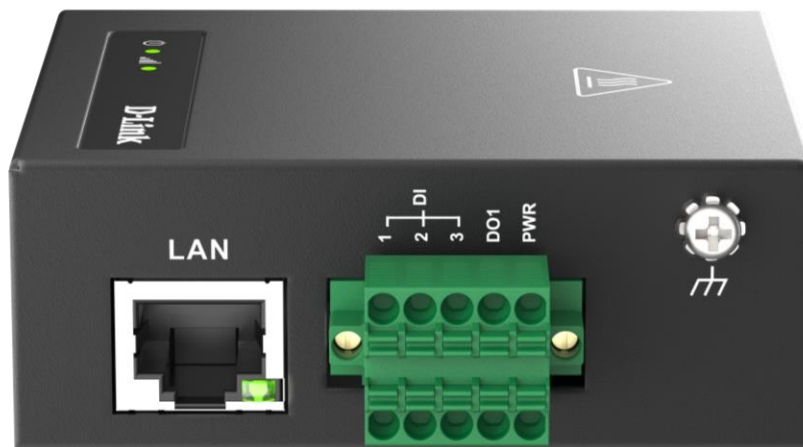


4G IIoT RTU

DOM-311-TSO

User Manual



Chapter 1 Introduction	5
1.1 Introduction	5
1.2 Contents List.....	6
1.2.1 Package Contents	6
1.3 Hardware Configuration	7
1.4 LED Indication	8
1.5 Installation& Maintenance Notice.....	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.....	14
1.6.2 Insert the SIM Card	14
1.6.3 Connecting Serial and I/O Devices	15
1.6.4 Connecting to the Network or a Host.....	16
1.6.5 Setup by Configuring WEB UI.....	16
Chapter 2 Status	17
2.1 Cellular	17
2.1.1 Network.....	17
2.1.2 Modem.....	18
2.1.3 Signal	21
2.1.4 Data Usage	22
2.2 Network.....	22
2.2.1 Client List.....	22
2.3 Security.....	23
2.3.1 VPN.....	24
Chapter 3 Setup	25
3.1 Network.....	25
3.1.1 Cellular	26
3.1.2 Ethernet	28
3.1.3 Port Forwarding	30

3.1.4 DDNS	33
3.2 Rouitng.....	34
3.2.1 Static Routing	34
3.2.2 Routing Information	35
3.3 System	36
3.3.1 System Time.....	36
3.3.2 Language.....	37
3.3.3 System Information	37
3.3.4 Scheduling	38
3.3.5 Data Cap	39
3.4 Bus&Protocol	40
3.4.1 Port Configuration.....	40
3.4.2 Virtual COM.....	41
3.4.3 Modubs	48
Chapter 4 Advance.....	54
4.1 Digital Input/Output.....	54
4.2 Data to Server	58
4.1.1 RESTful.....	58
4.1.2 Heartbeat.....	59
4.1.3 MQTT	61
Chapter 5 Security.....	65
5.1 VPN	65
5.1.1 OpenVPN	65
5.2 Firewall	68
5.2.1 Packet Filters	68
5.2.2 MAC Control.....	71
5.2.3 IPS	73
Chapter 6 Administrator.....	75
6.1 Manager.....	75
6.1.1 FW Upgrade.....	75
6.1.2 Password & MMI	76
6.1.3 Reboot & Reset	77

- 6.1.4 SSH 78
- 6.1.5 Remote Administrator..... 78
- 6.1.6 Device Management 79
- 6.2 Utility..... 80
 - 6.2.1 SMS..... 80
 - 6.2.2 Command Script..... 84

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of D-Link DOM-311-TSO 4G module-based remote terminal unit (RTU). With this RTU 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 3G/4G WAN connection.
- Provide one Ethernet port for comprehensive LAN connection.
- Simple Web GUI is used for basic setting and check the 3G/4G status.
- Designed easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications.
- RS232/485 interface for serial data transmission
- Designed Multiple DI/O for sensor data transmission
- Wide power input range and wide working temperature to meet site environments

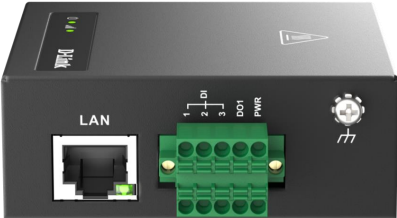
Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

4G IIT RTU

1.2 Contents List

1.2.1 Package Contents

#Standard Package

Items	Description	Contents	Quantity
1	DOM-311-TSO 4G IIoT RTU		1pcs
2	Cellular Antenna		2pcs
3	RJ45 Cable		1pcs
4	10 Pin Terminal Block		1pcs
5	Power Adapter (12V/1A)		1pcs
6	DIN-Rail Kit		1 set (DIN rail x1, screw x3)

#Optional Package

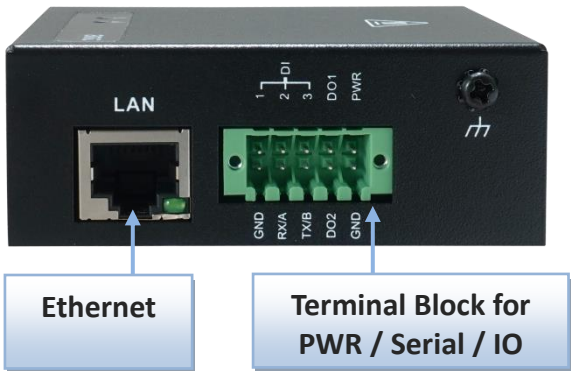
Items	Description	Contents	Quantity
-------	-------------	----------	----------

4G IIT RTU

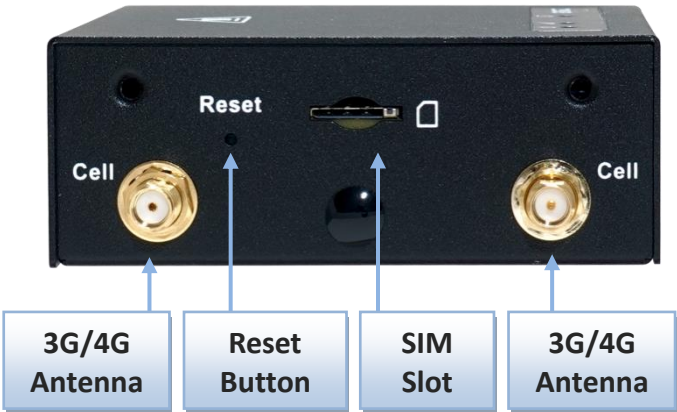
1	Wall-MountKit		1 set (Bracket x1, screw x3)
---	---------------	--	---------------------------------

1.3 Hardware Configuration

➤ Right View



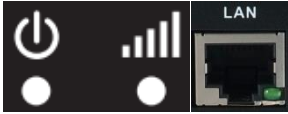
➤ LeftView



※Reset Button

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

1.4 LED Indication



Indication	LEDColor	Description
 Power	Blue	Steady On: Device power is on Off: Device power is off
 Cellular	Blue Red	Red Steady on: Cellular is not ready or no cellular signal. Red Flash: Cellular is ready but register status is not ready. Blue Steady On: The signal is ready and register to operator. Blue Fast Flash: State on LTE. Blue Slow Flash: State on 3G.
Ethernet	Green	Green and Steady On: A Ethernet device is connected. Green and Flash: Data transmission through Ethernet.

1.5 Installation& Maintenance Notice

1.5.1 System Requirements

Network Requirements	• AnEthernet RJ45cable • 4G cellular service subscription • 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: • Microsoft Edge 119 or higher • Chrome 73 or higher • Firefox 60.0 or higher

1.5.2 Warning



Attention

- DC 54V/1.67A power adapters are recommended.
- 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 using this product and accessories outdoors.

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 complies 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 WiFi product marketed in US must be 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

1.a Frequency Band for Cellular Connection (for EC25-EU version)

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink:1920-1980 MHz Downlink:2110-2170 MHz	23.1dBm
LTE FDD BAND 3	Uplink:1710-1785 MHz Downlink:1805-1880 MHz	23.0dBm
LTE FDD BAND 7	Uplink:2500-2570 MHz Downlink:2620-2690 MHz	22.8dBm
LTE FDD BAND 8	Uplink:880-915 MHz Downlink:925-960 MHz	23.2dBm
LTE FDD BAND 20	Uplink:832-862 MHz Downlink:791-821 MHz	23.5dBm
LTE FDD BAND 28A	Uplink: 704 -723 MHz Downlink: 759 -778MHz	23dBm
LTE FDD BAND 38	Uplink: 2570-2620 MHz Downlink: 2570-2620 MHz	21.7dBm
LTE FDD BAND 40	Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz	21.5dBm
WCDMA BAND 1	Uplink:1920-1980 MHz Downlink:2110-2170 MHz	23.3dBm
WCDMA BAND 8	Uplink:880-915 MHz Downlink:925-960 MHz	
E-GSM	Uplink:880-915 MHz Downlink:925-960 MHz	32.9 dBm
DCS	Uplink:1710-1785 MHz Downlink:1805-1880 MHz	29.9 dBm

(2) DoC Information

Please contact D-Link.

(3) RF Exposure Statements

To comply with RF exposure limits established in FCC, the distance between the antenna or antennas and the user should not be less than 20 cm (7.87”).

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.

4G IIT RTU

(4) Unit Mounting Notice

The product is suitable for mounting at heights $\leq 2\text{m}$ (approx. 6 ft), or in a cabinet.

Ensure the unit is fixed tightly to reduce the likelihood of injury due to exposure to mechanical hazards if dropped.

(5) Manufacture Information

Manufacture Name: D-Link Corp.

Manufacture Address: No. 289, Xinhua 3rd Rd., Neihu District, Taipei 11494, Taiwan, R.O.C.

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The DOM-311-TSO 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 middle area of DOM-311-TSO. You need to remove the outer SIM card cover before installing or removing an inserted SIM card. Please follow below instructions to install or remove a SIM card. After SIM card is well installed or removed, put back the outer SIM card cover.

Step 1:

Loosen the screws and remove the SIM covers as shown on the right..



Step 2:

Push the SIM card into the slot.



Step 3:

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



1.6.3 Connecting Serial and I/O Devices

The DOM-311-TSO series product provides a 10-pin terminal block for one serial port (RS232/485), three digital input (DI), and two digital output (DO). Connect the field device(s) to the I/O ports with the right pin assignments as shown below.



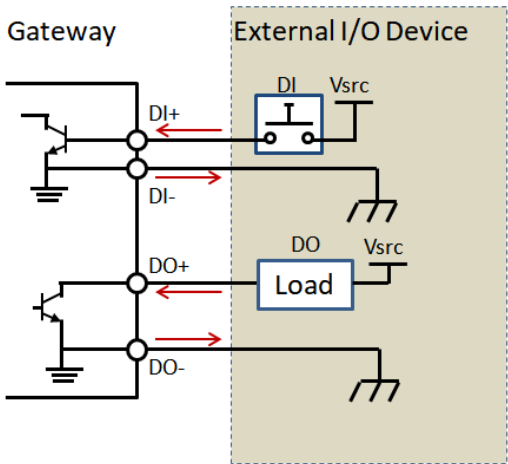
Pinout Definition

Pin1	Pin2	Pin3	Pin4	Pin5
DI1	DI2	DI3	DO1	PWR
Pin6	Pin7	Pin8	Pin9	Pin10
GND	RX/A	TX/B	DO2	GND

Digital I/O Specification

Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2V
Digital Output	Non-Relay mode	Max. 30V/1.25W

Example of Connection Diagram



1.6.4 Connecting to the Network or a Host

The DOM-311-TSO series provides one RJ45 port to connect to 10/100Mbps 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.

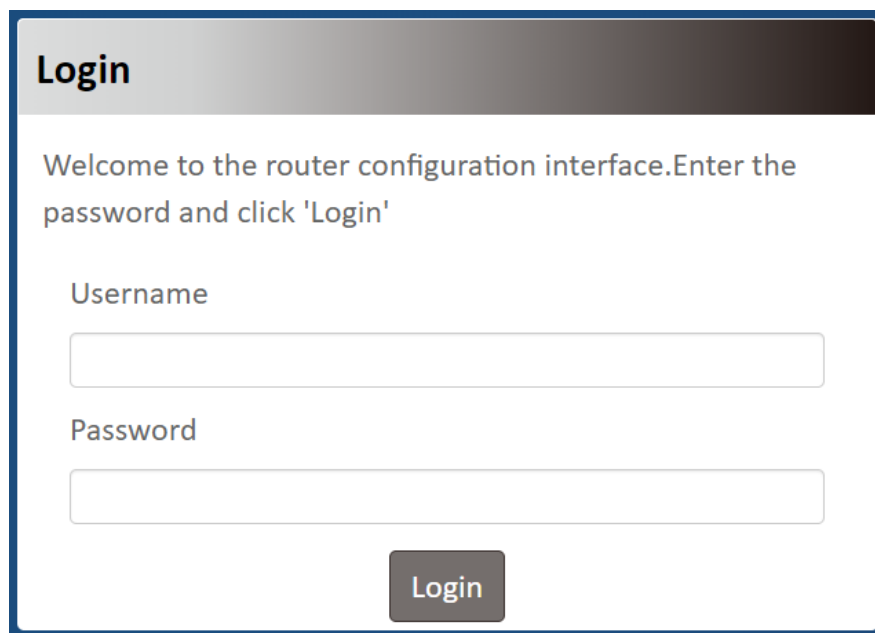
1.6.5 Setup by Configuring WEB UI

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.

A screenshot of a web-based login page for a router configuration interface. The page has a dark blue header with the word 'Login' in white. Below the header, there is a light gray box containing the text: 'Welcome to the router configuration interface. Enter the password and click 'Login''. Underneath this, there are two input fields: one labeled 'Username' and one labeled 'Password'. At the bottom right of the form, there is a dark gray button with the word 'Login' in white text.

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

Status

Cellular

Network

Security

DashBoard

Setup

Security

Administrator

Logout

Network

Modem

Signal

IPv4 Network

Mode	NAT
Link Status	Disconnected
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0

2.1.1 Network

Network

Modem

Signal

Data Usage

IPv4 Network

Mode	NAT
Link Status	Connected 0 day 0:26:18
IP Address	100.120.108.6
Netmask	255.255.255.252
Gateway	100.120.108.5

Network Page	
Item	Description
Mode	Network type NAT
Link Status	Display cellular network statusconnected or disconnected and Connexion Time.
Ip address	Base station distribution network ip
Netmask	Display cellular network netmask
Gateway	Display cellular network gateway

2.1.2 Modem

Network

Modem

Signal

Modem Information

IMEI

860728062718585

Advanced Information

Advanced

Service Information

SIM

SIM-A

SIM Status

Ready

Register Status

Registered

Operator

Chunghwa Telecom

Service Type

LTE

Band

Band 3

Advanced Information

Advanced

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

Advanced information

IMEI

864303054321859

Temperature

50 °C

Band Capability

B1,B3,B7,B8,B20,B28,B38,B40,B41

Close

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

Service Information	
SIM	SIM-A
SIM Status	Ready
Register Status	Registered
Operator	Chunghwa Telecom
Service Type	LTE
Band	Band 3
Advanced Information	<button>Advanced</button>

Service information Page	
Item	Description
Sim	Display card slot
Sim status	Displayread sim status
Register status	Display base station registration statusregistered or not register
Operator	Operator name
Service type	Displaycorresponding types of network signals
Band	Connected frequency band
Advanced Information	Clicl“advanced”button to show Advanced Information

Advanced information

MCC	466
MNC	92
Roaming	No
Cell ID	965E40E
Band	Band 7
LAC	0
TAC	36400

Close

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

Network

Modem

Signal

Cellular Signal

Service Type	LTE
Operator	Chunghwa Telecom
RSSI	-59
Advanced Information	Advanced

CellularSignal Page	
Item	Description
Service type	Display corresponding types of network signals.
Operator	Operator name
RSSI	Display Received Signal
Advanced Information	Click“advanced”button to show Advanced Information

Advanced information

RSSI	-59
RSRP	-90
RSRQ	-12
SINR	1.70
RSCP	0
ECIO	0

Close

Advanced Information Page	
Item	Description
RSSI	Display Received Signal
RSRP	Display Signal ReceivedPower
RSRQ	Display Signal ReceivedQuality
SINR	DisplayInterference Strength
RSCP	DisplaySignalReceivedPower
ECIO	DisplayinterferenceRatio

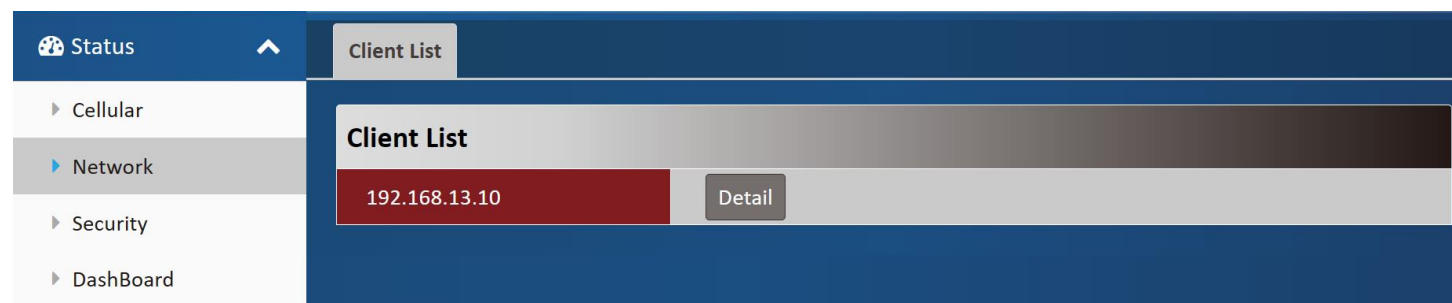
2.1.4 Data Usage

Traffic Statistics	
Traffic Statistics (RX+TX)	GB
Downlink Traffic Statistics	GB
Uplink Traffic Statistics	GB
Clear Statistics	Clear

Data Usage Page	
Item	Description
Traffic Statistics(RX + TX)	Display current Data usage of Cellular Newtork.
Downlink Traffic Statistics	
Uplink Traffic Statistics	

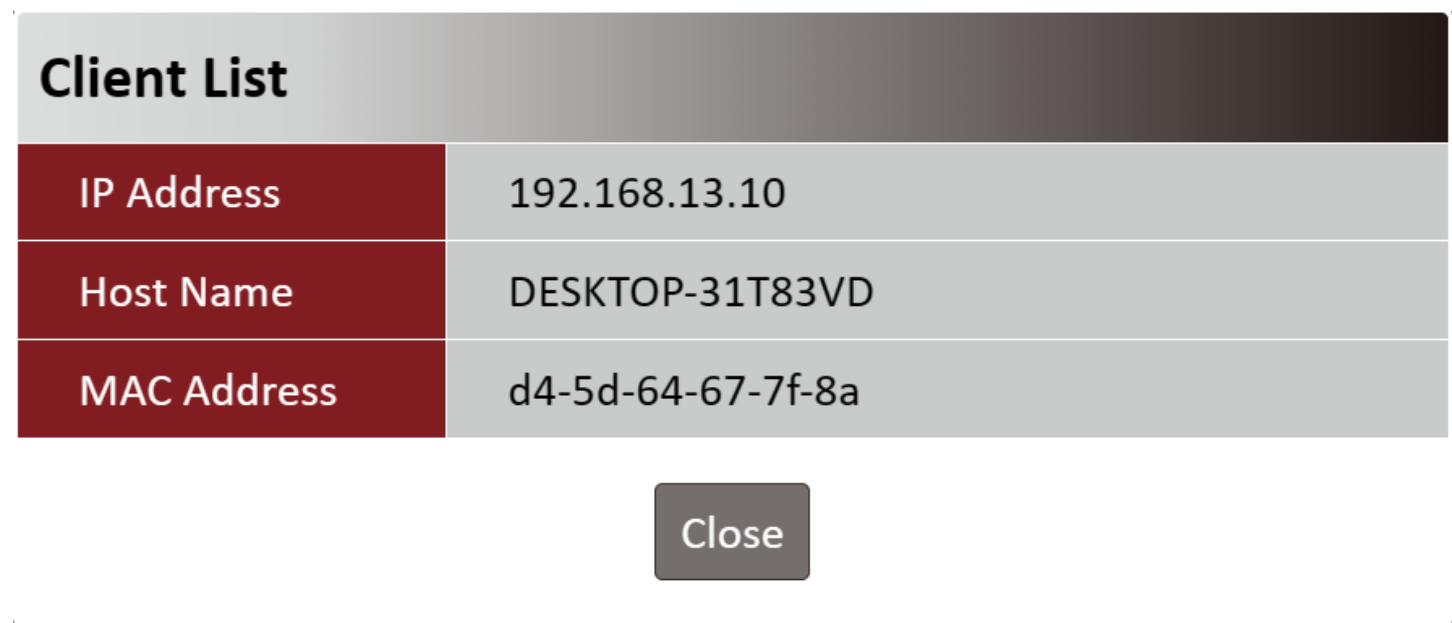
2.2 Network

2.2.1 Client List



Go to **Status > Network > Client List** tab.

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



LAN Client List		
Item	Value setting	Description
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.

2.3 Security

Status

Cellular

Security

Setup

VPN

OpenVPN Client Name

OpenVPN Client #1

Advanced

2.3.1 VPN

OpenVPN Client Name

OpenVPN Client #1

Advanced

Openvpn client name Page	
Item	Description
Openvpn client #1	Click "advanced" button to show Advanced Information

Advanced Information

OpenVPN Client Name	OpenVPN Client #1
Remote IP/FQDN	122.146.196.220
Remote Subnet	192.168.218.0 / 24
Virtual IP	0.0.0.0
Conn.Time	00:00:00:00
Conn.Status	Disconnected

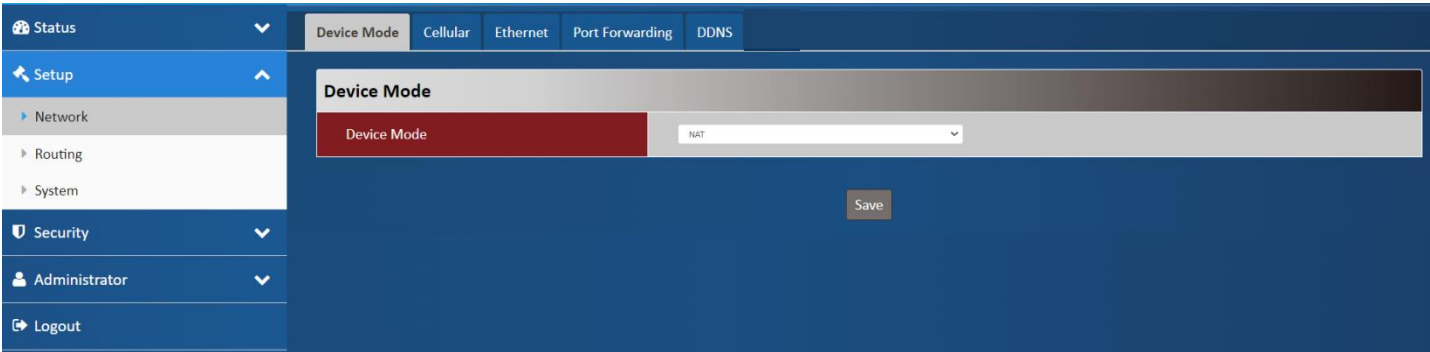
Close

Advanced Information Page	
Item	Description
Openvpn client name	VpnClient name
Remote ip/FQDN	Vpn server ip or FQDN
Remote subnet	Vpn server remote subnet
Virtual ip	Vpn virtual ip
Conn.time	Displayconnected time
Conn.status	Displayconnected or disconnected

Chapter 3 Setup

The DOM-311-TSO connect to a machine via the Ethernet interface for 3G/4G network connection. DOM-311-TSO also provides another function with NAT router. It can help the network application more flexible.

3.1 Network



Network	
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.

3.1.1 Cellular

74%

Status

Setup

Network

Routing

System

Security

Administrator

Logout

Device Mode

Cellular

Ethernet

Port Forwarding

DDNS

Cellular Access

Network Type	Auto
APN	Manual
Manual APN	
Username	
Password	
Authentication	Auto
IP Type	IPv4
IP Mode	Dynamic IP Static IP Config
PIN Code	
Roaming	☐ Enable
MTU Setup	☐ Enable (68~1500)
Keep Alive	☐ Enable IP Address: 8.8.8.8 Interval: 60 (2~14400 seconds)
Discard Ping from WAN	☐ Enable

Save

Cellular Access		
Item	Value setting	Description
Network Type	1. A must-fill setting 2. By default Auto is selected	Auto/3G only / 4G only: Please select one depend as your Cellular Network.
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 2. String format : any text	Enter the APN you want to use to establish the connection. This is a must-fillsetting if you selected Manual APN as APN scheme.
Username	1. Anoptional setting 2. String format : any text	Enter the optional Username settings if your ISP provided such settings to you.
Password	1. Anoptional 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	Select PAP (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server.

	selected	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 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	If the PIN (Personal Identification Number) code is required to unlock your SIM card, enter the PIN code you set.
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.
Discard Ping 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.

Static IP Configuration

IP	0.0.0.0	
Subnet Mask	255.255.255.0 (/24)	▼
Default Gateway	0.0.0.0	(Optional)
Primary DNS	0.0.0.0	(Optional)
Secondary DNS	0.0.0.0	(Optional)

Save

Close

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	TheSubnetMask of this configed static IP.
Default Gateway	1. IPv4 format. 2. An optional setting	Thegatewaysettingofthisconfiged static IP.
Primary DNS	1. IPv4 format. 2. An optional setting	Assigned DNS server of this configed static IP.
Secondary DNS	1. IPv4 format. 2. An optional setting	Assigned DNS server of this configed static IP.

3.1.2 Ethernet

Device Mode
Cellular
Ethernet
Port Forwarding
DDNS

Ethernet IP

IP	192.168.123.254
Netmask	255.255.255.0 (/24) ▾
DHCP Server	☒ Enable
DHCP Setting	DHCP Config

Save

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

IP Pool Start	5
IP Pool End	10
Lease Time	3600

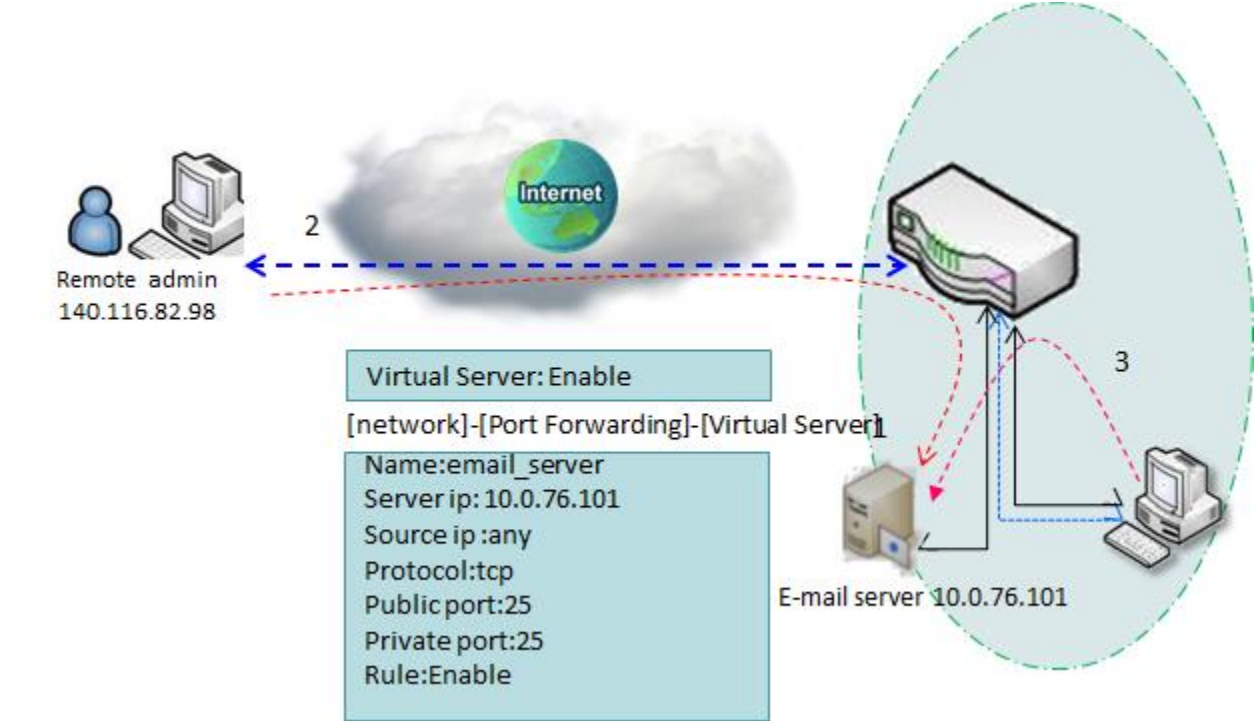
Save

Close

DHCP Setting Item	Value setting	Description
IP Pool Start	1. numericstring 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. numeric 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. numeric string format. 2. A must-fill setting	The Lease Time of this DHCP Server. <u>ValueRange:</u> 300 ~ 604800 seconds.

3.1.3 Port Forwarding

"Virtual Server"allows you to access servers with the global IP address of the gateway as if they are servers existed in 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.



Device Mode

Cellular

Ethernet

Port Forwarding

DDNS

PoE

Virtual Server

Virtual Server

☐ Enable

Add

Save

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

Name		
Server IP		
Source IP	Any	
Protocol	TCP(6)	
Public Port	Single Port	
Private Port	Single Port	
Rule	☐ Enable	

Save

Close

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. <u>Value Range</u>: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. <u>Value Range</u>: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. <u>Value Range</u>: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 filled setting 2. The box is unchecked by default.	Check the Enable box to activate the rule.

Rule Name

test

Edit

Delete

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

3.1.4 DDNS

Device Mode	Cellular	Ethernet	Port Forwarding	DDNS
Configuration				
DDNS	☐ Enable			
Provider	DynDNS.org ▼			
Host Name				
User Name / E-Mail				
Password / Key				

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 etc...
Host Name	1. String format can be any text 2. A Must-fill setting	Your registered host name of DDNS Service. <u>Value Range:0 ~ 63 characters.</u>
User Name / E-Mail	1. String format can be any text 2. A Must-fill setting	Enter your User name or E-mail addresss ofDDNS Service.
Password / Key	1. String format can be any text 2. A Must-fill setting	Enter your Password or Key ofDDNS Service.

3.2 Routitng

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 packets to different peer gateways based on the routing table. You need to define the static routing information in gateway routing rule list.

Status

Setup

Network

Routing

System

Static Routing

Routing Information

Static Routing

☐ Enable

Add

Save

Static Routing	Value setting	Description
Item		
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

Name

Destination IP

Subnet Mask

Gateway IP

Interface

Metric

Rule

LAN

☐ Enable

Save

Close

Static Routing Rule Configuration	Value setting	Description
Item		
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 filled setting	Specify the Destination IP of this static routing rule.
Subnet Mask	1.255.255.255.0 (/24) is	Specify the Subnet Mask of this static routing rule.

	set by default	
Gateway IP	1. IPv4 Format 2. A Must filled 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. Numeric String Format 2. A Must filled setting	The Metric of this static routing rule. <i>Value Range: 0 ~ 255.</i>
Rule	The box is unchecked by default.	Click the Enable to activate static routing functions.

3.2.2 Routing Information

Static Routing

Routing Information

Routing Information

192.168.123.0

Detail

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

Routing Information

Destination IP	192.168.123.0
Subnet Mask	255.255.255.0
Gateway IP	0.0.0.0
Interface	LAN
Metric	0

Close

3.3 System

This section provides the configuration of system features.

Status

Setup

Network

Routing

System

Security

Administrator

Logout

System Time

Language

System Information

Scheduling

System Time

Current Time

Thu Dec 7 07:28:19 2023

Sync Time

Auto

Time Zone

(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

NTP Server

pool.ntp.org

Daylight Saving

☐ Enable

Start Date

1 / 1 / 0 (Month/Day/Hour)

End Date

1 / 1 / 0 (Month/Day/Hour)

Action

Action

Save

3.3.1 System Time

System Time

Language

System Information

Scheduling

System Time

Current Time

Thu Dec 7 07:29:10 2023

Sync Time

Auto

Time Zone

(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

NTP Server

pool.ntp.org

Daylight Saving

☐ Enable

Start Date

1 / 1 / 0 (Month/Day/Hour)

End Date

1 / 1 / 0 (Month/Day/Hour)

Action

Action

Save

System time Item	Value setting	Description
Current Time	N/A	Show the current time of the unit.

Sync Time	1. A must-fillitem. 2. Auto is selected by default.	When select Auto , unit will sync the time via cellular cell, 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-fillitem. 2. GMT+00 :00 is selected by default.	Select a time zone that this device locates in
NTP Server	1. A must-fillitem.	Indicate which NTP server will be used of the time synchronization.
Daylight Saving	1. It is an optional item. 2. Un-checked 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 Language

System Time
Language
System Information
Scheduling

Configuration

Language List
English

Save

Configuration Item	Value setting	Description
Language List	1. A must-fillitem. 2. English is selected by default.	Language setting of the WebGUI.

3.3.3 System Information

System Time
System Information
Scheduling
Data Cap

System Information

Model Name
DOM-311-TSO A1

Serial Number
ZZ24700051

Device Up-Time
0day 0hr 8min 1sec

System Information

Item	Value setting	Description
Model Name	N/A	Show the model name of the device

3.3.4 Scheduling

System Time

Language

System Information

Scheduling

Time Schedule

Time Schedule

Add

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

Time Schedule Configuration

Rule Name

Rule Policy

Inactivate

The Selected Days and Hours Below.

Time Period Definition

Week Day

Every Day

Start Time (hh:mm)

End Time (hh:mm)

Save

Close

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

3.3.5 Data Cap

System Time
System Information
Scheduling
Data Cap

Configuration

Data Cap	☐ Enable
Amount	20 GB
Warning Ratio (%)	100%
Reset Date monthly	10
Current Ratio (%)	Datacap is disabled
Current Ratio (GB)	
Send SMS	☐ Enable
Phone Number	You should add the International Phone Code before the phone number. For a Polish phone number it is +48 (+48XXYYZZZ).
Reset	Reset

Configuration		
Item	Value Setting	Description
Data Cap	Un-Checked 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	Un-Checked by default.	Check the Enable box to activate the connection restriction function.
Phone Number	1. An Optional setting.	When send smsEnable,canSet the sending SMS object

3.4 Bus&Protocol

This section provides the configuration of bus&Protocol features.

3.4.1 Port Configuration

Port Configuration

Virtual COM

Serial Port Definition

Operation Mode	Virtual COM
Interface	RS-232
Baud Rate	38400
Data Bits	8
Stop Bits	1
Flow Control	None
Parity	None

Port Configuration Window		
Item	Value setting	Description
Operation Mode	Disable is set by default	It displays the current selected operation mode for the serial interface. Depending on the purchase 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 the cable length and the installed environment. The longer cable, the lower baud rate for it.
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. The supporting of Flow Control depends on the purchased model.
Parity	None is set by default	Select None / Even / Odd for Parity bit.

Save	N/A	Click Save button to save the settings.
------	-----	--

3.4.2 Virtual COM

When DOM-311-TSO is set to “Virtual COM” in Port Configuration.

Port Configuration	Virtual COM	
--------------------	-------------	--

Serial Port Definition

Operation Mode	Virtual COM
----------------	-------------

Operation Mode Definition for each Serial Port	
Operation Mode	Disable ▾
Listen Port	4001 (1-65535)
Trust Type	Allow All ▾
Max Connection	0 (1-128)
Connection Control	Always on ▾
Connection Idle Timeout	0 (0-3600 secs)
Alive Check Timeout	0 (0-3600 secs)

Data Packing	
Data Buffer Length	0 (0-1024)
Delimiter Character 1	0 (Hex) ☐ Enable
Delimiter Character 2	0 (Hex) ☐ Enable
Data Timeout Transmit	0 (0-1000 ms)

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. Device disconnects from the server when the connection is Idle for a specified period. You may also enable full time connection with the TCP server.

Enable TCP Client Mode Window		
Item	Value setting	Description
Operation Mode	A Must filled 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

		disconnect at idle timeout.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time 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	1. 0 is set by default 2. Range 0 to 3600 sec.	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. <u>Value Range:</u> 0 ~ 3600 seconds.

Data Packing Configuration		
Item	Value setting	Description
Data Buffer Length	1.An optional filled setting 2.Default value is 0	Enter the data buffer length for the serial port. <u>Value Range:</u> 0 ~ 1024.
Delimiter Character 1	1.An optional filled setting 2.Default value is 0	Check the Enable box to activate the Delimiter character 1, and enter the Hex code for it. <u>Value Range:</u> 0x00 ~ 0xFF.
Delimiter Character 2	1.An optional filled setting 2.Default value is 0	Check the Enable box to activate the Delimiter character 2, and enter the Hex code for it. <u>Value Range:</u> 0x00 ~ 0xFF.
Data Timeout Transmit	1.An optional filled 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. <u>Value Range:</u> 0 ~ 1000ms.
Save	N/A	Click the Save button to save the configuration

Specify Legal Host IP/FQDN

Legal Host IP/FQDN Definition	
Legal Host IP/FQDN Definition #1	Edit
Legal Host IP/FQDN Definition #2	Edit
Legal Host IP/FQDN Definition #3	Edit
Legal Host IP/FQDN Definition #4	Edit

Legal Host IP/FQDN Definition #1

To Remote Host	IP 0.0.0.0
Remote Port	0 (1-65535)
Enable	☒ Enable

Legal Host IP/FQDN Definition #1~4

Item	Value setting	Description
Enable	The box is unchecked by default	Check the Enable box to enable the TCP server configuration.
To Remote Host	A Must filled setting	Press Edit button to enter IP address or FQDN of the remote TCP server to transmit serial data.
Listen Port	1.A Must filled setting 2.Default value is 4001	Enter the TCP port number. This is the listen port of the remote TCP server. Value Range: 1 ~ 65535.
Save	N/A	Click the Save button to save the configuration

Enable TCP Server Mode

Configure the gateway as the 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.

Enable TCP Server Mode Window

Item	Value setting	Description
Operation Mode	A Must filled setting	Select TCP Server mode.
Listen Port	4001 is set by default	Indicate the listening port of TCP connection. Value Range: 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. 128 connections 2. 1 is set by default	Set the maximum number of concurrent TCP connections. Up to 128 simultaneous TCP connections can be established. Value Range: 1 ~ 128.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time 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 3600 sec.	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.
Enable	The box is 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.

SpecifyTrusted IP

Trusted IP Definition	
Trusted IP Definition #1	Edit
Trusted IP Definition #2	Edit
Trusted IP Definition #3	Edit
Trusted IP Definition #4	Edit

Trusted IP Definition #1

Host

Specific IP Address ▼0.0.0.0

Enable

☐ Enable

Save

Close

Legal Host IP Definition #1~4		
Item	Value setting	Description
Enable	The box is unchecked by default	Check the Enable box to enable the TCP server configuration.
Host	A Must filled setting	Enter the IP address range of allowed TCP clients.
Save	N/A	Click the Save button to save the configuration

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.

Enable UDP Mode Window		
Item	Value setting	Description
Operation Mode	A Must filled setting	Select UDP mode.
Listen Port	4001 is set by default	Indicate the listening port of UDP connection. Value Range: 1 ~ 65535
Enable	The box is unchecked by default.	Check the Enable box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click Save to save the settings
Undo	N/A	Click Undo to cancel the settings

SpecifyLegal Host IP/FQDN

Legal Host IP/FQDN Definition	
Legal Host IP/FQDN Definition #1	Edit
Legal Host IP/FQDN Definition #2	Edit
Legal Host IP/FQDN Definition #3	Edit
Legal Host IP/FQDN Definition #4	Edit

Legal Host IP/FQDN Definition #1

Remote Host	Specific IP Address 0.0.0.0
Remote Port	0 (1-65535)
Enable	☒ Enable

Legal Host IP/FQDN Definition #1~4		
Item	Value setting	Description
Enable	The box is unchecked by default	Check the Enable box to enable the Cconfiguration.
To Remote Host	A Must filled setting	Enter the IP address range of allowed clients.
Listen Port	1.A Must filled setting	Enter the TCP port number. This is the listen port of the remote TCP server.

4G IIT RTU

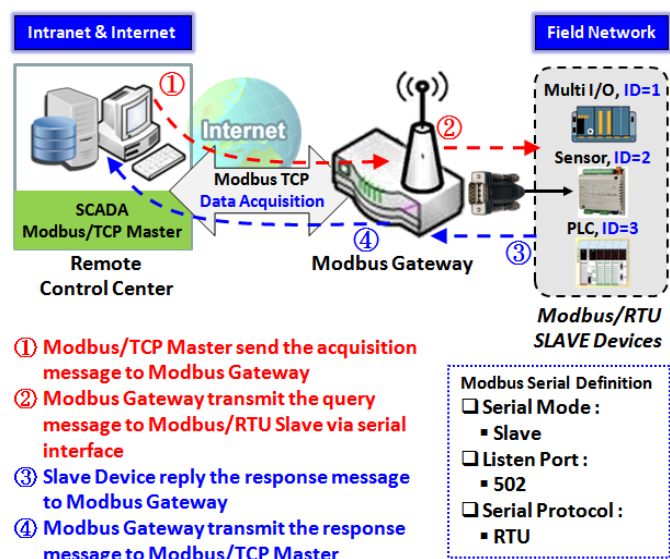
	2.Default value is 4001	<u>Value Range:</u> 1 ~ 65535.
Save	N/A	Click the Save button to save the configuration

3.4.3 Modubs

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 Modbus protocol as the communication standard. It is used to establish master-slave communication between intelligent devices.

However, the Ethernet-based Modbus protocol is so 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.

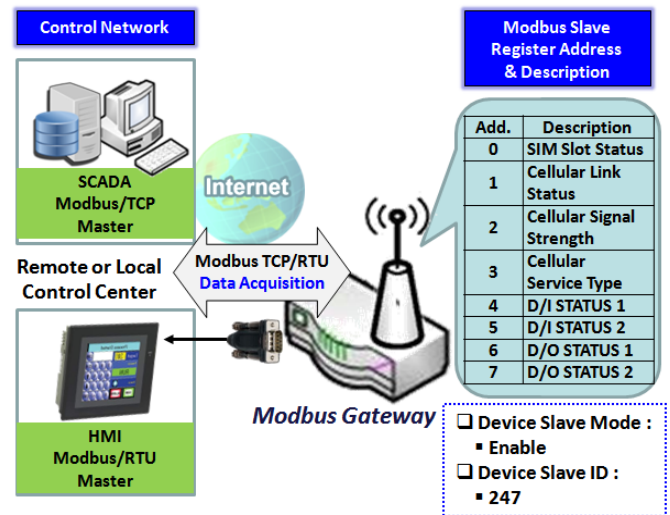
Modbus Gateway Scenario



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

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

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



ModbusSlaveScenario

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

With the Slave option enabled, the Modbus Master device can request the information or sending control

commands to the IoT Gateway, the Modbus TCP/RTU Slave device. And IoT Gateway executes corresponding processes and replies the Modbus Master devices.

When DOM-311-TSO is set to “Modbus” in Port Configuration.

Port Configuration	Modbus
Serial Port Definition	
Operation Mode	Modbus

Modbus Gateway Definition	
Mode	Disable
Device Slave Mode	☐ Enable 1 (1~247)
Listen Port	502 (1~65535)
Serial Protocol	RTU

Modbus Gateway Definition		
Item	Value setting	Description
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 a group of Modbus Slave devices. Disable: Select this to disable the respective Modbus gateway function for the selected serial port. Serial as Slave: Select this when the attached serial device(s) are all Modbus Slave devices. Serial as Master: Select this when the attached serial device is a Modbus Master device.
Device Slave Mode	Disable is set by default	Check the Enable box to activate the integrated Modbus Slave function, and enter the preferred ID for the integrated Modbus slave. So that, 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 Listen Port number if Slave device(s) is attached to the selected serial port. It is a don't care setting if a Master device is attached.

		<u>Value Range:</u> 1 ~ 65535. Note: Use different port number among the serial ports for the product 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.

Gateway Mode Configuration		
Response Timeout	1000	(1~65535 ms)
Timeout Retries	0	(0~5 times)
0Bh Exception	☐ Enable	
Tx Delay	☐ Enable	
TCP Connection Idle Time	300	(1~65535 Sec)
Maximum TCP Connections	1	(1~4 connections)
TCP Keep-alive	☐ Enable	
Modbus Master IP Access	Allow All	
Message Buffering	☐ Enable	

Modbus Gateway Configuration		
Item	Value setting	Description
Response Timeout	1000 ms is set by default	This sets the response timeout of the slave after master request sent. If the slave does not response within the specified time, data would be discarded. This applies to the serially attached Master sent request over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. <u>Value Range:</u> 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 would not buffer Master requests. If a value other than zero is specified, the gateway would store the Master request in the buffer and retries to send the request in a 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 hexcode based-error message will be send instead.

Value Range: 0 ~ 5.		
0Bh Exception	The box is 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 does not respond within the timeout interval.
Tx Delay	The box is unchecked by default.	Check the Enable box to activate to the minimum amount of time after receiving a response before the next message can be sent out. When TxDelay is enabled the Gateway would 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.
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 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 allowed maximum simultaneous TCP connections. Value Range: 1 ~ 4.
TCP Keep-alive	The box is 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.
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 consequently. So that, the buffered Master requests can further be configured to prioritize 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.

Specify Trusted Modbus Masters on the TCP network

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

Modbus Master IP Access	Specific IPs
Trusted IP 1	☐ Enable Specific IP Address 0.0.0.0
Trusted IP 2	☐ Enable Specific IP Address 0.0.0.0
Trusted IP 3	☐ Enable Specific IP Address 0.0.0.0
Trusted IP 4	☐ Enable Specific IP Address 0.0.0.0

Item	Value setting	Description
Source IP	A Must fill 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).
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 in the above. Click the **Edit** button to fill in the priority settings.

Modbus Priority 1	☐ Enable	IP Address	0
Modbus Priority 2	☐ Enable	IP Address	0
Modbus Priority 3	☐ Enable	IP Address	0
Modbus Priority 4	☐ Enable	IP Address	0

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 consequently. So that, the buffered Master requests can further be configured to prioritize 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	User can specify a Modbus identity with IP Address , Slave ID , or Function Code . The buffered Modbus message that matched 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 issued by Master.
Enable	Unchecked by default	Check the Enable box to enable the priority settings.

Supported Function Code for Integrated Modbus Slave

This setting can setup 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
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
157	DO_STATUS_4	R/W	0 : OFF, 1 : ON

Chapter 4 Advance

4.1 Digital Input/Output

Configuration

DI/DO

Action

☒ Enable

Specify Remote UDP hosts Window		
Item	Value setting	Description
Action	The box is unchecked by default	Check the Enable box to enable the DI/DO rule.
Save	N/A	Click Save to save the settings

Digital Input (DI) Profile Configuration

Profile Name

Description

DI Source

DI 1

Continues Update Status

☐ Enable (2~86400s)

Normal Level

Low

Signal Active Time

1 (seconds)

Profile

☒ Enable

Save

Close

Digital Input (DI) Profile Configuration		
Item	Value setting	Description
Profile Name	1. String format 2. A Must filled setting	Specify the DI Profile Name. <u>Value Range</u> :-1 ~ 32 characters.
Description	1. Any text 2. AnOptional setting	Specify a brief description for the profile.
DI Source	ID1 by default	Specify the DI Source. It could be ID1, ID2 or ID3 . The number of available DI source could be different for the purchased product.
Contiune Update Status	The box is 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. <u>Value Range</u> :2 ~86400 seconds. Note : To prevent receving 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. It could be Low or High .
Signal Active Time	1. Numeric String format 2. A Must filled setting	Specify the Signal Active Time. It could be from 1 to 10 seconds. The Signal Active Time setting will be ignored when ' Continue Update Status ' function is enabled <u>Value Range</u> :1 ~10 seconds.
Profile	The box is unchecked by default.	Click Enable box to activate this profile setting.

Digital Output (DO) Profile Configuration

Profile Name	
Description	
DO Source	DO 1
Normal Level	Low
Total Signal Period	(ms)
Repeat & Counter	☐ Enable
Duty Cycle	(%)
Profile	☒ Enable

Save

Close

Digital Output (DO) Profile Configuration

Item	Value setting	Description
Profile Name	1. String format 2. A Must filled setting	Specify the DO Profile Name. <u>Value Range</u> :-1 ~ 32 characters.
Description	1. Any text 2. AnOptional setting	Specify a brief description for the profile.
DO Source	ID1 by default	Specify the DO Source. It could be DO 1 or DO 2 .
Normal Level	Low by default	Specify the Normal Level. It could be Low or High .
Total Signal Period	1. Numeric String format 2. A Must filled setting	Specify the Total Signal Period. <u>Value Range</u> :10 ~10000 ms.
Repeat & Counter	The box is unchecked by default.	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. <u>Value Range</u> :0 ~ 65535.
Duty Cycle	1. Numeric String format 2. A Must filled setting	Specify the Duty Cycle for the Digital Output. <u>Value Range</u> :1 ~100 %.
Profile	The box is unchecked by default.	Click Enable box to activate this profile setting.

Managing Action Configuration

Action Name	
Description	
Event DI	11
Trigger Type	Period
Interval	0 (0~86400 seconds)
Action DO	11
Enable	☒ Enable

Managing Action Configuration

Item	Value setting	Description
Action Name	Blank by default	Specify a name or identifier for this managing event rule. Value Range: 0 ~ 64 characters.
Description	String format : any text.	Enter a brief description for the Managing Event.
Event ID	None by default	Specify the Event type and an event identifier / profile. The supported Event types could be: Digital Input: Select Digital Input and a DI profile you defined to specify a certain Digital Input Event; <i>Note: The available Event Type could be different for the purchased product.</i>
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.
Action DO	None by default	Digital Output: Select Digital Output checkbox and a DO profile you defined as the action for the event; <i>Note: The available Event Type could be different for the purchased product.</i>
Enable	The box is unchecked by default.	Click Enable box to activate this Managing Event setting.

4.2 Data to Server

4.1.1 RESTful

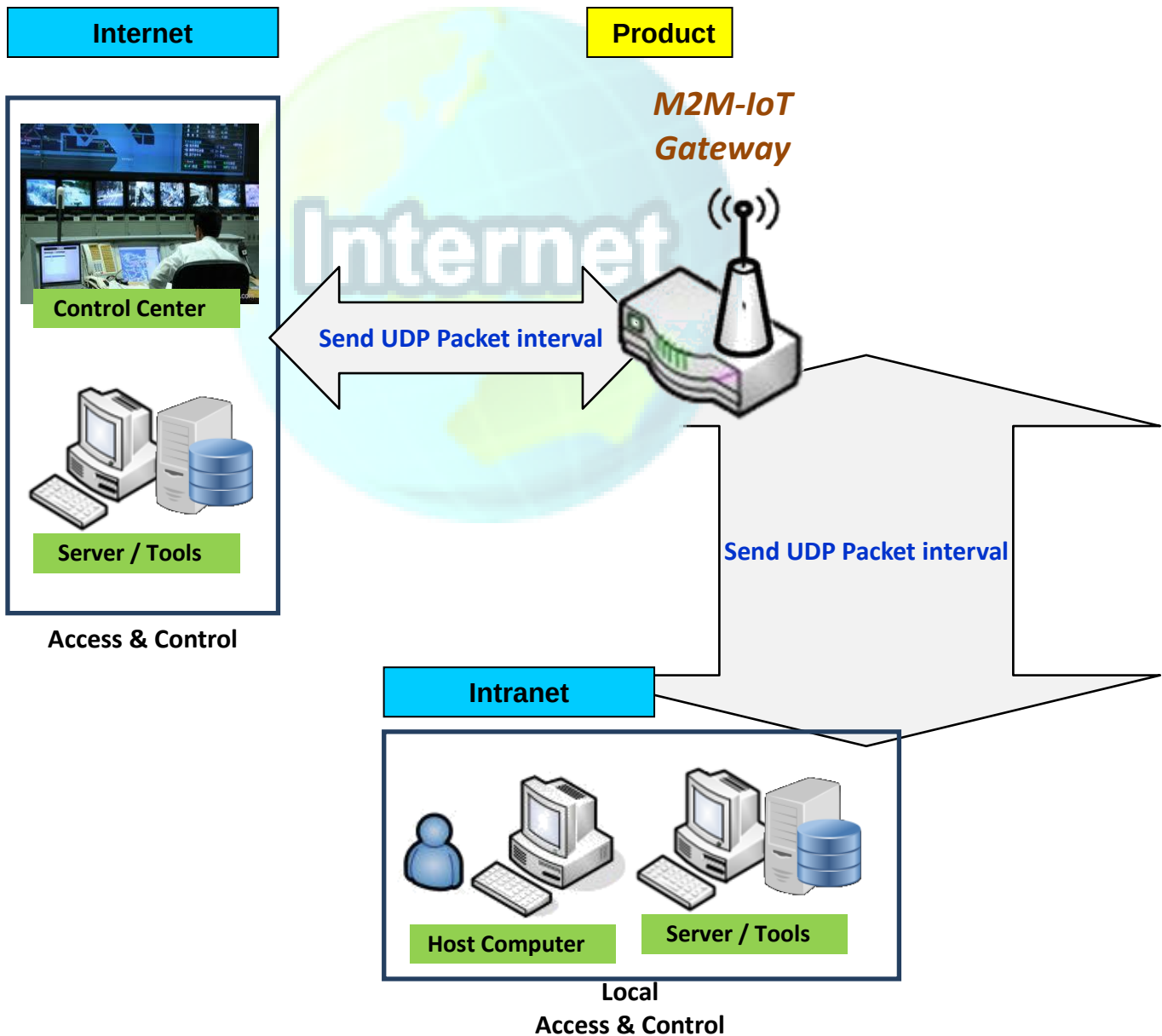
RESTful API is an interface that two computer systems use to exchange information securely over the internet or Local Network. The user can use PC with installed Node.js to connect the device, then get some information via RESTful API.

Configuration	
RESTful API	☒ Enable
Interface	
Port Number	0 (1~65535)

RESTful		
Item	Value setting	Description
RESTful	The box is unchecked by default	Check the Enable box to activate this RESTful function
Interface	A Must filled setting	Define the physical interface WAN/LAN to be used.
Port Number	A Must filled setting	Specify the Port for RESTful function to use. <u>Value Range: 1 ~ 65535.</u>

4.1.2 Heartbeat

Heartbeat is very simple and useful function. Based on UDP Format packet to send specific host on Internet or in Private Network. This function is also used to check if the mobile device receives good-signal in specific-area, especially it can send packet every sec.



RESTful	Heartbeat	MQTT
Configuration		
Heartbeat	☒ Enable	

Heartbeat Settings Rule Configuration	
Name	
Send Type	TCP v
IP Address / FQDN	
Port Number	5000 (1~65535)
Interval	60 (s)
Prefix Message	
Device Options	☒ Timestamp ☒ SN ☒ IMEI ☒ Cellular Info ☒ DI1 ☒ DI2 ☒ DI3 ☒ DO1 ☒ DO2
Heartbeat	☐ Enable

Save

Close

Heartbeat Item	Value setting	Description
Name	1. String format can be any text 2. A Must filled setting	Enter a packet filter rule name. Enter a name that is easy for you to remember. Value Range: 1 ~ 30 characters.
Send Type	A Must filled setting	TCP , UDP or Both
IP Address /FQDN	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.
Port Number	A Must filled setting	Specify UDP Port to send specific Server. Value Range: 1 ~ 65535.

4G IIT RTU

Interval	The value is 300 by default	Specify the time interval. <u>Value Range:</u> 10 ~ 86400 sec.
Prefix Message	1. String format 2. An optional filled setting	Specify the Prefix Message string as pre-defined identification for accessing the remote host, if required. <u>Value Range:</u> -1 ~ 32 characters.
Device Options.	Un-checked by default	Check which information of Device to send: Timestamp, SN, IMEI, Cellular Info and DI/DO Status
Enable		

4.1.3 MQTT

MQTT (Message Queuing Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe based messaging protocol. It works on top of the TCP/IP protocol. MQTT is a simple messaging protocol, designed for constrained devices with low-bandwidth. So, it's the perfect solution for IoT applications.

Play as a MQTT Client

The gateway supports MQTT Client function. It can play as a MQTT client and publish message to MQTT broker, or subscribe interested topic(s) from MQTT Broker(s).

RESTful	Heartbeat	MQTT
MQTT Client Function		
MQTT Client	☒ Enable	

MQTT Client Configuration

Connection Name	
Address	
Port Number	(1~65535)
Authentication	☐ Enable
Security	None
Client ID	
Keep Alive	60 (5~86400 Sec)
Enable	☐ Enable

Save

Close

MQTT Client Configuration		
Item	Value setting	Description
Connection Name	The box is unchecked by default.	Specify a name as the identifier of the MQTT Client. It can be identified with the Broker Name, or interested message (topic) Value Range: 1 ~ 64 characters.
Address	1. A Must-filled setting. 2. Blank by default	Specify the host name or IP address of the MQTT broker that the client is going to publish message to it, or subscribe messages from it.
Port Number	1. An Optional setting.	Specify a port as the port for MQTT connection. Value Range: 1 ~ 65535.
Authentication	1. An Optional setting. 2. The box is unchecked by default.	Check the box if user (account) authentication is required for subscribing the MQTT messages. With the box checked, you have to further specify Username and Password for the connection.
Security	1. An Optional setting. 2. None is set by default	Select the security scheme for the MQTT connection. None: no encryption is involved for the MQTT connection. SSL/TLS: SSL/TLS encryption is applied for security. You have to further specify required certificate files. Note: If SSL/TLS is selected, the listen port will be changed to 8883 accordingly by default.
Certificate	1. An Optional setting. 2. None is set by default	Select CA File / CERT File / Key File from the dropdown lists. If you don't have available items in the dropdown list, you have to define or create it first. Please refer to Object Definition>Certificate>Trusted Certificate .

		CA File could be defined in Trusted Certificate List. CERTFile could be defined in Trusted Client Certificate List. KEYFile could be defined in Trusted Client Key List.
Client ID	1. A Must-filled setting. 2. ID with device MAC is set by default	Specify an unique ID for the MQTT client. By default the MAC address is used as the ID string.
Keep Alive	1. An Optional setting. 2. 60 sec is set by default.	Specify a keep alive interval to keep the connection alive while the connection is idle. Value Range: 5 ~ 86400sec.
Enable	The box is unchecked by default.	Check the box to activate this MQTT Client configuration

Publish Message Configuration screen will appear.

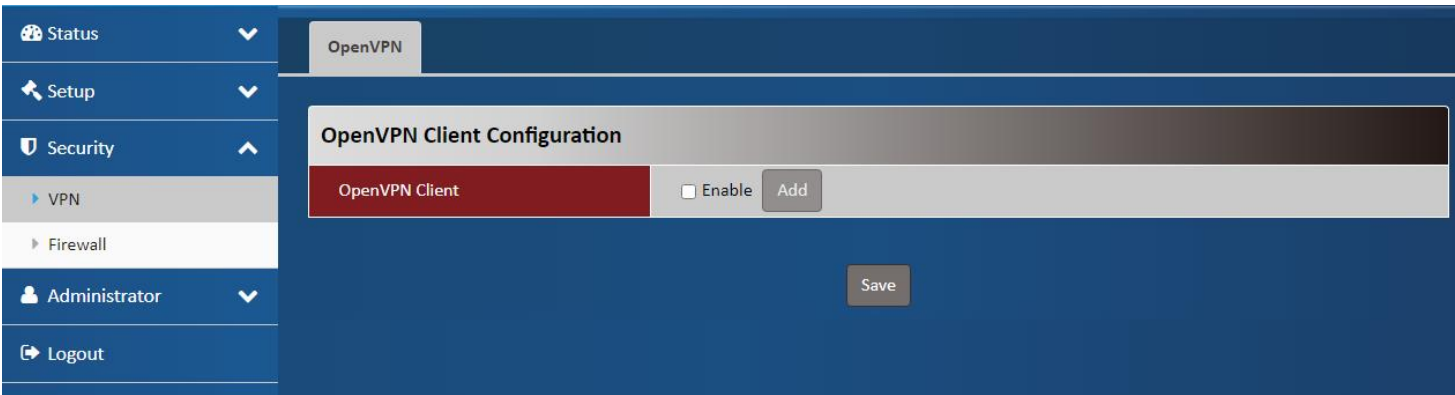
Publish Message Configuration

Topic	
Topics prefix	☐ Enable
Message Style	☒ Manual ☒ Timestamp ☒ SN ☒ IMEI ☒ Cellular Info ☒ DI1 ☒ DI2 ☒ DI3 ☒ DO1 ☒ DO2
Message	
QoS	☒ 0 (At most once) ☐ 1 (At least once) ☐ 2 (Exactly once)
Retained	☐ Enable
Publish Behavior	☐ Auto Publish
Enable	☐ Enable

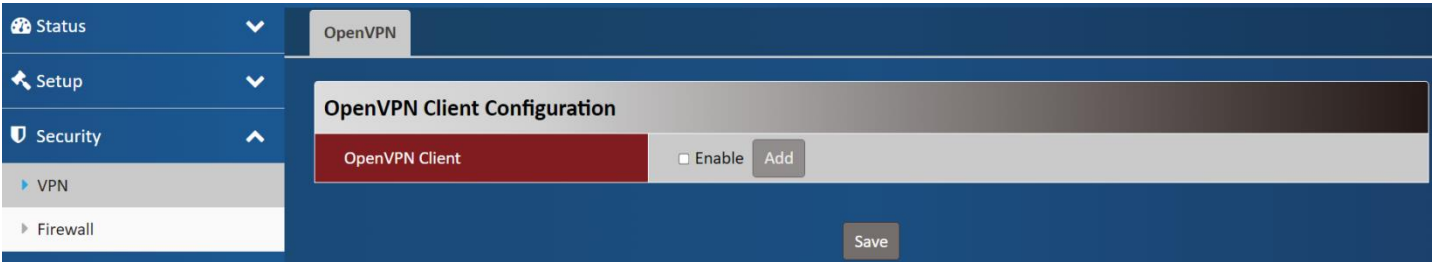
Publish Message Configuration		
Item	Value setting	Description
Topic	1. A Must-filled setting. 2. Blank by default	Specify the topic for the message to be published. Value Range: 1 ~ 64 characters, including the topiclevel separator '/', but excluding the wildcards '+' and '#'.

Topic prefix	The box is unchecked by default.	Check the box to add the predefined topic prefix into a MQTT message.
Message Style	1. An Optional-filled setting. 2. Manual is selected by default	Select a message style from the dropdown list. The supported styles are : Manual : The message is create manually, and you can specify the message content below. System Log : The message to be published are the System log of the device. Data Logging : The message to be published are the Data Logging recorded in the designated storage
Message	1. A Must-filled setting. 2. Blank by default	Specify the message content for the Manual publish message. Value Range : 1 ~ 256 characters.
QoS	1. An Optional setting. 2. 0 (At most once) is set by default	Select the QoS type for publishing a message. 0 (At most once) : the message will be published only once, and the broker and subscribed client(s) take no additional steps to acknowledge the delivery, no matter it is received or not. 1 (At least once) : the message will be published at least once until acknowledgement is received from the broker or subscribed client(s). 2 (Exactly once) : the message will be published to subscriber(s) once in a two-level handshake to ensure only one copy of the message is received.
Retained	The box is unchecked by default.	Check the box to activate this message retaining function.
Publish Behavior	The box is unchecked by default.	Check the box(es) for the expected publish behavior: Auto Publish : auto publish a message with specified time interval (1~65535 sec). When the Message or Data variation more than □lines. : publish a new message that varies from previous one for specified changes. Note: if Message style is set to Manual, only Auto Publish is available.
Enable	The box is unchecked by default.	Check the box to activate this publish message configuration.

Chapter 5 Security

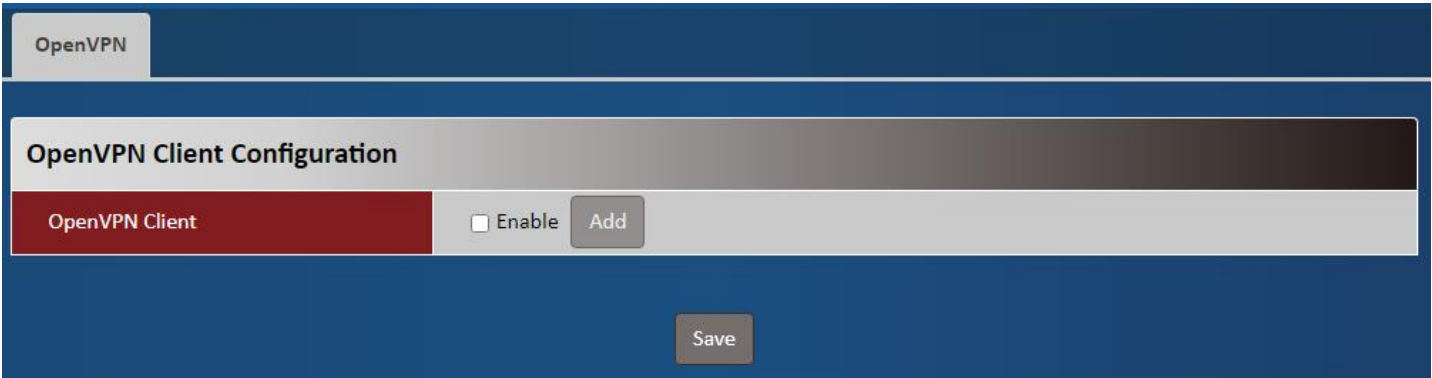


5.1 VPN



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

5.1.1 OpenVPN



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

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	lv4fXUZA1ssMXoV2lwpXWoOStYRR2ChLK0drfaoeJCA= -----END RSA PRIVATE KEY-----	
Encryption Cipher	Blowfish	
Hash Algorithm	SHA-1	
LZO Compression	Adaptive	
Persist Key	☐ Enable	
Persist Tun	☐ Enable	
Additional Configuration		
Tunnel	☒ Enable	

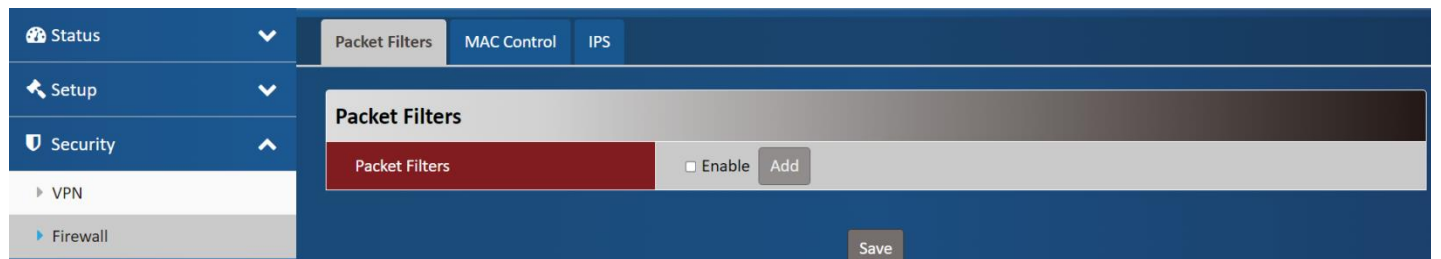
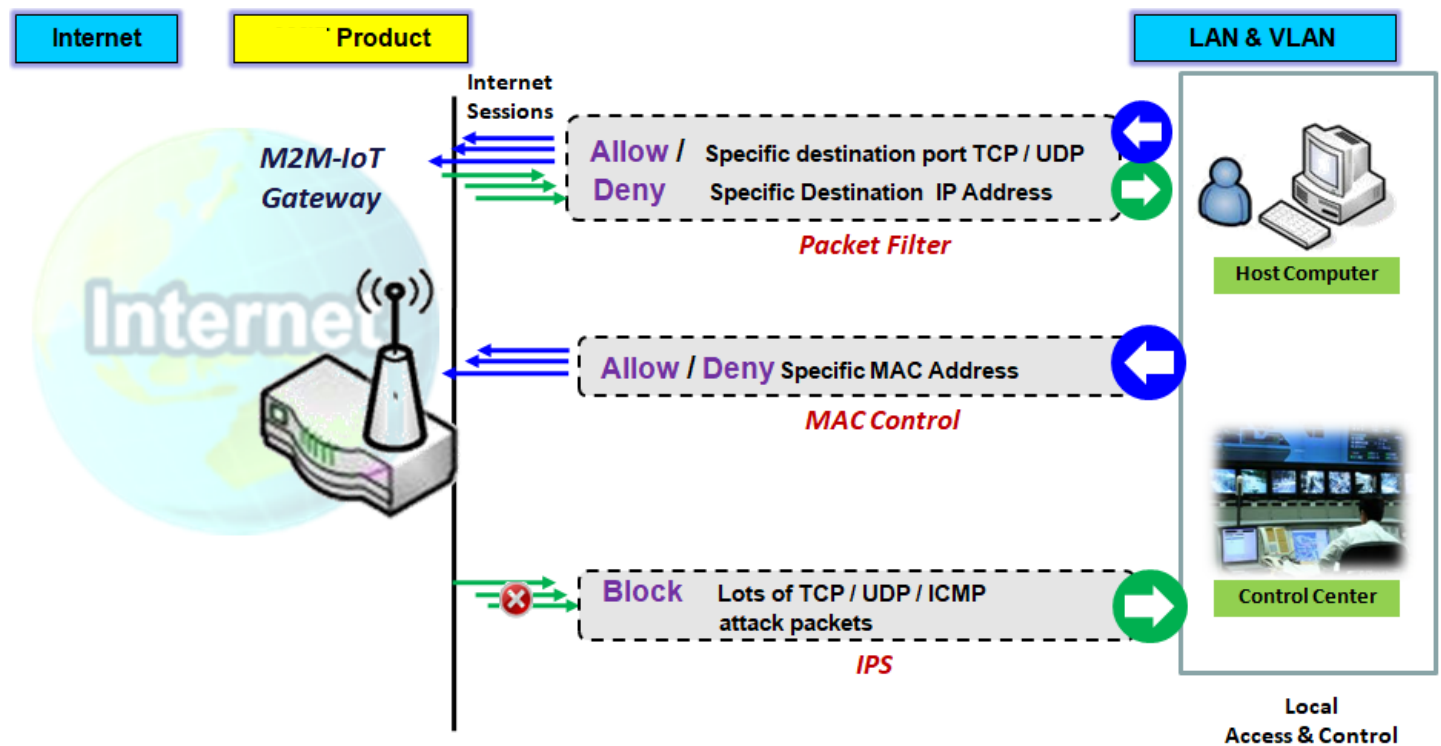
Save

Close

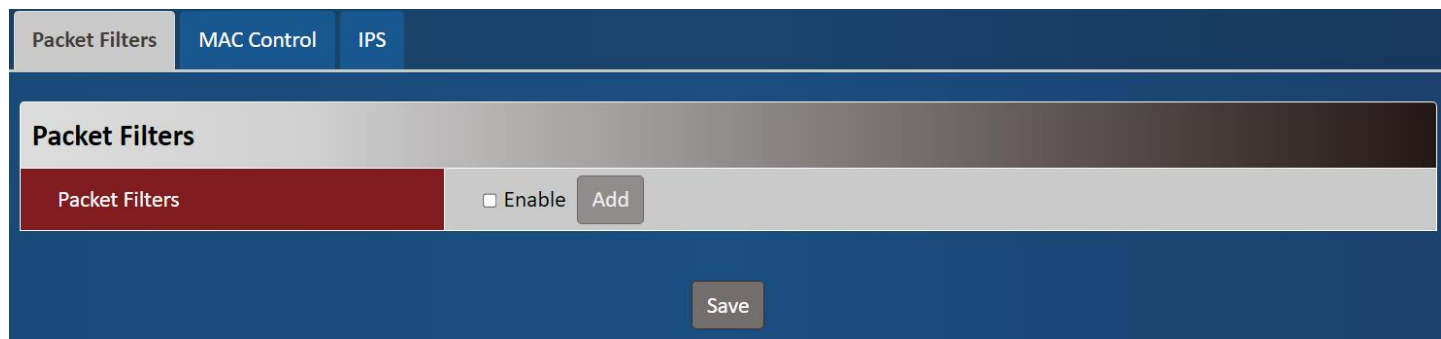
OpenVPN Client Rule Configuration Page		
Item	Value setting	Description
Name	1. String format can be any text	The name of current rule

	2. A must-fill setting	
Protocol	1. A must-fill setting 2. 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 2. 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 be SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable .
LZO Compression	By default Adaptive is selected.	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.

5.2 Firewall



5.2.1 Packet Filters



Packet Filters		
Item	Value setting	Description
Packet Fliters	The box is unchecked by	Check the Enable box to activate this Packet Fliter function

default

Click **Add** will pop-up **Packet Filter Rule Configuration** page

Packet Filter Rule Configuration

Name	test	
Source IP	IP Range 192.168.123.200 - 192.168.123.250	
Destination IP	Specific IP Address 195.165.124.33	
Source Interface	Any	
Destination Interface	Any	
Source MAC	AA:BB:CC:EE:DD:FF	
Protocol	Any	
Source Port	Any	
Destination Port	Single Port 80	
Time Schedule	(0) Always	
Rule	☒ Enable	

Save

Close

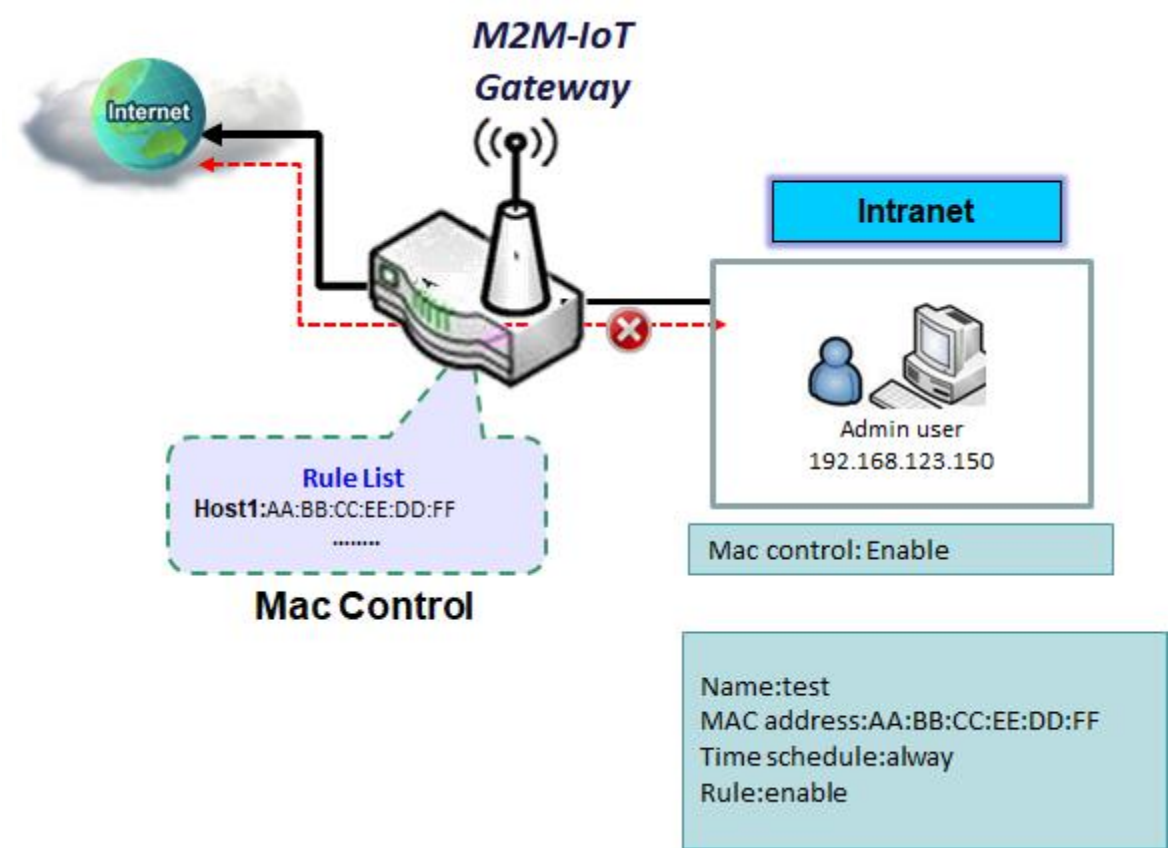
Packet Filter Rule Configuration		
Item	Value setting	Description
Name	1. String format can be any text 2. A must-fill setting	Enter a packet filter rule name. Enter a name that is easy for you to remember.
Source ip	1. A must-fill setting 2. By default Any is selected	This field is to specify the Source 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 LAN for 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 filled 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

5.2.2 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



Packet Filters MAC Control IPS

MAC Control

MAC Control ☐ Enable Add

Save

MAC Control 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

Name	test
MAC Address	AA:BB:CC:EE:DD:FF
Time Schedule	(0) Always
Rule	☒ Enable

Save

Close

Mac Control Rule Configuration		
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 filled 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

5.2.3 IPS

Packet Filters
MAC Control
IPS

IPS

IPS	☐ Enable
SYN Flood Defence	☐ Enable
SYN Flood Threshold	0 (100~10000)
Ping Flood Defence	☐ Enable
Ping Flood Threshold	0 (100~10000)
UDP Flood Defence	☐ Enable
UDP Flood Threshold	0 (100~10000)
Block Smurf Attack	☐ Enable
Block Land Attack	☐ Enable
Block Fraggle Attack	☐ Enable
Block Ping Of Death Attack	☐ Enable
Block Traceroute	☐ Enable

Save

IPS Page Item	Value setting	Description
IPS	The box is unchecked by default	Check the Enable box to activate this IPS function
Log enable	The box is unchecked by default	Check the Enable box to activate to activate Event Log.
SYN Flood Defense	The box is unchecked by default	Check the Enable box to activate this SYN Flood Defensefunction
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 Defence	The box is unchecked by default	Check the Enable box to activate this Ping Flood Defencefunction
Ping Flood Threshold	1. A must-fill setting	Specify the value range to block

	2. Traffic threshold is set to 0 by default 3. The value range can be from 100 to 10000.	
UDP Flood Defence	The box is unchecked by default	Check the Enable box to activate this UDP Flood Defencefunction
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 Attackfunction
Block Snork Attack	The box is unchecked by default	Check the Enable box to activate this Block SnorkAttackfunction
Block Land Attack	The box is unchecked by default	Check the Enable box to activate this Block Land Attackfunction
Block Fraggle Attack	The box is unchecked by default	Check the Enable box to activate this Block FraggleAttackfunction
ICMP Defender	The box is unchecked by default	Check the Enable box to activate this ICMP Defenderfunction
Unknown Protocol Defence	The box is unchecked by default	Check the Enable box to activate this Unknown Protocol Defencefunction
Block Ping Of Death Attack	The box is unchecked by default	Check the Enable box to activate this Block Ping Of Death Attackfunction
Block ICMP Fragment Attack	The box is unchecked by default	Check the Enable box to activate this Block ICMP Fragment Attackfunction
Block SYN Fragment Attack	The box is unchecked by default	Check the Enable box to activate this Block SYN Fragment Attackfunction
Block Traceroute	The box is unchecked by default	Check the Enable box to activate this Block Traceroutefunction
Block Teardrop Attack	The box is unchecked by default	Check the Enable box to activate this Block Teardrop Attackfunction
TCP Abnormal Attack	The box is unchecked by default	Check the Enable box to activate this TCP Abnormal Attackfunction
IP Spoofing Defence	The box is unchecked by default	Check the Enable box to activate this IP Spoofing Defencefunction

Chapter 6 Administrator

6.1 Manager

D-Link

Status

Setup

Advance

Security

Administrator

Manager

Utility

Logout

FW Upgrade

Password & MMI

Reboot & Reset

SSH

Remote Administrator

Device Management

Firmware Information

FW Version

1.00.00

FW Date

2024/07/10

Firmware Upgrade

FW Path

選擇檔案 未選擇任何檔案

Upgrade Action

Upgrade

6.1.1 FW Upgrade

Firmware Information

FW Version

1.00.00

FW Date

2024/07/10

Firmware Upgrade

FW Path

選擇檔案 未選擇任何檔案

Upgrade Action

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		
Backup Configuration Settings	Download Via Web UI	

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. Download: for backup the device configuration to a config.bin file. Upload: for restore a designated configuration file to the device. Via Web UI: to retrieve the configuration file via Web GUI.

6.1.2 Password & MMI

Username	
Username	admin
New 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	
Old Password	
New Password	
New Password Confirmation	

(NOTE: The password must be at least 10 characters long, and must contain at least 1 English letter and 1 number. The password cannot be the same as the login account.)

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	
Login	Password-Guessing Attack & MAX: 3 (times)
Login Timeout	☐ Enable 300 (seconds)

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 <i>"Already reaching maximum Password-Guessing times, please wait a few seconds!"</i> 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.
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 .

6.1.3 Reboot & Reset

FW Upgrade	Password & MMI	Reboot & Reset	SSH	Remote Administrator	Device Management
System Operation					
Reboot		Now Reboot			
Reset to Default		Reset			
Save					

System Operation Item	Value setting	Description
Reboot	Now is selected by default	Click 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.

6.1.4 SSH

FW Upgrade

Password & MMI

Reboot & Reset

SSH

Remote Administrator

Device Management

Configuration

SSH

LAN ☒ Enable WAN ☐ Enable Service Port : 22

Save

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.

6.1.5 Remote Administrator

FW Upgrade

Password & MMI

Reboot & Reset

SSH

Remote Administrator

Device Management

Remote Administrator Host Definition

Remote Administrator Host Definition

Add

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

Rule Configuration

Name		
Protocol	HTTP ▼	
Remote IP	Any IP ▼	
Subnet Mask	255.0.0.0 (/8) ▼	
Service Port	80	
Rule	☐ Enable	

Save

Close

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.

6.1.6 Device Management

Configuration

Device Management	☐ Enable
Input Service URL	
Input Server IP STUN traffic	
Self-Certification	☒ Enable

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 nameURL
Input server IP STUN traffic	Blank is set by default	Specify ANMS serverpublicip or domain name
Self-certification	The Enable box is checked by default	Check the Enable box to activate this Self-certification function

6.2 Utility

Status

Setup

Security

Administrator

Manager

Utility

Logout

SMS

SMS Service

SMS	☐ Enable
SMS Storage	SIM
Free Space	0 (0-10)
Event Management	☐ Enable <button>Edit</button>
SMS Forward Management	☐ Enable <button>Edit</button>

6.2.1 SMS

SMS Service

SMS	☐ Enable
SMS Storage	SIM
Free Space	0 (0-10)
Event Management	☐ Enable <button>Edit</button>
Message Prefix	☐ Enable

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
Message Prefix	The box is unchecked by default	Click the Enable box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to 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.

Account Configuration

Phone Number#1

Application

☐ Managing ☐ Notifying

Enable

☐

Phone Number#2

Application

☐ Managing ☐ Notifying

Enable

☐

Managing Events

Cellular Status

☐ Enable

Cellular Reconnect

☐ Enable

Reboot

☐ Enable

Notifying Events

Cellular Connected

☐ Enable

Save

Close

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
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
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	Enable the option and user can query the current connection status via sending SMS “ status ” from specify phone number which enables managing function.
Cellular Reconnect	The box is unchecked by default	Enable the option and user can force the current connection re-connect once via sending SMS “ reconnect ” from specify phone number which enables managing function.
Reboot	The box is unchecked by default	Enable the option and user can force the device reboot once via sending SMS “ reboot ” from specify phone number which enables managing function.

Notifying Events		
Item	Value setting	Description
Cellular Connected	The box is unchecked by default	Enable the option will send a SMS to show “ WAN Link UP-IP:xxx.xxx.xxx.xxx ” to specify phone number which enable Notifying function when cellular WAN establishes a connaction.

SMS Summary		
New SMS	0	
Received SMS	0	
Action	New SMS SMS Inbox	

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-upnewsms page Click sms inbox will pop-up sms inbox page

New SMS

Receiver

(Use '+' for International Format and ';' to Compose Multiple Rec eivers)

Text Message

Current Input Length: 0/512

Action

Send

Clear

Close

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		Clickthe Send button, above text message will be sent as a SMS. Clickthe Clear button, toclear text message

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

6.2.2 Command Script

Command Script

Command Script

0 / 4096

Enable

☐ Enable

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.