Version 1.00 | 06/21/2024



User Manual

5G Multi-Connect PoE Modem

DWM-314-GP

5G Multi-Connect PoE Modem

Chapter 1 Introduction 4
1.1 Introduction 4
1.2 Contents List 5
1.2.1 Package Contents 5
1.3 Hardware Configuration 6
1.4 LED Indication 8
1.5 Installation& MaintenanceNotice 8
1.5.1 SYSTEM REQUIREMENTS 8
1.5.2 WARNING 9
1.5.3 HOT SURFACE CAUTION 11
1.5.4 Product Information for CE RED Requirements 12
1.6 Hardware Installation 13
1.6.1 Mount the Unit 13
1.6.2 Insert the SIM Card 13
1.6.3 Connecting to the Network or a Host 14
1.6.4 Setup by Configuring WEB UI 14
Chapter 2 Status 15
2.1 Cellular 15
2.1.1. Network 15
2.1.2 Modem 16
2.1.3 Signal 19
2.1.4 Data Usage (Refer to 3.3.4) 20
2.2 Network 20
2.3 Security 20
2.3.1 VPN 20
2.4 DashBoard 21
2.4.1 PoE Status 22
Chapter 3 Setup 22
3.1 Network 22
3.1.1 Device Mode 23
3.1.2 Cellular 23
3.1.3 Ethernet 26
3.1.4 Port Forwarding 28
3.1.5 DDNS 31

3.1.6 PoE 32
3.2 Routing 33
3.2.1 Static Routing 33
3.2.2 Routing Information 35
3.3 System 36
3.3.1 System Time 36
3.3.2 System Information 37
3.3.3 Scheduling 37
3.3.4 Data Cap 39
Chapter 4 Security 39
4.1 VPN 40
4.1.1 OpenVPN 40
4.1.2 WireGuard 44
4.2 Firewall 47
4.2.1 Packet Filters 47
4.2.2 MAC Control 51
4.2.3 IPS 53
4.2.4 URL Block 54
Chapter 5 Administrator 55
5.1 Manager 55
5.1.1 FW Upgrade 55
5.1.2 Password & MMI 56
5.1.3 Reboot & Reset 57
5.1.4 SSH 58
5.1.5 Remote Administrator 58
5.1.6 Device management 59
5.2 Utility 60
5.2.1 SMS 60
5.2.2 Command Script 64
5.2.3 System log 64

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of D-Link's 5G Multi-Connect PoE Modem. With this 5G Modem you have made a great first step in the world of connected Internet of things (IoT) by simply inserting a SIM card from the local mobile carrier into this device to get things connected. This section gives you all the information you need to set up your device.

Main Features:

- Provide 5G WAN connection and is back compatible with 3G/4G.
- Provide two 1 Gigabit Ethernet ports for the LAN connection.
- Provide two 1 Gigabit Ethernet ports supporting 802.3at PoE connectivity
- Instinctive Web GUI is used for basic setting and check the cellular status.
- Designed easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

1.2 Contents List

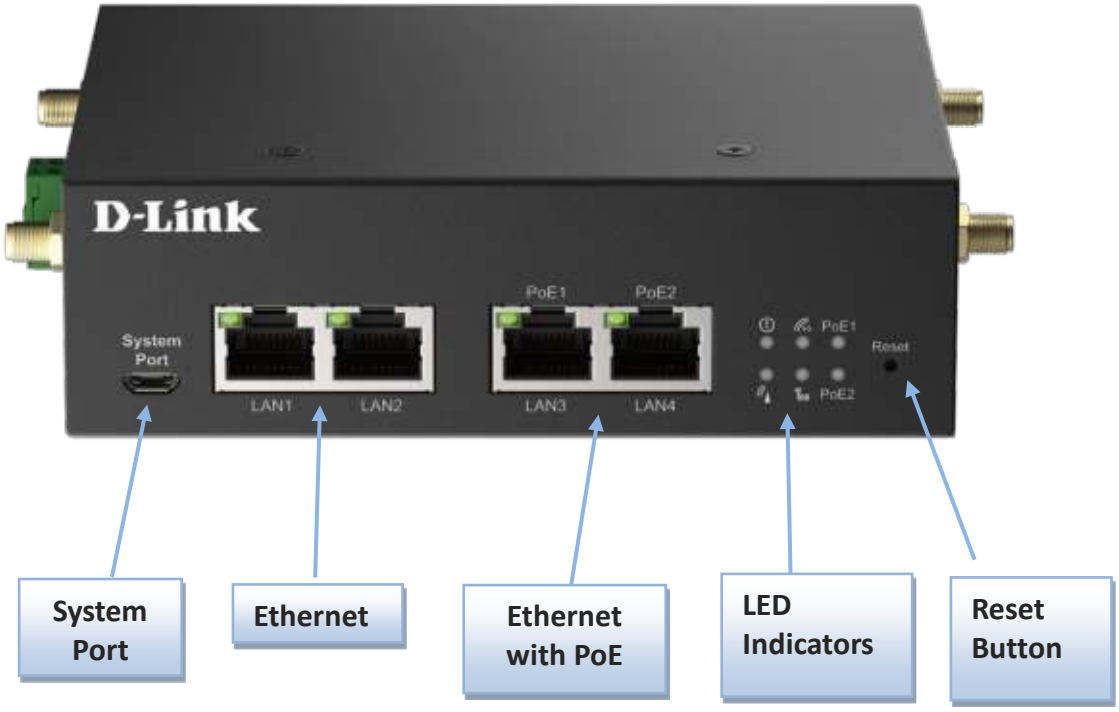
1.2.1 Package Contents

#Standard Package

Items	Description	Contents	Quantity
1	**DWM-314-GP** **5G Multi-Connect PoE Modem**		1pcs
2	**Cellular Antenna**		4pcs
3	**RJ45 Cable**		1pcs
4	**2 Pin Terminal Block**		1pcs
5	**Power Adapter** **(54V/1.67A)**		1pcs
6	**Power Cord**		1pcs
7	**DIN-Rail Bracket**		1 set (DIN rail: screw x3)

1.3Hardware Configuration

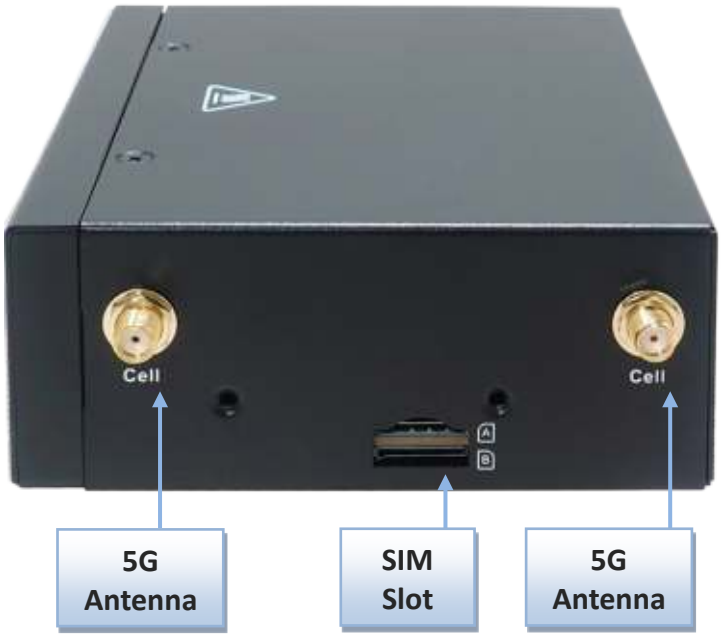
➢ Front View



※Reset Button

RESET button provides user a quick and easy way to restore the default setting. Press the RESET button continuously for more than 8 seconds, and then release it. The device will restore to factory default settings

- Right View

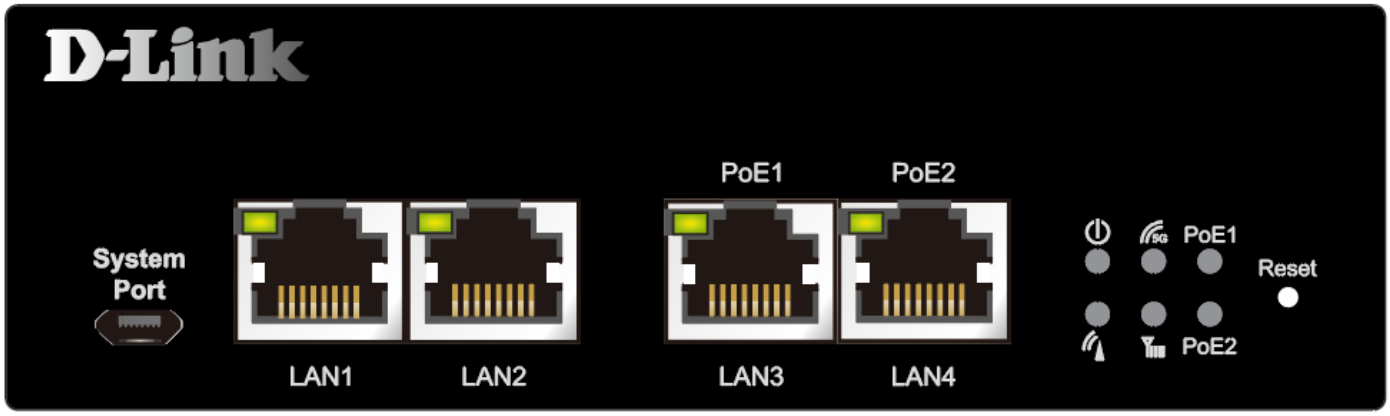


- Left View



.

1.4 LED Indication



Indication	LED Color	Description
Power	Blue	**Steady On**: Device power is on **Off**: Device power is off
Cellular	Blue	**Blue and Steady On:** Cellular is registering to network. **Blue and Flash:** Cellular is not registered to network.
5G/LTE	Blue	**Bule and steady on:** The device registers to 5G network **Blue and Flash:** The device registers to LTE network
Signal Strength	Blue	**Blue and Steady On:** Cellular signal is good. **Blue and Slow Flash:** Cellular signal is weak. **OFF:** No cellular signal.
PoE1 PoE2 PoE 1 ~ 2	Blue	**Steady On:** Supply PoE Power to Ethernet Port. **Off:** No PoE Power to Ethernet Port
Ethernet LAN1~4 (in RJ45 port)	Green	**Green and Steady On:** A Ethernet device is connected. **Green and Flash:** Data transmission through Ethernet.

1.5 Installation& MaintenanceNotice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• An Ethernet RJ45cable • 4G/5G cellular service subscription • 100/1000M Ethernet adapter on PC
Web-based Configuration Utility	**Computer with the following:**

Requirements	• Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 8.0 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 adapter that comes with the package. Using a different voltage rating power adaptor 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.
- Place the product on a stable surface and avoid

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR PORTABLE DEVICE USAGE (<20m from body/SAR needed)

Radiation Exposure Statement:

The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

FOR MOBILE DEVICE USAGE (>20cm/low power)

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must fixed to US operation channels only.

1.5.3 HOT SURFACE CAUTION



CAUTION: The surface temperature for the metallic enclosure can be very high!

Especially after operating for a long time, installed at a closed cabinet without air conditioning support, or in a high ambient temperature space.

DO NOT touch the hot surface while servicing!!

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.[1]

(1) Frequency Band & Maximum Power

Band Number	Frequency Band	Max. Output Power
WCDMA Band 1	1920 ~ 1980 MHz	24 dBm
WCDMA Band 5	824 ~ 849 MHz	24 dBm
WCDMA Band 8	880 ~ 915 MHz	24 dBm
LTE Band 1	1920 ~ 1980 MHz	23 dBm
LTE Band 3	1710 ~ 1785 MHz	23 dBm
LTE Band 5	824 ~ 849 MHz	23 dBm
LTE Band 7	2500 ~ 2570 MHz	23 dBm
LTE Band 8	880 ~ 915 MHz	23 dBm
LTE Band 20	832 ~ 862 MHz	23 dBm
LTE Band 28	703 ~ 748 MHz	23 dBm
LTE Band 38	2570 ~ 2620 MHz	26 dBm
LTE Band 40	2300 ~ 2400 MHz	23 dBm
LTE Band 41	2496 ~ 2690 MHz	26 dBm
LTE Band 42	3400 ~ 3600 MHz	26 dBm
LTE Band 43	3600 ~ 3800 MHz	26 dBm
5G NR Band n1	1920 ~ 1980 MHz	23 dBm
5G NR Band n3	1710 ~ 1785 MHz	23 dBm
5G NR Band n5	824 ~ 849 MHz	23 dBm
5G NR Band n7	2500 ~ 2570 MHz	23 dBm
5G NR Band n8	880 ~ 915 MHz	23 dBm
5G NR Band n20	832 ~ 862 MHz	23 dBm
5G NR Band n28	703 ~ 748 MHz	23 dBm
5G NR Band n38	2570 ~ 2620 MHz	26 dBm
5G NR Band n40	2300 ~ 2400 MHz	23 dBm
5G NR Band n40	2300 ~ 2400 MHz	23 dBm
5G NR Band n41	2496 ~ 2690 MHz	29 dBm
5G NR Band n77	3300 ~ 4200 MHz	29 dBm
5G NR Band n78	3300 ~ 3800 MHz	29 dBm

1. The information presented in this section is ONLY valid for the EU/EFTA regional version.For those non-CE/EFTA versions, please 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 device can be placed on a desktop, or use extender to place on DIN-Rail bracket or mount on the wall.

1.6.2 Insert the SIM Card

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

SIM card slot is located in the right side of device. You need to unscrew and remove the outer SIM card cover before installing or removing an inserted SIM card. Please follow below instructions to install or remove SIM card. After SIM card is well installed or removed, screw back the outer SIM card cover.

Step 1:
Loosen the screws as below and remove the SIM cover.



Step 2:
Push the SIM card into the slot A (SIM-A) or slot B (SIM-B).



Step 3:
Push the inserted SIM card again to reject it from the SIM slot.



1.6.3 Connecting to the Network or a Host

The DWM-314-GP provides four RJ45 ports to connect to 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 to connect this device to the host PC for device configuration.

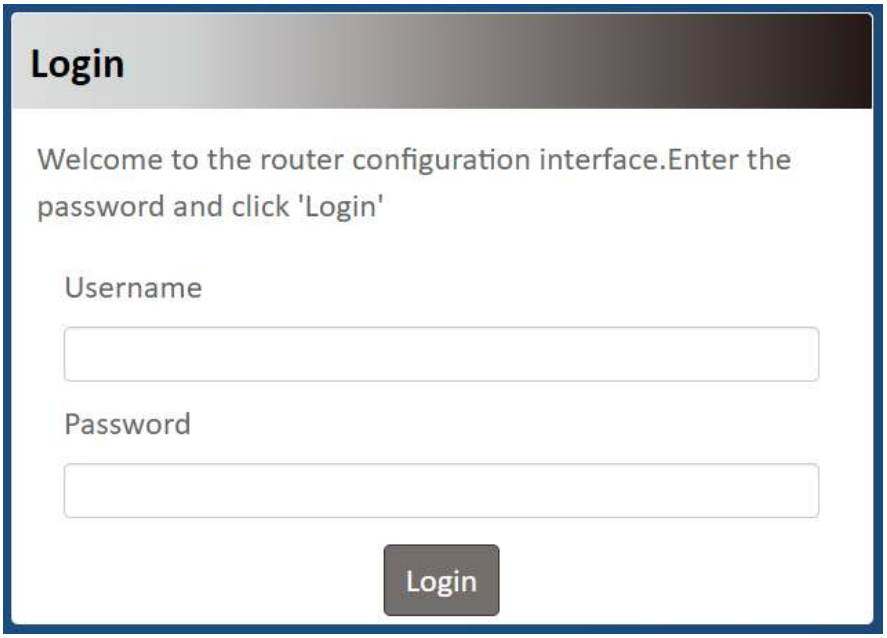
1.6.4 Setup by Configuring WEB UI

You can browse web UI to configure the device.

Type in the IP Address (http://192.168.0.1)[2]



When you see the login page, enter the user name and password and then click **'Login'** button.



The default setting for both username and password is **'admin'**[3].

2. The default LAN IP address of this gateway is 192.168.0.1 , If you change it, you need to login by using the new IP address.

3. For security concern, the login process will force user to change default password at the first time.

Chapter 2 Status

2.1 Cellular

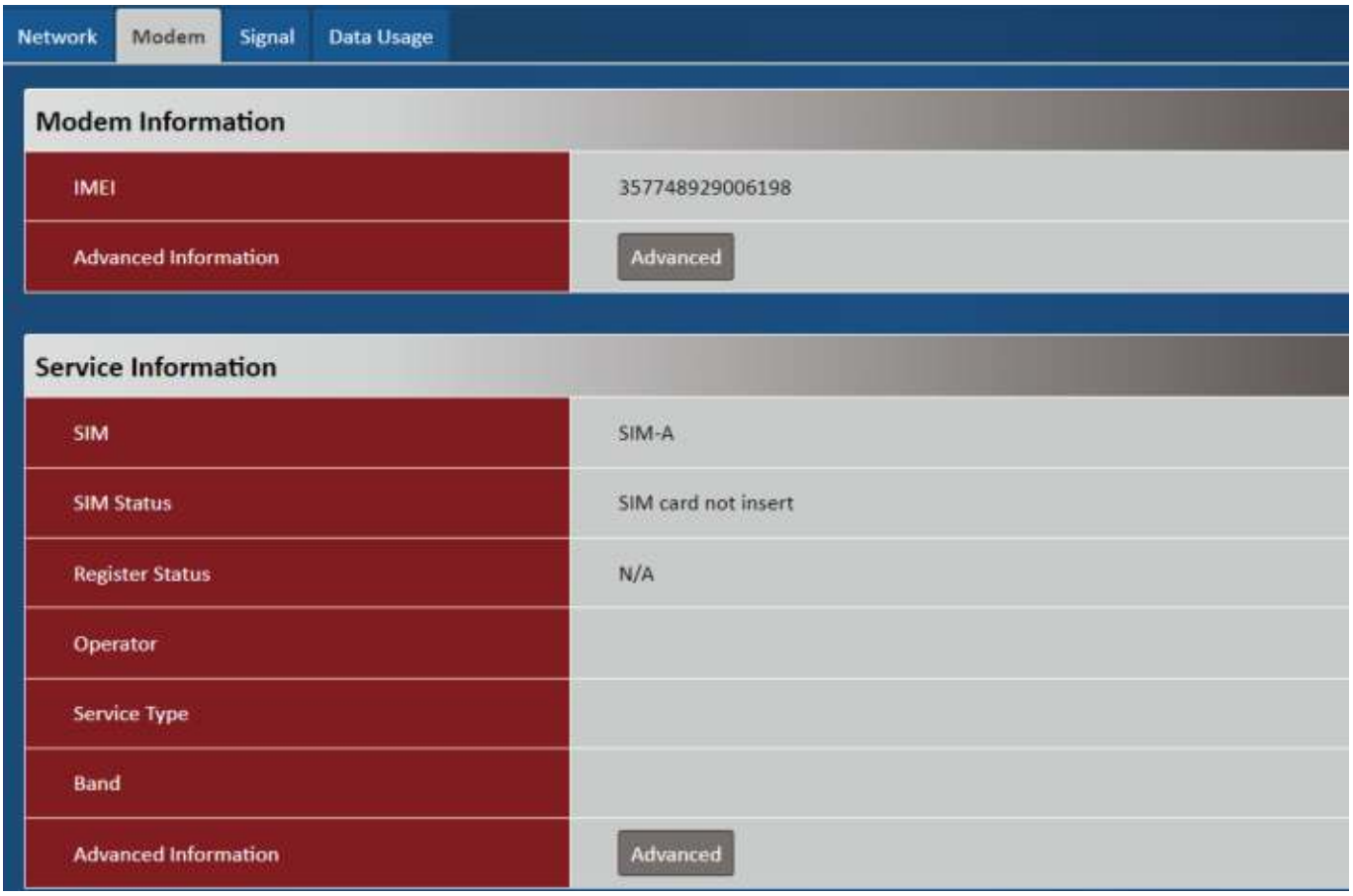


2.1.1. Network

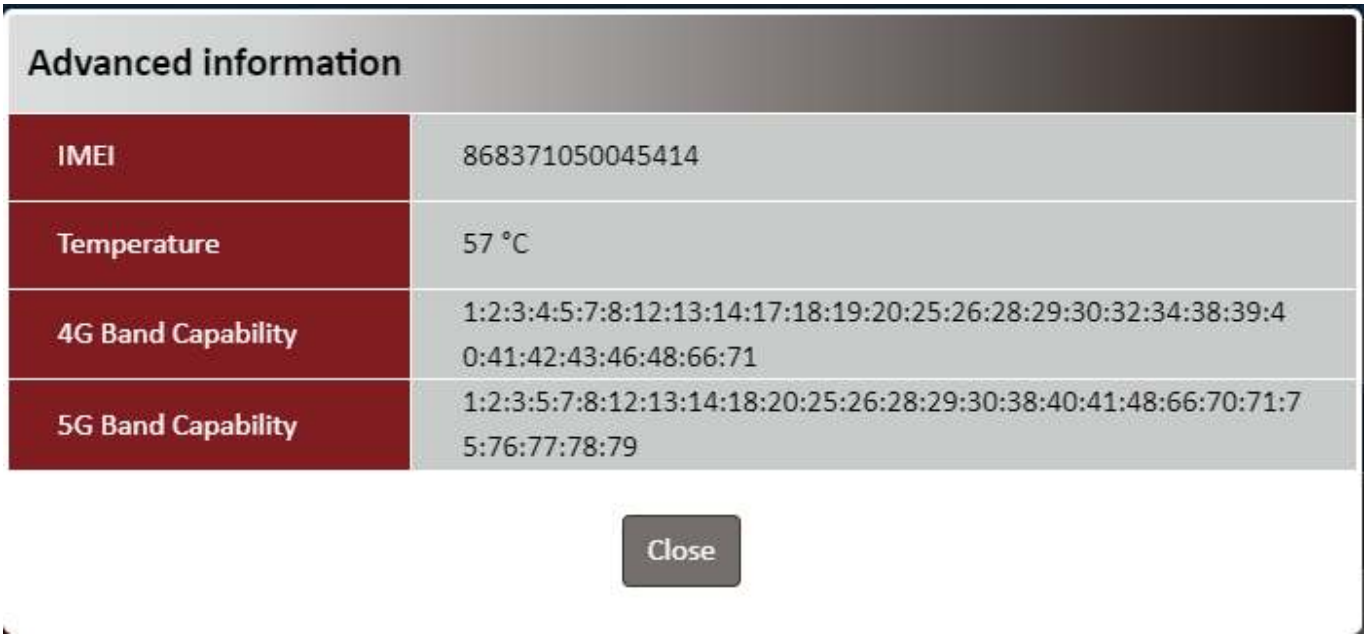


Network Page	
Item	**Description**
Mode	Network type NAT
Link Status	Display cellular network status connected or disconnected.
IP address	Base station distribution network IP
Netmask	Display cellular network netmask
Gateway	Display cellular network gateway

2.1.2 Modem



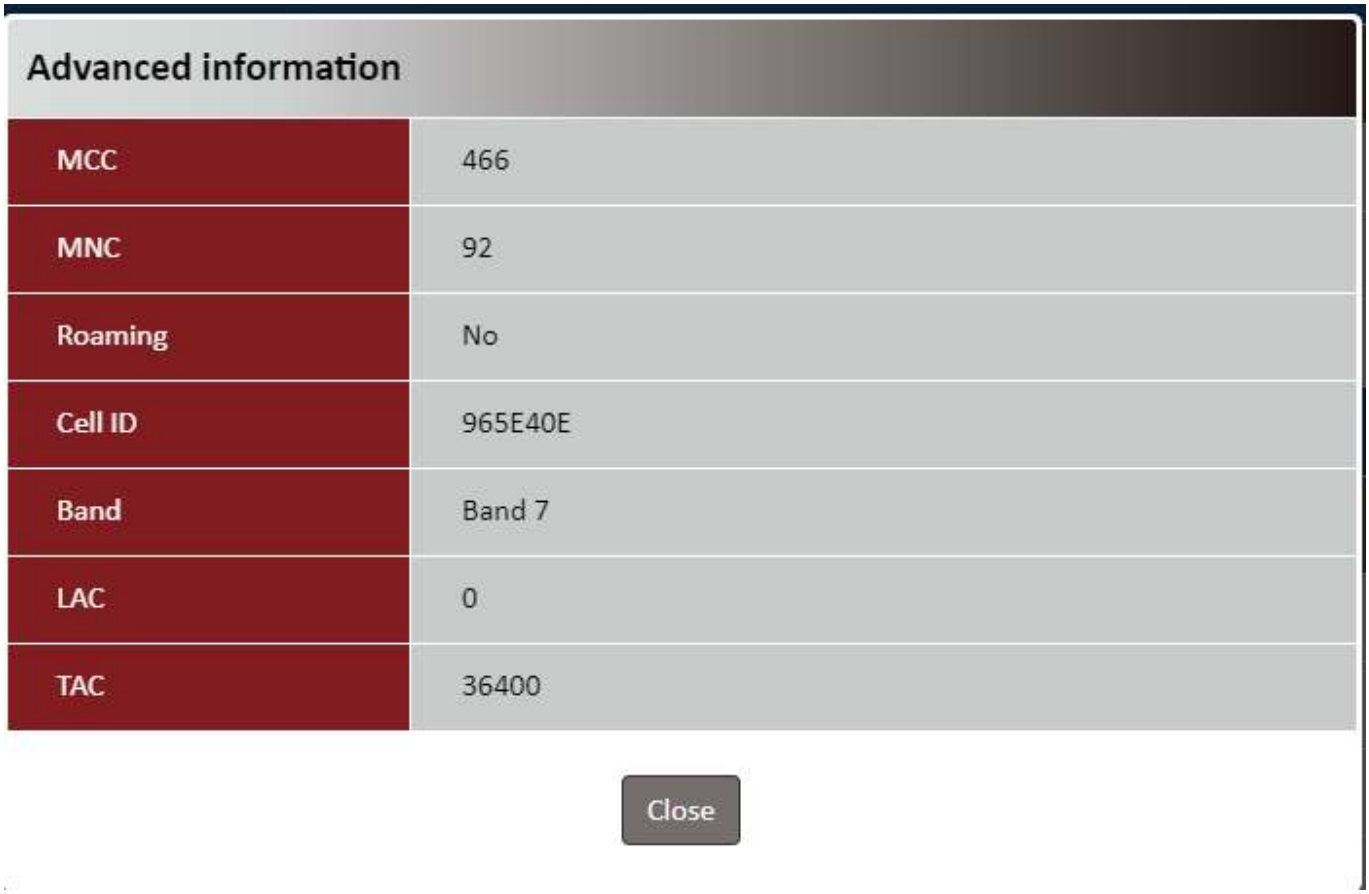
Modem information Page	
Item	**Description**
IMEI	Display modem IMEI information
Advanced Information	Click **advanced** button to show Advanced Information



Advanced Information Page	
Item	**Description**
IMEI	Display modem IMEI information
Temperature	Module temperature
4G Band capability	4G support band
5G Band capability	5G support band

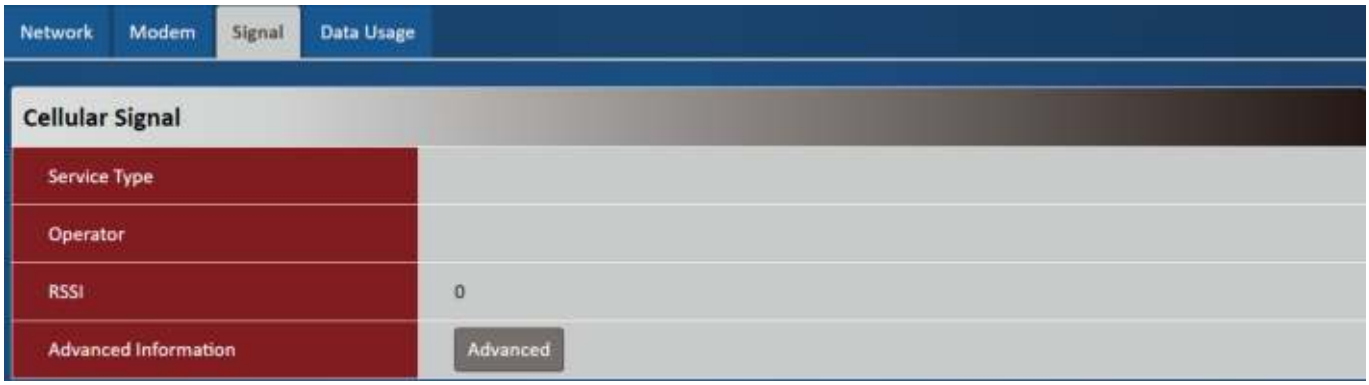


Service Information Page	
Item	**Description**
Sim	Display card slot
Sim status	Display read sim status
Register status	Display base station registration status registered or not register
Operator	Operator name
Service type	Display LTE /5G
Band	Connected frequency band
Advanced Information	Click **advanced** button to show Advanced Information

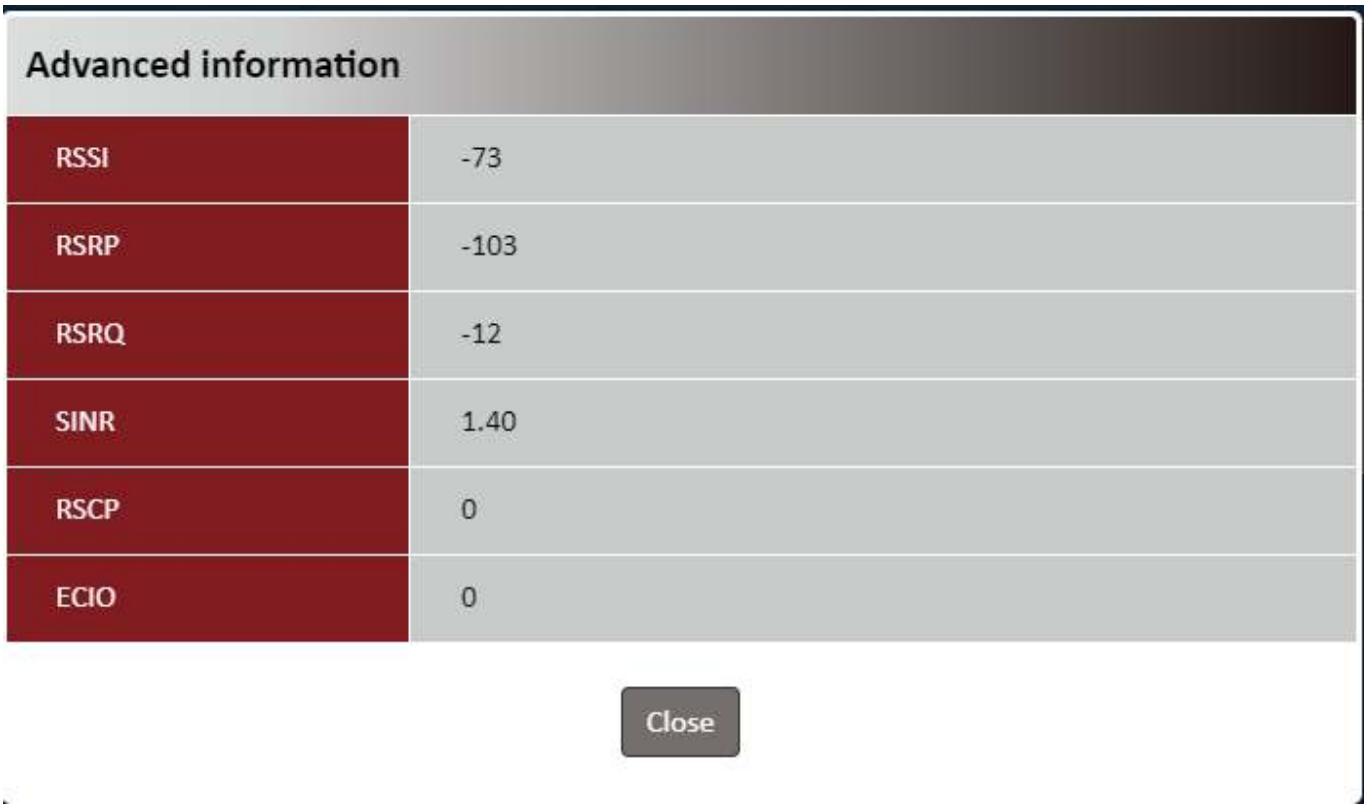


Advanced Information Page	
Item	**Description**
MCC	Display modem IMEI information
MNC	Module temperature
Roaming	Roaming status no or roaming
Cell id	Cell id
Band	Connected frequency band
LAC	Location Area Code
TAC	Tracking Area Number

2.1.3 Signal



Cellular Signal Page	
Item	**Description**
Service type	Cellular service type LTE /5G
Operator	Operator name
RSSI	Display Received Signal
Advanced Information	Click **advanced** button to show Advanced Information



Advanced Information Page	
Item	**Description**
RSSI	Display Received Signal
RSRP	Display Signal Received Power
RSRQ	Display Signal Received Quality
SINR	Display Interference Strength
RSCP	Display Signal received Power
ECIO	Display interference Ratio

2.1.4 Data Usage (Refer to 3.3.4)



2.2 Network



Network Page	
Item	**Description**
Client List	Display connected client list

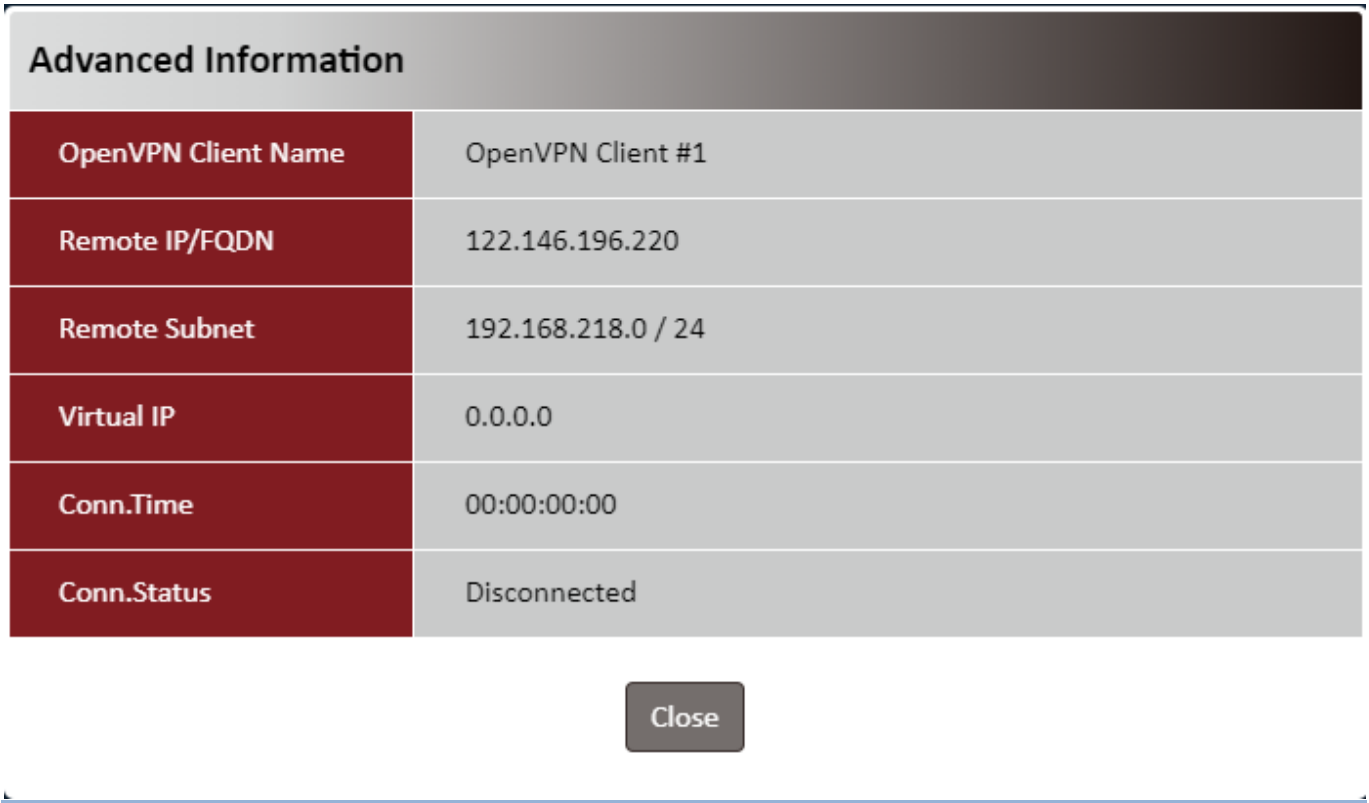
2.3 Security



2.3.1 VPN

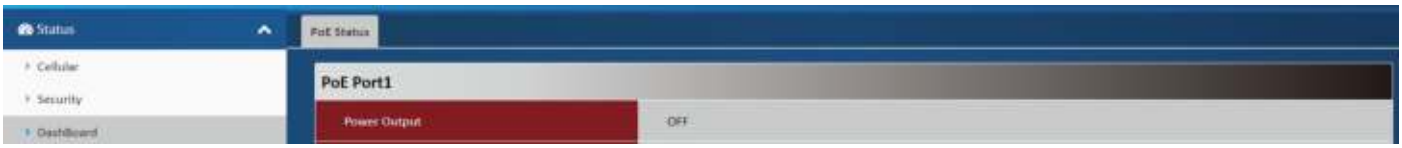


OpenVPN client name Page	
Item	**Description**
Openvpn client #1	Click **advanced** button to display the VPN connection status

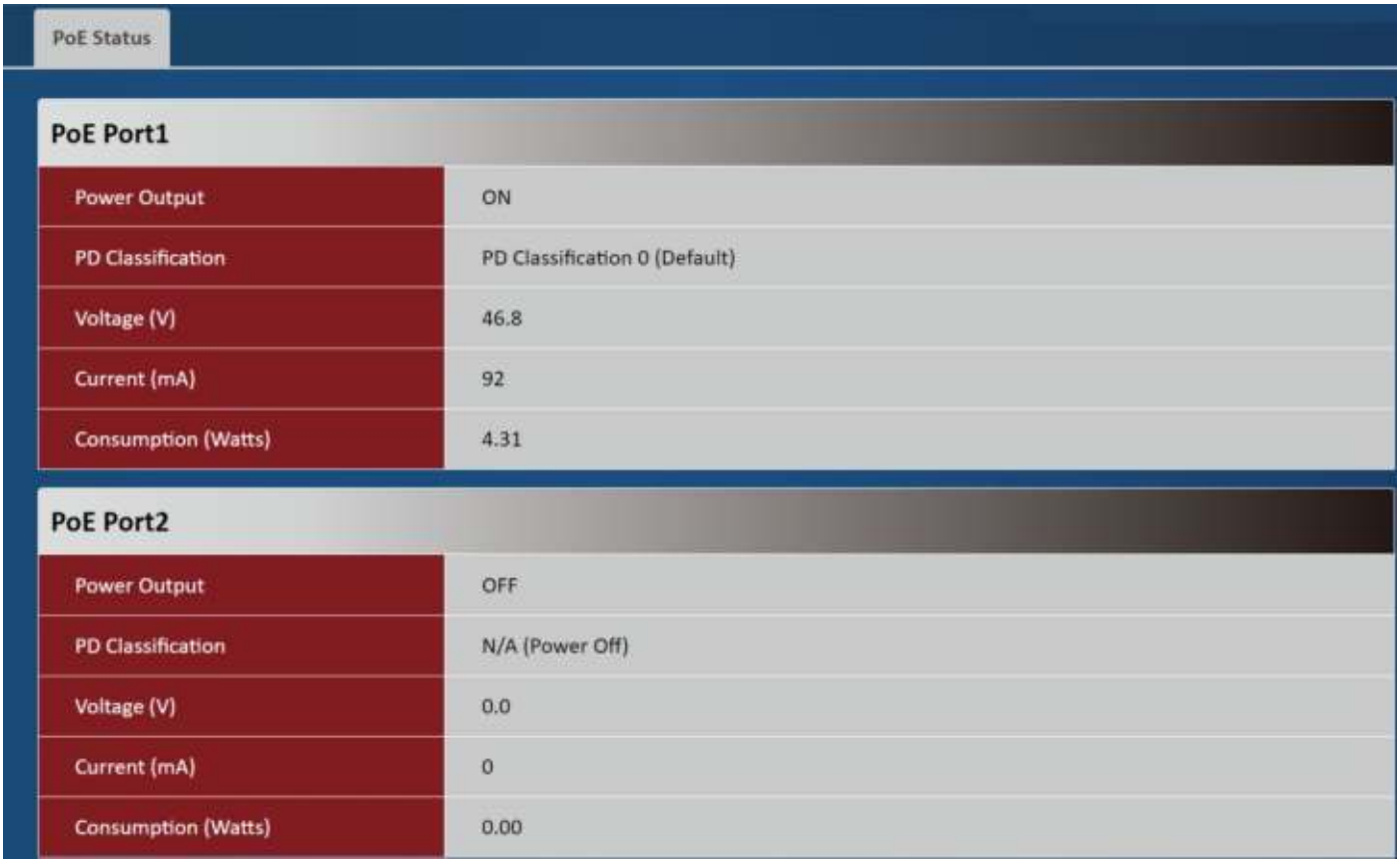


Advanced Information Page	
Item	**Description**
Openvpn client name	Vpn Client name
Remote IP/FQDN	Vpn server IP or FQDN
Remote subnet	Vpn server remote subnet
Virtual IP	Vpn virtual IP
Conn.time	Display connected time
Conn.status	Display connected or disconnected

2.4 DashBoard



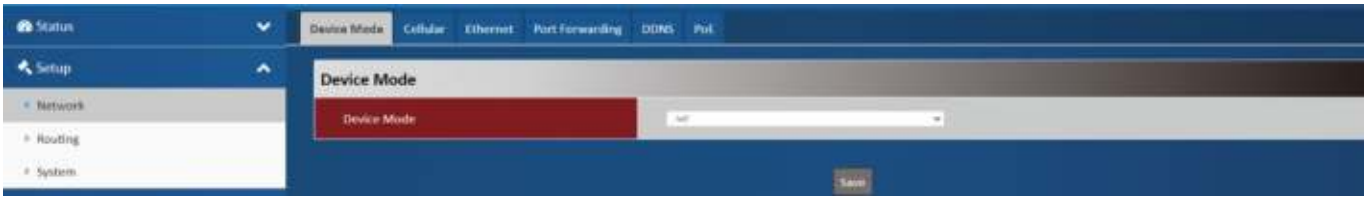
2.4.1 PoE Status



Chapter 3 Setup

The DWM-314-GP connects to a machine via the Ethernet interface for 3G/4G/5G network connection. The DWM-314-GP also provides another function with NAT router. It can help the network application to be more flexible.

3.1 Network



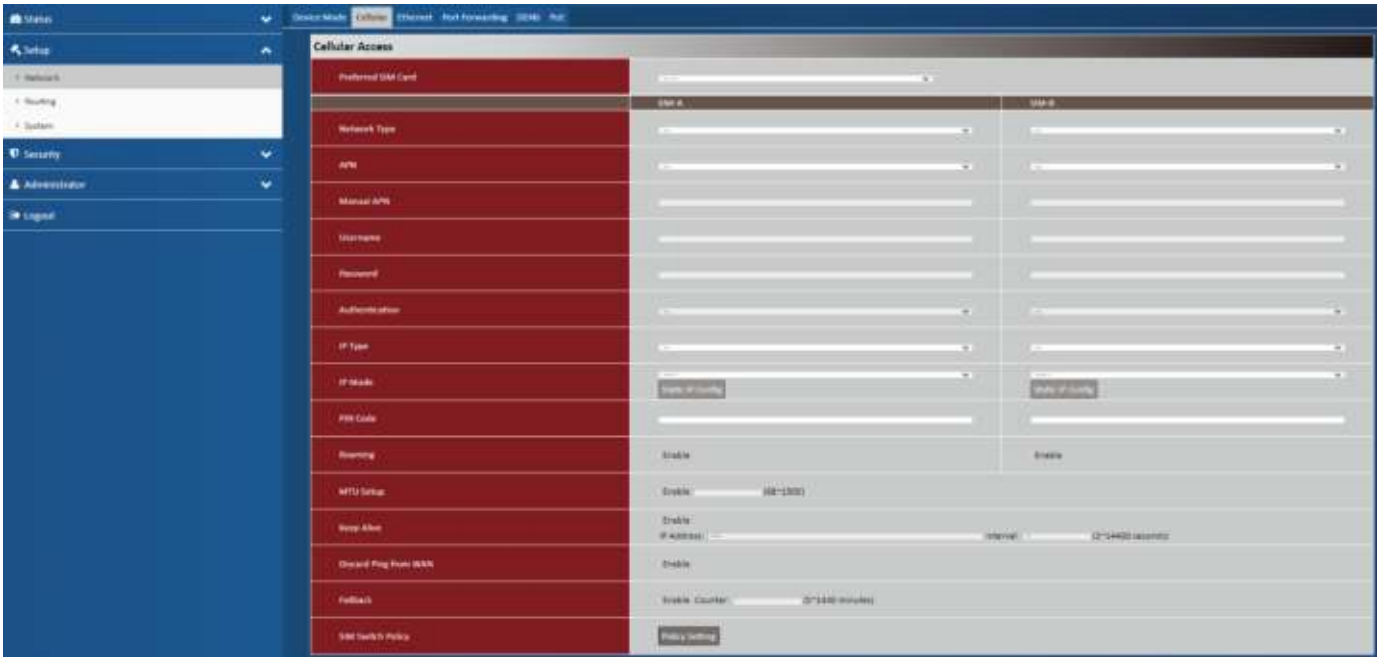
Network Page	
Item	**Description**
Device Mode	Set the unit operating mode
Cellular	Set the parameter for cellular network.
Ethernet	Set the IP of Ethernet and DHCP service
Port Forwarding	Enable specified port or protocol for service on connected device.
DDNS	Register a dynamic host name for the unit.
PoE	PoE port definition setting

3.1.1 Device Mode



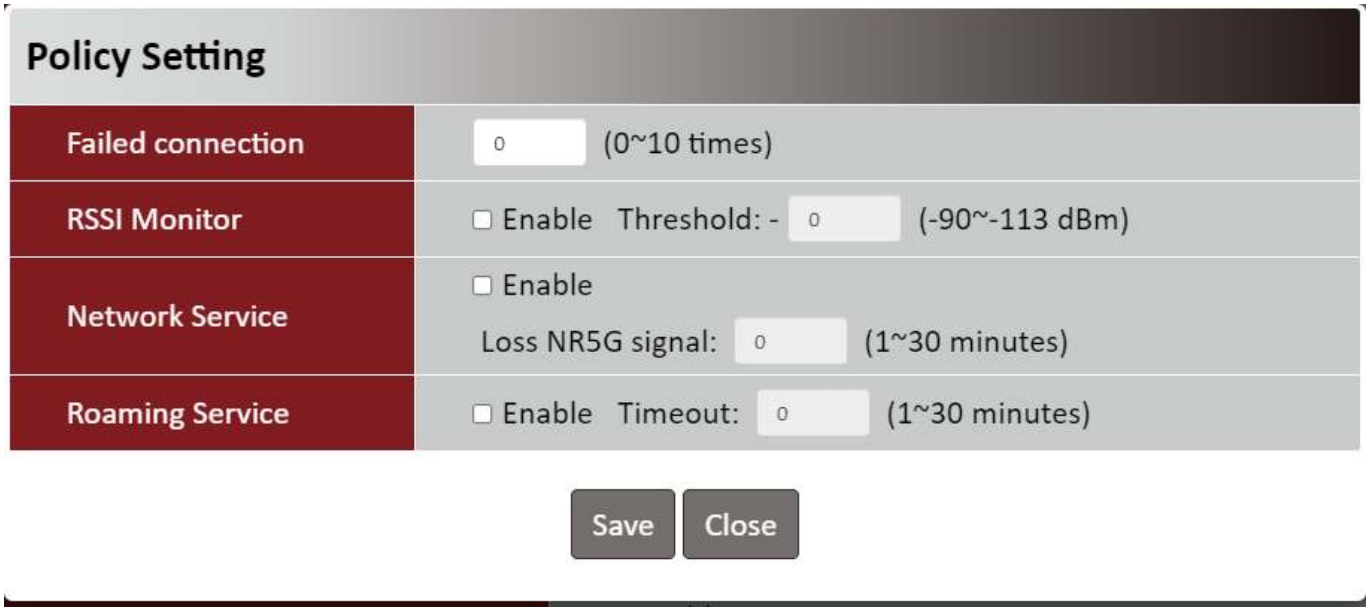
Device Mode		
Item	**Value setting**	**Description**
Device Mode	1. A Must-fill setting 2. By default **NAT** is selected	**NAT** The unit will provide a NAT service and provide a simple firewall for the connected device. **Modem** The unit will pass the cellular IP to connected device via Ethernet

3.1.2 Cellular

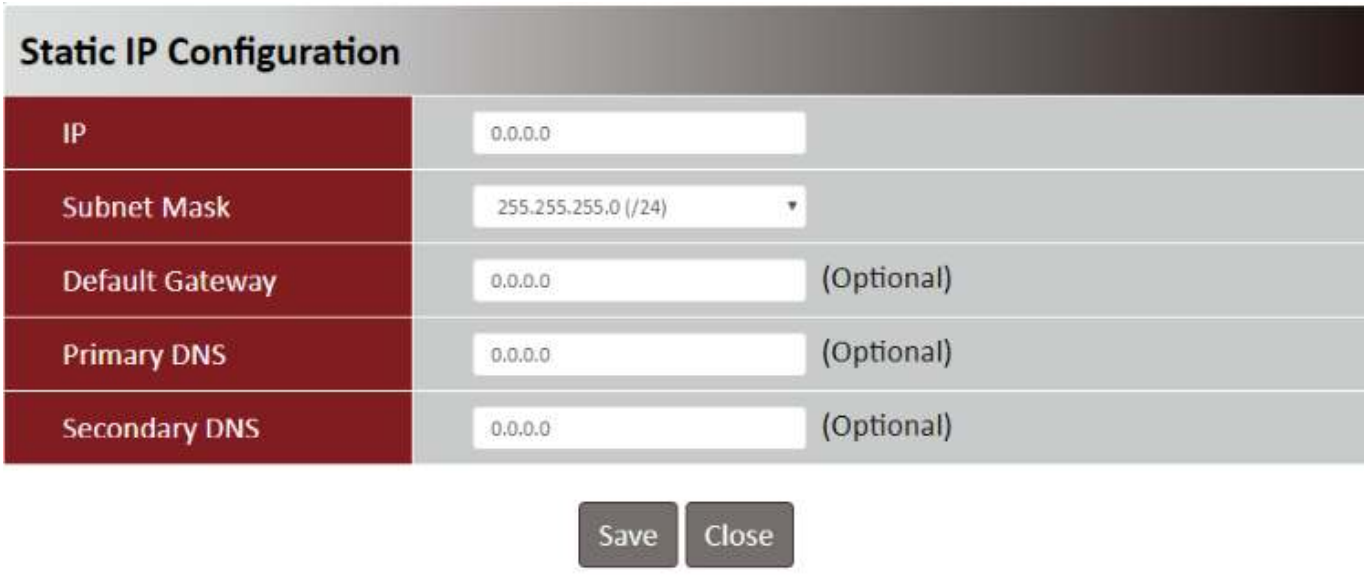


Device Mode		
Item	**Value setting**	**Description**
Preferred SIM Card	SIM-A First SIM-B First SIM-A Only SIM-B Only	To select the SIM connection mode
Network Type	Auto NR5G-SA NR5G-NSA LTE	To select the cellular signal connection type
APN	1. A Must-fill setting 2. By default **Auto** is selected	**Auto** The unit will detect the SIM and set an APN from internal database. **Manual** User must set APN manually.
Manual APN	1. A Must-fill setting	Enter the **APN** you want to use to establish the connection.

	2. String format : any text	This is a must-fill setting if you selected **Manual APN** as APN scheme.
Username	1. An Optional setting 2. String format : any text	Enter the optional **username** settings if your ISP provided such settings to you.
Password	1. An Optional setting 2. String format : any text	Enter the optional **Password** settings if your ISP provided such settings to you.
Authentication	1. A Must-fill 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 either **PAP** or **CHAP**.
IP Type	1. A Must-fill setting 2. By default **IPv4** is selected	Specify the IP type of the network service provided by your 3G/4G network. It can be **IPv4**, **IPv6**, or **IPv4v6**.
IP Mode	1. A Must-fill setting 2. By default **Dynamic IP IP** is selected	**Dynamic IP** The unit will get IP from cellular service.. **Static IP** The unit will set IP according to **Static IP Config**.
PIN Code	1. An Optional setting 2. String format : interger	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Roaming	1. An Optional setting 2. **Uncheck** by default	Check the checkbox to enable the modem to connect on the cellular network at roaming state.
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***:68 ~ 1500.
Keep Alive	1. An optional setting 2. Box is unchecked by default	Check the **Enable** box to activate the keep alive function. Input **IP Address** and **interval** to send an ICMP packet to check the network status.
DiscardPing from WAN	1. An Optional setting 2. **Uncheck** by default	The modem will not respond the ICMP request packet from remote hosts when the checkbox is checked.
Failback	1. **Uncheck** by default 2. 5 **minutes** by default	When Failback is checked, when the main WAN can be connected, it will switch to the main WAN after the set count time is up ***Value Range***:5 ~ 1440 minutes.
SIM Switch Policy		Click the **Policy Setting** button to define the SIM Switch policy or browse the current policy settings.

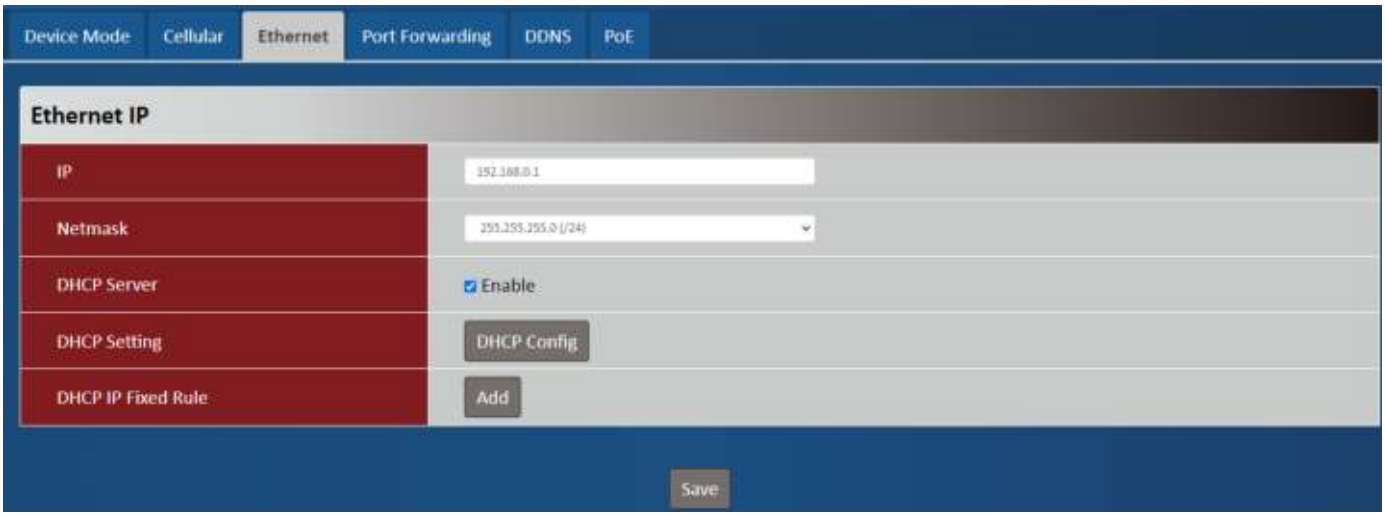


Policy Setting		
Item	**Value setting**	**Description**
Failed connection	1. 0 By default 2. Unchecked by default	Number of failed connections, After the number of times is reached, switch the SIM
RSSI Monitor	1.0 By default 2. Unchecked by default	When the signal is less than the set value, the SIM will be switched
Network service	1.0 By default 2.	When the loss NR5G signal reaches the set value time, start switching SIM
Roaming service	1. 0 By default	**Switch SIM when roaming timeout time reaches the set value**

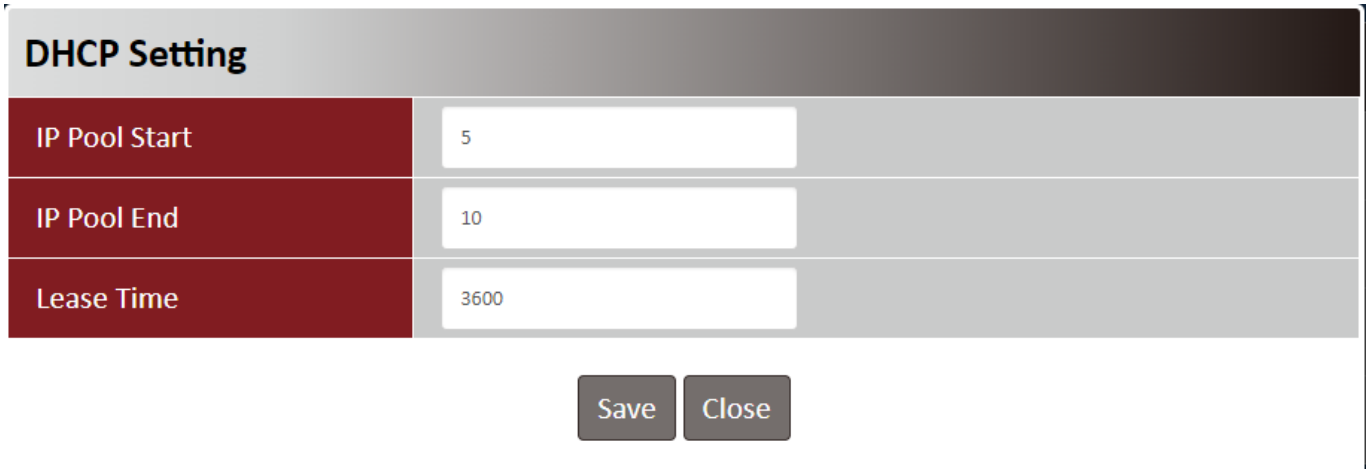


Static IP Configuration		
Item	**Value setting**	**Description**
IP	1. IPv4 format. 2. A Must-fill setting	The Static IP Address setting of this unit.
Subnet Mask	255.255.255.0 (/24) is set by default	The Subnet Mask of this configured static IP.
Default Gateway	1. IPv4 format. 2. An Optional setting	The gateway setting of this configured static IP.
Primary DNS	1. IPv4 format. 2. An Optional setting	Assigned DNS server of this configured static IP.
Secondary DNS	1. IPv4 format. 2. An Optional setting	Assigned DNS server of this configured static IP.

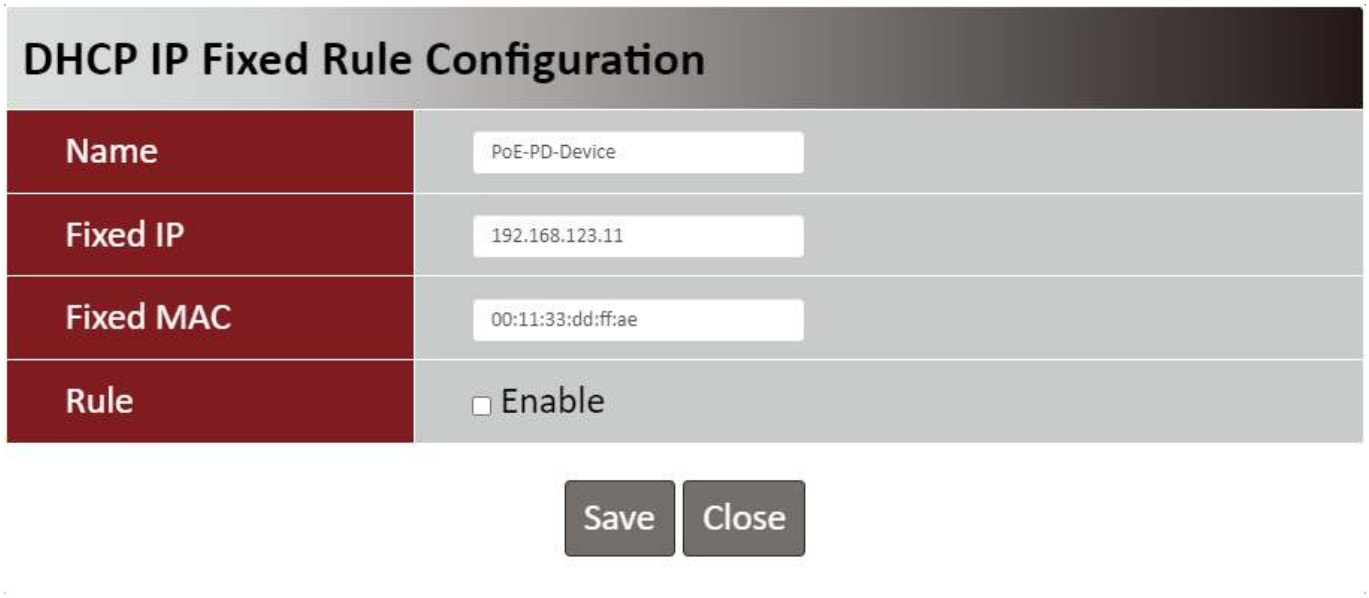
3.1.3 Ethernet



Ethernet IP		
Item	**Value setting**	**Description**
IP	1. IPv4 format. 2. A Must-fill setting	The LAN IP Address of this unit.
Netmask	255.255.255.0 (/24) is set by default	The Subnet Mask of this unit.
DHCP Server	The box is unchecked by default.	Click **Enable** box to activate DHCP Server.
DHCP Setting	N/A	Click **DHCP Config** button to pop-up the **DHCP Setting** page.



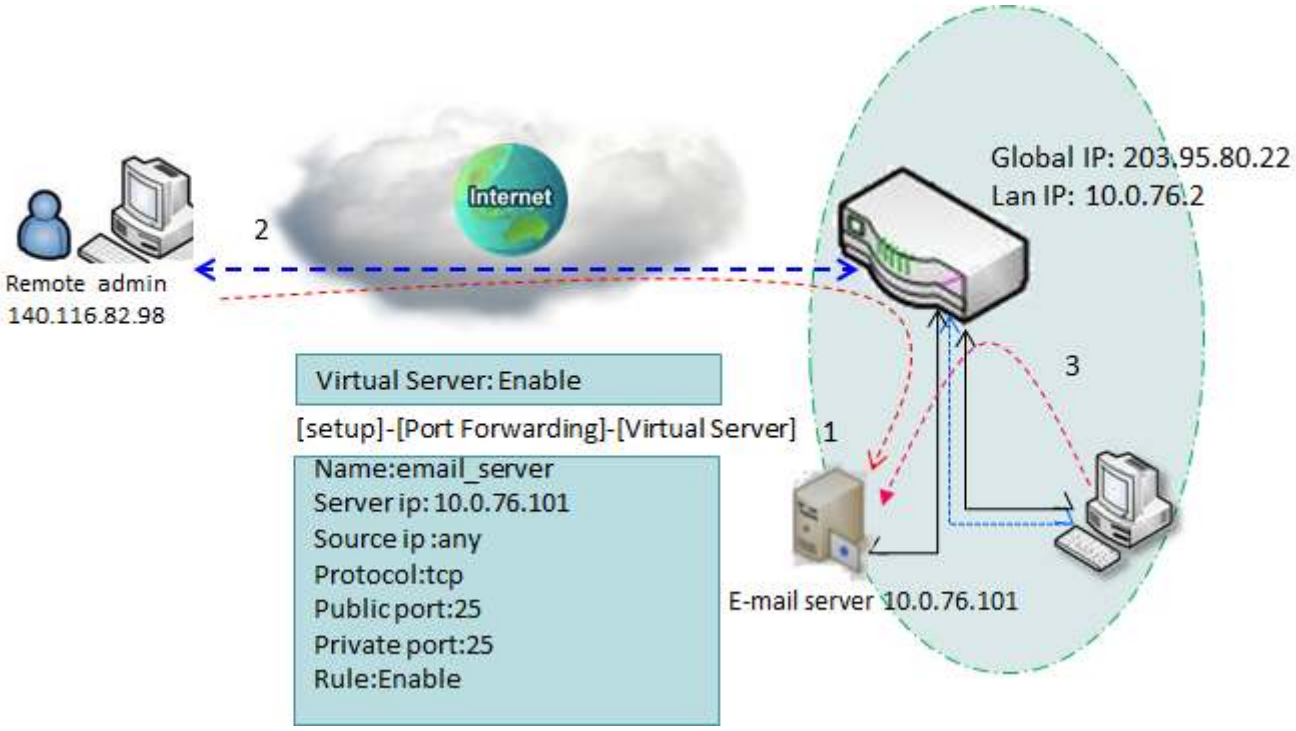
DHCP Setting		
Item	**Value setting**	**Description**
IP Pool Start	1. Numberic string format. 2. A Must-fill setting	The IP Pool of this DHCP Server. It is Starting Address entered in this field.
IP Pool End	1. Numberic string format. 2. A Must-fill setting	The IP Pool of this DHCP Server. It is Ending Address entered in this field.
Lease Time	1. Numberic string format. 2. A Must-fill setting	The Lease Time of this DHCP Server. ***Value Range*:** 300 ~ 604800 seconds.



DHCP IP Fixed Mapping		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A must-fill setting	The name of current rule.
Fixed IP	1. IPv4 format. 2. A must-fill setting	The IP Address of this mapping rule.
Fixed MAC	1. MAC Address string format 2. A must-fill setting	The MAC Address of this mapping rule.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.

3.1.4 Port Forwarding

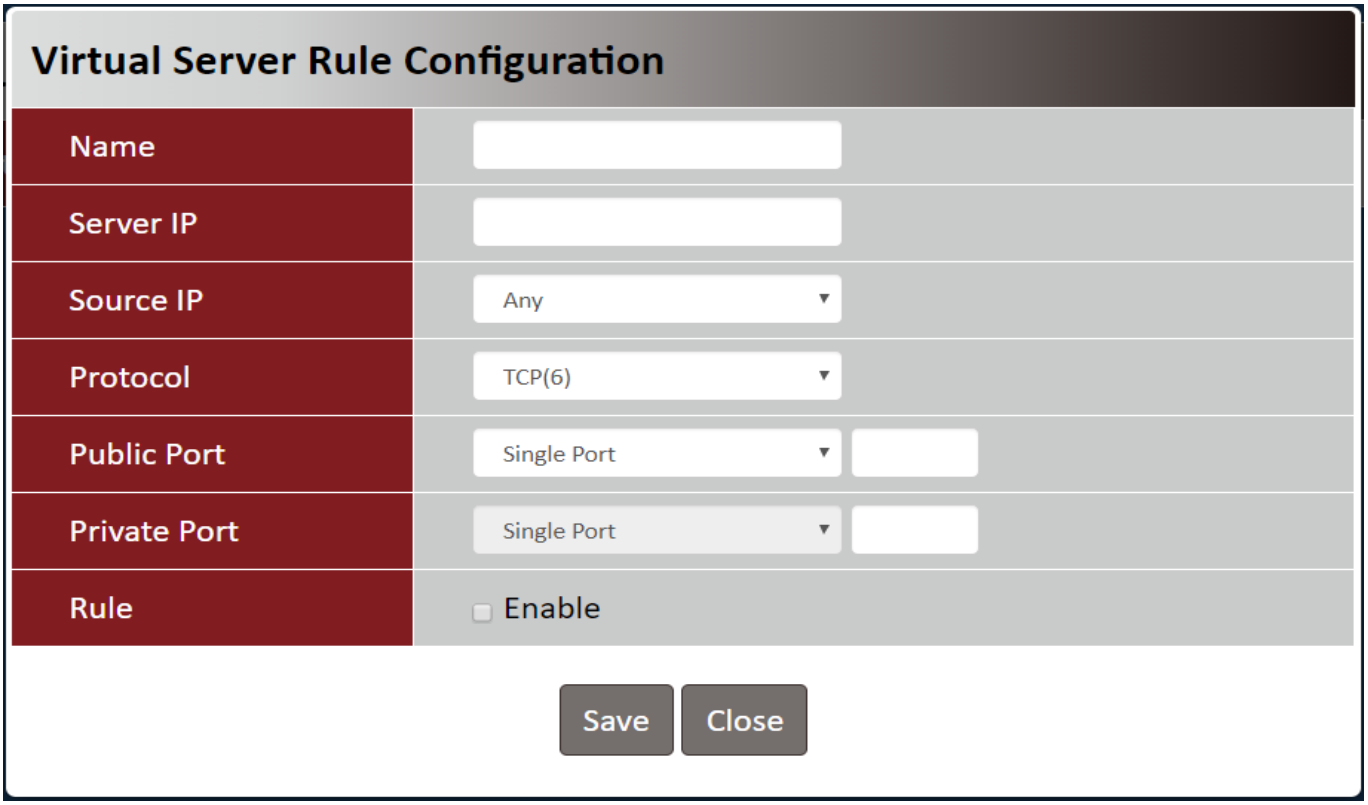
"Virtual Server" allows you to access servers with the global IP address of the gateway as if they are servers existing on the Internet. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side.





Virtual Server

Item	Value setting	Description
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function Click Add will pop-up Virtual Server Rule Configuration page.



Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must-fill setting	The name of current rule
Server IP	A Must-fill setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Source IP	1. A Must-fill setting 2. By default **Any** is selected	This field is to specify the **Source IP address**. Select **Any** to allow the access coming from any IP addresses. Select **Specific IP Address** to allow the access coming from an IP address. Select **IP Range** to allow the access coming from a specified range of IP address.
Protocol	A Must-fill setting	When **"TCP(6)"** is selected It means the option "Protocol" of packet filter rule is TCP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*:1 ~ 65535 for Public Port, Private Port. When **"UDP(17)"** is selected

		It means the option “Protocol” of packet filter rule is UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*:1 ~ 65535 for Public Port, Private Port. When **“TCP(6)& UDP(17)”** is selected It means the option “Protocol” of packet filter rule is TCP and UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*:1 ~ 65535 for Public Port, Private Port. When **“User-defined”** is selected It means the option “Protocol” of packet filter rule is User-defined. For **Protocol Number**, enter a port number.
Rule	1. An optional setting 2.The box is unchecked by default.	Check the Enable box to activate the rule.

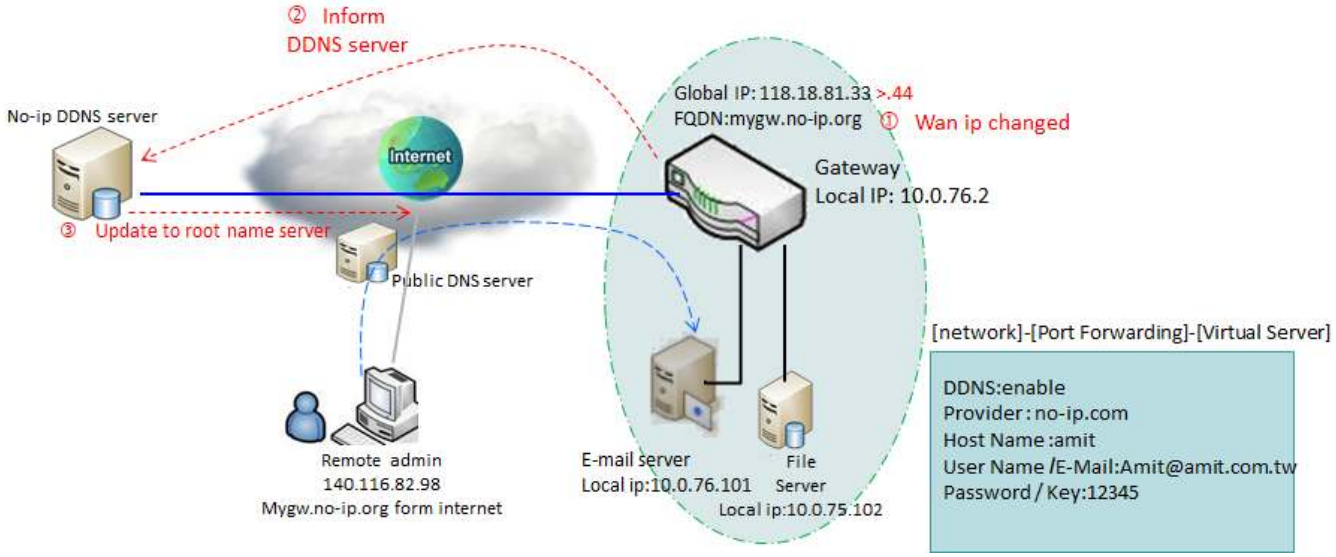


Virtual Server – Rule Name		
Item	**Value setting**	**Description**
Rule name	N/A	Click “**Edit**” button to pop-up **Virtual Server Rule Configuration** page to edit the rule. Click “**Delete**” button to delete this rule

3.1.5 DDNS

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.

DDNS **Scenario**





DDNS		
Item	**Value setting**	**Description**
DDNS	The box is unchecked by default	Check the **Enable** box to activate this function.
Provider	**DynDNS.org** is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org**, **NO-IP.com**,**TZO.com** etc...
Host Name	1. String format can be any text 2. A Must-fill setting	Your registered host name of DDNS Service. ***Value Range***:0 ~ 63 characters.
User Name / E-Mail	1. String format can be any text	Enter your User name or E-mail addresss ofDDNS Service.

	2. A Must-fill setting	
Password / Key	1. String format can be any text 2. A Must-fill setting	Enter your Password or Key ofDDNS Service.

3.1.6 PoE



PoE Port Definition		
Item	**Value setting**	**Description**
Port	The box is unchecked by default	Check the **Edit** box to activate Poe function.



PoE Port Definition		
Item	**Value setting**	**Description**
PD Ping Check	The box is unchecked (**Disable**) by default	Check the **Enable** box to activate PD Ping Check function. In addition to enable the function, you have to specify a timeout value for timeout check. ***Value Range***: 10 ~ 300 seconds.
PD No-response Action	**No Action** by default	Specify the the action to take when the PD doesn't reply the Ping check activity. (PD No-response). It could be **No Action** or **Power off/on**. Select **Power off/on** to restart the PD device, if required.
Time schedule	**Select one** is set by default	if you have set other schedule rules, there will be other options to select.

Enable	The box is unchecked by default	Check the **Enable** box to activate Poe function.

3.2 Routing



Routing		
Item	**Value setting**	**Description**
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function.
Routing Information	N/A	The routing information allows user to view the routing table and policy routing information.

3.2.1 Static Routing

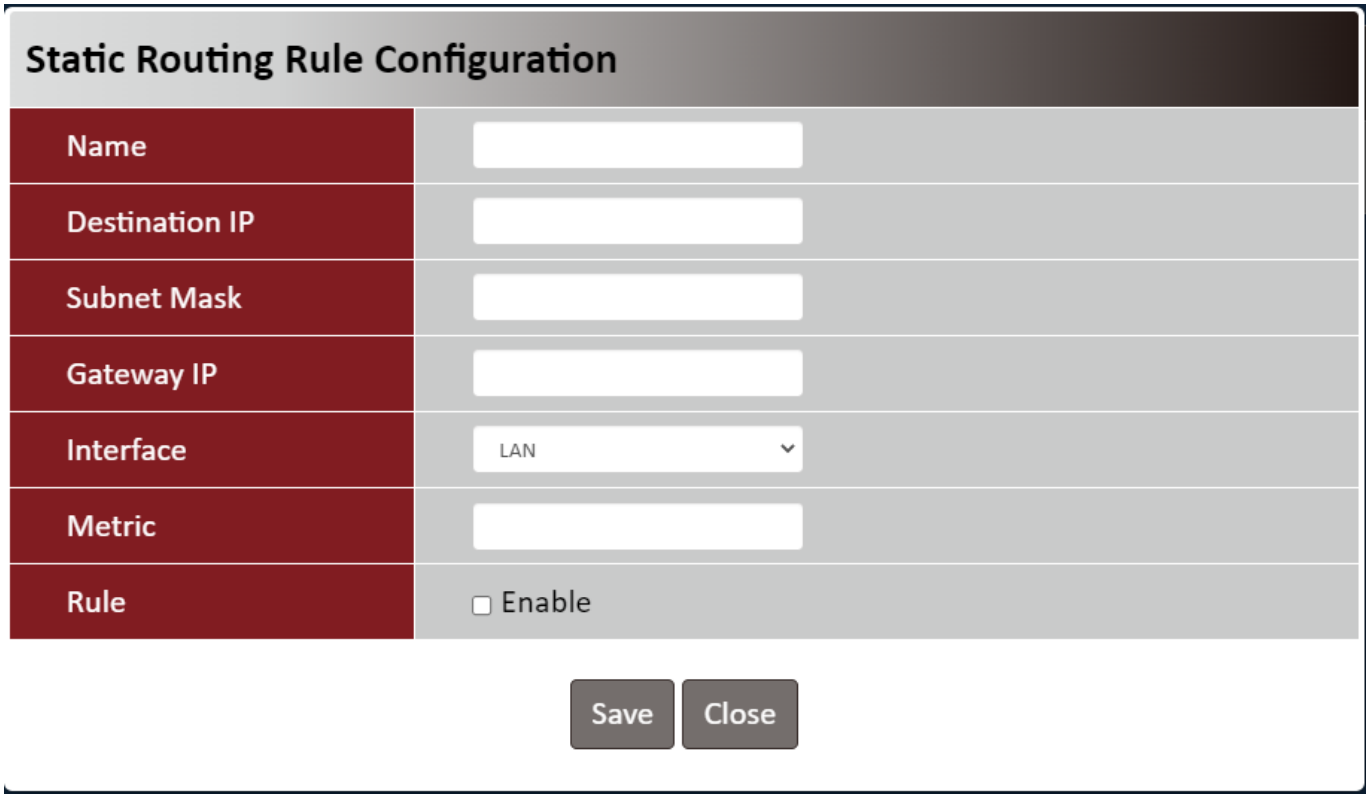
"Static Routing" function lets you define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the gateway. The gateway routes incoming packets to different peer gateways based on the routing table. You need to define the static routing information in gateway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

.

As shown in the diagram, when the destination is Google access, rule 1 set interface as Cellular, routing gateway as ISP gateway 192.168.121.253. All the packets to Google will go through WAN-1.



Static Routing		
Item	**Value setting**	**Description**
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function. Click Add will pop-up Static Routing Rule Configuration page.

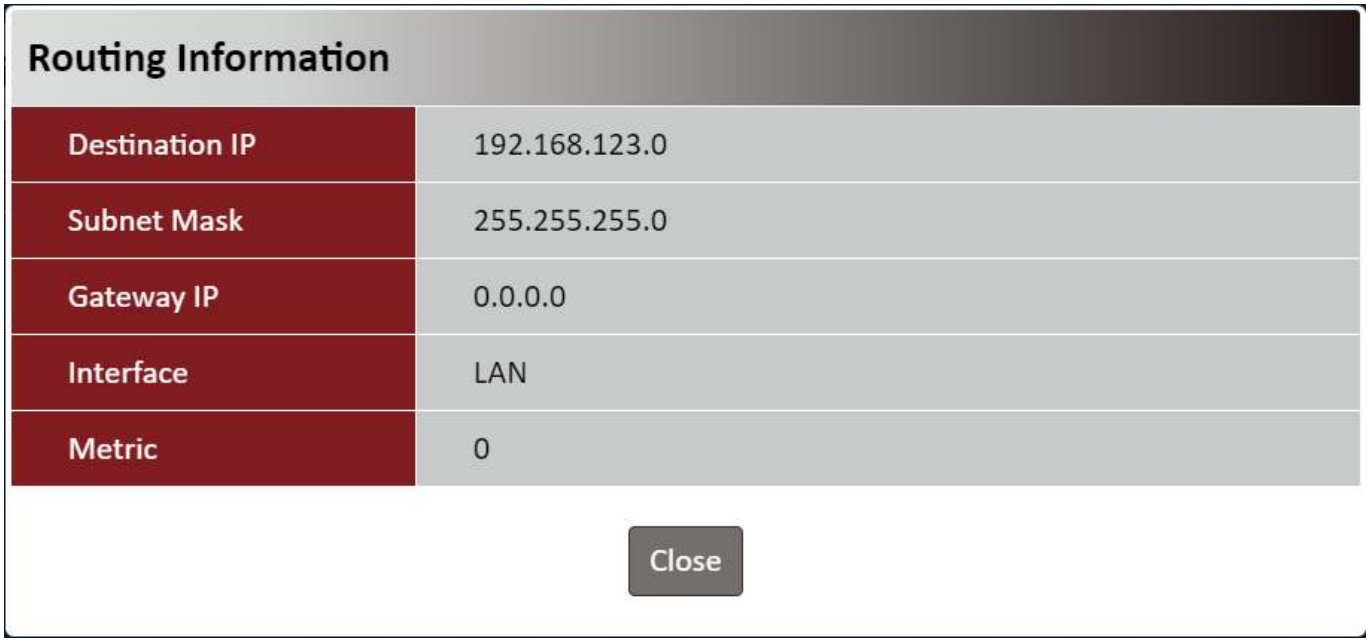


Static Routing Rule Configuration		
Item	**Value setting**	**Description**
Name	The box is unchecked by default	Check the **Enable** box to activate this function. Click Add will pop-up Static Routing Rule Configuration page.
Destination IP	1. IPv4 Format 2. A Must-fill setting	Specify the Destination IP of this static routing rule.
Subnet Mask	1.255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A Must-fill setting	Specify the Gateway IP of this static routing rule.
Interface	Lan is set by default	Select the Interface of this static routing rule. use the available WAN / LAN interfaces.
Metric	1. Numberic String Format 2. A Must-fill setting	The Metric of this static routing rule. Value Range: 0 ~ 255.
Rule	The box is unchecked by default.	Click the **Enable** to activate static routing functions.

3.2.2 Routing Information

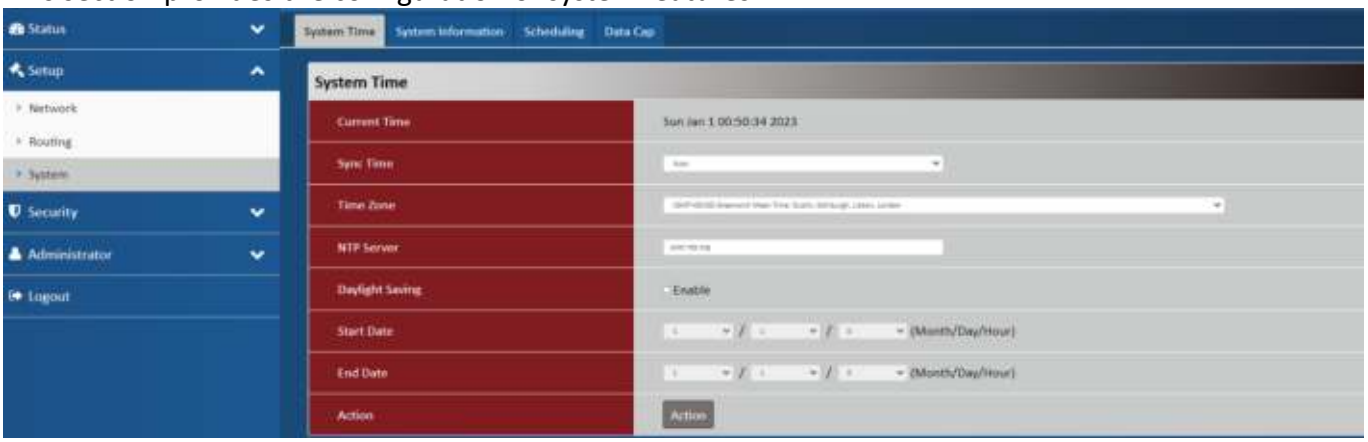


Routing Information		
Item	Value setting	Description
192.168.123.0	192.168.123.0 by default	Show default routing and static routing rule list

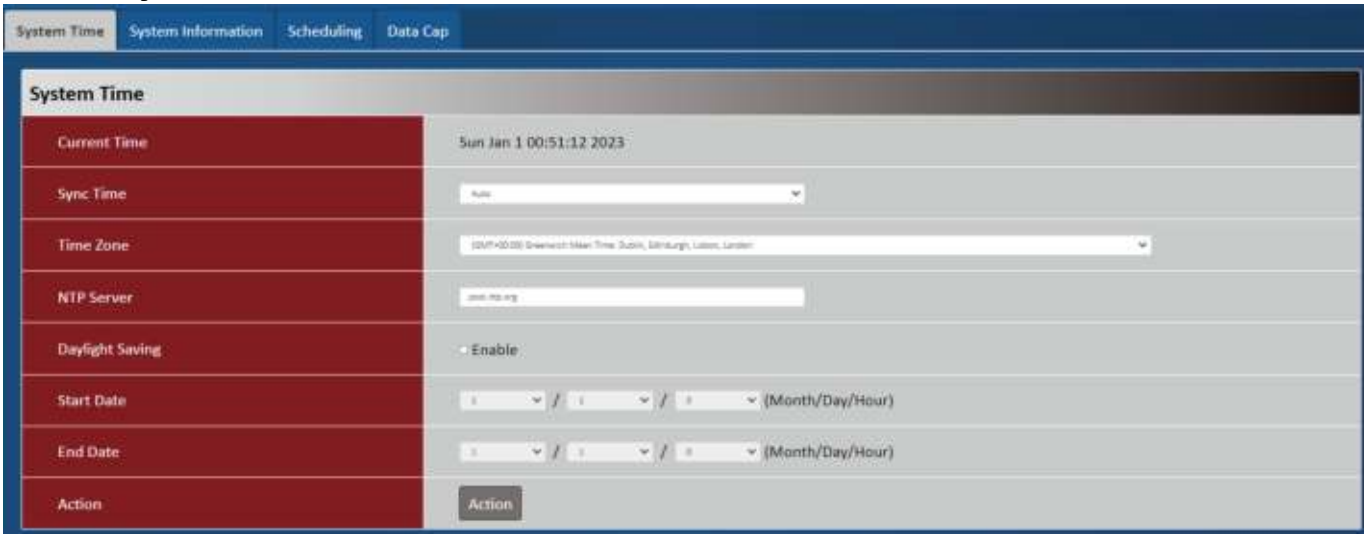


3.3 System

This section provides the configuration of system features.

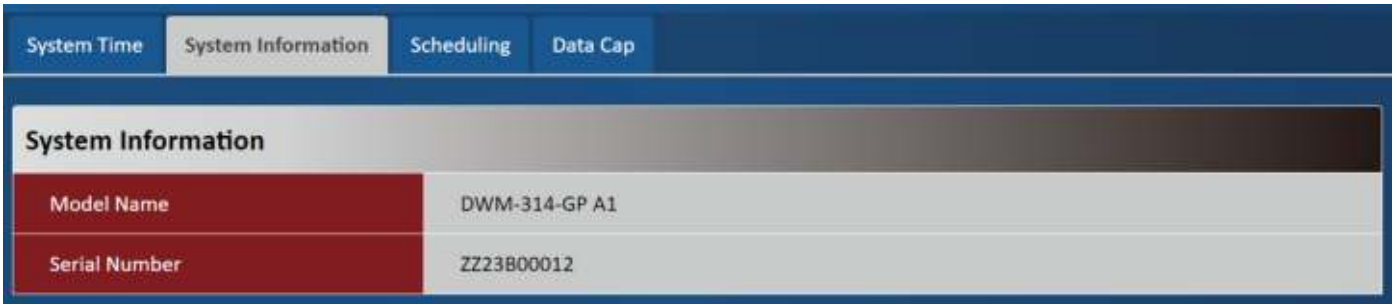


3.3.1 System Time



System Time		
Item	**Value setting**	**Description**
Current Time	N/A	Show the current time of the unit.
Sync Time	1. A Must-fill item. 2. **Auto** is selected by default.	When select **Auto**, unit will sync the time via cellular cell, and then try to use NTP if cellular cell doesn't provide time information. When select **NTP**, the unit will sync time via NTP service.
Time Zone	1. A Must-fill item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
NTP Server	1. A Must-fill item.	Indicates which NTP server will be used of the time synchronization.
Daylight Saving	1. It is an optional item. 2. Unchecked by default	Check the **Enable** button to activate the daylight saving function. When user enabled this function, user has to specify the **Start Date** and **End Date** for the daylight saving time duration.
Start Date	1. It is an optional item.	Start time for Daylight Saving.
End Date	1. It is an optional item.	End Time of Daylight Saving.
Action	N/A	Click **Action** to sync time immediately

3.3.2 System Information

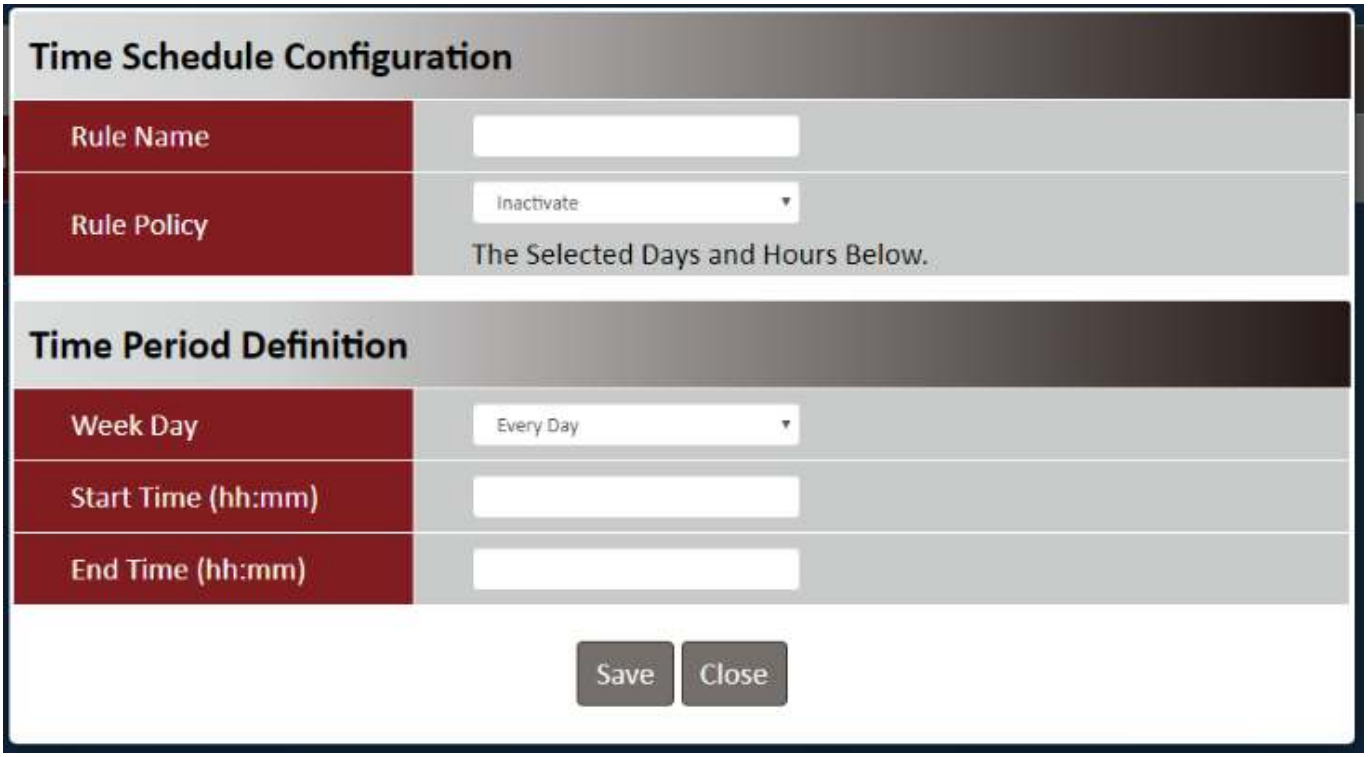


System Information		
Item	**Value setting**	**Description**
Model Name	DWM-314-GP	Show the model name of the device

3.3.3 Scheduling



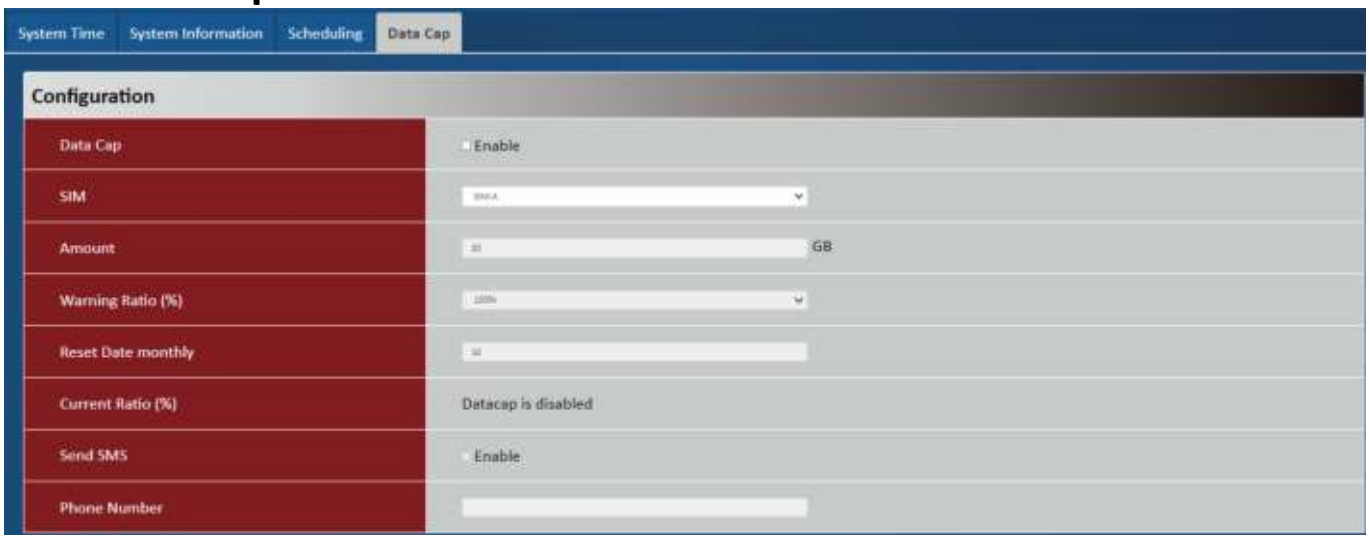
Scheduling		
Item	**Value setting**	**Description**
Time Schedule	N/A	Press **Add** to create a schedule rule for system.



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

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday

3.3.4 Data Cap



Configuration		
Item	**Value Setting**	**Description**
Data Cap	Unchecked by default.	Check the **Enable** box to activate the Data cap function.
SIM	**SIM A** by default.	Specify SIMA or SIMB
Amount	1. An Optional setting.	Specify the allowable data limitation for the defined cycle period
Warning Ration(%)	**100%** by default.	Send a notification when a set condition is met
Reset Date monthly	1.10by default. 2. An Optional setting.	Specify a certain day of each month as the periodic execution of reset data
Current Ratio(%)	0 by default	
Send SMS	unchecked by default.	Check the **Enable** box to activate the connection restriction function.
Phone Number	1. An Optional setting.	When send sms is Enable, can Set the sending SMS object

Chapter 4 Security



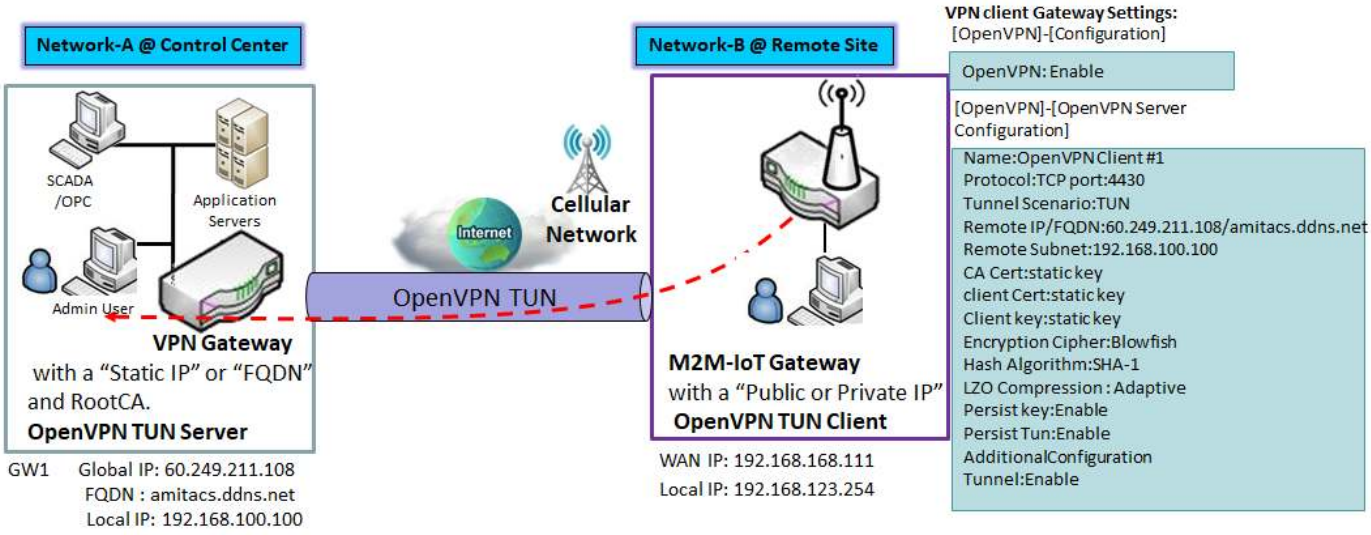
4.1 VPN



VPN Page		
Item	Value setting	Description
Openvpn	N/A	The OpenVPN setting allows user to create and configure OpenVPN tunnels.
WireGuard	N/A	The WireGuard setting allows user to create and configure WireGuard tunnels.

4.1.1 OpenVPN

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.OpenVPN Tun Scenario

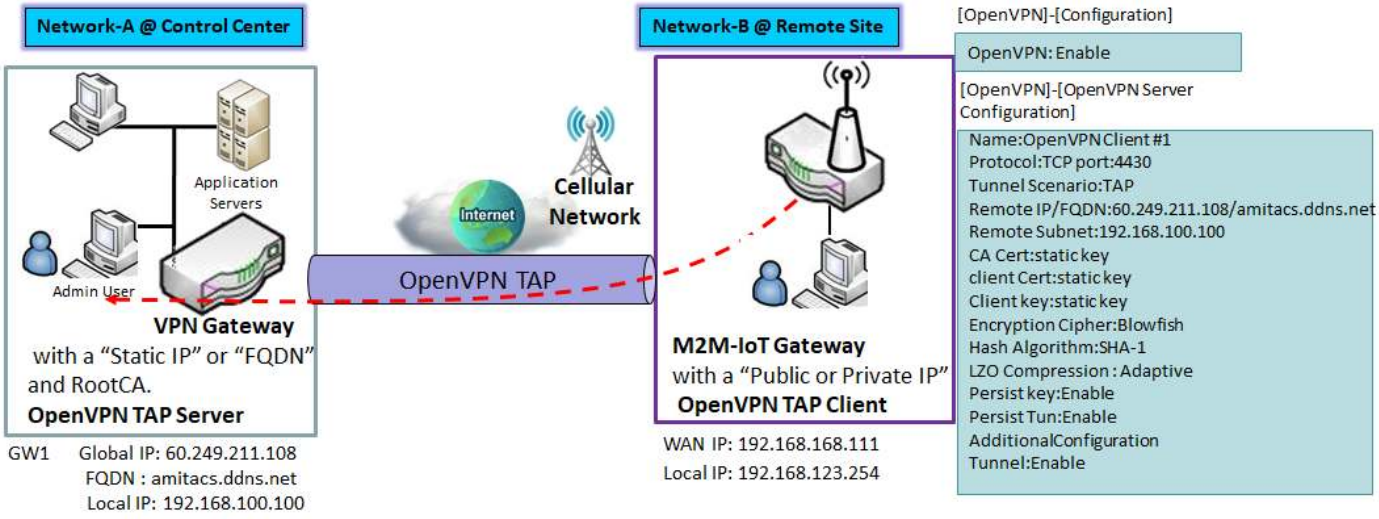


As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an OpenVPN TUN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which is belong to a virtual subnet that is different to the local subnet in Control Center.

OpenVPN Tap Scenario

If you want to offer remote access to the entire remote LAN for VPN client(s), you have to setup OpenVPN

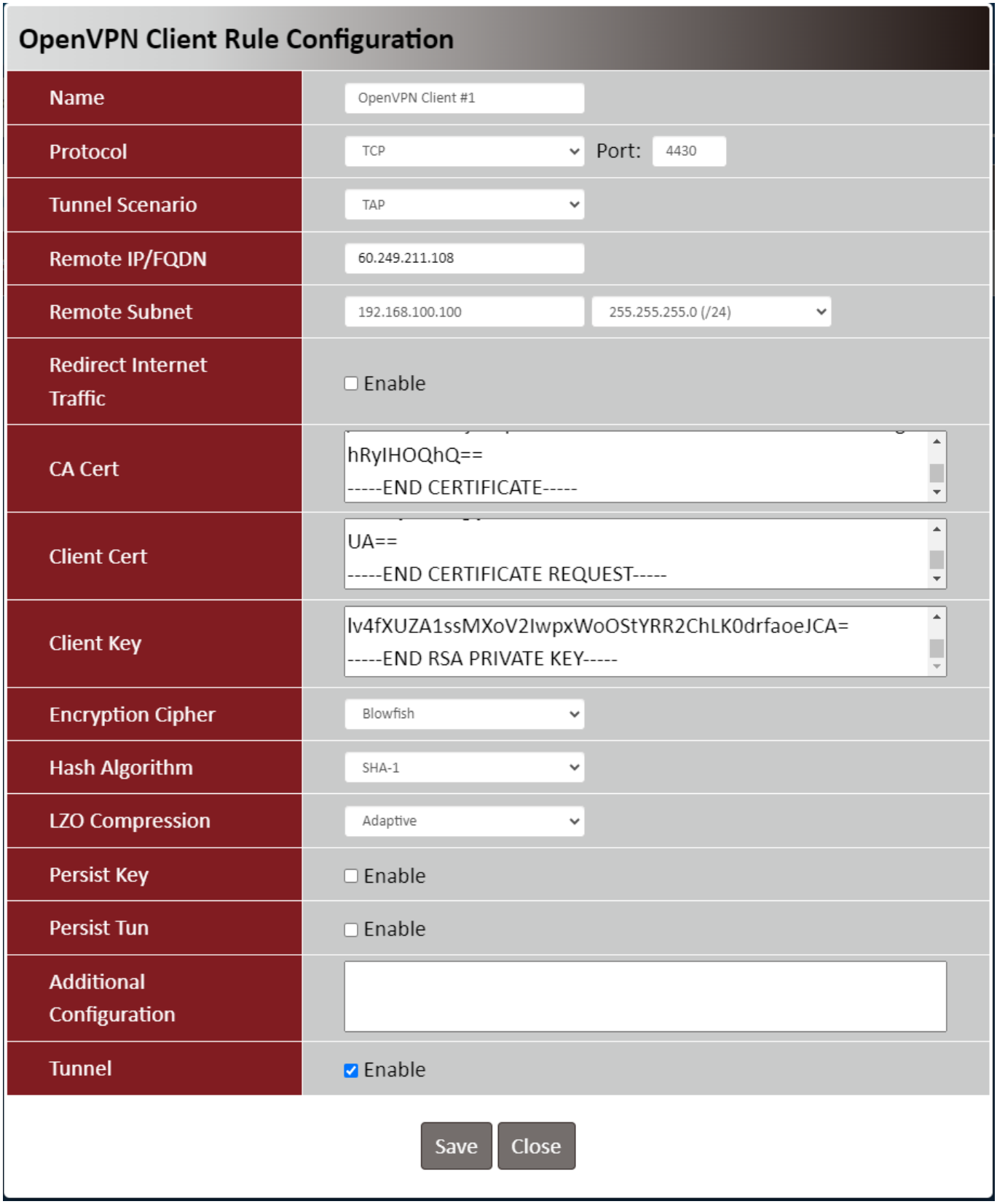
in “TAP” bridge mode.



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 the same subnet as that of local subnet in Control Center.

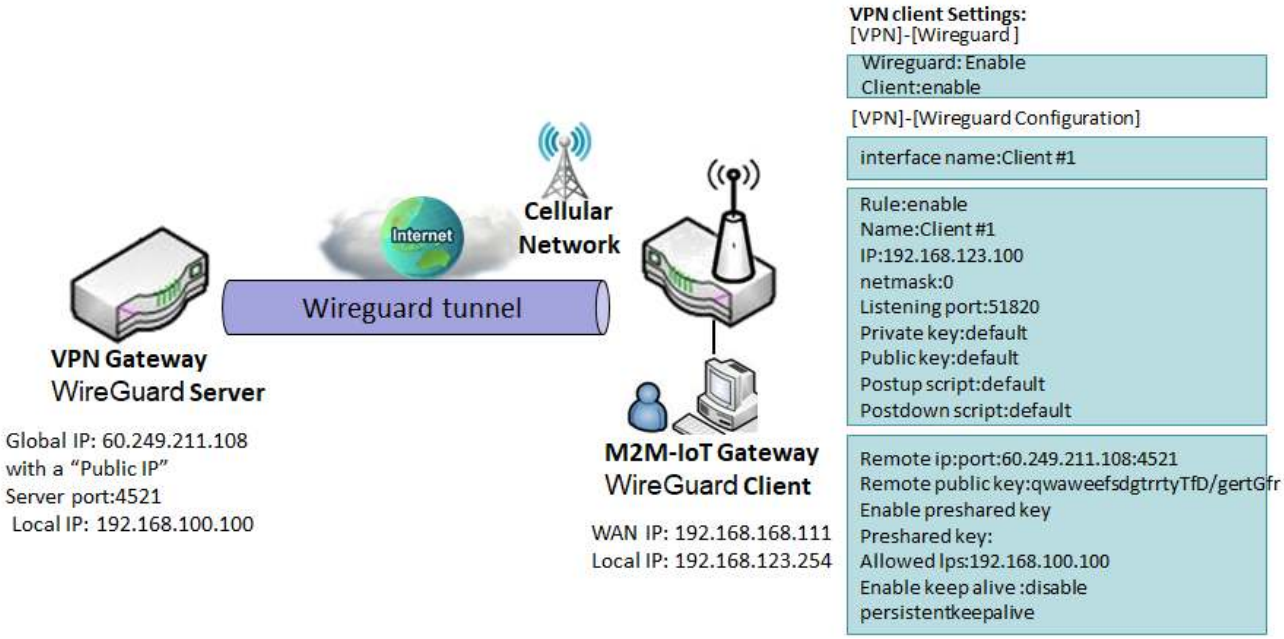


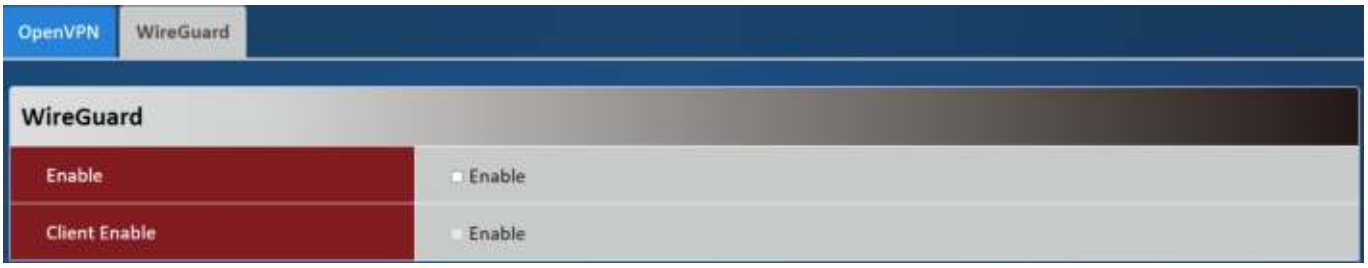
OpenVPN client configuration Page		
Item	**Value setting**	**Description**
Openvpn client	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function Click Add will pop-up OpenVPN Client Rule Configuration page.


OpenVPN Client Rule Configuration
Name
OpenVPN Client #1
Protocol
TCP
Port:
4430
Tunnel Scenario
TAP
Remote IP/FQDN
60.249.211.108
Remote Subnet
192.168.100.100
255.255.255.0 (/24)
Redirect Internet Traffic
Enable
CA Cert
hRyIHOQhQ==
-----END CERTIFICATE-----
Client Cert
UA==
-----END CERTIFICATE REQUEST-----
Client Key
lv4fXUZA1ssMXoV2IwpxWoOStYRR2ChLK0drfaoeJCA=
-----END RSA PRIVATE KEY-----
Encryption Cipher
Blowfish
Hash Algorithm
SHA-1
LZO Compression
Adaptive
Persist Key
Enable
Persist Tun
Enable
Additional Configuration
Tunnel
Enable
Save
Close

OpenVPN Client Rule Configuration Page		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must-fill setting	The name of current rule
Protocol	1. A Must-fill setting By default **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or UDP** -> The TCP protocol will be used to access the OpenVPN Server, and **Port** will be set as 4430 automatically. • Select **UDP** -> The UDP protocol will be used to access the OpenVPN Server, and **Port** will be set as 1194 automatically.
Tunnel Scenario	1. A Must-fill setting By default 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.
Remote IP/FQDN	A Must-fill setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate remote subnet function, and 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. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Internet Traffic** function.
CA Cert	A Must-fill setting	Paste the CA Cert static key
client Cert	A Must-fill setting	Paste the **client Cert** static key
Client key	A Must-fill setting	Paste the **Client key** static key
Encryption Cipher	1. A Must-fill setting. 2. By default **Blowfish** is selected.	Specify the **Encryption Cipher** from the dropdown list. It can be Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm** from the dropdown list. It can beSHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.
LZO Compression	By default **Adaptive** is	Specify the **LZO Compression** scheme.
Persist key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persist Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Additional Configuration	1. An Optional setting. 2. String format: any text	Specify the **Additional Configuration.**
Tunnel	The box is unchecked by default.	Click the **Enable** to activate OpenVPN functions.

4.1.2 WireGuard





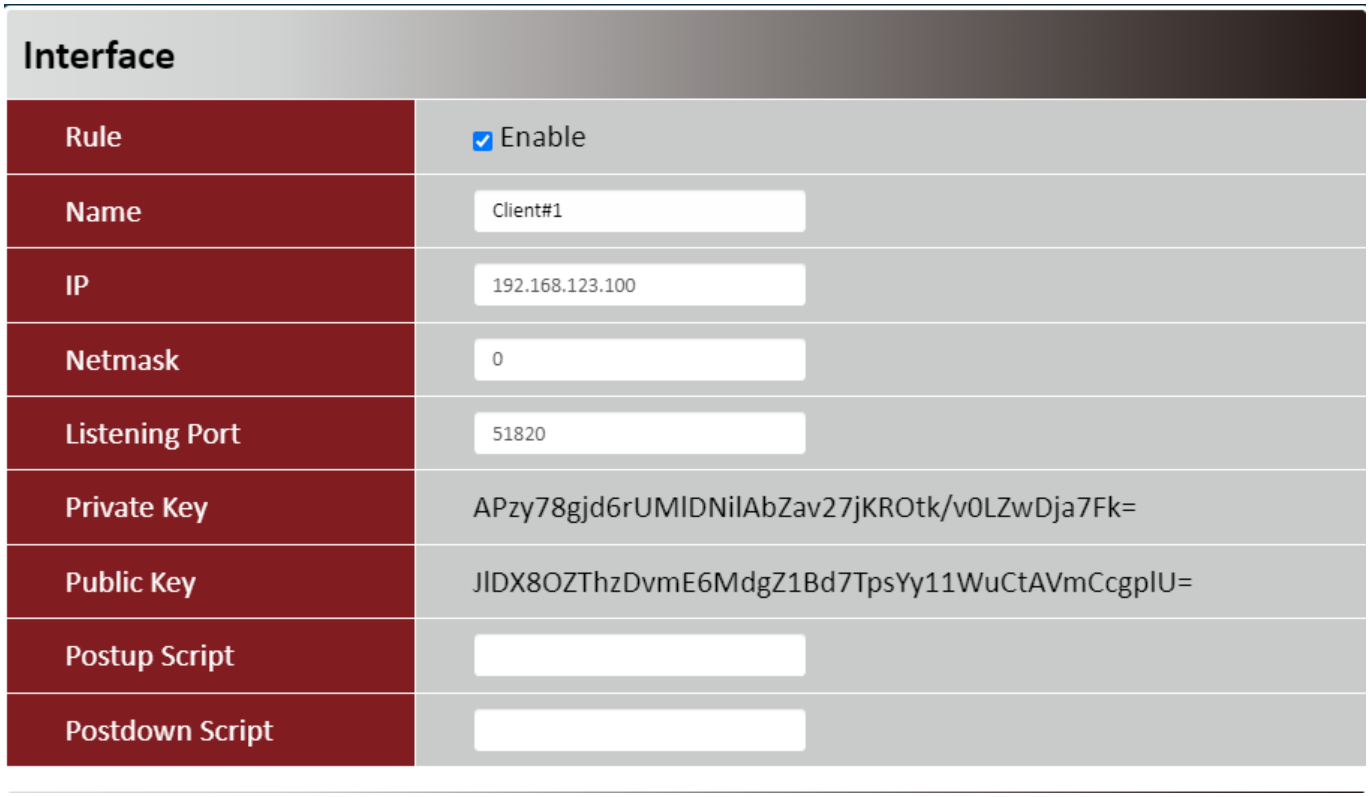
WireGuard Page		
Item	**Value setting**	**Description**
Enable	The box is unchecked by default	Check the **Enable** box to activate this WireGuard function
Client enable	The box is unchecked by default	Check the **Enable** box to activate this client function Click **Add** will pop-up **Interface** page



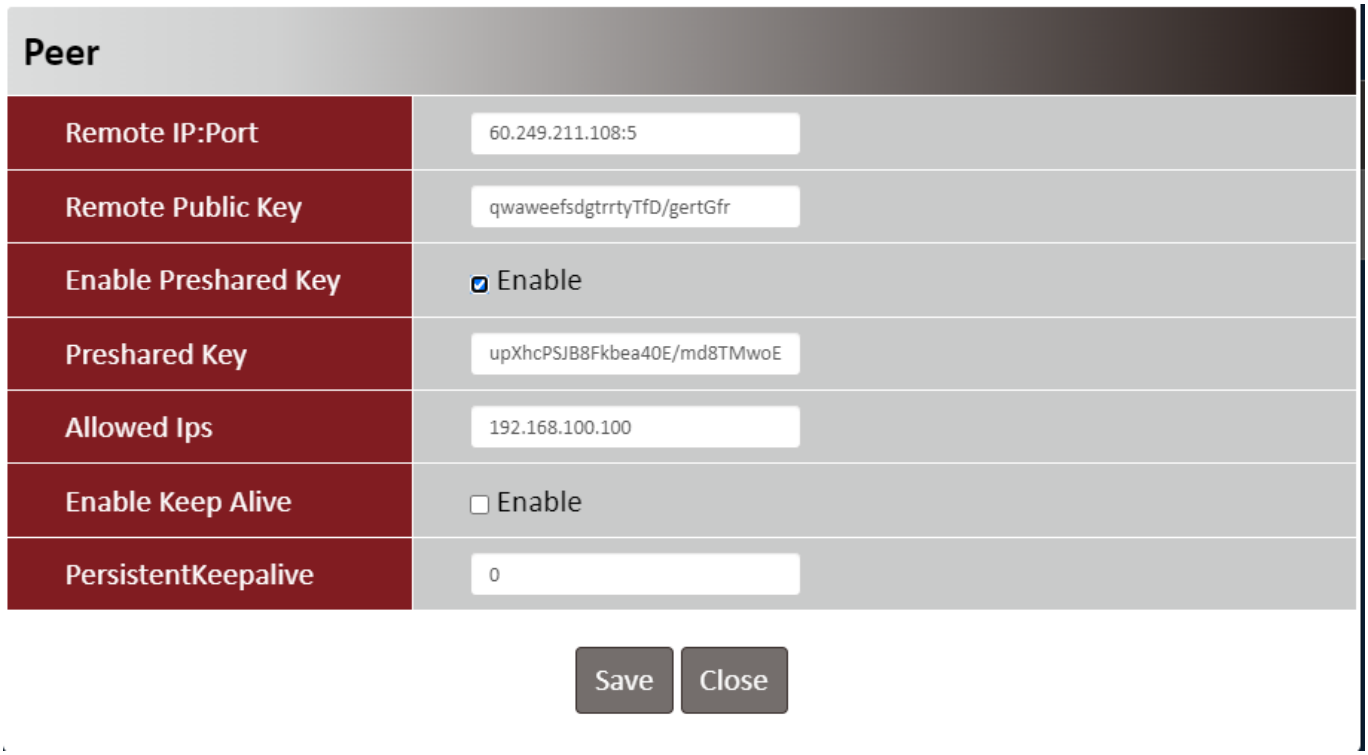
interface Page		
Item	**Value setting**	**Description**
name	A Must-fill setting	Specify a name as the identifier of the client.



Rule Page		
Item	Value setting	Description
Name	N/A	Check the **Edit** box to activate this WireGuard function Check the **Delete** box to delete Rule

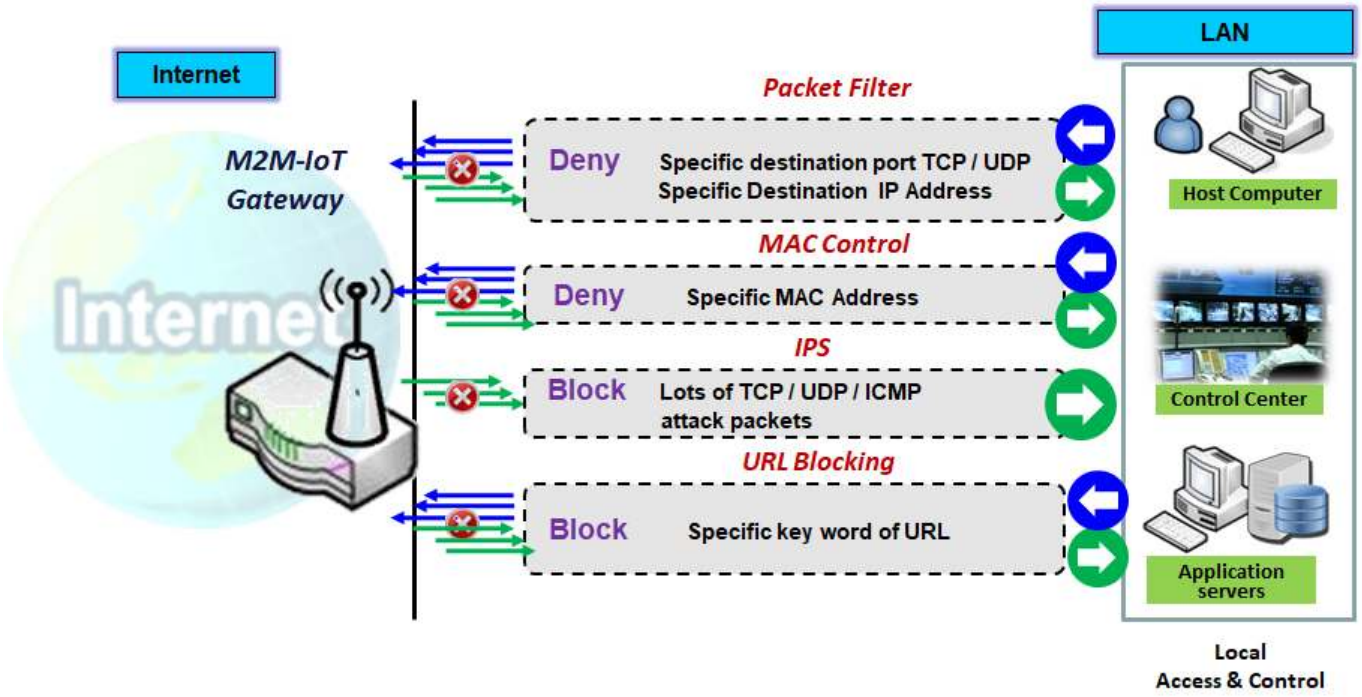


Interface Page		
Item	Value setting	Description
Rule	The box is unchecked by default	Check the **Enable** box to activate this WireGuard function
Name	A Must-fill setting.	Specify a name as the identifier of the client.
IP	A Must-fill setting.	Specify the server IP.
Netmask	0 by default	Specify the Netmask setting for the WireGuard server
Listening Port	51820 by default	Indicate the listening port of UDP connection.
Private Key	N/A	randomly generate client Private key
Public Key	N/A	randomly generate server Public key
Postup script	Blank is set by default	When the VPN service starts, the instructions to be executed are required
Postdown script	Blank is set by default	When the VPN service starts, the instructions to be executed are required

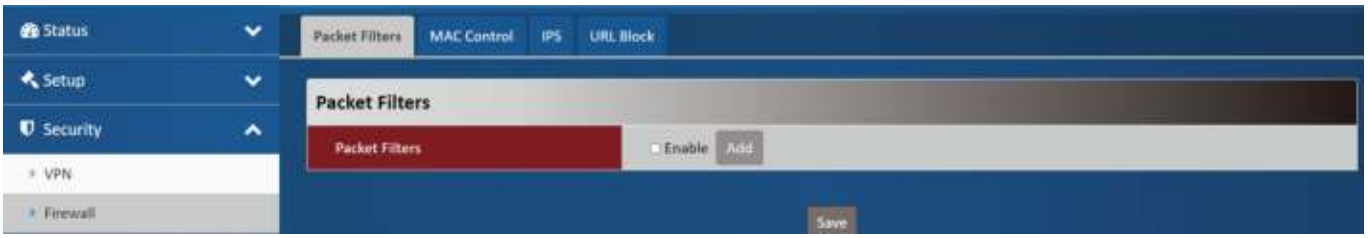


peer Page		
Item	**Value setting**	**Description**
Remote IP :Port	A Must-fill setting.	Specify the remote IP and port
Remote Public key	A Must-fill setting.	Specify the server public key
Enable Preshared key	The box is unchecked by default	Check the **Enable** box to activate this **Preshared key** function
Preshared key	N/A	randomly generate Preshared key
Allowed IPs	Blank is set by default	server LAN network segment
Enable keep Alive	The box is unchecked by default	Check the **Enable** box to activate this **keep Alive** function
Persistent keep alive	0 by default	Set connection confirmation interval

4.2 Firewall



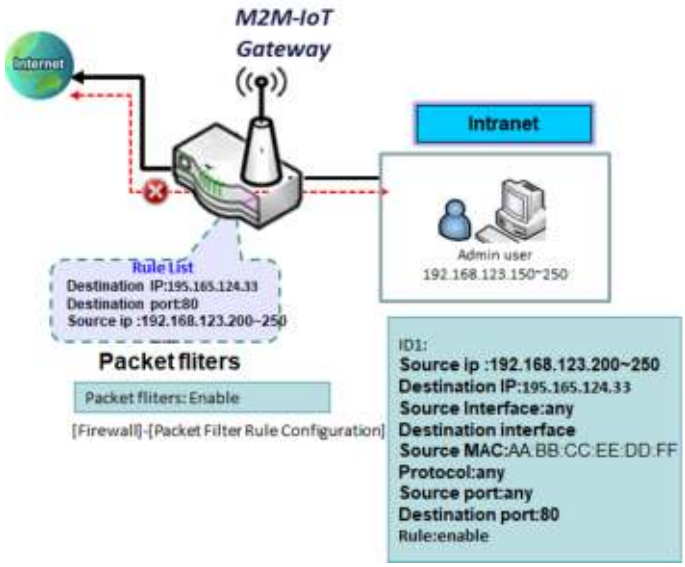
The firewall functions include Packet Filter, URL Blocking, MAC Control, IPS and some firewall options.



4.2.1 Packet Filters

"Packet Filter" function can let you define some filtering rules for incoming and outgoing packets. So the gateway can control what packets are all blocked to 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, the time schedule to which the rule will be active

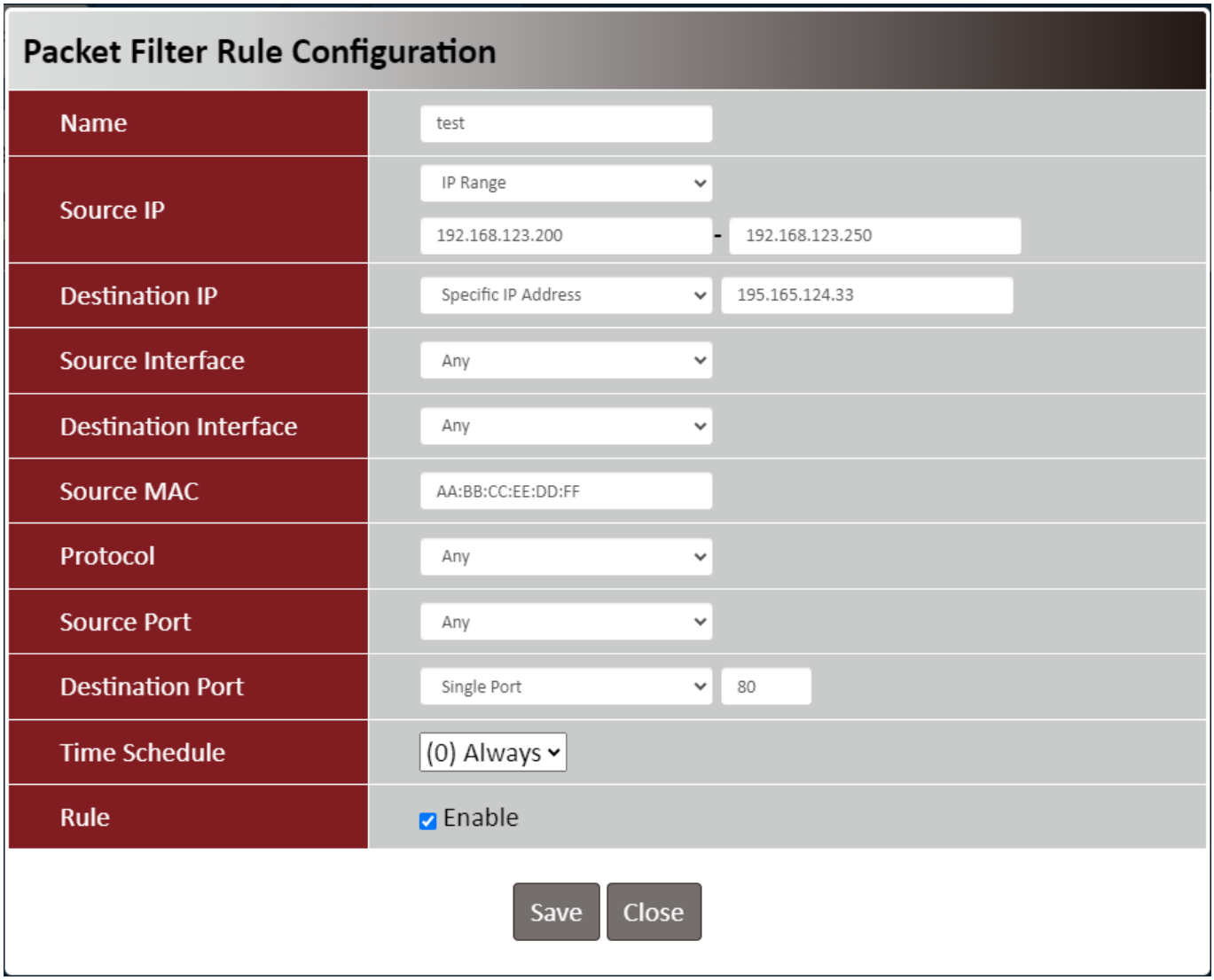
Packet Filter Scenario



As shown in the diagram, specify "Packet Filter Rule List" (block those match the following rules) and define the rules. Rule-1 is to block HTTP packets to pass, and Packets other than Rule1 let it pass through.
Under such configuration, the gateway will a block only HTTP packets, issued from the IP range 192.168.123.200 to 250



Packet Filters Page		
Item	**Value setting**	**Description**
Packet filters	The box is unchecked by default	Check the **Enable** box to activate this **Packet filter** function Click Add will pop-up Packet Filter Rule configuration page



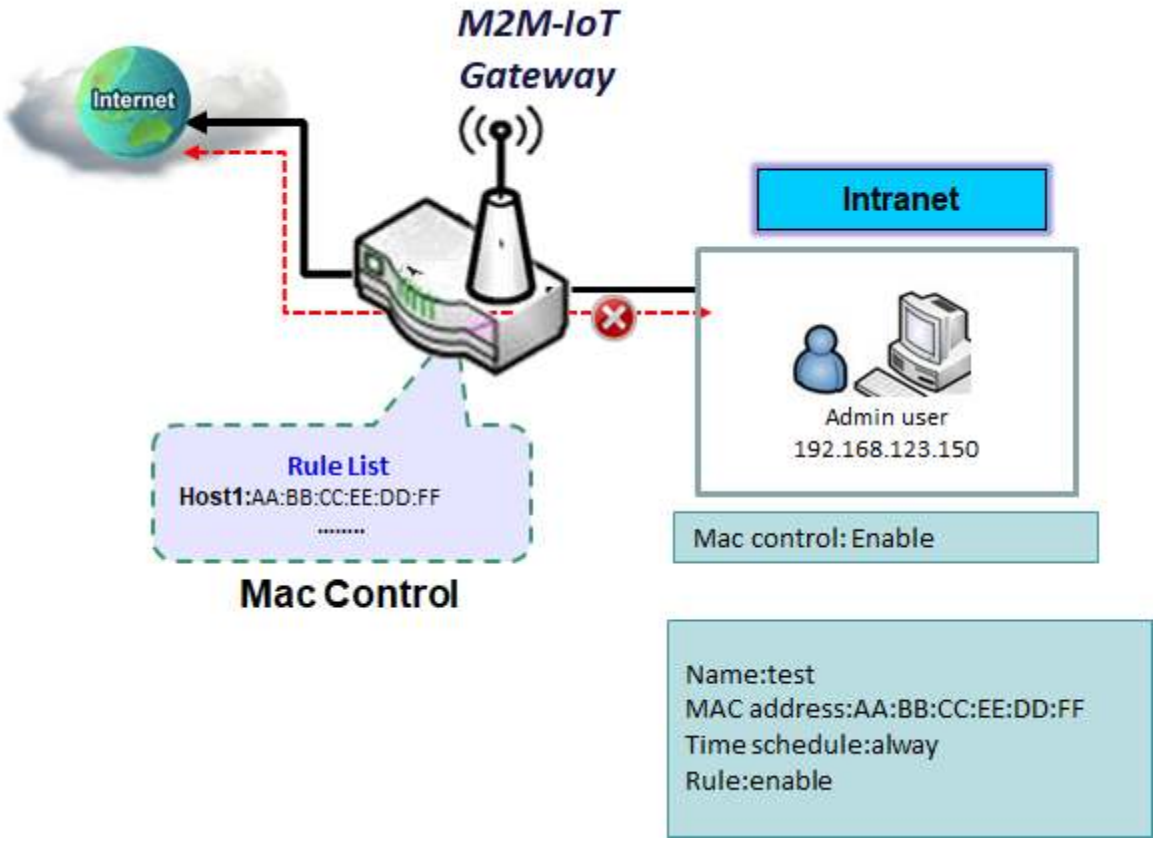
Packet Filter Rule Configuration Page		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must-fill setting	Enter a packet filter rule name. Enter a name that is easy for you to remember.
Source IP	1. A Must-fill setting 2. By default **Any** is selected	This field is 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.
Destination IP	1. A Must-fill 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.
Source Interface	1. A Must-fill 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 LANfor this field. Select **Any** to filter packets coming into the router from any interfaces.

Destination interface	1. A Must-fill 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. Select **Any** to filter packets leaving the router from any interfaces.
Source MAC	1.optional	specify the Source MAC address.
Protocol	1. A Must-fill setting 2. By default **Any** is selected	For **Protocol**, select **Any** to filter any protocol packets For **Protocol**, select **TCP** to filter tcp packets For **Protocol**, select **udp** to filter udp packets For **Protocol**, select **both** to filter both packets For **Protocol**, select **ICMP** to filter ICMP packets For **Protocol**, select **GRE** to filter **GRE** packets For **Protocol**, select **AH** to filter **AH** packets For **Protocol**, select **ESP** to filter **ESP** packets For **Protocol**, select **SCT** to filter **SCT** packets
Source port	1. A Must-fill setting 2. By default **Any** is selected	This field is to specify the **Source port**. Select **Any** to filter packets coming from any port. Select **single port** to Specify a unique port for the packets come to the port. Select **port Range** to filter packets coming from a specified range of port.
Destination port	1. A Must-fill setting 2. By default **Any** is selected	This field is to specify the **destination port**. Select **Any** to filter packets coming from any port. Select **single port** to filter a unique port for the packets come to the port. Select **port Range** to filter packets with a specified destination port range.
Time schedule	1. An optional setting 2. **(0)Always** is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0) Always.
Rule	The box is unchecked by default	Check the **Enable** box to activate this Packet Filter function

4.2.2 MAC Control

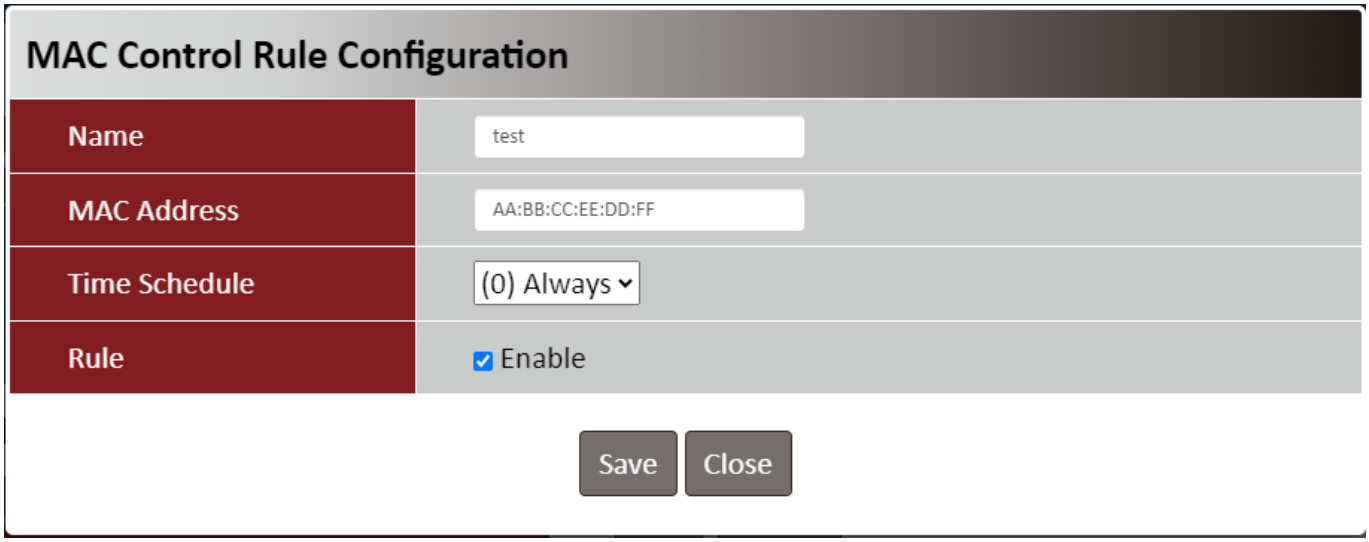
When the administrator wants to reject the traffics from some client hosts with specific MAC addresses, he can use the "MAC Control" function to reject with the black list configuration.

Mac control Scenario



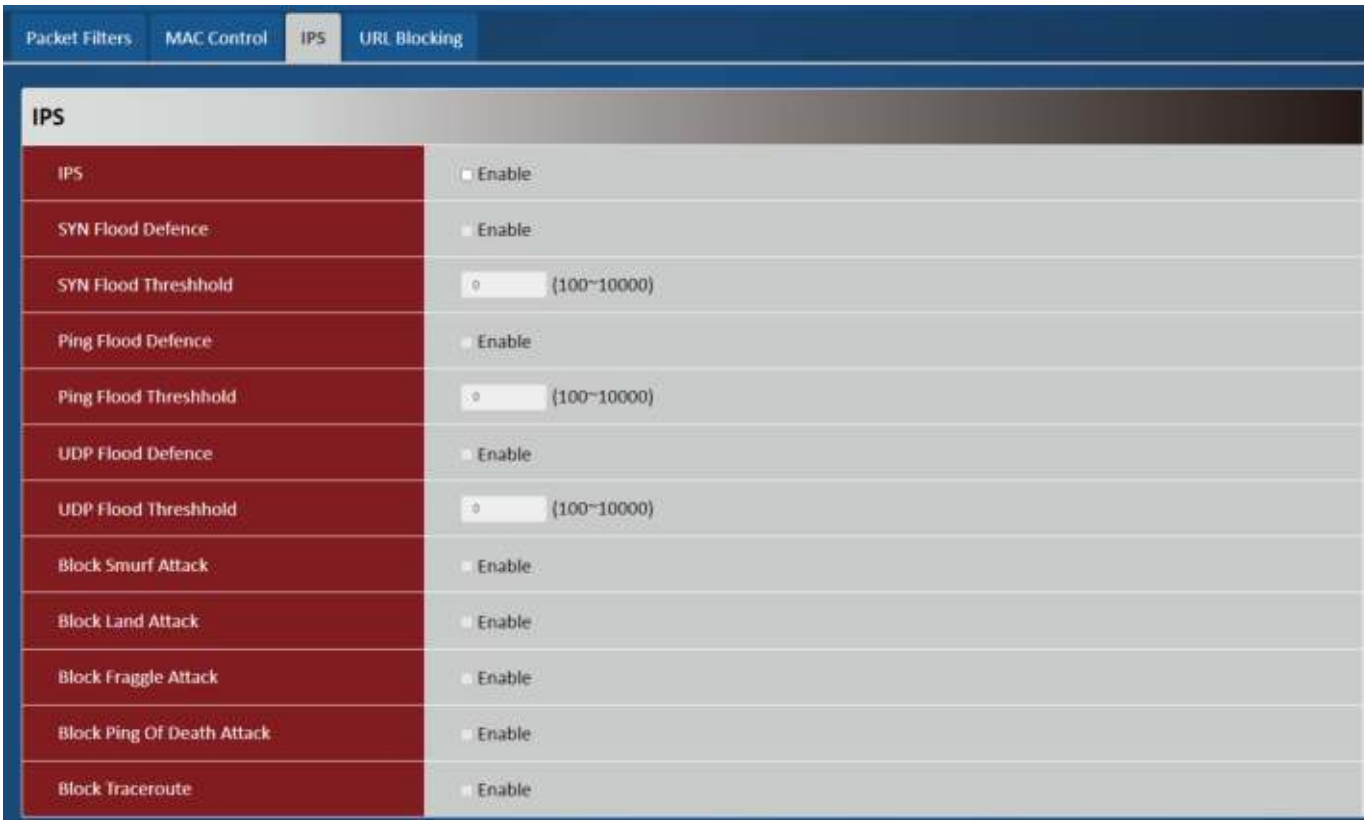


Mac Control Page		
Item	**Value setting**	**Description**
Mac control	The box is unchecked by default	Check the **Enable** box to activate this **Mac control** function Click Add will pop-up Mac control Rule configuration page



MAC Control Rule Configuration Page		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must-fill setting	Enter a mac rule name. Enter a name that is easy for you to remember.
Mac address	Blank is set by default	Specify the **Source MAC Address** to filter rule.
Time schedule	1. An Optional setting 2. **(0)Always** is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0) Always.
Rule	The box is unchecked by default	Check the **Enable** box to activate this **Mac control** function

4.2.3 IPS



IPS Page		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Check the **Enable** box to activate this IPS function
SYN Flood Defense	The box is unchecked by default	Check the **Enable** box to activate this SYN Flood Defense function
SYN Flood Threshold	1. A must-fill setting 2. Traffic threshold is set to 0 by default 3. The value range can be from 100 to 10000.	Specify the value range to block
Ping Flood Defense	The box is unchecked by default	Check the **Enable** box to activate this Ping Flood Defense function
Ping Flood Threshold	1. A must-fill setting 2. Traffic threshold is set to 0 by default 3. The value range can be from 100 to 10000.	Specify the value range to block
UDP Flood Defense	The box is unchecked by default	Check the **Enable** box to activate this UDP Flood Defense function
UDP Flood Threshold	1. A Must-fill setting 2. Traffic threshold is set to 0 by default 3. The value range can be from 100 to 10000.	Specify the value range to block

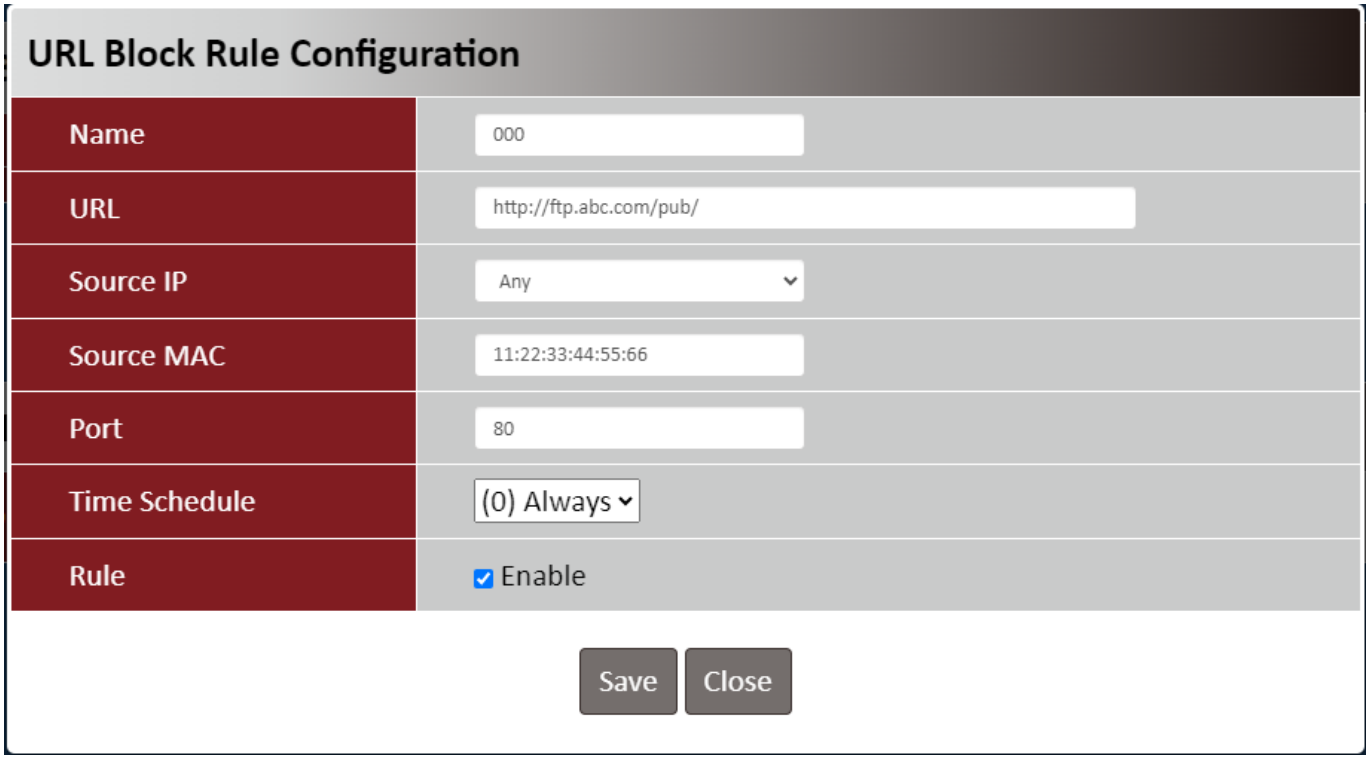
Block Smurf Attack	The box is unchecked by default	Check the **Enable** box to activate this Block Smurf Attack function
Block Land Attack	The box is unchecked by default	Check the **Enable** box to activate this Block Land Attack function
Block Fraggle Attack	The box is unchecked by default	Check the **Enable** box to activate this Block Fraggle Attack function
Block Ping Of Death Attack	The box is unchecked by default	Check the **Enable** box to activate this Block Ping Of Death Attack function
Block Traceroute	The box is unchecked by default	Check the **Enable** box to activate this Block Traceroute function

4.2.4 URL Block

"URL Blocking" function can let you define blocking rules for incoming and outgoing Web request packets. With defined rules, gateway can control the Web requests containing the complete URL.



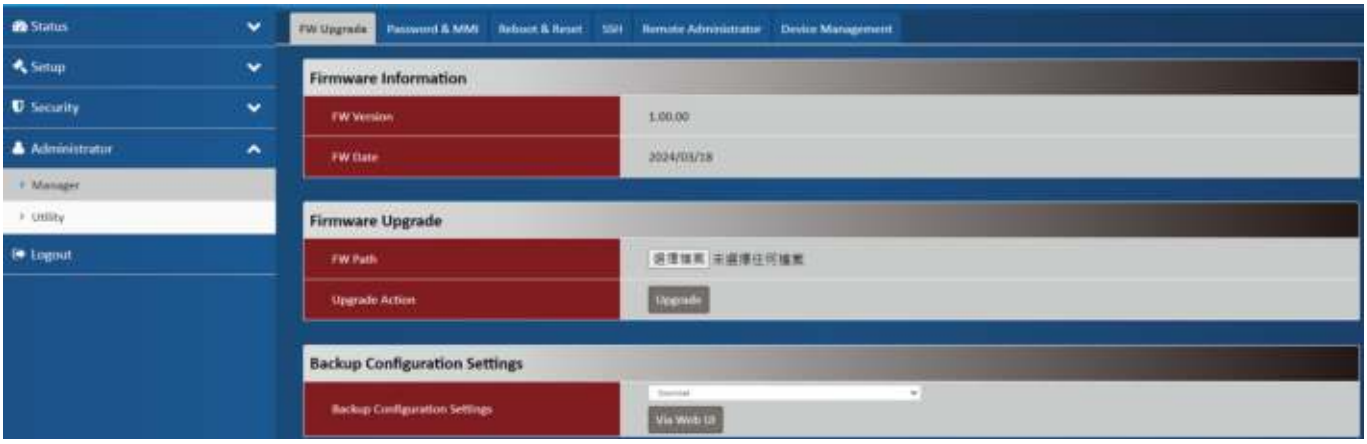
URL Block Page		
Item	**Value setting**	**Description**
URL Block	The box is unchecked by default	Check the **Enable** box to activate this **URL Block** function Click Add will pop-up URL Block Rule configuration page



URL Block Rule Configuration Page		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must-fill setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
URL	Blank is set by default	Specify URL, Domain Name, or Keyword list for URL checking.
Source IP	1.A Must-fill setting Any is set by default	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 entered in this field. Select IP Range to filter packets coming from a specified range of IP address entered in this field.
Source MAC	Blank is set by default	This field is to specify the **Source MAC address**.
port	Blank is set by default	This field is to specify the **port**
Time schedule	1. An optional setting 2. **(0)Always** is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0) Always.
Rule	The box is unchecked by default	Check the **Enable** box to activate this **URL Block** function

Chapter 5 Administrator

5.1 Manager



5.1.1 FW Upgrade



Firmware Information		
Item	**Value setting**	**Description**
FW Version	N/A	It displays the firmware version of the product
FW Date	N/A	It displays the build time of the firmware



Firmware Upgrade		
Item	**Value setting**	**Description**
FW Path	N/A	Select firmware file to be upgraded
Upgrade Action	N/A	Click **Upgrade** button to start upgrade process with selected FW

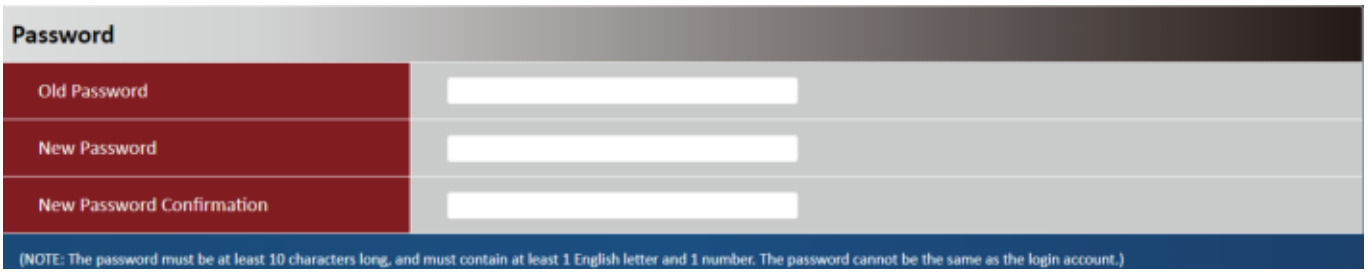


Backup Configuration Settings		
Item	**Value setting**	**Description**
Backup Configuration Settings	**Download** is selected by default	You can backup or restore the device configuration settings by clicking the ***Via Web UI*** button. Select "**Download**" to backup current configuration to a file. Select "**Upload**" to restore configuration from selected file.

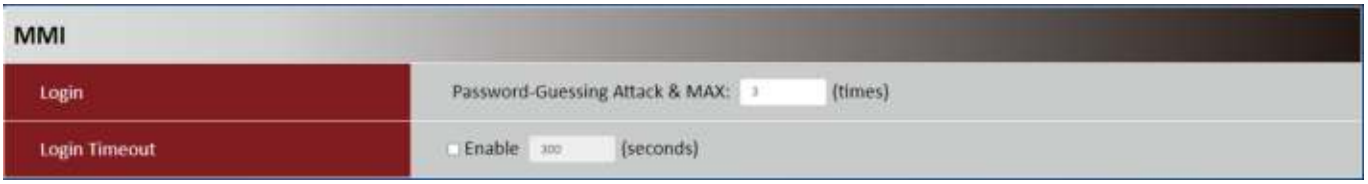
5.1.2 Password & MMI



Username		
Item	**Value setting**	**Description**
Username	1. The default username is 'admin'.	Display the current username for the administrator
New Username	String: any text	Enter the new username

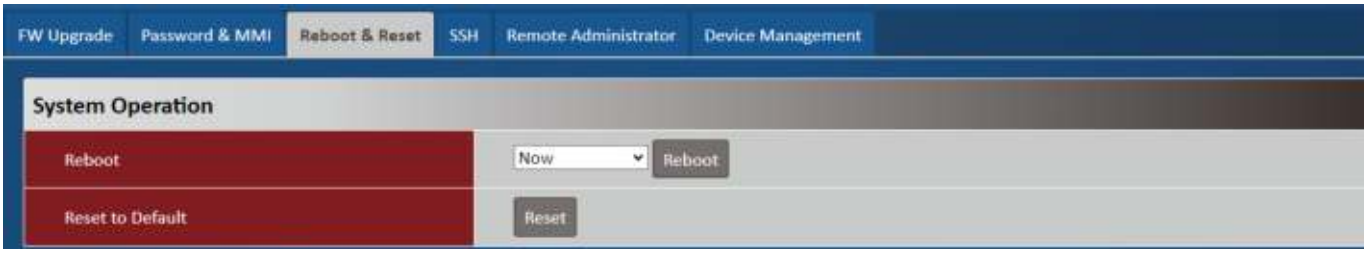


Password		
Item	**Value setting**	**Description**
Old Password	1. String: any text **2. The default password for web-based MMI is 'admin'.**	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password
New Password Confirmation	String: any text	Enter new password again to confirm



MMI		
Item	**Value setting**	**Description**
Login	3 times is set by default	Enter the login trial counting value. Value Range: 3 ~ 10. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will be displayed and ignore the following login trials.
Login Timeout	The Enable box is checked, and 300 is set by default.	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. ***Value Range***: 30 ~65535.

5.1.3 Reboot & Reset



System operation		
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
Reset to Default	N/A	Click the **Reset** button to reset the device configuration to its default value.

5.1.4 SSH



SSH		
Item	**Value setting**	**Description**
SSH	1. Default value is disable such service 1. By default **Service Port** is 22.	Check the **Enable** box to activate the 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.

5.1.5 Remote Administrator

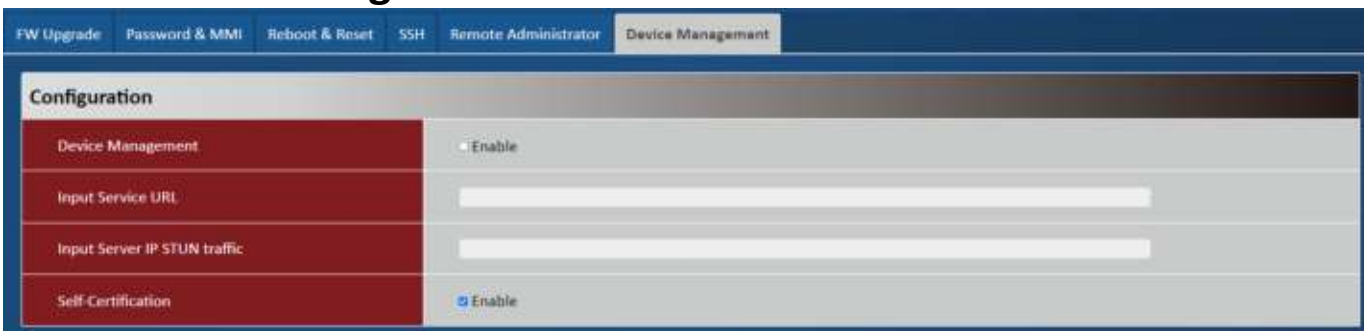


Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Remote Administrator Host Definition	N/A	Press “Add” to set a remote administrator rule



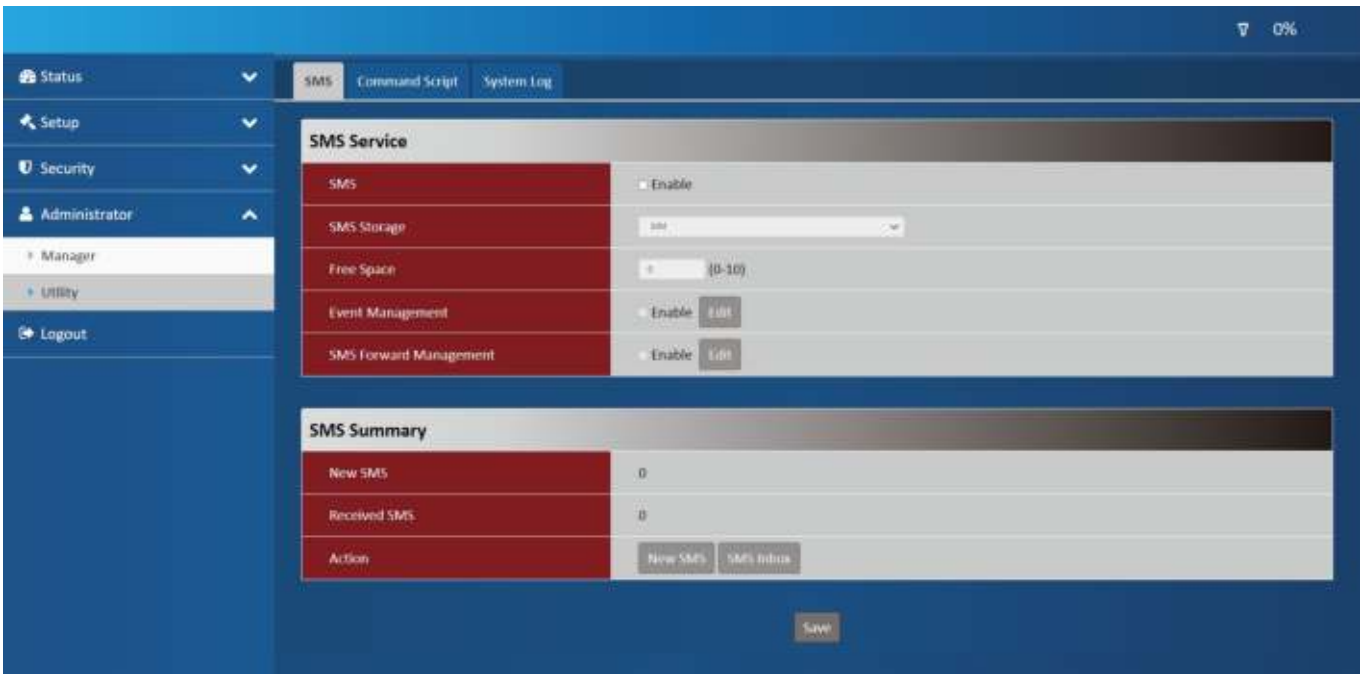
Rule Configuration		
Item	**Value setting**	**Description**
Name	String: any text	Set rule name
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
Remote IP	A Must-fill setting Any IP by default	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet.
Subnet Mask	255.0.0.0/8 by default	When Select Specific IP to allow the remote host coming from a specific subnet.
Service Port	1. 80 for HTTP by default	This field is to specify a Service Port to HTTP or HTTPS connection.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.

5.1.6 Device management

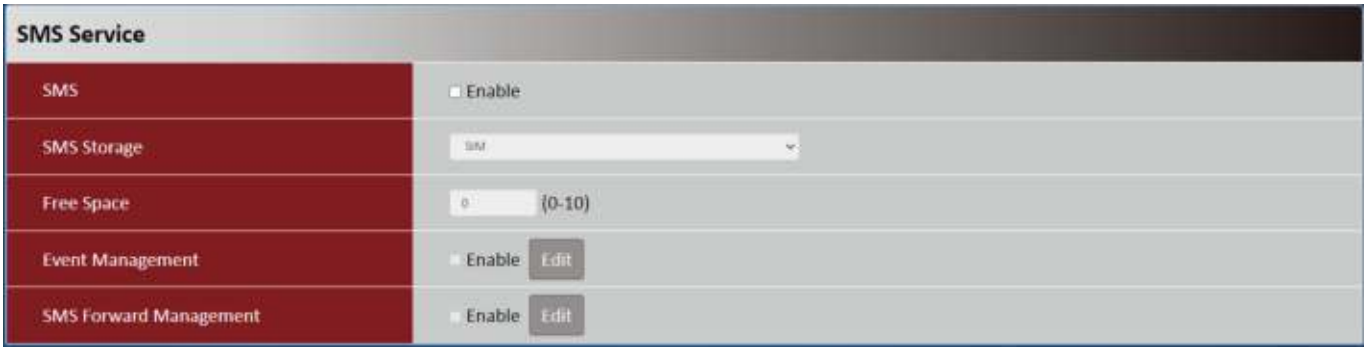


configuration		
Item	**Value setting**	**Description**
Device management	The box is unchecked by default	Check the **Enable** box to activate this **Device management** function
Input service URL	Blank is set by default	Specify ANMS service domain name URL
Input server IP stun traffic	Blank is set by default	Specify **ANMS server public IP or** domain name
Self-certification	The Enable box is checked by default	Check the **Enable** box to activate this **Self-certification** function

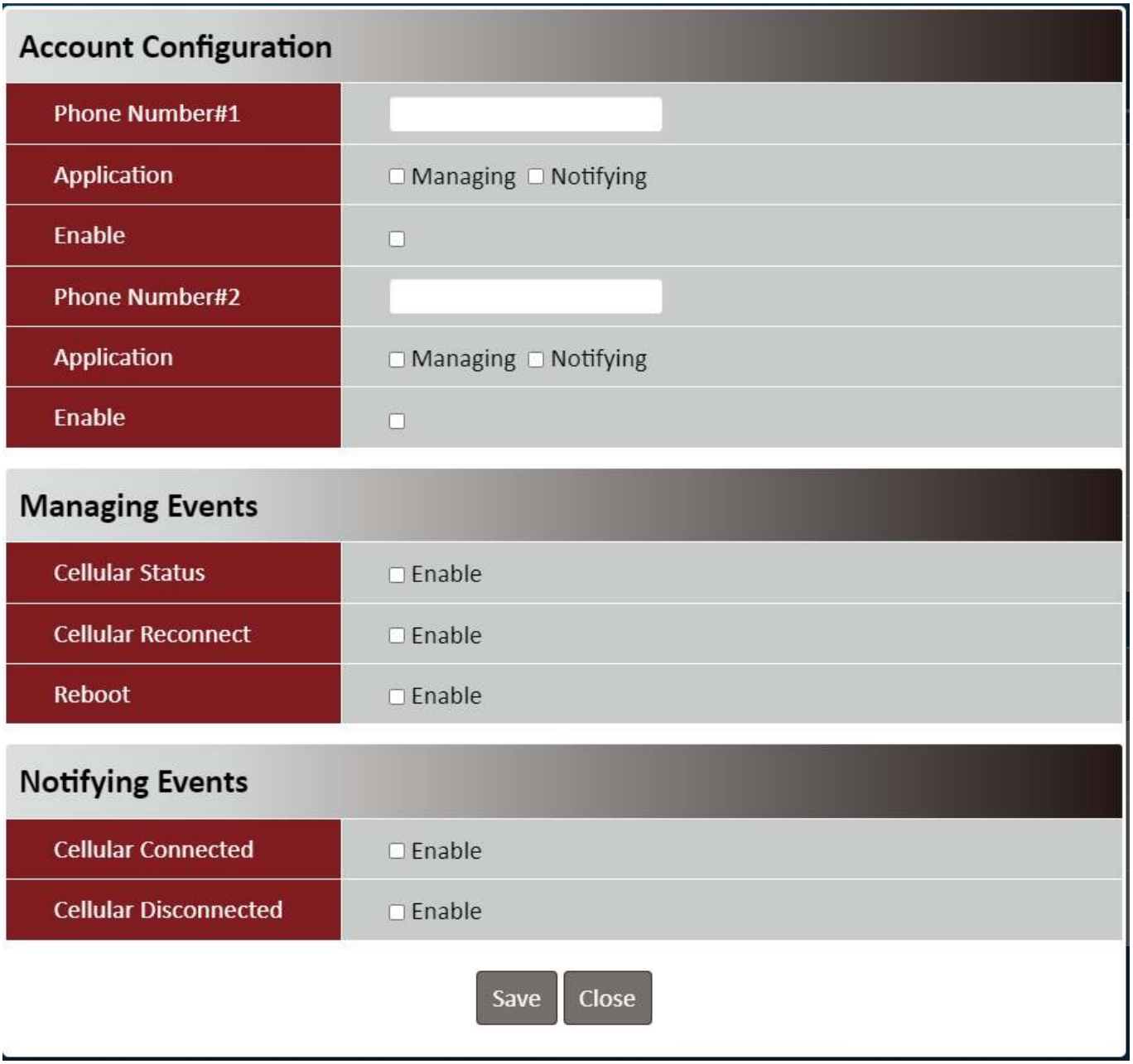
5.2 Utility



5.2.1 SMS



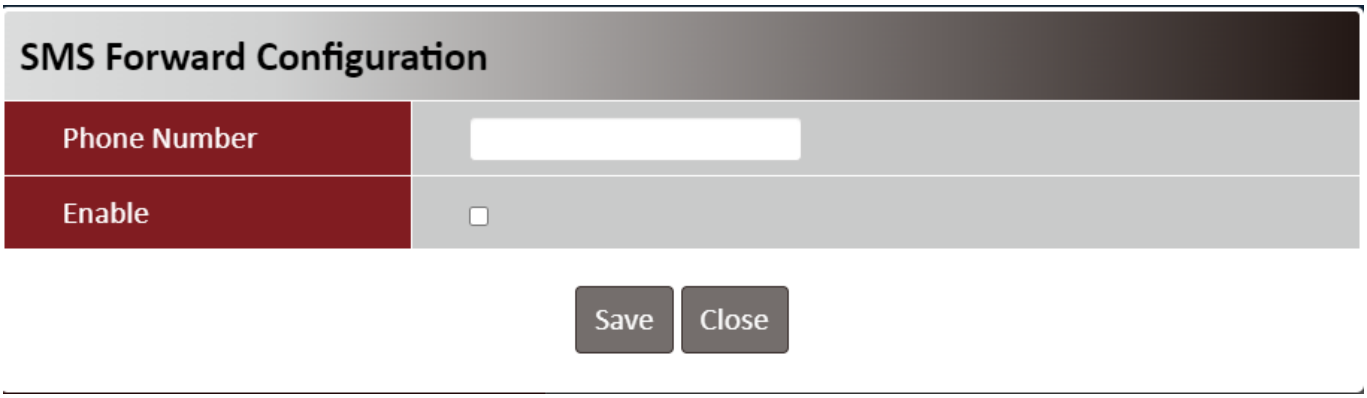
SMS service		
Item	**Value setting**	**Description**
SMS	The box is unchecked by default	Check the Enable box to activate this SMS function Click Add will pop-up Mac control Rule configuration page
SMS storage	SIM by default	Select SIM or modem storage
Free space	0 by default	specify a number (1-10) for message count to reserve some available storage space and prevent it from run out of storage.
Even management	The box is unchecked by default	Check the Enable box to activate this SMS function Click edit will pop-up account configuration page
SMS forward management	The box is unchecked by default	Check the Enable box to activate this SMS function Click edit will pop-up sms forward configuration page



Account configuration		
Item	**Value setting**	**Description**
Phone number#1	The box is unchecked by default	Sender Phone Number for the received SMS
application	The box is unchecked by default	Check the Enable box to activate this SMS function Check the Enable box to activate this SMS function
enable	The box is unchecked by default	Check the Enable box to activate this SMS function
Phone number#2	The box is unchecked by default	Sender Phone Number for the received SMS
application	The box is unchecked by default	Check the Enable box to activate this Managing Event function Check the Enable box to activate this Notifying Events function
enable	The box is unchecked by default	Check the Enable box to activate this SMS function

Managing Event		
Item	Value setting	Description
Cellular Status	The box is unchecked by default	Check the Enable box to activate this SMS notification function
Cellular Reconnect	The box is unchecked by default	Check the Enable box to activate this SMS notification function
Reboot	The box is unchecked by default	Check the Enable box to activate this SMS notification function

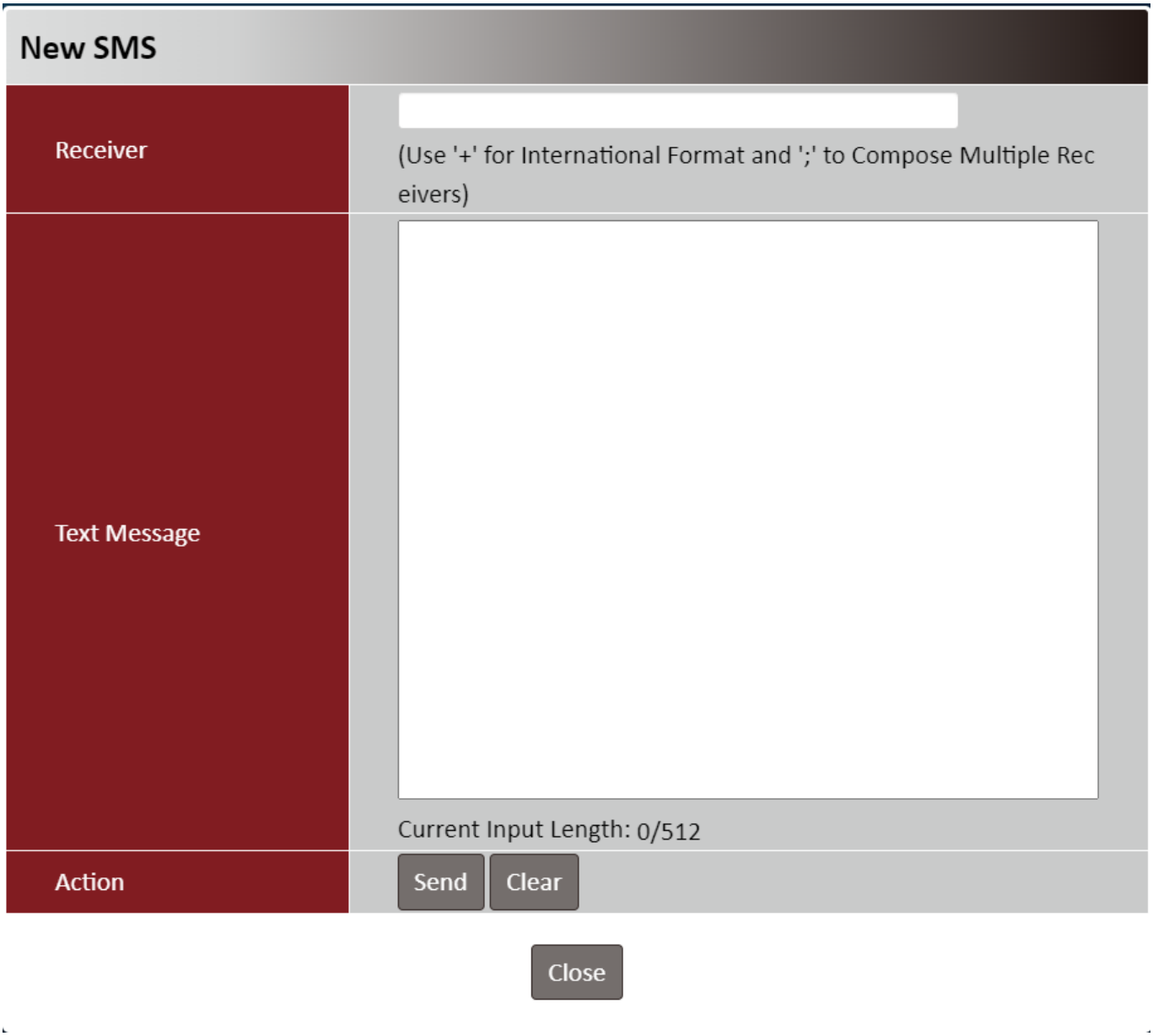
Notifying Events		
Item	Value setting	Description
Cellular Connected	The box is unchecked by default	Check the Enable box to activate this SMS notification function
Cellular Disconnected	The box is unchecked by default	Check the Enable box to activate this SMS notification function



SMS forward configuration		
Item	Value setting	Description
Phone number	1. A Must-fill setting 2.Any string	Sender Phone Number for the received SMS
Enable	The box is unchecked by default	Check the Enable box to activate the SMS function.



SMS summary		
Item	Value setting	Description
New sms	N/A	show new sms number
Received sms	N/A	show Received sms number
Action	N/A	Click new sms will pop-up new sms page Click sms inbox will pop-up sms inbox page

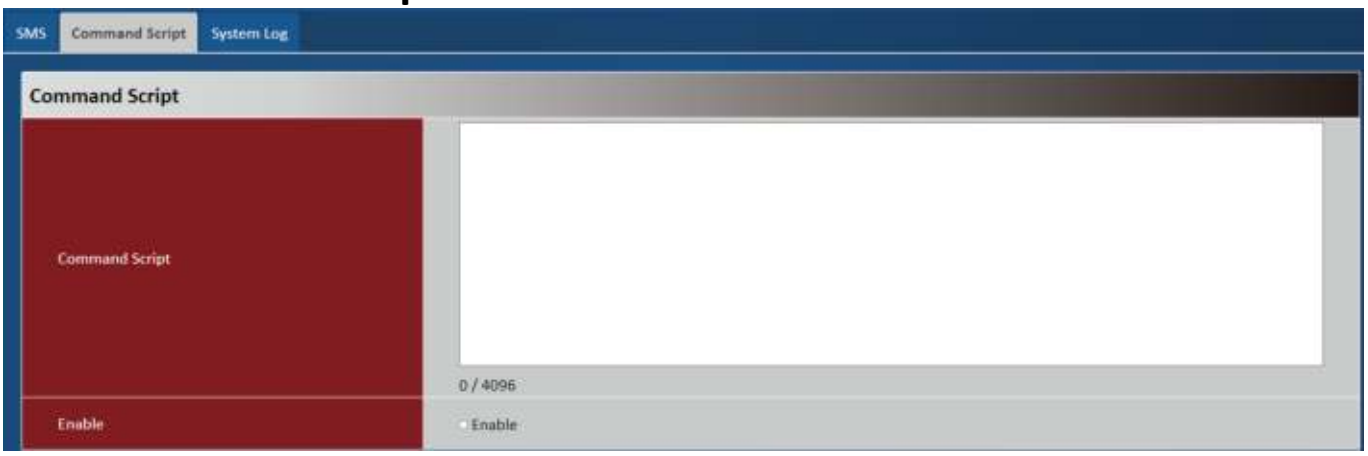


New SMS		
Item	**Value setting**	**Description**
Remote Administrator Host Definition	N/A	Write the receivers to send SMS. User need to add the semicolon and compose multiple receivers that can group send SMS.
Text Message	N/A	Write the SMS context to send SMS.
action		Click the Send button, above text message will be sent as a SMS. Click the clear button, to clear text message



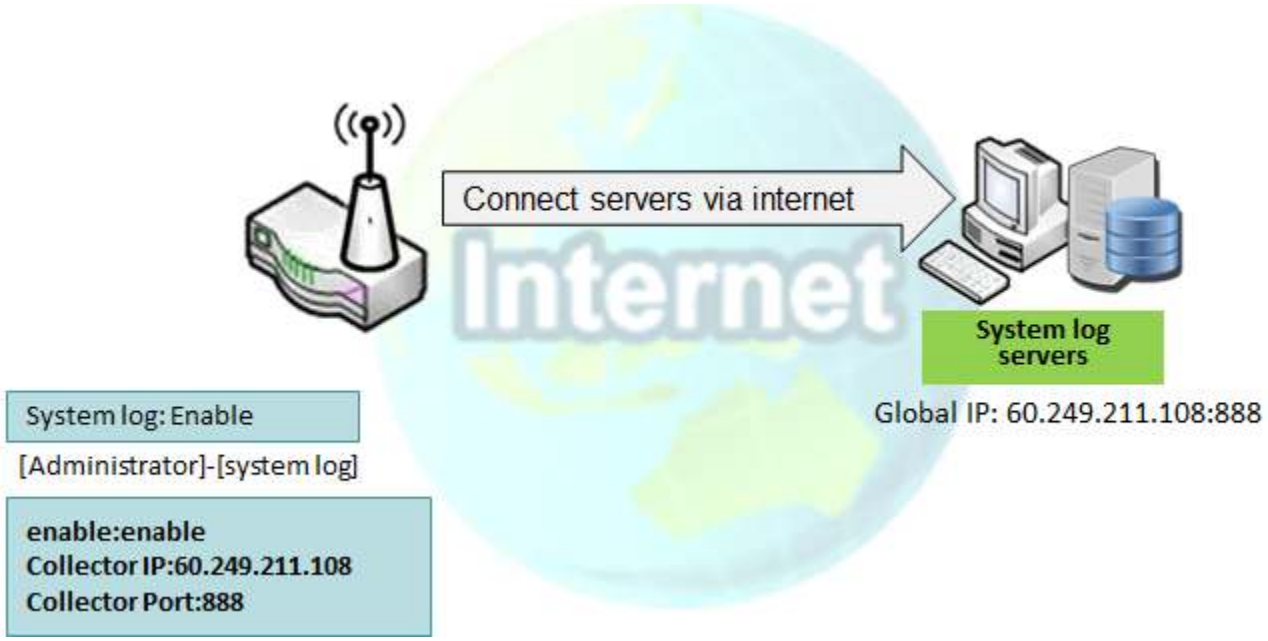
SMS inbox		
Item	**Value setting**	**Description**
none	N/A	read or delete SMS, reply SMS or forward SMS from this screen.

5.2.2 Command Script



Command Script		
Item	**Value setting**	**Description**
Command Script	1.An Optional setting 2.Any string	Enter a short description for the applied Command script.
Enable	The box is unchecked by default	Check the Enable box to activate the Command Script function.

5.2.3 System log





System log		
Item	Value setting	Description
Enable	The box is unchecked by default	Check the Enable box to activate the system log function
Collector IP	0.0.0.0 by default	Specify System log server IP
Collector Port	0 by default	Specify System log server port