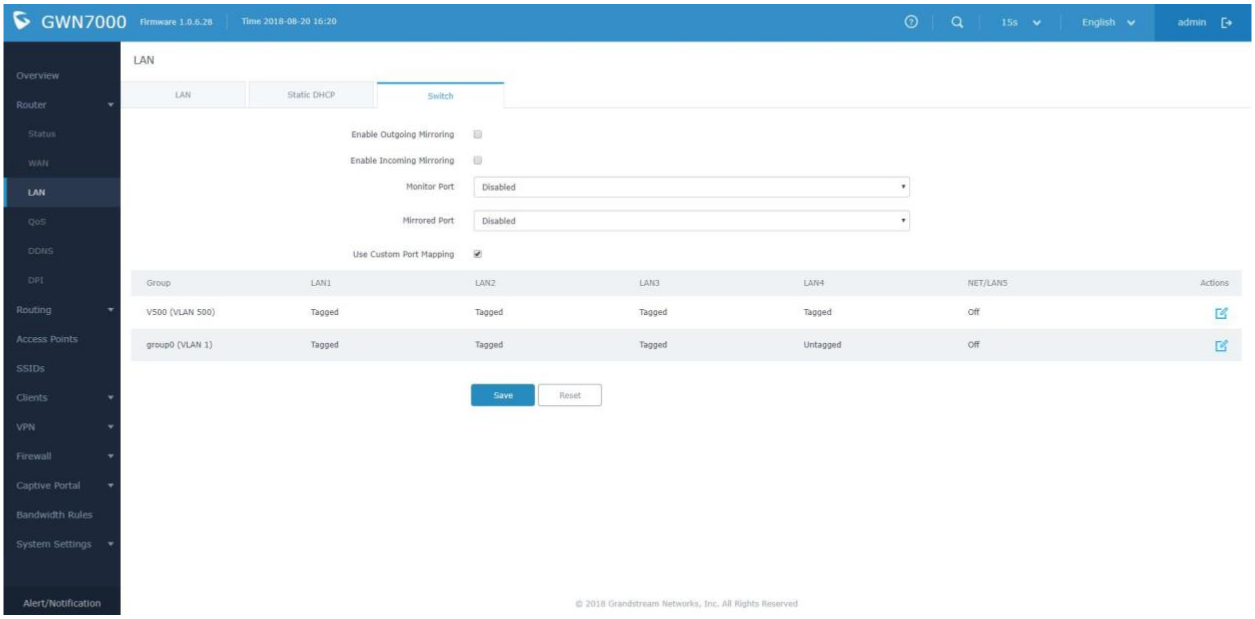
LAN Interfaces

| Interface | Status | Uptime | Link Speed |
|---|---|---|---|
| LAN1/PoE | ✗ | | |
| LAN2 | ✓ | 13s | 1000M/FD |
| LAN3 | ✗ | | |
| LAN4 | ✓ | 13s | 1000M/FD |
| NET | ✗ | | |

- **Switch Port LAN Mapping**

  Custom Port Mapping's configuration is located at **Router→LAN→Switch.**

  Through Customer Port Mapping, admin can configure port mirroring and also 802.1Q like VLAN Tagging on GWN7000 LAN ports.



LAN

Enable Outgoing Mirroring ☐

Enable Incoming Mirroring ☐

Monitor Port: Disabled

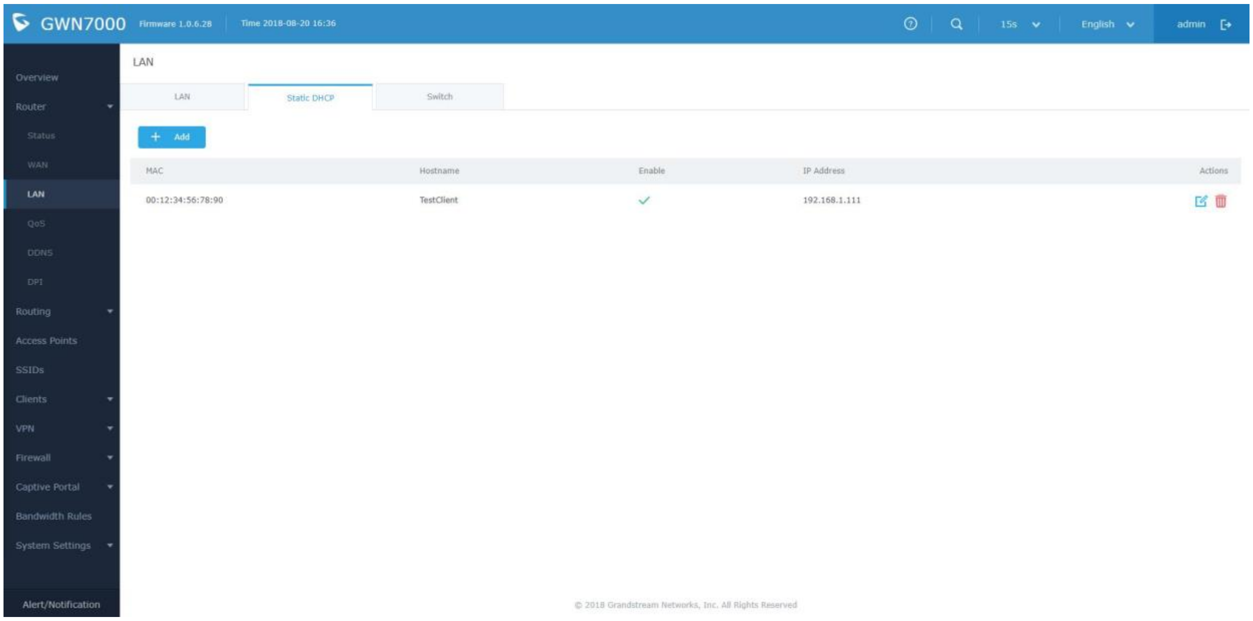
Mirrored Port: Disabled

Use Custom Port Mapping ☑

| Group | LAN1 | LAN2 | LAN3 | LAN4 | NET/LAN5 | Actions |
|---|---|---|---|---|---|---|
| V500 (VLAN 500) | Tagged | Tagged | Tagged | Tagged | Off | |
| group0 (VLAN 1) | Tagged | Tagged | Tagged | Untagged | Off | |

- **Static DHCP** (IP reserving on DHCP server)

  Static DHCP configuration is available at **Router→LAN→Static DHCP**



LAN

| MAC | Hostname | Enable | IP Address | Actions |
|---|---|---|---|---|
| 00:12:34:56:78:90 | TestClient | ✓ | 192.168.1.111 | |

- **Static IP reservation on OpenVPN client**

  Configuration is available at **VPN→OpenVPN→Client→Add or Edit→Local TUN IP Address or Remote TUN IP Address.**

- **DNS Rebind Attack Protection**

  Configuration is available at **System Settings→Maintenance→Basic→Rebind Protection.**

- **Sequential Upgrade**

  The sequential upgrade feature is an improvement to the standard upgrade procedure that triggers the firmware upgrade of one slave access point at a time, rather than all selected access points simultaneously. It’s available when you checked multiple slave Access Points for upgrading.

# FIRMWARE VERSION 1.0.4.23

## PRODUCT NAME

GWN7000

## DATE

9/6/2017

## IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.71 or higher.

## ENHANCEMENT

- Added support for enable/disable MPPE in both PPTP server and client.

## BUG FIX

- Fixed the issue that PPPoE username cannot be longer than 32 characters.
- Fixed the issue that when 6in4 tunnel is configured, firewall INPUT may work improperly by configuring src group other than ALL.
- Fixed the issue that IPv6 forwarding between LAN and WAN may be disable in some configurations.

## KNOWN ISSUE

- After blocking wireless client, blocked client will be displayed as wired in the clients list instead of showing in the Blocked client list. The client can still be unblocked from Global Blacklist under Client Access.
- Unrecognized traffic may be classified as HTTPS in Application Traffic.
- GWN PPTP client will fail to connect GWN PPTP server when client uses server's Additional WAN IP.
- Cert. Manager will be abnormal after generate a certificate with very long Chinese name.

- Client's name does not display in list of top clients of overview page.
- GWN7000 does not display NET Port clients on Clients page.
- DPI will function abnormally with multi-WAN configuration.
- OpenVPN Client will function abnormally with multi-WAN uplink.
- OpenVPN server is abnormal by using PSK mode.
- Modifying Client Subnet (OpenVPN Server) in User Manager needs reboot to work.

# FIRMWARE VERSION 1.0.4.20

## PRODUCT NAME

GWN7000

## DATE

8/11/2017

## IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.71 or higher.

## ENHANCEMENT

- Added support for **Additional Routed Subnets**
- Added support for **Timed Client Disconnect and Enhanced Client Blocking**
- Added support for **Client Bridge**

  GWN76xx Access Point is required for this feature.
- Added support for **Open App ID**
- Added support for **Syslog Server**
- Added support for **PPTP Server**
- Added support for **Smart Queue QoS**
- Added support for **Configurable web UI access port**
- Added support for **E-mail notifications**

**Note:**

For All new features that require GWN76xx AP, they require the slave AP to use matching firmware.

For GWN7610, please use firmware 1.0.4.20 or higher version.

## BUG FIX

- Fixed the bug which causes PPTP VPN low performance,
- Fixed OpenVPN server bug which causes routing failure from OpenVPN server to client in site-to-site VPN configuration.

## KNOWN ISSUE

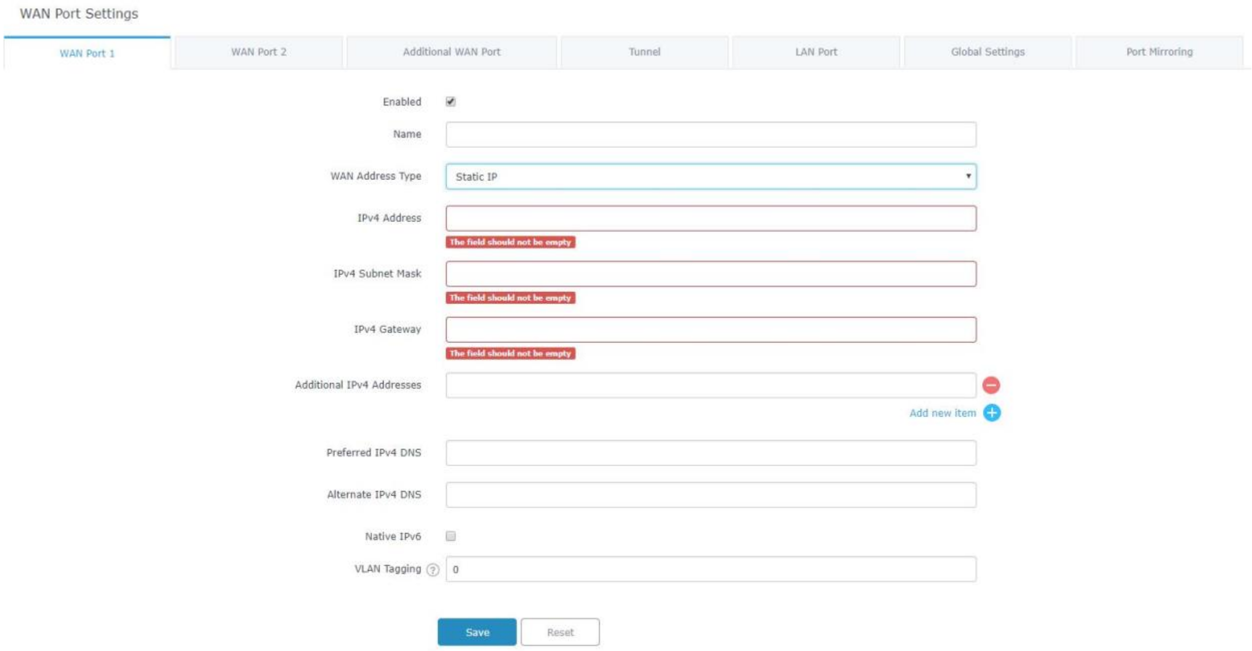
- After blocking wireless client, blocked client will be displayed as wired in the clients list instead of showing in the Blocked client list. The client can still be unblocked from Global Blacklist under Client Access.
- Unrecognized traffic may be classified as HTTPS in Application Traffic.
- GWN PPTP client will fail to connect GWN PPTP server when client uses server’s Additional WAN IP.
- Cert. Manager will be abnormal after generate a certificate with very long Chinese name.
- Client's name does not display in list of top clients of overview page.
- GWN7000 does not display NET Port clients on Clients page.
- DPI will function abnormally with multi-WAN configuration.
- OpenVPN Client will function abnormally with multi-WAN uplink.
- OpenVPN server is abnormal by using PSK mode.
- Modifying Client Subnet (OpenVPN Server) in User Manager needs reboot to work.

## NEW FEATURES OVERVIEW

- **Additional Routed Subnets**

  The additional routed subnets feature allows for the user to specify additional IP addresses to each LAN interface on the GWN7000. These IP address can be used for communicating with the web interface, SSH, or other services running on the device. Additional Firewall configuration is available for supporting this feature as well.

1) Additional IP for WAN interfaces:



WAN Port Settings

Enabled ☑

Name

WAN Address Type: Static IP

IPv4 Address
The field should not be empty

IPv4 Subnet Mask
The field should not be empty

IPv4 Gateway
The field should not be empty

Additional IPv4 Addresses

Add new item

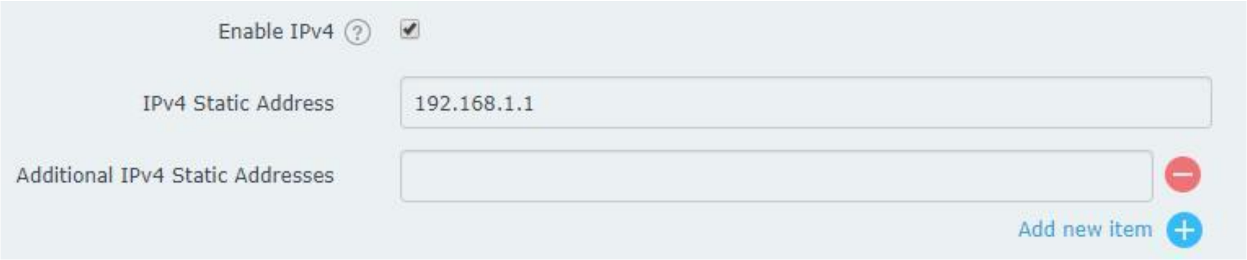
Preferred IPv4 DNS

Alternate IPv4 DNS

Native IPv6 □

VLAN Tagging: 0

2) Additional IP under Network Group configuration:



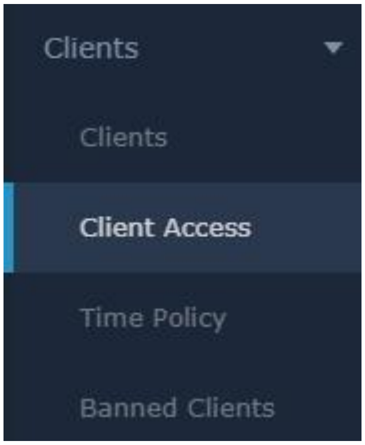
Enable IPv4 ☑

IPv4 Static Address: 192.168.1.1

Additional IPv4 Static Addresses

3) Firewall Input Rules with added destination IP configuration and Output Rules with added source IP configuration.

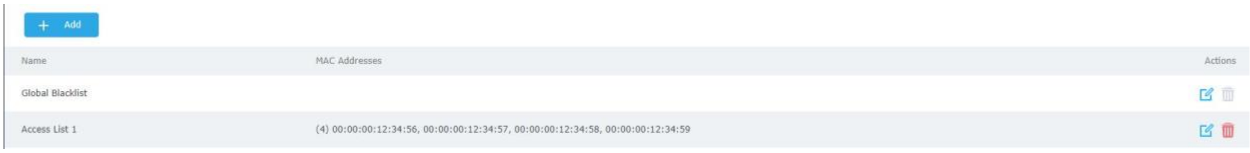
- **Timed Client Disconnect and Enhanced Client Blocking**



The Client Connection Permissions Management enhanced client blocking provides a more manageable method for Wi-Fi client whitelist and blacklist configuration. It allows any combination of globally-maintained connection access control lists to be applied to network groups as desired for blacklisting and whitelisting WIFI clients.

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 cooldown period.

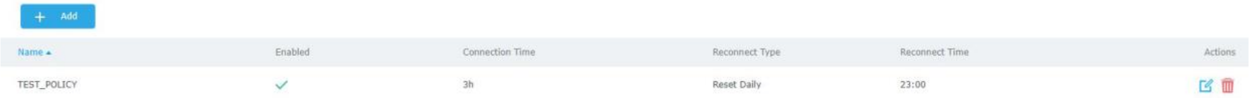
1) New Client bar (See picture on the right)



| Name | MAC Addresses | Actions |
|---|---|---|
| Global Blacklist | | |
| Access List 1 | (4) 00:00:00:12:34:56, 00:00:00:12:34:57, 00:00:00:12:34:58, 00:00:00:12:34:59 | |

2) Client Access

3) Time Policy



| Name ▲ | Enabled | Connection Time | Reconnect Type | Reconnect Time | Actions |
|---|---|---|---|---|---|
| TEST_POLICY | ✓ | 3h | Reset Daily | 23:00 | |

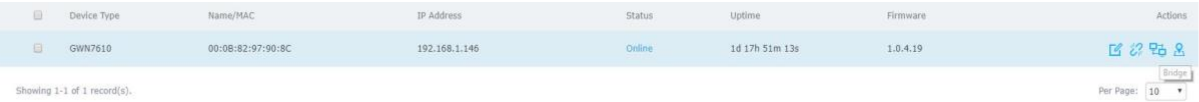
4) Banned Client This list is moved from original Client page to a separate page now.

- **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.

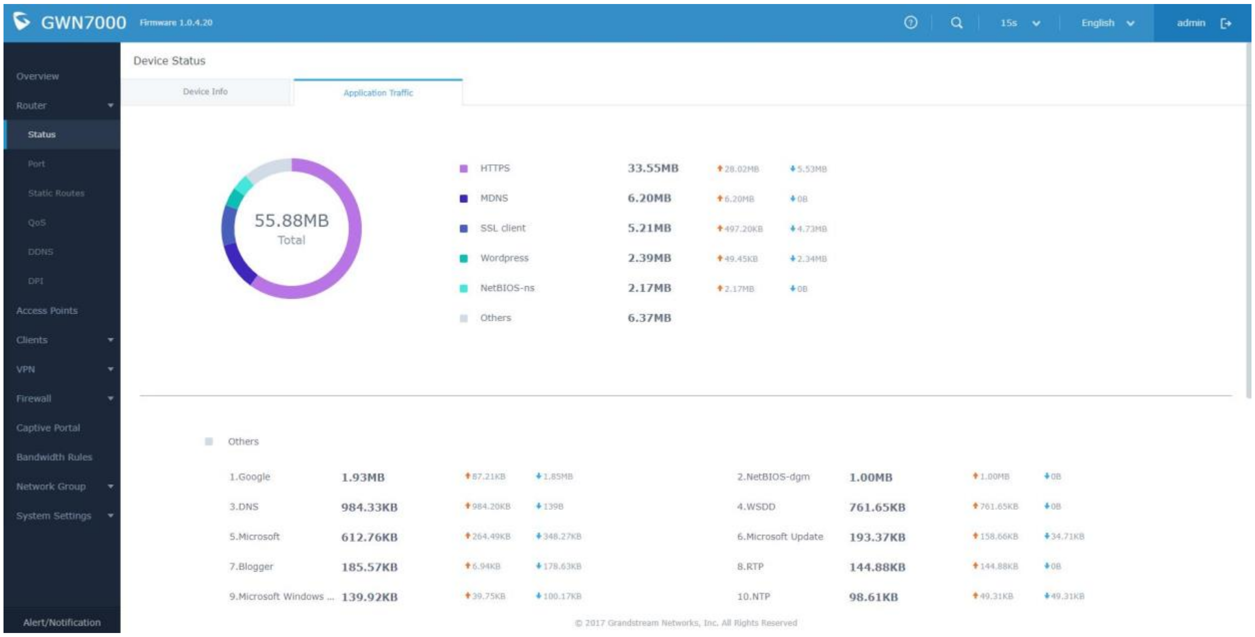


| □ | Device Type | Name/MAC | IP Address | Status | Uptime | Firmware | Actions |
|---|---|---|---|---|---|---|---|
| □ | GWN7610 | 00:0B:82:97:90:8C | 192.168.1.146 | Online | 1d 17h 51m 13s | 1.0.4.19 | |

Showing 1-1 of 1 record(s).

- **Open App ID**

Once DPI is enabled under Router feature. You will be able to see Application Traffic as below in Status:



| | | | | |
|---|---|---|---|---|
| ■ | HTTPS | 33.55MB | ↑28.02MB | ↓5.53MB |
| ■ | MDNS | 6.20MB | ↑6.20MB | ↓0B |
| ■ | SSL client | 5.21MB | ↑497.20KB | ↓4.73MB |
| ■ | Wordpress | 2.39MB | ↑49.45KB | ↓2.34MB |
| ■ | NetBIOS-ns | 2.17MB | ↑2.17MB | ↓0B |
| ■ | Others | 6.37MB | | |

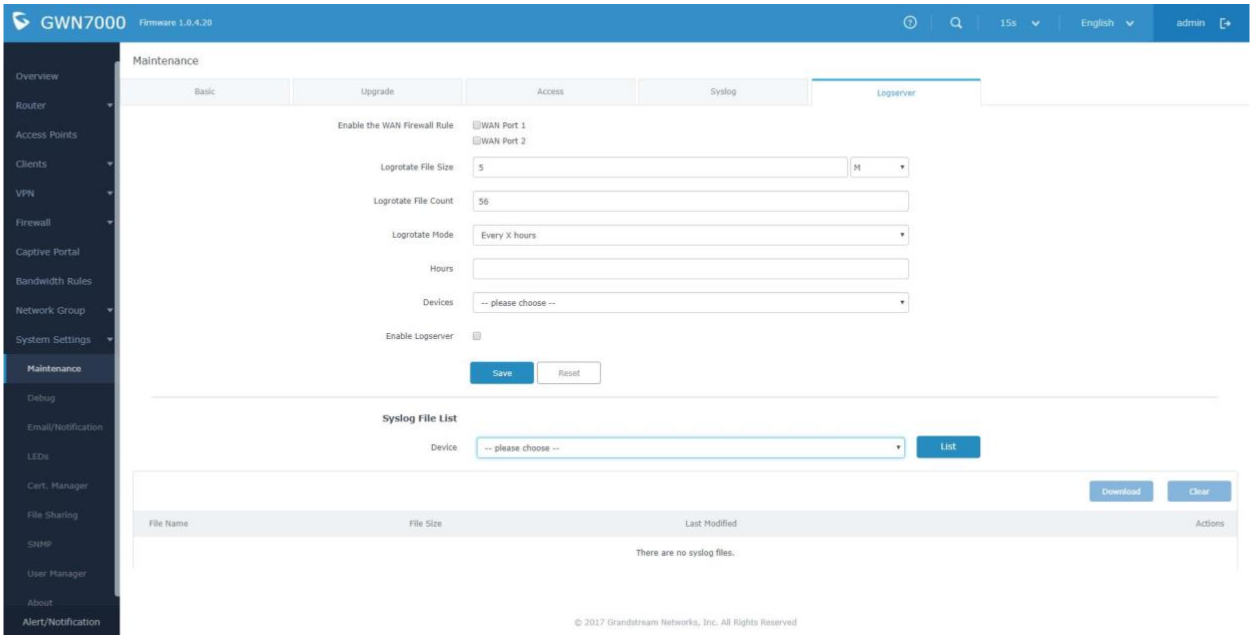
■ Others

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.Google | 1.93MB | ↑87.21KB | ↓1.85MB | 2.NetBIOS-dgm | 1.00MB | ↑1.00MB | ↓0B |
| 3.DNS | 984.33KB | ↑984.20KB | ↓139B | 4.WSDD | 761.65KB | ↑761.65KB | ↓0B |
| 5.Microsoft | 612.76KB | ↑264.49KB | ↓348.27KB | 6.Microsoft Update | 193.37KB | ↑158.66KB | ↓34.71KB |
| 7.Blogger | 185.57KB | ↑6.94KB | ↓178.63KB | 8.RTP | 144.88KB | ↑144.88KB | ↓0B |
| 9.Microsoft Windows ... | 139.92KB | ↑39.75KB | ↓100.17KB | 10.NTP | 98.61KB | ↑49.31KB | ↓49.31KB |

© 2017 Grandstream Networks, Inc. All Rights Reserved

- **Syslog Server**

Syslog Server is now available on GWN7000. Configuration page is as below:



| | |
|---|---|
| Enable the WAN Firewall Rule | □ WAN Port 1<br>□ WAN Port 2 |
| Logrotate File Size | 5 M |
| Logrotate File Count | 56 |
| Logrotate Mode | Every X hours |
| Hours | |
| Devices | -- please choose -- |
| Enable Logserver | □ |

Save Reset

**Syslog File List**

Device -- please choose -- List

Download Clear

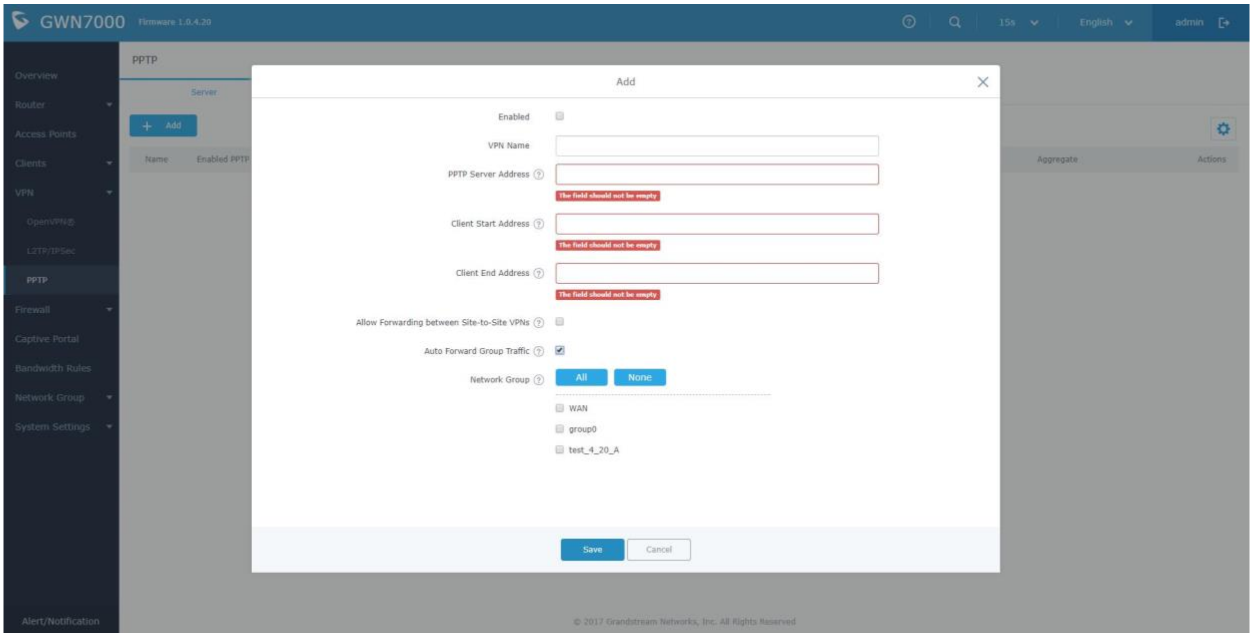
| File Name | File Size | Last Modified | Actions |
|---|---|---|---|

There are no syslog files.

© 2017 Grandstream Networks, Inc. All Rights Reserved

- **PPTP Server**

PPTP server is now available on GWN7000. Configuration page is as below:



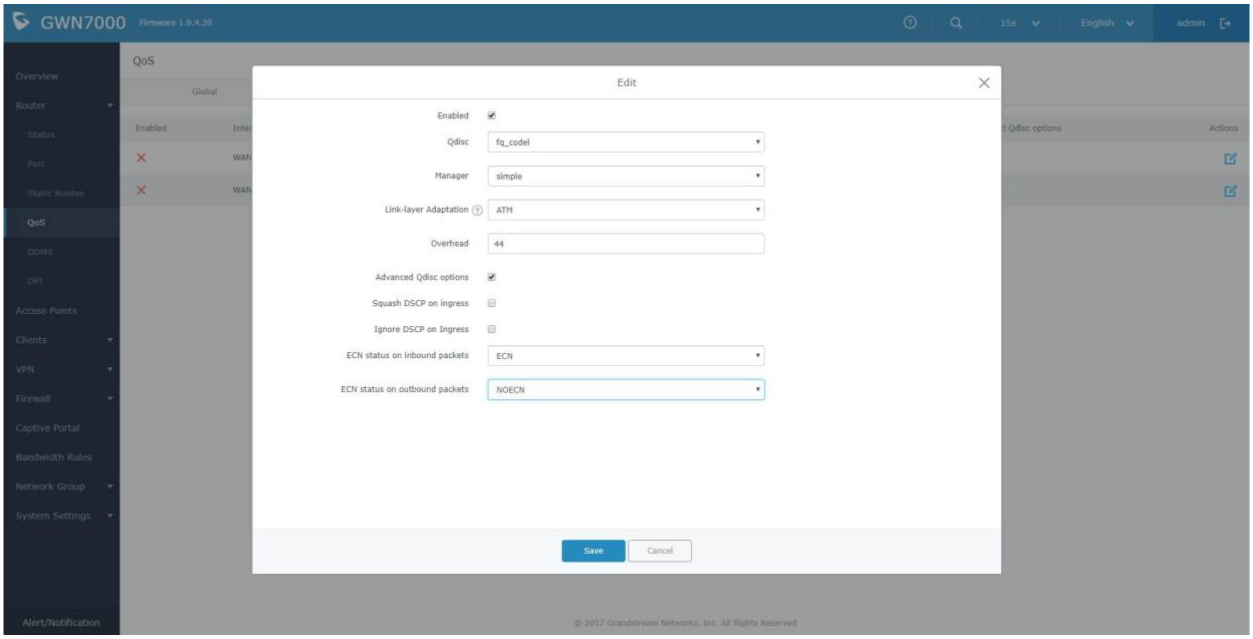
Add

Enabled □
VPN Name
PPTP Server Address
The field should not be empty
Client Start Address
The field should not be empty
Client End Address
The field should not be empty
Allow Forwarding between Site-to-Site VPNs □
Auto Forward Group Traffic ☑
Network Group All None
□ WAN
□ group0
□ test_4_20_A

Save Cancel

- **Smart Queue QoS**

The Smart Queue QoS will add a simple to configure, but very effective form of QoS that reduces buffer bloat and keeps latency at acceptable levels.



Edit

Enabled ☑
Qdisc: fq_codel
Manager: simple
Link-layer Adaptation: ATM
Overhead: 44
Advanced Qdisc options ☑
Squash DSCP on ingress □
Ignore DSCP on Ingress □
ECN status on inbound packets: ECN
ECN status on outbound packets: NOECN

Save Cancel

- **Configurable web UI access port**

  Under System →Maintenance, following configuration is available now:

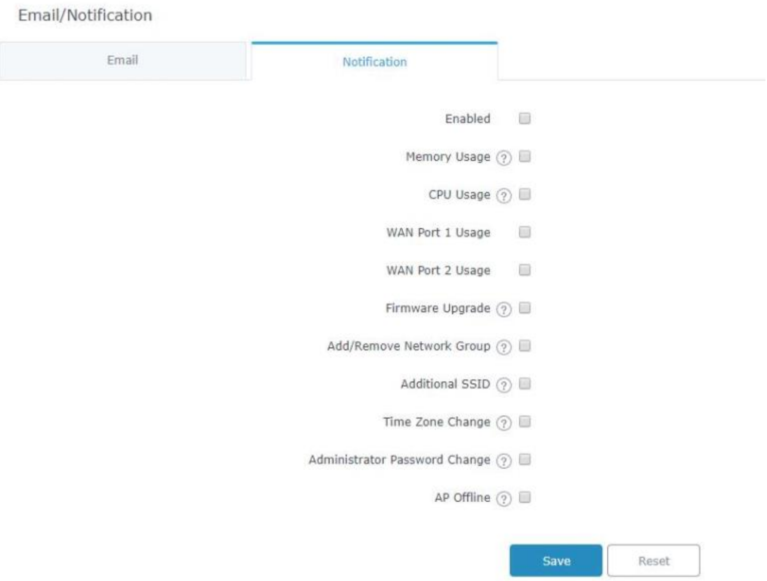
  1) Web WAN Access; 2) Web HTTP Access; 3) Web HTTPS Port

- **E-mail notifications**

  Email notification allows the administrator to select a predefined set of system events and to send notification upon the change of the set events.

  Email notification configuration is under System →Email/Notification.

  Selectable system events are listed as right-side screenshot.



Enabled □
Memory Usage ? □
CPU Usage ? □
WAN Port 1 Usage □
WAN Port 2 Usage □
Firmware Upgrade ? □
Add/Remove Network Group ? □
Additional SSID ? □
Time Zone Change ? □
Administrator Password Change ? □
AP Offline ? □

# FIRMWARE VERSION 1.0.2.75

## PRODUCT NAME

GWN7000

## DATE

6/20/2017

## IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.71 or higher.

## ENHANCEMENT

- Added support for Captive Portal

  GWN76xx Access Point is required for this feature.

- Added support for 802.11k/r (Enable Voice Enterprise)

  GWN76xx Access Point is required for this feature.

- Added support for Select band per SSID

  GWN76xx Access Point is required for this feature.

- Added support for Selectively enable b/g/n

  GWN76xx Access Point is required for this feature.

- Added support for Exact Radio Power Configuration in dBm

  GWN76xx Access Point is required for this feature.

- Added support for AP locating by blinking LED

  GWN76xx Access Point is required for this feature.

- Added support for Per-Client/Per-SSID bandwidth management

  GWN76xx Access Point is required for this feature.

- Added support for Limit client count per SSID

  GWN76xx Access Point is required for this feature.

- Added support for Slave AP LED control.

  GWN76xx Access Point is required for this feature.
- Added support for

WIFI schedule

GWN76xx Access Point is required for this feature.

- Added support for Enabling/Disabling DHCP option 66 for firmware upgrade

**Note:**

For All new features that require GWN76xx AP, they require the slave AP to use matching firmware.

For GWN7610, please use firmware 1.0.3.19 or higher version.

## BUG FIX

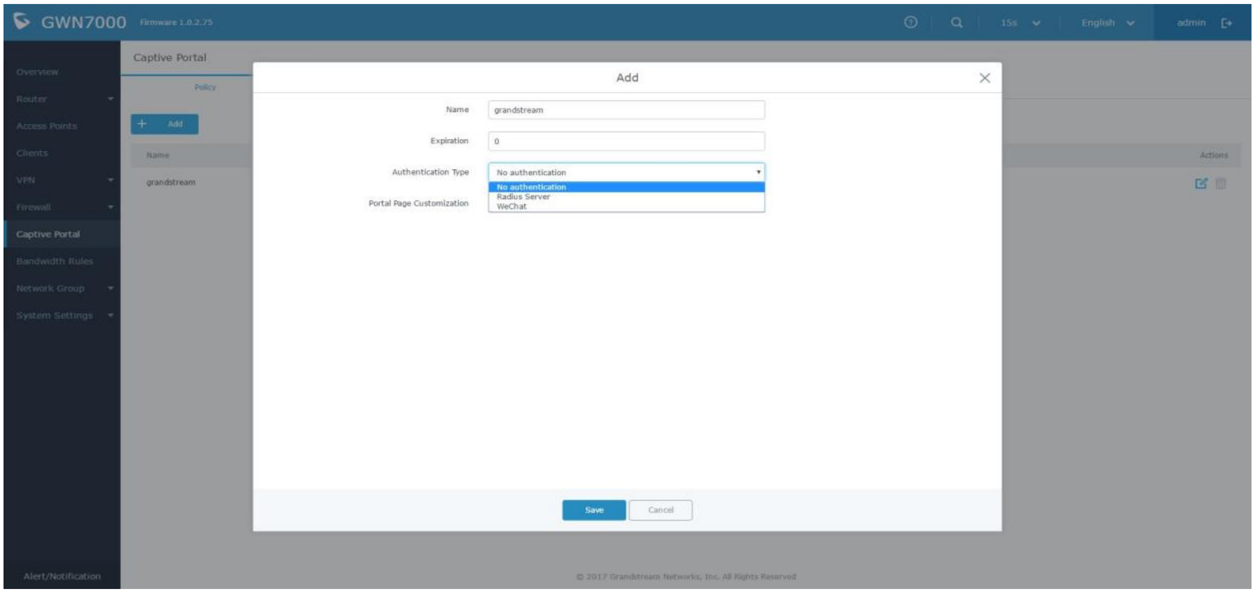
- Internal bug fixes

## KNOWN ISSUE

- Site-to-Site VPN has configuration issue, which causes one directional routing problem.
- Enabling both L2TP/IPsec VPN and QoS has low probability that QoS configuration may lost when applying the configuration on web.
- Banned Band steering feature still affect wireless Black/White/Banned client list feature. Please use Band steering or Black/White/Banned client list feature exclusively.

## NEW FEATURES OVERVIEW

- Captive Portal



Name: grandstream

Expiration: 0

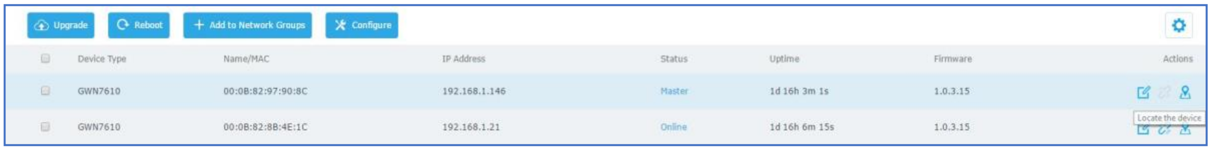
Authentication Type: No authentication

Portal Page Customization

Captive portal is supported in 1.0.2.75 now. We have 3 modes for authentication (No / Radius / WeChat) and customizable page.

- AP locating by blinking LED

  Now, when you can't match your AP list on web with your real AP deployment in the field, this feature will help you to find your AP.



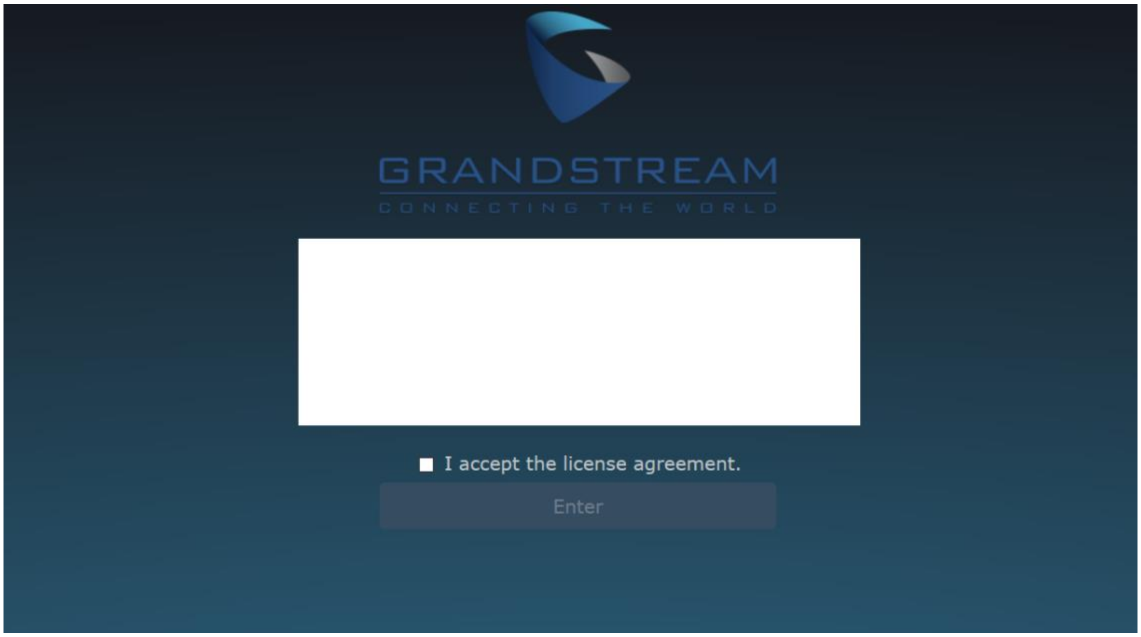
| ☐ | Device Type | Name/MAC | IP Address | Status | Uptime | Firmware | Actions |
|---|---|---|---|---|---|---|---|
| ☐ | GWN7610 | 00:0B:82:97:90:8C | 192.168.1.146 | Master | 1d 16h 3m 1s | 1.0.3.15 | |
| ☐ | GWN7610 | 00:0B:82:8B:4E:1C | 192.168.1.21 | Online | 1d 16h 6m 15s | 1.0.3.15 | |

- 802.11k/r (Enable Voice Enterprise)

  Configuration available at Network Group->Add/Edit->WiFi-> **Enable Voice Enterprise**.

- Select band per SSID

  Configuration available at Network Group->Add/Edit->WiFi-> **SSID band.**



- Selectively enable b/g/n

  Configuration available at Access Point->Edit->Configuration-> **Mode** (2.4G).

- Exact Radio Power Configuration in dBm

  Configuration available at Access Point->Edit->Configuration-> **Custom 2.4GHz Wireless Power** (dBm).

- Per-Client/Per-SSID bandwidth management

  Configuration available at

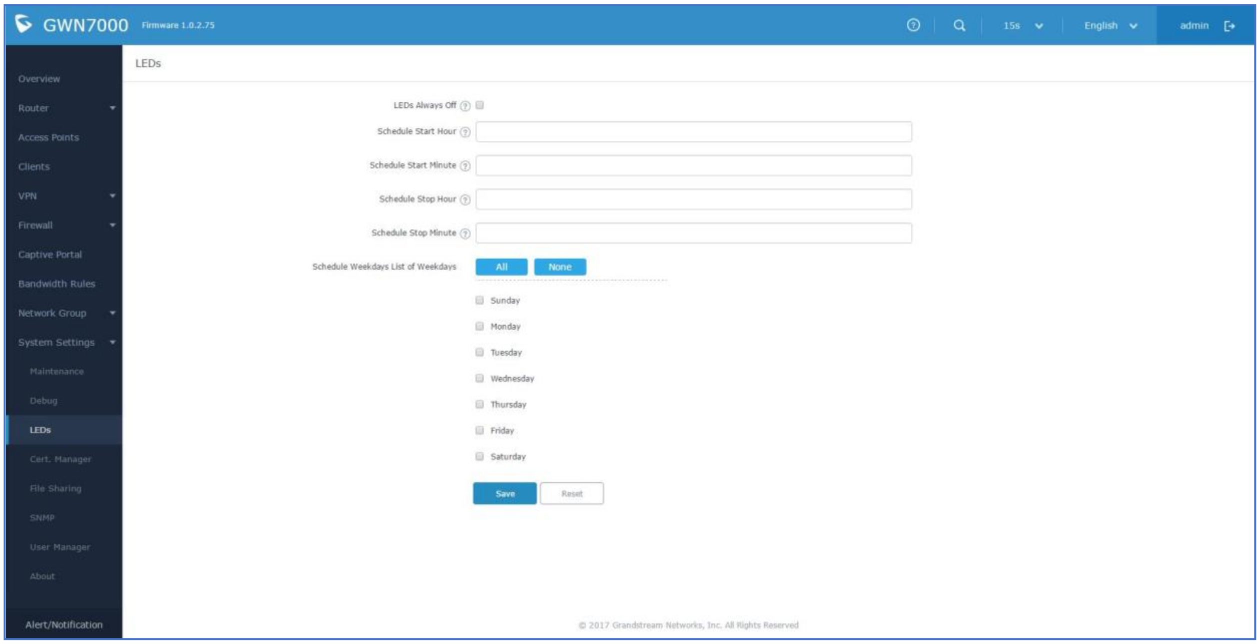
  Per-SSID: Network Group->Add/Edit->WiFi-> **Upstream Rate / Downstream Rate.**

  Per-Client: Client->Edit->Bandwidth Rules-> Add new item.

- Limit client count per SSID

  Configuration available at Network Group->Add/Edit->WiFi-> **Wireless Client Limit.**

- Slave AP LED control.



LEDs

LEDs Always Off ☐

Schedule Start Hour

Schedule Start Minute

Schedule Stop Hour

Schedule Stop Minute

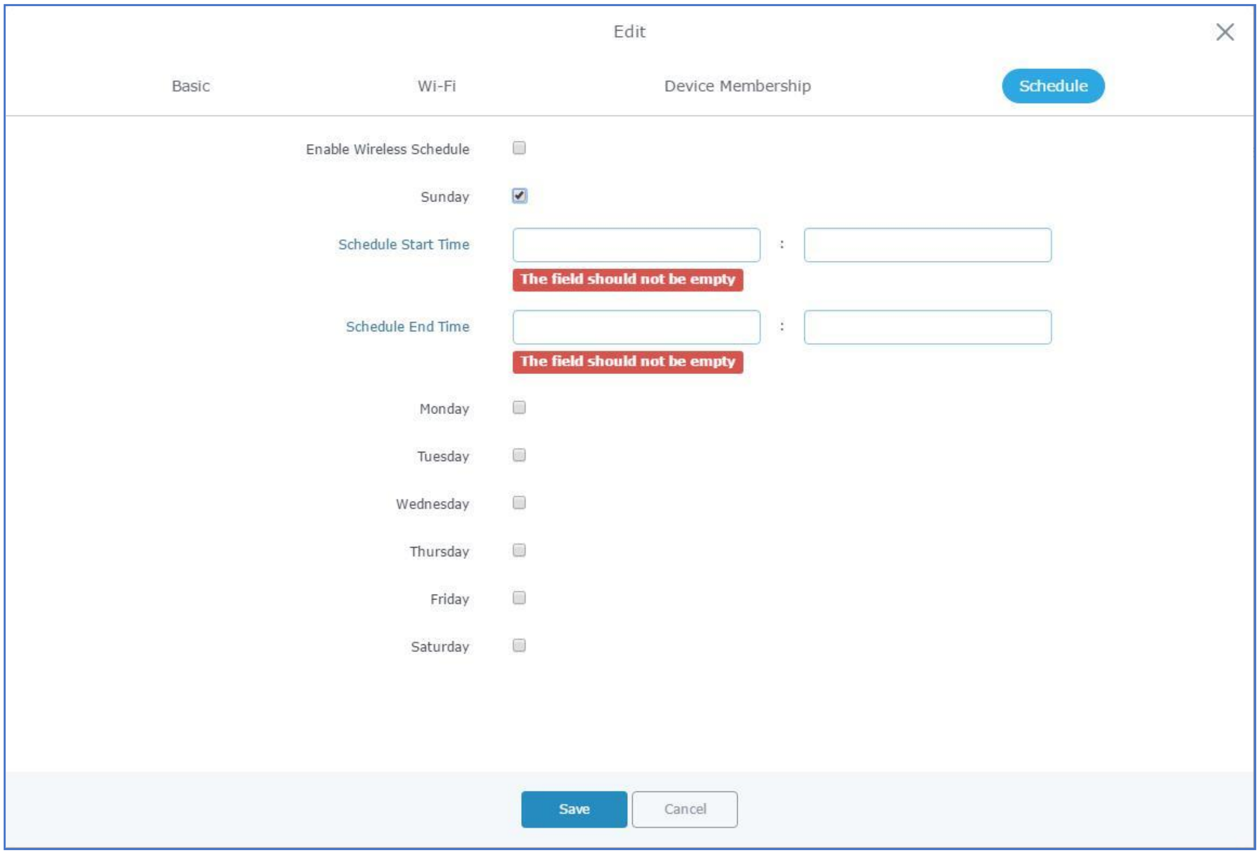
Schedule Weekdays List of Weekdays All None

☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

Save Reset

User can define the LED on/off schedule in following page.

- WIFI schedule



Enable Wireless Schedule ☐

Sunday ☑

Schedule Start Time [ ] : [ ]

The field should not be empty

Schedule End Time [ ] : [ ]

The field should not be empty

Monday ☐

Tuesday ☐

Wednesday ☐

Thursday ☐

Friday ☐

Saturday ☐

You can configure WIFI on/off schedule under Network Group->Edit->Schedule

- Enabling/Disabling DHCP option 66 for firmware upgrade

  Configuration available at System Settings->Maintenance->Upgrade-> **Allow DHCP options 66 and 43 override.**

# FIRMWARE VERSION 1.0.2.71

## PRODUCT NAME

GWN7000

## DATE

3/15/2017

## IMPORTANT UPGRADING NOTE

- **If your GWN7000 has firmware below 1.0.2.62 (1.0.2.62 not included), please refer to the beta forum upgrade guide or contact tech support for upgrade assistant.**

## NOTE

This is the initial official release of GWN7000.