

Grandstream Networks, Inc.

GDMS Networking

User Manual



Overview

GDMS Management is an enterprise-grade platform designed to provide a unified, centralized management system for a wide range of network and communication devices. It integrates GDMS Networking and GDMS Unified Communications to offer comprehensive oversight and control over network and communication infrastructure.

GDMS Networking is a core component of the GDMS Management platform, focused specifically on managing network devices. It provides a streamlined and centralized approach to handle access points (APs), routers, switches, and GCC devices. It simplifies and enhances network management, ensuring efficient, secure, and high-performance operations across multiple locations through an intuitive interface. GDMS Networking is a cloud-based solution while GWN Manager serves as the on-premise solution for robust network management within a local environment. Both solutions support the GDMS App on iOS® and Android® for mobile network management and monitoring.

PRODUCT OVERVIEW

Features Highlights

GDMS Networking	<ul style="list-style-type: none">• Software-as-a-Service (SaaS) Solution to manage all your Grandstream products (Access points, Routers, switches and All-in-one convergence devices), without any additional on-premise infrastructure.• High level security, since all the traffic between devices and cloud is secured.• Easy way to add new devices, either using device MAC address or Mobile App (Android® or iOS®).• No limits on number of sites or devices.
GWN Manager	<ul style="list-style-type: none">• Linux® (CentOS7, AlmaLinux9 and Ubuntu) based solution to secure and manage all your Grandstream devices.• Automatically discover and Adopt devices in your network.• Adopt device manually using SSH or through Web GUI by setting the Manager address and port.• Up to 50 000 devices, with high performance hardware.
Shared	<ul style="list-style-type: none">• Highly available with no single point of failure across the whole system.• Easy and intuitive dashboard for monitoring.• Network Group creation.• Devices and clients Centralized monitoring and management.• Captive portal configuration.• Bandwidth control per SSID, IP, or MAC address.• Unified GWN/GCC device management (GWN Routers, GWN Switches, GWN APs and GCC devices)• Inventory management• Map to locate devices and Heatmap.• Network topology

Features Highlights

Specifications

Function	<ul style="list-style-type: none">• Network-based GWN/GCC devices management• Network/devices/client monitoring
----------	--

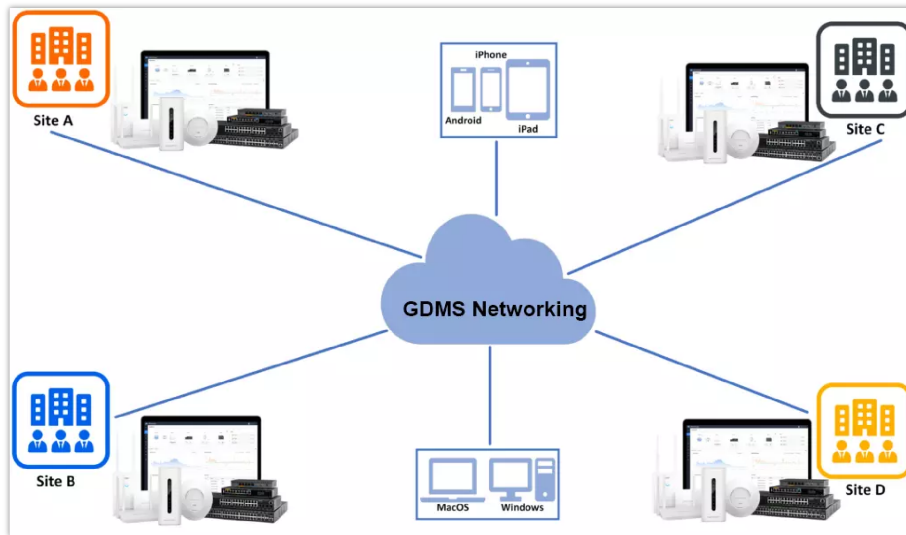
Security and Authentication	<ul style="list-style-type: none"> • Supports access policies configuration (blacklist, whitelist, time policy etc) • Multiple security modes including WPA, WPA2, WPA3, WEP, open, etc. • Bandwidth rules for client access • User and privilege management
Enterprise Features	<ul style="list-style-type: none"> • No limits on number of sites or devices for GDMS Networking and up to 50 000 devices for GWN Manager with high performance hardware. • Hosted by AWS with 99.99% uptime (GDMS Networking only) • Bank-grade TLS encryption from end-to-end • X.509 certificate-based authentication • Supports Wi-Fi Alliance Voice-Enterprise • Mobile app for iOS® and Android® • Real-time Wi-Fi Scan for deployment • URL access log collection • Multiple Wi-Fi performance optimization methods including band steering, Minimum RSSI, ARP Proxy, IP multicast to unicast, etc
Supported Devices	<ul style="list-style-type: none"> • Access points: GWN76xx(LR) • Routers: GWN7052/F, GWN7062 and GWN700x • Switches: GWN780x(P), GWN781x(P), GWN7806(P), GWN783x • All-in-one convergence devices: GCC601x(W)
Captive Portals	<ul style="list-style-type: none"> • Splash page with built-in WYSIWYG editor • Social media integration • Multiple captive portal authentications including simple password, radius, voucher, custom field etc. • External captive portal integration • Real-time guest statistics and monitoring • Advertisement integration with flexible strategies • Export guest info into file and automatically send to email
Centralized Management	<ul style="list-style-type: none"> • Local data forwarding, no user traffic sent to the controller • Network-based device management • Network/device/client monitoring • Layer2 and Layer3 based device discovery
Reporting and Monitoring	<ul style="list-style-type: none"> • Real-time Network and client monitoring • Detailed reports by network, devices, client etc. • Retrieval of historical data for statistical observations • Real-time alerts and event logs
Maintenance	<ul style="list-style-type: none"> • Ping/traceroute/capture • Both configuration and data backup • Scheduled devices firmware update and LED control • Change log for audit trail
Languages	English, Chinese, Spanish, German, Portuguese, French and more.

GDMS Networking specifications

GETTING TO KNOW GDMS Networking PLATFORM

GDMS Networking

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



GDMS Networking Architecture

Sign up to GDMS Networking

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



GDMS Login Page

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

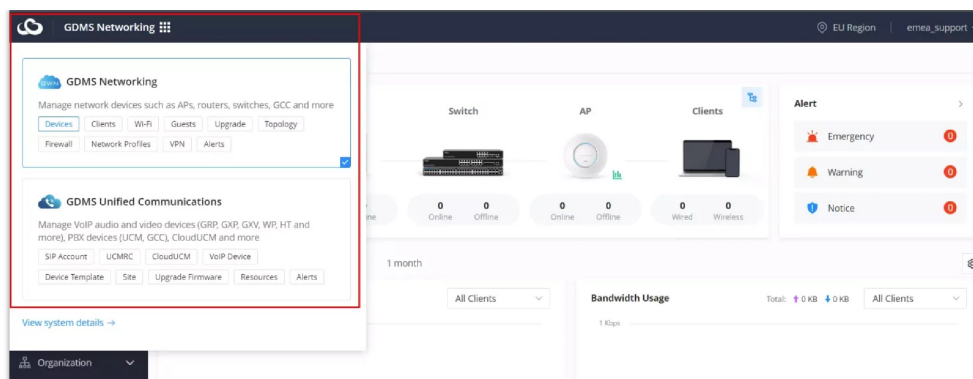
GDMS Sign-up page

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

GDMS Sign-up Settings

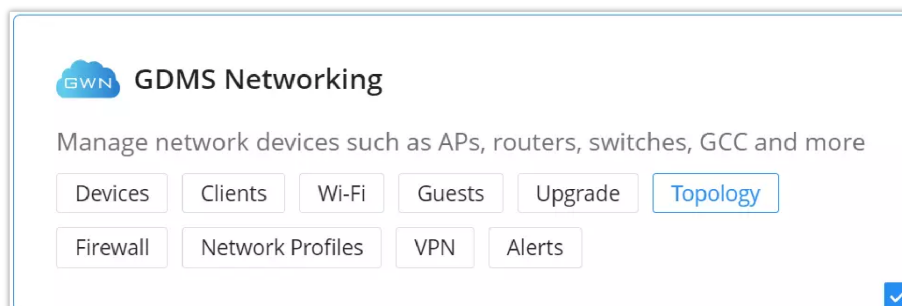
2. Once you create an account, you can access your GDMS Networking page for the first time and the following page will be displayed:

When the first page opens on GDMS Unified Communications, users can access GDMS Networking by clicking on the “**GDMS Networking**” option located in the top right corner, as shown below.



Select a System

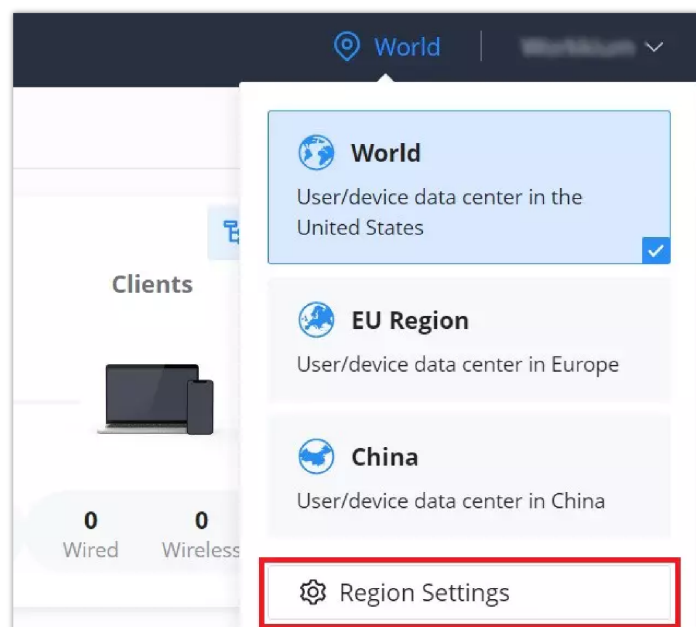
The user can access the modules listed in each category to jump quickly to the intended destination. See the example below for the GDSM Networking system.



GDSM Networking Module

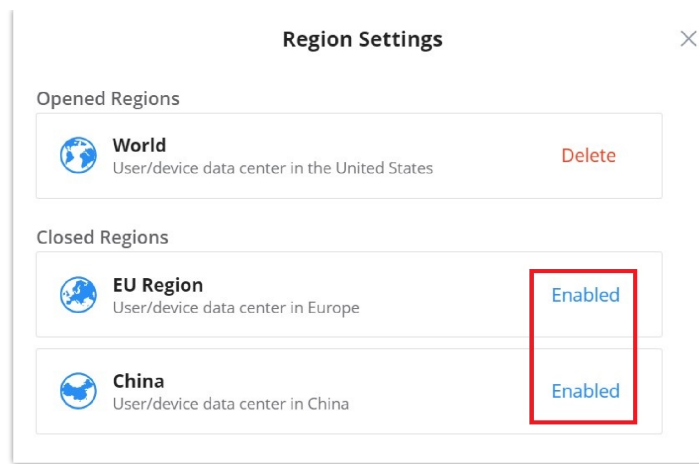
Region settings

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"**.

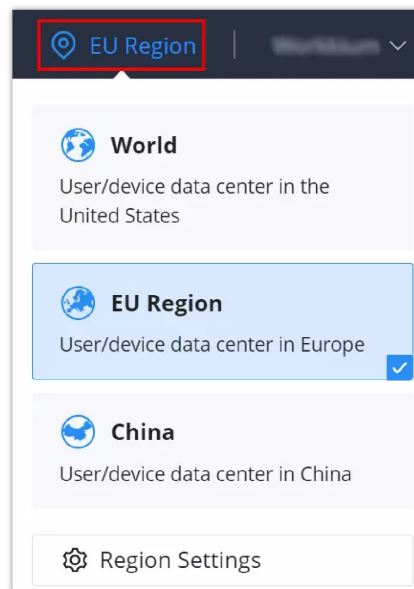


Region settings – delete & enable

Note:

Please note deleting a region will delete all data within that region.

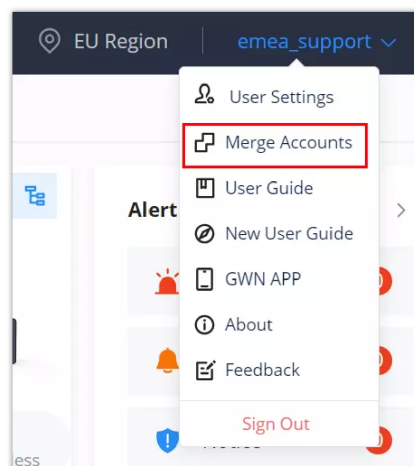
To start using the enabled region to store users/devices data, make sure it's selected on the main page as shown below:



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 GDMS Networking, 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	afuad@h3m@gmail.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

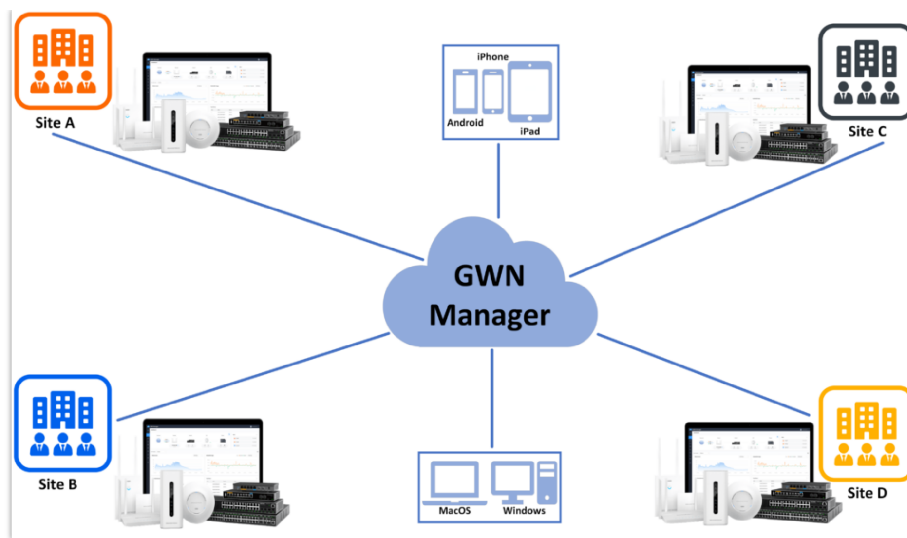
Merged accounts successfully

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 Grandstream devices Controller used to manage and monitor network devices including GWN Access points, GWN Routers, GWN Switches and GCC devices on your network.



GWN Manager Architecture

GWN Manager Hardware Requirements

Software Requirements	Hardware requirements
Operation System: <ul style="list-style-type: none"> CentOS 7 AlmaLinux OS 9 Ubuntu 	For up to 200 devices and 2 000 clients: <ul style="list-style-type: none"> CPU: Intel® Core™ i3-3240 or above RAM: 4GB or above Storage: 250GB (Dependent on the retained data)
	For up to 3 000 devices and 30 000 clients: <ul style="list-style-type: none"> CPU: Intel® Xeon® Silver 4210 RAM: 16GB or above Storage: 250GB (SSD preferred, depend on retained data size)
	For up to 10 000 devices and 200 000 clients: <ul style="list-style-type: none"> Intel® Xeon® Platinum 8175M or better 144GB or above 2x 1TB HDD
	For up to 30 000 devices and 600 000 clients: <ul style="list-style-type: none"> Intel® Xeon® Platinum 8175M or better 320GB or above 2x 2TB HDD
	For up to 50 000 devices and 1 000 000 clients: <ul style="list-style-type: none"> Intel® Xeon® Platinum 8358 or better 416GB or above 2x 3TB HDD

GWN Manager hardware requirements

Installation

To install GWN Manager please visit the links below:

[GWN Manager – Quick Installation Guide](#)

First Use

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

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

General	Specify the country/region and time zone for the default network. <i>Note: these parameters can be automatically detected by the system.</i>
User Account	Set up a username, password and email for local login.
Adopt Device	Select the GWN devices to be adopted by the default network. <i>Note: Access points, Routers available on the same LAN will be detected automatically.</i>
SSID Configuration	Create an SSID to be used by the default network for the first time. <i>Note: this SSID can be modified later.</i>
Summary	Review all the previous settings

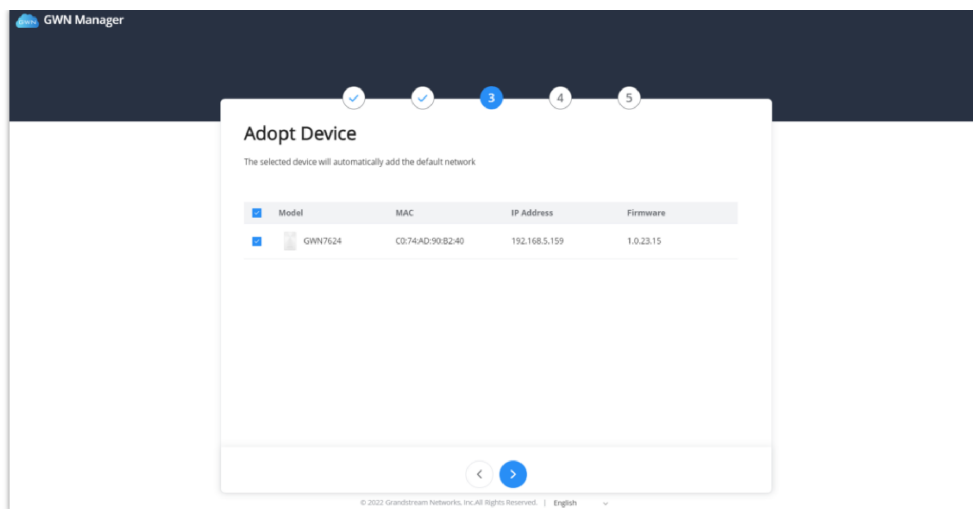
GWN Manager setup wizard

The screenshot shows the 'General' step of the GWN Manager setup wizard. The interface has a dark blue header with the 'GWN Manager' logo. Below the header is a progress bar with five numbered circles (1-5), where circle 1 is highlighted in blue. The main content area is white and contains the title 'General' and the instruction 'Sets the country/region and time zone of the default network'. On the left, there is a graphic of a globe with location pins. On the right, there are two dropdown menus: 'Country/Region' with 'Morocco(المغرب)' selected, and 'Timezone' with '(GMT+01:00) Casablanca, Monrovia' selected. At the bottom, there is a copyright notice '© 2022 Grandstream Networks, Inc. All Rights Reserved.' and a language selector set to 'English'.

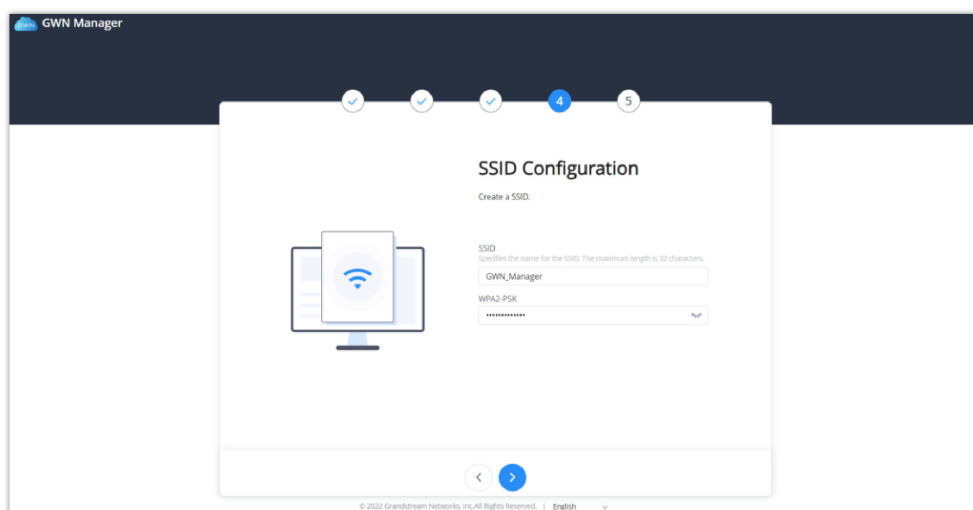
GWN Manager Wizard – Part 1

The screenshot shows the 'User Account' step of the GWN Manager setup wizard. The interface is similar to the previous step, with the progress bar now showing circle 2 highlighted in blue. The main content area is white and contains the title 'User Account' and the instruction 'Set up a Username and Password for local login.' On the left, there is a graphic of a computer monitor displaying a login form. On the right, there are four input fields: 'User name' (with a red asterisk and '1-64 characters' hint), 'Password' (with a red asterisk and '8-16 characters, only the numbers, letters or special characters' hint), 'Confirm Password', and 'Email' (with an email icon hint). At the bottom, there are navigation buttons: a back arrow, a highlighted blue forward arrow, and a copyright notice '© 2022 Grandstream Networks, Inc. All Rights Reserved.' with a language selector set to 'English'.

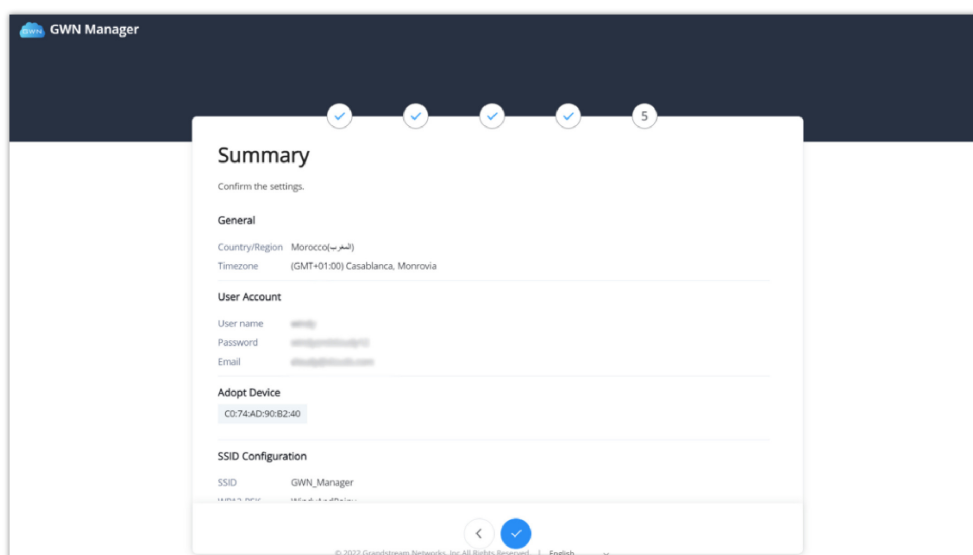
GWN Manager Wizard – Part 2



GWN Manager Wizard – part 3



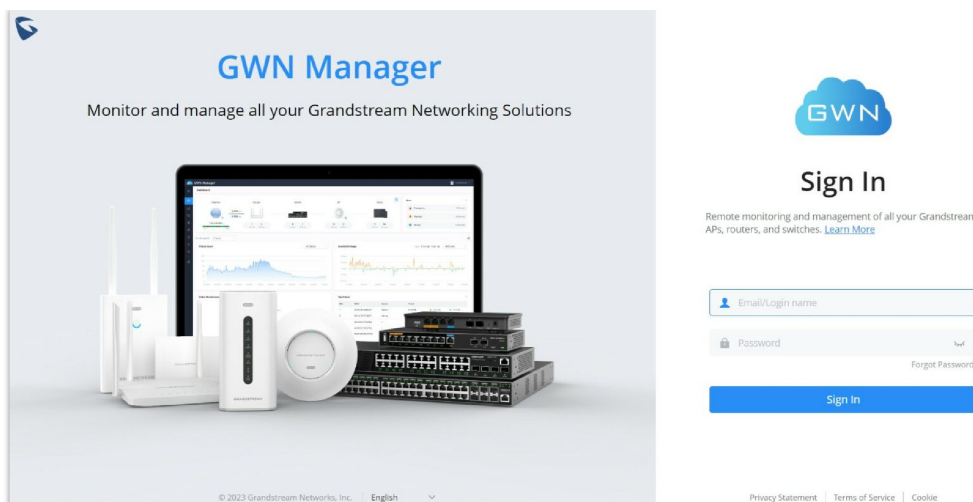
GWN Manager Wizard – part 4



GWN Manager Wizard – part 5

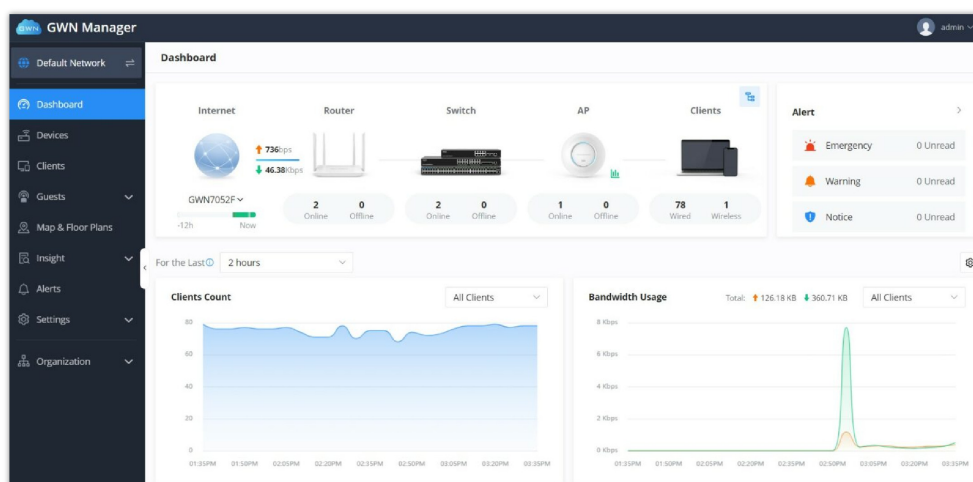
Sign up to GWN Manager

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



GWN Manager Login Page

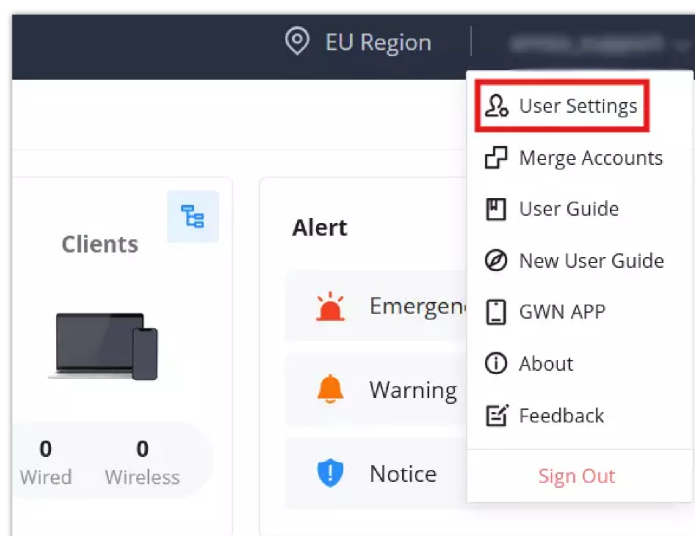
The following page will be displayed:



GWN Manager Dashboard

Users Settings

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



User Settings

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

User Settings

Nickname

Modify

Username

Modify

Email

Modify

Password

Modify

Language

English

Modify

Timezone

Modify

Time

12 hours

Modify

Date Format

YYYY/MM/DD

Modify

Appearance

Light

Modify

User Type

Enterprise

Modify

Company Name

Modify

Country

Morocco(المغرب)


Modify

Multi-Factor Safety Authentication

[Multi-Factor Authentication Instructions](#)


User 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](#)

User Settings – Multi-Factor Authentication

Nickname	Modifies the user nickname
Username	Modifies the username
Email	Modifies the Email address
Password	Changes the password
Language	Select the web UI language from the drop-down list
Timezone	Select the timezone from the drop-down list
Time	Select the time format: 12 hours or 24 hours
Date Format	Select the date format from the drop-down list
Appearance	Select the interface theme from the drop-down list: <ul style="list-style-type: none">Follow SystemLight

	<ul style="list-style-type: none"> • Dark. This setting customizes the platform's appearance for your account only.
User Type	Select the user type from the drop-down list
Company Name	Specifies the company name
Country	Select the country from the drop-down list
Multi-Factor Safety Authentication	Toggle ON/OFF the Multi-Factor authentication Note: for more details, visit Multi-Factor Authentication

User Settings

Theme Appearance

GDMS Networking includes a customizable **Appearance** setting, allowing each user to personalize the platform interface using **Light**, **Dark**, or **System Default** themes.

This setting enhances visual comfort—especially in low-light environments—and is applied on a **per-user basis**, without affecting other users in the same organization.

To access the appearance settings:

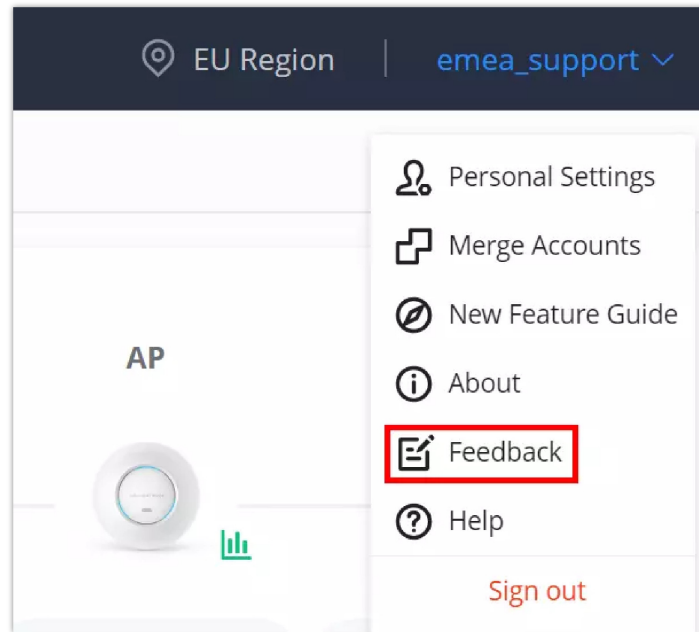
1. Click your **account icon** in the upper-right corner of the page.
2. Select **User Settings** from the dropdown menu.
3. On the **User Settings** page, locate the **Appearance** field.
4. Click **Modify** to open the theme selection dropdown.
5. Choose one of the available options:
 - **Follow System (Light)**: Automatically uses your operating system's current display theme.
 - **Light**: Standard white background with light color scheme.
 - **Dark**: Dark interface theme designed for low-light or night-time environments.
6. Click **Save** to apply the selected theme.

The screenshot shows the 'User Settings' interface. The 'Appearance' field is set to 'Dark'. The dropdown menu is open, showing three options: 'Follow System(Light)', 'Light', and 'Dark'. The 'Dark' option is currently selected and highlighted in blue. Other settings visible include Nickname, Username, Email, Password, Language (English), Timezone, Time (12 hours), Date Format (YYYY/MM/DD), User Type, Company Name, Country (Morocco), and Multi-Factor Safety Authentication (toggleed off).

Theme Appearance

Feedback

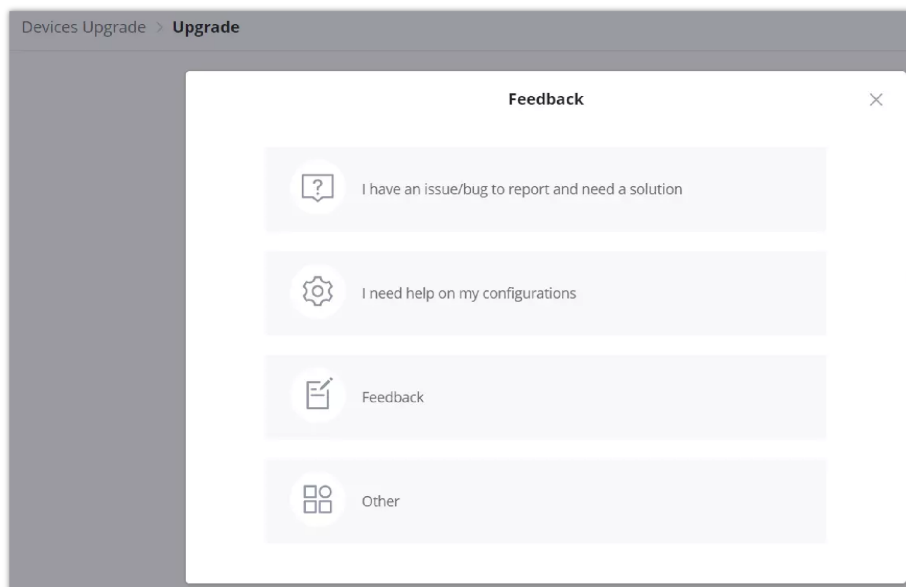
If the users have an issue/bug to report or need help about configurations or a general feedback, on the top right corner of the page, click on the account username then click on **"Feedback"** to send a feedback.



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.

Devices						
<div> <div> <div>↓</div> <div>Add</div> </div> <div>Export</div> <div>Group Management</div> <div>More</div> </div> <div> <div>All Status</div> <div>All Models</div> <div>MAC/Name/IP/Device Group</div> </div>						
<input type="checkbox"/>	Device Model	MAC	IP Address	Public IP Address	Device Group	Firmware
<input type="checkbox"/>	GWN7813P	C0:74:AD:GWN7813P	192.168.80.211		Default	1.0.1.8
<div> <div>Total 1</div> <div>10/page</div> <div>< 1 ></div> </div>						

Adding a new device to GDMS Networking

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 devices when added to the GDMS Networking 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 device (AP) – Manually

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

Add Device

Manual
Inventory
Import

Name

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: 	 C	0-64 characters
<input type="checkbox"/>	GWN7624	C0:74:AD: 	 0	0-64 characters

Cancel
Add

Adding a device – Inventory

5. Click on the “**Add**” button, the device will be added automatically to your GDMS 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

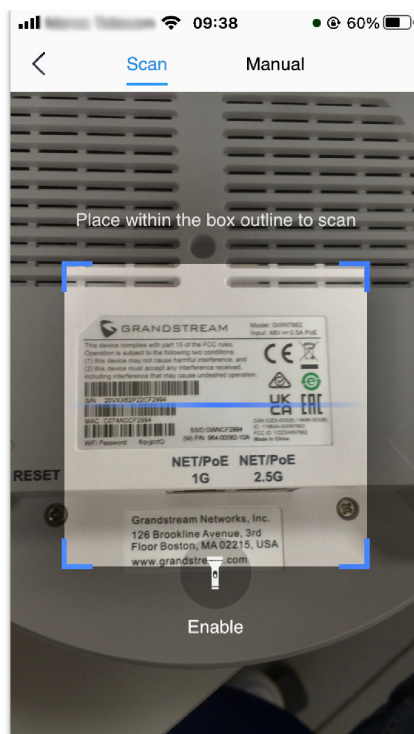
Method 2: Add a new device using GDMS Networking Application

An easy way to add a new device to your GDMS Networking is to use GDMS Application.

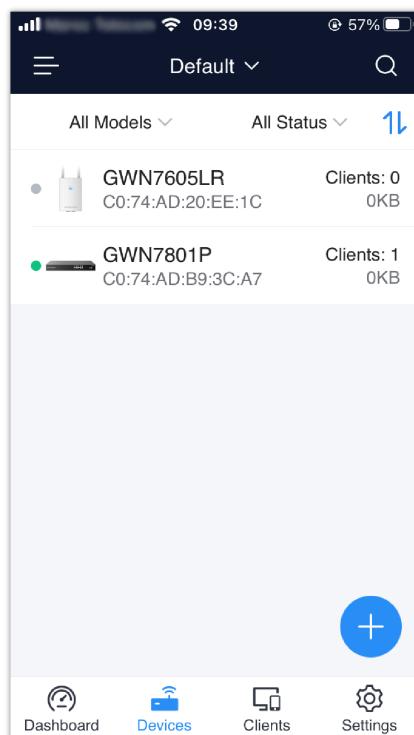
Note:

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

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



Adding a device to GDMS Networking using GDMS App – part 1



Adding a device to GDMS Networking using GDMS App – part 2

Once added, the list of devices will be displayed on GDMS Networking interface.

Devices						
Adopt Export Group Management More			All Status ▼ All Models ▼ <input type="text" value="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	CO:74:AD:	192.168.5.107	Default	154	
<input checked="" type="checkbox"/>	GWN7813P	CO:74:AD:	192.168.5.109	New Device Group	152	
			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 devices (Access points slaves) to the GDMS 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

Search

Transfer AP

Discover AP

Failover

Upgrade

Reboot

+ Add to SSIDs

✖ Configure

<input type="checkbox"/>	Device Type	Name/MAC	IP Address	Status	Uptime	Firmware	Actions
<input type="checkbox"/>	GWN7600	00:0B:82:8B:58:30	192.168.6.246	Master	20m 24s	1.0.6.23	

Showing 1-1 of 1 record(s).

Per Page: 10

Master AP – Access Points

2. Press 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

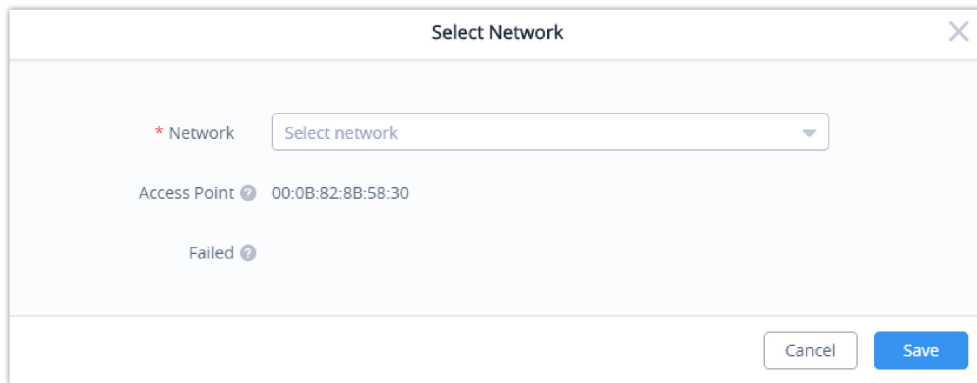
untransferable devices:

There are no untransferable devices.

Transfer AP to Cloud

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

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

A dialog box titled "Select Network" with a close button (X) in the top right corner. It contains a dropdown menu labeled "Network" with the text "Select network" inside. Below the dropdown, it shows "Access Point" with a question mark icon and the MAC address "00:0B:82:8B:58:30". Below that, it shows "Failed" with a question mark icon. At the bottom right, there are "Cancel" and "Save" buttons.

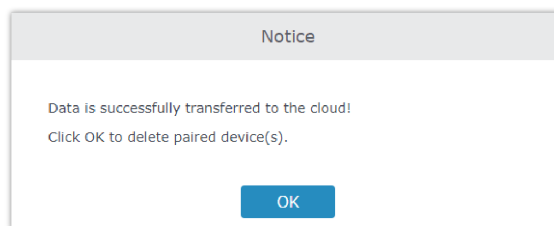
Select Network

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

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

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

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

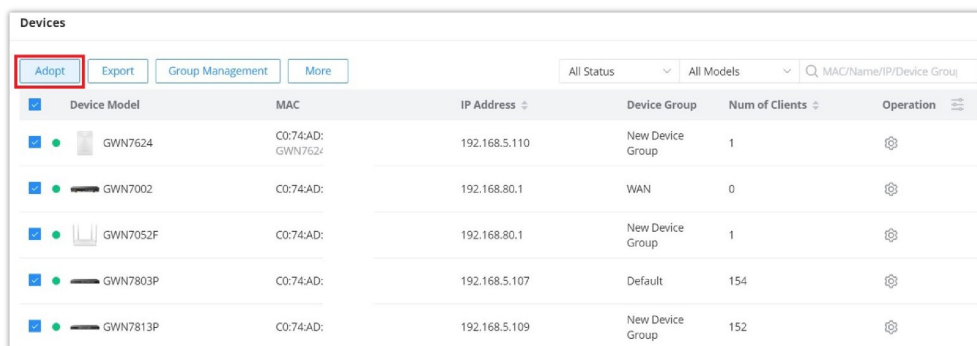
A dialog box titled "Notice" with a close button (X) in the top right corner. It contains the text "Data is successfully transferred to the cloud!" and "Click OK to delete paired device(s)." Below the text is an "OK" button.

Transfer AP to Cloud – Success

Adopt a Device to GWN Manager

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

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

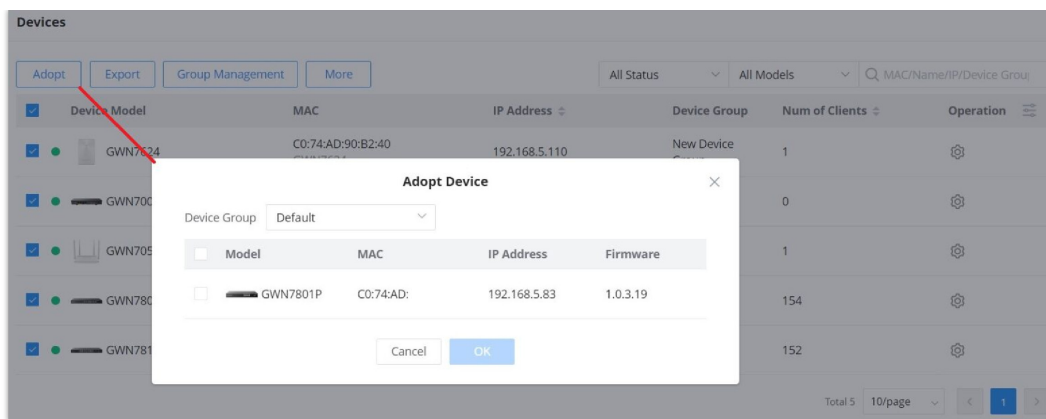
A screenshot of the "Devices" page in the GWN Manager Web UI. The page has a header with "Adopt", "Export", "Group Management", and "More" buttons. Below the header is a table with columns: Device Model, MAC, IP Address, Device Group, Num of Clients, and Operation. The table contains five rows of device information.

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 device to GWN Manager

3. If GWN Manager connects to the same local subnet as Grandstream 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 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.

When adopting a GWN router or a switch, the user will be prompted to enter the router/switch’s current administrator password, please refer to the screenshots below.

Adopt Device

ⓘ

Older versions of routers and switches do not support cloud management. Please upgrade to the latest version.

Opted in device groups

Default

All Models

MAC

	Model	MAC	IP Address	Firmware
<input type="checkbox"/>	GWN7801P	C0:74:AD:B9:3C:A7	192.168.5.125	1.0.5.52
<input type="checkbox"/>	GCC6010	EC:74:D7:17:F8:EA	192.168.5.1	1.0.1.8
<input checked="" type="checkbox"/>	GWN7002	C0:74:AD:BF:AF:50	192.168.5.147	1.0.5.35

Cancel

OK

Adopt Device

When clicking **“OK”**, the user will be prompted to enter the current password of the administrator account of the device to finish adopting the device.

Adopt Device

ⓘ

Older versions of routers and switches do not support cloud management. Please upgrade to the latest version.

Opted in device groups

Default

All Models

MAC

	Model	MAC	IP Address	Firmware
<input type="checkbox"/>	GWN7801P	C0:74:AD:B9:3C:A7	192.168.5.125	1.0.5.52
<input type="checkbox"/>	GCC6010	EC:74:D7:17:F8:EA	192.168.5.1	1.0.1.8
<input checked="" type="checkbox"/>	GWN7002	C0:74:AD:BF:AF:50	192.168.5.147	1.0.5.35

Cancel

OK

Enter The Password

Adopting devices manually

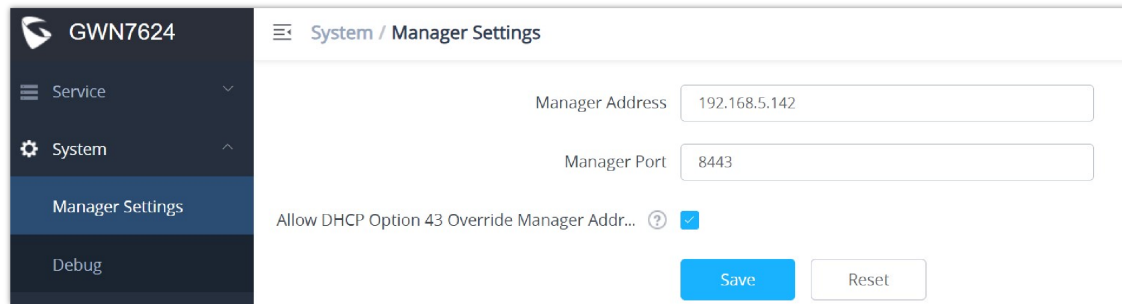
To manually configure the manager address and port on a GWN device, enable Manager Settings, fill in the Manager Address and Port, and finally click on the **“Save”** button. For each GWN device (AP, Router, or Switch), please check the steps below:

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)!

Select by pressing the [number] or [letter] and then ENTER
192.168.5.142:8443
```

Manager Settings – SSH

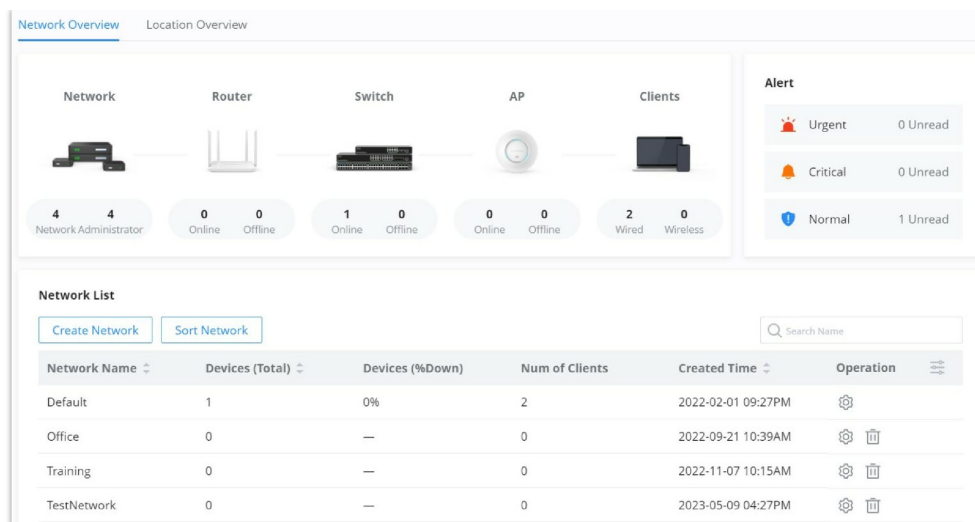
NETWORKS

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 list

The screenshot shows the 'Create Network' form. It has a header with 'Overview' and 'Create Network'. The form contains several fields: 'Network Name' (text input), 'Country/Region' (dropdown menu), 'Time Zone' (dropdown menu), 'Network Administrator' (text input), 'Optional Account' (dropdown menu), and 'Clone Network' (text input). Below the 'Clone Network' field, there is a list of existing networks to choose from: 'Default' and 'Office'.

Create Network

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

Create a New Network Settings

Move a device to a Network

To move a GWN device to another Network, please navigate to 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	

Configure

Reboot

Move

Push Configuration

Reset

Delete

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

Create Network

Sort Network

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	

Total 3

10/page

< 1 >

Network List

Overview > Network A

Share Network

* Network Name

Network A

1-64 characters

* Country/Region

Morocco(المغرب)

* Time Zone

(GMT+01:00) Casablanca, Monrovia

Network Administrator

Cancel

Save

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.

Cancel

Save

Share Network

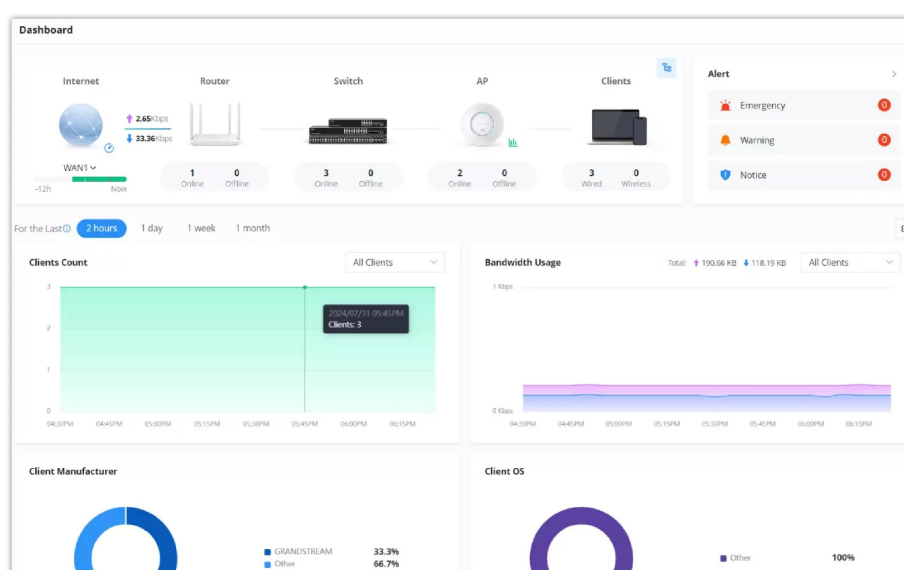
DASHBOARD

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

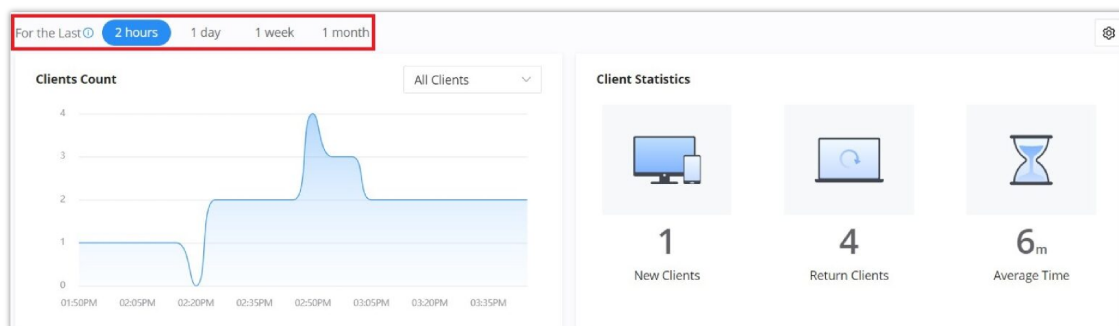
The user can choose the statistical duration of the data to review for the last 2 hours, 1 day, 1 week, 1 month, 3 months, or 6 months.

- **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:

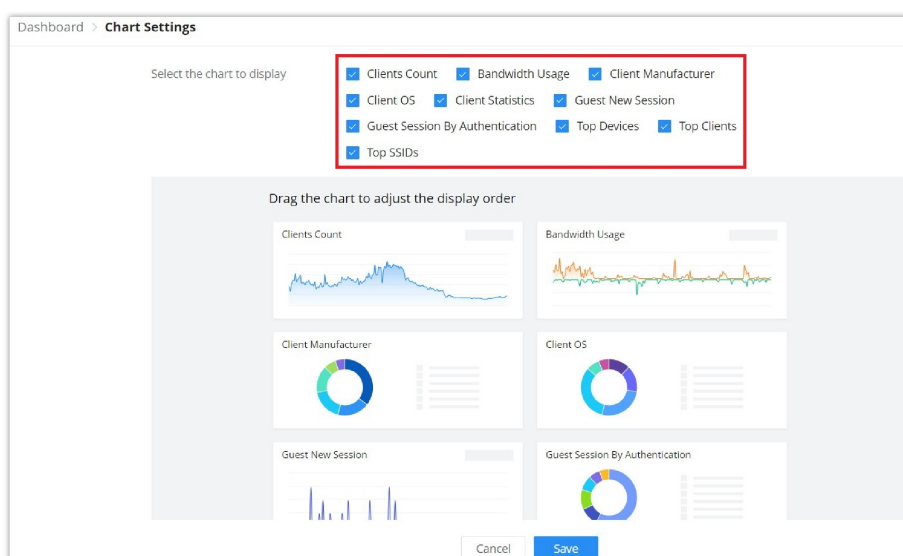
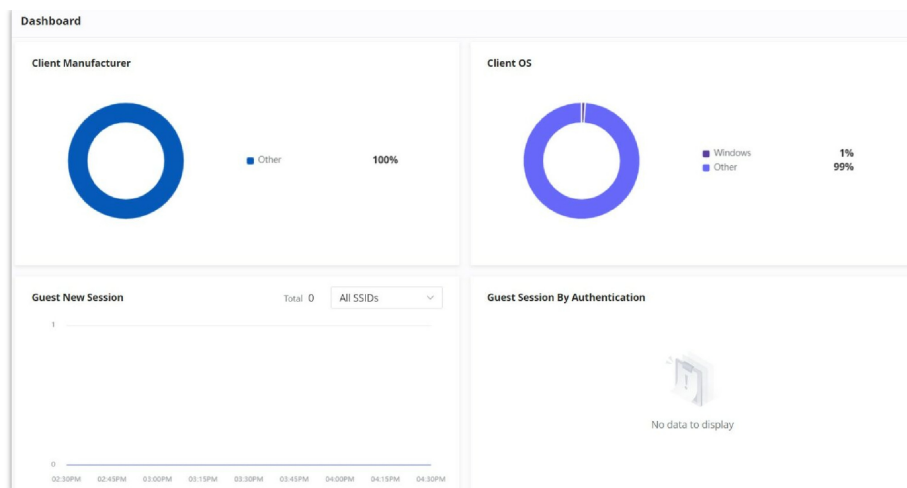


Chart Settings

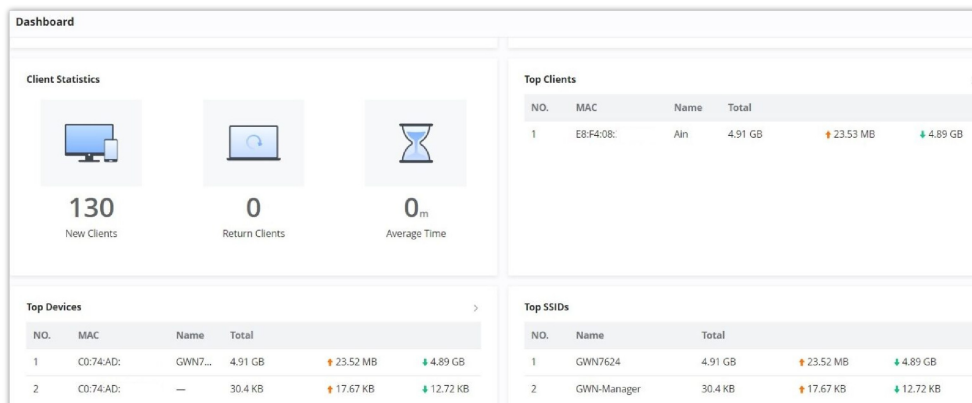
Client Count	It shows the number of clients connected at a specific period of time.
Client OS	It shows the Operating Systems used by Clients and the percentage of each.
Clients Statistics	Displays New Clients, Return Clients, and Average Time.
Top SSIDs	Displays the SSIDs that are mostly used by clients.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

Chart Settings

Example:



Example 1

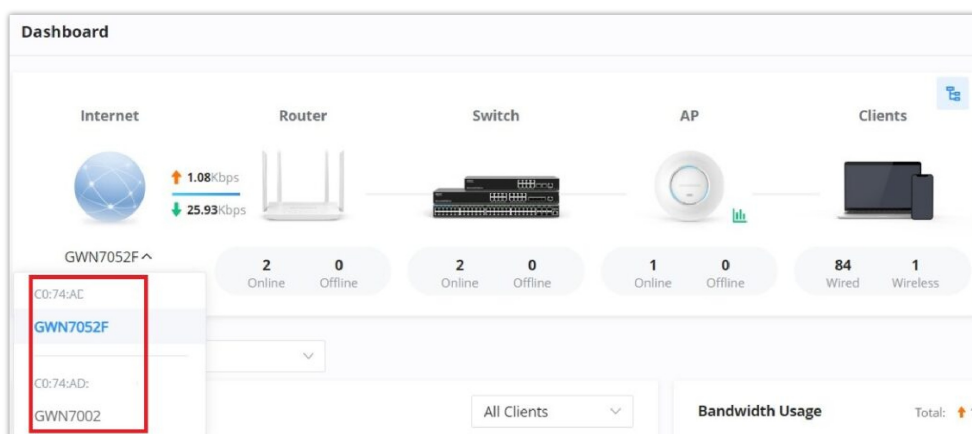


Example 2

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:



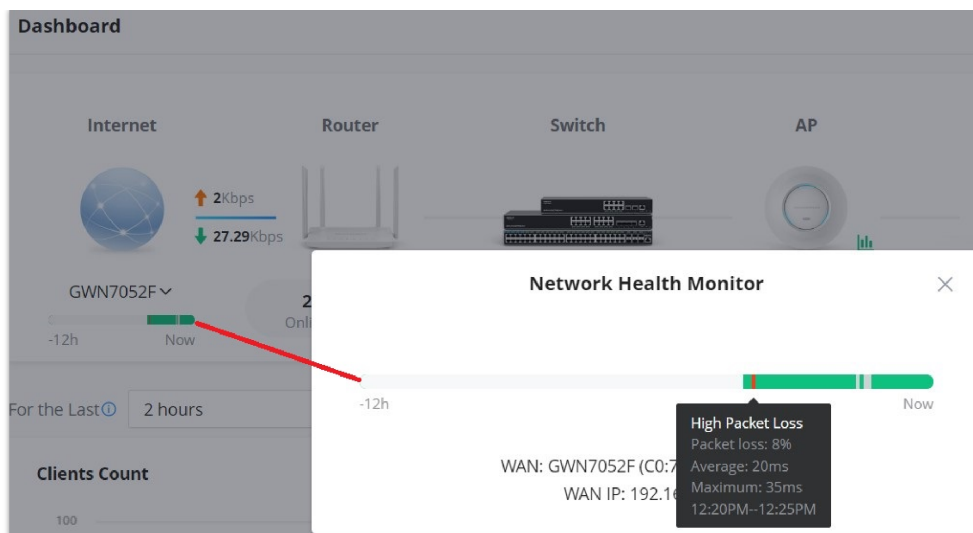
Network Health Monitor

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

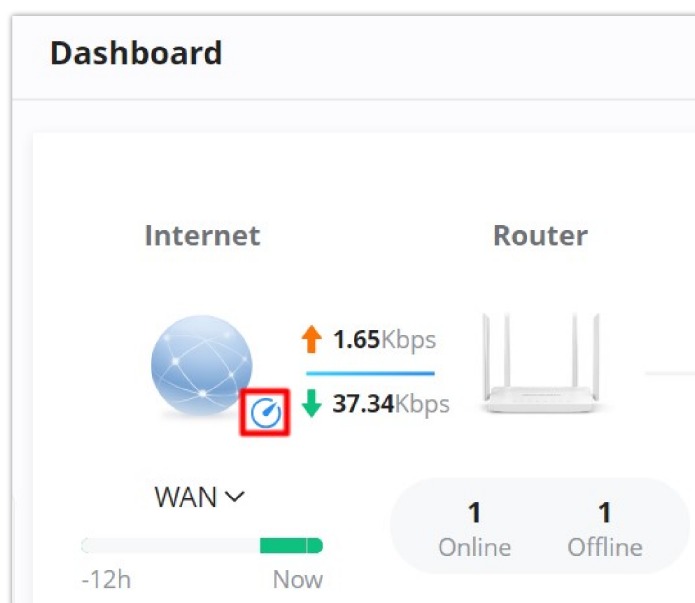
Red: High Packets Loss



Network Health Monitor

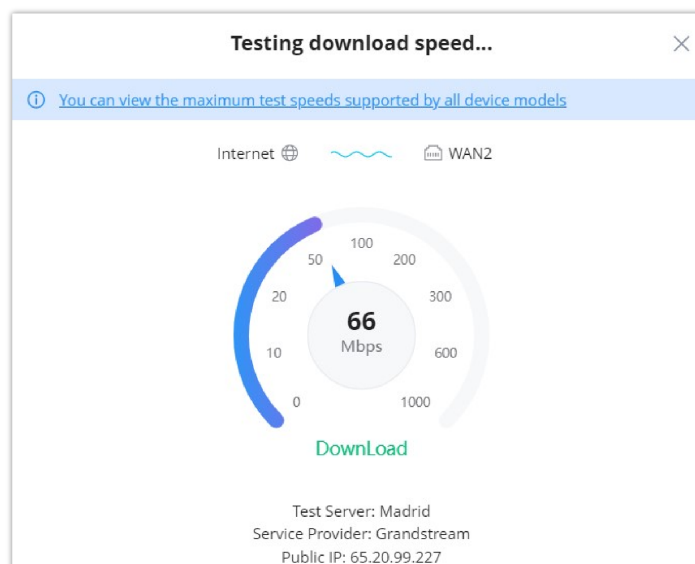
WAN Speed Test

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.



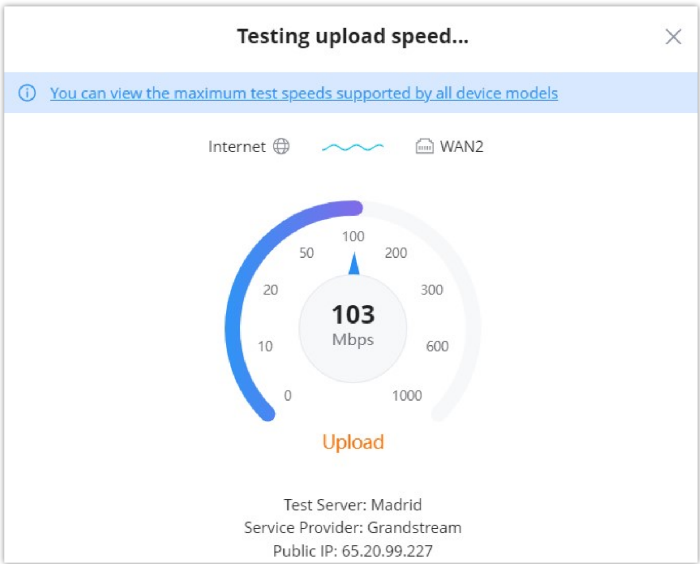
WAN Speed test

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



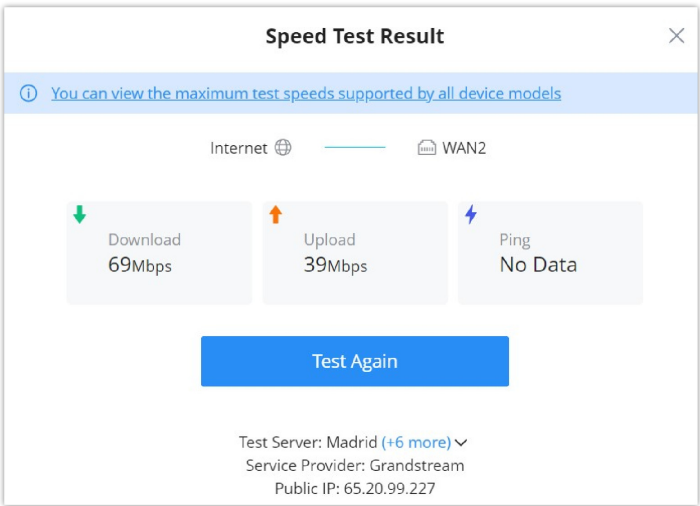
WAN Speed test – Download test

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](#).

GDMS Networking									
Device Comparison									
You may find out the differences on GDMS Networking 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
MLD Snooping									

Device Comparison – Maximum Speedtest Value

DEVICES

On this page, users can Add (GDMS Networking) 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:











Tx Power		Link Speed	Last Seen	Operation
2.4G	10dBm	100Mbps	2024/07/31 12:1	<input checked="" type="checkbox"/> Device Model
5G	—	—	—	<input type="checkbox"/> Name
2.4G	—	1000M...	2024/07/31 12:1	<input checked="" type="checkbox"/> MAC
5G	—	—	—	<input checked="" type="checkbox"/> IP Address
2.4G	—	—	2024/07/31 12:1	<input type="checkbox"/> Public IP Address
5G	—	—	—	<input type="checkbox"/> IPv6 Address
—	—	—	2024/07/31 12:1	<input type="checkbox"/> Device Group
—	—	—	2024/07/31 12:1	<input checked="" type="checkbox"/> Firmware
—	—	—	2024/07/31 12:1	<input checked="" type="checkbox"/> Uptime
—	—	—	2024/07/31 12:1	<input checked="" type="checkbox"/> Num of Clients
Total 6		10/page		<input checked="" type="checkbox"/> Usage
				<input checked="" type="checkbox"/> Channel
				<input checked="" type="checkbox"/> Tx Power
				<input checked="" type="checkbox"/> Link Speed
				<input checked="" type="checkbox"/> Last Seen

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.
- **Uplink Speed**: Displays the current uplink speed for routers and switches (e.g., 1Gbps, 2.5Gbps), improving real-time link monitoring.
- **First Seen**: Shows the date and time the device was first connected to GDMS Networking, useful for tracking onboarding history.
- **Last Seen**: displays the date and time of the device's most recent connection to GDMS.

For reference, please check the examples below:

Devices									
Add Export Group Management More				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	CO:74:AD:11:11:11	192.168.80.108	192.168.75.200	—	Default	1.0.25.15	
<input type="checkbox"/>	 GWN7605LR	GWN7605LR	CO:74:AD:11:11:11	192.168.80.226	192.168.75.200	—	Default	1.0.25.10	
<input type="checkbox"/>	 GWN7660LR	GWN7660LR	CO:74:AD:11:11:11	192.168.80.25	192.168.75.200	—	Default	1.0.25.15	
<input type="checkbox"/>	 GWN7813P	—	CO:74:AD:11:11:11	192.168.80.133	192.168.75.200	—	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 5G 1 44	2.4G 5G 20dBm 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 5G 6	2.4G 5G 20dBm	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						
<input type="checkbox"/>	Adopt	Export	Group Management	More	All Status	All Models
<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

Devices > Group Management			
Q Group name		GWN_Device	
Default		Move Devices	All Models
GWN_Device			
Routers			
WAN			
<input type="checkbox"/>	Device Model	MAC	Name
<input type="checkbox"/>	GWN7813P	C0:74:AD:DF:CC:94	—
<input type="checkbox"/>	GWN7624	C0:74:AD:90:B2:40	GWN7624

Group Management list

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

Devices > Group Management > Add New Device Group

The services of the device group will be applied to the subsequent new devices.

Name
Device Group
1-64 characters

Parent Group
Default

Device
GWN7003(C0:74:AD:90:B2:40) GWN7662(C0:74:AD:90:B2:40)

Remark
New Device Group
0-64 characters

Switch Pre-Provisioning
Only applies to the switches added the first time.

Port Settings
Port
1 +3
Port Profile
All VLANs
Trust DHCP Snooping
On

Port
5 +1
Port Profile
Default LAN
Trust DHCP Snooping
Off

Add New Item

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

Cancel Save

© 2023 Grandstream Networks, Inc.

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.

Switch Pre-Provisioning

ⓘ Only applies to the switches added the first time.

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

Add New Item

CLI Command

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

Cancel Save

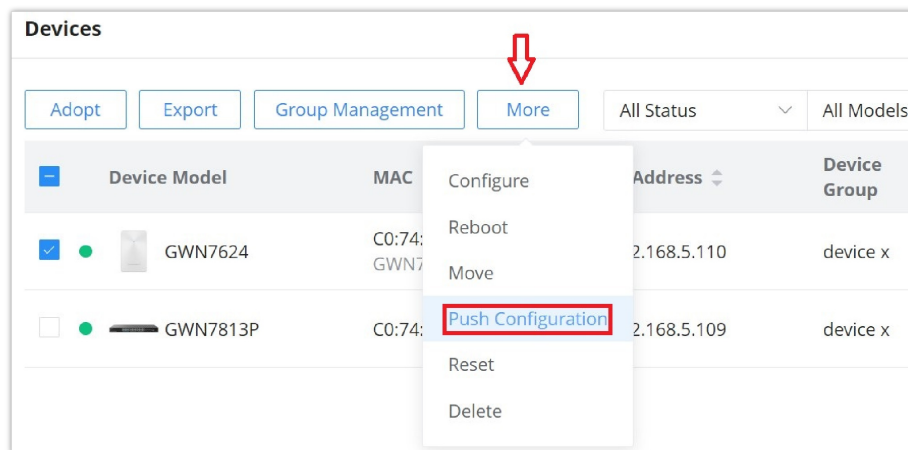
Switch Pre-Provisioning

Push Configuration

The push configuration feature helps to push GDMS Networking or GWN Manager configuration to the local side of added GWN devices either manually or automatically.

Manual Method

To manually push the GDMS Networking/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**”.

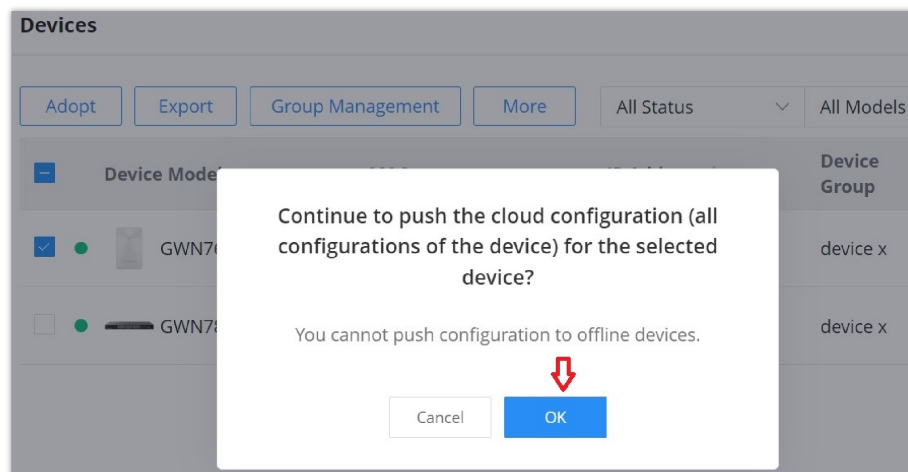


Devices page – Push configuration – part 1

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

Note:

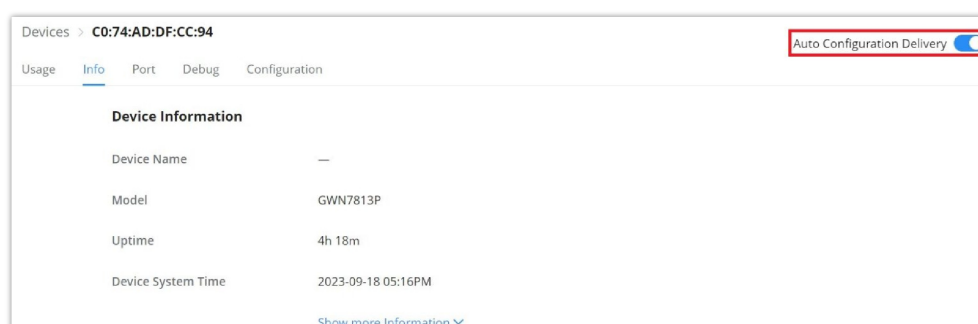
Push configuration does not work with offline GWN devices.



Devices page – Push configuration – Part 2

Automatic Method

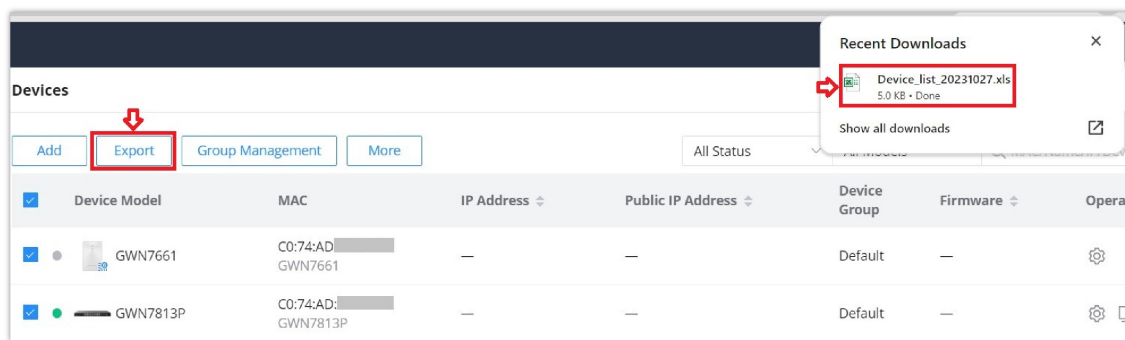
If the user wants to push the GDMS Networking/GWN Manager configuration automatically for the selected GWN device, navigate to **Web UI → Devices** page, then click on a GWN device or configuration icon, on the top of the page toggle ON “**Auto Configuration Delivery**”, please refer to the figure below:



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

Device Model	Mac	Name	IP Address	Connection IP Address	IPv6 Address	Device Group	Firmware	Running Time	Clients Count	Usage	Channel	Tx Power	Device Remarks	Serial Number
GWN7660	C0:74:AD:...	---	192.168.5.94	192.168.5.94	---	Default	1.0.25.10	---	0	---	2.4G	2.4G	---	---
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	---	---
GWN7803P	C0:74:AD:...	---	192.168.5.60	192.168.5.60	---	Default	1.0.3.37	3h 10m	77	---	5G 0	5G 0dBm	---	---

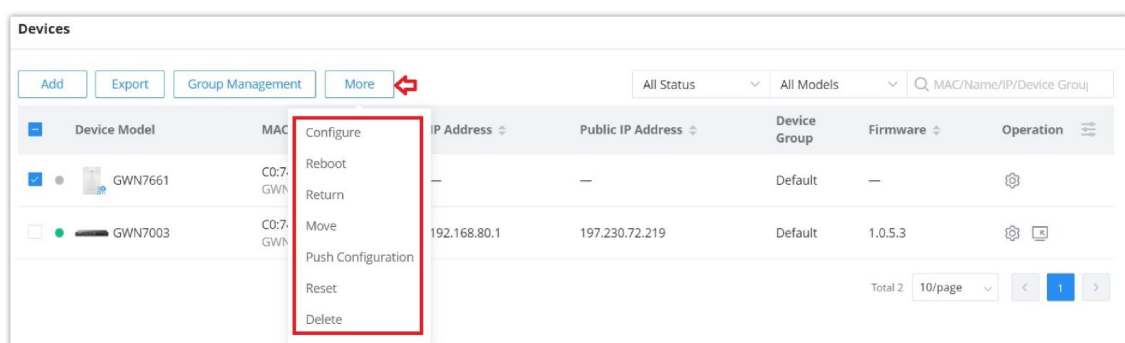
Devices Export – Excel file

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:



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.

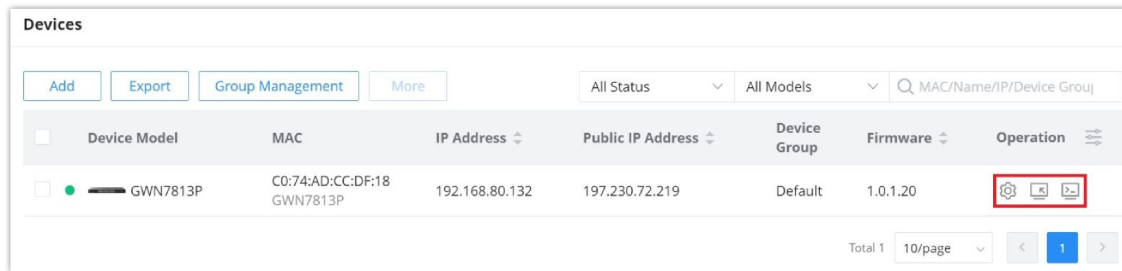
Move: to move a device from the current network to another network.

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							
Add Export Group Management More				All Status ▼ All Models ▼ <input type="text" value="MAC/Name/IP/Device Group"/>			
<input type="checkbox"/>	Device Model	MAC	IP Address ▼	Public IP Address ▼	Device Group	Firmware ▼	Operation ⋮
<input type="checkbox"/>	GWN7813P	C0:74:AD:CC:DF:18 GWN7813P	192.168.80.132	197.230.72.219	Default	1.0.1.20	

Total 1 10/page ◀ ▶

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.

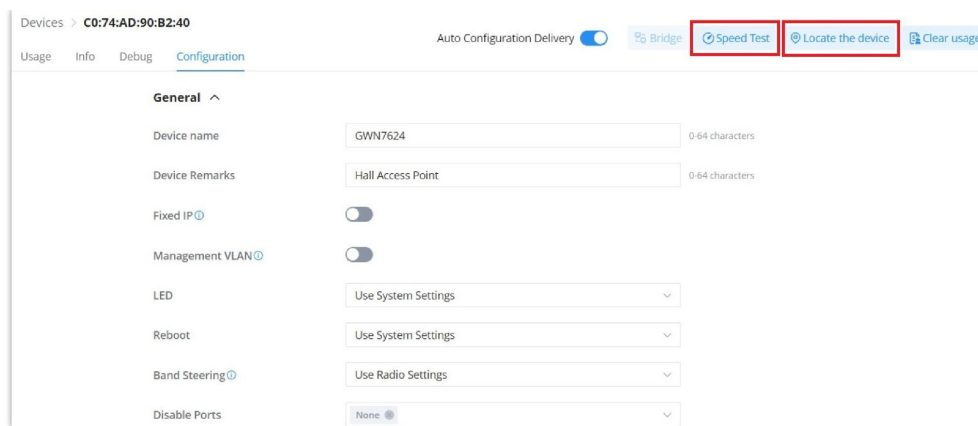
Note:

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:

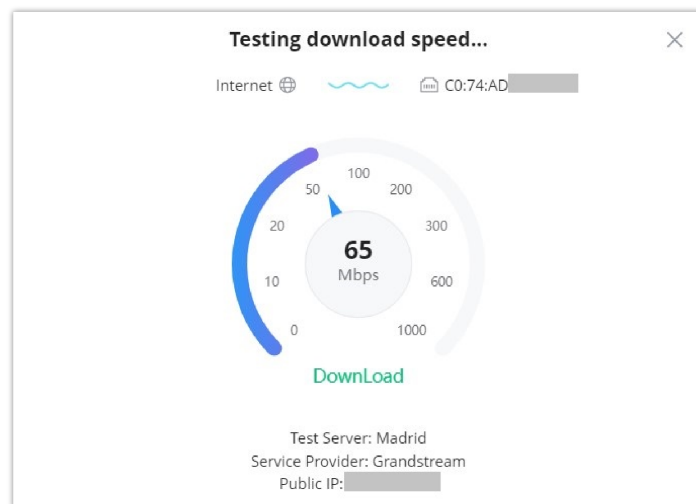


Devices – GWN AP

- **Speed Test:** is a feature on GWN APs to run a speed test directly from GDMS Networking 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:

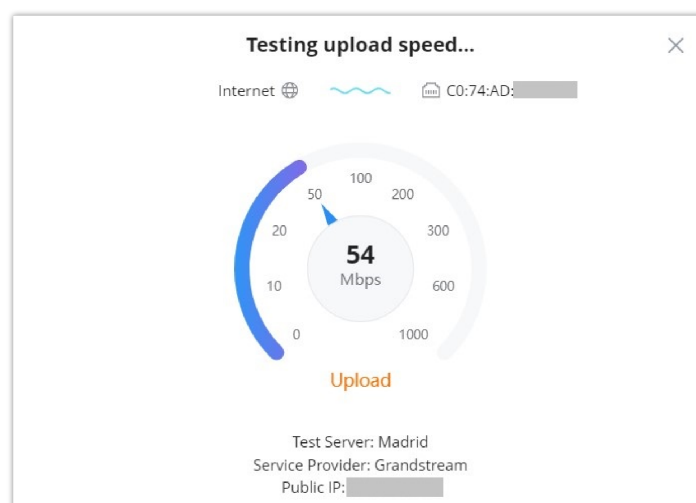
To start running the speed test, click on the “**Speed Test**” button, refer to the figure above.

The first speed test is testing download speed.



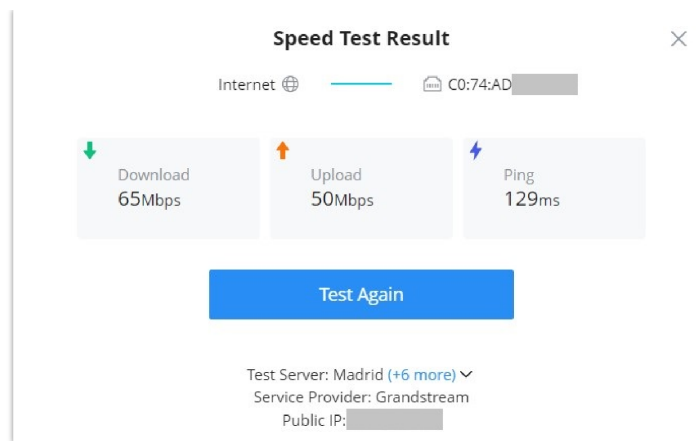
GWN APs Speed Test – Download

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:

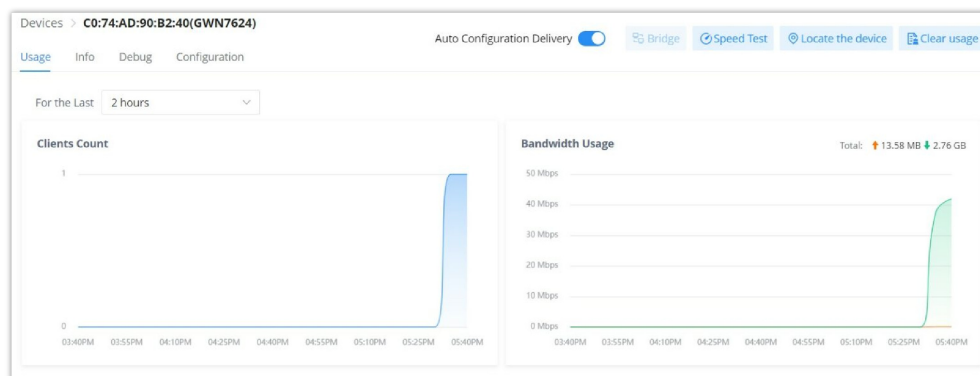
Speed Test feature is not supported on GWN7610 and GWN7602 APs.

- **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

- **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.

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

Usage **Info** Debug Configuration

Auto Configuration Delivery

Device Information

Device Name	GWN7624				
Model	GWN7624				
Link Speed	POE 1000 M/FD	LAN1 Disconnected	LAN2 Disconnected	LAN3 Disconnected	
Current rate	—				

[Show more Information](#)

RF Information

Radio	Channel	Wireless Power	Num of Clients	SSID	BSSID
2.4G	—	—	0	—	—
5G	—	—	0	—	—

Current Client

Hostname	IP Address	Total	Channel	RSSI
Ain E8:F4:08:3B:62:FD	192.168.5.154	1.31 GB 6.73 MB 1.3 GB	5G:44	-54

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.

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

BSSID

◦ 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 GDMS Networking/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)

Usage Info **Debug** Configuration

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

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.

The screenshot shows the configuration page for device GWN7624. The 'General' tab is active, displaying fields for Device name (GWN7624), Device Remarks (Hall Access Point), and various system settings like Fixed IP, Management VLAN, LED, Reboot, Band Steering, and Disable Ports. There are also fields for VLAN (LAN1, LAN2, LAN3) and a 2.4GHz radio toggle. Buttons for 'Back' and 'Save' are at the bottom.

GWN AP – Configuration

Note:

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

o **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.

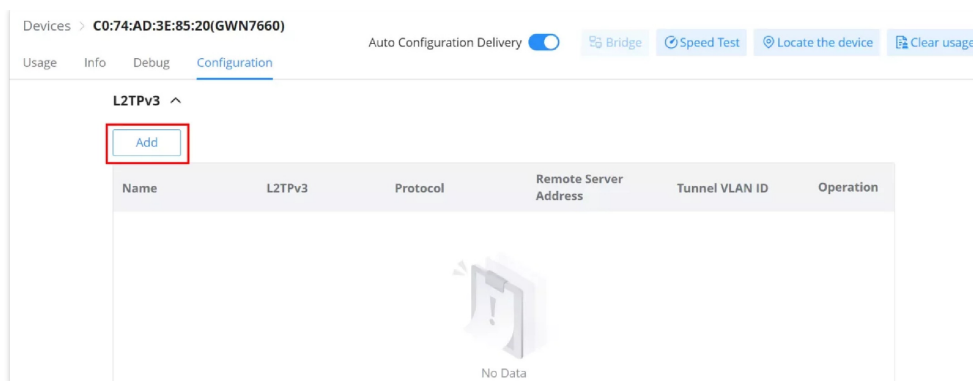
By leveraging L2TPv3, wireless clients associated with GWN Access Points are seamlessly integrated into the corporate network infrastructure. They receive IP addresses dynamically from the DHCP server hosted on the LNS, ensuring efficient network resource allocation and management.

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

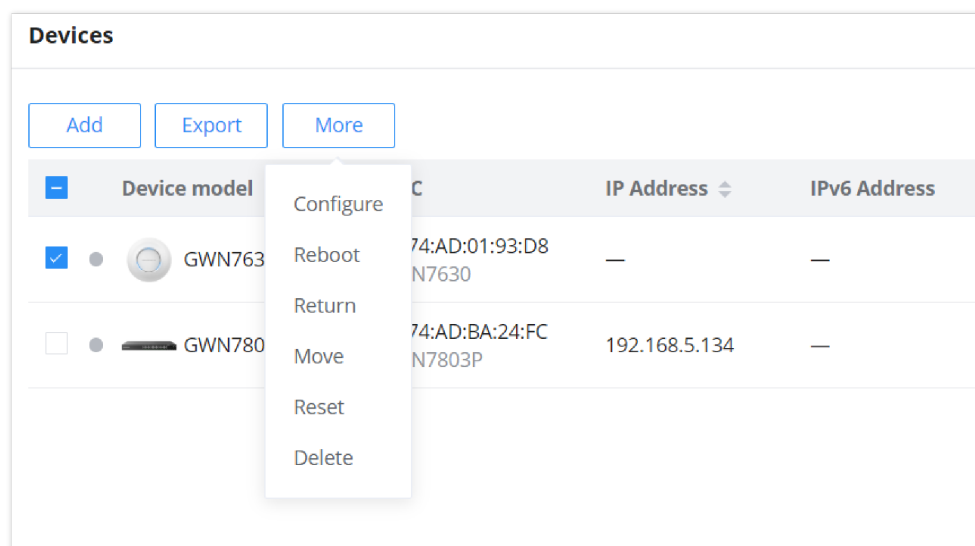
Add L2TPv3 – part 2

Name	Set the name of the tunnel.
L2TPv3	Enable/Disable the tunnel.
Protocol	Set the encapsulation type of the tunnel. Valid values for encapsulation are: UDP, IP .
Remote Server Address	Set the IP address of the remote peer.
Local Tunnel ID	Set the tunnel id, which is a 32-bit integer value. This uniquely identifies the tunnel.
Remote Tunnel ID	Set the peer tunnel id, which is a 32-bit integer value assigned to the tunnel by the peer.
Local Session ID	Set the session id, which is a 32-bit integer value. This uniquely identifies the session being created. The value used must match the peer_session_id value being used at the peer.
Remote Session ID	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 session_id value being used at the peer.
Local Cookie	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.
Remote Cookie	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.
MTU	Set the MTU. <i>Note: Please make sure the MTU values are consistent with the INS values.</i>
Tunnel VLAN ID	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/GCC device

o NAT Traversal

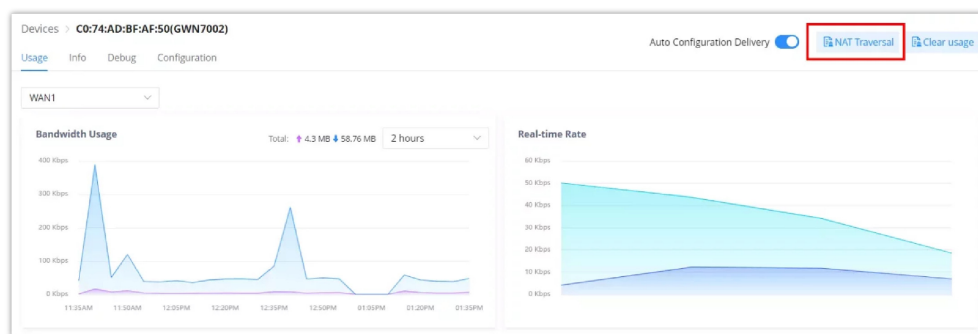
Network Address Translation (NAT) translates private IP addresses to a public IP address, allowing multiple devices to share one public IP. This poses a challenge for inbound connections from the internet. NAT Traversal facilitates these connections, making devices behind a NAT router accessible from the internet. This is essential for applications like VoIP, online gaming, and remote management.

Note:

NAT Traversal is only supported on GWN routers and GCC devices.

When a Grandstream GWN router/GCC device is added to the GDMS Cloud, the NAT Traversal option becomes available. This section will guide you through the configuration process with step-by-step instructions and screenshots.

To configure NAT Traversal, under Devices page, select a GWN router or GCC device then click on “**NAT Traversal**” as shown below:



GWN Router/GCC device – NAT Traversal

Click on the “**Add**” button to create a new NAT Traversal rule.

The screenshot shows the 'NAT Traversal' rule configuration page. The 'Add' button is highlighted with a red box. Below it is a table with columns: Name, Status, External Network Host/Port, Internal Network Host/Port, Service Type, Valid for, and Operation. The table contains one row for 'Grandstream device' with a status of 'On'. The 'Operation' column has icons for edit and delete. The bottom right shows 'Total 1' and '10/page'.

Name	Status	External Network Host/Port	Internal Network Host/Port	Service Type	Valid for	Operation
Grandstream device		13.38.221.13/16133	192.168.80.37/443	HTTPS	07/31 02:46P...	

Add NAT Traversal rule

Specify the Name, Service type, Internal IP address and the port, then click on “**Save**” button to save the rule.

Configure Service ✕

***Name**
1-64 characters

Service Type

***IP Address**

***Port**
1-65535 numbers

Cancel
Save

Add/Edit NAT Traversal rule

Finally, for the rule to take effect, enable it under status and click on **"Sign in"** to get redirected.

Devices > C0:74:AD:BF:AF:50(GWN7002) > NAT Traversal

Add

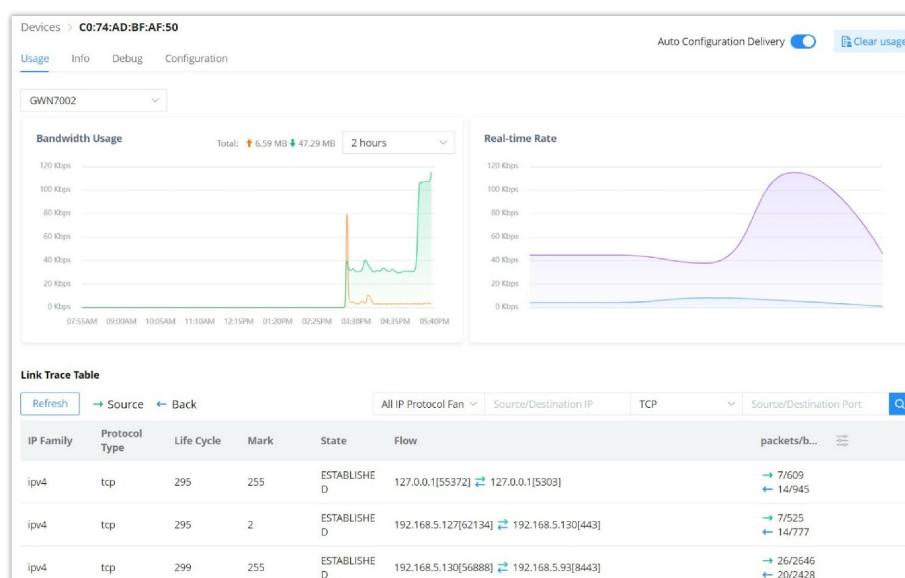
Name	Status	External Network Host/Port	Internal Network Host/Port	Service Type	Valid for	Operation
Grandstream device	<input checked="" type="checkbox"/>	13.38.221.13/16133	192.168.80.37/443	HTTPS	07/31 02:46P...	Sign In ⚙️ 🗑️

Total 1
10/page
<
1
>

Enable NAT Traversal

◦ GWN Router/GCC device – Usage

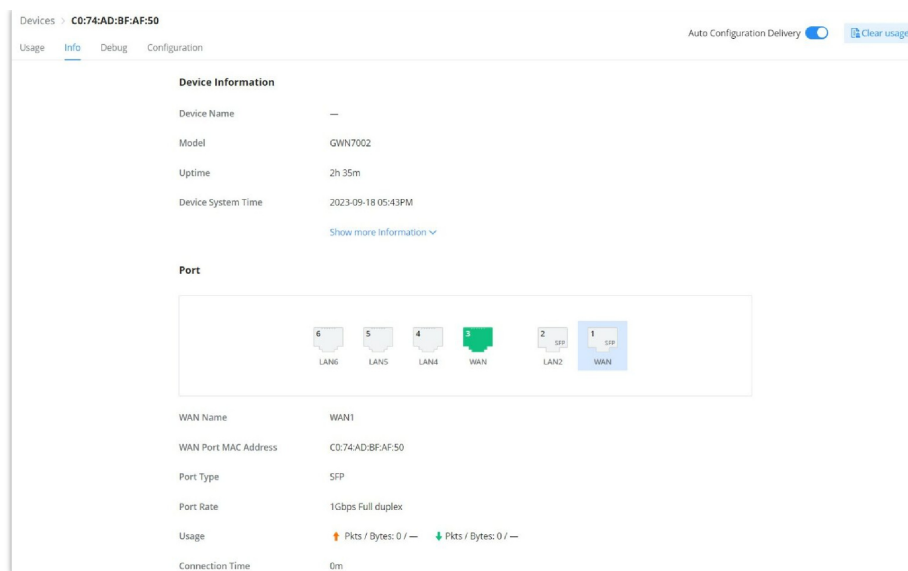
Same as the GWN AP usage tab, on this page, the user can find usage related to the GWN Router and GCC devices, like bandwidth usage, Real-time Rate, and even a Link Trace Table for detailed traffic data. Please refer to the figure below:



GWN Router/GCC device – Usage

◦ GWN Router/GCC Device – Info

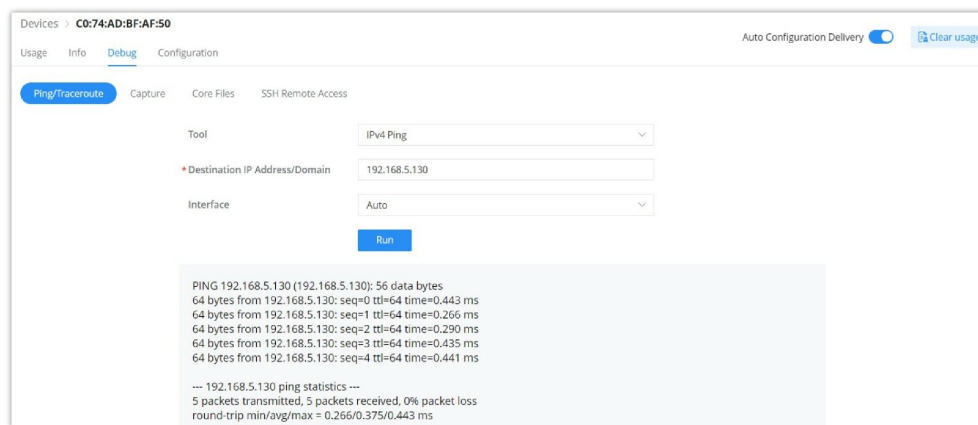
All the information related to the GWN router can be found here, including Device information (name, firmware, etc), GWN router ports' status (active ports), and information about IPv4 and IPv6 (IP address, DNS, etc).



GWN Router/GCC device – Info

◦ GWN Router/GCC Device – Debug

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



GWN Router/GCC device – Debug

◦ GWN Router/GCC Device – Configuration

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

General ^

Device name: GWN7002 (0-64 characters)

Device Remarks: (0-64 characters)

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

LED: Use System Settings

Reboot: Use System Settings

Network Acceleration ^

Acceleration Mode: Hardware Acceleration

Port ^

Physical Port	Port Name	Port Mode	Status	Port Configuration
1	ISP	WAN	<input checked="" type="checkbox"/>	
2	(0-64 characters)	LAN	<input checked="" type="checkbox"/>	None
3	Default WAN port	WAN	<input checked="" type="checkbox"/>	
4	(0-64 characters)	LAN	<input checked="" type="checkbox"/>	None
5	LAN by Default	LAN	<input checked="" type="checkbox"/>	None
6	(0-64 characters)	LAN	<input checked="" type="checkbox"/>	None

VLAN Interface ^

[Add](#)

VLAN	IPv4 Address/Prefix Length	IPv6	IPv6 Address Prefix/Prefix Length	Operation

[Back](#) [Save](#)

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/GCC device)

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/GCC device, 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:

Devices > C0:74:AD:BF:AF:50


Usage Info Debug Configuration





Auto Configuration Delivery ☒ [Clear usage](#)

5	LAN	<input checked="" type="checkbox"/>	All VLANs
6	LAN	<input checked="" type="checkbox"/>	All VLANs

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

VLAN Interface ^

[Add](#) 

VLAN	IPv4 Address/Prefix Length	IPv6	IPv6 Address Prefix/Prefix Length	Operation
20(Guests)	192.168.20.1/24	Disabled	—	 
30(Office)	192.168.30.1/24	Disabled	—	 

[Back](#) [Save](#)

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 ☐

Cancel

Save

GWN router/GCC device – 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 (Layer 2+ / Layer 3)

◦ 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) ▼

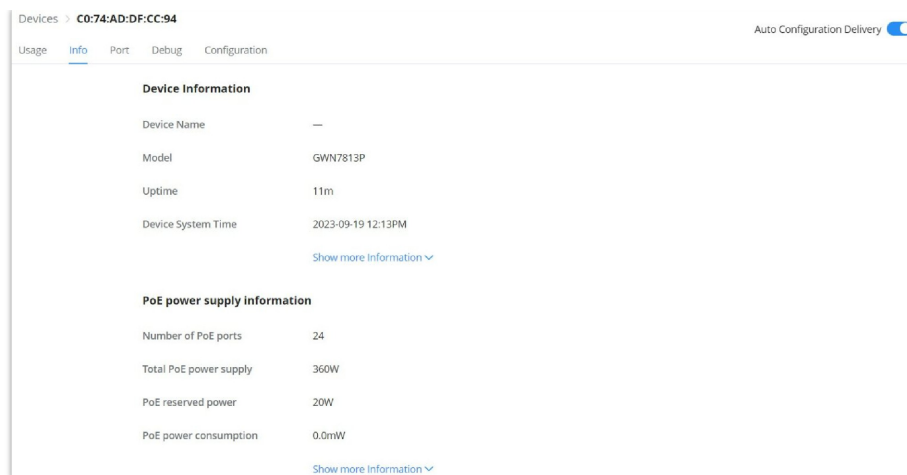
All Ports ▼

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**

The Port tab under each GWN switch device in GDMS Networking provides a centralized interface to monitor and configure individual Ethernet ports. This includes port status, traffic rates, VLAN tagging, link aggregation, speed controls, authentication methods, and security settings.

This page allows administrators to fine-tune port behavior to meet both performance and security needs in enterprise networks.

Port List and Status View:

At the top of the Port tab, users can see a graphical representation of all switch ports. Each port block displays real-time link status, port number, and traffic activity.

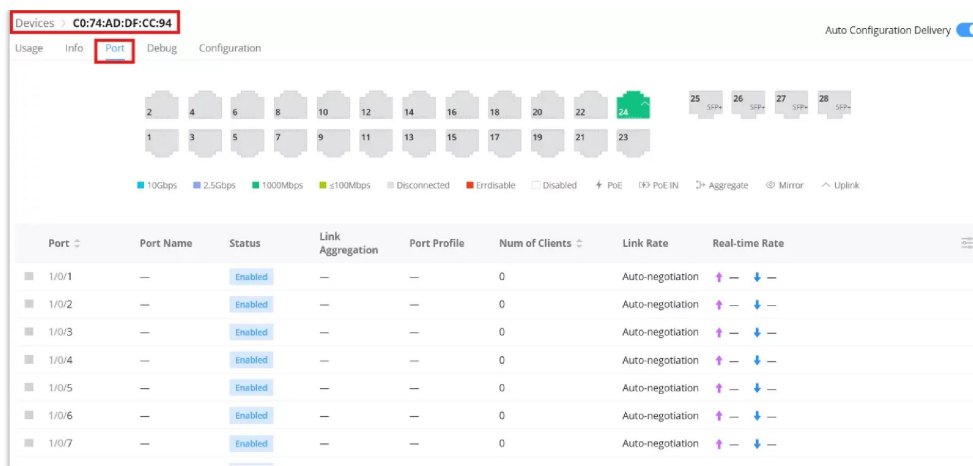
◦ **Visual Layout (Top Panel)**

The port layout gives a graphical overview of each port's current connection and status. Ports are color-coded by link speed:

- **10Gbps** – Cyan
- **2.5Gbps** – Blue
- **1000Mbps** – Green
- **≤100Mbps** – Yellow
- **Disconnected** – Gray
- **Errdisable** – Red
- **Disabled** – Light Gray

Icons can appear over ports to indicate special configuration:

- ⚡ PoE (Power over Ethernet)
- ↔ Aggregation (LAG)
- 👁 Mirror (monitoring enabled)
- ⬆ Uplink (indicates uplink port)



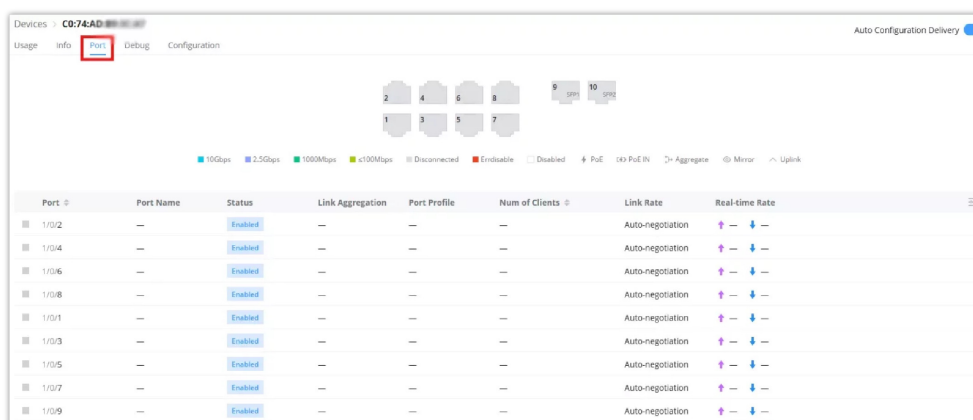
GWN Switch – Port page

This layout helps network admins visualize the topology and quickly locate key connections or issues.

Note:

Port capabilities such as PoE, link speed (e.g., 2.5Gbps, 10Gbps), vary by switch model. Refer to your specific GWN switch model specifications to confirm supported features.

Clicking on a port opens a detailed configuration panel for that individual port.



GWN Switch – Port page

After selecting a port, the panel expands to include key settings grouped into the following areas:

- **Basic Info:** Port name, enable status, link profile
- **General Settings:** VLANs, duplex mode, flow control
- **Security Settings:** MAC or 802.1X authentication, isolation, guest VLAN

The top section of the port settings includes:

- **Port Number & Name:** Displays the port number. You can assign a custom name for easier identification (up to 64 characters).
- **Port Enable:** Toggle to enable or disable the port.
- **Link Aggregation:** Assign this port to a Link Aggregation Group (LAG).
- **Link Aggregation Type:** Choose between *Static* or *LACP* (Link Aggregation Control Protocol).
- **LACP Protocol Priority:** Set the priority for this port in the LAG group. Lower values indicate higher priority (range: 1–65535).
- **LACP Packet Timeout Period:** Choose between *Slow* (30s timeout) or *Fast* (1s timeout) modes.
- **Port Profile / LAG Port Profile:**
 - When **LAG is not enabled**, this setting appears as **Port Profile**.
 - When the port is assigned to a **LAG group**, it becomes **LAG Port Profile**.

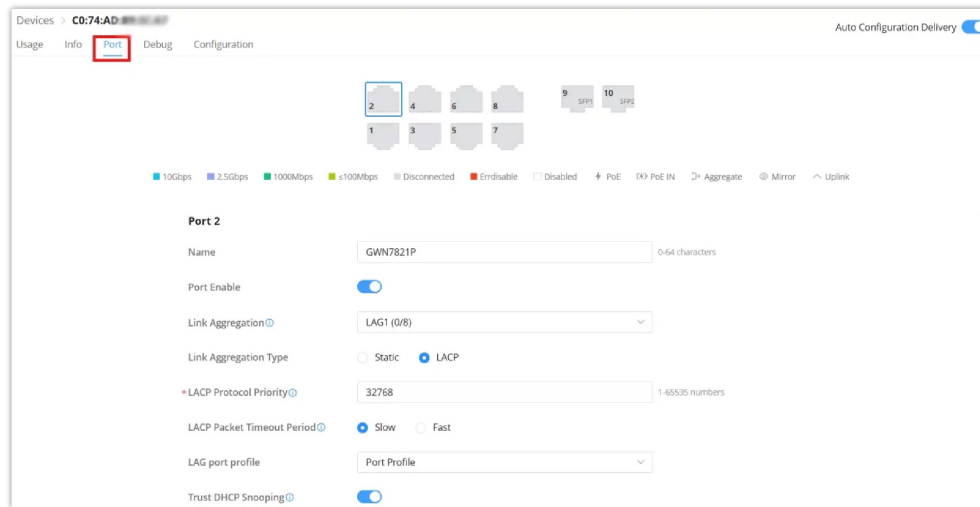
- In both cases, this setting applies a predefined profile to the port or virtual LAG interface.

Note: The profile is only effective if the Port Profile Override is disabled.

- **Trust DHCP Snooping:** Enable to allow DHCP responses from trusted sources on this port.

To configure or manage port profiles, go to:

Settings → Profile → Port Profile



GWN Switch – Port page – part 1

Port Configuration – Port Profile Override:

If **Port Profile Override** is enabled, the predefined port profile (or LAG port profile) will be ignored, and custom settings can be applied directly to the selected port. This is useful when specific port behavior is required outside of the standard profile applied to other ports.

The override settings are grouped into two sections: **General** and **Security**.

General Settings:

- **Native VLAN:** Selects the untagged VLAN for the port.
- **Allowed VLAN:** Lists the tagged VLANs allowed on the port.
- **Voice VLAN:** Enables dedicated VLAN for voice traffic (requires Voice VLAN to be enabled globally).
- **Rate:** Sets the interface speed (Auto or manual selection).
- **Duplex Mode:** Choose between *Auto-negotiation*, *Full-duplex*, or *Half-duplex*.
- **Flow Control:** Enables or disables Ethernet flow control.
- **Enable Port STP:** Enables Spanning Tree Protocol for the port.
- **Incoming/Outbound Speed Limit:** Allows rate limiting in both directions.
- **LLDP-MED:** Enables LLDP-MED protocol for enhanced device discovery and voice services.
- **Network Policy TLV:** Allows setting network policy TLVs (Voice VLAN must be enabled first).

Port Profile Override

Port Profile Override ☒ Once enabled, "Port Profile" will be invalid and the following custom configuration will be applied.

General ^

* Native VLAN

Allowed VLAN

Voice VLAN ☐ Please enable the Voice VLAN in the Global LAN Settings first

Rate

Duplex Mode ☒ Auto-negotiation ☐ Full-duplex ☐ Half-duplex

Flow Control ☐ Auto-negotiation ☒ Disabled ☐ Enable
When the duplex mode is "Half-Duplex", the flow control function does not take effect.

Enable Port STP ☐

Incoming Speed Limit ☐

Outbound Speed Limit ☐

LLDP-MED ☒

Network Policy TLV ☐ Please enable the Voice VLAN first.

GWN Switch – Port page – part 2

Security Settings:

- **Storm Control:** Enables protection against broadcast, multicast, or unknown unicast storms.
- **Port Isolation:** Isolates traffic from this port to others.
- **Port Security:** Allows MAC address-based security.
- **User Authentication Mode:** Selects between *None*, *MAC-based*, or *802.1X-based* authentication.
- **Authentication Type:** Configure MAC Authentication and/or 802.1X with method (e.g., RADIUS).
- **Guest VLAN:** Assigns a fallback VLAN for unauthenticated clients (requires global Voice VLAN).
- **Port Control:** Defines behavior (e.g., Auto, Force-Authorized, Force-Unauthorized).
- **Re-authentication:** Enables periodic re-authentication for connected clients.

Security ^

Storm Control ☐

Port Isolation ☐

Port Security ☐

User Authentication Mode

Authentication Type

Authentication Type	Method
<input checked="" type="checkbox"/> MAC Authentication	Preferred <input type="text" value="Alternative"/>
<input type="checkbox"/> 802.1X Authentication	RADIUS <input type="text" value=""/>

Guest VLAN ☐ Enable the Guest VLAN in the Global LAN Settings first

Port Control

Re-authentication ☐

GWN Switch – Port page – part 3

Note:

You can either apply a shared configuration using a Port Profile (set under: [Settings](#) → [Profile](#) → [Port Profile](#)) or override that profile for a specific port using this section. The override is ideal for one-off configurations, while profiles offer reusability and consistency across devices.

- **GWN Switch – Debug**

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

The screenshot shows the 'Debug' tab for a device with MAC address C0:74:AD:DF:CC:94. The 'Ping/Traceroute' tool is selected. The 'Tool' dropdown is set to 'IPv4 Traceroute'. The 'Destination IP Address/Domain' is '192.168.80.1'. A 'Run' button is present. Below the input fields, the output of the traceroute is displayed:

```

traceroute to 192.168.80.1 (192.168.80.1), 30 hops max, 38 byte packets
 1 192.168.5.1 (192.168.5.1) 0.000 ms 0.000 ms 0.000 ms
 2 * * *
 3
  
```

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.

The screenshot shows the 'Configuration' tab for the same device. Fields for 'Device name' (GWN7813P), 'Device Remarks' (Testing Switch), 'RADIUS Authentication' (Use global LAN settings), and 'Device Password' (masked) are visible. Below these is a 'VLAN Interface' section with an 'Add' button and a table of existing interfaces.

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

Cancel Save

VLAN Interface

Add

VLAN	Status	Type	IP Address	IPv6	IPv6 Local Link Address	IPv6 Global Unicast Address
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

Configure a GWN Switch (Layer 2 lite)

This section explains how to configure GWN Layer 2 Lite switches, such as the GWN7711P, using the GDMS Networking platform. Layer 2 Lite switches have a simpler interface compared to Layer 2+/Layer 3 switches, and not all features are available depending on the specific model. The following pages reflect the actual layout and tabs of the Web UI for easier orientation.

◦ Layer 2 Lite Switch – Usage – Traffic Statistics

The “Traffic Statistics” view under the Usage tab allows users to monitor packet flow in real-time for each individual port on the switch. It displays key metrics such as:

- InPackets / OutPackets
- InErrPackets / OutErrPackets

A statistical interval dropdown is available to refresh data every few seconds, and you can filter to show specific ports. Use the “Clear Traffic” button to reset statistics either for all ports or individually using the eraser icon in the Operation column.

Devices > EC:74:D7:0D:52:B9(GWN7711P) Auto Configuration Delivery ☒

Usage Info Port Debug Configuration

Traffic Statistics PoE Ports

Clear Traffic

Statistical Interval: 10 second(s) All Ports

Port	InPackets	InErrPackets	OutPackets	OutErrPackets	Operation
GE1	7640	0	37740	0	
GE2	0	0	0	0	
GE3	0	0	0	0	
GE4	0	0	0	0	
GE5	0	0	0	0	
GE6	0	0	0	0	
GE7	38695	0	8396	0	
GE8	0	0	0	0	

Layer 2 Lite Switch – Usage – Traffic Statistics

Layer 2 Lite Switch – Usage – PoE Ports

This page appears only if the switch model supports PoE. It displays detailed power usage for each PoE-enabled port, including:

- Current (mA)
- Current Power (mW)
- Power-Off Schedule
- Temperature (°C)
- Power Supply Mode (Auto, Force, Close)

At the top, a banner appears prompting users to match the total configured input power to the actual power supply. Failing to do so may result in unstable power delivery to connected devices. The “Set up now” link will lead users directly to the **Configuration** tab to adjust power input values.

Devices > EC:74:D7:0D:52:B9(GWN7711P) Auto Configuration Delivery ☒

Usage Info Port Debug Configuration

Traffic Statistics **PoE Ports**

Please ensure that the total input power supply is equal to the actual input power supply. If the power does not match, the PoE port may be powered abnormally. [Set up now](#)

All Ports

Port	Power Status	Current (mA)	Current power (mW)	PD Level	Temperature(°C)	Power-Off Schedule	Power Supply Mode	Operation
GE1	No power supplied	—	—	—	—	None	<input checked="" type="checkbox"/>	
GE2	No power supplied	—	—	—	—	None	<input checked="" type="checkbox"/>	
GE3	No power supplied	—	—	—	—	None	<input checked="" type="checkbox"/>	
GE4	No power supplied	—	—	—	—	None	<input checked="" type="checkbox"/>	

Layer 2 Lite Switch – Usage – PoE Ports

To configure PoE behavior per port, click the gear icon on the right. This opens advanced settings, allowing users to define the following:

- Port-specific Power Supply Standard (802.3af/at, 24V DC, 48V DC)
- Custom Power Limit (in Watts)
- Power Supply Mode (Auto / Force / Close)
- Power Priority (Highest, Second Highest, Lowest)

This lets the user fine-tune how power is allocated to each port, especially in cases where power is limited and needs to be prioritized.

Devices > EC:74:D7:0D:52:B9(GWN7711P) > **GE1**

Port: GE1

Power Supply Standard: 802.3af/at

Power Supply Mode: ☐ Auto ☐ Close ☒ Force

* Custom Limit(W): 10 1-30 numbers

Power Priority: ☐ Highest ☒ Second Highest ☐ Lowest

Layer 2 Lite Switch – PoE Ports- configure port

Note:

Some standards like 24V and 48V DC are available only on models like the GWN7710R that support them.

Devices > EC:74:D7:0D:52:B9(GWN7711P) > **GE1**

Port	GE1
Power Supply Standard	802.3af/at
Power Supply Mode	802.3af/at 24V DC 4Pair 48V DC 4Pair
* Custom Limit(W)	
Power Priority	<input type="radio"/> Highest <input checked="" type="radio"/> Second Highest <input type="radio"/> Lowest

1-30 numbers

Layer 2 Lite Switch – PoE Ports – power supply standard

◦ **Layer 2 Lite Switch – Info**

The Info tab provides a quick summary of system data including:

- Device Name
- Model
- System Uptime
- PoE Power Supply Information (Total capacity, reserved, consumption)

This tab is read-only and reflects current operating conditions. It also includes chip-level power status such as working condition and voltage delivery.

This is especially useful when troubleshooting PoE issues or confirming if the system is receiving and supplying adequate power.

Devices > EC:74:D7:0D:52:B9(GWN7711P)

Usage **Info** Port Debug Configuration

Device Information

Device Name	GWN7711P
Model	GWN7711P
Uptime	25m
Device System Time	—

[Show more Information](#) ▾

PoE power supply information

Number of PoE ports	4
Total PoE power supply	65W
PoE reserved power	5W
PoE power consumption	0mW
Configured power	—
PoE power supply support type	802.3af/802.3at/24V DC 2Pair/24V DC 4Pair/48V DC 4Pair
Chip1	Working Status: ON Power Supply Voltage: 52V

[Hide more Information](#) ▲

Layer 2 Lite Switch – Info

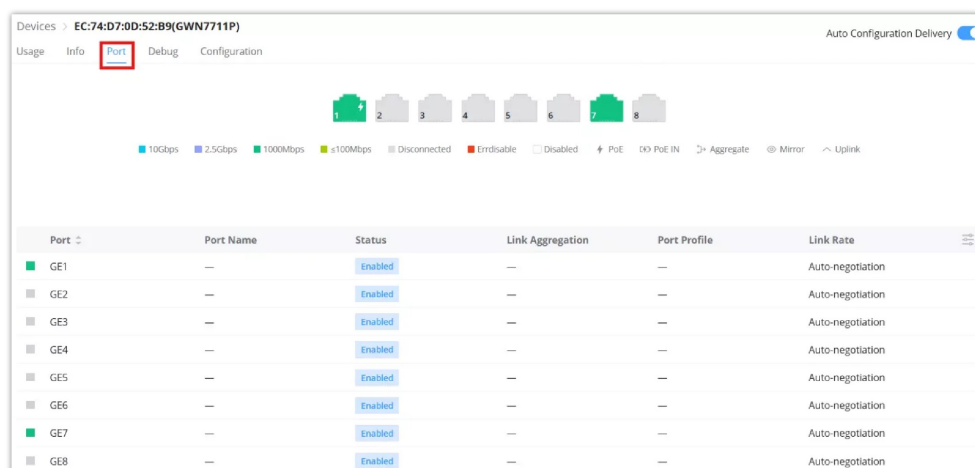
◦ **Layer 2 Lite Switch – Port**

The Port tab shows a visual representation of the switch's physical ports. Each port's color indicates its current link speed or state:

- Green: Connected (speed color-coded)
- Grey: Disconnected or Disabled

- Orange/Red: Error-disabled

It also displays PoE and LAG status icons per port. These indicators vary by model and capabilities – some support 10Gbps or 2.5Gbps depending on the hardware.



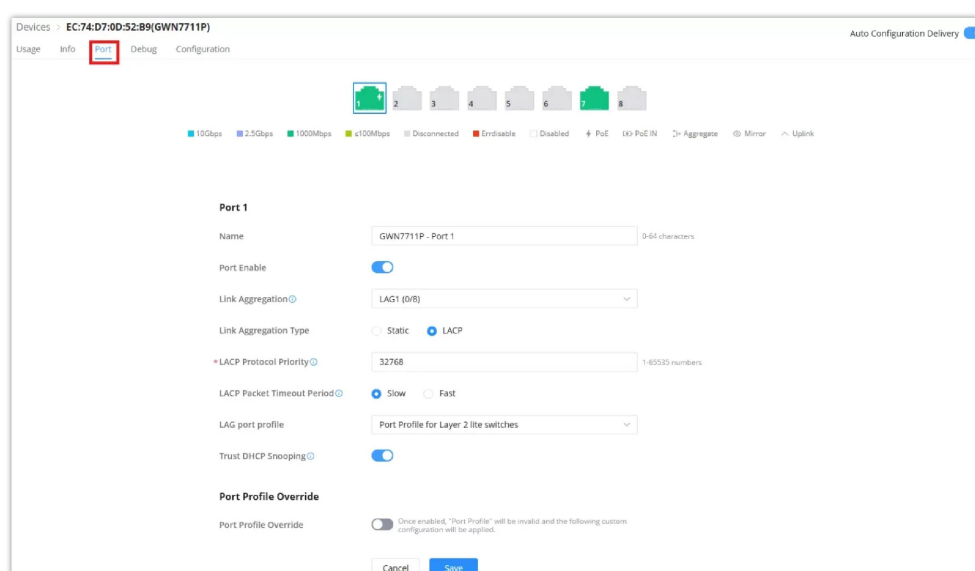
Layer 2 Lite Switch – Port page

Clicking on a port opens the configuration window. Here users can:

- Enable or disable the port
- Assign it to a Link Aggregation Group (LAG)
- Choose Aggregation Type (Static or LACP)
- Set LACP priority and timeout behavior
- Apply a Port Profile

If LAG is enabled, the user configures a LAG Profile. If LAG is disabled, the user can assign a standard Port Profile. These profiles are preconfigured templates stored in the system to simplify port configuration across multiple devices or ports. Check [Port Profile](#) for more info.

If “Port Profile Override” is toggled on, the system ignores the assigned Port Profile and allows direct manual configuration of port behavior.



Layer 2 Lite Switch – Edit port

Port Profile configuration allows users to set advanced parameters such as LLDP-MED, Voice VLAN, rate control, and more. These profiles can be created once and applied across supported switch models, including Layer 2, Layer 2 lite, and Layer 3 switches.

- **Layer 2 Lite Switch – Debug**

The Debug tab gives access to diagnostic tools, currently limited to Ping functionality. The tool allows the user to test network reachability for IPv4 addresses or domain names.

Enter the destination IP or domain, select the protocol type, and click "Run." The results will show round-trip time, packet loss, and other network diagnostic info.

This is useful for confirming whether a device has connectivity to upstream devices or the internet.

The screenshot shows the 'Debug' tab of the Layer 2 Lite Switch interface. The 'Tool' is set to 'IPv4 Ping' and the 'Destination IP Address/Domain' is '1.1.1.1'. A blue 'Run' button is visible. Below the button, the results of the ping are displayed: Host Address: 1.1.1.1, Number of Packets sent: 4, Number of Packets Received: 4, Packet Lost: 0, Minimum Round Trip Time: 23 ms, Maximum Round Trip Time: 27 ms, Average Round Trip Time: 24 ms, and Status: Ping succeed.

Layer 2 Lite Switch – Debug

◦ Layer 2 Lite Switch – Configuration

The Configuration tab allows users to customize device identity, location, and network behavior. Available fields include:

- Device Name
- Remarks
- Device Password (cloud-set password overrides local device password)
- Latitude and Longitude (can be manually entered or auto-filled if device is mapped)
- Total Power Input (W)

The Total Power Input value is critical for PoE stability. It should match the physical power supply connected to the switch. An incorrect setting may lead to ports not supplying power properly.

The lower section also includes IP Settings where users can:

- Set static or dynamic IP addressing
- Enable Static DNS
- Specify Preferred and Alternate DNS Servers

This section ensures the device can reliably connect to the network and resolve domain names.

The screenshot shows the 'Configuration' tab of the Layer 2 Lite Switch interface. The 'Device name' is 'GWN7711P' and the 'Device Remarks' is 'layer 2 lite Switch with 4 PoE+ ports'. The 'Device Password' field is empty. The 'Longitude' and 'Latitude' fields are empty. The 'Total Power Input (W)' is set to '65'. Below these fields, there is a warning message: 'Please ensure that the total input power supply is equal to the actual input power supply. If the power does not match, the PoE port may be powered abnormally.' The 'IP Settings' section shows 'IPv4 Address Type' set to 'Obtain IP Automatically (DHCP)', 'Static DNS' is enabled, 'Preferred DNS Server' is '8.8.4.4', and 'Alternative DNS Server' is '1.1.1.1'. The 'Auto Configuration Delivery' toggle is turned on.

Layer 2 Lite Switch – Configuration

CLIENTS

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

Clients

Export

Now Online

All Clients

Q

M

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

The users have also the option to set an icon for the client from the per-defined icons or add a new custom one as shown below:

Clients

Export

Hostname	Connection
<div><div></div><div>C0:74:AD:25:2A:08</div></div>	Wired
<div><div></div><div>C:99:57:BC:B9:F7</div></div>	Wired

Cell

Smart Watch

Camera

Robot Vacuum

TV

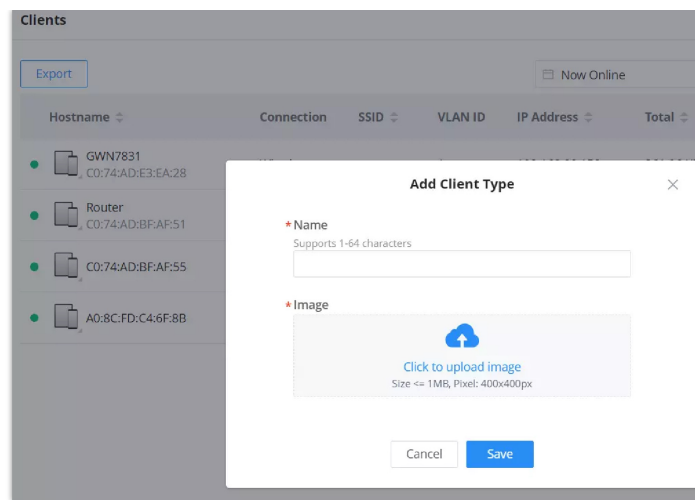
Printer

Other

Add New Type

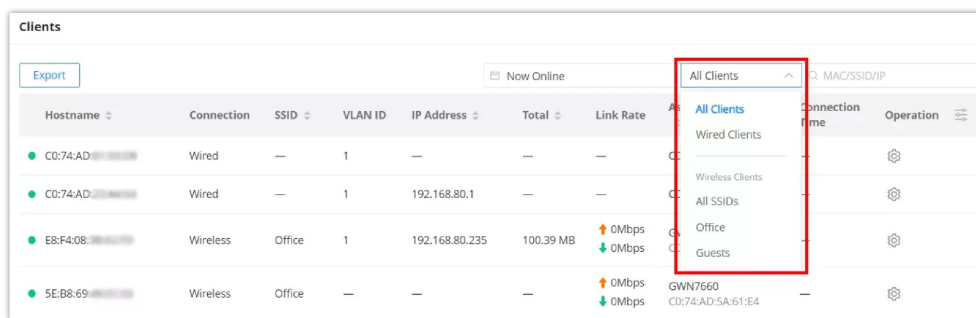
Clients page – set an icon

To add a custom icon, click on “Add New Type” as shown above, then upload the icon image and specify a name for it.



Clients page – set a custom icon

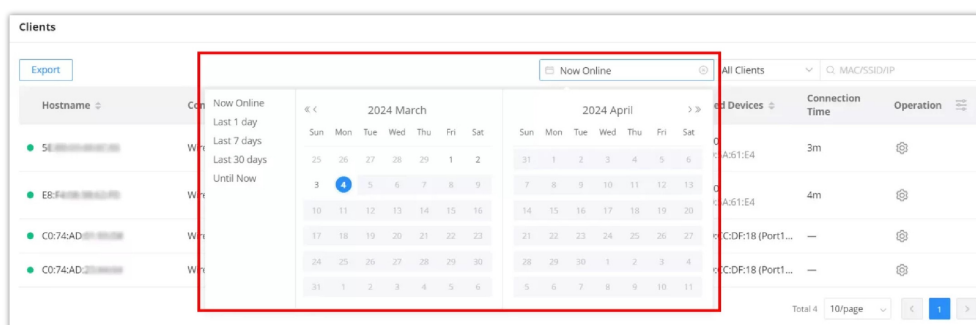
To make it easier for the users to find the connected clients, it's possible to filter by wired clients or wireless clients and even by SSID e.g. (Office, Guests ...), please refer to the figure below:



Clients Page – sorting

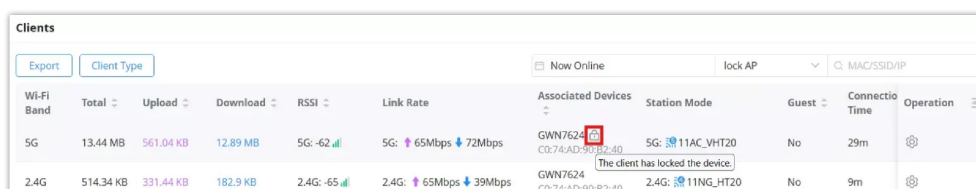
The same way, users can filter clients by wired and wireless connections, they also can filter by time (calendar), many options are available:

- **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

A **lock icon** is displayed next to the Access Point under the **Associated Devices** column to indicate that the connected client is locked to that specific AP. For more details check [Configure a Client](#).



Configure a Client

The **Client Configuration** tab allows users to customize settings for individual clients connected to the network. This includes blocking specific wireless clients, applying bandwidth restrictions, setting DHCP static IP assignments, and binding clients to specific Access Points (APs) with optional failover.

When a wireless client is selected, additional options are available:

- **Client Blocking** allows the administrator to block a wireless client from the network. This is applied via the Global Blocklist, which supports up to 1000 MAC entries. You can also specify whether the block is permanent (Always) or temporary.
- **Lock to the Access Point** allows binding the client to a specific AP. If enabled, the client will always connect to the assigned AP. An optional **Failover Access Point** can be set to provide redundancy in case the primary AP becomes unavailable.
- The **View All APs with Lock Devices** option provides a centralized list of all APs with locked clients, simplifying the process of tracking and managing client bindings.

Clients > E8:F4:08:3B:62:FD(Ain)

Usage Info **Configuration**

Hostname 0-64 characters

Client Blocking ☒ [View Global Blocklist](#)

Block duration ☒ Always ☐ Temporarily

Bandwidth Rules

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

Lock to the Access Point ☐ [View All APs with Lock Devices](#)

Client – Configuration part 1

Clients > E8:F4:08:3B:62:FD(Ain)

Usage Info **Configuration**

Hostname 0-64 characters

Client Blocking ☐ [View Global Blocklist](#)

Bandwidth Rules

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

Lock to the Access Point ☒ [View All APs with Lock Devices](#)

* Access Points

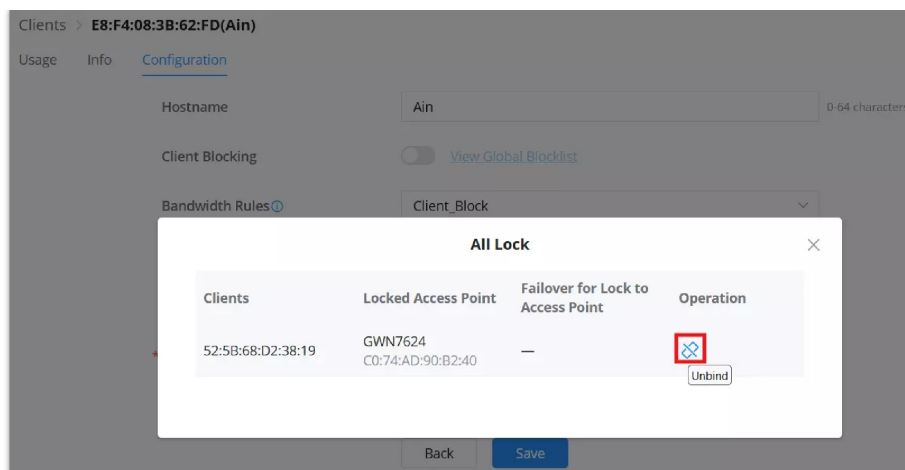
Failover for Lock to Access Point

[None](#)

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

Client – Configuration part 2

When viewing locked client devices under **View All APs with Lock Devices**, users can quickly **unbind** a client from its associated Access Point by clicking the **Unbind** icon in the *Operation* column.



Client – Configuration part 3

Field	Description
Hostname	The name assigned to the client device.
Client Blocking	Option to block the client device from accessing the network. <i>Notes:</i> Client Blocking and Lock to the Access Point can't be enabled at the same time. Only applicable to wireless clients. Click on View Global Blocklist to view the Global Blocklist or add new one.
Block Duration	Determines if the block is always or temporary. <ul style="list-style-type: none"> • Always: Will always block the client; • Temporarily: Blocks the client for a set period of time. Once the set duration is reached, the block automatically cancels.
Duration	Specifies the duration for the temporary block (in days, hours, and minutes).
Bandwidth Rules	Defines bandwidth rules applied to the client, select from the list or click on "Add New Bandwidth rule" to add a new one. <i>Note:</i> The bandwidth rule does not take effect on wired clients.
DHCP Static IP address binding	Enables binding the client to a specific IP address within the network.
VLAN	Specifies the VLAN to which the client is assigned.
IP Address	The static IP address assigned to the client.
Lock to the Access Point	Option to lock the client to a specific access point. <i>Note:</i> Client Blocking and Lock to the Access Point can't be enabled at the same time. View All APs with Lock Devices: opens a list view of all access points with locked clients and their assigned failover APs.
Access Point	Choose the primary AP the client will stay connected to.
Failover for Lock to Access Point	Optional backup AP. If the primary AP fails, the client will connect to this failover AP.

Client Configuration

Client usage

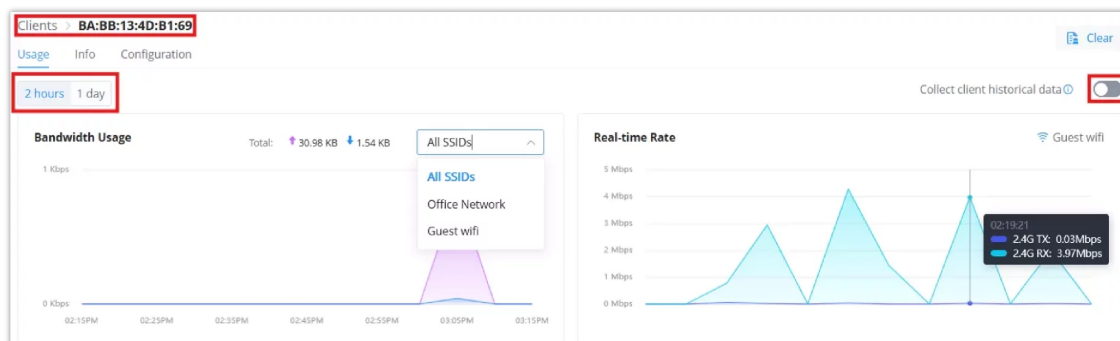
The **Usage** tab provides per-client bandwidth statistics and real-time rate monitoring. This is useful for reviewing network activity or diagnosing traffic-related issues per device.

Navigation: Clients → [Select a Client] → Usage Tab

- **Real-Time View & Short-Term Usage**

When **Collect client historical data** is **disabled**, the chart provides usage history over **short timeframes only**:

- **Selectable ranges:** 2 hours or 1 day
- **Real-time Rate Graph:** Continuously updates to reflect current bandwidth activity in Mbps
- **Bandwidth Usage Graph:** Displays total upload/download during selected timeframe
- **SSID Filter:** View usage for a specific SSID or across all SSIDs
- **Graph Tooltips:** Hover over any point on the graph to view upload/download at that time

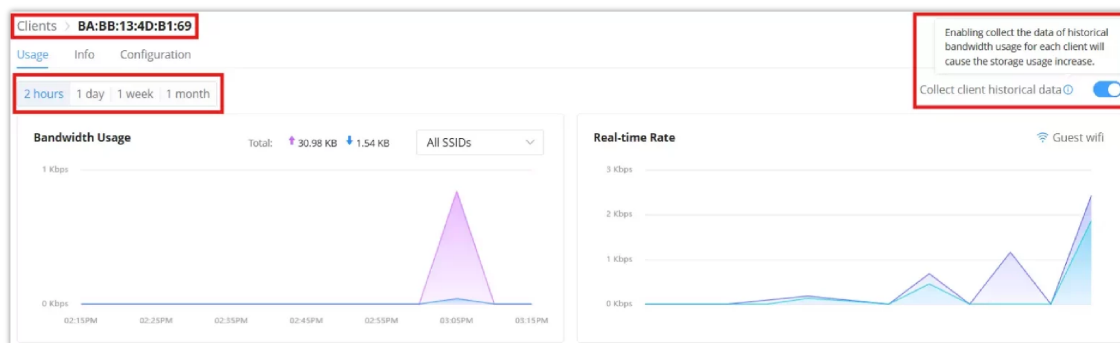


Client Usage – Collect client historical data off

- **Enabling Historical Usage Tracking**

If **Collect client historical data** is **enabled**, longer timeframes become available:

- **Additional ranges:** 1 week and 1 month
- Enables deeper usage analysis and bandwidth trend comparison over time
- A warning is displayed that enabling this will increase data storage usage



Client Usage – Collect client historical data on

Client info

On this page, info about the current client will 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.

Clients >

UsageInfoConfiguration

Basic

Hostname

—

Client Status

Online

IP Address

192.168.5.59

Current Rate

—

Show more Information

▼

History

Device	MAC	Connection Time
GWN7624	C0:74:AD: <div></div>	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.

Online Status

[Export](#) Search MAC

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	

Total 1 10/page < 1 >

Guests – Online Status

Voucher

The **Voucher** system in GDMS Networking allows admins to generate one-time or multi-use access codes for guests to join Wi-Fi securely—ideal for hotels, events, cafés, campuses, or any scenario where temporary access is needed.

Voucher Groups can be generated manually or based on a **Voucher Group Template**, allowing you to quickly reuse common settings like device quota, duration, or bandwidth limits.

◦ Accessing the Voucher Page:

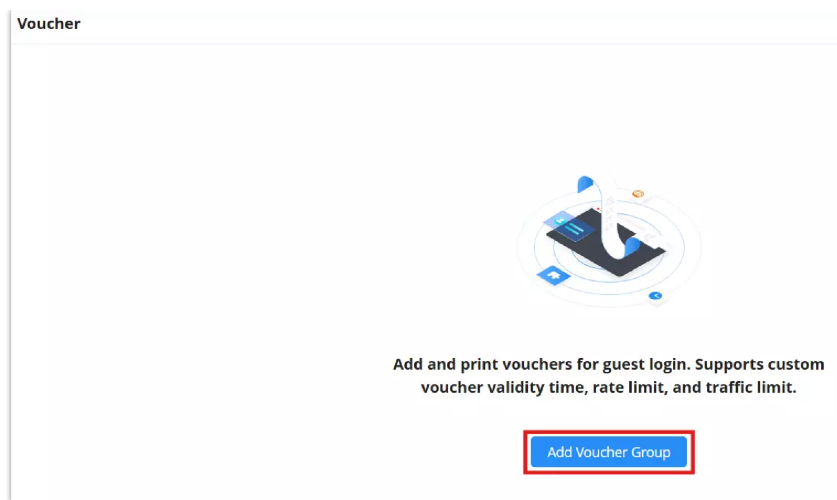
To begin voucher configuration:

- Navigate to Guests → Voucher
- This will bring up the voucher management screen

◦ Adding a New Voucher Group:

To add vouchers manually:

1. Click **Add Voucher Group**
2. Fill in the configuration form with the required parameters



Add Voucher Group button

Voucher **Add Voucher Group**

* Name 1-64 characters

Voucher Group Template ☐ Once enabled, the following configuration references the data in the template. [Configuration template](#)

* Quantity 1-1000 numbers

* Device Quota Range from 0-10000, 0 will be excluded

* Duration d h min

Maximum upload rate (Kbps) 1-999999 numbers

Maximum download rate (Kbps) 1-999999 numbers

Byte Limit (MB)

* Validity Time d

Notes 0-64 characters

Add Voucher Group

Field	Description
Name	Label for this batch of vouchers
Voucher Group Template	You can toggle Voucher Group Template ON to auto-fill the voucher fields with a predefined configuration.
Quantity	Number of vouchers to generate
Device Quota	Max number of devices per voucher
Duration	How long each voucher grants access (up to 365 days)
Max Upload/Download Rate	Optional speed limit in Kbps
Byte Limit (MB)	Optional traffic cap, can be per voucher or per device
Validity Time	Number of days this voucher group is valid after creation
Notes	Internal reference note

Add Voucher Group

Using Voucher Group Templates

You can toggle **Voucher Group Template** ON to auto-fill the voucher fields with a predefined configuration.

Templates help ensure consistency and save time when deploying large batches across different networks.

Voucher > Add Voucher Group > **Voucher Group Template**

① If you want to add a voucher group, you can refer to the configuration within the template

* Quantity: 10 (1-1000 numbers)

* Device Quota: 2 (Range from 0-10000, 0 will be excluded)

* Duration: 7 d 0 h 0 min

Maximum upload rate (Kbps): 2500 (1-999999 numbers)

Maximum download rate (Kbps): 5000 (1-999999 numbers)

Byte Limit (MB): 10000 (Per Voucher / Per Device)

* Validity Time: 90 d

Notes: Voucher Group Template (0-64 characters)

Cancel Save

Add Voucher Group Template

Important:

When the toggle is enabled, all relevant fields will auto-fill from the selected template. If disabled, you may edit all fields manually.

o Voucher Branding Options

To customize the printed/exported vouchers, click **Voucher Settings** on the voucher page.

You can upload a **logo** and define a **slogan** which will appear on the printed voucher layout.

Voucher

Add Voucher Group **Voucher Settings** Voucher Group Template

Name: Add Voucher Voucher Quota: 0/10 Duration: 7d Creator: emea_support Byte Limit (MB): 10000 / Per Voucher Created Time: 2025/04/11 12:05PM Validity Time: 2025/07/10 12:05PM Notes: welcome Operation: [Download] [Print] [Delete]

Voucher Settings

Logo: [Upload]

Slogan: Grandstream

Cancel Save

Voucher Branding Options

o Managing Vouchers

After creating a voucher group, you'll see it listed in the table. From the **Operations** column, you can:

- o Download the voucher set as CSV
- o Print vouchers for distribution
- o Delete the batch if needed

Voucher

Add Voucher Group Voucher Settings Voucher Group Template

Group Name

Name	Voucher Quota	Duration	Creator	Byte Limit (MB)	Created Time	Validity Time	Notes	Operation
Add Voucher	0/10	7d	emea_support	10000 / Per Voucher	2025/04/11 12:05PM	2025/07/10 12:05PM	welcome	[Download] [Print] [Delete]

Total 1 10/page

Managing Vouchers

Using the Voucher (Guest Access)

Once generated, vouchers are applied by assigning them to SSIDs configured with a **Splash Page**.

The Splash Page must be set to use **Voucher login mode**. When a guest connects, they'll be prompted to enter a valid voucher code.

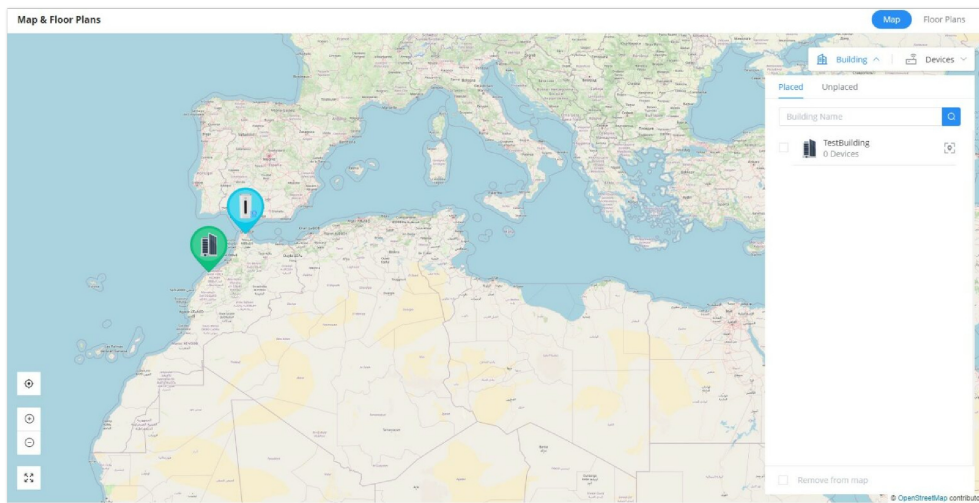
☛ For full setup of the Splash Page and guest portal options, see: [Splash Page Configuration Guide](#)

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:

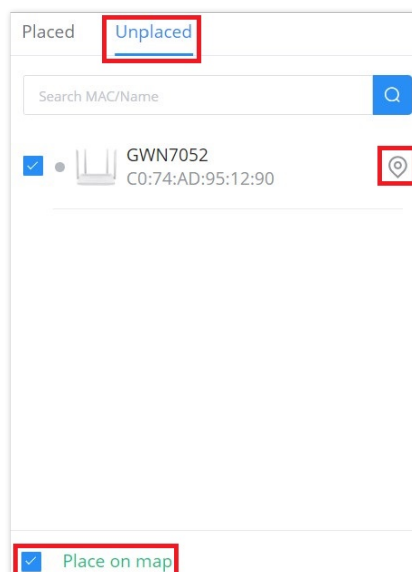


Map

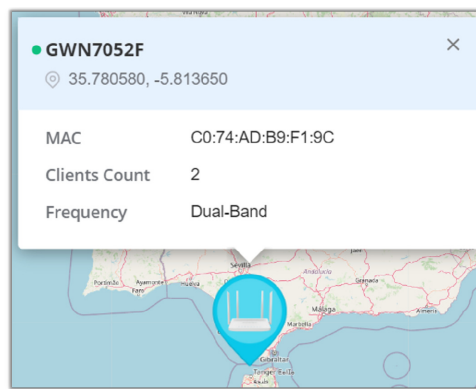
Note:

Map feature on GDMS Networking/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.

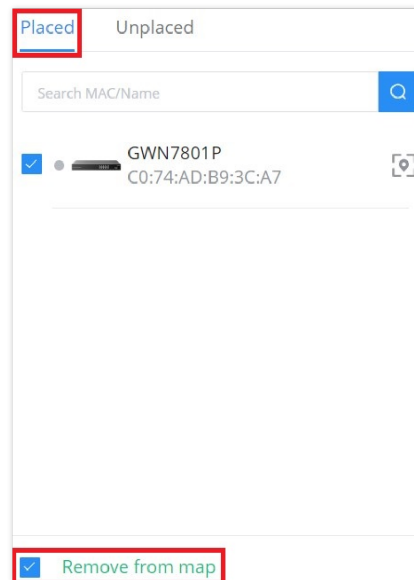


Unplaced devices



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 devices

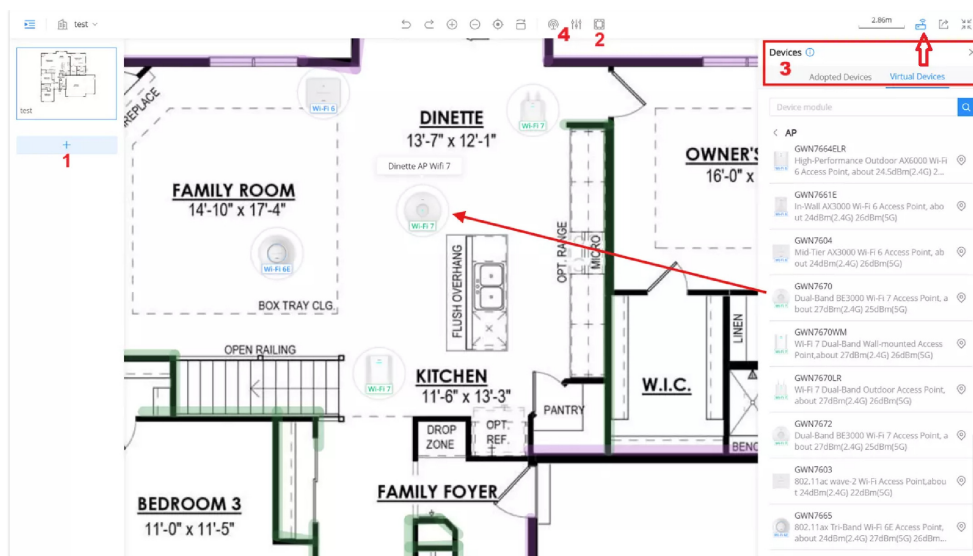
Note:

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:

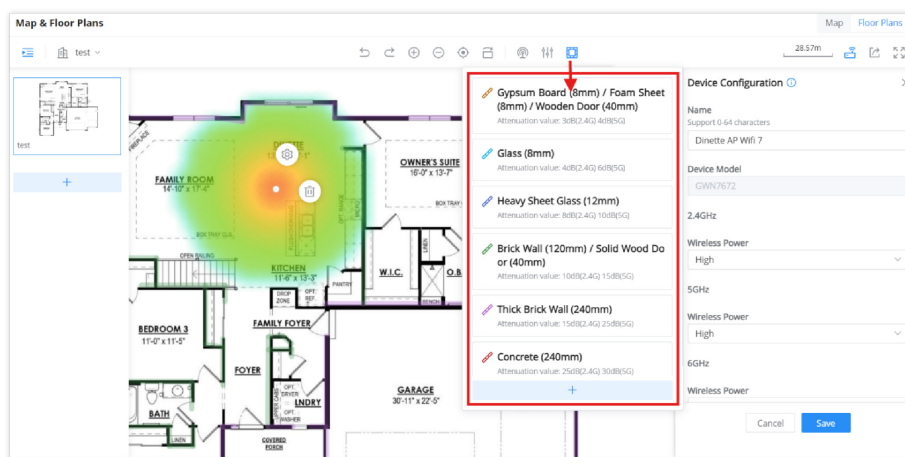


Floor Plans

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).

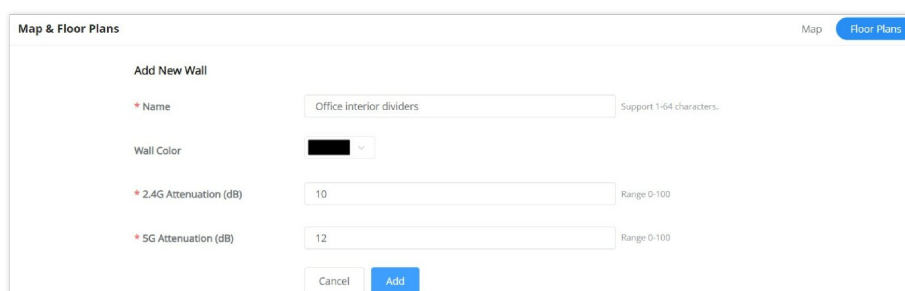
The walls and dividers available are:

- **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.



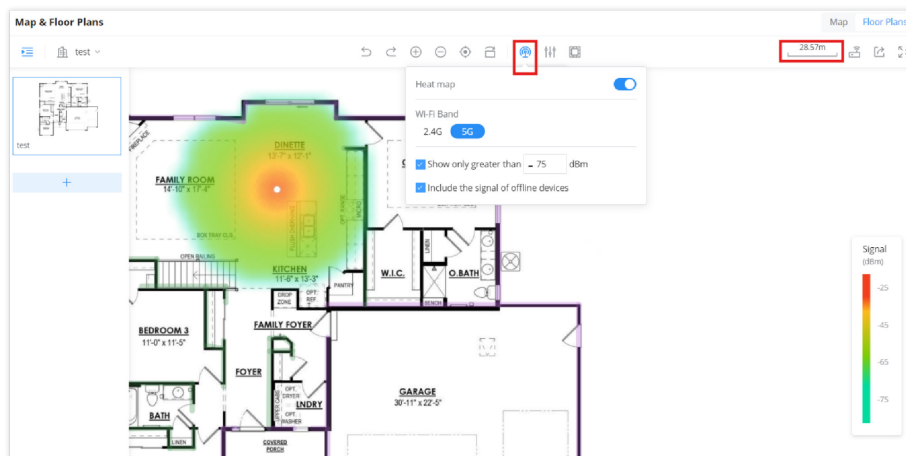
Floor Plans – Custom wall or divider

3. Under devices, please select the GWN device either from adopted ones or virtual ones then place it on the floor building accordingly then it will display the label of the device, also you can click on a device parameter icon then configure the device name, wireless power accordingly. There are also many other tools and option that can help the user to visualize the signal accurately like rotating the floor plan, zoom in or out, center the floor plan ...etc. Please refer to the figure below:



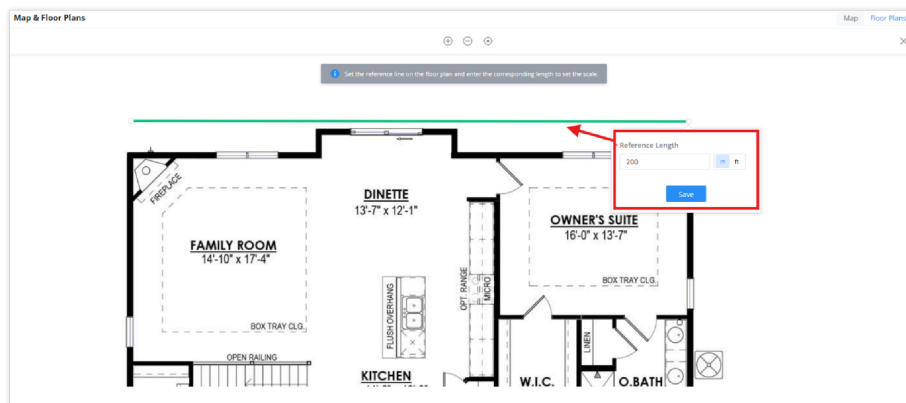
Floor Plans – Heat map

4. 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

For the wireless signal to be fully accurate, it’s very important to specify the Reference Length as accurately as possible by specifying a specific distance length then the system will use this as a reference to calculate the rest of the floor plan accordingly.



Floor Plans – Reference Length

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										
Detect Refresh		All Time		2.4G&5G		Q SSID/BSSID/Scanned by				
SSID	BSSID	Channel	Protocol	Bandwidth	Encryption	Manufacturer	Num of APs	Scanned by	RSSI	Last Seen
Building	9C:59:EB:8B:15:55	5G	802.11ac	80	WPA2	Netgear	1	C0:74:AD:90:B...	-92	2022-12-15 11...
Office - 1000	40:33:06:8B:15:55	5G	802.11ac	80	WPA2	Netgear	1	C0:74:AD:90:B...	-88	2022-12-15 11...
Office - 1001	B8:50:01:8B:15:55	5G	802.11ac	40+	WPA2	Netgear	1	C0:74:AD:90:B...	-95	2022-12-15 11...
Office - 1002	C0:74:AD:90:B...	5G	802.11ac	80	WPA2	Netgear	1	C0:74:AD:90:B...	-91	2022-12-15 11...
Office - 1003	84:3D:C6:8B:15:55	5G	802.11n/a	20	WPA2	Netgear	1	C0:74:AD:90:B...	-88	2022-12-15 11...
Office - 1004	FC:40:09:8B:15:55	5G	802.11ac	80	WPA2	Netgear	1	C0:74:AD:90:B...	-90	2022-12-15 11...
Office - 1005	B8:50:01:8B:15:55	5G	802.11ac	40+	WPA2	Netgear	1	C0:74:AD:90:B...	-95	2022-12-15 11...
Office - 1006	B8:50:01:8B:15:55	5G	802.11ac	40+	Open	Netgear	1	C0:74:AD:90:B...	-92	2022-12-15 11...
Office - 1007	C6:74:AD:90:B...	5G	802.11ac	80	Open	Netgear	1	C0:74:AD:90:B...	-91	2022-12-15 11...
Office - 1008	84:3D:C6:8B:15:55	5G	802.11n/a	20	Open	Netgear	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

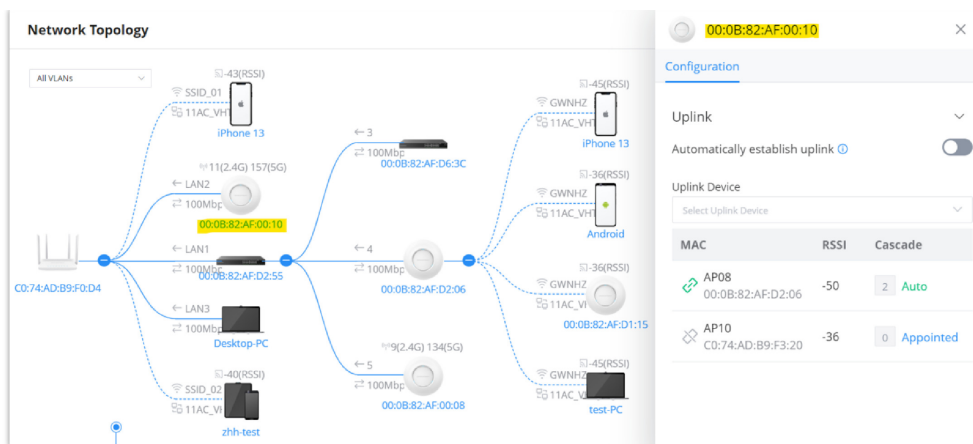
Network Topology shows an overview of the whole network starting from the GWN Router or GCC Convergence device (Internet access) including GWN Switches and Access Points as well as Clients, this way the administrator/monitor can have very quickly an overview of the network at a glance. By clicking on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

Features overview:

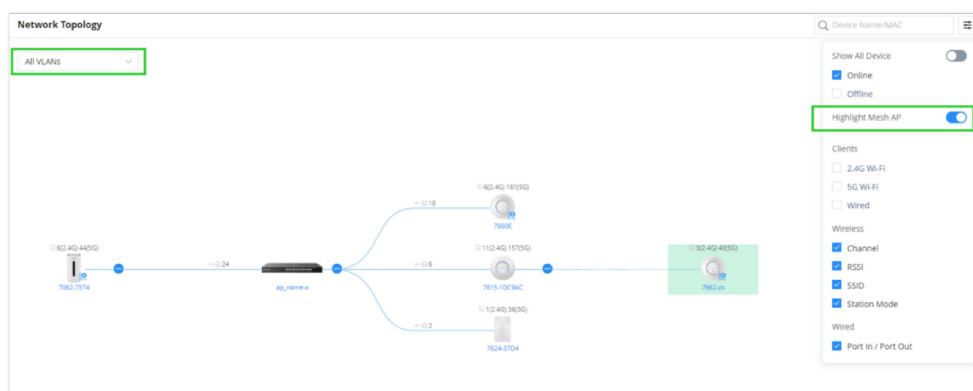
- Display network layout.
- Visualize gateway, switch, access point, and connected client device information.
- The topology map can be zoomed in, and out, and nodes are retractable, also topology supports vertical/horizontal orientation.
- Support Mesh AP and also the option to Highlight Mesh AP.
-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

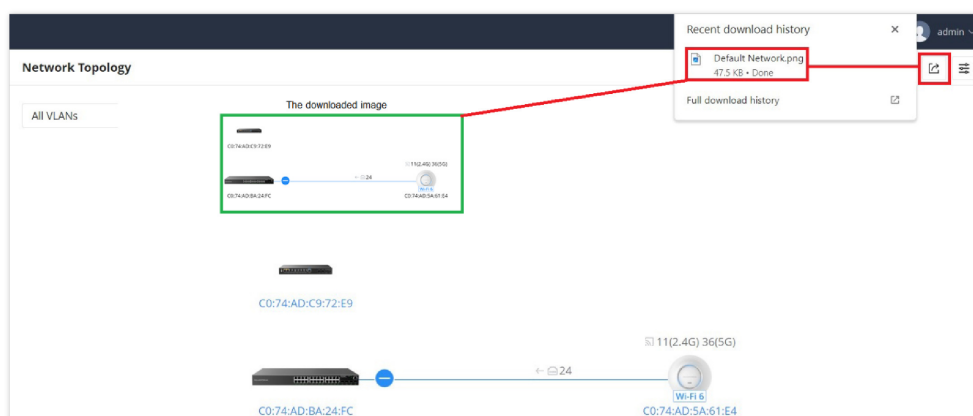


Network Topology – Highlight mesh

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.

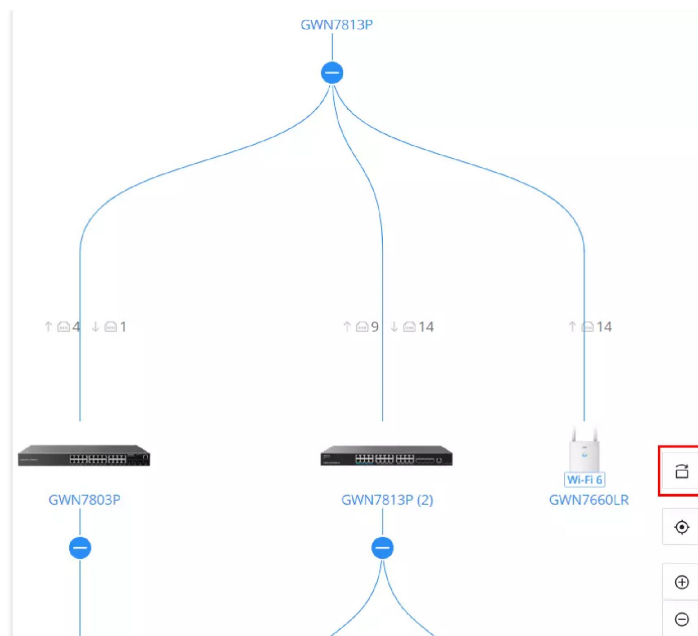
Note:

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



Network Topology – Export

It's also possible to change the topology orientation (vertically or horizontally), click on the orientation icon as shown below,



Network Topology – change orientation

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.

Alert Detail	Alert Type	Level	Alert Time
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-20 12:57PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-20 12:56PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-18 03:11PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-18 03:08PM

Alerts Types

Alert Levels

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

Alert Detail	Alert Type	Alert Level	Alert Time
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Emergency	2023-09-20 12:57PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Warning	2023-09-20 12:56PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-18 03:11PM
Device (C0:74:AD:B9:F1:9C) configuration has been modified by the local user	System	Notice	2023-09-18 03:08PM

Alerts Levels

Read/Unread Alerts

The user can filter the alerts by: **All or Unread**.

Alerts

Alert Settings

Alert Notification

Delete

Delete All

Mark All as Read

Start Date

End Date

All Types

Unread

All Levels

Q MAC/Name

Alert Detail

All

Unread

Alert Type

Level

Alert Time

Switch (C0:74:AD:...) offline more than 2 m

System

Warning

2025/03/26 03:11...

Switch (C0:74:AD:...) port 1/0/7 status is down

Network

Notice

2025/03/26 03:09...

Switch (C0:74:AD:...) port 1/0/8 status is up

Network

Notice

2025/03/26 01:28...

Switch (C0:74:AD:...) port 1/0/8 status is down

Network

Notice

2025/03/26 01:28...

Switch (C0:74:AD:...) port 1/0/8 status is up

Network

Notice

2025/03/26 01:27...

Switch (C0:74:AD:...) port 1/0/8 status is down

Network

Notice

2025/03/26 01:26...

Switch (C0:74:AD:...) port 1/0/8 status is up

Network

Notice

2025/03/26 12:42...

Switch (C0:74:AD:...) port 1/0/8 status is down

Network

Notice

2025/03/26 12:42...

Switch (C0:74:AD:...) port 1/0/7 status is up

Network

Notice

2025/03/26 12:41...

Switch (C0:74:AD:...) port 1/0/7 status is down

Network

Notice

2025/03/26 12:41...

Total 406

10/page

<

1

2

3

4

5

6

...

41

>

Alerts Unread Filter

Alert Settings

The **Alert Settings** page allows administrators to configure which system events will trigger notifications. Alerts are grouped into four categories:

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

Each alert type can be enabled or disabled independently. When selected, the system will notify users based on the defined conditions or thresholds.

System Alert

System Alerts notify administrators about general service or operational issues across routers, switches, and access points. These include device offline/online status, upgrade results, temperature issues, and alert exceptions.

Common examples include:

- Device offline/online for a specific duration
- Upgrade succeeded or failed
- Configuration sync failed
- Temperature or optical module warnings
- Device time deviation detection

Administrators can also exclude specific Access Points from offline alerts using the exception dropdown.

Alerts > **Alert Settings**

System Alert Performance Alert Security Alert Network Alert

Select alerts to be notified of

Cloud

- ☐ AP offline for more than 30 mins, but the selected AP does not generate any alert GWN7624C074AD908...
- ☐ AP online (After offline for 30 mins)
- ☐ Router offline for more than 30 mins
- ☐ Router online (After offline for 30 mins)
- ☐ Switch offline for more than 30 mins
- ☐ Switch online (After offline for 30 mins)
- ☐ Cancel/Return/Reject shared network
- ☐ 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

Alert Settings – part 1

Performance Alerts

Performance Alerts focus on resource usage and traffic thresholds. These alerts are useful for proactively monitoring bandwidth, CPU, memory, and client count across your network devices.

Examples of performance thresholds include:

- Network or SSID throughput exceeded (Cloud-level)
- CPU or memory usage exceeded (Router/Switch/AP)
- Channel usage or client count thresholds
- WAN or port-level throughput exceeded
- Packet loss on switch ports

Each threshold can be customized using percentage or Mbps values.

Alerts > **Alert Settings**

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

Select alerts to be notified of

Router

- ☐ 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

Security Alerts

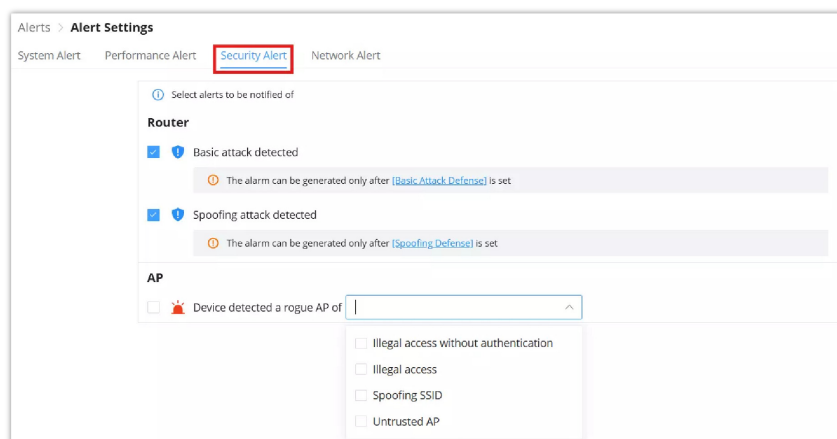
Security Alerts provide early warnings for potential attacks or rogue device detection. These events rely on enabling security features in advance.

Supported alerts include:

- Basic attack detected (e.g., DoS)
- Spoofing attack detected
- Rogue AP detected on the network

Note:

These alerts only activate when Basic Attack Defense or Spoofing Defense features are enabled.



Alert Settings – part 3

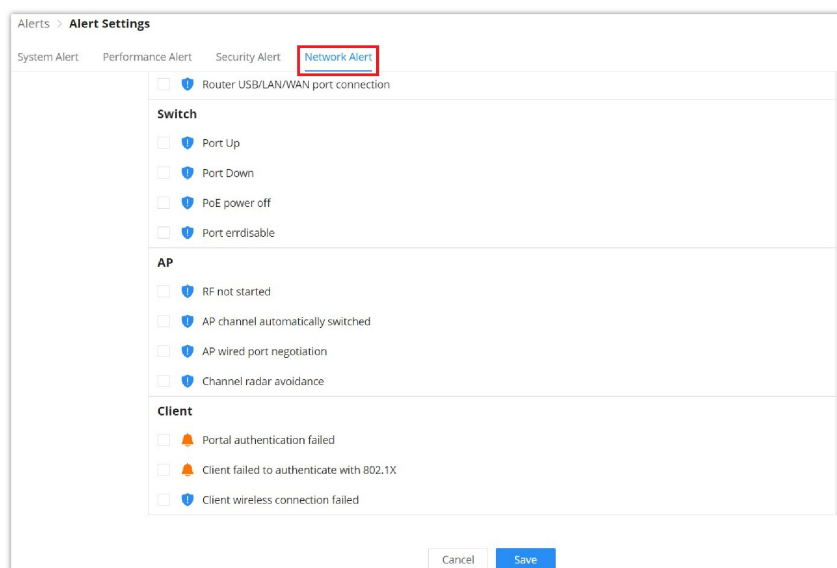
Network Alerts

Network Alerts report changes in port, RF, or client behavior across the network. This helps identify connectivity issues or disruptions at the physical and wireless levels.

Monitored conditions include:

- WAN/PPPoE failures or disconnections
- VPN tunnel and client status changes
- Port up/down status and PoE events
- Channel radar detection and RF activity
- Client authentication failures or wireless connection issues

These alerts provide deeper visibility into how devices and users interact with the network.



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
Cloud	
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
Cloud	
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"/>
Router	
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"/>
Switch	
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
AP	
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 ⓘ
Router	
 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"/>
Switch	
 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"/>
AP	
 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 displays all SSIDs configured under the current network. Each SSID is listed with key details, including:

- **Wi-Fi Status**
- **VLAN ID**
- **Wi-Fi Band** (e.g., 2.4GHz, 5GHz, or both)
- **Online Devices**
- **Security Type**
- **Portal Status**
- **Operation Controls**

The **Wi-Fi Band** column helps identify which frequency bands are currently in use for each SSID.

You can edit any SSID using the gear icon or click **+ Add** to create a new one.

All settings under this section are applied per SSID.

Global Radio Settings: This section manages radio parameters that apply across all SSIDs and access points. Use this panel to control default band behavior, transmit power, and other global wireless properties.

Mesh: enables wireless mesh networking between supported access points. Options include scan interval and cascading limits, helping extend coverage in environments without wired uplinks.

Wi-Fi

Wireless LAN

Q Name

+ Add

Name	Wi-Fi Status	VLAN ID	Wi-Fi Band	Online Devices	Security Type	Portal	Operation
Guest wifi	Enabled	—	2.4GHz,5GHz	1	Open	Disabled	
Office Network	Enabled	—	2.4GHz,5GHz	0	Open	Enabled	

Global Radio Settings

Mesh

Wi-Fi page

Add 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
Enable MLO	Allows the device to connect to multiple Wi-Fi bands (e.g., 2.4GHz + 5GHz and 6GHz) at the same time. Helps boost speed, reduce lag, and make the connection more stable. Requires compatible client devices.
Access Security	

Security Type	<p>Set the security type, 5 options are available:</p> <ul style="list-style-type: none"> ● Open : no security is required ● Personal: Select the WPA Pre-Shared Key and the WPA Mode ● Enterprise: Select Radius Authentication and WPA Mode. ● WPA2: Select the WPA2 Group. ● WPA3: Select the WPA3 Group.
802.11w	<p>Disabled: disable 802.11w;</p> <p>Optional: either 802.11w supported or unsupported clients can access the network;</p> <p>Required: only the clients that support 802.11w can access the network.</p>
Access Control	
MAC Filter	<p>Controls access based on device MAC addresses. Choose Allowlist to only let approved devices connect, or Blocklist to keep specific ones out. If no list is selected while Allowlist is enabled, no clients will be able to connect.</p> <p><i>Note: The total number of MAC addresses across all blocklists is limited to 1000 entries.</i></p>
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"> ● Radio Mode: Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76xx but they cannot communicate with each other. ● Internet Mode: Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76xx. ● Gateway MAC Mode: Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76xx access points. ● Custom MAC Address: All clients except for the added MAC addresses will be isolated from each other. <i>Note: The gateway MAC address must be included when configuring this.</i>
Client Time Policy	Configures the client time policy. Default is None.
Bandwidth Control	Select Bandwidth Control (Per-SSID or Per-Client), then select from the Bandwidth rules previously created.
Schedule	Select a schedule that will be applied to this SSID, schedules can be managed from the menu "Settings → Profiles → Schedule" .
OS Filter	<p>Whitelist or blacklist clients based on what OS they are using.</p> <ul style="list-style-type: none"> ● Disabled: the feature is disabled ● Whitelist: the user will select the OS that will be whitelisted ● Blacklist: the user will select the OS that will be blacklisted <p><i>Warning: This feature requires certain client functionality to work, and some clients' OS may not be supported.</i></p>
OS Whitelist/Blacklist	<p><i>Note: this option is only available if OS Filter is enabled.</i></p> <p>Select one or more or All from the list below:</p> <ul style="list-style-type: none"> ● All ● Windows® ● macOS® ● iOS® ● Linux® ● Android®
Device Assignment	

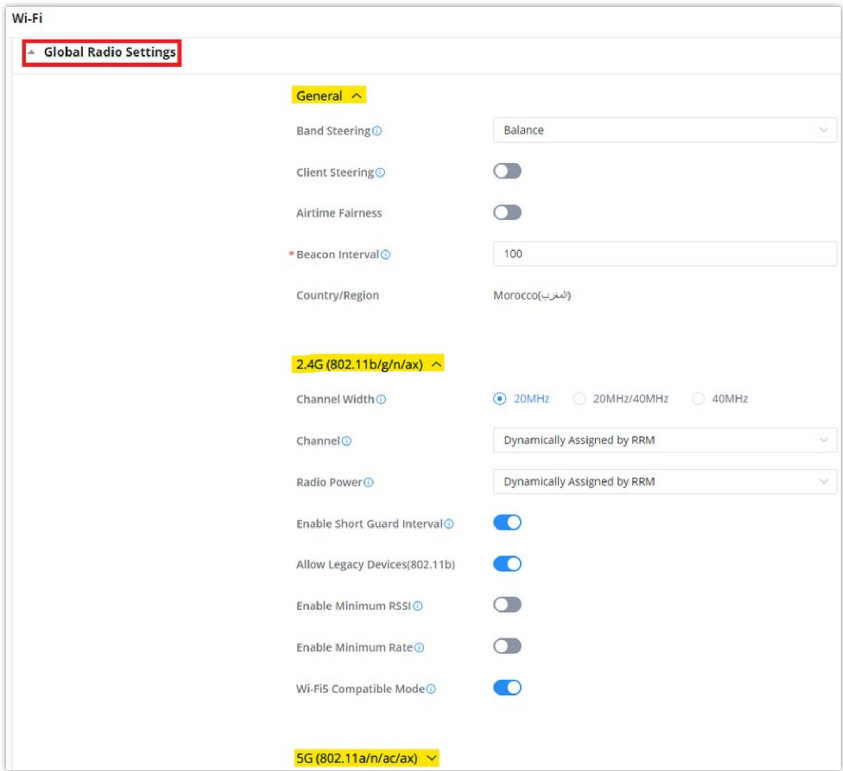
<p>Select from the Devices list the ones to be part of this SSID.</p> <p>Note: <i>If an AP or router that uses the Wi-Fi network is selected, new APs will be automatically added to the network.</i></p>	
Advanced	
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
DTIM Period	<p>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.</p> <p>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.</p> <p>Valid range: 1 – 10.</p>
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	<p>Disable: all of the broadcast and multicast packages will be forwarded to the wireless interface.</p> <p>Enable: all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND;</p> <p>Enable with Proxy ARP enabled: enable the optimization with Proxy ARP enabled in the meantime.</p>
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	<p>Enable this feature to help clients connected to the GWN76xx to perform better roaming decision.</p> <ul style="list-style-type: none"> • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. • When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. <p>Note: <i>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	<p>Click to enable Bonjour Gateway</p> <p>Note: <i>If enabled, client Bonjour requests on SSID can be forwarded to the VLAN of Bonjour services (such as Samba).</i></p>
Enable U-APSD	Configures whether to enable U-APSD (Unscheduled Automatic Power Save Delivery)

Target Wake Time	Enables TWT (Target Wake Time), a Wi-Fi 6/7 power-saving feature that lets the AP and clients agree on specific times to communicate. This reduces constant checking and helps compatible devices stay in low-power mode longer, extending battery life. <i>Note: Only available on Wi-Fi 6/7 models. Not effective if Wi-Fi 5 compatibility mode is enabled.</i>
------------------	--

Add Wireless LAN

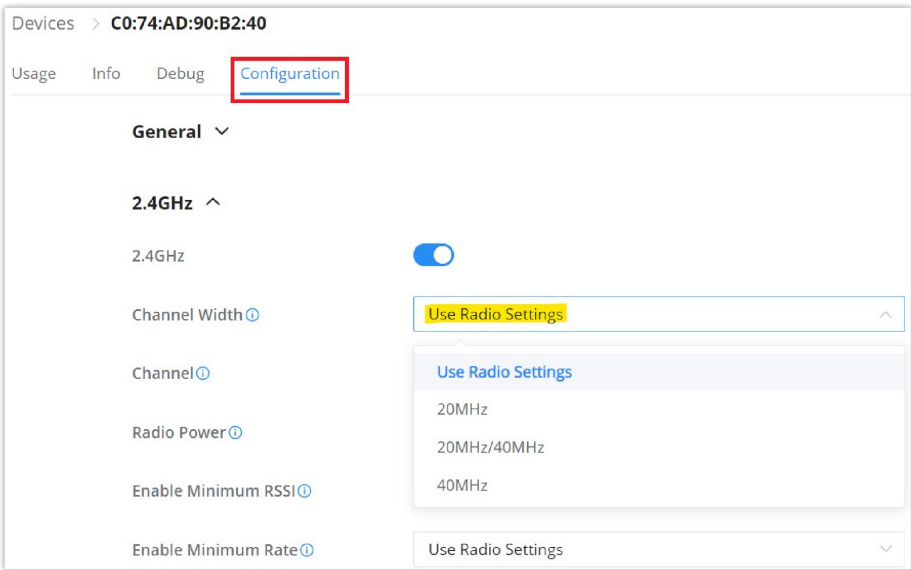
Global Radio Settings

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	<p>Select from the drop-down list, four options are available:</p> <ul style="list-style-type: none"> ● Disable Band Steering: Band steering is disabled ● 2.4G in priority: steer clients to 2.4G ● 5G in priority: steer clients to 5G ● Balance: balance between 2.4G and 5G.
Client Steering	<p>This feature will help Wi-Fi client to roam to other APs within same Network. Steering happens when clients is inactive or active clients with the standards 802.11K&V support.</p>
RSSI Threshold	<p>It will start monitoring the RSSI for the clients in order to redirect them to another GWN AP in the same network. This prevents clients from remaining associated with AP with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients. <i>Default is -75.</i></p>
Client Access Threshold	<p>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></p>
Airtime Fairness	<p>Allows faster clients to have more airtime than slower clients.</p>
Beacon Interval	<p>Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp...</p> <ul style="list-style-type: none"> ● Using High Beacon Interval: AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save WiFi clients energy consumption. ● Using Low Beacon Interval: AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by WiFi clients with weak signal. <p>Notes:</p> <ul style="list-style-type: none"> ● When AP enables several SSIDs with different interval values, the max value will take effect. ● When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. ● When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. ● When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500. ● Mesh feature will take up a share when it is enabled. <p><i>Default value is 100ms. Valid range: 40 – 500 ms.</i></p>
Country/Region	<p>Displays the country/region of the AP.</p>
2.4G/5G	
Channel Width	<p>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.</p>
Channel	<p>Select "Auto" or a Dynamically Assigned by RRM. <i>Default is "Auto".</i></p>
Custom Channel	<p>Select a custom channels. <i>Note: that the proposed channels depend on Country Settings under Settings → System.</i></p>
Radio Power	<p>Set the Radio Power, it can be Low, Medium, or High or Custom or Dynamically assigned by RRM or Auto.</p> <p><i>Note : Dynamically assigned by RRM activates TPC and CHD:</i></p> <ul style="list-style-type: none"> ● Transmit Power Control: TPC algorithm runs every 10 minutes. AP acquires the RSSI information of the neighbor by wireless scanning and establishes the neighbor table. The algorithm requires that there must be at least 3 neighbor APs with RSSI larger than -70dbm. Otherwise, power will not be adjusted.

	<ul style="list-style-type: none"> ● Coverage Hole Detection: CHD enables AP to decide whether to increase the AP power by the current SNR and SNR threshold of the connected clients. <p>Custom: allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.</p>
Enable Short Guard Interval	Check to activate this option to increase throughput.
Allow Legacy Devices (802.11b)	Check to support 802.11b devices to connect the AP in 802.11n/g mode. (2.4GHz setting)
Enable Minimum RSSI	Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm).
Minimum RSSI (dBm)	Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from “-94” or “-1”.
Enable Minimum Rate	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP.
Minimum Rate (Mbps)	Specify the minimum access rate. Once the client access rate is less than the specified value, AP will kick it off. Available values are: 1Mbps, 2Mbps, 5Mbps, 6Mbps, 9Mbps, 11Mbps or 12Mbps.
Wi-Fi5 Compatible Mode	Some old devices do not support Wi-Fi6 well and may not be able to scan the signal or connect poorly. After turning on this switch, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions.

Global Radio Settings

Mesh

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

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

- 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. For more details please refer to the figure and table below:

LAN > Add LAN

* LAN Name

1-64 characters

* VLAN ID

2-4094 numbers

VLAN-Only Network

☐

* Gateway

IPv4

IPv4

☒

* Gateway IPv4 Address/Prefix Length

/

Prefix length range 8-30

DHCP Service

IPv6

IPv6

☒

Interface ID

☒

If disabled, the LAN interface ID will be automatically generated based on the selected MAC.

* Custom Interface ID

: : :

Cancel

Save

Add VLAN

Field	Description	Notes
LAN Name	Name of the LAN interface (1–64 characters). Used for internal reference.	-

VLAN ID	Numeric ID for VLAN tagging (2–4094). VLAN 2 is now supported.	-
VLAN-Only Network	Enable to make the interface operate in VLAN-only mode (no IP stack or routing).	If enabled, disables all IP settings. Use for pure Layer 2 VLAN bridging.
Gateway	Select a gateway device (Router, Switch, or Device Group) managed by GDMS Networking.	You can assign a logical gateway from managed routers, switches, or device groups.
IPv4	Toggle to enable IPv4 addressing on the LAN interface.	-
Gateway IPv4 Address/Prefix Length	Define the LAN's gateway IP address and subnet prefix (CIDR format, e.g., 192.168.1.1/24).	Defines IP and subnet of the LAN segment. Needed for routing and DHCP.
DHCP Service	Choose DHCP Server, DHCP Relay, or Close (disable DHCP).	Use DHCP Server to assign IPs, Relay to forward requests, or Close to disable.
IPv6	Toggle to enable IPv6 addressing on the LAN interface.	-
Interface ID	Auto-generates the LAN interface ID based on the selected MAC address (if enabled).	Auto-fills the Interface ID based on MAC address unless disabled.
Custom Interface ID	Manually define a unique identifier for the IPv6 interface.	Only needed if a specific interface ID is required.
IPv6 Preferred DNS Server	Optional: Specify preferred DNS for IPv6 clients.	Only needed if using custom DNS for IPv6 clients.
IPv6 Alternative DNS Server	Optional: Specify a secondary DNS server for IPv6 clients.	Optional backup DNS server for IPv6.
IPv6 Relay from WAN	Toggle to allow DHCPv6 relay from the WAN interface.	Used when upstream router provides IPv6 settings via relay.
IPv6 Address Assignment	Choose assignment behavior for IPv6 addresses (if available).	Controls how IPv6 addresses are assigned (e.g., stateless or static).

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

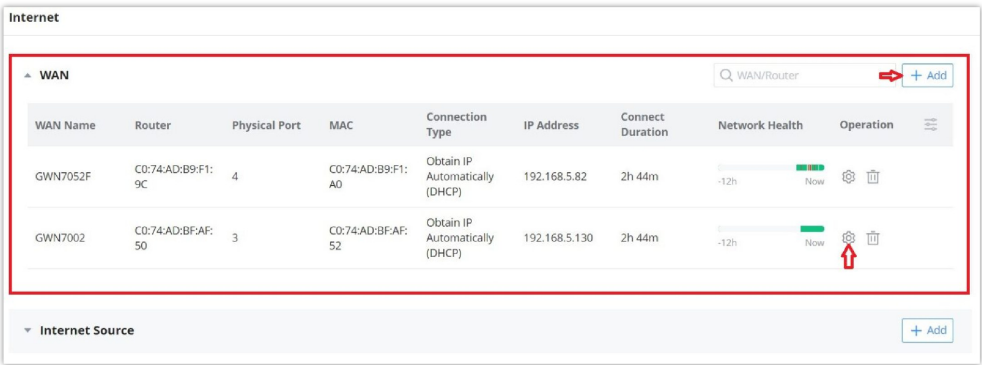
Internet

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 GDMS Networking/GWN Manager accordingly. Once, the WAN/Device group is added, then the user can monitor the network health for the last 12 hours.

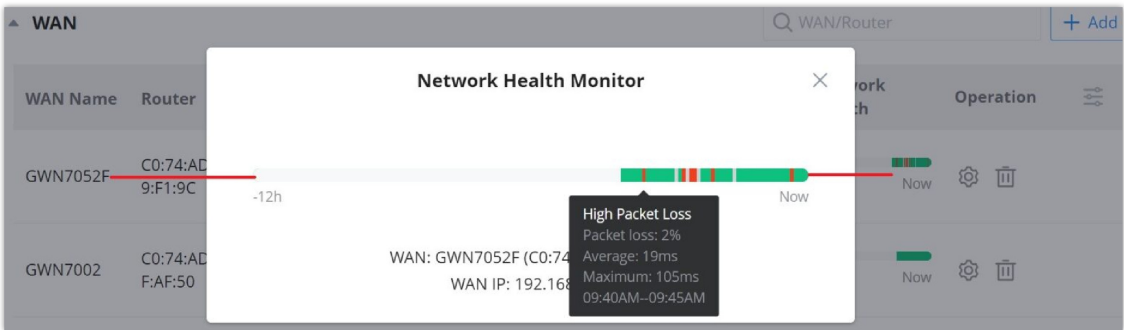
Please navigate to **Web UI → Settings → Internet page → WAN section.**



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 > **Add WAN**

DDNS

DDNS ☒

Service Provider

* Username

* Password

* Domain

If no account is available, please go to www.oray.com to register for a username, password and domain.

* IP Source ☒ WAN IP ☐ Public IP

* Update Interval (min) 1-1440 numbers

Cloud DDNS ☒

* Domain

Update Copy

* IP Source ☒ WAN IP ☐ Public IP

* Update Interval (min) 1-1440 numbers

DMZ

Destination Group

UPnP

UPnP ☐

Add/edit a WAN – part 3

WAN Name	Specify a name for the WAN
Router	Select a router or a Device group from the drop-down list

Physical Port	Select the physical port (WAN port) from the drop-down list
Connection Type	<ul style="list-style-type: none"> ● Obtain IP automatically (DHCP): When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. ● Enter IP Manually (Static IP): When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. ● Internet Access with PPPoE account (PPPoE): When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval, and Inter-Key Timeout (in seconds). <p><i>The default setting is "Obtain IP automatically (DHCP)"</i></p>
Static DNS	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server
Preferred DNS Server	Enter the preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
Maximum Transmission Unit (MTU)	<p>Configures the maximum transmission unit allowed on the WAN.</p> <ul style="list-style-type: none"> ● When using Ethernet, the valid range that can be set by the user is 576-1500 bytes. The default value is 1500. Please do not change the default value unless you have to. ● When using PPPoE, the valid range that can be set by the user is 576-1492 bytes. The default value is 1492. Please do not change the default value unless you have to.
WAN Port MAC Address	<p>Select from the drop-down list either to:</p> <ul style="list-style-type: none"> ● Use Default MAC Address ● Use Custom MAC Address <p><i>Default is "Use Default MAC Address"</i></p>
Custom MAC Address	Enter the custom MAC Address to be used with this WAN.
Tracking IP Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal.
Tracking IP Address 2	Add another alternative address for Tracking IP Address
VLAN Tag	Select if either to enable or disable VLAN Tag.
VLAN Tag ID	Enter the VLAN tag ID.
Priority	<p>Enter the priority</p> <p><i>Note: Range 0-7 and 7 is the highest priority</i></p>
Multiple Public IP Addresses	Please use with Port Forward function, so that you can access to router via public IP address.
Public IP Address	<p>Enter one or more public IP addresses</p> <p>Click on "+" icon or "-" icon to add or delete public IP addresses</p>
IPv6	
IPv6	Enable this option to use IPv6 on this specific WAN.
Connection Type	<p>Select the connection type from the drop-list, three options are available:</p> <ul style="list-style-type: none"> ● Obtain IP automatically (DHCPv6) ● Enter the IP manually (static IPv6)

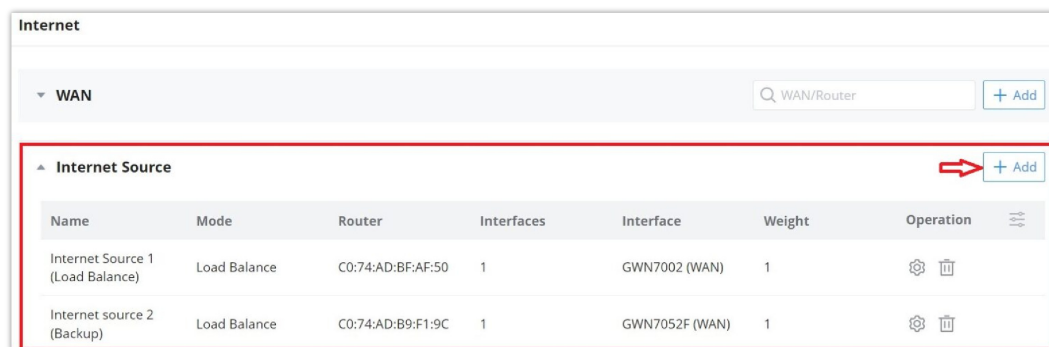
	<ul style="list-style-type: none"> Internet Access with PPPoE Account (PPPoE) <p>The default setting is “Obtain IP automatically (DHCPv6)”.</p>
Static DNS	Enable this option to enter statically assigned DNS
Preferred DNS Server	Enter the preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
IPv6 Relay to VLAN	Once enabled, relay IPv6 addresses to clients on the LAN side. Note: This function will take effect only "IPv6 Relay from WAN" is enabled on VLAN.
Tracking IPv6 Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal
Tracking IPv6 Address 2	Add another alternative address for Tracking IP Address
DDNS	
DDNS	Toggle ON or OFF the DDNS function, default is OFF <i>Note: On the router, DDNS function can only be enabled on one WAN port.</i>
Service Provider	Select the DDNS provider from the list <i>Note: Includes providers like no-ip.com, freedns.afraid.org, Oray, etc.</i>
Username	Enter the username for your DDNS account. <i>Note: Required for third-party DDNS providers.</i>
Password	Enter the password for your DDNS account. <i>Note: Required for third-party DDNS providers.</i>
Domain	Enter the domain registered with your DDNS provider. <i>Note: Must match the domain you've set up with the DDNS provider.</i>
IP Source	Choose whether to use the WAN IP or Public IP for DDNS updates. <i>Note: Select WAN IP to use in the same network segment. Public IP reflects external visibility.</i>
Update Interval (min)	Set how often the router updates the DDNS IP address. <i>Note: Valid range is 1 to 1440 minutes.</i>
Cloud DDNS	Enable to use GDMS Networking's built-in DDNS without an external provider. <i>Note: No login required. Automatically generates a *.gwn.ai domain.</i>
Domain (Cloud DDNS)	Displays the generated gwn.ai domain name. <i>Note: Read-only. Click 'Update' to regenerate the subdomain.</i>
IP Source (Cloud DDNS)	Choose WAN or Public IP for the cloud DDNS. <i>Note: Same logic as standard DDNS affects domain resolution visibility.</i>
Update Interval (min, Cloud DDNS)	Set how frequently the router reports the IP to GDMS cloud. <i>Note: Valid range is 1 to 1440 minutes.</i>
DMZ	
Destination Group	Select the destination group from the drop-down list.

UPnP	
UPnP	Toggle ON or OFF the UPnP function, default is OFF <i>Note: If UPnP (Universal Plug and Play) is enabled, devices on LAN can request the router to port forward automatically</i>
Destination Group	Select the destination group from the drop-down list.

Add/edit a WAN

Internet Source

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



Internet Source

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

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

Add an Internet Source

VPN

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

GDMS Networking 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.

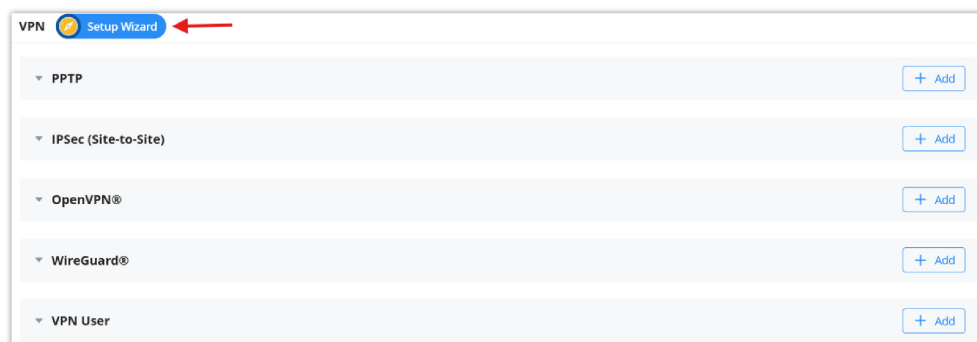
Setup Wizard

The **VPN Setup Wizard** is a step-by-step assistant designed to help users configure VPN tunnels more easily and quickly. It supports four common protocols:

- **OpenVPN®**
- **WireGuard®**
- **IPSec (Site-to-Site)**
- **PPTP**

The wizard helps users choose the correct scenario (e.g., client-to-site or site-to-site), fill in the minimum required settings, and deploy the VPN configuration in fewer steps. This is useful for both first-time setups and fast testing environments.

To access the wizard: Navigate to Settings → VPN → Setup Wizard



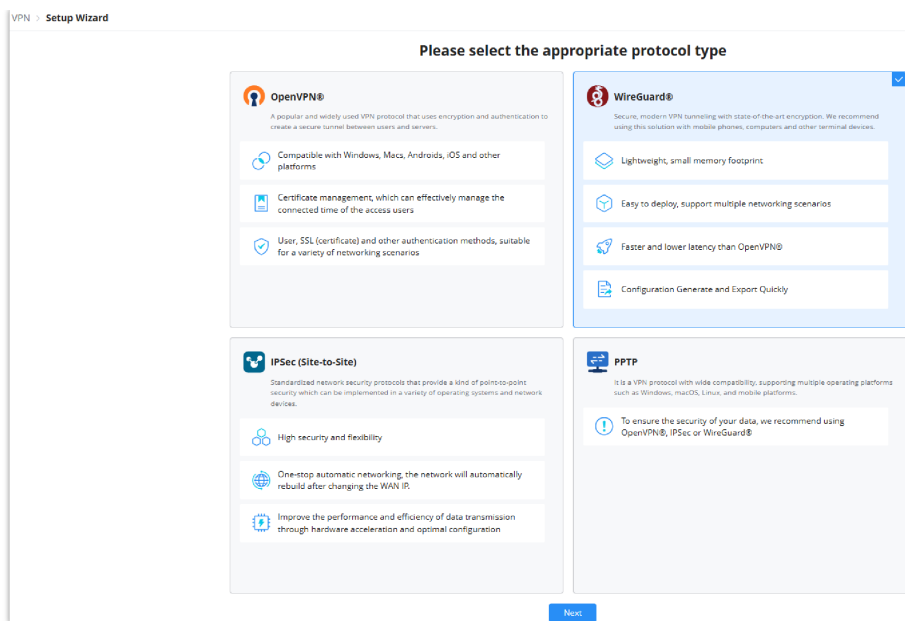
VPN Setup Wizard

Select a VPN Protocol

The wizard starts by letting you select a VPN type. Each has specific use cases and benefits.

Protocol Overviews:

- **OpenVPN®**:
Secure, open-source VPN protocol suitable for cross-platform connections (Windows, Mac, Android, iOS). Supports certificate-based authentication and is ideal for remote workforce access or site-to-site encryption over public networks.
- **WireGuard®**:
Lightweight and modern protocol with fast setup and minimal overhead. Ideal for mobile users or low-resource devices. Supports quick configuration export for peers.
- **IPSec (Site-to-Site)**:
Enterprise-grade encryption standard. Suitable for building permanent tunnels between two fixed locations (e.g., HQ ↔ Branch). Supports dynamic IP updates and hardware acceleration.
- **PPTP**:
Legacy protocol with broad compatibility. Easy to configure but not recommended for high-security needs. Best for internal or low-risk use cases.



Select a VPN Protocol

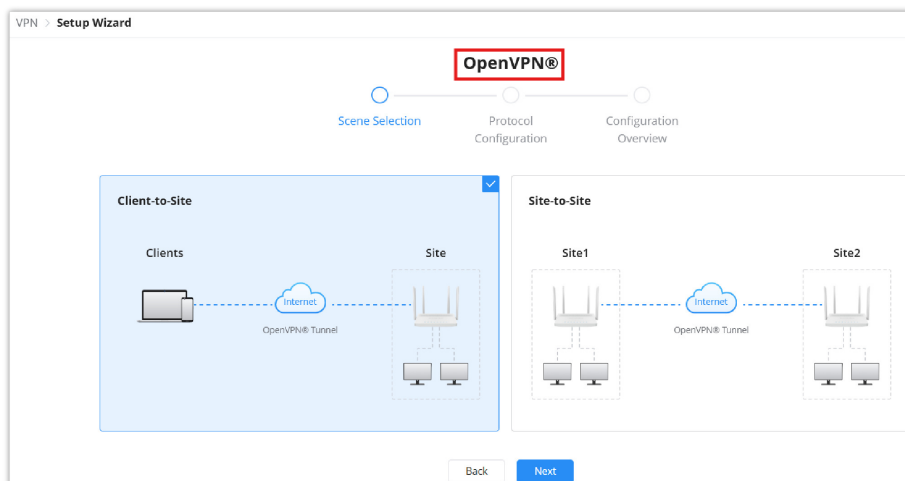
OpenVPN® Configuration Wizard

Choose between:

- **Client-to-Site** – For remote users to connect securely to a central office.
- **Site-to-Site** – To connect two office networks over the internet.

Once selected, the wizard will guide through server selection, certificate management, and encryption options.

For advanced configuration, refer to [OpenVPN® Manual Setup](#).



OpenVPN® Configuration Wizard

WireGuard® Configuration Wizard

WireGuard uses fewer parameters for faster setup. You'll be prompted to:

- Name the connection
- Choose the router and WAN interface
- Assign the local IP and subnet

For advanced features like Peers and Remote Clients, refer to [WireGuard® Manual Configuration](#).

VPN > Setup Wizard

WireGuard®

Interface Settings Scene Selection Protocol Configuration Configuration Overview

Select WireGuard® Add New WireGuard...

* Name: WireGuard Server 1-64 characters

* Router: Select Router

* Interface: Select WAN

* Local IP Address/Mask Length: 192.168.77.138 / 24 Mask Length 24-32

Back Next

WireGuard® Configuration Wizard

IPSec (Site-to-Site) Wizard

Designed for secure office-to-office tunnels. Simply select the Site-to-Site mode, and the wizard handles tunnel basics like endpoint roles and tunnel IPs.

Why use this:

- Ideal for permanent, encrypted connections between two static sites
- Supports automatic rebuild after WAN IP changes

For detailed control and manual tuning, see [IPSec Site-to-Site Setup](#).

VPN > Setup Wizard

IPSec (Site-to-Site)

Scene Selection Mode Selection Protocol Configuration Configuration Overview

Site-to-Site

Site1 Site2

Internet

IPSec Tunnel

Back Next

IPSec (Site-to-Site) Wizard

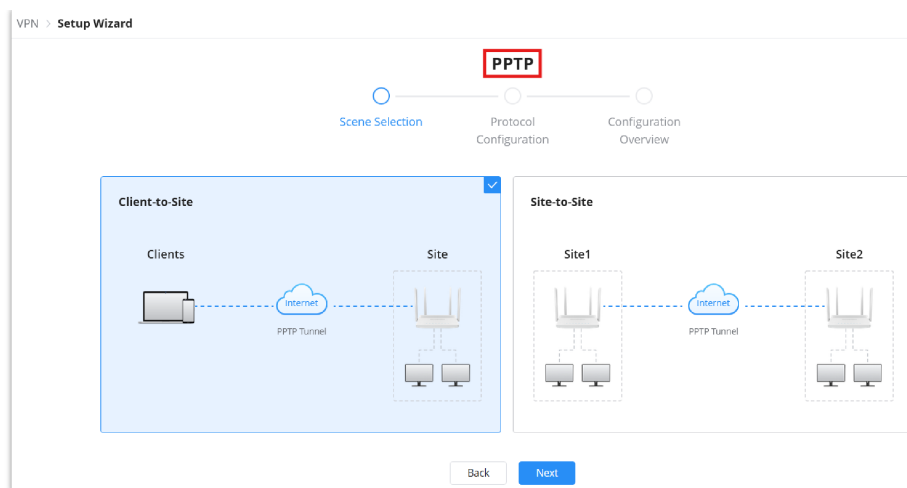
PPTP Wizard

Choose:

- **Client-to-Site** – For basic remote user access
- **Site-to-Site** – For simple office-to-office bridging

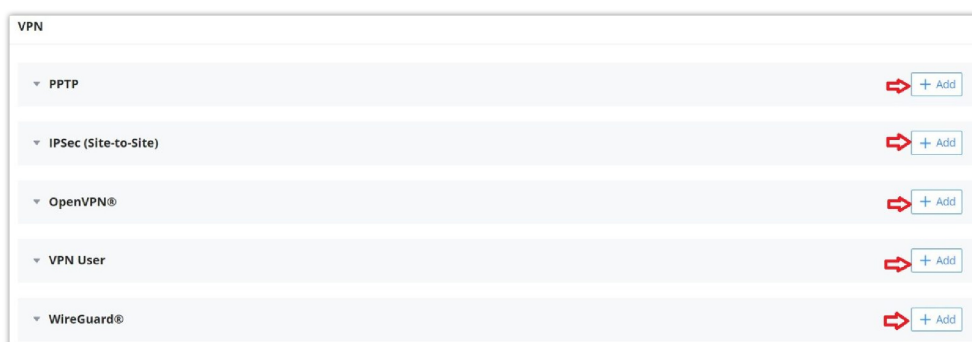
PPTP is the easiest to set up, but less secure. Only use it in trusted environments or for quick internal access.

For more configuration options, refer to [PPTP Setup](#).



PPTP Wizard

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

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.

The image shows the 'Add PPTP' configuration form. It has a 'Type' section with radio buttons for 'PPTP Client' (selected) and 'PPTP Server'. Below this are several fields:

- Name:** PPTP VPN (1-64 characters)
- Status:** A toggle switch is turned on, with a note: '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:** A toggle switch is turned on.
- IP Masquerading:** A toggle switch is turned on.
- MTU:** 1450 (576-1450 numbers)
- Remote Network:** 192.168.122.0 / 24

 At the bottom, there are 'Cancel' and 'Save' buttons, and a green '+ Add New Item' button.

VPN – Add PPTP Client

Type	Select either PPTP Client or PPTP Server to configure.
Name	Enter a name for the PPTP client.
Status	Toggle ON or OFF to enable or disable the PPTP Client VPN. <i>Note: PPTP Server: Once disabled, the PPTP service will also be disabled.</i>
Server Address	Enter the IP/Domain of the remote PPTP Server.
Username	Enter the Username for authentication with the VPN Server.
Password	Enter the Password for authentication with the VPN Server.
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
MPPE Encryption	Enable / disable the MPPE for data encryption. <i>By default, it's disabled.</i>
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (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 PPTP Server to configure.
Name	Enter a name for the PPTP Server.
Status	Toggle ON or OFF to enable or disable the PPTP Client/Server VPN. <i>Notes: Once disabled, the PPTP service will also be disabled.</i>
Server Local Address/Prefix Length	Specify the server local address with the prefix length
Client Start Address	specify client start IP address
Client End Address	specify client end IP address
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
MPPE Encryption	Enable / disable the MPPE for data encryption. <i>By default, it's disabled.</i>
LCP Echo Interval (sec)	Configures the LCP echo send interval.
LCP Echo Failure Threshold	Set the maximum number of Echo transfers. If it is not answered within the set request frames, the PPTP server will consider that the peer is disconnected and the connection will be terminated.
LCP Echo Adaptive	<ul style="list-style-type: none"> ● Once enabled: LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request. ● Once disabled: the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.
Maximum Receive Unit (MRU)	MRU indicates the size of the received packets. By default is 1450.
Preferred DNS Server	specify the preferred DNS server. <i>Ex: 8.8.8.8</i>
Alternative DNS Server	specify the alternative DNS server. <i>Ex: 1.1.1.1</i>

VPN – Add PPTP Server

IPSec (Site-to-Site)

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

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

GDMS Networking 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

General ^

Mode

☐ Manual

☒ Auto

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

*Name

IPsec VPN

1-64 characters

Status

☒

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

*Router

C0:74:AD:B9:F1:9C

*Interface

GWN7052F

*Peer

Network

Router

WAN

Default Networ

C0:74:AD:BF:AF

GWN7002

Cancel

Save

VPN – Add IPsec Auto

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

VPN – Add IPsec auto mode

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

VPN > Add IPSec

General ^

Mode

☒ Manual
☐ Auto

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

Name

IPSec Manual

1-64 characters

Status

☒

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

Remote Address

192.168.5.10

Router

C0:74:AD:BF:AF:50

Interface

GWN7002

Pre-shared Key

.....

1-32 characters

Local Network

192.168.122.0

/

24

Add New Item

Remote Network

192.168.80.0

/

24

Add New Item

Advanced Settings v

Cancel

Save

VPN – Add IPSec Manual mode

General	
Mode	<p>Select the mode: Manual or Auto.</p> <p>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.</p>
Name	Specify a name for IPSec VPN.
Status	<p>Toggle ON or OFF to enable or disable the IPSec VPN.</p> <p>Note: once disabled, the associated VPN services will also be disabled.</p>
Remote address	Specify the remote IP address
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
Pre-shared key	Specify a pre-shared key
Local Network	Set the local IP address and mask length of the protected traffic. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Remote Network	Set the peer IP address and mask length of the protected data flow. Please enter an IP address or subnet (e.g., 192.168.122.0/24)
Advanced Settings	
IKE Version	Select from the drop-down list the IKE version: IKEv1 or IKEv2.
IKE SA Lifetime (sec)	Specify the IKE SA Lifetime (sec), default is 28800.
Local Source IP	Enter the local Source IP address.
Local ID	Set the local ID to identify the identity of the local device for the remote device to verify its legitimacy.

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

PFS Group	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.

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

VPN > Add OpenVPN®

Type: ☐ OpenVPN® Client ☒ OpenVPN® Server

* Name: OpenVPN Server

Status: ☐ 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: ☐

Duplicate client certificates are allowed: ☐

Redirect Gateway: ☒

Cancel Save

VPN – Add OpenVPN® Server

Type	Select the OpenVPN®: Client or Server
Name	Enter a name for the OpenVPN® server.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Server. <i>Note: Once disabled, the OpenVPN® service will also be disabled.</i>
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. <i>The default protocol is UDP.</i>
Router	Select from the drop-down list the router/device group that this VPN will be using.
Interface	Select from the drop-down list the exact interface of the router/device group.
Local Port	Configure the listening port for OpenVPN® server. <i>The default value is 1194.</i>
Authentication Mode	Choose the server mode the OpenVPN® server will operate with. 4 modes are available:

	<ul style="list-style-type: none"> ● SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). ● User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). ● SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. ● PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
TLS Identity Authentication	<p>This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers.</p> <p>This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.</p>
TLS Identity Authentication Direction	Select from the drop-down list the direction of TLS Identity Authentication, three options are available (Server, Client or Both).
TLS Pre-Shared Key	If TLS Identity Authentication is enabled, enter the TLS Pre-Shared Key.
Duplicate client certificates are allowed	Click on " ON " to allow duplicate Client Certificates
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
Push Routes	<p>Specify route(s) to be pushed to all clients.</p> <p><i>Example: 10.0.0.1/8</i></p>
LZO Compression Algorithm	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificate	Select a generated CA from the dropdown list or add one.
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.
IPv4 Tunnel Network/Mask Length	<p>Enter the network range that the GWN70xx will be serving from to the OpenVPN® client.</p> <p><i>Note: The network format should be the following 10.0.10.0/16.</i></p> <p><i>The mask should be at least 16 bits.</i></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®: Client or Server
Name	Enter a name for the OpenVPN® Client.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Client. <i>Note: Once disabled, the associated VPN services will also be disabled.</i>
Protocol	Specify the transport protocol used. <ul style="list-style-type: none"> • UDP • TCP Note: 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"> • SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). • User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). • SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.

	<ul style="list-style-type: none"> ● PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	<p>Choose the encryption algorithm. The encryption algorithms supported are:</p> <ul style="list-style-type: none"> ● DES-CBC ● RC2-CBC ● DES-EDE-CBC ● DES-EDE3-CBC ● DESX-CBC ● BF-CBC ● RC2-40-CBC ● CAST5-CBC ● RC2-64-CBC ● AES-128-CBC ● AES-192-CBC ● AES-256-CBC ● SEED-CBC
Digest Algorithm	<p>Select the digest algorithm. The digest algorithms supported are:</p> <ul style="list-style-type: none"> ● MD5 ● RSA-MD5 ● SHA1 ● RSA-SHA1 ● DSA-SHA1-old ● DSA-SHA1 ● RSA-SHA1-2 ● DSA ● RIPEMD160 ● RSA-RIPEMD160 ● MD4 ● RSA-MD4 ● ecdsa-with-SHA1 ● RSA-SHA256 ● RSA-SHA384 ● RSA-SHA512 ● RSA-SHA224 ● SHA256 ● SHA384 ● SHA512 ● SHA224 ● whirlpool
TLS Identity Authentication	Enable TLS identity authentication direction.
TLS Identity Authentication Direction	<p>Select the identity authentication direction.</p> <ul style="list-style-type: none"> ● Server: Identity authentication is performed on the server side. ● Client: Identity authentication is performed on the client side. ● Both: Identity authentication is performed on both sides.
TLS Pre-Shared Key	Enter the TLS pre-shared key.
Routes	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
Deny Server Push Routes	If enabled, client will ignore routes pushed by the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on

	behalf of other machines.
LZO Compression	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no. LZO encoding provides a very high compression ratio with good performance. LZO encoding works especially well for CHAR and VARCHAR columns that store very long character strings.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificates	Click on “Upload” and select the CA certificate Note: This can be generated in System Settings → Certificates → CA Certificate
Client Certificate	Click on “Upload” and select the Client Certificate. Note: This can be generated in System Settings → Certificates → Certificate

VPN – Add OpenVPN® Client

VPN User

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

The screenshot shows the 'Add VPN User' configuration window. The 'Server Type' section has two radio buttons: 'PPTP' and 'OpenVPN®', with 'OpenVPN®' being selected and highlighted by a red box. Other fields include 'Name' (VPN User), 'Status' (toggle on), 'Server' (OpenVPN Server), 'Username' (OpenVPN_User1), 'Password' (P@ssW0rd), 'Client Subnet' (192.168.2.0 / 24), and 'Client Certificate' (Client Cert). The form also features an 'Add New Item' button with a plus icon and 'Cancel' and 'Save' buttons at the bottom.

VPN – Add VPN User

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

Client Subnet	Set the IP address and mask length of the subnet for the client to access. Please enter an IP address or subnet (e.g., 192.168.2.0/24)
Only if OpenVPN® is selected	
Client Certificate	Select from the drop-down list the client certificate.

VPN – Add VPN User

WireGuard®

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

GDMS Networking 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/TGqE9kGFIsxyY0BaoblCOZIWO30=
[Copy](#)

* MTU

1420

Cancel

Save

VPN – Add WireGuard®

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

	Click on " Copy " text to copy the public key.
MTU	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.

VPN – Add WireGuard®

Traffic Management

On this page, the user 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.

GDMS Networking 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.

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

+ Add

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

Static Routes

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

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

GDMS Networking 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									
<div> Static Routes <div>+ Add</div> </div>									
<div> IPv4 Static Route IPv6 Static Route </div>									
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	 	
<div> Policy Route <div>+ Add</div> </div>									
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"> ● All ● TCP ● UDP ● TCP/UDP ● ICMP
Router	Select from the drop-down list the router or the device group <i>Note: for device groups, only router group is supported</i>
Source Group	Select the source group from the drop-down list
Source IP Address/Mask Length	Set the source IP address and mask length of the packet to be matched. Please enter an IP address or subnet (e.g., 192.168.122.0/24)

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

Add Policy Route

Firewall and Security

The **Firewall & Security** page combines all configurations related to security and traffic control. It is divided into six main sections:

- Port Forwarding
- Wired Firewall Rules
- Wireless Firewall Rules
- Rogue AP
- Security Defense
- Advanced Security Settings

Click on any section to expand the list of rules or click the **Add** button to create a new configuration.



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:

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

Port Forwarding

Wired Firewall Rules

Wired Firewall Rules allow administrators to control traffic through the GWN devices using various rule types. Administrators can define rules to allow, deny, drop, or manipulate traffic based on source/destination, protocol, port, and more. These rules are essential for managing inbound and outbound network security and routing behavior.

To configure Wired Firewall Rules, navigate to:

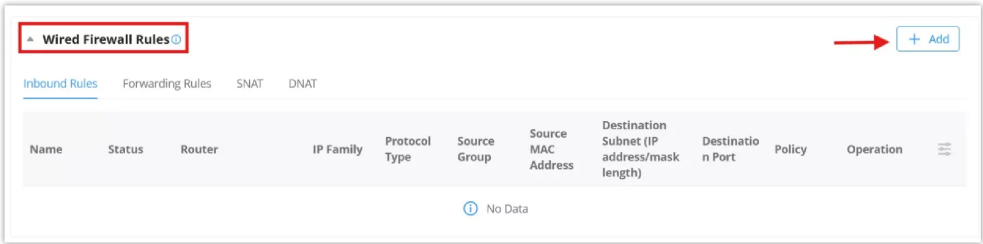
Web UI → Settings → Firewall & Security → Wired Firewall Rules tab

Four rule types are supported:

- **Inbound Rules** – Control incoming traffic to the network
- **Forwarding Rules** – Define how traffic is passed across network interfaces

- **SNAT Rules** – Rewrite the source address for outgoing packets
- **DNAT Rules** – Rewrite the destination address for incoming packets

Click the **+ Add** button to configure a new rule.



Wired Firewall Rules

Note:
Wired firewall rules apply only to Routers.

Inbound Rules

Inbound Rules control traffic entering the router from external networks. These rules are typically used to allow or restrict access to services hosted within the internal network.

You can define rules based on:

- Source group, MAC, IP, port
- Destination IP and port
- Protocol type
- Router and IP family (IPv4/IPv6)
- Action to take: Accept, Reject, or Drop

Firewall & Security > **Add Wired Firewall Rules**

Type

☒ Inbound Rules

☐ Forwarding Rules

☐ SNAT

☐ DNAT

* Name

Inbound Rule

1-64 characters

Status

☒

IP Family

☐ Any

☒ IPv4

☐ IPv6

* Protocol Type

UDP

* Router

Select Router/Group

* Source Group

Select

Source MAC Address

Source IP Address/Mask Length

/

Source Port

1-65535 numbers

Destination IP Address/Mask length

/

Destination Port

1-65535 numbers

Action

☒ Accept

☐ Reject

☐ Drop

Add Inbound Rule

Field	Description
Type	Select the type of firewall rule. For this setup, choose 'Inbound Rules'.

Name	Enter a descriptive name for the rule (1–64 characters). Example: Inbound Rule.
Status	Toggle this switch to enable or disable the rule.
IP Family	Choose the IP version to match traffic: Any, IPv4, or IPv6.
Protocol Type	Select the protocol to filter traffic. Options: TCP, UDP, UDP/TCP, ICMP, IGMP, ALL.
Router	Select a router group. Only router groups are supported for rule application.
Source Group	Choose the WAN or VLAN group where traffic originates from.
Source MAC Address	Optionally define a MAC address to narrow the rule scope. Leave blank for all MACs.
Source IP Address/Mask Length	Specify the originating IP or subnet. Example: 192.168.122.0/24.
Source Port	Optional. Use commas for multiple ports or ranges. Example: 4, 5-10.
Destination IP Address/Mask Length	Define where traffic is headed. Example: 192.168.1.0/24.
Destination Port	Optional. Use commas for multiple ports or ranges. Example: 80, 1000-2000.
Action	Choose how to treat matching traffic: - Accept: Allow - Reject: Deny with response - Drop: Deny silently

Add Inbound Rule

Forwarding Rules

Forwarding Rules define how traffic is relayed across internal interfaces. These are typically used to manage routing decisions between LAN segments or VLANs within the network.

Firewall & Security > Add Wired Firewall Rules

Type

☐ Inbound Rules

☒ Forwarding Rules

☐ SNAT

☐ DNAT

*Name

1-64 characters

Status

☒

IP Family

☒ Any

☐ IPv4

☐ IPv6

*Protocol Type

UDP

*Router

Select Router/Group

*Source Group

Select

Source MAC Address

Source IP Address/Mask Length

/

Source Port

1-65535 numbers

*Destination Group

Destination IP Address/Mask length

/

Destination Port

1-65535 numbers

Action

☒ Accept

☐ Reject

☐ Drop

Add Forwarding Rule

Field	Description
-------	-------------

Type	Select the type of the firewall rule. In this case, 'Forwarding Rules'.
Name	Enter a name to identify the forwarding rule (1–64 characters).
Status	Toggle the rule on or off.
IP Family	Select the IP version: IPv4, IPv6, or Any.
Protocol Type	Choose the type of traffic to control: TCP, UDP, UDP/TCP, ICMP, IGMP, or ALL.
Router	Select the router or router group this rule applies to (only router groups are supported).
Source Group	Select a source group such as a WAN or VLAN. If set to 'All', more specific rules take priority.
Source MAC Address	Optionally specify a source MAC address to match.
Source IP Address/Mask Length	Define the source IP or subnet (e.g., 192.168.122.0/24).
Source Port	Specify individual ports or ranges using commas (e.g., '4, 5-10').
Destination Group	Required: Select the destination group, such as WAN or VLAN.
Destination IP Address/Mask Length	Set the IP/subnet range targeted by the rule (e.g., 192.168.122.0/24).
Destination Port	Specify destination ports or ranges (e.g., '80, 1000-2000').
Action	Choose how to handle matching traffic: Accept (allow), Reject (deny with response), or Drop (silently discard).

Add Forwarding Rule

SNAT (Source NAT) Rules

SNAT Rules allow the router to rewrite the **source IP address** of outbound packets. This is typically used for hiding internal IP addresses behind a public IP when accessing external services.

Key configuration points include:

- Source IP and rewrite source IP
- Source and destination port mapping
- Destination group

SNAT ensures that return traffic can be routed correctly back to the originating device by modifying the source IP.

Firewall & Security > **Add Wired Firewall Rules**

Type ☐ Inbound Rules ☐ Forwarding Rules ☒ **SNAT**
☐ DNAT

* Name 1-64 characters

Status ☒

IP Family ☒ IPv4

* Protocol Type

* Router

* Source IP Address/Mask Length /

* Rewrite Source IP Address

Source Port 1-65535 numbers

Rewrite Source Port 1-65535 numbers

* Destination Group

Destination IP Address/Mask length /

Destination Port 1-65535 numbers

Add SNAT

Field	Description
Name	Enter a name for the SNAT rule (1–64 characters).
Status	Toggle to enable or disable the SNAT rule.
IP Family	Select IPv4 (currently the only supported type).
Protocol Type	Choose the applicable protocol: TCP, UDP, UDP/TCP, ICMP, IGMP, or ALL.
Router	Select the router or router group the rule applies to. Only router groups are supported.
Source IP Address/Mask Length	Specify the original source IP or subnet of the outgoing traffic (e.g., 192.168.1.0/24).
Rewrite Source IP Address	Enter the new IP address that will replace the original source IP.
Source Port	Optionally define the original source port(s) or port range(s), comma-separated (e.g., 80, 1000-2000).
Rewrite Source Port	Optionally enter the new source port(s) that should replace the original ones.
Destination Group	Select the destination group (WAN/VLAN).
Destination IP Address/Mask length	Optionally define the destination IP or subnet for filtering purposes (e.g., 10.1.1.0/24).
Destination Port	Optionally enter destination ports or port ranges to apply SNAT only to certain services.

Add SNAT

DNAT (Destination NAT) Rules

DNAT Rules allow the router to rewrite the **destination IP address** of incoming traffic. This is commonly used for port forwarding to internal hosts.

You can configure:

- Source conditions (group, IP, port)
- Destination group and IP
- Rewrite destination IP

DNAT is essential for exposing internal services to the outside world while preserving internal addressing.

Firewall & Security > Add Wired Firewall Rules

Type

Inbound Rules

DNAT

Forwarding Rules

SNAT

*Name

1-64 characters

Status

IP Family

IPv4

*Protocol Type

UDP/TCP

*Router

Select Router/Group

*Source Group

Select

Source IP Address/Mask Length

/

Source Port

1-65535 numbers

*Destination Group

Select

Destination IP Address/Mask length

/

*Rewrite Destination IP Address

Destination Port

1-65535 numbers

Rewrite Destination Port

1-65535 numbers

NAT Reflection

NAT Reflection Source

Internal

External

Add DNAT

Field	Description
Type	Select DNAT to configure destination network address translation.
Name	Enter a name for the DNAT rule (1–64 characters).
Status	Toggle to enable or disable this rule.
IP Family	Select IPv4 for DNAT rules (IPv6 is not supported for this rule type).
Protocol Type	Choose the protocol to match traffic (e.g., TCP, UDP, UDP/TCP, ICMP, IGMP, ALL).
Router	Select the router or router group where this rule will apply.
Source Group	Select the source group (WAN or VLAN) for matching incoming traffic.
Source IP Address/Mask Length	Enter source IP or subnet to match (e.g., 192.168.1.0/24).
Source Port	Define the original port or port range for the match (e.g., 80, 8000-8080).
Destination Group	Choose the destination group (WAN or VLAN).

Destination IP Address/Mask length	Specify the original destination IP address or subnet to match.
Rewrite Destination IP Address	Enter the internal IP to which the traffic will be redirected.
Destination Port	Original port(s) for matching the destination (e.g., 443, 1000-2000).
Rewrite Destination Port	Enter the new port(s) for redirecting the matched traffic.
NAT Reflection	Toggle to enable NAT reflection (loopback) for internal access via external IP.
NAT Reflection Source	Choose whether the NAT reflection source is 'Internal' or 'External'.

Add DNAT

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.

The screenshot displays the 'Add Wireless Firewall Rules' interface. It features two rule configurations. The first rule is an 'Inbound Rule' with a 'Deny' policy, targeting a 'Particular Network' with IP address 192.168.80.0 and subnet 255.255.255.0. The second rule is an 'Outbound Rule' with a 'Permit' policy, targeting 'All' destinations. A green arrow points from the 'Outbound Rules' radio button in the first rule to the 'Outbound Rules' radio button in the second rule. A green box highlights the second rule configuration, which also includes an 'SSID' field set to 'EMEA'.

Add Wireless Firewall Rules

Type	Select the type of the firewall rule: Inbound rules or Outbound rules
Name	Enter a name for the wireless firewall rule.
Service Protocol	Select the Service protocol type from the drop-down list.
Policy	<ul style="list-style-type: none"> ● Permit: Traffic from clients will be allowed. ● Deny: Traffic from clients will be denied.

Source	Select the source, it can be from a Particular IP or Network then enter the IP and/or the subnet. <i>Note: this option is only available when the type selected is Inbound rules.</i>
Destination	Select the destination, it can be from a Particular IP, Network or Domain. then enter the IP/Domain and/or the subnet.
SSID	If All is selected, this rule will also be applied to new SSIDs (Wireless LAN). <i>Note: this option is only available when the type selected is Outbound rules!</i>

Add Wireless Firewall Rules

Rogue AP

GDMS Networking 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.

The screenshot shows the 'Rogue AP' configuration page under 'Firewall & Security'. The 'Enable Rogue AP Detection' toggle is turned on. The 'Detect Range' is set to 'All Channels'. The 'Countermeasure Level' is set to 'Medium'. The 'Containment Range' is set to 'Same Channel'. The 'Sub-string for Spoofing SSID' has three entries: 'Grand', 'Stream', and 'EMEA'. There are also fields for 'Trusted AP' and 'Untrusted AP' MAC addresses, each with an 'Add New Item' button.

Rogue AP

Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect Range	Specify the rogue AP detect range. <ul style="list-style-type: none"> ● Same Channel: AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication. ● All channels: AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt. <i>Default is Same Channel.</i>
Countermeasure Level	Countermeasures level specifies the type of attacks which will be suspected by the AP. Select different levels: <ul style="list-style-type: none"> ● High: Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. ● Medium: Untrusted BSSID, Illegal access without authentication, Illegal access.

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

Rogue AP

Security Defense

The Defense Configuration features under Firewall & Security enhance the security posture of GDMS Networking-managed devices by providing protection against common network attacks such as DoS (Denial of Service), Flooding, Port Scanning, and Spoofing.

These settings allow administrators to fine-tune real-time defense behavior with flexible thresholds and control mechanisms to mitigate malicious traffic and spoofing attempts before they affect network performance or availability.

Navigate to: **Settings** → **Firewall & Security** → **Security Defense**

Basic Attack Defense

The **Basic Attack Defense** tab allows enabling protection against several types of network flood and scan attacks, with options to configure exception rules by IP address and set custom blocking thresholds and durations.

The screenshot shows the 'Firewall & Security' settings page with the 'Basic Attack Defense' tab selected. The 'Basic Attack Defense' toggle is turned on. Below it, there is an 'IP Exception' section with a dropdown menu set to 'IP Address' and an 'Add New Item' button. The 'Flood Attack Defense' section contains a table with four rows: SYN Flood Attack Defense, UDP Flood Attack Defense, ICMP Flood Attack Defense, and ACK Flood Attack Defense. Each row has a status toggle (all are on), a blocking threshold in pps, and a blocking duration in seconds. The 'Scan Attack Defense' section has a 'Port Scan Defense' row with a status toggle (on), a blocking threshold in packets/m, and a blocking duration in seconds. The 'Abnormal Packet Attack Defense' section has a 'Select what you want to defend' section with checkboxes for IP Option, TCP Flag, Land, Smurf, Fraggle, Ping of Death, Trace Route, IP Fragment, Unassigned Protocol Numbers, SMAC=DMAC, and Large ICMP Packet Control.

Status	Blocking Threshold (pps)	Blocking Duration (s)
SYN Flood Attack Defense	2000	300
UDP Flood Attack Defense	5000	300
ICMP Flood Attack Defense	250	300
ACK Flood Attack Defense	2000	300

Status	Blocking Threshold (packets/m)	Blocking Duration (s)
Port Scan Defense	50	100

Select what you want to defend

☒ IP Option
 ☒ TCP Flag
 ☒ Land
 ☐ Smurf
 ☐ Fraggle
 ☐ Ping of Death
 ☐ Trace Route
 ☐ IP Fragment
 ☐ Unassigned Protocol Numbers
 ☐ SMAC=DMAC
 ☐ Large ICMP Packet Control

Basic Attack Defense

Main Controls

- **Basic Attack Defense:** Enables or disables all attack defense features globally.
- **IP Exception:** Allows specific IP addresses to bypass defense rules.

Flood Attack Defense Types

- **SYN Flood Attack Defense:** Blocks excessive TCP SYN requests, commonly used in DoS attacks.
- **UDP Flood Attack Defense:** Blocks high volumes of UDP traffic.
- **ICMP Flood Attack Defense:** Protects against excessive ICMP ping requests.
- **ACK Flood Attack Defense:** Detects and blocks suspicious TCP ACK packet floods.

Each rule includes:

- **Status Toggle:** Enable or disable defense.
- **Blocking Threshold (pps):** Packets per second allowed before triggering the block.
- **Blocking Duration (s):** Duration in seconds that traffic is blocked after threshold is exceeded.

Scan Attack Defense

- **Port Scan Defense:** Detects and blocks traffic patterns that indicate port scanning activity.
 - **Blocking Threshold (packets/m):** Limit of packets per minute.
 - **Blocking Duration (s):** Block time after detection.

Abnormal Packet Attack Defense

Enables blocking for specific unusual or malformed packet types. Checkboxes allow you to selectively enable protection for:

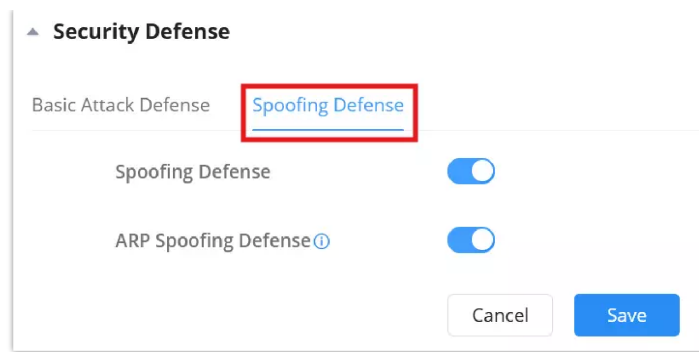
- IP Option
- TCP Flag
- Land Attack
- Smurf
- Fraggle
- Ping of Death
- Trace Route
- IP Fragment
- Unassigned Protocol Numbers
- SMAC=DMAC
- Large ICMP Packet Control

Spoofing Defense

The **Spoofing Defense** tab provides advanced protection against address spoofing threats, such as forged IP or MAC addresses used to disguise malicious actors on the network.

Features:

- **Spoofing Defense:** General toggle to enable spoofing countermeasures.
- **ARP Spoofing Defense:** Prevents manipulation of ARP responses to poison network address resolution.



Spoofing Defense

How it works:

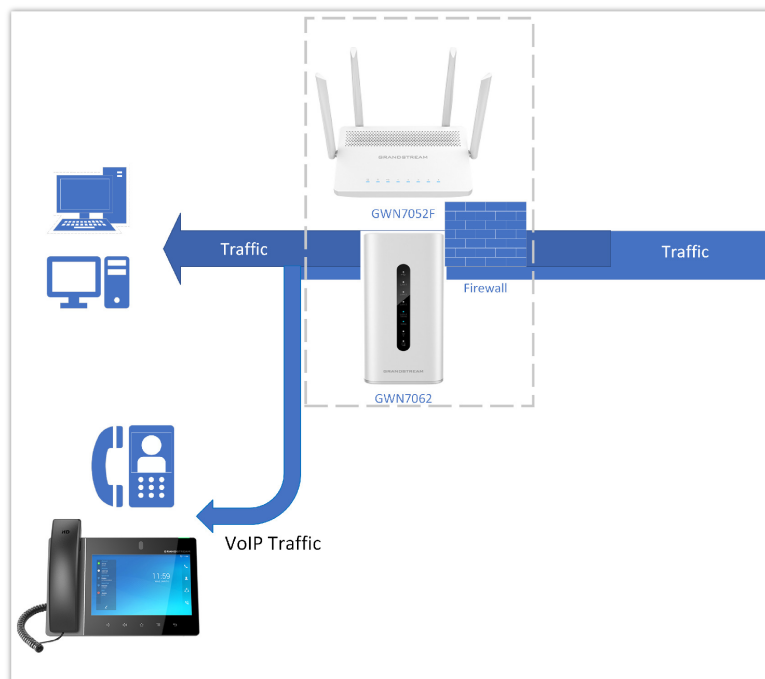
When enabled, GDMS verifies the consistency of the source and destination MAC addresses in the Ethernet frame and ARP header. If mismatches are detected, the ARP packets are discarded to protect against spoofing and ARP poisoning. Additionally, VRRP MAC addresses will not be added to the ARP table when this feature is active.

Notes:

- All defense rules are device-level settings managed through GDMS Networking and must be configured per network needs.
- Thresholds should be carefully set to balance security and network stability.
- These defense mechanisms are especially valuable for public-facing networks or deployments with heightened security requirements.

Application Layer Gateway (ALG)

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



Application Layer Gateway

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

ALG

PROFILES

Portal policy

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

Add Portal Policy

Internal Splash Page

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

Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, Internal or External. <i>Note: this table is only about internal splash page.</i>

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

External Splash page

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

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

- **Protocol Id:** input related services agreement No.

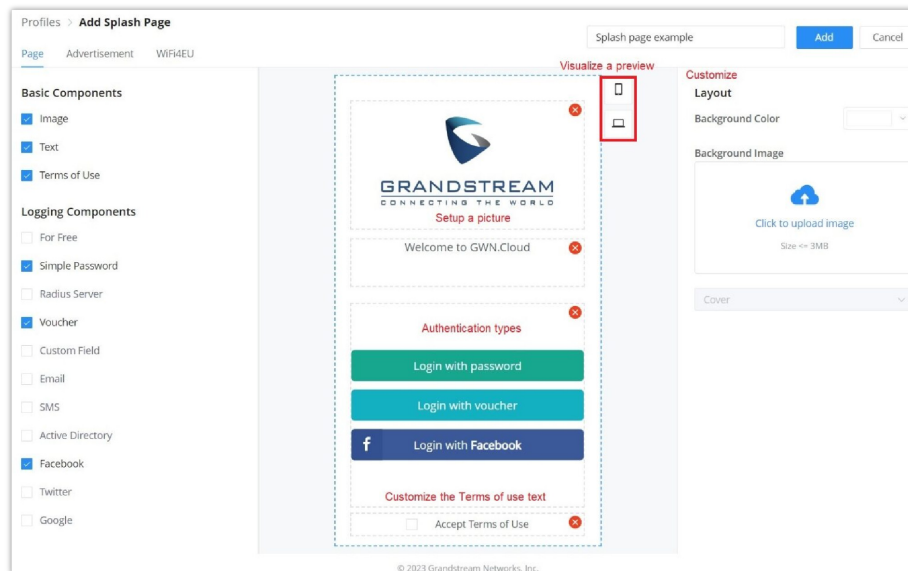
Portal Policy – External Splash Page

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.



Add Splash Page

Users can set the following:

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

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

Facebook	Authentication using Facebook account.
Twitter	Authentication using Twitter account.
Google	Authentication using Google account.

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.

Profiles > **Add Splash Page**

Splash page example Add Cancel

Page Advertisement **WiFi4EU**

WiFi4EU ☒

Once enabled, the top area of the splash page will display the information about WiFi4EU.

Language

English

* Network UUID

Networkuuid

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).

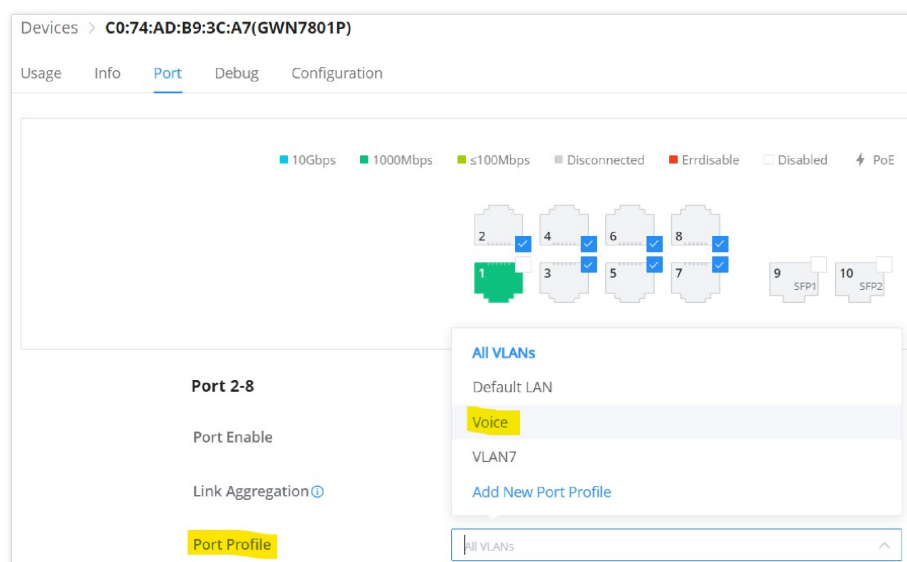
Voice VLAN	Toggle ON or OFF Voice VLAN. <i>Note: Please first enable the Voice VLAN in the Global LAN Settings.</i>
Rate	Specify the rate (port speed) from the drop-down list.
Duplex Mode	Select the duplex mode: <ul style="list-style-type: none"> ● Auto-negotiation: The duplex status of an interface is determined by auto-negotiation between the local port and the peer port. ● Full-duplex: Force full-duplex, and the interface allows sending and receiving data packets at the same time. ● Half duplex: Force half duplex, and the interface only send or receive packets at a time.
Flow Control	When enabled, if congestion occurs on the local device, the device sends a message to the peer device to notify it to stop sending packets temporarily. After receiving the message, the peer device stops sending packets to the local device. <i>Note: When duplex mode is "Half-duplex", the traffic control does not take effect.</i>
Enable Port STP	Toggle ON or OFF the Port STP.
Incoming Speed Limit	Toggle ON or OFF the incoming speed limit.
CIR (Kbps)	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
Outbound Speed Limit	Toggle ON or OFF the outbound speed limit.
CIR (Kbps)	Configures the Committed Information Rate, which is the average rate of the traffic to pass through.
LLDP-MED	Toggle ON or OFF the LLDP-MED.
Network Policy TLV	Toggle ON or OFF the network policy TLV.
Security	
Storm Control	Toggle ON or OFF storm control.
Broadcast	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
Unknown Multicast	Toggle ON or OFF Broadcast and then specify the control threshold (pps = packet per second).
Unknown Unicast	Toggle ON or OFF Unknown Unicast and then specify the control threshold (pps = packet per second).
Port Isolation	Toggle ON or OFF port isolation.
Port Security	Toggle ON or OFF port security. <i>Note: after enabled, start MAC address learning including the dynamic and static MAC addresses.</i>
Maximum number of MACs	Specify the maximum number of MAC addresses allowed. <i>Note: after the maximum number is reached, if a packet with a non-existing source MAC address is received, regardless of whether the destination MAC address exists or not, the switch will consider that there is an attack from an illegal user; and will protect the interface according to the port protection configuration.</i>
Sticky MAC	Toggle ON or OFF Sticky MAC. <i>Note: after enabled, the interface will convert the learned secure dynamic MAC address into Sticky MAC. If the maximum number of MAC addresses has been reached, the MAC addresses in the non-</i>

	<i>sticky MAC entries learned by the interface will be discarded, and whether to report a Trap alert is determined according to the port protection configuration.</i>
802.1X Authentication	Toggle ON or OFF 802.1x authentication.
User Authentication Mode	<p>Select the user authentication mode from the drop-down list</p> <ul style="list-style-type: none"> • Mac-based: allows multiple users to authenticate without affecting each other; • Port-based: allows multiple users to be authenticated. As long as one user passes the authentication, other users are exempt from authentication.
Method	Select the method from the drop-down list.
Guest VLAN	<p>Toggle Guest VLAN ON or OFF.</p> <p><i>Note: Enable the Guest VLAN in the Global LAN Settings first.</i></p>
Port Control	<p>Select the port control from the drop-down list:</p> <ul style="list-style-type: none"> • Disabled • Mandatory authentication • Mandatory non-authentication • Automatic
Re-authentication	Configures whether to enable re-authentication for the device connected to the port.

Add port profile

Once the Port profile is added 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 MAC Group feature in GDMS Networking allows administrators to define and manage groups of MAC addresses for use in authentication and access control policies across APs, routers, and switches. This centralized approach helps streamline the configuration of MAC-based authentication and improves consistency across the network.

You can assign a MAC Group to SSID settings, switch port policies, and access lists for granular client control. Each MAC Group can include multiple MAC address entries, each representing an individual device.

Navigation: Go to *Settings* → *Profiles* → *MAC Groups*

Create a MAC Group

To create a new MAC Group:

1. Click Add on the MAC Group page.
2. Enter a Group Name.
3. Add MAC addresses to the list using the Add MAC button.
4. Optionally, use the CSV import function for bulk entry.
5. Click Save.

Add MAC Groups [X]

Manual Import

***Name**
Supports 1-64 characters

MAC
Enter Client Name (Optional)

: : : : : [Red Minus]

Add New Item [Green Plus]

Cancel Add

Add MAC Groups

MAC Groups can be applied in various contexts depending on the device type, here are some examples:

For Access Points (GWN APs), MAC Groups can be selected under SSID settings using the MAC Authentication field ([Blocklist](#)). This allows or denies client access based on the MAC address.

For Switches (GWN78XX), MAC Groups can now be applied directly to port policies through MAC Authentication.

For Routers, MAC Groups may be referenced in various policy rules (depending on model and use-case), allowing consistent centralized access control across device types.

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 excuted.)

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	5Auu25GcsNLC52nZ	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.

PPSK Import CSV file

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

PPSK group – Access Security

Exporting PPSK Entries

Administrators can now easily export all PPSK entries within a PPSK group for backup, audit, or sharing purposes.

To export PPSKs:

1. Navigate to Settings → Profiles → PPSK
2. Locate the PPSK group you want to export
3. Click the **Download** icon in the **Operation** column

This will download a CSV file containing all configured PPSKs, including key assignments and user labels (if defined).

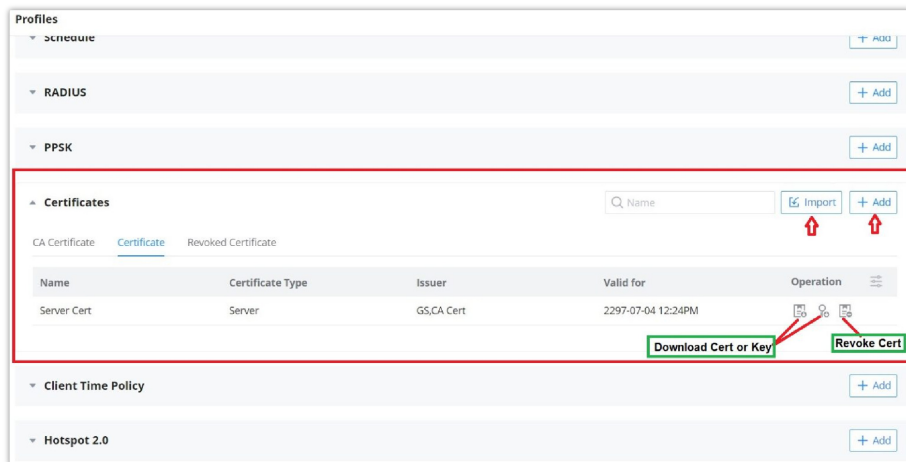
PPSK			
Q Name			+ Add
Name	Associated SSID	PPSKs Number	Operation
vb	—	2	⚙️ ⬇️ 🗑️
Test	—	1	⚙️ ⬇️ 🗑️

Exporting PPSK Entries

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 GDMS Networking or GWN Manager.



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

Digest Algorithm

* Expiration (D)

SAN ☒ None ☐ IP Address ☐ Domain

Country/Region

* State/Province

* City

* Organization

* Organizational Unit

* Email

Profiles – Add CA Certificate

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

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

Profiles – Add CA Certificate

Profiles > Add Certificate

Type
☐ CA Certificate
☒ Certificate

* Name

* CA Certificate

Certificate Type
☒ Server
☐ Client

Key Length

Digest Algorithm

* Expiration (D)

SAN
☒ None
☐ IP Address
☐ Domain

Country/Region

* State/Province

* City

* Organization

* Organizational Unit

* Email

Profiles – Add Certificate (Client or Server)

Type	Select the type of certificate either CA Certificate or Certificate .
Name	Enter the certificate's name.
CA Certificate	Select from the drop-down list the CA Certificate previously created.

Certificate Type	Select the certificate type either a server or a client certificate.
Key Length	<p>Choose the key length for generating the CA certificate. The following values are available:</p> <ul style="list-style-type: none"> ● 2048: 2048-bit keys are a good minimum. (Recommended). ● 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	<p>Select the digest algorithm.</p> <ul style="list-style-type: none"> ● SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. <p>Note: Hash is a one-way function, it cannot be decrypted back.</p>
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country/Region	Select a country from the dropdown list of countries. Example: "United States of America".
State/Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Profiles – Add Certificate (Client or Server)

Client Time Policy

The administrator can configure a Time policy 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

0

* HESSID ⓘ

Network Access

☒ Internet Access

Network Type

Private Network ▾

IPv4 Type

Address Type Not Available ▾

IPv6 Type

Address Type not Available ▾

Network Auth Type ⓘ

Not Configured ▾

Venue ▾

Operator Name ▾

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 ⓘ

Morocco(المغرب) ▾

Timezone

(GMT) Casablanca, Monrovia ▾

Auto Sync Time ⓘ

* AP Login Password ⓘ

..... > <

Device Password ⓘ

> <

LED

Always on ▾

Reboot Schedule

None ▾

Enable Client Connection Event

Subscribe to Client Historical Data ⓘ

Presence API ⓘ

Once enabled, if no API requests have been received for more than 1 week, it will be automatically disabled

Bluetooth API ⓘ

Automatically add to SSIDs ⓘ

System page – General

Country/Region	Select the country or region from the drop-down list. This can affect the number of channels depending on the country standards.
Timezone	Configure time zone for GWN APs. Please reboot the device to take effect.
Auto Sync Time	If enabled, all managed devices' system times will be synced with GWN Cloud
AP Login Password	Sets the APs login password with up to 8 characters. Alphanumeric characters and special characters - _ are supported
Device Password	Set the devices SSH remote login password other than APs (Routers and Switches), which is also the device web login password.
LED	Select whether to always turn ON or OFF the LEDs on the APs or apply a schedule for this function.
Reboot Schedule	Once scheduled, the current network will not work for a while during the scheduled period.
Enable Client Connection Event	When enabled, then Client connects/disconnects events are listed under Devices → GWN device → Info page.
Subscribe to Client Historical Data	Enabling collect the data of historical bandwidth usage for all clients in the network. <i>Note: this will cause the storage usage increase.</i>
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.

Bluetooth API	When enabled, Bluetooth client information detected near select Wi-Fi-enabled APs will be automatically collected. See API details for more information.
Automatically add to SSIDs	If enabled, newly added GWN APs and wireless routers will be automatically provisioned for all SSIDs.

System page – General

URL Access Log

The URL Access Log section allows administrators to configure how client browsing activity logs are stored, grouped, and exported. This feature helps with traffic analysis, domain grouping, and scheduled email reporting of access logs. Logs can be stored on the GDMS server and emailed periodically to designated recipients.

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: navigate to “**Settings → System page → URL Access Log section**” and enable the URL Access Log field.

Refer to the figure and table below for more details:

URL Access Log ^

Log Storage ⓘ

GDMS Server

Export URL Access Log ⓘ

[Export Immediately](#)

Group Metric by Main Domain

Customized Top-level Domain ⓘ

.us.com

+

Add New Item

Email Frequency

Monthly

* URL Log Receiver

admin@gs.com

+

Add New Item

URL Access Log

Field	Description
Log Storage	Select where to store the URL access logs. Options include 'Do not Store' and 'GDMS Server'. When GDMS Server is selected, logs are stored centrally.
If Log Storage is set to GDMS Server	
Export URL Access Log	Toggle to enable or disable exporting of URL access logs. When enabled, a download link is sent based on the configuration.
Export Immediately	Manual trigger to export URL logs immediately when the toggle is enabled.
Group Metric by Main Domain	Toggle to group statistics by the main domain instead of subdomains.
Customized Top-level Domain	Specify custom TLDs to be merged for traffic stats (e.g., .us.com). Default TLDs like .com are merged automatically.

Email Frequency	Set how often the log export link will be sent to the specified recipient(s). Options may include Daily, Weekly, Monthly.
URL Log Receiver	Specify one or more recipient email addresses to receive the exported log reports. Required field.

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 dialog box titled "Export" contains an information icon and the text "Specify the time range of the URL Access Log to be exported." Below this, it says "For the Last" followed by a red asterisk and "1-30 integers". A text input field contains the number "7", and to its right is the label "day(s)". At the bottom are "Cancel" and "Export" buttons.

Export Immediately

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

A small dialog box titled "Export succeed!" with a close button. Below the title is a blue hyperlink that says "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
	AP MAC	MAC	Hostname	User	Source IP	Destination IP	URL	HTTP Method
1			iPhone XS		192.168.5.133	17.253.113.204	http://captive.apple.com/	GET
2			Huawei Mate 20		192.168.5.133	17.167.192.94	https://gsp85-ssl.ls.apple.c	
3			Samsung Galaxy S10		192.168.5.133	81.192.28.179	https://netcts.cdn-apple.co	GET
4			OnePlus 7 Pro		192.168.5.133	17.134.127.250	https://gs-loc.apple.com	
5			Moto G7 Power		192.168.5.133	17.57.12.11	https://gsp64-ssl.ls.apple.c	
6			iPhone 11 Pro Max		192.168.5.133	173.194.76.101	https://s.youtube.com	
7			Google Pixel 4 XL		192.168.5.133	74.125.193.119	https://i.ytimg.com	
8			BlackBerry Key2 LE		192.168.5.133	172.217.18.42	https://youtubei.googleap	
9					192.168.5.133	17.125.249.8	https://p71-buy.itunes.ap	
10								

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.

The screenshot shows the 'System' settings page. The 'URL Access Log' section is expanded. Below it, the 'Guest Information' section is highlighted with a red border. It contains a toggle for 'Email Guest Information' which is turned on, an 'Email Frequency' dropdown set to 'Weekly', and an 'Email Receiver' field with the value 'Admin@grandstream.com'. There is an 'Add New Item' button with a green plus icon. Below the highlighted section are 'NAT Pool', 'SNMP', and 'Syslog' sections, each with a dropdown arrow. At the bottom are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the 'System' settings page. The 'Guest Information' section is expanded. Below it, the 'NAT Pool' section is highlighted with a red border. It contains fields for 'Default Gateway' (10.1.0.1), 'DHCP Server Subnet Mask' (255.255.255.0), 'DHCP Release Time (mins)' (720), 'DHCP Preferred DNS', and 'DHCP Alternate DNS'. A note '2-525600 numbers' is visible next to the release time field. Below the highlighted section are 'SNMP' and 'Syslog' sections, each with a dropdown arrow. At the bottom are 'Cancel' and 'Save' buttons.

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 1-32 characters

SNMPv3 ⓘ ☒

* Username 1-64 characters

Authentication Mode

* Authentication Password 8-32 characters

Privacy Mode ⓘ

* Privacy Password 8-32 characters

Syslog ▾

Cancel Save

SNMP

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

SNMP

Syslog

The **Syslog Capture** section provides flexible options for collecting system logs from selected devices (Access points, Routers, Switches...). Admins can choose between using a **Cloud Syslog Server** managed by GDMS, or a **Local Syslog Server** within their private network. Logs can be filtered by severity, and captures can be scheduled for specific durations and devices.

To enable this feature, follow the below steps: navigate to “**Settings → System page → Syslog section**”.

Refer to the figures and table below for more details:

Syslog ^

Syslog Server

Cloud Syslog Server

Syslog Level

Warning

Syslog Capture Expiration

0 d 0 h 10 min

Devices

C0:74:AD:21:BB:FC x

Client

DESKTOP-AV09UEH(6C... x

Syslog Capture

Capturing... Will stop at 2025/04/04 05:02PM

Stop

Delete

Q MAC

C0:74:AD:21:BB:FC >

Syslog – Cloud Syslog Server

Syslog ^

Syslog Server

Local Syslog Server

Local Syslog Server Address

192.168.5.10

Syslog Level

Warning

Protocol

UDP

Devices

C0:74:AD:21:BB:FC x

Client

DESKTOP-AV09UEH(6C... x

Syslog – Local Syslog Server

Field	Description
If Syslog Server is set to Cloud Syslog Server	
Syslog Server	Select the syslog server mode. Options: 'Cloud Syslog Server' or 'Local Syslog Server'.
Syslog Level	Select the severity of logs to capture. Levels include None, Emergency, Alert, Critical, Error, Warning, Notice, Information.
Syslog Capture Expiration	Set duration (in days, hours, minutes) for capturing logs. Capture will stop automatically upon expiration.
Devices	Select one or more devices (e.g., AP, Router) to capture system logs from. TCP protocol is not supported for switches.
Client	Select a specific client device (by MAC or name) to capture its logs.
Syslog Capture	Click this button to start the syslog capture for the selected duration and devices.
If Syslog Server is set to Local Syslog Server (extra fields)	
Local Syslog Server Address	Enter the IP address of the local syslog server (e.g., 192.168.5.10).

Protocol	Select the protocol (UDP or TCP) used for forwarding logs to the local syslog server.
----------	---

Syslog

ORGANIZATION

Overview

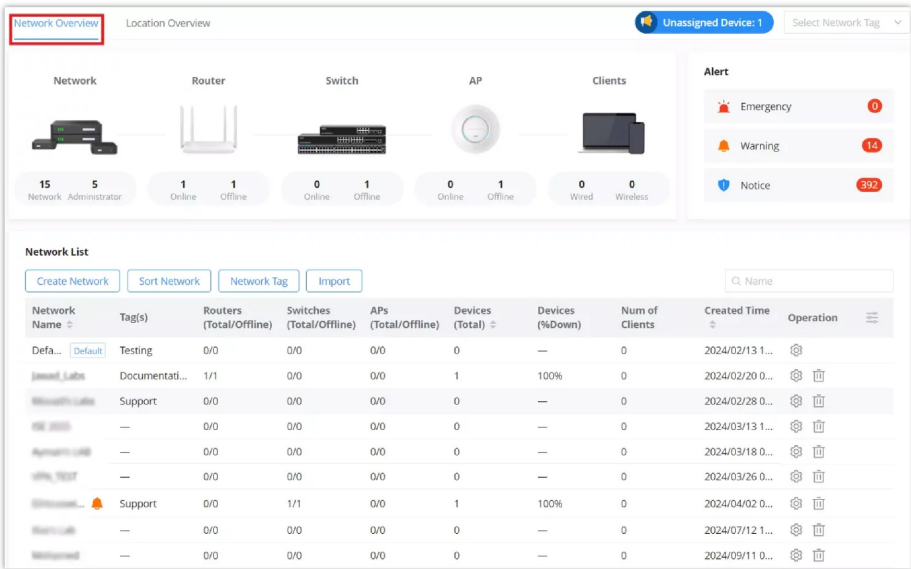
Network Overview

The **Network Overview** page provides a centralized view of all networks created within the GDMS Networking platform. It displays summarized statistics, quick action buttons, and new filtering and management options introduced in recent updates.

- **Top Summary Panel**

At the top of the page, a visual dashboard displays totals for:

- **Networks** and **Administrators**
- Online/offline status of **Routers, Switches, APs (Access Points)**
- Number of **Wired/Wireless Clients**

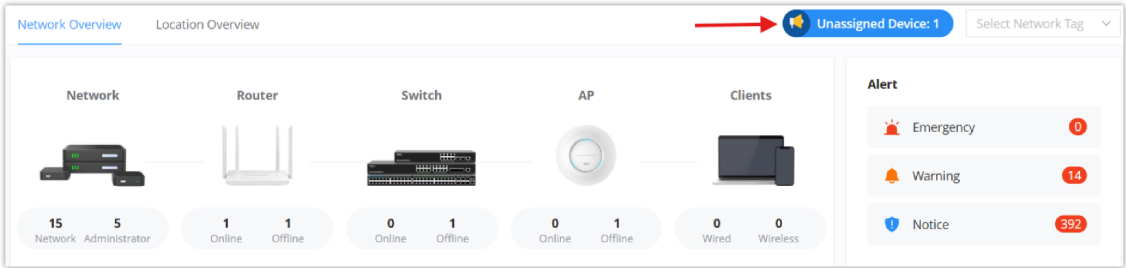


Network Overview page

This high-level overview helps users understand the infrastructure status across all configured networks.

- **Unassigned Devices Indicator**

A blue “**Unassigned Device**” button now appears in the top-right. It shows the number of Grandstream devices added to GDMS Networking that haven’t yet been assigned to any network. Clicking this button redirects you to assign the devices.



Network Overview – Unassigned Devices

- **Network Tags**

Each network can now be labeled with one or more **Network Tags**, which are shown in the **Tag(s)** column.

1. Tags allow users to **filter networks by category or usage**, improving manageability in large deployments.
2. The tag list can be customized by clicking **“Network Tag”** at the top of the Network List.

Network Overview – Manage Network Tags

◦ **Tag-Based Filtering**

A drop-down menu next to the Unassigned Device indicator lets users **filter the Network List by specific tags**, such as “Support”, “Documentation”, or “Testing”. Selecting a tag will only show the networks associated with it.

Network Overview – Tag based filtering

◦ **Creating a Network**

Clicking the **“Create Network”** button opens a form where you can:

- Enter the Network Name, Country/Region, and Time Zone
- Assign Network Administrator(s)
- Optionally set the network as default
- Add **tags** directly during creation

Overview > Create Network

* Network Name ⓘ

Support Team

1-64 characters

* Country/Region

Morocco(المغرب)

▼

* Time Zone

(GMT) Casablanca, Monrovia

▼

Network Administrator

www.support@morocco.support@agribusiness.com

support@agribusiness.com

support@agribusiness.com

Optional Account ▼

Clone Network

Default Network

▼

Default Network

☐ Once enabled, the current network will be set as the default

Tag(s)

Support ×

▼

Cancel

Save

- **Sorting Networks**

The **"Sort Network"** button opens a drag-and-drop interface to adjust the display order of networks in the dropdown list. This improves navigation, especially when managing many networks.

Network Sort

① Hold and drag the network to adjust the display order in the network drop-down box.

Default Network	↑	↓
General_Lab	↑	↓
Microsoft_Lab	↑	↓
10.10.10.1	↑	↓
AgilentLab	↑	↓
VMs_1007	↑	↓
@Houscience_Lab	↑	↓
Basic_Lab	↑	↓
Multimed	↑	↓
Addressable_Lab	↑	↓
Salinas_Network	↑	↓
VMHouscience	↑	↓

Cancel Save

- **Import Functionality**

The **“Import”** button now supports importing multiple types of configuration via `.csv` files:

- Network
- Device
- Device Group
- SSID

Network List

Create Network

Sort Network

Network Tag

Import

Network Name	Tag(s)	Routers (Total/Offline)	Switches (Total/Offline)	Access Points (Total/Offline)	WLANs (Total/Offline)
Default	Testing	0/0	0/0	0/0	0/0
Documentation	Documentation	1/1	0/0	0/0	0/0
Support	Support	0/0	0/0	0/0	0/0
—	—	0/0	0/0	0/0	0/0

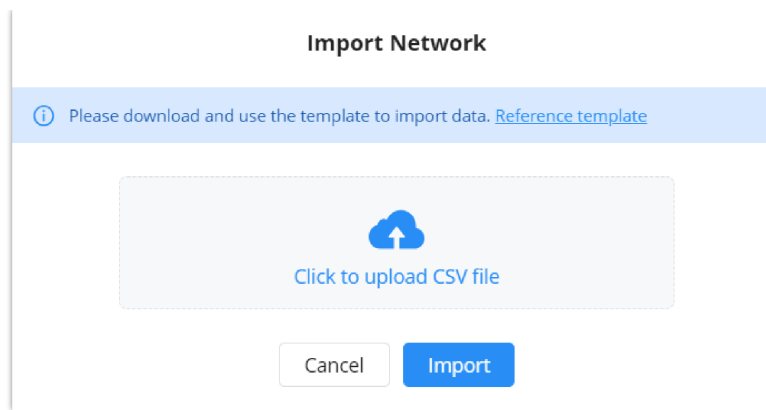
Network

Device

Device Group

SSID

Upon selection, you can download a reference template or upload a CSV file.



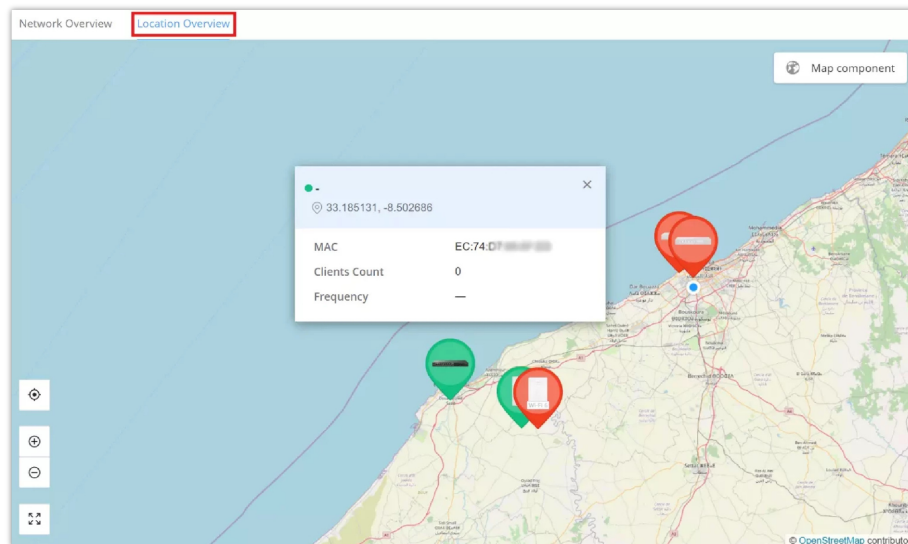
Network Overview – Upload CSV file

Location Overview

The **Location Overview** page provides a real-time geographic visualization of all network devices associated with your GDMS Networking organization. It consolidates device locations across **all networks** into a single interactive map view, offering a high-level operational snapshot.

This view supports device-level status indication, allowing administrators to quickly identify online/offline devices.

To access the Location Overview: Navigate to **Organization** → **Overview** → **Location Overview** tab.



Network Overview – Location Overview

Key Feature: Global Device Visibility

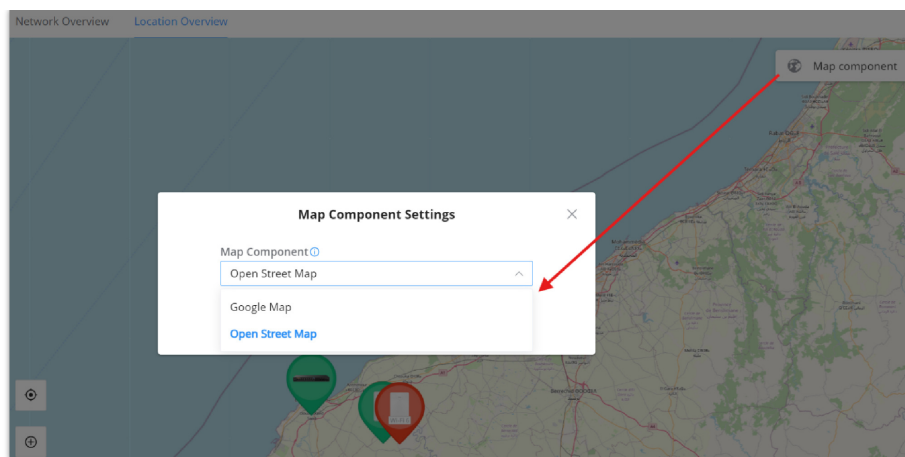
- The Location Overview shows **all devices** from all networks under the organization.
- Devices are represented as map pins:
 - **Green Pins:** Device is online and accessible via GDMS Networking.
 - **Red Pins:** Device is offline or currently unreachable.
- Devices include: Access Points, Routers, Switches, and GCC (Grandstream Cloud Controller) devices.

Note:

While Location Overview displays all devices, new device placement or configuration must be done at the individual network level [map](#).

Map Component Settings:

Users can choose between **Open Street Map** and **Google Map** as the underlying map component.



Location Overview – Map Component Settings

To change the map view:

1. Click on the **“Map Component”** button on the top-right of the map.
2. In the **Map Component Settings** popup, select the desired map type.
 - **Google Map** (requires a valid Google Maps API key)
 - **Open Street Map** (default)

Inventory

The **Inventory** section under **Organization → Inventory** allows users to manage all Grandstream devices registered to their GDMS Networking account.

Devices in the Inventory are claimed meaning they are associated with your organization and **cannot be claimed by another GDMS account**. This protects ownership and prevents duplicate configuration.

Devices can be:

- Claimed directly into the Inventory (without assigning to a network)
- Added directly to a network (which also claims them automatically)
- Removed from networks, but still remain in Inventory
- Deleted only if unassigned from all networks

Note:

Think of Inventory as your virtual device shelf a staging area for devices you own, regardless of whether they’re currently deployed.

Inventory						
Claim Device Assign to Network More			All Status ▾ All Devices ▾ All Models ▾ Q: MAC/Name/Network/Serial			
<input checked="" type="checkbox"/> Device Model	work	Serial Number	Claim Time	Assigned Time	Last Seen	
<input type="checkbox"/> GWN7062	Assign to Associated Company ISP Locking	T78923AA64	2025/04/11 02:50PM	2025/04/11 02:50PM	2025/04/11 04:47PM	
<input type="checkbox"/> GWN7630	Export Delete	259L9UXK52019294	2025/04/11 11:02AM	2025/04/11 11:02AM	2025/04/11 04:47PM	
<input type="checkbox"/> GWN7003		33B07R5648	2025/04/10 05:29PM	2025/04/10 05:29PM	2025/04/11 04:47PM	
<input type="checkbox"/> GWN7813P		20VXV6KP42DFCC94	2025/04/10 05:29PM	2025/04/10 05:29PM	2025/04/11 04:47PM	
<input type="checkbox"/> GWN7624		232SZUN3290B240	2025/04/07 05:42PM	2025/04/07 05:42PM	2025/04/11 04:47PM	
<input checked="" type="checkbox"/> GWN7711P		33C07B6530	2025/04/07 11:46AM	Unassigned Returns from the Jawad...	2025/04/11 04:47PM	
<input type="checkbox"/> GWN7660E		20VXZLGP72F03F94	2025/03/21 11:41AM	2025/03/21 11:41AM	2025/03/26 03:11PM	
Total 7			10/page < 1 >			

Inventory page

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

- **Filtering Options**

To simplify device management, the Inventory view includes multiple filtering tools. These filters help administrators locate devices quickly and perform actions at scale.

Available Filters:

- **Connection Status**
 - **All** devices
 - **Online** only
 - **Offline** only
- **Assignment Status**
 - Devices currently assigned to a network
 - Devices unassigned and available for deployment
- **Device Model**
 - Filter by specific hardware model (e.g., GWN7660, GWN7813P)
- **Search Field**
 - Search by MAC address
 - Device name
 - Serial number
 - Assigned network

These filters can be combined to refine results even further.

Claim Devices or Import

- **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 [X]

Manual Import

* Device MAC Address

c0 : 74 : ad : ff : ff : ff

* Password

To view the Device Label

..... [toggle]

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: [REDACTED]	—	[REDACTED]	2023-10-27 04:11PM	Unassigned	—
3	GWN7624	C0:74:AD: [REDACTED]	—	[REDACTED]	2023-10-27 02:38PM	Unassigned	2023-10-27 04:09PM
4	GWN7813P	C0:74:AD: [REDACTED]	Default	[REDACTED]	2023-10-27 02:16PM	2023-10-27 02:16PM	2023-10-27 03:59PM

Inventory – Export


- **Delete:** to delete a device from 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



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.

Sync from ERP

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							
Sync from ERP Assign to Network Assign to Associated Company Export Reclaim Device Return Device							
All Models	From All	All Status	All associated com	Q. MAC			
Device Model	MAC	Serial Number	Origin	Storage Time	State	Assign to	Operation
GWN7600	C0:74:AD:00:00:03	---	chidaim2@gs.com	22/12/2023 01:29	Returned	chidaim2@gs.com	
UCM6104	00:0B:82:8D:E7:76	21AWLSG308DE776	yxku company1234	28/11/2023 01:40	Unassigned	---	
UCM6104	00:0B:82:8D:E7:74	21AWLSG308DE774	yxku company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8E:6C:C0	24LUMHVG308E6CC0	yxku company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:F9	24LUMHVG308F97F9	yxku company1234	28/11/2023 01:40	Unassigned	---	
UCM6102	00:0B:82:8D:D4:7A	21AWL8LG308DD47A	yxku company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:F8	24LUMHVG308F97F8	yxku company1234	28/11/2023 01:40	Unassigned	---	
UCM6102	00:0B:82:8D:D4:7B	21AWL8LG308DD47B	yxku company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8F:97:FE	24LUMHVG308F97FE	yxku company1234	28/11/2023 01:40	Unassigned	---	
GXP2130	00:0B:82:8E:6C:BB	24LUMHVG308E6CBB	yxku company1234	28/11/2023 01:40	Unassigned	---	
				Total 39	10/page	1 2 3 4 5 6	

Reseller channel – example

ISP Locking

The ISP Locking feature in Grandstream GDMS Cloud allows administrators to lock some settings (default password, SSID, WAN configuration) for routers to ensure consistent network configuration and prevent unauthorized changes.

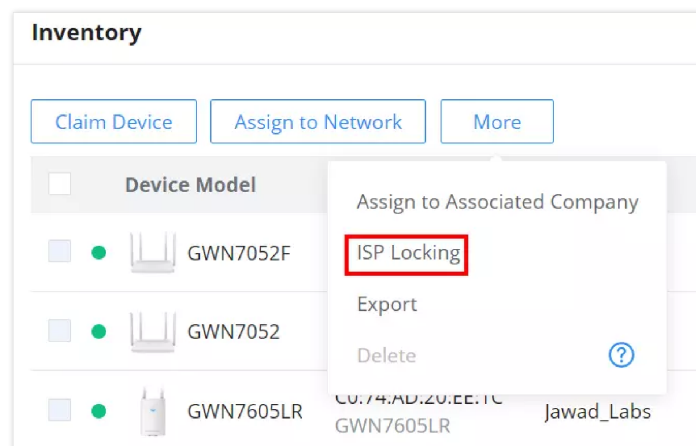
Note:

This feature is supported only on Grandstream GWN series routers.

Prerequisites

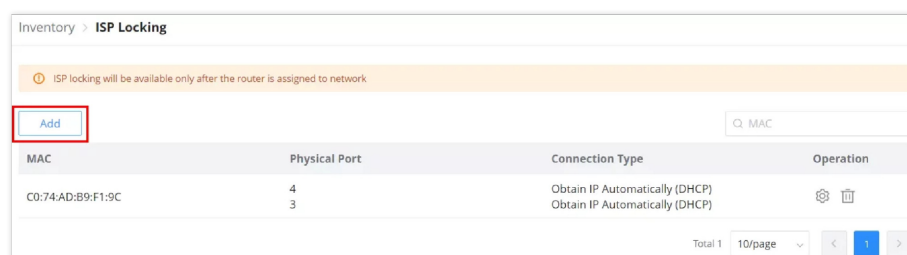
- The router must be assigned to a network within GDMS Cloud.
- Additional privileges are required to enable this feature on your GDMS account.

To configure ISP Locking, navigate to Organization → Inventory, then click on **"More"** after that click on **"ISP Locking"**. Refer to the figure below for a visual guide:



ISP Locking

To add a new router, click the **"Add"** button. To configure an existing router, click the **"Configure"** icon.



Add ISP Locking

Fill in the required details in the "Configure ISP Locking" form, which includes the default password, WAN configuration (including VLAN Tag), and SSID information (such as SSID name and password).

These new configurations will become the default settings even after the router is reset.

Note:

To activate ISP Locking, the router must be reset.

Configure ISP Locking

Connection Type

Obtain IP Automatically (DHCP)

Preferred DNS Server

1.1.1.1

Alternative DNS Server

8.8.8.8

VLAN Tag

3-4094 numbers

7

WAN2

SSID

Name

1-32 characters

ISP_Name

Cancel

Save

Configure ISP Locking

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

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.

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
Technician	helps in troubleshooting	<div><div></div><div></div></div>
GWN App User	Basic Settings	<div><div></div><div></div></div>
Support Team	help resolve issues	<div><div></div><div></div></div>
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

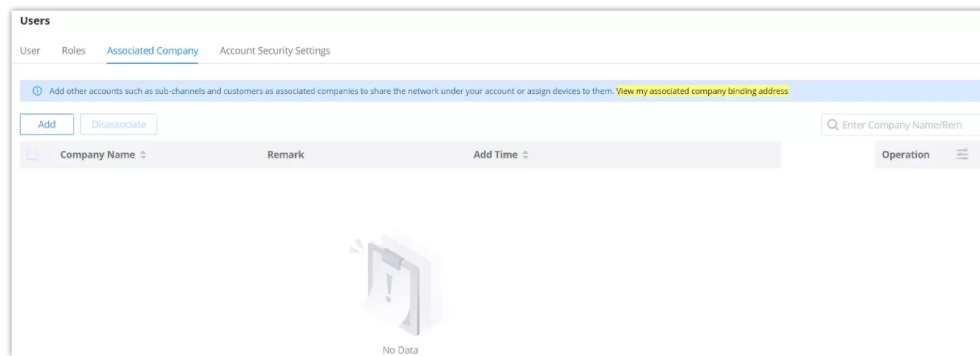
Note:

Custom role users can also log into the GWN APP.

Associated Company

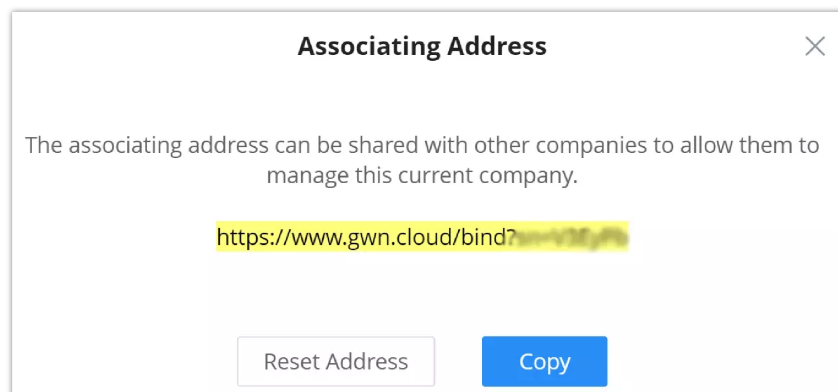
Users can add other accounts, such as sub-channels and customers, as Associated Companies. They can then share their network with them under the user name or assign devices to them.

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

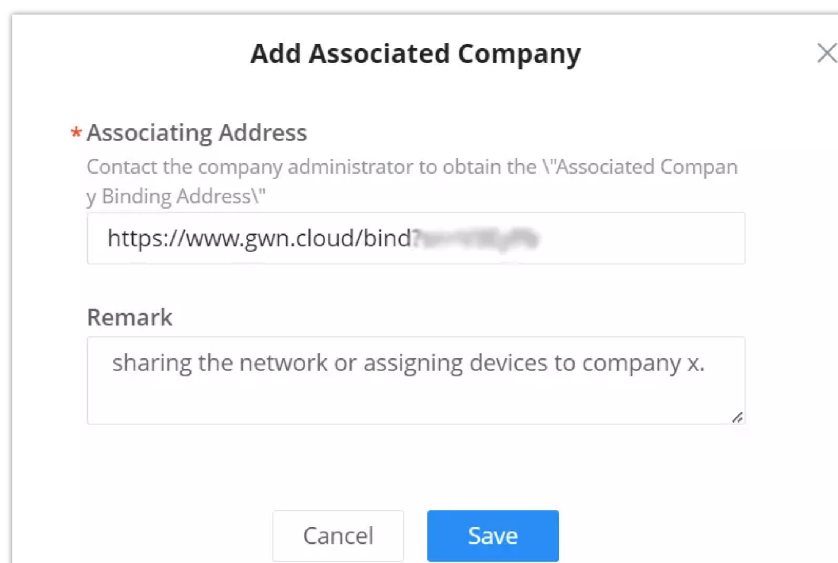


Associated company binding address

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: [email.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 share d account (history client statistic will not be shared), and you will no lon ger 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 GDMS Networking 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)	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. Note: The default value is 180.
Login Duration (min)	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. Note: The user can enter a value between 5 and 1440
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.

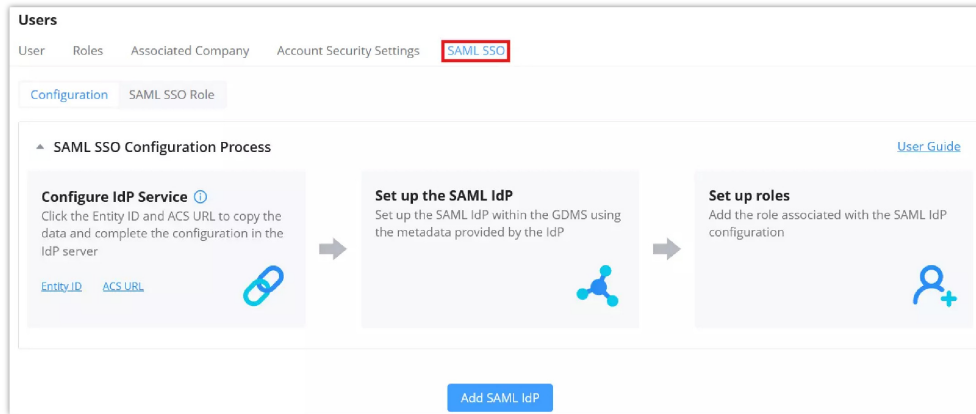
Account Security Settings

SAML SSO

SAML (Security Assertion Markup Language) Single Sign-On (SSO) allows users to authenticate into GDMS Networking using their organization's centralized identity provider (IdP). This enables streamlined and secure access across systems while reducing password fatigue and administrative overhead.

With SAML SSO, administrators can configure and manage external login services (e.g., Azure AD, Okta, etc.) for users in their GDMS Networking account. Once configured, users can log in through their IdP, and roles will be assigned based on mapped permissions in the system.

To access this feature, navigate to: **Organization** → **Users** → **SAML SSO tab**



SAML SSO page

SAML SSO Configuration

The **Configuration** tab displays a step-by-step process to set up SAML SSO for your organization. The setup includes:

1. Configure IdP Service

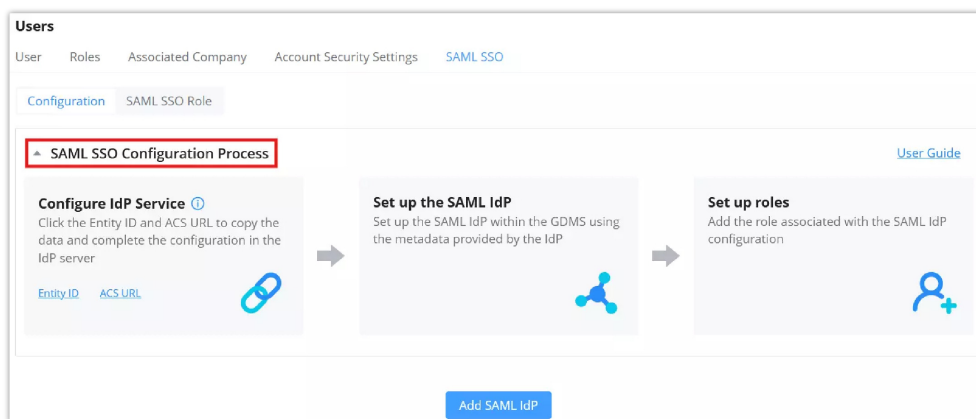
Copy the required metadata—**Entity ID** and **ACS URL**—to input into your IdP dashboard.

2. Set Up the SAML IdP

Input metadata from your identity provider into GDMS Networking to connect both ends.

3. Set Up Roles

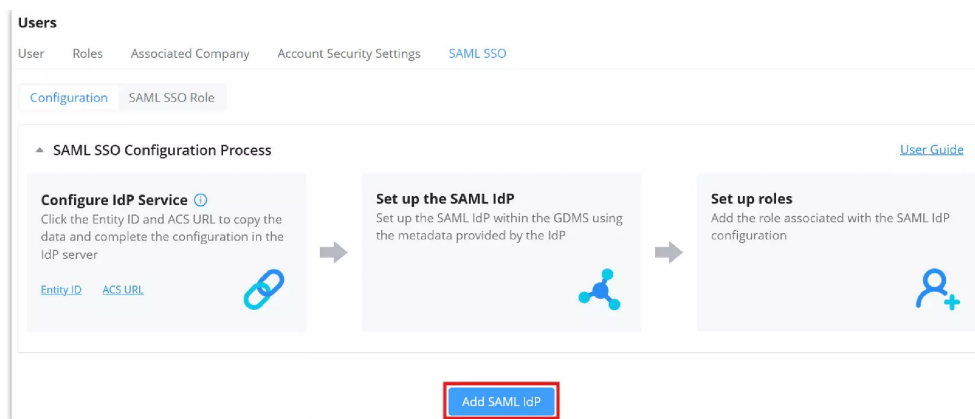
Define which users can access the system and what they are allowed to do by mapping roles.



SAML SSO Configuration Process

Clicking on **Entity ID** or **ACS URL** automatically copies the values to your clipboard for quick use in the IdP configuration panel.

Click the **Add SAML IdP** button to create a new configuration.



Add SAML Idp

When adding a new IdP, a detailed form appears. The key fields are:

Add SAML Idp

- **SSO Access Code**
A unique identifier used during login. This code is what users enter on the GDMS login page to trigger SSO. [Insert Screenshot – part 7 saml sso saml sso access code note]
- **IdP Entity ID**
The unique identifier of your identity provider.
- **X.509 cert SHA1 fingerprint**
This fingerprint from your IdP certificate is used for encryption and validation. [Insert Screenshot – part 8 saml sso saml x.509 cert sha1 fingerprint note]
- **SSO Login URL**
Where users will be redirected when their session expires or upon login. [Insert Screenshot – part 9 saml sso saml sso login url]
- **SSO Logout URL**
Optional. When users log out from GDMS, they'll also be logged out of the IdP if this URL is configured. [Insert Screenshot – part 10 saml sso saml sso logout url]

Once all required fields are completed, click **Save**.

SAML SSO Role

After configuring your SAML IdP, switch to the **SAML SSO Role** tab to create role mappings between the IdP and GDMS Networking.

Click the **Add** button to create a new role mapping.

Users

User Roles Associated Company Account Security Settings **SAML SSO**

Configuration **SAML SSO Role**

Add

Role Name Organization Network Operation

Add SAML SSO Role

Step 1: General Settings

Set a **Role Name** that exactly matches the role configured in your IdP.

Users > Add Role

General Settings UC Permissions Networking Permissions

* Role Name 1-64 characters

UC Organization **World** EU Region

Default ×

Networking **World** **EU Region**

Network-based × Default Network ×

☒ Auto Add New Network

Next

Add role – General Settings

Step 2: UC Permissions

Define permissions related to UC (Unified Communications) features.

Users > Add Role

General Settings **UC Permissions** Networking Permissions

< Basic UCMRC CloudUCM Resources Alerts Reseller Channel RPS Management Users System >

☒ All

☐ Dashboard

☐ Overview

Extension - SIP Account

☒ Account List ☐ Add Account ☐ Import Account ☐ Export Account ☒ Edit Account

☐ Delete Account ☐ Modify SIP Server ☐ Go to PBX/CloudUCM Web UI to edit extension

Extension - SIP Server

☒ SIP Server List ☐ Add Server ☐ Delete Server ☐ Edit Server

VoIP Device

☒ Device List ☐ Transfer Device ☒ Add Device ☐ Authorization Management ☐ Import Device

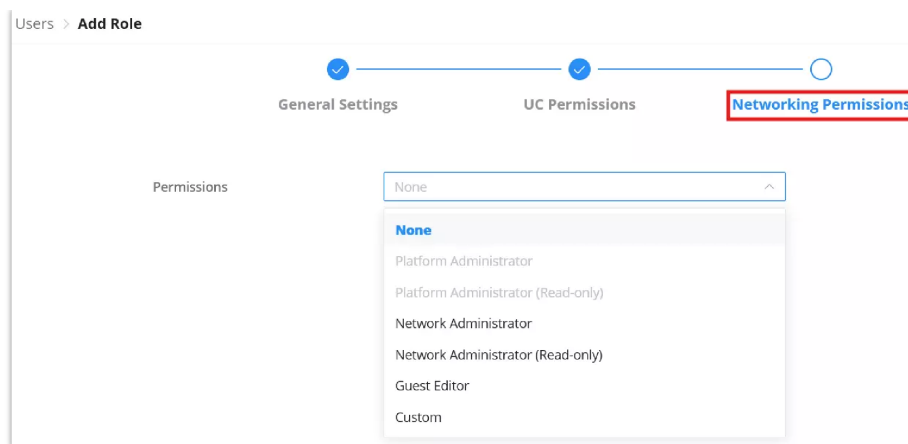
☐ Export Device ☐ Edit Device ☐ Delete Device ☐ Open Subscription ☐ Upgrade Firmware

Back **Next**

Add role – UC Permissions

Step 3: Networking Permissions

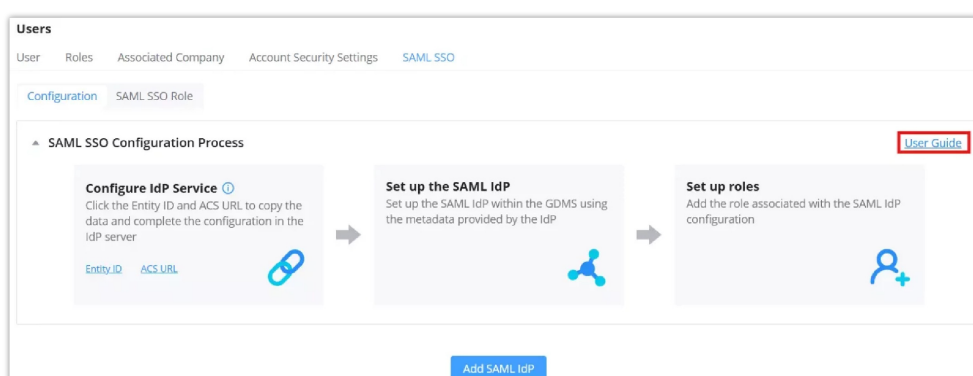
Choose networking-specific permissions or assign a custom role.



Add role – Networking Permissions

Additional Help

A detailed **User Guide** is available directly from the platform by clicking the **User Guide** link in the top-right of the Configuration tab.



SAML SSO – User Guide

Alternatively, you can access the documentation here: [GDMS SAML SSO User Guide](#)

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						
Devices Upgrade		Upgrade History				
Firmware		Upgrade Reminder <input checked="" type="checkbox"/>	All Networks	All Models	All Devices	Model/MAC/Firmware Ver
<input type="checkbox"/>	Device Model	MAC	Network Name	Firmware	Recommended Version	Scheduling
<input type="checkbox"/>	GWN7624	C0:74:AD:90:B2:40 GWN7624	Default Network	1.0.25.10	1.0.25.7	No
<input type="checkbox"/>	GWN7002	C0:74:AD:BF:AF:50	Default Network	1.0.4.6	1.0.3.5	No
<input type="checkbox"/>	GWN7052F	C0:74:AD:B9:F1:9C	GS Network	1.0.9.2	1.0.7.2	No
<input type="checkbox"/>	GWN7813P	C0:74:AD:DF:CC:94	Default Network	1.0.1.8	1.0.1.8	No
Total 4						10/page

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).

Devices Upgrade > Upgrade

Firmware Server

☒ Cloud
☐ Local (HTTP/HTTPS)

Firmware Version

Latest Recommended Version

Upgrade Time

☒ Upgrade Now
☐ Upgrade Later
☐ Upgrade Regularly

Remark

Upgrade

Add a comment about the upgrade

Cancel

OK

Upgrade in Batches

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:

GWN Manager

Upgrade

Devices Upgrade

Manager Upgrade

Upgrade History

Upgrade

Upgrade Reminder

Service	Version	Latest Firmware	Scheduling
GWN Manager	1.1.28.10	1.1.28.10	No

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

- Supports link speed display for Aps on the device list
- Supports cloning the LAN and wired firewall configuration
- Added Beta firmware display and supports upgrading to Beta
- Optimize client list Sorting
- Supports Local WAN Configuration Synchronization
- Added Phone Number length Settings for the authentication of Splash Page
- Optimized Feedback entry
- Added PPSK configuration, inventory information acquiring, and switch port information acquiring for API
- 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

🔍

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@grandsream.com	2023-11-16 04:32PM	Upgrade	<div><div><input checked="" type="checkbox"/> Schedule ID</div><div><input checked="" type="checkbox"/> Device Type</div><div><input checked="" type="checkbox"/> Device Model</div><div><input checked="" type="checkbox"/> Device Number</div><div><input checked="" type="checkbox"/> Target Version</div><div><input checked="" type="checkbox"/> Upgrade Status</div><div><input checked="" type="checkbox"/> Administrator</div><div><input checked="" type="checkbox"/> Scheduled Time</div><div><input checked="" type="checkbox"/> Remark</div></div>

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

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

<

1

>

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

jawad@grandstream.com

Add New Item

Cancel

Save

Create a report

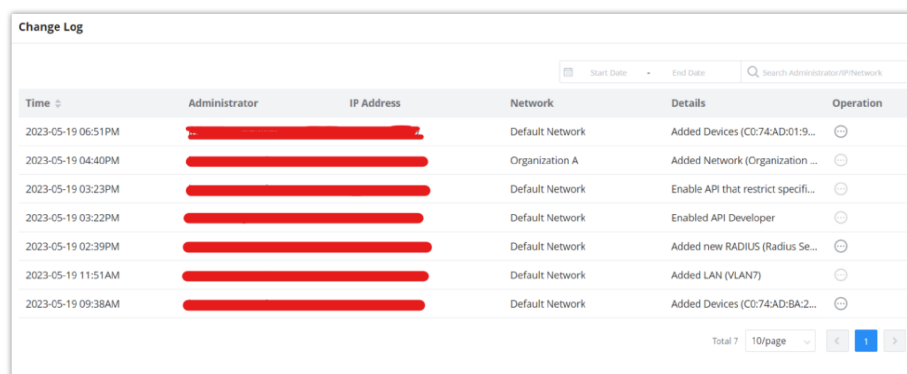
The following table explains different options for report settings:

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



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

Total 7 10/page

[Change Log](#)

To see more details, click on the three dots.

API Developer

The **API Developer Mode** in GDMS Networking allows organizations to securely integrate their network operations with external platforms, in-house tools, or automation workflows using a RESTful API.

This feature is designed for environments that require centralized monitoring, real-time alerts, automated provisioning, or system-to-system integration beyond the standard web interface.

Navigation: Go to **API Developer** from the main menu.



Enabling Developer Mode

To activate API Developer Mode:

1. Toggle the **Enable Developer Mode** option.
2. The system will generate:
 - **APP ID** – A unique identifier used for authenticating API requests.
 - **Secret Key** – A secure key used to obtain an access token.
3. Optionally, toggle **Restrict APIs to specific networks** to limit access only to networks associated with the logged-in user.

Authentication Requirements

To access GDMS Networking APIs, a valid **access token** must be generated. The authentication process depends on your settings:

- **If “Restrict APIs to specific networks” is disabled (default):**
You only need your **APP ID** and **Secret Key**.
- **If restriction is enabled:**
In addition to the APP ID and Secret Key, you must also provide your **GDMS account username and password**.
This adds a layer of security by ensuring the token only grants access to networks assigned to that user.

This flexible model allows both general integrations and tightly scoped access when required.

API Capabilities and Integration Highlights

GDMS Networking’s **API Developer Mode** provides secure, programmable access to the platform’s core features, allowing seamless integration with external systems and custom workflows.

The API supports a wide range of functions, including (but not limited to):

- Accessing real-time device and client data
- Automating configuration of networks, SSIDs, VLANs, and device groups
- Managing provisioning and deployment across distributed environments
- Receiving alerts through **Webhook integration**
- Retrieving **Bluetooth Low Energy (BLE) client data** from supported access points. Note: Bluetooth API must be enabled first under **Settings → System → General**.
- Configuring security features such as MAC-based authentication and RADIUS profiles
- Handling bulk import/export of network and device configurations

These capabilities enable IT teams and system integrators to build scalable, automated, and responsive network operations.

Developer Documentation

The full list of API endpoints, usage examples, authentication steps, and integration methods can be found in the official developer guide: [GWN API Developer Guide](#)

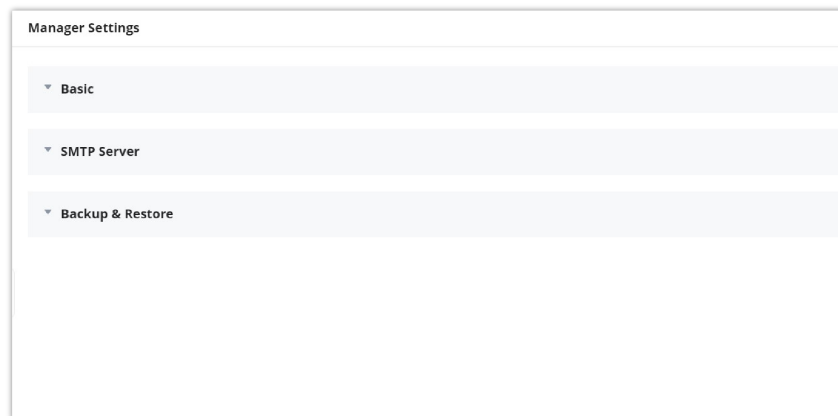
This includes:

- Access token generation
- Webhook payload format
- Endpoint descriptions and parameters
- Sample request/response structures
- Error code definitions

MANAGER SETTINGS

Note:

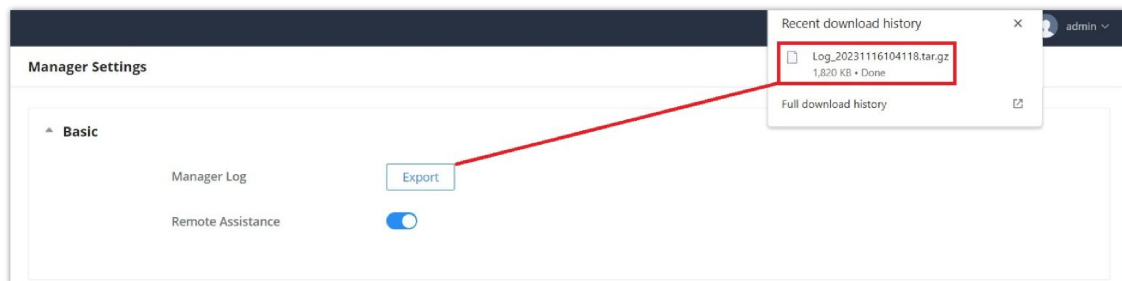
Manager Settings is only available for GWN Manager.



Manager Settings page

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.

SMTP Server

From Email Address

From Name

1 to 64 characters

SMTP Username

SMTP Password

* SMTP Host

* SMTP Port

Send test email

Cancel

Save

Manager Settings – SMTP Server

Backup & Restore

Users can Backup GWN Manager configuration as shown below:

Manager Settings

Basic

SMTP Server

Backup & Restore

Upload Backup

Upload

Manual Backup

Backup

Backup Settings

* File Storage Path

/gwn_backup

Retained Data Backup

Cancel

Save

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.

REQUIREMENTS

The following tables show the requirements of Grandstream networking products including GWN Access Points, GWN Routers, GWN Switches, GCC Devices, and GWN App versions (Android® and iOS®) for GWN Management Platforms (GDMS Networking & GWN Manager):

- GWN Access Points: minimum and recommended version**

Model	Minimum	Recommended
GCC6010	1.0.1.8	1.0.1.8

GCC6010W	1.0.1.8	1.0.1.8
GWN7001	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7002	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7003	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7052	1.0.5.34 (1.0.9.42 for GWN Manager)	1.0.9.42
GWN7052F	1.0.5.4 (1.0.9.42 for GWN Manager)	1.0.9.42
GWN7062	1.0.5.34 (1.0.9.42 for GWN Manager)	1.0.9.42

AP minimum and recommended version

○ **GWN Routers/GCC Devices: minimum and recommended version**

Model	Minimum	Recommended
GCC6010	1.0.1.8	1.0.1.8
GCC6010W	1.0.1.8	1.0.1.8
GWN7001	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7002	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7003	1.0.1.6 (1.0.5.35 for GWN Manager)	1.0.5.35
GWN7052	1.0.5.34 (1.0.9.42 for GWN Manager)	1.0.9.42
GWN7052F	1.0.5.4 (1.0.9.42 for GWN Manager)	1.0.9.42
GWN7062	1.0.5.34 (1.0.9.42 for GWN Manager)	1.0.9.42

GWN routers/GCC devices minimum and recommended version

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

Model	Minimum	Recommended
GWN7711	1.0.1.8	1.0.1.8
GWN7711P	1.0.1.8	1.0.1.8
GWN7801	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7801P	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7802	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7802P	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52

GWN7803	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7803P	1.0.3.19 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7806	1.0.1.14 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7806P	1.0.1.14 (1.0.5.52 for GWN Manager)	1.0.5.52
GWN7811	1.0.1.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7811P	1.0.1.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7812P	1.0.1.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7813	1.0.1.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7813P	1.0.1.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7816	1.0.3.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7816P	1.0.3.8 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7830	1.0.3.3 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7831	1.0.3.3 (1.0.7.64 for GWN Manager)	1.0.7.64
GWN7832	1.0.3.3 (1.0.7.64 for GWN Manager)	1.0.7.64

Switch minimum and recommended version

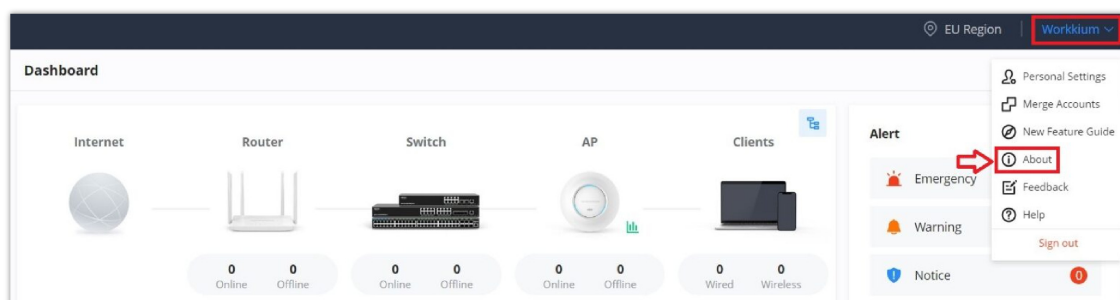
◦ **GWN App: minimum and recommended version**

Platform	Minimum	Recommended
iOS®	1.0.5	1.6.7
Android®	1.0.0.14	1.0.6.7

App minimum and recommended version

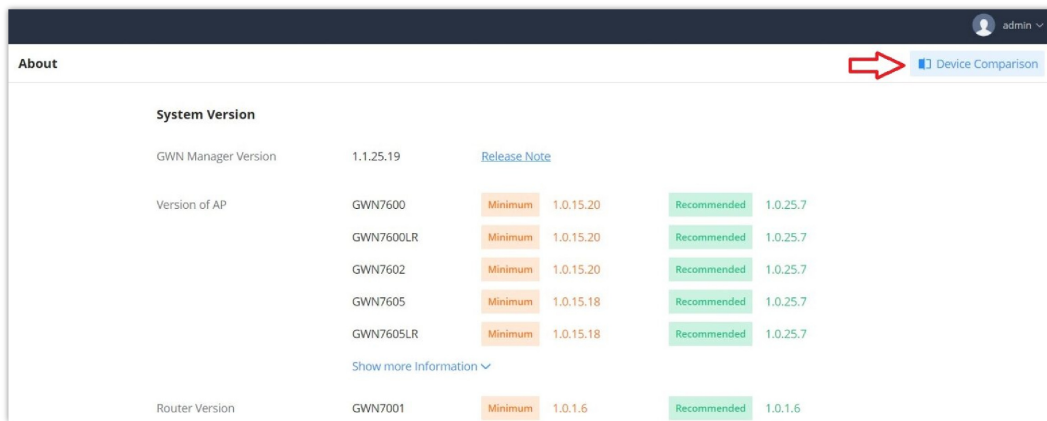
Requirements

To know more about the differences between Grandstream devices in terms of functions based on the recommended versions, please navigate to **GDMS Networking 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 Grandstream device and APP (iOS® and Android®). If a Beta firmware is available for a device it will be also shown here.

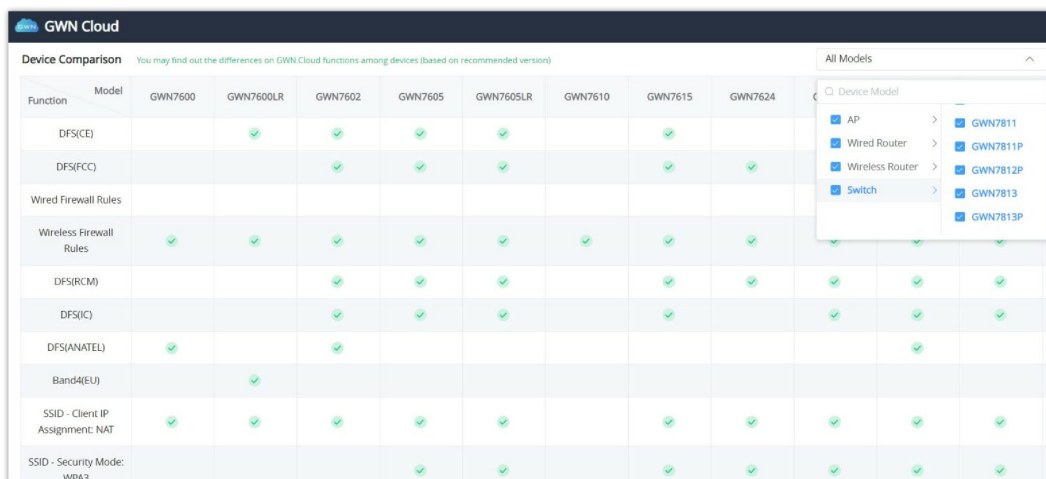


System Version					
GWN Manager Version	1.1.25.19	Release Note			
Version of AP	GWN7600	Minimum	1.0.15.20	Recommended	1.0.25.7
	GWN7600LR	Minimum	1.0.15.20	Recommended	1.0.25.7
	GWN7602	Minimum	1.0.15.20	Recommended	1.0.25.7
	GWN7605	Minimum	1.0.15.18	Recommended	1.0.25.7
	GWN7605LR	Minimum	1.0.15.18	Recommended	1.0.25.7
Show more Information ▾					
Router Version	GWN7001	Minimum	1.0.1.6	Recommended	1.0.1.6

Device Comparison – Step 2

AP Version	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 ▾						
		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)



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

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 1.1.33.2

- Added support for Webhook API alerts. [[API Developer](#)]
- Added support for BLE client API. [[API Developer](#)]
- Added rotating Floor Plans option and added more label information. [[Floor Plans](#)]
- Added support for MAC-based authentication, LACP on switch ports (for GWN78XX versions equal to or higher than 1.0.15.X). [[Configure a GWN Switch](#)]
- Added support for capturing switch syslogs. [[Syslog](#)]
- Added support for Voice VLAN, LLDP, and total input power configuration on GWN77XX. [[Configure a GWN Switch \(Layer 2 lite\)](#)]
- Added global blocklist limit to 1000. [[Wireless LAN](#)]
- Added "Power Supply Mode" in the switch POE status list. [[Configure a Switch](#)]
- Optimized the device list to display the uplink speed of routers and switches. [[Devices](#)]
- The Splash Portal password authentication now supports all characters (except spaces) for simple passwords. [[Splash page](#)]
- Optimized the client list to display Locked APs. [[Clients](#)]

Version 1.1.31.22

- Added Alert Icons to the network list. [[Network Overview](#)]
- Added filter for read/unread alerts on the alerts page. [[Alerts](#)]
- Support exception AP for offline alerts. [[System Alert](#)]
- Added the configuration of target wake-up time for SSID. [[Wi-Fi](#)]
- Added MAC authentication for SSID. [[Wi-Fi](#)]
- Added frequency band display of the SSID in the SSID list. [[Wireless LAN](#)]
- Added the SAML SSO Configuration to support SSO Login. [[SAML SSO](#)]
- Added defense configuration for DoS/Spoofing Attack. [[Security Defense](#)]
- Added Defense Alert for DoS/Spoofing attack. [[Security Alerts](#)]
- Added SNAT & DNAT configuration for GWN router. [[SNAT](#)] [[DNAT](#)]
- Added VPN Configure Wizard for fast and convenient setup for different VPN protocols. [[VPN Setup Wizard](#)]
- Display the locked access point for all set devices and added the configuration for the Failover Access Point. [[Configure a Client](#)]
- Added Network Tags for the network list in the overview page. [[Network Tags](#)]
- Added the function to Import Network/Device/Device Group/SSID configuration. [[Network Import](#)]
- Added Dark Web Theme support [[Theme Appearance](#)]
- Added Voucher Group Template configuration support. [[Voucher Group Template](#)]
- Added PPSK support for GWN routers and support PPSK download and export. [[PPSK](#)]
- Added VLAN2 configuration in LAN. [[LAN](#)]
- Added a method to sort RSSI by numerical order. [[Clients](#)]
- Added quick link to view Blocklist. [[Clients](#)]
- Added Real Time Chart for wireless client usage. [[Client usage](#)]
- Added filter for online/offline devices on inventory page. [[Inventory](#)]

- Added longitude and latitude configuration for devices. [[Devices](#)]
- Added display for Uplink Port of the switch. [[GWN Switch – Port](#)]
- Support the use of public IP for DDNS source IP. [[DDNS](#)]
- Support configuring the refresh interval for DDNS. [[DDNS](#)]
- Support RADIUS Profile configuration on API. [[API Developer](#)]

Version 1.1.29.15

Product Name: GDMS Networking

- Optimized the performance and stability for some business process. GWN.Cloud was renamed “GDMS Networking”. Unified GDMS entry and email notifications.
- Supports vertical and horizontal display for network topology. [[Network Topology](#)]
- Added timestamp of the last contact with GDMS Networking to the list of devices. [[Devices](#)]
- Supports router NAT Traversal to remote access devices. [[NAT Traversal](#)]
- Added selections of Icon Types for Clients. [[Clients](#)]
- Added client blocking duration setting. [[Clients](#)]
- Added a central control “Collect client historical data” for all available clients. [[System](#)]
- Support binding a client to a specific AP. [[Clients](#)]
- Supports ISP Locking for wireless routers. [[ISP Locking](#)]
- Supports setting the ports names of routers. [[Configure a device](#)]
- Added the API for basic router configuration (including port). [[API developer](#)]

Version 1.1.28.27

Product Name: GWN Manager

- Added security enhancement by verifying device password when adding a switch or a router. [[Adopt a Device to GWN Manager](#)]

Version 1.1.28.25

Product Name: GWN.Cloud and GWN Manager

- Added support of GCC601X SMB UC/Networking Convergence Solutions [[Requirements](#)]
- Added the ability to update AP info in real time when enter AP detailed page [[GWN AP Info](#)]
- Added the ability to customize MAC for client isolation in wireless LAN [[Add SSID](#)]
- Added a new feature of OS Filter in wireless LAN [[Add SSID](#)]

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.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

macOS® is a trademark of Apple Inc., registered in the U.S. and other countries.

Windows® is a trademark of Microsoft Corporation in the United States and other countries.
