Industrial LTE Cellular Gateway

EW50

User Manual

Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
A	Version 1	4/02/2018	First version of document
A	Version 2	5/02/2019	Minor fixes to images
A	Version 3	6/03/2019	Changed front cover picture
B	1	07/05/2019	Added TR-069 & LLDP function description
B	2	12/19/2019	Added max connections for TCP client and server
C	1	08/11/2020	New revision for updated firmware. Added Azure Agent.
C	2	12/01/2020	Changed key length to 2 ~ 256 characters
D	1	12/28/2021	Updated for MQTT function and document consistency
D	2	03/29/2022	Http/Https access GUI with TACAS+ note ; Remove supporting EtherWAN private MIB
D	3	04/28/2022	Remove VPN Hub & Spoke
D	4	04/28/2022	Notice on USB format & Micro SD storage

Contents

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this product: Industrial Cellular Gateway. For M2M (Machine-to-Machine) applications, EtherWAN Cellular Gateway is the right choice.

With a built-in world-class 4G LTE module, just insert a SIM card from local mobile carrier to access the Internet. The dual SIM design provides redundancy and a reliable WAN connection for critical applications. Through VPN tunneling technology, remote sites easily become a part of the local Intranet, and all data is transmitted in a secure link. The DI/DO feature allows the gateway to respond in real time to events detected by sensors.

This EW50 is equipped with a host of security features including VPN, firewall, NAT, port forwarding, DHCP server and other features for outdoor IP surveillance applications. Redundant dual SIM cards lossless data transmission and network connections.

Main Features:

- Built-in high speed LTE modem with dual SIMs for uplink traffic failover.
- Equipped with gigabit Ethernet ports to connect other IP-based devices.
- RS-232/485 serial ports for controlling legacy serial or Modbus devices.
- Digital I/O ports for integrating sensors, switches, or other alarm devices.
- Constructed with solid and easy-to-mount metal body for industrial environments and to work with a variety of M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail.

1.2 Contents List

1.2.1 Package Contents

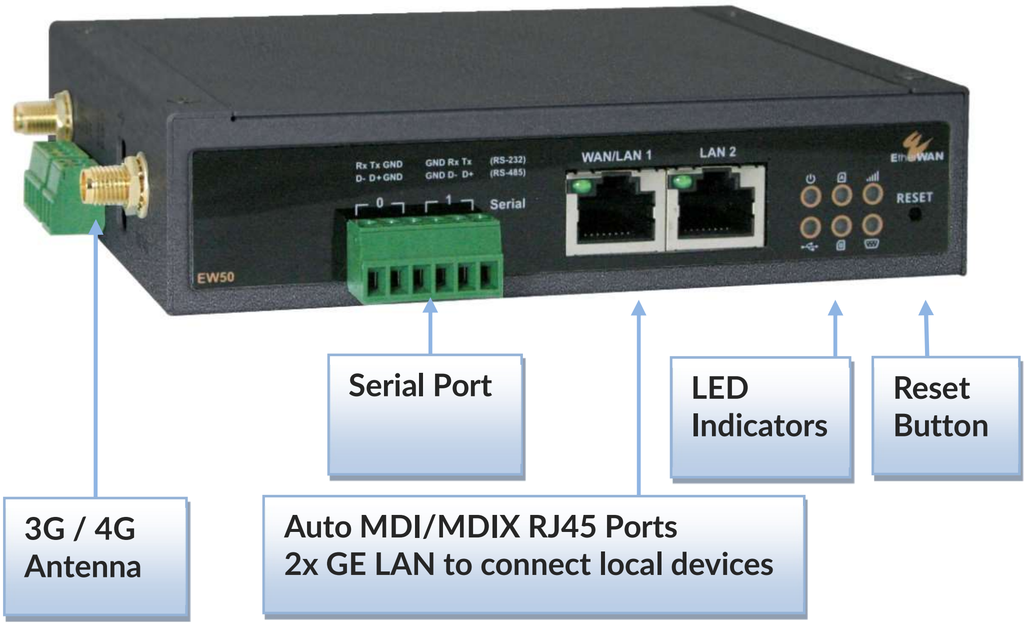
#Standard Package

Items	Description	Contents	Quantity
1	EW50 Industry LTE Cellular Gateway		1pcs
2	**Cellular Antenna**		2pcs
3	Power Adapter (DC 12V/2A) (*[1])		1pcs
3	**2 pin Terminal Block**		**1pcs**
4	**4 pin Terminal Block**		1pcs
5	**6 pin Terminal Block**		1pcs
7	**DIN-Rail Bracket**		1pcs

[1] The maximum power consumption of EW50 series products is 7 Watts.

1.3 Hardware Configuration

➢ Front View

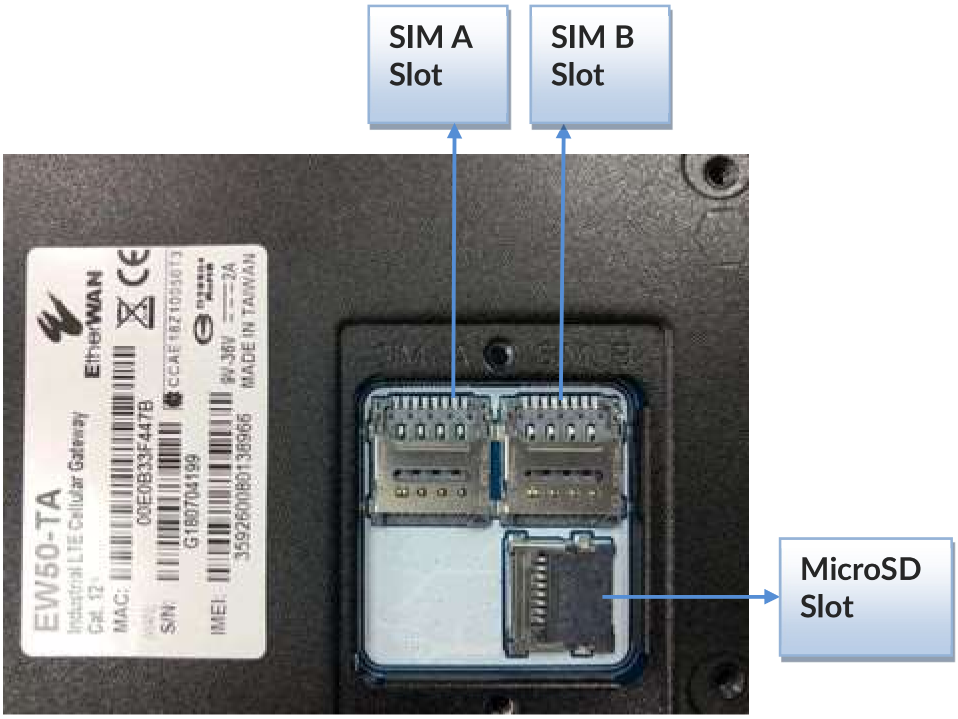


※**Reset Button**

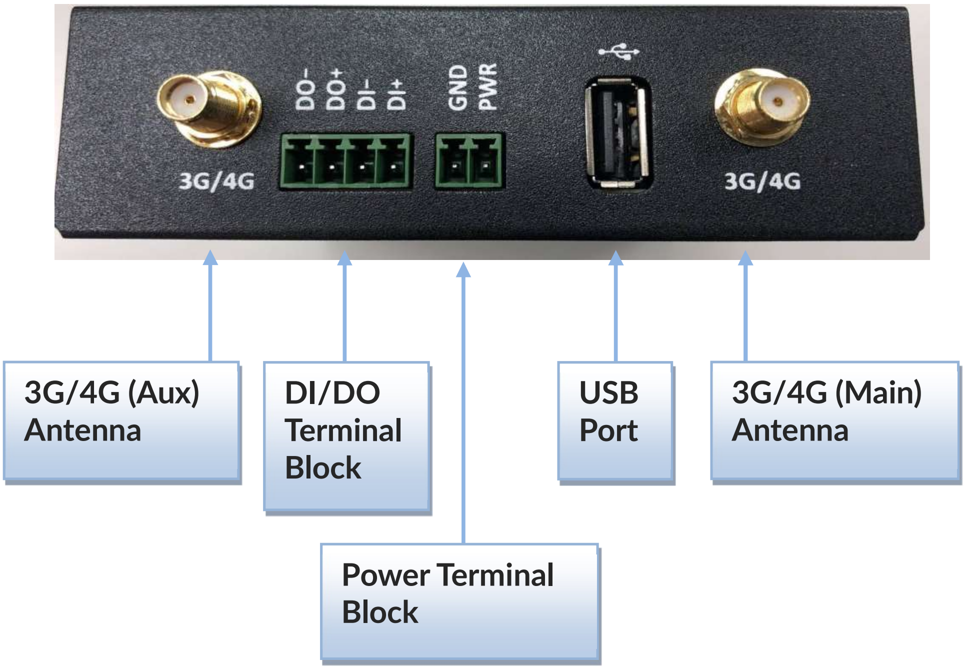
The RESET button provides a quick and easy way to restore the default settings. Press the RESET button continuously for 6 seconds, and then release it. The device will reset to factory default settings.

.

- Bottom View



- Left View



1.4 LED Indicators

LED Icon	Indication	LED Color	Description
⏻	Power Source	Blue	**Steady ON:** Device is powered ON.
⇸	USB	Blue	**OFF:** No Serial data transferred via USB port **Flashing:** Data packets being transferred via USB port
Ⓐ Ⓑ	SIM A/B	Blue	**OFF:** SIM not detected **Slow Flash (per Second):** SIM A/B was chosen for the connection **Steady ON**: Cellular connection successfully established (under SIM A/B)
📶	Cellular Signal	Blue	**Steady On:** Signal Strength is 61~100% **Slow Flash (per Second):** Signal Strength is 31~60% **Fast Flash (per 0.5 second):** Signal Strength is 0~30% **Very Fast Flash:** Device is in Recovery mode, or abnormal state.
▭	Serial	Blue	**OFF:** No serial data transferred via serial port **Flashing:** while data packet transferred via Serial port
🖧	WAN/LAN1 ~ LAN 2	Green	**Steady ON:** Ethernet connection of LAN or WAN is established. **Flashing:** Data packets are being transferred. **OFF:** No Ethernet cable attached, or device not linked.

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• A gigabit Ethernet RJ45 cable • 3G/4G cellular service subscription • 10/100/1000 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

1.5.2 WARNING

Attention

- Only use the power supply that complies with the power specification of the gateway. Using an out-of-spec voltage rating power source is dangerous and may damage the product.
- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.

1.5.3 HOT SURFACE CAUTION

CAUTION: The surface temperature for the metallic enclosure can be very high! **Especially after long periods of operation, when installed in a closed cabinet without air conditioning, or in a location with a high ambient temperature.**

DO NOT touch the hot surface!!

1.5.4 Product Information for CE RED Requirements

The following product information is required to be presented in product User Manual for latest CE RED requirements. [2]

(1) Frequency Band & Maximum Power

1.a Frequency Band for Cellular Connection

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23 ±2.7 dBm
LTE FDD BAND 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	
LTE FDD BAND 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	
LTE FDD BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
LTE FDD BAND 20	Uplink: 832-862 MHz Downlink: 791-821 MHz	
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	24 +1/-3 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
E-GSM	Uplink: 880-915 MHz Downlink: 925-960 MHz	33 ±2 dBm
DCS	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	30 ±2 dBm

(2) RF Exposure Statements

The antenna of the product, under normal conditions, should be at least 20 cm away from the body of the user.

[2] The information presented in this section is ONLY valid for the EU/EFTA regional version. For non-CE/EFTA versions, refer to the corresponding product specification.

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The EW50 series product can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories. The mounting accessories are not screwed on the product when shipped from factory. Screw the DIN-rail bracket on the product first.

1.6.2 Insert the SIM Card

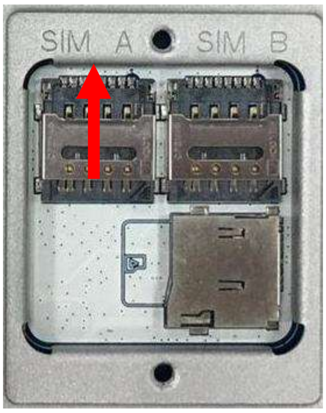
WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT DEVICE POWER IS SWITCHED OFF.

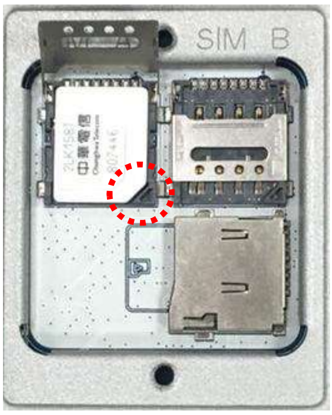
The SIM card slots are located at the bottom side of the housing. Unscrew and remove the outer SIM card cover before installing or removing the SIM card. After SIM card is correctly placed, return the outer SIM card cover to its original position and screw it in place.

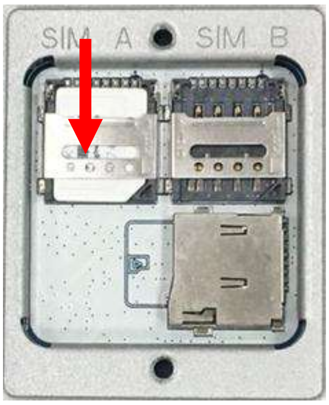
Step 1:
Pull the SIM holder in the direction indicated by the red arrow to unlock it.

Step 2:
Lift up the SIM holder, and insert the SIM card.

Step 3:
Put the SIM holder back, and push it in the direction indicated by the red arrow to lock it.

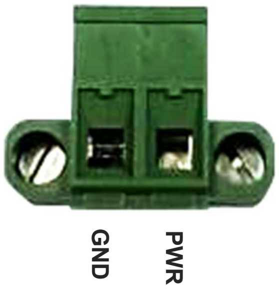




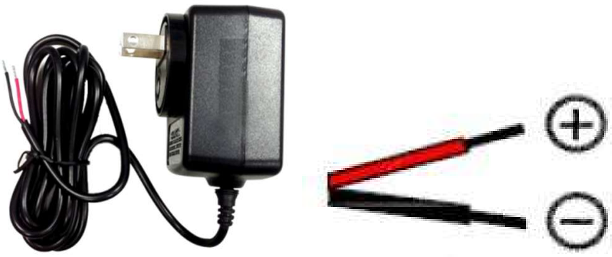


1.6.3 Connecting Power

The EW50 series products can be powered by connecting a DC power source to the terminal block. **It supports 9 to 36V DC power input**. The following picture indicates the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



There is a DC12V/1A power adapter[3] in the package for you to easily connect DC power adapter to this terminal block.

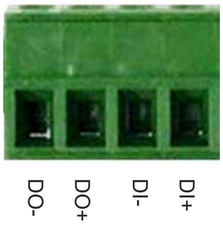


WARNNING: This commercial-grade power adapter (0-40°C) is mainly for ease of powering up the purchased device for initial configuration. It is not intended for operation in environments with extreme ranges of temperature. PREPARE OR PURCHASE AN INDUSTRIAL-GRADE POWER SUPPLY FOR LONG-TERM USE.

[3] The maximum power consumption of the EW50 series is 7 Watts.

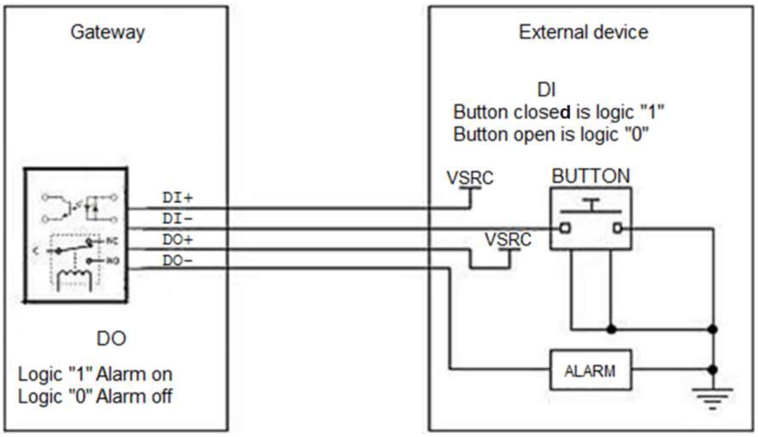
1.6.4 Connecting DI/DO Devices

There is one DI (digital input) and one DO (digital output) port next to the power terminal block. Refer to the following specification for connection of DI and DO devices.



Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2V
Digital Output	Voltage (Relay Mode)	Depends on external device Maximum voltage is 30V
	Maximum Current	1A

Example of Connection Diagram



1.6.6 Connecting Serial Devices

The EW50 has a 6-pin Terminal Block serial port for connecting to your serial device. Connect the serial device to the terminal block with the right pin assignments of RS-232/485 (shown below).

Pin 1 2 3 4 5 6

	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6
Port	SPort-0			SPort-1		
RS-232	RXD	TXD	GND	GND	RXD	TXD
RS-485	DATA-	DATA+	GND	GND	DATA-	DATA+

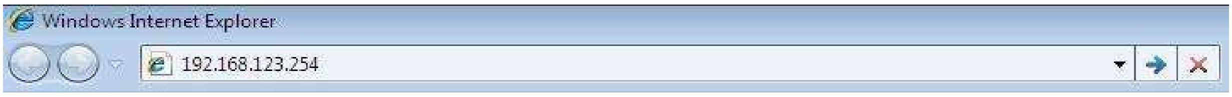
1.6.7 Connecting to the Network or a Host

The EW50 series provides RJ45 ports to connect 10/100/1000Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ45 port (LAN) of the device and plug another end of the Ethernet cable into your computer's network port. In this way, you can use the RJ45 Ethernet cable to connect to the host PC's Ethernet port for configuring the device.

1.6.8 Setup by Configuring WEB UI

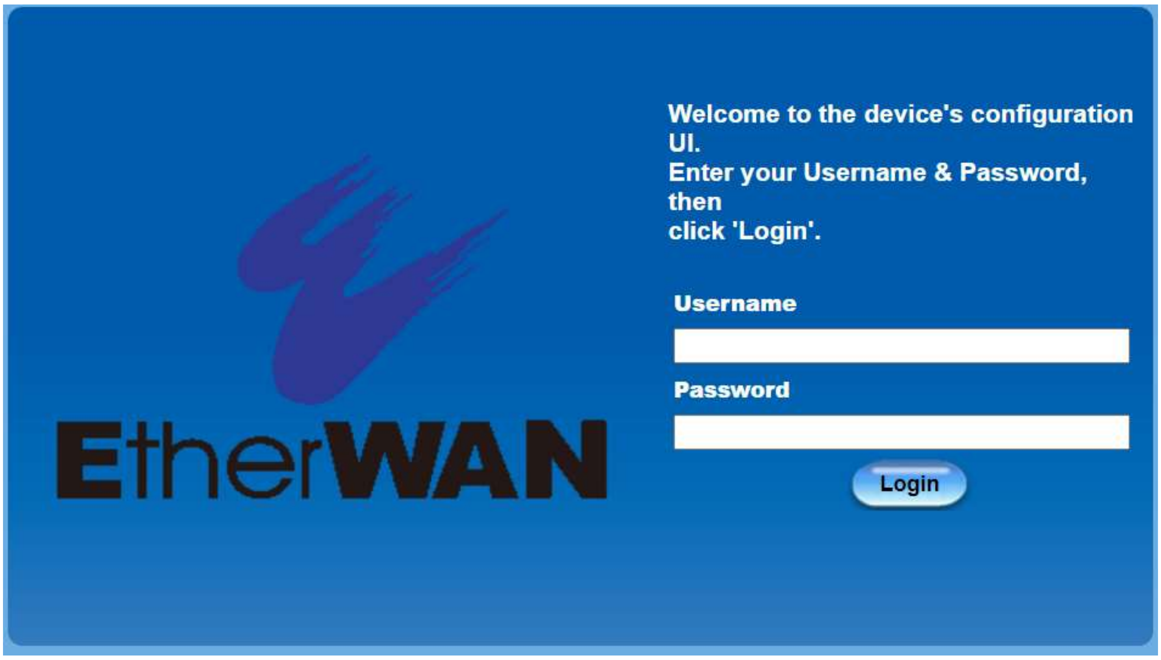
You can use the web UI to configure the device.

The IP Address is (**http://192.168.123.254**)[4]



192.168.123.254

When you see the login page, enter the default username and password **'admin'**[5] and then click the **'Login'** button.



Welcome to the device's configuration UI.
Enter your Username & Password, then
click 'Login'.

Username

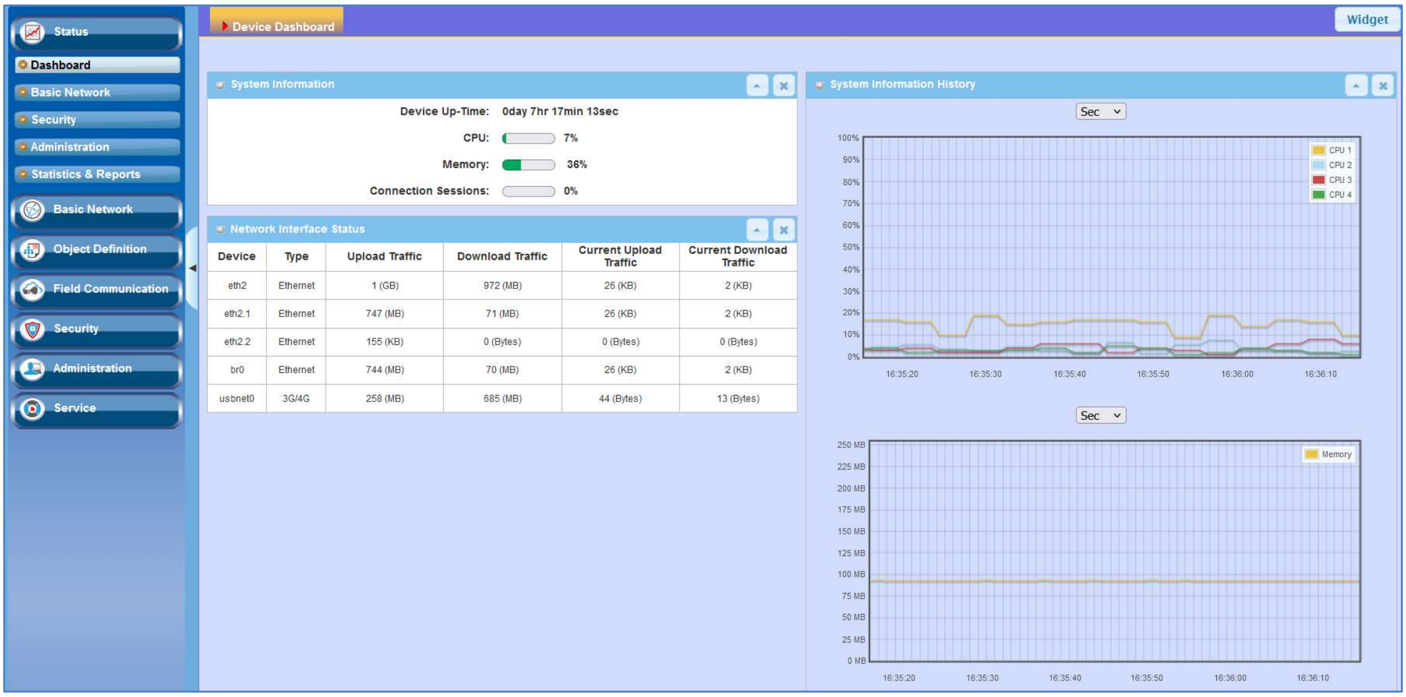
Password

[4] The default LAN IP address of this gateway is 192.168.123.254. If you change it, you will need to log in using the new IP address.

[5] You will be requested by the system to change this login password from the default value.

Chapter 2 Status

2.1 Dashboard



System Information

Device Up-Time: 0day 7hr 17min 13sec

CPU: 7%

Memory: 36%

Connection Sessions: 0%

Network Interface Status

Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	1 (GB)	972 (MB)	26 (KB)	2 (KB)
eth2.1	Ethernet	747 (MB)	71 (MB)	26 (KB)	2 (KB)
eth2.2	Ethernet	155 (KB)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	744 (MB)	70 (MB)	26 (KB)	2 (KB)
usbnet0	3G/4G	258 (MB)	685 (MB)	44 (Bytes)	13 (Bytes)

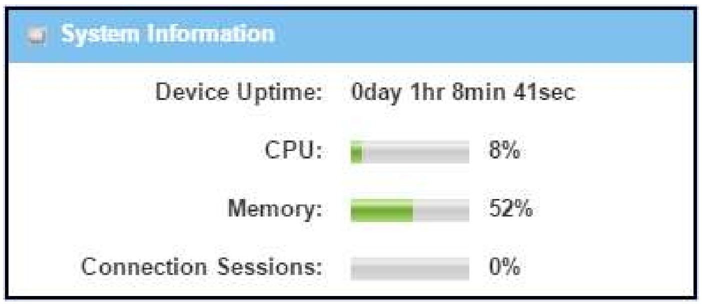
2.1.1 Device Dashboard

The **Device Dashboard** window shows the current status in graph or table format for quickly understanding the operation status of the gateway. The display will be refreshed once per second.

From the menu on the left, select Status > Dashboard > Device Dashboard tab.

System Information Status

The System Information screen shows the device Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.



System Information

Device Uptime: 0day 1hr 8min 41sec

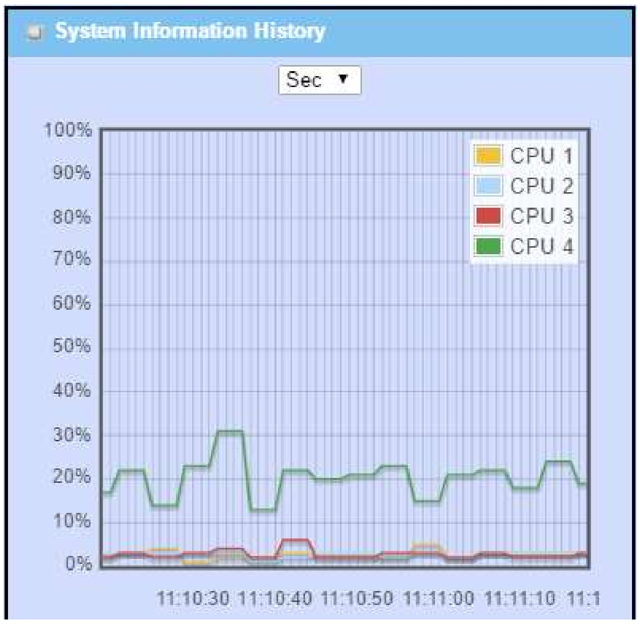
CPU: 8%

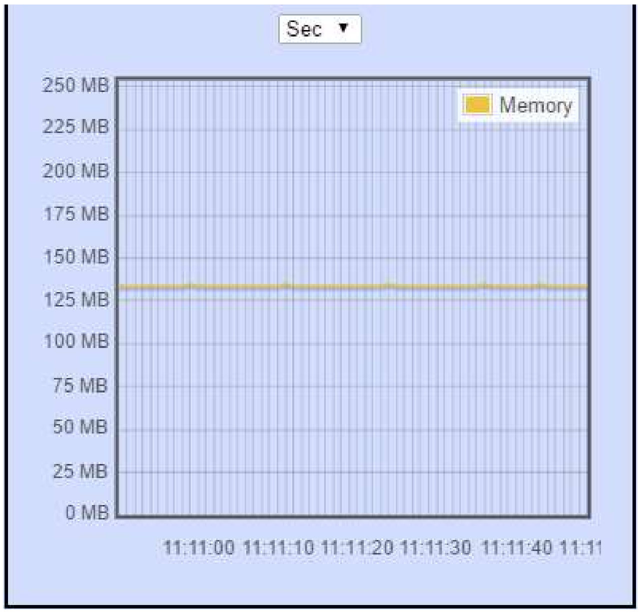
Memory: 52%

Connection Sessions: 0%

System Information History

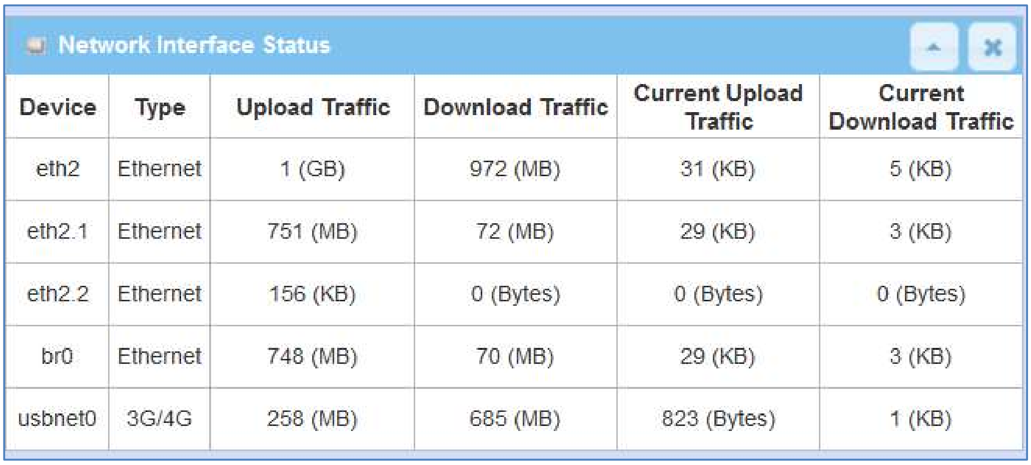
The System Information History screen shows statistical graphs for the CPU and memory.





Network Interface Status

The Network Interface Status screen shows the statistic information for each network interface of the gateway. The statistical information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.



Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	1 (GB)	972 (MB)	31 (KB)	5 (KB)
eth2.1	Ethernet	751 (MB)	72 (MB)	29 (KB)	3 (KB)
eth2.2	Ethernet	156 (KB)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	748 (MB)	70 (MB)	29 (KB)	3 (KB)
usbnet0	3G/4G	258 (MB)	685 (MB)	823 (Bytes)	1 (KB)

2.2 Basic Network

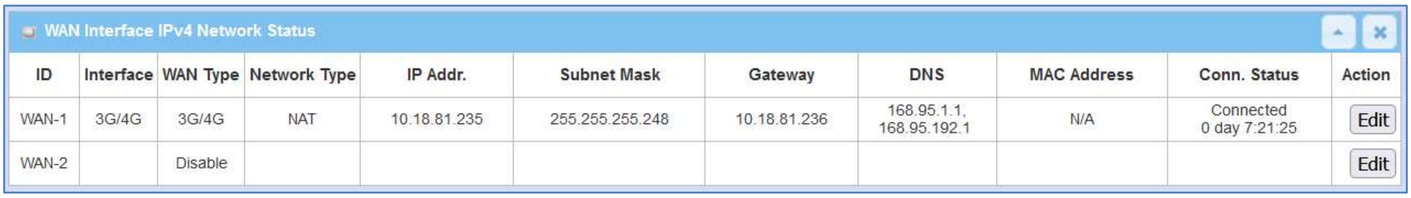
2.2.1 WAN & Uplink Status

Go to Status > Basic Network > WAN & Uplink tab.

The **WAN & Uplink Status** window shows the current status for different network types, including network configuration, connecting information, modem status and traffic statistics. The display will be refreshed every five seconds.

WAN interface IPv4 Network Status

The **WAN interface IPv4 Network Status** screen shows status information for IPv4 network.



WAN Interface IPv4 Network Status

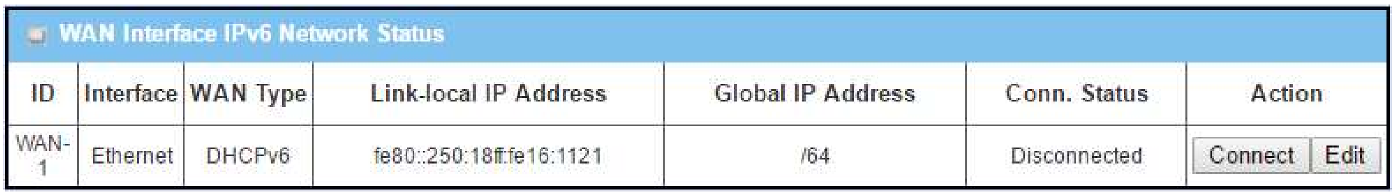
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	NAT	10.18.81.235	255.255.255.248	10.18.81.236	168.95.1.1, 168.95.192.1	N/A	Connected 0 day 7:21:25	Edit
WAN-2		Disable								Edit

WAN interface IPv4 Network Status		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc.
WAN Type	N/A	Displays the method which public IP address is obtained from the ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
Network Type	N/A	Displays the network type for the WAN interface(s). Depending on the model purchased, it can be NAT, Routing, Bridge, or IP Pass-through.
IP Addr.	N/A	Displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Subnet Mask	N/A	Displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Gateway	N/A	Displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
DNS	N/A	Displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
MAC Address	N/A	Displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	N/A	Displays the connection status of the device to your ISP. Status are Connected or disconnected.

Action	N/A	**Renew** button allows user to force the device to request an IP address from the DHCP server. Note: **Renew** button is available when DHCP WAN Type is used, and WAN connection is disconnected. **Release** button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: **Release** button is available when DHCP WAN Type is used, and WAN connection is connected. **Connect** button allows user to manually connect the device to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected. **Disconnect** button allows user to manually disconnect the device from the Internet. Note: **Disconnect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is connected.

WAN interface IPv6 Network Status

WAN interface IPv6 Network Status screen shows status information for IPv6 networks.



WAN Interface IPv6 Network Status

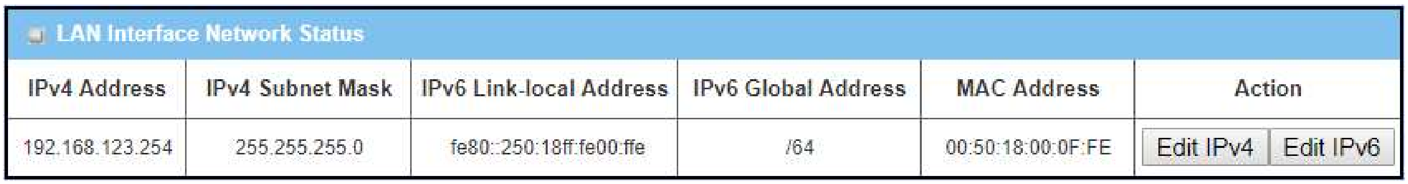
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	Ethernet	DHCPv6	fe80::250:18ff:fe16:1121	/64	Disconnected	Connect Edit

WAN interface IPv6 Network Status Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc.
WAN Type	N/A	Displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	Displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	Displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	Displays the connection status. The status can be connected, disconnected, and connecting.
Action	N/A	This area provides functional buttons.

		Edit Button when pressed, the web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 and IPv6 information of LAN networks.



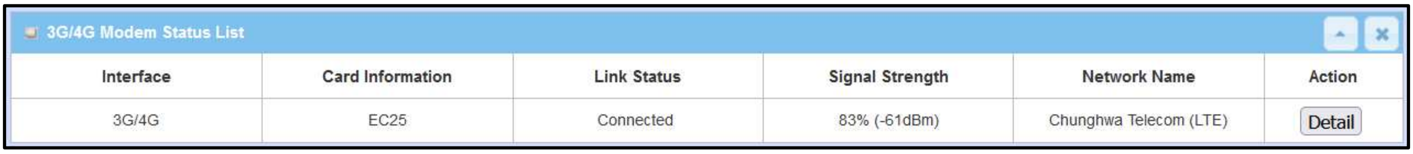
LAN Interface Network Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.123.254	255.255.255.0	fe80::250:18ff:fe00:ffe	/64	00:50:18:00:0F:FE	Edit IPv4 Edit IPv6

LAN Interface Network Status Item	Value setting	Description
IPv4 Address	N/A	Displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	Displays the current mask of the subnet.
IPv6 Link-local Address	N/A	Displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	N/A	It displays the LAN MAC Address of the gateway
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** will take you to the Ethernet LAN configuration page. (Basic Network > LAN & VLAN > Ethernet LAN tab). **Edit IPv6 Button** will take you to the IPv6 configuration page. (Basic Network > IPv6 > Configuration.)

3G/4G Modem Status

3G/4G Modem Status List screen shows status information for 3G/4G WAN network(s).



3G/4G Modem Status List

Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	EC25	Connected	83% (-61dBm)	Chunghwa Telecom (LTE)	Detail

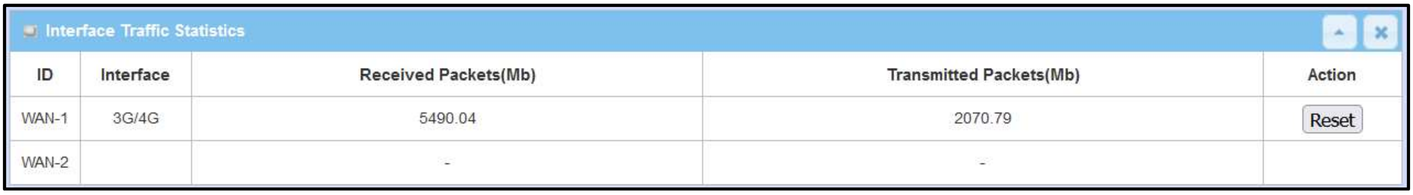
3G/4G Modem Status List Item	Value setting	Description
Interface	N/A	Displays the type of WAN physical interface. Note: Some device models may support two 3G/4G modules. Their physical interface names will be **3G/4G-1** and **3G/4G-2**.

Card Information	N/A	Displays the vendor’s 3G/4G modem model name.
Link Status	N/A	Displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	N/A	Displays the 3G/4G wireless signal level.
Network Name	N/A	Displays the name of the service network carrier.
Action	N/A	**Detail Button:** when pressed, windows with detailed information will appear. They are Modem Information, SIM Status, and Service Information. Refer to next page for more.

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, Service Information, and Signal Strength / Quality will appear.

Interface Traffic Statistics

Interface Traffic Statistics screen displays the Interface’s total transmitted packets.



Interface Traffic Statistics

ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	5490.04	2070.79	Reset
WAN-2		-	-	

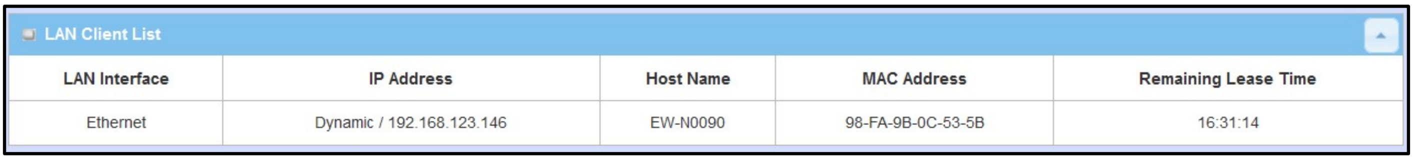
Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model, it can be Ethernet, 3G/4G, etc.
Received Packets (Mb)	N/A	Displays the downstream packets (Mb). It is reset when the device is rebooted.
Transmitted Packets (Mb)	N/A	Displays the upstream packets (Mb). It is reset when the device is rebooted.

2.2.2 LAN & VLAN Status

Go to **Status > Basic Network > LAN & VLAN** tab.

Client List

The **Client List** shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this gateway.



LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.123.146	EW-N0090	98-FA-9B-0C-53-5B	16:31:14

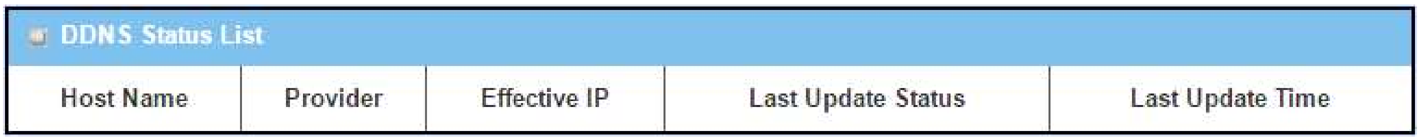
LAN Client List		
Item	**Value setting**	**Description**
LAN Interface	N/A	Client record of LAN Interface. String Format.
IP Address	N/A	Client record of IP Address Type and the IP Address. Type is String format, and the IP Address is IPv4 Format.
Host Name	N/A	Client record of Host Name. String Format.
MAC Address	N/A	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	N/A	Client record of Remaining Lease Time. Time Format.

2.2.3 DDNS Status

Go to **Status > Basic Network > DDNS** tab.

The **DDNS Status** window shows the current DDNS service in use, the last update status, and the last update time to the DDNS service server.

DDNS Status

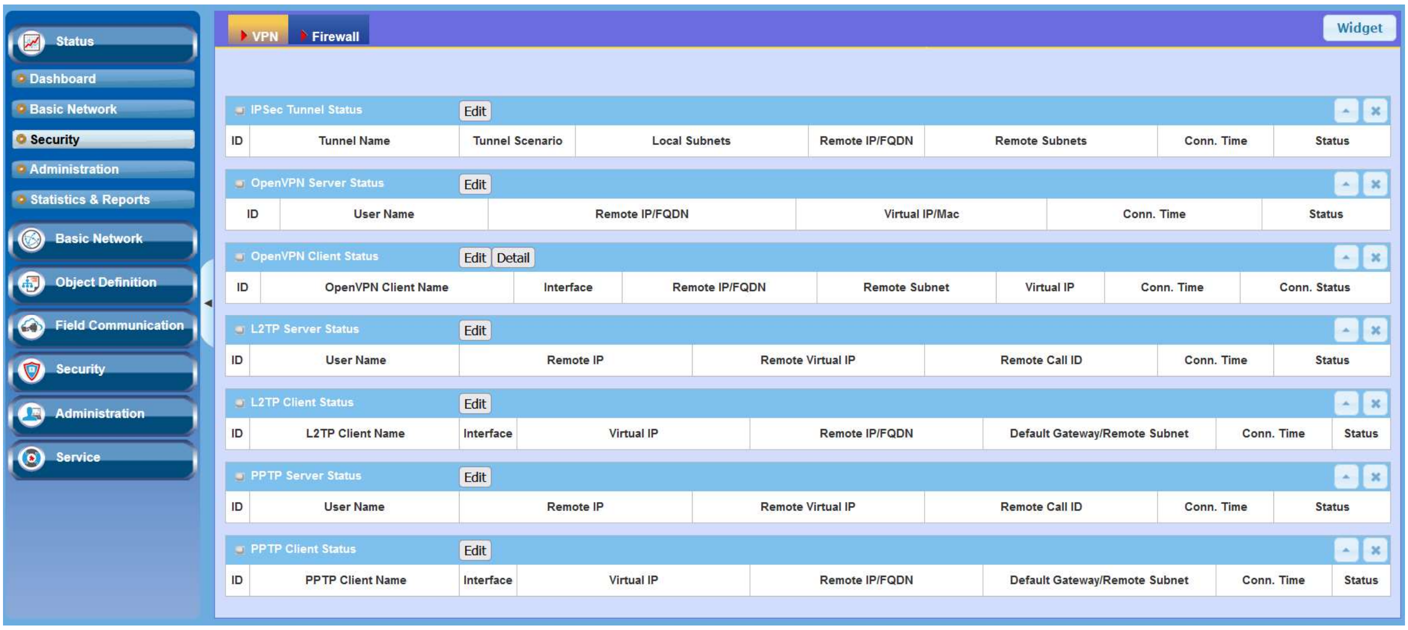


DDNS Status List

Host Name	Provider	Effective IP	Last Update Status	Last Update Time

DDNS Status Item	Value Setting	Description
Host Name	N/A	Displays the name you entered to identify DDNS service provider
Provider	N/A	Displays the DDNS server of DDNS service provider
Effective IP	N/A	Displays the public IP address of the device updated to the DDNS server
Last Update Status	N/A	Displays whether the last update of the device public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	N/A	Displays time stamp of the last update of public IP address to the DDNS server.
Refresh	N/A	The **refresh** button allows user to force the display to refresh information.

2.3 Security



IPSec Tunnel Status [Edit]

ID	Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

OpenVPN Server Status [Edit]

ID	User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

OpenVPN Client Status [Edit] [Detail]

ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status

L2TP Server Status [Edit]

ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

L2TP Client Status [Edit]

ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

PPTP Server Status [Edit]

ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

PPTP Client Status [Edit]

ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

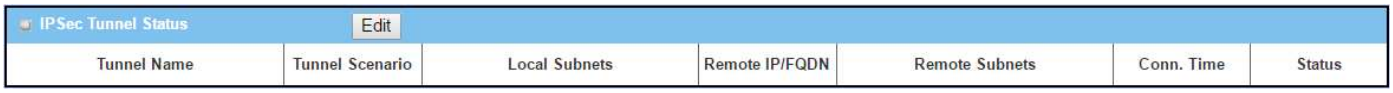
2.3.1 VPN Status

Go to **Status > Security > VPN** tab.

The **VPN Status** widow shows the overall VPN tunnel status. The display will be refreshed every five seconds.

IPsec Tunnel Status

IPsec Tunnel Status windows show the configuration for establishing IPsec VPN connection and current connection status.



IPSec Tunnel Status [Edit]

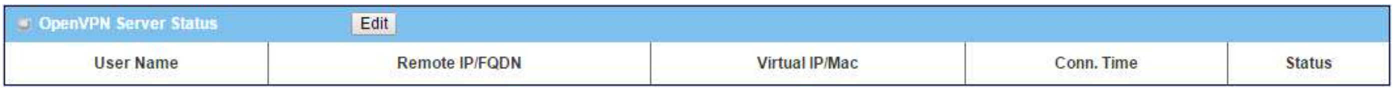
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

IPSec Tunnel Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	Displays the tunnel name you have entered.
Tunnel Scenario	N/A	Displays the Tunnel Scenario specified.
Local Subnets	N/A	Displays the Local Subnets specified.
Remote IP/FQDN	N/A	Displays the Remote IP/FQDN specified.
Remote Subnets	N/A	Displays the Remote Subnets specified.
Conn. Time	N/A	Displays the connection time for the IPsec tunnel.
Status	N/A	Displays the Status of the VPN connection: Connected, Disconnected, Wait for traffic, and Connecting.

Edit Button	N/A	Click the Edit Button to change IPsec setting, the web-based utility will take you to the IPsec configuration page. (**Security > VPN > IPsec** tab)

OpenVPN Server Status

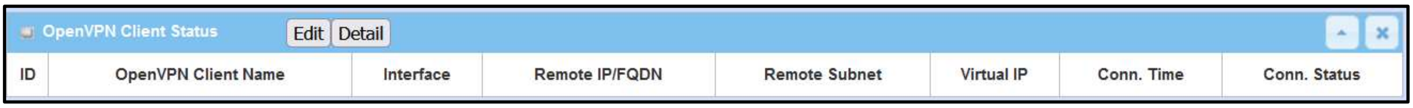
According to OpenVPN configuration, the **OpenVPN Server/Client Status** shows the status and statistics for the OpenVPN connection from the server side or client side.



User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

OpenVPN Server Status		
Item	**Value setting**	**Description**
User Name	N/A	Displays the Client name you have entered for identification.
Remote IP/FQDN	N/A	Displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	Displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	Displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

OpenVPN Client Status

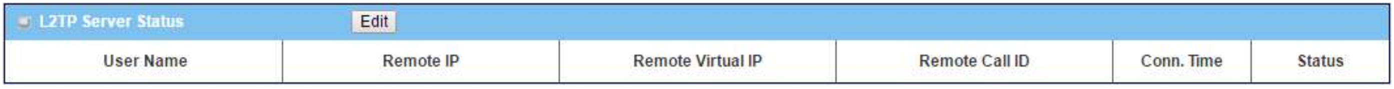


ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status

OpenVPN Client Status		
Item	**Value setting**	**Description**
OpenVPN Client Name	N/A	Displays the Client name you have entered for identification.
Interface	N/A	Displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	N/A	Displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	Displays the Remote Subnet specified.
Virtual IP	N/A	Displays the Virtual IP address of OpenVPN Client.
Conn. Time	N/A	Displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

L2TP Server/Client Status

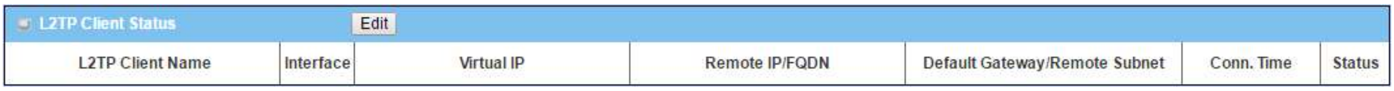
LT2TP Server/Client Status shows the configuration for establishing LT2TP tunnel and current connection status.



L2TP Server Status Edit

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

L2TP Server Status		
Item	**Value setting**	**Description**
User Name	N/A	Displays the login name of the user used for the connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	Displays the L2TP client Call ID.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of each of the L2TP client connection: Connected, Disconnect, Connecting
Edit	N/A	Click on **Edit** Button to change L2TP server settings, the web-based utility will take you to the L2TP server page. (**Security > VPN > L2TP** tab)



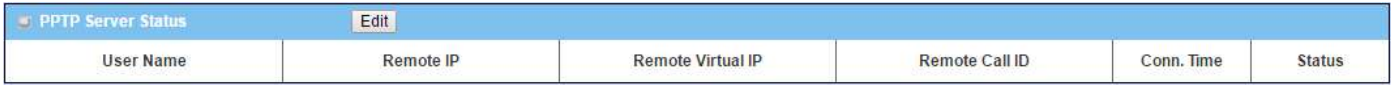
L2TP Client Status Edit

L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

L2TP Client Status		
Item	**Value setting**	**Description**
L2TP Client Name	N/A	Displays Name for the L2TP Client specified.
Interface	N/A	Displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	N/A	Displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway/Remote Subnet	N/A	Displays the specified IP address of the gateway device used to connect to the internet to connect to the L2TP server – the default gateway. Or other specified subnet if the default gateway is not used to connect to the L2TP server – the remote subnet.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of the VPN connection: Connected, Disconnect, and Connecting.
Edit	N/A	Click on **Edit** Button to change L2TP client settings, the web-based utility will take you to the L2TP client page. (**Security > VPN > L2TP** tab)

PPTP Server/Client Status

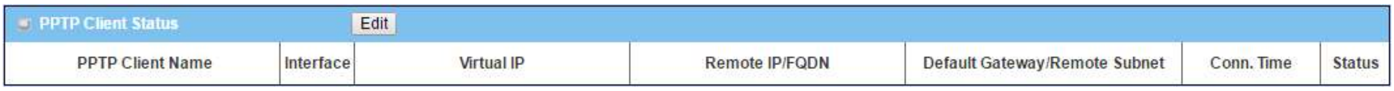
PPTP Server/Client Status shows the configuration for establishing PPTP tunnel and current connection status.



PPTP Server Status Edit

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

PPTP Server Status		
Item	**Value setting**	**Description**
User Name	N/A	Displays the login name of the user used for the connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	Displays the PPTP client Call ID.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of each of the PPTP client connection: Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP server settings, the web-based utility will take you to the PPTP server page. (**Security > VPN > PPTP** tab)



PPTP Client Status Edit

PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

PPTP Client Status		
Item	**Value setting**	**Description**
PPTP Client Name	N/A	Displays the Name for the PPTP Client specified.
Interface	N/A	Displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of PPTP server.
Remote IP/FQDN	N/A	Displays the PPTP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway / Remote Subnet	N/A	Displays the specified IP address of the gateway device used to connect to the internet to connect to the PPTP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the PPTP server –the remote subnet.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of the VPN connection: Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP client settings, the web-based utility will take you to the PPTP server page. (**Security > VPN > PPTP** tab)

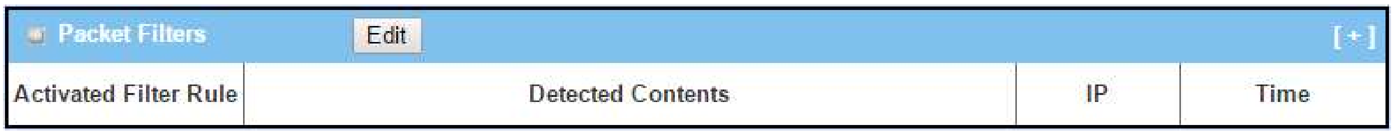
2.3.2 Firewall Status

Go to Status > Security > Firewall Status Tab.

The **Firewall Status** provides user a quick view of the firewall status and current firewall settings. It also keeps the log history of packets dropped by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options. The display will be refreshed every five seconds.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the **Edit** button will switch the view to the configuration page.

Packet Filter Status

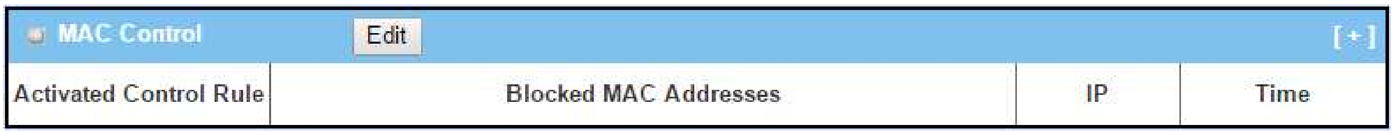


Activated Filter Rule	Detected Contents	IP	Time

Packet Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	The Packet Filter Rule name.
Detected Contents	N/A	The logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format: Source IP to Destination IP: Destination Protocol (TCP or UDP)
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Packet Filter Log Alert is enabled.
*Refer to **Security > Firewall > Packet Filter** tab. Check Log Alert and save the setting.*

MAC Control Status



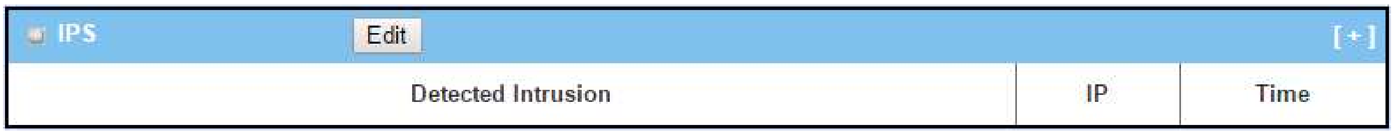
Activated Control Rule	Blocked MAC Addresses	IP	Time

MAC Control Status		
Item	**Value setting**	**Description**
Activated Control Rule	N/A	The MAC Control Rule name.
Blocked MAC Addresses	N/A	The MAC address of the logged packet.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure MAC Control Log Alert is enabled.

*Refer to **Security > Firewall > MAC Control** tab. Check Log Alert and save the setting.*

IPS Status

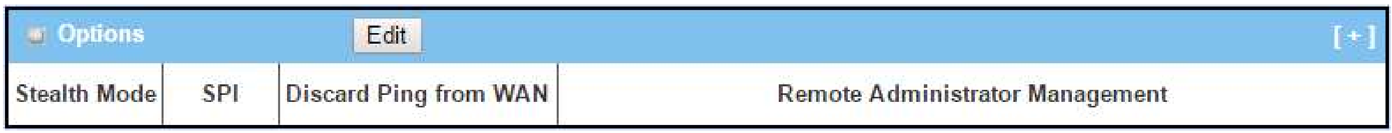


Detected Intrusion	IP	Time

IPS Firewall Status		
Item	**Value setting**	**Description**
Detected Intrusion	N/A	The intrusion type of the packets being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure IPS Log Alert is enabled.
*Refer to **Security > Firewall > IPS** tab. Check Log Alert and save the setting.*

Firewall Options Status



Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	N/A	Enable or Disable setting status of SPI on Firewall Options. String Format: Disable or Enable
Discard Ping from WAN	N/A	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	N/A	Enable or Disable setting status of Remote Administrator. If Remote Administrator is enabled, it shows the currently logged in administrator’s source IP address and login user name and the login time. Format: IP: "Source IP", User Name: "Login User Name", Time: "Date time" Example: IP: 192.168.127.39, User Name: admin, Time: Mar 3 01:34:13

Note: Ensure Firewall Options Log Alert is enabled.

*Refer to **Security > Firewall > Options** tab. Check Log Alert and save the setting.*

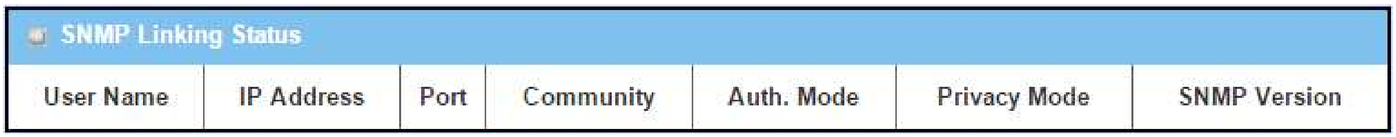
2.4 Administration

2.4.1 Configure & Manage Status

Go to Status > Administration > Configure & Manage tab.
The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP and UPnP. The display will be refreshed every five seconds.

SNMP Linking Status

SNMP Link Status screen shows the status of current active SNMP connections.



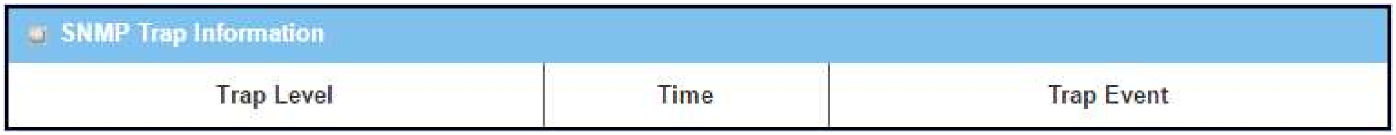
SNMP Linking Status

User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

SNMP Link Status Item	Value setting	Description
User Name	N/A	Displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	Displays the IP address of SNMP manager.
Port	N/A	Displays the port number used to maintain connection with the SNMP manager.
Community	N/A	Displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	Displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	Displays the privacy mode for version 3 only.
SNMP Version	N/A	Displays the SNMP Version employed.

SNMP Trap Information

SNMP Trap Information screen shows the status of current received SNMP traps.



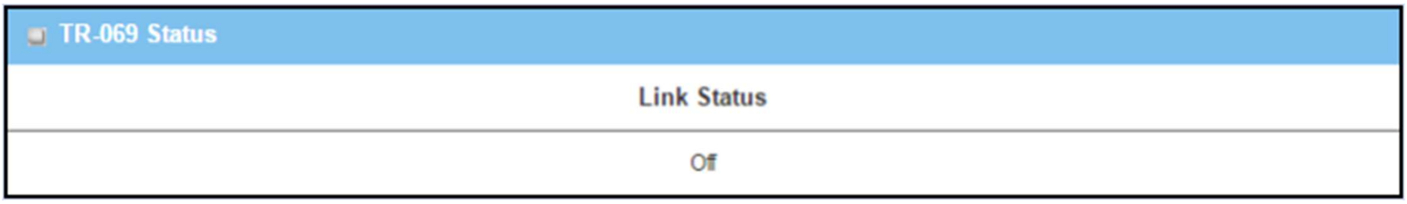
SNMP Trap Information

Trap Level	Time	Trap Event

SNMP Trap Information Item	Value setting	Description
Trap Level	N/A	Displays the trap level.
Time	N/A	Displays the timestamp of trap event.
Trap Event	N/A	Displays the IP address of the trap sender and event type.

TR-069 Status

The TR-069 Status screen shows the current connection status with the TR-068 server.



TR-069 Status

Link Status
Off

TR-069 Status Item	Value setting	Description
Link Status	N/A	It displays the current connection status with the TR-068 server. The connection status is either **On** when the device is connected with the TR-068 server or **Off** when disconnected.

2.4.2 Log Storage Status

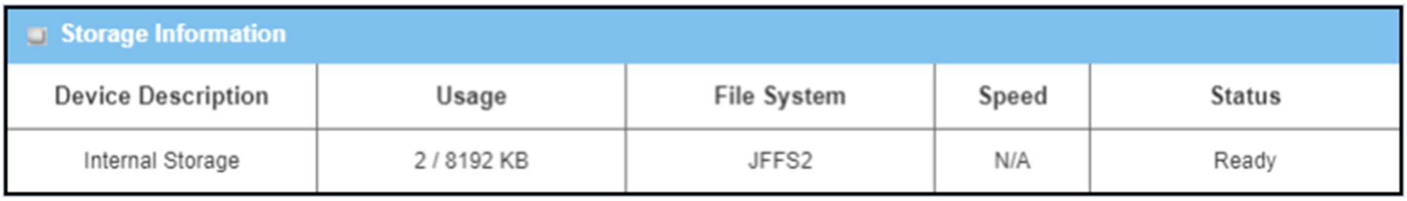
Go to Status > Administration > Log Storage tab.

The **Log Storage Status** screen shows the status for selected device storage.

Log Storage Status

Log Storage Status screen shows the status of current the selected device storage. The status includes Device Description, Usage, File System, Speed, and status

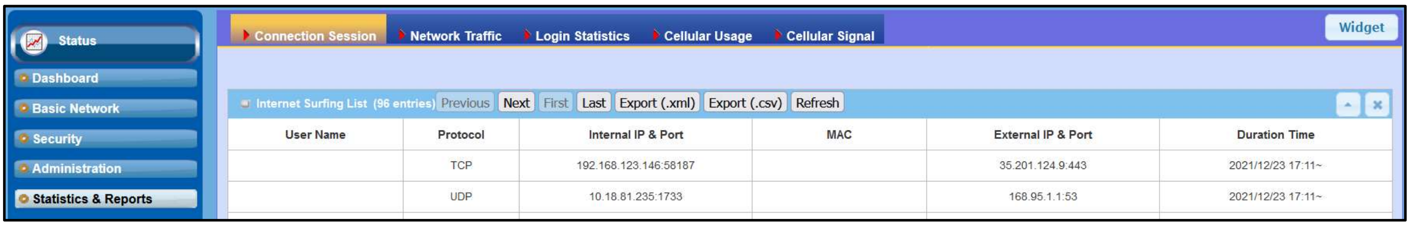
.



Storage Information

Device Description	Usage	File System	Speed	Status
Internal Storage	2 / 8192 KB	JFFS2	N/A	Ready

2.5 Statistics & Reports

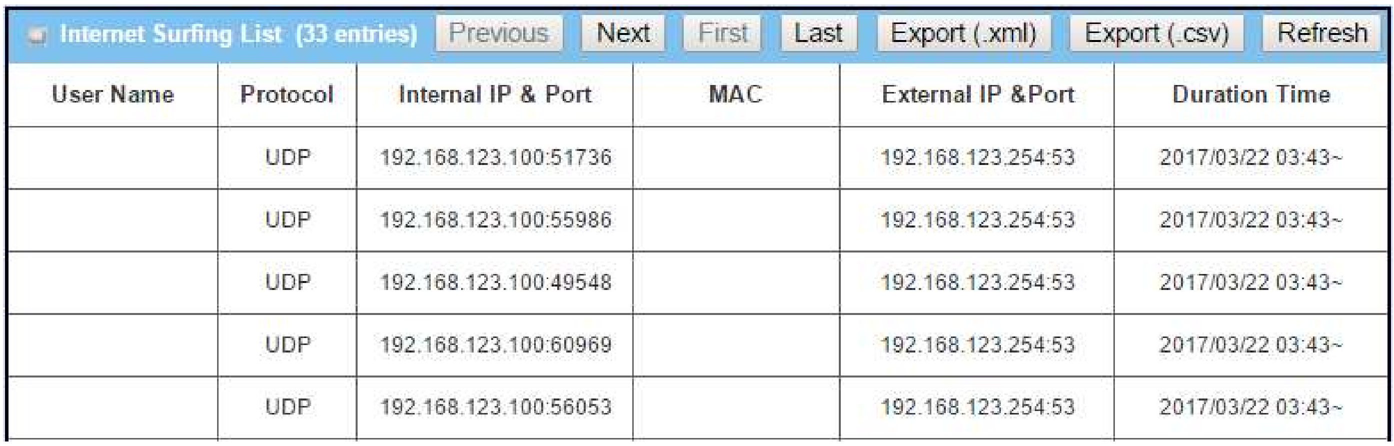


User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	TCP	192.168.123.146:58187		35.201.124.9:443	2021/12/23 17:11~
	UDP	10.18.81.235:1733		168.95.1.1:53	2021/12/23 17:11~

2.5.1 Connection Session

Go to Status > Statistics & Reports > Connection Session tab.

Internet Surfing Statistic shows the connection tracks on this router.



User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	UDP	192.168.123.100:51736		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:55986		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:49548		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:60969		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:56053		192.168.123.254:53	2017/03/22 03:43~

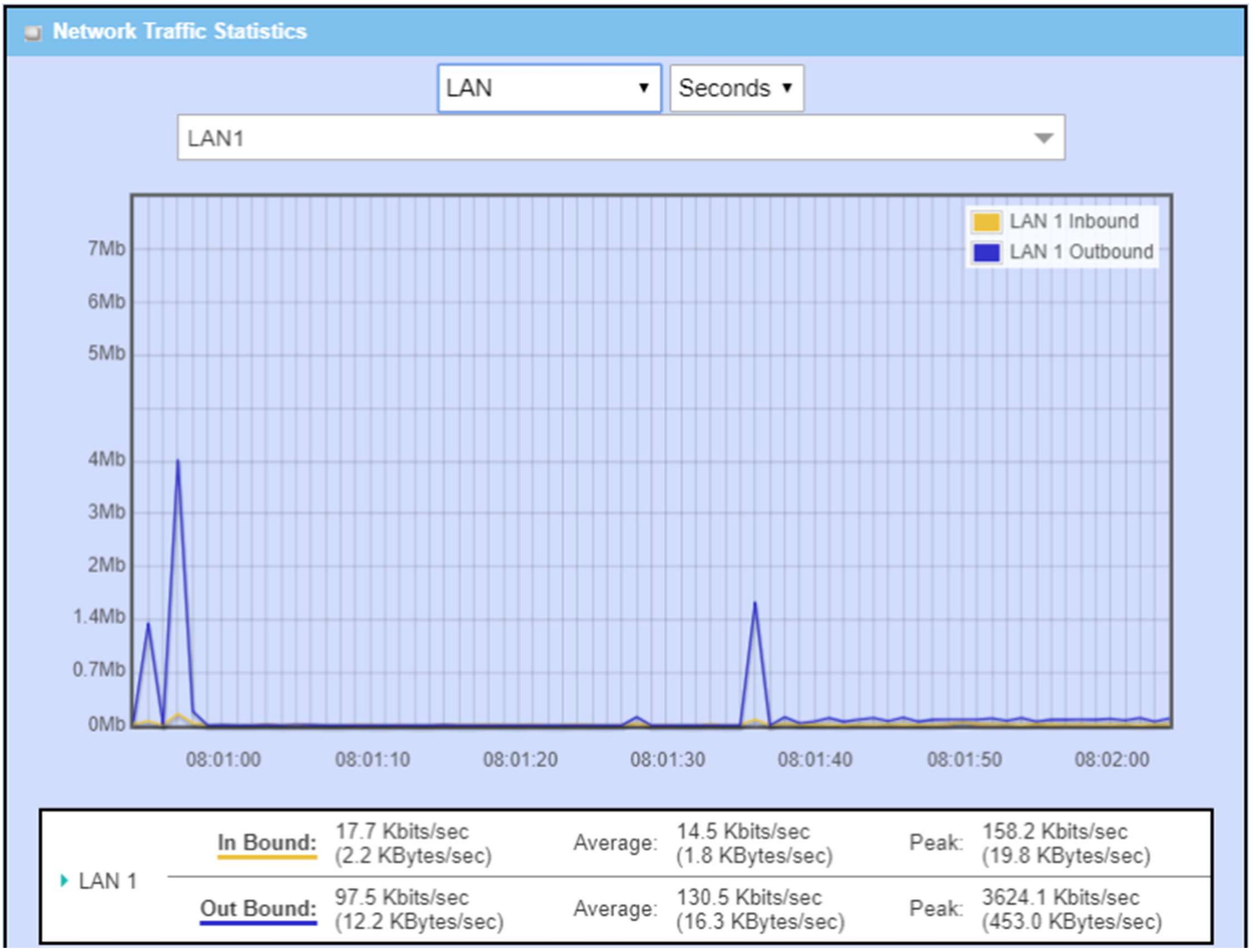
Internet Surfing Statistic		
Item	Value setting	Description
Previous	N/A	Click the **Previous** button to see the previous page of track list.
Next	N/A	Click the **Next** button to see the next page of track list.
First	N/A	Click the **First** button to see the first page of track list.
Last	N/A	Click the **Last** button to see the last page of track list.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the list to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the list to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the list.

2.5.2 Network Traffic

Go to Status > Statistics & Reports > Network traffic tab.

The **Network Traffic Statistics** screen shows the historical graph for the selected network interface.

You can change the interface drop list and select the interface and sampling time interval you want to monitor.

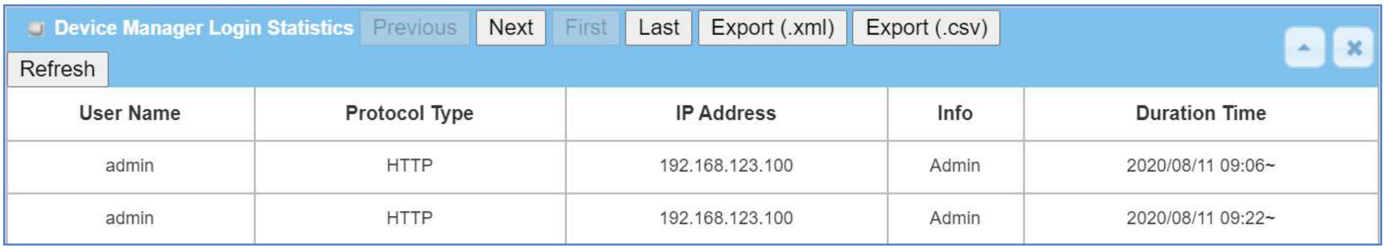


LAN 1	In Bound:	17.7 Kbits/sec (2.2 KBytes/sec)	Average:	14.5 Kbits/sec (1.8 KBytes/sec)	Peak:	158.2 Kbits/sec (19.8 KBytes/sec)
	Out Bound:	97.5 Kbits/sec (12.2 KBytes/sec)	Average:	130.5 Kbits/sec (16.3 KBytes/sec)	Peak:	3624.1 Kbits/sec (453.0 KBytes/sec)

2.5.3 Login Statistics

Go to Status > Statistics & Reports > Login Statistics tab.

Device Administration shows the login information.



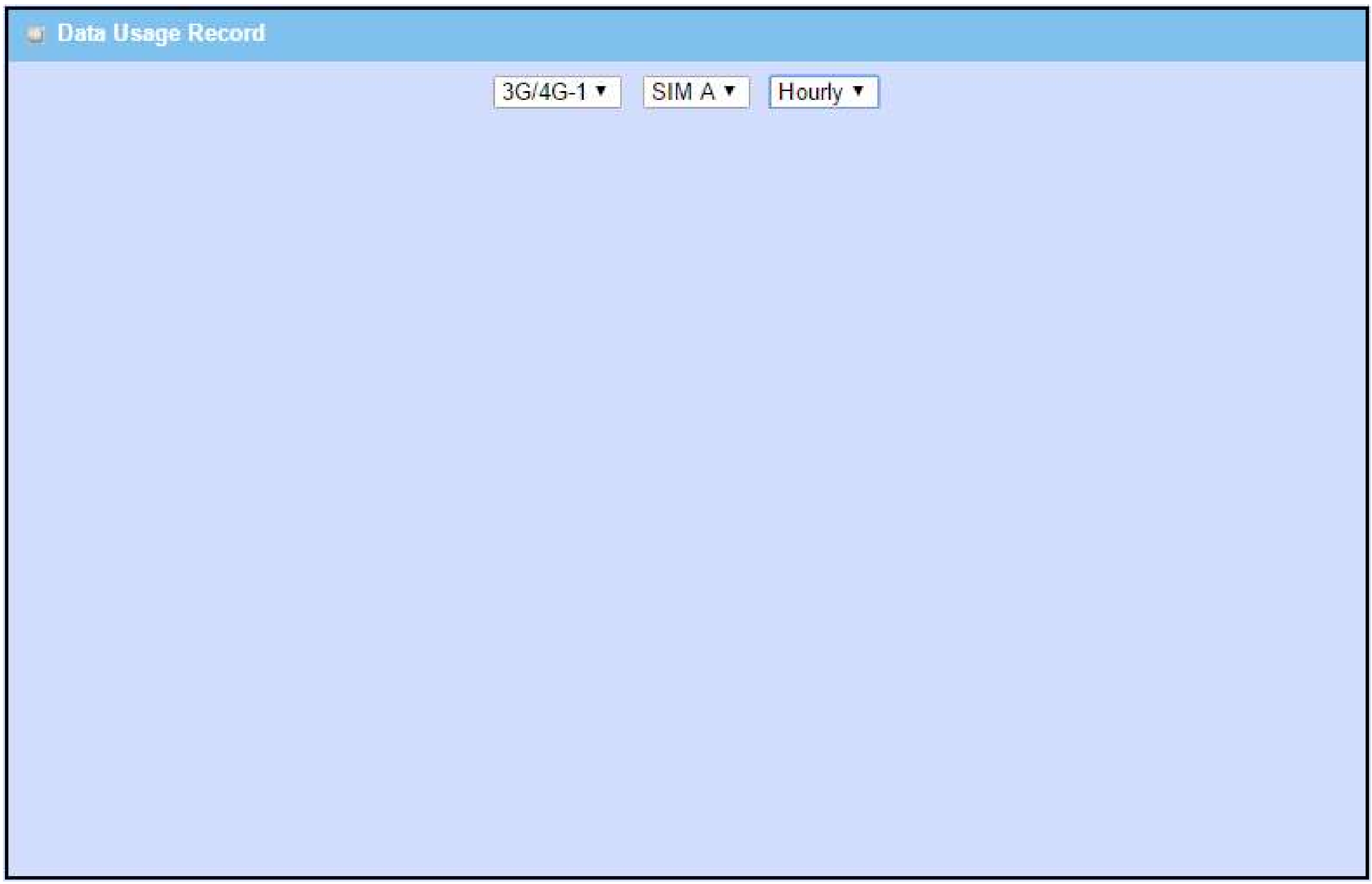
User Name	Protocol Type	IP Address	Info	Duration Time
admin	HTTP	192.168.123.100	Admin	2020/08/11 09:06~
admin	HTTP	192.168.123.100	Admin	2020/08/11 09:22~

Device Manager Login Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button to see the previous page of login statistics.
Next	N/A	Click the **Next** button to see the next page of login statistics.
First	N/A	Click the **First** button to see the first page of login statistics.
Last	N/A	Click the **Last** button to see the last page of login statistics.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the login statistics to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the login statistics.

2.5.4 Cellular Usage

Go to Status > Statistics & Reports > Cellular Usage tab.

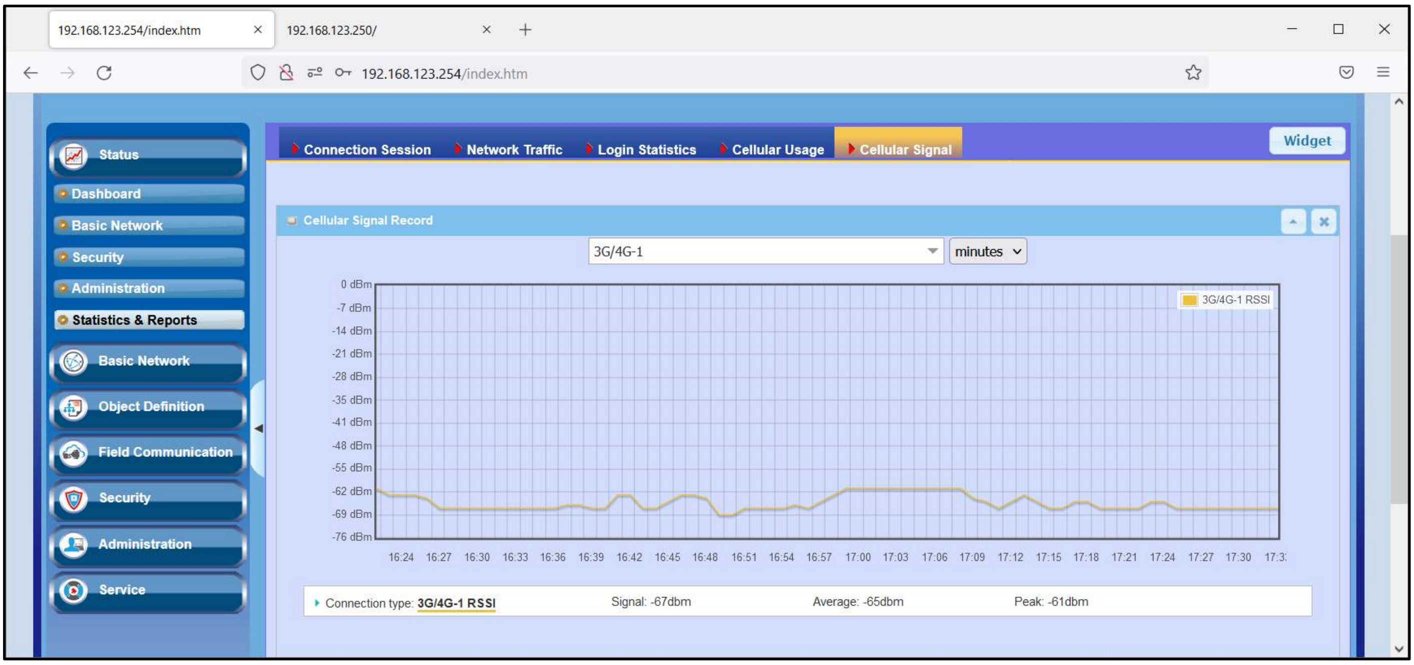
Cellular Usage screen shows data usage statistics for the selected cellular interface. The cellular data usage can be accumulated per hour or per day.



2.5.4 Cellular Signal

Go to Status > Statistics & Reports > Cellular Signal tab.

Cellular Usage screen shows signal information for the selected cellular interface.

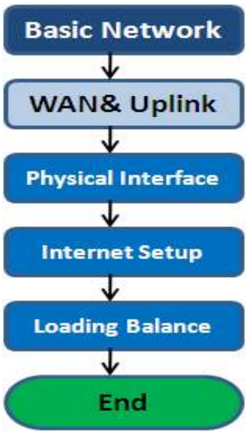


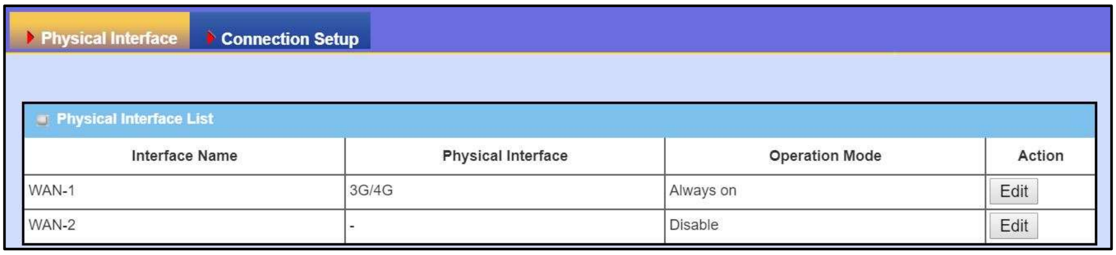
3G/4G-1 minutes

Connection type: 3G/4G-1 RSSI Signal: -67dbm Average: -65dbm Peak: -61dbm

Chapter 3 Basic Network

3.1 WAN & Uplink



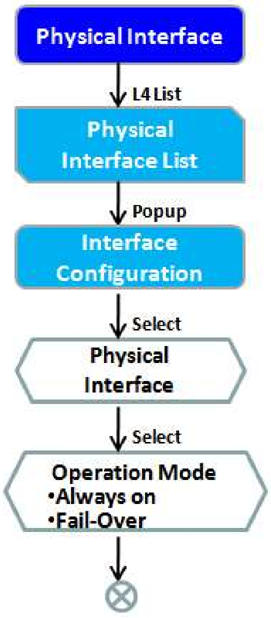


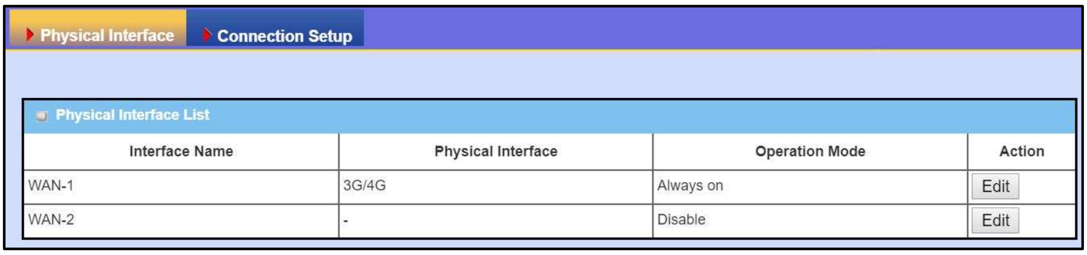
Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	Edit
WAN-2	-	Disable	Edit

The gateway provides multiple WAN interfaces to let client hosts in the Intranet of the gateway access the Internet via ISP. But ISPs apply various connection protocols to let gateways or user's devices dial in to ISPs and then link to the Internet via different kinds of media.

So, the WAN Connection lets you specify the WAN Physical Interface, WAN Internet Setup and WAN Load Balance for Intranet to access Internet. For each WAN interface, you must specify its physical interface first and then its Internet setup to connect to ISP. Since the gateway has multiple WAN interfaces, you can assign physical interface to participate in the Load Balance function.

3.1.1 Physical Interface





Physical Interface List

Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	Edit
WAN-2	-	Disable	Edit

M2M gateways are usually equipped with various WAN interfaces to support different WAN connection scenarios. You can configure the WAN interfaces one by one to get proper internet connection setup. **Refer to the product specification for the available WAN interfaces in your model.**

The first step to configure one WAN interface is to specify which kind of connection media is to be used for the WAN connection, as shown in "Physical Interface" page.

In the "Physical Interface" page, there are two configuration windows, "Physical Interface List" and "Interface Configuration". The "Physical Interface List" window shows all the available physical interfaces. After clicking on the "Edit" button for the interface in "Physical Interface List" window the "Interface Configuration" window will appear.

Physical Interface:

- **Ethernet WAN:** The gateway has one or more RJ45 WAN ports that can be configured to be WAN connections. You can directly connect to external DSL modem or setup behind a firewall device.
- **3G/4G WAN:** The gateway has one built-in 3G/4G cellular as WAN connection. For each cellular WAN, there are 1 or 2 SIM card slots.

Attention

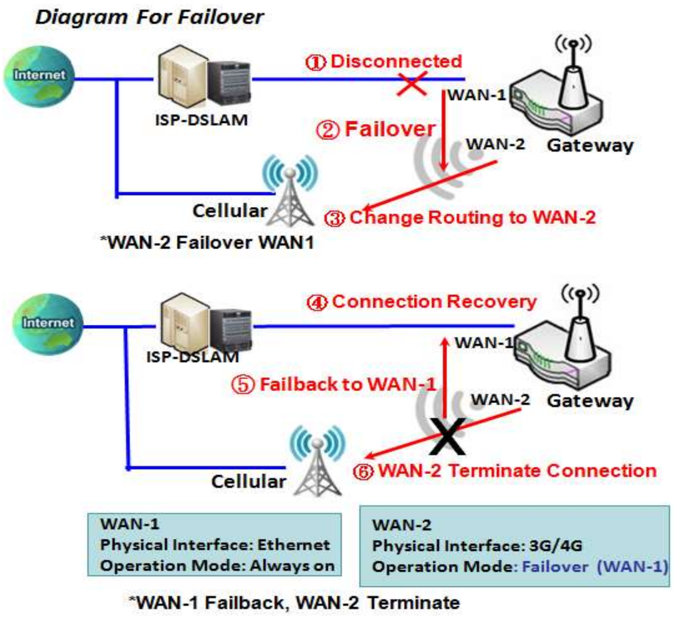
- POWER OFF the gateway before you insert or remove a SIM card.
- The SIM card can be damaged if you insert or remove SIM card while the gateway is in operation.

Operation Mode:

There are three option items “Always on”, “Failover”, and “Disable” for the operation mode setting.

Always on: Set this WAN interface to be active all the time. When two or more WAN are established at "Always on" mode, outgoing data will pass through these WAN connections based on load balance policies.

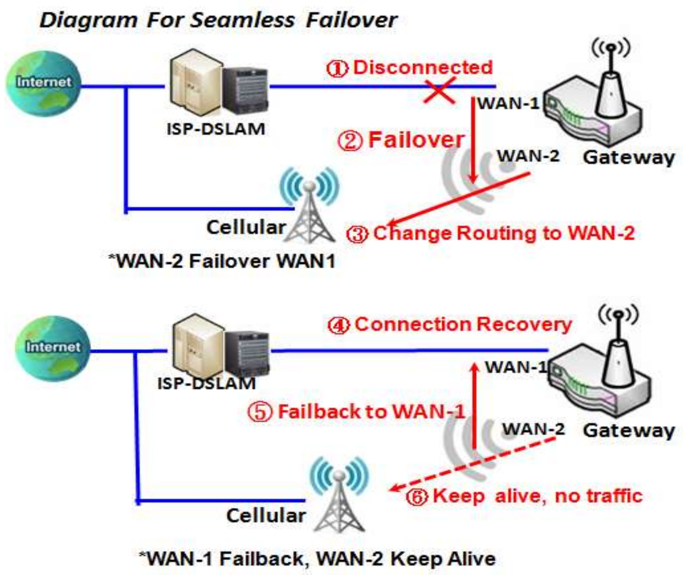
Failover:



A failover interface is a backup connection to the primary. That means only when the primary WAN connection is broken, the backup connection will be started up to substitute the primary connection.

As shown in the diagram, WAN-2 is backup WAN for WAN-1. WAN-1 serves as the primary connection with operation mode "Always on". WAN-2 won’t be activated until WAN-1 is disconnected. When WAN-1 connection is recovered, it will take over data traffic again. At that time, WAN-2 connection will be terminated.

Seamless Failover:



In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking the "Seamless" box in the configuration window, both the primary connection and the failover connection are started up after system rebooting. But only the primary connection executes data transfer, while the failover one just keeps the connection alive. As soon as the primary connection is lost, the system will switch to the failover connection.

When the “Seamless” enable checkbox is activated, it can allow the Failover interface to be connected continuously from the time the system boots up. The failover WAN interface maintains the connection without transferring data traffic. This is to shorten the switch time during failover process. When the primary connection is disconnected, failover interface will take over the data transfer mission instantly by only changing the routing path to the failover interface. The dialing-up time of failover connection is reduced since it has been connected beforehand.

VLAN Tagging

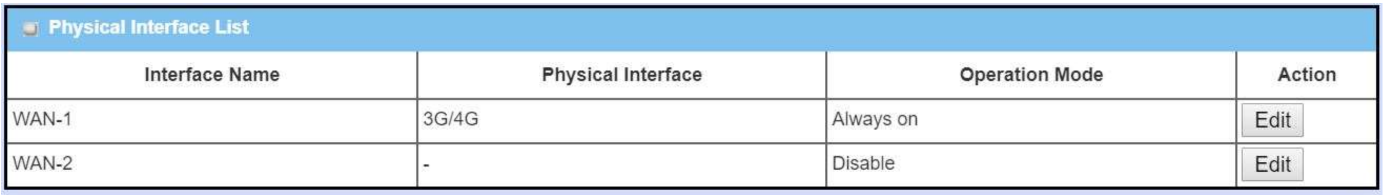
Sometimes, your ISP requires a VLAN tag to be inserted into the WAN packets from the Gateway for specific services. Please enable VLAN tagging and specify tag in the WAN physical interface. Please note that only Ethernet and ADSL physical interfaces support this feature. For devices with 3G/4G WAN only, it is disabled.

Physical Interface Setting

Go to Basic Network > WAN > Physical Interface tab.

The Physical Interface allows for the setup of the physical WAN interface and adjustment of WAN’s behavior.

Note: Number of available WAN Interfaces varies by model.

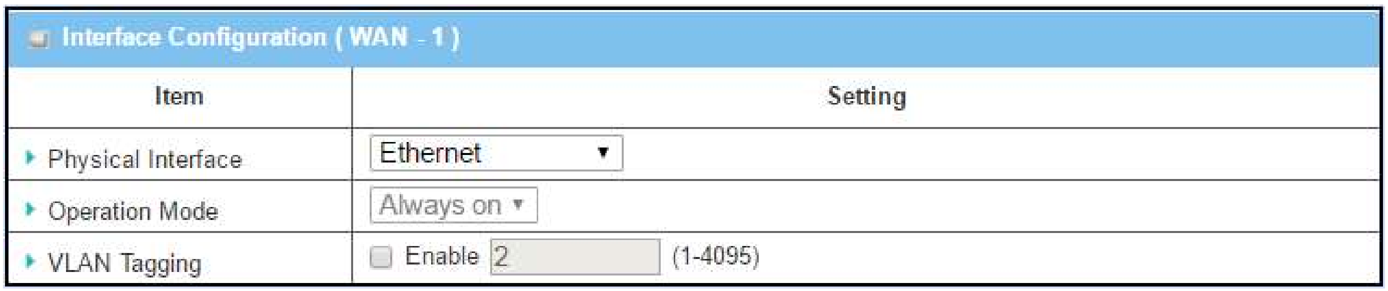


Physical Interface List

Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	Edit
WAN-2	-	Disable	Edit

When the **Edit** button is applied, an **Interface Configuration** screen will appear. WAN-1 interface is used in this example.

Interface Configuration:

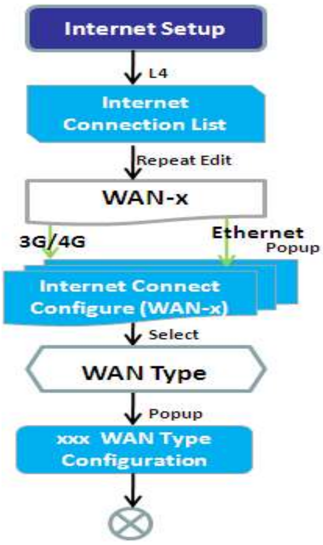


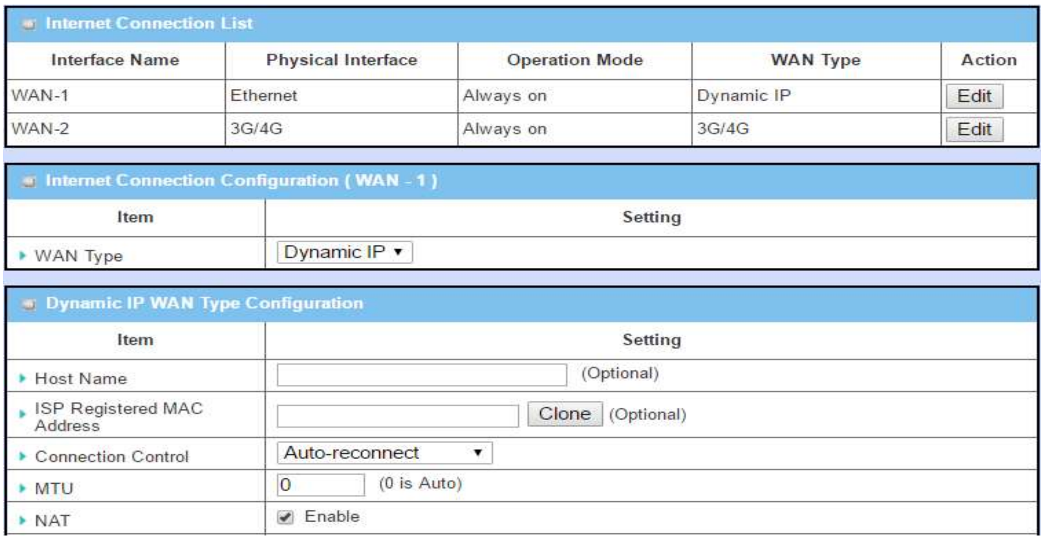
Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	Ethernet ▾
Operation Mode	Always on ▾
VLAN Tagging	□ Enable 2 (1-4095)

Interface Configuration		
Item	**Value setting**	**Description**
Physical Interface	1. Required setting 2. WAN-1 is the primary interface and is factory set to **Always on**.	Select one expected interface from the available interface dropdown list. Depending on the gateway model, **Disable** and **Failover** options will be available only to multiple WAN gateways. WAN-2 ~ WAN-4 interfaces are only available to multiple WAN gateways.
Operation Mode	Required setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link fails. Then select the primary or the existing secondary WAN interface to switch Failover from. (Note: for WAN-1, only **Always on** option is available.)
VLAN Tagging	Optional setting	Check **Enable** box to enter tag value provided by your ISP. Otherwise uncheck the box. *Value Range*: 1 ~ 4095. Note: This feature is NOT available for 3G/4G WAN connection.

3.1.2 Connection Setup





Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP ▾

Dynamic IP WAN Type Configuration

Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect ▾
MTU	0 (0 is Auto)
NAT	☑ Enable

After specifying the physical interface for each WAN connection, the connection profile must be configured to satisfy the dial-in process of the ISP, so that all client hosts in the Intranet of the gateway can access the Internet.

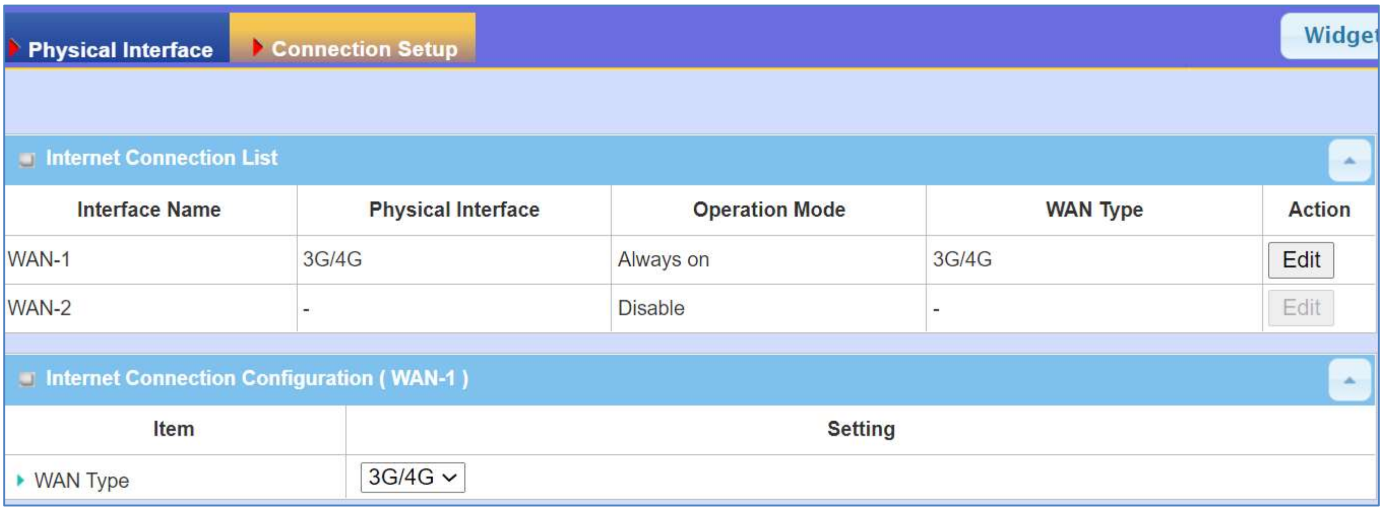
On the "Internet Setup" page there are some configuration windows: "Internet Connection List", "Internet Connection Configuration", "WAN Type Configuration" and related configuration windows for each WAN type. For the Internet setup of each WAN interface, you must specify its WAN type of physical interface first and then the related parameter configuration for that WAN type.

After clicking on the "Edit" button of a physical interface in "Internet Setup List" window, the "Internet Connection Configuration" window will appear to let you specify which kind of WAN type that you will use for that physical interface to make an Internet connection. Based on your chosen WAN type, you can configure necessary parameters in each corresponding configuration window.

Internet Connection

Configure Ethernet WAN Setting

When the **Edit** button is applied, the **Internet Connection Configuration** screen will appear. WAN-1 interface is used in this example. Click the Edit button to display the configuration screens shown below.

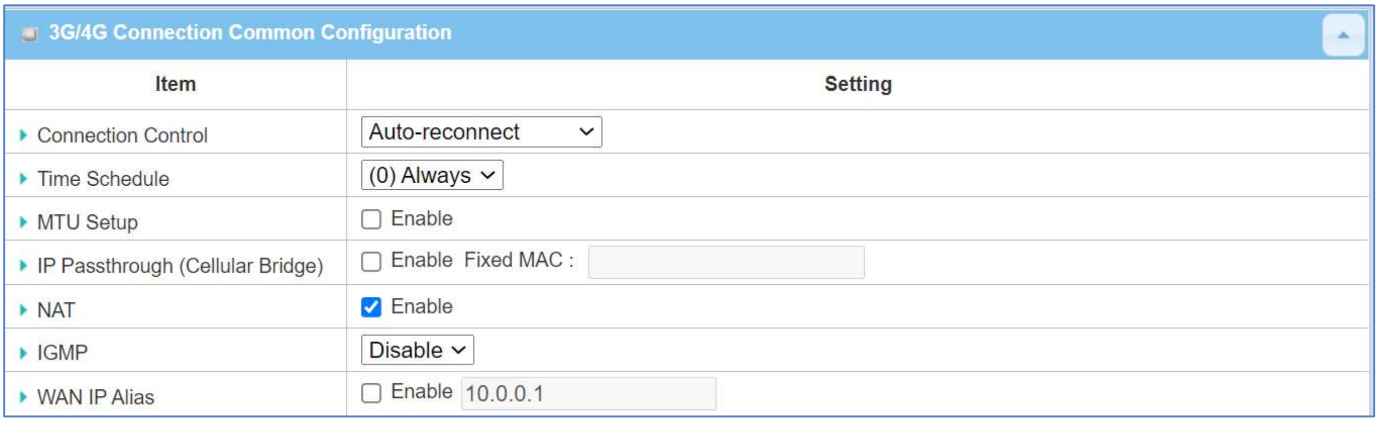


Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	Edit
WAN-2	-	Disable	-	Edit

Internet Connection Configuration (WAN-1)

Item	Setting
WAN Type	3G/4G



3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect
Time Schedule	(0) Always
MTU Setup	☐ Enable
IP Passthrough (Cellular Bridge)	☐ Enable Fixed MAC :
NAT	☑ Enable
IGMP	Disable
WAN IP Alias	☐ Enable 10.0.0.1

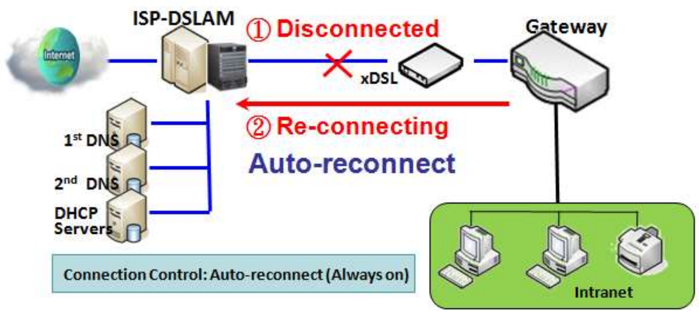
Ethernet WAN Common Configuration		
Item	**Value setting**	**Description**
Connection Control	Required setting	There are three connection modes. • **Auto-reconnect** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.**

		Internet connection will be inactive after it has been inactive for specified idle time.
Time Schedule	1. (0)Always	Connection always on.
MTU Setup	1. An Optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the **MTU** for the 3G/4G connection. **MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. ***Value Range***: 1200 ~ 1500.
IP Pass-through (Cellular Bridge)	1. Unchecked by default 2. String format for **Fixed MAC**: MAC address, e.g. 00:50:18:aa:bb:cc	When **Enable** box is checked, it means the device will directly assign the WAN IP to the first connected local LAN client. However, when an optional **Fixed MAC** is filled-in a non-zero value, only the client with this MAC address can obtain the WAN IP address. **Note**: When the **IP Pass-through** is on, **NAT** and **WAN IP Alias** will be unavailable until the function is disabled again.
NAT	1. An optional setting 2. NAT is enabled by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
IGMP	1. Required setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. **Uncheck** by default	Enable **WAN IP Alias** then enter the IP address provided by your service provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP addresses to your LAN.

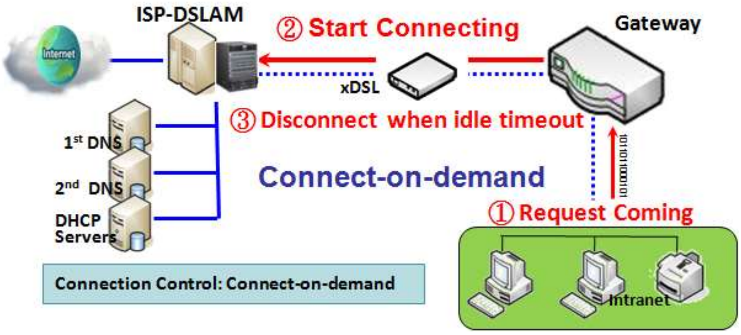
Ethernet Connection Common Configuration

There are some important parameters to be set up no matter which type of WAN is selected.

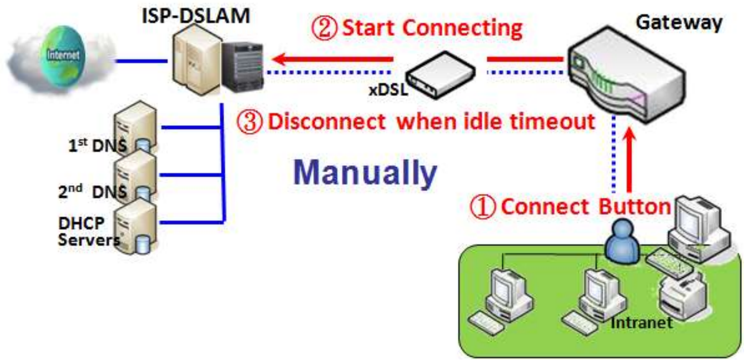
***Connection Control*.**



Auto-reconnect: The gateway will establish an Internet connection automatically once it has been booted up, and try to reconnect once the connection is down. It is recommended to choose this scheme for mission critical applications to ensure full-time Internet connection.



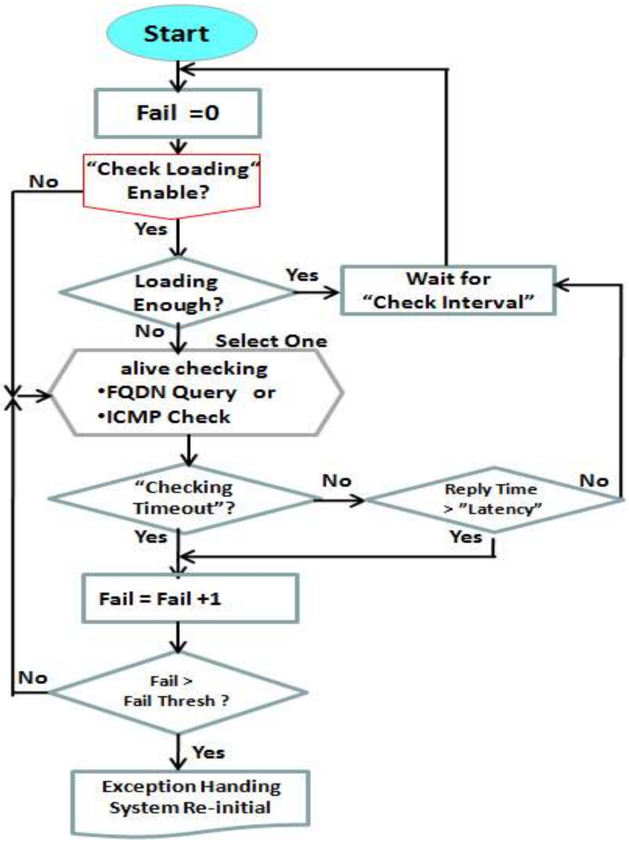
Connect-on-demand: The gateway will not start to establish an Internet connection until local data is going to be sent to the WAN side. After normal data transfer between LAN and WAN sides, this gateway will disconnect the WAN connection if idle time reaches value of **Maximum Idle Time**.



Manually: This gateway will not start to establish a WAN connection until the “Connect” button in web UI is pressed. After normal data transfer between LAN and WAN sides, this gateway will disconnect if idle time reaches value of **Maximum Idle Time**.

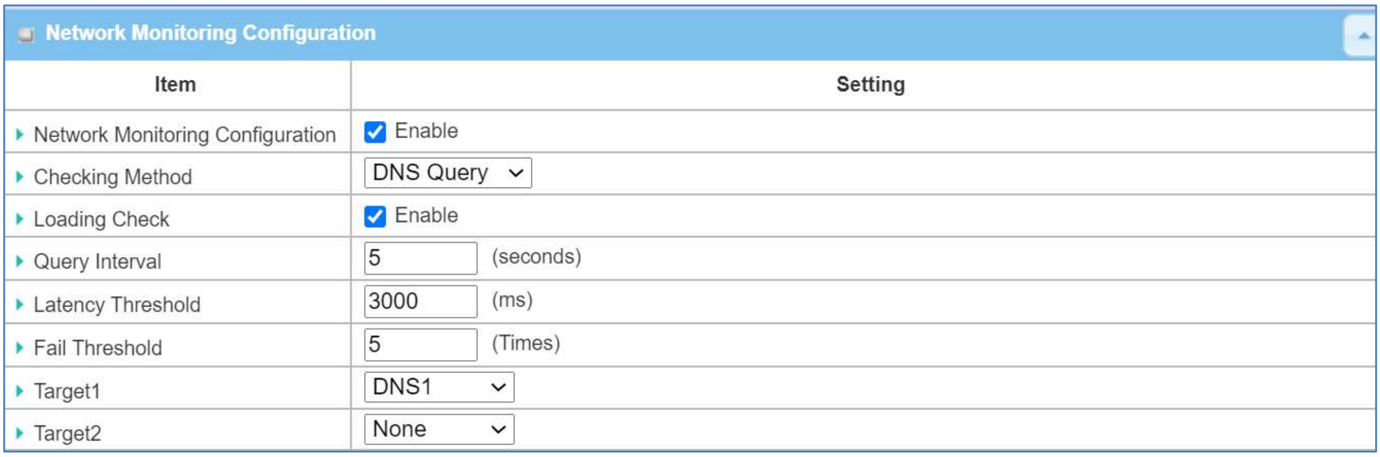
Note: If the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will not be available on both WANs as the system must set it to “Auto-reconnect” (Always on).

Network Monitoring



When it is necessary to monitor connection status continuously, "ICMP Check" and "FQDN Query" are used. When there is high connection traffic, checking packets will waste bandwidth, and the response time of replied packets may also increase. To prevent "Network Monitoring" from working abnormally, enabling the "Checking Loading" option will stop connection checking when there is high traffic. It will wait for another "Check Interval" and then check loading again.

When you do “Network Monitoring”, if the reply time is longer than "Latency" or no response time is longer than "Checking Timeout", the "Fail" count will be increased. If it is continuous and "Fail" count is more than the configured "Fail Threshold", the gateway will do an exception handling process and re-initialize the connection again. Otherwise, network monitoring process will restart.



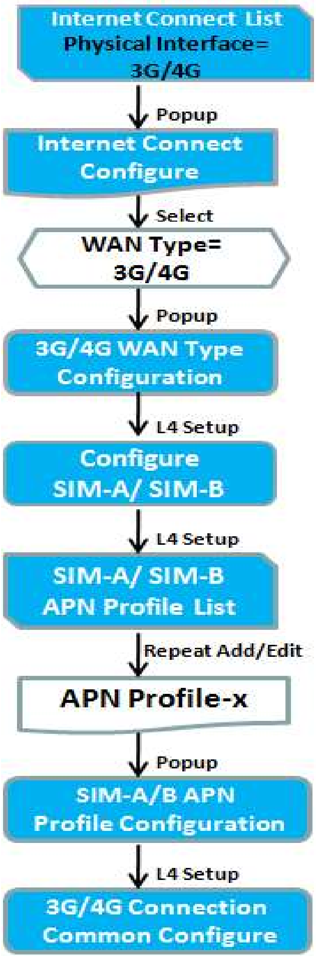
Network Monitoring Configuration

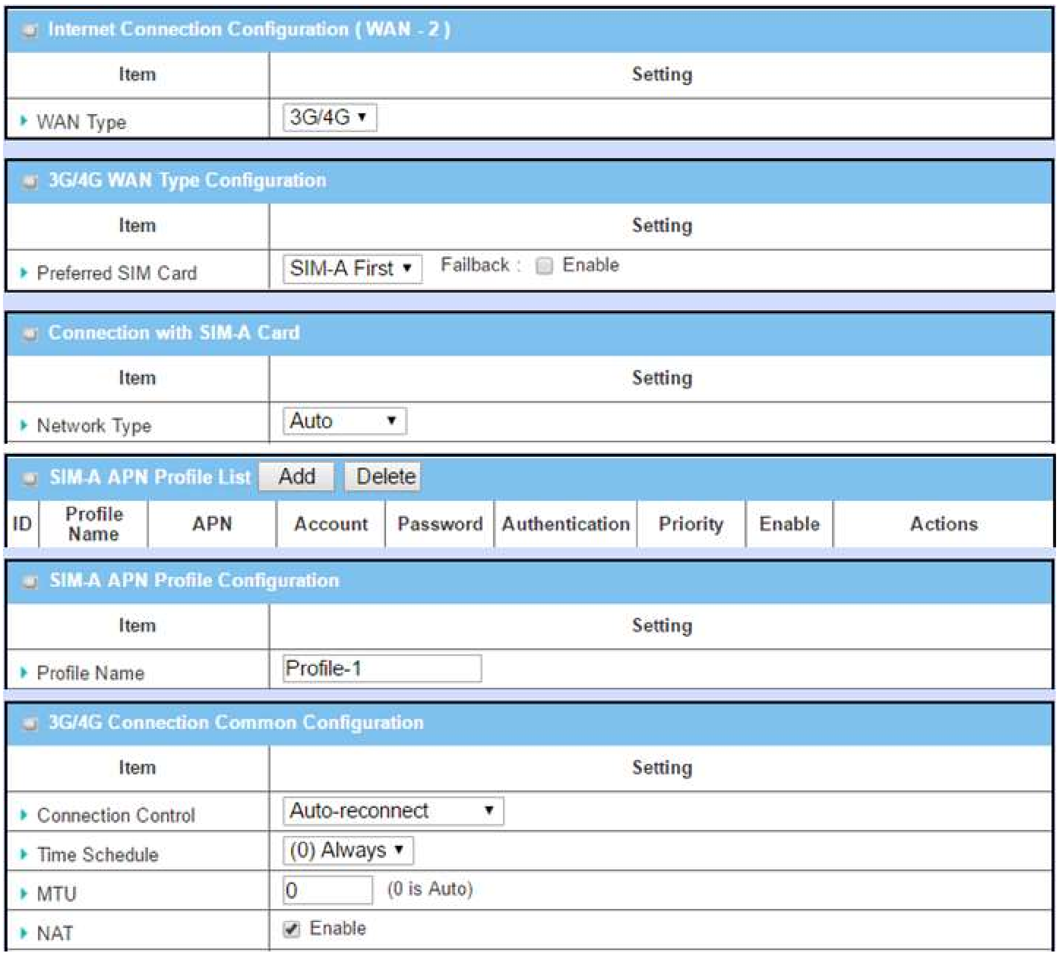
Item	Setting
Network Monitoring Configuration	☑ Enable
Checking Method	DNS Query
Loading Check	☑ Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)
Fail Threshold	5 (Times)
Target1	DNS1
Target2	None

Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. Optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. Optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets.
Loading Check	1. Optional setting 2. Box is checked by default	Check the **Enable** box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. **Latency Threshold** defines the tolerance threshold of responding time. **Fail Threshold** specifies the number of detected disconnections before the router recognizes the WAN link down status. Enter a number of detected disconnection times as the threshold for disconnection.
Query Interval	1. Optional setting 2. 5 seconds is selected by default.	Specify a time interval as the DNS **Query Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. **Value Range**: 2 ~ 14400.
Check Interval	1. Optional setting 2. 5 seconds is selected by default.	Specify a time interval as the ICMP **Checking Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. **Value Range:** 2 ~ 14400.
Latency Threshold	1. Optional setting 2. 3000 ms is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Latency Threshold** defines the tolerance threshold of responding time.

		Value Range: 2000 ~ 3000 seconds.
Fail Threshold	1. Optional setting 2. 5 times is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. **Value Range:** 1 ~ 10 times.
Target 1	1. Optional setting 2. **DNS1** is selected by default	**Target1 specifies** the first target of sending DNS query/ICMP request. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. Optional setting 2. **None** is selected by default	**Target1** specifies the second target of sending DNS query/ICMP requests. **None:** no second target is required. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.

Internet Connection – 3G/4G WAN




Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	3G/4G ▾

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First ▾ Failback : □ Enable

Connection with SIM-A Card

Item	Setting
Network Type	Auto ▾

SIM-A APN Profile List Add Delete

ID	Profile Name	APN	Account	Password	Authentication	Priority	Enable	Actions

SIM-A APN Profile Configuration

Item	Setting
Profile Name	Profile-1

3G/4G Connection Common Configuration

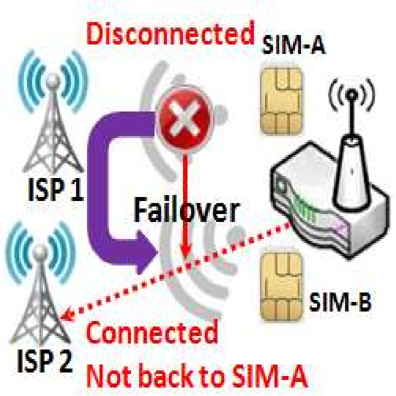
Item	Setting
Connection Control	Auto-reconnect ▾
Time Schedule	(0) Always ▾
MTU	0 (0 is Auto)
NAT	☑ Enable

Preferred SIM Card – Dual SIM Fail Over

For 3G/4G embedded devices, one embedded cellular module can create only one WAN interface. This device features dual SIM cards for one module with special fail-over mechanism. It is called Dual SIM Failover. This feature is useful for ISP switch-over when location is changed. Within "Dual SIM Failover," there are various usage scenarios, including "SIM-A First," "SIM-B First" with "Failback" enabled or not, and "SIM-A Only and "SIM-B Only".

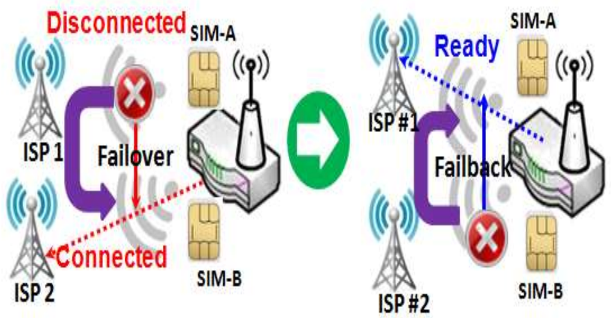
SIM-A/SIM-B only: When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one used for negotiation parameters between the gateway device and cellular ISP.

SIM-A / SIM-B first without Failback enabled



By default, the “SIM-A First” scenario is used to connect to cellular ISP for data transfer. In the case of “SIM-A First” or “SIM-B First” scenario, the gateway will try to connect to the Internet by using SIM-A or SIM-B card first. If the connection is broken, the gateway will automatically switch to use the other SIM card as an alternate and **will not switch back** to use original SIM card except when the current SIM connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transfer when current connection is still alive.

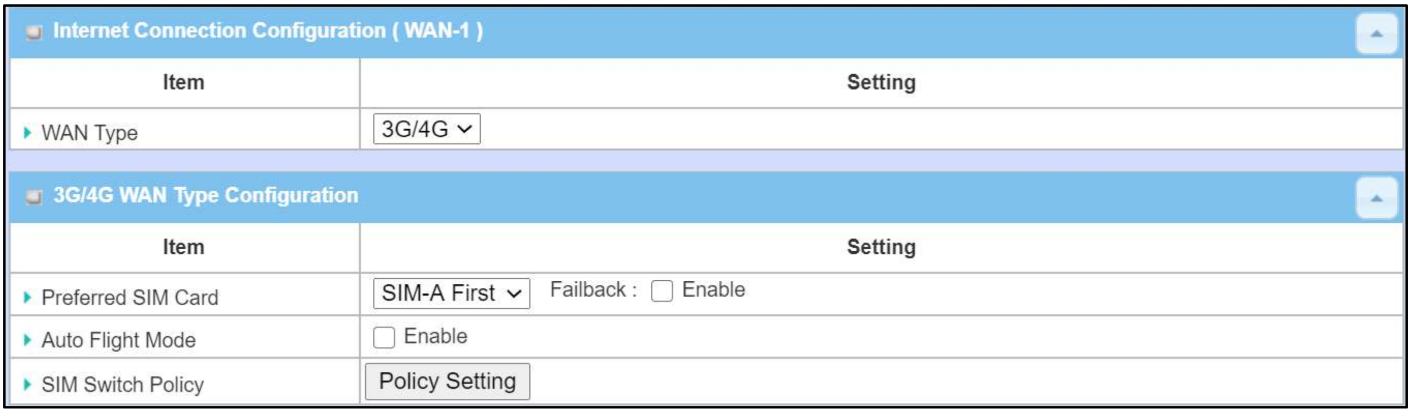
SIM-A / SIM-B first with Failback enabled



With Failback option enabled, “SIM-A First” scenario is used to connect when the connection is broken, gateway system will switch to use SIM-B. And when SIM-A connection is recovered, it will switch back to use the original SIM-A card

Configure 3G/4G WAN Setting

When the **Edit** button is applied, **Internet Connection Configuration**, and **3G/4G WAN Configuration** screens will appear.



Internet Connection Configuration (WAN-1)

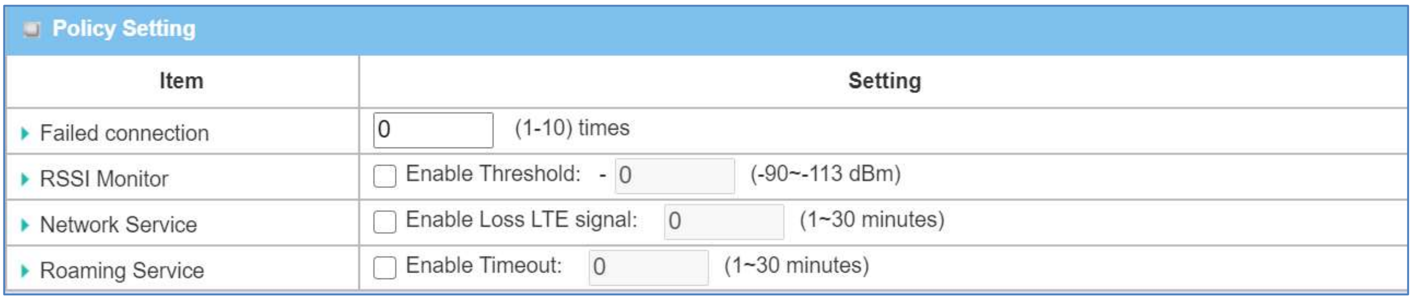
Item	Setting
WAN Type	3G/4G

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First Failback : □ Enable
Auto Flight Mode	□ Enable
SIM Switch Policy	Policy Setting

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	1. Required setting 2. **3G/4G** is set by default.	From the dropdown box, select the Internet connection method for 3G/4G WAN Connection. Only **3G/4G** is available for this model.
Preferred SIM Card	1. Required setting 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for the connection. When **SIM-A First** or **SIM-B First** is selected, it means the connection is built first by using SIM A/SIM B. If the connection fails, it will switch to the other SIM card and try to dial again, until the connection is up. When **SIM-A only** or **SIM-B only** is selected, it will try to dial up only using the SIM card you selected. When **Failback** is checked, it means if the connection is dialed-up not using the main SIM you selected, it will failback to the main SIM and try to establish the connection periodically. **Note_1**: For products with a single SIM design, only **SIM-A Only** option is available. **Note_2**: **Failback** is available only when **SIM-A First** or **SIM-B First** is selected.
Auto Flight Mode	Unchecked by default	Check the **Enable** box to activate the function. By default, if you disabled the **Auto Flight Mode**, the cellular module will always occupy a physical channel with cellular tower. It can get data connection instantly, and receive managing SMS all the time on required. If you enable the **Auto Flight Mode**, the gateway will pop up a message "Flight mode will cause cellular function to be malfunctioned when the data session is offline." , and it will make the cellular module into flight mode and disconnected with cellular tower physically. In, addition, whenever the cellular module is going to be used for data connection to backup the failed primary connection, the cellular module will be active to connect with cellular tower and get the data connection for use, it takes few more seconds. **Note:** Keep it unchecked unless your cellular ISP asked the connected gateway to enable the Auto Flight Mode.
SIM Switch Policy		Click the **Policy Setting** button to define the SIM switch policy or browse the current policy settings.

SIM Switch Policy Settings



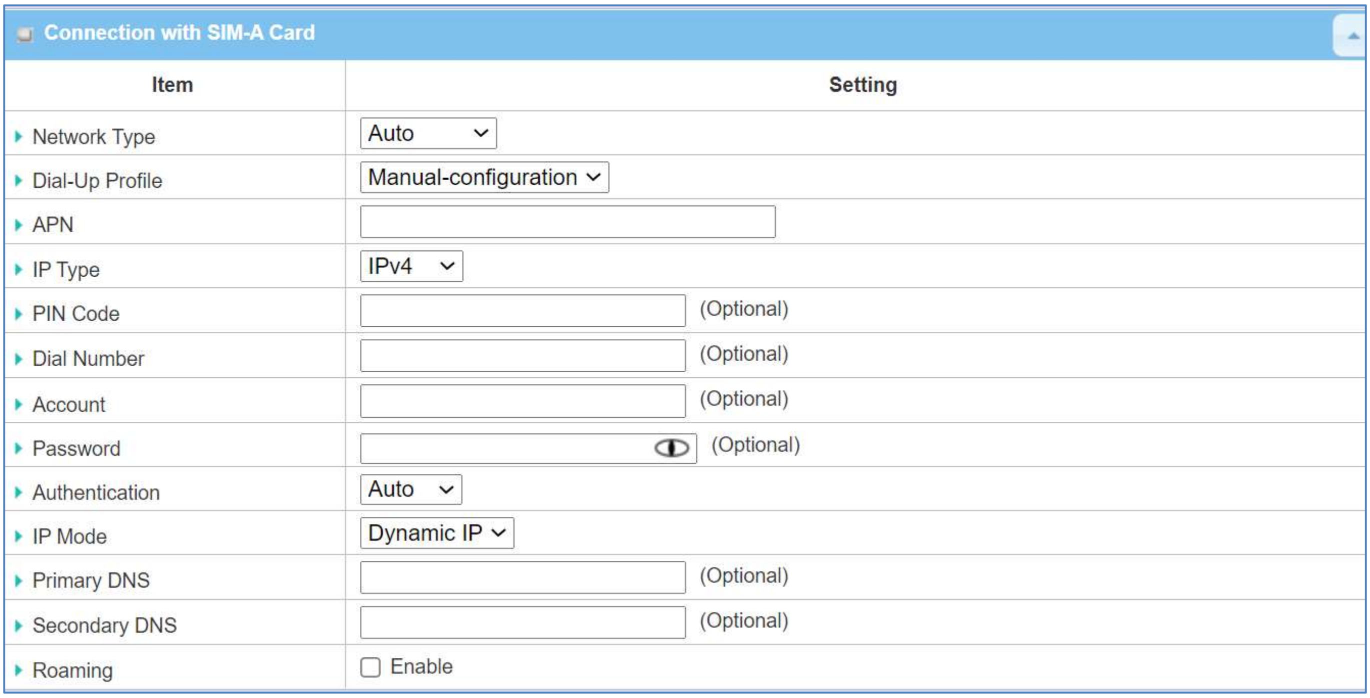
Policy Setting

Item	Setting
Failed connection	0 (1-10) times
RSSI Monitor	□ Enable Threshold: - 0 (-90~-113 dBm)
Network Service	□ Enable Loss LTE signal: 0 (1~30 minutes)
Roaming Service	□ Enable Timeout: 0 (1~30 minutes)

Policy Setting		
Item	**Value setting**	**Description**
Failed connection	1. Required setting 2. **0** is set by default.	When the number of disconnections reaches the set value, it will switch to another sim card. For example, if a value of 2 is entered, and the system cannot connect for two times in a row, then it will switch to the other sim card.
RSSI Monitor	1. Unchecked by default	Click to enable, and set a value between -90~-113 dBm. When the signal strength goes below the set value, it will switch to the other sim card.
Network Service	Unchecked by default	Click to enable, and enter a time in minutes between 1 and 30. When the time of lost LTE signal reaches the set value, it will switch to the other sim card.
Roaming Service	Unchecked by default	Click to enable, and enter a time in minutes between 1 and 30. When the time of roaming service reaches the set value, it will switch to the other SIM card to connect.

Configure SIM-A / SIM-B Card

Here you can set configurations for the cellular connection according to your requirements.



Connection with SIM-A Card

Item	Setting
Network Type	Auto
Dial-Up Profile	Manual-configuration
APN	
IP Type	IPv4
PIN Code	(Optional)
Dial Number	(Optional)
Account	(Optional)
Password	(Optional)
Authentication	Auto
IP Mode	Dynamic IP
Primary DNS	(Optional)
Secondary DNS	(Optional)
Roaming	□ Enable

Note 1: Configuration of SIM-B card follows the same rules as configuration of SIM-A Card.

Note 2: Both **Connection with SIM-A Card** and **Connection with SIM-B Card** will pop up only when the **SIM-A First** or **SIM-B First** is selected, otherwise only one will pop up.

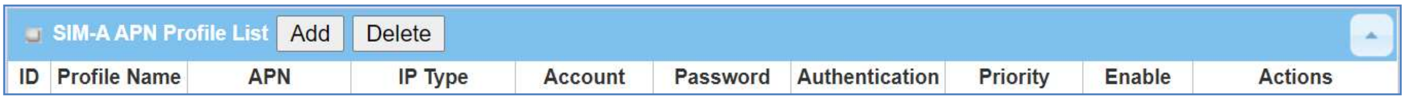
Connection with SIM-A/-B Card		
Item	**Value setting**	**Description**
Network Type	1. Required setting	Select **Auto** to register a network automatically, regardless of the network

	2. By default **Auto** is selected	type. Select **2G Only** to register 2G networks only. Select **2G Prefer** to register 2G networks first if available. Select **3G only** to register 3G networks only. Select **3G Prefer** to register 3G networks first if available. Select **LTE only** to register LTE networks only. **Note**: Options may vary by model.
Dial-Up Profile	1. Required setting 2. By default **Manual-configuration** is selected	Specify the type of dial-up profile for your 3G/4G network. It can be **Manual-configuration**, **APN Profile List**, or **Auto-detection**. Select **Manual-configuration** to set **APN** (Access Point Name), **Dial Number**, **Account**, and **Password** to what your carrier provides. Select **APN Profile List** to set more than one profile to dial up in turn, until the connection is established. A new field will pop up. Go to **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List** for details. Select **Auto-detection** to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database. **Note_1:** It is highly recommended to select the **Manual** or **APN Profile List** to specify the network for your subscription. Your ISP should provide such network settings. **Note_2:** If you select **Auto-detection,** it is likely to connect to an improper network, or fail to find a valid APN for your ISP.
APN	1. Required setting 2. String format: any text	Enter the **APN** you want to use to establish the connection. This is a required setting if you selected **Manual-configuration** as dial-up profile scheme.
IP Type	1. Required setting	Select **IPv4**, **IPv6**, or **IPv4/6**
PIN code	1. Optional setting 2. String format: integer	Enter the PIN (Personal Identification Number) code if needed to unlock your SIM card.
Dial Number, Account, Password	1. Optional setting 2. String format: any text	Enter the optional **Dial Number**, **Account**, and **Password** settings if your ISP provided these settings. Note: These settings are only displayed when **Manual-configuration** is selected.
Authentication	1. Required setting 2. By default **Auto** is selected	Select **PAP** (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server. Select **CHAP** (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server. When **Auto** is selected, it means it will authenticate with the server using either **PAP** or **CHAP**.
IP Mode	1. Required setting 2. By default **Dynamic IP** is selected	When **Dynamic IP** is selected, it means it will get all IP configurations from the carrier's server and set to the device directly. If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to **Static IP** mode and fill in all parameters that required, such as IP address, subnet mask and gateway. **Note**: **IP Subnet Mask** is a required setting. Make sure you have the right configuration.
Primary DNS	1. Optional setting 2. String format: IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.

Secondary DNS	1. Optional setting 2. String format: IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Roaming	Unchecked by default	Check the box to establish the connection even if the registration status is roaming, not in home network. **Note**: Additional charges may be incurred if the connection is set to roaming.

Create/Edit SIM-A / SIM-B APN Profile List

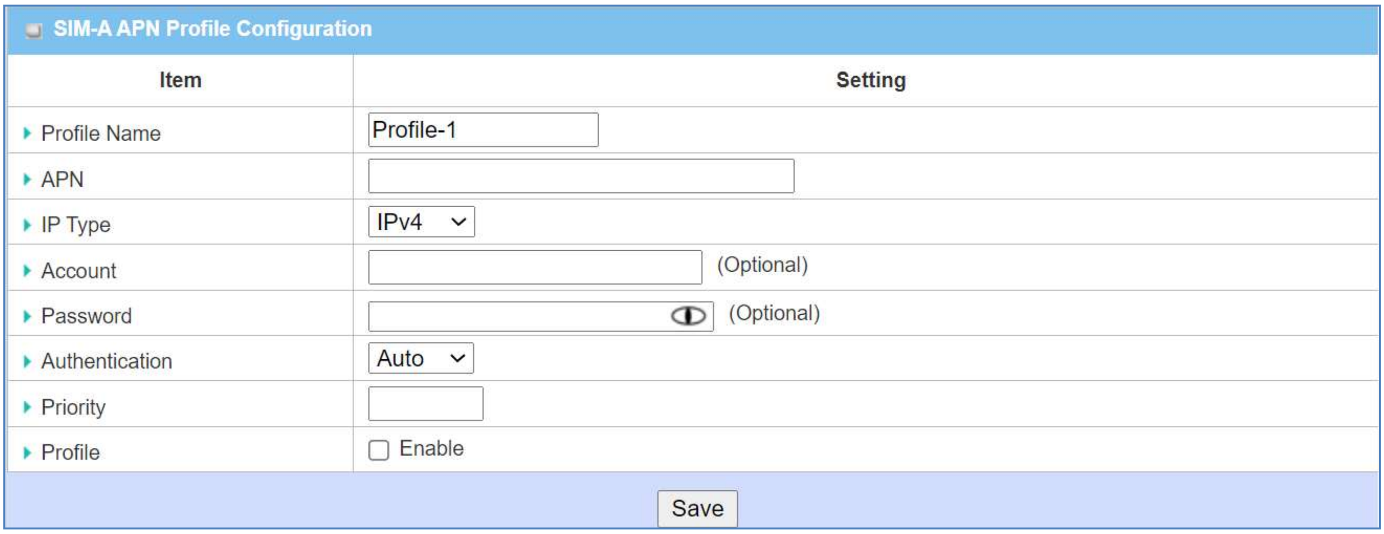
You can add a new APN profile for the connection, or modify the contents of an APN profile you have added. It is available only when you select **Dial-Up Profile** as **APN Profile List**.



ID	Profile Name	APN	IP Type	Account	Password	Authentication	Priority	Enable	Actions

This lists all the APN profiles you created, making it easy to check and modify. It is available only when you select **Dial-Up Profile** as **APN Profile List**.

When **Add** button is applied, an **APN Profile Configuration** screen will appear.



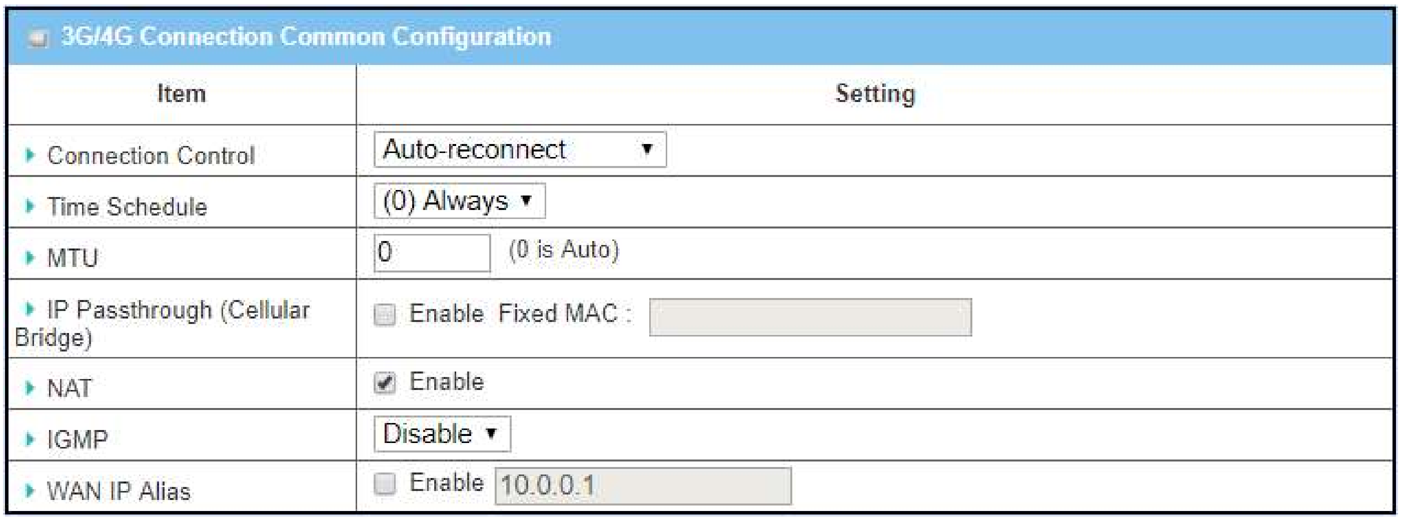
Item	Setting
Profile Name	Profile-1
APN	
IP Type	IPv4
Account	(Optional)
Password	(Optional)
Authentication	Auto
Priority	
Profile	☐ Enable

SIM-A/-B APN Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	1. By default **Profile-x** is listed 2. String format: any text	Enter the profile name you want to describe for this profile.
APN	String format: any text	Enter the **APN** you want to use to establish the connection.
IP Type	1. Required setting	Select **IPv4**, **IPv6**, or **IPv4/6**
Account	String format: any text	Enter the **Account** you want to use for the authentication. ***Value Range***: 0 ~ 53 characters.
Password	String format: any text	Enter the **Password** you want to use for the authentication.
Authentication	1. Required setting	Select the Authentication method for the 3G/4G connection.

	2. **Auto** is selected by default	It can be **Auto**, **PAP**, **CHAP**, or **None**.
Priority	1. Required setting 2. String format: integer	Enter the value for the dial-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number. ***Value Range***: 1 ~ 16.
Profile	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the previous page.

Setup 3G/4G Connection Common Configuration

Here you can change common configurations for 3G/4G WAN.

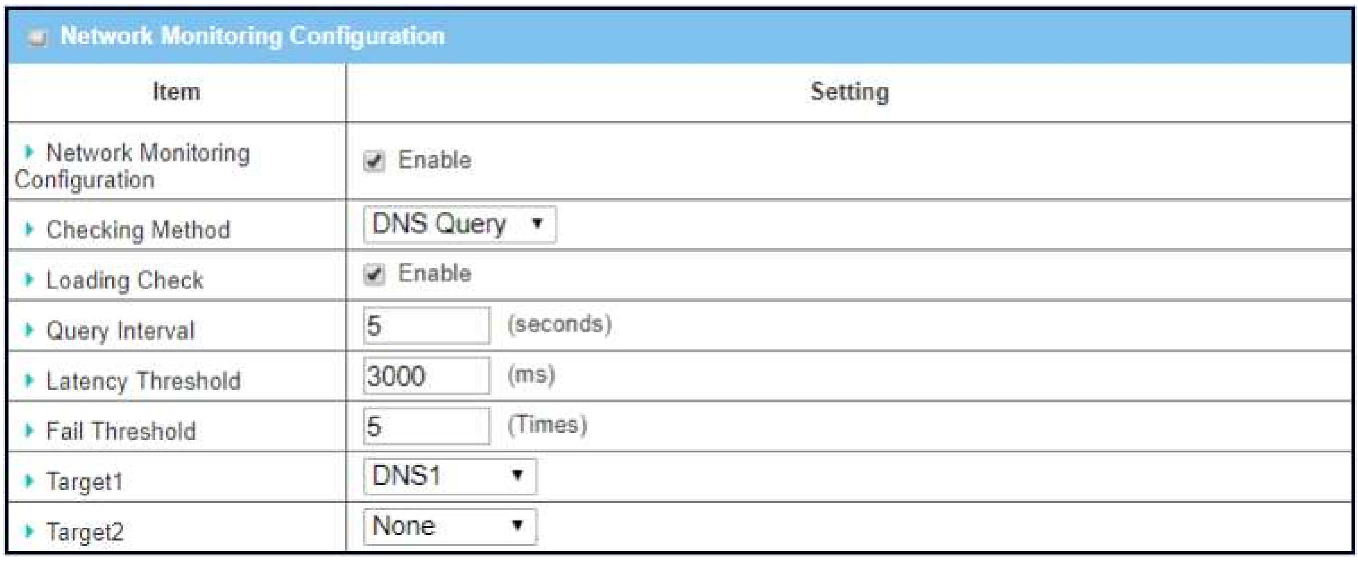


3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect ▾
Time Schedule	(0) Always ▾
MTU	0 (0 is Auto)
IP Passthrough (Cellular Bridge)	□ Enable Fixed MAC :
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

3G/4G Connection Common Configuration		
Item	**Value setting**	**Description**
Connection Control	By default **Auto-reconnect** is selected	When **Auto-reconnect** is selected, it means the device will try to keep the Internet connection on at all timed whenever the physical link is connected. When **Connect-on-demand** is selected, it means the Internet connection will be established only when data traffic is detected. When **Connect Manually** is selected, it means the **Connect** button must be clicked to dial up the connection manually. Please go to **Status > Basic Network > WAN & Uplink** tab for details. **Note**: If the WAN interface serves as the primary one for another WAN interface in Failover role(and vice versa), the Connection Control parameter will not be available on both WANs as the system must set it to "Auto-reconnect"
Time Schedule	1. Required setting	When **(0) Always** is selected, it means this WAN is operating all the time.

	2. By default **(0) Always** is selected	Once you have set other schedule rules, there will be other options to select. Please go to **Object Definition > Scheduling** for details.
MTU	1. Required setting 2. By default **0** is filled-in	Specify the **MTU** (Maximum Transmission Unit) for the 3G/4G connection. ***Value Range***: 512 ~ 1500, 0 is for auto.
IP Pass-through (Cellular Bridge)	1. Unchecked by default 2. String format for **Fixed MAC**: MAC address, e.g. 00:50:18:aa:bb:cc	When **Enable** box is checked, it means the device will directly assign the WAN IP to the first connected local LAN client. However, when an optional **Fixed MAC** is a non-zero value, it means only the client with this MAC address can get the WAN IP address. **Note**: When the **IP Pass-through** is on, **NAT** and **WAN IP Alias** will be unavailable until the function is disabled again.
NAT	Checked by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
IGMP	By default **Disable** is selected	Select **Auto** to enable **IGMP** function. Check the **Enable** box to enable **IGMP Proxy**.
WAN IP Alias	1. Unchecked by default 2. String format: IP address (IPv4 type)	Check the box to enable **WAN IP Alias**, and fill in the IP address you want to assign.



Network Monitoring Configuration

Item	Setting
Network Monitoring Configuration	☑ Enable
Checking Method	DNS Query ▾
Loading Check	☑ Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)
Fail Threshold	5 (Times)
Target1	DNS1 ▾
Target2	None ▾

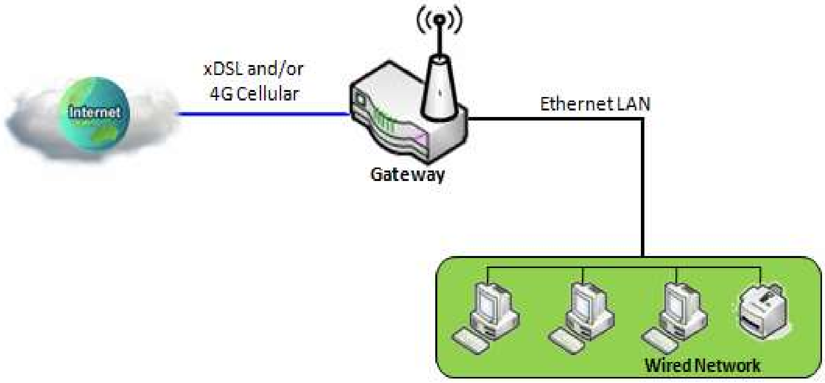
Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. Optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. Optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets.
Loading Check	1. Optional setting	Check the **Enable** box to activate the loading check function.

	2. Box is checked by default	Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. **Latency Threshold** defines the tolerance threshold of responding time. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detected disconnection times to be the threshold before disconnection is acknowledged.
Query Interval	1. Optional setting 2. 5 seconds is selected by default.	Specify a time interval as the DNS **Query Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. **Value Range:** 2 ~ 14400.
Check Interval	1. Optional setting 2. 5 seconds is selected by default.	Specify a time interval as the ICMP **Checking Interval**. Query Interval defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. **Value Range:** 2 ~ 14400.
Latency Threshold	1. Optional setting 2. 3000 ms is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Latency Threshold** defines the tolerance threshold of responding time. **Value Range:** 2000 ~ 3000 seconds.
Fail Threshold	1. Optional setting 2. 5 times is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. **Value Range:** 1 ~ 10 times.
Target 1	1. Optional setting 2. **DNS1** is selected by default	**Target1 specifies** the first target of sending DNS query/ICMP request. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. Optional setting 2. **None** is selected by default	**Target1 specifies** the second target of sending DNS query/ICMP request. **None:** no second target is required. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

3.2 LAN & VLAN

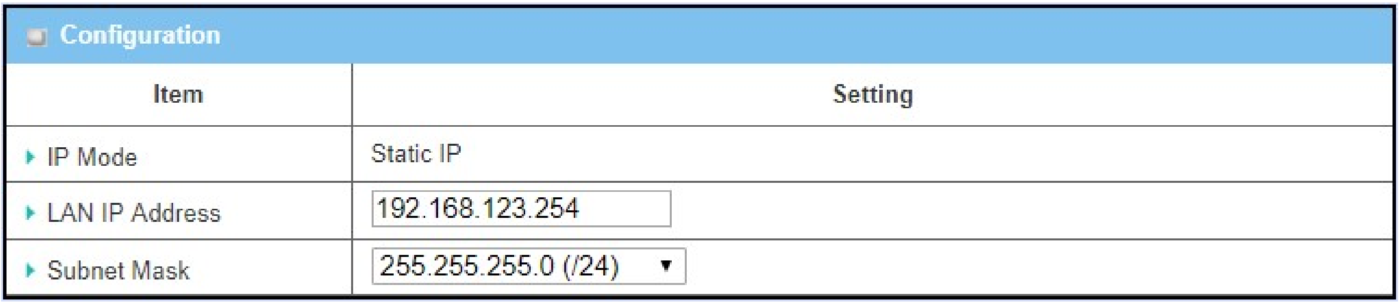
This section describes the configuration of LAN and VLAN. VLAN is an optional feature, and its presence depends on the gateway model.

3.2.1 Ethernet LAN



The Local Area Network (LAN) can be used to share data or files among computers attached to a network. The following diagram illustrates a network of wired and interconnected computers.

Follow the following instructions to set up an IPv4 Ethernet LAN.



Configuration

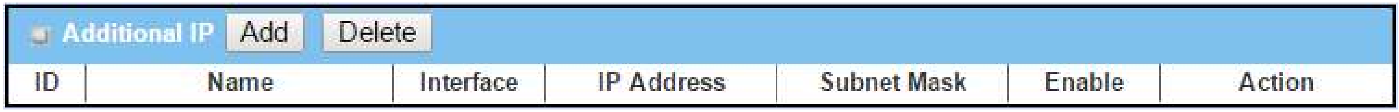
Item	Setting
IP Mode	Static IP
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24) ▾

Configuration Item	Value setting	Description
IP Mode	N/A	It shows the LAN IP mode for the gateway. **Static IP**: If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. **Dynamic IP**: If all the available WAN interfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	1. Required setting **2. 192.168.123.254 is set by default**	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. **Note**: This is also the IP address of the web UI. If you change it, you will need to enter the new IP address in the browser in order to see the web UI.
Subnet Mask	1. Required setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP

		addresses are allowed in this subnet. However, one of them is occupied by the LAN IP address of this gateway, so there are a maximum of 253 clients allowed in LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore previous settings.

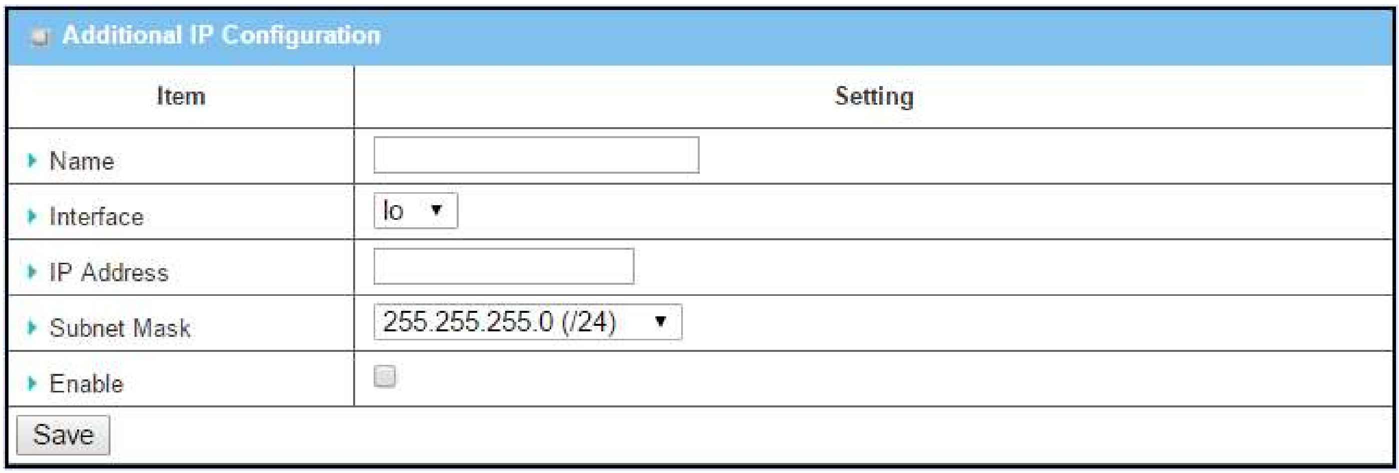
Create / Edit Additional IP

This gateway provides the LAN IP alias function for special management considerations. You can add additional LAN IPs for this gateway, and access this gateway through the additional IPs.



ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

When **Add** button is applied, The **Additional IP Configuration** screen will appear.



Item	Setting
Name	
Interface	lo ▼
IP Address	
Subnet Mask	255.255.255.0 (/24) ▼
Enable	□

Configuration Item	Value setting	Description
Name	1. Optional setting	Enter the name for the alias IP address.
Interface	1. Required setting 2. **lo** is set by default	Specify the Interface type. It can be **lo** or **br0**.
IP Address	1. Optional setting **2. 192.168.123.254 is set by default**	Enter the additional IP address for this device.
Subnet Mask	1. Required setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are a maximum of 253 clients allowed in the LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
Save	NA	Click the **Save** button to save the configuration

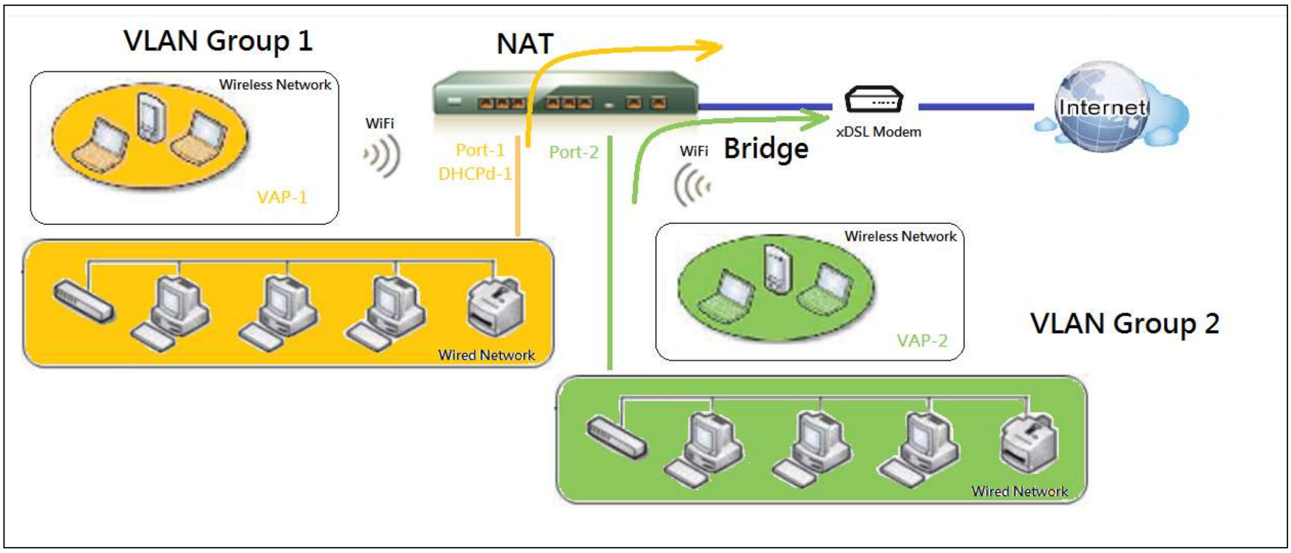
3.2.2 VLAN

VLAN (Virtual LAN) is a logical network under a certain switch or router device to group client hosts with a specific VLAN ID. This gateway supports both Port-based VLAN and Tag-based VLAN. These functions allow you to divide local network into different “virtual LANs”. It is common requirement for some application scenarios. For example, if there are various departments within an SMB, all client hosts in the same department should own common access privilege and QoS property. You can assign departments either by port-based VLAN or tag-based VLAN as a group, and then configure it as needed. In some cases, the ISP may need the router to support “VLAN tags” for certain kinds of services (e.g. IPTV). You can group all devices requiring this service in one tag-based VLAN.

If the gateway has only one physical Ethernet LAN port, only very limited configuration is available if you enable Port-based VLANs.

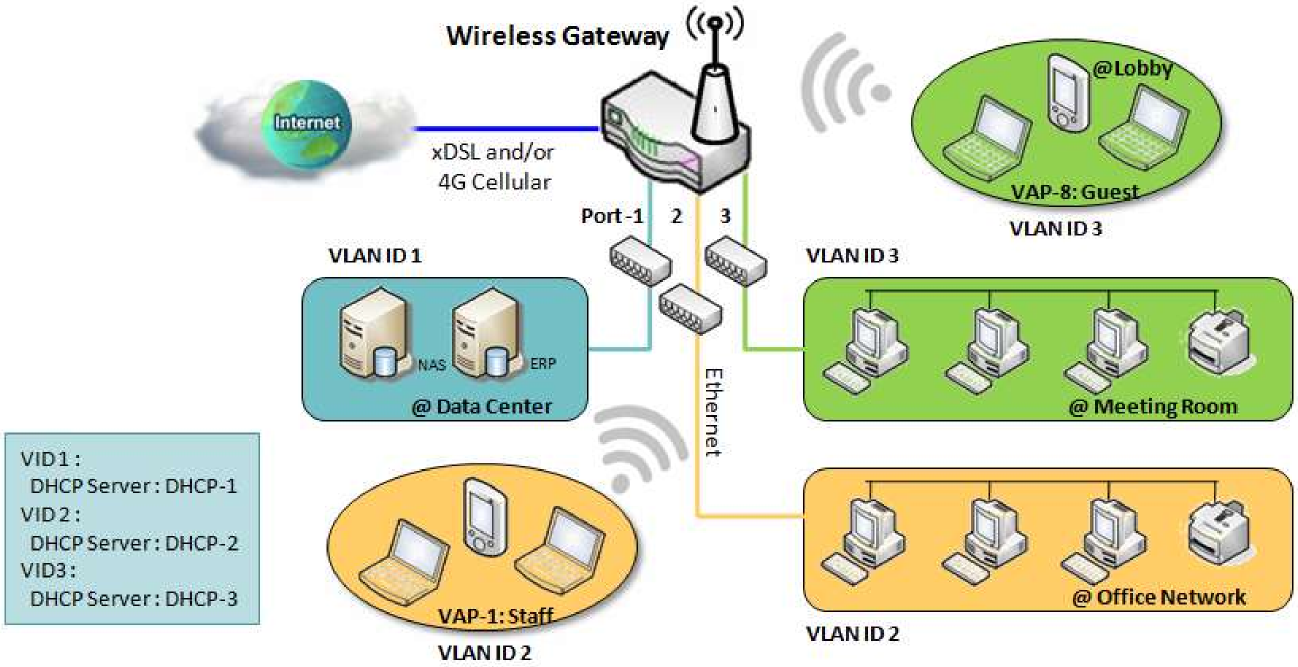
➢ Port-based VLAN

Port-based VLANs can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server can be allocated for a NAT VLAN group to let group host members obtain IP addresses. Thus, each host can access Internet via the NAT mechanism of business access gateway. In bridge mode, Intranet packet flow is delivered out WAN trunk port with VLAN tag to upper link for different services.



A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical LAN segment. The following is an example.

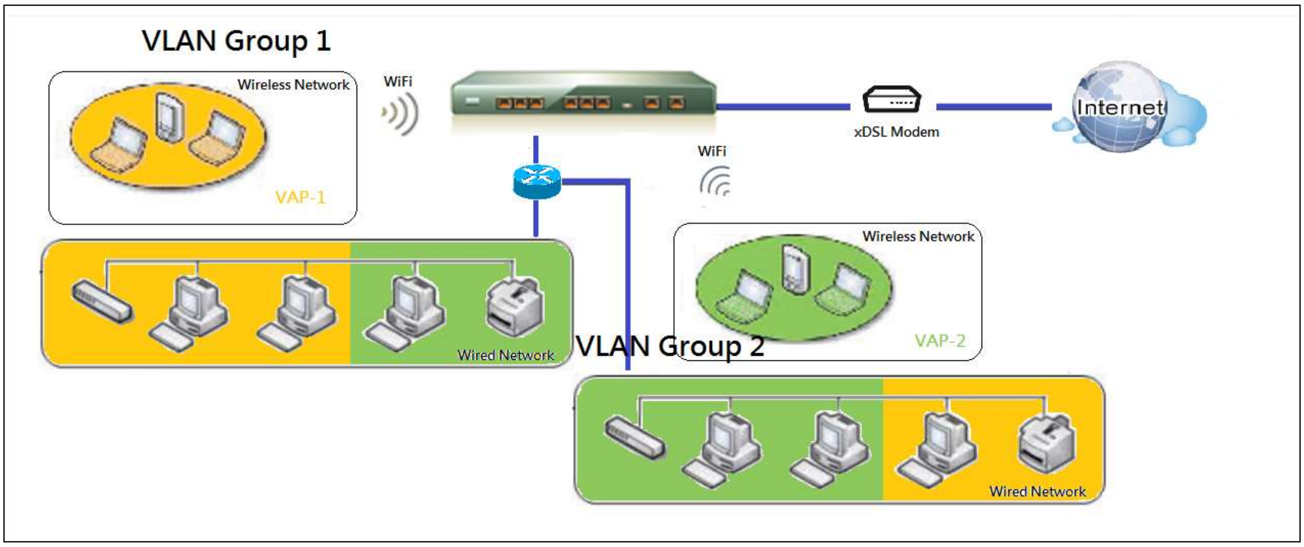
In a company, the administrator designs 3 network segments: Lobby/Meeting Room, Office, and Data Center. In a Wireless Gateway, the administrator can configure Lobby/Meeting Room segment with VLAN ID 3. The VLAN group includes Port-3 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. The office segment is configured with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode and DHCP-2 server equipped. Finally, the administrator also configures the Data Center segment with VLAN ID 1. The VLAN group includes Port-1 with NAT mode to WAN interface as shown in the following diagram.



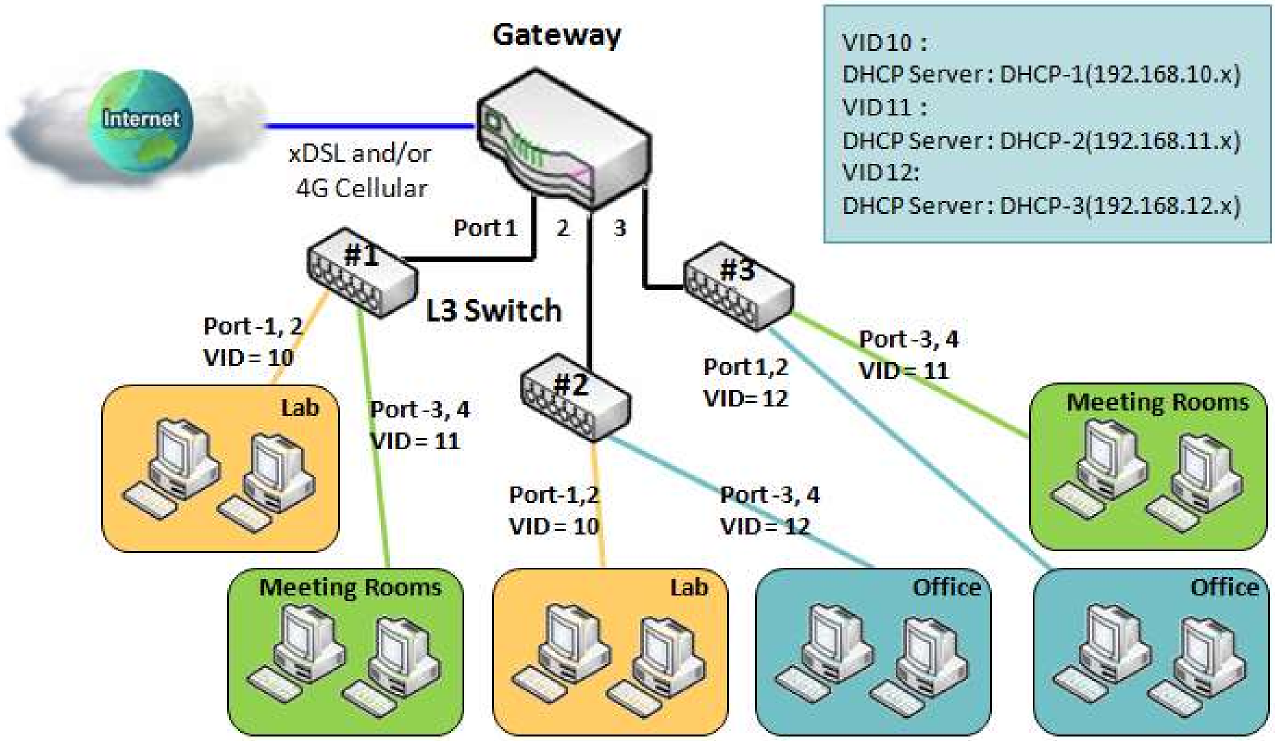
The above diagram shows a general case for a gateway with 3 Ethernet LAN ports. If the device has only one Ethernet LAN port, there will be only one VLAN group for the device. Under such a situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

➢ Tag-based VLAN

- ➢ The tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deployment in subnets. All packet flows can carry different VLAN tags even at the same physical Ethernet port. These flows can be directed to different destinations because they have differentiated tags. The approach is very useful to group hosts at different geographic locations into the same workgroup.
- ➢ Tag-based VLANs are also called VLAN Trunks. The VLAN Trunk collects all packet flows with different VLAN IDs from the router and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. The administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. The following is an example.



The administrator designs 3 network segments, Lab, Meeting Rooms, and Office. In a Secure VPN Gateway, the administrator can configure the Office segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configures the Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, client hosts in VLAN 11 group cannot access the Internet. At last, he configures the Lab segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet.

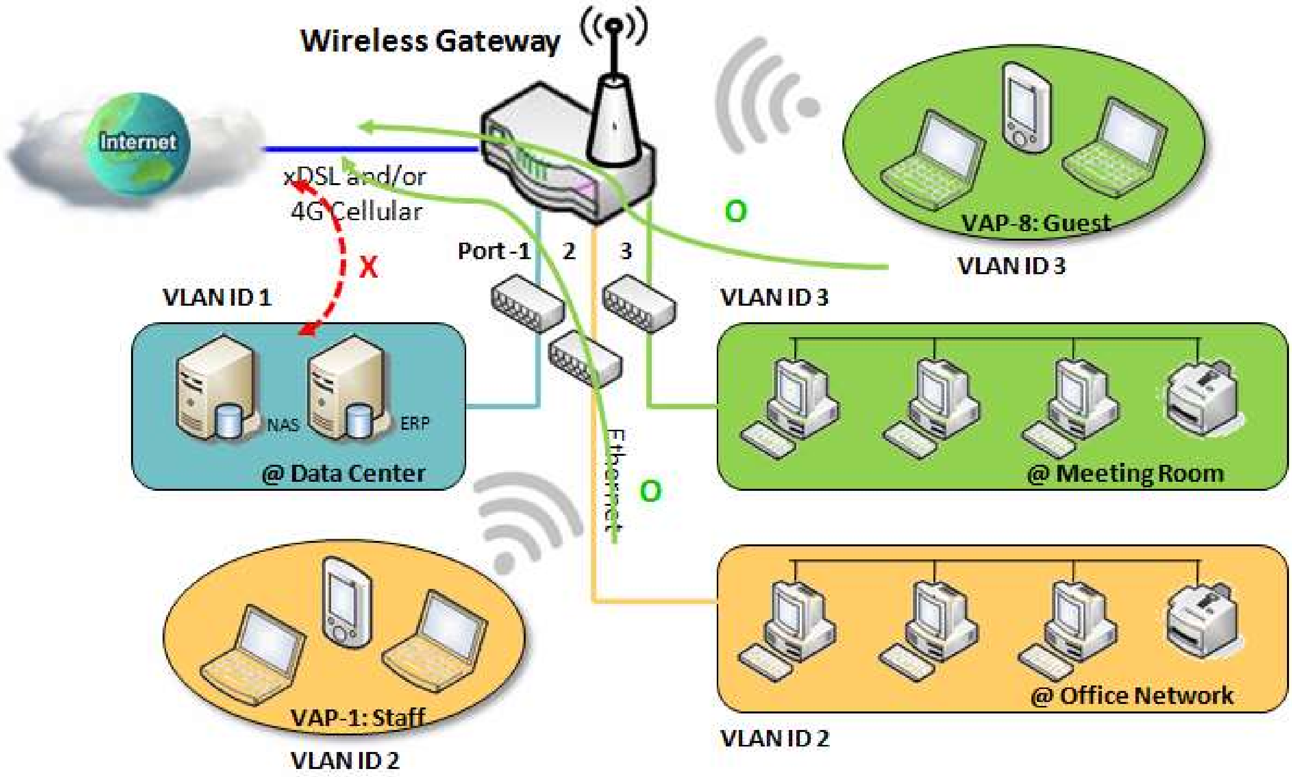


➢ VLAN Groups Access Control

The administrator can specify the Internet access permission for all VLAN groups. He can also configure which VLAN groups are allowed to communicate with each other.

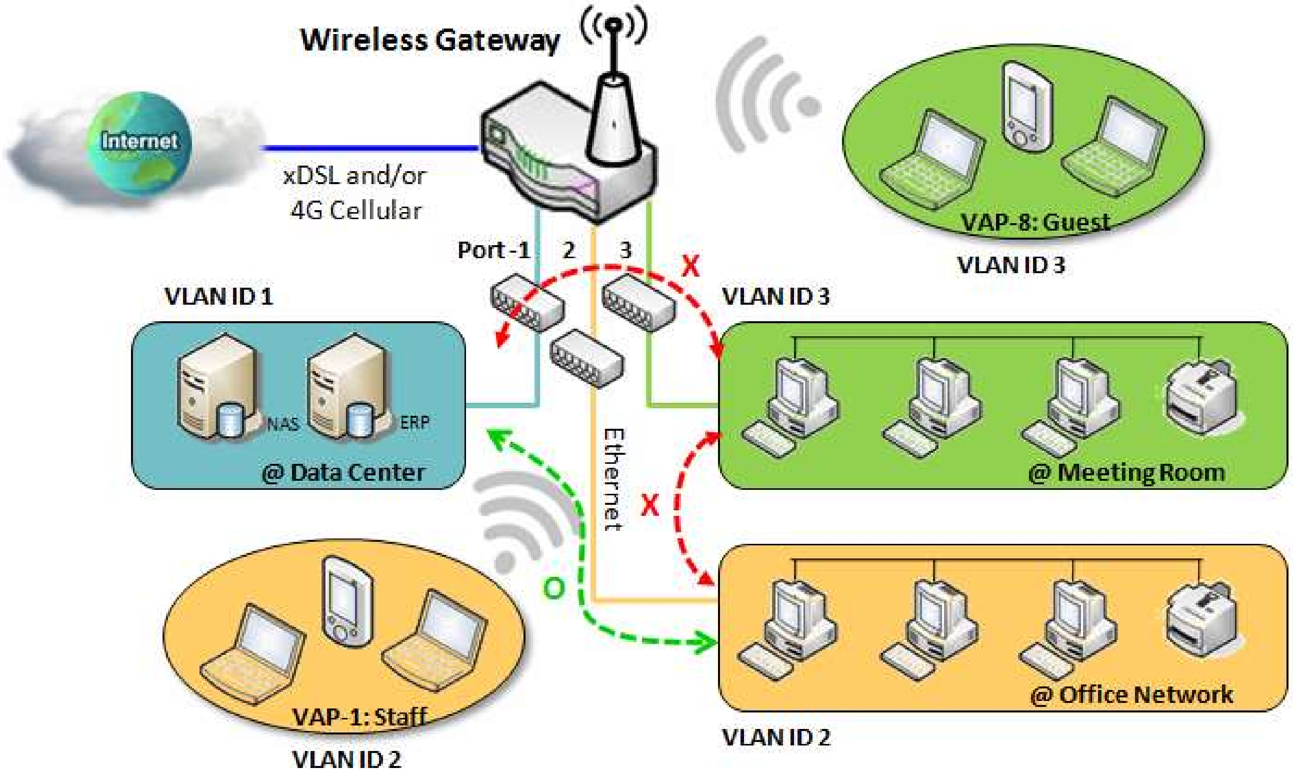
VLAN Group Internet Access

The administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 2 and 3 can access Internet but the one with VID 1 cannot access Internet. That is, visitors in the meeting room and staff in the office network can access Internet. But the computers/servers in data center cannot access Internet due to security considerations. The servers in the data center are only for trusted staff or are accessed through secure tunnels.



Inter VLAN Group Routing:

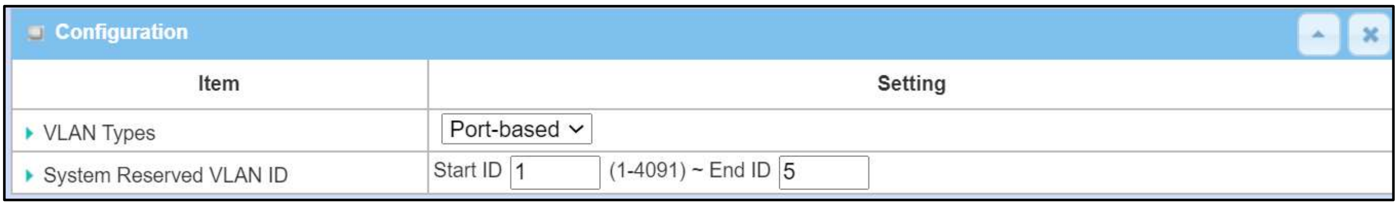
In Port-based tagging, the administrator can specify member hosts of one VLAN group to be able or not able to communicate with another VLAN group. This is a communication pair, and one VLAN group can join many communication pairs. But communication pairs do not have a transitive property. That is, if A can communicate with B, and B can communicate with C, it doesn't imply that A can communicate with C. An example is shown in the following diagram. VLAN groups of VID 1 and 2 can access each other but the ones between VID 1 and VID 3 and between VID 2 and VID 3 cannot.



VLAN Setting

Go to Basic Network > LAN & VLAN > VLAN Tab.

The VLAN function allows you to divide a local network into different virtual LANs, either port-based or tag-based.



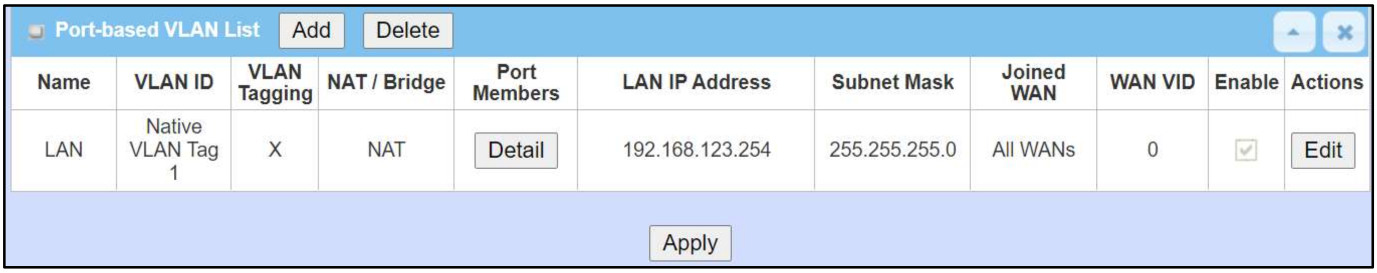
Configuration

Item	Setting
VLAN Types	Port-based
System Reserved VLAN ID	Start ID 1 (1-4091) ~ End ID 5

Configuration		
Item	**Value setting**	**Description**
VLAN Type	**Port-based** is selected by default	Select the VLAN type that you want to use. **Port-based**: Port-based VLAN allows you to add rules for each LAN port, and you can implement advanced controls with the VLAN ID. **Tag-based**: Tag-based VLAN allows you to add VLAN ID, and select members and DHCP Server for this VLAN ID. Go to **Tag-based VLAN List** table.
System Reserved VLAN ID	**1 ~ 5** is reserved by default	Specify the VLAN ID range that is reserved for the system operation. For the Port-based/Tag-based VLAN grouping, only use the ID outside the reserved range. **Value Range:** 1 ~ 4091.
Save	NA	Click the **Save** button to save the configuration

Port-based VLAN – Create/Edit VLAN Rules

The port-based VLAN allows you to customize each LAN port. There is a default rule that shows the configuration of all LAN ports. If your device has a DMZ port, you will see DMZ configuration too. The maximum number of rules is based on the number of LAN ports.



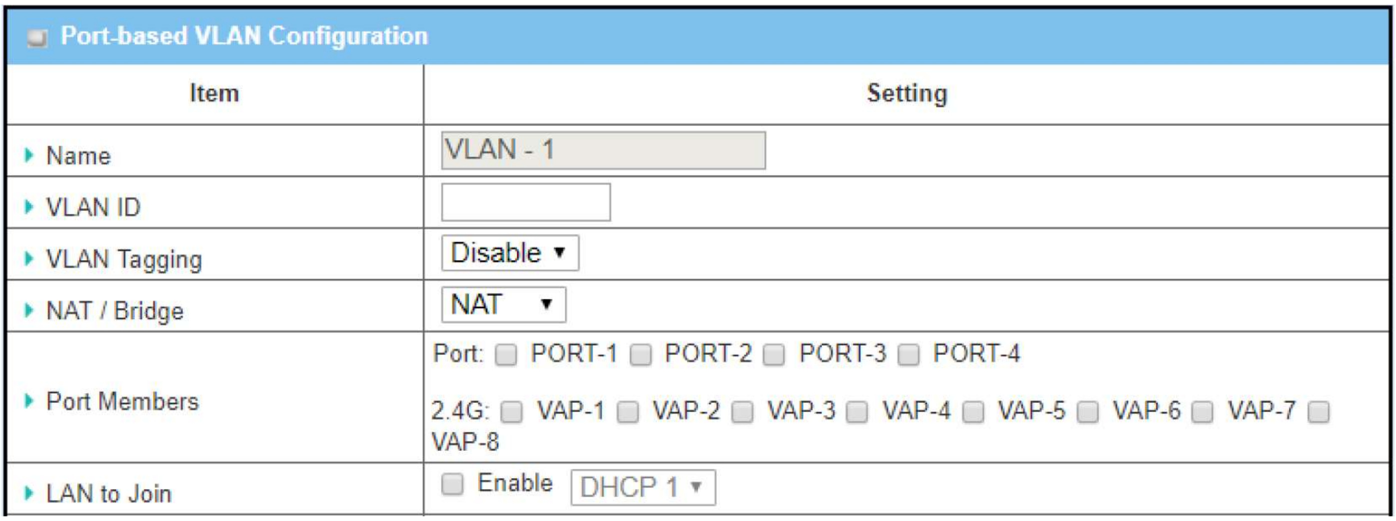
Port-based VLAN List Add Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit

Apply

When the **Add** button is applied, the Port-based VLAN Configuration screen will appear. It includes 3 sections: **Port-based VLAN Configuration**, **IP Fixed Mapping Rule List,** and **Inter VLAN Group Routing** (enter through a button).

Port-based VLAN – Configuration

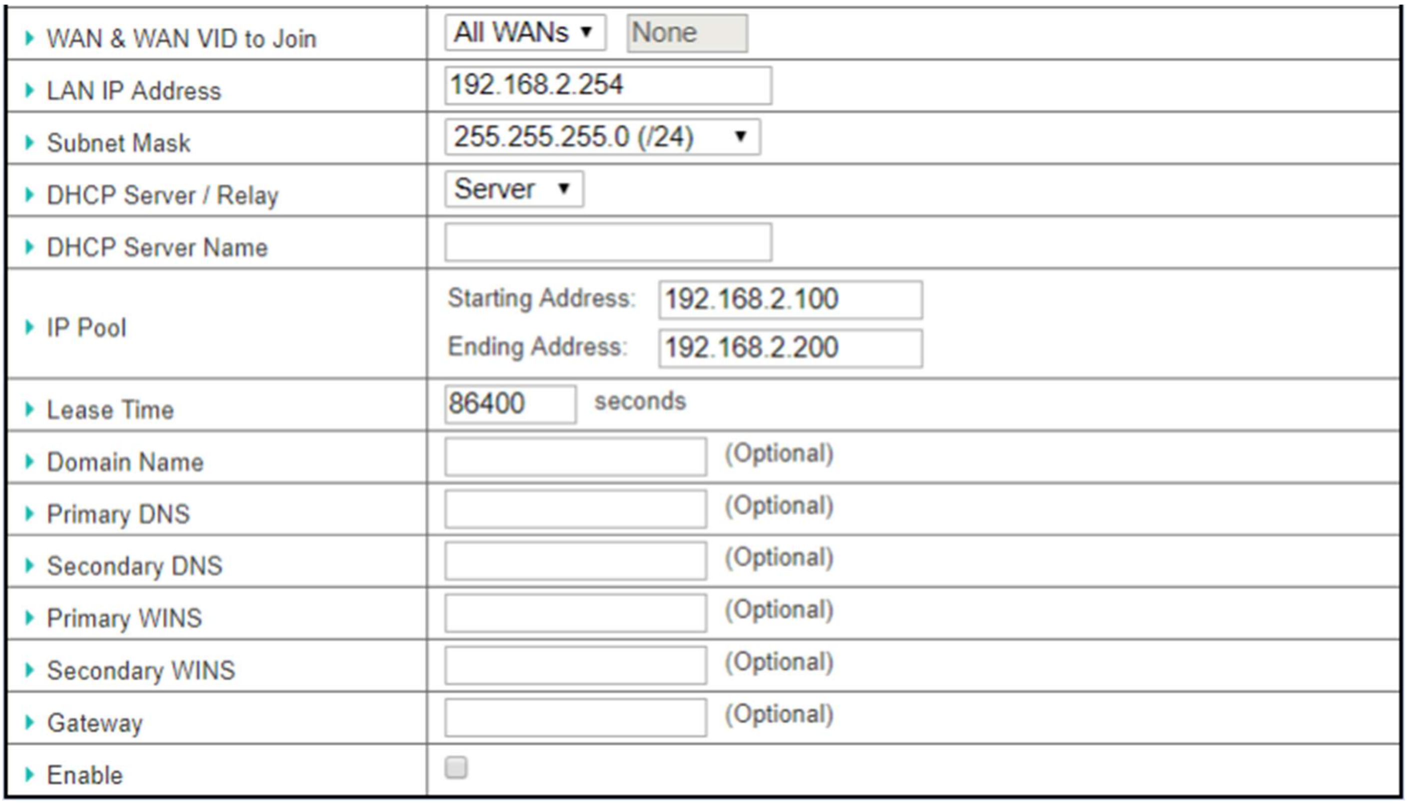


Port-based VLAN Configuration

Item	Setting
Name	VLAN - 1
VLAN ID	
VLAN Tagging	Disable ▾
NAT / Bridge	NAT ▾
Port Members	Port: □ PORT-1 □ PORT-2 □ PORT-3 □ PORT-4 2.4G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8
LAN to Join	□ Enable DHCP 1 ▾

Port-based VLAN Configuration		
Item	**Value setting**	**Description**
Name	1. Required setting 2. String format: already has default text	Define the **Name** of this rule. It has default text and cannot be modified.
VLAN ID	Required setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when **Disable** is selected.
NAT / Bridge	**NAT** is selected by default.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	Unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list will depend on product model.
LAN to Join	Unchecked by default.	Check the Enable box and select one of the defined DHCP Server for the List to define the DHCP server for the VLAN group. If you enabled this function, all the rest settings will be greyed out, not required to configured manually.

If you don’t bind the VLAN group to a pre-defined DHCP server, you have to further specify the following settings.

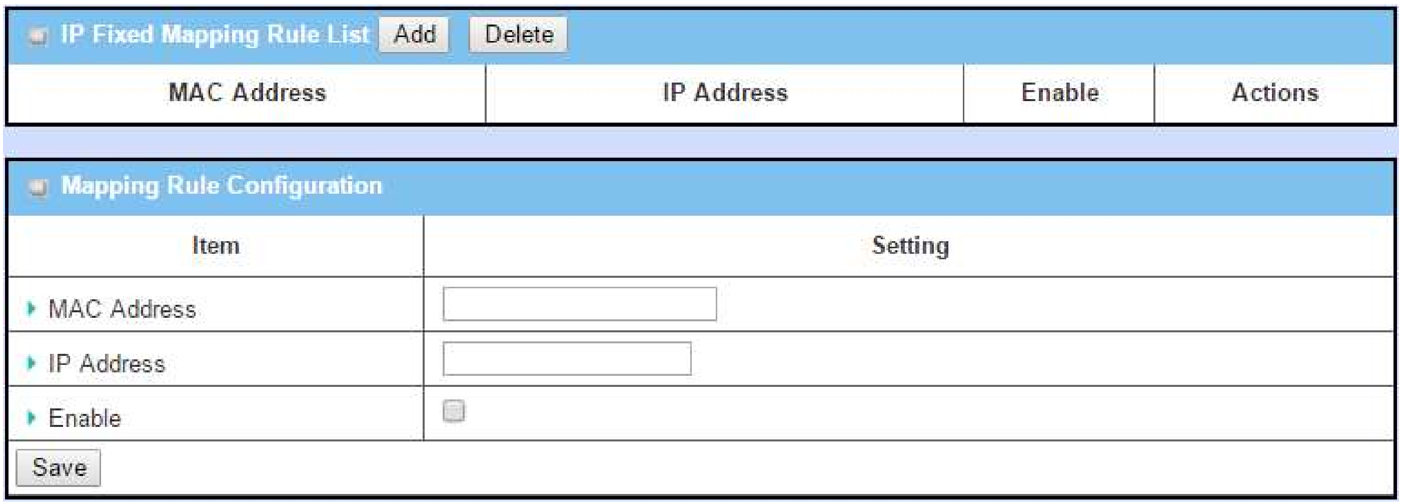


WAN & WAN VID to Join	All WANs ▾ None
LAN IP Address	192.168.2.254
Subnet Mask	255.255.255.0 (/24) ▾
DHCP Server / Relay	Server ▾
DHCP Server Name	
IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Enable	□

WAN & WAN VID to Join	**All WANs** is selected by default.	Select which **WAN** or **All WANs** that allow accessing Internet. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	Required setting	Assign an **IP Address** for the DHCP Server that the rule used, this IP address is a gateway IP.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Server /Relay	**Server** is selected by default.	Define the **DHCP Server** type. There are three types: **Server**, **Relay**, and **Disable**. **Relay**: Select **Relay** to enable DHCP Relay function for the VLAN group. You only need to fill the **DHCP Server IP Address** field. **Server**: Select **Server** to enable DHCP Server function for the VLAN group. You need to specify the DHCP Server settings. **Disable**: Select **Disable** to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP **Relay** only)	Required setting	If you select **Relay** type of DHCP Server, assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server.
DHCP Server Name	Required setting	Define name of the DHCP Server.
IP Pool	Required setting	Define the IP Pool range. There are **Starting Address** and **Ending Address** fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of **IP pool**.
Lease Time	Required setting	Define a period of time for an IP Address that the DHCP Server leases to a new device. By default, the **lease time** is 86400 seconds.

Domain Name	String format, any text	The Domain Name of this DHCP Server. ***Value Range***: 0 ~ 31 characters.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Enable	Unchecked by default	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore previous settings.

Additionally, you can add some IP rules to the **IP Fixed Mapping Rule List** if DHCP Server for the VLAN groups is required.



IP Fixed Mapping Rule List [Add] [Delete]

MAC Address	IP Address	Enable	Actions

Mapping Rule Configuration

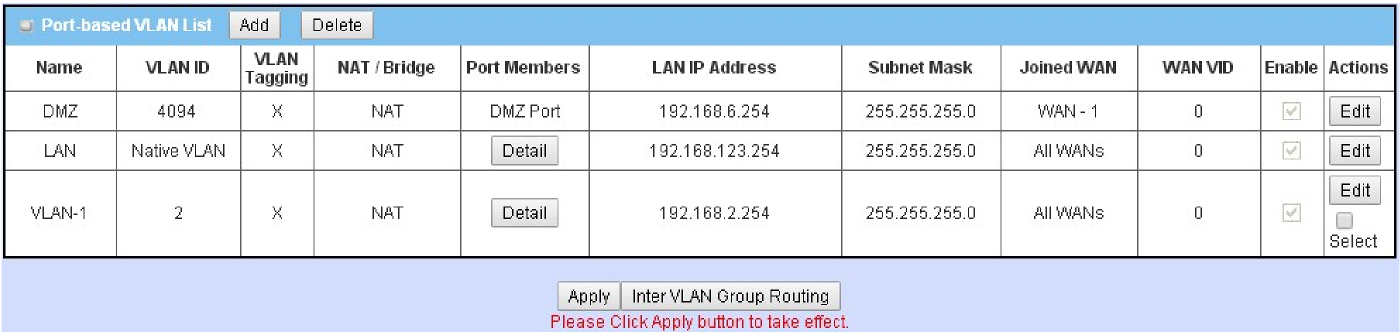
Item	Setting
MAC Address	
IP Address	
Enable	□

[Save]

When **Add** button is applied, the **Mapping Rule Configuration** screen will appear.

Mapping Rule Configuration Item	 Value setting	 Description
MAC Address	Required setting	Define the **MAC Address** target that the DHCP Server wants to match.
IP Address	Required setting	Define the **IP Address** that the DHCP Server will assign. If there is a request from the MAC Address filled in the above field, the DHCP Server will assign this **IP Address** to the client whose **MAC Address** matched the rule.
Enable	Unchecked by default	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration

Note: Always click on the **Apply** button to apply the changes after the web browser refresh has taken you back to the VLAN page.



Port-based VLAN List [Add] [Delete]

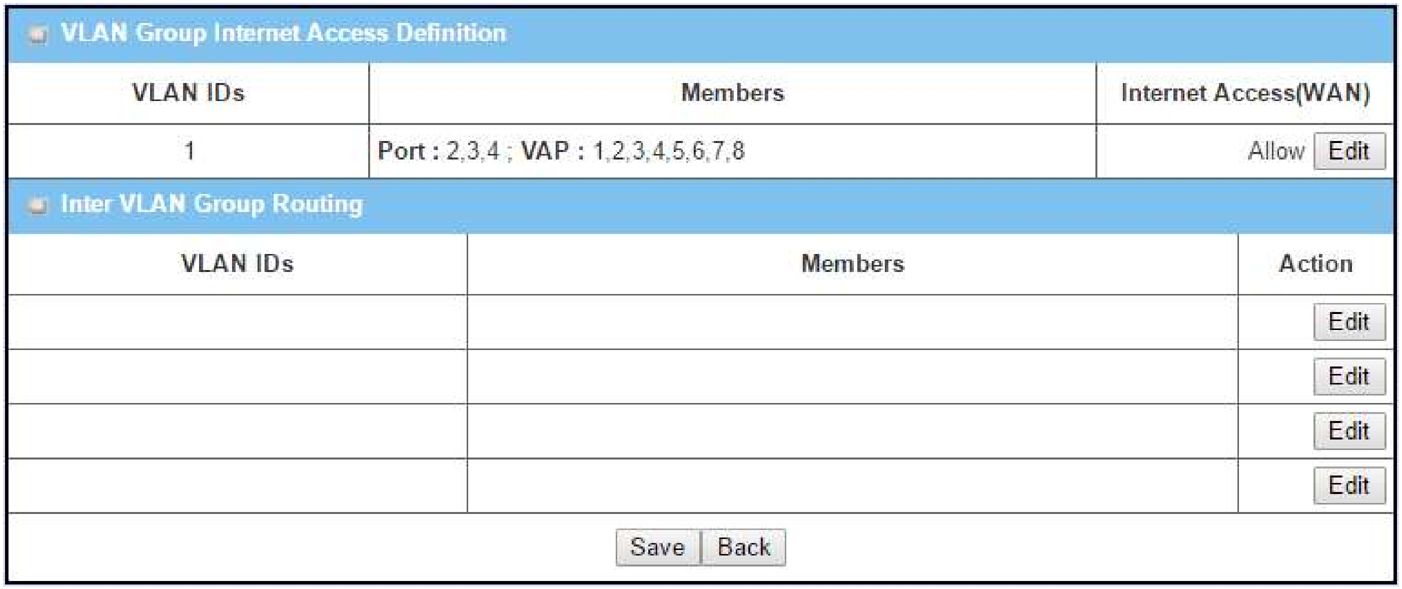
Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit
VLAN-1	2	X	NAT	Detail	192.168.2.254	255.255.255.0	All WANs	0	☑	Edit □ Select

[Apply] [Inter VLAN Group Routing]

Please Click Apply button to take effect.

Port-based VLAN – Inter VLAN Group Routing

Click the **VLAN Group Routing** button, and the **VLAN Group Internet Access Definition** and **Inter VLAN Group Routing** screen will appear.



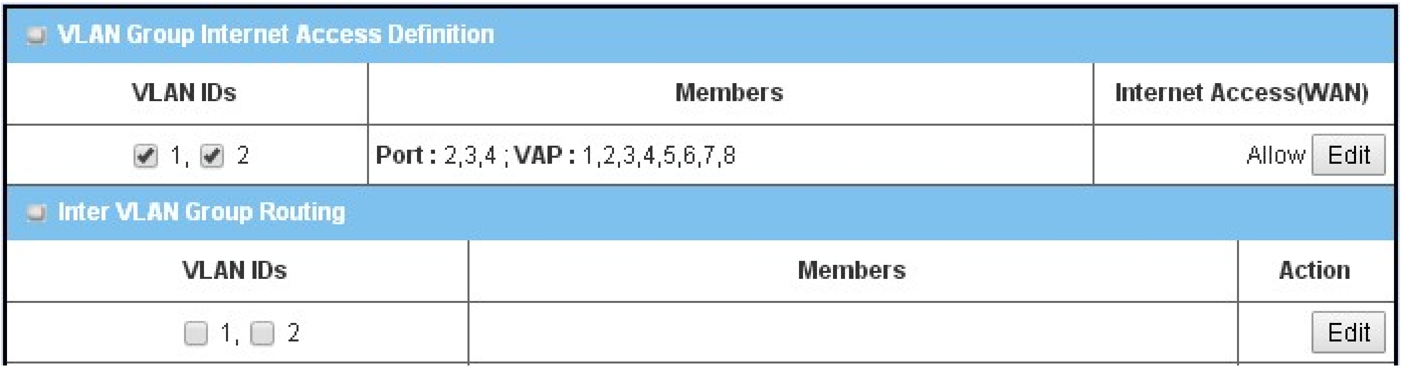
VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
1	Port : 2,3,4 ; VAP : 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

When the **Edit** button is applied, a screen similar to this will appear.



VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2	Port : 2,3,4 ; VAP : 1,2,3,4,5,6,7,8	Allow Edit

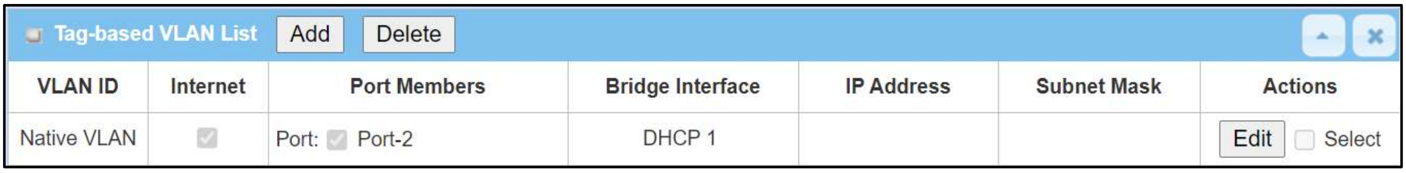
Inter VLAN Group Routing

VLAN IDs	Members	Action
□ 1, □ 2		Edit

Inter VLAN Group Routing		
Item	**Value setting**	**Description**
VLAN Group Internet Access Definition	All boxes are checked by default.	By default, all boxes are checked, meaning all **VLAN ID** members are allowed to access WAN interface. If a **VLAN ID** box is unchecked, it means the VLAN ID member can't access the Internet. Note: **VLAN ID 1** is always available; it is the default VLAN ID of the **LAN**. Other **VLAN IDs** are available only when they are enabled.
Inter VLAN Group Routing	Unchecked by default	Click the VLAN IDs box to enable the Inter VLAN access function. By default, members in different VLAN IDs can't access each other. The gateway supports up to 4 rules for **Inter VLAN Group Routing.** For example, if ID_1 and ID_2 are checked, it means members in VLAN ID_1 can access members of VLAN ID_2, and vice versa.
Save	N/A	Click the **Save** button to save the configuration

Tag-based VLAN – Create/Edit VLAN Rules

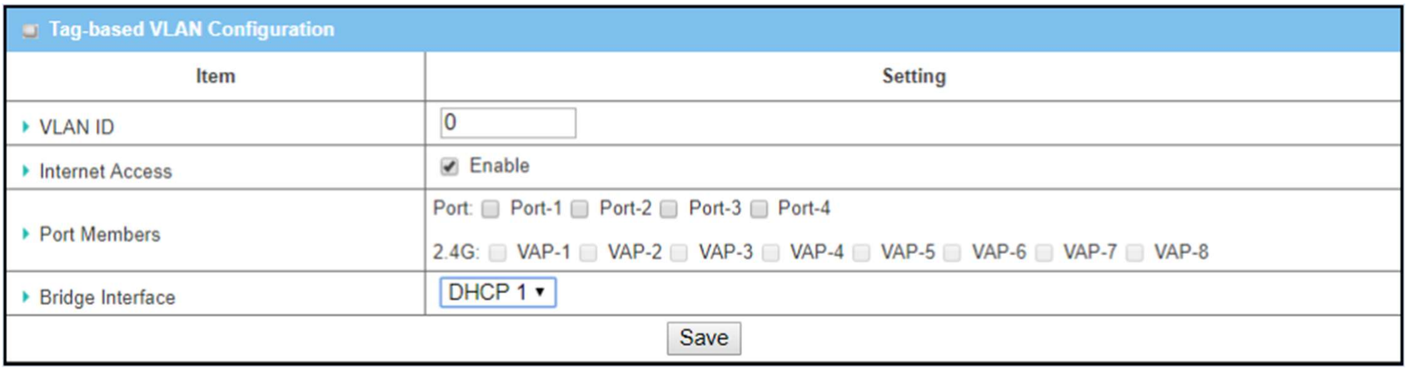
The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule that shows the configuration of all LAN ports and all VAPs. If your device has a DMZ port, you will see DMZ configuration too. The router supports up to a maximum of 128 tag-based VLAN rule sets.



Tag-based VLAN List Add Delete

VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	☑	Port: ☑ Port-2	DHCP 1			Edit □ Select

When the **Add** button is applied, the **Tag-based VLAN Configuration** screen will appear.



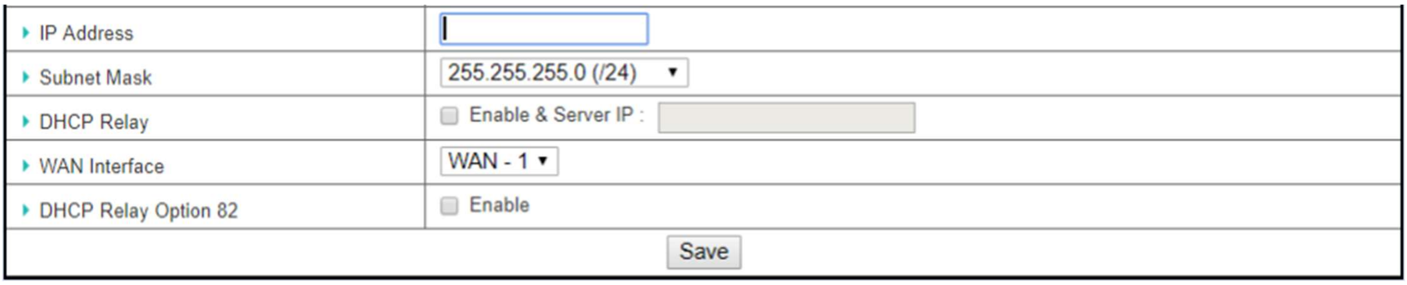
Tag-based VLAN Configuration

Item	Setting
VLAN ID	0
Internet Access	☑ Enable
Port Members	Port: □ Port-1 □ Port-2 □ Port-3 □ Port-4 2.4G: □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8
Bridge Interface	DHCP 1 ▾

Save

Tag-based VLAN Configuration		
Item	**Value setting**	**Description**
VLAN ID	Required setting	Define the **VLAN ID** number, range is 6~4094.
Internet Access	The box is checked by default.	Click **Enable** box to allow the members in the VLAN group access to internet.
Port Members	Unchecked by default	Check the LAN port box(es) to join the VLAN group. Check the VAP box(es) to join the VLAN group. Note: Only the wireless gateway has the VAP list.
Bridge Interface	**DHCP 1** is selected by default.	Select a predefined **DHCP Server**, **New** to define a new DHCP server for these members of this VLAN group.
Save	N/A	Click **Save** button to save the configuration Note: After clicking the **Save** button, always click the **Apply** button to apply the settings.

If you select New to create a new DHCP server setting for the VLAN group, you have to further specify the following configuration.

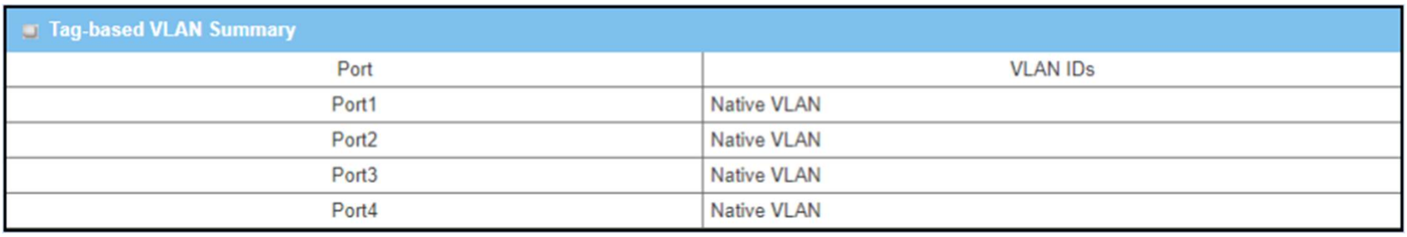


IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
DHCP Relay	□ Enable & Server IP :
WAN Interface	WAN - 1 ▾
DHCP Relay Option 82	□ Enable

Tag-based VLAN Configuration (part II)		
Item	**Value setting**	**Description**
IP Address	Required setting	Assign an IP Address for the DHCP Server that the rule used, this IP address is a gateway IP.
Subnet Mask	255.255.255.0(/24) is selected by default.	Select a Subnet Mask for the DHCP Server.
DHCP Relay	Unchecked by default	Check the box to enable the DHCP Relay function for the VLAN group, and you only need to fill the DHCP Server IP Address field.
WAN Interface	WAN-1 is selected by default	Select which WAN interface allows accessing the Internet.
DHCP Option 82	Optional setting	If you select Relay type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
Save	NA	Click the Save button to save the configuration
Undo	NA	Click the Undo button to restore what you just configured back to the previous setting.

Tag-based VLAN Summary

The configured tag-based VLAN group information will be displayed in the following screen.



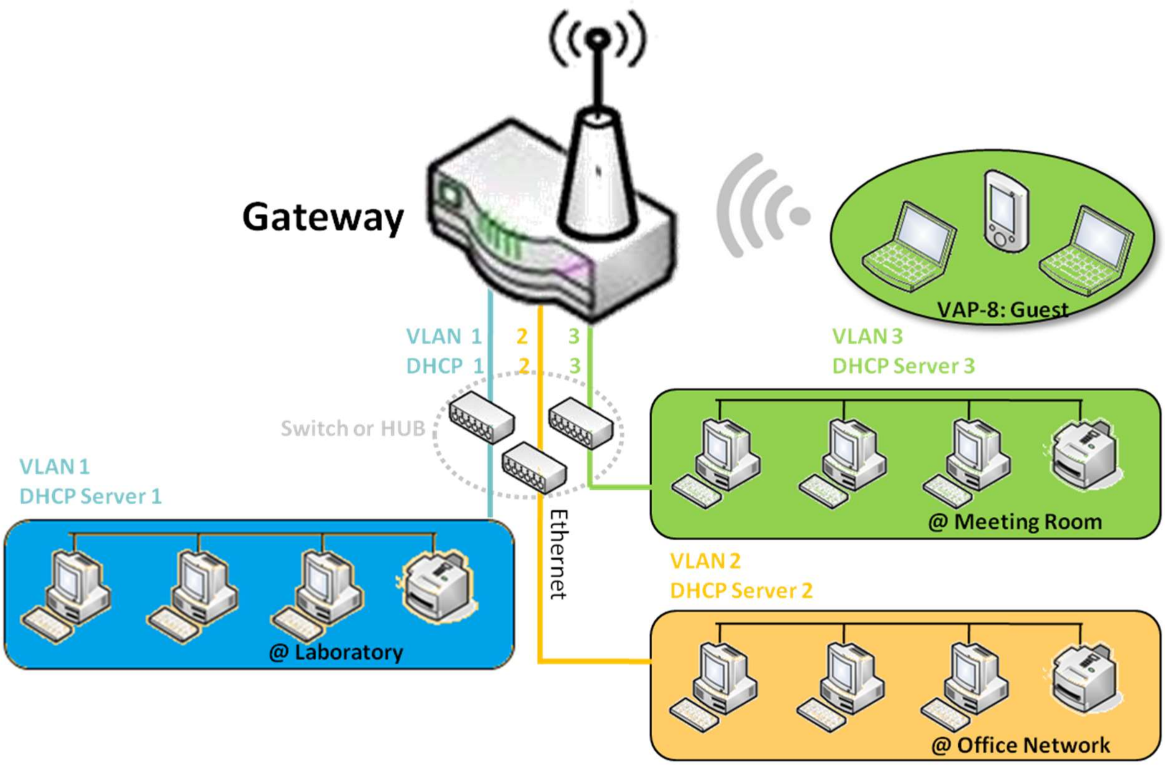
Tag-based VLAN Summary

Port	VLAN IDs
Port1	Native VLAN
Port2	Native VLAN
Port3	Native VLAN
Port4	Native VLAN

3.2.3 DHCP Server

➢ DHCP Server

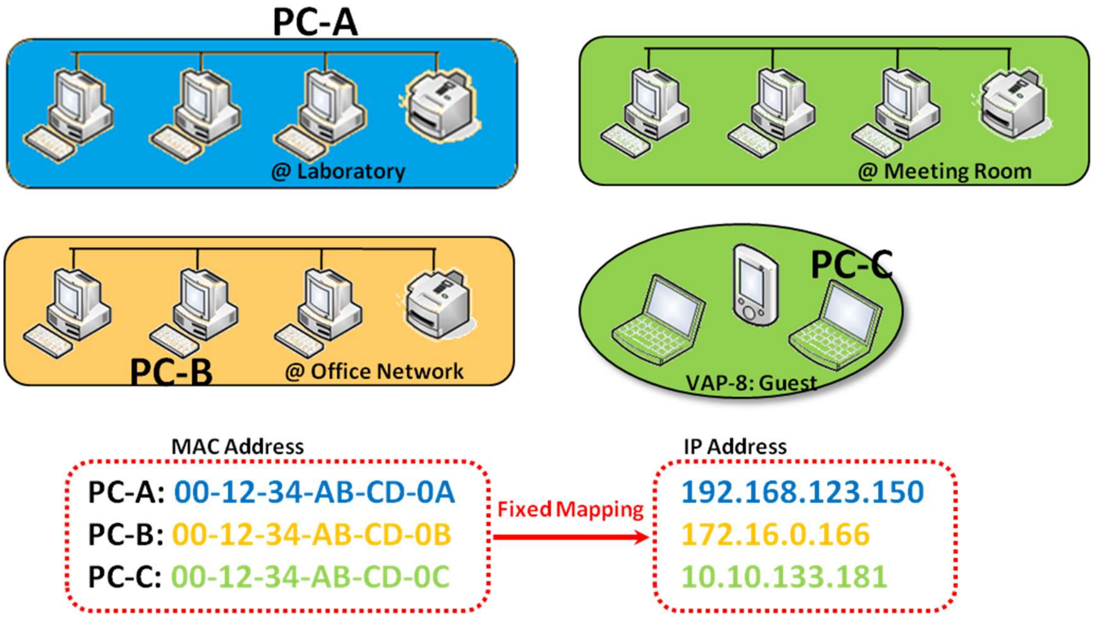
The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (refer to VLAN section for details). There is one default setting for whose LAN IP Address is the same as the gateway LAN interface, with its default Subnet Mask setting as “255.255.255.0”, and its default IP Pool range is from “.100” to “.200” as shown at the DHCP Server List page on gateway’s Web UI.



More DHCP server configurations can be added by clicking on the “Add” button behind “DHCP Server List”, or clicking on the “Edit” button at the end of each DHCP Server on list to edit the current settings. Additionally, you can select a DHCP Server and delete it by clicking on the “Select” check-box and the “Delete” button.

➢ Fixed Mapping

User can assign fixed IP address to a specific client MAC address, when targets already exist in the ***DHCP Client List***, or add other Mapping Rules manually in advance.



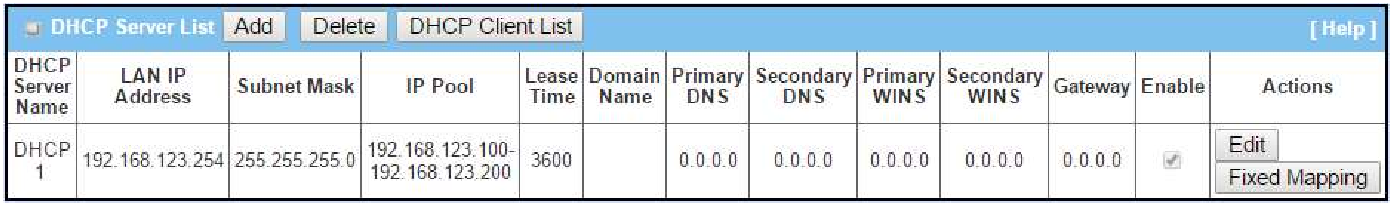
DHCP Server Setting

Go to Basic Network > LAN & VLAN > DHCP Server Tab.

The DHCP Server setting allows user to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

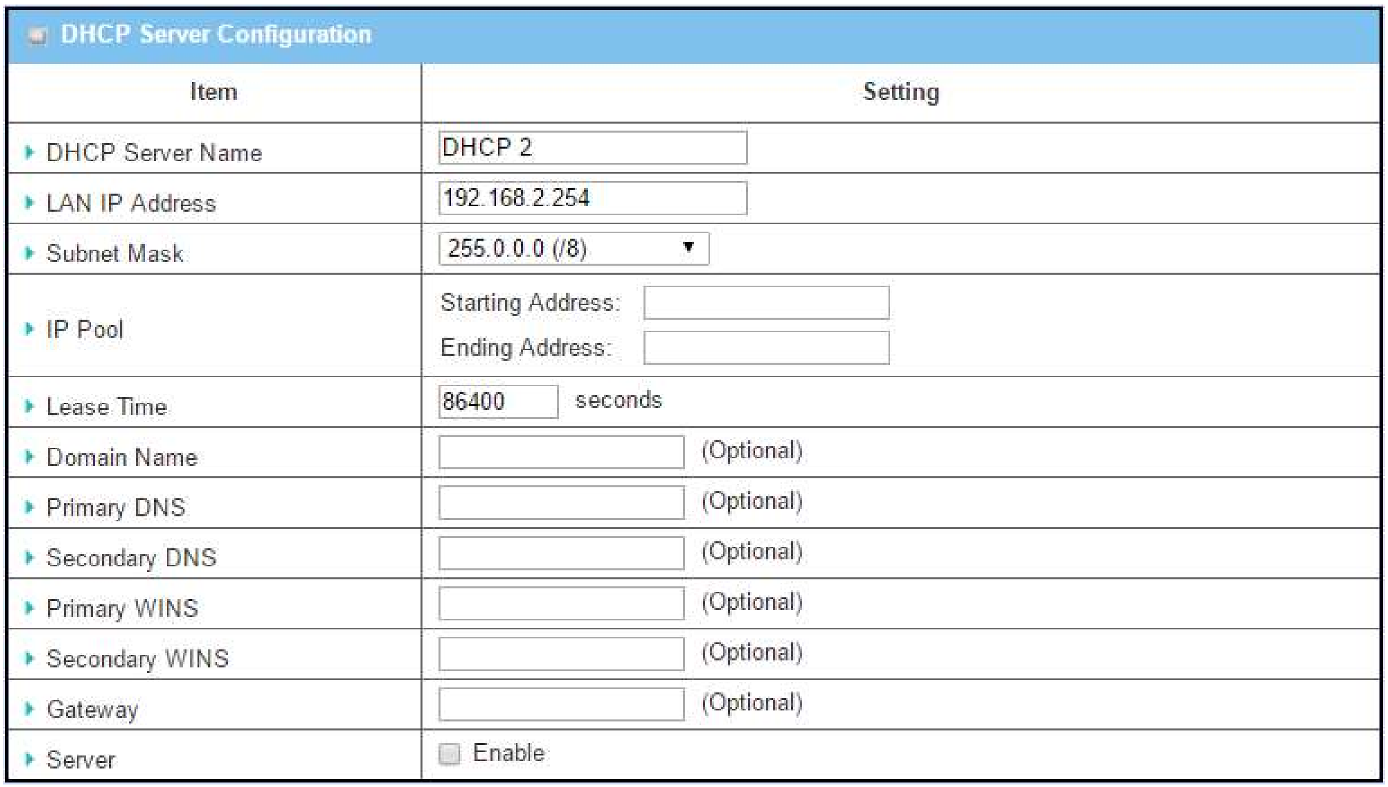
Create / Edit DHCP Server Policy

The gateway allows you to customize your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group). A maximum of 4 policy sets are supported.



DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100- 192.168.123.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit Fixed Mapping

When **Add** button is applied, the **DHCP Server Configuration** screen will appear.

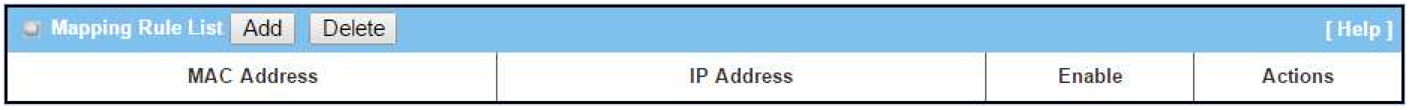


Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.254
Subnet Mask	255.0.0.0 (/8) ▼
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	□ Enable

DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format, any text 2. Required setting	Enter a DHCP Server name.
LAN IP Address	1. IPv4 format. 2. Required setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. Required setting	The IP Pool of this DHCP Server. It is composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	1. Numeric string format. 2. Required setting	The Lease Time of this DHCP Server. ***Value Range***: 300 ~ 604800 seconds.
Domain Name	String format, any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	Unchecked by default	Click **Enable** box to activate this DHCP Server.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

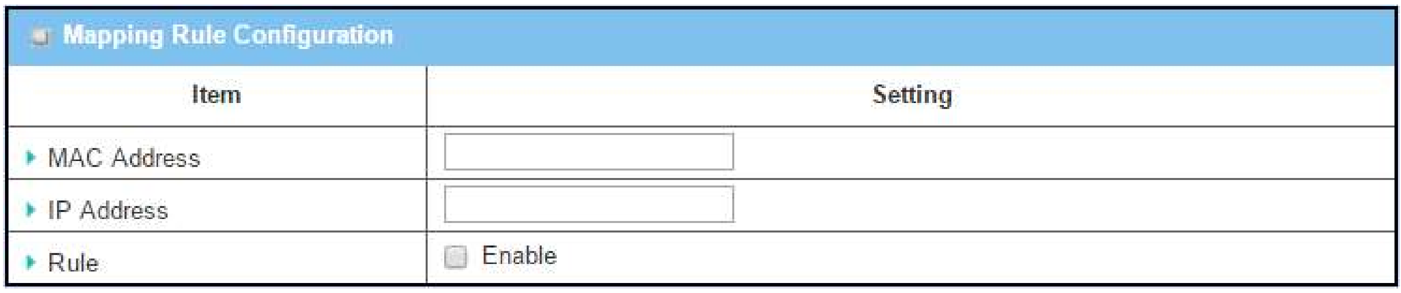
Create / Edit Mapping Rule List on DHCP Server

The gateway allows you to customize your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.



MAC Address	IP Address	Enable	Actions

When **Add** button is applied, the **Mapping Rule Configuration** screen will appear.



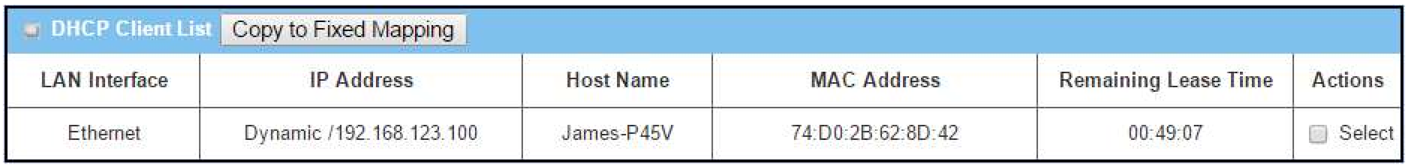
Mapping Rule Configuration

Item	Setting
MAC Address	
IP Address	
Rule	□ Enable

Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	1. MAC Address string format 2. Required setting	The MAC Address of this mapping rule.
IP Address	1. IPv4 format. 2. Required setting	The IP Address of this mapping rule.
Rule	Unchecked by default	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore previous settings.
Back	N/A	When the **Back** button is clicked the screen will return to the **DHCP Server Configuration** page.

View / Copy DHCP Client List

When **DHCP Client List** button is applied, **DHCP Client List** screen will appear.



DHCP Client List

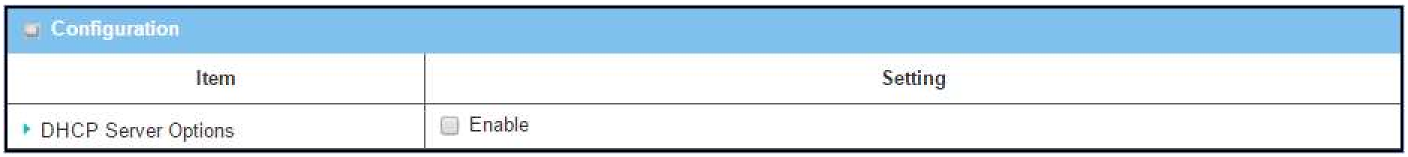
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.100	James-P45V	74:D0:2B:62:8D:42	00:49:07	□ Select

When the DHCP Client is selected and **Copy to Fixed Mapping** button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

Enable / Disable DHCP Server Options

The **DHCP Server Options** setting allows user to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function, and the DHCP Server will add the expected options in its sending out DHCPOFFER DHCPACK packages.

Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]

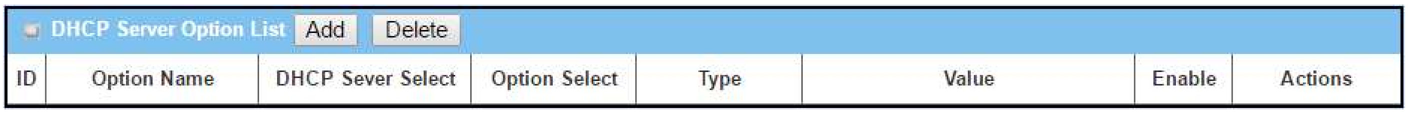


Configuration

Item	Setting
DHCP Server Options	□ Enable

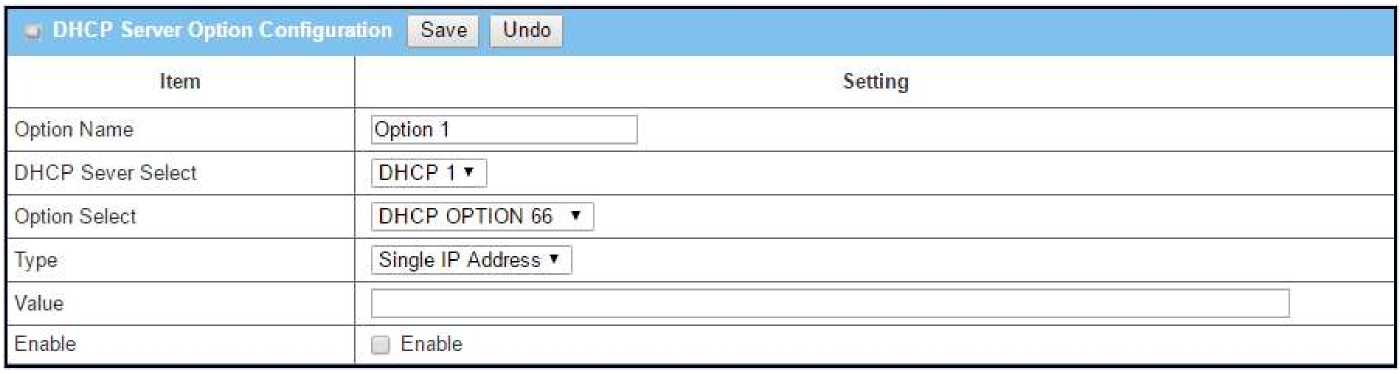
Create / Edit DHCP Server Options

The gateway supports up to a maximum of 99 option settings.



ID	Option Name	DHCP Sever Select	Option Select	Type	Value	Enable	Actions

When **Add/Edit** button is applied, the **DHCP Server Option Configuration** screen will appear.



Item	Setting
Option Name	Option 1
DHCP Sever Select	DHCP 1 ▾
Option Select	DHCP OPTION 66 ▾
Type	Single IP Address ▾
Value	
Enable	□ Enable

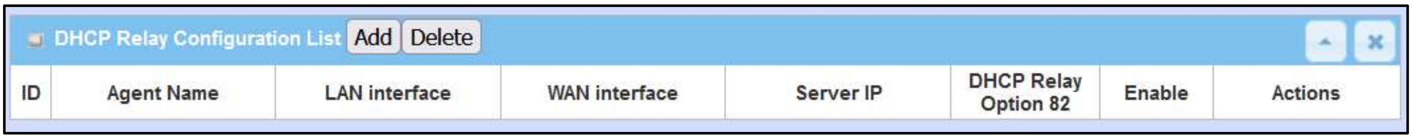
DHCP Server Option Configuration		
Item	**Value setting**	**Description**
Option Name	1. String format, any text 2. Required setting.	Enter a DHCP Server Option name.
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.

Option Select	1. Required setting.
	2. **Option 66** is selected by default.
		Choose the specific option from the dropdown list. It can be **Option 66, Option 72, Option 114, Option 42, Option 150, or Option 160.**
		Option 42 for NTP server;
		Option 66 for TFTP;
		Option 72 for www;
		Option 114 for URL.

<table>
<tr><td rowspan="8" colspan="2"><b>Type</b>
Dropdown list of DHCP server option value type</td><td colspan="3">Each option has different value types.</td></tr>
<tr><td rowspan="2">66</td><td colspan="2">Single IP address</td></tr>
<tr><td colspan="2">Single FQDN</td></tr>
<tr><td>72</td><td colspan="2">IP address list, separated by “,”</td></tr>
<tr><td>114</td><td colspan="2">Single URL</td></tr>
<tr><td>42</td><td colspan="2">IP address list, separated by “,”</td></tr>
<tr><td>150</td><td colspan="2">IP address list, separated by “,”</td></tr>
<tr><td>160</td><td colspan="2">Single IP address, Single FQDN</td></tr>
<tr><td rowspan="6"><b>Value</b></td><td rowspan="6">1. IPv4 format
2. FQDN format
3. IP list
4. URL format
5. Required setting</td><td colspan="3">Should conform to Type:</td></tr>
<tr><td></td><td>Type</td><td>Value</td></tr>
<tr><td rowspan="2">66</td><td>Single IP address</td><td>IPv4 format</td></tr>
<tr><td>Single FQDN</td><td>QDN format</td></tr>
<tr><td>72</td><td>IP address list, separated by “,”</td><td>IPv4 format, separated by “,”</td></tr>
<tr><td>114</td><td>Single URL</td><td>URL format</td></tr>
<tr><td><b>Enable</b></td><td>Unchecked by default</td><td colspan="3">Click <b>Enable</b> box to activate this setting.</td></tr>
<tr><td><b>Save</b></td><td><i>NA</i></td><td colspan="3">Click the <b>Save</b> button to save the setting.</td></tr>
<tr><td><b>Undo</b></td><td><i>NA</i></td><td colspan="3">When the <b>Undo</b> button is clicked the screen will return back with nothing changed.</td></tr>
</table>

Create / Edit DHCP Relay

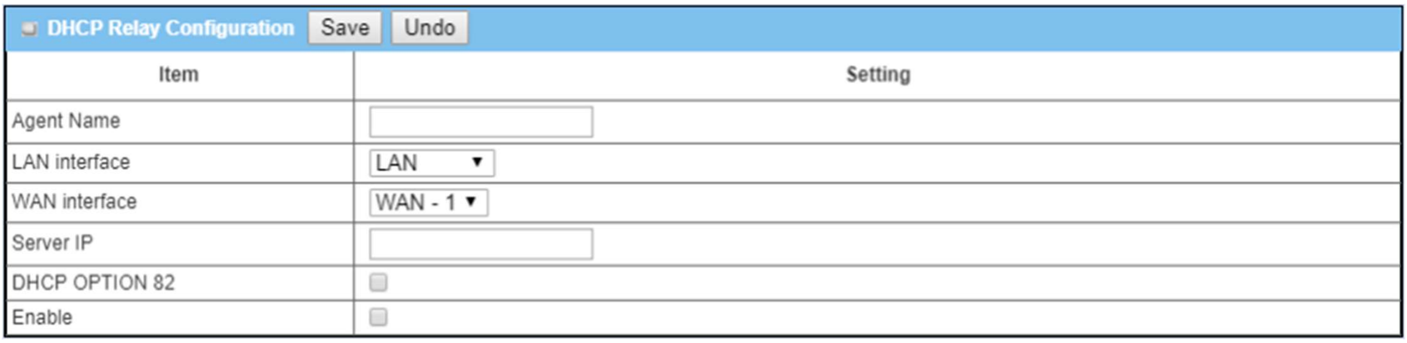
The gateway supports up to a maximum of 6 DHCP Relay configurations.



DHCP Relay Configuration List Add Delete

ID	Agent Name	LAN interface	WAN interface	Server IP	DHCP Relay Option 82	Enable	Actions

When **Add/Edit** button is applied, the **DHCP Relay Configuration** screen will appear.



DHCP Relay Configuration Save Undo

Item	Setting
Agent Name	
LAN interface	LAN ▼
WAN interface	WAN - 1 ▼
Server IP	
DHCP OPTION 82	□
Enable	□

DHCP Relay Configuration		
Item	**Value setting**	**Description**
Agent Name	1. String format, any text.	Enter a DHCP Relay name. Enter a name that is easy for you to understand.

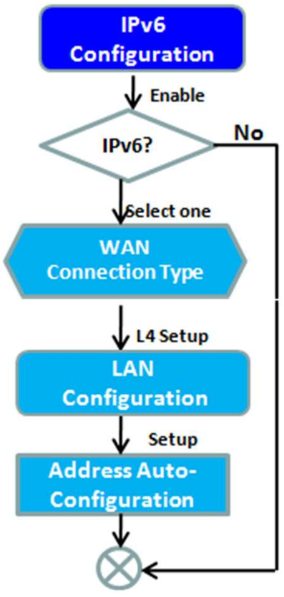
	2. Required setting.	**Value Range:** 1~64 characters.
LAN Interface	1. Required setting. 2. **LAN** is selected by default.	Choose a LAN Interface for the dropdown list to apply with the DHCP Relay function.
WAN Interface	1. Required setting. 2. **WAN-1** is selected by default.	Choose a WAN Interface for the dropdown list to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
Server IP	1. Required setting. 2. **null** by default	Assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
DHCP OPTION 82	Unchecked by default.	Click **Enable** box to activate DHCP OPTION 82 function. Option 82 is organized as a single DHCP option that contains circuit-ID information known by the relay agent. If the relayed DHCP server requires such information, you have to enable it, otherwise, just leave it as unchecked.
Enable	Unchecked by default.	Click **Enable** box to activate this setting.
Save	*NA*	Click the **Save** button to save the setting.
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.

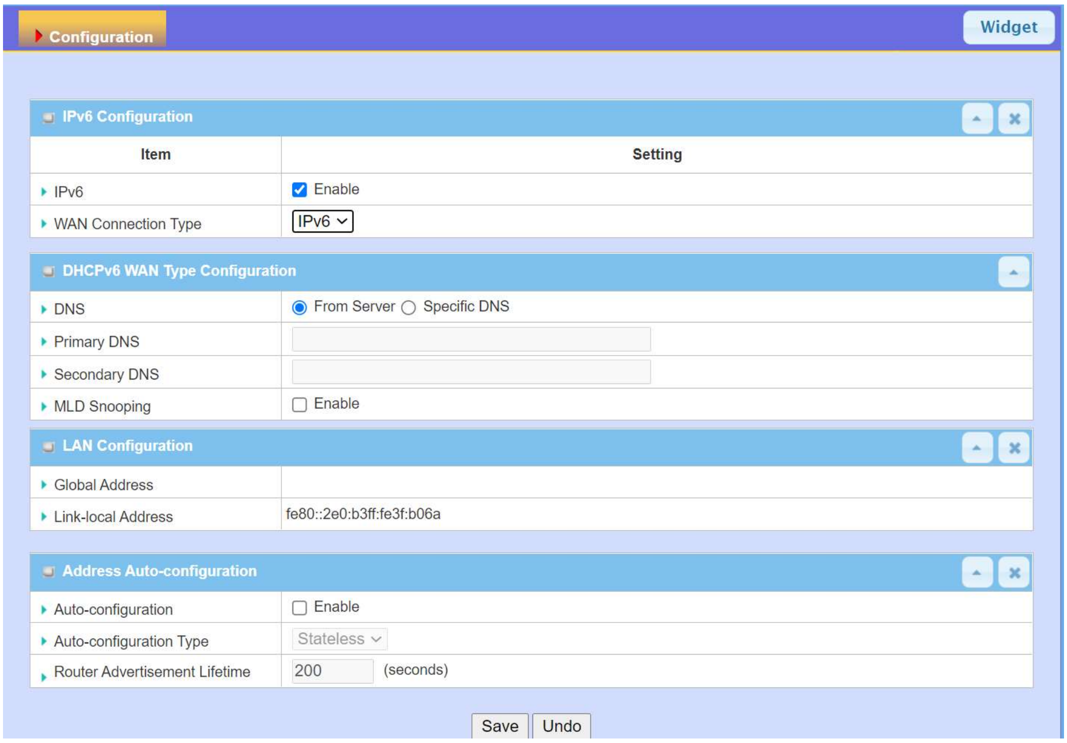
3.3 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers.

3.3.1 IPv6 Configuration





IPv6 Configuration

Item	Setting
IPv6	☑ Enable
WAN Connection Type	IPv6

DHCPv6 WAN Type Configuration

DNS	● From Server ○ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

LAN Configuration

Global Address	
Link-local Address	fe80::2e0:b3ff:fe3f:b06a

Address Auto-configuration

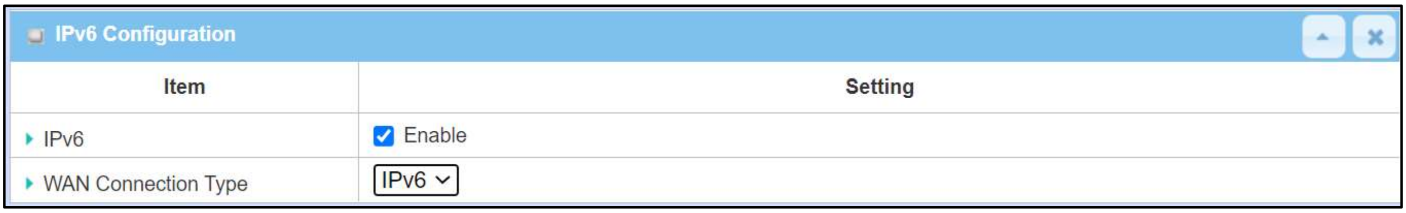
Auto-configuration	□ Enable
Auto-configuration Type	Stateless
Router Advertisement Lifetime	200 (seconds)

Only **IPv6** is supported. Please contact your ISP to understand IPv6 support and settings before you proceed with IPv6 setup.

IPv6 Configuration Setting

Go to Basic Network > IPv6 > Configuration Tab.

The **IPv6 Configuration** setting allows user to set the IPv6 connection type to access the IPv6 network.

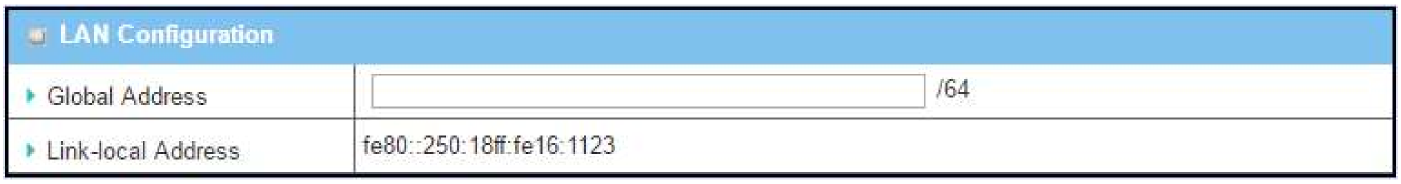


IPv6 Configuration

Item	Setting
IPv6	☑ Enable
WAN Connection Type	IPv6

IPv6 Configuration		
Item	**Value setting**	**Description**
IPv6	Unchecked by default	Check the **Enable** box to activate the IPv6 function.
WAN Connection Type	1. Can only be selected when IPv6 Enabled 2. Required setting	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. For products with only 3G/4G WAN interface, only **IPv6** is supported.

LAN Configuration



LAN Configuration

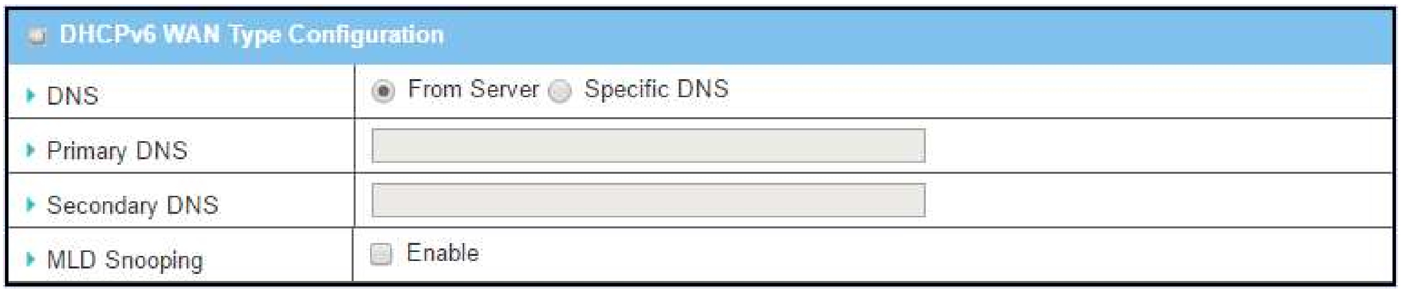
Global Address	/64
Link-local Address	fe80::250:18ff:fe16:1123

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Required setting	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)** to set up the LAN environment.

When the above settings are configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

DHCPv6 WAN Type Configuration

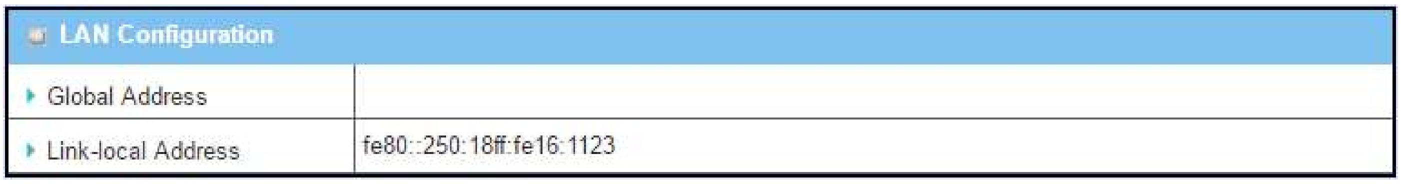


DHCPv6 WAN Type Configuration

DNS	● From Server ○ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

DHCPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
DNS	The option [From Server] is selected by default	Select the [Specific DNS] option to activate Primary DNS and Secondary DNS. Then fill in the DNS information.
Primary DNS	Cannot be modified by default	Enter the WAN **primary DNS Server**.
Secondary DNS	Cannot be modified by default	Enter the WAN **secondary DNS Server**.
MLD	Unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration



LAN Configuration

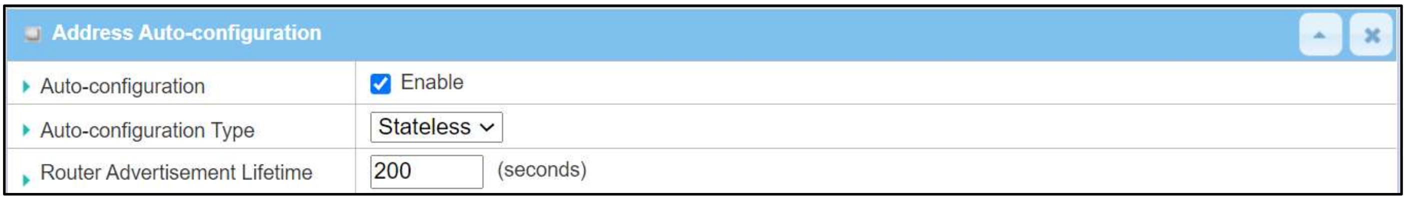
Global Address	
Link-local Address	fe80::250:18ff:fe16:1123

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	The LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Shows the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)** to set up the LAN environment.

When above settings are configured, click the **Save** button to save the configuration, and click **Reboot** button to reboot the router.

Address Auto-configuration



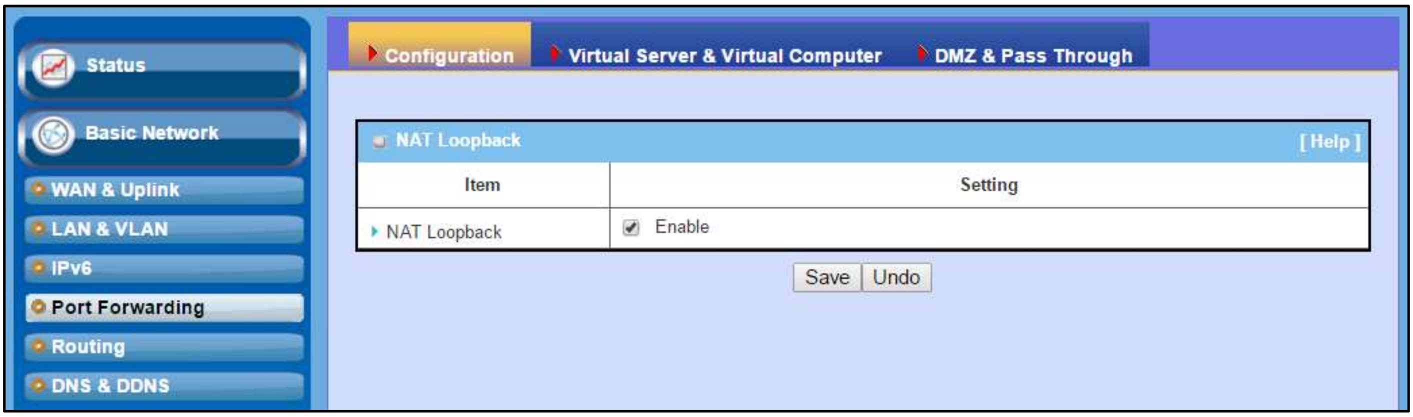
Address Auto-configuration

Auto-configuration	☑ Enable
Auto-configuration Type	Stateless
Router Advertisement Lifetime	200 (seconds)

Address Auto-configuration Item	Value setting	Description
Auto-configuration	Unchecked by default	Check to enable the Auto configuration feature.
Auto-configuration Type	1. Can be selected when **Auto-configuration** is enabled 2. Stateless is selected by default	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Stateless** to manage the Local Area Network to be SLAAC + RDNSS
Router Advertisement Lifetime	Required setting	Enter the Router Advertisement Lifetime (in seconds). 200 is set by default. *__Value Range__*: 0 ~ 65535

3.4 Port Forwarding

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion. This product embeds and activates the NAT function. You also can disable the NAT function in **[Basic Network]-[WAN & Uplink]-[Internet Setup]-[WAN Type Configuration]** page.



NAT Loopback [Help]

Item	Setting
NAT Loopback	☑ Enable

Usually all local hosts or servers behind corporate gateway are protected by NAT firewall. NAT firewall will filter out unrecognized packets to protect your Intranet. So, all local hosts are invisible to the outside world. Port forwarding or port mapping is function that redirects a communication request from one address and port number combination to assigned one. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number.

3.4.1 Configuration

NAT Loopback

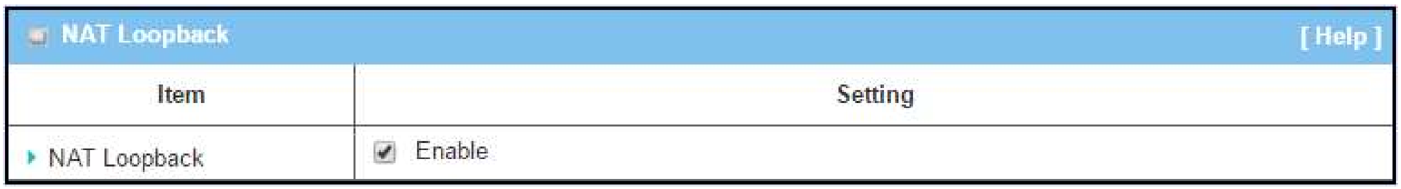
This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when NAT loopback feature is enabled. When accessing the email server from the LAN side or at the WAN side, you don't need to change the IP address of the mail server.

Configuration Setting

Go to Basic Network > Port Forwarding > Configuration tab.

The NAT Loopback allows user to access the WAN IP address from inside your local network.

Enable NAT Loopback

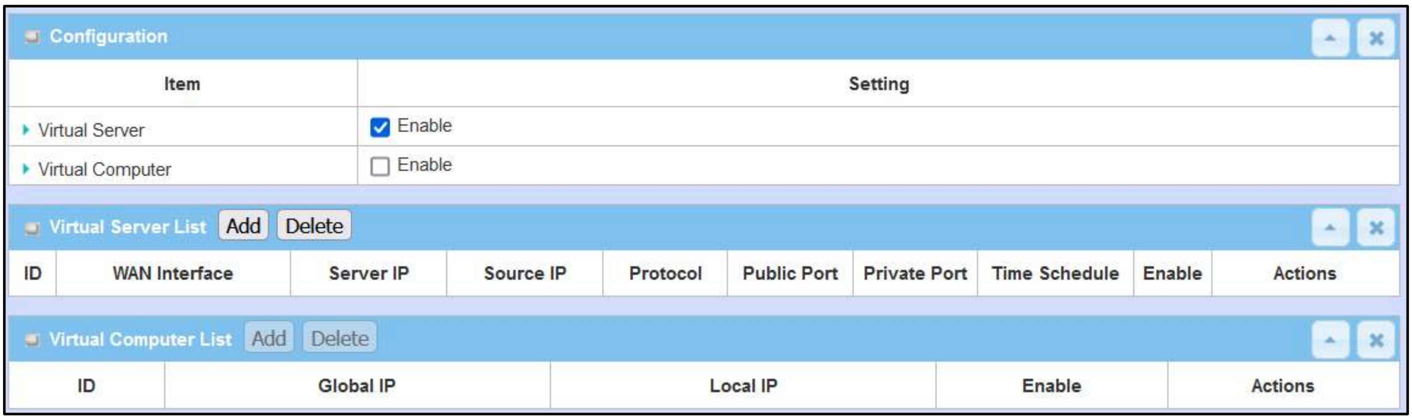


NAT Loopback [Help]

Item	Setting
NAT Loopback	☑ Enable

Configuration Item	Value setting	Description
NAT Loopback	Checked by default	Check the **Enable** box to activate the NAT function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel settings

3.4.2 Virtual Server & Virtual Computer



Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	□ Enable

Virtual Server List

ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Virtual Computer List

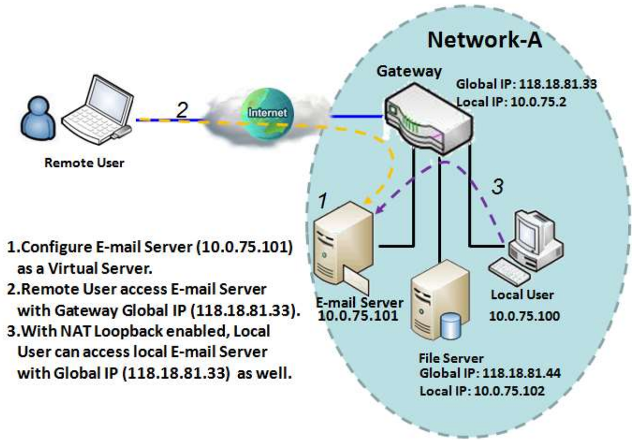
ID	Global IP	Local IP	Enable	Actions

There are some important Port Forwarding functions implemented within the gateway, including "Virtual Server", "NAT loopback" and "Virtual Computer".

These allow personnel to access servers behind the gateway from outside the network. Those servers can be set up by using "Virtual Server" feature. NAT Loopback can allow access to servers from the LAN side with a global IP address and no change in settings.

"Virtual computer" is a host behind a NAT gateway whose IP address is a global one and is visible to the outside world. Since it is behind NAT, it is protected by gateway firewall. To configure Virtual Computer, just map the local IP of the virtual computer to a global IP.

Virtual Server & NAT Loopback

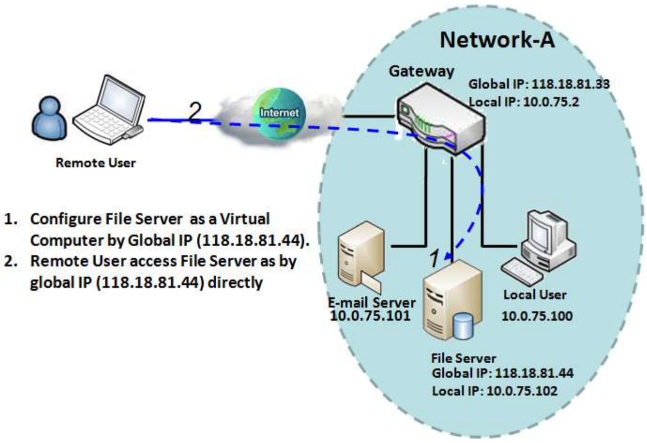


1.Configure E-mail Server (10.0.75.101) as a Virtual Server.
2.Remote User access E-mail Server with Gateway Global IP (118.18.81.33).
3.With NAT Loopback enabled, Local User can access local E-mail Server with Global IP (118.18.81.33) as well.

"Virtual Server" allows you to access servers with the global IP address or FQDN of the gateway as if they are servers existing on the Internet. But in fact, these servers are located in the Intranet and are physically behind the gateway. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side. As shown in the example, an E-mail virtual server is defined to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110. So, the remote user can access the E-mail server with the gateway's global IP 118.18.81.33 from its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

NAT Loopback allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set up a mail server on the LAN side, your local devices can access this mail server through the gateway's global IP address when NAT loopback is enabled. Then there is no need to change the IP address of the mail server.

Virtual Computer



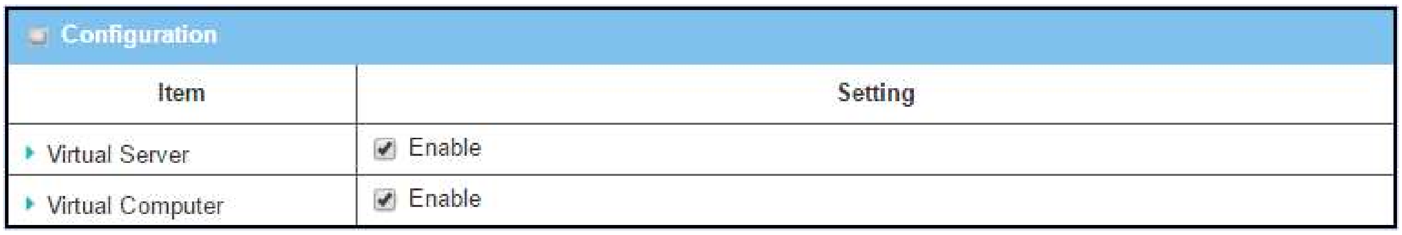
1. Configure File Server as a Virtual Computer by Global IP (118.18.81.44).
2. Remote User access File Server as by global IP (118.18.81.44) directly

"Virtual Computer" allows you to assign LAN hosts to global IP addresses, so that they can be visible to outside world. While so, they are protected by the gateway firewall as client hosts in the Intranet. For example, if you set up an FTP file server on the LAN side with local IP address 10.0.75.102 and global IP address 118.18.82.44, a remote user can access the file server while it is hidden behind the NAT gateway. That is because the gateway takes care of all access to the IP address 118.18.82.44, including forwarding access requests to the file server and to send the replies from the server to the outside world.

Virtual Server & Virtual Computer Setting

Go to Basic Network > Port Forwarding > Virtual Server & Virtual Computer tab.

Enable Virtual Server and Virtual Computer



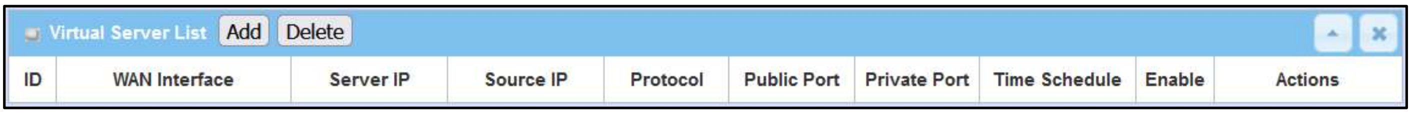
Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

Configuration Item	Value setting	Description
Virtual Server	Unchecked by default	Check the **Enable** box to activate this port forwarding function
Virtual Computer	The box is checked by default	Check the **Enable** box to activate this port forwarding function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.

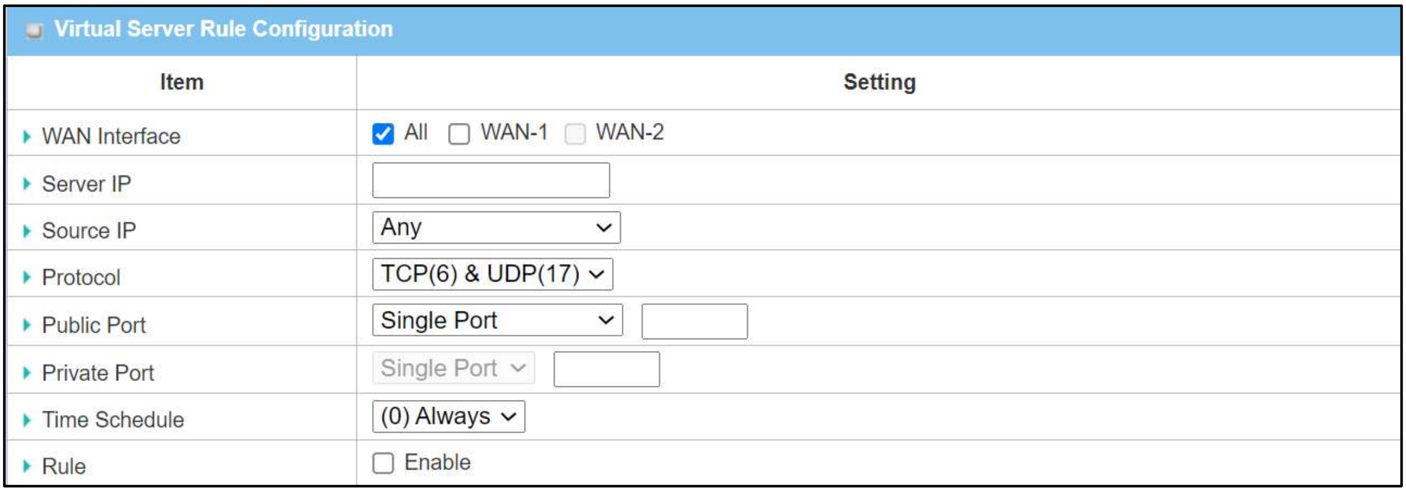
Create / Edit Virtual Server

The gateway allows you to customize your Virtual Server rules. It supports up to a maximum of 20 rule-based Virtual Server sets.



ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

When the **Add** button is applied, the **Virtual Server Rule Configuration** screen will appear.



Virtual Server Rule Configuration

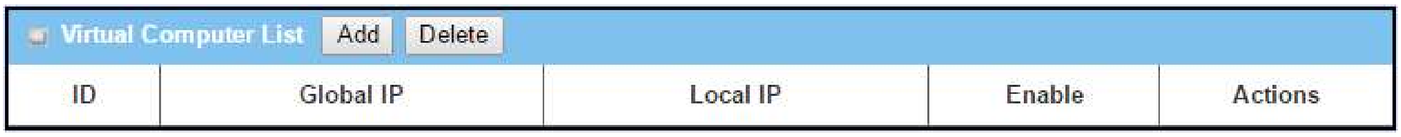
Item	Setting
WAN Interface	☑ All ☐ WAN-1 ☐ WAN-2
Server IP	
Source IP	Any
Protocol	TCP(6) & UDP(17)
Public Port	Single Port
Private Port	Single Port
Time Schedule	(0) Always
Rule	☐ Enable

Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
WAN Interface	1. Required setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the gateway. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the gateway from any interface. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
Server IP	Required setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Source IP	Required setting	Enter the source IP address.
Protocol	Required setting	When **"ICMPv4"** is selected, the protocol of packet filter rule is ICMPv4. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**Refer to **Scheduling setting** under **Object Definition).** Check **Enable** box to enable this rule. When **"TCP"** is selected, the protocol of packet filter rule is TCP. **Public Port** is a predefined port from **Well-known Service**, and **Private Port** is the same as **Public Port** number. **When Public Port** is set as **Single Port** and a port number specified, **Private Port** can be set as **Single Port** number. When Public Port is set as Port Range and a port range specified, Private Port can be set to Single Port or Port Range. *<u>Value Range</u>*: 1 ~ 65535 for Public Port, Private Port. When **"UDP"** is selected, the protocol of packet filter rule is UDP. **Public Port** is a predefined port from **Well-known Service**, and **Private Port** is the same as **Public Port** number. **When Public Port** is set as **Single Port** and a port number specified, **Private Port** can be set as **Single Port** number. When Public Port is set as Port Range and a port range specified, Private Port can be set to Single Port or Port Range.

		Value Range: 1 ~ 65535 for Public Port, Private Port. When **"TCP & UDP"** is selected, protocol of packet filter rule is TCP and UDP. **Public Port** is a predefined port from **Well-known Service**, and **Private Port** is the same as **Public Port** number. **When Public Port** is set as **Single Port** and a port number specified, **Private Port** can be set as **Single Port** number. When Public Port is set as Port Range and a port range specified, Private Port can be set to Single Port or Port Range. *Value Range*: 1 ~ 65535 for Public Port, Private Port. When **"GRE"** is selected, the protocol of packet filter rule is GRE.
		When **"ESP"** is selected, the protocol of packet filter rule is ESP. When **"SCTP"** is selected, the protocol of packet filter rule is SCTP. When **"User-defined"** is selected, the protocol of packet filter rule is User-defined. For **Protocol Number**, enter a port number.
Public Port		Select from **Well-known Service**, **Single Port**, or **Port range**. If Well-known Service is selected, select the desired service from the drop-down menu that will appear in the field on the right.
Private Port		Select **Single Port** or **Port Range**. Then enter the value(s) in the field(s) to the right.
Time Schedule	1. Optional setting 2. **(0)Always** Is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0)Always. (refer to Scheduling setting under Object Definition)
Rule	1. Optional setting 2.Unchecked by default	Check the Enable box to activate the rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	When the **Back** button is clicked the screen will return to previous page.

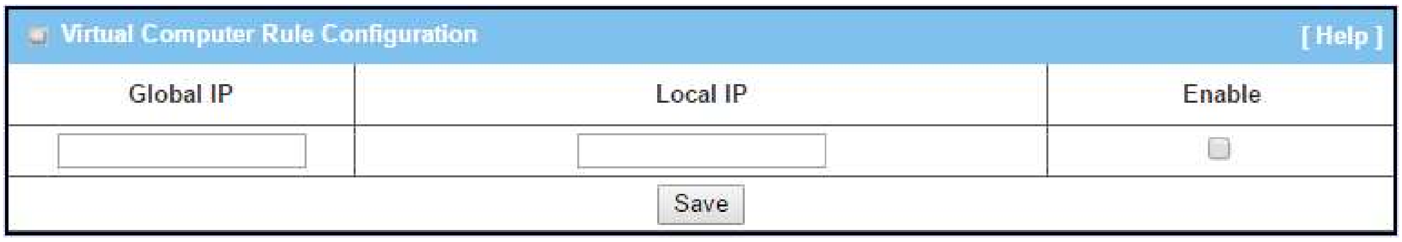
Create / Edit Virtual Computer

The gateway allows you to customize your Virtual Computer rules. It supports up to a maximum of 20 rule-based Virtual Computer sets.



ID	Global IP	Local IP	Enable	Actions

When the **Add** button is applied, the **Virtual Computer Rule Configuration** screen will appear.



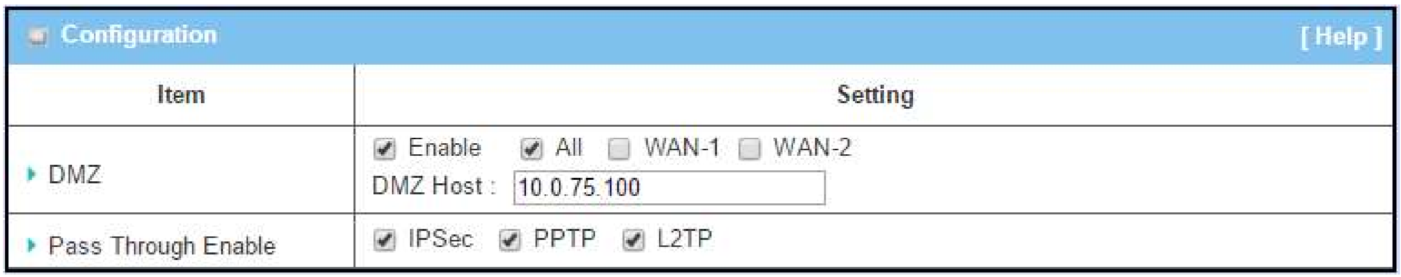
Global IP	Local IP	Enable
		□

Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	Required setting	Specify the IP address of the WAN IP.
Local IP	Required setting	Specify the IP address of the LAN IP.
Enable	N/A	Check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.

3.4.3 DMZ & Pass Through

A DMZ (Demilitarized Zone) Host is a host that is exposed to the Internet but still within the protection of a firewall by gateway device. This function allows a computer to execute 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. In some cases when a specific application is blocked by NAT mechanism, you can set the LAN computer as a DMZ host to solve this problem.

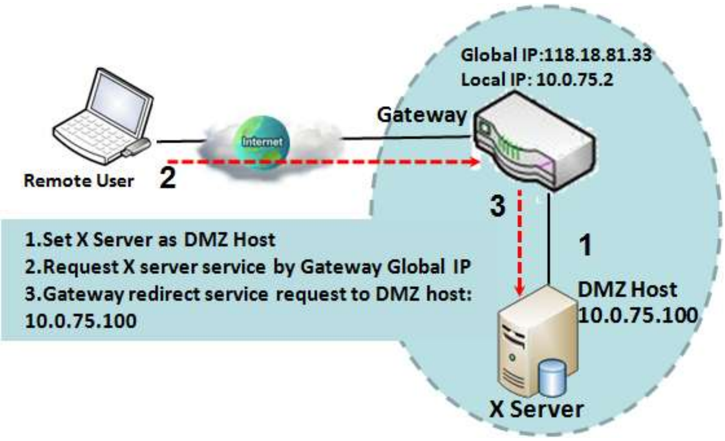
The DMZ function allows you to ask the gateway to pass through all normal packets to the DMZ host behind the NAT gateway only when these packets are not expected to be received by applications in the gateway or by other client hosts in the Intranet. The DMZ host is also protected by the gateway firewall. Activate the feature and specify the DMZ host with a host in the Intranet when needed.



Configuration [Help]

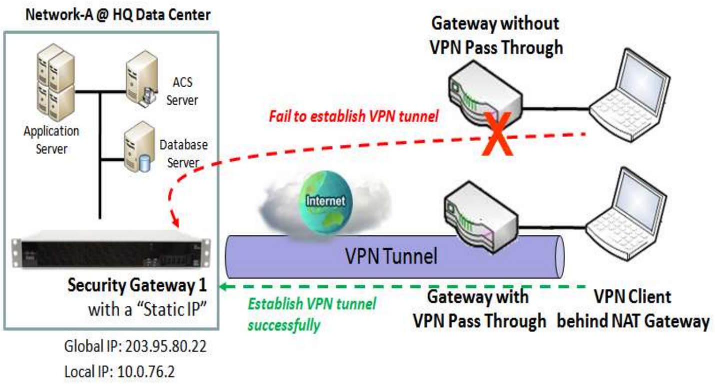
Item	Setting
DMZ	☑ Enable ☑ All □ WAN-1 □ WAN-2 DMZ Host : 10.0.75.100
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

DMZ Scenario


Global IP:118.18.81.33
Local IP: 10.0.75.2
Gateway
Internet
Remote User
2
3
1
1.Set X Server as DMZ Host
2.Request X server service by Gateway Global IP
3.Gateway redirect service request to DMZ host:
10.0.75.100
DMZ Host
10.0.75.100
X Server

When the network administrator wants to set up service daemons in a host behind a NAT gateway to allow remote users to actively request services from the server, the host should be configured as a DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. A remote user can request services from X server just as it is provided by the gateway whose global IP address is 118.18.81.33. The gateway will forward those packets, not belonging to any configured virtual server or applications, directly to the DMZ host.

VPN Pass through Scenario


Network-A @ HQ Data Center
ACS Server
Application Server
Database Server
Security Gateway 1 with a "Static IP"
Global IP: 203.95.80.22
Local IP: 10.0.76.2
Gateway without VPN Pass Through
Fail to establish VPN tunnel
Internet
VPN Tunnel
Establish VPN tunnel successfully
Gateway with VPN Pass Through
VPN Client behind NAT Gateway

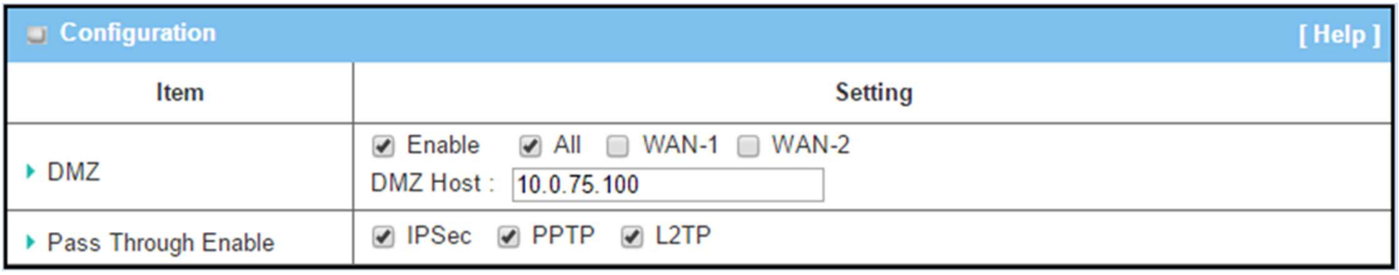
Since VPN traffic is different from that of TCP or UDP connection, it will be blocked by NAT gateway. To support the pass through function for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass through function for such application. The gateway supports the pass through function for IPsec, PPTP, and L2TP connections. Check the corresponding checkbox to activate it.

DMZ & Pass Through Setting

Go to Basic Network > Port Forwarding > DMZ & Pass Through tab.

The DMZ host is a host that is exposed to the Internet but is still within the protection of firewall by gateway device.

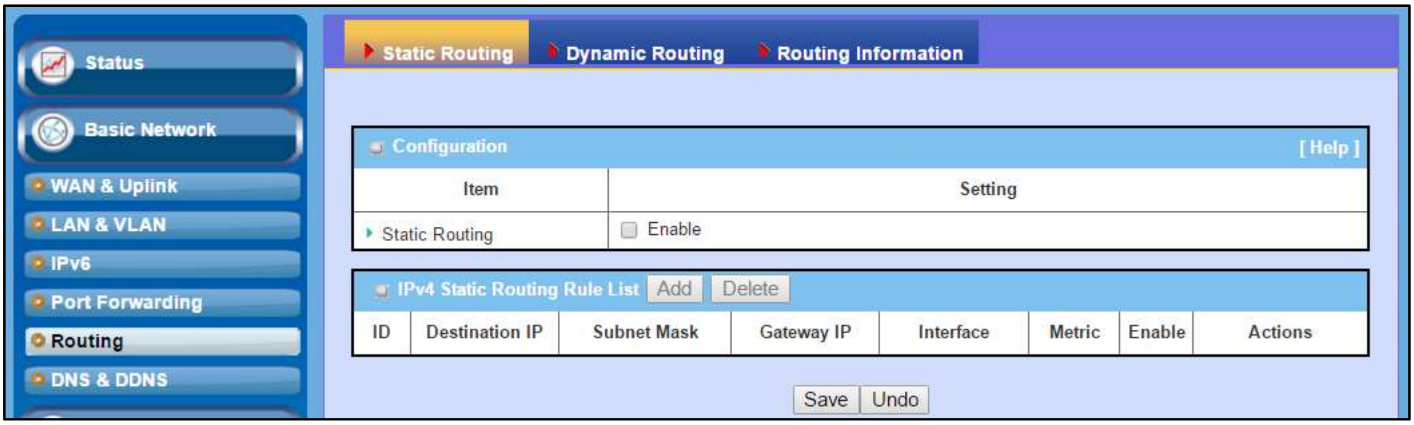
Enable DMZ and Pass Through


Configuration [Help]

Item	Setting
DMZ	☑ Enable ☑ All □ WAN-1 □ WAN-2 DMZ Host : 10.0.75.100
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

Configuration Item	Value setting	Description
DMZ	1. Required setting 2. Default is **ALL**.	Check the **Enable** box to activate the DMZ function Define the selected interface to be the packet-entering interface of the gateway, and fill in the IP address of Host LAN IP in **DMZ Host** field. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. **Note**: The available check boxes (**WAN-1** ~ **WAN-2**) depend on the number of WAN interfaces for the product.
Pass Through Enable	The boxes are checked by default	Check the box to enable pass through function for **IPsec**, **PPTP**, and **L2TP**. With the pass through function enabled, the VPN hosts behind the gateway can still connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

3.5 Routing



Configuration [Help]

Item	Setting
Static Routing	□ Enable

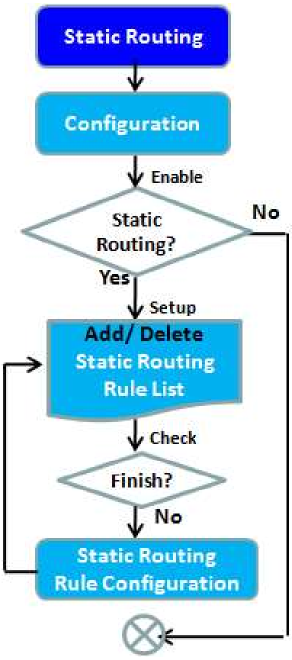
IPv4 Static Routing Rule List

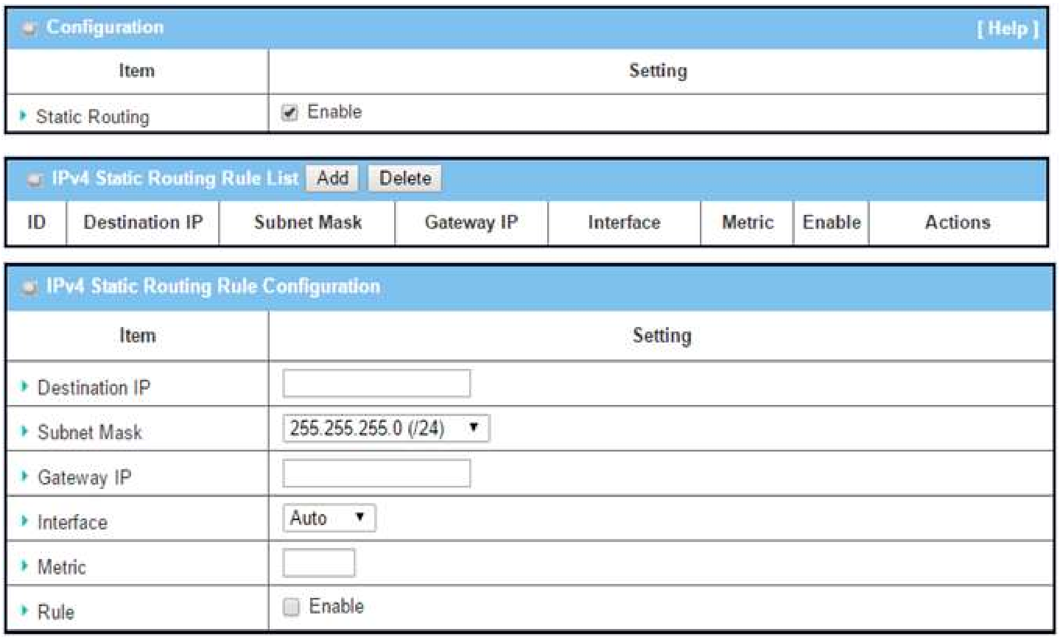
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

If you have more than one router and subnet, you will need to enable routing in order to allow packets to find a proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like electronic data networks (such as the Internet), by using packet switching technology. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time.

The routing tables can contain pre-defined routing paths for specific destinations. This is ***static routing***. However, if the contents of routing tables record the obtained routing paths from neighbor routers by using protocols such as RIP, OSPF and BGP, this is ***dynamic routing***. Both routing approaches will be illustrated. In addition, the gateway has advanced configurable routing software Quagga built-in for more complex routing applications. It can be configured via Telnet CLI.

3.5.1 Static Routing





Configuration [Help]

Item	Setting
Static Routing	☑ Enable

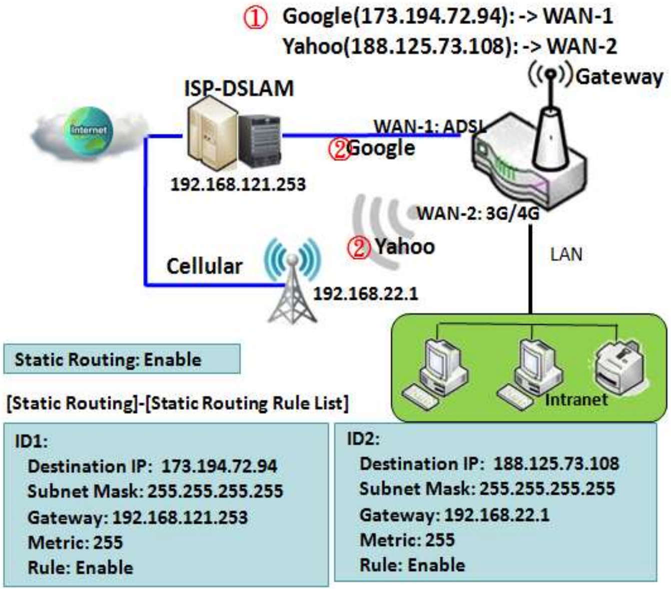
IPv4 Static Routing Rule List Add Delete

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

IPv4 Static Routing Rule Configuration

Item	Setting
Destination IP	
Subnet Mask	255.255.255.0 (/24) ▾
Gateway IP	
Interface	Auto ▾
Metric	
Rule	□ Enable

"Static Routing" lets you define the routing paths for some dedicated hosts/servers or subnets to be stored in the routing table of the gateway. The gateway routes incoming packets to different peer gateways based on the routing table. You need to define the static routing information in the gateway routing rule list.



Static Routing: Enable

[Static Routing]-[Static Routing Rule List]

ID1:
Destination IP: 173.194.72.94
Subnet Mask: 255.255.255.255
Gateway: 192.168.121.253
Metric: 255
Rule: Enable

ID2:
Destination IP: 188.125.73.108
Subnet Mask: 255.255.255.255
Gateway: 192.168.22.1
Metric: 255
Rule: Enable

When the administrator of the gateway wants to specify what kinds of packets will be transferred via which gateway interface and which peer gateway to their destination. It can be carried out by the "Static Routing" feature. Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding gateway interface that are defined in the system routing table by manual.

As shown in the diagram, when the destination is Google, rule 1 sets interface as ADSL, routing gateway as IP-DSLAM gateway 192.168.121.253. All packets to Google will go through WAN-1. The similar rule 2 sets 3G/4G as interface for traffic going to Yahoo.

Static Routing Setting

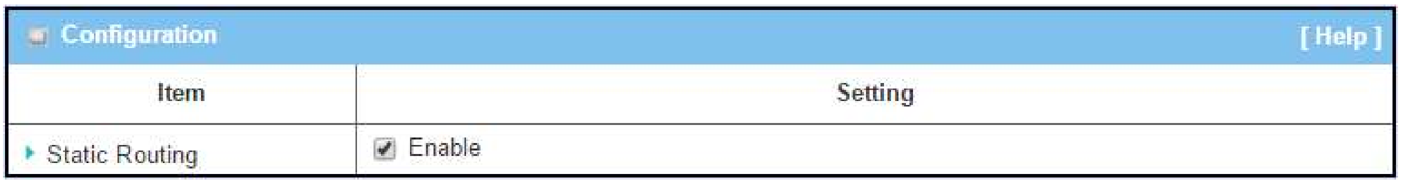
Go to **Basic Network** > **Routing** > **Static Routing** Tab.

There are three configuration windows for the static routing feature, including "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration". "Configuration" window lets you activate the global static routing feature. Even when there are existing routing rules, routing can be disabled temporarily by unchecking the Enable box. "Static Routing Rule List" window lists all your defined static routing rule entries. Use "Add" or "Edit" button to add and create one new static routing rule or to modify an existing one.

When "**Add**" or "**Edit**" button is applied, the "Static Routing Rule Configuration" window will appear to let you define a static routing rule.

Enable Static Routing

Check the **Enable** box to activate the "Static Routing" feature.



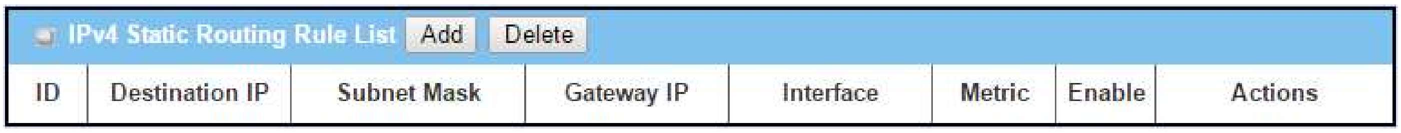
Configuration [Help]

Item	Setting
Static Routing	☑ Enable

Static Routing Item	Value setting	Description
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function

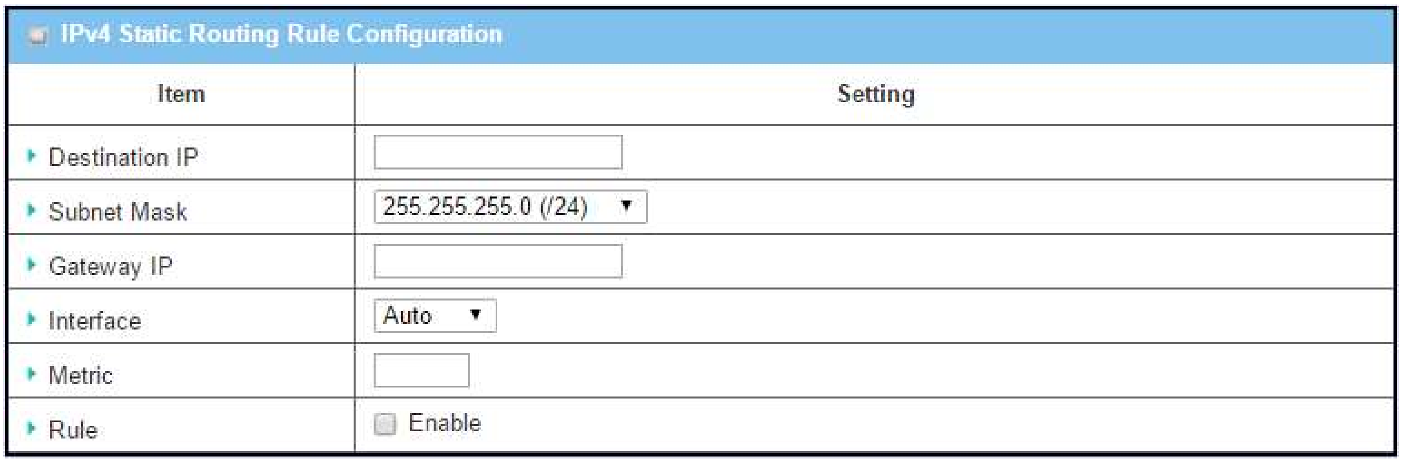
Create / Edit Static Routing Rules

The Static Routing Rule List shows the set up parameters of all static routing rule entries. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of peer gateway, the metric, and the rule activation.



ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

The gateway allows you to customize static routing rules. It supports up to a maximum of 64 rule sets. When the **Add** button is applied, the **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end of each static routing rule will let you modify the rule.

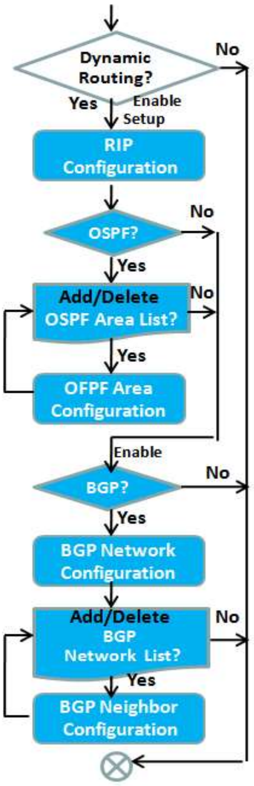


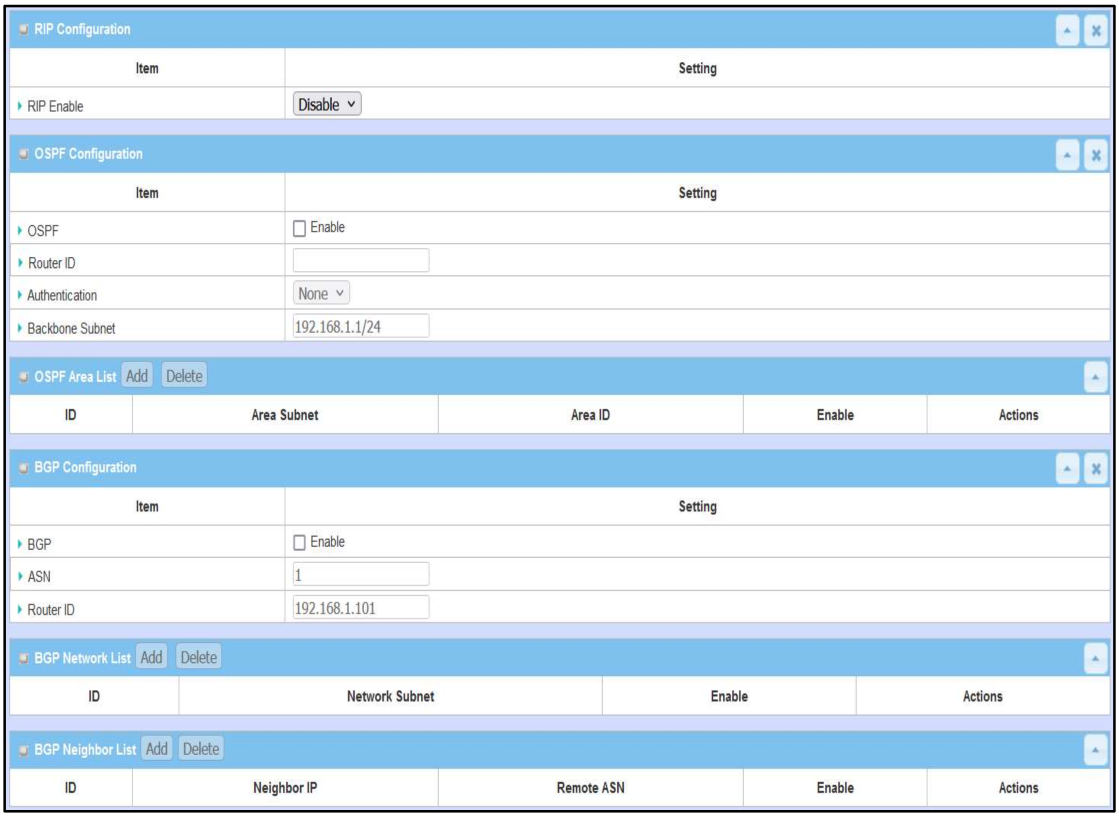
IPv4 Static Routing Rule Configuration

Item	Setting
Destination IP	
Subnet Mask	255.255.255.0 (/24) ▼
Gateway IP	
Interface	Auto ▼
Metric	
Rule	□ Enable

IPv4 Static Routing Item	Value setting	Description
Destination IP	1. IPv4 Format 2. Required setting	Specify the Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. Required setting	Specify the Gateway IP of this static routing rule.
Interface	Auto is set by default	Select the Interface of this static routing rule. It can be **Auto**, or the available WAN / LAN interfaces.
Metric	1. Numeric String Format 2. Required setting	The Metric of this static routing rule. Value Range: 0 ~ 255.
Rule	Unchecked by default	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore previous settings.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

3.5.2 Dynamic Routing





RIP Configuration

Item	Setting
RIP Enable	Disable

OSPF Configuration

Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None
Backbone Subnet	192.168.1.1/24

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

BGP Configuration

Item	Setting
BGP	□ Enable
ASN	1
Router ID	192.168.1.101

BGP Network List Add Delete

ID	Network Subnet	Enable	Actions

BGP Neighbor List Add Delete

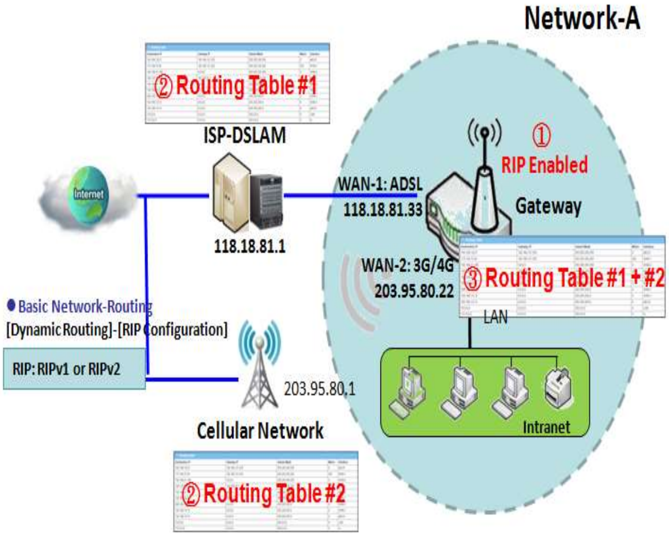
ID	Neighbor IP	Remote ASN	Enable	Actions

Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.

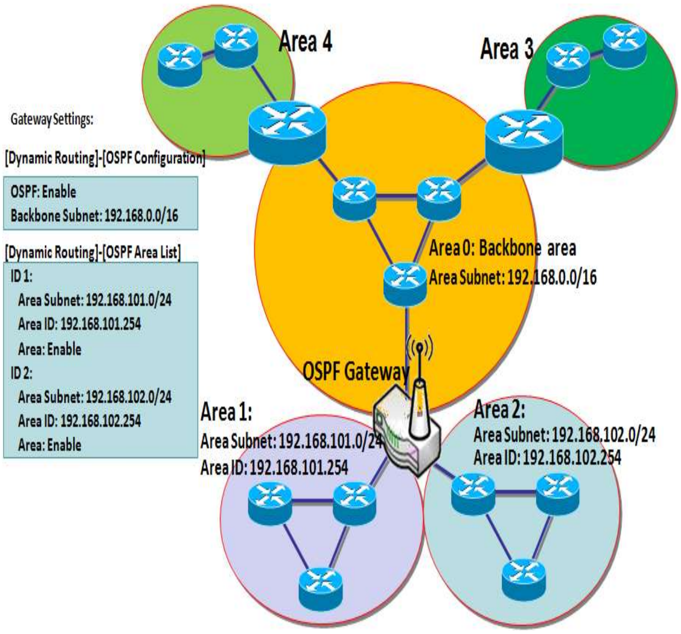
This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), to establish the routing table automatically. Dynamic routing can be very useful when there are many subnets in your network. Generally speaking, RIP is suitable for small networks. OSPF is more suitable for medium networks. BGP is more used for large network infrastructure.

The supported dynamic routing protocols are described as follows.

RIP Scenario



The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols. It employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.


Area 4
Area 3
Gateway Settings:
[Dynamic Routing]-[OSPF Configuration]
OSPF: Enable
Backbone Subnet: 192.168.0.0/16
[Dynamic Routing]-[OSPF Area List]
ID 1:
Area Subnet: 192.168.101.0/24
Area ID: 192.168.101.254
Area: Enable
ID 2:
Area Subnet: 192.168.102.0/24
Area ID: 192.168.102.254
Area: Enable
Area 0: Backbone area
Area Subnet: 192.168.0.0/16
OSPF Gateway
Area 1:
Area Subnet: 192.168.101.0/24
Area ID: 192.168.101.254
Area 2:
Area Subnet: 192.168.102.0/24
Area ID: 192.168.102.254

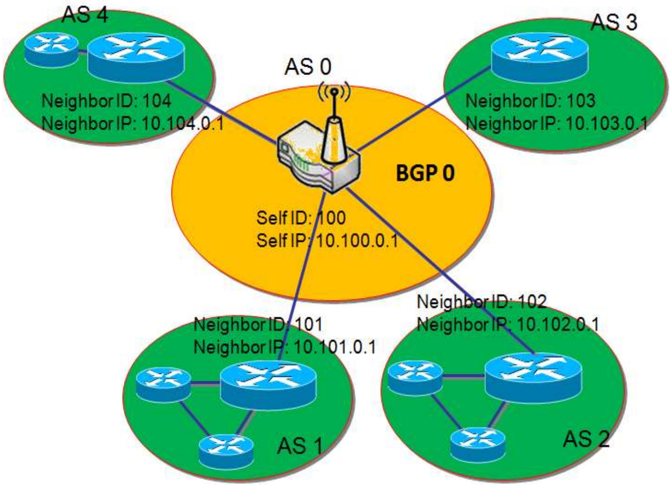
OSPF Scenario

Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table which routes datagrams based solely on the destination IP address.

The network administrator can deploy an OSPF gateway in large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are not linked to the enterprise backbone. Usually, an OSPF network is subdivided into routing areas to simplify administration and optimize traffic and resource utilization.

As shown in the diagram, the OSPF gateway gathers routing information from the backbone gateways in area 0, and will forward its routing information to the routers in area 1 and area 2 which are not in the backbone.

BGP Scenario



Border Gateway Protocol (BGP) is a standard exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It usually makes routing decisions based on paths, network policies, or rule-sets.

Most ISPs use BGP to establish routing between one another (especially for multihomed networks). Very large private IP networks also use BGP internally. The major BGP gateway within one AS will link with other border gateways for exchanging routing information. It will distribute the collected data in AS to all routers in other AS.

As shown in the diagram, BGP 0 is gateway to dominate AS0 (self IP is 10.100.0.1 and self ID is 100). It links with other BGP gateways on the Internet. The scenario is like a subnet in one ISP being linked with ones in other ISPs. By operating with BGP protocol, BGP 0 can gather routing information from other BGP gateways on the Internet. It then forwards the routing data to the routers in its dominated AS. Finally, the routers resided in AS 0 know how to route packets to other AS.

Dynamic Routing Setting

Go to **Basic Network** > **Routing** > **Dynamic Routing** Tab.

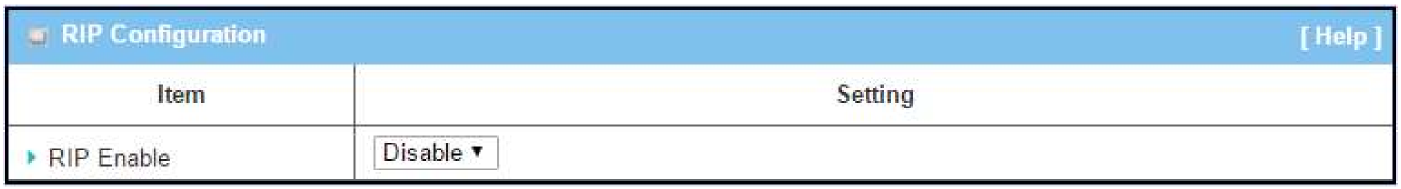
The dynamic routing setting allows user to customize RIP, OSPF, and BGP protocols through the router based on their office settings.

In the "Dynamic Routing" page, there are seven configuration windows for dynamic routing feature. They are "RIP Configuration", "OSPF Configuration", "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration". RIP, OSPF and BGP protocols can be configured individually.

The "RIP Configuration" window lets you choose which version of RIP protocol to be activated, or to disable it. The "OSPF Configuration" window lets you activate the OSPF dynamic routing protocol and specify its backbone subnet. Moreover, the "OSPF Area List" window lists all defined areas in the OSPF network. The "BGP Configuration" window will let you activate the BGP dynamic routing protocol and specify its own ID. The "BGP Neighbor List" window lists all defined neighbors in the BGP network.

RIP Configuration

The RIP configuration setting allows user to customize RIP protocol through the router based on their office setting.

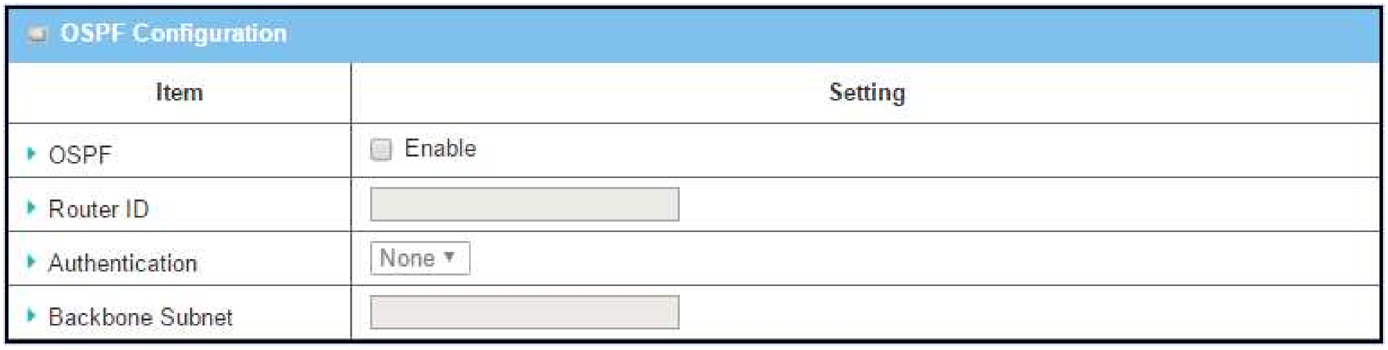


RIP Configuration [Help]

Item	Setting
RIP Enable	Disable ▼

RIP Configuration		
Item	**Value setting**	**Description**
RIP Enable	Disabled by default	Select **Disable** to disable RIP protocol. Select **RIP v1** to enable RIPv1 protocol. Select **RIP v2** to enable RIPv2 protocol.

OSPF Configuration



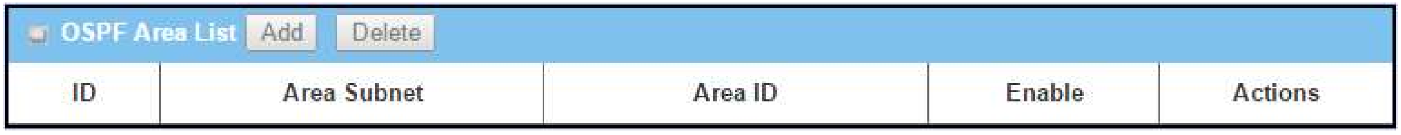
OSPF Configuration

Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None ▼
Backbone Subnet	

OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Click **Enable** box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. Required setting	The Router ID of this router in OSPF protocol
Authentication	**None** is set by default	The Authentication method of this router in OSPF protocol. Select **None** to disable Authentication in OSPF protocol. Select **Text** to enable Text Authentication with entered the Key in this field in OSPF protocol. Select **MD5** to enable MD5 Authentication with entered the ID and Key in these fields on OSPF protocol.
Backbone Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. Required setting	The Backbone Subnet of this router on OSPF protocol.

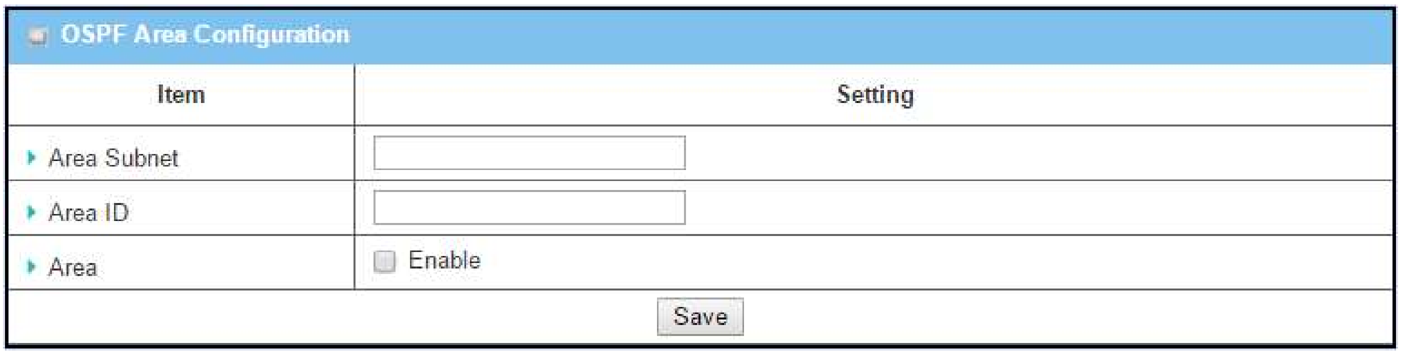
Create / Edit OSPF Area Rules

The gateway allows you to customize your OSPF Area List rules. It supports up to a maximum of 32 rule sets.



ID	Area Subnet	Area ID	Enable	Actions

When the **Add** button is applied, the **OSPF Area Rule Configuration** screen will appear.

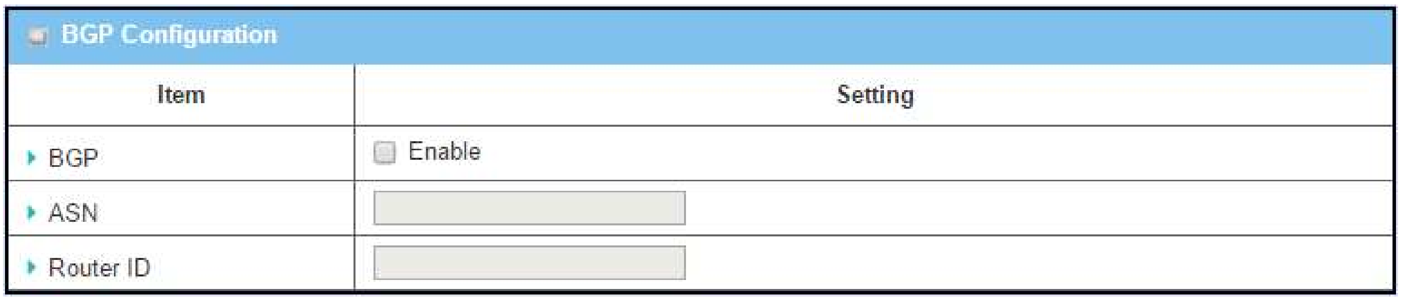


Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

OSPF Area Configuration Item	Value setting	Description
Area Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. Required setting	The Area Subnet of this router in OSPF Area List.
Area ID	1. IPv4 Format 2. Required setting	The Area ID of this router in OSPF Area List.
Area	Unchecked by default	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

BGP Configuration

The BGP configuration setting allows user to customize BGP protocol through the router setting.



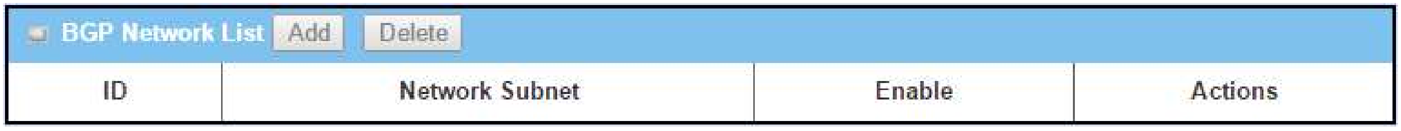
BGP Configuration

Item	Setting
BGP	□ Enable
ASN	
Router ID	

BGP Network Configuration		
Item	**Value setting**	**Description**
BGP	Unchecked by default	Check the **Enable** box to activate the BGP protocol.
ASN	1. Numeric String Format 2. Required setting	The ASN Number of this router on BGP protocol. ***Value Range***: 1 ~ 4294967295.
Router ID	1. IPv4 Format 2. Required setting	The Router ID of this router on BGP protocol.

Create / Edit BGP Network Rules

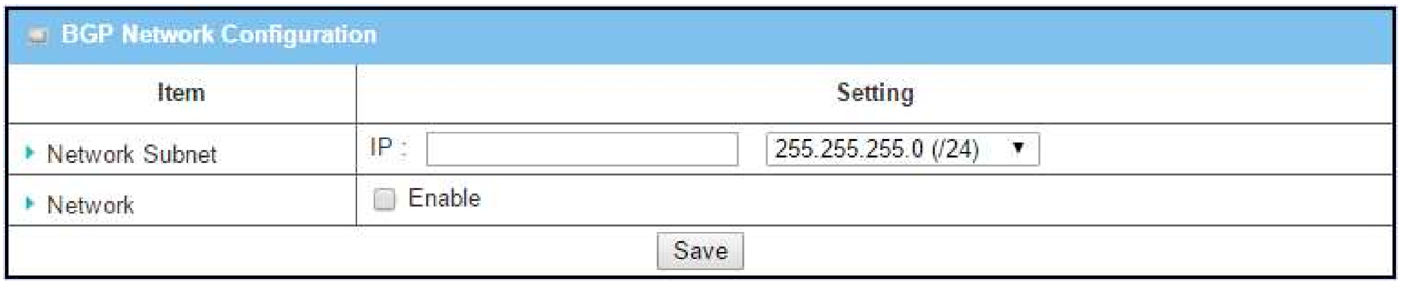
The gateway allows you to customize your BGP Network rules. It supports up to a maximum of 32 rule sets.



BGP Network List Add Delete

ID	Network Subnet	Enable	Actions

When the **Add** button is applied, the **BGP Network Rule Configuration** screen will appear.



BGP Network Configuration

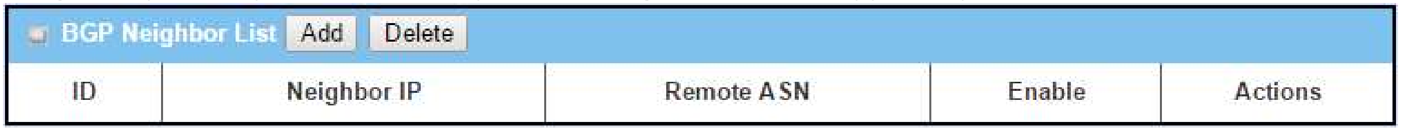
Item	Setting
Network Subnet	IP : 255.255.255.0 (/24) ▼
Network	□ Enable

Save

Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. Required setting	The Network Subnet of this router in BGP Network List. Enter the IP address in this field and the selected subnet mask.
Network	Unchecked by default	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Create / Edit BGP Neighbor Rules

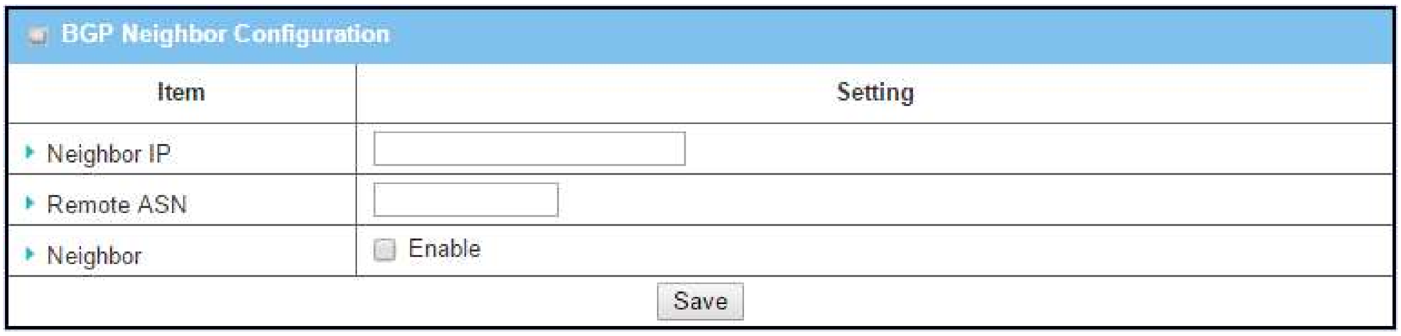
The gateway allows you to customize your BGP Neighbor rules. It supports up to a maximum of 32 rule sets.



BGP Neighbor List

ID	Neighbor IP	Remote ASN	Enable	Actions

When the **Add** button is applied, the **BGP Neighbor Rule Configuration** screen will appear.



BGP Neighbor Configuration

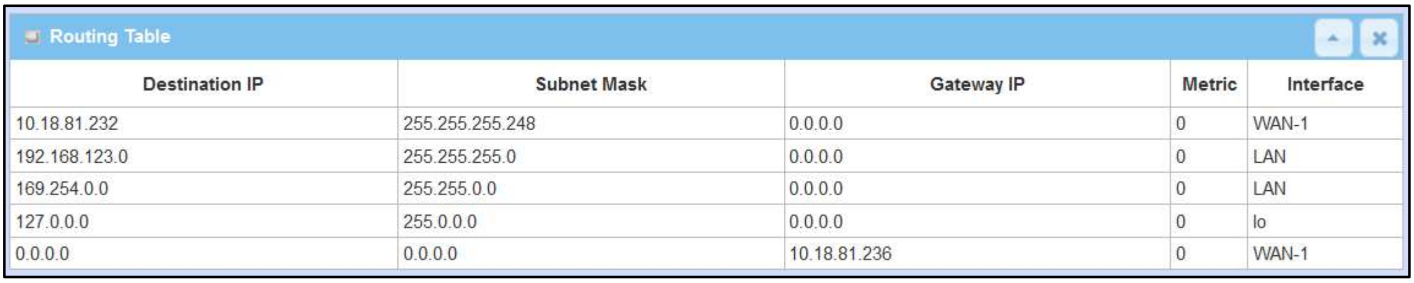
Item	Setting
Neighbor IP	
Remote ASN	
Neighbor	□ Enable

BGP Neighbor Configuration Item	 Value setting	 Description
Neighbor IP	1. IPv4 Format 2. Required setting	The Neighbor IP of this router on BGP Neighbor List.
Remote ASN	1. Numeric String Format 2. Required setting	The Remote ASN of this router on BGP Neighbor List. ***Value Range***: 1 ~ 4294967295.
Neighbor	Unchecked by default	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

3.5.3 Routing Information

The routing information allows the user to view the routing table and policy routing information. Policy Routing Information is only available when the **Load Balance** function is enabled and the **Load Balance Strategy** is **By User Policy**.

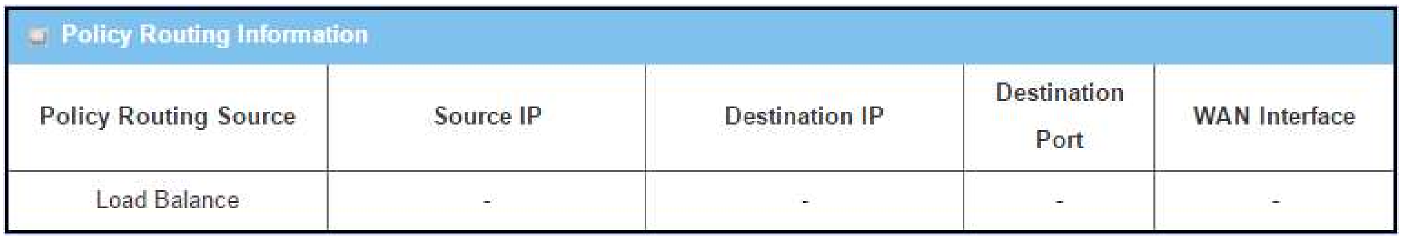
Go to Basic Network > Routing > Routing Information Tab.



Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
10.18.81.232	255.255.255.248	0.0.0.0	0	WAN-1
192.168.123.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo
0.0.0.0	0.0.0.0	10.18.81.236	0	WAN-1

Routing Table		
Item	**Value setting**	**Description**
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	N/A	Routing record of Gateway IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface	N/A	Routing record of Interface Type. String Format.



Policy Routing Information

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

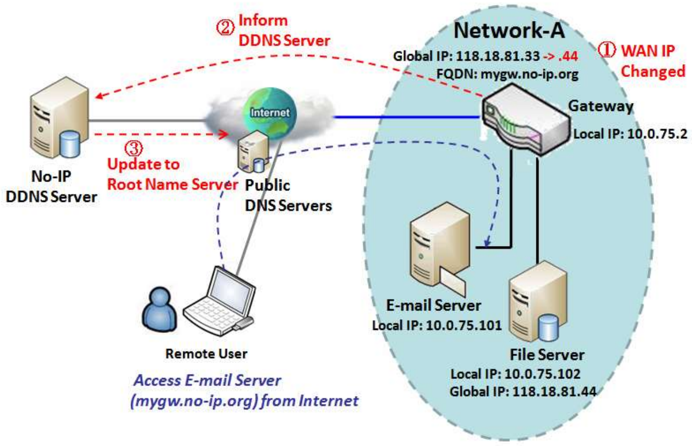
Policy Routing Information		
Item	**Value setting**	**Description**
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port. String Format.
WAN Interface	N/A	Policy Routing of WAN Interface. String Format.

3.6 DNS & DDNS

How does a user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider.

3.6.1 DNS & DDNS Configuration

Dynamic DNS



To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

The Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from various locations on the Internet. As shown in the diagram, the user registered a domain name to a third-party DDNS service provider (NO-IP) to use DDNS function. Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts or remote users on the Internet are able to link to your gateway by using your domain name regardless of the changing global IP address.

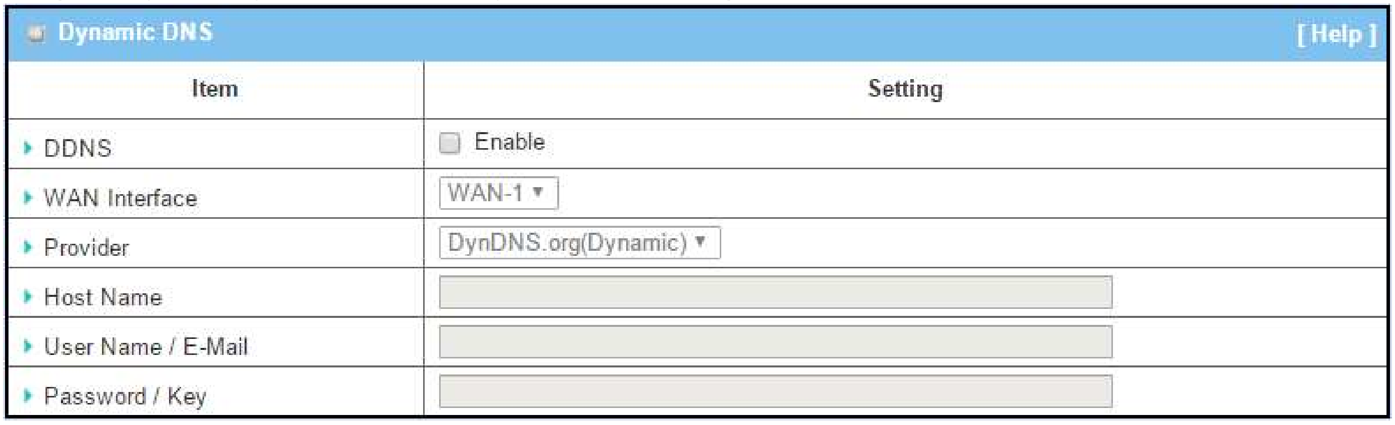
DNS & DDNS Setting

Go to **Basic Network** > **DNS & DDNS** > **Configuration** Tab.

The DNS & DDNS setting allows user to setup Dynamic DNS feature and DNS redirect rules.

Setup Dynamic DNS

The gateway allows you to customize Dynamic DNS settings.



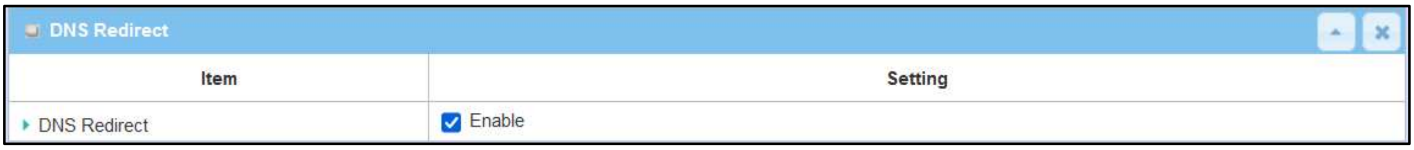
Dynamic DNS

Item	Setting
DDNS	□ Enable
WAN Interface	WAN-1 ▾
Provider	DynDNS.org(Dynamic) ▾
Host Name	
User Name / E-Mail	
Password / Key	

DDNS (Dynamic DNS) Configuration		
Item	**Value setting**	**Description**
DDNS	Unchecked by default	Check the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the gateway.
Provider	DynDNS.org (Dynamic) is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org(Dynamic)**, **DynDNS.org(Custom)**, **NO-IP.com**, etc...
Host Name	1. String format, any text 2. Required setting	Your registered host name of Dynamic DNS. ***Value Range***: 0 ~ 63 characters.
User Name / E-Mail	1. String format, any text 2. Required setting	Enter your User name or E-mail address of Dynamic DNS.
Password / Key	1. String format, any text 2. Required setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup DNS Redirect

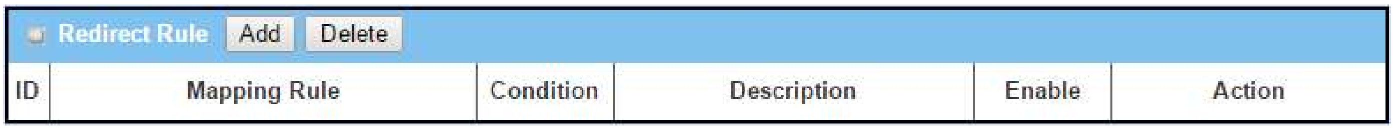
DNS redirect is a special function to redirect certain traffic to a specified host. The administrator can manage the internet / intranet traffic that will access a restricted DNS and force that traffic to be redirected to a specified host.



Item	Setting
DNS Redirect	☑ Enable

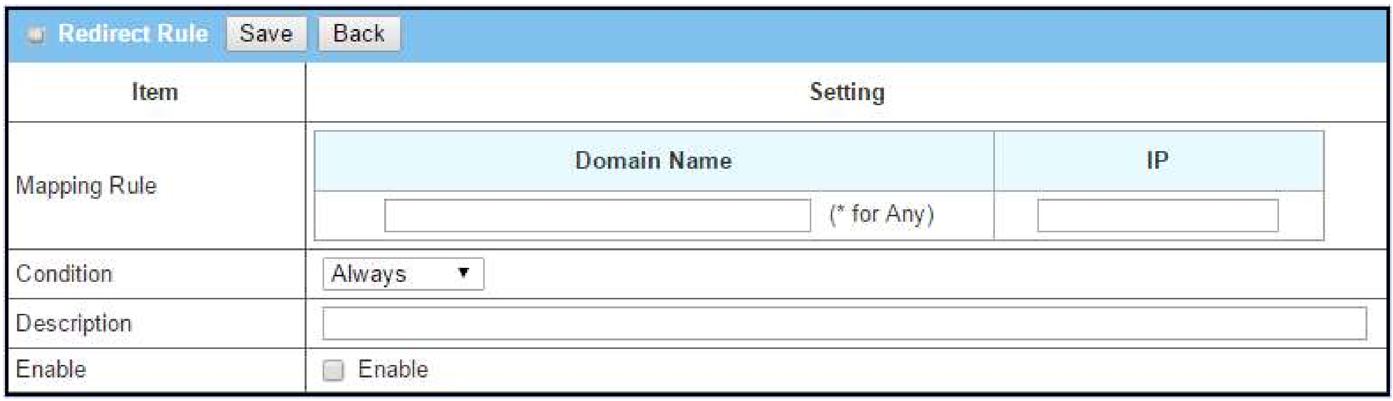
DNS Redirect Configuration		
Item	**Value setting**	**Description**
DNS Redirect	Unchecked by default	Check the **Enable** box to activate this function.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

If you enabled the DNS Redirect function, you have to further specify the redirect rules. According to the rules, the gateway can redirect the traffic that matches the DNS to a corresponding pre-defined IP address.



ID	Mapping Rule	Condition	Description	Enable	Action

When the **Add** button is applied, the **Redirect Rule** screen will appear.



Item	Setting
Mapping Rule	Domain Name: ________ (* for Any) IP: ________
Condition	Always ▼
Description	________
Enable	□ Enable

Redirect Rule Configuration		
Item	Value setting	Description
Domain Name	1. String format, any text 2. Required setting	Enter a domain name to be redirected. The traffic to specified domain name will be redirect to the following IP address. ***Value Range***: at least 1 character is required; '*' for any.
IP	1. IPv4 format 2. Required setting	Enter an IP Address as the target for the DNS redirect.
Condition	1. Required setting **2. Always is selected by default.**	Specify when the DNS redirect action can be applied. It can be **Always**, or **WAN Block**. **Always:** The DNS redirect function can be applied to matching DNS all the time. **WAN Block:** The DNS redirect function can be applied to matching DNS only when the WAN connection is disconnected, or un-reachable.
Description	1. String format, any text 2. Required setting	Enter a brief description for this rule. ***Value Range***: 0 ~ 63 characters.
Enable	Unchecked by default	Click the **Enable** button to activate this rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

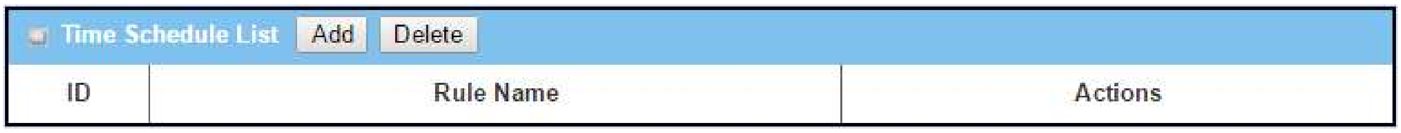
Chapter 4 Object Definition

4.1 Scheduling

Scheduling provides the ability to add/delete time schedule rules, which can be applied to other functions.

4.1.1 Scheduling Configuration

Go to Object Definition > Scheduling > Configuration tab.

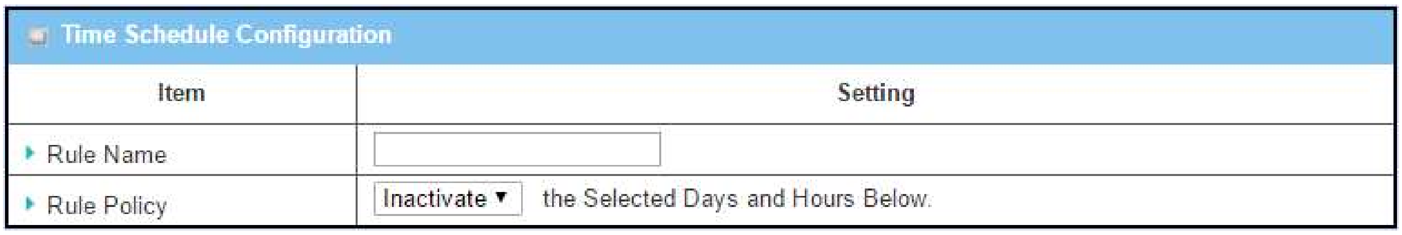


Time Schedule List Add Delete

ID	Rule Name	Actions

Button description		
Item	**Value setting**	**Description**
Add	N/A	Click the **Add** button to configure time schedule rule
Delete	N/A	Click the **Delete** button to delete selected rule(s)

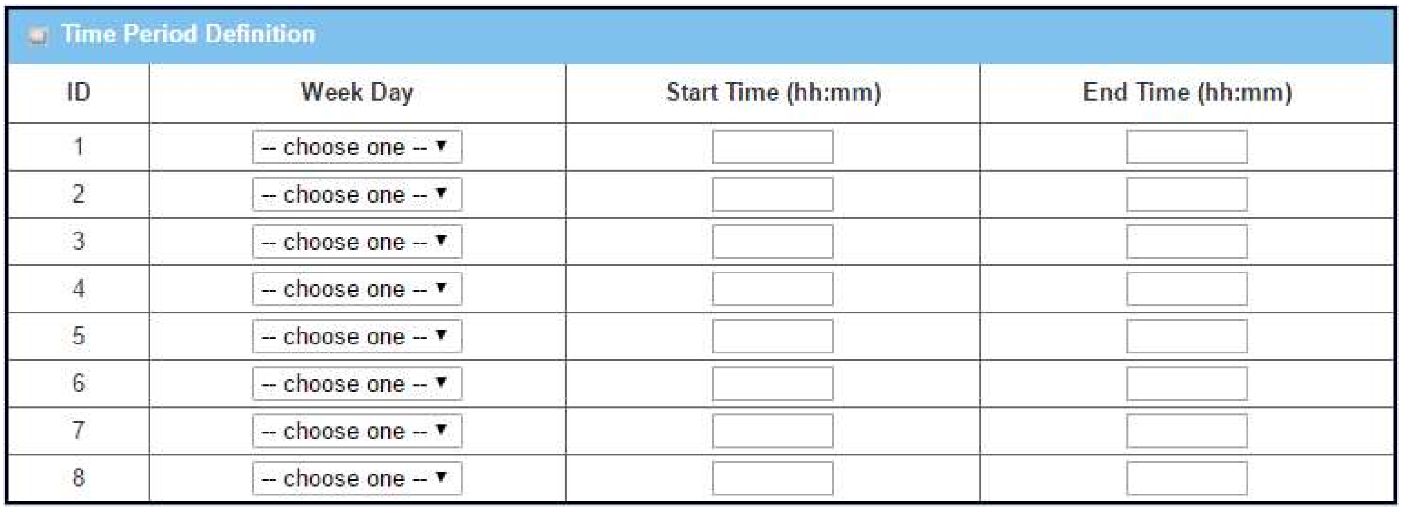
When the **Add** button is applied, the Time Schedule Configuration and Time Period Definition screens will appear.



Time Schedule Configuration

Item	Setting
Rule Name	
Rule Policy	Inactivate ▾ the Selected Days and Hours Below.

Time Schedule Configuration		
Item	**Value Setting**	**Description**
Rule Name	String: any text	Set rule name
Rule Policy	Default Inactivate	Inactivate/activate the function applied to in the time period below



Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▾		
2	-- choose one -- ▾		
3	-- choose one -- ▾		
4	-- choose one -- ▾		
5	-- choose one -- ▾		
6	-- choose one -- ▾		
7	-- choose one -- ▾		
8	-- choose one -- ▾		

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select every day or a weekday
Start Time	Time format (hh:mm)	Start time in selected weekday
End Time	Time format (hh:mm)	End time in selected weekday
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the time schedule list.

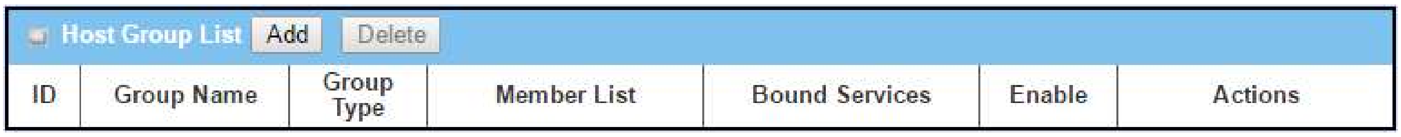
4.2 Grouping

The Grouping function allows the user to make groups for certain services.

4.2.1 Host Grouping

Go to Object Definition > Grouping > Host Grouping tab.

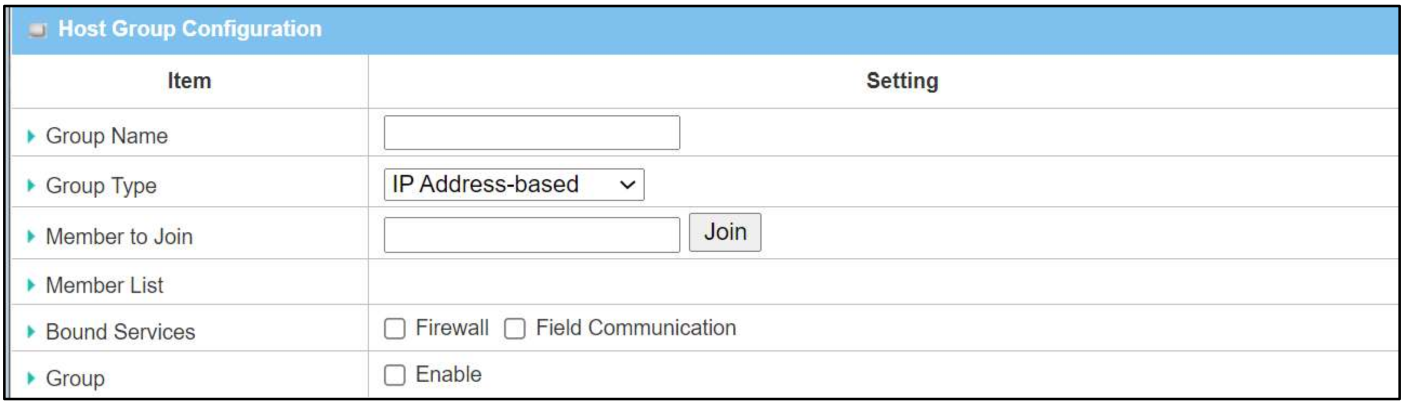
The Host Grouping function allows the user to make host groups for services, such as QoS, Firewall, and Communication Bus. The supported service types may differ by product type.



Host Group List Add Delete

ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

When the **Add** button is applied, the **Host Group Configuration** screen will appear.



Host Group Configuration

Item	Setting
Group Name	
Group Type	IP Address-based
Member to Join	Join
Member List	
Bound Services	□ Firewall □ Field Communication
Group	□ Enable

Host Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format, any text 2. Required setting	Enter a group name for the rule.
Group Type	1. **IP Address-based** is selected by default. 2. Required setting	Select the group type for the host group. It can be **IP Address-based**, **MAC Address-based**, or **Host Name-based**. When **IP Address-based** is selected, only IP addresses can be added in **Member to Join.** When **MAC Address-based** is selected, only MAC addresses can be added in **Member to Join.**

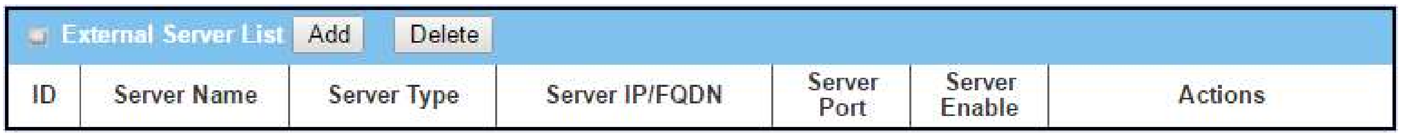
		When **Host Name-based** is selected, only host names can be added in **Member to Join.** Note: The available Group Types will differ depending on the device model.
Member to Join	N/A	Add the members to the group in this field. You can enter the member information as specified in the Member Type above, and press the **Join** button to add. Only one member can be added at a time.
Member List	NA	This field will indicate the hosts (members) contained in the group.
Bound Services	Boxes are unchecked by default	Binding services applied to the host group. If you enable the **Firewall**, the produced group can be used in firewall service.
Group	Unchecked by default	Check the **Enable** checkbox to activate the host group rule. The group will be bound to the selected service(s) for further configuration.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

4.3 External Server

Go to Object Definition > External Server > External Server tab.

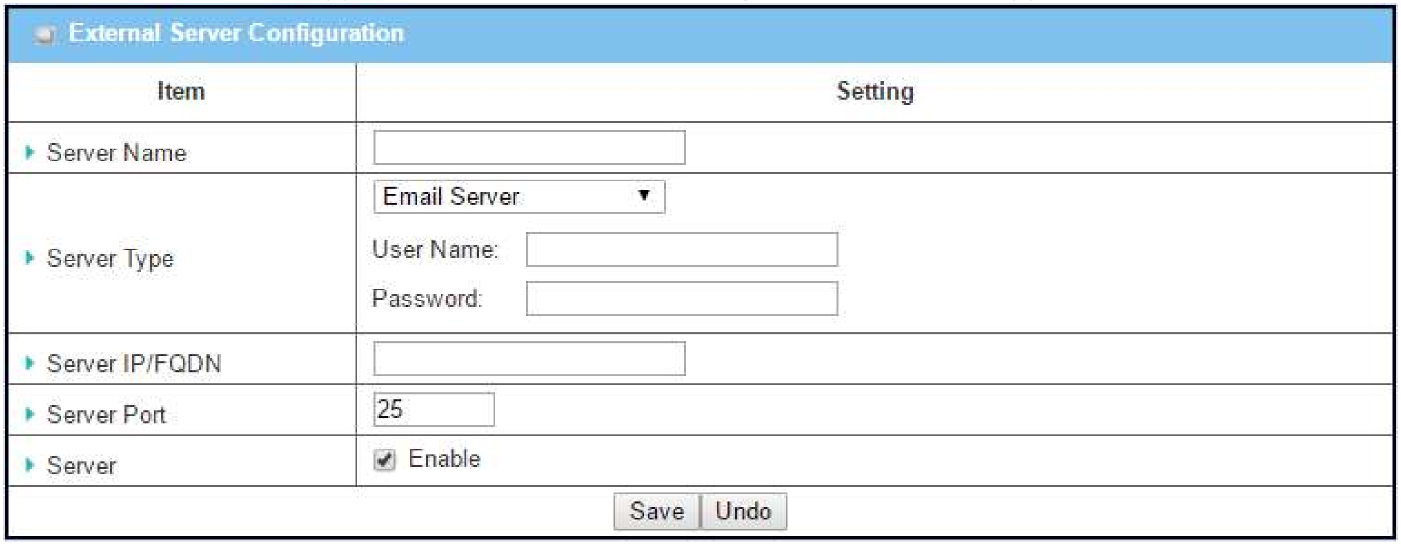
The External Server setting allows the user to add an external server.

Create External Server



ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

When the **Add** button is applied, the **External Server Configuration** screen will appear.



Item	Setting
Server Name	
Server Type	Email Server ▾ User Name: Password:
Server IP/FQDN	
Server Port	25
Server	☑ Enable

External Server Configuration		
Item	**Value setting**	**Description**
Sever Name	1. String format, any text 2. Required setting	Enter a server name.
Server Type	Required setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		Email Server (Required setting): When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text)
		RADIUS Server (Required setting): When **RADIUS Server** is selected, the following settings are also required. Primary: **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 15. Secondary: **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 15.
		Active Directory Server (Required setting): When **Active Directory Server** is selected, **Domain** setting is also required. **Domain** (String format: any text)
		LDAP Server (Required setting): When **LDAP Server** is selected, the following settings are also required. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text)
		UAM Server (Required setting): When **UAM Server** is selected, the following settings are also required. **Login URL** (String format: any text) **Shared Secret** (String format: any text) **NAS/Gateway ID** (String format: any text) **Location ID** (String format: any text) **Location Name** (String format: any text)
		TACACS+ Server (Required setting):

		When **TACACS+ Server** is selected, the following settings are also required. **Shared Key** (String format: any text) **Session Timeout** (String format: any number) The values must be between 1 and 60.
		SCEP Server (Required setting): When **SCEP Server** is selected, the following settings are also required. **Path** (String format: any text, by default **cgi-bin** is filled) **Application** (String format: any text, by default **pkiclient.exe** is filled)
		FTP(SFTP) Server (Required setting): When **FTP(SFTP) Server** is selected, the following settings are also required. **User Name** (String format: any text) **Password** (String format: any text) Protocol (Select FTP or SFTP) Encryption (Select Plain, Explicit FTPS or Implicit FTPS) Transfer mode (Select Passive or Active)
Server IP/FQDN	Required setting	Specify the IP address or FQDN used for the external server.
Server Port	Required setting	Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set. For **Email Server** 25 will be set by default; For **Syslog Server**, port 514 will be set by default; For **RADIUS Server**, port 1812 will be set by default; For **Active Directory Server**, port 389 will be set by default; For **LDAP Server**, port 389 will be set by default; For **UAM Server**, port 80 will be set by default; For **TACACS+ Server**, port 49 will be set by default; For **SCEP Server**, port 80 will be set by default; For **FTP(SFTP) Server**, port 21 will be set by default; *Value Range*: 1 ~ 65535.
Account Port	1. Required setting **2. 1813 is set by default**	Specify the accounting port used if you selected external RADIUS server. *Value Range*: 1 ~ 65535.
Server	The box is checked by default	Click **Enable to** activate this External Server.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the external server list.

4.4 Certificates

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

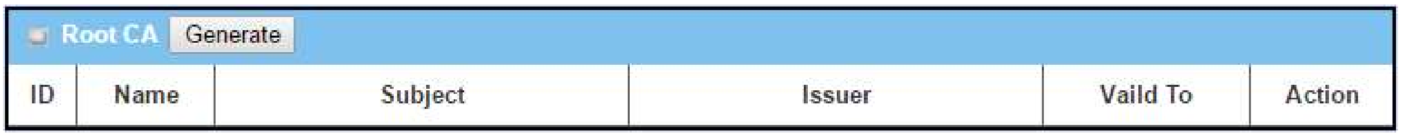
Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPsec tunneling for user authentication.

4.4.1 Configuration

The configuration setting allows user to create Root Certificate Authority (CA) certificates and configure enabling of SCEP. Root CA is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

Go to Object Definition > Certificate > Configuration tab.

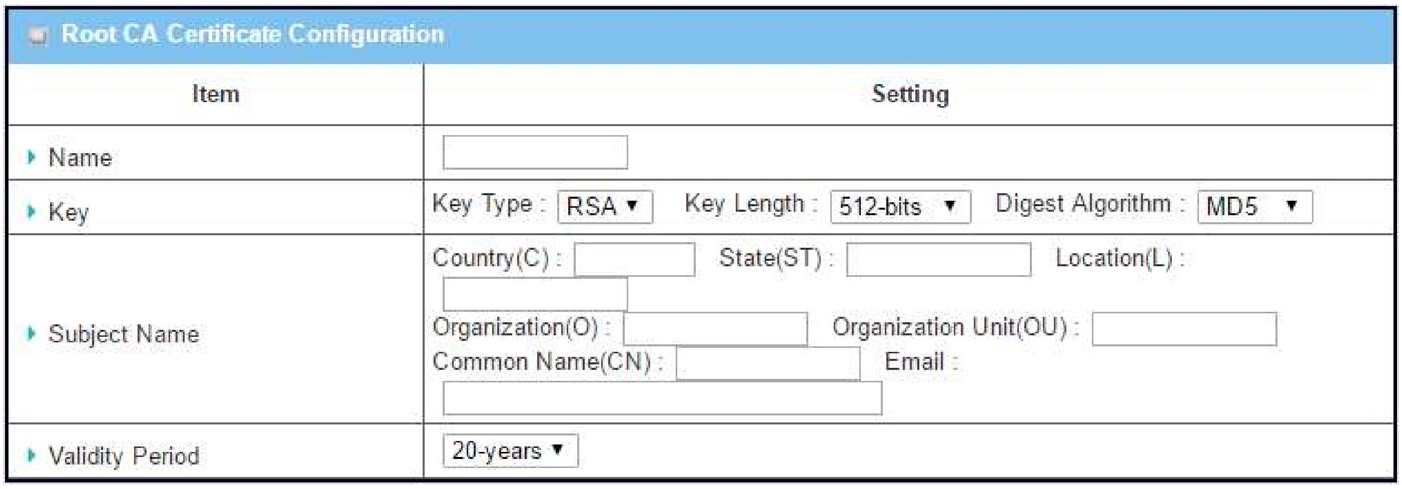
Create Root CA



Root CA Generate

ID	Name	Subject	Issuer	Vaild To	Action

When the **Generate** button is applied, the **Root CA Certificate Configuration** screen will appear. The required information to be filled for the root CA includes the name, key, subject name, and validity.



Root CA Certificate Configuration

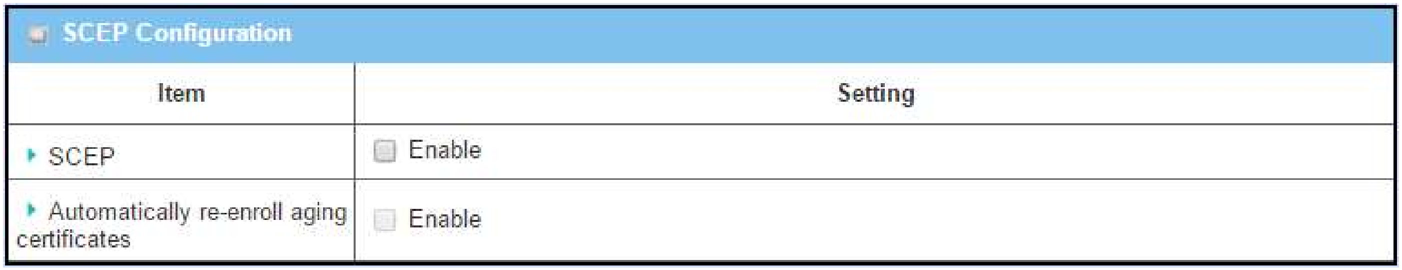
Item	Setting
Name	
Key	Key Type : RSA ▼ Key Length : 512-bits ▼ Digest Algorithm : MD5 ▼

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

Validity Period	20-years ▼

Root CA Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format, any text 2. Required setting	Enter a Root CA Certificate name. It will be a certificate file name
Key	Required setting	This field is to specify the key attribute of certificate. **Key Type** to set public-key cryptosystems. Only RSA is currently supported. **Key Length** to set the size measured in bits of the key used in a cryptographic algorithm. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates
Subject Name	Required setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address format.
Validity Period	Required setting	This field is to specify the validity period of certificate.

Set up SCEP



SCEP Configuration

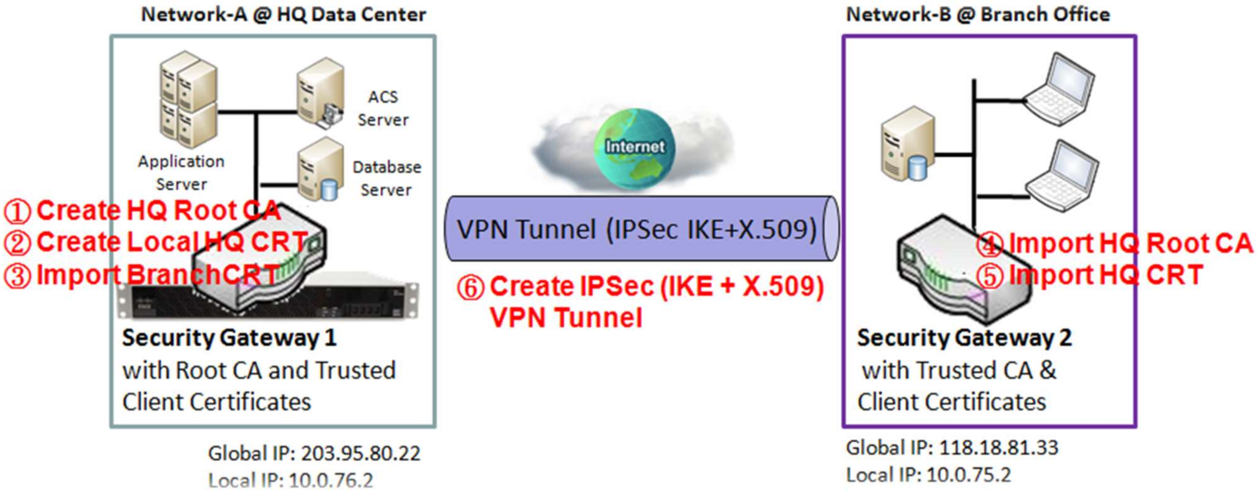
Item	Setting
SCEP	□ Enable
Automatically re-enroll aging certificates	□ Enable

SCEP Configuration		
Item	**Value setting**	**Description**
SCEP	Unchecked by default	Check the **Enable** box to activate SCEP function.
Automatically re-enroll aging certificates	Unchecked by default	When **SCEP** is activated, check the **Enable** box to activate this function. It will automatically check for certificate aging. If certificate is aging, it will activate SCEP function to re-enroll automatically.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

4.4.2 My Certificate

My Certificate includes a Local Certificate List. The Local Certificate List shows all generated certificates by the root CA for the gateway. It also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the gateway.

Self-signed Certificate Usage Scenario



Scenario Application Timing

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself or import any local certificates that are signed by other external CAs. It can also import trusted certificates for other CAs and Clients. In addition, since it has the root CA, it also can sign Certificate Signing Requests (CSR) to form corresponding certificates for others. These certificates can be used for two remote peers to make sure of their identity when establishing a VPN tunnel.

Scenario Description

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It imports a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. It imports the certificate into the Gateway 2 as a local certificate. In addition, it also imports the certificates of the root CA of Gateway 1 into Gateway 2 as the trusted ones. (Refer to following two sub-sections)

An IPsec VPN tunnel is established with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

The following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPsec VPN tunnel establishing, as shown in the above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use default value for parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Root CA Certificate Configuration]
Name	***HQRootCA***
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***TW*** State(ST): ***Taiwan*** Location(L): ***Taipei*** Organization(O): ***EWANHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQRootCA*** E-mail: ***hqrootca@etherwan.com.tw***

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***HQCRT*** Self-signed: ■
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***TW*** State(ST): ***Taiwan*** Location(L): ***Taipei*** Organization(O): ***EWANHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQCRT*** E-mail: ***hqcrt@etherwan.com.tw***

Configuration Path	[IPSec]-[Configuration]
IPSec	■ ***Enable***

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-101***
Interface	***WAN 1***
Tunnel Scenario	***Site to Site***
Operation Mode	***Always on***

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	***10.0.76.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.75.0***
Remote Netmask	***255.255.255.0***
Remote Gateway	***118.18.81.33***

Configuration Path	[IPSec]-[Authentication]
Key Management	***IKE+X.509*** Local Certificate: ***HQCRT*** Remote Certificate: ***BranchCRT***
Local ID	***User Name Network-A***
Remote ID	***User Name Network-B***

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	***Main Mode***
X-Auth	***None***

For Network-B at Branch Office

The following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPsec VPN tunnel establishing, as shown in the above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use the default value for parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***BranchCRT*** Self-signed: □
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***TW*** State(ST): ***Taiwan*** Location(L): ***Taipei*** Organization(O): ***EWANBranch*** Organization Unit(OU): ***BranchRD*** Common Name(CN): ***BranchCRT*** E-mail: ***branchcrt@etherwan.com.tw***

Configuration Path	[IPSec]-[Configuration]
IPSec	■ ***Enable***

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-102***
Interface	***WAN 1***
Tunnel Scenario	***Site to Site***
Operation Mode	***Always on***

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	***10.0.75.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.76.0***

Remote Netmask	***255.255.255.0***
Remote Gateway	***203.95.80.22***

Configuration Path	[IPSec]-[Authentication]
Key Management	***IKE+X.509*** Local Certificate: ***BranchCRT*** Remote Certificate: ***HQCRT***
Local ID	***User Name Network-B***
Remote ID	***User Name Network-A***

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	***Main Mode***
X-Auth	***None***

Scenario Operation Procedure

In the above diagram, "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. It imports the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate (BranchCRT) (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just download it.). Take the CSR to be signed by the root CA of Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of Gateway 2.

Gateway 2 can establish an IPsec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

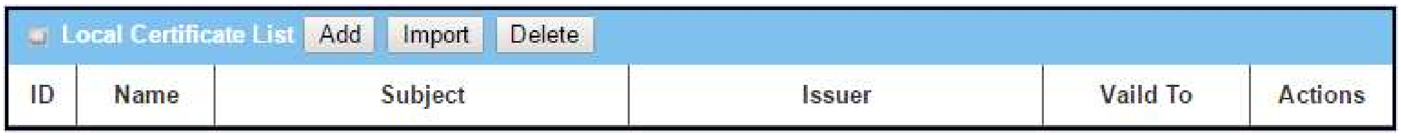
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

My Certificate Setting

Go to Object Definition > Certificate > My Certificate tab.

The My Certificate setting allows user to create local certificates. In "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. The "Local Certificate Configuration" window lets you enter the required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

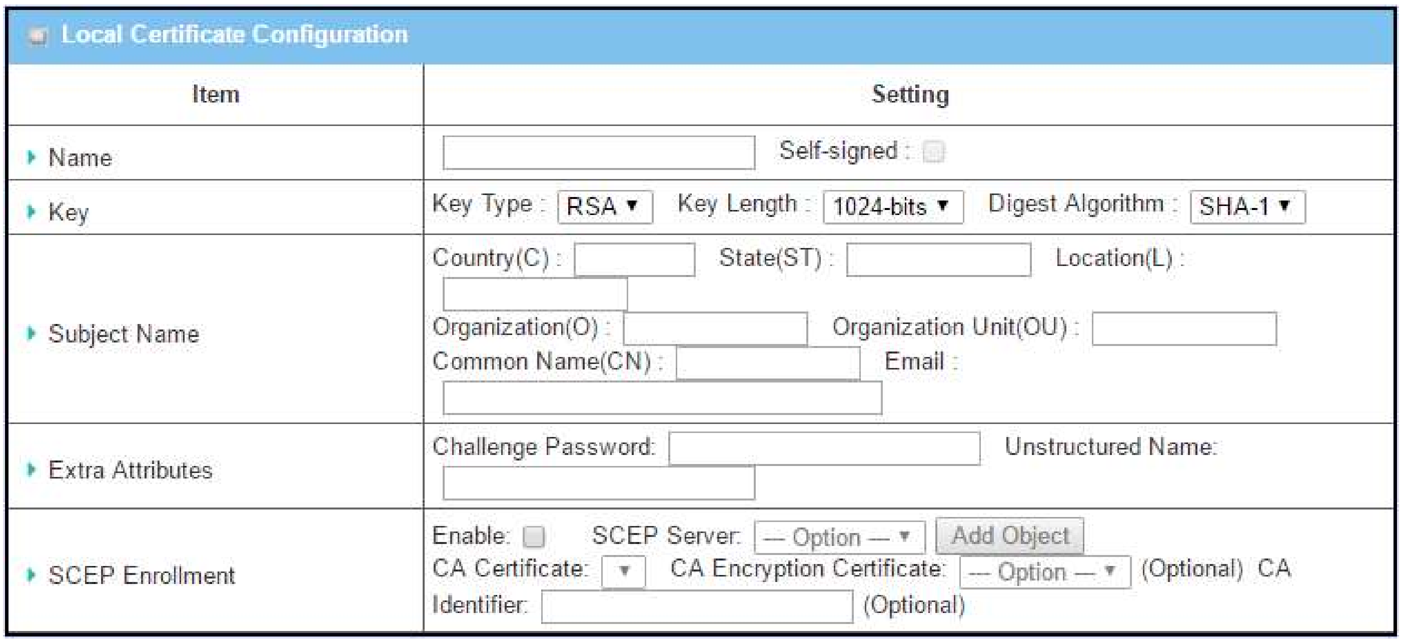
Create Local Certificate



Local Certificate List

ID	Name	Subject	Issuer	Vaild To	Actions

When the **Add** button is applied, the **Local Certificate Configuration** screen will appear. The required information to be filled for the certificate or CSR includes the name, key, and subject name. It is a certificate if the "Self-signed" box is checked; otherwise, it is a CSR.



Local Certificate Configuration

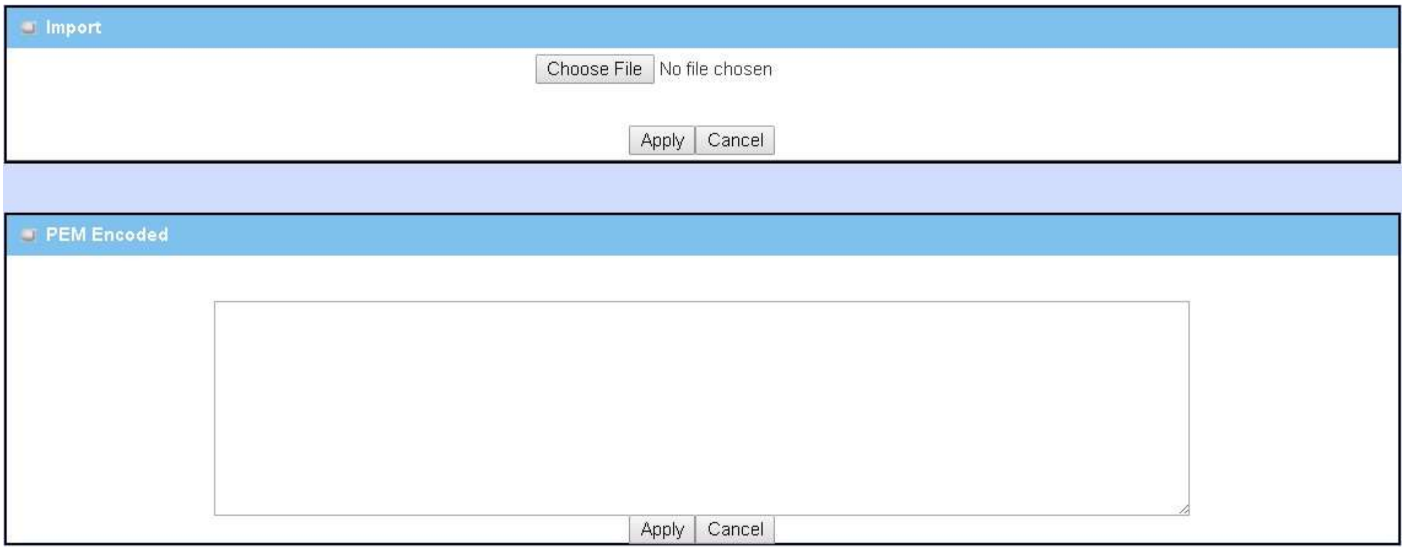
Item	Setting
Name	Self-signed : □
Key	Key Type : RSA ▾ Key Length : 1024-bits ▾ Digest Algorithm : SHA-1 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

Extra Attributes	Challenge Password: Unstructured Name:
SCEP Enrollment	Enable: □ SCEP Server: — Option — ▾ Add Object CA Certificate: ▾ CA Encryption Certificate: — Option — ▾ (Optional) CA Identifier: (Optional)

Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format, any text 2. Required setting	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	Required setting	This field is to specify the key attributes of certificate. **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	Required setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address format.
Extra Attributes	Required setting	This field is to specify the extra information for generating a certificate. **Challenge Password** for the password you can use to request certificate revocation in the future. **Unstructured Name** for additional information.
SCEP Enrollment	Required setting	This field is to specify the information for SCEP. To generate a certificate signing request (CSR) and have it signed by SCEP server online, check the **Enable** box. Select a **SCEP Server** to identify the SCEP server for use. The server detailed information can be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. Click the **Add Object** button to generate. Select a **CA Certificate** to identify which certificate can be accepted by SCEP server for authentication. It can be generated in Trusted Certificates. Select an optional **CA Encryption Certificate**, if it is required, to identify which certificate can be accepted by SCEP server for encryption data information. It can be generated in Trusted Certificates. Fill in optional **CA Identifier** to identify which CA can be used for signing certificates.
Save	N/A	Click the **Save** button to save the configuration.
Back	N/A	When the **Back** button is clicked, the screen will return to previous page.

When the **Import** button is applied, an Import screen will appear. You can import a certificate from an existing certificate file, or directly paste a PEM encoded string as the certificate.

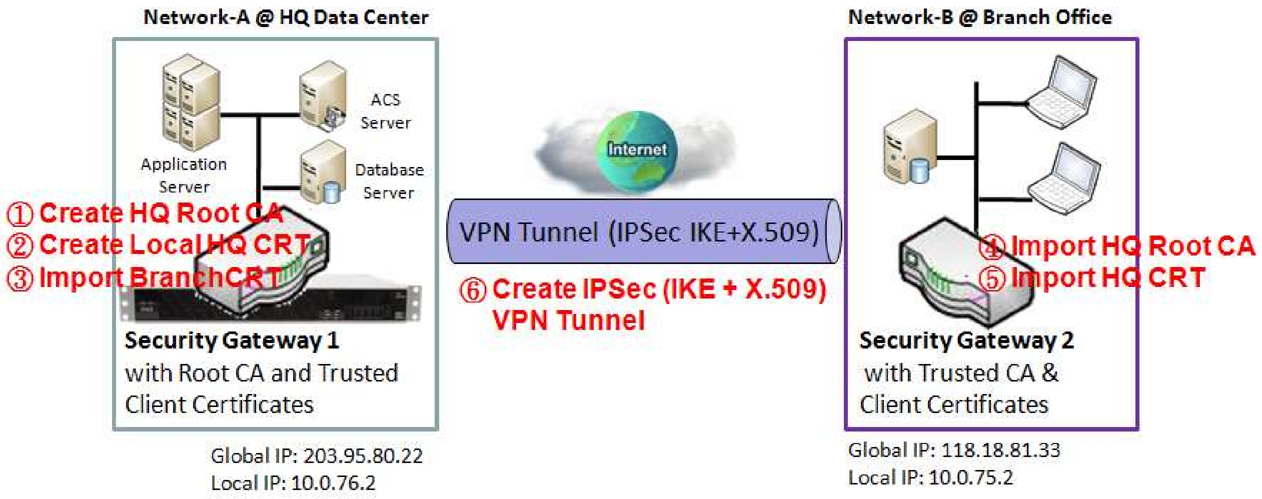


Import		
Item	**Value setting**	**Description**
Import	Required setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
PEM Encoded	1. String format, any text 2. Required setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the My Certificates page.

4.4.3 Trusted Certificate

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List contains the certificates of external trusted CAs. The Trusted Client Certificate List contains the others' certificates that you trust. The Trusted Client Key List contains the others' keys that you have trusted.

Self-signed Certificate Usage Scenario



Scenario Application Timing (same as described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates being signed by itself. It also imports trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to confirm their identity when establishing a VPN tunnel.

Scenario Description (same as described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It imports a trusted certificate (BranchCRT) – a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of Gateway 1 sign it to be the BranchCRT certificate. It imports the certificate into the Gateway 2 as a local certificate. It also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as trusted ones. (Refer to "My Certificate" and "Issue Certificate" sections).

An IPsec VPN tunnel can be established with IKE and X.509 protocols starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example is the same as described in "My Certificate" section.

For Network-A at HQ

The following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPsec VPN tunnel establishing, as shown in the above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issue Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	***BranchCRT.crt***

For Network-B at Branch Office

The following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in the above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issued Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	***HQRootCA.crt***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	***HQCRT.crt***

Scenario Operation Procedure (same as described in "My Certificate" section)

In the above diagram, "Gateway 1" is the gateway of Network-A located at headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B located at the branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 2 imports the certificates of the root CA and HQCRT that were generated and signed by Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Import the obtained BranchCRT certificate (the derived BranchCSR certificate after Gateway 1’s root CA signature) into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2. For more details, refer to the Network-B operation procedure in "My Certificate" section of this manual.

Gateway 2 can establish an IPsec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

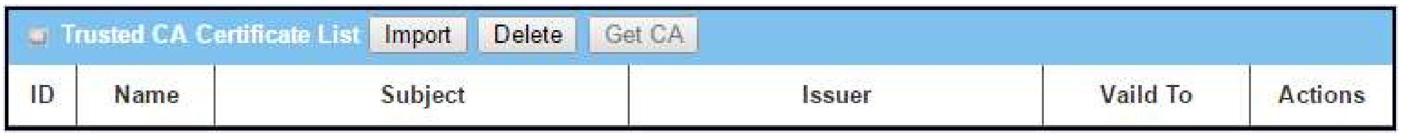
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Trusted Certificate Setting

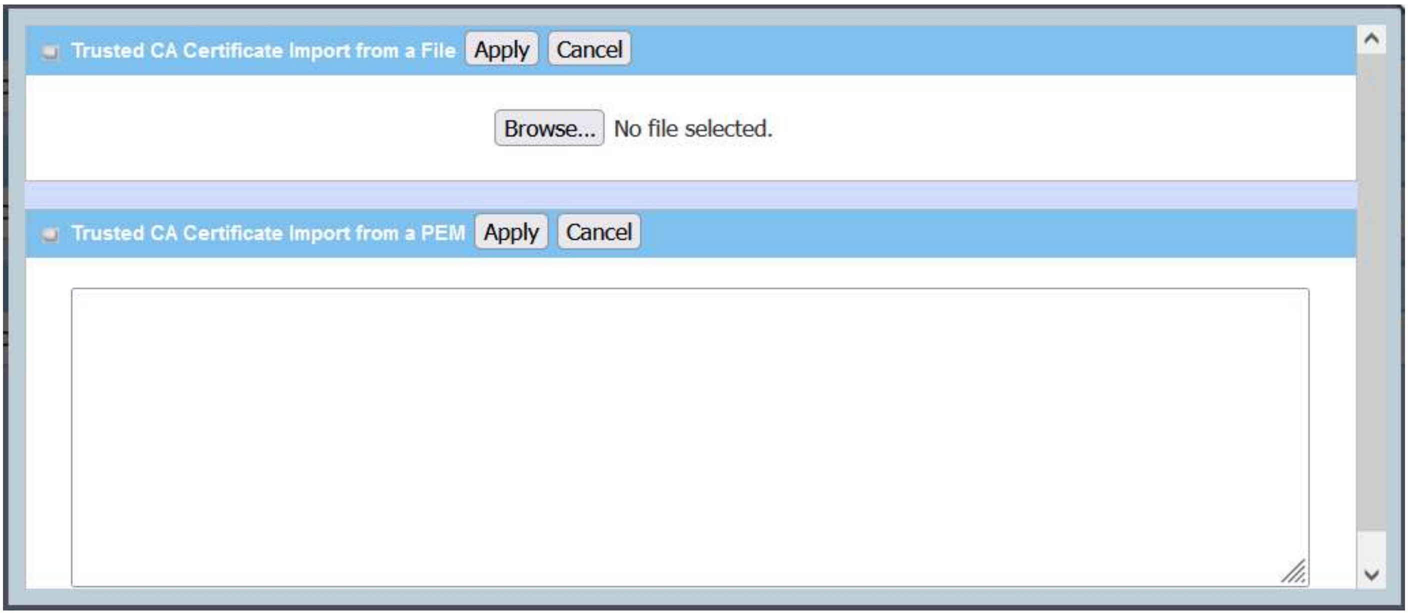
Go to Object Definition > Certificate > Trusted Certificate tab.

The Trusted Certificate setting allows the user to import trusted certificates and keys.

Import Trusted CA Certificate



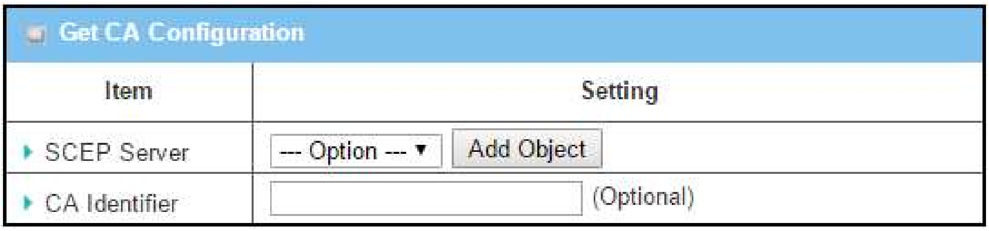
When **Import** button is applied, the **Trusted CA import** screen will appear. You can import a Trusted CA certificate from an existing certificate file, or directly paste a PEM encoded string as the certificate.


Trusted CA Certificate Import from a File
Apply
Cancel
Browse...
No file selected.
Trusted CA Certificate Import from a PEM
Apply
Cancel

Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	Required setting	Select a CA certificate file from user's computer, and click the **Apply** button to import the specified CA certificate file to the gateway.
Import from a PEM	1. String format, any text 2. Required setting	This is an alternative approach to importing a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string, and click the **Apply** button to import the specified CA certificate into the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Instead of importing a Trusted CA certificate with these approaches, you can also get the CA certificate from the SCEP server.

If **SCEP** is enabled (Refer to **Object Definition** > **Certificate** > **Configuration**), you can click **Get CA** button, a Get CA Configuration screen will appear.

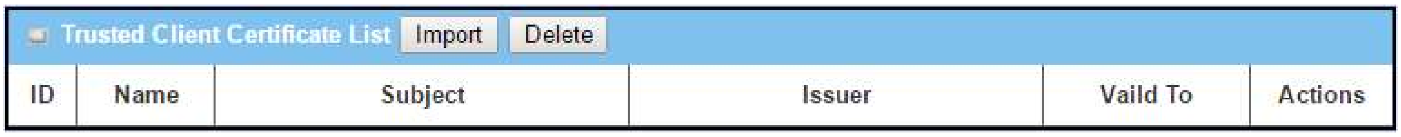


Get CA Configuration

Item	Setting
SCEP Server	--- Option --- ▾ Add Object
CA Identifier	(Optional)

Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	Required setting	Select a **SCEP Server** to identify the SCEP server for use. The server detailed information can be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. You may click **Add Object** button to generate.
CA Identifier	1. String format, any text	Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Close	N/A	Click the **Close** button to return to the Trusted Certificates page.

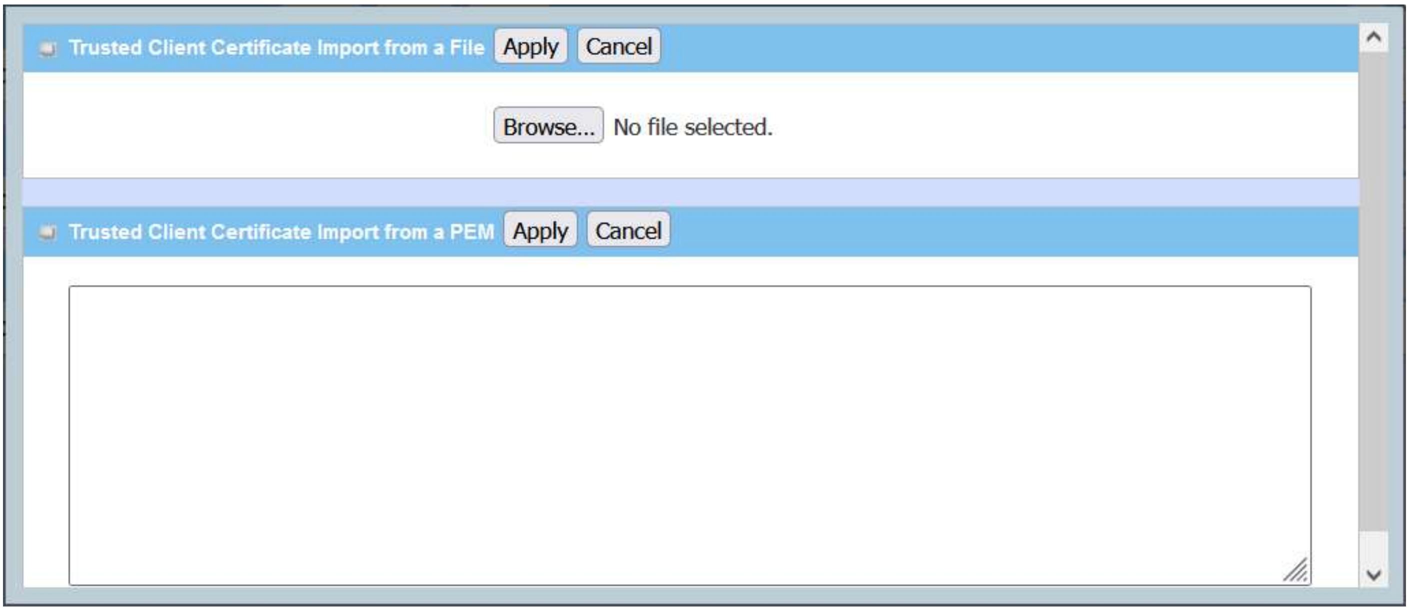
Import Trusted Client Certificate



Trusted Client Certificate List Import Delete

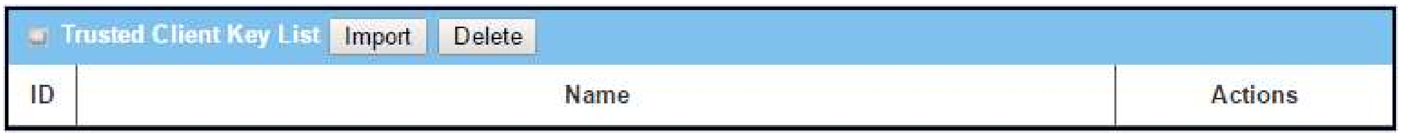
ID	Name	Subject	Issuer	Vaild To	Actions

When the **Import** button is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existing certificate file, or directly paste a PEM encoded string as the certificate.

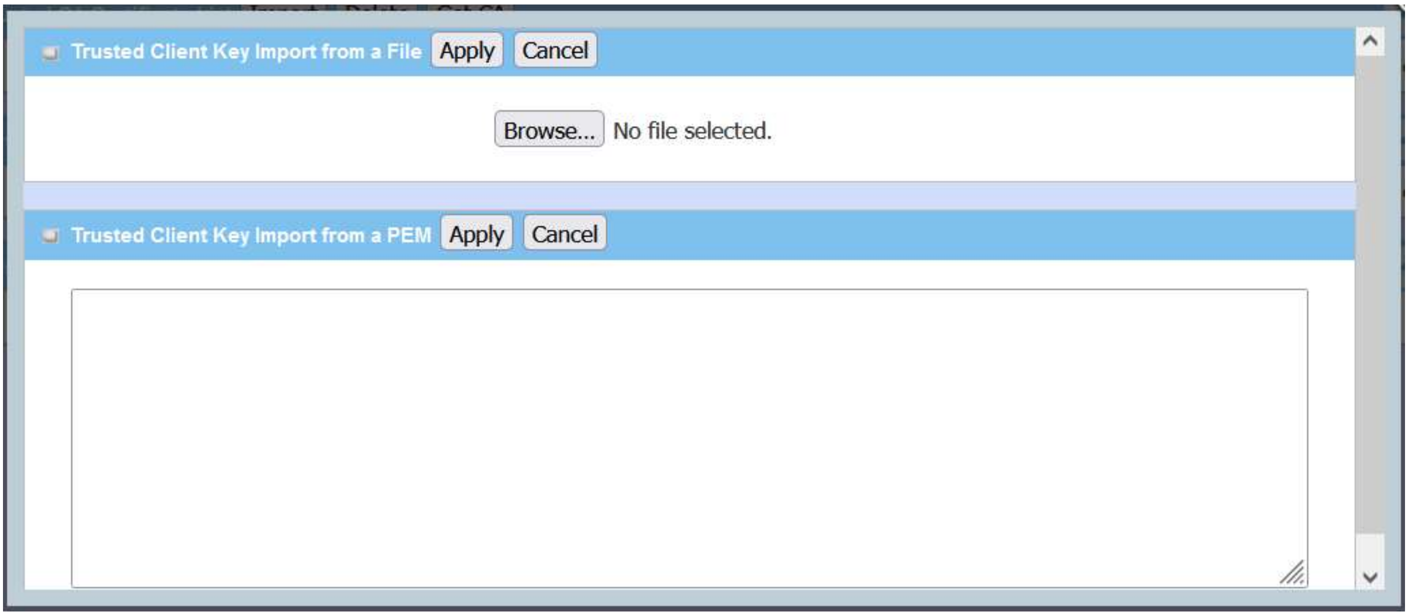

Trusted Client Certificate Import from a File
Apply
Cancel
Browse...
No file selected.
Trusted Client Certificate Import from a PEM
Apply
Cancel

Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import from a File	Required setting	Select a certificate file from a connected computer, and click the **Apply** button to import the specified certificate file to the gateway.
Import from a PEM	1. String format, any text 2. Required setting	This is an alternative approach to importing a certificate. You can directly enter (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Import Trusted Client Key



When the **Import** button is applied, the **Trusted Client Key Import** screen will appear. You can import a Trusted Client Key from an existed file, or directly paste a PEM encoded string as the key.


Trusted Client Key Import from a File
Apply
Cancel
Browse...
No file selected.
Trusted Client Key Import from a PEM
Apply
Cancel

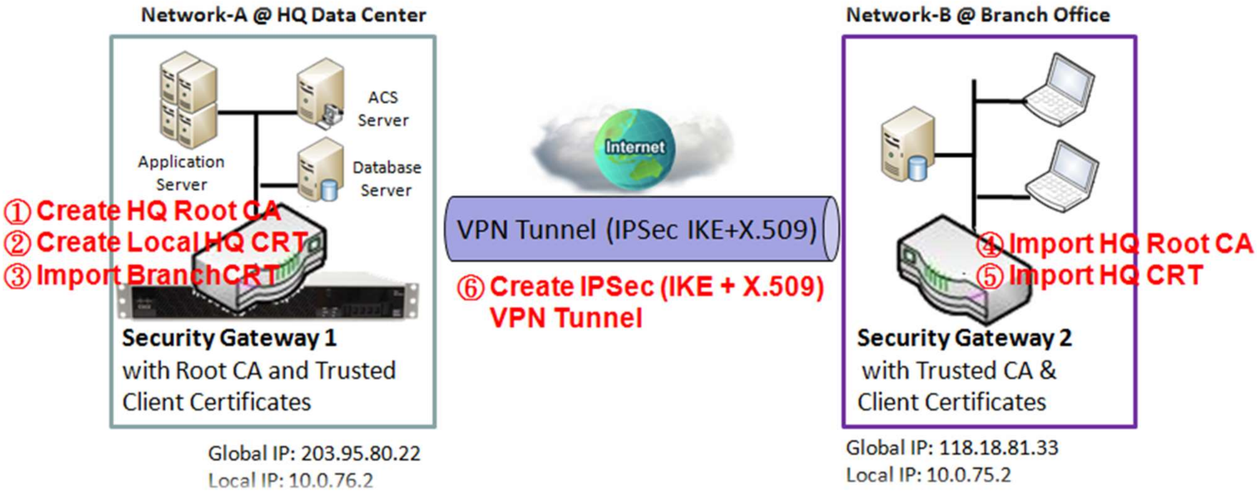
Trusted Client Key List		
Item	**Value setting**	**Description**
Import from a File	Required setting	Select a certificate key file from a connected computer, and click the **Apply** button to import the specified key file to the gateway.
Import from a PEM	1. String format, any text 2. Required setting	This is an alternative approach to importing a certificate key. You can directly enter (Copy and Paste) the PEM encoded certificate key string, and click the **Apply** button to import the specified certificate key to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate key.
Cancel	N/A	Click the **Cancel** button to discard the import operation. The screen will return to the Trusted Certificates page.

4.4.4 Issue Certificate

When you have a Certificate Signing Request (CSR) that needs to be certified by the root CA of the device, you can issue the request here and let the Root CA sign it. There are two approaches to issue a certificate. One is importing a CSR file from the managing PC and another is to copy-paste the CSR codes in gateway’s web-based utility, and then click the "Sign" button.

If the gateway signs a CSR successfully, the "Signed Certificate View" window will show the resulting certificate contents. In addition, a "Download" button will be available for downloading the certificate to a file to the managing PC.

Self-signed Certificate Usage Scenario



Scenario Application Timing (same as described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates signed by itself. It also imports trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to confirm their identity when establishing a VPN tunnel.

Scenario Description (same as described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It also imports a trusted certificate (BranchCRT) – a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it as the BranchCRT certificate. It imports the certificate into Gateway 2 as a local certificate. In addition, it also imports the certificates of the root CA of Gateway 1 into Gateway 2 as trusted ones. (Refer to "My Certificate" and "Trusted Certificate" sections).

It will establish an IPsec VPN tunnel with IKE and X.509 protocols starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example (same as described in "My Certificate" section)

For Network-A at HQ

The following tables list the parameter configuration as an example for the "Issue Certificate" function used in the user authentication of IPsec VPN tunnel establishing, as shown in the above diagram. The configuration example must be combined with the ones in "My Certificate" and "Trusted Certificate" sections to complete the setup for whole user scenario.

Configuration Path	[Issue Certificate]-[Certificate Signing Request Import from a File]
Browse	***C:/BranchCSR***
Command Button	***Sign***

Configuration Path	[Issue Certificate]-[Signed Certificate View]
Command Button	***Download*** (default name is "issued.crt")

Scenario Operation Procedure (same as the one described in "My Certificate" section)

In the above diagram, "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B in the branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. It imports the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate BranchCRT to be signed by root CA (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just download it). It takes the CSR to be signed by the root CA of Gateway 1 and obtains the BranchCRT certificate (which needs to be renamed). Import the certificate into the "Trusted Client Certificate List" of Gateway 1 and the "Local Certificate List" of Gateway 2.

Gateway 2 can establish an IPsec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

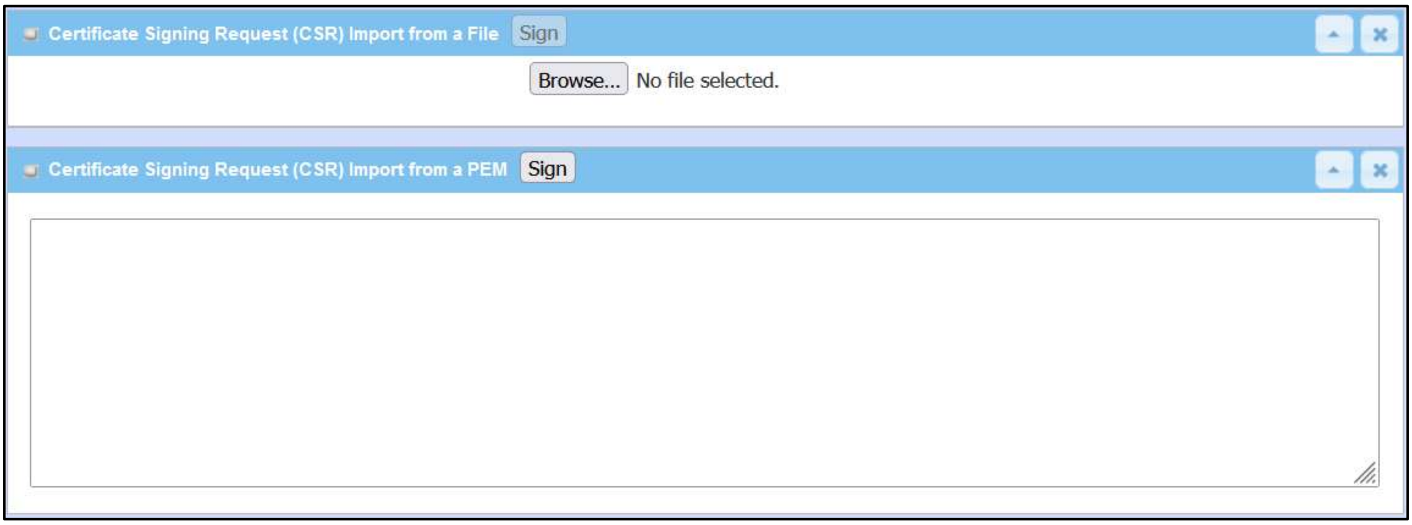
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Issue Certificate Setting

Go to Object Definition > Certificate > Issue Certificate tab.

The Issue Certificate setting allows the user to import Certificate Signing Request (CSR) to be signed by root CA.

Import and Issue Certificate

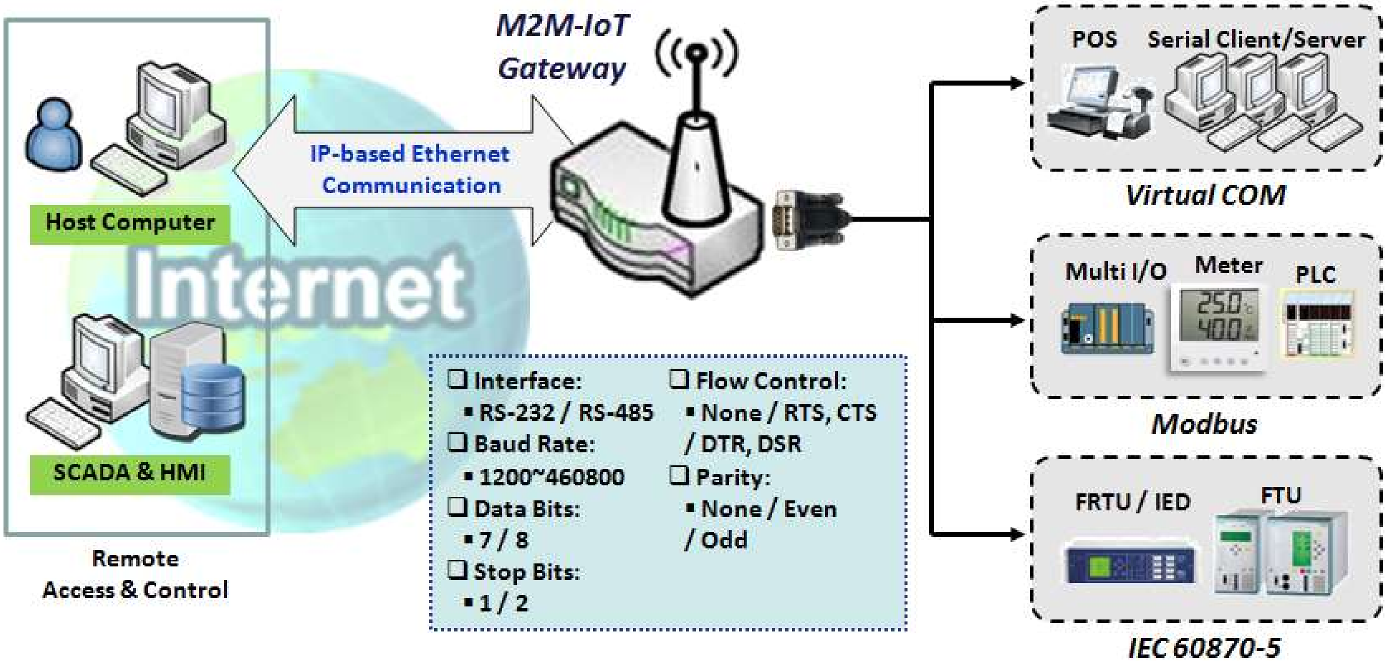

Certificate Signing Request (CSR) Import from a File
Sign
Browse...
No file selected.
Certificate Signing Request (CSR) Import from a PEM
Sign

Certificate Signing Request (CSR) Import from a File		
Item	**Value setting**	**Description**
Certificate Signing Request (CSR) Import from a File	Required setting	Select a certificate signing request file from your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format, any text 2. Required setting	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	When root CA exists, click the **Sign** button to sign and issue the imported certificate by root CA.

Chapter 5 Field Communication

5.1 Bus & Protocol

The gateway may be equipped with a serial port for serial communication by connecting an RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make allow for easy access to serial devices anywhere over a local LAN or the Internet. They can be "Virtual COM" and "Modbus".



5.1.1 Port Configuration

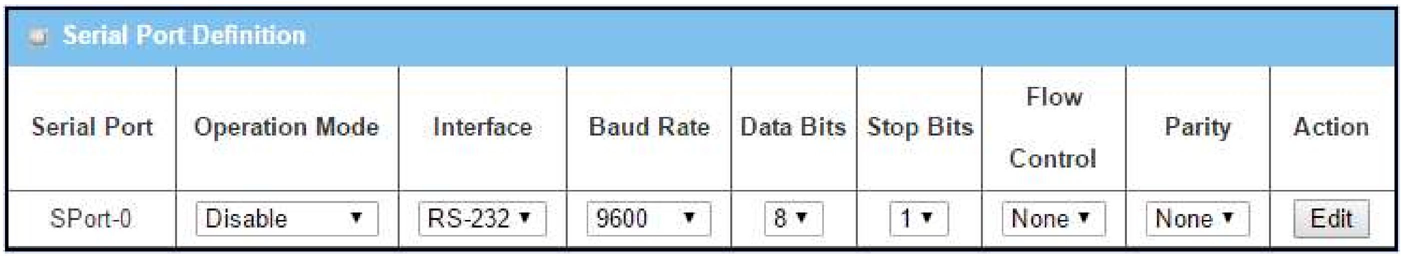
Before using the supported field communication function, like Virtual COM or Modbus, you need to configure the physical communication port first.

The port configuration screen allows user to configure the operation mode and physical layer settings for each serial interface, and also can quickly switch from one communication protocol to another for the serial port. The number of ports and type of the supported protocols will vary depending on gateway model.

Port Configuration Setting

Go to Field Communication > Bus & Protocol > Port Configuration tab.

In the "Port Configuration" page, there is only one configuration window for the serial port settings. The "Configuration" window lets you specify serial port parameters including the operation mode being "Virtual COM", "Modbus" or disabled, the interface being "RS-232" or "RS-485", the baud rate, the data bit length, the stop bit length, the flow control being "RTS/CTS", "DTS/DSR" or "None", and the parity.



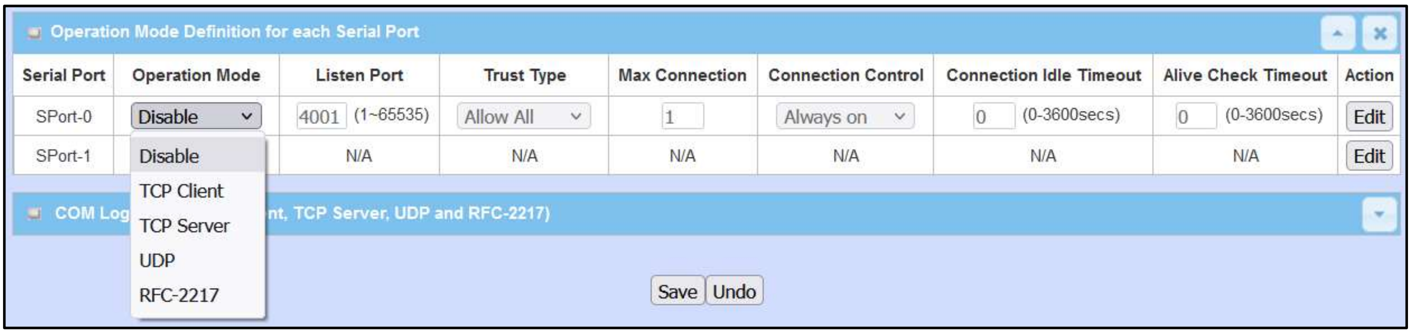
Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▼	RS-232 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	Edit

Port Configuration Window		
Item	**Value setting**	**Description**
Serial Port	*N/A*	Displays the serial port ID. The number of serial ports will vary depending on gateway model.
Operation Mode	Disable is set by default	Displays the current selected operation mode for the serial interface. Depending on the model, the available modes can be Virtual COM and Modbus.
Interface	RS-232 is set by default	Select RS-232 or RS-485 physical interface for connecting to the access device(s) with the same interface specification.
Baud Rate	19200 is set by default	Select the appropriate baud rate for serial device communication. RS-232: 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 RS-485 can use higher baud rate for 230400 and 460800. It depends on cable length and the installation environment.
Data Bits	8 is set by default	Select 8 or 7 for data bits.
Stop Bits	1 is set by default	Select 1 or 2 for stop bits.
Flow Control	None is set by default	Select None / RTS, CTS / DTS, DSR for Flow Control in RS-232 mode. Support for Flow Control depends on the model.
Parity	None is set by default	Select None / Even / Odd for Parity bit.
Action	N/A	Click **Edit** button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

5.1.2 Virtual COM

Create a virtual COM port on user's PC/Host to provide access to a serial device connected to the serial port on the gateway. This will allow access, control, and management of the connected serial device through the Internet (fixed line or cellular network). This is also known as Ethernet pass-through communication.



Operation Mode Definition for each Serial Port

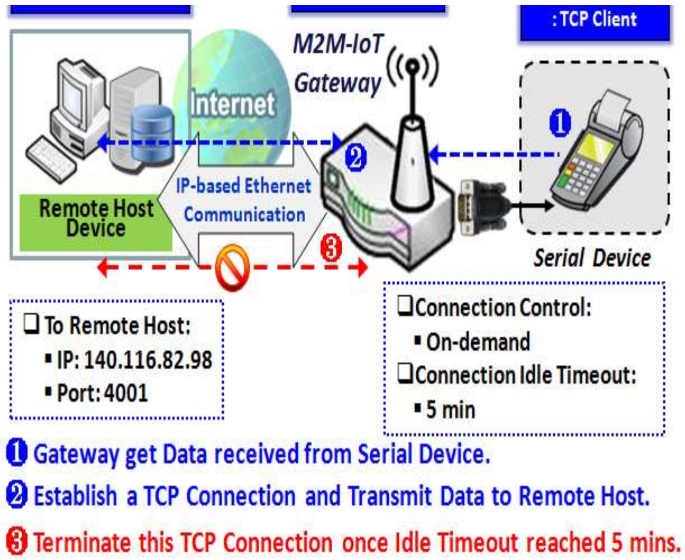
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Action
SPort-0	Disable	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)	Edit
SPort-1	Disable TCP Client TCP Server UDP RFC-2217	N/A	N/A	N/A	N/A	N/A	N/A	Edit

COM Log … nt, TCP Server, UDP and RFC-2217)

Save Undo

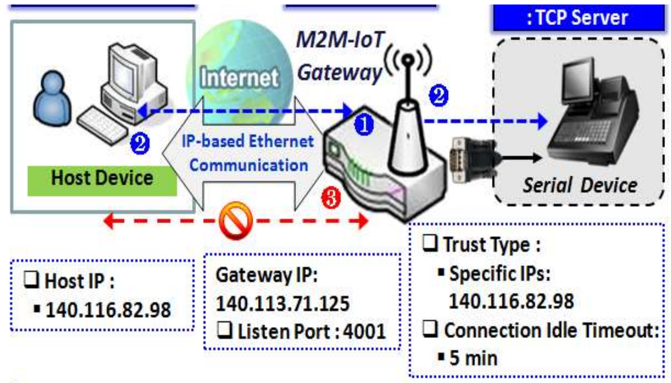
The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet, so that serial data can be accessed remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing of the connected serial device. These operation modes are illustrated below.

TCP Client Mode


:TCP Client
M2M-IoT Gateway
Internet
IP-based Ethernet Communication
Remote Host Device
Serial Device
❶
❷
❸
❑ To Remote Host:
▪ IP: 140.116.82.98
▪ Port: 4001
❑Connection Control:
▪ On-demand
❑Connection Idle Timeout:
▪ 5 min
❶ Gateway get Data received from Serial Device.
❷ Establish a TCP Connection and Transmit Data to Remote Host.
❸ Terminate this TCP Connection once Idle Timeout reached 5 mins.

When the administrator expects the gateway to actively establish a TCP connection to a pre-defined host computer when serial data arrives, the operation mode for the "Virtual COM" function is required to be "TCP Client" and when the connection control of virtual COM is "On-demand", once the gateway receives data from the connected serial device, it will establish a TCP connection to transfer the received serial data to the remote host. After the data has been transferred, the gateway automatically disconnects the established TCP session from the host computer by using the TCP alive check timeout or idle timeout settings.

TCP Server Mode



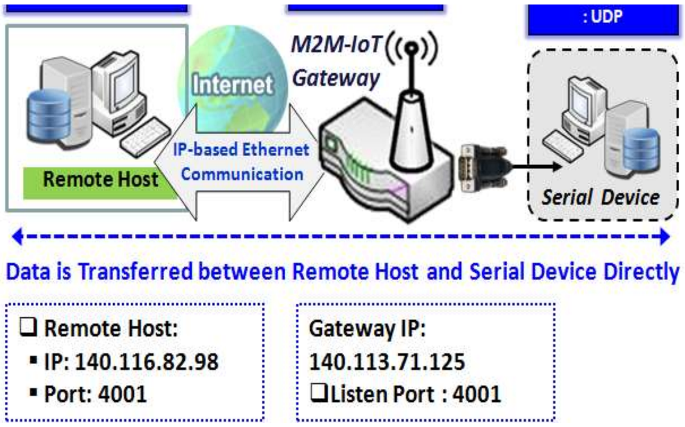
❶ Gateway remain Listening and Host will Establish a TCP Connection with it.

❷ Host Send Data then Gateway Transmit it to the Serial Device.

❸ Terminate this TCP Connection once Idle Timeout reached 5 mins.

When the administrator expects the gateway to wait passively for the serial data requests from the Host Device, and the Host will establish a TCP connection to get data from the serial device, the operation mode for the "Virtual COM" function is required to be "TCP Server". In this mode, the gateway provides a unique "IP: Port" address on a TCP/IP network. It supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time. After the data has been transferred, the TCP connection will be automatically disconnected from the host computer by using the TCP alive check timeout or idle timeout settings.

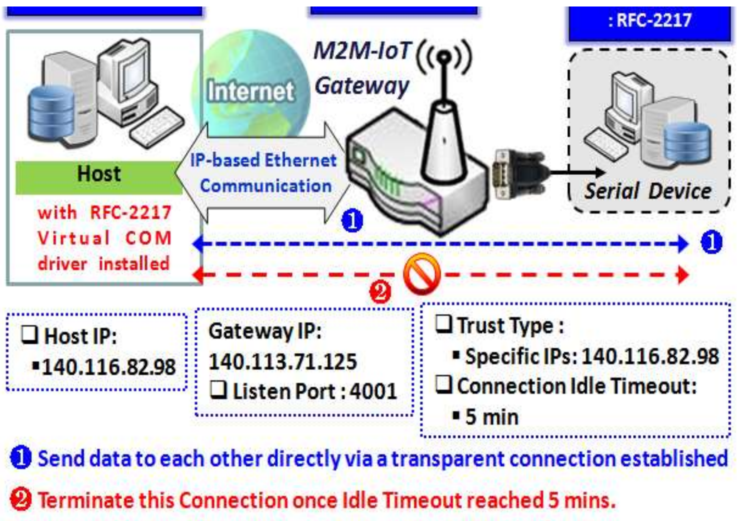
UDP Mode



If both the Remote Host Computer and the serial device are expected to initiate a data transfer when required, the operation mode for the "Virtual COM" function in the gateway is required to be "UDP". In this mode, the UDP data can be transferred between the gateway and multiple host computers from either peer, making this mode ideal for message display applications.

The remote host computer can directly send UDP data to the serial device via the gateway, and also receive UDP data from the serial device via the gateway at the same time. The gateway supports up to 4 legal hosts to connect simultaneously to the serial device via the gateway.

RFC-2217 Mode


: RFC-2217
Internet
M2M-IoT
Gateway
Serial Device
Host
with RFC-2217 Virtual COM driver installed
IP-based Ethernet Communication
❶
❷

❑ Host IP:
▪140.116.82.98

Gateway IP:
140.113.71.125
❑ Listen Port : 4001

❑ Trust Type :
▪ Specific IPs: 140.116.82.98
❑ Connection Idle Timeout:
▪ 5 min

❶ Send data to each other directly via a transparent connection established

❷ Terminate this Connection once Idle Timeout reached 5 mins.

RFC-2217 defines general COM port control options based on the Telnet protocol. A host computer with RFC-2217 driver installed can monitor and manage the remote serial device attached to the gateway's serial port as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the host computers to establish connection with.

Any 3rd party driver supporting RFC-2217 can be installed in the host computer. The driver establishes a transparent connection between host and serial device by mapping the IP:Port of the gateway's serial port to a virtual local COM port on the host computer.

The host computer can directly send data to the serial device via the gateway, and also receive data from the serial device via the gateway at the same time. The gateway supports up to 4 Internet host computers.

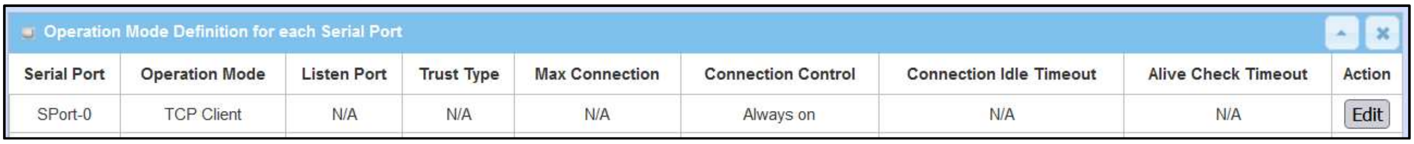
Virtual COM Setting

The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet, allowing users to access serial data remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device. By default, it is configured in Disable mode.

To use the Virtual COM function, specify the operation mode for the multi-function serial port first. Go to **Field Communication > Bus & Protocol > Port Configuration** tab, select the Virtual COM as the operation mode, and finish the related port configuration.
After that, go to **Field Communication > Bus & Protocol > Virtual COM** tab for detailed configuration of Virtual COM setting.

Enable TCP Client Mode

Configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, device initiates a TCP connection with a TCP server when there is data to transmit. The device disconnects from the server when the connection is Idle for a specified period. You can also enable full time connection with the TCP server.

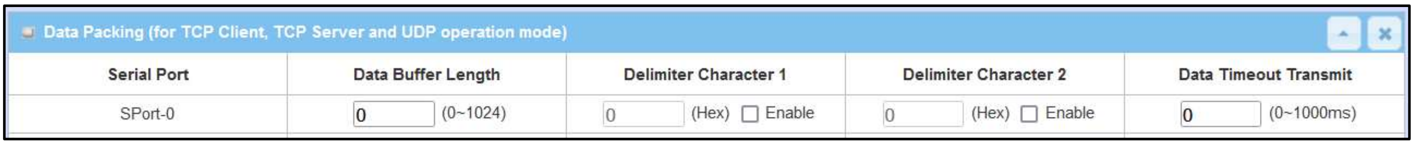


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Action
SPort-0	TCP Client	N/A	N/A	N/A	Always on	N/A	N/A	Edit

Enable TCP Client Mode Window		
Item	**Value setting**	**Description**
Operation Mode	Required setting	Select **TCP Client**.
Connection Control	**Always on** is set by default	Choose **Always on** for a TCP full time connection. Otherwise, choose **On-Demand** to initiate TCP connection only when required to transmit, and to disconnect at idle timeout.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 60 min.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when the idle time has elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. **Value Range:** 0 ~ 3600 seconds.
Alive Check Timeout	1. 0 is set by default 2. Range 0 to 60 min.	Enter the time period of alive-check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. **Value Range:** 0 ~ 3600 seconds.
Save	*N/A*	Click the **Save** button to save the configuration

Specify Data Packing Parameters

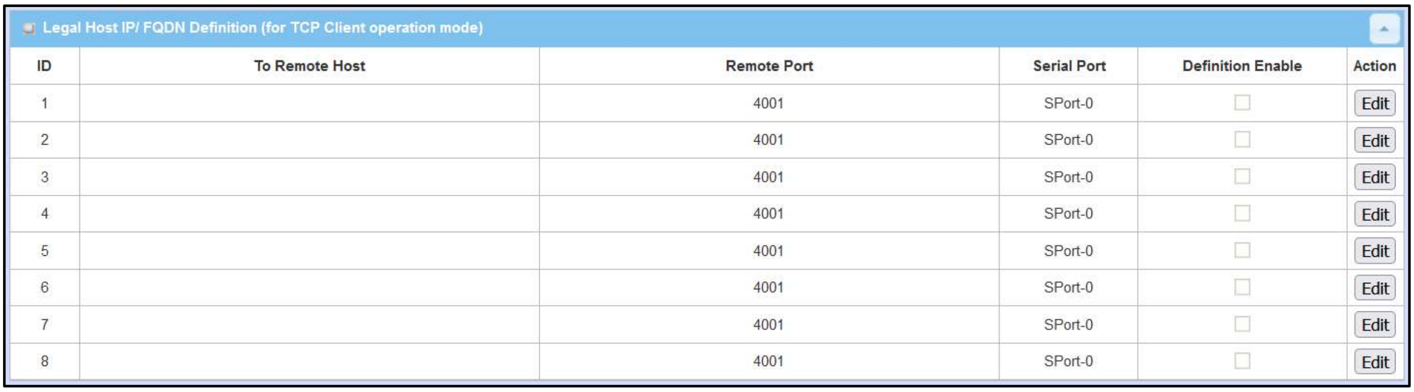


Data Packing (for TCP Client, TCP Server and UDP operation mode)

Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	0 (0~1024)	0 (Hex) □ Enable	0 (Hex) □ Enable	0 (0~1000ms)

Data Packing Configuration		
Item	**Value setting**	**Description**
Data Buffer Length	1. Optional setting 2. Default value is 0	Enter the data buffer length for the serial port. ***Value Range***: 0 ~ 1024.
Delimiter Character 1	1. Optional setting 2. Default value is 0	Check the **Enable** box to activate the Delimiter character 1, and enter the Hex code for it. ***Value Range***: 0x00 ~ 0xFF.
Delimiter Character 2	1. Optional setting 2. Default value is 0	Check the **Enable** box to activate the Delimiter character 2, and enter the Hex code for it. ***Value Range***: 0x00 ~ 0xFF.
Data Timeout Transmit	1. Optional setting 2. Default value is 0	Enter the data timeout interval for transmitting serial data through the port. By default, it is set to 0 and the timeout function is disabled. ***Value Range***: 0 ~ 1000ms.
Save	*N/A*	Click the **Save** button to save the configuration

Specify Remote TCP Server



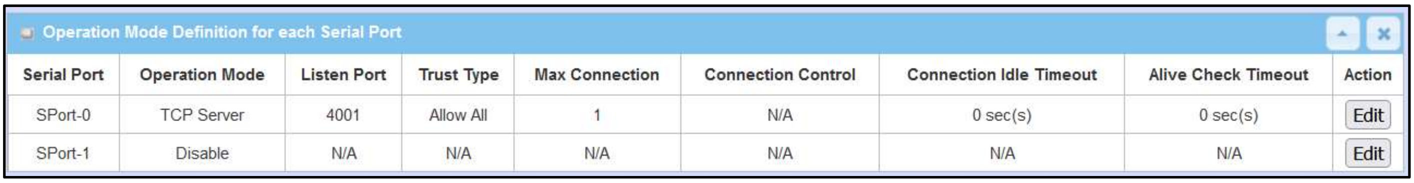
Legal Host IP/ FQDN Definition (for TCP Client operation mode)

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit
5		4001	SPort-0	□	Edit
6		4001	SPort-0	□	Edit
7		4001	SPort-0	□	Edit
8		4001	SPort-0	□	Edit

Specify TCP Server Window		
Item	**Value setting**	**Description**
To Remote Host	Required setting	Press **Edit** button to enter IP address or FQDN of the remote TCP server to transmit serial data.
Remote Port	1. Required setting 2. Default value is 4001	Enter the TCP port number. This is the listening port of the remote TCP server. ***Value Range***: 1 ~ 65535.
Serial Port	SPort-0 is set by default	Apply the TCP server connection for a selected serial port. Up to 4 TCP servers can be configured at the same time for each serial port.
Definition Enable	Unchecked by default	Check the **Enable** box to enable the TCP server configuration.
Save	*N/A*	Click the **Save** button to save the configuration

Enable TCP Server Mode

Configure the gateway as a TCP (Transmission Control Protocol) Server. The TCP Server waits for connections to be initiated by a remote TCP client device to receive serial data. The setting allows user to specify specific TCP clients or allow any to send serial data for serial data transmission bandwidth control and access control. The TCP Server supports up to 128 simultaneous connections to receive serial data from multiple TCP clients.



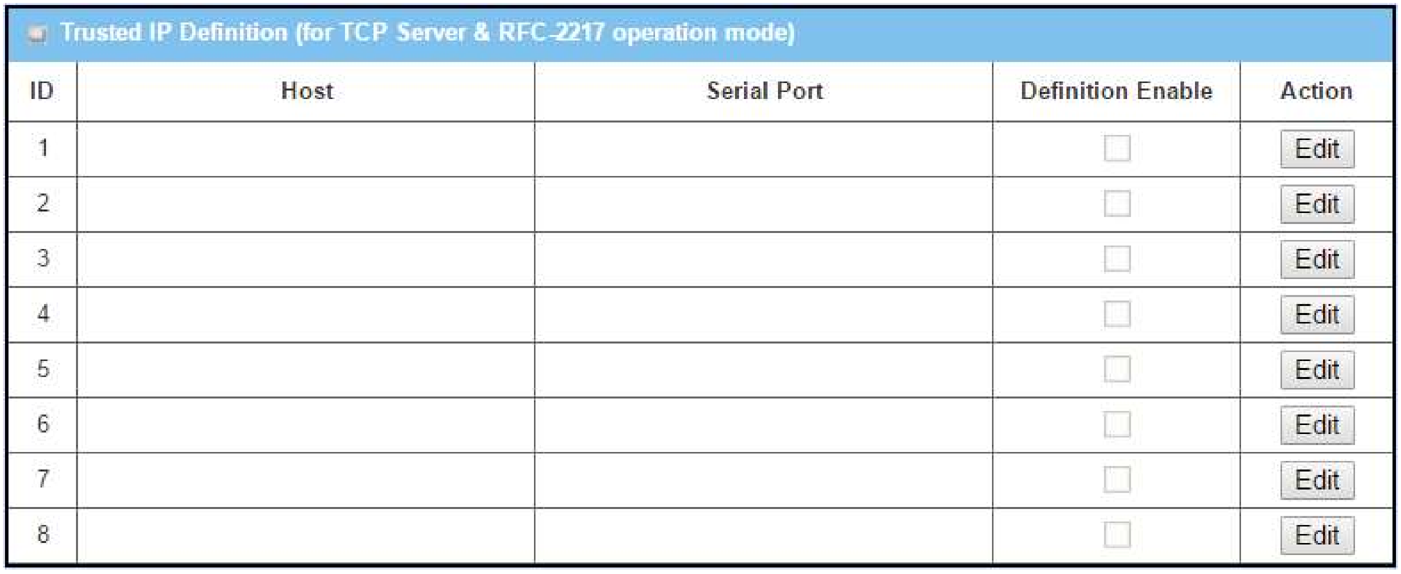
Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Action
SPort-0	TCP Server	4001	Allow All	1	N/A	0 sec(s)	0 sec(s)	Edit
SPort-1	Disable	N/A	N/A	N/A	N/A	N/A	N/A	Edit

Enable TCP Server Mode Window Item	Value setting	Description
Operation Mode	Required setting	Select **TCP Server** mode.
Listen Port	4001 is set by default	Indicate the listening port of the TCP connection. ***<u>Value Range</u>***: 1 ~ 65535.
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any TCP clients to connect. Otherwise choose **Specific IP** to limit certain TCP clients.
Max Connection	1. Max. 4 connections 2. 1 is set by default	Set the maximum number of concurrent TCP connections. Up to 4 simultaneous TCP connections can be established. ***<u>Value Range</u>***: 1 ~ 128.
Connection Idle Timeout	0 is set by default	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when the idle time has elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***<u>Value Range</u>***: 0 ~ 3600 seconds.
Alive Check Timeout	0 is set by default	Input the time period of alive-check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***<u>Value Range</u>***: 0 ~ 3600 seconds.
Enable	Unchecked by default	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	*N/A*	Click **Save** button to save the settings.

Specify TCP Clients for TCP Server Access

If you selected Specific IPs as the trust Type, the Trusted IP Definition window appears. The settings are valid for both TCP Server and RFC-2217 modes.



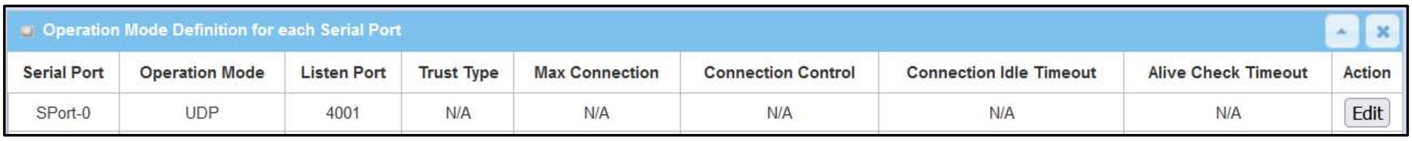
Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1			□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Specify TCP Clients Window		
Item	**Value setting**	**Description**
Host	Required setting	Enter the IP address range of allowed TCP clients.
Serial Port	Unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	Unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Enable UDP Mode

UDP (User Datagram Protocol) enables applications using UDP socket programs to communicate with the serial ports on the serial server. The UDP mode provides connectionless communications, which enable you to multicast data from the serial device to multiple host computers, and vice versa, making this mode ideal for message display applications.

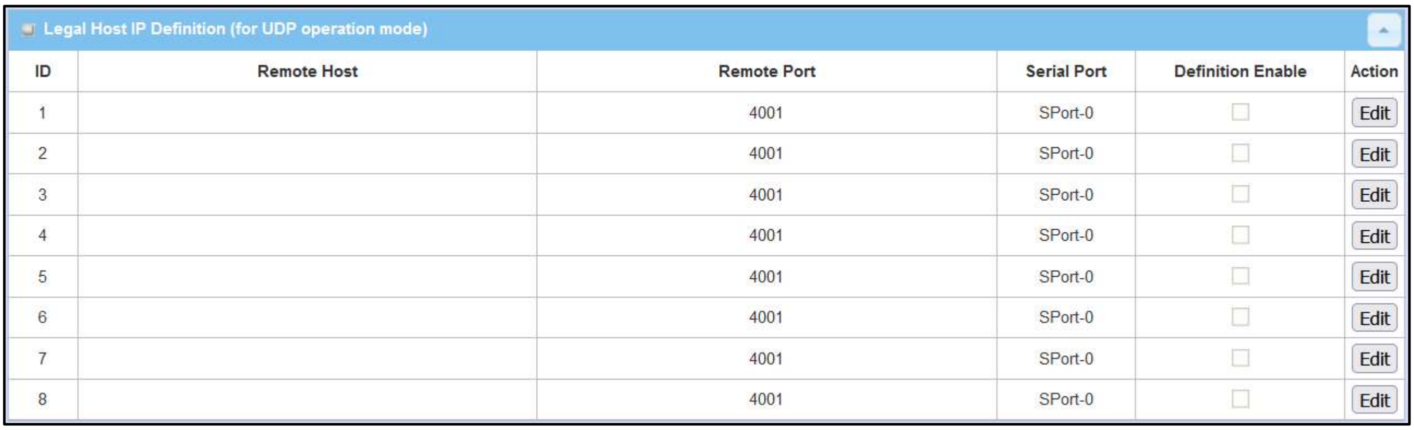


Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Action
SPort-0	UDP	4001	N/A	N/A	N/A	N/A	N/A	Edit

Enable UDP Mode Window		
Item	**Value setting**	**Description**
Operation Mode	Required setting	Select **UDP** mode.
Listen Port	4001 is set by default	Indicate the listening port of UDP connection. ***Value Range***: 1 ~ 65535
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Specify Remote UDP



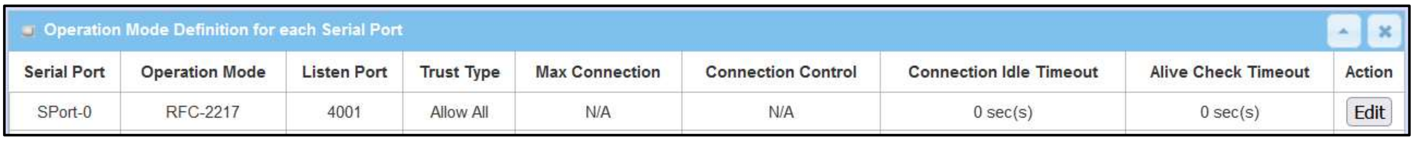
Legal Host IP Definition (for UDP operation mode)

ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit
5		4001	SPort-0	□	Edit
6		4001	SPort-0	□	Edit
7		4001	SPort-0	□	Edit
8		4001	SPort-0	□	Edit

Specify Remote UDP hosts Window		
Item	**Value setting**	**Description**
Host	Required setting	Press **Edit** button to enter IP address range of remote UDP hosts.
Remote Port	4001 is set by default	Indicate the UDP port of peer UDP hosts. ***Value Range***: 1 ~ 65535
Serial Port	SPort-0 is set by default	Apply the UDP hosts for a selected serial port. Up to 4 UDP servers can be configured at the same time for each serial port.
Definition Enable	Unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Enable RFC-2217 Mode

RFC-2217 defines general COM port control options based on the Telnet protocol. With the RFC-2217 mode, a remote host can monitor and manage remote serially attached devices as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the remote hosts to establish connection with.



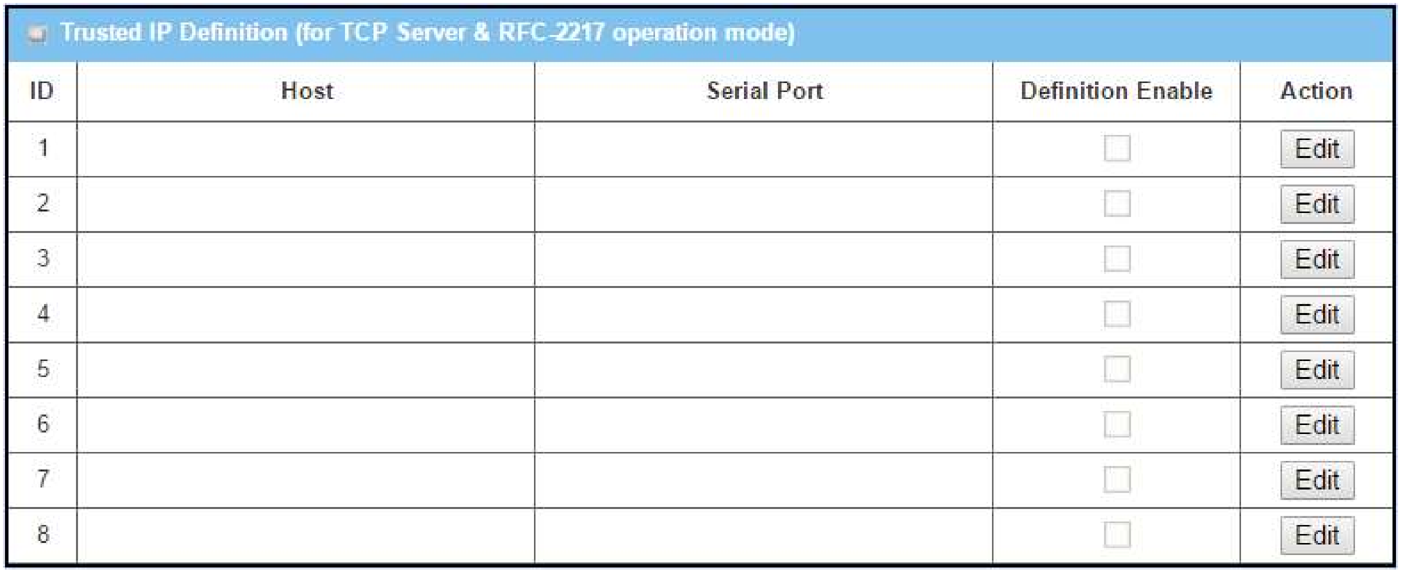
Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Action
SPort-0	RFC-2217	4001	Allow All	N/A	N/A	0 sec(s)	0 sec(s)	Edit

Enable RFC-2217 Mode Window Item	 Value setting	 Description
Operation Mode	Required setting	Select **RFC-2217** mode.
Listen Port	4001 is set by default	Indicate the listening port of RFC-2217 connection. ***Value Range***: 1 ~ 65535
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any clients to connect. Otherwise choose **Specific IP** to limit certain clients.
Connection Idle Timeout	0 is set by default	Enter the idle timeout in minutes. The idle timeout is used to disconnect the connection when the idle time has elapsed. Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***Value Range***: 0 ~ 3600 seconds.
Alive Check Timeout	0 is set by default	Input the time period of alive-check timeout. The connection will be terminated if no response time of alive-check is longer than this timeout setting. Alive check timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***Value Range***: 0 ~ 3600 seconds.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Specify Remote Host for Access

If you selected Specific IPs as the trust Type, the Trusted IP Definition window appears. The settings are valid for both TCP Server and RFC-2217 modes.



Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

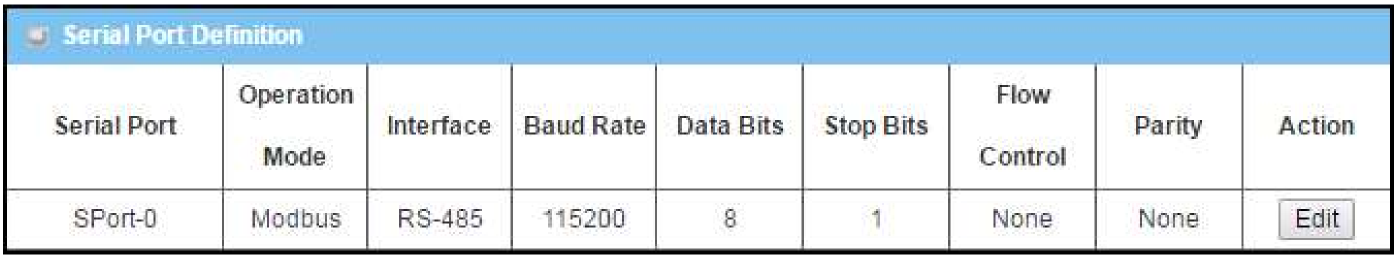
ID	Host	Serial Port	Definition Enable	Action
1			□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Specify RFC-2217 Clients for Access Window		
Item	**Value setting**	**Description**
Host	Required setting	Enter the IP address range of allowed clients.
Serial Port	Unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	Unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

5.1.3 Modbus

Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters use the Modbus protocol as the communication standard. It is used to establish master-slave communication between intelligent devices.

However, the Ethernet-based Modbus protocol is different from the original serial-based protocols. In order to integrate Modbus networks, the IoT Gateway, including one or more serial ports that support RS-232 and RS-485 communication interface, can automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus RTU/ASCII (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming or effort.

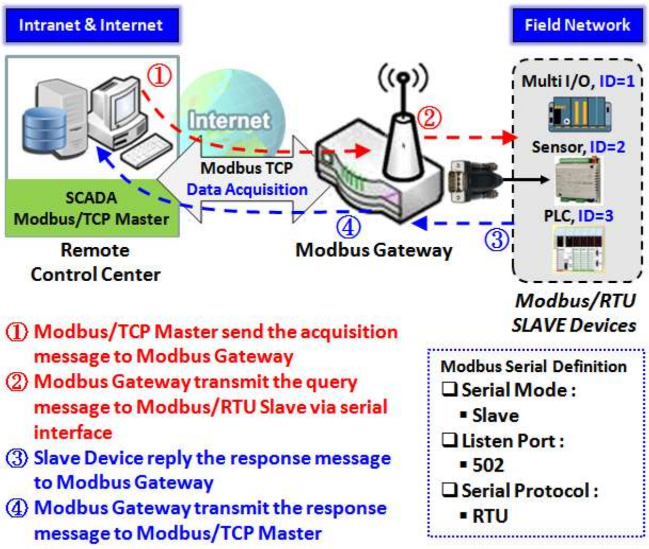


Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Modbus	RS-485	115200	8	1	None	None	Edit

NOTE: When Modbus devices are connected to/under the same serial port of IoT Modbus Gateway, those Modbus devices must use the same protocol with the same configuration (i.e., either Modbus RTU or Modbus ASCII with same Baud Rate setting).

Modbus Gateway Scenario



① Modbus/TCP Master send the acquisition message to Modbus Gateway
② Modbus Gateway transmit the query message to Modbus/RTU Slave via serial interface
③ Slave Device reply the response message to Modbus Gateway
④ Modbus Gateway transmit the response message to Modbus/TCP Master

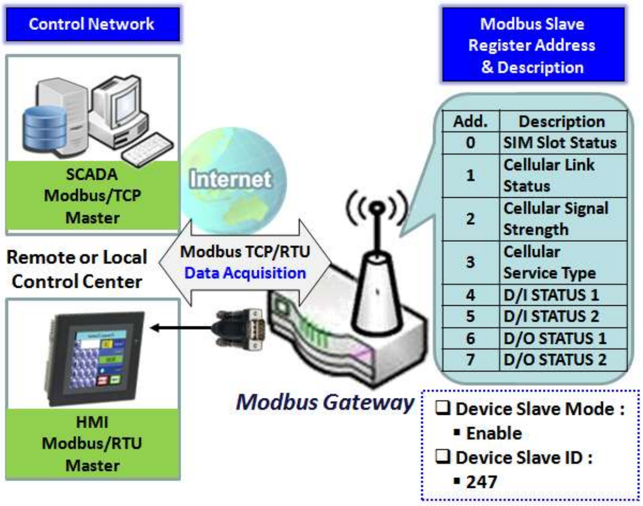
Modbus Serial Definition
❑ Serial Mode :
▪ Slave
❑ Listen Port :
▪ 502
❑ Serial Protocol :
▪ RTU

The IoT Gateway serves as a Modbus gateway to communicate with the Modbus TCP Master, the SCADA Server, located at a remote control center for Modbus device accessing.

The Modbus TCP Master requests the IoT Gateway to provide the Modbus devices' information, e.g., Data Acquisition or Register/Value Modification, via general Internet access, and the IoT Gateway serves as the gateway for data forwarding.

Under such configuration, the Modbus TCP Master requests the information from, or sends control commands to various Modbus/RTU Slave devices attached to the Modbus Gateway. The Modbus gateway executes corresponding processes and replies the Modbus/TCP Master with the results.

Modbus Slave Scenario



Add.	Description
0	SIM Slot Status
1	Cellular Link Status
2	Cellular Signal Strength
3	Cellular Service Type
4	D/I STATUS 1
5	D/I STATUS 2
6	D/O STATUS 1
7	D/O STATUS 2

❑ Device Slave Mode :
- Enable

❑ Device Slave ID :
- 247

In addition to behaving as a Modbus Gateway, there is an integrated Modbus Slave option for providing device status, such as Cellular Network and DI/DO status, to remote Modbus Master via Modbus communication.

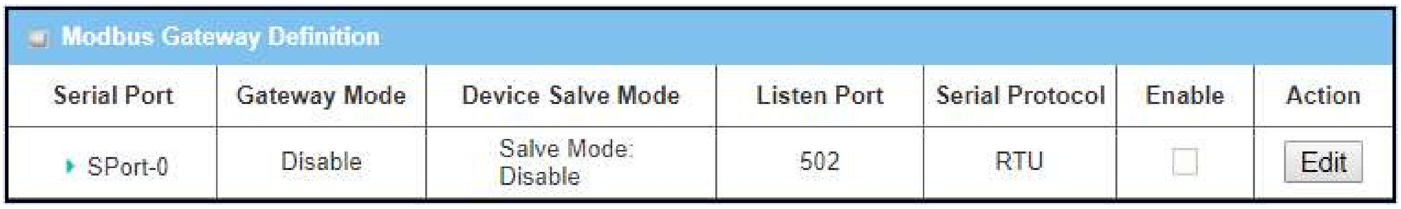
With the Slave option enabled, the Modbus Master device can request the information or send control commands to the IoT Gateway, the Modbus TCP/RTU Slave device. The IoT Gateway executes corresponding processes and replies to the Modbus Master devices.

Modbus Setting

Go to Field Communication > Bus & Protocol > Modbus tab.

The Modbus setting page enables user to configure the gateway to operate as a Modbus gateway, and allow access among Modbus TCP devices (which are connected to Ethernet network) and Modbus RTU/ASCII devices (which are connected to the Serial Port of the gateway). Once you have completed the Modbus settings in this section, select Modbus Operation Mode in the Port Configuration screen.

Define Modbus Gateway function for each Serial Port

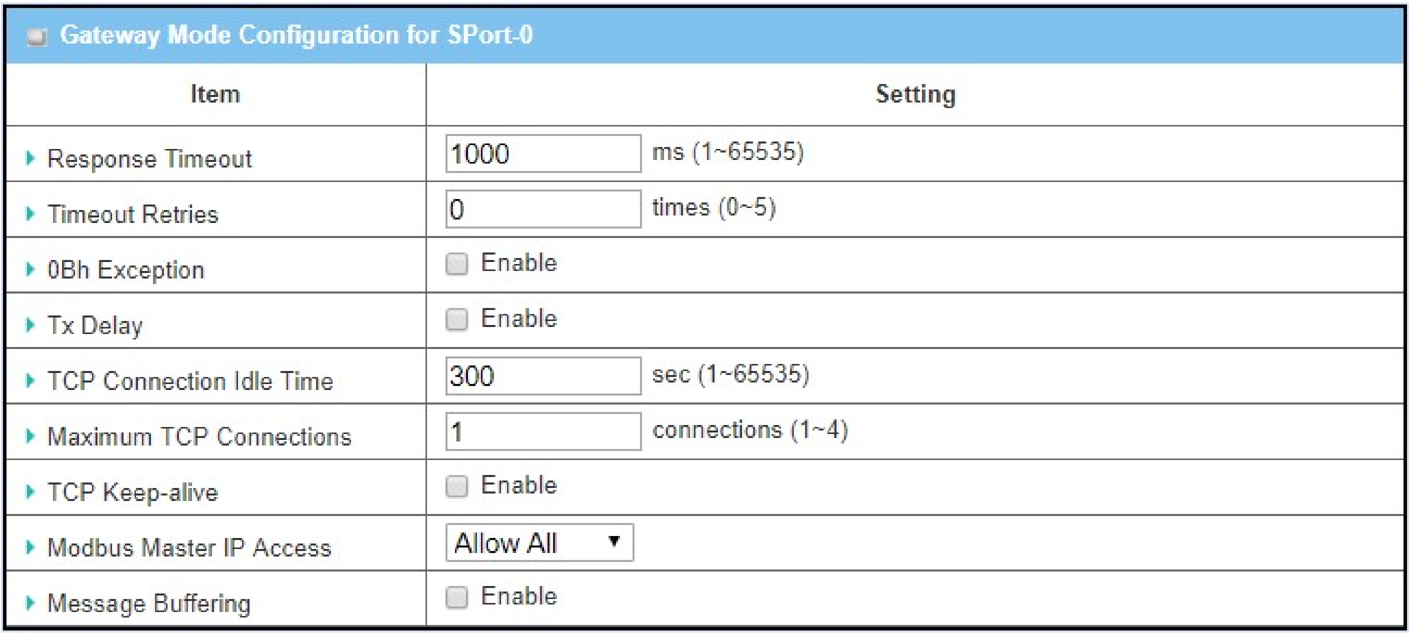


Modbus Gateway Definition

Serial Port	Gateway Mode	Device Salve Mode	Listen Port	Serial Protocol	Enable	Action
SPort-0	Disable	Salve Mode: Disable	502	RTU	□	Edit

Modbus Gateway Definition Item	Value setting	Description
Serial Port	N/A	Displays the name of the serial port used. E.g. SPort-0. The number of serial ports varies by model.
Gateway Mode	**Disable** is set by default	Specify the Modbus gateway mode for the selected serial port. It can be Disable, Serial as Slave or Serial as Master. A serial port can be attached with one Modbus Master, or daisy-chained in a group of Modbus Slave devices. **Disable**: Disable the Modbus gateway function for the selected serial port. **Serial as Slave**: For when attached serial device(s) are all Modbus Slave devices. **Serial as Master**: When the attached serial device is a Modbus Master device.
Device Slave Mode	Unchecked by default	Check the **Enable** box to activate the integrated Modbus Slave function, and enter the preferred ID for the integrated Modbus slave. It can function as a Modbus Slave device, and can be accessed with legacy Modbus Function Code from a SCADA management system. Supported Modbus commands are listed in the following Table. Value Range: 1 ~ 247.
Listen Port	1. **502** is set by default 2. Range 1 to 65535	Specify the Listening Port number if Slave device(s) is/are attached to the selected serial port. This setting is unneeded if a Master device is attached. *Value Range*: 1 ~ 65535. Note: Use different port numbers for the serial ports for products with multiple serial ports.
Serial Protocol	**RTU** is set by default	Select the serial protocol that is adopted by the attached Modbus device(s). It can be **RTU** or **ASCII**.
Enable	N/A	Displays whether the specific Modbus serial port is enabled or disabled. To enable or disable Modbus serial port, go to **Field Communication > Bus & Protocol > Port Configuration** tab, and set the operation mode as **Modbus**.

Specify Gateway Configuration



Gateway Mode Configuration for SPort-0

Item	Setting
Response Timeout	1000 ms (1~65535)
Timeout Retries	0 times (0~5)
0Bh Exception	□ Enable
Tx Delay	□ Enable
TCP Connection Idle Time	300 sec (1~65535)
Maximum TCP Connections	1 connections (1~4)
TCP Keep-alive	□ Enable
Modbus Master IP Access	Allow All ▾
Message Buffering	□ Enable

Gateway Mode Configuration for SPort-n		
Item	**Value setting**	**Description**
Response Timeout	**1000 ms** is set by default	Sets the response timeout of the slave after master request is sent. If the slave does not respond within the specified time, data will be discarded. This applies to the serially attached Master sent requests over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. ***Value Range***: 1 ~ 65535.
Timeout Retries	**0** is set by default	If the slave does not respond to the Master's request, the gateway will resend the request stored in the buffer. If Timeout retries is set to null (value zero), the gateway will not buffer Master requests. If a value other than zero is specified, the gateway will store the Master request in the buffer and retry sending the request the number of specified times. Once the retries are exhausted, the gateway will send a Modbus error message to the Master. However, if the 0Bh exception box is checked (see below), a 0Bh hex code based-error message will be send instead. Value Range: 0 ~ 5.
0Bh Exception	Unchecked by default	Check the **Enable** box to enable gateway to send a 0Bh exception code message to Modbus Master to indicate that the slave device did not respond within the timeout interval.
Tx Delay	Unchecked by default	Check the **Enable** box to activate the minimum amount of time after receiving a response before the next message can be sent out. When Tx Delay is enabled the Gateway will insert a Tx delay between Master requests. The delay gives sufficient time for the slave devices to turn their transmitters off and their receivers back on.

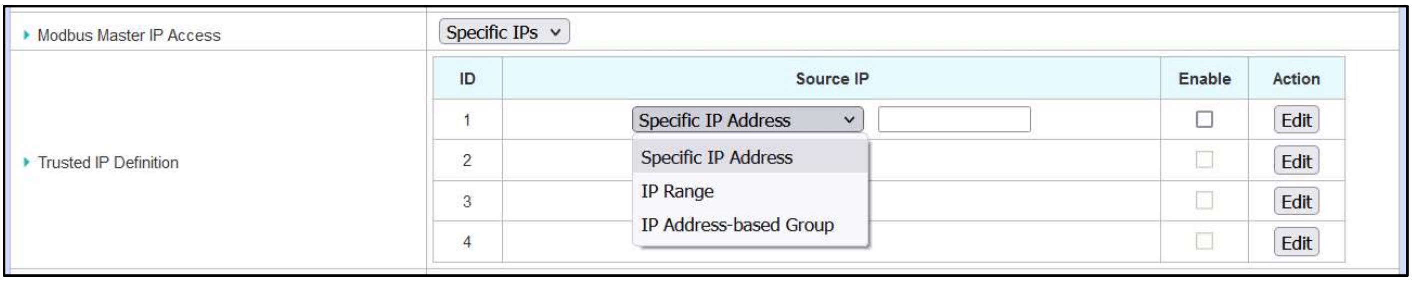
Setup TCP/IP Connection for Receiving Modbus Master Request

The following Modbus TCP Configuration items allow user to set up the TCP connection so that the remote Modbus Master can access the Modbus gateway. It also allows user to specify authorized masters on the TCP network.

Item	Value setting	Description
TCP Connection Idle Time	1. **300** is set by default 2. Range 1 to 65535	Enter the idle timeout in seconds. If the gateway does not receive another TCP request before the idle timeout has elapsed, the TCP session will be terminated automatically. *Value Range*: 1 ~ 65535.
Maximum TCP Connections	1. 4 is set by default 2. Range 1 to 4	Enter the maximum number of allowed simultaneous TCP connections. Value Range: 1 ~ 4.
TCP Keep-alive	Unchecked by default	Check the **Enable** box to ensure to keep the TCP session connected.
Modbus Master IP Access	**Allow All** is selected by default.	Specify authorized masters on the TCP network. Select **Allow All** to allow any Modbus Master to reach the attached Slave(s). Otherwise, limit only specific Master to reach the Slave(s) by selecting **Specific IPs**. When **Specific IPs** is selected, a Trusted IP Definition dialog will appear.

Specify Trusted Modbus Masters on the TCP network

When **Specific IPs** is selected, user must specify the Master(s) by their IP addresses to reach the serially attached Slave(s).



Modbus Master IP Access: Specific IPs

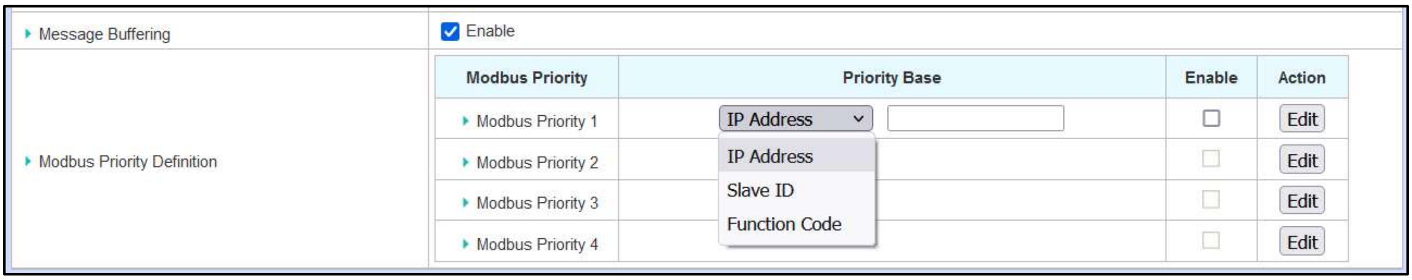
Trusted IP Definition

ID	Source IP	Enable	Action
1	Specific IP Address	□	Edit
2		□	Edit
3		□	Edit
4		□	Edit

Item	Value setting	Description
Source IP	Required setting	Select **Specific IP Address** to only allow an IP address of the allowed Master to access the attached Slave(s). Select **IP Range** to only allow a set range of IP addresses of the allowed Master to access the attached Slave(s). Select **IP Address-based Group** to only allow pre-defined group of IP address of the allowed Master to access the attached Slave(s). Note: group must be pre-defined before this selection becomes available. Refer to **Object Definition > Grouping > Host grouping**. You may also access group creation through the Add Rule shortcut button. Settings configured through the Add Rule button will also appear in the Host grouping setting screen. Check the **Enable** box to enable this rule.
Enable	Unchecked by default	Check the **Enable** box to enable this rule.

Modbus Priority Definition

Message Buffering must be enabled to prioritize Master request queue to transmit to Modbus Slave as mentioned above. Click the **Edit** button to fill in the priority settings.



Message Buffering: ☑ Enable

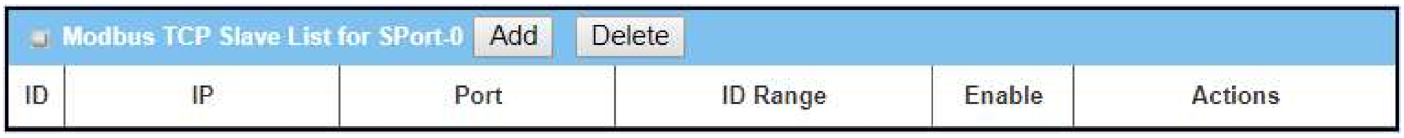
Modbus Priority Definition

Modbus Priority	Priority Base	Enable	Action
Modbus Priority 1	IP Address	□	Edit
Modbus Priority 2		□	Edit
Modbus Priority 3		□	Edit
Modbus Priority 4		□	Edit

Item	Value setting	Description
Message Buffering	1. Unchecked by default 2. Buffer up to 32 requests	Check the **Enable** box to buffer up to 32 requests from Modbus Master. If the **Enable** box is checked, a Modbus Priority Definition dialog will appear. Then the buffered Master requests can be further configured to prioritize the request queue to transmit to Slave based on Master's IP address if requests are coming from remote Master, or based on remote Slave ID if requests are coming from serially attached Master, or based on Function Code.
Modbus Priority	N/A	A Priority List for setting the priority of specified Modbus identity. Modbus Priority 1 ~ Modbus Priority 4.
Priority Base	IP Address by Default	Specify a Modbus identity with **IP Address**, **Slave ID**, or **Function Code**. The buffered Modbus message that matches the specified identity will be handled with given priority. The Modbus Master requests can be buffered to a certain priority queue according to the Master's IP address if requests are coming from remote Master, or the remote Slave's device ID if requests are coming from serially attached Master, or the specific Function Code that is issued by the Master.
Enable	Unchecked by default	Check the **Enable** box to enable the priority settings.
Save	N/A	Click the **Save** button to save the settings.

Specify Modbus TCP Slave device(s)

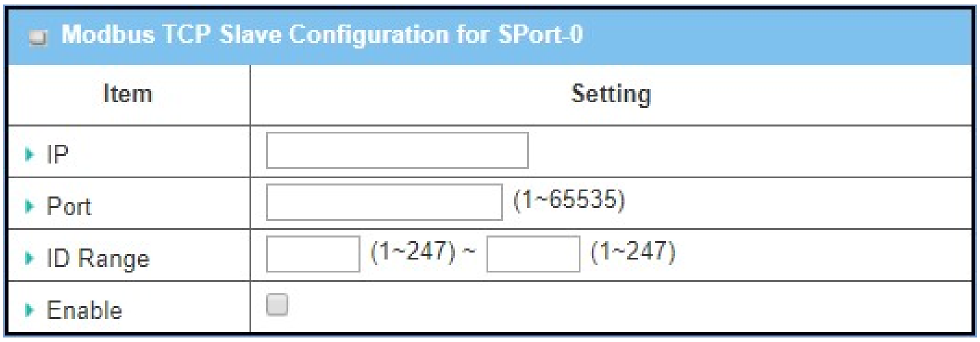
If there is a Modbus Master device attached to a serial port of the Modbus Gateway, the user must further specify the Modbus TCP Slave device(s) to send requests to or from the attached Modbus RTU/ASCII Master device.



Modbus TCP Slave List for SPort-0 [Add] [Delete]

ID	IP	Port	ID Range	Enable	Actions

When the **Add** button is applied, a **Modbus TCP Slave Configuration** screen will appear.



Modbus TCP Slave Configuration for SPort-0

Item	Setting
IP	
Port	(1~65535)
ID Range	(1~247) ~ (1~247)
Enable	□

Modbus Remote Slave Configuration		
Item	**Value setting**	**Description**
IP	Required setting	Enter the IP address of the remote Modbus TCP Slave device.
Port	1. Required setting 2. Range 1 to 65535	Enter the TCP port on which the remote Modbus TCP Slave device listens (to the TCP client session request). *Value Range*: 1 ~ 65535.
ID Range	Range 1 to 247	Enter the Modbus ID range for the Modbus TCP Slave(s) that will respond to the Master’s request. In addition to specifying the Slave IP and Port, for accessing Remote Modbus RTU Slave(s) located behind another Modbus Gateway, user must specify the Modus ID range of the Modbus RTU Slave(s). Value Range: 1 ~ 247.
Enable	Unchecked by default.	Check the **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.

Supported Function Code for Integrated Modbus Slave

This is for setting up the Gateway as a standalone Modbus Slave Device. Local SCADA Management System can treat the Gateway as a Slave device, and hence is able to read its information for device monitoring.

Currently, the integrated Modbus Slave device supports the following commands for accessing the 3G/4G Modem Status of the Gateway.

Function Code: 0x03(/Read). 0x06(/Write)
Address: 0 ~ 9999

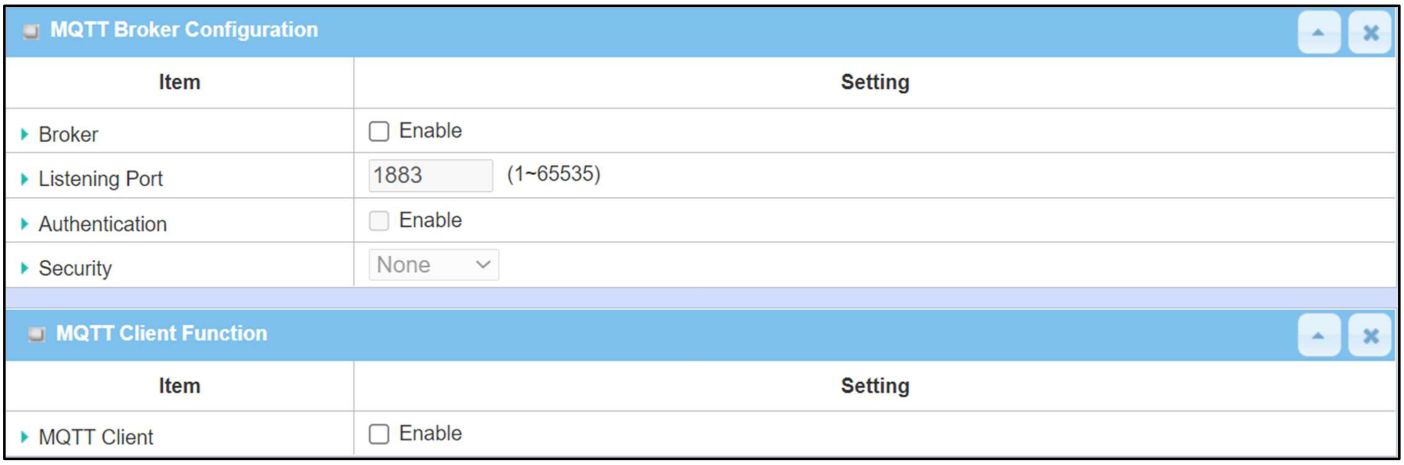
Register Address	Register Name	R / W	Register Range / Description
0	WAN-1 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Disconnected
1	WAN-2 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Disconnected
10	3G/4G_SERVICE_TYPE	R	0 ~ 7, 0=2G, 1=none, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
11	3G/4G_LINK_STATUS	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Disconnected
12	3G/4G_SIGNAL_STRENGTH	R	0 ~ 100
13	3G/4G_SIM_STATUS	R	0: SIM card with PIN code insert 1: SIM card ready 2: No SIM card
14	3G/4G_MCC	R	MCC Value
15	3G/4G_MNC	R	MNC Value
16	3G/4G_CS Register Status	R	0: Unregistered, 1: Registered
17	3G/4G_PS Register Status	R	0: Unregistered, 1: Registered
18	3G/4G_Roaming Status	R	0: Not Roaming, 1: Roaming
19	3G/4G_RSSI	R	RSSI Value
20	3G/4G_RSRP	R	RSRP Value
21	3G/4G_RSRQ	R	RSRQ Value
30	3G/4G_Module-2_SERVICE_TYPE	R	0 ~ 7, 0=2G, 1=none, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
31	3G/4G_Module-2_LINK_STATUS	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Disconnected
32	3G/4G_Module-2_SIGNAL_STRENGTH	R	0 ~ 100
33	3G/4G_Module-2_SIM_STATUS	R	0: SIM card with PIN code insert 1: SIM card ready 2: No SIM card
34	3G/4G_Module-2_MCC	R	MCC Value
35	3G/4G_Module-2_MNC	R	MNC Value
36	3G/4G_Module-2_CS Register Status	R	0: Unregistered, 1: Registered
37	3G/4G_Module-2_PS Register	R	0: Unregistered, 1: Registered

Register Address	Register Name	R / W	Register Range / Description
	Status		
38	3G/4G_Module-2_Roaming Status	R	0: Not Roaming, 1: Roaming
39	3G/4G_Module-2_RSSI	R	RSSI Value
40	3G/4G_Module-2_RSRP	R	RSRP Value
41	3G/4G_Module-2_RSRQ	R	RSRQ Value
70	ADSL_Download_Data rate	R	ADSL Download Data rate value (kbps)
71	ADSL_Upload_Data rate	R	ADSL Upload Data rate value (kbps)
72	ADSL SNR_Download	R	ADSL SNR Download value (dB)
73	ADSL SNR_Upload	R	ADSL SNR Upload value (dB)
74	ADSL modem link status	R	0: Disconnected, 1: Connected
101	VPN IPSec tunnel 1 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
102	VPN IPSec tunnel 2 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
103	VPN IPSec tunnel 3 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
104	VPN IPSec tunnel 4 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
105	VPN IPSec tunnel 5 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
106	VPN IPSec tunnel 6 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
107	VPN IPSec tunnel 7 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
108	VPN IPSec tunnel 8 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
109	VPN IPSec tunnel 9 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
110	VPN IPSec tunnel 10 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
111	VPN IPSec tunnel 11 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
112	VPN IPSec tunnel 12 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
113	VPN IPSec tunnel 13 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
114	VPN IPSec tunnel 14 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
115	VPN IPSec tunnel 15 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
116	VPN IPSec tunnel 16 status	R	1: Connected, 2: Wait for traffic , 3: Disconnected , 9: Connecting
150	DI_STATUS_1	R	0: OFF, 1: ON
151	DO_STATUS_1	R/W	0: OFF, 1: ON
152	DI_STATUS_2	R	0: OFF, 1: ON
153	DO_STATUS_2	R/W	0: OFF, 1: ON
154	DI_STATUS_3	R	0: OFF, 1: ON
155	DO_STATUS_3	R/W	0: OFF, 1: ON
156	DI_STATUS_4	R	0: OFF, 1: ON

Register Address	Register Name	R / W	Register Range / Description
157	DO_STATUS_4	R/W	0: OFF, 1: ON
201	Serial Port-0_Interface	R	1: RS-232, 3: RS-485
202	Serial Port-0_Baud Rate	R	Baud Rate Value
203	Serial Port-0_Data Bits	R	7 or 8
204	Serial Port-0_Stop Bits	R	1 or 2
205	Serial Port-0_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
206	Serial Port-0_Parity	R	0: None, 1: Odd, 2: Even
211	Serial Port-1_Interface	R	1: RS-232, 3: RS-485
212	Serial Port-1_Baud Rate	R	Baud Rate Value
213	Serial Port-1_Data Bits	R	7 or 8
214	Serial Port-1_Stop Bits	R	1 or 2
215	Serial Port-1_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
216	Serial Port-1_Parity	R	0: None, 1: Odd, 2: Even
221	Serial Port-2_Interface	R	1: RS-232, 3: RS-485
222	Serial Port-2_Baud Rate	R	Baud Rate Value
223	Serial Port-2_Data Bits	R	7 or 8
224	Serial Port-2_Stop Bits	R	1 or 2
225	Serial Port-2_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
226	Serial Port-2_Parity	R	0: None, 1: Odd, 2: Even
231	Serial Port-3_Interface	R	1: RS-232, 3: RS-485
232	Serial Port-3_Baud Rate	R	Baud Rate Value
233	Serial Port-3_Data Bits	R	7 or 8
234	Serial Port-3_Stop Bits	R	1 or 2
235	Serial Port-3_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
236	Serial Port-3_Parity	R	0: None, 1: Odd, 2: Even
9999	System_Reboot	W	Set 1 for System reboot.

5.2 Data Interchange

MQTT is a messaging protocol for small sensors and mobile devices. MQTT stands for Message Queuing Telemetry Transport. MQTT uses a publish-subscribe pattern to exchange messages. MQTT systems are comprised of one broker and several clients, where clients can either be publishers or subscribers. Publishers send data to the broker in the form of MQTT "topic" and "payload" packets. The broker then distributes the data to subscribers based on subscribed topics.



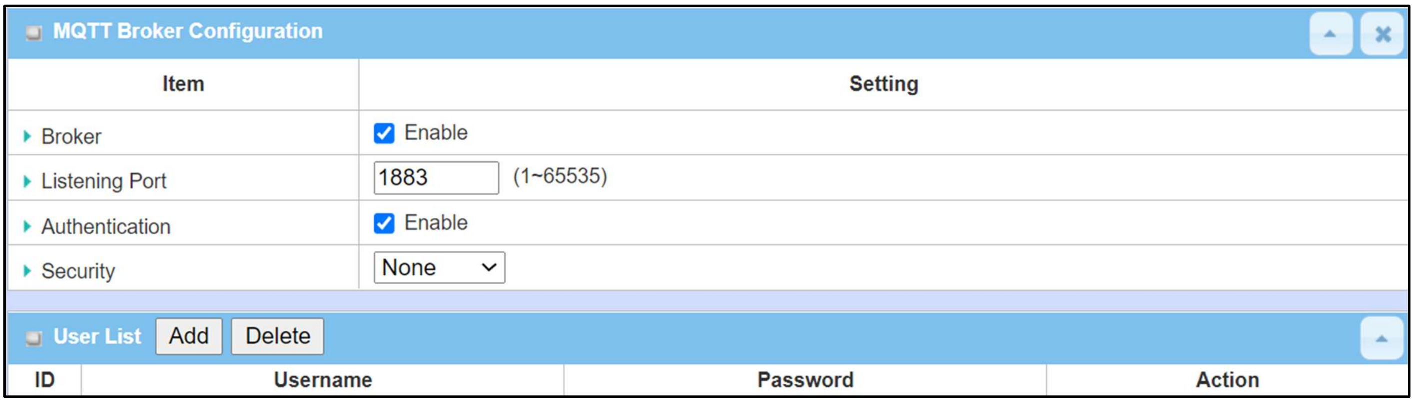
MQTT Broker Configuration

Item	Setting
Broker	□ Enable
Listening Port	1883 (1~65535)
Authentication	□ Enable
Security	None

MQTT Client Function

Item	Setting
MQTT Client	□ Enable

Configure the MQTT Broker



MQTT Broker Configuration

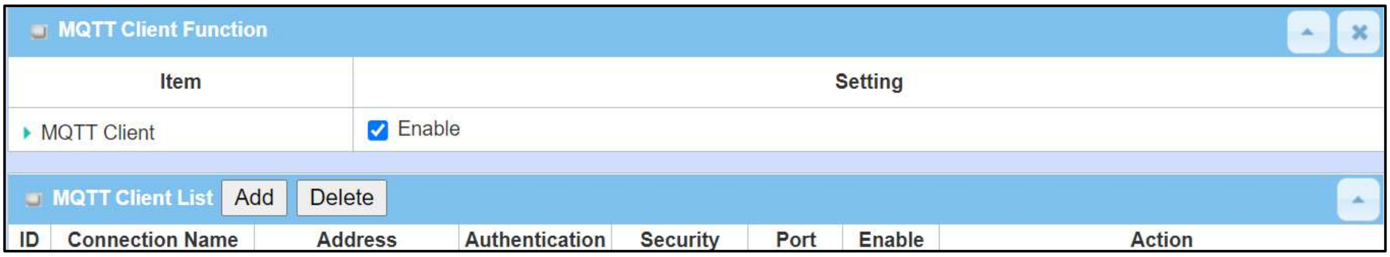
Item	Setting
Broker	☑ Enable
Listening Port	1883 (1~65535)
Authentication	☑ Enable
Security	None

User List Add Delete

ID	Username	Password	Action

MQTT Broker Configuration		
Item	**Value setting**	**Description**
Broker	Unchecked by default.	Check the **Enable** box to enable MQTT broker.
Listening Port	1. Required setting 2. Range 1 to 65535	Enter the TCP port for the MQTT Listener. Default port is 1883. *Value Range*: 1 ~ 65535.
Authentication	Unchecked by default.	Check box to enable authentication. When enabled, a user list module will appear, where you can add, edit, and delete users for authentication.
Security	**None** by default.	Select **SSL** or **TLS**.
Save	N/A	Click the **Save** button to save the settings.

Configure the MQTT Client Function



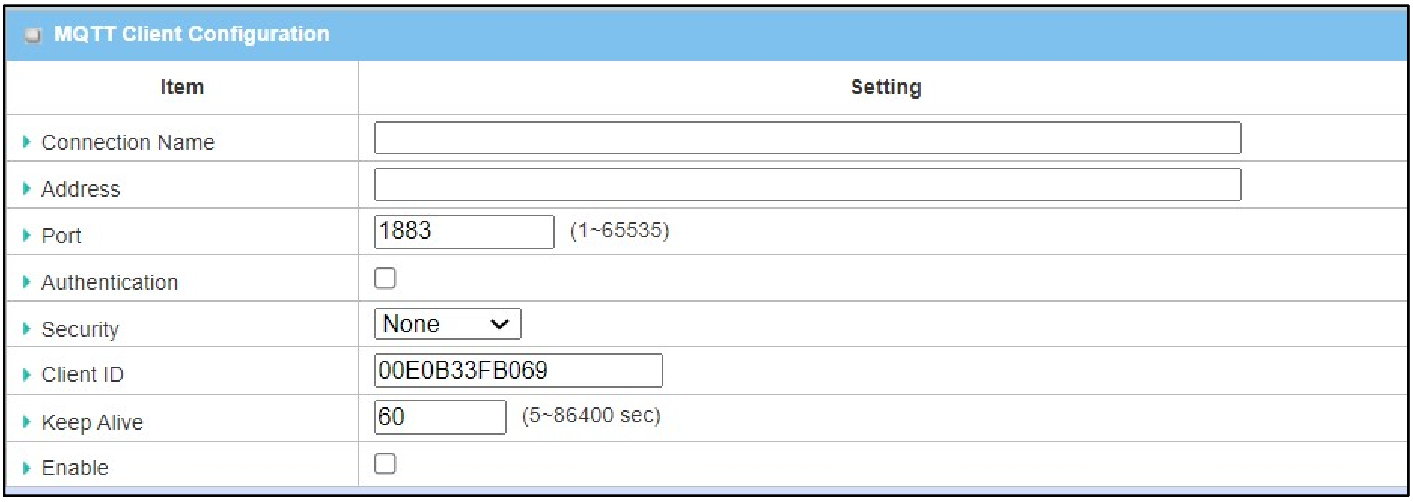
MQTT Client Function

Item	Setting
MQTT Client	☑ Enable

MQTT Client List Add Delete

ID	Connection Name	Address	Authentication	Security	Port	Enable	Action

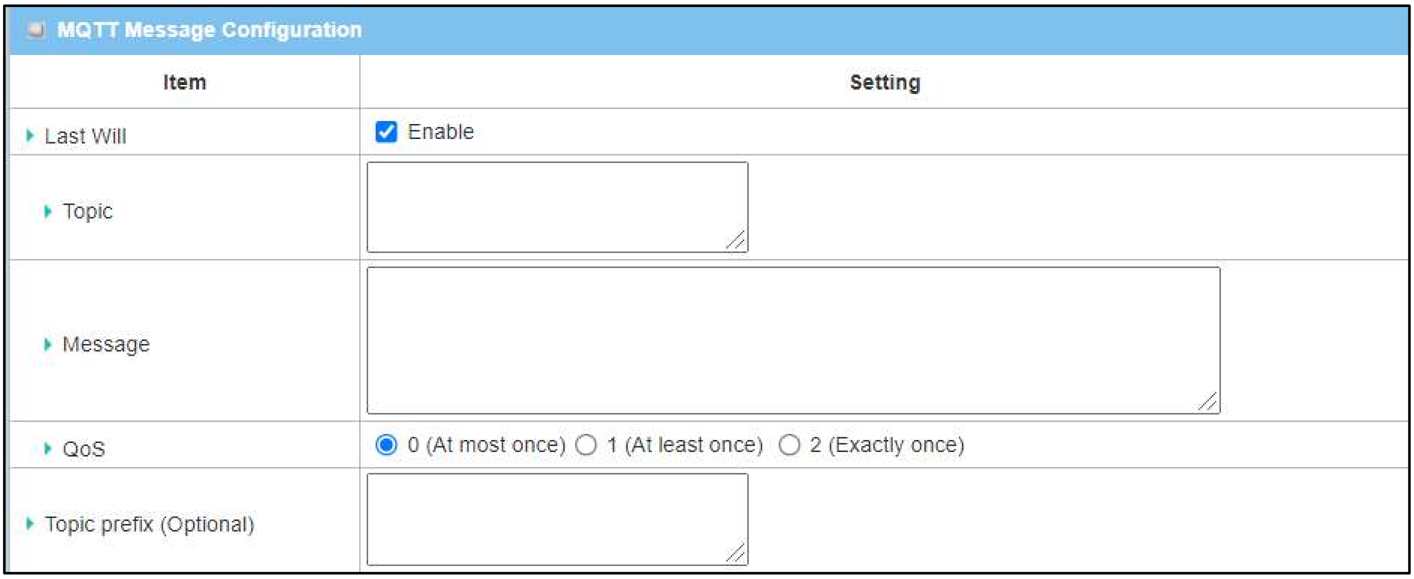
MQTT Client Configuration		
Item	**Value setting**	**Description**
MQTT Client	Unchecked by default.	Check the **Enable** box to enable MQTT Client. When enabled, an MQTT client list will appear. Click **Add** to add a new client. The MQTT Client Configuration module will appear.



MQTT Client Configuration

Item	Setting
Connection Name	
Address	
Port	1883 (1~65535)
Authentication	□
Security	None
Client ID	00E0B33FB069
Keep Alive	60 (5~86400 sec)
Enable	□

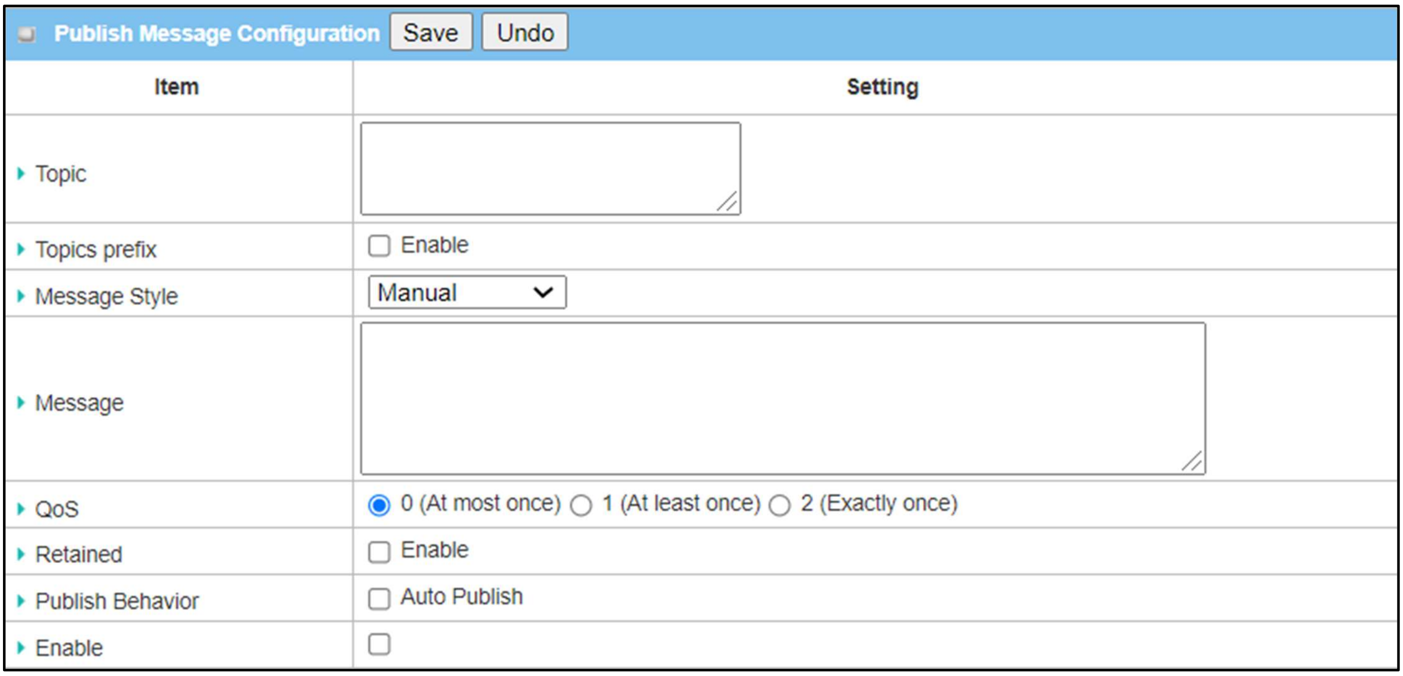
MQTT Client Configuration		
Item	**Value setting**	**Description**
Connection Name	Required field	Enter a unique name for the connection.
Address	Required field	Enter the IP address of the MQTT broker that the client will connect to.
Port	1883 by default	Enter the port to be used by the MQTT connection.
Authentication	Unchecked by default.	Check this box to enable Authentication, then enter the username and Password in the fields that will appear.
Security	**None** by default.	Select **SSL** or **TLS**.
Client ID	Required field.	Enter an ID to identify the MQTT session.
Keep Alive	60 seconds by default	Set the maximum time interval that can elapse between the point a client finishes transmitting a control packet and when it starts to send the next packet. Range is 5~86400 seconds.
Enable	Unchecked by default.	Check this box to enable this client



MQTT Message Configuration

Item	Setting
Last Will	☑ Enable
Topic	
Message	
QoS	● 0 (At most once) ○ 1 (At least once) ○ 2 (Exactly once)
Topic prefix (Optional)	

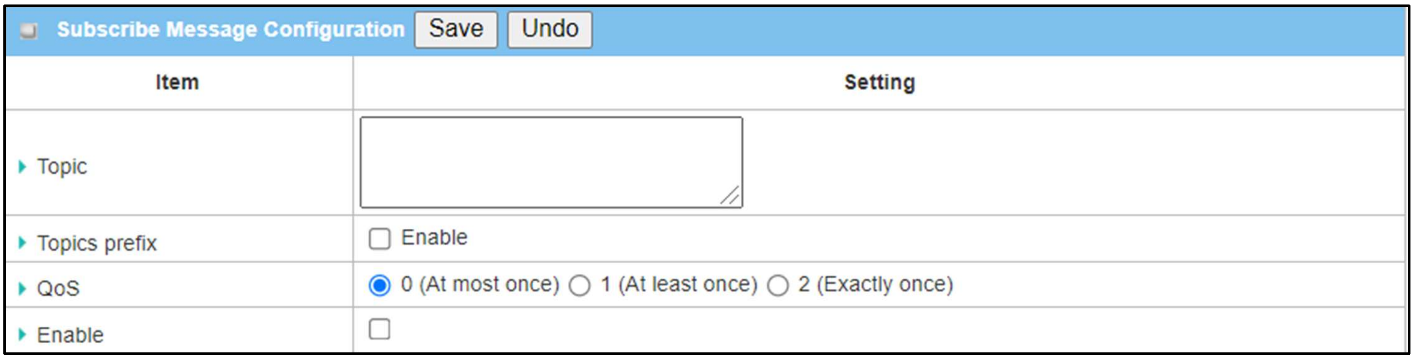
MQTT Message Configuration		
Item	**Value setting**	**Description**
Last Will	Unchecked by default	When Last Will is enabled, the fields below will appear.
Topic	Blank by default	Enter the Topic.
Message	Blank by default	Enter the message to be sent.
QoS	0 by default	Select 0 (At most once), 1 (At least once), or 2 (Exactly once)
Topic Prefix	Optional	Enter the Topic Prefix.



Publish Message Configuration

Item	Setting
Topics	
Topics prefix	□ Enable
Message Style	Manual
Message	
QoS	● 0 (At most once) ○ 1 (At least once) ○ 2 (Exactly once)
Retained	□ Enable
Publish Behavior	□ Auto Publish
Enable	□

Publish Message Configuration		
Item	**Value setting**	**Description**
Topic	Blank by default	Enter the message topic. Topics are case-sensitive.
Topics Prefix	Blank by default	Enter the Topic Prefix.
Message Style	**Manual** is set by default	Select Manual, System Log, or Data Logging.
Message	Blank by default	Enter the message to be published
QoS	0 by default	Select 0 (At most once), 1 (At least once), or 2 (Exactly once)
Retained	Unchecked by default	Enable to retain messages that are published when there are no subscribers.
Publish Behavior	Unchecked by default	Click the checkbox to enable Auto Publish function.
Enable	Unchecked by default.	Check this box to enable this message.



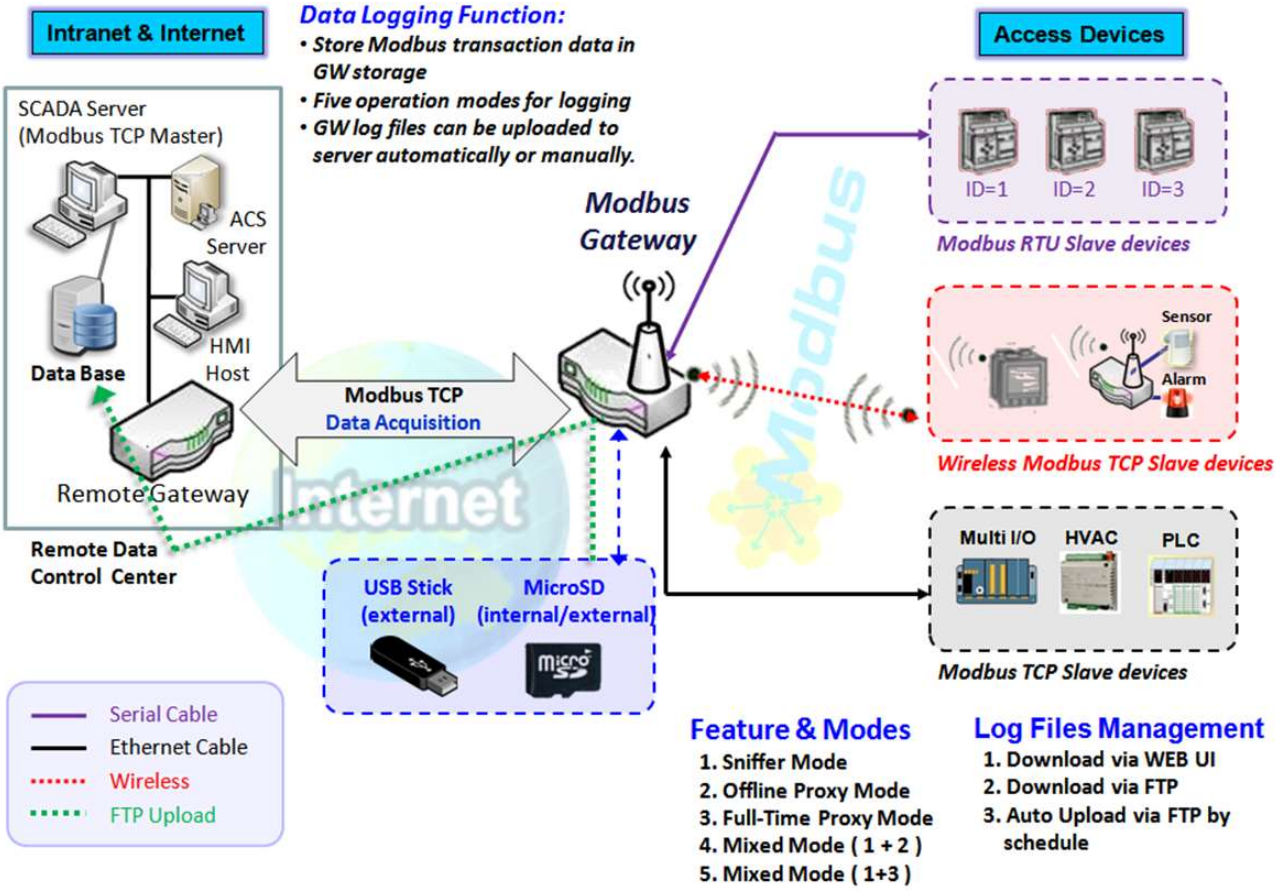
Item	Setting
Topic	
Topics prefix	□ Enable
QoS	● 0 (At most once) ○ 1 (At least once) ○ 2 (Exactly once)
Enable	□

Subscribe Message Configuration		
Item	**Value setting**	**Description**
Topic	Blank by default	
Topic Prefix	Blank by default	
QoS	0 by default	Select 0 (At most once), 1 (At least once), or 2 (Exactly once)
Enable	Unchecked by default.	Check this box to enable this subscribe message.

5.3 Data Logging

Data logging is the process of collecting and storing data over a period of time in order to analyze specific trends or record the data-based events/actions of a system, or connected devices. The data logging function is a very useful and important feature for SCADA telemetry; it makes the monitoring and analyzing of tasks easier by checking the status and historical data during whole data acquisition period.

Even facing network connection problems with a remote NOC/SCADA side, you can enable the data logging proxy function provided by the gateway and continue doing data acquisition and storing of the collected data in local storage (in .CSV file format). When the network connection is recovered, admin/user can download the data log files manually via FTP or web UI for further reference and maintenance.



The Modbus Cellular Gateway provides a complete data logging function for collecting the Modbus transaction data for application requirements. There are data logging schemes to meet different management requirements. They are Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and mixed modes for sniffer and proxy combinations.

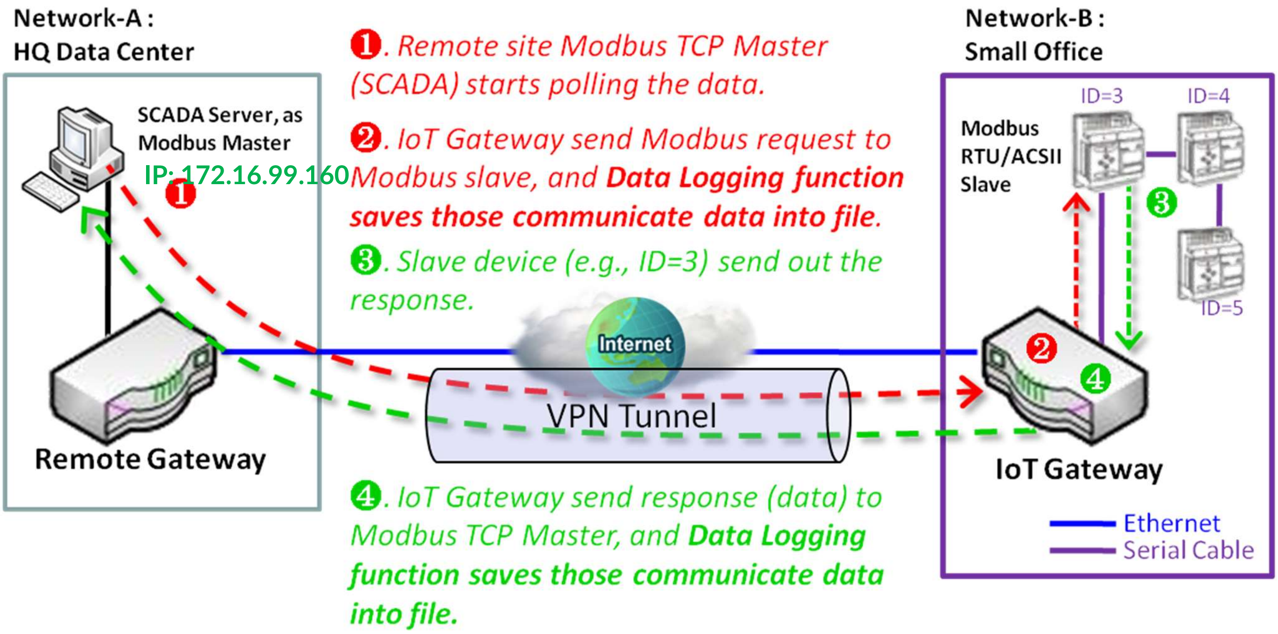
With Sniffer mode enabled, the gateway will monitor and record the communication among a specific Modbus Master and related slaves. It will store the Modbus communication as log files and the administrator can check what Modbus communication went over the Modbus gateway, and if there is any communication loss among the Master and Slave sides.

However, if there is a network connection problem between the Modbus gateway and remote NOC/SCADA, the remote Modbus server won't be able to reach the Slave devices attached to the Modbus gateway, and consequently, nothing can be monitored and stored under such situation.

With the Proxy mode option enabled, when the Modbus gateway loses the connection with specified Modbus server, it will take over the data acquisition task and keep collecting the required data from Slave devices automatically. Once the connection is recovered, the Modbus gateway will stop the data log proxy function. The remote Modbus server can continue its data acquisition process, and if required, the administrator can also retrieve the stored data log files.

Under the Data Logging Proxy mode, user must create some data acquisition rules via "Proxy Mode Rule Configuration" for the collecting of the Slave devices data by the Gateway. If the network connection to remote SCADA is lost unexpectedly, the Data Logging Proxy function will be triggered and begin to do the data polling tasks by these pre-defined rules running in background.

➢ Scenario for Sniffer Mode Data Logging



❶. *Remote site Modbus TCP Master (SCADA) starts polling the data.*

❷. *IoT Gateway send Modbus request to Modbus slave, and **Data Logging function saves those communicate data into file.***

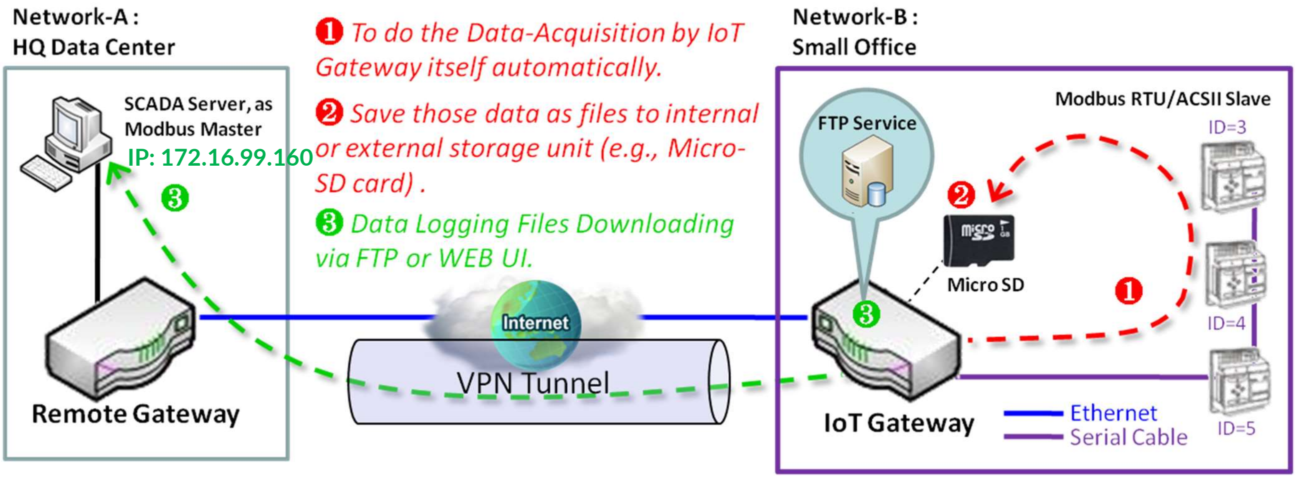
❸. *Slave device (e.g., ID=3) send out the response.*

❹. *IoT Gateway send response (data) to Modbus TCP Master, and **Data Logging function saves those communicate data into file.***

As Illustrated in the diagram, the Modbus gateway will store the following Modbus activities into a log file.

- The Modbus request sent from Remote Modbus TCP Master.
- The response (data) that is sent out from the polled Slave device (ID=3)

Scenario for Off-Line Proxy Mode Data Logging



As illustrated, when the connection to a remote Modbus Master is broken, the Modbus Gateway will activate the data logging proxy function and execute the pre-defined data acquisition task by itself.

- The Modbus request issued by the Modbus Gateway (Data Logging Proxy).
- The response (data) sent out from the polled Slave device (ID=3)

These data acquisition and data logging activities are repeated every 5 seconds until the connection is recovered.

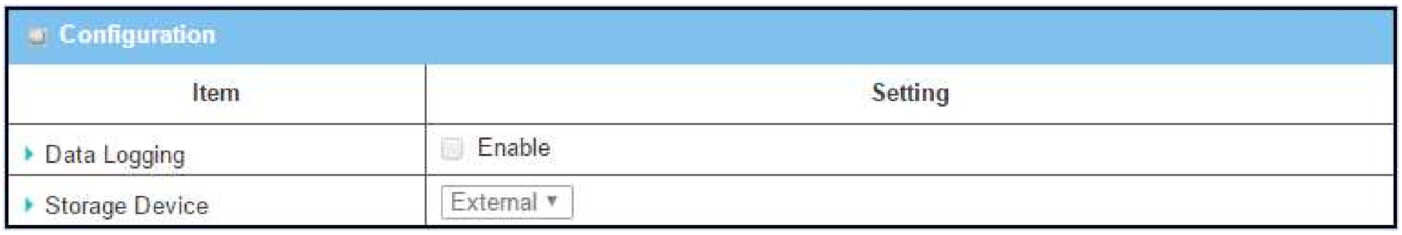
5.3.1 Data Logging Configuration

Data Logging is commonly used in monitoring systems to collect and analyze the field data. With proper configuration, the Gateway will record Modbus messages according to the specified rule list.

Go to Field Communication > Data Logging > Configuration tab. A warning message will appear:

“Please ensure the system time is already updated and corrected with the "System Time" sync feature first, or you may see the wrong time stamp shown in those data logging files.”

Enable Data Logging



Configuration

Item	Setting
Data Logging	□ Enable
Storage Device	External ▾

Configuration Item	Value setting	Description
Data Logging	Unchecked by default	Check the **Enable** box to activate to data logging function.
Storage Device	**External** is set by default	Choose the storage device to store the log files. It can be **External** or **Internal**, depending on the product specification.
Save	*NA*	Click the **Save** button to save the settings.

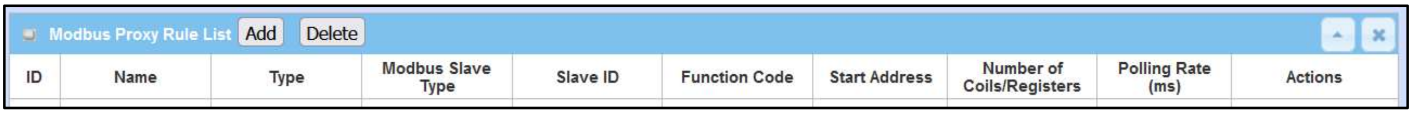
Note:

1. If there is no available storage device, the Enable checkbox will be grayed out, and can’t be enabled. If you select External Storage, connect the storage device first, and then enable the function and also set the required configuration.

2. Make sure the Modbus Operation Mode is selected and enabled, or there will be no Modbus transactions to be logged. Please refer to **Field Communication > Bus & Protocol > Port Configuration** and **Modbus** tabs.

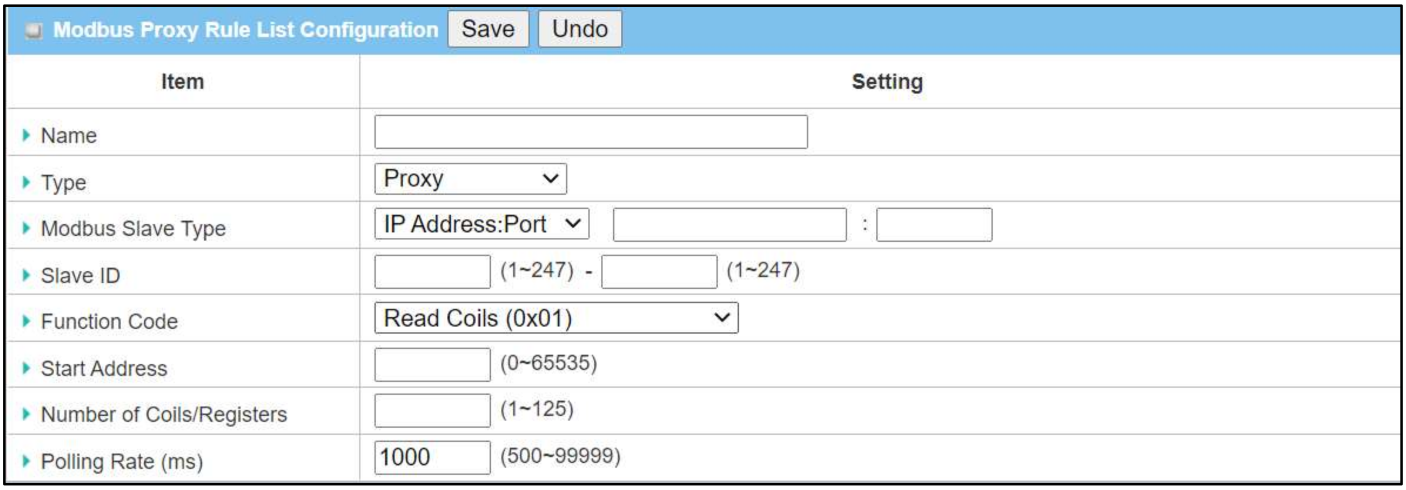
Create/Edit Modbus Proxy Rules

The Gateway allows you to customize your proxy mode rule list. It supports up to a maximum of 20 rules.



ID	Name	Type	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions

When the **Add** button is applied, the **Modbus Proxy Rule Configuration** screen will appear.



Item	Setting
Name	
Type	Proxy
Modbus Slave Type	IP Address:Port :
Slave ID	(1~247) - (1~247)
Function Code	Read Coils (0x01)
Start Address	(0~65535)
Number of Coils/Registers	(1~125)
Polling Rate (ms)	1000 (500~99999)

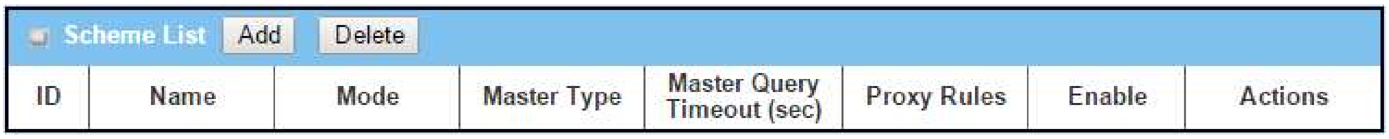
Modbus Proxy Rule Configuration		
Item	**Value setting**	**Description**
Name	Required setting.	Specify a name as the identifier of the Modbus proxy rule. ***Value Range***: 1 ~ 32 characters.
Type	**Proxy** is set by default	Select **Proxy** or **Proxy & Azure which send to Azure**.
Modbus Slave Type	**IP Address:Port** is selected by default.	Specify the Modbus Slave devices to which to apply the Modbus proxy rule. It can be **IP Address:Port** for Modbus TCP slaves or **Local Serial Port** for local attached Modbus RTU/ASCII slaves. ***Value Range***: 1 ~ 65535 for port number
Slave ID	1. Required setting. 2. Range 1 to 247	Specify the ID range for the slave device(s) to apply with the Modbus proxy rule. ***Value Range***: 1 ~ 247.
Function Code	**Read Coils (0x01)** is selected by default.	Specify a certain read function for the Data Logging Proxy to issue and record the responses from device(s).
Start Address	1. Required setting. 2. Range 0 to 65535	Specify the Start Address of registers to which to apply the specified function code. ***Value Range***: 0 ~ 65535.
Number of Coils/Registers	1. Required setting. 2. Range 1 to 125	Specify the number of coils/registers to which to apply the specified function code. ***Value Range***: 1 ~ 125. Note: **Start Address** plus **Number** must be smaller than 65536.
Polling Rate (ms)	1. Required setting. 2. **1000** ms is set by default	Enter the poll time in milliseconds for the Proxy Mode Rule. Once the proxy mode is activated, the Modbus Gateway will issue the pre-defined Modbus message at each Poll Time interval. ***Value Range***: 500 ~ 99999.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the changes.

5.3.2 Scheme Setup

There are five data logging schemes to meet different management requirements. They are Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and mixed modes for sniffer and proxy combinations. Configure the required data logging rules with selected scheme in this Scheme Setup page.

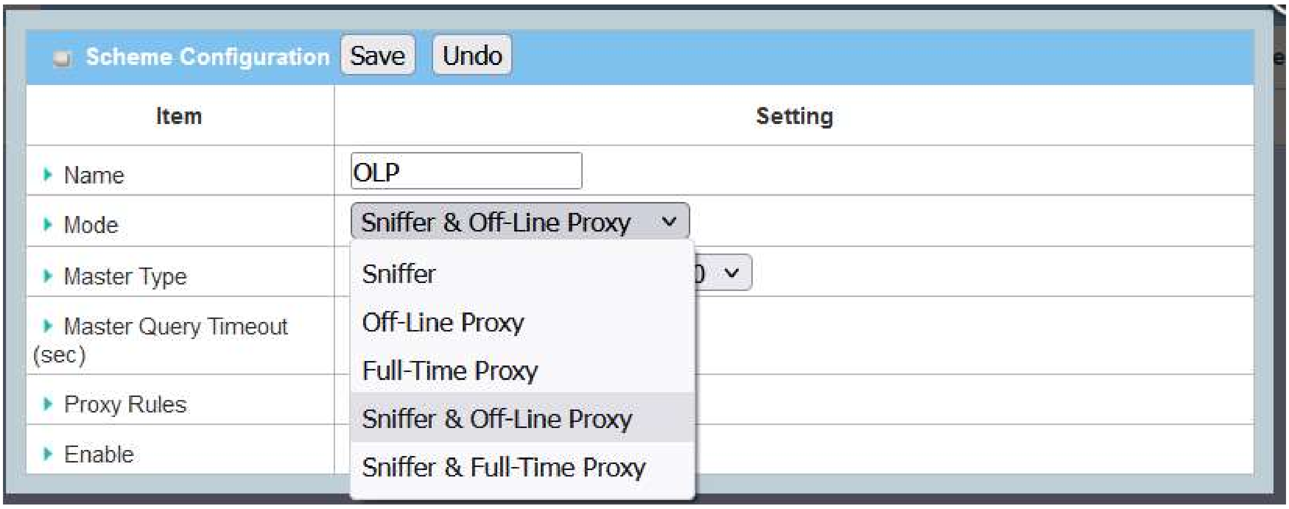
Go to Field Communication > Data Logging > Scheme Setup tab.

Create/Edit Data Logging Rules



ID	Name	Mode	Master Type	Master Query Timeout (sec)	Proxy Rules	Enable	Actions

When the **Add** button is applied, **Scheme Configuration** screen will appear.



Item	Setting
Name	OLP
Mode	Sniffer & Off-Line Proxy
Master Type	
Master Query Timeout (sec)	
Proxy Rules	
Enable	

Scheme Configuration		
Item	**Value setting**	**Description**
Name	Required setting.	Specify a name as the identifier of the data logging rule. ***Value Range***: 1 ~ 16 characters.
Mode	**Sniffer** is selected by default.	Select an expected data logging scheme for the data logging rule. There are five available schemes: **Sniffer**: The Modbus gateway will record all Modbus transactions between the Master and Slave devices. **Off-Line Proxy**: When the connection between the Modbus gateway and Master is lost, the pre-defined proxy rule will be triggered and the Modbus gateway will issue the specified function code to collect and record the data / status from the slave devices.

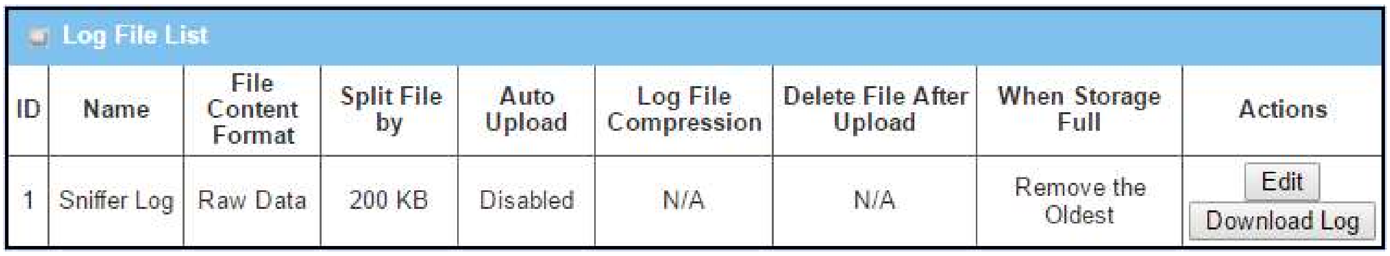
		Full-Time Proxy: The pre-defined proxy rule will be triggered all the time and the Modbus gateway will issue the specified function code to collect and record the data / status from the slave devices. **Sniffer & Off-Line Proxy**: This is a mixed mode for both Sniffer and Off-Line Proxy modes. **Sniffer & Full-Time Proxy**: This is a mixed mode for both Sniffer and Full-Time Proxy modes.
Master Type	**IP Address** is selected by default.	Specify the Modbus master device to apply with the data logging rule. It can be **IP Address** for Modbus TCP master, or **Local Serial Port** for local attached Modbus RTU/ASCII master.
Master Query Timeout (sec.)	1. Optional setting. 2. **60** sec is set by default 3. Range 1 to 99999	Specify the timeout value for querying the Modbus Master. If there is no response from the master within the specified timeout setting, the selected proxy rule will be triggered and applied with the data logging rule. Note: If Off-Line proxy scheme is selected, the timeout setting will be used to check. Otherwise, this value is not used.
Proxy Rules	Optional setting.	Select the Proxy rule to be applied with the data logging rule. Note: If any proxy scheme is selected, please create the required Proxy rules in advance, and select from the list.
Enable	Unchecked by default.	Check the box to activate the data logging rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the changes.

5.3.3 Log File Management

There are five data logging schemes to meet different management requirements. They are Sniffer Mode, Off-Line Proxy Mode, Full-Time Proxy Mode, and mixed modes for sniffer and proxy combinations. Configure the required data logging rules with a selected scheme in this Scheme Setup page.

Go to Field Communication > Data Logging > Log File Management tab.

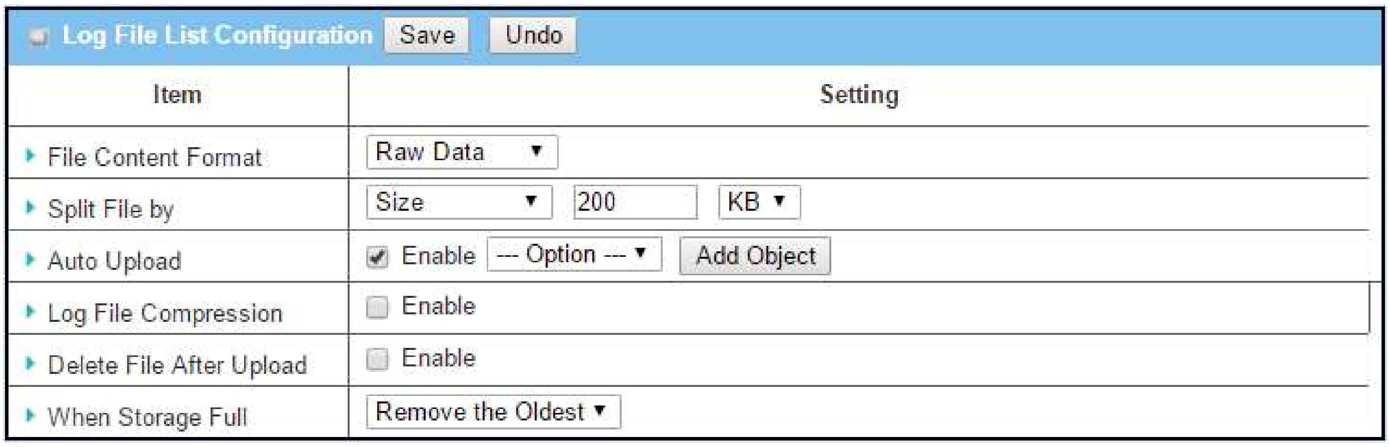
If the user has created data log rules in the **Field Communication > Data Logging > Scheme Setup** tab, there will be a log file list shown in the following Log File list screen. The default Log File management settings will be applied if they have not been changed via the **Edit** button.



Log File List

ID	Name	File Content Format	Split File by	Auto Upload	Log File Compression	Delete File After Upload	When Storage Full	Actions
1	Sniffer Log	Raw Data	200 KB	Disabled	N/A	N/A	Remove the Oldest	Edit Download Log

When the **Edit** button is applied, **Log File Configuration** screen will appear.



Log File List Configuration

Item	Setting
File Content Format	Raw Data ▾
Split File by	Size ▾ 200 KB ▾
Auto Upload	☑ Enable --- Option --- ▾ Add Object
Log File Compression	□ Enable
Delete File After Upload	□ Enable
When Storage Full	Remove the Oldest ▾

Log File Configuration		
Item	**Value setting**	**Description**
Name	N/A	The name of corresponding data log rule will be displayed. The default log file name will be named 'Name_yyyyMMddHHmmSS.csv'.
File Content Format	**Raw Data** is selected by default	Select the data format for the log files. It can be **Raw Data**, or **Modbus Type**.
Split File by	**Size** and **200 KB** are set by default	Specify the split file methodology. It can be by **Size**, or by **Time Interval**. Specify a certain file size or time interval for splitting the data logs into a series of files. ***Value Range***: 1 ~ 99999.
Auto Upload	1. Optional setting	Check the **Enable** box to activate the auto upload function for logged files.

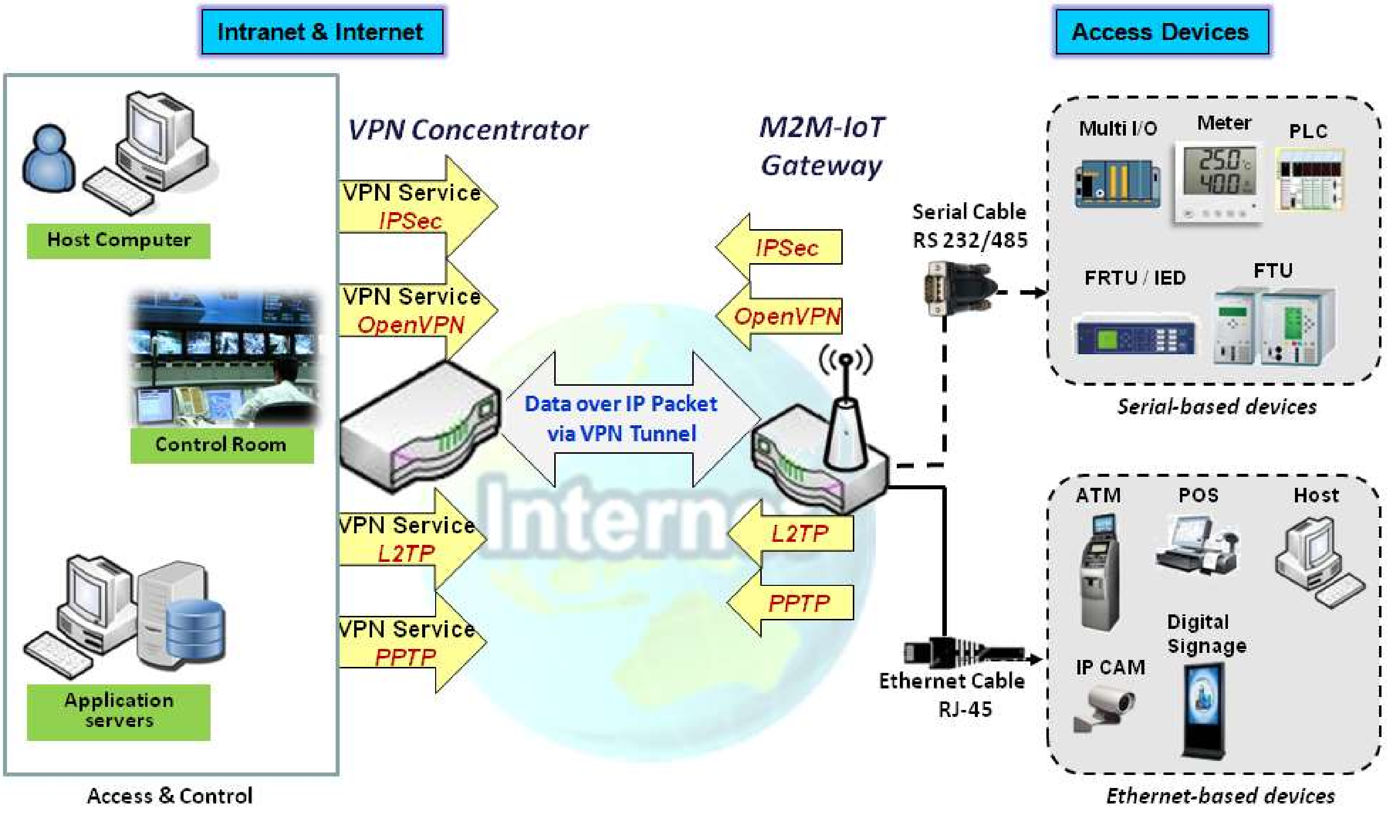
	2. Unchecked by default	Once enabled, specify an external FTP server from the dropdown list for auto uploading the log files to the server. Refer to **Object Definition > External Server > External Server** tab, or create the FTP server with the **Add Object** button.
Log File Compression	1. Optional setting 2. Unchecked by default	If Auto Upload is activated, user can further specify whether to compress the log file prior to its being uploaded. Check the **Enable** button to activate the Log File Compression function.
Delete File After Upload	1. Optional setting 2. Unchecked by default	If Auto Upload is activated, user can further specify whether to delete the transferred log from the gateway storage or not. Check the **Enable** button to activate the function.
When Storage Full	**Remove the Oldest** is selected by default	Specify the operation to take when the storage is full. It can be **Remove the Oldest** log file, or **Stop Recording**. When **Remove the Oldest** is selected, the gateway will delete the oldest file once the storage is full, and continue with the data logging activity; When **Stop Recording** is selected, the gateway will stop the data logging activity once the storage is full.
Save	*NA*	Click the **Save** button to save the settings.
Undo	*NA*	Click the **Undo** button to cancel the changes.

When the **Download Log** button is applied, the web browser will download a file named as ‘log.tar’ to the managing host computer.

Chapter 6 Security

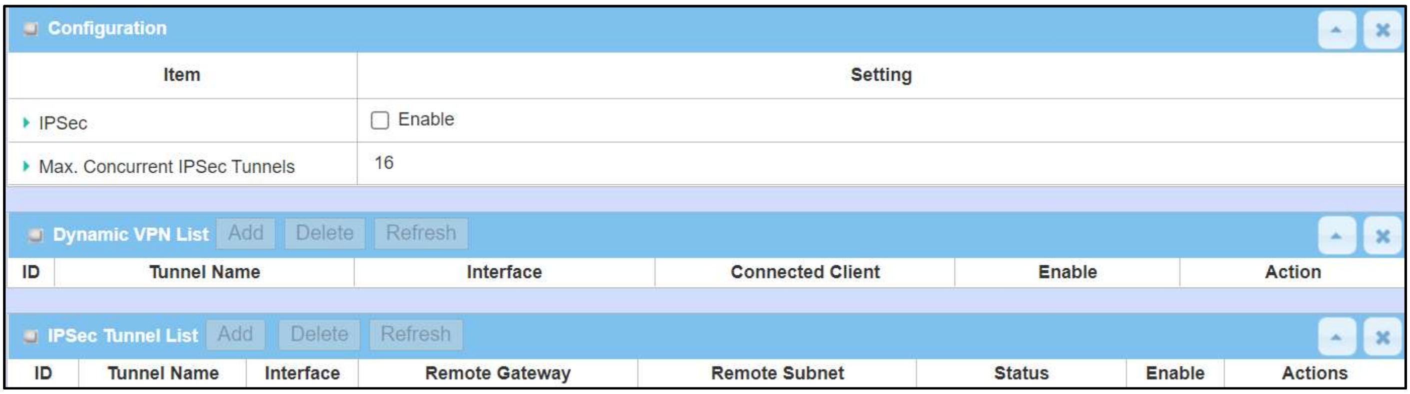
6.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.



The product series supports different tunneling technologies to establish secure tunnels between multiple sites for data transferring, such as IPsec, OpenVPN, L2TP (over IPsec), PPTP and GRE. Additionally, some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPsec, NAT Traversal and Dynamic VPN, are also supported.

6.1.1 IPSec



Configuration

Item	Setting
IPSec	☐ Enable
Max. Concurrent IPSec Tunnels	16

Dynamic VPN List Add Delete Refresh

ID	Tunnel Name	Interface	Connected Client	Enable	Action

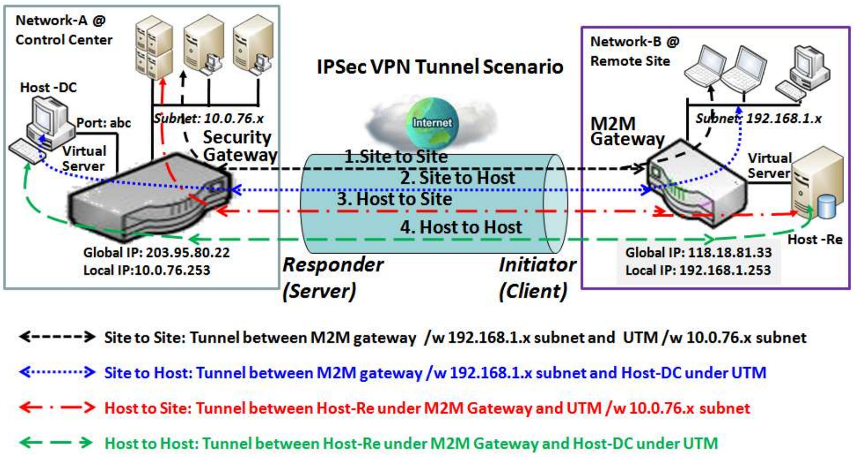
IPSec Tunnel List Add Delete Refresh

ID	Tunnel Name	Interface	Remote Gateway	Remote Subnet	Status	Enable	Actions

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

An IPsec VPN tunnel is established between IPsec client and server. Sometimes, we call the IPsec VPN client the initiator and the IPsec VPN server the responder. This gateway can be configured as different roles and establish a number of tunnels with various remote devices. Before going to set up the VPN connections, you may need to decide on the scenario type for the tunneling.

IPsec Tunnel Scenarios


Network-A @ Control Center
Host -DC
Port: abc
Virtual Server
Subnet: 10.0.76.x
Security Gateway
Global IP: 203.95.80.22
Local IP:10.0.76.253
IPSec VPN Tunnel Scenario
Internet
1.Site to Site
2. Site to Host
3. Host to Site
4. Host to Host
Responder (Server)
Initiator (Client)
Network-B @ Remote Site
M2M Gateway
Subnet: 192.168.1.x
Virtual Server
Host -Re
Global IP: 118.18.81.33
Local IP: 192.168.1.253
Site to Site: Tunnel between M2M gateway /w 192.168.1.x subnet and UTM /w 10.0.76.x subnet
Site to Host: Tunnel between M2M gateway /w 192.168.1.x subnet and Host-DC under UTM
Host to Site: Tunnel between Host-Re under M2M Gateway and UTM /w 10.0.76.x subnet
Host to Host: Tunnel between Host-Re under M2M Gateway and Host-DC under UTM

To build an IPsec tunnel, you need to enter the remote gateway global IP, and optional subnet if the hosts behind IPsec peer can access the remote site or hosts. Under such configuration, there are four scenarios:

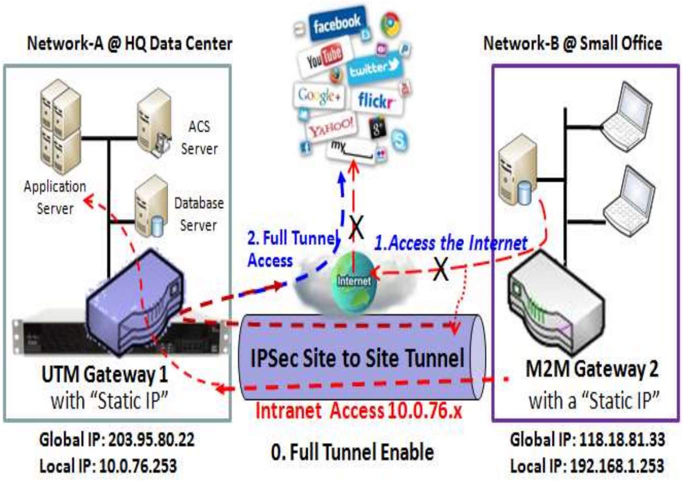
Site to Site: You need to set up remote gateway IP and subnet of both gateways. After the IPsec tunnel is established, hosts behind both gateways can communicate with each other through the tunnel.

Site to Host: Site to Host is suitable for tunneling between clients in a subnet and an application server (host). As in the diagram, the clients behind the M2M gateway can access to the host "Host-DC" located in the control center through Site to Host VPN tunnel.

Host to Site: For a single host (or mobile user) to access the resources located in an intranet, the Host to Site scenario can be applied.

Host to Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

Site to Site with "Full Tunnel" enabled



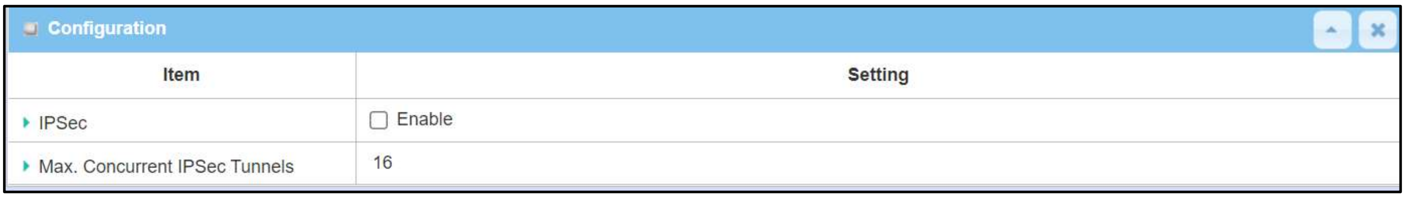
In "Site to Site" scenario, client hosts at the remote site can access enterprise resources in the Intranet of HQ gateway via an established IPsec tunnel, as described above. However, Internet access from remote sites still goes through the regular WAN connection. If you want all packets from remote site to be routed via this IPsec tunnel, including HQ server access and Internet access, enable the “Full Tunnel" setting. All traffic will go through the secure IPSec tunnel and route by the Security Gateway in control center.

IPSec Setting

Go to Security > VPN > IPSec tab.

The IPSec Setting allows user to create and configure IPSec tunnels.

Enable IPSec

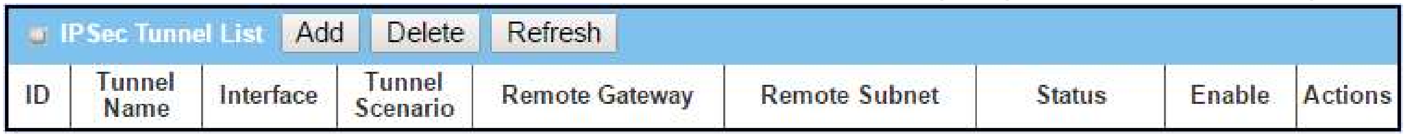


Item	Setting
IPSec	□ Enable
Max. Concurrent IPSec Tunnels	16

Configuration Window		
Item	**Value setting**	**Description**
IPsec	Unchecked by default	Click the **Enable** box to enable IPsec function.
Max. Concurrent IPSec Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPsec tunnel connections. The default value may differ depending on the device model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

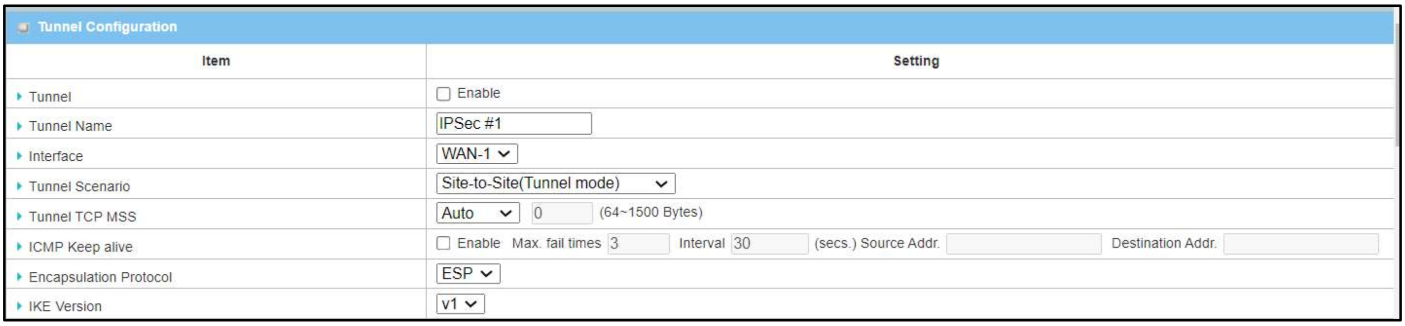
Create/Edit IPSec tunnel

Ensure that the IPsec enable box is checked to enable before further configuring the IPsec tunnel settings.



ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions

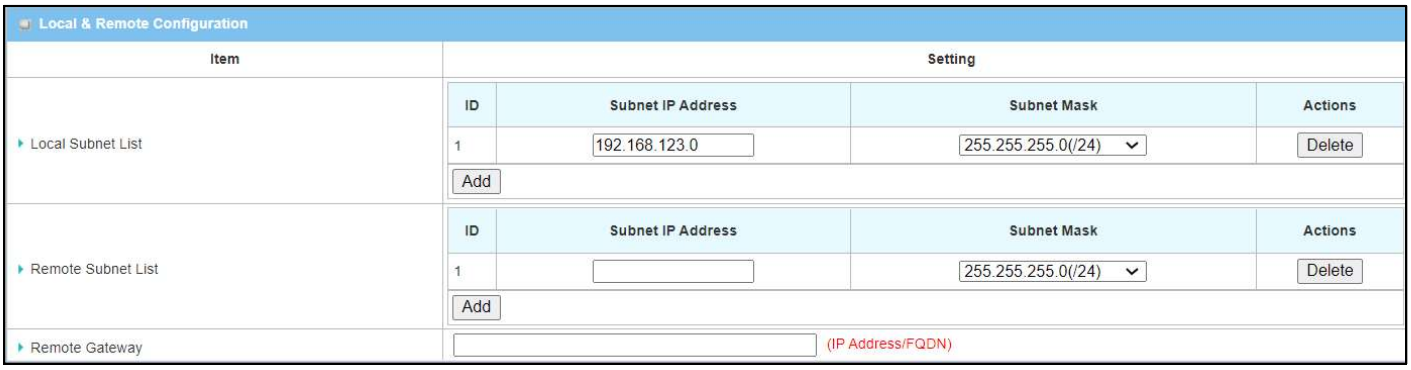
When **Add/Edit** button is applied, a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPsec Phase, and IPsec Proposal Definition. Configure the tunnel details for both local and remote VPN devices.



Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN-1
Tunnel Scenario	Site-to-Site(Tunnel mode)
Tunnel TCP MSS	Auto 0 (64~1500 Bytes)
ICMP Keep alive	□ Enable Max. fail times 3 Interval 30 (secs.) Source Addr. Destination Addr.
Encapsulation Protocol	ESP
IKE Version	v1

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the IPsec tunnel
Tunnel Name	1. Required setting 2. String format, text	Enter a tunnel name. ***Value Range***: 1 ~ 19 characters.
Interface	1. Required setting 2. **WAN 1** is selected by default	Select the interface on which IPsec tunnel is to be established. It can be any available WAN and LAN interface.
Tunnel Scenario	1. Required setting 2. **Site to site** is selected by default	Select an IPsec tunneling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. If LAN interface is selected, only **Host-to-Host** scenario is available. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPsec operates in tunnel mode. The difference is the number of subnets. With **Host-to-Host**, IPsec operates in transport mode.
Tunnel TCP MSS	Default is **Auto**	Maximum segment size. Select **Auto** or **Manual**. If Manual is selected, enter the largest amount of data in bytes.
ICMP Keep Alive	Unchecked by default	After enabling, enter the Max. fail times, Interval, and Source Address.
Encapsulation Protocol	1. Required setting 2. **ESP** is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPsec tunnel. Available encapsulations are **ESP** and **AH**.
IKE Version	V1 is default	Select **v1** or **v2**.

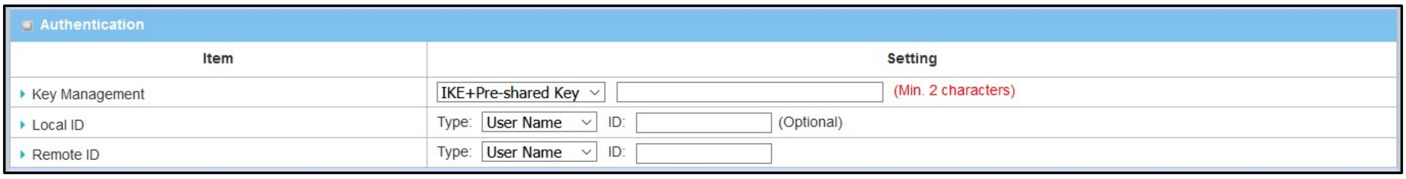


Local & Remote Configuration

Item	Setting			
Local Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	192.168.123.0	255.255.255.0(/24)	Delete
	Add			
Remote Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1		255.255.255.0(/24)	Delete
	Add			
Remote Gateway	(IP Address/FQDN)			

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	Required setting	Specify the Local Subnet IP address and Subnet Mask.

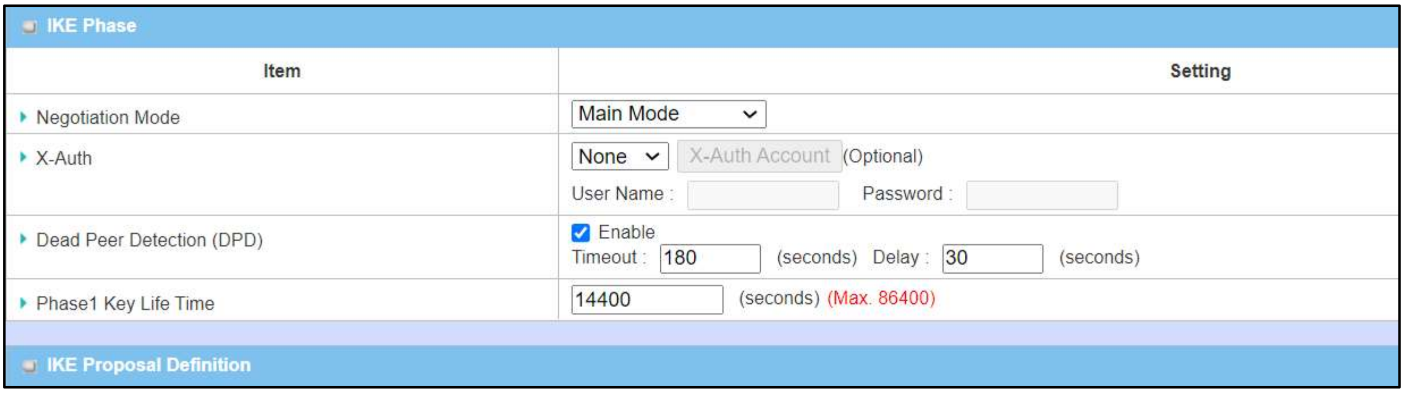
		Click the **Add** or **Delete** button to add or delete a Local Subnet. Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available. Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.
Remote Subnet List	Required setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	1. Required setting. 2. Format can be ipv4 address or FQDN	Specify the Remote Gateway.



Authentication

Item	Setting
Key Management	IKE+Pre-shared Key (Min. 2 characters)
Local ID	Type: User Name ID: (Optional)
Remote ID	Type: User Name ID:

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. Required setting 2. Pre-shared Key 2 to 256 characters.	Select Key Management from the dropdown box for this IPsec tunnel. **IKE+Pre-shared Key**: user needs to set a key (2 ~ 256 characters). **IKE+X.509**: user needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and also **Object Definition > Certificate** in web-based utility.
Local ID	Optional setting	Specify the Local ID for this IPsec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN. Select **Key ID** for Local ID and enter the Key ID (English letter or number).
Remote ID	Optional setting	Specify the Remote ID for this IPsec tunnel to authenticate. Select **User Name** for Remote ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Remote ID and enter the User@FQDN. Select **Key ID** for Remote ID and enter the Key ID (English letter or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

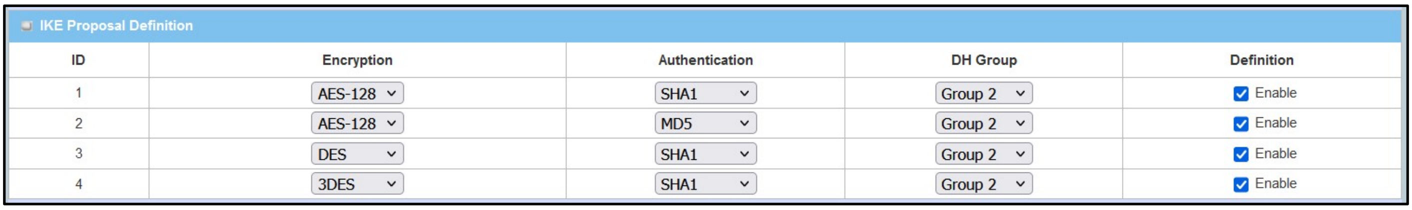


IKE Phase

Item	Setting
Negotiation Mode	Main Mode
X-Auth	None X-Auth Account (Optional) User Name : Password :
Dead Peer Detection (DPD)	☑ Enable Timeout : 180 (seconds) Delay : 30 (seconds)
Phase1 Key Life Time	14400 (seconds) (Max. 86400)

IKE Proposal Definition

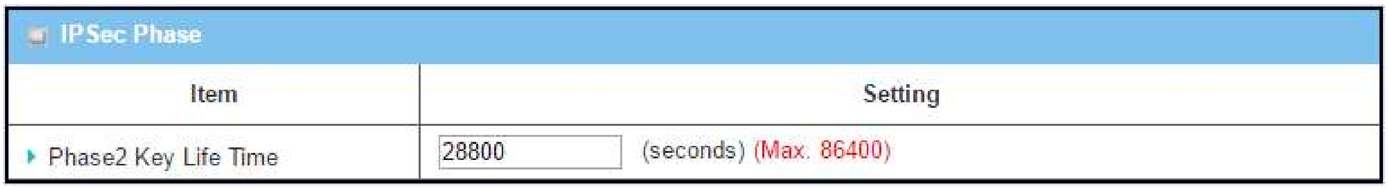
IKE Phase Window		
Item	**Value setting**	**Description**
Negotiation Mode	Main Mode is set by default	Specify the Negotiation Mode for this IPsec tunnel. Select Main Mode or Aggressive Mode.
X-Auth	None is selected by default	Specify the X-Auth role for this IPsec tunnel. Select Server, Client, or None. Selected Server for this gateway will be an X-Auth server. Click on the X-Auth Account button to create a remote X-Auth client account. Selected Client for this gateway will be an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
Dead Peer Detection (DPD)	1. Checked by default 2. Default Timeout 180s and Delay 30s	Click **Enable** box to enable **DPD** function. Specify the **Timeout** and **Delay** time in seconds. ***Value Range***: 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. Required setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. ***Value Range***: 30 ~ 86400.



IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-128	SHA1	Group 2	☑ Enable
2	AES-128	MD5	Group 2	☑ Enable
3	DES	SHA1	Group 2	☑ Enable
4	3DES	SHA1	Group 2	☑ Enable

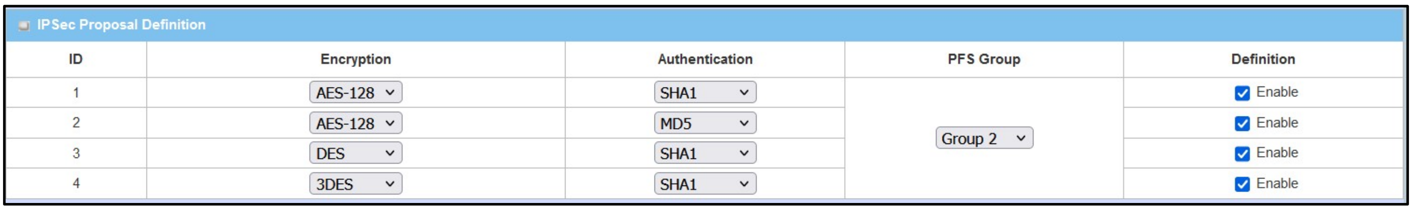
IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	Required setting	Specify the Phase 1 Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Specify the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Check the **Enable** box to enable this setting.



IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Phase Window		
Item	**Value setting**	**Description**
Phase2 Key Life Time	1. Required setting 2. 28800s is default 3. Max. 86400s	Specify the Phase2 Key Life Time in seconds. ***Value Range***: 30 ~ 86400.

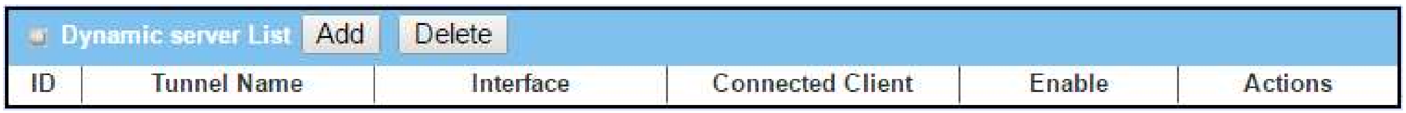


IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-128	SHA1	Group 2	☑ Enable
2	AES-128	MD5		☑ Enable
3	DES	SHA1		☑ Enable
4	3DES	SHA1		☑ Enable

IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	Required setting	Specify the Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256. Note: None is available only when Encapsulation Protocol is set as **AH**; it is not available for **ESP** Encapsulation. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Note: None and SHA2-256 are available only when Encapsulation Protocol is set as **ESP**; they are not available for **AH** Encapsulation. Specify the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Click **Enable** to enable this setting.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click **Back** to return to the previous page.

Create/Edit Dynamic VPN Server List

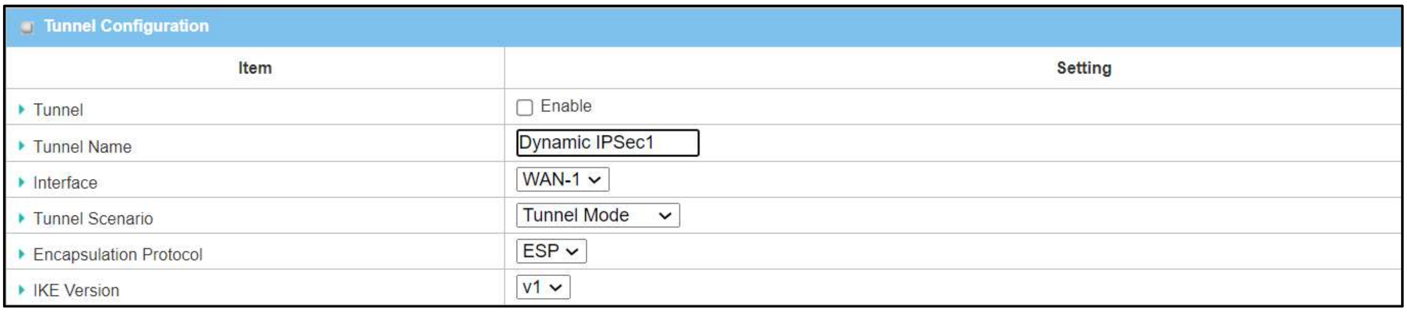


Dynamic server List Add Delete

ID	Tunnel Name	Interface	Connected Client	Enable	Actions

Similar to creating an IPsec VPN Tunnel for site/host to site/host scenario, when the **Edit** button is applied a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPsec Phase, and IPsec Proposal Definition. Configure the tunnel details for the gateway as a Dynamic VPN server.

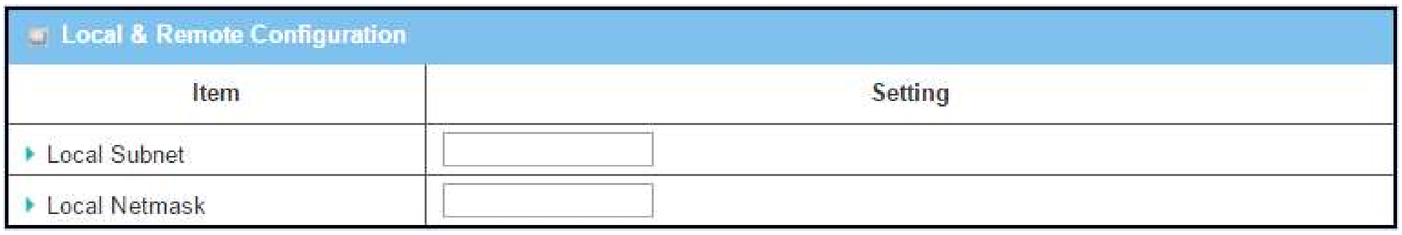
Note: You can configure one Dynamic VPN server for each WAN interface.



Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	Dynamic IPSec1
Interface	WAN-1
Tunnel Scenario	Tunnel Mode
Encapsulation Protocol	ESP
IKE Version	v1

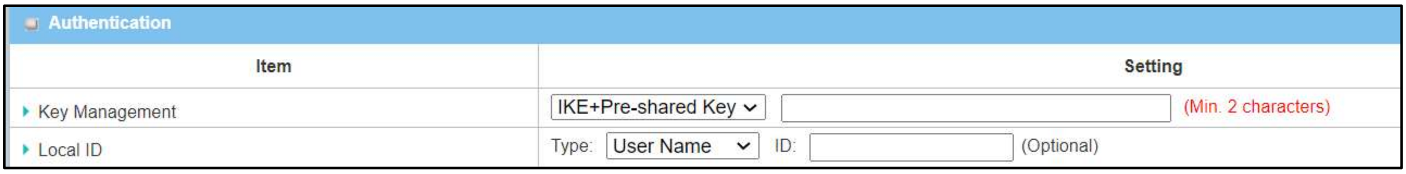
Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the Dynamic IPsec VPN tunnel.
Tunnel Name	1. Required setting 2. String format, any text	Enter a tunnel name. ***Value Range***: 1 ~ 19 characters.
Interface	1. Required setting 2. **WAN 1** is selected by default	Select WAN interface on which IPsec tunnel is to be established.
Tunnel Scenario	1. Required setting 2. Dynamic VPN is selected by default	The IPsec tunneling scenario is fixed to Dynamic VPN.
Encapsulation Protocol	1. Required setting 2. **ESP** is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPsec tunnel. Available encapsulations are **ESP** and **AH**.
IKE Version	V1 is selected by default	No other options on this model.



Local & Remote Configuration

Item	Setting
Local Subnet	
Local Netmask	

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	Required setting	Specify the Local Subnet IP address.
Local Netmask	Required setting	Specify the Local Subnet Mask.



Authentication

Item	Setting
Key Management	IKE+Pre-shared Key ⌄ ▭ (Min. 2 characters)
Local ID	Type: User Name ⌄ ID: ▭ (Optional)

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. Required setting 2. Pre-shared Key 2 to 256 characters.	Select Key Management from the dropdown box for this IPsec tunnel. **IKE+Pre-shared Key**: Set a key (2 ~ 256 characters).
Local ID	Optional setting	Specify the Local ID for this IPsec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN. Select **Key ID** for Local ID and enter the Key ID (letter or number).

For the remaining IKE Phase, IKE Proposal Definition, IPsec Phase, and IPsec Proposal Definition settings, they are the same as that of creating an IPsec Tunnel described in previous section. Please refer to the related descriptions.

6.1.2 OpenVPN

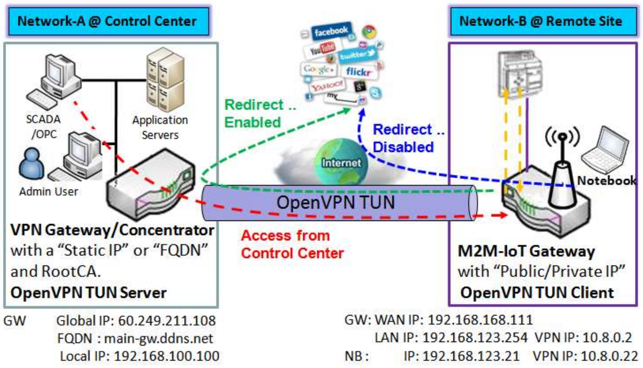
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN Tunneling is a Client and Server based tunneling technology. The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The OpenVPN Client may be a mobile user or mobile site with public IP or private IP, and requesting the OpenVPN tunnel connection. The product supports both OpenVPN Server and OpenVPN Client features to meet different application requirements.

There are two OpenVPN connection scenarios. They are the TAP and TUN scenarios. The product can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, specify which type of OpenVPN connection scenario is to be adopted.

OpenVPN TUN Scenario


Network-A @ Control Center
Network-B @ Remote Site
SCADA /OPC
Application Servers
Admin User
Redirect .. Enabled
Redirect .. Disabled
Internet
OpenVPN TUN
Notebook
Access from Control Center
VPN Gateway/Concentrator with a "Static IP" or "FQDN" and RootCA.
OpenVPN TUN Server
M2M-IoT Gateway with "Public/Private IP"
OpenVPN TUN Client
GW Global IP: 60.249.211.108
FQDN : main-gw.ddns.net
Local IP: 192.168.100.100
GW: WAN IP: 192.168.168.111
LAN IP: 192.168.123.254 VPN IP: 10.8.0.2
NB : IP: 192.168.123.21 VPN IP: 10.8.0.22

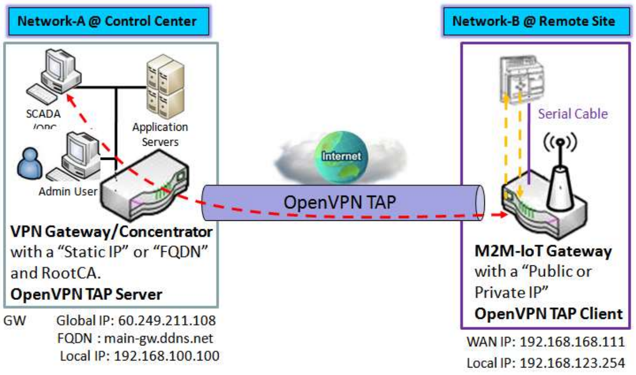
1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection estabilshed. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled & Redirect Internet Traffic enabled).
4. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 10.8.0.2.

The term "TUN" mode is referred to routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the OpenVPN server creates a "TUN" interface with its own IP address pool which is different to the local LAN. Remote hosts that dial-in will get an IP address inside the virtual network and will have access only to the server where OpenVPN resides.

If you want to offer remote access to a VPN server from client(s), and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an OpenVPN UN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which belongs to a virtual subnet that is different to the local subnet in Control Center. With such a connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; The SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (10.8.0.2).

OpenVPN TAP Scenario


Network-A @ Control Center
Network-B @ Remote Site
SCADA /OPC
Application Servers
Admin User
Internet
OpenVPN TAP
Serial Cable
VPN Gateway/Concentrator with a "Static IP" or "FQDN" and RootCA.
OpenVPN TAP Server
M2M-IoT Gateway with a "Public or Private IP"
OpenVPN TAP Client
GW Global IP: 60.249.211.108
FQDN : main-gw.ddns.net
Local IP: 192.168.100.100
WAN IP: 192.168.168.111
Local IP: 192.168.123.254

1. M2M-IoT Gateway (as OpenVPN TAP Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TAP Server).
2. M2M-IoT Gateway will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection estabilshed. (same subnet as in Control Center)
3. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 192.168.100.210.

The term "TAP" refers to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access resources on the LAN. To offer remote access to the entire remote LAN for VPN client(s), set up OpenVPN in “TAP” bridge mode.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TAP Client, and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP (192.168.100.210) which is on the same subnet as that of local subnet in Control Center. With this connection, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (192.168.100.210).

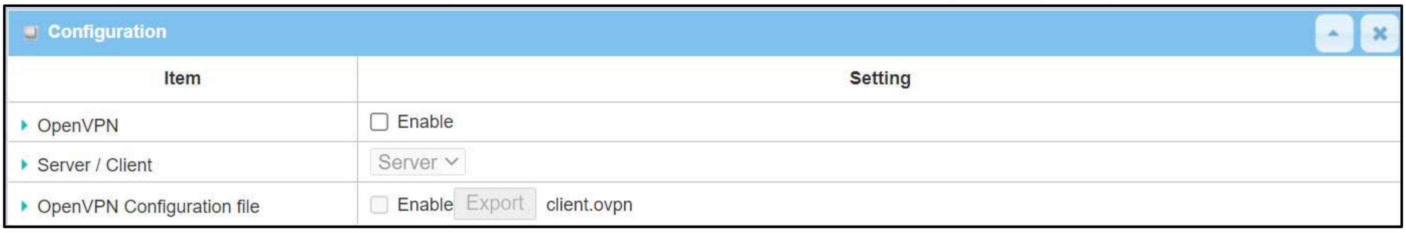
Open VPN Setting

Go to Security > VPN > OpenVPN tab.

The OpenVPN setting allows user to create and configure OpenVPN tunnels.

Enable OpenVPN

Enable OpenVPN and select a configuration, either server or client, for the gateway to operate.



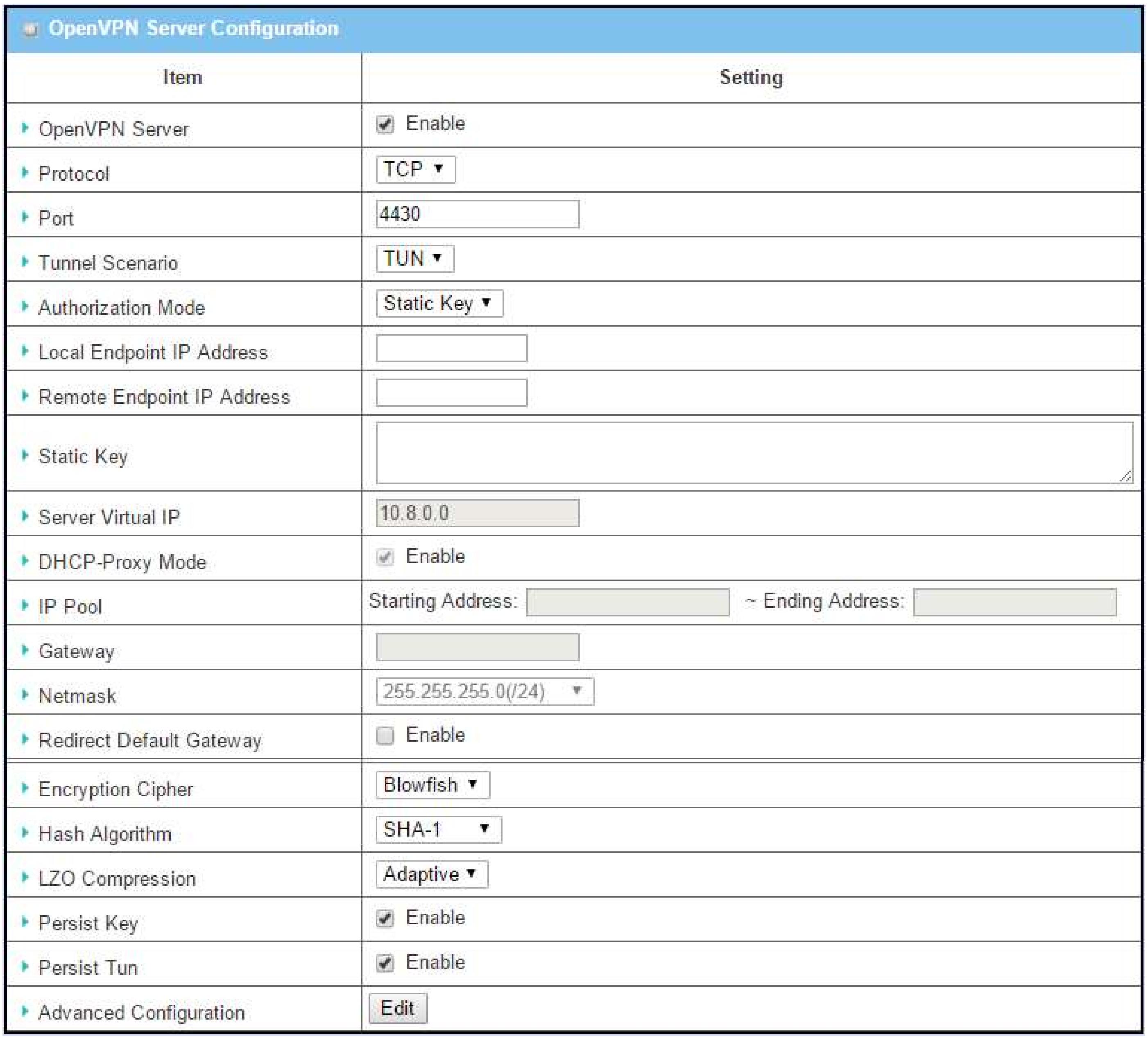
Item	Setting
OpenVPN	□ Enable
Server / Client	Server
OpenVPN Configuration file	□ Enable Export client.ovpn

Configuration		
Item	**Value setting**	**Description**
OpenVPN	Unchecked by default	Check the **Enable** box to activate the OpenVPN function.
Server/ Client	Server Configuration is selected by default.	When **Server** is selected, server configuration will be displayed below for further setup. When **Client** is selected, you can specify the client settings in another client configuration window.
OpenVPN Configuration file	Unchecked by default	Check the box to enable the uploading of an existing configuration file to an interface. Click the **Upgrade** button, the select the file to be uploaded.

As an OpenVPN Server

If **Server** is selected, an OpenVPN Server Configuration screen will appear. **OpenVPN Server Configuration** window lets you enable the OpenVPN server function and specify the virtual IP address of OpenVPN server when remote OpenVPN clients dial in, and the authentication protocol.

The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.



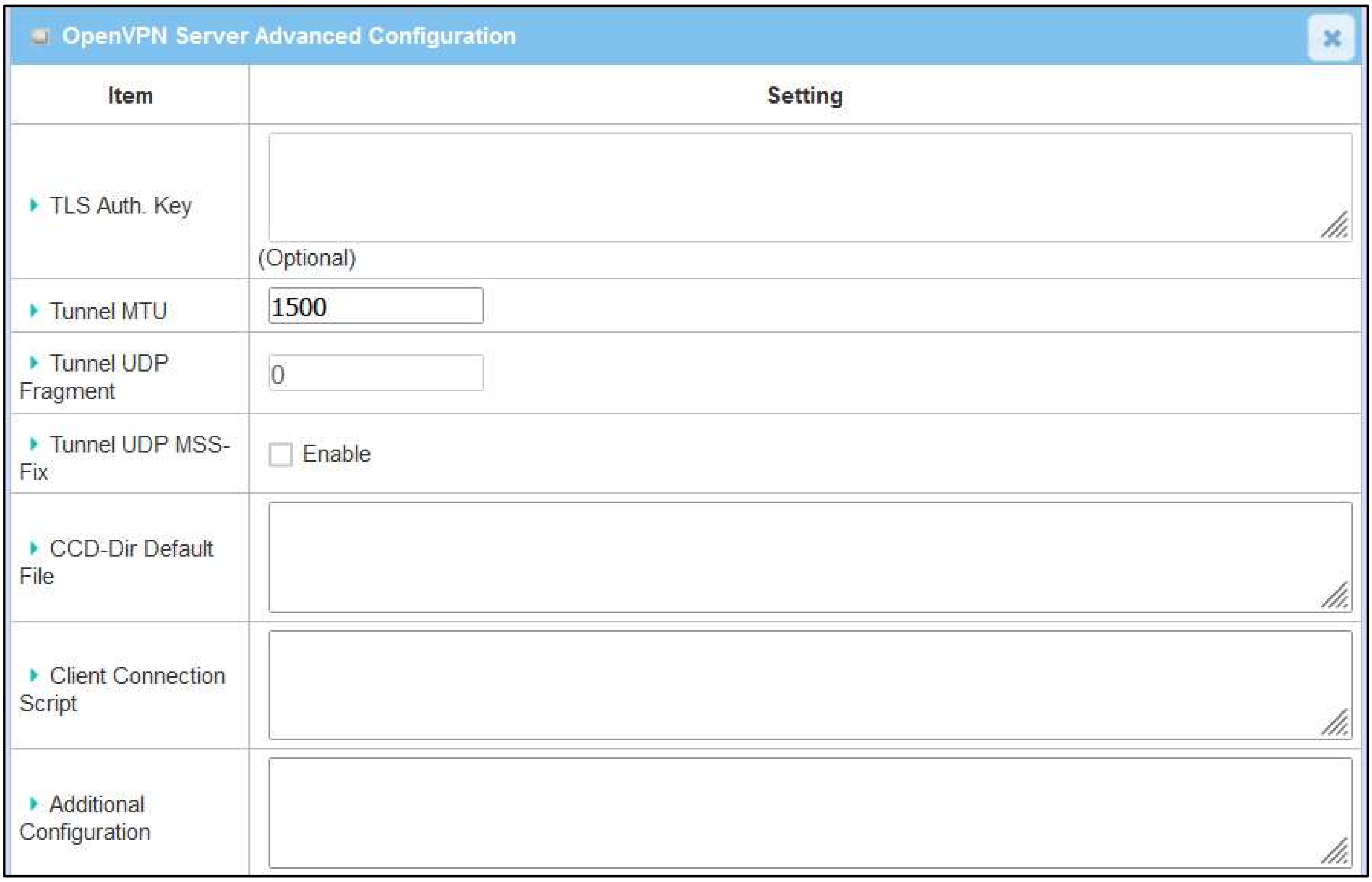
OpenVPN Server Configuration

Item	Setting
OpenVPN Server	☑ Enable
Protocol	TCP ▾
Port	4430
Tunnel Scenario	TUN ▾
Authorization Mode	Static Key ▾
Local Endpoint IP Address	
Remote Endpoint IP Address	
Static Key	
Server Virtual IP	10.8.0.0
DHCP-Proxy Mode	☑ Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24) ▾
Redirect Default Gateway	☐ Enable
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Persist Key	☑ Enable
Persist Tun	☑ Enable
Advanced Configuration	Edit

OpenVPN Server Configuration		
Item	**Value setting**	**Description**
OpenVPN Server	Unchecked by default	Click the **Enable** to activate OpenVPN Server functions.
Protocol	1. Required setting 2. By default **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or UDP** -> TCP will be used to access the OpenVPN Server, and **Port** will be set to 4430. • Select **UDP** -> UDP will be used to access the OpenVPN Server, and **Port** will be set to 1194.
Port	1. Required setting 2. By default **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server. ***Value Range***: 1 ~ 65535.
Tunnel Scenario	1. Required setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for connecting to the OpenVPN Server. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Authorization Mode	1. Required setting 2. By default **Static Key** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** -> OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert.** can be generated in Certificate. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Server Cert.** can be generated in Certificate. Refer to **Object Definition** > **Certificate** > **My Certificate**. • **Static Key** ->The OpenVPN will use static key (pre-shared) authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.
Local Endpoint IP Address	Required setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	Required setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	Required setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	Required setting	Specify the **Server Virtual IP**. ***Value Range***: The IP format is 10.y.0.0, the range of y is 1~254. Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.
DHCP-Proxy Mode	1. Required setting 2. The box is checked by default.	Check the **Enable** box to activate the **DHCP-Proxy Mode**. Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	Required setting	Specify the virtual **IP pool** setting for the OpenVPN server. Specify the **Starting Address** and **Ending Address** as the IP address pool for the OpenVPN clients. Note: IP Pool will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).

Gateway	Required setting	Specify the **Gateway** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Note: Gateway will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Netmask	By default **- select one -** is selected.	Specify the **Netmask** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. ***Value Range***: 255.255.255.0/24 (only support class C) Note_1: Netmask will be available when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled). Note_2: Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Gateway	1. Optional setting. 2. Unchecked by default	Check the **Enable** box to activate the **Redirect Default Gateway** function.
Encryption Cipher	1. Required setting. 2. By default **Blowfish** is selected.	Specify the **Encryption Cipher** from the dropdown list. Select from **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm** from the dropdown list. Select from **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. Select from **Adaptive/YES/NO/Default.**
Persis Key	1. Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.

When **Advanced Configuration** is selected, an OpenVPN Server Advanced Configuration screen will appear.

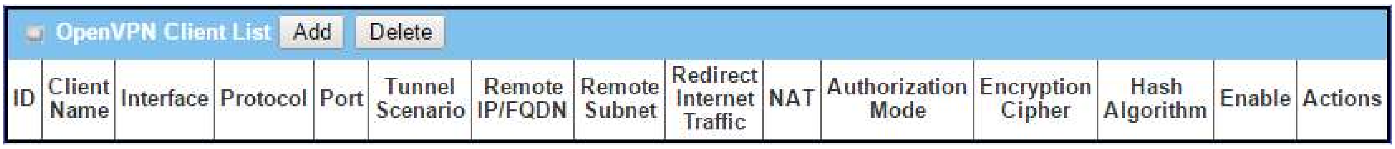


Item	Setting
TLS Auth. Key	(Optional)
Tunnel MTU	1500
Tunnel UDP Fragment	0
Tunnel UDP MSS-Fix	□ Enable
CCD-Dir Default File	
Client Connection Script	
Additional Configuration	

OpenVPN Server Advanced Configuration		
Item	**Value setting**	**Description**
TLS Auth. Key	1. Optional setting. 2. String format: any text	Specify the **TLS Auth. Key.** Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Tunnel MTU	1. Required setting 2. Default is **1500**	Specify the **Tunnel MTU.** ***Value Range***: 0 ~ 1500.
Tunnel UDP Fragment	1. Required setting 2. Default is **1500**	Specify the **Tunnel UDP Fragment.** By default, it is equal to **Tunnel MTU**. ***Value Range***: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	1. Optional setting. 2. Unchecked by default	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** Function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	1. Optional setting. 2. String format: any text	Specify the **CCD-Dir Default File.** ***Value Range***: 0 ~ 256 characters.
Client Connection Script	1. Optional setting. 2. String format: any text	Specify the **Client Connection Script.** ***Value Range***: 0 ~ 256 characters.
Additional Configuration	1. Optional setting. 2. String format: any text	Specify the **Additional Configuration.** ***Value Range***: 0 ~ 256 characters.

As an OpenVPN Client

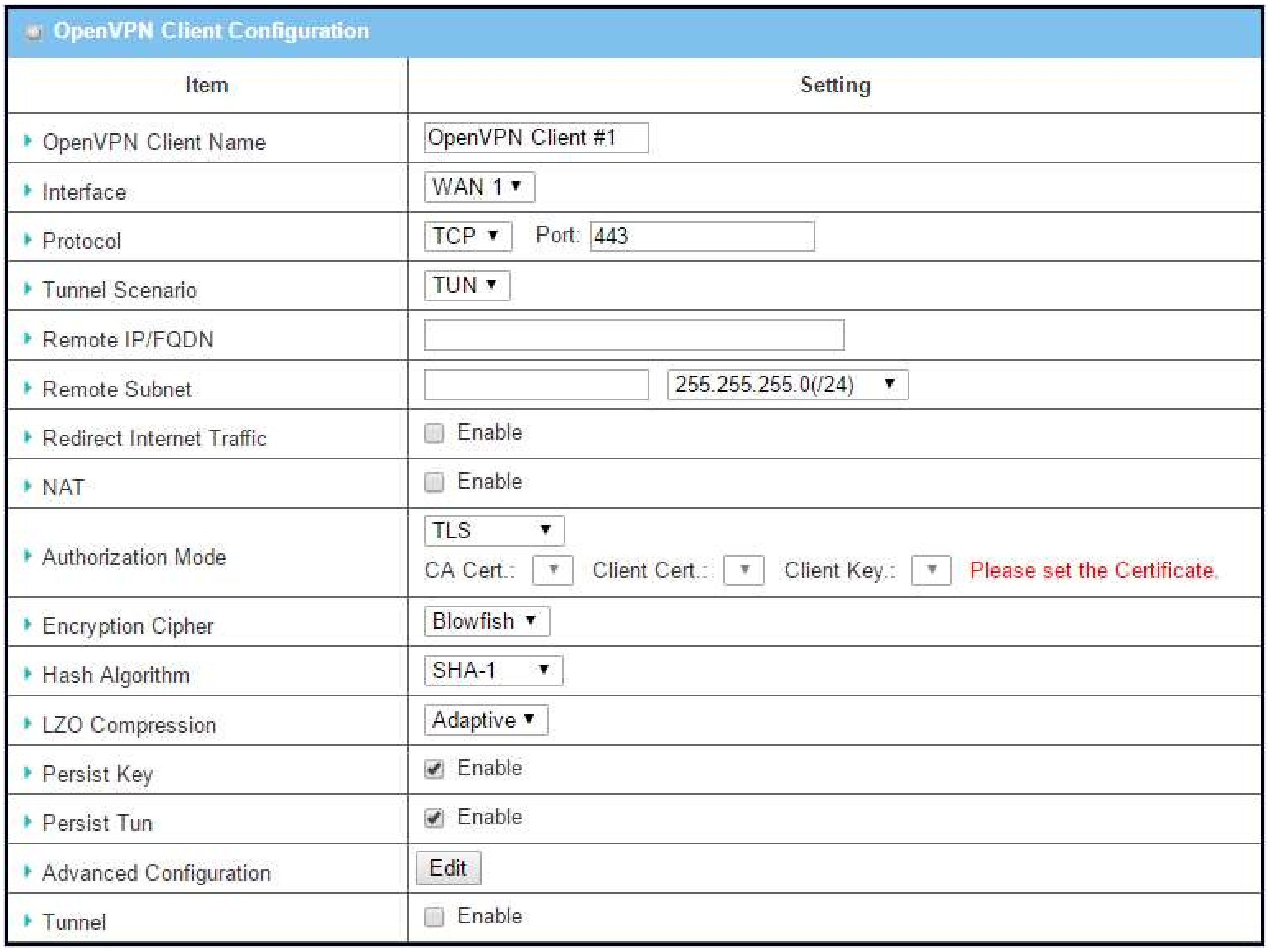
If **Client** is selected, an OpenVPN Client List screen will appear.



OpenVPN Client List

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

When **Add** button is applied, the OpenVPN Client Configuration screen will appear. **OpenVPN Client Configuration** window lets you specify the required parameters for an OpenVPN VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Tunnel Scenario", "Remote IP/FQDN", "Remote Subnet", "Authorization Mode", "Encryption Cipher", "Hash Algorithm" and tunnel activation.



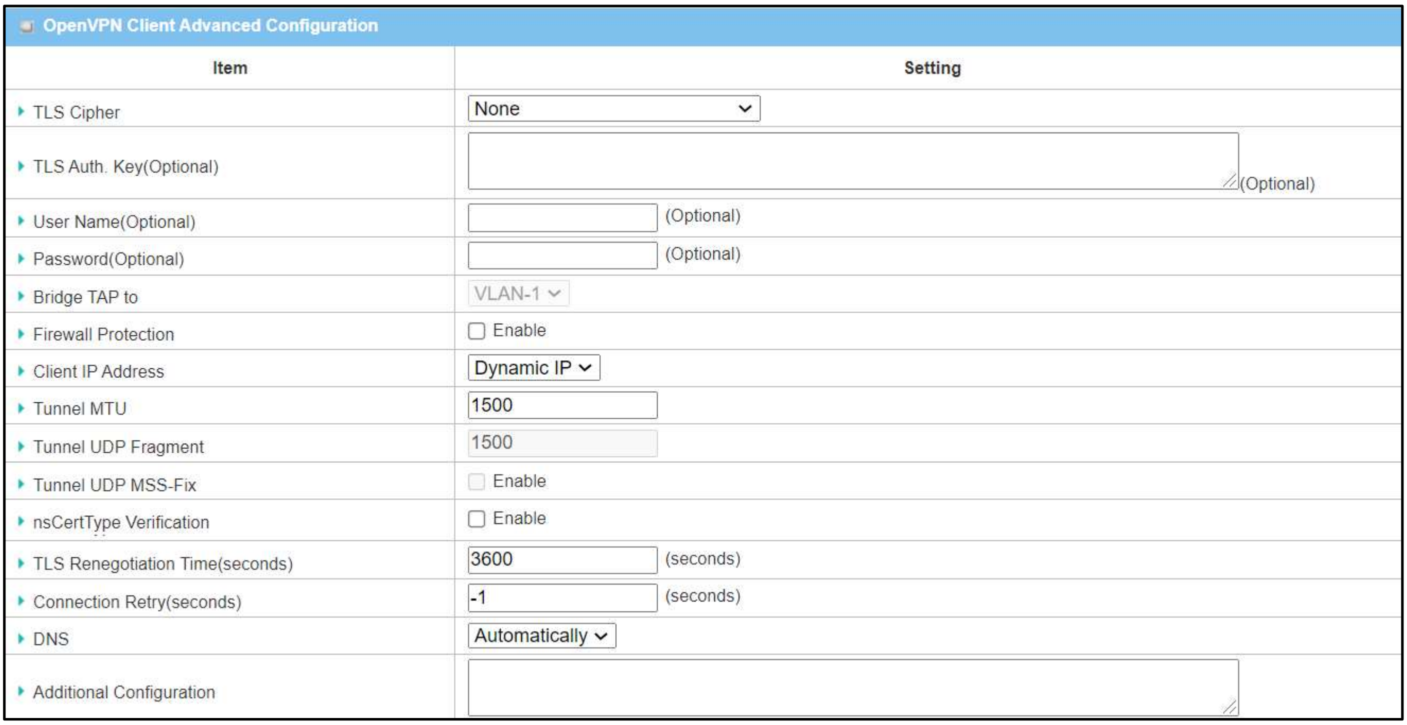
OpenVPN Client Configuration

Item	Setting
OpenVPN Client Name	OpenVPN Client #1
Interface	WAN 1 ▾
Protocol	TCP ▾ Port: 443
Tunnel Scenario	TUN ▾
Remote IP/FQDN	
Remote Subnet	255.255.255.0(/24) ▾
Redirect Internet Traffic	□ Enable
NAT	□ Enable
Authorization Mode	TLS ▾ CA Cert.: ▾ Client Cert.: ▾ Client Key.: ▾ Please set the Certificate.
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Persist Key	☑ Enable
Persist Tun	☑ Enable
Advanced Configuration	Edit
Tunnel	□ Enable

OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	Required setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list. ***Value Range***: 1 ~ 32 characters.
Interface	1. Required setting 2. By default **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	1. Required setting 2. By default **TCP** is selected.	Define the **Protocol** for the OpenVPN Client. • Select **TCP** -> OpenVPN will use TCP, and **Port** will be set to 443. • Select **UDP** -> OpenVPN will use UDP, and **Port** will be set to 1194.
Port	1. Required setting 2. By default **443** is set.	Specify the **Port** for the OpenVPN Client to use. ***Value Range***: 1 ~ 65535.
Tunnel Scenario	1. Required setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	Required setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Enter the IP address or FQDN.
Remote Subnet	Required setting	Specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Redirect Internet Traffic	1. Optional setting. 2. Unchecked by default	Check the **Enable** box to activate the **Redirect Internet Traffic** function.
NAT	1. Optional setting. 2. Unchecked by default	Check the **Enable** box to activate the **NAT** function.
Authorization Mode	1. Required setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** can be selected in Trusted CA Certificate List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Client Cert.** can be selected in Local Certificate List. Refer to **Object Definition** > **Certificate** > **My Certificate**. **Client Key** can be selected in Trusted Client key List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. • **Static Key** -> OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed.
Local Endpoint IP Address	Required setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	Required setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is

		chosen in Authorization Mode.
Static Key	Required setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** Select from **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm.** Select from **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. Select from **Adaptive/YES/NO/Default.**
Persis Key	1. Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. Optional setting. 2. Box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Tunnel	Unchecked by default	Check the **Enable** box to activate this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.

When **Advanced Configuration** is selected, an OpenVPN Client Advanced Configuration screen will appear.



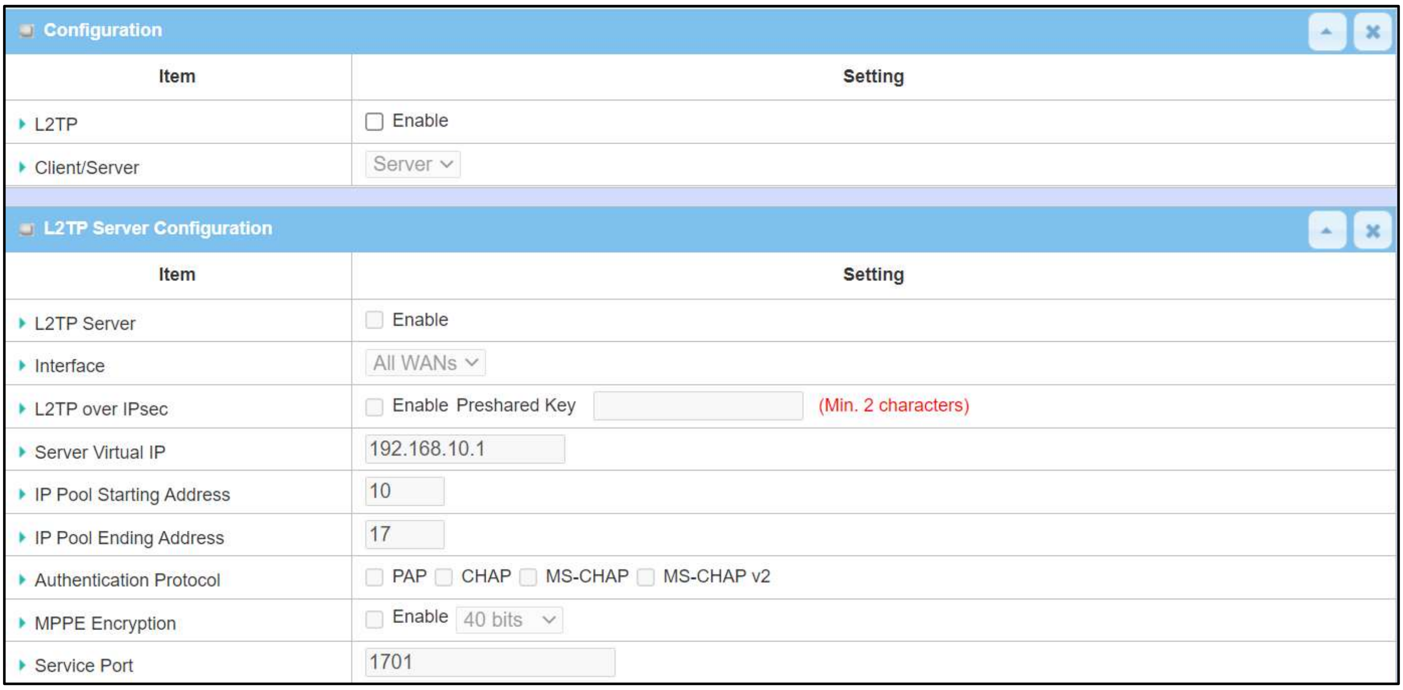
OpenVPN Client Advanced Configuration

Item	Setting
TLS Cipher	None
TLS Auth. Key(Optional)	(Optional)
User Name(Optional)	(Optional)
Password(Optional)	(Optional)
Bridge TAP to	VLAN-1
Firewall Protection	□ Enable
Client IP Address	Dynamic IP
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
nsCertType Verification	□ Enable
TLS Renegotiation Time(seconds)	3600 (seconds)
Connection Retry(seconds)	-1 (seconds)
DNS	Automatically
Additional Configuration	

OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. Required setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. Select from **None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. Optional setting. 2. String format: any text	Specify the **TLS Auth. Key** for connecting to an OpenVPN server, if the server requires it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	Optional setting.	Enter the **User account** for connecting to an OpenVPN server, if the server requires it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Password	Optional setting.	Enter the **Password** for connecting to an OpenVPN server, if the server requires it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Bridge TAP to	By default **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a certain local network interface or VLAN. Note: **Bridge TAP to** will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
Firewall Protection	Unchecked by default	Check the box to activate the **Firewall Protection** function.

		Note: Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client. Select from **Dynamic IP/Static IP.**
Tunnel MTU	1. Required setting 2. Default is 1500	Specify the value of **Tunnel MTU.** ***Value Range***: 0 ~ 1500.
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** ***Value Range***: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	Unchecked by default	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	Unchecked by default	Check the **Enable** box to activate the **nsCerType Verification** function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** ***Value Range***: -1 ~ 86400.
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that there is no need to execute connection retry. ***Value Range***: -1 ~ 86400, -1 means no retry is required.
DNS	By default **Automatically** is selected	Specify the setting of **DNS.** Select from **Automatically/Manually.**
Additional Configuration	Blank by default	Specify the **Additional Configuration.** ***Value Range***: 0 ~ 256 characters.

6.1.3 L2TP



Configuration

Item	Setting
L2TP	□ Enable
Client/Server	Server

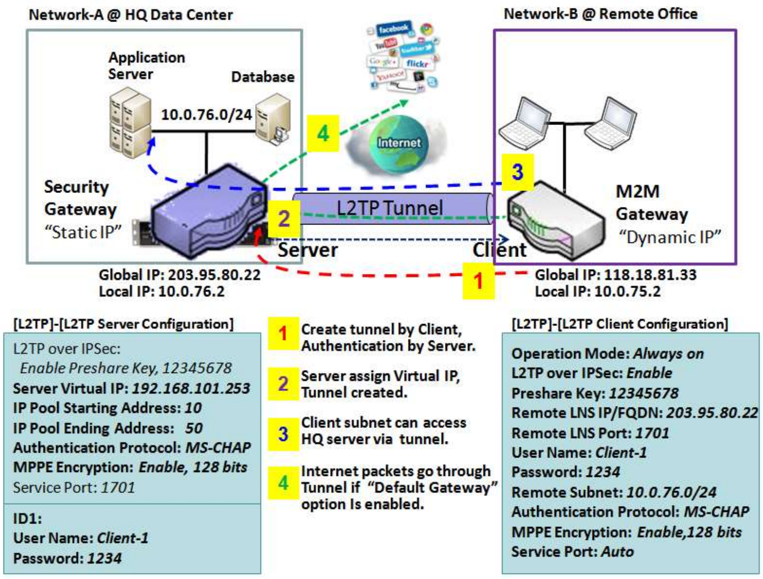
L2TP Server Configuration

Item	Setting
L2TP Server	□ Enable
Interface	All WANs
L2TP over IPsec	□ Enable Preshared Key (Min. 2 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits
Service Port	1701

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. This Gateway can behave as an L2TP server and an L2TP client both at the same time.

L2TP Server: It must have a static IP or a FQDN for clients to create L2TP tunnels. It also maintains “User Account list” (user name/ password) for client login authentication; There is a virtual IP pool to assign virtual IP to each connected L2TP client.

L2TP Client: It can be mobile users or gateways in remote offices with dynamic IP. To set up a tunnel, add “user name”, “password” and server’s global IP. In addition, identify the operation mode for each tunnel as main connection, failover for another tunnel, or load balance tunnel to increase overall bandwidth. Select “Default Gateway” or “Remote Subnet” for packet flow. You can also define what kind of traffic will pass through the L2TP tunnel in the “Default Gateway / Remote Subnet” parameter.



[L2TP]-[L2TP Server Configuration]

L2TP over IPSec:
Enable Preshare Key, 12345678
Server Virtual IP: ***192.168.101.253***
IP Pool Starting Address: ***10***
IP Pool Ending Address: ***50***
Authentication Protocol: ***MS-CHAP***
MPPE Encryption: ***Enable, 128 bits***
Service Port: *1701*

ID1:
User Name: ***Client-1***
Password: ***1234***

1 Create tunnel by Client, Authentication by Server.

2 Server assign Virtual IP, Tunnel created.

3 Client subnet can access HQ server via tunnel.

4 Internet packets go through Tunnel if “Default Gateway” option Is enabled.

[L2TP]-[L2TP Client Configuration]

Operation Mode: ***Always on***
L2TP over IPSec: ***Enable***
Preshare Key: ***12345678***
Remote LNS IP/FQDN: ***203.95.80.22***
Remote LNS Port: ***1701***
User Name: ***Client-1***
Password: ***1234***
Remote Subnet: ***10.0.76.0/24***
Authentication Protocol: ***MS-CHAP***
MPPE Encryption: ***Enable,128 bits***
Service Port: ***Auto***

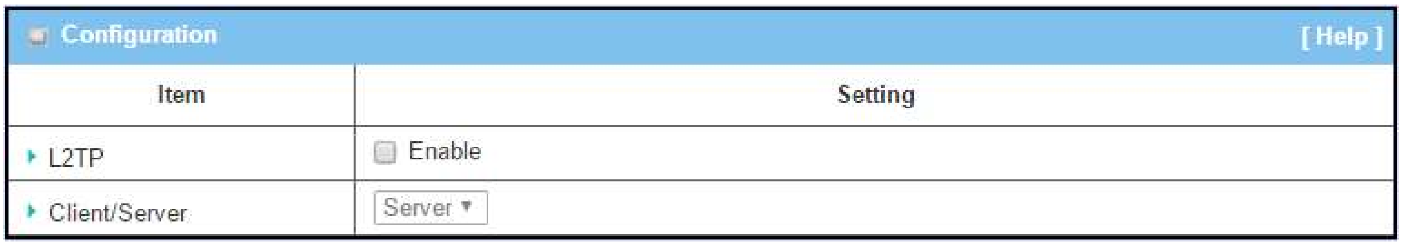
For the L2TP client peer, a Remote Subnet item is required for the Intranet of L2TP server peer. At L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP tunnel. Others will be transferred based on current routing policy of the gateway at L2TP client peer. But, if 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the L2TP client peer, and all packets, including the Internet accessing of L2TP client peer, will go through the established L2TP tunnel. That means the remote L2TP server peer controls the flow of any packets from the L2TP client peer. Those packets come through the L2TP tunnel.

L2TP Setting

Go to Security > VPN > L2TP tab.

The L2TP setting allows user to create and configure L2TP tunnels.

Enable L2TP



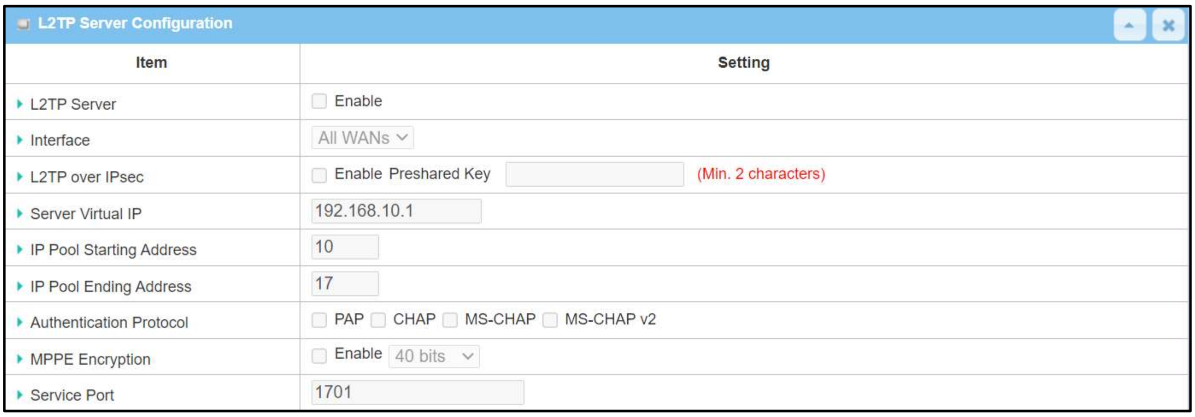
Configuration [Help]

Item	Setting
L2TP	□ Enable
Client/Server	Server ▾

Enable L2TP Window		
Item	**Value setting**	**Description**
L2TP	Unchecked by default	Click the **Enable** box to activate L2TP function.
Client/Server	Required setting	Specify the role of L2TP. Select **Server** or **Client** role for the gateway to take. Below are the configuration windows for L2TP Server and for Client.
Save	N/A	Click **Save** button to save the settings

As a L2TP Server

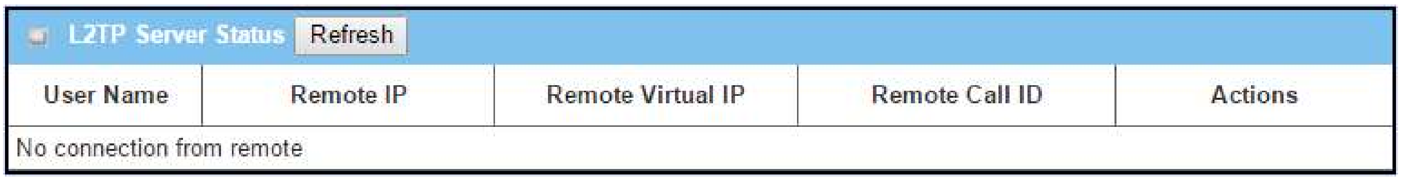
When **Server** is selected in Client/Server, the L2TP server Configuration will appear.



L2TP Server Configuration

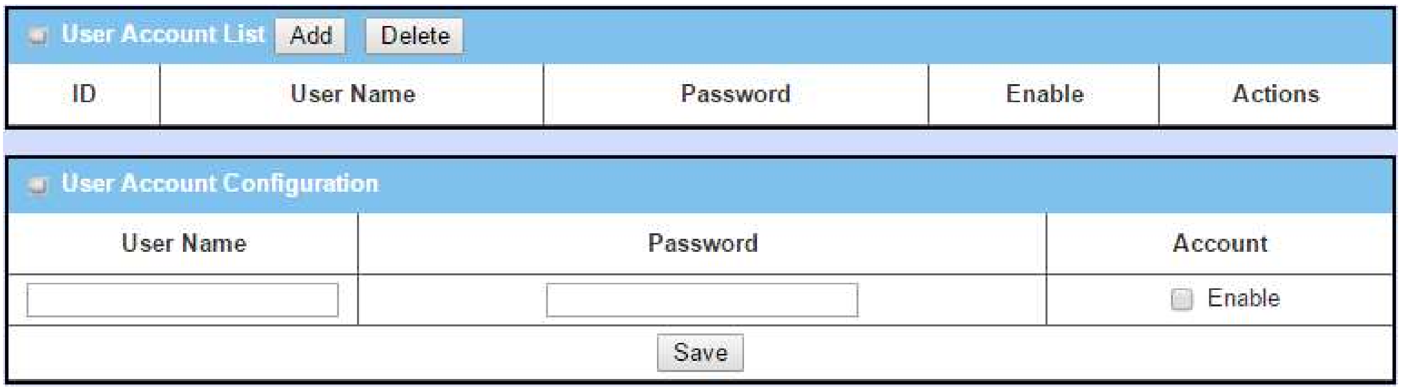
Item	Setting
L2TP Server	□ Enable
Interface	All WANs ▾
L2TP over IPsec	□ Enable Preshared Key (Min. 2 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▾
Service Port	1701

L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP Server	Unchecked by default	Click the **Enable** box to activate L2TP server
L2TP over IPSec	Unchecked by default	Click the **Enable** box to enable L2TP over IPsec and need to fill in the Pre-shared Key (8~32 characters).
Interface	Default is All Wans	Select the interface for the L2TP server.
Server Virtual IP	Required setting	Specify the L2TP server Virtual IP.
IP Pool Starting Address	1. Required setting **2. 10 is set by default.**	Specify the L2TP server starting IP of virtual IP pool. Value Range: 1 ~ 254.
IP Pool Ending Address	1. Required setting **2. 17 is set by default.**	Specify the L2TP server ending IP of virtual IP pool. ***Value Range***: >= Starting Address, and < (Starting Address + 8) or 254.
Authentication Protocol	Required setting	Select single or multiple Authentication Protocols for the L2TP server with which to authenticate L2TP clients. Available authentication protocols are **PAP** / **CHAP** / **MS-CHAP** / **MS-CHAP v2**.
MPPE Encryption	Required setting	Specify whether to support MPPE Protocol. Click the **Enable** box to enable MPPE and from dropdown box to select **40 bits** / **56 bits** / **128 bits**. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP** / **CHAP** options will not be available.
Service Port	Required setting	Specify the **Service Port** which L2TP server will use. ***Value Range***: 1 ~ 65535.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recover the configuration.



User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

L2TP Server Status		
Item	**Value setting**	**Description**
L2TP Server Status	N/A	Displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of connected L2TP clients. Click the **Refresh** button to renew the L2TP client information.



User Account List Add Delete

ID	User Name	Password	Enable	Actions

User Account Configuration

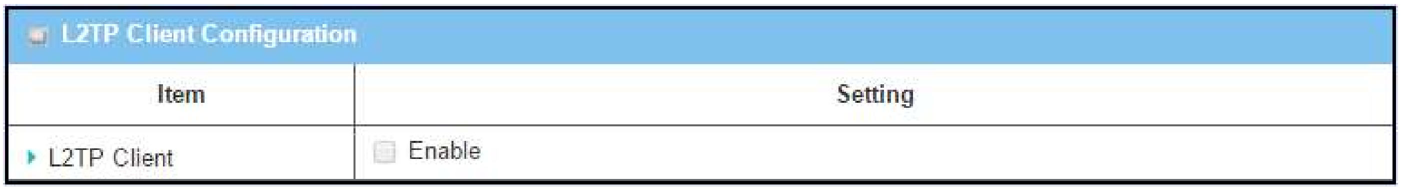
User Name	Password	Account
		□ Enable

Save

User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max. of 10 user accounts	This is the L2TP authentication user account entry. You can create and add accounts for remote clients to establish L2TP VPN connection to the gateway device. Click **Add** button to add a user account. Enter the User name and password. Then check the **enable** box to enable the user. Click **Save** button to save the new user account. The selected user account can permanently be deleted by clicking the **Delete** button. ***Value Range***: 1 ~ 32 characters.

As a L2TP Client

When Client is selected in Client/Server, the buttons to add and delete L2TP client list will become active.

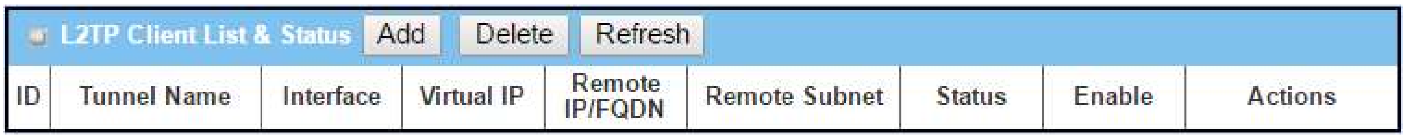


L2TP Client Configuration

Item	Setting
L2TP Client	□ Enable

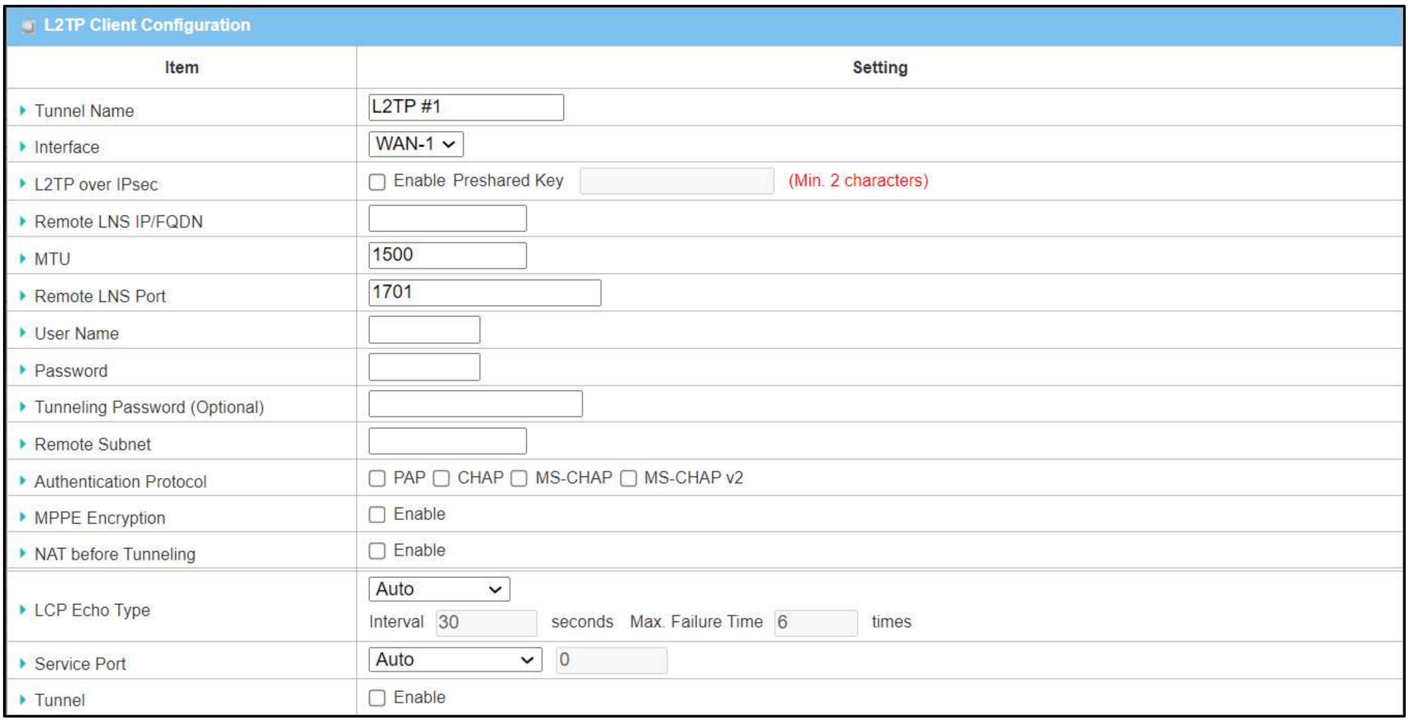
L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	Unchecked by default	Check the **Enable** box to enable L2TP client role of the gateway.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

Create/Edit L2TP Client



ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

When **Add** button is applied, a series of configuration screen will appear. You can add up to 8 L2TP Clients.

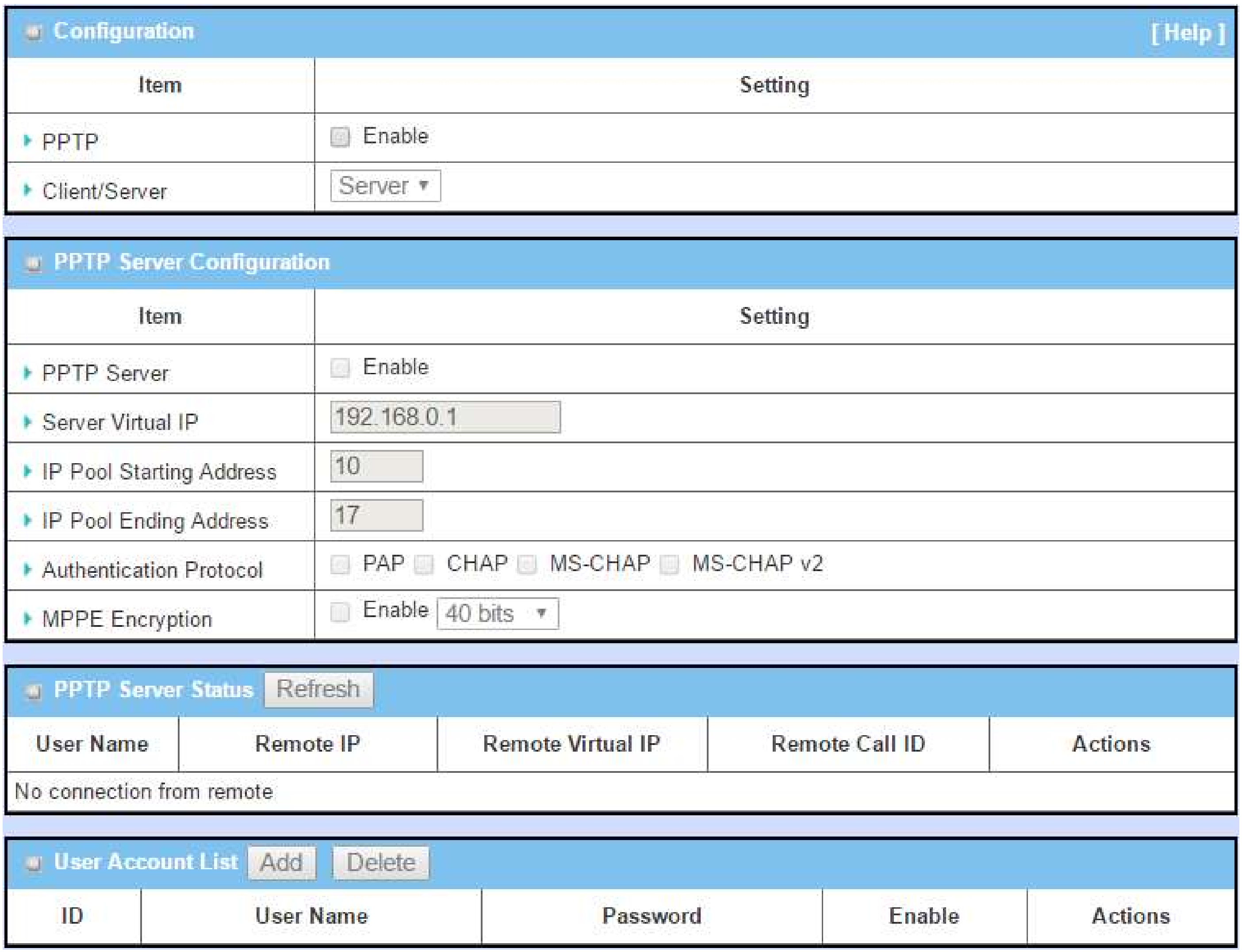


Item	Setting
Tunnel Name	L2TP #1
Interface	WAN-1
L2TP over IPsec	□ Enable Preshared Key (Min. 2 characters)
Remote LNS IP/FQDN	
MTU	1500
Remote LNS Port	1701
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable
NAT before Tunneling	□ Enable
LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
Service Port	Auto 0
Tunnel	□ Enable

L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
Tunnel Name	Required setting	Enter a tunnel name. ***Value Range***: 1 ~ 32 characters.
Interface	Required setting	Define the selected interface to be the used for this L2TP tunnel (**WAN-1** is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. **WAN-2).**
L2TP over IPSec	Unchecked by default	Check the **Enable** box to activate L2TP over IPsec, and further specify a Pre-shared Key (8~32 characters).
Remote LNS IP/FQDN	Required setting	Enter the public IP address or the FQDN of the L2TP server.
MTU	Default is 1500	Enter the maximum transmission unit
Remote LNS Port	1. Required setting 2. Default is **1701**	Enter the Remote LNS Port for this L2TP tunnel. ***Value Range***: 1 ~ 65535.

User Name	Required setting	Enter the **User Name** for this L2TP tunnel to be authenticated when connect to L2TP server. ***Value Range***: 1 ~ 32 characters.
Password	Required setting	Enter the **Password** for this L2TP tunnel to be authenticated when connect to L2TP server.
Tunneling Password(Optional)	Unchecked by default	Enter the **Tunneling Password** for this L2TP tunnel to authenticate.
Remote Subnet	Required setting	Specify the remote subnet for this L2TP tunnel to reach the L2TP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of L2TP VPN server. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at L2TP client peer. If you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peers, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flow of any packets from the L2TP client peer.
Authentication Protocol	1. Required setting 2. Unchecked by default	Specify one ore multiple **Authentication Protocol** for this L2TP tunnel. Available authentication methods are **PAP** / **CHAP** / **MS-CHAP** / **MS-CHAP v2**.
MPPE Encryption	1. Unchecked by default 2. Optional setting	Specify whether L2TP server supports the **MPPE Protocol**. Click the **Enable** box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP** / **CHAP** options will not be available.
NAT Before Tunneling	Unchecked by default	Click the checkbox to enable network address translation before tunneling.
LCP Echo Type	1. Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel. Select from **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. **Disable**: disable the LCP Echo. ***Value Range***: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Service Port	Required setting	Specify the **Service Port** for this L2TP tunnel to use. It can be **Auto**, **(1701) for Cisco)**, or **User-defined**. **Auto**: The system determines the service port. **1701 (for Cisco):** The system uses port 1701 for connecting with CISCO L2TP Server. **User-defined:** Enter the service port. The default value is 0. ***Value Range***: 0 ~ 65535.
Tunnel	Unchecked by default	Check the **Enable** box to enable this L2TP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

6.1.4 PPTP



Configuration [Help]

Item	Setting
PPTP	□ Enable
Client/Server	Server ▾

PPTP Server Configuration

Item	Setting
PPTP Server	□ Enable
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▾

PPTP Server Status Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

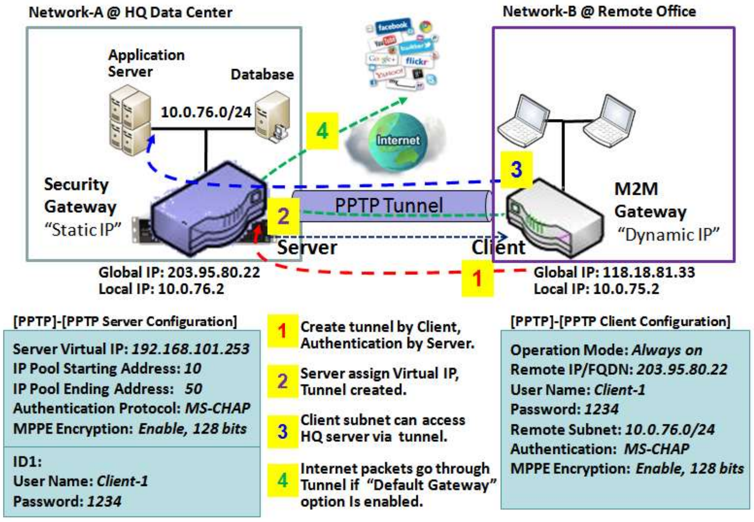
User Account List Add Delete

ID	User Name	Password	Enable	Actions

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. It is a client-server based technology. There are various levels of authentication and encryption for PPTP tunneling, usually natively as standard features of the Windows PPTP stack. The security gateway can play either "PPTP Server" role or "PPTP Client" role for a PPTP VPN tunnel, or both at the same time for different tunnels. PPTP tunnel process is nearly the same as L2TP.

PPTP Server: It must have a static IP or a FQDN for clients to create PPTP tunnels. It also maintains “User Account list” (user name / password) for client login authentication; There is a virtual IP pool to assign virtual IP to each connected PPTP client.

PPTP Client: It can be mobile users or gateways in remote offices with dynamic IP. To set up a tunnel, add “user name", "password" and server's global IP. In addition, it is required to identify the operation mode for each tunnel as main connection, failover for another tunnel, or load balance tunnel to increase overall bandwidth. Select "Default Gateway" or "Remote Subnet" for packet flow. You can also define what kind of traffic will pass through the PPTP tunnel in the "Default Gateway / Remote Subnet" parameter.



[PPTP]-[PPTP Server Configuration]

Server Virtual IP: *192.168.101.253*
IP Pool Starting Address: *10*
IP Pool Ending Address: *50*
Authentication Protocol: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

ID1:
User Name: *Client-1*
Password: *1234*

1 Create tunnel by Client, Authentication by Server.

2 Server assign Virtual IP, Tunnel created.

3 Client subnet can access HQ server via tunnel.

4 Internet packets go through Tunnel if "Default Gateway" option Is enabled.

[PPTP]-[PPTP Client Configuration]

Operation Mode: *Always on*
Remote IP/FQDN: *203.95.80.22*
User Name: *Client-1*
Password: *1234*
Remote Subnet: *10.0.76.0/24*
Authentication: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

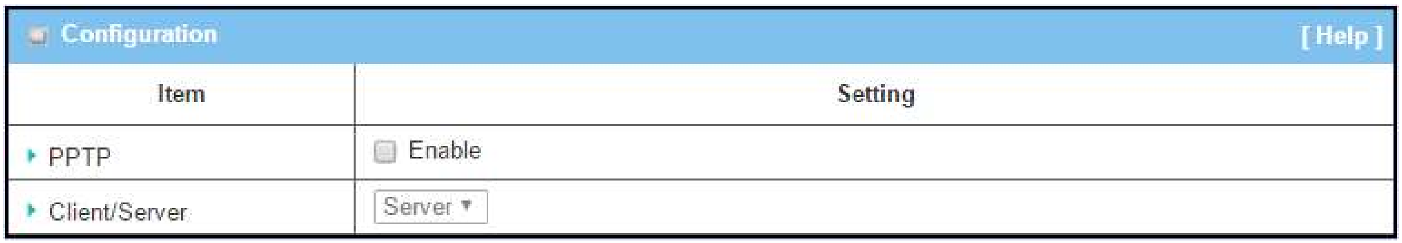
For the PPTP client peer, a Remote Subnet item is required. It is for the Intranet of PPTP server peer. At PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP tunnel. Others will be transferred based on current routing policy of the gateway at PPTP client peer. But, if 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the PPTP client peer, and all packets, including the Internet accessing of PPTP client peers, will go through the established PPTP tunnel. That means the remote PPTP server peer controls the flow of any packets from the PPTP client peer.

PPTP Setting

Go to Security > VPN > PPTP tab.

The PPTP setting allows user to create and configure PPTP tunnels.

Enable PPTP



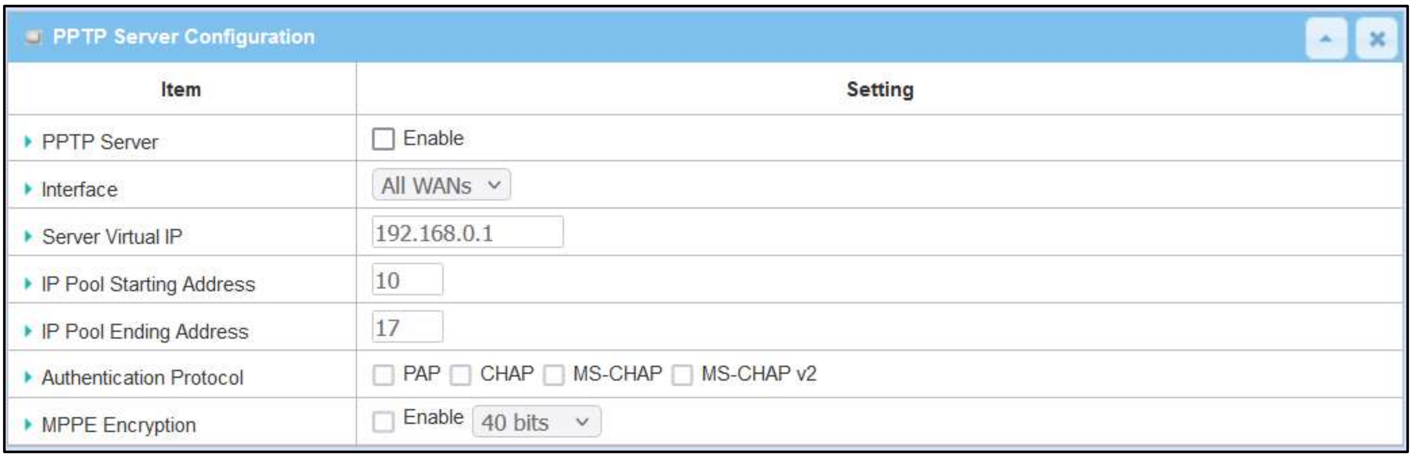
Configuration [Help]

Item	Setting
PPTP	□ Enable
Client/Server	Server ▾

Enable PPTP Window		
Item	**Value setting**	**Description**
PPTP	Unchecked by default	Click the **Enable** box to activate PPTP function.
Client/Server	Required setting	Specify the role of PPTP. Select **Server** or **Client** role. Below are the configuration windows for PPTP Server and for Client.
Save	N/A	Click **Save** button to save the settings.

As a PPTP Server

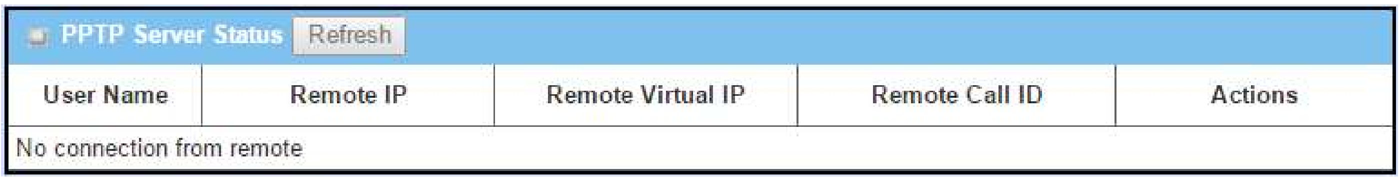
The gateway supports up to a maximum of 10 PPTP user accounts.
When **Server** in the Client/Server field is selected, the PPTP server configuration window will appear.



PPTP Server Configuration

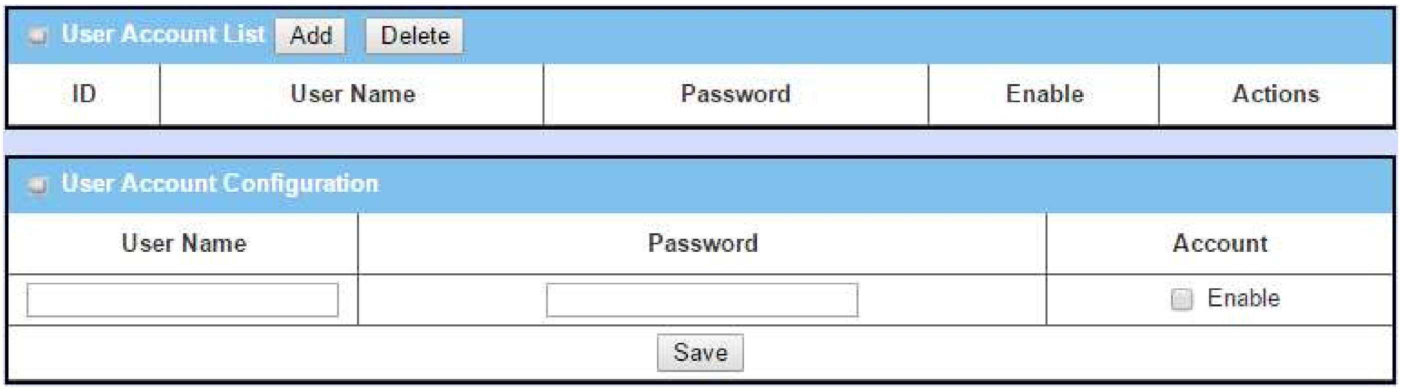
Item	Setting
PPTP Server	□ Enable
Interface	All WANs ⌄
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ⌄

PPTP Server Configuration Window		
Item	**Value setting**	**Description**
PPTP Server	Unchecked by default	Check the **Enable** box to enable PPTP server role of the gateway.
Interface	1. Required setting 2. WAN1 is selected by default	Define the selected interface to be the used for this PPTP tunnel (**WAN-1** is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. **WAN-2).**
Server Virtual IP	1. Required setting 2. Default is 192.168.0.1	Specify the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	1. Required setting 2. Default is **10**	This is the PPTP server's Virtual IP DHCP server. User can specify the first IP address for the subnet from which the PPTP client's IP address will be assigned. Value Range: 1 ~ 254.
IP Pool Ending Address	1. Required setting 2. Default is **17**	This is the PPTP server's Virtual IP DHCP server. User can specify the last IP address for the subnet from which the PPTP client's IP address will be assigned. ***Value Range***: >= Starting Address, and < (Starting Address + 8) or 254.
Authentication Protocol	1. Required setting 2. Unchecked by default	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols are **PAP** / **CHAP** / **MS-CHAP** / **MS-CHAP v2**.
MPPE Encryption	1. Required setting 2. Unchecked by default	Specify whether to support MPPE Protocol. Click the **Enable** box to enable MPPE and from dropdown box to select **40 bits** / **56 bits** / **128 bits**. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP** / **CHAP** options will not be available.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.



User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

PPTP Server Status Window		
Item	**Value setting**	**Description**
PPTP Server Status	N/A	Displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected PPTP clients. Click the **Refresh** button to renew the PPTP client information.



User Account List

ID	User Name	Password	Enable	Actions

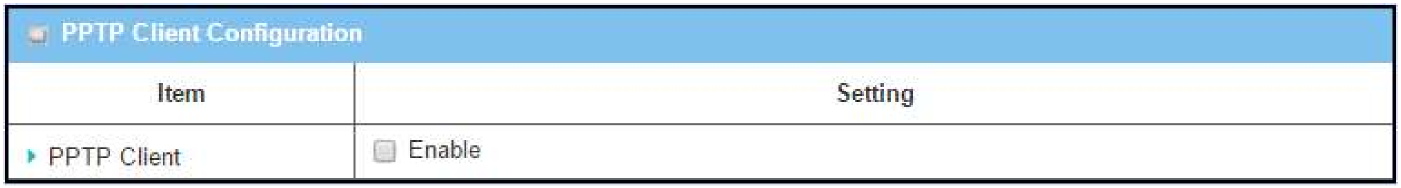
User Account Configuration

User Name	Password	Account
		□ Enable

User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max. of 10 user accounts	This is the PPTP authentication user account entry. You can create and add accounts for remote clients to establish PPTP VPN connection to the gateway device. Click **Add** button to add user account. Enter the User name and password. Then check the **enable** box to enable the user. Click **Save** button to save new user account. The selected user account can permanently be deleted by clicking the **Delete** button. ***Value Range***: 1 ~ 32 characters.

As a PPTP Client

When Client is selected in Client/Server, a series PPTP Client Configuration will appear.

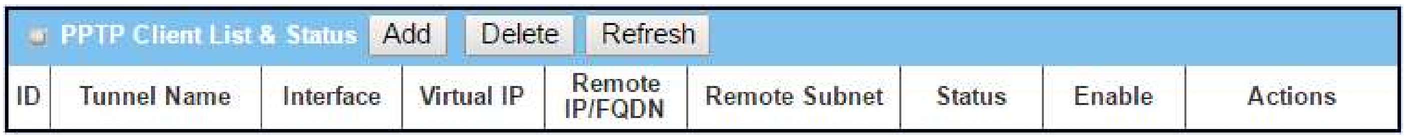


PPTP Client Configuration

Item	Setting
PPTP Client	□ Enable

PPTP Client Configuration		
Item	**Value setting**	**Description**
PPTP Client	Unchecked by default	Check the **Enable** box to enable PPTP client role of the gateway.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

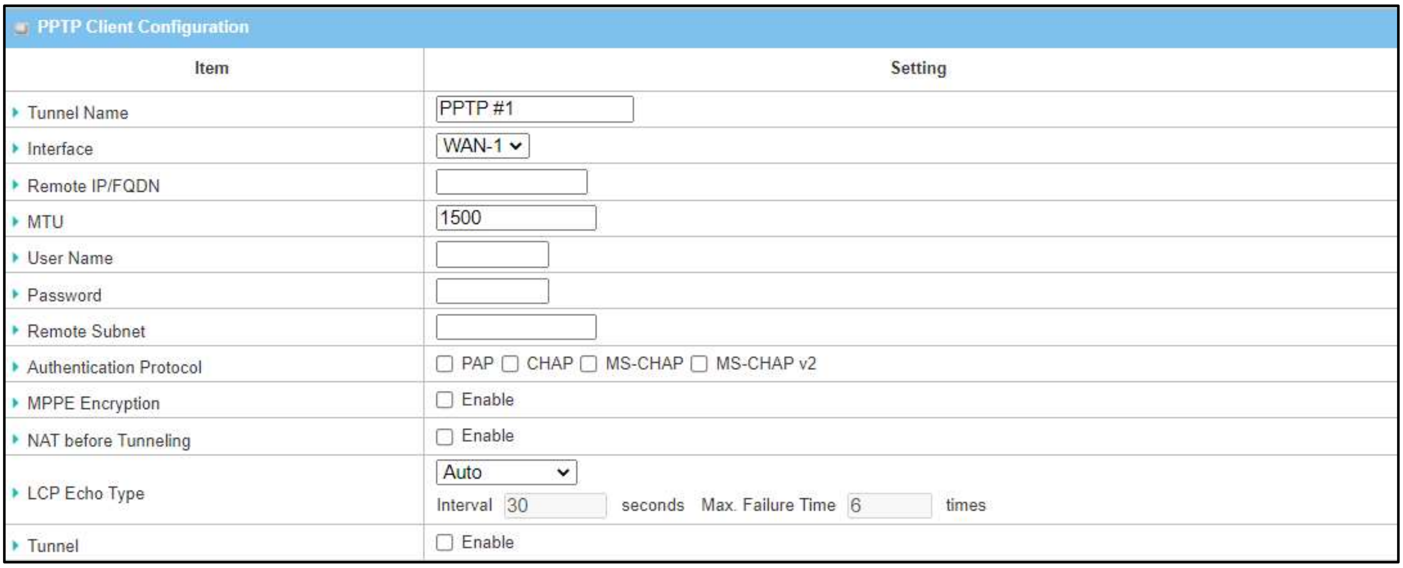
Create/Edit PPTP Client



PPTP Client List & Status

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

When **Add/Edit** button is applied, a series of PPTP Client Configuration screens will appear.



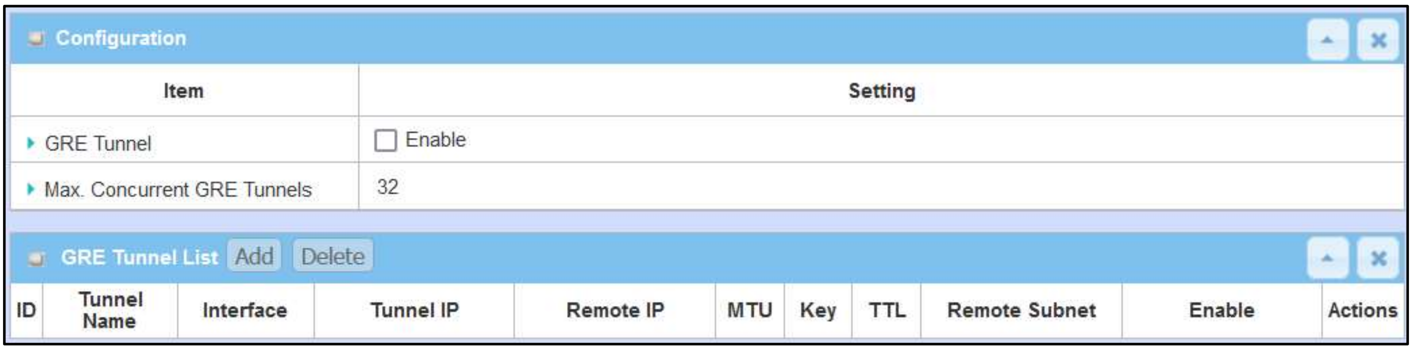
PPTP Client Configuration

Item	Setting
Tunnel Name	PPTP #1
Interface	WAN-1
Remote IP/FQDN	
MTU	1500
User Name	
Password	
Remote Subnet	
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable
NAT before Tunneling	□ Enable
LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
Tunnel	□ Enable

PPTP Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	Required setting	Enter a tunnel name. ***Value Range***: 1 ~ 32 characters.
Interface	1. Required setting 2. WAN1 is selected by default	Define the selected interface to be the used for this PPTP tunnel (**WAN-1** is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. **WAN-2).**
Operation Mode	1. Required setting 2. **Always on** is selected by default	Define operation mode for the PPTP Tunnel. It can be **Always On**, or **Failover**. If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: **Failover** mode is not available for gateways with a single WAN.
Remote IP/FQDN	1. Required setting. 2. Format can be ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
MTU	Default is 1500	Set the maximum transmission unit.
User Name	Required setting	Enter the **User Name** for this PPTP tunnel to be authenticated when connect to PPTP server. ***Value Range***: 1 ~ 32 characters.

Password	Required setting	Enter the **Password** for this PPTP tunnel to be authenticated when connect to PPTP server.
Remote Subnet	Required setting	Specify the remote subnet for this PPTP tunnel to reach PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of PPTP VPN server. At PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. If 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a default gateway setting for the PPTP client peer. All packets, including the Internet accessing of PPTP Client peers, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flow of any packets from the PPTP client peer.
Authentication Protocol	1. Required setting 2. Unchecked by default	Specify one or multiple **Authentication Protocols** for this PPTP tunnel. Available authentication methods are **PAP** / **CHAP** / **MS-CHAP** / **MS-CHAP v2**.
MPPE Encryption	1. Unchecked by default 2. Optional setting	Specify whether PPTP server supports **MPPE Protocol**. Click the **Enable** box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP** / **CHAP** options will not be available.
NAT Before Tunneling	Unchecked by default	Check to enable network address translation before tunneling.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this PPTP tunnel. It can be **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. **Disable**: disable the LCP Echo. ***Value Range***: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Tunnel	Unchecked by default	Check the **Enable** box to enable this PPTP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

6.1.5 GRE



Configuration

Item	Setting
GRE Tunnel	□ Enable
Max. Concurrent GRE Tunnels	32

GRE Tunnel List Add Delete

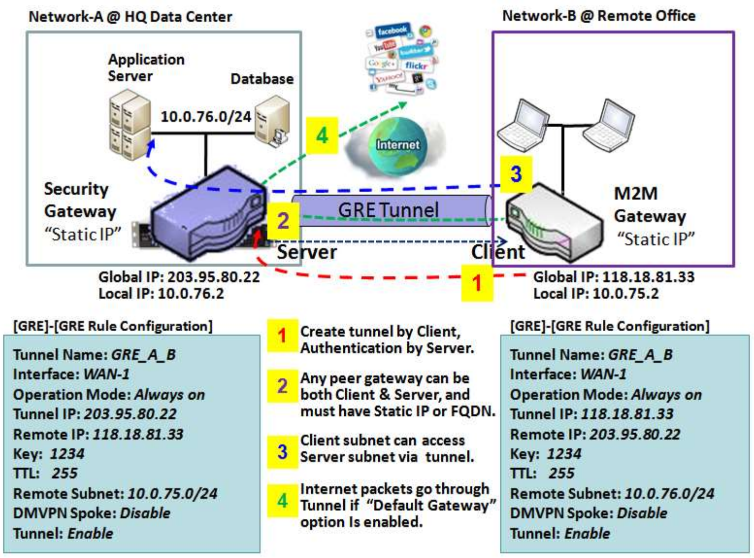
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

Deploy an M2M gateway for a remote site and establish a virtual private network with control center by using GRE tunneling. Then, all client hosts behind M2M gateway can make data communication with server hosts behind control center gateway.

GRE Tunneling is similar to IPsec Tunneling, with the client requesting the tunnel establishment with the server. Both the client and the server must have a Static IP or a FQDN. Any peer gateway can be worked as either a client or a server, even using the same set of configuration rules.

GRE Tunnel Scenario



[GRE]-[GRE Rule Configuration]

Tunnel Name: *GRE_A_B*
Interface: *WAN-1*
Operation Mode: *Always on*
Tunnel IP: *203.95.80.22*
Remote IP: *118.18.81.33*
Key: *1234*
TTL: *255*
Remote Subnet: *10.0.75.0/24*
DMVPN Spoke: *Disable*
Tunnel: *Enable*

1 Create tunnel by Client, Authentication by Server.

2 Any peer gateway can be both Client & Server, and must have Static IP or FQDN.

3 Client subnet can access Server subnet via tunnel.

4 Internet packets go through Tunnel if “Default Gateway” option Is enabled.

[GRE]-[GRE Rule Configuration]

Tunnel Name: *GRE_A_B*
Interface: *WAN-1*
Operation Mode: *Always on*
Tunnel IP: *118.18.81.33*
Remote IP: *203.95.80.22*
Key: *1234*
TTL: *255*
Remote Subnet: *10.0.76.0/24*
DMVPN Spoke: *Disable*
Tunnel: *Enable*

To setup a GRE tunnel, each peer needs to setup its global IP as tunnel IP and enter the other's global IP as remote IP.

Each peer must further specify the Remote Subnet item for the Intranet of GRE server peer. At GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the gateway at GRE client peer. But, if 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the GRE client peer, and all packets, including the Internet accessing of GRE client peers, will go through the established GRE tunnel. That means the remote GRE server peer controls the flow of any packets from the GRE client peer.

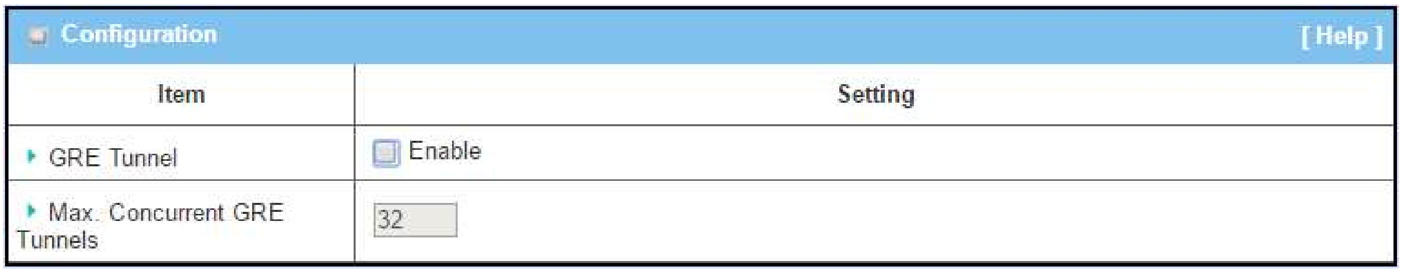
I

GRE Setting

Go to Security > VPN > GRE tab.

The GRE setting allows user to create and configure GRE tunnels.

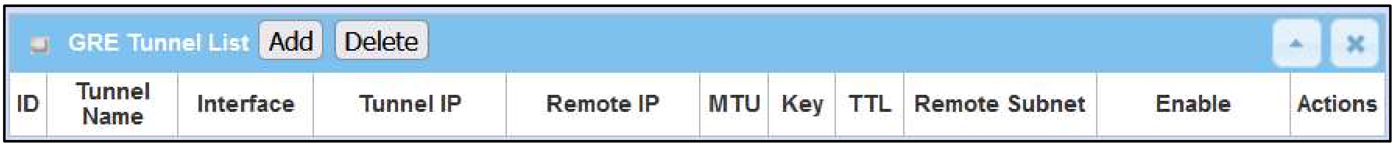
Enable GRE



Item	Setting
GRE Tunnel	□ Enable
Max. Concurrent GRE Tunnels	32

Enable GRE Window		
Item	**Value setting**	**Description**
GRE Tunnel	Unchecked by default	Click the **Enable** box to enable GRE function.
Max. Concurrent GRE Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous GRE tunnel connections. The default value will depend on the device model.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

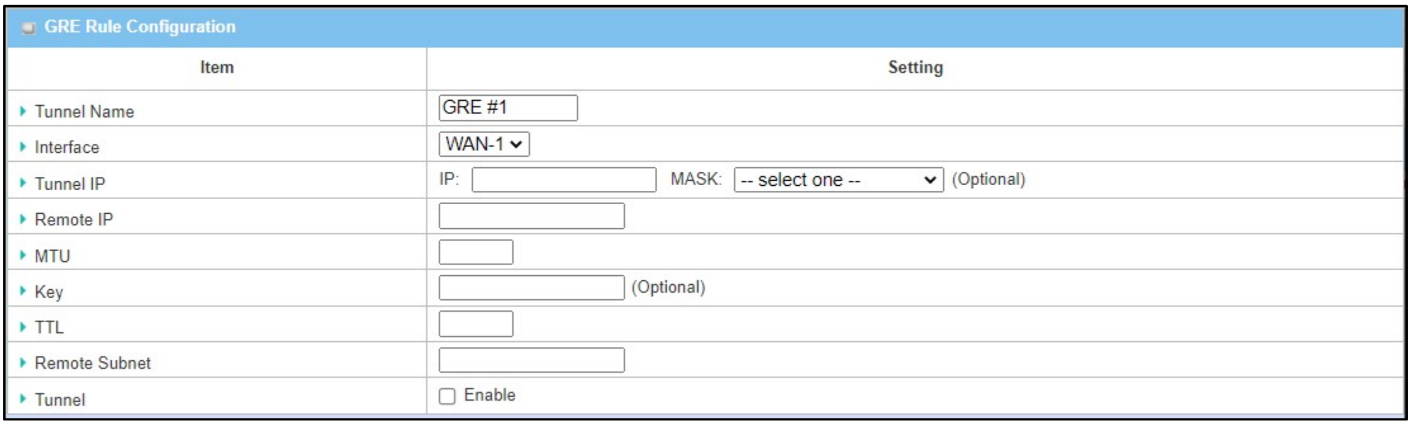
Create/Edit GRE tunnel



GRE Tunnel List Add Delete

ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions

When **Add/Edit** button is applied, a GRE Rule Configuration screen will appear.



GRE Rule Configuration

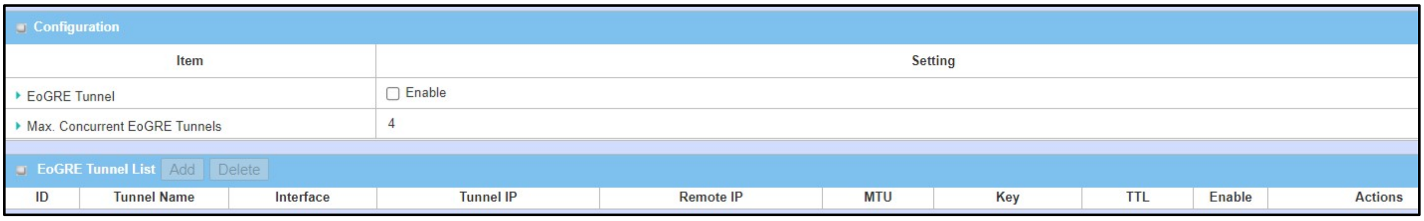
Item	Setting
Tunnel Name	GRE #1
Interface	WAN-1
Tunnel IP	IP: MASK: -- select one -- (Optional)
Remote IP	
MTU	
Key	(Optional)
TTL	
Remote Subnet	
Tunnel	□ Enable

GRE Rule Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	Required setting	Enter a tunnel name. ***Value Range***: 1 ~ 9 characters.
Interface	1. Required setting 2. **WAN 1** is selected by default	Select the interface on which GRE tunnel is to be established. It can be any available WAN and LAN interface.
Tunnel IP	Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	Required setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote GRE gateway.
MTU	Default is blank	Set the maximum transmission unit.
Key	Optional setting	Enter the Key for the GRE connection. ***Value Range***: 0 ~ 9999999999.
TTL	1. Required setting 2. 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel. Value Range: 1 ~ 255.
Remote Subnet	Required setting	Specify the remote subnet for this GRE tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of GRE server peer. At GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the security gateway at GRE client peer. If 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a default gateway setting for the GRE client peer, and all packets, including the Internet accessing of GRE client peers, will go through the established GRE tunnel. That

		means the remote GRE server peer controls the flow of any packets from the GRE client peer.
Tunnel	Unchecked by default	Check **Enable** box to enable this GRE tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

6.1.6 EoGRE

Ethernet over GRE (EoGRE) allows devices to bridge Ethernet traffic from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel.



Configuration

Item	Setting
EoGRE Tunnel	□ Enable
Max. Concurrent EoGRE Tunnels	4

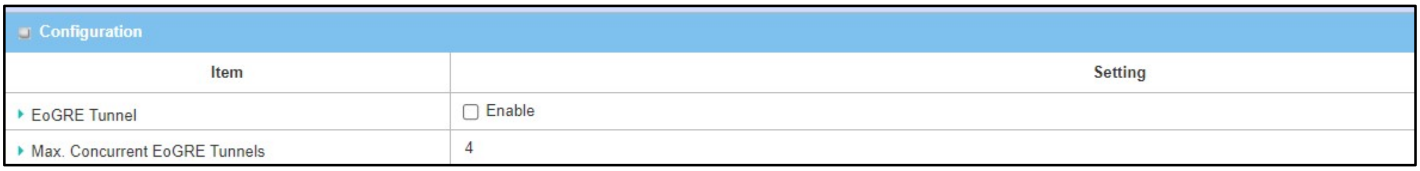
EoGRE Tunnel List

ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Enable	Actions

Go to Security > VPN > EoGRE tab.

The EoGRE setting allows user to create and configure EoGRE tunnels.

Enable eOGRE

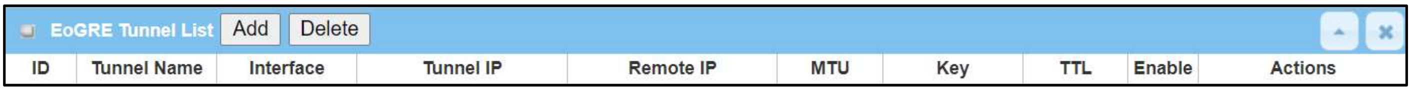


Configuration

Item	Setting
EoGRE Tunnel	□ Enable
Max. Concurrent EoGRE Tunnels	4

Enable GRE Window		
Item	**Value setting**	**Description**
EoGRE Tunnel	Unchecked by default	Click the **Enable** box to enable EoGRE function.
Max. Concurrent EoGRE Tunnels	Default is 4	The specified value will limit the maximum number of simultaneous EoGRE tunnel connections. The default value will depend on the device model.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

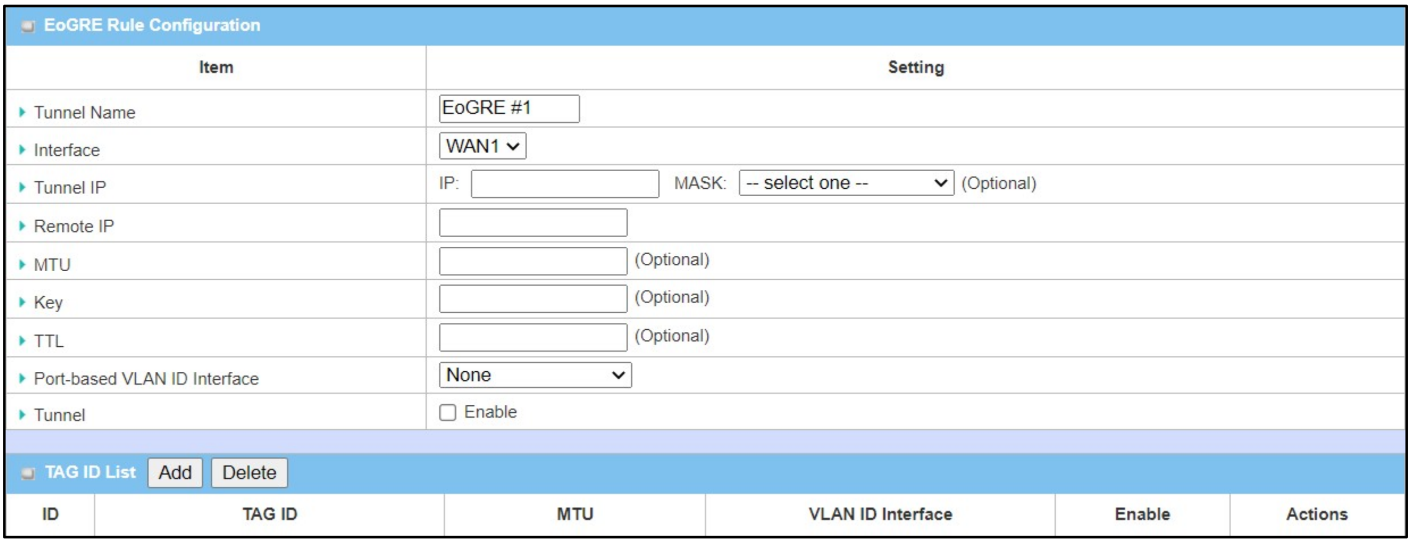
Create/Edit GRE tunnel



EoGRE Tunnel List Add Delete

ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Enable	Actions

When **Add/Edit** button is applied, a GRE Rule Configuration screen will appear.



EoGRE Rule Configuration

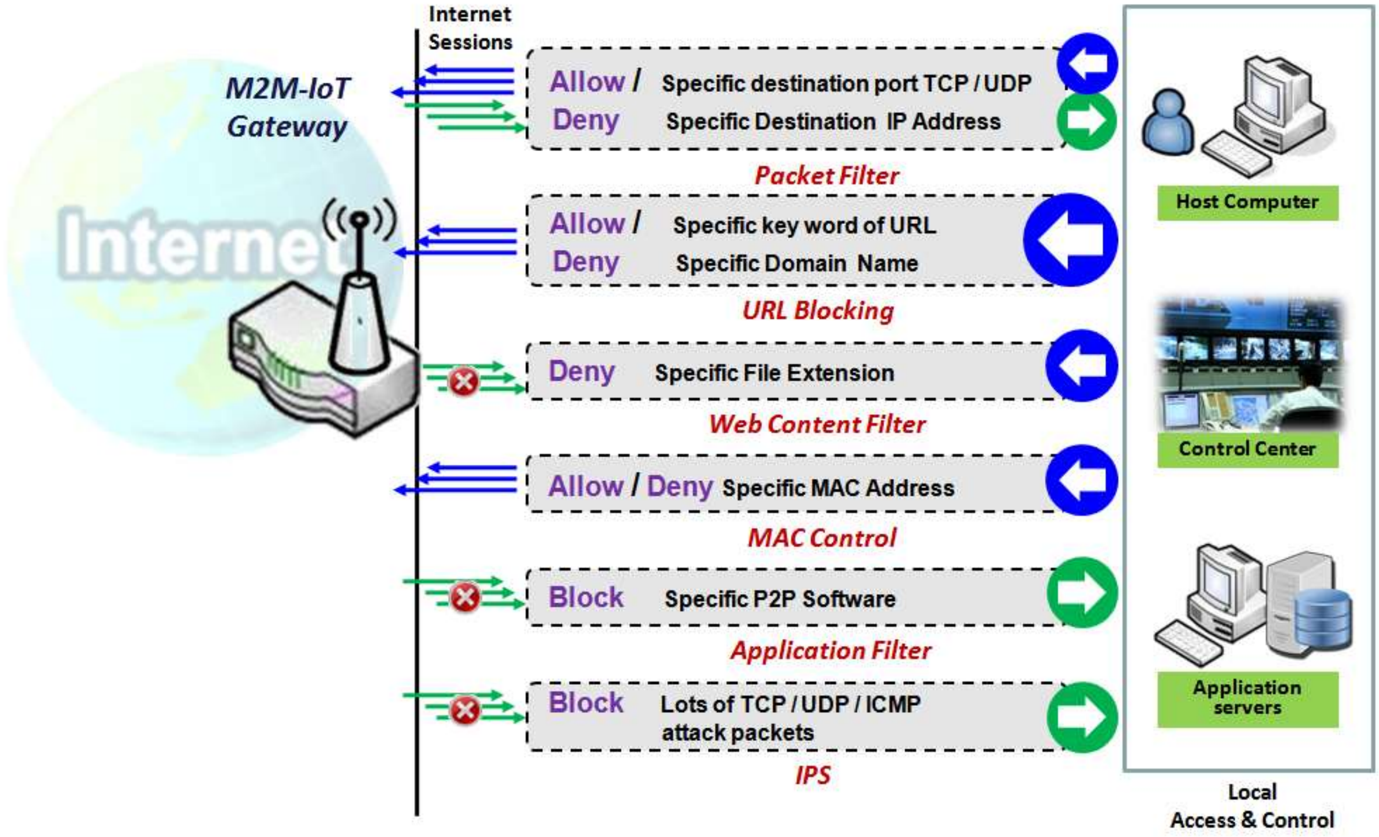
Item	Setting
Tunnel Name	EoGRE #1
Interface	WAN1
Tunnel IP	IP: MASK: -- select one -- (Optional)
Remote IP	
MTU	(Optional)
Key	(Optional)
TTL	(Optional)
Port-based VLAN ID Interface	None
Tunnel	□ Enable

TAG ID List Add Delete

ID	TAG ID	MTU	VLAN ID Interface	Enable	Actions

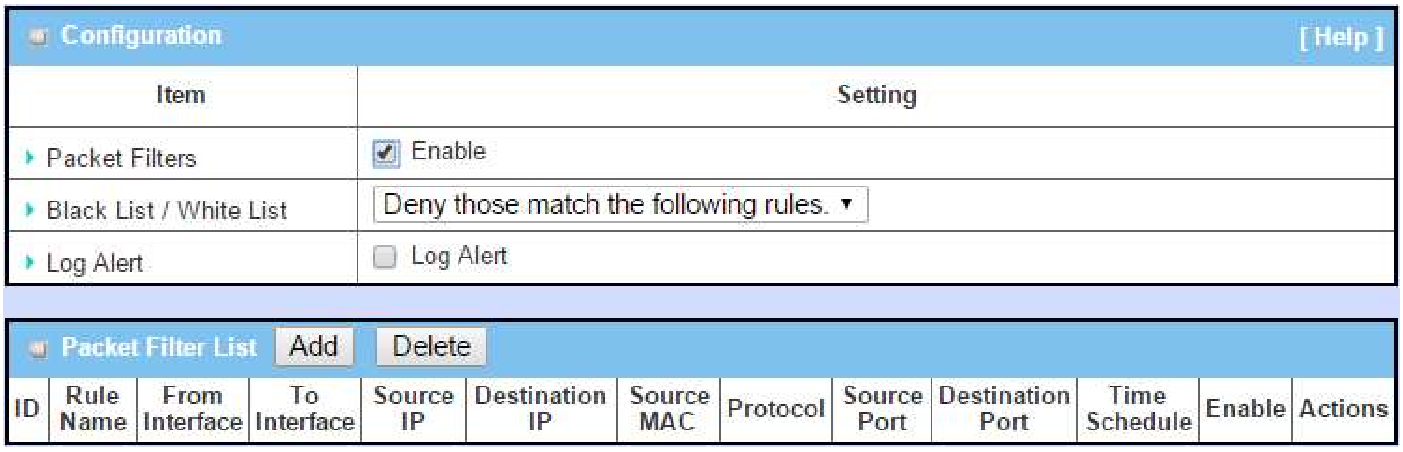
GRE Rule Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	Required setting	Enter a tunnel name. ***Value Range***: 1 ~ 9 characters.
Interface	1. Required setting 2. **WAN 1** is selected by default	Select the interface on which EoGRE tunnel is to be established.
Tunnel IP	Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	Required setting	Enter the Remote IP address of remote EoGRE tunnel gateway. Normally this is the public IP address of the remote EoGRE gateway.
MTU	Default is blank	Set the maximum transmission unit.
Key	Optional setting	Enter the Key for the GRE connection. ***Value Range***: 0 ~ 9999999999.
TTL	1. Optional setting 2. 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel. Value Range: 1 ~ 255.
Port-based VLAN ID Interface	Default is **None**	Select a VLAN to use for this tunnel.
Tunnel	Unchecked by default	Check **Enable** box to enable this EoGRE tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

6.2 Firewall



The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. Supported functions vary depending on the gateway model.

6.2.1 Packet Filter

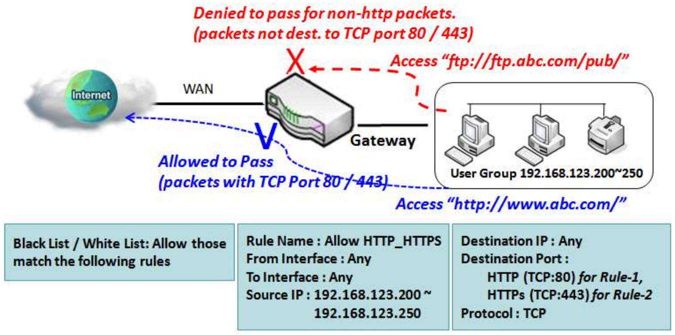


Item	Setting
Packet Filters	☑ Enable
Black List / White List	Deny those match the following rules. ▾
Log Alert	□ Log Alert

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

The "Packet Filter" function lets you define filtering rules for incoming and outgoing packets, allowing the gateway to control what packets are allowed or blocked as they pass through it. A packet filter rule should indicate from and to which interface the packet enters and leaves the gateway, the source and destination IP addresses, and destination service port type and port number. In addition, there should be a schedule for which the rule will be active.

Packet Filter with White List Scenario


Denied to pass for non-http packets.
(packets not dest. to TCP port 80 / 443)
Access "ftp://ftp.abc.com/pub/"
Internet
WAN
Gateway
Allowed to Pass
(packets with TCP Port 80 / 443)
User Group 192.168.123.200~250
Access "http://www.abc.com/"

Black List / White List: Allow those match the following rules

Rule Name : Allow HTTP_HTTPS
From Interface : Any
To Interface : Any
Source IP : 192.168.123.200 ~ 192.168.123.250

Destination IP : Any
Destination Port :
HTTP (TCP:80) *for Rule-1,*
HTTPs (TCP:443) *for Rule-2*
Protocol : TCP

As shown in the diagram, "Packet Filter Rule List" is specified as a white list (*Allow those matching the following rules*). Rule-1 is to allow HTTP packets to pass, and Rule-2 is to allow HTTPS packets to pass.

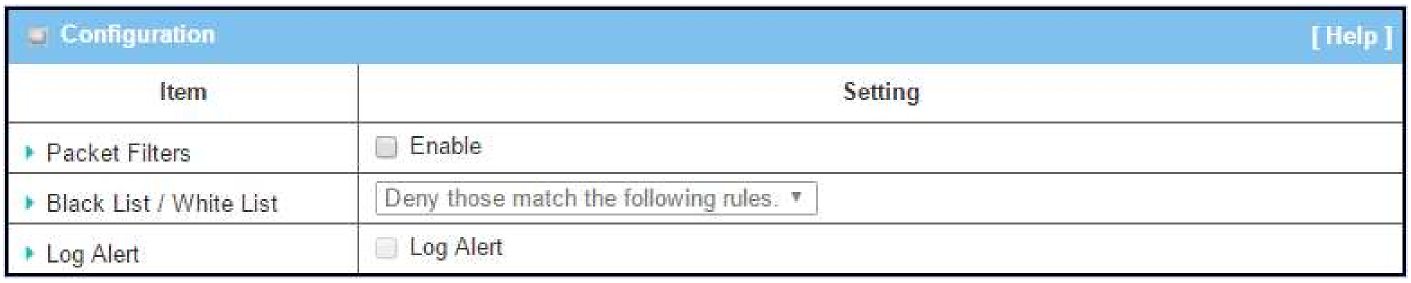
Under such configuration, the gateway will allow only HTTP and HTTPS packets, issued from the IP range 192.168.123.200 to 250, which are targeted to TCP port 80 or 443 to pass the WAN interface.

Packet Filter Setting

Go to Security > Firewall > Packet Filter Tab.

The packet filter setting allows user to create and customize packet filter policies to allow or reject specific inbound/outbound packets through the router based on their office setting.

Enable Packet Filter



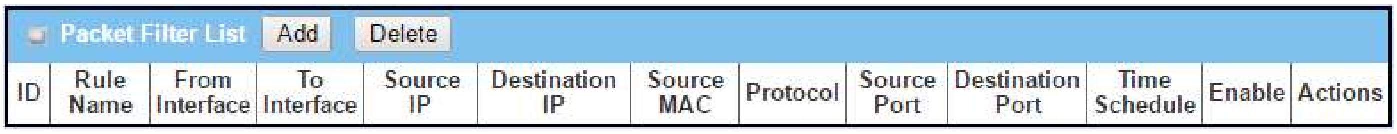
Item	Setting
Packet Filters	□ Enable
Black List / White List	Deny those match the following rules. ▾
Log Alert	□ Log Alert

Configuration Window		
Item Name	**Value setting**	**Description**
Packet Filter	Unchecked by default	Check the **Enable** box to activate the Packet Filter function

Black List / White List	Deny those match the following rules is set by default	When ***Deny those match the following rules*** is selected, as the name suggests, packets specified in the rules will be blocked –blacklisted. In contrast, with ***Allow those match the following rules***, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	Unchecked by default	Check the **Enable** box to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Packet Filter Rules

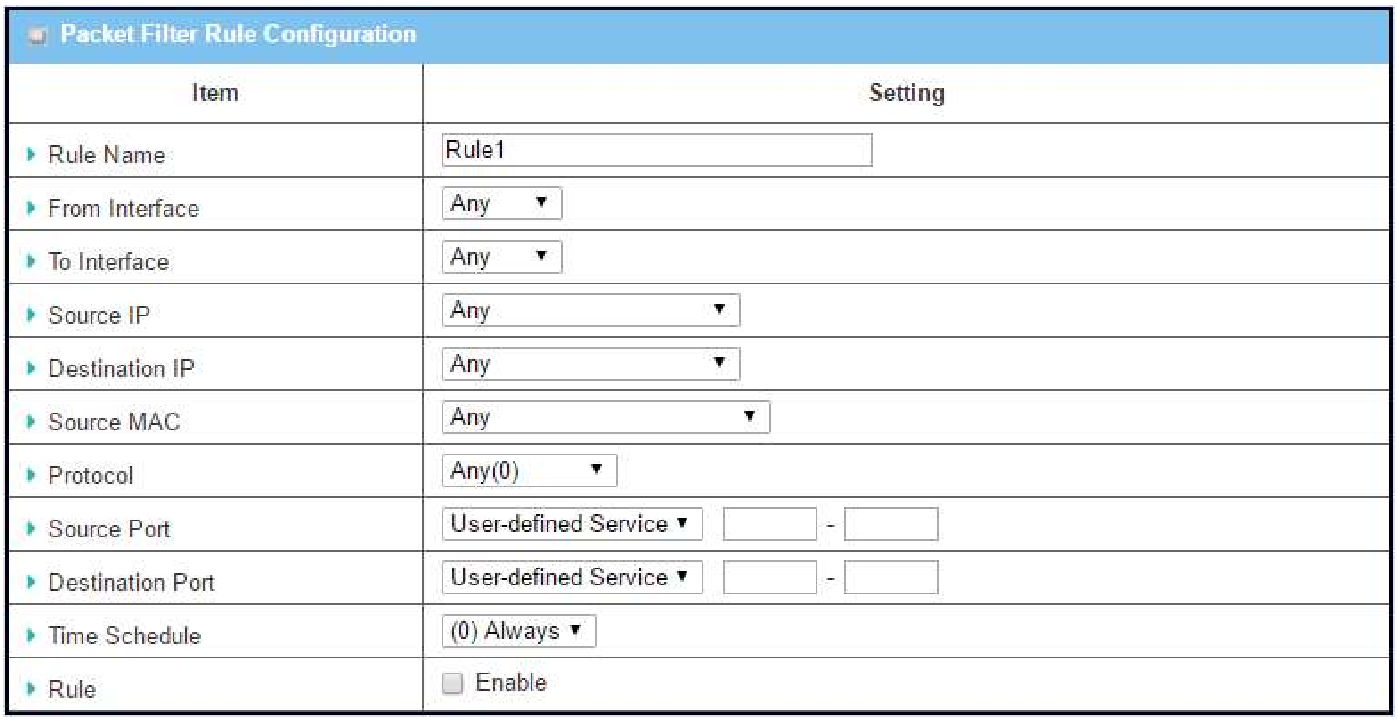
The gateway allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.



Packet Filter List Add Delete

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

When **Add** button is applied, **Packet Filter Rule Configuration** screen will appear.



Packet Filter Rule Configuration

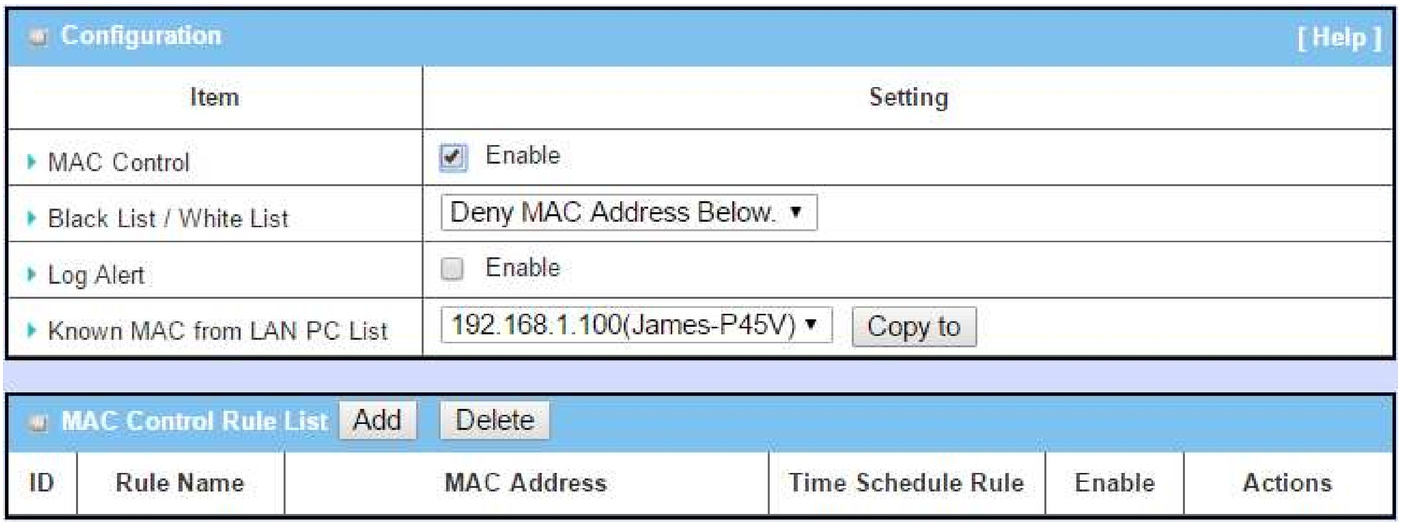
Item	Setting
Rule Name	Rule1
From Interface	Any ▾
To Interface	Any ▾
Source IP	Any ▾
Destination IP	Any ▾
Source MAC	Any ▾
Protocol	Any(0) ▾
Source Port	User-defined Service ▾ ___ - ___
Destination Port	User-defined Service ▾ ___ - ___
Time Schedule	(0) Always ▾
Rule	□ Enable

Packet Filter Rule Configuration		
Item Name	**Value setting**	**Description**
Rule Name	1. String format, any text 2. Required setting	Enter a packet filter rule name. ***Value Range***: 1 ~ 30 characters.

From Interface	1. Required setting **2. By default Any is selected**	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **LAN to WAN,** then select LAN for this field. If **VLAN-1 to WAN,** then select **VLAN-1** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
To Interface	1. Required setting 2. By default Any is selected	Define the selected interface to be the packet-leaving interface of the router. If the packets to be filtered are entering from **LAN to WAN, then** select **WAN** for this field. If **VLAN-1 to WAN,** then select **WAN** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets leaving the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
Source IP	1. Required setting 2. By default Any is selected	This field is to specify the **Source IP address**. Select **Any** to filter packets coming from any IP addresses. Select **Specific IP Address** to filter packets coming from an IP address. Select **IP Range** to filter packets coming from a specified range of IP address. Select **IP Address-based Group** to filter packets coming from a pre-defined group. Note: group must be pre-defined before this option becomes available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Destination IP	1. Required setting 2. By default Any is selected	This field is to specify the **Destination IP address**. Select **Any** to filter packets that are entering to any IP addresses. Select **Specific IP Address** to filter packets entering to an IP address entered in this field. Select **IP Range** to filter packets entering to a specified range of IP address entered in this field. Select **IP Address-based Group** to filter packets entering to a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button. Setting done through the **Add Rule** button will also appear in the **Host grouping** setting screen.
Source MAC	1. Required setting 2. By default Any is selected	This field is to specify the **Source MAC address**. Select **Any** to filter packets coming from any MAC addresses. Select **Specific MAC Address** to filter packets coming from a MAC address. Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Protocol	1. Required setting 2. By default Any(0) is selected	For **Protocol**, select **Any** to filter any protocol packets For **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range.

		For **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **ICMPv4** to filter ICMPv4 packets
		For **Protocol**, select **TCP** to filter **TCP** packets For **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. For **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **UDP** to filter **UDP** packets For **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. For **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **GRE** to filter **GRE** packets
		For **Protocol**, select **ESP** to filter **ESP** packets
		For **Protocol**, select **SCTP** to filter **SCTP** packets
		For **Protocol**, select **User-defined** to filter packets with specified port number. Then enter a pot number in **Protocol Number** box.
Time Schedule	Required setting	Apply **Time Schedule** to this rule, otherwise leave it as Always. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration** tab.
Rule	Unchecked by default	Click **Enable** box to activate this rule, then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

6.2.2 MAC Control



Configuration [Help]

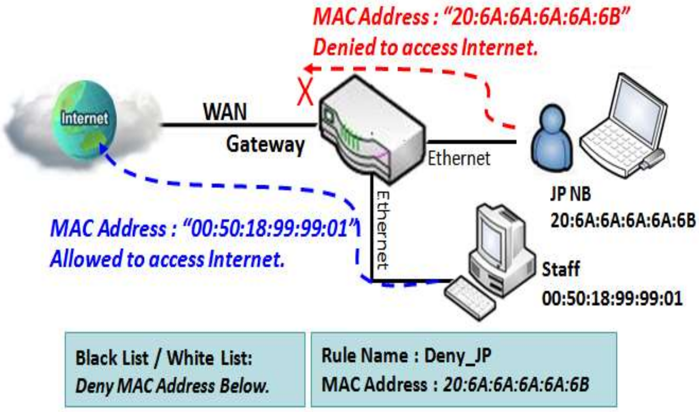
Item	Setting
MAC Control	☑ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.1.100(James-P45V) ▾ Copy to

MAC Control Rule List Add Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device's MAC address. When the administrator wants to reject the traffic from some client hosts with specific MAC addresses, the "MAC Control" function can be used to reject according to the blacklist configuration.

MAC Control with Blacklist Scenario


MAC Address : "20:6A:6A:6A:6A:6B"
Denied to access Internet.
Internet
WAN
Gateway
Ethernet
JP NB
20:6A:6A:6A:6A:6B
Ethernet
MAC Address : "00:50:18:99:99:01"
Allowed to access Internet.
Staff
00:50:18:99:99:01

Black List / White List:
Deny MAC Address Below.

Rule Name : Deny_JP
MAC Address : 20:6A:6A:6A:6A:6B

As shown in the diagram, enable the MAC control function and specify the "MAC Control Rule List" as a blacklist, and configure one MAC control rule for the gateway to deny the connection request from the "JP NB" with its own MAC address 20:6A:6A:6A:6A:6B.

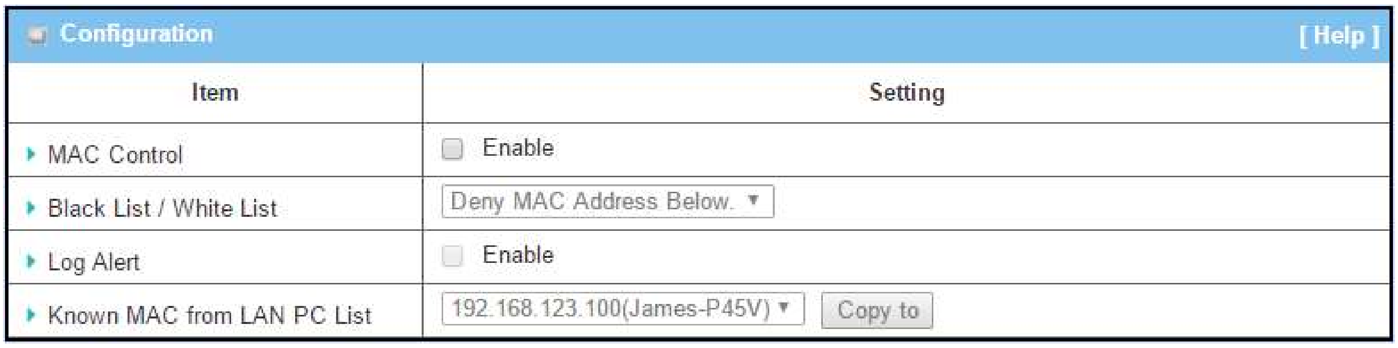
System will block connections from the "JP NB" to the gateway but allow others.

MAC Control Setting

Go to Security > Firewall > MAC Control Tab.

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address.

Enable MAC Control

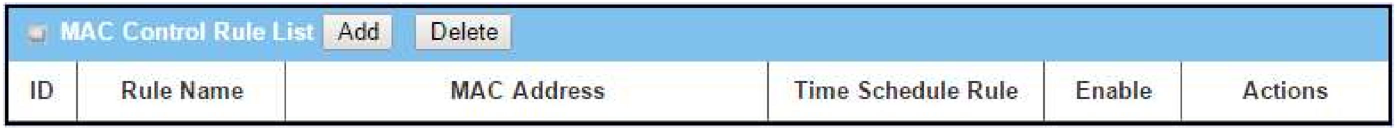


Item	Setting
MAC Control	□ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.123.100(James-P45V) ▾ [Copy to]

Configuration Window		
Item	**Value setting**	**Description**
MAC Control	Unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When ***Deny MAC Address Below*** is selected, as the name suggest, packets specified in the rules will be blocked – blacklisted. In contrast, with ***Allow MAC Address Below***, you can specifically white list the packets to pass, and the rest will be blocked.
Log Alert	Unchecked by default	Check the **Enable** box to activate to activate Event Log.
Known MAC from LAN PC List	N/A	Select a MAC Address from LAN Client List. Click the **Copy to** copy the selected **MAC Address** to the filter rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit MAC Control Rules

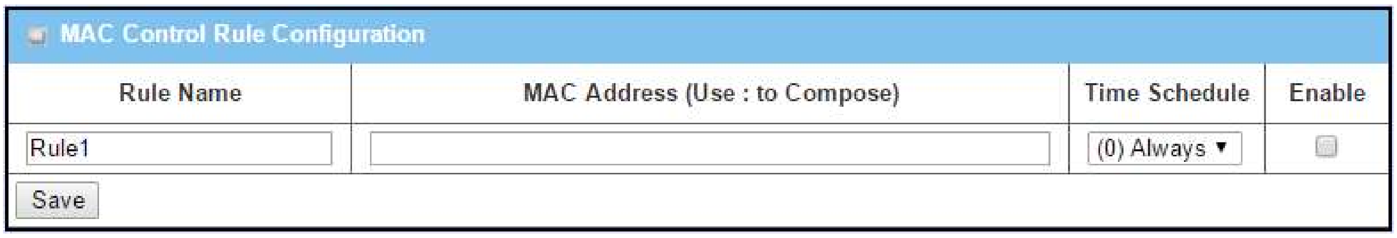
The gateway supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before creating control rules.



MAC Control Rule List

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

When **Add** button is applied, **Filter Rule Configuration** screen will appear.

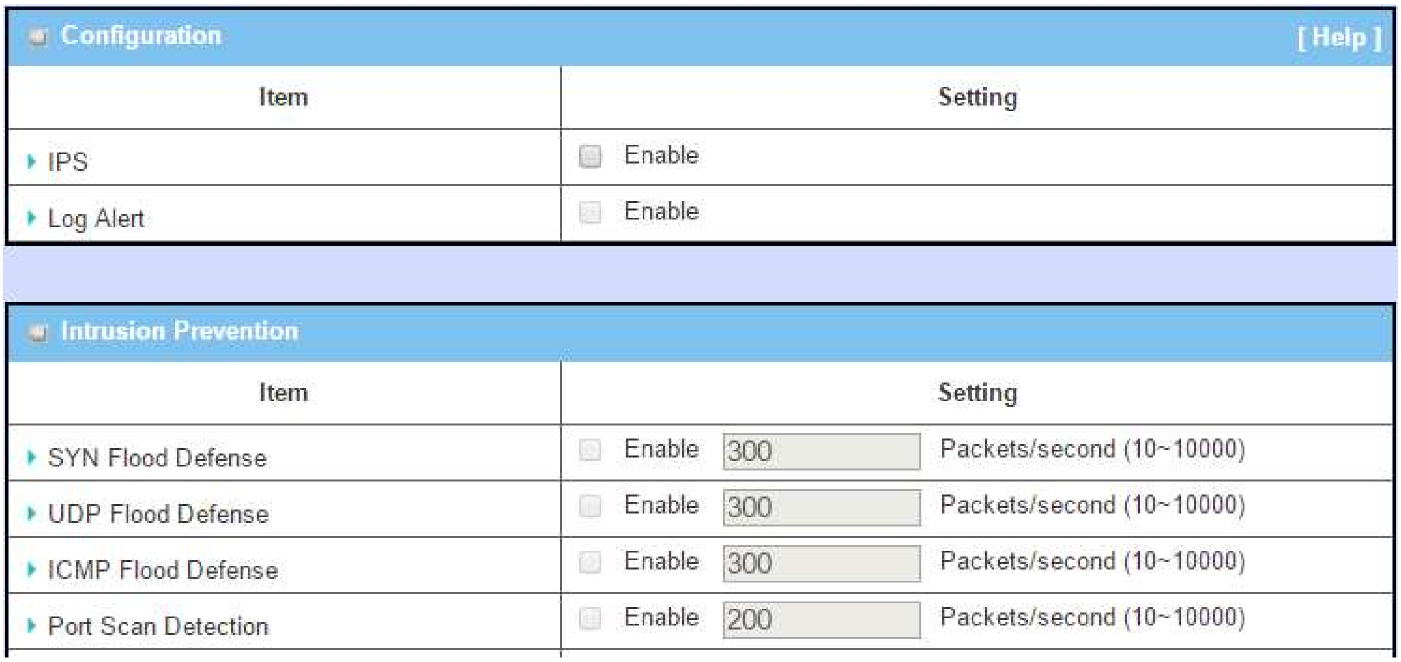


MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always ▾	□

MAC Control Rule Configuration Item	Value setting	Description
Rule Name	1. String format, any text 2. Required setting	Enter a MAC Control rule name.
MAC Address (Use: to Compose)	1. MAC Address string format 2. Required setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	Required setting	Apply **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration tab**
Enable	Unchecked by default	Click **Enable** box to activate this rule, and then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click **Back** to return to the MAC Control Configuration page.

6.2.3 IPS



Configuration [Help]

Item	Setting
IPS	□ Enable
Log Alert	□ Enable

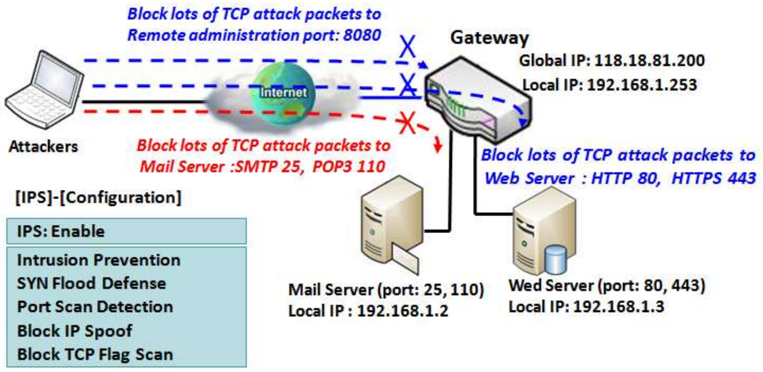
Intrusion Prevention

Item	Setting		
SYN Flood Defense	□ Enable	300	Packets/second (10~10000)
UDP Flood Defense	□ Enable	300	Packets/second (10~10000)
ICMP Flood Defense	□ Enable	300	Packets/second (10~10000)
Port Scan Detection	□ Enable	200	Packets/second (10~10000)

To provide application servers on the Internet, the administrator may need to open specific ports for services. However, there are some risks to open service ports to the Internet. In order to avoid such attack risks, it is important to enable IPS functions.

Intrusion Prevention System (IPS) is a network security appliance that monitors network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it. You can enable the IPS function and check the listed intrusion activities when needed. You can also enable the log alerting so that the system will record Intrusion events when corresponding intrusions are detected.

IPS Scenario


Block lots of TCP attack packets to
Remote administration port: 8080
Gateway
Global IP: 118.18.81.200
Local IP: 192.168.1.253
Internet
Attackers
Block lots of TCP attack packets to
Mail Server :SMTP 25, POP3 110
Block lots of TCP attack packets to
Web Server : HTTP 80, HTTPS 443
[IPS]-[Configuration]
IPS: Enable
Intrusion Prevention
SYN Flood Defense
Port Scan Detection
Block IP Spoof
Block TCP Flag Scan
Mail Server (port: 25, 110)
Local IP : 192.168.1.2
Wed Server (port: 80, 443)
Local IP: 192.168.1.3

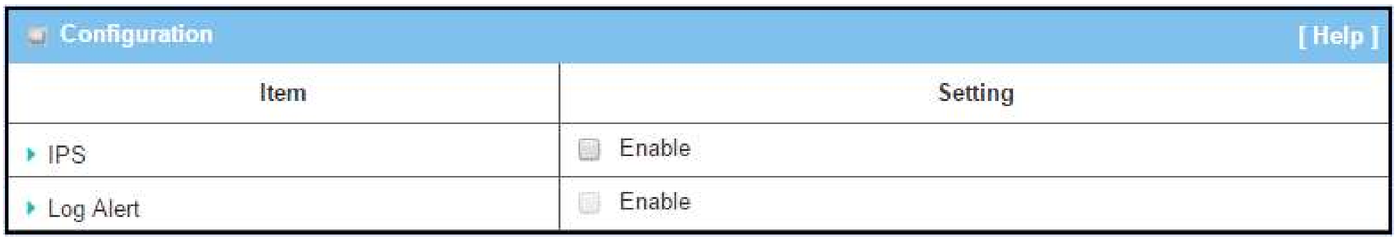
As shown in the diagram, the gateway serves as an E-mail server, Web Server and also provides TCP port 8080 for remote administration. So, remote users or unknown users can request those services from Internet. With IPS enabled, the gateway can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let normal ones pass through the gateway.

IPS Setting

Go to Security > Firewall > IPS Tab.

The Intrusion Prevention System (IPS) setting allows user to customize intrusion prevention rules to prevent malicious packets.

Enable IPS Firewall

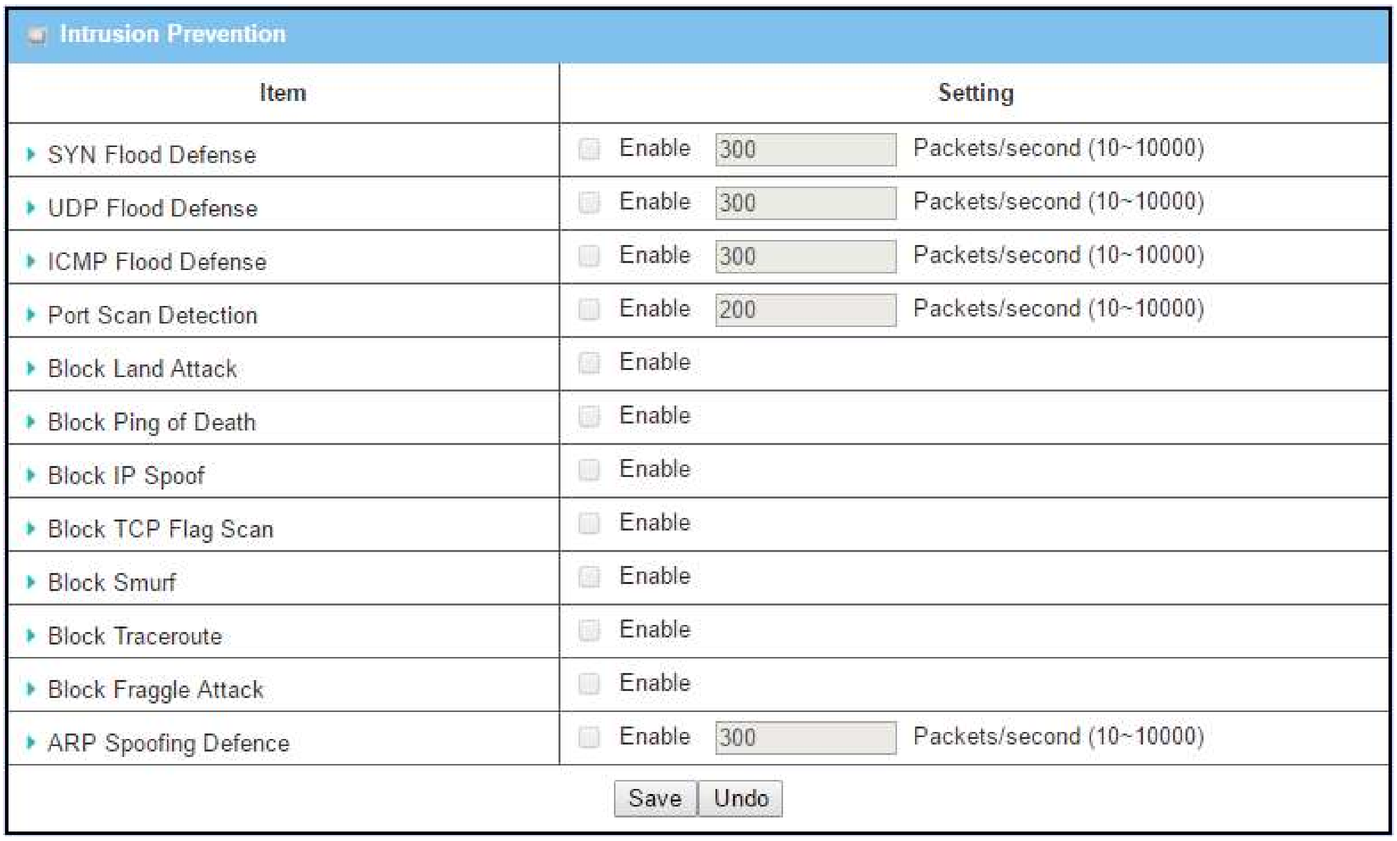


Item	Setting
IPS	□ Enable
Log Alert	□ Enable

Configuration Window		
Item	**Value setting**	**Description**
IPS	Unchecked by default	Check the **Enable** box to activate IPS function
Log Alert	Unchecked by default	Check the **Enable** box to activate to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Set up Intrusion Prevention Rules

The device allows you to select intrusion prevention rules you may want to enable. Ensure that the IPS is enabled before enabling the defense function.



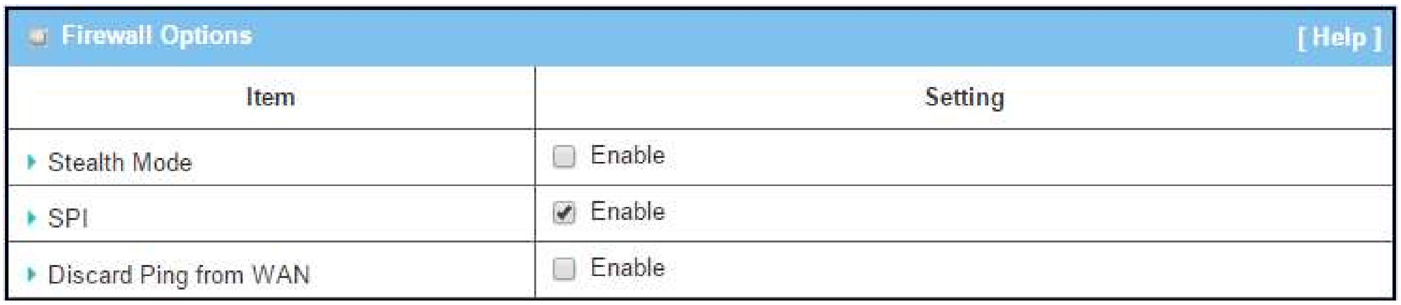
Intrusion Prevention

Item	Setting
SYN Flood Defense	□ Enable 300 Packets/second (10~10000)
UDP Flood Defense	□ Enable 300 Packets/second (10~10000)
ICMP Flood Defense	□ Enable 300 Packets/second (10~10000)
Port Scan Detection	□ Enable 200 Packets/second (10~10000)
Block Land Attack	□ Enable
Block Ping of Death	□ Enable
Block IP Spoof	□ Enable
Block TCP Flag Scan	□ Enable
Block Smurf	□ Enable
Block Traceroute	□ Enable
Block Fraggle Attack	□ Enable
ARP Spoofing Defence	□ Enable 300 Packets/second (10~10000)

Setup Intrusion Prevention Rules		
Item Name	**Value setting**	**Description**
SYN Flood Defense	1. Required setting 2. Unchecked by default 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
UDP Flood Defense		Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
ICMP Flood Defense		Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. ***Value Range***: 10 ~ 10000.
Port Scan Defection	1. Required setting 2. Unchecked by default 3. Traffic threshold is set to 200 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. *Value Range*: 10 ~ 10000.
Block Land		

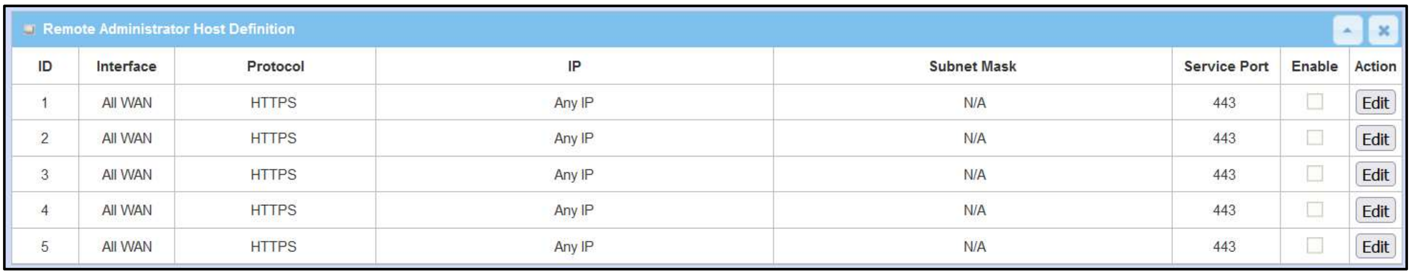
Attack **Block Ping of Death** **Block IP Spoof** **Block TCP Flag Scan** **Block Smurf** **Block Traceroute** **Block Fraggle Attack**	Unchecked by default	Click **Enable** box to activate this intrusion prevention rule.
ARP Spoofing Defence	1. Required setting 2. Unchecked by default 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. ***Value Range***: 10 ~ 10000.
Save	NA	Click **Save** to save the settings
Undo	NA	Click **Undo** to cancel the settings

6.2.4 Options



Firewall Options

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable



Remote Administrator Host Definition

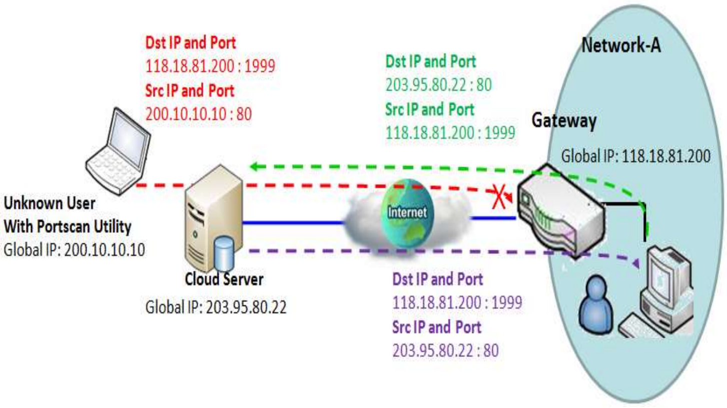
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTPS	Any IP	N/A	443	□	Edit
2	All WAN	HTTPS	Any IP	N/A	443	□	Edit
3	All WAN	HTTPS	Any IP	N/A	443	□	Edit
4	All WAN	HTTPS	Any IP	N/A	443	□	Edit
5	All WAN	HTTPS	Any IP	N/A	443	□	Edit

There are some additional useful firewall options in this page.

“Stealth Mode” lets the gateway not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet. “SPI” enables gateway to record the packet information like IP address, port address, ACK, SEQ number and so on while they pass through the gateway, and the gateway checks every incoming packet to detect if the packet is valid.

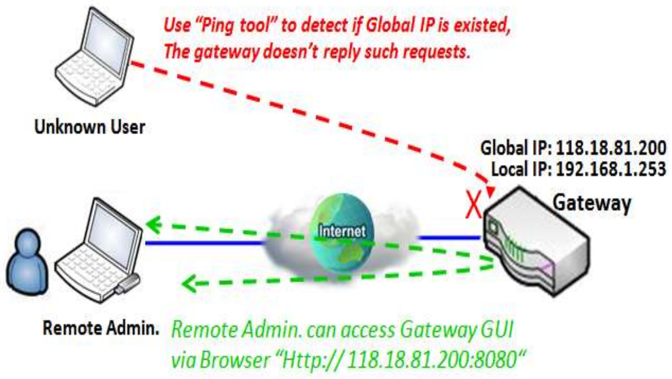
“Discard Ping from WAN” makes any host on the WAN side unable to ping this gateway. And finally, “Remote Administrator Hosts” enables you to perform administration tasks from a remote host. If this feature is enabled, only specified IP address(es) can perform remote administration.

Enable SPI Scenario



As shown in the diagram, the Gateway has the IP address of 118.18.81.200 for WAN interface and 192.168.1.253 for LAN interface. It serves as a NAT gateway. Users in Network-A initiate access to cloud server through the gateway. Sometimes, unknown users will simulate the packets but use different source IP to masquerade. With the SPI feature been enabled at the gateway, it will block such packets from unknown users.

Discard Ping from WAN & Remote Administrator Hosts Scenario


Use "Ping tool" to detect if Global IP is existed,
The gateway doesn't reply such requests.
Unknown User
Global IP: 118.18.81.200
Local IP: 192.168.1.253
Gateway
Internet
Remote Admin.
Remote Admin. can access Gateway GUI
via Browser "Http:// 118.18.81.200:8080"

"Discard Ping from WAN" makes any host on the WAN side unable to ping this gateway and receive ICMP packet reply. Enable the Discard Ping from WAN function to prevent security leaks when local users use the internet.

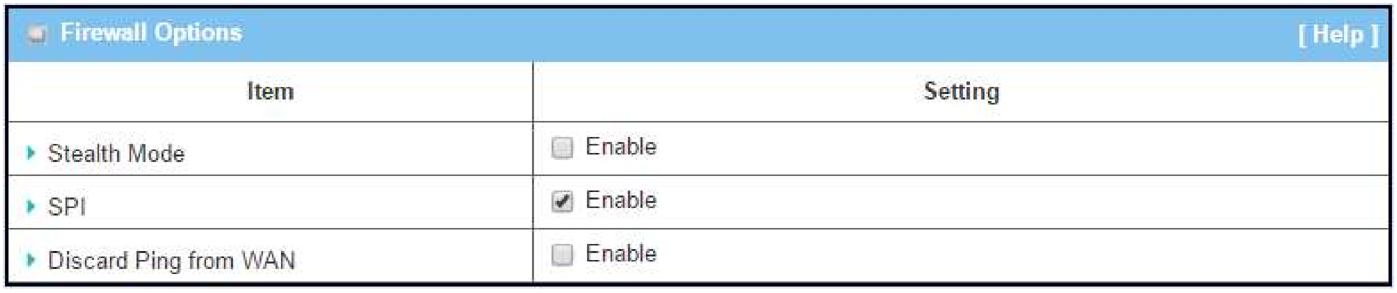
If the remote administrator knows the gateway's global IP, he/she can access the Gateway GUI via TCP port 8080.

Firewall Options Setting

Go to Security > Firewall > Options Tab.

The firewall options setting allows network administrator to modify the behavior of the firewall and to enable Remote Router Access Control.

Enable Firewall Options



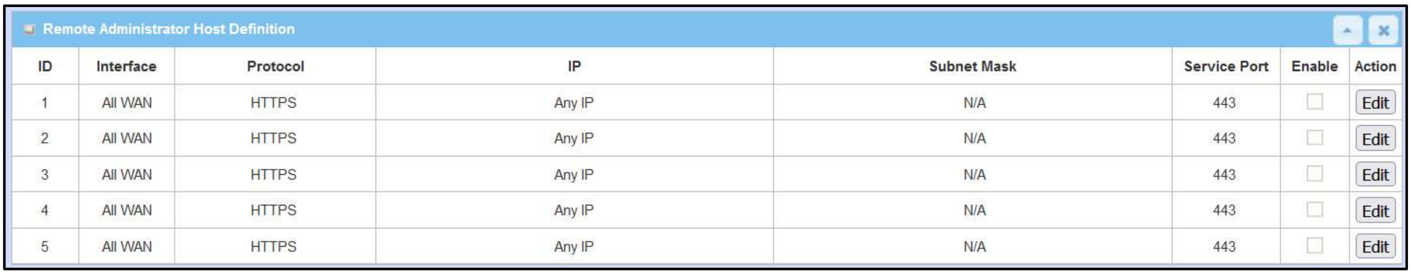
Firewall Options [Help]

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable

Firewall Options		
Item	**Value setting**	**Description**
Stealth Mode	Unchecked by default	Check the **Enable** box to activate the Stealth Mode function
SPI	Checked by default	Check the **Enable** box to activate the SPI function
Discard Ping from WAN	Unchecked by default	Check the **Enable** box to activate the Discard Ping from WAN function

Define Remote Administrator Host

The router allows the network administrator to manage the router remotely. The network administrator can assign specific IP address and service ports to allow access to the router.



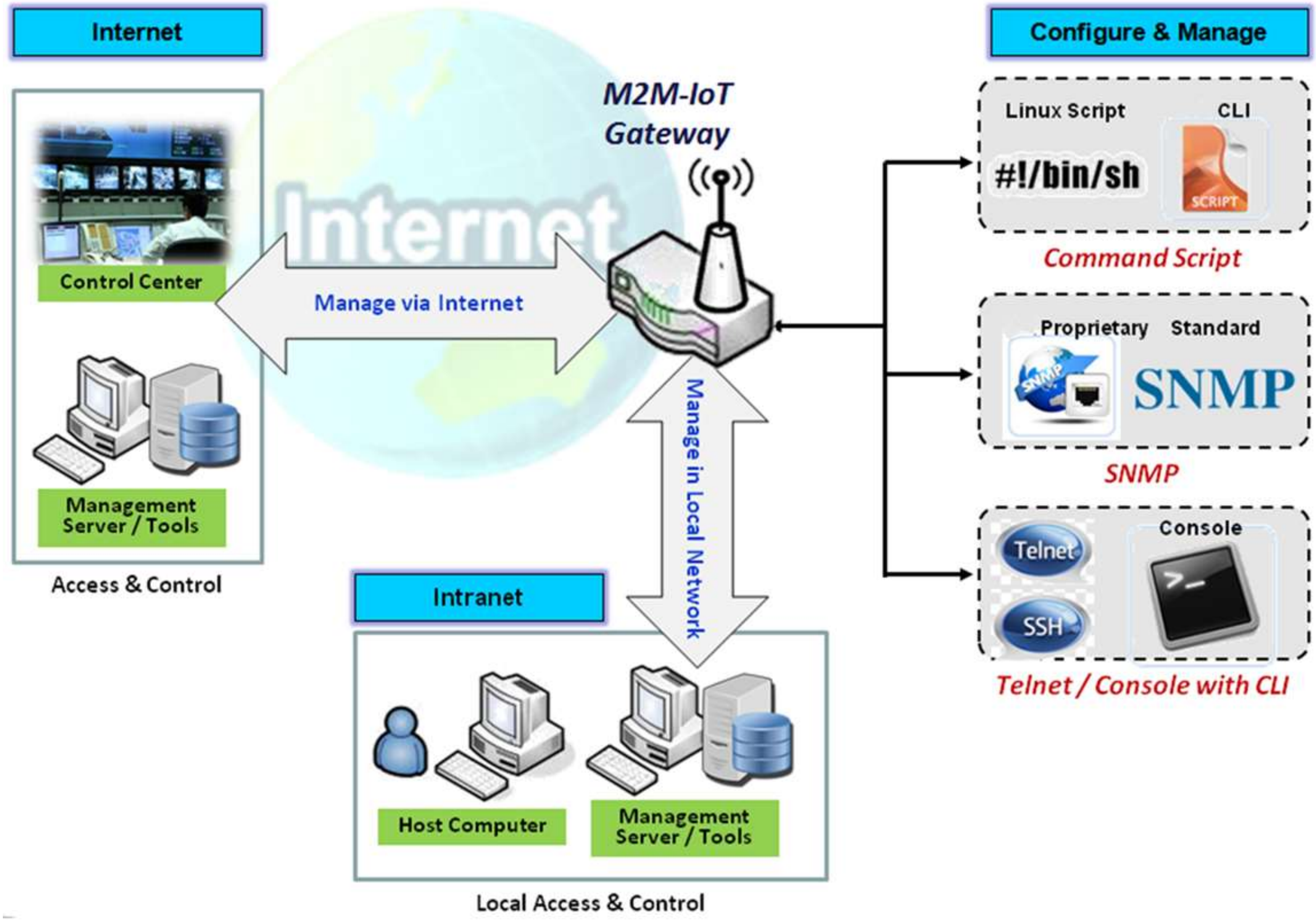
Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTPS	Any IP	N/A	443	□	Edit
2	All WAN	HTTPS	Any IP	N/A	443	□	Edit
3	All WAN	HTTPS	Any IP	N/A	443	□	Edit
4	All WAN	HTTPS	Any IP	N/A	443	□	Edit
5	All WAN	HTTPS	Any IP	N/A	443	□	Edit

Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
IP	Required setting	Specifies the remote host to assign access rights for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address and a selected **Subnet Mask** compose the subnet**.**
Service Port	80 for HTTP by default 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection. ***Value Range***: 1 ~ 65535.
Enabling the rule	Unchecked by default	Click **Enable** box to activate this rule.
Save	N/A	Click **Enable** box to activate this rule then save the settings.
Undo	N/A	Click **Undo** to cancel the settings

Chapter 7 Administration

7.1 Configure & Manage



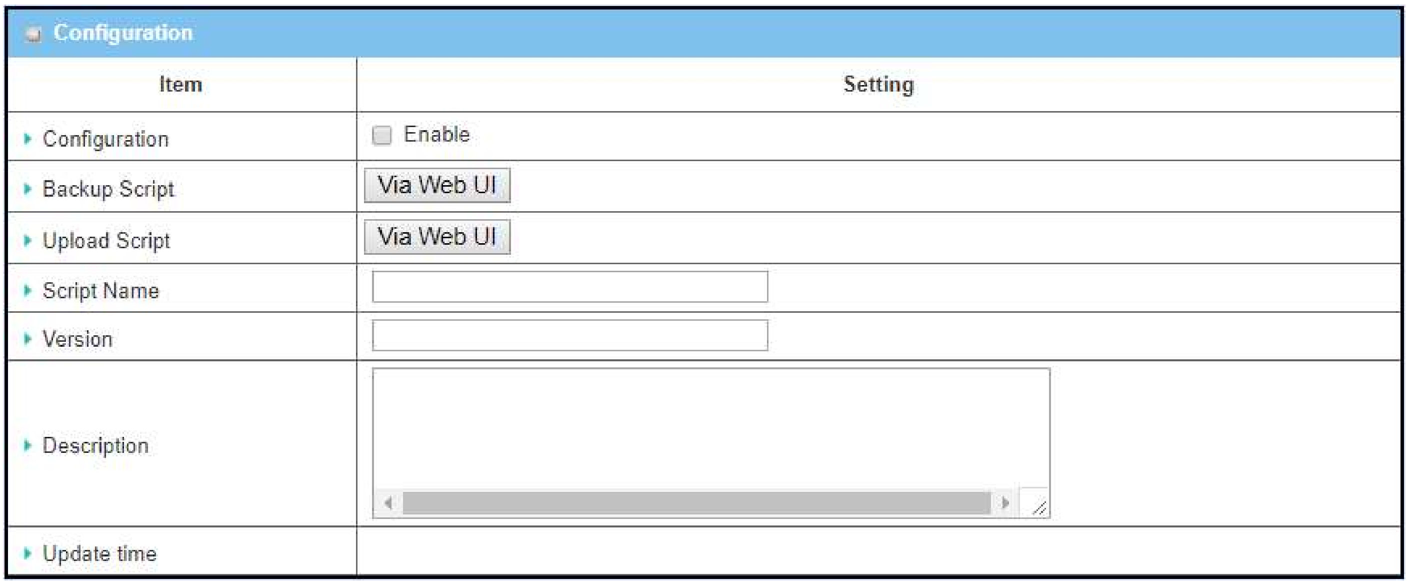
Configure & Manage refers to enterprise-wide administration of distributed systems including (and commonly in practice) computer systems. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being used. This device supports many system management protocols, such as Command Script, SNMP, and Telnet with CLI. You can set up those configurations in the "Configure & Manage" section.

7.1.1 Command Script

Command script configuration is the application that allows administrator to set up a pre-defined configuration in plain text style and apply configuration on startup.

Go to Administration > Command Script > Configuration Tab.

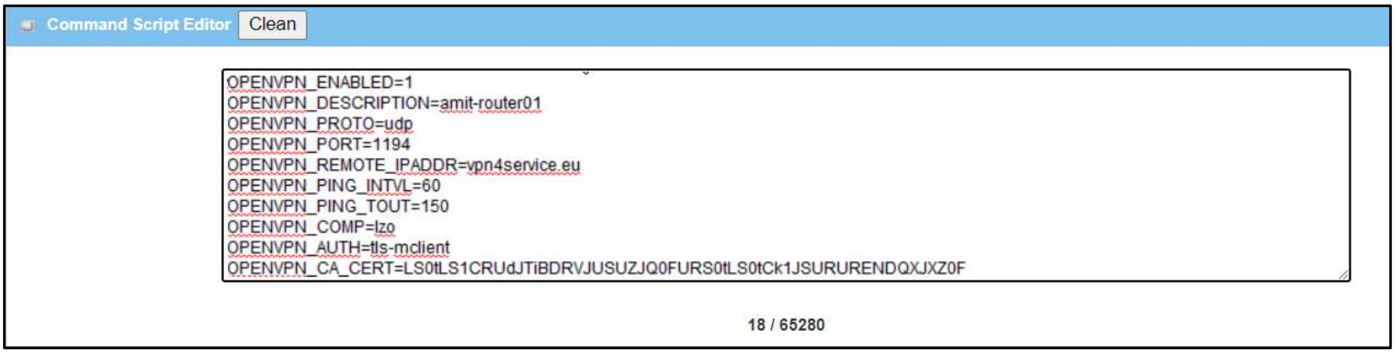
Enable Command Script Configuration



Item	Setting
Configuration	□ Enable
Backup Script	Via Web UI
Upload Script	Via Web UI
Script Name	
Version	
Description	
Update time	

Configuration Item	Value setting	Description
Configuration	Unchecked by default	Check the **Enable** box to activate the Command Script function.
Backup Script	N/A	Click the **Via Web UI** or **Via Storage** button to back up the existing command script in a .txt file. You can specify the script file name in **Script Name** below.
Upload Script	N/A	Click the **Via Web UI** or **Via Storage** button to Upload the existing command script from a specified .txt file.
Script Name	1. Optional setting **2. Any valid file name**	Specify a script file name for script backup, or display the selected upload script file name. ***Value Range***: 0 ~ 32 characters.
Version	1. Optional setting 2. Any string	Specify the version number for the applied Command script. ***Value Range***: 0 ~ 32 characters.
Description	1. Optional setting 2. Any string	Enter a short description for the applied Command script.
Update time	N/A	It records the upload time for last command script upload.

Edit/Backup Plain Text Command Script



```
OPENVPN_ENABLED=1
OPENVPN_DESCRIPTION=amit-router01
OPENVPN_PROTO=udp
OPENVPN_PORT=1194
OPENVPN_REMOTE_IPADDR=vpn4service.eu
OPENVPN_PING_INTVL=60
OPENVPN_PING_TOUT=150
OPENVPN_COMP=lzo
OPENVPN_AUTH=tls-mclient
OPENVPN_CA_CERT=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURURENDQXJXZ0F
```

18 / 65280

You can edit the plain text configuration settings in the configuration screen as shown above.

Command Script Editor		
Item	**Value setting**	**Description**
Clean	*NA*	Clean text area. (Click the **Save** button to further clean the configuration already saved in the system.)
Backup	*NA*	Backup and download configuration.
Save	*NA*	Save configuration

The supported plain text configuration items are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configuration with the **STARTUP** command. For configurations without a corresponding Linux command set to configure, you can configure them with a proprietary command set.

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1: enable 0: disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	Required Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • **TCP** or **TCP /UDP** -> OpenVPN will use TCP protocol, and **Port** will be set to 443. • **UDP** -> OpenVPN will use UDP protocol, and **Port** will be set to 1194.
OPENVPN_PORT	Required Setting	Specify the **Port** for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Enter the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. • **TLS** -> OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to be specified as well.

OPENVPN_CA_CERT	Required Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	Required Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	Required Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	IP	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1: enable 0: disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection.
PPP_PING	0: DNS Query 1: ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP requests.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.

STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with; the STARTUP command.
		For example,
		STARTUP=#!/bin/sh
		STARTUP=echo “startup done” > /tmp/demo

Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the gateway system also allows configuration via Telnet CLI. The administrator can use the proprietary Telnet command “***txtConfig***” and related action items to perform the plain system configuration.

The command format is: txtConfig (action) [option]

Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the “Backup” plain text configuration.
commit	an existing file	Commit the configuration content to database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain text system config. (ex: *txtConfig enable*)
disable	*NA*	Disable plain text system config. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)
run_immediately	an existing file	Assign a configuration file to apply.

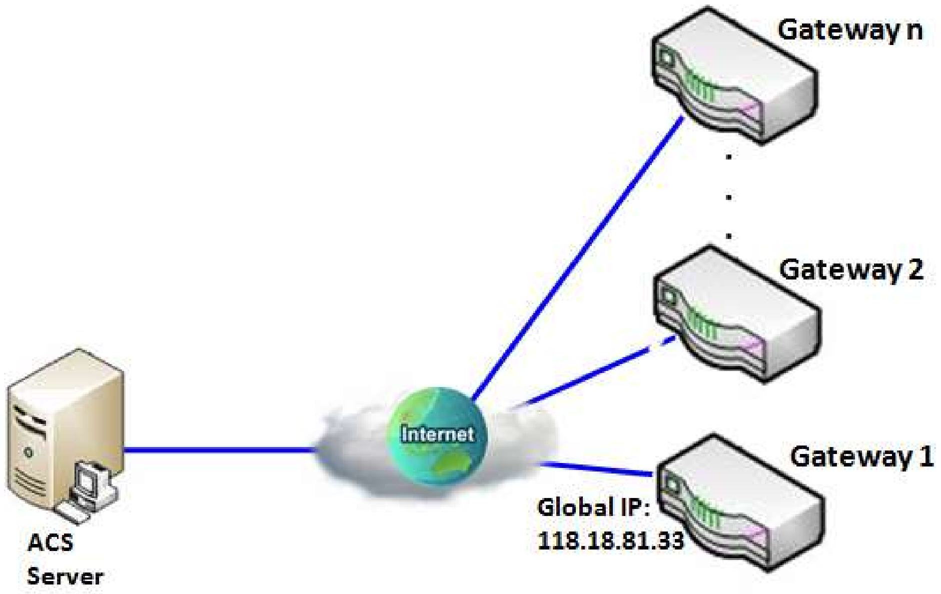
(ex: *txtConfig run_immediately /tmp/config*)

7.1.2 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

TR-069 is a customized feature for ISPs. It is not recommended that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one "[Help]" command let you see the same message about that.

Scenario - Managing deployed gateways through an ACS Server



Scenario Application Timing

When the enterprise data center wants to use an ACS server to manage remote gateways geographically distributed elsewhere in the world, the gateways in all branch offices must have an embedded TR-069 agent to communicate with the ACS server. So that the ACS server can configure, upgrade firmware, and monitor these gateways and their corresponding Intranets.

Scenario Description

The ACS server can configure, upgrade with latest firmware, and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

The ACS server can ask the gateways to execute some urgent jobs.

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "TR-069" enabling.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ Enable
ACS URL	http://qa.acslite.com/cpe.php
ACS User Name	ACSUserName
ACS Password	ACSPassword
ConnectionRequest Port	8099
ConnectionRequest User Name	ConnReqUserName
ConnectionRequest Password	ConnReqPassword
Inform	■ Enable Interval 900

Scenario Operation Procedure

In the above diagram, the ACS server can manage multiple gateways on the Internet. The "Gateway 1" is one of them and has 118.18.81.33 IP address for its WAN-1 interface.

When all remote gateways have booted up, they will try to connect to the ACS server.

Once the connections are established successfully, the ACS server can configure, upgrade with latest firmware, and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

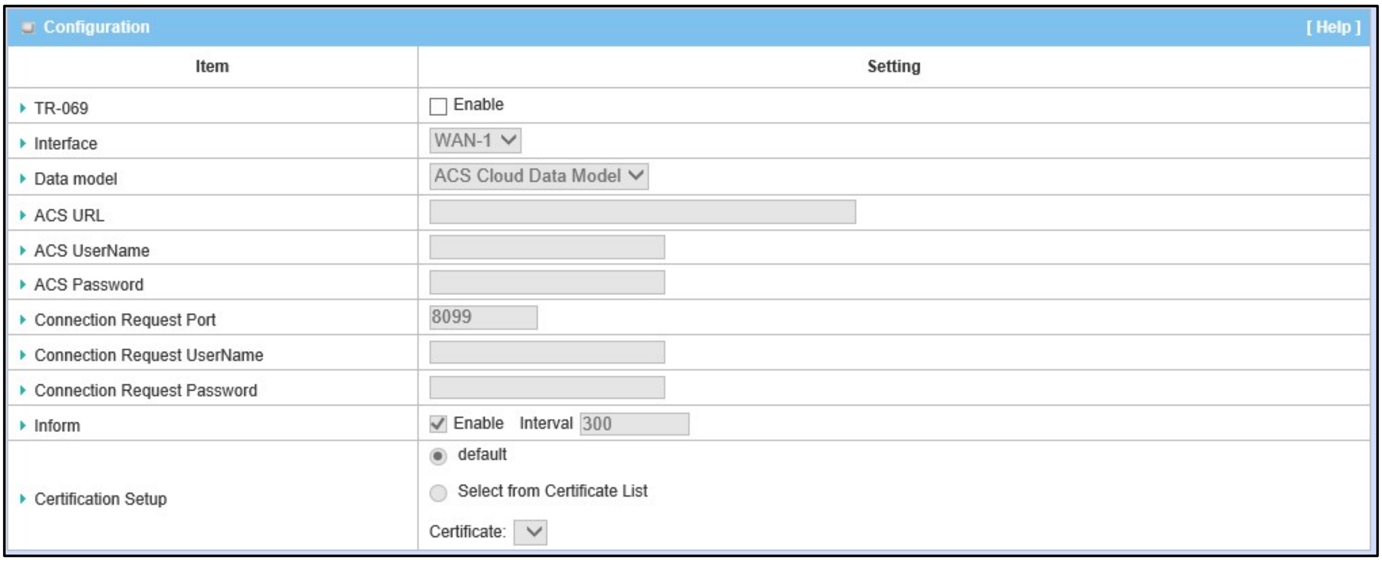
If the ACS server needs some urgent jobs to be done by the gateways, it will issue the "Connection Request" command to those gateways. And those gateways make immediate connections in response to the ACS server's immediate connection request for executing the urgent jobs.

TR-069 Setting

Go to Administration > Configure & Manage > TR-069 tab.

In "TR-069" page, there is only one configuration window for TR-069 function. In the window, you must specify the related information for your security gateway to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except for the inquiry time, there are no activities between the ACS server and the gateways until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the gateways urgently, it will ask these gateways by using connection request related information for immediate connection for inquiring jobs and executing.

Enable TR-069



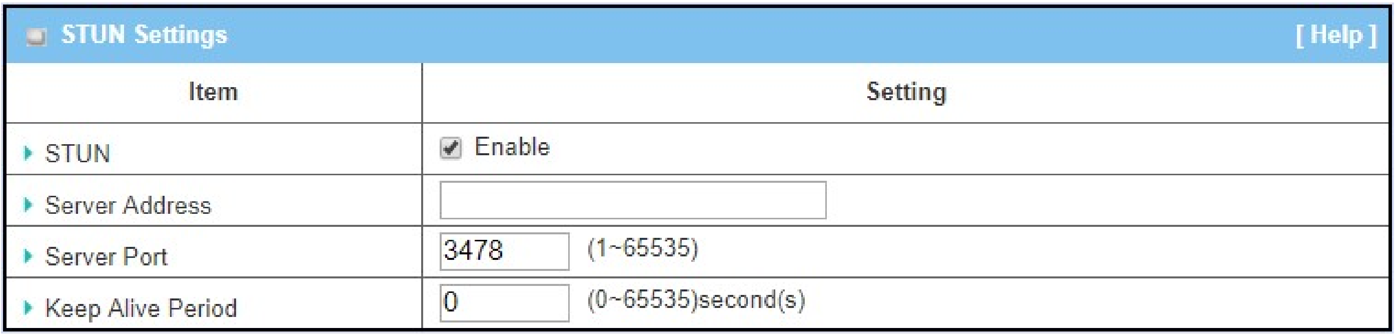
Configuration [Help]

Item	Setting
TR-069	□ Enable
Interface	WAN-1
Data model	ACS Cloud Data Model
ACS URL	
ACS UserName	
ACS Password	
Connection Request Port	8099
Connection Request UserName	
Connection Request Password	
Inform	☑ Enable Interval 300
Certification Setup	● default ○ Select from Certificate List Certificate:

TR-069		
Item	**Value setting**	**Description**
TR-069	The box is unchecked by default	Check the **Enable** box to activate TR-069 function.
Interface	**WAN-1** is selected by default.	When you finish set basic network WAN-1 ~ WAN-n, you can choose WAN-1 ~ WAN-n When you finish set Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface just like "IPSec #1"
Data Model	**ACS** is selected by default.	Select the TR-069 data model for the remote management. **Standard** : the ACS Server is a standard one, which fully complies with TR-069. **ACS Cloud Data Model**: Select this data model if you intend to use a Cloud ACS Server to managing the deployed gateways.
ACS URL	Required setting	You can ask ACS manager provide ACS URL and manually set
ACS Username	Required setting	You can ask ACS manager provide ACS username and manually set
ACS Password	Required setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	1. Required setting. **2. By default 8099 is set.**	You can ask ACS manager provide ACS ConnectionRequest Port and manually set *Value Range*: 0 ~ 65535.
ConnectionRequest UserName	Required setting	You can ask ACS manager provide ACS ConnectionRequest Username and manually set
ConnectionRequest Password	Required setting	You can ask ACS manager provide ACS ConnectionRequest Password and manually set
Inform	1. The box is checked by default. **2. The Interval value is 300 by default.**	When the **Enable** box is checked, the gateway (CPE) will periodicly send inform message to ACS Server according to the **Interval** setting. ***Value Range***: 0 ~ 86400 for Inform Interval.
Certification Setup	The **default** box is selected by default	You can leave it as **default** or select an expected certificate and key from the drop down list. Refer to **Object Definition > Certificate** Section for the Certificate configuration.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

When you finish setting **ACS URL ACS Username ACS Password,** your gateway (CPE, Client Premium Equipment) can send inform to ACS Server.
When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password**, ACS Server can ask the gateway (CPE) to send inform to ACS Server.

Enable STUN Server



STUN Settings [Help]

Item	Setting
STUN	☑ Enable
Server Address	
Server Port	3478 (1~65535)
Keep Alive Period	0 (0~65535)second(s)

STUN Settings Configuration		
Item	**Value setting**	**Description**
STUN	The box is checked by default	Check the **Enable** box to activate STUN function.
Server Address	1. String format: any IPv4 address 2. It is an optional item.	Specify the IP address for the expected STUN Server.
Server Port	1. An optional setting 2.**3478** is set by default	Specify the port number for the expected STUN Server. *Value Range*: 1 ~ 65535.
Keep Alive Period	1. An optional setting 2.**0** is set by default	Specify the keep alive time period for the connection with STUN Server. *Value Range*: 0 ~ 65535.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

7.1.3 SNMP

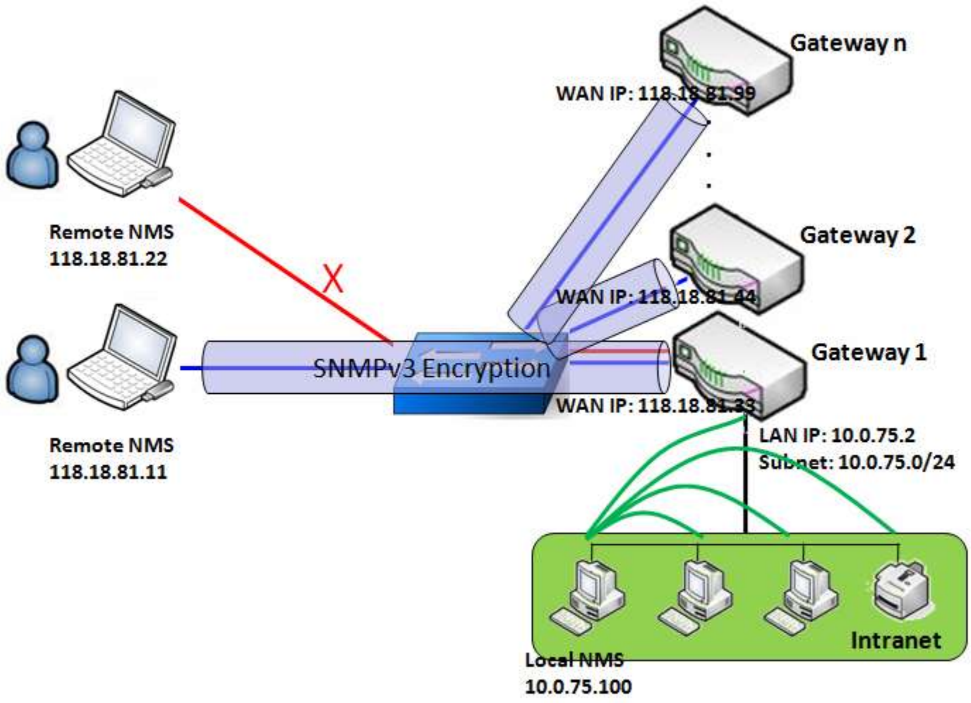
SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents deliver management data to the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follows: MIB-II (RFC 1213, Including IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB.

SNMP Management Scenario



Scenario Application Timing

There are two application scenarios for SNMP Network Management Systems (NMS). Local NMS is in the Intranet and manages all devices that support SNMP. Another is using Remote NMS to manage devices whose WAN interfaces are connected together by a switch or a router with UDP forwarding.

Scenario Description

The NMS server can monitor and configure the managed devices by using SNMP protocol, and those devices are located at where UDP packets can reach from NMS.

The managed devices report urgent trap events to the NMS servers.

Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses.

The remote NMS with privilege IP address can manage the devices, but the other remote NMS can't.

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in the above diagram with "SNMP" enabling at LAN and WAN interfaces.

Use default value for parameters that are not mentioned in the tables.

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ ***LAN*** ■ ***WAN***
Supported Versions	■ ***v1*** ■ ***v2c*** ■ ***v3***
Get / Set Community	***ReadCommunity / WriteCommunity***
Trap Event Receiver 1	***118.18.81.11***
WAN Access IP Address	***118.18.81.11***

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	***UserName1***	***UserName2***	***UserName3***
Password	***Password1***	***Password2***	***Disable***
Authentication	***MD5***	***SHA-1***	***Disable***
Encryption	***DES***	***Disable***	***Disable***
Privacy Mode	***authPriv***	***authNoPriv***	***noAuthNoPriv***
Privacy Key	***12345678***	***Disable***	***Disable***
Authority	***Read/Write***	***Read***	***Read***
Enable	■ ***Enable***	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In the above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. "Gateway 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

At first stage, the NMS manager prepares related information for all managed devices and records them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.

When the manager wants to configure the managed devices, the NMS system allows for that with SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol for configuring "Gateway 1". Only the "UserName1" account can let "Gateway 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one among them.

If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3.

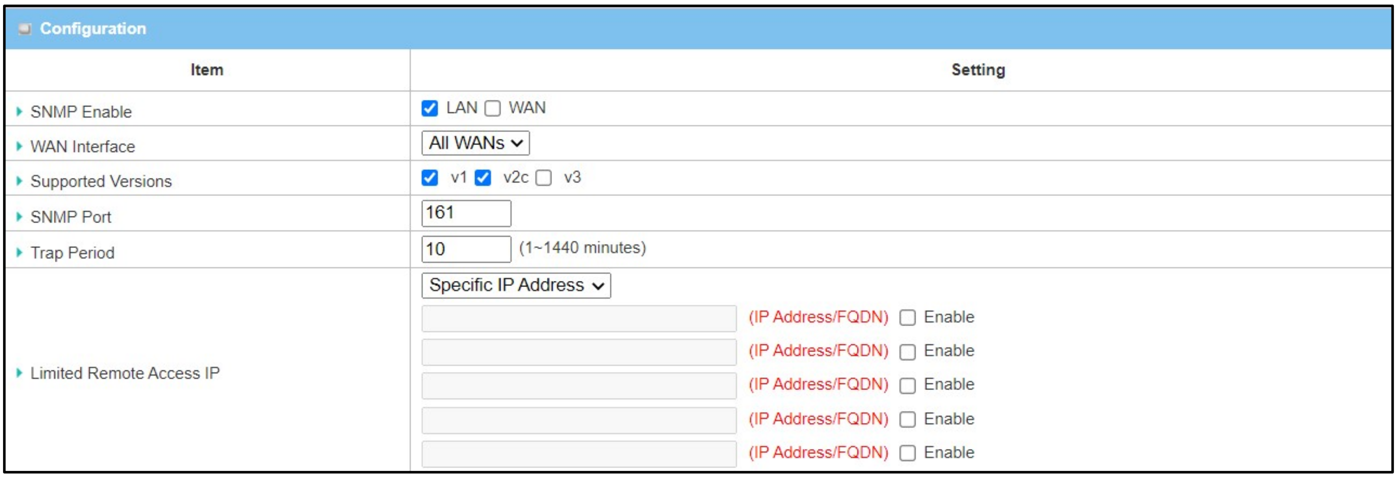
The remote NMS without privilege IP address can't manage "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

SNMP Setting

Go to Administration > Configure & Manage > SNMP tab.

The SNMP tab allows user to configure SNMP relevant settings, including interface, version, access control and trap receiver.

Enable SNMP



Configuration

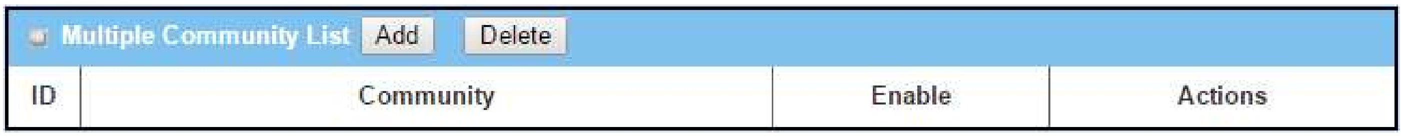
Item	Setting
SNMP Enable	☑ LAN ☐ WAN
WAN Interface	All WANs
Supported Versions	☑ v1 ☑ v2c ☐ v3
SNMP Port	161
Trap Period	10 (1~1440 minutes)
Limited Remote Access IP	Specific IP Address (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable

SNMP Item	Value setting	Description
SNMP Enable	1. Boxes are unchecked by default	Select the interface for the SNMP and enable SNMP functions. When **LAN** box is checked, it will activate SNMP functions and you can access SNMP from LAN side; When **WAN** box is checked, it will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	1. Required setting **2. ALL WANs is selected by default**	Specify the WAN interface that a remote SNMP host can use to access the device. By default, **All WANs** is selected, and there is no limitation for the WAN interface.
Supported Versions	1. Required setting 2. The boxes are unchecked by default	Select the version for the SNMP When **v1** box is checked, you can access SNMP version 1. When **v2** box is checked, you can access SNMP version 2. When **v3** box is checked, you can access SNMP version 3.
SNMP Port	1. String format: any port number 2. The default SNMP port is **161**. 3. Required setting	Specify the **SNMP Port**. Enter any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
Trap Period	Default is 10 minutes	Set the interval for the trap period.
Limited Remote	Blank by default	Set either a specific set of IP address or IP range to limit remote access.

Access IP	**Disabled by default**	
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Multiple Community

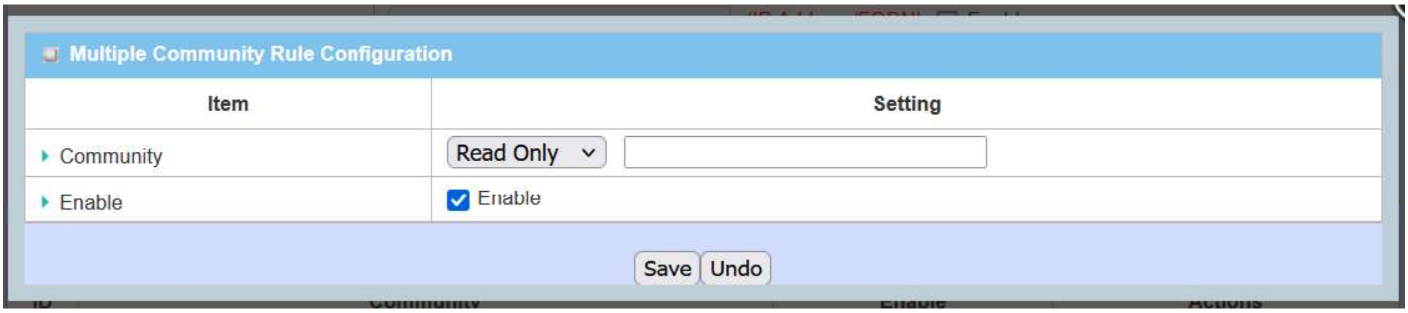
The SNMP allows you to customize your access control for version 1 and version 2 users. The router supports up to a maximum of 10 community sets.



Multiple Community List Add Delete

ID	Community	Enable	Actions

When **Add** button is applied, **Multiple Community Rule Configuration** screen will appear.



Multiple Community Rule Configuration

Item	Setting
Community	Read Only
Enable	☑ Enable

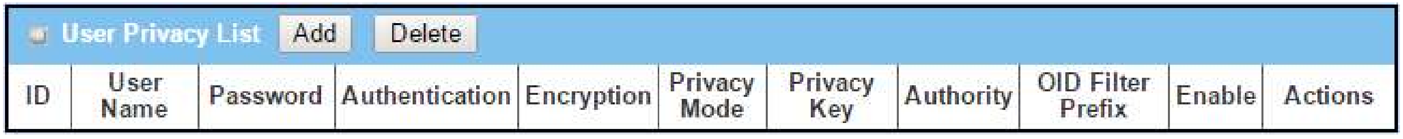
Save Undo

Multiple Community Rule Configuration		
Item	**Value setting**	**Description**
Community	1. Read Only is selected by default 2. Required setting 3. String format: any text	Specify this version 1 or version v2c user's community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	1. Box is checked by default	Click Enable to enable this version 1 or version v2c user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" to remind the user to click the main page Save button.
Undo	N/A	Click the **Undo** button to cancel the settings.

Create/Edit User Privacy

The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of

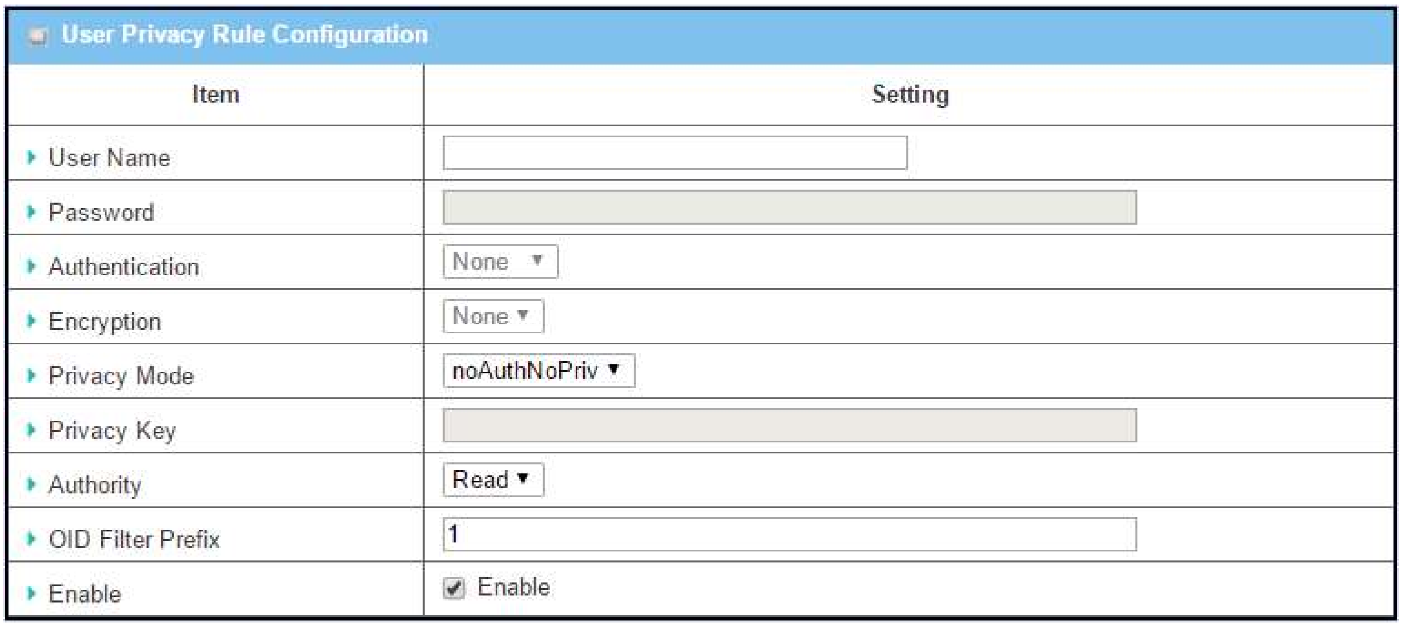
128 User Privacy sets.



User Privacy List

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

When **Add** button is applied, **User Privacy Rule Configuration** screen will appear.



User Privacy Rule Configuration

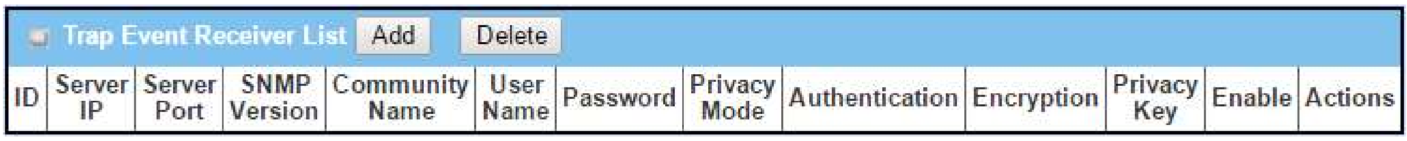
Item	Setting
User Name	
Password	
Authentication	None ▾
Encryption	None ▾
Privacy Mode	noAuthNoPriv ▾
Privacy Key	
Authority	Read ▾
OID Filter Prefix	1
Enable	☑ Enable

User Privacy Rule Configuration Item	Value setting	Description
User Name	1. Required setting 2. String format: any text	Specify the **User Name** for this version 3 user. ***Value Range***: 1 ~ 32 characters.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, specify the **Password** for this version 3 user. ***Value Range***: 8 ~ 64 characters.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, specify the **Encryption** protocols for this version 3 user. Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. noAuthNoPriv. No authentication types or encryption protocols are used. authNoPriv. Specify the Authentication and Password.

		authPriv. Specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, specify the **Privacy Key** (8 ~ 64 characters) for this version 3 user.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	1. Default value is 1 2. Required setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. ***Value Range***: 1 ~2080768.
Enable	1.The box is checked by default	Click **Enable** to enable this version 3 user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" to remind the user to click the main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

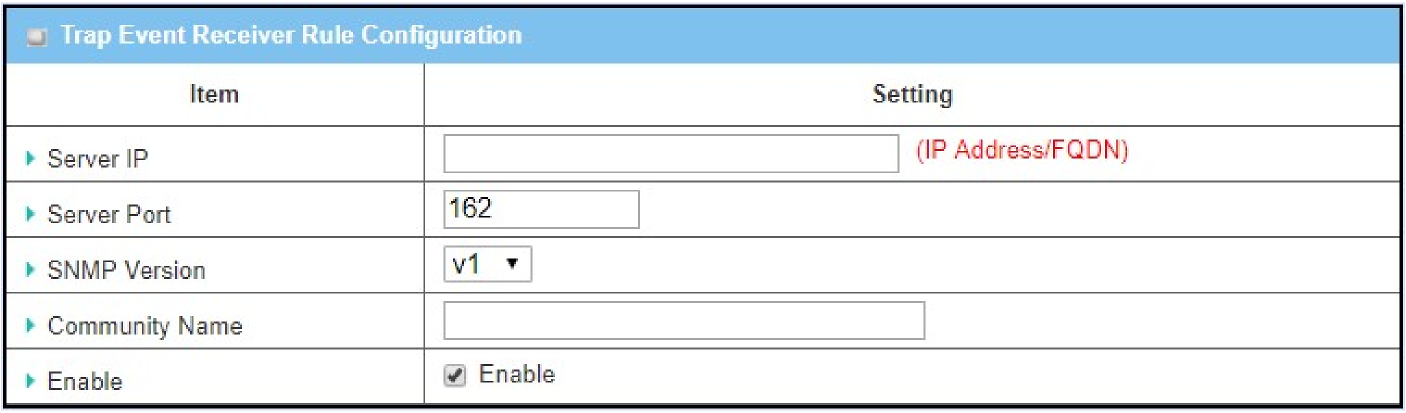
Create/Edit Trap Event Receiver

The SNMP allows you to customize your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.



ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions

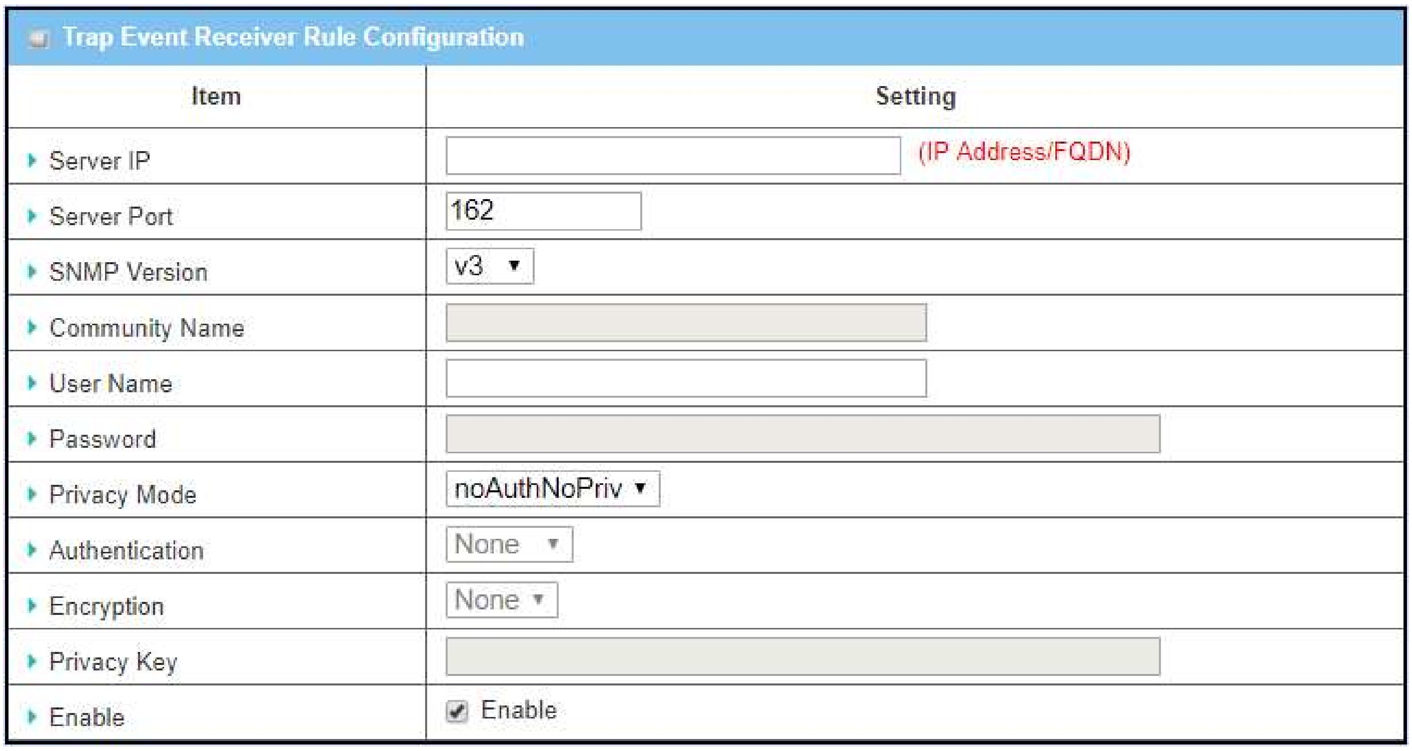
When the **Add** button is applied, **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will provide the version 1 required items.



Item	Setting
Server IP	(IP Address/FQDN)
Server Port	162
SNMP Version	v1 ▾
Community Name	
Enable	☑ Enable

When v2c is selected, the configuration screen is exactly the same as that of v1, except the version.

When v3 is selected, the configuration screen will provide more setting items for the version 3 Trap.



Trap Event Receiver Rule Configuration

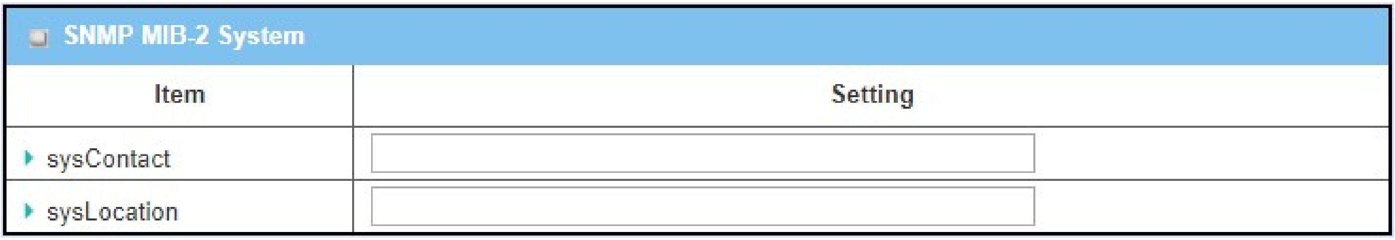
Item	Setting
Server IP	(IP Address/FQDN)
Server Port	162
SNMP Version	v3 ▾
Community Name	
User Name	
Password	
Privacy Mode	noAuthNoPriv ▾
Authentication	None ▾
Encryption	None ▾
Privacy Key	
Enable	☑ Enable

Trap Event Receiver Rule Configuration Item	 Value setting	 Description
Server IP	1. Required setting 2. String format: any IPv4 address or FQDN	Specify the trap **Server IP** or **FQDN**. Trap will be sent to the server IP/FQDN.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. Required setting	Specify the trap **Server Port**. Enter any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
SNMP Version	1. **v1** is selected by default	Select the version for the trap v1 The configuration screen will provide the version 1 required items. v2c The configuration screen will provide the version 2c required items. v3 The configuration screen will provide the version 3 required items.
Community Name	1. **v1** and **v2c** Required setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. ***Value Range***: 1 ~ 32 characters.
User Name	1. **v3** Required setting	Specify the **User Name** for this version 3 trap.

	2. String format: any text	***Value Range***: 1 ~ 32 characters.
Password	1. **v3** Required setting 2. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 trap. ***Value Range***: 8 ~ 64 characters.
Privacy Mode	1. **v3** Required setting 2. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 trap. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. **v3** Required setting 2. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 trap. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **v3** Required setting 2. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 trap. Selected the encryption protocols **DES / AES** to use.
Privacy Key	1. **v3** Required setting 2. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 trap.
Enable	Box is checked by default	Click **Enable** to enable this trap receiver.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" to remind the user to click the main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return the last page.

Specify SNMP MIB-2 System

If required, you can also specify the required information for the MIB-2 System.



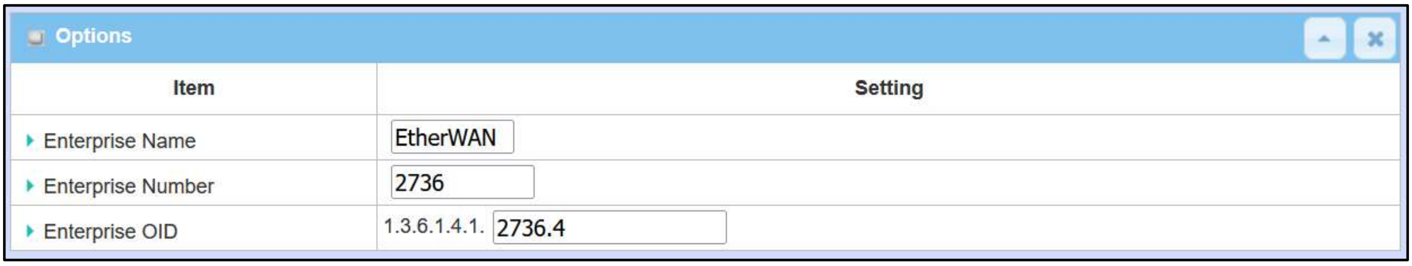
SNMP MIB-2 System

Item	Setting
sysContact	
sysLocation	

SNMP MIB-2 System Configuration		
Item	**Value setting**	**Description**
sysContact	1. Optional setting 2. String format: any text	Specify the contact information for MIB-2 system. ***Value Range***: 0 ~ 64 characters.
sysLocation	1. Optional setting 2. String format: any text	Specify the location information for MIB-2 system. ***Value Range***: 0 ~ 64 characters.

Edit SNMP Options

If you use some particular private MIB, you must enter the enterprise name, number and OID.
Note: EtherWAN doesn't support and provide private MIB.



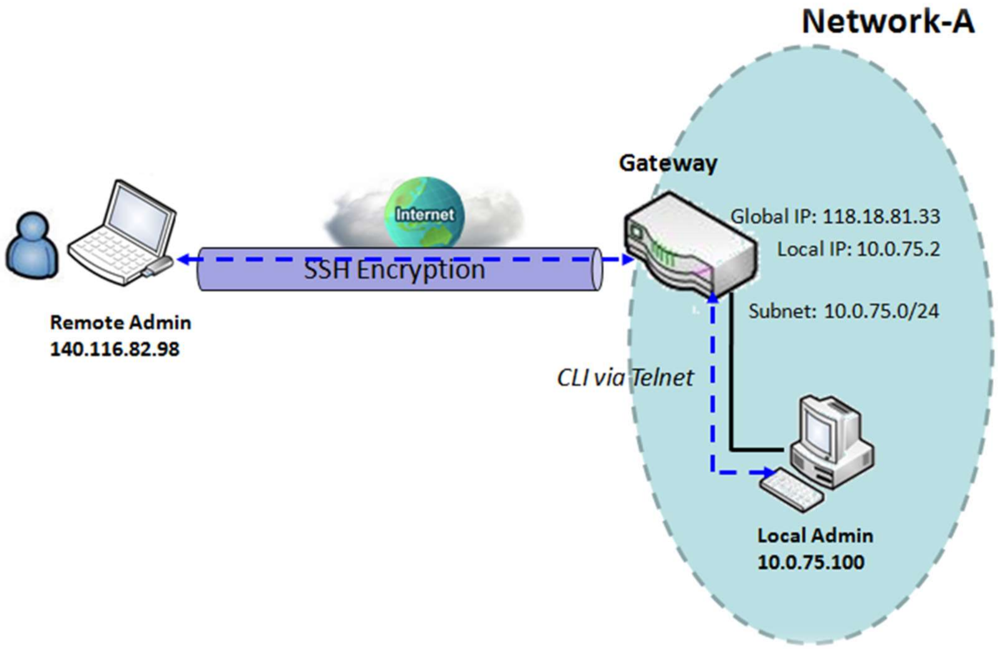
Item	Setting
Enterprise Name	EtherWAN
Enterprise Number	2736
Enterprise OID	1.3.6.1.4.1. 2736.4

Options		
Item	**Value setting**	**Description**
Enterprise Name	1. The default value is Etherwan 2. Required setting 3. String format: any text	Specify the **Enterprise Name** for the particular private MIB. ***Value Range***: 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '–', '_'.
Enterprise Number	The default value is 2736 2. Required setting 3. String format: any number	Specify the **Enterprise Number** for the particular private MIB. ***Value Range***: 1 ~2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.2736.4 2. Required setting 3. String format: any legal OID	Specify the **Enterprise OID** for the particular private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Click the **Save** button to save the configuration and apply your changes to SNMP functions.
Undo	N/A	Click the **Undo** button to cancel the settings.

7.1.4 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario



Scenario Application Timing

When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he/she may use "Telnet with CLI" function to do that by using Telnet or SSH utility.

Scenario Description

The Local Admin or the Remote Admin can manage the Gateway by using Telnet or SSH utility with privileged user name and password.

The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain text or encrypted text. It is suggested to use plain text in the Intranet for Local Admin to use Telnet, and encrypted text on the Internet for Remote Admin to use SSH.

Parameter Setup Example

The following table lists the parameter configuration as an example for the Gateway in the above diagram with "Telnet with CLI" enabled at LAN and WAN interfaces.

Use default value for parameters that are not mentioned in the table.

Configuration Path	[Telnet with CLI]-[Configuration]
Telnet	LAN: ■ ***Enable*** WAN: ***Enable*** Service Port ***23***
SSH	LAN: ■ ***Enable*** WAN: ■ ***Enable*** Service Port ***22*** ■ ***Enable***

Scenario Operation Procedure

In the above diagram, "Local Admin" or "Remote Admin" can manage the gateway from the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.

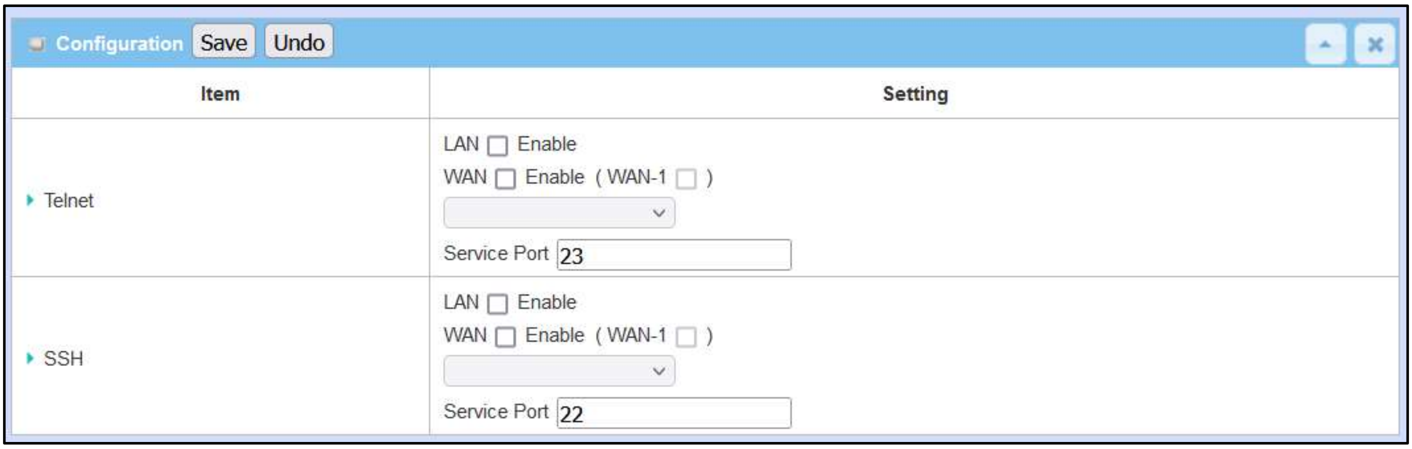
The "Local Admin" in the Intranet uses Telnet with a privileged account to log in to the Gateway.

The "Remote Admin" on the Internet uses SSH with a privileged account to log in to the Gateway.

Telnet & SSH Setting

Go to Administration > Configure & Manage > Telnet & SSH tab.

The Telnet & SSH setting allows administrator to access this device through the traditional Telnet or SSH Telnet program. Before you can Telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging Telnet and SSH.



Item	Setting
Telnet	LAN □ Enable WAN □ Enable (WAN-1 □) Service Port 23
SSH	LAN □ Enable WAN □ Enable (WAN-1 □) Service Port 22

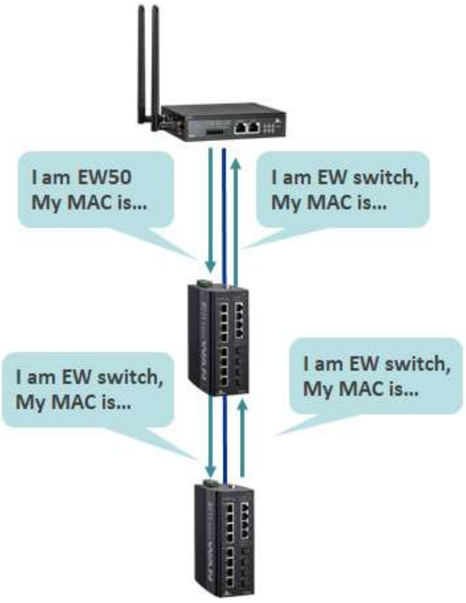
Configuration Item	Value setting	Description
Telnet	1. The LAN Enable box is checked by default. 2. By default **Service Port** is 23	Check the **Enable** box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces. You can set which number of Service Port you want to provide for the corresponding service. **Value Range:** 1 ~65535.
SSH	1. The LAN Enable box is checked by default. 2. By default **Service Port** is 22.	Check the Telnet **Enable** box to activate SSH Telnet function for connecting from LAN or WAN interfaces. You can set which number of Service Port you want to provide for the corresponding service. ***Value Range***: 1 ~65535.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

7.1.5 LLDP

LLDP is a network discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about devices to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management reachability and connection endpoint information from adjacent devices.

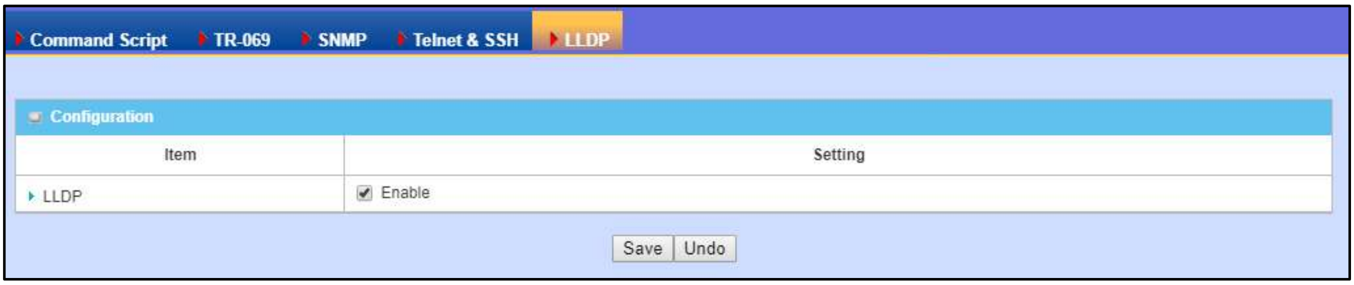
Using LLDP, a device is able to advertise its own identification information, its capabilities and media-specific configuration information, as well as learn the same information from the devices connected to it. LLDP advertises this information over Logical Link-Layer Control frames and the information received from other agents in IEEE-defined Management Information Bases (MIB) modules.

LLDP significantly aids in the deployment of any network device that supports the protocol. As a media independent protocol intended to be run on all IEEE 802 devices, LLDP may be used to discover routers, bridges, repeaters, WLAN APs, IP telephones, network camera or any LLDP-enabled device, regardless of manufacturer. Since LLDP runs over the data-link layer only, a switch running one network layer protocol can discover and learn about an access device running a different network layer protocol.



Note: If you are using EtherWAN's eVue network management utility, then make sure that LLDP is enabled on this and all other devices that you want to monitor with the software. eVue uses LLDP for its topology visualization.

To enable LLDP, check the box next to **Enable**, and then click **Save**.



Item	Setting
LLDP	☑ Enable

7.2 System Operation

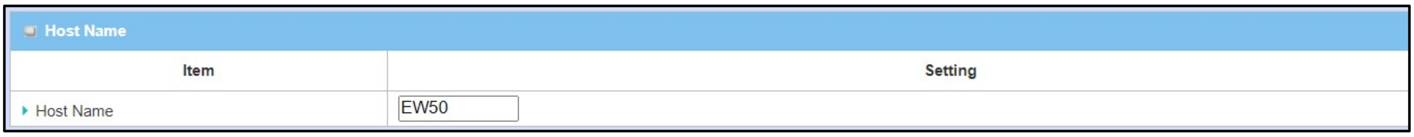
System Operation allows the network administrator to manage system and settings such as web-based utility, password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

7.2.1 Password & MMI

Go to Administration > System Operation > Password & MMI tab.

Setup Host Name

The Host Name screen allows network administrator to setup / change the host name of the gateway. Enter a new Host Name and click **Save**.

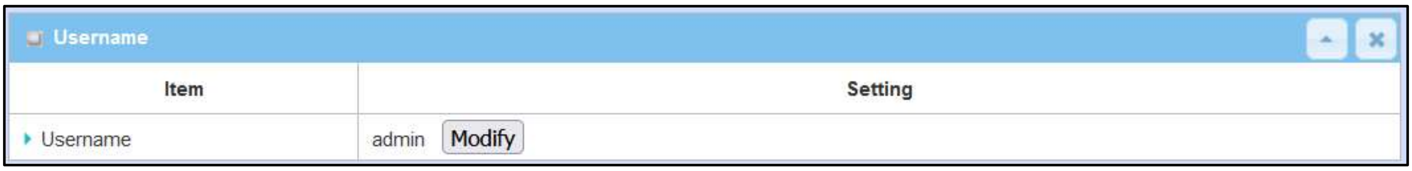


Host Name

Item	Setting
Host Name	EW50

Change UserName

Username screen allows network administrator to change the web-based MMI login account to access gateway. Click the Modify button and provide the new username setting.

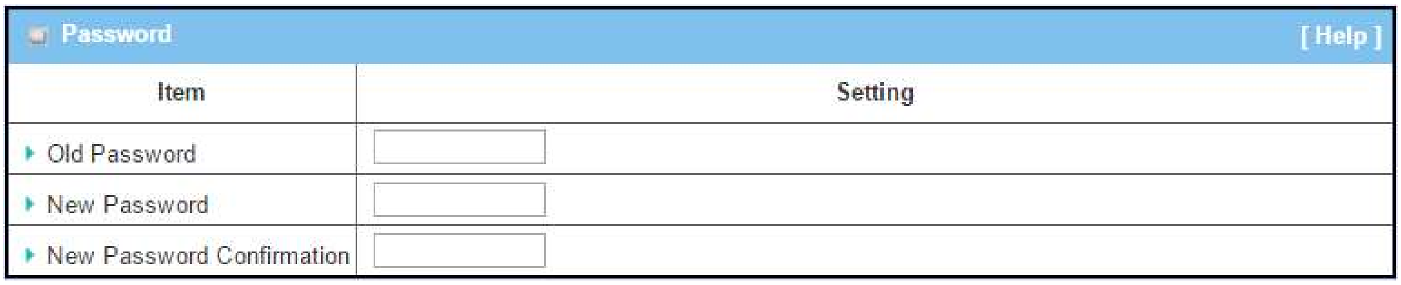


Username

Item	Setting
Username	admin Modify

Change Password

The change password screen allows network administrator to change the web-based MMI (Man-machine interface) login password.



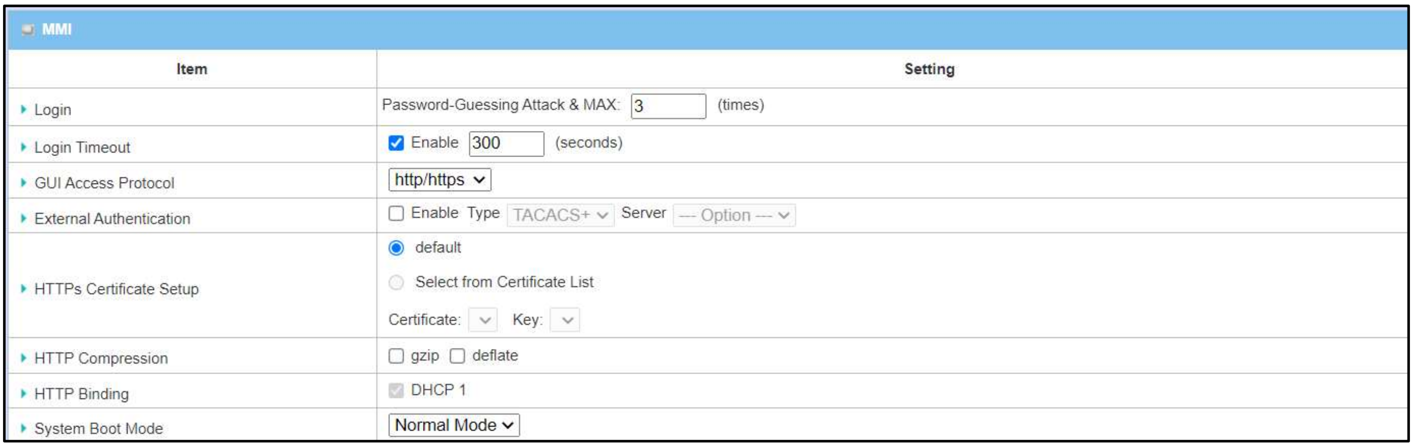
Password [Help]

Item	Setting
Old Password	
New Password	
New Password Confirmation	

Change Password		
Item	**Value Setting**	**Description**
Old Password	1. String: any text **2. Default password is 'admin'.**	Enter the current password.
New Password	String: any text	Enter new password
New Password Confirmation	String: any text	Enter new password again to confirm
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change MMI Setting for Accessing

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time.



MMI

Item	Setting
Login	Password-Guessing Attack & MAX: 3 (times)
Login Timeout	☑ Enable 300 (seconds)
GUI Access Protocol	http/https
External Authentication	□ Enable Type TACACS+ Server --- Option ---
HTTPs Certificate Setup	● default ○ Select from Certificate List Certificate: Key:
HTTP Compression	□ gzip □ deflate
HTTP Binding	☑ DHCP 1
System Boot Mode	Normal Mode

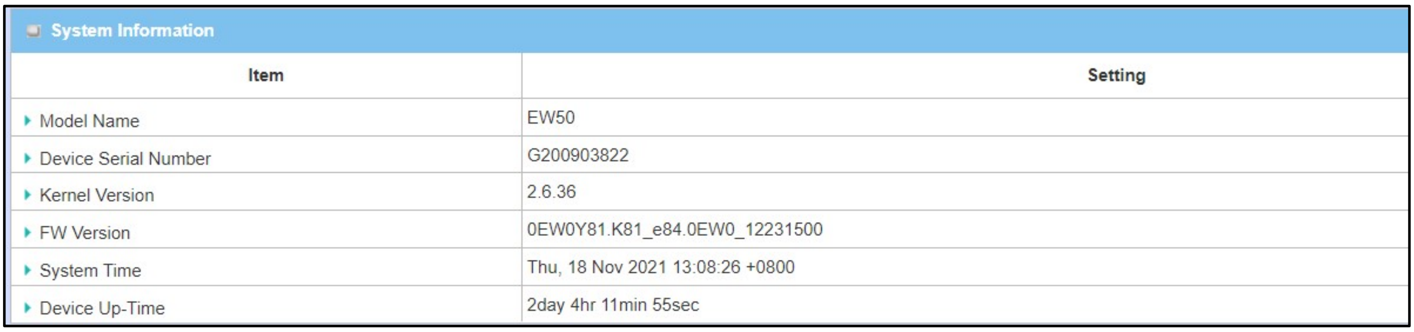
Note: Activating http/https on GUI Access Protocol will enable the use of TACACS+ as external authentication. If user uses Telnet/SSH login, EW50 will not support TACACS+ as an external authentication mechanism.

Web UI Item	Value Setting	Description
Login	3 times is set by default	Enter the login trial counting value. *Value Range*: 3 ~ 10. If someone tries to log in to the web GUI with incorrect password for more than this value, a warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will display and following login attempts ignored.
Login Timeout	Enable box is unchecked by default	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. *Value Range*: 30 ~ 65535.
GUI Access Protocol	**http/https** is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
External Authentication	Disabled by default	Check the box to enable external authentication, then select TACACS+. **Note:** Only in GUI access, TACACS+ will need to be selected.
HTTPs Certificate Setup	The **default** box is selected by default	If the https Access Protocol is selected, the HTTPs Certificate Setup option will be available for further configuration. You can leave it as default or select an expected certificate and key from the drop down list. Refer to Object **Definition > Certificate** Section for the Certificate configuration.
http Compression	unchecked by default.	Check the box (gzip, or deflate) if any compression method is preferred.
http Binding	1. Optional setting **2. DHCP-1 is checked by default**	Select the DHCP Server to bind with http access.
System Boot Mode	Normal mode is selected by default.	Select the system boot mode that will be adopted to boot up the device. **Normal Mode:** It takes longer boot up time, about 200 seconds, with complete firmware image check during the device booting. **Fast Mode:** It takes shorter boot up time, about 120 seconds, without checking the firmware image during the device booting. **Quick Mode:** It takes shorter boot up time, about 90 seconds, without checking the firmware image and create the internal database for User/Group/Captive Portal functions. **Note:** Use **Quick Mode** with care, once selected, the User/Group/Captive Portal function will become non-functional.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

7.2.2 System Information

The system Information screen gives network administrator a quick look up on the device information for the gateway.

Go to Administration > System Operation > System Information tab.



System Information

Item	Setting
Model Name	EW50
Device Serial Number	G200903822
Kernel Version	2.6.36
FW Version	0EW0Y81.K81_e84.0EW0_12231500
System Time	Thu, 18 Nov 2021 13:08:26 +0800
Device Up-Time	2day 4hr 11min 55sec

System Information		
Item	**Value Setting**	**Description**
Model Name	N/A	Displays the model name of this product.
Device Serial Number	N/A	Displays the serial number of this product.
Kernel Version	N/A	Displays the Linux kernel version of the product
FW Version	N/A	Displays the firmware version of the product
System Time	N/A	Displays the current system time that you browsed this web page.
Device Up-Time	N/A	Displays the statistics for the device up-time since last boot up.
Refresh	N/A	Click the **Refresh** button to update the system Information.

7.2.3 System Time

The gateway provides manual setup and auto-synchronized approaches for the administrator to set up the system time for the gateway. The supported time synchronization methods are Time Server, Manual, and PC. Select the method first, and then configure the corresponding settings.

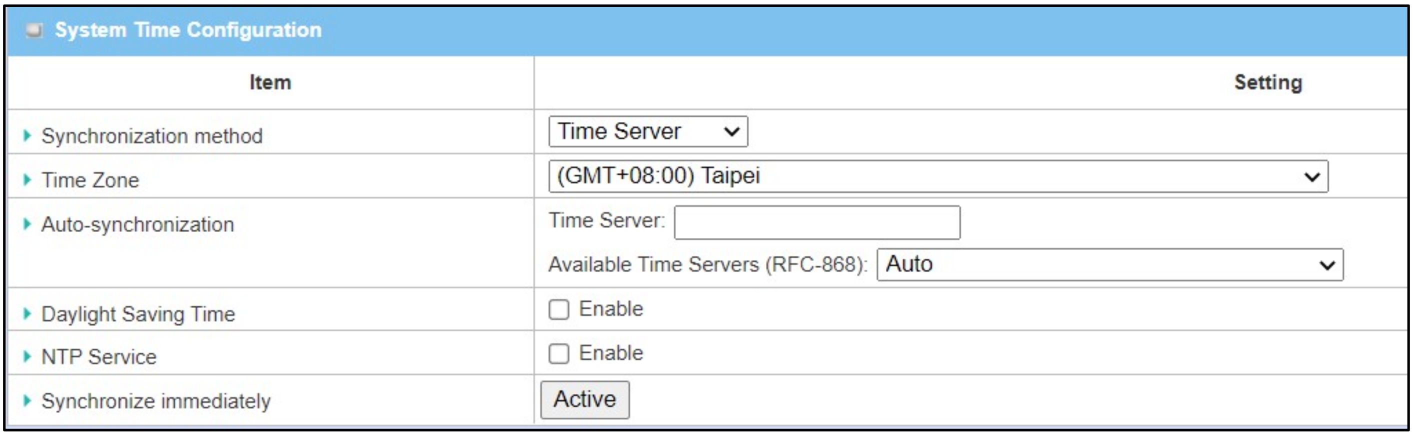
Instead of manually configuring the system time for the gateway, there are two simple and quick solutions to set the correct time as the system time for the gateway.

The first one is "Sync with Timer Server". Based on your selection of time zone and time server in the above time information configuration window, the system will communicate with time server by NTP Protocol to get system date and time after you click on the **Synchronize immediately** button.

The second one is "Sync with my PC". Select the method and the system will synchronize its date and time to the time of the administration PC.

Go to Administration > System Operation > System Time tab.

Synchronize with Time Server



System Time Configuration

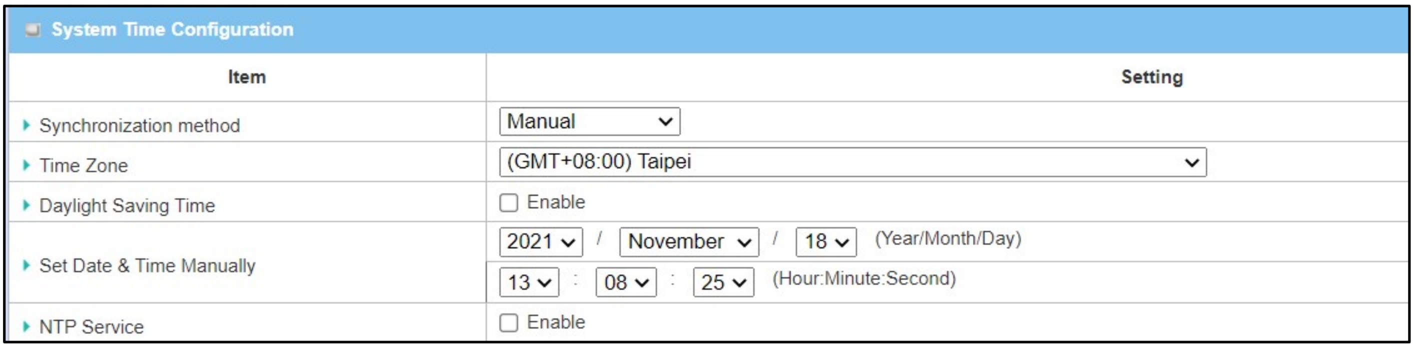
Item	Setting
Synchronization method	Time Server
Time Zone	(GMT+08:00) Taipei
Auto-synchronization	Time Server: Available Time Servers (RFC-868): Auto
Daylight Saving Time	□ Enable
NTP Service	□ Enable
Synchronize immediately	Active

System Time Information Item	Value Setting	Description
Synchronization method	1. Required item. **2. Time Server is selected by default.**	Select **Time Server** as the synchronization method for the system time.
Time Zone	1. Required item. 2. **GMT+00:00** is selected by default.	Select a time zone.
Auto-synchronization	1. Required item. 2. Auto is selected by default.	Enter the IP or FQDN for the NTP time server, or leave it as auto mode so that available servers will be used for time synchronization one by one.

Daylight Saving Time	1. Optional item. 2. Unchecked by default	Check the **Enable** button to activate the daylight saving function. When this function is enabled, specify the start and end date for the daylight saving time duration.
NTP Service	1. Optional item **2. Unchecked by default.**	Check the **Enable** button to activate the NTP Service function. When enabled, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Note: Remember to select a correct time zone for the device, otherwise, you will just get the UTC (Coordinated Universal Time) time, not the local time for the device.

Synchronize with Manually Setting



System Time Configuration

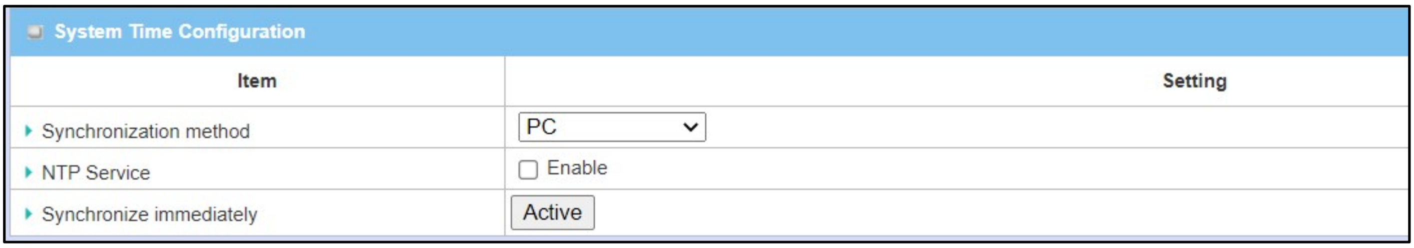
Item	Setting
Synchronization method	Manual
Time Zone	(GMT+08:00) Taipei
Daylight Saving Time	□ Enable
Set Date & Time Manually	2021 / November / 18 (Year/Month/Day) 13 : 08 : 25 (Hour:Minute:Second)
NTP Service	□ Enable

System Time Information

Item	Value Setting	Description
Synchronization method	1. Required item. **2. Time Server is selected by default.**	Select **Manual** as the synchronization method for the system time.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Daylight Saving Time	1. Optional item. 2. Unchecked by default	Check the **Enable** button to activate the daylight saving function. When this function is enabled, specify the start and end date for the daylight saving time duration.
Set Date & Time Manually	1. Optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
NTP Service	1. Optional item **2. Unchecked by default**	Check the **Enable** button to activate the NTP Service function. When enabled, the gateway can provide NTP server service for its local connected devices.

Save	N/A	Click the **Save** button to save the settings.

Synchronize with PC

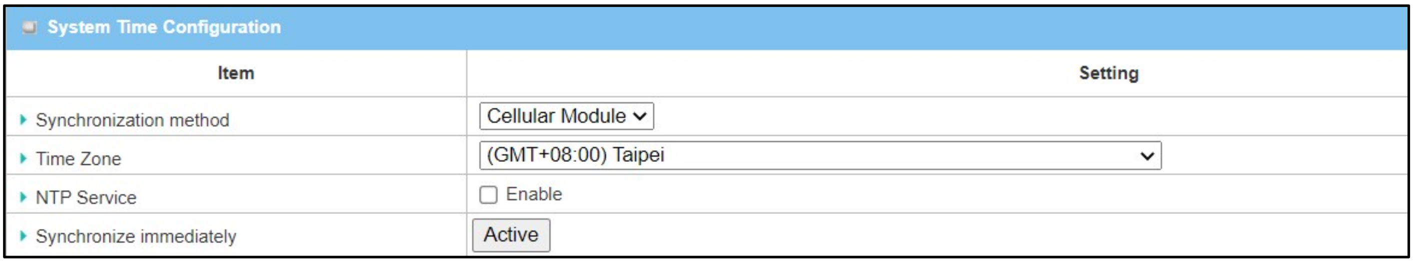


System Time Configuration

Item	Setting
Synchronization method	PC
NTP Service	□ Enable
Synchronize immediately	Active

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. Required item. **2. Time Server is selected by default.**	Select PC as the synchronization method for the system time to let system synchronize its date and time to the time of the administration PC.
NTP Service	1. Optional item **2. Unchecked by default**	Check the **Enable** button to activate the NTP Service function. When enabled, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.

Synchronize with Cellular Time Service



System Time Configuration

Item	Setting
Synchronization method	Cellular Module
Time Zone	(GMT+08:00) Taipei
NTP Service	□ Enable
Synchronize immediately	Active

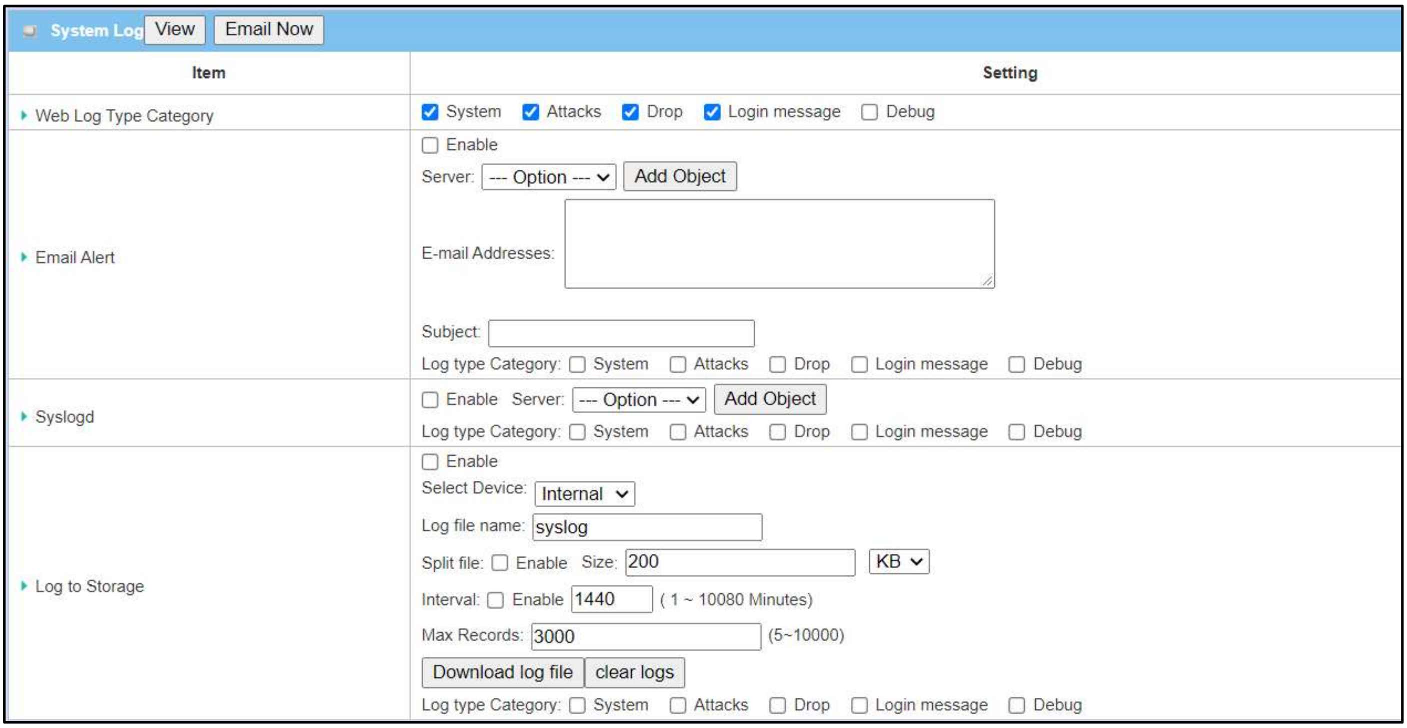
System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. Required item. **2. Time Server is selected by default.**	Select Cellular Module as the synchronization method for the system time to let system synchronize its date and time to the time provided from the connected mobile ISP.
Time Zone	1. Required item **2. GMT+00 :00 is selected by default.**	Select the time zone where the device is located.
NTP Service	1. Optional item **2. Unchecked by default**	Check the **Enable** button to activate the NTP Service function.

		When enabled, the gateway can provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Click the **Save** button to save the settings.

7.2.4 System Log

The system Log screen contains various event log tools to facilitate local event logging and remote reporting.

Go to Administration > System Operation > System Log tab.



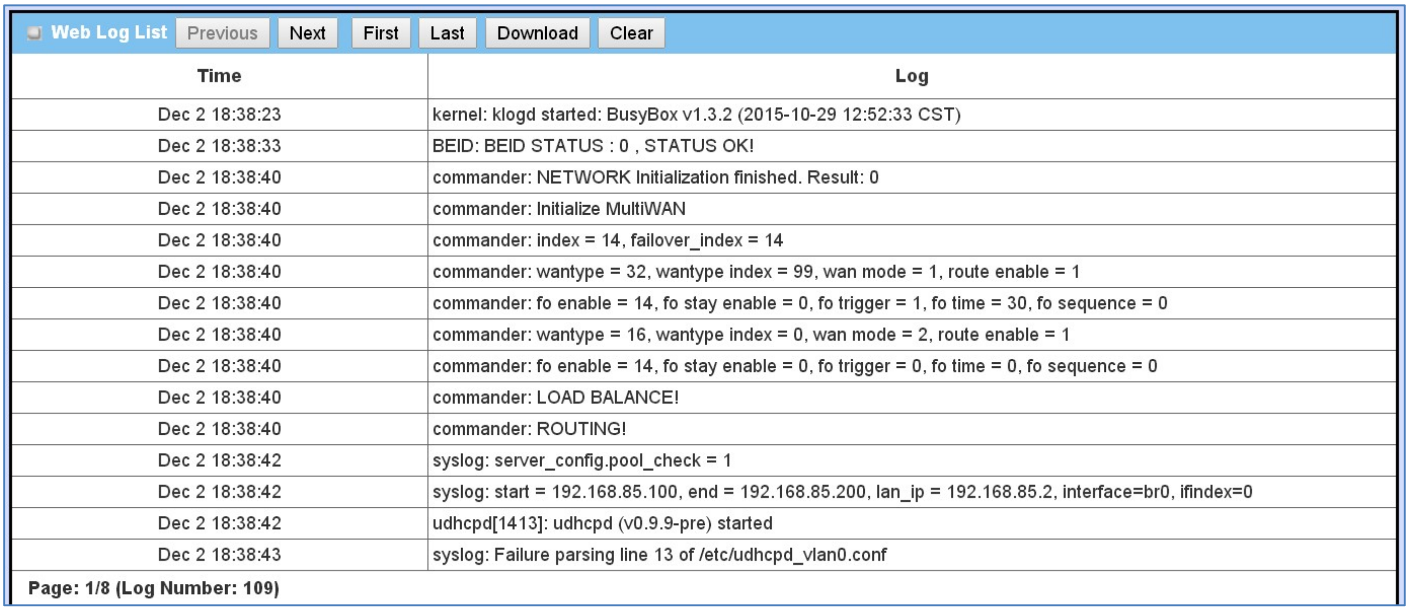
System Log [View] [Email Now]

Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- [Add Object] E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- [Add Object] Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Log to Storage	□ Enable Select Device: Internal Log file name: syslog Split file: □ Enable Size: 200 KB Interval: □ Enable 1440 (1 ~ 10080 Minutes) Max Records: 3000 (5~10000) [Download log file] [clear logs] Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

View & Email Log History

The **View** button allows for the viewing of log history. The **Email Now** button enables administrator to send instant Email for analysis.

View & Email Log History		
Item	**Value setting**	**Description**
View button	N/A	Click the **View** button to view Log History in Web Log List Window.
Email Now button	N/A	Click the **Email Now** button to send Log History via Email instantly.



Time	Log
Dec 2 18:38:23	kernel: klogd started: BusyBox v1.3.2 (2015-10-29 12:52:33 CST)
Dec 2 18:38:33	BEID: BEID STATUS : 0 , STATUS OK!
Dec 2 18:38:40	commander: NETWORK Initialization finished. Result: 0
Dec 2 18:38:40	commander: Initialize MultiWAN
Dec 2 18:38:40	commander: index = 14, failover_index = 14
Dec 2 18:38:40	commander: wantype = 32, wantype index = 99, wan mode = 1, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 1, fo time = 30, fo sequence = 0
Dec 2 18:38:40	commander: wantype = 16, wantype index = 0, wan mode = 2, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 0, fo time = 0, fo sequence = 0
Dec 2 18:38:40	commander: LOAD BALANCE!
Dec 2 18:38:40	commander: ROUTING!
Dec 2 18:38:42	syslog: server_config.pool_check = 1
Dec 2 18:38:42	syslog: start = 192.168.85.100, end = 192.168.85.200, lan_ip = 192.168.85.2, interface=br0, ifindex=0
Dec 2 18:38:42	udhcpd[1413]: udhcpd (v0.9.9-pre) started
Dec 2 18:38:43	syslog: Failure parsing line 13 of /etc/udhcpd_vlan0.conf

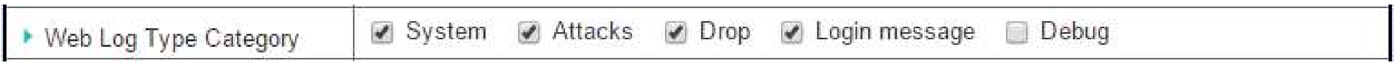
Page: 1/8 (Log Number: 109)

Web Log List Window		
Item	**Value Setting**	**Description**
Time column	N/A	Displays event time stamps
Log column	N/A	Displays Log messages

Web Log List Button Description		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button to move to the previous page.
Next	N/A	Click the **Next** button to move to the next page.
First	N/A	Click the **First** button to jump to the first page.
Last	N/A	Click the **Last** button to jump to the last page.
Download	N/A	Click the **Download** button to download log to your PC in tar file format.
Clear	N/A	Click the **Clear** button to clear all log.
Back	N/A	Click the **Back** button to return to the previous page.

Web Log Type Category

The Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section. Click on the View button to view Log History in the Web Log List window.

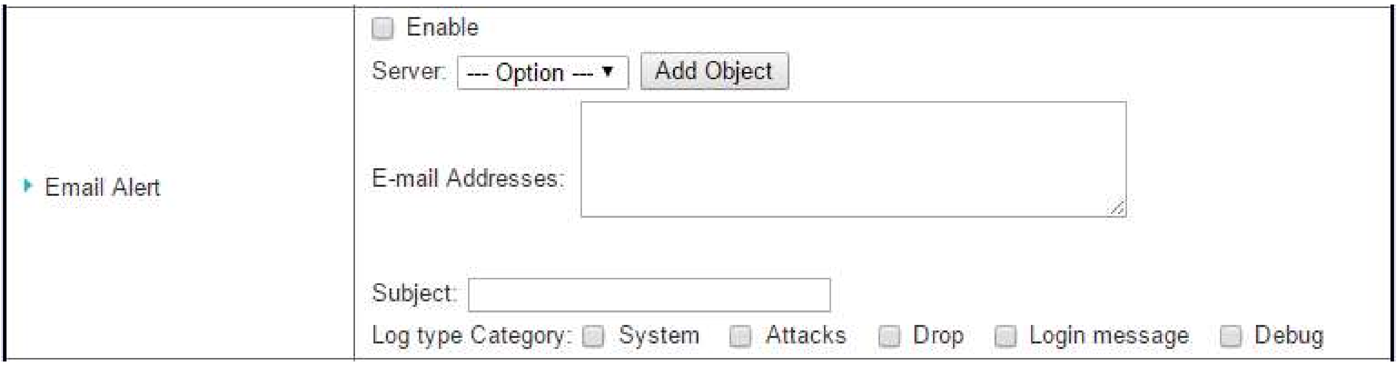


Web Log Type Category: ☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug

Web Log Type Category Setting Window		
Item	**Value Setting**	**Description**
System	Checked by default	Log system events and to display in the Web Log List window.
Attacks	Checked by default	Log attack events and to display in the Web Log List window.
Drop	Checked by default	Log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Log system login events and to display in the Web Log List window.
Debug	Unchecked by default	Log debug events and to display in the Web Log List window.

Email Alert

The Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.



Email Alert

□ Enable

Server: --- Option --- ▾ Add Object

E-mail Addresses:

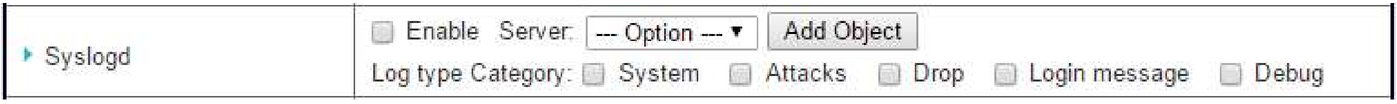
Subject:

Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check **Enable** box to enable sending event log messages to designated Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none is available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String: email format	Enter the recipient’s Email address. Separate Email addresses with comma ‘,’ or semicolon ‘;’ Enter the Email address in the format of ‘*myemail@domain.com*’
Subject	String: any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Syslogd

The Syslogd screen allows the network administrator to select the type of event to log and be sent to the designated Syslog server.



▸ Syslogd

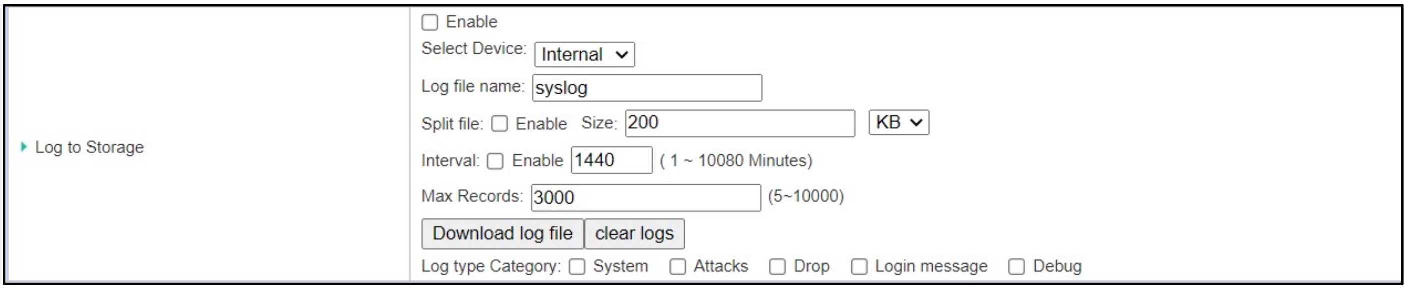
□ Enable Server: --- Option --- ▾ Add Object

Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
Server	N/A	Select one syslog server from the Server dropdown box to send event log to. If none is available, click the **Add Object** button to create a system log server. You may also add a system log server from the Object Definition > External Server > External Server tab.
Log type category	Unchecked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

Log to Storage

Log to Storage screen allows the network administrator to select the type of events to log and be stored at an internal or an external storage device.



▸ Log to Storage

□ Enable

Select Device: Internal ▾

Log file name: syslog

Split file: □ Enable Size: 200 KB ▾

Interval: □ Enable 1440 (1 ~ 10080 Minutes)

Max Records: 3000 (5~10000)

Download log file | clear logs

Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Unchecked by default	Enter log file name to save logs in designated storage.
Split file Enable	Unchecked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	**200 KB** is set by default	Enter the file size limit for each split log file. ***Value Range***: 10 ~1000.
Interval Enable	Unchecked by default	Check the **enable** box to enable the log interval setting.

Log Interval	**1440** is set by default	Enter the log interval setting. ***Value Range:*** 1 ~10080 Minutes.
Max Record	Default is 3000	Set the maximum number of records to be stored.
Log type category	Unchecked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

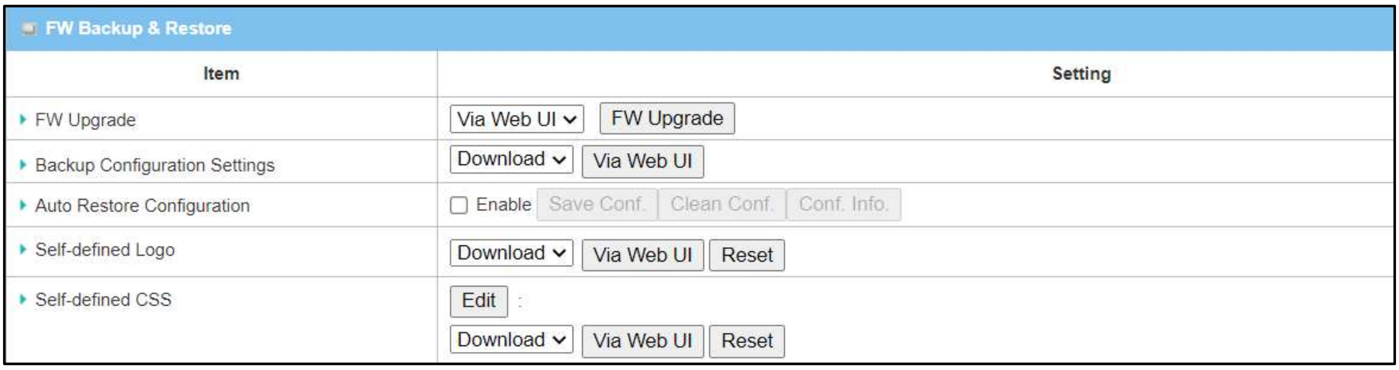
Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.
Clear Logs	N/A	Click the **Clear Logs** button to clear all stored logs.

7.2.5 Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available and also backup / restore the device configuration.

In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed.

Go to Administration > System Operation > Backup & Restore tab.



FW Backup & Restore

Item	Setting
FW Upgrade	Via Web UI ⌄ FW Upgrade
Backup Configuration Settings	Download ⌄ Via Web UI
Auto Restore Configuration	□ Enable Save Conf. Clean Conf. Conf. Info.
Self-defined Logo	Download ⌄ Via Web UI Reset
Self-defined CSS	Edit : Download ⌄ Via Web UI Reset

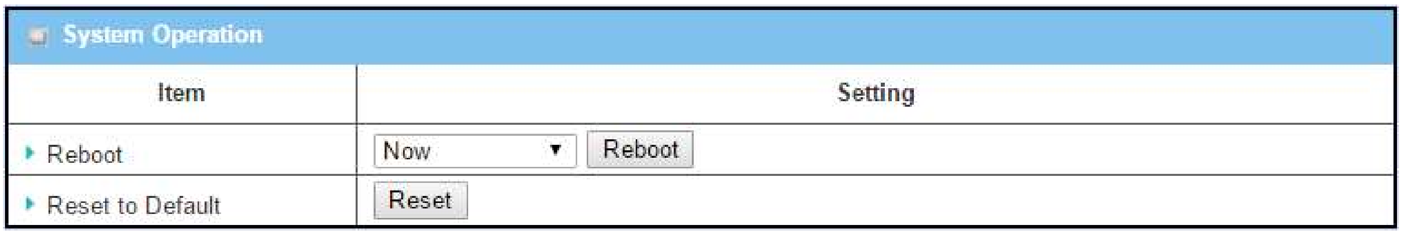
FW Backup & Restore Item	 Value Setting	 Description
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the “FW Upgrade” command button, specify the file name of new firmware by using the “Browse” button, and then click the “Upgrade” button to start the FW upgrading process. If you want to upgrade firmware which is from a GPL policy, please check “Accept unofficial firmware”
Backup Configuration Settings	Download is selected by default	You can back up or restore the device configuration settings by clicking the ***Via Web UI*** button. **Download**: for backing up the device configuration to a config.bin file. **Upload**: for restoring a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	Enable box is unchecked by default	Click the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf.** button, or clicking the **Clean Conf.** button to erase the stored customized configuration.
Self-defined Logo	N/A	Select Download or Upload button to download or upload a custom logo for the EW50.
Self-defined CSS	N/A	Edit, download, or upload the CSS for the device GUI.

6.2.6 Reboot & Reset

For some special reason or situation, you may need to reboot the gateway or reset the device configuration to its default settings. In addition to performing these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

Go to Administration > System Operation > Reboot & Reset tab.

In the Reboot & Reset window, you can reboot this device by clicking the “Reboot” button, and reset this device to default settings by clicking the “Reset” button.



System Operation

Item	Setting
Reboot	Now ▼ Reboot
Reset to Default	Reset

System Operation Window		
Item	**Value Setting**	**Description**
Reboot	Now is selected by default	Chick the **Reboot** button to reboot the gateway immediately or on a pre-defined time schedule. **Now**: Reboot immediately **Time Schedule**: Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated time to define a time schedule rule, go to **Object Definition > Scheduling > Configuration** tab.
Reset to Default	N/A	Click the **Reset** button to reset the device configuration to its default value.

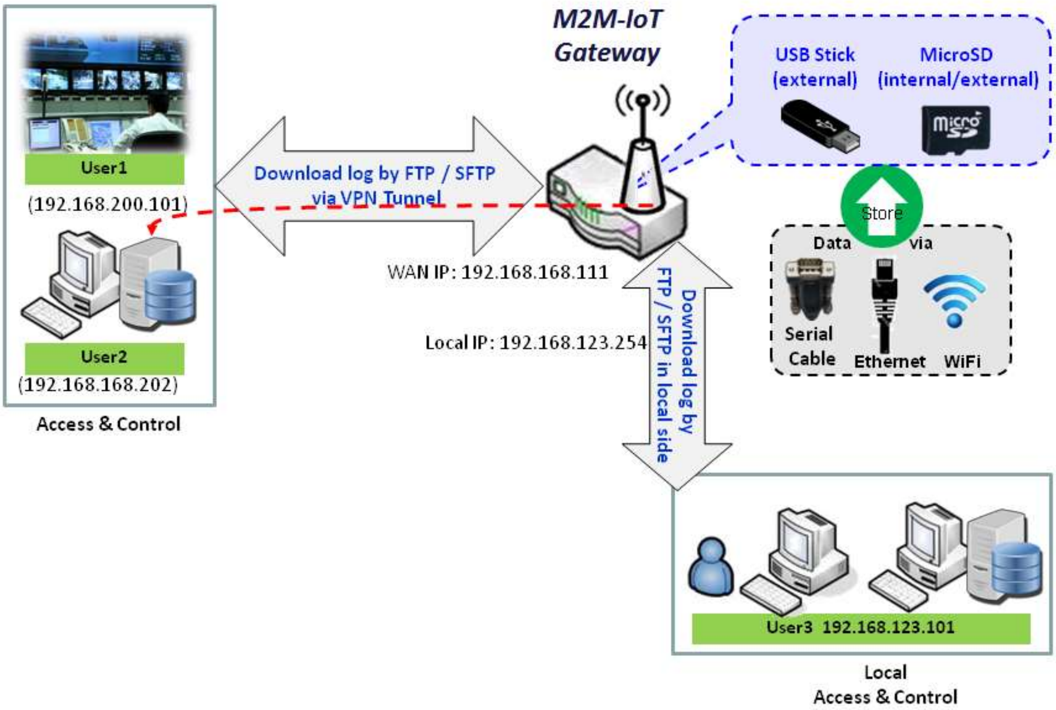
7.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can also connect anonymously if the server is configured to allow it.

For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

This gateway has an embedded FTP / SFTP server for administrator to download log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can log in to the server. After logging in, you can browse the log directory and have permission to download the stored log files and delete the files you have downloaded to make more storage space for further data logs.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.

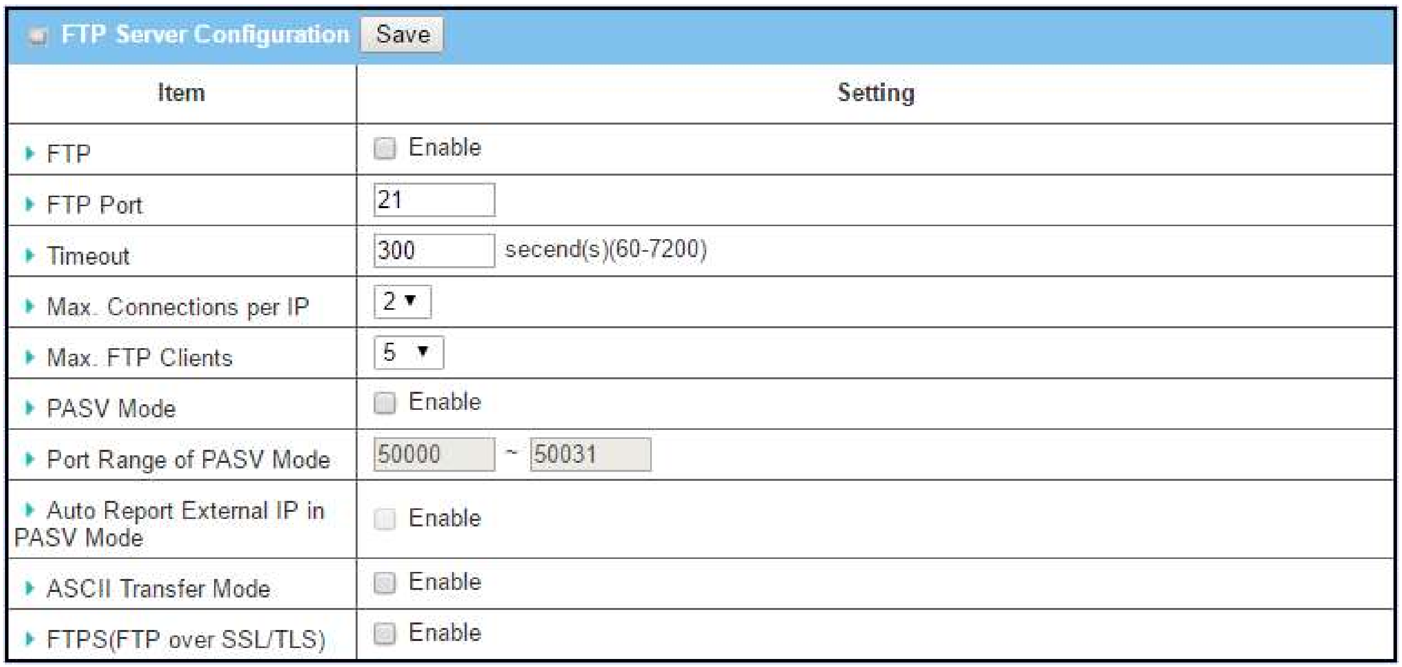


7.3.1 Server Configuration

This section allows user to set up the embedded FTP and SFTP server for retrieving log files.

Go to Administration > FTP > Server Configuration tab.

Enable FTP Server

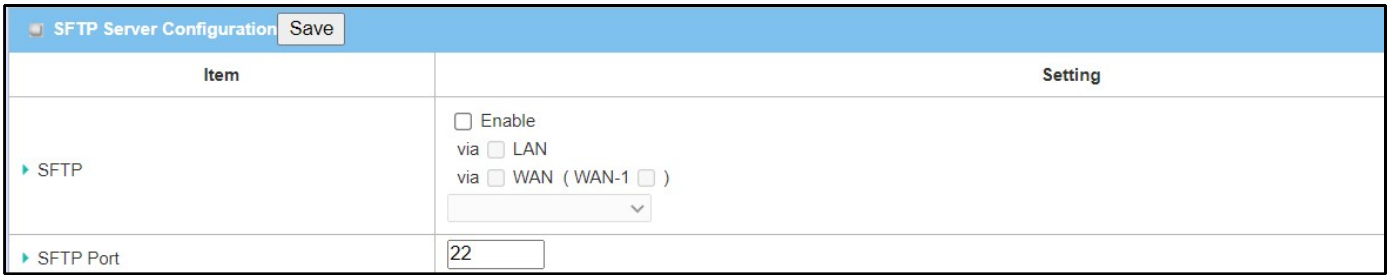


Item	Setting
FTP	□ Enable
FTP Port	21
Timeout	300 second(s)(60-7200)
Max. Connections per IP	2 ▾
Max. FTP Clients	5 ▾
PASV Mode	□ Enable
Port Range of PASV Mode	50000 ~ 50031
Auto Report External IP in PASV Mode	□ Enable
ASCII Transfer Mode	□ Enable
FTPS(FTP over SSL/TLS)	□ Enable

Configuration Item	Value setting	Description
FTP	Unchecked by default	Check **Enable** box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. Note: The embedded FTP Server is only for log downloading, so no write permission is implemented.
FTP Port	Port **21** is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port. ***Value Range***: 1 ~ 65535.
Timeout	**300** seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max. Connections per IP	**2** Clients are set by default.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	**5** Clients are set by default.	Specify the maximum number of clients for the FTP connection. Up to 32 clients are supported.

PASV Mode	Optional setting	Check the **Enable** box to activate the support of PASV mode for an FTP connection from FTP clients.
Port Range of PASV Mode	Port **50000** ~ **50031** is set by default.	Specify the port range to allocate for PASV style data connection. ***Value Range***: 1024 ~ 65535.
Auto Report External IP in PASV Mode	Optional setting	Check the **Enable** box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting	Check the **Enable** box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Check the **Enable** box to activate the support of secure connections via SSL/TLS.

Enable SFTP Server



Item	Setting
SFTP	□ Enable via □ LAN via □ WAN (WAN-1 □)
SFTP Port	22

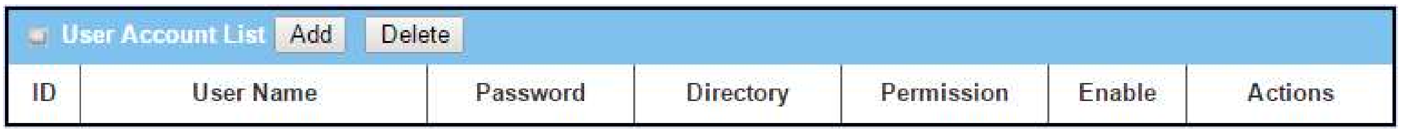
Configuration Item	Value setting	Description
SFTP	Unchecked by default	Check **Enable** box to activate the embedded SFTP Server function. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection. Select LAN or WAN for the SFTP connection.
SFTP Port	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. ***Value Range***: 1 ~ 65535.

7.3.2 User Account

This section allows the user to set up user accounts for logging to the embedded FTP and SFTP server to retrieve log files.

Go to Administration > FTP > User Account tab.

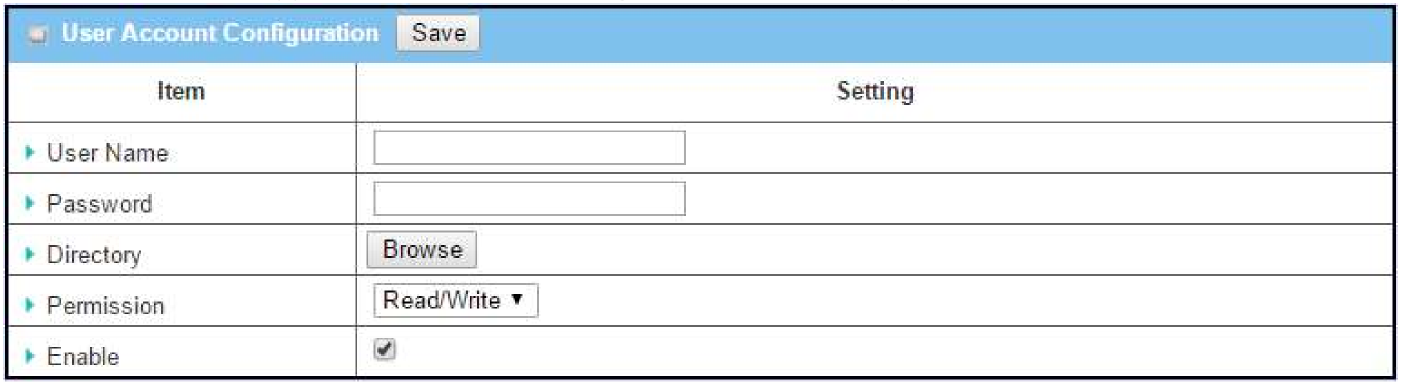
Create/Edit FTP User Accounts



User Account List

ID	User Name	Password	Directory	Permission	Enable	Actions

When **Add** button is applied, **User Account Configuration screen** will appear.



User Account Configuration

Item	Setting
User Name	
Password	
Directory	Browse
Permission	Read/Write ▼
Enable	☑

Configuration Item	Value setting	Description
User Name	String: non-blank string	Enter the user account name. ***Value Range***: 1 ~ 15 characters.
Password	String: no blank	Enter the user password.
Directory	N/A	Select a root directory after login.
Permission	**Read/Write** is selected by default.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no write permission is implemented, even if the **Read/Write** option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

7.4 Diagnostics

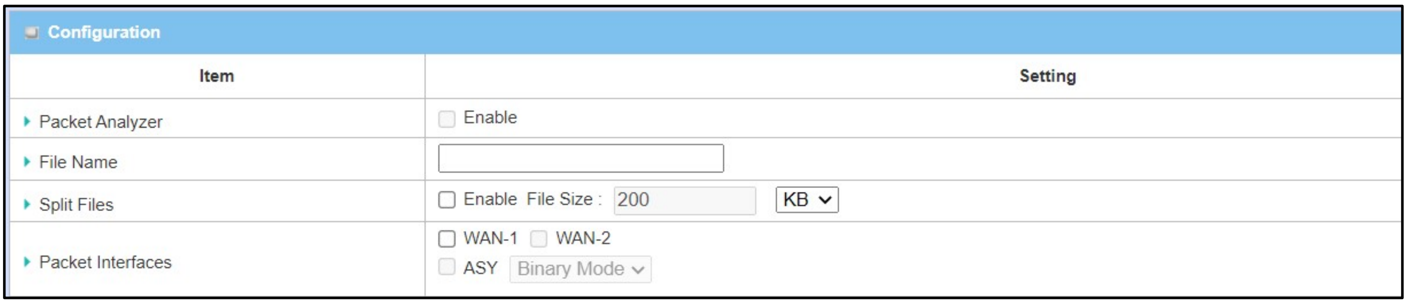
This gateway supports simple network diagnostic tools for the administrator to troubleshoot and analyze abnormal behavior or traffic passing through the gateway. There is be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and Tracert tools for testing the network connectivity issues.

7.4.1 Packet Analyzer

The Packet Analyzer can capture packets according to custom settings. User can specify interfaces to capture packets and filter by setting a rule. Ensure that log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** cannot be enabled.

Note: USB format should be FAT 32, it could be enabled by Mini tool ; Micro SD format should be EXT3, max.64GB. Recommend speed class 10 or above.

Go to Administration > Diagnostic > Packet Analyzer tab.



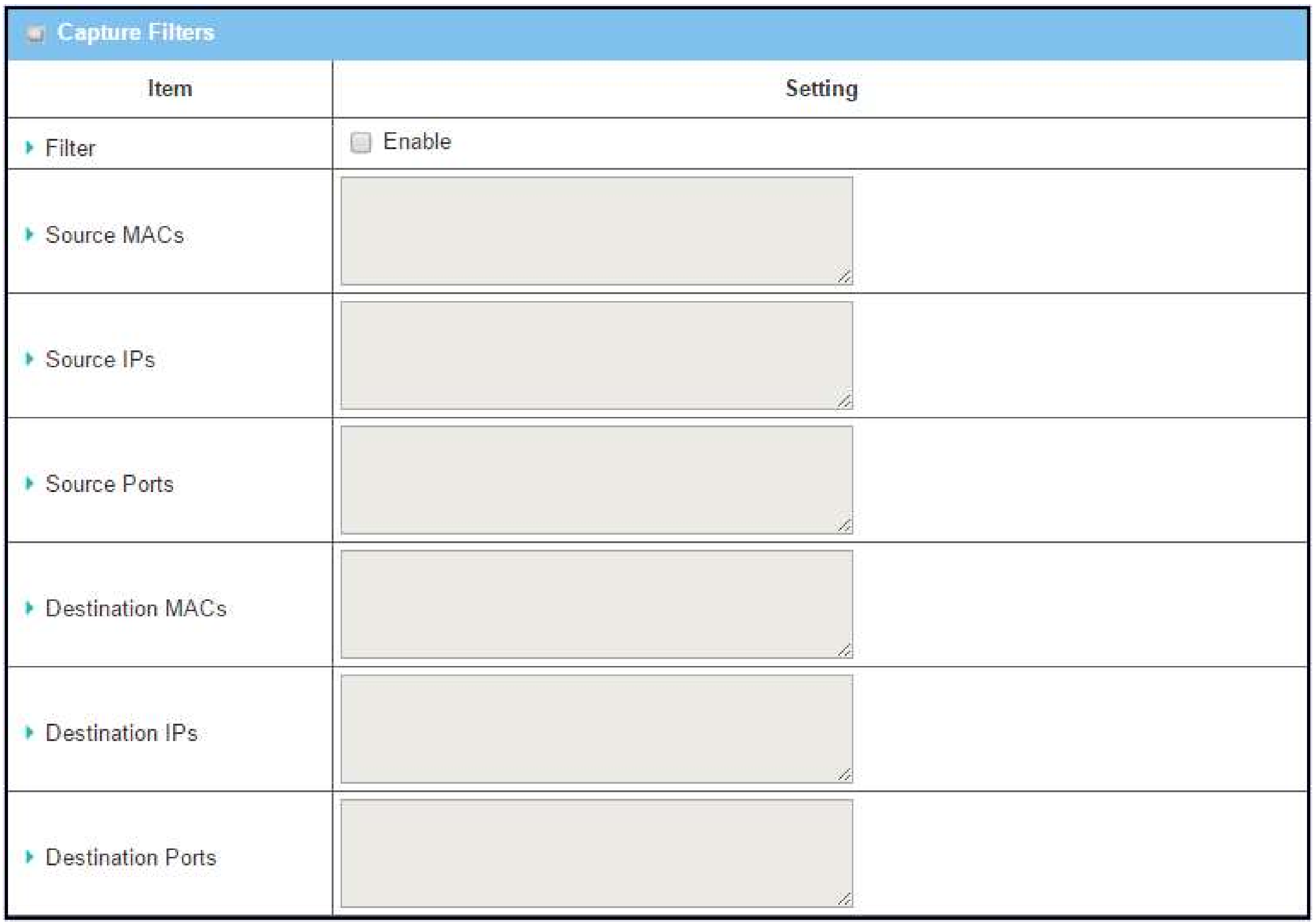
Configuration

Item	Setting
Packet Analyzer	□ Enable
File Name	
Split Files	□ Enable File Size : 200 KB
Packet Interfaces	□ WAN-1 □ WAN-2 □ ASY Binary Mode

Configuration		
Item	**Value setting**	**Description**
Packet Analyzer	Unchecked by default	Check **Enable** box to activate the Packet Analyzer function. If you cannot enable the checkbox, check if the storage is available. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. Optional setting 2. Default is blank, and the default file name is <**Interface**>_<**Date**>_<**index**>.	Enter a file name to save the captured packets in log storage. If **Split Files** option is also enabled, the file name will be appended with an index code “**_<index>”.** The file extension is **.pcap**.
Split Files	1. Optional setting 2. Default value of **File Size** is 200 KB.	Check **enable** box to split file whenever log file reaches the specified limit. If the **Split Files** option is enabled, you can further specify the **File Size** and **Unit** for the split files. ***Value Range***: 10 ~ 99999. NOTE: **File Size** cannot be less than 10 KB
Packet Interfaces	Optional setting	Define the interface(s) that **Packet Analyzer** should work on. At least one interface is required, but multiple selections are also accepted. Supported interfaces are: ● **WAN**: When the WAN is enabled at **Physical Interface**, it can be selected here. ● **ASY**: This means the serial communication interface. It is used to

		capture packets appearing in the **Field Communication**. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore previous settings.

Once you have enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which match the rules.



Capture Filters

Item	Setting
Filter	□ Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

Capture Fitters

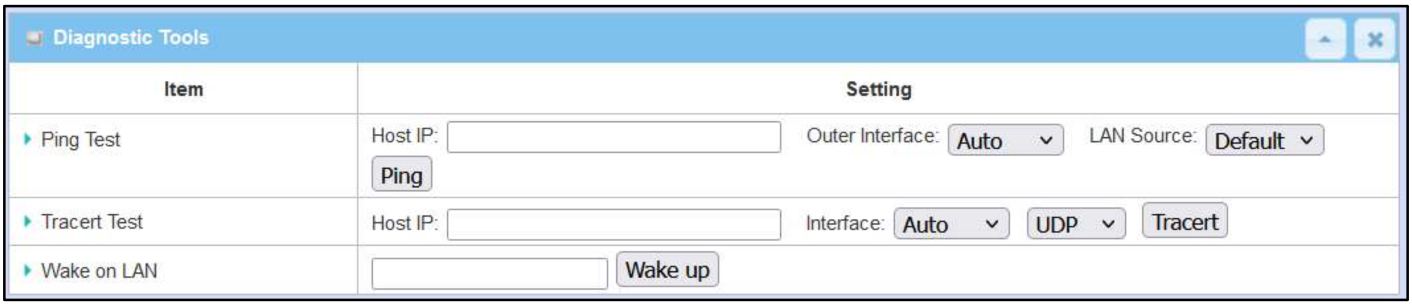
Item	Value setting	Description
Filter	Optional setting	Check **Enable** box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**, the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when matching any one MAC in the rule.
Source IPs	Optional setting	Define the filter rule with **Source IPs**, the source IP address of packets.

		Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when any IP is matched.
Source Ports	Optional setting	Define the filter rule with **Source Ports**, which means the source port of packets. The packets will be captured when any port is matched. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range***: 1 ~ 65535.
Destination MACs	Optional setting	Define the filter rule with **Destination MACs**, the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when any MAC address is matched.
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when any IP address in the rule is matched.
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**, the destination port of packets. The packets will be captured when any port in the rule is matched. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range***: 1 ~ 65535.

7.4.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check device connectivity.

Go to Administration > Diagnostic > Diagnostic Tools tab.



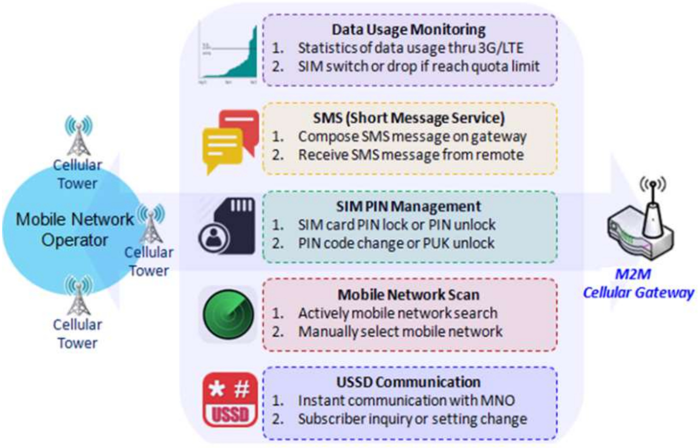
Diagnostic Tools

Item	Setting
Ping Test	Host IP: Outer Interface: Auto LAN Source: Default Ping
Tracert Test	Host IP: Interface: Auto UDP Tracert
Wake on LAN	Wake up

Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN and the test interface (LAN, WAN, or Auto), so the system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP). By default, it is **UDP**. The system will try to trace the specified host to test whether it is alive after clicking on **Tracert** button. A test result window will appear beneath it.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

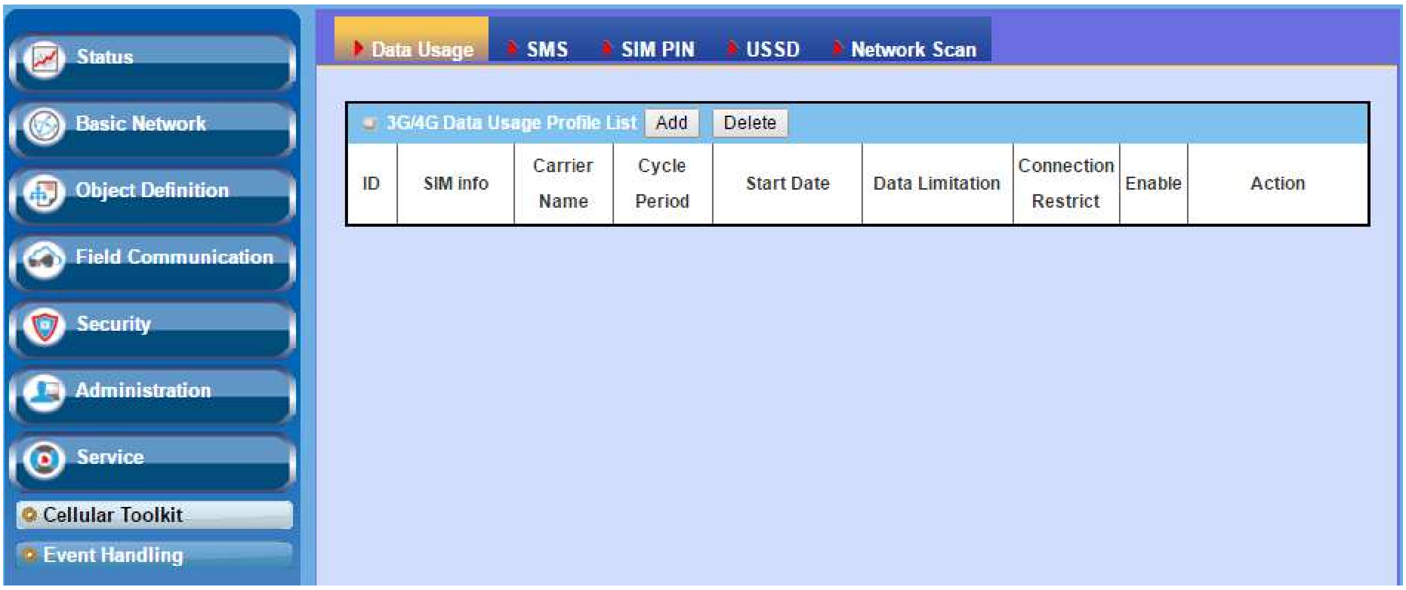
Chapter 8 Service

8.1 Cellular Toolkit


Data Usage Monitoring
1. Statistics of data usage thru 3G/LTE
2. SIM switch or drop if reach quota limit
SMS (Short Message Service)
1. Compose SMS message on gateway
2. Receive SMS message from remote
SIM PIN Management
1. SIM card PIN lock or PIN unlock
2. PIN code change or PUK unlock
Mobile Network Scan
1. Actively mobile network search
2. Manually select mobile network
USSD Communication
1. Instant communication with MNO
2. Subscriber inquiry or setting change
Cellular Tower
Mobile Network Operator
Cellular Tower
Cellular Tower
M2M Cellular Gateway

Besides cellular data connection, you may also want to monitor data usage of the cellular WAN, send text messages through SMS, change the PIN code of the SIM card, communicate with carrier/ISP by USSD (Unstructured Supplementary Service Data) command, or perform a cellular network scan for diagnostic purposes.

The Cellular Toolkit section includes several useful features that are related to cellular configuration or application. You can configure settings of Data Usage, SMS, SIM PIN, USSD, and Network Scan here. Please note that a valid SIM card is required to be inserted to device before you continue with the settings in this section.



3G/4G Data Usage Profile List

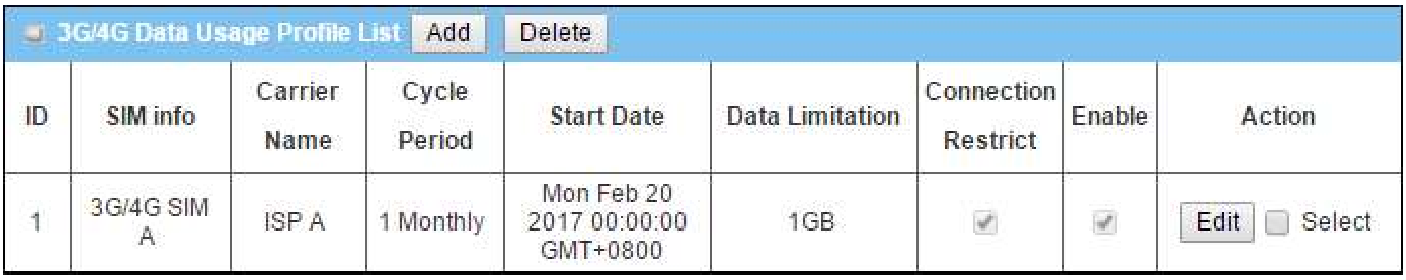
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

8.1.1 Data Usage

Most data plans for cellular connection have data caps. If data usage is over the set limit, it may result in a much lower data throughput that affects your operations, or an exceptionally high bill with over-quota surcharges.

With the Data Usage feature, the device will monitor cellular data usage continuously and take a preset action. Device can be set to drop the cellular data connection right away or, if a secondary SIM card is inserted, device will switch to the secondary SIM and establish another cellular data connection automatically.

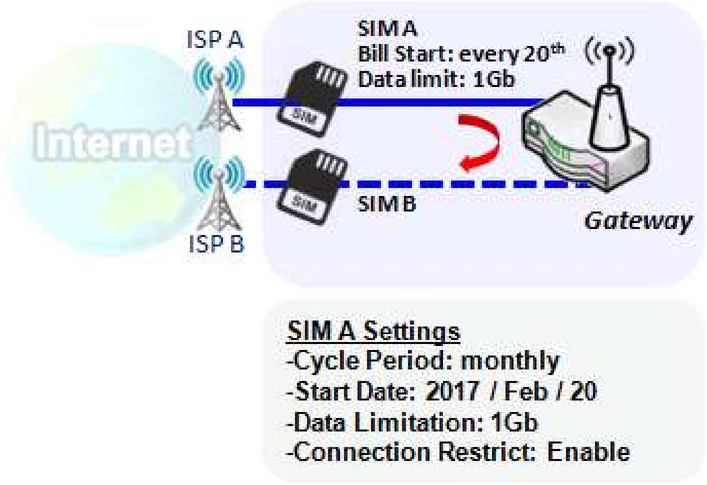
If Data Usage feature is enabled, the entire history of cellular data usage can be viewed at **Status** > **Statistics & Reports** > **Cellular Usage** tab.



3G/4G Data Usage Profile List Add Delete

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP A	1 Monthly	Mon Feb 20 2017 00:00:00 GMT+0800	1GB	✓	✓	Edit □ Select

3G/4G Data Usage

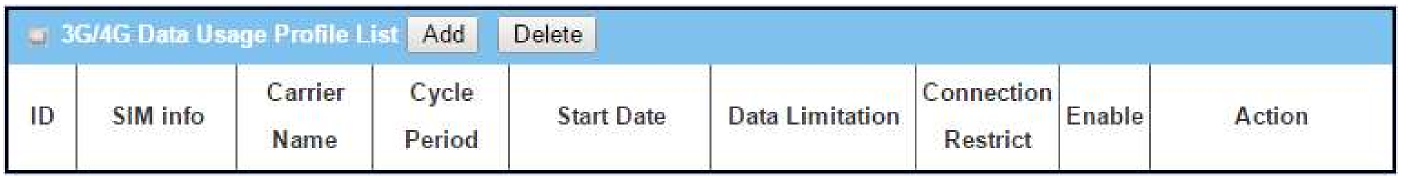


The data Usage feature allows the gateway device to continuously monitor cellular data usage and take action. In the diagram, the limit of SIM A is **1Gb** per month and billing start date is the **20th** of every month. The device can start a new calculation of data usage on every 20th of the month. **Enable Connection Restrict** will force the gateway to drop cellular connection of SIM A when data usage reaches 1Gb. If SIM failover feature is configured in **Internet Setup**, then the gateway will switch to SIM B and establish a new cellular data connection automatically.

Data Usage Setting

Go to **Service** > **Cellular Toolkit** > **Data Usage** tab.
To configure Data Usage, you need to know the billing start date, bill period, and data limit for your data plan.

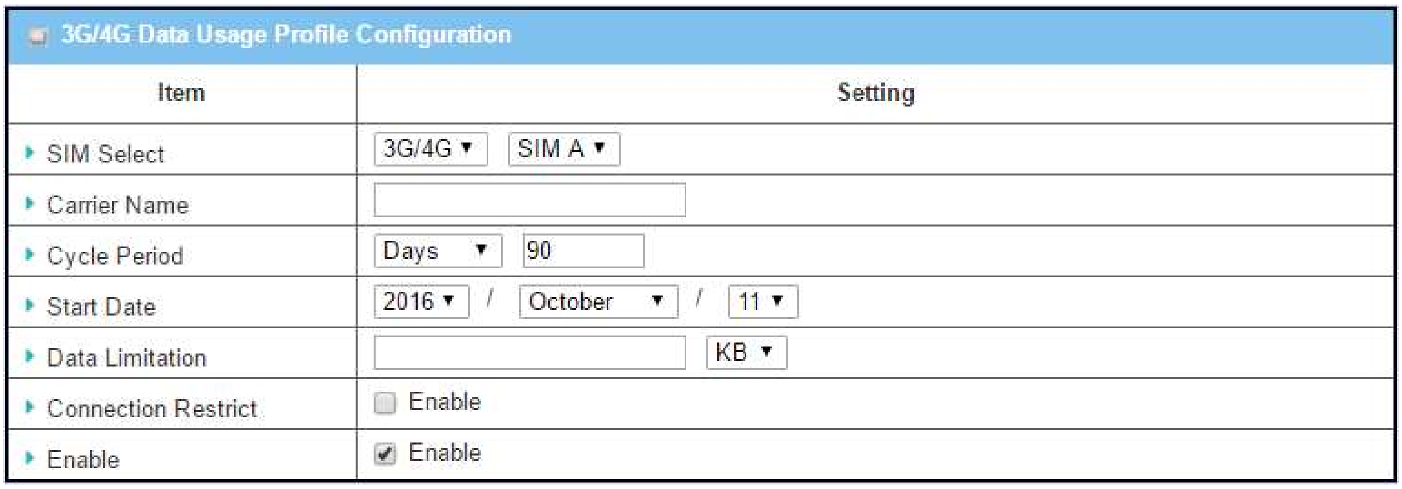
Create / Edit 3G/4G Data Usage Profile



3G/4G Data Usage Profile List [Add] [Delete]

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

When the **Add** button is applied, 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the Gateway.



3G/4G Data Usage Profile Configuration

Item	Setting
SIM Select	3G/4G ▾ SIM A ▾
Carrier Name	
Cycle Period	Days ▾ 90
Start Date	2016 ▾ / October ▾ / 11 ▾
Data Limitation	KB ▾
Connection Restrict	□ Enable
Enable	☑ Enable

3G/4G Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	**3G/4G-1** and **SIM A** by default.	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**), and a SIM card bound to the selected cellular interface to configure its data usage profile. **Note: 3G/4G-2** is only available for products with dual cellular modules.
Carrier Name	Optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	**Days** by default	The three types of cycle period are **Days**, **Weekly** and **Monthly**. **Days**: For per Days cycle periods, you must further specify the number of days in the second box. ***Value Range*****:** 1 ~ 90 days. **Weekly**, **Monthly**: The cycle period is one week or one month.
Start Date	N/A	Specify the date to start measuring network traffic. Don't select a day in the past. This will cause traffic statistics to be incorrect.
Data Limitation	N/A	Specify the allowable data limitation for the defined cycle period.
Connection Restrict	Un-Checked by default.	Check the **Enable** box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Un-Checked by default.	Check the **Enable** box to activate the data usage profile.

8.1.2 SMS

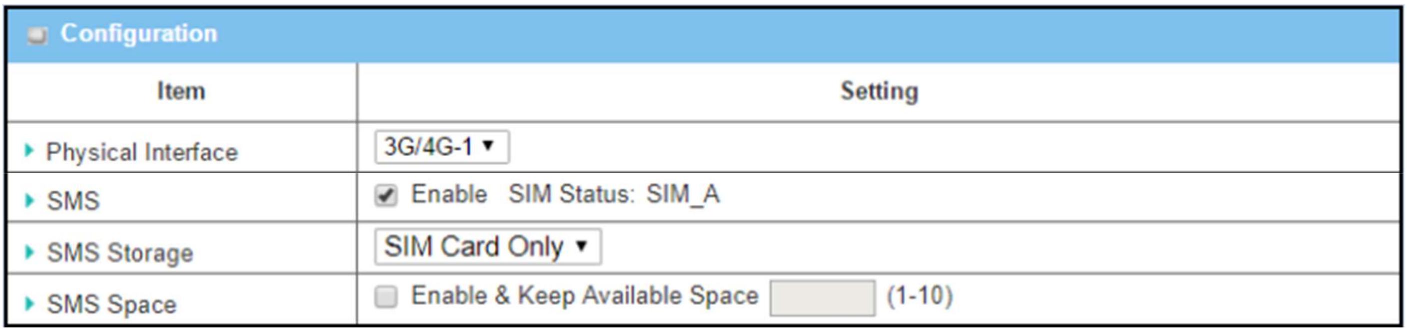
Short Message Service (SMS) is a text messaging service which is used to be widely-used on mobile phones. It uses standardized communications protocols to allow mobile phones or cellular devices to exchange short text messages in an instant and convenient way.

SMS Setting

Go to **Service** > **Cellular Toolkit** > **SMS** tab

With this gateway device, you can send SMS text messages or browse received SMS messages as you usually do on a cellular phone.

Setup SMS Configuration



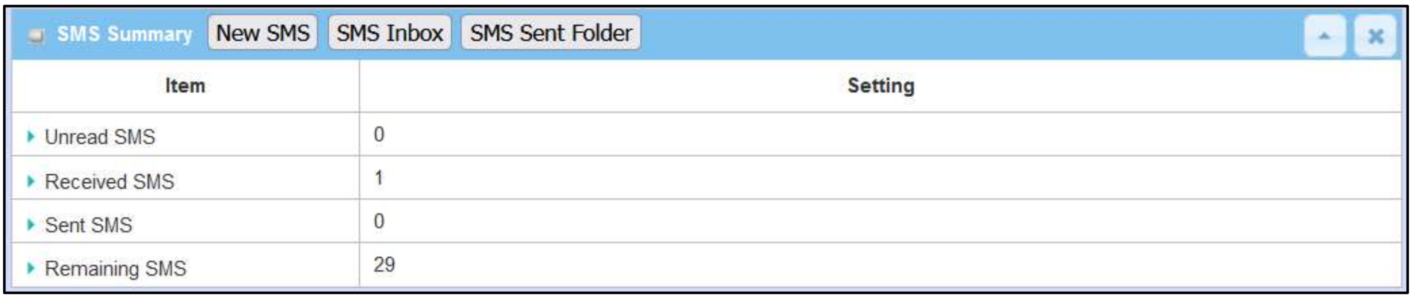
Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾
SMS	☑ Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▾
SMS Space	□ Enable & Keep Available Space [ ] (1-10)

Configuration Item	Value setting	Description
Physical Interface	**3G/4G-1** by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) for the following SMS function configuration. **Note: 3G/4G-2** is only available for products with dual cellular modules.
SMS	Checked by default	Check to enable SMS function.
SIM Status	N/A	Depends on current SIM status. The possible values are **SIM_A** or **SIM_B**.
SMS Storage	The box is **SIM Card Only** by default	This is the SMS storage location. Currently the only option is **SIM Card Only.**
SMS Space	Unchecked by default	Check the Enable box and specify a number (1-10) for message count to reserve some available storage space and prevent it from run out of storage. The oldest message(s) will be deleted when the SMS storage is nearly full.
Save	N/A	Click the **Save** button to save the settings

SMS Summary

Shows **Unread SMS**, **Received SMS**, **Remaining SMS**, and allows editing of SMS context to send, reading of SMS from SIM card.

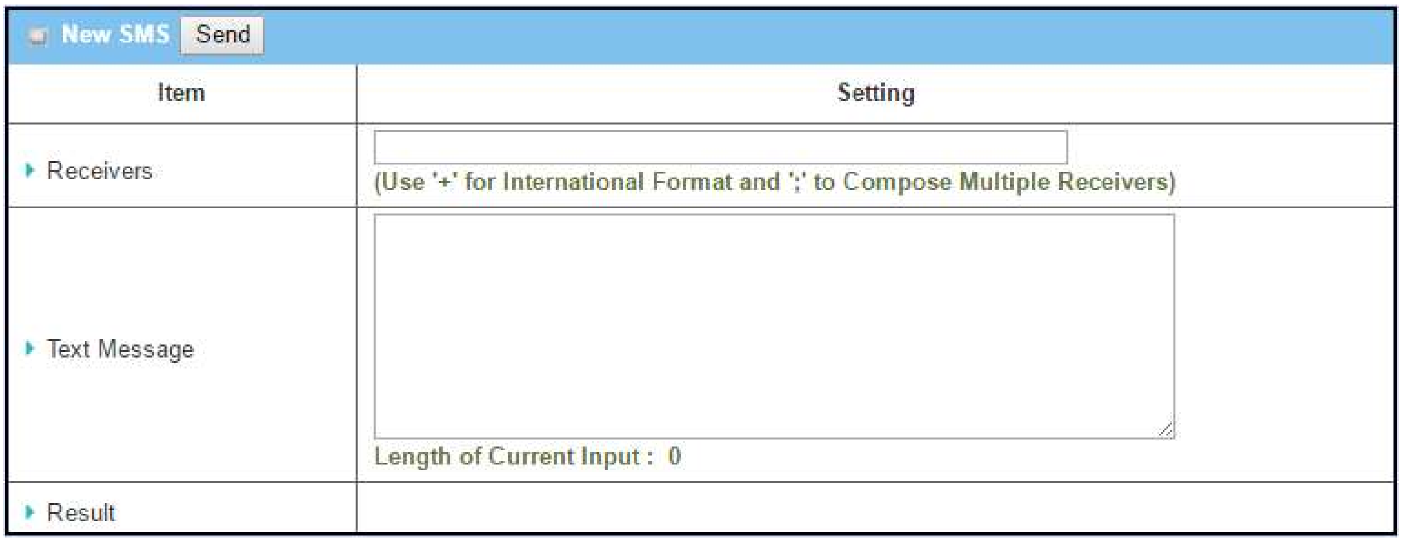


Item	Setting
Unread SMS	0
Received SMS	1
Sent SMS	0
Remaining SMS	29

SMS Summary		
Item	**Value setting**	**Description**
Unread SMS	N/A	If SIM card is inserted for first time, unread SMS value is zero. When new SMS are received but not read, this value increases.
Received SMS	N/A	This value records the number of SMS from SIM card.
Sent SMS	N/A	This value records the number of outgoing SMS. When one SMS is sent, this value Increases by one.
Remaining SMS	N/A	This value is SMS capacity minus received SMS.
New SMS	N/A	Click **New SMS** button, a **New SMS** screen appears. Refer to New SMS in the next page.
SMS Inbox	N/A	Click **SMS Inbox** button, a **SMS Inbox List** screen appears. User can read or delete SMS, reply SMS, or forward SMS from this screen. Refer to SMS Inbox List on the next page.
Refresh	N/A	Click the **Refresh** button to update the SMS summary.

New SMS

Configure SMS settings from this screen.

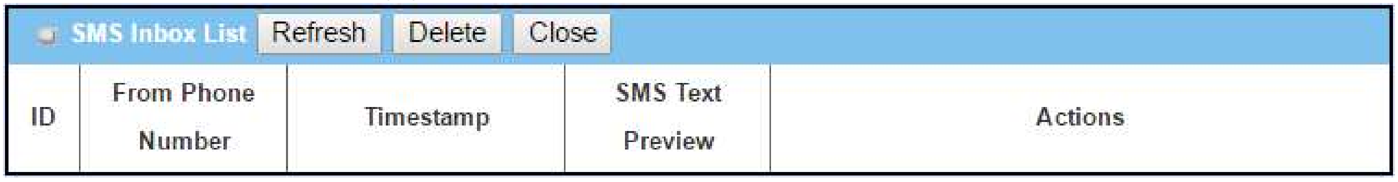


Item	Setting
Receivers	(Use '+' for International Format and ';' to Compose Multiple Receivers)
Text Message	Length of Current Input : 0
Result	

New SMS Item	Value setting	Description
Receivers	N/A	Enter the receivers to which the SMS will be sent. Add a semicolon to separate multiple receivers.
Text Message	N/A	Write the SMS content. A maximum length of 1023 characters is supported.
Send	N/A	Click the **Send** button have the text message sent as a SMS.
Result	N/A	If SMS has been sent successfully, it will show **Send OK**, otherwise **Send Failed** will be displayed.

SMS Inbox List

You can read or delete SMS, reply to SMS, or forward SMS from this screen.



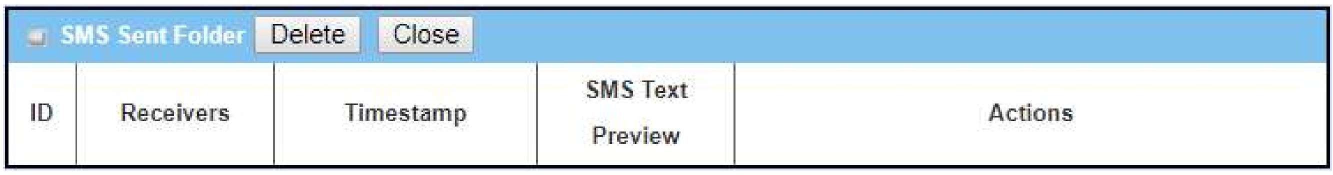
ID	From Phone Number	Timestamp	SMS Text Preview	Actions

SMS Inbox List Item	Value setting	Description
ID	N/A	The number of SMS.
From Phone Number	N/A	From phone number of SMS
Timestamp	N/A	Time received
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a specific message.
Action	Unchecked by default	Click the **Detail** button to read the SMS detail; Click the **Reply** / **Forward** button to reply/forward SMS.

		Check the box(es), and then click the **Delete** button to delete the SMS(s).
Refresh	N/A	Refresh the SMS Inbox list.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

SMS Sent Folder

You can read or delete SMS from this screen.



ID	Receivers	Timestamp	SMS Text Preview	Actions

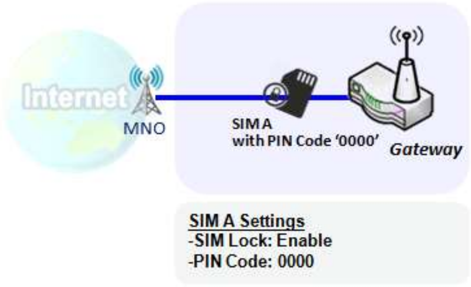
SMS Sent Folder		
Item	**Value setting**	**Description**
ID	N/A	The number of SMS.
Receivers	N/A	Receiver list for the sent SMS.
Timestamp	N/A	What time the SMS is sent
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a certain message.
Action	The box is unchecked by default	Click the **Detail** button to read the SMS detail Besides, you can check the box(es), and then click the **Delete** button to delete the checked record(s).
Refresh	N/A	Refresh the SMS Sent Folder.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

8.1.3 SIM PIN

In most cases, users need to insert a SIM card (a.k.a. UICC) into end devices connecting to a cellular network. The SIM card is usually released by mobile operators or service providers. Each SIM card has a unique number (so-called ICCID) for network owners or service providers to identify each subscriber. As SIM cards play an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access.

Enabling a PIN code in SIM card is an easy and effective way of protecting cellular devices from unauthorized access. This gateway device allows you to activate and manage PIN code son a SIM card through the web GUI.

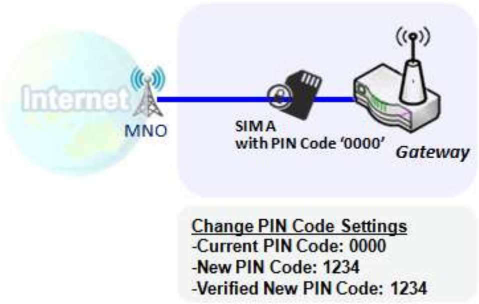
Activate PIN code on SIM Card



SIM A Settings
-SIM Lock: Enable
-PIN Code: 0000

This gateway device allows you to activate a PIN code on SIM card. This example shows how to activate PIN code on SIM-A for 3G/4G-1 with default PIN code “**0000**”.

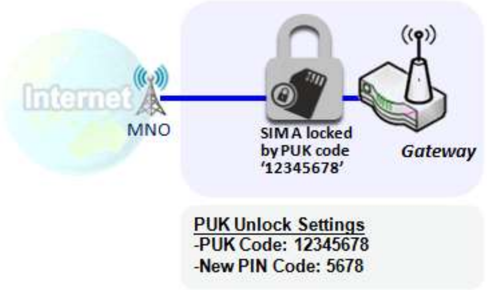
Change PIN code on SIM Card



Change PIN Code Settings
-Current PIN Code: 0000
-New PIN Code: 1234
-Verified New PIN Code: 1234

This gateway device allows you to change PIN code on SIM card. Following the example above, you need to type original PIN code “**0000**”, and then type new PIN code: ‘**1234**’ to set the new PIN code to ‘**1234**’. To confirm the new PIN code retype the new PIN code **1234** in the Verified New PIN Code field again.

Unlock SIM card by PUK Code



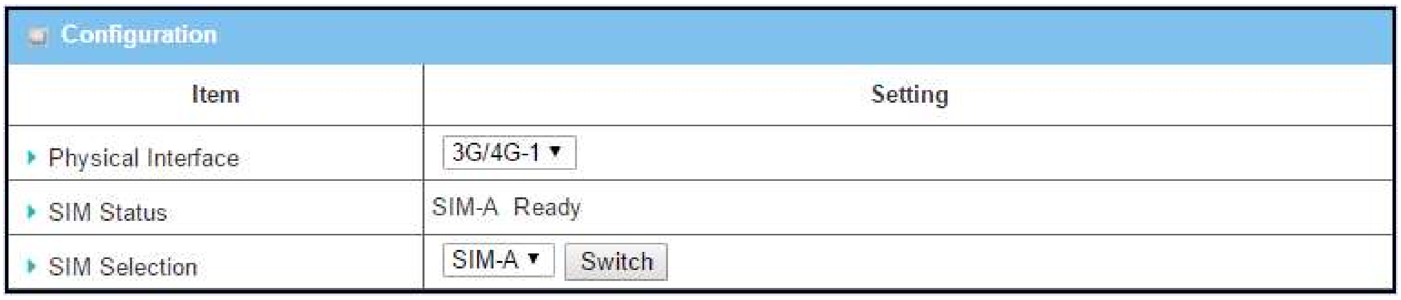
If you enter an incorrect PIN code at configuration page for 3G/4G-1 WAN over three times, then the SIM card will be locked by PUK (personal unlocking key) code. You will have to call a service number to get a PUK code to unlock the SIM card. In the diagram, the PUK code is "**12345678**" and new PIN code is "**5678**".

SIM PIN Setting

Go to **Service** > **Cellular Toolkit** > **SIM PIN** Tab

With the SIM PIN Function window, it allows you to enable or disable SIM lock (which means protected by PIN code), or change the PIN code. You can also see the information for remaining times of failure trials as mentioned earlier. If you run out of these failure trials, you will need to get a PUK code to unlock SIM card.

Select a SIM Card



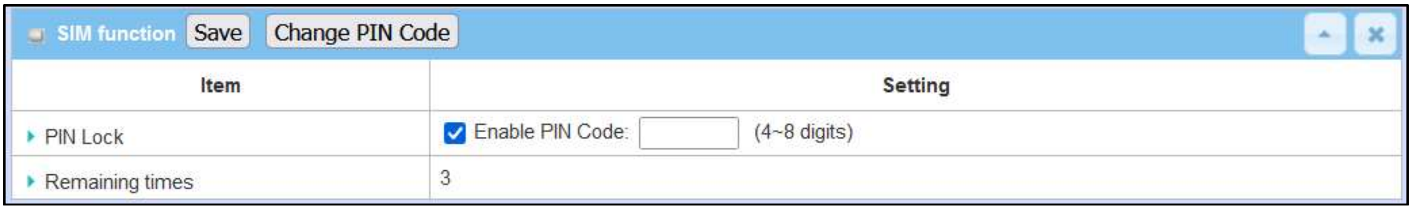
Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾
SIM Status	SIM-A Ready
SIM Selection	SIM-A ▾ Switch

Configuration Window		
Item	**Value setting**	**Description**
Physical Interface	The box is **3G/4G-1** by default	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) to change the SIM PIN setting for the selected SIM Card. **Note: 3G/4G-2** is only available for products with dual cellular modules.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status: **Ready**, **Not Insert**, or **SIM PIN**. **Ready** -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code. **Not Insert** -- No SIM card is inserted in that SIM slot. **SIM PIN** -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. SIM card is still in locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the **Switch** button, then the Gateway will switch SIM card to the other one. After that, you can configure the SIM card.

Enable / Change PIN Code

Enable or Disable PIN code (password) function, and even change PIN code function.

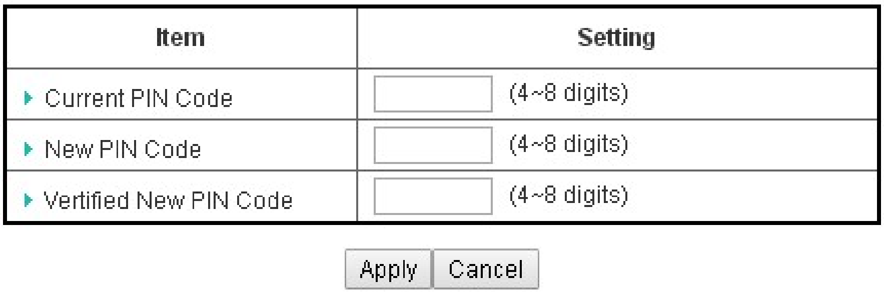


SIM function Save Change PIN Code

Item	Setting
PIN Lock	☑ Enable PIN Code: ▭ (4~8 digits)
Remaining times	3

SIM function Window		
Item Setting	**Value setting**	**Description**
PIN lock	Depends on SIM card	Click the **Enable** button to activate the SIM lock function. For the first time you want to enable the SIM lock function, fill in the PIN code as well, and then click the **Save** button to apply the setting.
Remaining times	Depends on SIM card	Represents the remaining trial times for the SIM PIN unlocking.
Save	N/A	Click the **Save** button to apply the setting.
Change PIN Code	N/A	Click the **Change PIN code** button to change the PIN code (password). If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. If you still want to change the PIN code, enable the SIM Lock function first, fill in the PIN code, and then click the **Save** button to enable. After that, you can click the **Change PIN code** button to change the PIN code.

When **Change PIN Code** button is clicked, the following screen will appear.



Item	Setting
Current PIN Code	▭ (4~8 digits)
New PIN Code	▭ (4~8 digits)
Vertified New PIN Code	▭ (4~8 digits)

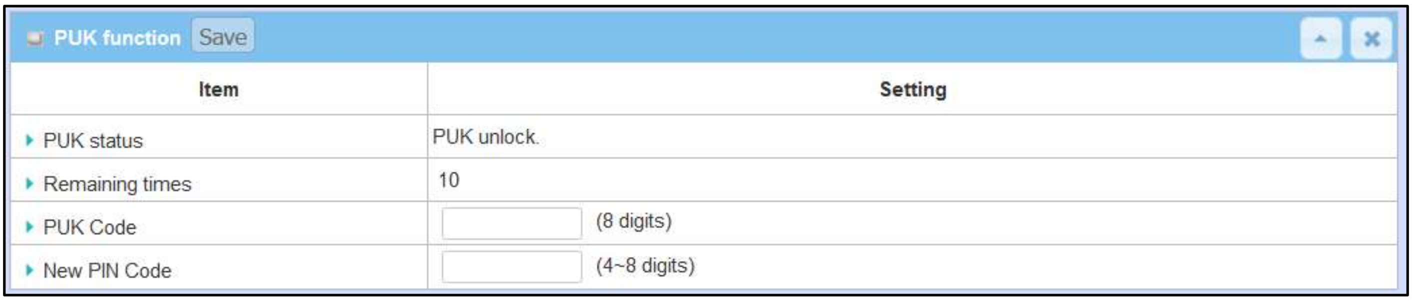
Apply Cancel

Item	Value Setting	Description
Current PIN Code	Required setting	Enter the current (old) PIN code of the SIM card.
New PIN Code	Required setting	Enter the new PIN Code.
Verified New PIN Code	Required setting	Confirm the new PIN Code again.
Apply	N/A	Click the **Apply** button to change the PIN code with specified new PIN code.
Cancel	N/A	Click the **Cancel** button to cancel the changes and keep current PIN code.

Note: If you changed the PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with the invalid (old) PIN code.

Unlock with a PUK Code

The PUK Function window is only available for configuration if that SIM card is locked by PUK code. Usually this happens after too many trials using an incorrect PIN code, and the remaining times in the SIM Function table turns to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and unlock the locked SIM card with the provided PUK code. After unlocking a SIM card by PUK code successfully, the SIM lock function will be activated automatically.



Item	Setting
PUK status	PUK unlock.
Remaining times	10
PUK Code	(8 digits)
New PIN Code	(4~8 digits)

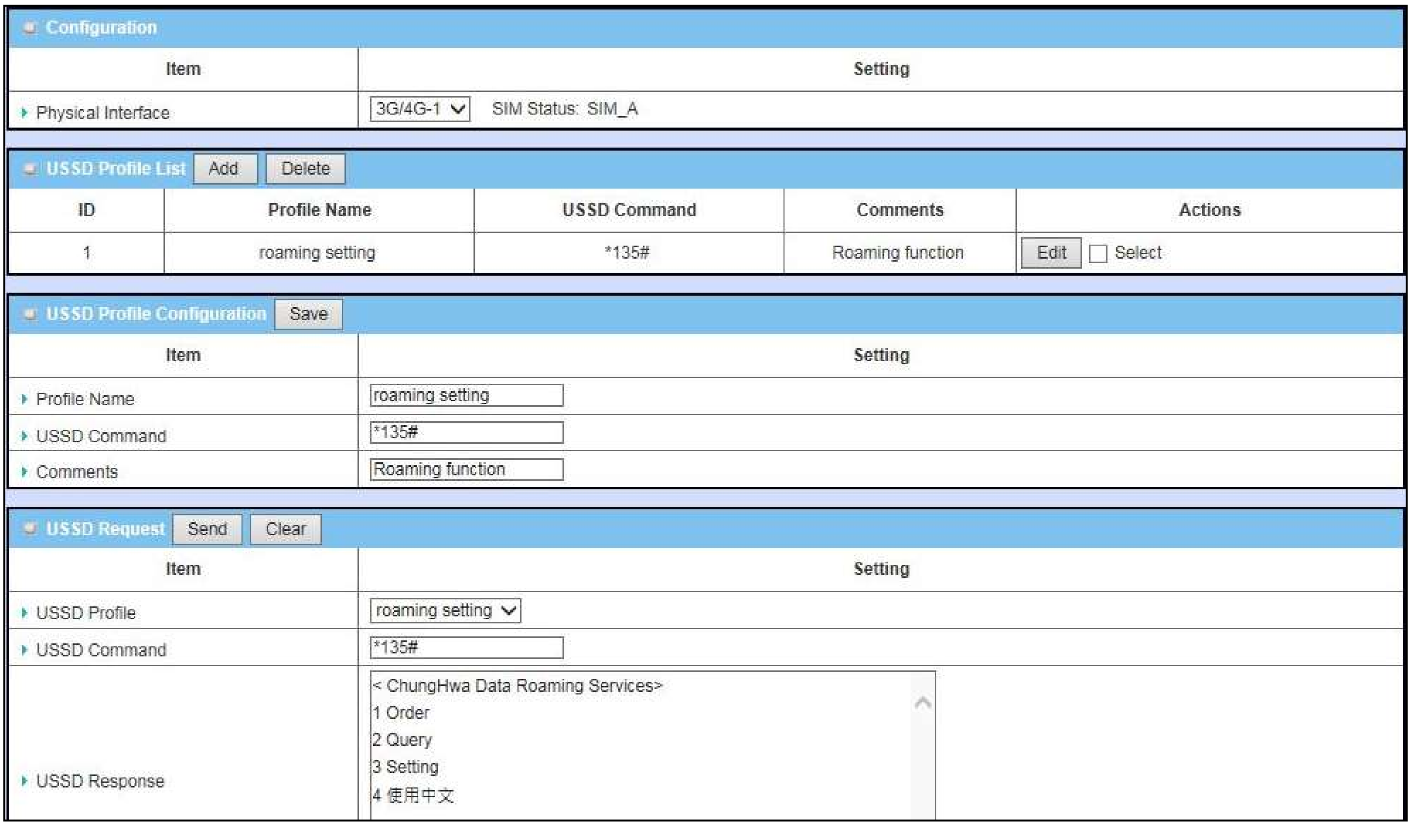
PUK Function Window		
Item	**Value setting**	**Description**
PUK status	**PUK Unlock** **/ PUK Lock**	Indication for the PUK status: **PUK Lock** or **PUK Unlock**. As mentioned earlier, the SIM card will be locked by PUK code after too many access attempts with an incorrect PIN code. In this case, the PUK Status will turns to **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	The remaining trial times for the PUK unlocking. Note: **DO NOT allow the remaining times to reach zero, it will damage the SIM card FOREVER !** Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	Required setting	Enter the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	Required setting	Enter the New PIN Code (4~8 digits) for the SIM card. You will have to ascertain your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	N/A	Click the **Save** button to apply the setting.

Note: If you changed the PUK code and PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with the invalid (old) PIN code.

8.1.4 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network.

An USSD message is up to 182 alphanumeric characters in length. Unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during an USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS.



Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A

USSD Profile List [Add] [Delete]

ID	Profile Name	USSD Command	Comments	Actions
1	roaming setting	*135#	Roaming function	[Edit] □ Select

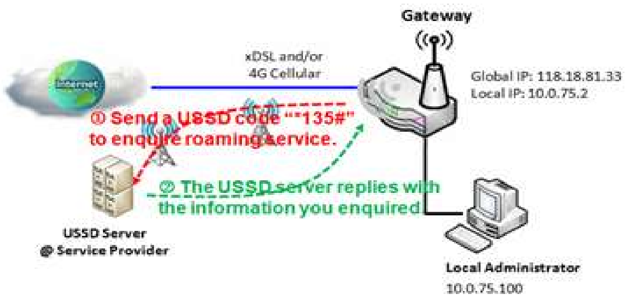
USSD Profile Configuration [Save]

Item	Setting
Profile Name	roaming setting
USSD Command	*135#
Comments	Roaming function

USSD Request [Send] [Clear]

Item	Setting
USSD Profile	roaming setting ▾
USSD Command	*135#
USSD Response	< ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文

USSD Scenario



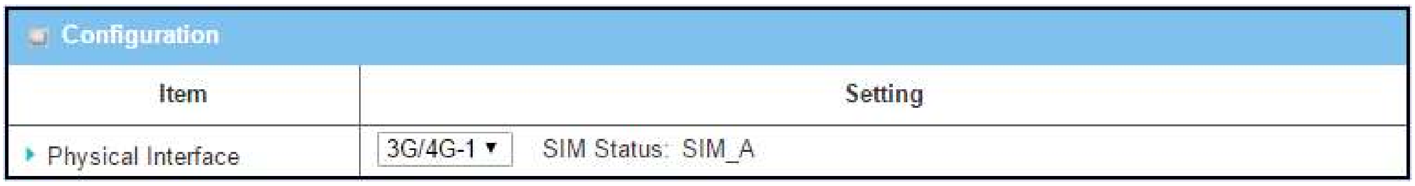
USSD allows you to have an instant bi-directional communication with the carrier/ISP. In the diagram, the USSD command '***135#**' refers to data roaming services. After sending that USSD command to carrier, you can get a response at window USSD Response. Please note the USSD command varies for different carriers/ISPs.

USSD Setting

Go to **Service** > **Cellular Toolkit** > **USSD** tab.

In the "USSD" page, there are four windows for the USSD function. The "Configuration" window lets you specify which 3G/4G module (physical interface) is used USSD, and the system will show which SIM card in the module is the current one. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that store pre-commands for activating a USSD session. An "Add" button in the window lets you add one new USSD profile and define the commands for the profile in the third window, "USSD Profile Configuration". When you want to start the activation of an USSD connection session to the USSD server, select the USSD profile or type in the correct pre-command, and then click on the "Send" button for the session. The responses from the USSD server will be displayed beneath the "USSD Command" line. When commands typed in the "USSD Command" field are sent, received responses will be displayed in the "USSD Response" blank space. User can communicate with the USSD server by sending USSD commands and getting USSD responses via the gateway.

USSD Configuration



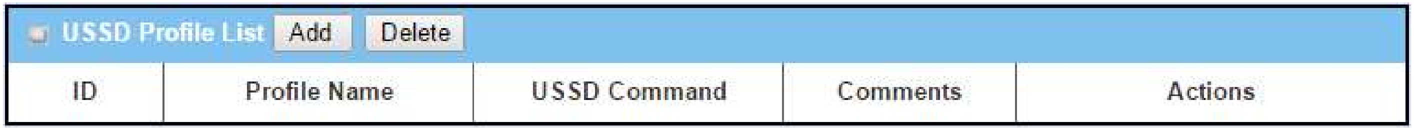
Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A

Configuration Item	Value setting	Description
Physical Interface	**3G/4G-1** is default.	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) to configure the USSD setting for the connected cellular service (identified with **SIM_A** or **SIM_B**). **Note: 3G/4G-2** is only available for products with dual cellular modules.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).

Create / Edit USSD Profile

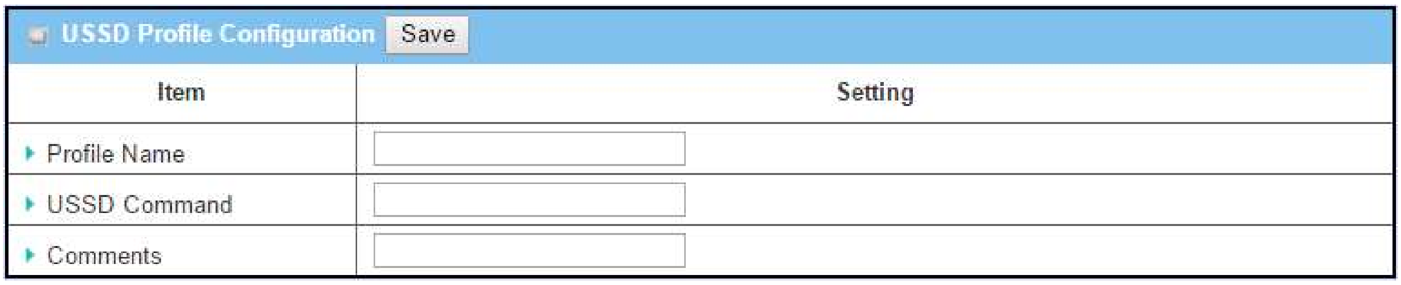
The cellular gateway allows you to customize your USSD profile. It supports up to a maximum of 35 USSD profiles.



USSD Profile List Add Delete

ID	Profile Name	USSD Command	Comments	Actions

When the **Add** button is applied, the **USSD Profile Configuration** screen will appear.

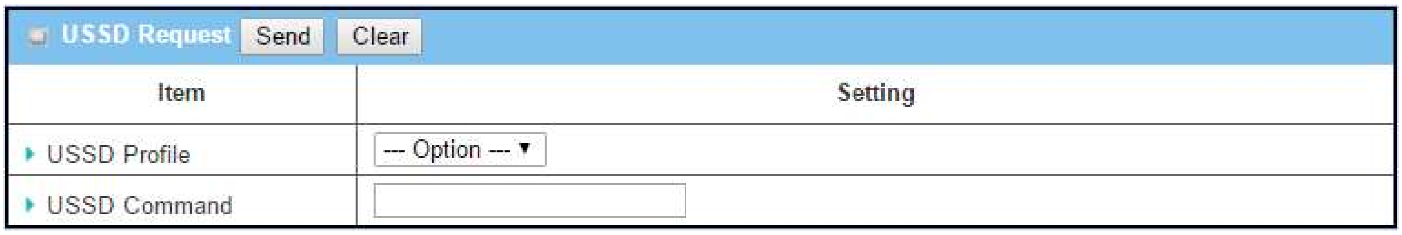


Item	Setting
Profile Name	
USSD Command	
Comments	

USSD Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	N/A	Enter a name for the USSD profile.
USSD Command	N/A	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad "0~9", "*", and "#". The USSD commands are highly related to the cellular service, please check with your service provider for details.
Comments	N/A	Enter a brief comment for the profile.

Send USSD Request

When you **send** the USSD command, the USSD Response screen will appear.
When click the **Clear** button, the USSD Response will disappear.



Item	Setting
USSD Profile	--- Option --- ▾
USSD Command	

USSD Request		
Item	**Value setting**	**Description**
USSD Profile	N/A	Select a USSD profile name from the dropdown list.
USSD Command	N/A	The USSD Command string of the selected profile will be shown here.
USSD Response	N/A	Click the **Send** button to send the USSD command, and the **USSD Response** screen will appear. You will see the response message of the corresponding service, receive the service SMS.

8.1.5 Network Scan

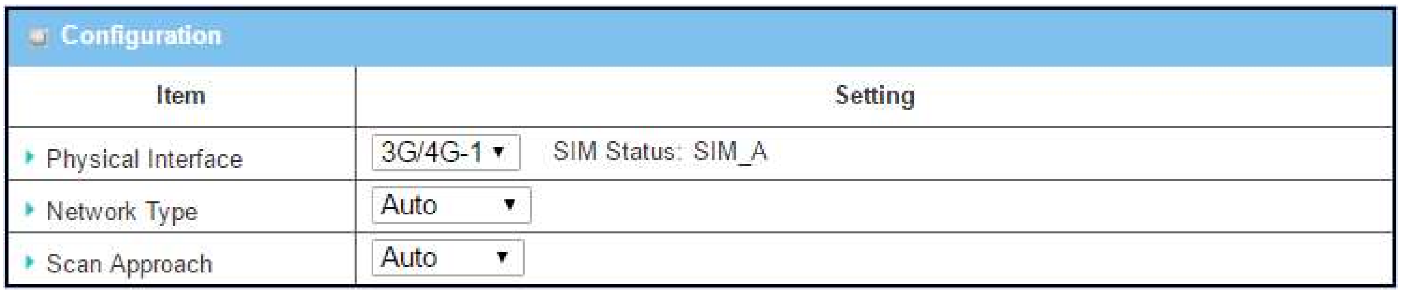
"Network Scan" function lets the administrator specify how the device will connect to the mobile system for data communication for each 3G/4G interface. For example, the administrator can specify which generation of mobile system is used for connection, 2G, 3G or LTE. Moreover, he/she can define their connection sequence for connecting to mobile systems. The administrator can also scan the mobile systems available manually, then select the target operator system and apply it. The manual scanning approach is used for problem diagnosis.

Network Scan Setting

Go to **Service** > **Cellular Toolkit** > **Network Scan** tab.

In the "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window lets you select which 3G/4G module (physical interface) is used to perform Network Scan, and the system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface by executing the network scan one after another. You can also specify the connection sequence of the targeted generation of mobile system, 2G/3G/LTE.

Network Scan Configuration

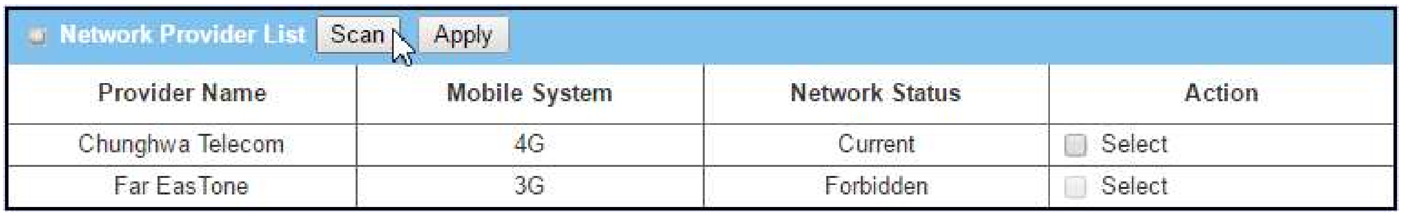


Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Network Type	Auto ▾
Scan Approach	Auto ▾

Configuration Item	Value setting	Description
Physical Interface	The box is **3G/4G-1** by default	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**) for the network scan function. **Note: 3G/4G-2** is only available for products with dual cellular modules.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	**Auto** is selected by default.	Specify the network type for the network scan function. It can be Auto, 2G Only, 2G prefer, 3G Only, 3G prefer, or LTE Only. When **Auto** is selected, the network will be registered automatically; If the **prefer** option is selected, network will be registered for your option first; If the **only** option is selected, network will be registered for your option only.
Scan Approach	**Auto** is selected by default.	When **Auto** selected, the cellular module registers automatically. If the **Manually** option is selected, a **Network Provider List** screen appears. Press **Scan** button to scan for the nearest base stations. Select (check the box) the preferred base stations then click **Apply** button to apply settings.
Save	N/A	Click **Save** to save the settings

The second window is the "Network Provider List" window, and it appears when the **Manually** Scan Approach is selected in the Configuration window. By clicking on the "Scan" button and waiting for 1 to 3 minutes, the found mobile operator systems will be displayed for you to choose from. Click again on the "Apply" button to have the system connect to that mobile operator system for the dedicated 3G/4G interface.



Provider Name	Mobile System	Network Status	Action
Chunghwa Telecom	4G	Current	□ Select
Far EasTone	3G	Forbidden	□ Select

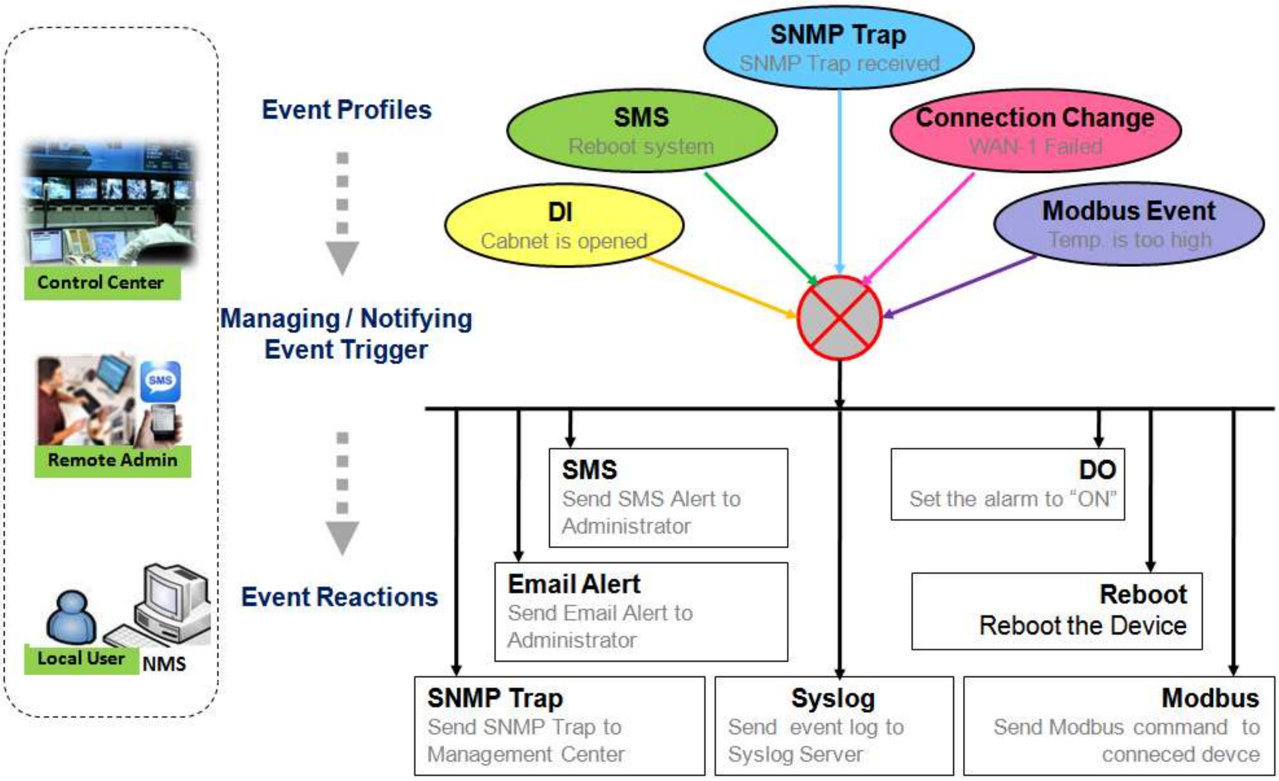
8.2 SMS & Event Handling

SMS & Event handling is the application that allows the administrator to setup pre-defined events, handlers, or response behavior with individual profiles. With proper configuration, the administrator can easily and remotely obtain the status and information via the gateway. Moreover, he/she can also handle and manage some important system related functions, even connected field bus devices and D/O devices.

The supported events are categorized into two groups: **managing events** and **notifying events**.

M**anaging events** are events that are used to manage the gateway or change the setting / status of the specific functionality of the gateway. On receiving a managing event, the gateway will take action to change the functionality, collect the required status for administration, and also change the status of a connected field bus device.

N**otifying events** are events in which some related objects have been triggered and corresponding actions are taken. It could be an event generated from the connected sensor, or a certain connected field bus device. Alerts can be sent by SMS message, Email, and SNMP Trap.



For ease of configuration, the administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant action on a certain event or managing the devices for advanced purposes. For example, sending/receiving remote managing SMS for the gateway's routine maintenance, field bus device status monitoring, digital sensor detection controlling, and so on. All such management and notification functions can be realized effectively via the Event Handling feature.

The following is the summary list for the provided profiles, and events:

(**Note**: The available profiles and events will vary depending on product model.)

- Profiles (Rules):
  - SMS Configuration and Accounts
  - Email Accounts
  - Digital Input (DI) profiles
  - Digital Output (DO) profiles
  - Modbus Managing Event profiles
  - Modbus Notifying Event profiles

- Managing Events:
  - Trigger Type: SMS, SNMP Trap, and Digital Input (DI).
  - Actions: Get the Network Status; or Configure the LAN/VLAN behavior, Wi-Fi behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, Digital Output behavior, and connected Modbus devices.

- Notifying Events:
  - Trigger Type: Digital Input, Power Change, Connection Change (WAN, LAN & VLAN, Wi-Fi, DDNS), Administration, Modbus, and Data Usage.
  - Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert; Change the status of connected Digital Output or Modbus devices.

To use the event handling function, enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items; they are the SMS Account Definition, Email Service Definition, Digital Input (DI) Profile Configuration, Digital Output (DO) Profile Configuration, and Modbus Definition.

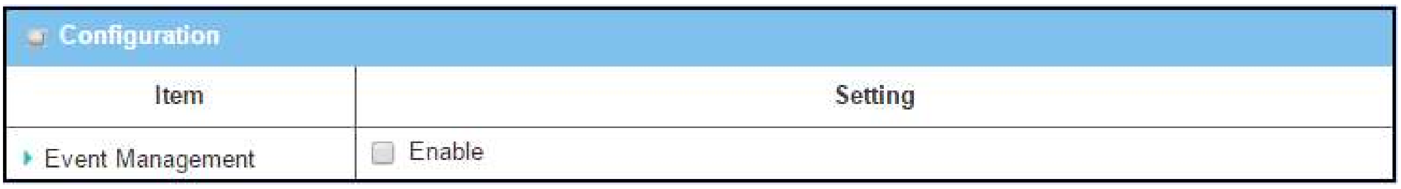
Then, configure each managing / notifying event by setting the event's trigger condition, and the corresponding actions for the event. For each event, multiple actions can be activated simultaneously.

8.2.1 Configuration

Go to **Service** > **Event Handling** > **Configuration** Tab.

Event handling is the service that allows administrator to set up pre-defined events, handlers, or response behavior with individual profiles.

Enable Event Management



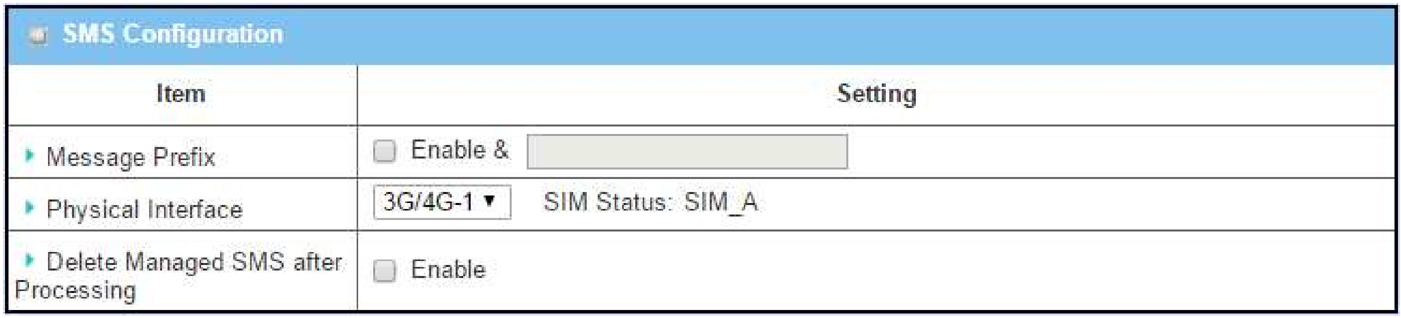
Configuration

Item	Setting
Event Management	□ Enable

Configuration Item	Value setting	Description
Event Management	Unchecked by default	Check the **Enable** box to activate the Event Management function.

Enable SMS Management

To use the SMS management function, configure these settings first.



SMS Configuration

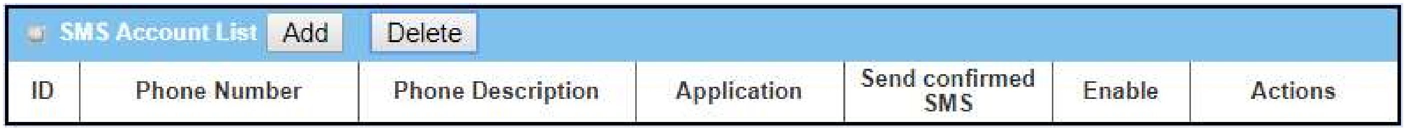
Item	Setting
Message Prefix	□ Enable &
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Delete Managed SMS after Processing	□ Enable

SMS Configuration Item	Value setting	Description
Message Prefix	Unchecked by default	Click the **Enable** box to enable the SMS prefix for validating the received SMS. Once the function is enabled, enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.

Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**). **Note: 3G/4G-2** is only available for products with dual cellular modules.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	Unchecked by default	Check the **Enable** box to delete the received managing event SMS after it has been processed.

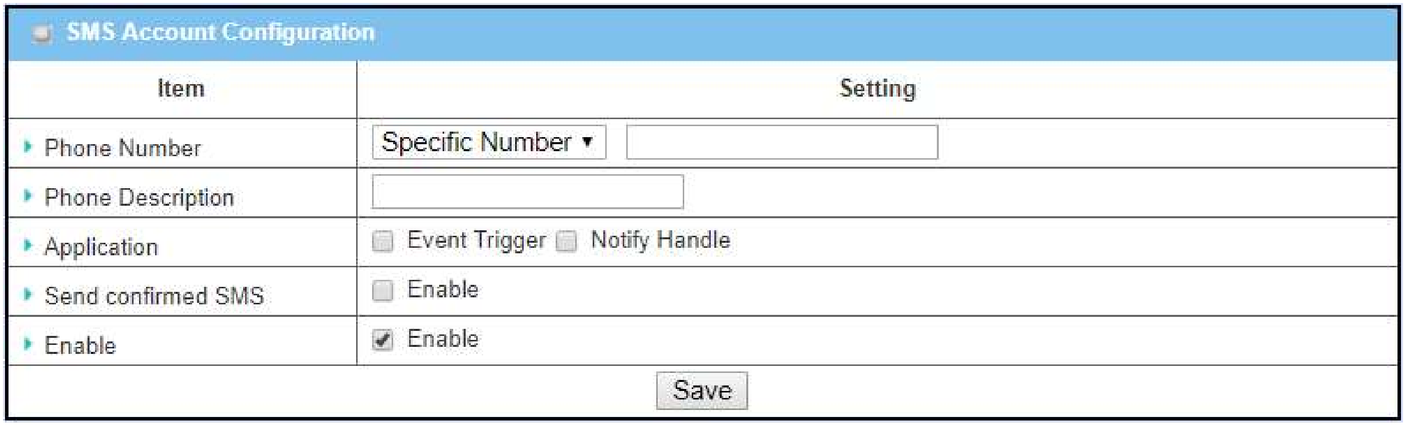
Create / Edit SMS Account

Set up the SMS Account for managing the gateway through SMS. It supports up to a maximum of 5 accounts.



ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.

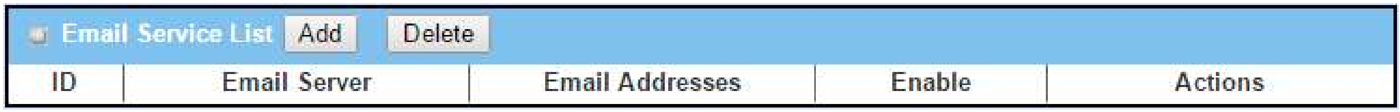


Item	Setting
Phone Number	Specific Number ▾
Phone Description	
Application	□ Event Trigger □ Notify Handle
Send confirmed SMS	□ Enable
Enable	☑ Enable

SMS Account Configuration		
Item	**Value setting**	**Description**
Phone Number	1. Mobile phone number format 2. Required setting	Select the Phone number policy from the dropdown list, and specify a mobile phone number as the SMS account identifier if required. It can be **Specific Number**, or **Allow Any**. If **Specific Number** is selected, specify the phone number as the SMS account identifier. ***Value Range***: -1 ~ 32 digits.
Phone Description	1. Any text 2. Optional setting	Specify a brief description for the SMS account.
Application	Required setting	Specify the application type. It could be **Event Trigger, Notify Handle,** or **both**. If the Phone Number policy is **Allow Any**, the Notify Handle will be unavailable.
Send confirmed SMS	1. Optional setting 2. Unchecked by default	Click the **Enable** box to activate the SMS response function. The gateway will send a confirmed message back to the sender whenever it receives a SMS managing event. The confirmed message is similar to following format: *"Device received a SMS with command xxxxx."*
Enable	Unchecked by default	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration.

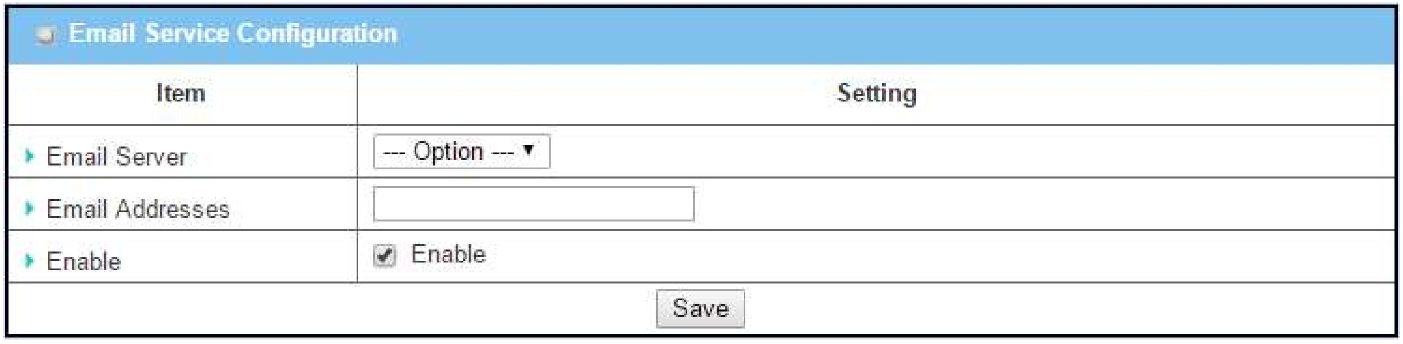
Create / Edit Email Service Account

Set up the Email Service Account for event notification. It supports up to a maximum of 5 accounts.



ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.

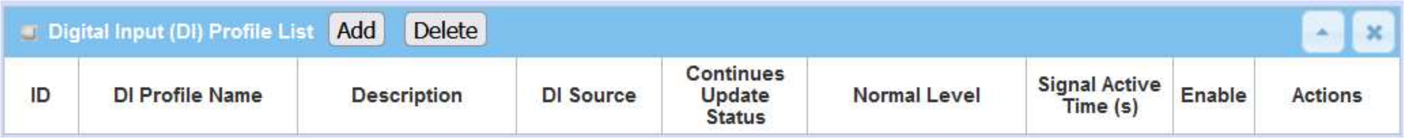


Item	Setting
Email Server	--- Option --- ▼
Email Addresses	
Enable	☑ Enable

Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. Required setting	Specify the Destination Email Addresses.
Enable	Unchecked by default	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

Create / Edit Digital Input (DI) Profile Rule (DI/DO support required)

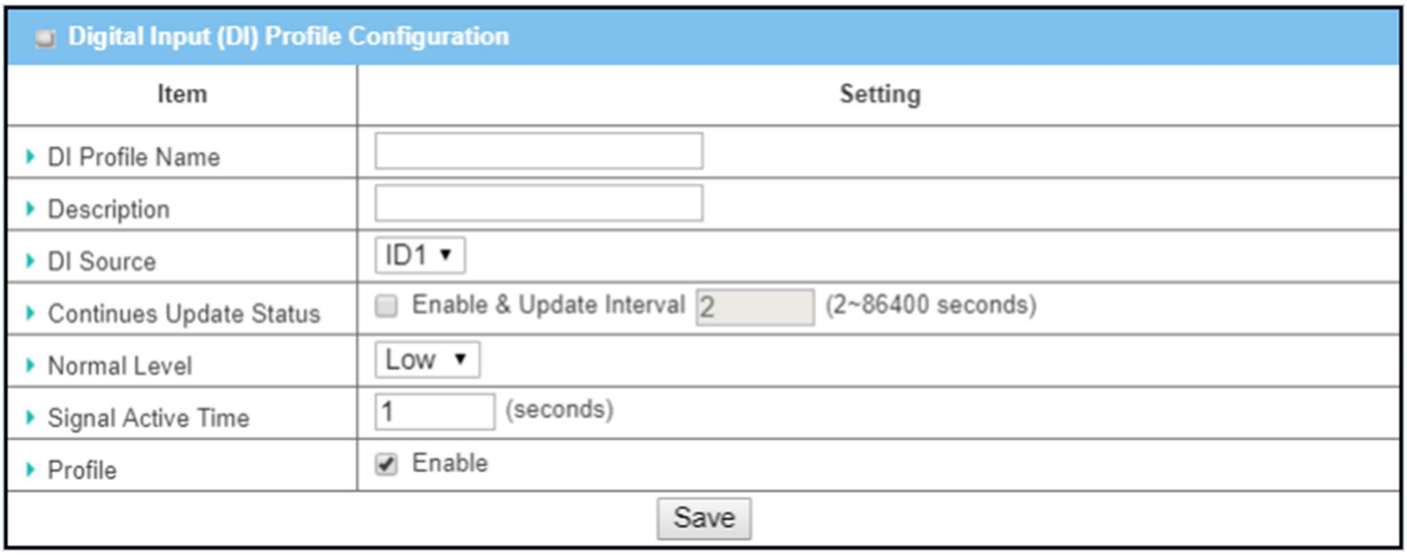
Set up the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.



Digital Input (DI) Profile List Add Delete

ID	DI Profile Name	Description	DI Source	Continues Update Status	Normal Level	Signal Active Time (s)	Enable	Actions

When the **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen will appear.



Digital Input (DI) Profile Configuration

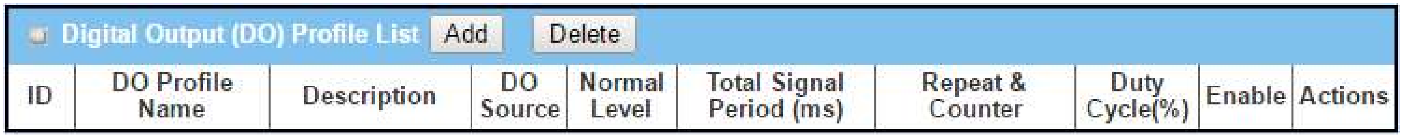
Item	Setting
DI Profile Name	
Description	
DI Source	ID1 ▾
Continues Update Status	□ Enable & Update Interval 2 (2~86400 seconds)
Normal Level	Low ▾
Signal Active Time	1 (seconds)
Profile	☑ Enable

Save

Digital Input (DI) Profile Configuration		
Item	**Value setting**	**Description**
DI Profile Name	1. String format 2. Required setting	Specify the DI Profile Name. ***Value Range***: -1 ~ 32 characters.
Description	1. Any text 2. Optional setting	Specify a brief description for the profile.
DI Source	**ID1** by default	Specify the DI Source. It could be **ID1** or **ID2**. The number of available DI sources will depend on the product model.
Continue Update Status	Unchecked by default	Click **Enable** box to activate this function for the DI event with designated update interval setting. If the event condition keeps active for a long time interval, the gateway will send repeated notify events for each check interval. **Value Range:** 2 ~ 86400 seconds. **Note:** To prevent receiving too much notify event for the same situation, you can adjust the check interval to a proper one for your application.
Normal Level	Low by default	Specify the Normal Level: **Low** or **High**.
Signal Active Time	1. Numeric String format 2. Required setting	Specify the Signal Active Time. ***Value Range***: 1 ~ 10 seconds.
Profile	Unchecked by default	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

Create / Edit Digital Output (DO) Profile Rule (DI/DO support required)

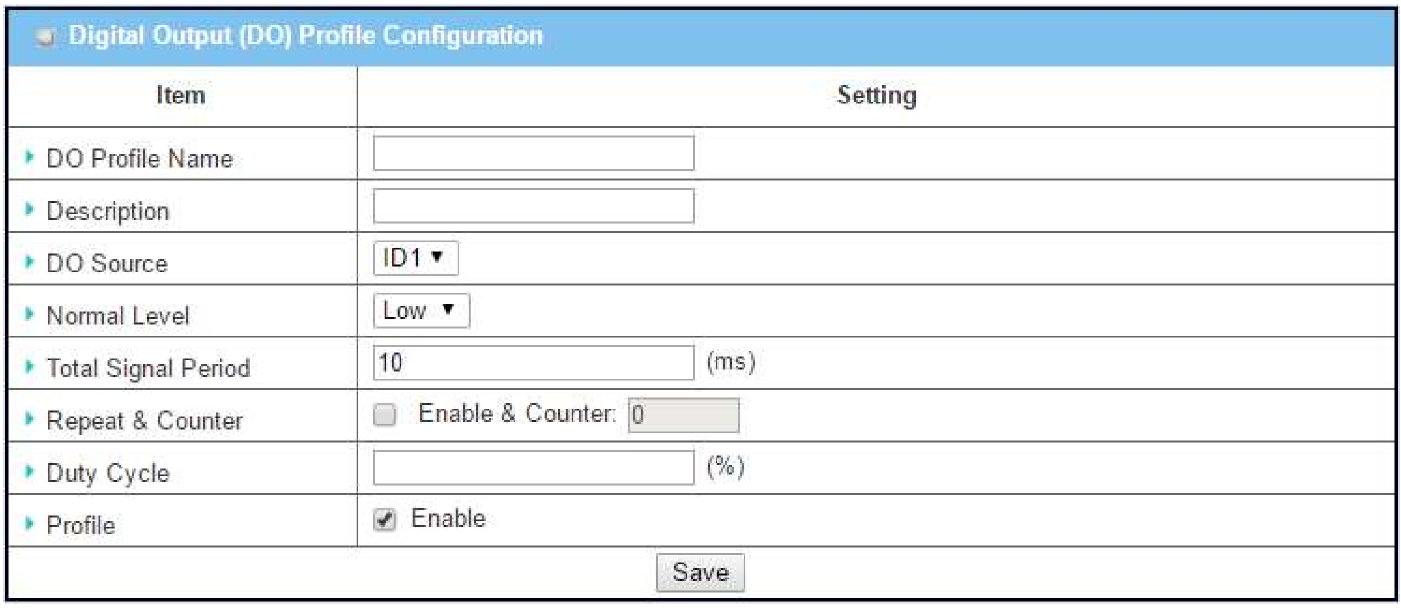
Set up the Digital Output (DO) Profile rules. It supports up to a maximum of 10 profiles.



Digital Output (DO) Profile List Add Delete

ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen will appear.



Digital Output (DO) Profile Configuration

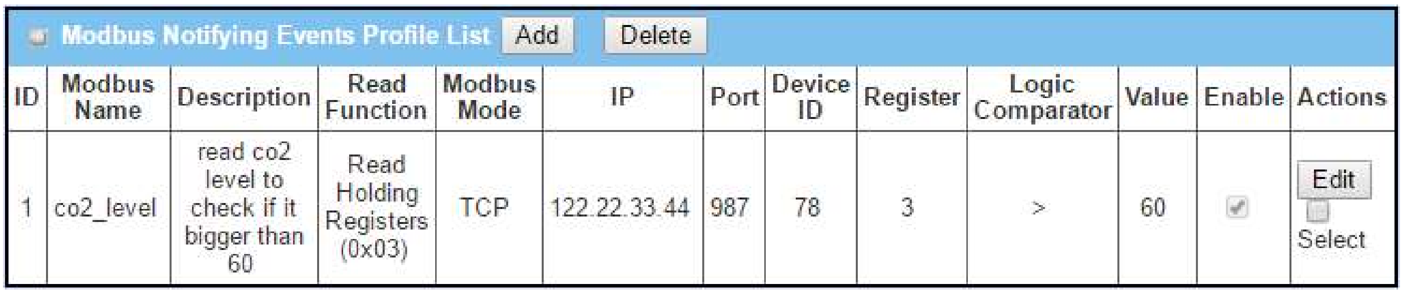
Item	Setting
DO Profile Name	
Description	
DO Source	ID1 ▾
Normal Level	Low ▾
Total Signal Period	10 (ms)
Repeat & Counter	□ Enable & Counter: 0
Duty Cycle	(%)
Profile	☑ Enable

Save

Digital Output (DO) Profile Configuration		
Item	**Value setting**	**Description**
DO Profile Name	1. String format 2. Required setting	Specify the DO Profile Name. ***Value Range***: -1 ~ 32 characters.
Description	1. Any text 2. Optional setting	Specify a brief description for the profile.
DO Source	**ID1** by default	Specify the DO Source.
Normal Level	Low by default	Specify the Normal Level: **Low** or **High**.
Total Signal Period	1. Numeric String format 2. Required setting	Specify the Total Signal Period. ***Value Range***: 10 ~ 120000 ms
Repeat & Counter	Unchecked by default	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. ***Value Range***: 0 ~ 65535
Duty Cycle	1. Numeric String format 2. Required setting	Specify the Duty Cycle for the Digital Output. ***Value Range***: 1 ~100 %
Profile	Unchecked by default	Click **Enable** box to activate this profile setting.
Save	N/A	Click the **Save** button to save the configuration.

Create / Edit Modbus Notifying Events Profile (Modbus support required)

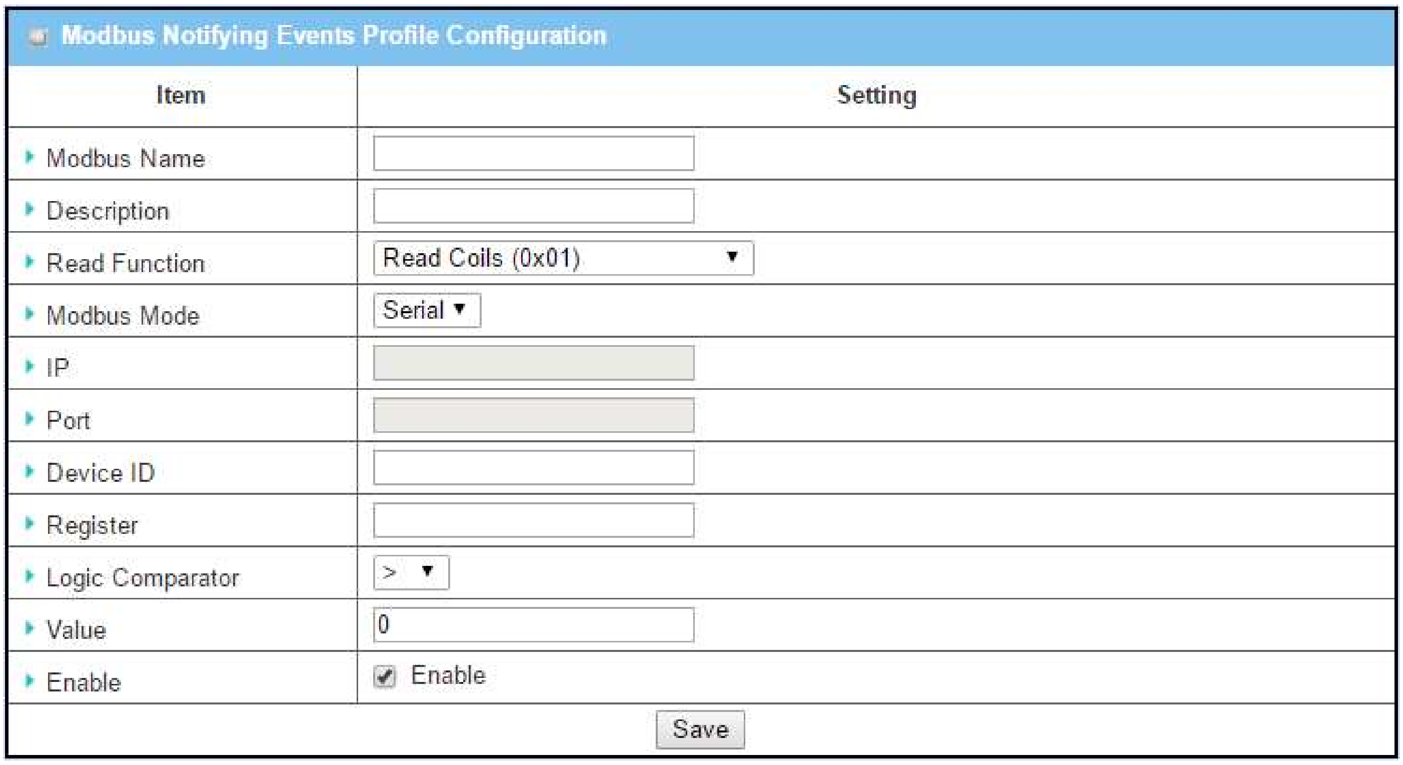
Set up the Modbus Notifying Events Profile. It supports up to a maximum of 10 profiles.



Modbus Notifying Events Profile List [Add] [Delete]

ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions
1	co2_level	read co2 level to check if it bigger than 60	Read Holding Registers (0x03)	TCP	122.22.33.44	987	78	3	>	60	☑	Edit □ Select

Click the **Add / Edit** button to configure the profile.



Modbus Notifying Events Profile Configuration

Item	Setting
Modbus Name	
Description	
Read Function	Read Coils (0x01) ▾
Modbus Mode	Serial ▾
IP	
Port	
Device ID	
Register	
Logic Comparator	> ▾
Value	0
Enable	☑ Enable

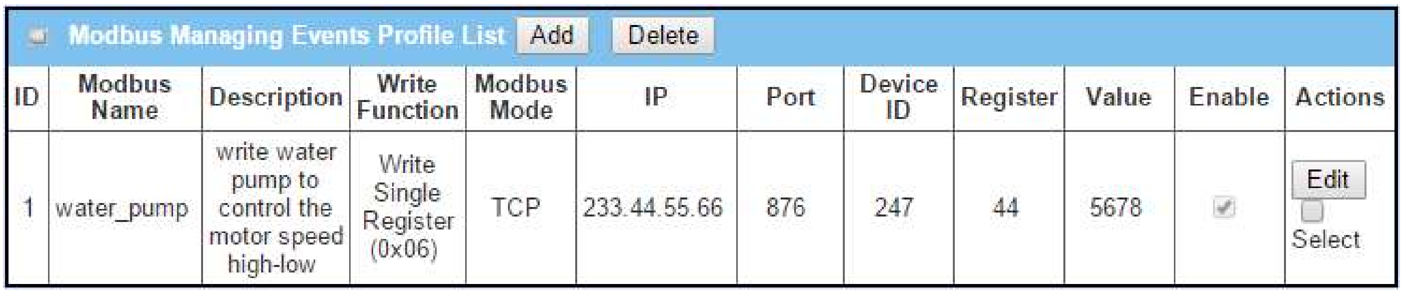
[Save]

Modbus Notifying Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. Required setting	Specify the Modbus profile name. ***Value Range***: -1 ~ 32 characters.
Description	1. Any text 2. Optional setting	Specify a brief description for the profile.
Read Function	Read Holding Registers by default	Specify the Read Function for **Notifying Events**.
Modbus	**Serial** by default	Specify the Modbus Mode: **Serial** or **TCP**.

Mode		
IP	1. NA for Serial on Modbus Mode. 2. Required setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode. 2. Required setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. ***Value Range*:** 1 ~ 65535.
Device ID	1. Numeric String format 2. Required setting	Specify the Device ID of the Modbus device. It can be from 1 to 247.
Register	1. Numeric String format 2. Required setting	Specify the Register number of the Modbus device. ***Value Range*:** 0 ~ 65535.
Logic Comparator	Logic Comparator '>' by default.	Specify the Logic Comparator for **Notifying Events**. It can be '>', '<', '=', '>=', or '<='.
Value	1. Numeric String format 2. Required setting	Specify the Value. ***Value Range*:** 0 ~ 65535.
Enable	Unchecked by default	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

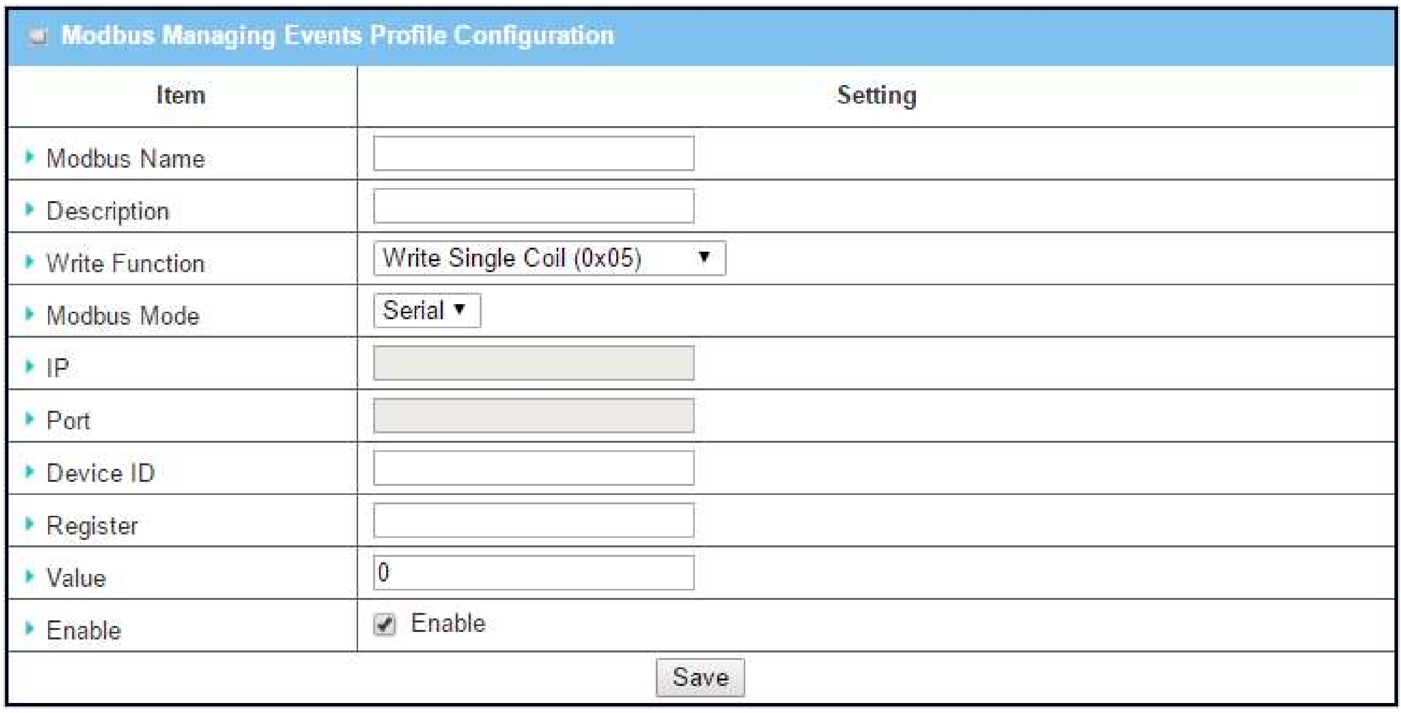
Create / Edit Modbus Managing Events Profile (Modbus support required)

Set up the Modbus Managing Events Profile. It supports up to a maximum of 10 profiles.



ID	Modbus Name	Description	Write Function	Modbus Mode	IP	Port	Device ID	Register	Value	Enable	Actions
1	water_pump	write water pump to control the motor speed high-low	Write Single Register (0x06)	TCP	233.44.55.66	876	247	44	5678	☑	Edit □ Select

You can click the **Add / Edit** button to configure the profile.



Modbus Managing Events Profile Configuration

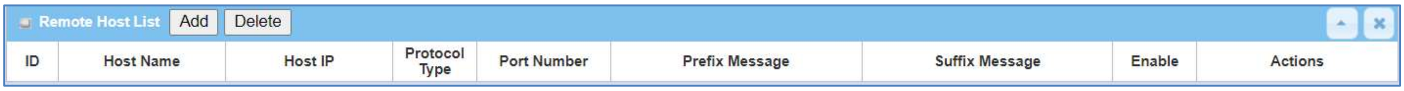
Item	Setting
Modbus Name	
Description	
Write Function	Write Single Coil (0x05) ▼
Modbus Mode	Serial ▼
IP	
Port	
Device ID	
Register	
Value	0
Enable	☑ Enable

Modbus Managing Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. Required setting	Specify the Modbus profile name. ***Value Range***: -1 ~ 32 characters.
Description	1. Any text 2. Optional setting	Specify a brief description for the profile.
Write Function	Write Single Registers by default	Specify the Write Function for **Managing Events**.
Modbus Mode	**Serial** by default	Specify the Modbus Mode: **Serial** or **TCP**.
IP	1. NA for Serial on Modbus	Specify the IP for TCP on Modbus Mode. IPv4 Format.

	Mode. 2. Required setting for TCP on Modbus Mode.	
Port	1. NA for Serial on Modbus Mode. 2. Required setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. ***Value Range***: 1 ~ 65535.
Device ID	1. Numeric String format 2. Required setting	Specify the Device ID of the Modbus device. ***Value Range***: 1 ~ 247.
Register	1. Numeric String format 2. Required setting	Specify the Register number of the Modbus device. ***Value Range***: 0 ~ 65535.
Value	1. Numeric String format 2. Required setting	Specify the Value. ***Value Range***: 0 ~ 65535.
Enable	Unchecked by default	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore previous settings.

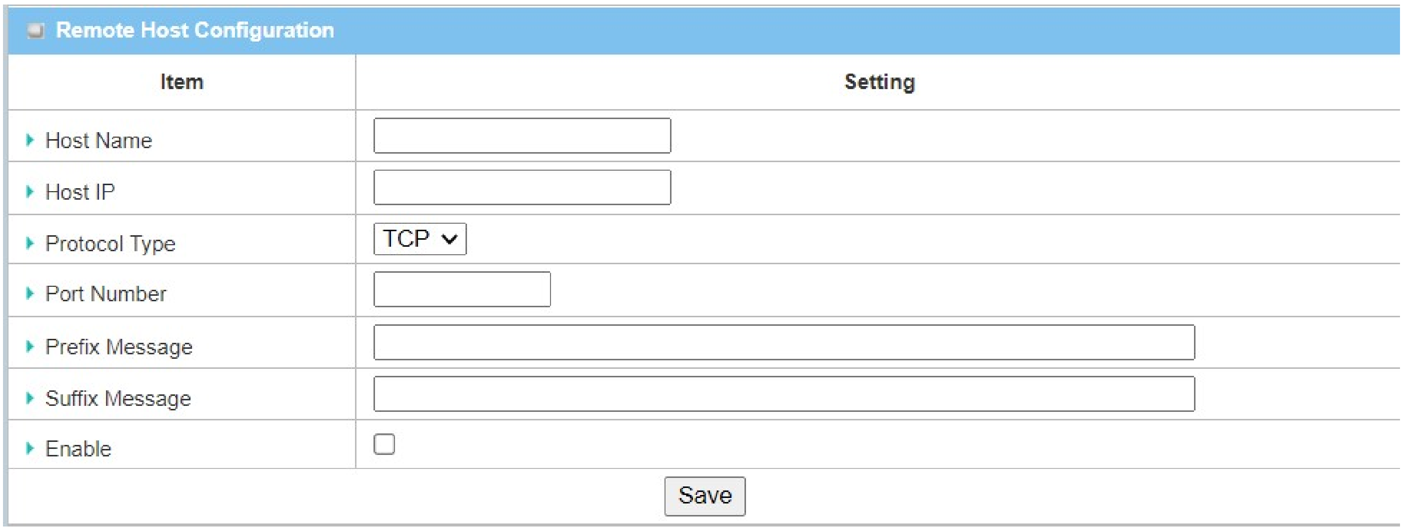
Create / Edit Remote Host List

Set up the remote hosts.



ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions

You can click the **Add / Edit** button to configure the profile.

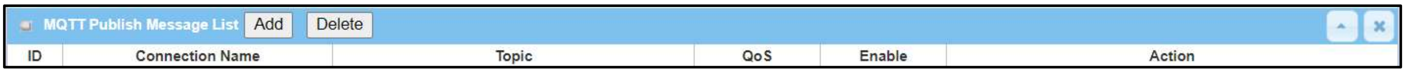


Item	Setting
Host Name	
Host IP	
Protocol Type	TCP
Port Number	
Prefix Message	
Suffix Message	
Enable	□

Remote Host Configuration Items		
Item	**Value setting**	**Description**
Host Name	1. String format 2. Required setting	Specify the remote host name. ***Value Range***: -1 ~ 32 characters.
Host IP	1. Default is blank 2. IP address format	Specify the IP address for the remote host.
Protocol Type	1. Required field 2. **TCP** is set by default	Select **TCP** or **UDP**.
Port Number	Blank by default	Enter the port number of the remote host
Prefix Message	Text field	Enter the prefix message.
Suffix Message	Text field	Enter the suffix message.
Enable	Unchecked by default	Click **Enable** box to activate this host profile.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore previous settings.

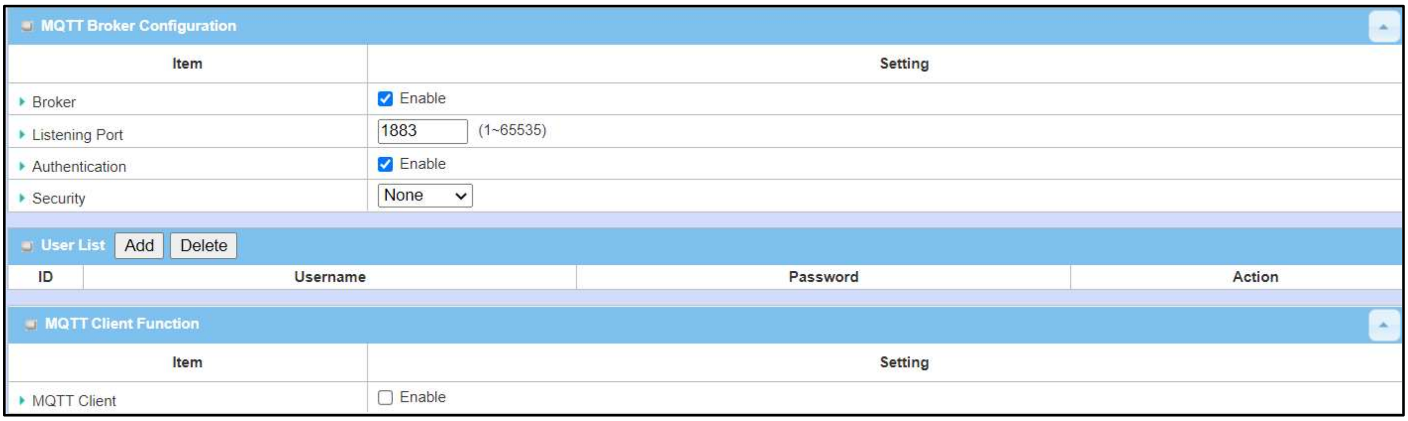
Create / MQTT Publish Message List

Set up MQTT message publishing.



ID	Connection Name	Topic	QoS	Enable	Action

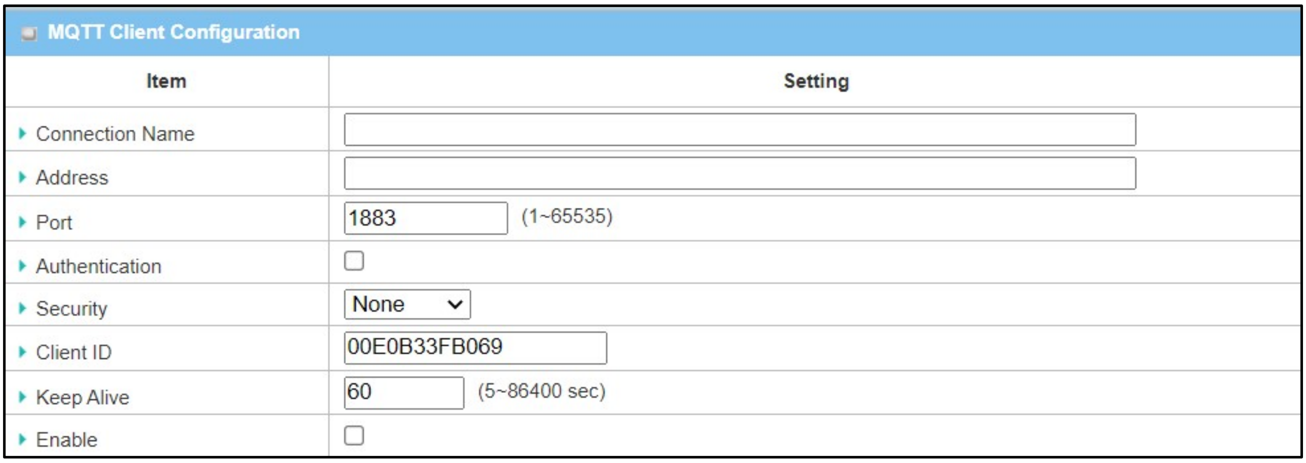
You can click the **Add / Edit** button to configure the profile.



Item	Setting
Broker	☑ Enable
Listening Port	1883 (1~65535)
Authentication	☑ Enable
Security	None

ID	Username	Password	Action

Item	Setting
MQTT Client	□ Enable



MQTT Client Configuration

Item	Setting
Connection Name	
Address	
Port	1883 (1~65535)
Authentication	□
Security	None
Client ID	00E0B33FB069
Keep Alive	60 (5~86400 sec)
Enable	□

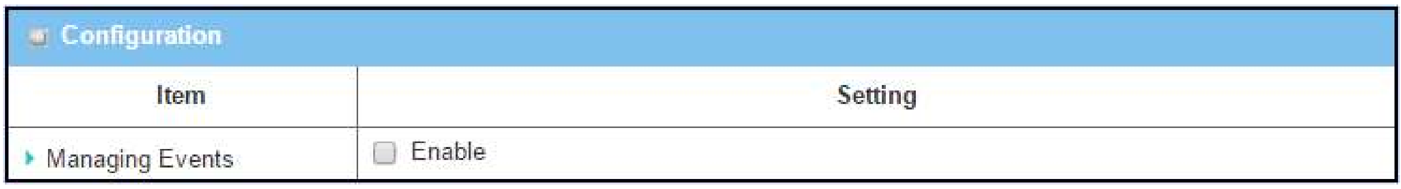
MQTT Broker Configuration		
Item	**Value setting**	**Description**
Broker	N/A	Check to enable MQTT broker.
Listening Port	Default is 1833	Enter the listening port for the MQTT broker
Authentication		Click to enable authentication.
Security		Select **None** or **SSL/TLS**.
User List		Click the Add button to add a user, then enter the username and password in the fields that appear.
MQTT Client Function	Unchecked by default.	When enabled, the MQTT client list will appear. Click the Add button to open the MQTT Client Configuration screen. Fields are the same as described in Section 4.2.

8.2.2 Managing Events

Managing Events allow the administrator to define the relationship (rule) among event triggers, handlers, and response.

Go to **Service** > **Event Handling** > **Managing Events** Tab.

Enable Managing Events



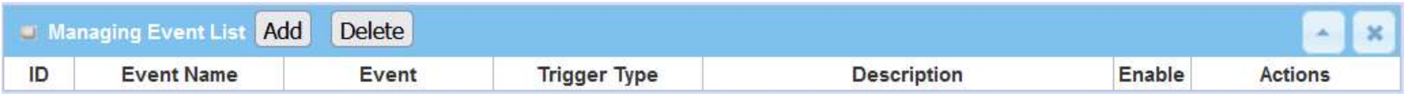
Configuration

Item	Setting
Managing Events	□ Enable

Configuration Item	Value setting	Description
Managing Events	Unchecked by default	Check the **Enable** box to activate the Managing Events function.

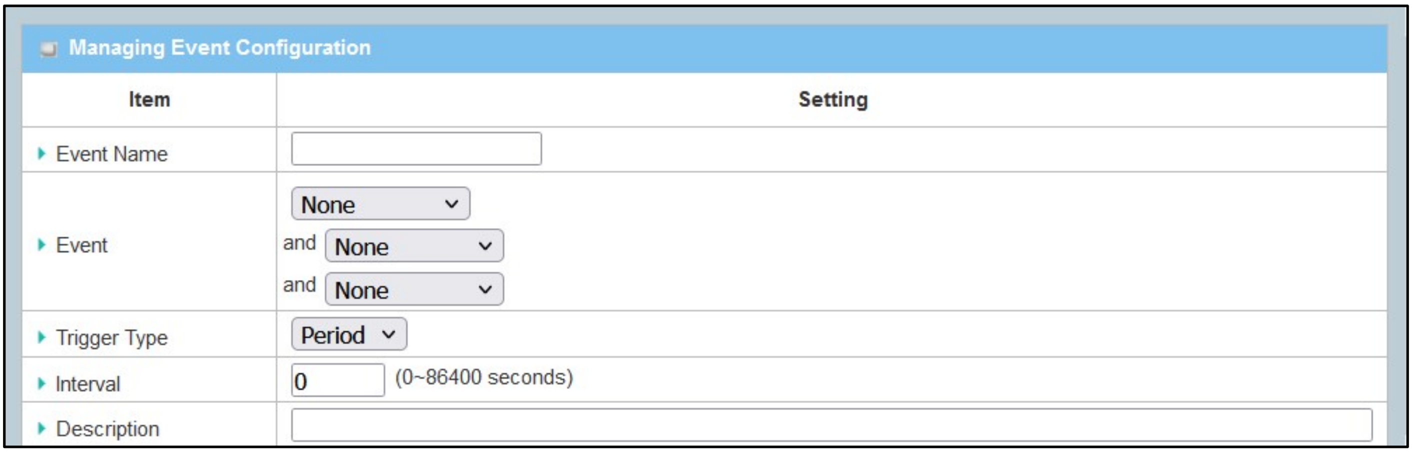
Create / Edit Managing Event Rules

Set up the Managing Event rules. It supports up to a maximum of 128 rules.



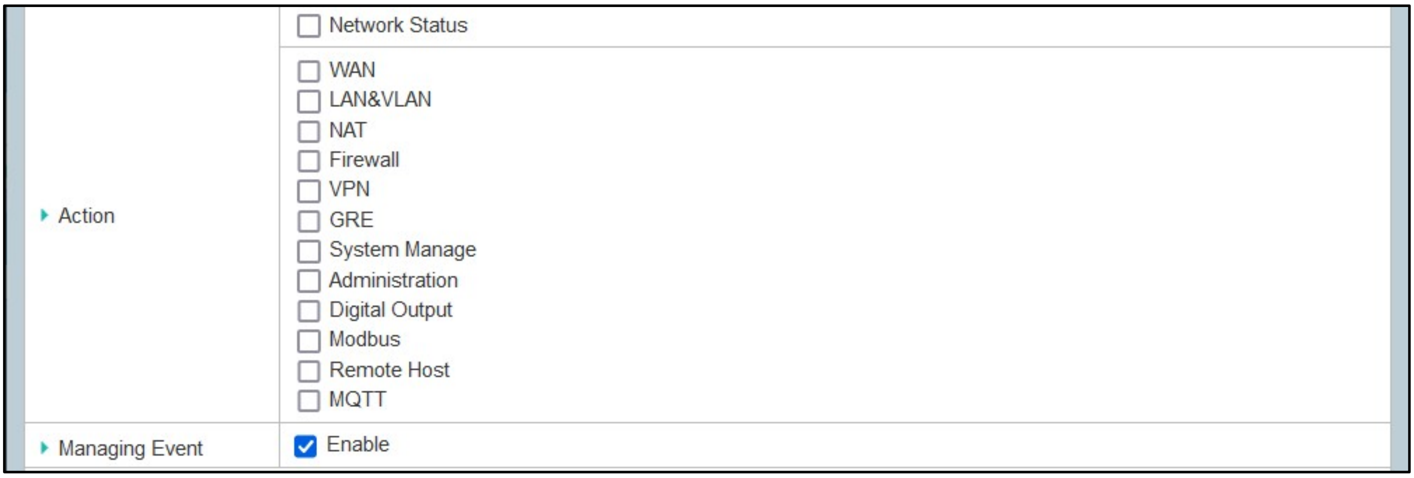
ID	Event Name	Event	Trigger Type	Description	Enable	Actions

When the **Add** or **Edit** button is applied, the **Managing Event Configuration** screen will appear.



Managing Event Configuration

Item	Setting
Event Name	
Event	None and None and None
Trigger Type	Period
Interval	0 (0~86400 seconds)
Description	



▸ Action	□ Network Status □ WAN □ LAN&VLAN □ NAT □ Firewall □ VPN □ GRE □ System Manage □ Administration □ Digital Output □ Modbus □ Remote Host □ MQTT
▸ Managing Event	☑ Enable

Managing Event Configuration		
Item	**Value setting**	**Description**
Event Name	Text field, blank by default	Specify a name for the event
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**, or **Digital Input**) and an event identifier / profile. **SMS**: Select **SMS** and enter the message in the textbox as the trigger condition for the event; **SNMP**: Select **SNMP Trap** and enter the message in the textbox to specify the SNMP Trap Event; **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event; *Note: The available Event Types will depend on product model.*
Trigger type	**Period** is selected by default	Specify the type of event trigger, either **Period** or **Once**. **Period:** Select **Period** and specify a time interval, the event will be repeatedly triggered on every time interval when the specified event condition holds. **Once:** Select **Once** and the event will be just triggered just one time when the specified event condition holds.
Interval	**0** is set by default	Specify the repeatedly event trigger time interval. ***Value Range:*** 0 ~86400 seconds.
Description	String format: any text.	Enter a brief description for the Managing Event.
Action	All boxes unchecked by default.	Specify **Network Status**, or at least one action to take when the expected event is triggered. **Network Status**: Select **Network Status** Checkbox to get the network status as the action for the event; network connection – SIM-A or SIM-B. **WAN: Specified Cellular WAN behavior - Connect/Disconnect, SIM switch, Auto/LTE/3G** **LAN&VLAN**: Select **LAN&VLAN** Checkbox and the relevant sub-items (Port link On/Off), and the gateway will change the settings as the action for the event; **NAT**: Select **NAT** Checkbox and the relevant sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will change the settings as the action for the event; **Firewall**: Select **Firewall** Checkbox and the relevant sub-items (Remote Administrator Host ID On/Off), the gateway will change the settings as the action for the event; **VPN**: Select **VPN** Checkbox and the relevant sub-items (IPsec Tunnel ON/Off,

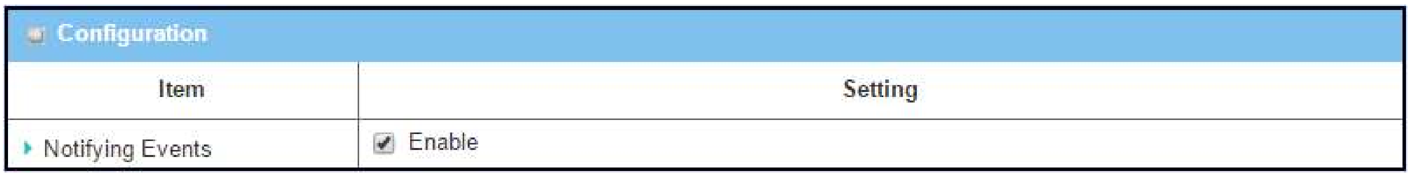
		PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will change the settings as the action for the event; **GRE**: Select **GRE** Checkbox and the relevant sub-items (GRE Tunnel On/Off), the gateway will change the settings as the action for the event; **System Manage**: Select **System Manage** Checkbox and the relevant sub-items (WAN SSH Service On/Off), the gateway will change the settings as the action for the event; **Administration**: Select **Administration** Checkbox and the relevant sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the gateway will change the settings as the action for the event; **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **Modbus**: Select **Modbus** checkbox and a Modbus Managing Event profile you defined as the action for the event; **Remote Host:** Select **Remote Host** checkbox and a Remote Host profile you defined as the action for the event; **MQTT**: Select MQTT as the action for the event. *Note: The available Event Types will depend on product model.*
Managing Event	Unchecked by default	Click **Enable** box to activate this Managing Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore previous settings.

8.2.3 Notifying Events

Go to **Service** > **Event Handling** > **Notifying Events** Tab.

Notifying Events setting allows administrator to define the relationship (rule) between event trigger and handlers.

Enable Notifying Events



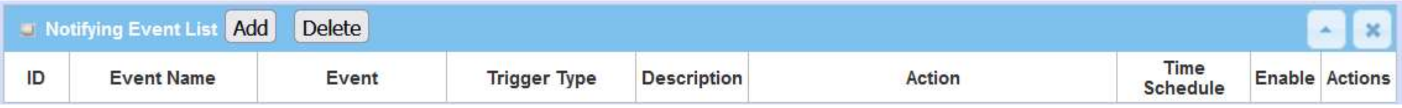
Configuration

Item	Setting
Notifying Events	☑ Enable

Configuration		
Item	**Value setting**	**Description**
Notifying Events	Unchecked by default	Check the **Enable** box to activate the Notifying Events function.

Create / Edit Notifying Event Rules

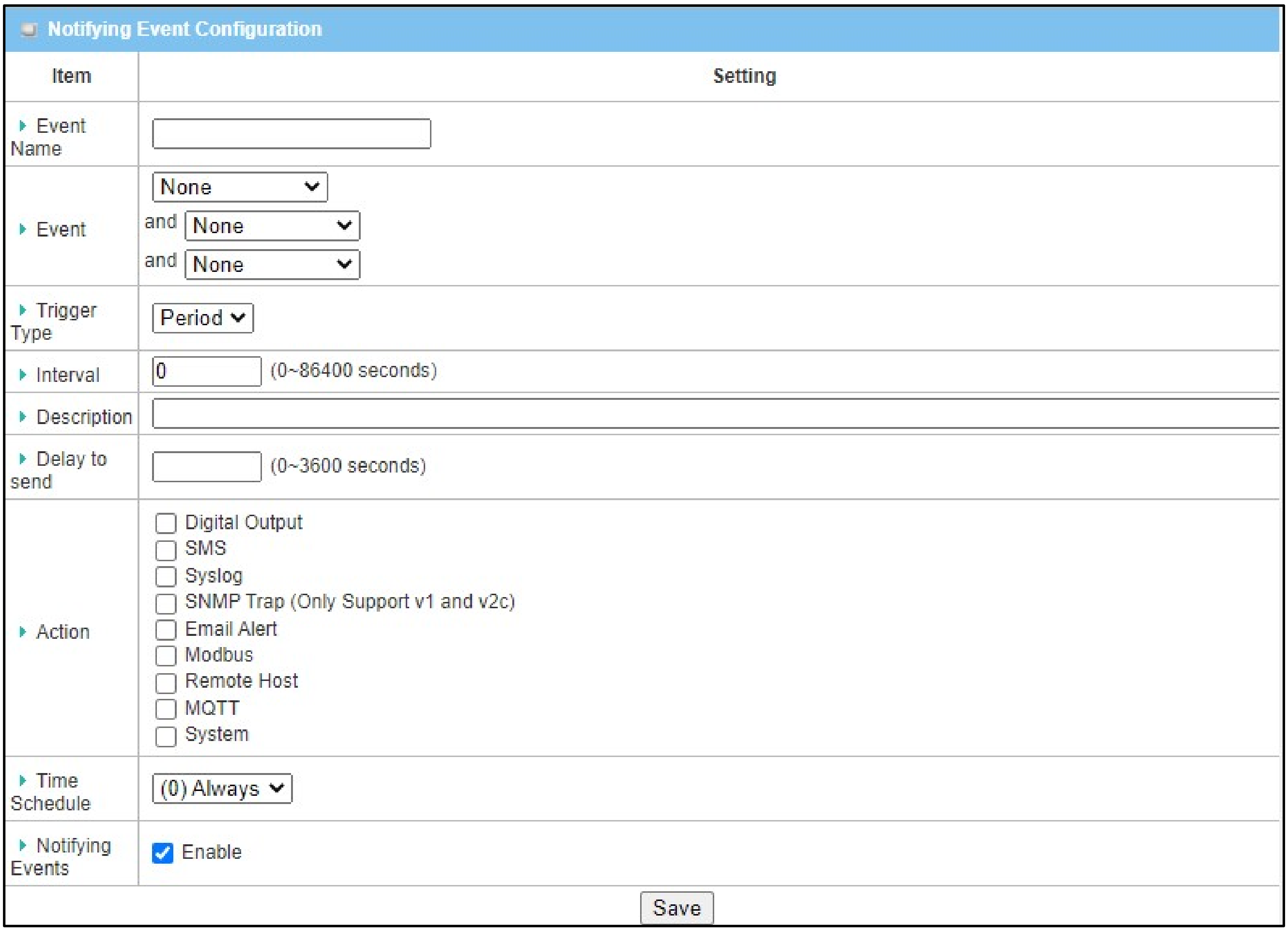
Set up your Notifying Event rules. Up to 128 rules are supported.



Notifying Event List Add Delete

ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

When **Add** or **Edit** button is applied, the **Notifying Event Configuration** screen will appear.



Notifying Event Configuration

Item	Setting
Event Name	
Event	None and None and None
Trigger Type	Period
Interval	0 (0~86400 seconds)
Description	
Delay to send	(0~3600 seconds)
Action	□ Digital Output □ SMS □ Syslog □ SNMP Trap (Only Support v1 and v2c) □ Email Alert □ Modbus □ Remote Host □ MQTT □ System
Time Schedule	(0) Always
Notifying Events	☑ Enable

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event Name	Text field, blank by default	Specify a name for the event.
Event	**None** by default	Specify the Event type and corresponding event configuration. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simultaneously (AND relation). The supported Event Types are: **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event; **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Modbus**: Select **Modbus** and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; **Data Usage**: Select **Data Usage**, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event; **MQTT**: Select MQTT as a trigger condition. **System**: Select System as a trigger condition.
Trigger type	**Period** is selected by default	Specify the type of event trigger, either **Period** or **Once**.

		Period: Select **Period** and specify a time interval, the event will be repeatedly triggered on every time interval when the specified event condition holds. **Once:** Select **Once** and the event will be just triggered just one time when the specified event condition holds.
Interval	**0** is set by default	Specify the repeatedly event trigger time interval. ***Value Range:*** 0 ~86400 seconds.
Description	String format: any text.	Enter a brief description for the Notifying Event.
Delay to Send	0-3600	Delay specified seconds to do action.
Action	All boxes unchecked by default.	Specify at least one action to take when the expected event is triggered. **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **SMS**: Select **SMS**, and the gateway will send out a SMS to all the defined SMS accounts as the action for the event; **Syslog**: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event; **Modbus**: Select **Modbus** and a Modbus Notifying Event profile you defined as the action for the event; **Remote Host:** Select **Remote Host** checkbox and a Remote Host profile you defined as the action for the event; **MQTT**: Select MQTT as the action for the event. **System**: Select System to reboot after 30 seconds as the action.
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	Unchecked by default	Click **Enable** box to activate this Notifying Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore previous settings.

8.3 Azure Agent

This feature allows for the upload of sensors' data to Azure Server via Azure Agent on the EW-50.

Data Flow is as follows:
Sensor→ EW-50 → Azure Server → Azure Remote Monitor

8.3.1 Azure Setup

The configuration steps are as follows:

1. Configure Azure Cloud
   Register and login Azure Server
   Install Azure Remote Monitor
   Build the IoT devices on IoT Hub
2. Configure EW-50
   Modbus RS-485 setting
   Azure Agent
3. Display on Azure Remote Monitor

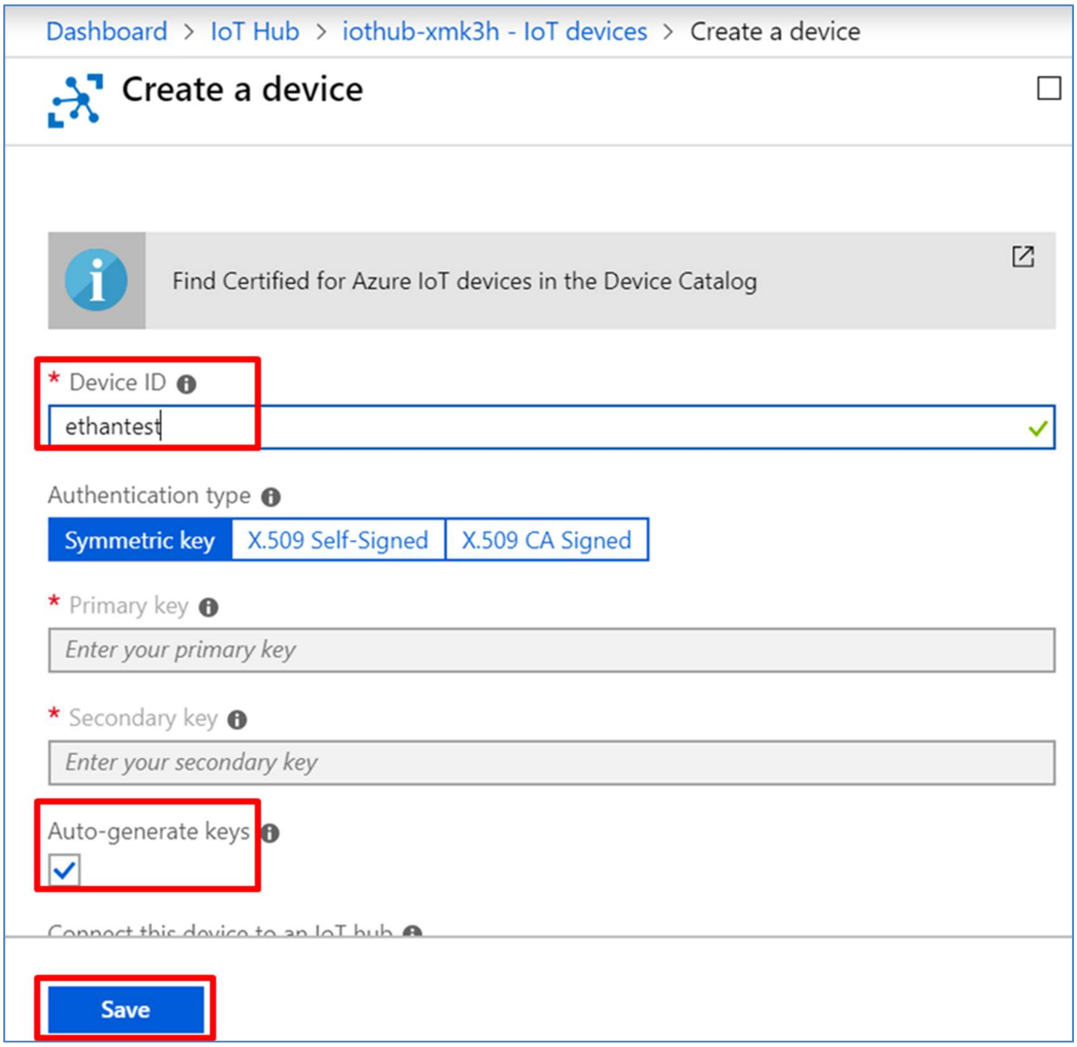
First, register and log in to the Microsoft Azure site.

https://portal.azure.com/
Then, install Azure Remote Monitor

https://www.azureiotsolutions.com/Accelerators

After installing and starting the Azure Remote Monitor, you will see the Azure Remote Monitor Page. You can add IoT devices to the Azure Server by clicking on **IoT Hub**, and then click on the **iothub-xmk3h**, which is created by Azure Remote Monitor.

Click on **IoT devices**.
Click **Add** to create a new IoT device.
Enter Device ID.
Select Auto-generate keys.
Save the configuration.



Dashboard > IoT Hub > iothub-xmk3h - IoT devices > Create a device

Create a device

Find Certified for Azure IoT devices in the Device Catalog

* Device ID: ethantest

Authentication type: Symmetric key | X.509 Self-Signed | X.509 CA Signed

* Primary key: Enter your primary key

* Secondary key: Enter your secondary key

Auto-generate keys ☑

Connect this device to an IoT hub

8.3.1 EW-50 Azure Configuration

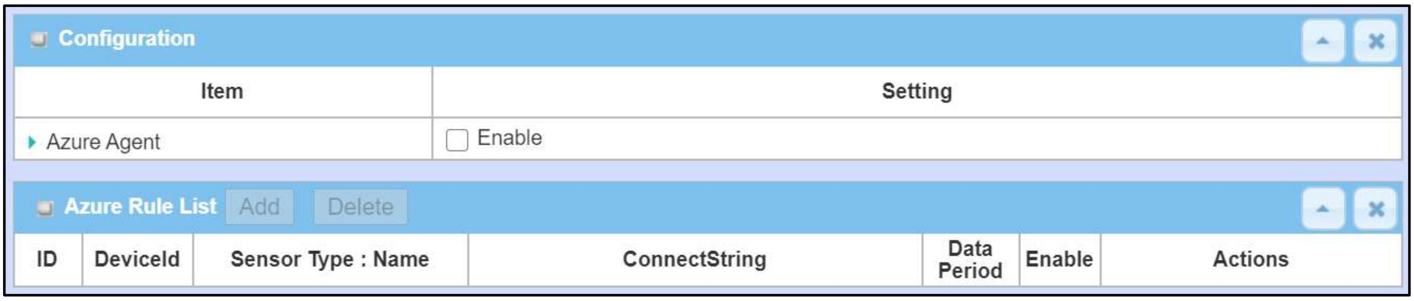
Go to **Field Communication** > **Bus & Protocol**> **Port Configuration** tab.

Refer to section 4.1.1 under **Field Communication**. Input the parameters and save the configuration.

Next, navigate to **Field Communication** > **Bus & Protocol**> **Modbus** tab.

Refer to section 4.1.3 under **Field Communication**. Input the parameters and save the configuration.

Go to **Service** > **Azure Agent** > **Configuration** Tab.



Configuration

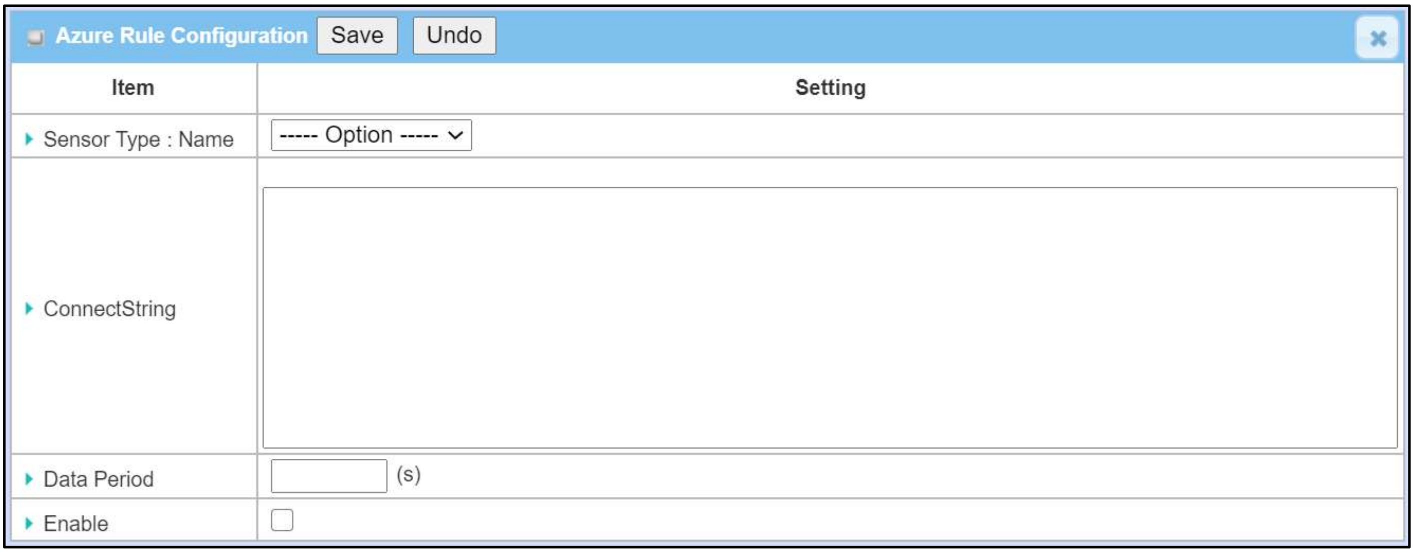
Item	Setting
Azure Agent	□ Enable

Azure Rule List Add Delete

ID	DeviceId	Sensor Type : Name	ConnectString	Data Period	Enable	Actions

Azure Agent Item	Value setting	Description
Azure Agent	Unchecked by default	Click **Enable** to enable Azure Agent function.
Azure Rule List	N/A	Click the Add button to create a new rule.
ID	N/A	Rule ID number.
Device ID	N/A	The device ID.
Sensor Type: Name	N/A	Name of the sensor type
ConnectString	N/A	Connection string for the device. This is obtained from the device you have set up on the Azure website.
Data Period	N/A	Data period.
Enable	N/A	Shows if the rule is enabled.
Actions		

When the Add button is clicked, the Azure Rule Configuration screen will display:

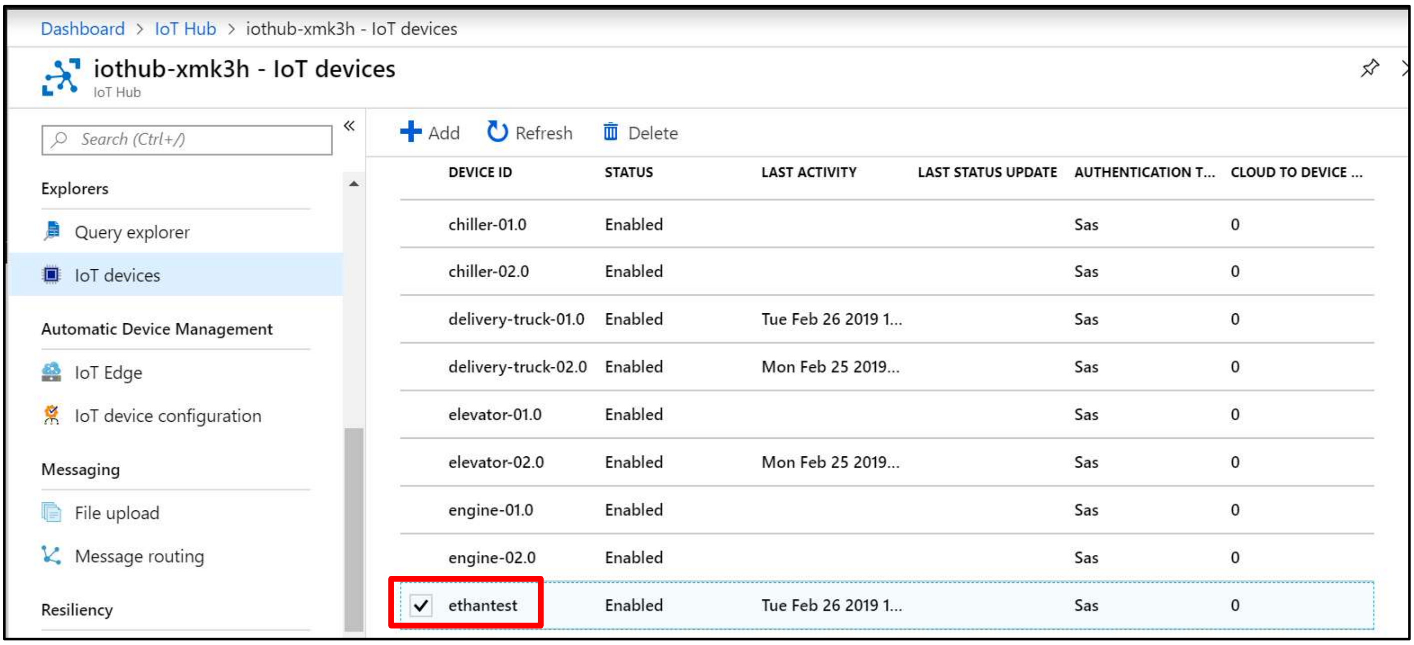


Azure Rule Configuration

Item	Setting
Sensor Type : Name	----- Option -----
ConnectString	
Data Period	(s)
Enable	□

Azure Rule Configuration		
Item	**Value setting**	**Description**
Sensor Type	N/A	Select the sensor type for the Azure Rule
Connectstring	N/A	Enter the corresponding connection string for the device.
Data Period		Enter the data period in seconds.
Enable		Click **Enable** to enable this rule.

Navigate to the Azure website, and click on the device that you have created.

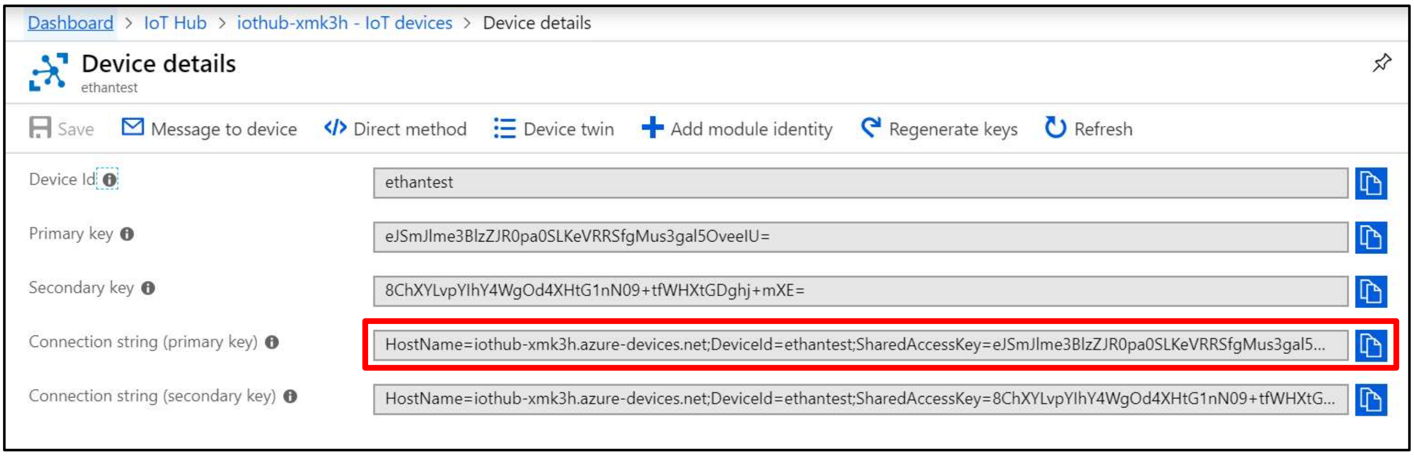


Dashboard > IoT Hub > iothub-xmk3h - IoT devices

iothub-xmk3h - IoT devices
IoT Hub

	DEVICE ID	STATUS	LAST ACTIVITY	LAST STATUS UPDATE	AUTHENTICATION T...	CLOUD TO DEVICE ...
	chiller-01.0	Enabled			Sas	0
	chiller-02.0	Enabled			Sas	0
	delivery-truck-01.0	Enabled	Tue Feb 26 2019 1...		Sas	0
	delivery-truck-02.0	Enabled	Mon Feb 25 2019...		Sas	0
	elevator-01.0	Enabled			Sas	0
	elevator-02.0	Enabled	Mon Feb 25 2019...		Sas	0
	engine-01.0	Enabled			Sas	0
	engine-02.0	Enabled			Sas	0
☑	ethantest	Enabled	Tue Feb 26 2019 1...		Sas	0

Click on the button to copy the Connection String.

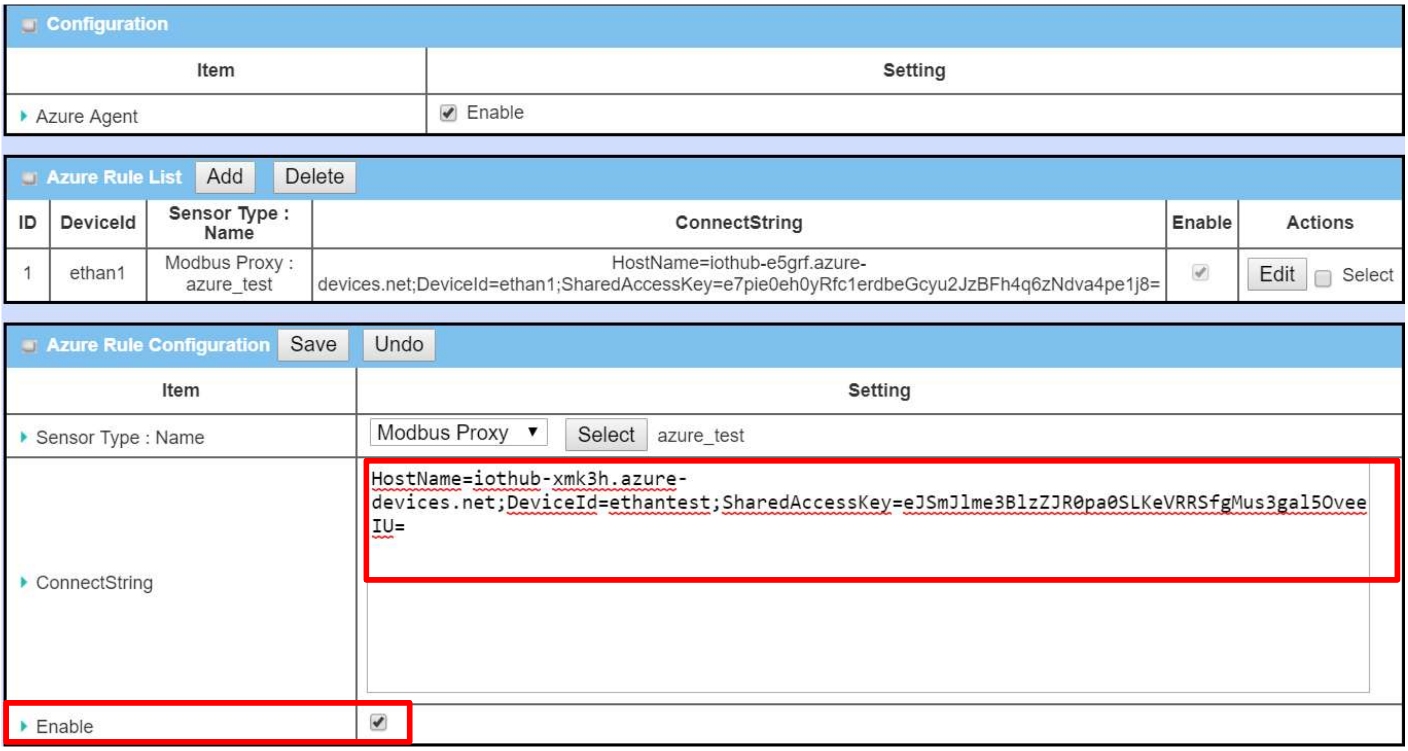


Dashboard > IoT Hub > iothub-xmk3h - IoT devices > Device details

Device details
ethantest

Device Id	ethantest
Primary key	eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5OveeIU=
Secondary key	8ChXYLvpYlhY4WgOd4XHtG1nN09+tfWHXtGDghj+mXE=
Connection string (primary key)	HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5...
Connection string (secondary key)	HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=8ChXYLvpYlhY4WgOd4XHtG1nN09+tfWHXtG...

Navigate back to the EW-50 web console, and paste the Connection String into the corresponding field. Click the checkbox to enable Azure Rule Configuration. Then click **Save**.



Configuration

Item	Setting
Azure Agent	☑ Enable

ID	DeviceId	Sensor Type : Name	ConnectString	Enable	Actions
1	ethan1	Modbus Proxy : azure_test	HostName=iothub-e5grf.azure-devices.net;DeviceId=ethan1;SharedAccessKey=e7pie0eh0yRfc1erdbeGcyu2JzBFh4q6zNdva4pe1j8=	☑	Edit □ Select

Item	Setting
Sensor Type : Name	Modbus Proxy ▼ Select azure_test
ConnectString	HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5OveeIU=
Enable	☑

Navigate to the Azure Remote Monitor web console, and click on the newly created device. You will be able to directly monitor the data from the device.

Specifications

Cellular Interface	
Standards	Cellular Frequency Bands: (Refer to order information for optional bands) 4G LTE: FDD-LTE, TDD-LTE 3G: WCDMA 2G: GSM/EDGE
Antenna connectors	2 x SMA Male
SIM Slots	2

Ethernet	
Standard	IEEE 802.3 10Base-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3ab 1000BASE-T
Ports	2 x RJ45 GE
Physical Layer	10/100/1000Base-T

Serial	
Ports	1 x RS-232/RS-485

I/O	
Digital I/O	1 x DI (“Logic 0”: 0~2V, “Logic 1”: 5V~30V), 1 x DO (Relay Mode, up to 30V / 1A)

Power	
Input Power	DC 9V ~ 36V
Power Consumption	Max. 7.0 Watts

EW50 Industrial LTE Cellular Gateway

Functions	
VLAN	Port-based, Tag-based VLAN
Port Forwarding	Virtual Server/ Computer, DMZ Host, PPTP/L2TP/IPSec Pass-through
Routing	Static, Dynamic: RIP1/RIP2, OSPF, BGP
QoS	Policy-based Bandwidth Control and Packet Flow Prioritization
Virtual COM	RFC 2217, TCP Client, TCP Server, UDP
Modbus	Modbus Slave; Modbus Gateway for Modbus TCP, Modbus RTU/ASCII Master/Slave Access
VPN	IPSec, OpenVPN, PPTP, L2TP, GRE
Firewall	SPI Firewall with Stealth Mode, IPS
Event Handling	Managing / Notifying Events; DI, DO, Modbus, SMS, Syslog, SNMP Trap, Email Alert, Reboot
Device Management Solution	eVue (Q4, 2018)

Physical	
Dimensions (W x D x H)	31 x 99 x 131mm (1.2 x 3.9 x 5.2”) (without mounting brackets)
Weight	0.9Kg (1.98lb)
Mounting	DIN-Rail

Environmental	
Operating Temperature	-30 to +70°C (-22 to +158°F)
Storage Temperature	-40 to +85°C (-40 to +185°F)
Relative Humidity	5% to 95% (non-condensing)

Regulatory Approvals	
Safety	EN 60950-1 EN 62368-1:2014
Cellular	PTCRB (TBD)
Emissions / Immunity	CE / NCC BSMI / VCCI

Contact Information

EtherWAN System, Inc.
www.etherwan.com

USA Office
2301 E. Winston Road
Anaheim, CA 9280
Tel: +1-714-779-3800
Email: info@etherwan.com

Pacific Rim Office
8F., No.2, Alley 6, Lane 235, Baoqiao Rd.
Xindian District, New Taipei City 231
Taiwan
Tel: +886 -2- 6629-8986
Email: info@etherwan.com.tw

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

EW50 Industrial LTE Cellular Gateway
March 31, 2022