Grandstream Networks, Inc.

GWN76xx - User Manual

GWN76xx - User Manual

OVERVIEW

Grandstream's powerful indoor and outdoor Wi-Fi Access Points (APs) offer high-performance networking and an exceptional Wi-Fi coverage range. The outdoor series offers a weatherproof-certified casing and supports up to a 300-meter coverage range. They are supported by GDMS Networking and GWN Manager, Grandstream's cloud and on-premises free management platforms. Each device also includes an embedded controller within the product's web user interface for easy administration of locally deployed Wi-Fi APs. GWN Wi-Fi APs are ideal for any size business or enterprise and can be scaled over time as your business grows.

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

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

PRODUCT OVERVIEW

Technical Specifications

Select an access point model below to open its technical specifications. Models are organized by Wi-Fi generation and deployment environment, with indoor models listed before outdoor models.

Wi-Fi Generation	Deployment	Model
Wi-Fi 5	Indoor	GWN7603
		GWN7605
		GWN7615
		GWN7624
		GWN7625
		GWN7630
	Outdoor	GWN7605CLR
		GWN7605LR
		GWN7630LR
Wi-Fi 6 / 6E	Indoor	GWN7604
		GWN7660
		GWN7660E
		GWN7660EM
		GWN7661
		GWN7661E
		GWN7662
		GWN7664

Wi-Fi 6 / 6E	Indoor	GWN7664E
		GWN7665
	Outdoor	GWN7660ELR
		GWN7660LR
		GWN7664ELR
		GWN7664LR
Wi-Fi 7	Indoor	GWN7670
		GWN7670E
		GWN7673
		GWN7670WM
		GWN7671
		GWN7672
		GWN7672L
		GWN7672WM
		GWN7674
	Outdoor	GWN7670ELR
		GWN7670LR

Service Ports

The following service ports are used by the **GWN76XX series models** covered in this user manual. These ports are associated with features such as management access, device discovery, and portal-based services:

Port	Protocol	Description
14	UDP	Used for automatic discovery of GWN Access Points within the local network (proprietary protocol).
22	TCP	Secure Shell (SSH) used for CLI access and remote command-line management.
80	TCP	HTTP access; used as an initial entry point and redirects to HTTPS (port 443).
443	TCP	HTTPS web interface; provides secure access to the GWN management UI.
8080	TCP	Captive portal redirect for guest access and authentication workflows.
8443	TCP	Encrypted web authentication; used for secure access to captive portal and guest services.
9443	TCP	Business portal services, such as voucher-based log downloads and extended access features.
10000	TCP	Used for multicast to unicast services

These ports apply specifically to the **GWN76XX series models** documented in this manual.

INSTALLATION

Select your access point model below to open its Quick Installation Guide. Models are organized by Wi-Fi generation and deployment environment, with indoor models listed before outdoor models. Each guide provides the package contents, port and power information, and mounting instructions for that model.

Wi-Fi Generation	Deployment	Model
Wi-Fi 5	Indoor	GWN7603
		GWN7605
		GWN7615
		GWN7624
		GWN7625
		GWN7630
	Outdoor	GWN7605CLR
		GWN7605LR
		GWN7630LR
Wi-Fi 6 / 6E	Indoor	GWN7604
		GWN7660
		GWN7660E
		GWN7660EM
		GWN7661
		GWN7661E
		GWN7662
		GWN7664
		GWN7664E
		GWN7665
	Outdoor	GWN7660ELR
		GWN7660LR
		GWN7664ELR
		GWN7664LR
Wi-Fi 7	Indoor	GWN7670
		GWN7670E/GWN7673
		GWN7670WM
		GWN7671
		GWN7672/GWN7672L
		GWN7672WM
		GWN7674
	Outdoor	GWN7670ELR
		GWN7670LR

GETTING STARTED

The GWN76XX Wireless Access Point provides an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN76XX's setup.

This section provides step-by-step instructions on how to read LED patterns, discover the GWN76XX, and use its Web GUI interface.

LED Patterns

The panel of the GWN76XX has different LED patterns for different activities, to help users read the status of the GWN76XX, whether it is powered up correctly, provisioned, in the upgrading process, and more. For more details, please refer to the table below.

LED Status	Indication
Off	Unit is powered off or the power supply is abnormal.
Blinking green	Firmware update in progress.
Solid green	Firmware update completed successfully.
Blinking red	Paired Subordinate AP deletion or factory reset initiated.
Solid red	Firmware update failed.
Solid purple	Unit is not provisioned.
Blinking blue	Unit provisioning is in progress.
Solid blue	Unit was provisioned successfully.
Blinking white	Access Point location feature is active.
Solid yellow	Mesh connection is disconnected.
Blinking purple	The Subordinate AP is disconnected from the Primary device, for example because the network connection is unavailable or the Primary device is offline.

Discover the GWN76XX

Once the GWN76XX is powered up and connected to the Network correctly, users can discover the GWN76XX using one of the following methods:

Method1: Discover the GWN76XX using its MAC address

1. Locate the MAC address on the stickers of the unit, which is located on the back of the device or on the package.
2. From a computer connected to the same network as the GWN76XX, type in the following address using the GWN76XX's MAC address on your browser **https://gwn_<mac>.local**

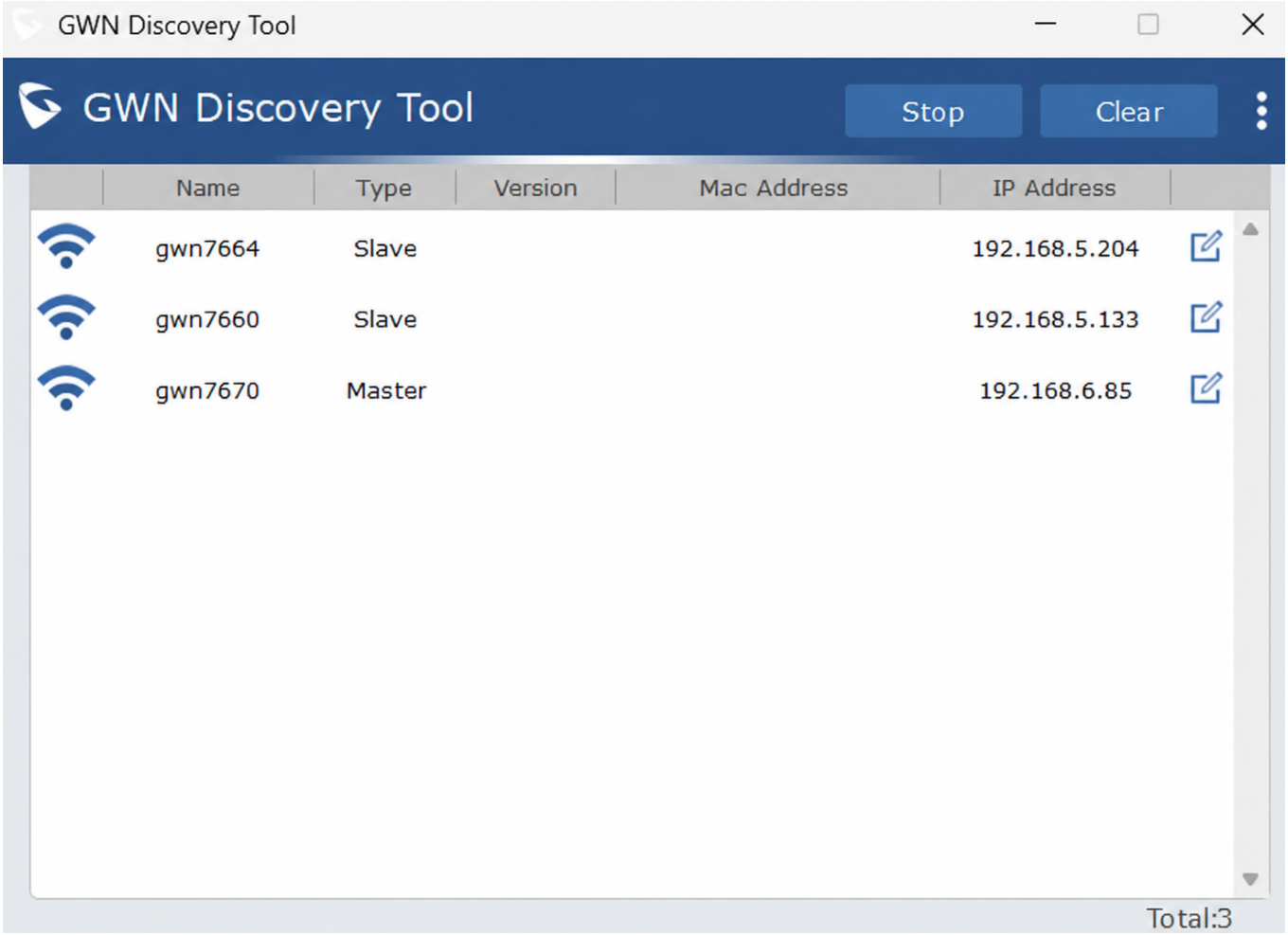
if a GWN76XX has the MAC address EC:74:D7:8B:58:30, this unit can be accessed by typing https://gwn_ec74d78b5830.local/ on the browser.



Discover the GWN76XX using its MAC Address

Method 2: Discover the GWN76XX using the GWN Discovery Tool

1. Download and install the GWN Discovery Tool from the following link: https://www.grandstream.com/support/tools
2. Open the GWNDiscoveryTool, click on Select to define the network interface, then click on Scan.
3. The tool will discover all GWN76XX Access Points connected on the network, showing their MAC, IP addresses, and firmware version.
4. Click on **Manage Device** to be redirected directly to the GWN76XX's configuration interface, or type in the displayed IP address in your browser.



GWN Discovery Tool

Use the Web GUI

Users can access the GWN76XX using its WebGUI. The following sections will explain how to access and use the Web Interface.

Access Web GUI

The GWN76XX embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome, etc.



GWN76XX Web GUI Login Page

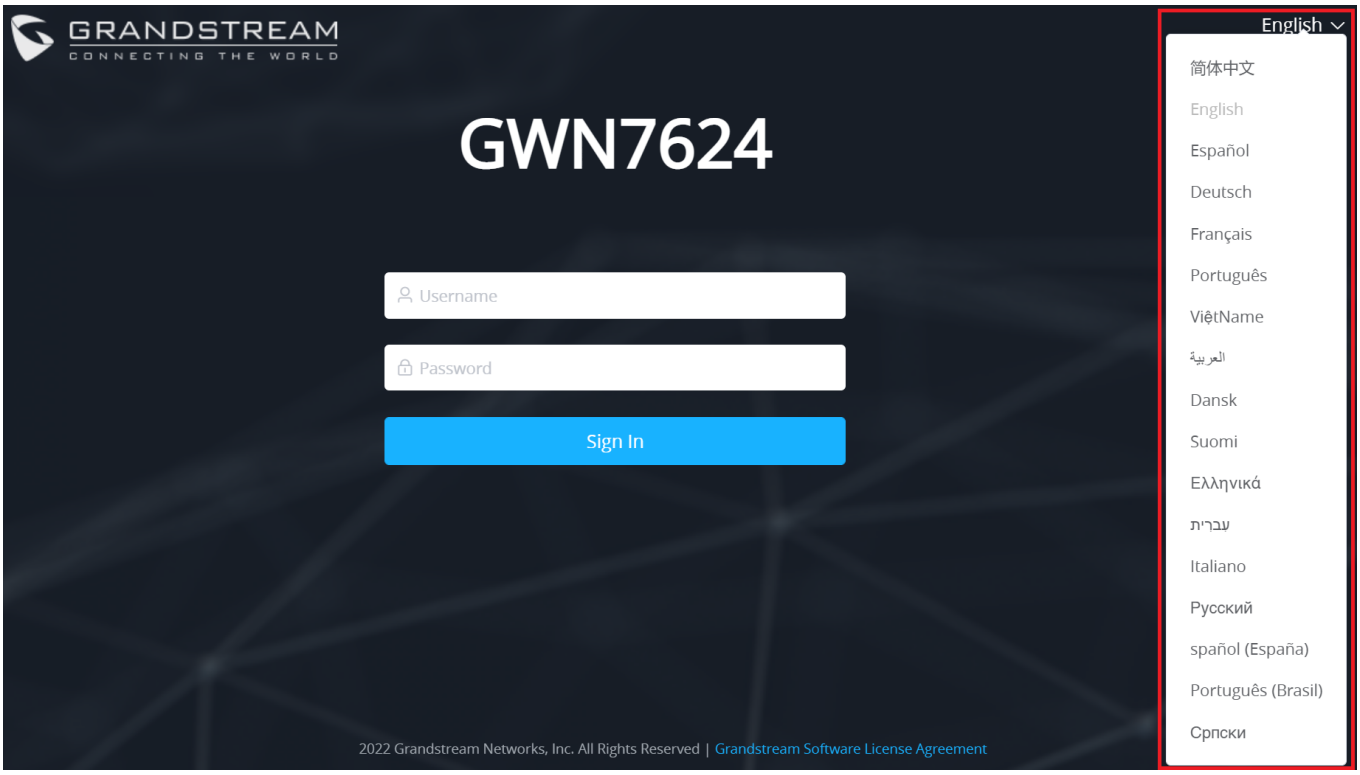
To access the Web GUI:

1. Make sure to use a computer connected to the same local Network as the GWN76XX.
2. Ensure the device is properly powered up.
3. Open a Web browser on the computer and type in the URL using the MAC address as shown in [Discover the GWN76XX] or the IP address using the following format: **http(s)://IP_Address**
4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is always "admin" and the password is the unique default Wi-Fi Password available on the sticker on the back of the unit.

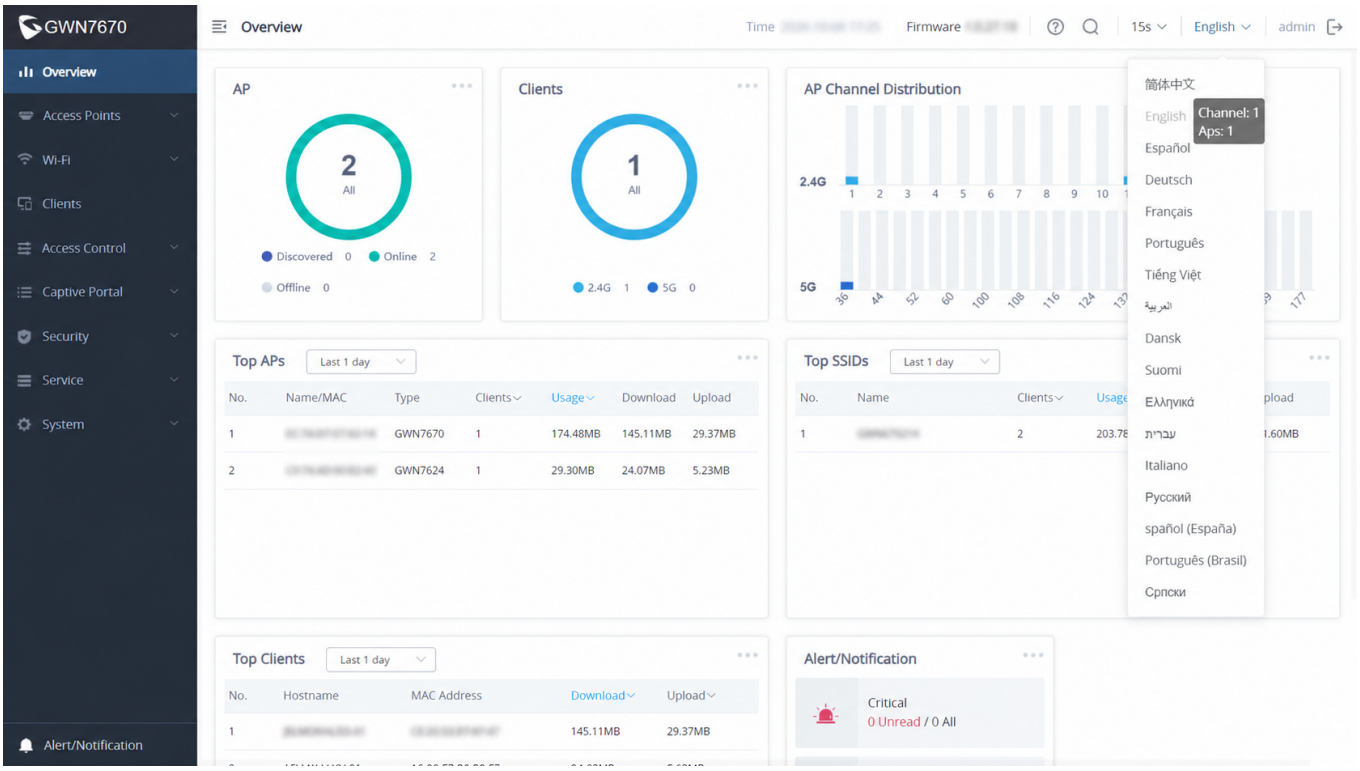
GWN AP's web UI access will be locked for 15 mins after 5 login failures

WEB GUI Languages

Currently, the GWN76XX series web GUI supports 17 languages, including English, Chinese, Spanish, etc. Users can select the displayed language at the upper right of the web GUI either before or after login.



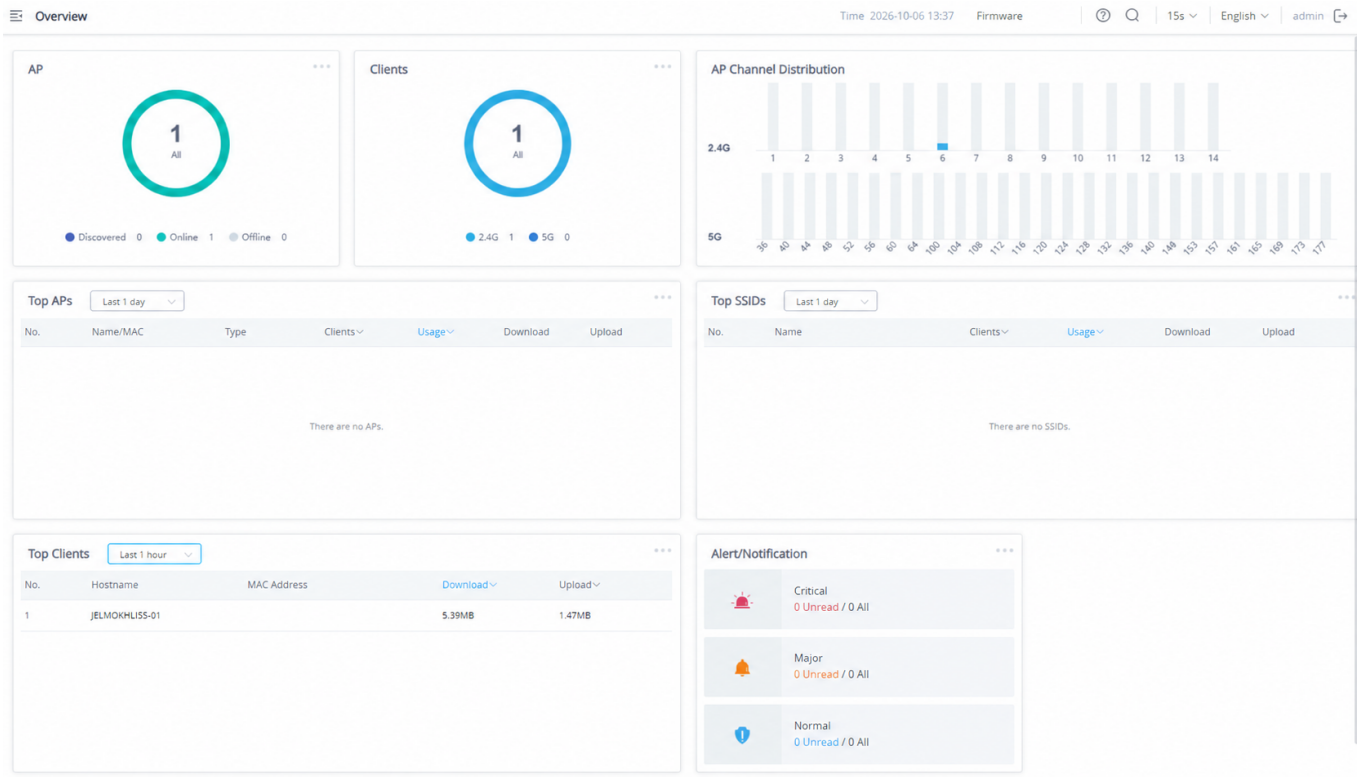
GWN76XX Web GUI Language (Login page)



GWN76XX Web GUI Language (Web Interface)

Overview Page

The overview is the first page shown after successful login to the GWN76XX's Web Interface. This page provides an overall view of the GWN76XX information presented in a Dashboard style for easy monitoring, along with firmware version and date-time information at the top.



GWN76XX Dashboard

Users can quickly see the status of the GWN76XX for different items. Please refer to the following table:

AP	Shows the number of Access Points that are Discovered, Paired (Online), and Offline. Users may click on to go to the Access Points page for basic and advanced configuration options for the APs.
Clients	Shows the total number of connected clients, and a count of connected clients to each Channel. Users may click on to go to the Clients page for more options.
AP Channel Distribution	Shows the Channel used for all APs that are paired with this Access Point.
Top AP	Shows the Top APs list, users may sort the list by number of clients connected to each AP or data usage, combining upload and download. Users may click on to go to the Access Points page for basic and advanced configuration options for the APs.
Top SSID	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on to go to the SSID page for more options.
Top Clients	Shows the Top Clients list, users may sort the list of clients by their upload or download. Users may click on to go to the Clients page for more options.
Alert/Notification	Shows 3 types of Alerts/Notifications: Critical, Major and Normal. Users can click to pop up the list of Alert and Notification.

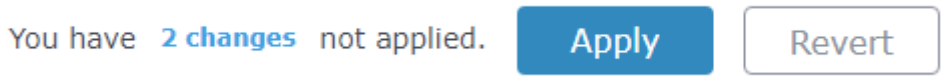
Overview

Note that Overview page in addition to other tabs can be updated each 15s, 1min ,2min and 5min or Never by clicking in the upper bar menu (Default is 15s).

New Firmware Notification: When a newer official firmware version is available, the primary AP displays an upgrade notification. Select the notification to open the release notes. For upgrade instructions, see UPGRADING AND BACKUP/RESTORE.

Save and Apply Changes

After changing a setting, select **Save**. The number of pending changes appears in the upper menu. Select **Apply Changes** to apply them.



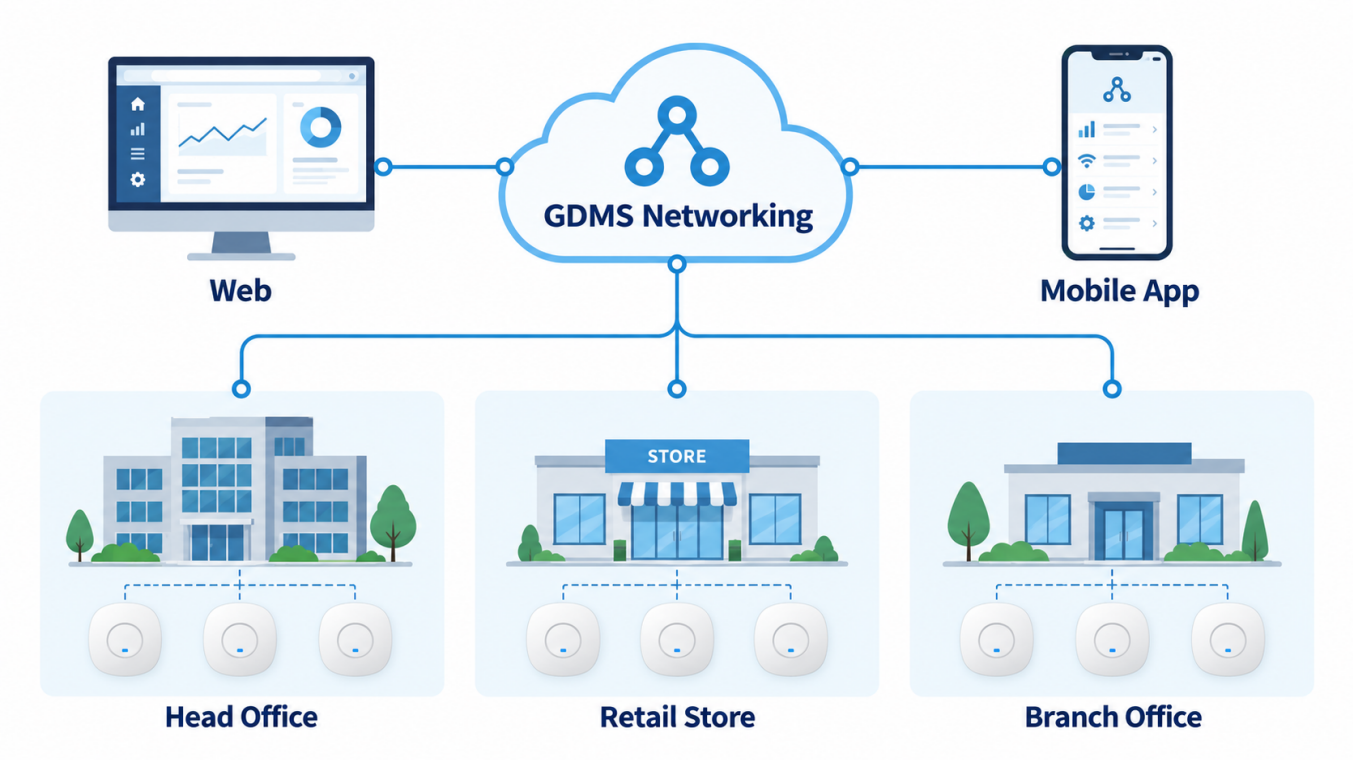
Apply Changes

GWN MANAGEMENT PLATFORMS

GDMS Networking

Grandstream GWN76xx access points can be centrally managed through **GDMS Networking**, Grandstream's cloud-based network management platform. Administrators can configure and monitor access points, review Network Health, perform maintenance, and troubleshoot devices remotely. Access GDMS Networking at https://www.gdms.cloud.

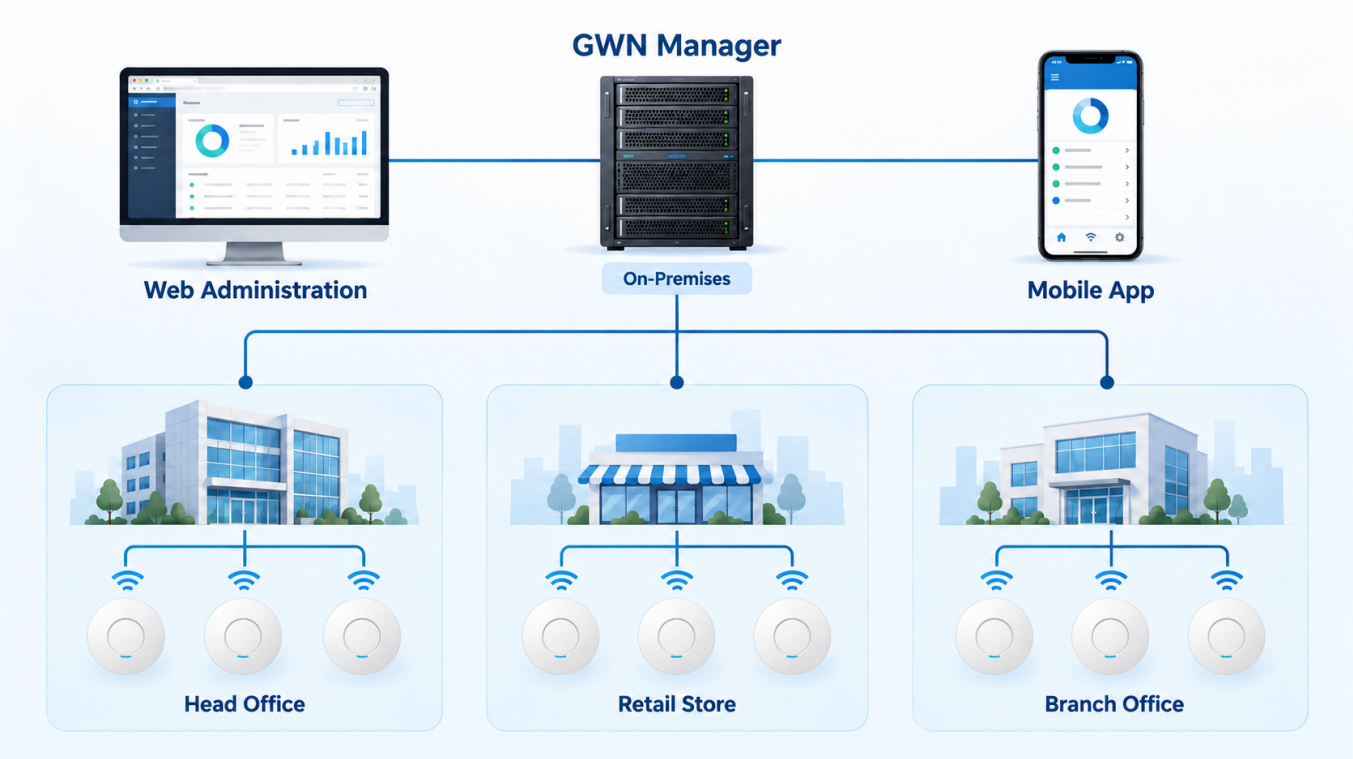
For detailed instructions, refer to the GWN Management Platforms User Guide. See Network Health for network-health monitoring and Bluetooth API for Bluetooth scan reporting.



GDMS Networking Architecture

GWN Manager

The GWN76XX can be managed and monitored by your GWN Manager account. GWN Manager On-premises Access Points Controller platform can be installed using the link below: https://www.grandstream.com/support/firmware



GWN Manager Architecture

GWN Manager installation is supported on virtual machines. Please refer to GWN Management Platform User Guide for more detailed information.

USING GWN76XX AS A STANDALONE ACCESS POINT

The GWN76XX can be used in Standalone mode, where it can act as a Primary Access Point Controller, or in Subordinate mode and managed by another GWN76XX Primary.

This section will describe how to use and configure the GWN76XX in standalone mode.

Connect to GWN76XX Default Wi-Fi Network

GWN76XX can be used as a standalone access point out of the box, or after a factory reset with Wi-Fi enabled by default.

After powering the GWN76XX and connecting it to the network, GWN76XX will broadcast a default SSID based on its MAC address GWN [MAC's last 6 digits], and a random password.

Note that GWN76XX's default SSID and password information are printed on the MAC tag of the unit as shown in the figure below.



MAC Tag Label

USING GWN76XX AS PRIMARY ACCESS POINT CONTROLLER

Primary Mode allows a GWN76XX to act as an Access Point Controller managing other GWN76XX access points. This will allow users to add other access points under one controller and manage them in an easy and centralized way

Primary/Subordinate mode is helpful with large installations that need more area zone coverage with the same controller.

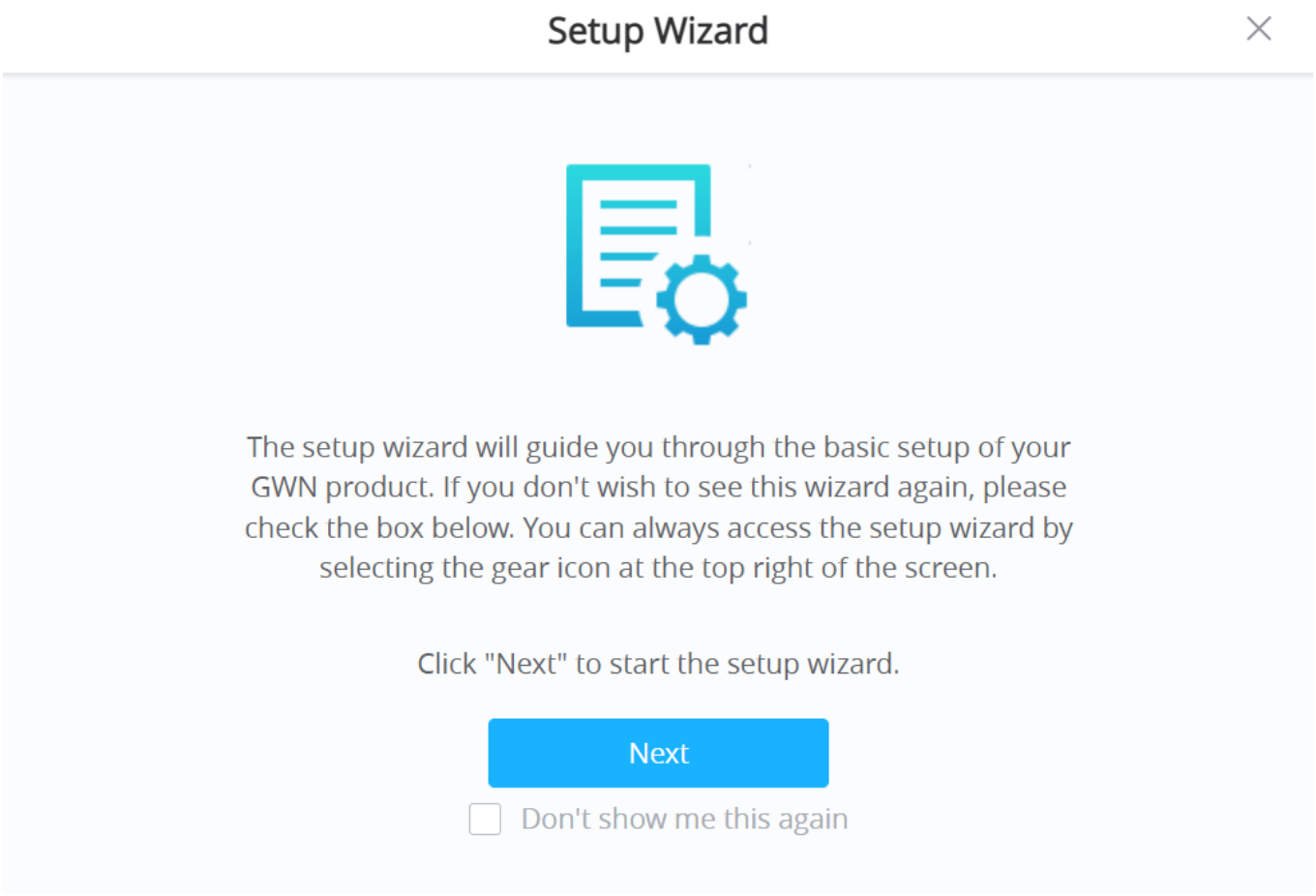


Login Page

Set unit as Primary option will forbid the GWN76XX Access Point from being paired by other Primary GWN76XX and can only act as a Primary Access point controller. Users will need to perform a factory reset to the GWN76XX , or unpair it from the initial GWN76XX to make it open to Primary Access Point mode again.

Login Page

After login, users can use the Setup Wizard tool to go through the configuration setup or exit and configure it manually. Setup Wizard can be accessed anytime by clicking on **Setup Wizard** while on the web interface.



Setup Wizard

Discover and Pair Other GWN76xx Access Points

First, note that by default, the GWN controller access point will automatically discover all APs connected to the same LAN (broadcast domain). There is also a possibility to pair and provision remote APs using DHCP option 43, with the primary direction explained below.

Primary Direction

To pair and manage access points located on remote networks, the admin needs to configure the IP address of the primary AP on DHCP option 43, which will be sent to the subordinate access point during the booting stage and allow the save/primary connection to be established remotely. GWN76xx accepts option 224 encapsulated in option 43, and the syntax is in TLV format. A simple example of DHCP 43 configuration would be:

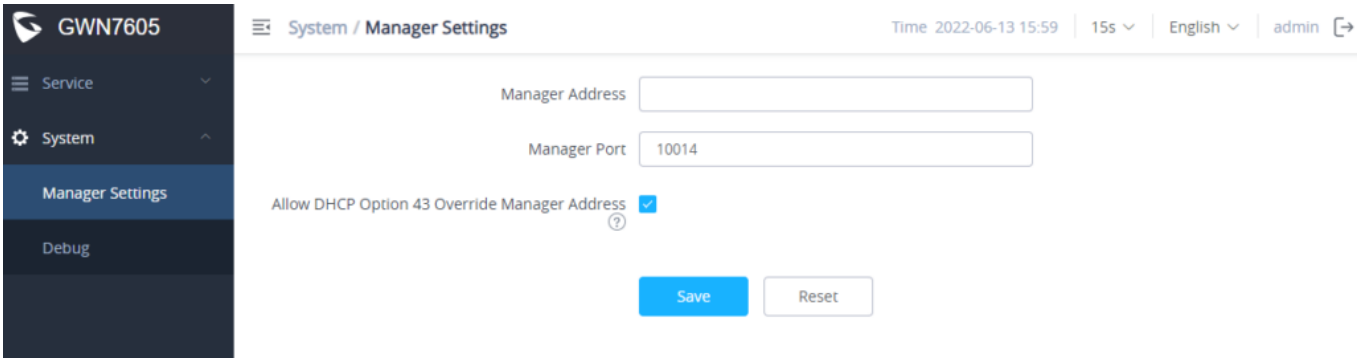
224(Type)12(Length)10.157.0.234(Value) translated into Hex as e00c31302e3135372e302e323334

Scenario example: a company has two offices connected via VPN (primary AP located on network 192.168.1.0/24 and subordinate AP located on remote network 192.168.2.0/2). On the remote network, the admin can set DHCP option 43 using the GWN70xx router as the following value: **encap:43,224,"192.168.1.100".**

- The subordinate AP has the option "**Allow DHCP Option 43 to override GWN Manager Address**" enabled

by default.

- With some DHCP servers or network environments, adding an **FF** byte at the end of the DHCP Option 43 HEX string may be required. Please refer to your DHCP server's documentation or vendor guidelines for details.

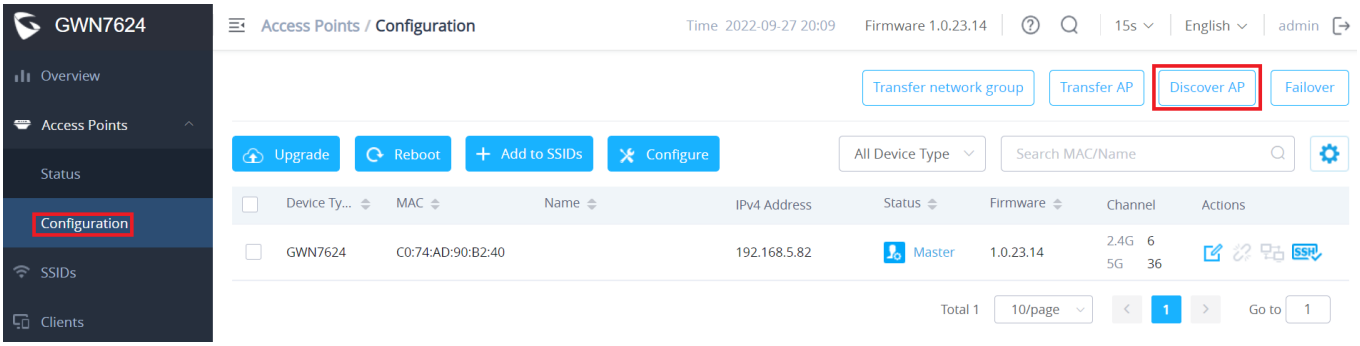


Option 43 Override

After that, the subordinate AP will be listed on the primary AP discovered devices and ready for the pairing and provisioning process, which is described in the next steps.

To pair a GWN76XX access point connected to the same Network as the GWN76XX, follow the steps below:

1. Connect to the GWN76xx Web GUI as Primary and go to **Access Points** -> **Configuration.**



Discover and Pair GWN76XX

2. Click on "**Discover**" button to discover access points within the GWN76xx Network, and the following page will appear.

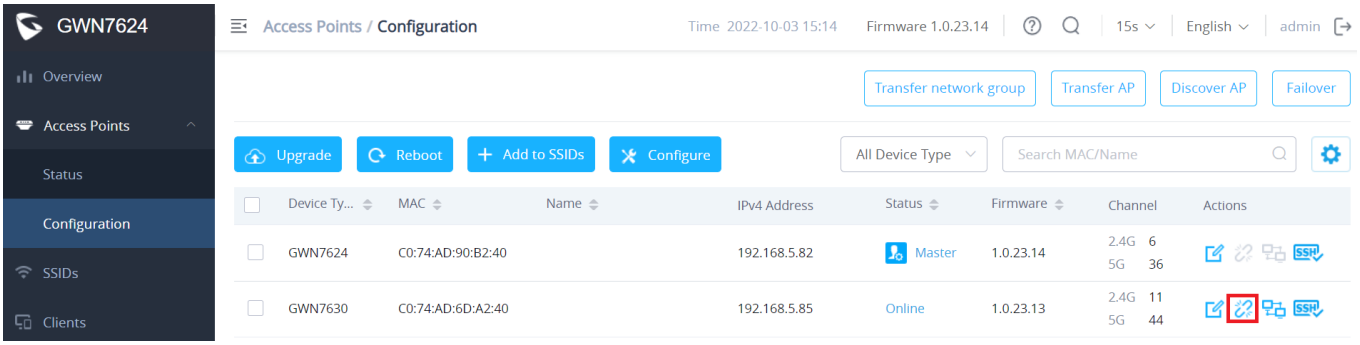


Discovered Devices

3. Click on Pair "**Link icon**" under Actions to pair the discovered access point as a subordinate with the

GWN76xx acting as the Primary.

After the access point appears online, select **Unpair** to remove it from the primary.



GWN76XX Online

If a GWN76XX is not being discovered or the pair icon is grey color, make sure that it is not being paired with another GWN76XX Access Point acting as Primary Controller. If yes, users will need to unpair it first, or reset it to factory default settings to make it available for pairing by other GWN76XX Access Point Controller

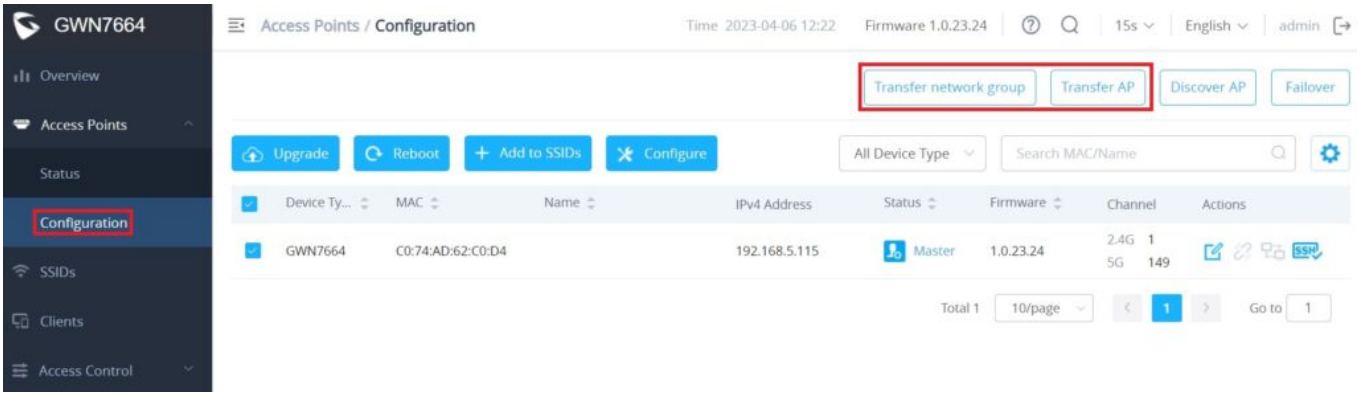
AP Location

To identify an access point by its blinking LED, open **Access Points -> Status** on the primary web GUI, then select **Locate** for the desired AP.

Transfer AP - Transfer Network Group

Select **Transfer AP** to transfer an access point from the local primary to **GDMS Networking** or **GWN Manager**. If the destination account already contains Network or Wi-Fi configurations, select an existing network or SSID when adopting the AP.

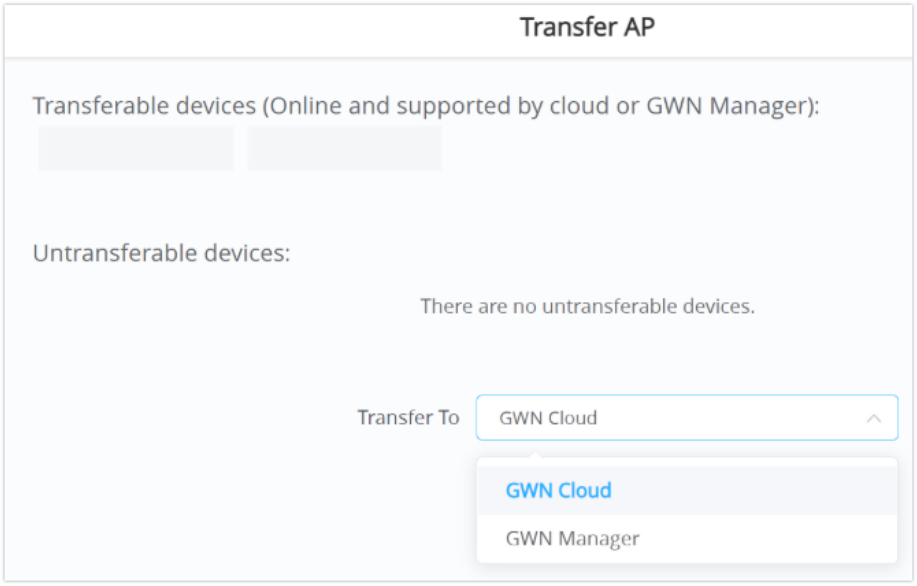
Navigate to **AP Web UI -> Access Points -> Configuration** page, please refer to the figure below:



Access points configuration page

Then select where to transfer the selected AP, either GDMS Networking or GWN Manager.

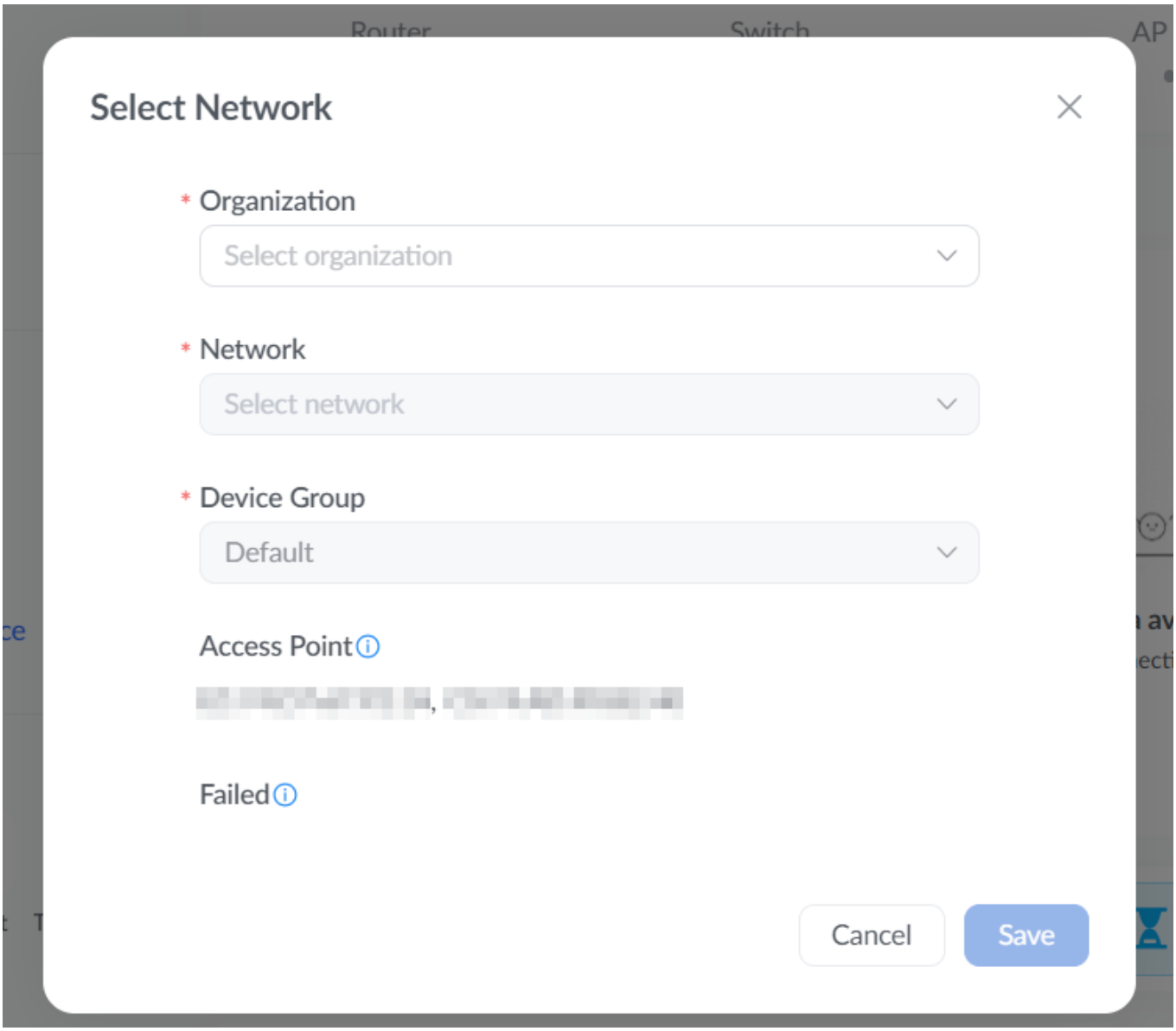
Then select where to transfer the selected AP, either GDMS Networking or GWN Manager.



Transfer AP

Transfer AP

After this step, you will be redirected to GDMS Networking or GWN Manager. In GDMS Networking, select the destination **Organization**, **Network**, and **Device Group**, then click **Save** to complete the transfer.



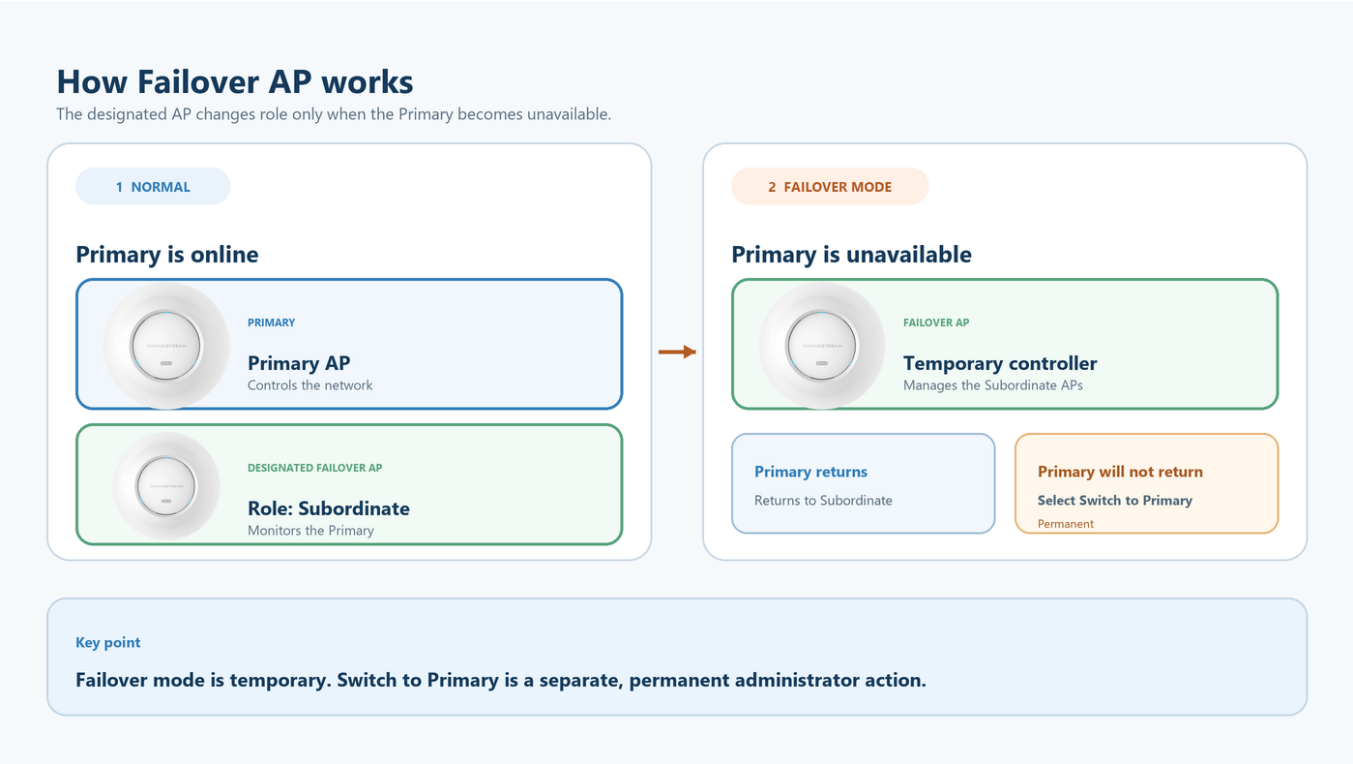
GDMS Networking - Select Network

Select **Transfer Configuration** to transfer the local configuration to the cloud account. For more details, please refer to the GDMS Networking - User Guide.

Failover AP

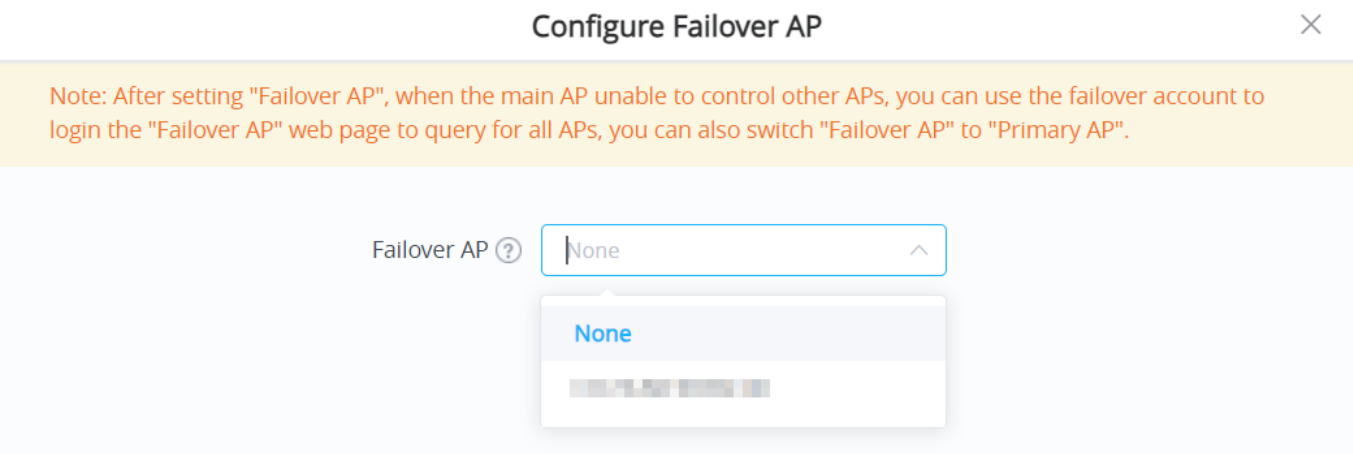
A **Failover AP** is a Subordinate AP designated to provide temporary controller redundancy in a Primary-Subordinate deployment. It receives the Primary AP's network configuration and monitors the Primary. If the Primary becomes unavailable, the Failover AP enters Failover mode and temporarily manages the remaining Subordinate APs. Detection and failover can take approximately 20 to 30 minutes.

If the original Primary returns, the Failover AP automatically returns to Subordinate mode. If the original Primary will not return, the administrator can sign in with the special **failover** account and select **Switch to Primary** to permanently promote the Failover AP to Primary.



How Failover AP works

To configure a Failover AP, log in to the Primary AP, navigate to **Access Points -> Configuration**, select **Failover**, and choose the Subordinate AP to designate.



Failover AP

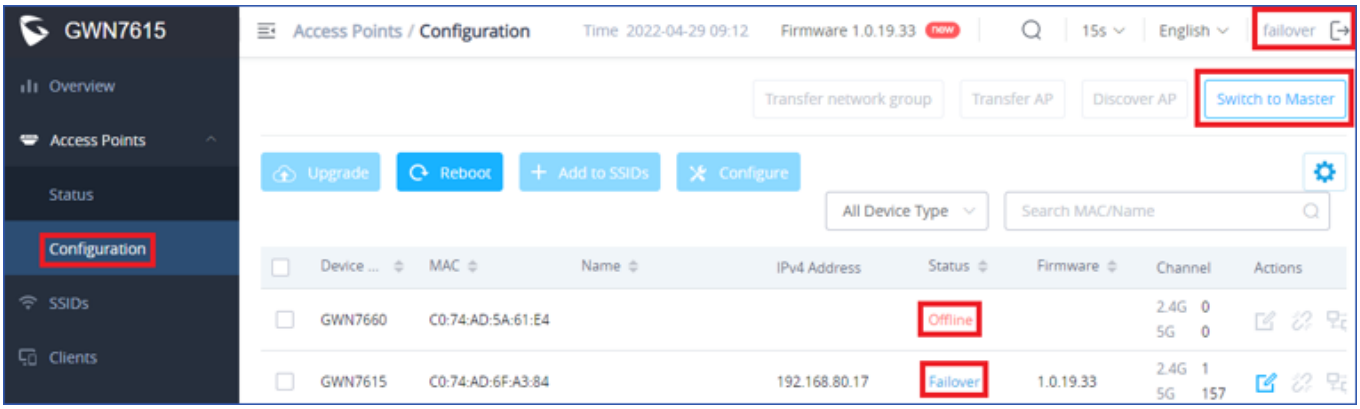
Failover Mode

After a Subordinate AP is designated, the Primary sends it the current network configuration. The Failover AP then monitors the Primary for conditions such as a network connection loss or power outage.

If the Primary becomes unavailable, the Failover AP enters Failover mode and temporarily manages the remaining Subordinate APs while waiting for the Primary to return.

During Failover mode, sign in to the Failover AP using the following credentials:

- **Username = failover**
- **Password = Primary AP administrator password**



Failover Mode GUI

In Failover mode, the web interface provides read-only access with limited operations. The administrator can still reboot managed Subordinate APs when needed.

If the original Primary will not return, select **Switch to Primary** to permanently promote the Failover AP to Primary. This restores full write access and transfers management of the remaining APs to the new Primary.

Selecting **Switch to Primary** is irreversible. The Failover AP becomes the new Primary, and the former Primary cannot automatically regain control.

After promotion, sign in to the new Primary with the username **admin** and the former Primary AP's administrator password.

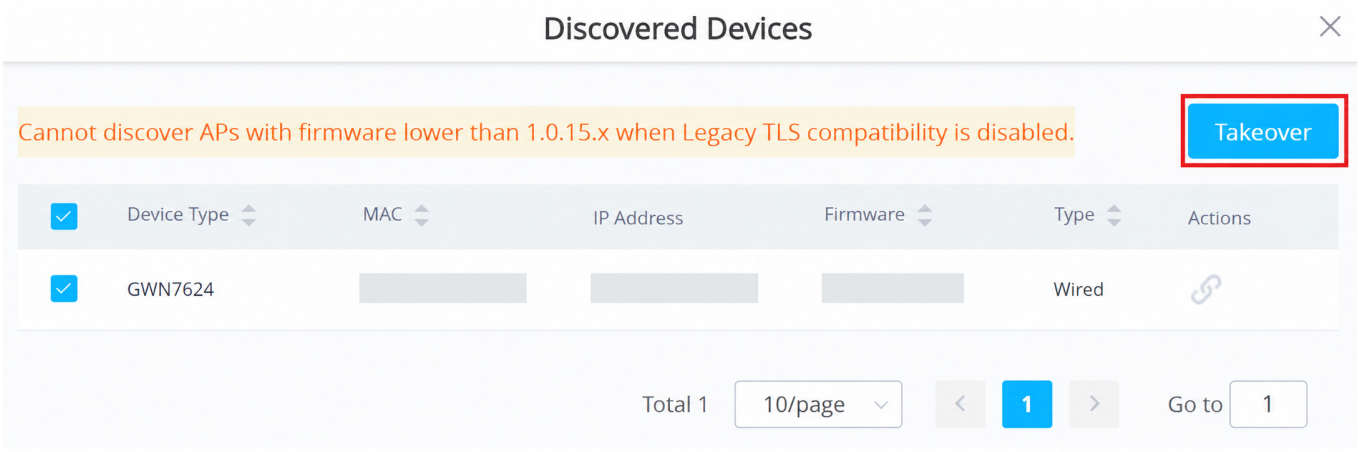
If you do not select **Switch to Primary** and the original Primary comes back online, the Failover AP automatically returns to Subordinate mode under the original Primary.

Takeover Feature

This feature re-pairs subordinate APs whose previous primary is offline with another primary AP on the same subnet.

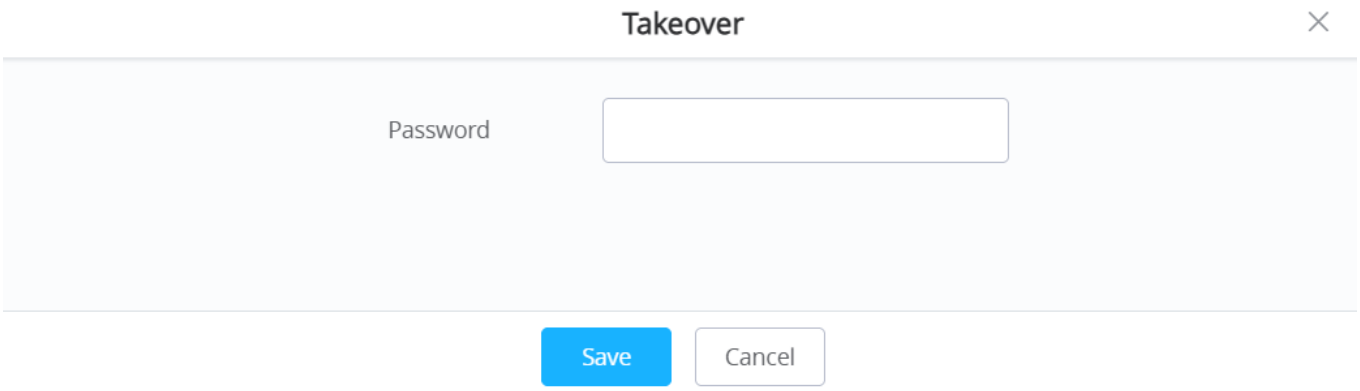
Step 1. Log in to the primary AP Web UI, open **Access Points -> Configuration**, then select **Discover AP**.

Step 2. Select one or more eligible discovered APs, then select **Takeover**.



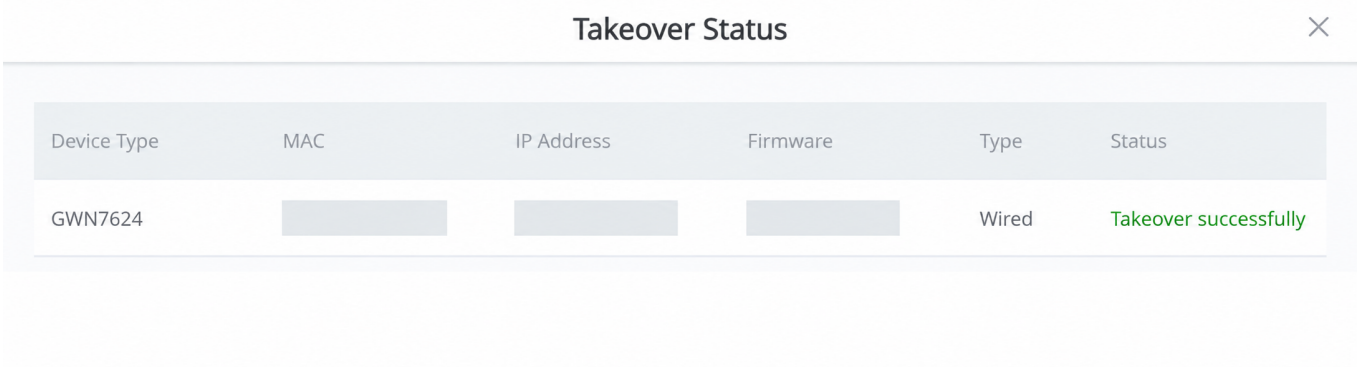
Selecting a discovered AP for takeover

Step 3. Enter the administrator password of the previous primary AP in **Password**, then select **Save**.



Entering the previous primary AP password

Step 4. Confirm that the AP displays **Takeover successfully** in the Takeover Status dialog.

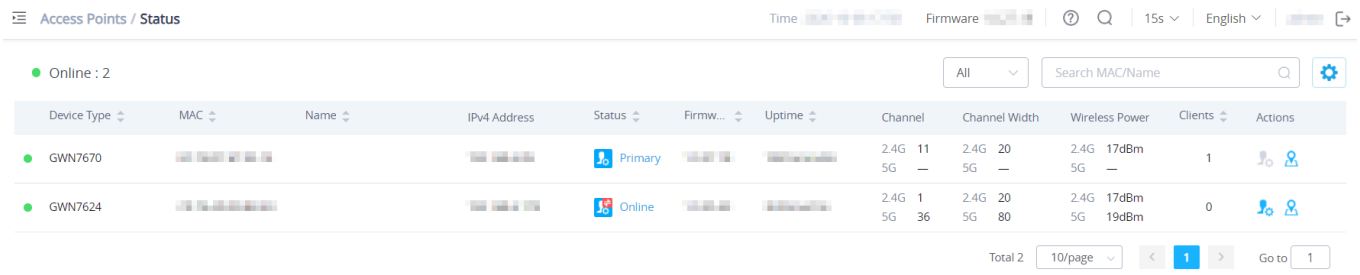


Successful AP takeover

Transfer to Primary

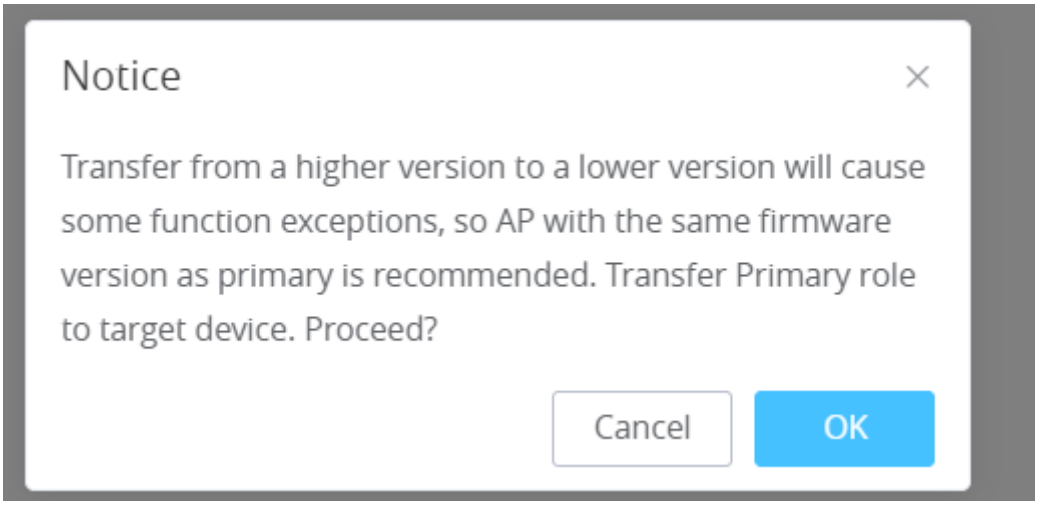
From the Primary Access Point, the Administrator does have the capability to assign any Secondary Access Point to become the new Primary to manage all the already paired Access points.

Navigate to **Web UI -> Access Points -> Status**, refer to the figure below:



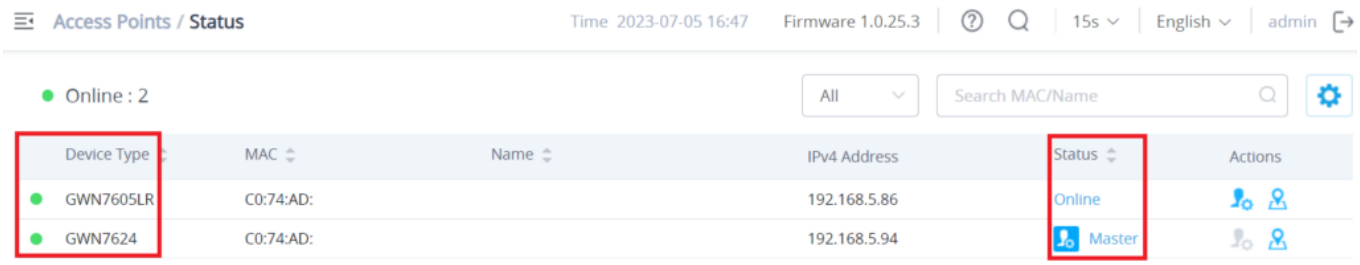
Switch to Primary

Select **Switch to Primary**. A warning message prompts you to confirm the operation.



Transfer Primary Role to another device confirmation message

When the process is finished, the original Primary will become a secondary for the new Assigned Primary, and to log in to the new Primary AP web interface, you will need to use the previous Primary Admin password.



The new assigned Primary AP web interface

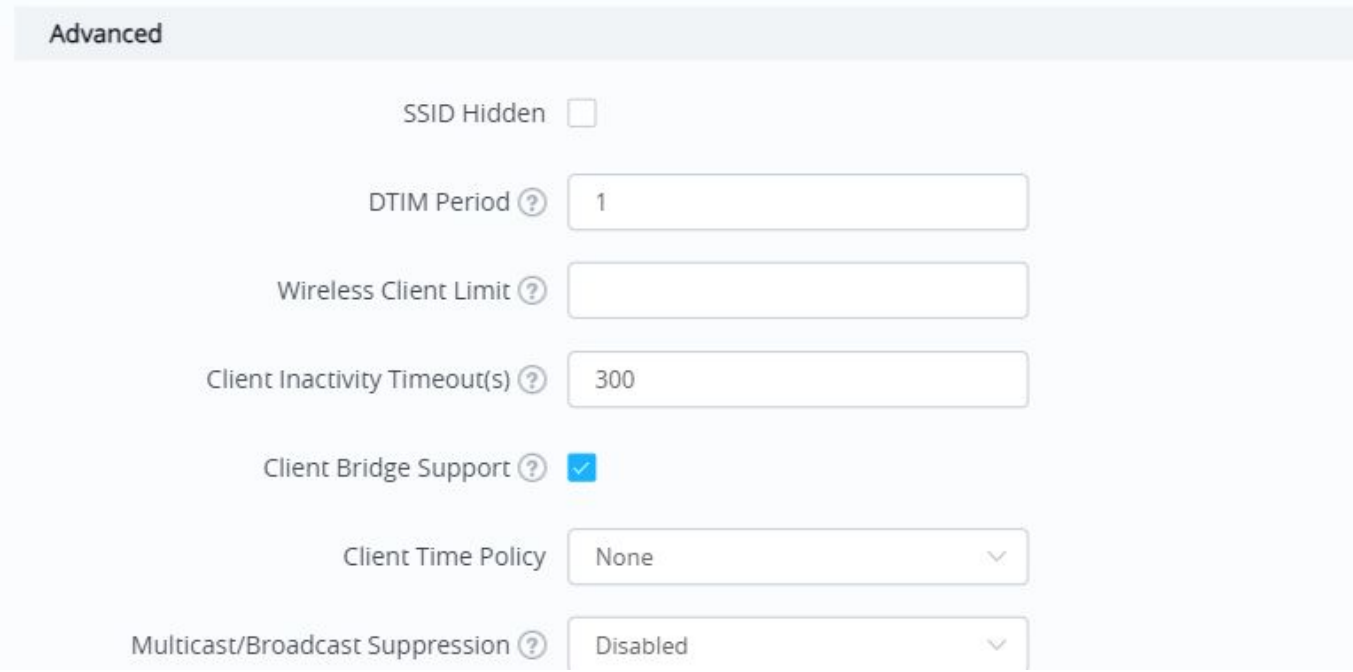
All the previously existed paired APs will be provisioned with the new Primary AP.

The Switch to Primary option is unlimited action and does not require any reset for the already paired APs.

Client Bridge

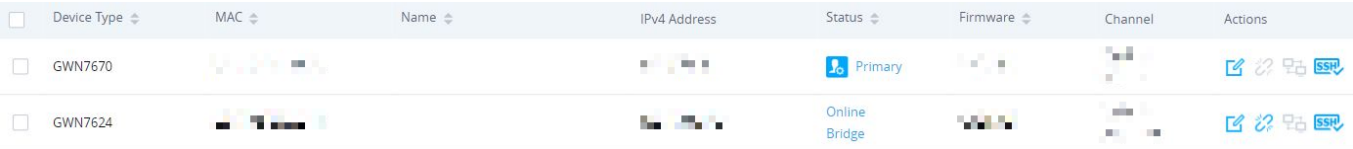
The Client Bridge feature allows an access point to connect wired-only devices to a wireless network through its LAN port. Client Bridge mode is separate from a mesh deployment, and an AP operating in this mode does not accept wireless clients.

To configure Client Bridge mode, navigate to **Wi-Fi -> SSID**, add or edit the SSID, set **Client IP Assignment** to **Bridge**, and enable **Client Bridge Support** under **Advanced**. Click **Save** to apply the SSID settings.



Enable Client Bridge Support

Next, navigate to **Access Points -> Configuration**. In the **Actions** column for the Secondary AP, select **Bridge** to convert the AP. When the conversion is complete, the **Status** column displays **Online Bridge**.



Client Bridge Status

Once an AP is converted to Client Bridge mode, it is no longer controlled as a normal Secondary AP by the Primary AP. A factory reset is required to return it to normal AP mode.

Assign a fixed IP address to the AP before activating Client Bridge mode.

Client Bridge Support must be enabled in the SSID settings.

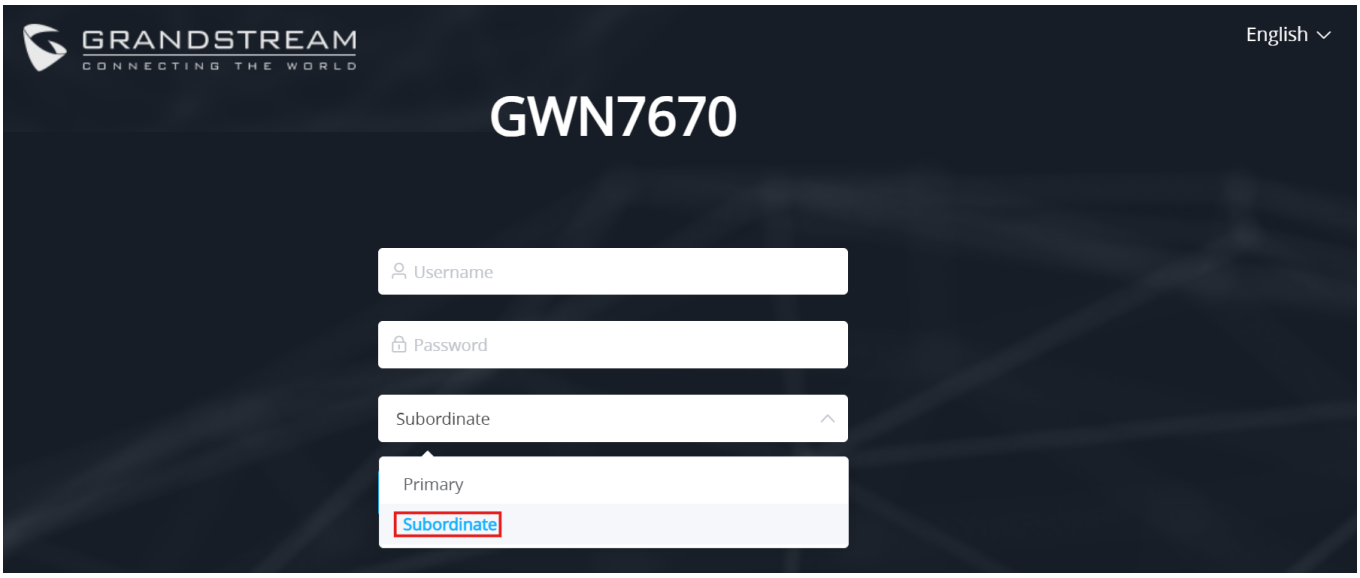
Client Bridge does not support 802.1X, PPSK without RADIUS, OSEN, WPA2/OSEN, MAC-Based RADIUS, or Captive Portal.

USING GWN76xx AS A SUBORDINATE ACCESS POINT

A GWN access point can be managed as a Subordinate by a Primary. The Primary can be another GWN access point, a GWN router, or GDMS Networking/GWN Manager.

If the GWN access point is added to either GDMS Networking or GWN Manager, the **Speed Test** feature will be available to users. For more details, please check GWN Management Platforms - User Guide (Configure a GWN Access Point).

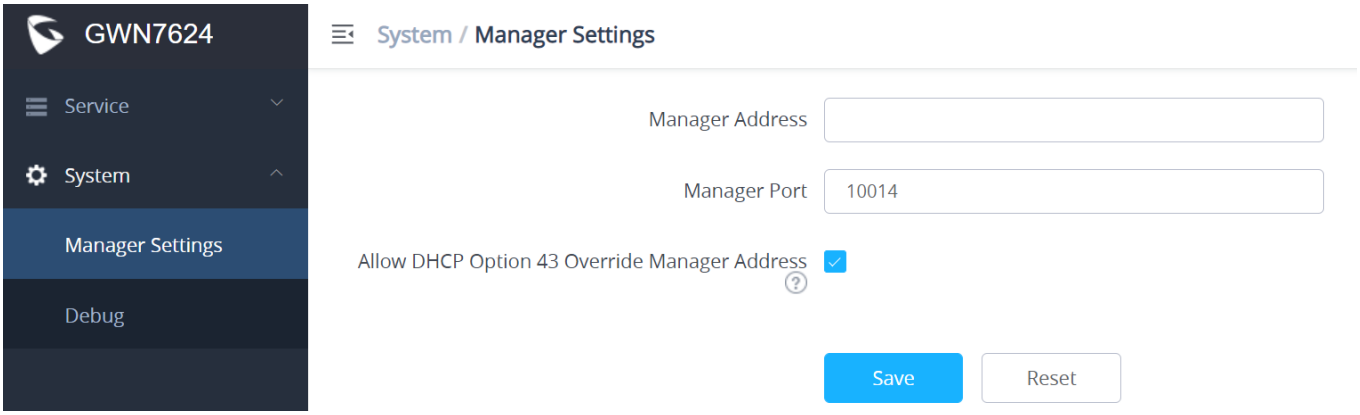
Subordinate mode allows users to access specific service and system settings.



GWN7670 Subordinate login page

Notes:

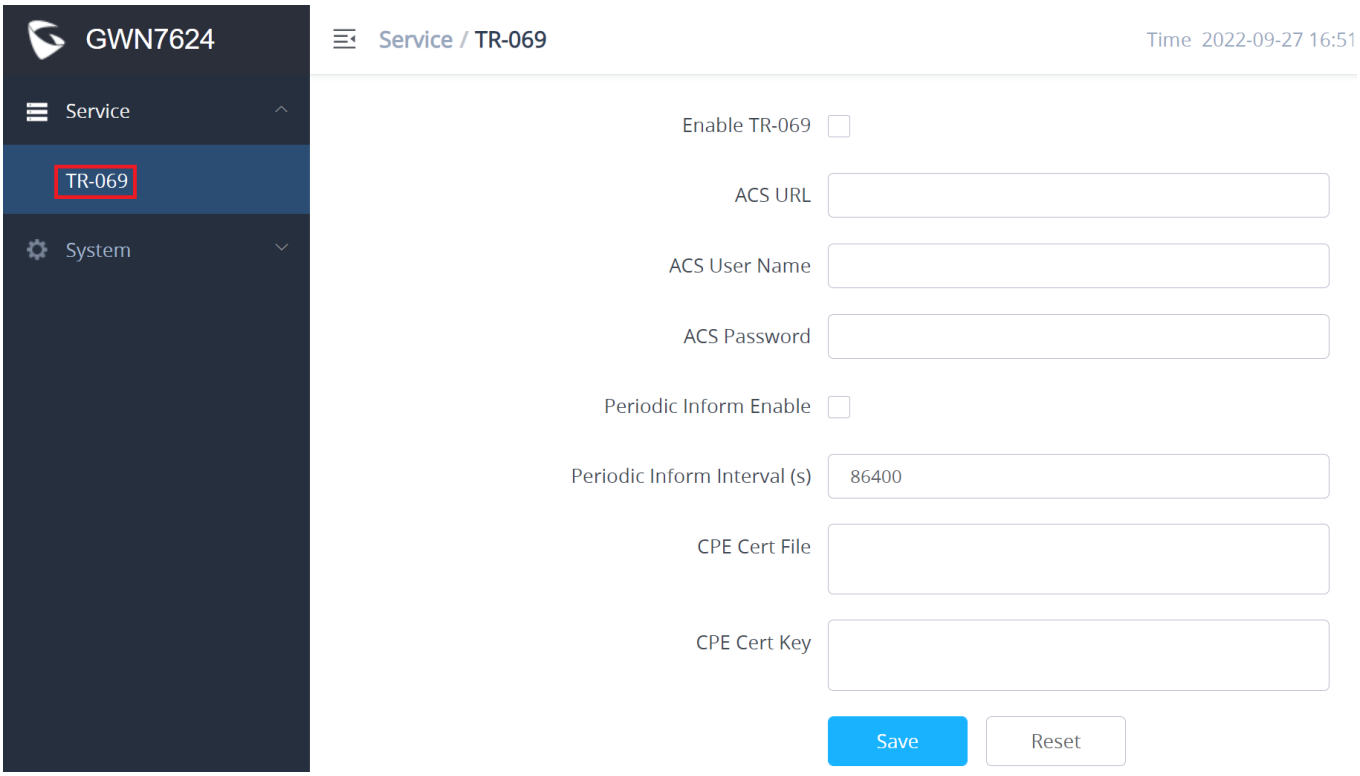
- If the AP is managed as a Subordinate by a Primary AP, the default username is admin, and the default password is the Primary AP's administrator password.
- If the AP is managed by GDMS Networking, the default username is admin, and the default password is the SSH Password configured under GDMS Networking -> System -> Settings.



Subordinate AP Web Interface

Service

The TR-069 interface page allows the settings to enable remote and safe configuration of network devices. Refer to section [TR-069] for details regarding each field.



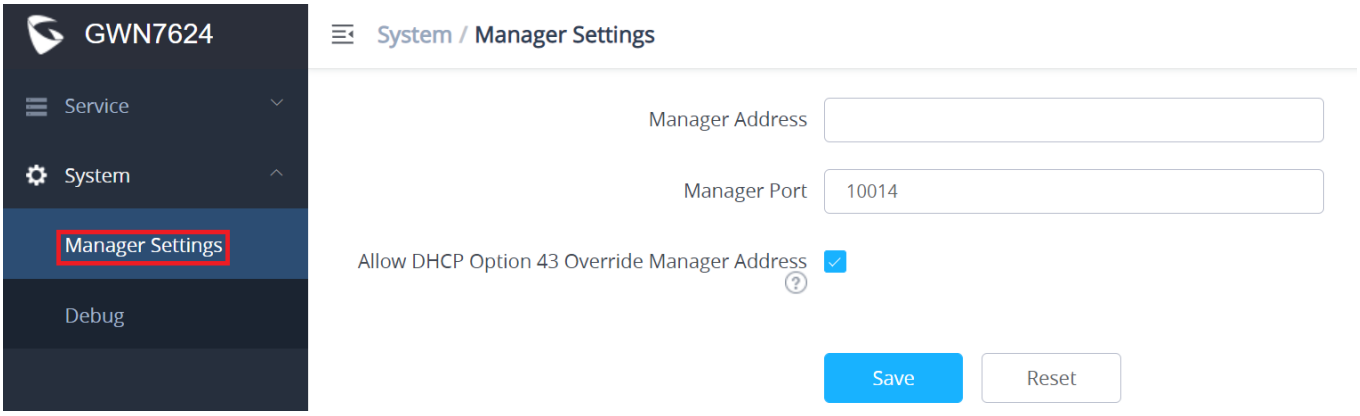
Subordinate AP Service Settings

System

The system section provides access to the Manager settings and Debug sections.

Manager Settings

The Primary (Manager Address) and Port can be found here to be discovered by the Manager.



Subordinate AP manager settings

Manager Address	Enter the IP address of the GWN Manager
Manager Port	Enter the port set for the GWN Manager
Allow DHCP Option 43 Override Manager Address	This configuration will not be effective if AP has been managed by cloud.

Manager settings

Debug

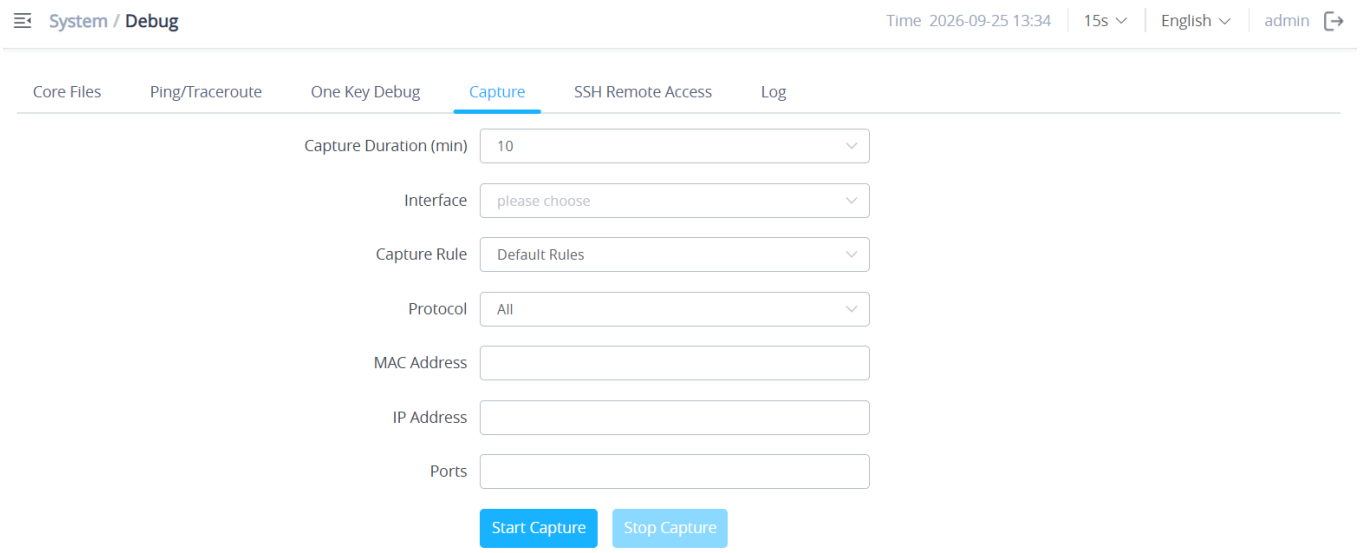
The subordinate AP web interface provides the following troubleshooting tabs under **System > Debug**.

Core Files: Displays core dump files generated after a crash for engineering analysis.

Ping/Traceroute: Runs ping and traceroute tests against a target IP address or URL.

System Debug: Collects Wireless, Portal, or Mesh troubleshooting data. **One Key Debug** generates a single package, while **Continuous Trace** captures logs until stopped and may increase CPU load or affect network performance. Generated packages are encrypted and stored under **Core Files**.

Capture: Captures packets directly from the subordinate AP web interface. Set the capture duration and interface, then optionally narrow the capture by rule, protocol, MAC address, IP address, or port before selecting **Start Capture**. Select **Stop Capture** to end an active capture.

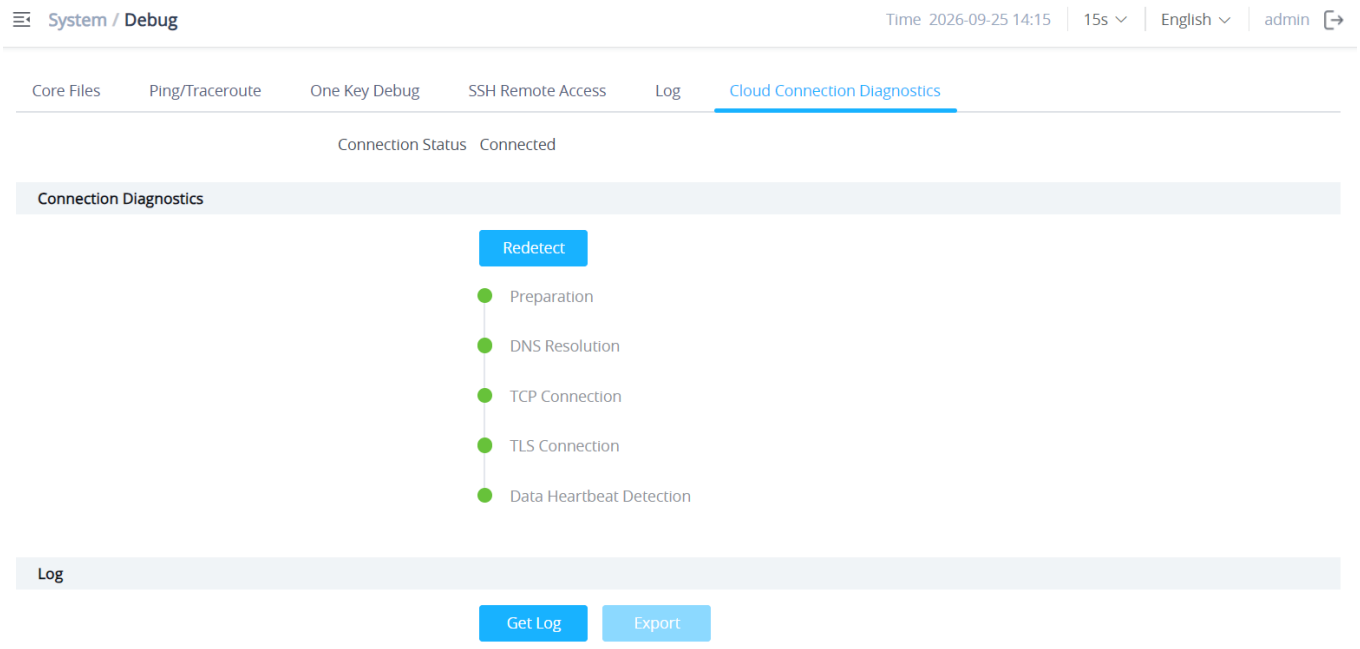


Packet capture on a GWN7670 running firmware 1.0.27.18 in subordinate mode

SSH Remote Access: Enables SSH remote access on the subordinate AP.

Log: Retrieves logs generated for troubleshooting.

Cloud Connection Diagnostics: Available on the local web interface when the subordinate AP is managed by GDMS Networking. It displays the cloud connection status and checks Preparation, DNS Resolution, TCP Connection, TLS Connection, and Data Heartbeat Detection. Select **Redetect** to run the checks again. Select **Get Log** to display the timestamped diagnostic log, then select **Export** to download it.



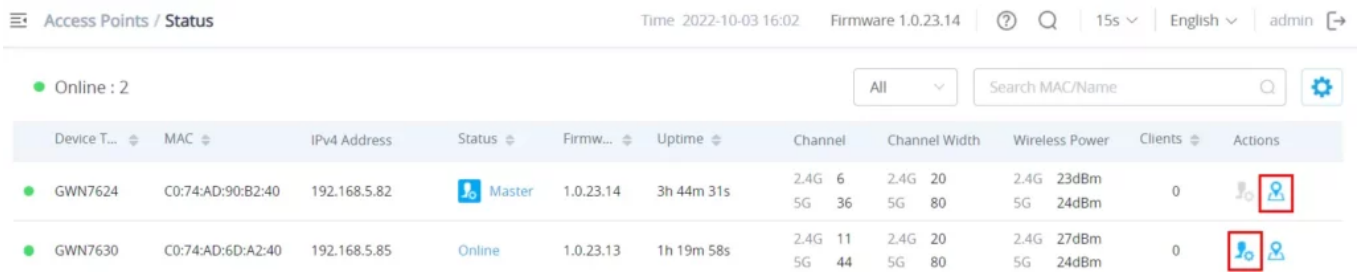
Cloud Connection Diagnostics on a GDMS-managed access point

ACCESS POINTS

From the access points page, the administrator can monitor different information regarding the access points of the selected network. This section is separated into 2 sub-sections: **Status and Configuration**.

Status

The **Status** page displays all access points assigned to the selected network. From this page, you can perform basic operations such as locating devices (initiating LED blinking in white) or switching a **Subordinate AP** to a **Primary AP**. Additionally, users can view detailed information about each access point and access a suite of debugging tools to diagnose and resolve issues effectively.

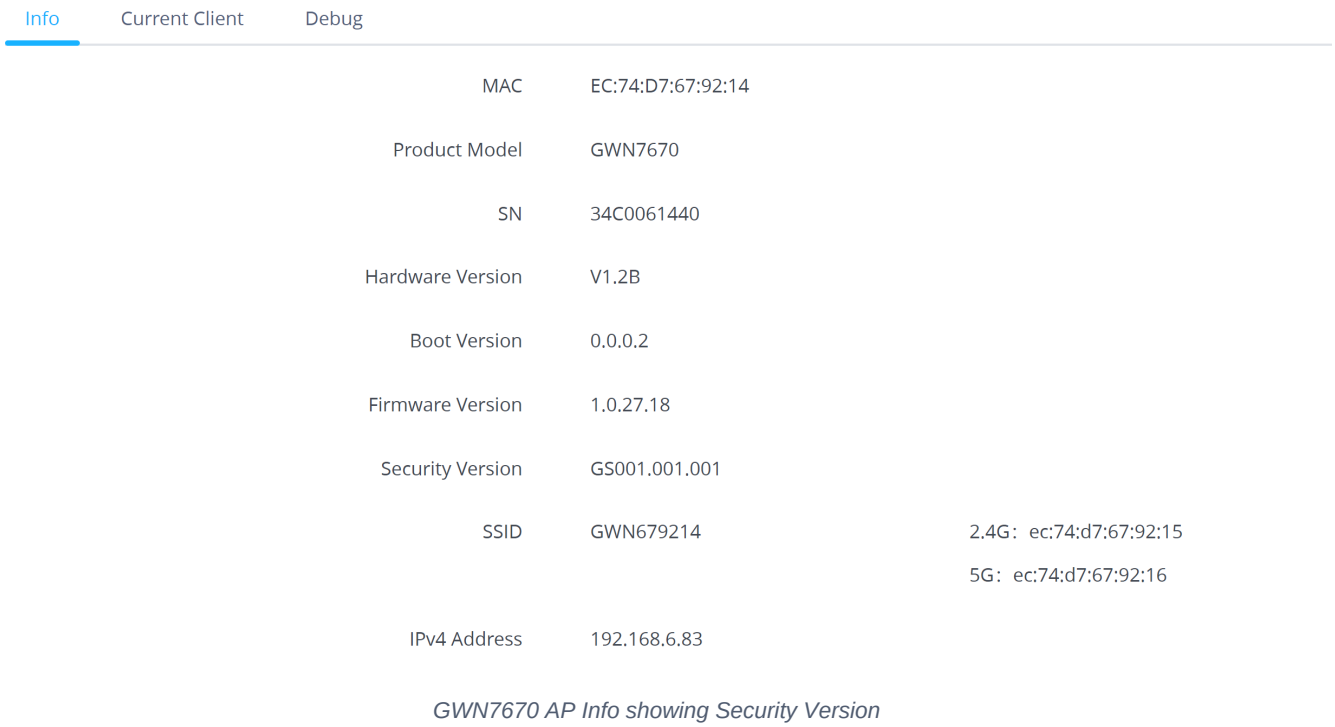


Access Points - Status

- To locate the access point, click the **Location Icon** (refer to the figure above). Once clicked, the LED on the access point will start blinking continuously until it is manually turned off.
- To transfer a **Subordinate Access Point (AP)** to a **Primary AP**, click the **Role Switch Icon** located next to the **Location Icon**. This action will swap the roles: the Subordinate AP will become the Primary, and the current Primary AP will switch to a Subordinate.

The new Primary AP will use the password of the previous Primary AP.

To get more detailed information about the status of a specific access point, users can click on the desired AP then a page similar to the following will show up:



GWN7670 AP Info showing Security Version

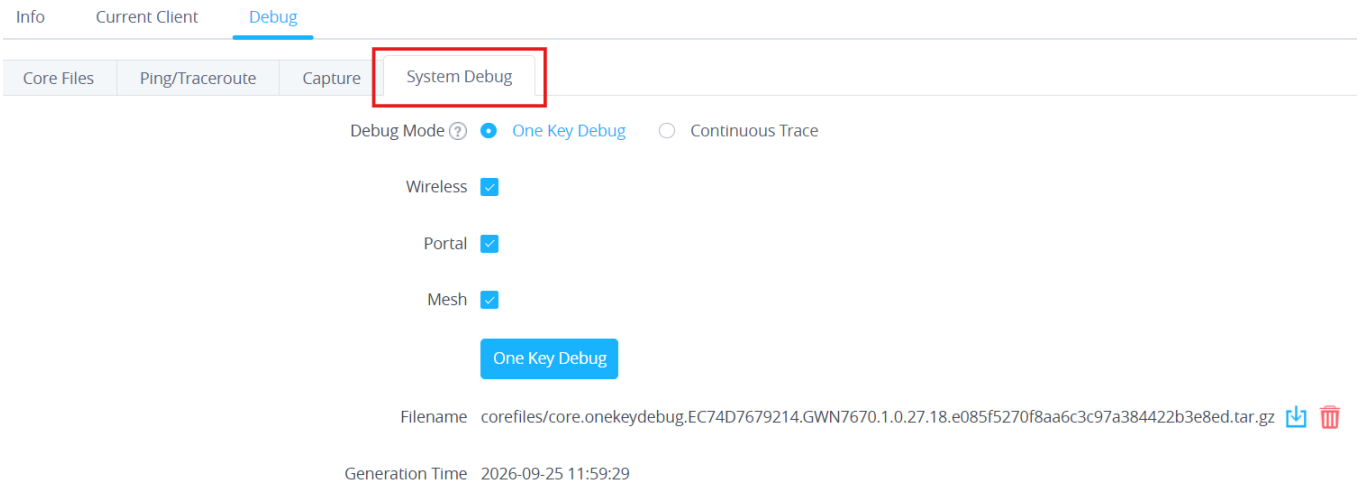
Basic info	Connector Typ : LC
	Wavelength: 850nm
	Transfer Distance : OM1:200m OM2:300m OM3:0m OM4:0m
	Speed : 2.44Gbps
Manufacture information	Vendor Name : OEM-W
	Vendor Part Number : SFP-2.5G-T
	Vendor Serial : PQH429J
	Manufacturing Date : 2023-03-24
	Version : A
Diagnostic info	DDM Support : Yes
	Temperature : +34.113°C
	Voltage : 3.32V
	Bias Current : 6.00mA
	Tx Power : -3.01dBm
	Rx Power :

GWN7660ELR AP Info - Example

The information displayed varies according to the hardware and software of each GWN76xx model, including port types, port speeds, and additional information fields.

The first tab, **Info**, shows general information about the access point, including the firmware version, security version, IP address, and uptime. The second tab, **Current Client**, displays the clients connected to this AP. The last tab, **Debug**, provides the following troubleshooting tools:

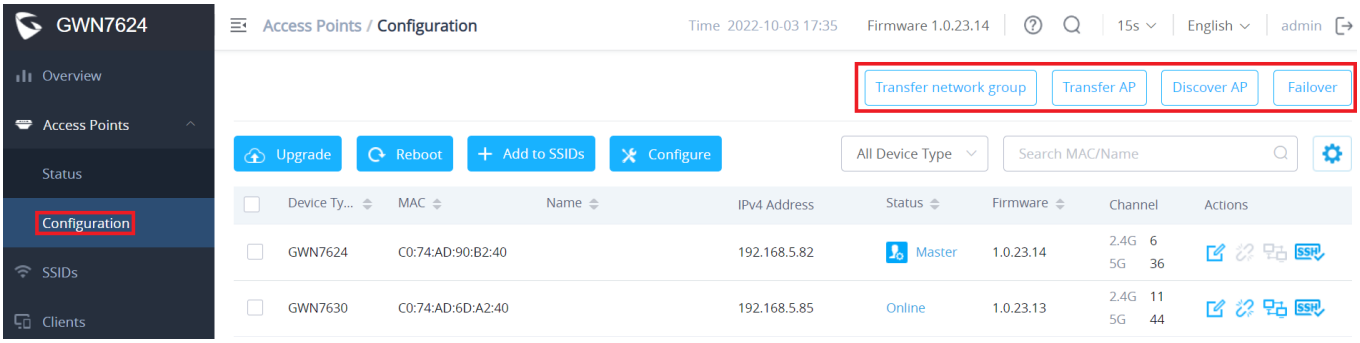
- **Core Files,** When a crash event happens on the unit, it will automatically generate a coredump file that can be used by the engineering team for debugging purposes.
- **Ping/Traceroute** tools, such as the **ping** utility, **traceroute** tool.
- **Capture** helps to capture traffic based on duration, interface, protocol, MAC address, IP address, and ports, and there is also the option for custom rules.
- **System Debug** captures Wireless, Portal, or Mesh troubleshooting data. Select **One Key Debug** to generate a single package, or **Continuous Trace** to capture logs continuously until stopped. Continuous Trace can increase CPU load and affect network performance. Generated System Debug packages are encrypted and stored under **Core Files**.



System Debug with a generated troubleshooting package

Configuration

The configuration page allows the administrator to Upgrade, Reboot, Add to SSIDs, Configure, Transfer network group, Transfer AP, Discover AP, Failover.



GWN7624 Configuration Page

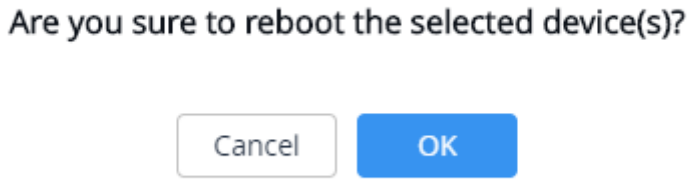
Upgrade

Select the subordinate access points, then select **Upgrade**.

Refer to [Upgrading Subordinate Access Points] for more details.

Reboot subordinate AP

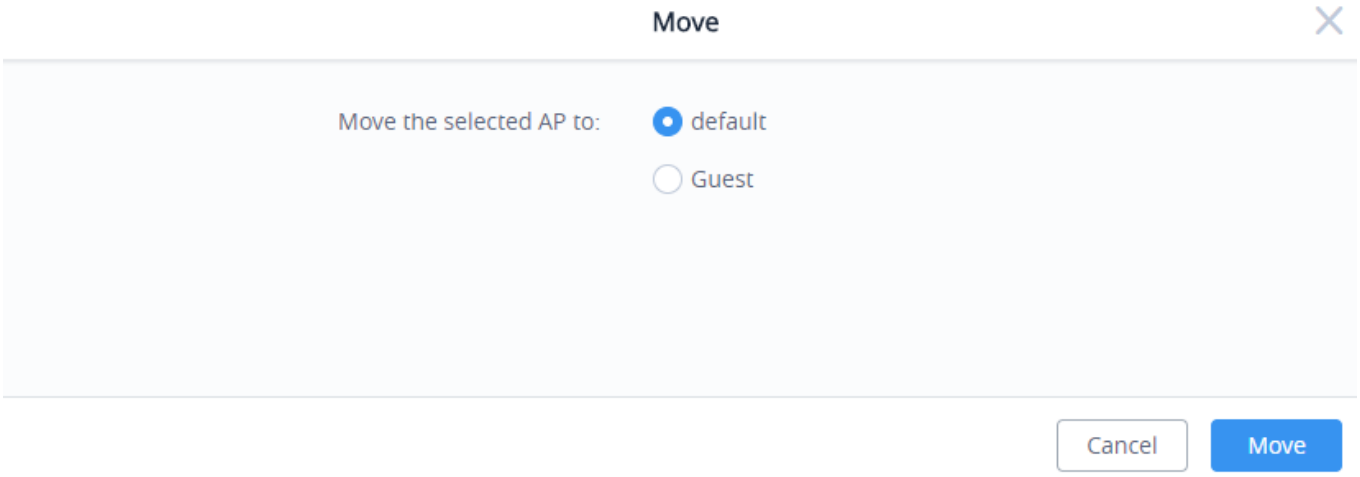
To reboot a subordinate access point, select it, then select **Reboot**. A confirmation message appears.



Reboot Access Point

Move Access Points

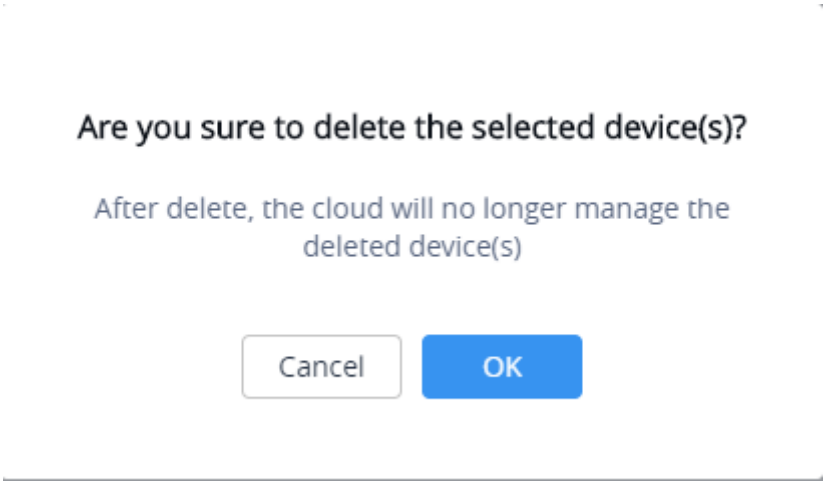
The administrator can move GWN Access points from one network to another. Click on Move button and the following window will popup, select the network where to move the access point and click on move.



Moving Access Points between Networks

Delete Access Points

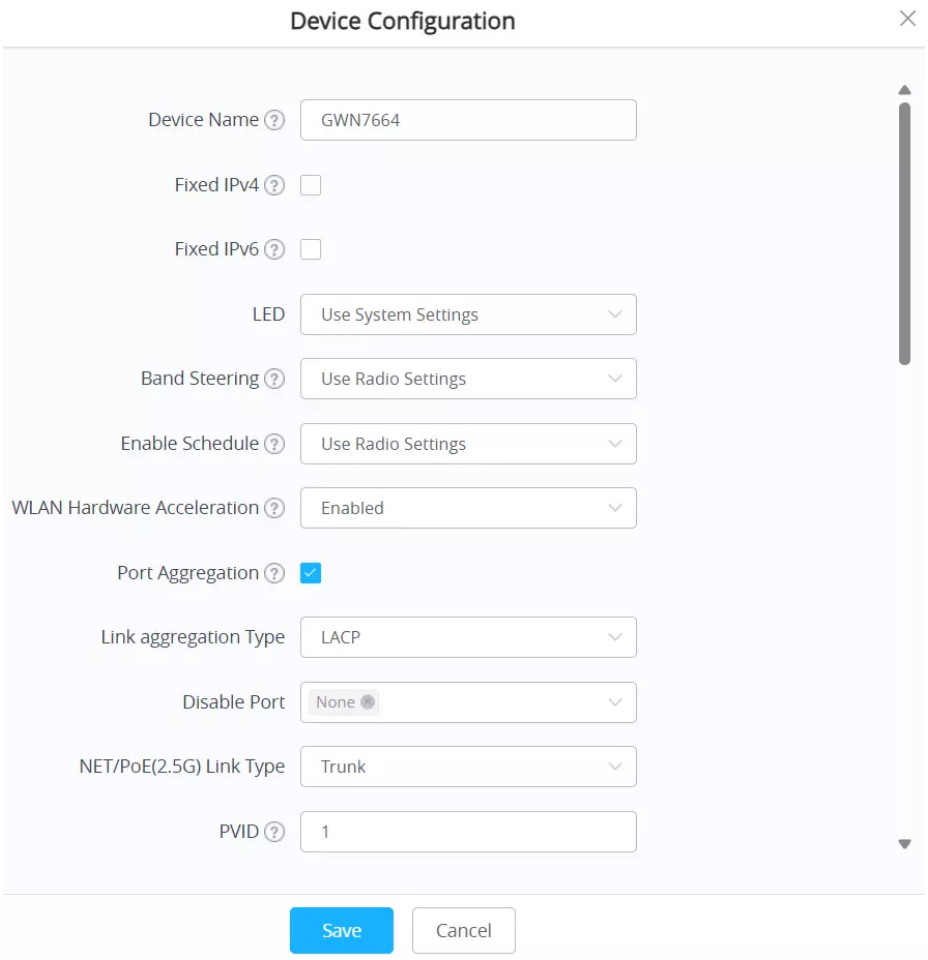
To delete an access point, select it, then click on the reboot button. The following confirmation message will be displayed:



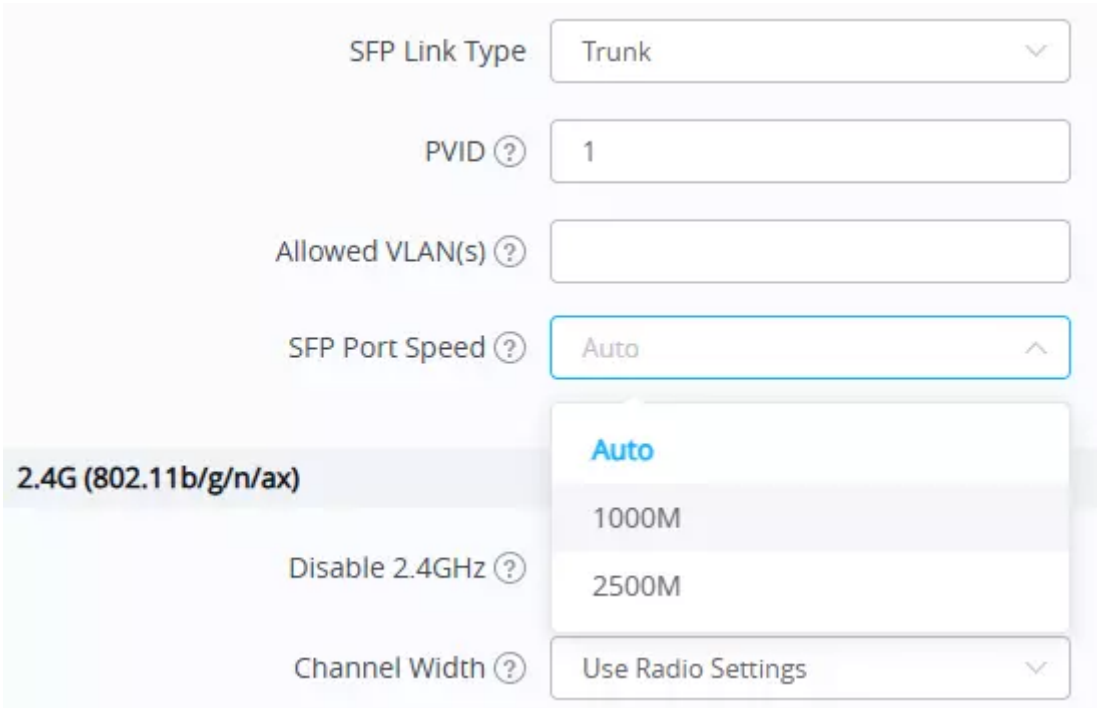
Delete Access Point

Configure Access Points

To configure an access point, select it, then select **Configure**. The configuration page opens.



Access Point Configuration Page - Example GWN7664



Access Point Configuration Page - Example GWN7660ELR

The number of ports, their types and speeds, as well as the supported wireless bands, vary based on the hardware specifications of the access point model.

The following settings can be configured from this page:

Device Name	Set GWN76xx's name to identify it along with its MAC address.
Fixed IPv4	Check this option to configure the device with a static IP configuration; it must be in the same subnet with the default Network Group; Once enabled, these fields will show up: IPv4 Address/IPv4 Subnet Mask/IPv4 Gateway/Preferred IPv4 DNS/Alternate IPv4 DNS.
Fixed IPv6	Check this option to configure the device with a static IP configuration; it must be in the same subnet with the default Network Group; Once enabled, these fields will show up: IPv6 Address/IPv6 Prefix Length/IPv6 Gateway/Preferred IPv6 DNS/Alternate IPv6 DNS.
Power Input Mode	Select the power input mode used by the access point. When PoE+ is selected, an access point that supports PSE can provide PoE output.
LED	Configure the LED: Four options are available: Use System Settings, Always on, Always off, or Schedule.
Band Steering	Band Steering will help redirect clients to a radio band 2.4G or 5G, depending on what is supported by the device, to increase efficiency and benefit from the maximum throughput.Four options are allowed:* Disable Band steering: This will disable the band steering feature and the access point will accept the band chosen by the client.* 2G in Priority: 2G Band will be prioritized over 5G Band.* 5G in Priority: 5G Band will be prioritized over 2G BandBalance: Band Steering will balance between the clients connected to 2G and 5G.* Use Radio Settings: GWN will use the value configured under Radio page.
Enable Schedule	Configure a schedule for when the Wi-Fi will be ON or Off, by default it is disabled. The user can enable it and select a schedule from the drop-down list or use radio settings.
WLAN Hardware Acceleration	This setting enables or disables hardware acceleration for WLAN operations. When enabled, the access point utilizes hardware resources to accelerate WLAN processing, potentially improving performance.Options:Enabled: Activates hardware acceleration. Disabled: Deactivates hardware acceleration.Note: Changes to this setting will take effect after the device reboots.
Fast SSID Build	When enabled and there are fewer than 8 SSIDs on the access point, creating or deleting SSIDs takes effect more quickly. This setting controls how fast the AP rebuilds SSIDs and can inherit the value from the radio settings.Note: This feature is not supported on SSIDs using MLO or WPA2/WPA3 with PPSK without RADIUS.
Port Aggregation	Enables bonding of Ethernet ports into a single logical uplink. Increases total bandwidth and provides link redundancy.Note: Must be supported on the peer device.
Link aggregation Type	Select the bonding method: LACP (dynamic negotiation) or Static (manual config).Note: Both sides must match to form a valid link group.
Disable Port	Select "NET" from the drop-down list to disable the Ethernet the NET port.
NET1/PoE(2.5G) Link Type / NET2/2.5G Link Type	Configure the link type for each available Ethernet port. On the GWN7670, the fields are NET1/PoE(2.5G) Link Type and NET2/2.5G Link Type. Each port can be configured as Trunk or Access.Note: The hardware specifications of the access point model determine the number of ports, their types and speeds.
PVID	Configures the VLAN ID of the port
Allowed VLAN(s)	Configure the VLAN ID(s) allowed to pass through the port. Multiple VLAN IDs can be entered such as 1,2,3,7. Up to 16 VLAN IDs can be configured. If no value is configured, the port allows all VLANs
2.4G/5G (802.11b/g/n/ax)	
Disable 2.4GHz / Disable 5GHz	Use Disable 2.4GHz or Disable 5GHz to disable the corresponding radio band on the access point.
Channel Width	Choose the Channel Width, note that wide channels will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in a very high-density environment. Default is "Use Radio Settings", the AP then will use the value configured under the Radio page.

Channel	Select Use Radio Settings, or a specified channel, default is Auto. Note that the proposed channels depend on Country Settings under System Settings -> Maintenance. Default is "Use Radio Settings", the AP then will use the value configured under Radio page.
Radio Power	Set the Radio Power according to the desired cell size. Available options are Low, Medium, High, Custom, and Use Radio Settings.When Custom is selected for the 2.4 GHz radio, enter the transmit power in Custom 2.4GHz Wireless Power (dBm). The default is Use Radio Settings, which applies the value configured on the Radio page.
Enable Minimum RSSI	Configure whether to enable/disable Minimum RSSI function. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.
Minimum Access Rate Limit	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and APs. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.
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.

Access Point Configuration Settings

The administrator can filter access points by Model or search by name/MAC of the device. Click on Save Button to save the changes and apply them to the AP.

Port Aggregation

Link Aggregation (also known as Port Bonding or LAG) allows GWN76xx access points to combine multiple Ethernet ports into a single logical uplink. This setup provides increased bandwidth and ensures redundancy in case one connection fails.

GWN76xx access points support two LAG types:

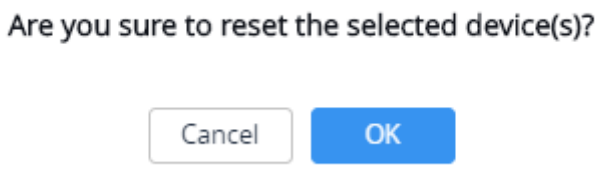
- **Static**: Manually configured, no negotiation required.
- **LACP (IEEE 802.3ad)**: Dynamically negotiates the link with supported devices.

For proper operation, make sure both connected ports use the same speed and aggregation mode.

For detailed configuration steps, best practices, and supported models, see the full guide: **GWN76xx - Link Aggregation Guide**

Reset Access Points

To reset an access point, select it, then select **Reset**. Select **Confirm** in the confirmation message.

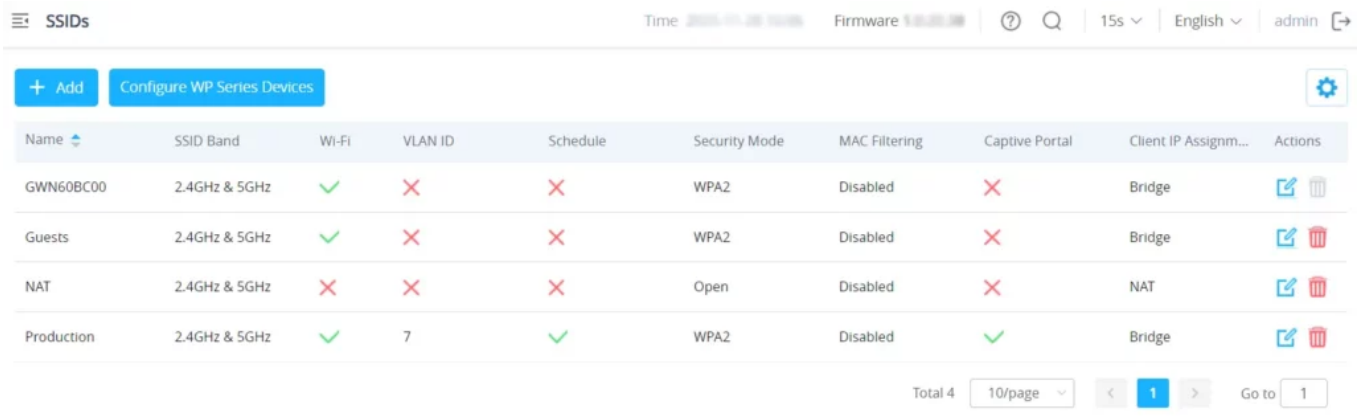


Reset Access Point

SSIDs

When using GWN76XX as Primary Access Point, users can create different SSIDs and assign GWN76XX Subordinate Access Points to them.

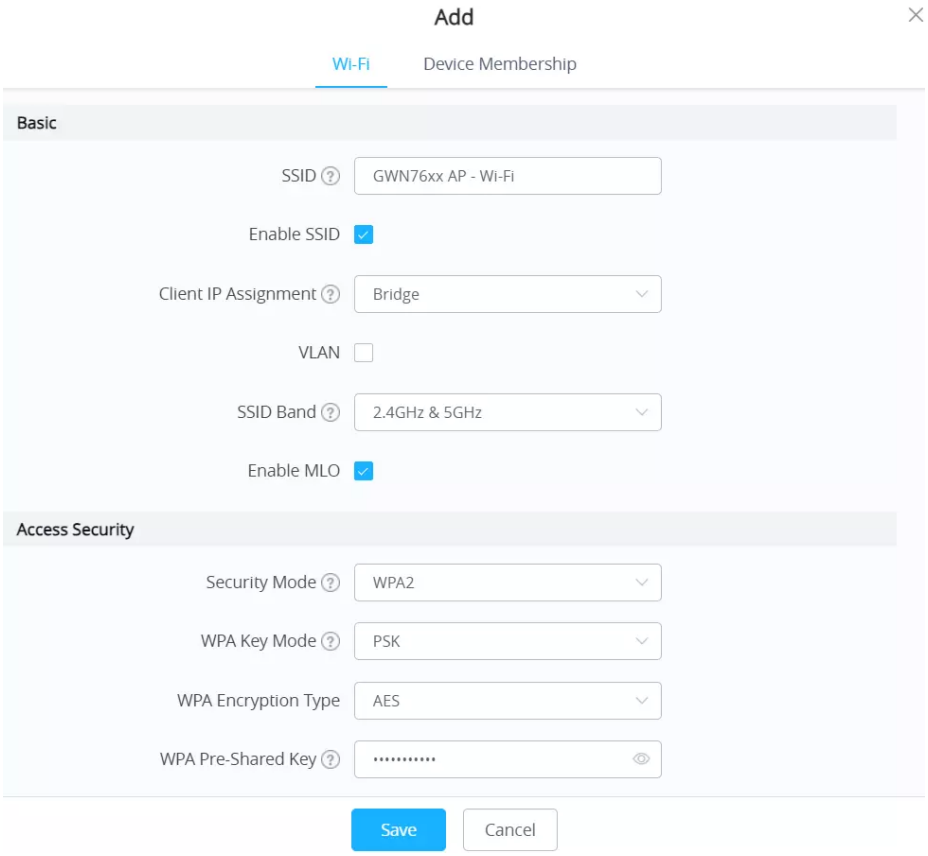
Log in as Primary to the GWN76XX Web GUI and open **SSIDs**. On models that display the **Wi-Fi** menu, open **Wi-Fi > SSID**.



SSIDs

On models that display the **Wi-Fi** menu, the SSID page is located at **Wi-Fi > SSID**. The configuration options are the same; only the menu location differs.

To create a new SSID, click on "**Add**" button.



Add a new SSID

When editing or adding a new SSID, users will have two tabs to configure:

- **Wi-Fi:** Please refer to the below table for Wi-Fi tab options

Basic	
SSID	Set or modify the SSID name.
Enable SSID	Check to enable Wi-Fi for the SSID.
Client IP Assignment	If set to Bridge mode, it allows the AP to pass the client's traffic to the network without modifying it, making the AP function transparently.If set to NAT mode, clients will get the IP addresses from the specified NAT pool. And clients connected to different APs are isolated from each other.
VLAN	Enable VLAN tagging for the SSID. This option is available when Client IP Assignment is set to Bridge.
VLAN ID	Enter the VLAN ID corresponding to the SSID. This is available when Client IP Assignment is set to Bridge and VLAN is enabled.
SSID Band	Select the Wi-Fi band the GWN AP will use: 2.4GHz, 5GHz, or 6GHz for Wi-Fi 6E models.
Enable MLO	Enables Multi-Link Operation (MLO), which allows simultaneous use of multiple links (e.g., on 2.4GHz, 5GHz and 6GHz) to enhance throughput and reliability.Note: Supported only on the Wi-Fi 7 AP.
Access Security	
Security Mode	Select the security mode used by the SSID. Available modes depend on the access-point model and selected radio band.WEP 64-bit: Uses a static 64-bit WEP key.WEP 128-bit: Uses a static 128-bit WEP key.WPA/WPA2: Supports PSK or 802.1X authentication.WPA2: Supports PSK, PPSK, Easy PSK, or 802.1X authentication.WPA2/WPA3: Supports SAE-PSK or 802.1X authentication.WPA3: Supports SAE, PPSK, or 802.1X authentication.WPA3-192: Uses 802.1X authentication with GCMP-256 or CCMP-256 encryption.OWE: Encrypts wireless traffic without requiring a pre-shared key.OSEN: Supports Hotspot 2.0 Release 2 online signup provisioning.Open: Does not require authentication and is not recommended for secured networks.Note: 802.1X authentication requires an external AAA server that supports PEAP-MSCHAPv2 or EAP-TLS.
WEP Key	Enter the WEP key. This field is available when Security Mode is set to WEP 64-bit or WEP 128-bit.
WPA Key Mode	Select the authentication method used by the SSID. Available modes depend on the selected Security Mode.PSK / SAE / SAE-PSK: Authenticates clients with a shared wireless password.802.1X: Authenticates clients through a RADIUS server.PPSK without RADIUS: Uses locally managed private pre-shared keys.PPSK with RADIUS: Uses private pre-shared keys with RADIUS authentication.Easy PSK: Combines pre-shared keys with RADIUS so different users or devices can use unique Wi-Fi passwords on the same WPA2 SSID. Clients connect with their assigned Wi-Fi password and do not enter 802.1X credentials. The AP uses RADIUS to identify the matching key or policy without requiring MAC-based RADIUS onboarding. Easy PSK is available only when Security Mode is set to WPA2. When selected, WPA Encryption Type is limited to AES; MAC-Based RADIUS, 802.11r, and Voice Enterprise are unavailable.Configure Easy PSK:Open Wi-Fi -> SSID, then add or edit an SSID.Set Security Mode to WPA2 and WPA Key Mode to Easy PSK. The interface limits WPA Encryption Type to AES.Enter the primary RADIUS Server Address, RADIUS Server Port (1812 by default), and RADIUS Server Secret. Enable and complete Secondary RADIUS Server when redundancy is required.Configure the external RADIUS service with the Easy PSK user and key policy required for the deployment, then save the SSID.Note: PPSK is supported with WPA2. Wi-Fi 7 models also support PPSK with WPA3.On models that display the Wi-Fi menu, manage PPSK profiles under Wi-Fi -> PPSK. Otherwise, use Access Control -> PPSK.
WPA Encryption Type	Select the encryption algorithm used by the selected security mode.AES: Uses the Advanced Encryption Standard.AES/TKIP: Allows AES and Temporal Key Integrity Protocol for compatibility with older clients.Note: Available choices depend on the selected Security Mode.

WPA Pre-Shared Key	Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters. This field is available only when "Security Mode" is set to "WPA/WPA2", "WPA2", "WPA2/WPA3" or "WPA3".
802.11w	Configure Protected Management Frames (802.11w) to protect management traffic against forgery and replay attacks.Disabled: Does not require 802.11w.Optional: Allows clients with or without 802.11w support.Required: Allows only clients that support 802.11w.
MAC-Based RADIUS	Once enabled, the client MAC address will be used as the username and password for access control through the RADIUS server.This option is unavailable when WPA Key Mode is set to Easy PSK.
MAC Format	Select the format used to send the client MAC address to the RADIUS server when MAC-Based RADIUS is enabled.Examples include aabbccddeeff, aa-bb-cc-dd-ee-ff, aa:bb:cc:dd:ee:ff, and their uppercase variants.
RADIUS Server Address	Configure the RADIUS authentication server address. This field is available with RADIUS-based WPA Key Modes, including 802.1X, PPSK with RADIUS, and Easy PSK.
RADIUS Server Port	Configure the RADIUS authentication server listening port. The default is 1812. This field is available with RADIUS-based WPA Key Modes, including 802.1X, PPSK with RADIUS, and Easy PSK.
RADIUS Server Secret	Enter the shared secret used between the access point and the RADIUS authentication server. This field is available with RADIUS-based WPA Key Modes, including 802.1X, PPSK with RADIUS, and Easy PSK.
Secondary RADIUS Server	Enable a secondary RADIUS authentication server for redundancy. This option is available with RADIUS-based WPA Key Modes, including 802.1X, PPSK with RADIUS, and Easy PSK. Configure the following fields:RADIUS Server Address: Enter the secondary RADIUS server address.RADIUS Server Port : Enter the secondary RADIUS server port. The default port is 1812 and the range is 1-65535.RADIUS Server Secret: Enter the secret password for client authentication with the secondary RADIUS server.
RADIUS Accounting Server	Configure the address for the RADIUS accounting server. This field is available only when "WPA Key Mode" is set to "802.1x".
RADIUS Accounting Server Port	Configure RADIUS accounting server listening port. Default is 1813. This field is available only when "WPA Key Mode" is set to "802.1x".
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server. This field is available only when "WPA Key Mode" is set to "802.1x".
Secondary RADIUS Accounting Server	Check the box to enable settings for a secondary RADIUS accounting server. Then you need to specify below three fields:RADIUS Accounting Server Address: Enter the secondary Accounting RADIUS server address.RADIUS Accounting Server Port: Configures the secondary RADIUS accounting server listening port. Default is 1813.RADIUS Accounting Server Secret: Enter the secret password for client authentication with the secondary RADIUS accounting server
RADIUS NAS ID	Enter the identifier sent by the access point to the RADIUS server as the NAS ID. The identifier allows the RADIUS server to distinguish this access point or SSID from others.This field is available when a RADIUS-based WPA Key Mode is used, including 802.1X, PPSK with RADIUS, or Easy PSK.
RADIUS NAS IP	Select the IP address sent by the access point to the RADIUS server as the NAS IP, such as This device IP or Main device IP. This field appears when a RADIUS-based WPA Key Mode is used, including Easy PSK.
Enable Hotspot 2.0	Check to activate Hotspot2.0 in the SSID. This field is available only when "WPA Key Mode" is set to "802.1x". Refer to [Hotspot 2.0] for more details
Hotspot 2.0 Profile	Select the Hotspot2.0 profile to use in the SSID. This field is available only when "WPA Key Mode" is set to "802.1x". Refer to [Hotspot 2.0] for more details

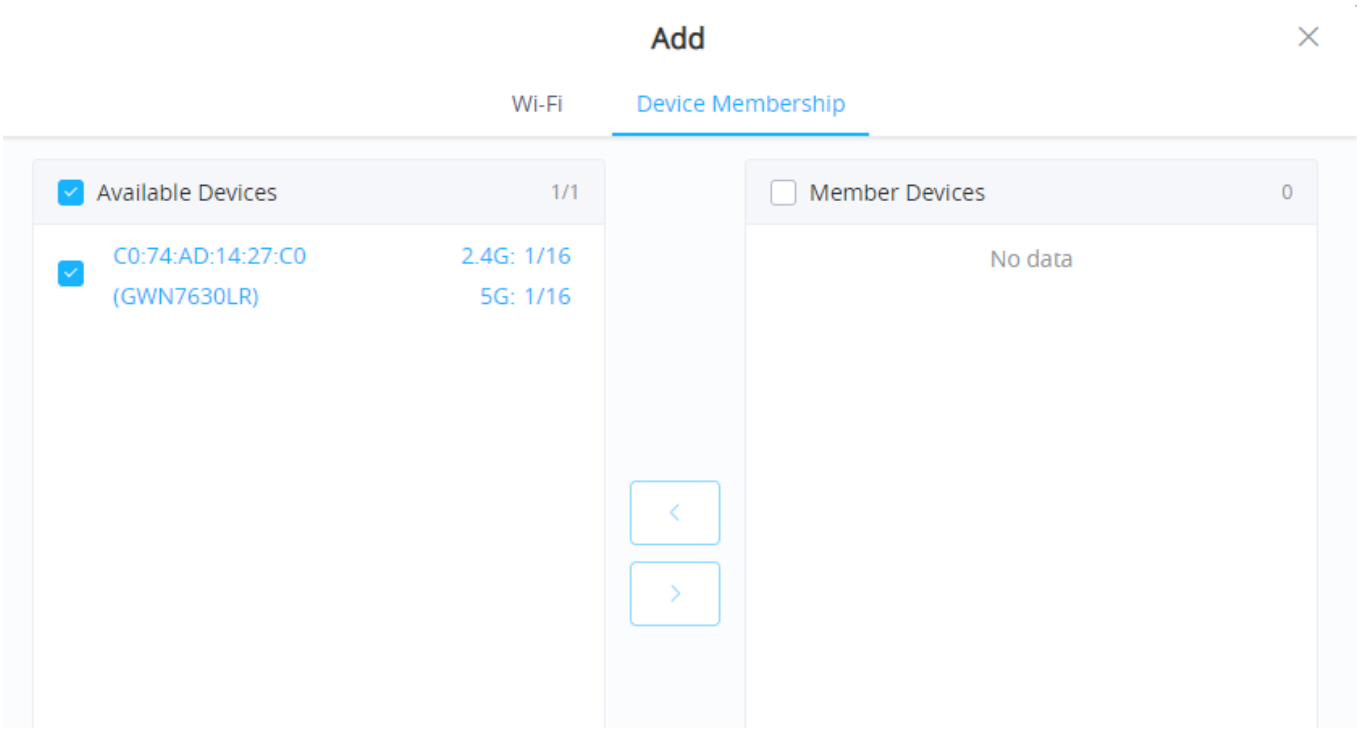
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded /included from connecting to the zone's Wi-Fi.Default is Disabled.
MAC Blacklist/Whitelist	This option is only available if Use MAC Filtering is set to Whitelist/Blacklist.Note: Clients in the selected access list can not access to the SSID. Total limited to 1024, contained the Global Blacklist.
Enable Dynamic VLAN (beta)	When enabled, clients will be assigned with an IP address from corresponding VLAN configured on the RADIUS user profile. This field is available only when "WPA Key Mode" is set to "802.1x".
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76XX. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available:Radio: Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76XX but they cannot communicate with each other.Internet: 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: Wireless client scan 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: customized MAC address, other wireless STAs are isolated. The gateway MAC address must be included in the customization.
IP Source Guard	Enable this option to require clients connected to the SSID to obtain an IP address through DHCP. Clients that manually configure a static IP address cannot access the Internet. This helps prevent clients from bypassing DHCP address controls or impersonating another device's IP address. Leave this option disabled if the SSID must support devices with manually configured static IP addresses.
Custom MAC Address	This field allows you to specify the custom MAC addresses that need to be isolated.Note: The gateway MAC address must also be included.Example: c0:74:ad:33:44:55, c0:74:ad:99:AA:BBPlus (+) Icon: Click this icon to add a new MAC address to the list. Minus (-) Icon: Click this icon to remove a MAC address from the list.
OS Filtering	Control SSID access according to the client operating system.Disabled: Do not filter clients by operating system.Blacklist: Block the selected operating systems.Whitelist: Allow only the selected operating systems.
OS Whitelist/Blacklist	Select the operating systems to block or allow, according to the selected OS Filtering mode.AllWindowsmacOSiOSLinuxAndroid
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	Configure the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Default value is 1, meaning that the AP will have DTIM broadcast every beacon. If set to 10, AP will have DTIM broadcast every 10 beacons. Valid range: 1 - 10.
Wireless Client Limit	Configure the limit for wireless clients. If there is a SSID per-radio on a LAN, each SSID will have the same limit. For example, setting a limit of 50 will limit EACH ssid to 50 users independently.Note: If set to 0, it disables the limit.
Client Inactivity Timeout(s)	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. Range from 60-3600 seconds.
Client Bridge Support	Configure the Client Bridge Support to allow the access point to be configured as a bridge to connect wired only clients wirelessly to the network. When an access point is configured in this way, it will share the Wi-Fi connection to the LAN ports directly. Once an SSID has Client Bridge Support enabled, the AP adopted in this SSID can be turned into Bridge Client mode by clicking the Bridge button.

Client Time Policy	Select a time policy to be applied to all clients connected to this SSID.
Multicast/Broadcast Suppression	When set as "Disabled": all of the broadcast and multicast packages will be forwarded to the wireless interface.When set as "Enabled": all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND;When set to "Enable with Proxy ARP enabled": AP will enable the optimization with Proxy ARP enabled in the meantime.
Convert IP multicast to unicast	When set as "Disabled": none of the multicast package will be converted;When set as "Passive mode": AP will never initiatively broadcast IGMP queries, and the IGMP snooping item will be aged out 300 seconds after it is registered, which may result in the failure of forwarding multicast data.When set as "Active mode": AP will initiatively broadcast IGMP queries to keep updating of the IGMP snooping items.
Enable Schedule	Enable this option to assign a schedule for the bandwidth rule.
Schedule	Within the time of schedule, SSID can be used.
Enable Voice Enterprise	Check to enable/disable Voice Enterprise. The roaming time will be reduced once enabled voice enterprise.This option is unavailable when WPA Key Mode is set to Easy PSK.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 faster. 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.Note: 11R is required for enterprise audio feature, 11V and 11K are optional. This field is available only when "Security Mode" is set to "WPA/WPA2" or "WPA2".
Enable 11R	Check to enable 802.11r. This field is available only when Security Mode is set to WPA/WPA2 or WPA2, and it is unavailable when WPA Key Mode is set to Easy PSK.
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
ARP Proxy	This option will enable GWN AP to answer the ARP requests from the LAN for its connected Wi-Fi clients. This is mainly to reduce the airtime consumed by ARP Packets.
Enable U-APSD	This option will allow the user to enable/disable the Unscheduled Automatic Power Save Delivery feature.
Enable Bonjour Gateway	Once enabled, the client Bonjour on the SSID is forwarded to the VLAN of the Bonjour service (such as Samba). Supported on GWN7605, GWN7605LR, GWN7615, GWN7630, GWN7630LR, GWN7660, GWN7660LR.
Target Wakeup Time	Configure whether to enable TWT (target wake up time) .Some terminal drivers are old and may have compatibility issues after being enabled.Note: Only take effect for WIFI6 models.
Enable Multi-VLAN	Enable Multi-VLAN for this SSID to assign different VLANs to connected devices.When enabled, specify the VLAN ID and associate it with AP devices connected to this SSID.Use the plus (+) icon to add new VLANs and APs, and the minus (-) icon to remove them.Note: This Multi-VLAN will have higher priority than the SSID VLAN.

SSID - Wi-Fi

- **Device Membership**: Used to add or remove paired access points from the SSID. The maximum number of SSIDs is counted separately for each supported radio band, such as 2.4 GHz, 5 GHz, or 6 GHz.

The maximum number of SSIDs supported per radio band varies by model. Refer to Technical Specifications and select the applicable access point model for its supported SSID limit.



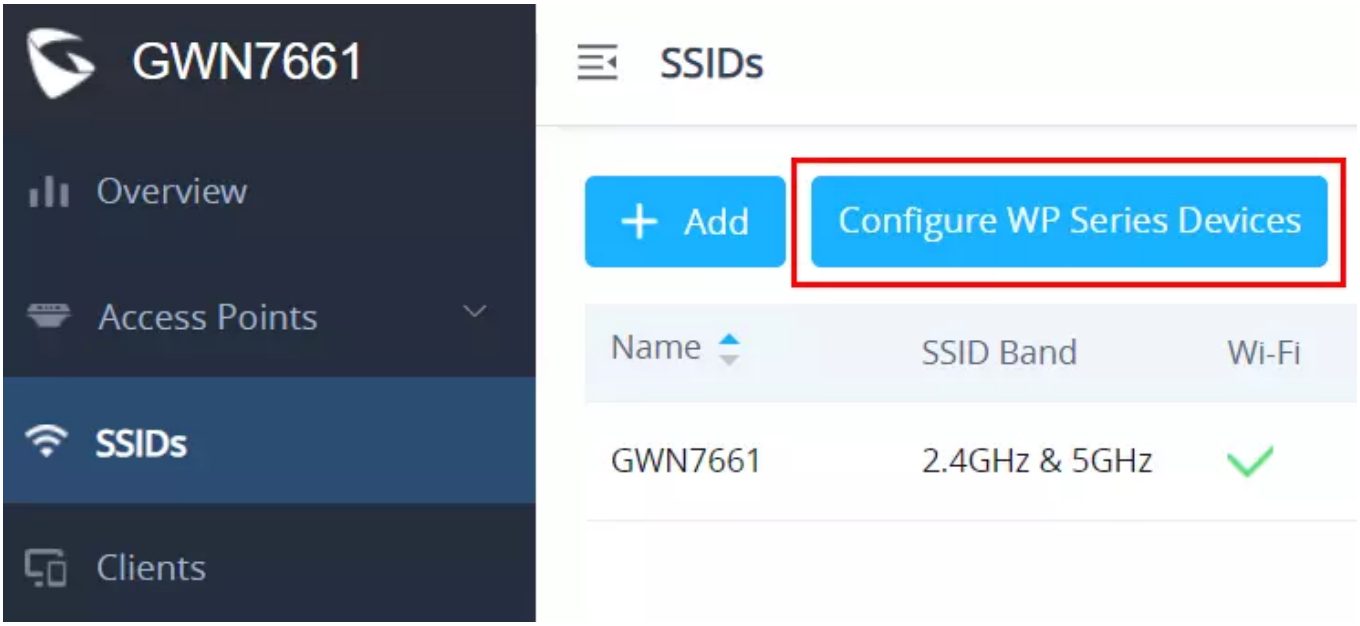
Device Membership

Select **Add** to assign the GWN76XX to the SSID, or select **Remove** to remove it.

Wi-Fi Phones (WP) series device fast configuration

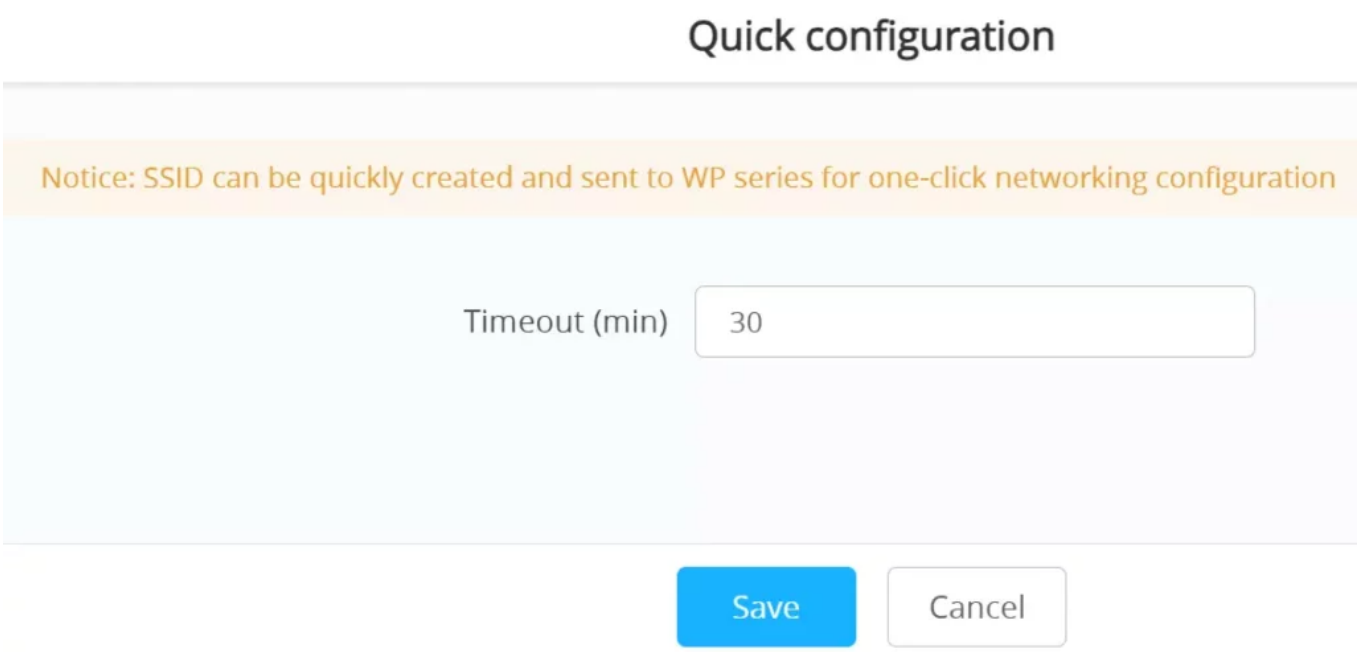
This feature helps to quickly create and configure SSID based on Wi-Fi phones (WP series) default configurations. WP phones come by default with an SSID name and password.

Navigate to **SSIDs** page, then click on **Configure WP Series Devices** button as shown below:



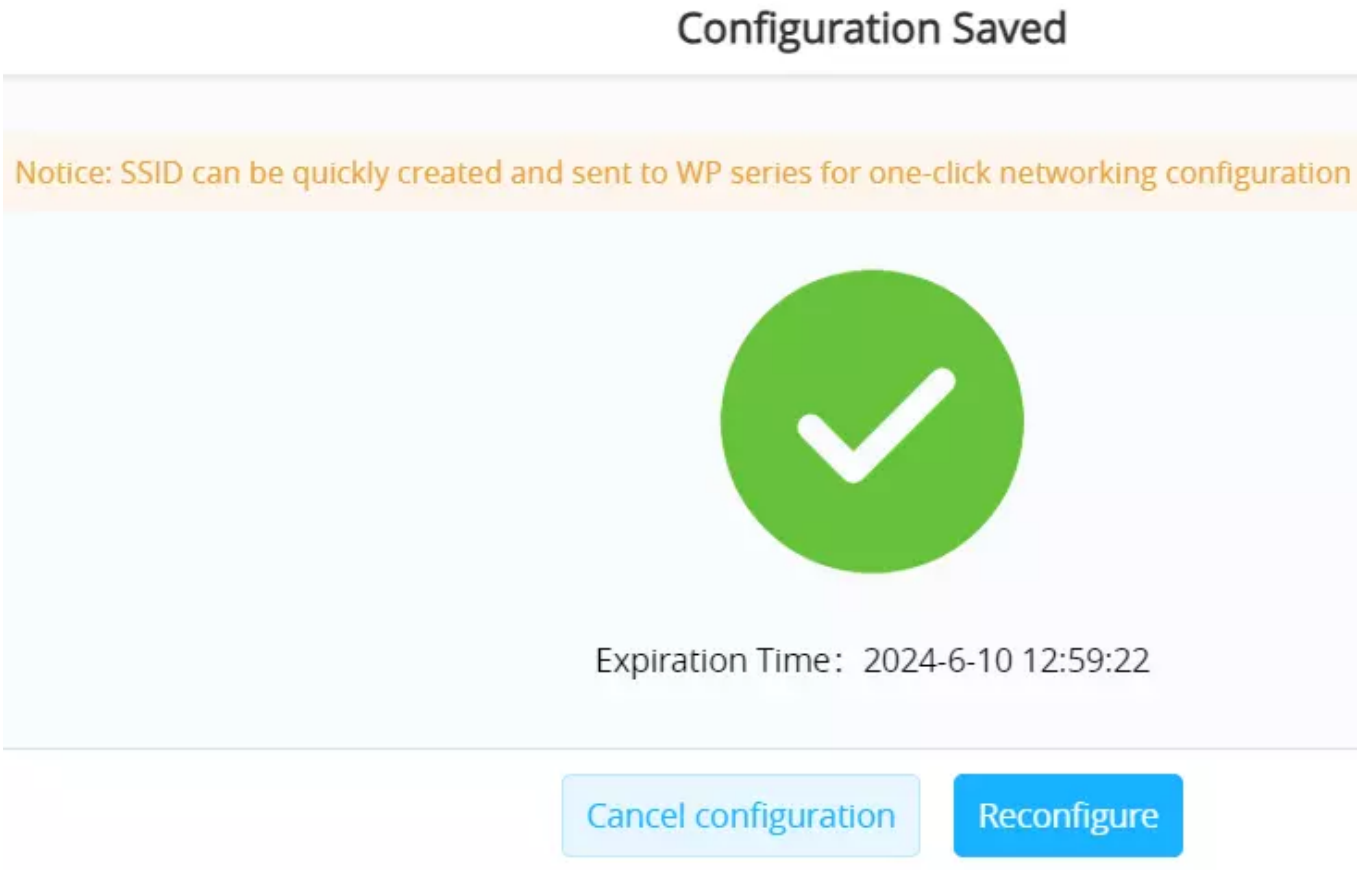
SSIDs -> Configure WP Series Devices

Specify the timeout duration for SSID (wp_master) to be visible; if no device was connected during that period, then it will be disabled, the timeout duration is in minutes within the range of 10-1440 minutes.

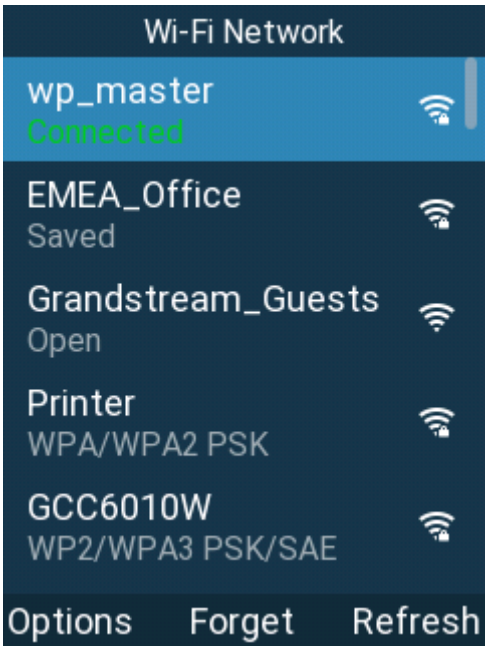


Configure WP Series Devices - Timeout

Click "**Save**" button, and use a WP phone to connect to the SSID (wp_master).



The SSID default password is already pre-configured with the WP phone.



WP phone

For more details visit:
https://documentation.grandstream.com/knowledge-base/wp816-user-guide/#auto-connection

Relay WiFi

Relay Wi-Fi (Wireless Extension) allows the access point to use an existing Wi-Fi network as its uplink instead of a wired Ethernet connection. In this mode, the AP joins another Wi-Fi network as a **client**, then continues to broadcast its own SSIDs (Wi-Fi) for local users.

This is useful when:

- There is no Ethernet cabling available at the installation point.
- The building provides only a shared Wi-Fi SSID (for example from a landlord or ISP router).
- You need temporary coverage for events, booths, or remote areas that are in Wi-Fi range but not in cabling range.
- The upstream AP is a different vendor and cannot participate in Mesh, but you still need additional coverage.

Relay Wi-Fi overview

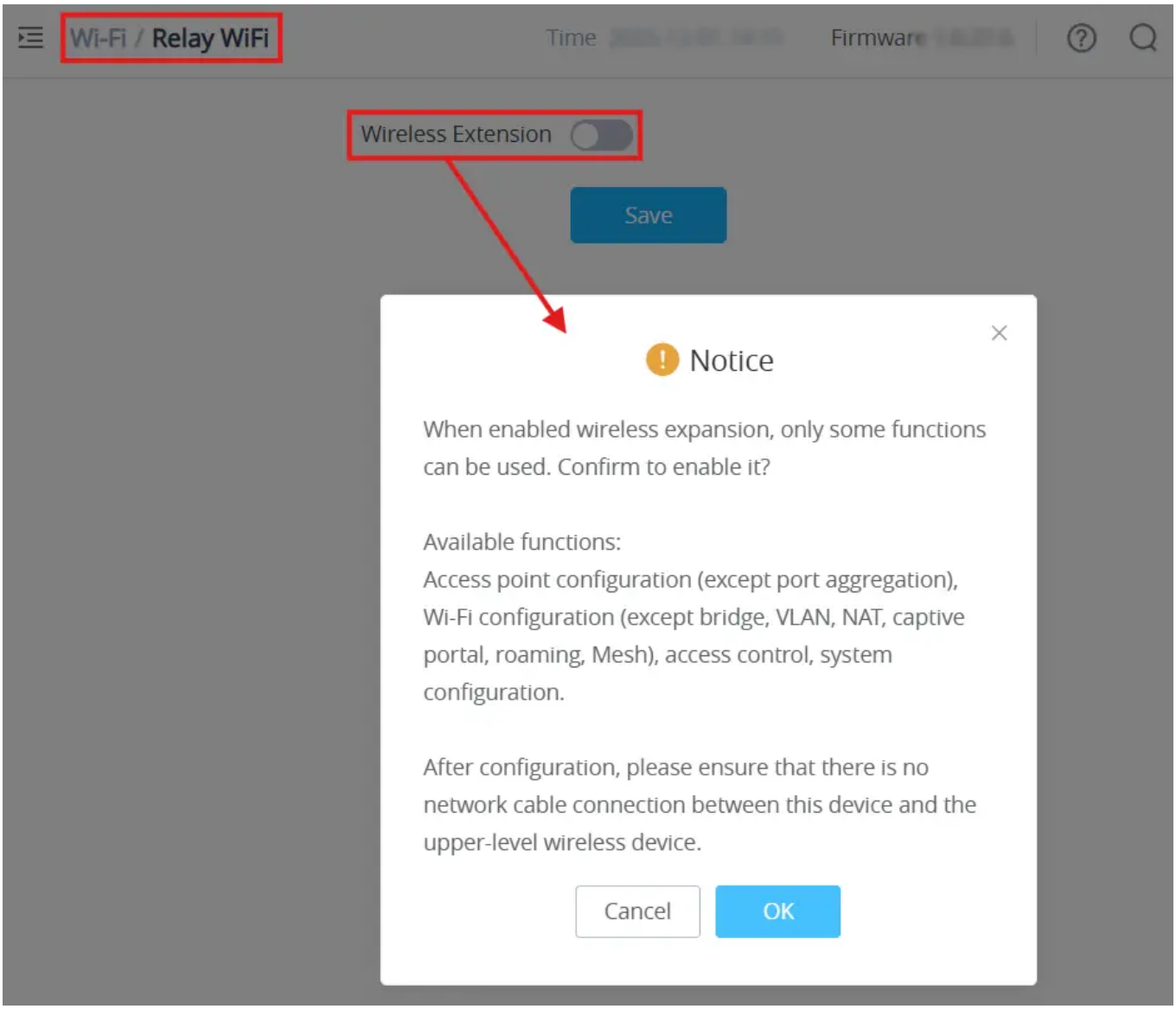
Relay Wi-Fi is configured from: **Wi-Fi -> Relay WiFi**

When you first enable **Wireless Extension**, a notice is displayed explaining the limitations of this mode. Only a subset of functions remains available:

Wireless Extension is unavailable while Mesh, client bridge, port aggregation, or failover is enabled.

- Access point configuration (except port aggregation)
- Wi-Fi configuration (excluding bridge, VLAN, NAT,captive portal, roaming and Mesh)
- Access control
- System configuration

After configuration is complete, the AP should be connected **only for power** (using PoE++). The Ethernet data link between this AP and the upstream wireless device must not be used; all data traffic will flow over the **wireless uplink**.

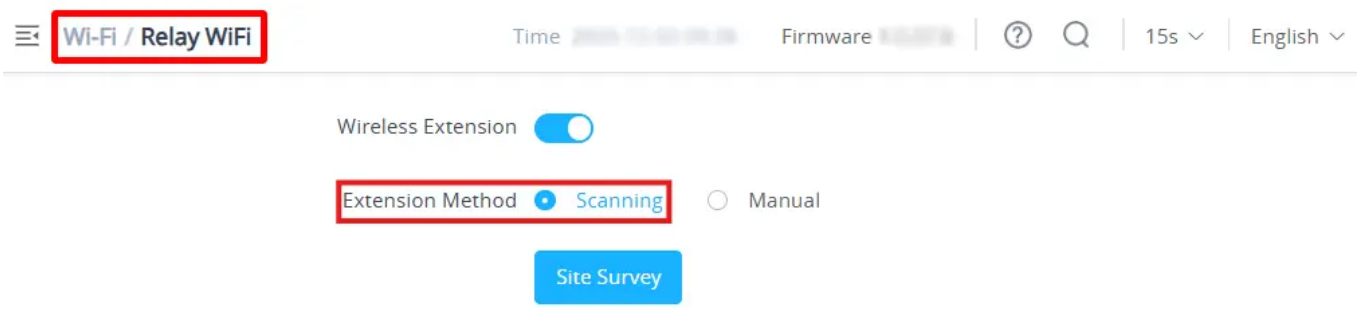


Relay WiFi

Enabling Wireless Extension

1. Log in to the AP Web GUI.
2. Navigate to **Wi-Fi -> Relay WiFi**.
3. Set **Wireless Extension** to **ON**.
4. Read the notice about available functions and click **OK** to confirm.
5. Click **Save** to apply the change.

After saving, additional options for the uplink configuration are displayed.



Enabling Wireless Extension

Choosing the extension method

Relay Wi-Fi supports two ways to select the upstream Wi-Fi:

- **Scanning (Site Survey):** the AP scans for nearby Wi-Fi networks and you choose one from the list.
- **Manual:** you manually enter the SSID and its security settings.

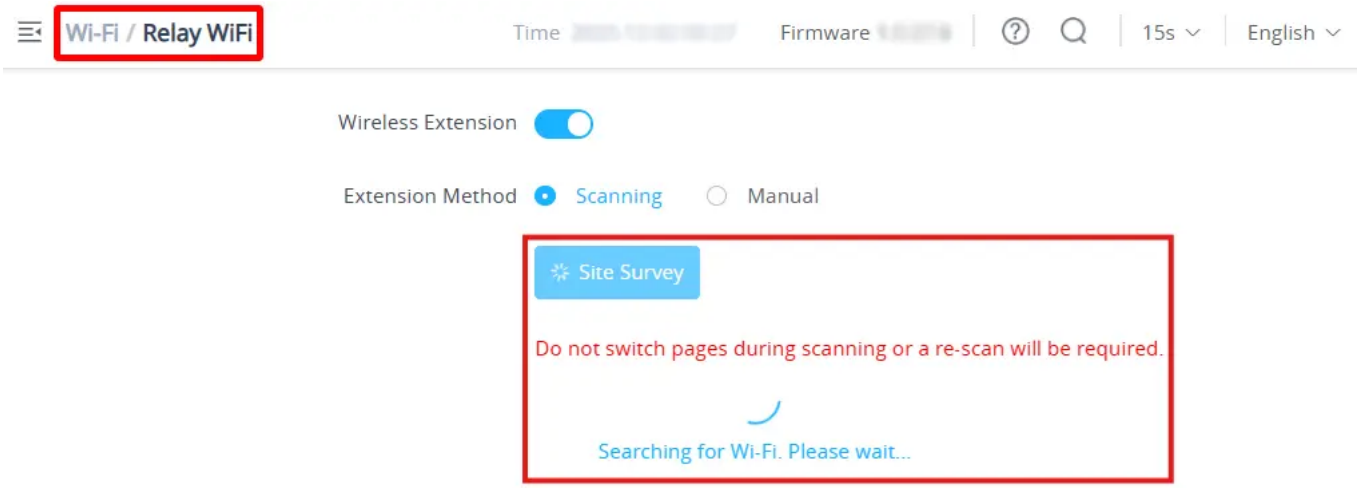
Both methods result in the AP joining the selected Wi-Fi network as a client.

Configuring Relay Wi-Fi using Scanning (Site Survey)

1. Under **Extension Method**, select **Scanning**.
2. Click **Site Survey**.

A progress panel appears indicating that the AP is scanning for visible Wi-Fi networks. While the scan is in progress, the page displays a warning such as:

Do not switch pages during scanning or a re-scan will be required. Searching for Wi-Fi. Please wait...



Configuring Relay Wi-Fi using Scanning (Site Survey)

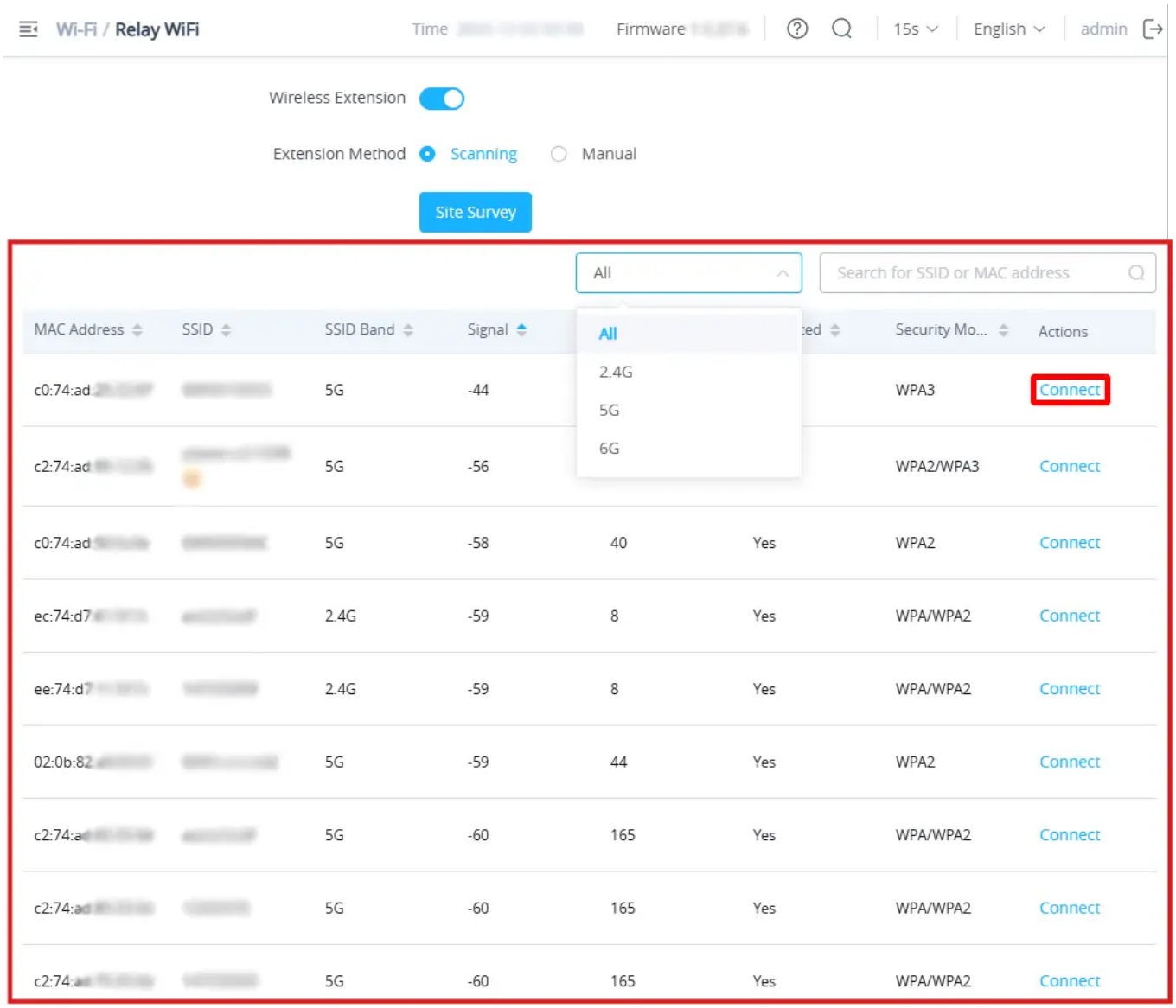
3. When the scan finishes, a table lists all detected SSIDs. Typical columns include:

   - **MAC Address (BSSID)** of the upstream AP
   - **SSID** name
   - **SSID Band** (2.4G / 5G / 6G)
   - **Signal** strength (dBm)
   - Whether the SSID is **Hidden**
   - **Security Mode** (for example Open, WPA2, WPA3)

4. You can:

   - Filter by band (All / 2.4G / 5G / 6G)
   - Search by SSID or MAC address using the search box

5. In the **Actions** column, click **Connect** for the Wi-Fi network you want to use as uplink.
6. If the network is secured, enter the correct Wi-Fi password when prompted and confirm.



Configuring Relay Wi-Fi using Scanning (Site Survey)

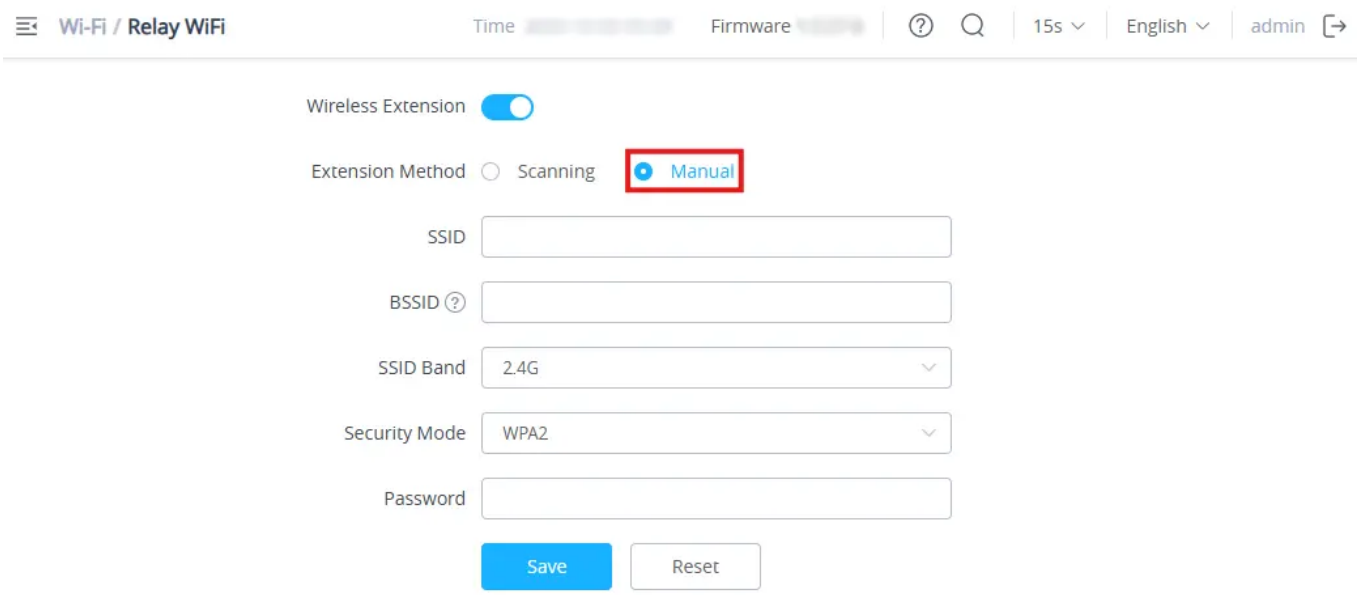
After successful authentication, the AP establishes a wireless link to the selected network and begins using it as its uplink.

Configuring Relay Wi-Fi using Manual settings

Manual mode is useful when the upstream SSID is hidden or when you want to specify the BSSID directly.

1. Under **Extension Method**, select **Manual**.
2. Fill in the fields:

   - **SSID**: the name of the upstream Wi-Fi network.
   - **BSSID**: (optional) the MAC address of the specific AP to connect to, if you want to lock the uplink to one radio.
   - **SSID Band**: select the band (2.4G / 5G / 6G) used by the uplink network.
   - **Security Mode**: choose the security type that matches the upstream SSID (for example WPA2 or WPA3).
   - **Password**: enter the Wi-Fi password when security is enabled.
3. Click **Save** to apply.



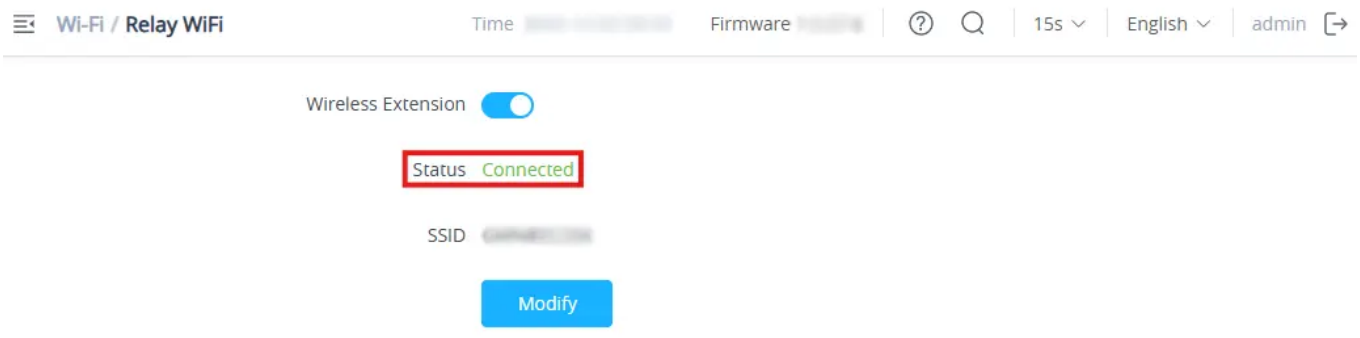
Configuring Relay Wi-Fi using Manual settings

The AP will attempt to connect to the specified Wi-Fi using the settings provided. If the password or parameters are incorrect, the status will indicate that the connection failed.

Verifying Relay Wi-Fi connection status

When the uplink connection succeeds, the Relay WiFi page shows a simplified view of the current state:

- **Wireless Extension** remains enabled.
- **Status** shows **Connected** (or a similar state if the uplink is down).
- The **SSID** field displays the name of the uplink Wi-Fi network currently in use.
- The **Modify** button allows you to change the configuration (for example to switch to another SSID or method).



Verifying Relay Wi-Fi connection status

At this point, the AP continues to broadcast its own SSIDs for clients, but instead of forwarding traffic over Ethernet, it uses the wireless uplink created by Relay Wi-Fi.

Confirming wireless uplink on the Status page

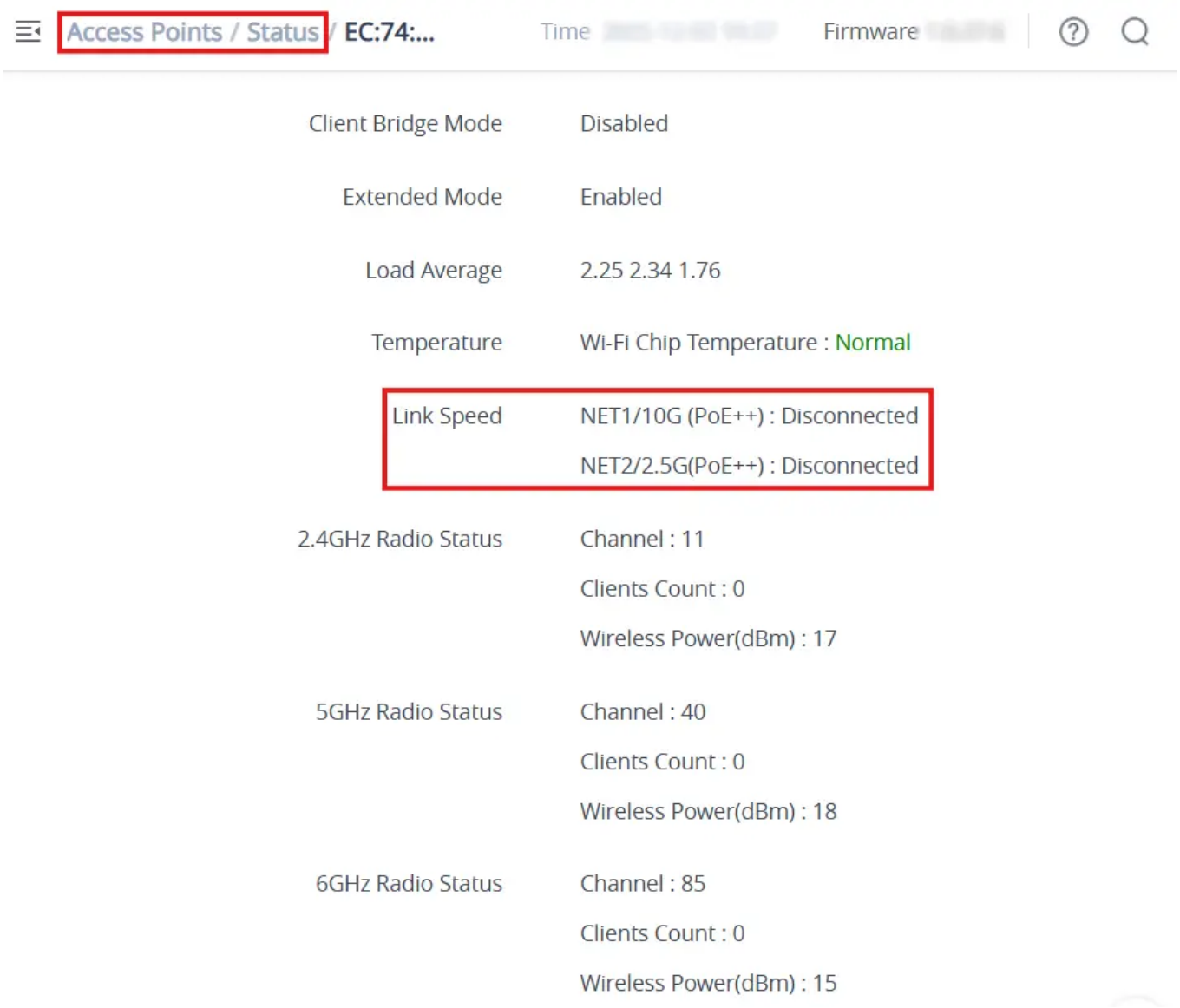
To verify that the AP is operating with a wireless uplink:

1. Ensure the Ethernet data cable between the AP and the upstream wireless device is disconnected. Power can still be supplied by a **PoE++ injector or a switch with PoE++ support**.
2. Go to **Access Points -> Status** and open the **Info** page for the AP.

In Relay Wi-Fi mode you can typically observe:

- **Extended Mode** is shown as **Enabled**.

- **Link Speed** for the wired interfaces (for example **NET1/10G** and **NET2/2.5G**) appears as**Disconnected**, confirming there is no active wired uplink.
- Radio status entries (2.4 GHz / 5 GHz / 6 GHz) remain **Enabled**, indicating that the AP continues to serve client devices normally over its own SSIDs.

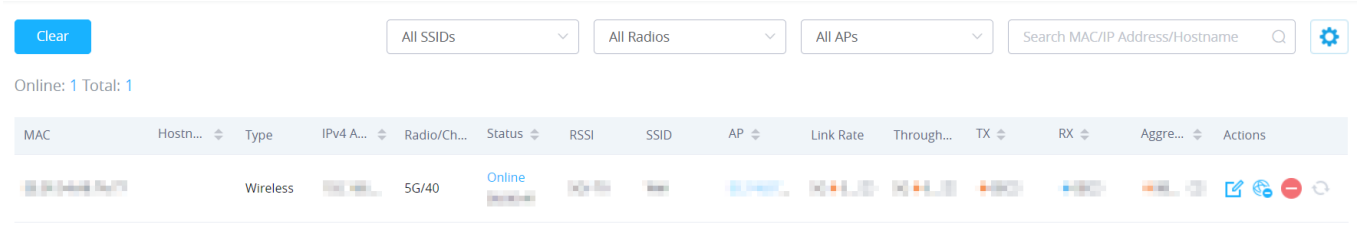


Confirming wireless uplink on the Status page

In this state, all user traffic flows from **clients -> AP SSIDs -> wireless uplink -> upstream Wi-Fi network**. Features that rely on a wired backhaul (such as VLAN trunking, bridge/NAT roles, captive portal or Mesh) remain unavailable, while basic Wi-Fi access and access control continue to function.

CLIENTS

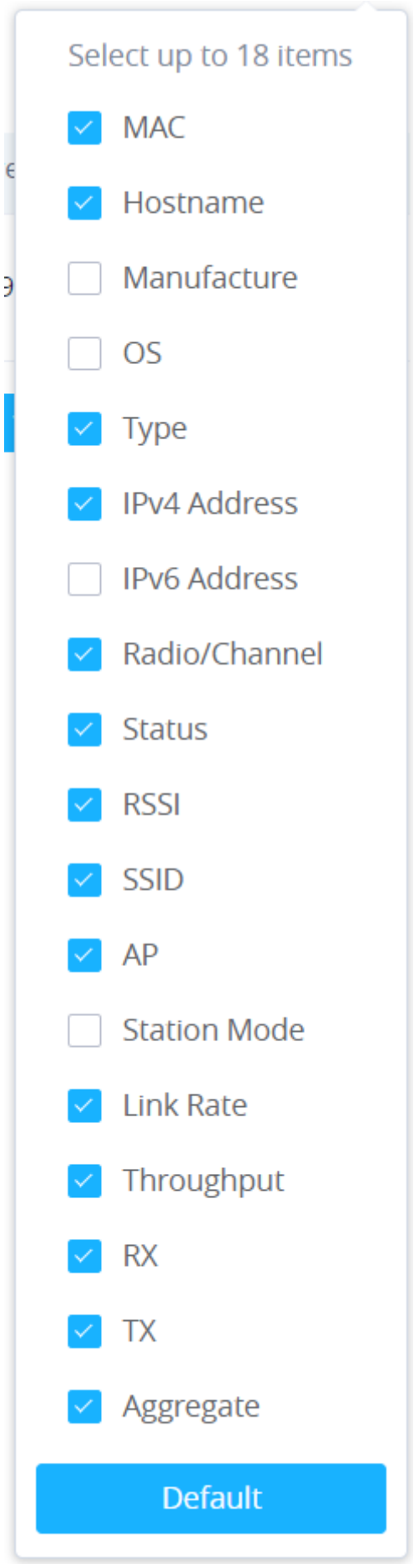
Users can access the list of clients connected to the GWN76XX from **Web GUI -> Clients** and perform different actions on wireless clients. Use **All SSIDs**, **All Radios**, and **All APs** to narrow the list, or use **Search MAC/IP Address/Hostname** to find a specific client.



Clients

- Select **Edit** under Actions to view the client status and modify basic settings such as the device name.
- Select **Block** to prevent the client MAC address from connecting to the zone's SSID.
- Select **Release IP Lease** to release the offline Wi-Fi client's IP lease.

Select **Column Settings** to choose up to 18 items to display. The available columns include separate **RX** and **TX** traffic values.

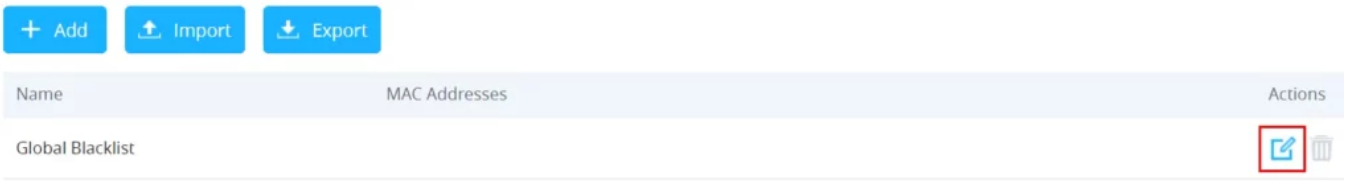


Clients - Column Settings

ACCESS CONTROL

Access List

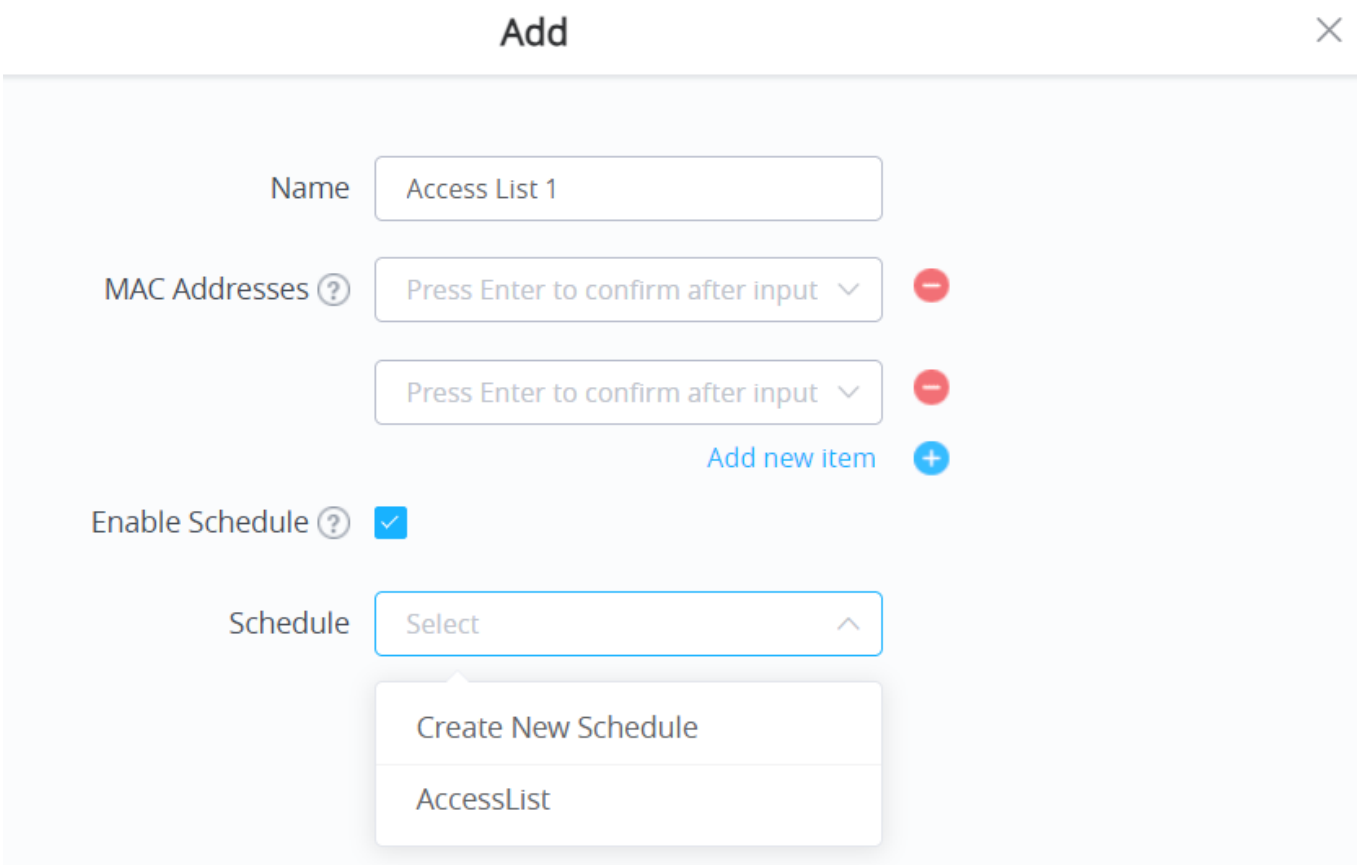
From this menu, users can manage the blacklist of clients that will be blocked from accessing the Wi-Fi network globally, click the "**Edit**" icon as shown below to add/remove MAC addresses of the client to/from global blacklist.



Global Blacklist

A second option is to add custom access lists that will be used as matching mechanism for MAC address filtering option under SSIDs to allow (whitelist) or disallow (blacklist) clients access to the Wi-Fi network.

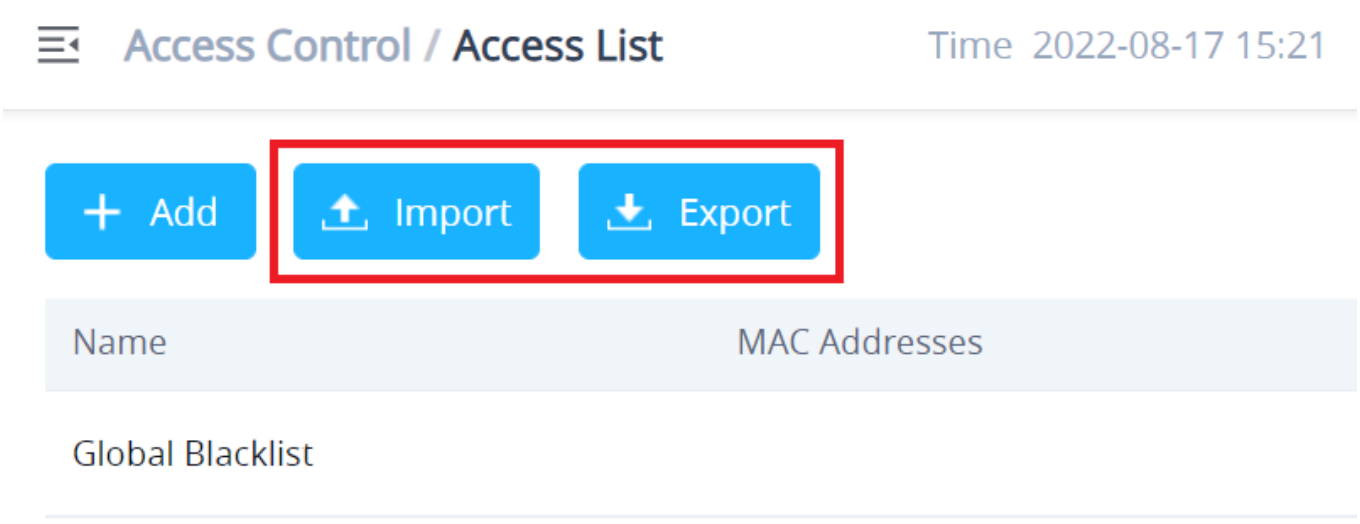
Select **Add** to create a custom access list. Enter a name, add the MAC addresses, and press **Enter** after each address. To limit when the access list is active, enable **Enable Schedule**, then select an existing schedule or choose **Create New Schedule**.



Adding an Access List and Schedule

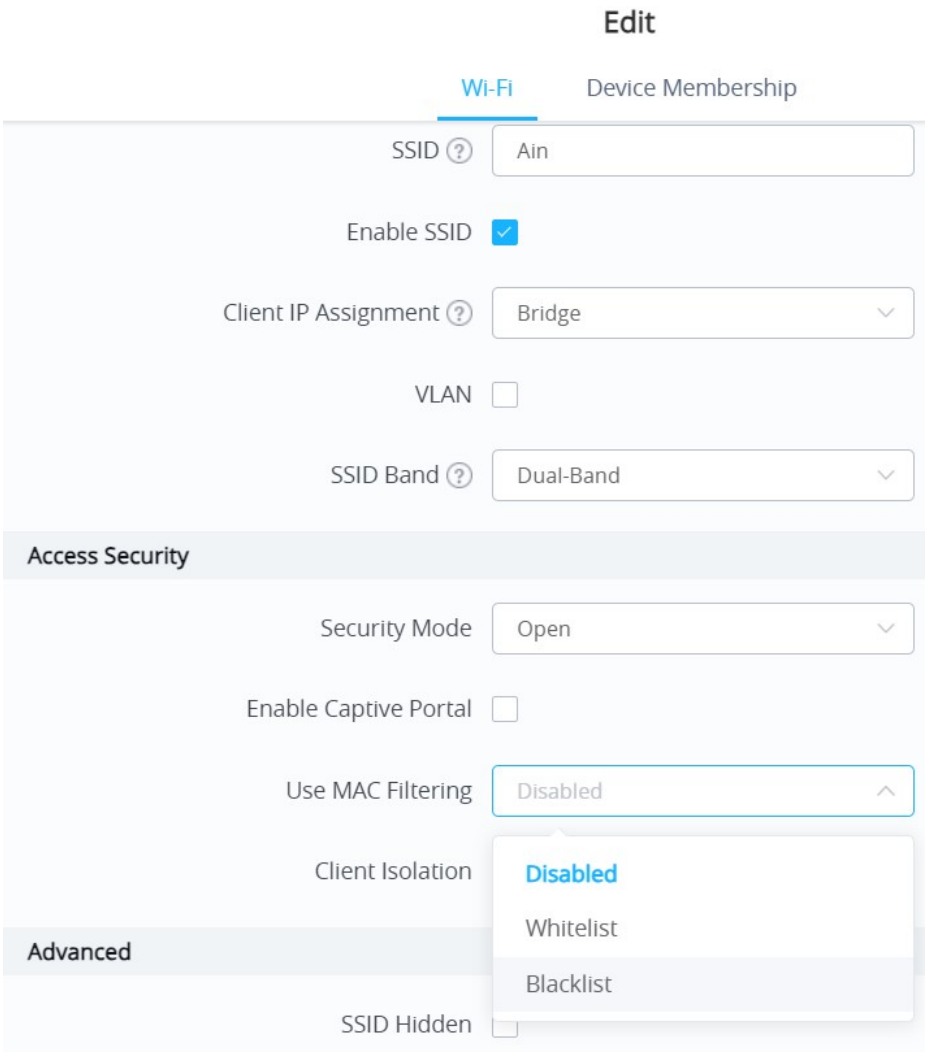
The total number of entries is limited to 1024, including the Global Blacklist.

Users can also Import/Export the client access lists in CSV format as shown below:



Import/Export the client access

Once this is done, this access list can be used under SSID Wi-Fi settings to filter clients either using whitelist or blacklist mode.



Use MAC Filtering

Time Policy

The timed client disconnect feature allows the system administrator to set a fixed time for which clients

should be allowed to connect to the access point, after which the client will no longer be allowed to connect until the user-configurable cool-down period is reached.

The configuration is based on a policy where the administrator can set the amount of time for which clients are allowed to connect to the Wi-Fi. The administrator can also set the reconnect type and value for the users to reconnect after they have been disconnected.

To create a new policy, go under **Captive Portal -> Time Policy** and add new one.

Then set the following parameters:

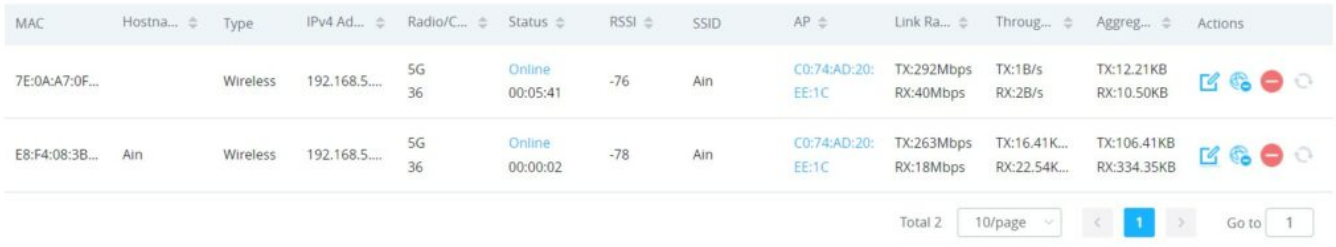
Option	Description
Name	Enter the name of the policy.
Enabled	Check the box to enable the policy.
Limit Client Connection Time	Set the amount of time a client may be connected.
Client Reconnect Timeout Type	Select the method with which we will reset a client's connection timer so they may reconnect again. Options are: Reset Daily. Reset Weekly. Reset Hourly. Timed Reset.
Client Reconnect Timeout	If "Timed Reset" is selected, this is the period for which the client will have to wait before reconnecting.
Day of the Week	If "Reset Weekly" is selected, this is the day when the reset will be applied.
Hour of the Day	If "Reset Weekly" or "Reset Daily" is selected, this is the hour and day when the reset will be applied.

Time Policy Parameters

Time tracking shall be accounted for on a per-policy basis, such that a client connected to any SSID assigned the time tracking policy will accrue a common counter, regardless of which SSID they are connected to (as long as those SSIDs all share the same time tracking policy).

Banned Clients

Clients blocked by the disconnect timeout cannot reconnect until the timeout resets. To restore access sooner, select **Unblock** for the client.



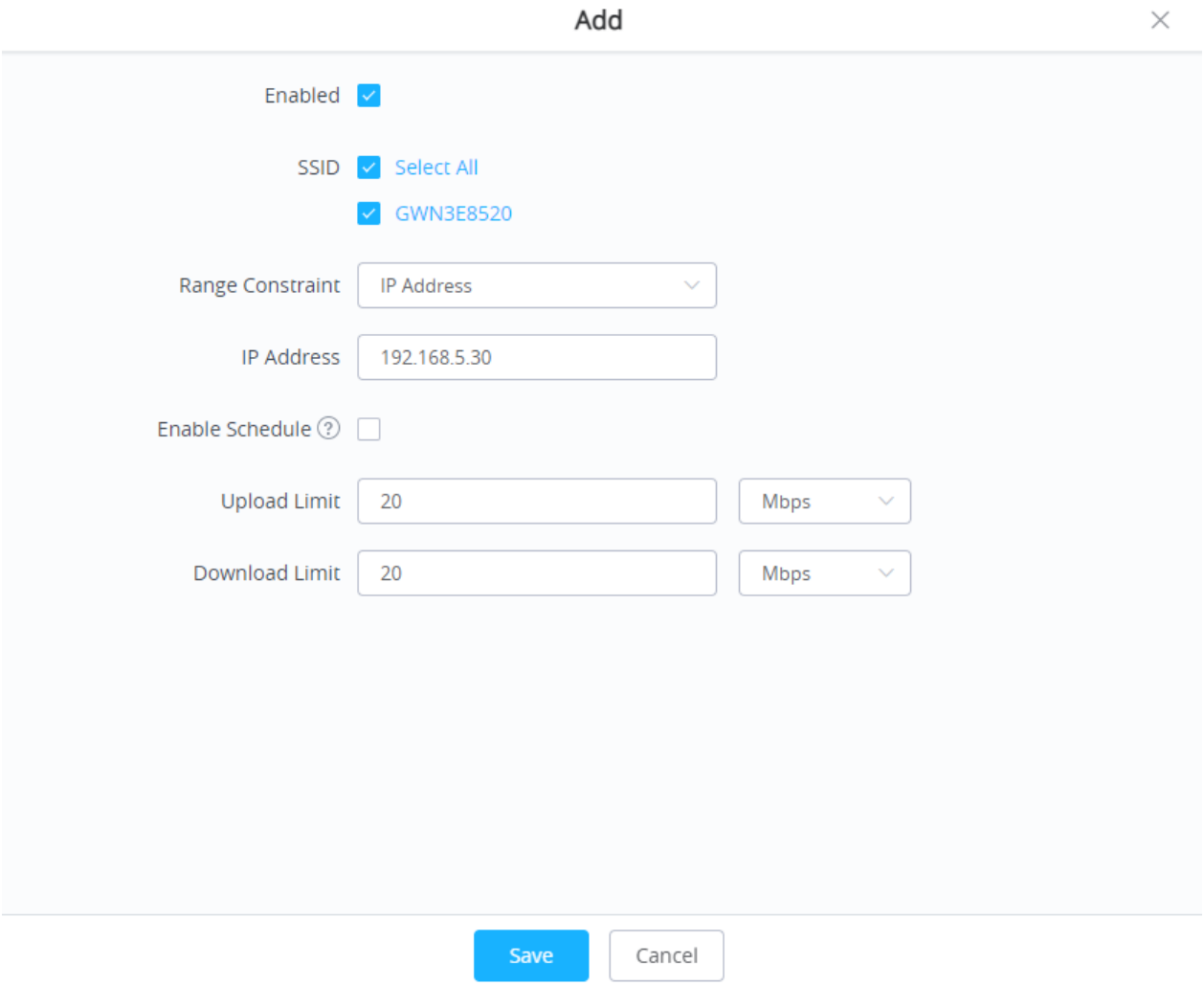
Ban/Unban Client

Bandwidth Rules

The bandwidth rule is a GWN76XX feature that allows users to limit bandwidth utilization per SSID or client (MAC address or IP address).

This option can be configured from the GWN76XX WebGUI under "Bandwidth Rules".

The following figure shows an example of MAC address rule limitation.



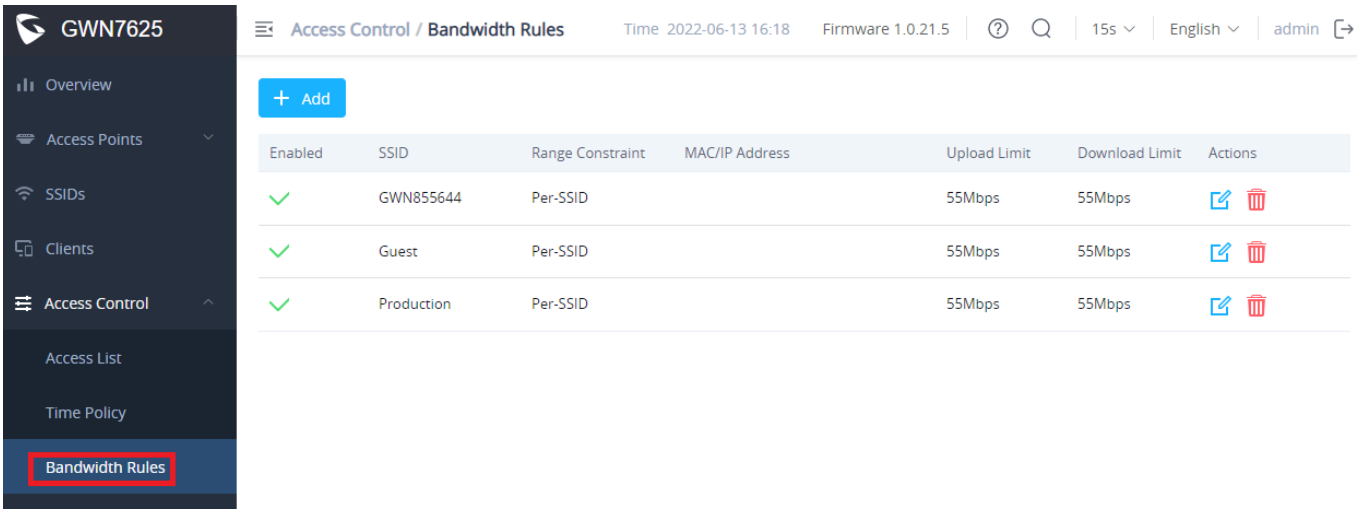
MAC Address Bandwidth Rule

Select **Add Rule** to create a bandwidth rule. The following table explains the available options.

Field	Description
Enabled	Enable/Disable the Bandwidth rule.
SSID	Select which SSID will be affected by the bandwidth rule limitation.
Range Constraint	Choose the type of rule to be applied on bandwidth utilization from the dropdown list, three options are available: Per-SSID: Set a bandwidth limitation on the SSID level. Per-User: Set a bandwidth limitation per Client. MAC: Set a bandwidth limitation per MAC address. IP Address: Set a bandwidth limitation per IP address.
MAC	Enter the MAC address of the device to which the limitation will be applied; this option appears only when the MAC type is selected.
IP address	Enter the IP address of the device to which the limitation will be applied; this option appears only when IP Address type is selected.
Enable Schedule	Enable this option to assign a schedule for the bandwidth rule.
Upload Limit	Specify the limit for the upload bandwidth using Kbps or Mbps.
Download Limit	Specify the limit for the download bandwidth using Kbps or Mbps.

Bandwidth Rules

The following figure shows examples of bandwidth rules:



Bandwidth Rules

The same settings for bandwidth management are available from the following menus:

Navigate on the web GUI under "**Clients -> Edit -> Bandwidth Rules**" where you can set the Upstream and Downstream rate in Mbps.

Private Pre-Shared Key (PPSK)

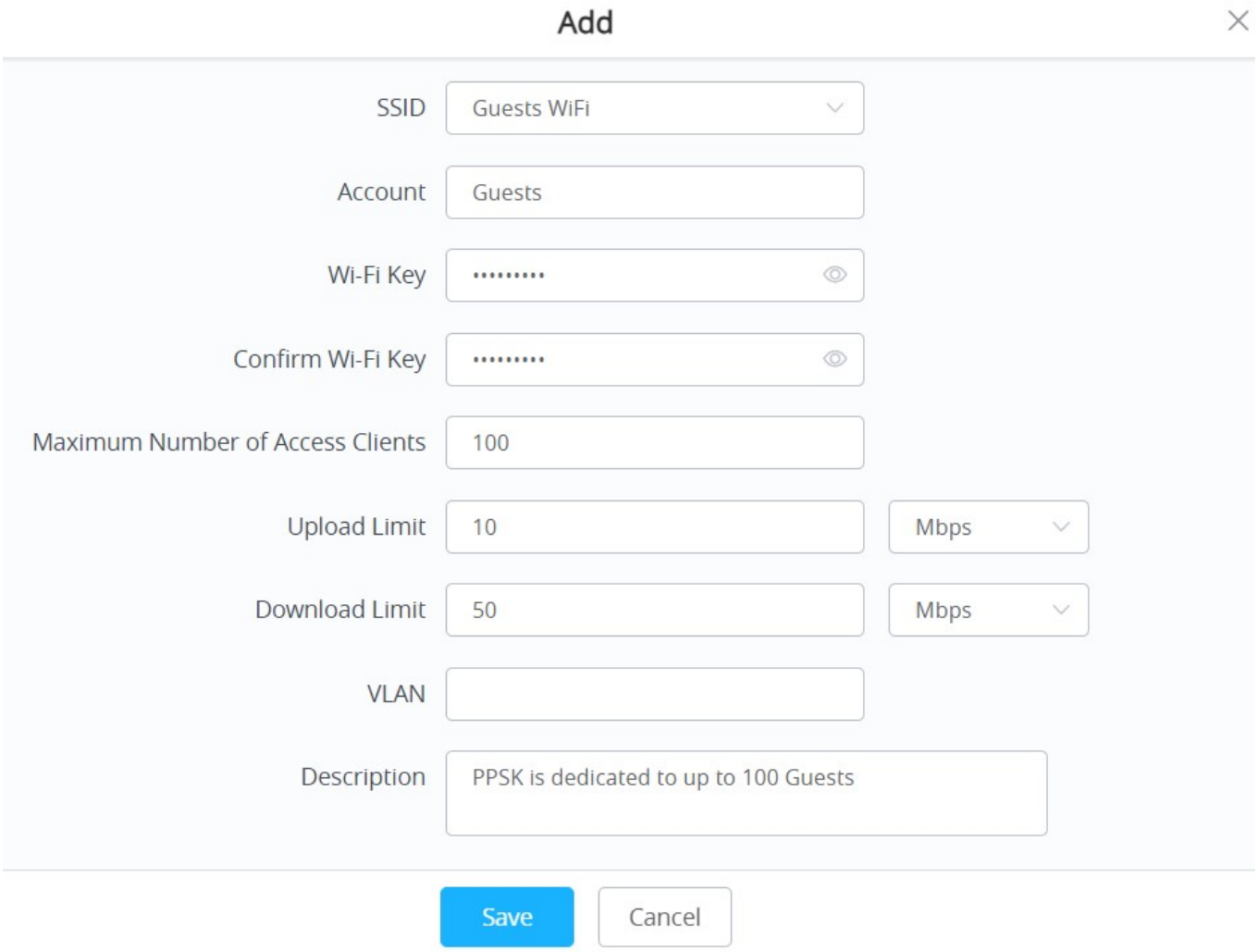
PPSK (Private Pre-Shared Key) is a way of creating Wi-Fi passwords per group of clients instead of using one single password for all clients. It's also possible to assign it to a single device client with a MAC Address.

Before adding a PPSK account, create an SSID and select **PPSK without RADIUS** or **PPSK with RADIUS** as the WPA Key Mode. On models that display the **Wi-Fi** menu, use **Wi-Fi > SSID**; otherwise, use **SSIDs**.

The maximum number of PPSK accounts depends on the access point model.

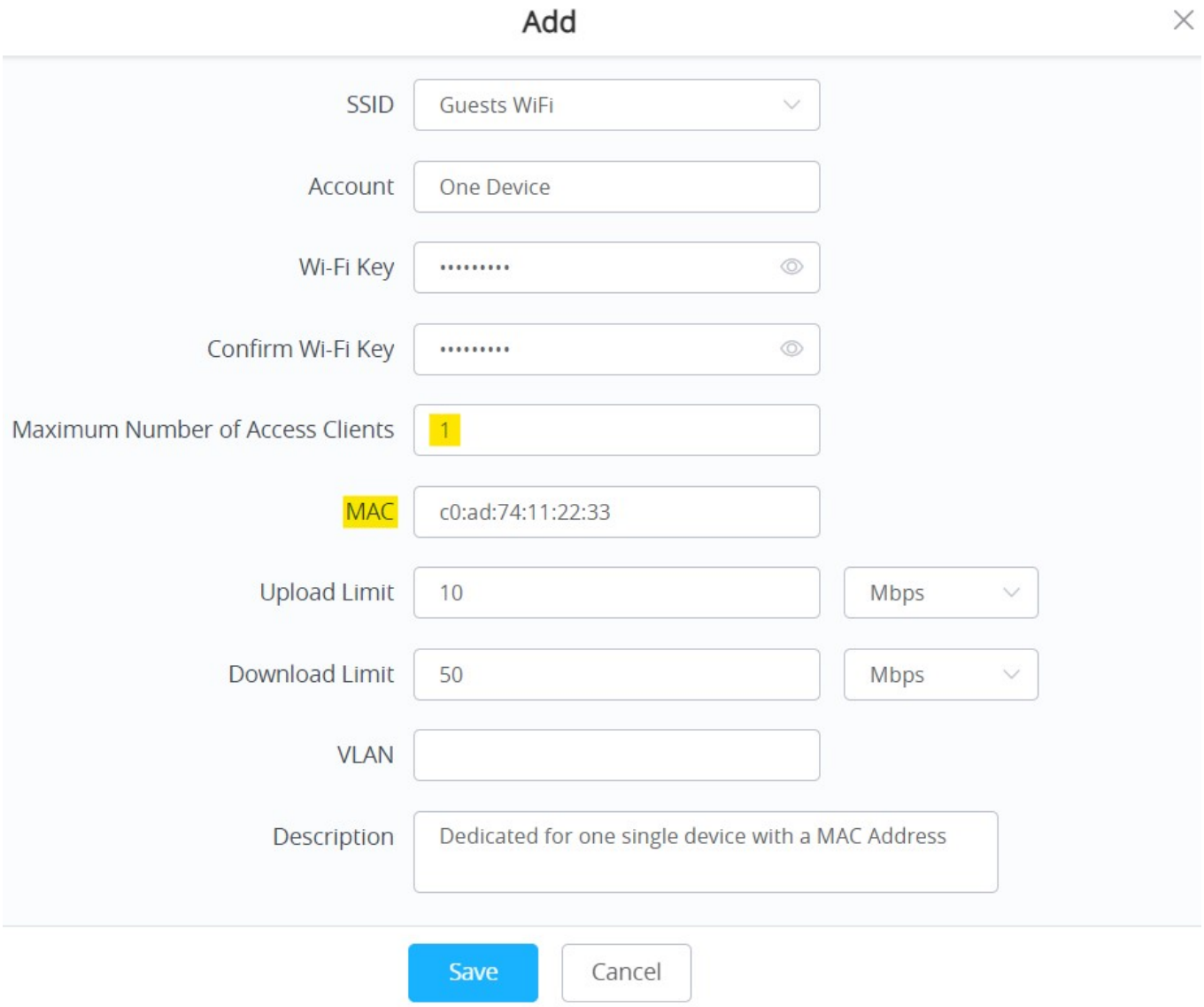
Maximum PPSK accounts	Models
2,500	GWN7672, GWN7672L, GWN7672WM, and GWN7674
1,000	GWN7660E, GWN7660ELR, GWN7661E, GWN7662, GWN7664E, GWN7664ELR, GWN7665, GWN7670, GWN7670E, GWN7670LR, GWN7670WM, and GWN7673
300	Other supported GWN76xx models

To configure PPSK, open **Wi-Fi > PPSK** on models that display the Wi-Fi menu; otherwise, open **Access Control > PPSK**. Use **Search VLAN/Account** to filter the PPSK account list, or select **Add** to create a PPSK account.



Add a PPSK Profile

In case where the Maximum Number of Access Clients set to 1, then an option to specify a MAC Address is added. Please refer to the figure below:



PPSK - Maximum Number of Access Clients

SSID	Select the SSID from the drop-down listNote: the SSID WPA Key Mode must be set to "PPSK Without RADIUS or With RADIUS".
Account	Set a name for this PPSK profile.
Wi-Fi Key	Enter a Wi-Fi key.
Confirm Wi-Fi Key	Confirm the Wi-Fi key (must be the same)
Maximum Number of Access Clients	Enter the maximum number of access clients (devices) that are allowed to use this key, once the maximum number is reached, the key will not be used to connect to Wi-Fi.
MAC	In case the maximum number of access clients is set to 1, then the user can specify the MAC address as well for even more security.
Upload Limit	set a max upload limit (Mbps/Kbps)
Download Limit	set a max download limit (Mbps/Kbps)
VLAN	specify a VLAN or leave it empty (Default VLAN).
Description	Enter a descritpion for this PPSK profile.

PPSK

CAPTIVE PORTAL

Captive Portal feature on GWN76XX AP helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet. Once connected to a GWN76XX AP, Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the GWN76XX Web page under "Captive Portal".

The page contains following sub-menus: **Guest**, **Policy List**, **Splash Page** and **Vouchers**.

Related Captive Portal Guides

Guide	Use this guide to
Social WiFi Guide	Configure a Social WiFi marketing portal for guest access.
Voucher Authentication	Generate and use time-limited voucher codes for guest access.
RADIUS Authentication	Authenticate captive portal users through a RADIUS server.
Captive Portal Authentication via Facebook	Configure social login using a Meta or Facebook account.
External Captive Portal API Guide	Implement a custom external captive portal server using the EXCAP API.
Captive Portal Authentication with Microsoft 365	Authenticate visitors using Microsoft work or school accounts.
Captive Portal Authentication with SAML SSO	Connect the captive portal to a compatible SAML identity provider.

Guest

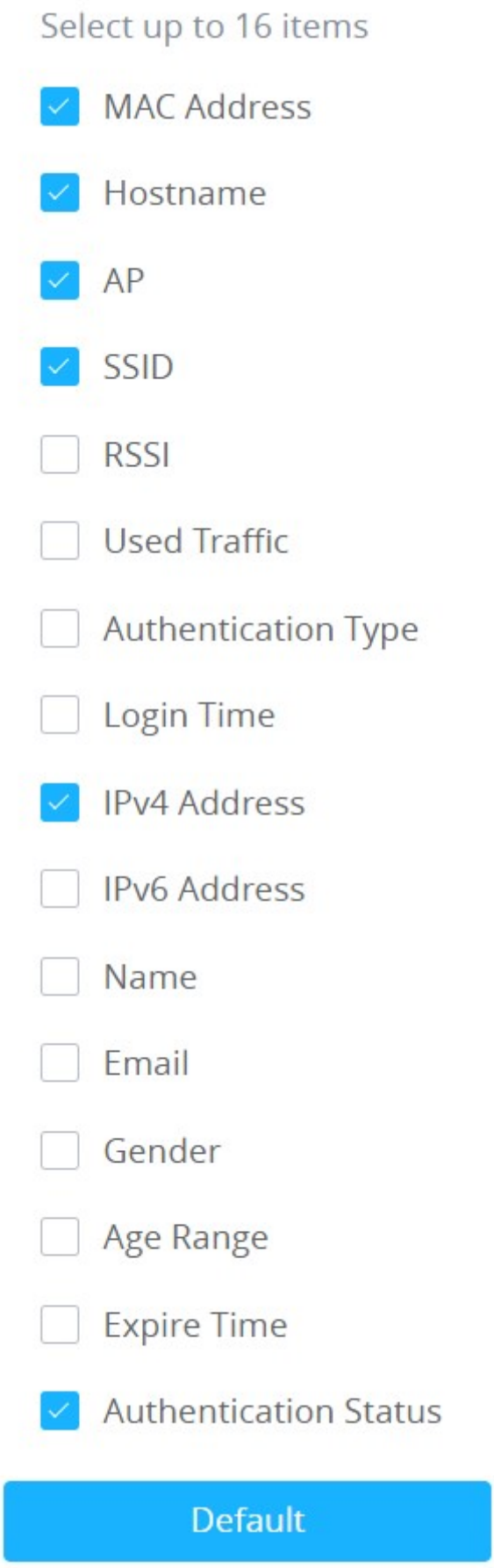
This section lists the clients connected or trying to connect to Wi-Fi via Captive Portal.



Captive Portal - Guest Page

Select **Kick Out** to disconnect the selected clients.

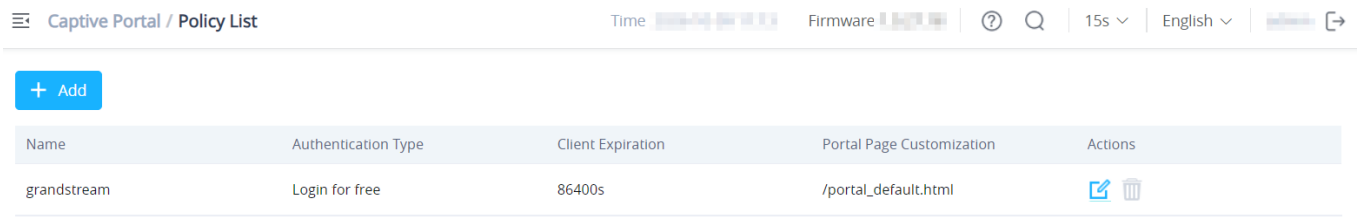
Select **Column Settings** to choose which items appear on the page. The following items are supported:



Captive Portal - Guest Page - Select Items

Policy List

Users can customize a portal policy in this page.



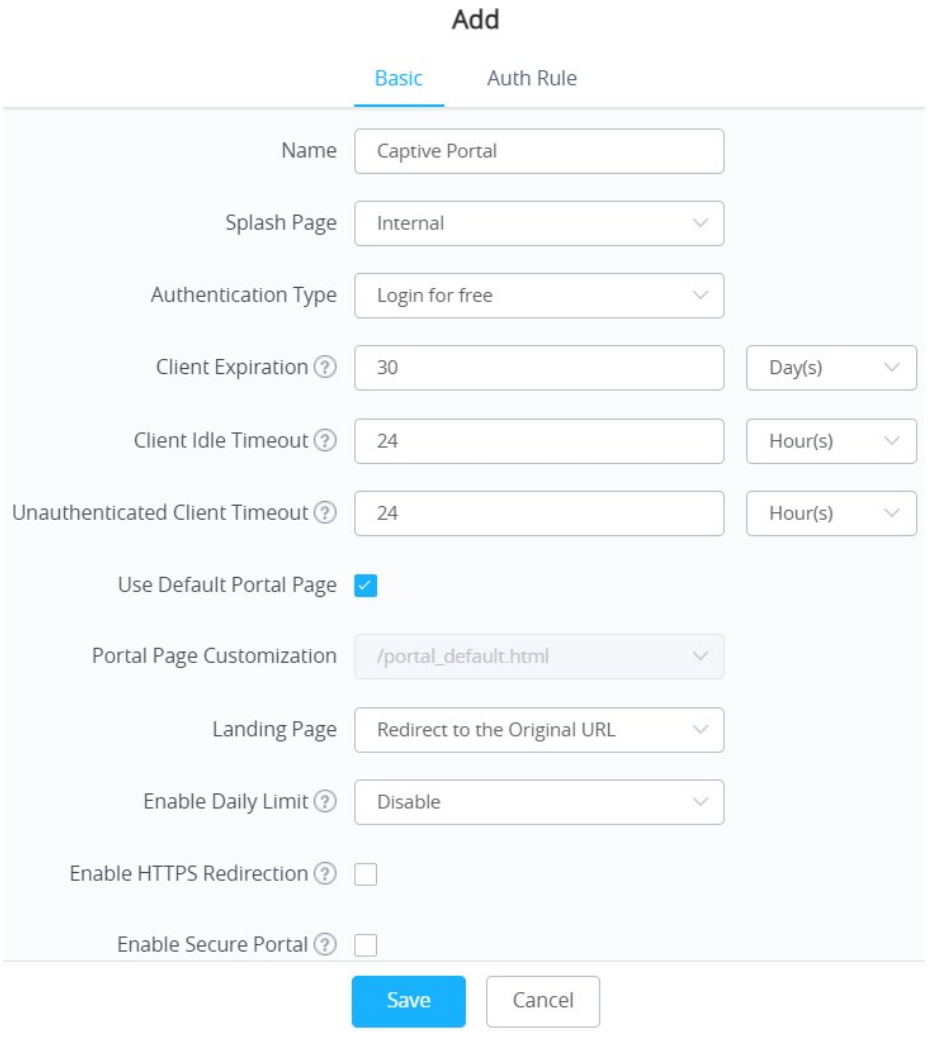
Captive Portal - Policy List

- Select **Edit** to edit the policy.
- Select **Delete** to delete the policy.
- Select **Add Policy** to add a 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 can be easily configured as shown in the next section.

MAC Allowlist: Select an existing MAC access list to allow the listed devices through this captive portal policy. If no list is available, select **Go to Create** to create one under **Access Control -> Access List**.

Administrator can use an internal or external splash page.



Add a New Policy

Internal Splash Page

Below table lists the items policy add page configures

Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, in this case "Internal"
Authentication Type	The following types of authentications are available: Log in for free: when choosing this option, the landing page feature will not provide any type of authentication instead, it will prompt users to accept the license agreement to gain access to the internet. Radius Server: Choosing this option will allow users to set up a RADIUS server to authenticate connecting clients. Social Login Authentication: Choosing this option will allow users to enable authentication on Facebook, X, Google, or Microsoft 365. Vouchers: Choose this page when using authentication via Vouchers. Login with password: Choose this page when using authentication via a password. SAML SSO: Choosing this option will allow users to authenticate clients using SSO Server. Active Directory: Choosing this option will allow users to set up an Active Directory server to authenticate connecting clients.
Client Expiration	Configure the period of validity, after the valid period, the client will be re-authenticated again.Note: the maximum duration is 30 days.
Client Idle Timeout	Configure the time when the client will automatically deauthenticate when it is idle. This does not apply to Voucher Captive portal mode.Note: the maximum duration is 24 hours.
Unauthenticated Client Timeout	Configure a timeout period, after which unauthenticated client devices will be disconnected, and reconnection is not allowed.Note: the maximum duration is 24 hours.
If Authentication Type is set to RADIUS Authentication	
RADIUS Server Address	Fill in the IP address of the RADIUS server.
RADIUS Server Port	Set the RADIUS server port, The default value is 1812.
RADIUS Server Secret	Fill in the key of the RADIUS server.
Radius Authentication Method	Select the RADIUS authentication method, 3 methods are available: PAP, CHAP and MS-CHAP.
Radius Retry Timeout(s)	Set the timeout for each authentication request sent to the Radius server. The valid range is 1 to 120 seconds.
Radius Retries	Set the maximum number of retires to send an authentication request for the Radius server. The valid range is 1 to 5.
If Authentication Type is set to "Social Login Authentication"	
Facebook	Check to enable/disable Facebook Authentication
Facebook App ID	Fill in the Facebook App ID.
Facebook APP Secret	Set the key for the portal, once clients want to connect to the Wi-Fi, they should enter this key.
X	Check this box to enable X authentication.
Force to Follow	If checked, users need to Follow owner before been authenticated.
Consumer Key	Enter the app Key to use X Login API.
Consumer Secret	Enter the app secret to use X Login API.
Google	Check this box to enable Google Authentication.
Google Client ID	Enter the Client Id to use Google Login API.
Google Client Key	Enter the Client Key to use Google Login API.
Microsoft 365	Check to enable Microsoft 365 authentication. Enabling this option also enables Secure Portal. Register an application in Microsoft Entra, then use its App ID and App Secret in the fields below. Configure the OAuth redirect URI as https://cwp.gwn.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=6.

Microsoft 365 Client ID	Enter the App ID from the Microsoft Entra application.
Microsoft 365 Client Key	Enter the App Secret from the Microsoft Entra application.
If Authentication Type is set to "Login with password"	
Login with password	Specify a password for the captive portal.
If Authentication Type is set to "SAML SSO"	
SSO Server URL	Fill in the IP address of the SSO server.
Redirect URL	Enter the redirect URL.
X.509 Cert SHA1 Fingerprint	enter the X.509 Cert SHA1 Fingerprint
If Authentication Type is set to "Active Directory"	
AD Server URL	Specify Active Directory URL
Redirect URL	Enter the redirect URL
X.509 Cert SHA1 Fingerprint	enter the X.509 Cert SHA1 Fingerprint
For all Authentication Types	
Use Default Portal Page	If checked, the users will be redirected to the default portal page once connected to the GWN.* If unchecked, users can manually select which Portal Page to use from Portal Page Customization drop-down list.
Portal Page Customization	Select the customized portal page from the drop-down list (if "Use Default Portal Page" is unchecked).
Landing Page	Choose the landing page, 2 options are available: Redirect to the Original URL. Redirect to External Page.
The Redirect External Page URL Address	Once the landing page is set to redirect to external page, user should set the URL address for redirecting.This field appears only when Landing Page is set to "Redirect to an External Page".
Enable Daily Limit	Disabled: Non -day access limit. According to the client limit: After opening, only the Guest is allowed to be connected once a day, and it is not allowed to authenticate again after the network use timeout. Limit by authentication: The guest is accessed once a day to any authentication method. Refresh the number of times every day.
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	Enable Secure Portal: If enabled, unauthorized guests will be redirected to the splash page by using HTTPS protocol. If not, the HTTP protocol will be used.

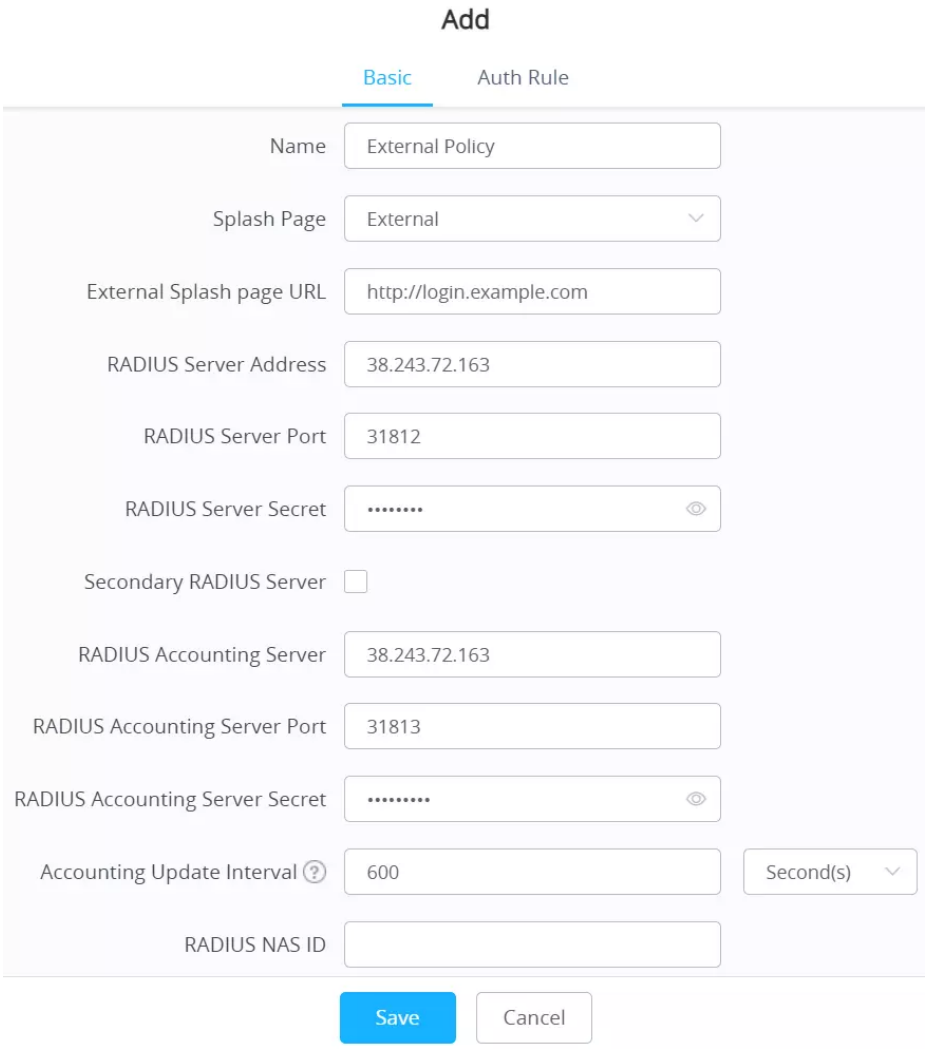
Captive Portal - Policy List - Splash Page is "Internal"

Notes:

If Facebook authentication is configured, you will need to log in your Facebook account of https://developers.facebook.com/apps , and set the OAuth redirect to : https://cwp.gwn.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3

If X authentication is configured, sign in to the X Developer Portal and set the callback URL to: http://cwp.gwn.cloud:8080/GsUserAuth.cgi

External Splash Page



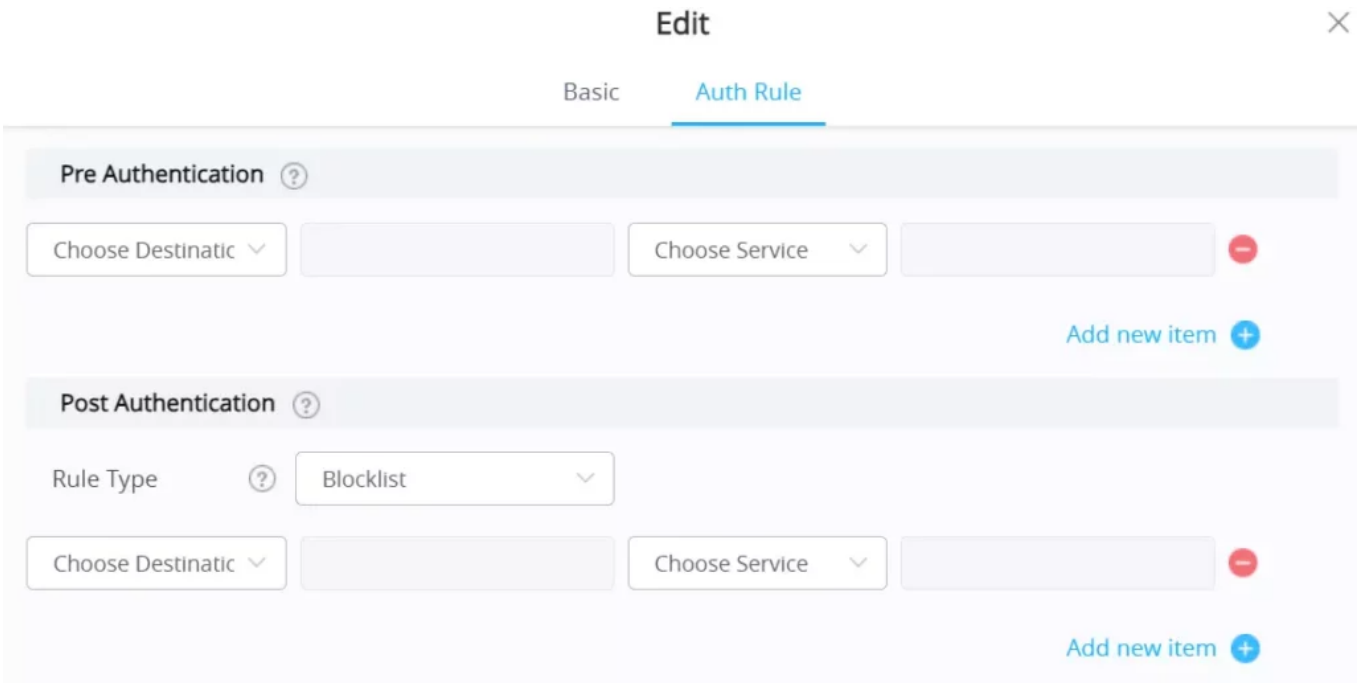
Policy List - External

Name	Name of the policy: e.g. External Policy
Splash Page	Type of splash page to use (Internal or External), in this case it's External: e.g. External
External Splash page URL	URL for the external splash page for user authentication:e.g. http://login.example.com
RADIUS Server Address	IP address of the RADIUS server used for authentication: e.g. 38.243.72.163
RADIUS Server Port	Port number for the RADIUS authentication server: e.g. 31912
RADIUS Server Secret	Shared secret for authenticating with the RADIUS server
Secondary RADIUS Server	Option to enable a secondary RADIUS server for redundancy
RADIUS Accounting Server	IP address of the RADIUS accounting server: 35.205.62.147
RADIUS Accounting Server Port	Port number for the RADIUS accounting server: e.g. 31913
RADIUS Accounting Server Secret	Shared secret for authenticating with the RADIUS accounting server.
Accounting Update Interval	Interval in seconds for sending accounting updates to the server: e.g. 600 seconds
RADIUS NAS ID	Network Access Server Identifier for the RADIUS server: Optional
Redirect URL	The URL to which users are redirected after successful authentication. This can be used to direct users to a specific landing page or website post-login. E.g. http://welcome.example.com

MAC-Based RADIUS	When enabled, the client's MAC address is used as both the RADIUS username and password for pre-portal authentication. If the RADIUS server verifies and confirms the presence of the client's MAC address in its database, the client is automatically authenticated. This simplifies the authentication process by allowing devices to bypass manual credential input during initial connection.Note: supported only GWN7670.
Enable HTTPS Redirection	When enabled, both HTTP and HTTPS requests from client devices are redirected using the HTTPS protocol. However, users may encounter an invalid certificate error during HTTPS browsing before authentication. If disabled, only HTTP requests will be redirected, ensuring a smoother user experience for HTTPS traffic prior to authentication.
Enable Secure Portal	When enabled, the communication between the client (STA) and the access point (AP) will use the HTTPS protocol, ensuring secure data transmission. If disabled, the communication will fall back to the less secure HTTP protocol.

Policy List - External

In case social media authentication is used, the user needs to allow some traffic between the AP and social medial platforms (Facebook API as example) to send authentication credentials and receive reply, this traffic can be allowed using the Authentication rules which are explained below.



Authentication rules

Pre-Authentication Rules

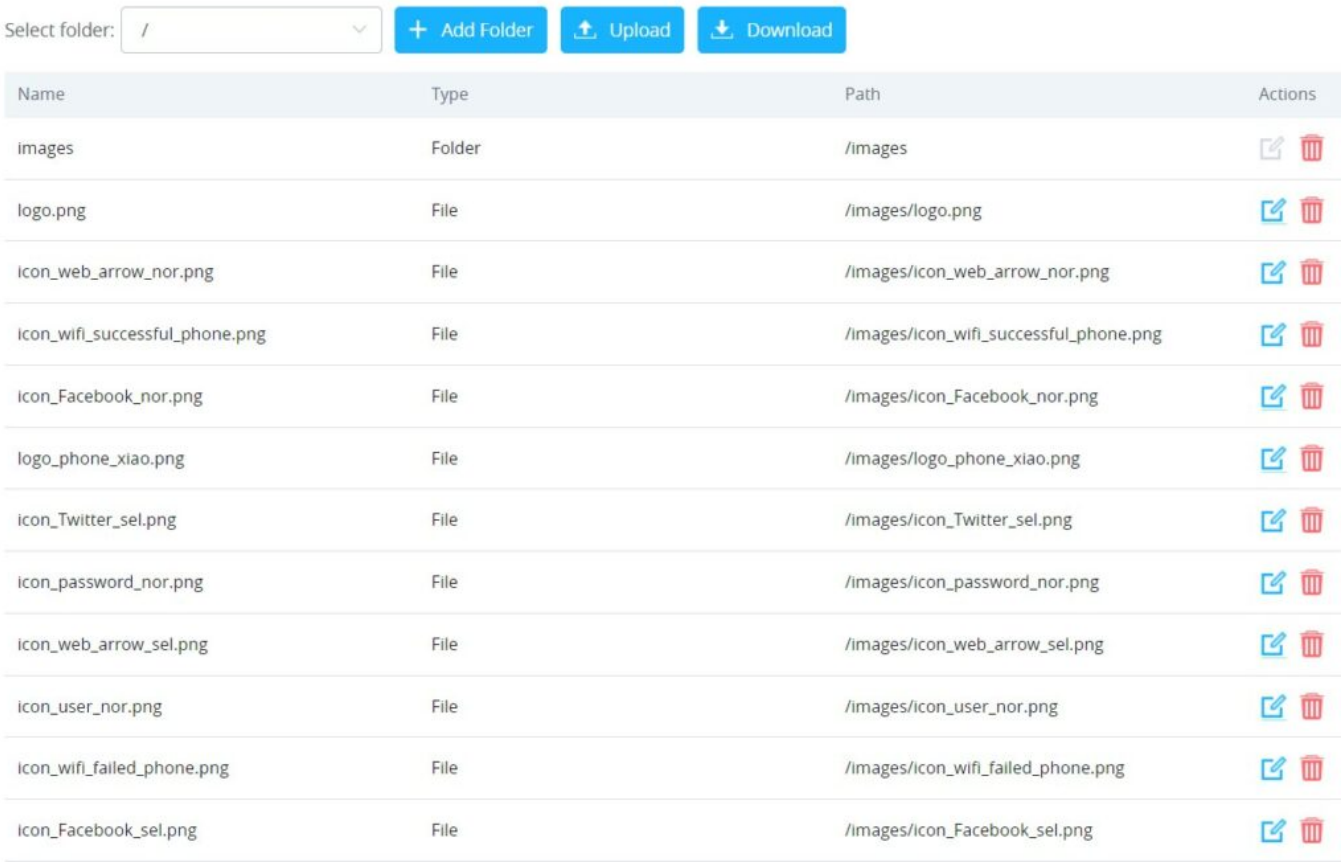
Using this option, users can set rules to match traffic that will be allowed for connected Wi-Fi users before the authentication process. For example, if users need to set up Facebook authentication, some traffic should be allowed to the Facebook server(s) to process the user's authentication. Or simply used to allow some type of traffic for unauthenticated users.

Post-Authentication Rules

On the other hand, post authentication rules are used to match traffic that will be banned for Wi-Fi clients after authentication. As an example, if you want to disallow connected Wi-Fi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that traffic and once a connected client passes the authentication process they will be banned from issuing telnet and SSH connections.

Splash Page

Files configuration page allows users to view and upload HTML pages and related files (images...).



Captive Portal - Splash Page

User can add folder in corresponding folder by selecting the folder and click **Add Folder**.

- Select **Upload** to upload a file from the local device.
- Select **Download** to download files from the Captive Portal folder.
- Select **Replace** to replace the selected file with a new one.
- Select **Delete** to delete the file.

Vouchers

Voucher Feature Description

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

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

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

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

The usage of voucher feature needs to be combined with captive portal that is explained after this section, in order to have the portal page requesting clients to enter voucher code for authentication.

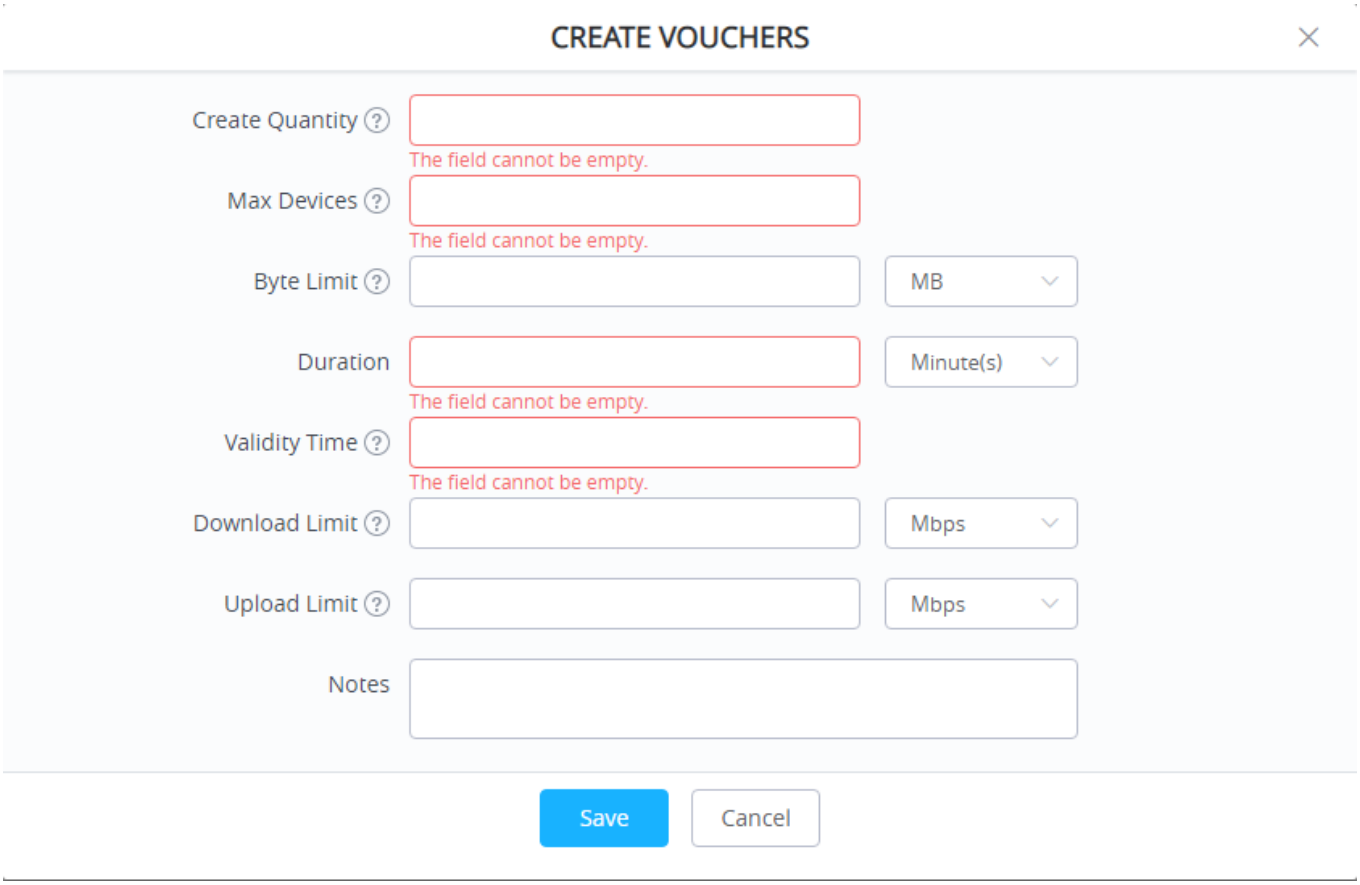
Voucher Configuration

To configure/create vouchers for clients to use, follow below steps:

1. On controller web GUI, navigate under "**Captive Portal** -> **Vouchers**"
2. Select **Add** to create a voucher.
3. Enter voucher details which are explained on the next table.
4. Press save to create the voucher(s).

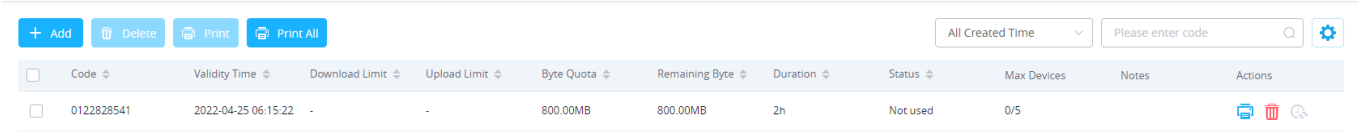
Notes:

- Users can specify how many vouchers to generate with the same profile, this way the GWN will generate as many vouchers as needed with the same settings to avoid creating them one by one.
- The administrators can verify the status of each voucher on the list (In use, not used, expired ...etc.).
- Select **Print** to print the voucher, **Delete** to delete it, or **Renew** to renew it.



Add Voucher Sample

The figure below shows the list of vouchers after GWN randomly generates the code for each one.



Vouchers List

Select **Delete** or **Print** to process the selected vouchers. Select **Print All** to print every voucher.

Use the **Date Filter** list to display vouchers created during a selected date and time range.

The following table summarizes descriptions for voucher configuration parameters:

Field	Description

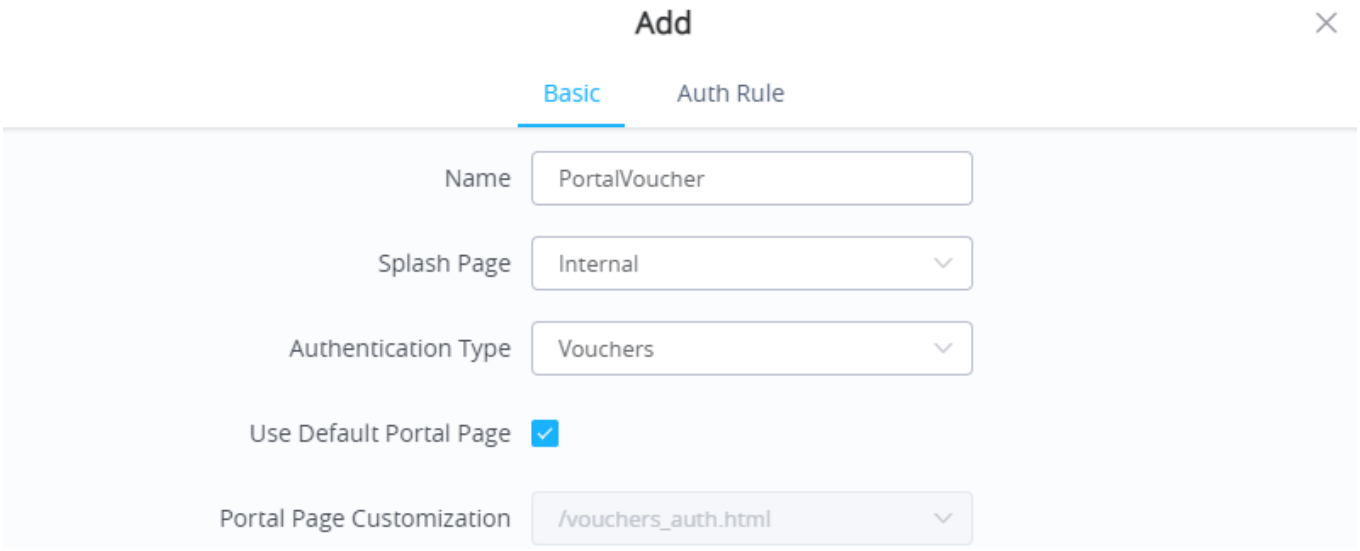
Create Quantity	Specify how many vouchers to generate with the same profile/settings (duration, bandwidth, and number of users). Valid range: 1 - 1000.
Max Devices	Specify the download byte limit for the voucher. The unit can be either M (Megabyte) or G (Gigabyte). Valid range: 10 - 1048576 (M), 1 - 1024 (G)
Byte Limit	Specify the download byte limit for the voucher. The unit can be either M (Megabyte) or G (Gigabyte). Valid range: 10 - 1048576 (M), 1 - 1024 (G)
Duration	Notes for the administrator when checking the vouchers list.
Validity Time	Set the validity period of the credentials, limited to 1-365. The unit is "day".
Download Limit	Set the download bandwidth speed limit (in Kbps or Mbps).
Upload Limit	Set the upload bandwidth speed limit (in Kbps or Mbps).
Notes	Notes for the administrator when checking the list vouchers list.

Voucher Parameters

Using Voucher with GWN Captive Portal

In order to successfully use the voucher feature, users will need to create a captive portal in order to request voucher authentication codes from users before allowing them to access the internet. More details about captive portal will be covered in the next section, for voucher configuration please follow below steps.

1. Go under "**Captive Portal** -> **Policy List**" menu.
2. Select **Add** to create a new captive portal policy.
3. Set the following parameters as shown on the screenshot for basic setup, then save and apply.



Captive Portal with Voucher authentication

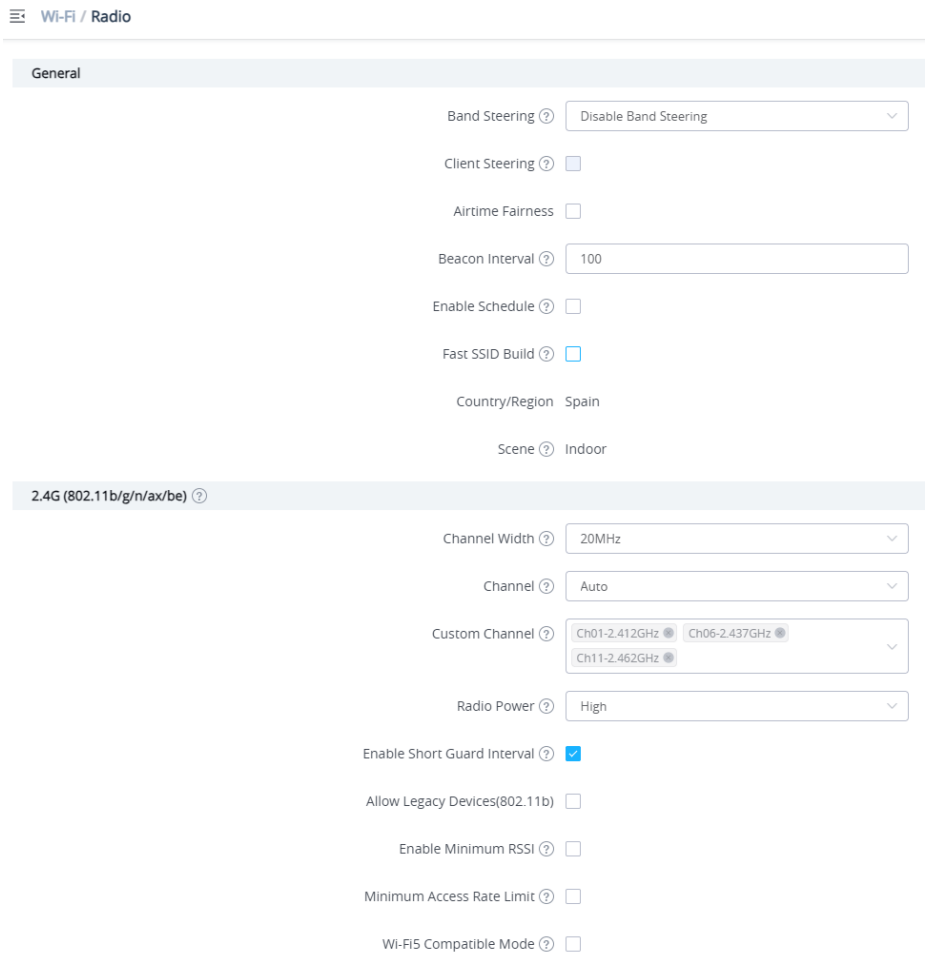
Then go under your SSID configuration page and enable the generated captive portal under the Wi-Fi settings tab.

RADIO

When using GWN76XX as a Primary Access Point, users can edit the frequency band used by the AP and channel used, along with the Transmission power for each band.

Log in as Primary to the GWN76XX Web GUI and go to **Radio.**

On models that display the **Wi-Fi** menu, open **Wi-Fi > Radio**. The radio configuration options are the same; only the menu location differs.



Radio

General	
Band Steering	Band Steering helps redirect dual-band and tri-band clients to the most appropriate radio band (2.4 GHz, 5 GHz, or 6 GHz, depending on what the access point supports) to improve performance and spectrum utilization.Four options are available:Disable Band steering: Disables band steering and the access point accepts the band chosen by the client.2G in Priority: Tri-band / dual-band clients are steered to the 2.4 GHz band when possible.5G in Priority: Tri-band / dual-band clients are steered to the 5 GHz band when possible.6G in Priority: Tri-band clients are steered to the 6 GHz band when available, taking advantage of the wider spectrum.Balance: The access point balances client connections across the 2.4 GHz, 5 GHz, and 6 GHz bands based on spectrum utilization.Note: It is recommended to enable Voice Enterprise on SSIDs that use Band Steering for better roaming and steering behavior.
Client Steering	This feature will help Wi-Fi clients to roam to other APs within the same Network. Note: Once enabled, Band Steering in Access Device -> Configuration -> Configure cannot be configured. SSID->Wifi Settings->802.11k will be enabled
RSSI Threshold (dBm)	This option is only available if Client Steering is enabled.Specify the RSSI Threshold before clients get steered away to another AP.Note: Must be an integer between -80 and -65.
Client Access Threshold	This option is only available if Client Steering is enabled.Specify the Client Access Threshold before the AP won't accept clients and they will be steer away to another AP with less connected clients.Note: Must be an integer between 10 and 100.
Airtime Fairness	Allow faster clients to have more airtime than slower clients.

Beacon Interval	Configure the beacon period, which decides the frequency the 802.11 beacon management frames AP transmits. Please input integrates from 40 to 500.When AP enables 0-2 SSIDs, the interval value will be effective are the values from 40 to 500.When AP enables 3-8 SSIDs, the interval value will be effective are the values from 100 to 500.When AP enables more than 8 SSIDs, the interval value will be effective are the values from 200 to 500.Note: mesh feature will take up a share when it is enabled.
Enable Schedule	Configure a schedule for when the Wi-Fi will be ON or Off, by default is disable or the user can enable it and select a shedule form the drop-down list or use radio settings.
Fast SSID Build	When enabled and there are fewer than 8 SSIDs on the access point, creating or deleting SSIDs takes effect more quickly. This setting controls how fast the AP rebuilds SSIDs and can inherit the value from the radio settings. Note: This feature is not supported on SSIDs using MLO or WPA2/WPA3 with PPSK without RADIUS.
Country/Region	Display the country/region of the AP.Note: To configure the country/Region, Navigate to System -> Settings page.
Scene	Configure whether to disable/enable 5.150-5.350GHz (channels 36-64) for outdoor usage.Note: The "Scene" is only effective for the outdoor type of access points.
2.4G/5G/6G (802.11b/g/n/ac/ax/be)	
Channel Width	Choose the Channel Width, note that a wider channel will give better speed/throughput, and a narrow channel will have less interference. 20MHz is suggested in a very high-density environment.
40MHz Channel Location	Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be Secondary below Primary, Primary below Secondary or Auto.
Channel	Select the working channel for this radio. The available channels depend on the selected band (e.g., 2.4 GHz, 5 GHz, or 6 GHz, depending on the model) and the configured regulatory domain.Auto: The access point evaluates the RF environment and selects an appropriate channel (from the allowed list) only once specifically when the radio starts or when the configuration is applied. The channel remains static during normal operation.Dynamically Assigned by RRM: The access point uses Radio Resource Management (RRM) to continuously evaluate RF conditions. It adjusts the channel in real-time to reduce interference and minimize channel overlap without requiring a reboot.Note: If the device is connected through a wireless Mesh, the channel may be determined by the mesh backhaul, and this setting might not take effect.Default is Auto.
Channel Scan	Controls how the radio performs channel scanning for RRM when Channel is set to Dynamically Assigned by RRM.Enable: Continuously scans the current working channel to collect RF information. This may cause brief interruptions and can disconnect connected clients.Auto: Scans only when no clients are connected to the radio and stops scanning when a client is connected, reducing impact on active clients.Schedule: Performs channel scanning only during the configured schedule period.
Schedule	Select the time profile during which channel scanning is allowed when Channel Scan is set to Schedule. The radio will perform channel scanning only within the selected time period (for example, during off-peak or maintenance hours).Note: This option is displayed only when Channel Scan is set to Schedule.
Custom Channel	Select the list of allowed channels for this radio. The available choices depend on the band (2.4 GHz, 5 GHz, or 6 GHz) and regulatory domain. When Channel is set to Auto or Dynamically Assigned by RRM, the access point will choose the working channel only from the channels selected here. Multiple selections are possible.

Radio Power	Set the Radio Power depending on the application, distance, and desired cell size. Options available typically include: "Low", "Medium", "High", "Custom", "Dynamically Assigned by RRM", and "Auto".Auto: The access point calculates and applies the most suitable transmission power only once-upon device boot-up or when a configuration change is applied. The power level remains static thereafter.Dynamically Assigned by RRM: The access point uses Radio Resource Management (RRM) to continuously monitor the RF environment. It actively adjusts the transmission power in real-time to optimize coverage and mitigate interference as environmental conditions change.The default is "High"
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	Configure whether to enable/disable Minimum RSSI function. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.
Minimum Access Rate Limit	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.
Wi-Fi5 Compatible Mode	Some old devices are not fully compatible with Wi-Fi6 and may not be able to scan the signal or have poor connection. After turning on this feature, it will switch to Wi-Fi5 mode to solve the compatibility problem. and turn off Wi-Fi6 related functions..

Radio - Global configuration

Model	CE	RCM	FCC	IC	ANATEL
GWN7603	Yes	Yes	Yes	Yes	Not listed
GWN7604	Yes	Yes	Yes	Yes	Not listed
GWN7605	Yes	Yes	Yes	Yes	Not listed
GWN7605CLR	Yes	Yes	Yes	Yes	Not listed
GWN7605LR	Yes	Yes	Yes	Yes	Not listed
GWN7615	Yes	Yes	Yes	Yes	Not listed
GWN7624	Not listed	Yes	Yes	Not listed	Not listed
GWN7625	Yes	Yes	Yes	Yes	Not listed
GWN7630	Yes	Yes	Yes	Yes	Yes
GWN7630LR	Yes	Yes	Yes	Yes	Not listed
GWN7660	Yes	Yes	Yes	Yes	Not listed
GWN7660E	Yes	Yes	Yes	Yes	Not listed
GWN7660ELR	Yes	Yes	Yes	Yes	Not listed
GWN7660EM	Yes	Yes	Yes	Yes	Not listed
GWN7660LR	Yes	Yes	Yes	Yes	Not listed
GWN7661	Yes	Yes	Yes	Yes	Not listed
GWN7661E	Yes	Yes	Yes	Yes	Not listed
GWN7662	Yes	Yes	Yes	Yes	Not listed
GWN7664	Yes	Yes	Yes	Yes	Not listed
GWN7664E	Yes	Yes	Yes	Yes	Not listed
GWN7664ELR	Yes	Yes	Yes	Yes	Not listed
GWN7664LR	Yes	Yes	Yes	Yes	Not listed

GWN7665	Yes	Yes	Yes	Yes	Not listed
GWN7670	Yes	Yes	Yes	Yes	Not listed
GWN7670E	Not listed	Not listed	Not listed	Not listed	Not listed
GWN7670ELR	Not listed	Not listed	Not listed	Not listed	Not listed
GWN7670LR	Yes	Yes	Yes	Yes	Not listed
GWN7670WM	Yes	Yes	Yes	Yes	Not listed
GWN7672	Yes	Yes	Yes	Yes	Not listed
GWN7672L	Not listed	Not listed	Not listed	Not listed	Not listed
GWN7672WM	Yes	Yes	Yes	Yes	Not listed
GWN7673	Not listed	Not listed	Not listed	Not listed	Not listed
GWN7674	Yes	Yes	Yes	Yes	Not listed

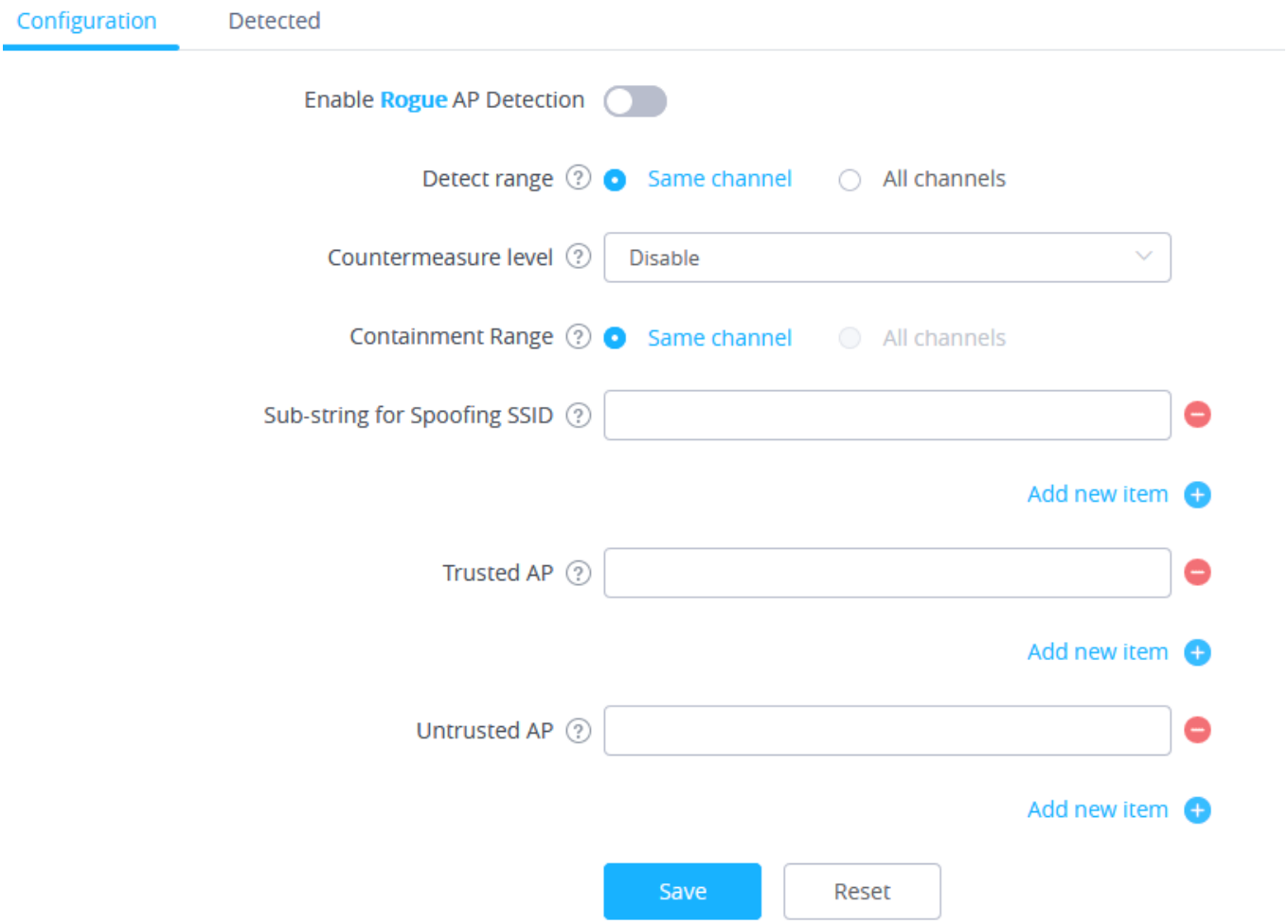
Source: GDMS Networking Device Comparison. Support reflects the recommended firmware listed by Grandstream. "Not listed" means the comparison page does not currently mark that model and regulatory domain as supported.

SECURITY

Rogue AP

The GWN Access Points offer the ability to prevent malicious intrusion to the network and increase the wireless security access of clients when introducing Rogue AP detection. The detected APs will be listed with all the details under the detected section for further intervention.

The figure below is the configuration page in order to enable Rogue AP detection, and we can set the trusted APs on the network.



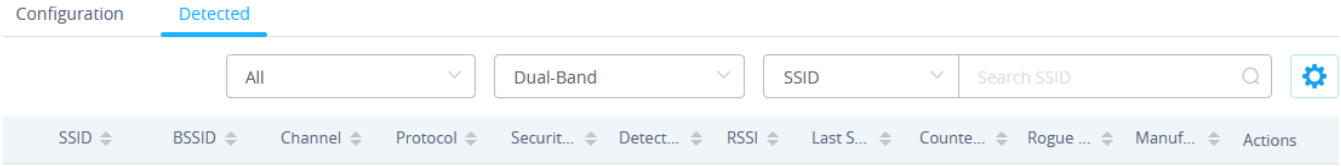
Rogue AP-Configuration

Field	Description
Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect range	Specify the rogue AP detect range. * 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. Default is Same Channel.
Countermeasure Level	Countermeasure level specifies the type of attacks which will be suspected by the AP. Select different levels: * High: Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. * Medium: Untrusted BSSID, Illegal access without authentication, Illegal access. * Low: Untrusted BSSID, Illegal access without authentication. Default is Disabled.
Containment Range	Specify the containment range: * 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 much AP performance. The default is Same Channel.
Sub-string for Spoofing SSID	Specify the containment range: * 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 much AP performance. The default is Same Channel.
Trusted AP	You can specify the MAC address of the trusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as a 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 an untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

Rogue AP

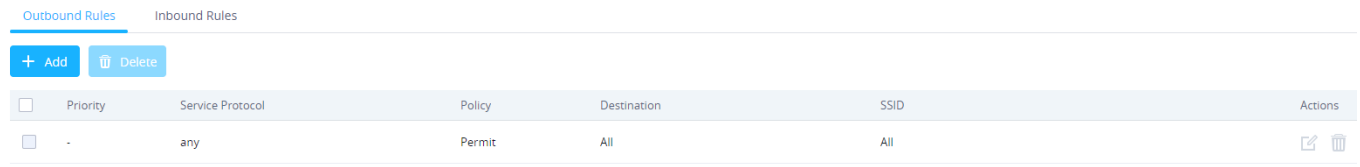
The figure below shows all rogue APs detected on the network by the GWN access point. Use **Search SSID** to filter the detected access points by network name.



Rogue AP-Detection

Firewall

This section allows users to control the outgoing and incoming traffic from clients by manually setting up policies to either deny or permit the traffic based on protocol type and by specifying SSIDs and destinations.

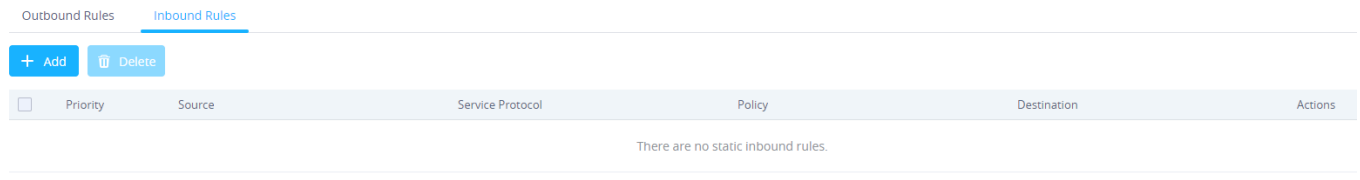


Firewall-Outbound

Field	Description
Service Protocol	Select the type of traffic to be affected by the outbound rule, like ICMP, HTTP, HTTPS... or you may add another type of traffic when selecting Custom. When set to Custom, the user could enter the following: * Protocol: TCP or UDP * Port: define the port used by this protocol.
Policy	Either select Permit or Deny Outbound traffic.
Destination	Select the type of traffic to be affected by the outbound rule, like ICMP, HTTP, HTTPS, or you may add another type of traffic when selecting Custom. When set to Custom, the user could enter the following: * Protocol: TCP or UDP * Port: define the port used by this protocol.
SSID	Select one or multiple SSIDs to apply the rule on.

Firewall- Outbound

The user can define outbound and inbound rules on the traffic from the options in the figure below:



Firewall-inbound

Field	Description
Service Protocol	Select type of traffic to be affected by the inbound rule, like ICMP, HTTP, HTTPS... or you may add another type of traffic when selecting Custom. When set to Custom, the user could enter the following: * Protocol: TCP or UDP * Port: define the port used by this protocol.
Policy	Either select Permit or Deny inbound traffic.

Source	Select either: * Particular IP: IP address of the source. * Particular Network: Network IP address. * All: the rule will apply to all destinations.
Destination	Configure the destination address. * All * Particular * IP Particular Domain * Particular Network

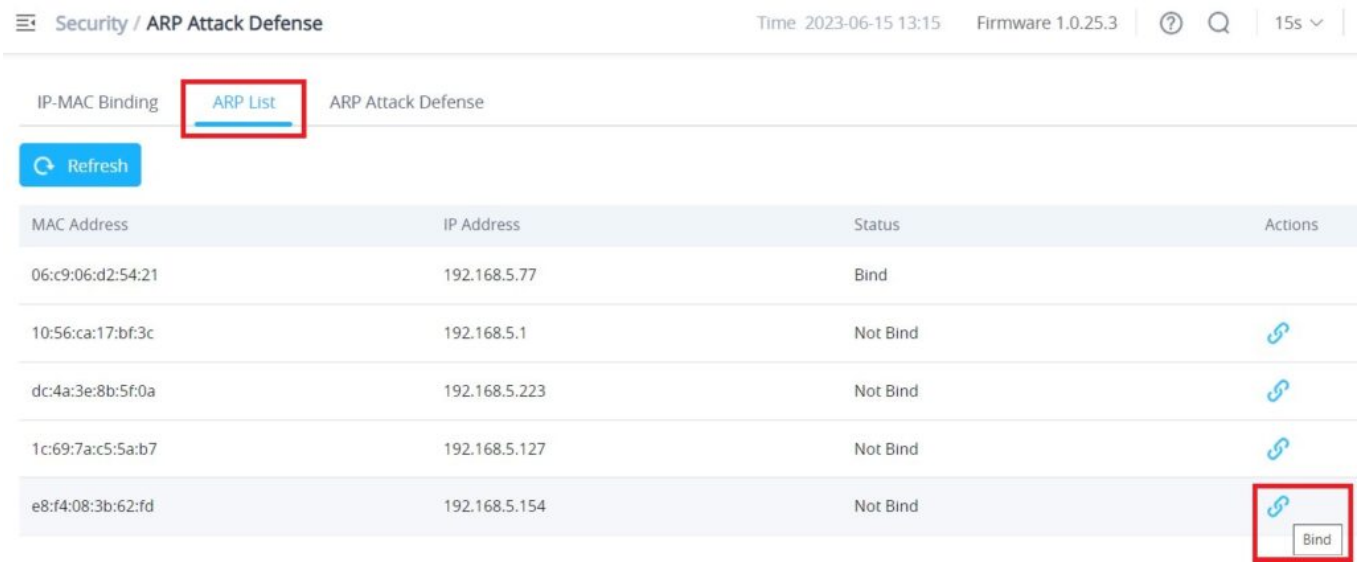
Firewall-Inbound

ARP Attack Defense

GWN Access points also support the ARP Attack Defense security feature. This feature protects clients from spoofing MAC addresses by binding the MAC address to an IP address.

ARP List

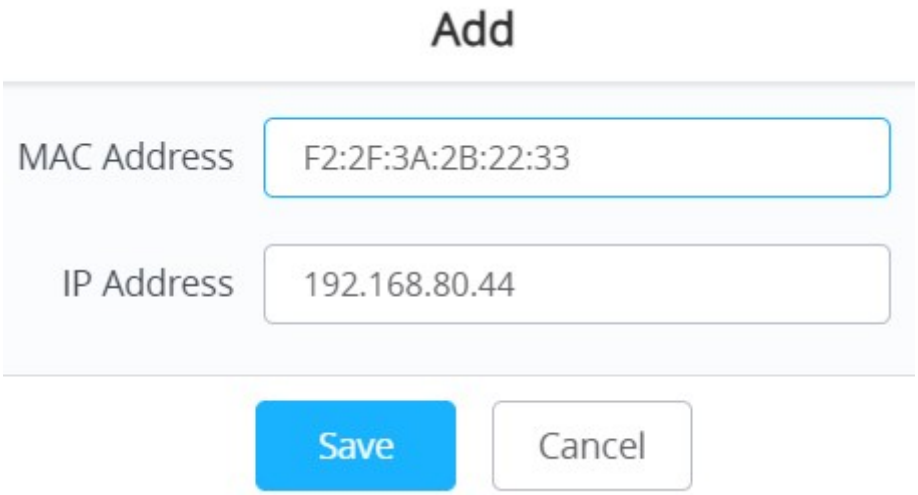
Navigate to **Web UI -> Security -> ARP Attack Defense**, on the ARP list tab, the user can see the current ARP table (MAC address -> IP address combination). Click on the "**Bind**" icon to bind the MAC address to an IP address.



ARP Attack Defense - ARP List

IP-MAC Binding

To make an IP-MAC address Binding manually, on the IP-MAC Binding tab, click on the "**Add**" button and then enter the IP address and the MAC address, then click save.



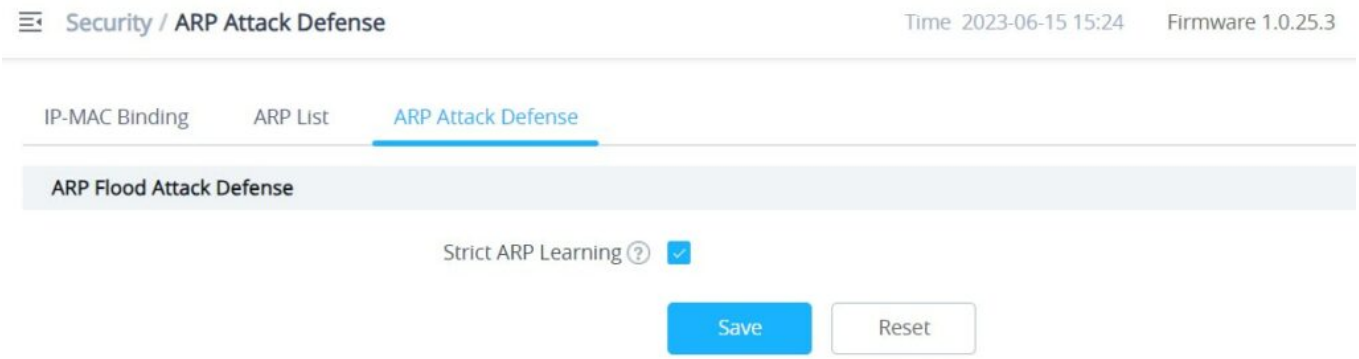
ARP Attack Defense - IP MAC Binding

To unbind or edit, click on the "**Delete** or **Edit**" icons under Actions. Please refer to the figure below:



ARP Attack Defense

Strict ARP Learning option only learns ARP from the ARP Reply responding to the ARP Request sent by this device.

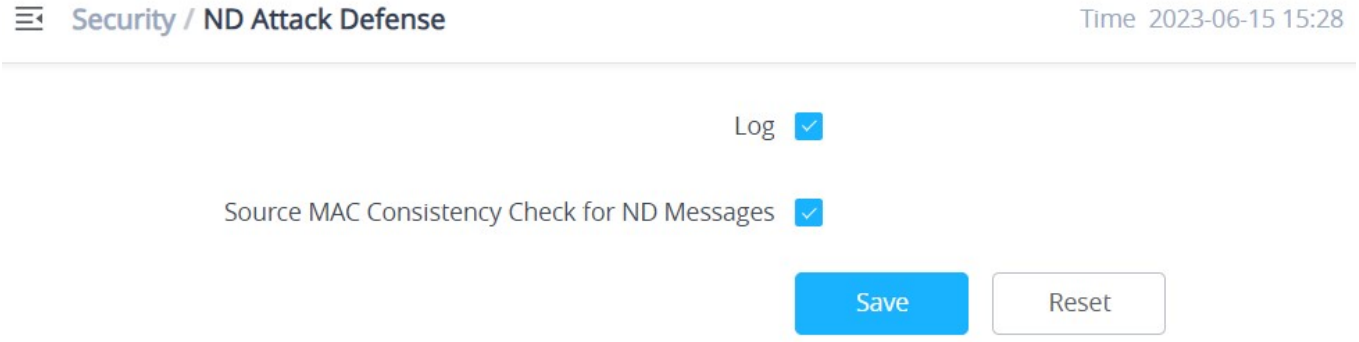


ARP Flood Attack Defense

Neighbor Discovery (ND) Attack Defense

ND Attack Defense is the equivalent of ARP Attack Defense, but using IPv6 addresses.

Navigate to **Web UI -> Security -> ND Attack Defense** page, then you can enable this security feature by clicking on "**Source MAC Consistency Check for ND Messages**", now the device will check for Source MAC addresses to avoid any spoofing. There is also the option to log these events by checking "**Log**" option.



ND Attack Defense

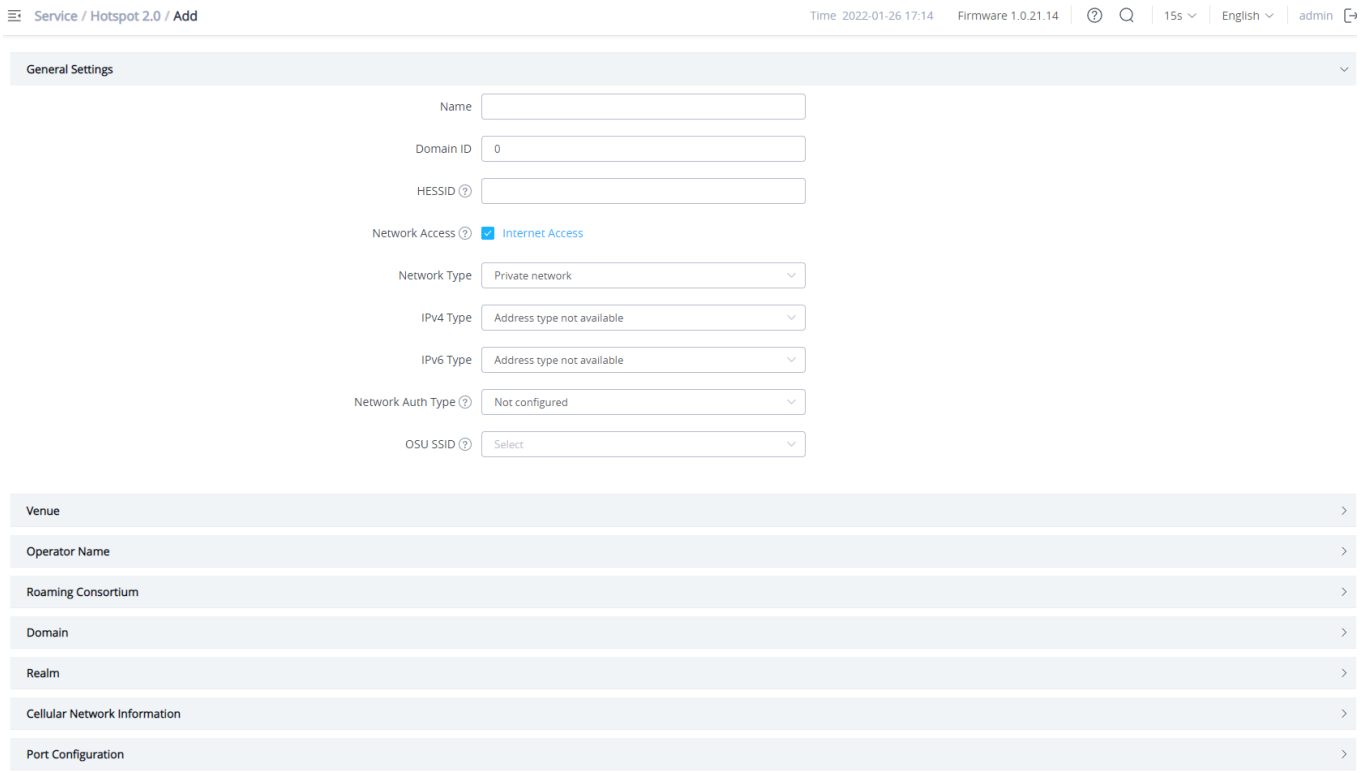
SERVICE

Hotspot 2.0

This section lists the configuration page for Hotspot 2.0. This is a technology that allows mobile devices to automatically connect to available Passpoint-certified Wi-Fi hotspots. This gives the device the liberty to hop from one hotspot on a network to another without the need to log in to each hotspot. This feature is currently in beta.

Note: GWN7660, GWN7630, GWN7630LR, GWN7605, GWN7605LR, GWN7615, GWN7625 GWN support Hotspot 2.0 R3beta

To enable this feature, proceed from the Access Point's web page -> Service -> Hotspot 2.0:



Hotspot 2.0

General Settings	
Name	Set name of the hotspot.
Domain ID	Set the Domain ID.
HESSID	Select IPv4 Type: * Address type not available * Public IPv4 address available * Port-restricted IPv4 address available * Single NATed private IPv4 address available * Double NATed private IPv4 address available * Port-restricted IPv4 address and single NATed IPv4 address available * Port-restricted IPv4 address and double NATed IPv4 address available * Availability of the address type is not known
Network Access	Enable or disable internet access.
Network Type	Select network type: * Private network * Private network with guest access * Chargeable public network * Free public network * Personal device network * Emergency services only network * Test or experimental * Wildcard
IPv4 Type	Select IPv4 Type: * Address type not available * Public IPv4 address available * Port-restricted IPv4 address available * Single NATed private IPv4 address available * Double NATed private IPv4 address available * Port-restricted IPv4 address and single NATed IPv4 address available * Port-restricted IPv4 address and double NATed IPv4 address available * Availability of the address type not known

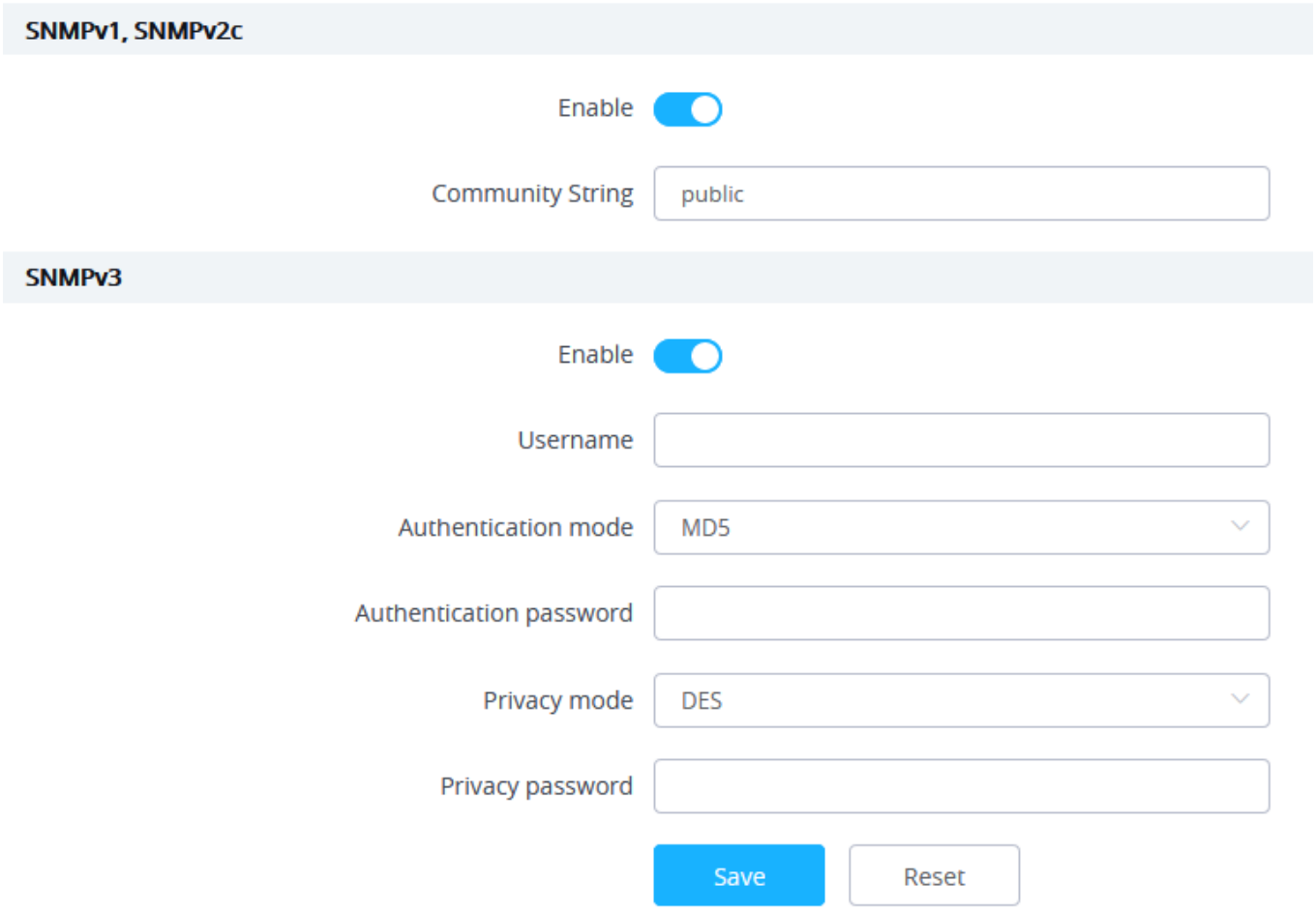
IPv6 Type	Select IPv6 Type: * Address type not available * Address type available * Availability of the address type is not known
Network Auth Type	Configure the Network authentication type to help users find and select the right network. Select either: * Acceptance of terms and conditions * On-line enrollment supported * http/https redirection * DNS redirection * Not configured
OSU SSID	Configure the Online Sign Up service's SSID. You need to add an SSID with Security Mode is Open, or OSEN or WPA2/OSEN.
Venue	
Venue Group	Select the Venue Group type: * Unspecified * Assembly * Business * Educational * Factory * Institutional * Mercantile * Storage * Utility * Vehicular * Outdoor
Venue Type	Select the Venue type, which will depend on the Venue Group.
Language Code	Select the language.
Venue Name	Set the Venue name.
Operator Name	
Language Code	Select the language.
Operator Name	Set the Operator name.
Roaming Consortium	
Roaming Consortium Name	Configure the Roaming Consortium Name to identify network operators. The format is H-H-H or H-H-H-H-H, where H is a 2-digit hexadecimal number.
Domain	
Domain	Enter the domain name.
Realm	
Realm	Select the EAP Method: EAP-TLS, EAP-SIM, EAP-TTLS, EAP-AKA, and EAP-AKA'.
Cellular Network Information	
Cellular Network Information	Enter the Name, Country Code, and Network Code.
Port Configuration	
IP Protocol	Configure the protocol type: ICMP, TCP, UDP, or ESP.
Port Number	Set the protocol port.
Port Status	Set the port status to either Open, Close, or Unknown.
Upload an XML file	
Filename	Specify the filename.
Time Stamp	Select the time stamp
Advice of Charge	
Type	Select the type: * Time-based * Data-volume-based * Time-and-data-volume-based * Unlimited
Realm	Select the Realm.
Language Code	Select the language code.
Currency Code	Select the currency: XSU, BTN, INR, CNY, MOP, HKD, XAF.
XML Content	Upload XML file
Advanced	
WAN Link Status	Set the WAN Link Status to either: Not configured, Link-up, Link-down or Link-test.

WAN Downlink Speed	Set Download speed.
WAN Uplink Speed	Set Upload speed.
GAS Fragmentation Limit	Set GAS fragmentation limit. Default is 1400.
GAS Comeback Delay	Set GAS comeback delay. Default is 0.
Disable Downstream Group-Addressed Forwarding	When this option is disabled, it means the DGAF is enabled, the AP will forward all downlink broadcast ARP messages and wireless group broadcasts. When this option is enabled, the DGAF function is disabled, the AP will discard all downlink broadcast ARP messages and wireless group broadcasts. Disable DGAF function to prevent attackers from using the vulnerability of all clients in the same BSS using the same Group Temporal Key (GTK) to forge Group address frames and then attack the clients.

Hotspot 2.0

SNMP

This section lists the SNMP options available to integrate the GWN76xx with monitoring systems.



SNMP

Field	Description
Enable	Enable SNMPv1/SNMPv2c.
Community String	Enter the SNMP Community string.
Enable	Enable SNMPv3.
Username	Enter the SNMPv3 authentication username.
Authentication Mode	Set the authentication mode to: either MD5 or SHA.

Authentication password	Enter the SNMPv3 authentication password.
Privacy Mode	Set the authentication mode to: either AES128 or DES.
Privacy password	Enter the privacy password.

SNMP

Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is a Layer 2 discovery protocol that allows directly connected network devices to exchange identification, interface, capability, and management information. GWN access points advertise this information automatically, helping administrators identify the access point, verify its connection, and map the local network topology from a neighboring LLDP-capable device.

The access point sends LLDP advertisements automatically and does not provide LLDP configuration parameters in its Web UI. To inspect the advertised information, use the LLDP neighbor or remote-device view on the directly connected LLDP-capable device. The procedure below uses a Grandstream switch as an example.

LLDP information advertised by the access point

An LLDP message is composed of Type-Length-Value (TLV) fields. Each TLV carries one category of information. The receiving device may use slightly different labels for the same information.

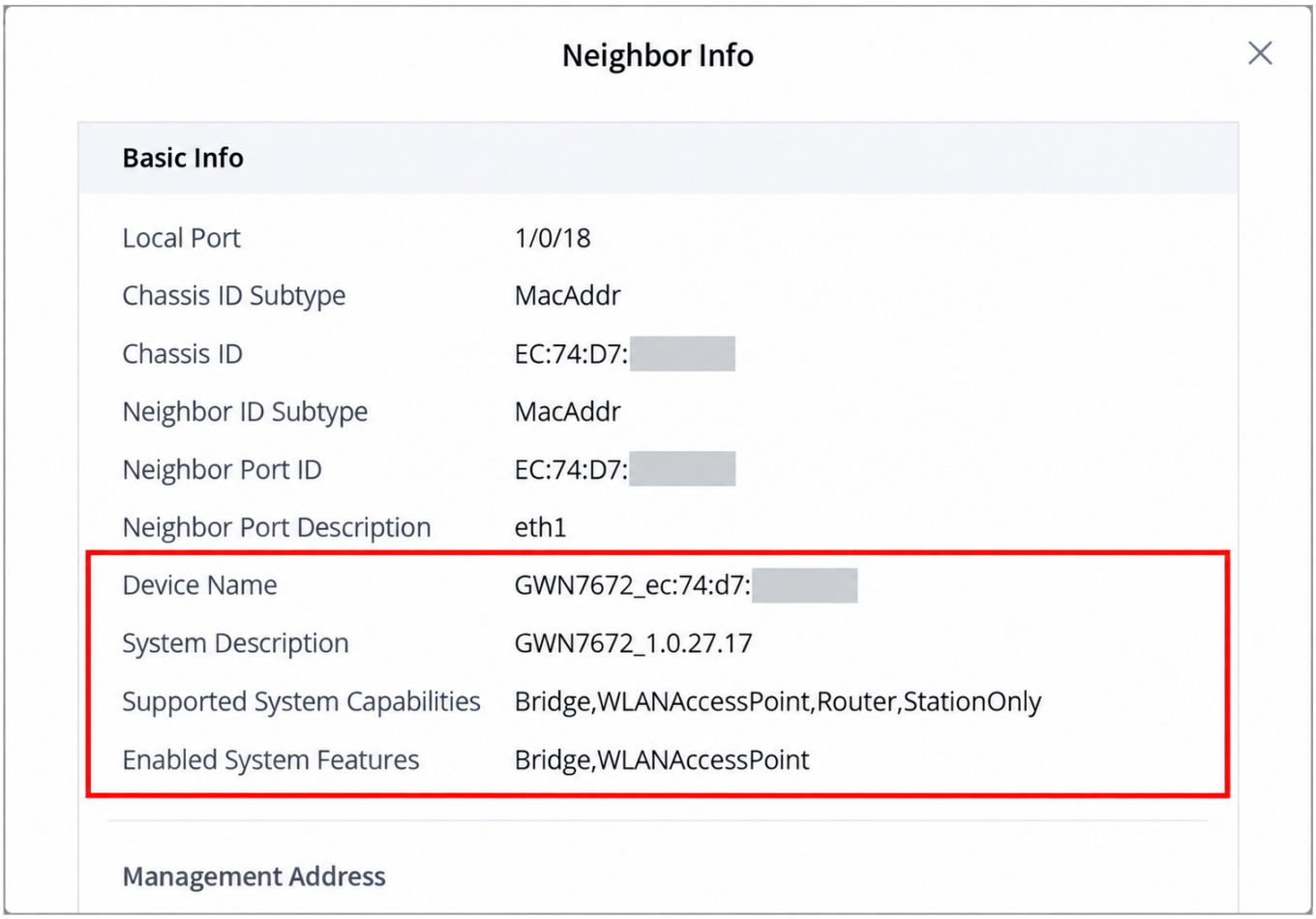
TLV or information	Behavior
Chassis ID	Identifies the access point. A neighboring LLDP-capable device commonly displays the AP device MAC address.
Port ID	Identifies the Ethernet interface connected to the neighboring device. The interface MAC address can differ from the Chassis ID.
Port Description	Provides the name of the connected Ethernet interface, such as eth1.
System Name	Identifies the access point by its advertised device name.
System Description	Provides device information such as the AP model and running firmware version.
System Capabilities	Reports the roles supported by the AP and the roles currently enabled, such as bridge and WLAN access point.
Management Address	Reports the IPv4 address advertised by the AP for management. The neighboring device may also display the interface subtype and interface number associated with the address.
Time to Live (TTL)	Tells the neighboring device how long to retain the entry if no newer LLDP advertisement is received.
IEEE 802.3 and LLDP-MED information	A compatible neighboring device may display additional link negotiation, aggregation, PoE, inventory, and LLDP-MED capability information.

Viewing LLDP information on a neighboring device

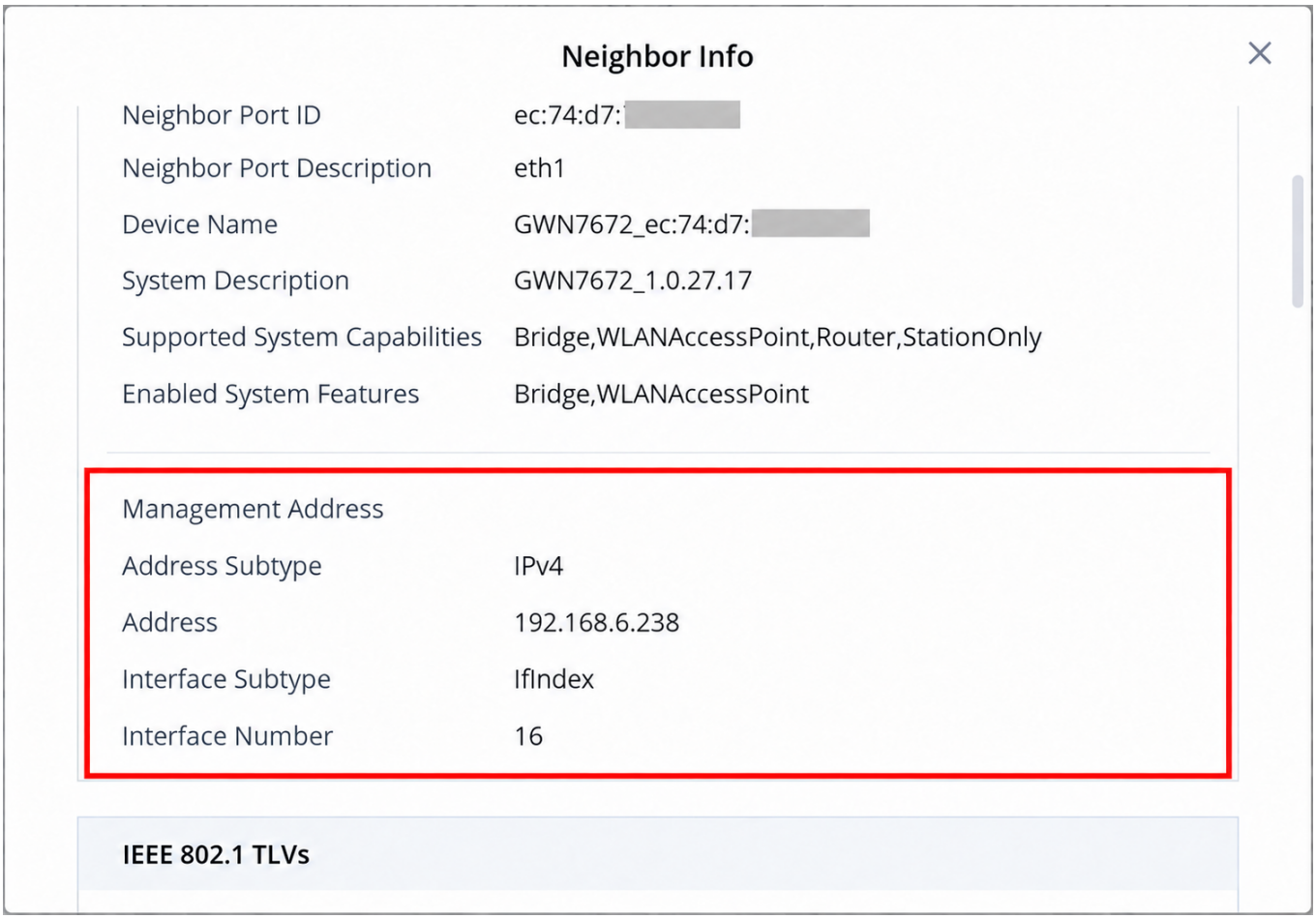
1. Connect the access point to a network interface on an LLDP-capable neighboring device.
2. Enable LLDP reception on that device and interface if required. The exact menu names depend on the device.
3. Open the LLDP neighbor or remote-device view and locate the entry for the interface connected to the access point.

4. Match the Chassis ID or Device Name with the access point, then open the entry to view its advertised Management Address and other TLVs.

In this example, a Grandstream switch displays LLDP information advertised by a connected Grandstream access point. Menu names, interface identifiers, and displayed values can differ on other LLDP-capable devices.



Access point identity and capabilities displayed by a Grandstream switch through LLDP



Management address information displayed in the same LLDP neighbor record

LLDP does not assign or change the AP IP address. The Management Address TLV only reports an address advertised by the access point.

Troubleshooting LLDP neighbor information

Observation	What to check
The AP does not appear in the neighbor table.	Confirm that the Ethernet link is active, LLDP reception is enabled on the neighboring device and correct interface, and the neighbor information has been refreshed after connecting the AP.
The advertised management address is unexpected.	Compare the advertised address with the current AP management address. Check the AP static or DHCP assignment and the management VLAN used by the connected interface.
The neighboring device continues to display an old address or device name.	Refresh the LLDP neighbor information and allow the previous entry to expire. A neighboring device can retain received information until its TTL reaches zero.
The Chassis ID and Port ID are different.	This can be expected. The Chassis ID identifies the AP, while the Port ID identifies the connected Ethernet interface.
The advertised address cannot be reached.	LLDP reports neighbor information but does not confirm IP connectivity. Verify the management VLAN, addressing, routing, and administrative access policy separately.

DHCP Server

Users could create and manage multiple DHCP server pools which will be mapped to the SSID using VLAN tag, for example when creating a DHCP pool under "**System Settings** -> **DHCP Server**" users need to set a VLAN ID and the same ID should be set under the SSID field to map the configured DHCP pool with the SSID. This way users could configure multiple SSIDs mapped to multiple VLANs on the network in which case they are isolated by layer 2 switching.

The table below summarizes the configuration parameters for DHCP server.

Field	Description
Name	Set the name of the DHCP Pool.
Enable	Enable/Disable the DHCP pool.
VLAN ID	Set a VLAN ID, same one should be set on SSID settings to map it with the DHCP pool.
DHCP Server Static Address	Configure the static address of the DHCP server (through which GWN Primary AP will be accessible).
DHCP Server Subnet Mask	Set the subnet mask for the DHCP Pool.
DHCP Start Address	Set the start address for DHCP
DHCP End Address	Set the end address for DHCP
DHCP Lease Time	Set the DHCP lease time for the clients (default 12h).
DHCP Options	Add the Option items for DHCP, detailed option contents can be found via: https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq
DHCP Gateway	Set the gateway for DHCP, and it is better to set the gateway, should be different that the static IP of the access point and on the same subnet.
DHCP Preferred DNS	Set the preferred DNS for DHCP
DHCP Alternated DNS	Set the alternated DNS for DHCP

DHCP Server Parameters

NAT Pool

GWN76xx NAT feature defines an address pool from which the Wi-Fi clients will acquire their IP address so that the access point acts as a lightweight home router.

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

Field	Description
Default Gateway	Set the gateway IP address. Note: The gateway address cannot be in the same network segment as the uplink network.
DHCP Server Subnet Mask	Set the gateway mask.
DHCP Lease Time	Set the DHCP Lease time.
DHCP Preferred DNS	Set the preferred DNS for DHCP
DHCP Alternate DNS	Set the alternated DNS for DHCP

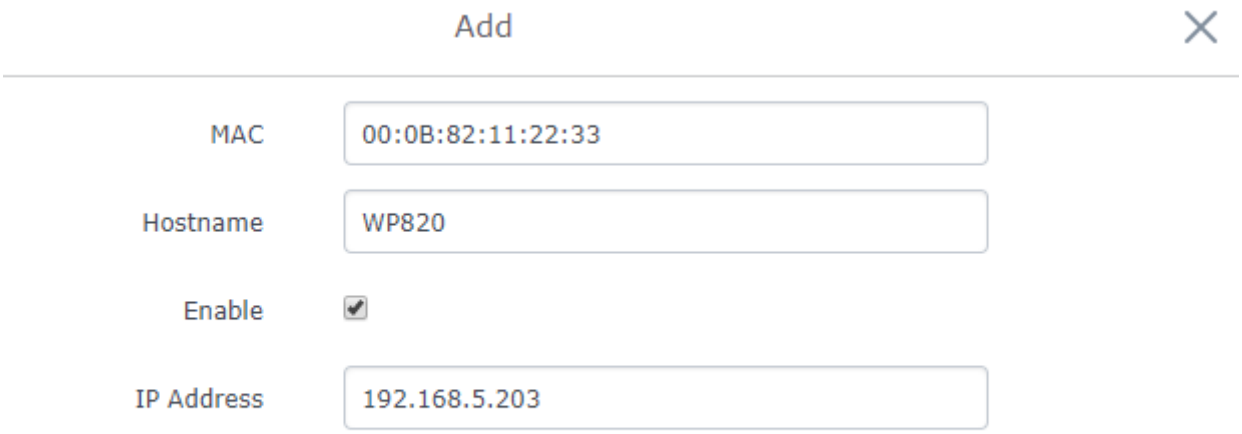
NAT Pool Parameters

Static DHCP

Users can use this feature in order to set static DHCP that binds to certain clients, to whom you do not want the IP address to change.

To configure Static DHCP, please follow below steps:

1. Select **Add** to create a new entry.
2. Enter the name of the device, along with its MAC address and IP address



DHCP Binding

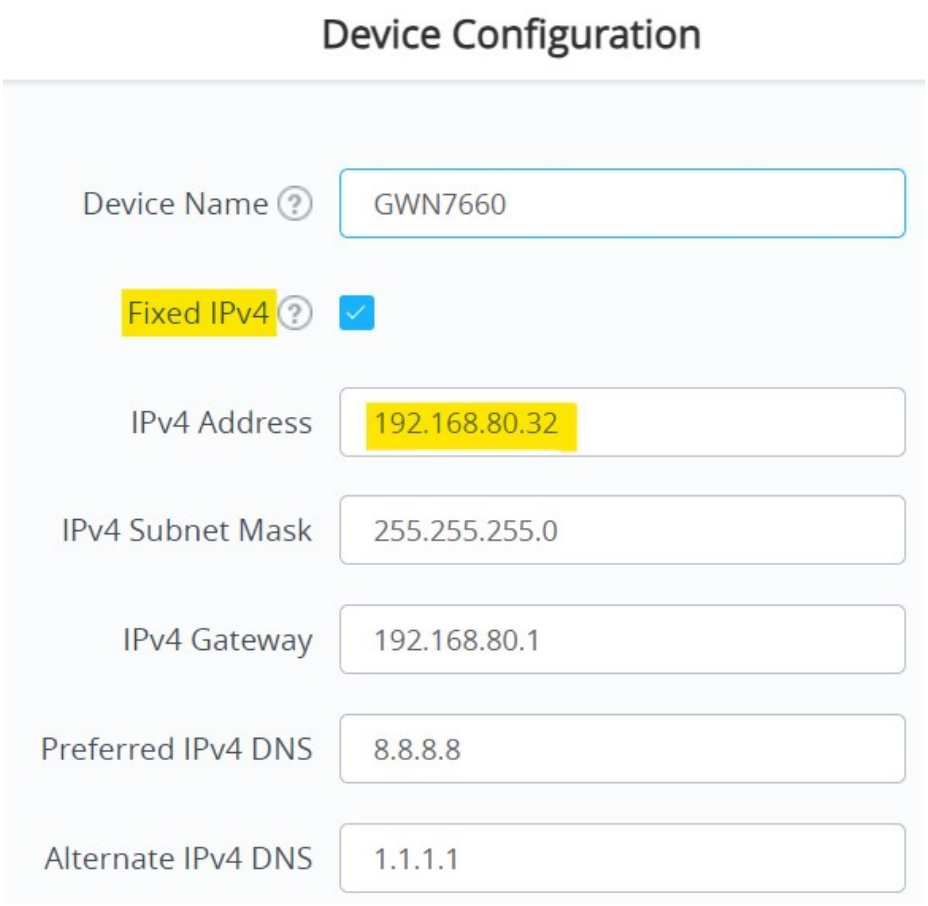
- Press Save and Apply to submit the changes.

DHCP Relay

DHCP Relay is a network device that forwards IP addresses from the DHCP Server to client devices, even if the DHCP server is on a different network (ex, VLAN). This way, we can have a dedicated DHCP server on many networks. GWN access points can be configured as a DHCP relay agent. Please follow the steps below:

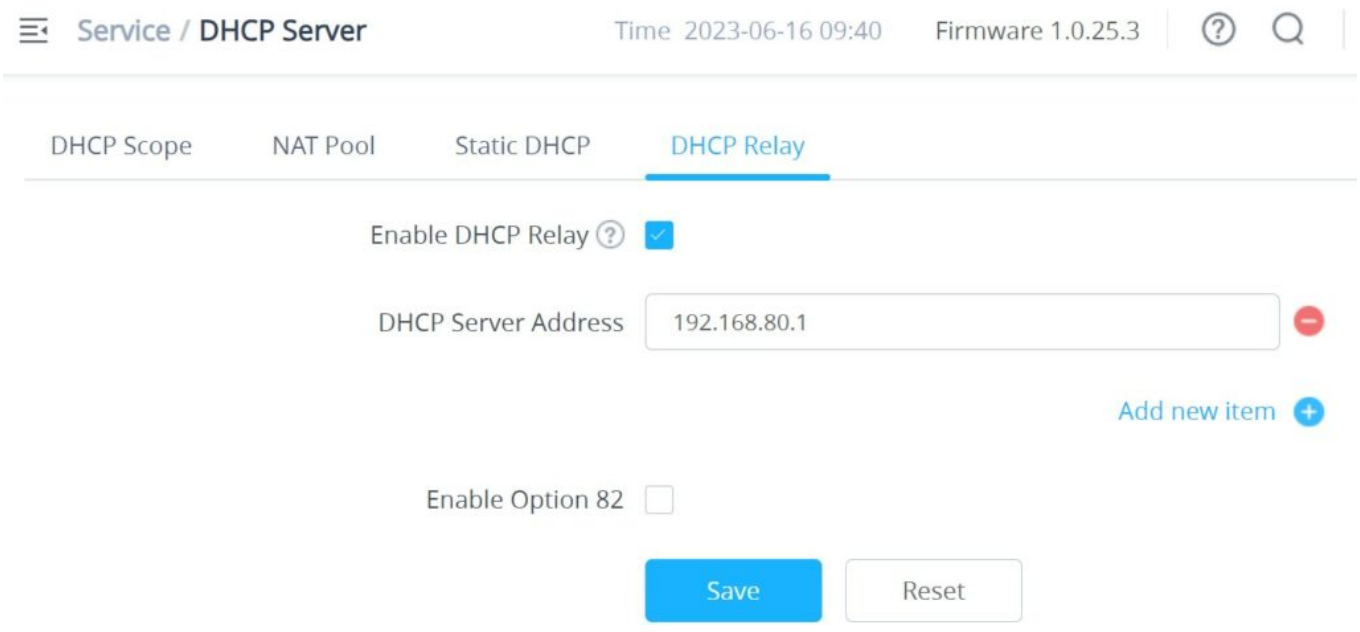
Prerequisite: Before configuring DHCP Relay, first we have to assign a static IP address to both devices that will be acting as a DHCP Server and DHCP Relay. In our case, it's two GWN76xx Access Points.

1. The first step in our example is to make a GWN access point as a DHCP Server, please refer to DHCP Server configuration.
2. Navigate to **Web UI -> Access Points -> Configuration**, click on the access point or click on the "**Edit**" icon, then the device configuration window will show up. Set a static IP for both access points (one acting as a DHCP Server and the other one as a DHCP Relay), please refer to the figure below.



Setting up a static IP

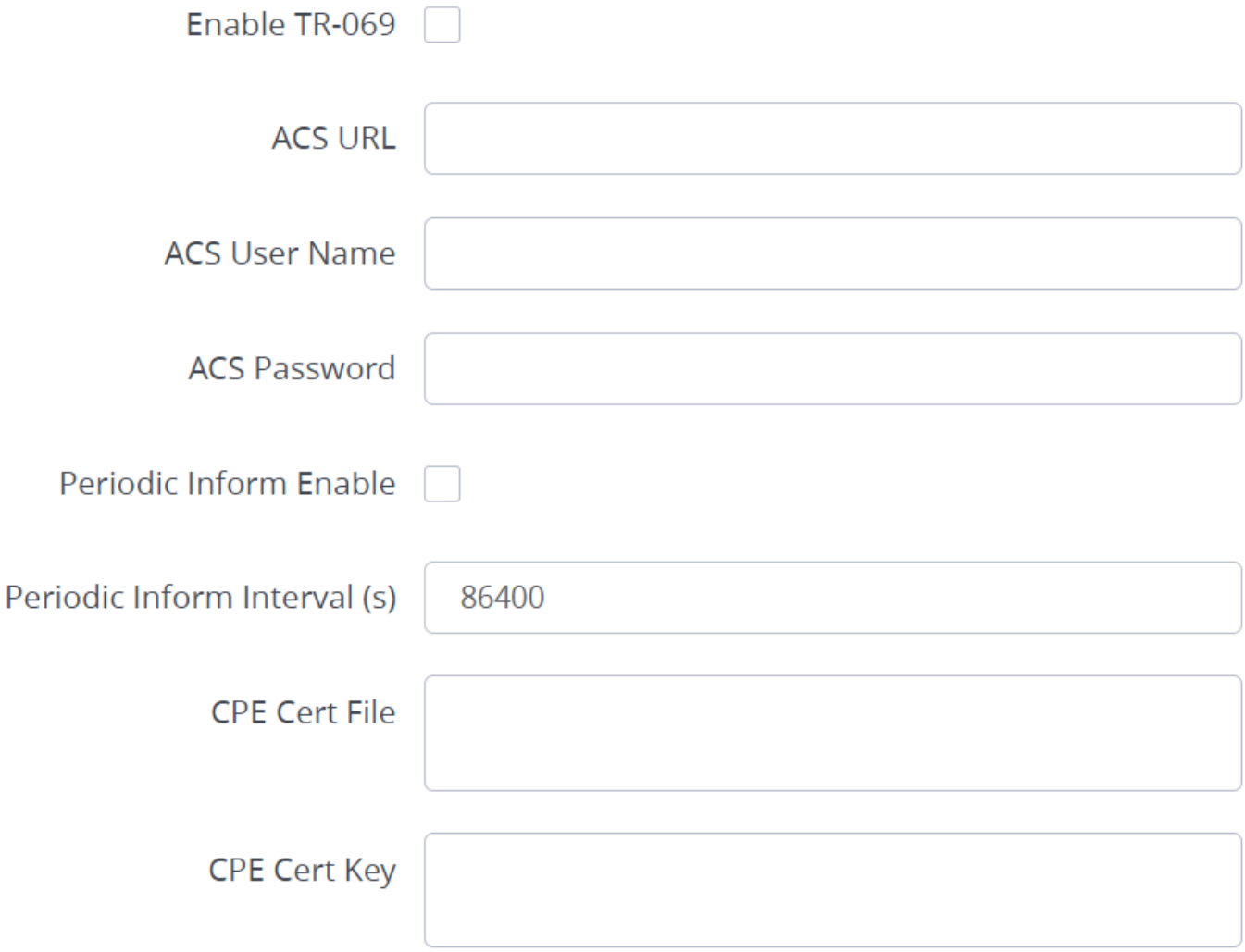
3. To configure DHCP Relay, please navigate to GWN access point **Web UI -> Service -> DHCP Server -> DHCP Relay** tab, then enable DHCP Relay and then enter the DHCP Server Address (ex, GWN access point).



DHCP Relay

A router-side configuration could be required to set up VLANs for both access points to be able to communicate.

TR-069



TR-069

Field	Description
Enable TR-069	Configure whether to enable TR-069. Note: Once enabled, this device cannot be managed by GDMS Networking anymore.
ACS URL	URL for TR-069 Auto Configuration Server (ACS).
ACS User Name	When AP sends a connection request to ACS, the username that ACS authenticates TR-069 client, that is AP, must be consistent with the configuration on the ACS side.
ACS Password	The password of ACS for AP authentication must be consistent with the configuration of ACS side.
Periodic Inform Enable	If enabled, AP will send connection inform packets to ACS regularly.
Periodic Inform Interval (s)	Enter the time interval when AP sends connection Inform packets to ACS regularly
CPE Cert File	Enter the certificate that AP needs to use when connecting to ACS through SSL.
CPE Cert Key	Enter the certificate key that AP needs to use when connecting to ACS through SSL.

TR-069

Notes:

1. Restrictions:

Both Primary and Subordinate (regardless of whether it has been taken over by GDMS Networking/Local Primary) support the TR-069 function, and you can go to their respective local web terminal to open TR-069 and make related configurations.

If the Subordinate under the GDMS Networking it will be disconnected from the Cloud. The AP can still show on the Cloud, but it is not manageable (similar to the AP taken over by the Primary can be added to the Cloud); if the Subordinate is under the Local Primary, the connection with the Local Primary will be disconnected, and the Primary will no longer show this AP.

2. Failover does not support the TR-069 function. When multiple slaves are managed under a Local Primary, set a subordinate to failover mode. When the Primary fails, the subordinate acts as the Primary to manage other slaves. At this time, if you want to migrate to the TR-069 platform, you can only configure TR-069 for each of the other Slaves through their own local web pages. So, they need to be migrated one by one, and APs in Failover mode cannot be migrated. (After the failover primary gets transferred into the official primary, by the admin to log in and confirm, there will be no such restriction anymore).

3. Primary supports the migration of the whole setup, including its slaves, to TR-069, and the behavior is irreversible. If the Primary turns on TR-069, all online Subordinate APs it controls will be migrated to the TR-069 platform, and the Primary's identity will also be changed to Subordinate. In this process, you need to ensure the TR-069 configuration information, especially the ACS URL is configured correctly; otherwise, the migration will fail, and all AP roles remain unchanged, and the function does not affect the use.

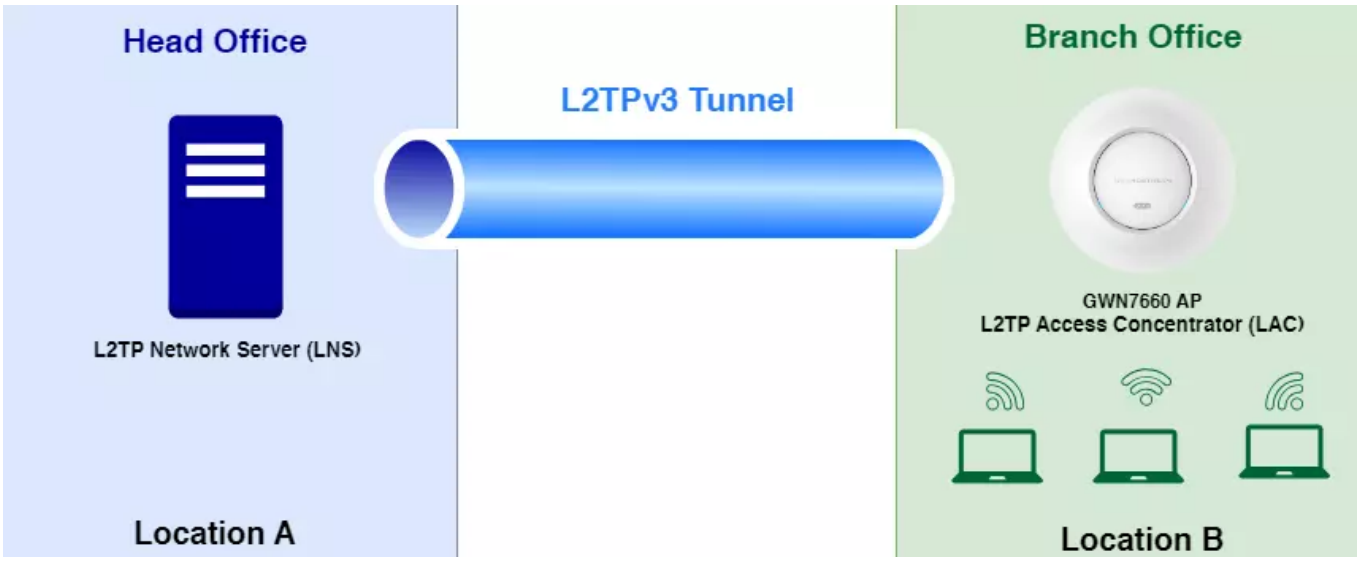
4. If a subordinate is offline, it will not be migrated to TR-069. After it goes online again, it will not be migrated to the TR-069 platform either. It is still in the state of being taken over by the original Primary, but is no longer managed by the Primary. It cannot be managed by Cloud, but can only be taken over by other Masters or factory reset.

5. APs managed by TR-069 can be "Take Over" by Local Primary. After Taken Over, TR-069 shuts down by itself, and the Local Primary issues the configuration to the AP to overwrite the original configuration from TR-069. This process will take a certain amount of time.

6. An AP under TR-069 will be disconnected from TR-069 by itself after the TR-069 function is turned off on the AP's local web UI, but it will not affect its function use and can continue to be taken over by Primary/GDMS Networking.

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

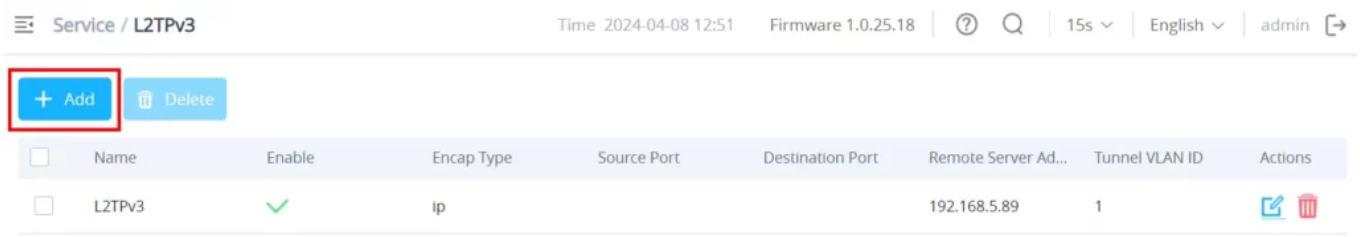
GWN Access Points, known for their reliability and performance, act as LACs and establish tunnels to the LNS, facilitating the encapsulation and transmission of all wireless clients' Layer 2 traffic. This architecture proves particularly beneficial in centralized network models where VLANs extend from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

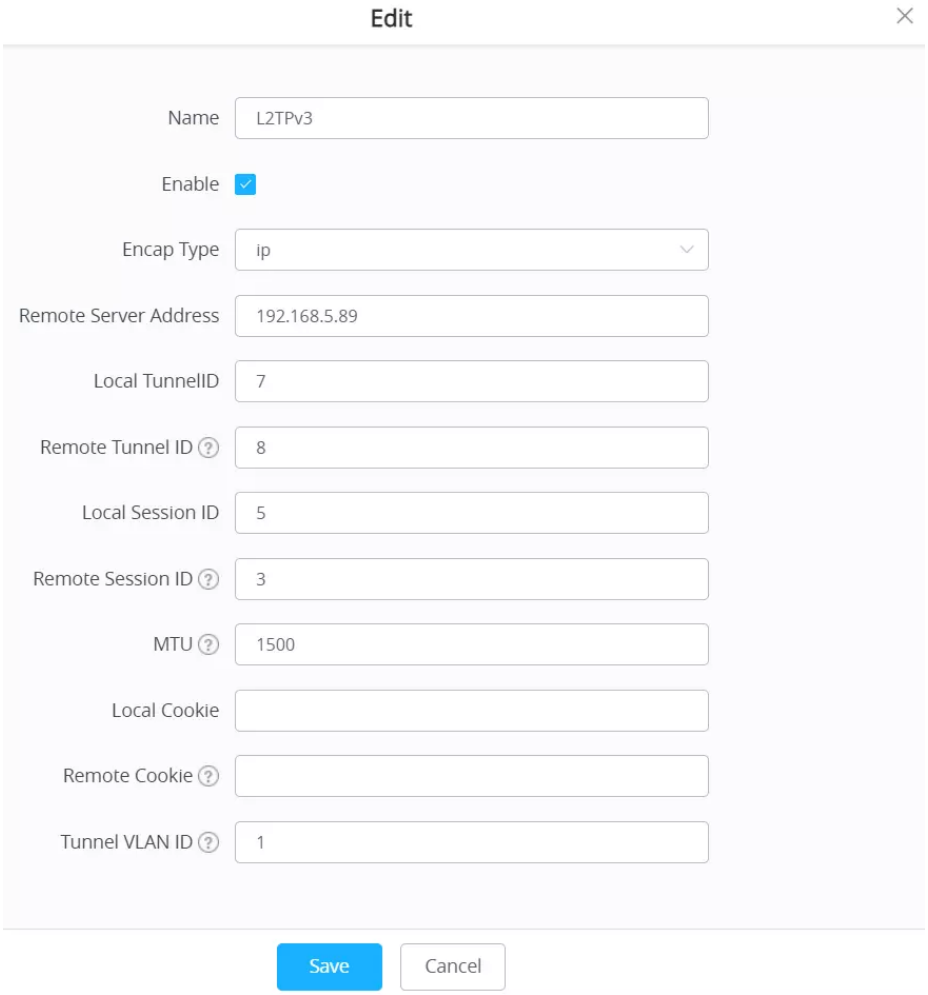
This feature is only supported on GWN7660(LR), GWN7664(LR), GWN7661 and GWN7662.

To add a L2TPv3 tunnel, navigate to **GWN76xx web UI -> Service -> L2TPv3**, then click on "**Add**" button as shown below:



L2TPv3

Please refer to the figure and table below:



Add L2TPv3

Name	Set the name of the tunnel.
Enable	Enable/Disable the tunnel.
Encap Type	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.
MTU	Set the MTU.Notes: * The MTU value is set to 1446 bytes by default and this value should only be changed for troubleshooting purposes.* Ensure both the L2TPv3 client and server have the same MTU value configured.
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.
Tunnel VLAN ID	Specify the VLAN IDNote: The tunnel ID must be set in SSID, and make sure that SSID only has the AP(s) who enabled L2TPv3.

Add L2TPv3

SYSTEM

The **System** section of the GWN76xx Access Point management interface is designed to provide administrators with comprehensive tools to manage and maintain the access point's core system settings. It includes the following subsections:

1. **Settings**: Configure general system options such as VLAN settings, time synchronization, and account management.
2. **Mesh**: Manage and optimize the device's mesh network configurations for seamless connectivity.
3. **Schedule**: Create and manage schedules for tasks like SSID broadcasting, device rebooting, etc.
4. **Maintenance**: Perform firmware upgrades, backup and restore configurations, and monitor system logs for troubleshooting.
5. **Alert**: Configure alerts and notifications for important events or system status changes.

This section is crucial for tailoring the behavior of the device to meet your network's operational requirements and maintaining optimal performance.

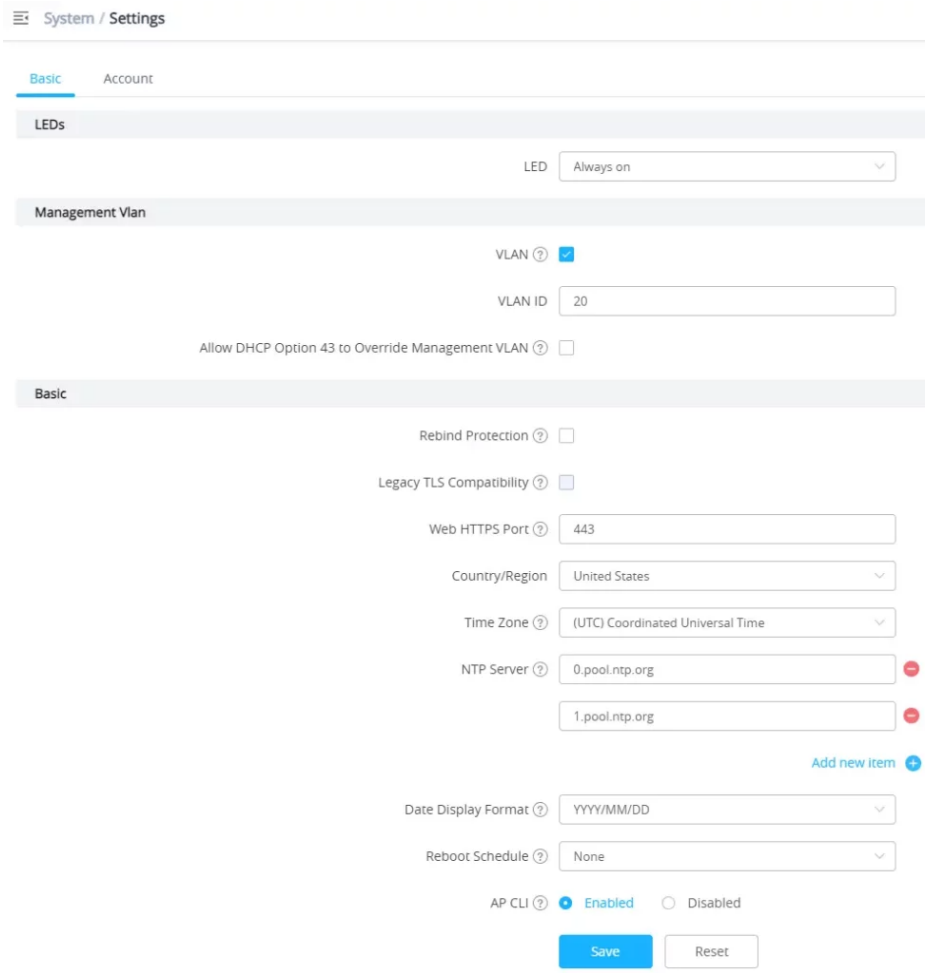
Settings

The **System -> Settings** page in the GWN76xx Access Point management interface allows administrators to configure fundamental system behaviors and account settings. This section is divided into two tabs:

1. **Basic**: For configuring general system settings, including VLANs, time settings, and network protocols.
2. **Account**: For managing the administrator account, updating passwords, and enabling web access for other users.

Basic

The **Basic** tab provides options to configure key system parameters like VLAN settings, NTP server details, and the system's timezone. Use this tab to tailor system behavior according to your network requirements.



settings page

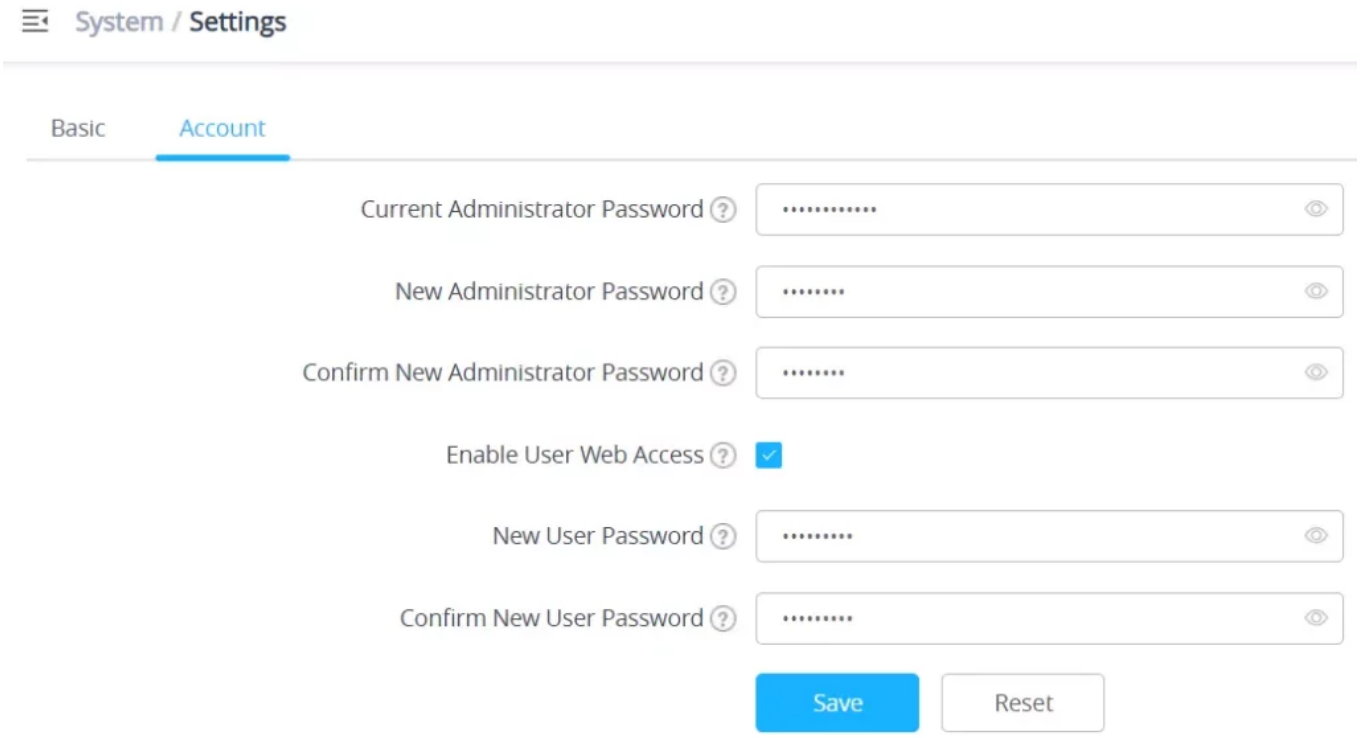
Field	Description
LEDS	
LED	Configures the status of the device's LED indicator. Always On: the LEDs always on. Always Off: the LEDs always off. Schedule: if schedule is selected, the user can specify the schedule under the schedule field.
Management Vlan	
VLAN	Enables or disables VLAN tagging for management traffic. If enable, AP will get ip from this vlan.
VLAN ID	Specifies the VLAN ID for management traffic.
Allow DHCP Option 43 to Override Management VLAN	Lets DHCP Option 43 override the configured Management VLAN ID. After enabled, AP will get provisioned for management VLAN via DHCP Option 43 from local DHCP server, and the default management VLAN will be overridden. Note: Once enabled, users cannot manually change the management VLAN.
Basic	
Rebind Protection	Enables protection against DNS rebind attacks. Anti domain name hijacking protection. If enabled, when the address returned by the superior DNS is a private LAN address, it will be regarded as a domain name hijacking, thus discarding the analytical result.If disabled, the analytical results will not be discarded.
Legacy TLS Compatibility	Allows compatibility with older TLS versions for secure communication. Once disabled, the primary AP can only manage subordinate APs with firmware version 1.0.15.x or higher. For security purpose, this function will no longer take effect for APs with firmware 1.0.22.x or higher.

Web HTTPS Port	Defines the HTTPS port for accessing the web management interface (default: 443).Note: Do not use some special ports,such as ports 1,21 and other special ports.
Country/Region	Sets the geographical region.
Time Zone	Configures the time zone for the system.
NTP Server	Specifies one or more Network Time Protocol (NTP) servers for time synchronization. the device will obtain the date and time from the server. The default settings is "129.6.15.28".
Date Display Format	Sets the format for displaying dates.
Reboot Schedule	Allows scheduling of automatic reboots. Once scheduled,the current network will not work for a while during the scheduled period.
AP CLI	Enable or disable admin access to the GWN Menu CLI via SSH.

Settings page

Account

The Account tab allows administrators to manage credentials for both the admin and user accounts, as well as enable web access for non-administrator users. This tab is crucial for maintaining security and granting access to additional users when necessary.



Account

Field	Description
Current Administrator Password	Enter administrator password.This field is case sensitive. The maximum length is 32 alphabet characters.
New Administrator Password	Allows the user to change the admin password. The password field is purposely blank after clicking the "Save" button for security purpose. This field is case sensitive with a maximum length of 32 characters.
Confirm New Administrator Password	Re-enter the new admin password to confirm.
Enable User Web Access	Allows enabling of web-based access for non-administrator user accounts.If selected, the user role is allowed to log in with a password, and the username will be in this case (user).Note: The password is reset each time it is disabled

New User Password	Configures the password for user-level web GUI access. This field is case sensitive with a maximum length of 32 characters.
Confirm New User Password	Re-enter the new user password to confirm.

Account

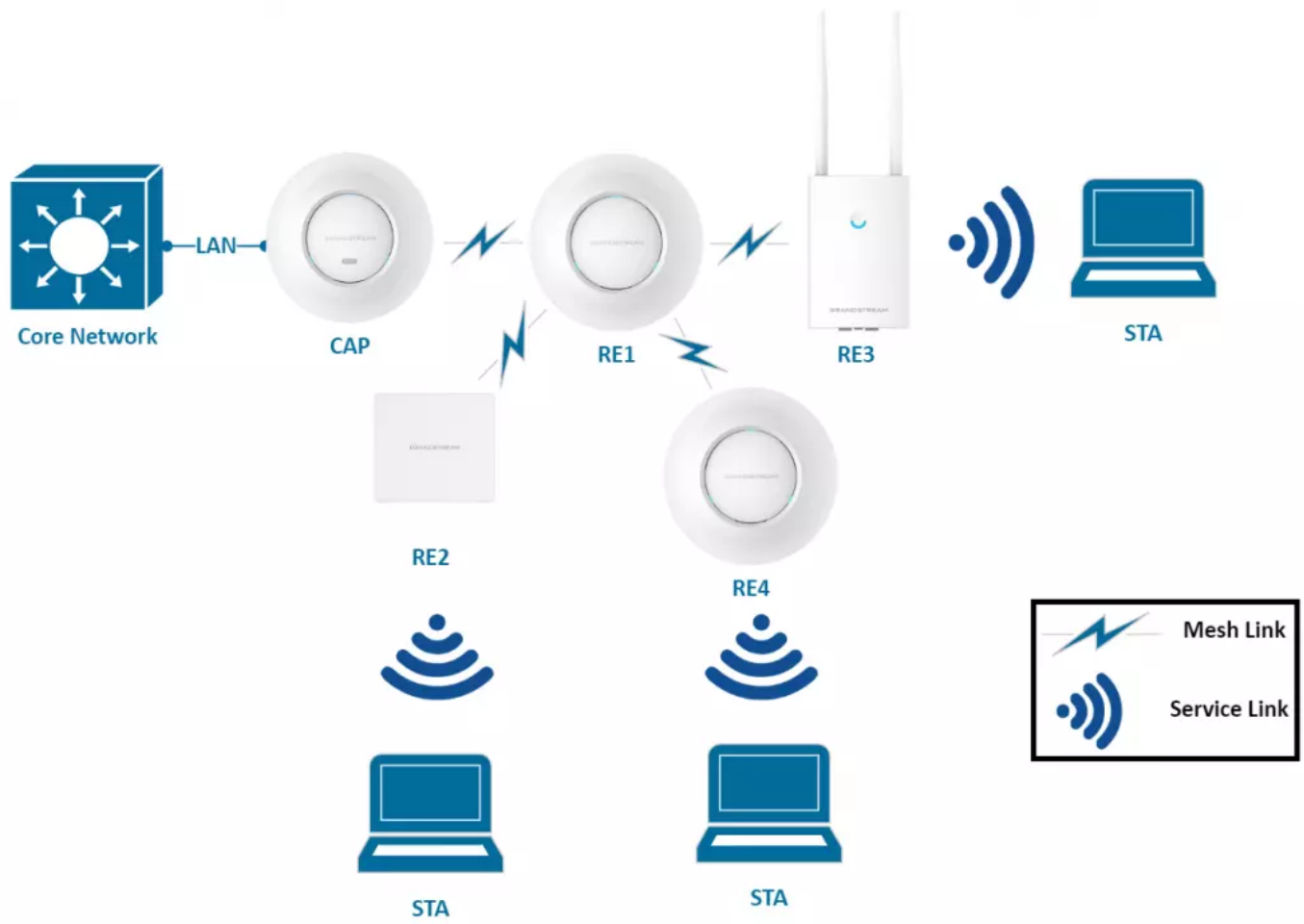
Passwords created for authentication via the web portal are securely stored in encrypted form.

Mesh

A Mesh Network creates a seamless wireless connection between multiple APs (Access Points), enabling efficient data traffic routing across the network. Instead of focusing on direct client association, the network leverages the capabilities of each AP to dynamically optimize connectivity. By continuously evaluating wireless channel performance, each AP intelligently selects optimal connections to maintain robust and efficient communication.

Types of Access Points in a Mesh Network

1. **CAP (Central Access Point):** An access point with an uplink connection to the wired network.
2. **RE (Range Extender):** An access point participating in the mesh network topology with a wireless uplink connection to the central network.



Mesh overview

Deploying Mesh Access Points (REs)

1. **Prepare the CAP Access Point:**

- Ensure the **CAP access point** are deployed and operational. The **CAP** can also act as the primary controller of the network.

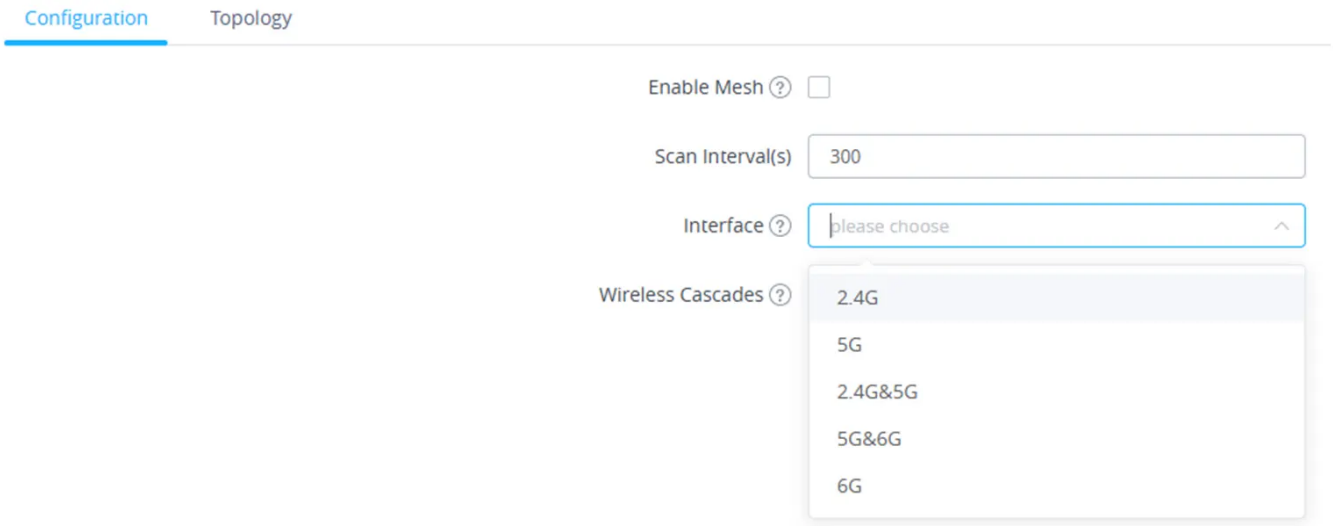
2. **Pair RE Access Points with the CAP:**

- Connect all **REs** to the same wired LAN **(same VLAN)** as the primary.
- Perform the discovery and pairing process through the **CAP's interface**.
- After pairing, deploy the REs in their respective locations to complete the setup.

3. **Configure Global Mesh Settings:**

- On GWN76XX, navigate to **System -> Settings -> Mesh** and configure the following parameters:

On models that display the **Wi-Fi** menu, open **Wi-Fi > Mesh**. The Mesh configuration options are the same; only the menu location differs.



Mesh Configuration

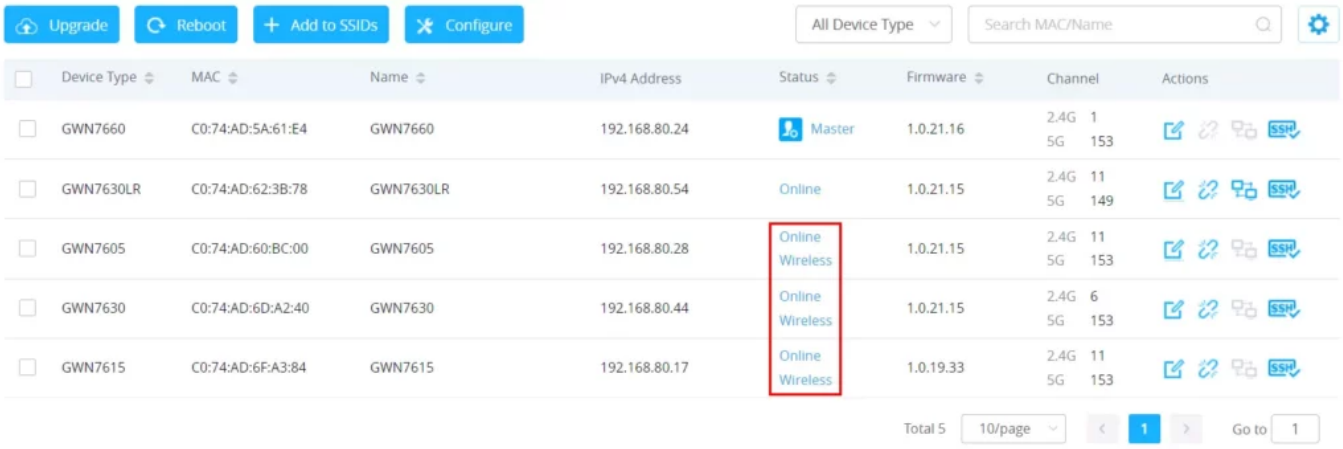
Field	Description
Enable Mesh	Activates the Mesh feature.Default is disabled.
Scan Interval(s)	Set the interval, in seconds, for scanning available Mesh neighbors.
Interface	Configures the wireless band used for Mesh backhaul connections between access points. Depending on the device model and its hardware capabilities, one or more of the following options may be available:2.4 GHz5 GHz6 GHz2.4 GHz & 5 GHz5 GHz & 6 GHzNotes:The actual options displayed in the Web UI depend on the specific model and its supported radios.6 GHz options are available only on models that support 6 GHz (for example Wi-Fi 7 models such as GWN7674). These models can use 6 GHz as a standalone Mesh band or in combination with 5 GHz.For best Mesh performance, it is recommended to use access points with similar radio capabilities and to configure the same Mesh band on all Mesh members.Higher-frequency bands (such as 5 GHz and 6 GHz) generally provide higher throughput but shorter range, while 2.4 GHz is primarily useful for compatibility and extended coverage and may limit overall Mesh throughput if used in the backhaul path.When different bands or band combinations are used in the same Mesh topology, the overall performance is typically constrained by the slowest link in the Mesh path.
Wireless Cascades	Defines the number of APs that can be cascaded wirelessly.Must be an integer between 1 and 3.

Mesh configuration on GWN76XX

Open the **Mesh Topology** tab to review the mesh links. Use **Search MAC/Name** to filter the topology by access-point MAC address or name.

4. **Manage the Mesh Network:**
   Once deployed and paired, manage all subordinate access points (**REs**) through the primary (**CAP**). Access the "**Access Points**" page on the **CAPs's interface**:

- APs in the "**Online Wireless**" state are REs with a **wireless uplink** to a CAP.
- APs in the "**Online**" state are connected via a **wired link**.



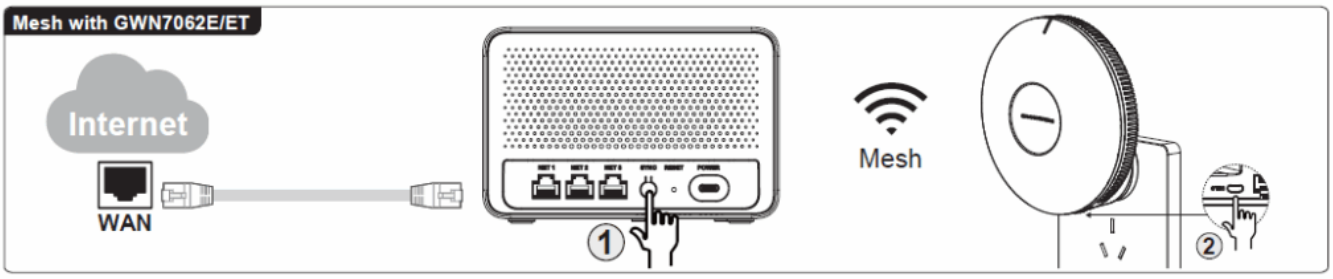
Mesh - Online Wireless

- When Mesh is enabled, the number of SSIDs in the same VLAN cannot exceed 5.
- Verify that no DHCP server is active or connected to the AP to prevent potential conflicts.

For more detailed information about the GWN Mesh network feature, refer to the "Mesh Network Guide."

Mesh Configuration with GWN7660EM

The GWN7660EM supports mesh networking with GWN routers (GWN7062E(T)) and wireless access points (GWN76XX series).
Follow the corresponding procedure below depending on the device used for mesh connection.



Mesh with Router GWN7062E(T)

Step 1: Factory Reset State

Ensure that the GWN7660EM is in a factory reset state. The **SYS LED** should display **solid pink**.

Step 2: Device Placement

Connect the GWN7660EM to the router using an **Ethernet cable**, or place it **close to the router** without connecting via cable.

Step 3: Trigger Mesh Scanning
On the router, either **press and hold the SYNC button for 3 seconds** or **log in to the router's Web GUI** to start scanning for mesh sub-nodes.
If the GWN7660EM is detected, its **SYS LED will begin blinking pink**.

Step 4: Initiate Mesh Pairing
When the GWN7660EM is used **wirelessly as a mesh access point** (no Ethernet cable connected to the router), press and hold the **SYNC button for 3 seconds** to start mesh pairing. Once initiated, the **SYS LED will blink pink, then turn solid pink** while the mesh link is being established.

However, when the GWN7660EM is **connected to the router using an Ethernet cable**, it will operate as a wired access point and **manual mesh setup is not required**. In this case, **do not press the SYNC button**, as the device will connect through the wired uplink automatically.

Step 5: Confirm Mesh Status

- **Solid Blue:** Mesh pairing completed successfully. During the pairing process, it is normal for the LED to temporarily display **pink**, **yellow**, or **blue**. After approximately **2 minutes**, the LED will stabilize to **solid blue**, indicating a successful mesh connection.
- **Solid Red:** Mesh pairing failed. After approximately **30 seconds**, the router LED will revert to **solid blue**, and the **GWN7660EM** LED will revert to **solid pink**, indicating that the device has stopped the pairing attempt.

For more detailed instructions on mesh configuration with routers, please refer to the GWN7062E/ET User Manual.

Mesh with Access Point (GWN76XX Series)

Step 1: Factory Reset State
Ensure that the GWN7660EM is in a factory reset state. The **SYS LED** should display **solid pink**.

Step 2: Start Scanning for APs
Press the SYNC button once. The SYS LED will begin blinking cyan, indicating that the device is scanning for nearby APs with mesh functionality enabled.
If the user has a specific target AP, place the GWN7660EM close to the target AP that has mesh option enabled before initiating the mesh operation. The GWN7660EM will automatically select the AP with the strongest signal for pairing. When both 2.4GHz and 5GHz devices are available, the 5GHz connection will be prioritized. Once the connection is successfully established, the SYS LED turns solid cyan, and the GWN7660EM will be connected in the mesh network.

Step 3: Take Over via Primary AP
Log in to the Primary AP within the same local network, and use the "Search AP" function to discover and take over or link the GWN7660EM.
The Primary AP will synchronize its configuration to the GWN7660EM. During this process, the SYS LED will blink blue.

Step 4: Confirm Mesh Status
When the mesh setup is successful, the SYS LED will turn solid blue. It is normal to see LED truns yellow before the mesh is completed.

If you want to mesh the GWN7660EM with a specific AP, place it close to the target AP before starting the mesh operation.

LED indication (GWN7660EM)

The table below indicates all the possible SYS LED behaviors and their signification.

Set up	SYS LED	Description
Mesh with router GWN7062E(T)	Solid pink (after factory rest)	Stand by
	Blinking pink	Scanned by other device(e.g. GWN7062E)
	Blinking pink speeds up	Device is waiting for user action. Press and hold the SYNC button for 3 seconds to begin pairing.
	Solid pink	Mesh in progress
	Solid blue	Mesh successful
	Solid red	Mesh failed
	Blink blue	Configuration in progress
	Solid yellow	Disconnected after mesh
Mesh with AP GWN76XX series	Solid pink (After factory rest)	Stand by
	blinking cyan	Press SYNC button on GWN7660EM once Scanning for nearby APs with mesh functionality enabled.
	solid cyan	GWN7660EM discovered by Primary AP .
	Blink blue	Configuration in progress
	Solid blue	Mesh connected
	Solid yellow	Disconnected after mesh

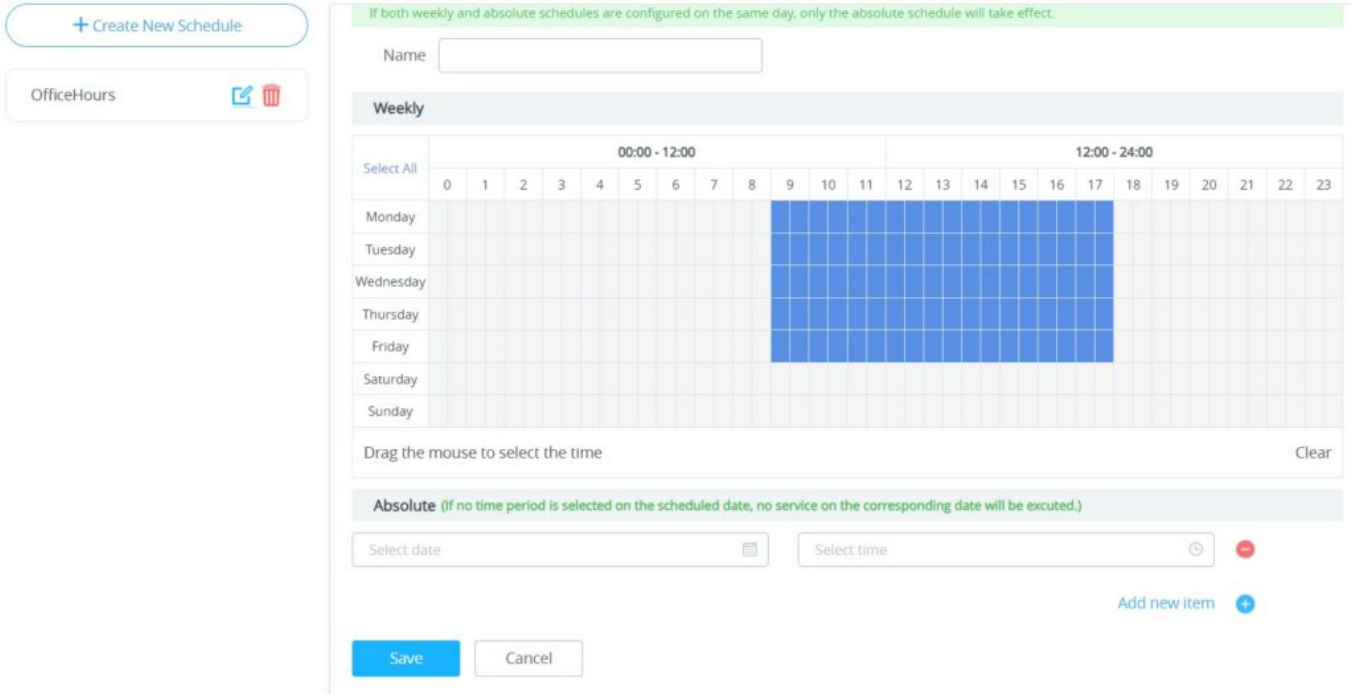
Schedule

Users can use the schedule configuration menu to set a specific schedule for GWN features while giving the flexibility to specify the date and time to turn ON/OFF the selected feature.

The Schedule can be used for setting up a specific time for Wi-Fi where the service will be active, or for an LED schedule, or bandwidth rules, etc.

To configure a new schedule, follow steps below:

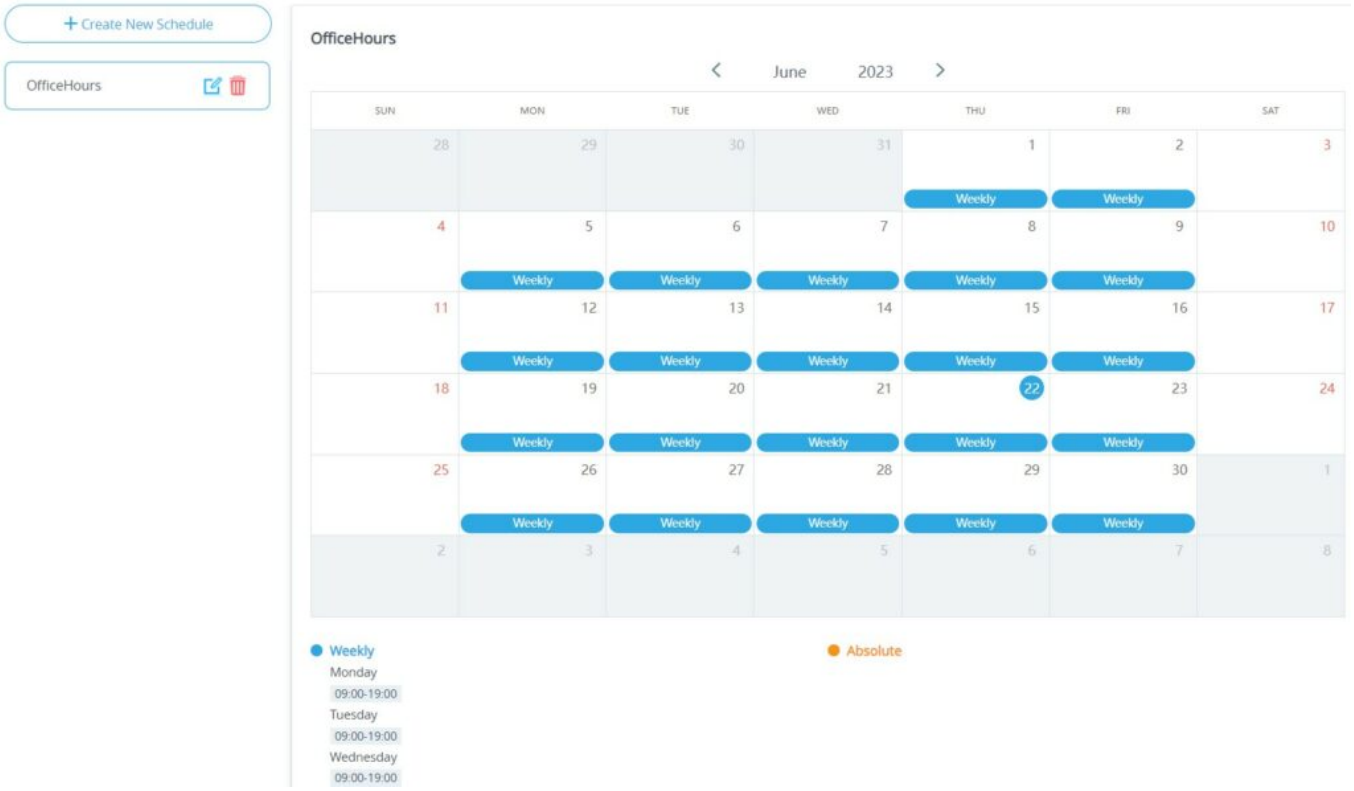
1. Go to **System -> Schedule** and click on **Create New Schedule**.



Create New Schedule

2. Select the periods on each day that will be included on the schedule and enter a name for the schedule (ex, office hours).
3. Users can choose to set a weekly schedule or an absolute schedule (for specific days, for example), and if both weekly schedule and absolute schedules are configured on the same day, then the absolute schedule will take effect and the weekly program will be cancelled for that specific date.
4. Once the schedule periods are selected, click on **Save** to save the schedule.

The list of created schedules will be displayed as shown in the figure below. With the possibility to edit or delete each schedule:



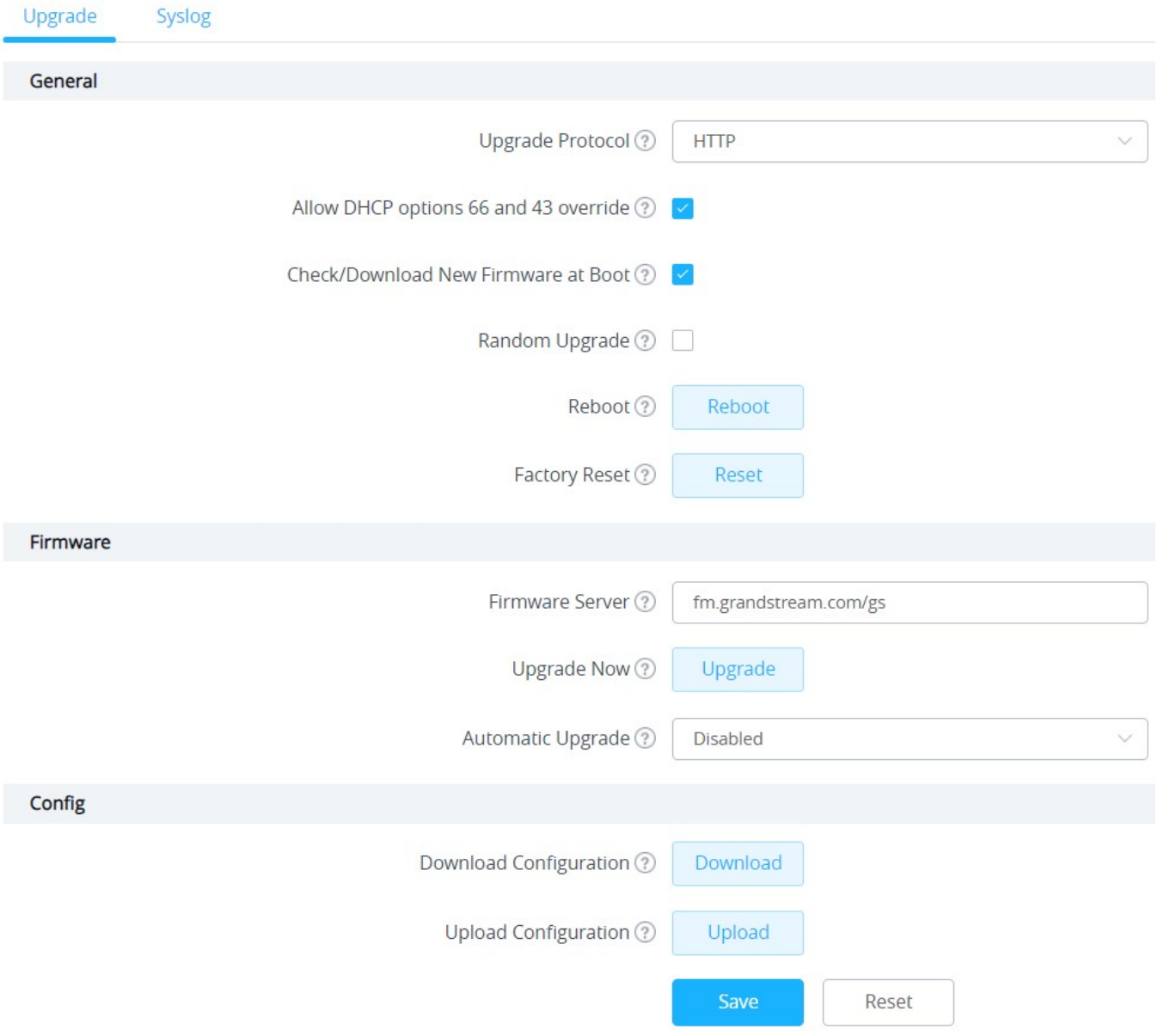
Schedules List

Maintenance

Upgrade

The Upgrade Web page allows upgrade-related configuration.

Random Upgrade: Enable this option to schedule the firmware upgrade at a random time within 30 minutes after the access point boots.



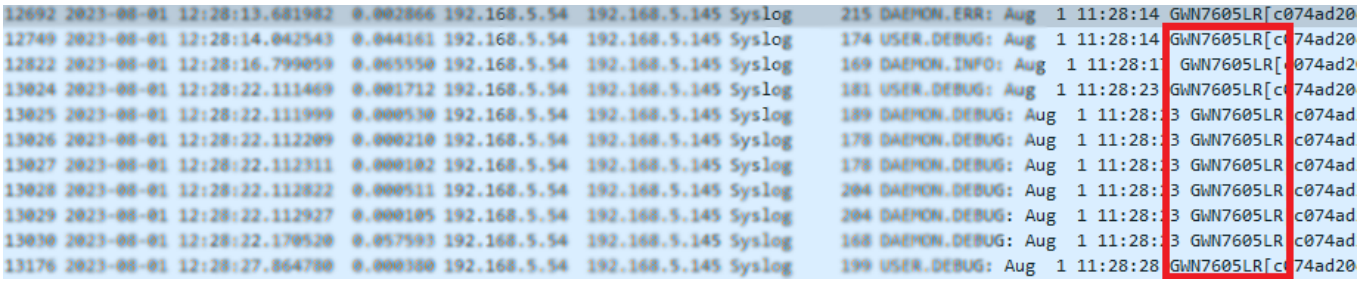
Upgrade

Syslog

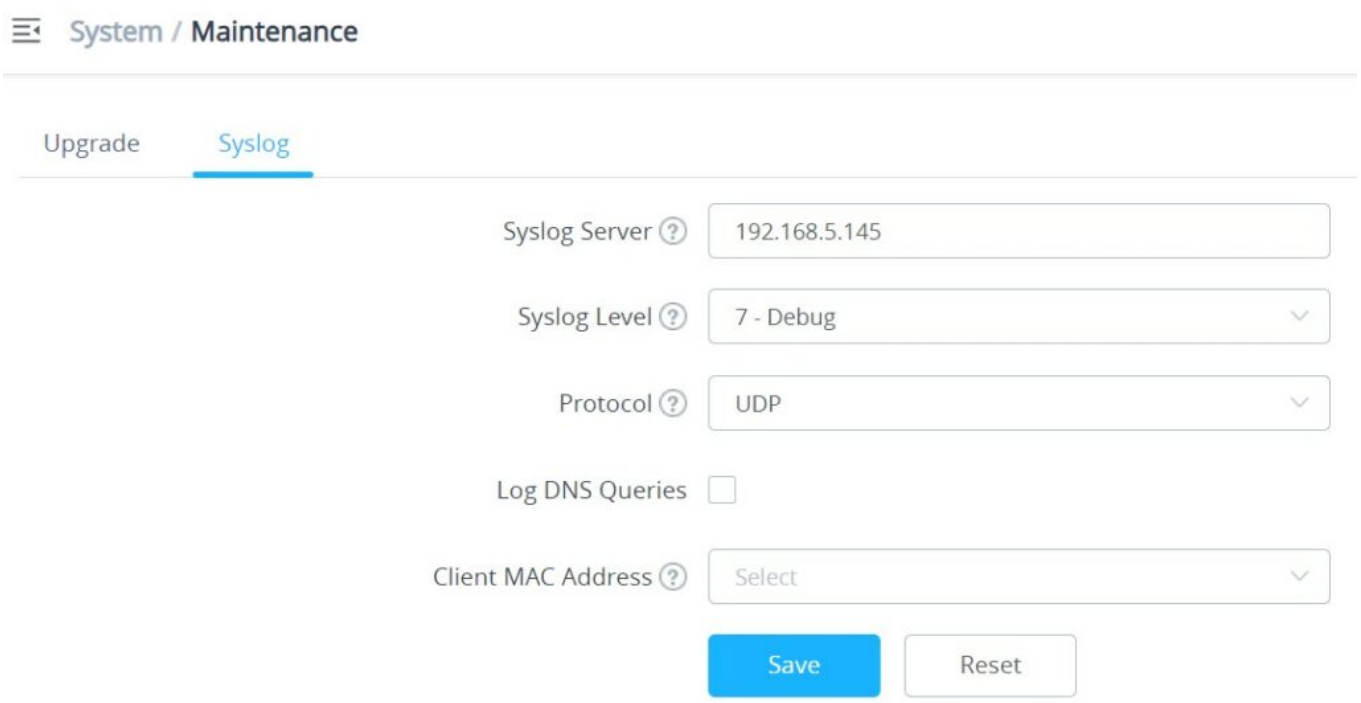
On the GWN76XX, users could dump the syslog information to a remote server under **Web GUI** -> **System** -> **Maintenance** -> **Syslog Tab**. Enter the syslog server hostname or IP address and select the level for the syslog information. Eight levels of syslog are available: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

The device name is added to syslog messages. To configure the device name please navigate to **Web UI -> Access Points -> Configuration** select the device, and click on the "**Configure**" button.

Here is an example of the device name shown in Wireshark capture, please refer to the figure below:



Wireshark - GWN76xx AP



Syslog

Field	Description
Syslog Server	Enter the IP address or URL of Syslog server.
Syslog Level	Select the level of Syslog, 8 levels are available: Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug.
Protocol	The protocol type sent to Syslog Server.
Log DNS Queries	Check to log DNS Queries.
Client MAC Address	Please configure the client MAC address for the log query.

Syslog Parameters

Alert

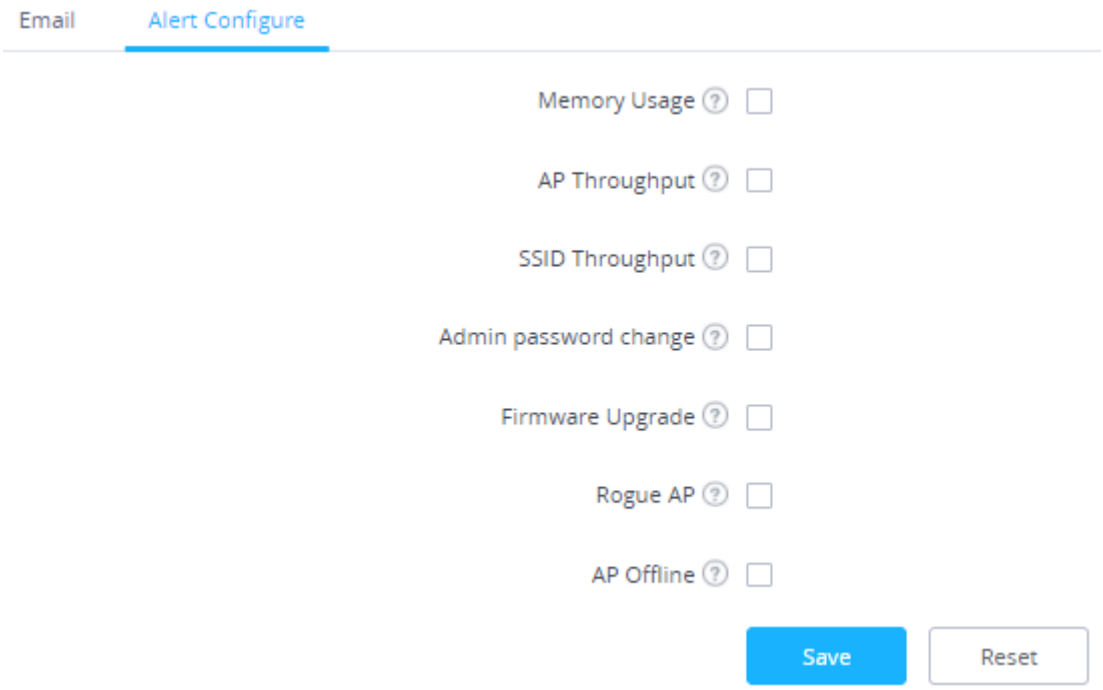
The Alert page allows the administrator to select a predefined set of system events and to send notifications upon the change of the set of events via email.

Email

Field	Description
Enable Email Notification	Set whether to enable Email notification.

Email configuration

Alert Configure



Alert Configure

The following table describes the notification configuration settings:

Filed	Description
Memory Usage	Configure whether to send a notification if memory usage is greater than the configured threshold.
AP Throughput	Once enabled, the primary will generate an Alert when AP throughput reaches the configured threshold.
SSID Throughput	Once enabled, the primary will generate an Alert when SSID throughput reaches the configured threshold.
Admin Password Change	Configure whether to send a notification on admin password change.
Firmware upgrade	Configure whether to send a notification on firmware upgrade.
Rogue AP	Once enabled, the system will generate an Alert when there is a Rogue AP detected.
AP Offline	Configure whether to send a notification when an AP goes offline.

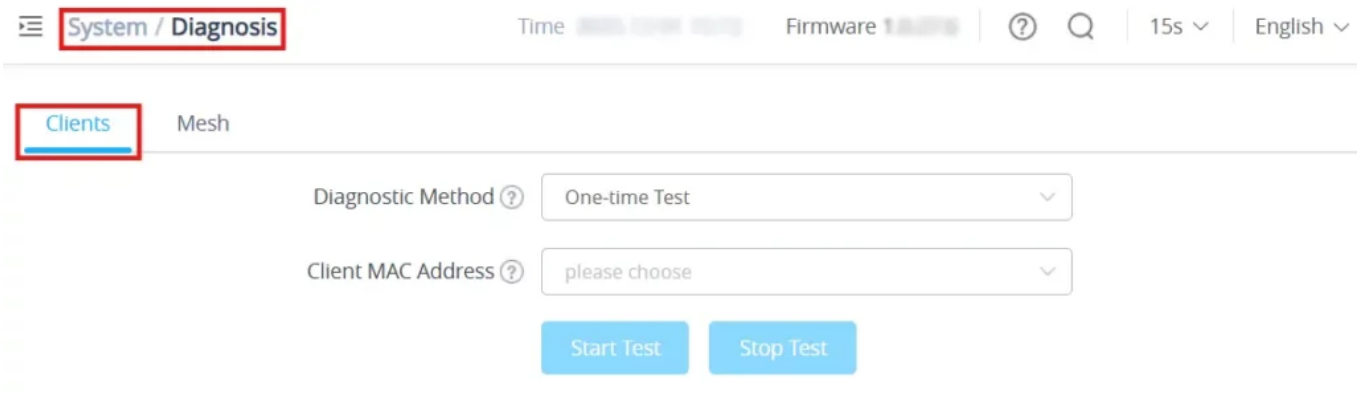
Email Events

Diagnosis

The Diagnosis page provides tools to monitor and troubleshoot wireless clients and Mesh devices on the access point.

Clients tab

Use this tab to run diagnostic tests for specific wireless clients.



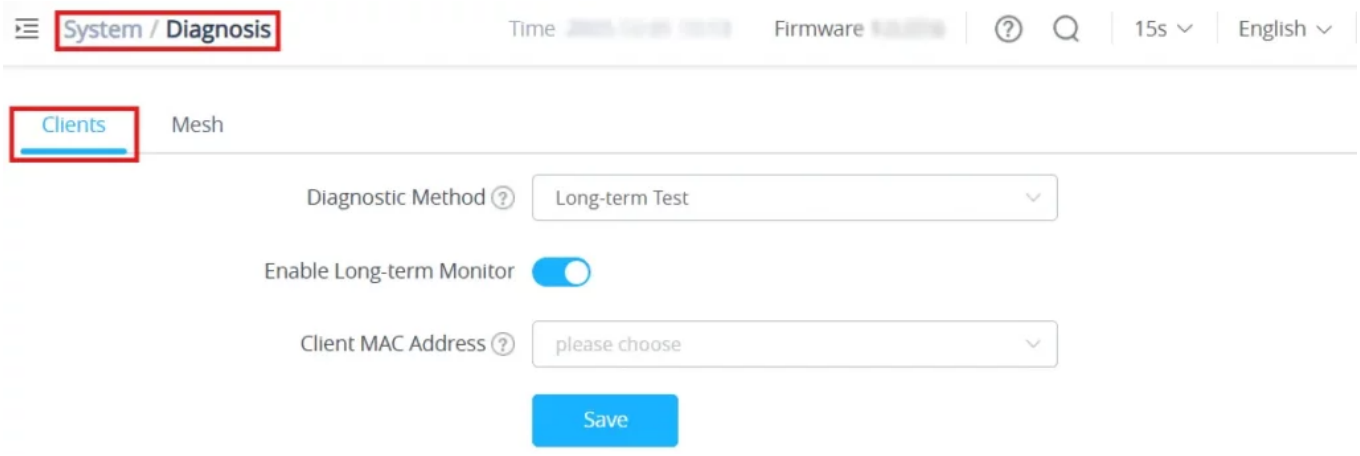
Diagnosis -> Clients -> Diagnostic Method set to Diagnostic Method

- **Diagnostic Method**: Select the type of diagnostic test for the selected clients:

  - **One-time Test**: runs an on-demand test for the selected client(s). Use this to quickly check the current connection status or behavior.
  - **Long-term Test**: enables continuous monitoring for the selected client(s). Long-term monitoring logs are written to the configured Syslog server. When using this option, make sure that the Syslog service is enabled on the device and that the log level is set to **Notice** or higher so that diagnosis logs are recorded.
- **Client MAC Address**: Select the wireless client MAC address to be monitored. Up to **8** client MAC addresses can be configured for diagnosis at the same time.
- **Start Test / Stop Test** (One-time Test): When **Diagnostic Method** is set to One-time Test, click **Start Test** to begin collecting diagnostic information for the selected client(s). Click **Stop Test** to end the test.

When **Diagnostic Method** is set to Long-term Test, the page displays an additional control:

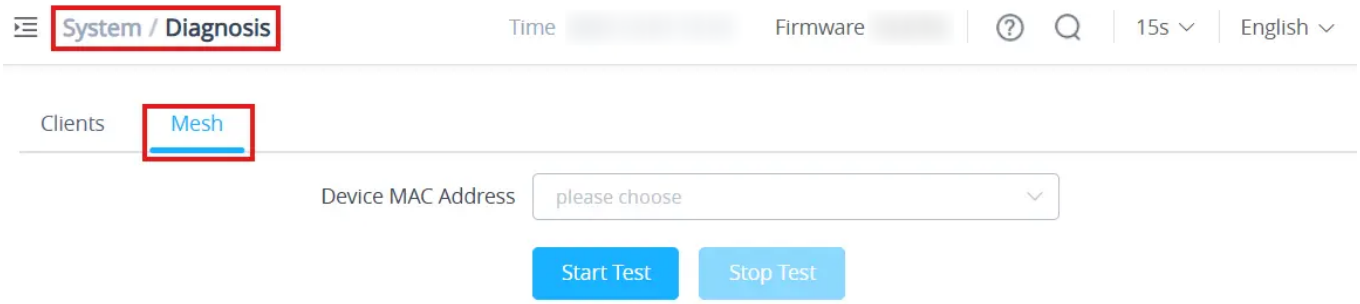
- **Enable Long-term Monitor**
  Enable this option to start long-term monitoring for the selected client MAC address(es). Click **Save** to apply the setting. Monitoring continues until this option is disabled. Long-term results are stored in the Syslog server rather than shown only on the web interface.



Diagnosis -> Clients -> Diagnostic Method set to Long-term Test

Mesh tab

Use this tab to run diagnostics for Mesh devices that are connected in a Mesh topology.



Diagnosis Mesh

- **Device MAC Address**: Select the Mesh access point (by MAC address) to be diagnosed.
- **Start Test / Stop Test**: Click **Start Test** to begin the diagnostic test for the selected Mesh device. Click **Stop Test** to end the test.

Note: Diagnosis functions are intended for monitoring and troubleshooting only. They do not change the wireless configuration, but long-term tests can generate additional log traffic on the Syslog server, especially when multiple clients are monitored.

UPGRADING AND BACKUP/RESTORE

Upgrading Firmware

The GWN76XX can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN76XX.

Upgrading via Web GUI

The GWN76XX can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP, or HTTPS; the server name can be a FQDN or an IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

192.168.5.87

Go to **Web GUI -> System Settings -> Maintenance -> Upgrade**. Configure the firmware server and download method, then select **Upgrade**.

Upgrading Subordinate Access Points

When the GWN76XX is being paired as a subordinate using another GWN76XX Access Point acting as a Controller, users can upgrade their paired access points from the GWN76XX Primary Controller.

To upgrade a subordinate access point, log in to the GWN76XX acting as Primary Controller and go to **Access Points.**



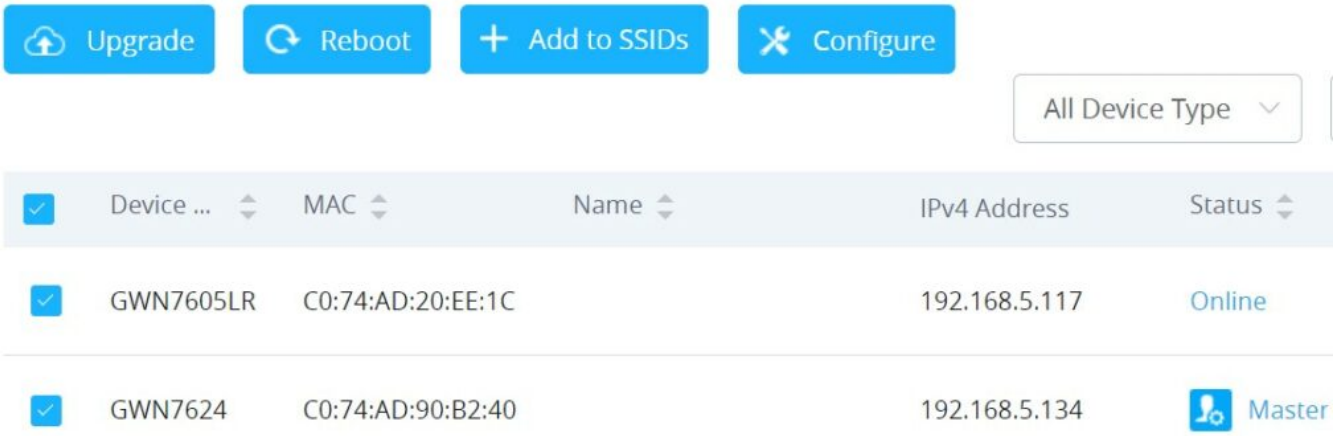
Access Points

Confirm that the firmware server path is correct under Maintenance, select the access points, then select **Upgrade**.

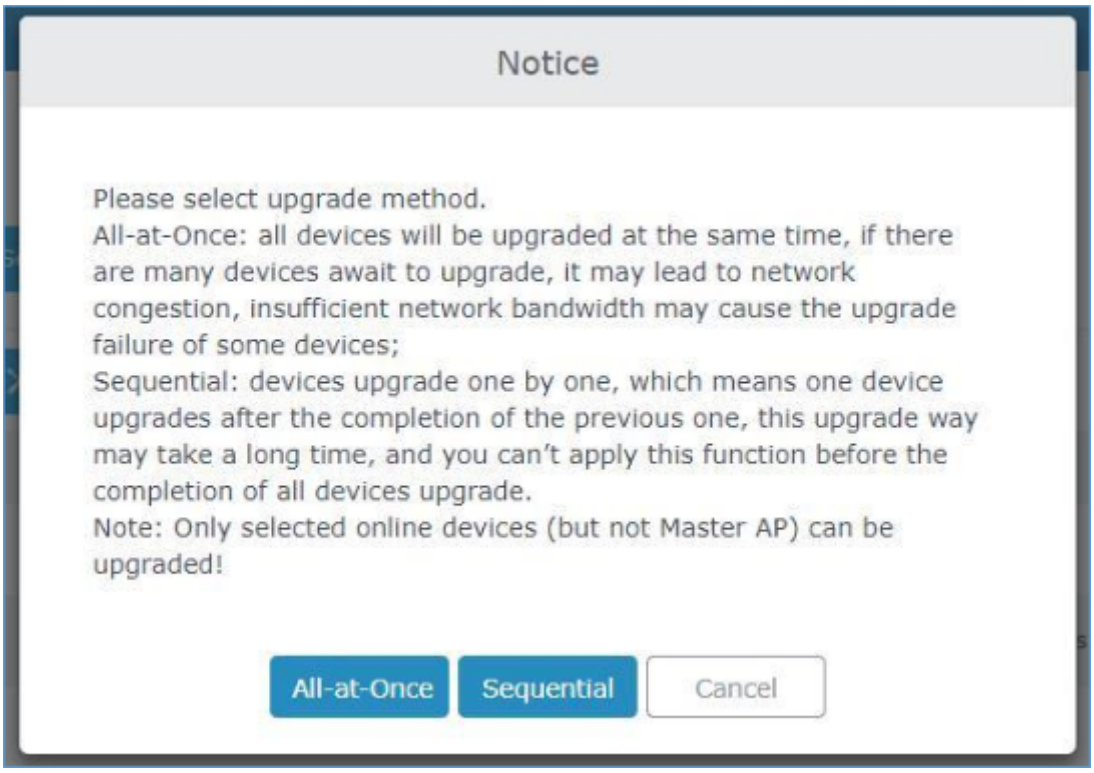
Sequential Upgrade

If you choose multiple subordinate devices to upgrade their firmware, two options are available: "All-at-Once" and "Sequential". "All-at-Once" will use the default method, all checked slaves will upgrade their firmware at the same time, while using the "Sequential" upgrade method, the slaves will upgrade their firmware one by one.

- Avoid an entire Wi-Fi service interruption by a full system firmware upgrade.
- Reduce network bandwidth consumption caused by firmware downloading.



Choosing multiple devices



All-at-Once and Sequential Upgrade

During a sequential upgrade, the **upgrade progress indicator** shows how many selected subordinate access points have been upgraded.

Configuration Backup and Restore

The GWN76XX configuration can be backed up locally. The backup file will be used to restore the configuration on GWN76XX when necessary.

Download Configuration

Users can download the GWN76XX configuration for restore purposes under **Web GUI**->**System Settings**-> **Maintenance->Upgrade**.

Select **Download** to save the configuration file locally.

Upload Configuration

Users can upload a configuration file to the GWN76XX under **Web GUI->System Settings->Maintenance->Upgrade**.

Select **Browse**, then choose the configuration file to upload.

Please note that the GWN76XX will reboot after the configuration file is restored successfully.

Reset and reboot

- To reboot the device, open **Web GUI -> System Settings -> Maintenance -> Upgrade**, then select **Reboot** .
- Select **Factory Reset** to restore all GWN76XX options to their factory defaults.

EXPERIENCING THE GWN76xx Wi-Fi ACCESS POINTS

Please visit our website: https://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 purchasing the Grandstream GWN76XX Wi-Fi Access Point, it will be sure to bring convenience and color to both your business and personal life

Thank you again for purchasing the Grandstream GWN76XX Wi-Fi Access Point, it will be sure to bring convenience and color to both your business and personal life

CHANGE LOG

This section documents significant changes from previous versions of the GWN76xx user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.27.21

Product Name: GWN7604

- No major changes.

Firmware Version 1.0.27.20

Product Name: GWN7660E / GWN7661E / GWN7664E / GWN7664ELR

- No major changes.

Product Name: GWN7604 / GWN7660 / GWN7660LR / GWN7661 / GWN7664 / GWN7664LR

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]
- Optimized One-Key Debug with encryption support and renamed it to System Debug. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz Mesh support. [Mesh]
- Optimized RRM scanning. [Radio]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]
- Added IP Source Guard (IPSG). [SSIDs]
- Added Network Health monitoring for Cloud management. [GDMS Networking]

Product Name: GWN7662 / GWN7665

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]
- Optimized One-Key Debug with encryption support and renamed it to System Debug. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz Mesh support. [Mesh]
- Optimized RRM scanning. [Radio]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]
- Added IP Source Guard (IPSG). [SSIDs]
- Added Network Health monitoring for Cloud management. [GDMS Networking]
- Expanded PPSK support to up to 1,000 keys. [PPSK]

Product Name: GWN7672

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]
- Optimized One-Key Debug with encryption support and renamed it to System Debug. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz Mesh support. [Mesh]
- Optimized RRM scanning. [Radio]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]

Product Name: GWN7672L / GWN7672WM / GWN7674

- No major changes.

Firmware Version 1.0.27.19

Product Name: GWN7660E / GWN7660ELR / GWN7661E / GWN7664E / GWN7664ELR

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]

- Optimized One-Key Debug with encryption support and renamed it to System Debug. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz Mesh support. [Mesh]
- Optimized RRM scanning. [Radio]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]
- Added IP Source Guard (IPSG). [SSIDs]
- Added Network Health monitoring for Cloud management. [GDMS Networking]
- Expanded PPSK support to up to 1,000 keys. [PPSK]

Firmware Version 1.0.27.18

Product Name: GWN7670 / GWN7670WM / GWN7670LR

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]
- Optimized One-Key Debug with encryption support and renamed it to System Debug. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz Mesh support. [Mesh]
- Optimized RRM scanning. [Radio]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]
- Added IP Source Guard (IPSG). [SSIDs]
- Added Network Health monitoring for Cloud management. [GDMS Networking]
- Expanded PPSK support to up to 1,000 keys. [PPSK]

Firmware Version 1.0.27.17

Product Name: GWN7670 / GWN7670WM / GWN7670LR / GWN7672 / GWN7672L / GWN7674

- Added Cloud Network Health support. [GDMS Networking]
- Added IP Source Guard (IPSG) for SSIDs. [SSIDs]

Product Name: GWN7672WM

- Initial release for GWN7672WM.

Firmware Version 1.0.27.9

Product Name: GWN7673

- Initial release for GWN7673.

Firmware Version 1.0.27.6

Product Name: GWN7660E / GWN7660ELR / GWN7661E / GWN7664E / GWN7664ELR / GWN7665

- Added MAC address format configuration for MAC authentication. [SSIDs]
- Added System Debug support for Cloud management. [Debug]
- Added Microsoft 365 authentication support for Captive Portal. [Captive Portal Policy List]
- Added Wi-Fi Extension support. [Relay WiFi]
- Added security version information. [Status]
- Added packet capture support through the slave AP web interface. [Debug]
- Added Bluetooth scan reporting for Cloud management. [GDMS Networking]
- Added diagnostic tools. [Diagnosis]
- Added a RADIUS NAS ID configuration option. [SSIDs]
- Added Fast SSID Creation. [Radio]
- Added 2.4 GHz and dual-band 2.4 GHz/5 GHz mesh support. [Mesh]
- Added OWE support. [SSIDs]
- Added Easy PSK support. [SSIDs]
- Added Power Input Mode for GWN7661E. [Configure Access Points]
- Expanded PPSK support to up to 1,000 keys. [PPSK]

Product Name: GWN7674

- Initial release for GWN7674.

Firmware Version 1.0.25.18

Product Name: GWN7672

- Added RRM scan support [Radio]

Firmware Version 1.0.25.17

Product Name: GWN7670 / GWN7670WM / GWN7670LR

- No major changes.

Firmware Version 1.0.25.45

Product Name: GWN7660E

- No major changes.

Firmware Version 1.0.25.12

Product Name: GWN7661E / GWN7604

- No major changes.

Firmware Version 1.0.25.43

Product Name: GWN7660ELR / GWN7665 / GWN7603

- No major changes.

Firmware Version 1.0.25.15

Product Name: GWN7672

- No major changes.

Firmware Version 1.0.25.42

Product Name: GWN7660(LR) / 7661 / 7662 / 7664(LR) / 7630(LR) / 7615 / 7624 / 7625

- No major changes.

Firmware Version 1.0.25.43

Product Name: GWN7605 / GWN7605LR

- No major changes.

Firmware Version 1.0.25.14

Product Name: GWN7670 / GWN7670WM / GWN7670LR

- No major changes.

Firmware Version 1.0.25.7

Product Name: GWN7660EM

- This is the initial version for GWN7660EM

Firmware Version 1.0.25.42

Product Name: GWN7660E / GWN7660ELR / GWN7664E / GWN7664ELR / GWN7665 / GWN7603 / GWN7605 / GWN7605LR

- No major changes

Firmware Version 1.0.25.41

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR / GWN7630 / GWN7630LR / GWN7615 / GWN7624 / GWN7625

- No major changes

Firmware Version 1.0.25.13

Product Name: GWN7672 / GWN7670WM / GWN7670

- No major changes

Firmware Version 1.0.25.10

Product Name: GWN7604 / GWN7661E

- Added DFS interface support for Thailand. [Basic]
- Added Network Security Certification for EU RED 3.3

Firmware Version 1.0.25.8

Product Name: GWN7604 / GWN7661E

- Allowed Norway channels. [Settings]

Firmware Version 1.0.25.39

Product Name: GWN7660E / GWN7660ELR / GWN7664E / GWN7664ELR

- No major changes

Firmware Version 1.0.25.38

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR / GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- No major changes

Firmware Version 1.0.25.34

Product Name: GWN7670

- This is the initial release of GWN7670.
- Added LLDP.
- Added MAC authentication support. [External Splash Page]
- Added MLO support. [SSID]
- Added WPA3 support for PPSK. [SSID]
- Added AP CLI feature. [Settings]

Firmware Version 1.0.25.34

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR / GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615 / GWN7624 / GWN7625 / GWN7660E / GWN7660ELR / GWN7664E / GWN7664ELR / GWN7665 / GWN7603

- No major changes

Firmware Version 1.0.25.33

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR / GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615 / GWN7624 / GWN7625

- Added new LED Pattern for uplink down/no network [LED Patterns]
- Added WP series device fast configuration support [WP device fast configuration]
- Added support for multi-VLAN Wi-Fi roaming [SSID]
- Added L2TPv3 tunnel support. (GWN7661/GWN7662/GWN7664) [L2TPv3]
- Added support for MAC-based RADIUS authentication [SSID]
- Added support of OS filtering [SSID]
- Increased the number of MAC addresses which can be added in the Client isolation [SSID]
- Increased Whitelist/Blacklist limit to 1024. [Access List]
- Added LLDP protocol support.

Firmware Version 1.0.25.7

Product Name: GWN7665

- No major changes

Firmware Version 1.0.25.19

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR / GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615 / GWN7624 / GWN7625

- No major changes

Firmware Version 1.0.25.18

Product Name: GWN7660 / GWN7660LR

- Added L2TPv3 tunnel support [L2TPv3]

Firmware Version 1.0.25.15

Product Name: GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.25.10

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7624 / GWN7625 / GWN7630 / GWN7630LR / GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR

- Added support for Speed Test [GWN AP as a slave]

Firmware Version 1.0.25.9

Product Name: GWN7662

- No major changes

Firmware Version 1.0.25.8

Product Name: GWN7661

- No major changes

Firmware Version 1.0.25.7

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Increased PPSK accounts. [PPSK]
- Increased the client expiration time to 30 days. [Captive Portal]
- Added device name in Syslog messages. [Syslog]
- Added support for custom Channel on 2.4G band. [Radio]

Firmware Version 1.0.25.3

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.25.1

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Added support of ARP defense [ARP Attack Defense]
- Added support of IPv6 ND defense [ND Attack Defense]
- Added support for disabling Ethernet port [configure access points]
- Added support of DHCP relay and option82 [DHCP Relay]
- Added support of trunk/access mode for NET/PoE port [configure access points]
- Added support of External syslog protocol selection [Syslog]
- Added support for collecting logs by MAC [Syslog]
- Added support of Captive Portal - Active Directory Auth (LDAP) [Captive Portal]
- Added support of Captive Portal - kick out timeout unauthenticated clients [Captive Portal]
- Added support of Captive Portal - Daily access limit by auth method [Internal Splash page]
- Added support for switching RF timer [Radio]

Firmware Version 1.0.23.27

Product Name: GWN7662

- This is the initial release of GWN7662

Firmware Version 1.0.23.24

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.23.22

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Added support for GWN Cloud v1.1.23.27 and GWN Manager v1.1.23.27

Firmware Version 1.0.23.15/1.0.23.7

Version 1.0.23.15

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7630 / GWN7630LR / GWN7624 / GWN7625

- No major changes

Version 1.0.23.7

Product Name: GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.23.14

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7625

- No major changes

Firmware Version 1.0.23.13/1.0.23.6

Version 1.0.23.13

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR

- No major changes

Version 1.0.23.6

Product Name: GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.23.9

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7625 / GWN7630 / GWN7630LR

- Added support of more DFS Channels. [Scene]

Firmware Version 1.0.23.7

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7625 / GWN7630 / GWN7630LR

- Added support of Import/Export the client access lists in CSV format [Access List]
- Added support of 802.11h
- Added support of PPSK [SSIDs]
- Added support of PassPoint R3 [Hotspot 2.0]
- Added support of 15 languages
- Added support of Management VLAN [Basic]
- Added support of Active Directory [Internal Splash Page]

Firmware Version 1.0.23.3

Product Name: GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Added support of Link aggregation for GWN7664/GWN7664LR

Firmware Version 1.0.21.16

Product Name: GWN7660 / GWN7664

- No major changes.

Firmware Version 1.0.21.15

Product Name: GWN7630 / GWN7630LR

- Added support of Hotspot 2.0 R3Beta for GWN7630/GWN7630LR. [Hotspot 2.0]

Firmware Version 1.0.21.14/15

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7630 / GWN7630LR / GWN7660 / GWN7664

- Added support of Hotspot 2.0 R3Beta for GWN7660. [Hotspot 2.0]
- Added support of Bonjour Gateway. [Enable Bonjour Gateway]

Firmware Version 1.0.21.7

Product Name: GWN7660

- Enable FCC DFS channels for GWN7660 [Table 39: DFS Channels supported by Model]

Firmware Version 1.0.21.6

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- Upgraded the max number of supported SSIDs [MAX SSID on each band]
- Added Option to turn off U-APSD function [Wi-Fi]
- Added IPv6 support for internal GWN services [Access Point Configuration Settings]
- Added feature to Transfer AP to GWN manager [Transfer AP]
- Added feature to allow Each AP to disable/Enable 2.4GHz or 5GHz independently [Table 20: Access Point Configuration Settings]
- Added feature of TR-069 [TR-069]
- Added feature of Google Authentication [Captive Portal - Policy List - Splash Page is "Internal"]
- Added feature to Delete inbound and outbound rules in batches [Firewall]
- Added feature to save network abnormal log to Flash [Debug]
- Added feature of Web lock for failed login [Access Web GUI]

Firmware Version 1.0.19.32

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- No major changes.

Firmware Version 1.0.19.14

Product Name: GWN7660

- This is the initial version for GWN7660

Firmware Version 1.0.19.29

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- No major changes

Firmware Version 1.0.19.25

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- No major changes

Firmware Version 1.0.19.22

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR

- Added support for WPA3. [Security Mode]
- Added support for Secondary RADIUS Server. [Secondary RADIUS Server]
- Added support for Rogue AP Alert. [Alert Configure]
- Added support of NET port VLAN settings. [Net Port Type]

Firmware Version 1.0.19.15

- No major changes

Firmware Version 1.0.19.9

- Added support of Rogue AP Detection. [Rogue AP]
- Added support of 802.11w. [802.11w]
- Added support of AutoTX Power. [RADIO]
- Added Captive Portal Enhancement. [CAPTIVE PORTAL]
- Added support of SNMP. [SNMP]
- Added support of more DFS Channels. [Scene]
- Added support of NAT. [NAT]
- Added support of Firewall. [Firewall]
- Added support of Hotspot 2.0 Beta. [Hotspot 2.0]
- Added support of Multicast/Broadcast Suppression. [Multicast/Broadcast Suppression]

- Extended support of RRM to GWN Cloud and remaining AP models. [Transmit Power Control][Coverage Hole Detection][Dynamic Channel Assignment]
- Added support of Active IGMP for the feature Convert IP multicast to unicast enhancement. [Convert IP multicast to unicast]
- Allow DHCP Option43 to override GWN Manager Address. [Allow DHCP Option 43 to override GWN Manager Address]

Firmware Version 1.0.15.20

Product Name: GWN7630 / GWN7630LR

- Added support for more DFS channels [Scene]

Firmware Version 1.0.15.18

Product Name: GWN7605

- Added support for CE/RCM DFS channels [Scene]

Firmware Version 1.0.15.15

Product Name: GWN7605

- Added yellow LED pattern to indicate Mesh disconnection [LED Status]

Firmware Version 1.0.15.5

Product Name: GWN7605

- This is the initial version for GWN7605

Firmware Version 1.0.15.4

Product Name: GWN7630 / GWN7630LR

- Added support of GWM Manager. [GWN Manager]
- Added LED pattern of yellow to indicate Mesh disconnection. [LED Patterns]
- Upgraded TLS to version 1.2

Firmware Version 1.0.15.6

Product Name: GWN7630 / GWN7630LR

- Added support for FCC DFS channels on GWN7630/GWN7630LR. [Scene]

Firmware Version 1.0.11.10

Product Name: GWN7630LR

- This is the initial version for GWN7630LR.

Firmware Version 1.0.11.8

Product Name: GWN7630

- Added support of DFS channel in EU for GWN7630. [Scene]
- Added support for Client Steering. [Client Steering]
- Added support for Minimum Rate Control. [RADIO]
- Added support for batch operations for Takeover.[Takeover Feature]
- Added support for Client inactivity timeout. [SSID]
- Enhanced Voucher feature by displaying remaining bytes. [Vouchers]
- Changed LED Pattern. [LED Patterns]
- Changed Local Master External Portal Configuration. [External Splash Page]
- Changed the default setting of Mesh to OFF. [Mesh]