



# Grandstream Networks, Inc.

---

## GWN Management Platforms User Guide



# WELCOME

Thank you for using the Grandstream GWN Management Platform.

GWN Management Platforms are enterprise-grade Wi-Fi network management platforms that offer 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 businesses 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 a 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

The 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):

- **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



<b>GWN7664</b>	1.0.21.4	1.0.25.10
<b>GWN7664LR</b>	1.0.23.4	1.0.25.10

*AP minimum and recommended version*

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

<b>Model</b>	<b>Minimum</b>	<b>Recommended</b>
<b>GWN7001</b>	1.0.1.6	1.0.5.30
<b>GWN7002</b>	1.0.1.6	1.0.5.30
<b>GWN7003</b>	1.0.1.6	1.0.5.30
<b>GWN7052</b>	1.0.5.34	1.0.9.34
<b>GWN7052F</b>	1.0.5.4	1.0.9.34
<b>GWN7062</b>	1.0.5.34	1.0.9.34

*Router minimum and recommended version*

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

<b>Model</b>	<b>Minimum</b>	<b>Recommended</b>
<b>GWN7801</b>	1.0.3.19	1.0.3.37
<b>GWN7801P</b>	1.0.3.19	1.0.3.37
<b>GWN7802</b>	1.0.3.19	1.0.3.37
<b>GWN7802P</b>	1.0.3.19	1.0.3.37
<b>GWN7803</b>	1.0.3.19	1.0.3.37
<b>GWN7803P</b>	1.0.3.19	1.0.3.37
<b>GWN7806</b>	1.0.1.14	1.0.1.14
<b>GWN7806P</b>	1.0.1.14	1.0.1.14
<b>GWN7811</b>	1.0.1.8	1.0.1.20
<b>GWN7811P</b>	1.0.1.8	1.0.1.20
<b>GWN7812P</b>	1.0.1.8	1.0.1.20
<b>GWN7813</b>	1.0.1.8	1.0.1.20
<b>GWN7813P</b>	1.0.1.8	1.0.1.20

<b>GWN7816</b>	1.0.3.8	1.0.3.8
<b>GWN7816P</b>	1.0.3.8	1.0.3.8
<b>GWN7830</b>	1.0.3.3	1.0.3.3
<b>GWN7831</b>	1.0.3.3	1.0.3.3
<b>GWN7832</b>	1.0.3.3	1.0.3.3

*Switch minimum and recommended version*

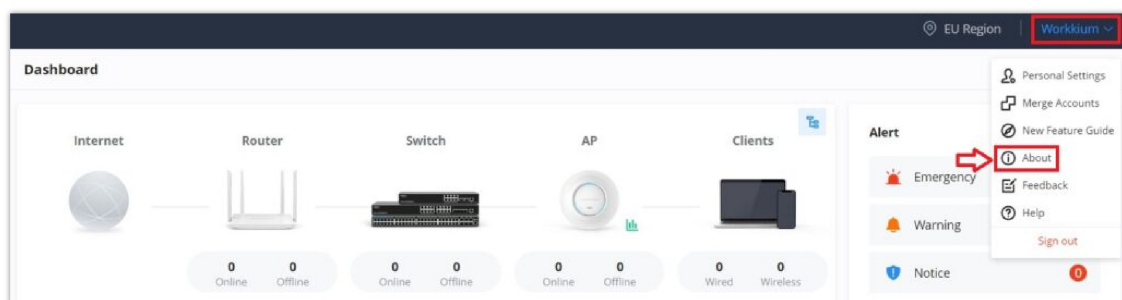
◦ **GWN App: minimum and recommended version**

<b>Platform</b>	<b>Minimum</b>	<b>Recommended</b>
<b>iOS</b>	1.0.5	1.6.7
<b>Android</b>	1.0.0.14	1.0.6.7

*App minimum and recommended version*

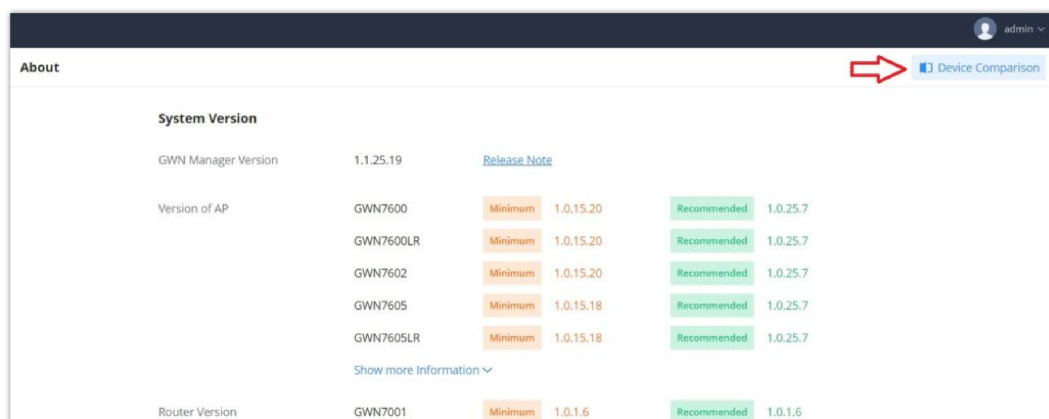
*Requirements*

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*

On this page, the users can find the minimum and recommended firmware version for each GWN device and APP (iOS® and Android®). If a Beta firmware is available for a GWN device it will be also shown here.



*Device Comparison – Step 2*

GWN7801	Minimum	0.0.0.0	Official	1.0.5.23	Beta	1.0.5.23
GWN7801P	Minimum		Official	1.0.5.23	Beta	1.0.5.23
Show more information v						
AP Version						
	Minimum		Official			
	Minimum		Official			
GWN7600	Minimum	1.0.15.20	Official	1.0.23.6		
GWN7600LR	Minimum	1.0.15.20	Official	1.0.23.6		
GWN7602	Minimum	1.0.15.20	Official	1.0.25.14	Beta	1.0.25.14

Device Comparison – Step 2 (Beta firmware)

GWN Cloud										
Device Comparison You may find out the differences on GWN Cloud Functions among devices (based on recommended version)										
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 – Step 3

## PRODUCT OVERVIEW

### Features Highlights

<b>GWN.Cloud</b>	<ul style="list-style-type: none"> <li>• Software-as-a-Service (SaaS) Solution to manage all your Grandstream GWN products (Access points, Routers and switches), without any additional on-premise infrastructure.</li> <li>• High level security, since all the traffic between GWN devices and cloud is secured.</li> <li>• Easy way to add new GWN devices, either using device MAC address or Mobile App (Android or iOS).</li> <li>• No limits on number of sites or GWN devices.</li> </ul>
<b>GWN Manager</b>	<ul style="list-style-type: none"> <li>• Linux (CentOS7, AlmaLinux9 and Ubuntu) based solution to secure and manage all your Grandstream GWN devices.</li> <li>• Automatically discover and Adopt GWN devices in your network.</li> <li>• Adopt GWN device manually using SSH or through Web GUI by setting the Manager address and port.</li> <li>• Up to 3000 GWN devices, with high performance hardware.</li> </ul>
<b>Shared</b>	<ul style="list-style-type: none"> <li>• Highly available with no single point of failure across the whole system.</li> <li>• Easy and intuitive dashboard for monitoring.</li> <li>• Network Group creation.</li> <li>• GWN devices and clients Centralized monitoring and management.</li> <li>• Captive portal configuration.</li> <li>• Bandwidth control per SSID, IP, or MAC address.</li> <li>• Unified GWN device management (GWN Routers, GWN Switches and GWN APs)</li> <li>• Inventory management</li> <li>• Map to locate devices and Heatmap.</li> <li>• Network topology</li> </ul>

### Features Highlights

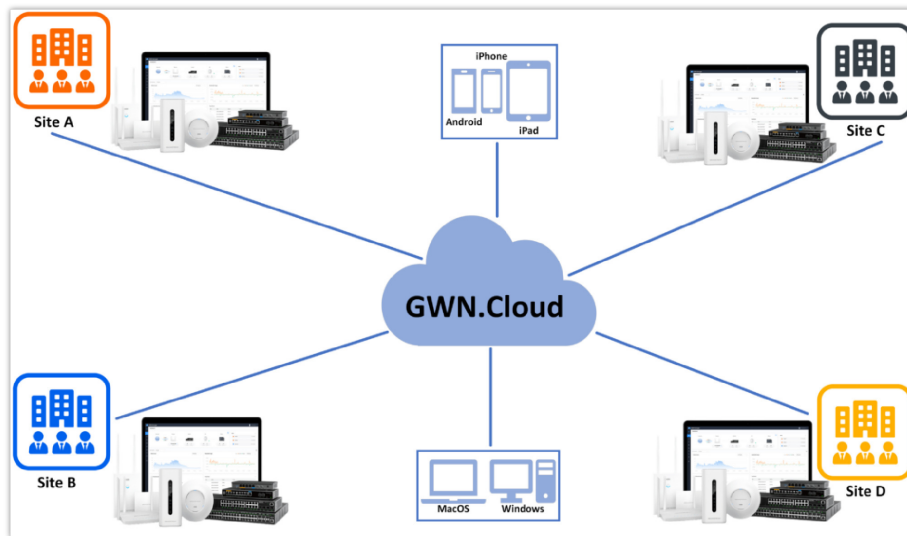
## Specifications

<b>Function</b>	<ul style="list-style-type: none"> <li>● Network-based GWN devices management</li> <li>● Network/GWN devices/client monitoring</li> </ul>
<b>Security and Authentication</b>	<ul style="list-style-type: none"> <li>● Supports access policies configuration (blacklist, whitelist, time policy etc)</li> <li>● Multiple security modes including WPA, WPA2, WPA3,WEP, open, etc.</li> <li>● Bandwidth rules for client access</li> <li>● User and privilege management</li> </ul>
<b>Enterprise Features</b>	<ul style="list-style-type: none"> <li>● 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.</li> <li>● Hosted by AWS with 99.99% uptime (GWN.Cloud only)</li> <li>● Bank-grade TLS encryption from end-to-end</li> <li>● X.509 certificate-based authentication</li> <li>● Supports Wi-Fi Alliance Voice-Enterprise</li> <li>● Mobile app for iOS and Android</li> <li>● Real-time Wi-Fi Scan for deployment</li> <li>● URL access log collection</li> <li>● Multiple Wi-Fi performance optimization methods including band steering, Minimum RSSI, ARP Proxy, IP multicast to unicast, etc</li> </ul>
<b>Supported Devices</b>	<ul style="list-style-type: none"> <li>● <b>Access points:</b> GWN76xx(LR)</li> <li>● <b>Routers:</b> GWN7052/F, GWN7062 and GWN700x</li> <li>● <b>Switches:</b> GWN780x(P), GWN781x(P) and GWN7806(P)</li> </ul>
<b>Captive Portals</b>	<ul style="list-style-type: none"> <li>● Splash page with built-in WYSIWYG editor</li> <li>● Social media integration</li> <li>● Multiple captive portal authentications including simple password, radius, voucher, custom field etc.</li> <li>● External captive portal integration</li> <li>● Real-time guest statistics and monitoring</li> <li>● Advertisement integration with flexible strategies</li> <li>● Export guest info into file and automatically send to email</li> </ul>
<b>Centralized Management</b>	<ul style="list-style-type: none"> <li>● Local data forwarding, no user traffic sent to the controller</li> <li>● Network-based GWN device management</li> <li>● Network/GWN device/client monitoring</li> <li>● Layer2 and Layer3 based GWN device discovery</li> </ul>
<b>Reporting and Monitoring</b>	<ul style="list-style-type: none"> <li>● Real-time Network and client monitoring</li> <li>● Detailed reports by network, GWN devices, client etc.</li> <li>● Retrieval of historical data for statistical observations</li> <li>● Real-time alerts and event logs</li> </ul>
<b>Maintenance</b>	<ul style="list-style-type: none"> <li>● Ping/traceroute/capture</li> <li>● Both configuration and data backup</li> <li>● Scheduled GWN devices firmware update and LED control</li> <li>● Change log for audit trail</li> </ul>
<b>Languages</b>	English, Chinese, Spanish, German, Portuguese, French and more.

# GETTING TO KNOW GWN MANAGEMENT PLATFORM

## GWN.Cloud

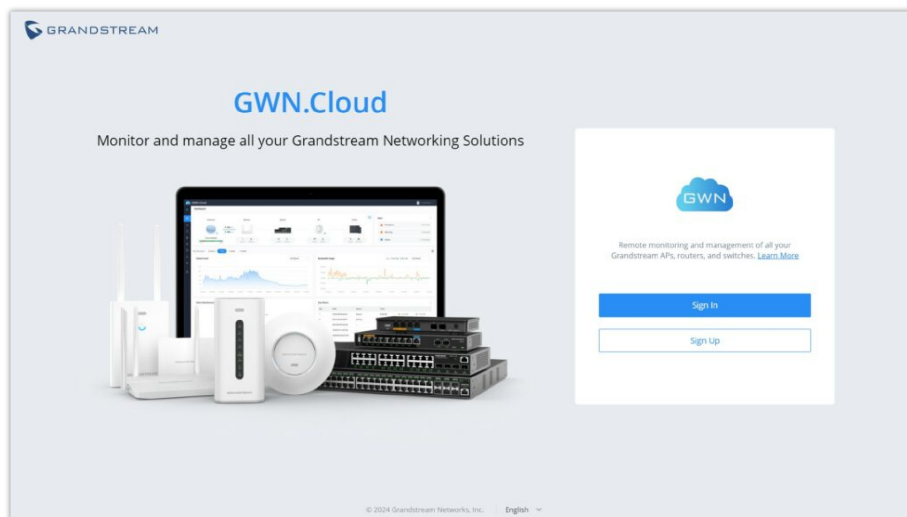
GWN.Cloud is a cloud-based platform used to manage and monitor GWN devices (Access Points, Routers, Switches) wherever they are as long as they are connected to the internet. The platform can be accessed using the following link: <https://www.gwn.cloud>. It provides an easy and intuitive web-based configuration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



*GWN.Cloud Architecture*

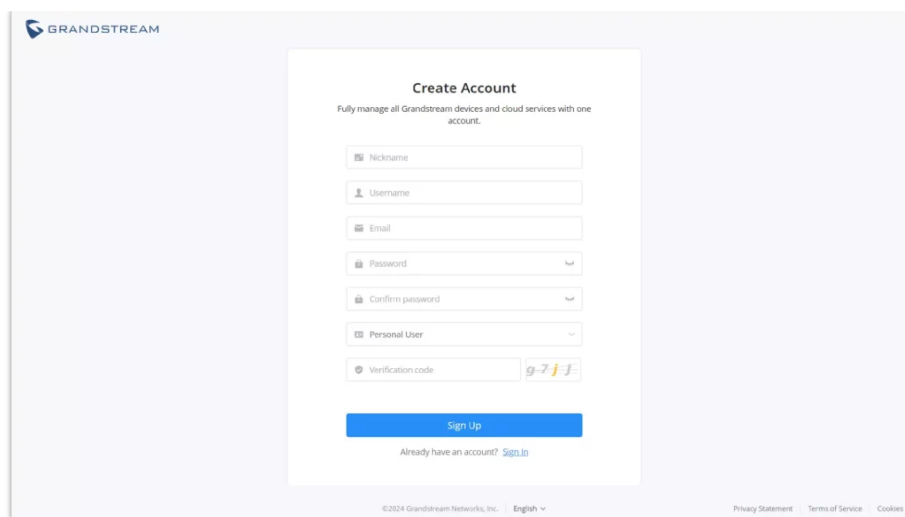
## Sign up to GWN.Cloud

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.



**GRANDSTREAM**

### Create Account

Fully manage all Grandstream devices and cloud services with one account.

Nickname

Username

Email

Password

Confirm password

Personal User

Verification code

[Sign Up](#)

Already have an account? [Sign In](#)

©2024 Grandstream Networks, Inc. English

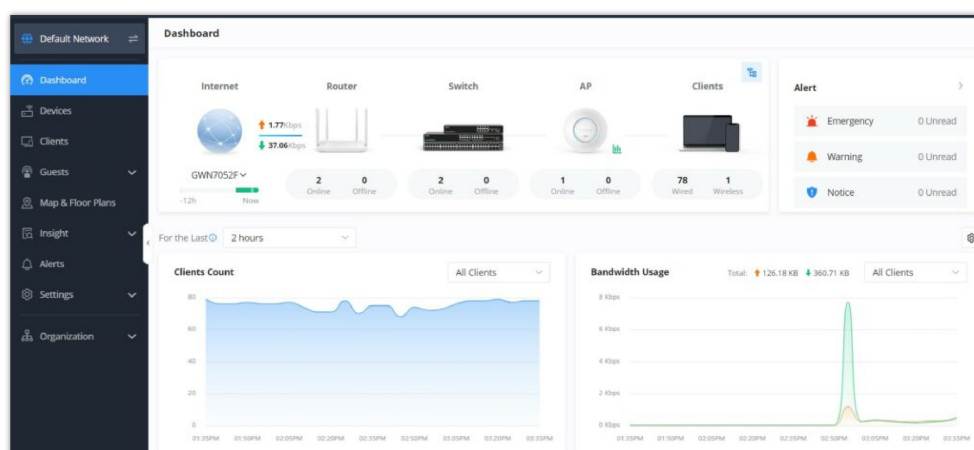
[Privacy Statement](#) [Terms of Service](#) [Cookies](#)

GWN.Cloud Sign-up page

<b>Nickname</b>	Specify a nickname of this account.
<b>Username</b>	Specify a username for this account.
<b>Email</b>	Enter the email address.
<b>Password</b>	Specify a password for the account <i>Note: 8-16 characters, must be a combination of numbers, letters, and special characters.</i>
<b>Confirm password</b>	Re-enter the password again.
<b>User type</b>	Select from the drop-down list the type of user: <ul style="list-style-type: none"> <li>Enterprise</li> <li>Server provider</li> <li>Channel Reseller</li> <li>System Integrator</li> <li>Personal User</li> </ul>
<b>Company Name</b>	Enter the company name if the type of user is set to Enterprise, Server provider, Channel reseller, System integrator.
<b>Verification code</b>	Copy the verification from the Captcha.

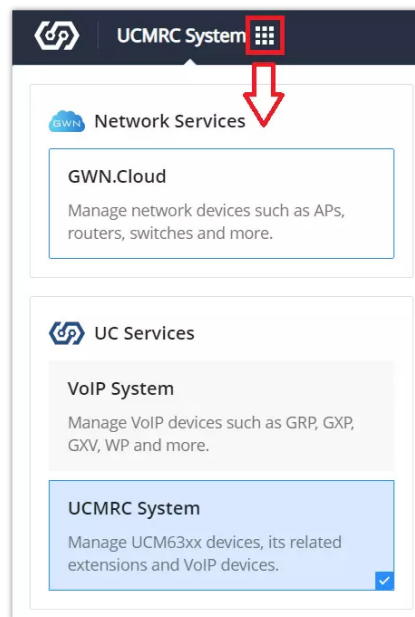
## GWN.Cloud Sign-up Settings

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



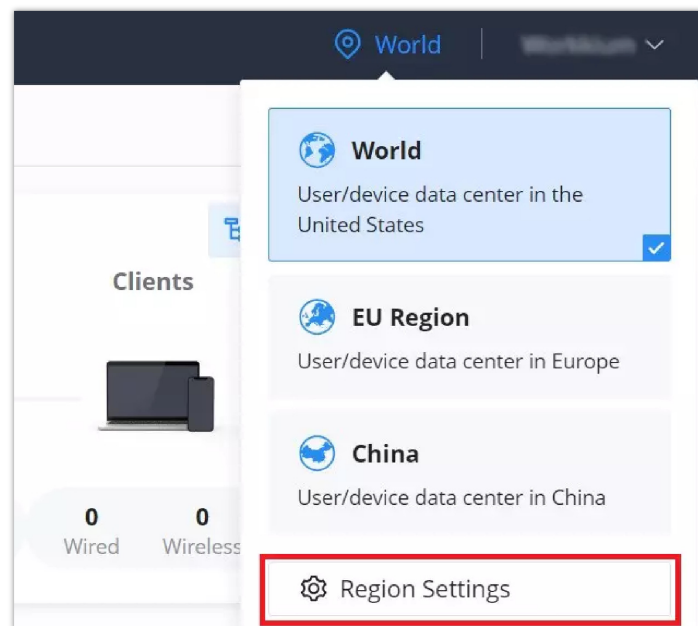
## Region settings

To switch to network services (GWN.Cloud) when the user was in another service such as (VoIP system or UCMRC system), on the top left of the web page, click on the dots icon and select GWN.Cloud under Network Services as shown below:



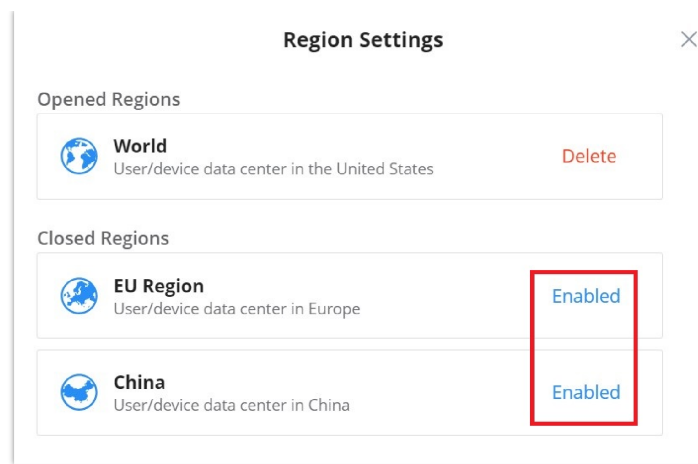
Network Services

Region settings allows the users to enable different regions (data center). To enable or delete a region, on the top right of the page click on **the location icon** → **region settings** as shown below:



Region settings

The users and devices data is stored in the enabled regions, to delete a region click on **"Delete"**, and to enable a region click on **"Enabled"**.

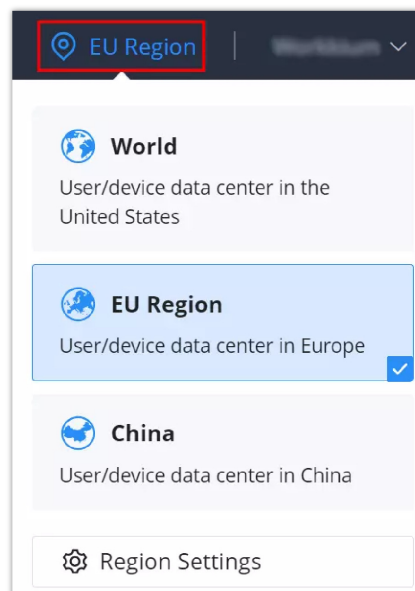


*Region settings – delete & enable*

**Note:**

Please note deleting a region will delete all data within that region including GWN.cloud data and GDMS data.

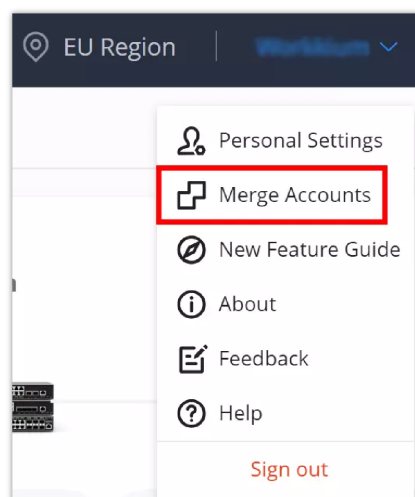
To start using the enabled region to store users/devices data, make sure it's selected on the main page as shown below:



*The selected region (EU Region)*

## Merge Accounts

Merge accounts feature allows users to merge different account with different services and regions into one single base account. On the main page of GWN.Cloud, top right corner of the page, click on the account name then select Merge Accounts as shown below:






## Merge Accounts


Click on “**+Accounts to Be Merged**” button to add more account, then select the base account that will be used for centralized management.

### Merge Accounts

 Merge multiple accounts into one for centralized management.  
[How to merge accounts?](#)

Select the account that will be used as the base account for centralized management.  
All information from the other accounts such as sub-accounts, role permissions, devices and settings will be transferred to the current account upon merging. Note: The system settings and API developer configurations of the current account will be used.

#### Current Login Account

Account after Merge 

Username	Email	Enterprise	Enabled Platforms
Wenbin	wenbin@gmail.com	None	UC Services ( World, EU Region, China) GWN.Cloud ( World, EU Region, China)

#### Account To Be Merged 1

Username	Email	Enterprise	Enabled Platforms
afuad@h3m.com	afuad@h3m.com	—	UC Services ( World) GWN.Cloud ( World)


[+ Accounts to Be Merged](#)

Cancel

Merge

## Merge Accounts

### Merged accounts successfully



The selected account (Wenbin) can be used to log into GDMS and GWN.Cloud in the future.

Start Use

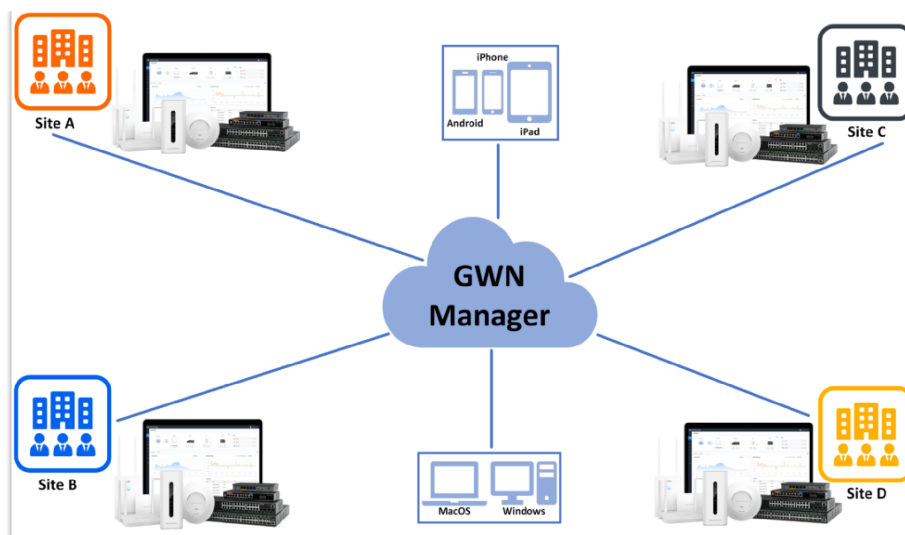
Merged accounts successfully

### Note:

The base account will be used for centralized management and all information from the other accounts such as sub-accounts, role permissions, devices and settings will be transferred to the base account upon merging. The system settings and API developer configurations of the current account will be used.

## GWN Manager

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



GWN Manager Architecture

## GWN Manager hardware requirements

- OS: CentOS7, AlmaLinux9 and Ubuntu.

- 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:

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

1

2


3

4

5

General

Sets the country/region and time zone of the default network



Country/Region

Morocco(المغرب) ▾

Timezone

(GMT+01:00) Casablanca, Monrovia ▾

© 2022 Grandstream Networks, Inc.All Rights Reserved. | English ▾

GWN Manager Wizard – Part 1

GWN Manager

✓

2


3

4

5

User Account

Set up a Username and Password for local login.



\* User name

3-64 characters

\* Password

8-16 characters, only the numbers, letters or special characters

\* Confirm Password

\* Email

<

>

© 2022 Grandstream Networks, Inc.All Rights Reserved. | English ▾

GWN Manager Wizard – Part 2

GWN Manager

✓

✓


3

4

5

Adopt Device

The selected device will automatically add the default network

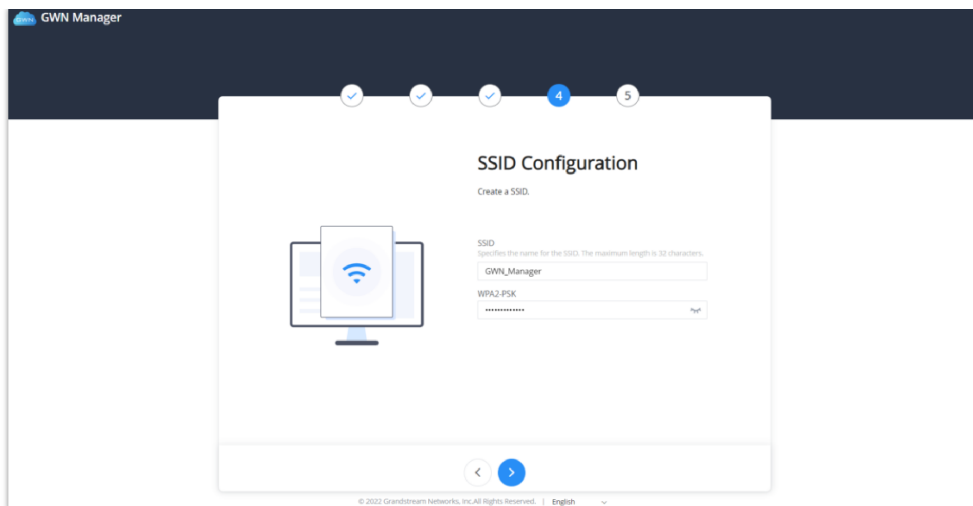
<input checked="" type="checkbox"/>	Model	MAC	IP Address	Firmware
<input checked="" type="checkbox"/>	 GWN7624	C0:74:AD:90:B2:40	192.168.5.159	1.0.23.15

<

>

© 2022 Grandstream Networks, Inc.All Rights Reserved. | English ▾

GWN Manager Wizard – part 3




**GWN Manager**

1 2 3 4 5

### SSID Configuration

Create a SSID.



SSID

Specifies the name for the SSID. The maximum length is 32 characters.

GWN\_Manager

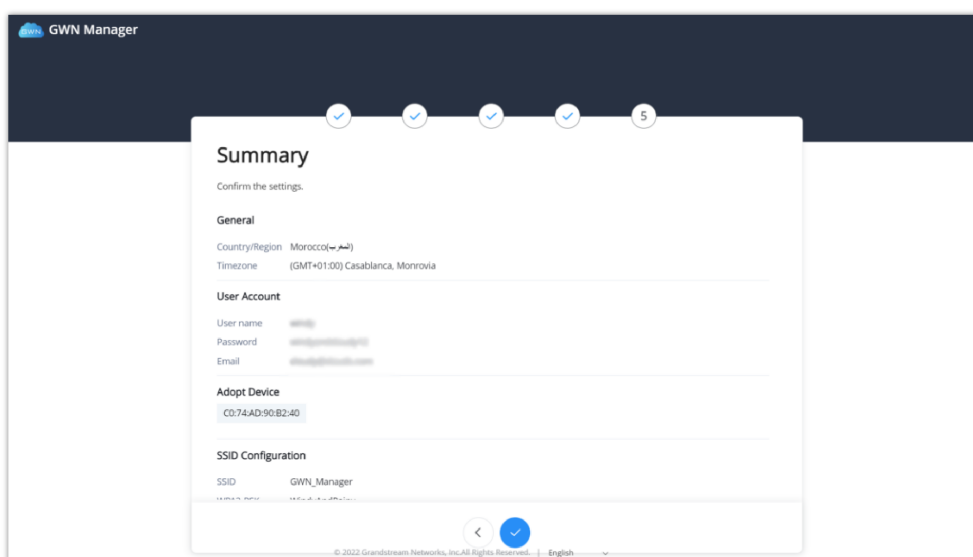
WPA2-PSK

\*\*\*\*\*

< >

© 2023 Grandstream Networks, Inc. All Rights Reserved. | English

GWN Manager Wizard – part 4



**GWN Manager**

1 2 3 4 5

### Summary

Confirm the settings.

**General**

Country/Region Morocco (المغرب)

Timezone (GMT+01:00) Casablanca, Monrovia

**User Account**

User name admin

Password admin12345678

Email admin@grandstream.com

**Adopt Device**

C0:74:AD:90:B2:40

**SSID Configuration**

SSID	WPA2-PSK
GWN_Manager	WPA2-PSK-*****

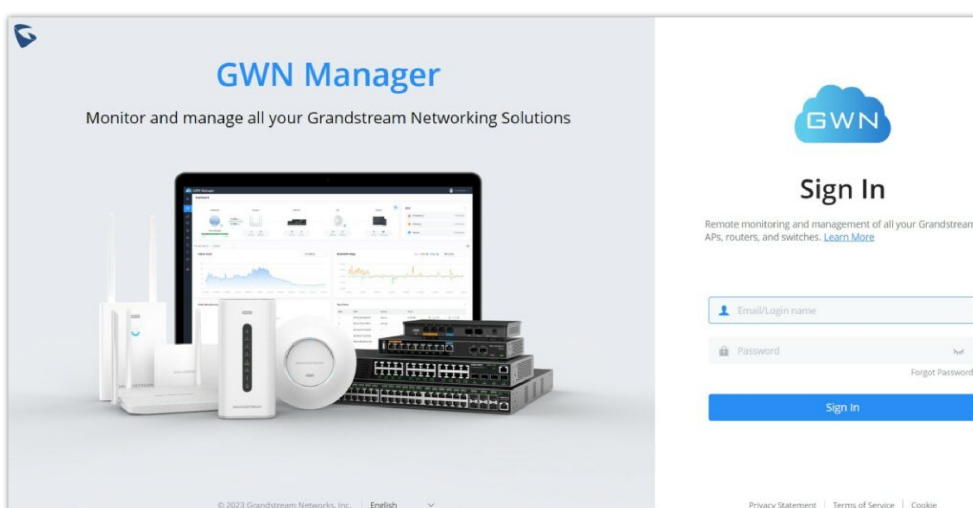
< >

© 2023 Grandstream Networks, Inc. All Rights Reserved. | English

GWN Manager Wizard – part 5


## Sign up to GWN Manager


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



**GWN Manager**

Monitor and manage all your Grandstream Networking Solutions





### Sign In

Remote monitoring and management of all your Grandstream APs, routers, and switches. [Learn More](#)

Email/Login name

Password

[Forgot Password?](#)

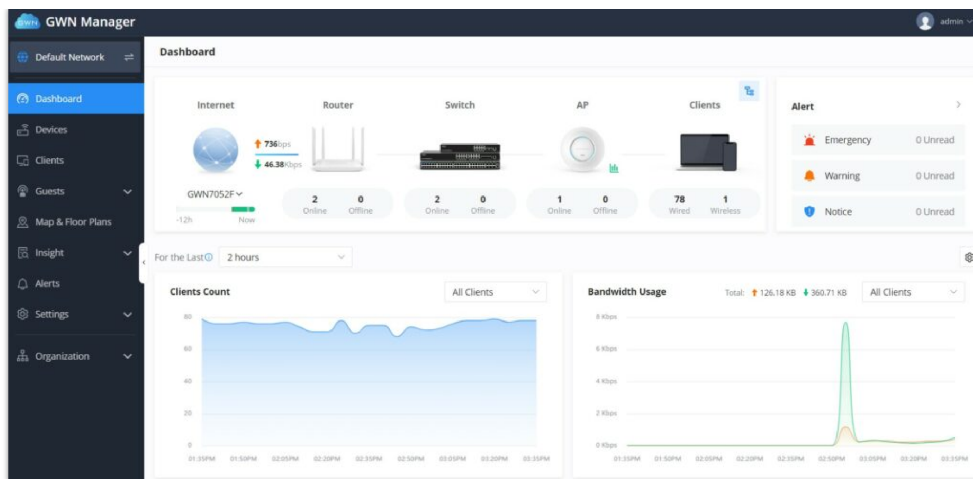
**Sign in**

© 2023 Grandstream Networks, Inc. | English

[Privacy Statement](#) | [Terms of Service](#) | [Cookie](#)

GWN Manager Login Page

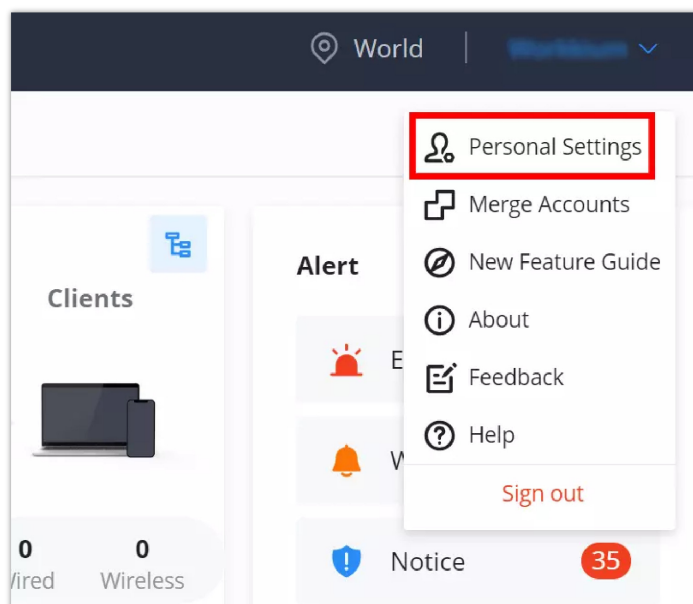
The following page will be displayed:



GWN Manager Dashboard

## Personal Settings

To edit the personal settings of the currently log in account, click on the name account from **the top right corner** → **Click on Personal Settings** a new page displaying the account details will be displayed, refer to the figure below:



Personal Settings

To modify a field click on **"Modify"** text, refer to the figures and table below:


The screenshot shows the 'User Settings' form. The form contains the following fields and their current values:

Field	Value	Action
Nickname	WorldStream	Modify
Username	WorldStream	Modify
Email	worldstream@gmail.com	Modify
Password	*****	Modify
Language	English	Modify
Timezone	(GMT+01:00) Casablanca, Monrovia	Modify
Time	12 hours	Modify
Date Format	YYYY-MM-DD	Modify
User Type	Personal User	Modify
Company Name	-	Modify
Country	Morocco (المغرب)	Modify
Multi-Factor Safety Authentication	<input type="checkbox"/>	<a href="#">Multi-Factor Authentication Instructions</a>


The form also includes a 'Delete business account' button in the top right corner and a footer with copyright information and links to Privacy Statement, Terms of Service, and Cookies.

Personal Settings


**Select Authentication Method**



**Authentication App**  
Authenticate via a code generated by an app installed on your mobile device or PC.



**TOTP Hardware Token**  
Authenticate via a code displayed on a "time-based one-time password" (TOTP) hardware token.



**FIDO Security Key**  
Authenticate via a code generated by YubiKey or other devices that support FIDO security keys.

[Multi-Factor Authentication Instructions](#)

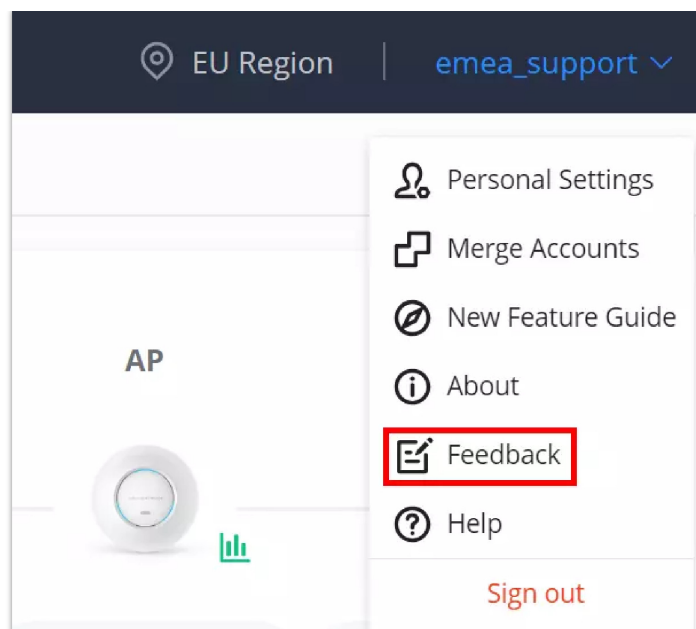
*Personal Settings – Multi-Factor Authentication*

<b>Nickname</b>	Modifies the user nickname
<b>Username</b>	Modifies the username
<b>Email</b>	Modifies the Email address
<b>Password</b>	Changes the password
<b>Language</b>	Select the web UI language from the drop-down list
<b>Timezone</b>	Select the timezone from the drop-down list
<b>Time</b>	Select the time format: 12 hours or 24 hours
<b>Date Format</b>	Select the date format from the drop-down list
<b>User Type</b>	Select the user type from the drop-down list
<b>Company Name</b>	Specifies the company name
<b>Country</b>	Select the country from the drop-down list
<b>Multi-Factor Safety Authentication</b>	Toggle ON/OFF the Multi-Factor authentication Note: for more details, visit <a href="#">Multi-Factor Authentication</a>

*Personal Settings*

## Feedback

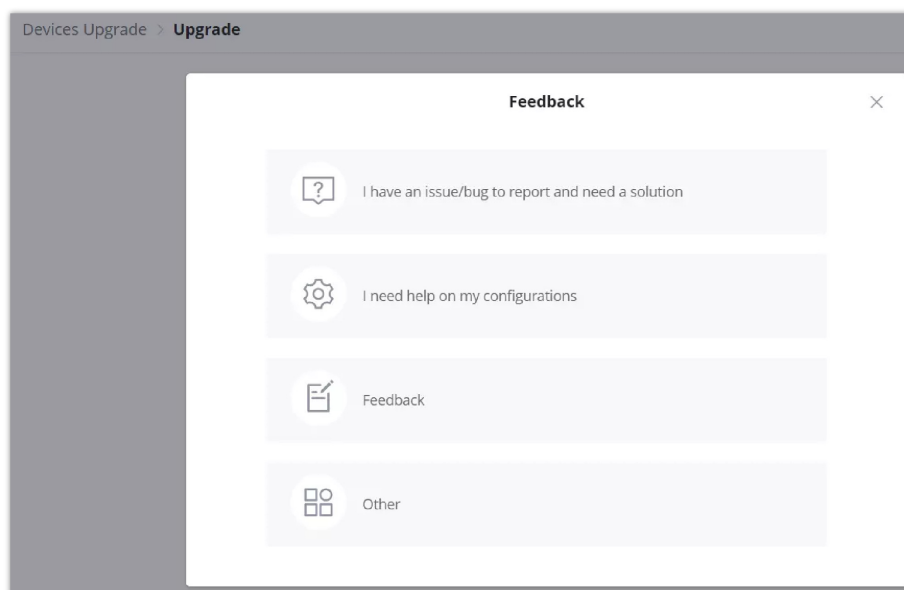
If the users have an issue/bug to report or need help about configurations or a general feedback, on the top right corner of the page, click on the account username then click on **"Feedback"** to send a feedback.



*Feedback*

Then, select what type of feedback:

- I have an issue/bug to report and need a solution (forwards the users to [Grandstream helpdesk](#))
- I need help on my configurations (forwards the users to [Grandstream helpdesk](#))
- Feedback.
- Other.



*Feedback types*

If Feedback or Other is selected, this page will be shown for users to specify the issue/bug/feedback with attachments (e.g. syslog) and emails for contact.

Report an Issue

\* Please enter your feedback

You can directly paste screenshots and web pictures here as attachments

( File type: zip, tar, rar, xls,xlsx,txt,docx,doc,jpeg,jpg,png,pdf,mp4,avi,wav, csv, gz )

\* Please enter your email address so that we can contact you in time.

emea\_support@grandstream.com

+ Add Email

Cancel

Submit

## GETTING STARTED WITH GWN MANAGEMENT PLATFORM

## Add a GWN Device to GWN Cloud

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

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

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

GWN device MAC and Password



**Devices**

[Add](#)
[Export](#)
[Group Management](#)
[More](#)

All Status ▾ All Models ▾

<input type="checkbox"/>	Device Model	MAC	IP Address ▾	Public IP Address ▾	Device Group	Firmware ▾	Operation
<input type="checkbox"/>	GWN7813P	C0:74:AD:GWN7813P	192.168.80.211		Default	1.0.1.8	

Total 1 10/page < 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  
GWN7624

**\*MAC**  
c0 : ad : 74 : 00 : 00 : 00

**\*Password**  
.....

**Equipment Remarks**  
0-64 characters  
Hall AP

Cancel Add

Adding a GWN device (AP) – Manually

If the GWN device is a router, the users will have to option to automatically synchronize router local WAN configurations to GWN.Cloud and also assign the SSIDs that are already in the network to the newly added router.

### Add Device

Manual Inventory Import

**Device added successfully**

☒ Automatically synchronize router local WAN configurations to GWN.Cloud  
The synchronization will begin after the device is online.

☐ Assign the SSID in this network to the newly added router.  
If selected, the SSID created in the local web interface will be overwritten. Device management can be carried out within Wi-Fi -> Wireless LAN.

Cancel OK

Router

Cancel Add

Adding a GWN Router – Manually

**Add Device**

Manual   Inventory   Import

Device Group: Default

All Models   Q MAC/SN

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

Cancel   **Add**

*Adding a GWN device – Inventory*

5. Click on the “**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 the **Import** Tab and click on the “**Add**” button to select a CSV file.

**Add Device**

Manual   Inventory   Import

Click to upload CSV file

click to download the [reference template](#).

Cancel   **Add**

*Import the CSV file for devices*

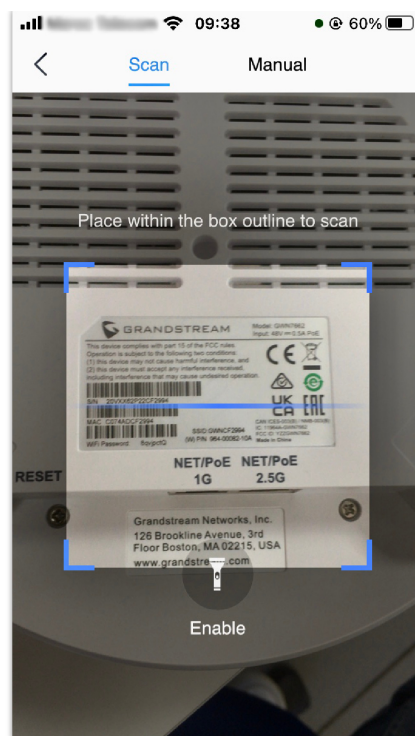
### **Method 2: Add a new GWN device using GWN.Cloud Application**

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

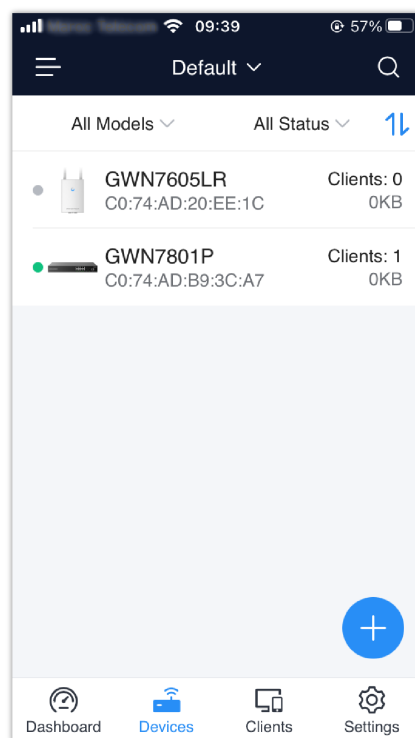
#### **Note:**

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

The operation is done by scanning the barcode from the 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.

Devices

Adopt

Export

Group Management

More

All Status

All Models

MAC/Name/IP/Device Group

<input checked="" type="checkbox"/> Device Model	IP Address	Device Group	Num of Clients	Operation
<input checked="" type="checkbox"/> GWN7624	192.168.5.110	New Device Group	1	
<input checked="" type="checkbox"/> GWN7002	192.168.80.1	WAN	0	
<input checked="" type="checkbox"/> GWN7052F	192.168.80.1	New Device Group	1	
<input checked="" type="checkbox"/> GWN7803P	C0:74:AD:192.168.5.107	Default	154	
<input checked="" type="checkbox"/> GWN7813P	C0:74:AD:192.168.5.109	New Device Group	152	

Configure

Reboot

Move

Push Configuration

Reset

Delete

Total 5

10/page

<

1

>

GWN devices list

### Method 3: Transfer from Local Master

In the case where a local master is 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 the 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**.

Overview Access Points Clients Captive Portal Bandwidth Rules SSID System Settings	Access Points							
	Device Type <span>▼</span>		<input type="text"/>		<a href="#">Transfer AP</a> <a href="#">Discover AP</a> <a href="#">Failover</a>			
	<a href="#">Upgrade</a>		<a href="#">Reboot</a>		<a href="#">+ Add to SSIDs</a> <a href="#">✕ Configure</a>			
	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions	
	GWN7600	00:0B:82:8B:58:30	192.168.6.246	Master	20m 24s	1.0.6.23		

Master AP – Access Points

2. Press [Transfer AP](#) button. A new window will display the “Transferable devices” list as shown below.

Transfer AP to cloud
✕

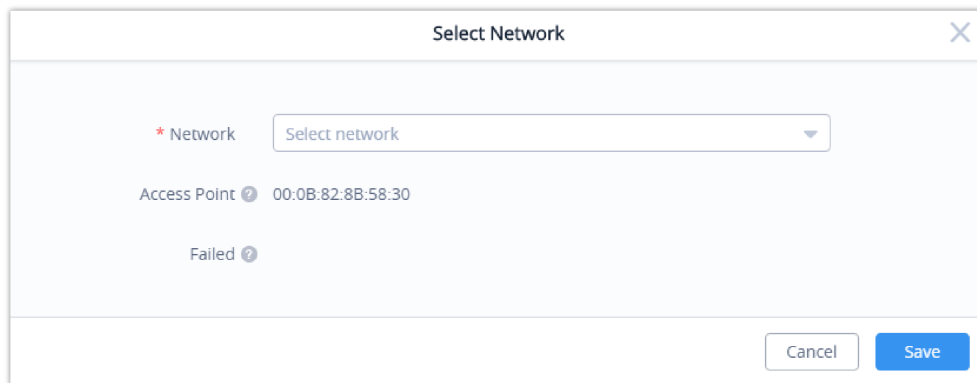
Transferable devices (online and supported by cloud):  
00:0B:82:8B:58:30

untransferable devices:  
There are no untransferable devices.

[Transfer](#)
[Cancel](#)

### Transfer AP to Cloud

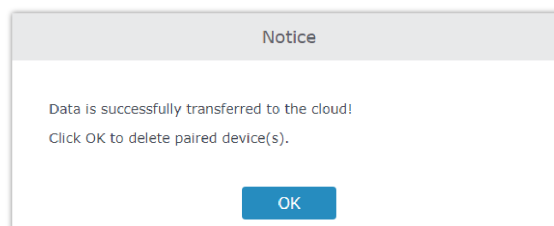
- Press **Transfer** button. The web browser will redirect to GWN.Cloud login page.
- Once logged in to the cloud, the configuration page "Select Network" will be displayed:



The "Select Network" dialog box features a title bar with a close button. Inside, there is a label "\* Network" followed by a dropdown menu currently showing "Select network". Below this, the "Access Point" is listed as "00:0B:82:8B:58:30" with a help icon. A "Failed" status is also shown with a help icon. At the bottom right, there are "Cancel" and "Save" buttons.

### Select Network

- **Access Point:** Shows the MAC address of the passed check device.
  - **Failed:** Shows the MAC address of the authentication failed or added.
- Select **Network** from the drop-down list to which the AP will be assigned.
  - Press the **Save** button to confirm.
  - Once added to the cloud, Master AP web UI will display following successful notice.

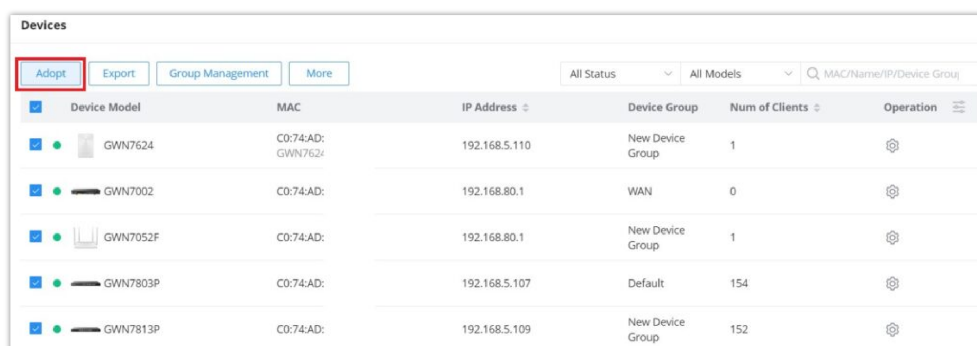


### Transfer AP to Cloud – Success

## Adopt a GWN Device to GWN Manager

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

- Navigate to **GWN Manager Web UI → Devices**
- Click on the "**Adopt**" button.



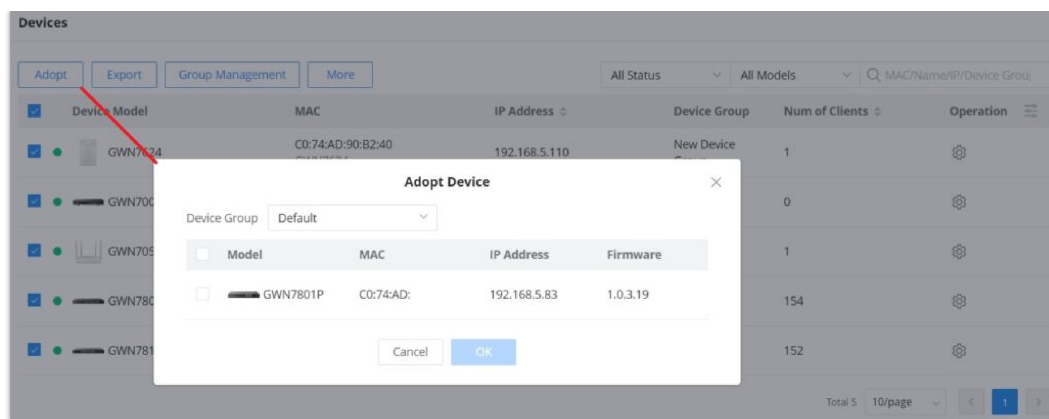
The "Devices" page in the GWN Manager web UI shows a table of discovered devices. The "Adopt" button is highlighted with a red box. The table lists five devices with their models, MAC addresses, IP addresses, device groups, and number of clients.

Device Model	MAC	IP Address	Device Group	Num of Clients	Operation
GWN7624	C0:74:AD:GWN7624	192.168.5.110	New Device Group	1	
GWN7002	C0:74:AD:	192.168.80.1	WAN	0	
GWN7052F	C0:74:AD:	192.168.80.1	New Device Group	1	
GWN7803P	C0:74:AD:	192.168.5.107	Default	154	
GWN7813P	C0:74:AD:	192.168.5.109	New Device Group	152	

### Adding a new GWN device to GWN Manager

- 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 the “**OK**” button.

## Adopting GWN devices manually

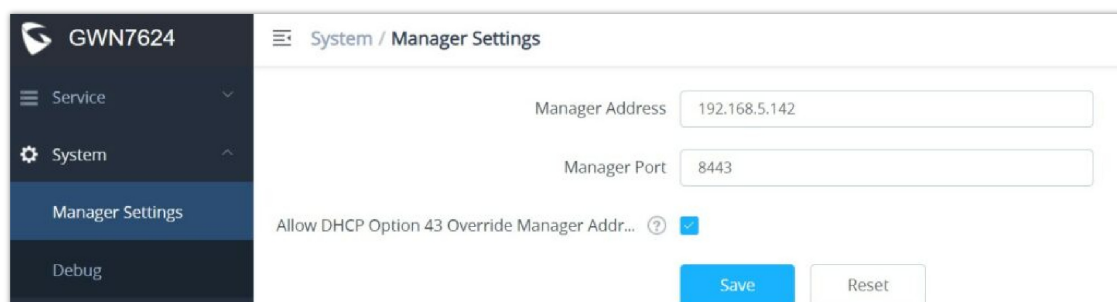
To manually configure the manager address and port on a GWN device, enable Manager Settings, fill in the Manager Address and Port, and finally click on the “**Save**” button. For each GWN device (AP, Router, or Switch), please check the steps below:

### Note:

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

You can log into the WebUI of a 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 the 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)!
192.168.5.142:8443
Select by pressing the [number] or [letter] and then ENTER

```

Manager Settings – SSH

## NETWORKS

The network page provides 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 **the** “Create Network” button and enter the network name, country/region, time zone, and Network Administrator, and select a network in case you want to clone a previously created network.

**Network Overview** | Location Overview

**Network** | Router | Switch | AP | Clients

4 | 4 | 0 | 0 | 1 | 0 | 0 | 0 | 2 | 0

Network Administrator | Online | Offline | Online | Offline | Online | Offline | Wired | Wireless

**Alert**

- Urgent: 0 Unread
- Critical: 0 Unread
- Normal: 1 Unread

**Network List**

Create Network | Sort Network | Search Name

Network Name	Devices (Total)	Devices (%Down)	Num of Clients	Created Time	Operation
Default	1	0%	2	2022-02-01 09:27PM	⚙️
Office	0	—	0	2022-09-21 10:39AM	⚙️ 🗑️
Training	0	—	0	2022-11-07 10:15AM	⚙️ 🗑️
TestNetwork	0	—	0	2023-05-09 04:27PM	⚙️ 🗑️

Network list

Overview > **Create Network**

\* Network Name ⓘ

Guests Network

\* Country/Region

Morocco(المغرب) ▾

\* Time Zone

(GMT+01:00) Casablanca, Monrovia ▾

Network Administrator

newadmin@org.local.com

newadmin@org.local.com

newadmin@org.local.com

Optional Account ▾

Clone Network

Select a network to clone

Default

Office

Create Network

Setting	Description
<b>Network Name</b>	Enter the Network Name to identify different networks in your environment.
<b>Country/Region</b>	Select the country/Region, this is required to set the Wi-Fi specifications of your country on GWN devices.
<b>Time Zone</b>	Select your time zone.
<b>Network Administrator</b>	This field displays the list of administrators that can manage this network.
<b>Clone network</b>	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 the Devices page, select the desired devices, click on the **“More”** button then select **“Move”**, after that a pop window will appear to choose the destination network to which the selected devices will be moved.

Devices

Adopt

Export

Group Management

More

All Status ▾

All Models ▾

Q MAC/Name/IP/Device Group

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 a different network

## Share a Network

GWN Platforms allow sharing of a network among the administrators of 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					
<a href="#">Create Network</a> <a href="#">Sort Network</a>		<input type="text" value="Search Name"/>			
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	
<div>Total 3</div> <div>10/page</div> <div> </div>					

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

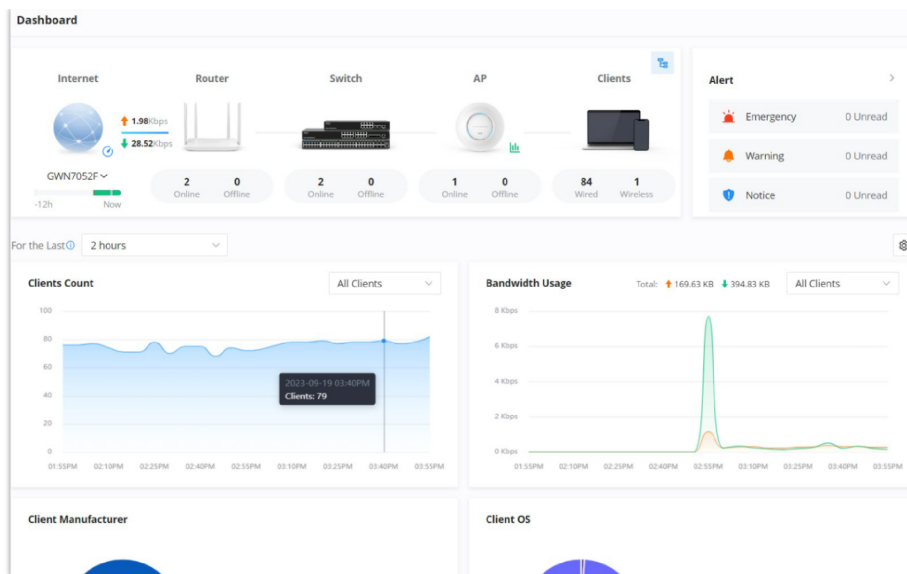
## DASHBOARD

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 also displays an Alerts preview and the user can click on 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.



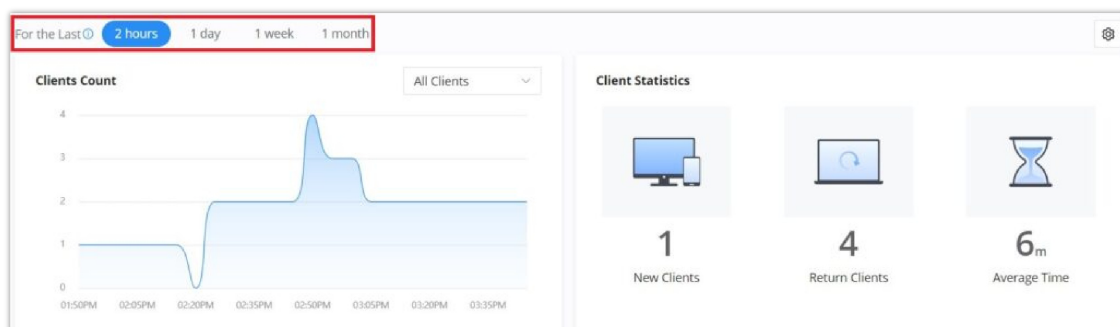
Dashboard

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


- **2 hours and one day:** Refresh and record data every 5 minutes.
- **1 week:** Refresh and record data every 30 minutes.
- **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, and refer to the figure below:

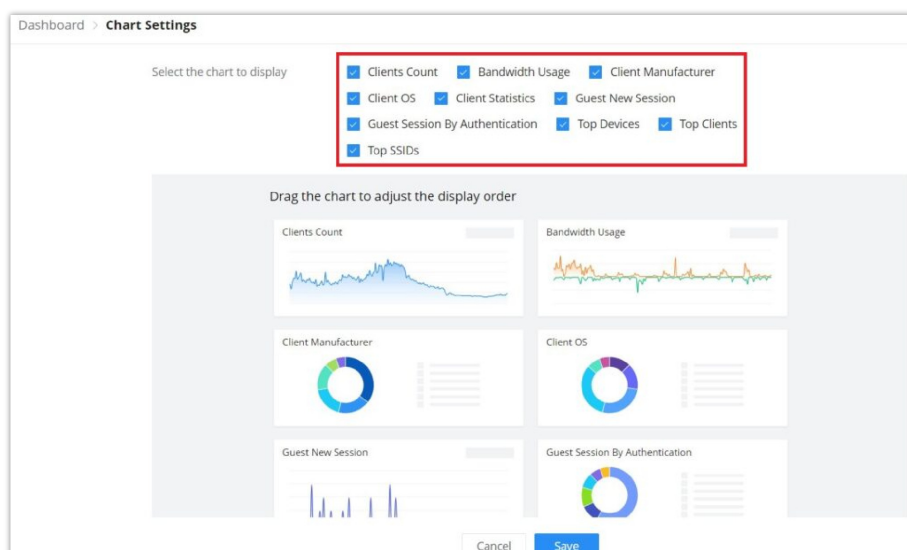
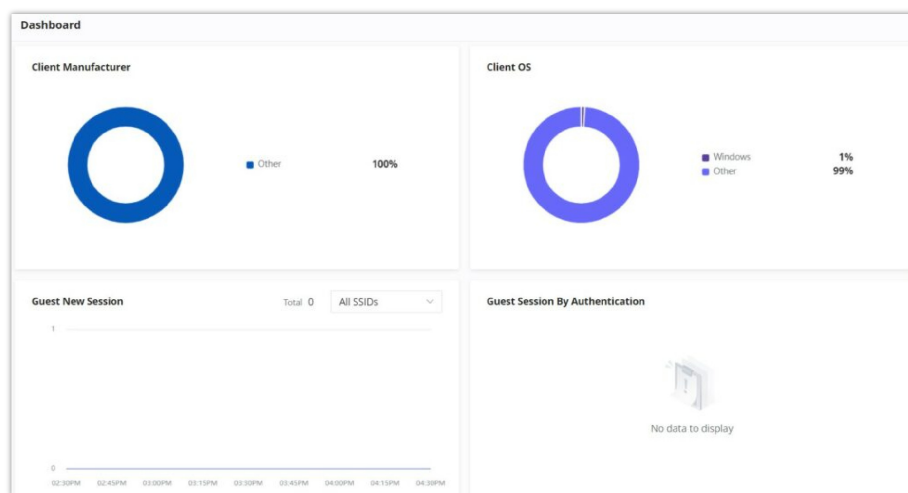


Chart Settings

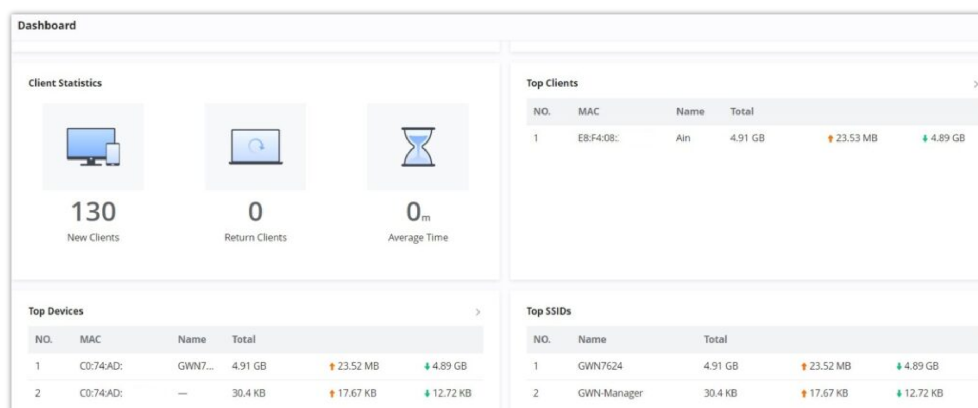
<b>Client Count</b>	It shows the number of clients connected at a specific period of time.
<b>Client OS</b>	It shows the Operating Systems used by Clients and the percentage of each.
<b>Clients Statistics</b>	Displays New Clients, Return Clients, and Average Time.
<b>Top SSIDs</b>	Displays the SSIDs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

### Chart Settings

Example:



Example 1

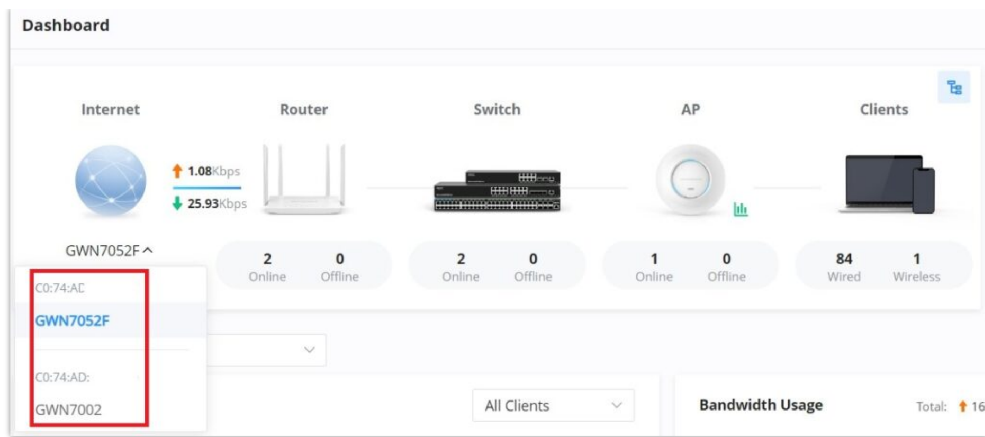


Example 2

## Network Health Monitor

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

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



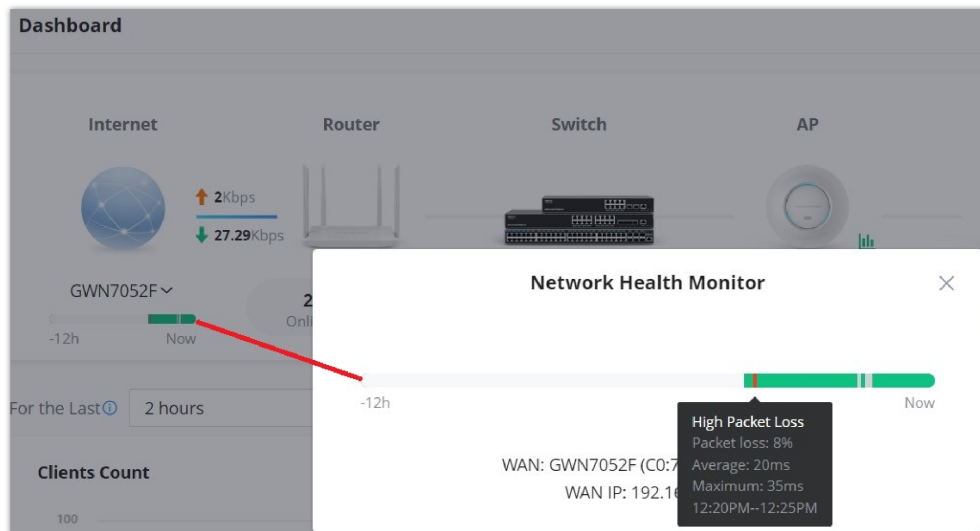
Network Health Monitor

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

**Green:** Online

**Grey:** Offline

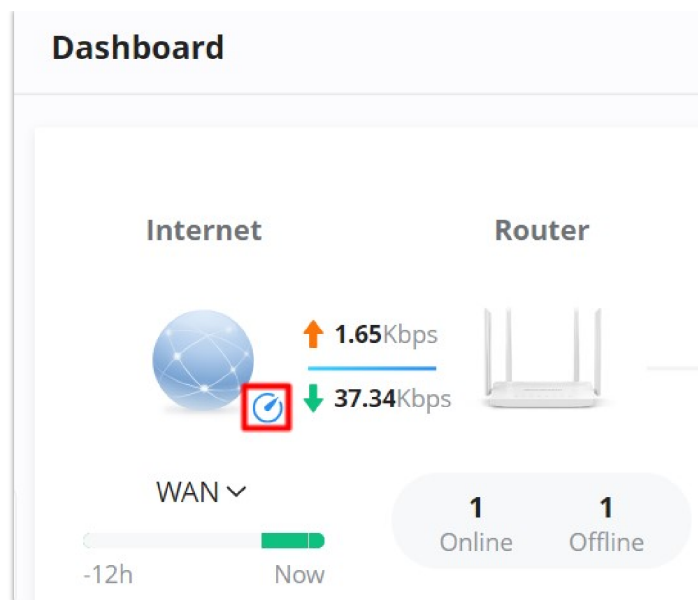
**Red:** High Packets Loss



Network Health Monitor

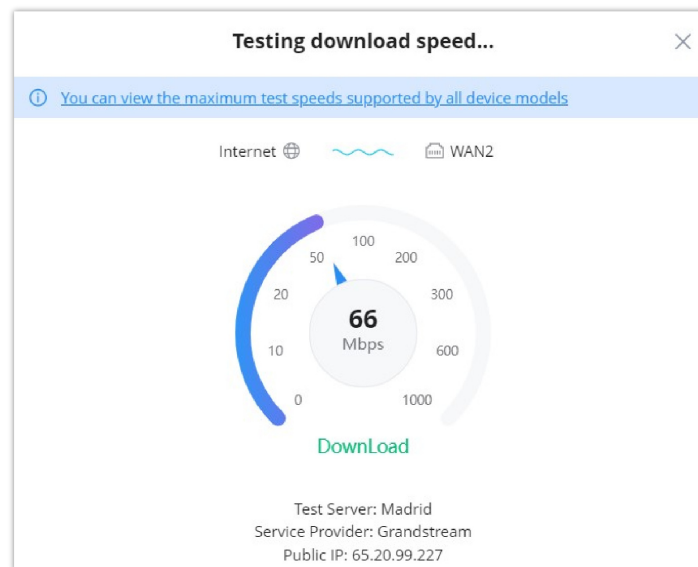
## WAN Speed Test

When a GWN router is added to the GWN Management and the WAN is added under **Settings → Internet → WAN**, The user can click on the speed test icon as shown below to run the speed test of the select WAN.



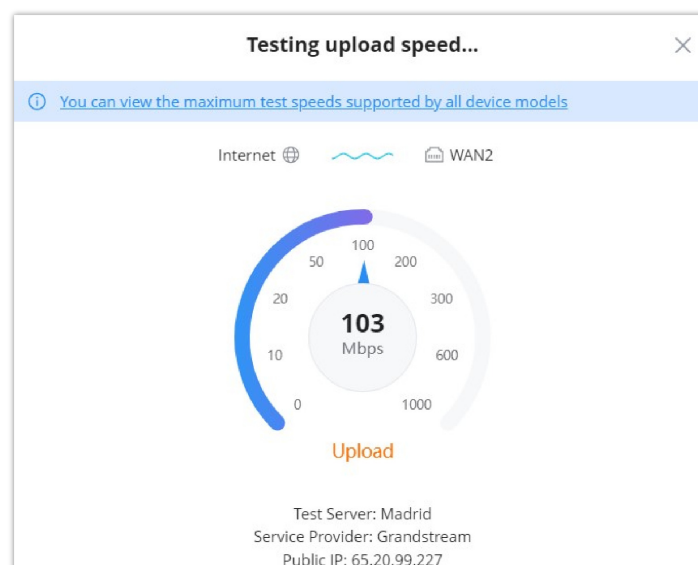
WAN Speed test

First, select the WAN under internet, then click on the speed test icon, then the download test will start.



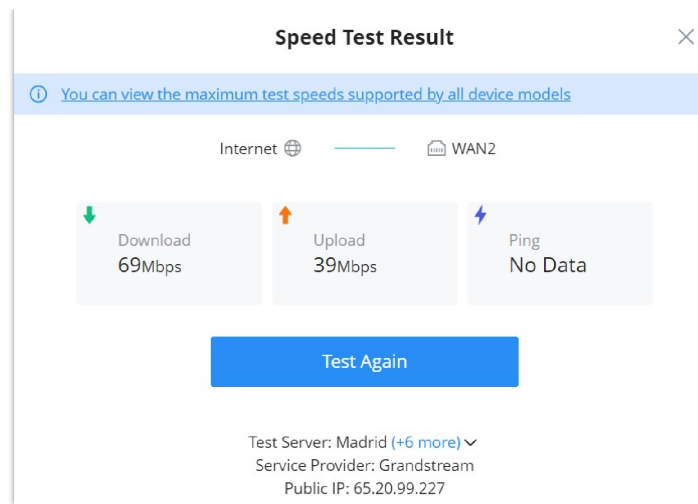
WAN Speed test – Download test

Once the download test is over, the upload test will start next.



WAN Speed test – Upload test

Finally, the speed test result will be shown with download, upload rates.



WAN Speed test – result

**Note:**

The speed test result could be affected by the hardware limitation, for more details about the maximum speed rate for each GWN device, click on the link as shown in the figure above or visit [Device Comparison page](#).

GWN Cloud									
Device Comparison You may find out the differences on GWN Cloud functions among devices (based on recommended version)									
Function	Model	GWN7600	GWN7600LR	GWN7602	GWN7605	GWN7605LR	GWN7610	GWN7615	GWN7624
DFS(CE)			✓	✓	✓	✓		✓	
SpeedTest		✓	✓	✓	✓	✓	✓	✓	✓
Maximum Speedtest Value		550Mbps	550Mbps	130Mbps	450Mbps	450Mbps	130Mbps	450Mbps	450Mbps
DFS(FCC)				✓	✓	✓		✓	✓

Device Comparison – Maximum Speedtest Value

## DEVICES

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

Also displays all the related information for the GWN devices on the current network, to add/remove columns, click on **"Parameters icon"** as shown below:

All Status		All Models		Q MAC/Name/IP/Device Group	
Channel		Tx Power		Link Speed	Operation
2.4G	1	2.4G	20dBm	1000Mb	<input checked="" type="checkbox"/> Device Model <input checked="" type="checkbox"/> Name <input checked="" type="checkbox"/> MAC <input type="checkbox"/> IP Address <input type="checkbox"/> Public IP Address <input type="checkbox"/> IPv6 Address <input type="checkbox"/> Device Group <input type="checkbox"/> Firmware <input type="checkbox"/> Uptime <input checked="" type="checkbox"/> Num of Clients <input checked="" type="checkbox"/> Usage <input checked="" type="checkbox"/> Channel <input checked="" type="checkbox"/> Tx Power <input checked="" type="checkbox"/> Link Speed
5G	44	5G	23dBm	1000Mb	
2.4G	—	2.4G	—	10Mbps	
5G	36	5G	19dBm	10Mbps	
2.4G	6	2.4G	20dBm	100Mbps	
5G	—	5G	—	100Mbps	
—	—	—	—	—	
				Total 4	10/page

Devices list – part 1

Many information can be viewed from this page:

- **Device Model**
- **Name**
- **MAC address**
- **IP address**
- **Public IP address**
- **IPv6 address**
- **Device group**
- **Firmware**
- **Uptime**
- **Number of Clients**
- **Usage**
- **Channel**: displays GWN APs used channels on all bands.
- **TX Power**: displays transmission power on wireless devices e.g. GWN APs in dBm.
- **Link Speed**: if a GWN AP is connected for example to GWN Switch on a 1Gbps port, then the link speed will be 1Gbps.

For reference, please check the examples below:

Devices									
<a href="#">Add</a> <a href="#">Export</a> <a href="#">Group Management</a> <a href="#">More</a>				All Status		All Models	Q. MAC/Name/IP/Device Group		
<input type="checkbox"/>	Device Model	Name	MAC	IP Address	Public IP Address	IPv6 Address	Device Group	Firmware	Operation
<input type="checkbox"/>	GWN7664	GWN7664	C0:74:AD:90:B2:40	192.168.80.108	192.168.5.110	—	Default	1.0.25.15	
<input type="checkbox"/>	GWN7605LR	GWN7605LR	C0:74:AD:90:B2:40	192.168.80.226	192.168.5.110	—	Default	1.0.25.10	
<input type="checkbox"/>	GWN7660LR	GWN7660LR	C0:74:AD:90:B2:40	192.168.80.25	192.168.5.110	—	Default	1.0.25.15	
<input type="checkbox"/>	GWN7813P	—	C0:74:AD:90:B2:40	192.168.80.133	192.168.5.110	—	Default	1.0.1.7	

Devices list – part 2

<input type="checkbox"/>	Device Model	MAC	Uptime	Num of Clients	Usage	Channel	Tx Power	Link Speed	Operation
<input type="checkbox"/>	GWN7664	C0:74:AD:90:B2:40 GWN7664	16m	1	5.28 MB	2.4G 1 5G 44	2.4G 20dBm 5G 23dBm	1000Mbps	
<input type="checkbox"/>	GWN7605LR	C0:74:AD:90:B2:40 GWN7605LR	42m	0	15.45 KB	2.4G — 5G 36	2.4G — 5G 19dBm	10Mbps	
<input type="checkbox"/>	GWN7660LR	C0:74:AD:90:B2:40 GWN7660LR	42m	0	1.93 KB	2.4G 6 5G —	2.4G 20dBm 5G —	100Mbps	
<input type="checkbox"/>	GWN7813P	C0:74:AD:90:B2:40	1h 2m	3	—	—	—	—	

Devices list – part 3

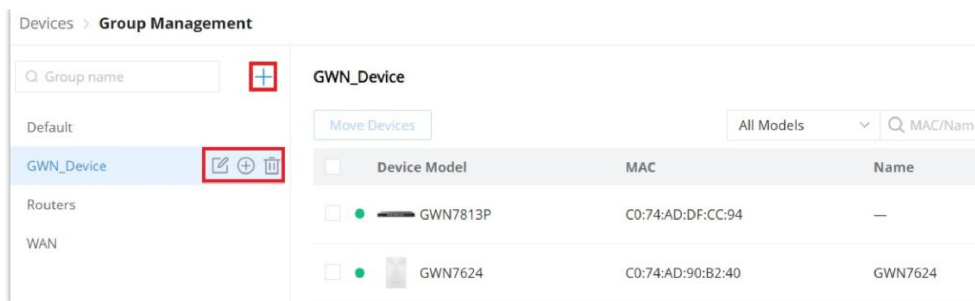
## Group Management

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 configurations 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 the **Web UI → Devices** page then click on the **“Group Management”** button.

Devices						
<a href="#">Adopt</a> <a href="#">Export</a> <a href="#">Group Management</a> <a href="#">More</a>				All Status	All Models	Q. MAC/Name/IP/Device G
<input type="checkbox"/>	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



Group Management list

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

The screenshot shows the 'Add New Device Group' form. It includes fields for 'Name' (Device Group), 'Parent Group' (Default), 'Device' (GWN7003(C0:74:AD:...) and GWN7662(C0:74:AD:...)), and 'Remark' (New Device Group). Below these is a 'Switch Pre-Provisioning' section with a note: 'Only applies to the switches added the first time.' This section contains 'Port Settings' with two rows: Port 1 (+3) with 'All VLANs' profile and 'On' Trust DHCP Snooping; and Port 5 (+1) with 'Default LAN' profile and 'Off' Trust DHCP Snooping. There's an 'Add New Item' button. A 'CLI Command' text area contains an example configuration. At the bottom are 'Cancel' and 'Save' buttons. The footer says '© 2023 Grandstream Networks, Inc.'.

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 contain wireless devices e.g.: GWN APs.
- For the Router parameter under Settings → Internet → Add WAN, the device group must contain only routers of the same mode.

## Switch Pre-Provisioning

The 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

In 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 port settings. Please refer to the figure below:

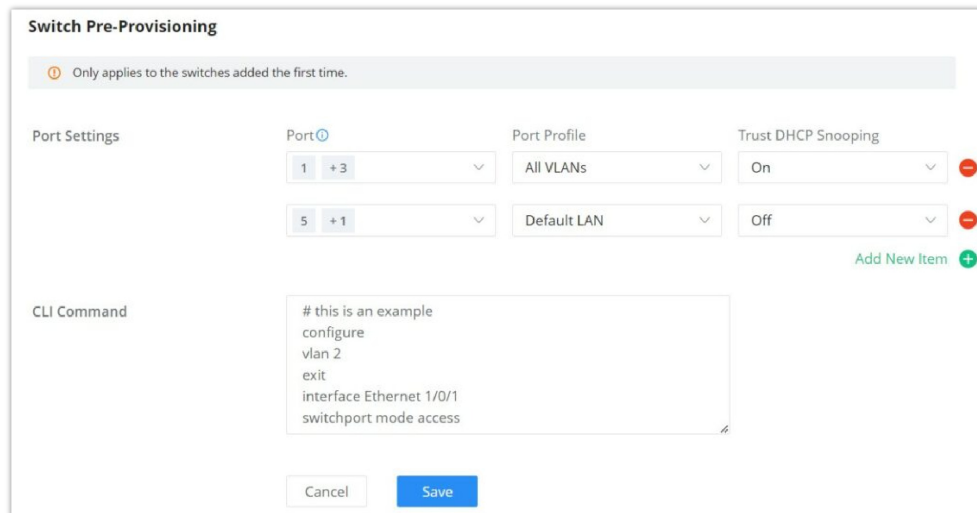


**Note:**

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 the comment line.



The 'Switch Pre-Provisioning' window includes a note: 'Only applies to the switches added the first time.' It features 'Port Settings' with two rows: the first row has '1' and '+3' in a dropdown, 'All VLANs' in a dropdown, and 'On' for 'Trust DHCP Snooping'; the second row has '5' and '+1' in a dropdown, 'Default LAN' in a dropdown, and 'Off' for 'Trust DHCP Snooping'. There are red minus icons next to the 'On' and 'Off' settings, and a green '+ Add New Item' button. The 'CLI Command' section contains a text area with the example: '# this is an example', 'configure', 'vlan 2', 'exit', 'interface Ethernet 1/0/1', 'switchport mode access'. At the bottom are 'Cancel' and 'Save' buttons.

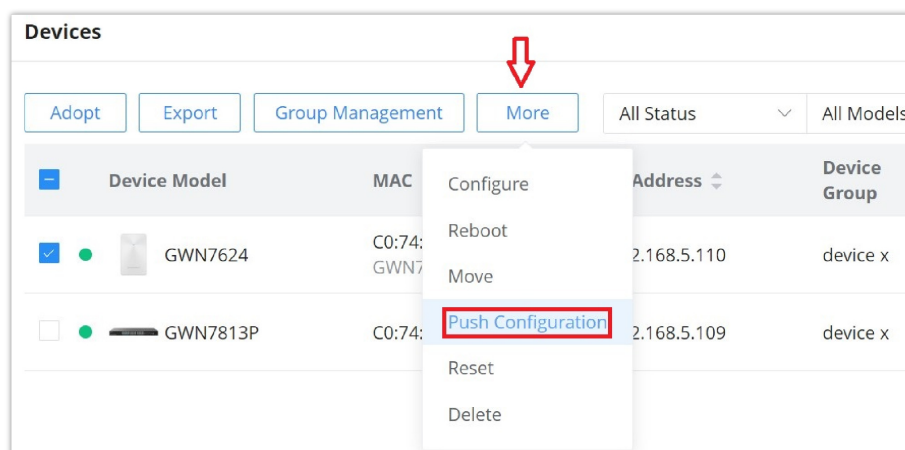
Switch Pre-Provisioning

## Push Configuration

The 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 the **"More"** button, next click on **"Push Configuration"**.



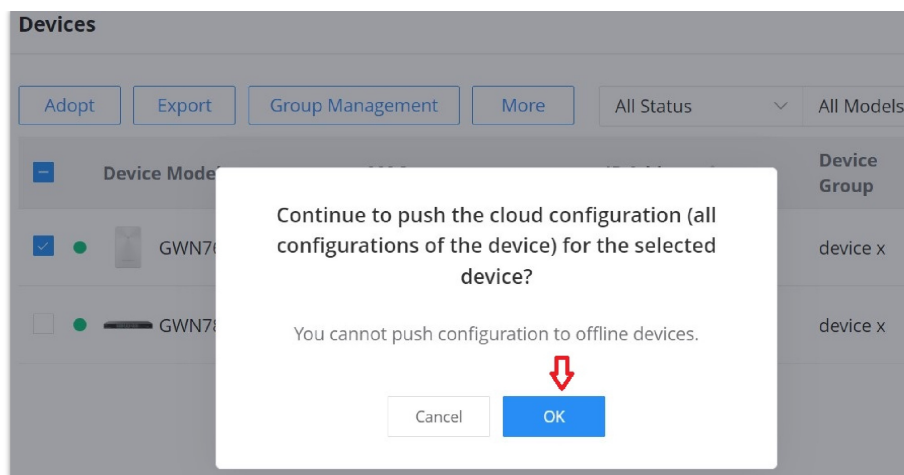
The 'Devices' page shows a table with columns: Device Model, MAC, Address, and Device Group. Two devices are listed: GWN7624 (MAC C0:74:GWN7, Address 2.168.5.110) and GWN7813P (MAC C0:74:, Address 2.168.5.109). Above the table are buttons: Adopt, Export, Group Management, and More. A red arrow points to the 'More' button. A context menu is open over the 'More' button, listing: Configure, Reboot, Move, Push Configuration (highlighted with a red box), Reset, and Delete.

Devices page – Push configuration – part 1

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

**Note:**

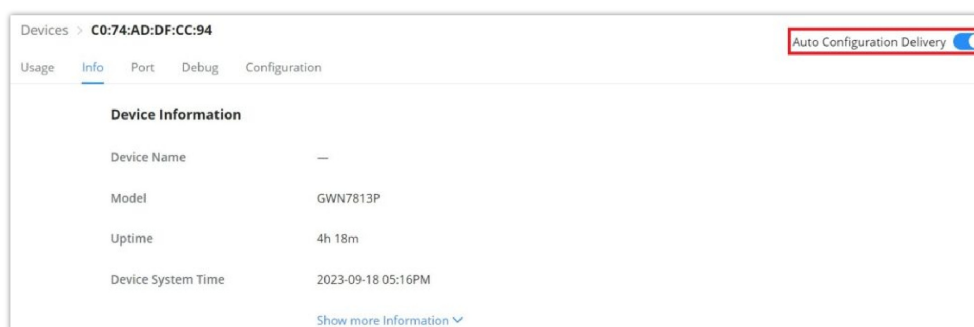
Push configuration does not work with offline GWN devices.



Devices page – Push configuration – Part 2

## Automatic Method

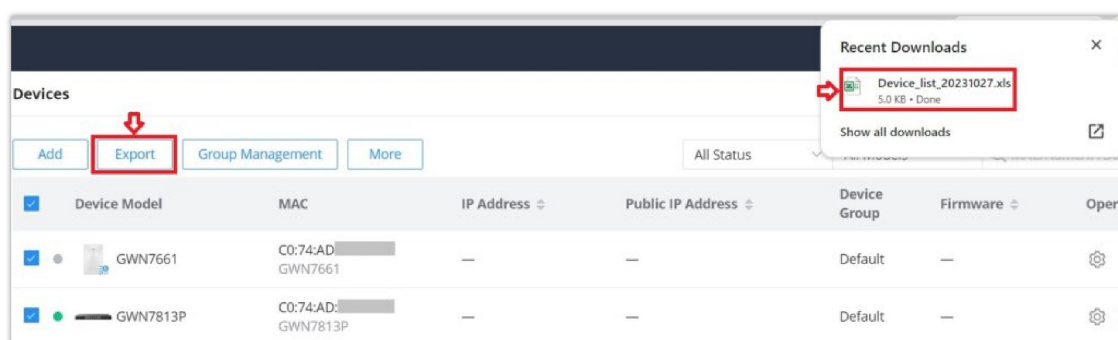
If the user wants to push the GWN.Cloud/GWN Manager configuration automatically for the selected GWN device, navigate to **Web UI → Devices** page, then click on a GWN device or configuration icon, on the top of the page toggle ON **“Auto Configuration Delivery”**, please refer to the figure below:



Auto Configuration Delivery

## Export

The user can click on the **“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

A1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Device Model	Mac	Name	IP Address	Connection IP Address	IP-v6 Address	Device Group	Firmware	Running Time	Clients Count	Usage	Channel	Tx Power	Device Remarks	Serial Number
2	GWN7860	C0:74:AD:...	—	192.168.5.94	192.168.5.94	—	Default	1.0.25.10	—	0	—	2.4G	2.4G	—	—
3	GWN7003	C0:74:AD:...	—	192.168.80.1	192.168.5.98	fe80::c274:adff:fec9:72e9	Default	1.0.5.6	3h 9m	0	—	2.4G 0	2.4G 0dBm	—	—
4	GWN7803P	C0:74:AD:...	—	192.168.5.60	192.168.5.60	—	Default	1.0.3.37	3h 10m	77	—	5G 0	5G 0dBm	—	—

Devices Export – Excel file

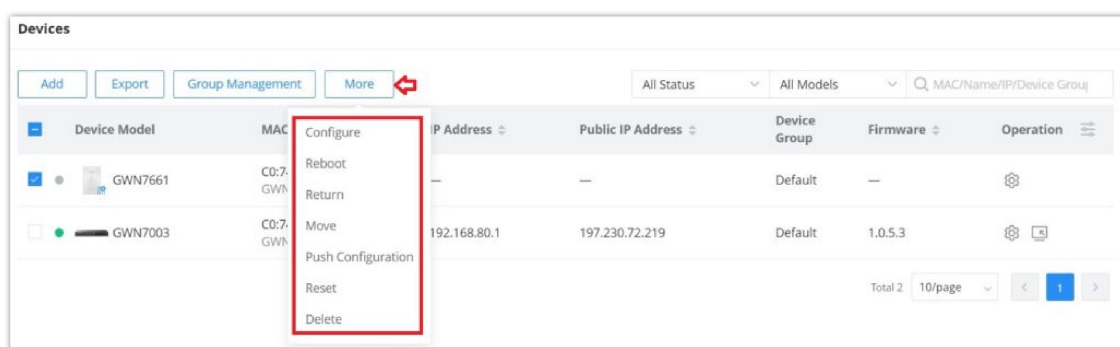
The exported file contains the following information about all the devices:

- 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 the **“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.

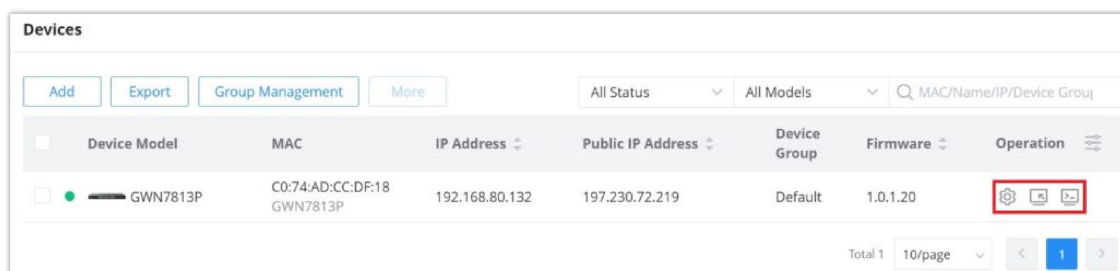
**Move:** to move a device from the current network to another network.

**Reset:** to reset a device.

**Delete:** to delete a device.

## Operation

Under Operation, the user can find more tools that can help with managing GWN devices.



*Devices – Operation*

: Click to configure the GWN device.

: Remove access to the GWN device Web UI.

: Web CLI.

```
Username: admin
Password: *****
GWN7813P#
```

Web CLI

## Configure a device

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

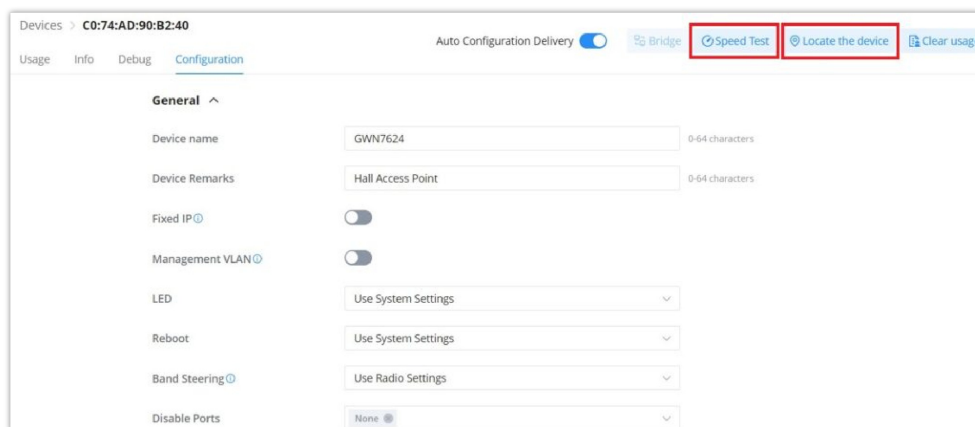
### Note:

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

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

## Configure a GWN Access Point

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



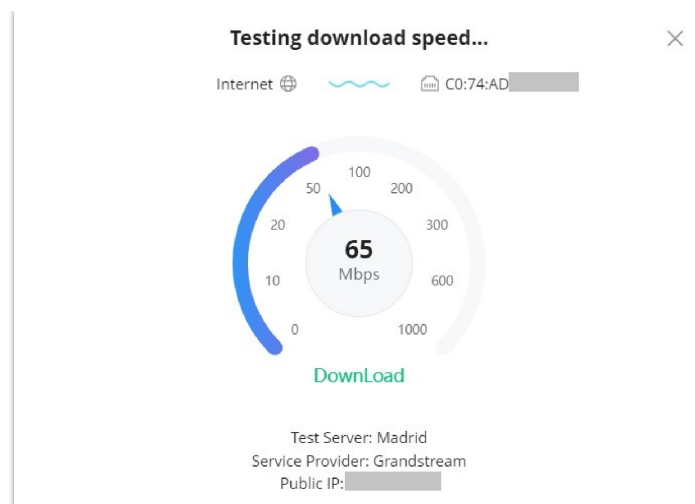
The screenshot displays the configuration interface for a GWN Access Point. At the top, there's a breadcrumb 'Devices > C0:74:AD:90:B2:40' and a toggle for 'Auto Configuration Delivery'. Navigation tabs include 'Usage', 'Info', 'Debug', and 'Configuration'. Action buttons like 'Bridge', 'Speed Test', 'Locate the device', and 'Clear usage' are visible. The 'General' section is expanded, showing various settings: 'Device name' (GWN7624), 'Device Remarks' (Hall Access Point), 'Fixed IP' (disabled), 'Management VLAN' (disabled), 'LED' (Use System Settings), 'Reboot' (Use System Settings), 'Band Steering' (Use Radio Settings), and 'Disable Ports' (None).

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:

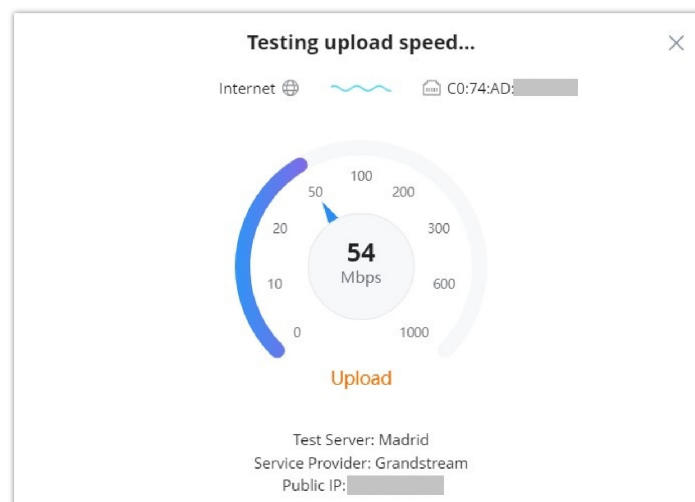
To start running the speed test, click on the “**Speed Test**” button, refer to the figure above.

The first speed test is testing download speed.



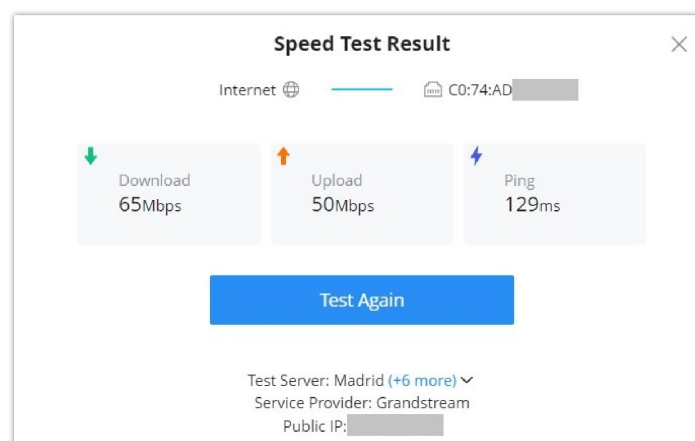
*GWN APs Speed Test – Download*

Once, the 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 the **"Test Again"** button.



*GWN APs Speed Test – Result*

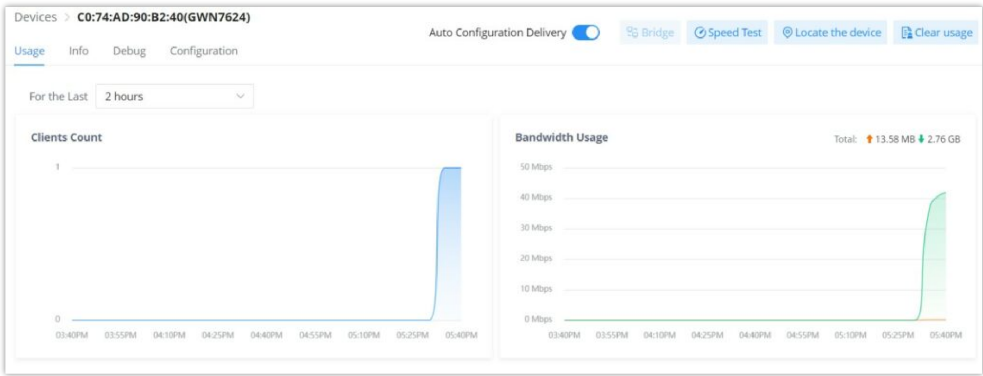
**Note:**

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

- **Locate the device:** easily locate the device by clicking on the **"Locate the device"** button, a white light will flash for 2 minutes, or click on the **"Close"** button.
- **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 month.

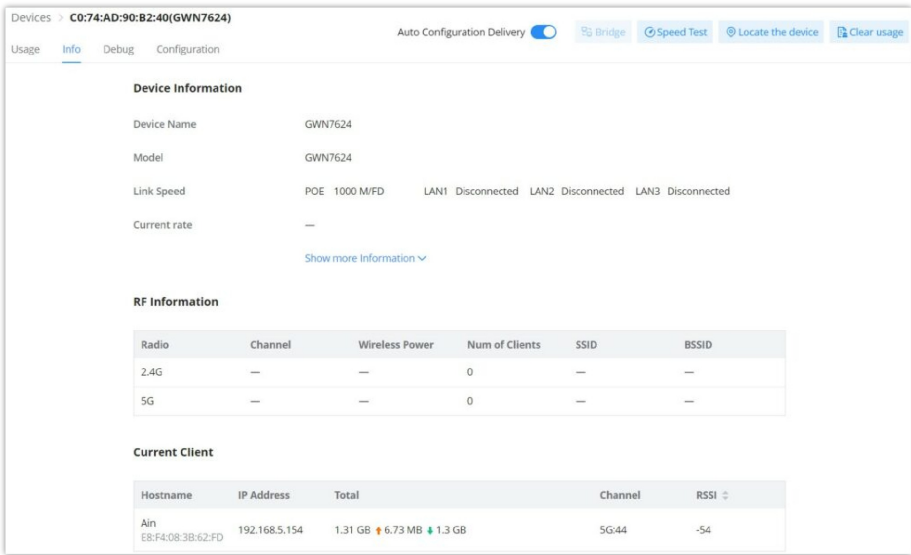
**Clear usage:** to clear collected data from the AP (Bandwidth usage and Client Count).



GWN AP – Usage

o **GWN Access point – Info**

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



GWN AP – Info

**RF Information (BSSID)**

The 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 the 2.4GHz antenna and another BSSID for the 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 the 2.4GHz antenna BSSID is C0:74:AD:XX:XX:41, and for the 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.

Devices > C0:74:AD:90:B2:40 (GWN7624)

Usage Info Debug Configuration

Bridge Locate the device Clear usage

Equipment Remarks Access Point

[Hide more Information ^](#)

Radio	Channel	Wireless Power	Num of Clients	SSID	BSSID
2.4G	1	6dbm	0	Guests	c0:74:ad:90:b2:41
5G	36	8dbm	1	Guests	c0:74:ad:90:b2:42

BSSID

#### ◦ GWN Access point – Debug

GWN APs have many debug tools to help diagnose 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.

Devices > C0:74:AD:90:B2:40 (GWN7624)

Auto Configuration Delivery ☒ Bridge Speed Test Locate the device Clear usage

Usage Info Debug Configuration

Ping/Traceroute Capture Core Files SSH Remote Access Event log

Tool IPv4 Ping

Destination IP Address/Domain 192.168.5.10

Run

```

PING 192.168.5.10 (192.168.5.10): 56 data bytes
64 bytes from 192.168.5.10: seq=0 ttl=64 time=2.255 ms
64 bytes from 192.168.5.10: seq=1 ttl=64 time=0.565 ms
64 bytes from 192.168.5.10: seq=2 ttl=64 time=0.553 ms
64 bytes from 192.168.5.10: seq=3 ttl=64 time=0.567 ms
64 bytes from 192.168.5.10: seq=4 ttl=64 time=0.567 ms

--- 192.168.5.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.553/0.901/2.255 ms
  
```

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.

Devices > C0:74:AD:90:B2:40 (GWN7624)

Auto Configuration Delivery ☒ Bridge Speed Test Locate the device Clear usage

Usage Info Debug Configuration

General

Device name GWN7624 0-64 characters

Device Remarks Hall Access Point 0-64 characters

Fixed IP ☐

Management VLAN ☐

LED Use System Settings

Reboot Use System Settings

Band Steering Use Radio Settings

Disable Ports None

VLAN (LAN1) Please enter VLAN ID

VLAN (LAN2) Please enter VLAN ID

VLAN (LAN3) Please enter VLAN ID

2.4GHz

2.4GHz ☒

Back Save

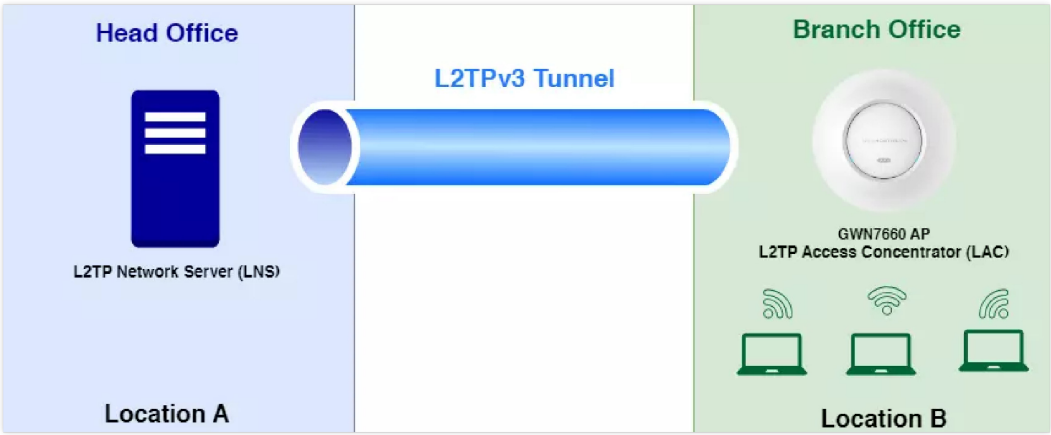
GWN AP – Configuration

**Note:**

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

◦ **GWN AP L2TPv3**

L2TPv3 (Layer 2 Tunneling Protocol version 3) is a versatile protocol widely utilized for tunneling Layer 2 traffic over IP networks. When implemented on GWN Access Points acting as L2TP Access Concentrators (LACs) connecting to a central L2TP Network Server (LNS), it enables seamless and secure communication for wireless clients.



L2TPv3 Diagram

GWN Access Points, known for their reliability and performance, acting as LACs establish tunnels to the LNS, facilitating the encapsulation and transmission of all wireless clients’ Layer 2 traffic. This architecture proves particularly beneficial in centralized network models where VLANs extend from corporate environments to remote branch sites.

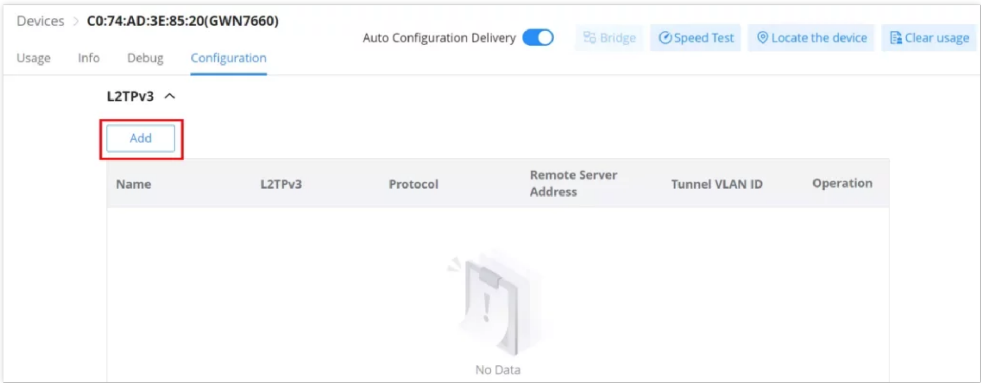
By leveraging L2TPv3, wireless clients associated with GWN Access Points are seamlessly integrated into the corporate network infrastructure. They receive IP addresses dynamically from the DHCP server hosted on the LNS, ensuring efficient network resource allocation and management.

This integration empowers organizations with scalable and secure wireless connectivity solutions, optimized for various deployment scenarios. Whether for small businesses or enterprise environments, the utilization of L2TPv3 on GWN Access Points offers a robust framework for extending network capabilities while maintaining high levels of performance and security.

**Note:**

This feature is only supported on GWN7660 and GWN7660LR.

To add a L2TPv3 tunnel, click on “**Add**” button as shown below:



L2TPv3

**Note:**

It is best to set the MTU to match the server to avoid network connectivity issues.

Please refer to the figure and table below:



Add L2TPv3

×

\*

Name

1-32 characters

L2TPv3 Tunnel

L2TPv3

Protocol

IP

UDP

\*

Remote Server Address

197.99.53.22

\*

Local Tunnel ID

1-4294967295 numbers

1111

\*

Remote Tunnel ID

1-4294967295 numbers

7

Add L2TPv3 – part 1

\*

Local Session ID

1-4294967295 numbers

5

\*

Remote Session ID

1-4294967295 numbers

3

Local Cookie

Supports 8-bit or 16-bit hexadecimal strings

Remote Cookie

Supports 8-bit or 16-bit hexadecimal strings

MTU

576-1500 numbers

1500

\*

Tunnel VLAN ID

Valid range is 2-4093, excluding 666

2

Cancel

Save

Add L2TPv3 – part 2

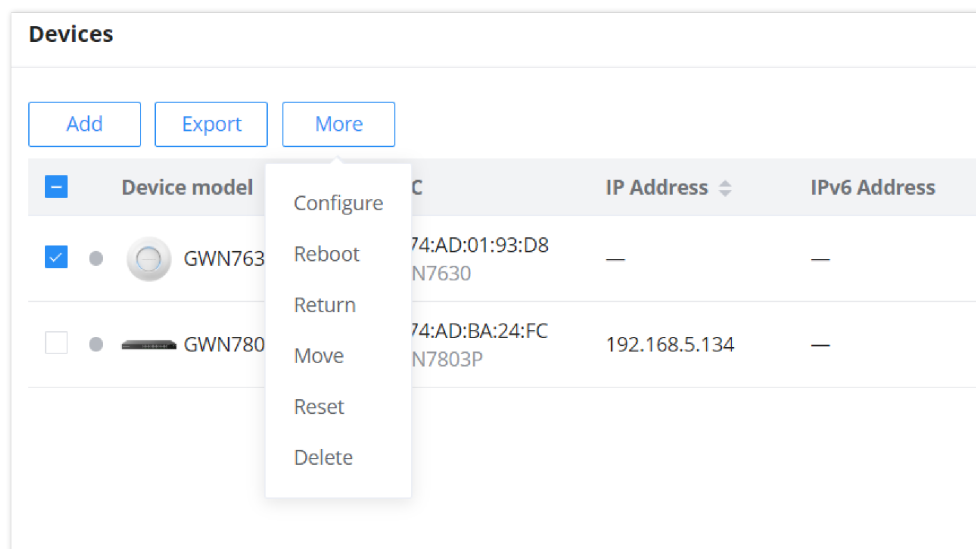
<b>Name</b>	Set the name of the tunnel.
<b>L2TPv3</b>	Enable/Disable the tunnel.
<b>Protocol</b>	Set the encapsulation type of the tunnel. Valid values for encapsulation are: <b>UDP, IP</b> .
<b>Remote Server Address</b>	Set the IP address of the remote peer.
<b>Local Tunnel ID</b>	Set the tunnel id, which is a 32-bit integer value. This uniquely identifies the tunnel.
<b>Remote Tunnel ID</b>	Set the peer tunnel id, which is a 32-bit integer value assigned to the tunnel by the peer.
<b>Local Session ID</b>	Set the session id, which is a 32-bit integer value. This uniquely identifies the session being created. The value used must match the <code>peer_session_id</code> value being used at the peer.
<b>Remote Session ID</b>	Set the peer session id, which is a 32-bit integer value assigned to the session by the peer. The value used must match the <code>session_id</code> value being used at the peer.

<b>Local Cookie</b>	Set an optional cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the peer_cookie value set at the peer. The cookie value is carried in L2TP data packets and is checked for expected value at the peer. Default setting is no cookie used.
<b>Remote Cookie</b>	Set an optional peer cookie value to be assigned to the session. This is a 4 or 8 byte value, specified as 8 or 16 hex digits, e.g. 014d3636deadbeef. The value must match the cookie value set at the peer. It tells the local system what cookie value to expect to find in received L2TP packets. Default is no cookie used.
<b>MTU</b>	Set the MTU. <i>Note: Please make sure the MTU values are consistent with the INS values.</i>
<b>Tunnel VLAN ID</b>	Specify the VLAN ID <i>Note: The tunnel ID must be set in SSID, and make sure that SSID only has the AP(s) who enabled L2TPv3.</i>

*Add L2TPv3*

### Configure GWN Access Points in Batches

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



*Batch Configuration of GWN Access Points*

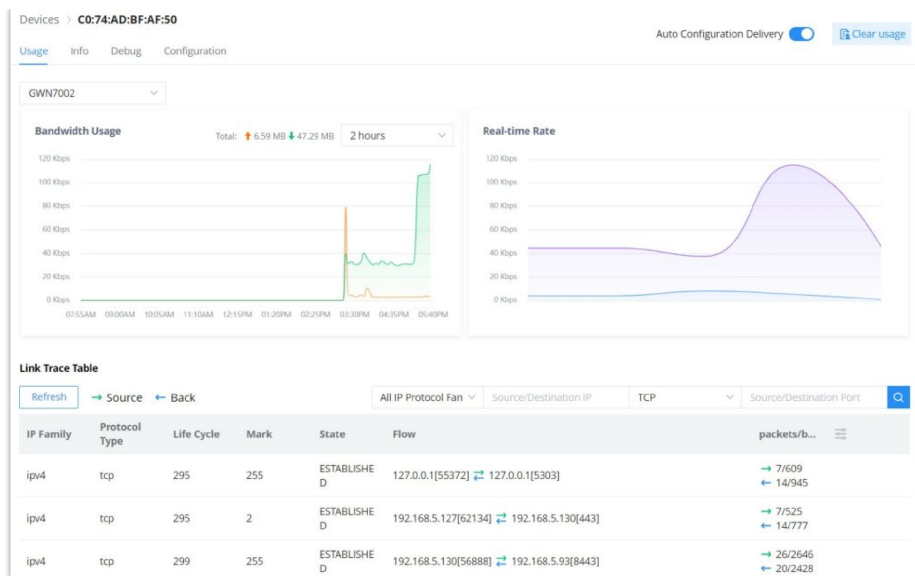
#### Note:

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

### Configure a GWN Router

#### o GWN Router – Usage

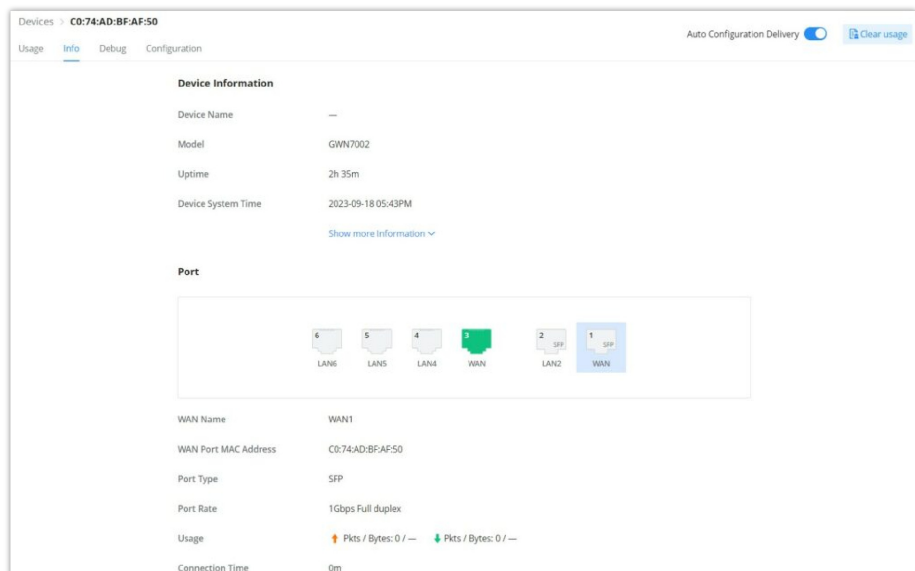
Same as the GWN AP usage tab, on this page, the user can find usage related to the GWN Router, like bandwidth usage, Real-time Rate, and even a Link Trace Table for detailed traffic data. Please refer to the figure below:



GWN Router – Usage

### o GWN Router – Info

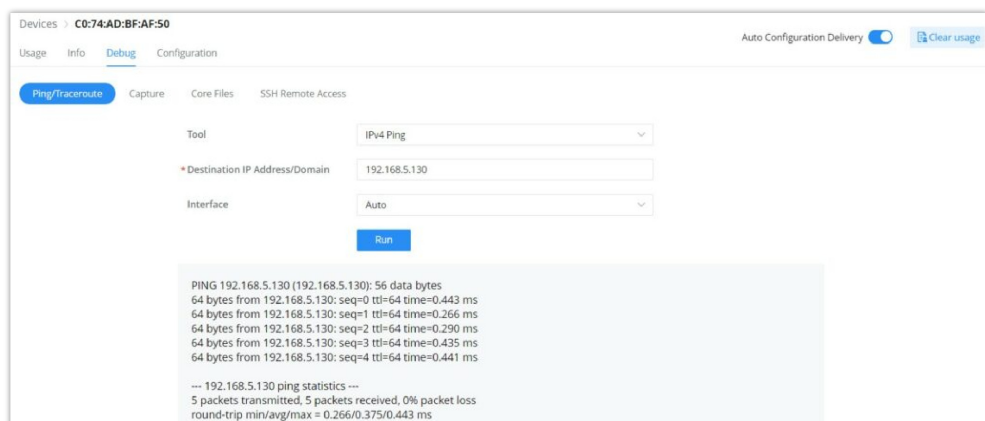
All the information related to the GWN router can be found here, including Device information (name, firmware, etc), GWN router ports' status (active ports), and information about IPv4 and IPv6 (IP address, DNS, etc).



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

The screenshot shows the 'Configuration' tab for a device with MAC address C0:74:AD:BF:AF:50. It includes sections for General settings (Device name, Device Remarks, LED, Reboot), Network Acceleration, Port configuration (Physical Port, Port Mode, Status, Port Configuration), and a VLAN Interface table with columns for VLAN, IPv4 Address/Prefix Length, IPv6, IPv6 Address Prefix/Prefix Length, and Operation. Buttons for 'Add', 'Back', and 'Save' are visible.

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 turns 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 the **“Add”** button or configure a previously created one by clicking on the **“Configure icon”** under operation, refer to the figure below:

This screenshot highlights the 'VLAN Interface' section within the router configuration. It shows a table with existing interfaces: '20(Guests)' with IP 192.168.20.1/24 and '30(Office)' with IP 192.168.30.1/24, both with disabled IPv6. A red box and arrow point to the 'Add' button. Another red arrow points to the 'Configure icon' (gear) in the 'Operation' column for the '30(Office)' interface.

GWN Router configuration – VLAN Interface

Then, select the VLAN from the list or visit the [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.

✕

### Configure VLAN Interface

○ 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.

**\* VLAN** ⓘ

30(Office) ▼

**\* IPv4 Address/Prefix Length**

Prefix length range 8-30

192.168.30.1 / 24

IPv6 ☐

*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

### ○ GWN Switch – Usage

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

Devices > C0:74:AD:DF:CC:94
Auto Configuration Delivery ☒

Usage
Info
Port
Debug
Configuration

Traffic Statistics
PoE Ports

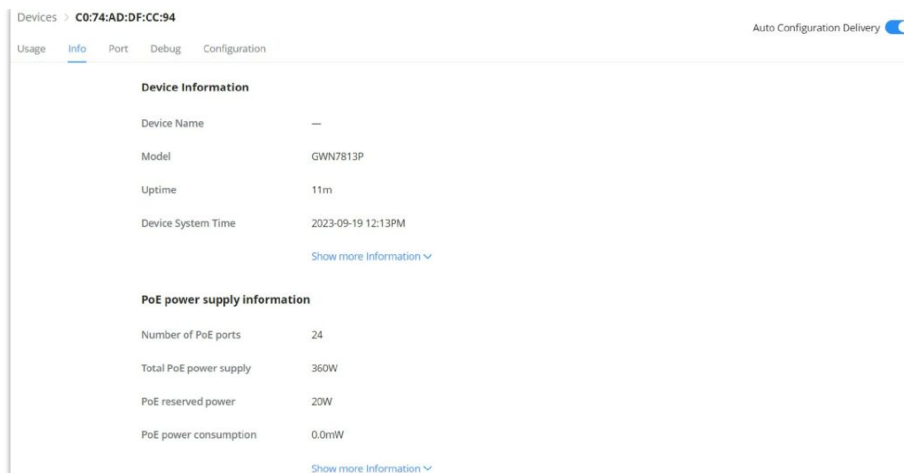
Clear Traffic
Statistical Interval ⓘ 10 second(s) ▼
All Ports ▼

Port	Receive Rate	InOctets	InPackets	InErrPackets	Transmit Rate	OutOctets	OutPackets	OutErrPackets	Operation
1/0/1	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/2	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/3	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/4	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/5	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/6	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/7	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️
1/0/8	0.0 bps	0 B	0	0	0.0 bps	0 B	0	0	🗑️

*GWN Switch – Usage*

### ○ GWN Switch – Info

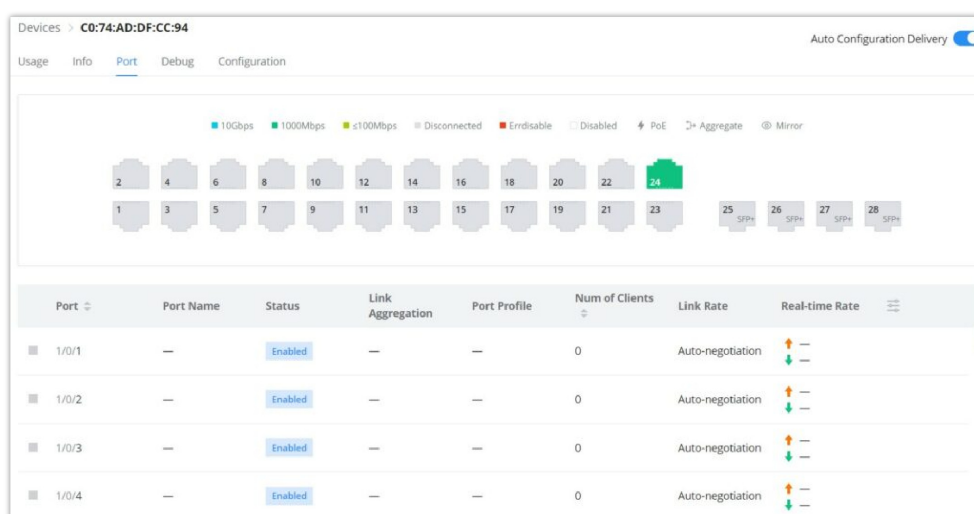
Relevant GWN switch information or PoE power supply information can be found here.



GWN Switch – Info

#### ◦ GWN Switch – Port

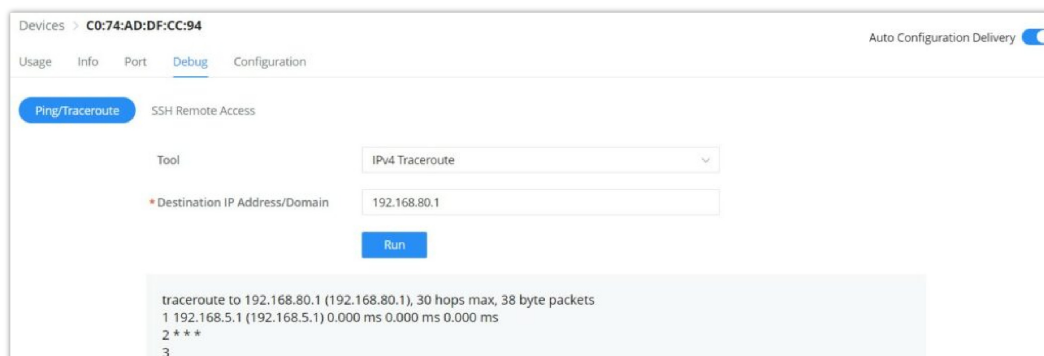
On the Port tab, under devices configuration only for GWN switches, the user can view GWN switch ports status and also configure them (enable/disable a port, Link Aggregation, Port Mirroring, etc). Please refer to the figure below:



GWN Switch – Port

#### ◦ GWN Switch – Debug

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



GWN Switch – Debug

#### ◦ GWN Switch – Configuration

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

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

Devices > C0:74:AD:DF:CC:94 Auto Configuration Delivery ☒

Usage Info Port Debug Configuration

Device name: GWN7813P (0-64 characters)

Device Remarks: Testing Switch (0-64 characters)

RADIUS Authentication: Use global LAN settings

Device Password: (8-32 characters, must include two of the following: numbers, letters and special characters)

**VLAN Interface**

All Types ▾

VLAN ▾	Status	Type	IP Address	IPv6	IPv6 Local Link Address	IPv6 Global Unicast Address	Operation
--------	--------	------	------------	------	-------------------------	-----------------------------	-----------

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 the **"Add"** button or click on the **"Configure icon"** to edit a previously added one. Refer to the figure below:

Devices > C0:74:AD:BA:24:FC Auto Configuration Delivery ☒

Usage Info Port Debug Configuration





Device Remarks: (0-64 characters)

RADIUS Authentication: Use global LAN settings

Device Password: (8-32 characters, must include two of the following: numbers, letters and special characters)

**VLAN Interface**

All Types ▾

VLAN ▾	Status	Type	IP Address	IPv6	IPv6 Local Link Address	IPv6 Global Unicast Address	Operation
40(Test Unit)	Down	Dynamic	—	Disabled	—	—	
20(Guests)	Down	Dynamic	0.0.0.0	Disabled	—	—	 
30(Office)	Down	Static	192.168.30.1	Disabled	—	—	 

GWN Switch configuration – VLAN Interface

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

**Configure VLAN Interface**

✕

**\* VLAN** ⓘ

30(Office)
▼

**IPv4 Address Type**

☒ Static IP
☐ DHCP

**\* IPv4 Address/Prefix Length**

Prefix length range 8-30

192.168.30.1

/

24

**IPv6** ☐

Cancel

Save

*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:

Export

Now Online
All Clients
Q

Hostname	Connection	SSID	VLAN ID	IP Address	Total	RSSI	Associated Devices	Station Mode	Conne Time
<span style="color: green;">●</span> Ain	Wireless	GWN76...	1	192.168.5.154	690.59 KB	-55	GWN7624 C0:74:AD:...	11AC_VH...	1h28m
<span style="color: green;">●</span>	Wired	—	1	192.168.0.1	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	—	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	—	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	—	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	—	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	—	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	Wired	—	1	192.168.5.113	—	—	C0:74:AD:...	—	0m
<span style="color: green;">●</span>	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*

To make it easier for the users to find the connected clients, it's possible to filter by wired clients or wireless clients and even by SSID e.g. (Office, Guests ...), please refer to the figure below:

Export

Now Online
All Clients
Q

Hostname	Connection	SSID	VLAN ID	IP Address	Total	Link Rate	Associated Devices	Station Mode	Connection Time	Operation
<span style="color: green;">●</span> C0:74:AD:...	Wired	—	1	—	—	—	C0:74:AD:...	—	0m	⚙
<span style="color: green;">●</span> C0:74:AD:...	Wired	—	1	192.168.80.1	—	—	C0:74:AD:...	—	0m	⚙
<span style="color: green;">●</span> E8:F4:08:...	Wireless	Office	1	192.168.80.235	100.39 MB	0Mbps	C0:74:AD:...	—	0m	⚙
<span style="color: green;">●</span> 5E:B8:69:...	Wireless	Office	—	—	—	0Mbps	GWN7660 C0:74:AD:5A:61:E4	—	0m	⚙

All Clients
⌵

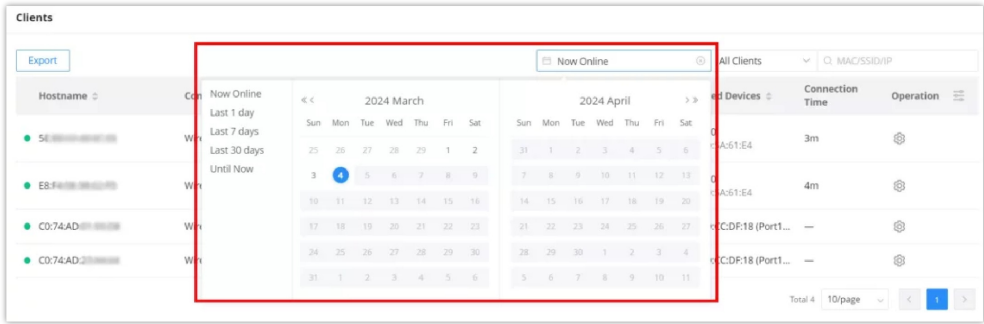
All Clients
Wired Clients
Wireless Clients
All SSIDs
Office
Guests

*Clients Page – sorting*



The same way, users can filter clients by wired and wireless connections, they also can filter by time (calendar), many options are available:

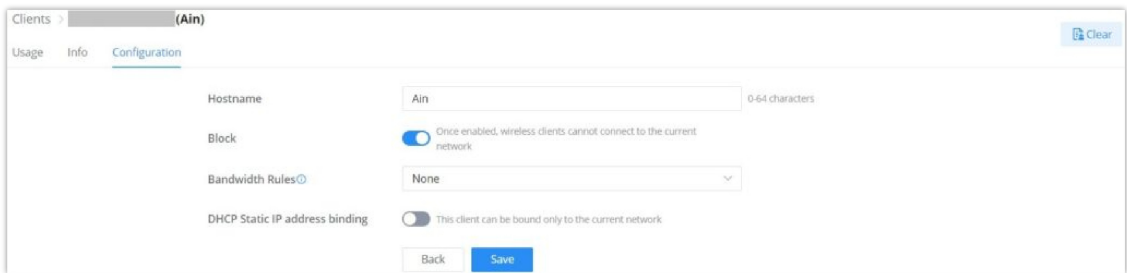
- **Now Online:** displays currently connected clients.
- **By day:** displays connected clients from a past day selected from the calendar.
- **Last 1 day:** displays connected clients of the last day.
- **Last 7 Days:** displays connected clients of the last 7 days.
- **Last 30 days:** displays connected clients of the last 30 days.
- **Until Now:** displays all connected clients until the current moment.



Clients Page – calendar

### 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.

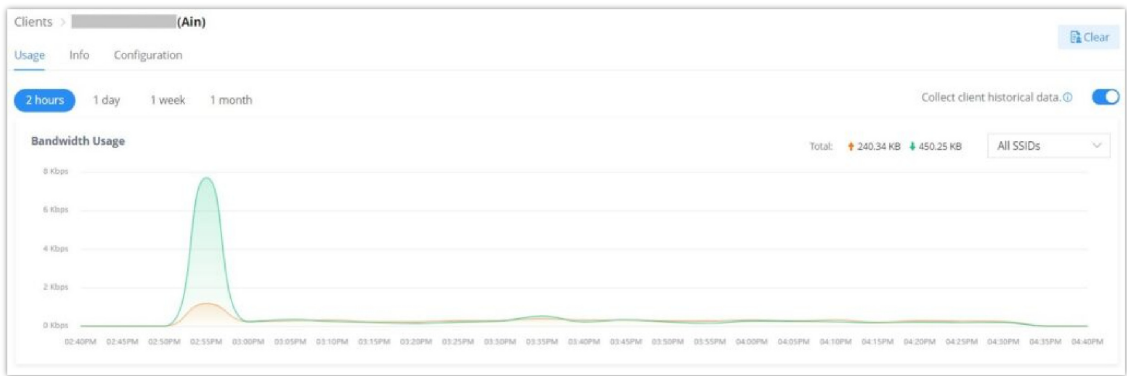


Client – Configuration

### 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  to clear the data.

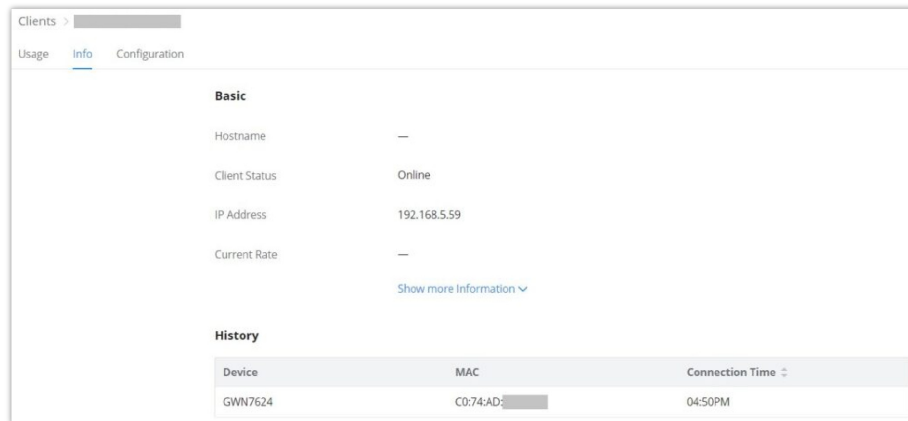


Client Usage

### Client info

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

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



History		
Device	MAC	Connection Time
GWN7624	C0:74:AD:...	04:50PM

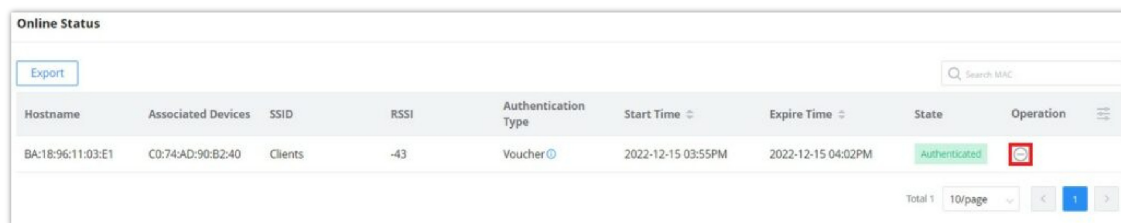
Client Info

## GUESTS

### Online Status

This page displays information about the clients connected via the 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.

The 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 the "Export" button, and selecting the export time period for all users which connected to the captive portal during that period.



Hostname	Associated Devices	SSID	RSSI	Authentication Type	Start Time	Expire Time	State	Operation
BA:18:96:11:03:E1	C0:74:AD:90:B2:40	Clients	-43	Voucher	2022-12-15 03:55PM	2022-12-15 04:02PM	Authenticated	

Guests – Online Status

### Voucher

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

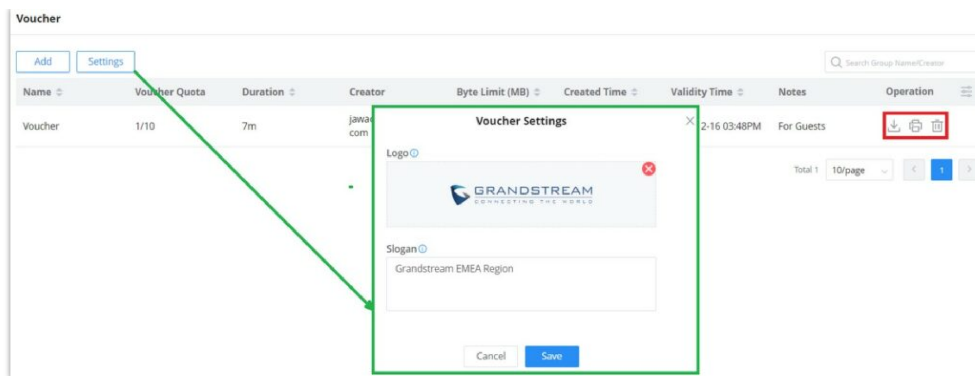
As an example, a coffee shop could offer internet access to customers via Wi-Fi using voucher codes that can be delivered on each command. Once the voucher expires the client can no longer connect to the internet.

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

Another interesting feature is that the admin can set data bandwidth limitations 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.



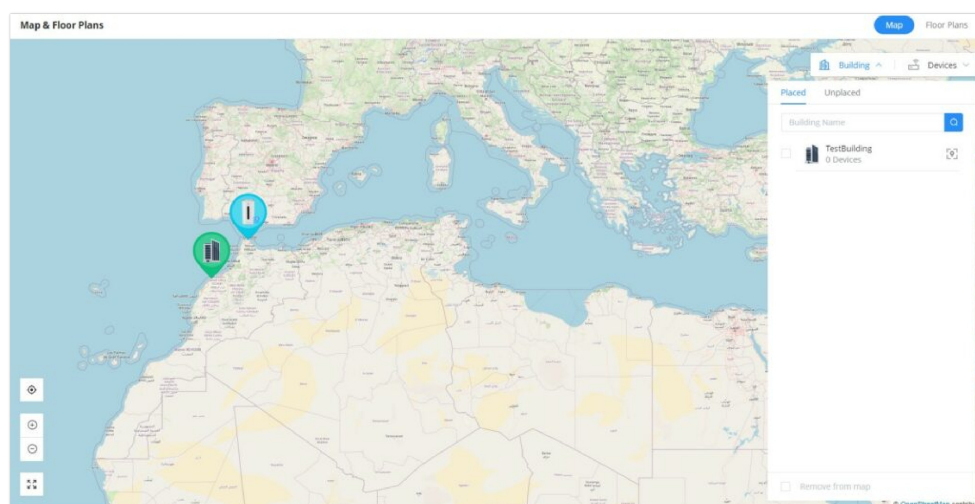
*Voucher page*

## 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 the **"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.

Placed **Unplaced**

Search MAC/Name

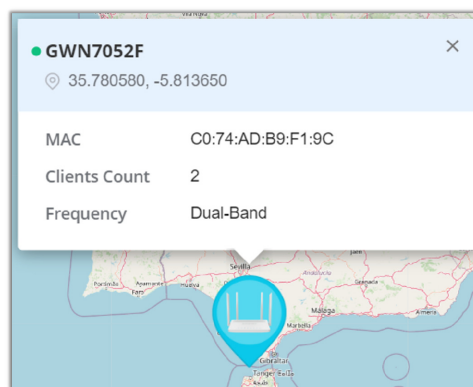
☒


GWN7052  
C0:74:AD:95:12:90



☒ Place on map

Unplaced devices




Placed GWN device


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

**Placed** Unplaced

Search MAC/Name

☒


GWN7801P  
C0:74:AD:B9:3C:A7



☒ Remove from map

Placed devices

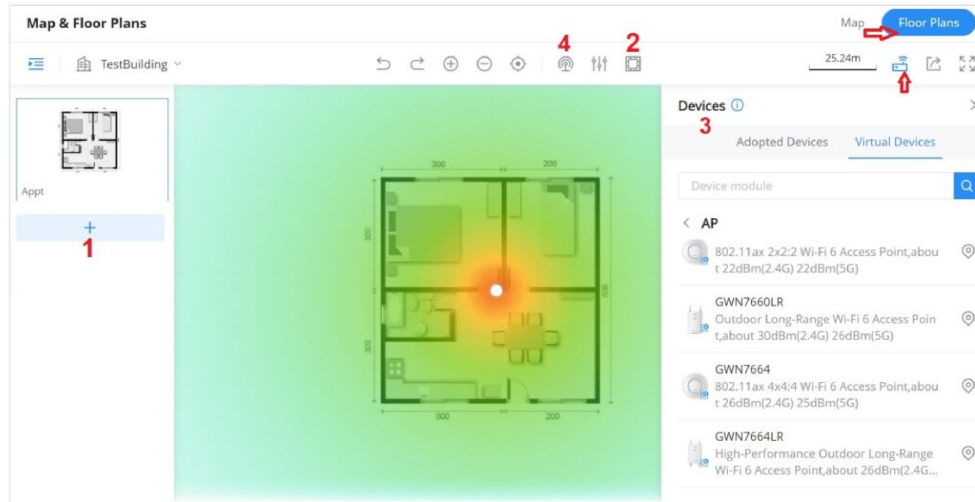
**Note:**

GWN management supports Open Street and Google Maps.

## Floor Plans

The 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 the area, and an 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:

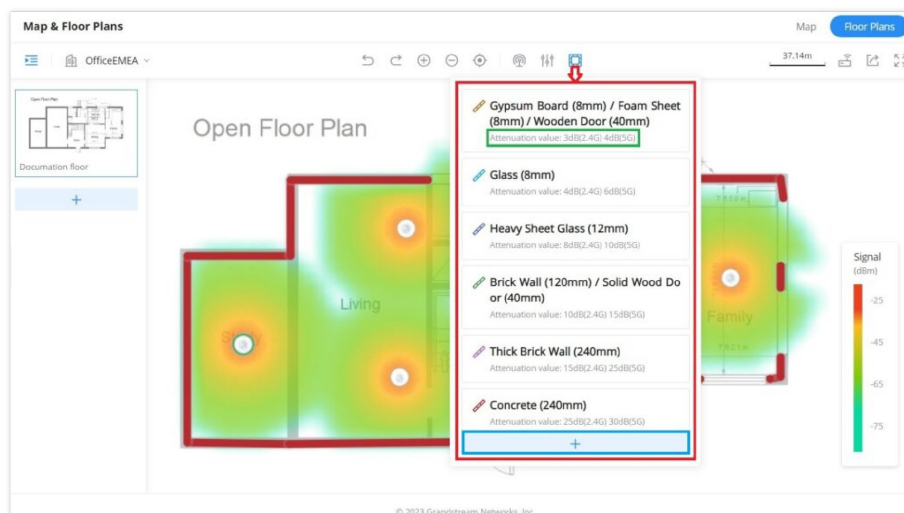


Floor Plans

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

The walls and dividers available are:

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



Floor Plans – Wall Types

Click on the "+" button as shown above to add a custom wall or a divider.

**Map & Floor Plans** Map Floor Plans

**Add New Wall**

\* Name:  Support 1-64 characters.

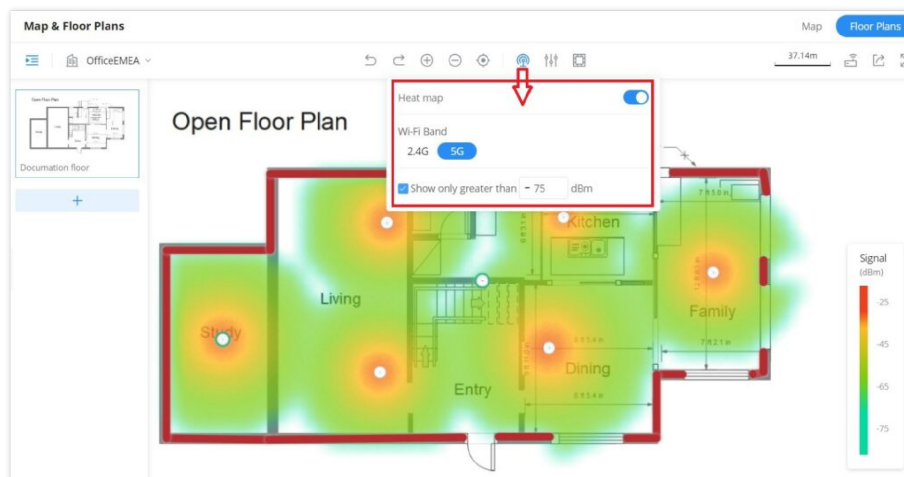
Wall Color:

\* 2.4G Attenuation (dB):  Range 0-100

\* 5G Attenuation (dB):  Range 0-100

*Floor Plans – Custom wall or divider*

1. Under devices, please select the GWN device either from adopted ones or virtual ones then place it 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 signals 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 to help the administrator 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.

**Site Survey**

All Time | 2.4G&5G |

SSID	BSSID	Channel	Protocol	Bandwidth	Encryption	Manufacturer	Num of APs	Scanned by	RSSI	Last Seen
Meeting	9C:C9:EB:00:00:00	5G	802.11ac	80	WPA2	Netgear	1	C0:74:AD:90:B...	-92	2022-12-15 11...
Office-Wireless	40:33:06:00:00:00	5G	802.11ac	80	WPA2	TP-Link	1	C0:74:AD:90:B...	-88	2022-12-15 11...
Office-Wi-Fi	B8:50:D1:00:00:00	5G	802.11ac	40+	WPA2	TP-Link	1	C0:74:AD:90:B...	-95	2022-12-15 11...
Office-Wi-Fi-2	C0:74:AD:90:00:00	5G	802.11ac	80	WPA2	TP-Link	1	C0:74:AD:90:B...	-91	2022-12-15 11...
Office-Wi-Fi-3	B4:3D:C8:00:00:00	5G	802.11n/a	20	WPA2	TP-Link	1	C0:74:AD:90:B...	-88	2022-12-15 11...
Office-Wi-Fi-4	FC:4B:09:00:00:00	5G	802.11ac	80	WPA2	TP-Link	1	C0:74:AD:90:B...	-90	2022-12-15 11...
Office-Wi-Fi-5	B8:50:D1:00:00:00	5G	802.11ac	40+	WPA2	TP-Link	1	C0:74:AD:90:B...	-95	2022-12-15 11...
Office-Wi-Fi-6	B8:50:D1:00:00:00	5G	802.11ac	40+	Open	TP-Link	1	C0:74:AD:90:B...	-92	2022-12-15 11...
Office-Wi-Fi-7	C6:74:AD:90:00:00	5G	802.11ac	80	Open	TP-Link	1	C0:74:AD:90:B...	-91	2022-12-15 11...
Office-Wi-Fi-8	B4:3D:C8:00:00:00	5G	802.11n/a	20	Open	TP-Link	1	C0:74:AD:90:B...	-88	2022-12-15 11...

Total 117 | 10/page | 1 2 3 4 5 6 ... 12

*Site Survey*

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


## Network Topology

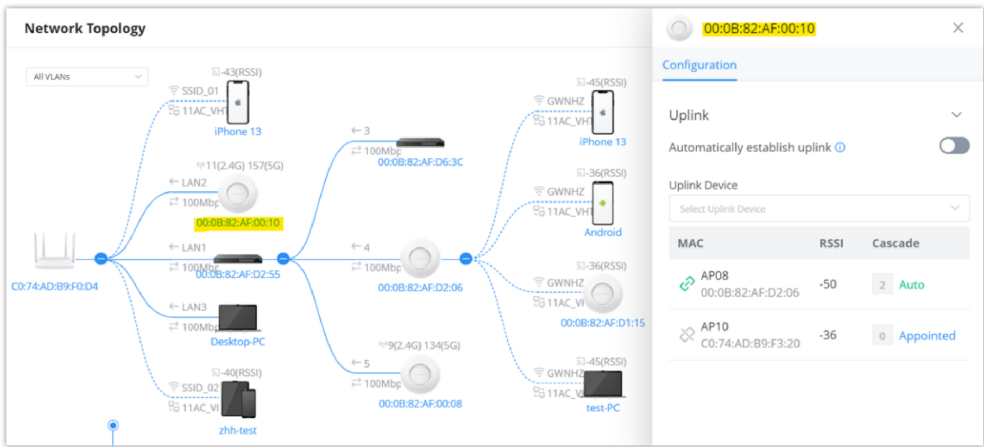
Network Topology shows an overview of the whole network starting from the GWN Router (Internet access) including GWN Switches and Access Points as well as Clients, this way the administrator/monitor can have very quickly an overview of the network at a glance. By clicking on a GWN device or a Client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

## Features overview:

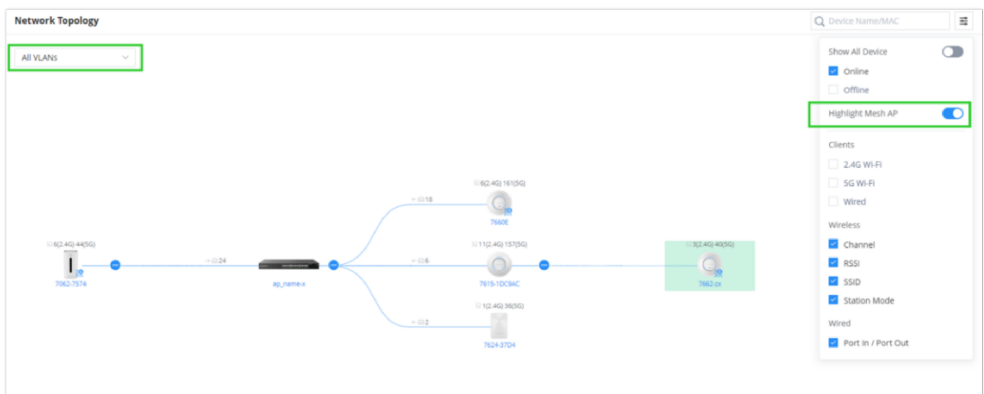
- Display network layout
- Visualize gateway, switch, access point, and connected client device information
- The topology map can be zoomed in, and out, and nodes are retractable
- Support Mesh AP and also the option to Highlight Mesh AP
- VLAN information filtering

### Notes:

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



## Network Topology

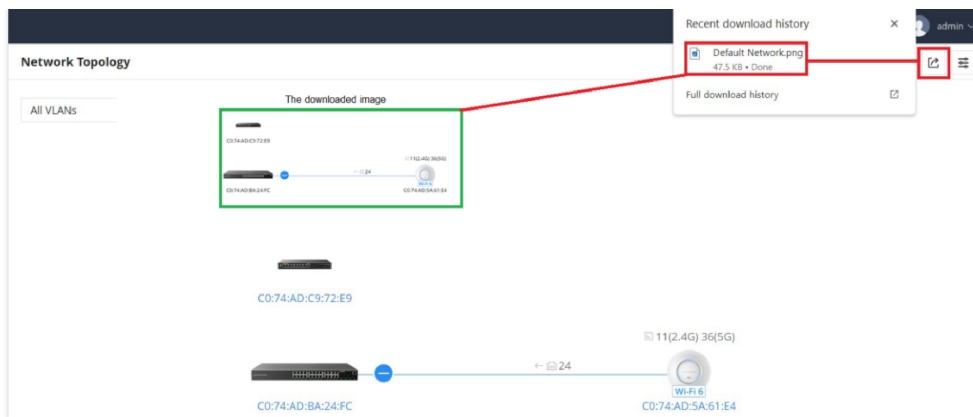


## Network Topology – Highlight mesh

To backup the current topology or share it, on the top right corner of the page, click on the **"Export"** button, and 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

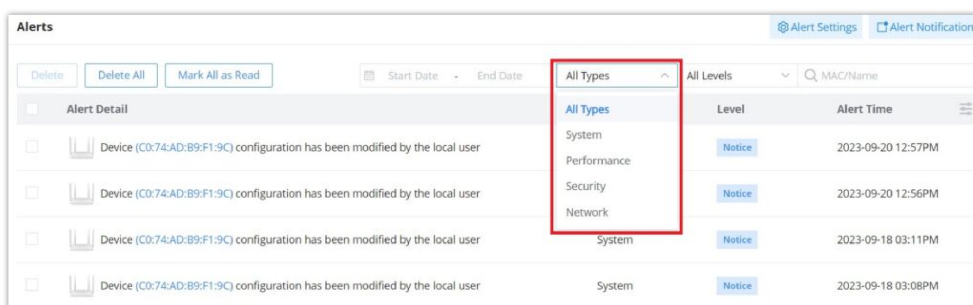
## ALERTS

The 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 that have been generated, please navigate to **the Web UI → Alerts** page.

The alerts can be displayed either by type or level. 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.

### Alert Types

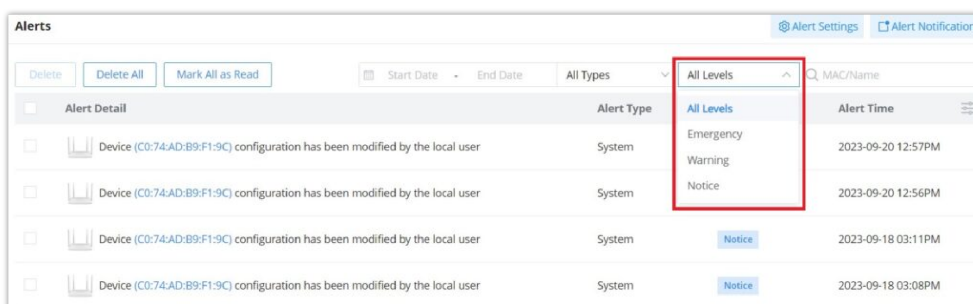
The available types are **System, Performance, Security, and Network**, or the user can choose to display all the types.



Alerts Types

### Alert Levels

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



Alerts Levels

## Alert Settings

On 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 Clients.

Alerts > **Alert Settings**

System Alert Performance Alert Security Alert Network Alert

☐ Device configuration sync failed

☒ The current device has a time deviation of 30 minutes  
 ⓘ Turn on (Auto Sync Time) to avoid time deviation

**Router**

☐ Router upgraded successfully

☐ Router upgrade failed

☐ Router temperature is too high

**Switch**

☐ Switch temperature is too high

☐ Failure detected; Select

☐ 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

**AP**

☐ AP upgraded successfully

☐ AP upgrade failed

☐ AP temperature is too high

Cancel Save

Alert Settings – part 1

Alerts > **Alert Settings**

System Alert Performance Alert Security Alert Network Alert

☒ 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

**Switch**

☒ CPU Usage exceeded 90 %

☒ Memory Usage exceeded 90 %

☒ Switch Port Packet Loss Rate exceeded 10 %

**AP**

☒ CPU Usage exceeded 90 %

☒ Memory Usage exceeded 90 %

☒ 2.4GHz Channel Usage exceeded 60 %

☒ 5GHz Channel Usage exceeded 60 %

Cancel Save

Alert Settings – part 2

Alerts > **Alert Settings**

System Alert Performance Alert Security Alert Network Alert

ⓘ Select alerts to be notified of

**AP**

☐ Device detected a rogue AP of Untrusted AP Spoofing SSID

Cancel Save

Alert Settings – part 3

Alerts > **Alert Settings**

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

☐ Router USB/LAN/WAN port connection

**Switch**

☐ Port Up

☐ Port Down

☐ PoE power off

☐ Port errdisable

**AP**

☐ RF not started

☐ AP channel automatically switched

☐ AP wired port negotiation

☐ Channel radar avoidance

**Client**

☐ Portal authentication failed

☐ Client failed to authenticate with 802.1X

☐ Client wireless connection failed

Cancel Save

Alert Settings – part 4

## Alert Notification

On this page, Email 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.

Email Address

Documentaction-center@grandstream.com

EMEA@grandstream.com

Add New Item

System Alert Performance Alert Security Alert Network Alert

Alert Detail	Notification Type
<b>Cloud</b>	
AP offline for more than 30 mins	Web <input checked="" type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
AP online (After offline for 30 mins)	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Router offline for more than 30 mins	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input checked="" type="checkbox"/>
Router online (After offline for 30 mins)	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
Switch offline for more than 30 mins	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input checked="" type="checkbox"/>
Switch online (After offline for 30 mins)	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Cancel/Return Shared Network	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input checked="" type="checkbox"/>
Device configuration sync failed	Web <input checked="" type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>

System Alert Notifications

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

Alert Detail	Notification Type ⓘ
<b>Cloud</b>	
Network Throughput exceeded 999Mbps	Web <input checked="" type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
SSID Throughput exceeded 444Mbps	Web <input checked="" type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
<b>Router</b>	
CPU Usage exceeded 90%	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input checked="" type="checkbox"/>
Memory Usage exceeded 90%	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
2.4GHz Channel Usage exceeded 60%	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
5GHz Channel Usage exceeded 60%	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input checked="" type="checkbox"/>
2.4GHz Clients exceeded 20	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
5GHz Clients exceeded 20	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
WAN port throughput exceeded 50Mbps	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
WAN port uplink Bandwidth exceeded 50Mbps	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
WAN port downlink Bandwidth exceeded 50Mbps	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
<b>Switch</b>	
CPU Usage exceeded 90%	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input checked="" type="checkbox"/>
Memory Usage exceeded 90%	Web <input type="checkbox"/> Email <input type="checkbox"/> App <input type="checkbox"/>
Switch Port Packet Loss Rate exceeded 10%	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>

Cancel Save

### 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 ⓘ
<b>AP</b>	
Device detected a rogue AP of Illegal access without authentication,Illegal access,Spoofing SSID,Untrusted AP	Web <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> App <input checked="" type="checkbox"/>

Cancel Save

### Security Alert Notifications

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

Alert Detail	Notification Type ⓘ
<b>Router</b>	
Network failed	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
PPPoE connection failed	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
RF not started	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
WAN is down	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Channel radar avoidance	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
RADIUS server failed	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Router USB/LAN/WAN port connection	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
<b>Switch</b>	
Port Up	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Port Down	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
PoE power off	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
Port errdisable	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
<b>AP</b>	
RF not started	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
AP channel automatically switched	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>
AP wired port negotiation	Web <input type="checkbox"/> Email <input checked="" type="checkbox"/> App <input type="checkbox"/>

Cancel Save

### Network Alert Notifications

# SETTINGS

## Wi-Fi

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

## Wireless LAN

Under the 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 + Add button to add a new SSID, the configuration can be only specific to this SSID, to configure radios for all SSIDs please click on section two **“Global Radio Settings”**.

Wi-Fi

Wireless LAN

Search Name

+ Add

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

Global Radio Settings

Mesh

Enable Mesh

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

\* Scan Interval

5

1-5 numbers

\* Wireless Cascade

3

1-3 numbers

Cancel

Save

Wi-Fi page

## Add an SSID

To add a new SSID, navigate to Web UI → Settings → Wi-Fi page → Wireless LAN section then click the “Add” button. A new page will pop up, enter different settings to add a new SSID.

Wi-Fi

Add Wireless LAN

Basic

WiFi

\* SSID

Office

1-32 characters

Client IP Assignment

Bridge

Associated VLAN

Enable Captive Portal

SSID Band

Dual-Band

Access Security

Access Control

Device Assignment

Advanced

Cancel

Save

Add wireless LAN

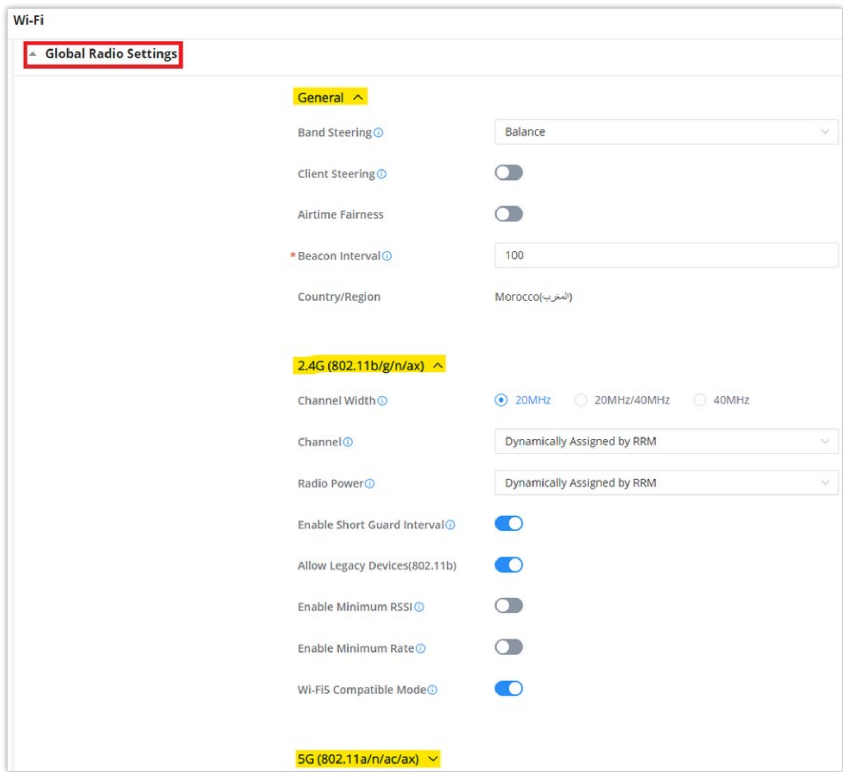
Basic	
WiFi	Check to enable Wi-Fi for the SSID
SSID	Set or modify the SSID name.
Client IP Assignment	Select between Bridge or NAT
Associated VLAN	Check to Enable VLAN and enter VLAN ID, otherwise, this SSID will be using the default network group.
Enable Captive Portal	Click on the checkbox to enable 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	<p>Set the security type, 5 options are available:</p> <ul style="list-style-type: none"> <li>● Open : no security is required</li> <li>● Personal: Select the WPA Pre-Shared Key and the WPA Mode</li> <li>● Enterprise: Select Radius Authentication and WPA Mode.</li> <li>● PPSK: Select the PPSK Group.</li> <li>● Hotspot2.0 OSEN: Select the RADIUS Authentication</li> </ul>
802.11w	<p><b>Disabled:</b> disable 802.11w;</p> <p><b>Optional:</b> either 802.11w supported or unsupported clients can access the network;</p> <p><b>Required:</b> only the clients that support 802.11w can access the network.</p>
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	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>Radio Mode:</b> Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76xx but they cannot communicate with each other.</li> <li>● <b>Internet Mode:</b> 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.</li> <li>● <b>Gateway MAC Mode:</b> 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.</li> </ul>
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 <b>"Settings → Profiles → Schedule"</b> .
Device Assignment	
<p>Select from the Devices list the ones to be part of this SSID.</p> <p><i><b>Note:</b> If an AP or router that uses the Wi-Fi network is selected, new APs will be automatically added to the network.</i></p>	

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	<b>Disable:</b> all of the broadcast and multicast packages will be forwarded to the wireless interface. <b>Enable:</b> all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND; <b>Enable with Proxy ARP enabled:</b> 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"> <li>• <b>The 802.11k</b> 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.</li> <li>• 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.</li> <li>• <b>802.11v</b> 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.</li> </ul> <p><i>Note: 11R is required for enterprise audio feature, 11V and 11K are optional.</i></p> <p>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

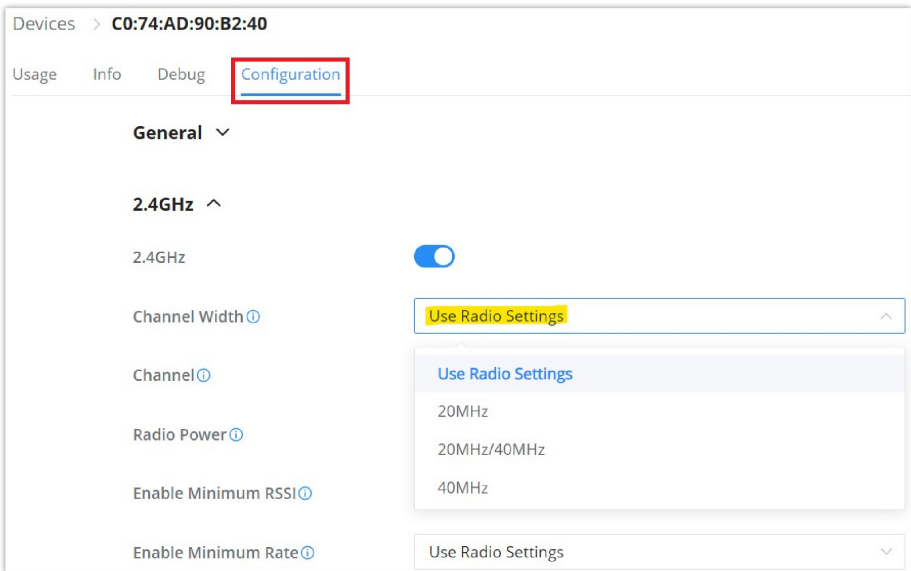
Global Radio Settings

On this page the Administrator can configure the global radio settings which will affect all the GWN devices with the wireless signal, it's a convenient way to configure all the device's 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 to the table below:

General	
Band Steering	Select from the drop-down list, four options are available: <ul style="list-style-type: none"><li>• <b>Disable Band Steering:</b> Band steering is disabled</li></ul>

	<ul style="list-style-type: none"> <li>● <b>2.4G in priority:</b> steer clients to 2.4G</li> <li>● <b>5G in priority:</b> steer clients to 5G</li> <li>● <b>Balance:</b> balance between 2.4G and 5G.</li> </ul>
<b>Client Steering</b>	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.
<b>RSSI Threshold</b>	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 poor connectivity and reduce performance for other clients. <i>Default is -75.</i>
<b>Client Access Threshold</b>	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>
<b>Airtime Fairness</b>	Allows faster clients to have more airtime than slower clients.
<b>Beacon Interval</b>	<p>Configures interval between beacon transmissions/broadcasts.</p> <p>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"> <li>● <b>Using High Beacon Interval:</b> 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.</li> <li>● <b>Using Low Beacon Interval:</b> 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.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● When AP enables several SSIDs with different interval values, the max value will take effect.</li> <li>● When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500.</li> <li>● 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.</li> <li>● When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500.</li> <li>● Mesh feature will take up a share when it is enabled.</li> </ul> <p><i>Default value is 100ms. Valid range: 40 – 500 ms.</i></p>
<b>Country/Region</b>	Displays the country/region of the AP.
<b>2.4G/5G</b>	
<b>Channel Width</b>	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.
<b>Channel</b>	Select "Auto" or a Dynamically Assigned by RRM. <i>Default is "Auto".</i>
<b>Custom Channel</b>	<p>Select a custom channels.</p> <p><b>Note:</b> that the proposed channels depend on Country Settings under Settings → System.</p>
<b>Radio Power</b>	<p>Set the Radio Power, it can be Low, Medium, or High or Custom or Dynamically assigned by RRM or Auto.</p> <p><b>Note :</b> Dynamically assigned by RRM activates TPC and CHD:</p> <ul style="list-style-type: none"> <li>● <b>Transmit Power Control:</b> 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.</li> <li>● <b>Coverage Hole Detection:</b> CHD enables AP to decide whether to increase the AP power by the current SNR and SNR threshold of the connected clients.</li> </ul> <p><b>Custom:</b> 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>



<b>Enable Short Guard Interval</b>	Check to activate this option to increase throughput.
<b>Allow Legacy Devices (802.11b)</b>	Check to support 802.11b devices to connect the AP in 802.11n/g mode. (2.4GHz setting)
<b>Enable Minimum RSSI</b>	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm).
<b>Minimum RSSI (dBm)</b>	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”.
<b>Enable Minimum Rate</b>	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP.
<b>Minimum Rate (Mbps)</b>	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.
<b>Wi-Fi5 Compatible Mode</b>	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):

- The advantages of a wired network are security, anti-interference, and stable bandwidth.
- The disadvantages are high construction cost, long periods 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, a Wireless Mesh Network is an effective complement to 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:

[GWN76xx Mesh Network Guide](#)

Users can set some Mesh Network parameters under the menu “**Settings** → **Wi-Fi** → **Mesh**”, as shown in the figure below:

Wi-Fi

Wireless LAN
+ Add

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

Cancel
Save

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 affect all the added GWN switches.

LAN

LAN
+ Add

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 [+ Add](#) 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
1-4094 numbers

VLAN-Only Network
☐

\* Gateway

IPv4
☒

\* Gateway IPv4 Address/Prefix Length

Prefix length range 8-30

DHCP Service

\* IPv4 Address Pool

\* Release Time (m)
60-2880 numbers

DHCP Option

Option
Type
Service
Content

Hexadecimal str

Preferred DNS Server

Alternative DNS Server

IPv6
☐

Cancel
Save

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

None

Voice VLAN

Voice VLAN

Multicast

IGMP Snooping VLAN

Select LAN

MLD Snooping VLAN

Select LAN

Unknown Multicast Message ⓘ

Flooding

DHCP Snooping Settings

DHCP Snooping

802.1X

Guest VLAN ⓘ

Other

\*Jumbo Frame

9216

Black Hole MAC Address

None

Cancel

Save

## 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. <b>Range:</b> 1518-10000
Black Hole MAC Address	Select a Black Hole MAC Address from the list or click Add New MAC group

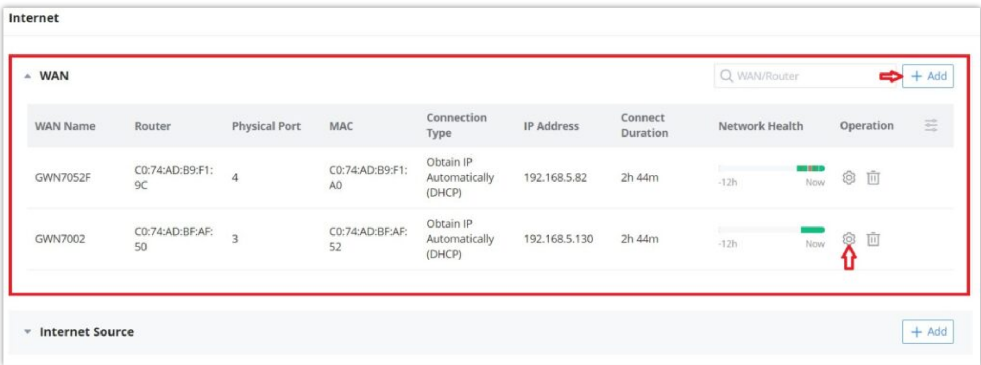
## Internet

Internet configurations 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.

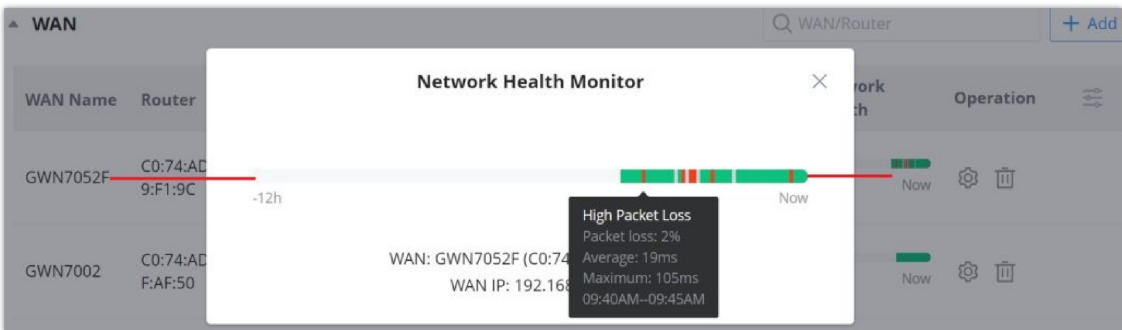
Please navigate to **Web UI → Settings → Internet page → WAN section**.



WAN

- **Network Health**

Network Health is a feature that monitors 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

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

To edit a WAN click on the entry or click on the **“Configure icon”** under operation, and to add a WAN click on the **“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:

Internet > GWN7052F Sync

\* WAN Name  1-64 characters

\* Router

\* Physical Port

Connection Type

Static DNS ☒

\* Preferred DNS Server

Alternative DNS Server

\* Maximum Transmission Unit (MTU)  576-1500 numbers

WAN Port MAC Address

\* Tracking IP Address 1

Tracking IP Address 2

VLAN Tag ☒

\* VLAN Tag ID  3-4094 numbers

Add/edit a WAN – part 1

Internet > GWN7052F Sync

\* Priority  Range 0-7 and 7 is the highest priority

Multiple Public IP Addresses ☒

\* Public IP Address

[Add New Item](#)

**IPv6**

IPv6 ☒

Connection Type

Static DNS ☒

\* Preferred DNS Server

Alternative DNS Server

IPv6 Relay to VLAN ☒ If enabled, IPv6 addresses will be relayed to LAN-side clients.

Tracking IPv6 Address 1

Tracking IPv6 Address 2

Add/edit a WAN – part 2

Internet > GWN7052F Sync

Tracking IPv6 Address 2

**DDNS**

DDNS ☒

Service Provider

\* Username

\* Password

\* Domain

If no account is available, please go to [www.no-ip.pl](http://www.no-ip.pl) to register for a username, password and domain.

**DMZ**

Destination Group

**UPnP**

UPnP ☒

\* Destination Group

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"> <li><b>Obtain IP automatically (DHCP):</b> When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server.</li> </ul>

	<ul style="list-style-type: none"> <li>● <b>Enter IP Manually (Static IP):</b> 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.</li> <li>● <b>Internet Access with PPPoE account (PPPoE):</b> When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval, and Inter-Key Timeout (in seconds).</li> </ul> <p><i>The default setting is “Obtain IP automatically (DHCP)”</i></p>
<b>Static DNS</b>	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server
<b>Preferred DNS Server</b>	Enter the preferred DNS Server
<b>Alternative DNS Server</b>	Enter the Alternative DNS Server
<b>Maximum Transmission Unit (MTU)</b>	<p>Configures the maximum transmission unit allowed on the WAN.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 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.</li> </ul>
<b>WAN Port MAC Address</b>	<p>Select from the drop-down list either to:</p> <ul style="list-style-type: none"> <li>● Use Default MAC Address</li> <li>● Use Custom MAC Address</li> </ul> <p><i>Default is "Use Default MAC Address"</i></p>
<b>Custom MAC Address</b>	Enter the custom MAC Address to be used with this WAN.
<b>Tracking IP Address 1</b>	Configures tracking IP address of WAN port to determine whether the WAN port network is normal.
<b>Tracking IP Address 2</b>	Add another alternative address for Tracking IP Address
<b>VLAN Tag</b>	Select if either to enable or disable VLAN Tag.
<b>VLAN Tag ID</b>	Enter the VLAN tag ID.
<b>Priority</b>	<p>Enter the priority</p> <p><b>Note:</b> Range 0-7 and 7 is the highest priority</p>
<b>Multiple Public IP Addresses</b>	Please use with Port Forward function, so that you can access to router via public IP address.
<b>Public IP Address</b>	<p>Enter one or more public IP addresses</p> <p>Click on "+" icon or "-" icon to add or delete public IP addresses</p>
<b>IPv6</b>	
<b>IPv6</b>	Enable this option to use IPv6 on this specific WAN.
<b>Connection Type</b>	<p>Select the connection type from the drop-list, three options are available:</p> <ul style="list-style-type: none"> <li>● Obtain IP automatically (DHCPv6)</li> <li>● Enter the IP manually (static IPv6)</li> <li>● Internet Access with PPPoE Account (PPPoE)</li> </ul> <p><i>The default setting is “Obtain IP automatically (DHCPv6)”.</i></p>
<b>Static DNS</b>	Enable this option to enter statically assigned DNS

<b>Preferred DNS Server</b>	Enter the preferred DNS Server
<b>Alternative DNS Server</b>	Enter the Alternative DNS Server
<b>IPv6 Relay to VLAN</b>	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.
<b>Tracking IPv6 Address 1</b>	Configures tracking IP address of WAN port to determine whether the WAN port network is normal
<b>Tracking IPv6 Address 2</b>	Add another alternative address for Tracking IP Address
<b>DDNS</b>	
<b>DDNS</b>	Toggle ON or OFF the DDNS function, default is OFF <i><b>Note:</b> On the router, DDNS function can only be enabled on one WAN port</i>
<b>Service Provider</b>	Select the DDNS provider from the list <i><b>Note:</b> If no account is available, please go to <a href="http://www.oray.com">www.oray.com</a> to register for a username, password and domain</i>
<b>Username</b>	Enter the Username
<b>Password</b>	Enter the Password
<b>Domain</b>	Enter the Domain
<b>DMZ</b>	
<b>Destination Group</b>	Select the destination group from the drop-down list.
<b>UPnP</b>	
<b>UPnP</b>	Toggle ON or OFF the UPnP function, default is OFF <i><b>Note:</b> If UPnP (Universal Plug and Play) is enabled, devices on LAN can request the router to port forward automatically</i>
<b>Destination Group</b>	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 the **"Add"** button to add a new one, refer to the figure below:

Internet							
▼ WAN		Q WAN/Router		+ Add			
▲ Internet Source				→ + Add			
Name	Mode	Router	Interfaces	Interface	Weight	Operation	
Internet Source 1 (Load Balance)	Load Balance	C0:74:AD:BF:AF:50	1	GWN7002 (WAN)	1	⚙️	🗑️
Internet source 2 (Backup)	Load Balance	C0:74:AD:B9:F1:9C	1	GWN7052F (WAN)	1	⚙️	🗑️

*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.

Interface	Weight
GWN7002 (WAN)	9
GWN7002 (WAN2) (WAN)	2

*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 the **"Add"** button as shown in the figure below:

VPN Type	Action
PPTP	+ Add
IPSec (Site-to-Site)	+ Add
OpenVPN®	+ Add
VPN User	+ Add
WireGuard®	+ Add

*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.



The 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

Type

PPTP Client

PPTP Server

\* Name

PPTP VPN

1-64 characters

Status

Once disabled, the associated VPN services will also be disabled.

\* Server Address

192.168.5.7

\* Username

GSuser3

1-64 characters

\* Password

\*\*\*\*\*

1-32 characters

\* Router

C0:74:AD:BF:AF:50

\* Interface

GWN7002

MPPE Encryption

IP Masquerading

\* MTU

1450

576-1450 numbers

Remote Network

192.168.122.0

/

24

Add New Item

Cancel

Save

VPN – Add PPTP Client

Type	Select either <b>PPTP Client</b> 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 (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
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

Type

☐ PPTP Client
☒ PPTP Server

\*Name

PPTP Server

Status

☐ Once disabled, the PPTP service will also be disabled.

\*Server Local Address/Prefix Length

192.168.5.10 / 24

\*Client Start Address

192.168.5.2

\*Client End Address

192.168.5.10

\*Router

C0:74:AD:BF:AF:50

\*Interface

GWN7002

MPPE Encryption

☒

LCP Echo Interval (sec)

20

LCP Echo Failure Threshold

3

LCP Echo Adaptive

☐

\*MTU

1450

Cancel

Save

VPN – Add PPTP Server

Type	Select either PPTP Client or <b>PPTP Server</b> 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"> <li>● <b>Once enabled:</b> LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request.</li> <li>● <b>Once disabled:</b> the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval</li> </ul>

<b>Maximum Transmission Unit (MTU)</b>	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.
<b>Maximum Receive Unit (MRU)</b>	MRU indicates the size of the received packets. By default is 1450.
<b>Preferred DNS Server</b>	specify the preferred DNS server. <i>Ex: 8.8.8.8</i>
<b>Alternative DNS Server</b>	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 encrypt and secure traffic between two sites using two GWN routers. It supports manual configuration and auto mode.

#### VPN – Add IPSec Auto

<b>Mode</b>	Select the mode: Manual or <b>Auto</b> . <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>
<b>Name</b>	Specify a name for IPSec VPN.
<b>Status</b>	Toggle ON or OFF to enable or disable the IPSec VPN. <i>Note: Once disabled, the associated VPN services will also be disabled.</i>
<b>Router</b>	Select from the drop-down list the router/device group that this VPN will be using.
<b>Interface</b>	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:

The screenshot shows the 'Add IPsec' configuration window. The 'General' tab is active. The 'Mode' is set to 'Manual'. The 'Name' is 'IPSec Manual'. The 'Status' is 'ON'. The 'Remote Address' is '192.168.5.10'. The 'Router' is 'C0:74:AD:BFAF:50'. The 'Interface' is 'GWN7002'. The 'Pre-shared Key' is masked with asterisks. The 'Local Network' is '192.168.122.0' with a mask of '24'. The 'Remote Network' is '192.168.80.0' with a mask of '24'. There are 'Add New Item' buttons for both network fields. The 'Advanced Settings' section is collapsed. At the bottom are 'Cancel' and 'Save' buttons.

### 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.

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

	<ul style="list-style-type: none"> <li>• SHA-1</li> <li>• SHA2-256</li> </ul> Default is SHA2-256
<b>PFS Group</b>	Select from the drop-down list the PFS group, the available ones are: Group 2,5,14. Default is disabled.

#### 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 the client and server side.

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

VPN > Add OpenVPN®

Type	<input type="radio"/> OpenVPN® Client <input checked="" type="radio"/> OpenVPN® Server
* Name	OpenVPN Server
Status	<input type="checkbox"/> Once disabled, the OpenVPN® service will also be disabled.
Protocol	UDP
* Router	C0:74:AD:BF:AF:50
* Interface	GWN7002
* Local Port	1194
Authentication Mode	SSL
Encryption Algorithm	AES-256-CBC
Digest Algorithm	SHA256
TLS Identity Authentication	<input type="checkbox"/>
Duplicate client certificates are allowed	<input type="checkbox"/>
Redirect Gateway	<input checked="" type="checkbox"/>
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>

#### VPN – Add OpenVPN® Server

<b>Type</b>	Select the OpenVPN®: Client or <b>Server</b>
<b>Name</b>	Enter a name for the OpenVPN® server.
<b>Status</b>	Toggle ON or OFF to enable or disable the OpenVPN® Server. <i><b>Note:</b> Once disabled, the OpenVPN® service will also be disabled.</i>
<b>Protocol</b>	Choose the Transport protocol from the dropdown list, either TCP or UDP. <i>The default protocol is <b>UDP</b>.</i>
<b>Router</b>	Select from the drop-down list the router/device group that this VPN will be using.
<b>Interface</b>	Select from the drop-down list the exact interface of the router/device group.
<b>Local Port</b>	Configure the listening port for OpenVPN® server. <i>The default value is <b>1194</b>.</i>

<b>Authentication Mode</b>	<p>Choose the server mode the OpenVPN® server will operate with. 4 modes are available:</p> <ul style="list-style-type: none"> <li>• <b>SSL:</b> 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).</li> <li>• <b>User Authentication:</b> 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).</li> <li>• <b>SSL + User Authentication:</b> Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.</li> <li>• <b>PSK:</b> 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).</li> </ul>
<b>Encryption Algorithm</b>	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
<b>Digest Algorithm</b>	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.
<b>TLS Identity Authentication</b>	<p>This option uses a static <b>Pre-Shared Key (PSK)</b> that must be generated in advance and shared among all peers.</p> <p>This feature adds extra protection to the <b>TLS</b> channel by requiring that incoming packets have a valid signature generated using the PSK key.</p>
<b>TLS Identity Authentication Direction</b>	Select from the drop-down list the direction of TLS Identity Authentication, three options are available ( <b>Server, Client or Both</b> ).
<b>TLS Pre-Shared Key</b>	If TLS Identity Authentication is enabled, enter the TLS Pre-Shared Key.
<b>Duplicate client certificates are allowed</b>	Click on " <b>ON</b> " to allow duplicate Client Certificates
<b>Redirect Gateway</b>	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
<b>Push Routes</b>	<p>Specify route(s) to be pushed to all clients.</p> <p><i>Example: 10.0.0.1/8</i></p>
<b>LZO Compression Algorithm</b>	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.
<b>Allow Peer to Change IP</b>	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
<b>CA Certificate</b>	Select a generated CA from the dropdown list or add one.
<b>Server Certificate</b>	Select a generated Server Certificate from the dropdown list or add one.
<b>IPv4 Tunnel Network/Mask Length</b>	<p>Enter the network range that the GWN70xx will be serving from to the OpenVPN® client.</p> <p><b>Note:</b> The network format should be the following 10.0.10.0/16.</p> <p>The mask should be at least 16 bits.</p>

VPN > Add OpenVPN®

Type ☒ OpenVPN® Client ☐ OpenVPN® Server

\* Name  1-64 characters

Status ☐ Once disabled, the associated VPN services will also be disabled.

Protocol  ▾

\* Router  ▾

\* Interface  ▾

\* Local Port  1-65535 numbers

\* Remote OpenVPN® Server

\* OpenVPN® Port  1-65535 numbers

Authentication Mode  ▾

Encryption Algorithm  ▾

Digest Algorithm  ▾

TLS Identity Authentication ☐

VPN – Add OpenVPN® Client

Type	Select the OpenVPN®: <b>Client</b> or Server
Name	Enter a name for the OpenVPN® Client.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Client. <i><b>Note:</b> Once disabled, the associated VPN services will also be disabled.</i>
Protocol	Specify the transport protocol used. <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> </ul> <b>Note:</b> The default protocol is UDP.
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	Choose the server mode the OpenVPN® server will operate with. 4 modes are available: <ul style="list-style-type: none"> <li>• <b>SSL:</b> 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).</li> <li>• <b>User Authentication:</b> 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).</li> <li>• <b>SSL + User Authentication:</b> Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.</li> </ul>



	<ul style="list-style-type: none"> <li>• <b>PSK:</b> 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).</li> </ul>
<b>Encryption Algorithm</b>	<p>Choose the encryption algorithm. The encryption algorithms supported are:</p> <ul style="list-style-type: none"> <li>• DES-CBC</li> <li>• RC2-CBC</li> <li>• DES-EDE-CBC</li> <li>• DES-EDE3-CBC</li> <li>• DESX-CBC</li> <li>• BF-CBC</li> <li>• RC2-40-CBC</li> <li>• CAST5-CBC</li> <li>• RC2-64-CBC</li> <li>• AES-128-CBC</li> <li>• AES-192-CBC</li> <li>• AES-256-CBC</li> <li>• SEED-CBC</li> </ul>
<b>Digest Algorithm</b>	<p>Select the digest algorithm. The digest algorithms supported are:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• RSA-MD5</li> <li>• SHA1</li> <li>• RSA-SHA1</li> <li>• DSA-SHA1-old</li> <li>• DSA-SHA1</li> <li>• RSA-SHA1-2</li> <li>• DSA</li> <li>• RIPEMD160</li> <li>• RSA-RIPEMD160</li> <li>• MD4</li> <li>• RSA-MD4</li> <li>• ecdsa-with-SHA1</li> <li>• RSA-SHA256</li> <li>• RSA-SHA384</li> <li>• RSA-SHA512</li> <li>• RSA-SHA224</li> <li>• SHA256</li> <li>• SHA384</li> <li>• SHA512</li> <li>• SHA224</li> <li>• whirlpool</li> </ul>
<b>TLS Identity Authentication</b>	Enable TLS identity authentication direction.
<b>TLS Identity Authentication Direction</b>	<p>Select the identity authentication direction.</p> <ul style="list-style-type: none"> <li>• Server: Identity authentication is performed on the server side.</li> <li>• Client: Identity authentication is performed on the client side.</li> <li>• Both: Identity authentication is performed on both sides.</li> </ul>
<b>TLS Pre-Shared Key</b>	Enter the TLS pre-shared key.
<b>Routes</b>	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
<b>Deny Server Push Routes</b>	If enabled, client will ignore routes pushed by the server.
<b>IP Masquerading</b>	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.
<b>LZO Compression</b>	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.
<b>Allow Peer to Change IP</b>	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
<b>CA Certificates</b>	Click on “Upload” and select the CA certificate Note: This can be generated in System Settings → Certificates → CA Certificate
<b>Client Certificate</b>	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' interface. It contains the following fields and options:

- Name:** Text input field with 'VPN User' entered.
- Status:** Toggle switch, currently turned on.
- Server Type:** Radio buttons for 'PPTP' and 'OpenVPN®'. 'OpenVPN®' is selected and highlighted with a red box.
- Server:** Dropdown menu showing 'OpenVPN Server'.
- Username:** Text input field with 'OpenVPN\_User1' entered.
- Password:** Text input field with 'P@ssW0rd' entered.
- Client Subnet:** Text input field with '192.168.2.0' and a dropdown for '24'.
- Client Certificate:** Dropdown menu showing 'Client Cert'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

#### VPN – Add VPN User

<b>Name</b>	Enter a name for the user. This name will not be used to log in.
<b>Status</b>	Enable or disable this account.
<b>Server Type</b>	Choose the type of the server. <ul style="list-style-type: none"> <li>• PPTP</li> <li>• OpenVPN®</li> </ul>
<b>Server Name</b>	Select the VPN server from the drop-list
<b>Username</b>	Enter the username. This username will be used to log in. <i>Note: only alphanumeric characters and @ ! \$ % - _ are supported.</i>
<b>Password</b>	Enter the password. <i>Note: only alphanumeric characters and @ ! \$ % - _ are supported.</i>

<b>Client Subnet</b>	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)
<b>Only if OpenVPN® is selected</b>	
<b>Client Certificate</b>	Select from the drop-down list the client certificate.

#### VPN – Add VPN User

## WireGuard®

WireGuard® is a 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 a private key can be generated with one click then after that the public key can be copied and shared with the client.

VPN > Add WireGuard®

\* Name

WireGuard VPN

Status

☐ 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/TGqE9kGFIsxyYOBaoblCOZIWO30=  
[Copy](#)

\* MTU

1420

Cancel

Save

#### VPN – Add WireGuard®

<b>Name</b>	Specify a name for Wireguard® VPN.
<b>Status</b>	Toggle ON or OFF to enable or disable the Wireguard® VPN.
<b>Router</b>	Select from the drop-down list the router/device group that this VPN will be using.
<b>Interface</b>	Select from the drop-down list the exact interface of the router/device group. <i>Note: one WAN only supports creating one WireGuard®.</i>
<b>Listening Port</b>	Set the local listening port when establishing a WireGaurd® tunnel. <i>Default: 51820</i>
<b>Server Local Address/Prefix Length</b>	Specify the server local address with the prefix length
<b>Private Key</b>	Click on "One-Click Generation" text to generate a private key.
<b>Public Key</b>	The public key will be generated according to the private key.

	Click on " <b>Copy</b> " 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

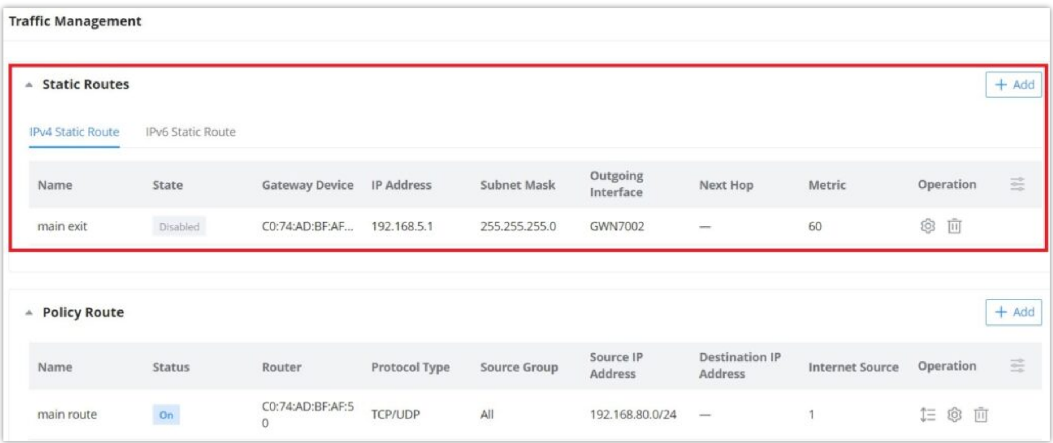
On this page, the user can manage traffic by either adding static routes (IPv4 or IPv6) or adding Policy Routes.

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 changes.

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.



Static Routes

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

Traffic Management > Add Static Route

Type

☒ IPv4 Static Route ☐ IPv6 Static Route

\* Name

IPv4 Static Route

Supports 1-64 characters

Status

☒

\* 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

\* Metric

60






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.

Traffic Management									
Static Routes									
IPv4 Static Route IPv6 Static Route									
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	  	

Policy Route

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

Traffic Management > main route

\*

Name

main route

1-64 characters

Status

IP Family

IPv4

Protocol Type

TCP/UDP

\*

Router

C0:74:AD:...

\*

Source Group

All

Source IP Address/Mask Length

192.168.80.0

/

24

Source Port

1-65535 numbers

Destination IP address/mask length

/

Destination Port

1-65535 numbers

\*

Internet Source

Internet Source 1

Schedule

None

Cancel

Save

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"><li>● All</li><li>● TCP</li><li>● UDP</li><li>● TCP/UDP</li><li>● ICMP</li></ul>
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)

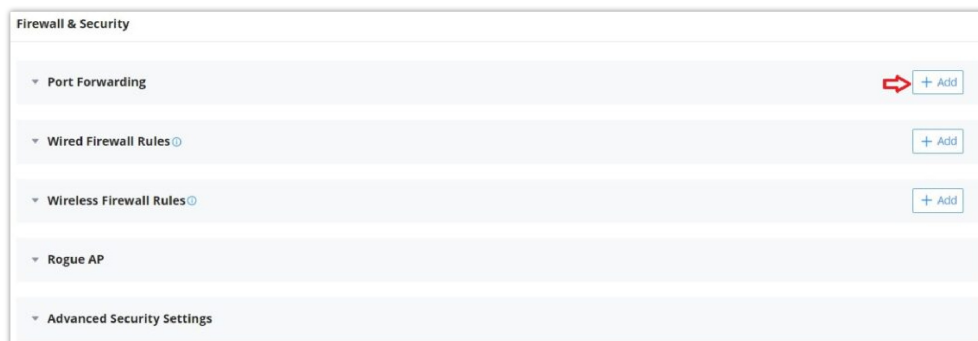
<b>Destination IP address/mask length</b>	Set the destination IP address and mask length to match the packet. For example, 192.168.122.0/24
<b>Internet Source</b>	Select the internet source (WAN/Load Balance/Backup) from the drop-down list
<b>Schedule</b>	Select a schedule from the drop-down list or click on "Add New Schedule" to add one.

*Add Policy Route*

## Firewall and Security

The Firewall & Security page combines all the configurations 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 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**.

Firewall & Security > Add Port Forwarding

\* Name

Port Forwarding

1-64 characters

Status

☒

Protocol Type

☒ TCP/UDP
☐ TCP
☐ UDP

\* Interface

WAN1

Source IP Address ⓘ

\* Source Port ⓘ

24

1-65535 numbers

\* Destination Group

Default LAN

\* Destination IP Address

192.168.5.85

\* Destination Port ⓘ

24

1-65535 numbers

Cancel

Save

*Port Forwarding*

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

<b>Name</b>	Enter a name for the port forwarding rule.
-------------	--

<b>Status</b>	Toggle on/off the rule status.
<b>Protocol Type</b>	Select a protocol, users can select TCP, UDP or TCP/UDP.
<b>Interface</b>	Select the WAN port
<b>Source IP Address</b>	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
<b>Source Port</b>	Set a single or a range of Ports.
<b>Destination Group</b>	Select VLAN group.
<b>Destination IP Address</b>	Set the destination IP address.
<b>Destination Port</b>	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.

The screenshot shows the 'Add Wired Firewall Rules' configuration page. The breadcrumb is 'Firewall & Security > Add Wired Firewall Rules'. The form includes the following fields and options:

- Type:** Radio buttons for 'Inbound Rules' (selected) and 'Forwarding Rules'.
- \* Name:** Text input with 'Allow' entered. A note '1-64 characters' is shown.
- Status:** Toggle switch is turned on.
- Type:** Radio buttons for 'Any' (selected), 'IPv4', and 'IPv6'.
- Protocol Type:** Dropdown menu with 'UDP' selected.
- \* Source Group:** Dropdown menu with 'WAN1' selected.
- Source MAC Address:** Text input with a placeholder ' : : : : '.
- Source IP Address/Mask Length:** Text input with '192.168.5.0/24' entered.
- Source Port:** Text input with '602' entered. A note '1-65535 numbers' is shown.
- Destination IP Address/Mask Length:** Text input with '192.168.122.0/24' entered.
- Destination Port:** Text input with '602' entered. A note '1-65535 numbers' is shown.
- Action:** Radio buttons for 'Accept' (selected), 'Reject', and 'Drop'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

### Wired Firewall Rules

<b>Type</b>	Select the type of the firewall rule: <b>Inbound</b> or <b>Forwarding rule</b>
<b>Name</b>	Enter a name for the wired firewall rule.

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

#### 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: <b>Inbound rules</b> or <b>Outbound rules</b>
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"> <li>● <b>Permit:</b> Traffic from clients will be allowed.</li> <li>● <b>Deny:</b> Traffic from clients will be denied.</li> </ul>
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 into the network and increase the wireless security access of clients when introducing the Rogue AP detection feature to the adopted/paired GWN devices. The detected devices will be listed with all the details under the “**Alerts**” page for further intervention.

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

Firewall & Security
Rogue AP

Enable Rogue AP Detection

Detect Range

☐ Same Channel
☒ All Channels

Countermeasure Level

Medium

Containment Range

☒ Same Channel
☐ All Channels

Sub-string for Spoofing SSID

Grand

Stream

EMEA

Add New Item

Trusted AP

c0 : ad : 74 : 0c : 47 : da

Add New Item

Untrusted AP

: : : : :

Add New Item

Cancel
Save

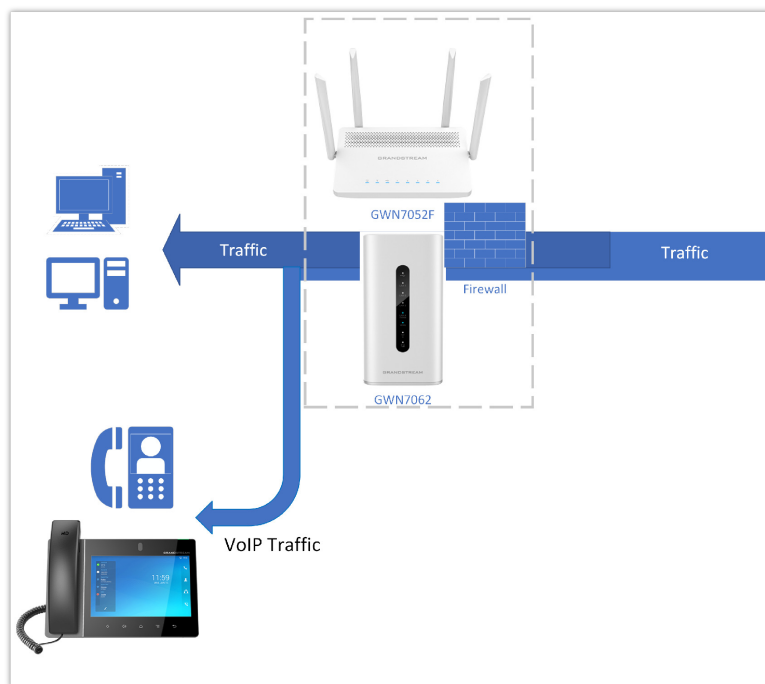
Rogue AP

<b>Enable Rogue AP Detection</b>	Select to either to enable or disable Rogue AP scan.
<b>Detect Range</b>	<p>Specify the rogue AP detect range.</p> <ul style="list-style-type: none"> <li>• <b>Same Channel:</b> AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication.</li> <li>• <b>All channels:</b> AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt.</li> </ul> <p><i>Default is Same Channel.</i></p>
<b>Countermeasure Level</b>	<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"> <li>• <b>High:</b> Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID.</li> <li>• <b>Medium:</b> Untrusted BSSID, Illegal access without authentication, Illegal access.</li> <li>• <b>Low:</b> Untrusted BSSID, Illegal access without authentication</li> </ul> <p><i>Default is Disabled.</i></p>
<b>Containment Range</b>	<p>Specify the containment range:</p> <ul style="list-style-type: none"> <li>• <b>Same channel:</b> detect AP will countermeasure the APs in the same channel.</li> <li>• <b>ALL channels:</b> detect AP will countermeasure the APs in all channels at the cost of consuming of much AP performance.</li> </ul> <p><i>Default is Same Channel.</i></p>
<b>Sub-string for Spoofing SSID</b>	The AP broadcasting SSID with the specified string will be classified as a Spoofing SSID.
<b>Trusted AP</b>	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.
<b>Untrusted AP</b>	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**.

The screenshot shows the 'Firewall & Security' settings page. The 'Advanced Security Settings' tab is selected. Under the 'ALG' section, the following settings are visible:

- SIP Protocol:** Enabled (toggle switch). Description: Supports both UDP and TCP SIP packets.
- \* Listening Port:** 5060. Range: 1-65535 numbers.
- PTSP Protocol:** Enabled (toggle switch). Description: Supports only TCP RSTP packets.
- \* Listening Port:** 554. Range: 1-65535 numbers.

Buttons for 'Cancel' and 'Save' are at the bottom of the ALG section.

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 in 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 a user username 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.

Profiles > **Add Portal Policy**

\*Name  1-64 characters

Splash page

\*Client Expiration ⓘ  day(s)  hour(s)  minute(s)

Client Idle Timeout ⓘ  5-1440 numbers

Timeout Duration of Unauthenticated Clients (minutes) ⓘ  1-1440 numbers

Failsafe Mode ⓘ ☒

Daily Limit ⓘ

\*Splash Page Customization ⓘ

Landing Page ⓘ

Enable HTTPS Redirection ⓘ ☐

Add Portal Policy

## Internal Splash Page

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

<b>Name</b>	Enter the name of the Captive Portal policy
<b>Splash Page</b>	Select Splash Page type, Internal or External. <i>Note: this table is only about internal splash page.</i>
<b>Client Expiration</b>	Configures the period of validity, after the valid period, the client will be re-authenticated again.
<b>Client Idle Timeout</b>	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>
<b>Timeout Duration of Unauthenticated Clients (minutes)</b>	Set the timeout time for unauthenticated clients. After the timeout, unauthenticated client devices are disabled from using Wi-Fi.
<b>Failsafe Mode</b>	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>
<b>Daily Limit</b>	<ul style="list-style-type: none"> <li>● <b>Disabled:</b> Daily access is not limited.</li> <li>● <b>Limit by Client:</b> Guest can access only once a day.</li> <li>● <b>Limit by Authentication Type:</b> Users can access each authentication mode only once a day.</li> </ul>
<b>Splash Page Customization</b>	Select a splash page from the drop-down list or click " <b>Add New Splash Page</b> ".
<b>Landing Page</b>	Choose the landing page, 2 options are available: <ul style="list-style-type: none"> <li>● Redirect to the Original URL.</li> <li>● Redirect to External Page.</li> </ul>
<b>Enable HTTPS Redirection</b>	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.

<b>Enable Secure Portal</b>	If enabled, HTTPS protocol will be used in the communication between STA and AP. Otherwise, the HTTP protocol will be used.
<b>Pre Authentication Rule(s)</b>	
<b>Destination</b>	Destination can be either IP Address, Hostname or Subnet/Prefix
<b>Service</b>	<ul style="list-style-type: none"> <li>● <b>All:</b> no limitation.</li> <li>● <b>Web:</b> web related services.</li> <li>● <b>TCP Port:</b> input integer between 1~65535.</li> <li>● <b>UDP Port:</b> input integer between 1~65535.</li> <li>● <b>Protocol Id:</b> input related services agreement No.</li> </ul>
<b>Post Authentication Rule Type</b>	<ul style="list-style-type: none"> <li>● If set to “<b>Blocklist</b>”, access to all except the rules added.</li> <li>● if set to “<b>Allowlist</b>”,only access the rules added.</li> </ul>
<b>Post Authentication Rule(s)</b>	
<b>Destination</b>	Destination can be either IP Address, Hostname or Subnet/Prefix
<b>Service</b>	<ul style="list-style-type: none"> <li>● <b>All:</b> no limitation.</li> <li>● <b>Web:</b> web related services.</li> <li>● <b>TCP Port:</b> input integer between 1~65535.</li> <li>● <b>UDP Port:</b> input integer between 1~65535.</li> <li>● <b>Protocol Id:</b> input related services agreement No.</li> </ul>

*Portal Policy – Internal Splash Page*

## External Splash page

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

<b>Name</b>	Enter the name of the Captive Portal policy
<b>Splash Page</b>	Select Splash Page type, Internal or External. <i><b>Note:</b> this table is only about external splash page.</i>
<b>Platform</b>	Select the Radius Authentication Method provided by external portal platform.
<b>If Linkyfi, Purple or Universal Platform is selected</b>	
<b>External Splash Server Address</b>	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.
<b>RADIUS Authentication</b>	Select a RADIUS from the drop-down list or click on " <b>Add New Radius</b> ".
<b>If Aiwifi platform is selected</b>	
<b>URL Pre-shared Key</b>	The configuration will be used to generate the signature. Please enter 20-32 characters, support entering numbers, English, characters (excluding spaces)
<b>Timeout Duration of Unauthenticated Clients (minutes)</b>	Set the timeout time for unauthenticated clients. After the timeout, unauthenticated client devices are disabled from using Wi-Fi.

<b>External page</b>	Please enter the Redirect URL provided by external portal platform.
<b>Enable HTTPS Redirection</b>	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.
<b>Pre Authentication Rule(s)</b>	
<b>Destination</b>	Destination can be either IP Address, Hostname or Subnet/Prefix
<b>Service</b>	<ul style="list-style-type: none"> <li>● <b>All:</b> no limitation.</li> <li>● <b>Web:</b> web related services.</li> <li>● <b>TCP Port:</b> input integer between 1~65535.</li> <li>● <b>UDP Port:</b> input integer between 1~65535.</li> <li>● <b>Protocol Id:</b> input related services agreement No.</li> </ul>
<b>Post Authentication Rule Type</b>	<ul style="list-style-type: none"> <li>● If set to “<b>Blocklist</b>”, access to all except the rules added.</li> <li>● if set to “<b>Allowlist</b>”,only access the rules added.</li> </ul>
<b>Post Authentication Rule(s)</b>	
<b>Destination</b>	Destination can be either IP Address, Hostname or Subnet/Prefix
<b>Service</b>	<ul style="list-style-type: none"> <li>● <b>All:</b> no limitation.</li> <li>● <b>Web:</b> web related services.</li> <li>● <b>TCP Port:</b> input integer between 1~65535.</li> <li>● <b>UDP Port:</b> input integer between 1~65535.</li> <li>● <b>Protocol Id:</b> input related services agreement No.</li> </ul>

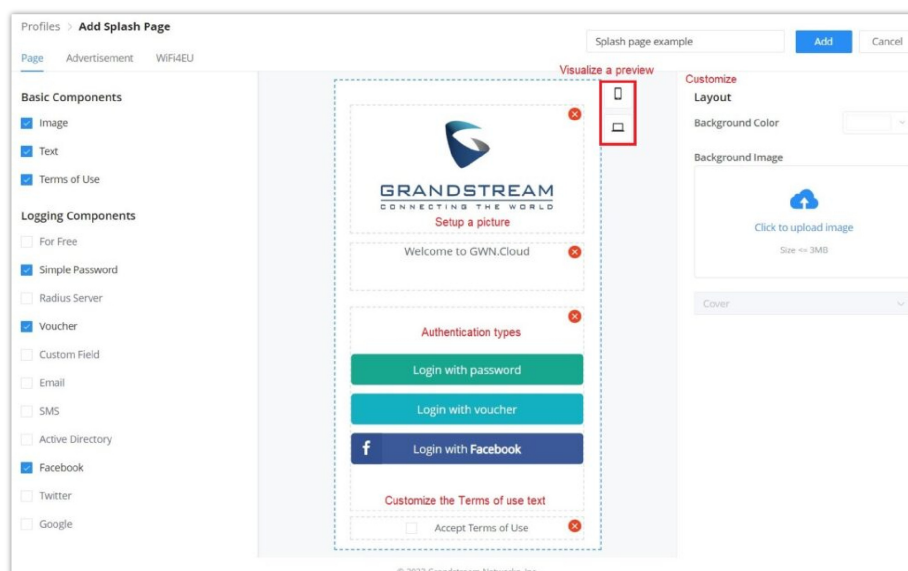
Portal Policy – External Splash Page

## 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 to 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 a very rich manipulation tool.



Users can set the following:

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

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

#### Splash page – *Authentication types*

- Set up a picture (Company Logo) to be displayed on the splash page.
- Customize the layout of the page and background colors.
- Customize the Terms of Use text.
- 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, advertisements can be enabled and forced on each access point, where users will be forced to view media content (images or videos) before being granted access to the network.

Click on the **"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 are 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**.



General

Profile Name

Voice

Native VLAN

7 (VLAN7)

Allowed VLAN

7 (VLAN7)

Voice VLAN

Please enable the Voice VLAN in the Global LAN Settings first

Rate

Auto

Duplex Mode

Self-negotiation

Full-duplex

Half-duplex

Flow Control

Self-negotiation

Disabled

Enable

When duplex mode is "Half-duplex", the traffic control does not take effect.

Enable Port STP

Incoming Speed Limit

Outbound Speed Limit

LLDP-MED

Network Policy TLV

Please enable the Voice VLAN first.

Add port profile – General

Security

Storm Control

Port Isolation

Port Security

802.1X Authentication

Cancel

Save

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"> <li><b>Auto-negotiation:</b> The duplex status of an interface is determined by auto-negotiation between the local port and the peer port.</li> <li><b>Full-duplex:</b> Force full-duplex, and the interface allows sending and receiving data packets at the same time.</li> <li><b>Half duplex:</b> Force half duplex, and the interface only send or receive packets at a time.</li> </ul>
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.

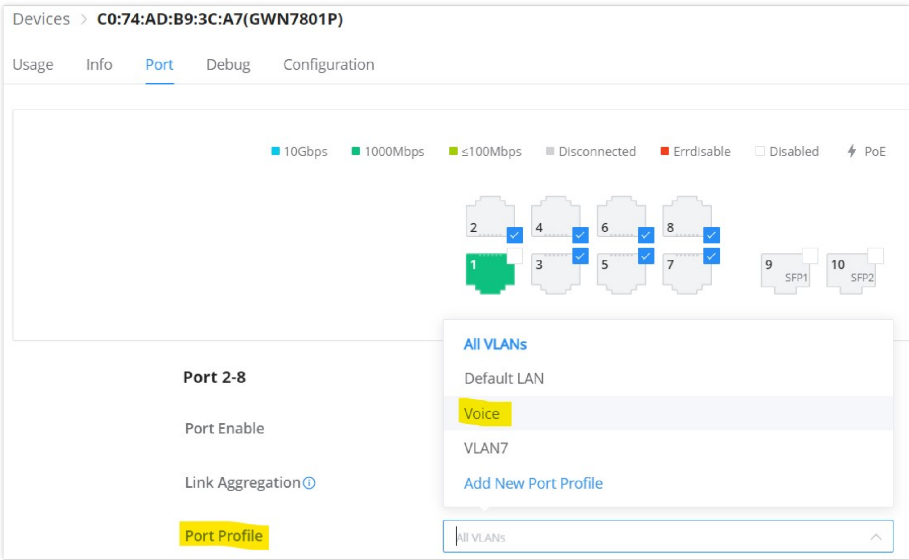
<b>CIR (Kbps)</b>	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
<b>Outbound Speed Limit</b>	Toggle ON or OFF the outbound speed limit.
<b>CIR (Kbps)</b>	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
<b>LLDP-MED</b>	Toggle ON or OFF the LLDP-MED.
<b>Network Policy TLV</b>	Toggle ON or OFF the network policy TLV.
<b>Security</b>	
<b>Storm Control</b>	Toggle ON or OFF storm control.
<b>Broadcast</b>	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
<b>Unknown Multicast</b>	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
<b>Unknown Unicast</b>	Toggle ON or OFF Unknown Unicast and then specify the control threshold (pps = packet per second).
<b>Port Isolation</b>	Toggle ON or OFF port isolation.
<b>Port Security</b>	Toggle ON or OFF port security. <i><b>Note:</b> after enabled, start MAC address learning including the dynamic and static MAC addresses.</i>
<b>Maximum number of MACs</b>	Specify the maximum number of MAC addresses allowed. <i><b>Note:</b> 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>
<b>Sticky MAC</b>	Toggle ON or OFF Sticky MAC. <i><b>Note:</b> 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>
<b>802.1X Authentication</b>	Toggle ON or OFF 802.1x authentication.
<b>User Authentication Mode</b>	Select the user authentication mode from the drop-down list <ul style="list-style-type: none"> <li>● <b>Mac-based:</b> allows multiple users to authenticate without affecting each other;</li> <li>● <b>Port-based:</b> allows multiple users to be authenticated. As long as one user passes the authentication, other users are exempt from authentication.</li> </ul>
<b>Method</b>	Select the method from the drop-down list.
<b>Guest VLAN</b>	Toggle Guest VLAN ON or OFF. <i><b>Note:</b> Enable the Guest VLAN in the Global LAN Settings first.</i>
<b>Port Control</b>	Select the port control from the drop-down list: <ul style="list-style-type: none"> <li>● Disabled</li> <li>● Mandatory authentication</li> <li>● Mandatory non-authentication</li> </ul>

	<ul style="list-style-type: none"><li>• Automatic</li></ul>
<b>Re-authentication</b>	Configures whether to enable re-authentication for the device connected to the port.

*Add port profile*

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

Under the **Devices** page, select the relevant device, and under the **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

Manual

Import

\*

Name

Supports 1-64 characters

MAC

Enter Client Name (Optional)

:

:

:

:

:

Add New Item

Cancel

Add

*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

Cancel

Add

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

Weekly

Time Zone

(GMT+01:00) Casablanca, Monrovia

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.)

Select date

Select time

Cancel

Save

Create Schedule

## RADIUS

This page allows 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	<input type="text"/> 1812	<input type="text"/>

Add New Item +

RADIUS Accounting Servers ⓘ

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

Add New Item +

RADIUS NAS ID ⓘ  0-48 characters

\* Attempt Limit ⓘ  1 1-5 numbers

\* Radius Retry Timeout (s) ⓘ  10 1-120 numbers

\* Accounting Update Interval (s) ⓘ  30-604800 numbers

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

Cancel Save

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 the **"Add"** button to add a new PPSK Group.

Profiles > **Add PPSK Group**

\* Name  PPSK\_Group 1-64 characters

PPSK

Cancel Save

Add PPSK Group

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

**Add PPSK**

Manual Auto Import

\* Number of PPSKs  
1-300 numbers  
 300

\* PPSK Name Prefix ⓘ  
1-60 characters  
 Guests

\* Passphrase Length ⓘ  
8-64 numbers  
 16

\* Max Num of Access Clients ⓘ  
1-100 numbers  
 50

Bandwidth Control ☐

VLAN

Cancel Save

PPSK Autoconfiguration

## 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 of up to 50.

Profiles > **Add PPSK Group**

\* Name  1-64 characters

PPSK

Account Name	Wi-Fi Password	Max Num of Access Clients	MAC	VLAN	Bandwidth Usage	Operation
Guests_1	ep9KKWwT4ALqj3Ty	50	—	—	—	
Guests_2	5Auu25GcsNLcS2n2	50	—	—	—	
Guests_3	5KVePtn2nQANBjuX	50	—	—	—	
Guests_4	Jm8Zbhvjy9gDv8ga	50	—	—	—	
Guests_5	hAQBse4gKYPMgbfv	50	—	—	—	
Guests_6	u64d76m4ShFpevSt	50	—	—	—	
Guests_7	uk7RtDGDpYE9kLU9	50	—	—	—	
Guests_8	gSPsTSyBzFB49uHD	50	—	—	—	

*Add PPSK – Auto*

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

**Add PPSK**

Manual Auto Import

\* Account Name  
1-64 characters

\* Wi-Fi Password  
8-64 characters

\* Max Num of Access Clients ⓘ  
If only one device is allowed to access the PPSK account, a MAC address can be bound to it.

MAC ⓘ  
 :  :  :  :  :

Bandwidth Control

*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.

**Add PPSK**

Manual   Auto   Import

① Please download and use the template to import data [reference template](#)

  
 Click to upload CSV file

PPSK Import CSV file

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

Wi-Fi > **Add Wireless LAN**

**Basic** ^

WiFi ☒

\* SSID ⓘ Guests

Client IP Assignment ⓘ Bridge

Associated VLAN ☐

Enable Captive Portal ☐

SSID Band Dual-Band

**Access Security** ^

Security Type PPSK

\* PPSK Group Select

802.11w ⓘ

Guests

[Add New PPSK Group](#)

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 the client or server side.

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

**Profiles**

- ▼ **schedule** [+ Add](#)
- ▼ **RADIUS** [+ Add](#)
- ▼ **PPSK** [+ Add](#)
- ▲ **Certificates**

[Import](#) [+ Add](#)

Name	Certificate Type	Issuer	Valid for	Operation
Server Cert	Server	GS CA Cert	2297-07-04 12:24PM	<a href="#">Download Cert or Key</a> <a href="#">Revoke Cert</a>
- ▼ **Client Time Policy** [+ Add](#)
- ▼ **Hotspot 2.0** [+ Add](#)

Profiles – Certificates

This page will be shown after clicking on the “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

2048

Digest Algorithm

SHA256

\* Expiration (D)

SAN

☒ None ☐ IP Address ☐ Domain

Country/Region

United States

\* State/Province

\* City

\* Organization

\* Organizational Unit

\* Email

Cancel

Save

Profiles – Add CA Certificate

Type	Select the type of certificate either <b>CA Certificate</b> 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"><li>● <b>2048</b>: 2048-bit keys are a good minimum. (Recommended).</li><li>● <b>4096</b>: 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.</li></ul>
Digest Algorithm	<p>Select the digest algorithm.</p> <ul style="list-style-type: none"><li>● <b>SHA256</b>: This digest algorithm generates an almost unique, fixed-size 256 bit hash.</li></ul> <p><b>Note:</b> 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: "EMEAreion@grandstream.com"
-------	--

### Profiles – Add CA Certificate

Profiles > Add Certificate

Type

☐ CA Certificate
☒ Certificate

\* Name

Server Cert

\* CA Certificate

CA Cert

Certificate Type

☒ Server
☐ Client

Key Length

2048

Digest Algorithm

SHA256

\* Expiration (D)

999

SAN

☒ None
☐ IP Address
☐ Domain

Country/Region

United States

\* State/Province

Massachusetts

\* City

Boston

\* Organization

Grandstream

\* Organizational Unit

Grandstream

\* Email

GS@grandstream.com

Cancel

Save

### Profiles – Add Certificate (Client or Server)

Type	Select the type of certificate either CA Certificate or <b>Certificate</b> .
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	<p>Choose the key length for generating the CA certificate. The following values are available:</p> <ul style="list-style-type: none"> <li>● <b>2048:</b> 2048-bit keys are a good minimum. (Recommended).</li> <li>● <b>4096:</b> 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.</li> </ul>
Digest Algorithm	<p>Select the digest algorithm.</p> <ul style="list-style-type: none"> <li>● <b>SHA256:</b> This digest algorithm generates an almost unique, fixed-size 256 bit hash.</li> </ul> <p><b>Note:</b> 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 that will dictate how much a client connects to the Wi-Fi if this policy is applied for the SSID.

Add Time Policy

Enable Time Policy

\*

Name

Supports 1-64 characters

Time Policy

\*

Validity Time

0

d

1

h

0

m

\*

Reset Cycle

Reset Daily

\*

Reset Time

12

:00

AM

Time Zone

(GMT+01:00) Casablanca, Monrovia

Cancel

Add

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 minute to 365 days.
Reset Cycle	Set up a Reset mode: Daily, Weekly, or Periodically
Reset Time	When the Reset Cycle is Daily: configure the time of the day. When the Reset Cycle is Weekly: configure the time and the day of the week When the Reset Cycle is Periodic: 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.

Profiles > Add Hotspot 2.0

**General** ^

\* Name

Domain ID

\* HESSID ⓘ

Network Access ☒ Internet Access

Network Type

IPv4 Type

IPv6 Type

Network Auth Type ⓘ

**Venue** v

**Operator Name** v

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 United States

Timezone (GMT+01:00) Casablanca, Monrovia

Auto Sync Time

\* AP Login Password

Device Password

LED Always on

Reboot Schedule None

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 <b>Devices</b> → <b>GWN device</b> → <b>Info</b> 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 the form of a downloadable link providing a CSV file format containing all the website logs visited for each client during the defined period (daily, weekly, or monthly basis).

To enable this feature, follow the below steps:

1. Go under "**Settings** → **System page** → **URL Access Log section**" and enable the URL Access Log field, this will configure the GWN Manager System to start recording the website logs visited by the clients.
2. The option "**Group Metric by Main Domain**" can be also enabled then the user can configure 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).
3. Enable Export URL Access Log.
4. Administrators can choose to set the Email Frequency to be generated either on a daily, weekly, or monthly basis.
5. Configure the URL Log Receiver Email.

The screenshot shows the 'System' settings page. The 'URL Access Log' section is highlighted with a red box. It contains the following settings:

- URL Access Log**: Enabled (toggle switch).
- Group Metric by Main Domain**: Enabled (toggle switch).
- Customized Top-level Domain**: .us.com (text input field).
- Export URL Access Log**: Enabled (toggle switch) with a link to 'Export Immediately'.
- Email Frequency**: Monthly (dropdown menu).
- \* URL Log Receiver**: admin@gs.com (text input field).

There are 'Add New Item' buttons (green plus icons) next to the 'Customized Top-level Domain' and 'URL Log Receiver' fields.

URL Access Log

In this example, the administrator will start receiving, every week, 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.

The 'Export' dialog box is shown. It has a title bar with 'Export' and a close button. The main content area has a blue header with an information icon and the text 'Specify the time range of the URL Access Log to be exported.' Below this, there is a section for 'For the Last' with a sub-label '1-30 integers'. A text input field contains the number '7', followed by the label 'day(s)'. At the bottom, there are 'Cancel' and 'Export' buttons.

Export Immediately

5. Click on the "**Export**" button and notice the success confirmation message:

The confirmation message is displayed in a light blue box with a close button. It says 'Export succeed!' and includes a link 'Click to download URL Access Log'.

Export Succeed

6. 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, the client's hostname as well as 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/i	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://netets.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.googleap	
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. To enable this feature, follow the below steps:

1. Go under **"Settings → System page → Guest Information section"** and enable the 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.

System

URL Access Log

Guest Information

Email Guest Information
☒
Email Frequency
Weekly
\* Email Receiver
Admin@grandstream.com
Add New Item

NAT Pool

SNMP

Syslog

Cancel
Save

Guest Information

## NAT pool

Users can use this feature 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 lightweight router.

#### Note:

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

System

URL Access Log

Guest Information

**NAT Pool**

\* Default Gateway: 10.1.0.1

\* DHCP Server Subnet Mask: 255.255.255.0

\* DHCP Release Time (mins): 720 (2-525600 numbers)

DHCP Preferred DNS

DHCP Alternate DNS

SNMP

Syslog

Cancel Save

NAT Pool

Navigate to **Web UI** → **Settings** → **System page (NAT Pool section)**, 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 the SNMP feature under **Web UI** → **Settings** → **System page (SNMP section)**.

System

NAT Pool

**SNMP**

SNMPv1, SNMPv2c: ☒

\* Community String: public (1-32 characters)

SNMPv3: ☒

\* Username: (1-64 characters)

Authentication Mode: MD5

\* Authentication Password: (8-32 characters)

Privacy Mode: DES

\* Privacy Password: (8-32 characters)

Syslog

Cancel Save

SNMP

<b>SNMPv1, SNMPv2c</b>	Enable Enable SNMPv1/SNMPv2c.
<b>Community String</b>	Enter the SNMP Community string.
<b>SNMPv3</b>	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>
<b>Username</b>	Enter the SNMPv3 username.
<b>Authentication Mode</b>	Set the Authentication mode to: either MD5 or SHA.

<b>Authentication password</b>	Enter the SNMPv3 authentication password.
<b>Privacy Mode</b>	Set the Privacy mode to: either AES128 or DES. <i><b>Note:</b> AES128 mode is only for routers and APs. Switches use DES mode.</i>
<b>Privacy password</b>	Enter the privacy password.

SNMP

Syslog

Configure Syslog settings 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

Cloud Syslog Server

Syslog Level

Debug

Syslog Capture Expiration ⓘ

0

day(s)

0

hour(s)

10

minute(s)

Devices ⓘ

GWN7052(C0:74:AD:9... X GWN7605LR(C0:74:A... X

Syslog Capture

Delete

Search MAC

GWN7052  
C0:74:AD:95:12:90

GWN7605LR  
C0:74:AD:20:EE:1C

GWN7801P  
C0:74:AD:B9:3C:A7

Cancel

Save

Syslog

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

Syslog

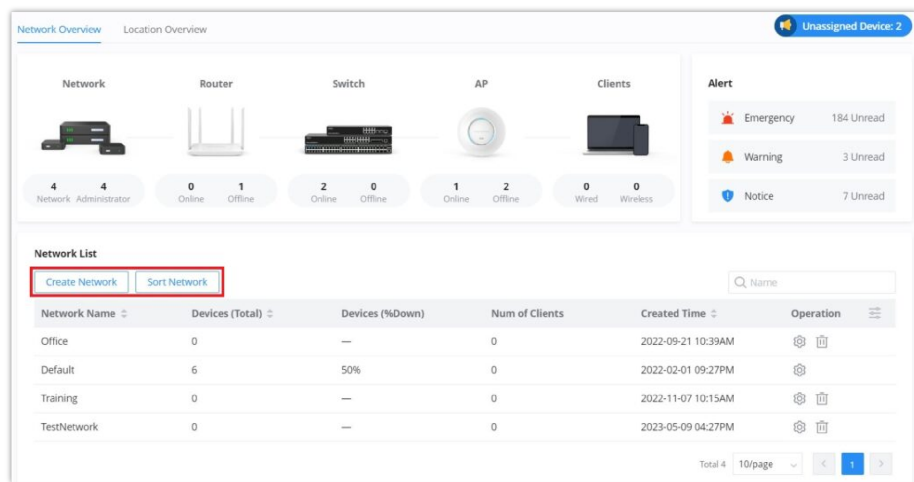
ORGANIZATION

Overview

Network Overview

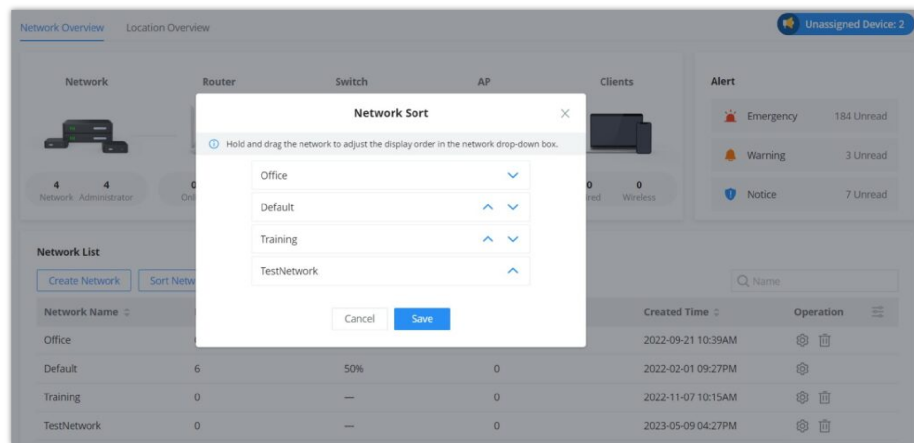


The overview page offers a bird’s-eye look at all the GWN devices that have been added to the organization. This includes GWN routers, GWN switches, GWN APs, and clients. In addition to that, the user can see the number of networks created by that organization and the number of administrators in the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



Organization – Overview

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

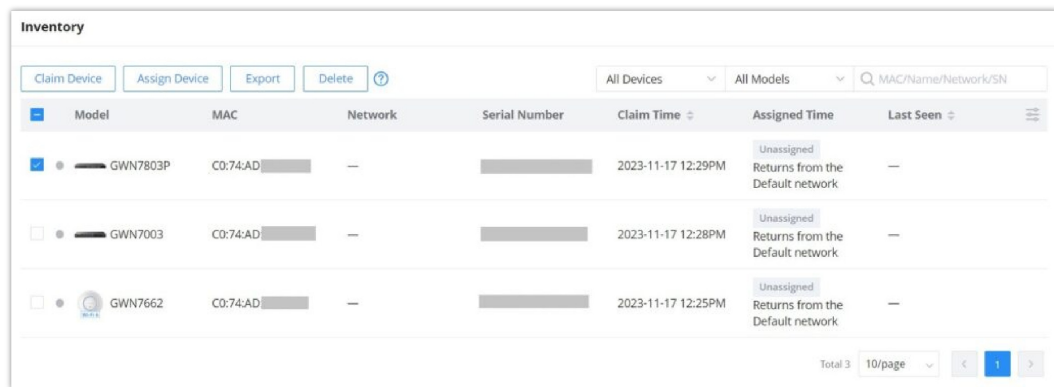


Organization – Overview – Sort network

Inventory

The 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 the “**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, it will not be assigned to any network.

Claim Device

Manual

Import

\* Device MAC Address

c0

:

74

:

ad

:

ff

:

ff

:

ff

\* Password

To view the Device Label

.....

Cancel

Claim

Inventory – Claim Device

- **Assign Device:** to assign the device to the 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.

	A	B	C	D	E	F	G
1	Model	Mac	Network	Serial Number	Claimed Time	Assigned Time	Last Seen
2	GWN7661	C0:74:AD	—		2023-10-27 04:11PM	Unassigned	—
3	GWN7624	C0:74:AD	—		2023-10-27 02:38PM	Unassigned	2023-10-27 04:09PM
4	GWN7813P	C0:74:AD	Default		2023-10-27 02:16PM	2023-10-27 02:16PM	2023-10-27 03:59PM

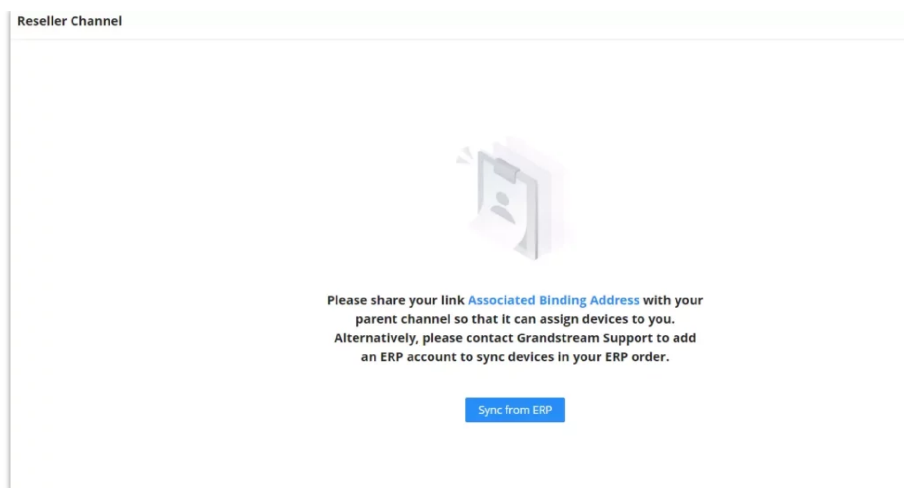
Inventory – Export

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

Reseller Channel

Reseller Channel will be able to support the establishment of the hierarchy agent partnership, retrieve device from ERP, and assign device to network groups or channels/agents:

1. Support first-level channel or agent to bind the ERP ID and sync the device.
2. Support assigning/returning/reclaiming device to network or associated company.



Reseller channel

### Note:

Please share your link Associated Binding Address with your parent channel so that it can assign devices to you. Alternatively, please contact Grandstream Support to add an ERP account to sync devices in your ERP order.

Reseller Channel							
<a href="#">Sync from ERP</a> <a href="#">Assign to Network</a> <a href="#">Assign to Associated Company</a> <a href="#">Export</a> <a href="#">Reclaim Device</a> <a href="#">Return Device</a>							
All Models	From All	All Status	All associated com	Q: MAC			
Device Model	MAC	Serial Number	Origin	Storage Time	State	Assign to	Operation
GWN7600	C074AD:00:00:03	---	chidam2@gs.com	22/12/2023 01:29	Returned	chidam2@gs.com	
UCM6104	00:0B:82:8D:E7:76	21AWLSAG308DE776	yxuu company1234	28/11/2023 01:40	Unassigned	---	
UCM6104	00:0B:82:8D:E7:74	21AWLSAG308DE774	yxuu company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8E:5C:C9	24UMHVG3086CC9	yxuu company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:F9	24UMHVG3086F9F9	yxuu company1234	28/11/2023 01:40	Unassigned	---	
UCM6102	00:0B:82:8D:D4:7A	21AWLJLG308ED47A	yxuu company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:F8	24UMHVG3086F9F8	yxuu company1234	28/11/2023 01:40	Unassigned	---	
UCM6102	00:0B:82:8D:D4:7B	21AWLJLG308ED47B	yxuu company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:FE	24UMHVG3086F9FE	yxuu company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8E:5C:BB	24UMHVG30865CBB	yxuu company1234	28/11/2023 01:40	Unassigned	---	
Total 59 10 pages							

Reseller channel – example

## Users

User Management allows the administrators to create multiple accounts for different users to log in to the platform. There are 6 base different access levels to monitor and manage GWN devices, it's also possible to create a [custom role](#) with custom privileges.

- Super Administrator (the initial administrator)
- Platform Administrator
- Platform Administrator (Read Only)
- Network Administrator
- Network Administrator (Read Only)
- Guest Editor

<b>Super Administrator</b>	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).
<b>Platform Administrator</b>	This account can create networks and create platform administrators, network administrators, and guest administrators.
<b>Platform Administrator (Read-only)</b>	This account has read-only access to networks and sub-accounts.
<b>Network Administrator</b>	Under this account, all network and sub-accounts have read/write permissions and can create guest administrators for their managed networks.
<b>Network Administrator (Read-only)</b>	This account has read-only permissions for its networks.
<b>Guest Editor</b>	This account has read/write permissions for limited management features within a specified network.

User Management – base roles

### 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 User

To add a new user, navigate to **Organization** → **Users** → **User** page, then click on **"Add"** button to add a new user. Then specify the nickname, email address, Role, and the networks allowed to be accessed by this user in all regions, there is also the option to enable multi-factor authentication or to add the user to newly created networks automatically.

Add User

Nickname

0-64 characters

Support

\* Email Address

Supports 1-64 characters

Support@grandstream.com

\* Role ⓘ

Network Administrator (Read-only)

Multi-Factor Authentication

☐

\* Network

World EU Region China

HOTEL1

☒ Auto Add New Network

Cancel

Add

Add user

## Roles

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 navigate to **Organization** → **Users** → **Roles**, then click on **"Add"** as shown below:

Users		
User	Roles	Associated Company Account Security Settings
Add		
Role Name	Description	Operation
Technicien	helps in troubleshooting	<input checked="" type="checkbox"/> <input type="checkbox"/>
GWN App User	Basic Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>
Support Team	help resolve issues	<input checked="" type="checkbox"/> <input type="checkbox"/>
Super Administrator	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	This account can create networks and create platform administrators, network administrators, and guest administrators.	
Platform Administrator (Read-only)	This account has read-only access to networks and sub-accounts.	
Network Administrator	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)	This account has read-only permissions for its networks.	
Guest Editor	This account has read/write permissions for limited management features within a specified network.	

Roles page

Under **"Organization"** tab, select the organization privileges for this user.

Users > Add Role (For GWN.Cloud)

\* Role Name  1-64 characters

Description  0-256 characters

\* Privilege Content

Organization Network

☐ All Organization Privilege

☒ Overview

☒ Network Overview (Read-only) ☒ Location Overview (Read-only) ☐ Configure Network

☐ Network Sort ☐ Share Network ☐ Configure Map Component

☒ Inventory

☒ Device Information (Read-only) ☐ Export Device Information

☐ Reseller Channel

☐ Reseller Channel List (Read-only) ☐ Configure Reseller Channel Info

☐ Users

☐ User List (Read-only) ☐ Role List (Read-only) ☐ Associated Company (Read-only)

☐ Configure User ☐ Configure Role ☐ Configure Associated Company

☒ Upgrade

☒ Upgrade Information (Read-only) ☒ Upgrade Configuration

### Add Role – Organization Privileges

Under “**Network**” tab, select the network privileges for this user.

Users > Add Role (For GWN.Cloud)

\* Role Name  1-64 characters

Description  0-256 characters

\* Privilege Content

Organization **Network**

☐ All Network Privilege

☐ Dashboard

☒ Devices

☒ Device Information (Read-only) ☐ Add Device ☒ Export Device Information

☐ More Buttons ☒ Device Configuration ☐ Remote Access ☐ Clear Traffic

☐ Auto Configuration Delivery ☐ Bridge device ☒ Speed Test ☐ Locate device

☒ Debug device ☐ PoE Port Configuration ☒ Port Configuration ☐ Group Management

☐ Web CLI

☒ Clients

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

☐ Subscribe to Client Historical Data ☐ Clear Traffic

☒ Online Status

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

### Add Role – Network Privileges

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

**Add User**

Nickname  
0-64 characters

\* Email Address  
Supports 1-64 characters

\* Role

Multi-Factor Authentication  
☐

\* Network  
**World** EU Region China

☐ Auto Add New Network

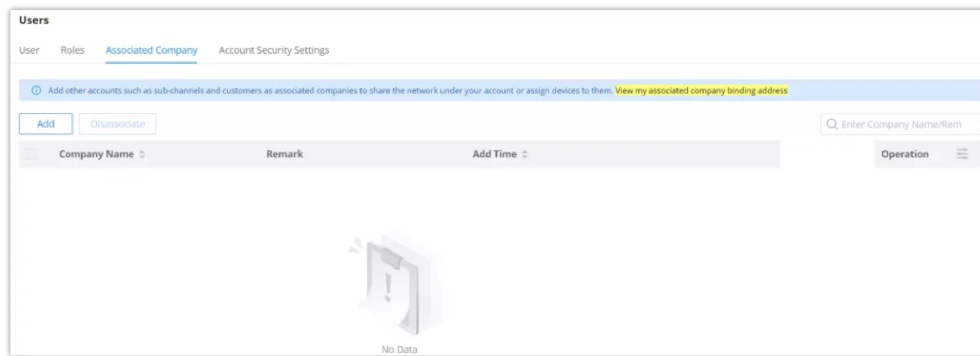
**Note:**

Custom role users can also log into the GWN APP.

## Associated Company

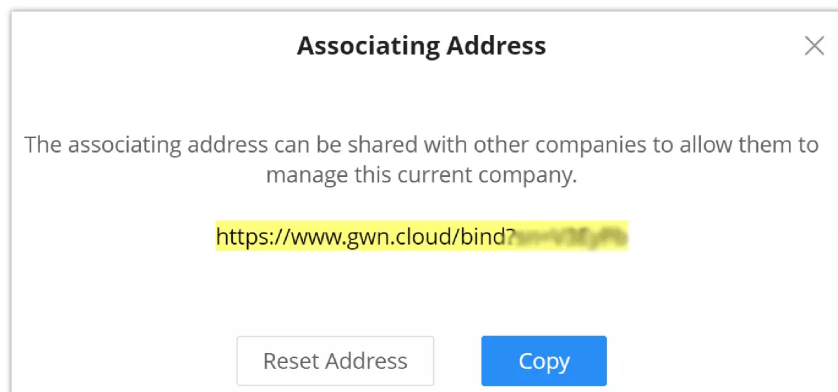
Users can add other accounts, such as sub-channels and customers, as Associated Companies. They can then share their network with them under the user name or assign devices to them.

Navigate to **Organization → Users → Associated Company**, then click on **"Add"** button to add an associated company.

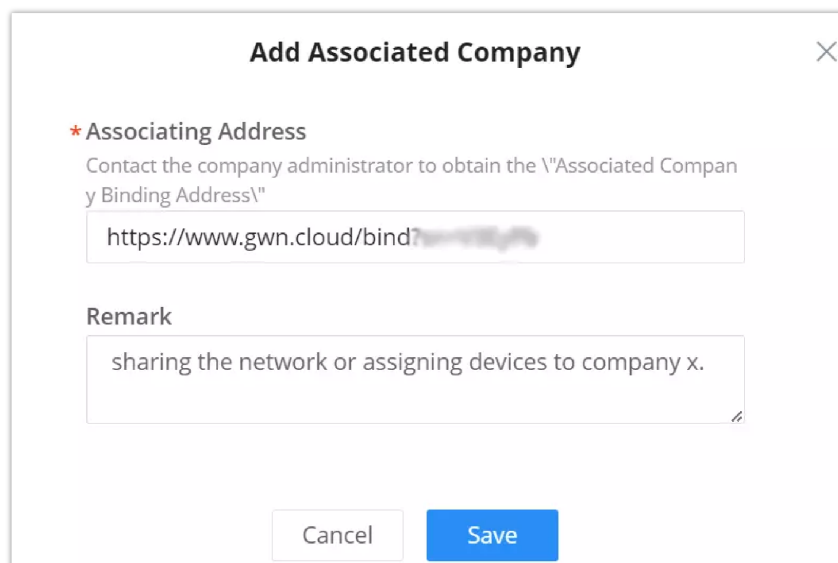


Associated company binding address

To add an associated company, the associating address is required, and it can be found under **Organization → Users → Associated Company**, then click on **"View my associated company binding address"** as shown above.



Associated company binding address



Add associated company

Once the associated company is added, devices under **Organization → Inventory** can be assigned to the newly added associated company, as shown in the example below:

Inventory

[Claim Device](#)
[Assign to Network](#)
[Assign to Associated Company](#)
[Export](#)
[Delete](#)

All Devices ▾ All Models ▾ Q MAC/Name/Network/Serial

Device Model	MAC	Network	Serial Number	Claim Time	Assigned Time	Last Seen
GWN7813P	C0:74:AD:CC:DF:18	—	20VXV6KP22CCDF18	2024/02/28 11:33AM	Unassigned Returns from the Jawad_Labs network	2024/02/28 05:55PM

Assign to associated company

Inventory > Assign to Associated Company

⚠ Devices assigned to associated companies will automatically be removed from your inventory.

\* Associated Company: Workkium

\* Target Device(s): ☒ Specify Device ☐ Enter MAC address

All Models ▾ Q MAC

MAC	Device Model	MAC	Device Model	Operation
C0:74:AD:CC:DF:18	GWN7813P	C0:74:AD:CC:DF:18	GWN7813P	⊖

Total 1 10/page < 1 >

[Cancel](#) [Assign](#)

Assign devices to associated company

It's also possible to share an entire network with an associated company under **Organization** → **Overview** (the default network can't be shared with an associated company). Please check the example below:

Overview > Jawad\_Labs

[Share Network](#)

\* Network Name: Jawad\_Labs 1-64 characters

\* Country/Region: Morocco(المغرب)

\* Time Zone: (GMT+01:00) Casablanca, Monrovia

Network Administrator: support@grandstream.com

[Cancel](#) [Save](#)

Share a network with Associated Company

Share Network

☐ 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.

Share with

☐ account name  
 Can only be shared with admin accounts in the same region.

☒ Associated Company  
 Can only be shared with associated companies in the same region.

Workkium

[Cancel](#) [Save](#)

Share a network with Associated Company

## Account Security Settings

To enhance GWN.Cloud security, users can enable **Password Security** and with this option the users can set a password expiration period (days) where the password must be changed and even not be the same as the previous one(s). Also account idle timeout and login duration can be configured here (minutes). Multi-Factor authentication can be enabled on all accounts.

**Note:**

Account Security Settings affects all accounts (including this account), and only this account can view these settings.

Users

UserRolesAssociated CompanyAccount Security Settings

Account Security Settings affects all accounts (including this account), and only this account can view these settings.

Password Security

Password Security

\* Password Expiration (days)

90

30-180 numbers

\* No Repeating Passwords

1

1-20 numbers

Account Security

\* Idle Timeout (min)

180

5-1440 numbers

Login Duration (min)

720

5-1440 numbers

Multi-Factor Safety Authentication

Once enabled, all accounts will be enabled.

Cancel

Save

Account Security Settings

Password Security	
Password Security	Toggle on/off the password security.
Password Expiration (days)	Specify the number of days of validity of a password. Once the number of days configured has elapsed, the user will be prompted to change his/her password upon login.
No Repeating Passwords	Settings this option will prevent the user from using a password which he/she had previously used. You can set the number of previous passwords which have been used to prevent them from being used again as a new password.
Account Security	
Idle Timeout (min)	<div>This configures the number of minutes of a user being idle on the web GUI before he/she can be automatically logged out by the system. The user can enter a value from 5 to 1440 minutes. Configuring this value is required.</div> <div><b>Note:</b> The default value is 180.</div>
Login Duration (min)	<div>This configures the number of minutes a login session can last before the user is logged out automatically by the system. The user has to log in again to start after being logged out.</div> <div><b>Note:</b> The user can enter a value between 5 and 1440</div>
Multi-factor Authentication	If MFA is enabled, all accounts (including this account) will be required to use multi-factor authentication. This cannot be disabled by other users. If disabled, users will be able to toggle MFA for their own accounts.

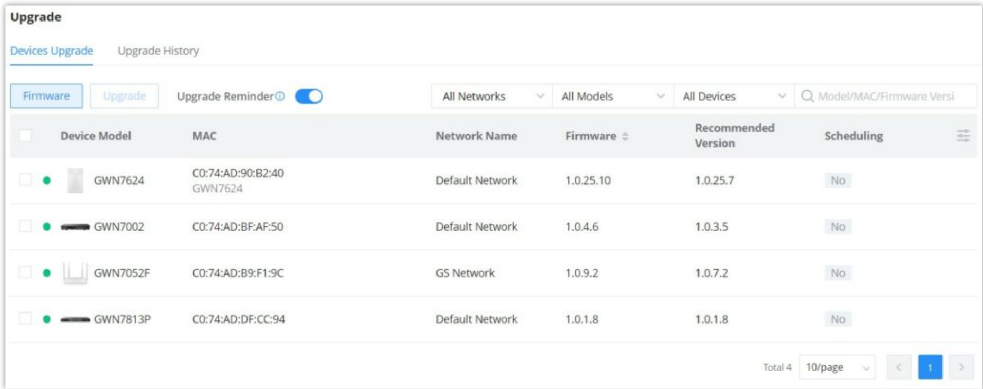
Account Security Settings



# Upgrade

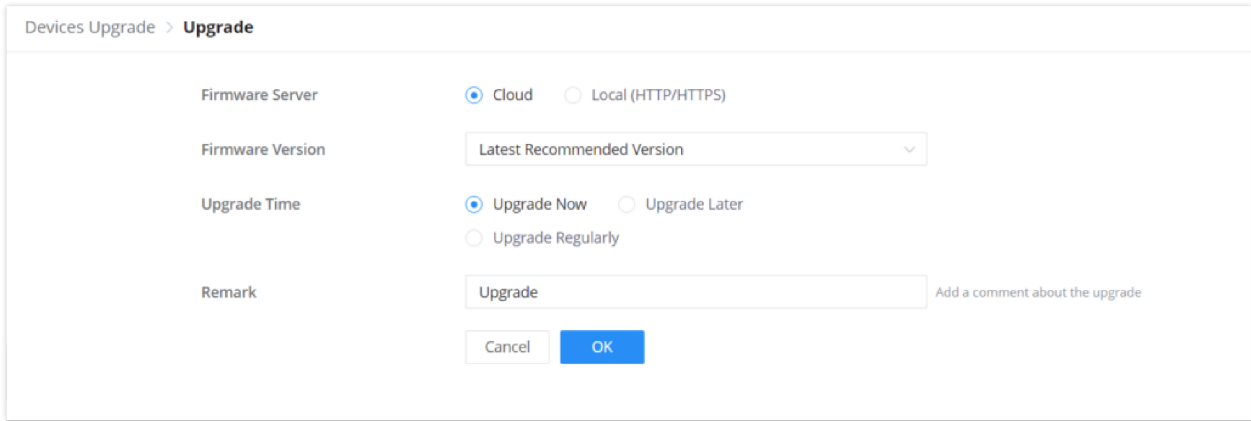
## Devices Upgrade

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



Upgrade

Select the devices you wish to upgrade then click **“Upgrade”**. Under **“Firmware Version”** the users can select which version to upgrade to (Beta Firmware is also supported but not recommended).

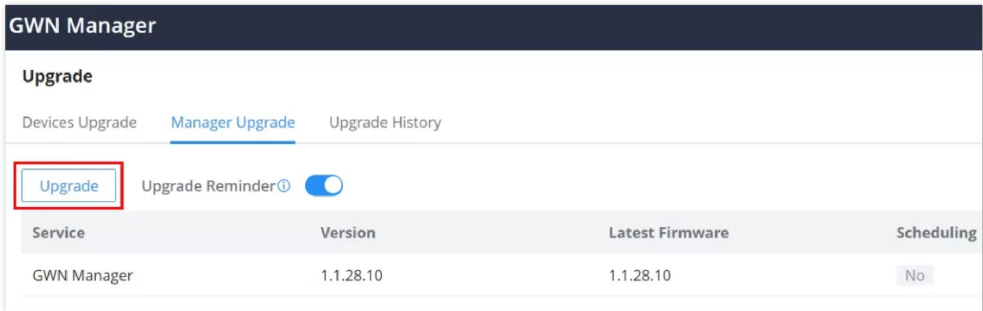


Upgrade in Batches

## Manager Upgrade

The users can upgrade the GWN Manager directly from the Web UI, by navigating to **Organization → Upgrade** page → **Manager Upgrade** tab.

On this page, the users can see the current version and the latest firmware available, to upgrade to the latest firmware, please click on **“Upgrade”** button as shown below:



Manager Upgrade

The users have the option to upgrade now, upgrade later or upgrade regularly, a remark or comment about the upgrade can be also added. The overall features related to the upgrade will be listed under.

GWN Manager

Upgrade > Manager Upgrade

Upgrade

Latest Firmware

Upgrade Time

☒ Upgrade Now
☐ Upgrade Later
☐ Upgrade Regularly

Remark

Manager Upgrade

Add a comment about the upgrade

Release Note

GWN\_Manager 1.1.28.10

1. Supports link speed display for Aps on the device list  
2. Supports cloning the LAN and wired firewall configuration  
3. Added Beta firmware display and supports upgrading to Beta  
4. Optimize client list Sorting  
5. Supports Local WAN Configuration Synchronization  
6. Added Phone Number length Settings for the authentication of Splash Page  
7. Optimized Feedback entry  
8. Added PPSK configuration, inventory information acquiring, and switch port information acquiring for API  
9. Internal bug fixes

Cancel

OK

Upgrade the GWN Manager

## 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.

Upgrade

Devices Upgrade

Upgrade History

Q Device MAC

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	<input checked="" type="checkbox"/> Schedule ID <input checked="" type="checkbox"/> Device Type <input checked="" type="checkbox"/> Device Model <input checked="" type="checkbox"/> Device Number <input checked="" type="checkbox"/> Target Version <input checked="" type="checkbox"/> Upgrade Status <input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> Scheduled Time <input checked="" type="checkbox"/> Remark

Total 1 10/page

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 (client count, bandwidth usage, client and guest statistics...etc.)

Report

Report Management

Generated Report

Create Report

Search Title

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	

Total 2 10/page

Report

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

Report

Create Report

\*Title

Daily

1-64 characters

\*Network

Staff

\*Report Contents

☒ Clients Count

☒ Bandwidth Usage

☒ Client Statistics  
(Client Manufacturer, Client OS, New Clients, Return Clients, Average Duration)

☒ Guest Statistics  
(Guest sessions and guest authentication sessions)

☒ Top Devices

Top 5

☒ Top Clients

Top 5

☒ Top SSIDs

Top 5

☒ Top Websites

Top 5

Report Frequency

Daily

Report Generate Time

Now

Email Address

javad@grandstream.com

Add New Item

Cancel

Save

Create a report

The following table explains 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. <b>Note:</b> The maximum number of 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"> <li>• <b>Clients Count:</b> reports the number of clients for all the SSIDs under the selected network group.</li> <li>• <b>Bandwidth Usage:</b> The download and upload level statistics for all the SSIDs for the selected network group</li> <li>• <b>Clients Statistics:</b> reports the statistics for the different client manufacturers, client OS, the number of new clients as well as the return clients, and the average duration.</li> <li>• <b>Guest Statistics:</b> reports statistics about the clients connected via the Captive portal including the Guest New session, the Max concurrent New session, and the login failure.</li> <li>• <b>Top Devices:</b> reports the top 5/20/50 devices that consumed the max of the bandwidth/data.</li> <li>• <b>Top Clients:</b> Lists the top 5/20/50 clients that downloaded/uploaded the max of data</li> <li>• <b>Top SSIDs:</b> reports the top 5/20/50 SSIDs that are mostly used by clients.</li> <li>• <b>Top Websites:</b> reports the top 5/20/50 websites that are mostly visited by clients.</li> </ul>
Report Frequency	Specify the report frequency to be generated either daily, weekly, monthly, or custom range.
Date	Specify the Start and Date for the report to be generated when selecting "Custom Range" as <b>Report Frequency</b> .
Report Generate Time	Select either to generate the report now or at a later time
Time	Specify when you want the report to be generated. This field appears 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

Change Log

Start Date

End Date

Search Administrator/IP/Network

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

Total 7

10/page

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

Reset

Restrict APIs to specific networks

Disable API Developer Mode

API Developer

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

## MANAGER SETTINGS

**Note:**

Manager Settings is only available for GWN Manager.

Manager Settings

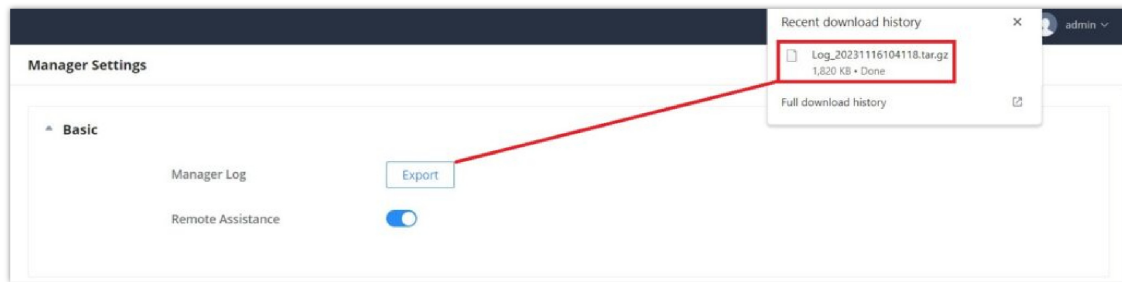
Basic

SMTP Server

Backup & Restore

## Basic

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



Manager Settings – Basic

## SMTP Server

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

A screenshot of the 'SMTP Server' configuration form. It 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'. At the bottom, there 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' window with the 'Backup & Restore' section expanded. It contains two main options: 'Upload Backup' with an 'Upload' button and 'Manual Backup' with a 'Backup' button. Below these is a 'Backup Settings' section with a 'File Storage Path' field containing '/gwn\_backup' and a 'Retained Data Backup' toggle switch. At the bottom are 'Cancel' and 'Save' buttons.

*Backup and Restore*

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

## 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 1.1.28.9 – 1.1.28.10

Product Name: GWN.Cloud(1.1.28.9) and GWN Manager(1.1.28.10)

- Supports link speed display for APs on the device list. [\[Devices\]](#)
- Supports L2TPv3 configuration on GWN7660 series APs (supported only GWN.Cloud) [\[GWN AP L2TPv3\]](#)
- Supports cloning the LAN and wired firewall configuration [\[Create a new network\]](#)
- Added Beta firmware display and supports upgrading to Beta. [\[Requirements\]](#)
- Optimized client list sorting. [\[Clients\]](#)
- Supports local WAN configuration synchronization. [\[Add device to GWN.Cloud\]](#)
- Optimized Feedback entry. [\[Feedback\]](#)

- Added PPSK configuration, inventory information acquiring, and switch port information acquiring for API. [\[API Developer\]](#)
- Added GWN Manager Upgrade support [\[Manager Upgrade\]](#)

### Version 1.1.27.13

Product Name: GWN.Cloud and GWN Manager

- Added Regions/Systems Switch to allow multiple regions/systems to be opened. [\[Region settings\]](#)
- Upgraded Account Permission, allowing comprehensive management of all Grandstream services and enable all systems in the selected region. [\[Merge Accounts\]](#)
- Added Associated Company to support cross-region/cross-system management on channels and customers for network sharing and device allocation. [\[Associated Company\]](#)
- Added Reseller Channel to support the establishment of hierarchy in agent partnership, obtain device from ERP, and assign device to network groups or channels/agents. [\[Reseller Channel\]](#)
- Optimized User Management, unified management of account and password security. [\[account security settings\]](#)
- Optimized Personal Settings page and added user type settings. [\[Personal Settings\]](#)
- Added API support for exporting the switch information, mainly the information and port modules in the switch details, and the information of the global switch settings. [\[API\]](#)
- Added API support for PPSK configuration. [\[API\]](#)

### 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 log in 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, and pre-set features for switches in the group. And a new way to select device groups in multiple businesses. [\[Group management\]](#)
- 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, and 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 the 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" on the external splash page [\[Portal Policy\]](#)
- Support the option "URL Pre-shared Key" when selecting Aiwifi as the platform of the 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 the 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 the 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 statistics by Main Domain rather 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 for deleting the voucher in use. [[Voucher](#)]
- Added support of client name in CSV file when importing access list. [[Access List](#)]
- Added configuration of secondary radius server for WLAN 802.1x authentication. [[Wi-Fi Settings](#)]
- Added WPA3 support in the 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: the 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 the GWN Cloud page. [[Feedback](#)]
- 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 an 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.**

---