

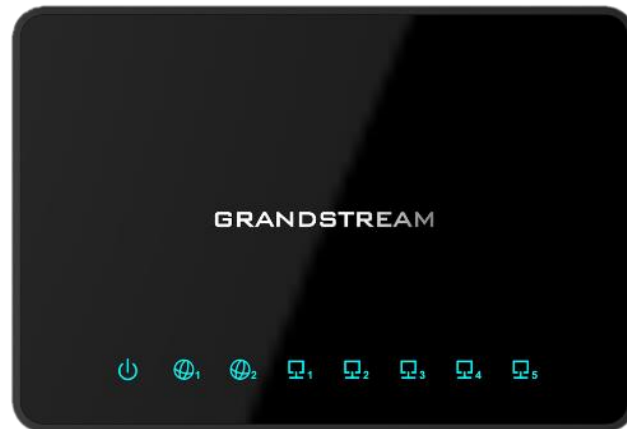
# Grandstream Networks, Inc.

---

GWN7000

Enterprise Multi-WAN Gigabit VPN Router

User Manual



## **COPYRIGHT**

©2016 Grandstream Networks, Inc. <http://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this guide is available for download here:

<http://www.grandstream.com/support>

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.

## **OPEN SOURCE LICENSES**

GWN7000 firmware contains third-party open source software. Grandstream Open source licenses can be downloaded from Grandstream web site from [here](#)

## **CAUTION**

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

## **WARNING**

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



# Table of Contents

<b>DOCUMENT PURPOSE .....</b>	<b>9</b>
<b>CHANGE LOG .....</b>	<b>10</b>
Firmware Version 1.0.2.71 .....	10
<b>WELCOME .....</b>	<b>11</b>
<b>PRODUCT OVERVIEW .....</b>	<b>12</b>
Technical Specifications .....	12
<b>INSTALLATION .....</b>	<b>14</b>
Equipment Packaging .....	14
Connect your GWN7000 .....	14
Safety Compliances .....	15
Warranty .....	15
<b>GETTING STARTED .....</b>	<b>16</b>
LED Indicators .....	16
Use the WEB GUI .....	16
<i>Access WEB GUI .....</i>	<i>16</i>
<i>WEB GUI Languages .....</i>	<i>18</i>
<i>WEB GUI Configuration .....</i>	<i>19</i>
<i>Overview Page .....</i>	<i>20</i>
<i>Save and Apply Changes .....</i>	<i>21</i>
<b>ROUTER CONFIGURATION .....</b>	<b>22</b>
Status .....	22
Ports Configuration .....	23
<i>WAN Ports Settings .....</i>	<i>23</i>
<i>Tunnel .....</i>	<i>24</i>
<i>Global Settings .....</i>	<i>25</i>
<i>Port Mirroring .....</i>	<i>26</i>
Static Routes .....	26
QoS .....	28
DDNS .....	31



<b>SETTING UP A WIRELESS NETWORK .....</b>	<b>32</b>
Discover and Pair GWN76xx Access Points .....	32
Network Groups .....	35
<i>Create an SSID under a Network Group .....</i>	<i>40</i>
<i>Additional SSID under Same Network Group .....</i>	<i>41</i>
<b>CLIENTS CONFIGURATION .....</b>	<b>43</b>
Clients .....	43
<i>Status .....</i>	<i>43</i>
<i>Edit IP and Name .....</i>	<i>44</i>
<i>Block a client .....</i>	<i>45</i>
<b>VPN (VIRTUAL PRIVATE NETWORK).....</b>	<b>46</b>
Overview .....	46
OpenVPN® Server Configuration .....	46
<i>Generate Self-Issued Certificate Authority (CA) .....</i>	<i>46</i>
<i>Generate Server/Client Certificates .....</i>	<i>49</i>
<i>Create OpenVPN® Server .....</i>	<i>56</i>
OpenVPN® Client configuration .....	60
L2TP/IPSEC Configuration .....	64
<i>GWN7000 L2TP/IPSec Client Configuration .....</i>	<i>64</i>
PPTP CONFIGURATION.....	67
<i>GWN7000 Client Configuration .....</i>	<i>67</i>
<b>FIREWALL.....</b>	<b>70</b>
Basic Settings .....	70
<i>General Settings .....</i>	<i>70</i>
<i>Port Forwarding .....</i>	<i>70</i>
<i>DMZ .....</i>	<i>71</i>
<i>Inter-Group Traffic Forwarding .....</i>	<i>72</i>
<i>UPnP .....</i>	<i>73</i>
Traffic Rules Settings .....	74
Firewall Advanced Settings.....	75
<i>General Settings .....</i>	<i>75</i>
<i>SNAT .....</i>	<i>76</i>
<i>DNAT .....</i>	<i>77</i>
<b>MAINTENANCE AND TROUBLESHOOTING .....</b>	<b>79</b>



Maintenance .....	79
Debug .....	80
<i>Capture</i> .....	80
<i>Ping/Traceroute</i> .....	81
<i>Syslog</i> .....	83
<i>NAT Table</i> .....	83
File Sharing .....	84
SNMP (Pending) .....	86
<b>UPGRADING AND PROVISIONING .....</b>	<b>88</b>
Upgrading Firmware .....	88
<i>Upgrading via WEB GUI</i> .....	88
Provisioning and backup .....	89
<i>Download Configuration</i> .....	89
<i>Configuration Server</i> .....	89
Reset and reboot .....	90
<b>EXPERIENCING THE GWN7000 ENTERPRISE ROUTER .....</b>	<b>91</b>



## Table of Tables

Table 1: GWN7000 Technical Specifications .....	12
Table 2: GWN7000 Equipment Packaging.....	14
Table 3: LED Indicators .....	16
Table 4: Overview.....	20
Table 5: GWN7000 WEB GUI -> Router ->Port -> WAN Port (1,2) .....	23
Table 6: 6in4 Tunnels .....	24
Table 7: 6rd Tunnels.....	25
Table 8: aiccu Tunnels.....	25
Table 9: GWN7000 WEB GUI->Router->Port->Global Settings .....	26
Table 10: Port Mirroring.....	26
Table 11: IPv4 Static Routes .....	27
Table 12: IPv6 Static Routes.....	27
Table 13: QoS Basic.....	29
Table 14: Upstream QoS.....	29
Table 15: QoS Policer .....	30
Table 16: Device Configuration .....	33
Table 17: Basic.....	36
Table 18: Wi-Fi .....	38
Table 19: CA Certificate.....	47
Table 20: Server Certificate.....	50
Table 21: Client Certificat .....	54
Table 22: OpenVPN® Server .....	57
Table 23: OpenVPN® Client .....	62
Table 24: L2TP Configuration.....	65
Table 25: PPTP Configuration.....	68
Table 26: Port Forward.....	71
Table 27: DMZ.....	72
Table 28: UPnP Settings .....	73
Table 29: Firewall Traffic Rules .....	74
Table 30: Firewall-General Settings .....	75
Table 31: SNAT .....	76
Table 32: DNAT .....	77
Table 33: Maintenance .....	79
Table 34: Debug-Capture .....	81
Table 35: Add a New File to Share.....	85
Table 36: SNMP Basic Page .....	86
Table 37: SNMP Advanced Page .....	87
Table 38: Network Upgrade Configuration .....	88



## Table of Figures

Figure 1: GWN7000 Front View .....	14
Figure 2: GWN7000 Back View .....	15
Figure 3: GWN7000 Web GUI Login Page .....	17
Figure 4: Change Password on first boot.....	18
Figure 5: Setup Wizard .....	18
Figure 6: GWN7000 Web GUI Language .....	19
Figure 7: GWN7000 Web GUI Language .....	19
Figure 8: Overview Page.....	20
Figure 9: Apply Changes.....	21
Figure 10: Router's Status .....	22
Figure 11: QoS .....	28
Figure 12: Discover AP .....	32
Figure 13: Discovered Devices .....	33
Figure 14: GWN7610 online.....	33
Figure 15: Network Group.....	35
Figure 16: Add a New Network Group .....	36
Figure 17: Device Membership .....	39
Figure 18: Add AP to Network Group from Access Points Page.....	40
Figure 19: Create an SSID.....	41
Figure 20: Additional SSID .....	42
Figure 21: Additional SSID Created .....	42
Figure 22: Clients .....	43
Figure 23: Client's Status .....	44
Figure 24: Client's Configuration .....	44
Figure 25: Block a Client .....	45
Figure 26: Unban Client .....	45
Figure 27: Create CA Certificate .....	47
Figure 28: CA Certificate .....	49
Figure 29: Generate Server Certificates .....	50
Figure 30: User Management .....	52
Figure 31: Client Certificat.....	54
Figure 32: Create OpenVPN® Server.....	57
Figure 33: OpenVPN®.....	60
Figure 34: OpenVPN® Client.....	61
Figure 35: OpenVPN® Client.....	64
Figure 36: L2TP Client Configuration.....	65
Figure 37: L2TP Client .....	67
Figure 38: PPTP Client Configuration .....	68



Figure 39: PPTP Client .....	69
Figure 40: Basic->General Settings .....	70
Figure 41: Port Forward .....	71
Figure 42: DMZ .....	72
Figure 43: Inter-group Traffic Forwarding .....	72
Figure 44: Enabling inter-group traffic.....	73
Figure 45: Traffic Rules Settings .....	74
Figure 46: Capture Files.....	81
Figure 47: IP Ping .....	82
Figure 48: Traceroute.....	82
Figure 49: Syslog .....	83
Figure 50: NAT table .....	84
Figure 51: Add a New File to Share .....	85
Figure 52: File Share Actions .....	85
Figure 53: Access File Share .....	86





## DOCUMENT PURPOSE

This document describes how to configure the GWN7000 to manage wired and wireless networks via an intuitive WebGUI. The intended audiences of this document are network administrators. Please visit <http://www.grandstream.com/support> to download the latest “GWN7000 User Manual”.

This guide covers following topics:

- [Product Overview](#)
- [Installation](#)
- [Getting Started](#)
- [Router Configuration](#)
- [Setting up a Wireless Network](#)
- [Clients Configuration](#)
- [VPN](#)
- [Firewall](#)
- [Maintenance and Troubleshooting](#)
- [Experiencing the GWN7000 Enterprise Router](#)



## CHANGE LOG

This section documents significant changes from previous versions of the GWN7000 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 1.0.2.71**

- This is the initial version.



## WELCOME

Thank you for purchasing Grandstream GWN7000 Enterprise Multi-WAN Gigabit VPN Router.

The GWN7000 is a powerful enterprise-grade multi-WAN Gigabit VPN router. Ideal for the enterprise, small-to-medium business, retail, education, hospitality and medical markets, the GWN7000 supports comprehensive Wi-Fi and VPN solutions that can be shared across one or many different physical locations. It features high-performance routing and switching power and a hardware-accelerated VPN client/server for secure inter-office connectivity. To maximize network reliability, the GWN7000 supports traffic load balancing and failover. The GWN7000 features an integrated controller and automated provisioning master that can setup and manage up to 300+ in-network GWN series Wi-Fi Access Points. This can be easily operated through the product's intuitive web browser user interface, which also offers a central panel to monitor and control the entire network.



**Caution:**

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



**Warning:**

Please do not use a different power adaptor with the GWN7000 as it may cause damage to the products and void the manufacturer warranty.

---



## PRODUCT OVERVIEW

### Technical Specifications

**Table 1: GWN7000 Technical Specifications**

<b>Network Interfaces</b>	<ul style="list-style-type: none"> <li>• 2 x autosensing 10/100/1000 WAN Ports</li> <li>• 1 x autosensing 10/100/1000 configurable as LAN, WAN or VoIP port</li> <li>• 4 x autosensing 10/100/1000 LAN Ports</li> </ul>
<b>WAN</b>	<ul style="list-style-type: none"> <li>• DHCP</li> <li>• Static IP</li> <li>• PPPoE</li> <li>• Load balance &amp; failover</li> <li>• Rule based routing</li> </ul>
<b>LAN</b>	<ul style="list-style-type: none"> <li>• DHCP server</li> <li>• DNS Cache</li> <li>• Multiple zones</li> <li>• VLAN</li> </ul>
<b>Auxiliary Ports</b>	<ul style="list-style-type: none"> <li>• 2 x USB 3.0 ports</li> <li>• 1 x Reset Pinhole</li> </ul>
<b>Routing Performance</b>	Up to 1 million packets/second with 64-byte packet size
<b>USB</b>	<ul style="list-style-type: none"> <li>• 3G/4G/LTE as WAN</li> <li>• Printer sharing</li> <li>• File sharing</li> </ul>
<b>Network Protocols</b>	<ul style="list-style-type: none"> <li>• IPv4, IPv6, 802.1Q, 802.1p</li> </ul>
<b>VPN</b>	<ul style="list-style-type: none"> <li>• Protocols: PPTP, L2TP/IPSec, OpenVPN®</li> <li>• Client, Server or pass through</li> </ul>
<b>LED</b>	8 green-color LEDs for device tracking and status indication
<b>Mounting</b>	Indoor wall mount, Desktop
<b>QoS</b>	VLAN, TOS, supports multiple traffic classes, filter by port, IP address, DSCP, and policing
<b>Firewall</b>	NAT, DMZ, Port Forwarding, SPI, UPnP
<b>Auto Provisioning Capability</b>	Embedded provisioning controller to manage up to 300+ GWN series Wi-Fi APs
<b>Management</b>	Web, CLI
<b>Power</b>	<ul style="list-style-type: none"> <li>• 802.3at PoE</li> <li>• Included Power Supply: 12V/2A</li> </ul>



	<ul style="list-style-type: none"><li>• Max power consumption: 16W</li></ul>
<b>Environmental</b>	<ul style="list-style-type: none"><li>• Operation: 0°C to 50°C</li><li>• Storage: -10°C to 60°C</li><li>• Humidity: 10% to 90% Non-condensing</li></ul>
<b>Physical</b>	Unit Dimensions: 200 x 136 x 37mm; Unit Weight: 570g Entire Package Dimensions: 324 x 163.5 x 54mm; Entire Package Weight: 930g
<b>Package Content</b>	<ul style="list-style-type: none"><li>• GWN7000 Enterprise Router</li><li>• 12V/2A Power Adapter</li><li>• Quick Installation Guide</li><li>• GPL License</li></ul>
<b>Compliance</b>	FCC, CE, RCM, IC



## INSTALLATION

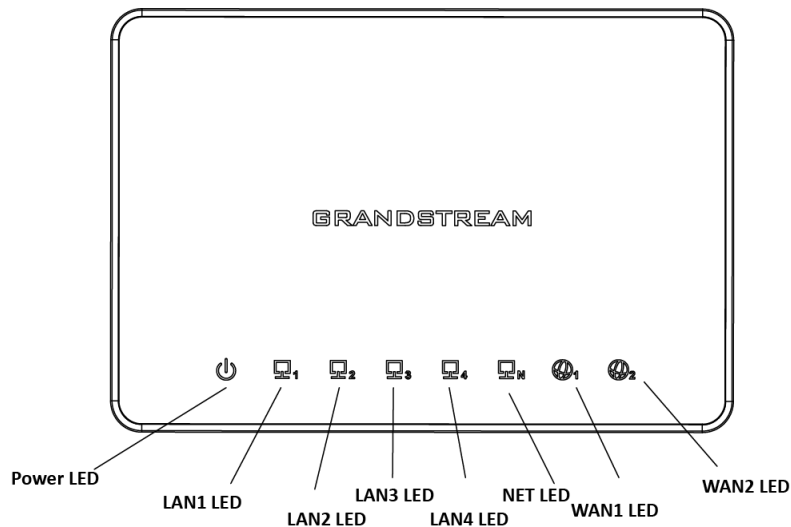
Before deploying and configuring the GWN7000, the device needs to be properly powered up and connected to the network. This section describes detailed information on installation, connection and warranty policy of the GWN7000.

### Equipment Packaging

**Table 2: GWN7000 Equipment Packaging**

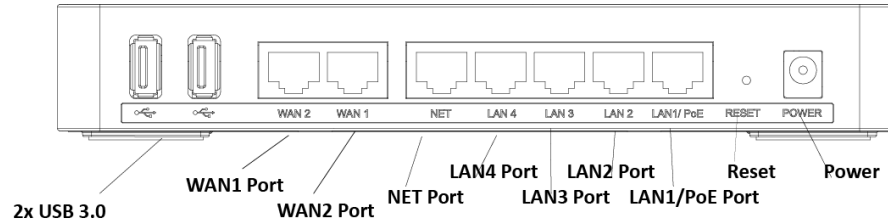
<b>Main Case</b>	Yes (1)
<b>Power adaptor</b>	Yes (1)
<b>Quick Installation Guide</b>	Yes (1)
<b>GPL License</b>	Yes (1)

### Connect your GWN7000



**Figure 1: GWN7000 Front View**





**Figure 2: GWN7000 Back View**

To set up the GWN7000, follow the steps below:

1. Connect one end of an RJ-45 Ethernet cable into the WAN1 or/and WAN2 port(s) of the GWN7000.
2. Connect the other end of the Ethernet cable(s) into a DSL modem or router(s).
3. Connect the 12V DC power adapter into the power jack on the back of the GWN7000. Insert the main plug of the power adapter into a surge-protected power outlet.
4. Wait for the GWN7000 to boot up and connect to internet/network. In the front of the GWN7000 the Power LED will be in solid green, and the WAN LED will flash in green.
5. Connect one of the LAN ports to your computer, the associated LED ports will flash in green.
6. (Optional) Connect LAN ports to your GWN76xx access points or/and other devices, the associated LED ports will flash in green.

## Safety Compliances

The GWN7000 Enterprise Router complies with FCC/CE and various safety standards. The GWN7000 power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN7000 package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

## Warranty

If the GWN7000 Enterprise Router was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for a RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.



## GETTING STARTED

The GWN7000 Enterprise Router provides an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN7000's setup.

This section provides step-by-step instructions on how to read LED indicators and use Web GUI interface of the GWN7000.

### LED Indicators

The front panel of the GWN7000 has LED indicators for power and interfaces activities, the table below describes the LED indicators status.

**Table 3: LED Indicators**

LED	Status	Indication
<b>POWER</b>	OFF	GWN7000 is powered off or abnormal power supply.
	Solid green	GWN7000 is powered on correctly.
<b>WAN (1,2)</b>	Flashing green	GWN7000 is connected as a client to another network and data is transferring.
	Solid green	GWN7000 is connected as a client to another network and there is no activity.
<b>LAN (1,2,3,4,5)</b>	Flashing green	A device is connected to the corresponding LAN port and data is transferring.
	Solid green	A device is connected to the corresponding LAN port and there is no activity.

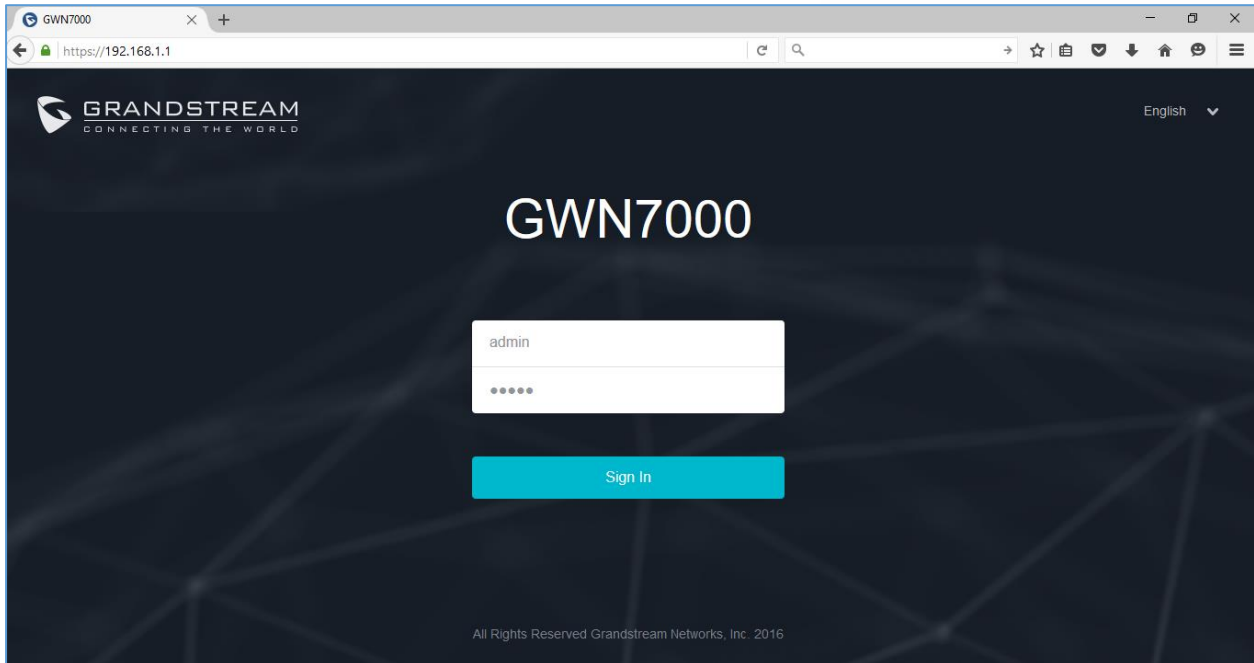
### Use the WEB GUI

#### Access WEB GUI

The GWN7000 embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome.







**Figure 3: GWN7000 Web GUI Login Page**

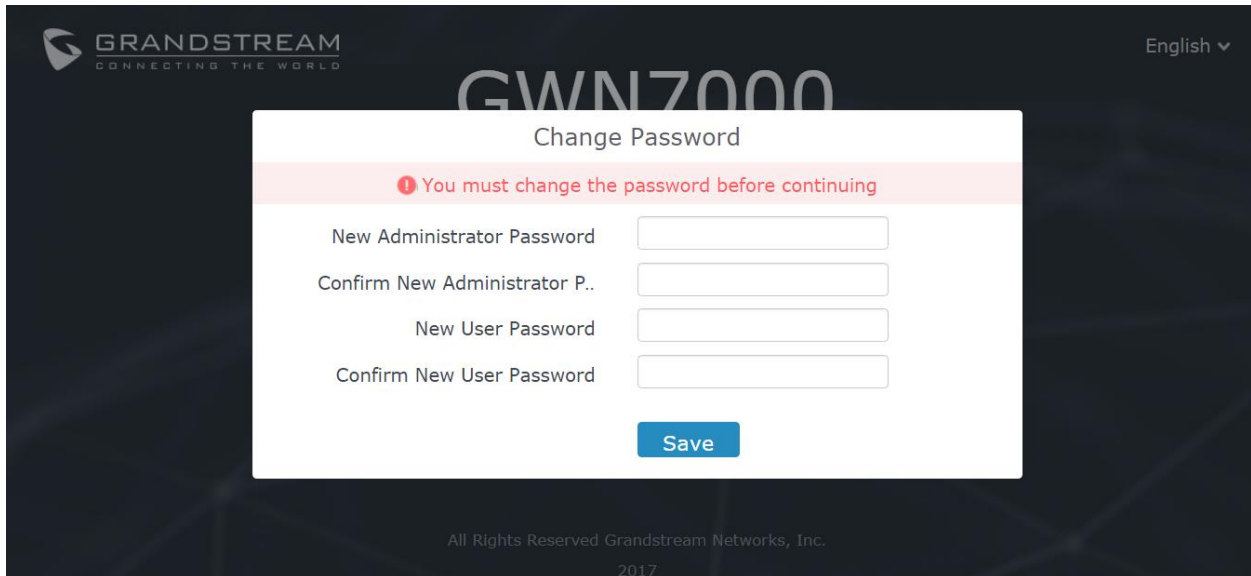
To access the Web GUI:

1. Connect a computer to a LAN Port of the GWN7000.
2. Ensure the device is properly powered up, and the Power, 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://192.168.1.1> (Default IP address).
4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username and password are "admin" and "admin".


**Note:** At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing GWN7000 web interface.

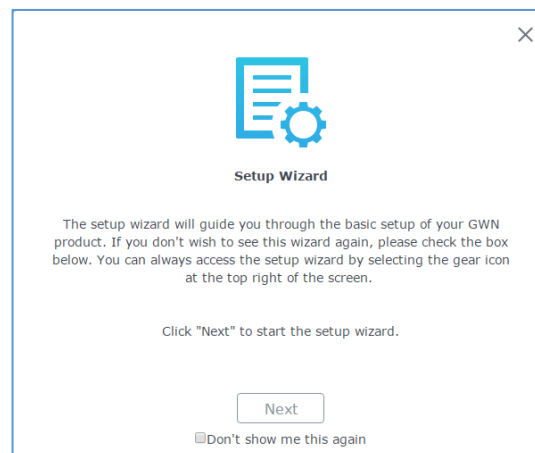
The password field is case sensitive with a maximum length of 32 characters. Using strong password including letters, digits and special characters is recommended for security purposes.





**Figure 4: Change Password on first boot**

At first login, a Setup Wizard tool will pop up to help going through the configuration setup, or exit to configure manually. Setup Wizard can be accessed anytime by clicking on  while on the web interface.



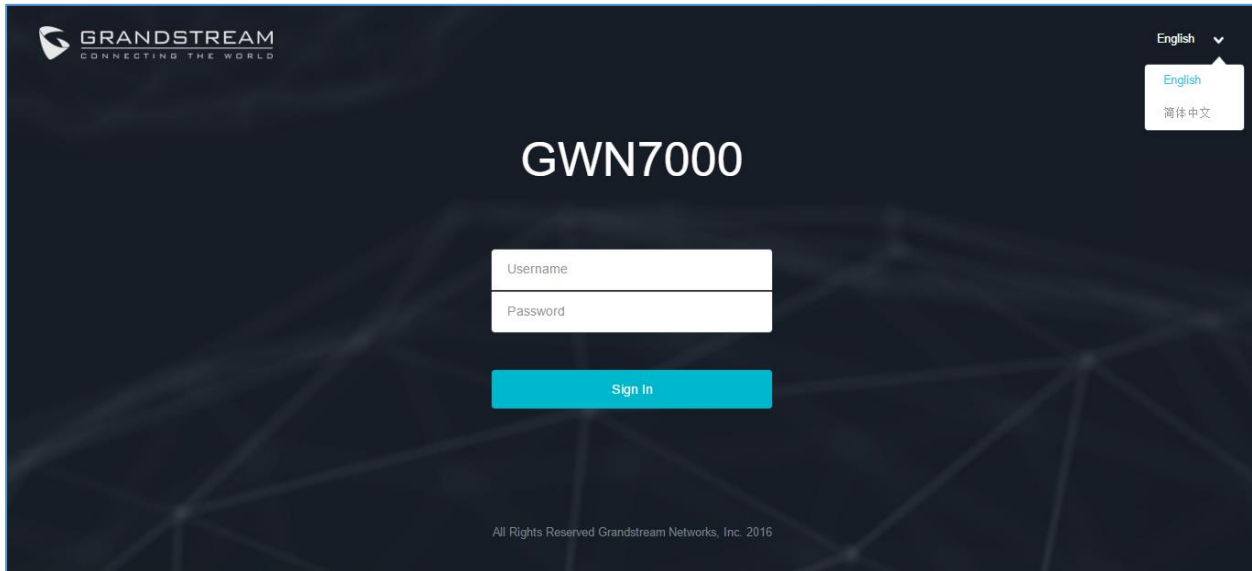
**Figure 5: Setup Wizard**

## WEB GUI Languages

Currently the GWN7000 series web GUI supports **English** and **Simplified Chinese**.

To change default language, select the displayed language at the upper right of the web GUI either before or after logging in.





**Figure 6: GWN7000 Web GUI Language**



**Figure 7: GWN7000 Web GUI Language**

## WEB GUI Configuration

GWN7000 web GUI includes 8 main sections to configure and manage the router and check connection status.

- **Overview:** Provides an overall view of the GWN7000's information presented in a Dashboard style for easy monitoring.
- **Router:** Displays device's status and used to configure ports settings such as IP configuration for WAN ports, load balancing, failover, static routes, port mirroring, QoS and DDNS.
- **Access Points:** To add, pair and manage discovered access points.
- **Clients:** Shows and manages the list of the clients connected to LAN ports of the GWN7000 and wireless clients connected via GWN76xx access points.
- **VPN:** Configures OpenVPN® Client/Server, PPTP and L2TP/IPSec client tunnels.
- **Firewall:** Basic and advanced Firewall configuration to securely manage router's incoming/outgoing traffic.
- **Network Group:** To add and manage wireless network groups using paired access points via VLANs.
- **System Settings:** For Maintenance and debugging features, as well as generating certificates and file sharing.



## Overview Page

Overview is the first page shown after successful login to the GWN7000's Web Interface. It provides an overall view of the GWN7000's information presented in a Dashboard style for easy monitoring.

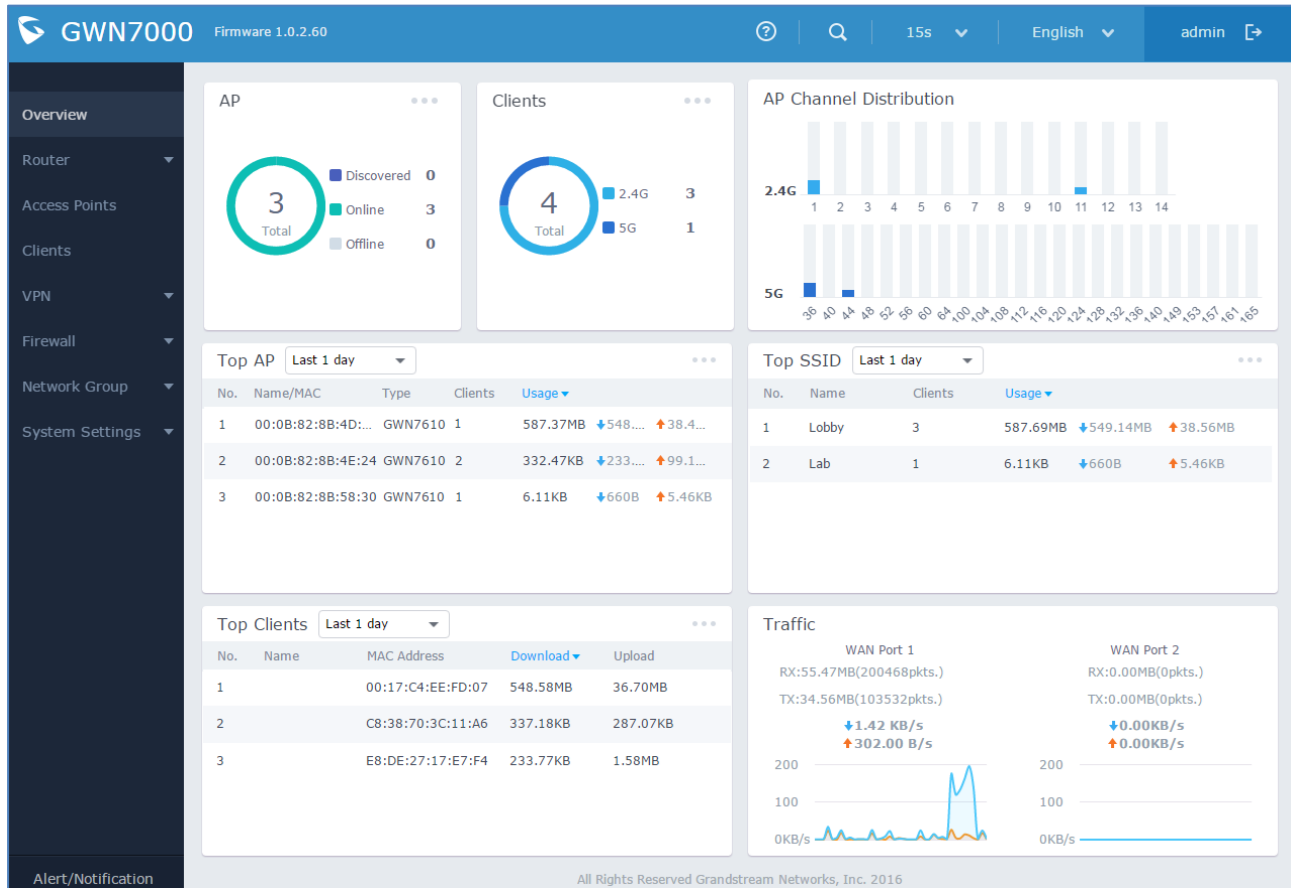







Figure 8: Overview Page


It is used to show the status of the GWN7000 for different items, please refer to the following table for each item:

Table 4: Overview

<b>AP</b>	Shows the number of Access Points that are Discovered, Paired (Online) and Offline. Click on  to go to Access Points' page for basic and advanced configuration options for the APs
<b>Clients</b>	Shows the total number of connected clients, and a count for clients connected to each Channel. Click on  to go to Clients page for more options.
<b>AP Channel Distribution</b>	Shows the Channel used for all APs that are paired with this Access Point.

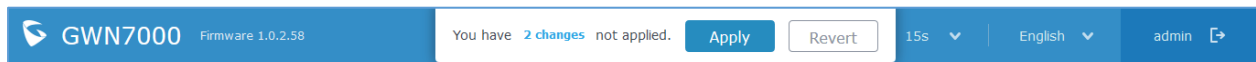


<b>Top AP</b>	Shows the Top APs list, assort the list by number of clients connected to each AP or data usage combining upload and download. Click on  to go to Access Points page for basic and advanced configuration options for the APs.
<b>Top SSID</b>	Shows the Top SSIDs list, assort the list by number of clients connected to each SSID or data usage combining upload and download. Click on  to go to Network Group page for more options.
<b>Top Clients</b>	Shows the Top Clients list, assort the list of clients by their upload or download. Click on  to go to Clients page for more options.
<b>Traffic</b>	Shows the sent/received traffic data speeds on both WAN ports.

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

## Save and Apply Changes

When clicking on "Save" button after configuring or changing any option on the web GUI pages. A message mentioning the number of changes will appear on the upper menu.



**Figure 9: Apply Changes**

Click on  button to apply changes, or  to undo the changes.



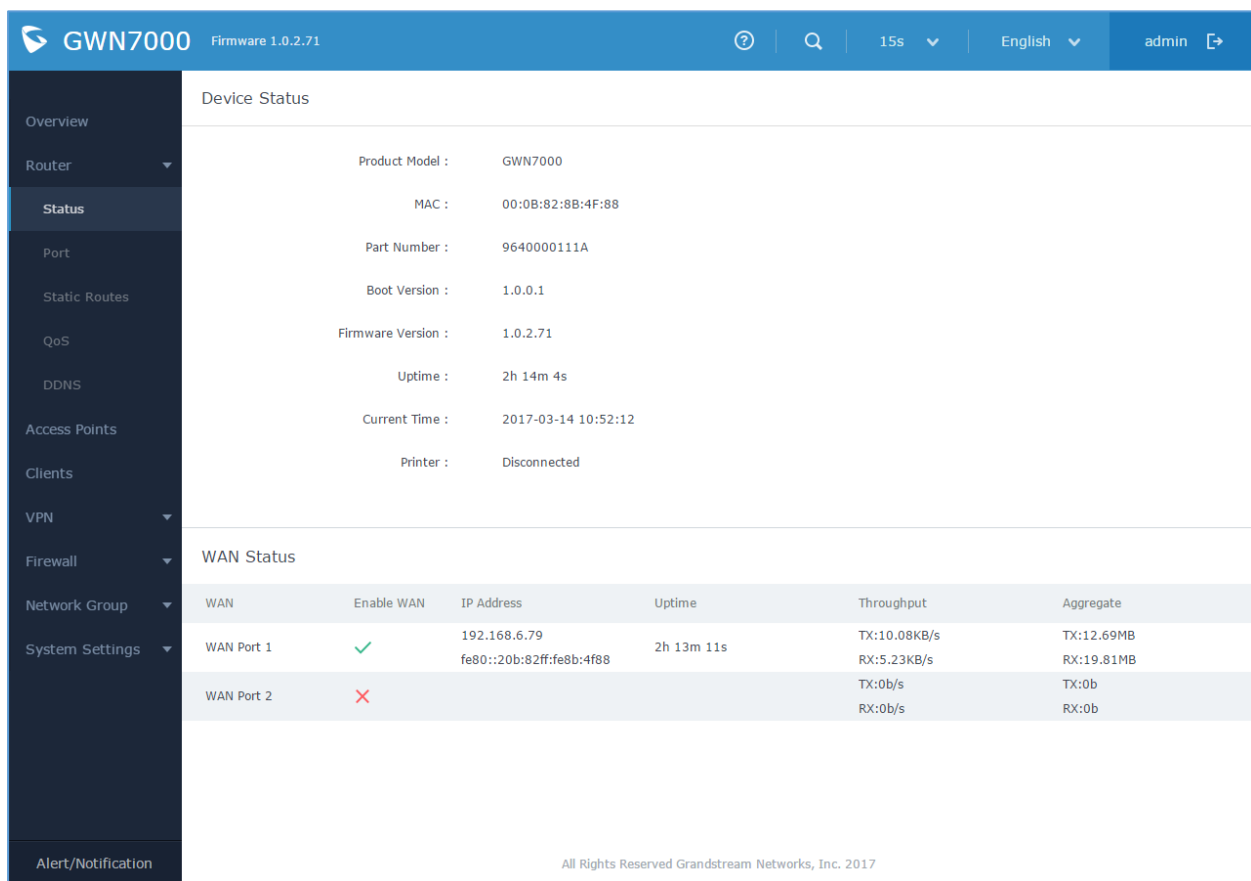
## ROUTER CONFIGURATION

This section includes configuration pages for network WAN ports, static routes, QoS and DDNS and shows also the router status.

### Status

Status page displays **Device Status** to check MAC address, Part Number, Firmware related information and Uptime for the GWN7000; and **WAN Status** showing general information about WAN Ports such as uptime, current throughput, aggregate usage, and IP address.

Router's Status page can be accessed from **Web GUI->Router->Status**.



Device Status	
Product Model :	GWN7000
MAC :	00:08:82:8B:4F:88
Part Number :	9640000111A
Boot Version :	1.0.0.1
Firmware Version :	1.0.2.71
Uptime :	2h 14m 4s
Current Time :	2017-03-14 10:52:12
Printer :	Disconnected

WAN Status						
WAN	Enable WAN	IP Address	Uptime	Throughput	Aggregate	
WAN Port 1	✓	192.168.6.79 fe80::20b:82ff:fe8b:4f88	2h 13m 11s	TX:10.08KB/s RX:5.23KB/s	TX:12.69MB RX:19.81MB	
WAN Port 2	✗			TX:0b/s RX:0b/s	TX:0b RX:0b	

All Rights Reserved Grandstream Networks, Inc. 2017

**Figure 10: Router's Status**



## Ports Configuration

Connect to GWN7000's Web GUI from a computer connected to a LAN port and go to **Router->Port** page for Port configuration.

### WAN Ports Settings

The GWN7000 has 2 WAN ports configured as DHCP clients by default. Each port can be connected with DSL modem or routers.

WAN ports support also setting static IPv4/IPv6 addresses, and configure PPPoE for each WAN port.

Please refer to the following table for basic network configuration parameters on WAN ports for GWN7000.

**Table 5: GWN7000 WEB GUI -> Router ->Port -> WAN Port (1,2)**

<b>Enabled</b>	Choose whether to enable or disable the WAN port.
<b>WAN Address Type</b>	<p>Select "DHCP", "Static" or "PPPoE" mode on the WAN interfaces of GWN7000. The default setting is "DHCP".</p> <ul style="list-style-type: none"> <li> <b>DHCP</b>            When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server.         </li> <li> <b>Static</b>            When selected, the user should set a static IPv4 address, Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well.         </li> <li> <b>PPPoE</b>            When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval and Inter-Key Timeout (in seconds).         </li> </ul>
<b>Preferred IPv4 DNS</b>	Enter the preferred DNS server address (IPv4 address). If Preferred DNS is set, GWN7000 will use it in priority.
<b>Alternate IPv4 DNS</b>	Enter the Alternate DNS server address (IPv4 address). If Preferred DNS is set, GWN7000 will use it in when the Preferred DNS fails.
<b>Native IPv6</b>	<p>Used to enable assigning IPv6 address to GWN7000.</p> <p>Once checked users will be able to configure following fields: "IPv6 Address Assignment", "Preferred IPv6 DNS", "Alternate IPv6 DNS" and "IPv6 Relay to LAN".</p>
<b>IPv6 Address Assignment</b>	<p>This option is appearing when enabling "Native IPv6" option.</p> <p>Select "Auto" to get an IPv6 address from DHCP server or "Static" to configure manually an IPv6 address. If set to Static, the following fields should be configured:</p> <ul style="list-style-type: none"> <li> <b>IPv6 Address/Prefix Length</b>            Used to set an IPv6 address/Prefix length when using Static IPv6 option         </li> </ul>



	<p>Example: <i>fec0:470:28:5b2::1/64</i></p> <ul style="list-style-type: none"> <li>• <b>IPv6 Gateway</b> Used to define the Gateway's IPv6 address.</li> <li>• <b>IPv6 Prefix/IPv6 Prefix Length</b> Enter the IPv6 prefix and IPv6 prefix length. Example: <i>::1/64</i></li> </ul>
<b>Preferred IPv6 DNS</b>	<p>This option appears only when “Native IPv6” option is enabled. It is used to set a preferred DNS server address (IPv6 address). If Preferred DNS is set, GWN7000 will use it in priority.</p>
<b>Alternate IPv6 DNS</b>	<p>This option appears only when “Native IPv6” option is enabled. It is used to set an Alternate DNS server address (IPv6 address). If Preferred DNS is set, GWN7000 will use it in when the Preferred DNS fails.</p>
<b>IPv6 Relay to LAN</b>	<p>This option appears only when “Native IPv6” option is enabled. When enabled the GWN7000 will relay IPv6 address to LAN clients</p>
<b>Multi-WAN</b>	<p>These options are used when both WAN ports are enabled and using Failover feature:</p> <ul style="list-style-type: none"> <li>• <b>Tracking IP</b> Configures the tracking IP(s). ICMP packets are being used to track the IP(s) address(es). When the tracking fails, the GWN7000 will use the secondary WAN port as failover. Default IP used is 8.8.8.8.</li> <li>• <b>Tracking Timeout (sec)</b> Configures tracking timeout in seconds. Default value is 2.</li> <li>• <b>Tracking Interval (sec)</b> Configures the track interval in seconds. Default value is 5.</li> <li>• <b>Bandwidth</b> Specifies the bandwidth for the port, e.g: “100k”, “1M” or “100M”.</li> </ul>
<b>VLAN Tagging</b>	<p>Used to enable VLAN tagging. If set to “0” the VLAN tagging will be disabled, otherwise set a VLAN value between 5 and 4093. Default is 0.</p>

## Tunnel

Tunnel page is used to set IPv6 tunnels on WAN ports via IPv6 tunnel brokers service providers, this serves the purpose of transferring IPv6 packets over IPv4 Network. It supports creating 6in4, 6rd and aiccu tunnels. Please refer to below tables for each tunnel type.

**Table 6: 6in4 Tunnels**

<b>WAN Interface</b>	Choose the WAN port on which to setup the 6in4 tunnel.
<b>MTU</b>	Set the Maximum Transmission Unit value. The valid range is 64-9000.





	Default value is 1500.
<b>6in4 IPv4 Peer Address</b>	Enter the IPv4 tunnel endpoint at the tunnel's provider.
<b>6in4 Tunnel Endpoint IPv6 Address</b>	Enter the local IPv6 address delegated to the tunnel endpoint. Example: 2001:db8:2222::2/64
<b>6in4 Routed Prefix</b>	Set the routable prefix given by the tunnel provider to allow LAN clients to get addresses from that prefix.
<b>Tunnel ID</b>	Specifies the tunnel's ID.
<b>Username</b>	Set the username used to login into the tunnel broker.
<b>Password</b>	Set the password (used for endpoint update).
<b>Update Key</b>	Set the update key, it overrides the password used for endpoint update.

**Table 7: 6rd Tunnels**

<b>WAN Interface</b>	Choose the WAN port on which to setup the 6rd tunnel.
<b>MTU</b>	Set the Maximum Transmission Unit value. The valid range is 64-9000. Default value is 1500.
<b>6rd IPv4 Peer Address</b>	Enter the IPv4 Peer address.
<b>6rd IPv6 Address Prefix</b>	Specifies the IPv6 prefix given by the provider. Example: 2001:B000::/32
<b>IPv6 Prefix Length</b>	Specifies the IPv6 prefix length (Value between 1 and 128). Example: 32
<b>IPv4 Prefix Length</b>	Specifies the prefix length of the IPv4 transport address. (Value between 1 and 32).

**Table 8: aiccu Tunnels**

<b>WAN Interface</b>	Choose the WAN port on which to setup the aiccu tunnel.
<b>Username</b>	Enter the Username (Provided by signing up with SixXS Tunnel Broker)
<b>Password</b>	Enter the Username's password



## Global Settings

This section specifies operating mode for multi-WAN that will be used for enabling/disabling Failover and Load Balancing on WAN ports, and banning MAC addresses.

The following table shows the configuration parameters for Multi-WAN settings



**Table 9: GWN7000 WEB GUI->Router->Port->Global Settings**

<b>Multi-WAN</b>	Three options are available: <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Failover</li> <li>• Load Balance + Failover</li> </ul>
<b>Disabled</b>	This will disable Multi-WAN feature
<b>Failover</b>	If chosen failover will be enabled on WAN ports, admins need to choose the Primary WAN port to be used. When selected, user can set <b>Multi-WAN</b> parameters on WAN ports.
<b>Load Balance + Failover</b>	In addition to failover, load balance will be used on both ports to optimize the resource utilization. Please note that for this feature to work, WAN ports should be connected to different networks. When selected, user can set <b>Multi-WAN</b> parameters on WAN ports.
<b>Banned Client MAC</b>	Shows the list of banned clients MAC addresses, other MAC addresses could be also added by clicking on  or removed by clicking on  .
<b>MAC Override</b>	MAC Override feature is used to give a virtual MAC address to the GWN7000, in order that any client connected to the Router will be using the entered MAC address. <b>Note:</b> Please make sure to enter the Override MAC address in lower cases.

## Port Mirroring

With port mirroring enabled, the GWN7000 will send a copy of all network packets seen on one LAN port to another port, where the packet can be analyzed. Refer to the below table for the available fields to configure.

**Table 10: Port Mirroring**

<b>Enable Outgoing Mirroring</b>	Check to enable outgoing mirroring for a LAN port. Default is “Disabled”
<b>Enable Incoming Mirroring</b>	Check to enable incoming mirroring for a LAN port. Default is “Disabled”
<b>Mirroring Port</b>	Select which LAN port that will be mirroring traffic. Default is “Disabled”
<b>Mirrored Port</b>	Select which LAN port that will act as mirrored port. Default is “Disabled”

## Static Routes

GWN7000 supports setting manually static IPv4 and IPv6 routes as well as displaying routing table entries.




Static routes configuration page can be accessed from GWN7000 WebGUI->**Router->Static Routes:**



Three tabs are available:

- **Routes** to view routing table entries.
- **IPv4** to create, edit or delete static IPv4 static routes.
- **IPv6** to create, edit or delete static IPv6 static routes.

Following actions are available in both **IPv4** and **IPv6** tabs:

- To add a new static route, click on 
- To edit a static route, click on 
- To delete a static route, click on 

Refer to the following tables when editing or creating IPv4/IPv6 static routes:

**Table 11: IPv4 Static Routes**

<b>Name</b>	Enter the Name of the static route to be configured.
<b>Enabled</b>	Select whether to enable or disable this static route.
<b>Source Group</b>	Choose the LAN's Network Group, which will be using this static route.
<b>Target Network/Host</b>	Enter the Network/Host IP address on which to route the traffic to. Example: 192.168.5.0
<b>Netmask</b>	Enter the Network/Host Netmask. Example: 255.255.255.0
<b>Gateway</b>	Enter the Gateway's IP address. Example: 192.168.5.1.
<b>Metric</b>	Set the metric value. The valid range is 0-255. Default value is 1.

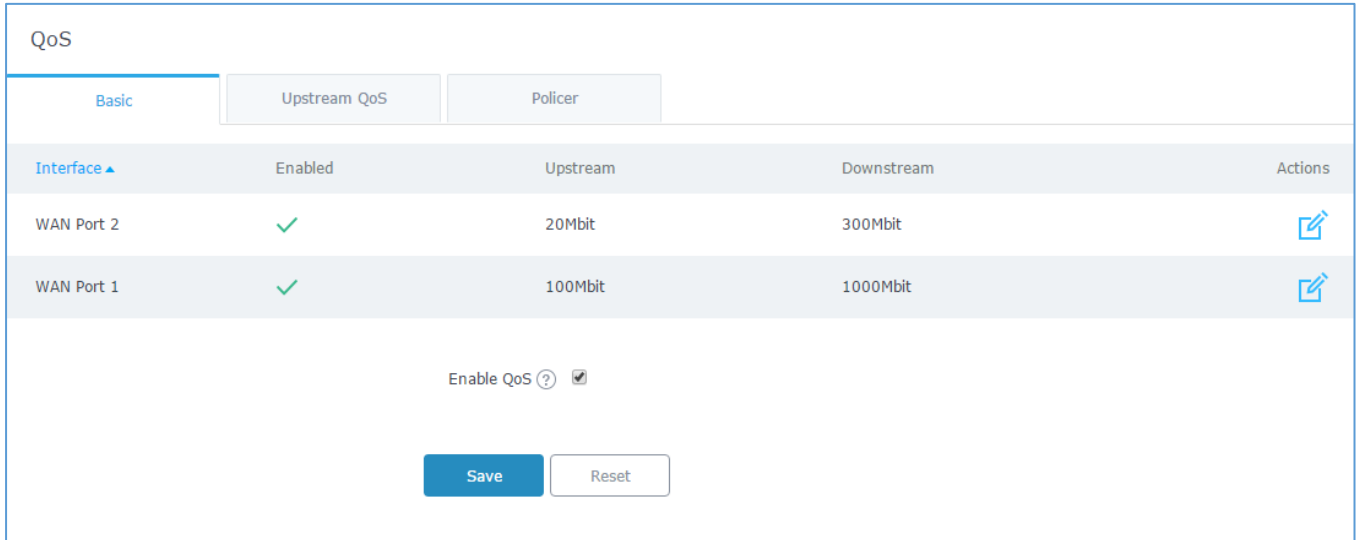
**Table 12: IPv6 Static Routes**



<b>Name</b>	Enter the Name of the static route to be configured.
<b>Enable</b>	Select whether to enable or disable this static route.
<b>Group</b>	Choose the LAN's Network Group
<b>Target Network/Host</b>	Enter the Network/Host IP address on which to route the traffic to. 2001:db8:3c4d:4::/64
<b>Gateway</b>	Enter the Gateway's IP address. fec0:470:28:5b2::1/64
<b>Metric</b>	Set the metric value. The valid range is 0-255. Default value is 1.



## QoS

The GWN7000 offers the possibility to enable and configure QoS on both WAN and LAN interfaces, this will help to manage in more depth the network traffic to define priority and classify different services and protocols in a scheduled manner.



Interface ▲	Enabled	Upstream	Downstream	Actions
WAN Port 2	✓	20Mbit	300Mbit	
WAN Port 1	✓	100Mbit	1000Mbit	


Enable QoS 

Figure 11: QoS

To activate QoS, check “**Enable QoS**”. Three tabs are available for configuration:

- **Basic:** Download and upload bandwidth speeds settings on each WAN interface.
- **Upstream QoS:** Upstream QoS allows creating Traffic Classes to prioritize traffic for specific resources on the network by controlling transmission/upload rate. Note that different classes can be created and assigned as Traffic filters by respecting following conditions:
  - ✓ The total of Upstream bandwidth values of each created class should not exceed the upstream bandwidth value configured in **Basic**.
  - ✓ The remaining bandwidth will be lent to the next priority level of class.
  - ✓ All filter options are summed together.
- **Policer:** While Upstream QoS is dealing with traffic transmission, Policer is controlling the incoming traffic. Thus, allowing to create rules to specific targets to set priority and received traffic rate, giving the GWN7000 the ability to drop the exceeding traffic when reaching the configured maximum rate.

Refer to the following tables for each tab option:



**Table 13: QoS Basic**

<b>Enabled</b>	Check to enable upstream and downstream bandwidth speeds for the selected WAN interface.
<b>Upstream</b>	<p>Set the Upstream value to specify the upload bandwidth for selected interface, the value should end with Mbit, Kbit or with no unit if the set value is referring to “bit” unit.</p> <p>Note that the set value will affect and limit the bandwidth values on created classes on <b>QoS Upstream</b>.</p> <p>Examples: <i>500Mbit</i>  <i>100Kbit</i>  <i>500</i></p>
<b>Downstream</b>	<p>Set the Downstream value to specify the download bandwidth speed for selected interface, the value should end with “Mbit”, “Kbit” or with no unit if the set value is referring to “bit” unit.</p> <p>Examples: <i>1000Mbit</i>  <i>100Kbit</i>  <i>500</i></p>

**Table 14: Upstream QoS**

Traffic Class	
<b>Name</b>	Define a name for the traffic class.
<b>Priority</b>	Set the priority of the traffic class, the lower the value, the highest the priority. Valid range is between 1 and 64.
<b>Interface</b>	Select the WAN interface from which the traffic will be classified, make sure to enable the desired interface it from <b>QoS Basic</b> in order to appear.
<b>Upstream</b>	<p>Set Upstream bandwidth value. The value should end with “Mbit”, “Kbit” or with no unit if the set value is referring to “bit” unit.</p> <p>Note that the sum of created classes should have upstream bandwidth speeds lower than the Upstream bandwidth value configured on <b>QoS Basic</b>.</p> <p>Examples: <i>100Mbit</i>  <i>100Kbit</i>  <i>500</i></p>
Traffic Filter	
<b>Class</b>	Select a class from created traffic classes using drop-down menu.
<b>Name</b>	Define a Name for the traffic filter rule.
<b>DSCP</b>	Choose the Differentiated Services Code Point (DSCP) value from drop-down list. Default is 0.
<b>IP Source Address</b>	Specify the Source IP address from which the traffic filter rule will be applied.



<b>IP Destination Address</b>	Specify the Destination IP address to which the traffic filter rule will be applied.
<b>TCP Source Port</b>	Specify the TCP Source port from which the traffic filter rule will be applied.
<b>TCP Destination Port</b>	Specify the TCP Source port to which the traffic filter rule will be applied.
<b>UDP Source Port</b>	Specify the UDP Source port from which the traffic filter rule will be applied.
<b>UDP Destination Port</b>	Specify the UDP Source port to which the traffic filter rule will be applied.
<b>Group Source</b>	Choose the LAN group of the specified Source IP address. If no Source IP address has been defined, the rule will be applied to all members of that LAN group.

**Table 15: QoS Policer**

<b>Name</b>	Define a Name for the Policer rule.
<b>Interface</b>	Select an interface from which the traffic will be policed, make sure to enable the desired interface it from <b>QoS Basic</b> in order to appear.
<b>Priority</b>	Set the priority of the traffic class, the lower the value, the highest the priority. Valid range is between 1 and 64.
<b>Rate</b>	Set a Rate value for download bandwidth when applying policer rule.
<b>DSCP</b>	Choose the Differentiated Services Code Point (DSCP) value from drop-down list. Default is 0.
<b>IP Source Address</b>	Specify the Source IP address from which the policer rule will be applied.
<b>IP Destination Address</b>	Specify the Destination IP address to which the policer rule will be applied.
<b>TCP Source Port</b>	Specify the TCP Source port from which the policer rule will be applied.
<b>TCP Destination Port</b>	Specify the TCP Source port to which the policer rule will be applied.
<b>UDP Source Port</b>	Specify the UDP Source port from which the policer rule will be applied.
<b>UDP Destination Port</b>	Specify the UDP Source port to which the policer rule will be applied.
<b>Group Source</b>	Choose the LAN group of the specified Source IP address. If no Source IP address has been defined, the rule will be applied to all members of that LAN group.



## DDNS

DDNS allows accessing GWN7000 via domain name instead of IP address, the GWN7000 supports following DDNS providers:

- Dyndns.org
- Changeip.com
- Zoneedit.com
- Free.editedns.net
- Freedns.afraid.org
- He.Net
- Dnsomatic.Com
- No-ip.pl
- Myonlineportal.net

Before configuring DDNS settings on the GWN7000, make sure first to create and confirm the DDNS account via supported providers.

Following steps illustrates how to configure the DDNS settings on your GWN7000:

1. Access to GWN7000 web GUI, and navigate to **Router -> DDNS**, and enable **DDNS** service.
2. Fill in the domain name created with DDNS provider under **Domain Name** field.
3. Enter your account username and password under **Username** and **Password** fields.
4. Specify the WAN interface to which DDNS is applied under **Network interface** field.
5. (Optional) For advanced configuration, it is also possible log to Syslog and modify the values of refreshing fields so to check periodically the updated IP address.



## SETTING UP A WIRELESS NETWORK

The GWN7000 Enterprise Router provides the user with the capability to create a wireless network by adding multiple GWN76xx series access points, with connectivity over the most common wireless standards (802.11b/g/n) operating in both 2.4GHz and 5GHz range.

The GWN7000 integrates multiple layers of security including the IEEE 802.1x port-based authentication protocol, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA and WPA2) and firewall and VPN tunnels.

This chapter will introduce how to discover, add the GWN76xx access points, create and manage Wi-Fi Networks.

For more details about Grandstream GWN76xx Access points, refer to <http://www.grandstream.com/products/networking-solutions/wifi-access-points>

### Discover and Pair GWN76xx Access Points

The GWN76xx are powerful access points, which are fully compatible with the GWN7000 and can be added with one click, provisioned and managed in an easy and intuitive way. Once a GWN76xx is successfully connected and has an IP from the GWN7000 router, user can then pair it to the GWN7000 and associate it with a Network Group.

To Pair a GWN76xx access point connected as LAN client to the GWN7000, follow the below steps:

1. Connect to the GWN7000 Web GUI and go to **Access Points**.

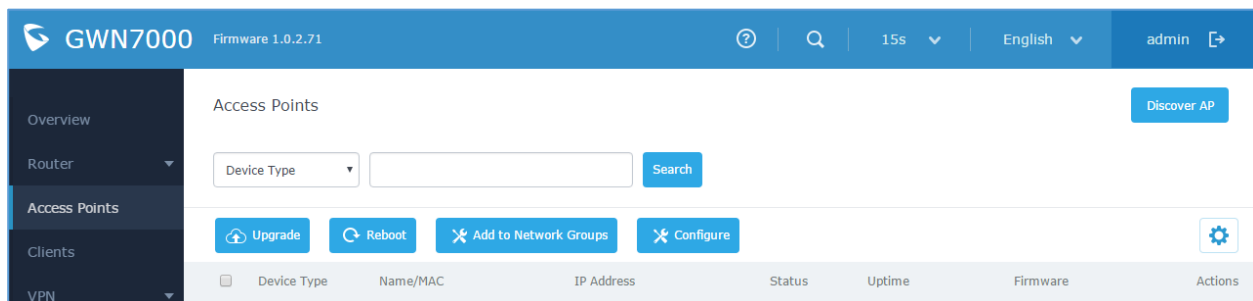


Figure 12: Discover AP





- Click on [Discover AP](#) to discover access points within GWN7000's Network, the following page will appear.

Discovered Devices				
Device Type	MAC	IP Address	Firmware	Actions
GWN7610	00:0B:82:8B:4D:D8	192.168.5.156	1.0.2.12	
GWN7600	00:0B:82:8B:58:30	192.168.5.140	1.0.1.30	

Showing 1-2 of 2 record(s). Per Page:

**Figure 13: Discovered Devices**

- Click on Pair under Actions, to pair the discovered Access Point with the GWN7000.
- The paired GWN76xx will appear Online, Click on to unpair it.

<input type="checkbox"/>	GWN7610	00:0B:82:8B:4D:D8	192.168.5.156	Online	56m 27s	1.0.2.12	
--------------------------	---------	-------------------	---------------	--------	---------	----------	--

**Figure 14: GWN7610 online**

- Click on next to paired access point to check device configuration for its status, users connected to it and configuration, or select multiple GWN76xx APs from the same model, and click on [Configure](#) to apply same configuration on selected units.

Refer to below table for Device Configuration tabs.

**Table 16: Device Configuration**

<b>Status</b>	Shows the device's status information such as Firmware version, IP Address, Link Speed, Uptime, and Users count via different Radio channels.
<b>Users</b>	Shows the users connected to the GWN76xx access point.
<b>Configuration</b>	<ul style="list-style-type: none"> <li><b>Device Name:</b> Set GWN76xx's name to identify it along with its MAC address.</li> </ul>



- **Fixed IP:** Used to set a static IP for the GWN76xx, if checked, the following needs to be configured:
  - IPv4 Address:* Enter the IPv4 address to be set as static for the device
  - IPv4 Subnet Mask:* Enter the Subnet Mask.
  - IPv4 Gateway:* Enter the Network Gateway's IPv4 Address.
  - Preferred IPv4 DNS:* Enter the Primary IPv4 DNS.
  - Alternate IPv4 DNS:* Enter the Alternate IPv4 DNS.
- **Frequency:** Set the GWN76xx's frequency, it can be either 2.4GHz, 5GHz or Dual-band.
- **Enable Band Steering:** When Frequency is set to Dual-Band, check this option to enable Band Steering on the Access Point, this will help redirecting clients to a radio band accordingly for efficient use and to benefit from the maximum throughput supported by the client.
- **Mode:** Choose the mode for the frequency band, 802.11n/g/b for 2.4Ghz and 802.11ac for 5Ghz.
- **Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high density environment.
- **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, it can be set it to be "Secondary Below Primary", "Primary Below Secondary" or "Auto".
- **Channel:** Select "Auto" or a specific channel. Default is "Auto". Note that the proposed channels depend on **Country** Settings under **System Settings-->Maintenance**.
- **Enable Short Guard Interval:** Check to activate this option to half the guard interval (from 800ns to 400ns) ensuring that distinct transmissions do not interfere with one another, this will help increasing throughput.
- **Active Spatial Streams:** Choose active spatial stream. Available options: "Auto", "1 stream", "2 streams" and "3 streams" (For GWN7610).



- **Radio Power:** Set the Radio Power depending on desired cell size to be broadcasted, three options are available: “Low”, “Medium” or “High”. Default is “High”.

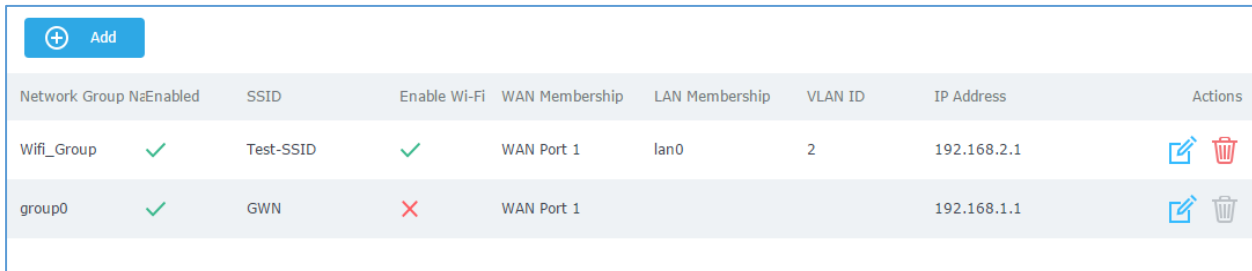
### Note

If a GWN76xx is not being paired, or the pair icon is grey color, make sure that it is not being paired with another GWN7000 Router or GWN76xx Access Point acting as Master Controller, if yes, it needs to be unpaired first, or reset to factory default settings to make it available for pairing.

## Network Groups

GWN7000 support creating up to 16 different Network groups separated by VLANs and adding paired GWN76xx Access Points.

To access Network Groups configuration page, log in to the GWN7000 WebGUI and go to **Network Group->Network Group**.









Network Group Name	Enabled	SSID	Enable Wi-Fi	WAN Membership	LAN Membership	VLAN ID	IP Address	Actions
Wifi_Group	✓	Test-SSID	✓	WAN Port 1	lan0	2	192.168.2.1	 
group0	✓	GWN	✗	WAN Port 1			192.168.1.1	 

Figure 15: Network Group

The GWN7000 will have a default network group named group0, click on  to edit it, or click on

 to add a new network group.

Basic
Wi-Fi
Device Membership

Network Group Name ?

Enabled

WAN Membership ?  ▼

LAN Membership ?  ▼

VLAN

VLAN ID

Enable IPv4 ?

IPv4 Static Address

IPv4 Subnet Mask

DHCP Enabled for IPv4

DHCP Start Address

DHCP End Address

**Figure 16: Add a New Network Group**





When editing or adding a new network group, following tabs will appear to configure a network group:

- **Basic:** Used to name the network group, and set a VLAN ID if adding a new network group, and addressing plans, refer to below table for each field.

**Table 17: Basic**

<b>Network Group Name</b>	Specifies the name for the network group.
<b>WAN Membership</b>	Select the WAN port membership. Or use Multi-WAN option if enabled under <b>Router-&gt;Port-&gt;Global Settings</b>
<b>LAN Membership</b>	Select the LAN port membership.



<b>VLAN</b>	Check to enable VLAN. This field is appearing only when having more than a network group.
<b>VLAN ID</b>	Set a VLAN ID. Valid range is between 2 and 4093.
<b>Enable IPv4</b>	Check to enable IPv4 addressing for this network group
<b>IPv4 Static Address</b>	Set a static IPv4 address for the network group when enabling IPv4.
<b>IPv4 Subnet Mask</b>	Set the Subnet Mask.
<b>DHCP Enabled for IPv4</b>	Check to enable DHCP using IPv4. This will allow clients connected to this network group to get IPv4 addresses automatically from GWN7000 acting as DHCP server.
<b>DHCP Start Address</b>	Set the starting IPv4 address for this network group's clients.
<b>DHCP End Address</b>	Set the ending IPv4 address for this network group's clients
<b>DHCP Lease Time</b>	Set the lease time for DHCP clients, the value can be defined in hours, minutes, or as "infinite". Default lease time is "12h".
<b>DHCPv4 Options</b>	<p>Set the DHCP options. Click on  to add another option, and  to delete an option.</p> <p><b>Example: 44,192.168.2.50</b> for DHCP option 44 and 192.168.2.50 is the WINS server's address.</p> <p>Please refer to the following link for DHCP options syntax:  <a href="https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq">https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq</a></p>
<b>DHCPv4 Relay Enabled</b>	Enable this option, if you want the GWN7000 relays the DHCP requests from clients to another DHCP server(s). Once checked Click on  to add another DHCPv4 Relay Target, and  to delete a DHCPv4 Relay Target.
<b>Enable IPv4</b>	Check to enable IPv6 addressing for this network group.
<b>IPv6 Relay from WAN</b>	Check to allow GWN7000 to relay IPv6 DHCP request from network group's clients to WAN port.
<b>DHCP Enabled for IPv6</b>	Check weather to enable IPv6 DHCP server for this network group.
<b>IPv6 Prefix for Assignment</b>	<p>Set the prefix value to be assigned to the network group. Valid range is between 1 to 64.</p> <p>Example: 64 will assign /64 prefixes.</p>
<b>IPv6 Subnet Hint</b>	Set the subnet mask value.
<b>IPv6 Uplink</b>	Select the WAN port.
<b>Enable Landing Page</b>	Check to enable landing page when connecting to this network group's Wi-Fi. This will allow setting a landing page URL where wireless users will be redirected automatically to the configured URL.
<b>Landing Page URL</b>	Set the landing page URL to which clients will be redirected once connected to the network group's Wi-Fi.



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

**Table 18: Wi-Fi**

<b>Enable Wi-Fi</b>	Check to enable Wi-Fi for the network group.
<b>SSID</b>	Set or modify the SSID name.
<b>SSID Hidden</b>	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, potential wireless clients will need to specify SSID name and authentication password manually.
<b>Security Mode</b>	Set the security mode for encryption, 5 options are available: <ul style="list-style-type: none"> <li>• <b>WEP 64-bit:</b> Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5.</li> <li>• <b>WEP 128-bit:</b> Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13.</li> <li>• <b>WPA/WPA2:</b> Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type.</li> <li>• <b>WPA2:</b> Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. Recommended configuration for authentication.</li> <li>• <b>Open:</b> No password is required. Users will be connected without authentication. Not recommended for security reasons.</li> </ul>
<b>Use MAC Filtering</b>	Choose Blacklist/Whitelist to specify MAC addresses to be excluded/included from connecting to the zone’s Wi-Fi. Default is Disabled.
<b>Client Isolation</b>	Client isolation feature blocks any TCP/IP connection between connected wireless clients via GWN76xx’s WiFi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi.  If enabled, the default LAN Gateway’s MAC address must be specified under <b>Gateway MAC Address</b> field. The clients will not be able to discover, ping or access other wireless devices connected to GWN7000’s network groups and only access to the default gateway, which usually means Internet access.



	<p>If disabled, clients will have full access to any device connected to the network, including wireless clients across network groups.</p> <p>Default is "Disabled".</p>
<b>Gateway MAC Address</b>	<p>This field is required when using <b>Client Isolation</b>, so users will not lose access to the Network (usually Internet).</p> <p>Type in the default LAN Gateway's MAC address (router's MAC address for instance) in hexadecimal separated by ":".</p> <p>Example: 00:0B:82:8B:4D:D8</p>
<b>RSSI Enabled</b>	<p>Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in <b>Minimum RSSI (dBm)</b>.</p>
<b>Minimum RSSI (dBm)</b>	<p>Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1".</p>

- **Device Membership:** Used to add or remove paired access points to the network group.

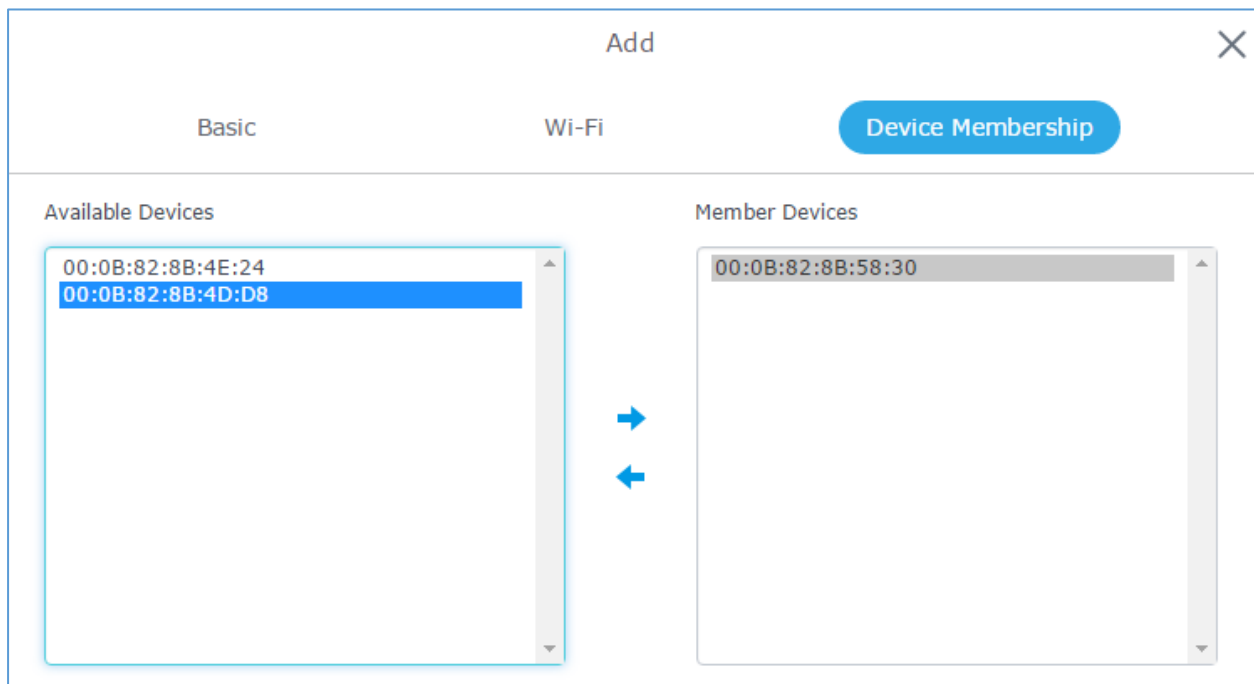





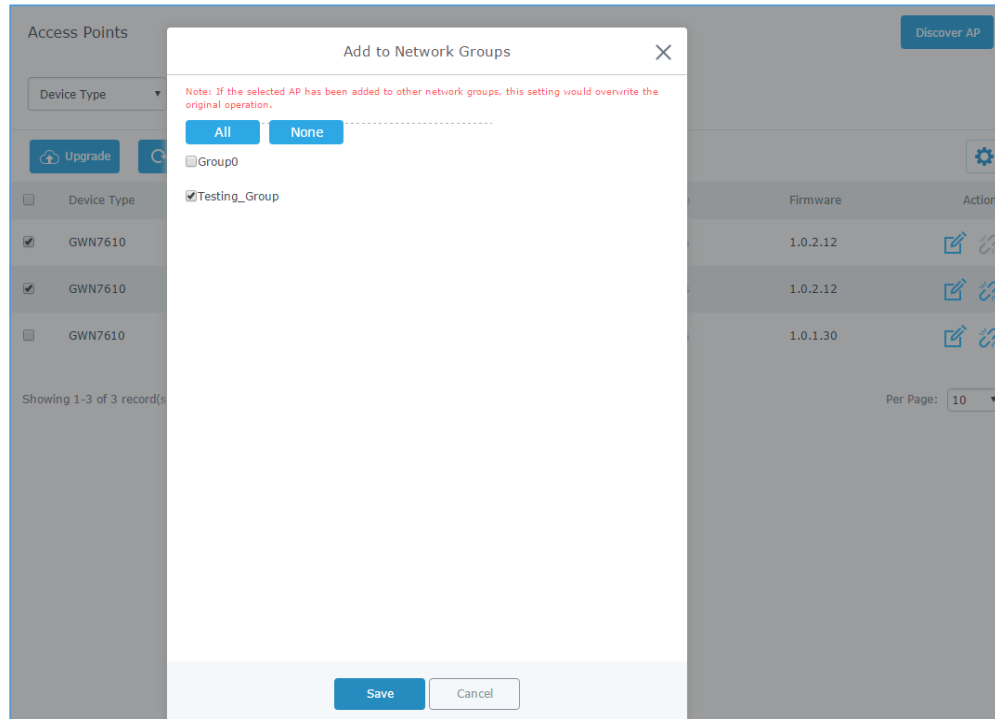
Figure 17: Device Membership

Click on  to add the GWN76xx to the network group, or click on  to remove it.



It is also possible to add a device to a Network Group from Access Points Page:

- Select the desired AP to add to a Network Group and click on 



**Figure 18: Add AP to Network Group from Access Points Page**

- Check to select the desired Network, on which the selected APs will be added, as shown in the above figure.

### Create an SSID under a Network Group

Under Network Group Page, click to edit a network group or create a new network group and go to Wi-Fi tab.





Add ✕

Basic
Wi-Fi
Device Membership

Enable Wi-Fi

SSID ?

SSID Hidden

Security Mode

WPA Key Mode

WPA Encryption Type

WPA Pre-Shared Key ?  👁

Use MAC Filtering

Client Isolation ?

Enable RSSI ?

Minimum RSSI (dBm) ?

Save
Cancel

**Figure 19: Create an SSID**

Refer to [Table 18: Wi-Fi] for Wi-Fi options.

### **Additional SSID under Same Network Group**

GWN7000 provides the ability to create an additional SSID under the same group.

To create an additional SSID go to **Network Group->Additional SSID**.



Add ✕

Enable Additional SSID

SSID ?

Network Group Membership ? group0 ▼

SSID Hidden ? group0  
Testing\_Group

Security Mode ? WPA2 ▼

WPA Key Mode ? PSK ▼

WPA Encryption Type ? AES ▼

WPA Pre-Shared Key ? •••••• ?

Use MAC Filtering ? Disabled ▼

Client Isolation ?

Enable RSSI ?

Minimum RSSI (dBm) ?

Save
Cancel

**Figure 20: Additional SSID**

Select one of the available network groups from **Network Group Membership** dropdown menu; this will create an additional SSID with the same Device Membership configured when creating the main network group.

SSID	Enabled	Network Group	Hidden	Security Mode	MAC Filtering	Client Isolati...	RSSI	Actions
Additional_SSID	✓	group0	✗	WPA2	Disabled	✗	✗	

**Figure 21: Additional SSID Created**

Click on to delete the additional SSID, or to edit it.























## CLIENTS CONFIGURATION

### Clients

Connected clients to different network groups can be shown and managed from a single interface.


Clients list can be accessed from GWN7000's **Web GUI** -> **Clients** to perform different actions to wired and wireless clients.

GWN7000 Enterprise Router with its DHCP server enabled on LAN ports level, will assign automatically an IP address to the devices connected to its LAN ports like a computer or GWN76xx access points and to wireless clients connected to paired GWN76xx access points.

MAC	Hostname	Type	IP Address	Radio/Channel Status	AP	Throughput	Aggregate	Actions
00:0B:82:76:F4:29		Wired	192.168.6.213	Offline	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
00:0B:82:75:21:20		Wired	192.168.6.141	Online	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
B0:83:FE:6D:3C:C6		Wired	192.168.6.237	Online	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
00:0B:82:6B:10:52		Wired	192.168.6.145	Offline	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
00:0B:82:5E:66:D9		Wired	192.168.6.229	Offline	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
24:77:03:C8:72:90	DESKTOP-1A7...	Wireless	192.168.6.150	5GHz 36 Offline	00:0B:82:8B:4E:28	TX:515B/s RX:0b/s	TX:5.61MB RX:6.78MB	 
24:77:03:F3:E4:14	DESKTOP-UDU...	Wireless	192.168.6.93	2.4GHz 1 Offline	00:0B:82:8B:4D:D4	TX:17.47KB/s RX:24.09KB/s	TX:34.95KB RX:48.18KB	 
A4:1F:72:6B:FD:09	EMEA-PC.Ian	Wired	192.168.6.74	Offline	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
88:51:FB:57:7D:B0	Surveillance-PC...	Wired	192.168.6.75	Online	Wired	TX:0b/s RX:0b/s	TX:0b RX:0b	 
F0:9A:51:0B:82:33	android-c887b...	Wireless	192.168.6.29	2.4GHz 1 Offline	00:0B:82:8B:4D:D4	TX:0b/s RX:0b/s	TX:652.51KB RX:113.40KB	 

Showing 61-70 of 123 record(s). ◀ 1 2 3 4 5 6 7 8 ... 12 13 ▶ Jump to:  Go Per Page: 10 ▼

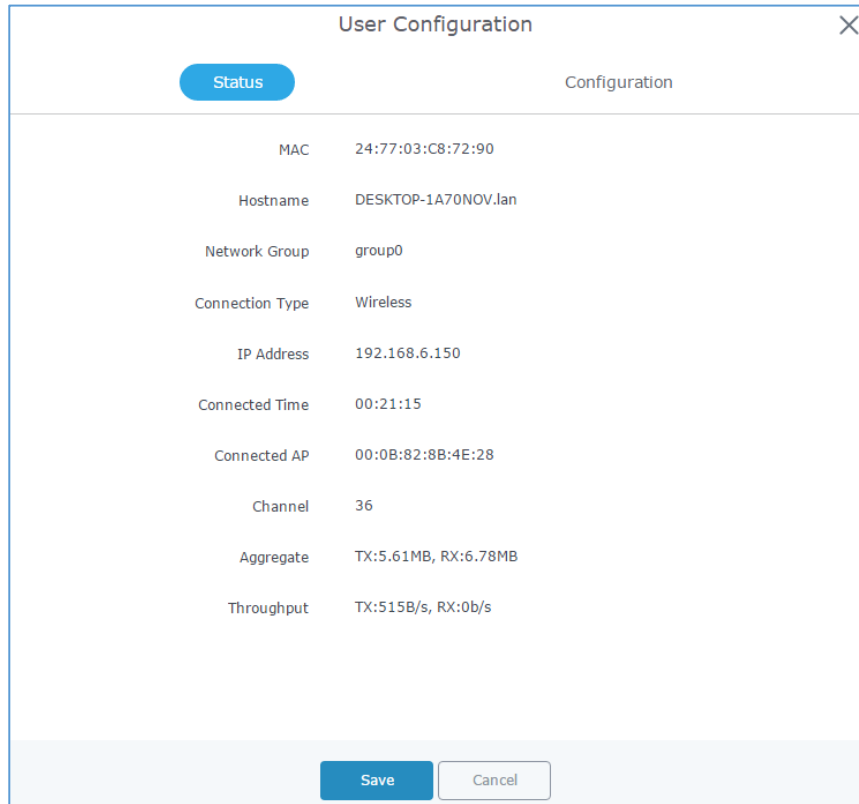
Figure 22: Clients

Click on  under Actions to check a client's status and modify its configuration.

### Status

Used to check user's basic information such as MAC address, IP address, which Network group does it belong to, and to which access point if it is a wireless client, as well as Throughput and Aggregate usage.

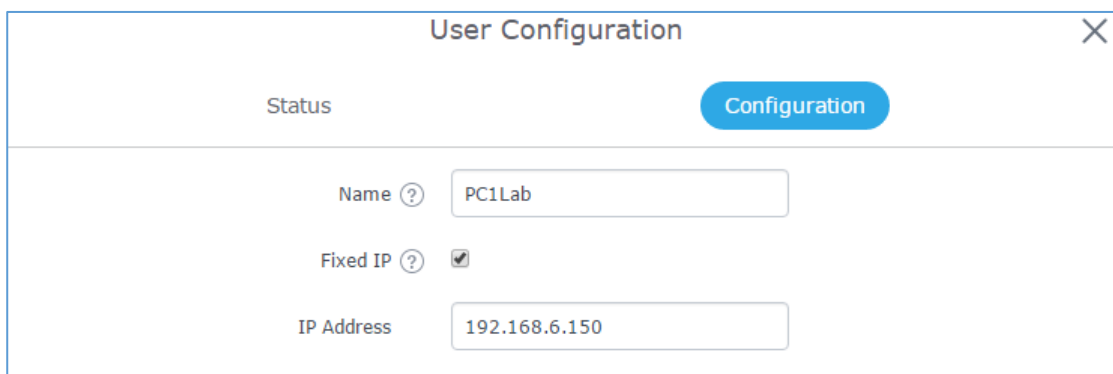




**Figure 23: Client's Status**

### Edit IP and Name


Configuration tab allowing to set a name for a client and set a static IP.





**Figure 24: Client's Configuration**



## Block a client

To block a client, click on  under actions, this will add automatically the blocked client to *Banned Client MAC* list under **Router->Port->Global Settings**.

MAC	Hostname	Type	IP Address	Radio/Channel	Status	AP	Throughput	Aggregate	Actions
C8:38:70:3C:11:A6	android-ce522...	Wireless	192.168.1.32	2.4GHz 11	Online 00:06:38	00:0B:82:8B:4E:24	TX:844B/s RX:1.14KB/s	TX:93.06KB RX:73.33KB	 



Showing 1-1 of 1 record(s) Per Page: 10 



Figure 25: Block a Client

To unban a client, go to **Router -> Port -> Global Settings**. Click on  to remove it from the banned list.

WAN Port Settings

WAN Port 1
WAN Port 2
Tunnel
LAN Port
Global Settings
Port Mirroring

Multi-WAN  Disabled

Banned Client MAC   


[Add new item](#) 

Figure 26: Unban Client



## VPN (VIRTUAL PRIVATE NETWORK)

### Overview

VPN allows the GWN7000 to be connected to a remote VPN server using PPTP, L2TP/IPSec and OpenVPN® protocols, or configure an OpenVPN® server and generate certificates and keys for clients, VPN page can be accessed from the GWN7000 Web GUI -> **VPN**.

### OpenVPN® Server Configuration


To use the GWN7000 as an OpenVPN® server, you will need to start creating OpenVPN® 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/clients certificates.

GWN7000 certificates can be managed from WebGUI -> **System Settings -> Cert. Manager**.

### 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. The 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 below steps:

1. Navigate to “**System Settings -> Cert. Manager -> CAs**” on the GWN7000 web GUI.
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 below figure showing an example of configuration and below table showing all available options with their respective description.



**Add**

Common Name	<input type="text" value="CATest"/>
Key Length	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="2048"/>
Digest Algorithm	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="SHA256"/>
Lifetime (days)	<input type="text" value="120"/>
Country Code	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="MA"/>
State or Province	<input type="text" value="Casablanca"/>
City	<input type="text" value="Casablanca"/>
Organization	<input type="text" value="GS"/>
Organization Unit	<input type="text" value="Gs"/>
Email Address	<input type="text" value="grandstream@gmail.com"/>



**Figure 27: Create CA Certificate**

**Table 19: CA Certificate**

Field	Description
<b>Common Name</b>	Enter the common name for the CA. It could be any name to identify this certificate. Example: "CATest".
<b>Key Length</b>	Choose the key length for generating the CA certificate.  Following values are available: <ul style="list-style-type: none"> <li><b>1024:</b> 1024-bit keys are no longer sufficient to protect against attacks.</li> <li><b>2048:</b> 2048-bit keys are a good minimum. (Recommended).</li> </ul>

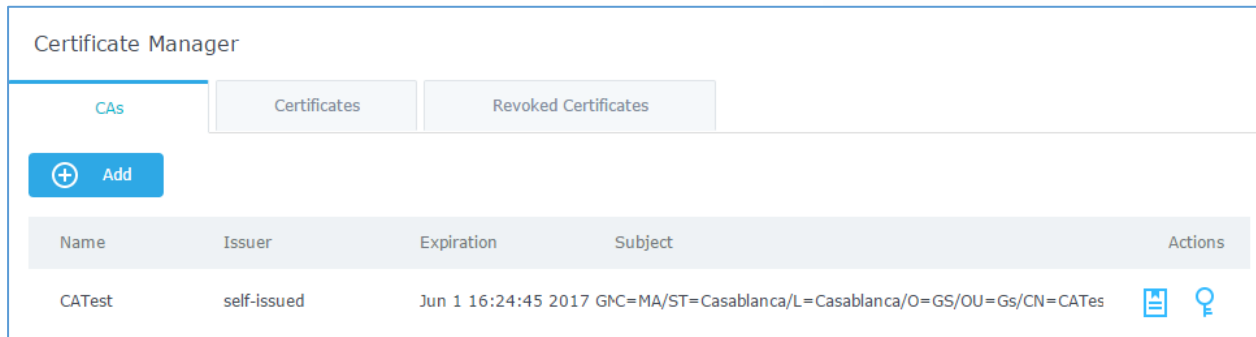


	<ul style="list-style-type: none"> <li>• <b>4096:</b> 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.</li> </ul>
<b>Digest Algorithm</b>	<p>Choose the digest algorithm:</p> <ul style="list-style-type: none"> <li>• <b>SHA1:</b> This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input.</li> <li>• <b>SHA-256:</b> This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back.</li> </ul>
<b>Lifetime (days)</b>	<p>Enter the validity date for the CA certificate in days. In our example, set to “120”.</p>
<b>Country Code</b>	<p>Select a country code from the dropdown list. Example: “MA”.</p>
<b>State or Province</b>	<p>Enter a state name or province. Example: “Casablanca”.</p>
<b>City</b>	<p>Enter a city name. Example: “Casablanca”.</p>
<b>Organization</b>	<p>Enter the organization name. Example: “GS”.</p>
<b>Organization Unit</b>	<p>Enter the organization unit name. Example: “Gs”.</p>
<b>Email Address</b>	<p>Enter an email address. Example: “grandstream@gmail.com”</p>

4. Click on  button after completing all the fields for the CA certificate.
5. Click on  button to export the CA to local computer. The CA file has extension “.crt”.








**Figure 28: CA Certificate**

## Generate Server/Client Certificates

Create both server and client certificates for encrypted communication between clients and GWN7000 acting as an OpenVPN® server.

### ❖ Creating Server Certificate

To create server certificate, follow below steps:

1. Navigate to **“System Settings -> Cert. Manager -> Certificates”**.
2. Click on  button. A popup window will appear.

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



**Add**

Common Name	<input type="text" value="ServerCertificate"/>
CA Certificate	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; padding-right: 5px; width: 100%;" type="text" value="CATest"/>
Certificate Type	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; padding-right: 5px; width: 100%;" type="text" value="Server"/>
Key Length	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; padding-right: 5px; width: 100%;" type="text" value="2048"/>
Digest Algorithm	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; padding-right: 5px; width: 100%;" type="text" value="SHA256"/>
Lifetime (days)	<input type="text" value="120"/>
Country Code	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; padding-right: 5px; width: 100%;" type="text" value="MA"/>
State or Province	<input type="text" value="Casablanca"/>
City	<input type="text" value="Casablanca"/>
Organization	<input type="text" value="GS"/>
Email Address	<input type="text" value="cert@grandstream.com"/>

**Figure 29: Generate Server Certificates**


**Table 20: Server Certificate**


Field	Description
<b>Common Name</b>	Enter the common name for the server certificate. It could be any name to identify this certificate. Example: "ServerCertificate".
<b>CA Certificate</b>	Select CA certificate previously generated from the drop down list. Example: "CATest".
<b>Certificate Type</b>	Choose the certificate type from the drop down list. It can be either a client or a server certificate. Choose "Server" to generate server certificate.




<b>Key Length</b>	<p>Choose the key length for generating the server certificate.</p> <p>Following values are available:</p> <ul style="list-style-type: none"> <li>• <b>1024:</b> 1024-bit keys are no longer sufficient to protect against attacks. Not recommended.</li> <li>• <b>2048:</b> 2048-bit keys are a good minimum. Recommended.</li> <li>• <b>4096:</b> 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.</li> </ul>
<b>Digest Algorithm</b>	<p>Choose the digest algorithm:</p> <ul style="list-style-type: none"> <li>• <b>SHA1:</b> This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input.</li> <li>• <b>SHA-256:</b> This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back</li> </ul>
<b>Lifetime (days)</b>	<p>Enter the validity date for the server certificate in days.</p> <p>In our example, set to “120”.</p>
<b>Country Code</b>	<p>Select a country code from the dropdown list.</p> <p>Example: “MA”.</p>
<b>State or Province</b>	<p>Enter a state name or province.</p> <p>Example: “Casablanca”.</p>
<b>City</b>	<p>Enter a city name.</p> <p>Example: “Casablanca”.</p>
<b>Organization</b>	<p>Enter the organization name.</p> <p>Example: “GS”.</p>
<b>Email Address</b>	<p>Enter an email address.</p> <p>Example: “Cert@grandstream.com”.</p>

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

Click on  button to export the server certificate file in “.crt” format.

Click on  button to export the server key file in “. key” format.



Click on  button to revoke the server certificate if no longer needed.


**Notes:**

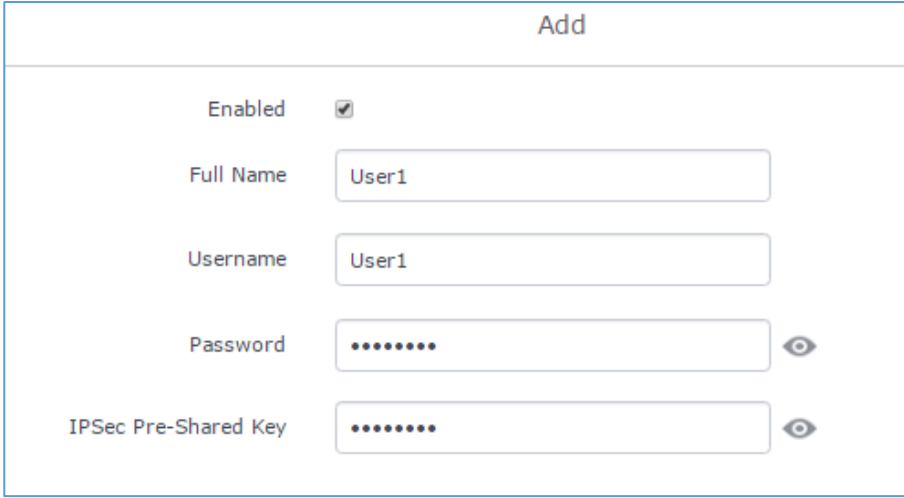
- The server certificates (.crt and .key) will be used by the GWN7000 when acting as a server.
- The server certificates (.crt and .key) can be exported and used on another OpenVPN® server.

❖ **Creating Client Certificate**

To create client certificate, follow below steps:

**1- Create Users**

- a. Navigate to “System Settings > User Manager”.
- b. Click on  button. The following window will pop up.



**Figure 30: User Management**

- c. Enter User information based on below descriptions.


Field	Description
<b>Enabled</b>	Check to enable the user.
<b>Full Name</b>	Choose full name to identify the users.
<b>Username</b>	Choose username to distinguish client’s certificate.



<b>Password</b>	Enter user password for each username.
<b>IPSec Pre-Shared Key</b>	Enter the pre-shared key to connect to VPN server. This field is used when clients are using pre-shared key.

- d. Repeat above steps for each user.

## 2- Create Client Certificate

- a. Navigate under “**System Settings -> Cert. Manager -> Certificates**”.
- b. Click on  button. The following window will pop up.
- c. Enter client certificate information based on below descriptions.



**Add**

Common Name	<input type="text" value="ClientCertificate"/>
CA Certificate	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="CATest"/> ▼
Certificate Type	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="Client"/> ▼
Username	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="User1"/> ▼
Key Length	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="2048"/> ▼
Digest Algorithm	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="SHA256"/> ▼
Lifetime (days)	<input type="text" value="120"/>
Country Code	<input style="border-bottom: 1px solid #ccc; text-align: right; font-size: 0.8em; color: #666; cursor: pointer; padding-right: 5px;" type="text" value="MA"/> ▼
State or Province	<input type="text" value="Casablanca"/>
City	<input type="text" value="Casablanca"/>
Organization	<input type="text" value="GS"/>
Email Address	<input type="text" value="user@grandstream.com"/>

**Figure 31: Client Certificat**

**Table 21: Client Certificat**



Field	Description
<b>Common Name</b>	Enter the common name for the client certificate. It could be any name to identify this certificate. Example: "ClientCertificate".
<b>CA Certificate</b>	Select the generated CA certificate from the drop down list.




<b>Certificate Type</b>	Choose the certificate type from the drop down list. It can be either a client or server certificate.
<b>Username</b>	Select created user to generate his certificate.
<b>Key Length</b>	Choose the key length for generating the client certificate. Following values are available: <ul style="list-style-type: none"> <li>• <b>1024:</b> 1024-bit keys are no longer sufficient to protect against attacks. Not recommended.</li> <li>• <b>2048:</b> 2048-bit keys are a good minimum. Recommended.</li> <li>• <b>4096:</b> 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.</li> </ul>
<b>Digest Algorithm</b>	Choose the digest algorithm: <ul style="list-style-type: none"> <li>• <b>SHA1:</b> This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input.</li> <li>• <b>SHA-256:</b> This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back</li> </ul>
<b>Lifetime (days)</b>	Enter the validity date for the client certificate in days. Example: "120".
<b>Country Code</b>	Select a country code from the dropdown list. Example: "MA".
<b>State or Province</b>	Enter a state name or province. Example: "Casablanca".
<b>City</b>	Enter a city name. Example: "Casablanca".
<b>Organization</b>	Enter the organization name. Example: "GS".
<b>Email Address</b>	Enter an email address. Example: "user@grandstream.com".

- d. Click on  after completing all the fields for the client certificate.



- e. Click on  to export the client certificate file in “.crt” format.
- f. Click on  to export the client key file in “.key” format.

Click on  to revoke the client certificate if no longer needed.

The client certificates (“.crt” and “.key”) will be used by clients connected to the GWN7000 in order to establish TLS handshake.


**Notes:**

- Client certificates generated from the GWN7000 need to be uploaded to the clients.
- For security improvement, each client needs to have his own 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 “VPN > OpenVPN® > Server”.

To create a new VPN server, follow below steps:

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





Add

---

Enabled

VPN Name

Server Mode

Protocol

Interface

Local Port

Encryption Algorithm

Digest Algorithm

TLS Authentication

Certificate Authority

Server Certificate

IPv4 Tunnel Network

Redirect Gateway

Automatic Firewall Rule

Auto Forward Group Traffic

LZO Compression

Allow Peer to Change IP

**Figure 32: Create OpenVPN® Server**

**Table 22: OpenVPN® Server**



Field	Description
<b>Enable</b>	Click on the checkbox in order to enable the OpenVPN® server feature.
<b>VPN Name</b>	Enter a name for the OpenVPN® server.
<b>Server Mode</b>	Choose the server mode the OpenVPN® server will operate with.



	<p>4 modes are available:</p> <ul style="list-style-type: none"> <li>• <b>PSK:</b> 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.</li> <li>• <b>SSL:</b> 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).</li> <li>• <b>User Auth:</b> 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).</li> <li>• <b>SSL + User Auth:</b> Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.  Most secure, as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).</li> </ul>
<b>Protocol</b>	Choose the Transport protocol from the dropdown list, either TCP or UDP. The default protocol is UDP.
<b>Interface</b>	Select the interface used to connect the GWN7000 to the uplink, either WAN1, WAN2 or All.
<b>Local Port</b>	Configure the listening port for OpenVPN® server. The default value is 1194.
<b>Encryption Algorithm</b>	Choose the encryption algorithm from the drop down list, in order to encrypt data so that the receiver can decrypt it using same algorithm.
<b>Digest Algorithm</b>	Choose the digest algorithm from the drop down 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.



<b>TLS Authentication</b>	<p>This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers.</p> <p>This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.</p>
<b>TLS Pre-Shared Key</b>	Enter the generated TLS Pre-Shared Key when using TLS Authentication.
<b>Certificate Authority</b>	Select a generated CA from the drop down list.
<b>Server Certificate</b>	Select a generated Server Certificate from the drop down list.
<b>IPv4 Tunnel Network</b>	<p>Enter the network range that the GWN7000 will be serving from to the OpenVPN® client.</p> <p><b>Note:</b> The network format should be the following <b>10.0.10.0/16</b>. The mask should be at least 16 bits.</p>
<b>Redirect Gateway</b>	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
<b>Automatic Firewall Rule</b>	Enable automatic firewall rule.
<b>Auto Forward Group Traffic</b>	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
<b>LZO Compression</b>	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.
<b>Allow Peer to Change IP</b>	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.



2. Click  after completing all the fields.
3. Click  on top of the WebGUI in order to apply changes.



OpenVPN®

Server Client

+ Add


Name	Enabled	IP Address	Uptime	Status	Throughput	Aggregate	Actions
GWNOpenVPNS...	✓	10.10.0.1	1m 50s	Connected	TX:0b/s RX:0b/s	TX:384.66KB RX:420B	 

Showing 1-1 of 1 record(s). Per Page: 10

Figure 33: OpenVPN®

## OpenVPN® Client configuration

The GWN7000 act as both, an OpenVPN® client and server, once users and **client certificate** created, navigate under “VPN > OpenVPN® > Client” and follow steps below:

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



Add

Enabled	<input checked="" type="checkbox"/>
VPN Name	<input type="text" value="OpenVPNClient"/>
Protocol <span style="font-size: small;">(?)</span>	<input style="border-bottom: 1px solid #ccc;" type="text" value="UDP"/> ▼
Interface	<input style="border-bottom: 1px solid #ccc;" type="text" value="WAN Port 1"/> ▼
Local Port <span style="font-size: small;">(?)</span>	<input type="text" value="1194"/>
Remote OpenVPN® Server <span style="font-size: small;">(?)</span>	<input type="text" value="192.168.5.143"/>
Remote OpenVPN® Server Port <span style="font-size: small;">(?)</span>	<input type="text" value="1194"/>
Auth Mode	<input style="border-bottom: 1px solid #ccc;" type="text" value="SSL"/> ▼
Encryption Algorithm	<input style="border-bottom: 1px solid #ccc;" type="text" value="BF-CBC"/> ▼
Digest Algorithm	<input style="border-bottom: 1px solid #ccc;" type="text" value="SHA1"/> ▼
TLS Authentication	<input type="checkbox"/>
Auto Forward Group Traffic <span style="font-size: small;">(?)</span>	<input checked="" type="checkbox"/>
Network Group <span style="font-size: small;">(?)</span>	<div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">All</span> <span style="background-color: #6c757d; color: white; padding: 2px 5px; border-radius: 3px;">None</span> </div> <hr style="border-top: 1px dashed #ccc; margin: 5px 0;"/> <input checked="" type="checkbox"/> group0
Routes	<input style="width: 100%;" type="text"/> <span style="color: #007bff; font-weight: bold; font-size: 1.2em;">+</span>
Don't Pull Routes	<input type="checkbox"/>
Force Default Route through S...	<input type="checkbox"/>
IP Masquerading <span style="font-size: small;">(?)</span>	<input type="checkbox"/>
LZO Compression <span style="font-size: small;">(?)</span>	<input style="border-bottom: 1px solid #ccc;" type="text" value="Yes"/> ▼
Allow Peer to Change IP <span style="font-size: small;">(?)</span>	<input type="checkbox"/>
CA Certificate <span style="font-size: small;">(?)</span>	<input style="width: 80%;" type="text" value="/data/vpn1-ca.crt"/> <input style="float: right;" type="button" value="Upload"/>
Client Certificate <span style="font-size: small;">(?)</span>	<input style="width: 80%;" type="text" value="/data/vpn1-client.pem"/> <input style="float: right;" type="button" value="Upload"/>
Client Private Key <span style="font-size: small;">(?)</span>	<input style="width: 80%;" type="text" value="/data/vpn1-server.key"/> <input style="float: right;" type="button" value="Upload"/>
Client Private Key Password	<input style="width: 100%;" type="password"/> <span style="font-size: 1.2em;">👁</span>

**Figure 34: OpenVPN® Client**



**Table 23: OpenVPN® Client**



Field	Description
<b>Enable</b>	Click on the checkbox to enable the OpenVPN® client feature.
<b>VPN Name</b>	Enter a name for the OpenVPN® client.
<b>Protocol</b>	Choose the Transport protocol from the dropdown list, either TCP or UDP. The default protocol is UDP.
<b>Interface</b>	Select the interface used to connect the GWN7000 to the uplink, either WAN1, WAN2 or All.
<b>Local Port</b>	Configure the listening port for OpenVPN® server. Default is 1194.
<b>Remote OpenVPN® Server</b>	Configure the remote OpenVPN® server IP address.
<b>Remote OpenVPN® Server Port</b>	Configure the remote OpenVPN® server port.
<b>Auth Mode</b>	<p>Choose the server mode the OpenVPN® server will operate with, 4 modes are available:</p> <ul style="list-style-type: none"> <li>• <b>PSK:</b> 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.</li> <li>• <b>SSL:</b> 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).</li> <li>• <b>User Auth:</b> 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).</li> <li>• <b>SSL + User Auth:</b> Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key.  Most secure, as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).</li> </ul>

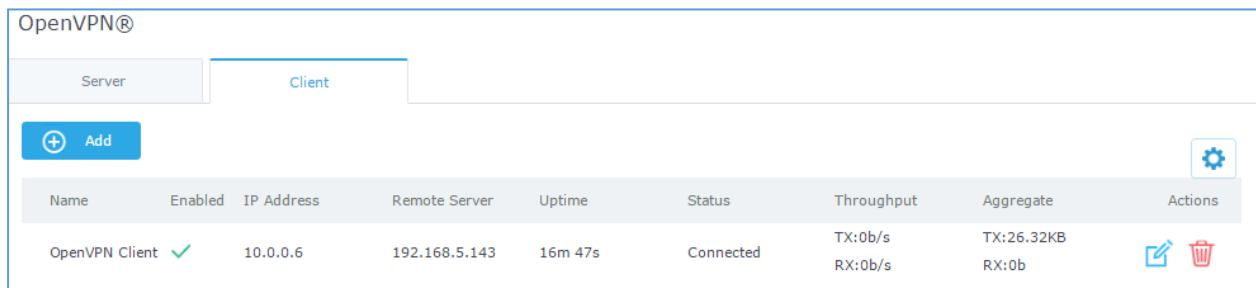


<b>Encryption Algorithm</b>	Choose the encryption algorithm from the drop down list, in order to encrypt data so that the receiver can decrypt it using the same algorithm.
<b>Digest Algorithm</b>	Choose the digest algorithm from the drop down list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
<b>TLS Authentication</b>	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.
<b>TLS Pre-Shared Key</b>	Enter the generated TLS Pre-Shared Key when using TLS Authentication.
<b>Auto Forward Group Traffic</b>	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
<b>Network Group</b>	Select the Network group to which the client belongs, or select All Network Groups.
<b>Routes</b>	This feature allows specifying and adding custom routes.
<b>Don't Pull Routes</b>	If enabled, client will ignore routes pushed by the server.
<b>Force Default Route through Server</b>	Force a default route to the server.
<b>IP Masquerading</b>	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.
<b>LZO Compression</b>	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.
<b>Allow Peer to Change IP</b>	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
<b>CA Certificate</b>	Click on "Upload" and select the "CA" certificate generated previously on this guide.
<b>Client Certificate</b>	Click on "Upload" and select the "Client Certificate" generated previously on this guide.



<b>Client Private Key</b>	Click on “Upload” and select the “Client Private Key” generated previously on this guide.
<b>Client Private Key Password</b>	Enter the client private key password

2. Click  after completing all the fields.
3. Click  on top of the webGUI in order to apply changes.




**Figure 35: OpenVPN® Client**

## L2TP/IPSEC 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.

### GWN7000 L2TP/IPSec Client Configuration

To configure L2TP client on the GWN7000, navigate under “VPN -> L2TP/IPSec” and set the following:

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





Enabled

VPN Name

WAN Port

Remote L2TP Server

Username

Password

Connection Type

Pre-Shared Key

Auto Forward Group Traffic

Network Group

---

group0

Remote Subnet

Use Tunnel as Default Route

IP Masquerading

Use DNS from Server

Number of Attempts to Reconn...

Use Builtin IPv6-management

Port Forwarding Rules

Port Trigger Rules

**Figure 36: L2TP Client Configuration**


**Table 24: L2TP Configuration**

Field	Description
<b>Enable</b>	Click on the checkbox in order to enable the L2TP client feature.
<b>VPN Name</b>	Enter a name for the L2TP client.
<b>WAN Port</b>	Select which WAN port is connected to the uplink, either WAN1 or WAN2.
<b>Remote L2TP Server</b>	Enter the IP/Domain of the remote L2TP Server.
<b>Username</b>	Enter the Username for authentication against the VPN Server.



<b>Password</b>	Enter the Password for authentication against the VPN Server.
<b>Connection Type</b>	<p>Select either Transport mode or Tunnel mode:</p> <ul style="list-style-type: none"> <li>• <b>Transport mode</b> is commonly used between end stations or between an end station and a gateway, if the gateway is being treated as a host.</li> <li>• <b>Tunnel mode</b> is used between gateways, or at an end station to a gateway, the gateway acting as a proxy for the hosts behind it.</li> </ul>
<b>Pre-Shared Key</b>	Enter the L2TP pre-shared key.
<b>Auto Forward Group Traffic</b>	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
<b>Remote Subnet</b>	<p>Configures the remote subnet for the VPN.</p> <p>The format should be “IP/Mask” where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32.</p> <p>For example: 192.168.5.0/24</p>
<b>Use Tunnel as Default Route</b>	Enable this option so that L2TP/IPSec VPN Tunnel will be used by default.
<b>IP Masquerading</b>	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.
<b>Use DNS from Server</b>	Enable this option to retrieve DNS from the VPN server.
<b>Number of Attempts to Reconnect</b>	Configures the number of attempts to reconnect the L2TP client, if this number is exceeded, the client will be disconnected from the L2TP/IP Server.
<b>Use Built-in IPv6 management</b>	Enable the IPv6 management for the VPN.
<b>Port Forwarding Rules</b>	Enter the port-forwarding rule to be used for the VPN.
<b>Port Trigger Rules</b>	Enter the port trigger rule to be used for the VPN.

2- Click  after completing all the fields.

3- Click  on top of the web GUI to apply changes.



+ Add										⚙️
Name	Enab... IP Address	Remote Server	Username	Uptime	Status	Throughput	Aggregate	Actions		
L2TP	✓ none	testvpn12tp.vpnazure.net	vpn		Connecting	TX:0b/s RX:0b/s	TX:83.77KB RX:0b			
Showing 1-1 of 1 record(s).										Per Page: 10 ▼


**Figure 37: 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 that enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet. Point-to-Point Tunneling Protocol (PPTP) allows the creation of virtual private networks (VPNs), which tunnel TCP/IP traffic through the Internet.

### GWN7000 Client Configuration

To configure PPTP client on the GWN7000, navigate under “**VPN -> PPTP**” and set the following:

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




Add

Enabled

VPN Name

Remote PPTP Server

Username

Password  

Auto Forward Group Traffic

Network Group

---

group0

Remote Subnet

Use Tunnel as Default Route

IP Masquerading

Use DNS from Server

Number of Attempts to Reconnect

Use Builtin IPv6-management

Port Forwarding Rules

Port Trigger Rules


**Figure 38: PPTP Client Configuration**


**Table 25: PPTP Configuration**



Field	Description
<b>Enable</b>	Click on the checkbox to enable the PPTP VPN client feature.
<b>VPN Name</b>	Enter a name for the PPTP client.
<b>Remote PPTP Server</b>	Enter the IP/Domain of the remote PPTP Server.
<b>Username</b>	Enter the Username for authentication against the VPN Server.
<b>Password</b>	Enter the Password for authentication against the VPN Server.



<b>Auto Forward Group Traffic</b>	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
<b>Remote Subnet</b>	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. For example: 192.168.5.0/24
<b>Use Tunnel as Default Route</b>	Enable this option so that PPTP VPN Tunnel will be used by default.
<b>IP Masquerading</b>	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.
<b>Use DNS from Server</b>	Enable this option to retrieve DNS from the VPN server.
<b>Number of Attempts to Reconnect</b>	Configures the number of attempts to reconnect the PPTP client, if this number is exceeded, the client will be disconnected from the PPTP Server.
<b>Use Built-in IPv6 management</b>	Enable the IPv6 management for the VPN.
<b>Port Forwarding Rules</b>	Enter the port-forwarding rule to be used for the VPN.
<b>Port Trigger Rules</b>	Enter the port trigger rule to be used for the VPN.

2- Click  after completing all the fields.

3- Click  on top of the webGUI to apply changes.

Name	Enabl...IP Address	Remote Server	Username	Uptime	Status	Throughput	Aggregate	Actions
PPTP VPN ✓	172.16.36.97	euro214.vpnbook.com	vpnbook	23m 31s	Connected	TX:0b/s RX:0b/s	TX:512B RX:616B	 

Showing 1-1 of 1 record(s). Per Page: 10 ▼

**Figure 39: PPTP Client**



## FIREWALL

GWN7000 supports firewall feature to control incoming and outgoing traffic by restricting or rejecting specific traffic, as well as preventing attacks to the GWN7000 networks for enhanced security.

The Firewall feature includes 3 menus:

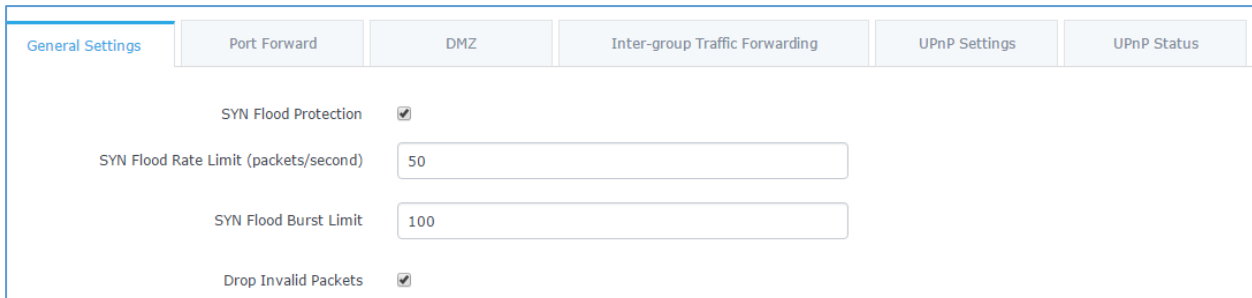
- **Basic Settings:** Used to enable SYN Flood, setup port forwarding, DMZ, inter-group traffic forwarding and UPnP.
- **Traffic Rules:** Used to control incoming/outgoing traffic in customized scheduled times, and taking actions for specified rules such as Accept; Reject and Drop.
- **Advanced:** Used to setup SNAT and DNAT.

### Basic Settings

#### General Settings

SYN Flood Protection is used to avoid DOS attacks.

SYN Flood Protection is enabled by default on GWN7000, you can edit the “SYN Flood Rate Limit”, “SYN Flood Burst Limit” and whether to drop or no the invalid packets as shown in the below screenshot





General Settings	Port Forward	DMZ	Inter-group Traffic Forwarding	UPnP Settings	UPnP Status
SYN Flood Protection	<input checked="" type="checkbox"/>				
SYN Flood Rate Limit (packets/second)	<input type="text" value="50"/>				
SYN Flood Burst Limit	<input type="text" value="100"/>				
Drop Invalid Packets	<input checked="" type="checkbox"/>				

**Figure 40: Basic->General Settings**

### Port Forwarding






Port forwarding allows redirecting a communication request from one address and port number combination to another.

Below are different possible actions:

- To add a Port Forward rule, click on  .
- To edit a Port Forward rule, click on  .



- To delete a Port Forward rule, click on  .

Firewall Basic Settings																	
General Settings		Port Forward		DMZ		Inter-group Traffic Forwarding		UPnP Settings		UPnP Status							
<div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px; display: inline-block;">  Add         </div>																	
Name	Enabled	Protocol	Src Group	Src Port(s)	Dest Group	Dest IP	Dest Port(s)	Actions									
HTTPs	✓	TCP/UDP	WAN Port 1	7777	group0	192.168.1.1	443	 									
GWN7610	✓	TCP/UDP	WAN Port 1	8888	group0	192.168.1.76	443	 									

**Figure 41: Port Forward**




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

**Table 26: Port Forward**

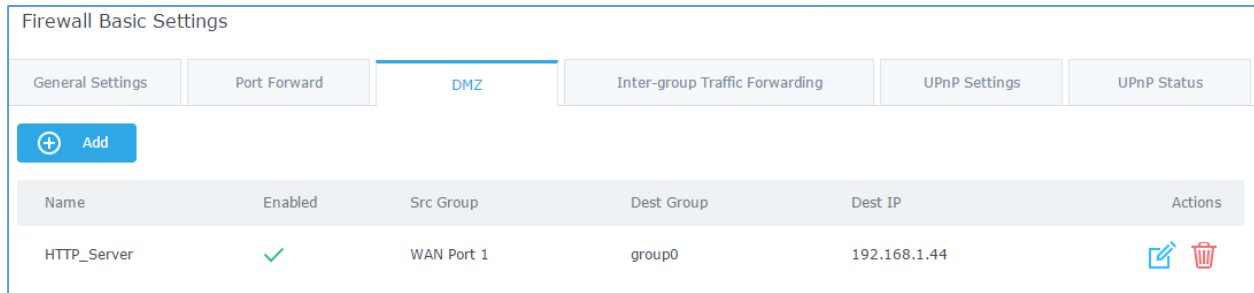
<b>Name</b>	Specify a name for the port forward rule.
<b>Enabled</b>	Check to enable this port forward rule.
<b>Protocol</b>	Select a protocol, users can select TCP, UDP or TCP/UDP.
<b>Source Group</b>	Select the WAN Interface.
<b>Source Port</b>	Set the Source Port number.
<b>Destination Group</b>	Select the LAN group.
<b>Destination IP</b>	Set the destination IP address.
<b>Destination Port</b>	Set the Destination Port number.

## DMZ

GWN7000 support DMZ, where it is possible to specify a LAN client to be put on the DMZ.

- To add an IP into the DMZ, click on  Add .
- To edit a DMZ entry, click on  .
- To delete a DMZ entry, click on  .





**Figure 42: DMZ**

Refer to below table for DMZ fields:

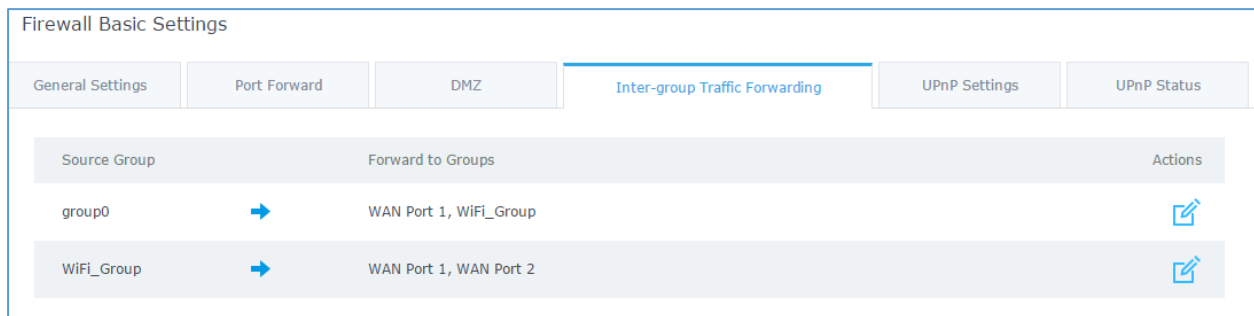
**Table 27: DMZ**

<b>Name</b>	Specify a name for the DMZ entry.
<b>Enabled</b>	Check to enable this DMZ entry.
<b>Source Group</b>	Select the WAN interface
<b>Destination Group</b>	Select the LAN group.
<b>Destination IP</b>	Set the destination IP address.




## Inter-Group Traffic Forwarding

GWN7000 offers the possibility to allow traffic between different groups and interfaces.

Users can select to edit a source group and add to it other network groups and WAN interfaces to allow inter-group traffic between the selected members.

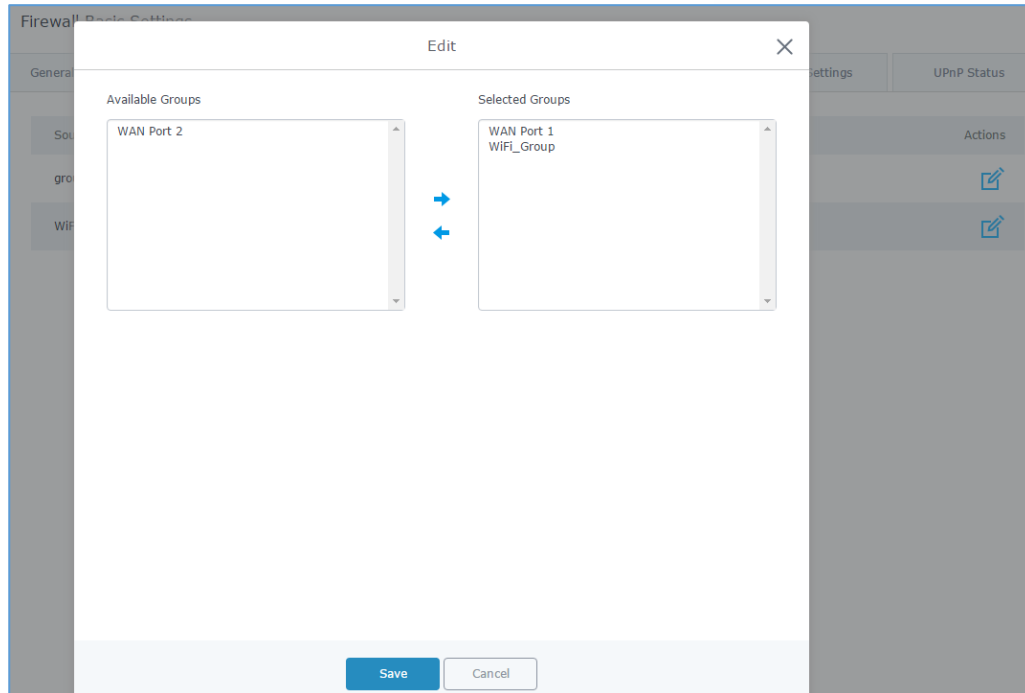


**Figure 43: Inter-group Traffic Forwarding**

Click on  next to source group, and click on  to add groups and interfaces to selected groups, or click on  to remove members from selected groups as shown in below figure







**Figure 44: Enabling inter-group traffic**

## UPnP

GWN7000 supports UPnP that enables programs running on a host to configure automatically port forwarding.

UPnP allows a program to make the GWN7000 to open necessary ports, without any intervention from the user, without making any check.

UPnP settings can be accessed from GWN7000 WebGUI->**Firewall->Basic->UPnP Settings**.

Refer to below Table for UPnP settings.

**Table 28: UPnP Settings**




<b>Enable Daemon</b>	Check to enable Daemon for UPnP.
<b>External Interface</b>	Select the WAN interface to allow external connection to resources that enables UPnP.
<b>Internal Interface</b>	Check the LAN network group on which to activate UPnP.
<b>Enable UPnP</b>	Check to Enable UPnP for the LAN clients on selected network group.
<b>Enable NAT-PMP</b>	Check to enable automatic NAT Port Mapping (NAT-PMP).
<b>Secure Mode</b>	Check to activate secure mode for devices that activate UPnP.
<b>Logging to Syslog</b>	Choose whether to log activities for UPnP into Syslog.
<b>Download Speed</b>	Set the Download speed value in KB/s. Default is 2048
<b>Upload Speed</b>	Set the Upload speed value in KB/s. Default is 1024.

























## Traffic Rules Settings

GWN7000 offers the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times, and taking actions for specified rules such as Accept; Reject and Drop.

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

- To add new rule, Click on  Add .
- To edit a rule, Click on  .
- To delete a rule, Click on  .

Firewall Traffic Rules Settings									
Input		Output		Forward					
All Input Rules		<input checked="" type="checkbox"/> Show default rules		 Add					
Name	Enabled	Protocol	Src	Src Port(s)	Src MAC	Dest Port(s)	Schedule	Firewall Actio..	Actions
Allow-DHCP	<input checked="" type="checkbox"/>	IPv4 UDP	WAN Port 1			68		Accept	  
Allow-Ping	<input checked="" type="checkbox"/>	IPv4 ICMP	WAN Port 1					Accept	  
Allow-IGMP	<input checked="" type="checkbox"/>	IPv4 IGMP	WAN Port 1					Accept	  
Allow-DHCPv6	<input checked="" type="checkbox"/>	IPv6 UDP	WAN Port 1		fe80::/10	546		Accept	  
Allow-MLD	<input checked="" type="checkbox"/>	IPv6 ICMP	WAN Port 1		fe80::/10			Accept	  
Allow-ICMPv6	<input checked="" type="checkbox"/>	IPv6 ICMP	WAN Port 1					Accept	  
Allow-DHCPv6	<input checked="" type="checkbox"/>	IPv4 UDP	WAN Port 2			68		Reject	  





**Figure 45: Traffic Rules Settings**

Refer to below table for each tab, when editing or creating a traffic rule:

**Table 29: Firewall Traffic Rules**

<b>Name</b>	Specify a name for the traffic rule.
<b>Enabled</b>	Check to enable this rule.
<b>IP Family</b>	Select the IP version, three options are available: IPv4, IPv6 or Any.
<b>Source Group</b>	Select a WAN interface or a LAN group for Source Group, or select All.
<b>Protocol</b>	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP, UDP-Lite, ICMP, AH, SCTP, IGMP and All.
<b>Source IP Address</b>	Set the Source IP address, it can be an IPv4 or IPv6 address.
<b>Source MAC address</b>	Set the Source MAC address.



<b>Schedule Start Date</b>	Click on  icon to schedule a start date for this rule to be applied.
<b>Schedule End Date</b>	Click on  icon to schedule an end date for this rule to cease effect.
<b>Schedule Start Time</b>	Click on  icon to schedule a start time for this rule to be applied.
<b>Schedule End Time</b>	Click on  icon to schedule an end time for this rule to cease effect.
<b>Schedule Weekdays List of Weekdays</b>	Select the days, on which the traffic rule will be applied, the unselected days will ignore this rule.
<b>Schedule Days of the Month</b>	Enter the days of the months (separated by space) on which the traffic rule will be applied. Example: 5 10 15 This will be applied only on 5 <sup>th</sup> , 10 <sup>th</sup> and 15 <sup>th</sup> day monthly.
<b>Treat Time Values as UTC Instead of Local Time</b>	Check to use UTC as time zone for the specified times, instead of using GWN7000's local time.
<b>Firewall Action</b>	Select which action to perform for the given traffic rule, 3 options are available: Accept, Reject or Drop.

## Firewall Advanced Settings

Firewall Advanced Settings page provides the ability to setup input/output policies for each WAN interface and LAN groups; as well as setting configuration for Static and Dynamic NAT.

### General Settings

Click on  next to a WAN interface or Network group to edit its input and output policies.

Refer to below table for general settings options

**Table 30: Firewall-General Settings**




<b>Input Policy</b>	Select which action to apply to all incoming traffic to this interface/LAN group, 3 actions are available: Accept, Reject and Drop.
<b>Output Policy</b>	Select which action to apply to all outgoing traffic from this interface/LAN group, 3 actions are available: Accept, Reject and Drop.
<b>IP Masquerading</b>	Check to enable IP Masquerading, this will allow 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.



<b>MSS Clamping</b>	Check to enable MSS Clamping. This will provide a method to prevent fragmentation when the MTU value on the communication path is lower than the MSS value.
<b>Log Dropped and Reject Traffic to Syslog</b>	Check to send all rejected and dropped traffic logs to configured Syslog Server.
<b>Limit for Dropped and Rejected Traffic</b>	Specify the limit for dropped and reject traffic. The value format is N/unit, where N is a digit number, and unit can either be in second, minute, hour or day.



## SNAT

Following actions are available for SNAT.



- To add new SNAT entry, click on  Add .
- To edit a SNAT entry, click on  .
- To delete a SNAT rule, click on  .

Refer to below table when creating or editing an SNAT entry

**Table 31: SNAT**




<b>Name</b>	Specify a name for the SNAT entry
<b>Enabled</b>	Check to enable this SNAT entry.
<b>IP Family</b>	Select the IP version, three options are available: IPv4, IPv6 or Any.
<b>Source Group</b>	Select a WAN interface or a LAN group for Source Group, or select All.
<b>Destination Group</b>	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.
<b>Protocol</b>	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
<b>Source IP</b>	Set the Source IP address.
<b>Rewrite IP</b>	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
<b>Destination IP</b>	Set the Destination IP address.
<b>Schedule Start Date</b>	Click on  icon to schedule a start date for this SNAT entry to be applied.
<b>Schedule End Date</b>	Click on  icon to schedule an end date for this SNAT entry to end.



<b>Schedule Start Time</b>	Click on  icon to schedule a start time for this SNAT entry to be applied.
<b>Schedule End Time</b>	Click on  icon to schedule an end time for this SNAT entry to end.
<b>Schedule Weekdays List of Weekdays</b>	Select the days, on which the SNAT entry will be applied, the unselected days will ignore this rule.
<b>Schedule Days of the Month</b>	Enter the days of the months (separated by space) on which the SNAT entry will be applied. Example: 5 10 15 This will be applied only on 5 <sup>th</sup> , 10 <sup>th</sup> and 15 <sup>th</sup> day monthly.
<b>Treat Time Values as UTC Instead of Local Time</b>	Check to use UTC as time zone for the specified times, instead of using GWN7000's local time.

## DNAT

Following actions are available for DNAT:





- To add new DNAT entry, click on  .
- To edit a DNAT entry, click on  .
- To delete a DNAT rule, click on  .

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

**Table 32: DNAT**

<b>Name</b>	Specify a name for the DNAT entry
<b>Enabled</b>	Check to enable this DNAT entry.
<b>IP Family</b>	Select the IP version, three options are available: IPv4, IPv6 or Any.
<b>Source Group</b>	Select a WAN interface or a LAN group for Source Group, or select All.
<b>Destination Group</b>	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.
<b>Protocol</b>	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
<b>Source IP</b>	Set the Source IP address.
<b>Rewrite IP</b>	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
<b>Destination IP</b>	Set the Destination IP address.



<b>Schedule Start Date</b>	Click on  icon to schedule a start date for this DNAT entry to be applied.
<b>Schedule End Date</b>	Click on  icon to schedule an end date for this DNAT entry to end.
<b>Schedule Start Time</b>	Click on  icon to schedule a start time for this DNAT entry to be applied.
<b>Schedule End Time</b>	Click on  icon to schedule an end time for this DNAT entry to end.
<b>Schedule Weekdays List of Weekdays</b>	Select the days, on which the DNAT entry will be applied, the unselected days will ignore this rule.
<b>Schedule Days of the Month</b>	Enter the days of the months (separated by space) on which the DNAT entry will be applied. Example: 5 10 15 This will be applied only on 5 <sup>th</sup> , 10 <sup>th</sup> and 15 <sup>th</sup> day monthly.
<b>Treat Time Values as UTC Instead of Local Time</b>	Check to use UTC as time zone for the specified times, instead of using GWN7000's local time.
<b>Enable NAT Reflection</b>	Check to enable NAT Reflection for this DNAT entry to allow the access of a service via the public IP address from inside the local network.



## MAINTENANCE AND TROUBLESHOOTING

GWN7000 offers multiple tools and options for maintenance and debugging to help further troubleshooting and monitoring the GWN7000 resources.

### Maintenance

Maintenance page can be accessed from GWN7000 WebGUI-> **System Settings-> Maintenance**. Refer to below table for maintenance tabs and fields.

**Table 33: Maintenance**

Basic	
<b>Country</b>	Select the country from the drop-down list.
<b>Time Zone</b>	Configure time zone for the GWN7000. Please reboot the device to take effect.
<b>NTP Server</b>	Configure the IP address or URL of the NTP server, the device will obtain the date and time from the configured server.
<b>Date Display Format</b>	Change the Date Display Format, three options are possible YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY
Upgrade	
<b>Authenticate Config File</b>	Authenticate configuration file before acceptance. Default is disabled.
<b>XML Config File Password</b>	Enter the password for encrypting the XML configuration file using OpenSSL. The password is used to decrypt the XML configuration file if it is encrypted via OpenSSL.
<b>Upgrade Via</b>	Specify uploading method for firmware and configuration. 3 options are available: HTTP, HTTPS and TFTP.
<b>Firmware Server</b>	Configure the IP address or URL for the firmware upgrade server.
<b>Config Server</b>	Configure the IP address or URL for the configuration file server.
<b>Check Update on Boot</b>	Choose whether to enable or disable automatic upgrade and provisioning after reboot. Default is disabled.
<b>Automatic Upgrade Check Interval(m)</b>	Specify the time period to check for firmware upgrade (in minutes).
<b>Reboot</b>	Click on Reboot button to reboot the device
<b>Download Configuration</b>	Click on Download to download the device's configuration file.
<b>Upgrade Now</b>	Click on Upgrade, to launch firmware/config file provisioning. Please make sure to Save and Apply changes before clicking on Upgrade.
<b>Factory Reset</b>	Click on Reset to restore the GWN7000 as well as all online GWN76xx units to factory default settings



Access	
<b>Current Administrator Password</b>	Enter the current administrator password
<b>New Administrator Password</b>	Change the current password. This field is case sensitive with a maximum length of 32 characters.
<b>Confirm New Administrator Password</b>	Enter the new administrator password one more time to confirm.
<b>User Password</b>	Configure the password for user-level Web GUI access. This field is case sensitive with a maximum length of 32 characters.
<b>User Password Confirmation</b>	Enter the new User password again to confirm.
Syslog	
<b>Syslog Server</b>	Enter the IP address or URL of Syslog server. Please reboot the GWN7000 to take effect.
<b>Syslog Level</b>	Select the level of Syslog, 5 levels are available: <b>None</b> , <b>Debug</b> , <b>Info</b> , <b>Warning</b> and <b>Error</b> . Please reboot the GWN7000 to take effect.

## Debug


Many debugging tools are available on GWN7000's WebGUI to check the status and troubleshoot GWN7000's services and networks.

Debug page offers 4 tabs: Capture, Ping/Traceroute, Syslog and Nat Table.

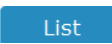
### Capture

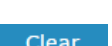

This section is used to capture packet traces from the GWN7000 interfaces (WAN ports and network groups) for troubleshooting purpose or monitoring...

It is needed to plug an USB storage device to one of the USB ports on the back of the GWN7000.

Click on  to start capturing on a certain device plugged to the USB port.

Click on  to stop the capture.



Click on  to show the captured files on a chosen device, and the capture files details will appear,

click on  to delete all files, click on  next to a capture file to download it on a local folder, or

click on  to delete it.





Captured File List				
Device <span>?</span> PARTITION A				List
				Clear
File Name	File Size	File Count	Last Modified	Actions
capture_09-02-16_09h-03m-08s	19.76 MB	1	09-02-2016 09:06:24	 

**Figure 46: Capture Files**

The below table will show different fields used on capture page

**Table 34: Debug-Capture**

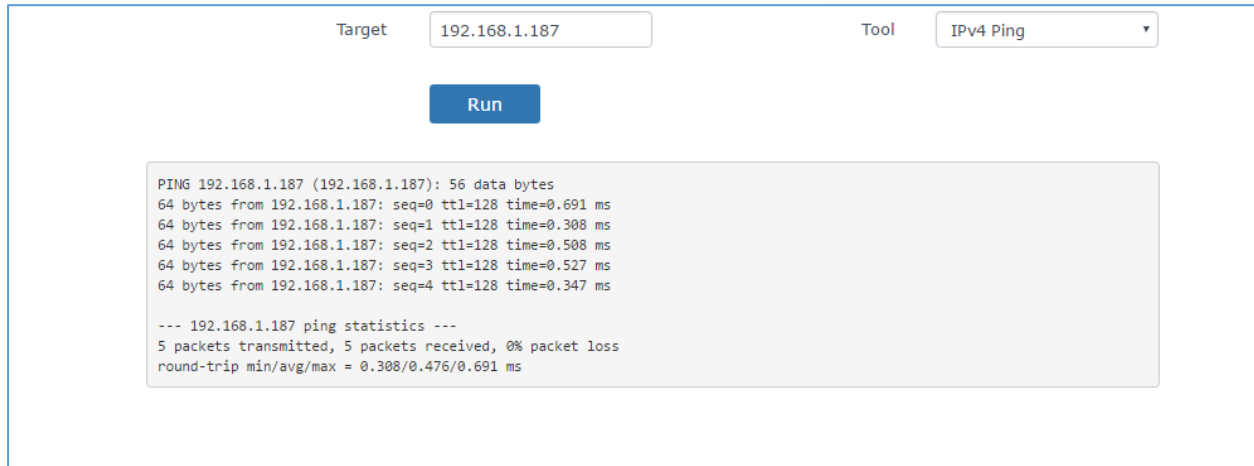
<b>File Name</b>	Enter the name of the capture file that will be generated.
<b>Interface</b>	Choose an Interface (WAN port1 or 2, or a network group) from where to begin the capture.
<b>Device</b>	Choose a device plugged to USB port to save the capture once started.
<b>File Size</b>	Set a File size that the capture will not exceed (Optional field).
<b>Rotate Count</b>	Set a value for rotating captures (Optional Field).
<b>Direction</b>	Choose if you want to get all traffic or only outgoing or incoming to the chosen interface.
<b>Source Port</b>	Set the Source Port to filter capture traffic coming from the defined source port.
<b>Destination Port</b>	Set the Destination Port to filter capture traffic coming from the defined port.
<b>Source IP</b>	Set the Source IP to filter capture traffic coming from the defined source IP.
<b>Dest IP</b>	Set the Destination IP to filter capture traffic coming from the defined destination IP.
<b>Protocol</b>	Choose ALL or a specific protocol to capture (IP, ARP, RARP, TCP, UDP, ICMP, IPv6)

## Ping/Traceroute

Ping and Traceroute are useful debugging tools to verify reachability with other clients across the network (WAN or LAN). The GWN7000 offers both Ping and Traceroute tools for IPv4 and IPv6 protocols.

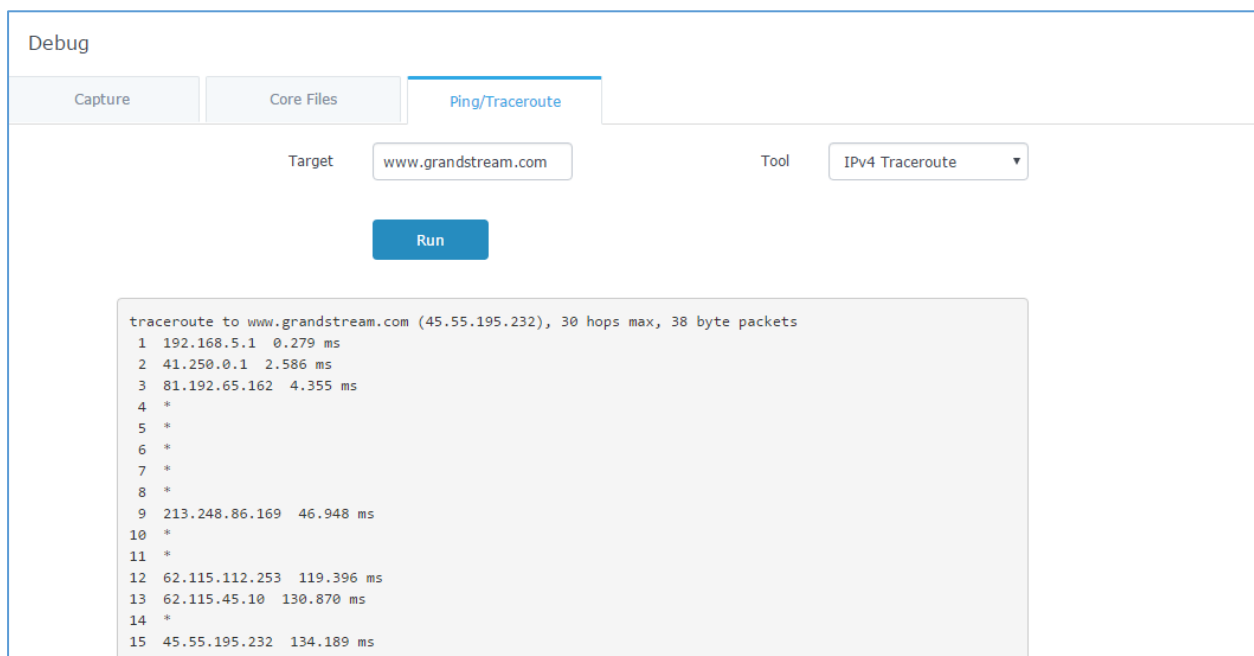
To use these tools, go to GWN7000 WebGUI->**System Settings->Debug** and click on **Ping/Traceroute**.





**Figure 47: IP Ping**

- Next to **Tool** choose from the dropdown menu:
  - IPv4 Ping for an IPv4 Ping test to Target
  - IPv6 Ping for an IPv6 Ping test to Target
  - IPv4 Traceroute for an IPv4 Traceroute to Target
  - IPv6 Traceroute for an IPv6 Traceroute to Target
- Type in the destination's IP address/domain name in **Target** field.
- Click on **Run**.



**Figure 48: Traceroute**

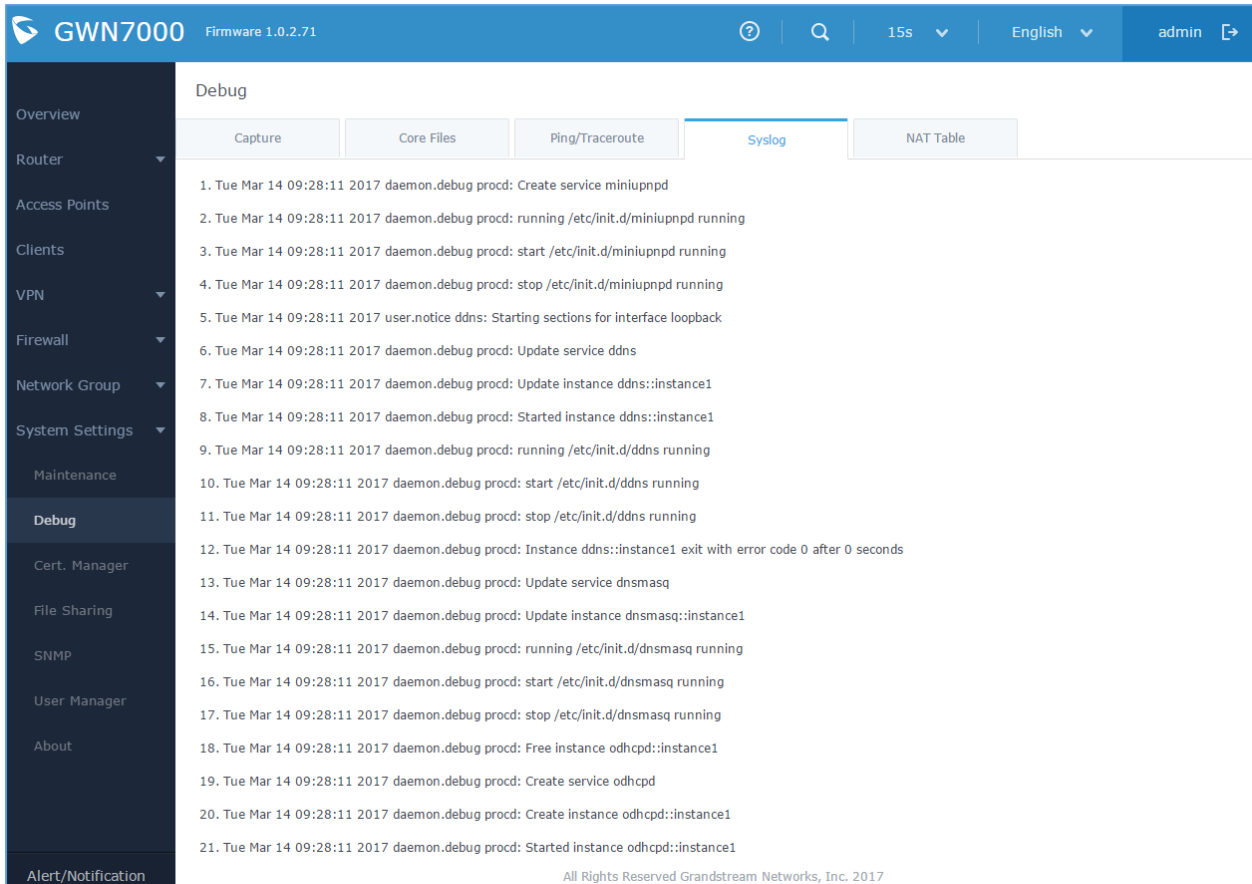


## Syslog

GWN7000 supports dumping the syslog information to a remote server under Web GUI ->**System Settings->Maintenance->Syslog**.

Enter the syslog server hostname or IP address and select the level for the syslog information. Five levels of syslog are available: None, Debug, Info, Warning, and Error.

Syslog messages are also displayed in real time under Web GUI ->**System Settings->Debug->Syslog**.



The screenshot shows the GWN7000 Web GUI interface. The top navigation bar includes the device name 'GWN7000', firmware version '1.0.2.71', a search icon, a refresh button labeled '15s', a language dropdown set to 'English', and a user profile 'admin'. The left sidebar contains a menu with categories like Overview, Router, Access Points, Clients, VPN, Firewall, Network Group, System Settings, Maintenance, Debug, Cert. Manager, File Sharing, SNMP, User Manager, and About. The 'Debug' category is selected, and the 'Syslog' sub-tab is active. The main content area displays a list of 21 syslog messages, each with a timestamp and a detailed log entry. The messages describe the startup and configuration of various services such as miniupnpd, ddns, and dnsmasq. At the bottom of the interface, there is a footer that reads 'All Rights Reserved Grandstream Networks, Inc. 2017'.

**Figure 49: Syslog**

## NAT Table

NAT table is updated dynamically on GWN7000's WebGUI, to check the NAT table go to **System Settings->Debug->NAT Table**.




Protocol	Expires	Source	Destination	Source Port	Dest Port	TX / RX Packets	TX / RX Bytes
<b>IPv4 Connections</b>							
TCP	9	192.168.5.106	192.168.5.139	49886	443	6 / 6	409B / 828B
TCP	60	192.168.5.106	192.168.5.139	49912	443	7 / 7	1.07KB / 1.62KB
TCP	90	192.168.5.106	192.168.5.139	49935	443	4 / 6	317B / 828B
TCP	60	192.168.5.106	192.168.5.139	49901	443	6 / 6	409B / 828B
UDP	30	127.0.0.1	127.0.0.1	52441	53	1 / 1	53B / 53B
TCP	75	192.168.5.106	192.168.5.139	49926	443	8 / 8	1.58KB / 1.65KB
UDP	45	127.0.0.1	127.0.0.1	47074	53	1 / 1	53B / 53B
TCP	103	192.168.5.106	192.168.5.139	49943	443	7 / 7	1.07KB / 1.64KB
TCP	90	192.168.5.106	192.168.5.139	49936	443	8 / 8	1.58KB / 1.65KB
UDP	0	127.0.0.1	127.0.0.1	59067	53	1 / 1	53B / 53B
<b>IPv6 Connections</b>							
Protocol	Expires	Source	Destination	Source Port	Dest Port	TX / RX Packets	TX / RX Bytes
Showing 1-10 of 140 record(s).							
<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> <input type="button" value="6"/> <input type="button" value="7"/> <input type="button" value="8"/> <input type="button" value="..."/> <input type="button" value="13"/> <input type="button" value="14"/> <input type="button" value="▶"/>							
Jump to: <input type="text"/> <input type="button" value="Go"/>							
Per Page: <input type="text" value="10"/>							
All Rights Reserved Grandstream Networks, Inc. 2016							

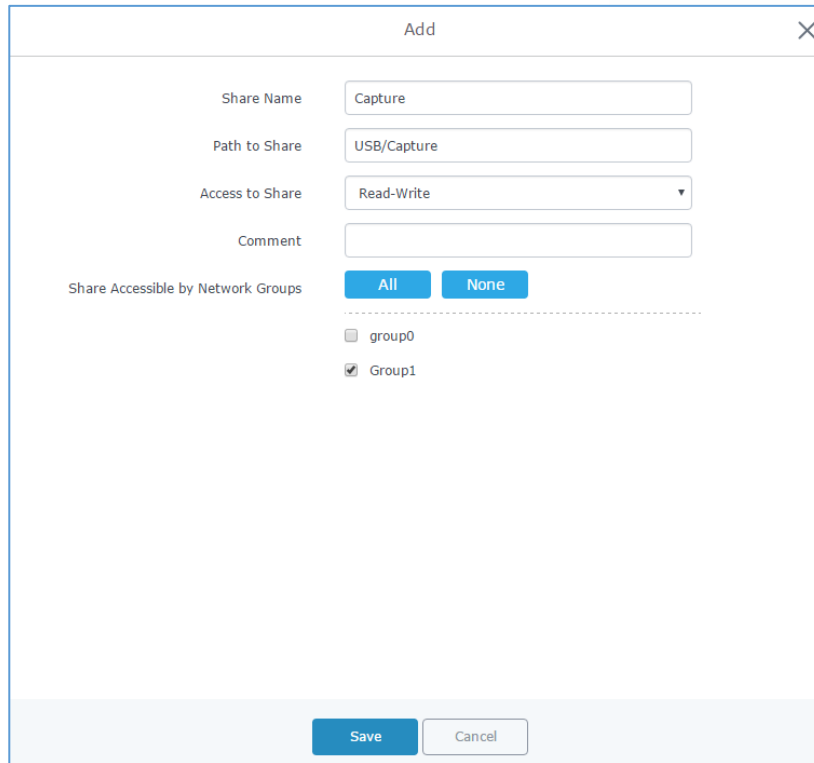
**Figure 50: NAT table**

## File Sharing

The GWN7000 has 2 USB ports that can be also used for file sharing, to enable file sharing on devices plugged on the USB ports, go to **System Settings -> File Sharing**.

Click on  to share a directory and its contents on a device connected to one of the USB ports of the GWN7000, the following figure will pop up.









**Figure 51: Add a New File to Share**

**Table 35: Add a New File to Share**

<b>Share Name</b>	Enter the share name
<b>Path to Share</b>	Choose from the drop menu the path to share.
<b>Access to Share</b>	Choose whether to allow users to <b>Read/Write</b> or <b>Read Only</b> on the shared path.
<b>Comment</b>	Enter a comment for the added shared file.
<b>Share Accessible by Network Groups</b>	Choose whether to allow <b>All</b> LAN network groups to access the shared path, restrict access by selecting only some groups or <b>None</b> .

Edit a Shared Folder by clicking on  or delete it by clicking on 

Share Name	Path to Share	Access to Share	Comment	Actions
Captures	PARTITION A/captures/	Read/Write		 

**Figure 52: File Share Actions**

A device connected to one of the allowed network groups to the shared files can use the following path for access: [\\GWN\\_Address\Share\\_Name](\\GWN_Address\Share_Name) Where **GWN\_Address** is the GWN7000 IP address, and **Share\_Name** is the Share Name created for the File Share. It is also possible to map a network drive on Windows, or use a Samba client on Linux machine.



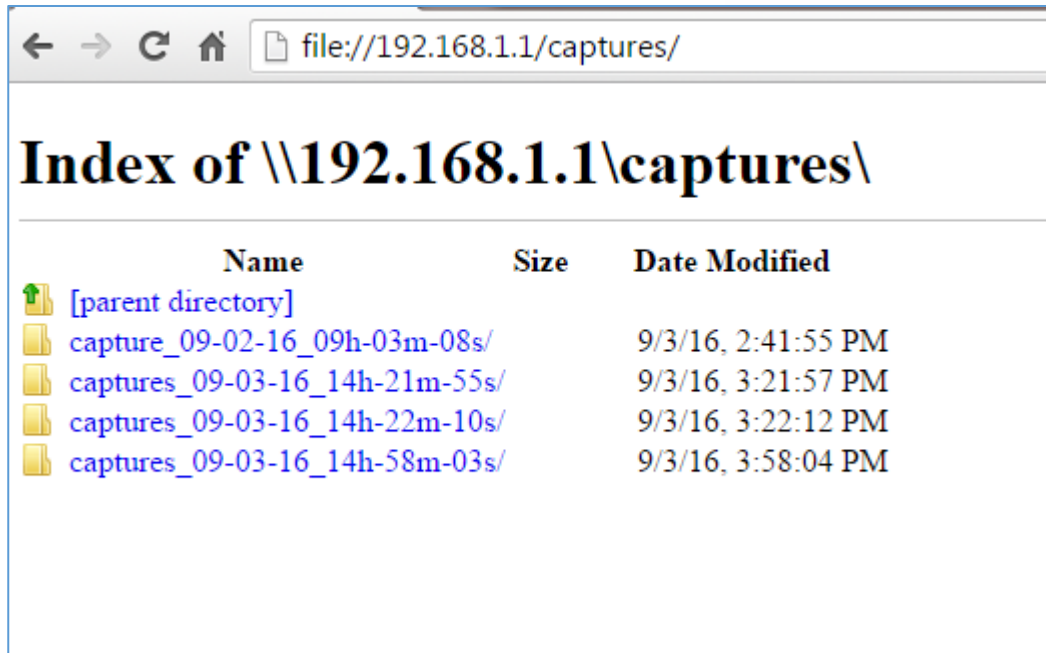


Figure 53: Access File Share

## SNMP (Pending)

GWN7000 supports 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 GWN7000 Web GUI -> **System Settings**-> **SNMP**, this page has two tabs: Basic and Advanced, refer to the below tables for each tab.



Table 36: SNMP Basic Page

<b>System Location</b>	Set the System Location information, for example: <i>SNMP-Server Lobby GWN.</i>
<b>System Contact</b>	Set the System Contact information, for example: Contact <i>Supervisor_GWN via extension is 1000.</i>
<b>System Name</b>	Set the System Name information, for example: <i>Supervisor_GWN.</i>
<b>Read-Only Community for IPv4</b>	Gives the permission for the set community to access and read only to devices in management information base via IPv4 Protocol.
<b>Read-Write Community for IPv4</b>	Gives the permission for the set community to access and read/write to devices in management information base via IPv4 Protocol.
<b>Read-Only Community for IPv6</b>	Gives the permission for the set community to access and read only to devices in management information base via IPv6 Protocol.



<b>Read-Write Community for IPv6</b>	Gives the permission for the set community to access and read/write to devices in management information base via IPv6 Protocol.
<b>Trap Type</b>	Choose the Trap Type from drop-down menu, 4 options are available: None, SNMPv1, SNMPv2c and SNMPv2cInforms.
<b>Monitoring Host</b>	Enter the Monitoring Host's IP/Domain Name (Network Management System "NMS")
<b>Monitoring Host Port</b>	Enter the Monitoring Host's Port (Network Management System "NMS")
<b>Trap Community</b>	Enter the Trap Community string to authenticate the client against the server.

**Table 37: SNMP Advanced Page**

<b>SNMP Service Listening on</b>	<p>Click on  to add an SNMP Service Listening on:</p> <ul style="list-style-type: none"> <li>• Set the <b>Transport</b> Type: UDPv4, UDPv6, TCPv4 or TCPv6.</li> <li>• Choose the <b>IP Address</b> from drop-down menu list.</li> <li>• Set the <b>Port</b> number on which the GWN7000 will listen on.</li> </ul>
<b>SNMPv3 Users</b>	<p>Click on  to add an SNMPv3 User:</p> <ul style="list-style-type: none"> <li>• Set the <b>Username</b> for authentication.</li> <li>• Choose the <b>Authentication</b> type, 2 options are available: SHA and MD5.</li> <li>• Set the Authentication Password from <b>Authentication Passphrase</b>.</li> <li>• Enter the Password again to confirm from <b>Authentication Passphrase Confirmation</b>.</li> <li>• Choose the <b>Privacy Protocol</b>, 3 options are available: None, DES and AES.</li> <li>• Set the <b>Privacy Passphrase</b>.</li> <li>• Enter the <b>Privacy Passphrase</b> in <b>Privacy Passphrase Confirmation</b> field.</li> </ul>



## UPGRADING AND PROVISIONING

### Upgrading Firmware

The GWN7000 can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN7000.

#### Upgrading via WEB GUI


The GWN7000 can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

#### Examples of valid URLs:

firmware.grandstream.com/BETA  
 192.168.5.87

The upgrading configuration can be accessed via **Web GUI->Router->Maintenance->Upgrade**.

**Table 38: Network Upgrade Configuration**

<b>Upgrade Via</b>	Choose the firmware upgrade method: TFTP, HTTP or HTTPS.
<b>Firmware Server</b>	Define the server path for the firmware server.
<b>Check Update on Boot</b>	Allows the device to check if there is a firmware from the configured firmware server at boot.
<b>Automatic Upgrade check interval(m)</b>	Set the value for automatic upgrade check in minutes.
<b>Upgrade Now</b>	Click on  button to begin the upgrade. Note that the device will reboot after downloading the firmware.



**Note:**

Please do not interrupt or power cycle the GWN7000 during upgrading process.

---





Service providers should maintain their own firmware upgrade servers. For users who do not have TFTP/HTTP/HTTPS server, some free windows version TFTP servers are available for download from [http://www.solarwinds.com/products/freetools/free\\_tftp\\_server.aspx](http://www.solarwinds.com/products/freetools/free_tftp_server.aspx)  
<http://tftpd32.jounin.net>

Please check our website at <http://www.grandstream.com/support/firmware> for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the GWN7000 to the same LAN segment;
3. Launch the TFTP server and go to the File menu->Configure->Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the GWN7000 web configuration interface;
5. Configure the Firmware Server to the IP address of the PC;
6. Update the changes and reboot the GWN7000.

End users can also choose to download a free HTTP server from <http://httpd.apache.org/> or use Microsoft IIS web server.

## Provisioning and backup

The GWN7000 configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GWN7000 when necessary.

### Download Configuration

Download the GWN7000 configurations for restore purpose under **Web GUI->Router->Maintenance->Upgrade**

Click on  to download locally the configuration file.

### Configuration Server


Configuration Server Page allows to provision the GWN7000 by putting the config file on a TFTP/HTTP or HTTPS server, and set Config Server to the TFTP/HTTP or HTTPS server used in order for the GWN7000 to be provisioned with that config server file.



## Reset and reboot

Used to reboot and reset the device to factory functions under **Web GUI**->

**Router->Maintenance->Upgrade** by clicking on  button.

 Will restore all the online GWN76xx as well as well as the GWN7000 itself to factory settings.



## EXPERIENCING THE GWN7000 ENTERPRISE ROUTER

Please visit our website: <http://www.grandstream.com> to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our [product related documentation](#), [FAQs](#) and [User and Developer Forum](#) for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all of your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

Thank you again for purchasing Grandstream GWN7000 Enterprise Multi-WAN Gigabit VPN Router, it will be sure to bring convenience and color to both your business and personal life

© 2002-2014 OpenVPN Technologies, Inc.

OpenVPN is a registered trademark of OpenVPN Technologies, Inc.



