

GWN76xx Firmware Release Notes

IMPORTANT UPGRADING NOTE

1. [7/15/2021] [GWN7610 / GWN7600 / GWN7600LR] Please upgrade to 1.0.19.29 for security fix against Wi-Fi FragAttacks.
2. [6/4/2021] [GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615] Please upgrade to 1.0.19.29 for security fix against Wi-Fi FragAttacks.
3. [3/14/2020] [All APs 1.0.15.x] Due to the security enhancement, unless **Legacy TLS Compatibility** (only available on 1.0.15.4 or higher version) is enabled, master AP on 1.0.15.4 or higher firmware will not compatible with slave AP on firmware lower than 1.0.15.4. Master AP on firmware lower than 1.0.15.4 will also not be compatible with slave AP on firmware 1.0.15.4 or higher. Cloud and GWN Manager will still support both firmwares.
4. [3/14/2020] [All APs 1.0.15.x] Do not use 1.0.15.x AP firmware with GWN7000 1.0.9.x or lower version.
5. [12/14/2018] [All APs 1.0.8.17] In order to enable your AP's capability of connecting GWN Cloud EU server, AP needs to be upgraded to 1.0.8.17 or above.
6. [6/15/2018] [GWN7600&7600LR 1.0.6.41] Starting from 1.0.6.x, GWN7600 and GWN7600LR will share same firmware file name gwn7600fw.bin. As a result, when GWN7600LR upgrades from pre-1.0.6.x to latest firmware, it will still retrieve firmware with name gwn7600lrfw.bin, and when GWN7600LR upgrades from 1.0.6.x or post-1.0.6.x to other firmware, it will retrieve firmware with name gwn7600fw.bin. So, when your GWN7600LR upgrades from pre-1.0.6.x firmware, you will need to manually modify the target firmware name to gwn7600lrfw.bin.
7. [1/26/2017] [All APs 1.0.5.15] For firmware 1.0.5.15 (GWN7610) and 1.0.5.13 (GWN7600&GWN7600LR) , this is only for GWN7610/GWN7600/GWN7600LR master deployment. All

users with GWN7000 as master are NOT encouraged to upgrade until 1.0.5.x matching firmware is available for GWN7000, due to the compatibility of new features.

8. [8/11/2017] [All APs 1.0.4.22] Please upgrade to 1.0.4.12 or higher version to get the patch for WPA2 4-way handshake vulnerability.
9. [8/11/2017] [GWN7610 1.0.3.21] Before starting to upgrade to latest firmware, please make sure your GWN7610's firmware version is 1.0.2.108 or higher. Also, please make sure your GWN7000 master (if any)'s firmware version is 1.0.2.71 or higher.

Table of Content

IMPORTANT UPGRADING NOTE	1
[GWN7602]FIRMWARE VERSION 1.0.19.34	10
PRODUCT NAME	10
DATE	10
FIRMWARE FILE INFORMATION	10
CHANGES/ENHANCEMENT	10
FIRMWARE VERSION 1.0.21.16	11
PRODUCT NAME	11
DATE	11
FIRMWARE FILE INFORMATION	11
CHANGES/ENHANCEMENT	11
FIRMWARE VERSION 1.0.21.15	12
PRODUCT NAME	12
DATE	12
FIRMWARE FILE INFORMATION	12
CHANGES/ENHANCEMENT	12
FIRMWARE VERSION 1.0.21.14/15	13
PRODUCT NAME	13
DATE	13
FIRMWARE FILE INFORMATION	13
CHANGES/ENHANCEMENT	13
NEW FEATURE OVERVIEW.....	13
FIRMWARE VERSION 1.0.21.7	15
PRODUCT NAME	15
DATE	15
FIRMWARE FILE INFORMATION	15
CHANGES/ENHANCEMENT	15
NEW FEATURE OVERVIEW.....	15
FIRMWARE VERSION 1.0.21.6	17
PRODUCT NAME	17
DATE	17
FIRMWARE FILE INFORMATION	17

CHANGES/ENHANCEMENT	17
NEW FEATURE OVERVIEW.....	18
FIRMWARE VERSION 1.0.19.32	24
PRODUCT NAME	24
DATE	24
FIRMWARE FILE INFORMATION	24
CHANGES/ENHANCEMENT	24
FIRMWARE VERSION 1.0.19.29	25
PRODUCT NAME	25
DATE	25
FIRMWARE FILE INFORMATION	25
CHANGES/ENHANCEMENT	25
FIRMWARE VERSION 1.0.19.25	26
PRODUCT NAME	26
DATE	26
FIRMWARE FILE INFORMATION	26
CHANGES/ENHANCEMENT	26
FIRMWARE VERSION 1.0.19.22/23	28
PRODUCT NAME	28
DATE	28
FIRMWARE FILE INFORMATION	28
CHANGES/ENHANCEMENT	28
NEW FEATURE OVERVIEW.....	29
FIRMWARE VERSION 1.0.19.15	31
PRODUCT NAME	31
DATE	31
FIRMWARE FILE INFORMATION	31
CHANGES/ENHANCEMENT	31
FIRMWARE VERSION 1.0.19.14	32
PRODUCT NAME	32
DATE	32
FIRMWARE FILE INFORMATION	32
CHANGES/ENHANCEMENT	32
FIRMWARE VERSION 1.0.19.9	34

PRODUCT NAME	34
DATE	34
FIRMWARE FILE INFORMATION	34
CHANGES/ENHANCEMENT	34
FIRMWARE VERSION 1.0.19.5	35
PRODUCT NAME	35
DATE	35
FIRMWARE FILE INFORMATION	35
CHANGES/ENHANCEMENT	35
FIRMWARE VERSION 1.0.19.4	36
PRODUCT NAME	36
DATE	36
FIRMWARE FILE INFORMATION	36
CHANGES/ENHANCEMENT	36
NEW FEATURE OVERVIEW.....	38
FIRMWARE VERSION 1.0.15.18	44
PRODUCT NAME	44
DATE	44
FIRMWARE FILE INFORMATION	44
CHANGES/ENHANCEMENT	44
FIRMWARE VERSION 1.0.15.18 & 1.0.15.20	45
PRODUCT NAME	45
DATE	45
FIRMWARE FILE INFORMATION	45
CHANGES/ENHANCEMENT	46
FIRMWARE VERSION 1.0.15.15	47
PRODUCT NAME	47
DATE	47
IMPORTANT UPGRADING NOTE.....	47
FIRMWARE FILE INFORMATION	47
PRODUCT LIMITATION	47
CHANGES/ENHANCEMENT	48
FIRMWARE VERSION 1.0.15.4 & 1.0.15.6	49
PRODUCT NAME	49
DATE	49

IMPORTANT UPGRADING NOTE.....	49
FIRMWARE FILE INFORMATION	49
CHANGES/ENHANCEMENT	49
NEW FEATURE OVERVIEW.....	50
FIRMWARE VERSION 1.0.11.8.....	52
PRODUCT NAME	52
DATE	52
FIRMWARE FILE INFORMATION	52
CHANGES/ENHANCEMENT	52
FIRMWARE VERSION 1.0.11.2.....	53
PRODUCT NAME	53
DATE	53
FIRMWARE FILE INFORMATION	53
CHANGES/ENHANCEMENT	53
NEW FEATURE OVERVIEW.....	54
FIRMWARE VERSION 1.0.9.13	56
PRODUCT NAME	56
DATE	56
FIRMWARE FILE INFORMATION	56
CHANGES/ENHANCEMENT	56
FIRMWARE VERSION 1.0.9.12	57
PRODUCT NAME	57
DATE	57
FIRMWARE FILE INFORMATION	57
CHANGES/ENHANCEMENT	57
NEW FEATURE OVERVIEW.....	57
FIRMWARE VERSION 1.0.8.18	62
PRODUCT NAME	62
DATE	62
FIRMWARE FILE INFORMATION	62
IMPORTANT UPGRADING NOTE.....	62
CHANGES/ENHANCEMENT	62
NEW FEATURE OVERVIEW.....	63
FIRMWARE VERSION 1.0.8.9	66
PRODUCT NAME	66

DATE	66
FIRMWARE FILE INFORMATION	66
CHANGES/ENHANCEMENT	66
NEW FEATURE OVERVIEW.....	66
FIRMWARE VERSION 1.0.7.13	68
PRODUCT NAME	68
DATE	68
FIRMWARE FILE INFORMATION	68
IMPORTANT UPGRADING NOTE.....	68
CHANGES/ENHANCEMENT	69
NEW FEATURE OVERVIEW.....	69
[GWN7610]FIRMWARE VERSION 1.0.6.43.....	75
PRODUCT NAME	75
DATE	75
FIRMWARE FILE INFORMATION	75
ENHANCEMENT	75
NEW FEATURE OVERVIEW.....	76
[GWN7600&7600LR]FIRMWARE VERSION 1.0.6.41	79
PRODUCT NAME	79
DATE	79
FIRMWARE FILE INFORMATION	79
ENHANCEMENT	79
IMPORTANT UPGRADING NOTE.....	79
NEW FEATURE OVERVIEW.....	80
[GWN7610]FIRMWARE VERSION 1.0.5.15.....	83
PRODUCT NAME	83
DATE	83
IMPORTANT UPGRADING NOTE.....	83
ENHANCEMENT	83
BUG FIX	83
NEW FEATURE OVERVIEW.....	83
[GWN7600&7600LR]FIRMWARE VERSION 1.0.5.13	89
PRODUCT NAME	89
DATE	89
FIRMWARE FILE INFORMATION	89
IMPORTANT UPGRADING NOTE.....	89

ENHANCEMENT	89
BUG FIX	90
KNOWN ISSUE.....	90
NEW FEATURE OVERVIEW.....	90
[GWN7610]FIRMWARE VERSION 1.0.4.22	96
PRODUCT NAME	96
DATE	96
BUG FIX	96
[GWN7610]FIRMWARE VERSION 1.0.4.20	97
PRODUCT NAME	97
DATE	97
IMPORTANT UPGRADING NOTE.....	97
ENHANCEMENT	97
BUG FIX	97
KNOWN ISSUE.....	98
NEW FEATURE OVERVIEW.....	98
[GWN7600&7600LR]FIRMWARE VERSION 1.0.4.12	101
PRODUCT NAME	101
DATE	101
ENHANCEMENT	101
BUG FIX	101
KNOWN ISSUE.....	102
NEW FEATURE OVERVIEW.....	102
[GWN7600&7600LR]FIRMWARE VERSION 1.0.3.25	105
PRODUCT NAME	105
DATE	105
IMPORTANT UPGRADING NOTE.....	105
BUG FIX	105
KNOWN ISSUE.....	106
[GWN7610]FIRMWARE VERSION 1.0.3.21	107
PRODUCT NAME	107
DATE	107
IMPORTANT UPGRADING NOTE.....	107
ENHANCEMENT	107
BUG FIX	107
KNOWN ISSUE.....	107

[GWN7600&7600LR]FIRMWARE VERSION 1.0.3.19 108

PRODUCT NAME 108
 DATE 108
 ENHANCEMENT 108
 BUG FIX 108
 KNOWN ISSUE..... 109
 NEW FEATURE OVERVIEW..... 109

[GWN7610]FIRMWARE VERSION 1.0.3.19 115

PRODUCT NAME 115
 DATE 115
 IMPORTANT UPGRADING NOTE..... 115
 ENHANCEMENT 115
 BUG FIX 115
 KNOWN ISSUE..... 116
 NEW FEATURE OVERVIEW..... 116

[GWN7610]FIRMWARE VERSION 1.0.2.108..... 119

PRODUCT NAME 119
 DATE 119
 IMPORTANT UPGRADING NOTE..... 119
 ENHANCEMENT 119
 KNOWN ISSUE..... 119
 NEW FEATURE OVERVIEW..... 120

[GWN7600&7600LR]FIRMWARE VERSION 1.0.1.36 122

PRODUCT NAME 122
 DATE 122
 IMPORTANT UPGRADING NOTE..... 122

[GWN7610]FIRMWARE VERSION 1.0.2.15..... 123

PRODUCT NAME 123
 DATE 123
 IMPORTANT UPGRADING NOTE..... 123

[GWN7602] FIRMWARE VERSION 1.0.19.34

PRODUCT NAME

GWN7602

DATE

4/4/2022

FIRMWARE FILE INFORMATION

- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: 320a03cbd35f1ab015a74bb023cb5890

CHANGES/ENHANCEMENT

- Enabled band 3 and band 4 channels for Israel

FIRMWARE VERSION 1.0.21.16

PRODUCT NAME

GWN7660 / GWN7664

DATE

2/24/2022

FIRMWARE FILE INFORMATION

- GWN7660 Firmware file name: gwn7660fw.bin
MD5 checksum: 040e78c4cc84cd4001ec9fd5a740fa7f
- GWN7664 Firmware file name: gwn7664fw.bin
MD5 checksum: 2b220767ed88abcd6218240747c134ae

CHANGES/ENHANCEMENT

- Fixed a radio issue that US module of GWN7660&7664 may not be able to select DFS channel.
- Internal bug fixes

FIRMWARE VERSION 1.0.21.15

PRODUCT NAME

GWN7630 / GWN7630LR

DATE

1/19/2022

FIRMWARE FILE INFORMATION

- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin – 1.0.21.15
MD5 checksum: 89f9df9ca91e25ed3ba8f21d2b81bae8

CHANGES/ENHANCEMENT

- Added support of **Hotspot 2.0 R3^{Beta}** for GWN7630/GWN7630LR

FIRMWARE VERSION 1.0.21.14/15

PRODUCT NAME

GWN7605 / GWN7605LR / GWN7615 / GWN7630 / GWN7630LR / GWN7660 / GWN7664

DATE

1/7/2022

FIRMWARE FILE INFORMATION

- GWN7615 Firmware file name: gwn7615fw.bin – 1.0.21.14
MD5 checksum: 84811f268ad70fe8cb40b18e5c23a54e
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin – 1.0.21.14
MD5 checksum: d89d9cc7653dcb8cda568c6eff01e944
- GWN7660 Firmware file name: gwn7660fw.bin – 1.0.21.14
MD5 checksum: f83ccfe41843464d429f596cec7c0f87
- GWN7605/7605LR Firmware file name: gwn7605fw.bin – 1.0.21.15
MD5 checksum: 09928b531736123b1efdd4b56fd99be5
- GWN7664 Firmware file name: gwn7664fw.bin – 1.0.21.15
MD5 checksum: ed78b0a7b8a5f54d83adcbd6d58b48ce

CHANGES/ENHANCEMENT


- Added support of **Hotspot 2.0 R3^{Beta}** for GWN7660
- Added support of **Bonjour Gateway**
- Internal bug fixes

NEW FEATURE OVERVIEW

- **Bonjour Gateway**

This feature will allow Bonjour protocol to be broadcast into configured VLAN.

Configuration is available at:

Network → SSID → Edit  → Wi-Fi → Advanced → Enable Bonjour Gateway

FIRMWARE VERSION 1.0.21.7

PRODUCT NAME

GWN7600 / GWN7600LR / GWN7610 / GWN7660

DATE

11/5/2021

FIRMWARE FILE INFORMATION

- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
 MD5 checksum: 9e4f2b4b2acf9f96d650af91e38a0963
- GWN7610 Firmware file name: gwn7610fw.bin
 MD5 checksum: d9e7eda4f64270a5e1800b1f7f71757
- GWN7660 Firmware file name: gwn7660fw.bin
 MD5 checksum: 435d918cc98c429ac3a2036c67169ec7

CHANGES/ENHANCEMENT

- Sync new features of 1.0.21.6 from other models
- Enable FCC **DFS channels** for gwn7660
- Internal bug fixes

NEW FEATURE OVERVIEW

- **DFS channels**

Now SSID max number is separately counter in each band (2.4GHz or 5Ghz). The maximum allowed SSID for each band now is as below:

1.0.21.7	CE	RCM	FCC	IC	ANATEL(Brazil)
GWN7610	-	-	-	-	-
GWN7600	-	-	-	-	Yes
GWN7600LR	Yes	-	-	-	-

1.0.21.7	CE	RCM	FCC	IC	ANATEL(Brazil)
GWN7630	Yes	Yes	Yes	Yes	Yes
GWN7630LR	Yes	Yes	Yes	Yes	-
GWN7602	Yes	Yes	Yes	Yes	Yes
GWN7605	Yes	Yes	Yes	Yes	-
GWN7605LR	Yes	Yes	Yes	Yes	-
GWN7615	Yes	Yes	Yes	Yes	-
GWN7660	Yes	Coming soon	Yes	Coming soon	-

FIRMWARE VERSION 1.0.21.6

PRODUCT NAME

GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

DATE

10/27/2021

FIRMWARE FILE INFORMATION

- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: dbb89a9e9398d7a475c28c8b0f377665
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: d33aa163653518b0f6e4e8c845d3595e
- GWN7615 Firmware file name: gwn7615fw.bin
- MD5 checksum: 6deab7cb22653691db67342e438cd0c2

CHANGES/ENHANCEMENT

- **Upgraded the max number of supported SSIDs**
- **Added Option to turn off U-APSD function**
- **Added feature of reporting Probe request RSSI information** (Requires GWN.Cloud)
- **Added IPv6 support for internal GWN services**
- **Added feature to Transfer AP to GWN manager**
- **Added feature to allow Each AP to disable/Enable 2.4GHz or 5GHz independently**
- **Added feature of TR-069**
- **Added feature of Google Authentication**
- **Added feature to Delete inbound and outbound rules in batches**
- **Added feature to Save network abnormal log to Flash**
- **Added feature of Web lock for failed login**

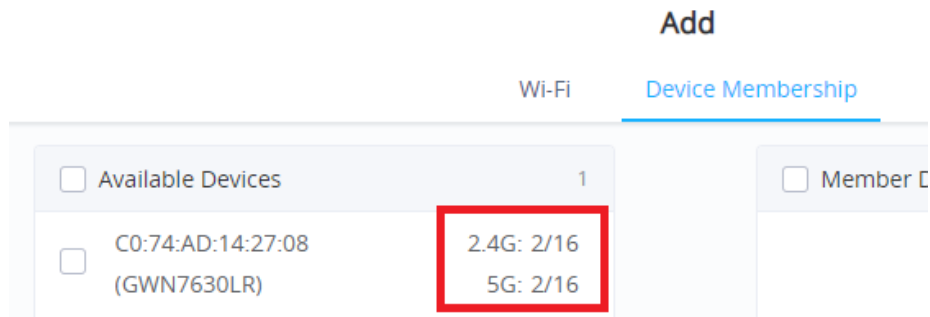
NEW FEATURE OVERVIEW

- **Upgraded the max number of supported SSIDs**

Now SSID max number is separately counter in each band (2.4GHz or 5GHz). The maximum allowed SSID for each band now is as below:

Model	MAX SSID on each band without Mesh/with Mesh
GWN7600/7600LR	16/14
GWN7602	4/4
GWN7605/7605LR	8/6
GWN7610	16/14
GWN7615	16/14
GWN7630/7630LR	16/14
GWN7660/7660LR	16/14
GWN7664	16/14

Interfaces are also updated according to the new limit.



- **Option to turn off U-APSD function**

U-APSD (Unscheduled Automatic Power Save Delivery) now can be turned of by option from

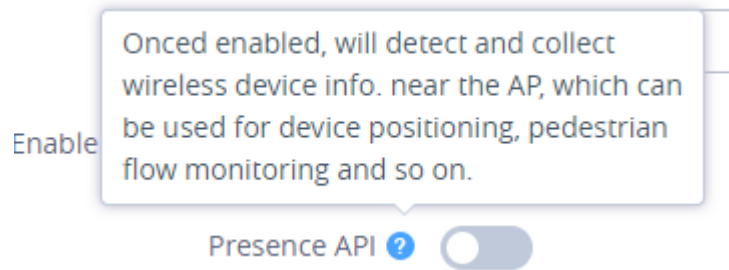
Network → SSID → Edit  → Wi-Fi → Advanced → Enable U-APSD

- **Probe request RSSI information**

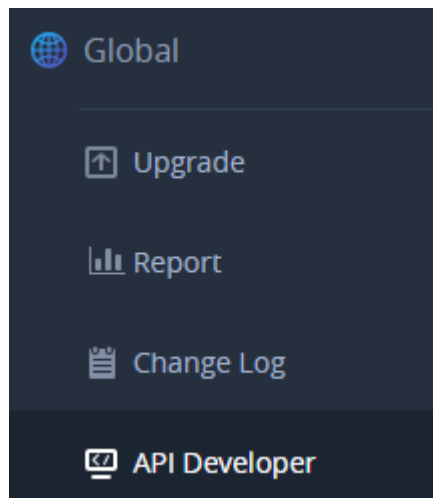
This information is mainly used for client geo analytics, so that further service can be provided based on client location.

To turn on this feature, configuration option is available at GWN.Cloud:

Network→System→Settings→General→Presence API



The API information is available from GWN Cloud



Detail for this API is under API Reference→Client→7. Obtain the signal strength of the clients around the AP

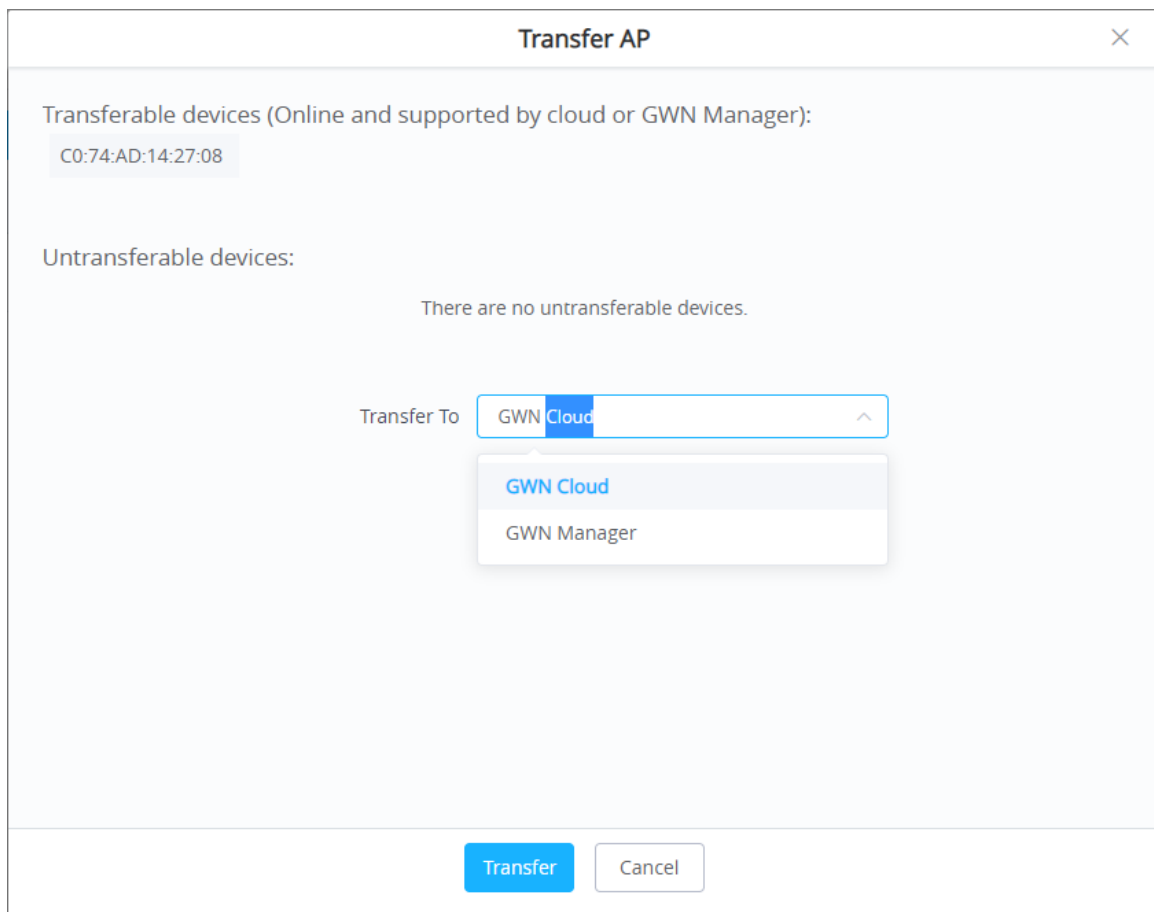
- **IPv6 support for internal GWN services**

Now GWN AP will not only pass IPv6 packets, AP will be able to take IPv6 address for internal services. If dynamic IPv6 assignment is not available in your network, you can configure static IPv6 address on AP management interface. Configuration is available at

Access Point→Configuration→Edit  →Fixed IPv6

- **Transfer AP to GWN manager**

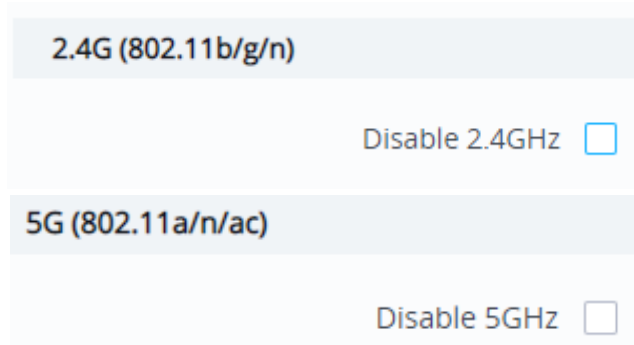
GWN manager option is available in Transfer AP feature now.



- **Each AP to disable/Enable 2.4GHz or 5GHz independently**

Each AP now can independently disable/enable its 2.4GHz band or 5GHz band.

Configuration option is available at Access Point → Configuration → Edit  → 2.4G/5G



- **TR-069**

Configuration options are available at Service→TR069.

TR-069 feature is mutual exclusive to some GWN.Cloud and Master features. For detail please refer to GWN User Manual.

Enable TR-069

ACS URL

ACS User Name

ACS Password

Periodic Inform Enable

Periodic Inform Interval (s)

CPE Cert File

CPE Cert Key

- **Google Authentication**

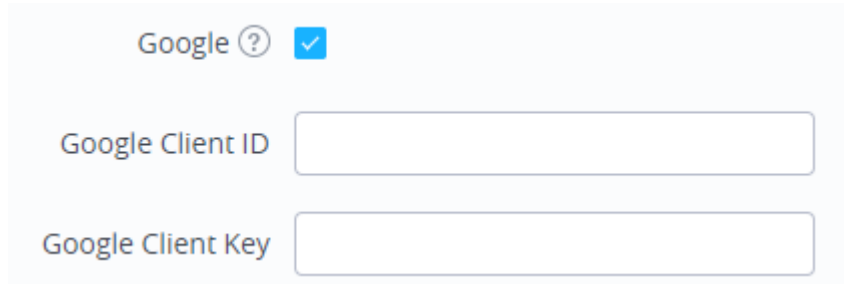
Google Authentication now is added to Captive Portal. Related configuration options are available at Captive Portal→Policy List→Add/Edit→Basic

Select Authentication Type to Social Login Authentication, and then you can select Google.

Next, you will need to configure on Google cloud platform,

Go to <https://console.developers.google.com/apis/credentials>, and setup your App.

Retrieve you Client ID and Client Key and copy them onto your GWN.



Google

Google Client ID

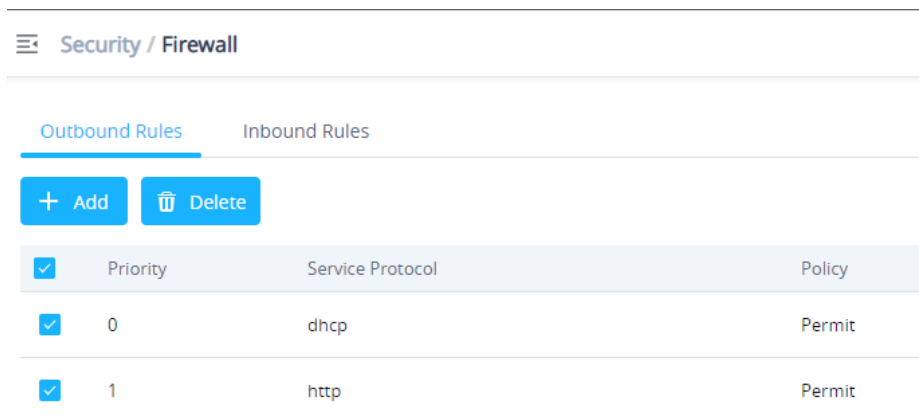
Google Client Key

Meanwhile configurate your Oauth redirect URI:

'https://cwp.gwn.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=4'.

- **Delete inbound and outbound rules in batches**

Now you can delete inbound/outbound rules in batches by checking the box in front of the rules.



Security / Firewall

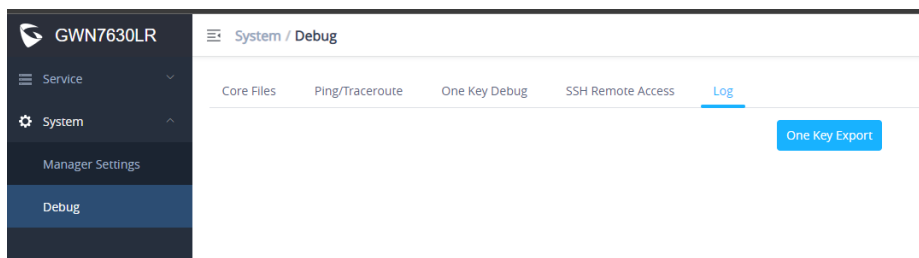
Outbound Rules Inbound Rules

+ Add Delete

<input checked="" type="checkbox"/>	Priority	Service Protocol	Policy
<input checked="" type="checkbox"/>	0	dhcp	Permit
<input checked="" type="checkbox"/>	1	http	Permit

- **Save network abnormal log to Flash**

When slave APs lost upper link network to its Master, Master will have no way to get log from Slaves. This scenario is especially common during a Mesh network troubleshooting. Now, with this feature, network can login slave AP's webUI to retrieve the log from interface below:



GWN7630LR

System / Debug

Core Files Ping/Traceroute One Key Debug SSH Remote Access Log

One Key Export

- **Web lock for failed login**

Now, GWN AP's webUI access will be locked for 15 mins after 5 login failures.

FIRMWARE VERSION 1.0.19.32

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

7/15/2021

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 3523fcfccbf1d0ad3a06cb4389340fdb
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: b576f7bd25f3728574c885acdb2bd8a4
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 9e37d1d485ba06bc990cc93540a18123
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: a3fcb6dcfbfb086ec89c2c9d59bee6df
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: ebaa7f81a22e33829e1db4d23ee9e9df
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: 14883d6401e978630d250ad32f7af563

CHANGES/ENHANCEMENT

- Fixed the security issue from Wi-Fi FragAttacks (GWN7610 / GWN7600 / GWN7600LR).
- Fixed a NAT issue causing some client with fixed IP unable to access external network.
- Fixed a MESH link issue caused by ipv6 environment.

FIRMWARE VERSION 1.0.19.29

PRODUCT NAME

GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

DATE

6/4/2021

FIRMWARE FILE INFORMATION

- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: a741ea98e0248271a61cdc331a77cc0d
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: c9c8d6b79c38b917351192b8f6061957
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: b86e8467e3a88470456f0f7b151be7a0

CHANGES/ENHANCEMENT

- Fixed the security issue from Wi-Fi FragAttacks (GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615).

FIRMWARE VERSION 1.0.19.25

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

3/29/2021

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 033447bf5c51f20099bbf1e3b35dfde8
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 2e5200b8b62891f456fbef68e5613eef
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 8b3528dfb29a671f6fa588cf12df3798
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: 013e13b41757790c3f4ec84decb67fde
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: 1db0b79c378d3071e9d8846fdf0bff82
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: f2f2477224dca9a29d14ad07c17cdf3a

CHANGES/ENHANCEMENT

- Fixed an issue of GWN7602 LAN port incorrect status display.
- Fixed an issue that GWN7630 broadcast an unknown SSID when client bridge is setup.
- Fixed an issue that causes AP to go offline when channel width is changed.

- Fixed an issue of Email SMTP settings not working.
- Fixed an issue of GWN7605lr's 5G radio interface incorrect when Country/Region select Europe and Scene select outdoor.
- Fixed an issue that causes WP810 disconnection when roaming between GWN APs.
- Internal bug fixes.

FIRMWARE VERSION 1.0.19.22/23

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

2/3/2021

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin - 1.0.19.23
MD5 checksum: ecb2557fd35d59515c7751a3cadd9f9d
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin - 1.0.19.23
MD5 checksum: 3a53f81c433bec5a9d158e26b47ee25f
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin - 1.0.19.22
MD5 checksum: 841cdd8ce3ce1bd997d725926239b9de
- GWN7602 Firmware file name: gwn7602fw.bin - 1.0.19.22
MD5 checksum: 638ac9849fafad42cce401576466a508
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin - 1.0.19.22
MD5 checksum: 990963089c1eb2c81f0dda9618d1691d
- GWN7615 Firmware file name: gwn7615fw.bin - 1.0.19.22
MD5 checksum: 8d27194e45c15d78dae61865363a08d5

CHANGES/ENHANCEMENT

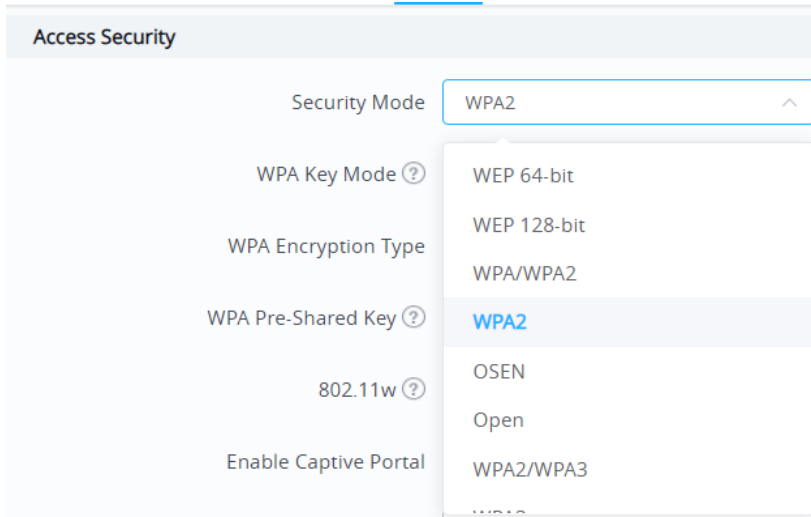
- Added support of **WPA3** (gwn7600/7600lr/7610/7602 does NOT support)
- Added support of **Secondary RADIUS Server**
- Added support of **Rogue AP Alert**

- Added support of **NET port VLAN settings** (gwn7600/7600lr/7610 does NOT support)

NEW FEATURE OVERVIEW

- **WPA3**

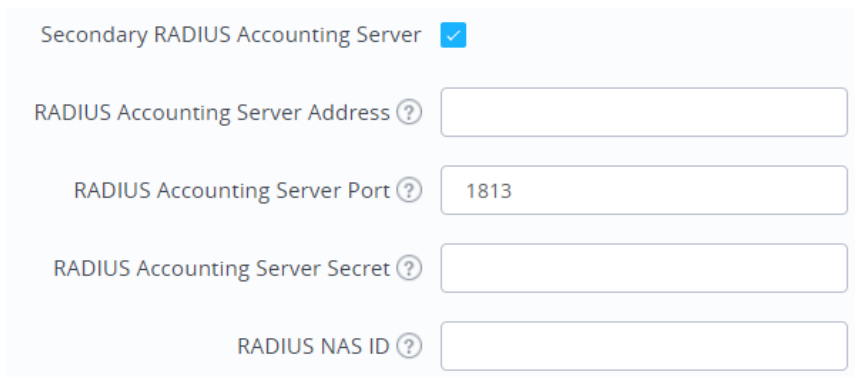
Configuration is available at SSID→Edit→Wi-Fi→Access Security→Security Mode.



The screenshot shows the 'Access Security' configuration page. The 'Security Mode' dropdown menu is open, displaying the following options: WEP 64-bit, WEP 128-bit, WPA/WPA2, **WPA2** (highlighted), OSEN, Open, WPA2/WPA3, and WPA3. The 'WPA Pre-Shared Key' field is also visible.

- **Secondary RADIUS Server**

Configuration is available at SSID→Edit→Wi-Fi→Access Security. Once you choose 802.1x mode, secondary radius server can be configured additional to the primary.



The screenshot shows the configuration fields for a Secondary RADIUS Accounting Server. The 'Secondary RADIUS Accounting Server' checkbox is checked. The fields are: RADIUS Accounting Server Address (empty), RADIUS Accounting Server Port (1813), RADIUS Accounting Server Secret (empty), and RADIUS NAS ID (empty).

- **Rogue AP Alert**

Configuration is available at System→Alert→Alert configuration→Rogue AP.

Email [Alert Configure](#)

Memory Usage

AP Throughput

SSID Throughput

Admin password change

Firmware Upgrade

Rogue AP

AP Offline

[Save](#) [Reset](#)

- **NET port VLAN settings**

Configuration is available at Access Points→Configuration→Edit→NET port Type.

You can configure Trunk port or Access port. When chose Access, you also need to specify its VLAN ID.

NET Port Type

VLAN (NET)

[Access](#)

FIRMWARE VERSION 1.0.19.15

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

1/20/2021

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 8a8265aab6d3bd03b0f76a0e6a73691e
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: a69514b2d275ace4d67c041d0e1a0cb4
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 073577079373c78e9e8f535ffb2d95a3
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: 4a8edca192626f8c13455676912536a0
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: 5b51ddfd8b8f43aa75625298dc1cc187
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: 5170b60090e052f517c9355d995096d5

CHANGES/ENHANCEMENT

- Fixed a RRM bug that failed to adjust power and channel due to adjacent AP detection failure
- Fixed a NAT mode issue causing client cannot get IP address
- Fixed an issue that illegal IP assigned to AP causes AP to go offline

FIRMWARE VERSION 1.0.19.14

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

12/23/2020

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: f1f997996b45afc86a258949152506aa
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 6b2cad61637d70af024501febbfcd615
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: d8c46486e455a952f22cf709627b7a53
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: dcd2c2a4a458a27f4fd8e21ff47edc9
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: a88ee8d9358f44e2ed480f07f113d83ad
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: c1d4e91a9133d932d761a4c680c0f176

CHANGES/ENHANCEMENT

- Fixed a system crash for GWN7630
- Fixed an always offline issue of Mesh RE-AP
- Fixed a bug causes packet random drops on SSID with VLAN tag

- Fixed an AP database issue cause no top statics displays on controller
- Fixed an issue that snmpd could not be stopped, which leads to AP unable to reboot
- Fixed an issue that AP may response on DHCP client discover

FIRMWARE VERSION 1.0.19.9

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

11/23/2020

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 91ff30b55a7bce19b907a062bc5961e5
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: f8c3c17cd66d2bad98cf7f0160b34b5d
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 7677853facb5b3e289f327778223646d
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: ae82645da8244ac4bc2c145340154720
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: ee5d903f4ab6675e2ff7e049c6b8569b
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: c3b579fa79b130ae63bc31ac1469a75a

CHANGES/ENHANCEMENT

- Fixed a system crash
- Fixed TCP connection closes randomly when SSID Mode is set to NAT mode

FIRMWARE VERSION 1.0.19.5

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

10/26/2020

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: a262250fc097ef0b813fb763cfa1e1da
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 8291180c86dbcefc98ce632f19cd55d5
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 23966c749f4c8620ed91886a81cc8aaf
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: b16e2e12cc31af8cc00be07bf402723f
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: 28d6bc126effbb57e751589484d19b76
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: fe9e32ed72a645c2330b4f63818848ae

CHANGES/ENHANCEMENT

- Fixed a memory leak in syslog.

FIRMWARE VERSION 1.0.19.4

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 / GWN7605 /
GWN7605LR / GWN7615

DATE

10/14/2020

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: c65e623737970a8d7c424f1ce3952e6f
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 77720de92704ba7a0f4055c4edc80997
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: a5791f5336690abcdebea8f909c0bcd6
- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: ccda6948a0ae687ce8394440fa9f6c38
- GWN7605/GWN7605LR Firmware file name: gwn7605fw.bin
MD5 checksum: 3471df0289af7b0d61d44560e715faba
- GWN7615 Firmware file name: gwn7615fw.bin
MD5 checksum: 81414c1a8b3893def9da843e6f1e7132

CHANGES/ENHANCEMENT

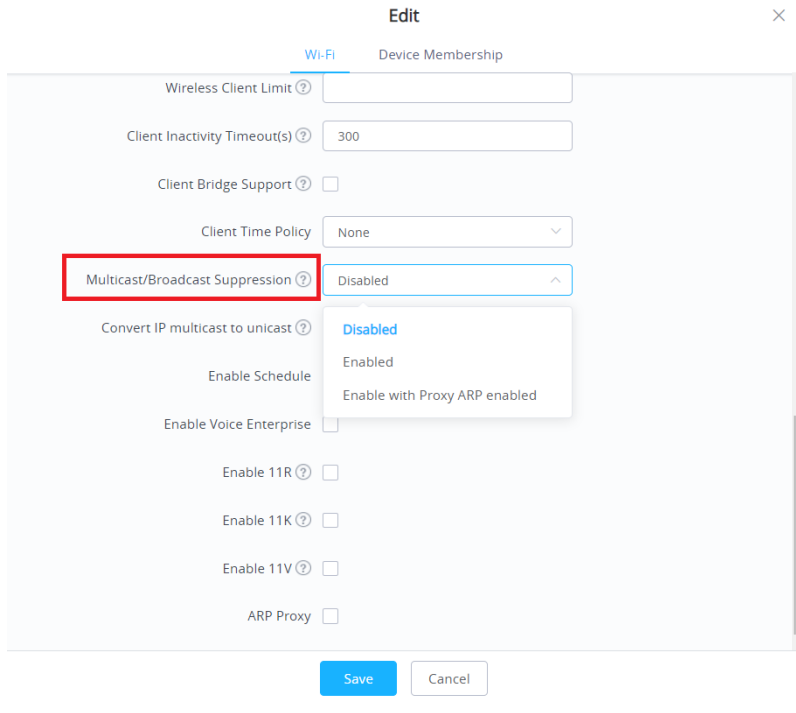
- Added support of **Multicast/Broadcast Suppression**
- Extended support of **RRM** to GWN Cloud and remaining AP models
- Added support of **Active IGMP** for feature Convert IP multicast to unicast enhancement

- Added support of **Rogue AP Detection**
- Added support of **802.11w**
- Added support of **Auto TX Power**
- Added **Captive Portal Enhancement**
- Added support of **SNMP**
- Added support of **Allow DHCP Option 43 to override GWN Manager Address**
- Added enhancement as **AP local master Email/Notification optimization**
- Added enhancement as **AP local master WebUI optimization**
- Added support of more DFS Channels
- **FCC and IC DFS** for 7605/7605LR/7615
ANATEL(Brazil) DFS for 7600/7630/7602
- Added support of **NAT** (GWN7610 not supported)
- Added support of **Firewall**
- Added support of **Hotspot 2.0^{Beta}** (GWN7610 & GWN7602 not supported)

NEW FEATURE OVERVIEW

- **Multicast/Broadcast Suppression**

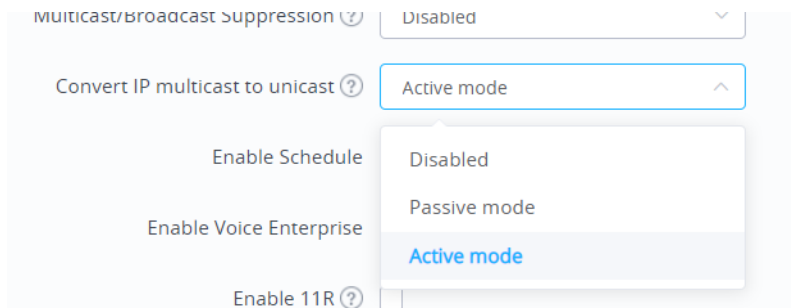
Broadcast or Multicast packet consumes a lot of air bandwidth. By enable Multicast/Broadcast Suppression, all the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND. Enable with ARP Proxy is also available. Configuration is available at SSIDs→Wi-Fi→Advanced as below:



The screenshot shows the 'Edit' configuration window for Wi-Fi settings. The 'Multicast/Broadcast Suppression' dropdown menu is open, showing options: Disabled, Enabled, and Enable with Proxy ARP enabled. The 'Disabled' option is currently selected. Other visible settings include Wireless Client Limit, Client Inactivity Timeout(s) (300), Client Bridge Support, Client Time Policy (None), Convert IP multicast to unicast (Disabled), Enable Schedule, Enable Voice Enterprise, Enable 11R, Enable 11K, Enable 11V, and ARP Proxy.

- **Active IGMP**

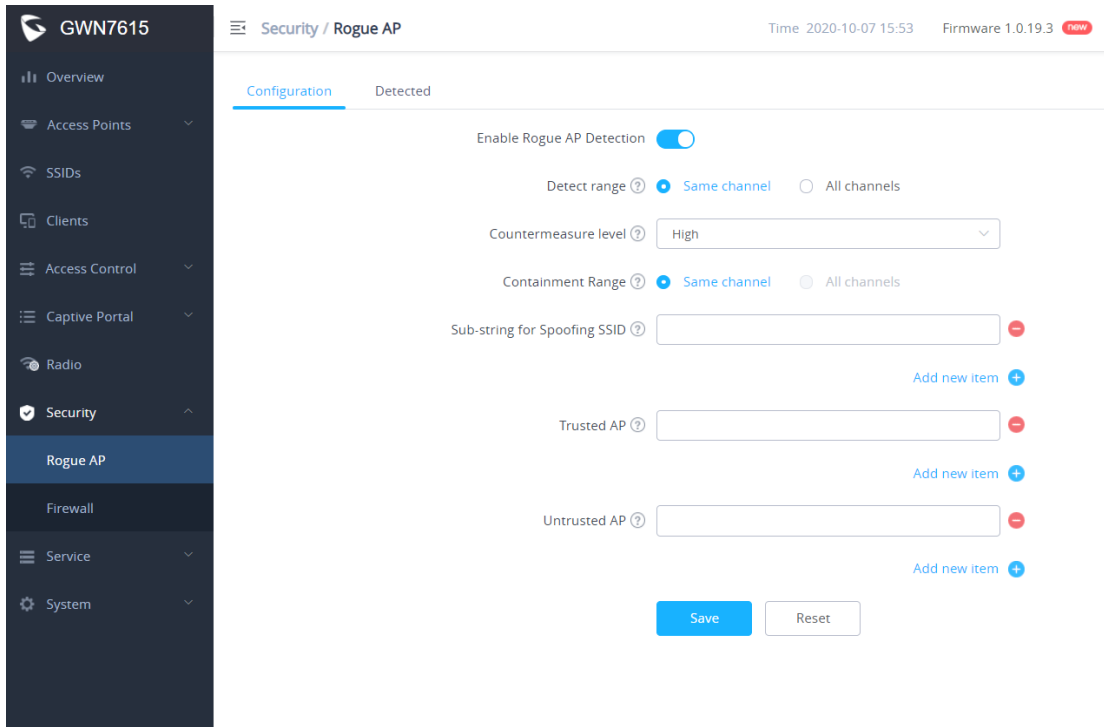
This option will optimize the multicast to unicast feature in the case that there is no multicast router in LAN. By enable it, AP will initiatively broadcast IGMP queries to keep updating of the IGMP snooping items. Configuration is available at SSIDs→Wi-Fi→Advanced.



The screenshot shows the configuration window with the 'Convert IP multicast to unicast' dropdown menu open. The 'Active mode' option is selected. Other visible settings include Multicast/Broadcast Suppression (Disabled), Enable Schedule, Enable Voice Enterprise, and Enable 11R.

- **Rogue AP Detection**

New security feature to detect rogue AP in the service area.



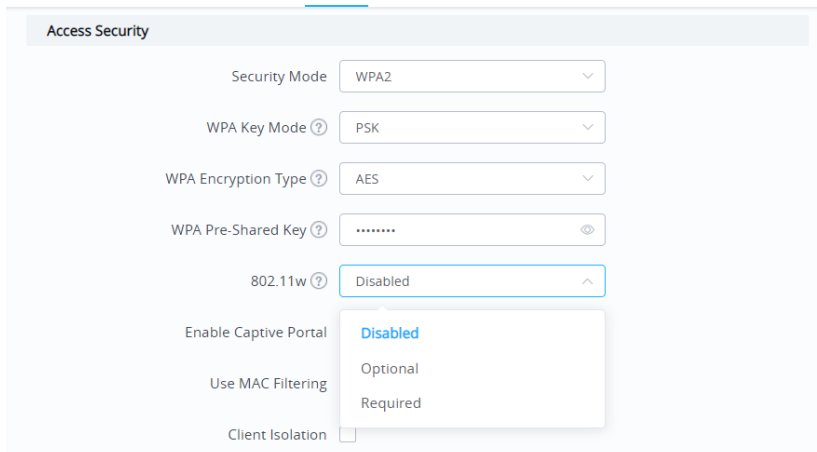
- **802.11w**

Configuration is available under SSIDs→Wi-Fi→Access Security.

2 modes are available for 802.11w: Optional and Required.

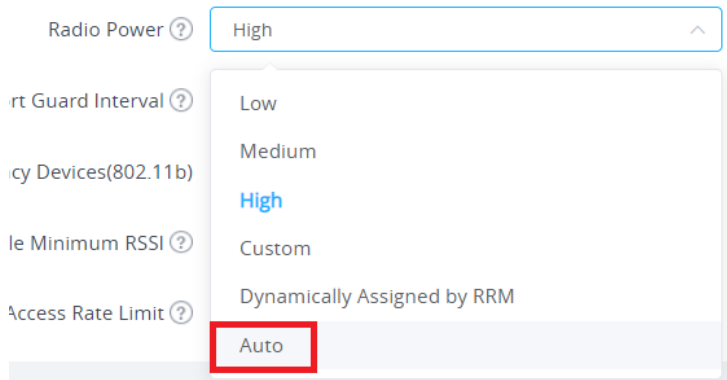
Optional: Either 802.11w supported or unsupported clients can have the network access authority.

Required: only the client supported 802.11w have the network access authority.



- **Auto TX Power**

Configuration is available under Radio→2.4G/5G→Radio Power



The screenshot shows a configuration interface with a dropdown menu for 'Radio Power'. The dropdown is open, showing options: Low, Medium, High (highlighted in blue), Custom, and Dynamically Assigned by RRM. Below these options, the 'Auto' option is highlighted with a red rectangular box.

- **Captive Portal Enhancement**

- 1) Enable HTTPS Function Optimization

Original "Enable HTTPS" is divided into two options

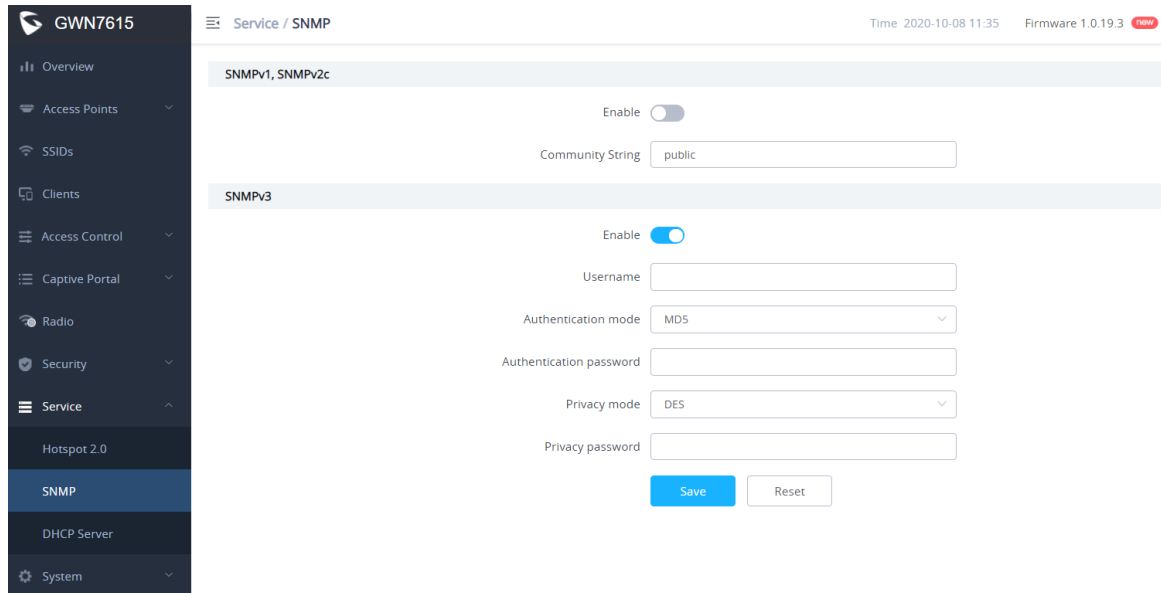
- a. Enable HTTPS Redirection: If enabled, both HTTP and HTTPS requests sent from stations will be redirected by using HTTPS protocol. And station may receive an invalid certification error while doing HTTPS browsing before authentication. If disabled, only the http request will be redirected.
- b. Enable Secure Portal: If enabled, unauthorized guests will be redirected to the splash page by using HTTPS protocol. If not, the HTTP protocol will be used.

- 2) New option - Idle Timeout: Specify the idle timeout value for guest network connection. Once timed out, guest should re-authenticate for further network use. Please note that this option is not applicable to voucher guests.

- 3) Portal Page loading optimization: resolved some loading issue

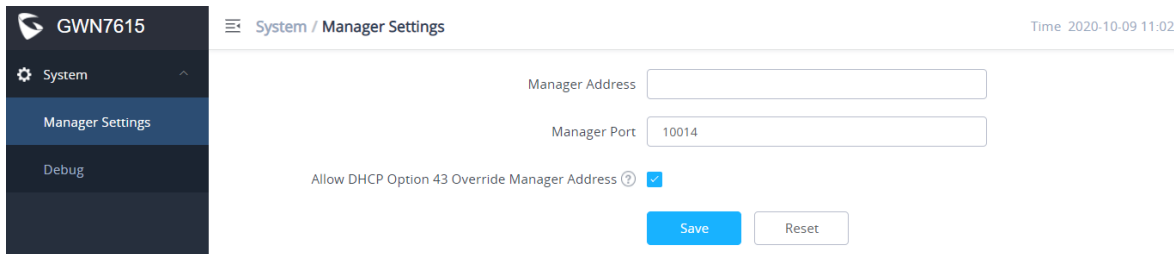
- **SNMP**

Configuration is available under Service→SNMP



- **Allow DHCP Option 43 to override GWN Manager Address**

This configuration is available when admin login in Slave mode. It is enabled by default.



- **AP local master Email/Notification optimization**

Now Master AP centralize all events from slaves and send Email/Notification events, instead of having each slave send independently.

- **AP local master WebUI optimization**

Now local master WebUI matches GWN Cloud and GWN Manager WebUI.

- **FCC and IC DFS** for 7605/7605LR/7615

ANATEL(Brazil) DFS for 7600/7630/7602

Below it the current DFS table for GWN APs as of 1.0.19.4

1.0.19.4	CE	RCM	FCC	IC	ANATEL(Brazil)
GWN7610	-	-	-	-	-
GWN7600	-	-	-	-	Yes
GWN7600LR	Yes	-	-	-	-
GWN7630	Yes	Yes	Yes	Yes	Yes
GWN7630LR	Yes	Yes	Yes	Yes	-
GWN7602	Yes	Yes	Yes	Yes	Yes
GWN7605	Yes	Yes	Yes	Yes	-
GWN7605LR	Yes	Yes	Yes	Yes	-
GWN7615	Yes	Yes	Yes	Yes	-

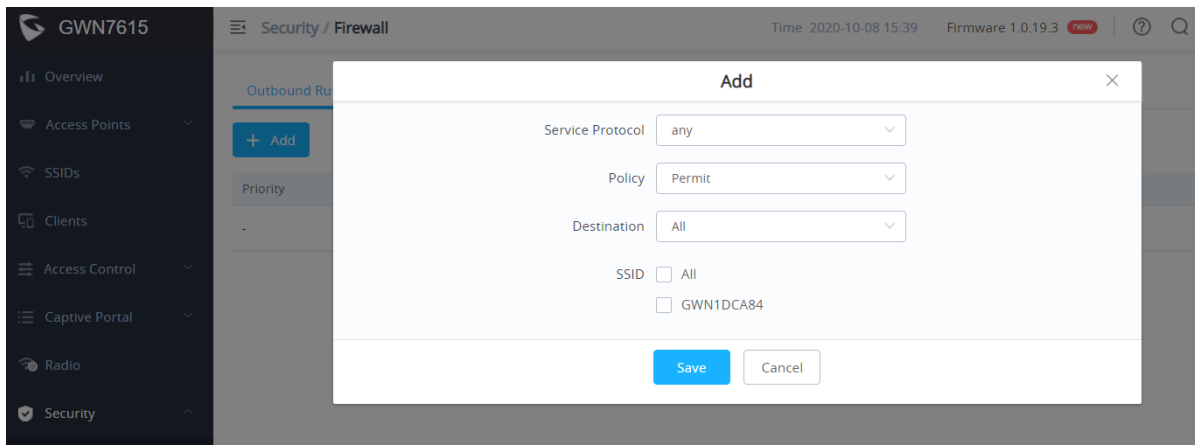
- **NAT** (GWN7610 not supported)

NAT feature is added to GWN AP. Along with DHCP server and firewall feature, GWN AP now can perform as a lightweight home router.

Configuration is available at Service→DHCP Server→NAT Pool

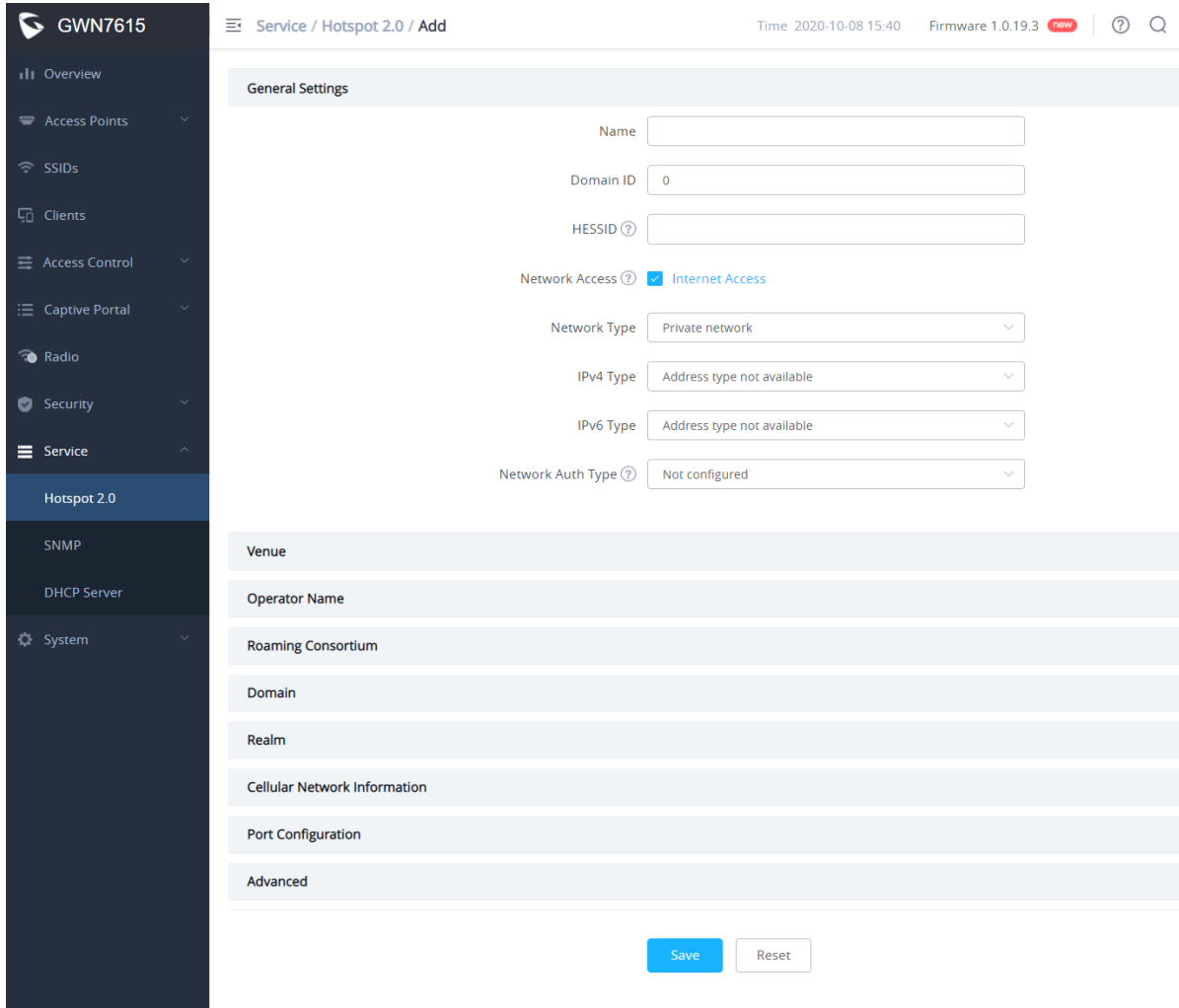
- **Firewall**

Configuration is available at Security→Firewall→Outbound/Inbound Rules



- **Hotspot 2.0** ^{Beta} (GWN7610 & GWN7602 not supported)

Configuration is available at Service→Hotspot 2.0



GWN7615 | Service / Hotspot 2.0 / Add | Time 2020-10-08 15:40 | Firmware 1.0.19.3 New | ? Q

General Settings

Name

Domain ID

HESSID ?

Network Access ? Internet Access

Network Type

IPv4 Type

IPv6 Type

Network Auth Type ?

Venue

Operator Name

Roaming Consortium

Domain

Realm

Cellular Network Information

Port Configuration

Advanced

FIRMWARE VERSION 1.0.15.18

PRODUCT NAME

GWN7605LR / GWN7615 – 1.0.15.18

DATE

6/18/2020

FIRMWARE FILE INFORMATION

- GWN7605LR Firmware file name: gwn7605fw.bin
 MD5 checksum: f2950a672756cf906076965a3bffe3ba
- GWN7615 Firmware file name: gwn7615fw.bin
 MD5 checksum: e57ff82ddac585f005ff327de9fd58f3

CHANGES/ENHANCEMENT

- Added GWN7605LR and GWN7615 two models into GWN AP family

Please refer to below table for the up to date DFS support matrix.

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 – 1.0.15.20 GWN7605 / GWN7605LR / GWN7615 – 1.0.15.18				
6/18/2020	CE	RCM	FCC	IC
GWN7610	-	-	-	-
GWN7600	-	-	-	-
GWN7600LR	Yes	-	-	-
GWN7630	Yes	Yes	Yes	Yes
GWN7630LR	Yes	Yes	Yes	Yes
GWN7602	Yes	Yes	Yes	Yes
GWN7605	Yes	Yes	-	-
GWN7605LR	Yes	Yes	-	-
GWN7615	Yes	Yes	-	-

FIRMWARE VERSION 1.0.15.18 & 1.0.15.20

PRODUCT NAME

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 – 1.0.15.20

GWN7605 – 1.0.15.18

DATE

5/21/2020

FIRMWARE FILE INFORMATION

- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: d490a7c670e15c67698b64949196fe77
- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: d1b97769ef66cde9793a2ec8e763a513
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 54e00a2d6610c690e51822f2f4c29ebd
- GWN7605 Firmware file name: gwn7602fw.bin
MD5 checksum: 2b142615d2598570c65eaec0427a8d5d
- GWN7605 Firmware file name: gwn7605fw.bin
MD5 checksum: f2950a672756cf906076965a3bffe3ba

CHANGES/ENHANCEMENT

- Added support of more DFS channels
- Fixed internal bugs

Please refer to below table for the up to date DFS support matrix.

GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602 – 1.0.15.20 GWN7605 – 1.0.15.18				
5/21/2020	CE	RCM	FCC	IC
GWN7610	-	-	-	-
GWN7600	-	-	-	-
GWN7600LR	Yes	-	-	-
GWN7630	Yes	Yes	Yes	Yes
GWN7630LR	Yes	Yes	Yes	Yes
GWN7602	Yes	Yes	Yes	Yes
GWN7605	Yes	Yes	-	-

FIRMWARE VERSION 1.0.15.15

PRODUCT NAME

GWN7602

DATE

4/24/2020

IMPORTANT UPGRADING NOTE

- Due to the security enhancement, unless Legacy TLS Compatibility (only available on 1.0.15.4 or higher version) is enabled, master AP on 1.0.15.4 or higher firmware will not compatible with slave AP on firmware lower than 1.0.15.4. Master AP on firmware lower than 1.0.15.4 will also not be compatible with slave AP on firmware 1.0.15.4 or higher. Cloud and GWN Manager will still support both firmwares.
- Do not use 1.0.15.x AP firmware with GWN7000 1.0.9.4 or lower version. Only GWN7000 1.0.9.5 or higher supports TLS 1.2.

FIRMWARE FILE INFORMATION

- GWN7602 Firmware file name: gwn7602fw.bin
MD5 checksum: 8546ca24b002c1e429557d7a920a1a3f

PRODUCT LIMITATION

GWN7602 Feature Difference with other GWN APs:

- GWN7602 captive portal does not support https.
- GWN7602 can't be master and can only be slave.
- GWN7602 mesh feature only support Re (Repeater) roll and cannot cascading downward.
- GWN7602 support switching and VLAN on LAN ports.
- GWN7602 only support 4 SSID.

- Right now, other GWN AP's local master has not supported 7602 management yet.
- GWN7602 does not support advance GWN AP features: band steering/client steering/RRM/wireless bridge/airtime fairness/minimum rate.

CHANGES/ENHANCEMENT

- Added LED pattern of yellow to indicate Mesh disconnection
- Added support of FCC DFS for gwn7602
- Added support of CE DFS for gwn7602
- Added support of RCM DFS for gwn7602
- Added support of IC DFS for gwn7602
- Fixed Social Facebook Auth issue
- Fixed TLS Security Issue
- Improved Wi-Fi stability

FIRMWARE VERSION 1.0.15.4 & 1.0.15.6

PRODUCT NAME

GWN7300/GWN7630LR - 1.0.15.6

GWN7610/GWN7600/GWN7600LR – 1.0.15.4

DATE

3/16/2020

IMPORTANT UPGRADING NOTE

- Due to the security enhancement, unless Legacy TLS Compatibility (only available on 1.0.15.4 or higher version) is enabled, master AP on 1.0.15.4 or higher firmware will not compatible with slave AP on firmware lower than 1.0.15.4. Master AP on firmware lower than 1.0.15.4 will also not be compatible with slave AP on firmware 1.0.15.4 or higher. Cloud and GWN Manager will still support both firmwares.
- Do not use 1.0.15.x AP firmware with GWN7000 1.0.9.x or lower version.

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 907ec3840d2f85e35ef6498a0f1e19c6
- GWN7600/GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: a735272124f62b34ab90a286200a705e
- GWN7630/GWN7630LR Firmware file name: gwn7630fw.bin
MD5 checksum: 8d5cea02bea2ea5e6aff299d3995ba02

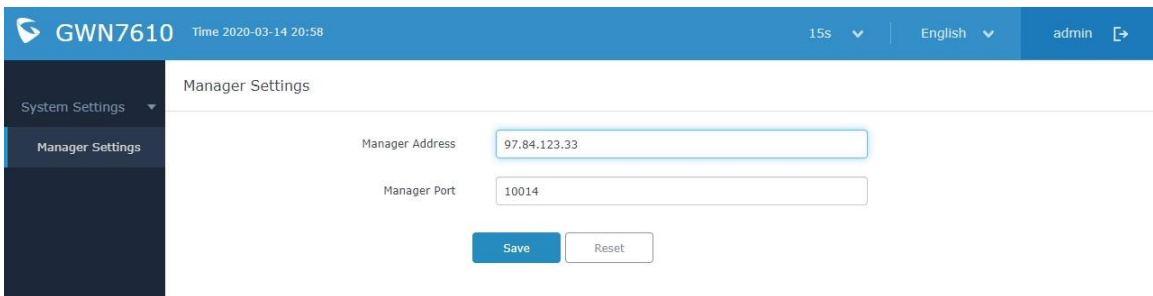
CHANGES/ENHANCEMENT

- Added **Support for GWN Manager**
- Added support for **FCC DFS channels** on gwn7630/gwn7630lr

- Added LED pattern of yellow to indicate Mesh disconnection
- **Security enhancement: Upgraded TLS to version 1.2**
- Internal bug fixes

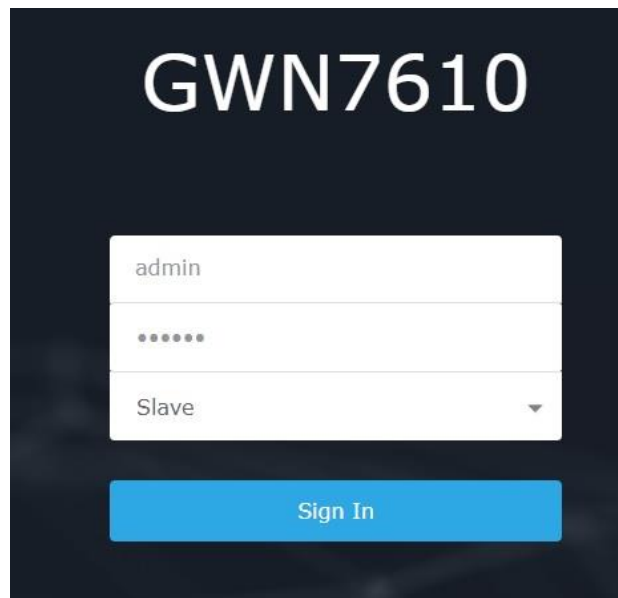
NEW FEATURE OVERVIEW

- **Support for GWN Manager**
 - 1) Now APs can be discovered by GWN Manager.
 - 2) With the support for GWN Manager being added, a layer 3 discovery feature has been added too.



The screenshot shows the 'Manager Settings' page in the GWN7610 web interface. The page has a blue header with the device name 'GWN7610', the time '2020-03-14 20:58', a '15s' timer, 'English' language selection, and an 'admin' user profile. A left sidebar contains 'System Settings' and 'Manager Settings'. The main content area has two input fields: 'Manager Address' with the value '97.84.123.33' and 'Manager Port' with the value '10014'. Below these fields are 'Save' and 'Reset' buttons.

When device boot in factory default, by login in Slave mode, you can add the IP address of your GWN



The screenshot shows the login screen for the GWN7610 device. The background is dark blue with 'GWN7610' in large white text at the top. Below the title is a white login form with three input fields: 'admin' (username), a masked password field with six dots, and a dropdown menu currently set to 'Slave'. A large blue 'Sign In' button is positioned at the bottom of the form.

Manager. After save and apply, it may take few minutes for GWN Manager to be able to adopt the AP.

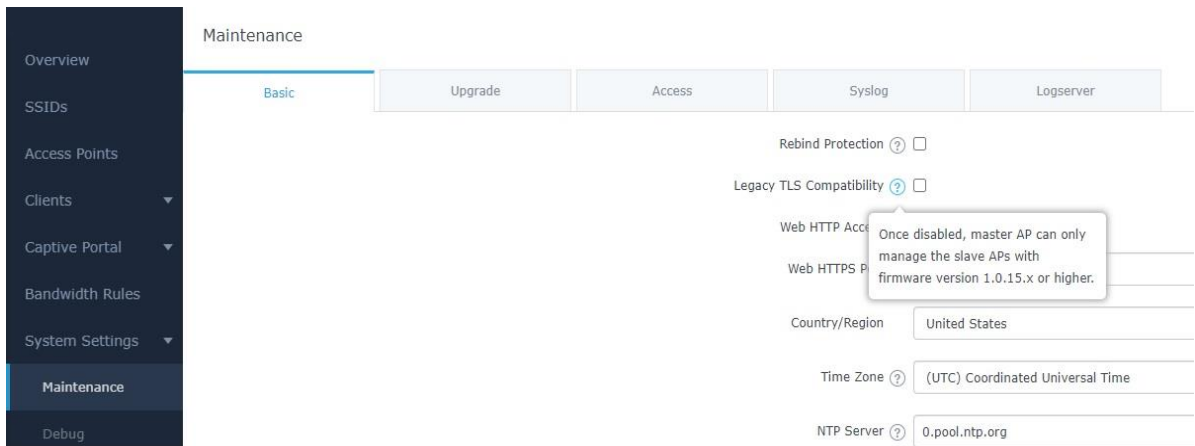
- **FCC DFS channels**

Below is the DFS channel support table for GWN APs.

3/16/2020	CE	FCC
GWN7610	No	No
GWN7600	No	No
GWN7600LR	Yes	No
GWN7630	Yes	Yes
GWN7630LR	Yes	Yes
GWN7602	Yes	No

- **Security enhancement: Upgraded TLS to version 1.2**

Due to the security enhancement, unless **Legacy TLS Compatibility** (only available on 1.0.15.4 or higher version) is enabled, master AP on 1.0.15.4 or higher firmware will not compatible with slave AP on firmware lower than 1.0.15.4. Master AP on firmware lower than 1.0.15.4 will also not be compatible with slave AP on firmware 1.0.15.4 or higher. Cloud and GWN Manager will still support both firmwares.



The screenshot shows the 'Maintenance' section of the Grandstream web interface. The left sidebar contains a menu with 'Maintenance' highlighted. The main content area has tabs for 'Basic', 'Upgrade', 'Access', 'Syslog', and 'Logserver'. Under the 'Basic' tab, there are several settings: 'Rebind Protection' (disabled), 'Legacy TLS Compatibility' (disabled), 'Web HTTP Access' (disabled), 'Web HTTPS Port' (disabled), 'Country/Region' (United States), 'Time Zone' ((UTC) Coordinated Universal Time), and 'NTP Server' (0.pool.ntp.org). A tooltip is displayed over the 'Legacy TLS Compatibility' checkbox, stating: 'Once disabled, master AP can only manage the slave APs with firmware version 1.0.15.x or higher.'

FIRMWARE VERSION 1.0.11.8

PRODUCT NAME

GWN7630

DATE

11/14/2019

FIRMWARE FILE INFORMATION

- GWN7630 Firmware file name: gwn7630fw.bin
MD5 checksum: b62ebfd577024eb6cfb05ce54be7b9e8

CHANGES/ENHANCEMENT

- Added support of DFS channel in EU for GWN7630. Now both GWN7600LR and GWN7630 support DFS channel in EU.
- Internal fix for possible re-association of expired Vouchers.

FIRMWARE VERSION 1.0.11.2

PRODUCT NAME

GWN7610; GWN7600; GWN7600LR; GWN7630

DATE

10/16/2019

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: bc53beca73855b62103797b252aaa2d7
- GWN7600/7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 50bcfa41627545b098ef1cbca0af1ac4
- GWN7630 Firmware file name: gwn7630fw.bin
MD5 checksum: b62ebfd577024eb6cfb05ce54be7b9e8

CHANGES/ENHANCEMENT

- Internal fix for network capture uploading issue from Access Point to Cloud.
- Internal fix for possible re-association of expired Vouchers.
- Added feature of **Site Survey** at GWN Cloud only
- Added feature of **Minimum Rate Control**
- Added feature of **SSH Remote Access**
- Added feature of **External Portal Support Socifi Platform**
- Added feature of **Client inactivity timeout**
- Added feature of **Upgrade Regularly at Cloud**
- Added feature of **Client Steering**^{Beta}: Sticky Client Steering and Load Balancing Steering
- Enhanced feature of **Voucher: display of remaining bytes**
- Enhanced feature of **Takeover: Supports batch operations**

- Enhanced feature of **Dynamic VLAN**
- Changed **LED pattern**
 - When AP is not managed, AP will show solid purple instead of flashing purple
- Changed **Local Master External Portal configuration**
 - Combine all supported platforms into one configuration
- Changed **default setting of Mesh to OFF**
- Removed **Wechat from Wi-Fi portal authentication**
 - Tencent shut down the service.

NEW FEATURE OVERVIEW

- **Site Survey**

This feature will allow Network Administrator to scan the Wi-Fi environment. The scan result will provide useful information for Admin to plan and adjust the Wi-Fi deployment or settings, in order to optimize the Wi-Fi performance of the site.

Site survey is only available on GWN cloud. It's located at **NETWORK→Insight→Site Survey**.

- **Minimum Rate Control**

The settings of this feature are located at **NETWORK→SSIDs→Configuration→Edit→Wi-Fi Settings→Enable Minimum Rate**. By enable this, it will help to eliminated the legacy connection which slow the total performance of the Wi-Fi network.

- **Client Steering^{Beta}**

This feature will help Wi-Fi client to roam to other APs within same Network. Roaming threshold can be configured under **NETWORK→Access Points→Configuration→Edit→Client Steering** by parameters of **RSSI Threshold** and **Client Access Threshold**. Both parameters will show up only when **Client Steering** is enabled.

- **SSH Remote Access**

This feature enables SSH access from GWN cloud to your AP device, and this is mainly for extra troubleshooting method. To enable this, you can find configuration at **NETWORK→Access Points→Status→Click on the AP→Debug**.

- **External Portal Support Socifi Platform**

This is supported by **Universal Platform** configuration under **NETWORK→Captive Portal→Policy List→Add→Splash Page: External→Platform: Universal Platform**.

- **Client inactivity timeout**

This feature will remove the Client record from current Client list, in order to generate accurate report. Default was 300 seconds, and now it's configurable at **NETWORK→SSIDs→Configuration→Edit→Wi-Fi Settings→Client Inactivity Timeout**.

- **Upgrade Regularly at Cloud**

This feature allows APs to check latest firmware and upgrade by a preassigned schedule. Configuration is available at **NETWORK→System→Upgrade→Upgrade Time→Upgrade Regularly**. Schedule is configured at **NETWORK→System→Schedule**.

- **Enhanced feature of Dynamic VLAN**

Now when using 802.1X authentication on your SSID with dynamic VLAN assignment. Admin does not need to create all VLAN SSIDs to match destination VLAN. On 1.0.11.1, AP will trunk its Ethernet with the VLAN assigned to Wi-Fi client through 802.1X.

FIRMWARE VERSION 1.0.9.13

PRODUCT NAME

GWN7610; GWN7600; GWN7600LR;

DATE

6/24/2019

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 1aefac86dc272944c05d2557c63dd190
- GWN7600/7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: f411e92c88a0ede5a48329963ac96682

CHANGES/ENHANCEMENT

- Added new OUI “C0:74:AD” support for GWN7610, GWN7600, and GWN7600LR. GWN7630LR already supported it on 1.0.9.12.

FIRMWARE VERSION 1.0.9.12

PRODUCT NAME

GWN7610; GWN7600; GWN7600LR; GWN7630

DATE

6/11/2019

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: a1c0e58525efa9513c0581dab3059496
- GWN7600/7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: 05fcb911ef517b1ab6e423e7abee5de8
- GWN7630 Firmware file name: gwn7630fw.bin
MD5 checksum: 5cd325ecc1278d547e4643fe00e19330

CHANGES/ENHANCEMENT

- Added feature of **Slave AP Transfer**
- Added feature of **Client Negotiate Speed Display**
- Added feature of **One Key Debugging**
- Enhanced Captive Portal by feature of **HTTPS Portal Trusted Certificate with Auto Update**

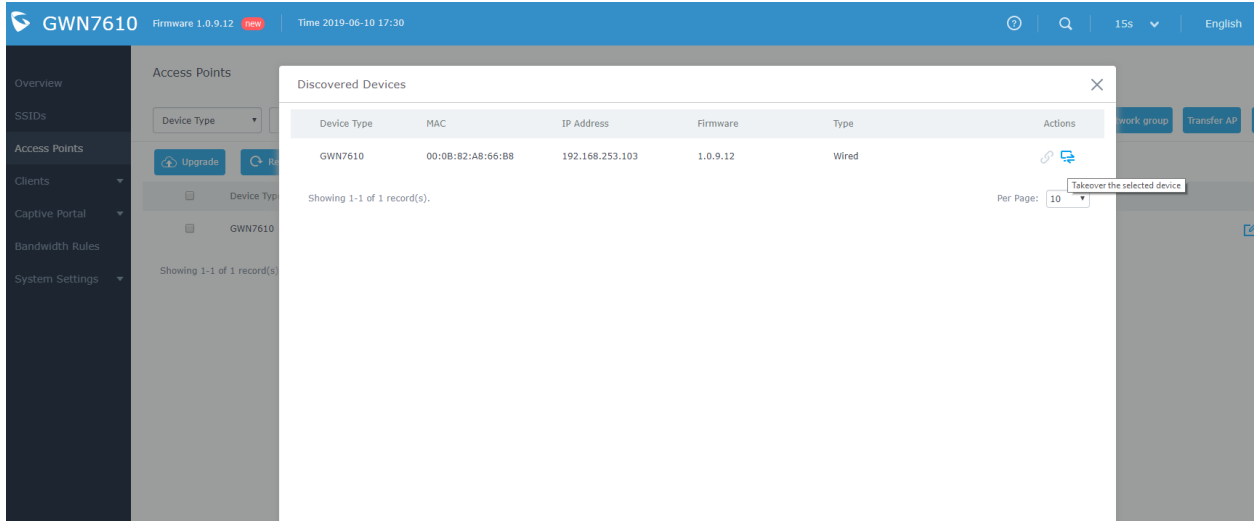
NEW FEATURE OVERVIEW

- **Slave AP Transfer**

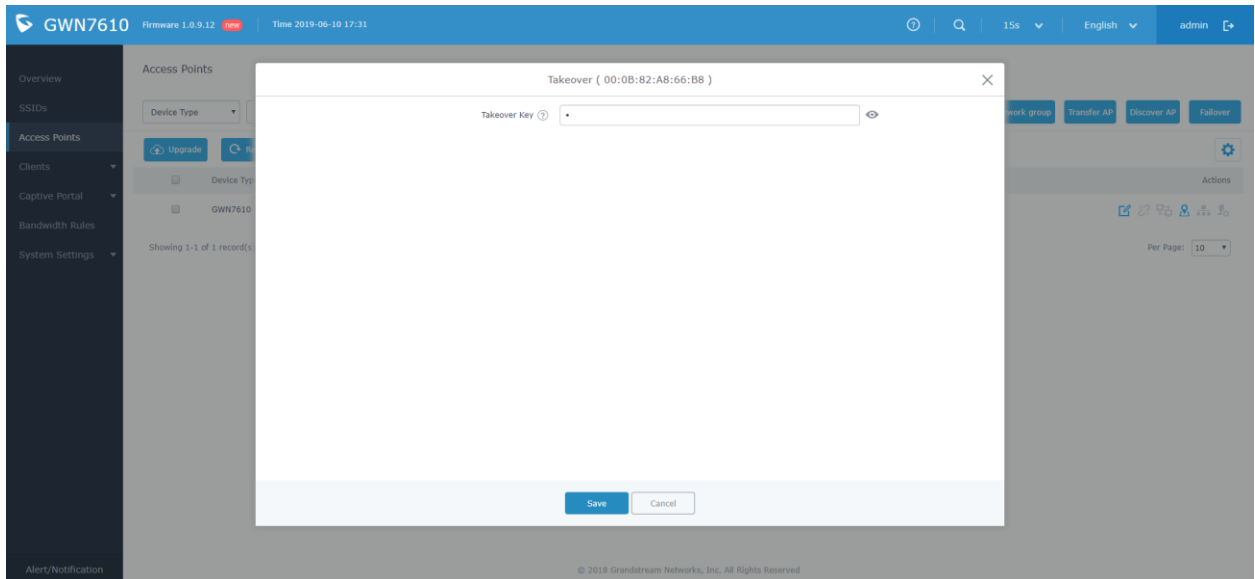
This is an enhancement feature upon **Failover Master**

. Now, when a master fails, even there is no failover master configured, Admin can still bring up a new Master and uses the old master key (admin password) to take over old slaves.

When admin add a new master into the master-failed network. New master will be able to discover the paired old slave as below.

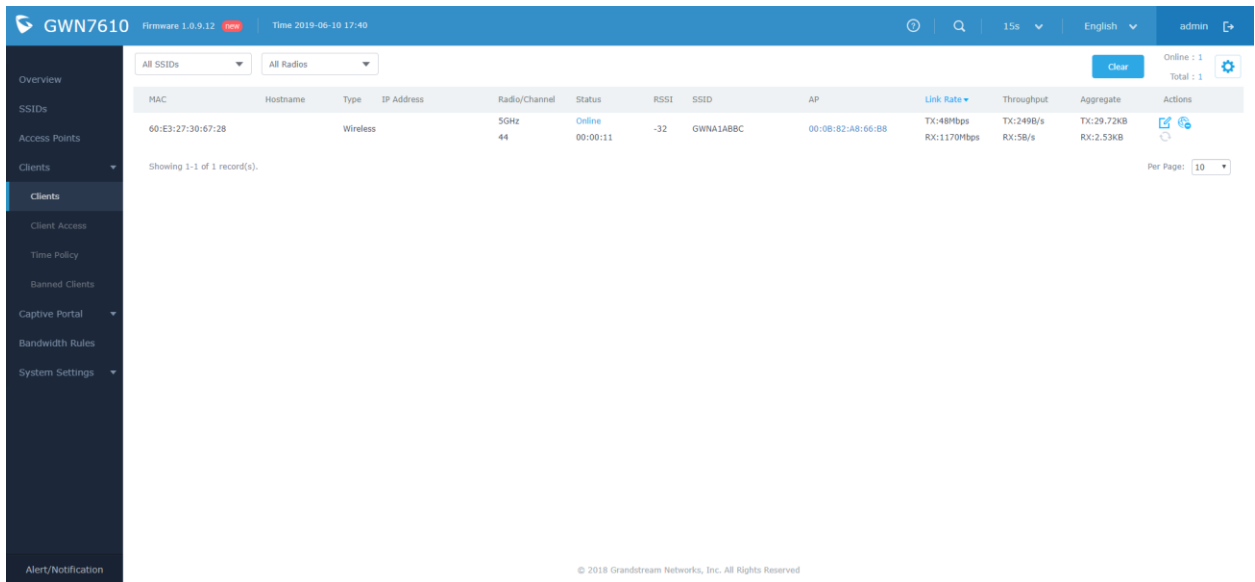


By Clicking on the “Takeover the selected device”, admin will be asked for the takeover key, which is the old master admin password.



Once takeover key is validated, slave AP will be transferred to the new master.

- **Client Negotiate Speed Display**



The screenshot shows the Grandstream GWN7610 web interface. The top navigation bar includes the device name 'GWN7610', firmware version '1.0.9.12', and the time '2019-06-10 17:40'. A sidebar on the left contains navigation options: Overview, SSIDs, Access Points, Clients (selected), Client Access, Time Policy, Banned Clients, Captive Portal, Bandwidth Rules, and System Settings. The main content area displays a table of client information under the 'Clients' section. The table has columns for MAC, Hostname, Type, IP Address, Radio/Channel, Status, RSSI, SSID, AP, Link Rate, Throughput, and Aggregate. A single client record is shown with MAC '60:E3:27:30:67:28', Type 'Wireless', Radio/Channel '44', Status 'Online', RSSI '-32', SSID 'GWINA1ABBC', AP '00:08:82:A8:66:88', and Link Rate 'TX:48Mbps, RX:1170Mbps'. The interface also shows 'Showing 1-1 of 1 record(s)' and 'Per Page: 10'.

This is displayed as **Link Rate** under Clients page.

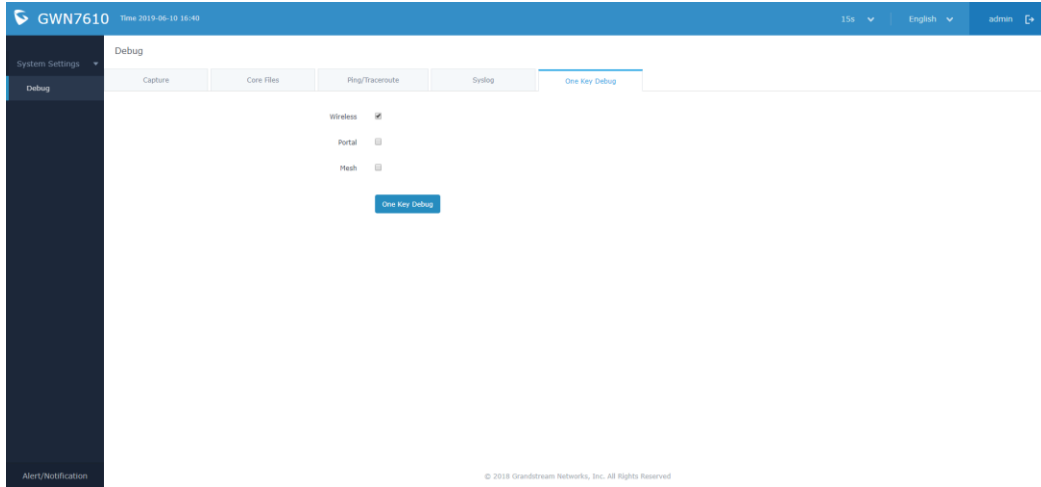
- **One Key Debugging**

For better local troubleshooting data collection, now slave APs all have their own web page login.

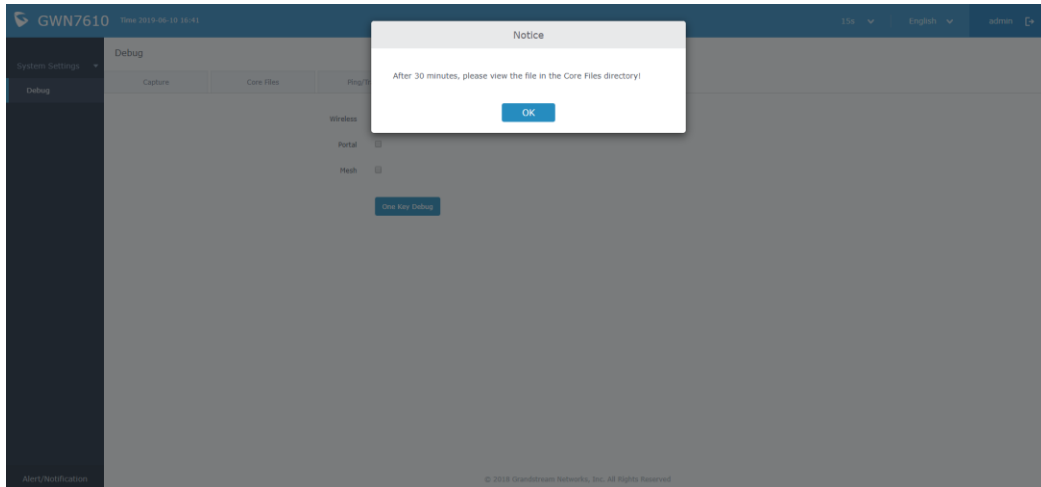


The screenshot shows the Grandstream GWN7610 web interface login screen. The top left corner features the Grandstream logo and 'CONNECTING THE WORLD'. The top right corner shows the language 'English'. The main content area displays 'GWN7610' in large white text. Below this, there are two input fields for 'Username' and 'Password', and a blue 'Sign In' button. At the bottom of the screen, it says 'The AP is paired' and 'All Rights Reserved Grandstream Networks, Inc. 2018'.

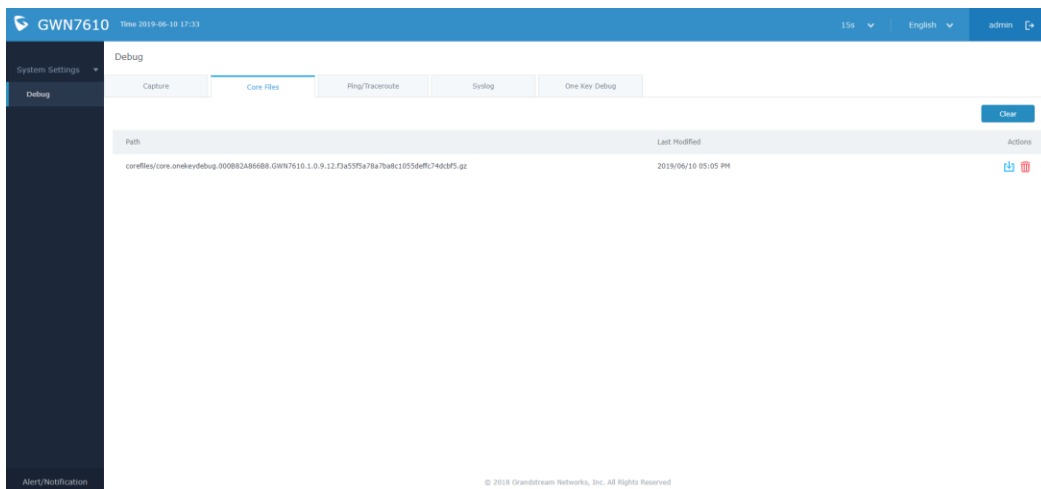
Once login, you will see Debug page as below



Besides original debugging methods. Now you have new method as One Key Debug.



Once activated, in 30 minutes, this AP will generate local debug core file.



- **HTTPS Portal Trusted Certificate with Auto Update**

This feature will solve the untrusted certificate warning reported by web browser in your HTTPS enabled captive portal deployment.

FIRMWARE VERSION 1.0.8.18

PRODUCT NAME

GWN7610; GWN7600; GWN7600LR

DATE

1/10/2019

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: 0057d240a1dee02e126d80308f5395c4
- GWN7600/7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: f1166de7f2a1a51ca96f242c8da518f2

IMPORTANT UPGRADING NOTE

- In order to enable your AP's capability of connecting GWN Cloud EU server, AP needs to be upgraded to 1.0.8.17 or above. Otherwise, your AP will always be offline from your EU server portal.

CHANGES/ENHANCEMENT

- Added feature of **Advertisement**¹ for Captive Portal
- Added feature of **Custom Field**¹ for Captive Portal Splash Page
- Added feature of **ARP Proxy**
- Added feature of **Clear client data**¹
- Enhanced Event log by **WiFi authentication event**¹
- Enhanced Bandwidth Rules by adding option to **limit bandwidth Per-Client** and adding **Total Bandwidth Usage**¹ on Overview Bandwidth Chart
- Added **EU Server support**¹

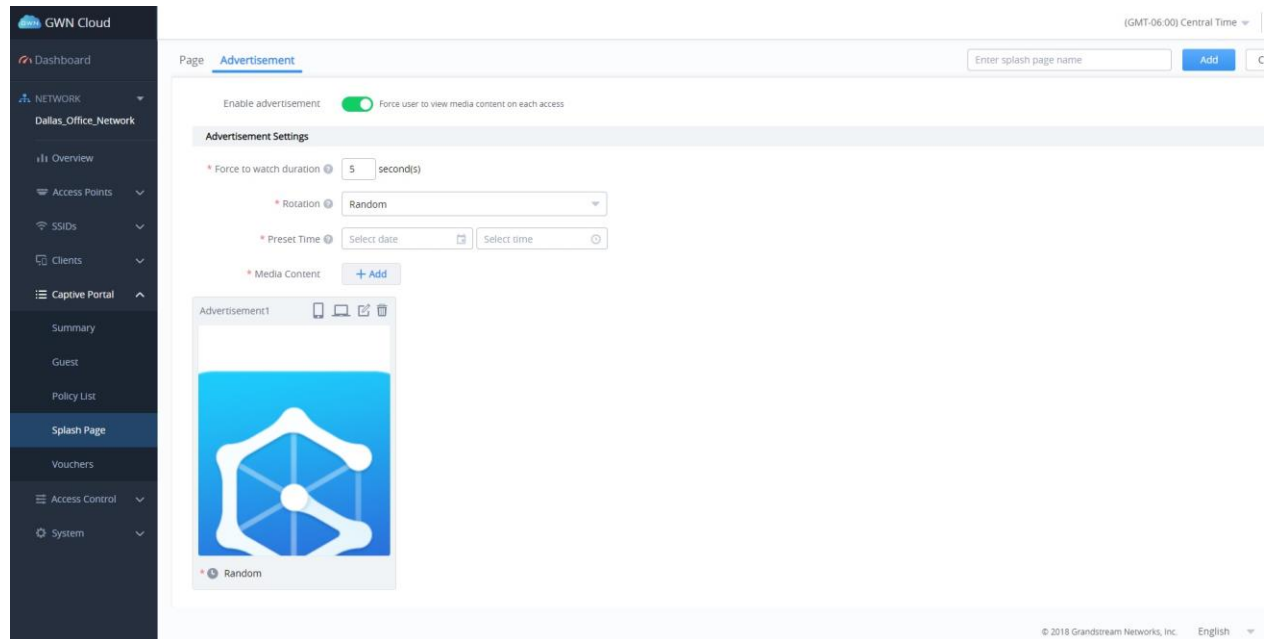
¹ This feature is only available on GWN Cloud, and local master does not have it.

NEW FEATURE OVERVIEW

- **Advertisement**

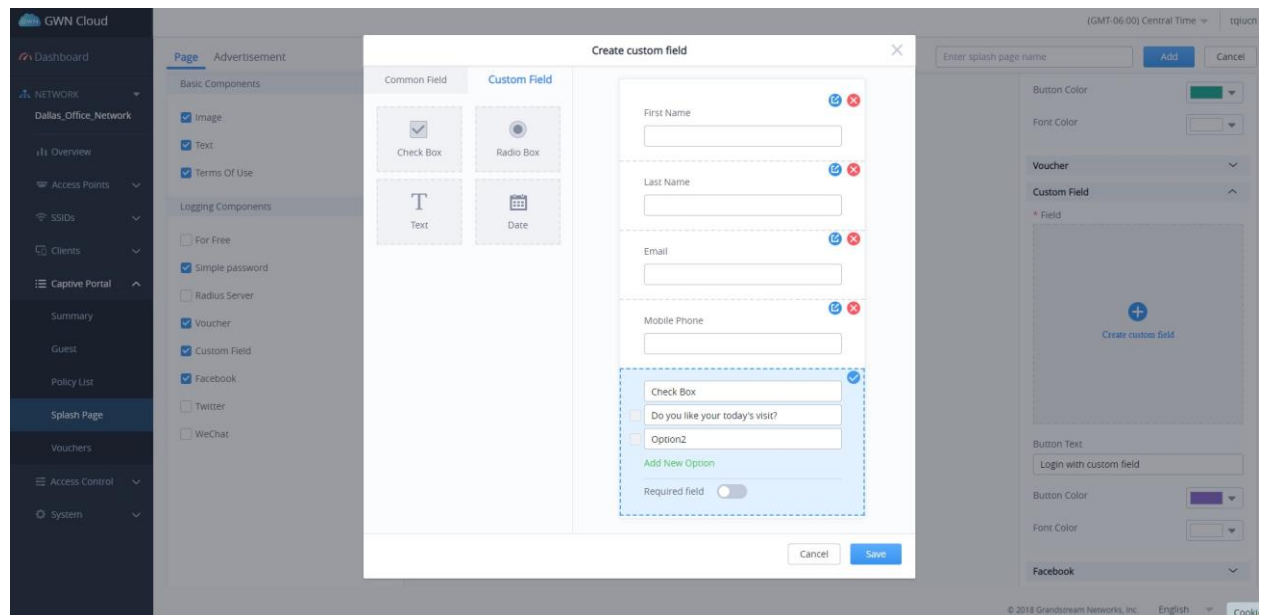
Marketing feature to play advertisement upon captive portal login for WiFi users.

Configurations are available at Cloud menu: **Captive Portal** → **Splash Page** → **Advertisement**



- **Custom Field**

By adding customizable field to your captive portal splash page to collect user information.



- **ARP Proxy**

This feature will enable GWN AP to answer the ARP requests from its LAN for its connected WiFi client. This is mainly to reduce the airtime consumed by ARP packets.

To enable this feature, configuration is available at

Cloud:

NETWORK → SSIDs → Configuration → Wi-Fi Settings → ARP Proxy

Local Master:

SSIDs → Configuration → Wi-Fi → ARP Proxy

- **Clear client data**

This feature will allow admin to clear collected data from Wi-Fi clients. This is mainly for certain data security regulation compliance.

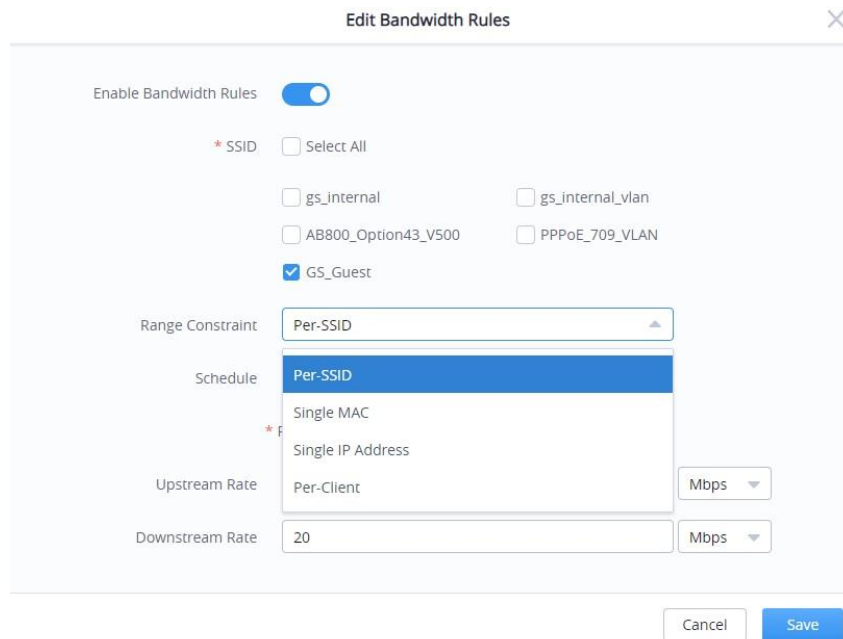
- **WiFi authentication event**

This is an enhancement for WiFi troubleshooting.

2018-12-13 16:30:19	74:DA:EA:84:CD:28	gs_internal	gs_internal	WPA-PSK deauthentication (four-way handshake failure)
2018-12-13 16:30:19	74:DA:EA:84:CD:28	gs_internal	gs_internal	WPA-PSK authentication failure

- **limit bandwidth Per-Client**

This is an enhancement for bandwidth control upon all the other available types.



- **EU Server support**

User now will be able to choose US server or EU server to store their data at. This is mainly for GDPR regulation compliance.



FIRMWARE VERSION 1.0.8.9

PRODUCT NAME

GWN7610

GWN7600

GWN7600LR

DATE

11/21/2018

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: e35fdb2803278d2305cee46c1c436deb
- GWN7600/7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: f934883870b24d911b604fedfc7a5fed

CHANGES/ENHANCEMENT

- Added feature of **URL Logging**¹
- Added feature of **Dynamic Transmit Power Control** as WP820 RF enhancement
- Enhanced Mesh by adding feature of **Switching RE & CAP according to network**
- Enhanced Core File Debugging by adding feature of **OopsTrack**
- Fixed the bug that manual configured Mesh topology may change after reboot
- Fixed a memory leak

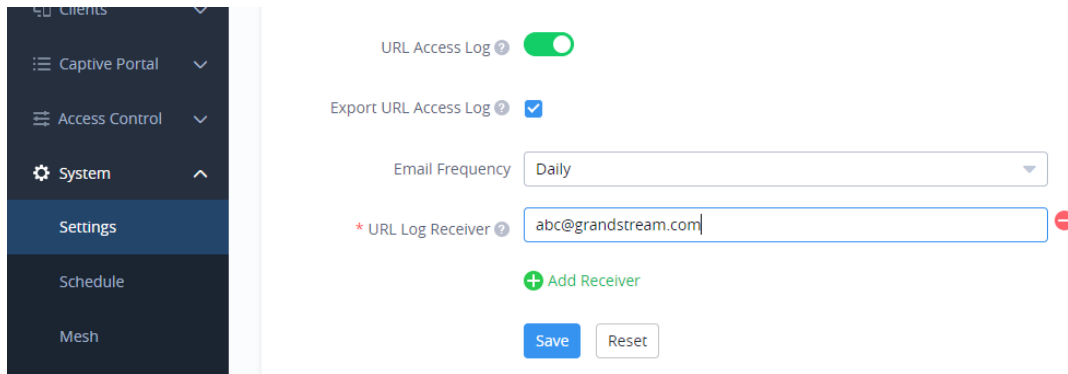
NEW FEATURE OVERVIEW

- **URL Logging**¹

GWN AP now can log user URL visiting history onto GWN server, and report to Admin on timely schedule.

¹ URL Logging is only available at GWN Cloud, and local master configuration does not support this feature.

To enable configuration, option is available at Cloud menu: **System** → **Settings**



- **Dynamic Transmit Power Control**

This feature will enhance the RF performance of WP8xx Grandstream WiFi handset. No configuration is needed.

- **Switching RE & CAP according to network**

This is enhancement to GWN Mesh setup. Now mesh topology will be more precise on identifying the CAP or RE APs. System will not only detect the network cable connection for CAP election, but also check the IP address acquiring.

- **OopsTrack**

This is enhancement on the core file debugging. It will collect and save kernel stack information for debugging when AP crashes.

FIRMWARE VERSION 1.0.7.13

PRODUCT NAME

GWN7610&GWN7600&7600LR

DATE

10/18/2018

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5 checksum: c13f4e003ff70e6b4e37627b0e7d2013
- GWN7600 Firmware file name: gwn7600fw.bin
MD5 checksum: c425a264b8053aac9cef33644db23477
- GWN7600LR Firmware file name: gwn7600fw.bin
MD5 checksum: c425a264b8053aac9cef33644db23477

IMPORTANT UPGRADING NOTE

Facebook and Twitter captive portal authentication backend changed. This change will lead to following result:

1. If Facebook authentication is configured on older GWN Cloud version. You will need to log in your Facebook account of <https://developers.facebook.com/apps>, and set the OAuth redirect URI to <https://cwp.gwn.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3>
2. If Twitter authentication is configured on older GWN Cloud version. You will need to log in your Twitter account of <https://apps.twitter.com/app>, and set the callback URLs to <http://cwp.gwn.cloud:8080/GsUserAuth.cgi?GsUserAuthMethod=5>
3. Also, you will need to make sure your AP is upgraded to 1.0.7.x, since the older AP firmware will not work with new GWN Cloud for Facebook Login or Twitter Login only.


CHANGES/ENHANCEMENT

- Added feature of **RRM^{Beta 1}**
- Added feature of **Mesh** for GWN7610²
- Added feature of **External Captive Portal Support**
- Added feature of **AP Scheduling Reboot**
- Added feature of **Change Log³**
- Added feature of WiFi **Statistic Report³**
- Added feature of **Configuration Quick Navigation³**
- Added feature of Captive Portal Guest **Summary**
- Changed **SSID limit³**
- Enhanced **Access Point Status**
- Enhanced **WiFi Service** by adding configurable options of **Beacon Interval**, **DTIM Period**, and **Convert IP multicast to unicast**.
- Enhanced **Client Information**
- Enhanced **Captive Portal features**
- Enhanced **GWN Cloud mobile app**

NEW FEATURE OVERVIEW

- **RRM^{Beta}**

Radio Resource Management (RRM), includes three major features below. This feature is only available

Local Master: **Access Point** →  **Edit** → **Configuration**

- **Dynamic Channel Assignment⁴** Once enabled, AP will try to allocate and move to the best channel during operation, unlike Auto Channel Selection (ACS) which online scan and assign channel when WiFi interface goes up for one.

¹ Local Master only

² Mesh is already supported on GWN7600 and GWN7600LR in previous feature pack

³ GWN Cloud only

⁴ **Dynamic Channel Assignment** is not supported on GWN7610.

- **Transmit Power Control** TPC algorithm runs every 10 minutes. AP acquires the RSSI information of the neighbor by wireless scanning and establishes the neighbor table. The algorithm requires that there must be at least 3 neighbor APs with larger than -70dbm in RSSI. Otherwise, power will not be adjusted.
 - **Coverage Hole Detection** CHD enables AP to decide whether to increase the AP power by the current SNR and SNR threshold of the connected clients.
-
- **External Captive Portal Support**
Linkyfi¹ and Purple² as external captive portal are supported now on GWN APs for both local master and GWN Cloud.
Configurations now are available at **Captive Portal** → **Policy List** → **Add/Edit** → **Splash Page**
Choose **External**, and then choose platform to configure.

 - **AP Scheduling Reboot**
You can schedule reboot for your APs. Configuration is available at:
 - Local Master: **System Settings** → **Maintenance** → **Basic** → **Reboot Schedule**
 - GWN Cloud: **NETWORK** → **System** → **Settings** → **Reboot Schedule**You will need to have a time schedule defined for this feature to adopt.

 - **Change Log**
Change log is now recorded on GWN Cloud. You can access the log from **[Your account]** on top right corner → **Change Log**.

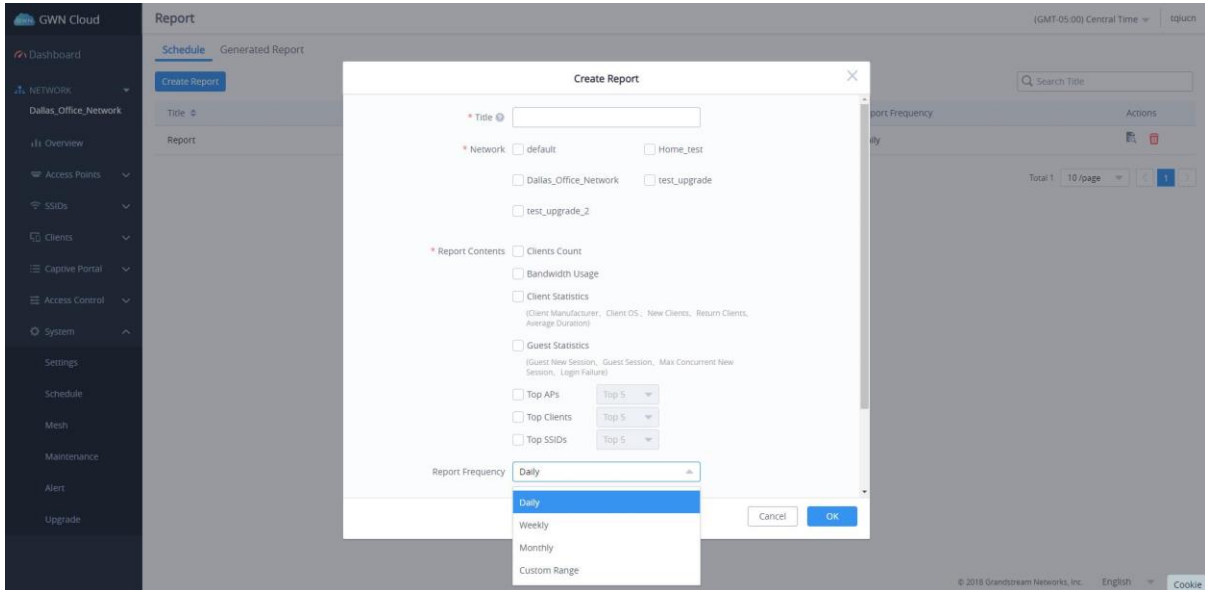
Note: ¹ Linkyfi <https://www.avsystem.com/products/linkyfi/>

² Purple <https://purple.ai/>

- **Statistic Report**

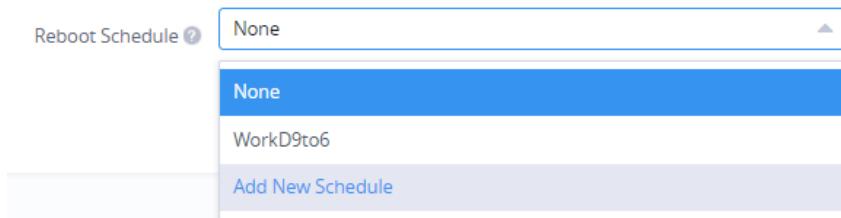
On GWN Cloud, you can configure server to send report to you periodically. Configuration is available at:

[Your account] on top right corner → **Report** → **Schedule** → **Create Report**



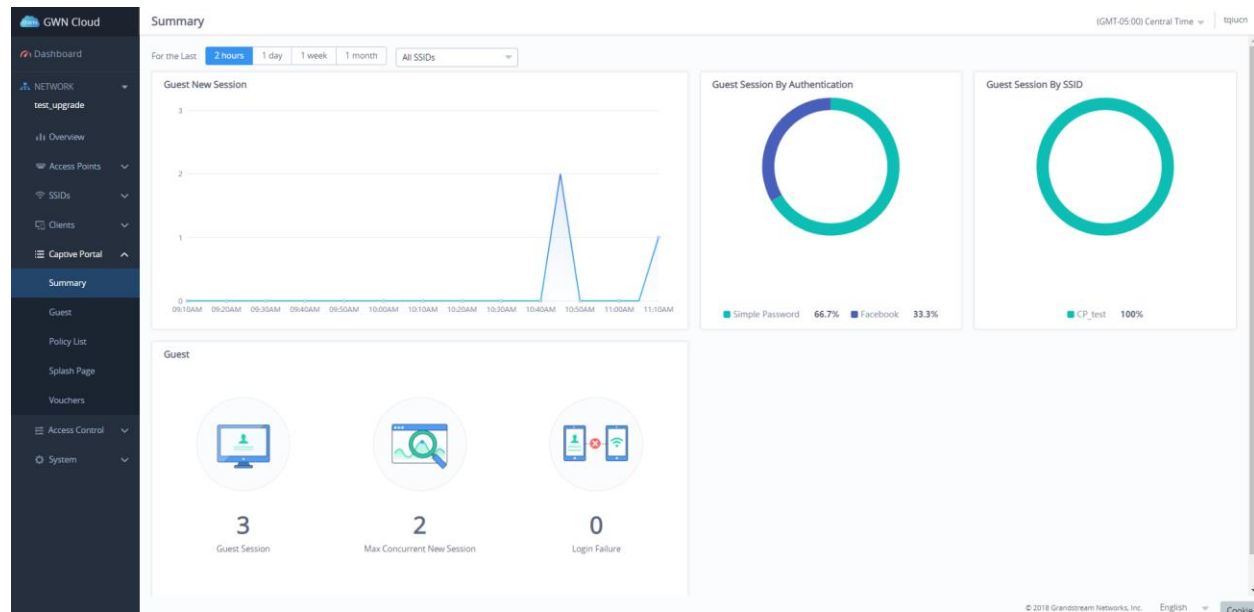
- **Configuration Quick Navigation**

Now on GWN Cloud support Configuration Quick Navigation. This feature will help to quick move to prerequisite settings during configuration. For example, when you configure a AP scheduling reboot, but you don't have a time schedule reconfigured. Then you will see an option as **Add New Schedule**.



- **Captive Portal Guest Summary**

GWN Cloud now gives a summary of captive portal login Guest Summary as below:



- **SSID limit** changes

In previous GWN Cloud version, every Network has limit of 16 SSID. In FP6 GWN Cloud version, limit in Network has been removed, but when any AP has reach to its limit of 16 SSID, it will be shown in grey in the new SSID's available devices, and cannot be added to new SSID anymore.

- **Access Point Status** Enhancement

CPU and Memory information is added in Access Points **Status**.

For Email Alert, feature is enhanced for AP offline event to report when AP goes back online.

- **WiFi Service** Enhancement

Three configurable options, as **Beacon Interval**, **DTIM Period**, and **Convert IP multicast to unicast**, are available at

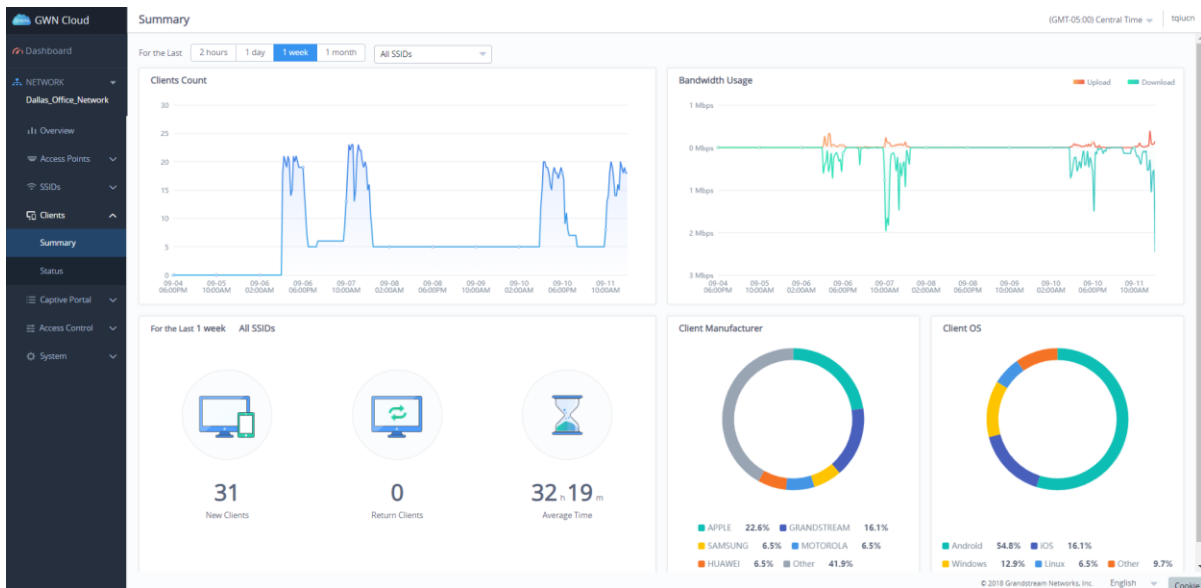
- Local Master: **SSID** → **Add/Edit** → **Beacon Interval / DTIM Period / Multicast to Unicast**
- GWN Cloud: **NETWORK** → **SSID** → **Add/Edit** → **Advanced** → **Beacon Interval / DTIM Period / Convert IP Multicast to Unicast**

- **Client Information Enhancement**


More WiFi client's information is collected on GWN AP. And statistic is shown in graphic on GWN Cloud and text only format on Local Master.

- Local Master: Information is available at **Clients** → **Clients**, and information can be checked to display at the top right gear icon. 

- GWN Cloud:



And now, admin can name the clients not only on local master but also on GWN Cloud page **NETWORK** →

Clients → **Status** →  → **Hostname**

- **Captive Portal features Enhancement**

- **Failsafe mode:** AP will grant access to STA if AP can't reach to external authentication server. This feature only available in radius authentication and voucher authentication.

- **Byte limit** and **Daily limit**: Captive portal now can limit user connection by measuring data amount and times of a day.
- **Twitter authentication** enhanced: Twitter splash page has been redesigned, and **Force To Follow** option added. By enabling **Force To Follow** option, admin can request login WiFi user to follow his Twitter account when getting authenticated.

- **GWN Cloud mobile app** enhancement
 - Dashboard, on GWN Cloud Mobile app, now allow admin to select different Network to display, while all Networks' information is combined to display.
 - Deleting AP, on GWN Cloud Mobile app, now allow admin to delete APs from Networks.

[GWN7610] FIRMWARE VERSION 1.0.6.43

PRODUCT NAME

GWN7610

DATE

6/15/2018

FIRMWARE FILE INFORMATION

- GWN7610 Firmware file name: gwn7610fw.bin
MD5: ae52aea470e6bf0fdcca95b1537df8e9

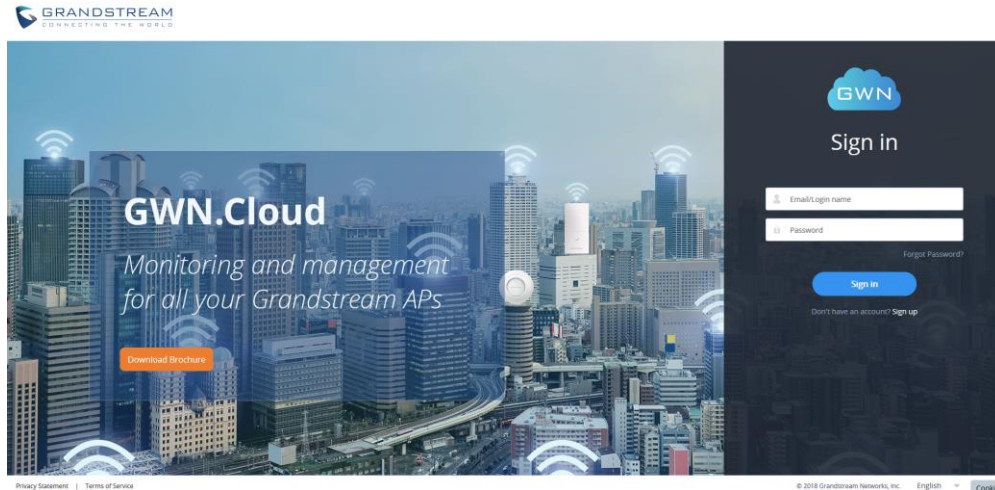
ENHANCEMENT

- Added support for **GWN.Cloud**
- Added support Outdoor/Indoor **Scene** WiFi channel configuration
- Added feature for **Transfer AP** and **Transfer Network Group** to Cloud
Newly designed
- **Feature Schedulingg**
- Split **Network Group** into separate **SSID** and **DHCP server** configurations

NEW FEATURE OVERVIEW

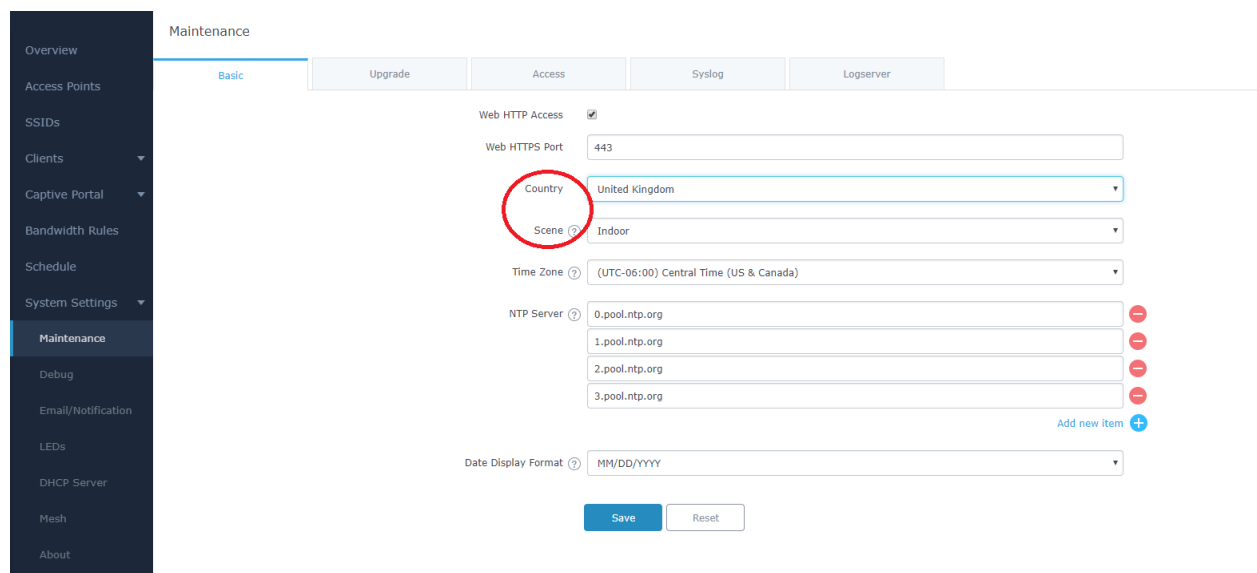
- **GWN.Cloud**

Since FP5, GWN AP can be managed by your **GWN.Cloud** account. **GWN.Cloud** web interface now can be accessed at <https://www.gwn.cloud>. Please refer to **GWN Cloud User Guide** for how to add your GWN AP to **GWN.Cloud**.



- Outdoor/Indoor **Scene** configuration

This configuration is available on your Master web, when your country has different outdoor/indoor WIFI channel regulations.



Maintenance

Basic Upgrade Access Syslog Logserver

Web HTTP Access

Web HTTPS Port 443

Country United Kingdom

Scene Indoor

Time Zone (UTC-06:00) Central Time (US & Canada)

NTP Server 0.pool.ntp.org

1.pool.ntp.org

2.pool.ntp.org

3.pool.ntp.org

Add new item

Date Display Format MM/DD/YYYY

Save Reset

- **Transfer AP and Transfer Network Group**

Transfer AP feature will allow you to easily transfer your AP from local master to your GWN.Cloud account.

When you already have network/WiFi configurations on your cloud account, use this feature will let you to choose cloud existing network/SSID to adopt your local AP. Note: local configurations will not be transferred.

Transfer Network Group feature will allow you to transfer your local configurations to your cloud account.

Access Points

	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
<input type="checkbox"/>	GWN7610	Front_AP_unlocked 00:0B:82:A1:A6:AC	192.168.254.35	Master	13d 1h 57m 50s	1.0.6.40	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Share"/> <input type="button" value="Group"/> <input type="button" value="Info"/>
<input type="checkbox"/>	GWN7610	Back_AP_Locked_EU 00:0B:82:A8:66:A8	192.168.254.36	Offline	11d 20h 26m 0s	1.0.6.40	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Share"/> <input type="button" value="Group"/> <input type="button" value="Info"/>

- **Feature Scheduling**

We have newly designed feature scheduling. Please refer to user manually for configuration details.

Add Schedule

Click [+](#) to create new schedule

Weekly

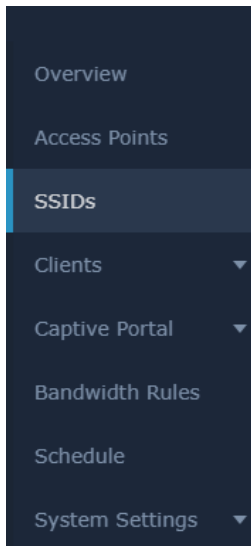
Select All	Sun	Mon	Tues	Wed	Thur	Fri	Sat
00:00-00:30							
00:30-01:00							
01:00-01:30							
01:30-02:00							
02:00-02:30							
02:30-03:00							
03:00-03:30							
03:30-04:00							
04:00-04:30							
04:30-05:00							
05:00-05:30							
05:30-06:00							
06:00-06:30							
06:30-07:00	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

Absolute

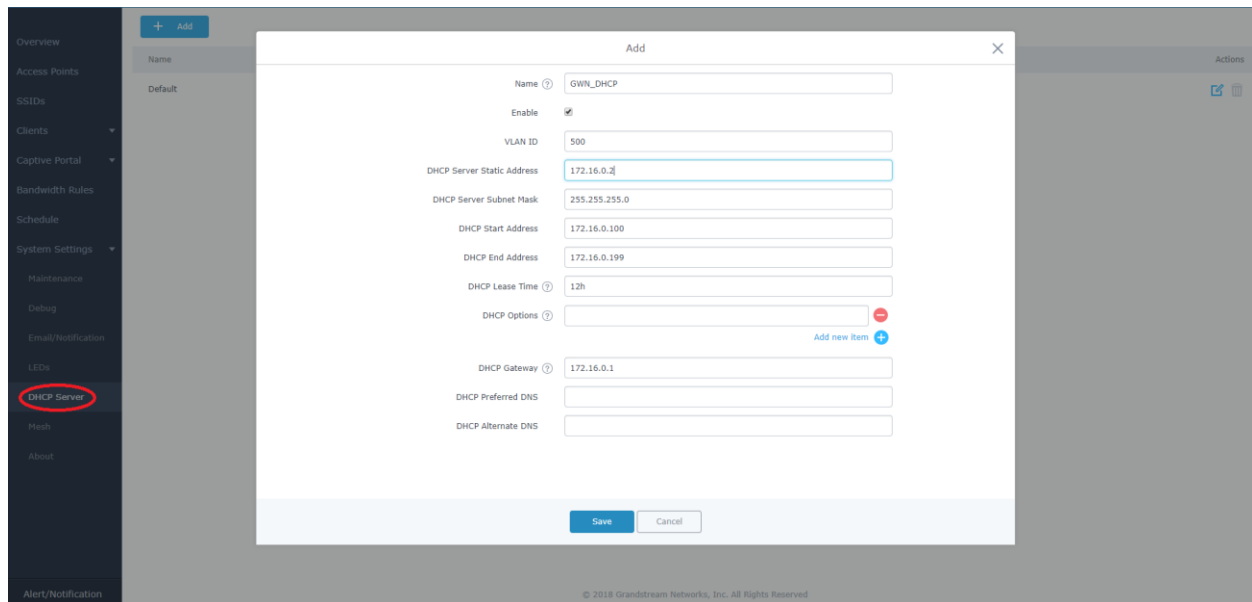
- **SSID and DHCP server** configurations

Now the original **Network Group** configuration is split into **SSID** and **DHCP server** configurations.

SSID is located at below menu bar.



DHCP server configuration is moved to System settings.



[GWN7600&7600LR] FIRMWARE VERSION 1.0.6.41

PRODUCT NAME

GWN7600&7600LR

DATE

6/15/2018

FIRMWARE FILE INFORMATION

- GWN7600&7600LR Firmware file name: gwn7600fw.bin
MD5: 8659930c6fe9601f551d87df9ae381ed
- GWN7600LR Firmware file name: gwn7600lrfw.bin
MD5: 61784977a1a698e3d85f376200124010

ENHANCEMENT

- Added support for **GWN.Cloud**
- Added support Outdoor/Indoor **Scene** WiFi channel configuration
- Added feature for **Transfer AP** and **Transfer Network Group** to Cloud
Newly designed
- **Feature Scheduling**
- Split **Network Group** into separate **SSID** and **DHCP server** configurations

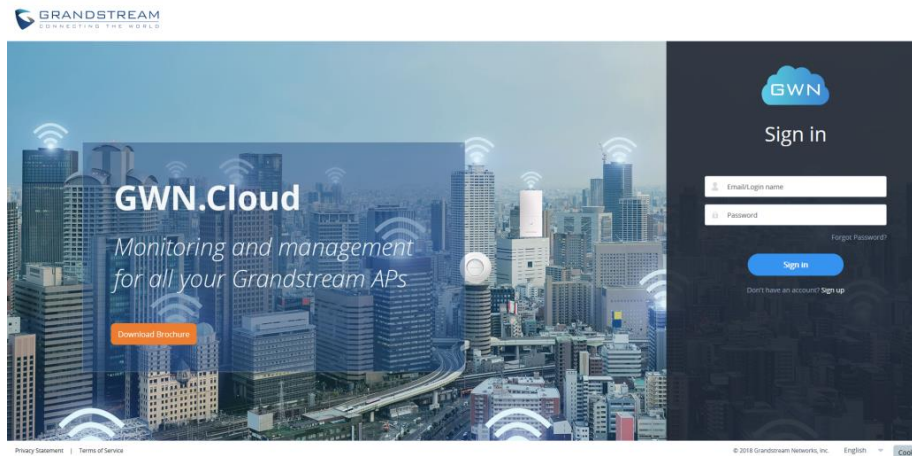
IMPORTANT UPGRADING NOTE

1. Starting from 1.0.6.x, GWN7600 and GWN7600LR will share same firmware file name gwn7600fw.bin. As a result, when GWN7600LR upgrades from pre-1.0.6.x to latest firmware, it will still retrieve firmware with name gwn7600lrfw.bin, and when GWN7600LR upgrades from 1.0.6.x or post-1.0.6.x to other firmware, it will retrieve firmware with name gwn7600fw.bin. So, when your GWN7600LR upgrades from pre-1.0.6.x firmware, you will need to manually modify the target firmware name to gwn7600lrfw.bin.

NEW FEATURE OVERVIEW

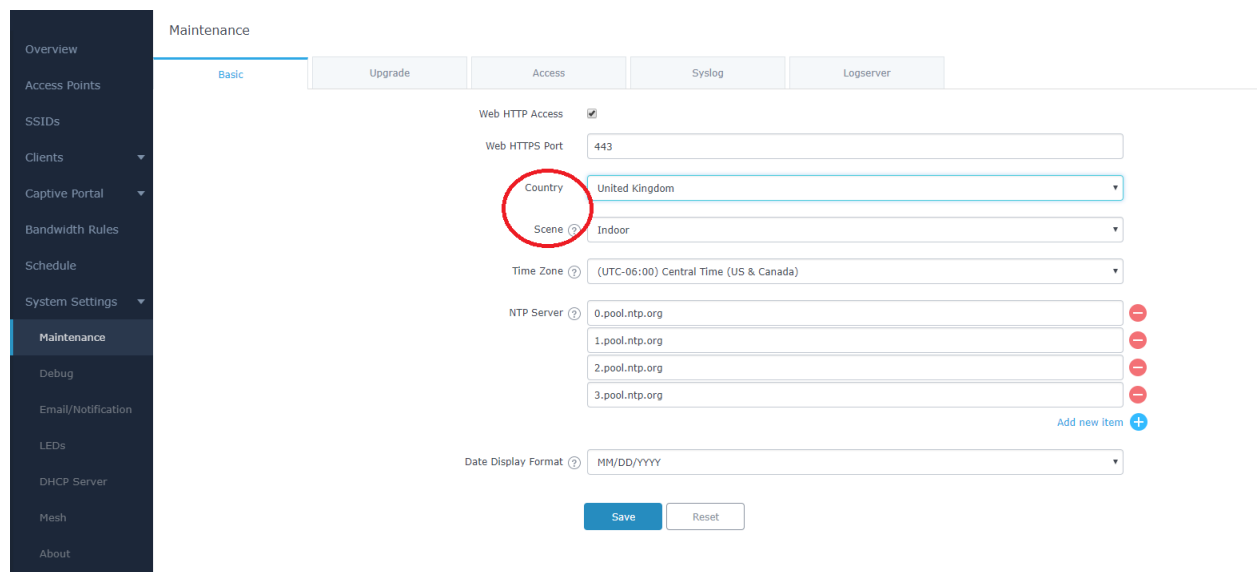
- **GWN.Cloud**

Since FP5, GWN AP can be managed by your **GWN.Cloud** account. **GWN.Cloud** web interface now can be accessed at <https://www.gwn.cloud>. Please refer to **GWN Cloud User Guide** for how to add your GWN AP to **GWN.Cloud**.



- **Outdoor/Indoor Scene configuration**

This configuration is available on your Master web, when your country has different outdoor/indoor WIFI channel regulations.



Maintenance

Basic Upgrade Access Syslog Logserver

Web HTTP Access

Web HTTPS Port 443

Country United Kingdom

Scene Indoor

Time Zone (UTC-06:00) Central Time (US & Canada)

NTP Server 0.pool.ntp.org

1.pool.ntp.org

2.pool.ntp.org

3.pool.ntp.org

Add new item

Date Display Format MM/DD/YYYY

Save Reset

- **Transfer AP and Transfer Network Group**

Transfer AP feature will allow you to easily transfer your AP from local master to your GWN.Cloud account.

When you already have network/WiFi configurations on your cloud account, use this feature will let you to choose cloud existing network/SSID to adopt your local AP. Note: local configurations will not be transferred.

Transfer Network Group feature will allow you to transfer your local configurations to your cloud account.

Access Points

Transfer network group
Transfer AP
Discover AP
Failover

Upgrade
Reboot
+ Add to SSIDs
✖ Configure

⚙

☐	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
☐	GWN7610	Front_AP_unlocked 00:08:B2:A1:A6:AC	192.168.254.35	Master	13d 1h 57m 50s	1.0.6.40	🔗 🔄 📄 👤 🗑
☐	GWN7610	Back_AP_locked_EU 00:08:B2:A8:66:A8	192.168.254.36	Offline	11d 20h 26m 0s	1.0.6.40	🔗 🔄 📄 👤 🗑

- **Feature Scheduling**

We have newly designed feature scheduling. Please refer to user manually for configuration details.

+ Create New Schedule

Click + to create new schedule

Add Schedule

Name

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

📅
⏰
➖

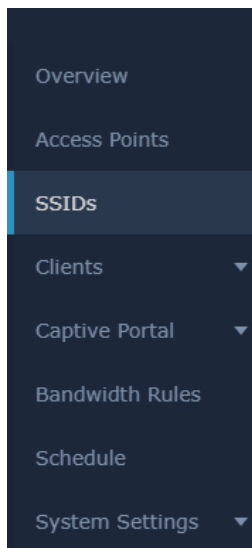
Add new Item +

Save
Cancel

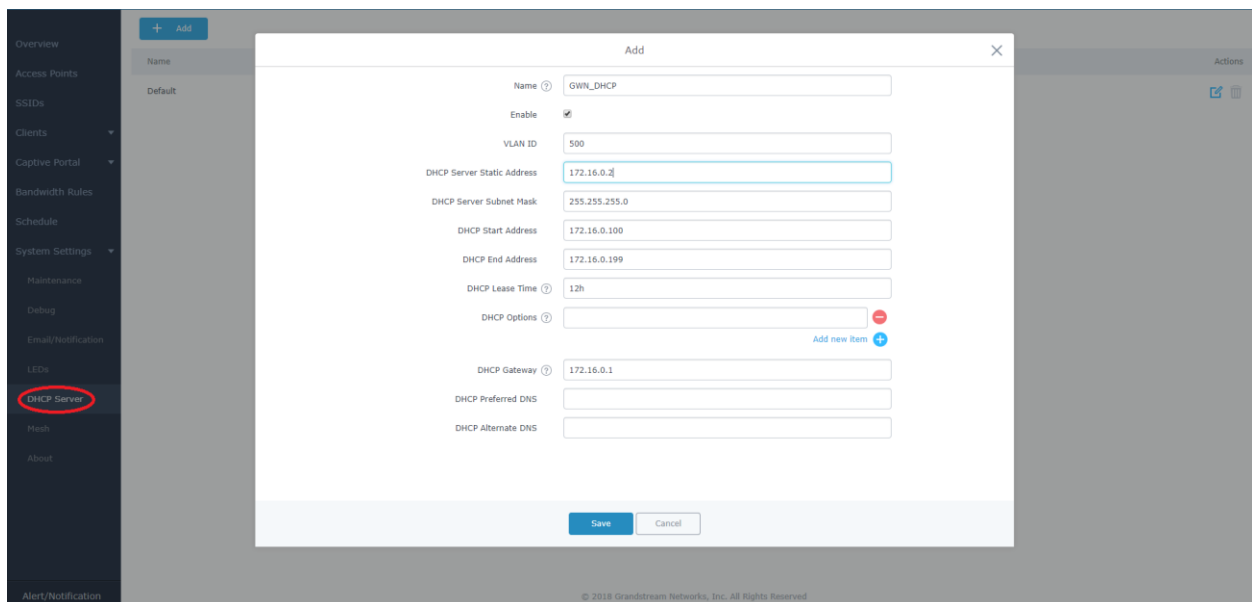
- **SSID and DHCP server** configurations

Now the original **Network Group** configuration is split into **SSID** and **DHCP server** configurations.

SSID is located at below menu bar.



DHCP server configuration is moved to System settings.



[GWN7610] FIRMWARE VERSION 1.0.5.15

PRODUCT NAME

GWN7610

DATE

1/26/2017

IMPORTANT UPGRADING NOTE

- For firmware 1.0.5.15, this is only for GWN7610/GWN7600/GWN7600LR master deployment. All users with GWN7000 as master are NOT encouraged to upgrade until 1.0.5.x matching firmware is available for GWN7000, due to the compatibility of new features.

ENHANCEMENT

- Added support for **New Firmware Reminder on Master Web**
- Added support for **Sequential Upgrade**
Added support for
- **Feature Scheduling**
- Added support for **Master Direction**
- Added support for **Master Transfer**
- Added support for **Airtime Fairness**
- Added support for **Social login/Voucher**

BUG FIX

- Wifi client may fail to connect if SSID uses 2.4G only with WEP authentication.
- The Bandwidth Rules schedule configurations require a reboot to take effect.

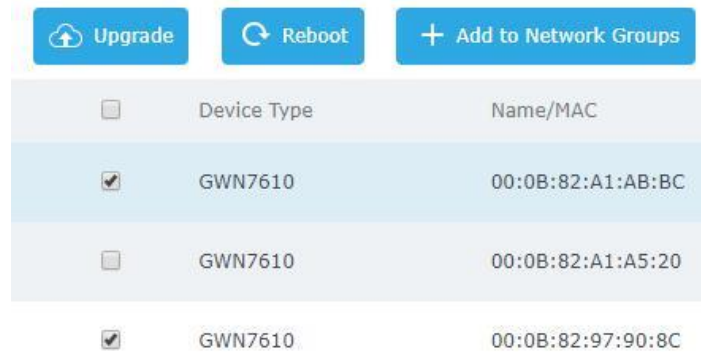
NEW FEATURE OVERVIEW

- **New Firmware Reminder on Master Web**

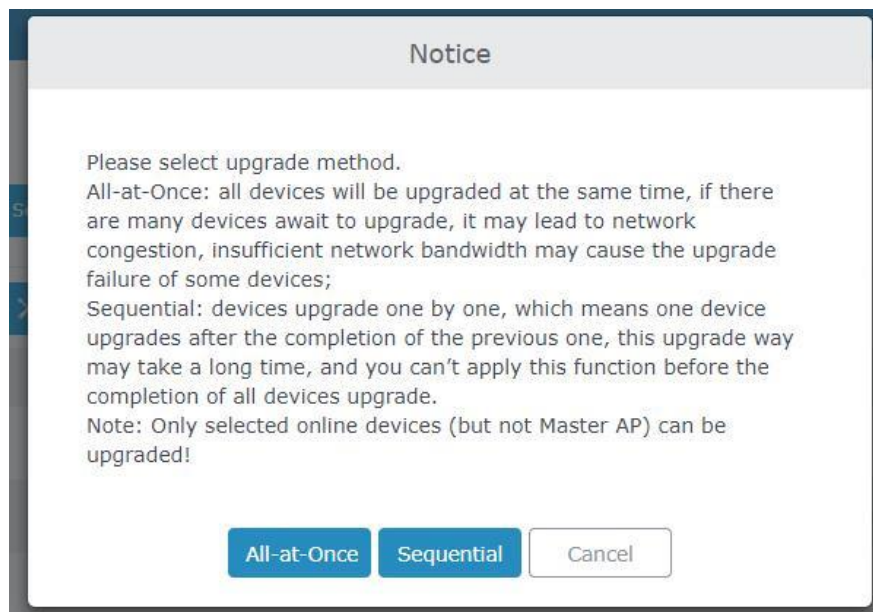


Once a different OFFICIAL firmware than current running firmware is detected on Grandstream Network website by master GWN7610, a “NEW” icon will appear to remind network administrator to upgrade. Clicking on the “NEW” icon will open the new firmware’s release note.

- **Sequential Upgrade**



Now if you choose multiple slave devices to upgrade their firmware, two options as “All-at-Once” and “Sequential” are available. “All-at-Once” will trigger the traditional way that all checked slaves will try to retrieve and change their firmware at the same time, while “Sequential” upgrade will let the slaves to



upgrade one by one in order to 1) avoid entire wifi service interruption by full system firmware upgrade; 2) reduce network stress caused by firmware downloading.


Access Points  1 / 2

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

- **Feature Scheduling**

Scheduled bandwidth control or client access control is available now under System Settings→Schedule

Add

Enabled	<input type="checkbox"/>
Name	<input style="border: 1px solid red;" type="text"/> The field should not be empty
Scheduled Feature	<input style="border: 1px solid #ccc;" type="text" value="Bandwidth"/>
Bandwidth Rules	<input style="border: 1px solid red;" type="text"/> The field should not be empty
Schedule Type	<input style="border: 1px solid #ccc;" type="text" value="Daily"/>
Month for Turn On <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Month for Turn Off <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Day of Month for Turn On <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Day of Month for Turn Off <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Day of Week for Turn On <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Day of Week for Turn Off <small>(?)</small>	<input style="border: 1px solid #ccc;" type="text" value="*"/>
Schedule On Time	<input style="border: 1px solid #ccc;" type="text"/> 

Please be noted that you will need a Bandwidth rule (can be created in Bandwidth Rules) or a Client Access list (can be created under Client→Client Access), in order to create a schedule.

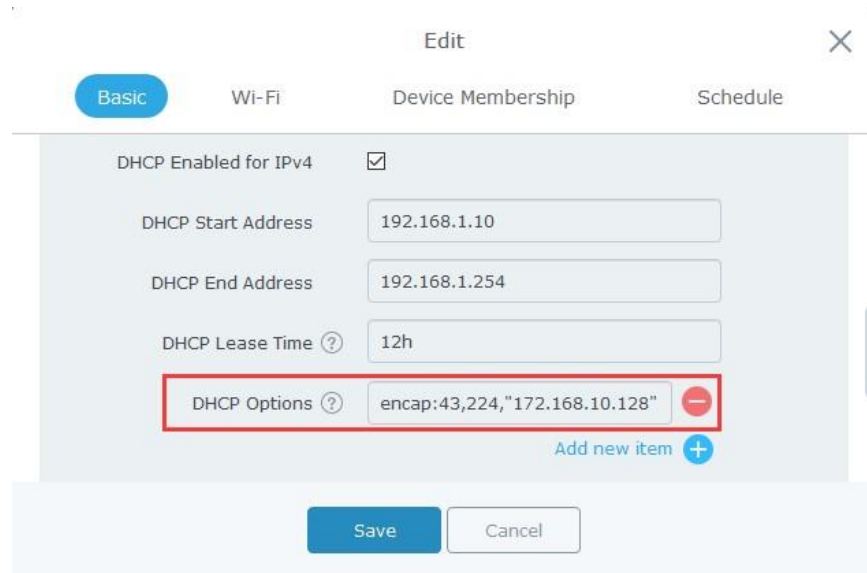
- **Master Direction**

When GWN7610 slave is not in the same broadcast domain with its master, this feature is available for all factory configured GWN7610 to find its master IP address offered by local DHCP option 43.

GWN7610 accepts option 224 encapsulated in option43, and the syntax is in TLV format. So, the for a simple example of DHCP 43 configuration would be:

224(Type)12(Length)10.157.0.234(Value) translated into Hex as e00c31302e3135372e302e323334

For DHCP server configuration on GWN7000, which translates the values automatically, is as follows:



- **Master Transfer**

Access Points

Device Type Search Discover AP | Failover

Upgrade Reboot + Add to Network Groups Configure Settings

Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7610	00:08:82:A1:AB:BC	192.168.253.230	Online	52m 53s	1.0.5.11	
GWN7610	00:08:82:A1:A5:20	192.168.253.175	Master	6m 57s	1.0.5.11	

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

Now an easier way to transfer your master authority from one unit to another available unit is available on Access Point management page. By clicking the Transfer to Master button above in red circle, the designated slave unit will be upgraded to master and current master will be downgraded to slave accordingly.

- **Airtime Fairness**

Turning Airtime Fairness ON or OFF options can be found under Access Point→Edit→Configuration→Airtime Fairness.

- **Social login/Voucher**

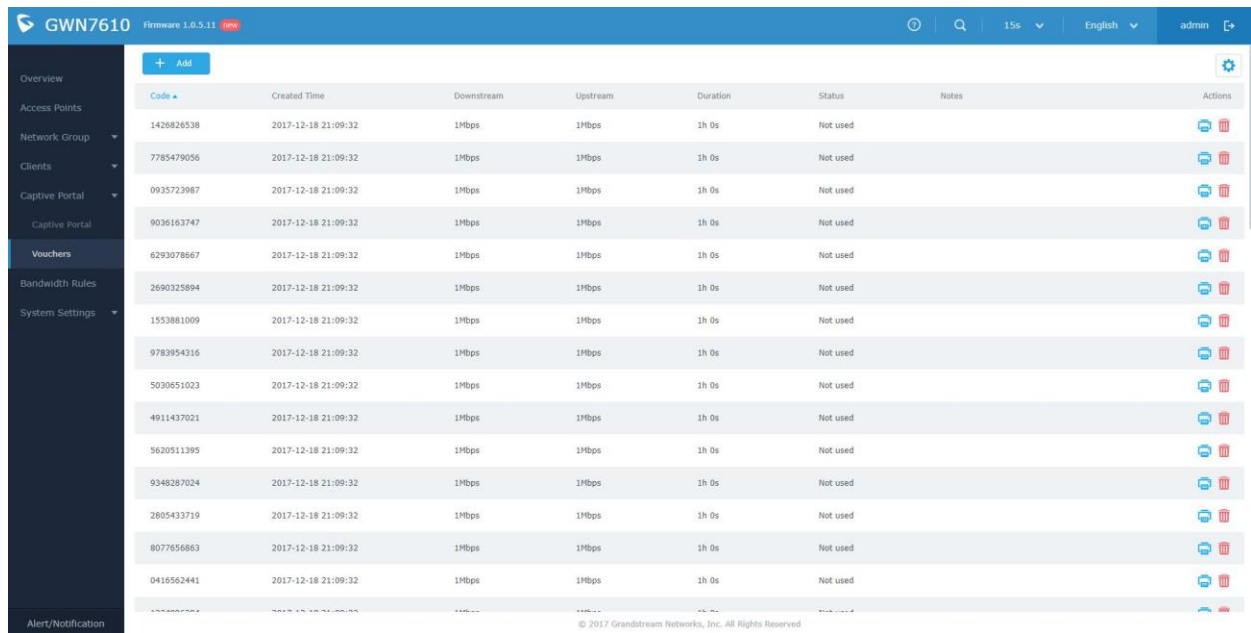
As an enhancement of Captive Portal, social Login as Wechat/Facebook/Twitter have been added.































Add

Name	<input style="width: 100%;" type="text"/>	
	The field should not be empty	
Authentication Type	<input style="width: 100%;" type="text" value="Social Login Authentication"/>	
Expiration (?)	<input style="width: 60%;" type="text"/>	<input style="width: 30%;" type="text" value="seconds"/>
	The field should not be empty	
WeChat	<input type="checkbox"/>	
Facebook (?)	<input type="checkbox"/>	
Twitter (?)	<input type="checkbox"/>	
Use Default Portal Page	<input checked="" type="checkbox"/>	
Portal Page Customization	<input style="width: 100%;" type="text" value="/social_auth.html"/>	
Landing Page	<input style="width: 100%;" type="text" value="Redirect to the Original URL"/>	

Also, Voucher is added as another Captive Portal authentication option.

Voucher management interface is available under Captive Portal→Vouchers



Code	Created Time	Downstream	Upstream	Duration	Status	Notes	Actions
1426826538	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
7785479056	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
0935723987	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
9036163747	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
6293078667	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
2690325894	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
1553881009	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
9783954316	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
5030651023	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
4911437021	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
5620511395	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
9348287024	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
2805433719	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
8077656863	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 
0416562441	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		 

© 2017 Grandstream Networks, Inc. All Rights Reserved

[GWN7600&7600LR] FIRMWARE VERSION 1.0.5.13

PRODUCT NAME

GWN7600/GWN7600LR

DATE

2/12/2018

FIRMWARE FILE INFORMATION

- GWN7600 Firmware file name: gwn7600fw.bin
MD5: 0e02717ca35b7563df41091fdbd1612c
- GWN7600LR Firmware file name: gwn7600lrfw.bin
MD5: 9acb5a9db5ce4f179ec7bb5c4be596cd

IMPORTANT UPGRADING NOTE

- For firmware 1.0.5.13, this is only for GWN7610/GWN7600/GWN7600LR master deployment. All users with GWN7000 as master are NOT encouraged to upgrade until 1.0.5.x matching firmware is available for GWN7000, due to the compatibility of new features.

ENHANCEMENT

- Added support for **New Firmware Reminder on Master Web**
- Added support for **Sequential Upgrade**
Added support for
- **Feature Scheduling**
- Added support for **Master Direction**
- Added support for **Master Transfer**
- Added support for **Airtime Fairness**

- Added support for **Social login/Voucher**
- Added support for **Mesh Network**

BUG FIX

- There is low probability that auto pop-up portal page of the iOS couldn't be displayed normally.
- “Hostname” on client page and the “Top AP” \ “Top SSID” \ “Top Clients” on overview page may show empty occasionally.

KNOWN ISSUE

- Configuring Radius server address with domain name instead of IP will cause the WIFI under configuration become open without authentication. Note: issue will be addressed in next feature packet release.
- After clicking on the reset button in maintenance page, there is chance to prompt "Reset failed!" wrongly.

NEW FEATURE OVERVIEW




- **New Firmware Reminder on Master Web**

Once a different OFFICIAL firmware than current running firmware is detected on Grandstream Network website by master GWN7610, a “NEW” icon will appear to remind network administrator to upgrade.

Clicking on the “NEW” icon will open the new firmware’s release note.



- **Sequential Upgrade**

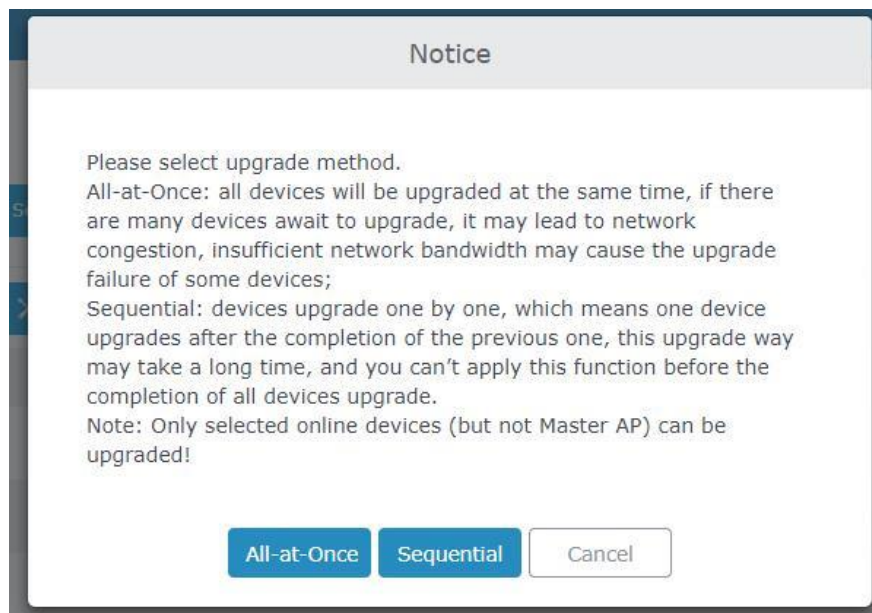
 Upgrade
 Reboot
 Add to Network Groups

<input type="checkbox"/>	Device Type	Name/MAC
<input checked="" type="checkbox"/>	GWN7610	00:0B:82:A1:AB:BC
<input type="checkbox"/>	GWN7610	00:0B:82:A1:A5:20
<input checked="" type="checkbox"/>	GWN7610	00:0B:82:97:90:8C

Now if you choose multiple slave devices to upgrade their firmware, two options as “All-at-Once” and “Sequential” are available. “All-at-Once” will trigger the traditional way that all checked slaves will try to retrieve and change their firmware at the same time, while “Sequential” upgrade will let the slaves to upgrade one by one in order to 1) avoid entire wifi service interruption by full system firmware upgrade; 2) reduce network stress caused by firmware downloading.

Access Points  1 / 2

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



- **Airtime Fairness**

Turning Airtime Fairness ON or OFF options can be found under Access Point→Edit→Configuration→Airtime Fairness.

- **Feature Scheduling**

Scheduled bandwidth control or client access control is available now under System Settings→Schedule

Add

Enabled

Name
The field should not be empty

Scheduled Feature

Bandwidth Rules
The field should not be empty

Schedule Type

Month for Turn On


Month for Turn Off

Day of Month for Turn On

Day of Month for Turn Off

Day of Week for Turn On

Day of Week for Turn Off

Schedule On Time 

Please be noted that you will need a Bandwidth rule (can be created in Bandwidth Rules) or a Client Access list (can be created under Client→Client Access), in order to create a schedule.

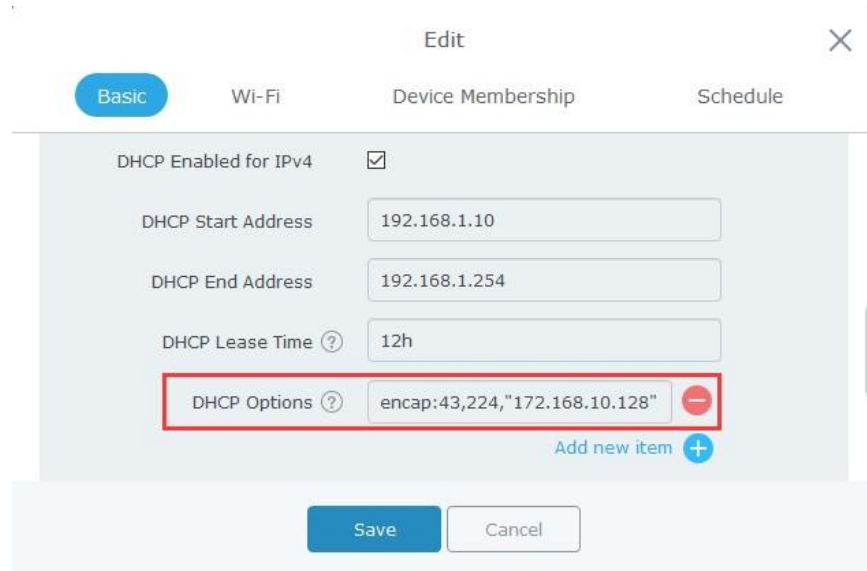
- **Master Direction**

When GWN7610 slave is not in the same broadcast domain with its master, this feature is available for all factory configured GWN7610 to find its master IP address offered by local DHCP option 43.

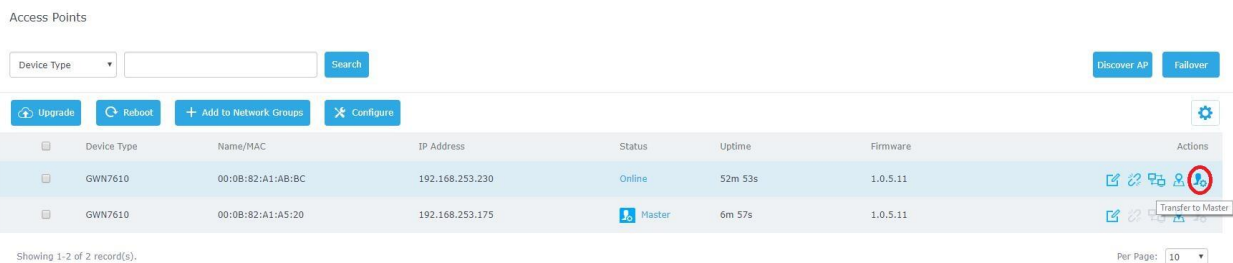
GWN7610 accepts option 224 encapsulated in option43, and the syntax is in TLV format. So, the for a simple example of DHCP 43 configuration would be:

224(Type)12(Length)10.157.0.234(Value) translated into Hex as e00c31302e3135372e302e323334

For DHCP server configuration on GWN7000, which translates the values automatically, is as follows:



- **Master Transfer**



Now an easier way to transfer your master authority from one unit to another available unit is available on Access Point management page. By clicking the Transfer to Master button above in red circle, the designated slave unit will be upgraded to master and current master will be downgraded to slave accordingly.

- **Social login/Voucher**

As an enhancement of Captive Portal, social Login as Wechat/Facebook/Twitter have been added.

Add

Name

The field should not be empty

Authentication Type

Expiration

The field should not be empty

WeChat

Facebook

Twitter

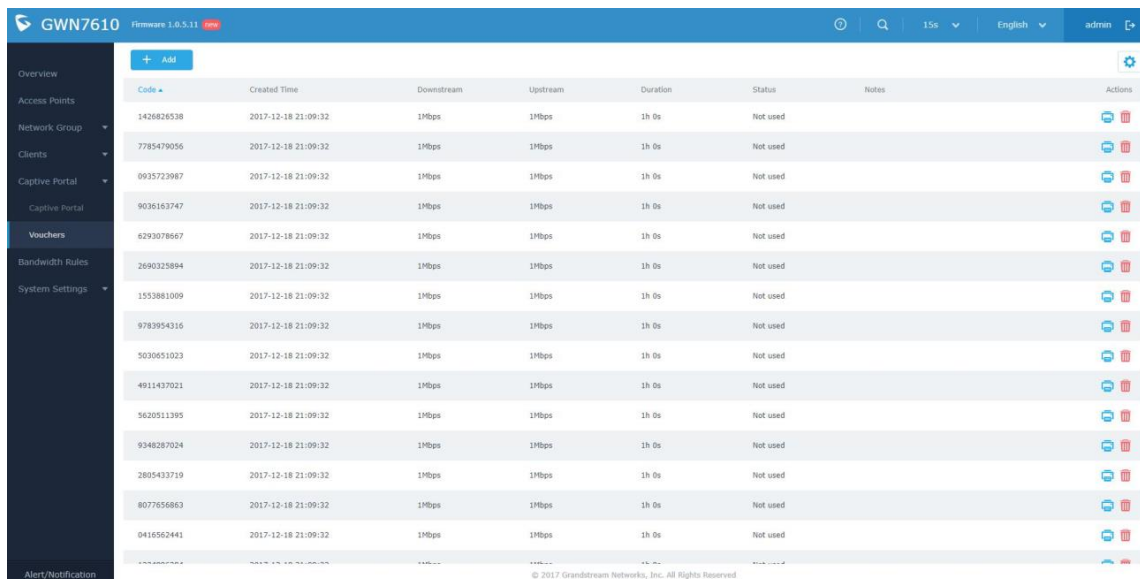
Use Default Portal Page

Portal Page Customization

Landing Page

Also, Voucher is added as another Captive Portal authentication option.

Voucher management interface is available under Captive Portal→Vouchers



The screenshot shows the 'Vouchers' management page in the Grandstream GWN7610 firmware. The page has a blue header with the title 'GWN7610 Firmware 1.0.5.11' and user 'admin'. A sidebar on the left contains navigation options: Overview, Access Points, Network Group, Clients, Captive Portal, Vouchers (selected), Bandwidth Rules, and System Settings. The main content area features a table with columns: Code, Created Time, Downstream, Upstream, Duration, Status, Notes, and Actions. There are 18 rows of voucher data, all with a status of 'Not used'. Each row has a 'Code' starting with '1426826538' and a 'Created Time' of '2017-12-18 21:09:32'. The 'Actions' column contains icons for edit, delete, and refresh.

Code	Created Time	Downstream	Upstream	Duration	Status	Notes	Actions
1426826538	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
7785479056	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
0935723987	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
9036163747	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
6293078667	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
2690325894	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
1553881009	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
9783954316	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
5030651023	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
4911437021	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
5620511395	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
9348287024	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
2805433719	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
8077656863	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]
0416562441	2017-12-18 21:09:32	1Mbps	1Mbps	1h 0s	Not used		[edit] [delete] [refresh]

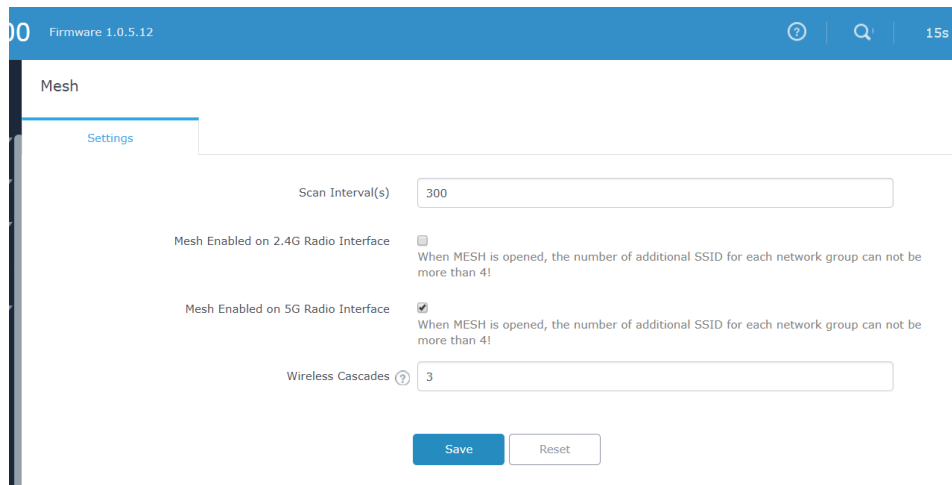
- **Mesh Network**



Mesh feature is now available for your GWN7600/7600LR wireless deployment!

With Mesh setup, APs can connect wirelessly to each other and cooperate with one another to efficiently route data from/to clients.

To use Mesh feature, here is some basic instructions:

- 1) Add all APs you want to use to form a mesh network in to a same network group.
- 2) Configure mesh under System Settings → Mesh



- 3) Disconnect network of those APs, except the root AP or APs for uplink internet access, and power those back on at the location you want to install.
- 4) Wait... The process of forming Mesh network may take several minutes. Once one AP has allocated itself into the Mesh network, its status will change from “online” to  to
- 5) At this moment, you can check the Mesh topology by clicking 
- 6) Mesh topology is automatically calculated; however, you still can modify it manually by specifying each AP’s wireless uplink in AP edit page tag “Uplink”.

[GWN7610] FIRMWARE VERSION 1.0.4.22

PRODUCT NAME

GWN7610

DATE

11/14/2017

BUG FIX

- Fixed the WPA2 4-way handshake vulnerability*
- Fixed the WPA2 802.11r vulnerability*

*Note: Please refer to our white paper of “WPA Security Vulnerability” here:

<http://www.grandstream.com/sites/default/files/Resources/WPA%20Security%20Vulnerability.pdf>

[GWN7610] FIRMWARE VERSION 1.0.4.20

PRODUCT NAME

GWN7610

DATE

10/31/2017

IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.108* or higher.
- Before starting to upgrade, please make sure your GWN7000 (the master device)'s firmware version is 1.0.2.71* or higher.

**GWN7610 firmware 1.0.2.108 package is available for downloading at*

http://firmware.grandstream.com/Release_GWN7610_1.0.2.108.zip

**GWN7000 firmware 1.0.2.75 package is available for downloading at*

http://firmware.grandstream.com/Release_GWN7000_1.0.2.75.zip

ENHANCEMENT

- Added support for **Timed Client Disconnect and Enhanced Client Blocking**
- Added support for **Client Bridge**
- Added support for **Syslog Server**
- Added support for **Configurable web UI access port**
- Added support for **E-mail notifications**

BUG FIX

- Internal bug fixes.
- Banned Band steering feature does not affect wireless Black/White/Banned client list feature anymore.

KNOWN ISSUE

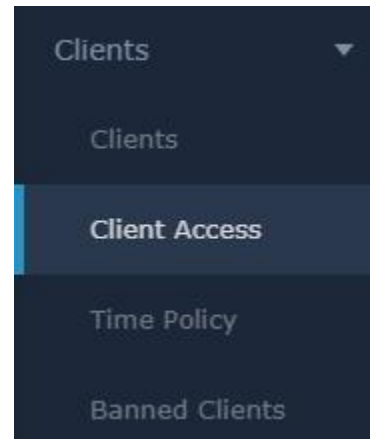
- After blocking wireless client, blocked client will be displayed as wired in the clients list instead of showing in the Blocked client list. The client can still be unblocked from Global Blacklist under Client Access.

NEW FEATURE OVERVIEW





- **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)
- 2) Client Access

+ Add		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

+ Add		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

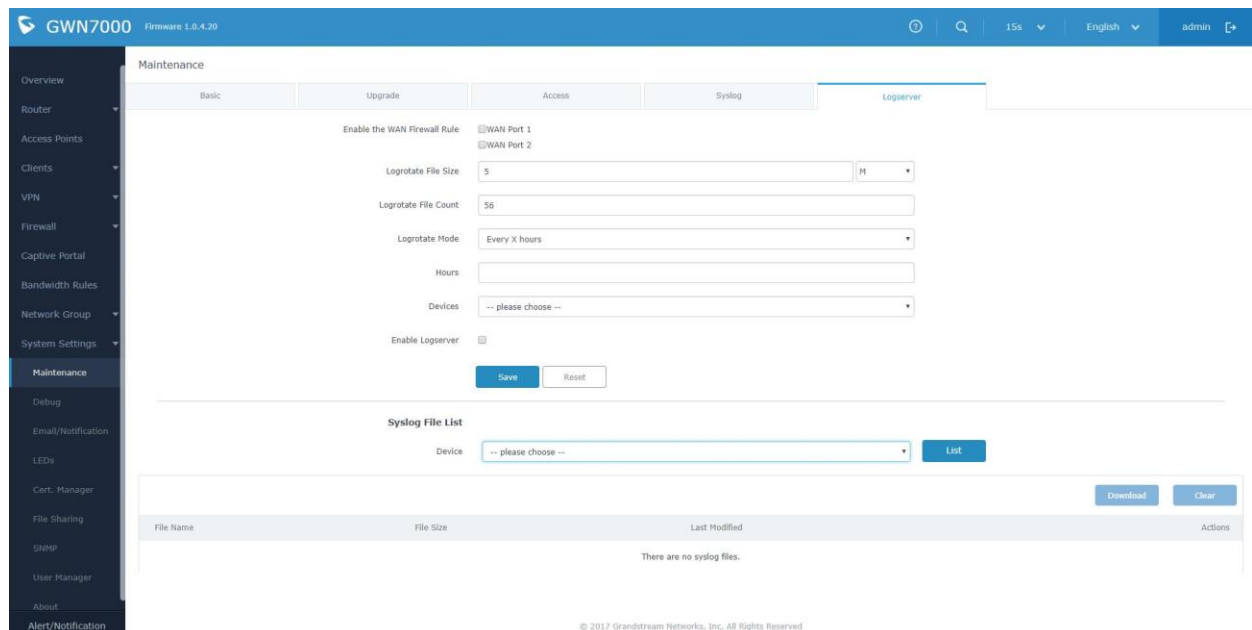
Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7610	00:08:82:97:90:8C	192.168.1.146	Online	1d 17h 51m 13s	1.0.4.19	Refresh Refresh Refresh Bridge

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

anymore, and a factory reset is required to turn it back into normal AP mode.

- **Syslog Server**

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



The screenshot shows the GWN7000 web interface. The top navigation bar includes 'GWN7000 Firmware: 1.0.4.20', search, language (English), and user (admin). The left sidebar lists various system settings. The main content area is titled 'Maintenance' and has tabs for 'Basic', 'Upgrade', 'Access', 'Syslog', and 'Logserver'. The 'Logserver' tab is active, showing configuration options for WAN Firewall Rules, Logrotate File Size (5 MB), Logrotate File Count (56), Logrotate Mode (Every X hours), Hours, and Devices. There is an 'Enable Logserver' checkbox and 'Save'/'Reset' buttons. Below this is a 'Syslog File List' section with a 'Device' dropdown and a 'List' button. At the bottom, there are 'Download' and 'Clear' buttons and a table header for 'File Name', 'File Size', 'Last Modified', and 'Actions'. The table currently shows 'There are no syslog files.'

- **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 below:

Email/Notification

Email Notification

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 ?

Save Reset

[GWN7600&7600LR] FIRMWARE VERSION 1.0.4.12

PRODUCT NAME

GWN7600, GWN7600LR

DATE

10/31/2017

ENHANCEMENT

- Added support for **Timed Client Disconnect and Enhanced Client Blocking**
- Added support for **Client Bridge**
- Added support for **Syslog Server**
- Added support for **Configurable web UI access port**
- Added support for **E-mail notifications**

BUG FIX

- Fixed the WPA2 4-way handshake vulnerability*
- Fixed the WPA2 802.11r vulnerability*

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

<http://www.grandstream.com/sites/default/files/Resources/WPA%20Security%20Vulnerability.pdf>

- Fixed the issue that “Band Steering” option requires a system reboot to take effect.
- Fixed the issue that “Gateway MAC address” options and requires a system reboot to take effect.
- Fixed the issue that when Facebook and WeChat authentication are enabled at the same time, client cannot redirect to landing page after Facebook auth success.

- Fixed the issue that after many times of enabling and disabling Captive Portal, there is chances that WIFI clients can access to Internet without authentication challenge.

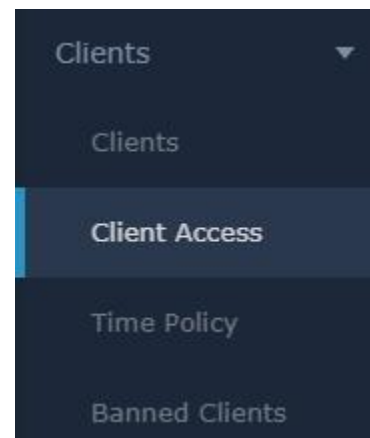
KNOWN ISSUE

- Configuring Radius server address with domain name instead of IP will cause the WIFI under configuration become open without authentication.
- “Hostname” on client page and the “Top AP” \ “Top SSID” \ “Top Clients” on overview page may show empty occasionally.
- After clicking on the reset button in maintenance page, it may prompt "Reset failed!".

NEW FEATURE OVERVIEW





- **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.



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

6) Client Access

+ Add		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	 

7) Time Policy

+ Add		Name	Enabled	Connection Time	Reconnect Type	Reconnect Time	Actions
		TEST_POLICY		3h	Reset Daily	23:00	 




8) 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 is turned into Client Bridge mode, it cannot be controlled by a Master

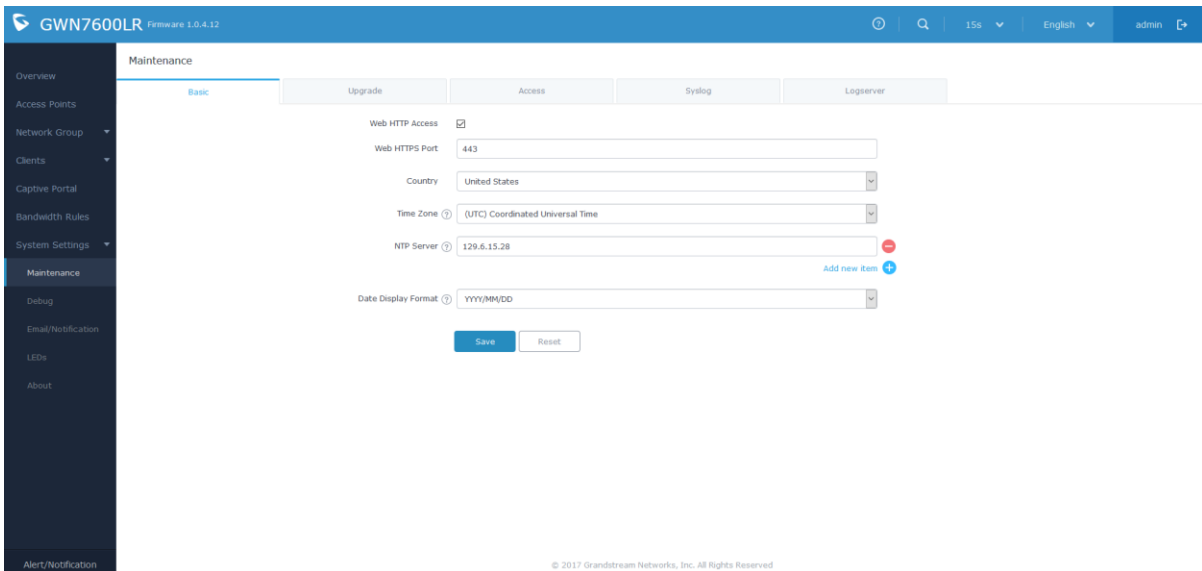
Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
GWN7610	00:08:82:97:90:8C	192.168.1.146	Online	1d 17h 51m 13s	1.0.4.19	  

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

anymore, and a factory reset is required to turn it back into normal AP mode.

- **Syslog Server**

Syslog Server is now available on GWN7600 and GWN700LR. Configuration page is as below:



The screenshot shows the configuration page for the Syslog Server on a GWN7600LR device. The page title is "GWN7600LR Firmware 1.0.4.12". The navigation menu on the left includes Overview, Access Points, Network Group, Clients, Captive Portal, Bandwidth Rules, System Settings, Maintenance (selected), Debug, Email/Notification, LEDs, and About. The Maintenance section has tabs for Basic, Upgrade, Access, Syslog, and Logserver. The Syslog tab is active, showing the following settings:

- Web HTTP Access:
- Web HTTPS Port: 443
- Country: United States
- Time Zone: (UTC) Coordinated Universal Time
- NTP Server: 129.6.15.28
- Date Display Format: YYYY/MM/DD

Buttons for "Save" and "Reset" are located at the bottom of the configuration area. A footer note reads "© 2017 Grandstream Networks, Inc. All Rights Reserved".

- **Configurable web UI access port**

Under System →Maintenance, following configuration is available now:

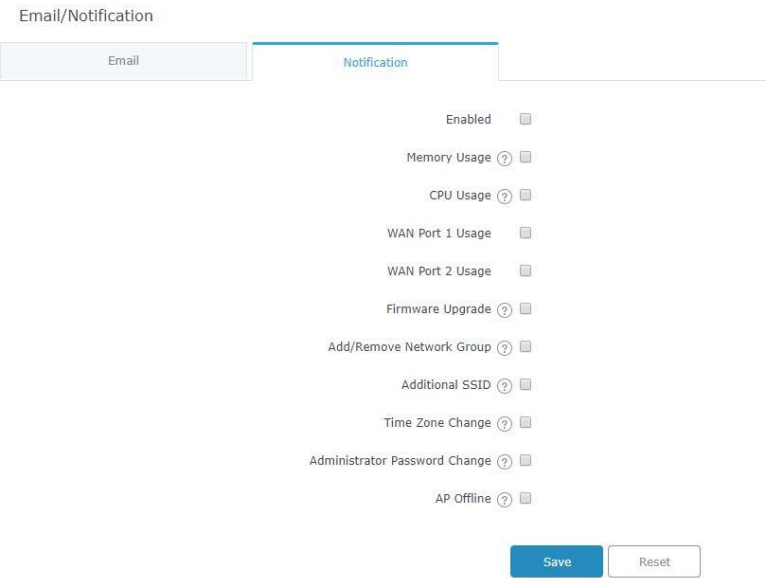
- 2) Web WAN Access;
- 2) Web HTTP Access;
- 3) Web HTTPS Port

- **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  below:



Email/Notification	
Email	Notification
<input type="checkbox"/>	Enabled <input type="checkbox"/>
<input type="checkbox"/>	Memory Usage (?) <input type="checkbox"/>
<input type="checkbox"/>	CPU Usage (?) <input type="checkbox"/>
<input type="checkbox"/>	WAN Port 1 Usage <input type="checkbox"/>
<input type="checkbox"/>	WAN Port 2 Usage <input type="checkbox"/>
<input type="checkbox"/>	Firmware Upgrade (?) <input type="checkbox"/>
<input type="checkbox"/>	Add/Remove Network Group (?) <input type="checkbox"/>
<input type="checkbox"/>	Additional SSID (?) <input type="checkbox"/>
<input type="checkbox"/>	Time Zone Change (?) <input type="checkbox"/>
<input type="checkbox"/>	Administrator Password Change (?) <input type="checkbox"/>
<input type="checkbox"/>	AP Offline (?) <input type="checkbox"/>

[GWN7600&7600LR] FIRMWARE VERSION 1.0.3.25

PRODUCT NAME

GWN7600, GWN7600LR

DATE

9/20/2017

IMPORTANT UPGRADING NOTE

This is the initial official release of GWN7600LR

BUG FIX

- Fixed issue that GWN7600's 5G radio power won't take effect after select frequency to only 5G.
- Fixed issue that WiFi client cannot connect to the 802.11g AP WIFI when it uses the 802.11b protocol.
- Fixed issue that WeChat authentication for Captive portal sometimes behaves abnormal and it will be hard for WIFI client to authenticate when issue happens.
- Fixed issue that Captive Portal Policy changes require a reboot to take effect.
- Fixed issue that device cannot catch packet if a value is set in "File Size" option.
- Fixed issue that 2.4GHz mode need to be enabled for changing Channel Width and Active Spatial Streams.
- Fixed issue that WeChat authentication of Captive portal does not work, when adopting WIFI has WEP security mode.
- Fixed issue that If only 802.11r is enabled, Voice enterprise feature will not take effect.
- Fixed issue that iPhone does not work with current Minimum RSSI design.
- Internal bug fixes

KNOWN ISSUE

- "Band Steering" and "Gateway MAC address" options and requires a system reboot to take effect.
- Configuring Radius server address with domain name instead of IP will cause the WIFI under configuration become open without authentication.
- "Hostname" on client page and the "Top AP" \ "Top SSID" \ "Top Clients" on overview page may show empty occasionally.
- After clicking on the reset button in maintenance page, it may prompt "Reset failed!".
- When Facebook and WeChat authentication are enabled at the same time, client cannot redirect to landing page after Facebook auth success.
- After many times of enabling and disabling Captive Portal, there is chances that WIFI clients can access to Internet without authentication challenge.

[GWN7610] FIRMWARE VERSION 1.0.3.21

PRODUCT NAME

GWN7610

DATE

8/11/2017

IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.108 or higher.
- Before starting to upgrade, please make sure your GWN7000 (the master device)'s firmware version is 1.0.2.71 or higher.

ENHANCEMENT

BUG FIX

- Fixed the issue that beacon frame has a random information element

KNOWN ISSUE

- 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.

-

[GWN7600&7600LR] FIRMWARE VERSION 1.0.3.19

PRODUCT NAME

GWN7600

DATE

7/14/2017

ENHANCEMENT

- Added support for **Captive Portal Enhancement**
- Added support for 802.11k/r/v (Enable Voice Enterprise)
- Added support for Failover Master
- Added support for VLAN assignment via RADIUS
- Added support for Select Band per SSID Added support for Exact Radio Power Configuration in dBm
- Added support for AP Locating by Blinking LED
- Added support for Per-Client/Per-SSID Bandwidth Management
- Added support for Limit Client Count per SSID
- Added support for WIFI schedule
- Added support for LED control
- Added support for Enabling/Disabling DHCP option 66 for firmware upgrade

BUG FIX

- Internal bug fixes

KNOWN ISSUE

- "Band Steering" and "Gateway MAC address" options and requires a system reboot to take effect.
- Configuring Radius server address with domain name instead of IP will cause the WIFI under configuration become open without authentication.
- "Hostname" on client page and the "Top AP" \ "Top SSID" \ "Top Clients" on overview page may show empty occasionally.
- GWN7600's 5G radio power won't take effect after select frequency to only 5G.
- Client cannot connect to the 802.11g AP WIFI when it uses the 802.11b protocol.
- After clicking on the reset button in maintenance page, it may prompt "Reset failed!".
- WeChat authentication for Captive portal sometimes behaves abnormal and it will be hard for WIFI client to authenticate when issue happens.
- When Facebook and WeChat authentication are enabled at the same time, client cannot redirect to landing page after Facebook auth success.
- After many times of enabling and disabling Captive Portal, there is chances that WIFI clients can access to Internet without authentication challenge.
- Device cannot catch packet if a value is set in "File Size" option.
- Captive Portal Policy changes require a reboot to take effect.
- 2.4GHz mode need to be enabled for changing Channel Width and Active Spatial Streams.
- WeChat authentication of Captive portal does not work, when adopting WIFI has WEP security mode.
- If only 802.11r is enabled, Voice enterprise feature will not take effect.
- iPhone does not work with current Minimum RSSI design.

NEW FEATURE OVERVIEW

- Captive Portal

You can configure different portal policies with names and adopt one policy while configuring your Network groups. Captive portal now also supports authentication by Radius and WeChat/Facebook.

Add ✕

Name

The field should not be empty

Expiration(s)

The field should not be empty

Authentication Type

WeChat Authentication

Facebook Authentication

Portal Page Customization

Landing Page

Enable HTTPS

Pre Authentication Rule(s)

Post Authentication Rule(s)

- 802.11k/r/v (Enable Voice Enterprise)

Configuration available at Network Group->Add/Edit->WIFI-> **Enable Voice Enterprise / Enable 11R / Enable 11K / Enable 11V**

Enable Voice Enterprise

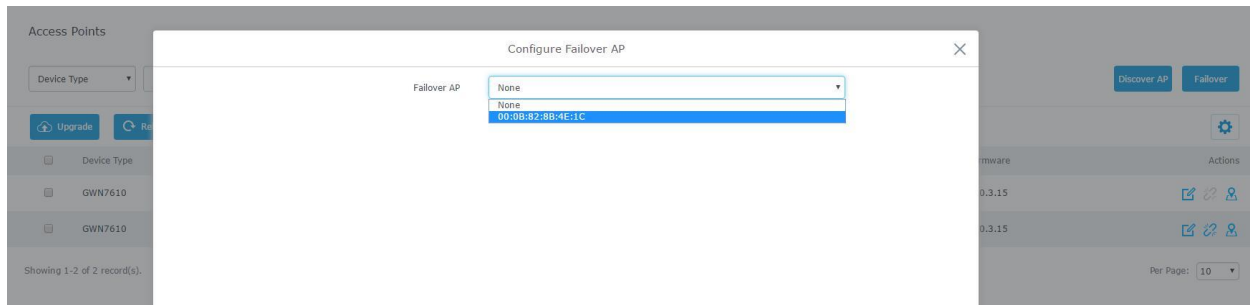
Enable 11R

Enable 11K

Enable 11V

- Failover Master

Failover Master is supported on GWN7600LR now. You can specify a slave AP as failover master. Whenever it detects the master is down, it will promote itself to be as failover master. After then, if master comes back, failover master will automatically go back to slave mode, or if the master doesn't come back to alive, Administrator can login to turn the failover master to true master and take over all controls.



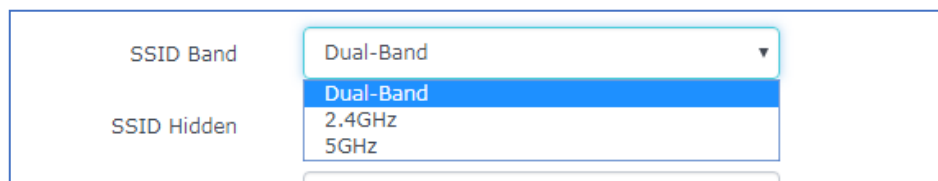
- AP Locating by Blinking LED

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	Locate the device
GWN7610	00:0B:82:8B:4E:1C	192.168.1.21	Online	1d 16h 6m 15s	1.0.3.15	Locate the device

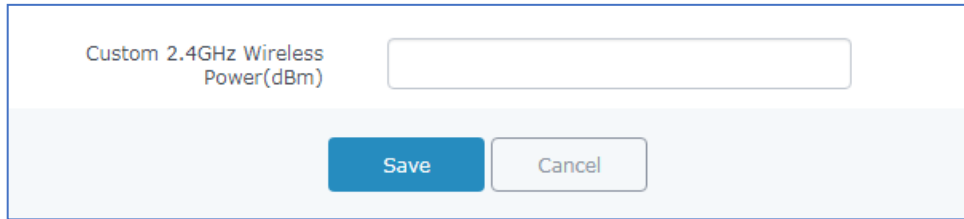
- Select Band per SSID

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



- Exact Radio Power Configuration in dBm

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



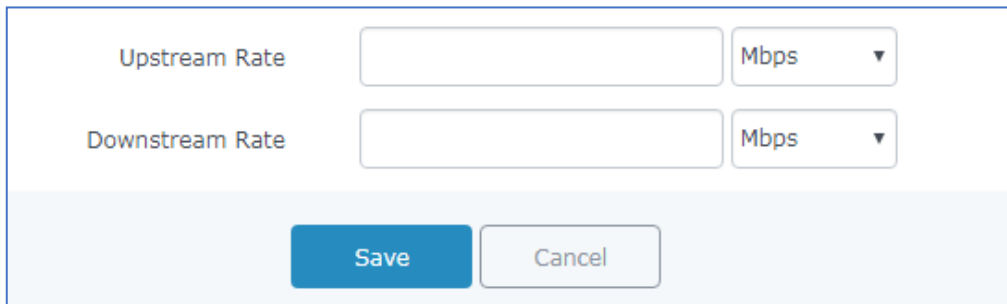
Custom 2.4GHz Wireless Power(dBm)

Save Cancel

- Per-Client/Per-SSID Bandwidth Management

Configuration available at

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

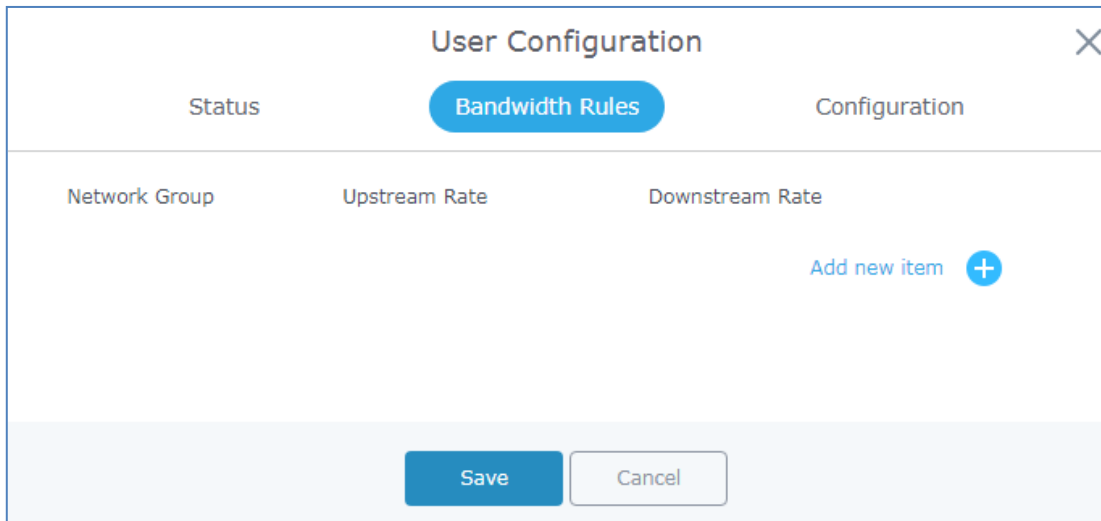


Upstream Rate Mbps ▾

Downstream Rate Mbps ▾

Save Cancel

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



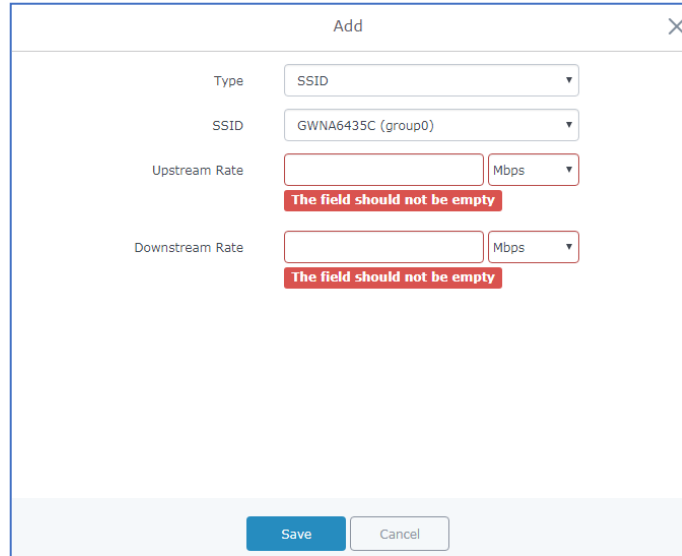
User Configuration [X]

Status **Bandwidth Rules** Configuration

Network Group	Upstream Rate	Downstream Rate
Add new item +		

Save Cancel

General configuration: **Bandwidth Rules** on left root menu bar.



Dialog: Add

Type: SSID

SSID: GWNA6435C (group0)

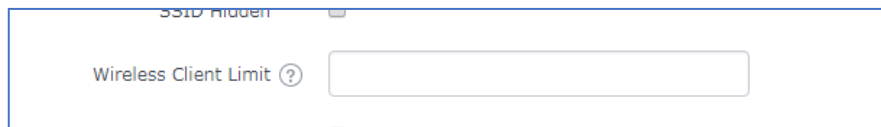
Upstream Rate: Mbps
 The field should not be empty

Downstream Rate: Mbps
 The field should not be empty

Buttons: Save, Cancel

- Limit Client Count per SSID

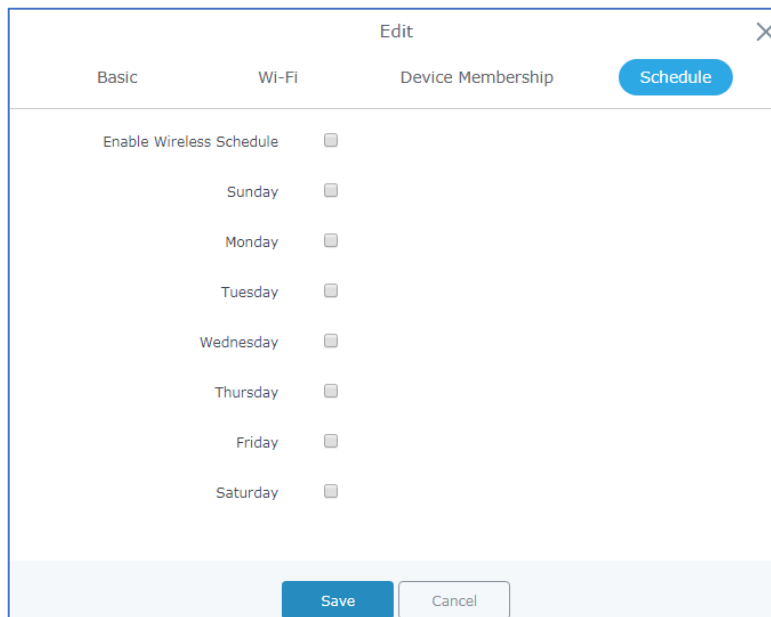
Configuration available at Network Group->Add/Edit->WIFI-> **Wireless Client Limit**.



Wireless Client Limit ?

- WIFI schedule

User can configure WIFI on/off schedule under Network Group->Edit->**Schedule**.



Dialog: Edit

Basic | Wi-Fi | Device Membership | **Schedule**

Enable Wireless Schedule

Sunday

Monday

Tuesday

Wednesday

Thursday

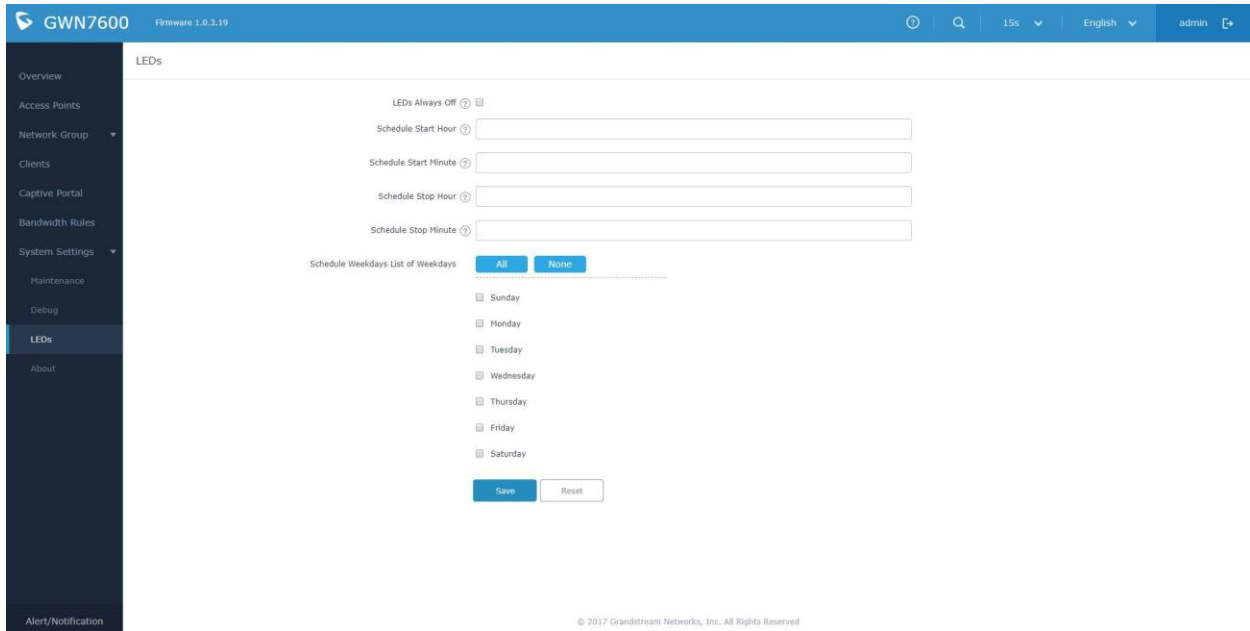
Friday

Saturday

Buttons: Save, Cancel

- LED control

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



- Enabling/Disabling DHCP option 66 for firmware upgrade

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

Allow DHCP options 66 and 43 override

[GWN7610] FIRMWARE VERSION 1.0.3.19

PRODUCT NAME

GWN7610

DATE

6/20/2017

IMPORTANT UPGRADING NOTE

- Before starting to upgrade, please make sure your GWN7610's firmware version is 1.0.2.108 or higher.
- Before starting to upgrade, please make sure your GWN7000 (the master device)'s firmware version is 1.0.2.71 or higher.

ENHANCEMENT

- Added support for **Captive Portal Enhancement** Added support for 802.11k/r/v (Enable Voice Enterprise) Added support for Failover Master
- Added support for VLAN assignment via RADIUS
- Added support for Select Band per SSID Added support for Selectively Enable b/g/n
- Added support for Exact Radio Power Configuration in dBm
- Added support for AP Locating by Blinking LED
- Added support for Per-Client/Per-SSID Bandwidth Management
- Added support for Limit Client Count per SSID
- Added support for Enabling/Disabling DHCP option 66 for firmware upgrade

BUG FIX

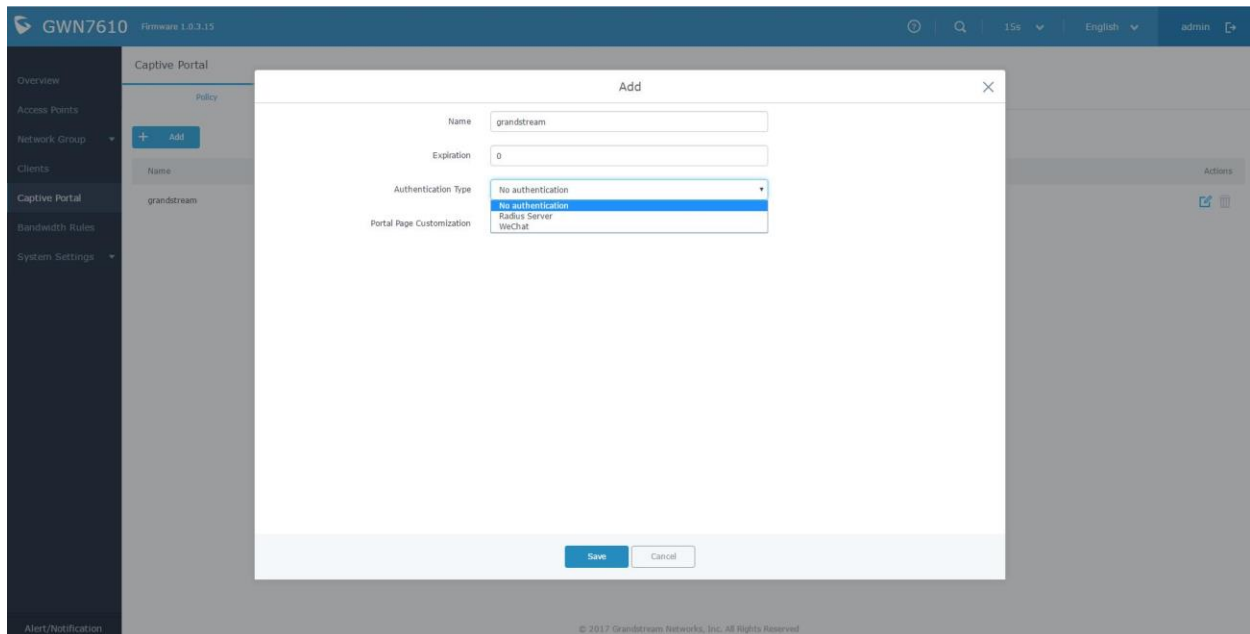
- Internal bug fixes

KNOWN ISSUE

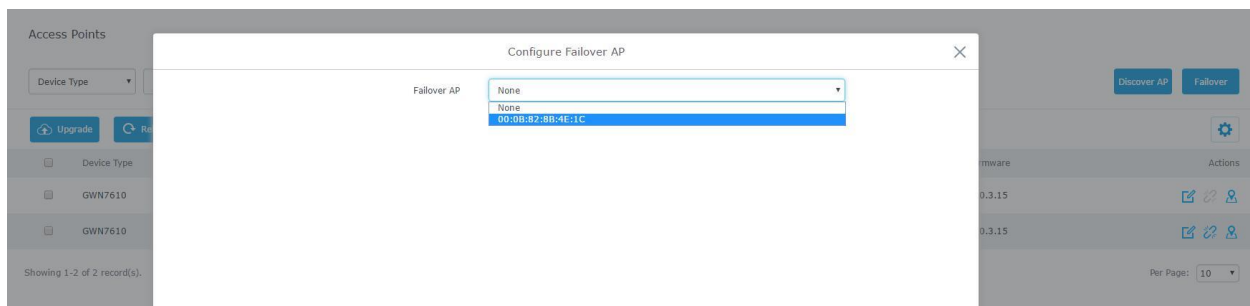
- Banned Band steering feature still affect wireless Black/White/Banned client list feature. Please use Band steering or Black/White/Banned client list feature exclusively.

NEW FEATURE OVERVIEW

- Captive Portal Enhancement
 1. Now you can configure different portal policies with names and adopt one policy while configuring your Network groups.
 2. Now captive portal starts to support authentication by Radius and WeChat.



- Failover Master









Failover Master is supported on GWN7610 now. You can specify a slave AP as failover master. Whenever it detects the master is down, it will promote itself to be as failover master. After then, if master comes back,

failover master will automatically go back to slave mode, or if the master doesn't come back to alive, Administrator can login to turn the failover master to true master and take over all controls.

- 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**.

- Enabling/Disabling DHCP option 66 for firmware upgrade

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

[GWN7610]FIRMWARE VERSION 1.0.2.108

PRODUCT NAME

GWN7610

DATE

4/19/2017

IMPORTANT UPGRADING NOTE

- Controller protocol security enhancement is important for secured provision from Master to Slave. So once a master with 1.0.2.108 found a slave with 1.0.2.15, it will disable the slave's wifi and show the slave's firmware version in RED BOLD to remind user to upgrade the slave. (This is implemented on GWN7000 version 1.0.2.71 too)

ENHANCEMENT

- Controller protocol security enhancement
- LED control
- Captive Portal
- Additional SSID
- WIFI schedule
- Client Isolation enhancement
- Syslog stored on unit and displayed on web is available now
- Few web enhancement.

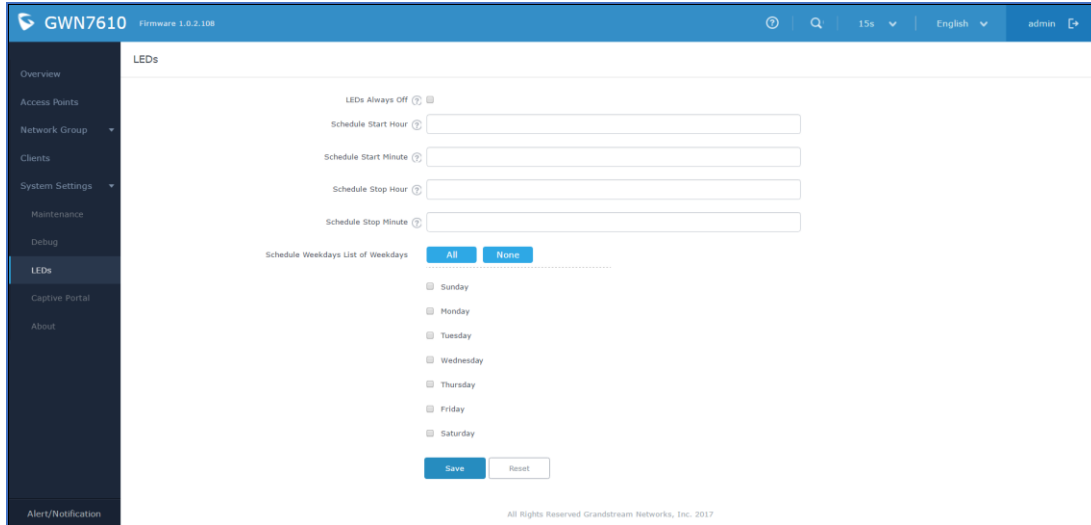
KNOWN ISSUE

- 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 FEATURE OVERVIEW

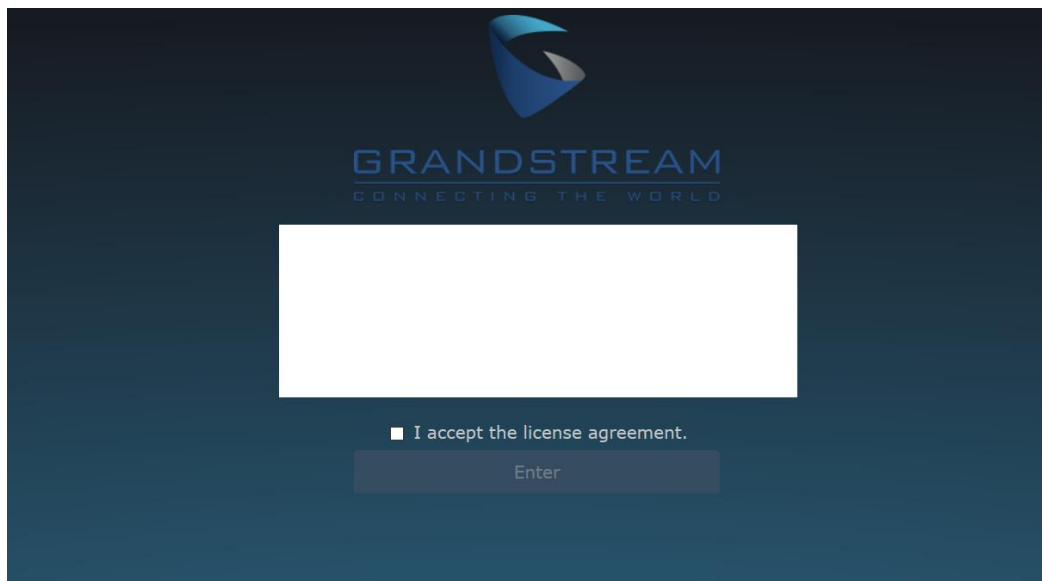
- LED control

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



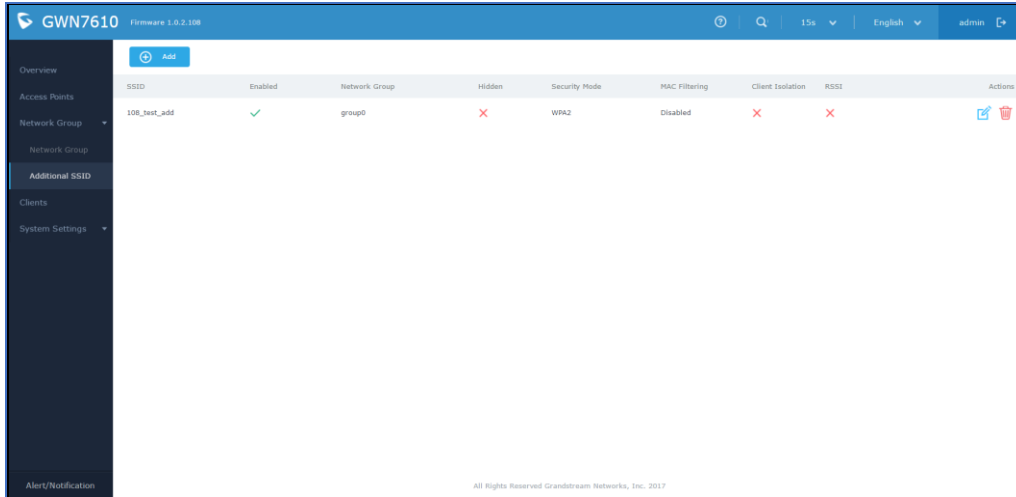
- Captive Portal

Configurations are available under System settings. Now user can customize the portal web page including their service terms by uploading splash.html and related web files in “Files” tag. (The blank window below is left for the service term to be customized)



- Additional SSID

Now user can add additional SSID to any network group by configuring the following page.

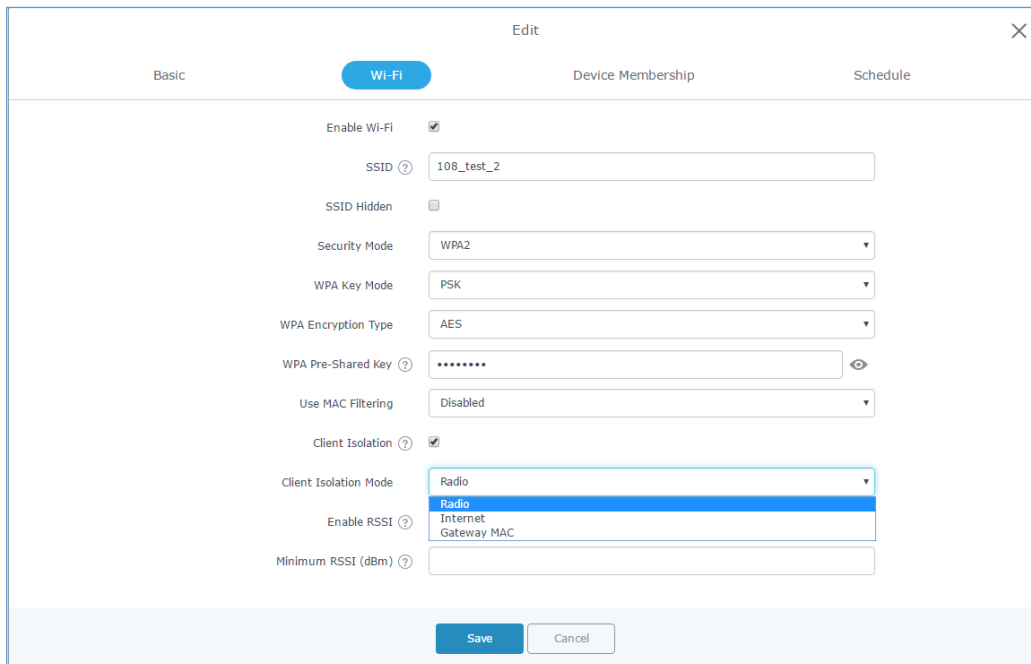


- **WIFI schedule**

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

- **Client Isolation enhancement**

Now, 3 client isolation modes (Radio/Internet/Gateway MAC) are available now. Please refer to user manual for the detailed features.



[GWN7600&7600LR]FIRMWARE VERSION 1.0.1.36

PRODUCT NAME

GWN7600

DATE

3/15/2017

IMPORTANT UPGRADING NOTE

This is the initial official release of GWN7600

[GWN7610]FIRMWARE VERSION 1.0.2.15

PRODUCT NAME

GWN7610

DATE

1/31/2017

IMPORTANT UPGRADING NOTE

This is the initial official release of GWN7610