



Grandstream Networks, Inc.

GWN Management Platforms
User Guide



WELCOME

Thank you for using Grandstream GWN Management Platform.

GWN Management Platforms are enterprise-grade Wi-Fi network management platforms that offer a centralized, streamlined network management and monitoring. This includes GWN.Cloud, the cloud-based platform and the GWN Manager which is a Linux based platform and GWN App for Android™ and iOS. It allows business to deploy a secure Wi-Fi network in seconds and manage these networks across multiple locations through a web user interface. Users can keep an eye on the network's performance with real-time monitoring, alerts, statistics and reports that can be viewed using a web browser or the mobile application. Support unified management for different types of GWN devices (Router, Switches, AP) in one network and SDN design, to make the network management more simple, and user friendly.

REQUIREMENTS

Following tables show the requirements of Grandstream networking products including GWN Access Points, GWN Routers, GWN Switches and GWN App versions (Android and iOS) for GWN Management Platforms (GWN.Cloud & GWN Manager):

- o **GWN Access Points: minimum and recommended version**

Model	Minimum	Recommended
GWN7600	1.0.15.20	1.0.25.10
GWN7600LR	1.0.15.20	1.0.25.10
GWN7602	1.0.15.20	1.0.25.10
GWN7605	1.0.15.18	1.0.25.10
GWN7605LR	1.0.15.18	1.0.25.10
GWN7610	1.0.15.18	1.0.25.10
GWN7615	1.0.15.18	1.0.25.10
GWN7624	1.0.21.5	1.0.25.10
GWN7625	1.0.21.5	1.0.25.10
GWN7630	1.0.15.20	1.0.25.10
GWN7630LR	1.0.15.20	1.0.25.10
GWN7660	1.0.19.4	1.0.25.10
GWN7660LR	1.0.19.4	1.0.25.10
GWN7661	1.0.23.26	1.0.25.10
GWN7662	1.0.23.27	1.0.25.10
GWN7664	1.0.21.4	1.0.25.10
GWN7664LR	1.0.23.4	1.0.25.10

○ **GWN Routers: minimum and recommended version**

Model	Minimum	Recommended
GWN7001	1.0.1.6	1.0.3.5
GWN7002	1.0.1.6	1.0.3.5
GWN7003	1.0.1.6	1.0.3.5
GWN7052	1.0.5.34	1.0.7.2
GWN7052F	1.0.5.4	1.0.7.2
GWN7062	1.0.5.34	1.0.7.2

Router minimum and recommended version

○ **GWN Switches: minimum and recommended version**

Model	Minimum	Recommended
GWN7801	1.0.3.19	1.0.3.19
GWN7801P	1.0.3.19	1.0.3.19
GWN7802	1.0.3.19	1.0.3.19
GWN7802P	1.0.3.19	1.0.3.19
GWN7803	1.0.3.19	1.0.3.19
GWN7803P	1.0.3.19	1.0.3.19
GWN7806	1.0.1.14	1.0.1.14
GWN7806P	1.0.1.14	1.0.1.14
GWN7811	1.0.1.8	1.0.1.8
GWN7811P	1.0.1.8	1.0.1.8
GWN7812P	1.0.1.8	1.0.1.8
GWN7813	1.0.1.8	1.0.1.8
GWN7813P	1.0.1.8	1.0.1.8

Switch minimum and recommended version

○ **GWN App: minimum and recommended version**

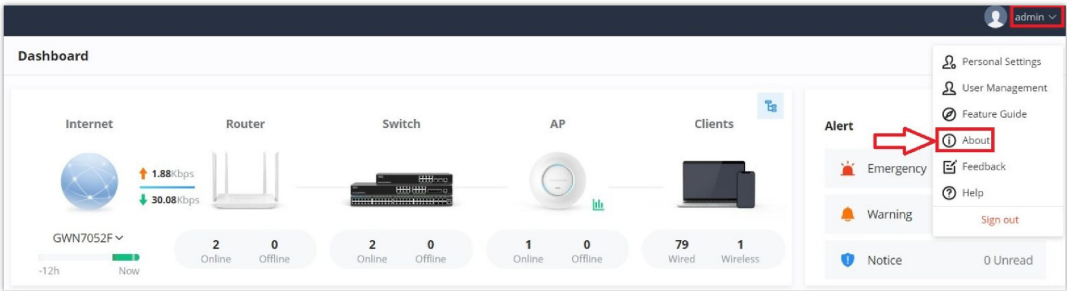
Platform	Minimum	Recommended
iOS	1.0.5	1.3.14

Android	1.0.0.14	1.0.3.14
---------	----------	----------

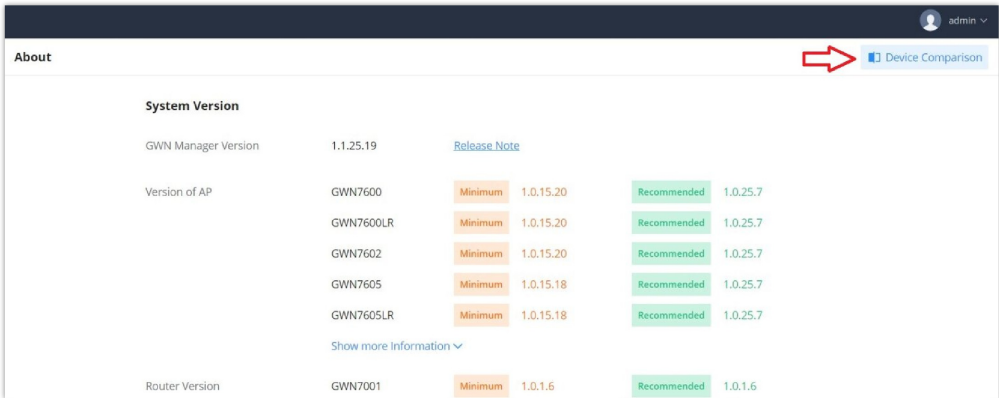
App minimum and recommended version

Requirements

To know more about the differences between devices in terms of functions based on the recommended versions, please navigate to **GWN.Cloud Web UI** → **About** → **Device Comparison**. refer to the figures below:



Device Comparison – Step 1



Device Comparison – Step 2

Function	Model	GWN7600	GWN7600LR	GWN7602	GWN7605	GWN7605LR	GWN7610	GWN7615	GWN7624
DFS(CE)			✓	✓	✓	✓		✓	
DFS(FCC)				✓	✓	✓		✓	
Wired Firewall Rules									
Wireless Firewall Rules		✓	✓	✓	✓	✓	✓	✓	✓
DFS(RCM)				✓	✓	✓		✓	✓
DFS(IC)				✓		✓		✓	✓
DFS(ANATEL)		✓		✓					✓
Band4(EU)			✓						
SSID - Client IP Assignment: NAT		✓	✓	✓	✓	✓	✓	✓	✓
SSID - Security Mode: WPA3				✓	✓		✓	✓	✓

Device Comparison

PRODUCT OVERVIEW

Features Highlights

GWN.Cloud	<ul style="list-style-type: none"> • Software-as-a-Service (SaaS) Solution to manage all your Grandstream GWN products (Access points, Routers and switches), without any additional on-premise infrastructure. • High level security, since all the traffic between GWN devices and cloud is secured. • Easy way to add new GWN devices, either using device MAC address or Mobile App (Android or iOS). • No limits on number of sites or GWN devices.
GWN Manager	<ul style="list-style-type: none"> • Linux based solution to secure and manage all your Grandstream GWN devices.

	<ul style="list-style-type: none"> • Automatically discover and Adopt GWN devices in your network. • Adopt GWN device manually using SSH or through Web GUI by setting the Manager address and port. • Up to 3000 GWN devices, with high performance hardware.
Shared	<ul style="list-style-type: none"> • Highly available with no single point of failure across the whole system. • Easy and intuitive dashboard for monitoring. • Network Group creation. • GWN devices and clients Centralized monitoring and management. • Captive portal configuration. • Bandwidth control per SSID, IP, or MAC address. • Unified GWN device management (Access points: GWN76xx, Routers: GWN7052/F and GWN7062) • Inventory management • Map to locate devices • Network topology

Features Highlights

Specifications

Function	<ul style="list-style-type: none"> • Network-based GWN devices management • Network/GWN devices/client monitoring
Security and Authentication	<ul style="list-style-type: none"> • Supports access policies configuration (blacklist, whitelist, time policy etc) • Multiple security modes including WPA, WPA2, WPA3, WEP, open, etc. • Bandwidth rules for client access • User and privilege management
Enterprise Features	<ul style="list-style-type: none"> • No limits on number of sites or GWN devices for GWN.Cloud and up to 3000 GWN devices for GWN Manager with high performance hardware. • Hosted by AWS with 99.99% uptime (GWN.Cloud only) • Bank-grade TLS encryption from end-to-end • X.509 certificate-based authentication • Supports Wi-Fi Alliance Voice-Enterprise • Mobile app for iOS and Android • Real-time Wi-Fi Scan for deployment • URL access log collection • Multiple Wi-Fi performance optimization methods including band steering, Minimum RSSI, ARP Proxy, IP multicast to unicast, etc
Supported Devices	<ul style="list-style-type: none"> • Access points: GWN76xx(LR) • Routers: GWN7052/F, GWN7062 and GWN700x • Switches: GWN780x(P), GWN781x(P) and GWN7806(P)
Captive Portals	<ul style="list-style-type: none"> • Splash page with built-in WYSIWYG editor • Social media integration • Multiple captive portal authentications including simple password, radius, voucher, custom field etc. • External captive portal integration • Real-time guest statistics and monitoring • Advertisement integration with flexible strategies • Export guest info into file and automatically send to email
Centralized Management	<ul style="list-style-type: none"> • Local data forwarding, no user traffic sent to the controller • Network-based GWN device management • Network/GWN device/client monitoring • Layer2 and Layer3 based GWN device discovery

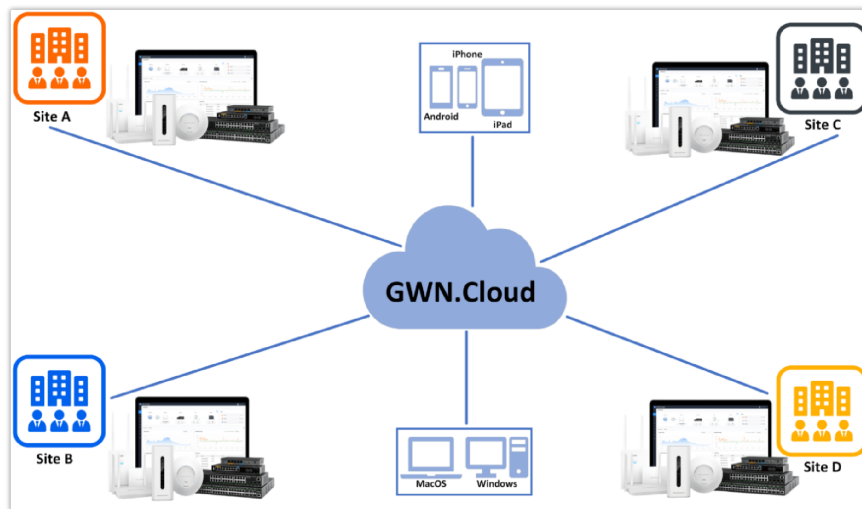
Reporting and Monitoring	<ul style="list-style-type: none"> • Real-time Network and client monitoring • Detailed reports by network, GWN devices, client etc. • Retrieval of historical data for statistical observations • Real-time alerts and event logs
Maintenance	<ul style="list-style-type: none"> • Ping/traceroute/capture • Both configuration and data backup • Scheduled GWN devices firmware update and LED control • Change log for audit trail
Languages	English, Chinese, Spanish, German, Portuguese, French and more.

GWN Management Platform specifications

GETTING TO KNOW GWN MANAGEMENT PLATFORM

GWN.Cloud

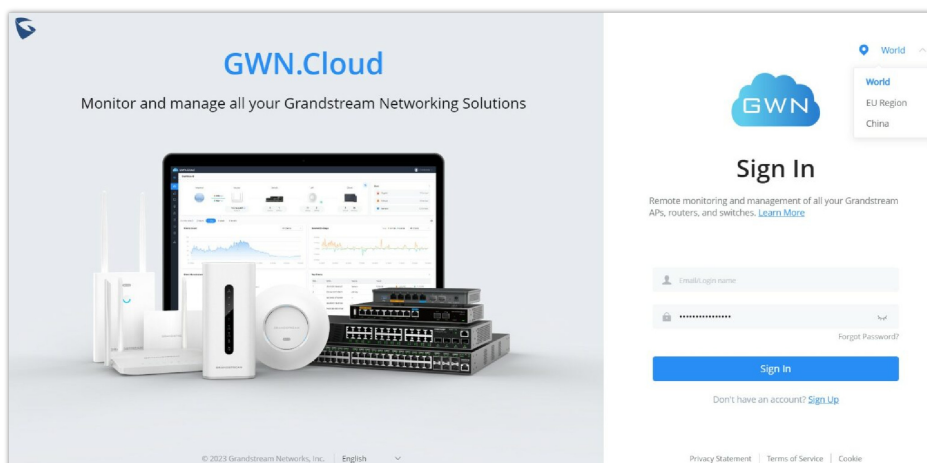
GWN.Cloud is a cloud-based platform used to manage and monitor GWN devices (Access Points, Routers, Switches) wherever they are as long as they are connected to the internet. The platform can be accessed using the following link: <https://www.gwn.cloud>. It provides an easy and intuitive web-based configuration interface as well as an Android and iOS App.



GWN.Cloud Architecture

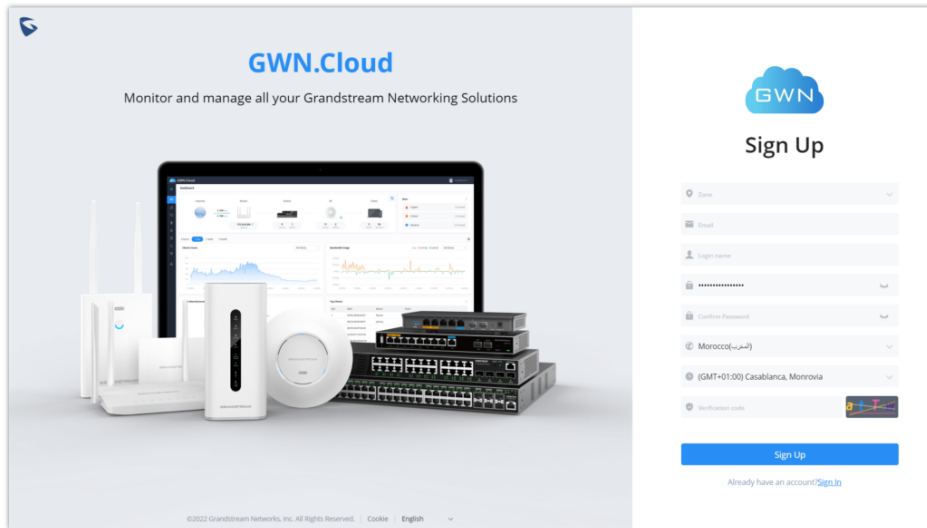
Sign up to GWN.Cloud

When accessing GWN.Cloud for the first time, users are required to sign up. The following screen will be displayed:



GWN.Cloud Login Page

1. Click on Sign up to go to the sign-up screen, then enter the required information.

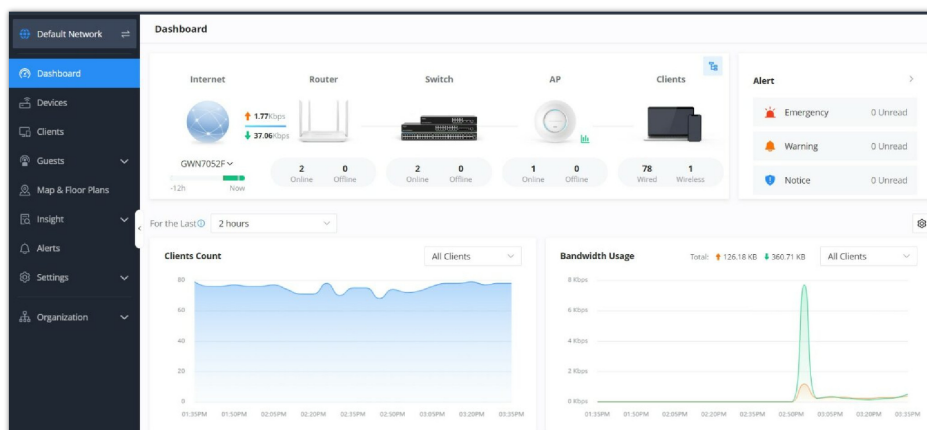


GWN.Cloud Sign up page

Zone	Users will need to choose US server or EU server to store their data at. This is mainly for GDPR regulation compliance.
Email	This email will be used to receive account activation link and also can be used as a username when login to GWN.Cloud.
Login name	Enter the login name that will be used to login to your GWN.Cloud space.
Password	Enter the password for Login authentication
Confirm password	Confirm the previously entered password
Country/Region	Enter the country/region on which applies to your account.
Time zone	Set your time zone.
Confirmation code	Copy the confirmation from the Captcha.

GWN.Cloud Sign up Settings

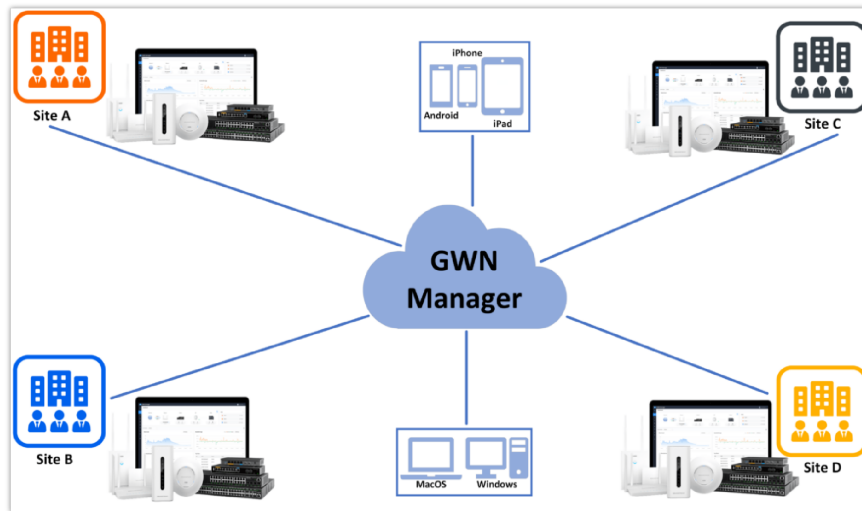
2. Once you create an account, you can access to your GWN.Cloud page for the first time and the following page will be displayed:



GWN.Cloud Dashboard

GWN Manager

GWN Manager is an On-premise GWN devices Controller used to manage and monitor GWN network devices including Access points, Routers on your network.



GWN Manager Architecture

GWN Manager hardware requirements

- OS: Linux Redhat7, CentOS 7

- Hardware:

For up to 200 APs and 2000 Clients:

- CPU: Intel® Core™ i3-3240 or above
- RAM: 4GB or above
- Storage: 250GB (dependent on retained data)

For up to 3000 devices and 30000 Clients:

- CPU: Intel® Xeon® Silver 4210
- RAM: 16GB or above
- Storage: 250GB (SSD preferred, depend on retained data size)

GWN Manager hardware requirements

Installation

To install GWN Manager please visit the links below:

[GWN Manager – Quick Installation Guide](#)

[GWN Manager – Deploying a Virtual Machine from an OVA file](#)

First Use

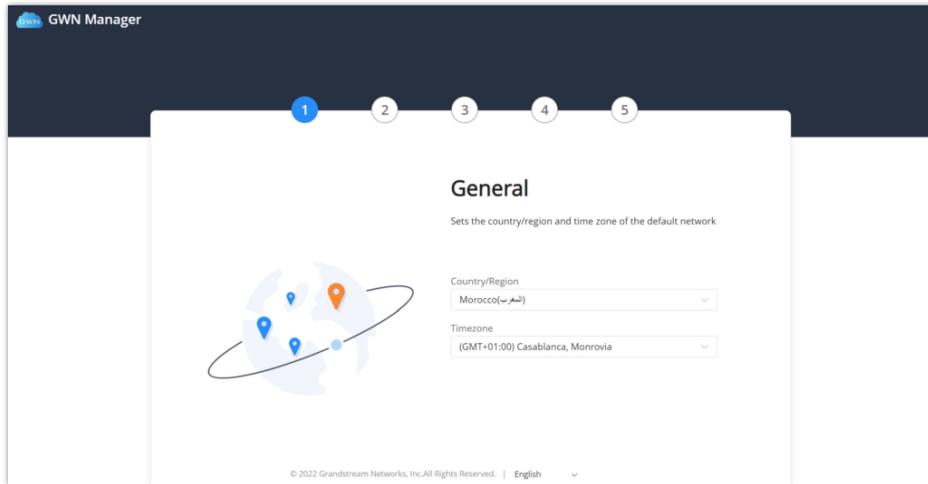
The GWN Manager provides an easy and intuitive Web UI to manage and monitor GWN network devices, it provides users access to all GWN settings, without any additional on-premise infrastructure.

On first use, users need to fill in additional information following the GWN Manager Wizard:

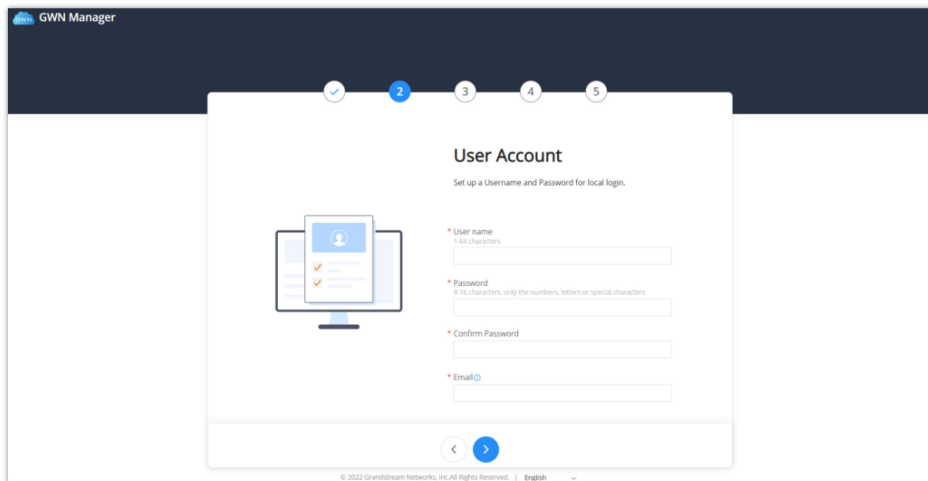
General	Specify the country/region and time zone for the default network. <i>Note: these parameters can be automatically detected by the system.</i>
User Account	Set up a username, password and email for local login.

Adopt Device	Select the GWN devices to be adopted by the default network. <i>Note: Access points, Routers available on the same LAN will be detected automatically.</i>
SSID Configuration	Create an SSID to be used by the default network for the first time. <i>Note: this SSID can be modified later.</i>
Summary	Review all the previous settings

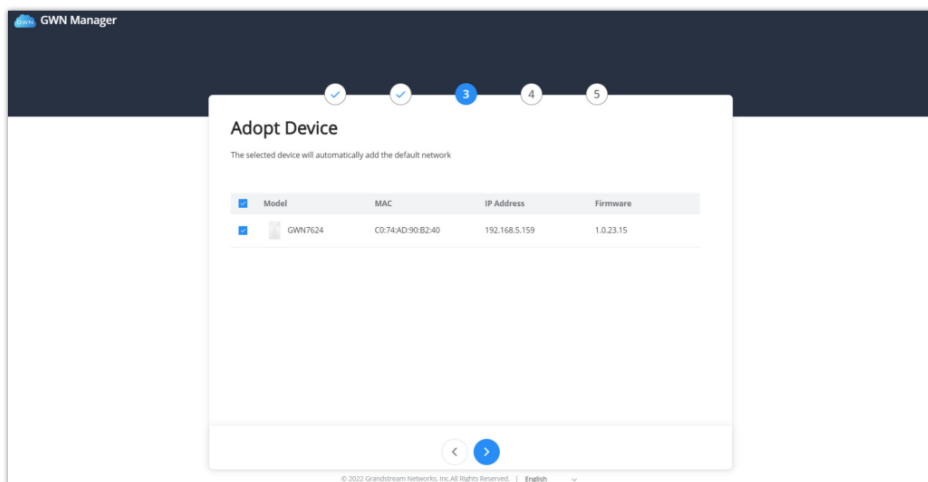
GWN Manager setup wizard



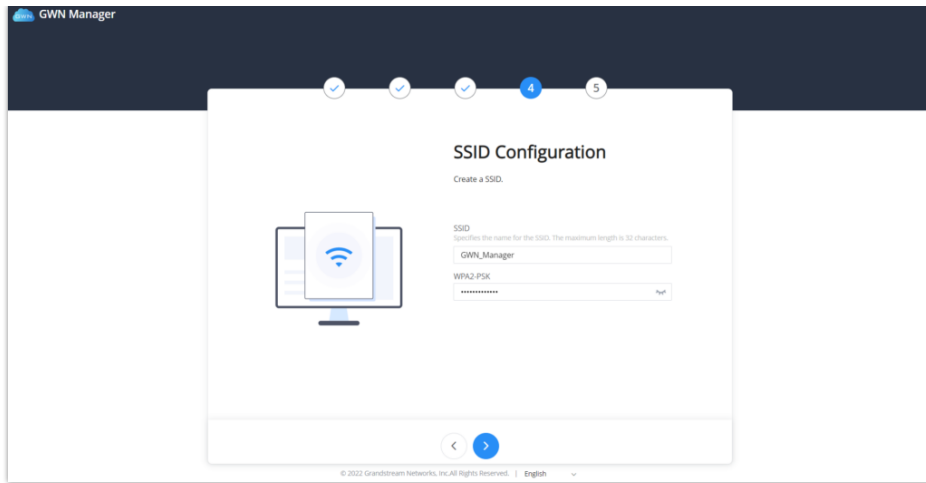
GWN Manager Wizard – Part 1



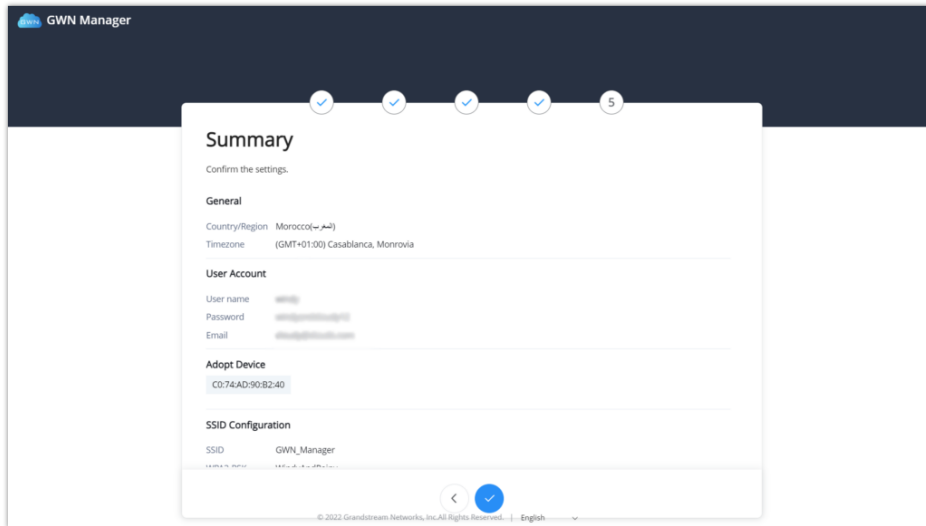
GWN Manager Wizard – Part 2



GWN Manager Wizard – part 3



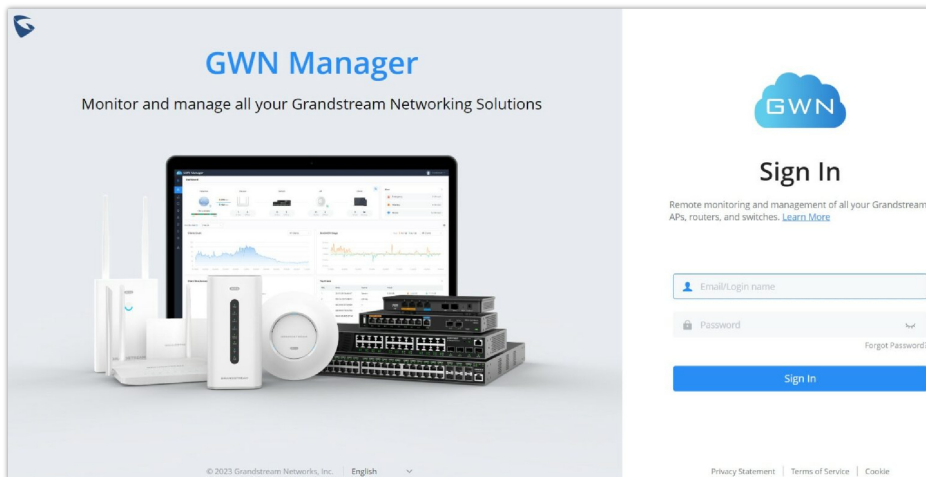
GWN Manager Wizard – part 4



GWN Manager Wizard – part 5

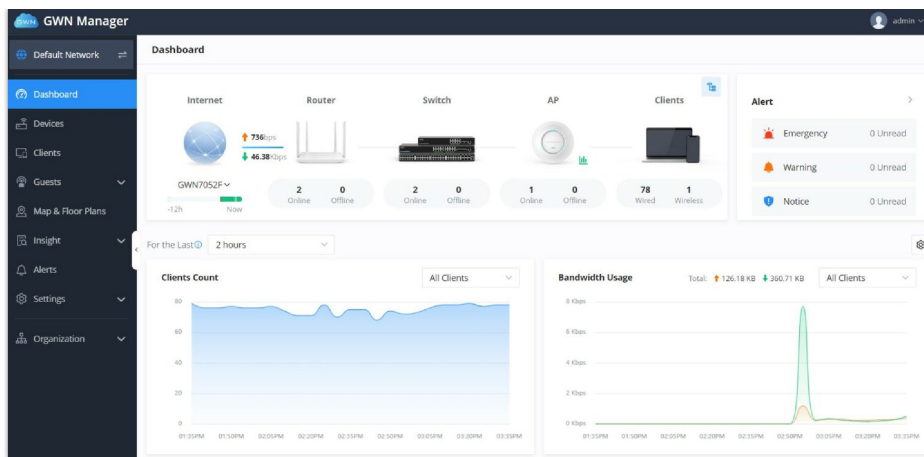
Sign up to GWN Manager

Enter the previously configured user credentials to access the GWN Manager GUI:



GWN Manager Login Page

The following page will be displayed:



GWN Manager Dashboard

GETTING STARTED WITH GWN MANAGEMENT PLATFORM

The GWN Management Platforms provide an easy and intuitive Web UI or mobile app (both Android & iOS versions) to manage and monitor GWN devices (Access points, Routers and Switches), it provides users access to all GWN devices settings, without any additional on-premise infrastructure.

Add a GWN Device to GWN Cloud

To add a GWN device to GWN.Cloud, the administrator needs two information:

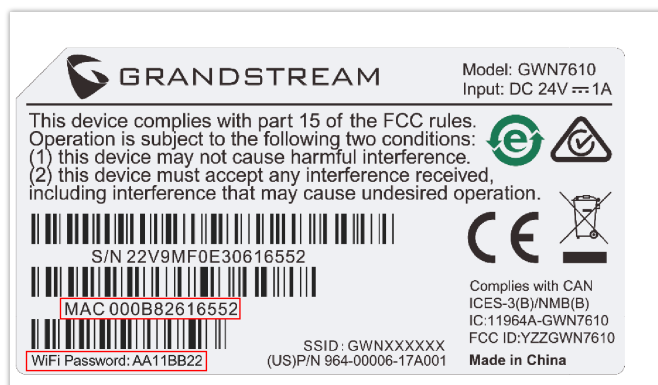
- o MAC address of the GWN device.
- o Password in the back of the unit.

There are 3 methods to add GWN device to the cloud:

1. **Method 1: Adding New GWN device Manually**
2. **Method 2: Adding New GWN device using GWN Application**
3. **Method 3: Transfer APs control from Local Master** (only for GWN Access points)

Method 1: Add a new GWN device manually

1. Locate the MAC address on the MAC tag of the unit, which is on device, or on the package.
2. Locate the Password.



GWN device MAC and Password

3. Navigate to **Devices** and click on **"Add"** button.

Devices

All Status All Models

<input type="checkbox"/>	Device Model	MAC	IP Address <input type="button" value="v"/>	Public IP Address <input type="button" value="v"/>	Device Group	Firmware <input type="button" value="v"/>	Operation <input type="button" value="v"/>
<input type="checkbox"/>	GWN7813P	C0:74:AD: [redacted] GWN7813P	192.168.80.211	[redacted]	Default	1.0.1.8	

Total 1

Adding a new GWN device to GWN.Cloud

4. Select a name for the device then enter the MAC address and Password, the user has also the option to add equipment remarks to easily identify the GWN devices when added to the GWN.Cloud or GWN Manager. Also, there is the option to select a device from the [Inventory](#) (previously claimed). Please, check the figures below:

Add Device

[Manual](#) [Inventory](#) [Import](#)

Name
1-64 characters

*** MAC**
 : : : : :

*** Password**

Equipment Remarks
0-64 characters

Adding a GWN device – Manual

Add Device

[Manual](#) [Inventory](#) [Import](#)

Device Group

<input type="checkbox"/>	Device Model	MAC	Serial Number	Device Name
<input checked="" type="checkbox"/>	GWN7661	C0:74:AD: [redacted]	[redacted] C	<input type="text" value="0-64 characters"/>
<input type="checkbox"/>	GWN7624	C0:74:AD: [redacted]	[redacted] 0	<input type="text" value="0-64 characters"/>

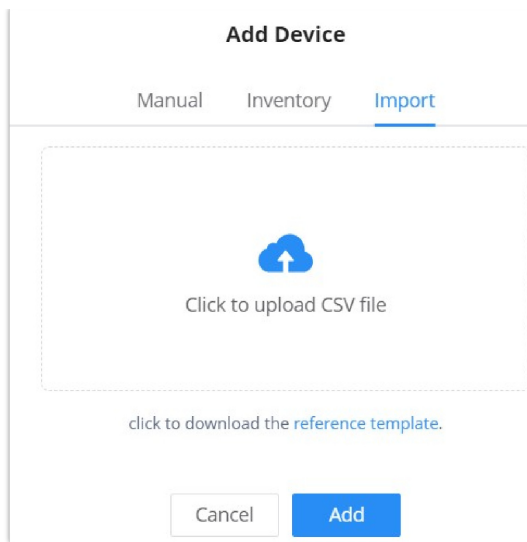
Adding a GWN device – Inventory

5. Click on **"Add"** button, the device will be added automatically to your Cloud account and you will be able to monitor/manage it.

Bulk-add devices using CSV file import

Another option for bulk-add devices is to use CSV file upload.

After clicking on **"Add"** under the menu **Devices**, click on **Import** Tab and click on **"Add"** button to select a CSV file.



Import CSV file for devices

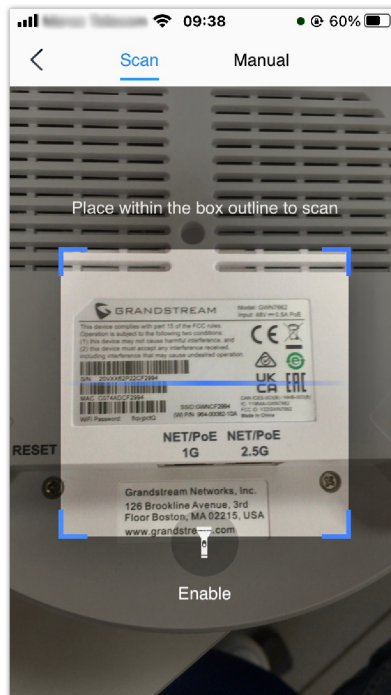
Method 2: Add a new GWN device using GWN.Cloud Application

An easy way to add new device to your GWN.Cloud is to use GWN.Cloud Application.

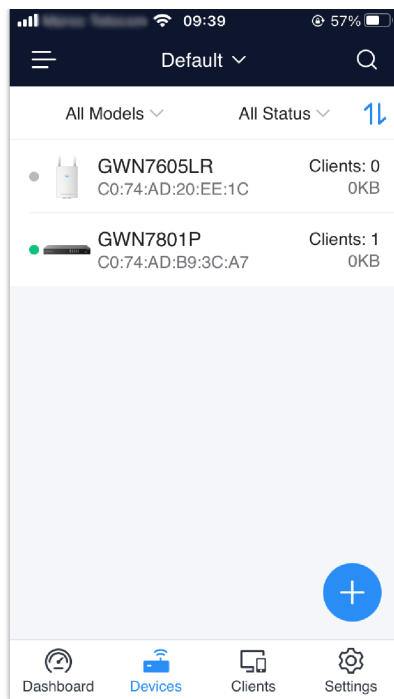
Note:

GWN App is available on Google Play for Android and App Store for iOS.

The operation is done by scanning the barcode from GWN device's sticker.



Adding a device to GWN.Cloud using GWN App – part 1



Adding a device to GWN.Cloud using GWN App – part 2

Once added, the list of devices will be displayed on GWN.Cloud interface.

Device Model	IP Address	Device Group	Num of Clients	Operation
GWN7624	192.168.5.110	New Device Group	1	⚙️
GWN7002	192.168.80.1	WAN	0	⚙️
GWN7052F	192.168.80.1	New Device Group	1	⚙️
GWN7803P	192.168.5.107	Default	154	⚙️
GWN7813P	192.168.5.109	New Device Group	152	⚙️

GWN devices list

Method 3: Transfer from Local Master

In the case where there is a local master managing the Access points. Another method to add GWN devices (Access points slaves) to the cloud is by transferring them to the cloud from the local Master. Follow these steps to achieve this:

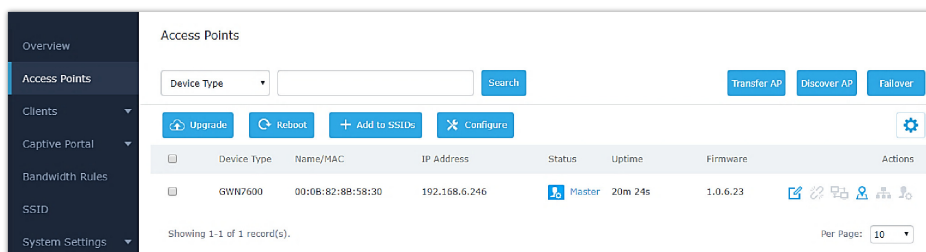
Note:

Transfer from local master method is only available for GWN Access points.

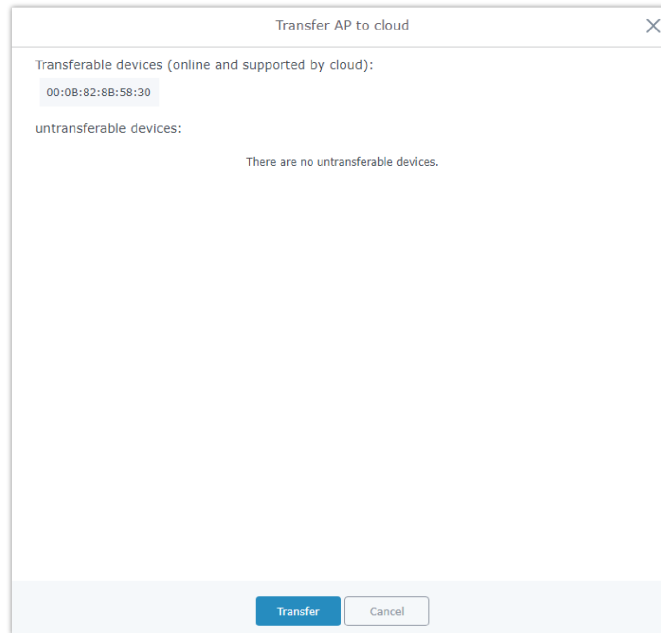
Note:

The following example is based on Access points where one of them is acting as a Local Master and the rest are Slaves.

1. Access the web UI of the local master and go to **Access Points**.



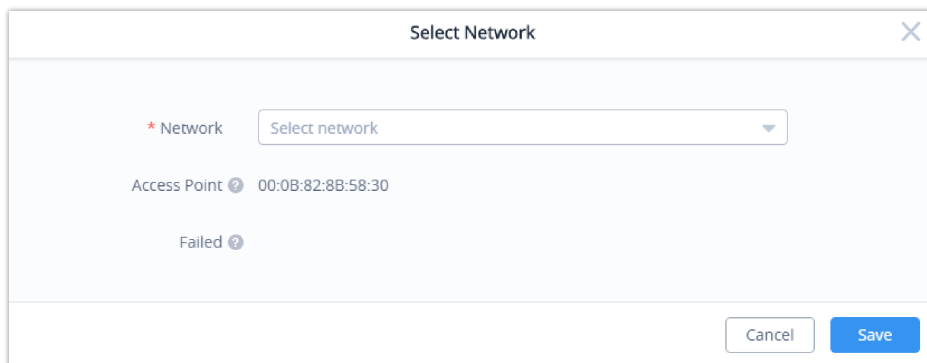
2. Press **Transfer AP** button. A new window will display “Transferable devices” list as shown below.



Transfer AP to Cloud

3. Press **Transfer** button. The web browser will redirect to GWN.Cloud login page.

4. Once logged in to the cloud, the configuration page “Select Network” will be displayed:



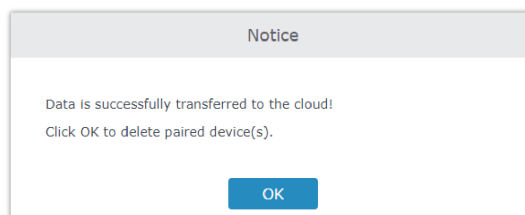
Select Network

- **Access Point:** Shows the MAC address of the passed check device.
- **Failed:** Shows the MAC address of the authentication failed or added.

5. Select **Network** from the drop-down list to which the AP will be assigned.

6. Press **Save** button to confirm.

7. Once added to the cloud, Master AP web UI will display following successful notice.



Transfer AP to Cloud – Success

Adopt a GWN Device to GWN Manager

To add GWN devices (router, switch or access point) to GWN manager:

1. Navigate to **GWN Manager Web UI → Devices**

2. Click on **“Adopt”** button.



Adding a new GWN device to GWN Manager

3. If GWN Manager connects to the same local subnet as GWN devices, it can discover the devices automatically via layer 2 broadcast. GWN devices accept DHCP option 224 encapsulated in option 43 to direct the controller. An example of DHCP option 43 configuration would be:

```
224 (type) 18 (length) 172.16.1.124:10014 (value) translated into Hex as e0123137322e31362e312e3132343a3130303134
```



Auto detect GWN devices

4. Select a device by checking the box on its left. Or select all by checking the top box. Then click **“OK”** button.

Adopting GWN devices manually

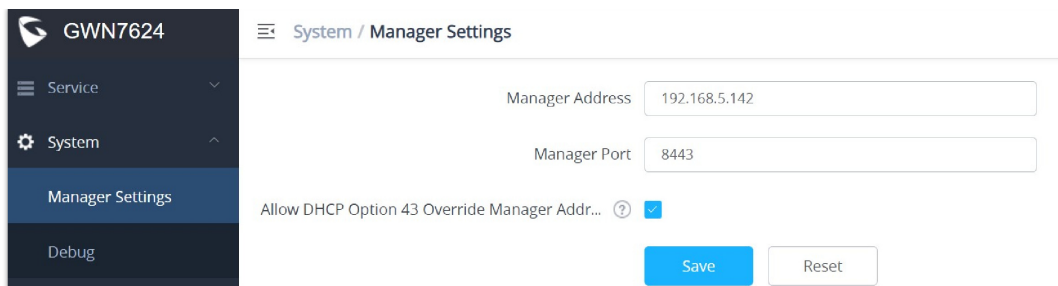
To manually configure the manager address and port on a GWN device, enable Manager Settings and fill in the Manager Address and Port and finally click on **“Save”** button. For each GWN device (AP, Router or Switch), please check the steps below:

Note:

We are going to use the example of a Slave Access point.

You can log into WebUI of slave AP or an unpaired AP to set the Manager address and port.

For GWN APs, please log in to the GWN AP in slave mode, then navigate to **GWN AP Web UI** → **System** → **Manager Settings**.



Manager Settings – Slave WebGUI

For GWN routers, please navigate to **GWN Router Web UI** → **System Settings** → **Basic Settings** page → **Manager Server Settings** tab.

For GWN switches, please navigate to **GWN Switch Web UI** → **System** → **Access Control** page → **Manager Settings** tab.

It's also possible to SSH a slave AP and use GWN menu to set the Manager address and port (8443).

```

Main Menu
[1] Status
[4] Clients
[9] Maintenance
[11] Software Manager
[0] Debug

[x] Exit
Select by pressing the [number] or [letter] and then ENTER
11
Software Manager

[1] Manager Address: :10014
[x] Back
Select by pressing the [number] or [letter] and then ENTER
1
[x] Back

Enter Manager Address Please input ip/domain:port (e.g. x.x.x.x:10014)!
Select by pressing the [number] or [letter] and then ENTER
192.168.5.142:8443
  
```

Manager Settings – SSH

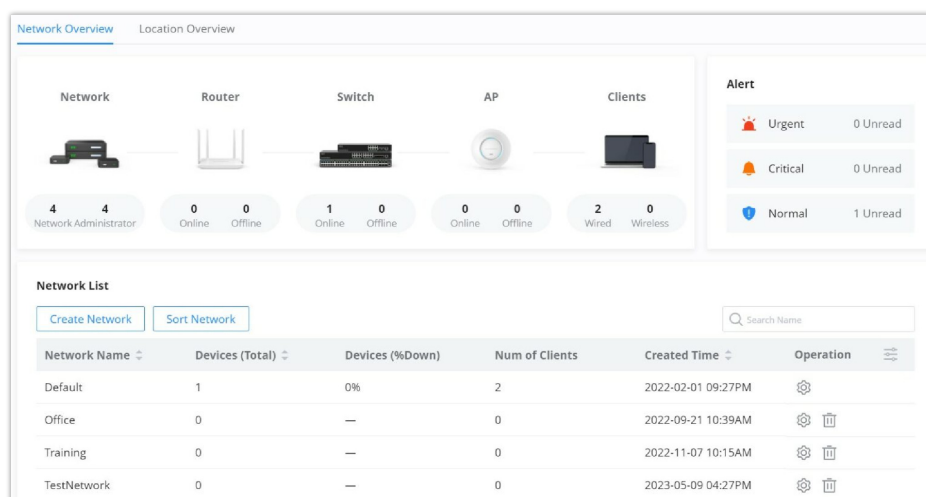
NETWORKS

The network page provides an information regarding all the network groups created under your account, once the administrator selects one network all the other configuration pages will change to reflect the information related to the selected network.

Create a new Network

To create a new Network:

1. Navigate to **GWN Manager Web UI** → **Organization** → **Overview** → **Network Overview Tab**, all the previously created networks will be displayed here.
2. Click on **“Create Network”** button and enter the network name, country/region, time zone, Network Administrator and select a network in case you want to clone a previously created network.



Network list

Overview > **Create Network**

* Network Name

* Country/Region

* Time Zone

Network Administrator

Optional Account ▾

Clone Network

Default
Office

Create Network

Setting	Description
Network Name	Enter the network Name to identify different networks in your environment.
Country/Region	Select the country/Region, this is required to set the Wi-Fi specifications of your country on GWN devices.
Time Zone	Select your time zone.
Network Administrator	This field displays the list of administrators that can manage this network.
Clone network	When you have an existing Network, you can choose to clone the new one with the already existing network.

Create a New Network Settings

Move a device to a Network

To move a GWN device to another Network, please navigate to **Devices page**, then select the desired devices, click on **“More”** button then select **“Move”**, after that a pop window will appear to choose the destination network where the selected devices will be moved to.

The screenshot shows the 'Devices' page with a table of devices. A red arrow points to the 'More' button in the top navigation bar. A context menu is open over the first device, GWN7624, with the 'Move' option highlighted in red.

Device Model	IP Address	Device Group	Num of Clients	Operation
<input checked="" type="checkbox"/> GWN7624	192.168.5.110	New Device Group	1	
<input type="checkbox"/> GWN7002	192.168.80.1	WAN	0	
<input type="checkbox"/> GWN7052F	192.168.80.1	New Device Group	1	
<input type="checkbox"/> GWN7803P	192.168.5.107	Default	166	
<input type="checkbox"/> GWN7813P	192.168.5.109	New Device Group	146	

Move a Device to different network

Share a Network

GWN Platforms allow sharing a network among the administrators on the organization. To share a network please navigate to **Organization** → **Overview**, then click the configuration icon of the network you wish to share.

Network List

[Create Network](#) [Sort Network](#)

Network Name	Devices (Total)	Devices (%Down)	Num of Clients	Created Time	Operation
Network A	0	—	0	2023-05-19 10:19PM	
Organization A	0	—	0	2023-05-19 04:40PM	
Default Network	2	100%	0	2022-12-23 10:02AM	

Total 3

Network List

Overview > **Network A** [Share Network](#)

* Network Name 1-64 characters

* Country/Region

* Time Zone

Network Administrator

Edit Network

Share Network ✕

Sharing Permission

Co-management
Manage the current network with another user


Transfer Management
The current network management authority will be issued to the shared account (history client statistic will not be shared), and you will no longer manage it.

Read-only Privilege
The co-management will have read-only access to the current network.

* **Shared Account**
The region's super administrator's email address must be used.

Share Network

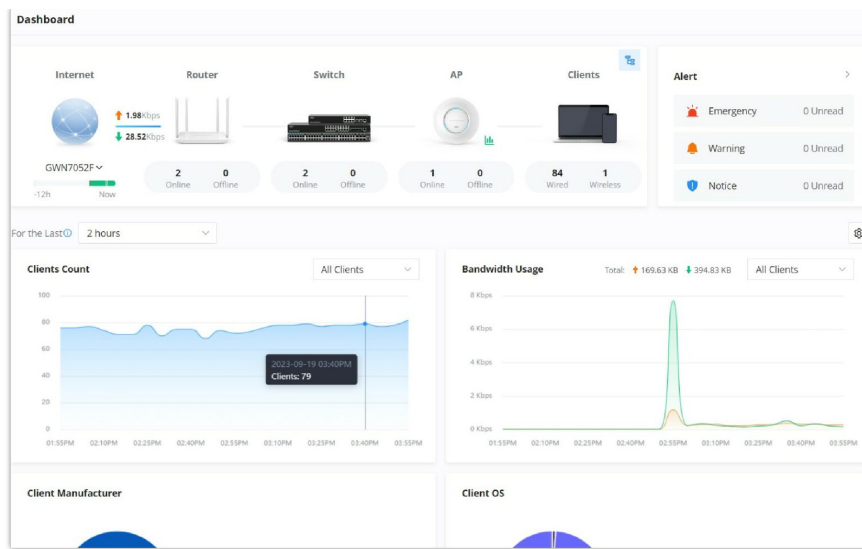
DASHBOARD

The Dashboard page provides general information that can be used to monitor GWN devices (The Router with its WAN IP, Switches and Access Points) and Clients. It also displays the number of Devices online and offline and as for Clients it displays the number of wired and wireless clients. It does also displays Alerts preview and the user can click on  icon to open the Alerts page with more details.

Note:

Clicking on one of the devices, will redirect the user to the Devices page, and clicking on Clients will redirect the user to the Clients page.

Click on this icon  to get redirected to the Network Topology page.

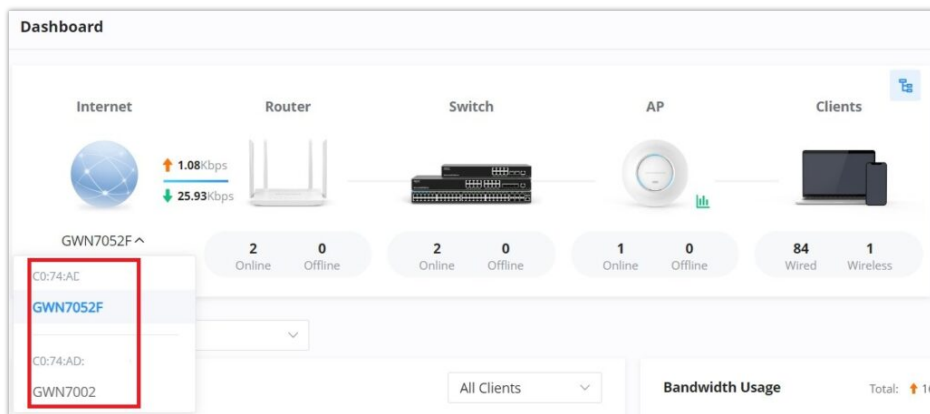


Dashboard

Network Health Monitor

Network Health Monitor is a feature that monitor the WAN (WAN ports or Device group) and displays the WAN status for the last 12 hours for each WAN with color code.

On Dashboard page, under internet section select the WAN port. Please refer to the figure below:



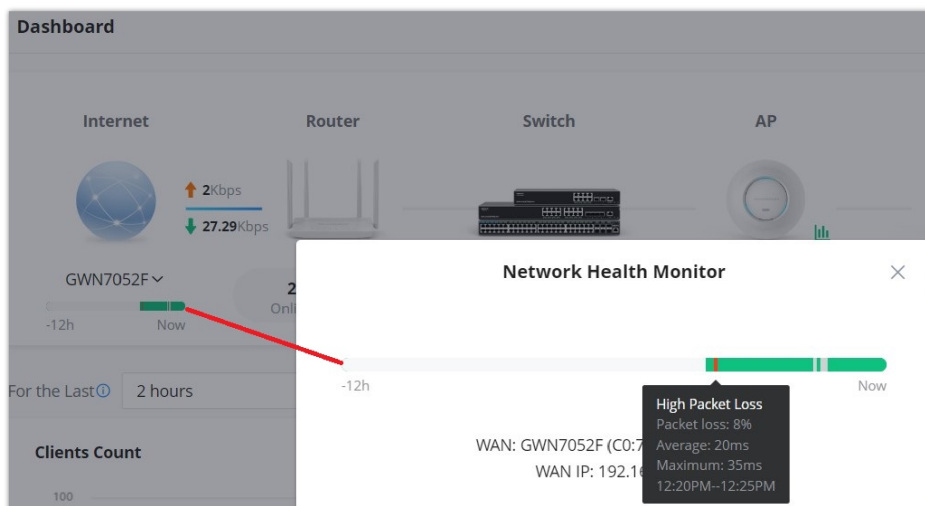
Network Health Monitor

Then, Click on the time bar to get a full view of the last 12 hours status, hover the cursor over the color to get more details and the duration. Please check the color code meaning below:

Green: Online

Grey: Offline

Red: High Packets Loss

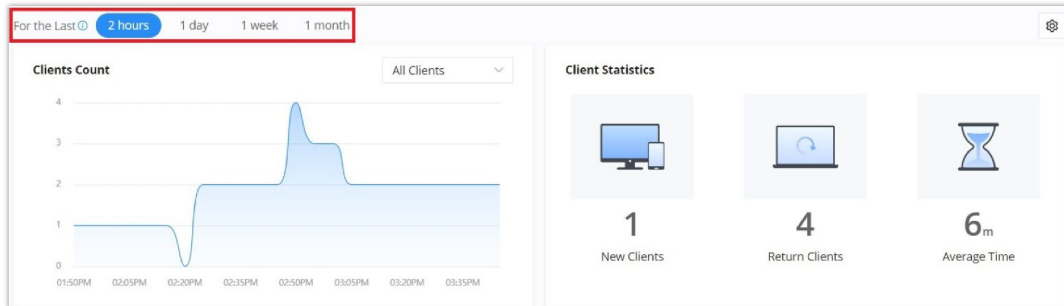


The user can choose the statistical duration of the data to review for the last 2 hours, 1 day, 1 week, 1 month, 3 month or 6 month.

- o **2 hours and one day:** Refresh and record data every 5 minutes.
- o **1 week:** Refresh and record data every 30 minutes.
- o **1, 3, and 6 months:** Refresh and record data every 3 hours.

Note:

3 months and 6 months duration are available on GWN Manager.



Charts Time

To customize the Dashboard page by adding or removing charts, please click on this icon, refer to the figure below:

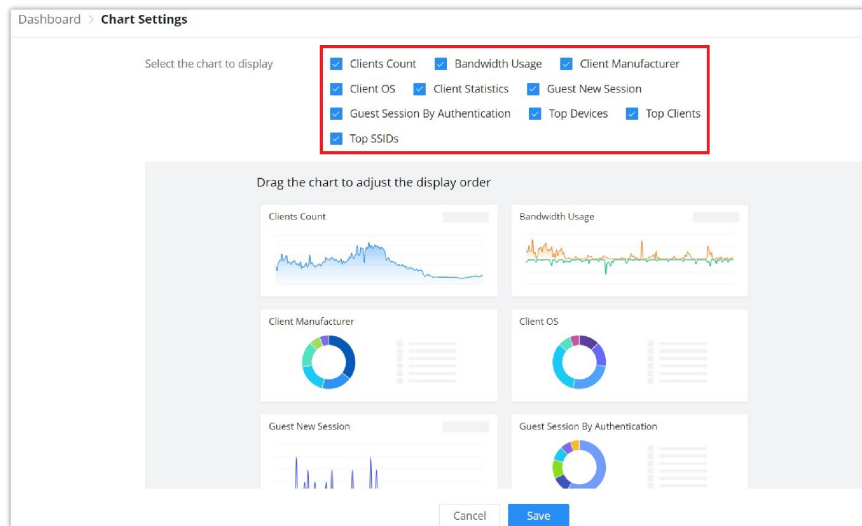
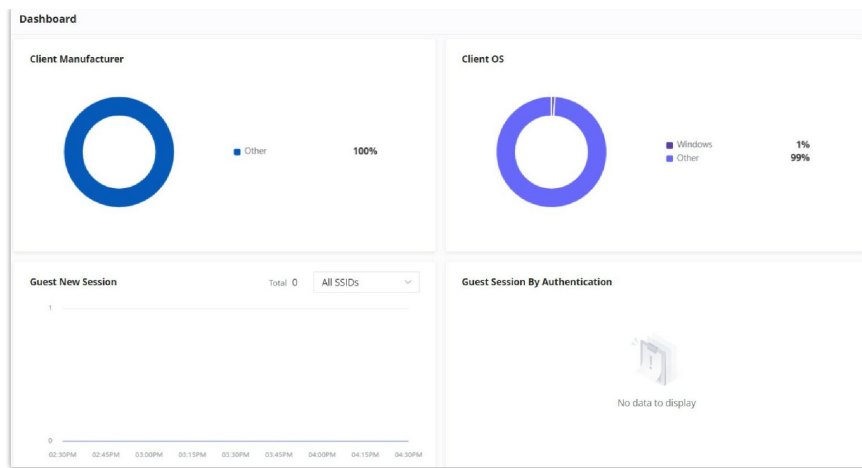


Chart Settings

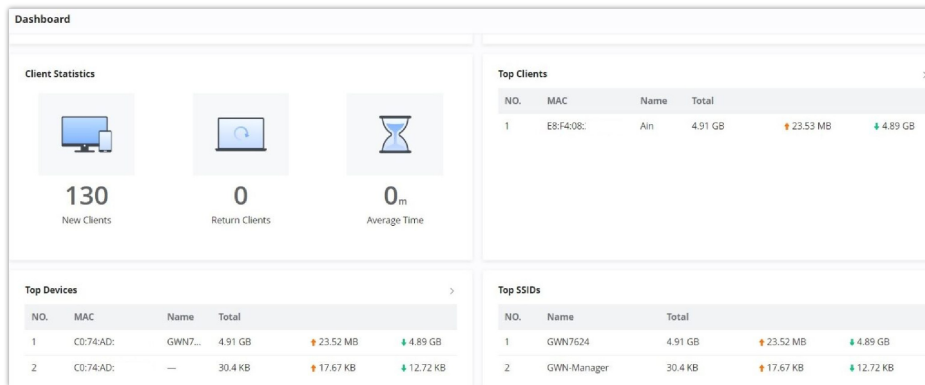
Client Count	It shows the number of clients connected at a specific period of time.
Client OS	It shows the Operating Systems used by Clients and the percentage of each.
Clients Statistics	Displays New Clients, Return Clients and Average Time.
Top SSIDs	Displays the SSIDs that are mostly used by clients.
Bandwidth Usage	This section shows the bandwidth usage (Upload/Download) by all the clients, it provides the BW statistics for both Download and upload.
Guest New Session	Displays the period of time, where new Guest session started and ended.
Top Clients	Lists the clients that downloaded/uploaded the max of data
Client Manufacturer	Displays the percentage of each Manufacturer used by Clients.
Guest Session by Authentication	Displays the percentage of Guest session by Authentication
Top Devices	Lists the devices by amount of the total usage.

Chart Settings

Example:



Example 1



Example 2

DEVICES

In this page users can Add (GWN.Cloud) or Adopt (GWN manager), export list of devices, move to a different network/Device group, reset, delete, configure, reboot or push configuration.

Group Management

Group management is a logical group that contains devices either for the same model or different models. This helps to make GWN devices management even easier, for example there is a pre-set features for switches when added to a group or when the user wants to apply certain configuration on many devices at the same time, he can apply them on the device group that contains these devices etc.

To create or edit a Device group, please navigate to **Web UI** → **Devices** page then click on **“Group Management”** button.

Devices

Adopt | Export | **Group Management** | More

All Status | All Models | Q MAC/Name/IP/Device G

Device Model	MAC	IP Address	Device Group	Num of Clients	Operation
<input type="checkbox"/> GWN7624	C0:74:AD:90:B2:40 GWN7624	192.168.5.110	device x	0	
<input type="checkbox"/> GWN7813P	C0:74:AD:DF:CC:94	192.168.5.109	device x	142	

Group Management

Devices > Group Management

Q Group name

Default **GWN_Device**

Move Devices | All Models | Q MAC/Name

Device Model	MAC	Name
<input type="checkbox"/> GWN7813P	C0:74:AD:DF:CC:94	—
<input type="checkbox"/> GWN7624	C0:74:AD:90:B2:40	GWN7624

Group Management list

To add a new Device group or add devices to previously created Device group click on “+” icon, to delete or modify a Device group click on “Edit” or “Delete” icons respectively.

Add a Device Group

Note:

Please note that device group depends on the configuration for example:

- For Wireless LAN (Wi-Fi or SSID), the device group must only contains wireless devices e.g: GWN APs.
- For Router parameter under Settings → Internet → Add WAN, the device group must contains only routers of the same mode.

Switch Pre-Provisioning

Switch Pre-Provisioning feature allows the user to pre-configure port settings and CLI commands for the switches that belong to the same device group. Once the GWN switches are added to the device group the pre-configurations will take effect.

Note:

Only applies to the switches added the first time.

- **Port Settings**

On this section, the user can pre-configure the switch ports with a port profile and Trust DHCP Snooping (On or Off).

Click on “+” or “-” icons to add or delete a port settings. Please refer to the figure below:

Note:

If the port is not selected on the device, it will not take effect.

- **CLI Command**

The user can enter the CLI commands here, separated by “Enter”. Please use English and characters only, and use the “#” key for comment line.

Switch Pre-Provisioning

Only applies to the switches added the first time.

Port Settings

Port	Port Profile	Trust DHCP Snooping
1 +3	All VLANs	On
5 +1	Default LAN	Off

CLI Command

```
# this is an example
configure
vlan 2
exit
interface Ethernet 1/0/1
switchport mode access
```

Cancel Save

Switch Pre-Provisioning

Push Configuration

Push configuration feature helps to push GWN.Cloud or GWN Manager configuration to the local side of added GWN devices either manually or automatically.

Manual Method

To manually push the GWN.Cloud/GWN Manager configuration to the local side of a GWN device, please navigate to **Web UI** → **Devices** page, then select a device and click on **"More"** button, next click on **"Push Configuration"**.

The screenshot shows the 'Devices' page with a table of devices. A red arrow points to the 'More' button above the table. The table has columns for Device Model, MAC, Address, and Device Group. A context menu is open over the second device, with 'Push Configuration' highlighted in red.

Device Model	MAC	Address	Device Group
GWN7624	C0:74:GWN7	2.168.5.110	device x
GWN7813P	C0:74:	2.168.5.109	device x

Devices page – Push configuration – part 1

A confirmation dialog will pop up to confirm the push configuration, to proceed click on **"OK"** button.

Note:

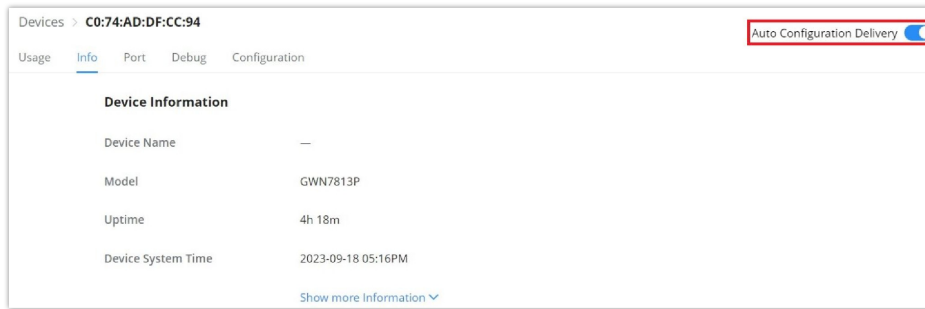
Push configuration does not work with offline GWN devices.

The screenshot shows the 'Devices' page with a confirmation dialog box overlaid. The dialog box contains the text: 'Continue to push the cloud configuration (all configurations of the device) for the selected device?' and 'You cannot push configuration to offline devices.' There are 'Cancel' and 'OK' buttons at the bottom, with a red arrow pointing to the 'OK' button.

Devices page – Push configuration – part 2

Automatic method

If the user wants to push the GWN.Cloud/GWN Manager configuration automatically for the selected GWN device, navigate to **Web UI** → **Devices** page, then click on a GWN device or configuration icon, on the top of the page toggle ON **"Auto Configuration Delivery"**, please refer to the figure below:



Auto Configuration Delivery

Export

The user can click on **"Export"** button to download a file (Excel file) that contains all the devices on this network with details. Please refer to the figures below:



Devices Export



Devices Export – Excel file

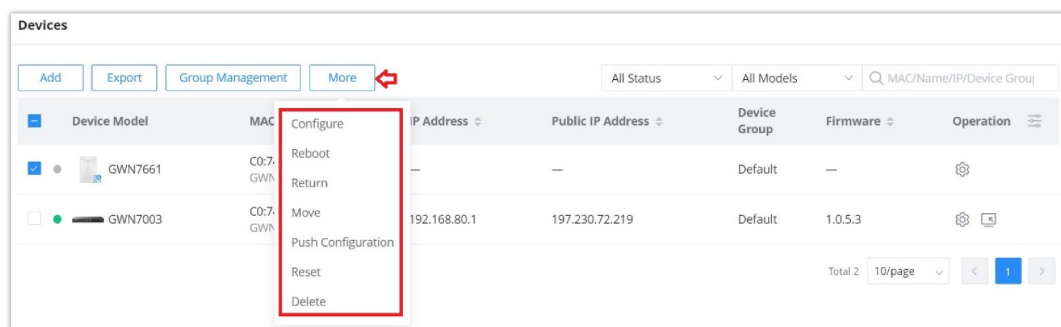
The exported file contains the following information about all the devices:

- Device Model
- MAC Address
- Name
- IP Address
- Connection IP Address
- IPv6 Address
- Device Group
- Firmware Version
- Running Time
- Clients Count
- Usage
- Channel (For GWN APs & GWN Wireless Routers)
- Tx Power

- Device Remarks
- Serial Number

More

To view more options, please click on “More” button as shown below:



Devices – More

Reboot: to reboot the GWN device.

Return: Returning a device will transfer it from its current network to the [inventory](#), where it can be reassigned.

Move: to move a device from the current network to another network.

Reset: to reset a device.

Delete: to delete a device.

Configure a device

The configuration page allows the administrator to name, reboot, configure etc. GWN devices.

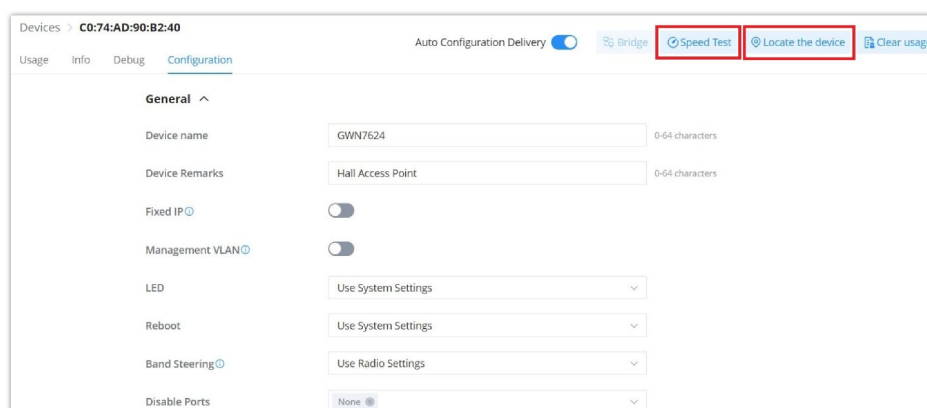
Note:

This page is dependent on the MAC device, each GWN device may require different configurations.

Navigate to **Web UI** → **Devices** page, then click on a GWN device entry or click on configuration icon.

Configure a GWN Access Point

On the Devices page, when the user click on a GWN Access point, there are many options on the top of the page dedicated only for GWN Access points:

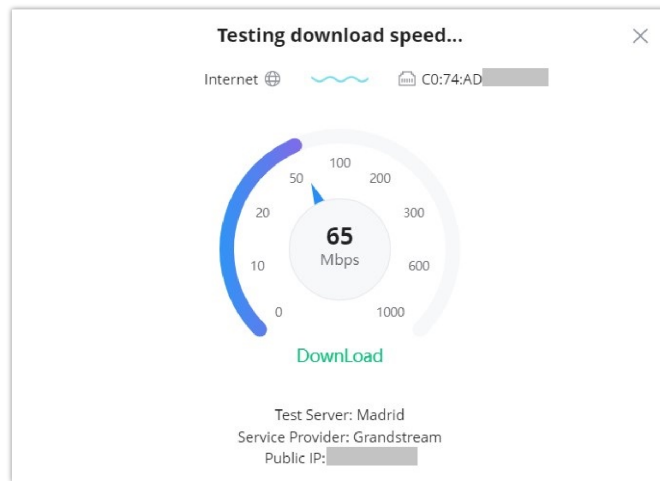


Devices – GWN AP

- **Speed Test:** is a feature on GWN APs to run a speed test directly from GWN.Cloud or GWN manager, making it easier for the administrators to check many GWN APs performance from one single interface. For more details, please refer to the figures below:

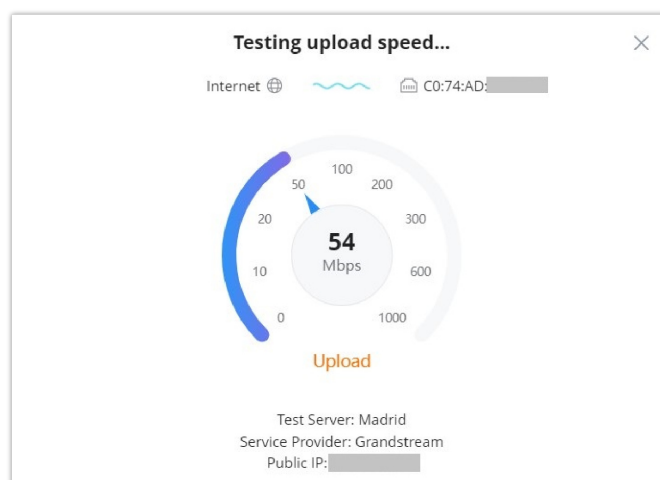
To start running the speed test, click on “**Speed Test**” button, refer to the figure above.

The first speed test is testing download speed.



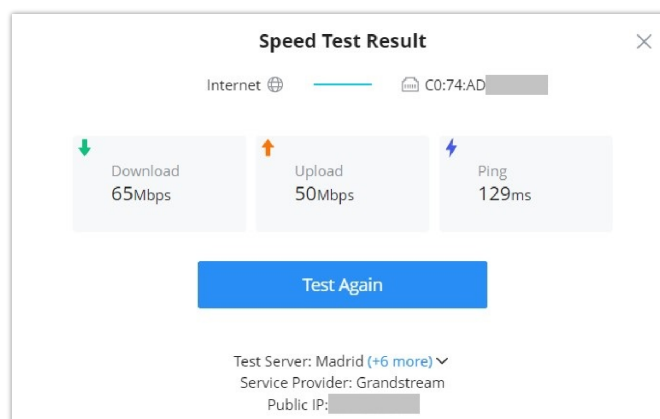
GWN APs Speed Test – Download

Once, download speed test is over, the second test is testing upload speed.



GWN APs Speed Test – Upload

Finally, the user will be able to see the final result, including Download/Upload speed and also the Ping response time in ms (Millisecond). To run the speed test again, click on "Test Again" button.



GWN APs Speed Test – Result

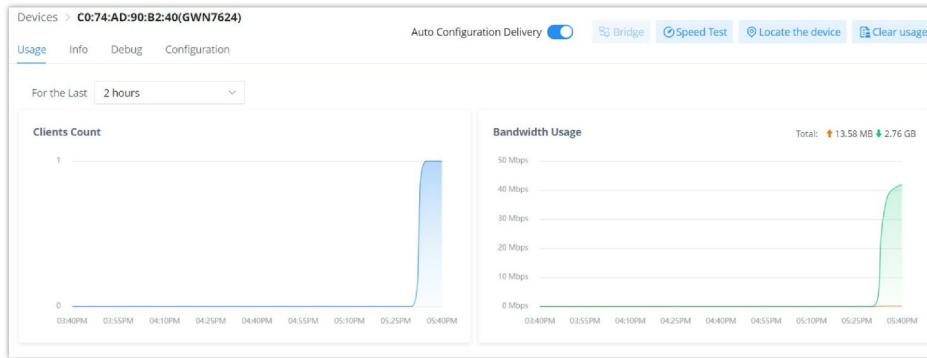
Note:

Speed Test feature is not supported on GWN7610 and GWN7602 APs.

- o **Locate the device:** easily locate the device by clicking on "Locate the device" button, a white light will be flashing for 2 minutes or click on "Close" button.
- o **GWN Access point – Usage**

This page shows the usage of the GWN AP (Bandwidth usage and Client Count) the data shown can be filtered from 2 hours up to 1 months.

Clear usage: to clear collected data from the AP (Bandwidth usage and Client Count).



GWN AP – Usage

o **GWN Access point – Info**

On this page, many info related to the GWN AP information (firmware, Uptime, etc), RF (Radio Frequency) and Current Client can be found here.

The screenshot shows the 'Info' tab for device C0:74:AD:90:B2:40 (GWN7624). It contains three main sections:

- Device Information:**
 - Device Name: GWN7624
 - Model: GWN7624
 - Link Speed: POE 1000 M/FD LAN1 Disconnected LAN2 Disconnected LAN3 Disconnected
 - Current rate: —
- RF Information:**

Radio	Channel	Wireless Power	Num of Clients	SSID	BSSID
2.4G	—	—	0	—	—
5G	—	—	0	—	—
- Current Client:**

Hostname	IP Address	Total	Channel	RSSI
Ain	192.168.5.154	1.31 GB ↑ 6.73 MB ↓ 1.3 GB	5G:44	-54

GWN AP – Info

RF Information (BSSID)

Basic Service Set Identifier (BSSID) is the MAC address of the wireless interface or precisely the radio antenna (2.4GHz or 5GHz). For example, on the GWN7624 access point we will have two BSSIDs, one for 2.4GHz antenna and another BSSID for 5GHz antenna. The two MAC addresses for both antennas will be based on the original device MAC address. In our example, GWN7624 MAC address is C0:74:AD:XX:XX:40 then 2.4GHz antenna BSSID is C0:74:AD:XX:XX:41 and for 5GHz antenna is C0:74:AD:XX:XX:42. Access points include the BSSID in their beacons and probes responses.

Navigate to **web UI** → **Devices** → **Info** then scroll down to RF Information (BSSID). Refer to the image below.

Note:

RF Information is only available for devices with wireless signal (Wi-Fi) like GWN access points or GWN wireless routers.

The screenshot shows the 'Info' tab for device C0:74:AD:XX:XX:40 (GWN7624). The 'RF Information' table is highlighted with a red border:

Radio	Channel	Wireless Power	Num of Clients	SSID	BSSID
2.4G	1	6dbm	0	Guests	c0:74:ad:XX:XX:41
5G	36	8dbm	1	Guests	c0:74:ad:XX:XX:42

BSSID

o **GWN Access point – Debug**

GWN APs have many debug tools to help diagnostic the issues:

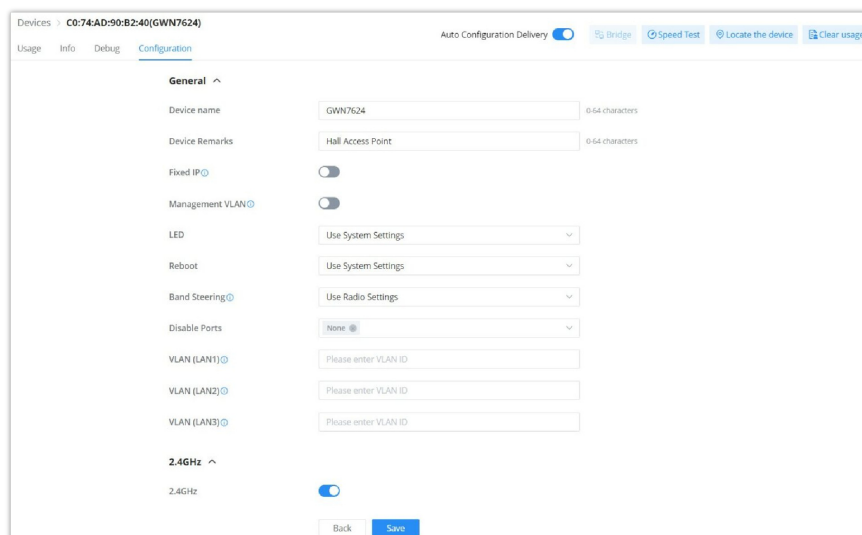
- **Ping/Traceroute:** ping and traceroute to check the reachability or the trace of an IP/Domain.
- **Capture:** to capture the traffic of GWN AP or GWN.Cloud/Manager (a file will be downloaded to your local machine).
- **Core Files:** Core Files will be listed here when generated.
- **SSH Remote Access:** to allow SSH remote access
- **Event log:** a list of events related to the GWN AP.



GWN AP – Debug

- **GWN Access point – Configuration**

On this page, the administrator can configure GWN AP related settings like (name, band steering, VLAN, RF etc). This configuration is only limited to this GWN AP.



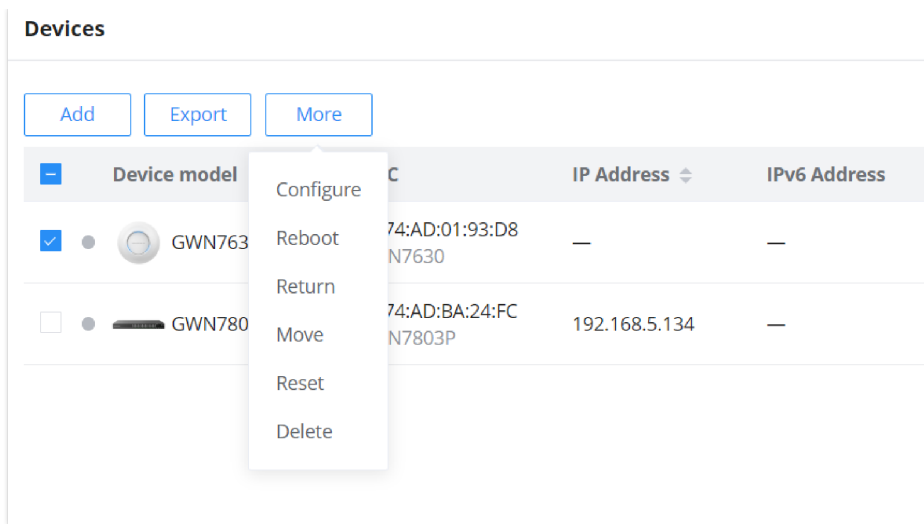
GWN AP – Configuration

Note:

To configure the Global Radio Settings, navigate to **Web UI → Settings → Wi-Fi page → Global Radio Settings page.**

Configure GWN Access Points in Batches

GWN Management platforms allow configuring GWN access points in batches, to do that please select the access points then click on "More", then click "Configure" as shown in the figure below.



Batch Configuration of GWN Access Points

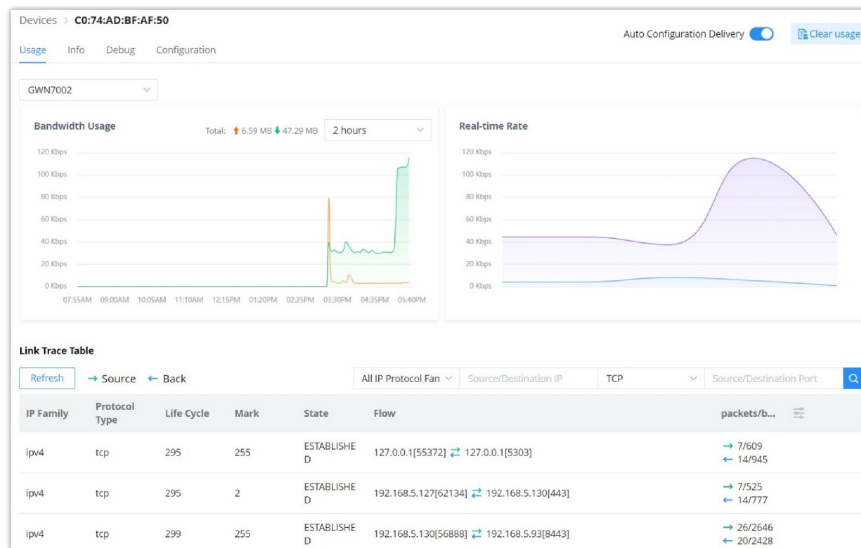
Note:

Batch configuration of GWN Access Points is for same model only.

Configure a GWN Router

o GWN Router – Usage

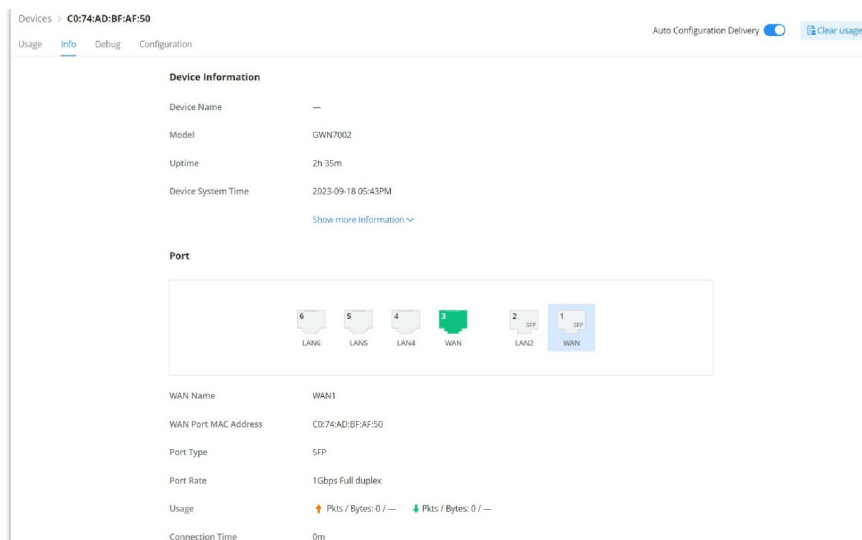
Same as the GWN AP usage tab, also on this page, the user can find usage related to the GWN Router, like bandwidth usage, Real-time Rate and even Link Trace Table for detailed traffic data. Please refer to the figure below:



GWN Router – Usage

o GWN Router – Info

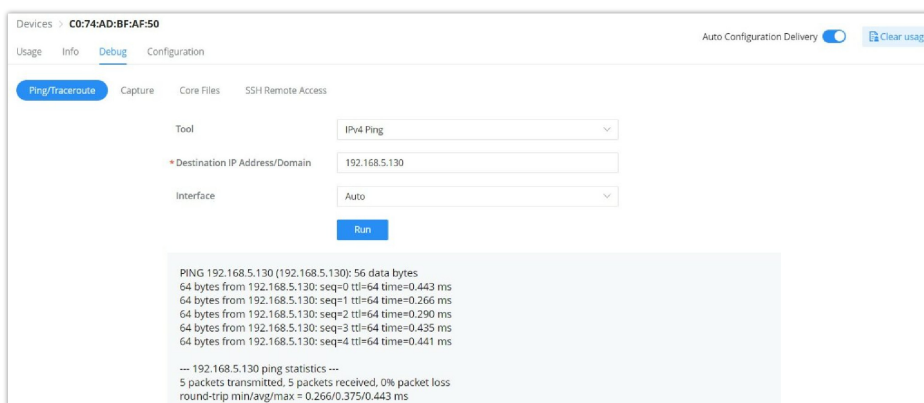
All the information related to GWN router can be found here, including Device information (name, firmware etc), GWN router ports status (active ports) and information about IPv4 and IPv6 (IP address, DNS etc).



GWN Router – Info

o **GWN Router – Debug**

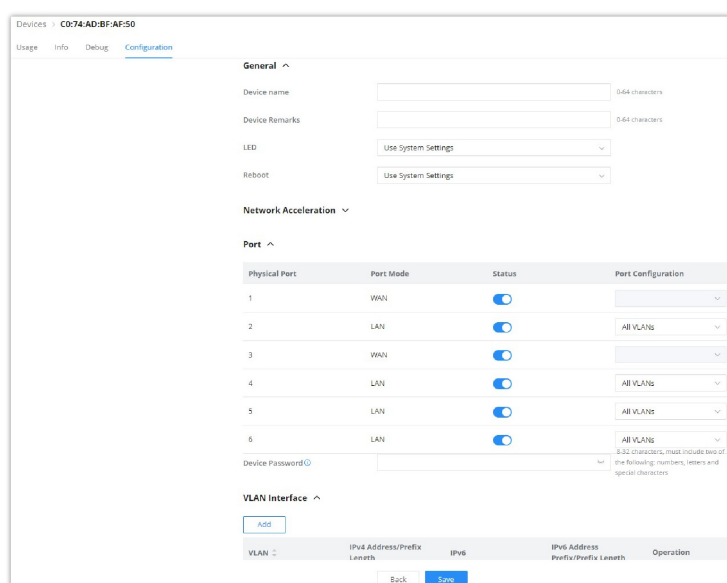
The same debug tools found on GWN APs can be found here, please check [GWN Access Points](#).



GWN Router – Debug

o **GWN Router – Configuration**

On GWN router configuration tab, the user can configure GWN router like device name, Network Acceleration, enable/disable physical ports (WAN/LAN) and add/edit VLAN interfaces. Please refer to the figure below:



GWN Router – Configuration

Note:

To configure the Global Radio Settings for wireless routers, navigate to **Web UI → Settings → Wi-Fi page → Global Radio Settings page**.

VLAN Interface (interface for GWN routers)

VLAN Interface as the name suggests turn a VLAN into a virtual interface that can be routed using layer 3 routing by giving this interface an IP address. To add a VLAN interface for GWN routers, please click on "**Add**" button or configure a previously created one by clicking on the "**configure icon**" under operation, refer to the figure below:



GWN Router configuration – VLAN Interface

Then, select the VLAN from the list or visit [LAN](#) page to create a VLAN (with or without DHCP Server) first in case there are no VLANs listed, then specify an IPv4 or IPv6 Address/Prefix for this VLAN interface.



GWN router – Add/Edit VLAN Interface

Note:

Before configuring the IP address, configure the default route for the device in the static route to prevent the VSwitch from losing the default route and unable to connect to the cloud.

Configure a GWN Switch

- o **GWN Switch – Usage**

As for GWN Switches usage tab, traffic statistics or PoE Ports power usage can be found here. The user can click on “**Clear Traffic**” button to clear all the traffic or click on “**clear**” icon under operation to clear traffic only for a specific port.



GWN Switch – Usage

- o **GWN Switch – Info**

Relevant GWN switch information or PoE power supply information can be found here.



GWN Switch – Info

- o **GWN Switch – Port**

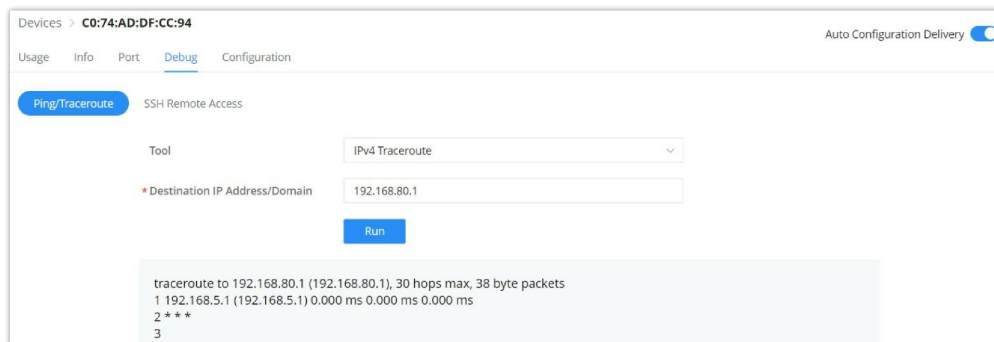
On the Port tab, under devices configuration only for GWN switches, the user can view GWN switch ports status and also configure them (enable/disable a port, Link Aggregation, Port Mirroring etc). Please refer to the figure below:



GWN Switch – Port

- o **GWN Switch – Debug**

Debugging tools like ping/traceroute are also available for GWN switches, as well as SSH Remote Access.

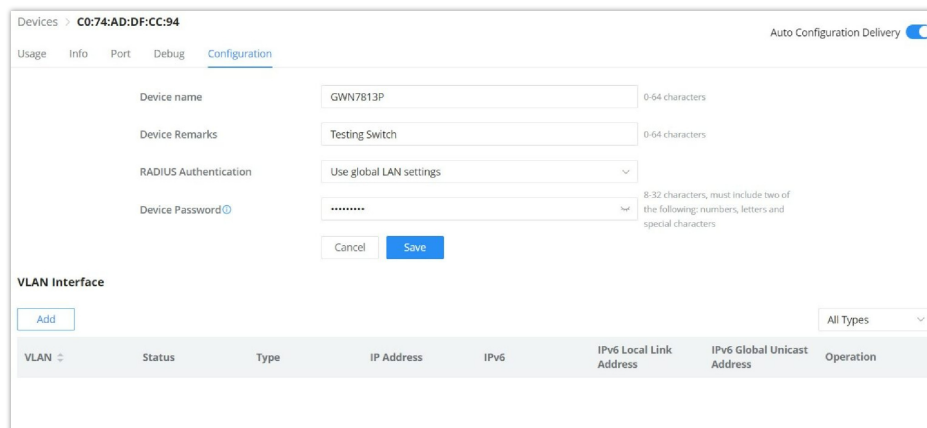


GWN Switch – Debug

- o **GWN Switch – Configuration**

On this tab, under devices (only for GWN switches), the user can configure GWN switch related configuration like switch name, RADIUS Authentication and VLAN interfaces.

Device Password: Set the devices SSH remote login password other than APs, which is also the device web login password.



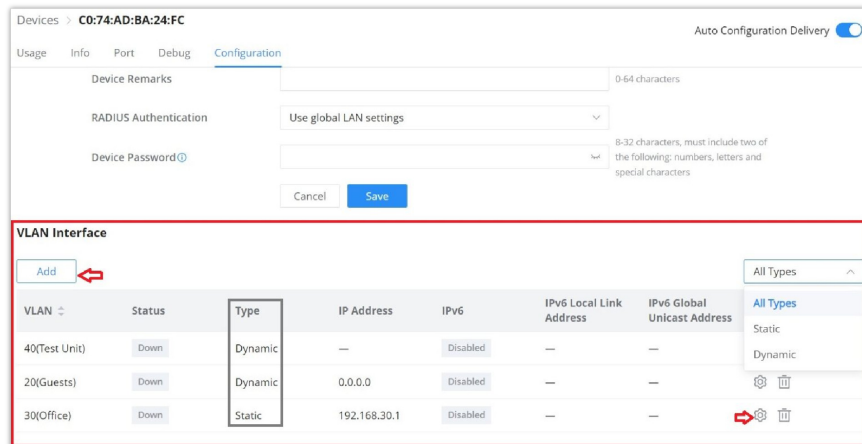
GWN Switch – Configuration

VLAN Interface (interface for GWN switches)

Hosts in different VLANs cannot communicate directly and need to be forwarded through routers or layer 3 switching protocols.

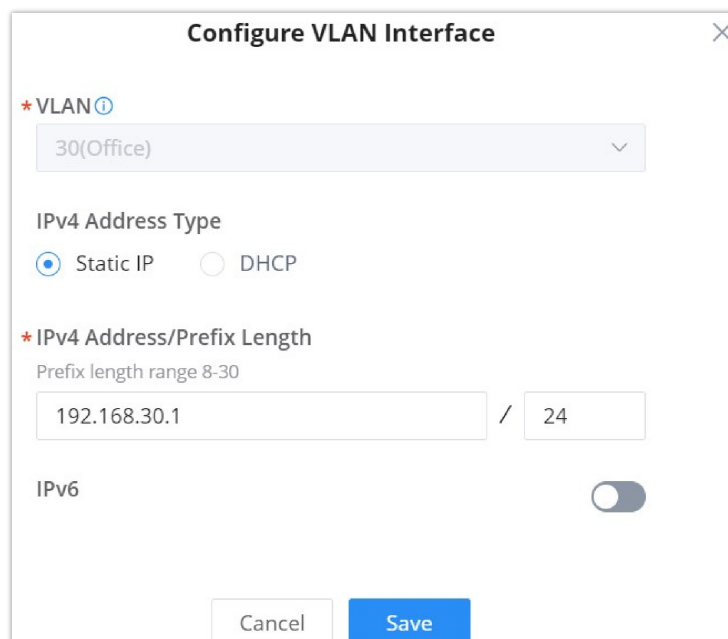
A VLAN interface is a virtual interface in Layer 3 mode and is mainly used to implement Layer 3 communication between VLANs, it does not exist on the device as a physical entity. Each VLAN corresponds to an interface by configuring an IP address for it, it can be used as the gateway address of each port in the VLAN so that packets between different VLANs can be forwarded to each other on Layer 3 routing through the VLAN interfaces. GWN switches support IPv4 interfaces as well as IPv6.

To add a VLAN Interface for GWN switches, click on **“Add”** button or click on **“Configure icon”** to edit previously added one. Refer to the figure below:



GWN Switch configuration – VLAN Interface

- **If DHCP is selected:** hosts will obtain IP addresses automatically from whatever DHCP pool configured from example like a router.
- **If Static IP is selected:** for hosts to obtain IP addresses, the user must configure a VLAN with DHCP Server, create or edit VLAN first [Lan](#).



GWN Switch – Add/Edit VLAN Interface

CLIENTS

From The client’s page, the administrator can monitor and manage all the clients connected to the network/GWN devices. A list of all connected clients with their related info like connection type, IP Address, Total bandwidth, Associated Devices (GWN AP, Router or switch) etc. will be also displayed, for more info about the client or related configuration please click on the client or click on the configuration icon. Please refer to the figure below:

Clients

Export Now Online All Clients Q

Hostname	Connection	SSID	VLAN ID	IP Address	Total	RSSI	Associated Devices	Station Mode	Conne Time
Ain	Wireless	GWN76...	1	192.168.5.154	690.59 KB	-55	GWN7624 C0:74:AD:...	11AC_VH...	1h28m
	Wired	---	1	192.168.0.1	---	---	C0:74:AD:...	---	0m
	Wired	---	1	---	---	---	C0:74:AD:...	---	0m
	Wired	---	1	---	---	---	C0:74:AD:...	---	0m
	Wired	---	1	---	---	---	C0:74:AD:...	---	0m
	Wired	---	1	---	---	---	C0:74:AD:...	---	0m
	Wired	---	1	192.168.5.113	---	---	C0:74:AD:...	---	0m
	Wired	---	1	192.168.5.85	---	---	C0:74:AD:...	---	0m

- Hostname
- Connection
- SSID
- VLAN ID
- IP Address
- IPv6 Address
- Wi-Fi Band
- Total
- Upload
- Download
- RSSI
- Link Rate
- Associated Devices
- Station Mode
- Guest
- Connection Time
- OS
- Manufacturer
- First Seen
- Last Seen

Clients page

Configure a client

Per client configuration is available to assign a name or block (only wireless clients) access to the network, also specifying bandwidth rules or enabling DHCP Static address binding.

Clients > (Ain) Clear

Usage Info Configuration

Hostname: 0-64 characters

Block: Once enabled, wireless clients cannot connect to the current network

Bandwidth Rules:

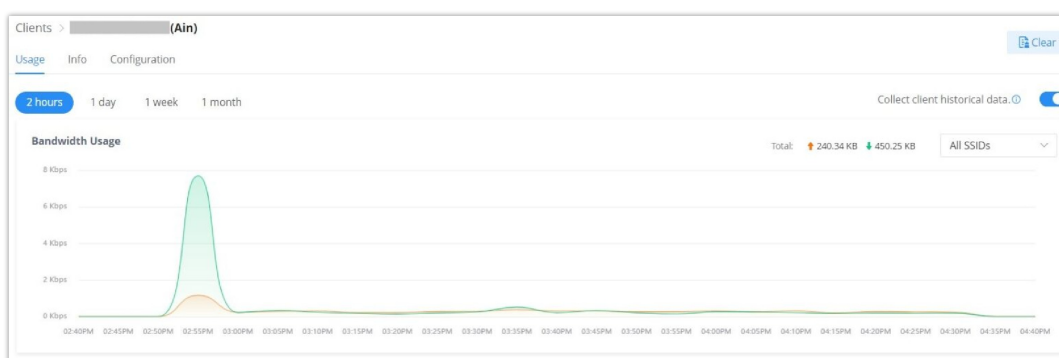
DHCP Static IP address binding: This client can be bound only to the current network

Client – Configuration

Client usage

To get more info about the client usage please navigate to **Web UI** → **Clients** → **Usage**, Bandwidth usage per SSID or All SSIDs can be displayed here with the option to specify the duration 2 hours, 1 day, 1 week or 1 month.

Click on Clear to clear the data.

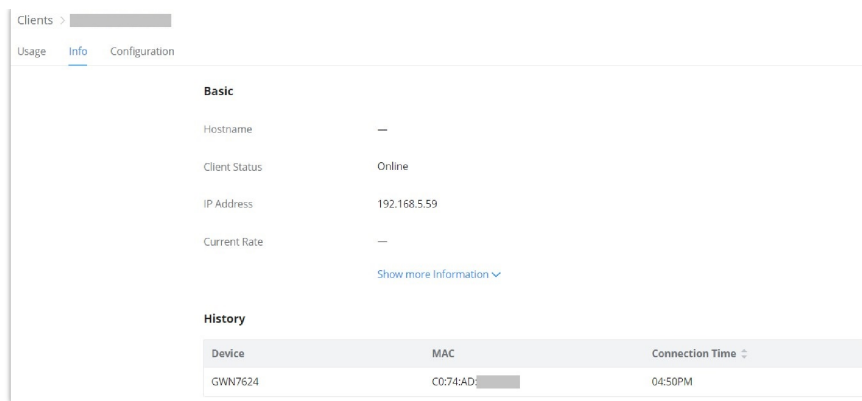


Client Usage

Client info

In this page, info about the current client will be displayed showing the client Hostname, Client Status, IP Address, Current rate etc.

Click on **“Show more information”** to get more info about the client.



Client Info

GUESTS

Online status

This page displays information about the clients connected via Captive portal including the MAC address, Hostname, Authentication Type, the device they are connected to, Certification state, SSID as well as the RSSI and Data usage.

Administrator can also export a .csv file containing all the guest information (Client MAC address; Authentication Form when choosing Custom Field, Last Visit...etc.) by clicking on "Export" button, and selecting the export time period for all users which connected to the captive portal during that period.



Guests – Online status

Voucher

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

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

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

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

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

Click on  button to add a new voucher.



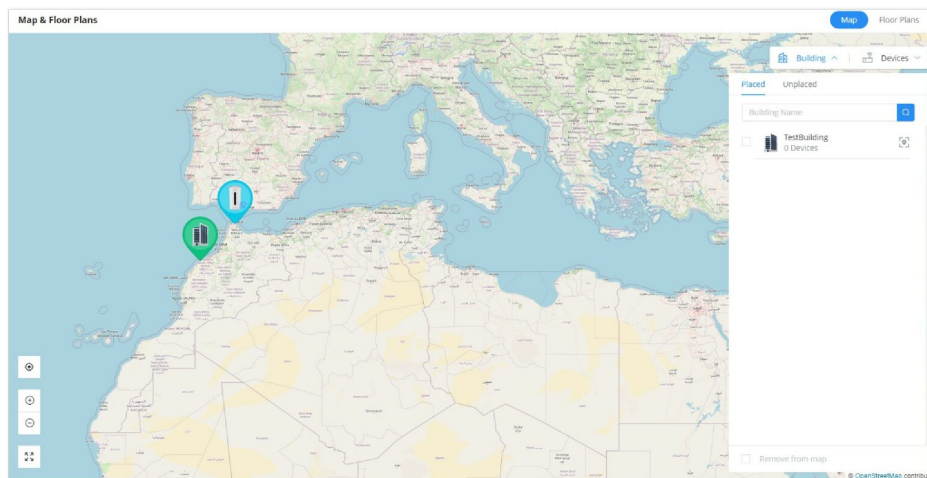
Voucher page

MAP & FLOOR PLANS

Map

With the Map feature, the administrators can link GWN devices or buildings to certain places on the Map, either manually on the Map or automatically using the device IP address, which will help to geolocate GWN devices or to link them to a different location (ex: company branch).

To place GWN Devices/Building on the Map, please navigate to **Web UI** → **Map & Floor Plans** (under Map tab). Please refer to the figure below:

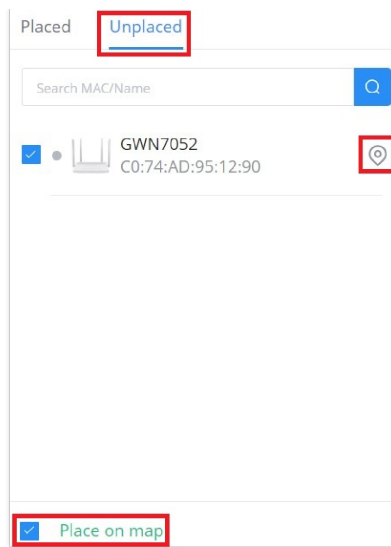


Map

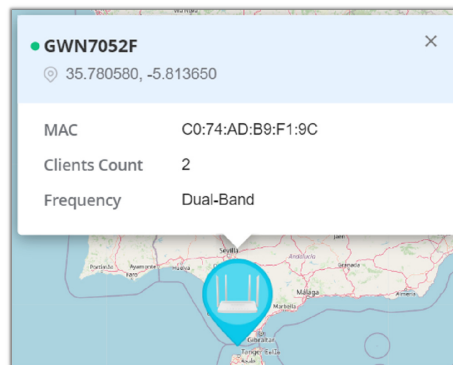
Note:

Map feature on GWN.Cloud/GWN Manager supports both OpenStreetMap and Google Maps.

Select "**Building**" or "**Devices**" and under "**Unplaced**" select the device/building then click on "**Map**" icon to manually place the GWN device on the map, or click on "**Place on map**" to be placed based on the IP address.

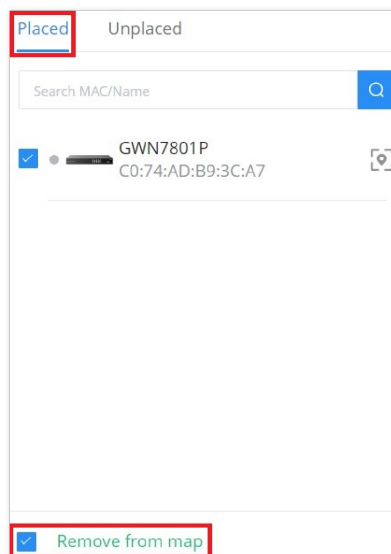


Unplaced devices



Placed GWN device

To remove the GWN device/building from the Map, please select the device/building then click on **"Remove from map"**.



Placed devices

Note:

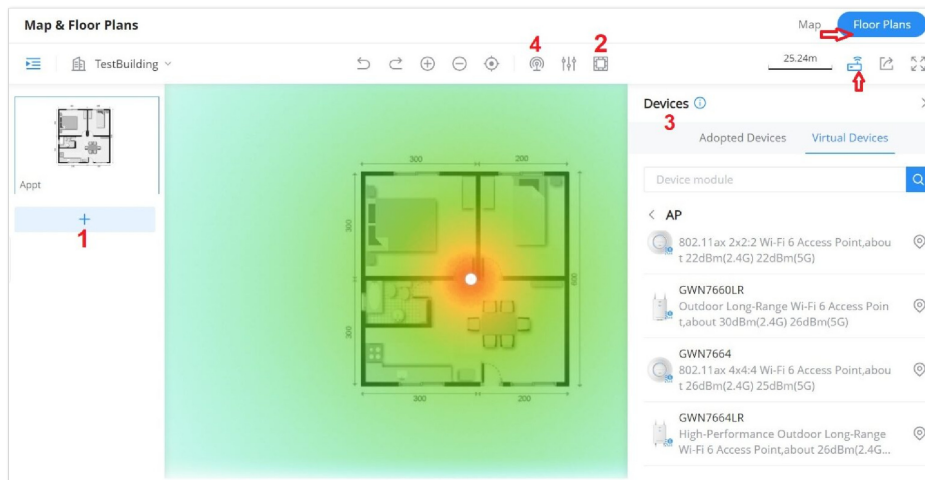
GWN management supports Open Street and Google Maps.

Floor Plans

Floor Plans feature is a very convenient way to deploy devices in the right places within the building this way the wireless signal will be able to cover all the area, a RF heat map preview helps the user to easily predict the best place to deploy a GWN device, and this can be even done using a virtual GWN device like GWN access points or GWN wireless routers. In the case of

a large deployment of GWN APs in a building with many walls, Glass, etc. and a large surface area, this feature helps the deployment team to accurately and easily pinpoint the appropriate spots to deploy GWN APs for Wi-Fi signal to cover all the building areas and satisfy the users wireless experience.

Please navigate to **Web UI** → **Map & Floor Plans** (under Floor Plans tab). Please refer to the figure below:

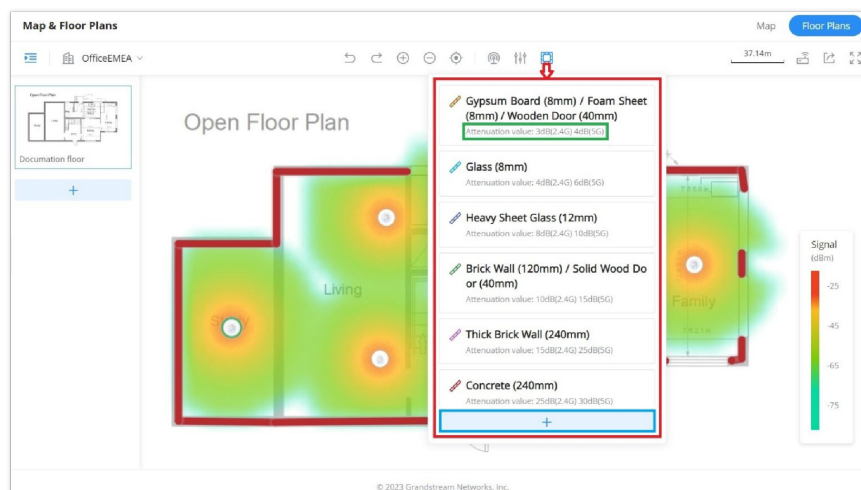


Floor Plans

1. First, Upload the Floor Plan image by clicking on “+” icon on the left side of the page.
2. Then, optionally you can add walls and dividers on the floor plan or click on “+” button to add a custom wall or divider with 2.4G and 5G attenuation values (dB).

The walls and dividers available are:

- o **Gypsum Board (8mm) / Foam Sheet (8mm) / Wooden Door (40mm)**
Attenuation value: 3dB(2.4G) 4dB(5G)
- o **Glass (8mm); Attenuation value:** 4dB(2.4G) 6dB(5G)
- o **Heavy Sheet Glass (12mm); Attenuation value:** 8dB(2.4G) 10dB(5G)
- o **Brick Wall (120mm) / Solid Wood Door (40mm); Attenuation value:** 10dB(2.4G) 15dB(5G)
- o **Thick Brick Wall (240mm); Attenuation value:** 15dB(2.4G) 25dB(5G)
- o **Concrete (240mm); Attenuation value:** 25dB(2.4G) 30dB(5G)



Floor Plans – Wall Types

Click on “+” button as shown above to add a custom wall or a divider.



Floor Plans – Custom wall or divider

1. Under devices, please select the GWN device either from adopted ones or virtual ones then place on the floor building accordingly.
2. Finally, click on the **Heat Map** icon and select either 2.4G or 5G wireless signal to be able to see the full range of the wireless signal. Also, it's possible to show only signal greater than the specified dBm, this way the user can hide the weak signal from the heat map.



Floor Plans – Heat map

INSIGHTS

Site Survey

An integrated Wi-Fi Scanner is supported on GWN Management Platforms helps the administrator to scan the wireless networks in the area and to display extensive information including: SSID's name, AP's MAC address, Channel used, Wi-Fi Standard, Bandwidth, security standard used, Manufacturer, RSSI, ... and more.

SSID	BSSID	Channel	Protocol	Bandwidth	Encryption	Manufacturer	Num of APs	Scanned by	RSSI	Last Seen
WiFi1	9C:C9:EB:80:00:00	5G	802.11ac	80	WPA2	NETGEAR	1	C0:74:AD:90:B...	-92	2022-12-15 11...
WiFi2	40:33:06:80:00:00	5G	802.11ac	80	WPA2	NETGEAR	1	C0:74:AD:90:B...	-88	2022-12-15 11...
WiFi3	B8:50:01:80:00:00	5G	802.11ac	40+	WPA2	NETGEAR	1	C0:74:AD:90:B...	-95	2022-12-15 11...
WiFi4	C0:74:AD:90:B...	5G	802.11ac	80	WPA2	NETGEAR	1	C0:74:AD:90:B...	-91	2022-12-15 11...
WiFi5	84:3D:C6:80:00:00	5G	802.11n/a	20	WPA2	NETGEAR	1	C0:74:AD:90:B...	-88	2022-12-15 11...
WiFi6	FC:40:09:80:00:00	5G	802.11ac	80	WPA2	NETGEAR	1	C0:74:AD:90:B...	-90	2022-12-15 11...
WiFi7	B8:50:01:80:00:00	5G	802.11ac	40+	WPA2	NETGEAR	1	C0:74:AD:90:B...	-95	2022-12-15 11...
WiFi8	B8:50:01:80:00:00	5G	802.11ac	40+	Open	NETGEAR	1	C0:74:AD:90:B...	-92	2022-12-15 11...
WiFi9	C6:74:AD:90:B...	5G	802.11ac	80	Open	NETGEAR	1	C0:74:AD:90:B...	-91	2022-12-15 11...
WiFi10	84:3D:C6:80:00:00	5G	802.11n/a	20	Open	NETGEAR	1	C0:74:AD:90:B...	-88	2022-12-15 11...

Site Survey

Users can press “Detect” button to run the Wi-Fi scanner or press “Refresh” button to refresh the results page.


Network Topology

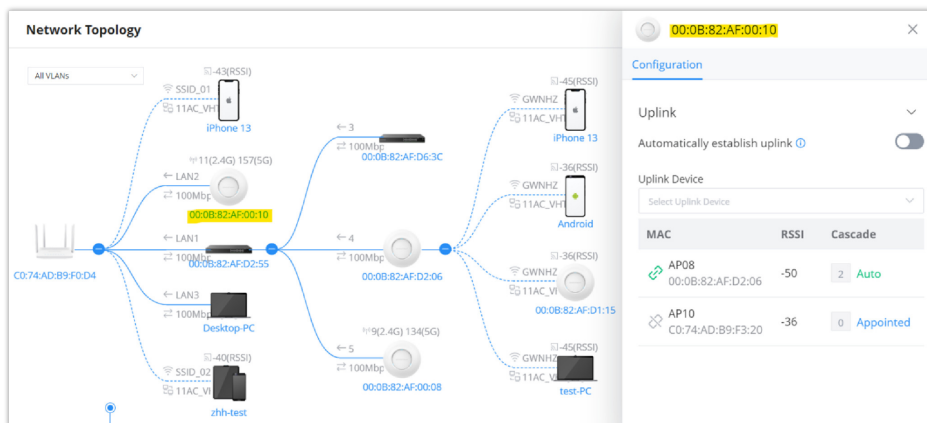
Network Topology shows an overview of the whole network starting from the GWN Router (Internet access) including GWN Switches and Access Points as well as Clients, this way the administrator/monitor can have very quickly an overview about the network in a glance. By clicking on a GWN device or a Client more information can be displayed.

Features overview:

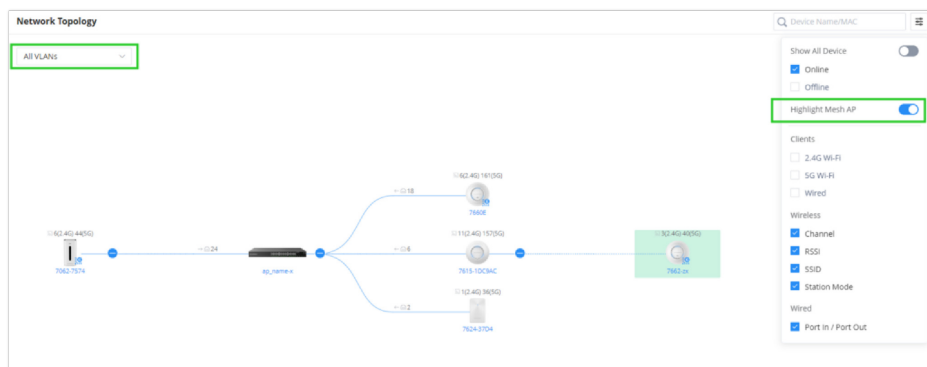
- Display network layout
- Visualize gateway, switch, access point, and connected client device information
- The topology map can be zoomed in, out, and nodes are retractable
- Support Mesh AP and also the option to Highlight Mesh AP
- VLAN information filtering

Notes:

- Click on  to collapse that part of the network.
- Dashed lines means wireless connection while solid lines means wired connection.



Network Topology

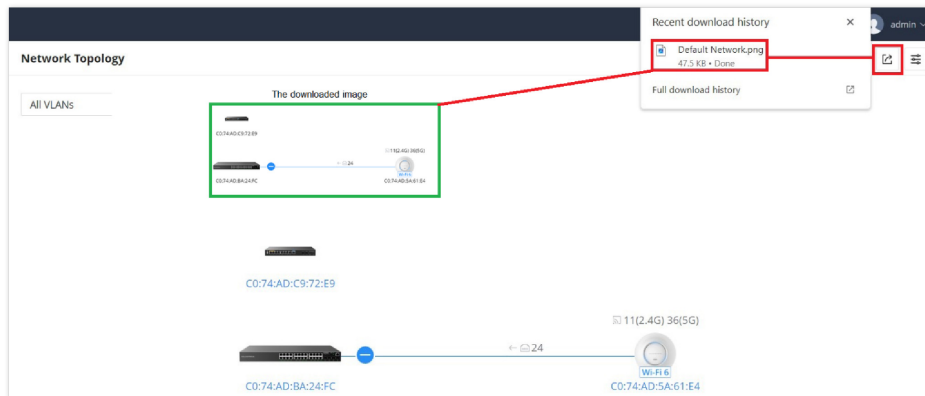


Network Topology – Highlight mesh

To backup the current topology or share it, on the top right corner of the page, click on **"Export"** button, a PNG image will be downloaded.

Note:

For the best result adjust the network topology to the best viewable size before exporting.



Network Topology – Export

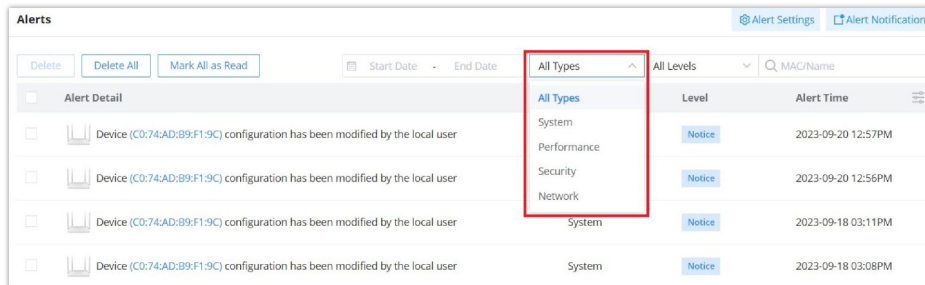
ALERTS

Alerts page displays alerts about the network, the user can specify to display only certain types like (**System, Performance, Security or Network**) or the levels. To check the alerts which have been generated, please navigate to **Web UI → Alerts** page.

The alerts can be displayed either by type or levels. However, that is not the only way to display them. The user can filter through the alert log using a date interval or search by MAC address or device name.

- o **Alert Types**

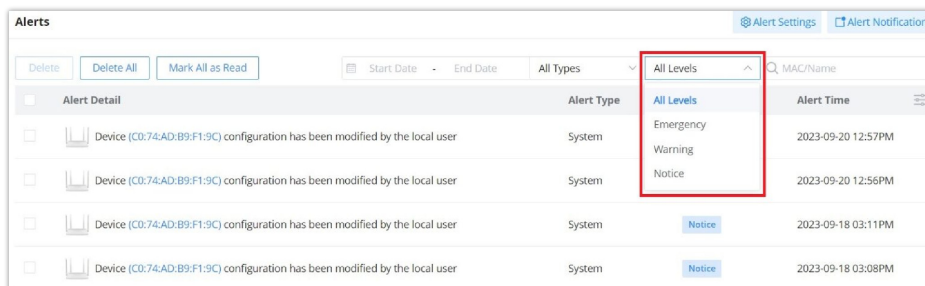
The available types are **System, Performance, Security, Network**, or the user can choose to display all the types.



Alerts Types

- o **Alert Levels**

The user can filter the alert level by the following levels: **All Levels, Emergency, Warning or Notice**.



Alerts Levels

Alert Settings

In this page the user can select the alerts to be displayed, four categories or alerts are available (**system, performance, security and network**) and each category has even more options. Please check the figures below:

- **System Alert** includes: GWN.Cloud/GWN Manager, GWN Routers, GWN Switches and GWN Access points.
- **Performance Alert** includes: GWN.Cloud/GWN Manager, GWN Routers, GWN Switches and GWN Access points.
- **Security Alert:** GWN Access points (Rogue AP).
- **Network Alert** includes: GWN Routers, GWN Switches, GWN Access points and Client.

The screenshot shows the 'Alert Settings' page with the 'System Alert' tab selected. The 'System Alert' tab is highlighted with a red box. The page is divided into four sections: System Alert, Router, Switch, and AP. Each section contains a list of alerts with checkboxes and icons. The 'System Alert' section includes:

- Device configuration sync failed
- The current device has a time deviation of 30 minutes. Below this is a button: 'Turn on [Auto Sync Time] to avoid time deviation'.

 The 'Router' section includes:

- Router upgraded successfully
- Router upgrade failed
- Router temperature is too high

 The 'Switch' section includes:

- Switch temperature is too high
- Failure detected: Select (dropdown menu)
- The signal of the switch optical module is lost
- Abnormal temperature detected on the switch optical module
- Switch backup failed
- Switch upgraded successfully
- Switch upgrade failed

 The 'AP' section includes:

- AP upgraded successfully
- AP upgrade failed
- AP temperature is too high

 At the bottom right, there are 'Cancel' and 'Save' buttons.

Alert Settings – part 1

The screenshot shows the 'Alert Settings' page with the 'Performance Alert' tab selected. The 'Performance Alert' tab is highlighted with a red box. The page is divided into three sections: Router, Switch, and AP. Each section contains a list of alerts with checkboxes and icons, and some have input fields for thresholds. The 'Router' section includes:

- CPU Usage exceeded 90 %
- Memory Usage exceeded 90 %
- 2.4GHz Channel Usage exceeded 60 %
- 5GHz Channel Usage exceeded 60 %
- 2.4GHz Clients exceeded 20
- 5GHz Clients exceeded 20
- WAN port throughput exceeded 50 Mbps
- WAN port uplink Bandwidth exceeded 50 Mbps
- WAN port downlink Bandwidth exceeded 50 Mbps

 The 'Switch' section includes:

- CPU Usage exceeded 90 %
- Memory Usage exceeded 90 %
- Switch Port Packet Loss Rate exceeded 10 %

 The 'AP' section includes:

- CPU Usage exceeded 90 %
- Memory Usage exceeded 90 %
- 2.4GHz Channel Usage exceeded 60 %
- 5GHz Channel Usage exceeded 60 %

 At the bottom right, there are 'Cancel' and 'Save' buttons.

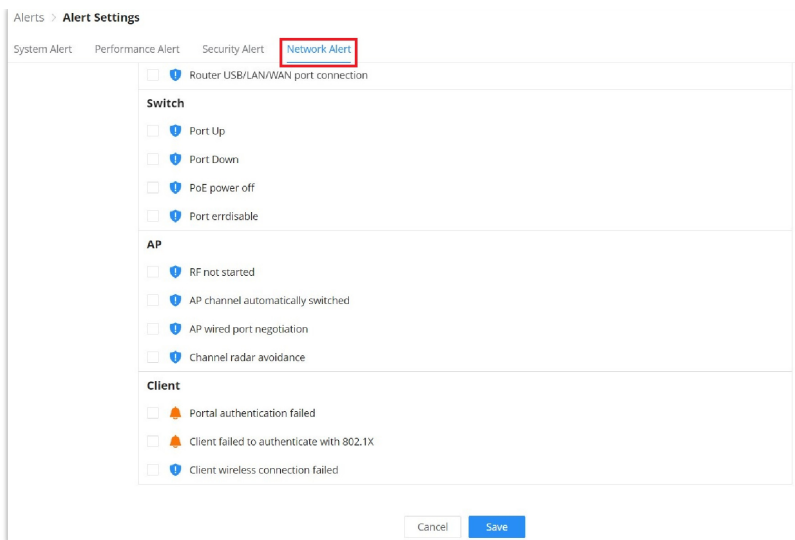
Alert Settings – part 2

The screenshot shows the 'Alert Settings' page with the 'Security Alert' tab selected. The 'Security Alert' tab is highlighted with a red box. The page is divided into one section: AP. It contains a list of alerts with checkboxes and icons. The 'AP' section includes:

- Device detected a rogue AP of Untrusted AP Spoofing SSID (dropdown menu)

 At the bottom right, there are 'Cancel' and 'Save' buttons.

Alert Settings – part 3



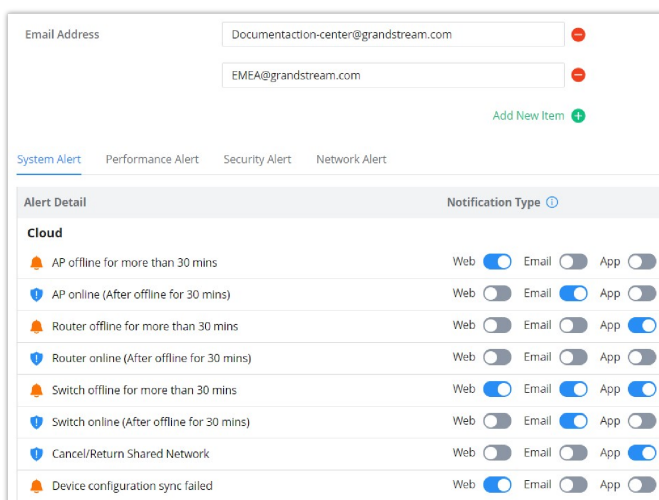
Alert Settings – part 4

Alert Notification

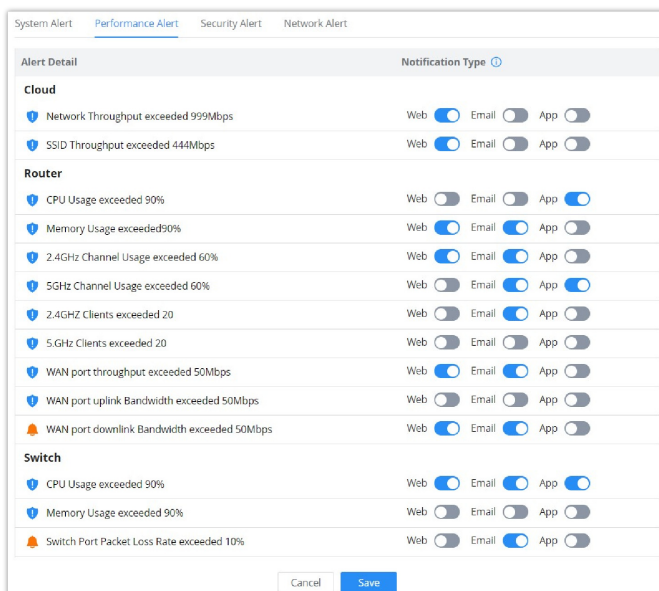
In this page, Emails addresses can be specified to receive notifications for the selected alerts, the notifications can be sent to the configured emails, web or App.

Note:

Each account can independently set alerts they want to receive and the email address to receive them.



System Alert Notifications



Performance Alert Notifications

Each account can independently set alerts they want to receive and the email address to receive them.

Email Address

Documentaction-center@grandstream.com

EMEA@grandstream.com

Add@more.com

[Add New Item](#)

System Alert Performance Alert **Security Alert** Network Alert

Alert Detail Notification Type

AP

Device detected a rogue AP of illegal access without authentication,illegal access,Spoofing SSID,Untrusted AP

Web Email App

Security Alert Notifications

System Alert Performance Alert Security Alert **Network Alert**

Alert Detail Notification Type

Router

Network failed Web Email App

PPPoE connection failed Web Email App

RF not started Web Email App

WAN is down Web Email App

Channel radar avoidance Web Email App

RADIUS server failed Web Email App

Router USB/LAN/WAN port connection Web Email App

Switch

Port Up Web Email App

Port Down Web Email App

PoE power off Web Email App

Port errdisable Web Email App

AP

RF not started Web Email App

AP channel automatically switched Web Email App

AP wired port negotiation Web Email App

Network Alert Notifications

SETTINGS

Wi-Fi

All the related settings about Wi-Fi can be found in this page, split into 2 sections Wireless LAN, Global Radio Settings and Mesh.

Wireless LAN

Under Wireless LAN section, SSIDs will displayed with Wi-Fi Status and Online Devices etc. for configuration click on the SSID or configuration icon.

the user can also click on button to add new SSID, the configuration can be only specific for this SSID, to configure radios for all SSIDs please click on section two **"Global Radio Settings"**.

Wi-Fi

Wireless LAN

Name	Wi-Fi Status	VLAN ID	Online Devices	Security Type	Portal	Operation
EMEA	Enabled	—	4	Personal	Disabled	
Staff	Enabled	—	1	Personal	Disabled	

Global Radio Settings

Mesh

Enable Mesh The AP only support 5 SSIDs under the same VLAN if enabled.

* Scan Interval 1-5 numbers

* Wireless Cascade 1-3 numbers

Wi-Fi page

Add a SSID

To add new SSID, navigate to **Web UI** → **Settings** → **Wi-Fi page** → **Wireless LAN section** then click "Add" button. A new page will popup, enter different settings to add new SSID.



Add wireless LAN

Basic	
WiFi	Check to enable Wi-Fi for the SSID
SSID	Set or modify the SSID name.
Client IP Assignment	Select between Bridge or NAT

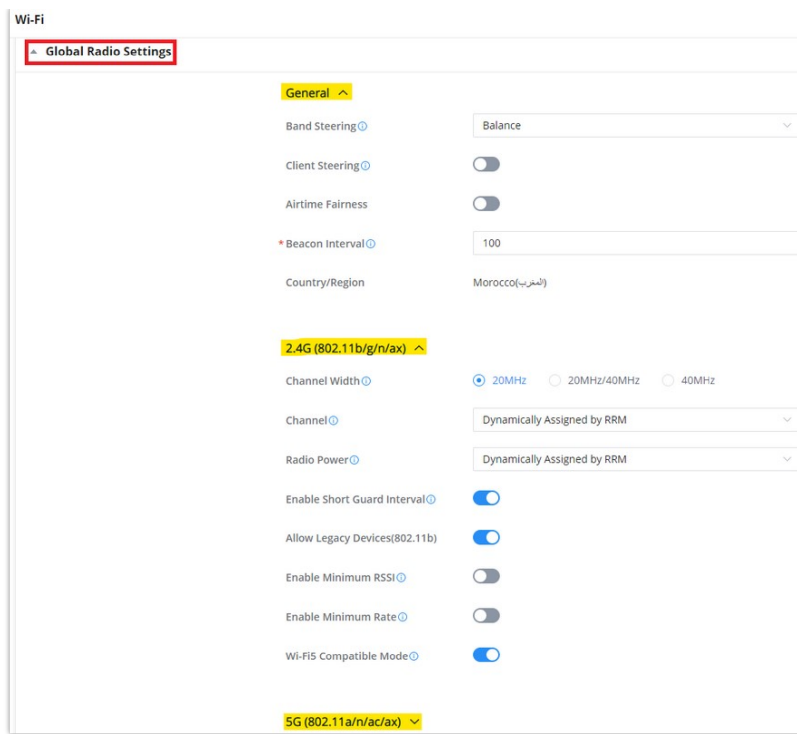
Associated VLAN	Check to Enable VLAN and enter VLAN ID, otherwise, this SSID will be using the default network group.
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: Dual-Band, 2.4GHz or 5GHz
Access Security	
Security Type	Set the security type, 5 options are available: <ul style="list-style-type: none"> ● Open : no security is required ● Personal: Select the WPA Pre-Shared Key and the WPA Mode ● Enterprise: Select Radius Authentication and WPA Mode. ● PPSK: Select the PPSK Group. ● Hotspot2.0 OSEN: Select the RADIUS Authentication
802.11w	Disabled: disable 802.11w; Optional: either 802.11w supported or unsupported clients can access the network; Required: only the clients that support 802.11w can access the network.
Access Control	
MAC Filter	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to Wi-Fi. Default is Disabled.
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76xx's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Available modes are: <ul style="list-style-type: none"> ● Radio Mode: Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76xx but they cannot communicate with each other. ● Internet Mode: Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76xx. ● Gateway MAC Mode: Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76xx access points.
Client Time Policy	Configures the client time policy. Default is None.
Bandwidth Control	Select Bandwidth Control (Per-SSID or Per-Client), then select from the Bandwidth rules previously created.
Schedule	Select a schedule that will be applied to this SSID, schedules can be managed from the menu " Settings → Profiles → Schedule ".
Device Assignment	
Select from the Devices list the ones to be part of this SSID. <i>Note: If an AP or router that uses the Wi-Fi network is selected, new APs will be automatically added to the network.</i>	
Advanced	
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
DTIM Period	Configures the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Default value is 1, meaning that AP will have DTIM broadcast every beacon. If set to 10, AP will have

	DTIM broadcast every 10 beacons. Valid range: 1 – 10.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a network group, each SSID will have the same limit. So, setting a limit of 50 will limit each SSID to 50 users independently. 0 means limit is disabled.
Client Inactivity Timeout	AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.
Multicast/Broadcast Suppression	Disable: all of the broadcast and multicast packages will be forwarded to the wireless interface. Enable: all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND; Enable with Proxy ARP enabled: enable the optimization with Proxy ARP enabled in the meantime.
Convert IP multicast to unicast	Once selected, AP will convert multicast streams into unicast streams over the wireless link. Which helps to enhance the quality and reliability of video/audio stream and preserve the bandwidth available to the non-video/audio clients.
Enable Voice Enterprise	Enable this feature to help clients connected to the GWN76xx to perform better roaming decision. <ul style="list-style-type: none"> • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. <p><i>Note: 11R is required for enterprise audio feature, 11V and 11K are optional.</i> Enable Voice Enterprise is only available under "WPA/WPA2" and "WPA2" Security Mode.</p>
Enable 802.11r	Check to enable 802.11r
Enable 802.11k	Check to enable 802.11k
Enable 802.11v	Check to enable 802.11v
ARP Proxy	Once enabled, AP will avoid transferring the ARP messages to Stations, while initiatively answer the ARP requests in the LAN.
Enable Bonjour Gateway	Click to enable Bonjour Gateway <i>Note: If enabled, client Bonjour requests on SSID can be forwarded to the VLAN of Bonjour services (such as Samba).</i>
Enable U-APSD	Configures whether to enable U-APSD (Unscheduled Automatic Power Save Delivery)

Add Wireless LAN

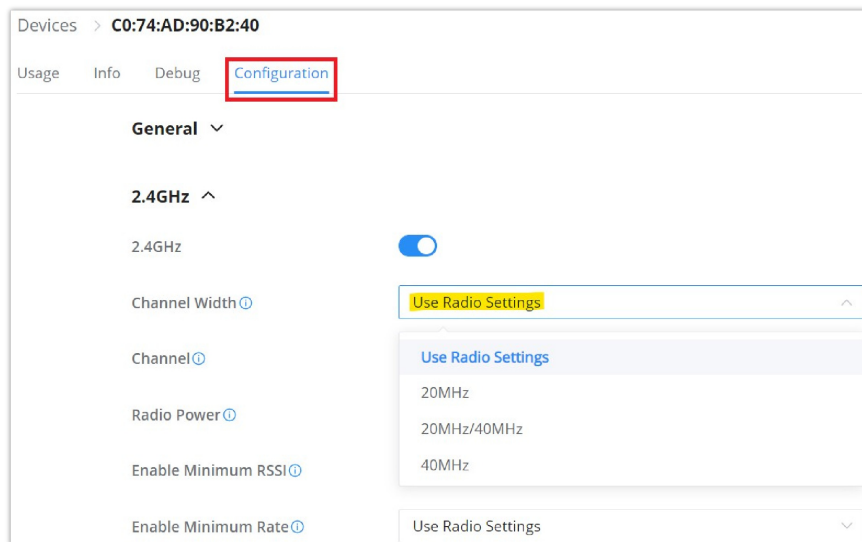
Global Radio Settings

In this page the Administrator can configure the global radio settings which will affect all the GWN devices with wireless signal, it's a convenient way to configure all the devices wireless signal at once.



Global Radio Settings

To configure a specific device (GWN AP or Wireless GWN router), navigate to **Web UI** → **Devices**, then click on the device or the configuration icon then select the configuration Tab. Refer to the figure below:



Device Configuration

Selecting the option “**Use Radio Settings**” from the drop-down list will use the settings configured on the **Global Radio Settings** section.

Please refer the table below:

General	
Band Steering	<p>Select from the drop-down list, four options are available:</p> <ul style="list-style-type: none"> ● Disable Band Steering: Band steering is disabled ● 2.4G in priority: steer clients to 2.4G ● 5G in priority: steer clients to 5G ● Balance: balance between 2.4G and 5G.
Client Steering	<p>This feature will help Wi-Fi client to roam to other APs within same Network. Steering happens when clients is inactive or active clients with the standards 802.11K&V support.</p>
RSSI Threshold	<p>It will start monitoring the RSSI for the clients in order to redirect them to another GWN AP in the same network. This prevents clients from remaining associated with AP with less than ideal RSSI, which can cause</p>

	poor connectivity and reduce performance for other clients. <i>Default is -75.</i>
Client Access Threshold	It will start monitoring the number of clients' connections with the AP, once reaching configured threshold, it will roam to the other. <i>Default is 30.</i>
Airtime Fairness	Allows faster clients to have more airtime than slower clients.
Beacon Interval	<p>Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp...</p> <ul style="list-style-type: none"> ● Using High Beacon Interval: AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save WiFi clients energy consumption. ● Using Low Beacon Interval: AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by WiFi clients with weak signal. <p>Notes:</p> <ul style="list-style-type: none"> ● When AP enables several SSIDs with different interval values, the max value will take effect. ● When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. ● When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. ● When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500. ● Mesh feature will take up a share when it is enabled. <p><i>Default value is 100ms. Valid range: 40 – 500 ms.</i></p>
Country/Region	Displays the country/region of the AP.
2.4G/5G	
Channel Width	Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20MHz is suggested in very high-density environment.
Channel	Select "Auto" or a Dynamically Assigned by RRM. <i>Default is "Auto".</i>
Custom Channel	Select a custom channels. <i>Note: that the proposed channels depend on Country Settings under Settings → System.</i>
Radio Power	<p>Set the Radio Power, it can be Low, Medium, or High or Custom or Dynamically assigned by RRM or Auto.</p> <p><i>Note : Dynamically assigned by RRM activates TPC and CHD:</i></p> <ul style="list-style-type: none"> ● 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 RSSI larger than -70dbm. 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. <p>Custom: allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.</p>
Enable Short Guard Interval	Check to activate this option to increase throughput.
Allow Legacy Devices (802.11b)	Check to support 802.11b devices to connect the AP in 802.11n/g mode. (2.4GHz setting)
Enable Minimum RSSI	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm).
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1".

Enable Minimum Rate	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP.
Minimum Rate (Mbps)	Specify the minimum access rate. Once the client access rate is less than the specified value, AP will kick it off. Available values are: 1Mbps, 2Mbps, 5Mbps, 6Mbps, 9Mbps, 11Mbps or 12Mbps.
Wi-Fi5 Compatible Mode	Some old devices do not support Wi-Fi6 well and may not be able to scan the signal or connect poorly. After turning on this switch, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions.

Global Radio Settings

Mesh

Wireless Mesh Network is a wireless extension of the traditional wired network using multiple access points connected through wireless links to areas where wired access is not an option while also expanding the coverage of the WLAN network.

In the traditional WLAN network, the uplink of the AP is a wired network (usually an Ethernet Link):

- o The advantages of a wired network are security, anti-interference and stable bandwidth.
- o The disadvantages are high construction cost, long period of planning and deployment, and difficulty of change in case a modification is needed.

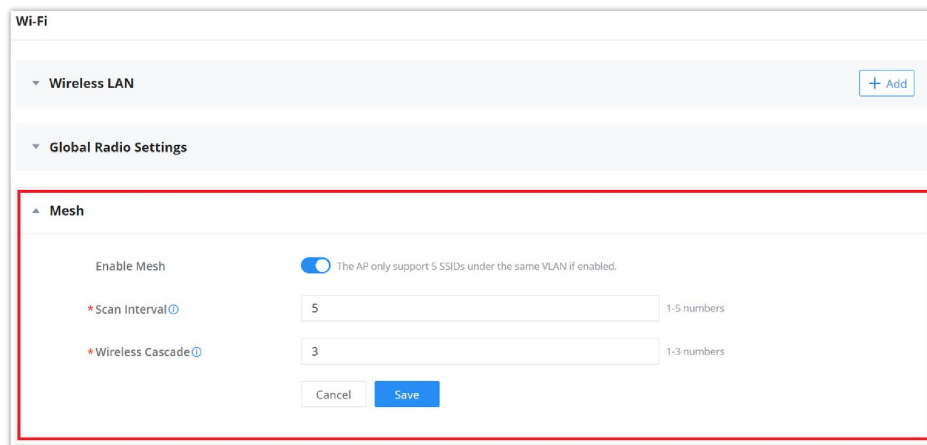
However, these are precisely the advantages of wireless networks. As a result, Wireless Mesh Network is an effective complement of wired network.

In addition, Mesh networking provides a mechanism for network redundancy. When an abnormality occurs in a wired network, an AP suffering the uplink failure can keep the data service continuity through its Mesh network.

For more details about the GWN Mesh Network feature, please don't hesitate to read the following technical paper:

https://www.grandstream.com/sites/default/files/Resources/GWN76XX_Mesh_Network.pdf

Users can setup some Mesh Network parameters under the menu **"Settings → Wi-Fi → Mesh"**, as shown on the figure below:



Mesh

LAN

This page shows all the created VLANs as well as the Default VLAN (Default LAN), as well as the global switch settings that affects all the added GWN switches.

LAN

LAN

Name	VLAN ID	Gateway	Gateway IPv4	Gateway IPv6	Operation
Default LAN	1	C0:74:AD:DF:CC:94	—	—	

Global Switch Settings

LAN page

The user can click on button to add a LAN/VLAN, then specify the name, VLAN ID, Gateway and IPv4/IPv6.

LAN > Add LAN

* LAN Name: 1-64 characters

* VLAN ID: 3-4094 numbers

VLAN-Only Network:

* Gateway:

IPv4

IPv4:

* Gateway IPv4 Address/Prefix Length: / Prefix length range: 8-30

DHCP Service:

* IPv4 Address Pool: -

* Release Time (m): 60-3850 numbers

DHCP Option: Type: Service: Content:

Preferred DNS Server:

Alternative DNS Server:

IPv6

IPv6:

Add VLAN

Global Switch Settings

Global Switch Settings allow the user to configure the general settings for all the GWN78XX switches which have been added to the account, instead of configuring the settings individually for each switch.

Global Switch Settings

RADIUS Authentication

RADIUS Authentication:

Voice VLAN

Voice VLAN:

Multicast

IGMP Snooping VLAN:

MLD Snooping VLAN:

Unknown Multicast Message:

DHCP Snooping Settings

DHCP Snooping:

802.1X

Guest VLAN:

Other

* Jumbo Frame:

Black Hole MAC Address:

Global Switch Settings

Radius Authentication	
Radius Authentication	Select a Radius server or click Add New RADIUS

Voice VLAN	
Voice VLAN	Toggle voice VLAN on/off.
Multicast	
IGMP Snooping VLAN	Select the IGMP Snooping VLAN.
MLD Snooping VLAN	Select the MLD Snooping VLAN.
Unknown Multicast Message	Configures how the switch (IGMP Snooping/MLD Snooping) handles packets from unknown groups.
DHCP Snooping Settings	
DHCP Snooping	Toggle DHCP Snooping on/off
802.1X	
Guest VLAN	Configures whether to enable the guest VLAN function for the global port.
Other	
Jumbo Frame	Enter the size of the jumbo frame. Range: 1518-10000
Black Hole MAC Address	Select a Black Hole MAC Address from the list or click Add New MAC group

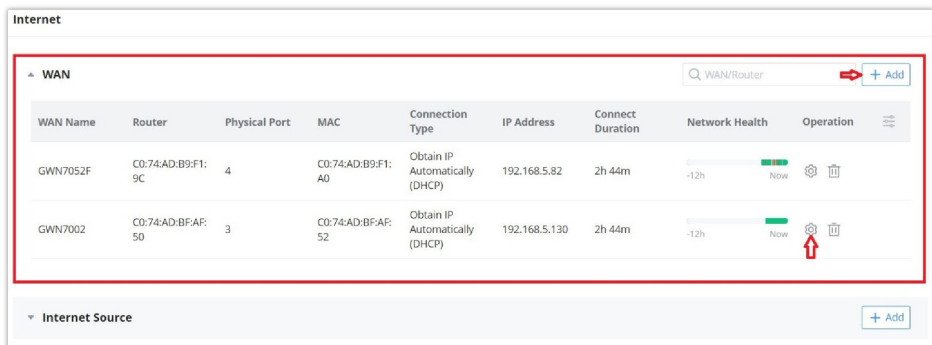
Internet

Internet configuration like adding/configuring WAN ports or configuring Load-balancing/backup (Failover) between the WANs port are found here, please navigate to **Web UI** → **Settings** → **Internet** page.

WAN

In this section, the user can add WAN (router WAN port or a device group) or edit previously created WAN ports and the number of WAN ports is determined by how many GWN routers are added/adopted to GWN.Cloud/GWN Manager accordingly. Once, the WAN/Device group is added, then the user can monitor the network health for the last 12 hours.

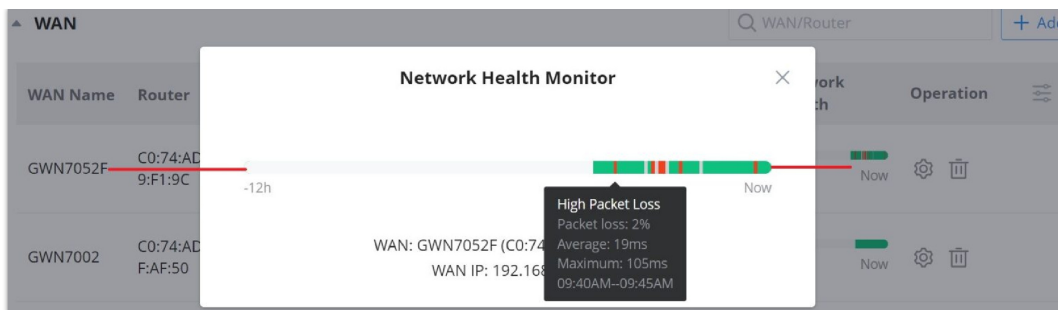
Please navigate to **Web UI** → **Settings** → **Internet** page → **WAN** section.



WAN

- o **Network Health**

Network Health is a feature that monitor the WAN (WAN ports or Device group) and displays the status for the last 12 hours for each WAN/device group with color code.



Network Health

Hover with the cursor over the color to see more details like Packet loss percentage, duration etc.

Green: Online

Grey: Offline

Red: High Packets Loss

- o **Add or Edit a WAN/Device group**

To edit a WAN click on the entry or click on “**Configure icon**” under operation, and to add a WAN click on “**Add**” button on the top of the page. on the next page, the user can configure the WAN name, router (WAN port or logical device group), physical port, connection type (DHCP, Static or PPPoE), MTU, DDNS, DMZ, UPnP, etc. Please check the figures and table below:

This screenshot shows the configuration form for WAN GWN7052F. The fields are as follows:

- WAN Name: GWN7052F (1-64 characters)
- Router: C0:74:AD-B9:F1:9C
- Physical Port: 4
- Connection Type: Obtain IP Automatically (DHCP)
- Static DNS:
- Preferred DNS Server: 8.8.4.4
- Alternative DNS Server: (empty)
- Maximum Transmission Unit (MTU): 1500 (576-1500 numbers)
- WAN Port MAC Address: Use Default MAC Address
- Tracking IP Address 1: 8.8.8.8
- Tracking IP Address 2: (empty)
- VLAN Tag:
- VLAN Tag ID: (empty) (3-4094 numbers)

Add/edit a WAN – part 1

This screenshot shows the configuration form for WAN GWN7052F, focusing on IPv6 settings. The fields are as follows:

- Priority: 0 (Range 0-7 and 7 is the highest priority)
- Multiple Public IP Addresses:
- Public IP Address: (empty) Add New Item (+)
- IPv6** (highlighted in red)
- IPv6:
- Connection Type: Obtain IP Automatically (DHCPv6)
- Static DNS:
- Preferred DNS Server: (empty)
- Alternative DNS Server: (empty)
- IPv6 Relay to VLAN: If enabled, IPv6 addresses will be relayed to LAN-side clients.
- Tracking IPv6 Address 1: (empty)
- Tracking IPv6 Address 2: (empty)

Add/edit a WAN – part 2

The screenshot shows a configuration page for a WAN connection. At the top, there's a breadcrumb 'Internet > GWN7052F' and a 'Sync' button. The main content is divided into three sections: DDNS, DMZ, and UPnP. The DDNS section has a toggle switch turned on, a 'Service Provider' dropdown set to 'no-ip.pl', and input fields for 'Username' (GS), 'Password' (masked), and 'Domain' (GS.ddns.net). A small note below says: 'If no account is available, please go to www.no-ip.pl to register for a username, password and domain.' The DMZ section has a 'Destination Group' dropdown set to 'None'. The UPnP section has a toggle switch turned on and a 'Destination Group' dropdown set to 'Select'. At the bottom are 'Cancel' and 'Save' buttons.

Add/edit a WAN – part 3

WAN Name	Specify a name for the WAN
Router	Select a router or a Device group from the drop-down list
Physical Port	Select the physical port (WAN port) from the drop-down list
Connection Type	<ul style="list-style-type: none"> ● Obtain IP automatically (DHCP): When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. ● Enter IP Manually (Static IP): When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. ● Internet Access with PPPoE account (PPPoE): When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval, and Inter-Key Timeout (in seconds). <p><i>The default setting is “Obtain IP automatically (DHCP)”</i></p>
Static DNS	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server
Preferred DNS Server	Enter the preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
Maximum Transmission Unit (MTU)	<p>Configures the maximum transmission unit allowed on the WAN.</p> <ul style="list-style-type: none"> ● When using Ethernet, the valid range that can be set by the user is 576-1500 bytes. The default value is 1500. Please do not change the default value unless you have to. ● When using PPPoE, the valid range that can be set by the user is 576-1492 bytes. The default value is 1492. Please do not change the default value unless you have to.
WAN Port MAC Address	<p>Select from the drop-down list either to:</p> <ul style="list-style-type: none"> ● Use Default MAC Address ● Use Custom MAC Address <p><i>Default is "Use Default MAC Address"</i></p>
Custom MAC Address	Enter the custom MAC Address to be used with this WAN.
Tracking IP Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal.
Tracking IP Address 2	Add another alternative address for Tracking IP Address
VLAN Tag	Select if either to enable or disable VLAN Tag.

VLAN Tag ID	Enter the VLAN tag ID.
Priority	Enter the priority <i>Note: Range 0-7 and 7 is the highest priority</i>
Multiple Public IP Addresses	Please use with Port Forward function, so that you can access to router via public IP address.
Public IP Address	Enter one or more public IP addresses Click on "+" icon or "-" icon to add or delete public IP addresses
IPv6	
IPv6	Enable this option to use IPv6 on this specific WAN.
Connection Type	Select the connection type from the drop-list, three options are available: <ul style="list-style-type: none"> ● Obtain IP automatically (DHCPv6) ● Enter the IP manually (static IPv6) ● Internet Access with PPPoE Account (PPPoE) <i>The default setting is "Obtain IP automatically (DHCPv6)".</i>
Static DNS	Enable this option to enter statically assigned DNS
Preferred DNS Server	Enter the preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
IPv6 Relay to VLAN	Once enabled, relay IPv6 addresses to clients on the LAN side. Note: This function will take effect only "IPv6 Relay from WAN" is enabled on VLAN.
Tracking IPv6 Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal
Tracking IPv6 Address 2	Add another alternative address for Tracking IP Address
DDNS	
DDNS	Toggle ON or OFF the DDNS function, default is OFF <i>Note: On the router, DDNS function can only be enabled on one WAN port</i>
Service Provider	Select the DDNS provider from the list <i>Note: If no account is available, please go to www.oray.com to register for a username, password and domain</i>
Username	Enter the Username
Password	Enter the Password
Domain	Enter the Domain
DMZ	
Destination Group	Select the destination group from the drop-down list.
UPnP	
UPnP	Toggle ON or OFF the UPnP function, default is OFF <i>Note: If UPnP (Universal Plug and Play) is enabled, devices on LAN can request the router to port forward automatically</i>

Destination Group	Select the destination group from the drop-down list.
--------------------------	---

Add/edit a WAN

Internet Source

In this section of internet configuration, under internet source, the user can configure load balancing or backup (Failover) between the previously added WANs. Either click on the entry or "**Configure icon**" to edit previously added internet sources or click on "**Add**" button to add a new one, refer to the figure below:



Internet Source

Here, the user can specify the name for the Load Balance or Backup, select the router/device group and specify the weight for each uplink.

- **Default:** If enabled, the subsequent WAN added by the router will be associated with the Internet Source
- **Interface:** In an Internet source, each interface can only be selected once, and only interfaces of the same router or the same device group are supported in an Internet source.
- **Weight:** Weight value determines the ratio at which connections are sent through each member. The default is 1. Enter a value from 1~10 with 10 being the highest weight.



Add an Internet Source

VPN

GWN.Cloud and GWN Manager support many VPNs including PPTP, IPSec (Site-to-Site), OpenVPN® and WireGuard®.

GWN.Cloud and GWN Manager support more than one GWN router with single or multi-WAN on the same network, thus when configuring a VPN it's important to specify which router (WAN/Device group) and interface will be used.

- **PPTP:** supports client and server.
- **IPSec (Site-to-Site):** supports manual and auto mode.
- **OpenVPN®:** supports client and server.
- **WireGuard®:** server side.

To add a new VPN or a VPN user, please navigate to **Web UI** → **Settings** → **VPN** and then click on "**Add**" button as shown in the figure below:



VPN

PPTP

PPTP is a data-link layer protocol for wide area networks (WANs) based on the Point-to-Point Protocol (PPP) and developed by Microsoft that enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet. Point-to-Point Tunneling Protocol (PPTP) allows the creation of virtual private networks (VPNs), which tunnel TCP/IP traffic through the Internet.

Below figure shows the configuration for adding a PPTP Client, it's also possible the say way to add a PPTP Server. When adding a PPTP Client make sure to specify the username and password as well.



VPN – Add PPTP Client

Type	Select either PPTP Client or PPTP Server to configure.
Name	Enter a name for the PPTP client.
Status	Toggle ON or OFF to enable or disable the PPTP Client VPN. <i>Note: PPTP Server: Once disabled, the PPTP service will also be disabled.</i>
Server Address	Enter the IP/Domain of the remote PPTP Server.
Username	Enter the Username for authentication with the VPN Server.
Password	Enter the Password for authentication with the VPN Server.
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
MPPE Encryption	Enable / disable the MPPE for data encryption. <i>By default, it's disabled.</i>
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.

(MTU)	
Remote Subnet	Configures the remote subnet for the VPN. The format should be “IP/Mask” where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32. <i>example: 192.168.5.0/24</i>

VPN – Add PPTP Client

VPN – Add PPTP Server

Type	Select either PPTP Client or PPTP Server to configure.
Name	Enter a name for the PPTP Server.
Status	Toggle ON or OFF to enable or disable the PPTP Client/Server VPN. <i>Notes: Once disabled, the PPTP service will also be disabled.</i>
Server Local Address/Prefix Length	Specify the server local address with the prefix length
Client Start Address	specify client start IP address
Client End Address	specify client end IP address
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
MPPE Encryption	Enable / disable the MPPE for data encryption. <i>By default, it's disabled.</i>
LCP Echo Interval (sec)	Configures the LCP echo send interval.
LCP Echo Failure Threshold	Set the maximum number of Echo transfers. If it is not answered within the set request frames, the PPTP server will consider that the peer is disconnected and the connection will be terminated.

LCP Echo Adaptive	<ul style="list-style-type: none"> ● Once enabled: LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request. ● Once disabled: the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.
Maximum Receive Unit (MRU)	MRU indicates the size of the received packets. By default is 1450.
Preferred DNS Server	specify the preferred DNS server. <i>Ex: 8.8.8.8</i>
Alternative DNS Server	specify the alternative DNS server. <i>Ex: 1.1.1.1</i>

VPN – Add PPTP Server

IPSec (Site-to-Site)

Internet Security protocol- IPsec is mainly used to authenticate and encrypt packets of data sent over the network layer. To accomplish this, they use two security protocols – ESP (Encapsulation Security Payload) and AH (Authentication Header), the former provides both authentications as well as encryption whereas the latter provides only authentication for the data packets. Since both authentication and encryption are equally desirable, most of the implementations use ESP.

IPsec supports two different encryption modes, they are Tunnel (default) and Transport mode. Tunnel mode is used to encrypt both payloads as well as the header of an IP packet, which is considered to be more secure. Transport mode is used to encrypt only the payload of an IP packet, which is generally used in gateway or host implementations.

GWN.Cloud and GWN Manager support IPsec (Site-to-Site) that can help encrypts and secures traffic between two sites using two GWN routers. It supports manual configuration and auto mode.

VPN – Add IPSec Auto

Mode	Select the mode: Manual or Auto . <i>Note: If Auto is selected, the LAN subnet and WAN IP will be automatically set to the peer router, and will synchronize automatically after the change, and the IPSec link will not be disconnected due to the change of WAN IP.</i>
Name	Specify a name for IPSec VPN.
Status	Toggle ON or OFF to enable or disable the IPSec VPN. <i>Note: Once disabled, the associated VPN services will also be disabled.</i>
Router	Select from the drop-down list the router/device group that this VPN will be using.

Interface	Select from the drop-down list the exact interface of the router/device group.
Peer	Set the IP address of the WAN port so the peer network automatically connects with the current network.

VPN – Add IPSec auto mode

For the manual mode, please refer to the figure and table below:



VPN – Add IPSec Manual mode

General	
Mode	Select the mode: Manual or Auto. <i>Note: If Auto is selected, the LAN subnet and WAN IP will be automatically set to the peer router, and will synchronize automatically after the change, and the IPSec link will not be disconnected due to the change of WAN IP.</i>
Name	Specify a name for IPSec VPN.
Status	Toggle ON or OFF to enable or disable the IPSec VPN. <i>Note: once disabled, the associated VPN services will also be disabled.</i>
Remote address	Specify the remote IP address
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
Pre-shared key	Specify a pre-shared key

Local Network	Set the local IP address and mask length of the protected traffic. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Remote Network	Set the peer IP address and mask length of the protected data flow. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Advanced Settings	
IKE Version	Select from the drop-down list the IKE version: IKEv1 or IKEv2.
IKE SA Lifetime (sec)	Specify the IKE SA Lifetime (sec), default is 28800.
Local Source IP	Enter the local Source IP address.
Local ID	Set the local ID to identify the identity of the local device for the remote device to verify its legitimacy.
Remote ID	Set the remote ID to authenticate the identity of the remote device. This parameter must be consistent with the local ID set on the remote device.
Negotiation Mode	Select the negotiation mode from the drop-list, two options are list: Main or Aggressive.
Encryption Algorithm	<p>Select from the drop-down list the encryption algorithm to use, the available ones are:</p> <ul style="list-style-type: none"> ● 3DES ● AES-128 ● AES-192 ● AES-256 <p>Default is AES-256</p>
Hash Algorithm	<p>Select from the drop-down list the Hash algorithm to use, the available ones are:</p> <ul style="list-style-type: none"> ● MD5 ● SHA-1 ● SHA2-256 <p>Default is SHA2-256</p>
DH Group	DH (Diffie-Hellman) group, select from the drop-down list the DH group, available groups are Group 2,5,14,19,20,21.
Reconnect	Set whether to renegotiate the connection when it is about to expire.
Number of Reconnections	Specify the number of reconnections. <i>Note: The range is 0-10. 0 means continuous attempts to negotiate a connection.</i>
DPD (Dead Peer Detection)	Toggle ON or OFF DPD. <i>Note: DPD is a method that is used by devices to check for the current existence and availability of IPsec peers.</i>
DPD Delay Time (sec)	Set the delay time for connecting DPD keepalive packets.
DPD Idle Time (sec)	Set the amount of time to remain idle if no response is received from the peer.
DPD Action	<ul style="list-style-type: none"> ● Hold: Hold IPsec routes and delete IPsec SA. ● Clear: Delete IPsec routes, IPsec and IKE SA. ● Restart: Delete IPsec routes, IPsec SA, and IKE SA, then re-initiate the negotiation.
IPsec SA Lifetime (sec)	Specify the IPsec SA lifetime, default is 3600.

ESP Encryption Algorithm	<p>Select from the drop-down list the ESP Encryption Algorithm, the available ones are:</p> <ul style="list-style-type: none"> • 3DES • AES-128 • AES-192 • AES-256 <p>Default is AES-256.</p>
ESP Hash Algorithm	<p>Select from the drop-down list the ESP Hash Algorithm, the available ones are:</p> <ul style="list-style-type: none"> • MD5 • SHA-1 • SHA2-256 <p>Default is SHA2-256</p>
PFS Group	<p>Select from the drop-down list the PFS group, the available ones are: Group 2,5,14.</p> <p>Default is disabled.</p>

VPN – Add IPSec Manual mode

OpenVPN®

OpenVPN® is a virtual private network system that secures site-to-site or point-to-point traffic in routed or bridged configurations and remote access facilities. It supports both client and server side.

GWN.Cloud and GWN Manager support both OpenVPN® Client and Server side also certificates management for ease of use.

The screenshot shows the 'Add OpenVPN®' configuration page. The 'Type' field is set to 'OpenVPN® Server', which is highlighted with a red box. The 'Name' field contains 'OpenVPN Server'. The 'Status' is turned off, with a note: 'Once disabled, the OpenVPN® service will also be disabled.' The 'Protocol' is set to 'UDP'. The 'Router' is 'C0:74:AD:BF:AF:50', 'Interface' is 'GWN7002', and 'Local Port' is '1194'. The 'Authentication Mode' is 'SSL', 'Encryption Algorithm' is 'AES-256-CBC', and 'Digest Algorithm' is 'SHA256'. 'TLS Identity Authentication' and 'Duplicate client certificates are allowed' are both disabled. 'Redirect Gateway' is enabled. 'Cancel' and 'Save' buttons are at the bottom.

VPN – Add OpenVPN® Server

Type	Select the OpenVPN®: Client or Server
Name	Enter a name for the OpenVPN® server.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Server. <i>Note: Once disabled, the OpenVPN® service will also be disabled.</i>
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. <i>The default protocol is UDP.</i>

Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
Local Port	Configure the listening port for OpenVPN® server. <i>The default value is 1194.</i>
Authentication Mode	<p>Choose the server mode the OpenVPN® server will operate with. 4 modes are available:</p> <ul style="list-style-type: none"> ● SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). ● User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). ● SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. ● PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
TLS Identity Authentication	<p>This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers.</p> <p>This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.</p>
TLS Identity Authentication Direction	Select from the drop-down list the direction of TLS Identity Authentication, three options are available (Server, Client or Both).
TLS Pre-Shared Key	If TLS Identity Authentication is enabled, enter the TLS Pre-Shared Key.
Duplicate client certificates are allowed	Click on " ON " to allow duplicate Client Certificates
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
Push Routes	Specify route(s) to be pushed to all clients. <i>Example: 10.0.0.1/8</i>
LZO Compression Algorithm	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificate	Select a generated CA from the dropdown list or add one.
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.

IPv4 Tunnel Network/Mask Length	Enter the network range that the GWN70xx will be serving from to the OpenVPN® client. <i>Note: The network format should be the following 10.0.10.0/16. The mask should be at least 16 bits.</i>
--	--

VPN – Add OpenVPN® Server



VPN – Add OpenVPN® Client

Type	Select the OpenVPN®: Client or Server
Name	Enter a name for the OpenVPN® Client.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Client. <i>Note: Once disabled, the associated VPN services will also be disabled.</i>
Protocol	Specify the transport protocol used. <ul style="list-style-type: none"> • UDP • TCP <i>Note: The default protocol is UDP.</i>
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
Local Port	Configures the client port for OpenVPN®.The port between the OpenVPN® client and the client or between the client and the server should not be the same.

Remote OpenVPN® Server	Configures the remote OpenVPN® server. Both IP address and domain name are supported.
OpenVPN® Port	Configures the remote OpenVPN® server port
Authentication Mode	<p>Choose the server mode the OpenVPN® server will operate with. 4 modes are available:</p> <ul style="list-style-type: none"> • SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). • User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). • SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. • PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	<p>Choose the encryption algorithm. The encryption algorithms supported are:</p> <ul style="list-style-type: none"> • DES-CBC • RC2-CBC • DES-EDE-CBC • DES-EDE3-CBC • DESX-CBC • BF-CBC • RC2-40-CBC • CAST5-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC
Digest Algorithm	<p>Select the digest algorithm. The digest algorithms supported are:</p> <ul style="list-style-type: none"> • MD5 • RSA-MD5 • SHA1 • RSA-SHA1 • DSA-SHA1-old • DSA-SHA1 • RSA-SHA1-2 • DSA • RIPEMD160 • RSA-RIPEMD160 • MD4 • RSA-MD4 • ecdsa-with-SHA1 • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 • RSA-SHA224 • SHA256 • SHA384 • SHA512 • SHA224 • whirlpool
TLS Identity Authentication	Enable TLS identity authentication direction.

TLS Identity Authentication Direction	Select the identity authentication direction. <ul style="list-style-type: none"> • Server: Identity authentication is performed on the server side. • Client: Identity authentication is performed on the client side. • Both: Identity authentication is performed on both sides.
TLS Pre-Shared Key	Enter the TLS pre-shared key.
Routes	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
Deny Server Push Routes	If enabled, client will ignore routes pushed by the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
LZO Compression	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no. LZO encoding provides a very high compression ratio with good performance. LZO encoding works especially well for CHAR and VARCHAR columns that store very long character strings.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificates	Click on “Upload” and select the CA certificate Note: This can be generated in System Settings → Certificates → CA Certificate
Client Certificate	Click on “Upload” and select the Client Certificate. Note: This can be generated in System Settings → Certificates → Certificate

VPN – Add OpenVPN® Client

VPN User

In this section, the user can add a VPN user for either PPTP VPN or OpenVPN®. Please refer to the figure and table below:

The screenshot shows the 'Add VPN User' configuration interface. The 'Server Type' dropdown is set to 'OpenVPN®', which is highlighted with a red box. Other fields include 'Name' (VPN User), 'Status' (checked), 'Server' (OpenVPN Server), 'Username' (OpenVPN_User1), 'Password' (P@ssW0rd), 'Client Subnet' (192.168.2.0 / 24), and 'Client Certificate' (Client Cert). There are 'Cancel' and 'Save' buttons at the bottom.

VPN – Add VPN User

Name	Enter a name for the user. This name will not be used to log in.
Status	Enable or disable this account.
Server Type	Choose the type of the server. <ul style="list-style-type: none"> • PPTP

	<ul style="list-style-type: none"> • OpenVPN®
Server Name	Select the VPN server from the drop-list
Username	Enter the username. This username will be used to log in. <i>Note: only alphanumeric characters and @ ! \$ % - _ are supported.</i>
Password	Enter the password. <i>Note: only alphanumeric characters and @ ! \$ % - _ are supported.</i>
Client Subnet	Set the IP address and mask length of the subnet for the client to access. Please enter an IP address or subnet (e.g., 192.168.2.0/24)
Only if OpenVPN® is selected	
Client Certificate	Select from the drop-down list the client certificate.

VPN – Add VPN User

WireGuard®

WireGuard® is free and open source VPN solution that encrypts virtual private networks, easy to use, high performance and secure.

GWN.Cloud and GWN Manager support WireGuard® as well, a Server local address can be specified while private key can be generate with one-click then after that the public key can be copied and shared with the client.

VPN > **Add WireGuard®**

* Name	WireGuard VPN
Status	<input type="checkbox"/> Once disabled, the associated WireGuard® service will also be disabled.
* Router	C0:74:AD:BF:AF:50
* Interface	GWN7002
* Listening Port	51820
* Server Local Address/Prefix Length	192.168.7.0 / 24
* Private Key	yEXeLmFGEFgMj3VELbenSM92Gshq8+jvYX5h6mw98Ho= One-Click Generation
Public Key	Lp+f9uAcf9Nhpsd/TGqE9kGFIsxyYOBaobiCOZIWO30= Copy
* MTU	1420

VPN – Add WireGuard®

Name	Specify a name for Wireguard® VPN.
Status	Toggle ON or OFF to enable or disable the Wireguard® VPN.
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group. <i>Note: one WAN only supports creating one WireGuard®.</i>
Listening Port	Set the local listening port when establishing a WireGaurd® tunnel. <i>Default: 51820</i>

Server Local Address/Prefix Length	Specify the server local address with the prefix length
Private Key	Click on "One-Click Generation" text to generate a private key.
Public Key	The public key will be generated according to the private key. Click on "Copy" text to copy the public key.
MTU	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.

VPN – Add WireGuard®

Traffic Management

On this page, the user is able to manage traffic by either adding static routes (IPv4 or IPv6) or adding Policy Routes.

Static Routes

Static routing is a form of routing by manually configuring the routing entries, rather than using a dynamic routing traffic for any service that requires a static address that never change.

GWN.Cloud and GWN Manager support setting manually **IPv4 or IPv6 Static Routes** which can be accessed from **Web UI → Settings → Traffic Management page → Static Routes section.**


All the Static routes either IPv4 or IPv6 will be listed here.

The screenshot shows the 'Traffic Management' interface. It has two main sections: 'Static Routes' and 'Policy Route'. The 'Static Routes' section is highlighted with a red box and contains a table with one entry: 'main exit' with a 'Disabled' state. The 'Policy Route' section contains a table with one entry: 'main route' with an 'On' status.

Static Routes									
Name	State	Gateway Device	IP Address	Subnet Mask	Outgoing Interface	Next Hop	Metric	Operation	
main exit	Disabled	C0:74:AD:BF:AF...	192.168.5.1	255.255.255.0	GWN7002	—	60	⚙️ 🗑️	

Policy Route									
Name	Status	Router	Protocol Type	Source Group	Source IP Address	Destination IP Address	Internet Source	Operation	
main route	On	C0:74:AD:BF:AF:50	TCP/UDP	All	192.168.80.0/24	—	1	⚙️ 🗑️	

Static Routes

Click on  button to add a static route, the user has the option between IPv4 or IPv6.

The 'Add Static Route' form is shown with the following fields and values:

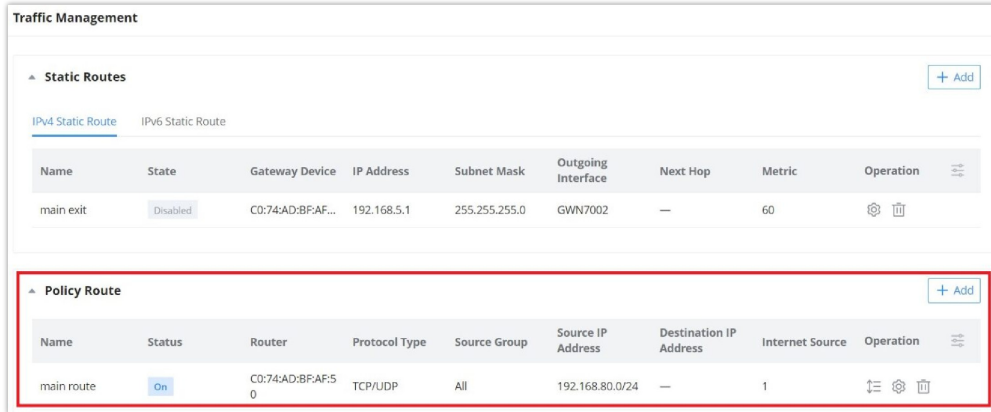
- Type: IPv4 Static Route IPv6 Static Route
- Name: IPv4 Static Route (Supports 1-64 characters)
- Status: On
- Gateway Device: C0:74:AD:95:12:90
- Destination IP Address: 192.168.5.85
- Subnet Mask: 255.255.255.0
- Outgoing Interface: WAN1
- Next Hop: (empty)
- Metric: 60

Buttons: Cancel, Add

Add Static Route

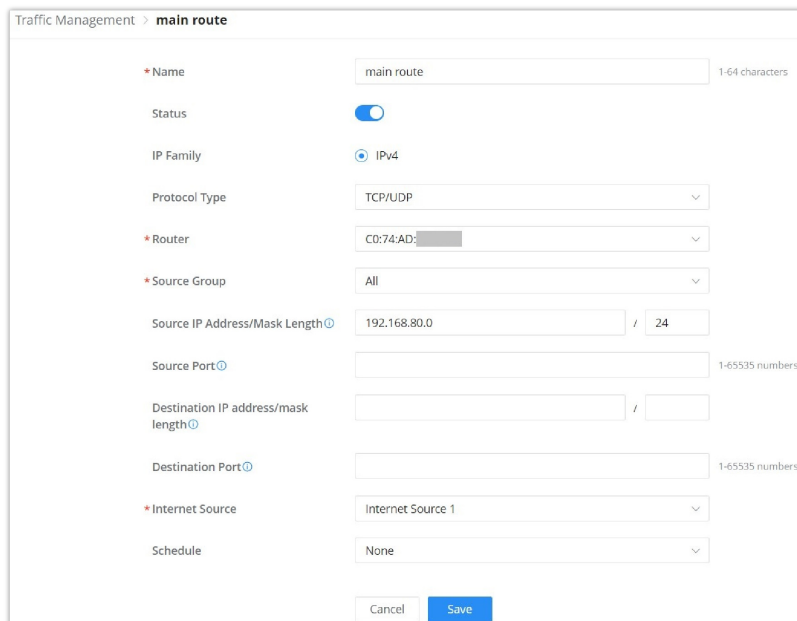
Policy Route

GWN.Cloud and GWN Manager support managing more than one GWN router on the same network, with multiple GWN routers added, the user will have many [internet sources](#), which will enable the user to specify which traffic can be forwarded to an internet source (Load Balance/Backup). Also a schedule can be applied to this policy route to only be active based on the [schedule](#) selected.



Policy Route

Navigate **Web UI** → **Settings** → **Traffic Management page** → **Policy route section** and then click on **“Add”** button to add a policy route, please refer to the figure below:



Add Policy Route

Name	Specify a name for the policy route
Status	Toggle ON or OFF to enable or disable the policy route
IP Family	IP Family, default is IPv4
Protocol Type	Select from the drop-down list the protocol type: <ul style="list-style-type: none"> • All • TCP • UDP • TCP/UDP • ICMP
Router	Select from the drop-down list the router or the device group <i>Note: for device groups, only router group is supported</i>
Source Group	Select the source group from the drop-down list

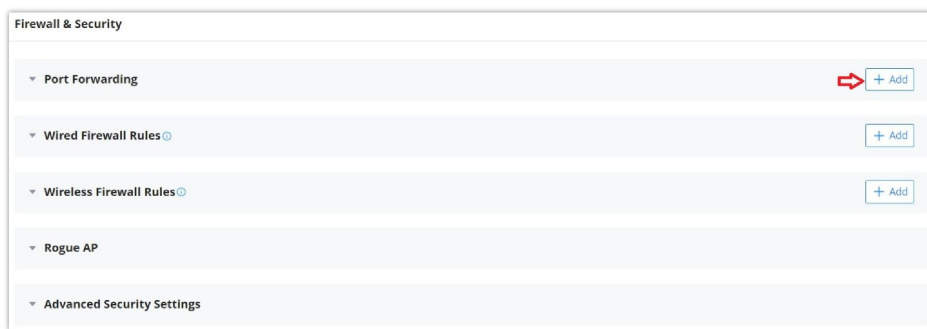
Source IP Address/Mask Length	Set the source IP address and mask length of the packet to be matched. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Destination IP address/mask length	Set the destination IP address and mask length to match the packet. For example, 192.168.122.0/24
Internet Source	Select the internet source (WAN/Load Balance/Backup) from the drop-down list
Schedule	Select a schedule from the drop-down list or click on "Add New Schedule" to add one.

Add Policy Route

Firewall and Security

Firewall & Security page combine all the related configuration related to firewall and security, split into 5 sections (Port Forwarding, Wired Firewall Rules, Wireless Firewall Rules, Rogue AP and Advanced Security Settings).

Click on a section to expand the list or click on [+ Add](#) button to add more.



Firewall and Security

Port Forwarding

Port forwarding is redirecting the communication request from one address and port to another one address and port. A source IP Address and port will be mapped to a Destination IP Address, port and Group.

To add port forwarding, navigate to **Web UI** → **Settings** → **Firewall & Security page** → **Port Forwarding tab**.

Port Forwarding

Refer to the following table for the Port Forwarding option when editing or creating a port-forwarding rule:

Name	Enter a name for the port forwarding rule.
-------------	--

Status	Toggle on/off the rule status.
Protocol Type	Select a protocol, users can select TCP, UDP or TCP/UDP.
Interface	Select the WAN port
Source IP Address	Sets the IP address that external users access to this device. If not set, any IP address on the corresponding WAN port can be used
Source Port	Set a single or a range of Ports.
Destination Group	Select VLAN group.
Destination IP Address	Set the destination IP address.
Destination Port	Set a single or a range of Ports.

Port Forwarding

Wired Firewall Rules

The administrator can Accept, Reject or Drop wired traffic using inbound rules or forwarding rules, navigate to **Web UI** → **Settings** → **Firewall & Security page** → **Wired Firewall Rules tab**.

- **Accept:** To allow the traffic to go through.
- **Deny:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

Note:

Wired firewall rules apply only to Routers.

Wired Firewall Rules

Type	Select the type of the firewall rule: Inbound or Forwarding rule
Name	Enter a name for the wired firewall rule.
Status	Toggle on or off the wired firewall rule.

IP Family	Select the IP Family used: IPv4, IPv6 or Any
Protocol Type	Select the protocol type from the drop-down list.
Source Group	Select the source group, it can be either a WAN or VLAN. <i>Note: If set to "All", more specific rules will take priority.</i>
Source MAC Address	Specify a source MAC Address, else the rule will be applied on all MAC addresses.
Source IP Address/Mask Length	Sets the source IP address of the external device. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Source Port	Separate multiple ports and port ranges with commas (e.g., "4, 5-10").
Destination Group	Select the Destination group: WAN or VLAN <i>Note: This option is only available when selecting Forwarding rules</i>
Destination IP Address/Mask length	Sets the IP address that external devices access the router. Please an IP address or subnet (e.g., 192.168.122.0/24).
Destination Port	Separate multiple ports and port ranges with commas (e.g., "4, 5-10").
Action	<ul style="list-style-type: none"> ● Accept: Requests from external clients will be allowed. ● Deny: Requests from external clients will be denied, and a response will be returned. ● Drop: Requests from external device will be dropped, and no response will be given.

Wired Firewall Rules

Wireless Firewall Rules

This section is located under **Web UI** → **Settings** → **Firewall & Security page** → **Wireless Firewall rules tab**, it does allow users to control the outgoing and incoming traffic from clients connected to the adopted/paired GWN devices by manually setting up policies to either deny or permit the traffic for wireless traffic based on protocol type and by specifying SSIDs and destinations.

Note:

Wireless firewall rules apply only to AP.

Add Wireless Firewall Rules

Type	Select the type of the firewall rule: Inbound rules or Outbound rules
-------------	---

Name	Enter a name for the wireless firewall rule.
Service Protocol	Select the Service protocol type from the drop-down list.
Policy	<ul style="list-style-type: none"> ● Permit: Traffic from clients will be allowed. ● Deny: Traffic from clients will be denied.
Source	Select the source, it can be from a Particular IP or Network then enter the IP and/or the subnet. <i>Note: this option is only available when the type selected is Inbound rules.</i>
Destination	Select the destination, it can be from a Particular IP, Network or Domain. then enter the IP/Domain and/or the subnet.
SSID	If All is selected, this rule will also be applied to new SSIDs (Wireless LAN). <i>Note: this option is only available when the type selected is Outbound rules!</i>

Add Wireless Firewall Rules

Rogue AP

GWN Cloud and GWN Manager offer the ability to prevent malicious intrusion to the network and increases the wireless security access of clients when introducing Rogue AP detection feature to the adopted/paired GWN devices. The detected devices will be listed with all the details under “**Alerts**” page for further intervention.

Navigate to **Settings** → **Firewall & Security page** → **Rogue AP section**, The below figure shows the configuration page in order to enable Rogue AP detection.

Rogue AP

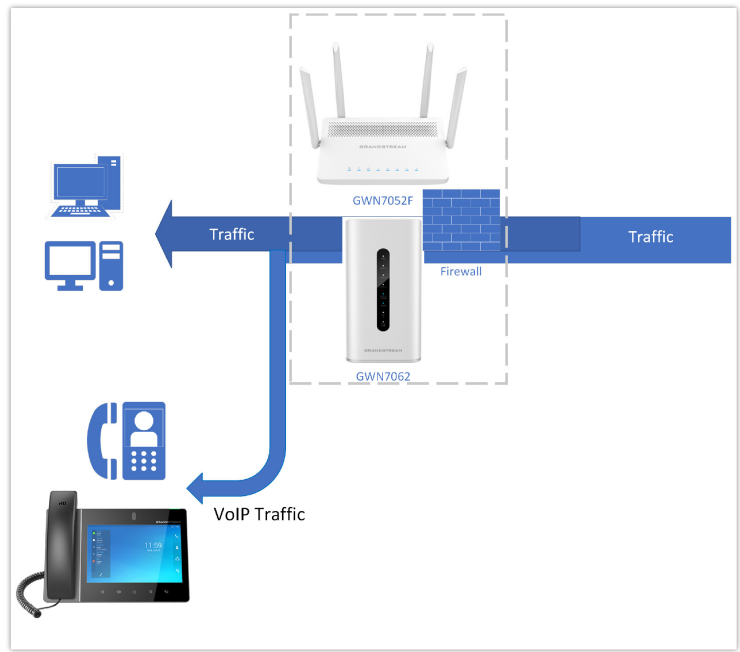
Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect Range	<p>Specify the rogue AP detect range.</p> <ul style="list-style-type: none"> ● Same Channel: AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication. ● All channels: AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt. <p><i>Default is Same Channel.</i></p>

Countermeasure Level	<p>Countermeasures level specifies the type of attacks which will be suspected by the AP. Select different levels:</p> <ul style="list-style-type: none"> • High: Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. • Medium: Untrusted BSSID, Illegal access without authentication, Illegal access. • Low: Untrusted BSSID, Illegal access without authentication <p><i>Default is Disabled.</i></p>
Containment Range	<p>Specify the containment range:</p> <ul style="list-style-type: none"> • Same channel: detect AP will countermeasure the APs in the same channel. • ALL channels: detect AP will countermeasure the APs in all channels at the cost of consuming of much AP performance. <p><i>Default is Same Channel.</i></p>
Sub-string for Spoofing SSID	The AP broadcasting SSID with the specified string will be classified as a Spoofing SSID.
Trusted AP	You can specify MAC address of the trusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as trusted AP, no countermeasures will be executed on it.
Untrusted AP	You can specify MAC address of the untrusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

Rogue AP

Application Layer Gateway (ALG)

ALG stands for **Application Layer Gateway**. Its purpose is to prevent some of the problems caused by router firewalls by inspecting VoIP traffic (packets) and if necessary modifying it.



Application Layer Gateway

To configure ALG, navigate to **Web GUI → Settings → Firewall & Security page → Advanced Security Settings tab.**

ALG

PROFILES

Portal policy

The policy configuration page allows adding multiple captive portal policies which will be applied to SSIDs and contains options for different authentication types a splash page that can be easily configured as shown on the next section.

Each SSID can be assigned a different captive portal policy, for example company ABC could have a specified Wi-Fi for staff people who can access via a portal policy requiring user name and password for authentication, and another SSID for guest people who can sign in via their Facebook account; also, they could assign either an internal or external Splash page.

Add Portal Policy

Internal Splash Page

Please refer to the table below when configuring Internal Splash Page.

Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, Internal or External. <i>Note: this table is only about internal splash page.</i>
Client Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Client Idle Timeout	Specify the idle timeout value for guest network connection. Once timed out, guest should re-authenticate for further network use.

	<i>Note: this option is not applicable to voucher guests and payment guests.</i>
Timeout Duration of Unauthenticated Clients (minutes)	Set the timeout time for unauthenticated clients. After the timeout, unauthenticated client devices are disabled from using Wi-Fi.
Failsafe Mode	Once enabled, guest can access internet when the authentication server or external portal is unreachable. <i>Note: only the Radius, custom field and Voucher authentications support this feature.</i>
Daily Limit	<ul style="list-style-type: none"> ● Disabled: Daily access is not limited. ● Limit by Client: Guest can access only once a day. ● Limit by Authentication Type: Users can access each authentication mode only once a day.
Splash Page Customization	Select a splash page from the drop-down list or click " Add New Splash Page ".
Landing Page	Choose the landing page, 2 options are available: <ul style="list-style-type: none"> ● Redirect to the Original URL. ● Redirect to External Page.
Enable HTTPS Redirection	Check to enable/disable HTTPS service. 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.
Enable Secure Portal	If enabled, HTTPS protocol will be used in the communication between STA and AP. Otherwise, the HTTP protocol will be used.
Pre Authentication Rule(s)	
Destination	Destination can be either IP Address, Hostname or Subnet/Prefix
Service	<ul style="list-style-type: none"> ● All: no limitation. ● Web: web related services. ● TCP Port: input integer between 1~65535. ● UDP Port: input integer between 1~65535. ● Protocol Id: input related services agreement No.
Post Authentication Rule Type	<ul style="list-style-type: none"> ● If set to "Blocklist", access to all except the rules added. ● if set to "Allowlist", only access the rules added.
Post Authentication Rule(s)	
Destination	Destination can be either IP Address, Hostname or Subnet/Prefix
Service	<ul style="list-style-type: none"> ● All: no limitation. ● Web: web related services. ● TCP Port: input integer between 1~65535. ● UDP Port: input integer between 1~65535. ● Protocol Id: input related services agreement No.

Portal Policy – Internal Splash Page

External Splash page

Please refer to the table below when configuring External Splash Page.

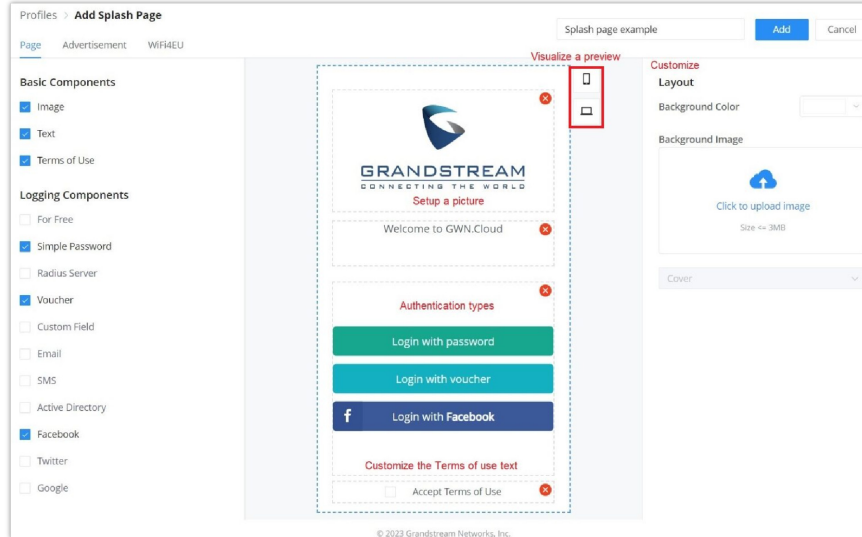
Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, Internal or External. <i>Note: this table is only about external splash page.</i>
Platform	Select the Radius Authentication Method provided by external portal platform.
If Linkyfi, Purple or Universal Platform is selected	
External Splash Server Address	Enter the External Splash Page URL, and make sure to enter the pre-authentication rules request by the external portal platform in the pre-authentication configuration option.
RADIUS Authentication	Select a RADIUS from the drop-down list or click on "Add New Radius".
If Aiwifi platform is selected	
URL Pre-shared Key	The configuration will be used to generate the signature. Please enter 20-32 characters, support entering numbers, English, characters (excluding spaces)
Timeout Duration of Unauthenticated Clients (minutes)	Set the timeout time for unauthenticated clients. After the timeout, unauthenticated client devices are disabled from using Wi-Fi.
External page	Please enter the Redirect URL provided by external portal platform.
Enable HTTPS Redirection	Check to enable/disable HTTPS service. 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.
Pre Authentication Rule(s)	
Destination	Destination can be either IP Address, Hostname or Subnet/Prefix
Service	<ul style="list-style-type: none"> ● All: no limitation. ● Web: web related services. ● TCP Port: input integer between 1~65535. ● UDP Port: input integer between 1~65535. ● Protocol Id: input related services agreement No.
Post Authentication Rule Type	<ul style="list-style-type: none"> ● If set to "Blocklist", access to all except the rules added. ● if set to "Allowlist", only access the rules added.
Post Authentication Rule(s)	
Destination	Destination can be either IP Address, Hostname or Subnet/Prefix
Service	<ul style="list-style-type: none"> ● All: no limitation. ● Web: web related services. ● TCP Port: input integer between 1~65535. ● UDP Port: input integer between 1~65535. ● Protocol Id: input related services agreement No.

Splash page

Splash page allows users with an easy to configure menu to generate a customized splash page that will be displayed to the users when trying to connect to the Wi-Fi.

On this menu, users can create multiple splash pages and assign each one of them on a separate captive portal policy to enforce the selected authentication type.

The generation tool provides an intuitive “WYSIWYG” method to customize a captive portal with very rich manipulation tool.



Add Splash Page

Users can set the following:

- **Authentication type:** Add one or more ways from the supported authentication methods:

For Free	Clients can log in without authentication.
Simple Password	The user can specify a password that clients must enter to authenticate.
Radius Server	Authentication using a RADIUS server.
Voucher	Authentication using a Voucher code.
Custom Field	The user can specify a custom field depending on the information needed: <ul style="list-style-type: none"> ● Text ● Check Box ● Radio Box ● Date
Email	Authentication using Email.
SMS	Authentication using SMS, with Twilio or Amazon SMS Service Provider.
Active Directory	Authentication using Active Directory.
Facebook	Authentication using Facebook account.
Twitter	Authentication using Twitter account.
Google	Authentication using Google account.

- o **Setup a picture (company Logo)** to be displayed on the splash page.
- o **Customize** the layout of the page and background colors.
- o **Customize the Terms of use text.**
- o **Visualize a preview** for both mobile devices and laptops.

Note:

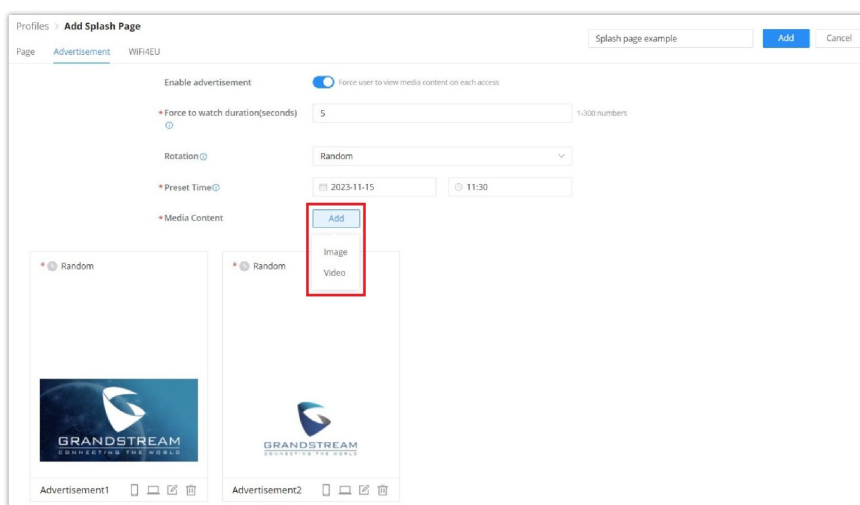
On each splash page, the maximum number of authentication methods is 5 methods.

Advertisement

On this page, advertisement can be enabled and forced on each access point, where users will be forced to view media content (images or videos) before granted access to the network.

Click on **“Add”** button to add media content (images or videos) then specify the **“Force to watch duration”** (in seconds).

Rotation: when there are many media contents, the user can specify the rotation (Random, Regular interval or Regular time), then the preset time can be specified.

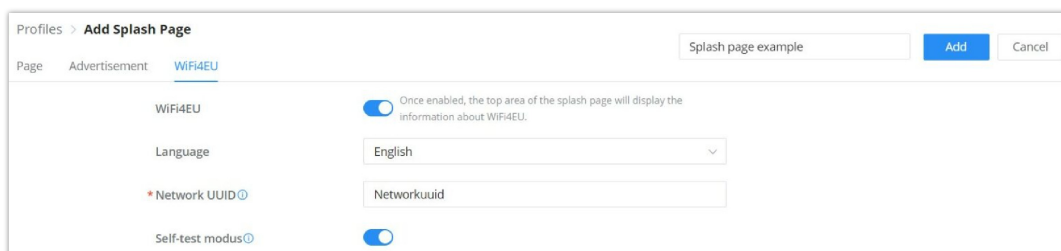


Splash Page – Advertisement

WiFi4EU

Once enabled, the top area of the splash page will display the information about WiFi4EU. The language can be set as well as the Network UUID.

Self-test modus: A WiFi4EU supplier can test if the snippet is correctly installed and if its portal is compliant by enabling the snippet self-test modus.



Splash Page – WiFi4EU

Port profile

Port profiles is a convenient way to provision a GWN device (ex: GWN switches) interfaces easily. Name a profile then select the relevant configurations, like VLAN, Rate, Speed limit, LLDP etc. Also for security we can enable Storm control, Port Isolation, Port Security and 801.1X Authentication.

Note:

A VLAN is also considered as a port profile.

To create a new Port Profile or edit an existing one, please navigate to **Web UI → Settings → Profiles page → Port Profile section.**

Add port profile – General

Add port profile – Security

General	
Profile Name	Specify a name for the profile.
Native VLAN	Select from the drop-down list the native VLAN (Default LAN).
Allowed VLAN	Check the allowed VLANs from the drop-down list (one VLAN or more).
Voice VLAN	Toggle ON or OFF Voice VLAN. <i>Note: Please first enable the Voice VLAN in the Global LAN Settings.</i>
Rate	Specify the rate (port speed) from the drop-down list.
Duplex Mode	Select the duplex mode: <ul style="list-style-type: none"> ● Auto-negotiation: The duplex status of an interface is determined by auto-negotiation between the local port and the peer port. ● Full-duplex: Force full-duplex, and the interface allows sending and receiving data packets at the same time. ● Half duplex: Force half duplex, and the interface only send or receive packets at a time.
Flow Control	When enabled, if congestion occurs on the local device, the device sends a message to the peer device to notify it to stop sending packets temporarily. After receiving the message, the peer device stops sending packets to the local device. <i>Note: When duplex mode is "Half-duplex", the traffic control does not take effect.</i>
Enable Port STP	Toggle ON or OFF the Port STP.

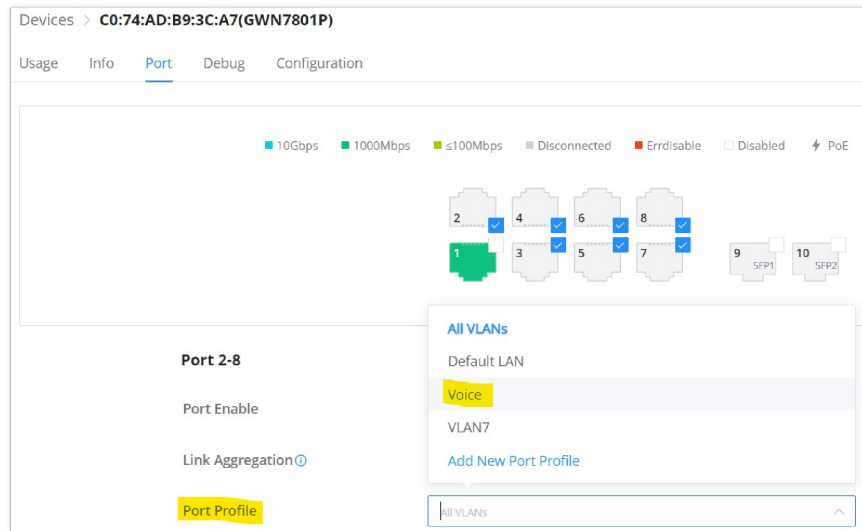
Incoming Speed Limit	Toggle ON or OFF the incoming speed limit.
CIR (Kbps)	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
Outbound Speed Limit	Toggle ON or OFF the outbound speed limit.
CIR (Kbps)	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
LLDP-MED	Toggle ON or OFF the LLDP-MED.
Network Policy TLV	Toggle ON or OFF the network policy TLV.
Security	
Storm Control	Toggle ON or OFF storm control.
Broadcast	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
Unknown Multicast	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
Unknown Unicast	Toggle ON or OFF Unknown Unicast and then specify the control threshold (pps = packet per second).
Port Isolation	Toggle ON or OFF port isolation.
Port Security	Toggle ON or OFF port security. <i>Note: after enabled, start MAC address learning including the dynamic and static MAC addresses.</i>
Maximum number of MACs	Specify the maximum number of MAC addresses allowed. <i>Note: after the maximum number is reached, if a packet with a non-existing source MAC address is received, regardless of whether the destination MAC address exists or not, the switch will consider that there is an attack from an illegal user, and will protect the interface according to the port protection configuration.</i>
Sticky MAC	Toggle ON or OFF Sticky MAC. <i>Note: after enabled, the interface will convert the learned secure dynamic MAC address into Sticky MAC. If the maximum number of MAC addresses has been reached, the MAC addresses in the non-sticky MAC entries learned by the interface will be discarded, and whether to report a Trap alert is determined according to the port protection configuration.</i>
802.1X Authentication	Toggle ON or OFF 802.1x authentication.
User Authentication Mode	Select the user authentication mode from the drop-down list <ul style="list-style-type: none"> ● Mac-based: allows multiple users to authenticate without affecting each other; ● Port-based: allows multiple users to be authenticated. As long as one user passes the authentication, other users are exempt from authentication.
Method	Select the method from the drop-down list.
Guest VLAN	Toggle Guest VLAN ON or OFF. <i>Note: Enable the Guest VLAN in the Global LAN Settings first.</i>
Port Control	Select the port control from the drop-down list: <ul style="list-style-type: none"> ● Disabled ● Mandatory authentication ● Mandatory non-authentication ● Automatic

Re-authentication	Configures whether to enable re-authentication for the device connected to the port.
--------------------------	--

Add port profile

Once the Port profile is added then the user can apply it on a GWN device/device group ports (ex: GWN switches).

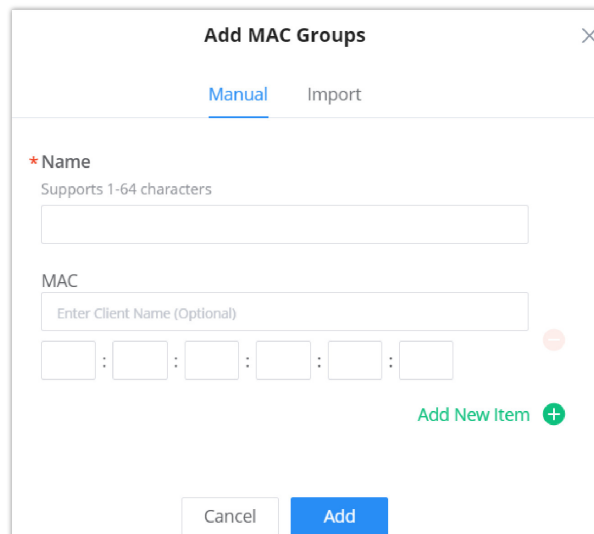
Under **Devices** page, select the relevant device and under **Port tab**, select the ports then apply the Port Profile on these ports. please refer to the figure below:



GWN switch – port

Mac Groups

The user can create a group of MAC addresses to be used on the SSID as a Whitelist or Blacklist for allowing or blocking clients. There is also the option to import a CSV file containing all the MAC addresses.



Add MAC Groups

Note:

The global blacklist blocks only clients connected to the AP with a limit of 256 MAC addresses per list

Bandwidth rules

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

Add Bandwidth Rules

*** Name**
Supports 1-64 characters

Schedule Policy
None

*** Please fill in at least one of the following items**

Upload Limit(Kbps)
A number range of 1-1000000

Download Limit(Kbps)
A number range of 1-1000000

Add Bandwidth rules

Schedule

A schedule can be created here to be applied in many places like rebooting or LED for example.

Profiles > **Create Schedule**

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

*** Name**

Time Zone

Weekly

Unselect All	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
05:00AM - 05:30AM							
05:30AM - 06:00AM							
06:00AM - 06:30AM							
06:30AM - 07:00AM							
07:00AM - 07:30AM							
07:30AM - 08:00AM							
08:00AM - 08:30AM							
08:30AM - 09:00AM							
09:00AM - 09:30AM							
09:30AM - 10:00AM							

Absolute Date/Time (If no time period is selected on the scheduled date, no service on the corresponding date will be executed.)

Create Schedule

RADIUS

This page allow the user to add a RADIUS to be used in Portal policy or Wi-Fi security for example.

Profiles > **Add RADIUS**

* Name 1-64 characters

* Authentication Servers

Server Address	Port	Secret
<input type="text"/> Host name/IP address	1812	<input type="text"/>

RADIUS Accounting Servers

Server Address	Port	Secret
<input type="text"/> Host name/IP address	1813	<input type="text"/>

RADIUS NAS ID 0-48 characters

* Attempt Limit 1-5 numbers

* Radius Retry Timeout (s) 1-120 numbers

* Accounting Update Interval (s) 30-604800 numbers

Dynamic VLAN If enabled, VLAN of the accessing client can be dynamically changed

Add RADIUS

Private Pre-Shared Key (PPSK)

PPSK (Private Pre-Shared Key) is a way of creating Wi-Fi passwords per group of clients instead of using one single password for all clients.

To configure PPSK, **please navigate to Web UI → Settings → Profiles → PPSK**, then click on **“Add”** button to add a new PPSK Group.

Profiles > **Add PPSK Group**

* Name 1-64 characters

PPSK

Add PPSK Group

Give the PPSK Group a name, and after that click on **“Add”** button to add a new PPSK.

Add PPSK

Manual Auto Import

* Number of PPSKs
1-300 numbers

* PPSK Name Prefix 1-60 characters

* Passphrase Length 8-64 numbers

* Max Num of Access Clients 1-100 numbers

Bandwidth Control

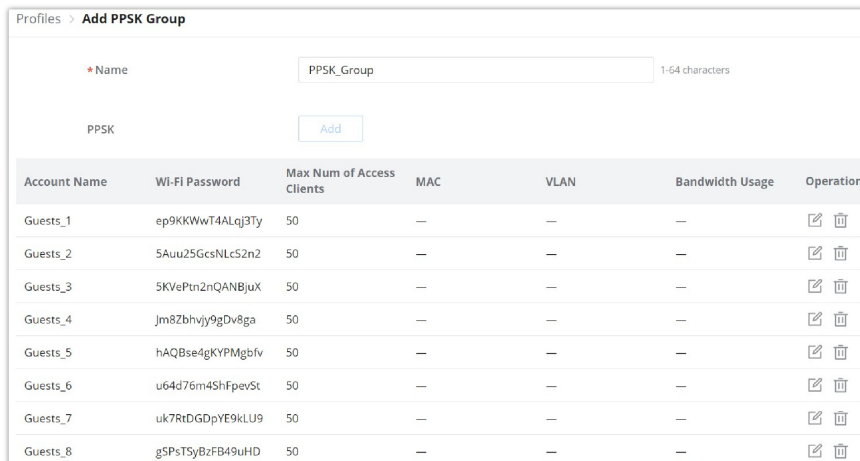
VLAN

PPSK Auto configuration

Note

The maximum number of PPSK per Group is 300.

This is the result of the above configuration. 300 PPSKs have been created with a maximum number of access clients up to 50.

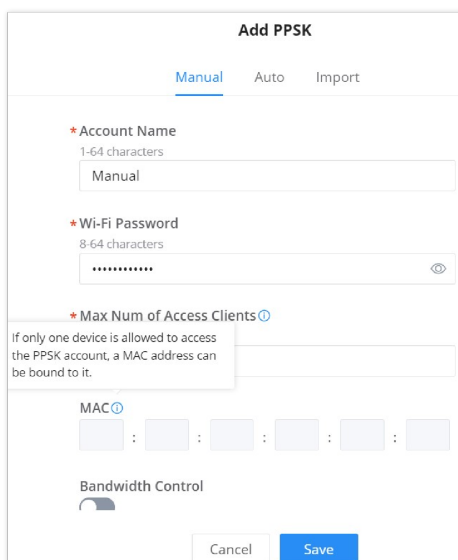


The screenshot shows the 'Add PPSK Group' configuration page. At the top, there is a form with a 'Name' field containing 'PPSK_Group' and a character count of '1-64 characters'. Below this is a 'PPSK' section with an 'Add' button. The main part of the page is a table with the following columns: Account Name, Wi-Fi Password, Max Num of Access Clients, MAC, VLAN, Bandwidth Usage, and Operation. The table contains 8 rows of guest accounts, each with a unique Wi-Fi password and a maximum of 50 access clients.

Account Name	Wi-Fi Password	Max Num of Access Clients	MAC	VLAN	Bandwidth Usage	Operation
Guests_1	ep9KKWwT4ALqj3Ty	50	—	—	—	
Guests_2	5Auu25GcsNLc52n2	50	—	—	—	
Guests_3	5KVePtn2nQANBjuX	50	—	—	—	
Guests_4	Jm8Zbhvjy9gDv8ga	50	—	—	—	
Guests_5	hAQBse4gKYPMgbfv	50	—	—	—	
Guests_6	u64d76m45HfpevSt	50	—	—	—	
Guests_7	uk7RrDGDpYE9kLU9	50	—	—	—	
Guests_8	gSPsTSyBzFB49uHD	50	—	—	—	

Add PPSK – Auto

It's also possible to manually assign a Wi-Fi password for a number of clients.



The screenshot shows the 'Add PPSK' manual configuration page. It has three tabs: 'Manual' (selected), 'Auto', and 'Import'. The form includes the following fields: 'Account Name' (1-64 characters) with the value 'Manual'; 'Wi-Fi Password' (8-64 characters) shown as masked characters; 'Max Num of Access Clients' (with a help icon) and a tooltip that reads 'If only one device is allowed to access the PPSK account, a MAC address can be bound to it.'; 'MAC' field with a help icon and a placeholder for a MAC address in the format 'XX:XX:XX:XX:XX:XX'; and a 'Bandwidth Control' section with a slider icon. At the bottom, there are 'Cancel' and 'Save' buttons.

PPSK – Manual

If only one device is allowed to access the PPSK account, a MAC address can be bound to it.

Another way is to upload a CSV file, please download the reference template.



PPSK Import CSV file

Now, the user can apply this PPSK group to any SSID, refer to the figure below:



PPSK group – Access Security

Certificates

In this section, the user can create CA, Client and Server certificates that can be used with OpenVPN either for client or server side.

The user can either click on "Add" button to add a new certificate or click on "Import" button to import them from his local machine to the GWN.Cloud or GWN Manager.



Profiles – Certificates

This page will be shown after clicking on add button, then the user can select between a CA Certificate or a Certificate which can be either for a Server or a Client based on the option "Certificate Type". Please refer to the figures and tables below:

Profiles > **Add Certificate**

Type CA Certificate Certificate

* Name

Key Length

Digest Algorithm

* Expiration (D)

SAN None IP Address Domain

Country/Region

* State/Province

* City

* Organization

* Organizational Unit

* Email

Profiles – Add CA Certificate

Type	Select the type of certificate either CA Certificate or Certificate.
Name	Enter the certificate's name.
Key Length	<p>Choose the key length for generating the CA certificate. The following values are available:</p> <ul style="list-style-type: none"> ● 2048: 2048-bit keys are a good minimum. (Recommended). ● 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.

Digest Algorithm	Select the digest algorithm. <ul style="list-style-type: none"> ● SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. Note: Hash is a one-way function, it cannot be decrypted back.
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country/Region	Select a country from the dropdown list of countries. Example: "United States of America".
State/Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Profiles – Add CA Certificate

Profiles – Add Certificate (Client or Server)

Type	Select the type of certificate either CA Certificate or Certificate .
Name	Enter the certificate's name.
CA Certificate	Select from the drop-down list the CA Certificate previously created.
Certificate Type	Select the certificate type either a server or a client certificate.
Key Length	Choose the key length for generating the CA certificate. The following values are available: <ul style="list-style-type: none"> ● 2048: 2048-bit keys are a good minimum. (Recommended).

	<ul style="list-style-type: none"> ● 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	<p>Select the digest algorithm.</p> <ul style="list-style-type: none"> ● SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. <p>Note: Hash is a one-way function, it cannot be decrypted back.</p>
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country/Region	Select a country from the dropdown list of countries. Example: "United States of America".
State/Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Profiles – Add Certificate (Client or Server)

Client Time Policy

The administrator can configure a Time policy which will dictate for how much a client connect to the Wi-Fi if this policy is applied for the SSID.

Add Time Policy

Enable Time Policy	Check/Uncheck to Enable/Disable Policy
Name	Enter a name to identify the Policy. Supports 1 to 64 characters, including numbers, letters and special characters.
Validity Time	Configure the policy duration from 1 minutes to 365 days.
Reset Cycle	Set up a Reset mode: Daily, Weekly or Periodically
Reset Time	When Reset Cycle is Daily: configure the time of the day When Reset Cycle is Weekly: configure the time and the day of the week When Reset Cycle is Periodically: configure the period (d//h/m)

Time Zone	Detected Automatically.This parameter can be changed under System Settings
------------------	--

Add Time Policy

Hotspot 2.0

Hotspot 2.0, also known as HS2.0 or Passpoint, is a set of industry specifications developed by the Wi-Fi Alliance to improve the connectivity and user experience of Wi-Fi networks, particularly in public places. The goal of Hotspot 2.0 is to make Wi-Fi connectivity as seamless and secure as cellular networks.

Key features of Hotspot 2.0 include

- 1. Automatic Authentication:** Hotspot 2.0 enables automatic and secure connection to Wi-Fi networks without user intervention. Devices can automatically connect to Wi-Fi hotspots, similar to how cellular networks work.
- 2. Seamless Roaming:** With Hotspot 2.0, users can roam between different Wi-Fi networks without having to re-authenticate. This is especially useful in environments with multiple Wi-Fi access points, such as airports, shopping malls and other public spaces.
- 3. Passpoint:** Passpoint is a specific implementation of Hotspot 2.0 that allows mobile devices to automatically discover and connect to Wi-Fi networks that are part of the Passpoint ecosystem. Passpoint provides a streamlined and secure connection process, making it easier for users to connect to Wi-Fi hotspots.

Hotspot 2.0 is particularly relevant in environments where reliable and secure Wi-Fi connectivity is essential, such as airports, hotels and other public spaces. It improves the overall user experience by making Wi-Fi connectivity more like cellular connectivity, with automatic authentication and seamless roaming.

Add Hotspot 2.0

SYSTEM

General

Navigate to **Web UI** → **Settings** → **System** → **under General** to configure General settings like Country/Region, Time zone, Time, LED, Reboot Schedule etc.

System

General ^

Country/Region

Timezone

Auto Sync Time

* AP Login Password

Device Password

LED

Reboot Schedule

Enable Client Connection Event

Presence API

Automatically add to SSIDs

System page – General

Country/Region	Select the country or region from the drop-down list. This can affect the number of channels depending on the country standards.
Timezone	Configure time zone for GWN APs. Please reboot the device to take effect.
Auto Sync Time	If enabled, all managed devices' system times will be synced with GWN Cloud
AP Login Password	Sets the APs login password with up to 8 characters. Alphanumeric characters and special characters - _ are supported
Device Password	Set the devices SSH remote login password other than APs (Routers and Switches), which is also the device web login password.
LED	Select whether to always turn ON or OFF the LEDs on the APs or apply a schedule for this function.
Reboot Schedule	Once scheduled, the current network will not work for a while during the scheduled period.
Enable Client Connection Event	When enabled, then Client connects/disconnects events are listed under Devices → GWN device → Info page.
Presence API	Once enabled, will detect and collect wireless device info. near the AP, which can be used for device positioning, pedestrian flow monitoring and so on.
Automatically add to SSIDs	GWN devices will be added to SSID automatically

System page – General

URL Access Log

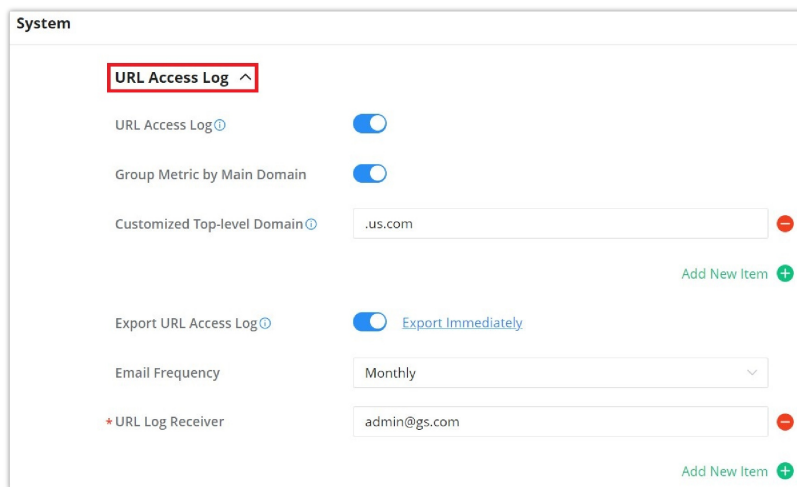
Administrators can easily configure the platform to record, monitor and maintain a log of all the websites visited by the clients connected to the paired GWN devices.

The platform System will send these logs via Email to the configured Log Receiver in a form of downloadable link providing a CSV file format containing all the websites logs visited for each client during the defined period (daily, weekly or monthly basis).

In order to enable this feature, follow below steps:

1. Go under "**Settings** → **System page** → **URL Access Log section**" and enable URL Access Log field, this will configure the GWN Manager System to start recording the websites logs visited by the clients.

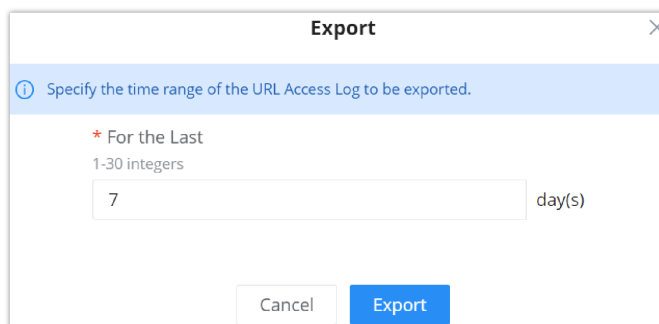
- The option “**Group Metric by Main Domain**” can be also enabled then the user can configures the top domains to be merged. This will merge the page views for the configured domains. The regular top domains will automatically merge without any configuration (such as .com).
- Enable Export URL Access Log.
- Administrators can choose to set the Email Frequency to be generated either on a daily, weekly or monthly basis.
- Configure the URL Log Receiver Email.



URL Access Log

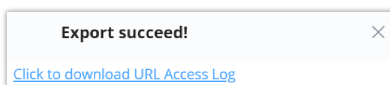
In this example, the administrator will start receiving, on a weekly basis, an Email containing a downloadable link providing a CSV file containing the websites visited by the clients during the last day.

Users can click on “**Export Immediately**”, and then specify the time range of the URL Access Log during the last (1 – 30) days to be exported immediately.



Export Immediately

- Click on “**Export**” button and notice the success confirmation message:



Export Succeed

- Click the highlighted link to Download the log file and save it locally.

Once downloaded, administrators will have a CSV file tracking the Internet activity for all the clients connected to the paired GWN devices.

The CSV file will contain columns displaying the AP MAC address, client’s hostname as well the device MAC address, the Source and Destination IP, the URL logs, the HTTP Method (GET/POST) and the time of request.

	A	B	C	D	E	F	G	H
1	AP MAC	MAC	Hostname	User / Source IP	Destination IP	URL	HTTP Method	
2			iPhone XS	192.168.5.133	17.253.113.204	http://captive.apple.com/GET		
3			Huawei Mate 20	192.168.5.133	17.167.192.94	https://gsp85-ssl.ls.apple.c		
4			Samsung Galaxy S10	192.168.5.133	81.192.28.179	http://netcts.cdn-apple.co GET		
5			OnePlus 7 Pro	192.168.5.133	17.134.127.250	https://gs-loc.apple.com		
6			Moto G7 Power	192.168.5.133	17.57.12.11	https://gsp64-ssl.ls.apple.c		
7			iPhone 11 Pro Max	192.168.5.133	173.194.76.101	https://s.youtube.com		
8			Google Pixel 4 XL	192.168.5.133	74.125.193.119	https://i.ytimg.com		
9			BlackBerry Key2 LE	192.168.5.133	172.217.18.42	https://youtubei.googleapp		
10				192.168.5.133	17.125.249.8	https://p71-buy.itunes.app		

URL Access Log- CSV file example

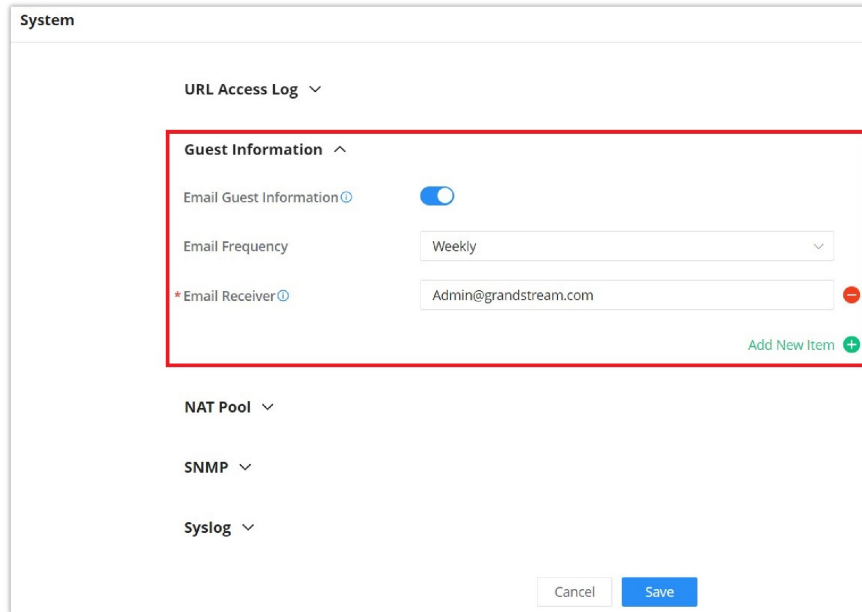
Note:

The Platform Database will keep storage of reports for 30 days, after that, they will be automatically erased from the system

Guest Information

If enabled, the cloud server will periodically send out the log download link based on the configured email settings. In order to enable this feature, follow below steps:

1. Go under “**Settings** → **System page** → **Guest Information section**” and enable Guest Information field.
2. Choose to set the Email Frequency to be generated either on a daily, weekly or monthly basis.
3. Configure the Email Receiver.



The screenshot shows the 'System' settings page. The 'Guest Information' section is highlighted with a red border. It contains the following fields:

- URL Access Log** (dropdown menu)
- Guest Information** (dropdown menu)
- Email Guest Information** (toggle switch, currently turned on)
- Email Frequency** (dropdown menu, set to 'Weekly')
- *Email Receiver** (text input field, set to 'Admin@grandstream.com')
- Add New Item** (green plus icon)

Below the Guest Information section, there are other sections: **NAT Pool**, **SNMP**, and **Syslog**, each with a dropdown arrow. At the bottom of the page, there are 'Cancel' and 'Save' buttons.

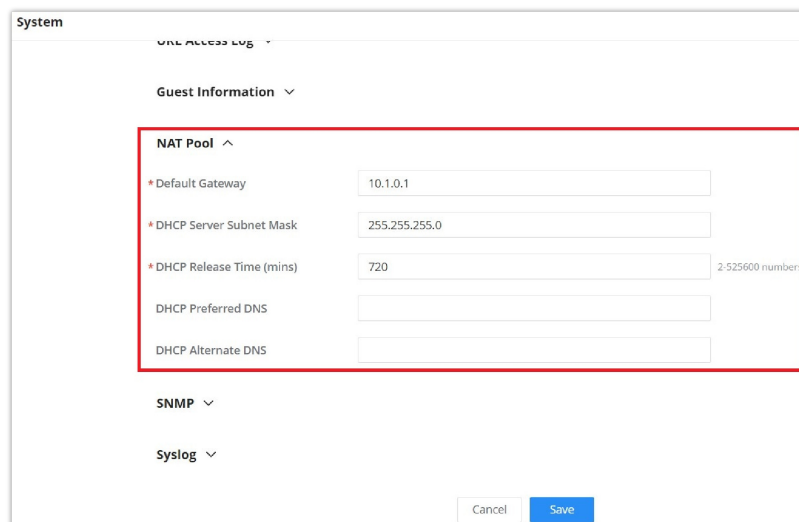
Guest Information

NAT pool

Users can use this feature in order to set an address Pool from which the clients that are connected to the adopted/paired devices will acquire their IP address in that way GWN devices will act as a light weight router.

Note:

This option cannot be enabled when Client Assignment IP is set to Bridge mode.



The screenshot shows the 'System' settings page. The 'NAT Pool' section is highlighted with a red border. It contains the following fields:

- URL Access Log** (dropdown menu)
- Guest Information** (dropdown menu)
- NAT Pool** (dropdown menu)
- *Default Gateway** (text input field, set to '10.1.0.1')
- *DHCP Server Subnet Mask** (text input field, set to '255.255.255.0')
- *DHCP Release Time (mins)** (text input field, set to '720', with a note '2-525600 numbers' to the right)
- DHCP Preferred DNS** (text input field)
- DHCP Alternate DNS** (text input field)

Below the NAT Pool section, there are other sections: **SNMP** and **Syslog**, each with a dropdown arrow. At the bottom of the page, there are 'Cancel' and 'Save' buttons.

NAT Pool

Navigate to **Web UI** → **Settings** → **System page (NAT Pool section)**, in order to configure the Gateway, DHCP Server Subnet Mask, DHCP Lease Time and DHCP Preferred/Alternate DNS.

SNMP

This section lists the SNMPv1, SNMPv2c, and SNMPv3 options available to integrate the adopted/paired GWN devices with enterprise monitoring systems.

Users can enable SNMP feature under **Web UI** → **Settings** → **System page (SNMP section)**.

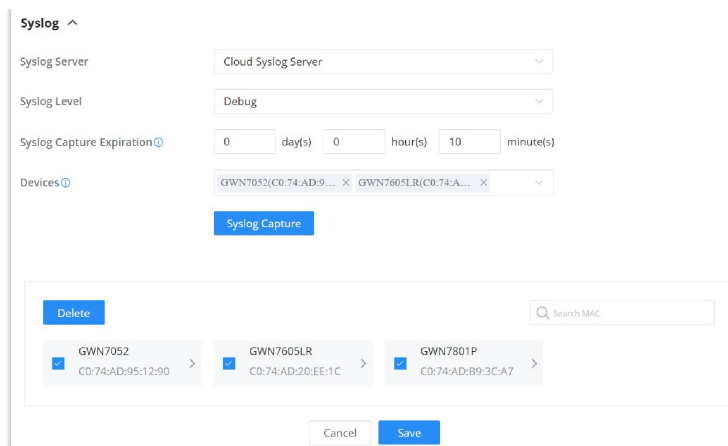
SNMP

SNMPv1, SNMPv2c	Enable Enable SNMPv1/SNMPv2c.
Community String	Enter the SNMP Community string.
SNMPv3	Enable SNMPv3. <i>Note: If the SNMPv3 function of the switch is required to work, SNMPv1 and SNMPv2c should be enabled at the same time.</i>
Username	Enter the SNMPv3 username.
Authentication Mode	Set the Authentication mode to: either MD5 or SHA.
Authentication password	Enter the SNMPv3 authentication password.
Privacy Mode	Set the Privacy mode to: either AES128 or DES. <i>Note: AES128 mode is only for routers and APs. Switches use DES mode.</i>
Privacy password	Enter the privacy password.

SNMP

Syslog

Configure Syslog settings in order to have GWN devices sending log messages to your debugging syslog server. There are two options, either to use the built-in GWN.Cloud syslog server or a Local syslog server and in this case the user will have to enter the local syslog server address.



Syslog

Syslog Server	Select the syslog server from the list: <ul style="list-style-type: none"> • Cloud Syslog Server • Local Syslog Server
Local Syslog Server Address	Enter the IP address or URL of the syslog server.
Syslog Level	Select the level of Syslog, 8 levels are available: None, Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug
Protocol	Sets the protocol used by the system log server. Default port for both UDP and TCP is 514.
Devices	Select the devices to capture syslogs from

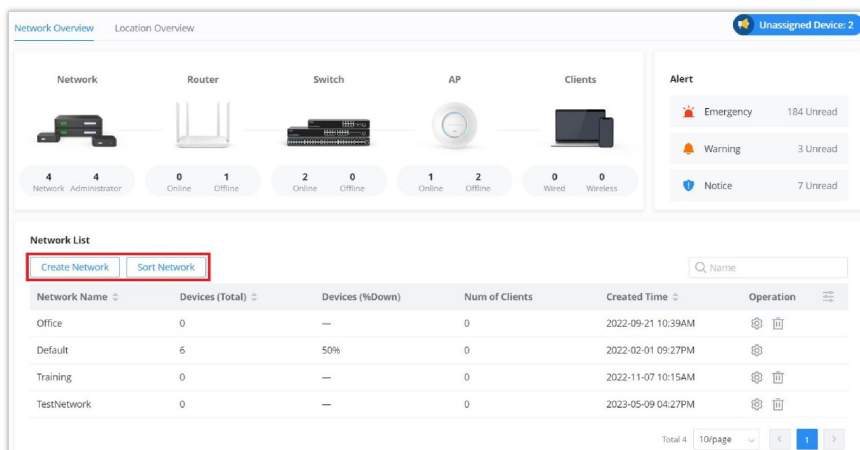
Syslog

ORGANIZATION

Overview

Network Overview

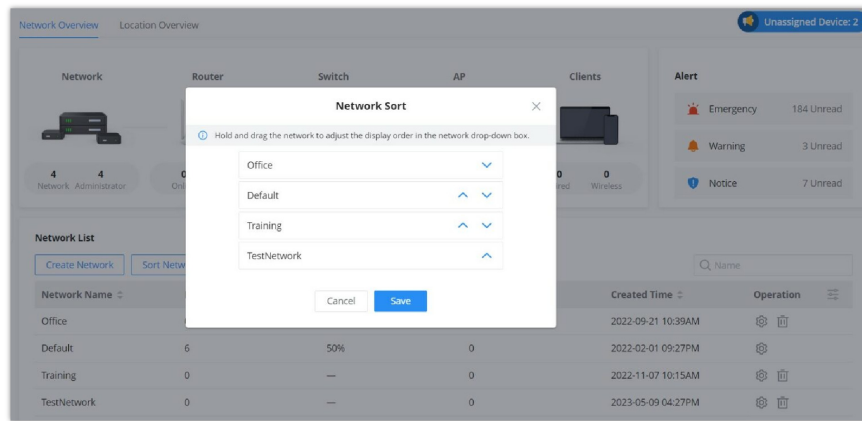
The overview page offers a bird eye look at all the GWN devices which have been added to the organization. This includes GWN routers, GWN switches, GWN APs, and clients. In addition to that, the user can see the number of networks created that organization and the number of the administrators in the organization.



Organization – Overview

- o Click on **“Create Network”** button to create a [new network](#).

- Click on **"Sort Network"** button to sort network order, the first one on the list will be the primary network (the network that will be selected after a login).

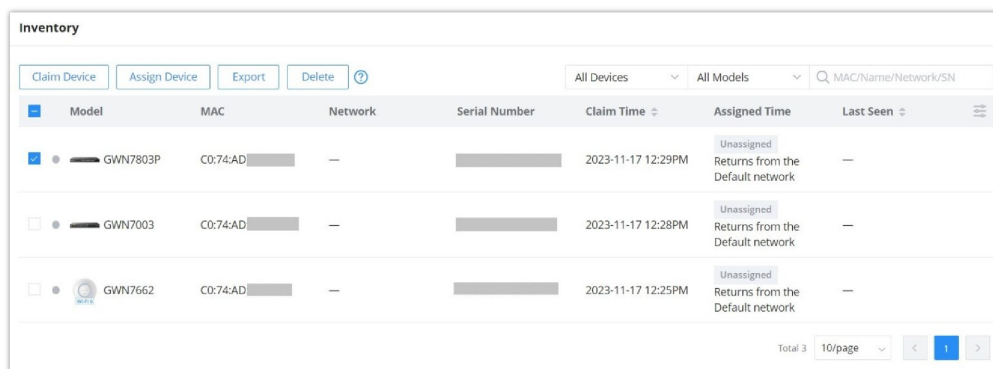


Organization – Overview – Sort network

Inventory

Inventory page lists all the GWN devices in all networks, including online and offline ones. Click on a device to be redirected to the Devices page for more options.

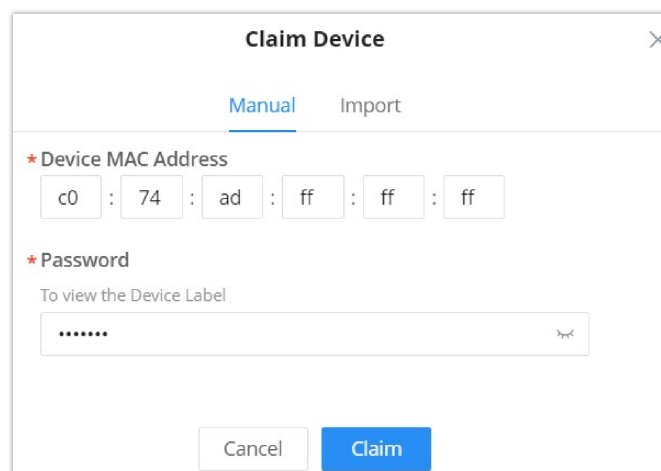
On this page, the user can see each GWN device related information: model, MAC address, network, serial number, claim time, assigned time (and which network it has been returned from) and last seen.



Inventory page

The user can click on **"Export"** button to export a CSV file containing all the GWN devices.

- **Claim Device:** to claim a device (GWN device MAC address and Password is required) even if the GWN device is offline, and it will not be assigned to any network.



Inventory – Claim Device

- **Assign Device:** to assign the device to network (it will added to the selected network).

Assign Device ✕

*** Network**

Office ▼

Device Group

Default ▼

Selected Devices

Enter the device name. Supports up to 64 characters

C0:74:AD:CC:D9:EC GWN7661

Cancel

Assign

Inventory – Assign Device

- **Export:** to export a CSV file containing all the GWN devices.

A1	Model	Mac	Network	Serial Number	Claimed Time	Assigned Time	Last Seen
1	GWN7661	C0:74:AD: [REDACTED]	—	[REDACTED]	2023-10-27 04:11PM	Unassigned	—
2	GWN7624	C0:74:AD: [REDACTED]	—	[REDACTED]	2023-10-27 02:38PM	Unassigned	2023-10-27 04:09PM
3	GWN7813P	C0:74:AD: [REDACTED]	Default	[REDACTED]	2023-10-27 02:16PM	2023-10-27 02:16PM	2023-10-27 03:59PM

Inventory – Export

- **Delete:** to delete a device from GWN management platform.

Upgrade

This feature allows upgrading GWN devices. Under **“Upgrade”** menu allows administrator to manage GWN devices firmware, trigger immediate upgrade or Upgrade reminder. There is also the option for Upgrade History on the second tab.

Upgrade

Devices Upgrade Upgrade History

Firmware
Upgrade
Upgrade Reminder
All Networks ▼
All Models ▼
All Devices ▼
Q Model/MAC/Firmware Versi

☐	Device Model	MAC	Network Name	Firmware	Recommended Version	Scheduling
☐	GWN7624	C0:74:AD:90:B2:40 GWN7624	Default Network	1.0.25.10	1.0.25.7	No
☐	GWN7002	C0:74:AD:BF:AF:50	Default Network	1.0.4.6	1.0.3.5	No
☐	GWN7052F	C0:74:AD:B9:F1:9C	GS Network	1.0.9.2	1.0.7.2	No
☐	GWN7813P	C0:74:AD:DF:CC:94	Default Network	1.0.1.8	1.0.1.8	No

Total 4 10/page < 1 >

Upgrade

Select the devices you wish to upgrade then click “Upgrade”.

Devices Upgrade > **Upgrade**

Firmware Server Cloud Local (HTTP/HTTPS)

Firmware Version Latest Recommended Version ▼

Upgrade Time Upgrade Now Upgrade Later
 Upgrade Regularly

Remark Upgrade Add a comment about the upgrade

Cancel

OK

Upgrade in Batches

Upgrade History

On the upgrade history tab, the user can see the upgrade history of all GWN devices with details information like (device model, firmware version, upgrade status, etc), it's also possible to search for a device using its MAC address.

Schedule ID	Device Type	Device Model	Device Number	Target Version	Upgrade Status	Administrator	Scheduled Time	Remark	Operation
1	AP	GWN7660	1	1.0.25.10	Successful	admin@grandstream.com	2023-11-16 04:32PM	Upgrade	

Upgrade History

Report

Administrators can generate and configure the platform to send reports periodically to the configured email addresses. Each report can be related to one or more different Network groups, providing Wi-Fi statistics (clients count, bandwidth usage, client and guest statistics...etc.)

Title	Scheduled Time	Creator	Report Frequency	Operation
Custom Report	2022-12-16 04:00PM	jawad@grandstream.com	Daily	
Daily	2022-12-20 03:32PM	jawad@grandstream.com	Daily	

Report

To generate the report, click on **“Create a Report”** button, a new page displaying the report details will be displayed.

Create a report

The following table provides an explanation about different options for report settings:

Field	Description
Title	Specify the report title. The maximum length is 64 alphabet characters.

Network	Specify the Network Group to be included in the generated report. Note: Maximum network groups that can be selected is 100.
Report Contents	Specify the report contents for the <i>selected network group(s)</i> , the contents can include: <ul style="list-style-type: none"> • Clients Count: reports the number of clients for all the SSIDs under selected network group. • Bandwidth Usage: The download and upload level statistics for all the SSIDs for the selected network group • Clients Statistics: reports the statistics for the different client manufacturer, client OS, the number for new clients as well as the return clients and the average duration. • Guest Statistics: reports statistics about the clients connected via Captive portal including the Guest New session, the Max concurrent New session, the login failure. • Top Devices: reports the top 5/20/50 devices that consumed the max of the bandwidth/data. • Top Clients: Lists the top 5/20/50 clients that downloaded/uploaded the max of data • Top SSIDs: reports the top 5/20/50 SSIDs that are mostly used by clients. • Top Websites: reports the top 5/20/50 websites that are mostly visited by clients.
Report Frequency	Specify the report frequency to be generated either on daily basis, weekly, monthly or custom range.
Date	Specify the Start and Date for the report to be generated when selecting "Custom Range" as Report Frequency .
Report Generate Time	Select either to generate the report now, or at later time
Time	Specify when you want the report to be generated. This field appear when selecting "Later" in "Report Generate Time".
Email Address	Enter the mail address(es) to which the report will be sent.

Create a report

Organization Change Log

Time	Administrator	IP Address	Network	Details	Operation
2023-05-19 06:51PM	[REDACTED]	[REDACTED]	Default Network	Added Devices (C0:74:AD:01:9...	⋮
2023-05-19 04:40PM	[REDACTED]	[REDACTED]	Organization A	Added Network (Organization ...	⋮
2023-05-19 03:23PM	[REDACTED]	[REDACTED]	Default Network	Enable API that restrict specifi...	⋮
2023-05-19 03:22PM	[REDACTED]	[REDACTED]	Default Network	Enabled API Developer	⋮
2023-05-19 02:39PM	[REDACTED]	[REDACTED]	Default Network	Added new RADIUS (Radius Se...	⋮
2023-05-19 11:51AM	[REDACTED]	[REDACTED]	Default Network	Added LAN (VLAN7)	⋮
2023-05-19 09:38AM	[REDACTED]	[REDACTED]	Default Network	Added Devices (C0:74:AD:BA:2...	⋮

Change Log

To see more details, click on the three dots.

API developer

Third-party applications can use API developer mode to enable even more features.

API Developer

Enterprises can enable API Developer Mode to invoke various GWN features via API in third-party applications. [View More Details](#) →

API Developer Info

APP ID: 100851

Secret Key: Vxw [REDACTED] [Reset](#)

Restrict APIs to specific networks

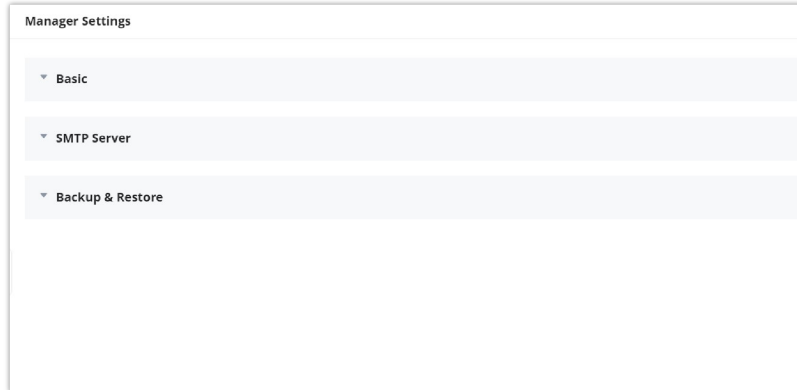
[Disable API Developer Mode](#)

For further details, please refer to the [GWN API Developer Guide](#)

MANAGER SETTINGS

Note:

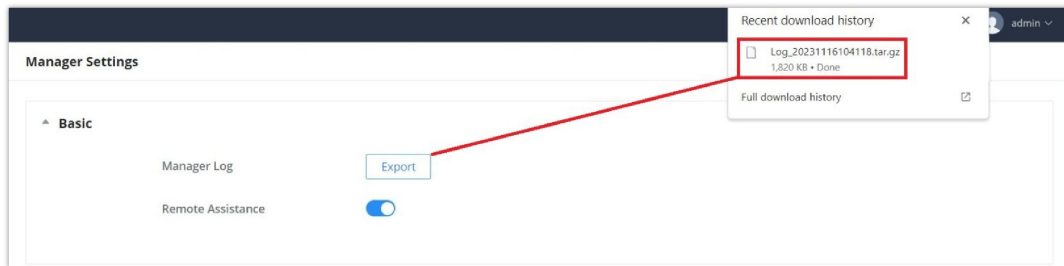
Manager Settings is only available for GWN Manager.



Manager Settings page

Basic

On this section, the user can download the Manager log files by clicking on “**Export**” button as shown below, as well as enabling “**Remote Assistance**” in case the users need a professional help from experts or support.



Manager Settings – Basic

SMTP Server

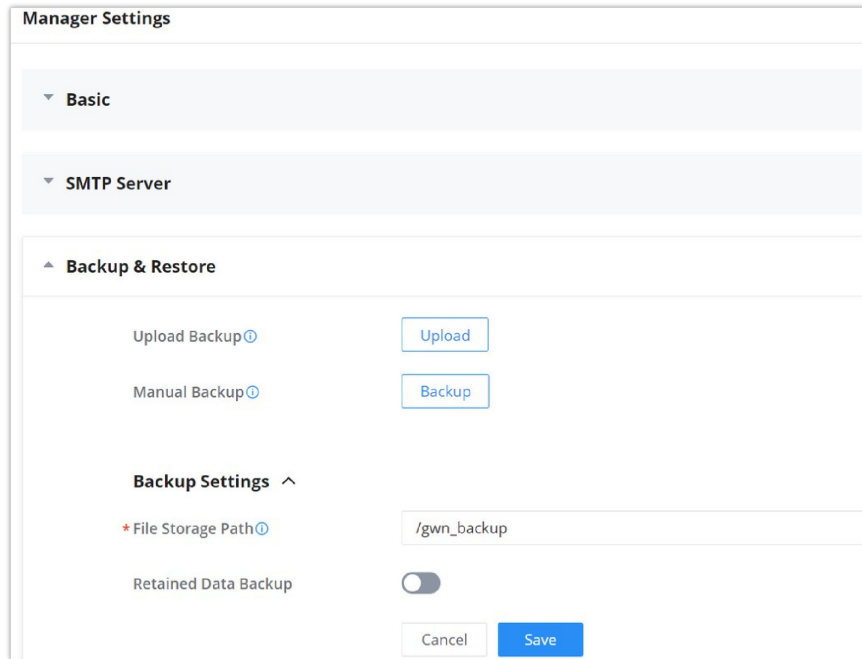
To enable email notifications from GWN Manager, the user needs first to setup SMTP Server here, once the SMTP Server configuration is set, please click on “**Send test email**” button to test if it’s working or not.

 A screenshot of the 'SMTP Server' configuration form. It has a white background and a dark blue header. The form contains several input fields: 'From Email Address', 'From Name' (with a character count '1 to 64 characters'), 'SMTP Username', 'SMTP Password', '* SMTP Host', and '* SMTP Port'. Below the input fields are three buttons: 'Send test email', 'Cancel', and 'Save'.

Manager Settings – SMTP Server

Backup & Restore

Users can Backup GWN Manager configuration as shown below:



The screenshot shows the 'Manager Settings' interface with the 'Backup & Restore' section expanded. It includes buttons for 'Upload Backup' and 'Manual Backup', a 'Backup Settings' section with a 'File Storage Path' field containing '/gwn_backup', and a 'Retained Data Backup' toggle switch. 'Cancel' and 'Save' buttons are at the bottom.

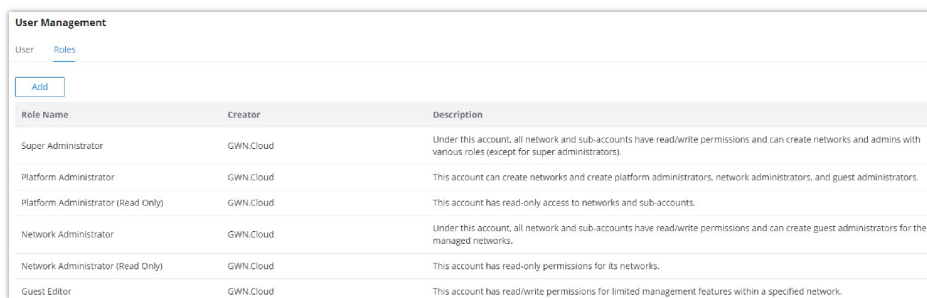
Backup and Restore

Users can either click **“Upload”** button to import backup from the local directory. Or, click **“Backup”** button to backup immediately.

USER MANAGEMENT

User Management allows the administrator to create multiple accounts for different users to login to the platform. There are 5 different access levels to monitor and manage GWN devices:

- Super Administrator
- Platform Administrator
- Platform Administrator (Read Only)
- Network Administrator
- Network Administrator (Read Only)
- Guest Editor



Role Name	Creator	Description
Super Administrator	GWN.Cloud	Under this account, all network and sub-accounts have read/write permissions and can create networks and admins with various roles (except for super administrators).
Platform Administrator	GWN.Cloud	This account can create networks and create platform administrators, network administrators, and guest administrators.
Platform Administrator (Read Only)	GWN.Cloud	This account has read-only access to networks and sub-accounts.
Network Administrator	GWN.Cloud	Under this account, all network and sub-accounts have read/write permissions and can create guest administrators for their managed networks.
Network Administrator (Read Only)	GWN.Cloud	This account has read-only permissions for its networks.
Guest Editor	GWN.Cloud	This account has read/write permissions for limited management features within a specified network.

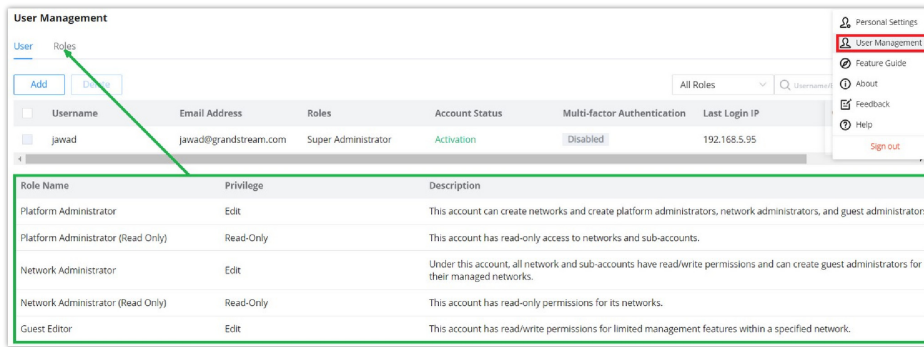
User Management

Note:

The Super administrator is an admin with top authority, using this privilege users can create/delete accounts with any privilege level. Each account has a unique Super Administrator which is created automatically when signing in.

Add New Users

To list all the users managing an account, Click on **username** from the top right corner → **User Management**, refer to the figure below:



User Management page

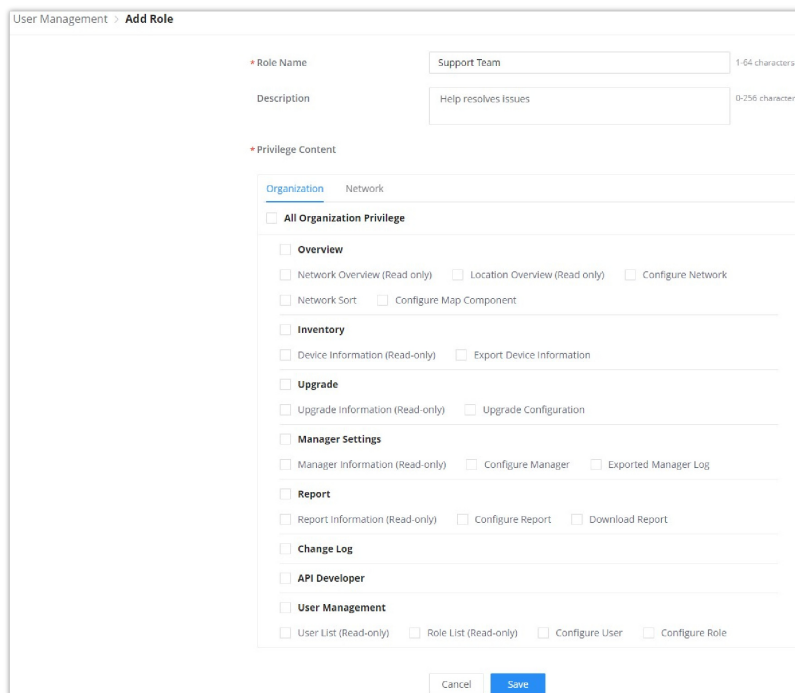
To add a new user, click on "Add" button then enter the email address and select the privilege to assign to the new user.

Note:

When selecting privilege "Network Administrator" or "Guest Editor", the networks that will be monitored by this user should be selected, the new user will have access to those networks only.

Add New Role

In addition to the roles predefined, the user can add a custom role and choose which privileges to assign to the role. To add a new role, please click on your account name on the top right corner of the web UI, then select "User Management, after that click on "Role" tab then click on "Add".



Add Role – Organization Privileges

*Privilege Content

Organization [Network](#)

All Network Privilege

Dashboard

Devices

Device Information (Read-only) Adopt Device Export Device Information

More Buttons Device Configuration Clear Traffic Auto Configuration Delivery

Bridge device Locate device Debug device PoE Port Configuration

Port Configuration Group Management

Clients

Client Information (Read-only) Export Client Information Client Configuration

Subscribe to Client Historical Data Clear Traffic

Guests - Online Status

Guest Information (Read-only) Export Guest Information Remove Guests

Guests - Voucher

Voucher Information (Read-only) Configure Voucher Group Voucher Settings

Download Voucher Group Print Voucher

Map & Floor Plans

Map Information (Read-only) Place Buildings/Devices Configure Floor Plan

Network Privileges 1

Insight - Site Survey

Insight - Network Topology

Topology Information (Read-only) Configure Mesh

Alerts

Alert Information (Read-only) Delete Delete All Mark All as Read

Alert Settings Alert Notification Settings

Settings - Wi-Fi

Wireless LAN (Read-only) Global Radio Settings (Read-only) Mesh (Read-only)

Configure Wireless LAN Configure Global Radio Settings Configure Mesh

Settings - LAN

LAN (Read-only) Global Switch Settings (Read-only) Configure LAN

Configure Global Switch Settings

Settings - Internet

WAN (Read-only) Internet Source (Read-only) Configure WAN

Configure Internet Source

Settings - VPN

PPTP (Read Only) IPSec (Read Only) OpenVPN® (Read Only)

Wireguard® (Read Only) VPN User (Read Only) Configure PPTP Client/Server

Configure IPSec (Site-to-Site) Configure OpenVPN® Client/Server

Configure Wireguard® Configure VPN User

Network Privilege 2

Settings - Firewall & Security

Port Forward (Read-only) Wired Firewall (Read-only) Wireless Firewall (Read-only)

Rogue Ap (Read-only) Advanced Security Settings (Read-only) Configure Port Forward

Configure Wired Firewall Configure Wireless Firewall Configure Rogue Ap

Configure Advanced Security Settings

Settings - Profiles

Portal Policy (Read-only) Splash Page (Read-only) Port Profile (Read-only)

MAC Group (Read-only) Bandwidth Rules (Read-only) Schedule (Read-only)

RADIUS (Read-only) PPSK (Read-only) Client Time Policy (Read-only)

Hotspot 2.0 (Read-only) Configure Portal Policy Configure Splash Page

Configure Port Profile Configure MAC Group Configure Bandwidth Rules

Configure Schedule Configure RADIUS Configure PPSK

Configure Client Time Policy Configure Hotspot 2.0

Settings - System

System Information (Read-only) Configure System Export URL Access Log

Network Privilege 3

Then create a new user account and assign the new role to it.

Add User ✕

*** Email Address**
Supports 1-64 characters

*** Role** ⓘ

*** Network**

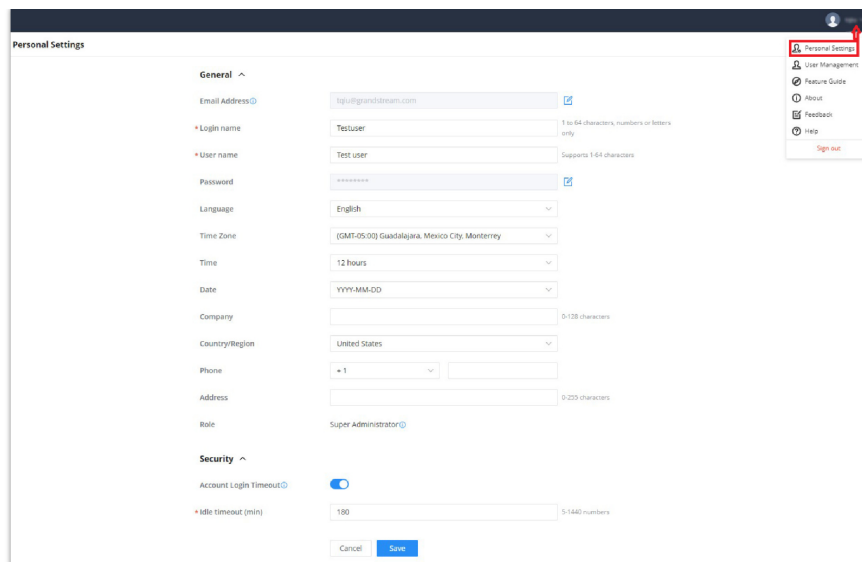
Assign The New Role

Note:

Custom role users can also login to GWN APP.

Personal Settings

To edit an account, click on its name from the top right corner → Click on **Personal Settings** a new page displaying the account details will be displayed.



Personal Settings

General	
Email Address	The email address of the Initial Administrator. Click on change to change this email address
Login name	Username used for login authentication
User name	This is the name that will be displayed on the top right corner of the web page when login as super administrator
Password	Password used for login authentication
Language	Select the language from the drop-down list.
Time Zone	Select the time zone from the drop-down list
Time	Select from the drop-down list 12 hour or 24 hour format
Date	Select from the drop-down list the date format
Company	Enter the company name
Country/Region	Select the country/region from the list
Phone	Enter the phone number
Address	Enter the address
Role	Displays the role of the current user. <i>Note: in the case of Initial Administrator, Read and write permissions on all networks and accounts</i>
Security	
Account Login Timeout	Once enabled,the administrators will be logged out automatically after being idle for the specified time period or being exceeded the maximum login time.
Idle timeout (min)	Specify the idle timeout, please enter an integer from 5 to 1440.
Maximum Login Duration(min)	Specify the maximum login duration in minutes from 5 to 720.

Synchronize Maximum Login Duration for Sub-Administrators	Once enabled, the sub-administrators idle timeout and maximum login duration will be the same as the super administrator and cannot be modified
Password Security	Toggle ON or OFF password security.
Password Expiration (days)	Specify the password expiration in (days). valid range from 30 to 180.
Mandatory Password History (pcs)	New password cannot be the same as the last N passwords used. N: valid range from 1 to 20.
Multi-Factor Safety Authentication	Toggle ON to enable Mutli-Factor Safety Authentication.

Personal Settings

EXPERIENCING GWN MANAGEMENT PLATFORMS

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

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

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

Thank you again for using Grandstream GWN Management Platforms, it will be sure to bring convenience to both your business and personal life.

CHANGE LOG

This section documents significant changes from previous versions of the GWN Management Platform User Manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Version 1.1.26.11

Product Name: GWN.Cloud and GWN Manager

- Added Pre-Provisioning for Switch in device management for port Setting, port profile, and DHCP Snooping. [[Switch Pre-Provisioning](#)]
- Added remarks and serial number fields for device export. [[Devices](#)]
- Added more default Wall Types and optimized attenuation values for Floor Plans. [[Floor Plans](#)]
- Added support for topology export. [[Network Topology](#)]
- Added MAC search field in Upgrade History. [[Upgrade History](#)]
- Added a column to display the network that the device was returned from. [[Inventory](#)]
- Added support for custom role users to login to GWN APP. [[User Management](#)]
- Increased Password Security, added password expiration and conflict limits configuration. [[Personal Settings](#)]
- Added support hiding Weak Heat Map signal. [[Floor Plans](#)]
- Removed SMTP Username/Password requirement. [[SMTP Server](#)]

Version 1.1.25.23

Product Name: GWN.Cloud and GWN Manager

- Added features of multiple VPN tunneling methods such as PPTP, IPSec, OpenVPN®, and WireGuard®, and IPSec supports automatic networking mode. [[VPN](#)]
- Added the feature of managing multiple routers at the same time on the same network. [[Devices](#)]

- Added device group management, pre-set features for switches in the group. And a new way to select device group in the multiple business. [[Group management](#)]
- Added the feature of pushing cloud configuration to the local side of the device, and the push method includes manual and automatic. [[Devices](#)]
- Added a new feature for network speed test of APs. [[configure a GWN Access Point](#)]
- Added a new feature for 12-hour network health monitoring of WAN ports. [[WAN](#)]
- Added a new feature of policy routes. [[Policy routes](#)]
- Added a new feature of certificate management. [[Certificate](#)]
- Added floor plan management features, support device RF heat map preview, convenient device placement planning. [[Floor plans](#)]
- Added the feature of Cloud DDNS service. [[WAN](#)]
- Added a new feature of VLAN interface configuration for routers. [[Configure a GWN Router](#)]
- Added alerts such as abnormal device time, abnormal temperature of the optical module, and VPN-related alerts [[Alerts](#)]
- Supports automatic time synchronization between routers and switches with cloud [[System](#)]
- Supports IPv6 PD/prefix length configuration in WAN [[WAN](#)]
- Added the ability to set the Primary Network for cloud [[Network Overview](#)]
- Added the ability to retrieve Guest information with API commands.
- Added the ability to display the Wi-Fi version used in the client's information [[Clients](#)]
- Added the ability to Customize the Channel in 2.4G band [[Wi-Fi](#)]
- Added the ability to disable the Router LAN ports [[Configure a GWN router](#)]
- Added the ability to configure the router/switch device password from GWN Cloud [[Configure a device](#)]
- Added the ability to support batch or single configuration for the Device Password [[System](#)]
- Added the ability to highlight mesh devices in Network Topology [[Topology](#)]
- Added the ability to configure Port Profile for Device Group [[Port profile](#)]
- Added the ability to display the router's LAN IP address [[Devices](#)]
- Added a new feature of VLAN Interface configuration for routers [[Configure a GWN router](#)]
- Added API support for Device Name and Equipment Remarks.

Version 1.1.24.28

Product Name: GWN.Cloud and GWN Manager

- Adjust the upper limit to 300 on the number of PPSK in a group [[PPSK](#)]
- Support to display the switch port info on the client list when the client connects to the switch [[Clients](#)]
- Support the option "Timeout Duration of Unauthenticated Clients" in external splash page [[Portal Policy](#)]
- Support the option "URL Pre-shared Key" when select Aiwifi as the platform of external splash page [[Portal Policy](#)]

Version 1.1.24.23

Product Name: GWN.Cloud and GWN Manager

- Added the unified management for model of GWN7801(P), GWN7802(P), GWN7803(P)
- Added the support for Device Information, Configuration, and Debug under Device menu for GWN switch models [[Configure a GWN Switch](#)]
- Added the support for GWN switches & port configurations through Global Switch Settings and Port Profiles [[DEVICES](#)]
- Added the support for GWN switches in Topology (including wired devices hierarchy relationship) [[Network Topology](#)]
- Added the support of GWN switches' Alert events [[ALERTS](#)]
- Added a new feature of user role management and customizable role privilege [[USER MANAGEMENT](#)]
- Added a new feature of Organization Overview [[ORGANIZATION](#)]
- Added a new feature of Map for device location management [[Map](#)]
- Added a new feature of AP batch configuration [[Configuration](#)]
- Added a new feature of displaying Change logs' content details [[Organization Change Log](#)]

- Added a new feature of transferring management permission for shared Network [[Share a Network](#)]
- Added a new feature of restricting APIs to specific networks [[API Developer](#)]
- Added a new feature of batch firmware upgrade for different GWN models to recommended version [[Upgrade](#)]
- Added a new feature of disabling AP's Ports [[Configuration](#)]
- Added a new feature of Limit by Authentication Type for Daily Limit of Captive Portal [[Profiles](#)]
- Added a new feature of Active Directory into Splash Page Logging Components [[Splash Page](#)]
- Added a new feature of grouping top website statistic by Main Domain than URL
- Added a new feature of PPSK With Radius into SSID Security Type [[Wireless LAN](#)]

Version 1.1.23.27

Product Name: GWN.Cloud and GWN Manager

- New Cloud Web Portal, SDN concept & UI design
- Unified GWN device management (Access points, Routers, Switches) [[Devices](#)]
- Inventory management [[Inventory](#)]
- New Network topology (replacing the old mesh topology) [[Network Topology](#)]
- New Alert design and support more alert events [[Alerts](#)]

Version 1.0.22.23

Product Name: GWN Manager

- Added feature of U-APSD for AP [[SSID](#)]
- Added feature of Email authentication for Captive Portal [[Splash page](#)]
- Added feature of post authentication rules for Captive Portal [[Portal Policy](#)]
- Added feature of service auto start after machine reboot for GWN Manager

Version 1.0.21.17

Product Name: GWN Manager

- Added feature of reporting Probe request RSSI information
- Added feature to export APs, clients, and alerts [[Devices](#)] [[Clients](#)]
- Added feature of Google Authentication [[Splash page](#)]
- Added feature of WiFi4EU [[Splash page](#)]
- Added feature of SMS authentication for Captive Portal [[Splash page](#)]
- Added feature of Hotspot 2.0 R3 [[Hotspot 2.0](#)]
- Added support to transfer APs to GWN Manager

Version 1.0.19.8

Product Name: GWN Manager

- No major changes.

Version 1.0.19.7

Product Name: GWN Manager

- Added support of deleting the voucher in use. [[Voucher](#)]
- Added support of client name in csv file when import access list. [[Access List](#)]
- Added configuration of secondary radius server for WLAN 802.1x authentication. [[Wi-Fi Settings](#)]
- Added WPA3 support in SSID setting. [[Wi-Fi Settings](#)]
- Added NET Port Type option for AP setting

Version 1.0.19.2

Product Name: GWN Manager

- Added support of Top Website statistic graph [[Overview](#)]
- Added support of Guest Count statistic graph [[Captive Portal Summary](#)]
- Added manager role: Network Administrator [[USER MANAGEMENT](#)]
- Added support of API Developer [[API Developer](#)]
- Added support of Access List Import in CSV [[Access List](#)]
- Added support of Rogue AP Detection [[Rogue AP](#)]
- Added support of SNMP [[SNMP](#)]
- Added support of Allow DHCP Option 43 to override GWN Manager Address [[Discover GWN76xx](#)]
- Added support of NAT [[NAT Pool](#)]
- Added support of Firewall [[Firewall](#)]
- Added support of Hotspot 2.0 Beta [[Hotspot 2.0](#)]

Version 1.0.10.7

Product Name: GWN.Cloud

- Added Site Survey feature [[Site Survey](#)]
- Added feature of Minimum Rate Control. [[Enable Minimum Rate](#)]
- Added feature of SSH Remote Access. [[SSH Remote Access](#)]
- Added feature of External Portal support Socifi Platform.
- Added feature of Client inactivity timeout. [[Client Inactivity Timeout](#)]
- Added feature of Upgrade Regularly [[Upgrade](#)]
- Added feature of Client Steering [[Client Steering](#)]
- Enhanced feature of Voucher: display of remaining bytes. [[Voucher](#)]
- Enhanced feature of Dynamic VLAN
- Changed LED patterns [[GWN76xx LED Patterns](#)]

Version 1.0.9.8

Product Name: GWN.Cloud

- Added support for collecting user feedback from GWN Cloud page.
- Added support for Voucher Style Customization. [[Voucher](#)]
- Added support for video URL. [[Advertisement](#)]
- Added support to export Guest Information via Email. [[Email Guest Information](#)]
- Added support for client RX/TX Rate display. [[Dashboard](#)]
- Expanded Max Devices to use the same Voucher. [[Voucher](#)]
- Added support to enable/disable client connection/disconnection events.

Version 1.0.8.17

Product Name: GWN.Cloud

- Added support for Advertisement for Captive Portal [[Advertisement](#)]
- Added support for Custom Field for Captive Portal Splash Page [[Splash Page](#)]
- Added feature of ARP Proxy. [[ARP Proxy](#)]
- Added support of Clear client data. [[Clients](#)]
- Enhanced Event log by Wi-Fi authentication event. [[Event Log per AP](#)]
- Added EU Server support. [[Zone](#)]
- Enhanced Bandwidth Rules by adding option to limit bandwidth Per-Client. [[Range Constraint](#)]
- Added Total Bandwidth Usage Display [[Dashboard](#)]

- Added Export Immediately feature for URL Access Logs. [[URL Access Log](#)]

Version 1.0.8.7

Product Name: GWN.Cloud

- Added support for URL logging (Except for GWN7610). [[URL Access Log](#)]

Version 1.0.7.18

Product Name: GWN.Cloud

- Enhanced Client Information. [[Dashboard](#)]
- Enhanced Access Point status. [[Info](#)]
- Added Reset access point button. [[Reset Device](#)]
- Added External Captive Portal Support. [[External Splash Page](#)]
- Added AP Scheduling Reboot. [[Reboot Schedule](#)]
- Added Change Log section. [[Change Log](#)]
- Added Account idle timeout. [[Account Idle timeout](#)]
- Added feature of Wi-Fi Statistic Report. [[Report](#)]
- Added feature of Captive Portal Guest Summary. [[Guests](#)]
- Changed SSID limit. [[SSID](#)]
- Enhanced Wi-Fi Service by adding configurable options. [[Wi-Fi](#)]
- Enhanced Captive Portal features. [[Failsafe Mode](#)] [[Daily Limit](#)] [[Byte Quota](#)] [[Force To Follow](#)] [[Portal Policy](#)]

Version 1.0.0.37

Product Name: GWN.Cloud

- This is the initial version for GWN.Cloud.

Version 1.0.0.33

Product Name: GWN Manager

- This is the initial version for GWN Manager.

Android™ is a trademark of Google LLC.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license by Apple Inc.
