Grandstream Networks, Inc.

GWN700x Series

User Manual

WELCOME

GWN7001/7002/7003 are Multi-WAN Gigabit VPN routers with built-in firewalls that allow businesses to build comprehensive wired, wireless and VPN networks for one or many locations. They offer high-performance routing and switching power along with built-in VPN support for secure in-office and inter-office connectivity. To provide enterprise-grade security protection and ensure stable network operation, the GWN 7001/7002/7003 features a built-in firewall with advanced content security, filtering, threat detection, attack prevention and more. To maximize network reliability, they support traffic load balancing, failover (WAN backup) and bandwidth management capabilities. The GWN7001 includes 6 Gigabit Ethernet ports.The GWN7002/GWN7003 include 2 2.5 Gigabit SFP ports, 4/9 Gigabit Ethernet ports, and 2 PoE output ports that allow them to provide power to other endpoints. These routers can manage themselves and up to 150 Grandstream GWN Series Wi-Fi APs thanks to an embedded controller located in the products' web user interface. These routers can also be managed with GDMS Networking and GWN Manager, Grandstream's free cloud and on-premise network management tools. By providing high-performance routing, VPN support, powerful security protection and easy-to-use network management tools, the GWN Gigabit VPN routers are ideal for a wide variety of deployments including small-to- medium businesses, retail, education, hospitality, healthcare and more.

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

Please do not use a different power adapter with the GWN700X routers as it may cause damage to the products and void the manufacturer warranty.

PRODUCT OVERVIEW

Technical Specifications

	GWN7001	GWN7002	GWN7003
CPU	Dual ARM Cortex A53 1GHz		
Memory and NAT Sessions	256MB RAM, 256MB Flash, 30K NAT sessions	256MB RAM, 256MB Flash, 30K NAT sessions	512MB RAM, 256MB Flash, 60K NAT sessions
Network Interfaces	6x Gigabit Ethernet ports **All ports are WAN/LAN configurable.*	2x 2.5 Gigabit SFP ports and 4x Gigabit Ethernet ports **All ports are WAN/LAN configurable*	2x 2.5 Gigabit SFP ports and 9 x Gigabit Ethernet ports **All ports are WAN/LAN configurable*
Number of VLANs Supported	Create up to 16 VLANs		Create up to 32 VLANs
NAT Routing & IPSec VPN Performance	2.2Gbps		
IPsec VPN Throughput	530Mbps		
Auxiliary Ports	1x USB 2.0 port, 1 x Reset Pinhole		
Mounting	● Desktop ● Wall mounting ● 19" standard rack (only for GWN7003)		
LEDs	8 x single-color LEDs for device tracking and status indication		13 x single-color LEDs for device tracking and status indication

Connection Type	DHCP, Static IP, PPPoE, PPTP, L2TP		
Network Protocols	IPv4, IPv6, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1x, IEEE 802.3, IEEE 802.3, IEEE802.3u, IEEE802.3x, IEEE 802.3ab		
QoS	● VLAN, TOS ● Support multiple traffic classes, filter by port, IP address, DSCP, and policing ● App QoS ● VoIP Prioritizing		
Firewall	DDNS, Port Forwarding, DMZ, UPnP, Anti-DoS, traffic rules, NAT, ALG, TURN Service		
VPN	● SSL VPN Server / Client-to Site ● IPsec VPN Client-to-Site / Site-to-Site ● PPTP VPN Server / Client-to-Site ● L2TP Client-to-Site ● WireGuard ● IPSec Encryption: DES, 3DE, AES ● IPSec Authentication: MD5, SHA-1, SHA2-256 ● IPSec Key Exchange: Main/Aggressive Mode, Pres-shared Key, DH Groups 1/2/5/14 ● IPSec Protocols: ESP ● IPsec NAT Traversal ● SSL VPN Encryption: AES, DES ● SSL Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 ● SSL VPN Certificate: RSA ● PPTP Encrpytion: MPPE 40-bit, 128-bit, IPSec ● PPTP/L2TP Authentication: MS-CHAPv1/2		
Max Concurrent VPN Tunnels	Up to 50 Tunnels	Up to 50 Tunnels	Up to 100 Tunnels
Network Management	GWN7001 embedded controller can manage itself and up to 100 GWN APs.	GWN7002 embedded controller can manage itself and up to 100 GWN APs.	GWN7003 embedded controller can manage itself and up to 150 GWN APs.
	GWN.Cloud offers a free cloud management platform for unlimited GWN Routers and GWN APs		
PoE Input	N/A	Standard: IEEE 802.3af/at	
PoE Output	N/A	2 x PoE out ports Passive 48V or IEEE802.3af	
PoE Power Budget	N/A	24V DC 1A: 12.8W 24V DC 1.5A: 24.8W	
Power & Green Energy Efficieny	Universal power adaptor included Input: 100-240VAC 50-60Hz Output: 12V DC 1A (12W)	Universal power adaptor included Input: 100-240VAC 50-60Hz Output: 24V DC 1A (24W)	
Environmental	Operation: 0°Cto 40°C Storage: -30°C to 60°C Humidity: 10% to 90% Non-condensing		
Physical	Unit Dimension: 210mm(L)x130mm(W)x35mm(H); Unit Weight: 453g Entire Package Dimension: 246mm(L)x235mm(W)x45mm(H); Entire Package Weight: 672g	Unit Dimension: 210mm(L)x130mm(W)x35mm(H); Unit Weight: 505g Entire Package Dimension: 246mm(L)x235mm(W)x54mm(H); Entire Package Weight: 730g	Unit Dimension: 260mm(L)x149mm(W)x35mm(H); Unit Weight: 1096g Entire Package Dimension: 297mm(L)x255.5mm(W)x54mm(H); Entire Package Weight: 1443g

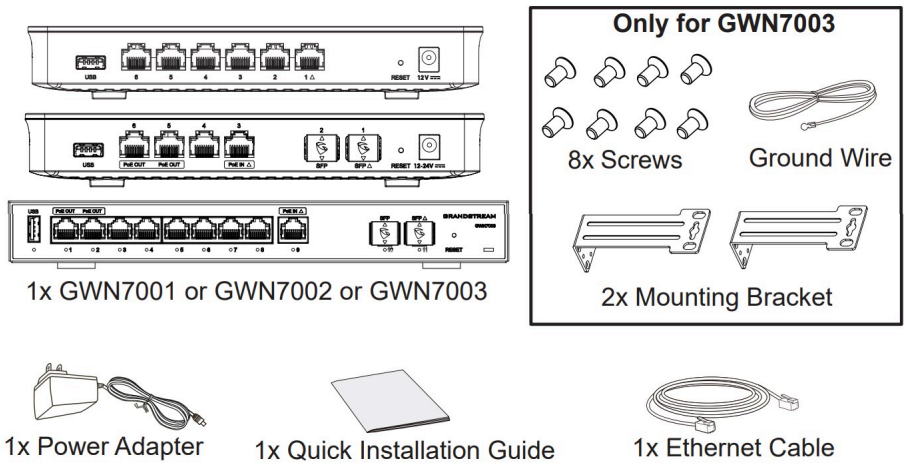
Package Content	GWN7001 router, universal power supply unit, network cable, quick installation guide	GWN7002 router, universal power supply unit, network cable, quick installation guide	GWN7003 router, universal power supply unit, network cable, quick installation guide, 8 x screws, 1 ground wire, 2 x mounting brackets.
Compliance	FCC, CE, RCM, UC, UKCA		

GWN700x Technical Specifications

INSTALLATION

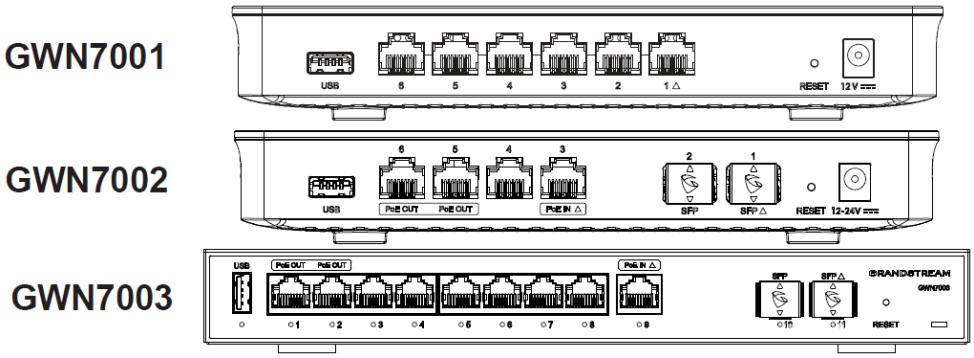
Before deploying and configuring the GWN700x router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN700x router.

Package Contents

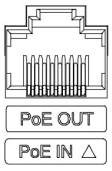


GWN700x Package Content

GWN700x Ports



GWN700x ports

No.	Port	Description
1		● **GWN7001**: 6x Gigabit Ethernet ports ● **GWN7002:** 4x Gigabit Ethernet ports ● **GWN7003:** 9 x Gigabit Ethernet ports **Note:** *All ports support WAN/LAN configurable.* *The Gigabit Ethernet ports include 2 x PoE OUT ports and 1 x PoE IN port (GWN7002/7003 only).*
2	SFP △	2x 2.5 Gigabit SFP ports (GWN7002/7003 only).

3		USB 2.0 port
4		● **GWN7001:** Power adapter connector (DC 12V, 1A) ● **GWN7002:** Power adapter connector (DC 24V, 1A) ● **GWN7003:** Power adapter connector (DC 24V, 1A)
5		Grounding terminal (GWN7003 only).
6	RESET	Factory Reset pinhole. Press for 5 seconds to reset factory default settings

GWN700x ports

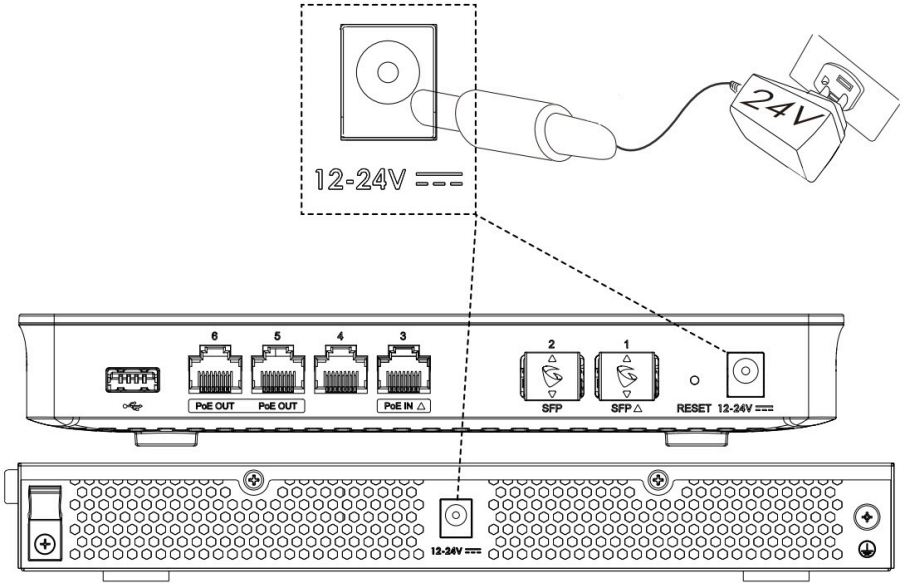
Note:

Ports with this symbol △ are configured to be used as a WAN port by default at the factory.

Powering and Connecting GWN700x

1. **Power the GWN700x**

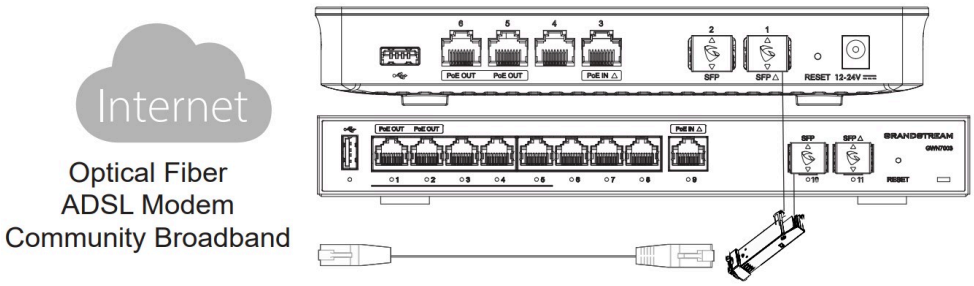
GWN7002/GWN7003 can be powered on using the right PSU (DC 24V, 1A) or PoE (IEEE 802.3af/at).



Powering the GWN700x routers

2. **Connect to the Internet**

Connect the LAN/WAN or SFP/WAN port to an optical fiber broadband modem, ADSL broadband modem, or community broadband interface.



Connect GWN700x to the Internet

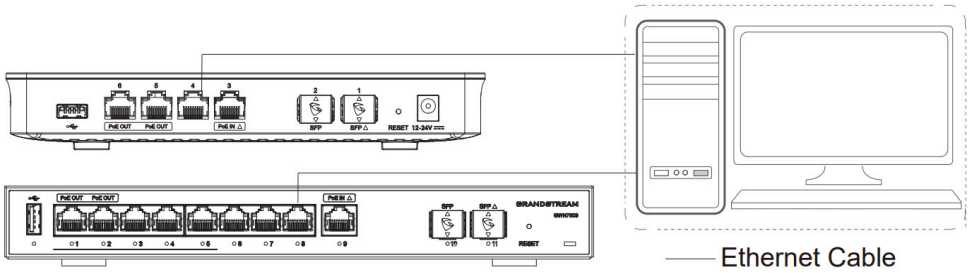
Note:

The △ sign indicates the default WAN ports:

- GWN7001: Ethernet port 1
- GWN7002: Ethernet port 3 and SFP 1
- GWN7003: Ethernet port 9 and SFP 11

3. **Connect to GWN7002/7003 Network**

Connect your computer to one of the LAN ports.

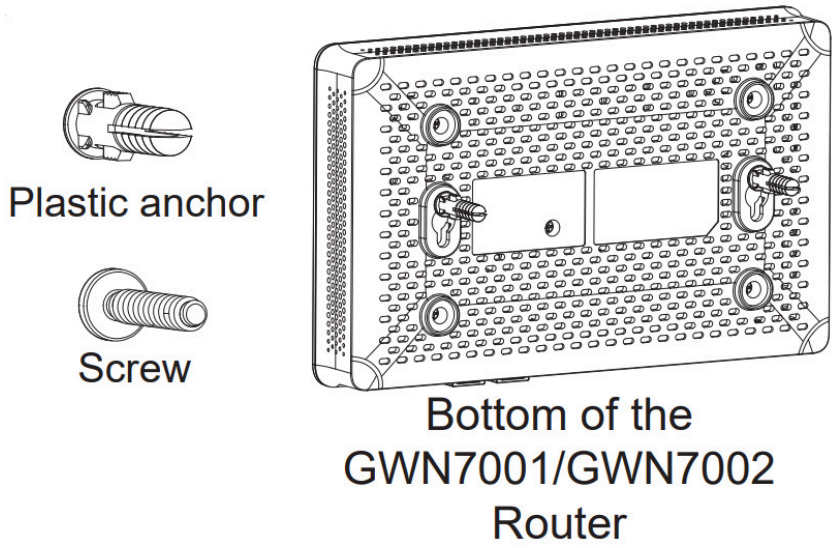


GWN700x network

GWN700x installation

- **Mounting GWN7001/7002 to the Wall**

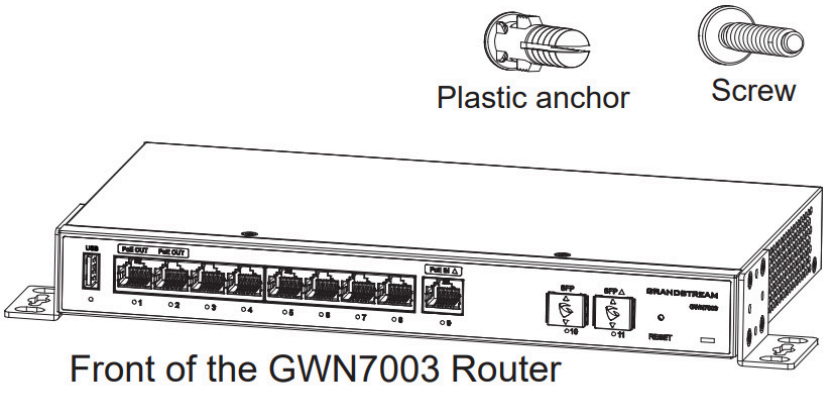
1. Using a drill, make two holes in the wall with 135.0mm spacing, 6.0mm diameter. Put a plastic anchor and screw (not provided) on each hole.
2. Mount the GWN7001/7002 router on the mounting screws.



GWN7001/7002 Wall Mounting

- **Mounting GWN7003 to the Wall**

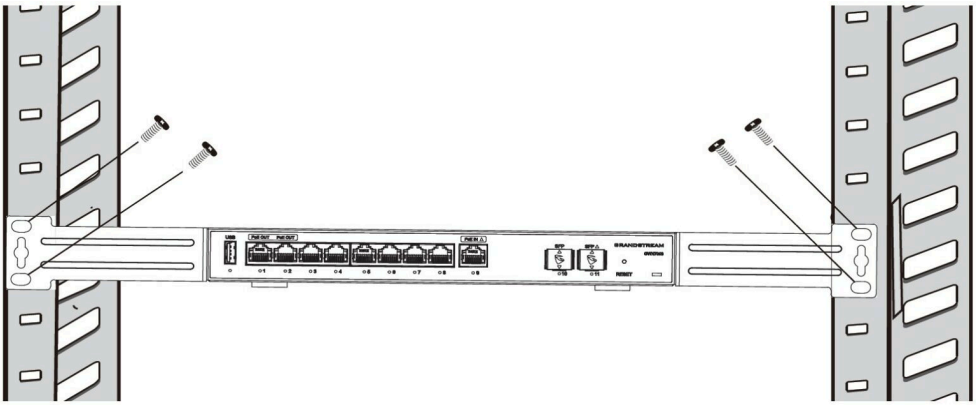
1. Use the provided screws to fix the two L-shaped Mounting bracket (rotated 90°) on both sides of the GWN7003 router.
2. Stick the router port up and horizontally on the selected wall, mark the position of the screw hole on the L-shaped mounting brackets with a marker. Then, drill a hole at the marked position with an impact drill, and drill the plastic anchors (prepared by yourself) into the drilled hole in the wall.
3. Use a screwdriver to tighten the screws (prepared by yourself) that have passed through the L-shaped mounting brackets to ensure that the GWN7003 router is firmly installed on the wall.



GWN7003 Wall Mount

- **Install on a 19" Standard Rack**

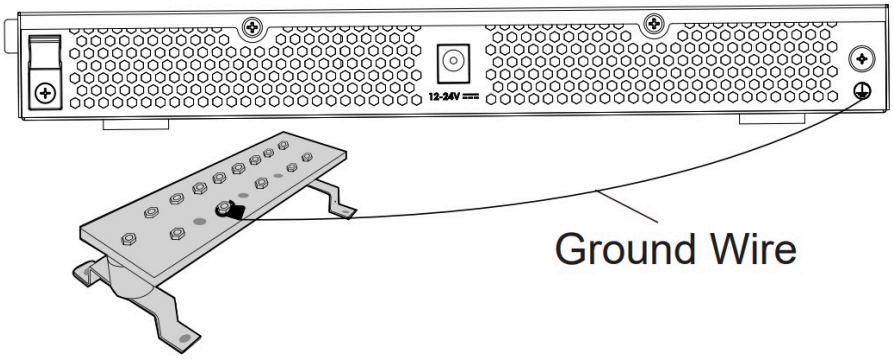
1. Check the grounding and stability of the rack.
2. Install the two L-shaped rack-mounting in the accessories on both sides of the router, and fix them with the screws provided.
3. Place the router in a proper position in the rack and support it by the bracket.
4. Fix the L-shaped rack mounting to the guide grooves at both ends of the rack with screws(prepared by yourself) to ensure that the router is stably and horizontally installed on the rack.



19" standard rack installation

- **Grounding GWN7003**

1. Remove the ground screw from the back of the router, and connect one end of the ground cable to the wiring terminal of the router.
2. Put the ground screw back into the screw hole, and tighten it with a screwdriver.
3. Connect the other end of the ground cable to other device that has been grounded or directly to the terminal of the ground bar in the equipment room.



Grounding GWN7003

Note:

GWN7002/GWN7003's default password information is printed on the MAC tag at the bottom of the unit.

Safety Compliances

The GWN700x Router complies with FCC/CE and various safety standards. The GWN700x power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN700x package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If the GWN700x Router was purchased from a reseller, please contact the company where the device was purchased for a replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

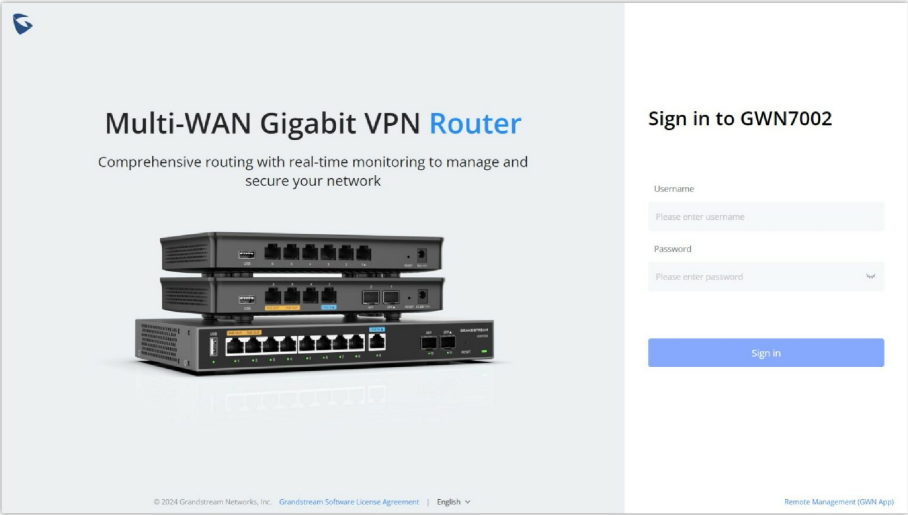
GETTING STARTED

The GWN700x Multi-WAN Gigabit VPN Routers provide an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN700x's setup.

Use the WEB GUI

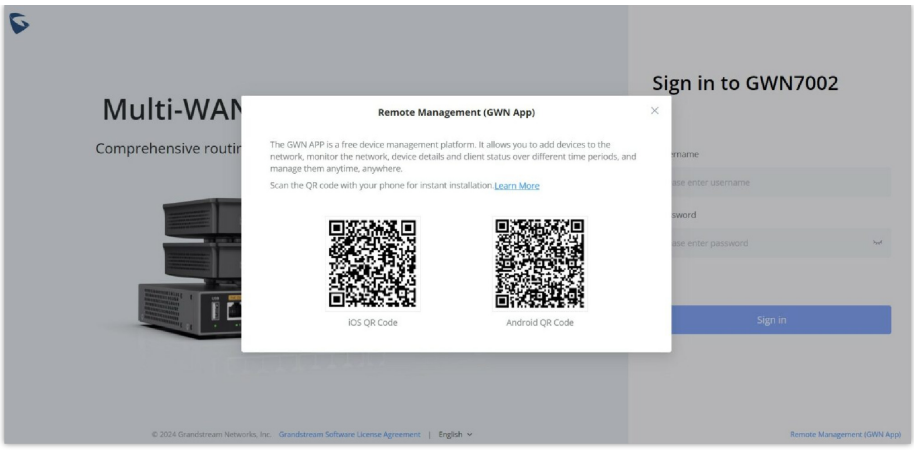
Access WEB GUI

The GWN700x 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, or Google Chrome.



GWN700x Web GUI Login Page

To download the App, click on **Remote Management (GWN App)**.



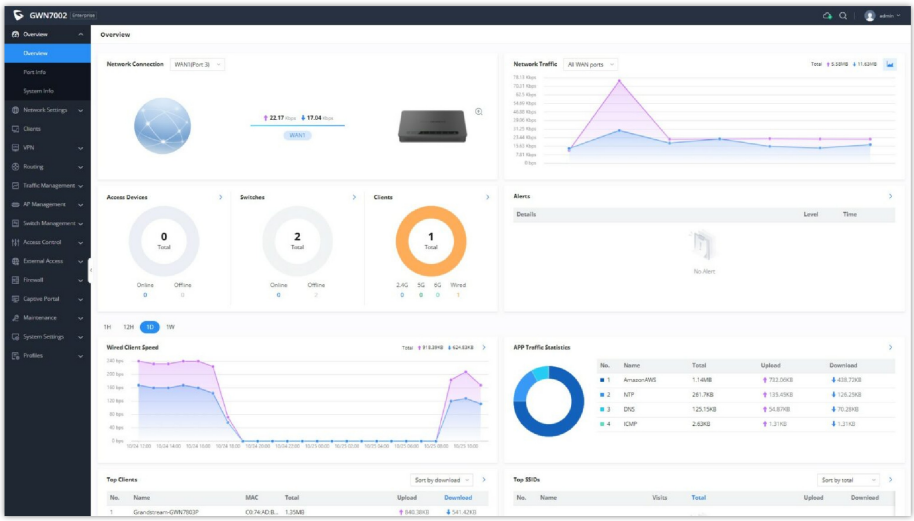
Remote Management (GWN App)

To access the Web GUI:

1. Connect a computer to a LAN port of the GWN700x.
2. Ensure the device is properly powered up, and the Power and LAN port LEDs light up in green.
3. Open a Web browser on the computer and enter the web GUI URL in the following format: https://192.168.80.1 (Default IP address).
4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is "admin" and the default password is printed on the MAC tag of the unit.

At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing the GWN700x web interface. The password field is case-sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits, and special characters are recommended for security purposes.

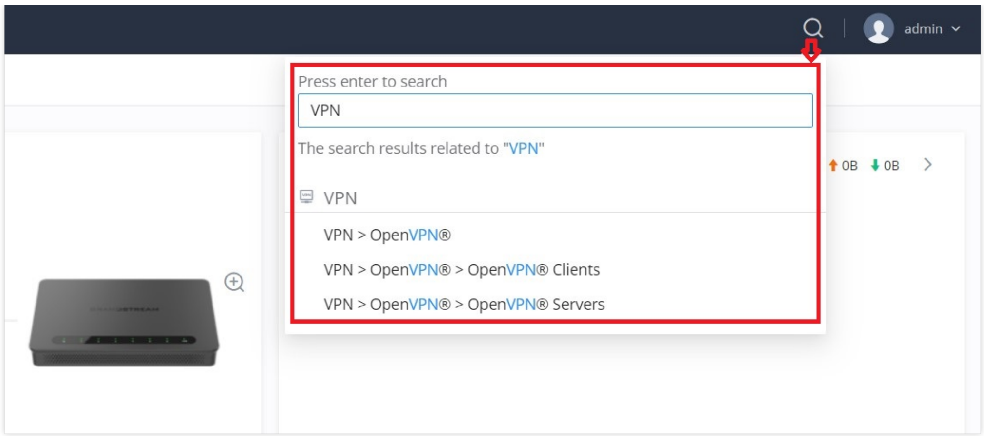
Once the user enters the password, this is the initial page that will be shown. This page contains general information and status about the router.



WEB GUI Configuration

Search

To make it easier for the user to find a particular option quickly, the GWN700X web UI has a search feature which can be accessed by clicking on the magnifier icon on the top right corner of the screen and typing the option name.

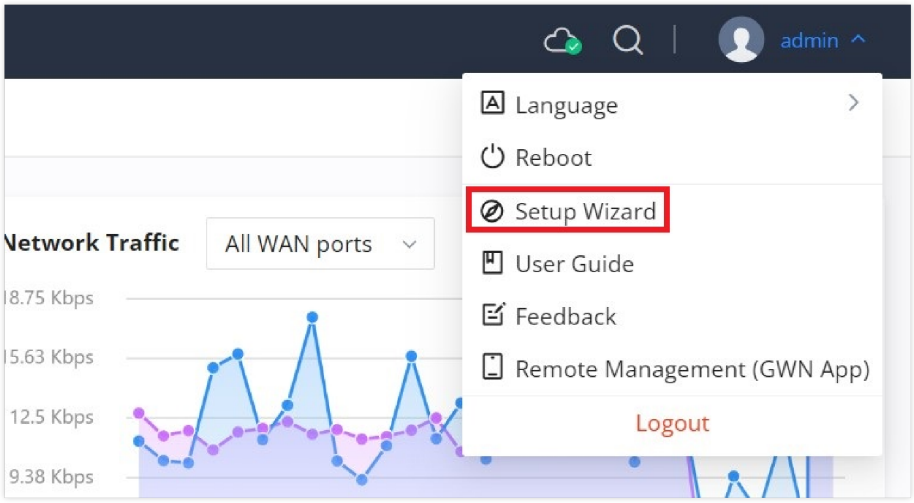


Search

Setup Wizard and Feedback

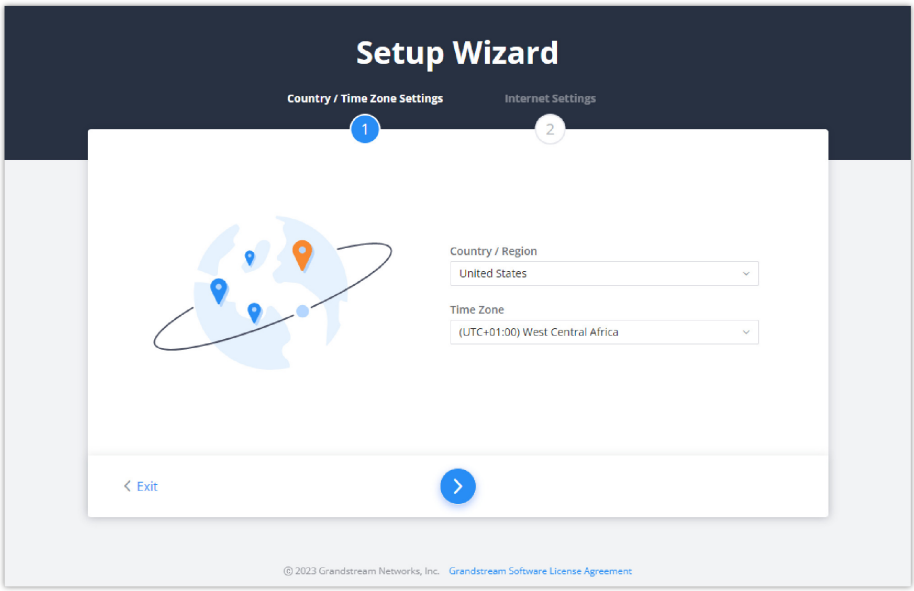
Setup Wizard

If the user missed the Setup Wizard at the first boot of GWN700X. It's accessible all the time at the top of the page and it contains the necessary settings that the user must configure in 2 steps, first country and time zone, and Internet Settings.



Setup Wizard

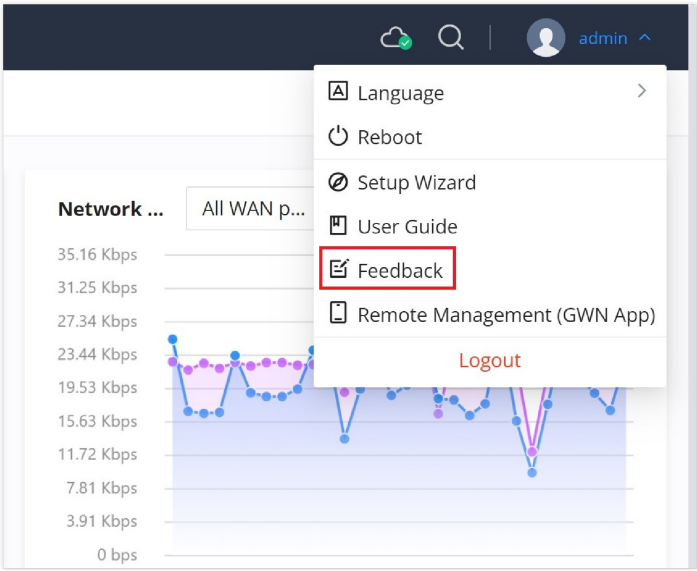
Click on button to go through the setup wizard.



Setup Wizard

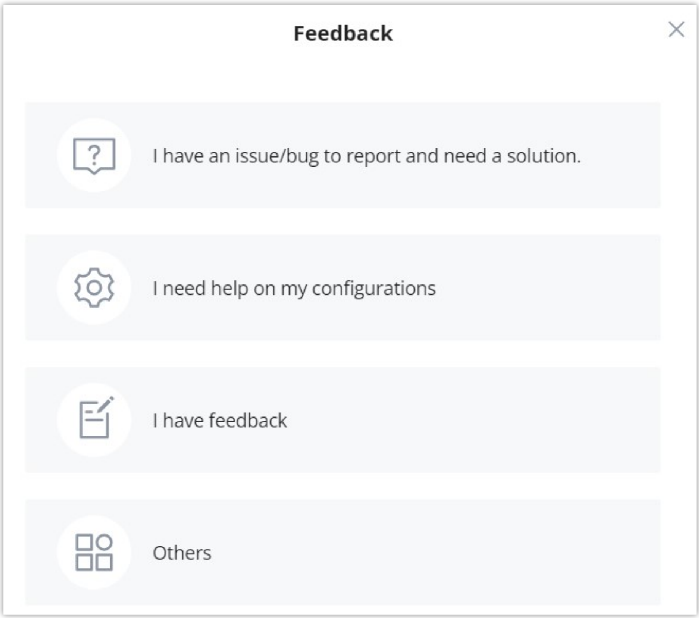
Feedback

If the user has a question or a suggestion to make the GWN700x product even better or has an issue, he can always send feedback, in case of a problem it's better as well to include Syslog as it may help solve the problem faster.



Feedback – part 1

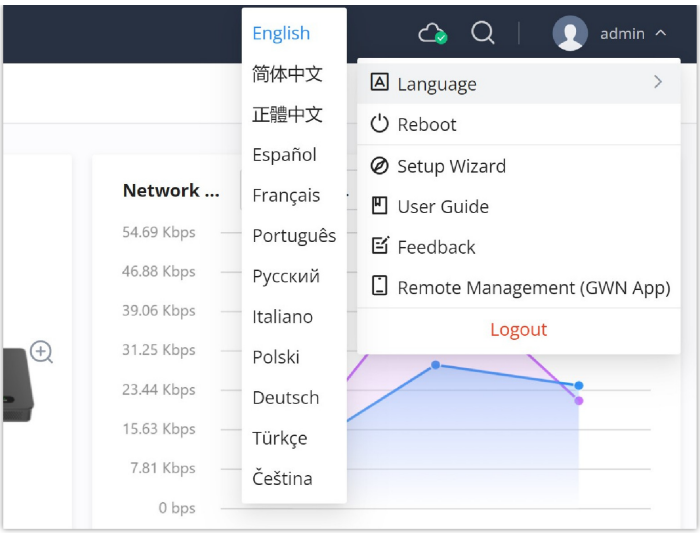
After that, click on the corresponding feedback type to get redirected to the help-desk.



Feedback – part 2

Web UI Languages

To change the Web UI interface language, on the right corner of the page, click on the username and then click on Language then select the preferred language as shown below:

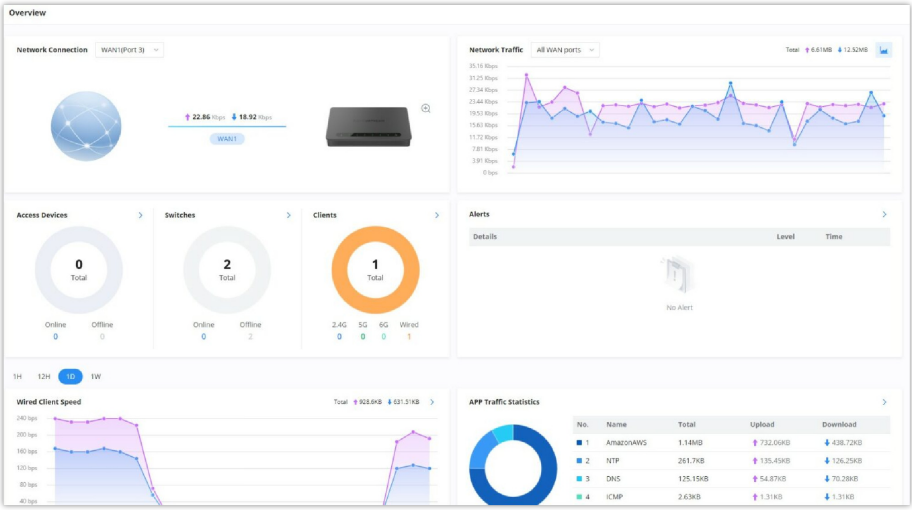


change language

OVERVIEW

Overview Page

Overview is the first page shown after successful login to the GWN700x's Web Interface. It provides an overall view of the GWN700x's information presented in a Dashboard style for easy monitoring. Please refer to the figure and table below:



Overview Page

Network Connection	Displays the current state of the network connection for the selected WAN port and shows the current upload and download speed. ***Note:*** *the user can select the WAN port from the drop-down list.*
Network Traffic	Shows network traffic in real time. ***Note:*** *the user can select the WAN port from the drop-down list or select All WAN ports.*
Access Devices	shows the total number of Access Devices online and offline.
Switches	Displays the number of switches managed by the router, both the offline and online ones.
Clients	Shows the total number of clients connected either wirelessly (2.4G, 5G and 6G) and also wired connections.
Alerts	Shows Alerts General, Important or Emergency with details and time.
Clients Speed	Displays Clients speed based on time (1H, 12H, 1D or 1W)

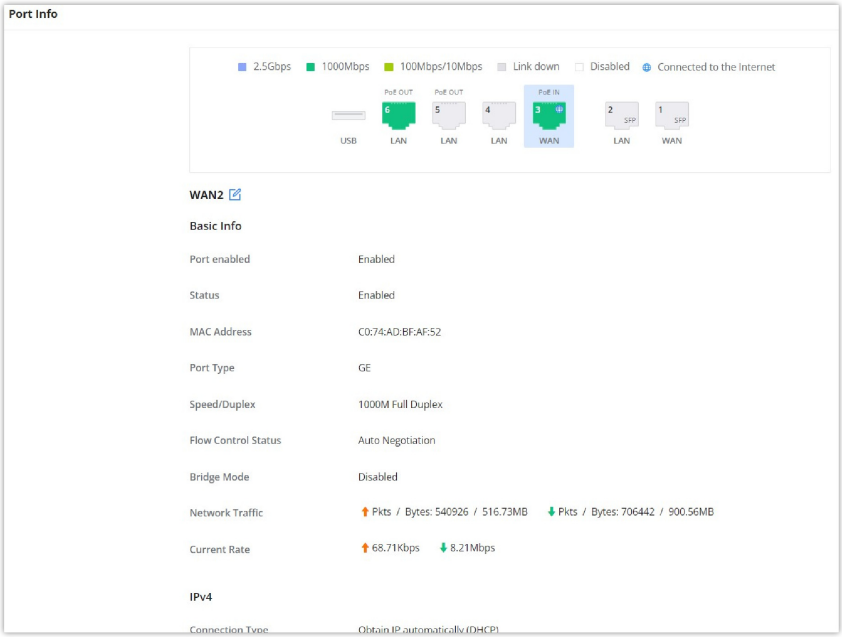
APP Traffic Statistics	Displays traffic statistics based on apps usage (%).
Top Clients	Shows the Top Clients list, users may assort the list of clients by their upload or download. Users may click on to go to Clients page for more options.
Top SSIDs	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on to go to SSID page for more options.
Top Access Devices	Shows the Top Access Devices list, assort the list by the number of clients connected to each access device or data usage combining upload and download. Click on the arrow to go to the access point page for basic and advanced configuration options.

Overview page

Port Info

Port Info page displays an overview of all ports status including the USB Port, Gigabits ports, and SFP ports, indicating the links up with green color and links down with grey color, furthermore the user can click on the port icon to get more info about the select link, refer to the figure below:

Navigate to **Web UI → Overview → Port Info**:

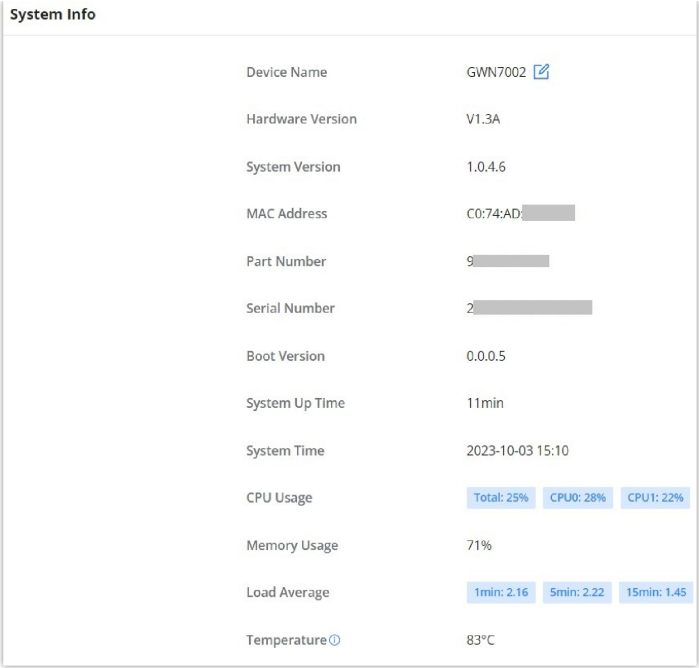


Port Info

System Info

System Info page shows many info related to GWN700x router like device name, system version, MAC address, system up time, CPU and memory usage, temperature, etc.

The router's System Info can be accessed from the **Web GUI → Overview → System Info Tab.**



System Info

NETWORK SETTINGS

In this section, the user can find general network settings of the router. These settings include WAN port configuration, general LAN ports configuration, in addition to IGMP protocol configuration, and hardware acceleration settings for the router.

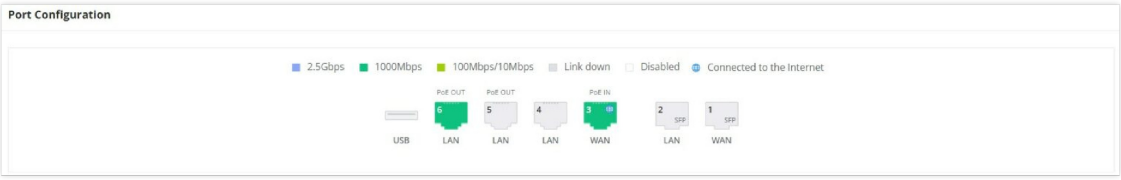
Port Configuration

To access port configuration, please access the user interface of the GWN700X router and then navigate to **Network Settings → Port Configuration**.

- **Port Status**

On the top, you can find the status of all the ports of the router.

- **Violet color:** port speed is 2.5Gbps (works only with SFP ports and 2.5Gbps SFP module).
- **Green color:** port speed is 1Gbps.
- **Light green color:** port speed is 100Mbps/10Mbps.
- **Grey color:** link down.
- **White color:** port disabled.
- **Internet icon:** port connected to the internet (for WAN ports).



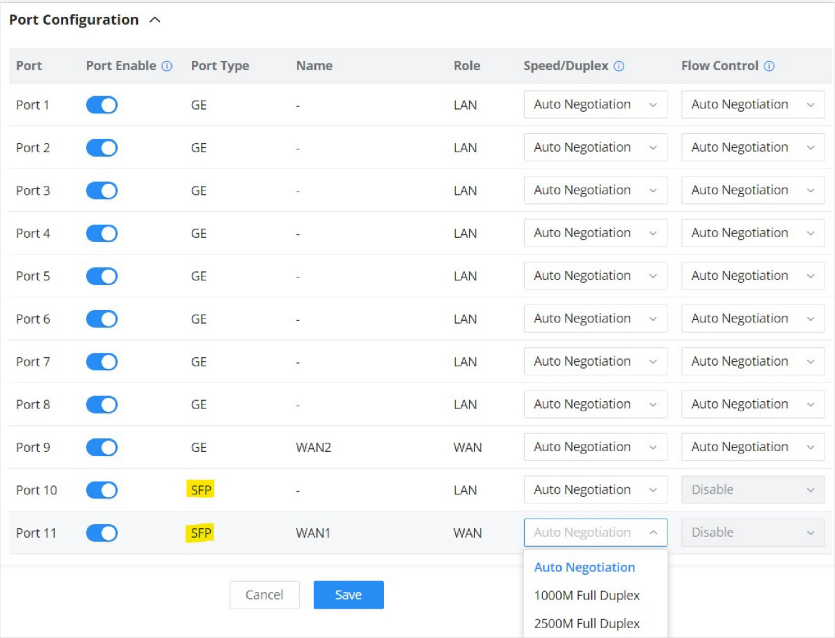
Port configuration – part 1

- **Port Configuration**

Port configuration page allows the user to configure the settings related to all the ports of the router; this includes the gigabit Ethernet ports as well as the SFP ports. The settings that can be edited include flow control, speed and duplex mode.

Note:

SFP ports support 2.5G SFP module.



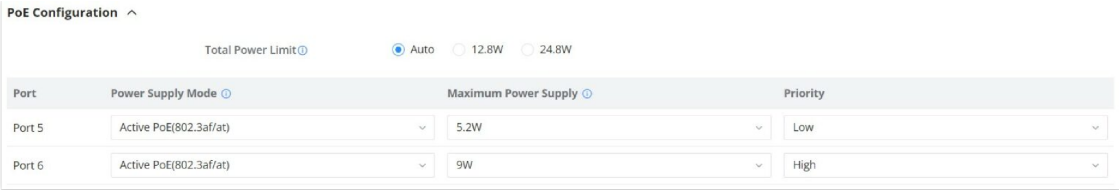
Port configuration – part 2

Port	This field indicates the port number.
Port enabled	Toggle ON or OFF the port. ***Note:*** *When set to disabled, this physical port is disabled and all port-based configurations do not take effect.*
Port Type	This field indicates the port type. ● **GE:** Stands for Gigabit Ethernet ● **SFP:** Small form-factor Pluggable
Name	This indicates the port name.
Role	This indicates the port role. ● **LAN** ● **WAN**
Speed/Duplex	In this setting, the user can configure the duplex mode as well as the speed of the port. The speed of the port can be set to: 10M, 100M, and 1000M for Ethernet ports and 1000M, 2500M for SFP ports. The duplex setting of the port can be set to: *Half Duplex* and *Full Duplex*. When the mode is set to **Auto Negotiation,** the router will determine based on the settings negotiated with the device connected.
Flow Control	The user can enable or disable flow control using this option. ***Note:*** *When the setting is set to Auto Negotiation, the router will determine based on the settings negotiated with the device connected.*

Port configuration – part 2

- **PoE Configuration**

The user can also control the total power limited that the router can supply through PoE. The power supplied can also be controlled on the port level.



Port configuration – PoE configuration

Total Power Limit	This configures the power limit which can be supplied through PoE. ● **Auto:** Automatically detect the type of the power supply and select the output power. When the DC/PoE+ input is detected, the total power limit is 12.8W ● **12.8W:** This can be selected if the power adaptor output values which correspond to the following values: 24VDC 1A ● **24.8W:** This can be selected if power adaptor output values which corresponds to the following values: 24VDC 1.5A.
Port	This field indicates the port number.
Power Supply Mode	This option configures the power supply mode. ● **Active PoE (802.3af/at)** ● **48V Passive PoE** ● **Off** **Note:** When the 48V passive PoE mode is selected, the router will always supply power. It is not safe for non-POE powered devices (PD) to access this port. Please ensure that the connected PD devices support 48V passive PoE.
Maximum Power Supply	Configures the maximum power supplied by the router. ● **5.2W** ● **9W** ● **12.8W** **Note:** If the power supply mode is Active PoE (802.3af/at) or 48V passive PoE , ensure that the sum of the maximum power supplied to all ports is less than the total power limit.
Priority	Specify the priority of the port in terms of the power supply. ● **High** ● **Low**

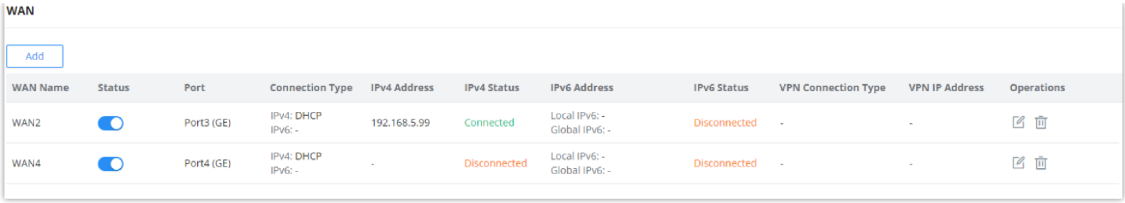
Port configuration – PoE configuration

WAN

The WAN ports can be connected to a DSL modem or a router. WAN port support also sets up static IPv4/IPv6 addresses and configure PPPoE.

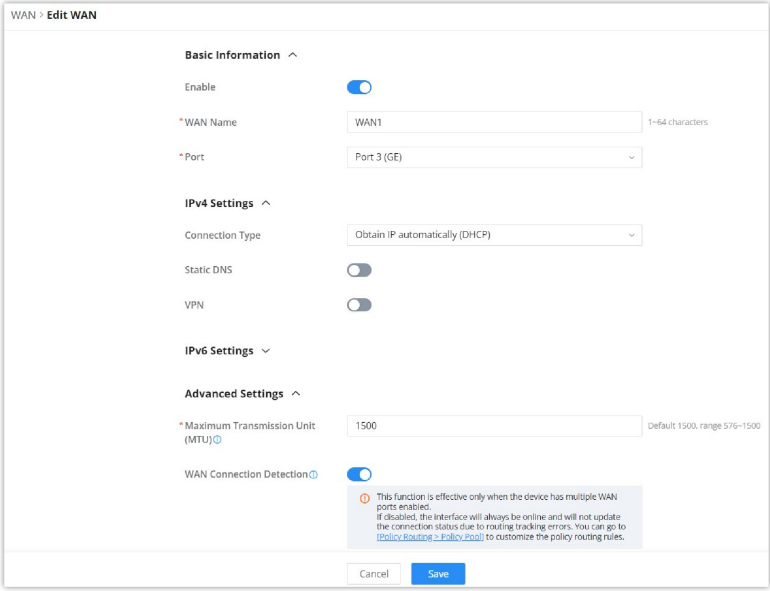
On this page, the user can modify the setting for each WAN port, and also can delete or even add another WAN, Adding a WAN port will reduce the LAN ports number. In the case where there is more than one WAN port, load balancing or backup (Failover) can be configured.

If a GWN router is added to either GDMS Networking or GWN Manager, the **WAN Speed Test** feature will be available to users. Please for more details check GWN Management Platforms – User Guide (WAN Speed Test).



WAN page

Click on Add to add another WAN port or click on the "**edit icon**" to edit the previously created ones.



Add or Edit WAN

Please refer to the following table for network configuration parameters on the WAN port.

Basic Information	
Enable	Click to enable or disable the WAN
WAN Name	Enter a name for the WAN port
Port	Select from the drop-down list the port to be used as a WAN.
IPv4 Settings	
Connection Type	• **Obtain IP automatically (DHCP):** When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. • **Enter IP Manually (Static IP):** When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. • **Internet Access with PPPoE account (PPPoE):** When selected, enter the PPPoE account and password. PPPoE Service Name is optional and specifies the service identifier required by some ISPs to connect to specific network services. Leave blank unless provided by your ISP. *The default setting is "**Obtain IP automatically (DHCP)**".*
Static DNS	Toggle **ON** or **OFF** to enable or disable static DNS
Preferred DNS Server	Enter the preferred DNS Server, ex: 8.8.8.8
Alternative DNS Server	Enter the altenative DNS Server, ex: 1.1.1.1

VPN	Toggle **ON** or **OFF** to enable or disable VPN
VPN Connection Type	● **L2TP:** Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by internet service providers (ISPs) to enable virtual private networks (VPNs). ● **PPTP:** Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks.
Username	Enter the username to authenticate into the VPN server.
Password	Enter the password to authenticate into the VPN server.
Server Address	Enter the IP address or the FQDN of the VPN server.
MPEE Encryption (if PPTP is selected)	When PPTP is chosen as the **VPN Connection Type**, the user can choose to toggle on or off the MPEE Encryption.
IP Type	● **Dynamic IP:** The IP will be assigned statically using DHCP. ● **Static IP:** The IP will be assigned statically.
IP Address	If IP Type is set to **Static IP**, specifies the static IP address.
Subnet Mask	If IP Type is set to **Static IP**, specifies the subnet mask.
Default Gateway	If IP Type is set to **Static IP**, specifies the default gateway.
VPN Static DNS	Enable this option to use the statically assigned DNS server addresses.
Preferred DNS Server	If VPN Static DNS is enabled, specifies the preferred DNS server.
Alternative DNS Server	If VPN Static DNS is enabled, specifies the alternative DNS server.
Maximum Transmission Unit (MTU)	This configures the value of the maximum transmit unit. The valid range for this value is 576 - 1460. The default value is 1430. ***Note:*** *Please do not change this value unless it's necessary.*
IPv6 Settings	
IPv6	Enable this option to use IPv6 on this specific WAN port.
Connection Type	● Obtain IP automatically (DHCPv6) ● Enter the IP manually (static IPv6) ● Internet Access with PPPoE account (PPPoE): must enabled and configured on IPv4 then the user must enter the PPPoE credentials (PPPoE Account, PPPoE Password) and PPPoE Service name is optional.
IPv6 Address/Prefix Length	When the **Connection Type** is set to *Static IP,* the user can enter the static IP address and prefix length. ***Note:*** *This option appears only when the* ***Connection Type*** *is set to Static IPv6.*

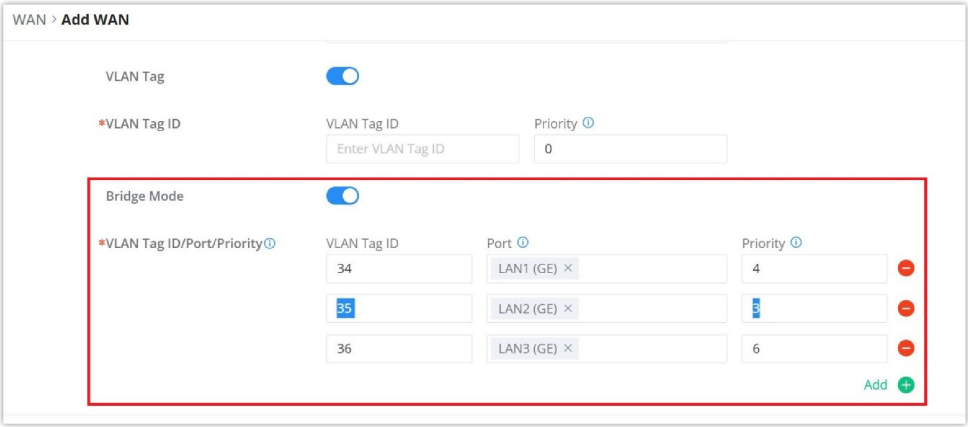
IPv6 PD/Prefix Length	When the **Connection Type** is set to Static IP, the user can enter the IPv6 PD and prefix length. ***Note:*** *This option appears only when the* ***Connection Type*** *is set to Static IPv6.*
Default Gateway	Enter the IP address of the default gateway ***Note:*** *This option appears only when the* ***Connection Type*** *is set to Static IPv6.*
Static DNS	Enable this option to enter statically assigned DNS. ***Note:*** *This option appears only when the* ***Connection Type*** *is set to DHCPv6.*
Preferred DNS Server	Enter the IP address of the preferred DNS server. ***Note:*** *This option appears only when the* ***Connection Type*** *is set to Static IPv6.*
Alternative DNS Server	Enter the IP address of the alternative DNS server ***Note:*** *This option appears only when the* ***Connection Type*** *is set to Static IPv6.*
IPv6 Relay to VLAN	Once enabled, relay IPv6 addresses to clients on the LAN side. Note: This function will take effect only "IPv6 Relay from WAN" is enabled on VLAN.
Advanced Settings	
Maximum Transmission Unit (MTU)	Configures the maximum transmission unit allowed on the wan port. ● When using **Obtain IP automatically (DHCP)**, the valid range that can be set by the user is 576-1500 bytes. The default value is 1500. Please do not change the default value unless you have to. ● When using **PPPoE**, the valid range that can be set by the user is 576-1492 bytes. The default value is 1492. Please do not change the default value unless you have to. ● When **IPv6** is enabled on the WAN, the minimum MTU is 1280.
WAN Connection Detection	Enables detection of WAN status when multiple WAN ports are active. If disabled, the WAN is always considered online, which can cause routing errors. Enabling this feature allows Policy Routing to switch to a standby WAN when the primary connection fails. Customize rules in Policy **Routing > Policy Pool**.
Tracking IP Type	Select system Default, or select Custom to specify a custom tracking IP e,g. 8.8.88.
Tracking IP	Enter the tracking IP if Tracking IP Type set to custom, click on Plus **icon** to add more.
VLAN Tag	Toggle **ON** or **OFF** to enable or disable VLAN Tag
VLAN Tag ID	Enter the VLAN Tag ID with the priority ***Notes****:* *• Priority is 0~7 with 7 being the highest priority. Default is 0.* *• Multiple WANs can use the same VLAN ID.*
Bridge mode	Toggle ON to enable Bridge Mode, which allows the WAN port to act as a bridge between specific VLANs.
VLAN Tag ID/Port/Priority	• Enter the VLAN Tag ID and assign a port for traffic bridging. • Set the priority for the VLAN traffic (0-7), where 7 represents the highest priority.
Multiple Public IP Address	Toggle **ON** or **OFF** to enable or disable Multiple Public IP Address ***Note:*** *Please use with Port Forward function, so that you can access to router via public IP address.*
Public IP Address	Enter a public IP address ***Note:*** *Click on "Plus" or "minus" icons to add or delete public IP addresses.*

WAN Settings

Triple play

Triple Play feature the user to benefit from multi-service plan (depends on ISP provider), and with a single WAN connection each service e.g: Internet, Voice (VoIP) and IPTV can be separated using VLANs and a specific port.

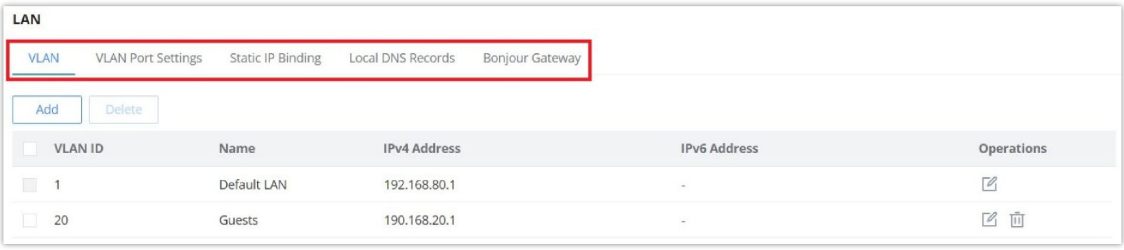
Navigate to **Network Settings** → **WAN** → **Edit/Add WAN**, then scroll down and search for Bridge Mode, please refer the figure below:



Triple Play

LAN

To access the LAN configuration page, log in to the GWN700x WebGUI and go to **Network Settings** → **LAN**. VLAN configuration such as adding VLANs or setting up a VLAN port can be found here on this page, as well as the ability to add Static IP Bindings, local DNS Records and Bonjour Gateway.



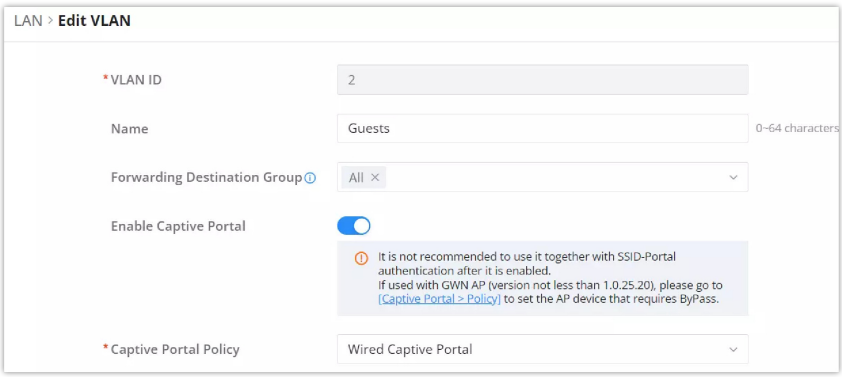
LAN configuration

VLAN

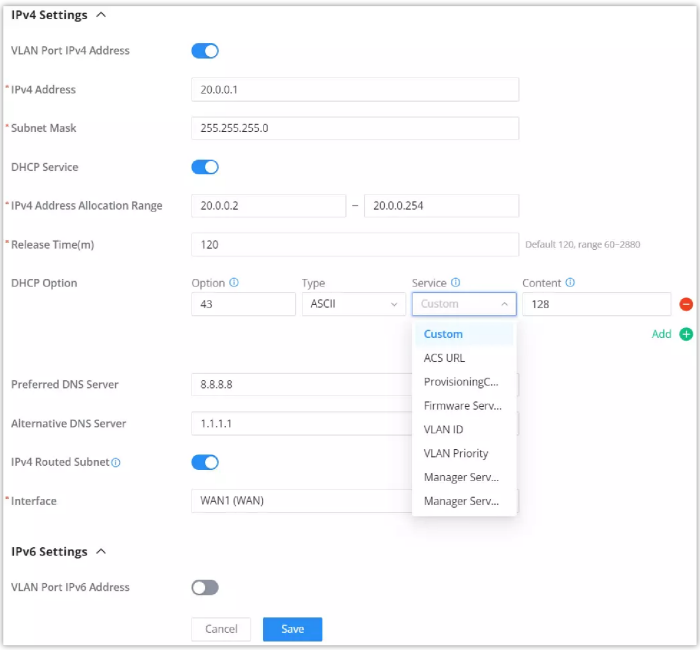
GWN700x router integrates VLAN to enhance security and add more functionalities and features. VLAN tags can be used with SSIDs to separate them from the rest, also the user can allow these VLANs only on specific LANs for more control and isolation and they can be used as well with policy routing.

- **Add or Edit VLAN**

To Add or Edit a VLAN, Navigate to **Router Interface** → **Network Settings** → **LAN**. Click on + Add button or click on Edit button.



Add or Edit VLAN – Part 1



Add or Edit VLAN – Part 2

VLAN ID	Enter a VLAN ID ***Note**: VLAN ID range is from 2 to 4094.*
Name	Enter the VLAN name
Forwarding Destination Group	By default, "**All**" is selected, and the interfaces set in the default rule of the policy pool (WAN or VPN) are selected by default and cannot be unchecked here, and subsequent new interfaces are automatically included.
Enable Captive Portal	Toggle this option to activate Captive Portal authentication for devices connected through this VLAN. It is not recommended to enable this alongside SSID-Portal authentication. If using a GWN AP with firmware version 1.0.25.20 or later, ensure to configure ByPass for the AP under Captive Portal > Policy to avoid conflicts.
Captive Portal Policy	Select the Captive portal policy from the drop-down list or click on "**Add Policy** " to add a new one.
VLAN Port IPv4 Address	
IPv4 address	Enter IPv4 Address
Subnet Mask	Enter Subnet Mask
DHCP Server	By default it's "**Off**", choose "**On**" to specifiy the IPv4 address Allocation Range
IPv4 Address Allocation Range	Enter the start and the end of the IPv4 address Allocation Range.
Release Time(m)	The default value is 120, and the valid range is 60~2880.
DHCP Option	Select the option, type, service and content for each DHCP option. Click on "**Plus**" or "**Minus**" icons to add or delete an entry. ● **Option:** The range is 2-254, exclude 6, 50-54, 56, 58, 59, 61, 82 ● **Type:** three options are possible: ASCII, HEX and IP address ● **Service:** When the option is 43 and the type is an ASCII string, the service can be selected. DHCP Option 43 is typically used for vendor-specific configurations and can vary depending on the device. ● **Content:** "Hexadecimal String", please enter XX:XX:XX format or a valid even-bit hexadecimal string. "ASCII string" or "Decimal" , the content limit is 1-255 characters. Here are some commonly configured

	services: • **ACS URL:** Auto-Configuration Server URL for TR-069 protocol, allowing remote management. • **Provisioning Code:** Used for specifying a unique identifier for automatic provisioning. • **VLAN ID:** Can be set to assign a specific VLAN ID to a device. Bootstrap URL: URL for devices to pull initial configuration files. • **Time Servers:** Configure specific time server addresses for devices. • **TFTP Servers:** Define TFTP server addresses for firmware or configuration files. • **Network Policy Settings:** Define policies that might be needed by VoIP or IP phones for network access.
Preferred DNS Server	Enter the Preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
IPv4 Routed Subnet	Once enabled, clients under the VLAN will be allowed to access the Internet using their real IP addresses.
Interface	Select the WAN interface from the drop-down list
VLAN Port IPv6 Address	
IPv6 Address Source	Select from the drop-down list the WAN port
Interface ID	Toggle **ON** or **OFF** the interface ID
Customize Interface ID	Enter the interface ID
IPv6 Preferred DNS Server	Enter the IPv6 Preferred DNS Server
IPv6 Alternative DNS Server	Enter the IPv6 Alternative DNS Server
IPv6 Relay form WAN	Once enabled, clients will get IPv6 addresses directly from the WAN side. ***Note:*** *This function will take effect only "IPv6 Relay to VLAN" is enabled on the WAN side.*
IPv6 Address Assignment	Select from the drop-down list the IPv6 address assignment ● Disable ● SLAAC ● Stateless DHCPv6 ● Stateful DHCPv6

Add/edit VLAN

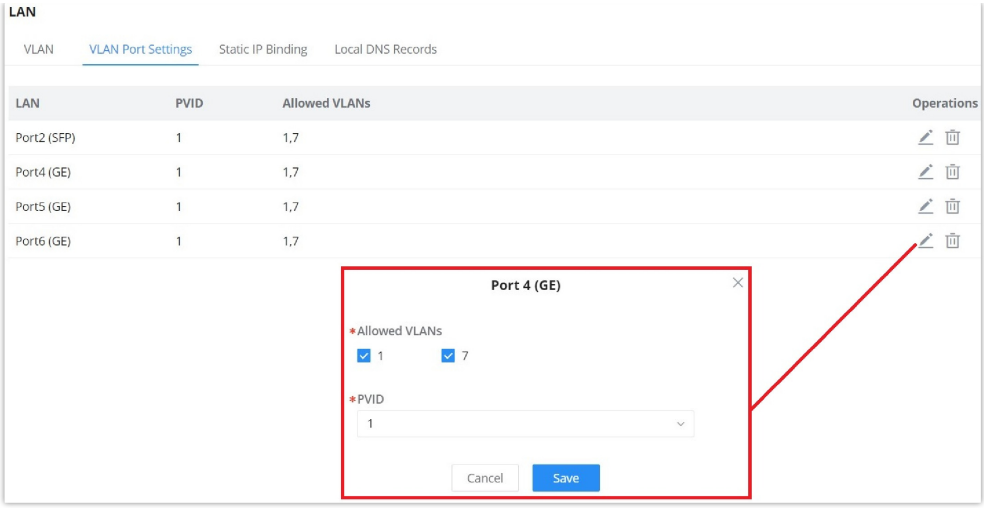
Note

Find below the number of VLANs which can be created in each model:

- **GWN7001:** 16 VLANs
- **GWN7002:** 16 VLANs
- **GWN7003:** 32 VLANs

VLAN Port Settings

The user can use LAN ports to allow only specific VLANs on each LAN port and in case there are more than one VLAN then there is an option to choose one VLAN as the default VLAN ID (PVID or Port VLAN Identifier). Click on to edit the VLAN Port Settings or click on to delete that configuration and bring back the default settings which is by default VLAN 1.



VLAN Ports

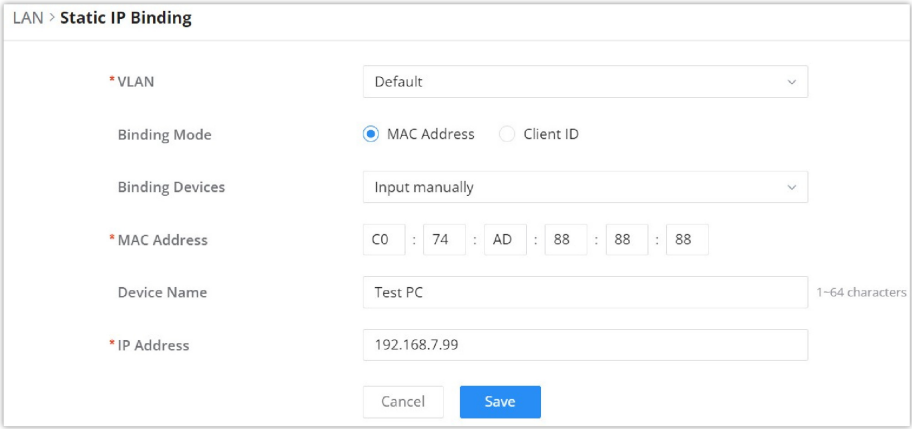
Allowed VLANs	Choose the VLANS to be allowed on this port.
PVID	Select the Port VLAN Identifier or the default VLAN ID

VLAN Port Settings

Static IP Binding

The user can set IP static binding to devices in which the IP address will be bound to the MAC address. Any traffic that is received by the router which does not have the corresponding IP address and MAC address combination will not be forwarded.

To configure Static IP Binding, please navigate to **Network Settings** → **LAN** → **Static IP Binding**, refer to the figure and table below:



Static IP Binding

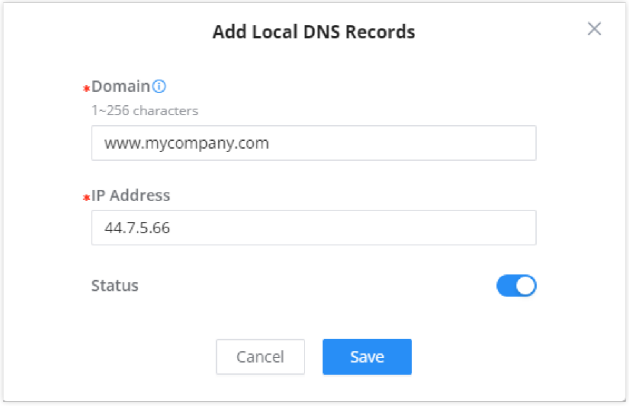
VLAN	Select the VLAN from the drop-down list.
Binding Mode	select the binding mode, either using the client MAC address or Client ID.
Binding Devices	Select the device MAC address from connected devices list. ***Note:*** *only available bindind mode is set to MAC Address.*
Client ID Type	Select the client ID type, either based on: ● MAC Address ● ASCII ● Hex ***Note:*** *only available bindind mode is set to Client ID.*

MAC Address	Enter the MAC Address ***Note:*** *only available bindind mode or Client ID Type is set to MAC Address*
ASCII	Enter the ASCII ***Note:*** *only available Client ID Type is set to ASCII*
Hex	Please enter XX:XX:XX:XX format or a valid even-digit hexadecimal number string, the first two digits need to enter the type value. ***Note:*** *only available Client ID Type is set to Hex*
Device Name	Enter a name for the device
IP Address	Enter the static IP address based on the VLAN selected previously.

Static IP Binding

Local DNS Records

Local DNS Records is a feature that allows the user to a DNS records into the router which can be used to map the domain name to an IP address. This feature can be used when the user needs to access a specific server using a domain name instead of an IP address when they do not want to include the entry in public DNS servers. To add a local DNS record, please navigate to **Network Settings** → **LAN** → **Local DNS Records**, then click "Add"



Add Local DNS Records

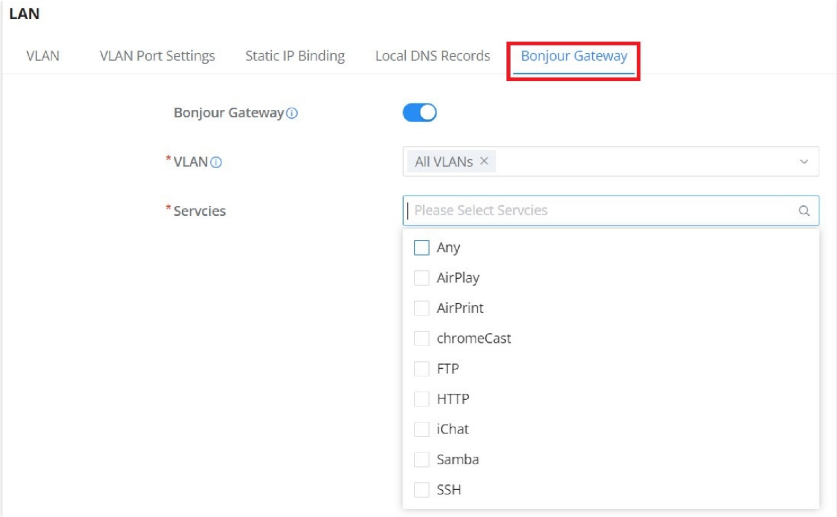
- Enter the domain name in "Domain"
- Then, enter the IP address to which the domain name will be mapped to.
- Toggle on the "Status" for the mapping to take effect.

Bonjour Gateway

The Boujour service is a zero-configuration network that enables automatic discovery of devices and services on a local network. For example: it can be used on a local network to share printers with Windows® and Apple® devices.

Once enabled, Bonjour services (such as Samba) can be provided to Bonjour supporting clients under multiple VLANs. Once enabled, configure the services of the VLANs and proxies that need to intercommunicate.

To start using Bonjour Gateway, Toggle ON or OFF the service first, then select the VLAN and the services as shown below:



Bonjour Gateway

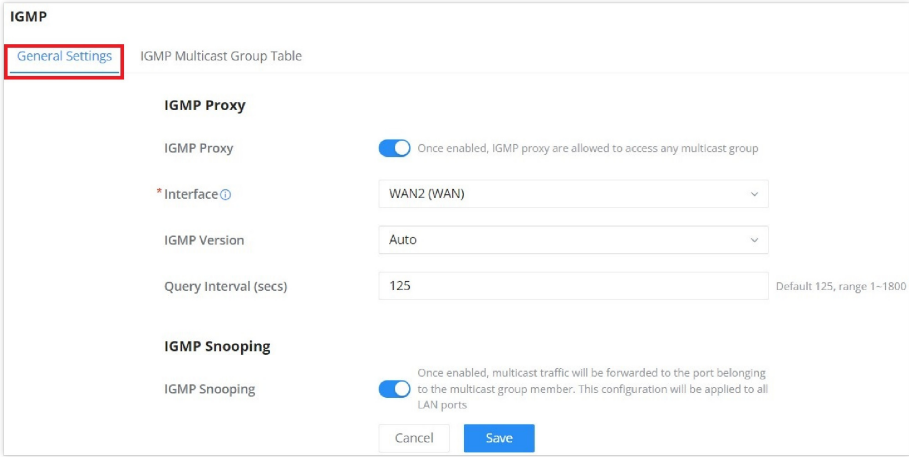
IGMP

When IGMP Proxy is enabled, the GWN router can issue IGMP messages on behalf of the clients behind it, then the GWN router will be able to access any multicast group.

To start using IGMP Proxy:

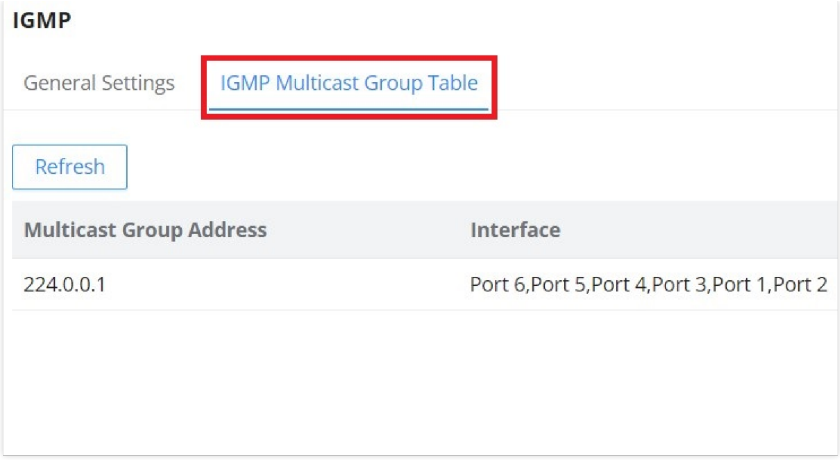
1. Toggle ON IGMP Proxy first.
2. Select the WAN interface to be used from the drop-down list (***Note:*** *IGMP proxy cannot be enabled on a WAN port with bridge mode enabled*)
3. Select the version, be default is Auto.

The user can also enable IGMP Snooping. Once enabled, multicast traffic will be forwarded to the port belonging to the multicast group member. This configuration will be applied to all LAN ports.



IGMP – General Settings

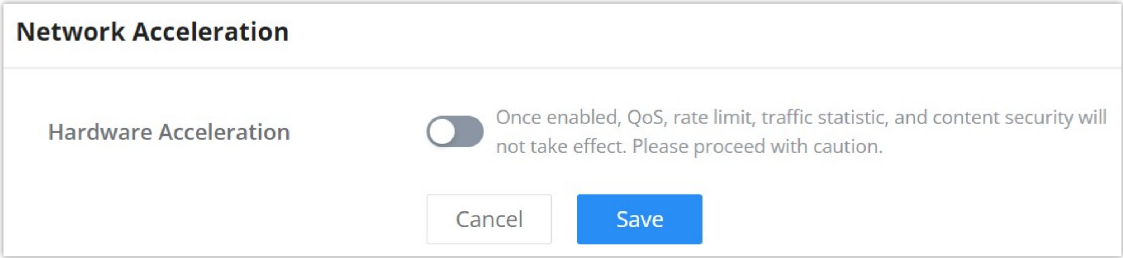
On the IGMP Multicast Group Table, all the active multicast groups will be displayed here.



IGMP – IGMP Multicast Group Table

Network Acceleration

Network acceleration allows the router to transfer data at a higher rate when Hardware acceleration is enabled. This ensures a high performance.



Hardware Acceleration

Once enabled, QoS, rate limit, traffic statistic, and content security will not take effect. Please proceed with caution.

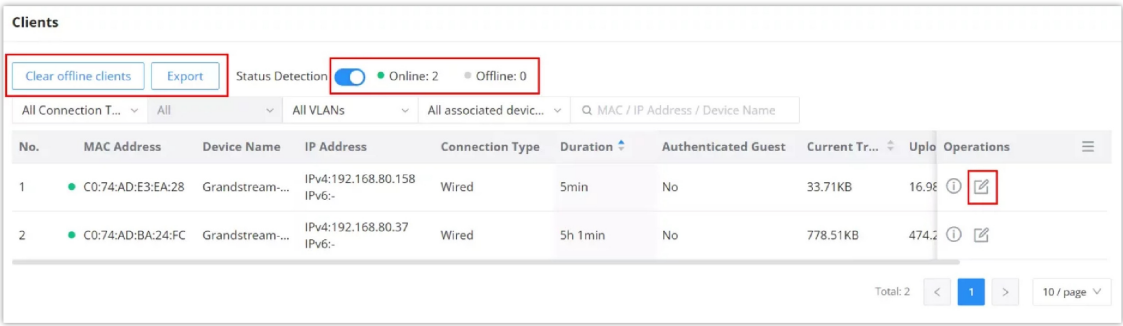
CLIENTS

Clients page keeps a list of all the devices and users connected currently or previously to different LAN subnets with details such as the MAC Address, the IP Address, the duration time, and the upload and download information etc.

The clients' list can be accessed from GWN700x's **Web GUI** → **Clients** to perform different actions for wired and wireless clients.

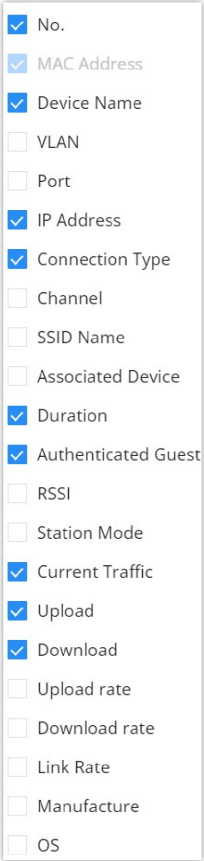
- Click on "**Clear offline clients**" to remove clients that are not connected from the list.
- Click on "**Export**" button to export clients list to local device in a EXCEL format.
- Click on "**Status Detection**" toggle to enable/disable the online and offline status.

Please refer to the figure and table below:



Clients Page

The users also have the option to customize this page by adding or removing desired columns, check the figure below for the available options:



Client page options

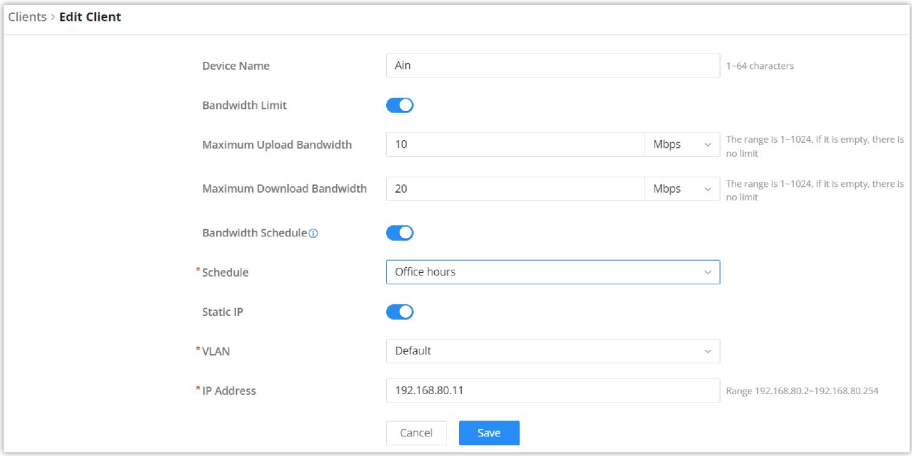
MAC Address	This section shows the MAC addresses of all the devices connected to the router.
Device Name	This section shows the names of all the devices connected to the router.
VLAN	Displays the VLAN the client connected to.
IP Address	This section shows the IP addresses of all the devices connected to the router.
Connection Type	This section shows the medium of connection that the device is using. There are two mediums which can be used to connect: ● **Wireless:** Using an access point with the router. ● **Wired:** Using an ethernet wired, either connected directly to one of the router's LAN ports, or through a switch.
Channel	If device is connected through an access point, the router will retrieve the information of which channel the device is connected to.
SSID Name	If device is connected through an access point, the router will retrieve the information of which SSID the device is connected to.
Associated Device	In case of an access point or an access point with the router, this section will show the MAC address of the device used
Duration	This indicates how long a device has been connected to the router.
RSSI	RSSI stands for *Received Signal Strength Indicator.* It indicates the wireless signal strength of the device connected to the AP paired with the router.

Station Mode	This field indicates the station mode of the access point.
Total	Total data exchanged between the device and the router.
Upload	Total uploaded data by the device.
Download	Total downloaded data by the device.
Current Rate	The real time WAN bandwidth used by the device.
Link Rate	This field indicates the total speed that the link can transfer.
Manufacturer	This field indicates the manufacturer of the device.
OS	This field indicates the operating system installed on the device.

Clients Page

- **Edit Device**

under the operations column click on "**Edit**" icon to set the name of the device, and assign a VLAN ID and static address to the device. It's also possible to limit bandwidth for this exact device and even assign a schedule to it from the list. Refer to the figure below:



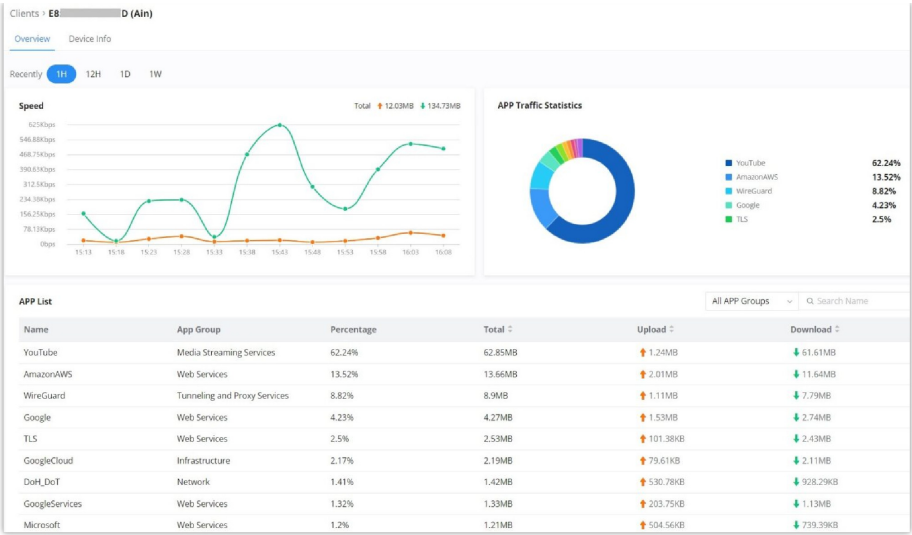
Edit Device

- **Delete Device**

To delete a device, go to the **Operations** column and click the button 🗑 then click "**Delete**". Please note that you can only delete the devices which are offline, the devices online cannot be deleted.

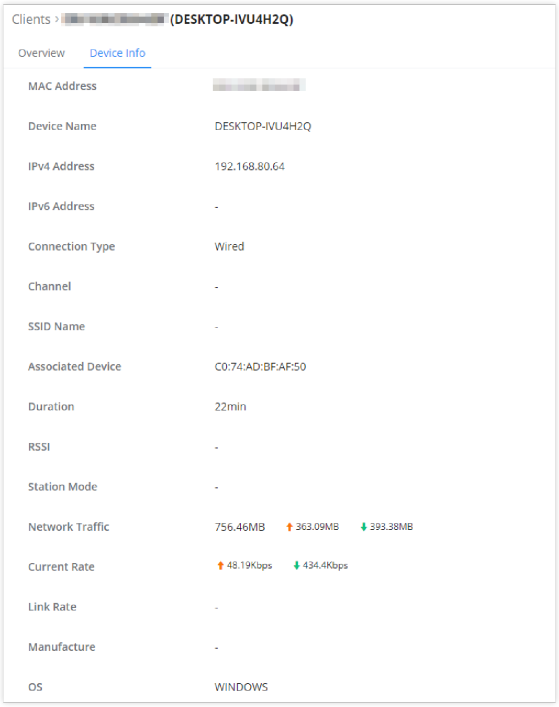
- **View Client Information and Report**

Click on a device to open the full report of the traffic used by the device. The report will contain the total data uploaded and downloaded, as well as the statistics used by each application on the device.



Device Overview

To see information related to the device, please click on **Device Info** tab.



Device Info

VPN

VPN stands for “Virtual Private Network” and it encrypts data in real time to establish a protected network connection when using public networks.

VPN allows the GWN700x routers to be connected to a remote VPN server using PPTP, IPSec, L2TP, OpenVPN® and WireGuard® protocols, or configure an OpenVPN® server and generate certificates and keys for clients.

GWN700X routers support the following VPN functions:

- **PPTP:** Client and server
- **IPSec:** Site-to-site and client-to-site
- **OpenVPN®**: Client and server
- **L2TP:** Client
- **WireGuard®**: Server

For more details on how to configure each VPN protocol separately, please refer to the below guides:

1. **OpenVPN®**
   - OpenVPN® Site-to-Site Guide
   - OpenVPN® Client-to-Site Guide
2. **L2TP**
   - L2TP Client Guide
3. **PPTP Guide**
   - PPTP Client-to-Server Guide
4. **WireGuard®**
   - WireGuard Site-to-Site Guide
   - WireGuard Client-to-Server Guide
5. **IPSec**
   - IPSec Site-to-Site Configuration Guide
   - IPSec Client-to Site Configuration Guide

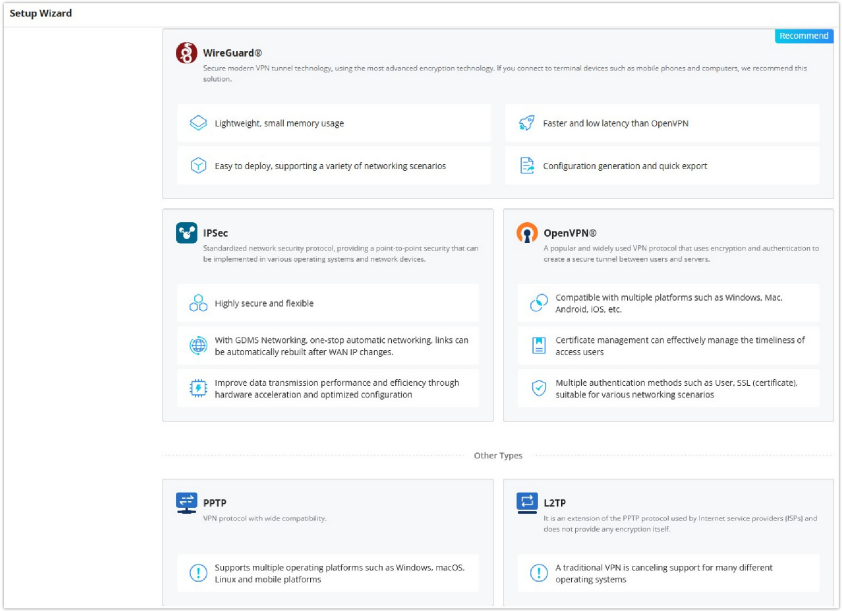
VPN page can be accessed from the GWN700x **Web GUI** → **VPN**.

Setup Wizard

The main purpose of the Setup Wizard is to help users quickly and efficiently configure VPNs like **WireGuard®, IPSec, OpenVPN®, PPTP**, and **L2TP**. It allows you to configure VPN connections with minimal manual input by automating most of the necessary steps and parameters. This makes it particularly useful for users who may not be familiar with more advanced networking settings.

- **Easy Deployment**: The wizard simplifies VPN deployment, supporting various networking scenarios, including both **client-to-site** and **site-to-site** connections.
- **Predefined Configuration**: Users can select from predefined VPN options, such as WireGuard®, IPSec, OpenVPN®, etc., based on their needs. Each type of VPN comes with different available scenes and configurations.

Purpose: The primary goal of this wizard is to make VPN setup **faster** and **easier** by automating many of the common settings. This reduces the likelihood of misconfigurations and ensures a smoother setup experience, especially for users who may not have in-depth knowledge of VPN protocols.



VPN Setup Wizard

Relation to Manual Configuration: It's important to note that the VPN Setup Wizard mirrors the **same configuration process** as manually configuring VPNs, but in a more user-friendly way. Advanced users can still manually configure VPNs if needed, but for most users, the wizard offers a more accessible method.

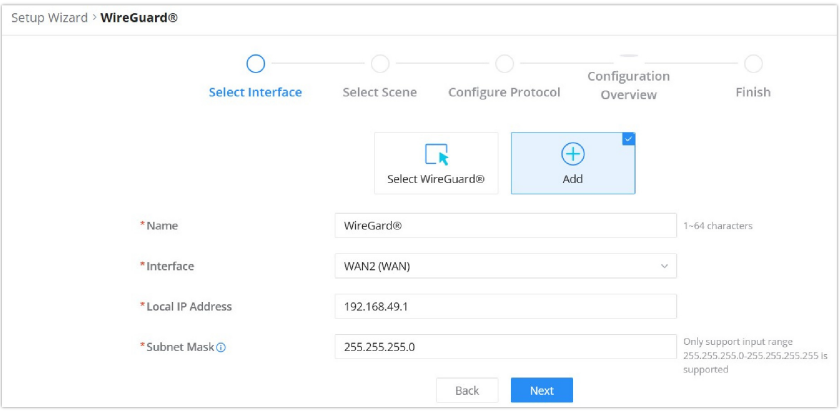
VPN-Type Specific:

The wizard is tailored for each VPN type. For instance:

- **WireGuard®**: Prioritizes fast, low-latency connections with a simple and secure setup.
- **IPSec**: Provides robust encryption and secure communication for both site-to-site and client-to-site scenarios.
- **OpenVPN®**: Allows more customizable security options, such as user-based certificate management and SSL encryption.
- **PPTP/L2TP**: While legacy protocols, these are supported for backward compatibility with older devices and systems.

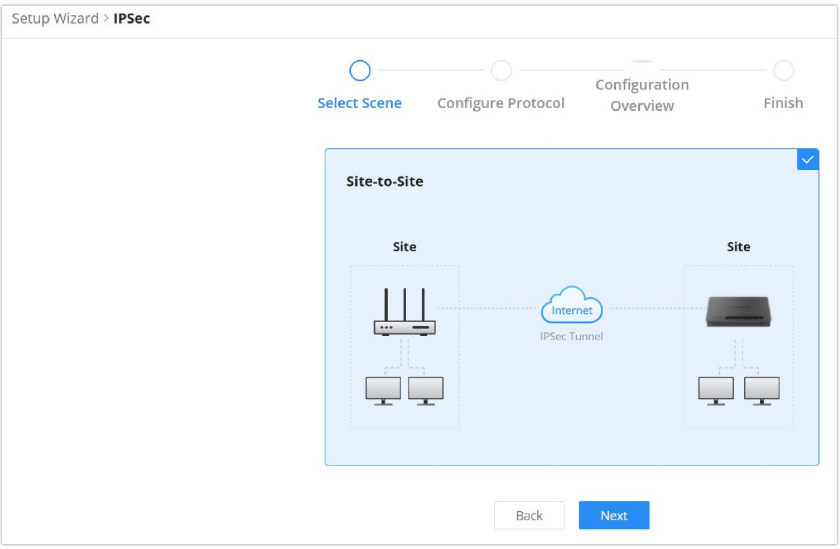
By following this wizard, users can rapidly configure the required VPN connections without needing to navigate complex settings manually, making it an ideal solution for businesses looking to enhance security without complexity.

- **WireGuard® Setup Wizard**



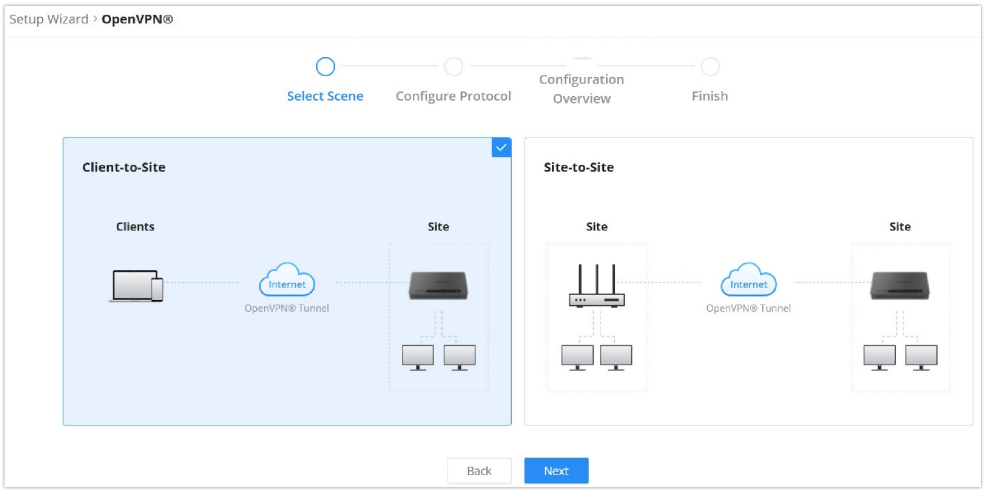
WireGuard® Example

- **IPSec Setup Wizard**



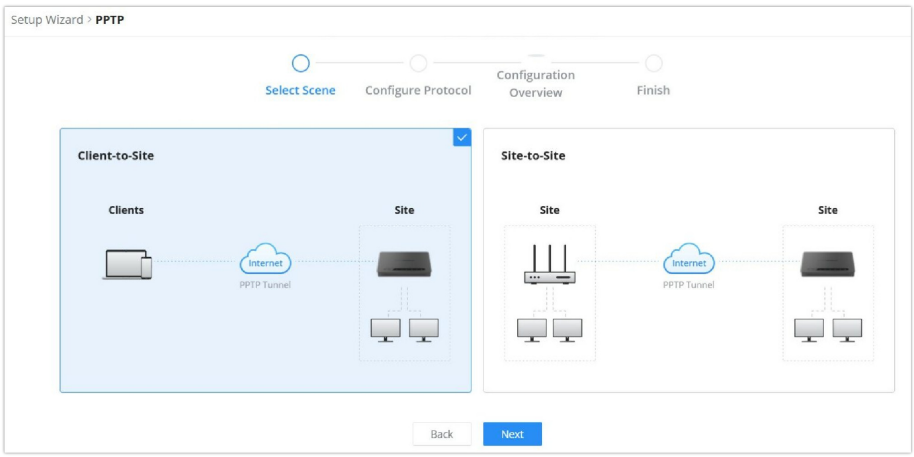
IPSec Example

- **OpenVPN® Setup Wizard**



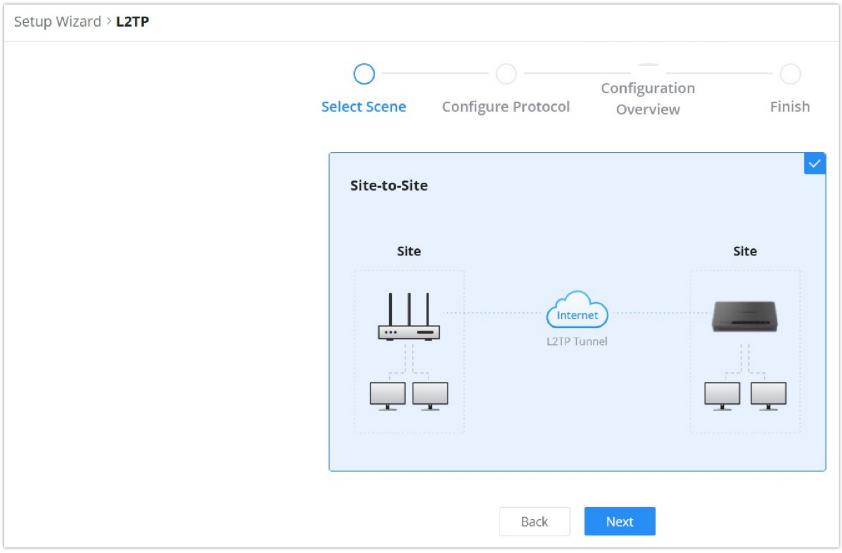
OpenVPN® Example

- **PPTP Setup Wizard**



PPTP Example

- **L2TP Setup Wizard**

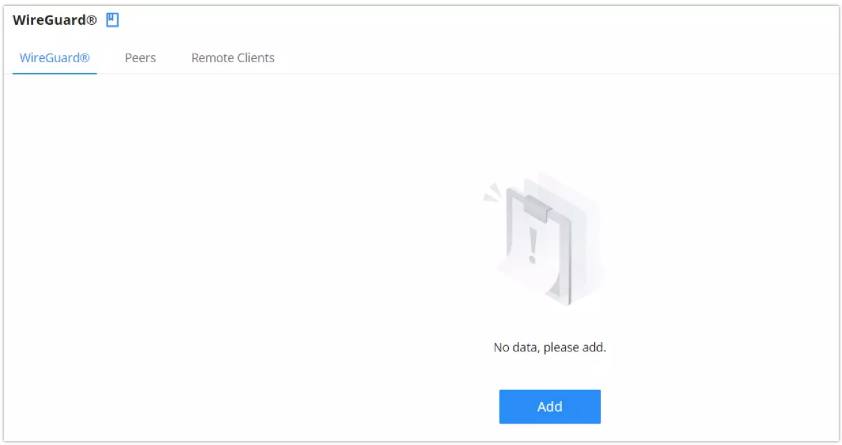


L2TP Example

WireGuard®

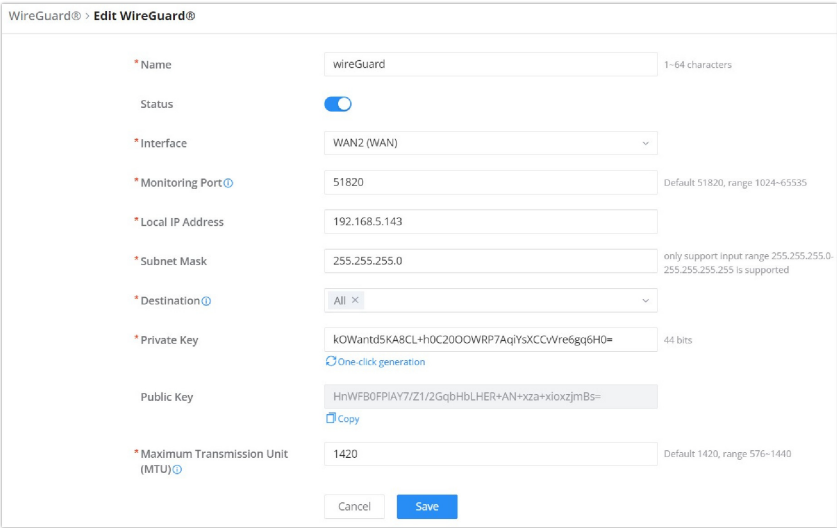
WireGuard® is a free, open-source VPN solution that offers high performance, ease of use, and robust security for encrypting virtual private networks. The GWN700x series routers support WireGuard® VPN with features like automatic client generation and QR code scanning for easy setup on mobile devices and other devices with camera support. WireGuard® can be configured to create Peers for Site-to-Site connections or to establish clients for terminal devices, such as mobile phones and computers.

To start using WireGuard® VPN, please navigate to **Web UI → VPN → WireGuard® page**. Click on "**Add**" button to add a WireGuard® server as shown below:



Add WireGuard®

Please refer to the figure and table below when filling up the fields.

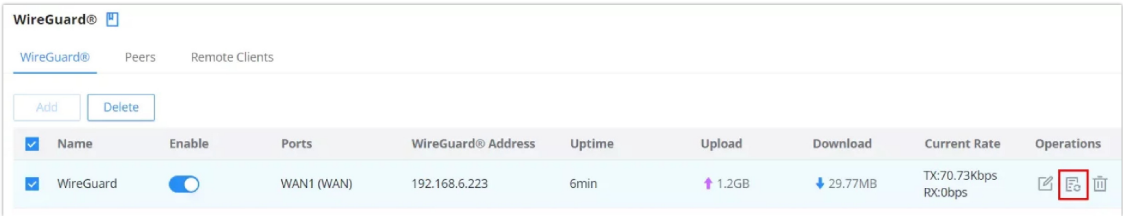


Add/Edit WireGuard®

Name	Specify a name for Wireguard® VPN.
Status	Toggle **ON** or **OFF** to enable or disable the Wireguard® VPN.
Interface	Select from the drop-down list the WAN port.
Monitoring Port	Set the local listening port when establishing a WireGaurd® tunnel. ***Default:*** *51820*
Local IP Address	Specify the network that WireGuard® clients (Peers) will get IP address from.
Subnet Mask	Configures the IP address range available to the Peers.
Destination	Select the Destination(s) from the drop-down list. ***Note:*** *When selecting "All", subsequent new interfaces will be automatically included.*
Private Key	Click on "**One-Click Generation**" text to generate a private key.
Public Key	The public key will be generated according to the private key. Click on "**Copy**" text to copy the public key.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.

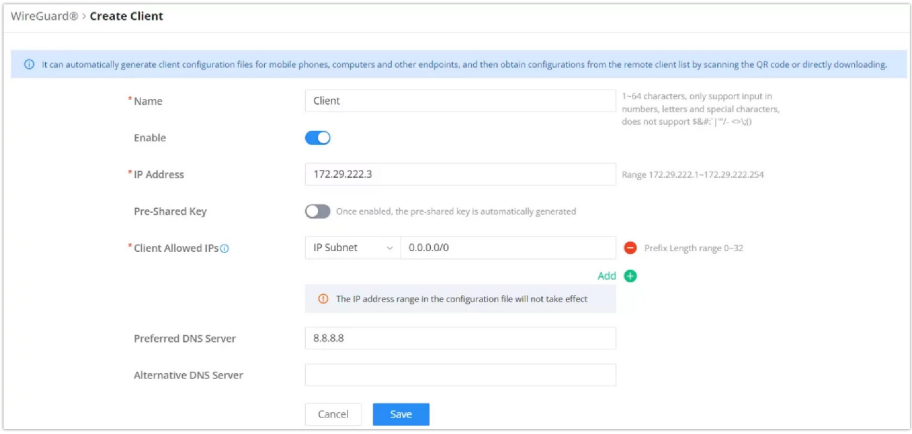
Add/Edit WireGuard®

Once finished configuring WireGuard®, click on " **Add client**" icon to generate clients very quickly and easily as shown in the figures below:



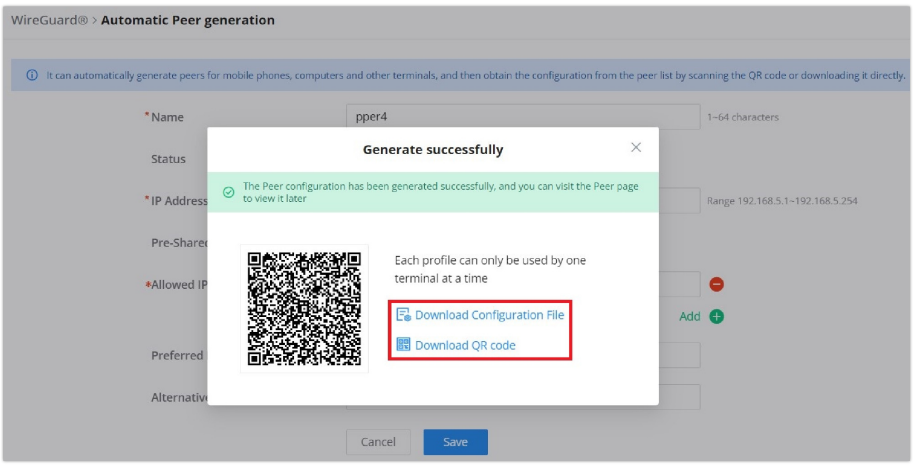
WireGuard® – Add Client

Enter a name and toggle status **ON** then click on "**Save**" button.



WireGuard® Add client – part 1

Now, the user can either download the configuration file and share it, or download QR code for devices like mobile phones to scan.

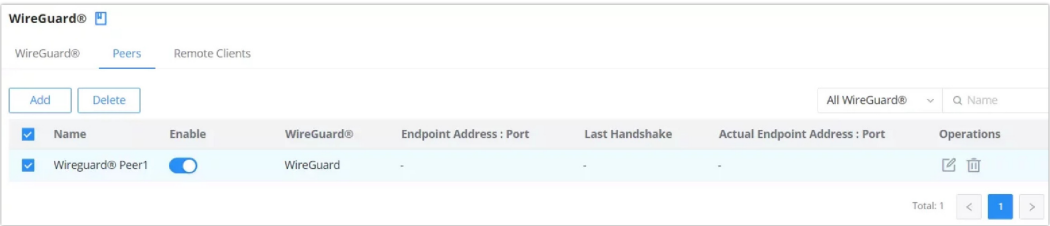


WireGuard® Add clients – part 2

For more details, refer to this guide: WireGuard® Site-to-Client.

Peers

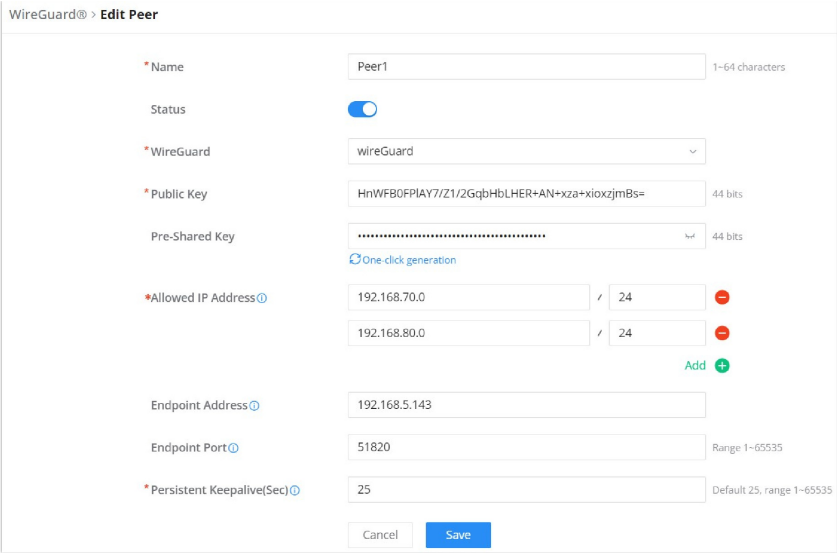
On the Peers tab, users can create Site-to-Site connections by clicking the '**Add**' button to configure new WireGuard peers.



WireGuard® – Peers tab

for more details, refer to this guide: WireGuard® Site-to-Site.

Please refer to the figure below when filling up the fields.



WireGuard® – add/edit peer

Remote Clients

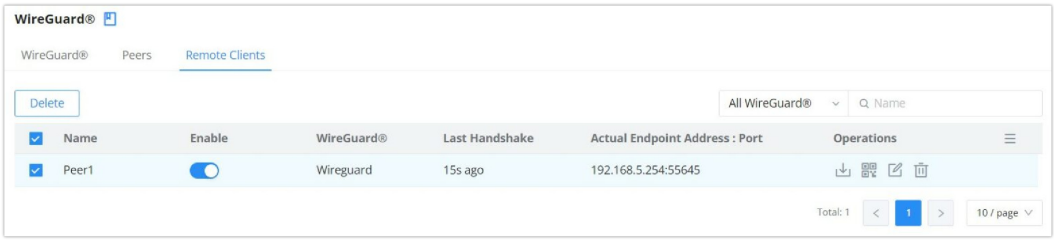
The **Remote Clients** tab displays a list of all connected WireGuard® clients. Each client connection is shown with relevant details such as:

- **Name**: The client's configured name.
- **Enable**: Toggle to enable or disable the connection for the client.
- **WireGuard®**: Displays the WireGuard® instance the client is connected to.
- **Last Handshake**: Shows when the last successful handshake with the client occurred.
- **Actual Endpoint Address : Port**: Displays the client's current IP address and port.

Operations include:

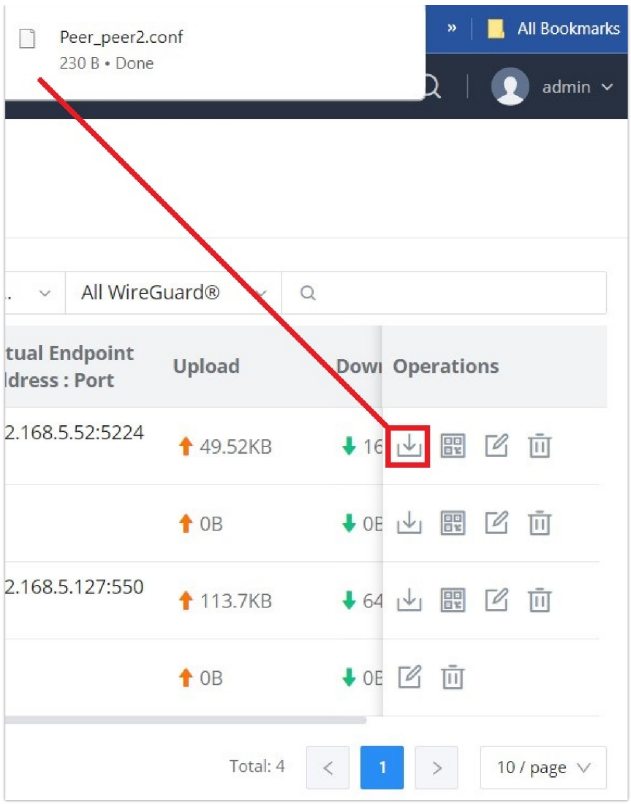
- View connection details.
- Download client configuration file or QR code.
- Edit or delete the client configuration

To view connected clients, navigate to **VPN → WireGuard® → Remote Clients**.



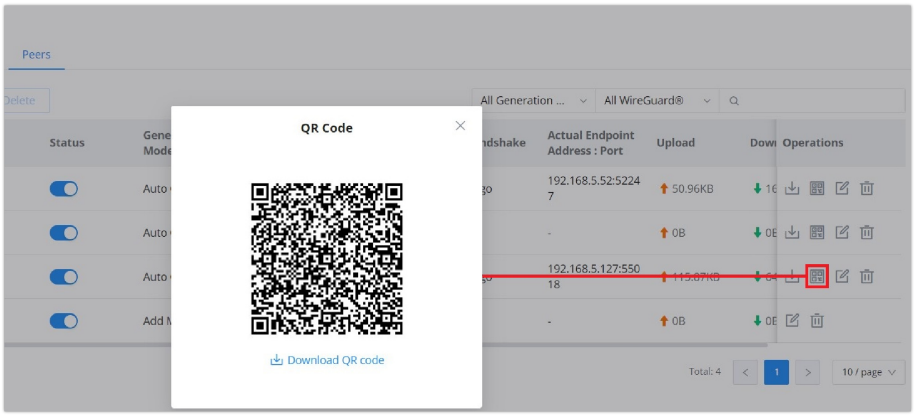
WireGuard® – Remote Clients

The user can download the config file after adding the client.



WireGuard® – download client config

Or scanning the QR code for devices with camera support.



WireGuard® – scan client config

IPSec

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

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

IPSec also involves IKE (Internet Key Exchange) protocol which is used to set up the Security Associations (SA). A Security Association establishes a set of shared security parameters between two network entities to provide secure network layer communication. These security parameters may include the cryptographic algorithm and mode, traffic encryption key, and parameters for the network data to be sent over the connection. Currently, there are two IKE versions available – IKEv1 and IKEv2. IKE works in two phases:

Phase 1: ISAKMP operations will be performed after a secure channel is established between two network entities.

Phase 2: Security Associations will be negotiated between two network entities.

IKE operates in three modes for exchanging keying information and establishing security associations – Main, Aggressive and Quick mode.

• **Main mode:** is used to establish phase 1 during the key exchange. It uses three two-way exchanges between the initiator and the receiver. In the first exchange, algorithms and hashes are exchanged. In the second exchange, shared keys are generated using the Diffie-Hellman exchange. In the last exchange, verification of each other's identities takes place.

• **Aggressive mode**: provides the same service as the main mode, but it uses two exchanges instead of three. It does not provide identity protection, which makes it vulnerable to hackers. The main mode is more secure than this.

• **Quick mode**: After establishing a secure channel using either the main mode or aggressive mode, the quick mode can be used to negotiate general IPsec security services and generate newly keyed material. They are always encrypted under the secure channel and use the hash payload that is used to authenticate the rest of the packet.

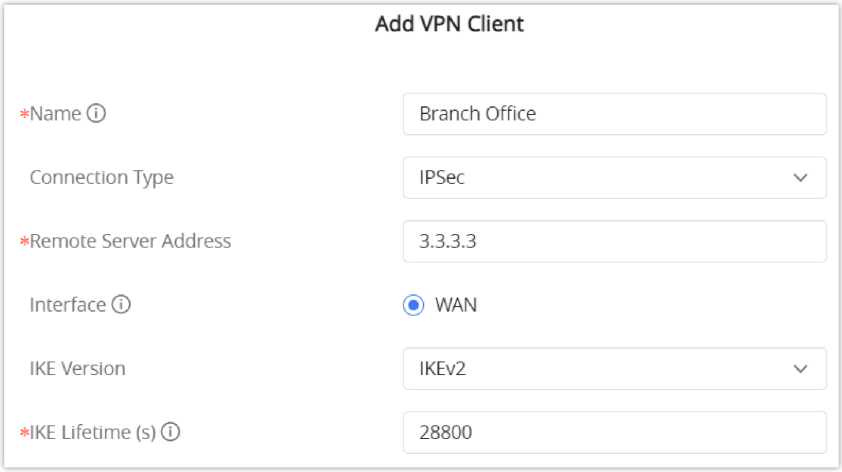
IPSec Site-to-Site

To build an IPSec secure tunnel between two sites located in two distant geographical locations, we can use the sample scenario below:

The branch office router needs to connect to the Headquarters office via an IPSec tunnel, on each side we have a GWN700x router. Users can configure the two devices as follows:

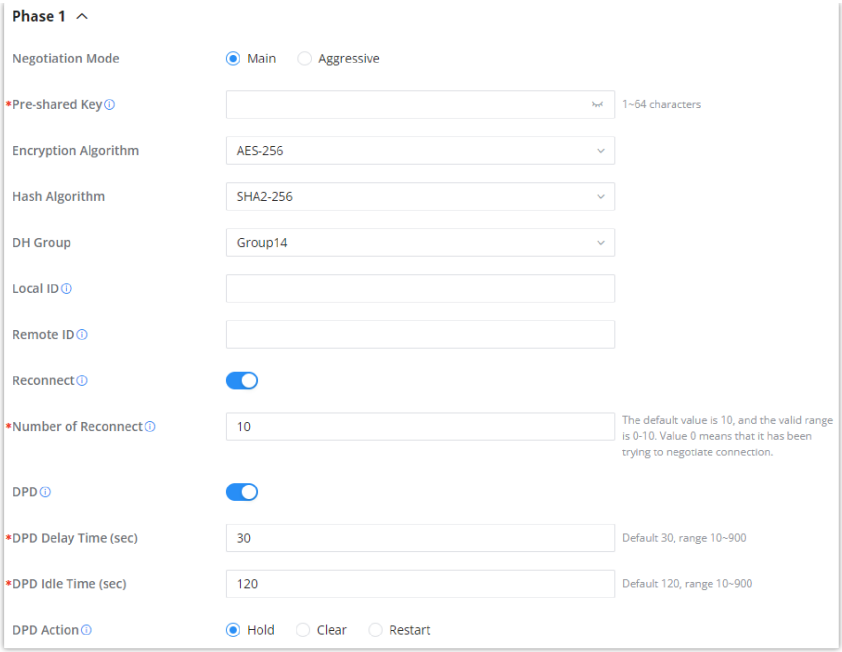
The branch office router runs a LAN subnet 192.168.1.0/24 and the HQ router runs a LAN subnet 192.168.3.0, the public IP of the branch office router is 1.1.1.1 and the IP of the HQ router is 2.2.2.2.

Go under **VPN** → **IPSec** → **Site-to-Site** then click on + Add to add a VPN Client.



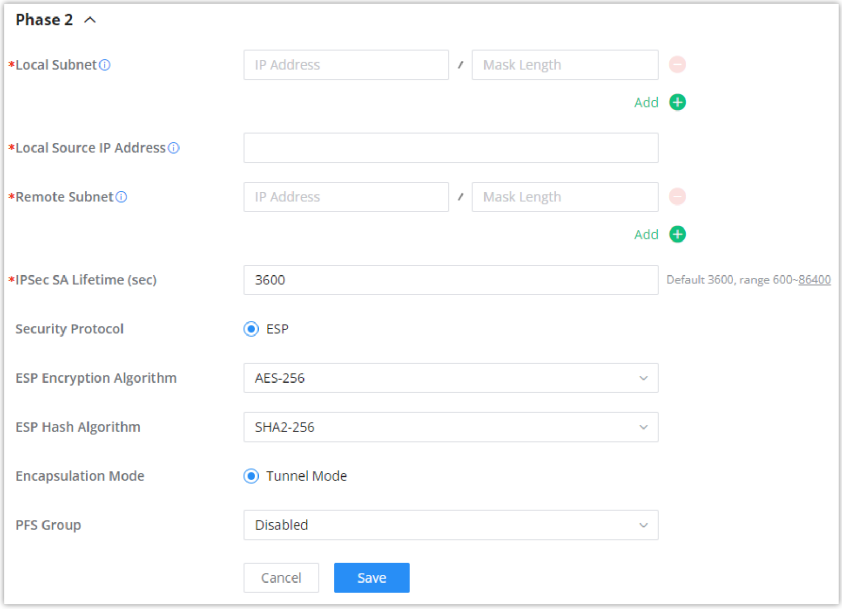
Add VPN Client – IPSec

○ **Phase 1**



Add VPN Client – Phase 1

○ **Phase 2**



Add VPN Client – Phase 2

After this is done, press "Save" and do the same for the HQ Router. The two routers will build the tunnel and the necessary routing information to route traffic through the tunnel back and from the branch office to the HQ network.

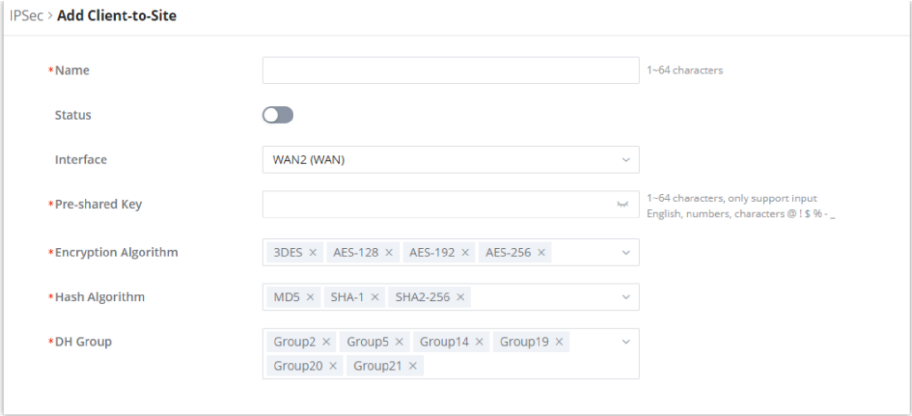
> **Note:**
>
> After the connection is established, the incoming packets from the remote subnet are automatically released, and it is not necessary to manually configure the firewall forwarding rules from WAN to LAN to release traffic.

- **Create the remote user credentials:**

To creates the remote user account which will be required to be entered on the client side and and authenticated on the server side, please refer to the **Remote Users** section.

IPSec Client-to-Site

Go under **VPN** → **IPSec** → **Client-to-Site** then fill in the following information:



Branch Office IPSec Configuration

OpenVPN®

OpenVPN®is a virtual private network solution that offers establishing a secure connection to a distant host, VPN provides the possibility to reach hosts which are located on local area network and be logically located in that same local area network, hence the name Virtual Private Network. The connection between the client and the server is authenticated using username and password or/and TLS encryption.

Typically, users can set a client-to-server connection, the client being a computer, and the server being a GWN router or a GCC device. The user can also set site-to-site VPN connection using OpenVPN® to interconnect two sites securely. In the following sections, you can find explanation for all the configuration fields for OpenVPN®.

OpenVPN® Client

There are two ways to use the GWN700x as an OpenVPN® client:

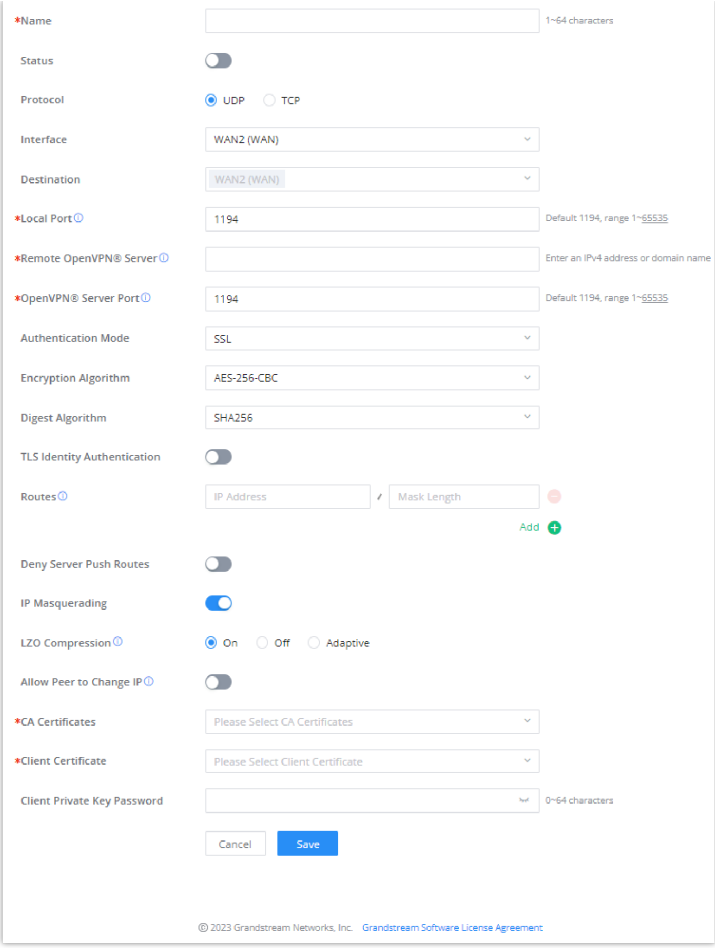
1. Upload client certificate created from an OpenVPN® server to GWN700x.

2. Create client/server certificates on GWN700x and upload the server certificate to the OpenVPN® server.

Go to Go to **VPN** → **OpenVPN®** → **OpenVPN® Clients** and follow the steps below:

Click on 

button. The following window will pop up.



OpenVPN® Client

Click Save after completing all the fields.

Name	Enter a name for the OpenVPN® Client.
Status	Toggle on/off the client account.
Protocol	Specify the transport protocol used. ● **UDP** ● **TCP** **Note:** The default protocol is UDP.
Interface	Select the WAN port to be used by the OpenVPN® client.
Destination	Select the WANs, VLANs and VPNs (clients) destinations that will be used by this OpenVPN® client.
Local Port	Configures the client port for OpenVPN®.The port between the OpenVPN® client and the client or between the client and the server should not be the same.
Remote OpenVPN® Server	Configures the remote OpenVPN® server. Both IP address and domain name are supported.
OpenVPN® Server Port	Configures the remote OpenVPN® server port
Authentication Mode	Choose the authentication mode. ● SSL ● User Authentication ● SSL + User Authentication ● PSK

Encryption Algorithm	Choose the encryption algorithm. The encryption algorithms supported are: ● **DES** ● **RC2-CBC** ● **DES-EDE-CBC** ● **DES-EDE3-CBC** ● **DESX-CBC** ● **BF-CBC** ● **RC2-40-CBC** ● **CAST5-CBC** ● **RC2-64-CBC** ● **AES-128-CBC** ● **AES-192-CBC** ● **AES-256-CBC** ● **SEED-CBC**
Digest Algorithm	Select the digest algorithm. The digest algorithms supported are: ● **MD5** ● **RSA-MD5** ● **SHA1** ● **RSA-SHA1** ● **DSA-SHA1-old** ● **DSA-SHA1** ● **RSA-SHA1-2** ● **DSA** ● **RIPEMD160** ● **RSA-RIPEMD160** ● **MD4** ● **RSA-MD4** ● **ecdsa-with-SHA1** ● **RSA-SHA256** ● **RSA-SHA384** ● **RSA-SHA512** ● **RSA-SHA224** ● **SHA256** ● **SHA384** ● **SHA512** ● **SHA224** ● **whirlpool**
TLS Identity Authentication	Enable TLS identity authentication direction.
TLS Identity Authentication Direction	Select the indentity authentication direction. ● Server: Indentity authentication is performed on the server side. ● Client: Identity authentication is performed on the client side. ● Both: Identity authentication is performed on both sides.
TLS Pre-Shared Key	Enter the TLS pre-shared key.
Routes	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
Deny Server Push Routes	If enabled, client will ignore routes pushed by the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
LZO Compression	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no.

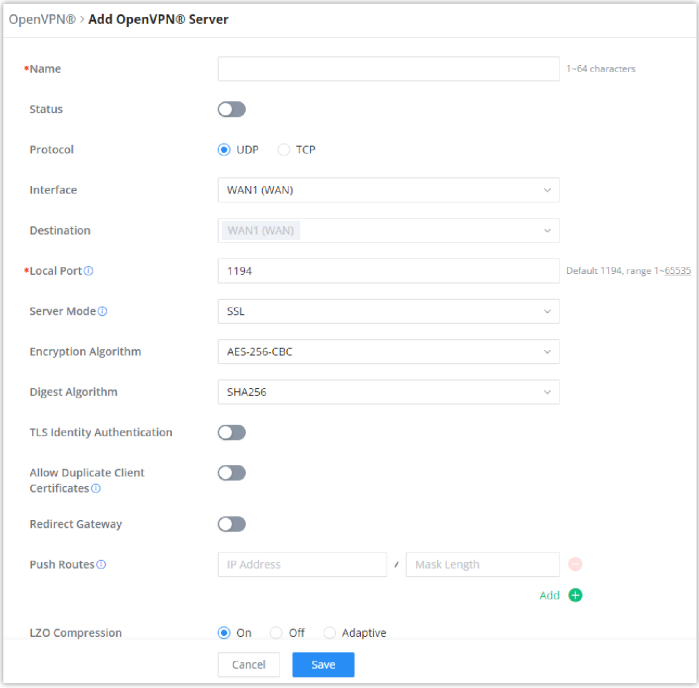
	LZO encoding provides a very high compression ratio with good performance. LZO encoding works especially well for CHAR and VARCHAR columns that store very long character strings.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificates	Click on "Upload" and select the CA certificate Note: This can be generated in System Settings → Certificates → CA Certificate
Client Certificate	Click on "Upload" and select the Client Certificate. Note: This can be generated in System Settings → Certificates → Certificate
Client Private Key Password	Enter the client private key password. Note: This can be configured in VPN → Remote User

OpenVPN® Client

OpenVPN® Server

To use the GWN700x as an OpenVPN® server, you will need to start creating an OpenVPN® certificates and remote users.

To create a new VPN server, navigating under **Web UI → VPN → OpenVPN® page → OpenVPN® Servers tab.**



Create OpenVPN® Server

Click Save after completing all the fields.

Refer to the table below:

Name	Enter a name for the OpenVPN® server.
Status	Toggle ON or OFF to enable or disable the OpenVPN® Server.
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. *The default protocol is **UDP**.*
Interface	Select from the drop-down list the exact interface (WAN).
Destination	Select from the drop-down list the destination (WAN or VLAN).

Local Port	Configure the listening port for OpenVPN® server. *The default value is **1194**.*
Server Mode	Choose the server mode the OpenVPN® server will operate with. 4 modes are available: ● **SSL:** Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). ● **User Authentication:** Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). ● **SSL + User Authentication:** Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. ● **PSK:** Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
TLS Identicy Authentication	This option uses a static **Pre-Shared Key** (**PSK**) that must be generated in advance and shared among all peers. This feature adds extra protection to the **TLS** channel by requiring that incoming packets have a valid signature generated using the PSK key.
TLS Identity Authentication Direction	Select from the drop-down list the direction of TLS Identity Authentication, three options are available **(Server, Client or Both)**.
TLS Pre-Shared Key	If TLS Identicy Authentication is enabled, enter the TLS Pre-Shared Key.
Allow Duplicate Client Certificates	Click on "**ON**" to allow duplicate Client Certificates
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
Push Routes	Specify route(s) to be pushed to all clients. *Example: 10.0.0.1/8*
LZO Compression Algorithm	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificate	Select a generated CA from the dropdown list or add one.
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.
IPv4 Tunnel Network/Mask Length	Enter the network range that the GWN70xx will be serving from to the OpenVPN® client. ***Note:** The network format should be the following 10.0.10.0/16.*

	The mask should be at least 16 bits.

Create OpenVPN® Server

- **Create the remote user credentials:**

To creates the remote user account which will be required to be entered on the client side and and authenticated on the server side, please refer to the **Remote Users** section.

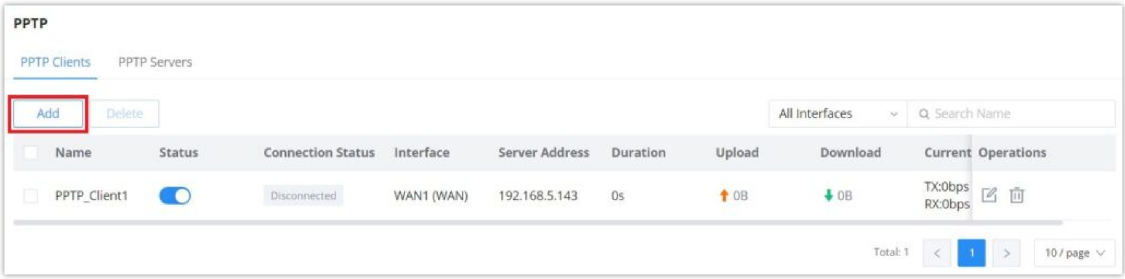
PPTP

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

PPTP Clients

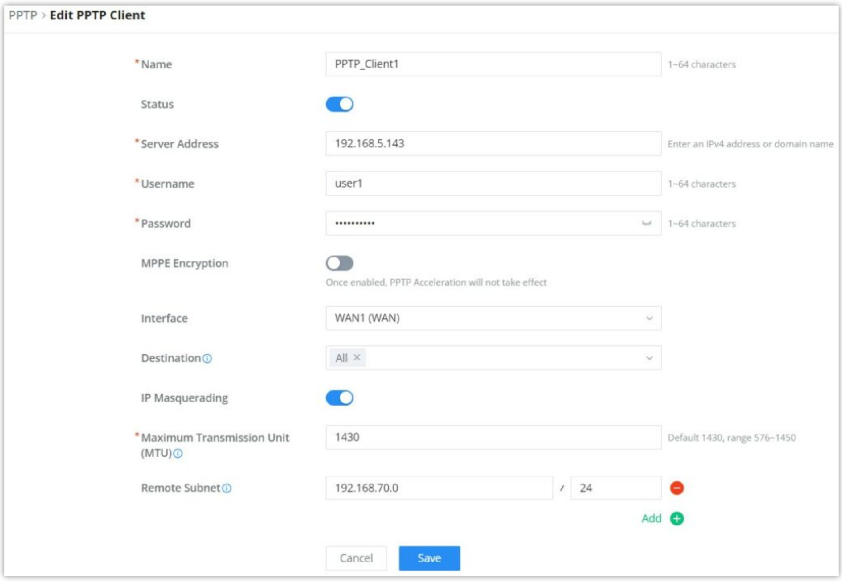
To configure the PPTP client on the GWN700x, navigate under **VPN** → **PPTP** → **PPTP Clients** and set the followings:

1. Click on "**Add**" button.



PPTP page

The following window will pop up.



PPTP Client Configuration

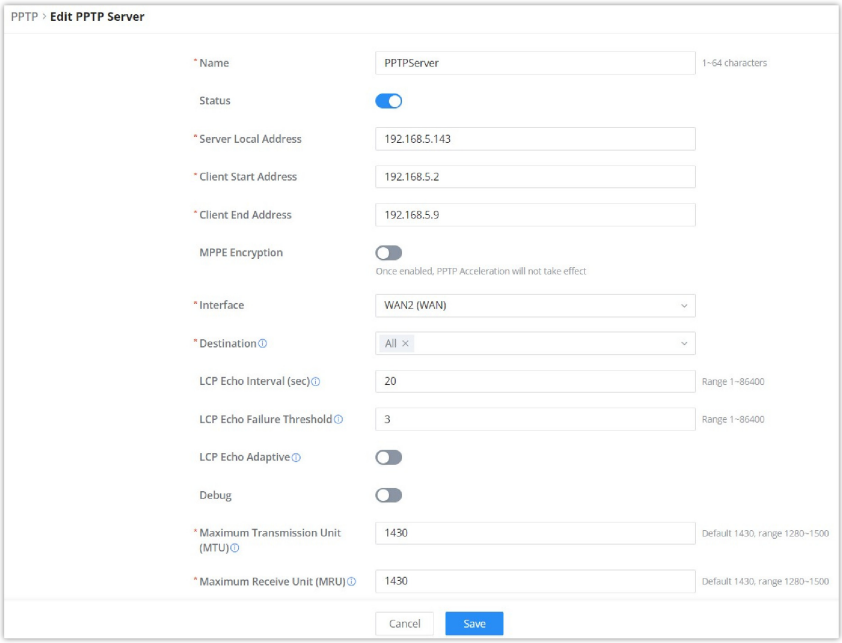
Name	Enter a name for the PPTP client.
Status	Toggle on/off the VPN client account.
Server Address	Enter the IP/Domain of the remote PPTP Server.

Username	Enter the Username for authentication with the VPN Server.
Password	Enter the Password for authentication with the VPN Server.
MPPE Encryption	Enable / disable the MPPE for data encryption. *By default, it's disabled.*
Interface	Choose the interfaces. ***Note:*** *Set forwarding rules in firewall automatically to allow traffic forwarded from VPN to the selected WAN port. If remote device is allowed to access, please set the corresponding forwarding rules in firewall.*
Destination	Choose to which destination group or WAN to allow traffic from the VPN, this will generate automatically a forwarding rule under the menu **Firewall → Traffic Rules → Forward.**
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
Remote Subnet	Configures the remote subnet for the VPN. The format should be "IP/Mask" where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32. ***example:*** *192.168.5.0/24*

PPTP Client Configuration

PPTP Servers

To add a PPTP Server, please navigate to **Web UI → VPN → PPTP page → PPTP Servers tab**, then click on "**Add**" button.



PPTP Sever

Name	Enter a name for the PPTP Server.
Status	Toggle ON or OFF to enable or disable the PPTP Server VPN.
Server Local Address	Specify the server local address

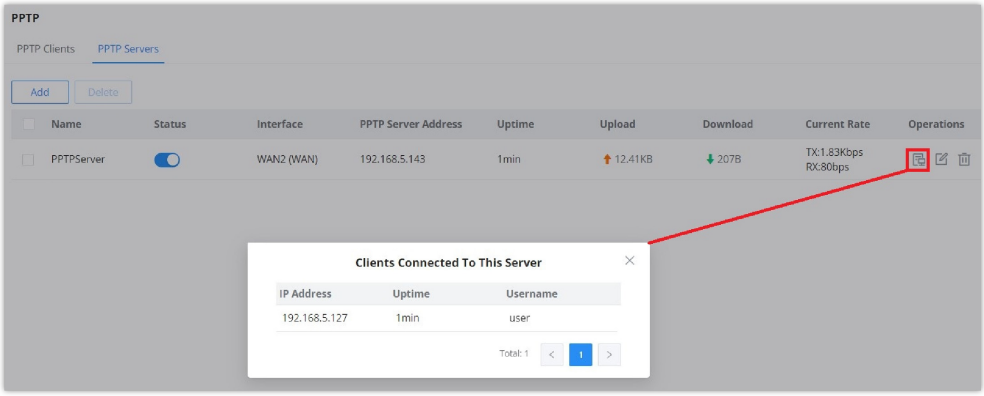
Client Start Address	specify client start IP address
Client End Address	specify client end IP address
MPPE Encryption	Enable / disable the MPPE for data encryption. *By default, it's disabled.*
Interface	Select from the drop-down list the exact interface (WAN port).
Destination	Select the Destination from the drop-down list (WAN or VLAN). ***Note:*** *When selecting "All", subsequent new interfaces will be automatically included.*
LCP Echo Interval (sec)	Configures the LCP echo send interval.
LCP Echo Failure Threshold	Set the maximum number of Echo transfers. If it is not answered within the set request frames, the PPTP server will consider that the peer is disconnected and the connection will be terminated.
LCP Echo Adaptive	• **Once enabled:** LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request. • **Once disabled:** the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval
Debug	Toggle On/Off to enable or disable debug.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.
Maximum Receive Unit (MRU)	MRU indicates the size of the received packets. By default is 1450.
Preferred DNS Server	specify the preferred DNS server. *Ex: 8.8.8.8*
Alternative DNS Server	specify the alternative DNS server. *Ex: 1.1.1.1*

PPTP Sever

- **Create the remote user credentials:**

To creates the remote user account which will be required to be entered on the client side and and authenticated on the server side, please refer to the **Remote Users** section.

To view the clients connected to this server, click on "**Client List**" icon as shown below:

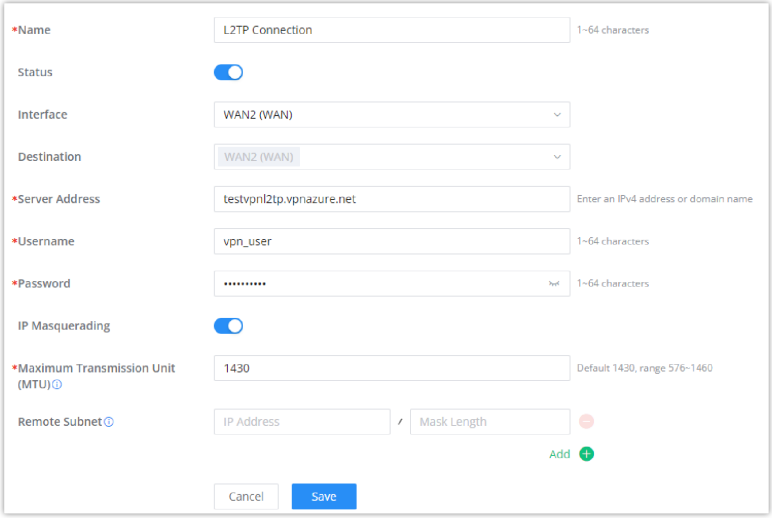


Clients connected to this server

L2TP

To configure the L2TP client on the GWN700x router, navigate under **"VPN → VPN Clients"** and set the followings:

1. Click on + Add button and the following window will pop up.

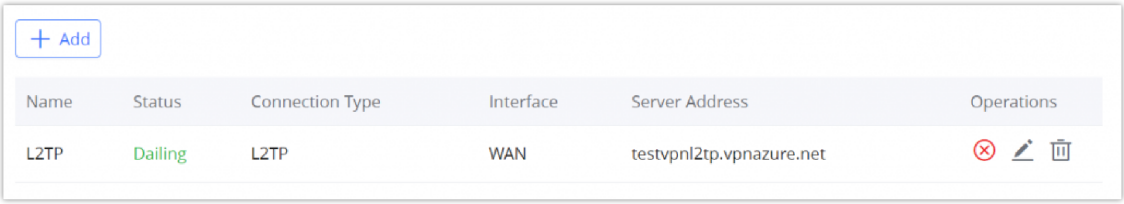


L2TP Client Configuration

Name	Set a name for this VPN tunnel.
Status	Toggle on/off this L2TP account.
Interface	Select the WAN port to be used by VPN.
Destination	Select the WANs, VLANs destinations that will be using this VPN.
Server Address	Enter the VPN IP address or FQDN.
Username	Enter VPN username that has been configured on the server side.
Password	Enter VPN password that has been configured on the server side.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
Remote Subnet	Enter the remote Subnet that has been configured on the server side.

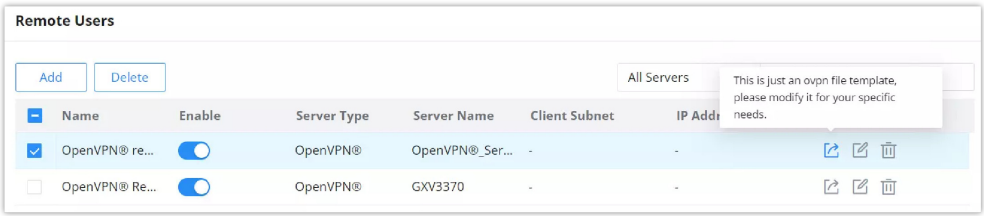
L2TP Client Configuration

Click Save after completing all the fields.



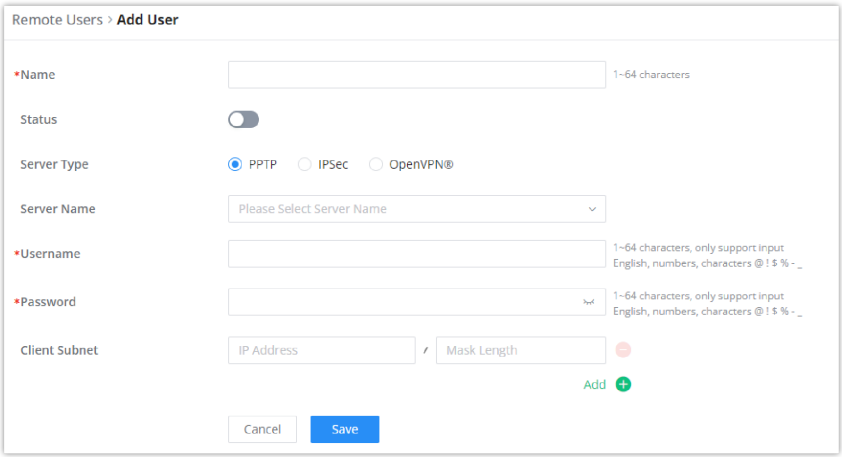
Remote Users

To create the VPN user accounts, please navigate to **VPN** → **Remote Users** then click "**Add**". The account configured will be used for the client to authenticate into the VPN server. The remote client user that can be created in this section is for PPTP, IPSec, and OpenVPN.



VPN Remote Users page

If the remote user is using OpenVPN®, the configuration file can be exported as an `.ovpn` file. This file can then be modified as needed to fit the user's requirements.



Add VPN Remote Users

Name	Enter a name for the user. This name will not be used to log in.
Status	Enable or disable this account.
Server Type	Choose the type of the server. • **PPTP** • **IPSec** • **OpenVPN**
Server Name	Enter the server's name.
Username	Enter the username. This username will be used to log in.
Password	Enter the password.
Client Subnet	Specify the client subnet.

Add VPN Remote Users

To authenticate a remote user into the VPN server successfully, the username and password are used alongside the client certificate. To create a client certificate please refer to Certificates section.

To configure the VPN clients for each VPN server type, please refer to the respective VPN client configuration above.

ROUTING

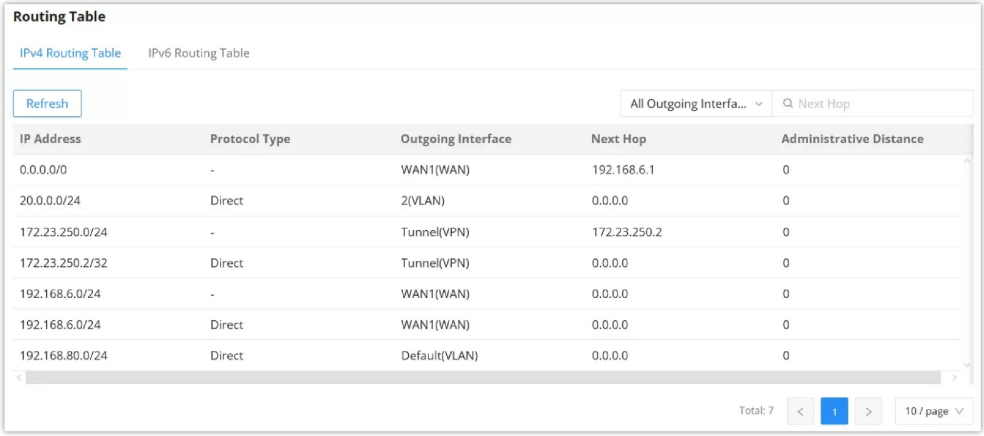
Routing Table

The **Routing Table** page displays the routes currently configured on your Grandstream device. It shows key information such as the IP address, protocol type, outgoing interface, next hop, and administrative distance for each route.

You can toggle between **IPv4 Routing Table** and **IPv6 Routing Table** using the tabs at the top of the page. Additionally, you can filter routes based on outgoing interfaces or search for a specific next hop.

- **IP Address**: The destination network or IP address.
- **Protocol Type**: Indicates the type of routing (e.g., Direct, Static, VPN).
- **Outgoing Interface**: The network interface used for routing traffic to the destination.
- **Next Hop**: The IP address of the next device in the routing path.
- **Administrative Distance**: The trustworthiness of the route.

To view the routing table, navigate to **Routing** → **Routing Table**.



IP Address	Protocol Type	Outgoing Interface	Next Hop	Administrative Distance
0.0.0.0/0	-	WAN1(WAN)	192.168.6.1	0
20.0.0.0/24	Direct	2(VLAN)	0.0.0.0	0
172.23.250.0/24	-	Tunnel(VPN)	172.23.250.2	0
172.23.250.2/32	Direct	Tunnel(VPN)	0.0.0.0	0
192.168.6.0/24	-	WAN1(WAN)	0.0.0.0	0
192.168.6.0/24	Direct	WAN1(WAN)	0.0.0.0	0
192.168.80.0/24	Direct	Default(VLAN)	0.0.0.0	0

Routing Table

Policy Routes

The Policy Routes feature on the GWN700X series allows network administrators to create advanced routing rules to efficiently manage traffic across multiple WAN interfaces. This feature supports three modes: **Load Balancing**, **Backup**, and **Standby**. Each mode serves a unique purpose to enhance network performance, ensure uninterrupted connectivity, and provide granular control over traffic distribution. These policies can be applied to specific VLANs for tailored traffic management.

> **Note:**
>
> It is also possible to implement load balancing, backup, and standby between WAN and VPN interfaces.

Policy Pool

To create a policy pool rule, follow these steps:

1. Navigate to **Routing** → **Policy Routes** in the web interface.
2. Open the **Policy Pool** tab.
3. Click the **Add** button to create a new rule.
4. Select the desired mode:
   - **Load Balance**
   - **Backup**
   - **Standby**
5. Assign the **Preferred Interface(s)** and configure their **Weight** values (1–10).

> **Note:**
>
> For the Weight: The default is 1 and value can be from 1~10 with 10 being the highest weight.

6. (Optional) Assign **Alternate Interface(s)** for **Backup** mode or **Standby Interface** for **Standby** mode.

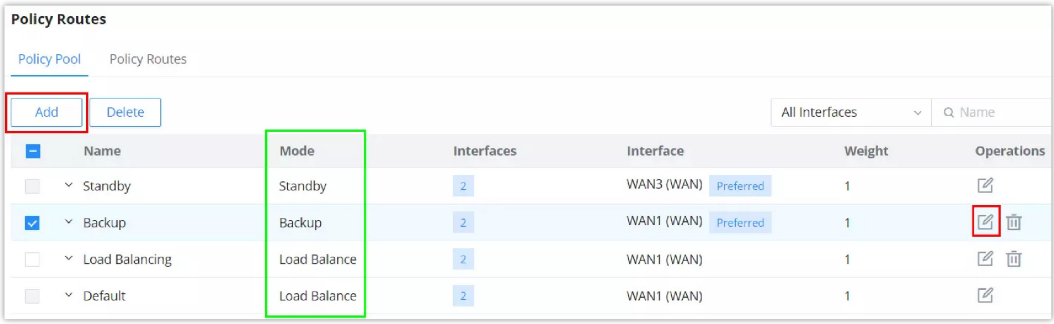
Note:

The number of WAN ports depends on GWN router model.

7. Save the configuration.

Key Details:

- You can configure these routes with either WAN or VPN interfaces.
- Once created, a policy pool can be applied to specific VLANs, enabling precise traffic management per VLAN.

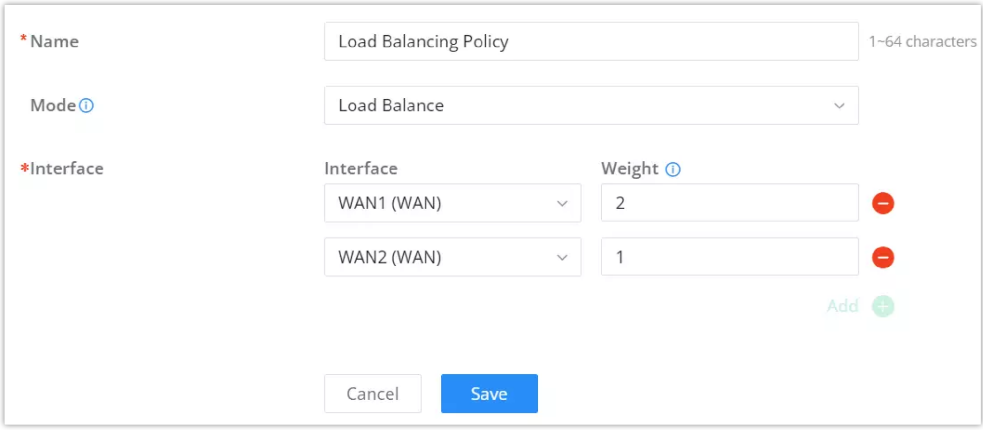


Policy Pool page

Load Balance Mode

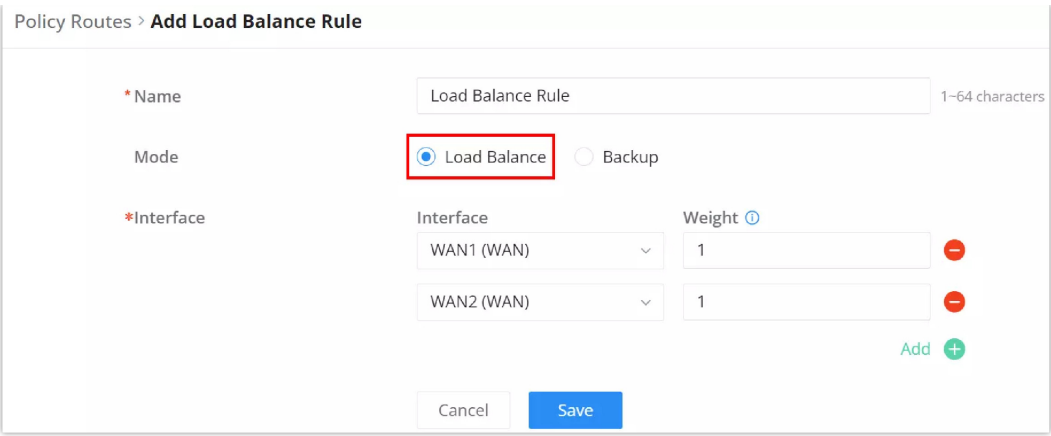
- **Purpose**: Distribute traffic evenly or proportionally across multiple WAN interfaces based on bandwidth capacity or network requirements.
- **How It Works**:
  - Configure weights for each WAN interface. For instance, if two WAN ports have weights of 1 and 2, traffic will be divided in a **1:2 ratio**. Similarly, setting weights to 1 and 1 will evenly distribute traffic in a **1:1 ratio** across both WAN interfaces.
  - Suitable for scenarios where bandwidth optimization and redundancy are required.
- **Advantages**:
  - Efficiently uses all available bandwidth.
  - Provides redundancy across multiple WAN connections.

Example 1: If you have WAN1 (100 Mbps) and WAN2 (50 Mbps), set weights as 2 and 1, respectively, to ensure balanced utilization proportional to bandwidth.



Load Balance mode – Example 1

Example 2: If you have WAN1 (100 Mbps) and WAN2 (100 Mbps), set their weights to 1 and 1, respectively, to ensure balanced utilization proportional to their bandwidth. In this configuration, the bandwidth will be evenly distributed between the two connections.



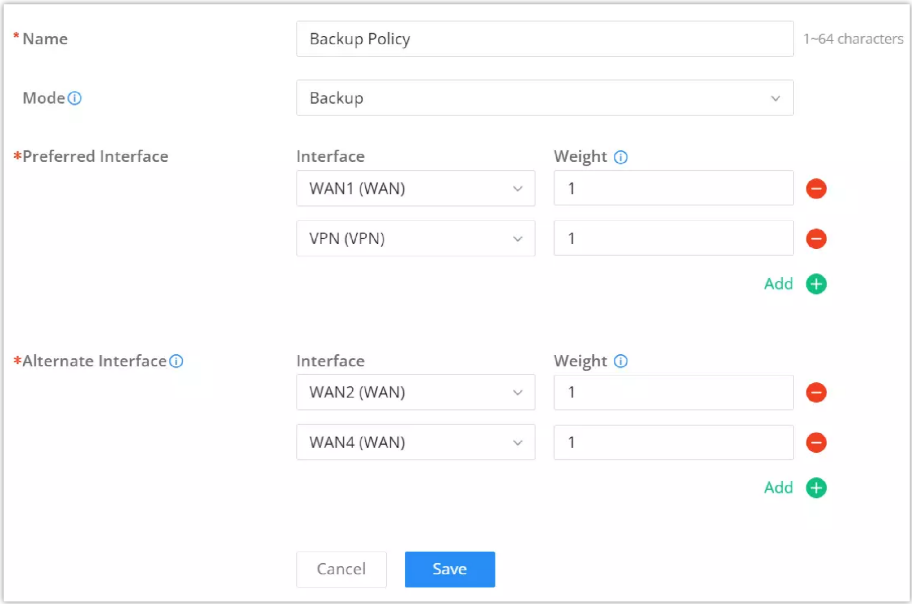
Load Balance Rule – Example 2

Backup Mode

- **Purpose**: Provide failover support by routing traffic to alternate interfaces when all preferred WAN interfaces fails.
- **How It Works**:
  - In backup mode, the backup interfaces remain active and ready to handle traffic if a failure is detected **on all preferred interfaces**. However, the alternate interfaces only become active when all preferred interfaces are down. Once activated, traffic is distributed across the alternate interfaces based on their assigned weights.
  - The status of the interfaces is monitored using ICMP replies to a tracking IP, which determines when the interface is up or down. For more details, refer to the WAN section. If the preferred interfaces come back online, traffic will revert to the primary interface after five consecutive tracking intervals (typically 60 seconds).
- **Key Features**:
  - Backup interfaces are always active.
  - Traffic can be distributed proportionally between preferred and backup interfaces if weights are configured.

Example:

If both the preferred interfaces, **WAN1 and VPN**, are down, only then will the alternate interfaces, **WAN2 and WAN4**, become active, with traffic distributed according to their assigned weights.



Policy Pool – Backup mode

Standby Mode

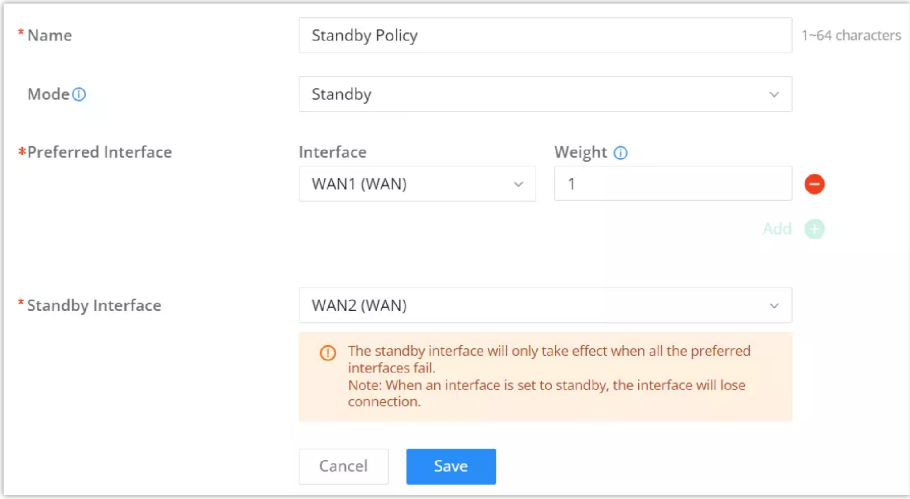
- **Purpose**: maintain a **single standby interface**, which is only activated when **all the primary interfaces fail**. This is especially useful in cases like PPPoE authentication conflicts, where multiple active sessions can cause issues.

- **How It Works**:
  - The standby interface remains inactive until all preferred (primary) interfaces fail. A Tracking IP Address (such as 1.1.1.1 or 8.8.8.8) is configured to monitor the status of the primary interface. The router pings this IP to check if the primary interface is up or down. If the pings fail continuously, the router switches to the standby interface.
  - For PPPoE, authentication occurs only when the standby interface is activated, preventing simultaneous session conflicts.
  - Failback occurs when the primary interface recovers, after five consecutive successful tracking intervals (typically 60 seconds) where the router pings a configured Tracking IP Address to check if the interface is back online. For PPPoE, failback may take up to 400 seconds due to session lock delays and the time required for PPPoE authentication to complete.

- **Key Features**:
  - Standby interface remains inactive to conserve resources, activating only when needed.
  - Resolves PPPoE authentication conflicts when the same account is configured across multiple WAN ports.
  - Ensures smooth failback after the primary interface recovers, with an extended failback period for PPPoE sessions.

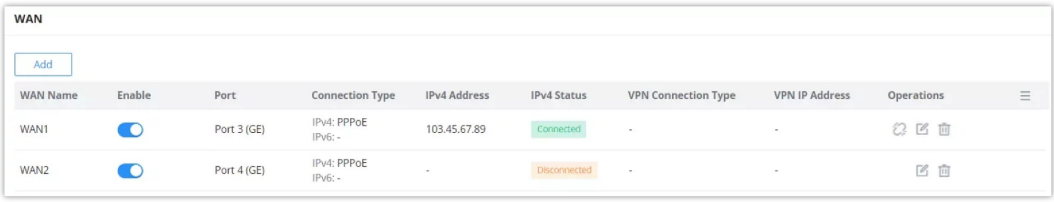
Example:

Use Standby Mode when two WAN ports require PPPoE with the same ISP credentials to prevent conflicts and maintain redundancy. For instance, WAN2 will store the PPPoE credentials but remain inactive. If WAN1, using the same credentials, fails or goes offline for any reason, WAN2 will automatically authenticate with the saved credentials and activate, ensuring seamless connectivity.



Policy Pool – Standby mode

Since **WAN2** is on **Standby**, it will not establish a connection until **WAN1** goes down or fails to connect.



WAN page – GWN700x

Comparison Table

Feature/Mode	Load Balancing	Backup Mode	Standby Mode
Purpose	Distribute traffic across **multiple interfaces.**	Failover with **active backup**.	Failover with **inactive standby**.

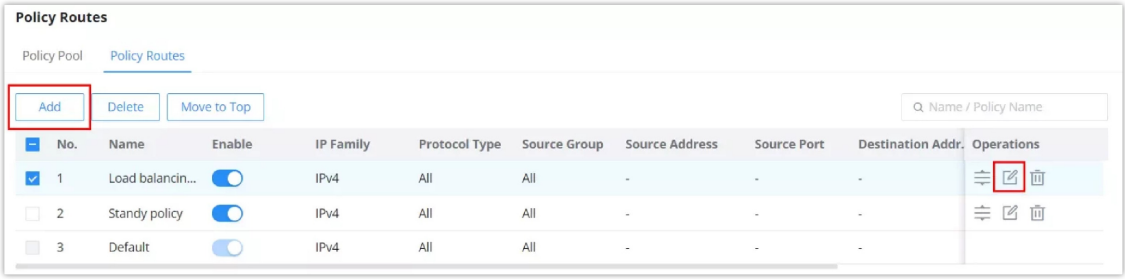
Feature/Mode	Load Balancing	Backup Mode	Standby Mode
Traffic Behavior	Balanced based on weights (Ratio).	When all preferred interfaces fail or become unavailable, the alternate interfaces will automatically take over. Traffic will be distributed proportionally between the alternate interfaces based on their configured weights, ensuring seamless failover	Activate the standby interface only when all preferred interfaces have failed**.**
Resource Usage	Utilizes all interfaces actively.	Backup interfaces are always active, and more than one interface can be configured as a backup.	The standby interface remains inactive, and only one interface can be designated as standby.

Policy Routes Modes Comparison

Policy Route

On the second tab (Policy Routes), the user can specify which Networks (VLAN) can use which Load Balance rule (must be created first), also the user can specify the protocol type, source and destination IP and even assign a schedule for it.

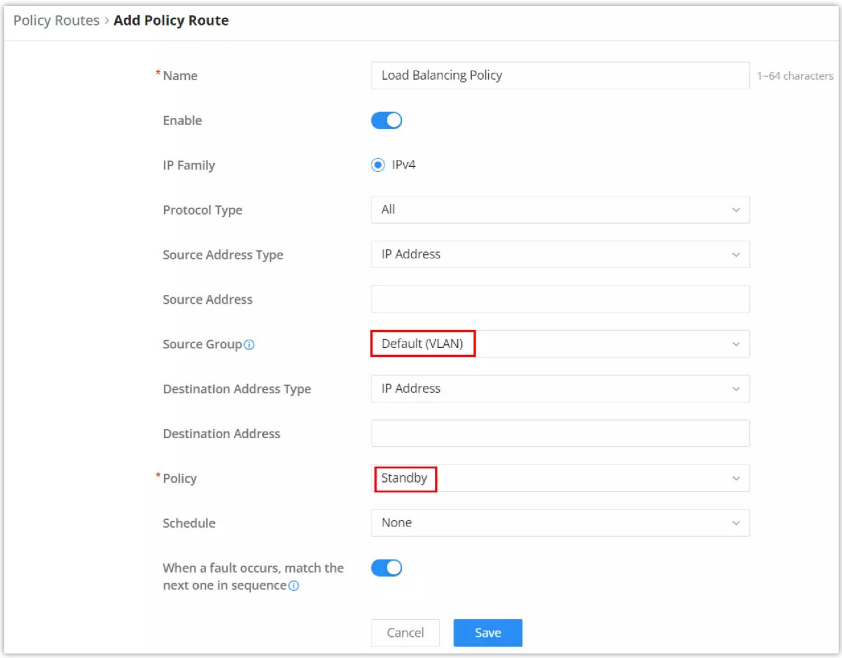
To create a Policy Route, please navigate to **Routing → Policy Routes page → Policy Routes tab**, then click on "**Add**" button to click on "**edit icon**" to edit as shown below:



Policy Routes page

Note:

When creating multiple policy routes, the order from top to bottom determines priority. Rules with lower numbers (No.) have higher priority. Users can also move a rule to the top by selecting it and clicking the 'Move to Top' button, giving it the highest priority within the list.



Add Policy Route

Note:

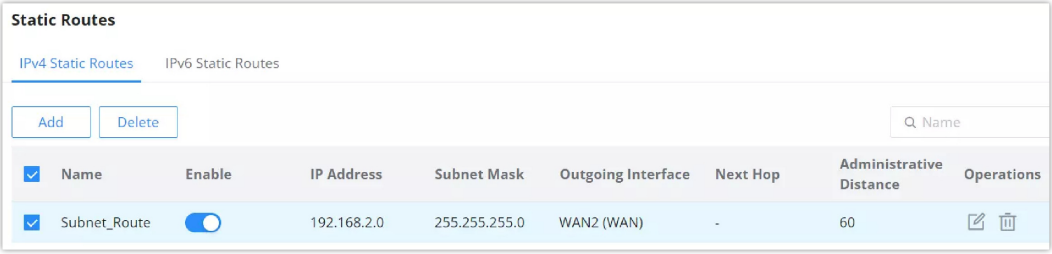
If the Source and Destination IP address field left empty, the policy route will take any IP address.

Static Routes

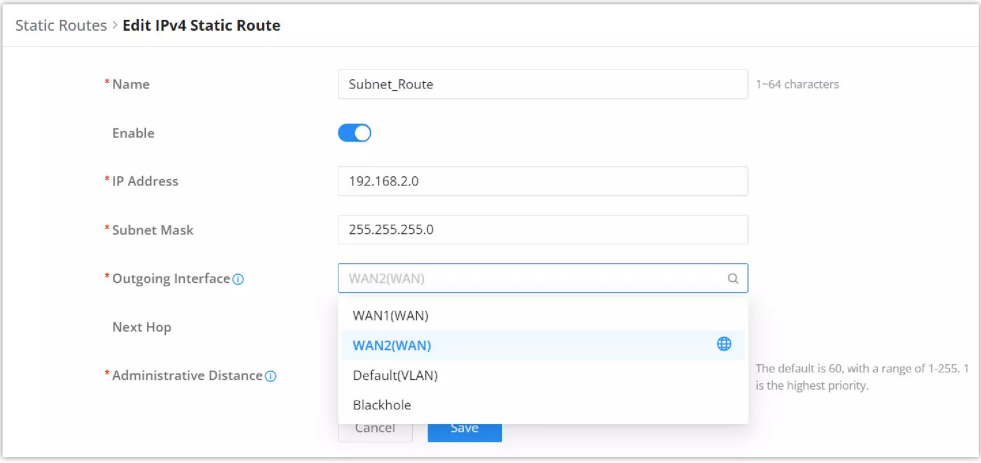
Static routing allows administrators to manually define routing paths instead of relying on dynamic routing protocols. This method is ideal for services requiring a consistent, unchanging route.

The **GWN700x** supports manual configuration of both IPv4 and IPv6 static routes, accessible through the Web GUI by navigating to **Routing** → **Static Routes**.

To add a new static route, click on the **Add** button and complete the necessary fields as described.



Static Routing Page



Add IPv4 Static Routing

Name	Assign a name for the route, such as 'Subnet_Route'.
Enable	Toggle this on to activate the route.
IP Address	Enter the destination network, e.g., 192.168.2.0.
Subnet Mask	Specify the subnet mask, e.g., 255.255.255.0.
Outgoing Interface	Select the interface the router should use for this route. For example, WAN1 for internet-bound traffic, or Blackhole to discard traffic to this destination.
Next Hop	Enter the IP address of the next router in the path to the destination network, if required.
Administrative Distance	Set a priority level for this route. Lower values indicate higher priority (default is 60). Use a lower value if you want this route to take precedence.

Add IPv4 Static Routing

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic routing protocol used in IP networks to determine the best path for data packets across the network. In Grandstream GWN routers, OSPF allows for efficient routing across large and complex networks by exchanging routing information between routers, ensuring each router knows the most optimal path to various network destinations.

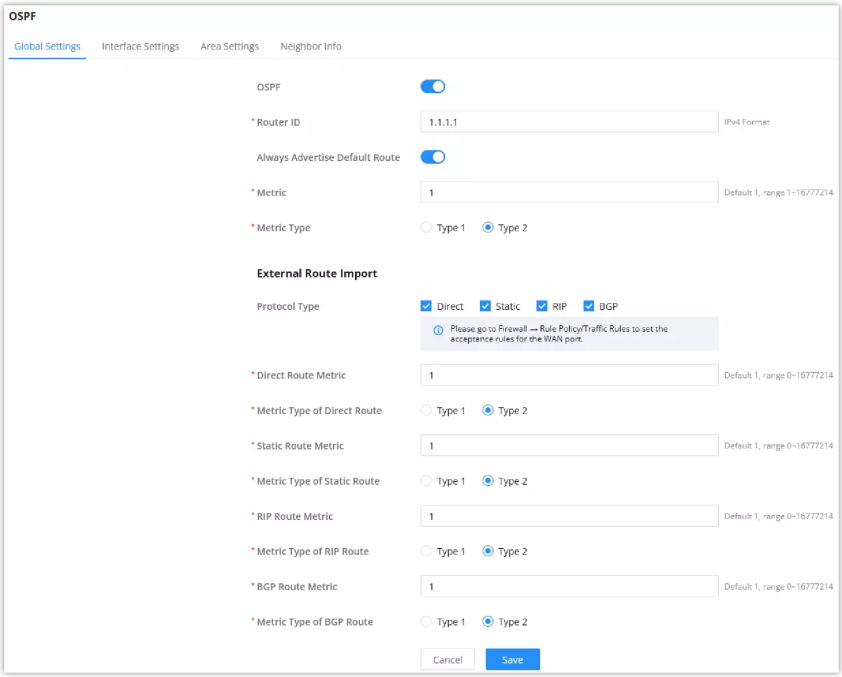
The GWN routers support a robust OSPF configuration to provide flexibility, security, and scalability for enterprise-level networks. OSPF is designed to work within an Autonomous System (AS), ensuring fast convergence and optimal routing decisions based on link state information.

To view or configure OSPF settings, navigate to **Routing → OSPF.**

Global Settings

The **Global Settings** tab contains important configurations to enable and fine-tune OSPF on your Grandstream GWN router. Some of the key options on this page include:

- **Router ID**: This field defines a unique IPv4 address that identifies your router within the OSPF network. It must be set for the router to participate in OSPF.
- **Always Advertise Default Route**: This toggle ensures that the router always advertises the default route (0.0.0.0/0) to other routers in the OSPF network, designating it as a gateway.
- **Metric**: The metric determines the cost of a route in OSPF. Lower values indicate a more preferred route, guiding the OSPF protocol in route selection.
- **Metric Type**: You can choose between:
  - **Type 1**: Considers both the OSPF metric and other route costs.
  - **Type 2**: Considers only the OSPF metric, typically used for external routes.
- **External Route Import**: This section allows you to import routes from other routing protocols such as **Direct**, **Static**, **RIP**, and **BGP**, giving you flexibility when integrating with different network setups.



OSPF – Global Settings

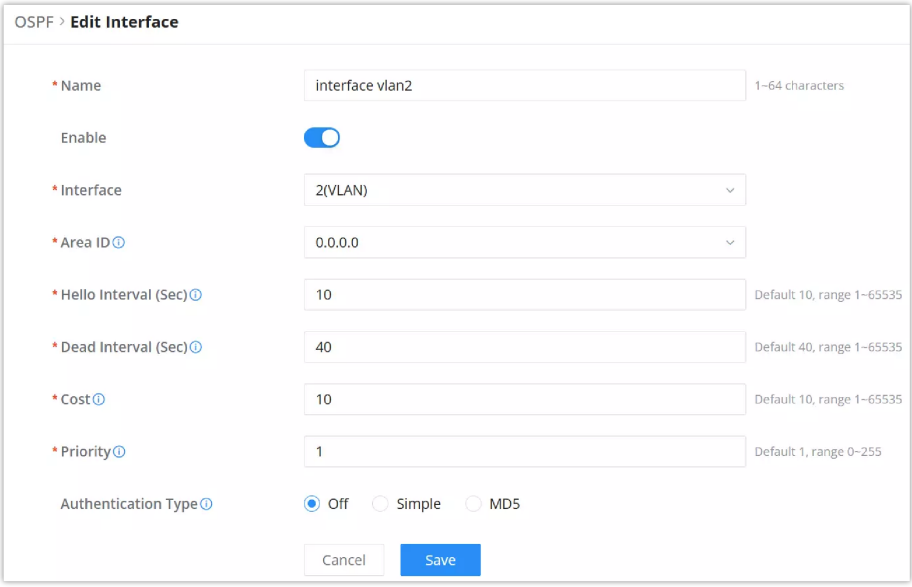
Interface Settings

In this section, users can view, add, or modify OSPF configurations for each interface on the device. The interface settings allow fine-tuning of OSPF behavior by defining key parameters like intervals for OSPF hello packets, authentication types, and the cost metric for each interface.

To navigate: **Routing** → **OSPF** → **Interface Settings**

OSPF – Interface Settings page

To add a new OSPF interface, they can click on the **Add** button. To edit an existing interface, click on the **Edit** icon next to the interface. Refer to the images for a visual guide.



OSPF – Add/Edit Interface Settings

Key Configurations:

- **Name**: A customizable label for the interface.
- **Enable**: Toggle to enable or disable OSPF for this interface.
- **Interface**: Select the specific interface (e.g., VLAN) where OSPF should run.
- **Area ID**: Identifies the OSPF area the interface belongs to (default: `0.0.0.0` for backbone).
- **Hello Interval (Sec)**: The interval between OSPF Hello packets to maintain neighbor relationships (default: 10 seconds).
- **Dead Interval (Sec)**: The interval after which a neighbor is considered down if no Hello packet is received (default: 40 seconds).
- **Cost**: Determines the OSPF route cost; lower values are preferred.
- **Priority**: Controls the interface's eligibility to become the Designated Router (DR).
- **Authentication Type**: Choose between **No Authentication**, **Simple Password**, or **MD5 Authentication** for OSPF packets.

These configurations help ensure optimal routing behavior and secure communication between OSPF-enabled devices.

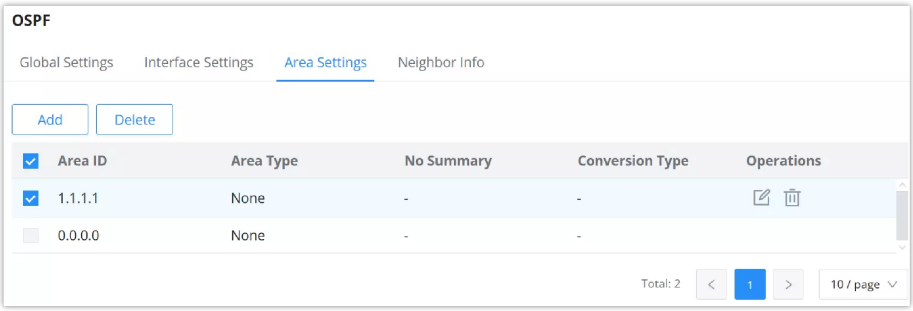
Area Settings

The OSPF **Area Settings** tab allows users to configure OSPF areas to optimize routing and control traffic within different network zones. This section is essential for network segmentation and ensuring efficient routing within the Open Shortest Path First (OSPF) protocol in Grandstream GWN routers. OSPF divides networks into multiple areas to decrease routing overhead and enhance scalability.

To navigate to this page, go to **Routing** → **OSPF** → **Area Settings**.

To Add or Edit an Area:

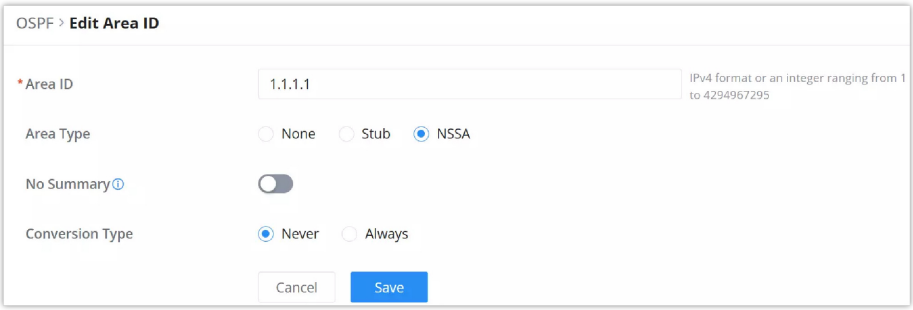
- Click the **Add** button to create a new area.
- Click the **Edit** icon next to an existing area to modify its configuration.



OSPF – Area Settings page

Key Configurations in Area Settings:

- **Area ID**: A unique identifier for the OSPF area, defined in IPv4 format or an integer.
- **Area Type**: Options include:
  - **None**: No special designation for the area.
  - **Stub**: Restricts external route advertisements to minimize routing overhead.
  - **NSSA (Not-So-Stubby Area)**: Balances between a stub and full OSPF area by allowing specific external routes.
- **No Summary**: Prevents summarized routes from being sent into the area, promoting more specific routing information.
- **Conversion Type**: Manages area type conversions:
  - **Never**: Disables conversion.
  - **Always**: Enables automatic conversion.



OSPF – Add/Edit Area Settings

Neighbor Info

The **Neighbor Info** tab provides a summary of neighboring OSPF routers that have formed adjacencies with your Grandstream GWN router. This feature helps monitor OSPF neighbor relationships and troubleshoot connectivity between routers in a network running OSPF.

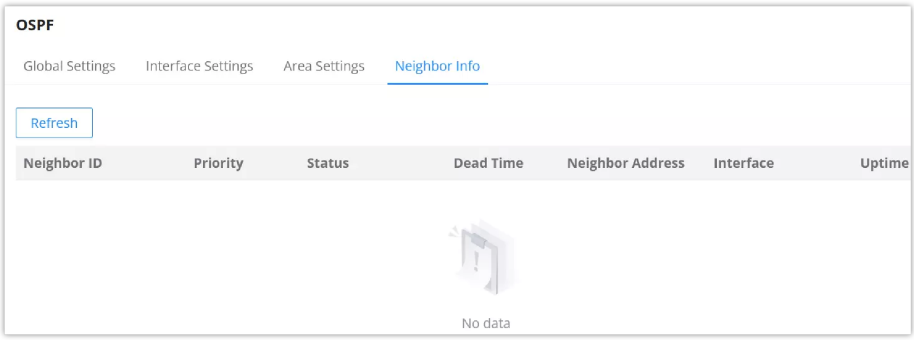
To view this information, navigate to **Routing** → **OSPF** → **Neighbor Info**.

Key Parameters Displayed in Neighbor Info

- **Neighbor ID**: The unique identifier of the neighboring router.
- **Priority**: Indicates the priority value of the neighbor, which helps in determining the designated router (DR) and backup designated router (BDR).
- **Status**: Shows the current state of the OSPF neighbor (e.g., Full, Init, 2-Way).
- **Dead Time**: The countdown before the neighbor is considered down, based on the Hello interval.
- **Neighbor Address**: The IP address of the neighbor.
- **Interface**: The interface on your router that is communicating with the neighbor.

- **Uptime**: The amount of time the OSPF neighbor relationship has been established.

This tab helps monitor OSPF relationships in real-time and identify potential routing issues.



OSPF – Neighbor Info

RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol used by routers to exchange routing information within a local network or across networks. In Grandstream GWN routers, RIP allows the configuration of both RIP Version 1 (RIPv1) and RIP Version 2 (RIPv2) to determine how routers communicate route information, maintain updated routing tables, and ensure efficient network management.

The **RIP** section is divided into four main tabs:

1. **Global Settings**
2. **Interface Settings**
3. **Route Advertisement**
4. **Neighbor Info**

Each tab provides specific configurations for setting up and managing RIP routing on your network.

RIP – Global Settings

The **Global Settings** tab is where the general RIP configuration is defined. You can enable RIP, choose the RIP version, and configure important parameters such as RIP Distance, Timers, and External Route Import options.

To navigate to this section: Go to **Routing** → **RIP** → **Global Settings**.

- **RIP**: Toggle to enable or disable RIP on the router.
- **RIP Version**:
  - **RIPv1**: Basic, classful routing protocol, no subnet information.
  - **RIPv2**: Classless routing protocol with subnet and route tags support.
- **RIP Distance**: Specifies the administrative distance for RIP routes, which helps in determining the reliability of the route (default is 120).
- **Always Advertise Default Route**: When enabled, the router will always advertise a default route to other routers.

Timer Configuration:

- **Update Timer**: The interval (in seconds) between route update messages.
- **Invalid Timer**: The duration (in seconds) after which a route is considered invalid if no update has been received.
- **Garbage Collection Timer**: The time after which an invalid route is removed from the routing table.

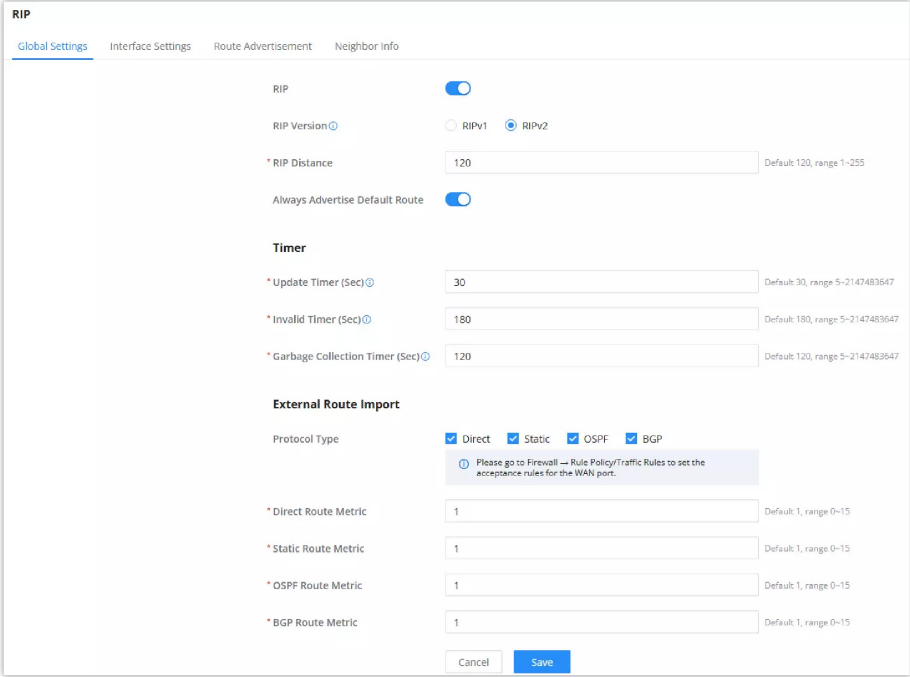
External Route Import:

You can configure the router to import external routes from the following sources:

- **Direct Routes**

- **Static Routes**
- **OSPF Routes**
- **BGP Routes**

For each protocol type, you can configure the metric values that affect the priority of the route.



RIP – Global Settings

RIP – Interface Settings

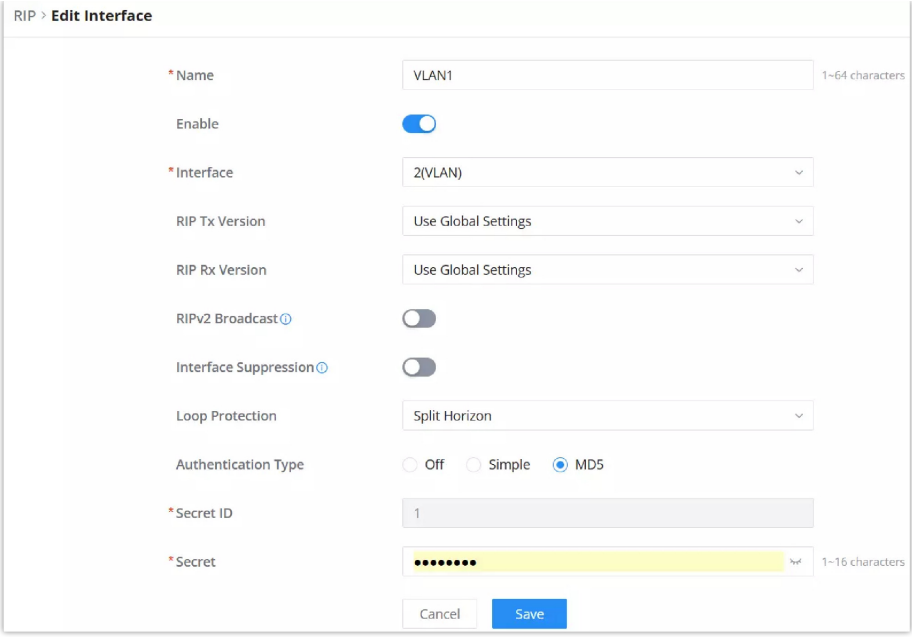
The **RIP Interface Settings** tab allows users to configure RIP interfaces on the GWN router. It displays a list of interfaces that can participate in the RIP routing protocol. Users can manage settings like the RIP version used for transmitting and receiving, authentication types, and other advanced options for RIP routing.

To add an interface, click the **Add** button, or to edit an interface, click the **edit icon**. See the provided images for visual guidance.

RIP – Interface Settings

Key Parameters:

- **Interface**: Specifies the interface that RIP will run on (e.g., VLAN, physical interface).
- **RIP Tx Version / RIP Rx Version**: Select the RIP version for transmitting and receiving routes.
- **RIPv2 Broadcast**: Enable/disable broadcasting RIP version 2 messages.
- **Interface Suppression**: Suppresses sending RIP updates on the interface.
- **Loop Protection**: Protects from routing loops using the **Split Horizon** method.
- **Authentication Type**: Choose the type of authentication for RIP (e.g., **MD5**).
- **Secret**: Authentication key (password) for MD5 or simple authentication.

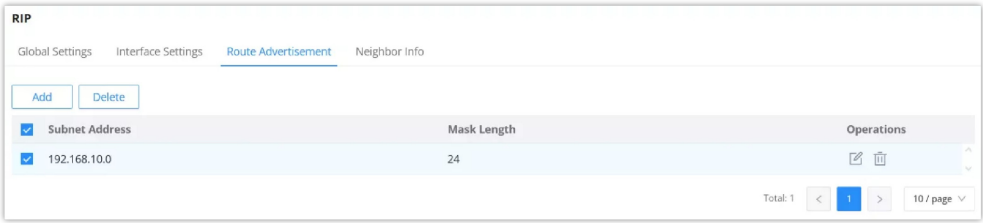


RIP – Add/Edit interface

RIP – Route Advertisement

The **Route Advertisement** tab in the RIP section allows users to define specific routes that need to be advertised to other routers in the network. This is essential for controlling which sub-networks are shared across the RIP protocol. Proper route advertisement ensures efficient routing and network management by determining what parts of the network can be reached through the RIP-enabled router.

Navigation: To view or modify Route Advertisement settings, navigate to **Routing** → **RIP** → **Route Advertisement**.

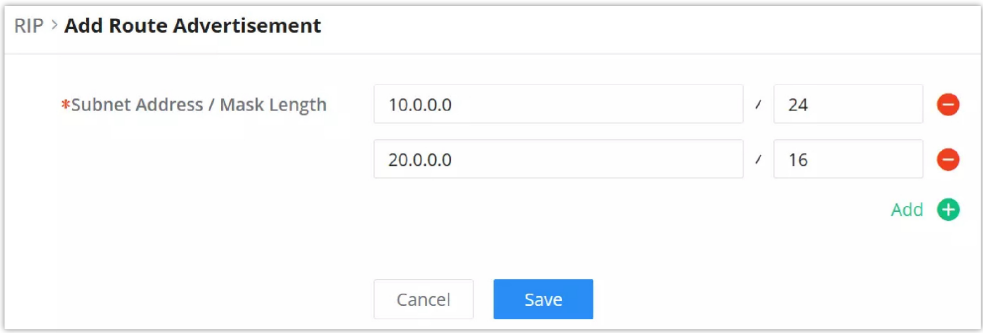


RIP – Route Advertisement

Key Features in the Route Advertisement Tab:

- **Subnet Address / Mask Length**: Displays the list of subnets being advertised along with their corresponding subnet mask lengths.
- **Add Route Advertisement**: This feature allows users to add one or more subnets to advertise across the network. When adding, users need to provide both the **Subnet Address** and the **Mask Length** (e.g., `/24` for Class C networks).
- **Operations**: Each route entry has options to edit or delete the advertisement.

If the user wishes to add a new route advertisement, they can click on the **Add** button and provide the required subnet address and mask length. Once configured, these routes will be shared across the network via RIP.



RIP – Add Route Advertisement

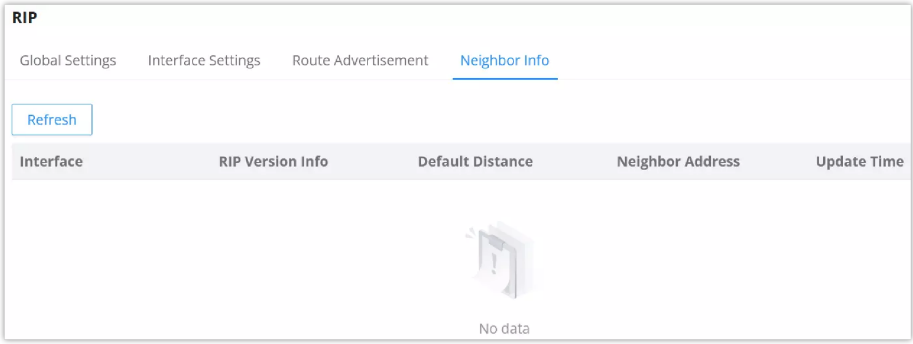
RIP – Neighbor Info

The **Neighbor Info** tab in the RIP configuration provides details about the neighboring RIP routers that communicate with the router to exchange routing information. This tab displays crucial information regarding the neighbors, which helps in managing and troubleshooting RIP routing within the network.

Navigation: To view RIP neighbor details, navigate to **Routing** → **RIP** → **Neighbor Info**.

Key Information Displayed:

- **Interface**: The network interface that is communicating with the neighbor router.
- **RIP Version Info**: Displays the version of RIP used by the neighbor router.
- **Default Distance**: Indicates the default administrative distance for the neighbor.
- **Neighbor Address**: The IP address of the neighboring RIP router.
- **Update Time**: The last time an update was received from the neighboring router.



RIP – Neighbor Info

Border Gateway Protocol (BGP)

The **Border Gateway Protocol (BGP)** is a key exterior gateway routing protocol used to exchange routing information between different autonomous systems (AS) over the internet. BGP plays a critical role in determining the best path for data packets as they travel across various networks. On Grandstream GWN routers, BGP is configured under the **Routing** section, offering a powerful solution for network administrators to control traffic between different AS networks.

To configure BGP on Grandstream routers, navigate to **Routing** → **BGP**.

BGP – Global Settings

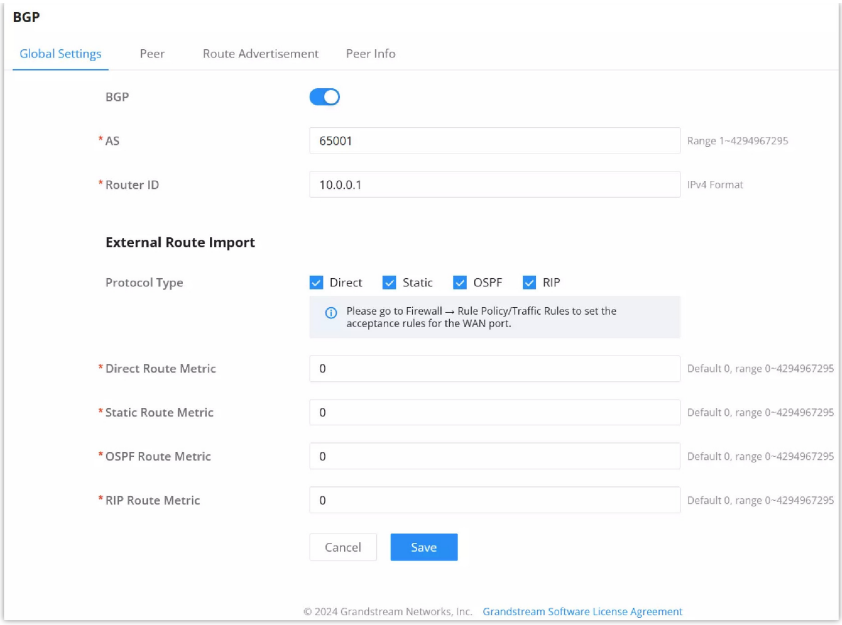
The **Global Settings** tab in BGP configuration allows the user to define the general BGP parameters essential for the protocol's operation.

Key Parameters:

- **AS (Autonomous System)**: The AS number identifies the autonomous system to which the router belongs. It is a required value with a valid range from 1 to 4,294,967,295.
- **Router ID**: A unique identifier in IPv4 format for the router. The router ID is required and helps identify this router in the BGP network.

External Route Import:

- This section allows users to configure which route types (Direct, Static, OSPF, and RIP) can be imported into the BGP routing table.
- **Protocol Type**: You can check the boxes for the route types to import, and set their respective route metrics, which determine the preference for routes. Lower metric values have higher preference.



BGP – Global Settings

Important Firewall Configuration Note:

For BGP to function correctly, it is essential to configure the firewall to allow communication on TCP port 179. Go to Firewall → Rule Policy/Traffic Rules and set rules that permit traffic on this port for the WAN interface. Without this configuration, subnets will be unable to communicate across BGP peers, preventing proper route exchange and connectivity between networks. This step is crucial for establishing a stable BGP connection and enabling subnet communication between autonomous systems.

BGP – Peer

In the BGP (Border Gateway Protocol) Peer tab, users can view, add, or edit BGP peers that are configured on the router. A BGP peer is a neighboring router with which routing information is exchanged. Peers are established through their IP address and ASN (Autonomous System Number).

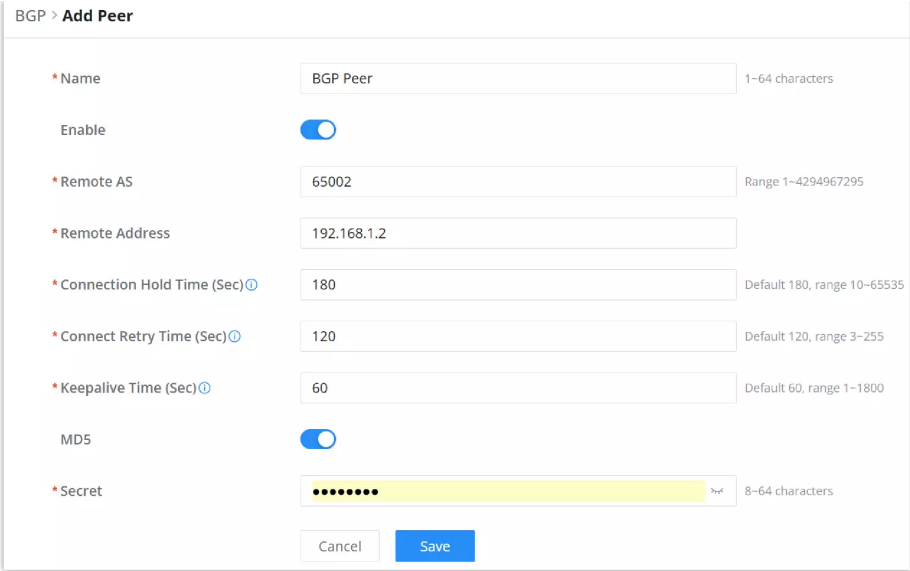
To add or modify a BGP peer:

- Click on the **Add** button to create a new peer.
- To modify an existing peer, click the **Edit** icon next to the peer you want to change.

BGP – Peer page

Key configurable fields in this tab include:

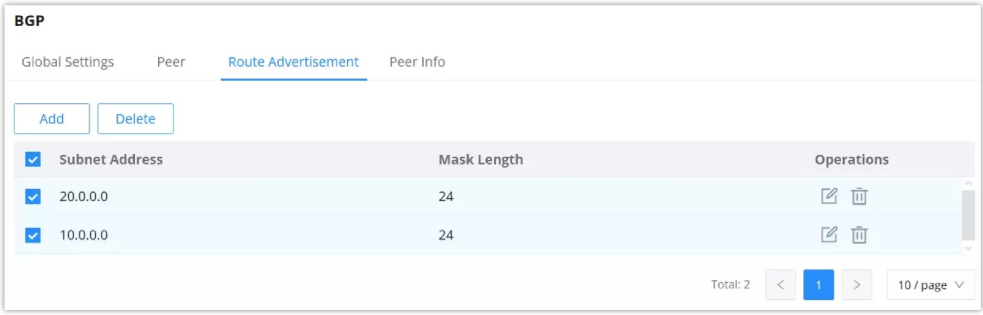
- **Remote AS**: The Autonomous System Number of the remote peer.
- **Remote Address**: The IP address of the remote BGP peer.
- **Connection Hold Time**: The maximum amount of time to hold a BGP connection without receiving a keepalive message.
- **Connect Retry Time**: The interval to retry establishing a BGP connection.
- **Keepalive Time**: The frequency of sending keepalive messages to ensure the peer is active.
- **MD5 Authentication**: Optional security for BGP connections using an MD5 password for session authentication.



BGP – Add/Edit Peer

BGP – Route Advertisement

The **Route Advertisement** tab allows users to manage BGP-advertised routes by adding or removing specific subnets. Here, you can define which networks are advertised to BGP peers.

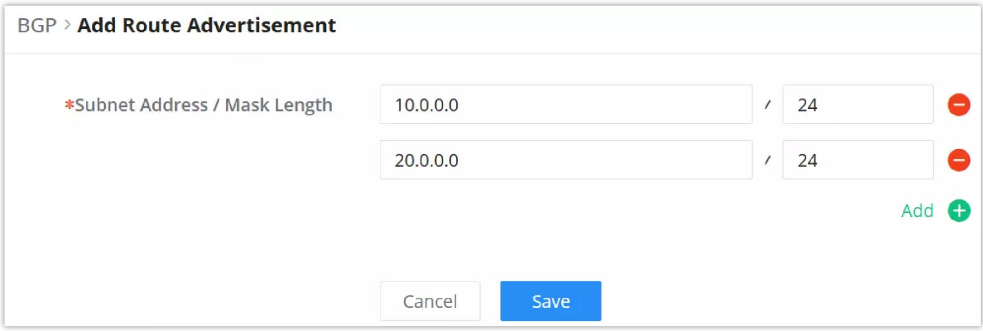


BGP – Route Advertisement page

To add or modify an advertised route, click **Add** or the **Edit** icon. The configuration will prompt you to enter the subnet address and mask length, then click **Save**.

Key configurable fields in this tab include:

Subnet Address / Mask Length: Specify the network's IP address and the corresponding subnet mask length (e.g., 10.0.0.0 / 24).



BGP – Add/Edit route advertisement

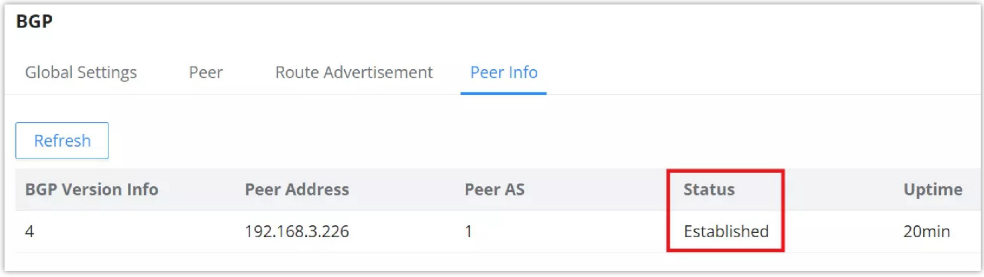
BGP – Peer Info

The **Peer Info** tab in the BGP section provides details on the active BGP peers. Here, users can monitor the status and connection of their BGP peers to ensure proper route exchange.

- **BGP Version Info**: Shows the BGP protocol version in use, typically version 4.
- **Peer Address**: Displays the IP address of the BGP peer.

- **Peer AS**: Shows the Autonomous System (AS) number of the peer.
- **Status**:
  - **Established**: Indicates a fully functional BGP connection where routes are being successfully exchanged between peers. This state confirms that the BGP connection is active and stable.
  - **Active**: Shows the BGP connection is active but may not have fully exchanged routes.
- **Uptime**: Tracks how long the peer connection has been established and active.

You can click the **Refresh** button to update the status of the peers. This allows users to verify quickly if their BGP peers are properly connected and whether routes are being exchanged as expected.

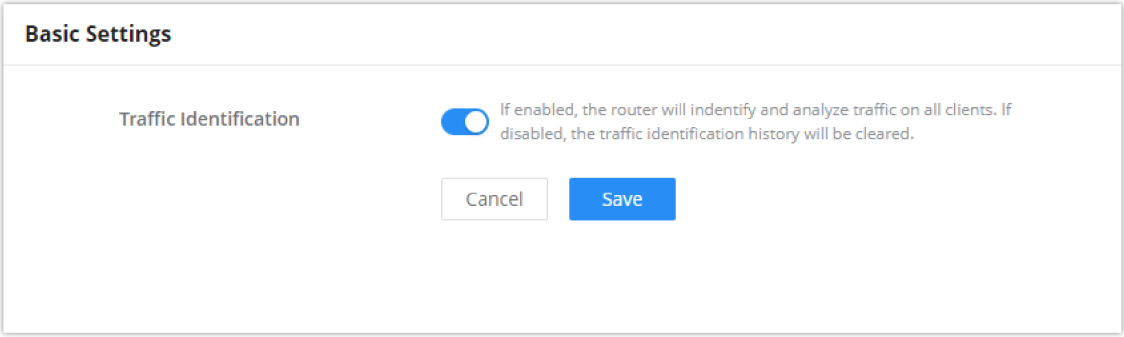


BGP – Peer Info

TRAFFIC MANAGEMENT

Traffic Management – Basic Settings

The GWN700x routers are capable of identifying and analyzing the traffic exchanged between the intranet clients and remote hosts located on the Internet. To enable this feature please navigate to the GUI of the router, then click on **Traffic Management** → **Basic Settings** and toggle on "Traffic Identification".

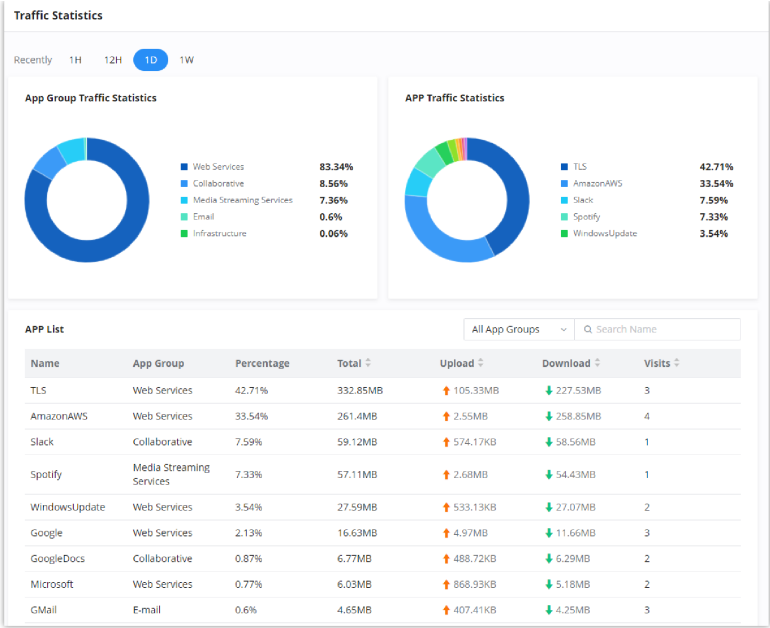


Enable Traffic Identification

Traffic Statistics

When "Traffic Identification" is enabled, the router will start identifying the traffic and generate statistics. The statistics will be represented graphically as shown in the screenshot below. The feature displays the name and the type of the service generating the traffic to easily identify which services are being used and which clients are using them.

> **Note**
>
> GWN7003 router supports up to a month of traffic statistics data.



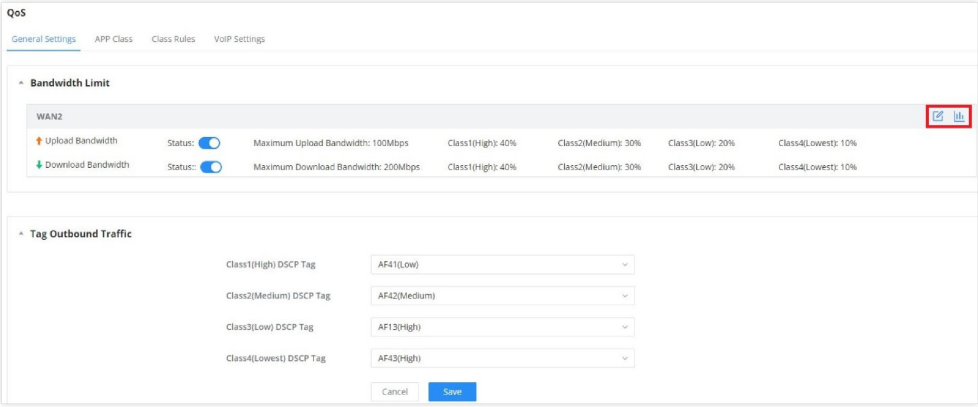
Traffic Statistics and Analysis

QoS

Quality of Service (QoS) is a feature that allows the prioritization if the latency-sensitive traffic exchanged between the WAN and the LAN hosts. This will offer more control over the usage of a limited bandwidth and ensures that all application services are not affected by the amount of the traffic exchanged.

General Settings – QoS

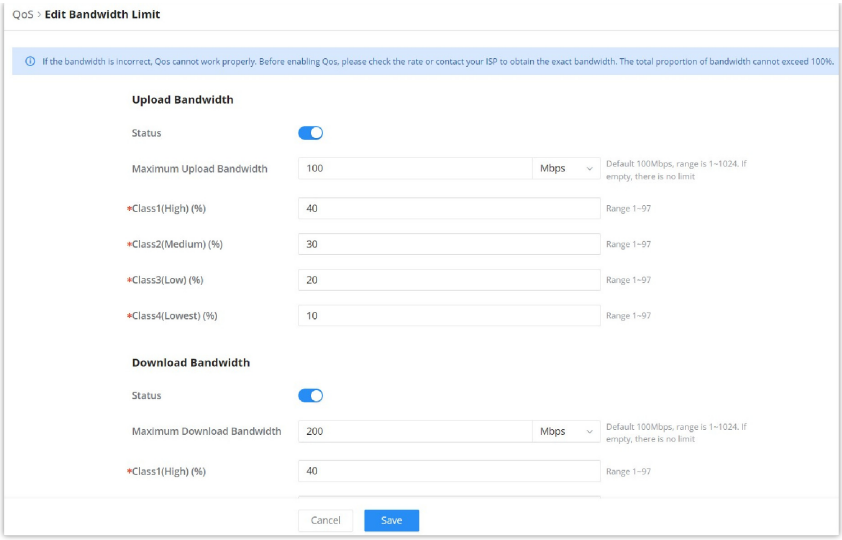
On this page, the user will be able to allocate a percentage of the download and the upload bandwidth to 4 classes. These classes can be assigned to applications to determine which application traffic will be prioritized, this includes the inbound and the outbound traffic. Also, it's possible to tag outbound traffic with DSCP tags for each class.



QoS – General Settings

To set Upload/Download bandwidth percentage for each class, click on edit button .

> **Note:**
>
> If the bandwidth value is incorrect, QoS might not work properly. Before enabling QoS, please check the upload and bandwidth rates if your connection, or contact your ISP to obtain the exact upload and download values. The total sum of the bandwidth percentages cannot exceed 100%.



WAN Port QoS Settings

Upload/Download Bandwidth	
Status	Toggle QoS for the WAN port on/off
Maximum Upload/Download Bandwidth	Specify the maximum upload/download speed for the WAN port.
Class1 (High)	Specify the bandwidth percentage allocated for Class 1.
Class2 (Medium)	Specify the bandwidth percentage allocated for Class 2.
Class3 (Low)	Specify the bandwidth percentage allocated for Class 3.
Class4 (Lowest)	Specify the bandwidth percentage allocated for Class 4.

Edit Bandwidth limit

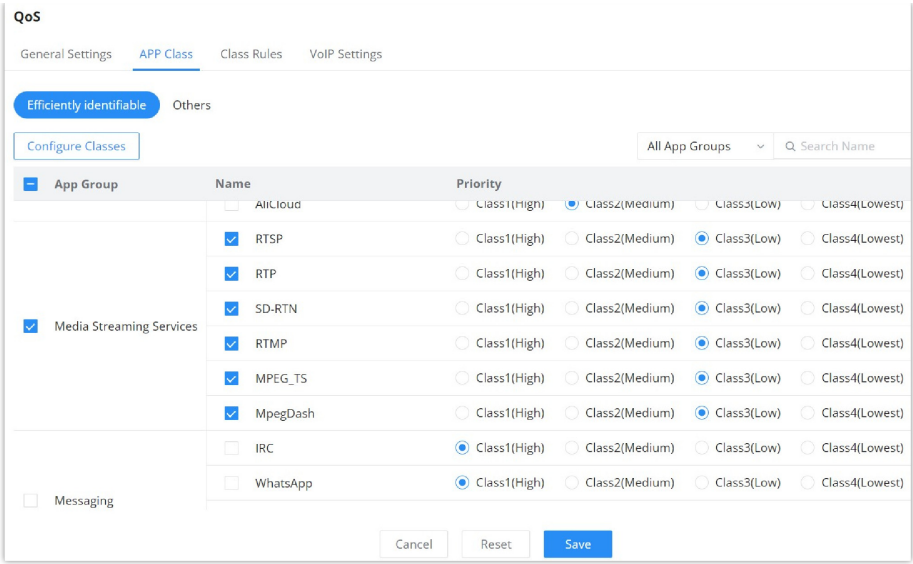
Click on bandwidth statistics icon to get a general overview for upload/download bandwidth status.

QoS – Upload/Download Bandwidth Status

APP Class

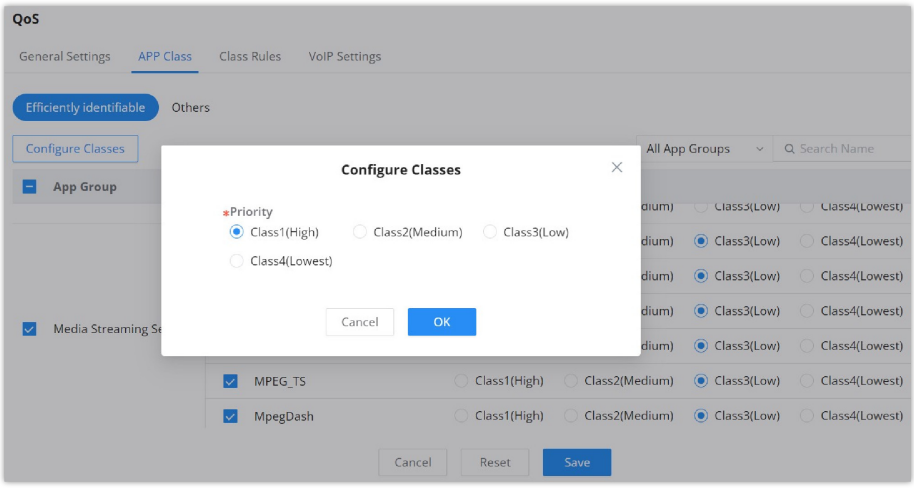
GWN700X routers can prioritize the traffic of each application individually. The priority level can be set in 4 classes, class 1 having the highest priority and class 4 having the lowest priority. To access APP Class settings, please access the web GUI of the router then navigate to **Traffic Management → QoS → APP Class.**

The user can either set the priority for the individual applications by selecting the priority of the corresponding applications.



QoS – APP Class

Or, the use can select the applications and application categories and then click "**Configure Classes**" then choose the adequate priority.



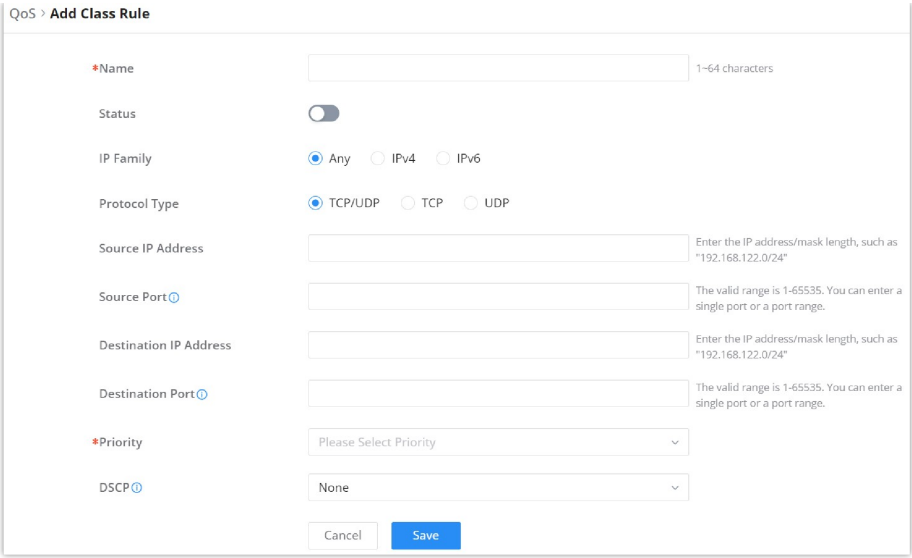
QoS – Apps Class – Configure Classes

Note

App Class may take sometime to be applied since the router needs to inspect a sufficient number of packets to identify the traffic generated by the application.

Class Rules

QoS class rules are rules which sets the QoS based on source or/and destination IP addresses, and source and destination ports.



QoS – Add Class Rules

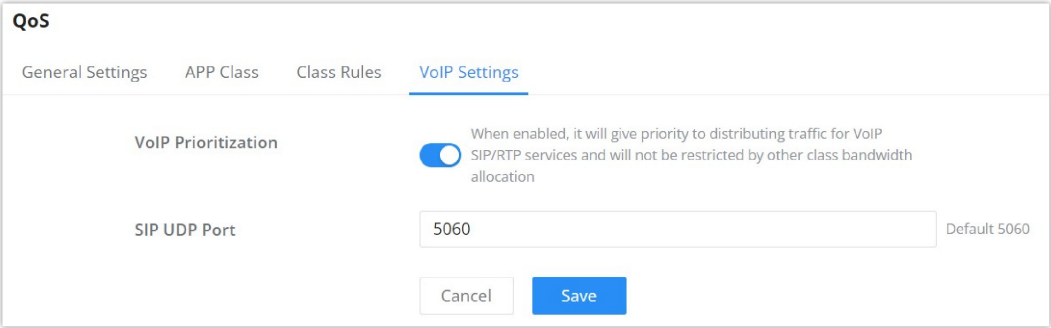
Name	Enter the name of the class. The character limit is 1-94 characters.
Status	Enable or disable the class's status.
IP Family	Choose the IP family: ● **Any:** The IP addresses allowed can either be IPv4 or IPv6. ● **IPv4:** The IP addresses allowed are strictly IPv4. ● **IPv6:** The IP addresses allowed are strictly IPv6.
Protocol Type	Choose the protocol type: ● **TCP/UDP:** The QoS class will apply to both TCP and UDP traffic. ● **TCP:** The QoS class will apply only to the TCP traffic. ● **UDP:** The QoS class will apply only to the UDP traffic.
Source IP Address	Enter the source IP address/mask length. E.g.,"192.168.122.0/24"
Source Port	Enter a single port number, multiple port numbers, or a range of ports number. **Example:** - To enter a single port number, type the port number such as "3074". - To enter multiple port numbers, type the port numbers with a comma in between each port number, such as "3074, 5060, 10000". - To enter a range of port, enter the first port number in the range, then type a dash (-) and enter the last port number in the range. E.g., "10000-20000" **Note:** The valid range of port numbers that can be entered is 1-65535.
Destination IP Address	Enter the destination IP address/mask length. E.g.,"192.168.122.0/24"
Destination Port	Enter a single port number, multiple port numbers, or a range of ports number. **Example:** - To enter a single port number, type the port number such as "3074". - To enter multiple port numbers, type the port numbers with a comma in between each port number, such as "3074, 5060, 10000". - To enter a range of port, enter the first port number in the range, then type a dash (-) and enter the last port number in the range. E.g., "10000-20000" **Note:** The valid range of port numbers that can be entered is 1-65535.
Priority	Select the class of priority.

DSCP	Choose a DSCP value.

QoS – Add Class Rules

VoIP Settings

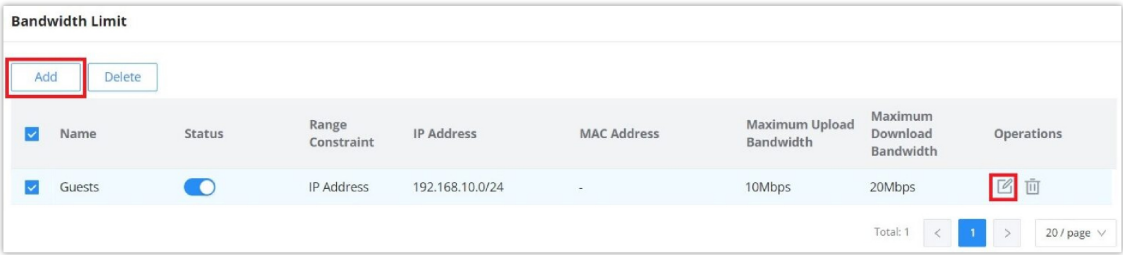
VoIP Settings in QoS allow the user to identify and prioritize the VoIP traffic that is forwarded by the router. To configure this option, please access the web UI of the GWN router and navigate to **Traffic Management** → **QoS** → **VoIP Settings**, then toggle on the "**VoIP Prioritization"**, after that specify the SIP UDP port, by default the port number is 5060.



VoIP Settings

Bandwidth Limit

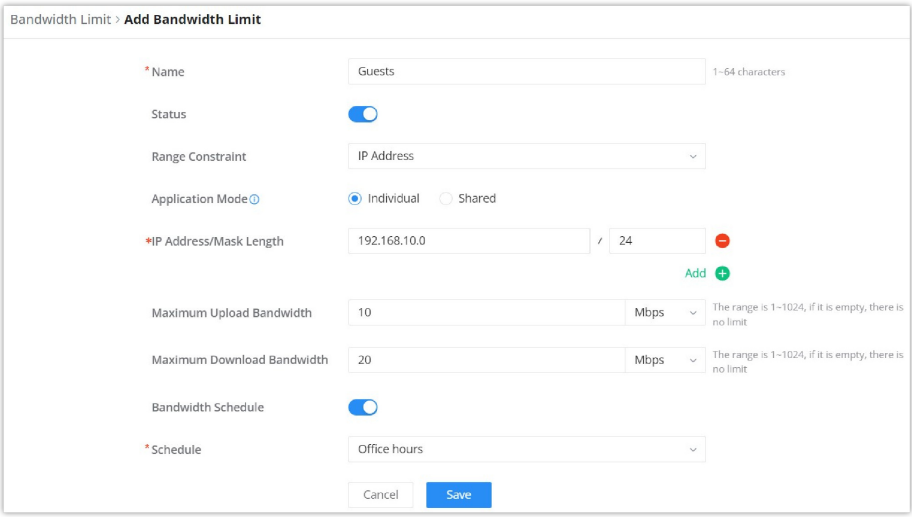
Bandwidth limit feature helps to limit bandwidth by specifying the maximum upload and download limit, then this limit can be applied on each IP/MAC address or applied on all IP addresses in the IP address range. Navigate to **Web UI** → **Traffic Management** → **Bandwidth Limit**.



Bandwidth Limit page

To add a bandwidth rule, please click on "**Add**" button or click on "**Edit**" icon as shown above.

Please refer to the figure below:



Add/edit Bandwidth rule

Note:

Application Mode: Select “Individual” to set the maximum upload bandwidth and maximum download bandwidth that can be used by each IP address, and “shared” to set the sum of the maximum upload bandwidth and maximum download bandwidth that can be used by all IP addresses in the IP address range.

AP MANAGEMENT

GWN700X routers come with an embedded controller for the GWN access points. The user can configure all the Wi-Fi related settings through the controller. When the APs are connected to the router, and they are paired with it, they will automatically inherit the configuration which has been set on the router’s AP Management section.

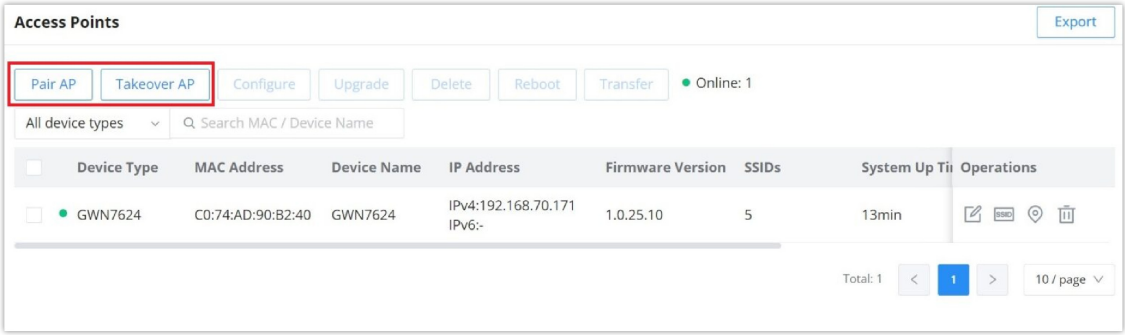
Access Points

In this section, the user can add the access point which can be controlled using the embedded controller within the router. The user can either pair or takeover an access point in order to be able to configure it. The configuration performed on the router AP embedded controller will be pushed to the access points; thus, offering a centralized management of the GWN access points.

Note

Please note that the GWN access point that the user wishes to configure must be on the same LAN as the router.

To add a GWN access point to the GWN router, please navigate to **Web UI → AP Management → Access Points**.



Access Points List

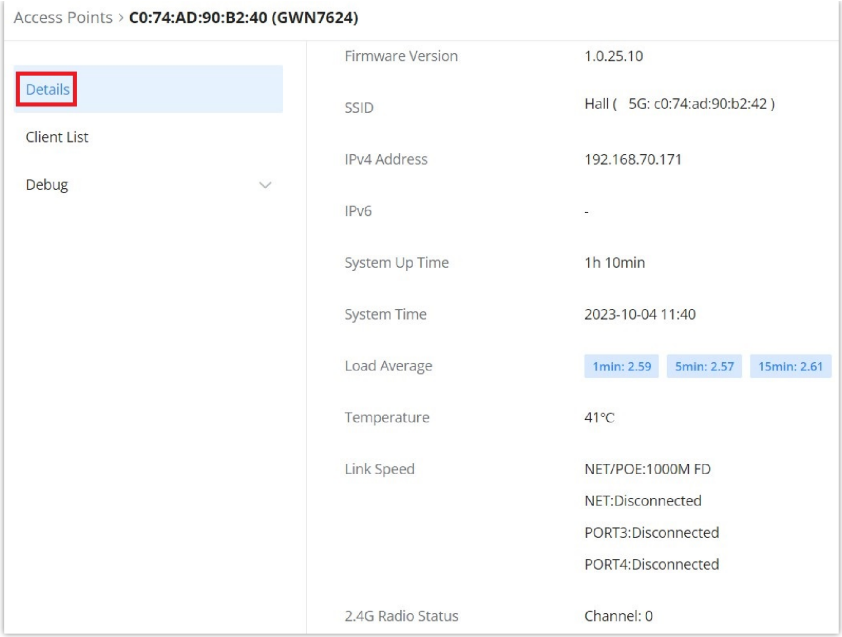
Pair AP: Use this button when pairing an AP which has not be set as a master.
Takeover AP: Use this button to take over an access point which has formerly been set as slave to a different master device. In order to pair the devices successfully, the network administrator must enter the password of the master device.

Note

While the router can create SSIDs and configure the Wi-Fi related settings, the router itself is not able to broadcast the SSID. Therefore, a GWN access point is required to broadcast the Wi-Fi signal.

Click on a paired GWN AP to view Details, Client list and debug tools. Please refer to the figures below:

Details section contains details about the paired AP like firmware version, SSID, IP address, Temperature, etc.

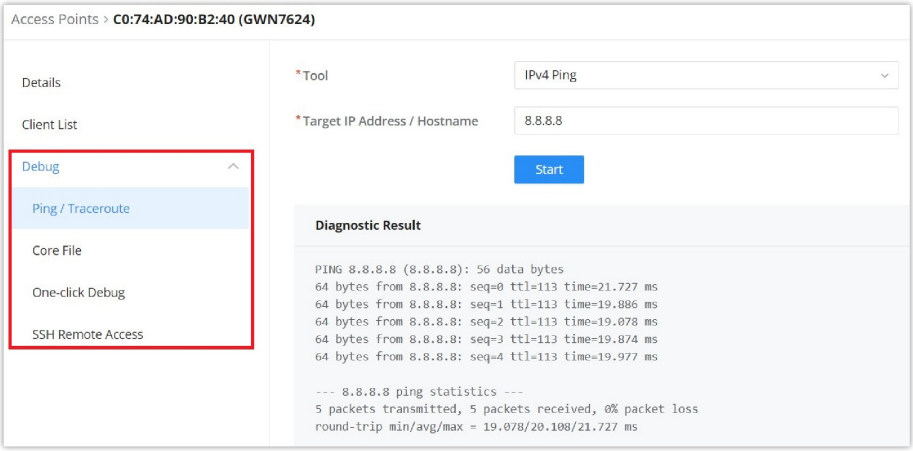


Paired APs – Details

Client List section lists all the connected clients trough this AP with many info like MAC Address, Device name, IP Address, bandwidth, etc.

Paired APs – Client list

Debug section provides the users with many debug tools to help diagnostics any issue like Ping/Traceroute, One-click Debug and SSH Remote Access.

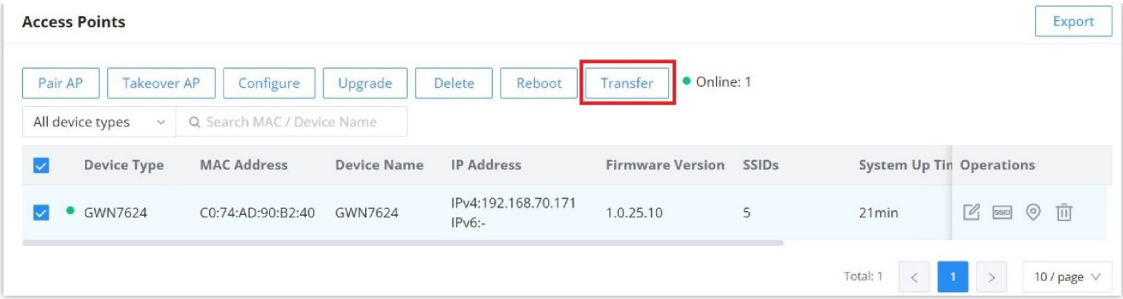


Paired APs – Debug

Transfer APs to GDMS Networking/GWN Manager

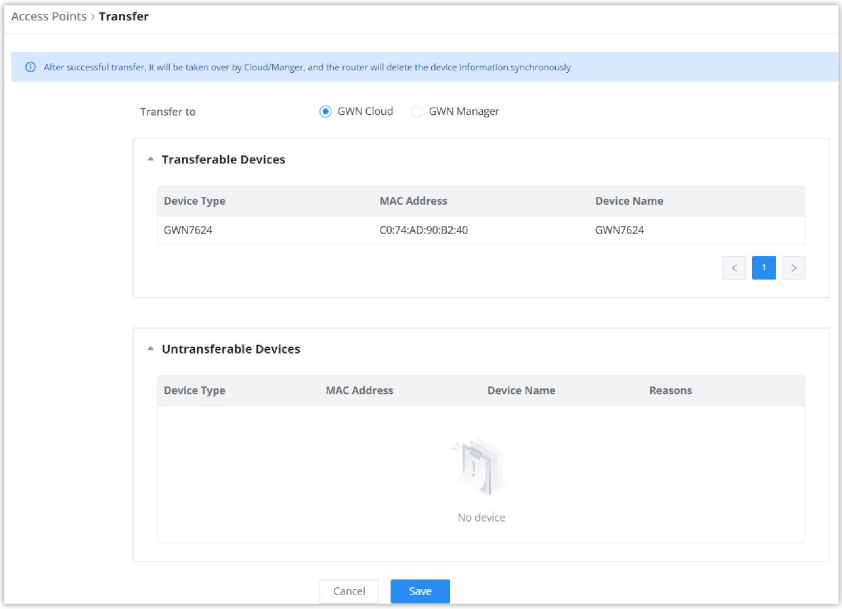
GWN routers also enables to users to transfer their paired GWN APs to GDMS Networking/GWN Manager.

On the **AP Management** → **Access Points** page, select the AP or APs then click on "**Transfer**" button as shown below:



Access Points List

On the next page, select either GDMS Networking or GWN Manager then click "**Save**" button. the user will be forwarded automatically to either GDMS Networking or GWN Manager to login.



Transfer AP to GDMS Networking or GWN Manager

Note:

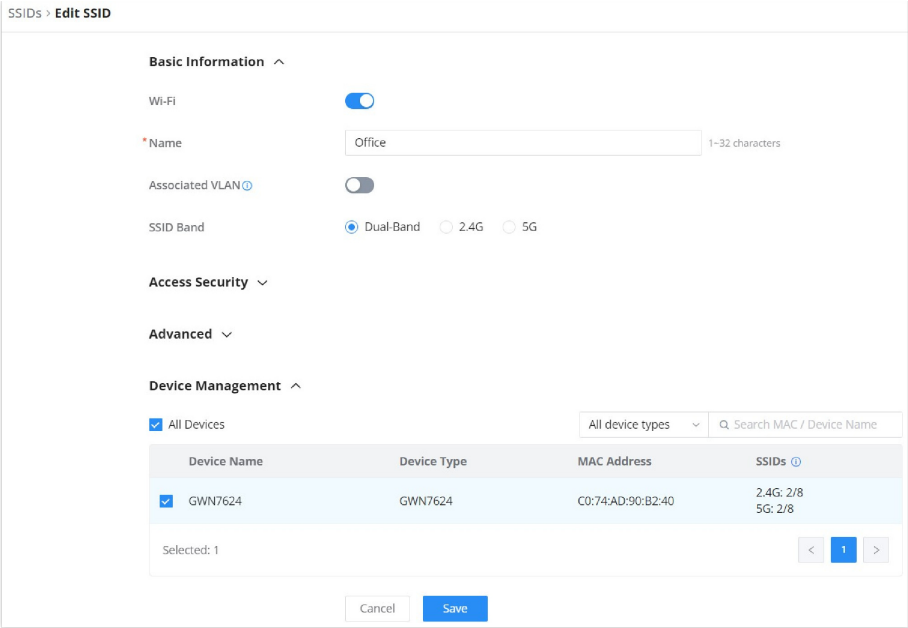
After successful transfer, it will be taken over by Cloud/Manger, and the router will delete the device information synchronously.

SSIDs

In this page, the user can configure SSID settings. The Wi-Fi SSID will be broadcasted by the paired access points. This offers a centralized control over the SSIDs created which makes managing many GWN access points easier and more convenient.

SSID page

In order to add an SSID, the user should click on "**Add**" button, then the following page will appear:



Add SSID

Basic Information	
Wi-Fi	Toggle on/off the Wi-Fi SSID.
Name	Enter the name of the SSID.
Associated VLAN	Toggle "**ON**" to enable VLAN, then specify the VLAN from the list or click on "**Add VLAN**" to add one.
SSID Band	Choose the Wi-Fi SSID band. ● **Dual-Band:** Both bands will be enabled. ● **2.4G:** Only 2.4G band is enabled. ● **5G:** Only 5G band is enabled.
Access Security	
Security Mode	Choose the security mode for the Wi-Fi SSID. ● **Open** ● **WPA/WPA2** ● **WPA2** ● **WPA2/WPA3** ● **WPA3** ● **WPA3-192**
WPA Key Mode	Choose the WPA key mode: ● **PSK** ● **802.1x** ● **PPSK without RADIUS** ● **PPSK with RADIUS**
WPA Encryption Type	Choose the encryption type: ● **AES** ● **AES/TKIP**
WPA Shared Key	Enter the shared key phrase. This key phrase will be required to enter when connecting to the Wi-Fi SSID.

Enable Captive Portal	Toggle Captive Portal on/off. ● **Captive Portal Policy:** Choose the created captive portal policy.
Blocklist Filtering	Choose a blocklist for the Wi-Fi SSID.
Client Isolation	● **Closed:** Allow access between wireless clients. ● **Radio:** All wireless clients will be isolated from each other. ● **Internet:** Access to any private IP address will be blocked. ● **Gateway MAC:** Private IP addresses except for the configured gateway will be blocked.
802.11w	● **Disabled** ● **Optional:** either 802.11w supported or unsupported clients can access the network. ● **Required:** only the clients that support 802.11w can access the network.
Advanced	
SSID Hidden	After enabled, wireless devices will not be able to scan this Wi-Fi, and can only connect by manually adding network.
DTIM Period	Configure the delivery traffic indication message (DTIM) period in beacons. Clients will check the device for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Please input an integer between 1 to 10.
Wireless Client Limit	Configure the limit for wireless client, valid from 1 to 256. If every Radio has an independent SSID, each SSID will have the same limit. Therefore, setting a limit of 256 will limit each SSID to 256 clients independently.
Client Inactivity Timeout (sec)	Router/AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.
Multicast Broadcast Suppression	● **Disabled:** all of the broadcast and multicast packages will be forwarded to the wireless interface. ● **Enabled:** all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND. ● **Enabled with ARP Proxy**: enable the optimization with ARP Proxy enabled in the meantime.
Convert IP Multicast to Unicast	● **Disabled:** No IP multicast packets will be converted to unicast packets. ● **Passive:** The device will not actively send IGMP queries, and the IGMP snooping entries may be aged after 300s and cannot be forwarded as multicast data. ● **Active:** The device will actively send IGMP queries and keep IGMP snooping entries updated.
Schedule	Enable then select from the drop-down list or create a time schedule when this SSID can be used.
Voice Enterprise	Enable voice enterprise.
802.11r	Enable 802.11r.
802.11k	Enable 802.11k.
802.11v	Enable 802.11v.
ARP Proxy	Once enabled, devices will avoid transferring the ARP messages to stations, while initiatively answer the ARP requests in the LAN.
U-APSD	Configures whether to enable U-APSD (Unscheduled Automatic Power Save Delivery).

Bandwidth Limit	Toggle ON/OFF Bandwidth limit ***Note:*** *If Hardware acceleration is enabled, Bandwidth Limit does not take effect. Please go to Network Settings/Network Acceleration to disable*
Maximum Upload Bandwidth	Limit the upload bandwidth used by this SSID. The range is 1~1024, if it is empty, there is no limit. The values can be set as Kbps or Mbps.
Maximum Download Bandwidth	Limit the download bandwidth used by this SSID. The range is 1~1024, if it is empty, there is no limit The values can be set as Kbps or Mbps.
Bandwidth Schedule	Toggle ON/OFF Bandwidth Schedule; if it's ON, then select a schedule from the drop-down list or click on "**Create Schedule**".
Device Management	
In this section, the user is able to add and remove the GWN access points that can broadcast the Wi-Fi SSID. There is also the option to search the device by MAC address or name.	

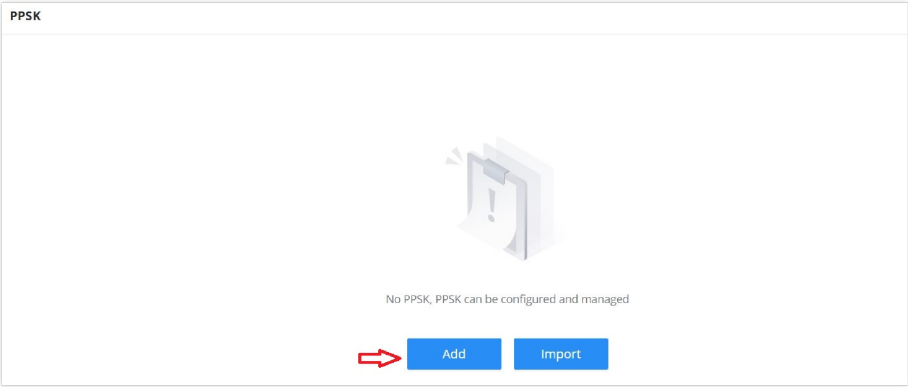
Add SSID

Private Pre-Shared Key (PPSK)

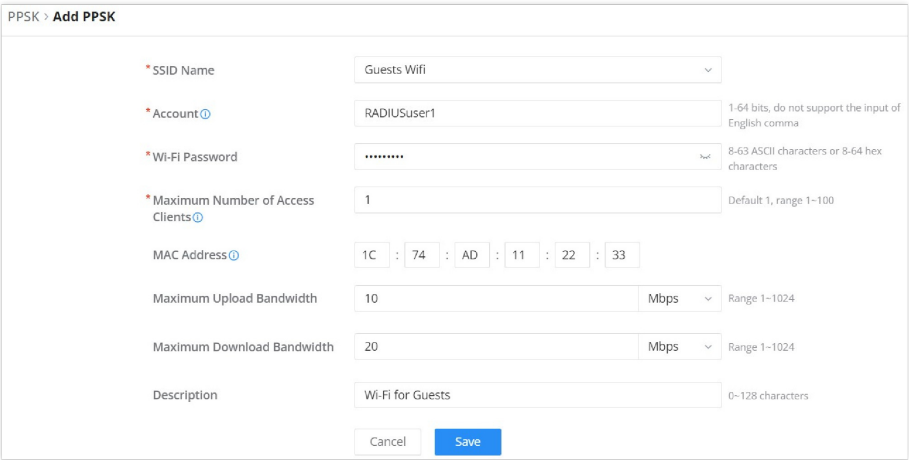
PPSK (Private Pre-Shared Key) is a way of creating Wi-Fi passwords per group of clients instead of using one single password for all clients. When configuring PPSK, the user can specify the Wi-Fi password, maximum number of access clients, maximum upload and download bandwidth.

To start using PPSK, please follow the steps below:

1. First, create an SSID with WPA key mode set to either PPSK without RADIUS or PPSK with RADIUS.
2. Navigate to **Web UI** → **AP Management** → **PPSK** page, then click on "**Add**" button then fill in the fields as shown below:



PPSK page



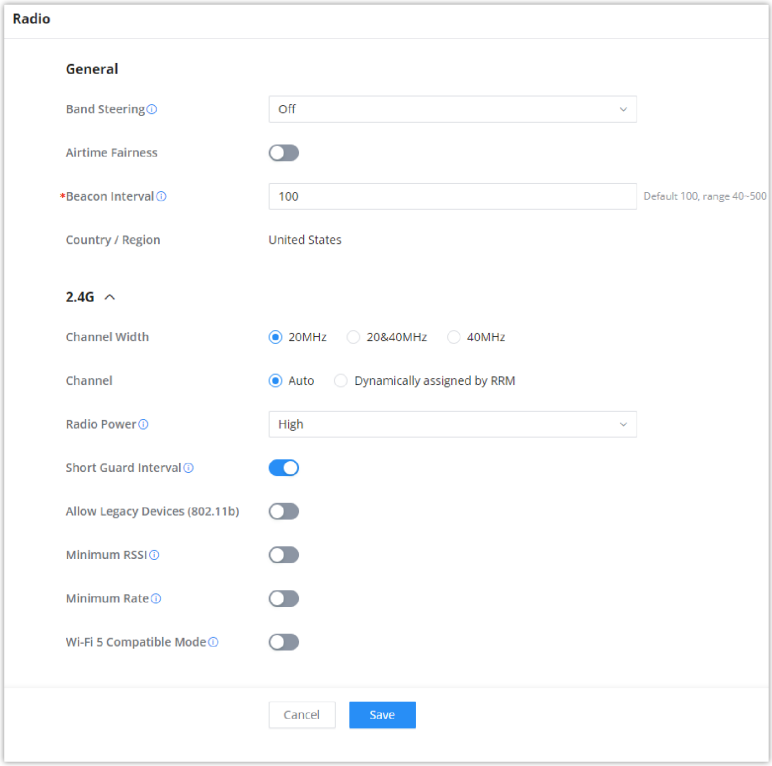
Add PPSK

SSID Name	Select from the drop-down list the SSID that has been previously configured with WPA Key mode set to PPSK without RADIUS or PPSK with RADIUS.
Account	If the WPA key mode in the selected SSID is "PPSK with RADIUS", the account is the user account of the RADIUS server.
Wi-Fi Password	Specify a Wi-Fi password
Maximum Number of Access Clients	Confgures the maximum number of devices allowed to be online for the same PPSK account.
MAC Address	Enter a MAC Address ***Note:*** *this field is only available if the Maximum Number of Access Clients is set to 1.*
Maximum Upload Bandwidth	Specify the maximum upload bandwidth in Mbps or Kbps.
Maximum Download Bandwidth	Specify the maximum downlolad bandwidth in Mbps or Kbps.
Description	Specify a description for the PPSK

Add PPSK

Radio

Under **AP Managements → Radio,** the user will be able to set the general wireless settings for all the Wi-Fi SSIDs created by the router. These settings will take effect on the level of the access points which are paired with the router.



Radio

General	
Band Steering	Band steering functions are divided into four items: 1) 2.4G in priority, lead the dual client to the 2.4G band; 2) 5G in priority, the dual client will be led to the 5G band with more abundant spectrum resources as far as possible; 3) Balance,access to the balance between these 2 bands according to the spectrum utilization rate

	of 2.4G and 5G. In order to better use this function, proposed to enable voice enterprise via SSIDs → Advanced → Enable Voice Enterprise.
Airtime Fairness	Enabling Airtime Fairness will make the transmission between the access point and the clients more efficient. This is achieved by offering equal airtime to all the devices connected to the access point.
Beacon Interval	Configures the beacon period, which decides the frequency the 802.11 beacon management frames router transmits. Please input an integer, from 40 to 500.1. When router enables several SSIDs with different interval values, the max value will take effect;2. When router enables less than 3 SSIDs, the interval value will be effective are the values from 40 to 500;3. When router enables more than 2 but less than 9 SSIDs, the interval value will be effective are the values from 100 to 500;4. When router 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.
Country / Region	This option shows the country/region which has been selected. To edit the region, please navigate to **System Settings → Basic Settings.**
2.4G & 5G	
Channel Width	Select the channel width. ● **2.4G**: 20Mhz, 20&40Mhz, 40Mhz ● **5G**: 20Mhz, 40Mhz, 80Mhz
Channel	Pick how the access points will be able to choose a specific channel. ● **Auto:** ● **Dynamically assigned by RRM:**
Radio Power	Please select the radio power according to the actual situation, too high radio power will increase the disturbance between devices. ● **Low** ● **Medium** ● **High** ● **Custom** ● **Dynamically Assigned by RRM** ● **Auto**
Short Guard Interval	This can improve the wireless connection rate if enabled under non multipath environment.
Allow Legacy Devices (802.11b) (2.4Ghz Only)	When the signal strength is lower than the minimum RSSI, the client will be disconnected (unless it's an Apple device).
Minimum RSSI	When the signal strength is lower than the minimum RSSI, the client will be disconnected (unless it's an Apple device).
Minimum Rate	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality.
Wi-Fi 5 Compatible Mode	Some old devices do not support Wi-Fi6 well, and may not be able to scan the signal or connect poorly. After enabled, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions.

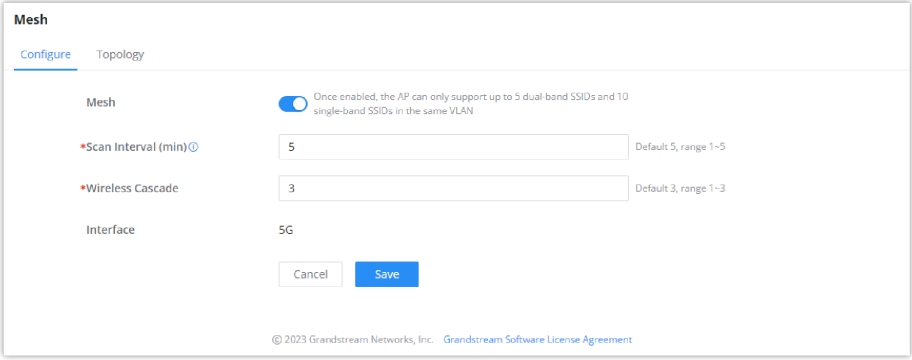
Radio

Mesh

Through the controller embedded in the GWN700X routers, the user can configure a Wi-Fi Mesh using the GWN access points. The configuration is centralized and the user can view the topology of the Mesh.

- **Configuration:**

To configure GWN access points in a Mesh network successfully, the user must pair the access points first with the GWN router, then configure the same SSID on the access points. Once that's done, the user should navigate to **AP Management** → **Mesh** → **Configure**, then enable Mesh and configure the related information as shown in the figure below.



Mesh Configuration

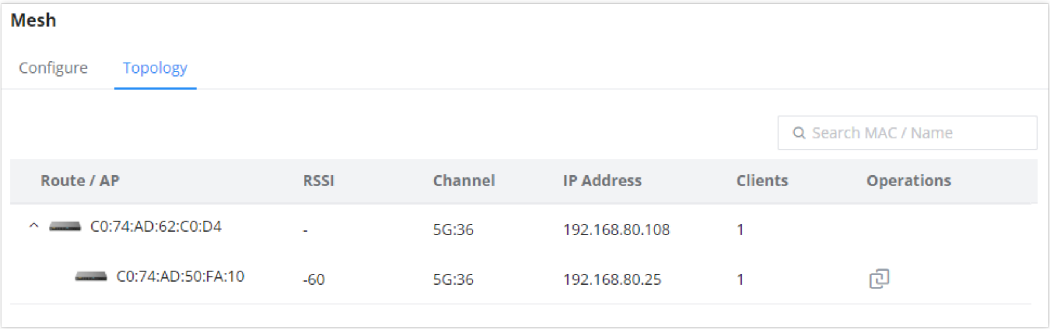
For more information about the parameters that need to be configured, please refer to the table below.

Mesh	Enable Mesh. Once enabled, the AP can only support up to 5 dual-band SSIDs and 10 single-band SSIDs in the same VLAN.
Scan Interval (min)	Configures the interval for the APs to scan the mesh. The valid range is 1-5. The default value is 5.
Wireless Cascade	Define the wireless cascade number. The valid range is 1-3. The default value is 3.
Interface	Displays which interface is going to be used for mesh.

Mesh Configuration

- **Topology:**

In this page, the user will be able to see the topology of the GWN access points when they are configured in a Mesh network. The page will display information related to the APs like the MAC address, RSSI, Channel, IP Address, and Clients. It will show as well the cascades in the Mesh.



Mesh Topology

Switch Management

The **Switch Management** feature allows administrators to monitor, configure, and manage multiple switches through the GWN router interface. With this feature, users can easily add switches to the management platform, take control of their configurations, upgrade firmware, and view performance metrics.

Key Features:

- **Switch Discovery**: Automatically discover available switches connected to the network for easy management.

- **Take over Device**: Add and take over switches for centralized management, allowing you to configure and monitor them directly from the GWN interface.
- **Upgrade, Reboot, and Export**: Perform administrative tasks like upgrading switch firmware, rebooting devices, and exporting a list of managed switches.
- **Detailed Monitoring**: View performance metrics, such as traffic statistics and PoE port details, for each switch.
- **Comprehensive Configuration**: Global switch settings and individual port configurations are available, enabling you to fine-tune your network based on specific needs.

This feature streamlines network management by providing a unified platform to control all switches in the environment, enhancing visibility, and reducing the complexity of managing multiple devices.

Switches

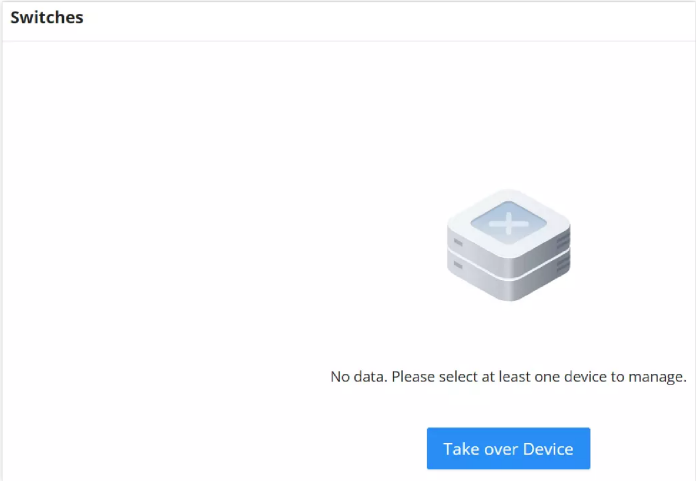
Take over Device (add switch)

- **Take over a switch**

To manage a switch for the first time in your GWN network, follow these steps to "take over" and configure it.

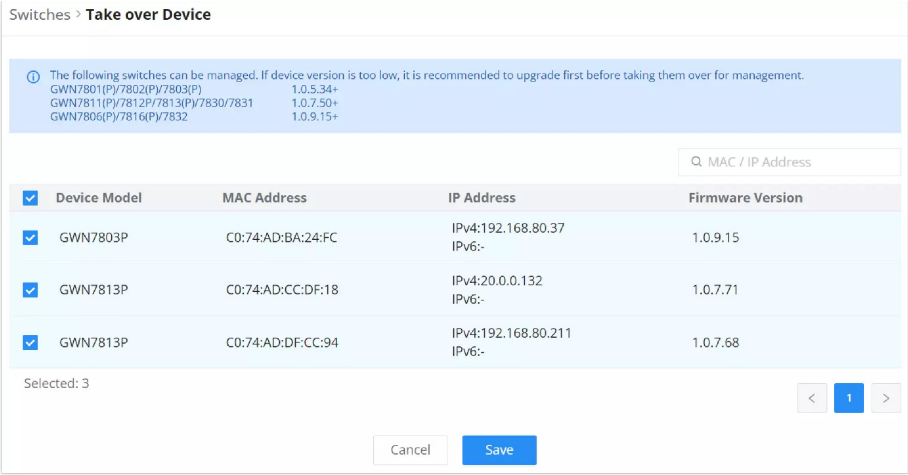
Steps to Take over a Switch:

1. **Navigate to**: **Switch Management** → **Switches.** This will bring you to the **Switches** table. If no devices have been added yet, you will see a prompt stating **"No data. Please select at least one device to manage."**



Switch Management

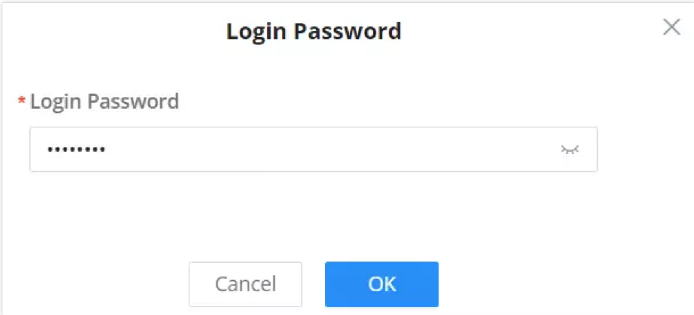
2. **Discover Available Switches**:
   Click on the **Take over Device** button. A new window will open showing all the switches in your network that are available for management. For each switch, you'll see:
   - **Device Model**
   - **MAC Address**
   - **IP Address (IPv4/IPv6)**
   - **Firmware Version**
     If the firmware version is outdated, an upgrade may be required before taking over the switch.



Discover Available Switches

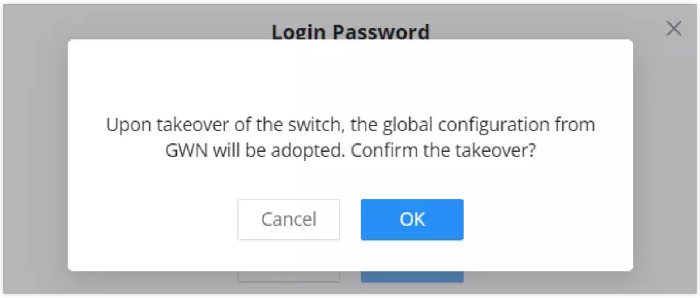
3. **Select the Switch**:
   Tick the checkbox next to the switch you want to take over. You can select multiple switches if desired. Click **Save** once your selection is made.

4. **Enter the Login Password**:
   For security, a password prompt will appear. Enter the **Login Password** of the switch to confirm and complete the takeover.



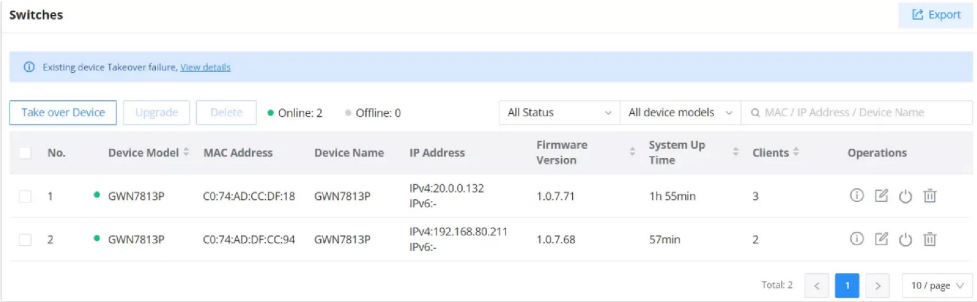
Enter the Login Password

5. **Confirm the Takeover**:
   A confirmation dialog will appear indicating that the global configuration from the GWN router will be adopted on the switch. Click **OK** to proceed.



Confirm the Takeover

6. **Review the Managed Switches**:
   Once successfully added, the switch will appear in the **Switches** table with the following details:
   - **Device Model**
   - **MAC Address**
   - **Device Name**
   - **IP Address**
   - **Firmware Version**
   - **System Up Time**
     You will also see a status for how many switches are **Online** and **Offline**.

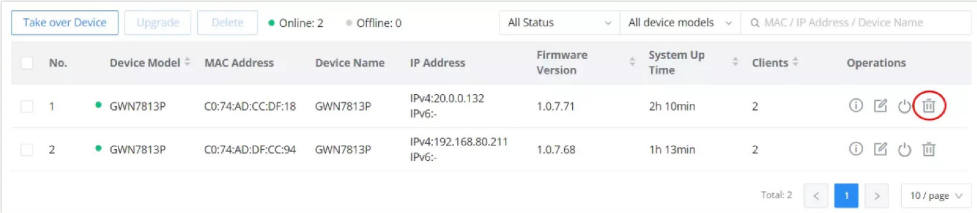


Review the Managed Switches

- **Delete (Remove) a switch**

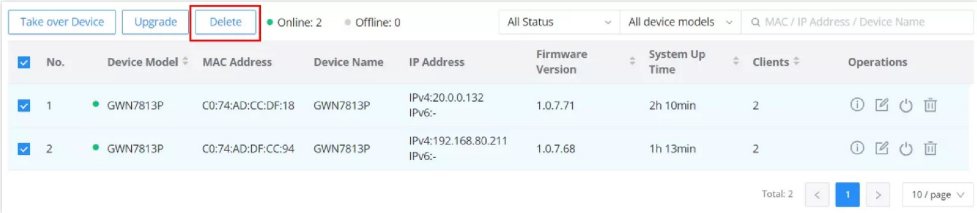
To remove a switch from the GWN router:

1. Navigate to: **Switch Management → Switches**.
2. **Delete a Single Switch:** in the **Operations** column of the Switches table, click the **Delete** icon next to the switch you wish to remove.



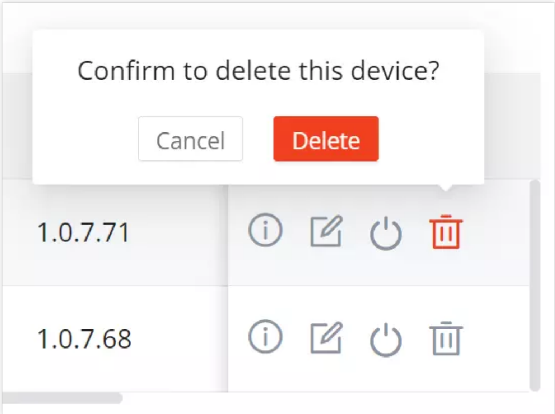
Delete (Remove) a switch – part 1

3. **Delete Multiple Switches:** alternatively, select multiple switches by checking the boxes next to their names, then click the **Delete** button at the top of the table.



Delete (Remove) a switch – part 2

4. **Confirmation:** confirm the deletion in the prompt that appears.



Delete (Remove) a switch – part 3

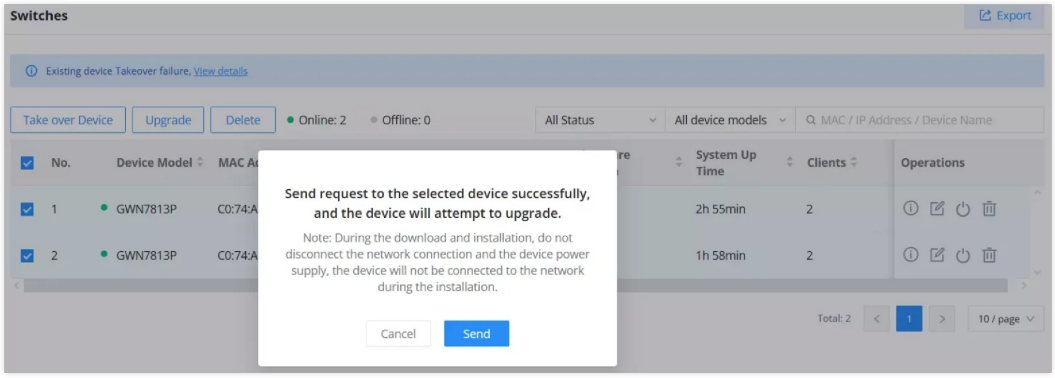
Upgrade, Reboot and Export

- **Upgrade switches**

1. Navigate to: **Switch Management → Switches.**
2. In the Switches table, select the switches you want to upgrade by checking the boxes.
3. Click **Upgrade**.

4. A prompt will appear: "*Send request to the selected device successfully, and the device will attempt to upgrade.*"
   - **Note**: Do not disconnect the network or power supply during the upgrade process.

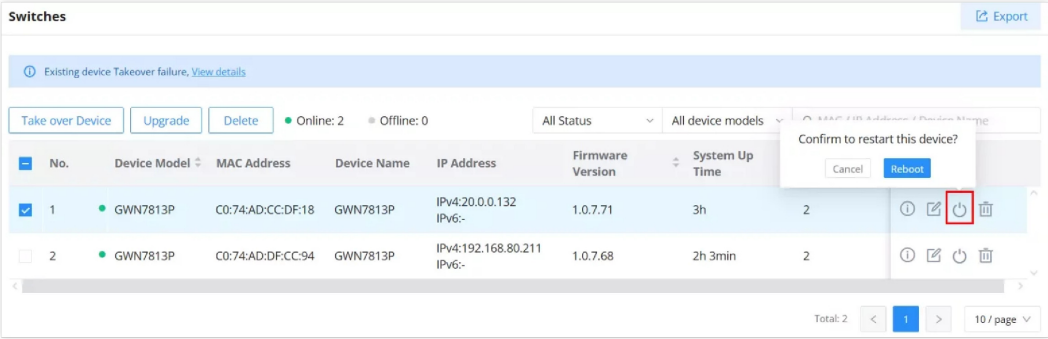
5. Click **Send** to initiate the upgrade.



Upgrade switches

- **Reboot switch**

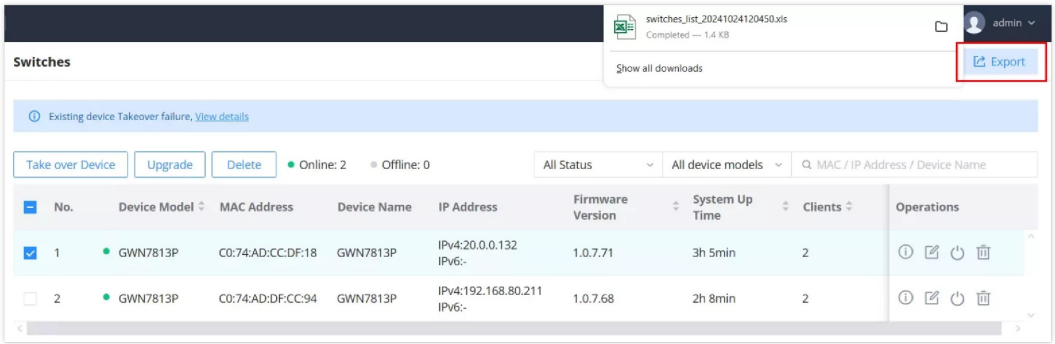
1. Navigate to: **Switch Management** → **Switches**.
2. In the **Switches** table, identify the switch you want to reboot.
3. Click the **Reboot** icon (power symbol) located under the **Operations** column.
4. A confirmation message will appear asking: "Confirm to restart this device?"
5. Click **Reboot** to restart the switch.



Reboot switches

- **Export switches list**

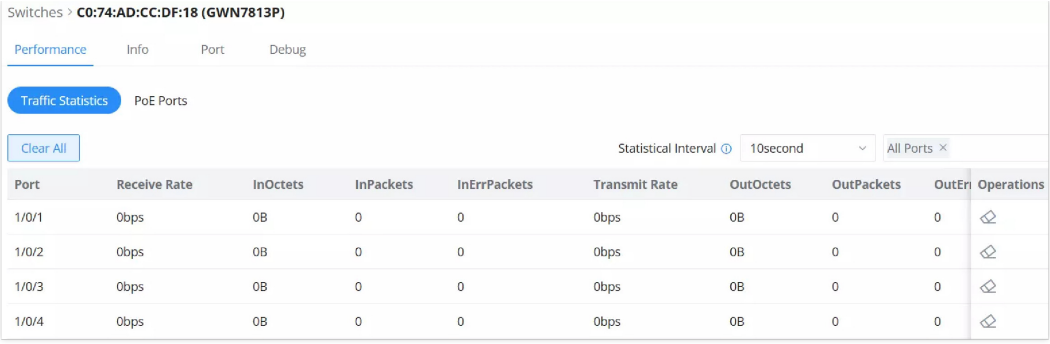
1. Navigate to: **Switch Management** → **Switches**.
2. In the **Switches** table, click the **Export** button located at the top-right corner.
3. The switch list will be downloaded as an Excel (.xls) file, containing details such as Device Model, MAC Address, IP Address, Firmware Version, and System Up Time.



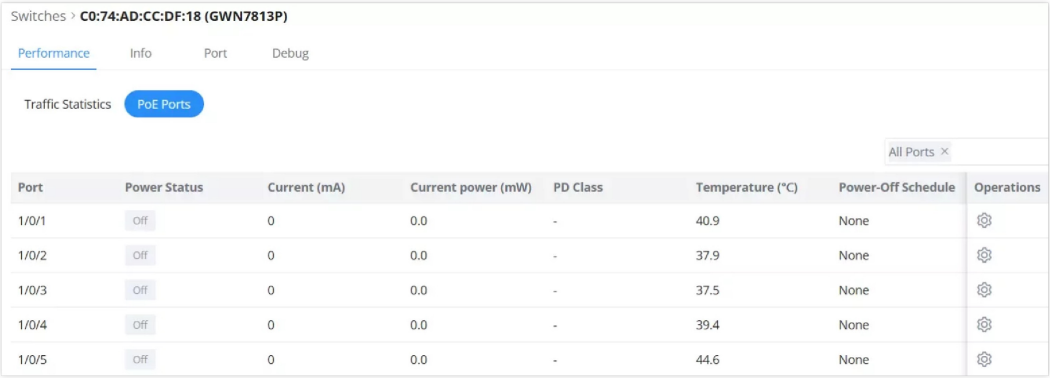
Export switches

Switch Details

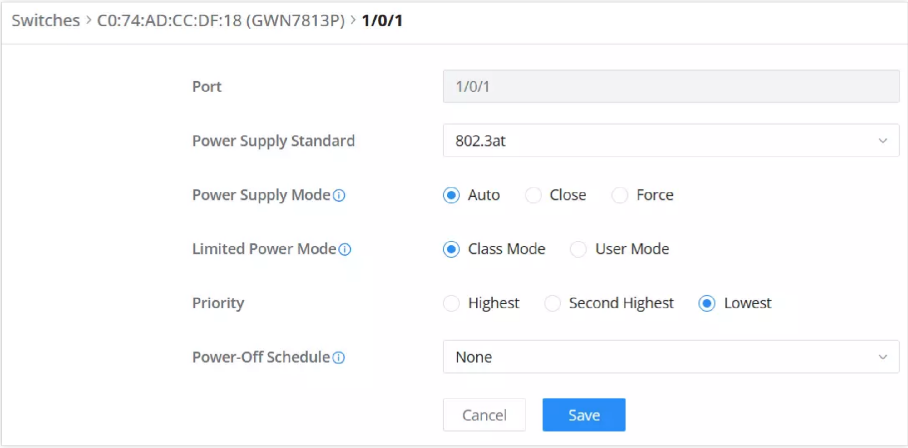
- **Performance**



Switch – Performance – Traffic Statistics

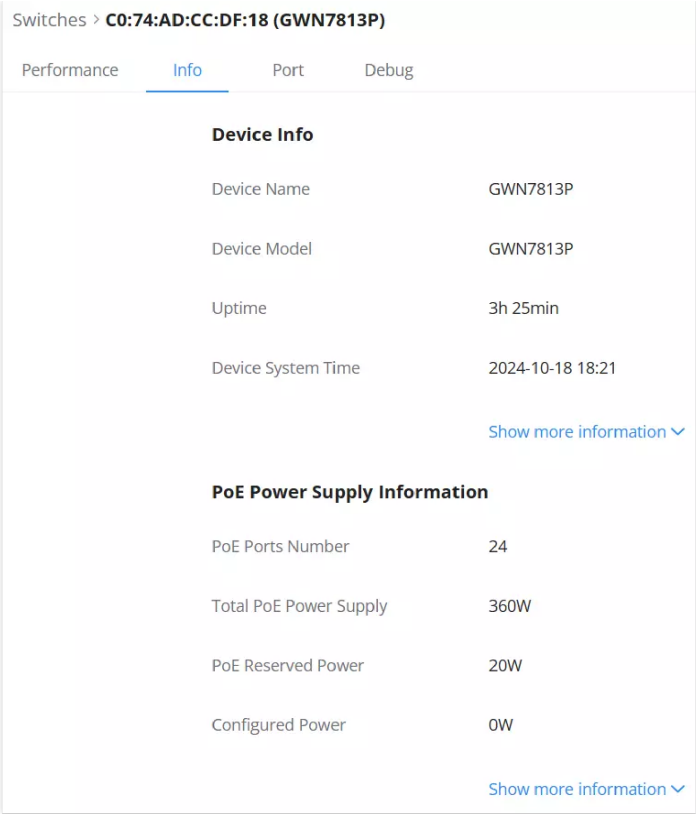


Switch – Performance – PoE Ports



Switch – Performance – Edit PoE

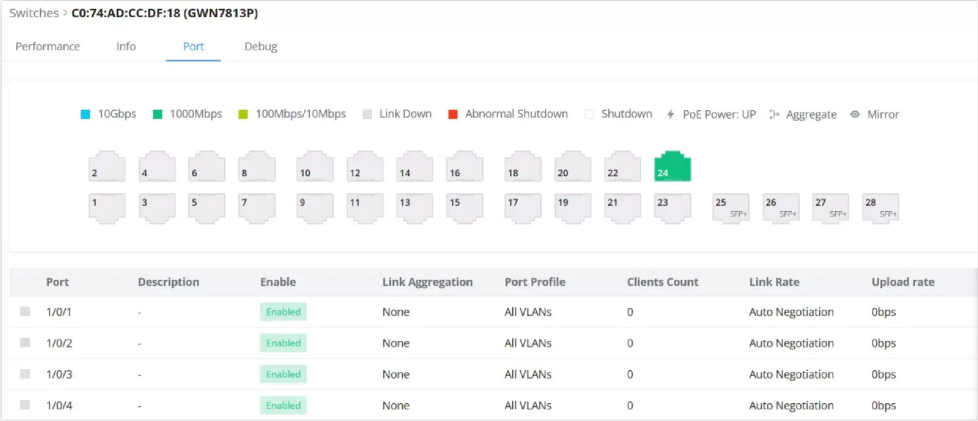
- **Info**



Switch – Info

- **Port**

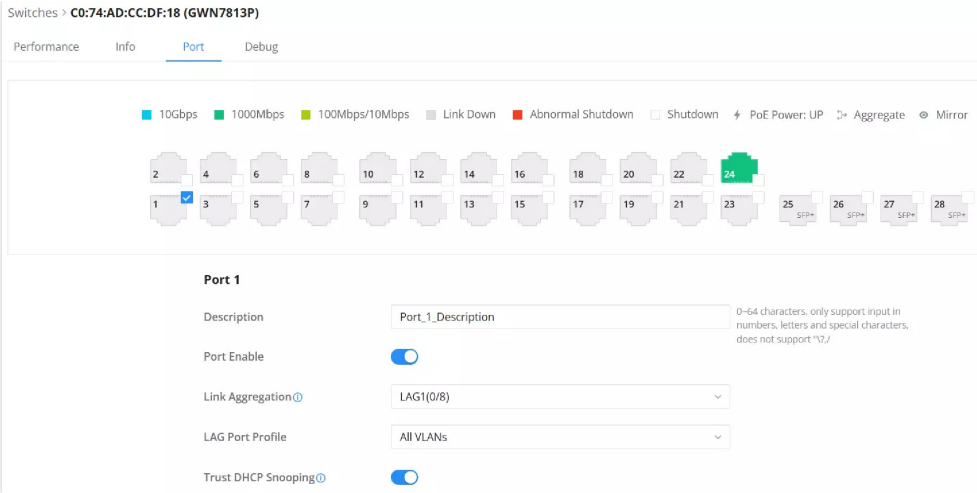
The Port Configuration page enables you to manage and fine-tune the behavior of each port. You can adjust network settings, security controls, VLAN profiles, and more for each individual port. This helps tailor each port's function to the specific needs of your network.



Switch Port – part 1

Port Details

- **Port Enable/Disable**: Switches the port on or off.
- **Description**: Option to label the port for easier management.
- **Link Aggregation (LAG)**: Assigns the port to a LAG group to increase throughput or redundancy.
- **Port Profile**: Selects from existing VLAN profiles or allows profile override for custom configurations.
- **Port Mirroring**: Mirrors traffic from one port to another for monitoring.
- **Trust DHCP Snooping**: Improves DHCP security by only allowing trusted DHCP traffic.



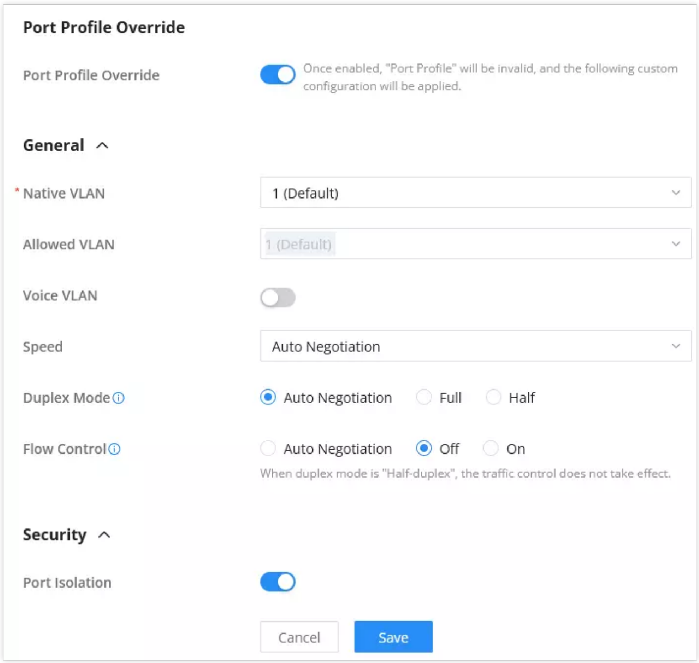
Switch Port – part 2

Port Profile Override This section allows custom configuration when the default port profile doesn't fit the requirements.

- **Native VLAN**: Specifies the VLAN for untagged traffic.
- **Allowed VLAN**: Defines which VLANs are permitted to pass through.
- **Voice VLAN**: Prioritizes voice traffic for QoS (Quality of Service).
- **Speed Settings**: Options include Auto-Negotiation, Full-Duplex, Half-Duplex, and more.
- **Flow Control**: Determines whether the port will use flow control to manage traffic congestion.

Security Options

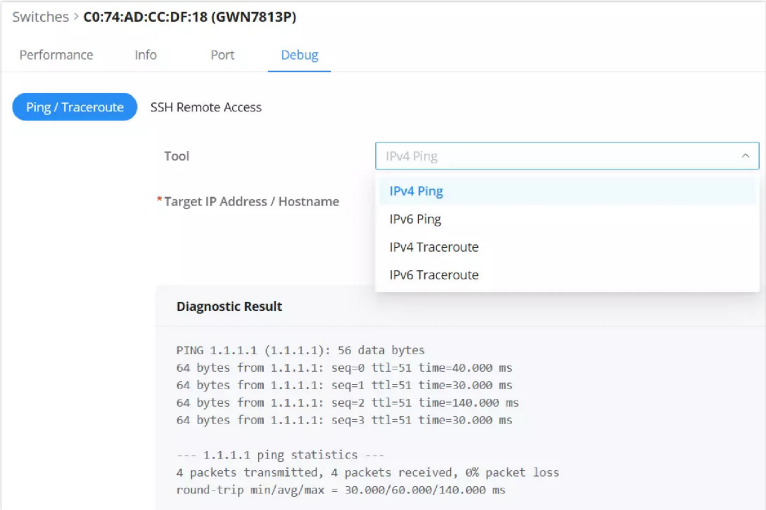
- **Storm Control**:
  - Prevents traffic floods (e.g., broadcast, multicast storms) that can degrade network performance by limiting the number of broadcast or multicast packets allowed.
- **Port Isolation**:
  - Restricts communication between devices on the same switch. When enabled, the port can only communicate with uplink ports and is isolated from other local ports for improved security.
- **Port Security**:
  - This feature limits the number of MAC addresses allowed on a port, preventing unauthorized devices from connecting.
- **802.1X Authentication**:
  - Provides network access control by authenticating devices attempting to connect to the network via this port. Commonly used in environments where device identity and security are important, such as enterprise networks.



- **Debug**

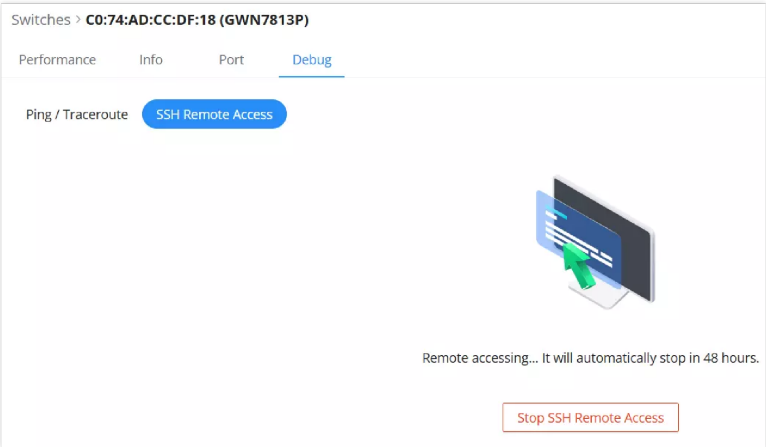
For the **Debug** function there are two primary functions:

1. **Ping/Traceroute**:
   - Select a diagnostic tool from the dropdown menu:
     - IPv4 Ping
     - IPv6 Ping
     - IPv4 Traceroute
     - IPv6 Traceroute
   - Enter the target IP address or hostname.
   - Click **Start** to initiate the diagnostic.
   - The diagnostic results will display packet transmission details, round-trip times, and packet loss, as shown.



Switch Debug – Ping/Traceroute

2. **SSH Remote Access**:
   - Enter the SSH password to start remote access.
   - A notification will confirm the remote session, which will terminate automatically after 48 hours.
   - To manually end the session, click **Stop SSH Remote Access**.

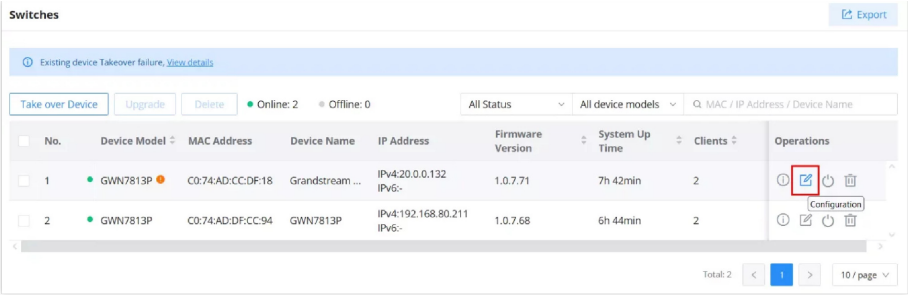


Switch Debug – SSH Remote Access

Switch Configuration

In this section, you can configure the **switch details**, manage **VLAN interfaces**, and set up **RADIUS authentication**.

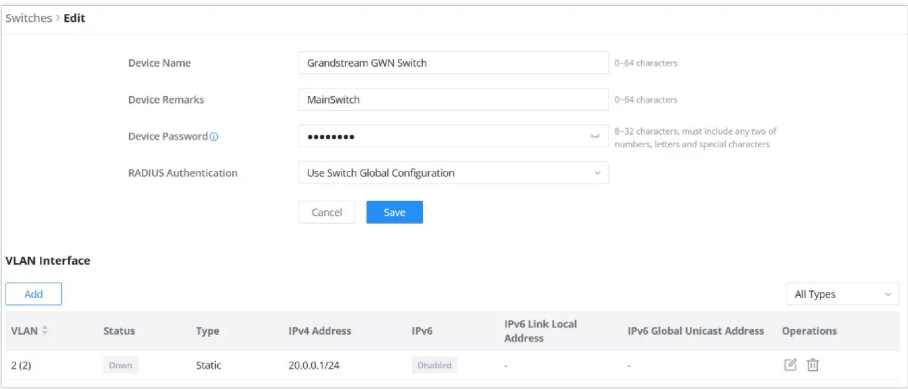
Access the Configuration Page:
In the **Switch Management** → **Switches** screen, click the **Configuration** icon next to the desired switch.



Switch configuration

Edit Switch Details:
The **Switches** → **Edit** page (as seen in the second image) allows you to configure:

- **Device Name** and **Remarks**
- **Device Password**
- **RADIUS Authentication**: You can choose to use the **Switch Global Configuration** or define a custom RADIUS setting by selecting from the dropdown or adding a new one by clicking **Add RADIUS Authentication**.



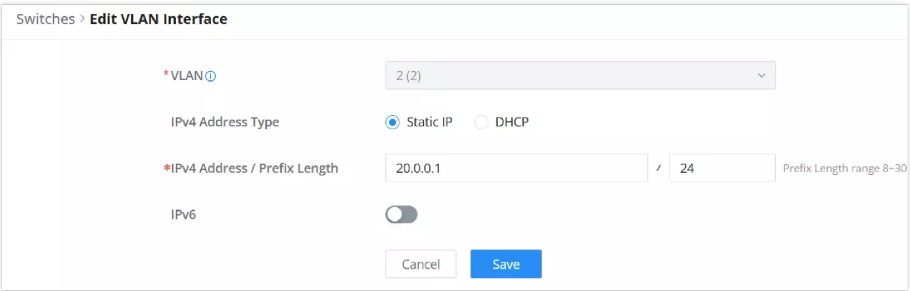
Switch configuration – part 2

Manage VLAN Interfaces:
Scroll to the **VLAN Interface** section where you can:

- **Add a VLAN** by clicking the **Add** button.
- **Edit existing VLAN** entries by clicking the pencil icon.
- View each VLAN's **status**, **type**, and **IP addresses**.

Add/Edit VLAN Interface:
When adding or editing, set the VLAN ID, choose IP settings (Static IP or DHCP), and configure IPv6 if required.

Save Changes:
After making your changes, click **Save** to apply the configuration.



Switch configuration – Add/Edit VLAN Interface

Configuration

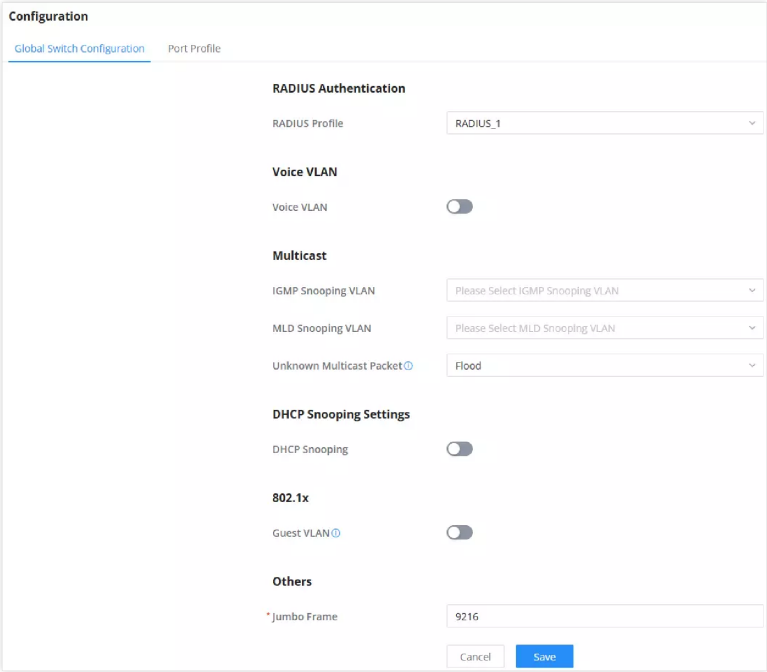
Global Switch Configuration

In the **Global Switch Configuration** section, you can configure settings that affect all switches in your network, ensuring consistent behavior across your entire switch infrastructure. This is distinct from configuring individual switches, as it provides network-wide settings.

Configurable Options:

- **RADIUS Authentication**:
  - Set a RADIUS profile for centralized authentication across switches.
- **Voice VLAN**:
  - Enable a dedicated VLAN for voice traffic, optimizing voice data flow.
- **Multicast**:
  - **IGMP/MLD Snooping VLAN**: Designate VLANs for IGMP and MLD snooping to manage multicast traffic efficiently.
  - **Unknown Multicast Packet**: Choose how to handle unknown multicast packets (e.g., Flood).
- **DHCP Snooping Settings**:
  - Enable DHCP snooping to prevent unauthorized DHCP servers.
- **802.1x**:
  - Set up guest VLAN for 802.1x-based authentication, securing access to the network.
- **Others**:
  - **Jumbo Frame**: Configure the maximum frame size, useful for reducing overhead in high-throughput networks.

Each of these settings is aimed at ensuring your network operates optimally by providing controls that apply universally across all switches under management.



Global Switch Configuration

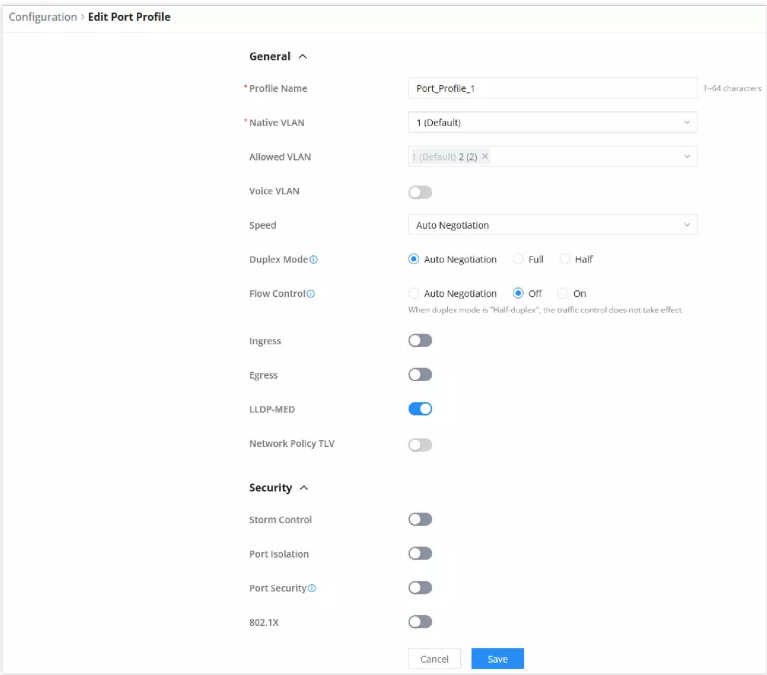
Port Profile

In the **Port Profile** section, you can manage settings that will be applied across multiple switch ports to maintain consistency in configuration. The configuration of port profiles ensures that multiple ports can follow a unified policy or set of rules. Key elements you can configure in this section include:

- **Profile Name**: Assign a custom name to the port profile for easy identification.
- **Native VLAN**: Specify the VLAN that will be considered the default for untagged traffic.
- **Allowed VLAN**: Define which VLANs are allowed on the ports using this profile.
- **Voice VLAN**: Enable and configure a separate VLAN for voice traffic, if needed.

- **Speed**: Set the data transmission speed for the port.
- **Duplex Mode**: Configure the port to operate in full, half-duplex, or auto-negotiation mode.
- **Flow Control**: Manage the ability to control the data flow for traffic congestion.
- **Ingress & Egress**: Control the flow of incoming and outgoing traffic.
- **LLDP-MED**: Enable LLDP-MED to facilitate auto-negotiation for voice and network devices.
- **Security Settings**:
  - **Storm Control**: Prevent traffic storms on the network.
  - **Port Isolation**: Isolate this port to limit communication with other ports.
  - **Port Security**: Set up port-based security to restrict unauthorized devices.
  - **802.1X**: Enable 802.1X for port-based network access control.

Switch – Port Profile

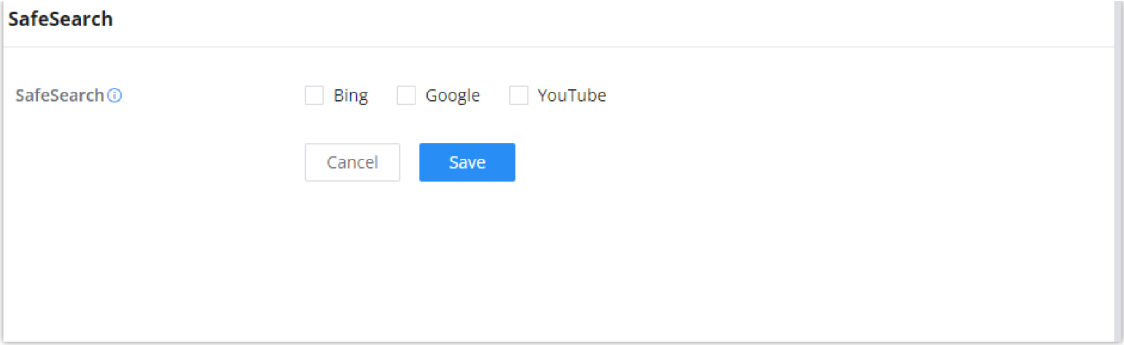


Add/Edit – Port profile

ACCESS CONTROL

SafeSearch

The GWN700X routers offer SafeSearch feature on Bing, Google, and Youtube. Enabling this option will hide any inappropriate or explicit search results from being displayed.



Site Control page

EXTERNAL ACCESS

By default, all the requests initiated from the WAN side are rejected by the router GWN700x external access features allow hosts located on the WAN side to access the services hosted on the LAN side of the GWN router.

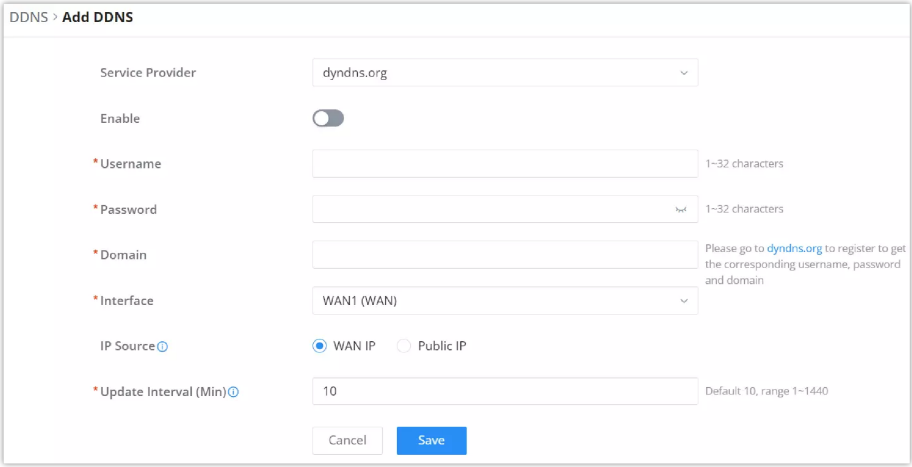
DDNS

Dynamic Domain Name System (DDNS) allows users to map a dynamic IP address to a fixed domain name, making it easier to access devices on networks where the IP address may change. This is especially useful for remote access to networked devices without requiring a static IP.

Grandstream GWN700x routers support DDNS configuration, enabling seamless remote access through a consistent domain name, regardless of IP changes. Key features include:

- **Multiple Provider Support**: Choose from popular DDNS providers to match your existing account.
- **Public IP Detection**: When positioned behind a NAT, the GWN700x can detect and register the public IP address for accurate DDNS updates.
- **Customizable Update Intervals**: Set the frequency of updates to ensure the DDNS server always has the current IP address.
- **Interface Selection**: Specify the WAN interface used for DDNS, allowing flexibility in multi-WAN environments.

These features make the GWN700x routers ideal for environments requiring reliable remote access, even in networks with dynamic IP addresses.



DDNS Page

Field	Description
Service Provider	Dropdown selection of available Dynamic DNS providers (e.g., dyndns.org, changeip.com, etc.). ***Note:*** *Requires registration at the chosen provider's website to obtain the domain, username, and password for DDNS services.*

Enable	Toggle to enable or disable the DDNS service for the selected provider.
Username	Enter the username provided by the DDNS service provider. Range: 1-32 characters.
Password	Enter the password associated with the DDNS service provider. Range: 1-32 characters.
Domain	Enter the domain or hostname to be updated by the DDNS service.
Interface	Select the WAN interface to associate with the DDNS update.
IP Source	Choose between 'WAN IP' or 'Public IP' for the source of IP to send to the DDNS provider. Default: WAN IP. ***Note:*** *Use 'Public IP' if behind a NAT to detect and use the device's public IP address for the DDNS update*
Update Interval (Min)	Set the interval in minutes for updating the IP address of the device to the DDNS server. Default: 10. Range: 1-1440. ***Note:*** *Increasing interval reduces frequency of updates to the DDNS server*

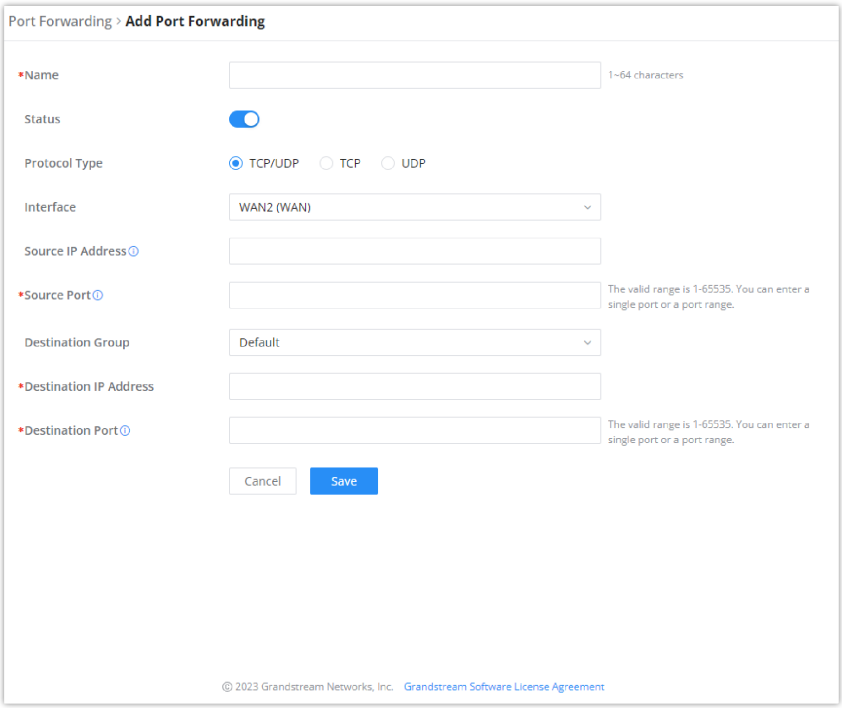
DDNS Page

Port Forward

Port forwarding allows forwarding requested initiated from the WAN side of the router to a LAN host. This is done by configuring either the port only, or the port and the IP address in case we want to restrict the access over that specific port to one IP address. Once the router receives the requested on the IP address, the router will verify the port on which the request has been initiated and will forward the request to the host IP address and the port of the host which is configured as the destination.

Port forwarding can be used in the case when a host on the WAN side wants to access a server on the LAN side.

Navigate to **GWN700x WEB UI → External Access → Port Forward**:



Port Forwarding page

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

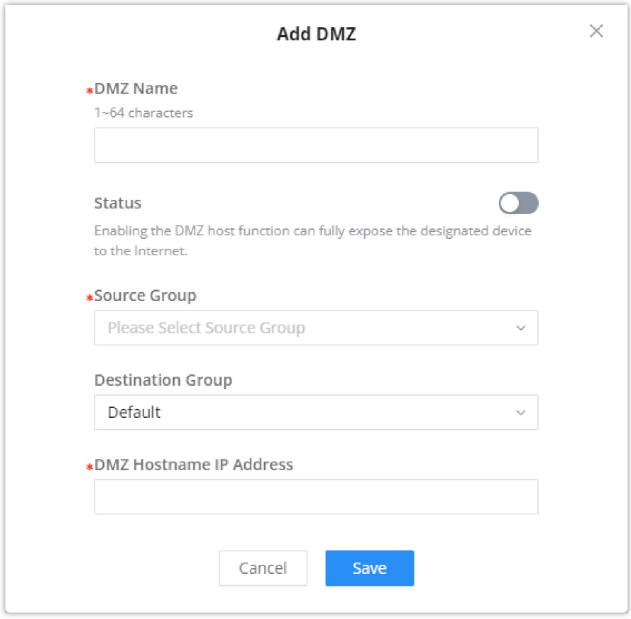
Name	Enter a name for the port forwarding rule.
Status	Toggle on/off the rule status.
Protocol Type	Select a protocol, users can select TCP, UDP or TCP/UDP.
Interface	Select the WAN port
Source IP Address	Sets the IP address that external users access to this device. If not set, any IP address on the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

Port Forwarding page

DMZ

Configuring the DMZ, the router will allow all the external access requests to the DMZ host. This is

This section can be accessed from **GWN700x Web GUI → External Access → DMZ**.
GWN700x supports **DMZ**, where it is possible to specify a Hostname IP Address to be put on the **DMZ**.



DMZ Page

Enabling the DMZ host function, the computer set as the DMZ host can be completely exposed to the Internet, realizing two-way unrestricted communication.

Refer to the below table for DMZ fields:

DMZ Name	Enter a name for the DMZ rule.
Status	Toggle on/off the status of the DMZ rule.

Source Group	Select the interface to allow access to the DMZ host.
Destination Group	Select the VLAN on which the DMZ host belong.
DMZ Hostname IP Address	Enter the DMZ host IP address.

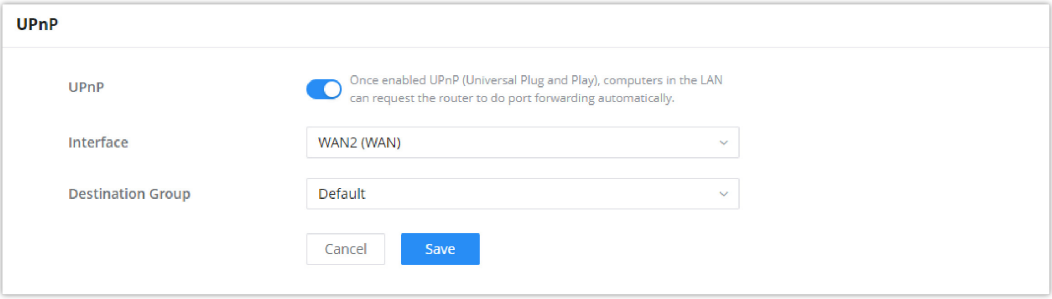
DMZ Page

UPnP

GWN700x supports UPnP that enables programs running on a host to configure automatically port forwarding.

UPnP allows a program to make the GWN700x open necessary ports, without any intervention from the user, without making any check.

UPnP settings can be accessed from GWN700x **Web GUI → External Access → UPnP.**

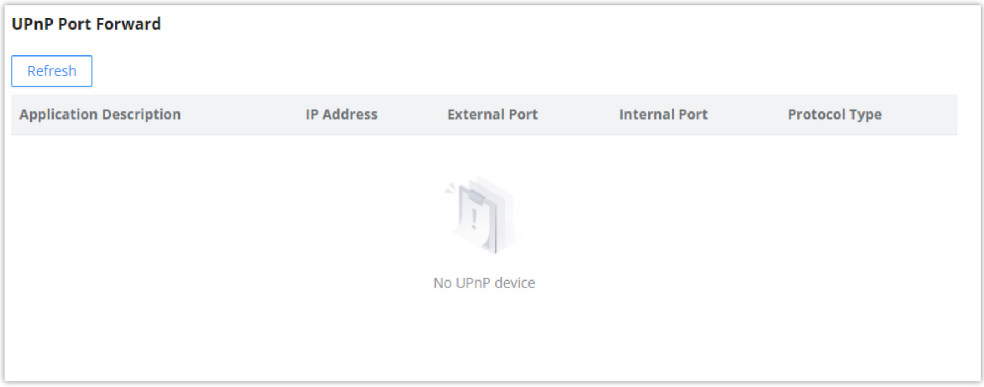


UPnP Settings

UPnP	Click on "**ON**" to enable UPnP. **Note**: Once enabled UPnP (Universal Plug and Play), computers in the LAN can request the router to do port forwarding automatically
Interface	Select the interface (WAN)
Destination Group	Select the LAN Group

UPnP Settings

When UPnP is enabled, the ports will be shown in the section below. The information shown includes application name, IP address of the LAN host which has requested the opening of the port, the external port number, the internet port number, and the transport protocol used (UDP or TCP).

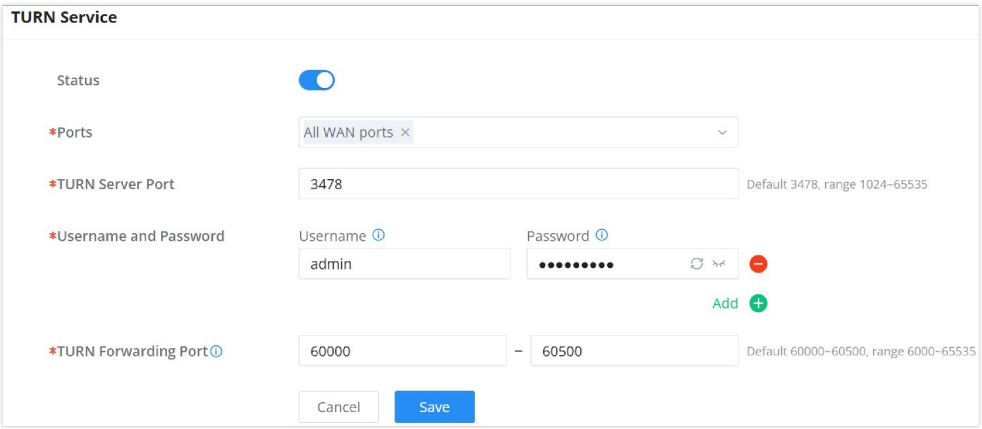


UPnP – Open Ports

TURN Service

TURN stands for Traversal Using Relays around NAT and it's a network service that helps establish peer-to-peer connections between devices that are behind a NAT or Firewall. Real-time communication like video conferencing, Voice over IP, etc benefit from TURN service to establish connections between peers when the NAT or the Firewall block or modify the traffic.

Navigate to **Web UI** → **External Access** → **TURN Service**. The service is OFF by default, toggle Status ON to turn on the service. The default TURN Server Port is 3478, also it's possible to add or remove username and password by clicking on "**minus**" and "**Plus**" icons.



TURN Service

Note:

- Turn Server port is by default 3478.
- For Turn Forwarding Port: do not modify the forwarding port range unless necessary. Ensure that the ports used by other services do not conflict with the TURN forwarding ports.
- TURN service is a NAT traversal solution for UC in private network and a VoIP media traffic NAT traversal gateway for Grandstream UCM and Wave.

FIREWALL

The Firewall in GWN routers enables the user to secure the network by blocking the most common attacks and allowing for more control over the traffic.

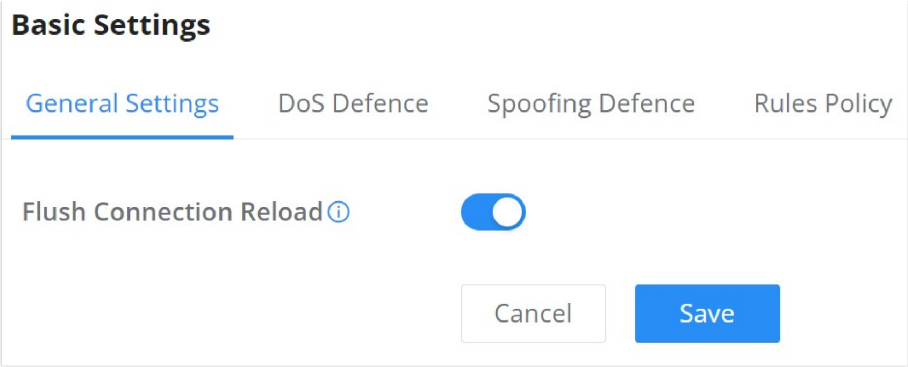
The Firewall section provides the ability to set up input/output policies for each WAN interface and LAN group as well as setting configuration for Static and Dynamic NAT and ALG.

Firewall – Basic Settings

General Settings

- **Flush Connection Reload**

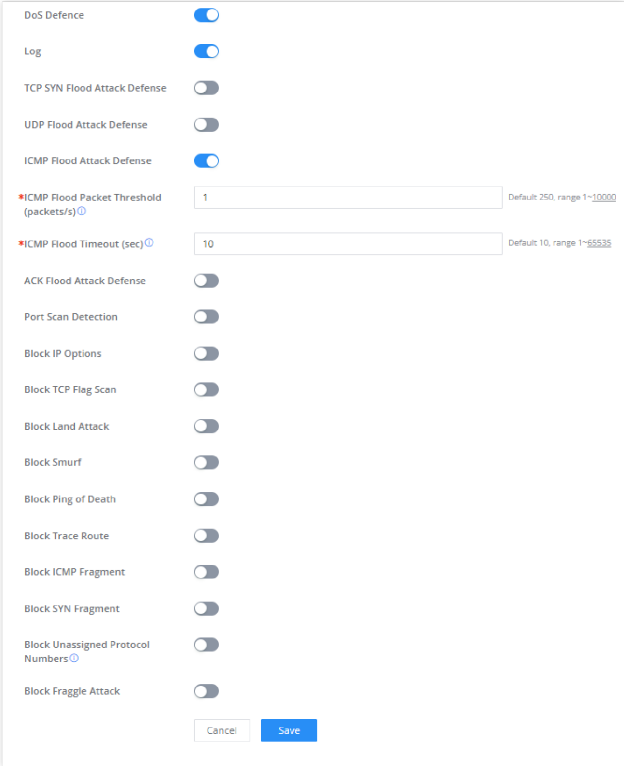
When this option is enabled and the firewall configuration changes are made, existing connections that had been permitted by the previous firewall rules will be terminated.
If the new firewall rules do not permit a previously established connection, it will be terminated and will not be able to reconnect. With this option disabled, existing connections are allowed to continue until they timeout,even if the new rules would not allow this connection to be established.



Firewall Basic Settings

DoS Defense

Denial-of-Service Attack is an attack aimed to make the network resources unavailable to legitimate users by flooding the target machine with so many requests causing the system to overload or even crash or shutdown.



DoS Defense

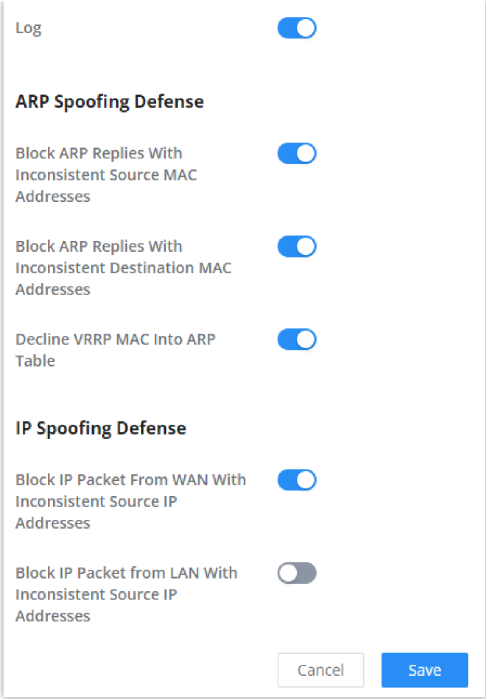
DoS Defence	Toggle on/off DoS Defence
Log	When this option is enabled, all the attempts of the attacks below will be recorded in a log.
TCP SYN Flood Attack Defense	When this option is enabled, the router will take counter measures to SYN Flood Attack. ● **TCP SYN Flood Packet Threshold (packets/s):** If the threshold of the TCP SYN packets from the Internet has exceeded the defined value, subsequent TCP SYN packets will be discarded within the specified timeout period. ● **TCP SYN Flood Timeout (sec):** If the number of TCP SYN packets received per second exceeds the threshold within the specified timeout period, attack defense will start immediately.
UDP Flood Attack Defense	When this option is enabled, the router will take counter measures to the UDP Flood Attack. ● **UDP Flood Packet Threshold (packets/s):** If the threshold of the UDP packets from the Internet has exceeded the defined value, subsequent UDP packets will be discarded within the specified timeout period.

	● **UTCP SYN Flood Timeout (sec):** If the average number of received UDP packets per second reaches the threshold within the timeout period, attack defense will start immediately.
ICMP Flood Attack Defense	When this option is enabled, the router will take counter measures to the ICMP Flood Attack. ● **ICMP Flood Packet Threshold (packets/s):** If the threshold of the ICMP packets from the Internet has exceeded the defined value, subsequent ICMP packets will be discarded within the specified timeout period. ● **ICMP Flood Timeout (sec):** If the average number of received ICMP packets per second reaches the threshold within the timeout period, attack defense will start immediately.
ACK Flood Attack Defense	When this option is enabled the router will take counter measures to ACK Flood Attack. ● **ACK Flood Packet Threshold (packets/s):** If the threshold if the ACK packets from the Internet has exceeded the defined value, subsequent ACK packets will be discarded within the specified timeout period. ● **ACK Flood Timeout (sec):** If the average number of received ACK packets per second reaches the threshold within the timeout period, attack defense will start immediately.
Port Scan Detection	When this option is enabled, the router will take counter measure to the port scanning attempts ● **Port Scan Packet Threshold (packets/s):** If the port packets reach the threshold, port scanning detection will start immediately.
Block IP Options	When this option is enabled, the router will ignore any IP packets with Options field.
Block TCP Flag Scan	When this option is enabled, the router will ignore any packets with unexpected information in the TCP flags.
Block Land Attack	When this option is enabled, the router will block any SYN packets which may have been spoofed and modified to set the source and the destination address to the address of the router. If this option is disabled, it might cause the router to be stuck in a loop of responding to itself.
Block Smurf	When this option is enabled, the router will drop any ICMP echo requests.
Block Ping of Death	When this option is enabled, the router will drop any abnormal or corrupted ping packets.
Block Traceroute	When this option is enabled, the router will not allow the traceroute requests initiated from the WAN side.
Block ICMP Fragment	When this option is enabled, the router will drop the ICMP packets which are fragmented.
Block SYN Fragment	When this option is enabled, the router will drop the SYN packets which are fragmented.
Block Unassigned Protocol Numbers	If enabled, the device will reject IP packets receiving IP protocol number greater than 133.
Block Fraggle Attack	If enabled, the router will drop any UDP broadcast packets initiate from the WAN side.

DoS Defense

Spoofing Defense

Spoofing defense section offers a number of counter-measures to the various spoofing techniques. To protect your network against spoofing, please enable the following measures in order to eliminate the risk of having your traffic intercepted and spoofed. GWN routers offer measures to counter spoofing on ARP information, as well as on IP information.



Spoofing Defense

ARP Spoofing Defense

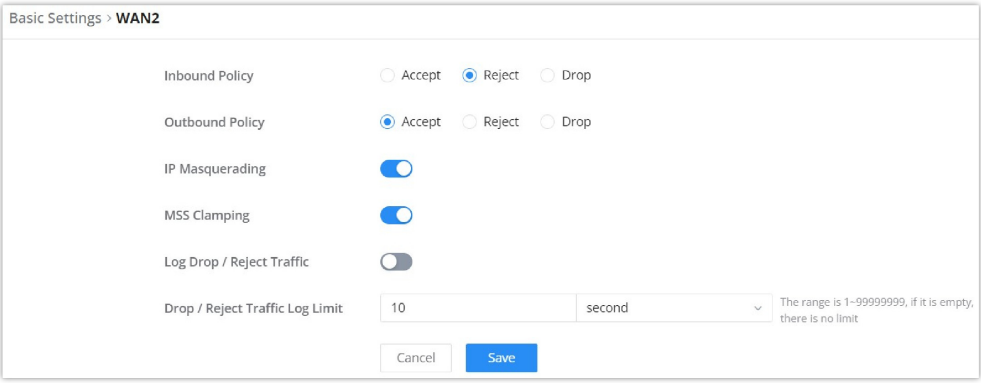
- **Block ARP Replies with Inconsistent Source MAC Addresses:** The router will verify the destination MAC address of a specific packet, and when the response is received by the router, it will verify the source MAC address and it will make sure that they match. Otherwise, the router will not forward the packet.
- **Block ARP Replies with Inconsistent Destination MAC Addresses:** The router will verify the source MAC address and when the response is received. The router will verify the destination MAC address and it will make sure that they match. Otherwise, the router will not forward the packet.
- **Decline VRRP MAC Into ARP Table:** The router will decline including any generated virtual MAC address in the ARP table.

IP Spoofing Defense

- Block IP Packet From WAN with Inconsistent Source IP Addresses: The router will verify the the IP address of the inbound packets, the source IP address has to match the destination IP address to which the request was initially sent to. If there is a mismatch between these two IP addresses, the router will drop the packet.
- Block IP Packet from LAN With Inconsistent Source IP Address: The router will verify the IP address of the packets forwarded. If the router discovers that there is a mismatch in the packet source IP address, the packet will not be forwarded.

Rules Policy

Rules policy allows to define how the router is going to handle the traffic based on whether it is inbound traffic or outbound traffic. This is done per WAN port as well as LAN ports of the router.



Rules Policy

- **Inbound Policy:** Define the decision that the router will take for the traffic initiated from the WAN. The options available are Accept, Reject, and Drop.
- **Outbound Traffic**: Define the decision that the router will take for the traffic initiated from the LAN side. The options available are Accept, Reject, and Drop.
- **IP Masquerading:** Enable IP masquerading. This will masque the IP address of the internal hosts.
- **MSS Clamping**: Enabling this option will allow the MSS (Maximum Segment Size) to be negotiated during the TCP session negotiation
- **Log Drop / Reject Traffic**: Enabling this option will generate a log of all the traffic that has been dropped or rejected.

Content Security

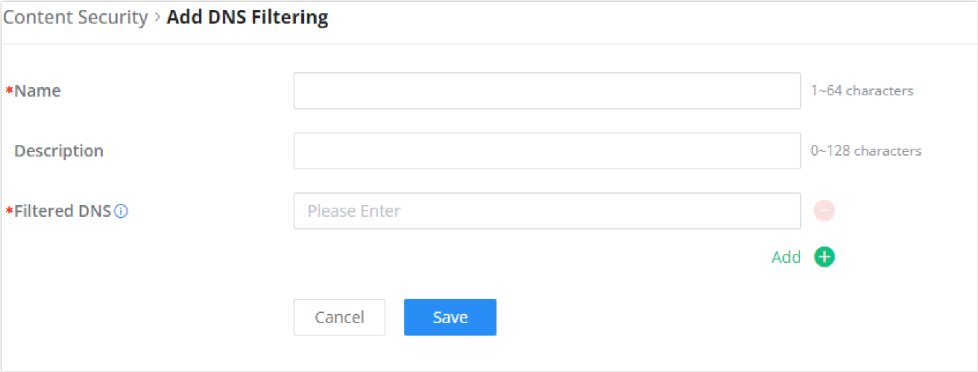
The content security feature on GWN700x routers uses DPI (Deep Packet Inspection) to allow users to filter (accept, deny or drop packets) content based on DNS, APP or URL. DNS and URL filtering uses keywords and wildcard * (which can represent any string) while APP filtering works by selecting APPs from a list organized in categories.

For more details about how to block (filter) DNS, APPs and URL, please visit the link below:

documentation.grandstream.com/knowledge-base/gwn700x-firewall-content-security

DNS Filtering

When DNS filtering is enabled, the router will filter the DNS requests initiated by the LAN hosts disallow the requests which match the queries which contains the strings and patterns specified in "Filtered DNS" field. To access DNS filtering, please access the web UI of the router then navigate to **Firewall → Content Security → DNS Filtering**.



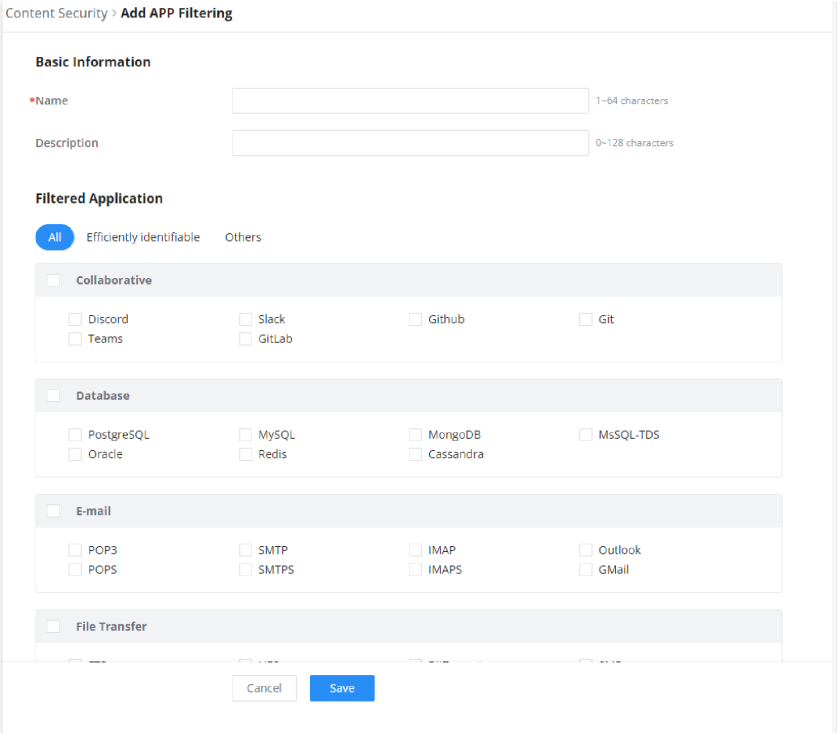
Add DNS Filtering

Name	Enter a name for the filtering rule.
Description	Enter a description for the filtering rule
Filtered DNS	Enter keywords and wildcard characters * (which can represent any string). Wildcard * can only be added before or after the input keyword, for example: *.imag, news*, *news*. Please enter a valid domain name, not an IP address.

Add DNS Filtering

APP Filtering

The user can restrict application(s) from accessing Internet. To restrict applications from accessing internet, please access the web UI of the router then navigate to **Firewall → Content Security → APP Filtering** and check the boxes of the applications then click "Save".



App Filtering

Enter the name of the rule along with the description, then choose the application which will be restricted from accessing the Internet. The user can choose the applications from two categories, “Efficiently Identifiable” application and “Others”. The first category can be quickly identifiable from a single network packet, while the second category require multiple packet inspection before the application is identified and blocked.

Note

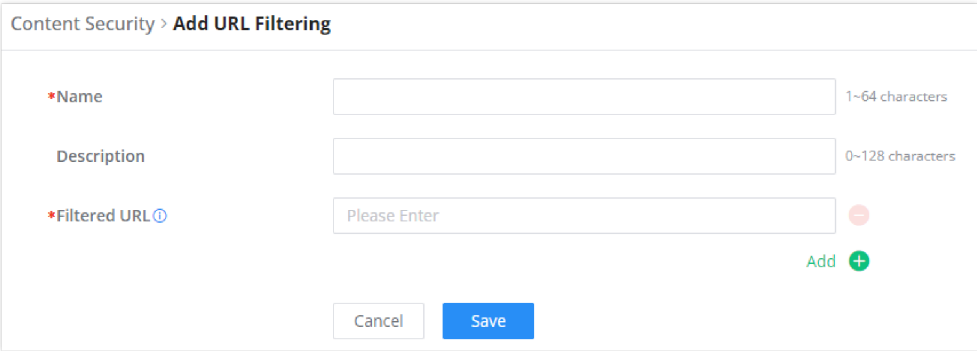
As the traffic keeps being generated by the applications on the network, the router will identify efficiently. Therefore, the list will be updated continuously.

URL Filtering

The user can restrict accessing to specific URLs by configuring this option. Enter the URL(s) in “Filter URL” field.

Note

Please note that URL Filtering feature is still in beta testing phase.



Add URL Filtering

Name	Enter a name for the URL Filtering rule.
Description	Enter a description for the URL Filtering rule.

Filtered URL	Enter keywords and wildcard characters * (which can represent any string). Wildcard * can only be added before or after the input keyword, for example: *.imag, news*, *news*. Only unencrypted http pages/requests are supported. https is not supported.

Add URL Filtering

Traffic Rules

GWN700x offers the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times and take actions for specified rules such as Accept, Reject and Drop.

Traffic Rules settings can be accessed from **GWN700x Web GUI → Firewall → Traffic Rules.**

Following actions are available to configure Input, output, and forward rules for configured protocols

- To add new rule, click on "**Add**" button .
- To edit a rule, click on "**Edit**" icon .
- To delete a rule, click on "**Delete**" icon .

Inbound Rules

The Inbound Rules page of the Grandstream GWN router's firewall settings is used to manage and configure the incoming traffic rules for the device. These rules are crucial for controlling which types of traffic are permitted or denied when entering the network through external sources or terminals.

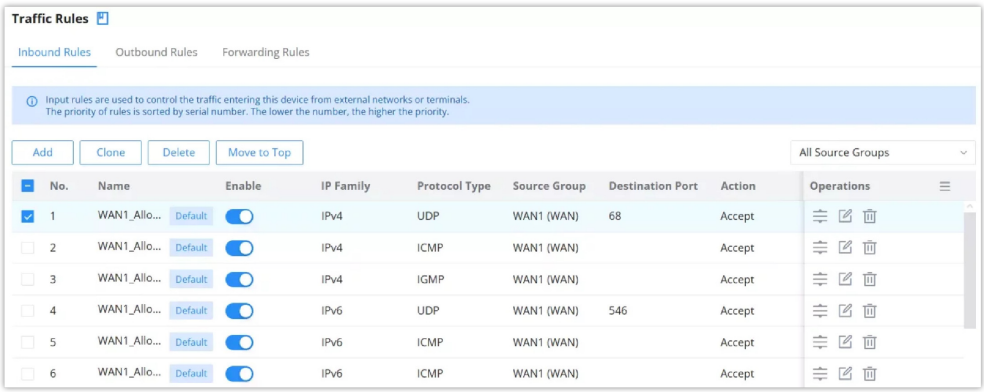
• **Accept:** To allow the traffic to go through.

• **Deny:** A reply will be sent to the remote side stating that the packet is rejected.

• **Drop:** The packet will be dropped without any notice to the remote side.

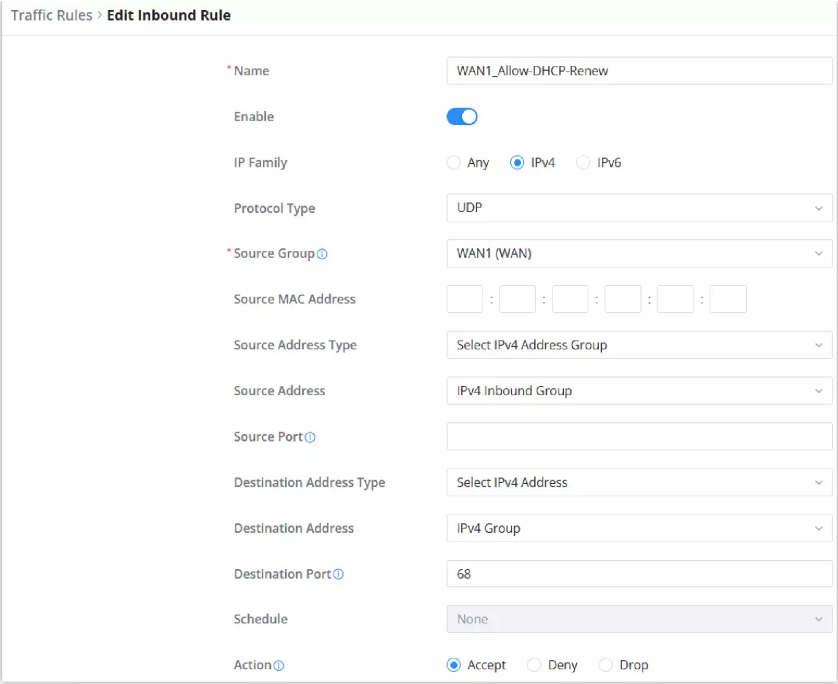
Alert:

- These inbound rules help define what external traffic can reach the internal network. Proper configuration ensures that necessary communication (such as DHCP and diagnostic pings) is allowed, while potentially harmful or unnecessary traffic can be restricted.
- The presence of a rule like Anti-lockout-Rule is crucial as it prevents administrative lockout, ensuring continued access to the router.
- Rules are sorted by priority, with a lower number indicating higher priority.

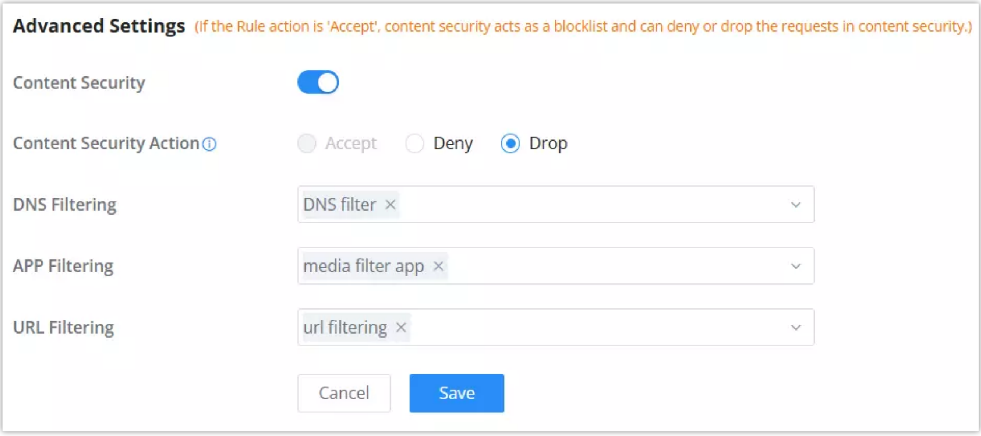


Traffic Rules – Inbound Rules page

- **Clone**: You can also duplicate a rule by clicking the "**Clone**" button, allowing you to create a copy that can be easily modified as needed.
- **Move to Top:** the priority of the rules are from the top to bottom, based on the "**No.**" the lower the number, the higher the priority, and the user can priorities any rule by clicking on "**Move to Top**" button giving the rule higher priority.



Traffic Rules – Add/Edit Inbound Rules – Part 1



Traffic Rules – Add/Edit Inbound Rules – Part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. ● **UDP** ● **TCP** ● **UDP/TCP** ● **ICMP** ● **IGMP** ● **All**
Source Group	Indicates the source network or interface (e.g., WAN1, WAN2 or VLAN or VPN) from which traffic originates. ***Note:*** *When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.*
Source MAC Address	Option to filter traffic by the MAC address of the source device.

Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Destination Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.
Destination Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.
Schedule	Optional field for scheduling when the rule is active (e.g., specific times or days). ***Note:*** *The absolute date/time set will not take effect in the schedule.*
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.
Advanced Settings ***Note:*** *If the Rule action is '**Accept**', content security acts as a blocklist and can deny or drop the requests in content security.*	
Content Security	Toggle switch to enable or disable content security filtering.
Content Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).
DNS Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).
APP Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.
URL Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.

Traffic Rules – Inbound Rules

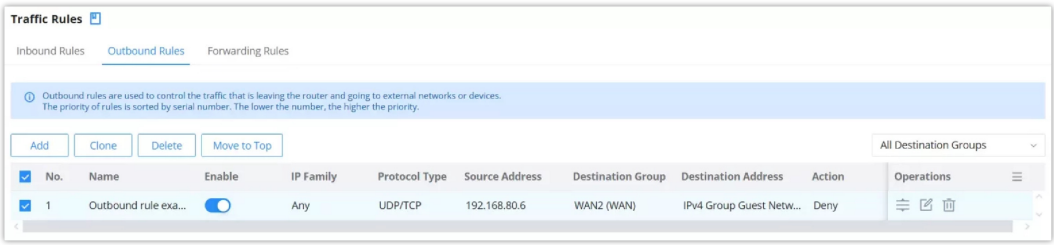
Outbound Rules

The GWN700x allows to filter outgoing traffic from the local LAN networks to outside networks and apply rules such as:

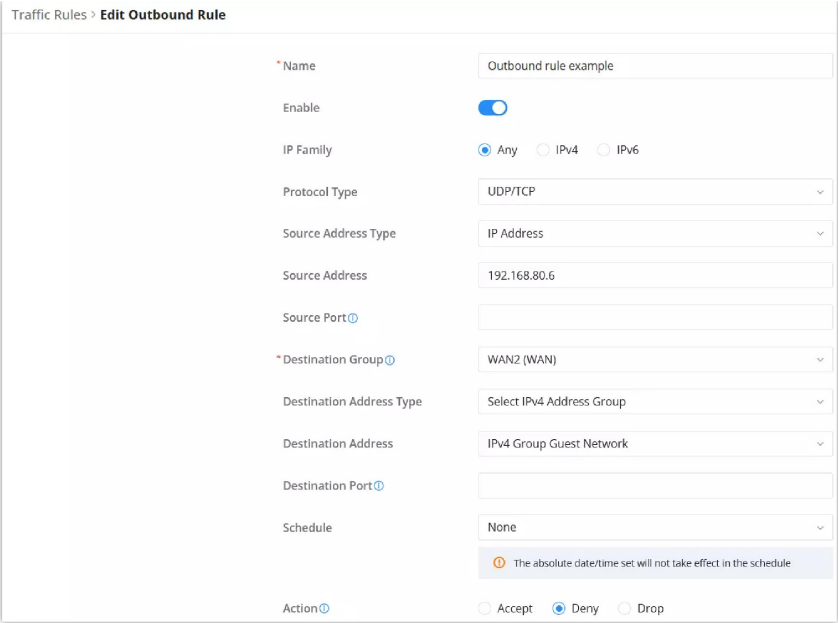
• **Accept:** To allow the traffic to go through.

• **Deny:** A reply will be sent to the remote side stating that the packet is rejected.

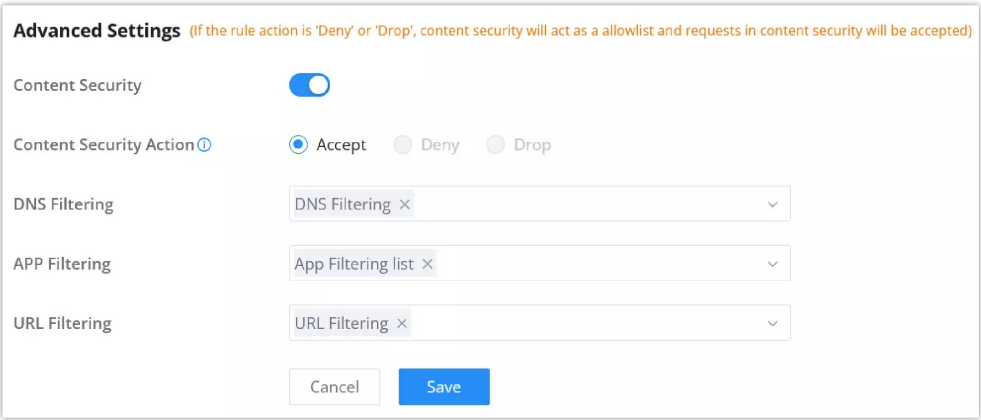
• **Drop:** The packet will be dropped without any notice to the remote side.



Traffic Rules – Outbound Rules



Traffic Rules – Add/Edit outbound Rules – Part 1



Traffic Rules – Add/Edit outbound Rules – Part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. • **UDP** • **TCP** • **UDP/TCP** • **ICMP** • **IGMP** • **All**
Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source MAC Address	Option to filter traffic by the MAC address of the source device.
Source Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.

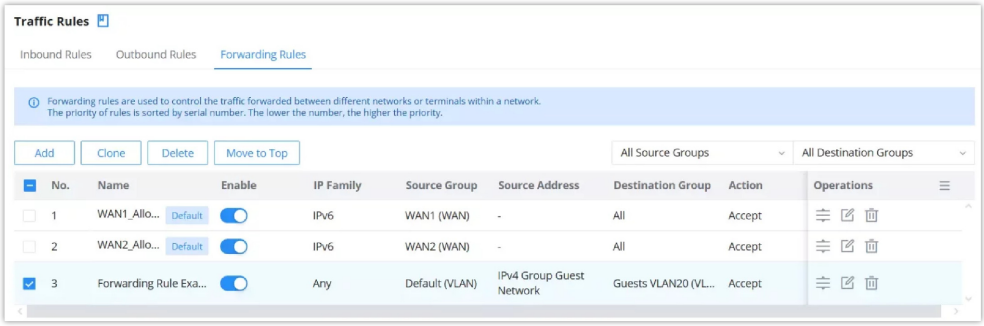
Destination Group	Indicates the destination network or interface (e.g., WAN1, WAN2 or VLAN or VPN). ***Note:*** *When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.*
Destination Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.
Destination Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.
Schedule	Optional field for scheduling when the rule is active (e.g., specific times or days). ***Note:*** *The absolute date/time set will not take effect in the schedule.*
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.
Advanced Settings ***Note:*** *If the Rule action is '**Accept**', content security acts as a blocklist and can deny or drop the requests in content security.*	
Content Security	Toggle switch to enable or disable content security filtering.
Content Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).
DNS Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).
APP Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.
URL Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.

Traffic Rules – Outbound Rules

Forwarding Rules

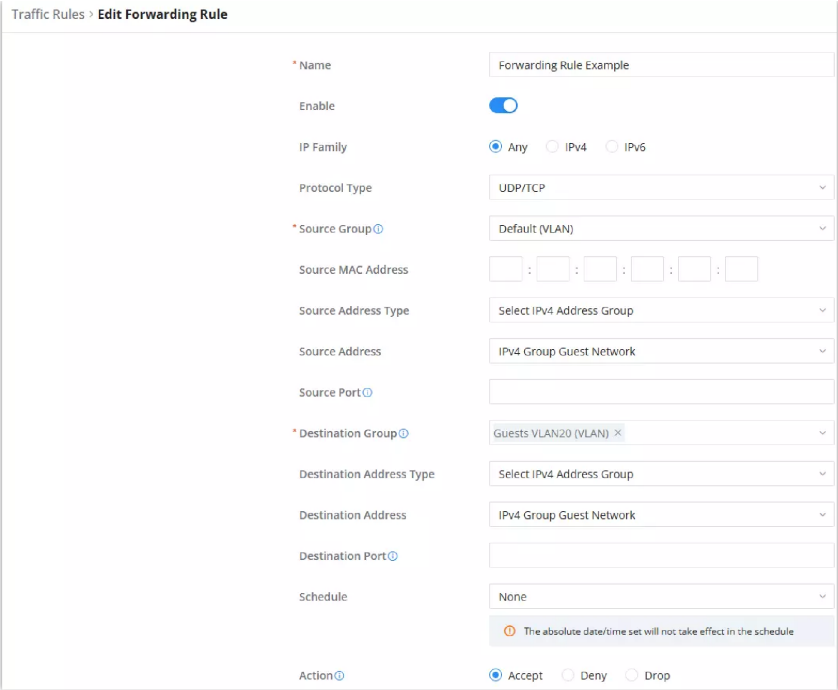
Forwarding rules control traffic flow between different networks (WAN, VLAN or VPN) or devices within a network, allowing administrators to manage access and enforce security policies. Each rule specifies conditions for traffic, such as source and destination groups, protocol types, and actions (e.g., **Accept**, **Deny**, or **Drop**).

Rules are prioritized by serial number—the lower the number, the higher the priority. This order ensures that high-priority rules are applied first, enabling precise control over network traffic and security. Advanced settings, like content and application filtering, offer additional layers of control for accepted traffic.

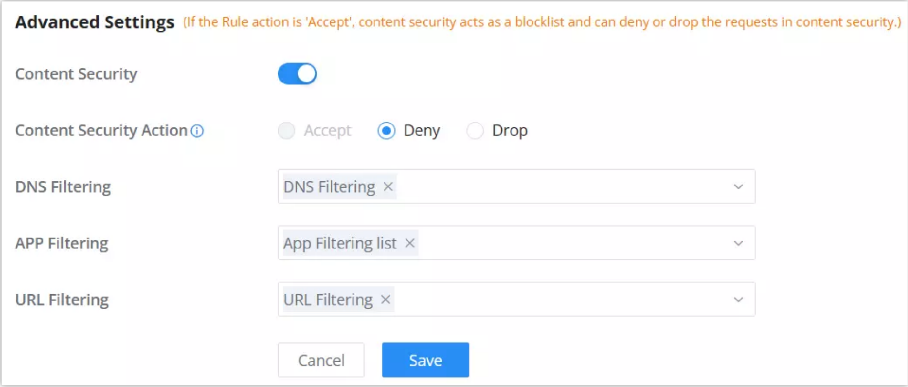


Traffic Rules – Forward Rules page

Click **Add** to create a new forwarding rule or **Edit** (pencil icon) next to an existing rule to modify it.



Traffic Rules – Add/Edit Forward Rules part 1



Traffic Rules – Add/Edit Forward Rules part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. ● **UDP** ● **TCP** ● **UDP/TCP** ● **ICMP** ● **IGMP** ● **All**
Source Group	Indicates the source network or interface (e.g., WAN1, WAN2 or VLAN or VPN) from which traffic originates. ***Note:*** *When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.*
Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source MAC Address	Option to filter traffic by the MAC address of the source device.

Source Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Destination Group	Indicates the destination network or interface (e.g., WAN1, WAN2 or VLAN or VPN). ***Note:*** *When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.*
Destination Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.
Destination Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.
Schedule	Optional field for scheduling when the rule is active (e.g., specific times or days). ***Note:*** *The absolute date/time set will not take effect in the schedule.*
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.
Advanced Settings ***Note:*** *If the Rule action is '**Accept**', content security acts as a blocklist and can deny or drop the requests in content security.*	
Content Security	Toggle switch to enable or disable content security filtering.
Content Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).
DNS Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).
APP Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.
URL Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.

Traffic Rules – Forwarding Rules

Advanced NAT

NAT or Network address translation as the name suggests it's a translation or mapping private or internal addresses to public IP addresses or vice versa, and the GWN routers support both.

- **SNAT :** Source NAT refers to the mapping of clients IP address (Private or Internal Addresses) to a public one.
- **DNAT :** Destination NAT is the reverse process of SNAT where packets will be redirected to a specific internal address.

The Firewall Advanced NAT page provides the ability to set up the configuration for Static and Dynamic NAT.

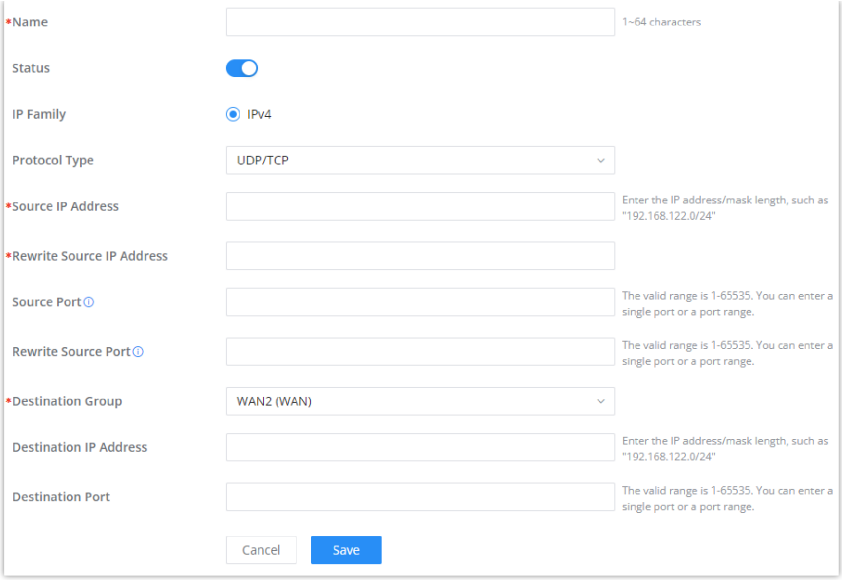
SNAT

Following actions are available for SNAT.

Click on + Add to add the Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.



SNAT page

Refer to the below table when creating or editing a SNAT entry:

Name	Specify a name for the SNAT entry
IP Family	Select the IP version, two options are available: IPv4 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP/TCP, UDP, TCP and All.
Source IP Address	Set the Source IP address.
Rewrite Source IP Address	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
Source Port	Set the Source Port
Rewrite Source Port	Set the Rewrite source port.
Destination Group	Select a WAN interface or a VLAN for Destination Group.
Destination IP Address	Set the Destination IP address.
Destination Port	Set the Destination Port

SNAT page

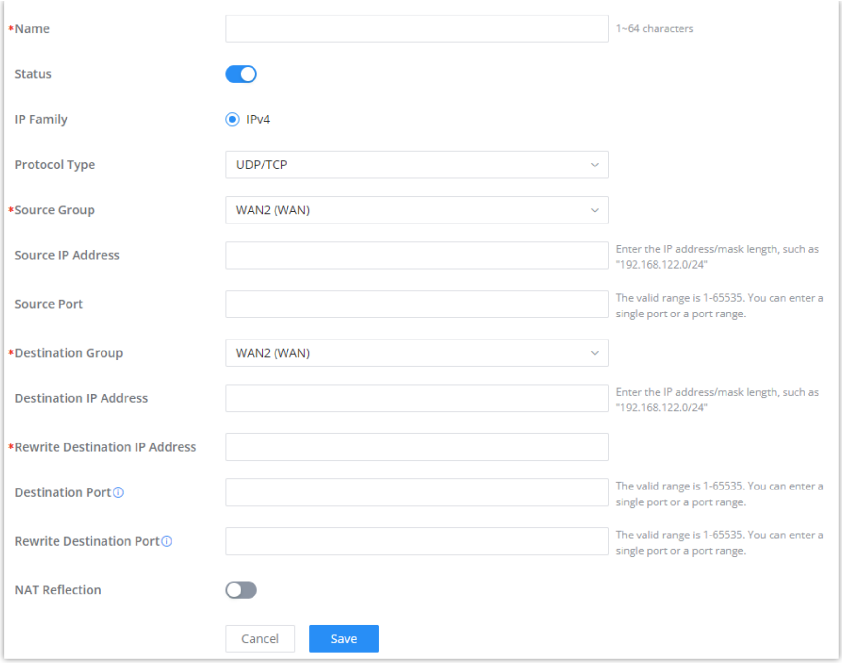
DNAT

The following actions are available for DNAT:

Click on + Add to add the Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.



Advanced NAT – DNAT

Refer to the below table when creating or editing a DNAT entry:

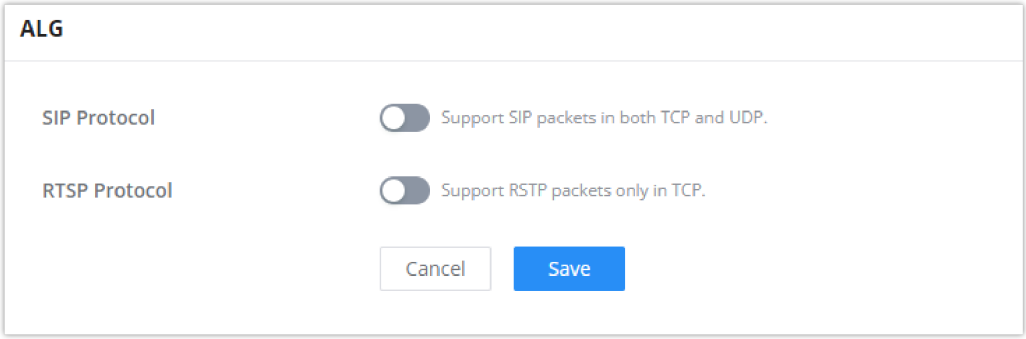
Name	Specify a name for the DNAT entry
IP Family	Select the IP version, three options are available: IPv4, IPv6 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
Source Group	Select a WAN interface or a LAN group for Source Group, or select All.
Source IP Address	Set the Source IP address.
Source Port	Set the Source Port.
Destination Group	Select a WAN interface or a LAN group for Destination Group, or select All. Make sure that destination and source groups are different to avoid conflict.
Destination IP Address	Set the Destination IP address.
Rewrite Destination IP Address	Set the Rewrite Destination IP Address.
Destination Port	Set the Destination Port.
Rewrite Destination Port	Set the Rewrite Destination Port
NAT Reflection	Click on "**ON**" to enable NAT Reflection
NAT Reflection Source	Select NAT Reflection either Internal or External.

Advanced NAT – DNAT

ALG

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

Navigate to **Web GUI** → **Firewall** → **ALG** to activate ALG.



ALG

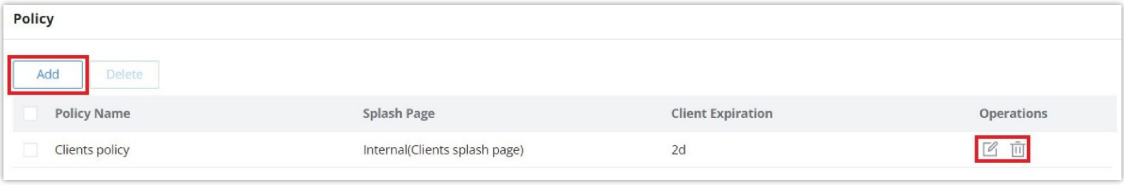
CAPTIVE PORTAL

Captive Portal feature on GWN700x helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access the Internet. Once connected Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

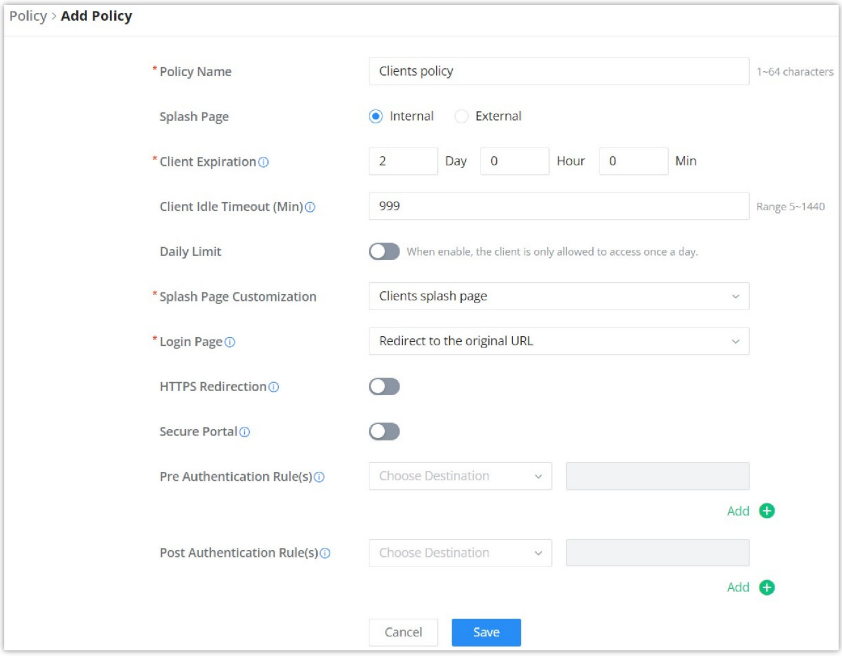
The Captive Portal feature can be configured from the GWN700x Web page under "**Captive Portal**".

Policy

Users can customize a portal policy on this page. Click on "**Add**" button to add new policy or click on "**Edit**" to edit previously added one.



Policy page



Policy page

The policy configuration page allows for adding multiple captive portal policies which will be applied to SSIDs and contain options for different authentication types.

Policy Name	Enter a policy name.
Splash Page	• **Internal** • **External**
Client Expiration	Specify the expiration time for client network connection. Once timed out, client should re-authenticate for further network use.
Client Idle Timeout (min)	Specify the idle timeout value for guest network connection. Once timed out, guest should re-authenticate for further network use.
Daily Limit	When enable, the client is only allowed to access once a day.
Splash Page Customization	Select the customized splash page.
Login Page	Set portal authentication through the page to automatically jump to the target page.
HTTPS Redirection	If enabled, both HTTP and HTTPS requests sent from stations will be redirected by using HTTPS protocol. And station may receive an invalid certification error while doing HTTPS browsing before authentication. If disabled, only the http request will be redirected.
Secure Portal	If enabled, HTTPS protocol will be used in the communication between STA and router. Otherwise, the HTTP protocol will be used.
Pre Authentication Rule (sec)	Set pre authentication rules, allowing clients access some URLs before authenticated successfully.
Post Authentication Rule (sec)	Set post authentications to restrict users from accessing the following addresses after authenticating successfully.

Policy page

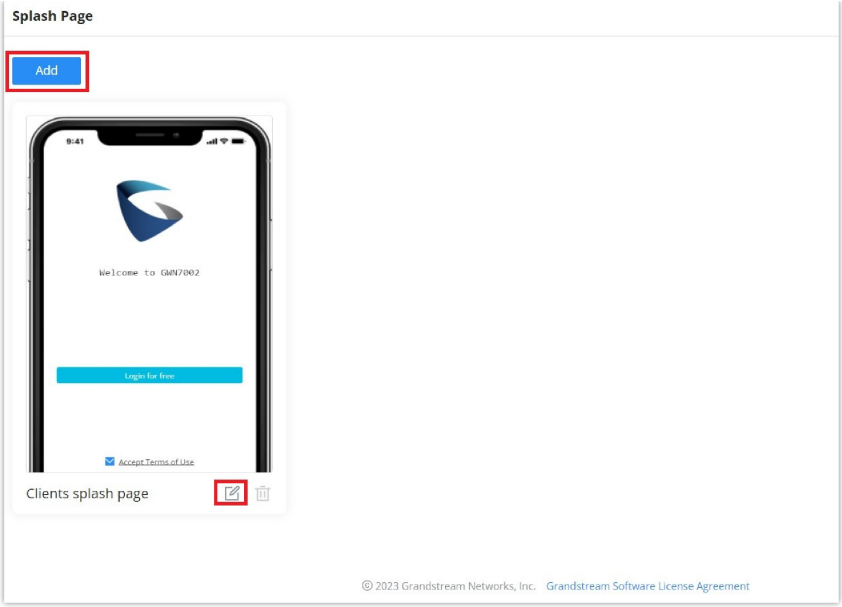
Splash Page

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

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

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

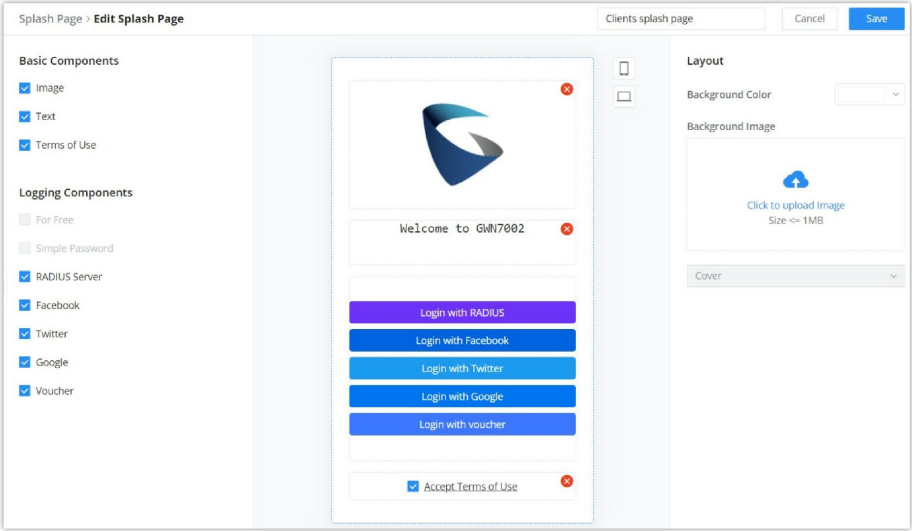
To add a splash page, click on “**Add**” button or click on “**Edit**” icon to edit previously added one.



Splash Page

Users can set the following:

- **Authentication type**: Add one or more ways from the supported authentication methods (Simple Password, Radius Server, For Free, Facebook, Twitter, Google and Voucher).
- **Set up a picture (company logo**) to be displayed on the splash page.
- **Customize** the layout of the page and background colors.
- **Customize the Terms of use text.**
- **Visualize a preview** for both mobile devices and laptops.

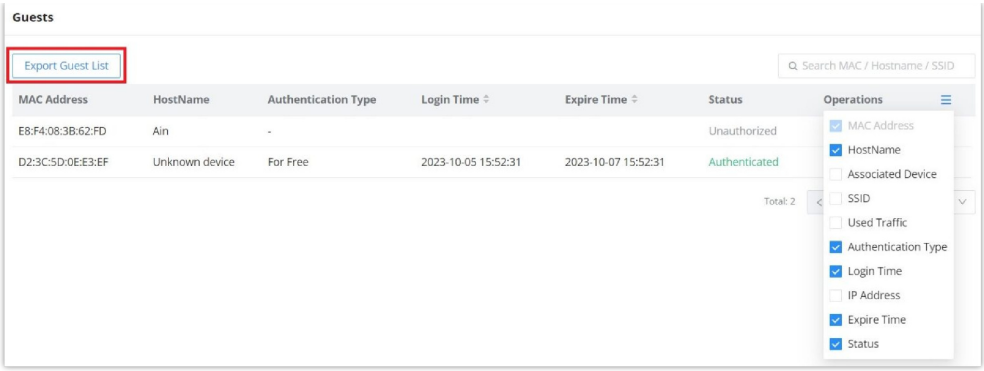


Add/edit a Splash page

Guests

This page displays information about the clients connected via Captive portal including the MAC address, Hostname, Authentication Type, etc.

To export the list of all guests, please click on "**Export Guest List**" button, then an EXCEL file will be downloaded.



Guest Page

Vouchers

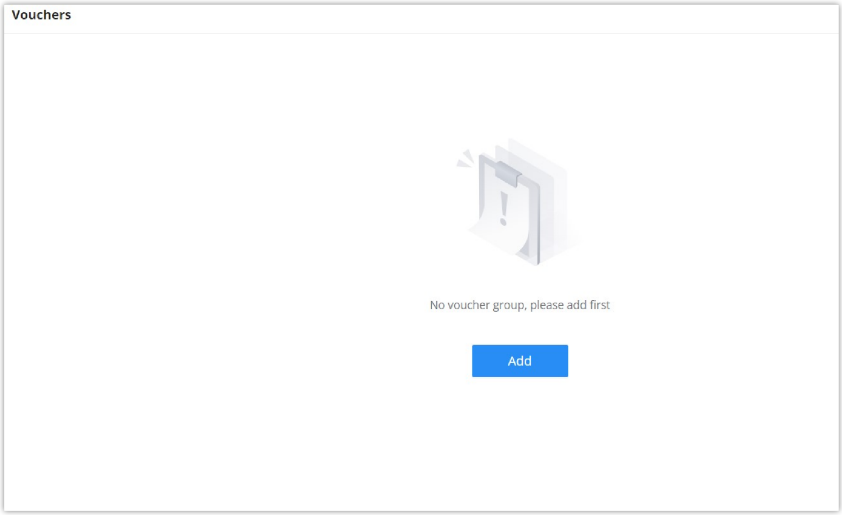
Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from platform controller.

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

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

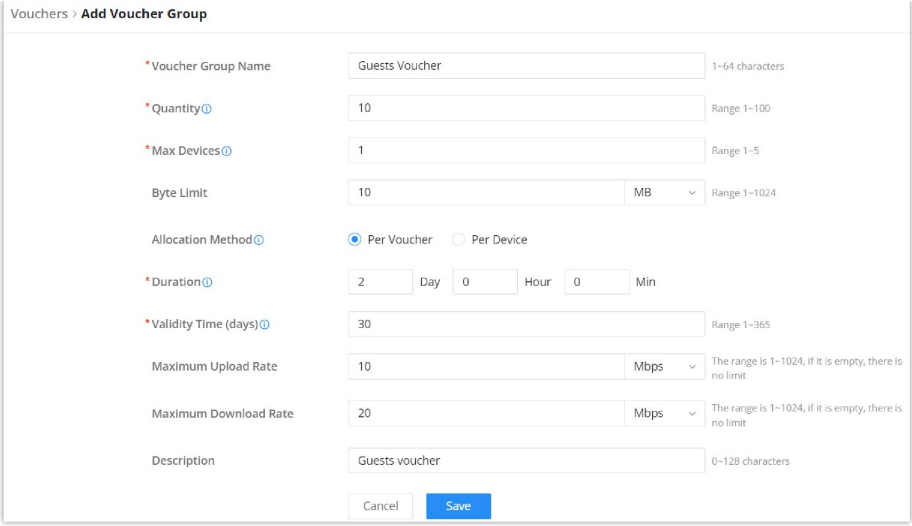
Another interesting feature is that the admin can set data bandwidth limitation on each created voucher depending on the current load on the network, users' profile (VIP customers get more speed than regular ones etc....) and the internet connection available (fiber, DSL or cable etc....) to avoid connection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

Click on "**Add**" button to create a voucher group.



Voucher page

Please refer to the figure below when filling up the fields.



Add/Edit Voucher

Note:

Clients connected trough captive portals including vouchers will be listed on the Guests page under **Captive Portal** → **Guests**.

MAINTENANCE

GWN700x offers multiple tools and options for maintenance and debugging to help further troubleshooting and monitoring the GWN700x resources.

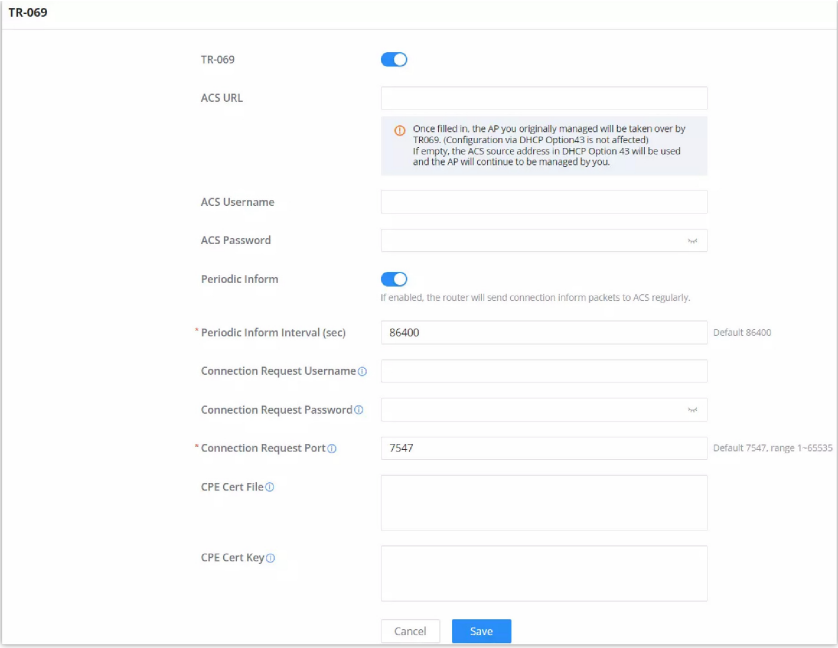
TR-069

It is a protocol for communication between CPE (Customer Premise Equipment) and an ACS (Auto Configuration Server) that provides secure auto-configuration as well as other CPE management functions within a common framework.

TR-069 stands for a "Technical Report" defined by the Broadband Forum that specifies the CWMP "CPE WAN Management Protocol". It commonly uses HTTP or HTTPS as transport for communication between CPE and the ACS. The message exchange is using SOAP (XML_RPC) for configuration and management of the device.

Important Note

Once populated, the AP you initially managed will be taken over by TR-069 (Configuration via DHCP Option 43 remains unaffected). If left blank, the ACS source address in DHCP Option 43 will be used, allowing the AP to continue being managed by you.



TR-069 page

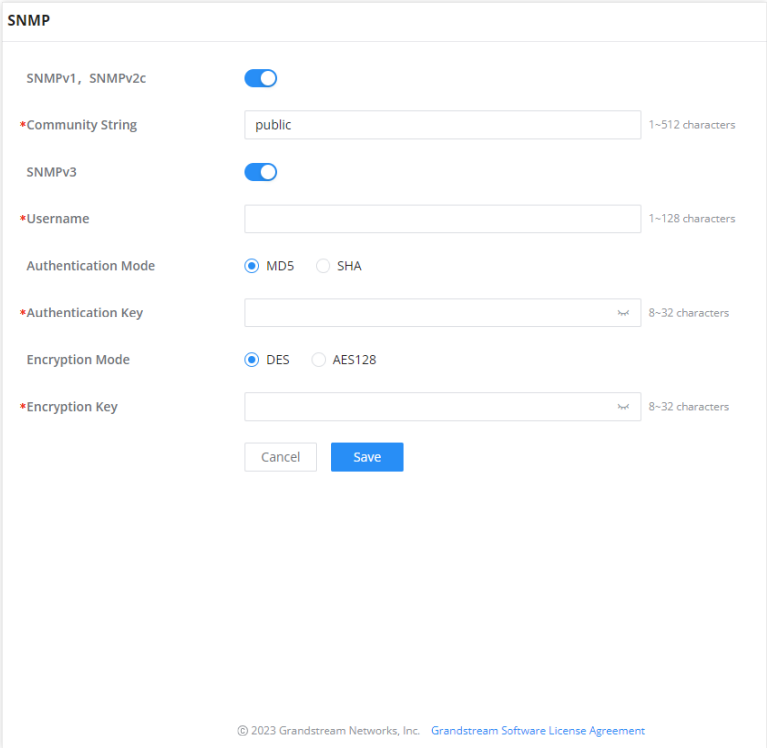
TR-069	Enable/disable TR-069 *TR-069 is enabled by default.*
ACS URL	Enter the FQDN or the IP address of the ACS server. ***Note:*** *If it is empty, the ACS source address in DHCP Option 43 is preferred.*
ACS Username	Enter the username.
ACS Password	Enter the password.
Periodic Inform	If enabled, the router will send connection inform packets to ACS regularly.
Periodic Inform Interval (sec)	This configures the time duration between each inform sent by the device to the ACS server. *Default is 86400.*
Connection Request Username	When ACS server sends a connection request to the router, the username that the router authenticates ACS must be consistent with the configuration of ACS side.
Connection Request Password	The password that the router authenticates ACS must be consistent with the configuration of ACS server.
Connection Request Port	The port for ACS to send connection request to the router. This port cannot be occupied by other device features. *Default is 7547.*
CPE Cert File	Enter the certificate that the router needs to use when connecting to ACS through SSL.
CPE Cert Key	Enter the certificate key that the router needs to use when connecting to ACS through SSL.

TR-069 page

SNMP

GWN700x routers support SNMP (Simple Network Management Protocol) which is widely used in network management for network monitoring for collecting information about monitored devices.

To configure SNMP settings, go to **GWN700x Web GUI → Maintenance → SNMP**, in this page the user can either enable SNMPv1, SNMPv2c, or enable SNMPv3, and enter all the necessary parameters.



SNMP

To configure SNMPv1 or SNMPv2, please refer to the table below:

SNMPv1, SNMPv2	Enable/disable SNMPv1 and SNMPv2
Community String	Enter the shared password of the community. **Note:**

SNMP – SNMPv1 or SNMPv2

To configure SNMPv3, please refer to the table below:

SNMPv3	Enable/disable SNMPv3.
Username	Enter a username.
Authentication Mode	Select the algorithm used for the authentication.
Authentication Key	Select the authentication password.
Encryption Mode	Select the encryption protocol used for the encryption of the data.
Encryption Key	Enter the encryption key.

SNMP – SNMPv3

Backup and Restore

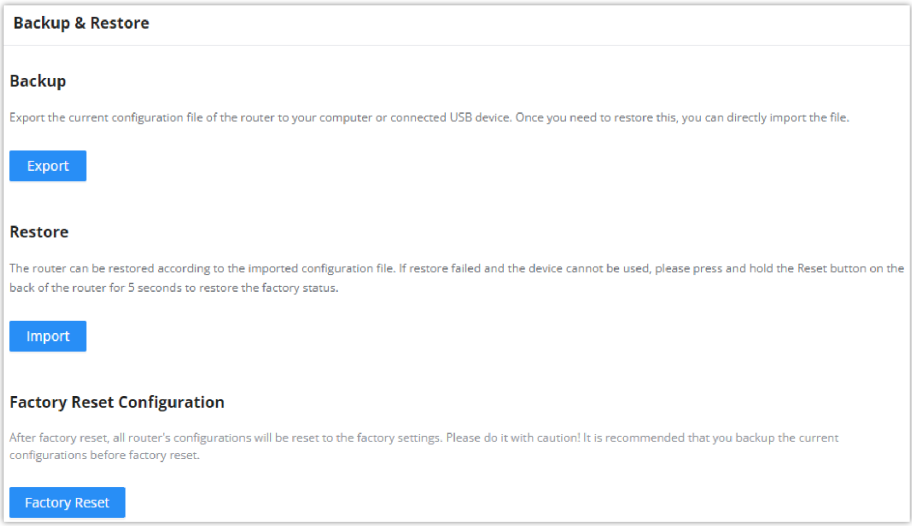
The GWN700x configuration can be backed up (e.g., when performing a firmware update), the configuration can be uploaded to the router by clicking on "**Import**" and selecting the back up file. This will load the backed up configuration back into the router quickly.

If the user wish to modify the configuration file before importing, then a **GWN Router Configuration Tool** can be used to make the necessary modifications to the configuration file. The tool is supported on Windows® and Linux environments. To download the tool: GWN Router Configuration Tool, then download the Windows® or Linux version accordingly.

Please, visit this guide on how to use the GWN Router Configuration Tool User Guide.

If the user wants to reset the device to its initial configuration, he/she can click one "Factory Reset".

> **Warning**
>
> Resetting the device to its factory settings will wipe all the configuration in the router and it cannot be restored unless the user has previously backed up the configuration. Please back up the configuration before performing a factory reset if you wish to keep a copy of your configuration.



Backup and Restore

System Diagnostics

Many debugging tools are available on GWN700x's Web GUI to check the status and troubleshoot GWN700x's services and networks.

To access these tools navigate to **"Web UI → System Settings → System Diagnosis"**

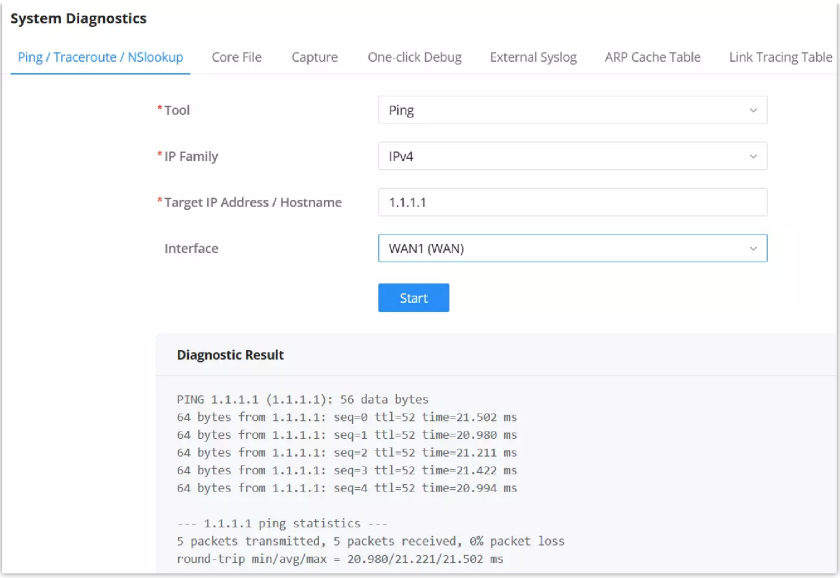
Ping/Traceroute/NSlookup

- **Ping**

The **Ping** tool is used to test connectivity between the router and a specific target IP address or hostname. It sends a series of packets to the destination and measures the time taken for the packets to return, providing useful information about network latency and connectivity.

- **Tool**: Select "Ping" from the dropdown.
- **IP Family**: Choose between IPv4 or IPv6.
- **Target IP Address / Hostname**: Enter the IP address or hostname you want to ping.
- **Interface**: Select the network interface (e.g., WAN1, WAN2) through which the test will be conducted.

Click **Start** to begin the test. The **Diagnostic Result** will display the round-trip time for each packet and the overall packet loss, if any.



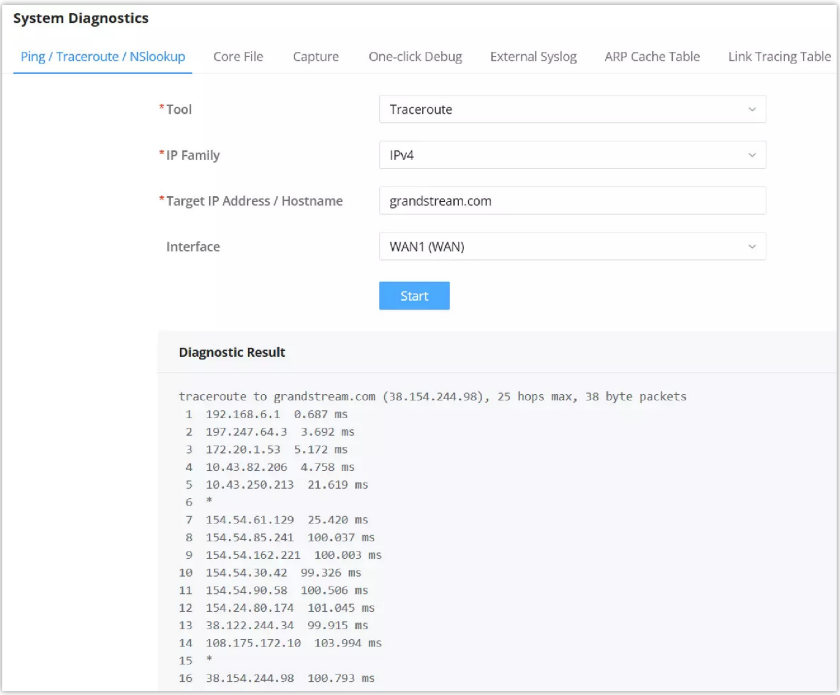
Ping

- **Traceroute**

The **Traceroute** tool identifies the path that packets take from the router to a specified destination. It lists each hop (intermediate routers) along the way and measures the time taken for the packets to reach each hop.

- **Tool**: Select “Traceroute” from the dropdown.
- **IP Family**: Choose between IPv4 or IPv6.
- **Target IP Address / Hostname**: Enter the IP address or hostname for tracing the route.
- **Interface**: Choose the network interface to send the traceroute request.

Click **Start** to initiate the traceroute. The **Diagnostic Result** will display each hop along the route to the target, along with the response times for each hop.



Traceroute

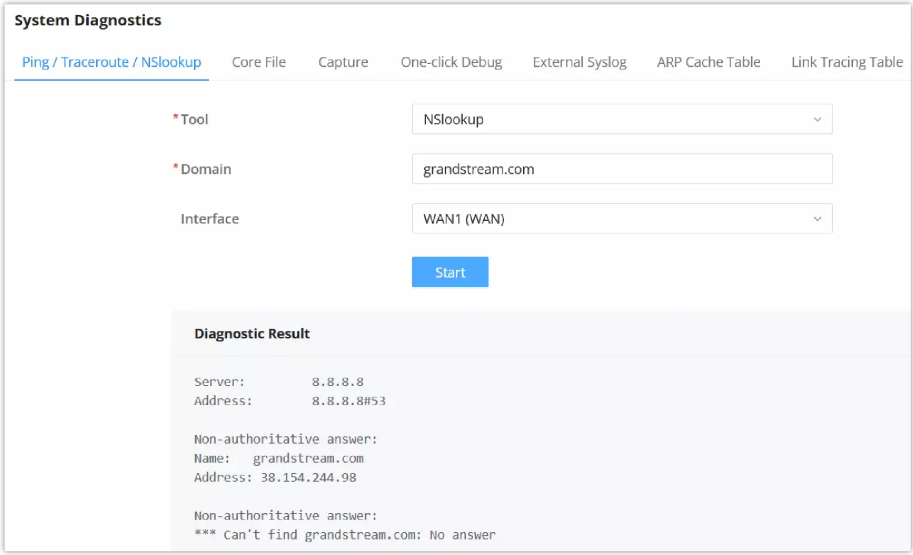
- **NSlookup**

The **NSlookup** tool is used to query DNS servers for domain name resolution. It retrieves the IP address associated with a domain name or vice versa, helping to diagnose DNS-related issues.

- **Tool**: Select “NSlookup” from the dropdown.
- **Domain**: Enter the domain name you want to query (e.g., “grandstream.com”).

- **Interface**: Select the interface to use for the DNS lookup.

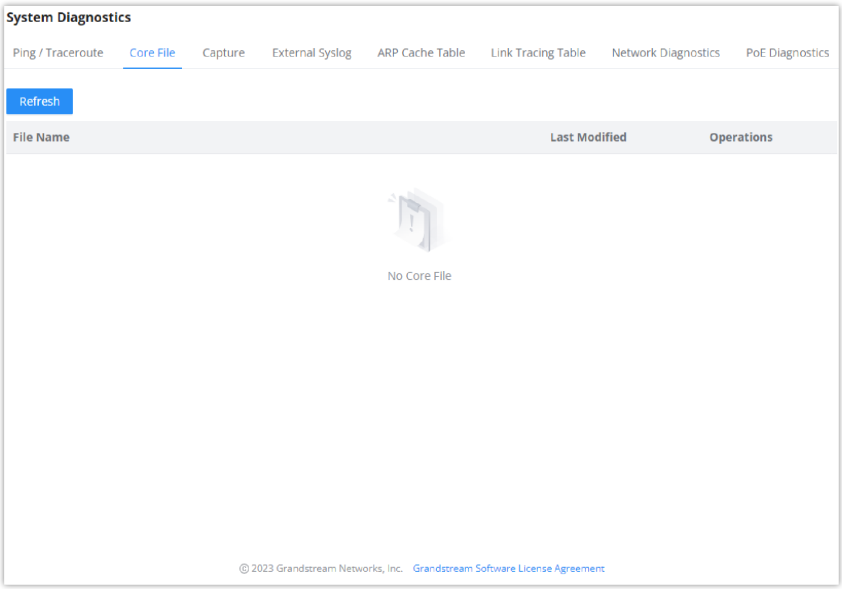
Click **Start** to run the query. The **Diagnostic Result** will display the DNS server queried, along with the resolved IP address or any error if the domain cannot be found.



NSlookup

Core File

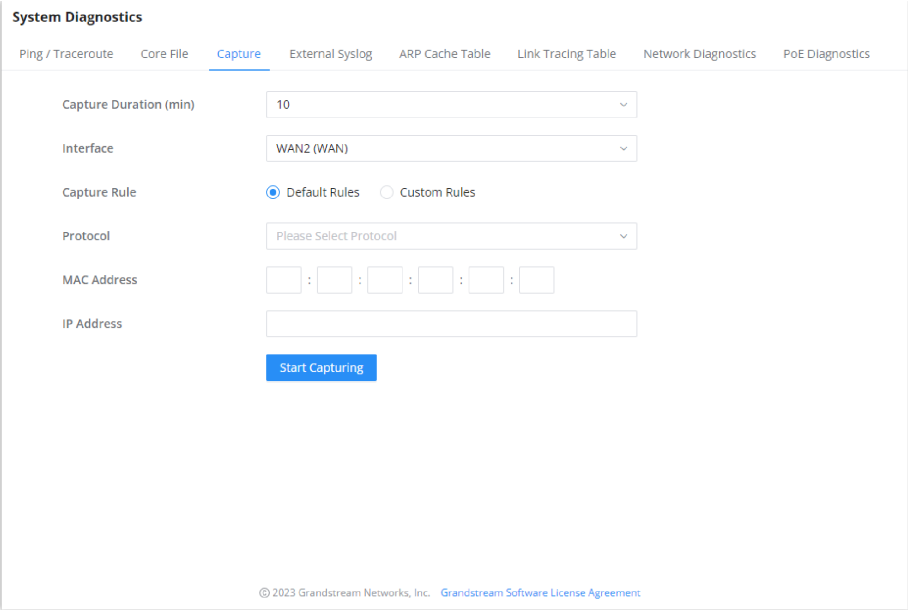
When a crash event happens on the unit, it will automatically generate a core dump file that can be used by the engineering team for debugging purposes.



Core File

Capture

This section is used to capture packet traces from the GWN700x interfaces (WAN ports and network groups) for troubleshooting purposes or monitoring. It's even possible to capture based on MAC address or IP Address, once done the user can click on Start Capturing and the file (CAP) will start downloading right away.

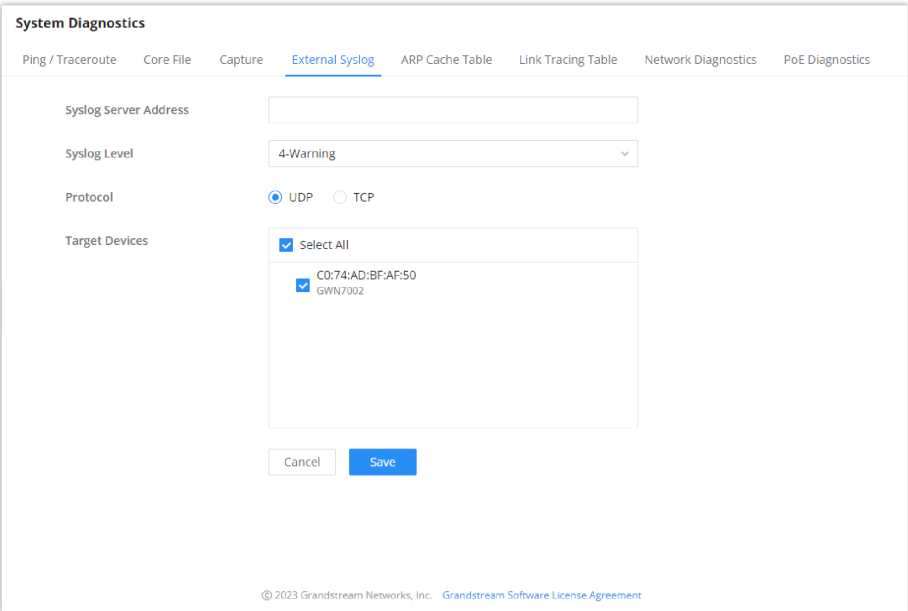


Capture

External Syslog

GWN700x routers support dumping the Syslog information to a remote server under **Web GUI → System Settings → System Diagnosis → External Syslog Tab**

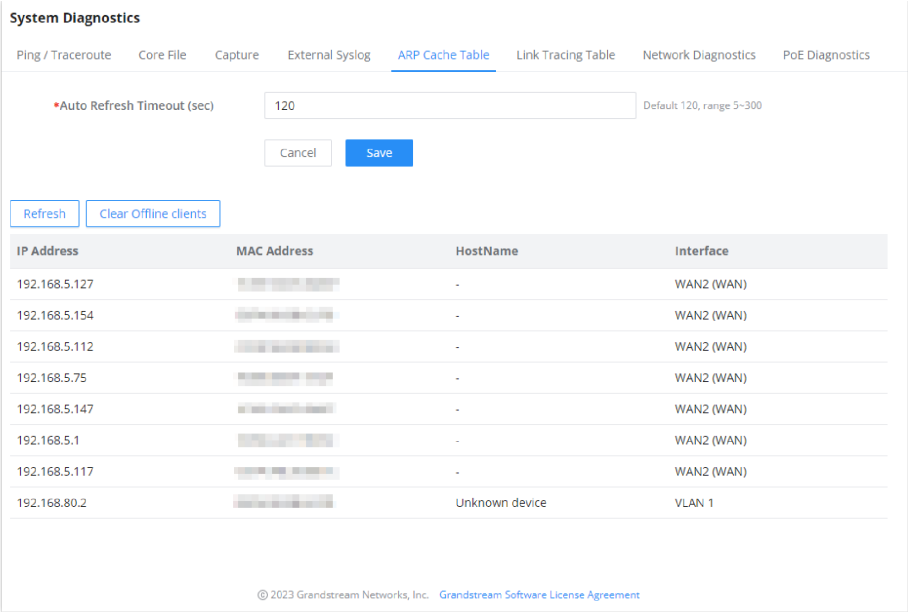
Enter the Syslog server Hostname or IP address and select the level for the Syslog information. Nine levels of Syslog are available: None, Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug.



External Syslog

ARP Cache Table

GWN700X router keeps an ARP table record of all the device which have been assigned an IP address from the router. The record will keep the devices information when the device is offline. To access the ARP Cache Table, please navigate to **System Diagnostics → ARP Cache Table**

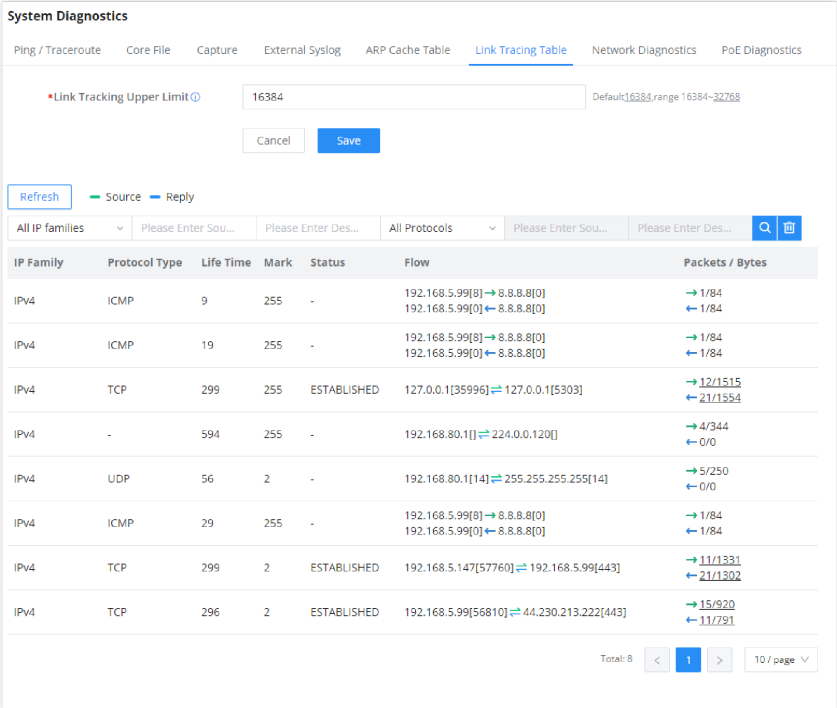


ARP Cache Table

Link Tracing Table

Link Tracing Table shows the flow of traffic by displaying the source IP address/Port (the green color) and the reply IP address/port (the blue color), also other information can be displayed like IP Family, Protocol Type, Life Time, Status, Packets/Bytes etc.

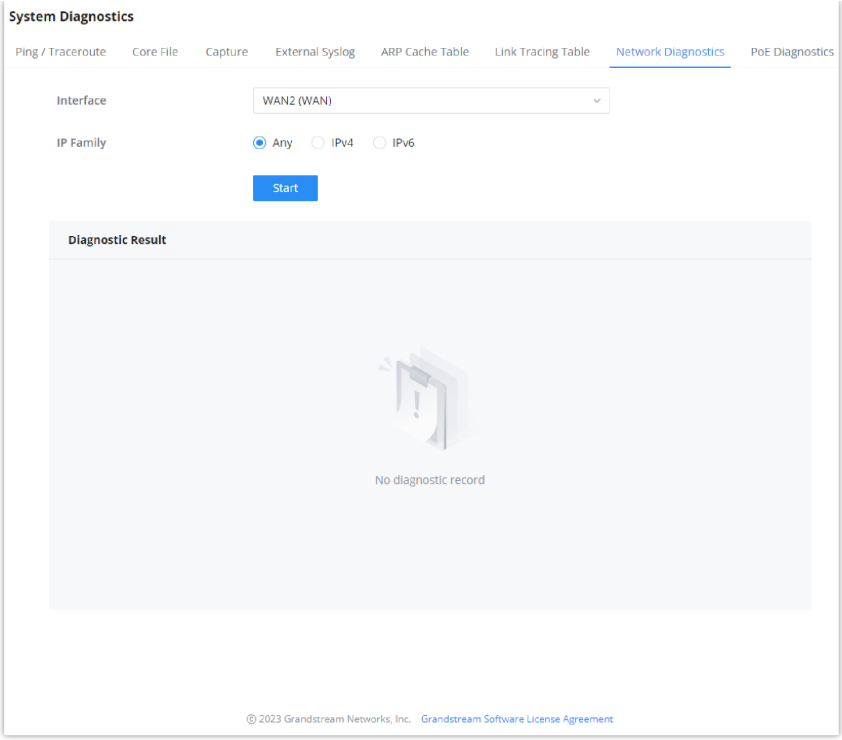
Users/Administrators can also delete the flow of certain IP addresses/Ports (Source and Destination) or then click on "**Delete**" button to clear the link tracing statistic.



Link Tracing Table

Network Diagnostics

Network diagnostics feature allows the user to quickly diagnose the connection link on a specific WAN interface.

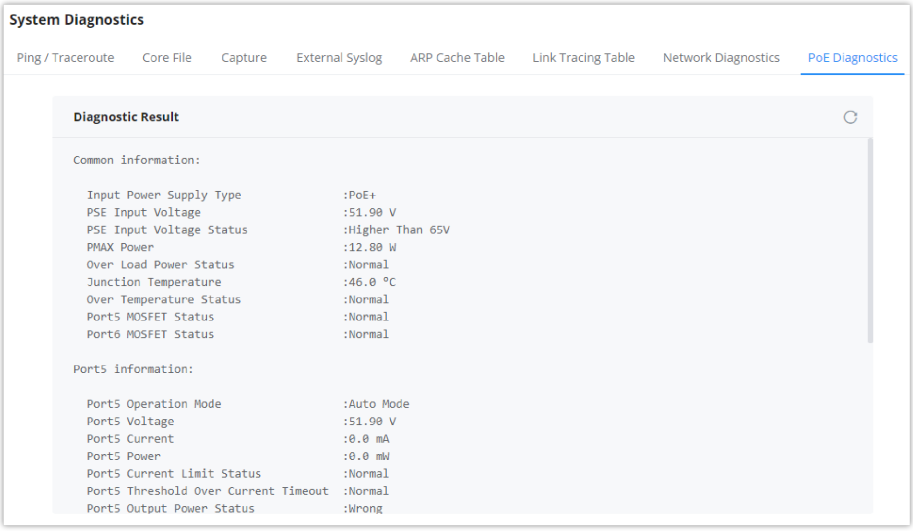


Network Diagnostics

PoE Diagnostics

PoE diagnostics page offers an insight about the ports and their components as well as the power used and the temperature. The information provided can be useful when the user encounters an issue with the PoE function of the GWN700X router.

> **Note**
>
> GWN7001 router does not support PoE.

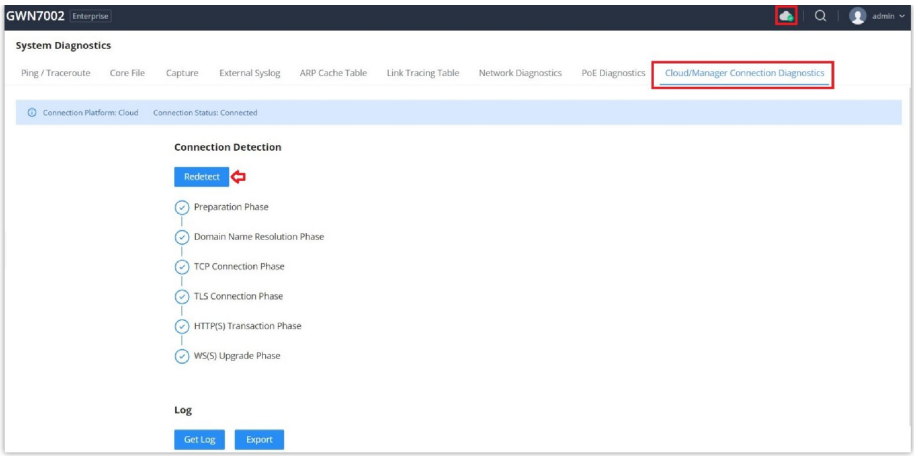


PoE Diagnostics

Cloud/Manager Connection Diagnostics

If the GWN700x router is added to the GDMS Networking or GWN Manager, it will display a Cloud icon with a green check mark (as shown in the figure below) indicating it's added to either GDMS Networking or GWN Manager.

In case there is an issue with the connection, then the user can navigate to **Maintenance → System Diagnosis → Cloud/Manager Connection Diagnostics** and then click on "**Detection**" or "**Redetect**" button to see in what stage/step the connection has failed.



Cloud/Manager Connection Diagnostics

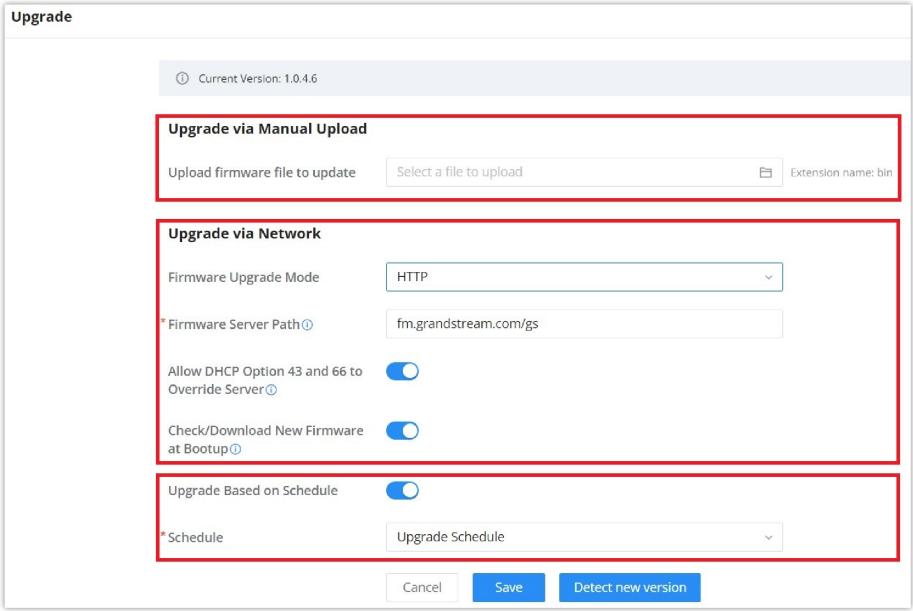
Note:

- The GWN700x router can detect its public IP address even when situated behind another router.
- Support GDMS Networking/GWN Manager connection detection across multiple links.

Upgrade

Under **Maintenance → Upgrade.** The user has the option to upgrade the GWN router via manual upload (a bin file) or via network either HTTP/HTTPS or TFTP or even schedule to upgrade in a specific time.

Please refer to the figure below:



Upgrade page

Alerts & Notifications

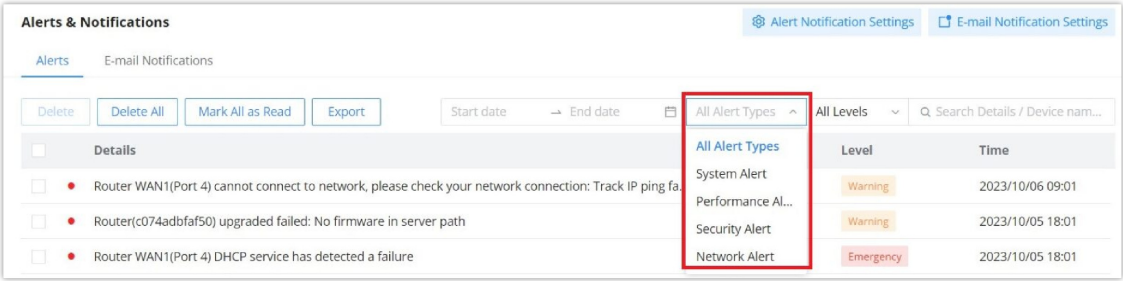
Alerts

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

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

Alerts Types

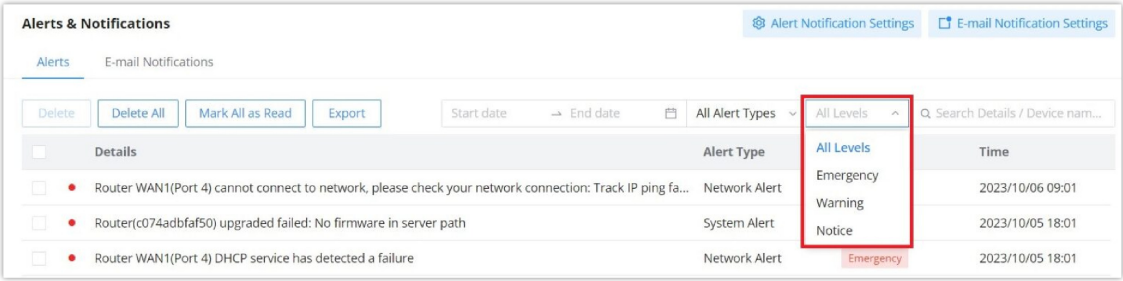
The available types are **System, Performance, Security, Network**, or the user can choose to display all the types.



Alerts Types

Alerts Levels

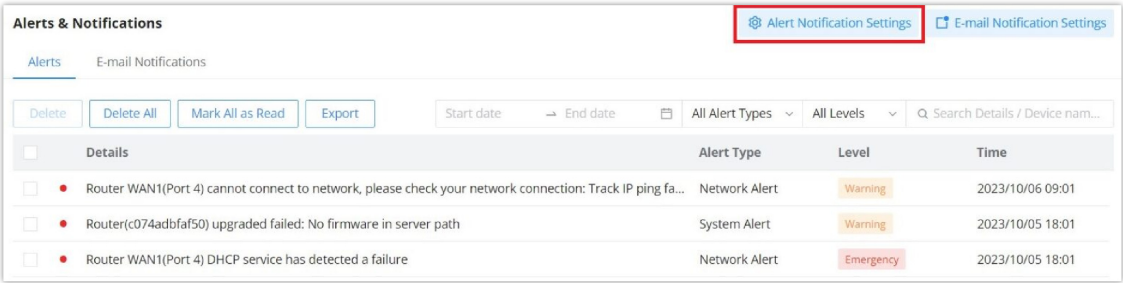
The user can filter the alert level by the following levels: **All Levels, Emergency, Warning or Notice**.



Alerts Levels

Alert Notification Settings

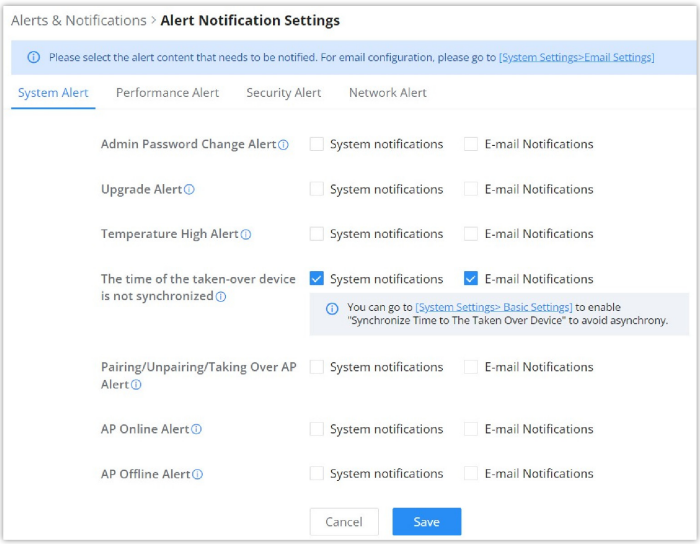
To enable the notifications on the Alerts tab, please click on "**Alert Notification Settings**" button as shown below:



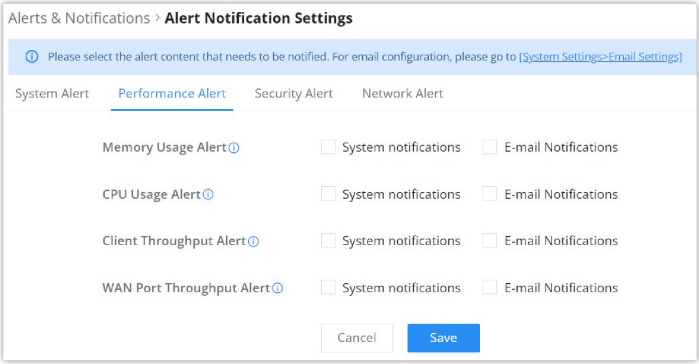
Alert Notification Settings

The figures below show all the possible alerts notifications that the user can enable on the Alerts tab, organized into 4 categories: **System** Alert, **Performance** Alert, **Security** Alert and **Network** Alert.

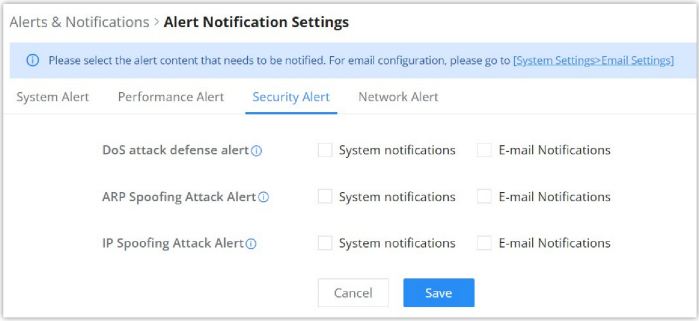
Please refer to the figures below:



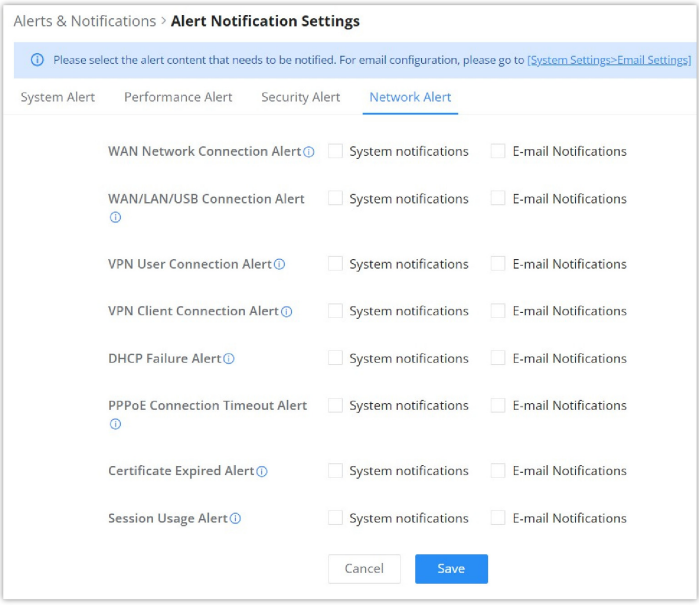
Alert Notification Settings – part 1



Alert Notification Settings – part 2



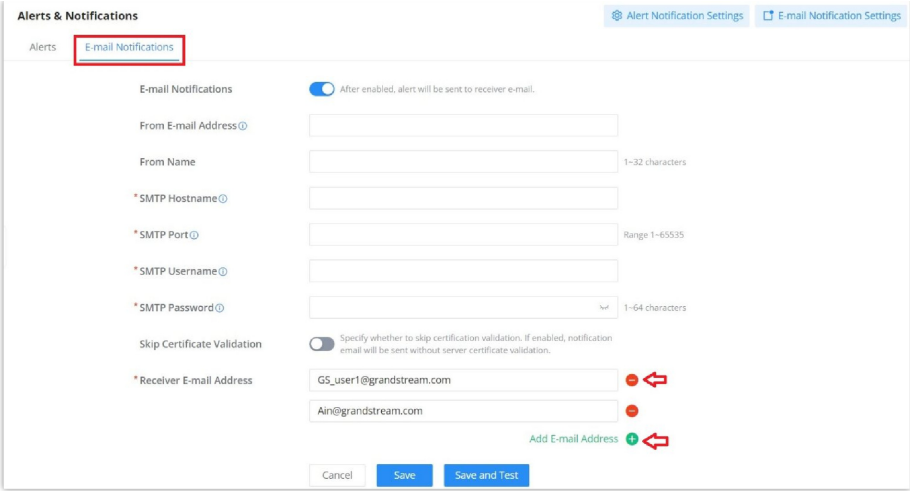
Alert Notification Settings – part 3



Alert Notification Settings – part 4

E-mail Notifications

On this tab, the user can setup the E-mails that will receive the notifications, once the feature is enabled, then the user can fill up the fields according to SMTP parameters. Refer to the figure below:



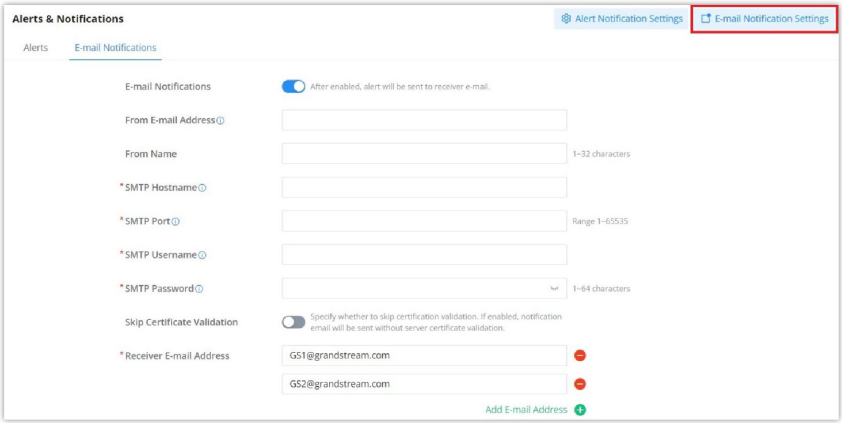
Alerts – E-mail Notifications

It's possible to add more than one receiver E-mail address as shown in the figure above.

- Click on "**Minus**" icon to delete the receiver E-mail address.
- Click on "**Plus**" icon to add the receiver E-mail address.

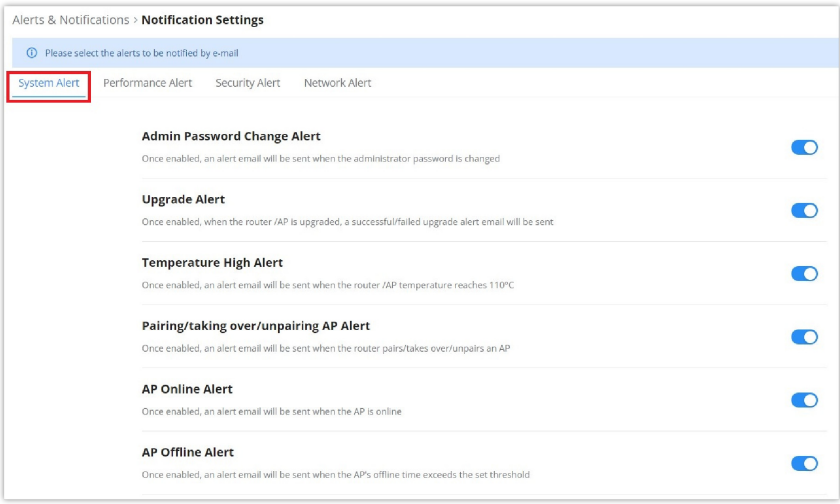
E-mail Notification Settings

To select what notifications will be sent to the receiver E-mail addresses, please click on "**E-mail Notification Settings**" button as shown below:

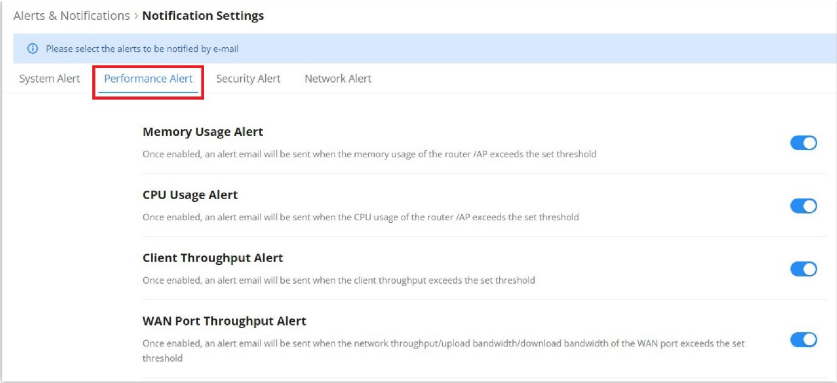


E-mail Notification Settings

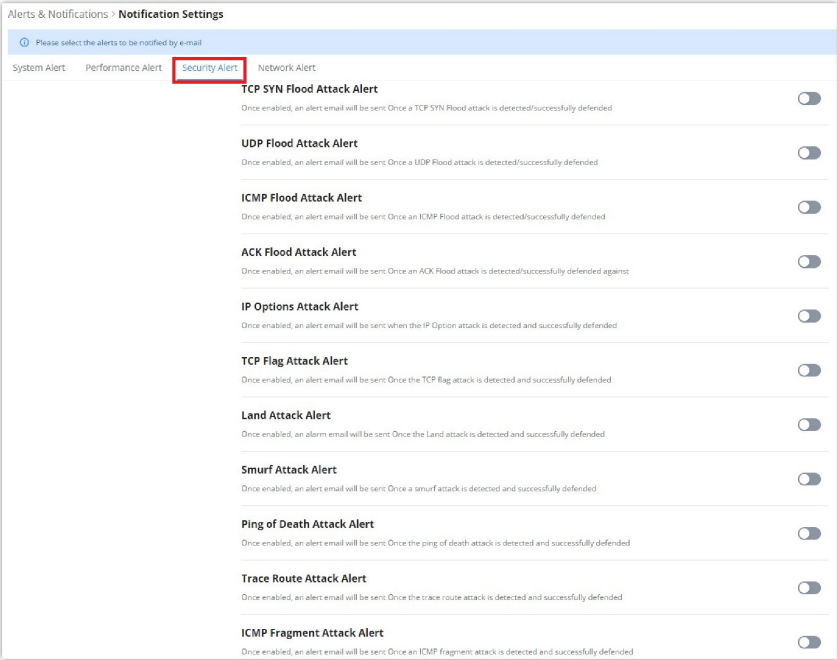
The figures below show all the possible E-mail notifications that the user can send to the pre-configured receiver E-mail Addresses, organized into 4 categories: **System** Alert, **Performance** Alert, **Security** Alert and **Network** Alert.



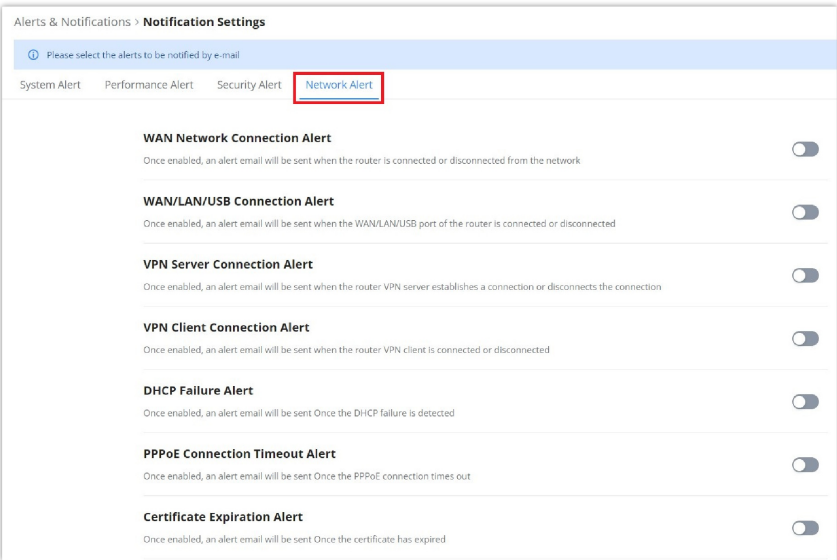
E-mail Notification Settings – part 1



E-mail Notification Settings – part 2



E-mail Notification Settings – part 3



E-mail Notification Settings – part 4

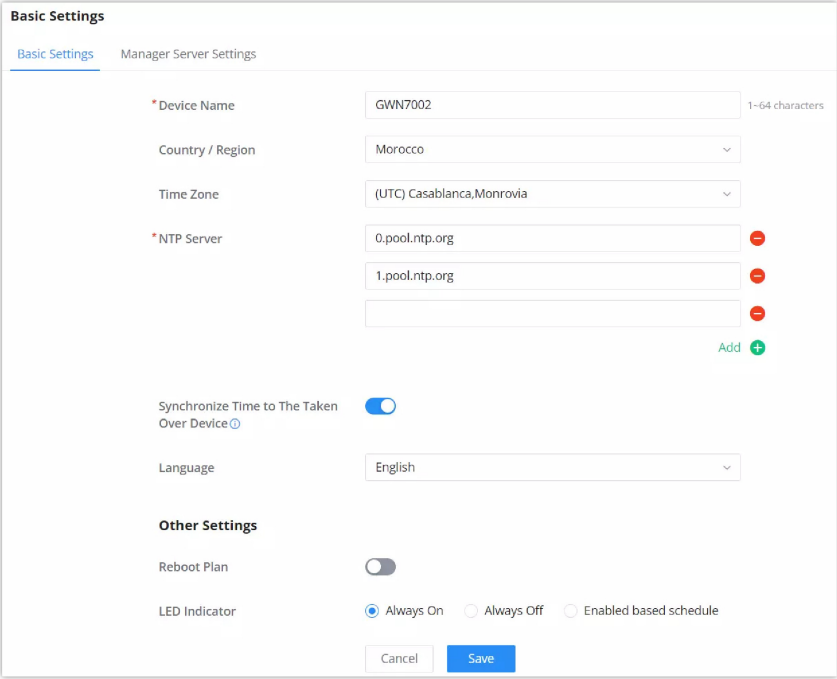
SYSTEM SETTINGS

Basic Settings

On the **Basic Settings** page, users can configure essential settings for the GWN700x router, including:

- **Device Name**: Assign a custom name for the router.

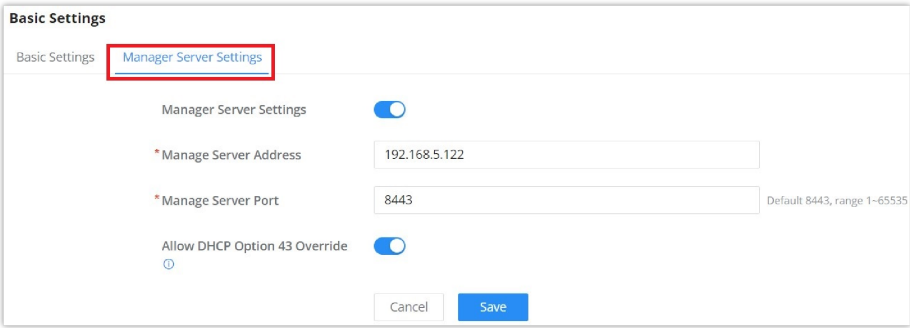
- **Country/Region** and **Time Zone**: Set the geographical location and time zone.
- **NTP Server**: Configure one or more NTP servers to synchronize the router's time. Click the **+** icon to add additional NTP servers, which is useful for ensuring time accuracy from multiple sources.
- **Synchronize Time to The Taken Over Device**: Once enabled, all devices managed by the router will directly synchronize with the router's NTP server time settings.
- **Language**: Choose the preferred display language.
- **Reboot Plan**: Set up a scheduled reboot if required by clicking on **Create Schedule** under the Reboot Plan section.
- **LED Indicator**: Configure the LED indicator to be Always On, Always Off, or based on a defined schedule.



Basic Settings

Manager Server Settings

In the case of GWN manager (on-premise GWN management solution), the user can specify the manager server address and port, there is also the option to allow DHCP option 43 override.



Manager Server Settings

Security Management

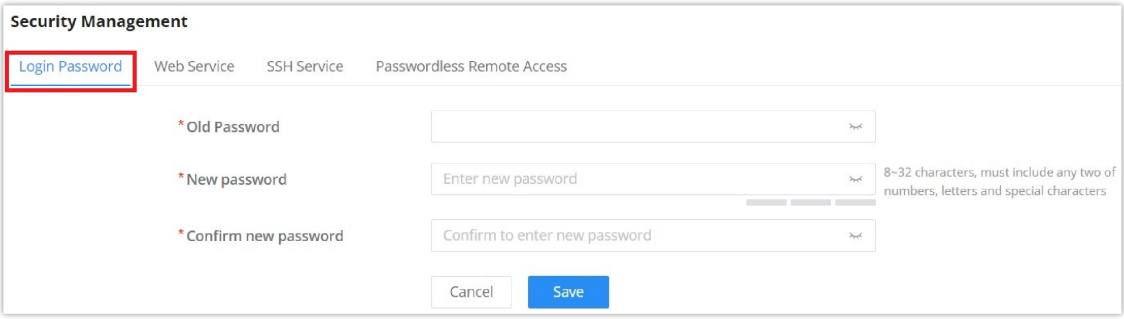
Under **"Web UI → System Settings → Security Management"** the user can change the login password and activate the web service for example web WAN port access for HTTPS port 443 as well as enabling SSH remote access.

Login Password

On this page, the user can change the password by entering the old password and then confirming the new password.

Note:

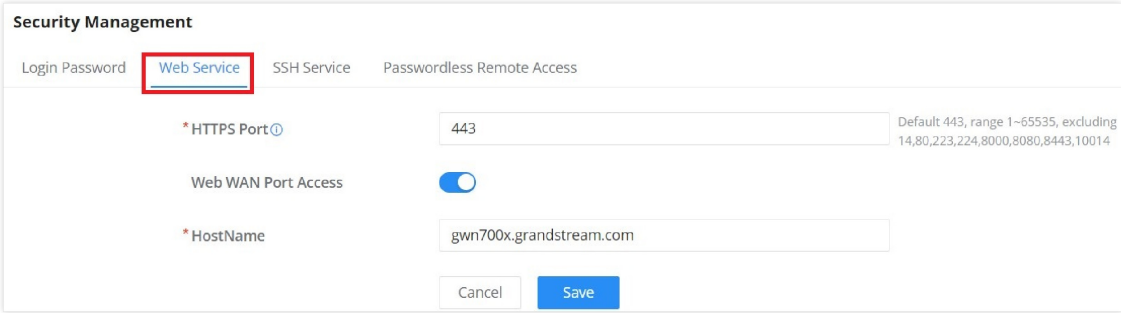
After changing the login password, the web will be forcibly logged out.



Security Management – Login Password

Web Service

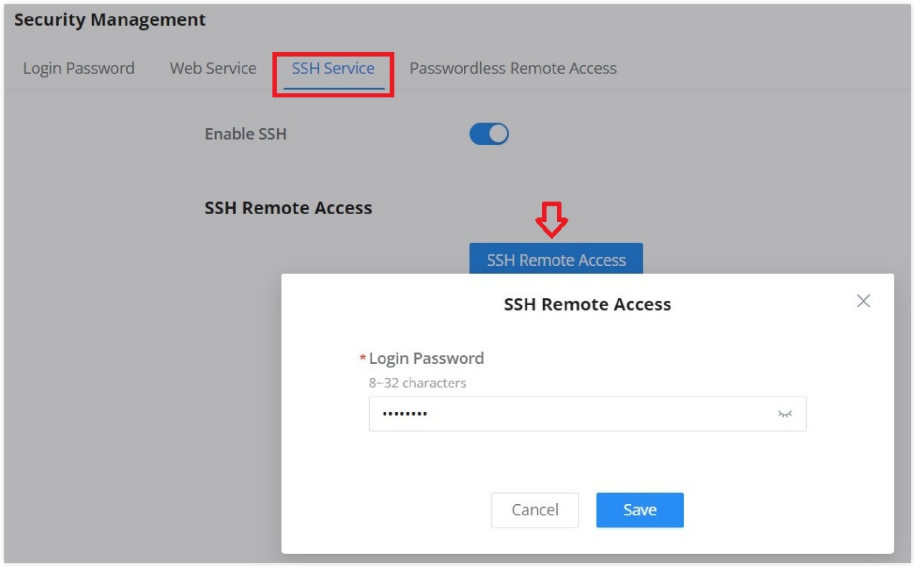
Web Service feature allows the user to access the router's web GUI from the WAN side. The connection is established over HTTPS for enhanced security. It's also possible to specify a hostname for the GWN700x router as shown in the figure below:



Security Management – Web Service

SSH Service

This feature allows the user to access the device using SSH remotely. Enable this option and click on "**SSH Remote Access**" button and then enter the SSH remote access password (login password). Once that's done, SSH access will be provided to remote users when they enter the correct password.



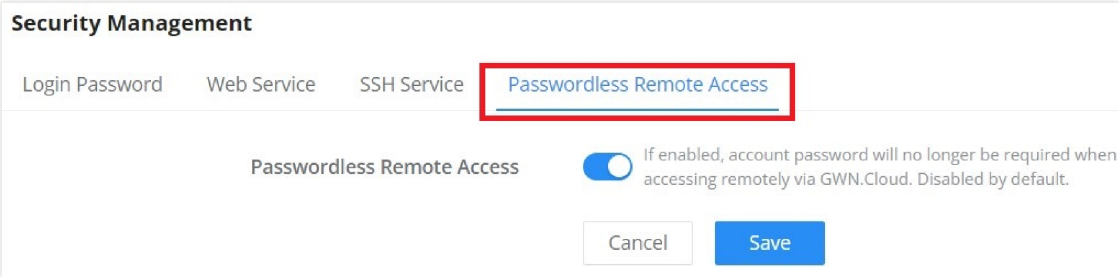
Security Management – SSH Service

Passwordless Remote Access

Enabling the Passwordless Remote Access feature, accessing the device using GDMS Networking will not require entering the password to be able to access the web GUI of the router.

Note

By default is disabled.



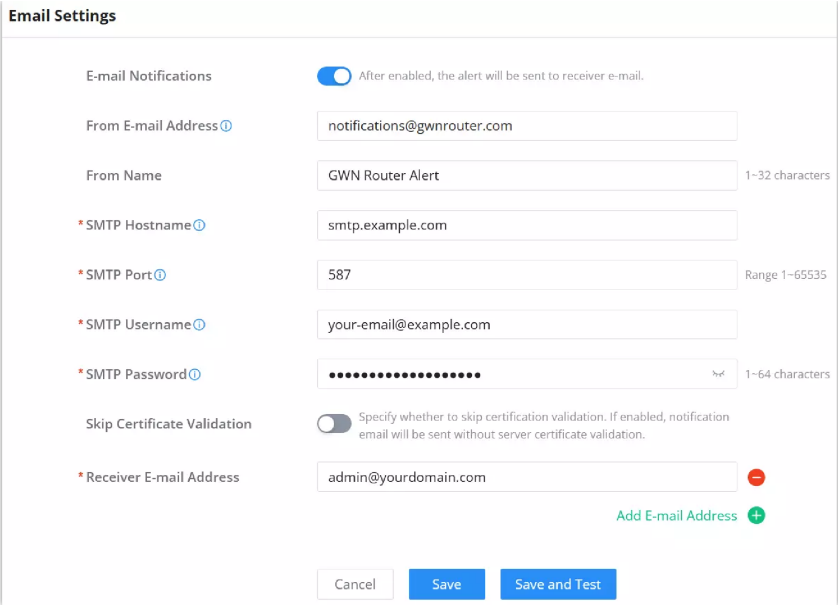
Security Management – Passwordless Remote Access

Email Settings

The *Email Settings* feature in the GWN router enables email alerts for network events and notifications. To configure email notifications, follow these steps:

1. **Enable Email Notifications**: Toggle the "Email Notifications" switch to enable alerts.
2. **Enter Sender Information**:
   - **From Email Address**: Enter the email address from which alerts will be sent. Example: `notifications@gwnrouter.com`.
   - **From Name**: Specify the sender name that will appear in alert emails. Example: `GWN Router Alert`.
3. **Configure SMTP Server**:
   - **SMTP Hostname**: Enter the SMTP server hostname. This is required for the router to connect to your email service provider. Example: `smtp.example.com`.
   - **SMTP Port**: Set the SMTP port used by your email provider. Common ports are 587 (for TLS) and 465 (for SSL).
   - **SMTP Username**: Input the email account's username. Example: `your-email@example.com`.
   - **SMTP Password**: Enter the password for the SMTP username.
4. **Certificate Validation**:
   - **Skip Certificate Validation**: Toggle this option only if your SMTP server does not support SSL certificates. Enabling this will send alerts without server certificate validation.
5. **Set Receiver Email Address**:
   - Add the email addresses to which notifications should be sent. Example: `admin@yourdomain.com`. Multiple addresses can be added by clicking "Add E-mail Address".
6. **Save Configuration**:
   - Click "Save" to apply the settings or "Save and Test" to test email notifications.

Note: Ensure that SMTP credentials are correct, and the SMTP server allows email relay for notifications to work properly.

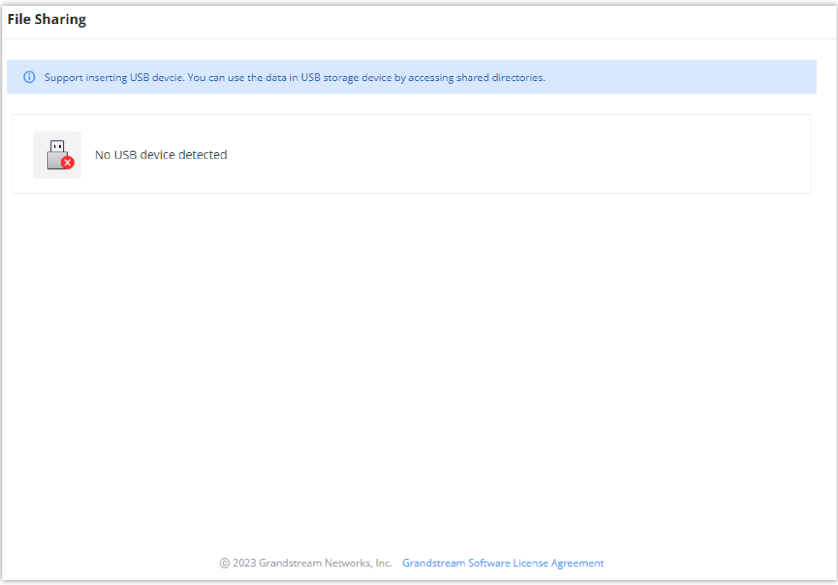


Email Settings

File Sharing

The GWN routers have a USB port that can be used for file sharing, either using a USB flash drive or a Hard Drive, enabling clients with Windows, Mac or Linux to access files easily on the local network. There is also an option to enable a password for security reasons.

Navigate to **System Settings → File Sharing.**



File Sharing

Profiles

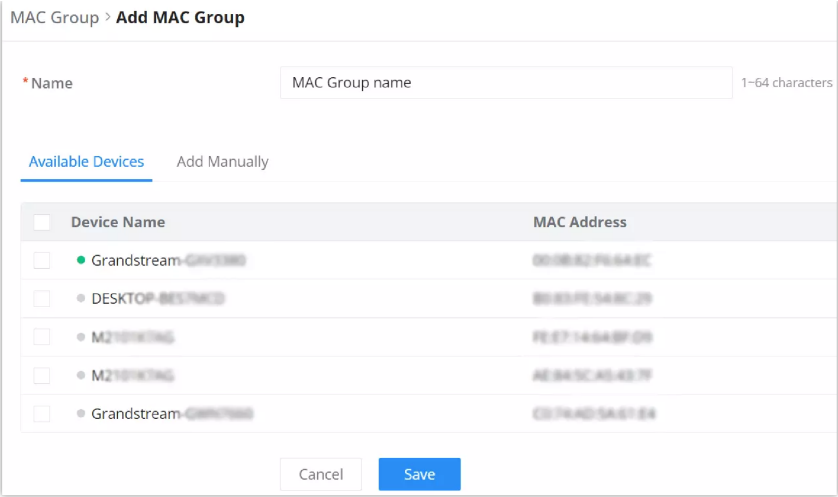
MAC Group

The MAC Group is a feature in GWN700x that enables the user to create a group of MAC addresses from the available ones or manually adding the MAC Address.

To create a new MAC group, Navigate under: "**Profiles → MAC Group"** then click on "**Add**" button.

- **Add devices from the list:**

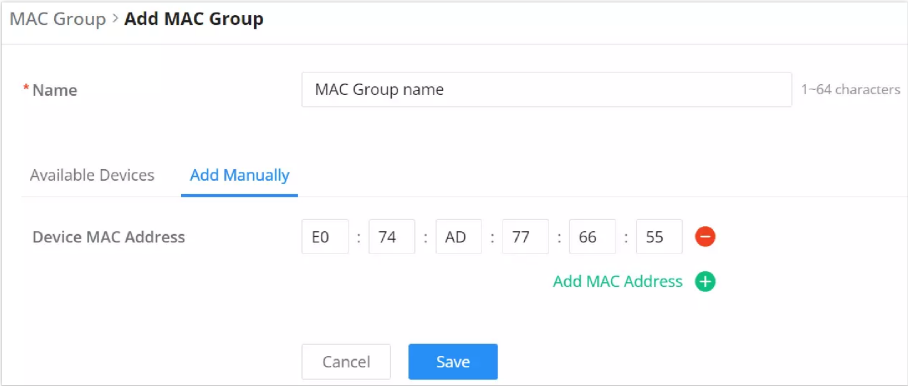
Enter the name of the MAC Group, then add the devices from the list.



Add MAC Group

- **Add Devices Manually:**

Enter the name of the MAC Group, then add the devices' MAC addresses.

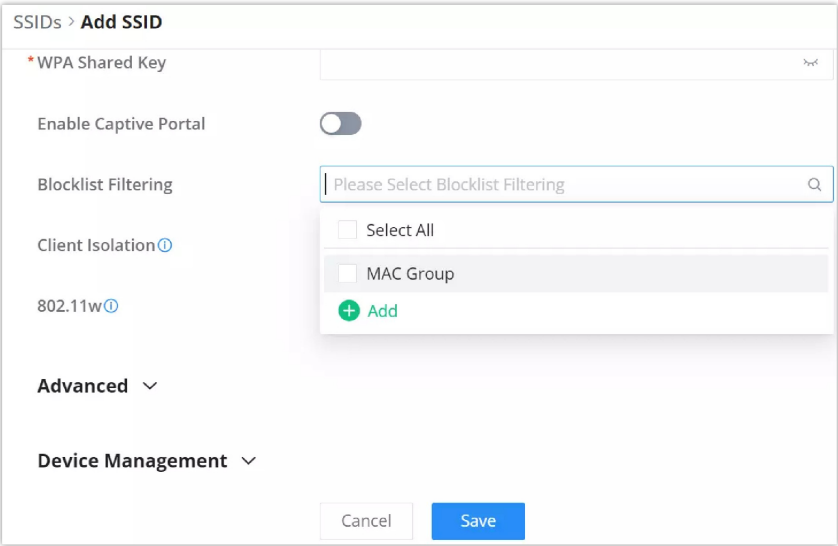


Add MAC address manually

After the MAC Group is created, to take effect the user needs to apply it, for example like the SSID:

Navigate to " **Web UI → AP Management → SSIDs**", either click on "**Add**" button to create new SSID or click on "**Edit**" icon to edit previously created SSID, scroll down to "**Access Security**" section then look for "**Blocklist Filtering**" option and finally select from the list the previously created MAC address, the user can select one or more, or click on "**Add**" at the bottom of the list to create new one.

Please refer to the figure below:



MAC Group – SSID example

IP Address Group

The **IP Address Group** feature allows users to manage groups of IP addresses for applying policies such as security rules, NAT, or firewall settings. Both **IPv4** and **IPv6** addresses are supported. By grouping addresses, you can manage multiple addresses with ease, improving policy efficiency and reducing errors.

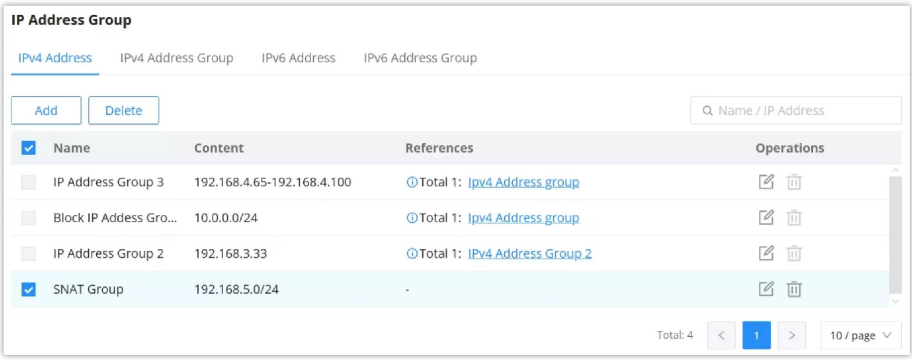
To configure IP Address Groups, follow these steps:
Navigate to **Profiles** → **IP Address Group** from the main menu.

IPv4 Address

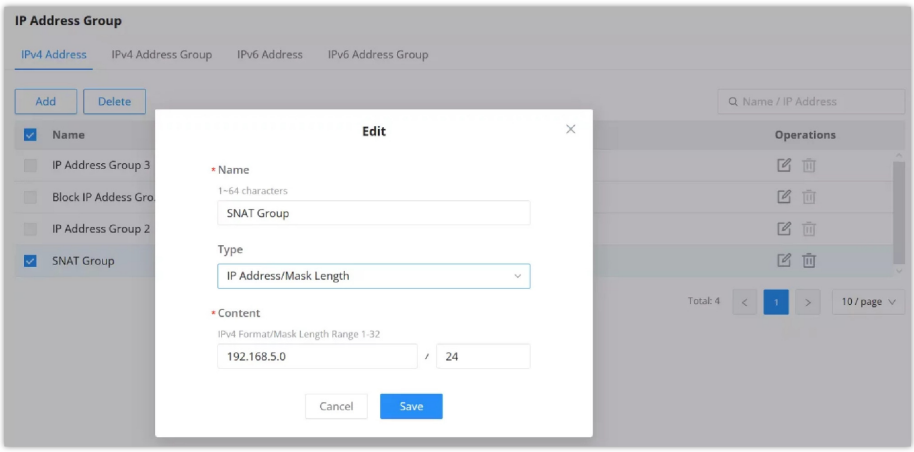
The **IPv4 Address** feature lets you add individual IPv4 addresses, subnets, or ranges for use in policies like NAT or firewall settings. Once addresses are added, you can group them for better management.

Steps to add an IPv4 Address:

1. Navigate to **Profiles** → **IP Address Group** → **IPv4 Address**.
2. Click **Add** to create a new IPv4 address.
3. Enter a **Name** for the address.
4. Select the **Type** from:
   - IP Address
   - IP Address/Mask Length
   - IP Address Range
5. Fill in the relevant details (e.g., IP address, subnet mask, or range).
6. Click **Save** to add the IPv4 address.



IP Address – IPv4 Address



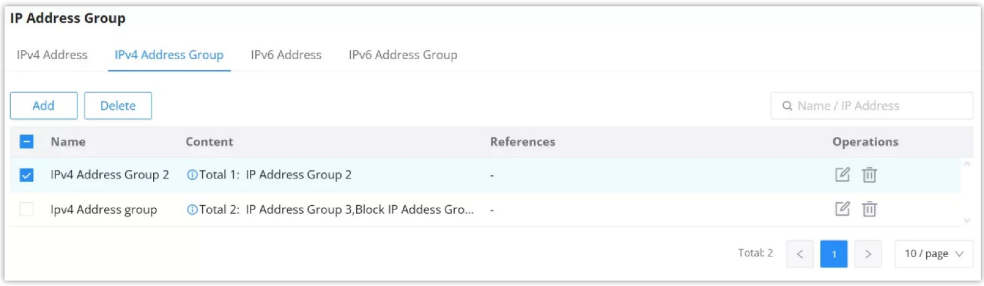
IP Address – Add IPv4 Address

IPv4 Address Group

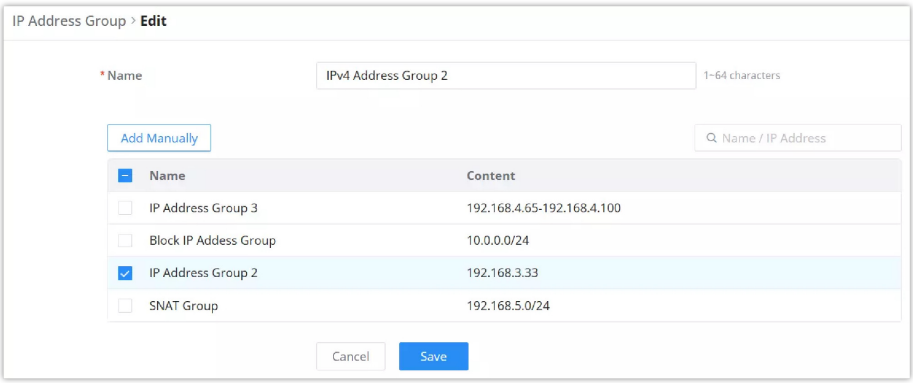
The **IPv4 Address Group** feature allows you to combine multiple IPv4 addresses into one group, simplifying the application of policies like SNAT or firewall rules.

Steps to create an IPv4 Address Group:

1. Navigate to **Profiles → IP Address Group → IPv4 Address Group**.
2. Click **Add** to create a new IPv4 group.
3. Enter a **Name** for the group.
4. Select the IPv4 addresses you wish to include in the group from the list.
5. Click **Save** to create the group.



IP Address Group – IPv4 Address



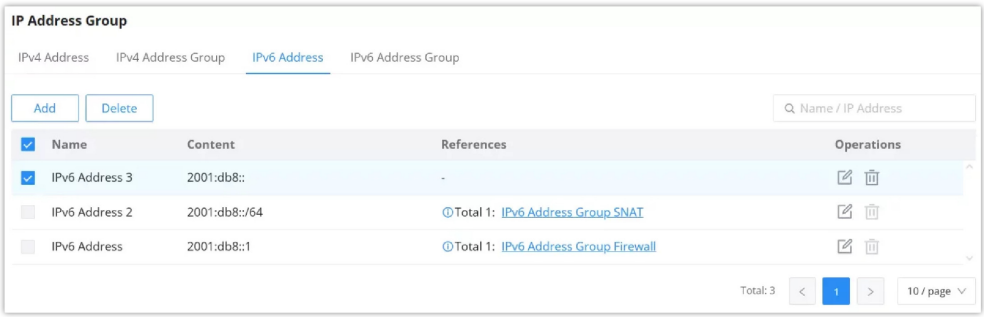
IP Address Group – Add IPv4 Address

IPv6 Address

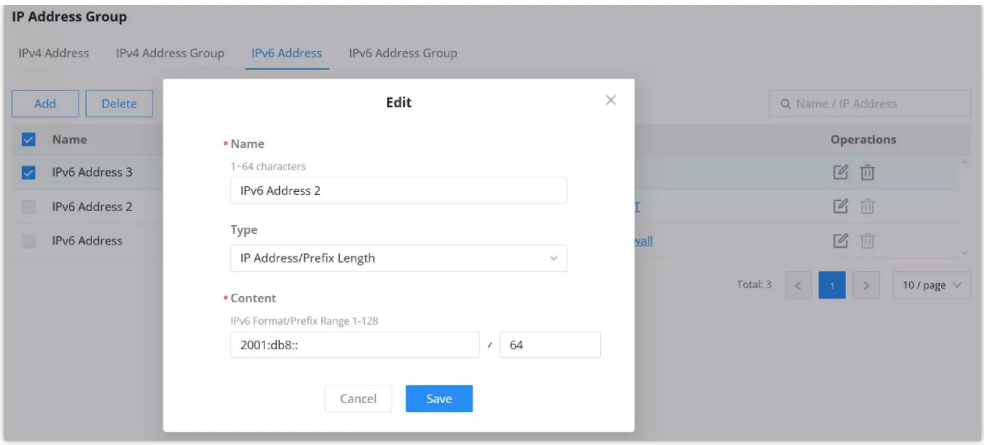
The **IPv6 Address** feature lets you add IPv6 addresses or networks, which can be used in settings such as firewall rules or NAT configurations.

Steps to add an IPv6 Address:

1. Navigate to **Profiles → IP Address Group → IPv6 Address**.
2. Click **Add** to create a new IPv6 address.
3. Enter a **Name** for the address.
4. Select the **Type**:
   - IP Address
   - IP Address/Prefix Length
5. Fill in the relevant IPv6 address or prefix.
6. Click **Save** to add the IPv6 address.



IPv6 Address



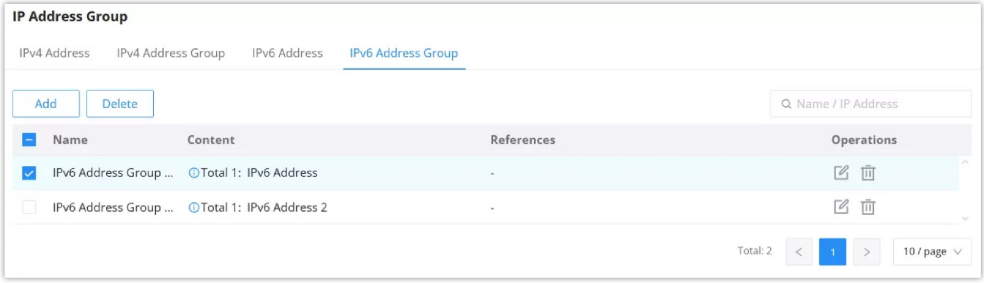
Add IPv6 Address

IPv6 Address Group

The **IPv6 Address Group** feature allows you to group multiple IPv6 addresses into one group. This makes it easier to apply policies to multiple addresses at once.

Steps to create an IPv6 Address Group:

1. Navigate to **Profiles** → **IP Address Group** → **IPv6 Address Group**.
2. Click **Add** to create a new IPv6 group.
3. Enter a **Name** for the group.
4. Select the IPv6 addresses to include from the list.
5. Click **Save** to create the group.



IPv6 Address Group

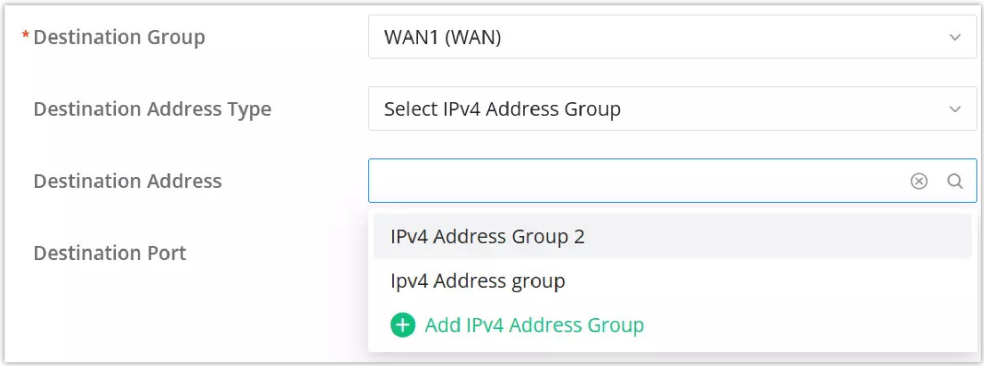
Add IPv6 Address Group

IP Address Group – Example

Here's an example of how to use an **IPv4 Address Group** in a **Source NAT (SNAT)** configuration:

1. Navigate to **Routing** → **SNAT**.
2. Click **Add** to create a new SNAT rule.
3. Select the **Destination Group** as **WAN1 (WAN)**.

4. Under **Destination Address Type**, choose **Select IPv4 Address Group**.
5. Under **Destination Address**, select the desired **IPv4 Address Group** from the list.
6. Configure other fields such as **Destination Port** as needed.
7. Click **Save** to apply the rule.



IP Address Group

FQDN (Fully Qualified Domain Name)

The FQDN feature allows you to define domain names that can be applied in traffic rules, firewall policies, or other configurations. It can also be paired with specific IP addresses, making it easier to manage domains instead of individual IP addresses.

You can create individual **FQDN Addresses** or group multiple FQDN addresses into an **FQDN Address Group** for easier management and application in rules.

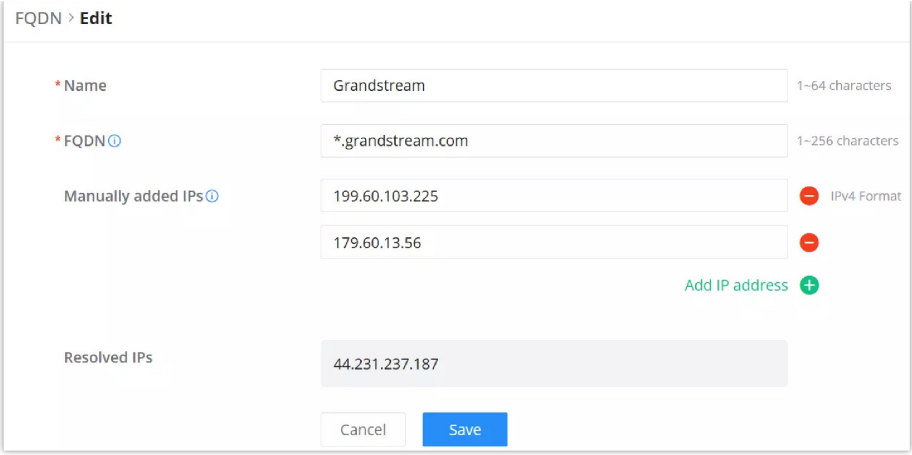
FQDN – Address

An FQDN Address is a domain name entry that can optionally be associated with up to eight IP addresses. This is useful for applying domain-based traffic filtering or rules.

To create an FQDN Address:

1. **Navigate to**: **Profiles → FQDN → Address**
2. Enter the following:
   - **Name**: Name of the FQDN address (e.g., "Grandstream").
   - **FQDN**: Enter the domain (e.g., `*.grandstream.com`). Wildcards can be used to match subdomains.
   - **Manually added IPs** (optional): Add up to 8 IP addresses to be associated with the FQDN.
3. Click **Save** to add the FQDN entry.

FQDN



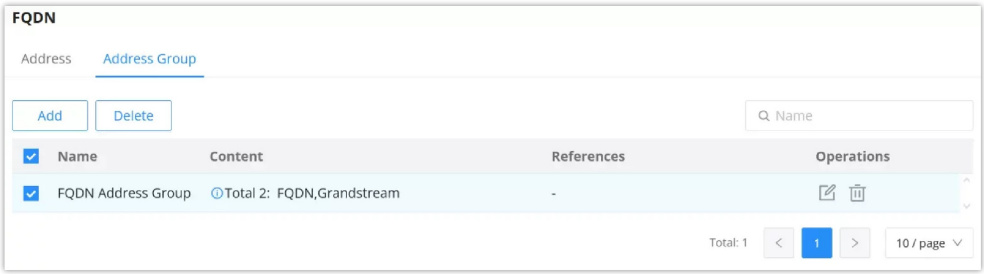
Add FQDN

FQDN – Address Group

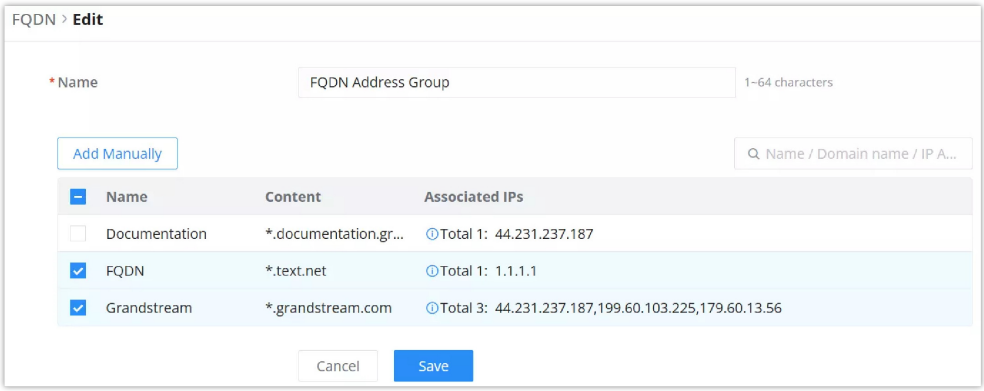
FQDN Address Groups allow you to group several FQDN addresses, which simplifies applying multiple FQDNs within traffic rules.

To create an FQDN Address Group:

1. **Navigate to**: **Profiles** → **FQDN** → **Address Group**
2. Provide a **Name** for the group.
3. Select the FQDN addresses to be included in the group.
4. Click **Save** to create the group.



FQDN – address group



FQDN – Add address group

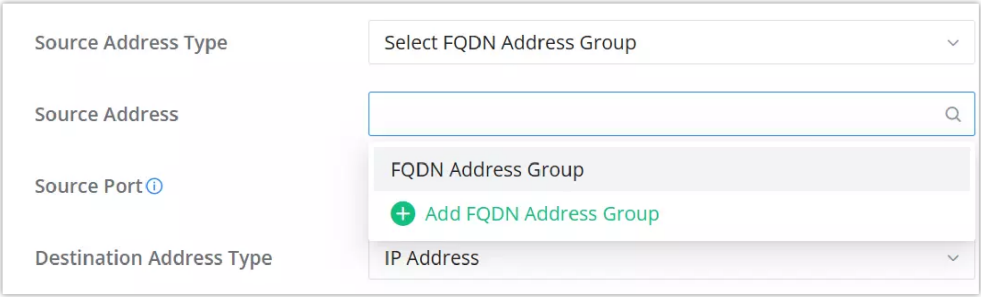
FQDN – Example

Here is an example of applying an FQDN Address Group in a firewall rule. This will show how to use domain-based filtering within your network.

Example: Applying FQDN Address Group in a Traffic Rule

1. **Navigate to**: **Firewall** → **Traffic Rules** → **Add Inbound Rule**.
2. For **Source Address Type**, select **FQDN Address Group**.

3. Select the previously created FQDN Address Group (e.g., “FQDN Address Group”).
4. Configure any other parameters as needed and click **Save**.



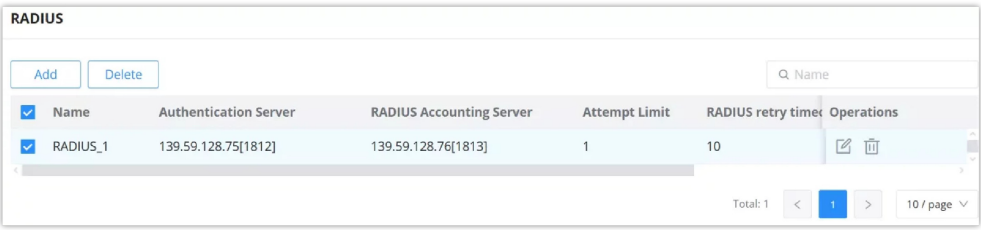
FQDN – Example

RADIUS

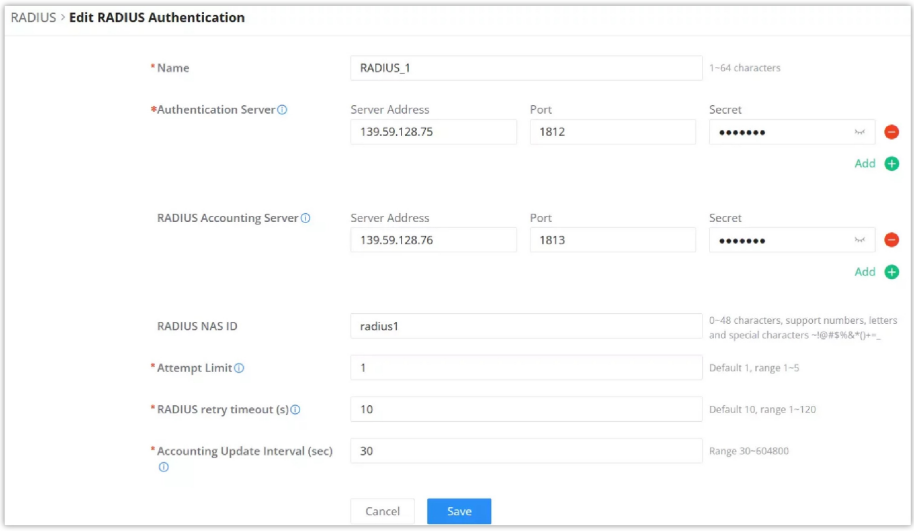
RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting for users or devices connecting to a network. In the GWN7002, the RADIUS feature allows network administrators to integrate external RADIUS servers for handling network access.

To create a RADIUS profile:

1. **Navigate to**: **Profiles** → **RADIUS** → **Add**.
2. **Enter the RADIUS server details**:
   - **Authentication Server**: Enter the server address and port for authentication (default port is 1812).
   - **RADIUS Accounting Server**: Enter the server address and port for accounting purposes (default port is 1813).
   - **RADIUS NAS ID**: Input the NAS ID (Network Access Server ID).
   - **Attempt Limit**: Specify the number of attempts before the server denies access.
   - **RADIUS Retry Timeout**: Set the time to wait before retrying a connection to the server (in seconds).
   - **Accounting Update Interval**: Set the interval at which accounting updates will be sent (in seconds).
3. **Save** the profile.



RADIUS

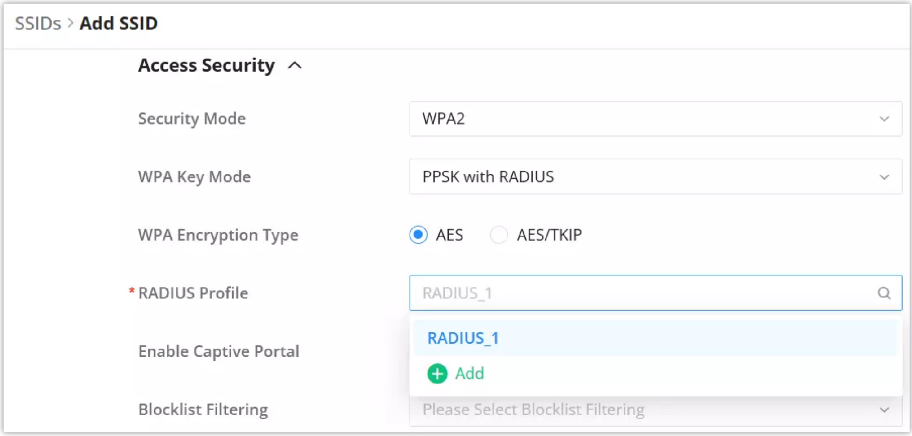


Add RADIUS

RADIUS – Example

Applying the RADIUS Profile to a Wi-Fi SSID:

1. **Navigate to**: **AP Management** → **SSIDs** → **Add**.
2. In the **Access Security** section, configure the following:
   - **Security Mode**: Select **WPA2**.
   - **WPA Key Mode**: Select **PPSK with RADIUS** or another option based on the required encryption method.
   - **RADIUS Profile**: Select the previously created **RADIUS Profile** from the dropdown list.
3. **Save** the settings.

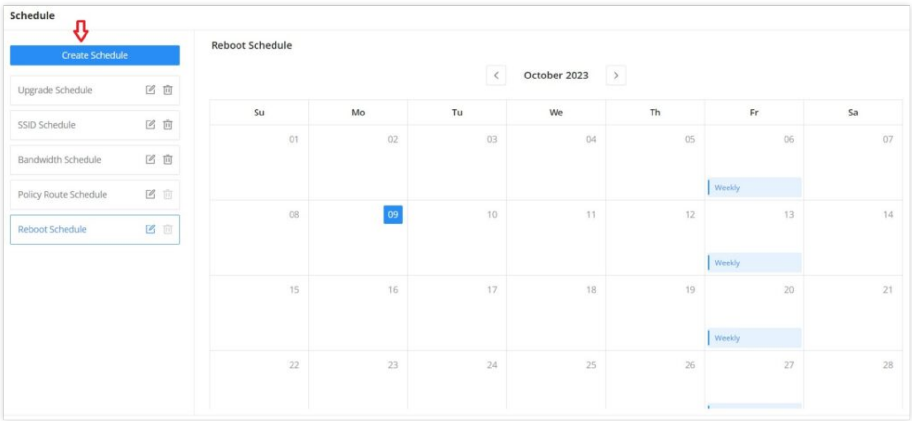


RADIUS – Example

Schedule

GWN routers allow the user to create a schedule, either weekly based or an absolute date/time (specific date and an interval), then these schedules can be assigned to various services on GWN routers: Upgrade, SSID, Bandwidth limit, Policy route and reboot.

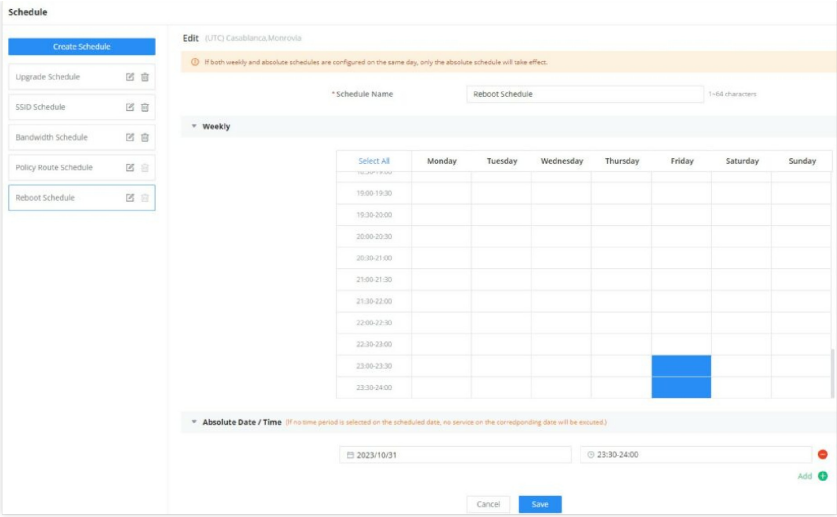
To create a schedule, navigate to **Profiles** → **Schedule**, then click on "**Create Schedule**" button as shown below:



Schedule page

Note:

- If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.
- (If no time period is selected on the scheduled date, no service on the corresponding date will be executed).

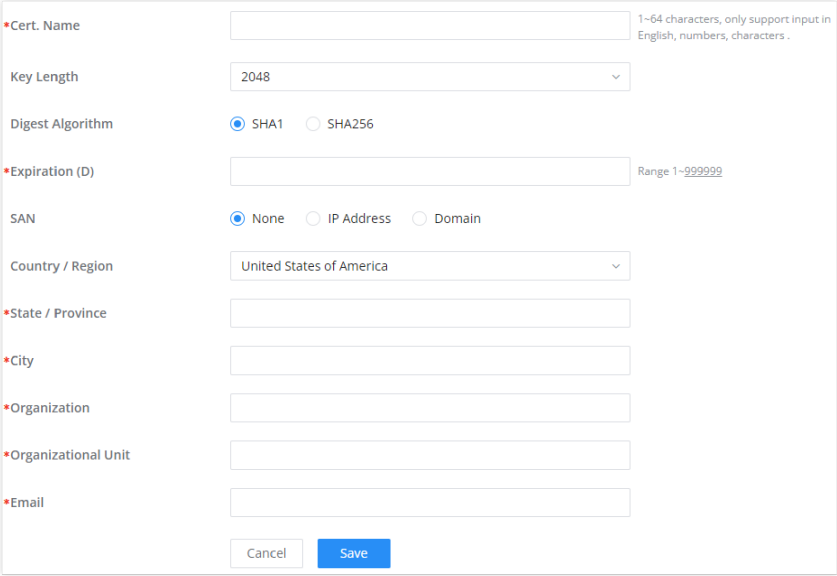


Add a schedule

Certificates

CA Certificates

In this section, the user can create a CA certificate. This certificate will authenticate the user when connected to the VPN server created on the router. This authentication will ensure that no identity is being usurped and that the data exchanged remain confidential. To create a certificate, please access the web GUI of the router and access **System Settings → Certificates → CA Certificates** then click "Add" and fill in the necessary information.



Add CA Certificate

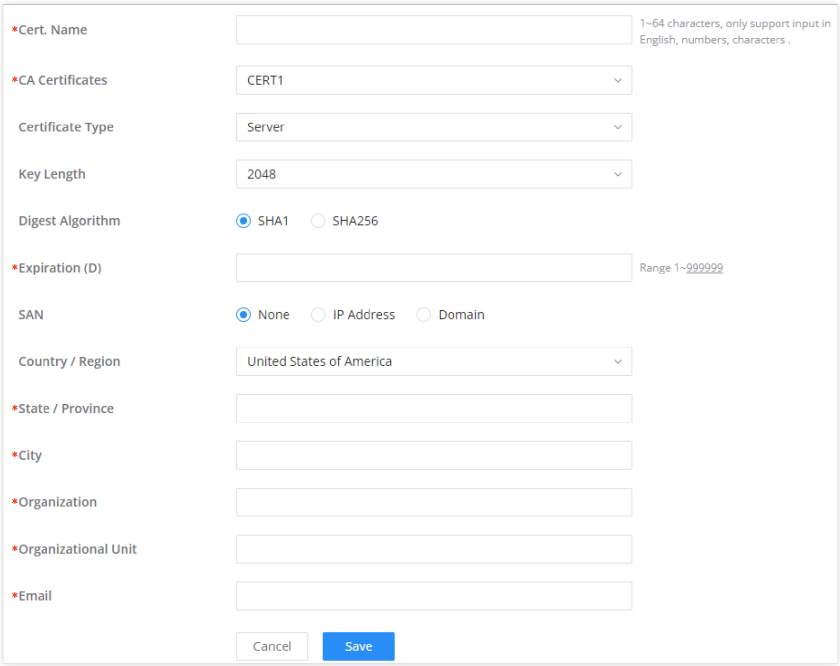
Cert. Name	Enter the Certificate name for the CA. ***Note:*** *It could be any name to identify this certificate. Example: "CATest".*
Key Length	Choose the key length for generating the CA certificate. The following values are available: ● **512:** 512-bit keys are not secure and it's better to avoid this option. ● **1024**: 1024-bit keys are no longer sufficient to protect against attacks. ● **2048:** 2048-bit keys are a good minimum. (Recommended). ● **4096:** 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: ● **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input.

	● **SHA256:** This digest algorithm generates an almost unique, fixed-size 256 bit hash. ***Note:*** *Hash is a one-way function, it cannot be decrypted back.*
Expiration (D)	Enter the validity date for the CA certificate in days. *The valid range is 1~999999..*
Country / Region	Select a country code from the dropdown list. *Example: "United Stated of America".*
State / Province	Enter a state name or province. *Example: "Casablanca".*
City	Enter a city name. *Example: "SanBern".*
Organization	Enter the organization's name. *Example: "GS".*
Organizational Unit	This field is the name of the department or organization unit making the request. *Example: "GS Sales".*
Email	Enter an email address. *Example: "EMEAregion@grandstream.com"*

Add CA Certificate

Certificate

In this section, the user can create a server or a client certificate. To create a certificate please access the web UI of the router, then navigate to **System Settings** → **Certificates** → **Add Certificate**, click "Add", then enter the necessary information regarding the certificate.



Add Certificate

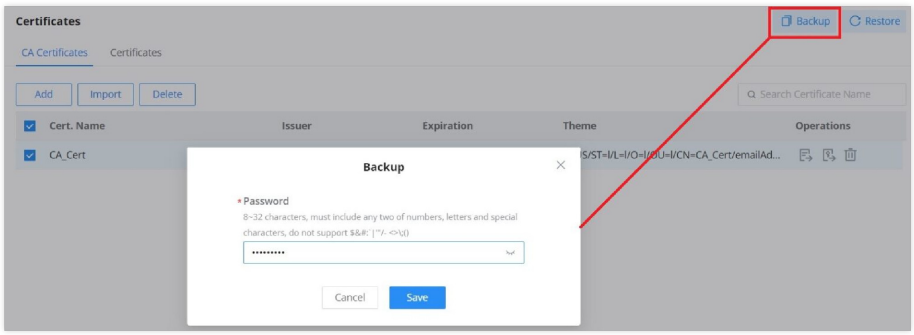
Cert. Name	Enter the certificate's name.
Key Length	Choose the key length for generating the CA certificate.The following values are available: ● **512:** 512-bit keys are not secure and it's better to avoid this option. ● **1024:** 1024-bit keys are no longer sufficient to protect against attacks.

	• **2048:** 2048-bit keys are a good minimum. (Recommended). • **4096:** 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Select the digest algorithm. • **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. • **SHA256:** This digest algorithm generates an almost unique, fixed-size 256 bit hash. **Note:** Hash is a one-way function, it cannot be decrypted back.
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country / Region	Select a country from the dropdown list of countries. Example: "United States of America".
State / Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Add Certificate

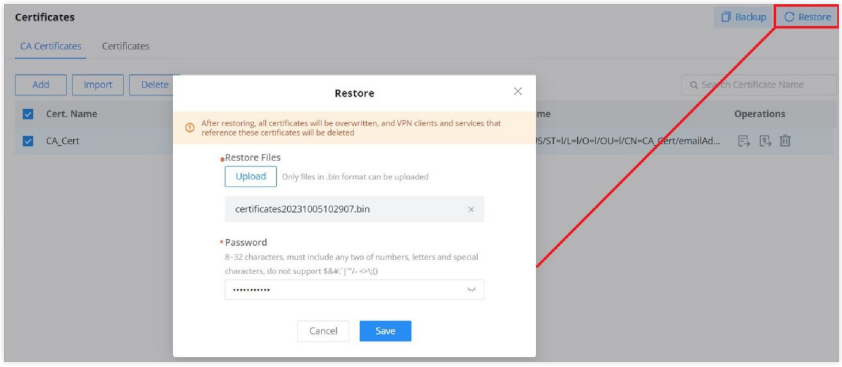
Certificates Backup and Restore

To backup the created certificates, first select all the desired certificates, then click on "**Backup**" button and enter a password to protect it as shown below:



Certificate Backup

To restore a certificate, click on "**Restore**" button, then upload the file and enter the password.



Certificate Restore

CHANGE LOG

This section documents significant changes from previous versions of the GWN700x routers 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 1.0.11.6

- Added support for VLAN2. [VLAN]
- Added support for nslookup. [System Diagnostics]
- Optimized Traceroute feature. [System Diagnostics]
- Added RADIUS configuration as a profile. [RADIUS]
- Optimized dynamic route WAN action rule. [WAN]
- Optimized WireGuard® configuration. [WireGuard®]
- Optimized Feedback configuration. [Feedback]
- Optimized Client list filtering. [Client]
- After changing the login password, the web will be forcibly logged out. [Security Management]
- OpenVPN/WireGuard® local ports automatically provide an available number. [WireGuard®][OpenVPN®]
- Added support for switch management. [Switch Management]
- Added switch statistics to the dashboard. [Overview]
- Added support for dynamic routing: OSPF/RIP/BGP. [OSPF] [RIP] [BGP]
- Added VPN configuration wizard. [VPN Setup Wizard]
- Added support for 6G band. [Overview]
- Added support for captive portal on wired network. [Captive Portal]
- Added multiple language support. [Web UI Languages]
- Added FQDN and FQDN group profile. [FQDN]
- Added object grouping profile support. [Profiles]
- Added support for nslookup [NSlookup]
- Added support for TR069, settings can be found under Maintenance. [tr-069]
- Cloud/Manager connection detection support multiple links. [Manager Servers Settings]
- Added "Service Name" filed to the WAN PPPoE configuration. [WAN]
- Added the feature Email Settings. [Email Settings]
- Added support for Standby on Demand mode for PPPoE. [WAN]
- Added standby mode in policy routing. [Policy Routing]
- Added the ability to detect the public IP when the GWN700x is behind another router. [GDMS Networking]
- GDMS Networking/GWN Manager connection detection support multiple links. [GDMS Networking/GWN Manager]
- Added support for cloud configuration of DDNS IP source and update interval. [DDNS]
- Added supports for cloud configuration of exempt IP, DoS defense, and Spoofing defense.
- Added support for cloud security alerts.
- Added support to configure blackhole for static routes. [Static Routes]
- Added support for exporting .ovpn files [VPN Remote Users]
- Optimized Alert & Notifications Web UI. [Alert & Notifications]
- Added support for setting up multiple NTP servers. [NTP Server]

Firmware Version 1.0.5.36

- No major change

Firmware Version 1.0.5.35

- No major change

Firmware Version 1.0.5.30

- Added the new feature of Speed test [WAN]

Firmware Version 1.0.5.7

- Removed the DHCP range restriction on Static IP assignment which was added in 1.0.5.6 [Static IP Binding]

Firmware Version 1.0.5.6

- Added new feature of WAN-Bridge Mode and VLAN tag priority [WAN]
- Added new feature of disabling the router ports [Port Configuration]
- Added more services under DHCP option 43 [LAN]
- Added IGMP proxy and IGMP snooping [IGMP]
- Added new feature of IP Routed Subnet [LAN]
- Added Bonjour Gateway [Bonjour Gateway]
- Added Binding Mode and Device Name under Static IP Binding [Static IP Binding]
- Added new feature of transferring GWN APs taken over by GWN router to GWN Cloud/Manager [AP Management]
- Added Client list under Access Point for clients connected currently to the AP [Access Points]
- Added PPSK (Private Pre-Shared Key) feature [PPSK]
- Added SSID Bandwidth limit feature with schedule support [SSIDs]
- Added WireGuard® VPN [WireGuard®]
- Added new feature of exporting clients list [Clients]
- Added clients bandwidth limit feature with schedule support [Clients]
- Added Bandwidth limit feature for both wireless and wired clients [Bandwidth Limit]
- Added more social authentication (Facebook, Twitter and Google) under Captive portal [Splash Page]
- Added Vouchers feature under Captive Portal [Vouchers]
- Added new feature of exporting Guest list [Guests]
- Added support for more alerts [Alerts]
- Added new feature of naming the GWN router [Basic Settings]
- Added new feature of customizing the Hostname [Web Service]
- Added GWN.Cloud/Manager connection status detection [System Diagnostics]
- Added EEE (Energy-Efficient Ethernet) feature [Port Configuration]
- Added the option to display a month-long time period in traffic statistics (only for GWN7003) [Traffic Statistics]
- Added TURN Service feature [TURN Service]

Firmware Version 1.0.3.5

- No major changes.

Firmware Version 1.0.3.4

- Added new feature of TURN server (Beta) [TURN Service]
- Added new feature of 2.5G SFP module support [Port Configuration]
- Added QoS bandwidth statistics feature [QoS]

Firmware Version 1.0.1.6

- This is the initial release.