

Grandstream Networks, Inc.

GWN700X

User Manual



GWN700X - 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 GWN.Cloud 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 <i>*All ports are WAN/LAN configurable.</i>	2x 2.5 Gigabit SFP ports and 4x Gigabit Ethernet ports <i>*All ports are WAN/LAN configurable</i>	2x 2.5 Gigabit SFP ports and 9 x Gigabit Ethernet ports <i>*All ports are WAN/LAN configurable</i>
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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Efficiency	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°C to 40°C Storage: -30°C to 60°C Humidity: 10% to 90% Non-condensing		

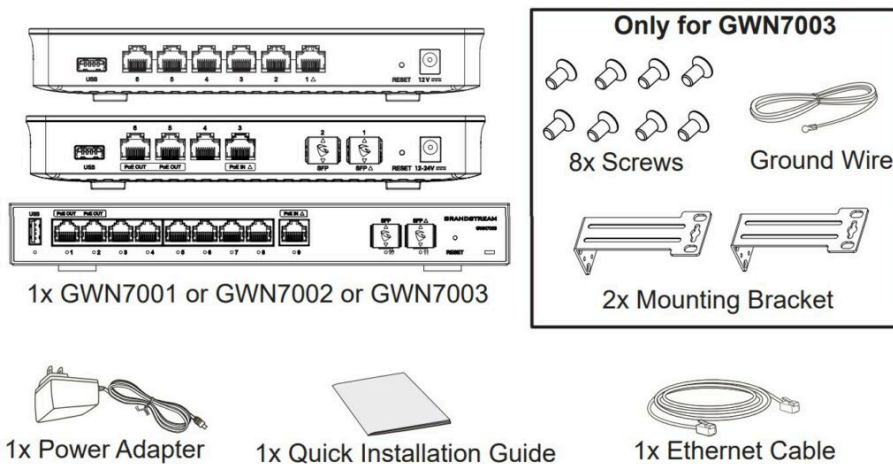
Physical	Unit Dimension: 210mm(L)x130mm(W)x35mm(H); Unit Weight: 453g Entire Package Dimension: 246mm(L)x235mm(W)x45mm(H); Entire Package Weight: 672g	Unit Dimension: 210mm(L)x130mm(W)x35mm(H); Unit Weight: 505g Entire Package Dimension: 246mm(L)x235mm(W)x54mm(H); Entire Package Weight: 730g	Unit Dimension: 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

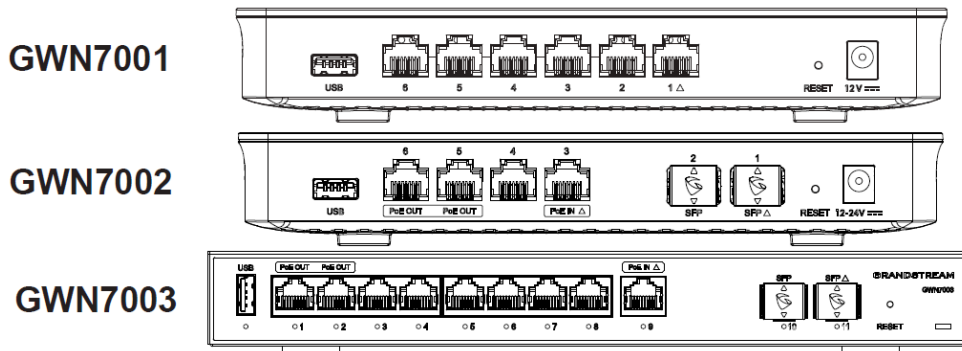
Before deploying and configuring the GWN700x router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN700x router.

Package Contents



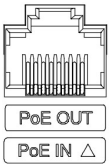





GWN700x Package Content

GWN700x Ports



GWN700x ports

No.	Port	Description
-----	------	-------------

1		<ul style="list-style-type: none"> ● GWN7001: 6x Gigabit Ethernet ports ● GWN7002: 4x Gigabit Ethernet ports ● GWN7003: 9 x Gigabit Ethernet ports <p>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).</p>
2		2x 2.5 Gigabit SFP ports (GWN7002/7003 only).
3		USB 2.0 port
4		<ul style="list-style-type: none"> ● 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		Factory Reset pinhole. Press for 5 seconds to reset factory default settings

GWN700x ports

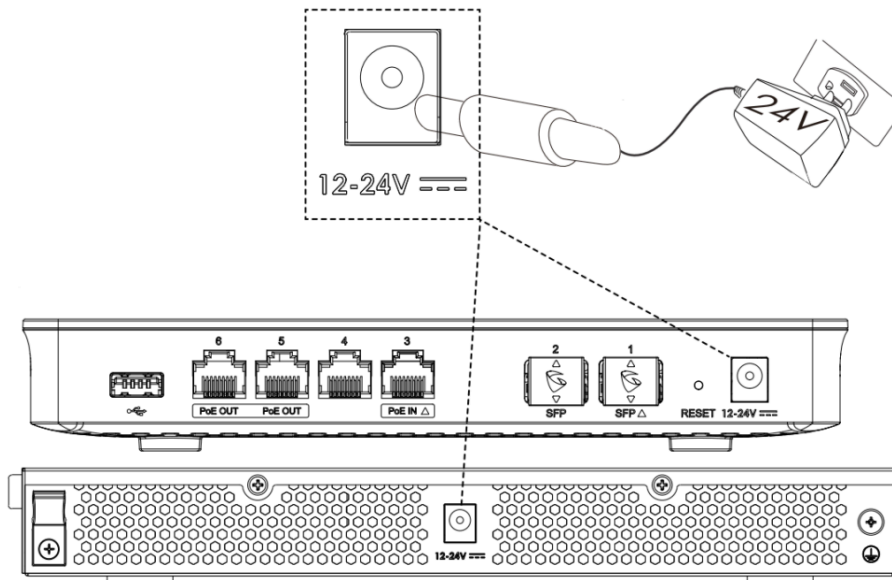
Note:

Ports with this symbol Δ 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).

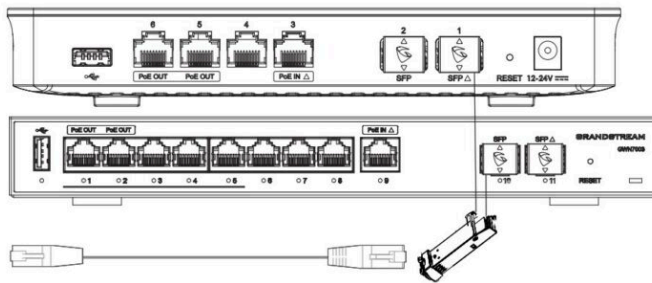


Powering the GWN700x routers

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.

Internet
 Optical Fiber
 ADSL Modem
 Community Broadband



Connect GWN700x to the Internet

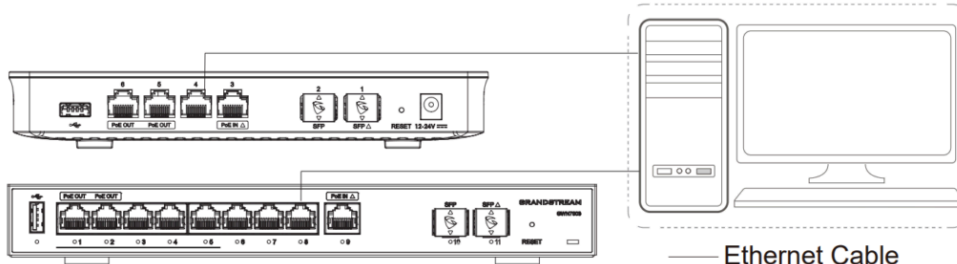
Note:

The Δ sign indicates the default WAN ports:

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

3. Connect to GWN7002/7003 Network

Connect your computer to one of the LAN ports.

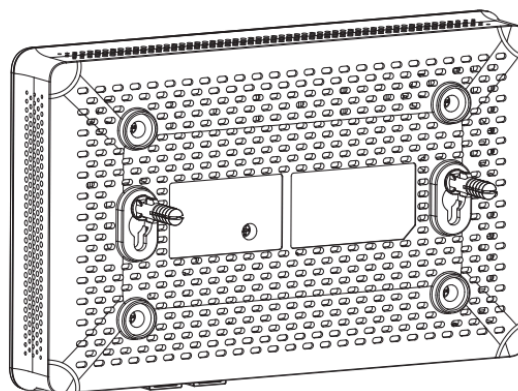
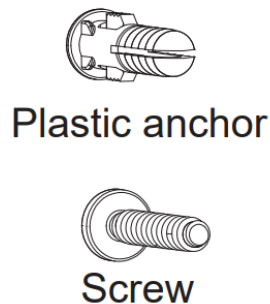


GWN700x network

GWN700x installation

o **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.

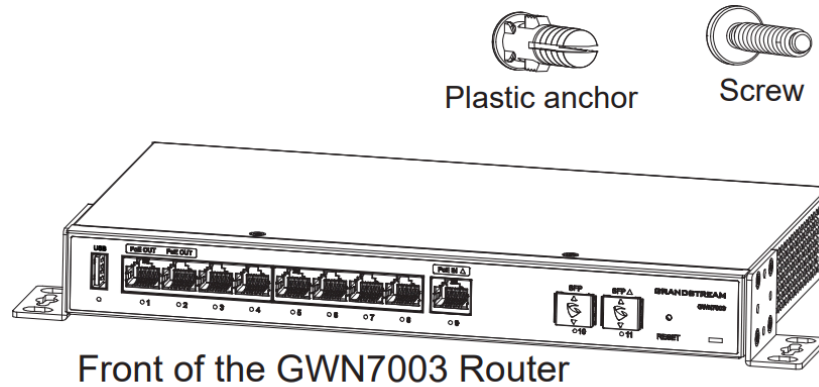


Bottom of the
 GWN7001/GWN7002
 Router

GWN7001/7002 Wall Mounting

o **Mounting GWN7003 to the Wall**

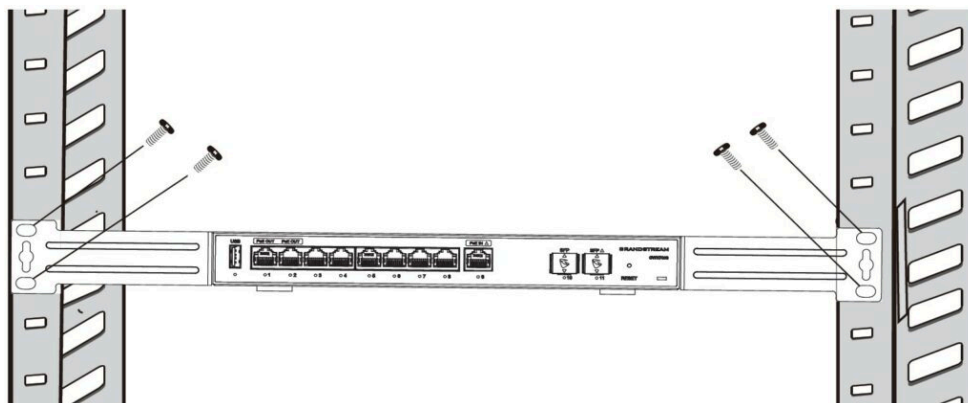
1. Use the provided screws to fix the two L-shaped Mounting bracket (rotated 90°) on both sides of the GWN7003 router.
2. Stick the router port up and horizontally on the selected wall, mark the position of the screw hole on the L-shaped mounting brackets with a marker. Then, drill a hole at the marked 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

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

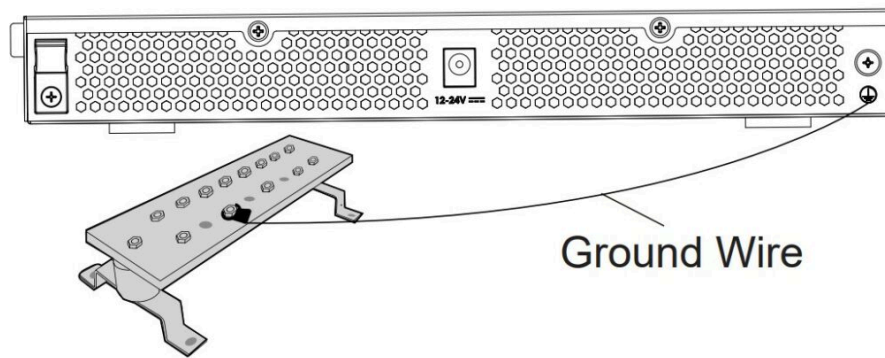
1. Check the grounding and stability of the rack.
2. Install the two L-shaped rack-mounting in the accessories on both sides of the router, and fix them with the screws provided.
3. Place the router in a proper position in the rack and support it by the bracket.
4. Fix the L-shaped rack mounting to the 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

o **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.



Ground Wire

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.

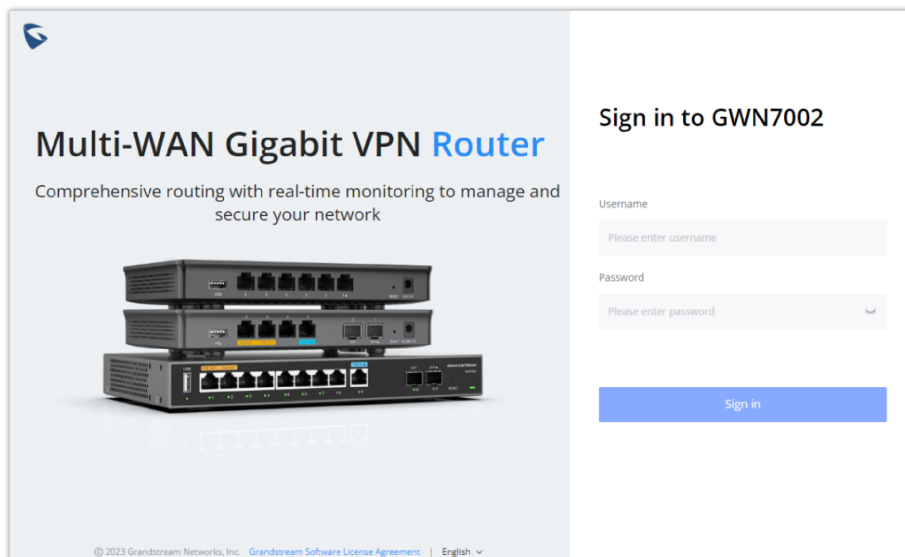
GETTING STARTED

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.

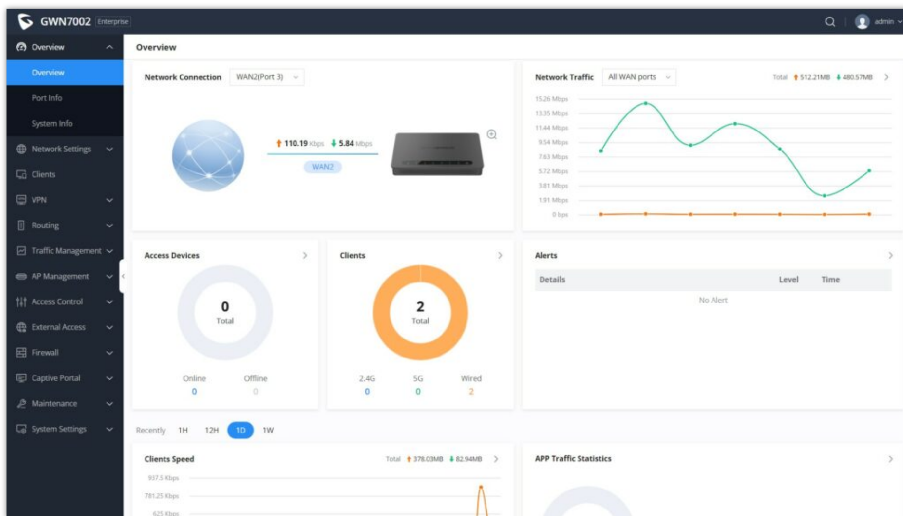


To access the Web GUI:

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.

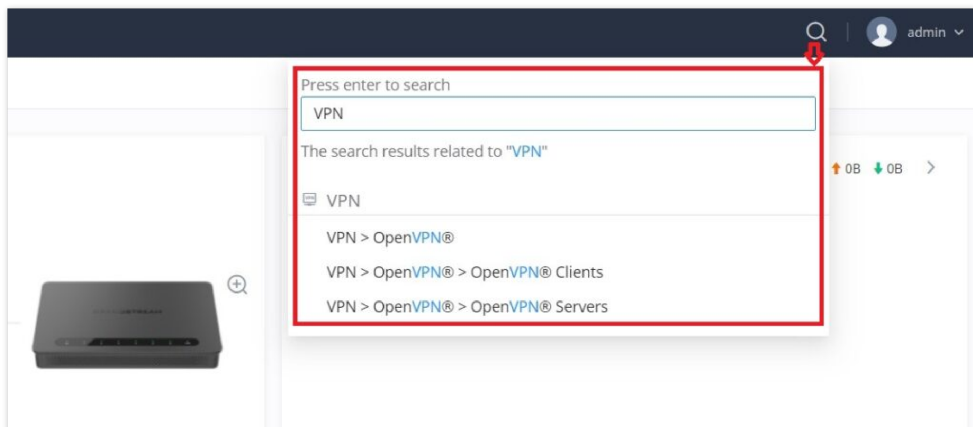
Once the user enters the password, this is the initial page that will be shown. This page contains general information and status about the router.



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.

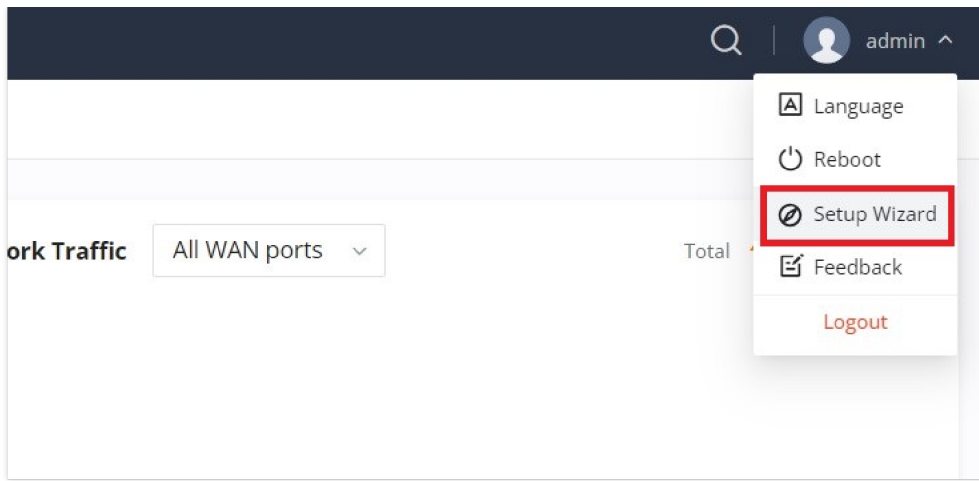


Search


Setup Wizard and Feedback

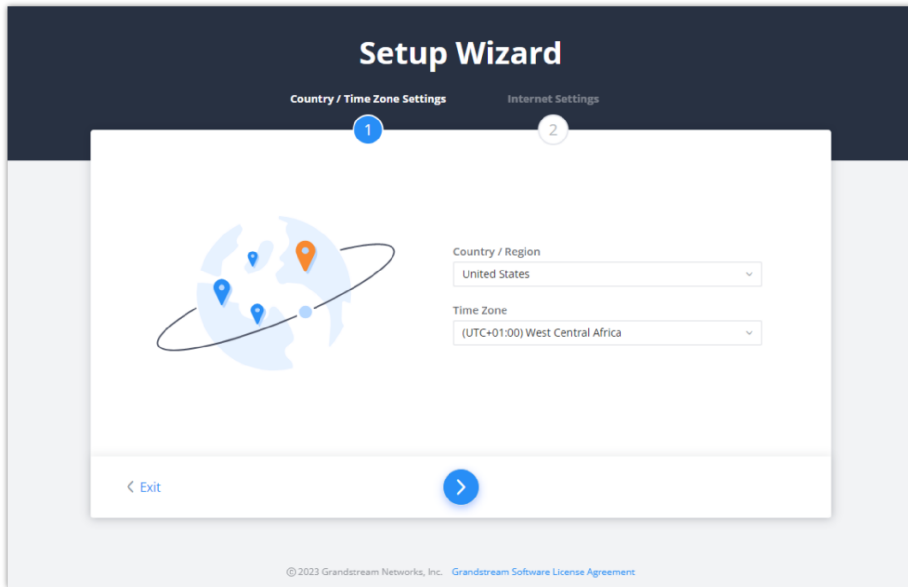
Setup Wizard

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

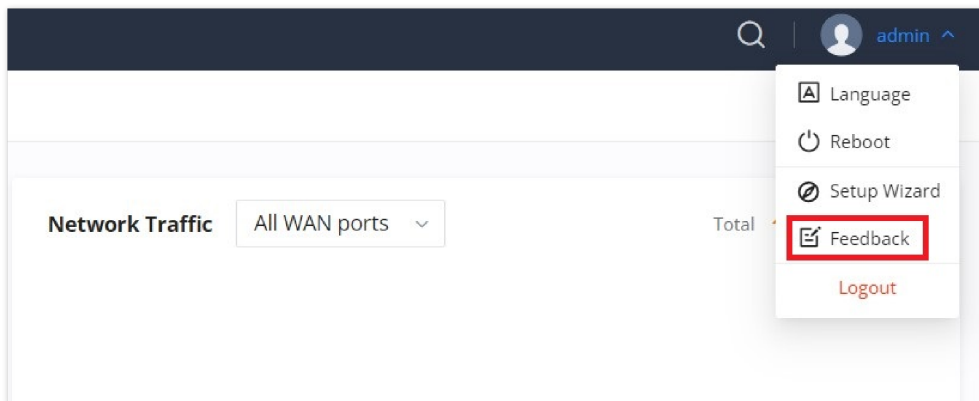
Click on  button to go through the setup wizard.



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

Feedback ✕

***Questions & Suggestions**

0/300

+
 Support JPEG, JPG, PNG image

Upload syslog at the same time.(Easy to better locate the problem)

***Contact Email Address**

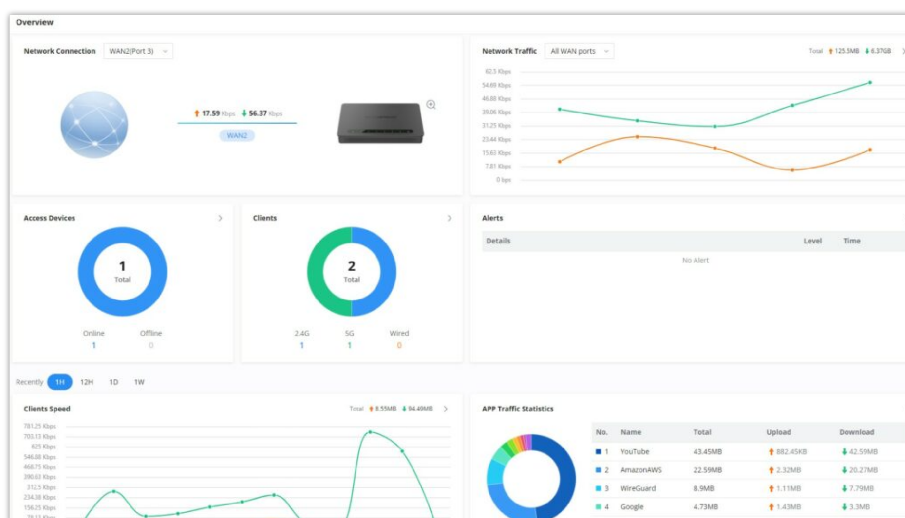
Cancel
Submit

Feedback – part 2

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	<p>Displays the current state of the network connection for the selected WAN port and shows the current upload and download speed.</p> <p>Note: the user can select the WAN port from the drop-down list.</p>
Network Traffic	<p>Shows network traffic in real time.</p> <p>Note: the user can select the WAN port from the drop-down list or select All WAN ports.</p>
Access Devices	<p>shows the total number of Access Devices online and offline.</p>
Clients	<p>Shows the total number of clients connected either wirelessly (2.4G and 5G) and also wired connections.</p>

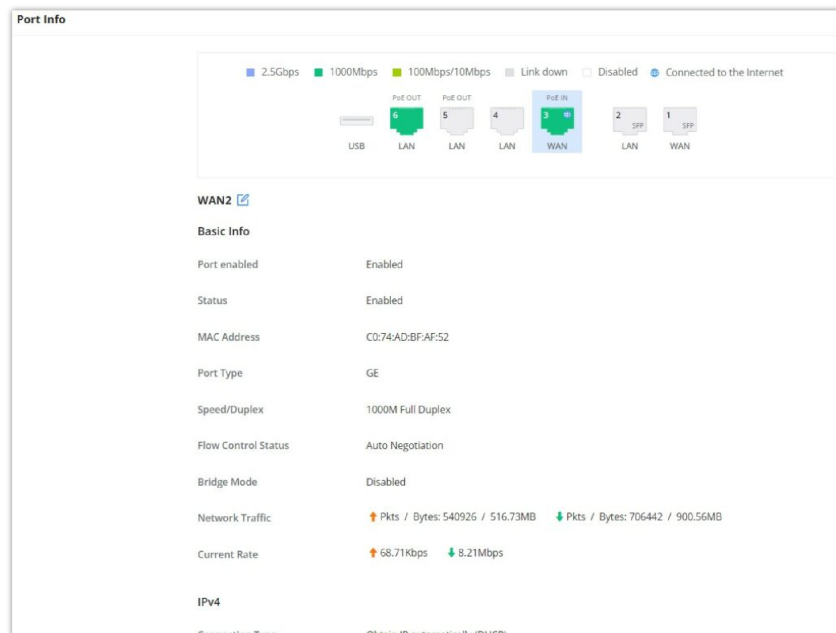
Alerts	Shows Alerts General, Important or Emergency with details and time.
Clients Speed	Displays Clients speed based on time (1H, 12H, 1D or 1W)
APP Traffic Statistics	Displays traffic statistics based on apps usage (%).
Top Clients	Shows the Top Clients list, users may assort the list of clients by 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	
Device Name	GWN7002 ✎
Hardware Version	V1.3A
System Version	1.0.4.6
MAC Address	C0:74:AD: [REDACTED]
Part Number	9 [REDACTED]
Serial Number	2 [REDACTED]
Boot Version	0.0.0.5
System Up Time	11min
System Time	2023-10-03 15:10
CPU Usage	Total: 25% CPU0: 28% CPU1: 22%
Memory Usage	71%
Load Average	1min: 2.16 5min: 2.22 15min: 1.45
Temperature ⓘ	83°C

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	Port Enable	Port Type	Name	Role	Speed/Duplex	Flow Control
Port 1	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 2	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 3	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 4	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 5	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 6	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 7	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 8	<input checked="" type="checkbox"/>	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port 9	<input checked="" type="checkbox"/>	GE	WAN2	WAN	Auto Negotiation	Auto Negotiation
Port 10	<input checked="" type="checkbox"/>	SFP	-	LAN	Auto Negotiation	Disable
Port 11	<input checked="" type="checkbox"/>	SFP	WAN1	WAN	Auto Negotiation	Disable

Cancel Save

Auto Negotiation
1000M Full Duplex
2500M Full Duplex

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. <ul style="list-style-type: none"> ● GE: Stands for Gigabit Ethernet ● SFP: Small form-factor Pluggable
Name	This indicates the port name.
Role	This indicates the port role. <ul style="list-style-type: none"> ● 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: <i>Half Duplex</i> and <i>Full Duplex</i> . 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 <i>Auto Negotiation</i> , 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.

The screenshot shows the PoE Configuration interface. At the top, there is a 'Total Power Limit' section with three radio buttons: 'Auto' (selected), '12.8W', and '24.8W'. Below this is a table with columns: 'Port', 'Power Supply Mode', 'Maximum Power Supply', and 'Priority'. The table contains two rows: 'Port 5' with 'Active PoE(802.3af/at)', '5.2W', and 'Low'; and 'Port 6' with 'Active PoE(802.3af/at)', '9W', and 'High'.

Port configuration – PoE configuration

<p>Total Power Limit</p>	<p>This configures the power limit which can be supplied through PoE.</p> <ul style="list-style-type: none"> ● 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.
<p>Port</p>	<p>This field indicates the port number.</p>
<p>Power Supply Mode</p>	<p>This option configures the power supply mode.</p> <ul style="list-style-type: none"> ● Active PoE (802.3af/at) ● 48V Passive PoE ● Off <p>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.</p>
<p>Maximum Power Supply</p>	<p>Configures the maximum power supplied by the router.</p> <ul style="list-style-type: none"> ● 5.2W ● 9W ● 12.8W <p>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.</p>
<p>Priority</p>	<p>Specify the priority of the port in terms of the power supply.</p> <ul style="list-style-type: none"> ● 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 GWN.Cloud 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 Name	Status	Port	Connection Type	IPv4 Address	IPv4 Status	IPv6 Address	IPv6 Status	VPN Connection Type	VPN IP Address	Operations
WAN2	<input checked="" type="checkbox"/>	Port3 (GE)	IPv4: DHCP IPv6: -	192.168.5.99	Connected	Local IPv6: - Global IPv6: -	Disconnected	-	-	
WAN4	<input checked="" type="checkbox"/>	Port4 (GE)	IPv4: DHCP IPv6: -	-	Disconnected	Local IPv6: - Global IPv6: -	Disconnected	-	-	

WAN page

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

WAN > Add WAN

Basic Information ^

Status:

*WAN Name: 1-64 characters

*Port:

IPv4 Settings ^

Connection Type:

Static DNS:

*Maximum Transmission Unit (MTU): Default 1500, range 576-1500

*Tracking IP Address 1:

Tracking IP Address 2:

VLAN Tag:

Bridge Mode:

*VLAN Tag ID / Port / Priority

VLAN Tag ID: Port: Priority:

Multiple Public IP Address:

VPN:

IPv6 Settings v

Add or Edit WAN

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

Basic Information	
Status	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	<ul style="list-style-type: none"> ● Obtain IP automatically (DHCP): When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. ● Enter IP Manually (Static IP): When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. ● Internet Access with PPPoE account (PPPoE): When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval, and Inter-Key Timeout (in seconds). <p><i>The default setting is "Obtain IP automatically (DHCP)".</i></p>
Static DNS	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 alternative DNS Server, ex: 1.1.1.1

Maximum Transmission Unit (MTU)	<p>Configures the maximum transmission unit allowed on the wan port.</p> <ul style="list-style-type: none"> • When using Ethernet, the valid range that can be set by the user is 576-1500 bytes. The default value is 1500. Please do not change the default value unless you have to. • When using PPPoE, the valid range that can be set by the user is 576-1492 bytes. The default value is 1492. Please do not change the default value unless you have to.
Tracking IP Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal.
Tracking IP Address 2	Add another alternative address for Tracking IP Address
VLAN Tag	Toggle ON or OFF to enable or disable VLAN Tag
VLAN Tag ID	<p>Enter the VLAN Tag ID with the priority</p> <p>Note: priority is 0~7 with 7 being the highest priority. Default is 0.</p>
Multiple Public IP Address	<p>Toggle ON or OFF to enable or disable Multiple Public IP Address</p> <p>Note: Please use with Port Forward function, so that you can access to router via public IP address.</p>
Public IP Address	<p>Enter a public IP address</p> <p>Note: Click on "Plus" or "minus" icons to add or delete public IP addresses.</p>
VPN	Toggle ON or OFF to enable or disable VPN
VPN Connection Type	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Dynamic IP: The IP will be assigned statically using DHCP. • Static IP: The IP will be assigned statically.
VPN Static DNS	Enable this option to use the statically assigned DNS server addresses.
Maximum Transmission Unit (MTU)	<p>This configures the value of the maximum transmit unit. The valid range for this value is 576 - 1460. The default value is 1430.</p> <p>Note: Please do not change this value unless it's necessary.</p>
IPv6 Settings	
IPv6	Enable this option to use IPv6 on this specific WAN port.

Connection Type	<ul style="list-style-type: none"> • Obtain IP automatically (DHCPv6) • Enter the IP manually (static IPv6) • Internet Access with PPPoE account (PPPoE): must enabled and configured on IPv4.
IPv6 Address	When the Connection Type is set to <i>Static IP</i> , the user can enter the static IP address in this field. Note: This option appears only when the Connection Type is set to <i>Static IPv6</i> .
Prefix Length	Enter the prefix length. Note: This option appears only when the Connection Type is set to <i>Static IPv6</i> .
Default Gateway	Enter the IP address of the default gateway Note: This option appears only when the Connection Type is set to <i>Static IPv6</i> .
Preferred DNS Server	Enter the IP address of the preferred DNS server. Note: This option appears only when the Connection Type is set to <i>Static IPv6</i> .
Alternative DNS Server	Enter the IP address of the alternative DNS server Note: This option appears only when the Connection Type is set to <i>Static IPv6</i> .
Static DNS	Enable this option to enter statically assigned DNS. Note: This option appears only when the Connection Type is set to DHCPv6.
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.

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:

WAN > Add WAN

VLAN Tag

*VLAN Tag ID Priority

Bridge Mode

*VLAN Tag ID/Port/Priority	VLAN Tag ID	Port	Priority
	34	LAN1 (GE) ×	4
	35	LAN2 (GE) ×	5
	36	LAN3 (GE) ×	6

Add +

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					
VLAN VLAN Port Settings Static IP Binding Local DNS Records Bonjour Gateway					
<input type="button" value="Add"/> <input type="button" value="Delete"/>					
<input type="checkbox"/>	VLAN ID	Name	IPv4 Address	IPv6 Address	Operations
<input type="checkbox"/>	1	Default LAN	192.168.80.1	-	
<input type="checkbox"/>	20	Guests	190.168.20.1	-	

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.

- o **Add or Edit VLAN**

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

LAN > Add VLAN

*VLAN ID: Range 3-4094

Name: 0-64 characters

Destination: x

VLAN Port IPv4 Address:

* IPv4 Address:

* Subnet Mask:

DHCP Service:

* IPv4 Address Allocation Range: -

* Release Time(m): Default: 120, range 60-2880

DHCP Option: Option Type Service Content

Preferred DNS Server:

Alternative DNS Server:

IPv4 Routed Subnet:

* Interface:

VLAN Port IPv6 Address:

Add or Edit VLAN

VLAN ID	Enter a VLAN ID Note: VLAN ID range is from 3 to 4094.
Name	Enter the VLAN name
Destination	To fast configure the VLAN's single-way data communication with WANs, other VLANs and VPNs. The option selected by default will be based on "Policy Routing" option to keep the default route accessible.
VLAN Port IPv4 Address	
IPv4 address	Enter IPv4 Address
Subnet Mask	Enter Subnet Mask
DHCP Server	By default it's "Off", choose "On" to specify 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	<p>Select the option, type, service and content for each DHCP option. Click on "Plus" or "Minus" icons to add or delete an entry.</p> <ul style="list-style-type: none"> ● 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. ● 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.
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	<p>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.</p>
IPv6 Address Assignment	<p>Select from the drop-down list the IPv6 address assignment</p> <ul style="list-style-type: none"> ● Disable ● SLAAC ● Stateless DHCPv6 ● Stateful DHCPv6



Add/edit VLAN

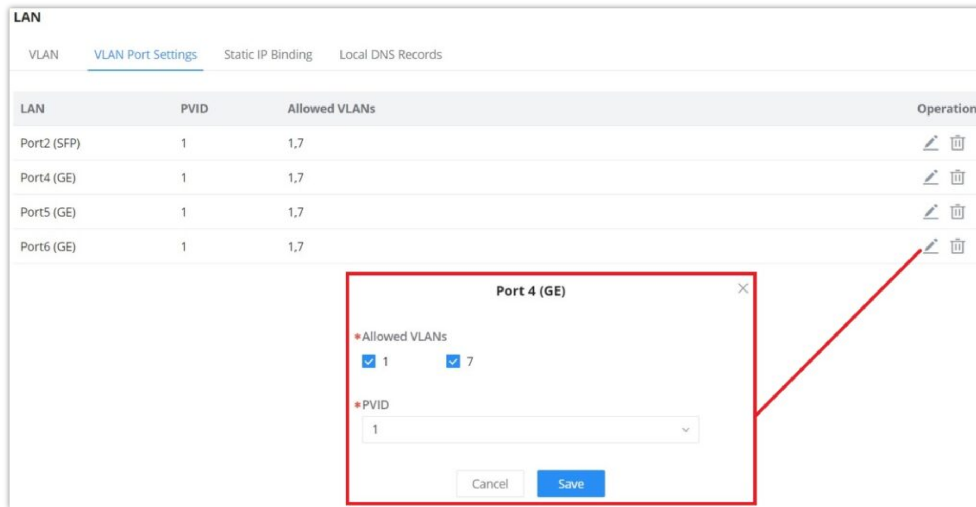
Note

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

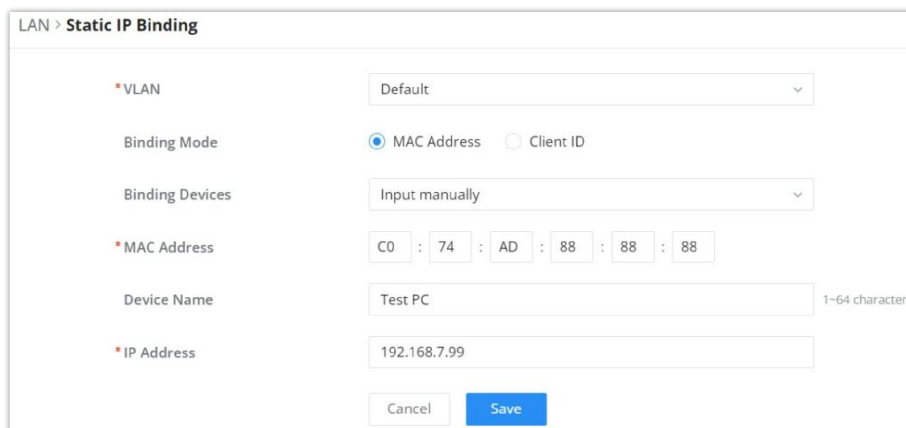
Allowed VLANs	Choose the VLANs to be allowed on this port.
PVID	Select the Port VLAN Identifier or the default VLAN ID

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 binding mode is set to MAC Address.

Client ID Type	Select the client ID type, either based on: <ul style="list-style-type: none"> • MAC Address • ASCII • Hex <i>Note: only available bindind mode is set to Client ID.</i>
MAC Address	Enter the MAC Address <i>Note: only available bindind mode or Client ID Type is set to MAC Address</i>
ASCII	Enter the ASCII <i>Note: only available Client ID Type is set to ASCII</i>
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. <i>Note: only available Client ID Type is set to Hex</i>
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

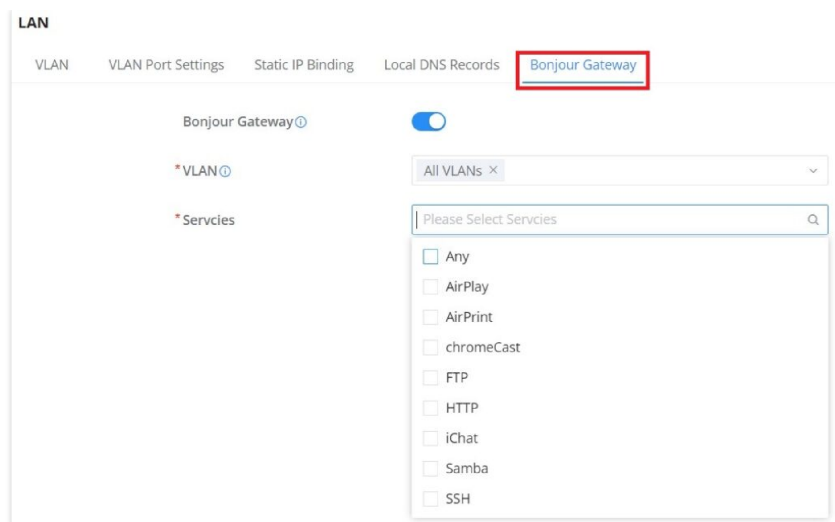
- Enter the domain name in "Domain"
- Then, enter the IP address to which the domain name will be mapped to.
- Toggle on the "Status" for the mapping to take effect.

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

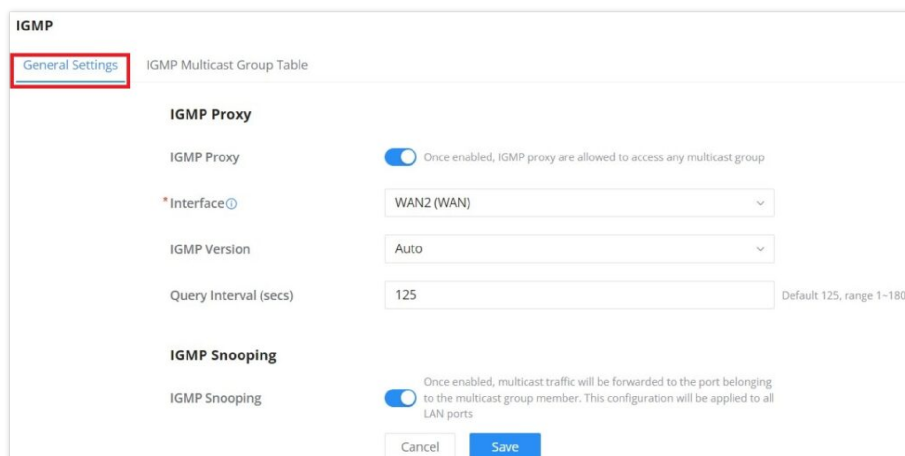
IGMP

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:

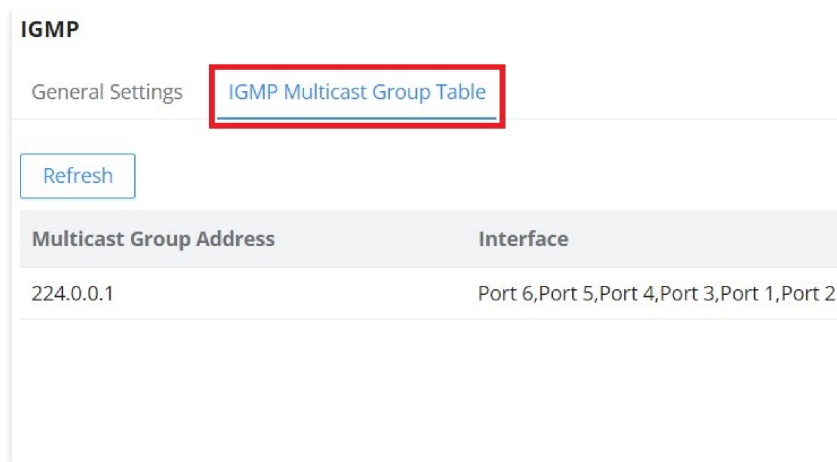
1. Toggle ON IGMP Proxy first.
2. Select the WAN interface to be used from the drop-down list (**Note:** IGMP proxy cannot be enabled on a WAN port with bridge mode enabled)
3. Select the version, be default is Auto.

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

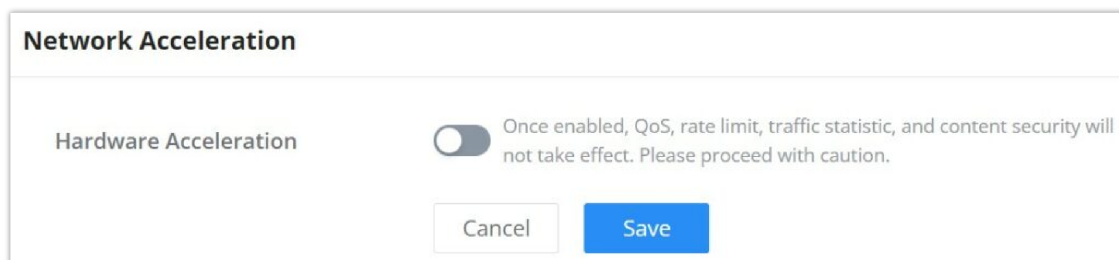
On the IGMP Multicast Group Table, all the active multicast groups will be displayed here.



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.

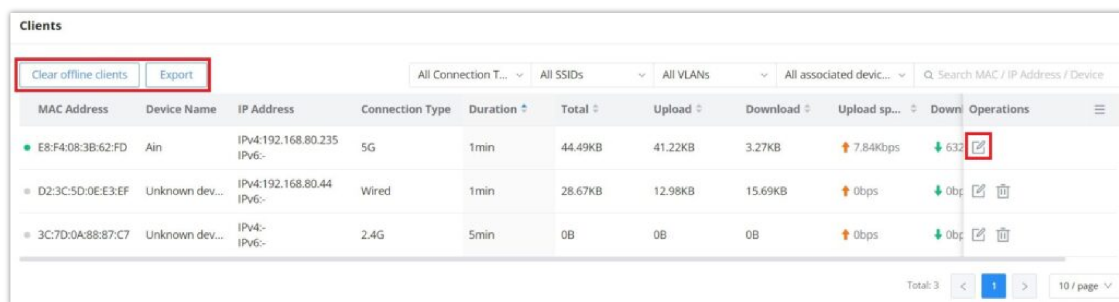
CLIENTS

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.

Please refer to the figure and table below:



Clients Page

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	<p>This section shows the medium of connection that the device is using. There are two mediums which can be used to connect:</p> <ul style="list-style-type: none"> ● 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 <i>Received Signal Strength Indicator</i> . 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:

Clients > **Edit Client**

Device Name: 1-64 characters

Bandwidth Limit:

Maximum Upload Bandwidth: Mbps The range is 1-1024, if it is empty, there is no limit

Maximum Download Bandwidth: Mbps The range is 1-1024, if it is empty, there is no limit

Bandwidth Schedule:

* Schedule:


Static IP:

* VLAN:

* IP Address: Range 192.168.80.2-192.168.80.254

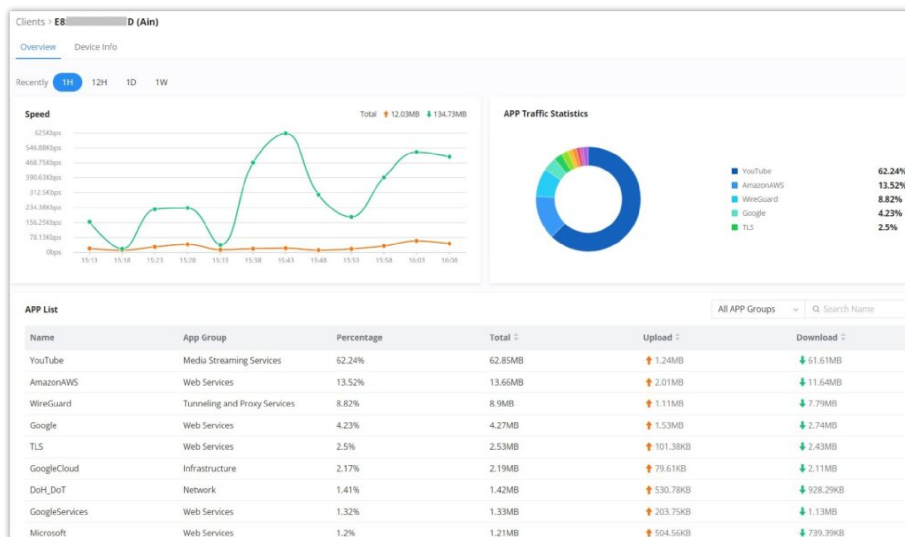
Edit Device

o **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.

o **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.

Clients > ██████████ (DESKTOP-IVU4H2Q)	
Overview Device Info	
MAC Address	██████████
Device Name	DESKTOP-IVU4H2Q
IPv4 Address	192.168.80.64
IPv6 Address	-
Connection Type	Wired
Channel	-
SSID Name	-
Associated Device	C0:74:AD:BF:AF:50
Duration	22min
RSSI	-
Station Mode	-
Network Traffic	756.46MB ↑ 363.09MB ↓ 393.38MB
Current Rate	↑ 48.19Kbps ↓ 434.4Kbps
Link Rate	-
Manufacture	-
OS	WINDOWS

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 (Beta)
- **OpenVPN®:** Client and server
- **L2TP:** Client
- **WireGuard®:** Server

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

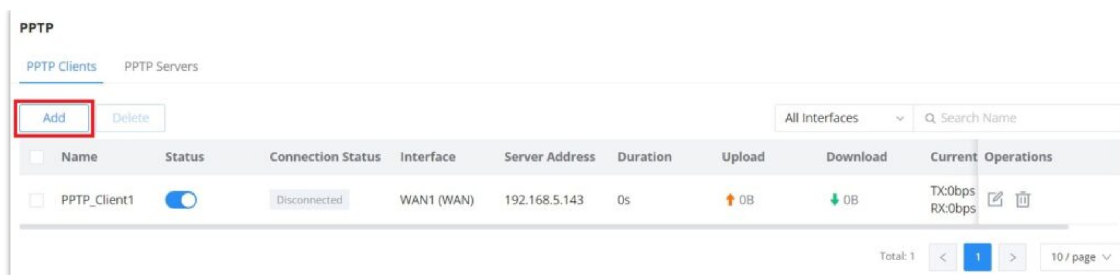
PPTP

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

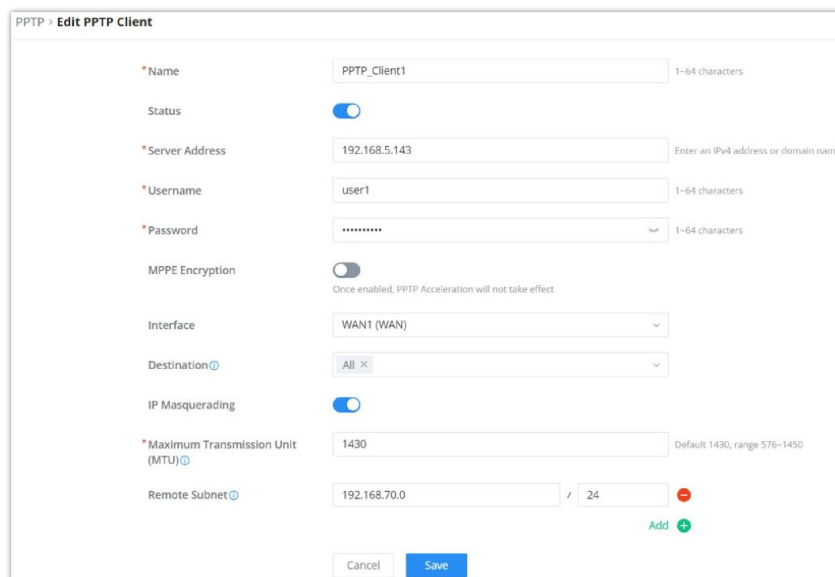
To configure the PPTP client on the GWN700x, navigate under **VPN** → **PPTP** → **PPTP Clients** and set the followings:

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. <i>By default, it's disabled.</i>
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	<p>Configures the remote subnet for the VPN.</p> <p>The format should be "IP/Mask" where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32.</p> <p>example: 192.168.5.0/24</p>
----------------------	---

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. <i>By default, it's disabled.</i>
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.

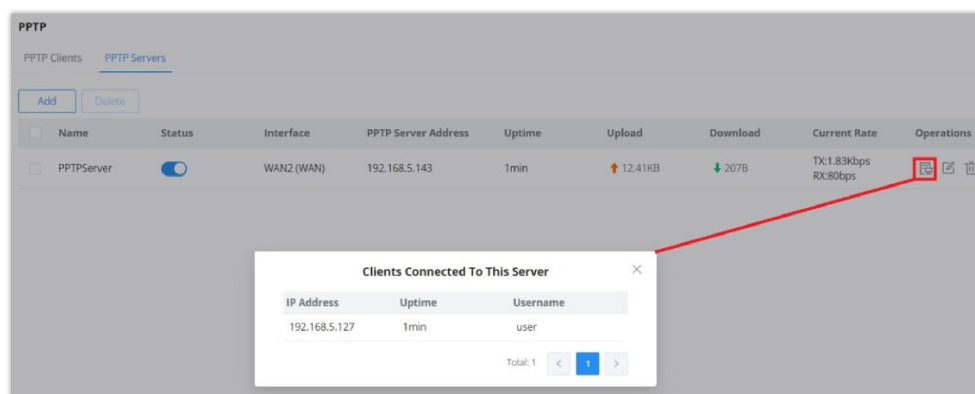
LCP Echo Adaptive	<ul style="list-style-type: none"> • Once enabled: LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request. • Once disabled: the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval
Debug	Toggle 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. <i>Ex: 8.8.8.8</i>
Alternative DNS Server	specify the alternative DNS server. <i>Ex: 1.1.1.1</i>

PPTP Sever

○ **Create the remote user credentials:**

To create the remote user account which will be required to be entered on the client side 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

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.

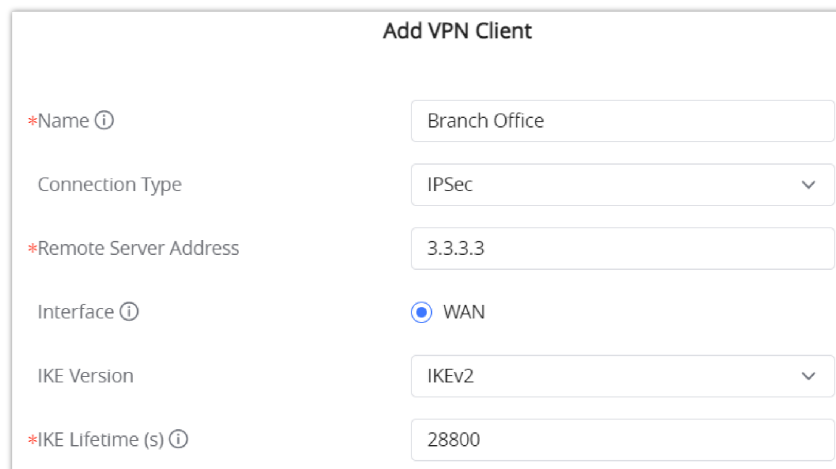
IPSec Site-to-Site

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	
*Name ⓘ	Branch Office
Connection Type	IPSec ▼
*Remote Server Address	3.3.3.3
Interface ⓘ	<input checked="" type="radio"/> WAN
IKE Version	IKEv2 ▼
*IKE Lifetime (s) ⓘ	28800

Add VPN Client – IPSec

○ Phase 1

Phase 1 ^

Negotiation Mode Main Aggressive

*Pre-shared Key 1-64 characters

Encryption Algorithm

Hash Algorithm

DH Group

Local ID

Remote ID

Reconnect

*Number of Reconnect The default value is 10, and the valid range is 0-10. Value 0 means that it has been trying to negotiate connection.

DPD

*DPD Delay Time (sec) Default: 30, range 10-900

*DPD Idle Time (sec) Default: 120, range 10-900

DPD Action Hold Clear Restart

Add VPN Client – Phase 1

○ **Phase 2**

Phase 2 ^

*Local Subnet /

*Local Source IP Address

*Remote Subnet /

*IPSec SA Lifetime (sec) Default: 3600, range 600-86400

Security Protocol ESP

ESP Encryption Algorithm

ESP Hash Algorithm

Encapsulation Mode Tunnel Mode

PFS Group

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 create the remote user account which will be required to be entered on the client side and authenticated on the server side, please refer to the [Remote Users](#) section.

IPSec Client-to-Site

Note

Please note that this feature is still in its beta testing phase.

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

Click on [+ Add](#) 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. <ul style="list-style-type: none"> • 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	<p>Choose the authentication mode.</p> <ul style="list-style-type: none"> • SSL • User Authentication • SSL + User Authentication • PSK
Encryption Algorithm	<p>Choose the encryption algorithm. The encryption algorithms supported are:</p> <ul style="list-style-type: none"> • 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	<p>Select the digest algorithm. The digest algorithms supported are:</p> <ul style="list-style-type: none"> • MD5 • RSA-MD5 • SHA1 • RSA-SHA1 • DSA-SHA1-old • DSA-SHA1 • RSA-SHA1-2 • DSA • RIPEMD160 • RSA-RIPEMD160 • MD4 • RSA-MD4 • ecdsa-with-SHA1 • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 • RSA-SHA224 • SHA256 • SHA384 • SHA512 • SHA224 • whirlpool
TLS Identity Authentication	<p>Enable TLS identity authentication direction.</p>
TLS Identity Authentication Direction	<p>Select the indentity authentication direction.</p> <ul style="list-style-type: none"> • 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	<p>Enter the TLS pre-shared key.</p>
Routes	<p>Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.</p>
Deny Server Push Routes	<p>If enabled, client will ignore routes pushed by the server.</p>

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**.

OpenVPN® > Add OpenVPN® Server

•Name 1-64 characters

Status

Protocol UDP TCP

Interface

Destination

•Local Port Default: 1194, range 1-65535

Server Mode

Encryption Algorithm

Digest Algorithm

TLS Identity Authentication

Allow Duplicate Client Certificates

Redirect Gateway

Push Routes /

LZO Compression On Off Adaptive

Create OpenVPN® Server

Click 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. <i>The default protocol is UDP.</i>
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. <i>The default value is 1194.</i>
Server Mode	Choose the server mode the OpenVPN® server will operate with. 4 modes are available: <ul style="list-style-type: none"> ● SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). ● User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). ● SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. ● PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
TLS Identity Authentication	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 Identity 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. <i>Example: 10.0.0.1/8</i>
LZO Compression Algorithm	Select whether to activate LZO compression or no, if set to "Adaptive", the server will make the decision whether this option will be enabled or no.

Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificate	Select a generated CA from the dropdown list or add one.
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.
IPv4 Tunnel Network/Mask Length	Enter the network range that the GWN70xx will be serving from to the OpenVPN® client. 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 create the remote user account which will be required to be entered on the client side and authenticated on the server side, please refer to the [Remote Users](#) section.

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.

+ Add

Name	Status	Connection Type	Interface	Server Address	Operations
L2TP	Dialing	L2TP	WAN	testvpn12tp.vpnazure.net	✖ ✎ 🗑

L2TP Client

WireGuard®

WireGuard® is free and open source VPN solution that encrypts virtual private networks, easy to use, high performance and secure. GWN700x routers series support WireGuard® VPN with automatic peer generation and QR code scanning for mobile phones and devices with camera support.

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:

WireGuard®
WireGuard® Peers

Add
Delete

<input type="checkbox"/>	Name	Status	Ports	WireGuard® Address	Uptime	Upload	Download	Current Rate	Operations
<input type="checkbox"/>	wireGuard	🔴	WAN2 (WAN)	192.168.5.143	21 min	↑ 1.36MB	↓ 608.27KB	TX:472bps RX:0bps	✎ 🗑

WireGuard® tab

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

WireGuard® > Edit WireGuard®

* Name 1-64 characters

Status

* Interface

* Monitoring Port Default 51820, range 1024-65535

* Local IP Address

* Subnet Mask only support input range 255.255.255.0-255.255.255.255 is supported

* Destination

* Private Key 44 bits
[One-click generation](#)

Public Key
[Copy](#)

* Maximum Transmission Unit (MTU) Default 1420, range 576-1440

Cancel
Save

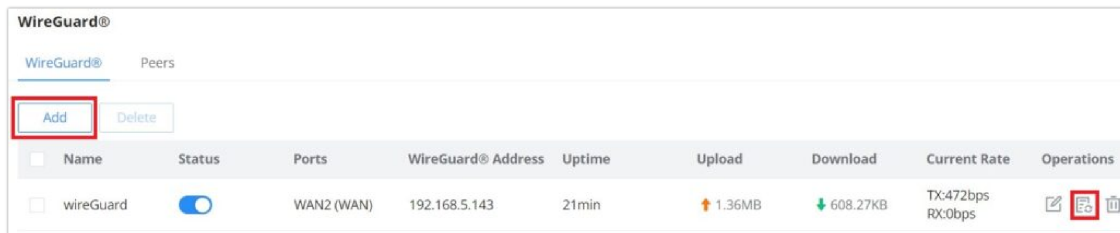
Add/Edit WireGuard®

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. <i>Default: 51820</i>
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. <i>Note: When selecting "All", subsequent new interfaces will be automatically included.</i>
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 "**Automatic peer generation**" icon to generate peers very quickly and easily as shown in the figures below:

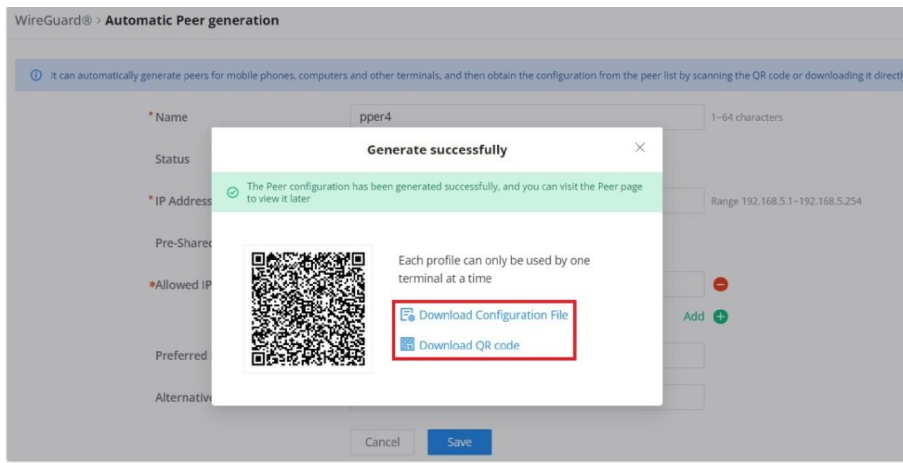


WireGuard® tab

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

WireGuard® Automatic Peer generation – 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® Automatic Peer generation – part 2

Peers

On the peers tab, the user can create peers manually by clicking on “Add” button.

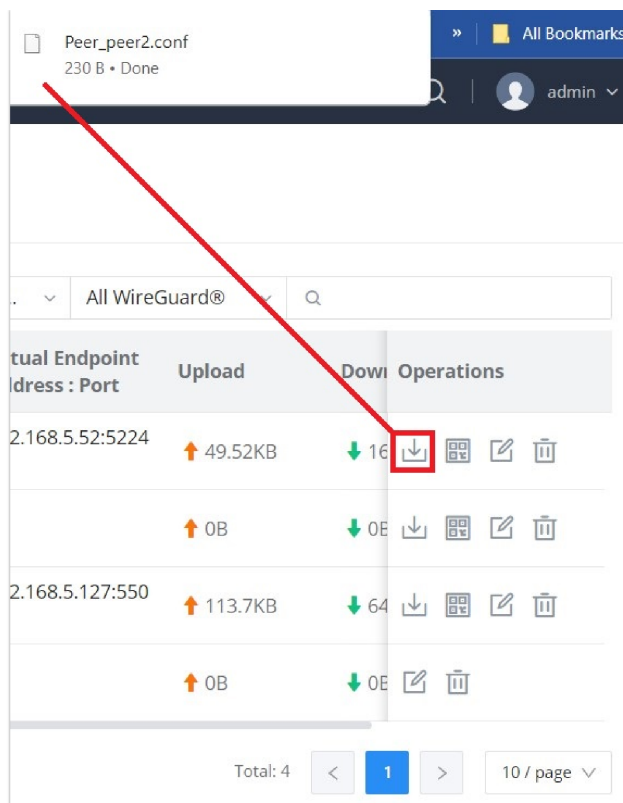
Name	Status	Generation Mode	WireGuard	Endpoint Address : Port	Last Handshake	Actual Endpoint Address : Port	Upload	Down	Operations
[Grey]	<input checked="" type="checkbox"/>	Auto Generated	wireGuard	-	6min ago	192.168.5.52:5224 7	↑ 40.7KB	↓ 16	[Icons]
[Grey]	<input checked="" type="checkbox"/>	Auto Generated	wireGuard	-	-	-	↑ 0B	↓ 0E	[Icons]
peer2	<input checked="" type="checkbox"/>	Auto Generated	wireGuard	-	6min ago	192.168.5.127:550 18	↑ 103.15KB	↓ 64	[Icons]
Peer1	<input checked="" type="checkbox"/>	Add Manually	wireGuard	192.168.5.143:518 20	-	-	↑ 0B	↓ 0E	[Icons]

WireGuard® – Peers tab

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

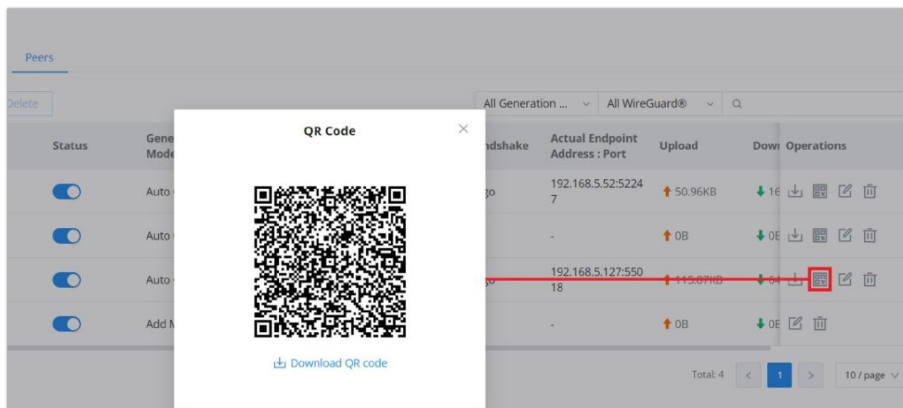
WireGuard® – add/edit peer

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



WireGuard® – download peer config

Or scanning the QR code for devices with camera support.



WireGuard® – scan peer config

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.

Remote Users > Add User

*Name 1~64 characters

Status

Server Type PPTP IPsec OpenVPN®

Server Name Please Select Server Name

*Username 1~64 characters, only support input English, numbers, characters @ ! \$ % _

*Password 1~64 characters, only support input English, numbers, characters @ ! \$ % _

Client Subnet IP Address / Mask Length

Add +

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. <ul style="list-style-type: none"> • 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.

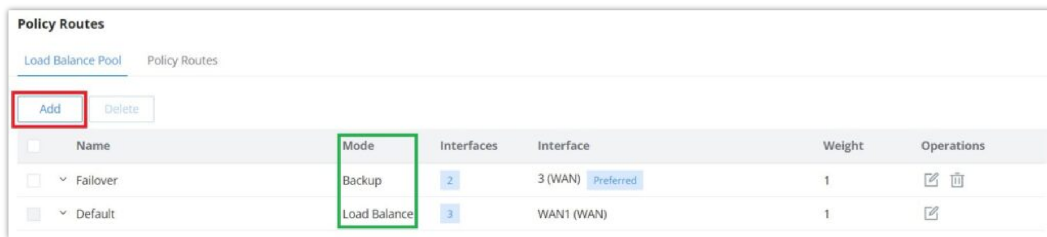
ROUTING

Policy Routes

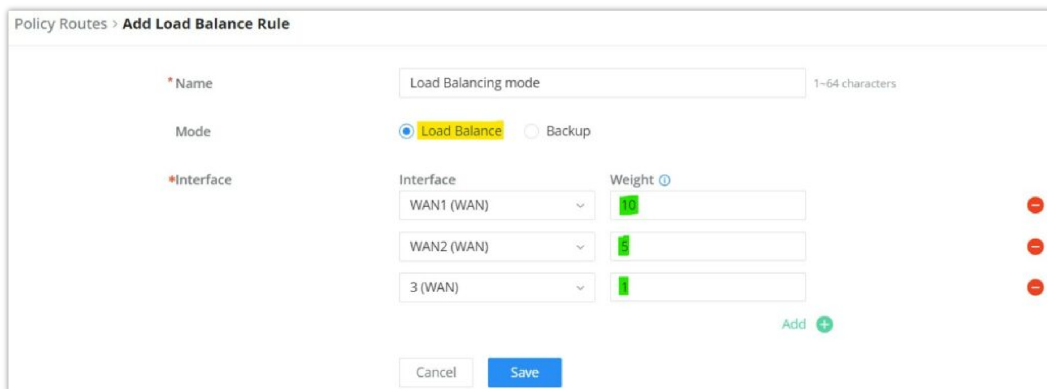
On this section, the user can create a policy route to either load balance or backup (Failover) between 2 or more WAN ports. This feature allows a network administrator to make advanced routing decisions for traffic passing through the router and for high granularity control over policies that dictate what WAN port and even VLAN, traffic should use. Traffic controlled this way can be balanced across multiple VLANs.

Load Balance Pool

To create a load balance rule, navigate to **Routing** → **Policy Routes page** → **Load Balance Pool tab**, click on **"Add"** button, then select the mode (Load Balance or Backup), after that select the WAN ports from the drop-down list and specify the Weight for each port added. Please refer to the figures below:



Load Balance Pool



Load Balance Pool – Load Balance mode

Policy Routes > **Edit Load Balance Rule**

*Name: Backup mode (1-64 characters)

Mode: Load Balance Backup

*Preferred Interface:

Interface	Weight
WAN1 (WAN)	10
WAN2 (WAN)	5

Add +

*Alternate Interface:

Interface	Weight
3 (WAN)	10
WAN 4 (WAN)	1

Add +

Cancel Save

Load Balance Pool – Backup mode

Note:

- For the Weight: The default is 1 and value can be from 1~10 with 10 being the highest weight.
- The number of WAN ports depends on GWN router model.

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 as shown below:

Policy Routes

Load Balance Pool: Policy Routes

Add Delete

Name	Status	IP Family	Protocol Type	Source Group	Source IP Address	Source Port	Destination IP Address	Destination Port	Load	Operations
Policy route	<input checked="" type="checkbox"/>	IPv4	All	Default (VLAN)	-	-	-	-	Back	

Policy Routes page

Policy Routes > **Edit Policy Route**

*Name: Policy route

Status:

IP Family: Any IPv4

Protocol Type: All

Source Group: Default (VLAN)

Source IP Address:

Destination IP Address:

*Load Balance: Backup mode

Schedule: Backup Schedule

Cancel Save

Add Policy Route


Note:

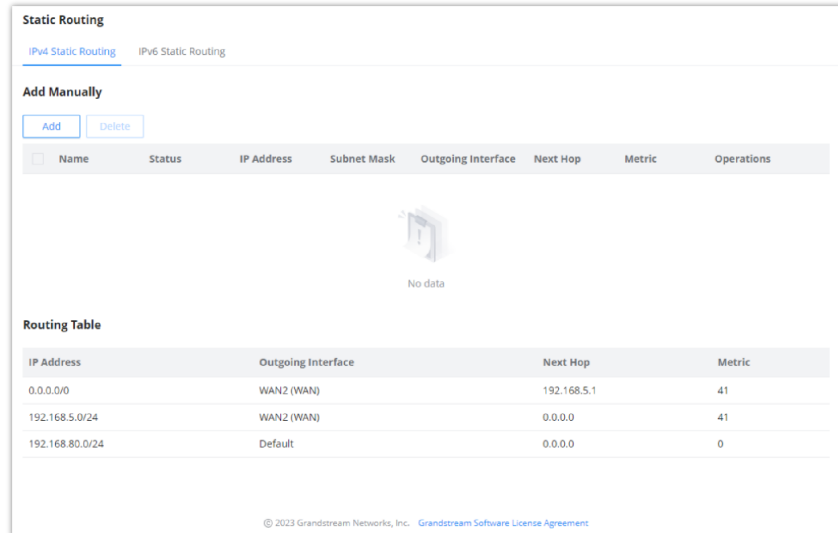
If the Source and Destination IP address field left empty, the policy route will take any IP address.

Static Routes

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

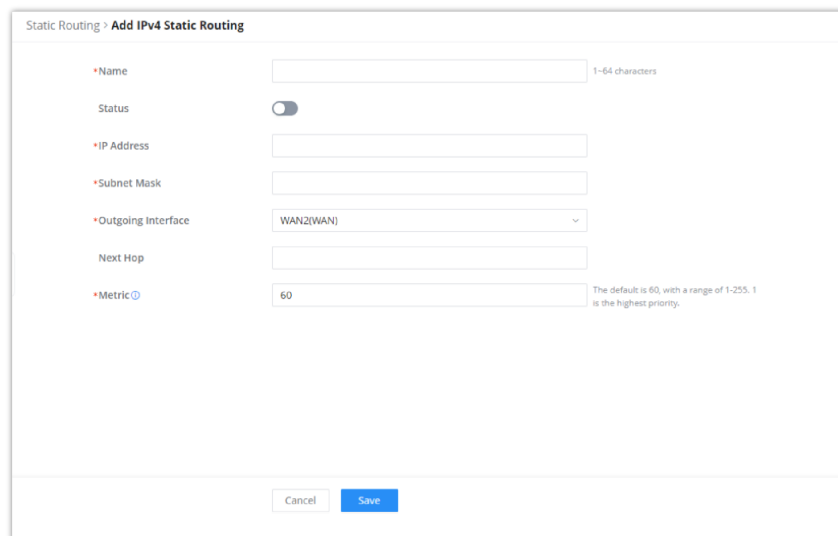
GWN700x supports setting manually **IPv4 or IPv6 Static Routes** which can be accessed from GWN700x WebGUI **Routing** → **Static Routing**.

To add a new Static Route, the user needs to click on 



IP Address	Outgoing Interface	Next Hop	Metric
0.0.0.0/0	WAN2 (WAN)	192.168.5.1	41
192.168.5.0/24	WAN2 (WAN)	0.0.0.0	41
192.168.80.0/24	Default	0.0.0.0	0

Static Routing Page



Add IPv4 Static Routing

Name	Specify a name for the Static Routing
Status	enable or disable the Static Routing
IP Address	Specify the IP address
Subnet Mask	Enter the Subnet Mask
Outgoing Interface	Select the interface
Next Hop	Specify the next Hop
Metric	When there are multiple routings in the network that can reach the same destination, the priority of routing rules can be adjusted by setting metric, and the packets will be forwarded according to the

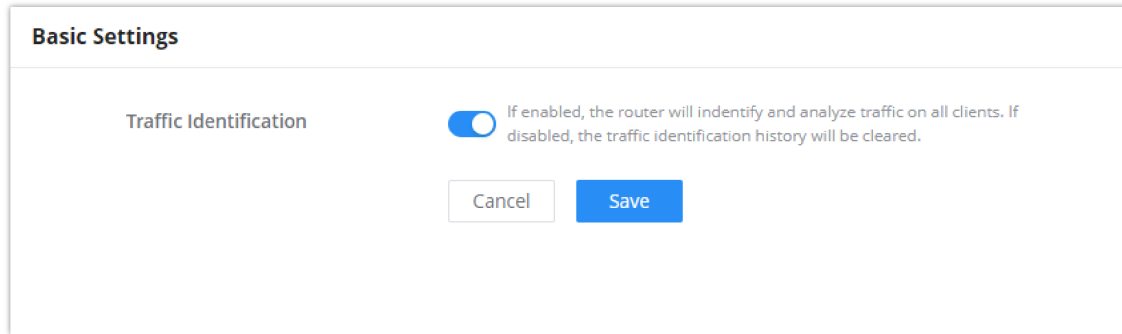
path with the smallest metric.

Add IPv4 Static Routing

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”.



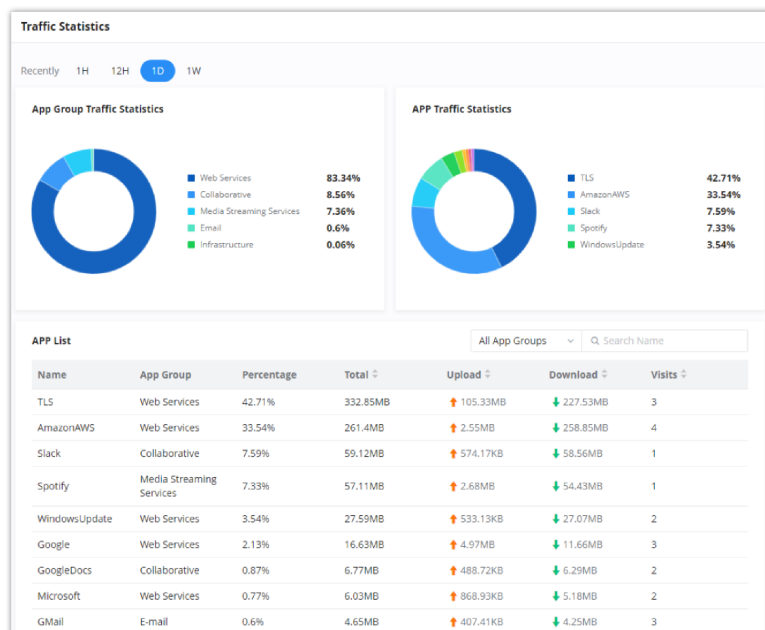
Enable Traffic Identification

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 of 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

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.

The screenshot shows the 'QoS' configuration page with tabs for 'General Settings', 'APP Class', 'Class Rules', and 'VoIP Settings'. Under 'Bandwidth Limit', the 'WAN2' section has an 'Edit' button highlighted in a red box. Below it, 'Upload Bandwidth' and 'Download Bandwidth' are both enabled. Maximum upload/download bandwidths are 100Mbps and 200Mbps respectively. Class allocations are: Class1(High): 40%, Class2(Medium): 30%, Class3(Low): 20%, and Class4(Lowest): 10%. The 'Tag Outbound Traffic' section has dropdown menus for DSCP tags: Class1(High) is AF41(Low), Class2(Medium) is AF42(Medium), Class3(Low) is AF13(High), and Class4(Lowest) is AF43(High). 'Cancel' and 'Save' buttons are at the bottom.

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%.


The 'Edit Bandwidth Limit' dialog box shows a warning: 'If the bandwidth is incorrect, QoS cannot work properly. Before enabling QoS, please check the rate or contact your ISP to obtain the exact bandwidth. The total proportion of bandwidth cannot exceed 100%.' Under 'Upload Bandwidth', status is on, max is 100 Mbps, and class percentages are 40%, 30%, 20%, and 10%. Under 'Download Bandwidth', status is on, max is 200 Mbps, and Class1(High) is 40%. 'Cancel' and 'Save' buttons are at the bottom.

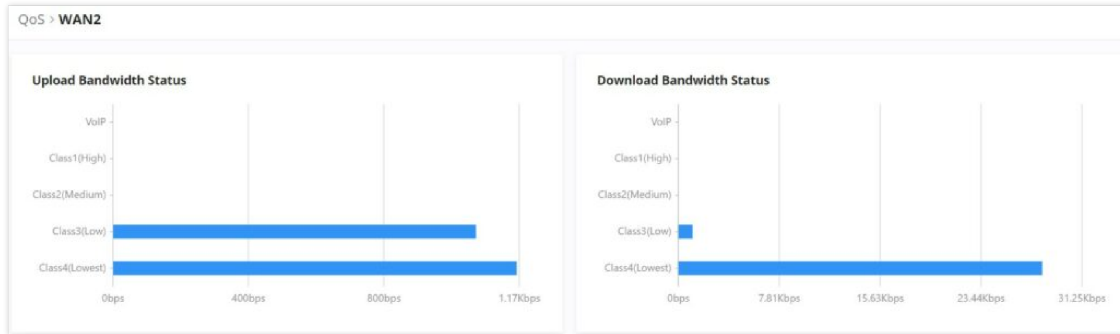
WAN Port QoS Settings

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

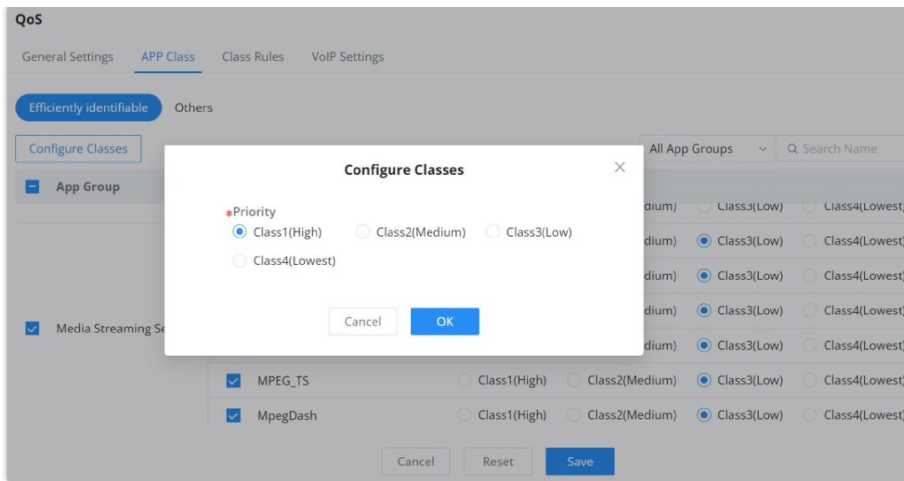
GWN700X routers can prioritize the traffic of each application individually. The priority level can be set in 4 classes, class 1 having the highest priority and class 4 having the lowest priority. To access APP Class settings, please access the web GUI of the router then navigate to **Traffic Management**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

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

The screenshot shows the 'APP Class' configuration page. It features a table with columns for 'App Group', 'Name', and 'Priority'. The 'Priority' column has radio buttons for Class1(High), Class2(Medium), Class3(Low), and Class4(Lowest). The 'Media Streaming Services' group is expanded, showing applications like RTSP, RTP, SD-RTN, RTMP, MPEG_TS, and MpegDash, all assigned to Class3(Low). Other groups like 'AllCloud', 'IRC', and 'WhatsApp' are assigned to Class1(High). There are 'Cancel', 'Reset', and 'Save' buttons at the bottom.

QoS – APP Class

Or, the user can select the applications and application categories and then click **“Configure Classes”** then choose the adequate priority.



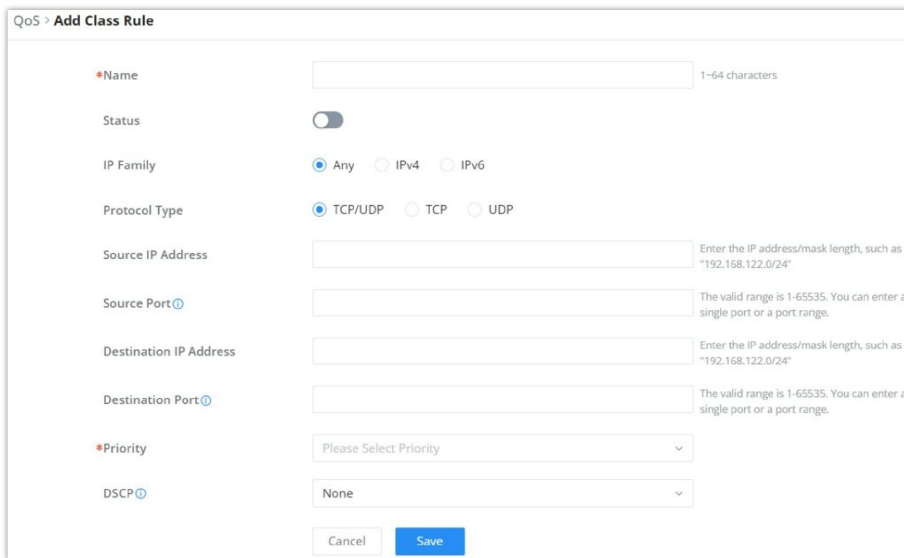
QoS – Apps Class – Configure Classes

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<p>Enter a single port number, multiple port numbers, or a range of ports number.</p> <p>Example:</p> <ul style="list-style-type: none"> - 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" <p>Note: The valid range of port numbers that can be entered is 1-65535.</p>
Destination IP Address	Enter the destination IP address/mask length. E.g., "192.168.122.0/24"
Destination Port	<p>Enter a single port number, multiple port numbers, or a range of ports number.</p> <p>Example:</p> <ul style="list-style-type: none"> - 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" <p>Note: The valid range of port numbers that can be entered is 1-65535.</p>
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.



The screenshot shows the 'QoS' configuration page with the 'VoIP Settings' tab selected. Under 'VoIP Prioritization', there is a toggle switch that is turned on, with a note: 'When enabled, it will give priority to distributing traffic for VoIP SIP/RTP services and will not be restricted by other class bandwidth allocation'. Below this, the 'SIP UDP Port' is set to '5060' in a text input field, with 'Default 5060' written to the right. At the bottom, there are 'Cancel' and 'Save' buttons.

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**.

The screenshot shows the 'Bandwidth Limit' configuration page. At the top, there are 'Add' and 'Delete' buttons, with 'Add' highlighted by a red box. Below is a table with the following columns: Name, Status, Range Constraint, IP Address, MAC Address, Maximum Upload Bandwidth, Maximum Download Bandwidth, and Operations. The table contains one row for 'Guests' with a status toggle on, a range constraint of 'IP Address', an IP address of '192.168.10.0/24', a MAC address of '-', a maximum upload bandwidth of '10Mbps', and a maximum download bandwidth of '20Mbps'. The 'Operations' column for the 'Guests' row has a red box around the edit icon.

Name	Status	Range Constraint	IP Address	MAC Address	Maximum Upload Bandwidth	Maximum Download Bandwidth	Operations
Guests	<input checked="" type="checkbox"/>	IP Address	192.168.10.0/24	-	10Mbps	20Mbps	 

Total: 1 < 1 > 20 / 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:

The screenshot shows the 'Add Bandwidth Limit' configuration window. It contains the following fields and options:

- Name:** Guests (1-64 characters)
- Status:** On (toggle)
- Range Constraint:** IP Address (dropdown)
- Application Mode:** Individual (selected), Shared
- IP Address/Mask Length:** 192.168.10.0 / 24 (with an 'Add' button)
- Maximum Upload Bandwidth:** 10 Mbps (with a note: 'The range is 1-1024, if it is empty, there is no limit')
- Maximum Download Bandwidth:** 20 Mbps (with a note: 'The range is 1-1024, if it is empty, there is no limit')
- Bandwidth Schedule:** On (toggle)
- Schedule:** Office hours (dropdown)
- Buttons:** Cancel, Save

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**.

The screenshot shows the 'Access Points' management page. At the top, there are buttons for 'Pair AP', 'Takeover AP', 'Configure', 'Upgrade', 'Delete', 'Reboot', and 'Transfer'. Below these is a search bar and a table of access points. The table has the following data:

Device Type	MAC Address	Device Name	IP Address	Firmware Version	SSIDs	System Up Time	Operations
GWN7624	C0:74:AD:90:B2:40	GWN7624	IPv4:192.168.70.171 IPv6:-	1.0.25.10	5	13min	[Edit] [Send] [Refresh] [Delete]

At the bottom right, it shows 'Total: 1' and a pagination control for '10 / page'.

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.

Access Points > C0:74:AD:90:B2:40 (GWN7624)

Details

Client List

Debug

Firmware Version: 1.0.25.10

SSID: Hall (5G: c0:74:ad:90:b2:42)

IPv4 Address: 192.168.70.171

IPv6: -

System Up Time: 1h 10min

System Time: 2023-10-04 11:40

Load Average: 1min: 2.59 5min: 2.57 15min: 2.61

Temperature: 41°C

Link Speed: NET/POE:1000M FD
NET:Disconnected
PORT3:Disconnected
PORT4:Disconnected

2.4G Radio Status: Channel: 0

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.

Access Points > C0:74:AD:90:B2:40 (GWN7624)

Details

Client List

Debug

MAC Address	Device Name	IP Address	Duration	Total	Upload	Download	Upload sp...	Download
E...D	Ain	IPv4:192.168.70.235 IPv6:-	28s	4.16KB	2.3KB	1.86KB	18.39Kbps	14.85K

Total: 1 < 1 > 10 / page

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.

Access Points > C0:74:AD:90:B2:40 (GWN7624)

Details

Client List

Debug

Ping / Traceroute

Core File

One-click Debug

SSH Remote Access

*Tool: IPv4 Ping

*Target IP Address / Hostname: 8.8.8.8

Start

Diagnostic Result

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=113 time=21.727 ms
64 bytes from 8.8.8.8: seq=1 ttl=113 time=19.886 ms
64 bytes from 8.8.8.8: seq=2 ttl=113 time=19.078 ms
64 bytes from 8.8.8.8: seq=3 ttl=113 time=19.874 ms
64 bytes from 8.8.8.8: seq=4 ttl=113 time=19.977 ms

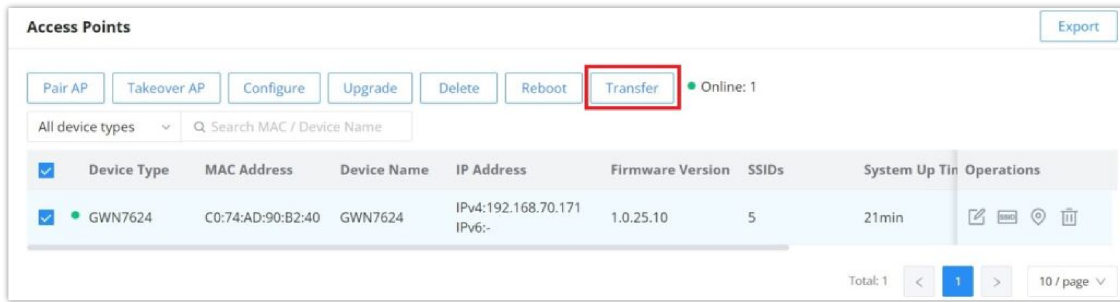
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 19.078/20.108/21.727 ms
```

Paired APs – Debug

Transfer APs to GWN.Cloud/GWN Manager

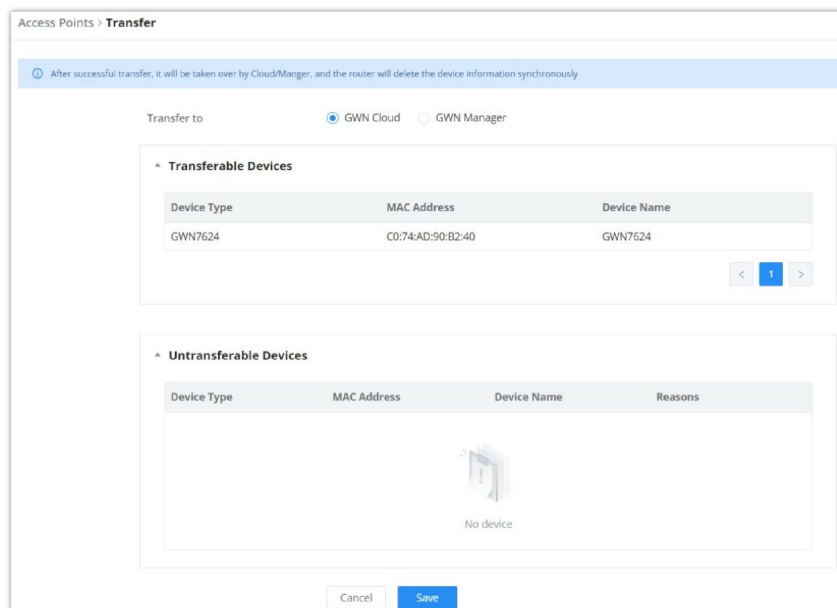
GWN routers also enables to users to transfer their paired GWN APs to GWN.Cloud/GWN Manager.

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 GWN Cloud or GWN Manager then click **“Save”** button. the user will be forwarded automatically to either GWN Cloud or GWN Manager to login.



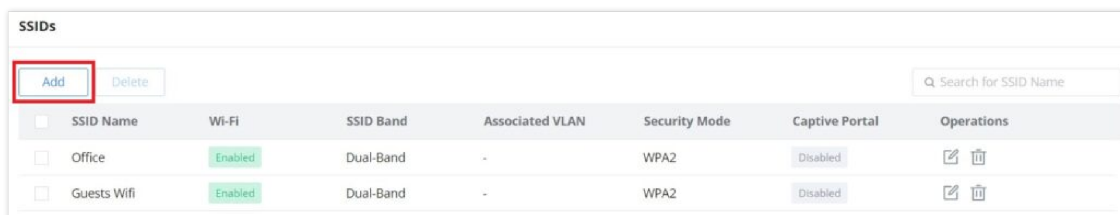
Transfer AP to GWN.Cloud or GWN Manager

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:

SSIDs > Edit SSID

Basic Information ^

Wi-Fi

* Name 1-32 characters

Associated VLAN

SSID Band Dual-Band 2.4G 5G

Access Security v

Advanced v

Device Management ^

All Devices

Device Name	Device Type	MAC Address	SSIDs
<input checked="" type="checkbox"/> GWN7624	GWN7624	C0:74:AD:90:B2:40	2.4G: 2/8 5G: 2/8

Selected: 1

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. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● Open ● WPA/WPA2 ● WPA2 ● WPA2/WPA3 ● WPA3 ● WPA3-192
WPA Key Mode	Choose the WPA key mode: <ul style="list-style-type: none"> ● PSK ● 802.1x ● PPSK without RADIUS ● PPSK with RADIUS
WPA Encryption Type	Choose the encryption type: <ul style="list-style-type: none"> ● 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	<p>Toggle Captive Portal on/off.</p> <ul style="list-style-type: none"> ● Captive Portal Policy: Choose the created captive portal policy.
Blocklist Filtering	Choose a blocklist for the Wi-Fi SSID.
Client Isolation	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.	

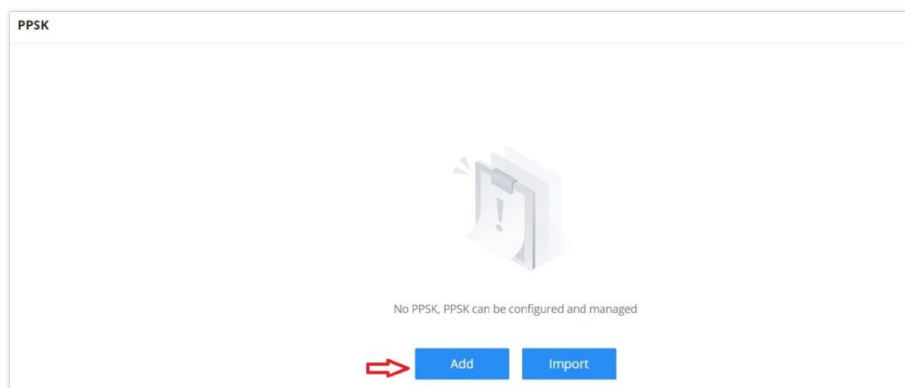
Add SSID

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

The screenshot shows the "Add PPSK" configuration form. The fields are as follows:

- * SSID Name:** Guests Wifi
- * Account:** RADIUSuser1 (Note: 1-64 bits, do not support the input of English comma)
- * Wi-Fi Password:** (Note: 8-63 ASCII characters or 8-64 hex characters)
- * Maximum Number of Access Clients:** 1 (Note: Default 1, range 1-100)
- MAC Address:** 1C : 74 : AD : 11 : 22 : 33
- Maximum Upload Bandwidth:** 10 Mbps (Note: Range 1-1024)
- Maximum Download Bandwidth:** 20 Mbps (Note: Range 1-1024)
- Description:** Wi-Fi for Guests (Note: 0-128 characters)

At the bottom, there are "Cancel" and "Save" buttons.

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	Configures 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 download 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

Airtime Fairness

*Beacon Interval Default: 100, range 40-500

Country / Region

2.4G

Channel Width 20MHz 20&40MHz 40MHz

Channel Auto Dynamically assigned by RRM

Radio Power

Short Guard Interval

Allow Legacy Devices (802.11b)

Minimum RSSI

Minimum Rate

Wi-Fi 5 Compatible Mode

Radio

General

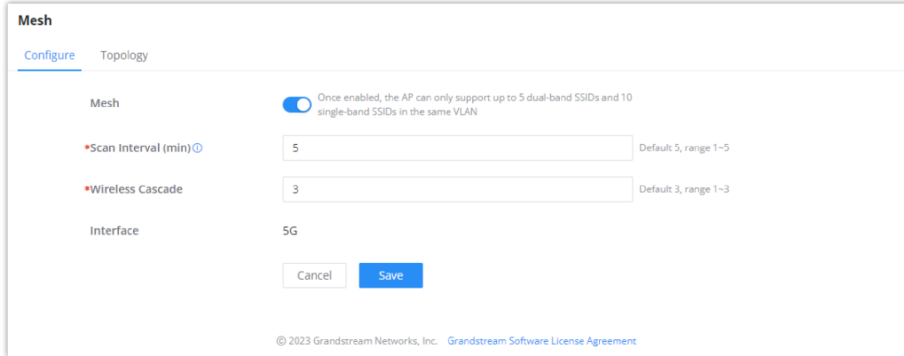
Band Steering	Band steering functions are divided into four items: 1) 2.4G in priority, lead the dual client to the 2.4G band; 2) 5G in priority, the dual client will be led to the 5G band with more abundant spectrum resources as far as possible; 3) Balance,access to the balance between these 2 bands 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. <ul style="list-style-type: none"> ● 2.4G: 20Mhz, 20&40Mhz, 40Mhz ● 5G: 20Mhz, 40Mhz, 80Mhz
Channel	Pick how the access points will be able to choose a specific channel. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● 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.

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.

- o **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

- o **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.

Route / AP	RSSI	Channel	IP Address	Clients	Operations
^ C0:74:AD:62:C0:D4	-	5G:36	192.168.80.108	1	
C0:74:AD:50:FA:10	-60	5G:36	192.168.80.25	1	

Mesh Topology

ACCESS CONTROL

GWN700x has features that can enable the user to block clients and sites as well and also limit the bandwidth per client or SSID.

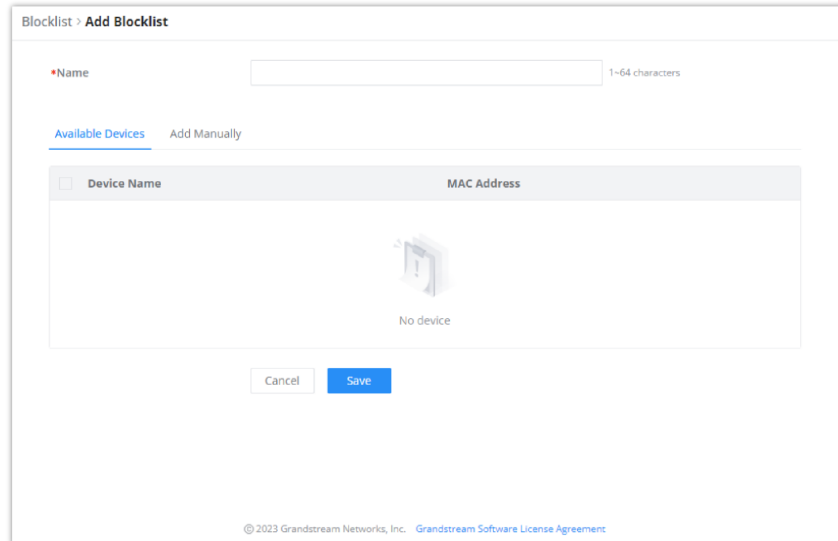
Blocklist

The Blocklist is a feature in GWN700x that enables the user to block wireless clients from the available ones or manually add the MAC Address.

To create a new Blocklist, Navigate under: "**Web UI** → **Access Control** → **Blocklist**".

- **Add devices from the list:**

Enter the name of the blocklist, then add the devices from the list.

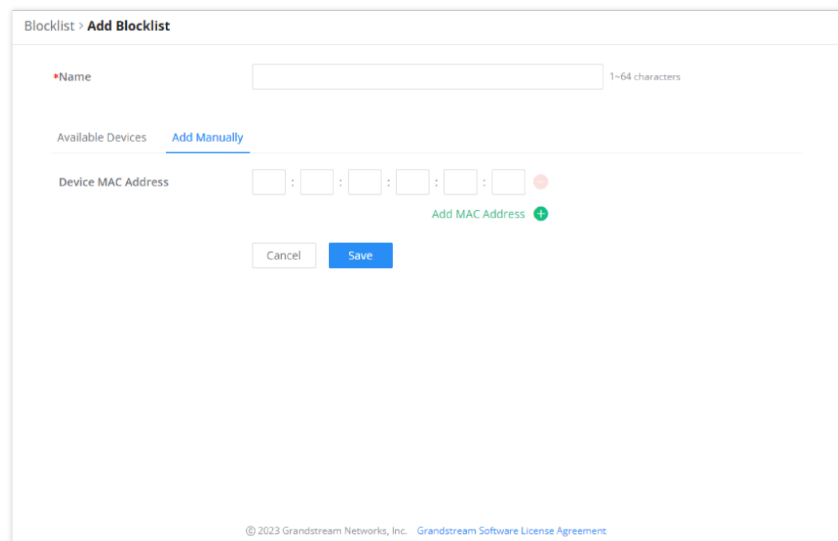


The screenshot shows the 'Blocklist > Add Blocklist' page. At the top, there is a text input field for 'Name' with a character count of '1-64 characters'. Below this, there are two tabs: 'Available Devices' (which is selected and underlined) and 'Add Manually'. The main content area is a table with two columns: 'Device Name' and 'MAC Address'. The table is currently empty, displaying a 'No device' message with a small icon of a device. At the bottom of the page, there are 'Cancel' and 'Save' buttons. A footer contains the copyright information: '© 2023 Grandstream Networks, Inc. Grandstream Software License Agreement'.

Blocklist Page

- **Add Devices Manually:**

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



The screenshot shows the 'Blocklist > Add Blocklist' page with the 'Add Manually' tab selected. The 'Name' input field is at the top. Below the tabs, there is a 'Device MAC Address' input field consisting of six boxes separated by colons, followed by a red minus sign and a green plus sign with the text 'Add MAC Address'. At the bottom, there are 'Cancel' and 'Save' buttons. The footer contains the copyright information: '© 2023 Grandstream Networks, Inc. Grandstream Software License Agreement'.

Add Blocklist

After the blocklist is created, to take effect the user needs to apply it on the desired 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 blocklists, the user can select one or more, or click on "**Create Blocklist**" at the bottom of the list to create new one.

Please refer to the figure below:

Access Security ^

Security Mode: WPA2

WPA Key Mode: PSK 802.1x

WPA Encryption Type: AES AES/TKIP

*WPA Shared Key: 8-63 ASCII characters or 8-64 hex characters

Enable Captive Portal:

Blocklist Filtering: Blocklist1 x |

Client Isolation: Blocklist1 [+ Add Blocklist](#)

802.11w: Disable Optional Required

SSID Configuration

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.

SafeSearch

SafeSearch Bing Google YouTube

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

1. Access to GWN700x web GUI, navigate to **External Access** → **DDNS**, and click to Add Service.
2. Fill in the domain name created with the DDNS provider under the Service Provider field.
3. Enter your account username and password under the User Name and Password fields.
4. Specify the Domain to which DDNS Account is applied under Domain.

DDNS > **Add DDNS**

Service Provider: dyndns.org

Status:

*Username: 1~32 characters

*Password: 1~32 characters

*Domain: Please go to dyndns.org to register to get the corresponding username, password and domain

Interface: WAN4 (WAN)

Service Provider	Select the DDNS provider from the list
Username	Enter the Username
Password	Enter the Password
Domain	Enter the Domain
Interface	Select the Interface

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.

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	<p>When this option is enabled, the router will take counter measures to SYN Flood Attack.</p> <ul style="list-style-type: none"> • 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	<p>When this option is enabled, the router will take counter measures to the UDP Flood Attack.</p> <ul style="list-style-type: none"> • 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	<p>When this option is enabled, the router will take counter measures to the ICMP Flood Attack.</p> <ul style="list-style-type: none"> • 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	<p>When this option is enabled the router will take counter measures to ACK Flood Attack.</p> <ul style="list-style-type: none"> • 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	<p>When this option is enabled, the router will take counter measure to the port scanning attempts</p> <ul style="list-style-type: none"> • 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.

Log

ARP Spoofing Defense

Block ARP Replies With Inconsistent Source MAC Addresses

Block ARP Replies With Inconsistent Destination MAC Addresses

Decline VRRP MAC Into ARP Table

IP Spoofing Defense

Block IP Packet From WAN With Inconsistent Source IP Addresses

Block IP Packet from LAN With Inconsistent Source IP Addresses

Cancel Save

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.

Basic Settings > WAN2

Inbound Policy Accept Reject Drop

Outbound Policy Accept Reject Drop

IP Masquerading

MSS Clamping

Log Drop / Reject Traffic

Drop / Reject Traffic Log Limit The range is 1-99999999, if it is empty, there is no limit.

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 masquerade 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**.

Content Security > Add DNS Filtering

*Name 1-64 characters

Description 0-128 characters

*Filtered DNS ⓘ +

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.

Content Security > **Add URL Filtering**

*Name 1-64 characters

Description 0-128 characters

*Filtered URL Please Enter -

Add +

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 .
- To edit a rule, click on .
- To delete a rule, click on .

Inbound Rules

The GWN700x allows to filter incoming traffic to networks group or port WAN 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											
Inbound Rules			Outbound Rules			Forwarding Rules					
Name	Status	IP Family	Protocol Type	Source Group	Source MAC Address	Source IP Address	Source Port	Destination IP Address	Destination Port	Action	Operations
<input type="checkbox"/> Anti-lockout-R...	<input checked="" type="checkbox"/>	Any	TCP	Default (VLAN)	-	-	-	-	22,80,443	Accept	
<input type="checkbox"/> WAN2_Alow-...	<input checked="" type="checkbox"/>	IPv4	UDP	WAN2 (WAN)	-	-	-	-	68	Accept	
<input type="checkbox"/> WAN2_Alow-...	<input checked="" type="checkbox"/>	IPv4	ICMP	WAN2 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/> WAN2_Alow-L...	<input checked="" type="checkbox"/>	IPv4	IGMP	WAN2 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/> WAN2_Alow-...	<input checked="" type="checkbox"/>	IPv6	UDP	WAN2 (WAN)	-	fe80::/10	-	fe80::/10	546	Accept	
<input type="checkbox"/> WAN2_Alow-...	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN2 (WAN)	-	fe80::/10	-	-	-	Accept	
<input type="checkbox"/> WAN2_Alow-L...	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN2 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/> Allow-DHCP-R...	<input checked="" type="checkbox"/>	IPv4	UDP	WAN4 (WAN)	-	-	-	-	68	Accept	
<input type="checkbox"/> Allow-Ping	<input checked="" type="checkbox"/>	IPv4	ICMP	WAN4 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/> Allow-IGMP	<input checked="" type="checkbox"/>	IPv4	IGMP	WAN4 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/> Allow-DHCPv6	<input checked="" type="checkbox"/>	IPv6	UDP	WAN4 (WAN)	-	fe80::/10	-	fe80::/10	546	Accept	
<input type="checkbox"/> Allow-MLD	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN4 (WAN)	-	fe80::/10	-	-	-	Accept	
<input type="checkbox"/> Allow-ICMPv6...	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN4 (WAN)	-	-	-	-	-	Accept	

Name	Enter the name of the inbound rule.
Status	Toggle on/off the status of the inbound rule.
IP Family	Pick the IP family. <ul style="list-style-type: none"> • Any • IPv4 • IPv6
Protocol Type	Choose the protocol type. <ul style="list-style-type: none"> • UDP • TCP • UDP/TCP • ICMP • IGMP • All
Source Group	If set to "All", rules will be matched in preference to other specific ones.
Source MAC Address	Specify the source MAC address.
Source IP Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Destination IP Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
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 dropped.

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 > **Add Outbound Rule**

***Name** 1-64 characters

Status

IP Family Any IPv4 IPv6

Protocol Type

Source IP Address Enter the IP address/mask length, such as "192.168.122.0/24"

Source Port The valid range is 1-65535. You can enter a single port or a port range.

***Destination Group**

Destination IP Address Enter the IP address/mask length, such as "192.168.122.0/24"

Destination Port The valid range is 1-65535. You can enter a single port or a port range.

Action Accept Deny Drop

Advanced Settings (If the Rule action is 'Accept', content security acts as a blocklist and can deny or drop the requests in content security.)

Content Security

Traffic Rules – Outbound Rules

Name	Enter the name of the outbound rule.
Status	Toggle on/off the status of the outbound rule.
IP Family	<p>Pick the IP family.</p> <ul style="list-style-type: none"> ● Any ● IPv4 ● IPv6
Protocol Type	<p>Choose the protocol type.</p> <ul style="list-style-type: none"> ● UDP ● TCP ● UDP/TCP ● ICMP ● IGMP ● All
Source IP Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Destination IP Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
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 dropped.
Advanced Settings	
Content Security	Enable content security, once enabled the user can customize security features which are described below.

Content Security Action	If set to "Accept", the router is allowed to access the external network. If set to "Deny", the access to external network is denied and the result is returned. If set to "Drop", the request of access to external network will be directly dropped.
DNS Filtering	Specify the DNS filtering rule.
APP Filtering	Specify the app filtering rule.
URL Filtering	Specify the URL filtering rule.

Traffic Rules – Outbound Rules

Forwarding Rules

GWN700x offers the possibility to allow traffic between different groups and interfaces.

Traffic Rules – Forward 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 to add the Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.

*Name	<input type="text"/>	1-64 characters
Status	<input checked="" type="checkbox"/>	
IP Family	<input checked="" type="radio"/> IPv4	
Protocol Type	UDP/TCP	
*Source IP Address	<input type="text"/>	Enter the IP address/mask length, such as "192.168.122.0/24"
*Rewrite Source IP Address	<input type="text"/>	
Source Port	<input type="text"/>	The valid range is 1-65535. You can enter a single port or a port range.
Rewrite Source Port	<input type="text"/>	The valid range is 1-65535. You can enter a single port or a port range.
*Destination Group	WAN2 (WAN)	
Destination IP Address	<input type="text"/>	Enter the IP address/mask length, such as "192.168.122.0/24"
Destination Port	<input type="text"/>	The valid range is 1-65535. You can enter a single port or a port range.
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

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 to add the Port Forward rule.

Click on to  edit a Port Forward rule.

Click on to  delete a Port Forward rule.

1-64 characters
 Status
 IP Family IPv4
 Protocol Type
 *Source Group
 Source IP Address Enter the IP address/mask length, such as "192.168.122.0/24"
 Source Port The valid range is 1-65535. You can enter a single port or a port range.
 *Destination Group
 Destination IP Address Enter the IP address/mask length, such as "192.168.122.0/24"
 *Rewrite Destination IP Address
 Destination Port The valid range is 1-65535. You can enter a single port or a port range.
 Rewrite Destination Port The valid range is 1-65535. You can enter a single port or a port range.
 NAT Reflection

Advanced NAT – DNAT

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

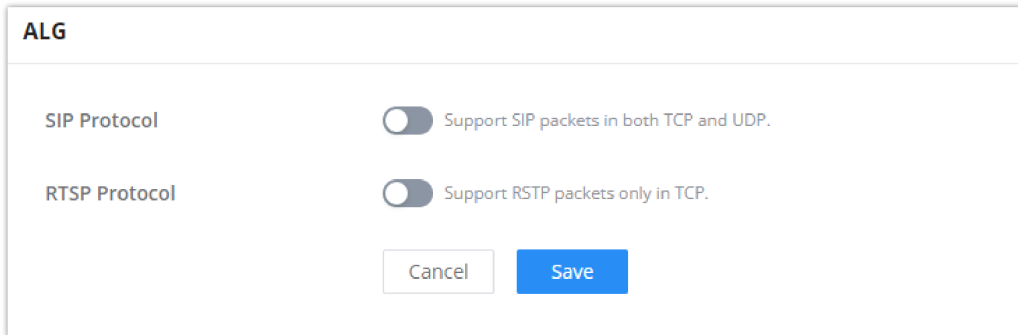
Name	Specify a name for the DNAT entry
IP Family	Select the IP version, three options are available: IPv4, IPv6 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
Source Group	Select a WAN interface or a LAN group for Source 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

SIP Protocol Support SIP packets in both TCP and UDP.

RTSP Protocol Support RSTP packets only in TCP.

Cancel Save

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**".

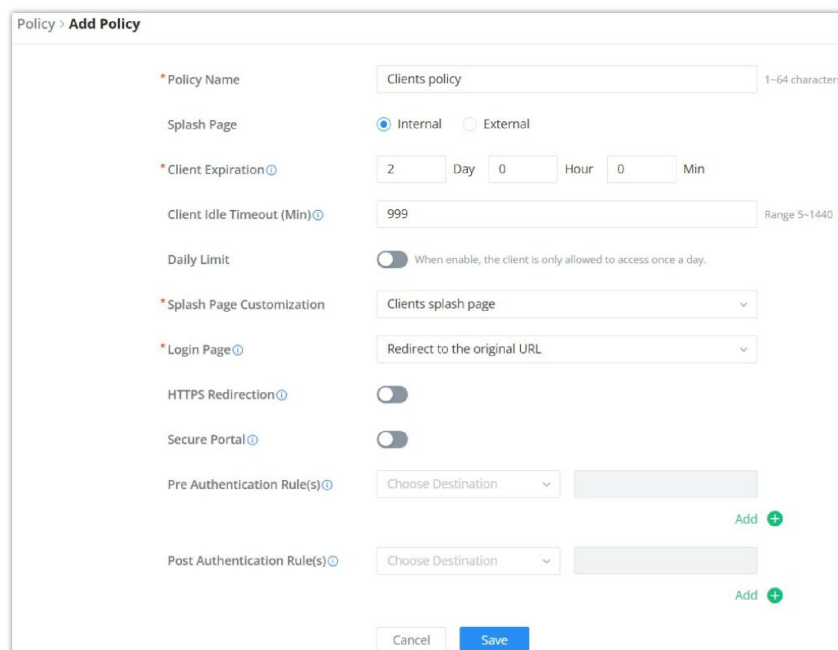
Policy

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 Name	Splash Page	Client Expiration	Operations
Clients policy	Internal(Clients splash page)	2d	 

Policy page



Policy > Add Policy

* Policy Name: Clients policy (1-64 characters)

Splash Page: Internal External

* Client Expiration: 2 Day 0 Hour 0 Min

Client Idle Timeout (Min): 999 (Range 5-1440)

Daily Limit: When enable, the client is only allowed to access once a day.

* Splash Page Customization: Clients splash page

* Login Page: Redirect to the original URL

HTTPS Redirection:

Secure Portal:

Pre Authentication Rule(s): Choose Destination Add +

Post Authentication Rule(s): Choose Destination Add +

Cancel Save

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	<ul style="list-style-type: none"> • 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

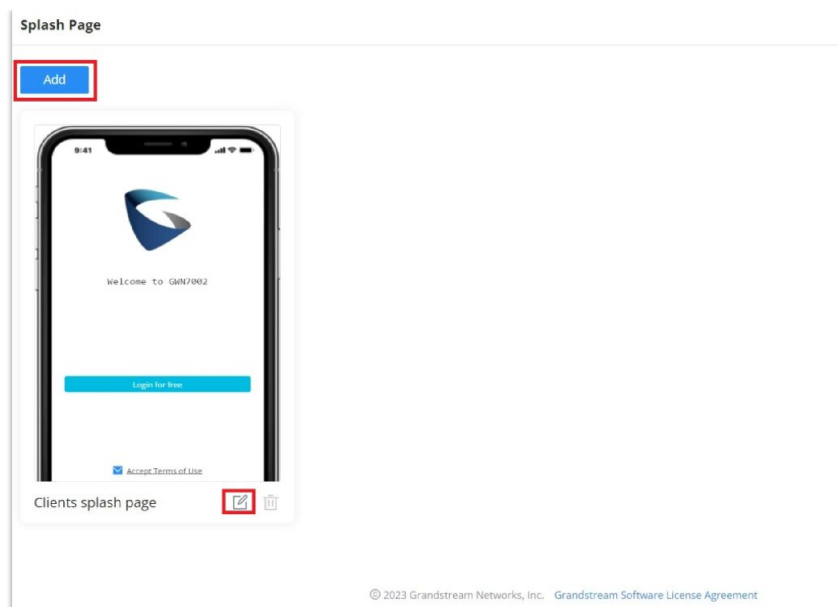
Splash Page

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.

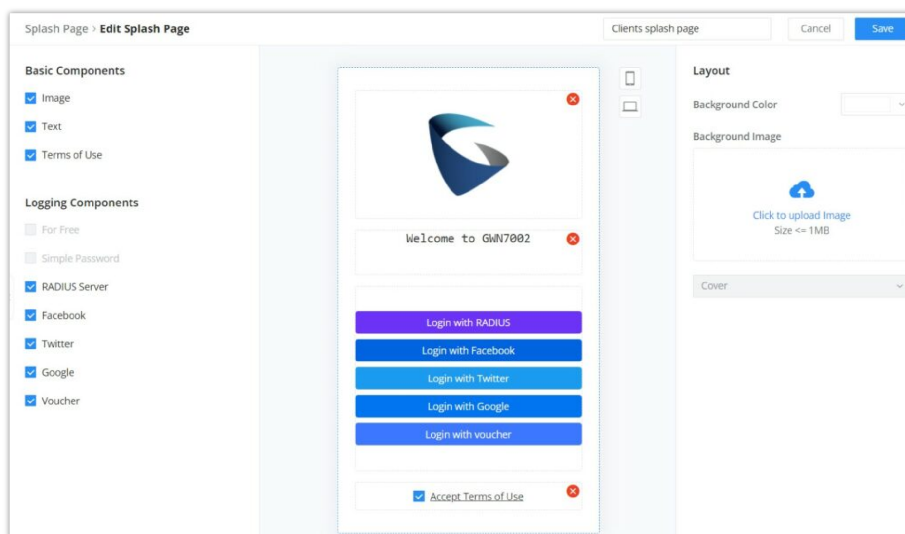
To add a splash page, click on “**Add**” button or click on “**Edit**” icon to edit previously added one.



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.

Guests

Export Guest List Search MAC / Hostname / SSID

MAC Address	HostName	Authentication Type	Login Time	Expire Time	Status	Operations
E8:F4:08:3B:62:FD	Alin	-			Unauthorized	<input type="checkbox"/> MAC Address <input checked="" type="checkbox"/> HostName <input type="checkbox"/> Associated Device
D2:3C:5D:0E:E3:EF	Unknown device	For Free	2023-10-05 15:52:31	2023-10-07 15:52:31	Authenticated	<input type="checkbox"/> SSID <input type="checkbox"/> Used Traffic <input checked="" type="checkbox"/> Authentication Type <input checked="" type="checkbox"/> Login Time <input type="checkbox"/> IP Address <input checked="" type="checkbox"/> Expire Time <input checked="" type="checkbox"/> Status

Total: 2

Guest Page

Vouchers

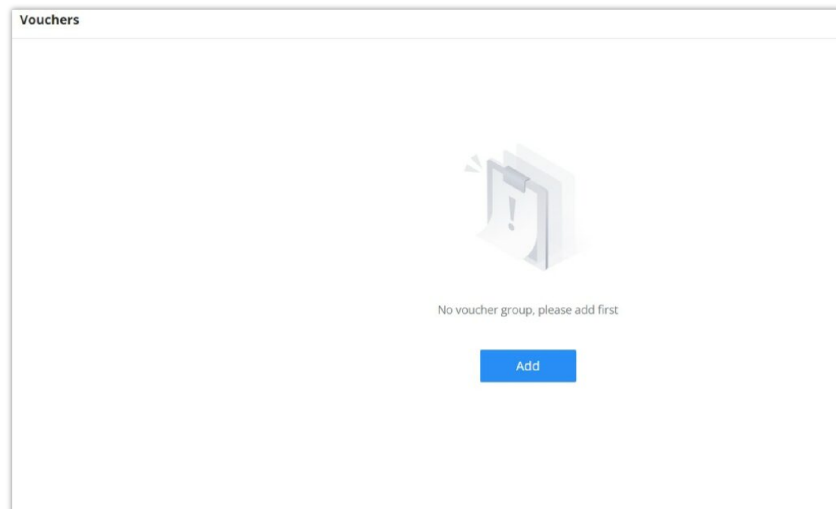
Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from platform controller.

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.

Vouchers > **Add Voucher Group**

* Voucher Group Name	<input type="text" value="Guests Voucher"/>	1-64 characters
* Quantity	<input type="text" value="10"/>	Range 1-100
* Max Devices	<input type="text" value="1"/>	Range 1-5
Byte Limit	<input type="text" value="10"/> <input type="text" value="MB"/>	Range 1-1024
Allocation Method	<input checked="" type="radio"/> Per Voucher <input type="radio"/> Per Device	
* Duration	<input type="text" value="2"/> Day <input type="text" value="0"/> Hour <input type="text" value="0"/> Min	
* Validity Time (days)	<input type="text" value="30"/>	Range 1-365
Maximum Upload Rate	<input type="text" value="10"/> <input type="text" value="Mbps"/>	The range is 1-1024, if it is empty, there is no limit
Maximum Download Rate	<input type="text" value="20"/> <input type="text" value="Mbps"/>	The range is 1-1024, if it is empty, there is no limit
Description	<input type="text" value="Guests voucher"/>	0-128 characters
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Add/Edit Voucher

Note:

Clients connected through 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

If enabled, GWN700x router cannot be managed by GWN.Cloud, and cannot continue to manage GWN76xx access points.

TR-069

ⓘ After tr-069 is enabled, the router cannot continue to manage GWN760X AP.

TR-069

•ACS URL

ACS Username

ACS Password

Periodic Inform If enabled, the router will send connection inform packets to ACS regularly.

Periodic Inform Interval (sec) Default:86400

Connection Request Username

Connection Request Password

Connection Request Port ⓘ Default: 7547, range: 1-65535

CPE Cert File ⓘ

CPE Cert Key ⓘ

© 2023 Grandstream Networks, Inc. [Grandstream Software License Agreement](#)

TR-069 page

TR-069	Enable/disable TR-069 <i>TR-069 is enabled by default.</i>
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. <i>Default is 86400.</i>
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. <i>Default is 7547.</i>
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.

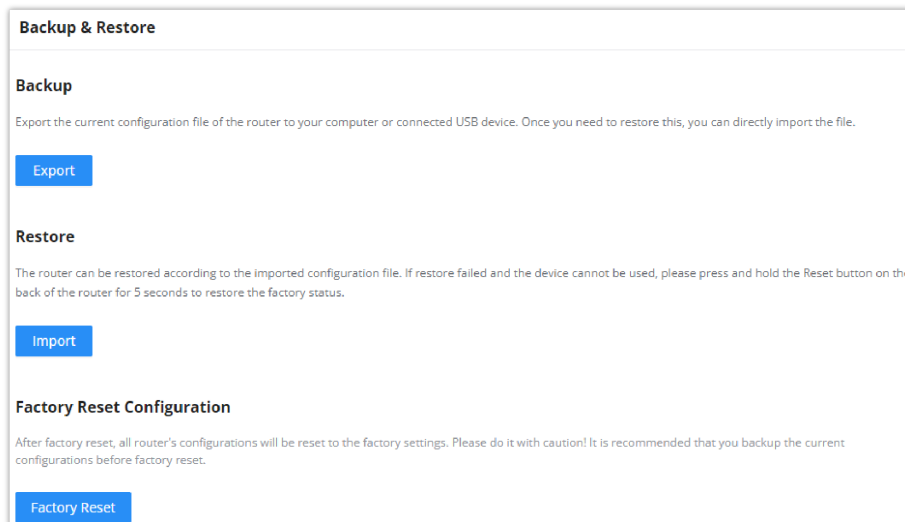
If the user wish to modify the configuration file before importing, then a **GWN Router Configuration Tool** can be used to make the necessary modifications to the configuration file. The tool is supported on Windows® and Linux environments. To download the tool: [GWN Router Configuration Tool](#), then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

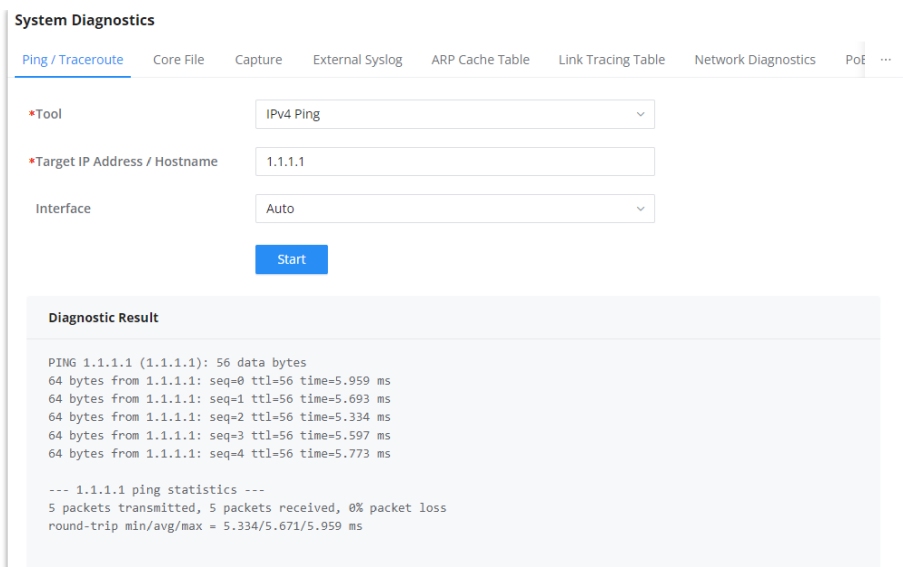
System Diagnostics

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

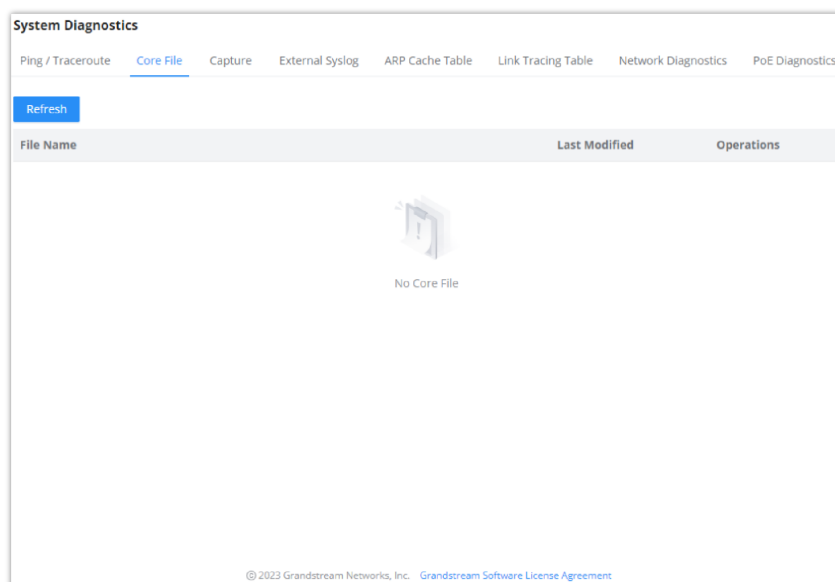
Ping and Traceroute are useful debugging tools to verify reachability with other clients across the network (WAN or LAN). The GWN700x offers both Ping and Traceroute tools for IPv4 and IPv6 protocols.



Ping/Traceroute

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**

System Diagnostics

Ping / Traceroute Core File Capture External Syslog ARP Cache Table Link Tracing Table Network Diagnostics PoE Diagnostics

Auto Refresh Timeout (sec) Default 120, range 5-300

IP Address	MAC Address	HostName	Interface
192.168.5.127	[REDACTED]	-	WAN2 (WAN)
192.168.5.154	[REDACTED]	-	WAN2 (WAN)
192.168.5.112	[REDACTED]	-	WAN2 (WAN)
192.168.5.75	[REDACTED]	-	WAN2 (WAN)
192.168.5.147	[REDACTED]	-	WAN2 (WAN)
192.168.5.1	[REDACTED]	-	WAN2 (WAN)
192.168.5.117	[REDACTED]	-	WAN2 (WAN)
192.168.80.2	[REDACTED]	Unknown device	VLAN 1

© 2023 Grandstream Networks, Inc. [Grandstream Software License Agreement](#)

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.

System Diagnostics

Ping / Traceroute Core File Capture External Syslog ARP Cache Table Link Tracing Table Network Diagnostics PoE Diagnostics

Link Tracking Upper Limit Default 16384, range 16384-32768

— Source — Reply

All IP families All Protocols

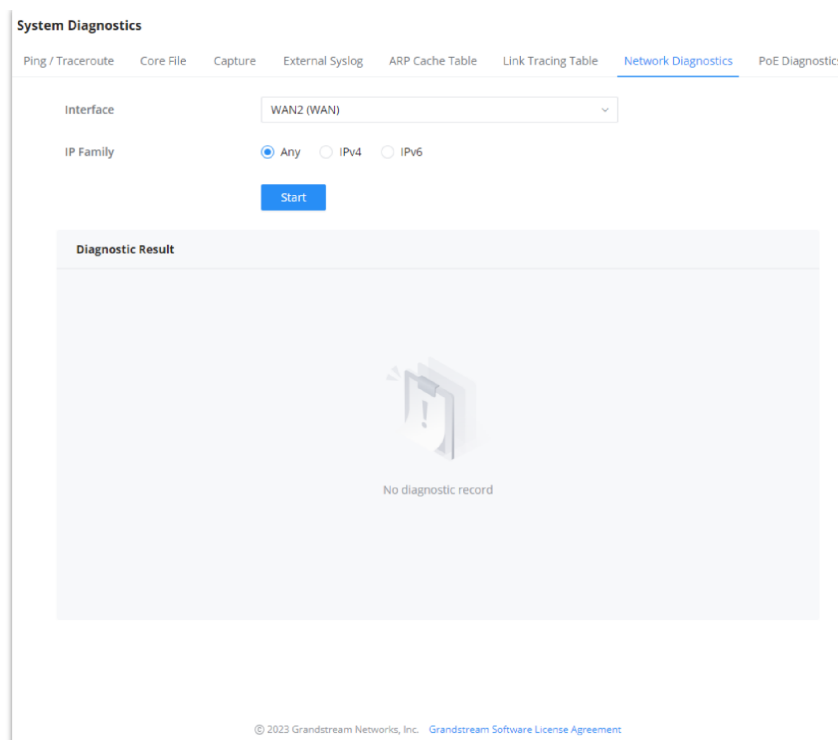
IP Family	Protocol Type	Life Time	Mark	Status	Flow	Packets / Bytes
IPv4	ICMP	9	255	-	192.168.5.99[8] → 8.8.8.8[0]	→ 1/84
					192.168.5.99[0] ← 8.8.8.8[0]	← 1/84
IPv4	ICMP	19	255	-	192.168.5.99[8] → 8.8.8.8[0]	→ 1/84
					192.168.5.99[0] ← 8.8.8.8[0]	← 1/84
IPv4	TCP	299	255	ESTABLISHED	127.0.0.1[35996] ⇄ 127.0.0.1[5303]	→ 12/1515 ← 21/1554
IPv4	-	594	255	-	192.168.80.1[] ⇄ 224.0.0.120[]	→ 4/344 ← 0/0
IPv4	UDP	56	2	-	192.168.80.1[14] ⇄ 255.255.255.255[14]	→ 5/250 ← 0/0
IPv4	ICMP	29	255	-	192.168.5.99[8] → 8.8.8.8[0]	→ 1/84
					192.168.5.99[0] ← 8.8.8.8[0]	← 1/84
IPv4	TCP	299	2	ESTABLISHED	192.168.5.147[57760] ⇄ 192.168.5.99[443]	→ 11/1331 ← 21/1302
					192.168.5.99[56810] ⇄ 44.230.213.222[443]	→ 15/920 ← 11/791

Total: 8 10 / page

Link Tracing Table

Network Diagnostics

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



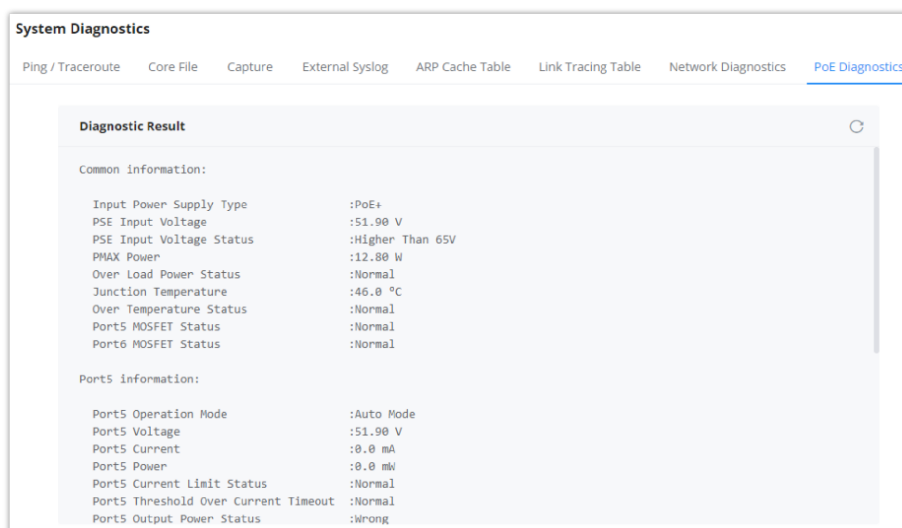
Network Diagnostics

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.

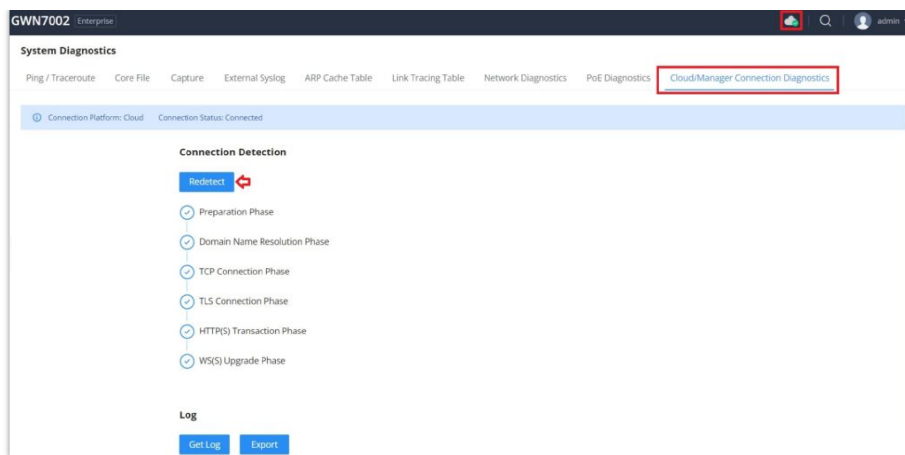


PoE Diagnostics

Cloud/Manager Connection Diagnostics

If the GWN700x router is added to the GWN.Cloud 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 GWN.Cloud 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.

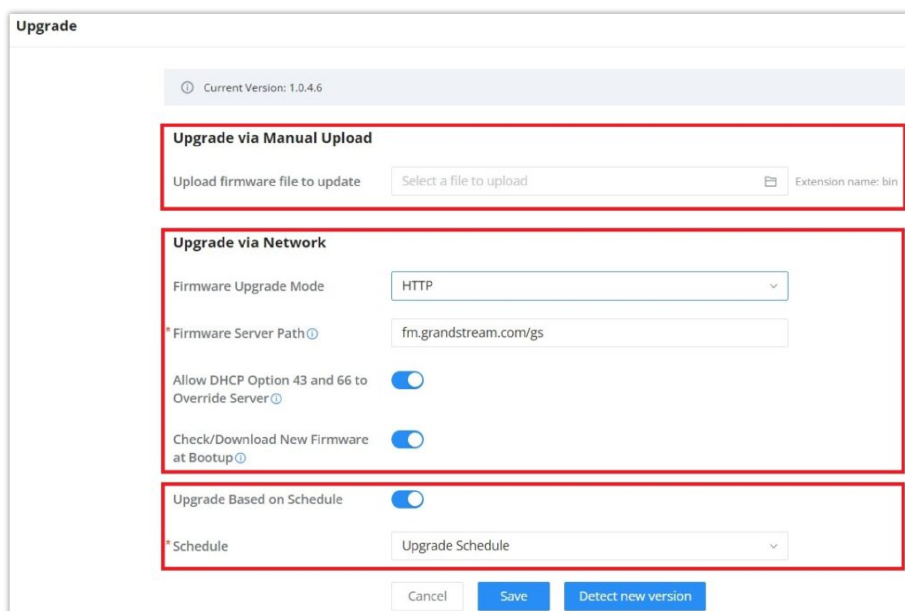


Cloud/Manager Connection Diagnostics

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

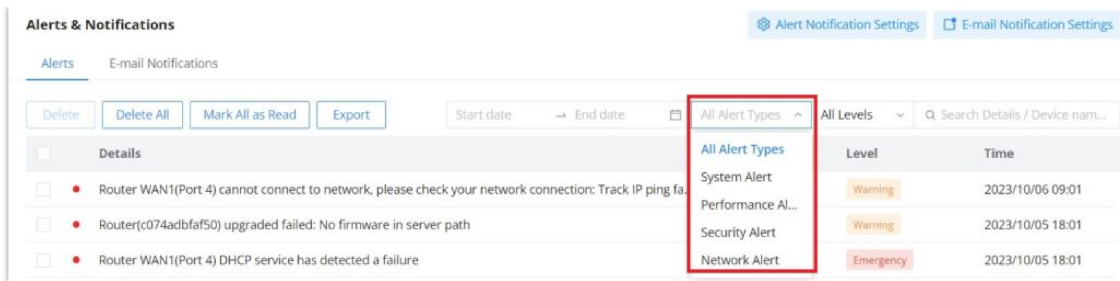
Alerts

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

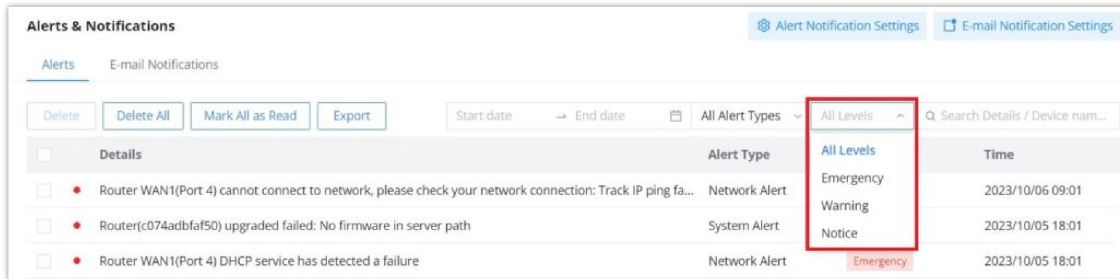
The available types are **System, Performance, Security, Network**, or the user can choose to display all the types.



Alerts Types

Alerts Levels

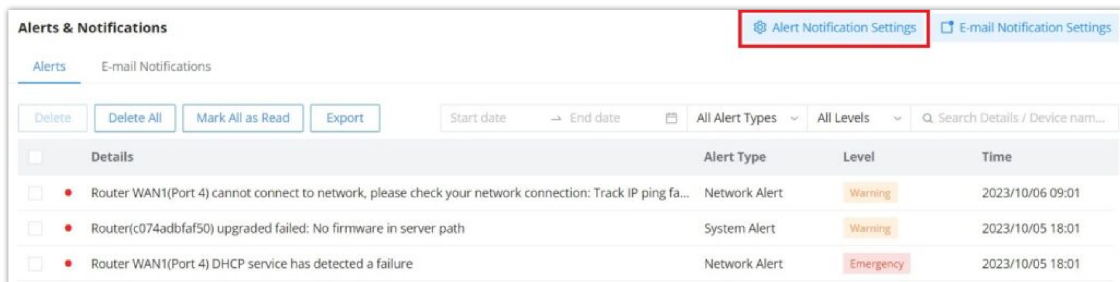
The user can filter the alert level by the following levels: **All Levels, Emergency, Warning or Notice.**



Alerts Levels

Alert Notification Settings

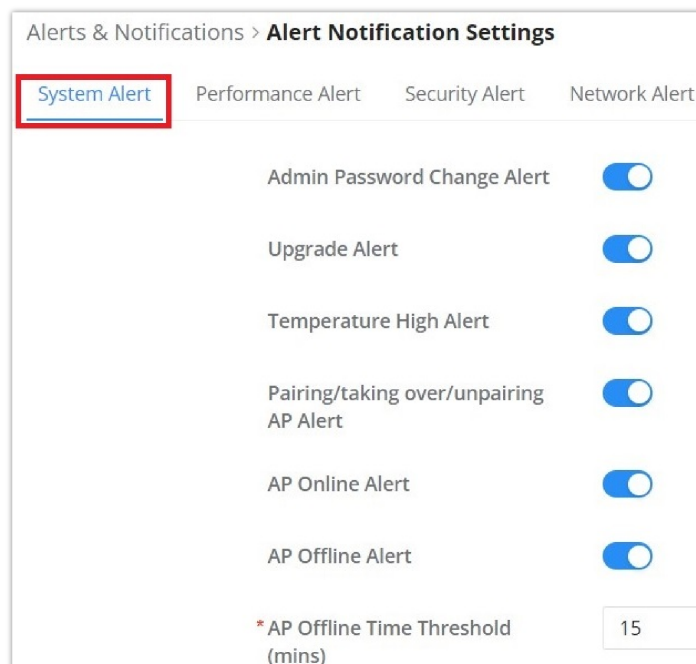
To enable the notifications on the Alerts tab, please click on **"Alert Notification Settings"** button as shown below:



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

Alerts & Notifications > **Alert Notification Settings**

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

Memory Usage Alert

* Memory Usage Threshold (%) Default 90, range 75-100

CPU Usage Alert

* CPU Usage Threshold (%) Default 90, range 75-100

Client Throughput Alert

Client Throughput Mbps Range 1-1024

WAN Port Throughput Alert

* WAN Port

WAN1

WAN Throughput Kbps Range 1-1024

WAN Uplink Bandwidth Kbps Range 1-1024

WAN Downlink Bandwidth Kbps Range 1-1024

Alert Notification Settings – part 2

Alerts & Notifications > **Alert Notification Settings**

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

TCP SYN Flood Attack Alert

UDP Flood Attack Alert

ICMP Flood Attack Alert

ACK Flood Attack Alert

IP Options Attack Alert

TCP Flag Attack Alert

Land Attack Alert

Smurf Attack Alert

Ping of Death Attack Alert

Trace Route Attack Alert

ICMP Fragment Attack Alert

SYN Fragment Attack Alert

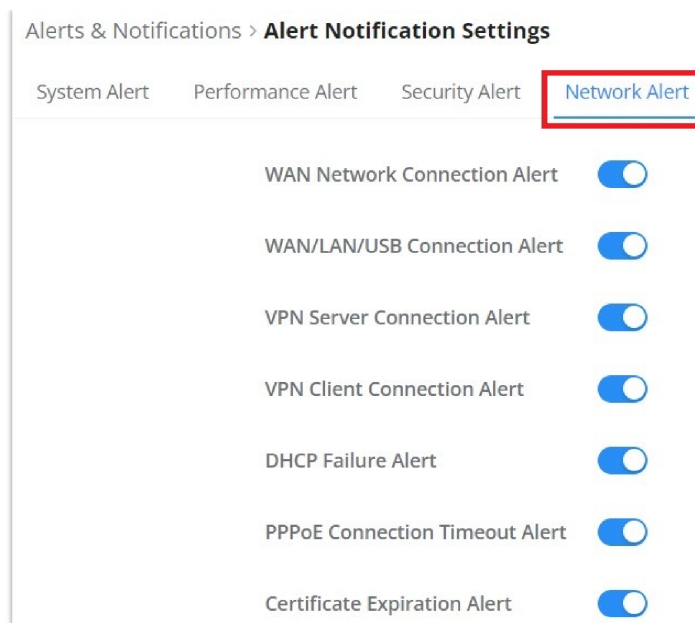
Unassigned Protocol Numbers Attack Alert

Fraggle Attack Alert

ARP Spoofing Attack Alert

IP Spoofing Attack Alert

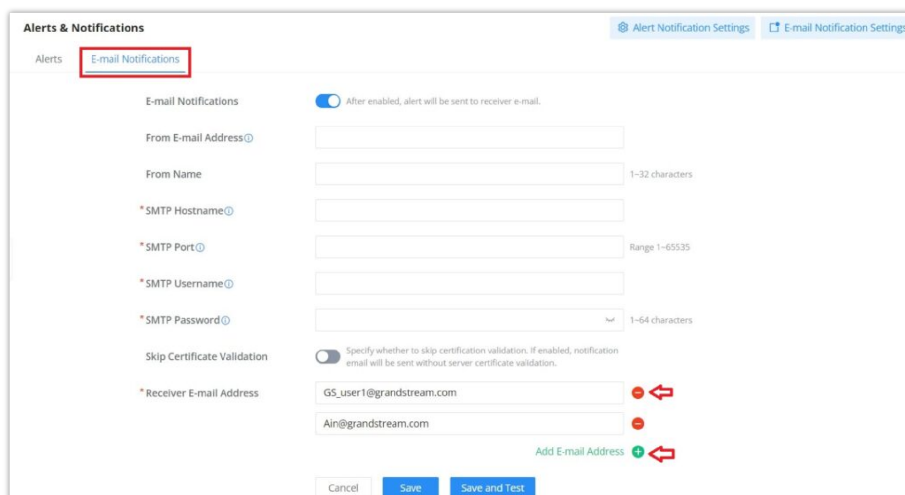
Alert Notification Settings – part 3



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:

The screenshot shows the 'E-mail Notifications' configuration page. At the top right, there are two tabs: 'Alert Notification Settings' and 'E-mail Notification Settings', with the latter being active and highlighted with a red box. The main content area includes a toggle for 'E-mail Notifications' which is turned on. Below this are several input fields: 'From E-mail Address', 'From Name', '*SMTP Hostname', '*SMTP Port', '*SMTP Username', and '*SMTP Password'. There is also a 'Skip Certificate Validation' toggle which is turned off. At the bottom, there is a list of 'Receiver E-mail Address' with two entries: 'GS1@grandstream.com' and 'GS2@grandstream.com', each with a red 'X' icon. An 'Add E-mail Address' button with a green plus icon is located at the bottom right.

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.

This screenshot shows the 'Notification Settings' page with the 'System Alert' tab selected and highlighted with a red box. The page title is 'Alerts & Notifications > Notification Settings'. A blue banner at the top says 'Please select the alerts to be notified by e-mail'. Below the banner are four tabs: 'System Alert', 'Performance Alert', 'Security Alert', and 'Network Alert'. The 'System Alert' tab contains six alert types, each with a description and a toggle switch: 'Admin Password Change Alert', 'Upgrade Alert', 'Temperature High Alert', 'Pairing/taking over/unpairing AP Alert', 'AP Online Alert', and 'AP Offline Alert'. All toggle switches are currently turned on.

E-mail Notification Settings – part 1

This screenshot shows the 'Notification Settings' page with the 'Performance Alert' tab selected and highlighted with a red box. The page title is 'Alerts & Notifications > Notification Settings'. A blue banner at the top says 'Please select the alerts to be notified by e-mail'. Below the banner are four tabs: 'System Alert', 'Performance Alert', 'Security Alert', and 'Network Alert'. The 'Performance Alert' tab contains four alert types, each with a description and a toggle switch: 'Memory Usage Alert', 'CPU Usage Alert', 'Client Throughput Alert', and 'WAN Port Throughput Alert'. All toggle switches are currently turned on.

E-mail Notification Settings – part 2

Alerts & Notifications > **Notification Settings**

Please select the alerts to be notified by e-mail

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

TCP SYN Flood Attack Alert Once enabled, an alert email will be sent: Once a TCP SYN Flood attack is detected/successfully defended	<input type="checkbox"/>
UDP Flood Attack Alert Once enabled, an alert email will be sent: Once a UDP Flood attack is detected/successfully defended	<input type="checkbox"/>
ICMP Flood Attack Alert Once enabled, an alert email will be sent: Once an ICMP Flood attack is detected/successfully defended	<input type="checkbox"/>
ACK Flood Attack Alert Once enabled, an alert email will be sent: Once an ACK Flood attack is detected/successfully defended against	<input type="checkbox"/>
IP Options Attack Alert Once enabled, an alert email will be sent: when the IP Option attack is detected and successfully defended	<input type="checkbox"/>
TCP Flag Attack Alert Once enabled, an alert email will be sent: Once the TCP flag attack is detected and successfully defended	<input type="checkbox"/>
Land Attack Alert Once enabled, an alert email will be sent: Once the Land attack is detected and successfully defended	<input type="checkbox"/>
Smurf Attack Alert Once enabled, an alert email will be sent: Once a smurf attack is detected and successfully defended	<input type="checkbox"/>
Ping of Death Attack Alert Once enabled, an alert email will be sent: Once the ping of death attack is detected and successfully defended	<input type="checkbox"/>
Trace Route Attack Alert Once enabled, an alert email will be sent: Once the trace route attack is detected and successfully defended	<input type="checkbox"/>
ICMP Fragment Attack Alert Once enabled, an alert email will be sent: Once an ICMP fragment attack is detected and successfully defended	<input type="checkbox"/>

E-mail Notification Settings – part 3

Alerts & Notifications > **Notification Settings**

Please select the alerts to be notified by e-mail

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

WAN Network Connection Alert Once enabled, an alert email will be sent when the router is connected or disconnected from the network	<input type="checkbox"/>
WAN/LAN/USB Connection Alert Once enabled, an alert email will be sent when the WAN/LAN/USB port of the router is connected or disconnected	<input type="checkbox"/>
VPN Server Connection Alert Once enabled, an alert email will be sent when the router VPN server establishes a connection or disconnects the connection	<input type="checkbox"/>
VPN Client Connection Alert Once enabled, an alert email will be sent when the router VPN client is connected or disconnected	<input type="checkbox"/>
DHCP Failure Alert Once enabled, an alert email will be sent: Once the DHCP failure is detected	<input type="checkbox"/>
PPPoE Connection Timeout Alert Once enabled, an alert email will be sent: Once the PPPoE connection times out	<input type="checkbox"/>
Certificate Expiration Alert Once enabled, an alert email will be sent: Once the certificate has expired	<input type="checkbox"/>

E-mail Notification Settings – part 4

SYSTEM SETTINGS

Basic Settings

On this page, the user is able to specify a name for the GWN700x router, and configures basic settings: country/region, time zone, NTP server, Reboot plan and LED Indicator either Always On, Always Off or even based on a schedule.

Basic Settings

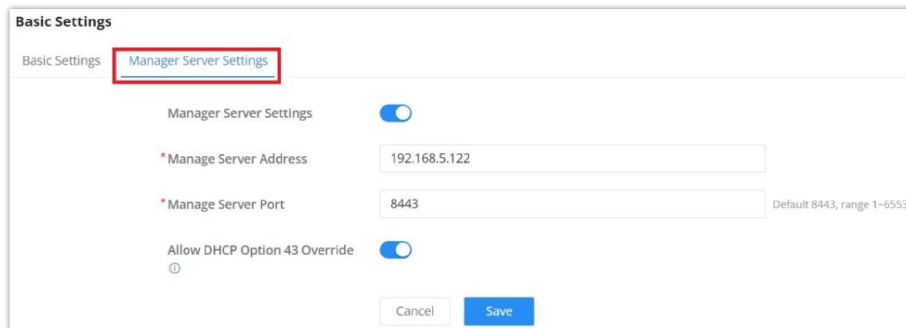
Basic Settings Manager Server Settings

* Device Name	<input type="text" value="GWN7002"/>	1-64 characters
Country / Region	<input type="text" value="Morocco"/>	
Time Zone	<input type="text" value="(UTC) Casablanca, Monrovia"/>	
* NTP Server	<input type="text" value="pool.ntp.org"/>	
Reboot Plan	<input type="text" value="Disabled"/>	
LED Indicator	<input checked="" type="radio"/> Always On <input type="radio"/> Always Off <input type="radio"/> Enabled based schedule	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

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.



The screenshot shows the 'Basic Settings' section with 'Manager Server Settings' selected. It includes a toggle for 'Manager Server Settings' (checked), a text field for '* Manage Server Address' (192.168.5.122), a text field for '* Manage Server Port' (8443) with a default of 8443 and a range of 1-65535, and a toggle for 'Allow DHCP Option 43 Override' (checked). There are 'Cancel' and 'Save' buttons at the bottom.

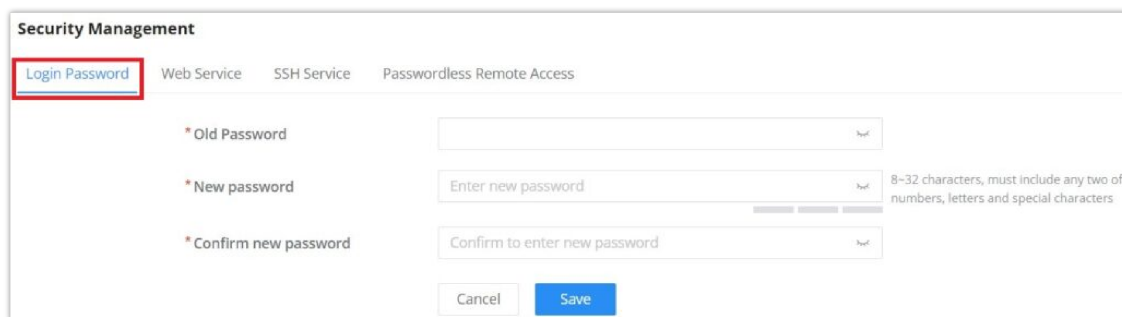
Manager Server Settings

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.

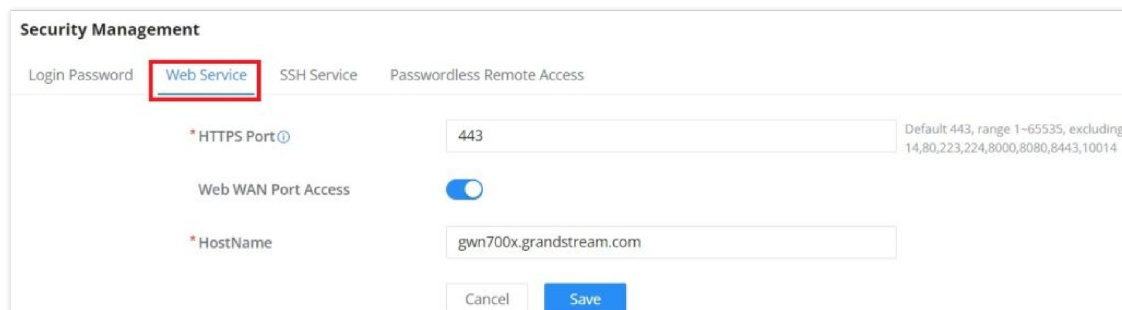


The screenshot shows the 'Security Management' section with 'Login Password' selected. It includes three text fields: '* Old Password', '* New password' (with a strength indicator and a note: '8-32 characters, must include any two of numbers, letters and special characters'), and '* Confirm new password'. There are 'Cancel' and 'Save' buttons at the bottom.

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:

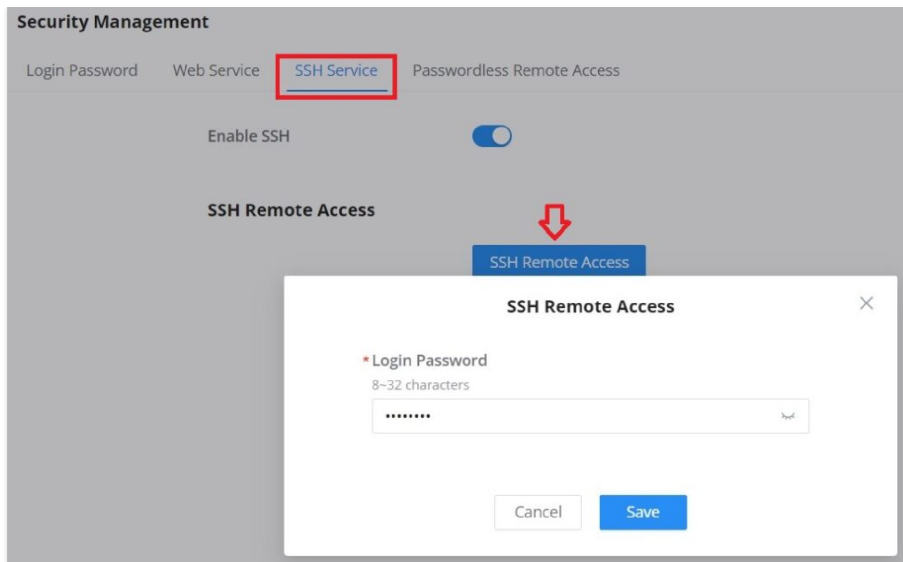


The screenshot shows the 'Security Management' section with 'Web Service' selected. It includes a text field for '* HTTPS Port' (443) with a default of 443 and a range of 1-65535, excluding 14,80,223,224,8000,8080,8443,10014. There is a toggle for 'Web WAN Port Access' (checked) and a text field for '* HostName' (gwn700x.grandstream.com). There are 'Cancel' and 'Save' buttons at the bottom.

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.



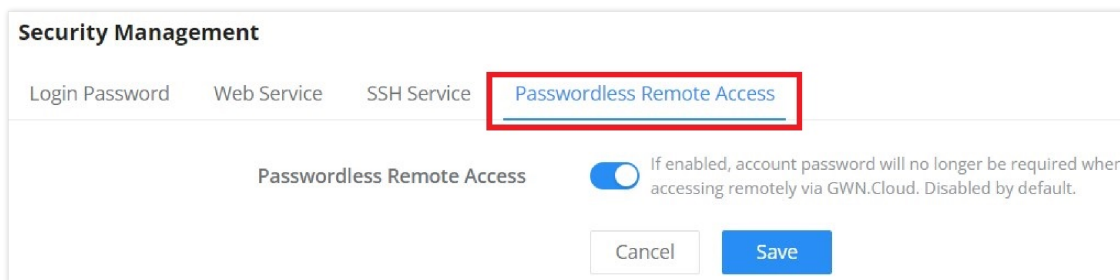
Security Management – SSH Service

Passwordless Remote Access

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

Note

By default is disabled.

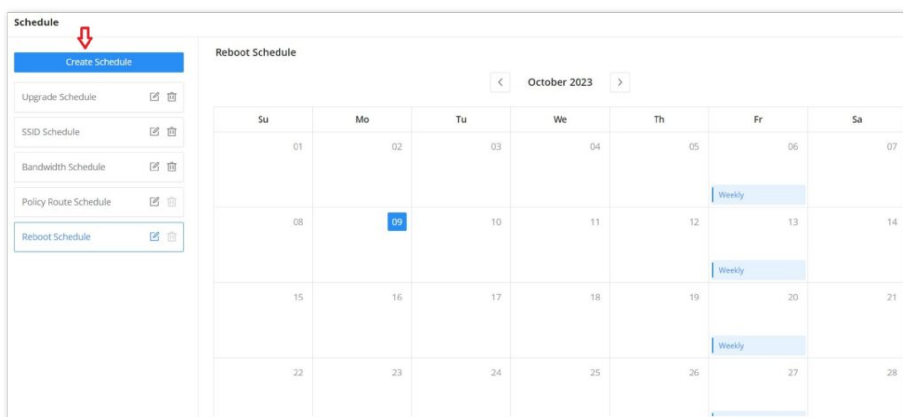


Security Management – Passwordless Remote Access

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.

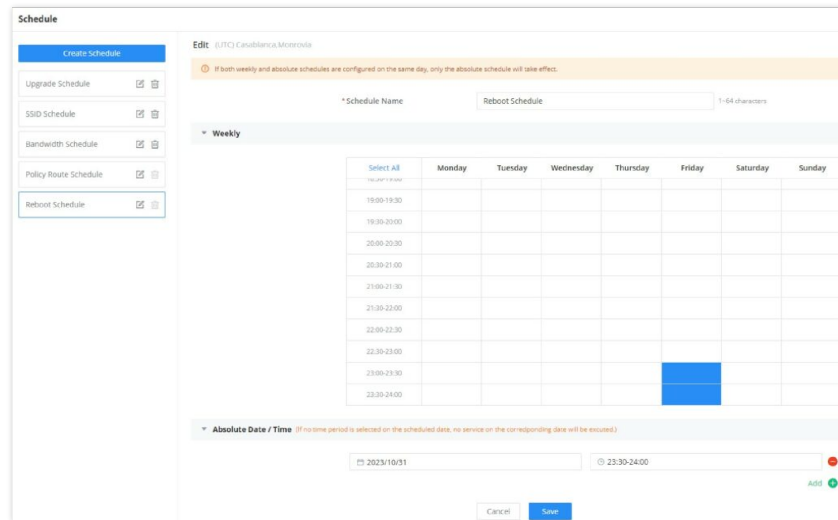
To create a schedule, navigate to **System Settings** → **Schedule**, then click on **“Create Schedule”** button as shown below:



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: <ul style="list-style-type: none">• 512: 512-bit keys are not secure and it's better to avoid this option.

	<ul style="list-style-type: none"> ● 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	<p>Choose the digest algorithm:</p> <ul style="list-style-type: none"> ● 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. <p><i>Note: Hash is a one-way function, it cannot be decrypted back.</i></p>
Expiration (D)	<p>Enter the validity date for the CA certificate in days. The valid range is 1~999999..</p>
Country / Region	<p>Select a country code from the dropdown list. Example: "United Stated of America".</p>
State / Province	<p>Enter a state name or province. Example: "Casablanca".</p>
City	<p>Enter a city name. Example: "SanBern".</p>
Organization	<p>Enter the organization's name. Example: "GS".</p>
Organizational Unit	<p>This field is the name of the department or organization unit making the request. Example: "GS Sales".</p>
Email	<p>Enter an email address. Example: "EMEAregion@grandstream.com"</p>

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.

*Cert. Name 1~64 characters, only support input in English, numbers, characters.

*CA Certificates

Certificate Type

Key Length

Digest Algorithm SHA1 SHA256

*Expiration (D) Range 1~999999

SAN None IP Address Domain

Country / Region

*State / Province

*City

*Organization

*Organizational Unit

*Email

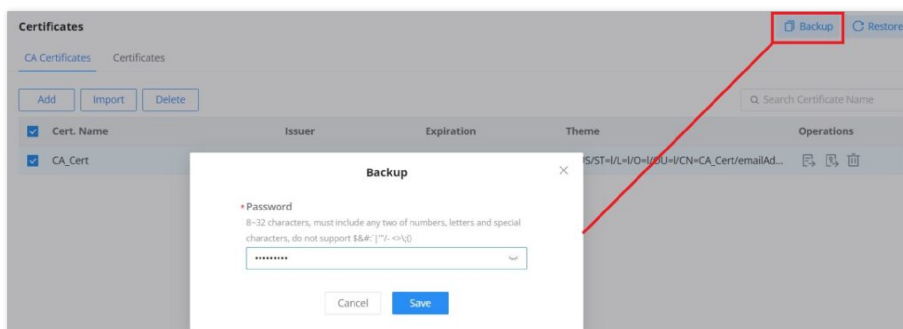
Add Certificate

Cert. Name	Enter the certificate's name.
Key Length	Choose the key length for generating the CA certificate. The following values are available: <ul style="list-style-type: none">● 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. <ul style="list-style-type: none">● 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

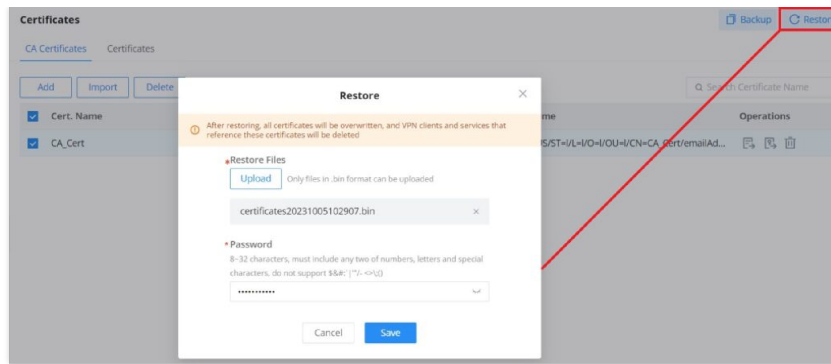
Certificates Backup and Restore

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.

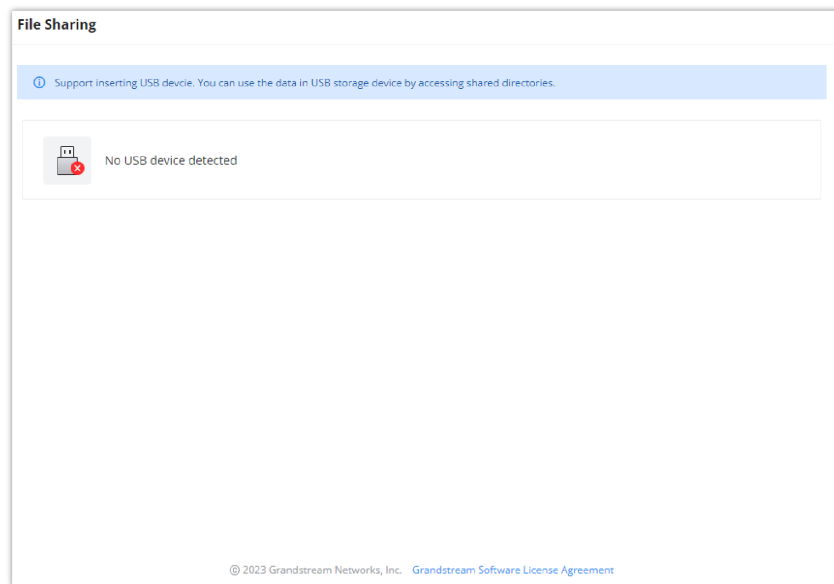


Certificate Restore

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

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 1.0.5.36

- 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.

Need Support?

Can't find the answer you're looking for? Don't worry we're here to help!

[CONTACT SUPPORT](#)