



Grandstream Networks, Inc.

GWN700x Series

GWN700x – User Manual



WELCOME

The GWN700X is a powerful enterprise-grade gigabit Multi-Wan firewall router including 2 SFP Ports and multiple Gigabit RJ45 ports that provides a comprehensive VPN solution in one and multiple scenarios. As a high-performance and dynamic firewall product, it supports DPI in-depth security detection and content security including URL filtering, domain name filtering, content filtering, safe search, application identification, traffic statistics, and other comprehensive attack protection, which can effectively ensure continuous and stable operation of enterprise core applications and services, and ensure enterprise management administrators can better monitor and manage network traffic. GWN700X integrates a series of rich functions, including NAT, firewall, VPN, load balancing, and bandwidth management capabilities. As a fanless PoE router, GWN700x can be powered by an external power adapter or IEEE 802.3af/at PoE Input, and 2x GbE ports can support 48V Passive or Active (IEEE802.3af Class 2) PoE output. It is also supported by GWN.Cloud and GWN Manager, Grandstream's free cloud and on-premise network management platform that makes managing your network or several networks across multiple locations easier than ever before. Ideal for the enterprise retail, education, hospitality, and medical markets.

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		
RAM/Flash	256MB/256MB		512MB/256MB
NAT Routing & IPSec VPN Performance	<ul style="list-style-type: none">• 2.2Gbps• 530Mbps IPSec VPN throughput		
Network Interfaces	6x Gigabit Ethernet ports <i>*All ports are WAN/LAN configurable.</i>	2 x Gigabit SFP ports and 4x Gigabit Ethernet ports <i>*All ports are WAN/LAN configurable</i>	2 x Gigabit SFP ports and 9 x Gigabit Ethernet ports <i>*All ports are WAN/LAN configurable</i>
Auxiliary Ports	1x USB 2.0 port, 1 x Reset Pinhole		
Mounting	<ul style="list-style-type: none">• Desktop• Wall mounting		
LEDs	8 x single-color LEDs for device tracking and status indication		13 x single-color LEDs for device tracking and status indication
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		

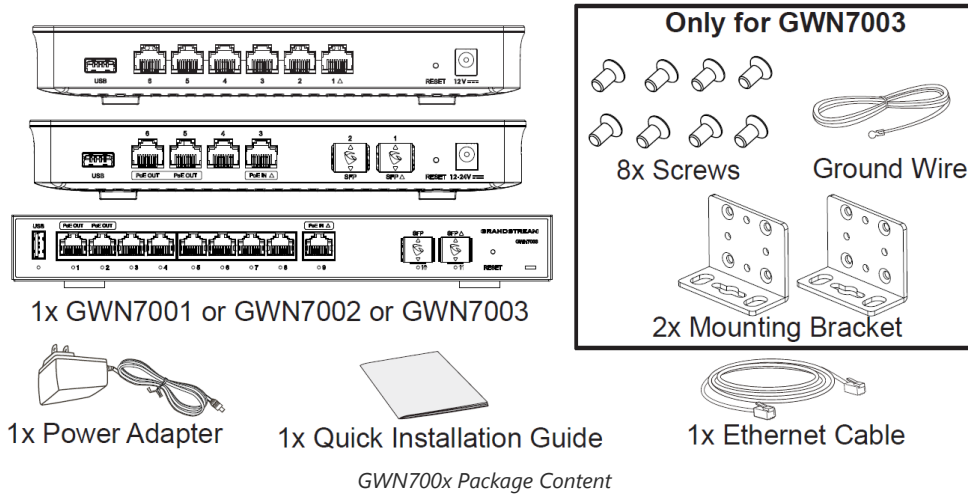
Firewall	DPI, DDNS, Port Forwarding, DMZ, UPnP, Anti-DoS, traffic rules, NAT, ALG		
VPN	<ul style="list-style-type: none"> • SSL VPN Server / Client-to Site • IPsec VPN Client-to-Site / Site-to-Site • PPTP VPN Server / Client-to-Site • L2TP Client-to-Site • IPsec Encryption: DES, 3DE, AES • IPsec Authentication: 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/L2TP Encryption: MPPE 40-bit, 128-bit, IPsec • PPTP/L2TP Authentication: MS-CHAPv1/2 		
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 50°C Storage: -10°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

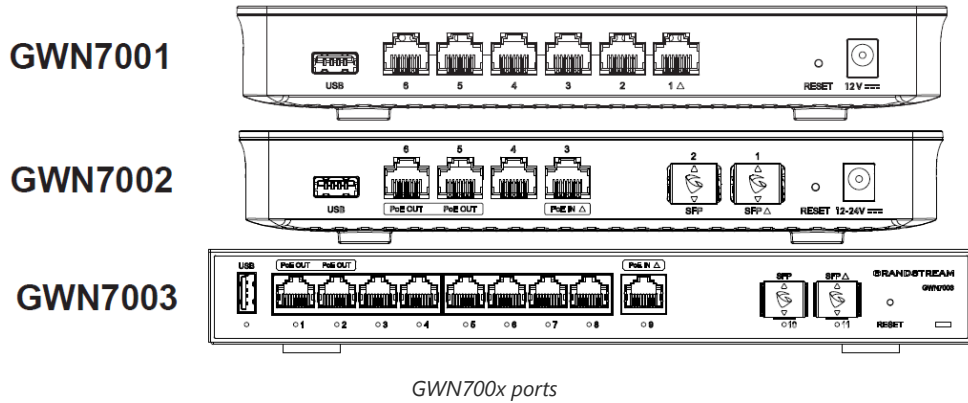
INSTALLATION

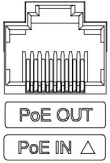





Before deploying and configuring the GWN700x router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN700x router.

Package Contents



GWN700x Ports

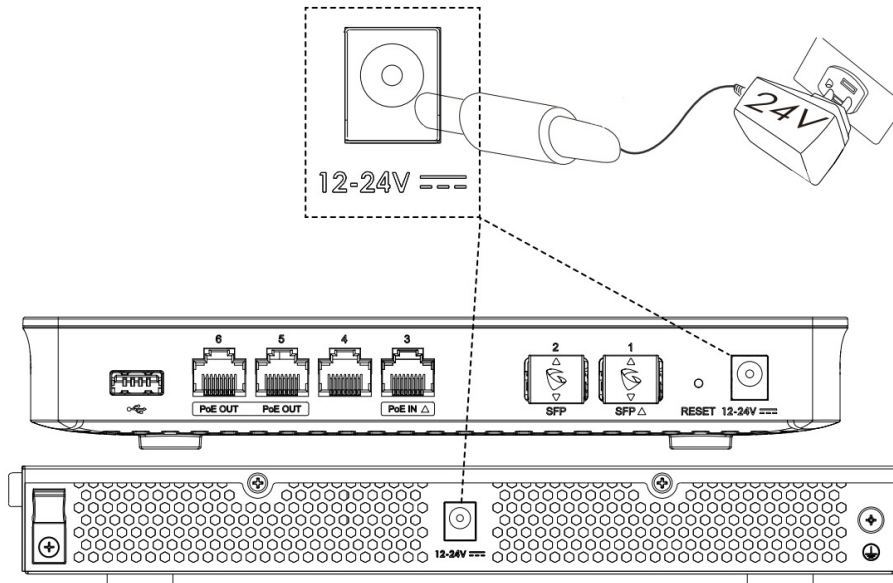


No.	Port	Description
1		<ul style="list-style-type: none"> • GWN7001: 6x Gigabit Ethernet ports • GWN7002: 4x Gigabit Ethernet ports • GWN7003: 9 x Gigabit Ethernet ports <p>Note: All ports support WAN/LAN configurable. The Gigabit Ethernet ports include 2 x PoE OUT ports and 1 x PoE IN port (GWN7002/7003 only).</p>
2		2 x 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

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).

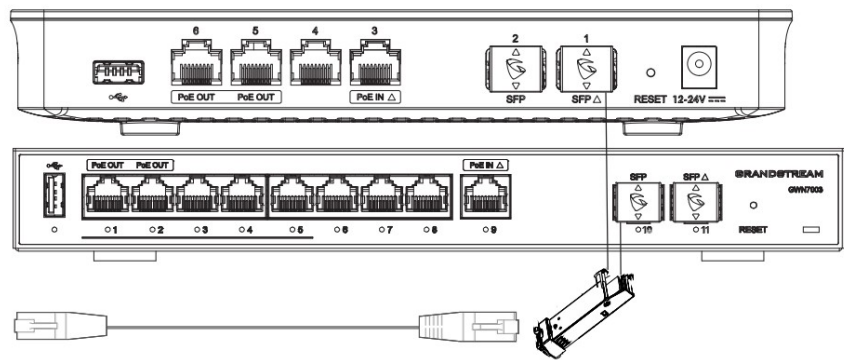


Powering the GWN700x routers

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.

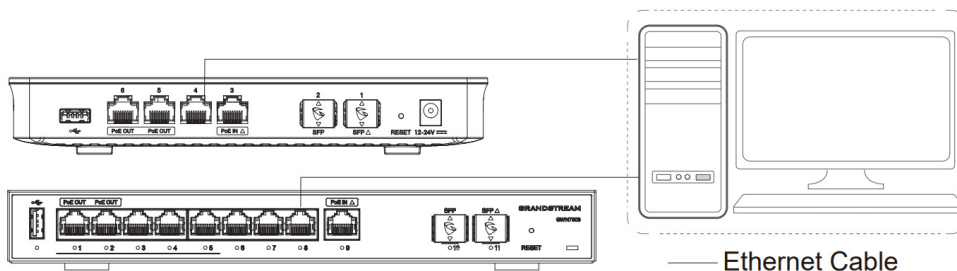
Internet
Optical Fiber
ADSL Modem
Community Broadband



Connect GWN700x to the Internet

3. Connect to GWN7002/7003 Network

Connect your computer to one of the LAN ports.



GWN700x network

Note:

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

Safety Compliances

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

Warranty

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

GETTING STARTED

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

Use the WEB GUI

Access WEB GUI

The GWN700x embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, or Google Chrome.



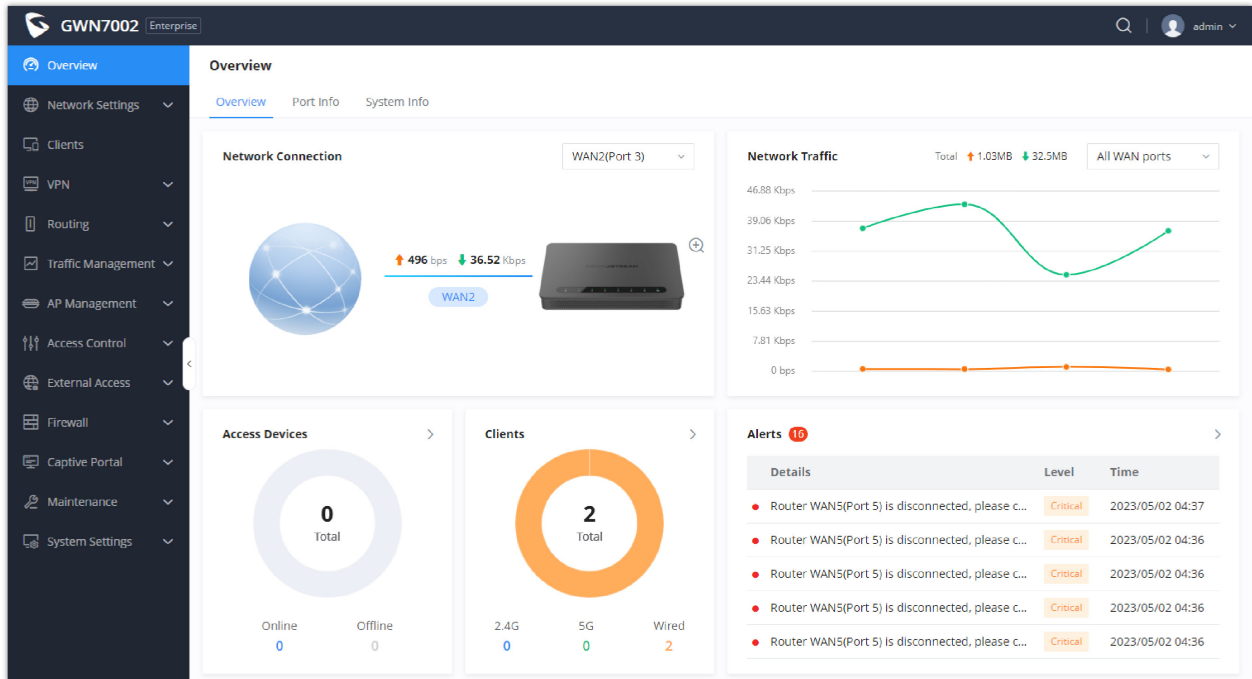
GWN700x Web GUI Login Page

To 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.

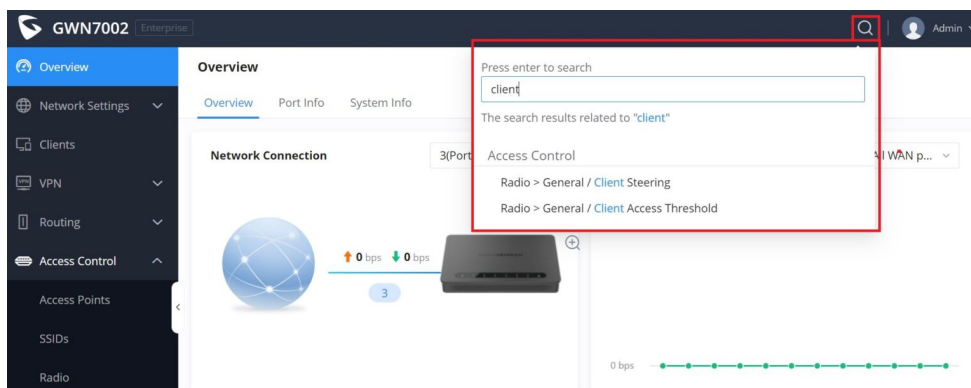
Once the user enters the password, this is the initial page that will be shown. This page contains general information about the router.



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.




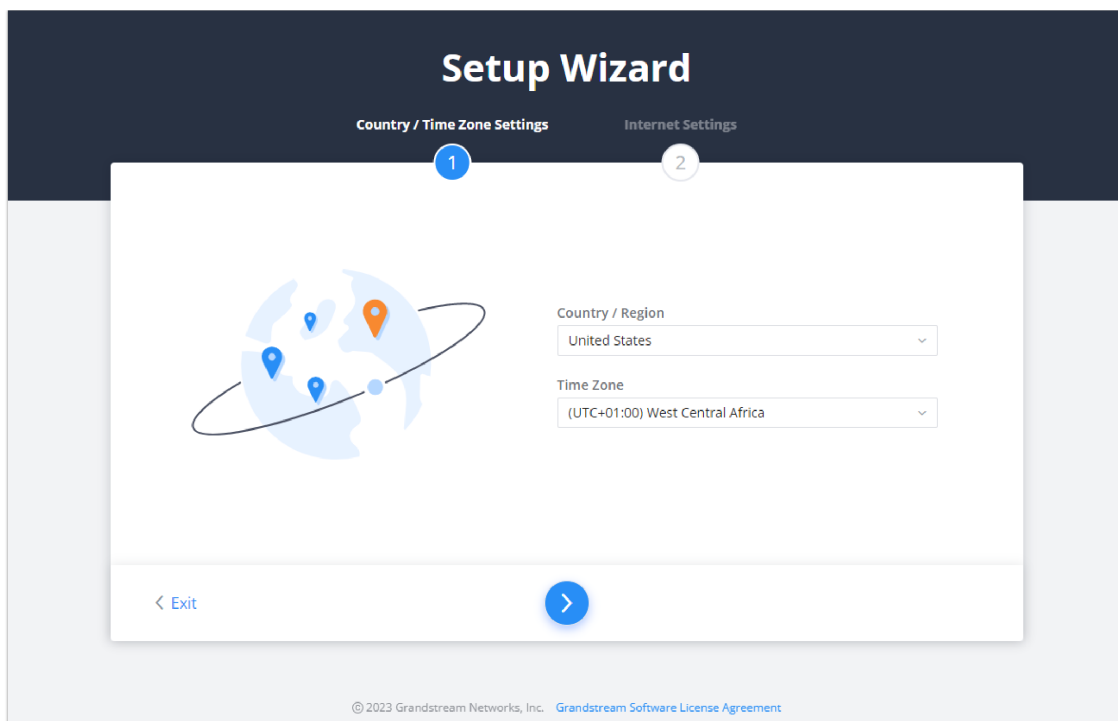
Search

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.

Click on  button to go through the setup wizard.



Setup Wizard

Feedback

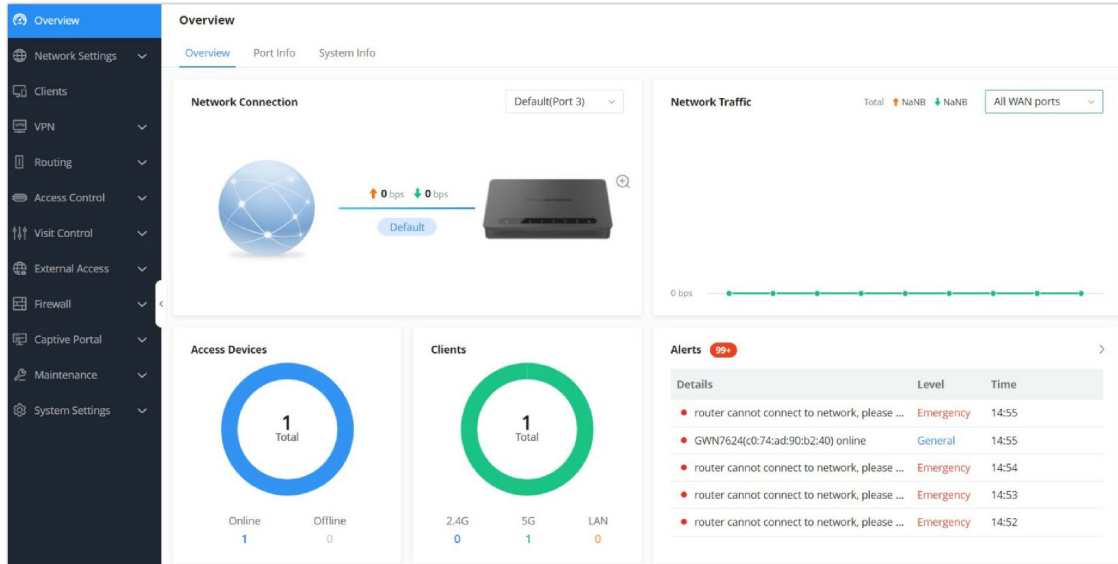
If the user has a question or a suggestion to make the GWN700x product even better or has an issue, he can always send feedback, in case of a problem it's better as well to include Syslog as it may help solve the problem faster.

Feedback

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 as well as the System Info (Product Name, System Version, MAC Address...). It is used to show the status of the GWN700x for different items like (upload and download speed, number of clients connected, bands used, access devices, network traffic, alerts, top access devices, top SSIDs, and top clients).



Overview Page

Network Connection	Display the current status of the router, is it connected or not, as well as showing the current upload and download speed.
Network Traffic	Shows network traffic in real time.
Access Devices	shows the total number of Access Devices online and offline.
Clients	Shows the total number of clients connected to 2.4G and 5G as well as the ones connected to the LAN.
Alerts	Shows Alerts General, Important or Emergency with details and time.
Clients Speed	Displays Clients speed based on time (1H, 12H, 1D or 1W)
Top Clients	Shows the Top Clients list, users may sort the list of clients by their upload or download. Users may click on to go to Clients page for more options.
Top SSIDs	Shows the Top SSIDs list, users may sort 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, sort 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.

System Info

System Info displays **Device Status** to check MAC address, Part Number, Firmware related information, and Uptime for the GWN700x and **WAN Status** showing general information about WAN Port such as IP address and Connection Type.

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

System Info	
Product Name	GWN7003
Hardware Version	V1.3A
System Version	1.0.1.6
MAC Address	C0:74:AD:C9:72:E9
Part Number	9640006813A
Serial Number	20VXVYZP10C972E9
Boot Version	0.0.0.5
System Up Time	1h 55min
System Time	2023-06-22 06:11
Load Average	1min: 2.38 5min: 2.32 15min: 2.28
Temperature ⓘ	76°C

System Info

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**:

The screenshot shows the 'Port Info' page in the router's Web GUI. At the top, there are navigation tabs for 'Overview', 'Port Info', and 'System Info'. Below the tabs is a port status overview diagram showing various ports: USB, PoE OUT (LAN 6, WAN 5), PoE IN (WAN 3), and SFP (LAN 2, LAN 1). A legend indicates that green icons represent 'Link up' and grey icons represent 'Link down'. The WAN2 port (PoE IN) is highlighted in blue.

WAN2 ⓘ

Basic Info

Status	Enabled
MAC Address	C0:74:AD:BF:AF:52
Port Type	GE
Speed/Duplex	1000M Full Duplex
Flow Control Status	Auto Negotiation
Network Traffic	↑ Pkts / Bytes: 9537 / 1.1MB ↓ Pkts / Bytes: 93352 / 35.5MB
Current Rate	↑ 552bps ↓ 15.1Kbps

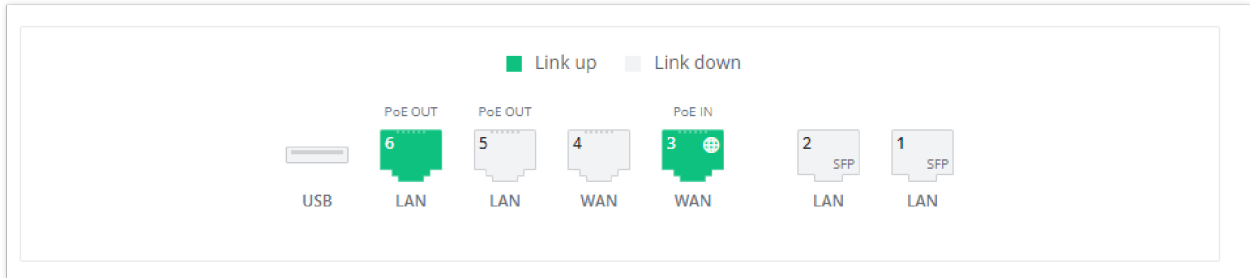
NETWORK SETTINGS

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. The ports connected will be highlighted in green, while the ports which are not connected will be shown in gray.



- **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 Type	Name	Role	Speed/Duplex	Flow Control
Port1	SFP	-	LAN	2500M Full Duplex	Disable
Port2	SFP	-	LAN	Auto Negotiation	Disable
Port3	GE	WAN2	WAN	1000M Full Duplex	Auto Negotiation
Port4	GE	WAN1	WAN	2500M Full Duplex	Auto Negotiation
Port5	GE	-	LAN	Auto Negotiation	Auto Negotiation
Port6	GE	-	LAN	100M Full Duplex	Auto Negotiation
Port7	GE	-	LAN	1000M Full Duplex	Auto Negotiation

Port	This field indicates the port number.
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

	<ul style="list-style-type: none"> • WAN
Speed/Duplex	<p>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. 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.</p>
Flow Control	<p>The user can enable or disable flow control using this option. When the setting is set to Auto Negotiation, the router will determine based on the settings negotiated with the device connected.</p> <p>Note:</p>

◦ **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.

PoE Configuration ^

Total Power Limit ⓘ Auto 12.8W 24.8W

Port	Power Supply Mode ⓘ	Maximum Power Supply ⓘ	Priority
Port5	Active PoE(802.3af/at) v	12.8W v	Low v
Port6	Active PoE(802.3af/at) v	12.8W v	High v

Total Power Limit	<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 corresponds to the following values: • 24.8W: This can be selected if power adaptor output values which corresponds to the following values: 24VDC 1.5A.
Port	<p>This field indicates the port number.</p>
Power Supply Mode	<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>
Maximum Power Supply	<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>
Priority	<p>Specify the priority of the port in terms of the power supply.</p> <ul style="list-style-type: none"> • High • Low

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.

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 Configuration

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

WAN > Edit 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

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>

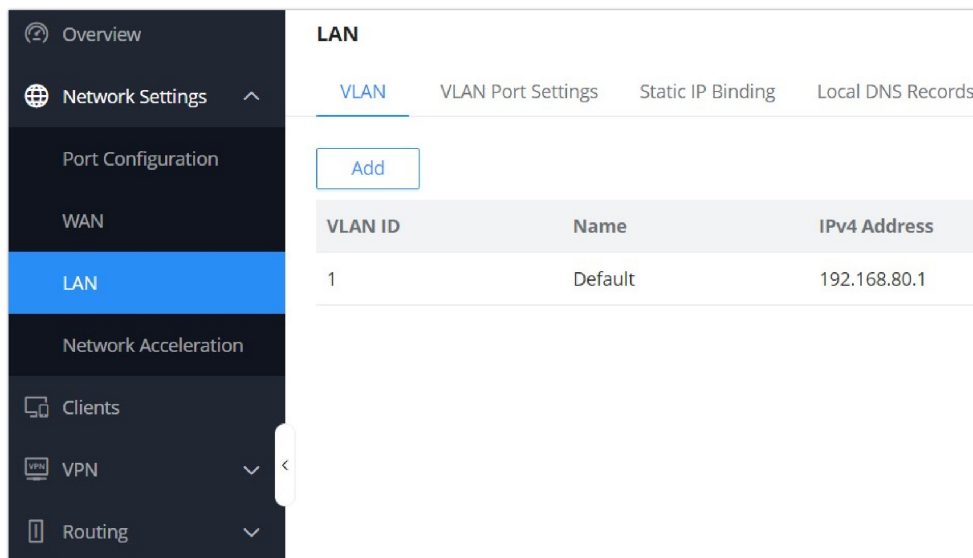
Static DNS	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server.
Maximum Transmission Unit (MTU)	Configures the maximum transmission unit allowed on the wan port. <ul style="list-style-type: none"> • When using Ethernet, the valid range that can be set by the user is 576-1500 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	Select if either to enable or disable VLAN Tag.
Multiple Public IP Address	Please use with Port Forward function, so that you can access to router via public IP address.
VPN	
VPN	<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	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)	This configures the value of the maximum transmit unit. The valid range for this value is 576 - 1460. The default value is 1430. Note: Please do not change this value unless it's necessary.
IPv6 Settings	
IPv6	Enable this option to use IPv6 on this specific WAN port.
Connection Type	<ul style="list-style-type: none"> • Obtain IP automatically (DHCPv6) • Enter the IP manually (static IPv6)
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

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.




LAN configuration

VLAN

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

◦ Add or Edit VLAN

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

 Edit button.

LAN > Add VLAN



*VLAN ID	<input type="text" value="7"/>
Name	<input type="text" value="Seven"/>
Destination ⓘ	<input type="text" value="WAN1 (WAN) WAN2 (WAN)"/>
VLAN Port IPv4 Address	<input checked="" type="checkbox"/>
*IPv4 Address	<input type="text" value="192.168.7.0"/>
*Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Service	<input type="checkbox"/>
VLAN Port IPv6 Address	<input type="checkbox"/>
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>

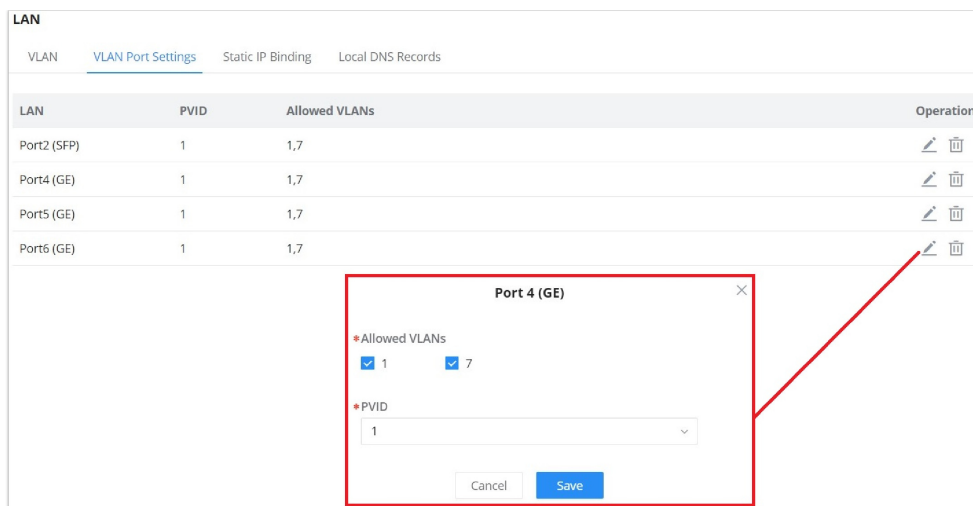
Add or Edit VLAN

VLAN ID	Enter a VLAN ID Note: VLAN ID range is from 3 to 4094. Up to 8 VLANs supported
Name	Enter the VLAN name
Destination	Select the destination interfaces (the WAN ports). Note: by default, interfaces in the Default rule of the load balancing pool is selected and cannot be deselected
VLAN Port IPv4 Address	Check IPv4 Address to specify the 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	Enter or Add DHCP Options
Preferred DNS Server	Enter the Preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server

Add or Edit VLAN

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

Users can use the feature to set **Static IP Binding** to certain clients, to whom they do not want the IP address to change.

To configure Static IP Binding, please follow the below steps:

- 1- Go under the menu **Network Settings** → **LAN** → **Static IP Binding**.
- 2- Click on "Add" button to create a new entry.
- 3- Enter the device's MAC address and IP address.

The 'Static IP Binding' modal window contains the following fields:

- VLAN:** A dropdown menu with 'Default' selected.
- Binding Devices:** A dropdown menu with a blurred selection.
- MAC Address:** A text field with a blurred input.
- *IP Address:** A text field with '192.168.80.' and a separate field with '235'.

'Cancel' and 'Save' buttons are located at the bottom.

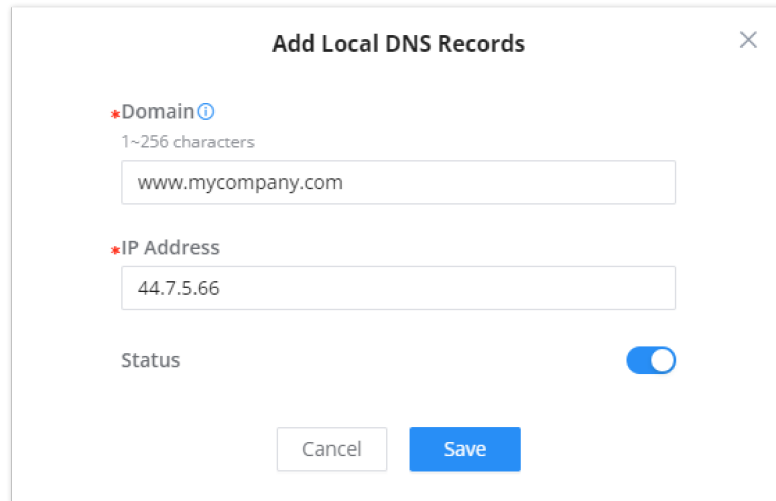
Static IP Binding

VLAN	Select the VLAN or Default VLAN
Binding Devices	Select to input manually by entering the MAC Address and IP Address or select from the clients list.
MAC Address	Enter the MAC Address
IP Address	Enter the IP Address

Static IP Binding

Local DNS Records

Local DNS Records is a feature that allows the user to add 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 [X]

*Domain ⓘ
1~256 characters
www.mycompany.com

*IP Address
44.7.5.66

Status

Cancel Save

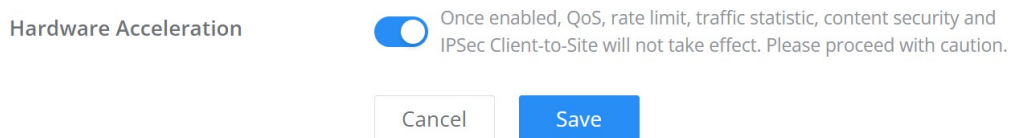
Add Local DNS Records

- 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.

Network Acceleration

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

Network Acceleration



Hardware Acceleration Once enabled, QoS, rate limit, traffic statistic, content security and IPSec Client-to-Site will not take effect. Please proceed with caution.

Cancel Save

Hardware Acceleration

Important

Once enabled, QoS, rate limit, traffic statistic, content security and IPSec Client-to-Site 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.


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

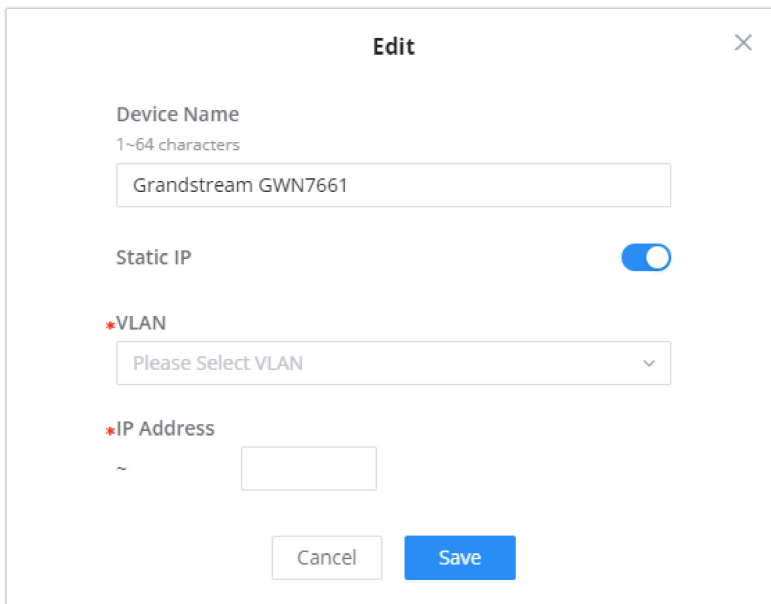
MAC Address	Device Name	IP Address	Connection Type	Duration	Total	Upload	Download	Operations
E8[redacted]	DESKTOP-M3K...	IPv4:192.168.8...	5G	1h 17min	3.39MB	887.26KB	2.53MB	[edit]
C0:74:AD[redacted]	Grandstream G...	IPv4:192.168.8...	Wired	21min	47.89KB	33.99KB	13.9KB	[edit]
C0:74:AD[redacted]	Grandstream G...	IPv4:192.168.8...	Wired	21min	7.65KB	7.28KB	380B	[edit]
[redacted]	Unknown device	IPv4:192.168.8...	Wired	1min	0B	0B	0B	[edit] [delete]

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.
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.</p> <p>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.


○ **Edit Device**

In 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.



Edit Device

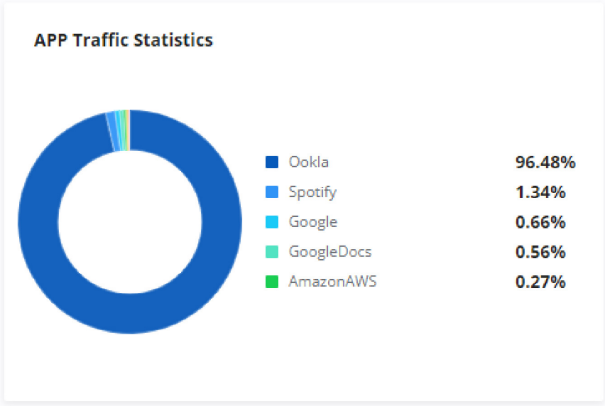
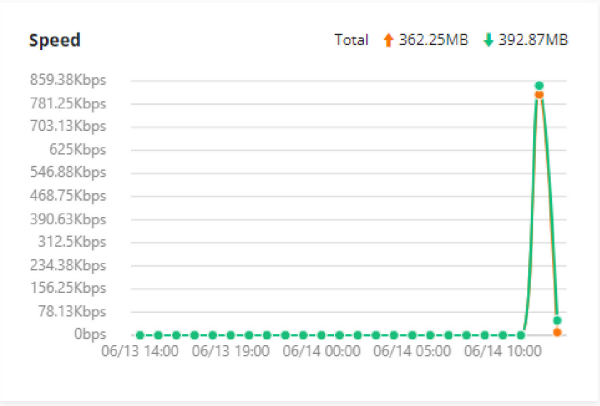
- **Delete Device**

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

- **View Client Information and Report**

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

Recently 1H 12H 1D 1W



APP List

All APP Groups Q Search Name

Name	App Group	Percentage	Total	Upload	Download
Ookla	Network	96.48%	703.49MB	↑ 349.84MB	↓ 353.64MB
Spotify	Media Streaming Services	1.34%	9.79MB	↑ 1.24MB	↓ 8.55MB
Google	Web Services	0.66%	4.85MB	↑ 1.39MB	↓ 3.45MB
GoogleDocs	Collaborative	0.56%	4.06MB	↑ 3.89MB	↓ 171.92KB
AmazonAWS	Web Services	0.27%	1.98MB	↑ 375.96KB	↓ 1.62MB
TLS	Web Services	0.21%	1.51MB	↑ 486.01KB	↓ 1.04MB
Wikipedia	Web Services	0.15%	1.11MB	↑ 21.39KB	↓ 1.08MB
GoogleServices	Web Services	0.09%	664.64KB	↑ 179.28KB	↓ 485.36KB

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

ROUTING

This section is about adding routes either Static Routing or Policy Routing that can be applied on an Interface WAN or LAN/VLAN where the user can specify the next Hop and Metric for the static routing or priority and weight for the policy routing.

Policy Routes

Load Balance Pool

The policy-based Routing feature allows a network administrator to make advanced routing decisions for traffic passing through the router. This feature allows 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.

Creating/Configuring Routing Policies

To configure a new routing policy, first users need to create members under the menu **Routing** → **Policy Routing**.

Policy Routing

[Load Balancing Pool](#) Policy Routing

[Add](#) [Delete](#)

<input type="checkbox"/>	Name	Mode	Interfaces	Interface	Weight	Operations
<input type="checkbox"/>	▼ Default	Load Balancing	3	WAN2 (WAN)	1	✎

Total: 1 [<](#) [1](#) [>](#) 10 / page [v](#)

Policy Routing page

Using Routing Policies

- **Add VLAN**

To use the routing policies created navigate to **“Network Settings → LAN”**, then add a new VLAN or edit previously created ones.

LAN > **Add VLAN**

*VLAN ID Range 3-4094

Name 0-64 characters

Destination [ⓘ](#) [v](#)

VLAN Port IPv4 Address

VLAN Port IPv6 Address

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

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

Add VLAN

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 **Network Settings → Routing → Static Routing**.

To add a new Static Route, the user needs to click on [+ Add](#)

Static Routing

[IPv4 Static Routing](#) [IPv6 Static Routing](#)

Add Manually

[Add](#) [Delete](#)

<input type="checkbox"/>	Name	Status	IP Address	Subnet Mask	Outgoing Interface	Next Hop	Metric	Operations
--------------------------	------	--------	------------	-------------	--------------------	----------	--------	------------



No data

Routing Table

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

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

Static Routing Page

Static Routing > Add IPv4 Static Routing

*Name 1~64 characters

Status

*IP Address

*Subnet Mask

*Outgoing Interface

Next Hop

*Metric The default is 60, with a range of 1-255. 1 is the highest priority.

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

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.
---------------	---

Static Routing

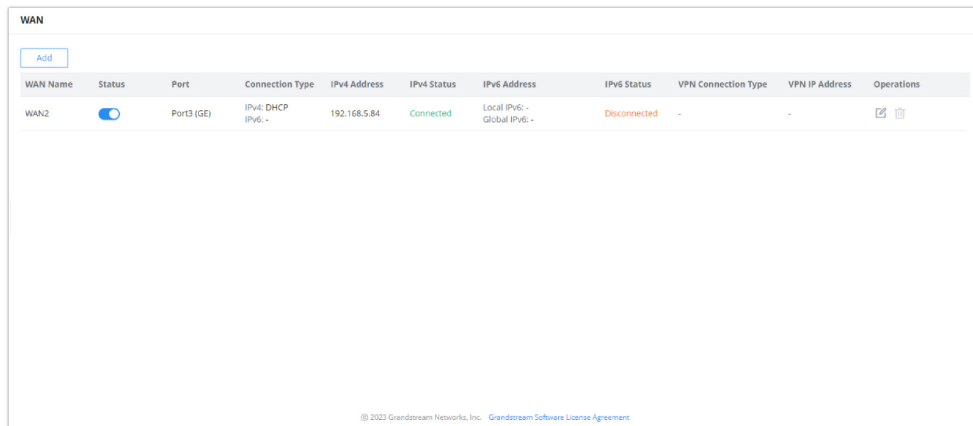
WAN Load Balancing

GWN700X series support load balancing using the multiple WAN feature it offers. Load balancing leverages the availability of multiple WAN ports to efficiently offload the traffic on one Internet and link and divide it among the Internet links available, which optimizes the use of the bandwidth.

To load balance between multiple WAN ports please follow the steps below:

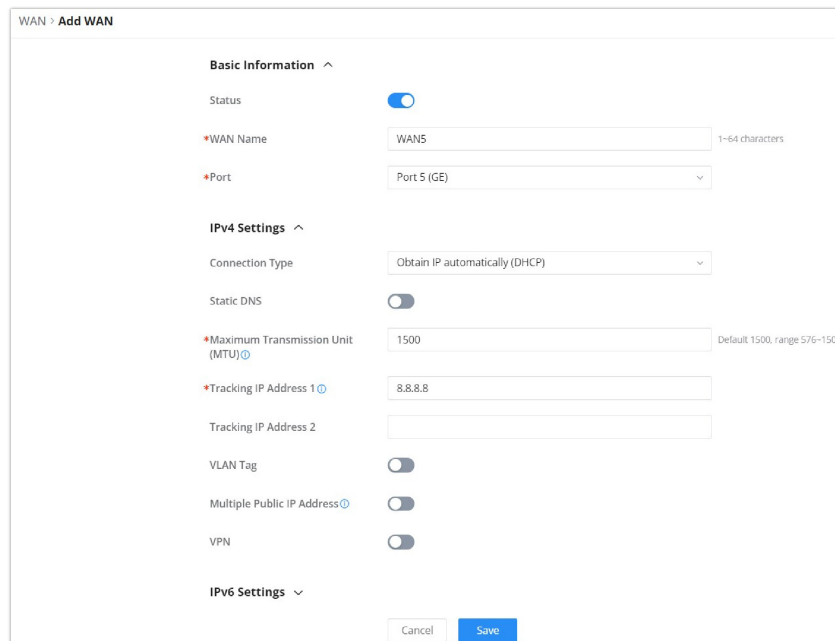
1. Configure multiple WAN ports

The first thing to do is to make sure that Dual WAN Port is Enabled under **Network Settings** → **WAN** → **WAN Port Settings**.



Enable Dual WAN Port

Click on [Add](#) to add a new WAN port.



Add WAN

On the configuration page, toggle on the status of the port to enable it, then give it a name and select the interface which you want to configure as a WAN port. Then, click "Save".

Once the port has been configure, the user can configure a load balancing routing policy.

2. Add Policy Routing

Navigate to **Routing** → **Policy Routing** and click on [+ Add](#)

Policy Routing > **Add Load Balancing Rule**

*Name 1~64 characters

Mode Load Balancing Backup

*Interface

Interface	Weight ⓘ	
<input type="text" value="WAN2 (WAN)"/>	<input type="text" value="1"/>	<input type="button" value="−"/>
<input type="text" value="WAN4 (WAN)"/>	<input type="text" value="1"/>	<input type="button" value="−"/>

[Add](#)

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

Add Policy Routing

Enter the name of the rule, then select “Load Balancing”. Then, Select the interfaces which will be performing the load balancing.

Enter the weight of each interface, the weight indicates the offloading rate to each link. The higher the weight, the higher then bandwidth offloaded to the link.

Failover

GWN routers support Failover, this feature enables the routers to use more than one WAN, and in case there is a link failure or any other issue, the GWN routers will pick that up and use the other WANs. The secondary WANs are considered as a backup.

Once you enable Dual WAN feature an option (**Tracking IP Address**) will appear to configure a destination (address), these addresses will be used to check if the WAN port is functional by pinging these pre-configured destinations.

These pre-configured addresses will be pinged every 10 seconds, and if there is no response to 5 consecutive pings (Packet loss) only then the router will switch to the other port.

Note

Packet loss/latency etc don't count as line failure.

Please navigate to **Network Settings** → **WAN** → **IPv4 Settings (or IPv6 Settings)** to configure **Tracking IP Addresses**, by default DNS 8.8.8.8 Address is used, the user can change the default address or add another address (**Tracking IP Address 2**).

Policy Routing > **Edit Load Balancing Rule**

* Name: Default
1~64 characters

Mode: Load Balancing Backup

Preferred Interface: Interface: WAN2 (WAN) Weight: 10

Alternate Interface: Interface: WAN4 (WAN) Weight: 1

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

Tracking IP Address

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".

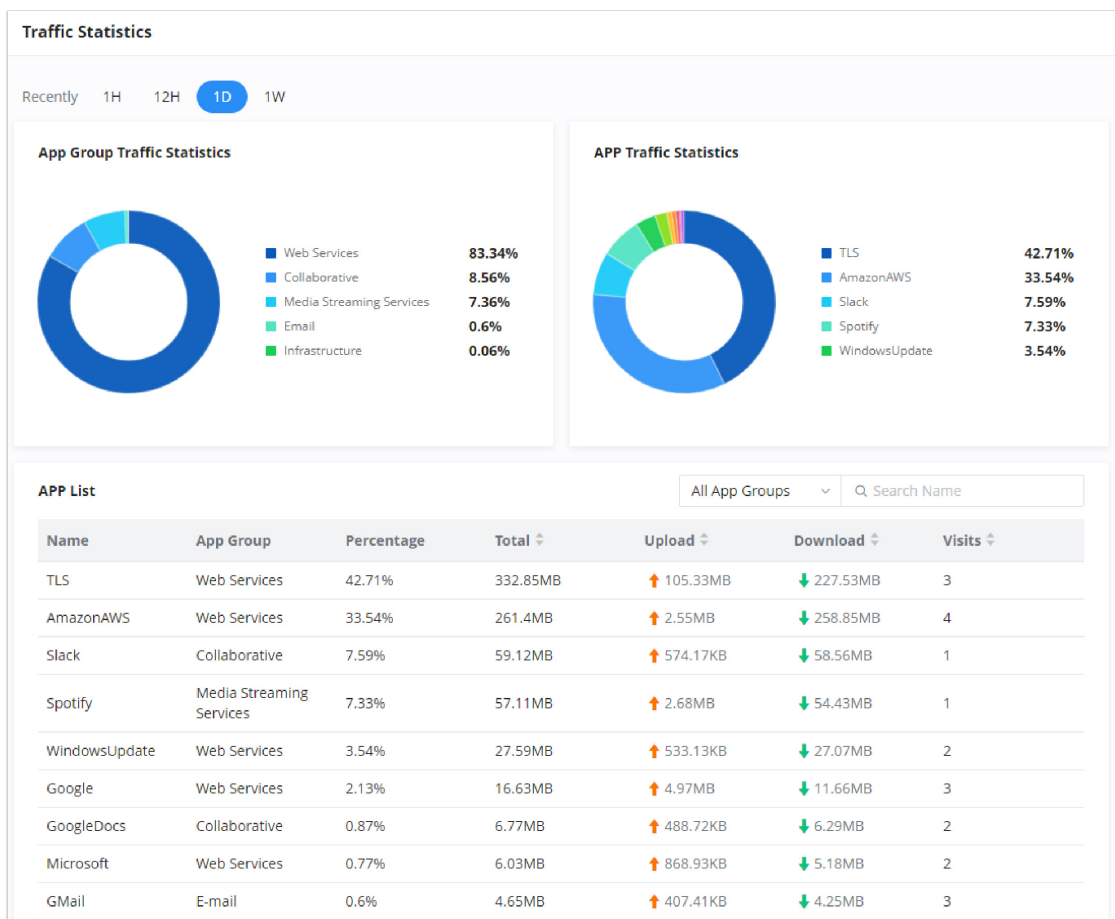
Basic Settings

Traffic Identification If enabled, the router will identify and analyze traffic on all clients. If disabled, the traffic identification history will be cleared.

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.



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.

QoS

[General Settings](#) [Class Rules](#) [Tag Outbound Traffic](#) [VoIP Settings](#) [APP QoS](#)

Port	Upload Bandwidth						Download Bandwidth				Operations
	Status	Maximum Upload Bandwidth	Class1(High)	Class2(Medium)	Class3(Low)	Class4(Lowest)	Status	Maximum Download Bandwidth	Class1(High)	Class2(Medium)	
WAN4	<input checked="" type="checkbox"/>	100Mbps	25%	25%	25%	25%	<input type="checkbox"/>	100Mbps	25%	25%	
WAN2	<input type="checkbox"/>	100Mbps	25%	25%	25%	25%	<input type="checkbox"/>	100Mbps	25%	25%	

QoS – General Settings

To define the rules of QoS for each port, click on edit button

QoS > **Edit General Settings**

ⓘ 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%.

Upload Bandwidth

Status

Maximum Upload Bandwidth Mbps Default 100Mbps, range is 1~1024. If empty, there is no limit

*Class1(High) (%) Range 1~97

*Class2(Medium) (%) Range 1~97

*Class3(Low) (%) Range 1~97

*Class4(Lowest) (%) Range 1~97

Download Bandwidth

Status

Maximum Download Bandwidth Mbps Default 100Mbps, range is 1~1024. If empty, there is no limit

*Class1(High) (%) Range 1~97

*Class2(Medium) (%) Range 1~97

*Class3(Low) (%) Range 1~97

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 Class1.
Class2 (Medium)	Specify the bandwidth percentage allocated for Class2.
Class1 (Low)	Specify the bandwidth percentage allocated for Class3.
Class1 (Lowest)	Specify the bandwidth percentage allocated for Class4.

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 Rule

***Name** 1~64 characters

Status

IP Family Any IPv4 IPv6

Protocol Type TCP/UDP TCP UDP

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 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.

DSCP

***Priority**

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

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	Enter a single port number, multiple port numbers, or a range of ports number. Example: - To enter a single port number, type the port number such as "3074". - To enter multiple port numbers, type the port numbers with a comma in between each port number, such as "3074, 5060, 10000". - To enter a range of port, enter the first port number in the range, then type a dash (-) and enter the last port number in the range. E.g., "10000-20000" Note: The valid range of port numbers that can be entered is 1-65535.
Destination IP Address	Enter the destination IP address/mask length. E.g., "192.168.122.0/24"

Destination Port	<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>
DSCP	Choose a DSCP value.
Priority	Select the class of priority.

Tag Outbound Traffic

When a specific tag is set for a certain class, the GWN700X will tag the outgoing traffic generated by the application which have been assigned to a class. To access **Tag Outbound Traffic**, please navigate to **Traffic Management** → **QoS** → **Tag Outbound Traffic**. To assign an application to a QoS class, please check the [APP QoS](#) section.

QoS

General Settings Class Rules Tag Outbound Traffic VoIP Settings APP QoS

Class1(High)

DSCP Tag

Class2(Medium)

DSCP Tag

Class3(Low)

DSCP Tag

Class4(Lowest)

DSCP Tag

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

Tag Outbound Traffic

Note

Please note that **Tag Outbound Traffic** will only take effects when QoS is enabled on the upload bandwidth of the WAN port.

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.

QoS

General Settings Class Rules Tag Outbound Traffic **VoIP Settings** APP QoS

VoIP Prioritization When enabled, it will give priority to distributing traffic for VoIP services and will not be restricted by other class bandwidth allocation

SIP UDP Port Default 5060

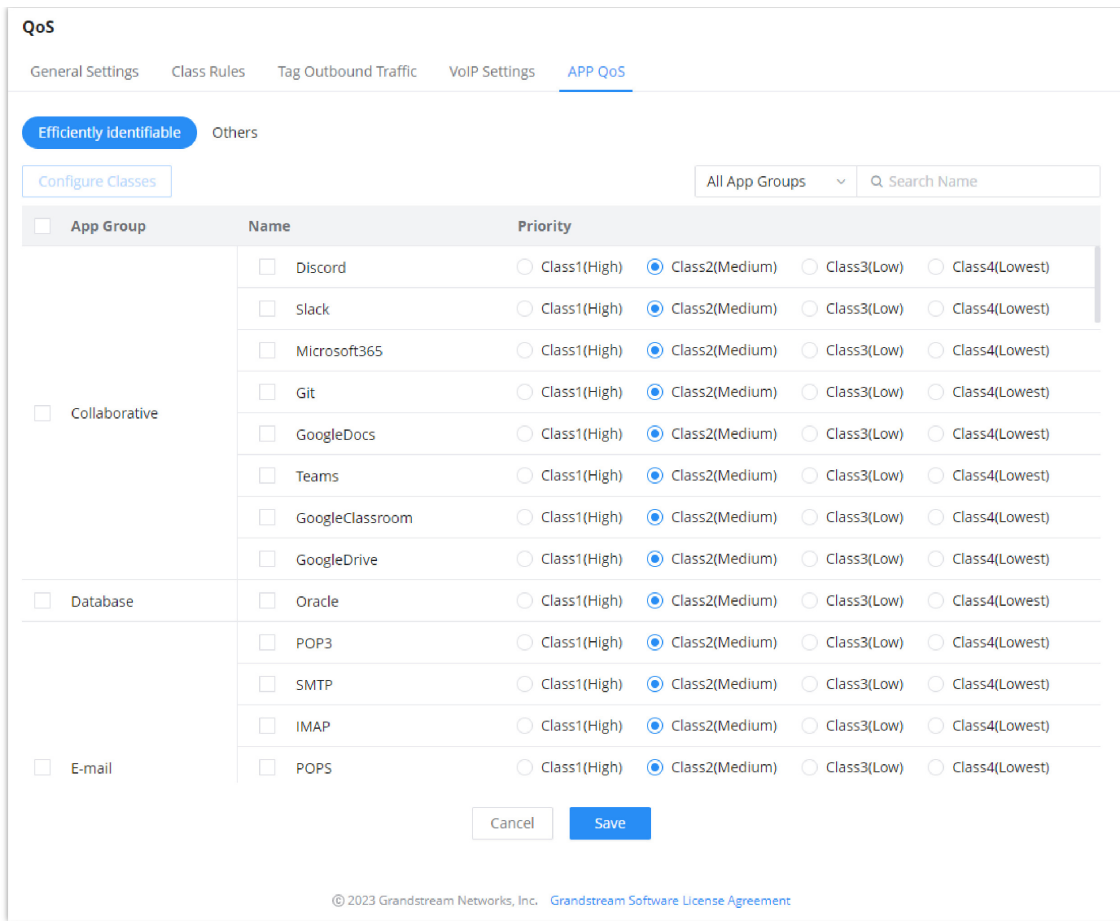
© 2023 Grandstream Networks, Inc. [Grandstream Software License Agreement](#)

VoIP Settings

APP QoS

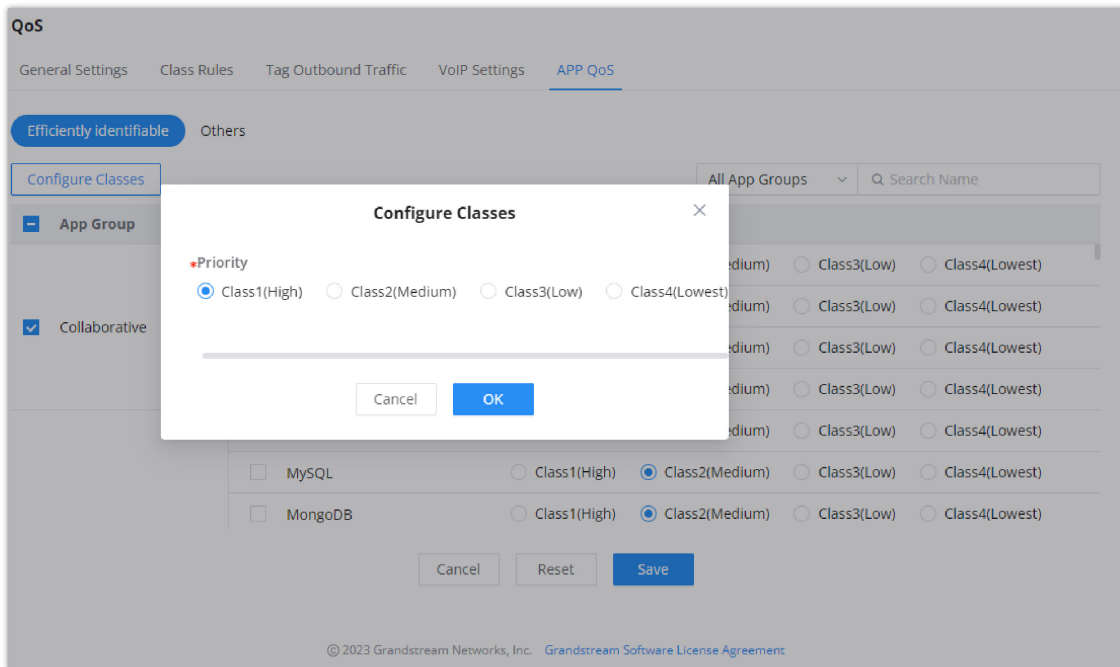
GWN700X routers can prioritize the traffic of each application individually. The priority level can be set in 4 classes, class 1 having the highest priority and class 4 having the lowest priority. To access APP QoS settings, please access the web GUI of the router then navigate to **Traffic Management**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

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



QoS

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



Apps QoS – Configure Classes

Note

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

AP MANAGEMENT

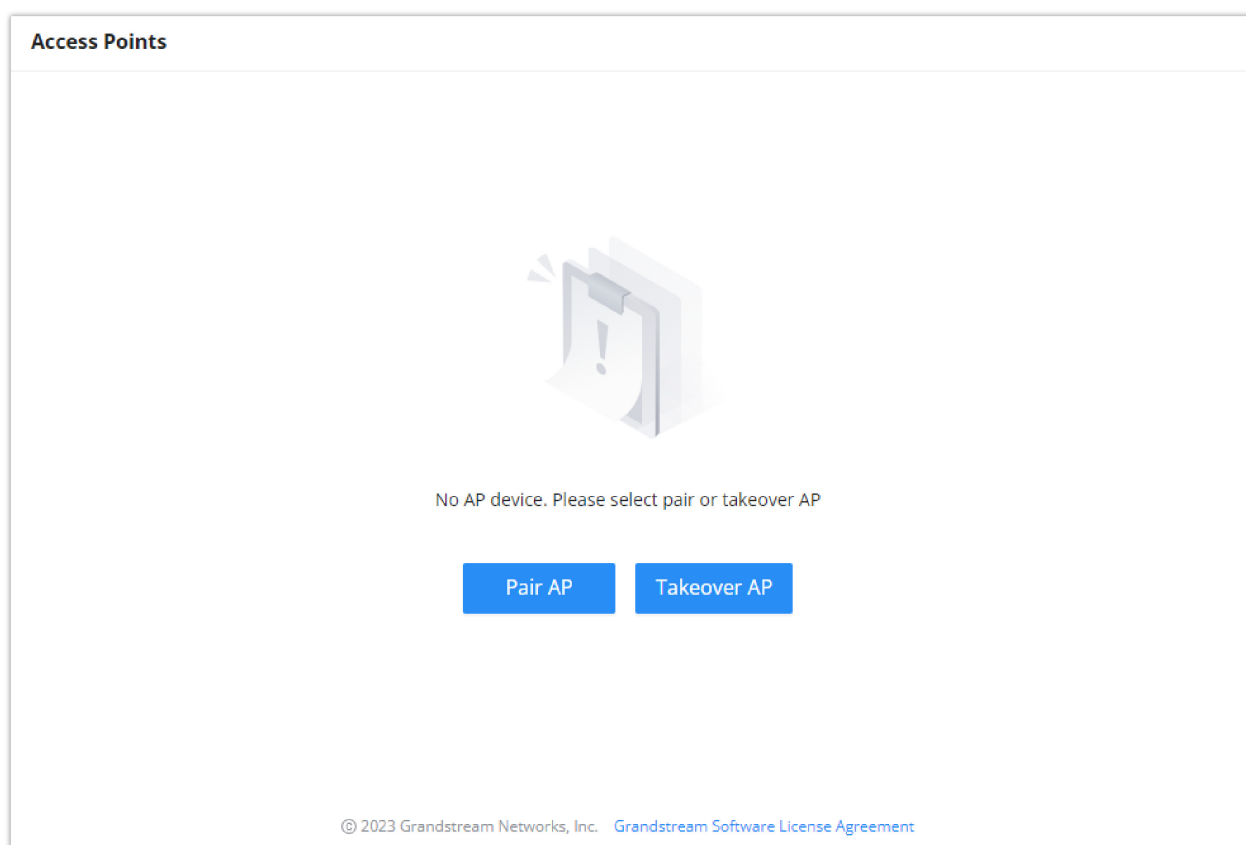
GWN700X routers come with an embedded controller for the GWN access points. The user can configure all the Wi-Fi related settings through the controller. When the APs are connected to the router, and they are paired with it, they will automatically inherit the configuration which has been set on the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



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 slaves 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.

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.

In order to add an SSID, the user should click on "Add" . Then the following page will appear:

SSIDs > Add SSID

Basic Information ^

Wi-Fi

*Name 1-32 characters

Associated VLAN

SSID Band Dual-Band 2.4G 5G

Access Security ^

Security Mode

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

Client Isolation

802.11w Disable Optional Required

Add SSID

Basic Information	
Wi-Fi	Toggle on/off the Wi-Fi SSID.
Name	Enter the name of the SSID.
Associated VLAN	When adding GWN7664LR or GWN7660LR to SSID, please enable the associated VLAN.
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

	<ul style="list-style-type: none"> • WPA2/WPA3 • WPA3 • WPA3-192
WPA Key Mode	<p>Choose the WPA key mode:</p> <ul style="list-style-type: none"> • PSK • 802.1x
WPA Encryption Type	<p>Choose the encryption type:</p> <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 • Radio • Internet • Gateway MAC
802.11w	<ul style="list-style-type: none"> • Disable • Optional • Required
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 and 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).
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.
Device Management	In this section, the user is able to add and remove the GWN access points which can broadcast the Wi-Fi SSID.

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 ⓘ

Off

Airtime Fairness



*Beacon Interval ⓘ

100

Default 100, range 40~500

Country / Region

United States

2.4G ^

Channel Width

20MHz 20&40MHz 40MHz

Channel

Auto Dynamically assigned by RRM

Radio Power ⓘ

High

Short Guard Interval ⓘ



Allow Legacy Devices (802.11b)



Minimum RSSI ⓘ



Minimum Rate ⓘ



Wi-Fi 5 Compatible Mode ⓘ



Cancel

Save

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.

○ 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

[Configure](#) [Topology](#)

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)** Default 5, range 1-5

***Wireless Cascade** Default 3, range 1-3

Interface

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

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.

○ **Topology:**

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

Mesh

[Configure](#) [Topology](#)

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

VPN (VIRTUAL PRIVATE NETWORK)

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, and OpenVPN® protocols, or configure an OpenVPN® server and generate certificates and keys for clients.

GWN700X routers support the following VPN functions:

- **PPTP:** Client and server.
- **IPSec:** Site-to-site and client-to-site.

- **OpenVPN®**: Client and server.
- **L2TP**: Client

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

OpenVPN®

OpenVPN® Server Configuration

To use the GWN700x as an OpenVPN® server, you will need to start creating a user account, OpenVPN® server certificates, and client certificates. Before generating server/client certificates, it is requested to generate first the Certificate Authority (CA), which will help to issue server/client certificates.

GWN700x certificates can be managed from **Web GUI** → **System Settings** → **Certificates**

Certificate > Add CA Certificate

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

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

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

Certificate Management

Generate Self-Issued Certificate Authority (CA)

A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entity's identity on the Internet. Electronic documents (a.k.a . digital certificates) are an essential part of secure communication and play an important part in the public key infrastructure (PKI).

To create a Certification Authority (CA), follow the below steps:

1. Navigate to "**Web GUI** → **System Settings** → **Certificate** → **CA Certificate**"
2. Click on button. A popup window will appear.
3. Enter the CA values including CN, Key Length, and Digest Algorithm ... depending on your needs.

Refer to the below figure showing an example of configuration and the table showing all available options with their respective descriptions.

Certificate > Add Certificate

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

* CA Certificate

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

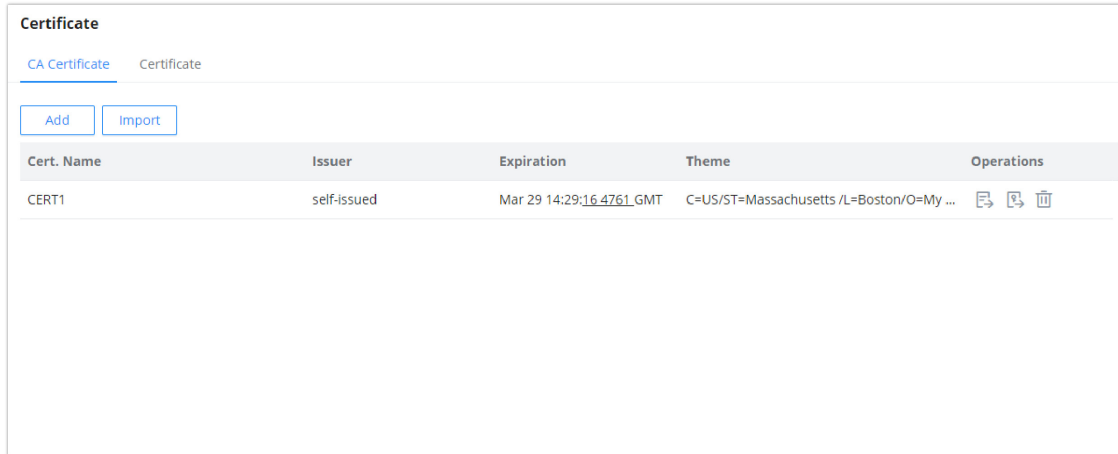
Add CA Certificate

Cert. Name	Enter the certificate's name.
Key Length	<p>Choose the key length for generating the CA certificate. The following values are available:</p> <ul style="list-style-type: none"> ● 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	<p>Select 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>Note: Hash is a one-way function, it cannot be decrypted back.</p>
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country / Region	Select a country from the dropdown list of countries. Example: "United States of America".
State / Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".

Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Click on  button after completing all the fields for the CA certificate.

Click on  button to export the CA to the local computer. The CA file has the extension ".crt".




CA Certificate

Generate Server/Client Certificates

Create both server and client certificates for encrypted communication between clients and GWN700x acting as an OpenVPN® server.

- o Creating Server Certificate

To create a server certificate, follow the below steps:

1. Navigate to **Web UI** → **System Settings** → **Certificates**
2. Click on  button. A popup window will appear.

Refer to the below figure showing an example of configuration and the table showing all available options with their respective descriptions.

Certificates > Add 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


Certificate Server


Cert. Name	Enter the certificate's name.
CA Certificate	Select a certificate authority
Certificate Type	Select the certificate type. <ul style="list-style-type: none"> • Server: Select this type for the certificates that will be used by a server. • Client: Select this type for the certificates that will be used by a client.
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. <p>Note: Hash is a one-way function, it cannot be decrypted back.</p>
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.

SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country / Region	Select a country from the dropdown list of countries. Example: "United States of America".
State / Province	Enter a state name or a province. Example: California
City	Enter a city name. Example: "San Diego"
Organization	Enter the organization's name. Example: "GS".
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

○ Click on  button after completing all the fields for the server certificate.

○ Click on  to export the server certificate file in ".crt" format.


○ Click on  to export the server key file in ".key" format.

○ Click on  to delete the server certificate if no longer needed.

- The server certificates (.crt and .key) will be used by the GWN70xx router when acting as a server.
- The server certificates (.crt and .key) can be exported and used on another OpenVPN® server
- Creating Client Certificate

To create a client certificate, follow the below steps:

1. Create Users

- Navigate to "Web UI → VPN → Remote Users"
- Click on  button. The following window will pop up.

Remote Users > Add User

*Name 1-64 characters

Status


Server Type PPTP IPsec OpenVPN®

Server Name

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

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

Client Subnet /

Add 

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

Enter User information based on the descriptions below

Name	Enter the name of the remote user.
Status	Toggle the account on or off.
Server Type	Choose OpenVPN as the type of the server.
Server Name	Select the server.
Username	Enter the username of the account.
Password	Enter the password of the account.
Client Subnet	Enter the client subnet and the subnet mask. The client will be assigned an IP address of this subnet.
Client Certificate	Select the client certificate.

2. Create Client Certificate

- Navigate to "**Web UI** → **System Settings** → **Certificates** → **Certificates**".
- Click on [+ Add](#) button. The following window will pop up.

Enter client certificate information based on the below descriptions.




Add Certificate

*Cert. Name	<input type="text" value="ClientCertificate"/>
*CA Certificate	<input type="text" value="Certificate"/>
Certificate Type	<input type="text" value="Client"/>
*Username	<input type="text" value="User 1"/>
Key Length	<input type="text" value="2048"/>
Digest Algorithm	<input type="text" value="SHA256"/>
*Expiration (D) ⓘ	<input type="text" value="120"/>
Country / Region	<input type="text" value="United States of America"/>
*State / Province	<input type="text" value="Newyork"/>
*City	<input type="text" value="Newyork"/>
*Organization	<input type="text" value="GS"/>
*Organizational Unit	<input type="text" value="GS"/>
*Email	<input type="text" value="Grandstream@gmail.com"/>

Client Certificate

Cert. Name	Enter the common name for the server certificate. Note: It could be any name to identify this certificate. Example: "ClientCertificate".
CA Certificate	Select the CA certificate previously generated from the drop-down list. Example: "CA Test".
Certificate Type	Choose the certificate type from the drop-down list. It can be either a client or a server certificate. Choose " Client " to generate a Client certificate.
Username	Select created user to generate his certificate.
Key Length	Choose the key length for generating the CA certificate. The following values are available: 512: 512-bit keys are not secure and it's better to avoid this option. 1024: 1024-bit keys are no longer sufficient to protect against attacks. 2048: 2048-bit keys are a good minimum. (Recommended). 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: SHA1: This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. Note: Hash is a one-way function, it cannot be decrypted back.
Expiration (D)	Enter the validity date for the CA certificate in days. The valid range is 1~999999.
Country / Region	Select a country code from the dropdown list. Example: "MA".
State / Province	Enter a state name or province. Example: "Casablanca".
City	Enter a city name. Example: "Casablanca".
Organization	Enter the organization's name. Example: "GS".
Organizational Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "user@grandstream.com"

Client Certificate

- Click on  to export the server certificate file in ".crt" format.
- Click on  to export the server key file in ".key" format.
- Click on  to delete the server certificate if no long
 1. Client certificates generated from the GWN70xx need to be uploaded to the clients.
 2. For security improvement, each client needs to have his username and certificate, this way even if a user is compromised, other users will not be affected.

Create OpenVPN® Server

Once client and server certificates are successfully created, you can create a new server, so that clients can be connected to it, by navigating under **Web UI** → **VPN** → **OpenVPN®** → **OpenVPN® Server**

To create a new VPN server, follow the below steps:

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:

OpenVPN® Service	Click on "ON" to enable the OpenVPN Server.
Name	Enter a name for the OpenVPN® server.
Server Mode	<p>Choose the server mode the OpenVPN® server will operate with. 4 modes are available:</p> <p>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).</p> <p>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).</p> <p>SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.</p> <p>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).</p>

Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. <i>The default protocol is UDP.</i>
Interface	Select the WAN port to be used by the OpenVPN® Server.
Destination	Select the WANs, VLANs and VPNs (clients) destinations that will be using this OpenVPN® Server.
Local Port	Configure the listening port for OpenVPN® server. <i>The default value is 1194.</i>
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
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	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.
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	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.

- **Create the remote user credentials:**


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

OpenVPN® Client Configuration

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

1. Upload client certificate created from an OpenVPN® server to GWN700x.
2. Create client/server certificates on GWN700x and upload the server certificate to the OpenVPN® server.

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

Click on  button. The following window will pop up.

The screenshot shows the configuration interface for an OpenVPN Client. It contains various settings such as Name, Status, Protocol (UDP/TCP), Interface, Destination, Local Port, Remote OpenVPN Server, OpenVPN Server Port, Authentication Mode, Encryption Algorithm, Digest Algorithm, TLS Identity Authentication, Routes (IP Address and Mask Length), Deny Server Push Routes, IP Masquerading, LZO Compression, Allow Peer to Change IP, CA Certificates, Client Certificate, and Client Private Key Password. There are 'Cancel' and 'Save' buttons at the bottom.

OpenVPN® Client

Click  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 <p>Note: The default protocol is UDP.</p>
Interface	Select the WAN port to be used by the OpenVPN® client.
Destination	Select the WANs, VLANs and VPNs (clients) destinations that will be used by this OpenVPN® client.
Local Port	Configures the client port for OpenVPN®.The port between the OpenVPN® client and the client or between the client and the server should not be the same.
Remote OpenVPN® Server	Configures the remote OpenVPN® server. Both IP address and domain name are supported.
OpenVPN® Server Port	Configures the remote OpenVPN® server port
Authentication Mode	Choose the authentication mode. <ul style="list-style-type: none"> • SSL • User Authentication • SSL + User Authentication

	<ul style="list-style-type: none"> • 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	Enable TLS identity authentication direction.
TLS Identity Authentication Direction	<p>Select the identity authentication direction.</p> <ul style="list-style-type: none"> • Server: Identity authentication is performed on the server side. • Client: Identity authentication is performed on the client side. • Both: Identity authentication is performed on both sides.
TLS Pre-Shared Key	Enter the TLS pre-shared key.
Routes	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
Deny Server Push Routes	If enabled, client will ignore routes pushed by the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.

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

L2TP Configuration

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

L2TP Client Configuration

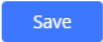
To configure the L2TP client on the GWN700x router, navigate under “**VPN → VPN Clients**” and set the followings:

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.

Click  after completing all the fields.

+ Add

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

L2TP Client

PPTP Configuration

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.

Server Configuration

*Name	<input type="text"/>	1~64 characters
Status	<input type="checkbox"/>	
*Server Local Address	<input type="text"/>	
*Client Start Address	<input type="text"/>	
*Client End Address	<input type="text"/>	
MPPE Encryption	<input type="checkbox"/>	
*Interface	<input type="text" value="Please Select Interface"/>	▼
*Destination	<input type="text" value="Please Select Destination"/>	▼
LCP Echo Interval (sec) ⓘ	<input type="text" value="20"/>	Range 1~86400
LCP Echo Failure Threshold ⓘ	<input type="text" value="3"/>	Range 1~86400
LCP Echo Adaptive ⓘ	<input type="checkbox"/>	
Debug	<input type="checkbox"/>	
*MTU	<input type="text" value="1430"/>	Default 1430, range 1280~1500
*MRU	<input type="text" value="1430"/>	Default 1430, range 1280~1500
Preferred DNS Server	<input type="text"/>	
Alternative DNS Server	<input type="text"/>	
	<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

PPTP Sever

o **Create the remote user credentials:**

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

Client Configuration

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

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

*Name 1~64 characters

Status

*Server Address Enter an IPv4 address or domain name

*Username 1~64 characters

*Password 1~64 characters

MPPE Encryption

Interface

Destination

IP Masquerading

*Maximum Transmission Unit (MTU) Default: 1430, range 576~1450

Remote Subnet / -







Add +

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. <i>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.</i>
Destination	Choose to which destination group or WAN to allow traffic from the VPN, this will generate automatically a forwarding rule under the menu Firewall → Traffic Rules → Forward .
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
Remote Subnet	Configures the remote subnet for the VPN. The format should be "IP/Mask" where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32.

example: 192.168.5.0/24

Click [Save](#) after completing all the fields.

Name	Status	Connection Type	Interface	Server Address	Operations
L2TP	Dialing	L2TP	WAN	testvpn12tp.vpnazure.net	  
PPTP	Dialing	PPTP	WAN	euro14.vpnbook.com	  

PPTP Client

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 Configuration

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

Add VPN Client – IPsec

○ **Phase 1**

Phase 1 ^

Negotiation Mode	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
*Pre-shared Key ⓘ	<input type="text"/> 1-64 characters
Encryption Algorithm	<input type="text" value="AES-256"/> ▼
Hash Algorithm	<input type="text" value="SHA2-256"/> ▼
DH Group	<input type="text" value="Group14"/> ▼
Local ID ⓘ	<input type="text"/>
Remote ID ⓘ	<input type="text"/>
Reconnect ⓘ	<input checked="" type="checkbox"/>
*Number of Reconnect ⓘ	<input type="text" value="10"/> <small>The default value is 10, and the valid range is 0-10. Value 0 means that it has been trying to negotiate connection.</small>
DPD ⓘ	<input checked="" type="checkbox"/>
*DPD Delay Time (sec)	<input type="text" value="30"/> <small>Default 30, range 10-900</small>
*DPD Idle Time (sec)	<input type="text" value="120"/> <small>Default 120, range 10-900</small>
DPD Action ⓘ	<input checked="" type="radio"/> Hold <input type="radio"/> Clear <input type="radio"/> Restart

Add VPN Client – Phase 1

○ **Phase 2**

Phase 2 ^

*Local Subnet / -
Add +

*Local Source IP Address

*Remote Subnet / -
Add +

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

Security Protocol ESP

ESP Encryption Algorithm v

ESP Hash Algorithm v

Encapsulation Mode Tunnel Mode

PFS Group v

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.

- o **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 Configuration

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:

IPSec > Add Client-to-Site

*Name 1-64 characters

Status

Interface v

*Pre-shared Key 1-64 characters, only support input English, numbers, characters @ ! \$ % -

*Encryption Algorithm v

*Hash Algorithm v

*DH Group v

Branch Office IPSec Configuration

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

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

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

Client Subnet /

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.

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.

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.

The screenshot shows the 'DDNS > Add DDNS' configuration page. It contains the following fields and options:

- Service Provider:** A dropdown menu with 'dyndns.org' selected.
- Status:** A toggle switch that is currently turned on.
- *Username:** A text input field with a '1-32 characters' character limit.
- *Password:** A text input field with a '1-32 characters' character limit and a password icon.
- *Domain:** A text input field with a note: 'Please go to dyndns.org to register to get the corresponding username, password and domain'.
- Interface:** A dropdown menu with 'WAN4 (WAN)' selected.

DDNS Page

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

DDNS

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 > Add Port Forwarding

*Name 1~64 characters

Status

Protocol Type TCP/UDP TCP UDP

Interface

Source IP Address

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

Destination Group

*Destination IP Address

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

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

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.

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**.

Add DMZ ✕

***DMZ Name**
1~64 characters

Status

Enabling the DMZ host function can fully expose the designated device to the Internet.

***Source Group**

Destination Group

***DMZ Hostname IP Address**

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

UPnP

Once enabled UPnP (Universal Plug and Play), computers in the LAN can request the router to do port forwarding automatically.

Interface

Destination Group

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

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 Port Forward

[Refresh](#)

Application Description	IP Address	External Port	Internal Port	Protocol Type
 No UPnP device				

UPnP – Open Ports

TURN Service (Beta)

TURN stands for Traversal Using Relays 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

Status

*Ports

*TURN Server Port Default 3478, range 1024-65535

*Username and Password

Username Password

[Add +](#)

*TURN Forwarding Port - Default 60000-60500, range 6000-65535

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

TURN Service

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.

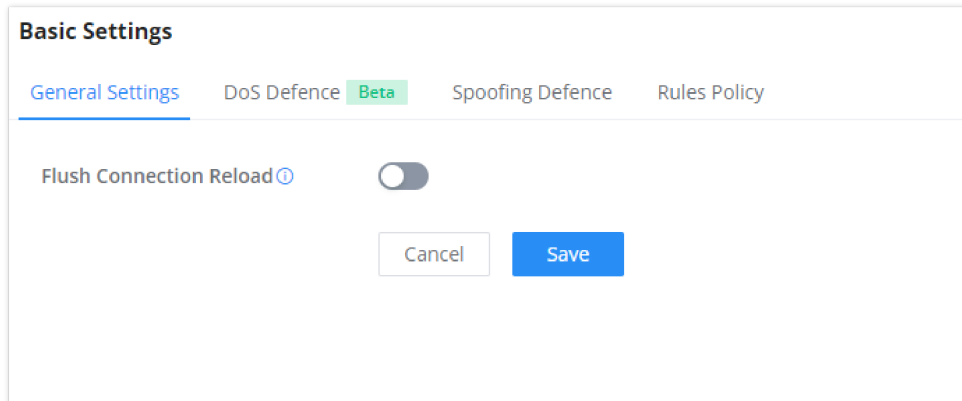
Basic Settings

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 Defence

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.

Note

Please note that this security module is currently in beta testing phase.

DoS Defence	<input checked="" type="checkbox"/>	
Log	<input checked="" type="checkbox"/>	
TCP SYN Flood Attack Defense	<input type="checkbox"/>	
UDP Flood Attack Defense	<input type="checkbox"/>	
ICMP Flood Attack Defense	<input checked="" type="checkbox"/>	
*ICMP Flood Packet Threshold (packets/s) ⓘ	<input type="text" value="1"/>	Default 250, range 1~10000
*ICMP Flood Timeout (sec) ⓘ	<input type="text" value="10"/>	Default 10, range 1~65535
ACK Flood Attack Defense	<input type="checkbox"/>	
Port Scan Detection	<input type="checkbox"/>	
Block IP Options	<input type="checkbox"/>	
Block TCP Flag Scan	<input type="checkbox"/>	
Block Land Attack	<input type="checkbox"/>	
Block Smurf	<input type="checkbox"/>	
Block Ping of Death	<input type="checkbox"/>	
Block Trace Route	<input type="checkbox"/>	
Block ICMP Fragment	<input type="checkbox"/>	
Block SYN Fragment	<input type="checkbox"/>	
Block Unassigned Protocol Numbers ⓘ	<input type="checkbox"/>	
Block Fraggle Attack	<input type="checkbox"/>	
		<input type="button" value="Cancel"/> <input type="button" value="Save"/>

DoS Defence

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	When this option is enabled, the router will take counter measures to the ICMP Flood Attack.

	<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	<p>When this option is enabled, the router will ignore any IP packets with Options field.</p>
Block TCP Flag Scan	<p>When this option is enabled, the router will ignore any packets with unexpected information in the TCP flags.</p>
Block Land Attack	<p>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.</p>
Block Smurf	<p>When this option is enabled, the router will drop any ICMP echo requests.</p>
Block Ping of Death	<p>When this option is enabled, the router will drop any abnormal or corrupted ping packets.</p>
Block Traceroute	<p>When this option is enabled, the router will not allow the traceroute requests initiated from the WAN side.</p>
Block ICMP Fragment	<p>When this option is enabled, the router will drop the ICMP packets which are fragmented.</p>
Block SYN Fragment	<p>When this option is enabled, the router will drop the SYN packets which are fragmented.</p>
Block Unassigned Protocol Numbers	<p>If enabled, the device will reject IP packets receiving IP protocol number greater than 133.</p>
Block Fraggle Attack	<p>If enabled, the router will drop any UDP broadcast packets initiate from the WAN side.</p>

Spoofing Defence

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

Spoofing Defence

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 1~999999, 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 allows users to filter (block) 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

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.

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".

Content Security > **Add APP Filtering**

Basic Information

*Name 1~64 characters

Description 0~128 characters

Filtered Application

All Efficiently identifiable Others

Collaborative

Discord Slack Github Git

Teams GitLab

Database

PostgreSQL MySQL MongoDB MsSQL-TDS

Oracle Redis Cassandra

E-mail

POP3 SMTP IMAP Outlook

POPS SMTPS IMAPS GMail

File Transfer

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	<input type="text"/>	1~64 characters
Description	<input type="text"/>	0~128 characters
*Filtered URL 	<input type="text" value="Please Enter"/>	
		Add 
	<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

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.

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  .
- 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												
											All Source Groups	
<input type="checkbox"/>	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_Allow...	<input checked="" type="checkbox"/>	IPv4	UDP	WAN2 (WAN)	-	-	-	-	68	Accept	
<input type="checkbox"/>	WAN2_Allow...	<input checked="" type="checkbox"/>	IPv4	ICMP	WAN2 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/>	WAN2_Allow-I...	<input checked="" type="checkbox"/>	IPv4	IGMP	WAN2 (WAN)	-	-	-	-	-	Accept	
<input type="checkbox"/>	WAN2_Allow...	<input checked="" type="checkbox"/>	IPv6	UDP	WAN2 (WAN)	-	fe80::/10	-	fe80::/10	546	Accept	
<input type="checkbox"/>	WAN2_Allow...	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN2 (WAN)	-	fe80::/10	-	-	-	Accept	
<input type="checkbox"/>	WAN2_Allow-I...	<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	

Traffic Rules – Inbound Rules

Name	Enter the name of the inbound rule.
Status	Toggle on/off the status of the inbound 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 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.
Advanced Settings	
Content Security	Enable content security, once enabled the user can customize security features which are described below.
Content Security Action	<p>If set to "Accept", the external devices are allowed to access the router.</p> <p>If set to "Deny", the access of the external devices is denied and the result is returned</p>

	If set to "Drop", the access request of the external device 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.

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

	<ul style="list-style-type: none"> • 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	<p>If set to "Accept", the router is allowed to access the external network.</p> <p>If set to "Deny", the access to external network is denied and the result is returned.</p> <p>If set to "Drop", the request of access to external network will be directly dropped.</p>
DNS Filtering	Specify the DNS filtering rule.
APP Filtering	Specify the app filtering rule.
URL Filtering	Specify the URL filtering rule.

Forwarding Rules

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

*Name	<input type="text"/>	1~64 characters
Status	<input checked="" type="checkbox"/>	
IP Family	<input checked="" type="radio"/> Any <input type="radio"/> IPv4 <input type="radio"/> IPv6	
Protocol Type	<input type="text" value="UDP"/>	
*Source Group ⓘ	<input type="text" value="Default (VLAN)"/>	
Source MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	
Source IP Address	<input type="text"/>	Enter the IP address/mask length, such as "192.168.122.0/24"
Source Port ⓘ	<input type="text"/>	The valid range is 1-65535. You can enter a single port or a port range.
*Destination Group	<input type="text" value="Please Select Destination Group"/>	
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.
Action ⓘ	<input checked="" type="radio"/> Accept <input type="radio"/> Deny <input type="radio"/> 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	<input type="checkbox"/>	
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

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

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.

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

Advanced NAT – DNAT

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

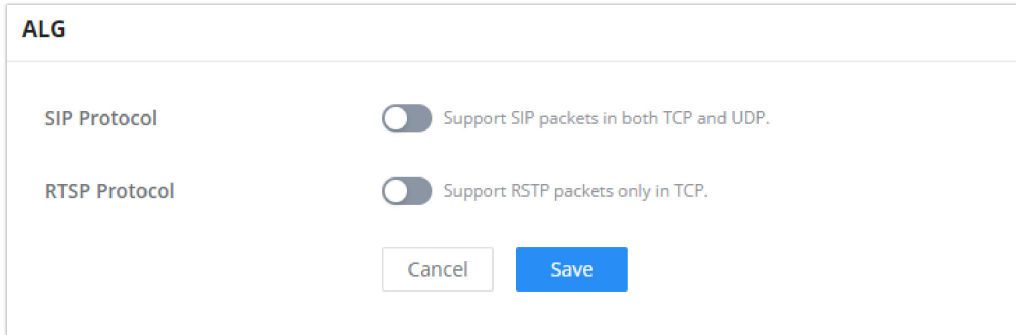
Name	Specify a name for the DNAT entry
IP Family	Select the IP version, three options are available: IPv4, IPv6 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
Source Group	Select a WAN interface or a LAN group for Source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

DNAT

ALG

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

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



ALG

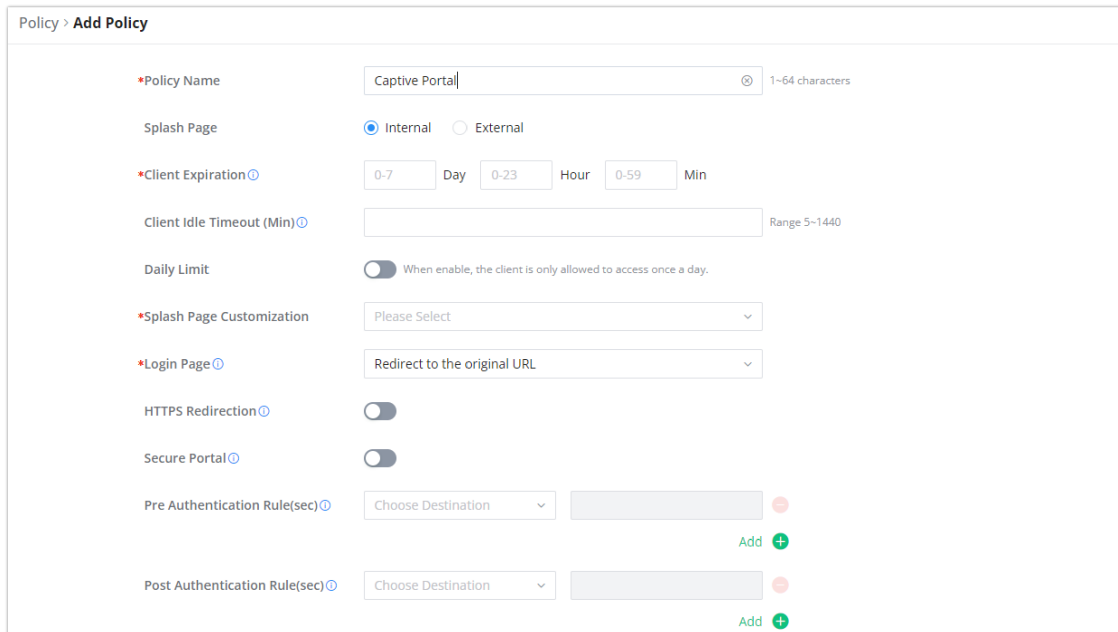
CAPTIVE PORTAL

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


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

Policy List

Users can customize a portal policy on this page.



Policy page

Click on  to add a captive portal policy.

Click on to  edit a captive portal policy.

Click on to  delete a captive portal policy.

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

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

Splash Page

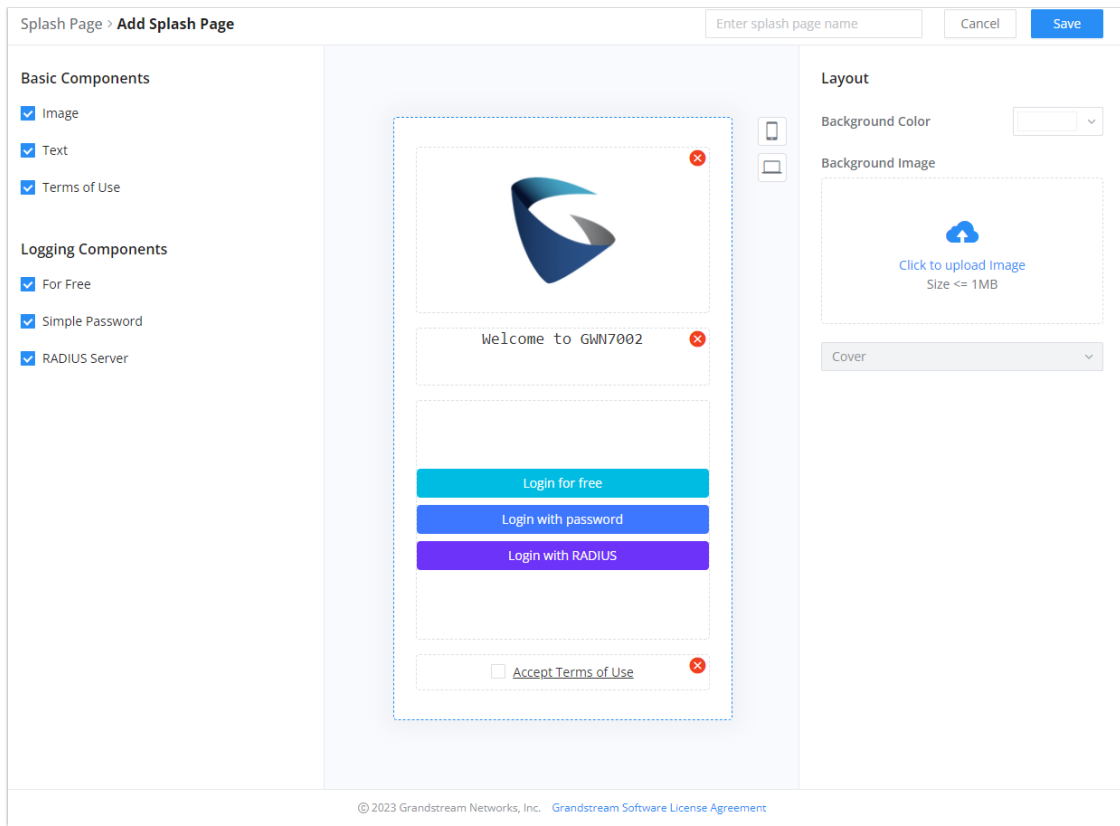
The splash page allows users with an easy-to-configure menu to generate a customized splash page that will be displayed to the users when trying to connect to the Wi-Fi.

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.

Users can set the following:

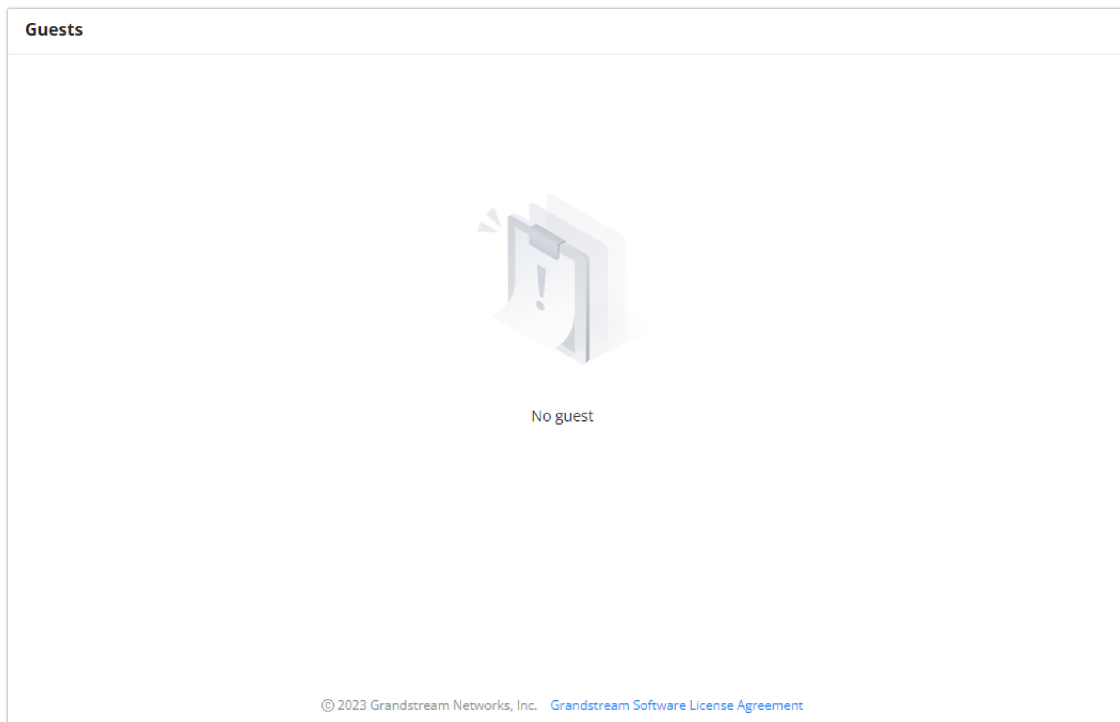
- **Authentication type:** Add one or more ways from the supported authentication methods (Simple Password, Radius Server, For Free).
- **Set up a picture (company logo)** to be displayed on the splash page.
- **Customize** the layout of the page and background colors.
- **Customize the Terms of use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




Splash Page

Guest

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



Captive Portal – Guest Page

○ Click on  delete button to cancel the authentication, the client must re-authenticate to use the network again.

○ Users can press  button to customize items to display on the page. The following items are supported:

<input checked="" type="checkbox"/>	MAC Address
<input checked="" type="checkbox"/>	HostName
<input checked="" type="checkbox"/>	Associated Device
<input checked="" type="checkbox"/>	SSID
<input checked="" type="checkbox"/>	Used Traffic
<input checked="" type="checkbox"/>	Authentication Type
<input checked="" type="checkbox"/>	Logging Time
<input checked="" type="checkbox"/>	IP Address
<input checked="" type="checkbox"/>	Expire Time
<input checked="" type="checkbox"/>	Status

Captive Portal – Guest Page – Select Items

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.

Blocklist > Add Blocklist

*Name 1~64 characters

Available Devices [Add Manually](#)

<input type="checkbox"/>	Device Name	MAC Address
 No device		

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

Blocklist Page

o **Add Devices Manually:**

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

Blocklist > Add Blocklist

*Name 1~64 characters

Available Devices [Add Manually](#)

Device MAC Address : : : : :

[Add MAC Address](#)

© 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

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 GWN76XX 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)

86400

Default [86400](#)

Connection Request Username



Connection Request Password



Connection Request Port

7547

Default 7547, range 1~[65535](#)

CPE Cert File

CPE Cert Key

Cancel

Save

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

TR-069 page

TR-069	Enable/disable TR-069
ACS URL	Enter the FQDN or the IP address of the ACS server.
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.
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.
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.
--------------	--

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

SNMPv1, SNMPv2c

*Community String 1~512 characters

SNMPv3

*Username 1~128 characters

Authentication Mode MD5 SHA

*Authentication Key 8~32 characters

Encryption Mode DES AES128

*Encryption Key 8~32 characters

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

SNMP

To configure SNMPv2, please refer to the table below:

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

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.

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 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 & Restore

Backup

Export the current configuration file of the router to your computer or connected USB device. Once you need to restore this, you can directly import the file.

[Export](#)

Restore

The router can be restored according to the imported configuration file. If restore failed and the device cannot be used, please press and hold the Reset button on the back of the router for 5 seconds to restore the factory status.

[Import](#)

Factory Reset Configuration

After factory reset, all router's configurations will be reset to the factory settings. Please do it with caution! It is recommended that you backup the current configurations before factory reset.

[Factory Reset](#)

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.

System Diagnostics

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

*Tool: IPv4 Ping

*Target IP Address / Hostname: 1.1.1.1

Interface: Auto

Start

Diagnostic Result

```

PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: seq=0 ttl=56 time=5.959 ms
64 bytes from 1.1.1.1: seq=1 ttl=56 time=5.693 ms
64 bytes from 1.1.1.1: seq=2 ttl=56 time=5.334 ms
64 bytes from 1.1.1.1: seq=3 ttl=56 time=5.597 ms
64 bytes from 1.1.1.1: seq=4 ttl=56 time=5.773 ms

--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.334/5.671/5.959 ms

```

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.

System Diagnostics

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

Refresh

File Name	Last Modified	Operations
 <p>No Core File</p>		

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

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.

System Diagnostics

[Ping / Traceroute](#) [Core File](#) [Capture](#) [External Syslog](#) [ARP Cache Table](#) [Link Tracing Table](#) [Network Diagnostics](#) [PoE Diagnostics](#)

Capture Duration (min)	<input type="text" value="10"/>
Interface	<input type="text" value="WAN2 (WAN)"/>
Capture Rule	<input checked="" type="radio"/> Default Rules <input type="radio"/> Custom Rules
Protocol	<input type="text" value="Please Select Protocol"/>
MAC Address	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>
IP Address	<input type="text"/>

[Start Capturing](#)

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

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.

System Diagnostics

[Ping / Traceroute](#)
[Core File](#)
[Capture](#)
[External Syslog](#)
[ARP Cache Table](#)
[Link Tracing Table](#)
[Network Diagnostics](#)
[PoE Diagnostics](#)

Syslog Server Address:

Syslog Level:

Protocol: UDP TCP

Target Devices:

- Select All
- C0:74:AD:BF:AF:50
GWN7002

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

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		-	WAN2 (WAN)
192.168.5.154		-	WAN2 (WAN)
192.168.5.112		-	WAN2 (WAN)
192.168.5.75		-	WAN2 (WAN)
192.168.5.147		-	WAN2 (WAN)
192.168.5.1		-	WAN2 (WAN)
192.168.5.117		-	WAN2 (WAN)
192.168.80.2		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	Please Enter Sou...	Please Enter Des...	All Protocols	Please Enter Sou...	Please Enter Des...	
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] 192.168.5.99[0] ← 8.8.8.8[0]	→ 1/84 ← 1/84
IPv4	ICMP	19	255	-	192.168.5.99[8] → 8.8.8.8[0] 192.168.5.99[0] ← 8.8.8.8[0]	→ 1/84 ← 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] 192.168.5.99[0] ← 8.8.8.8[0]	→ 1/84 ← 1/84
IPv4	TCP	299	2	ESTABLISHED	192.168.5.147[57760] ⇄ 192.168.5.99[443]	→ 11/1331 ← 21/1302
IPv4	TCP	296	2	ESTABLISHED	192.168.5.99[56810] ⇄ 44.230.213.222[443]	→ 15/920 ← 11/791

Total: 8 ▾

Link Tracing Table

Network Diagnostics

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


System Diagnostics

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

Interface:

IP Family: Any IPv4 IPv6

Diagnostic Result



No diagnostic record

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

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.

System Diagnostics

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

Diagnostic Result

Common information:

Input Power Supply Type	:PoE+
PSE Input Voltage	:51.90 V
PSE Input Voltage Status	:Higher Than 65V
PMAx Power	:12.80 W
Over Load Power Status	:Normal
Junction Temperature	:46.0 °C
Over Temperature Status	:Normal
Port5 MOSFET Status	:Normal
Port6 MOSFET Status	:Normal

Port5 information:

Port5 Operation Mode	:Auto Mode
Port5 Voltage	:51.90 V
Port5 Current	:0.0 mA
Port5 Power	:0.0 mW
Port5 Current Limit Status	:Normal
Port5 Threshold Over Current Timeout	:Normal
Port5 Output Power Status	:Wrong

PoE Diagnostics

Upgrade

Alerts & Notifications

The E-mail Notification page allows the administrator to select a predefined set of system events and to send notifications upon the change of the set events,

 Please select the alerts to be notified by e-mail

- Memory Usage
- Temperature
- Throughput
- Admin Password Modify
- Upgrade
- AP Online & Offline

Cancel

Save

E-mail Notification Events

SYSTEM SETTINGS

Basic Settings

Manager 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

Security Management

[Login Password](#) [Web Service](#) [SSH Service](#) [Passwordless Remote Access](#)

*Old Password

*New password 8-32 characters, must include any two of numbers, letters and special characters

*Confirm new password

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

Security Management

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.

*HTTPS Port ⓘ Default 443,655, excluding 10,14,80,223,224,8000,8001 range 1~ 35, 80,8443, 4

Web WAN Port Access

Web Service

SSH Service

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

Enable SSH

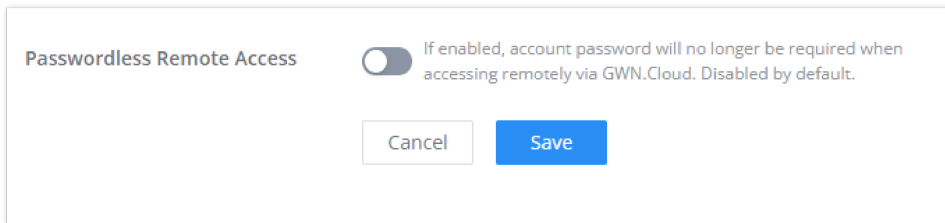
SSH Remote Access

*SSH Remote Access Password

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.

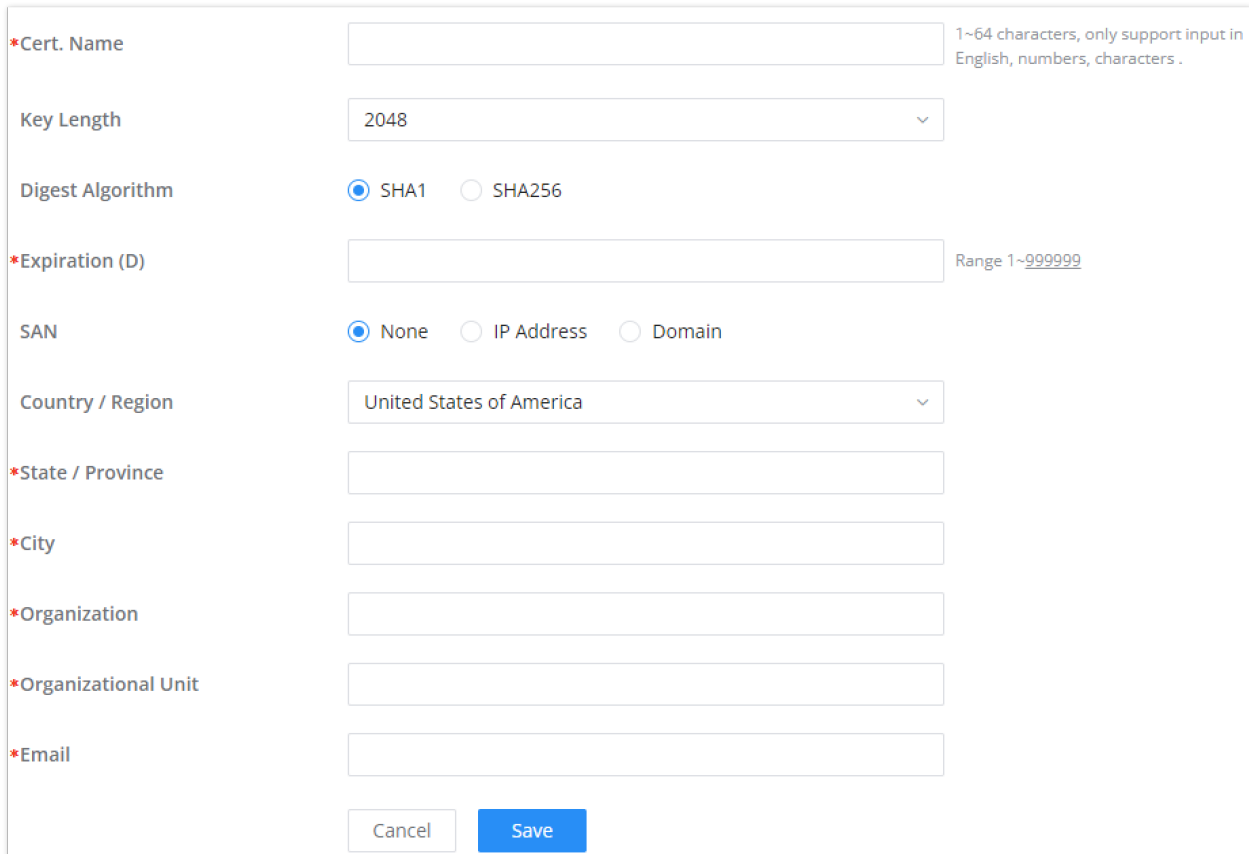


Passwordless Remote Access

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.



CA Certificate

Certificates

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	<input type="text"/>	1~64 characters, only support input in English, numbers, characters .
*CA Certificates	<input type="text" value="CERT1"/>	
Certificate Type	<input type="text" value="Server"/>	
Key Length	<input type="text" value="2048"/>	
Digest Algorithm	<input checked="" type="radio"/> SHA1 <input type="radio"/> SHA256	
*Expiration (D)	<input type="text"/>	Range 1~999999
SAN	<input checked="" type="radio"/> None <input type="radio"/> IP Address <input type="radio"/> Domain	
Country / Region	<input type="text" value="United States of America"/>	
*State / Province	<input type="text"/>	
*City	<input type="text"/>	
*Organization	<input type="text"/>	
*Organizational Unit	<input type="text"/>	
*Email	<input type="text"/>	
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Certificate

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

Support inserting USB device. You can use the data in USB storage device by accessing shared directories.



No USB device detected

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

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 1.0.3.4

- Added new feature of TURN server [[TURN Service](#)]
- Added new feature of 2.5G SFP module support [[Port Configuration](#)]

Firmware Version 1.0.1.6

- This is the initial release.