GWN7000 Firmware Release Note

IMPORTANT UPGRADING NOTE

- **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.**

Table of Content

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.

FIRMWARE FILE INFORMATION

- Firmware file name: gwn7000fw.bin

- MD5: 9349c9602a2571b5a1ef9763a2cd7ec3

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

WAN Port 1	WAN Port 2	Additional WAN Port	Tunnel	LAN Port	Global Settings	Port Mirroring

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 ⑦ [0]

[Save] [Reset]

2) Additional IP under Network Group configuration:

Enable IPv4 ⑦ ☑

IPv4 Static Address [192.168.1.1]

Additional IPv4 Static Addresses [   ] ⊖
Add new item ⊕

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.

Clients ▾

Clients

Client Access

Time Policy

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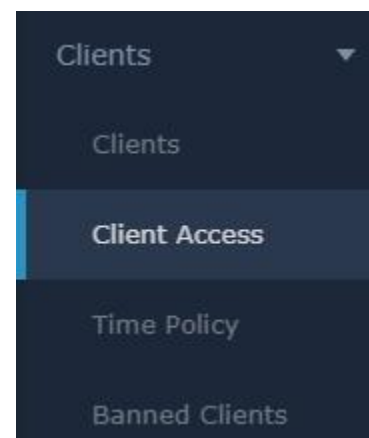
1) New Client bar (See picture on the right)

2) Client Access

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	

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).   Per Page: 10 ▼
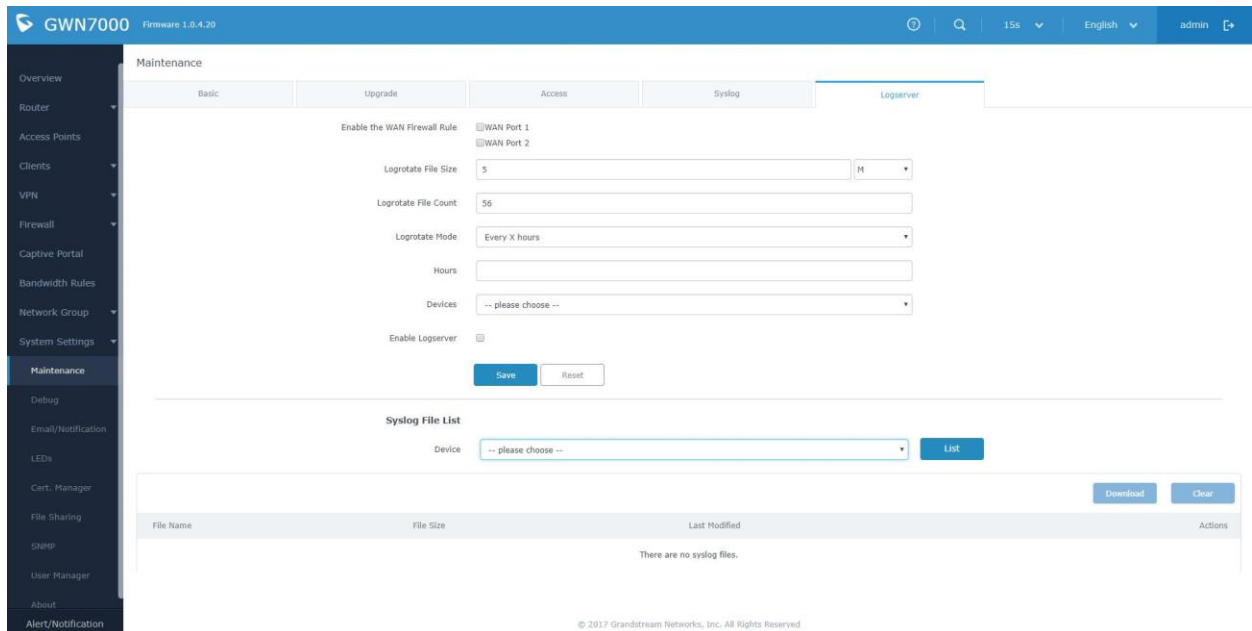
- **Open App ID**

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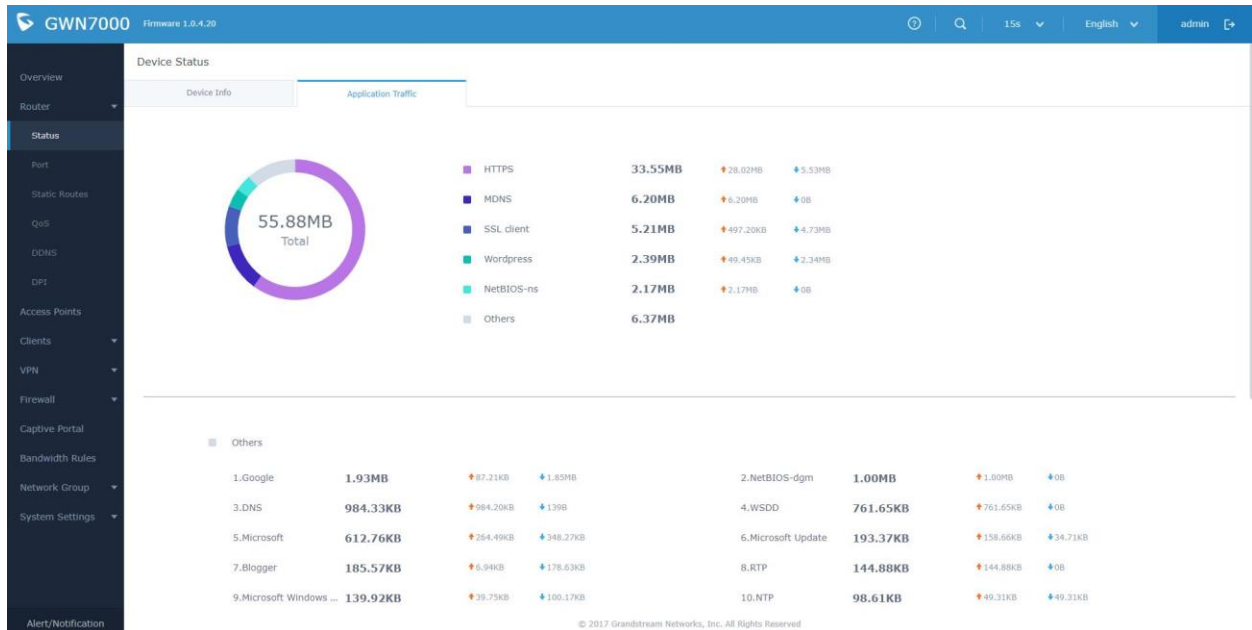
- **Syslog Server**

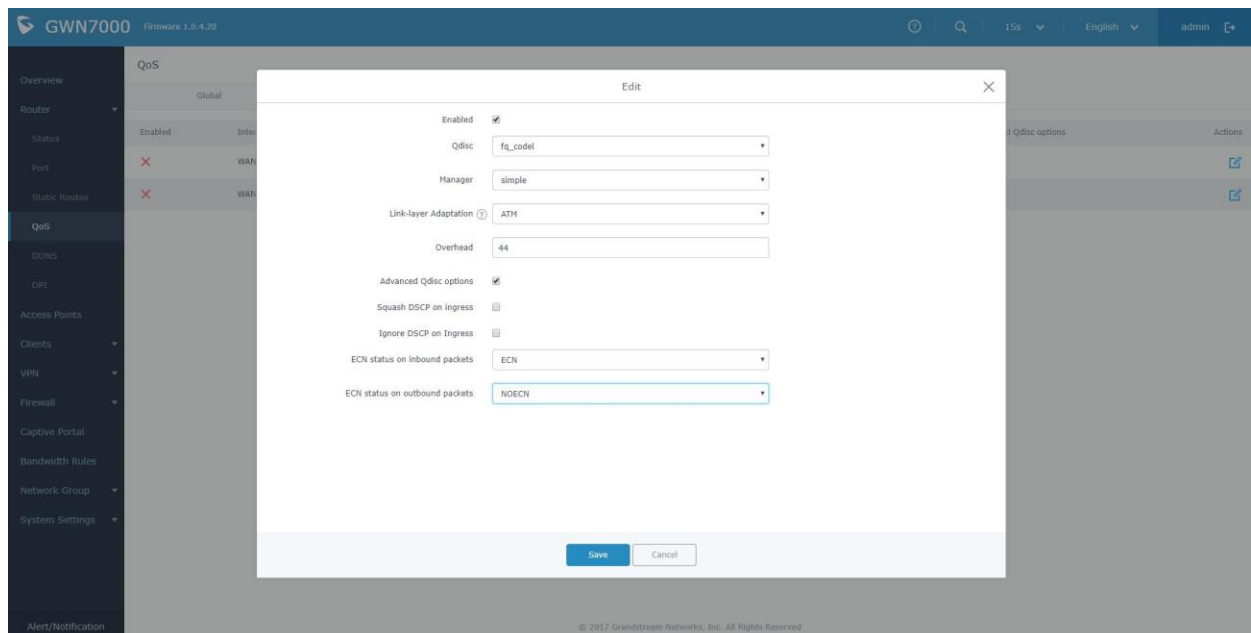 Syslog Server is now available on GWN7000. Configuration page is as below:

- **PPTP Server**

  PPTP server is now available on GWN7000. Configuration page is as below:
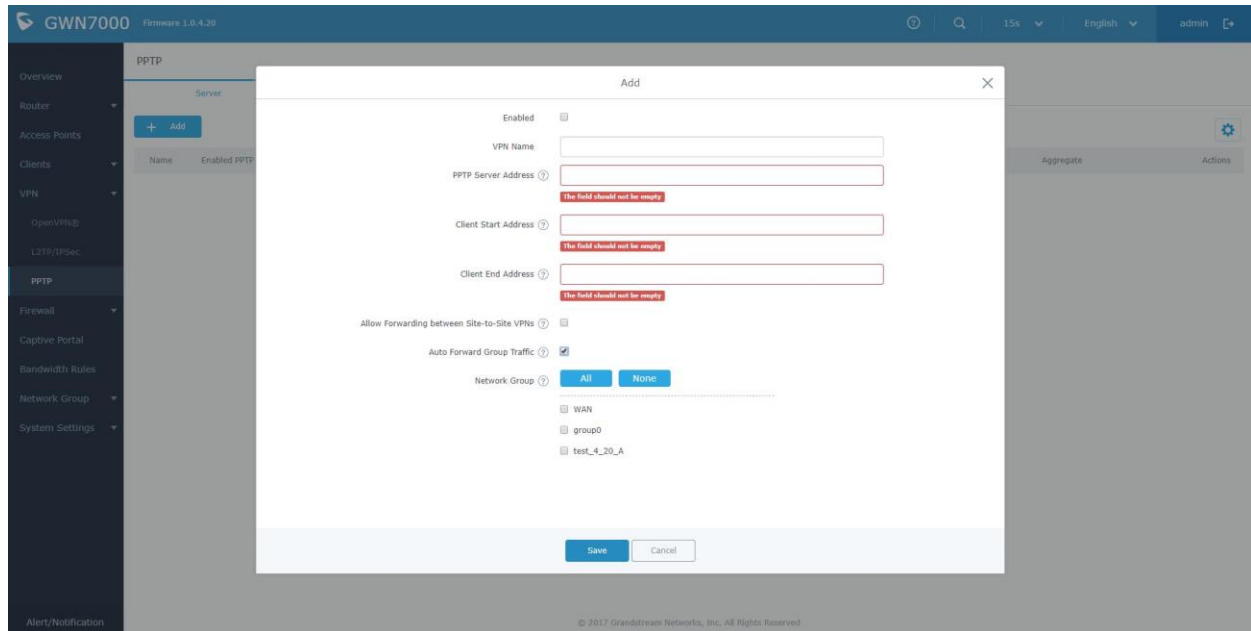
- **Smart Queue QoS**

  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.

- **Configurable web UI access port**

  Under System →Maintenance, following configuration is available now:
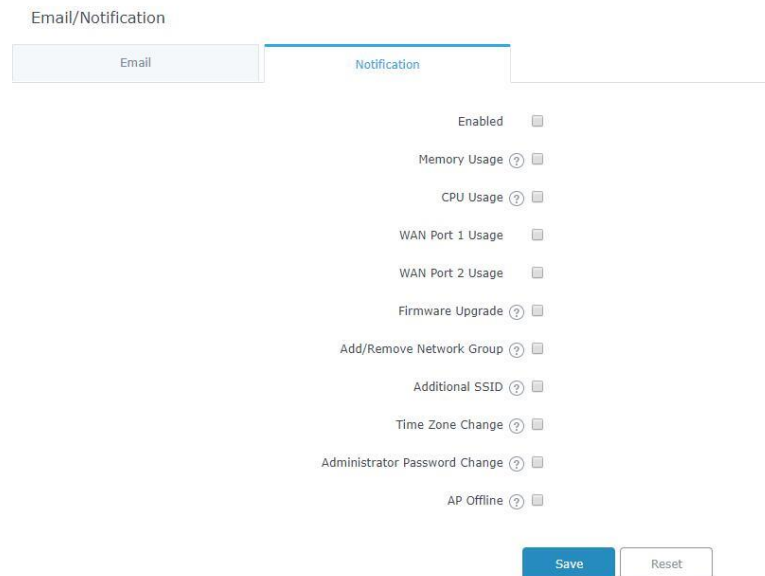
  1) Web WAN Access;   2) Web HTTP Access;   3) Web HTTPS Port

- **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.

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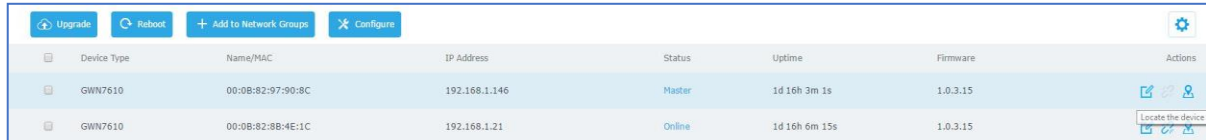
- Captive Portal
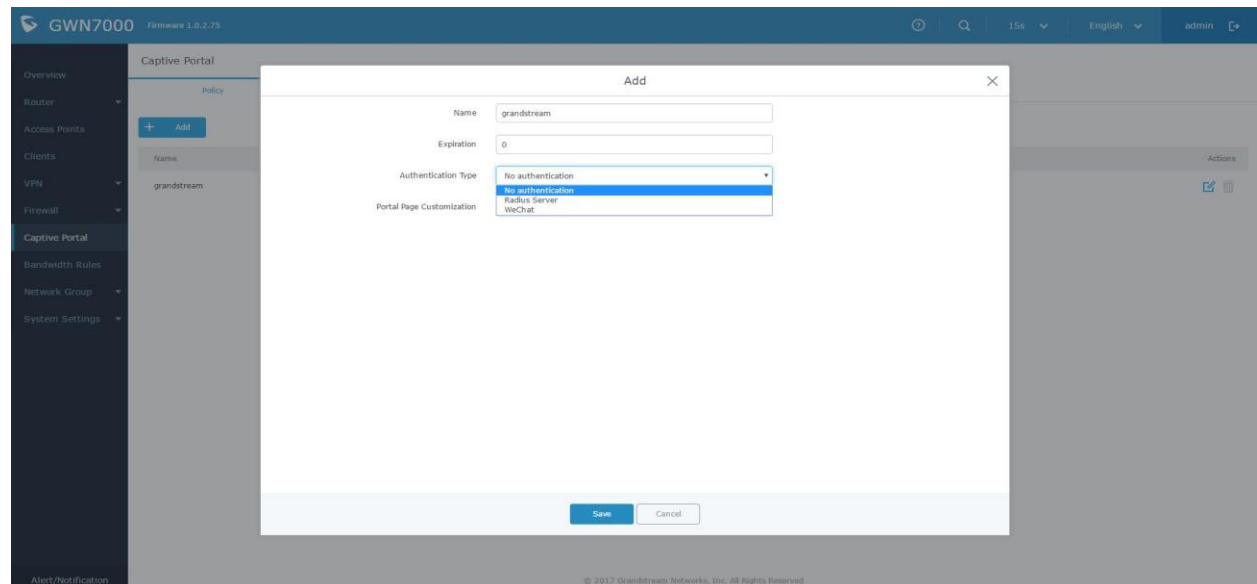
Captive portal is supported in 1.0.2.75 now. We have 3 modes for authentication (No / Radius / WeChat) and customizable page.

- 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.
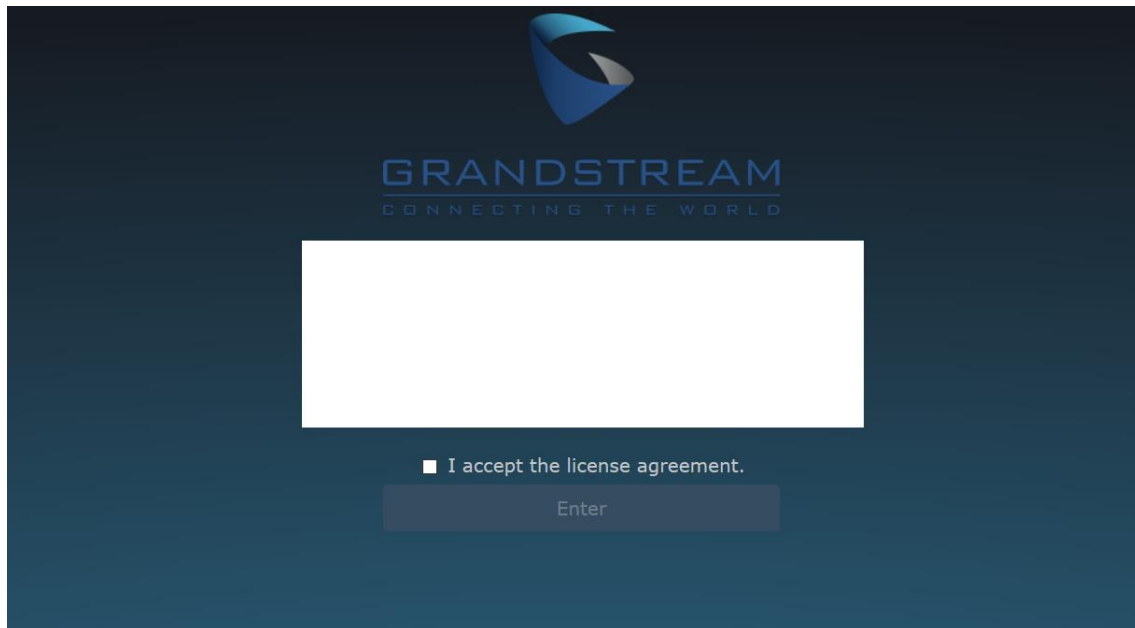

- 802.11k/r (Enable Voice Enterprise)

  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

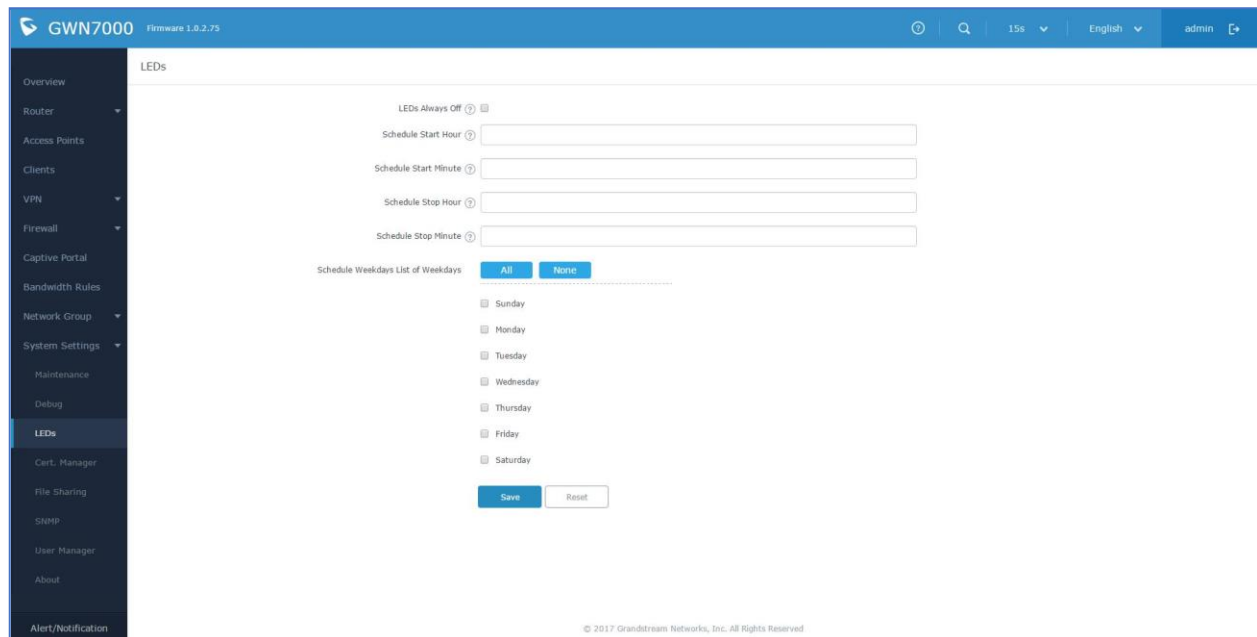 Configuration available at
  Per-SSID: Network Group->Add/Edit->WiFi-> **Upstream Rate / Downstream Rate.**
  Per-Client: Client->Edit->Bandwidth Rules-> Add new item.

- Limit client count per SSID

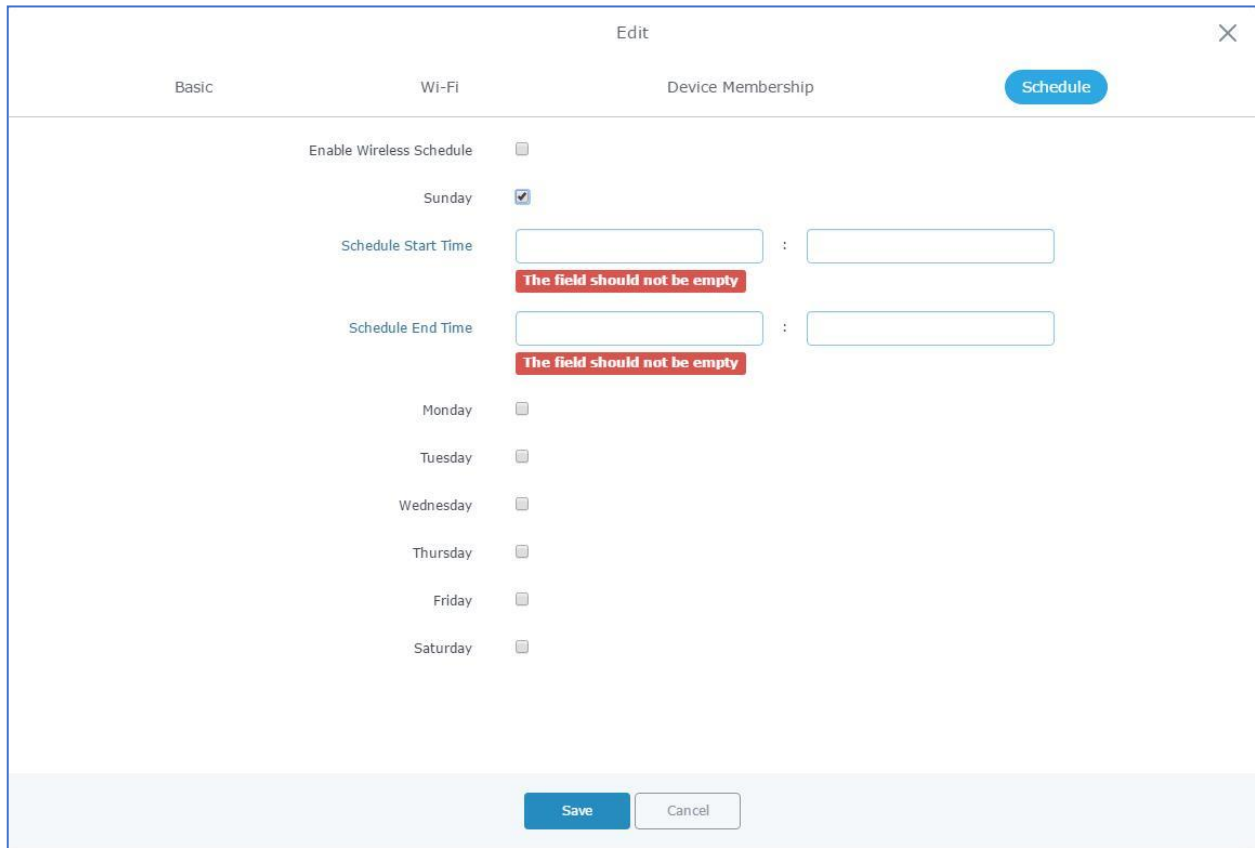 Configuration available at Network Group->Add/Edit->WiFi-> **Wireless Client Limit.**

- Slave AP LED control.

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

- WIFI schedule

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.