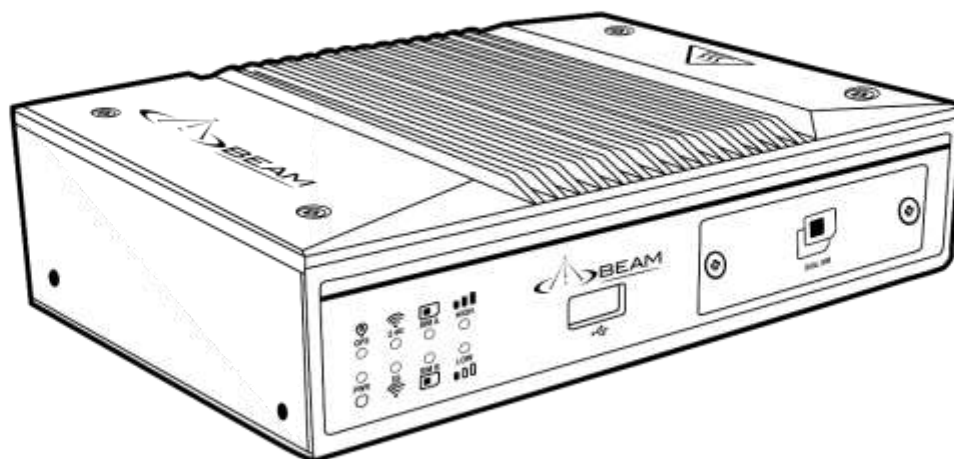




MG400 LTE Gateway

User Manual



Important Notice

The transmission and reception of data via wireless communications cannot be guaranteed because of the nature of wireless communications. Wireless data may be delayed or lost. Therefore, it is not recommended to use the MG400 in situations where emergency communications are required. Beam are not responsible for failure of delays or errors in wireless data transmitted or received by the MG400 and the damages caused by such failure.

Hazards and Safety

IMPORTANT! Please read the following information carefully before installing and using the MG400.

In a hazardous area: Do not connect or disconnect any cables (power cable, RJ45, digital input/output, serial, earthing, ignition, RF SMA). Do not plug in or unplug SIM cards or USB storage. Do not use the Reset button.

WARNING: Do not disassemble the MG400 or its accessories. There are no user-serviceable parts inside the MG400 or its accessories.

The design of the MG400 complies with international safety and radio standards. Refer to Appendix D – Compliance for safety standards. Do not operate the MG400 in an area near to equipment which is susceptible to radio interference, i.e. medical equipment, life support equipment, pacemakers, hearing aids, blasting caps and areas, aircrafts and airports. In such areas, the MG400 needs to be powered off.

For vehicle applications, do not place or install the MG400 in the area near or over an air bag or in the air bag deployment area. Mount the MG400 safely before driving your vehicle. Connection to the vehicle electrical system should be carried out by trained professional only. While driving, full attention always needs to be given, complying with local laws and regulations.

Small children

Do not leave the MG400 or its accessories within the reach of small children.

Accessories and external high gain antennas

Only use BEAM approved accessories with the MG400. Do not connect to incompatible products or accessories.

The MG400, with standard antennas in the package, complies with radio safety standards. Refer to Appendix D – Compliance for details. If external high gain antennas are required, it is recommended to select the antennas supplied by Beam. Antennas need to be installed with a separation distance of at least 20 cm from all persons. The antennas also needs to be isolated from any other transmitter or antennas. Before installing external high gain antennas, please read the body separation guidelines in the antenna installation guide.

COPYRIGHT

Copyright© 2019 Beam Holdings Limited. All rights reserved.

Trademark

Trademarks and registered trademarks are the property of Beam Holdings Limited or their respective owners.

Document history

This manual covers the following product:

Beam MG400 LTE Gateway

REVISION	CHANGE DESCRIPTION	DATE
01	MG400 User Manual	SEP 2019

Specifications are subject to change without notice.

Images shown may vary slightly from the actual product.

Overview	11
Target readers.....	11
1 Introduction	12
1.1 Standard package contents.....	12
1.2 MG400 overview	13
1.2.1 Front panel	13
1.2.2 Back panel.....	15
1.3 Installation.....	16
1.3.1 System requirement	16
1.3.2 Hardware installation.....	16
1.3.2.1 Important notes on installation.....	16
1.3.2.2 Mounting the unit	17
1.3.2.3 Inserting the SIM cards.....	18
1.3.2.4 Connecting terminal block	18
1.3.2.5 Connecting Ethernet ports.....	19
1.4 Connecting PC to MG400.....	20
1.4.1 Connecting via Wi-Fi.....	20
1.4.2 Connecting via Ethernet cable	20
1.4.3 Accessing the web GUI	20
2. Status.....	26
2.1 Dashboard	26

2.2 Network.....	28
2.2.1 WAN & Uplink.....	28
2.2.2 LAN & VLAN	33
2.2.3 Wi-Fi.....	34
2.2.4 DDNS.....	37
2.3 Security.....	38
2.3.1 VPN	38
2.3.2 Firewall	41
2.4 Administration	46
2.4.1 Remote Management.....	46
2.4.2 Log Storage	47
2.4.3 GNSS.....	47
2.5 Usage	48
2.5.1 Connection Records	48
2.5.2 Network Traffic.....	48
2.5.3 Login Info.....	49
2.5.4 Hotspot Usage	50
2.5.5 Cellular Usage.....	51
2.5.6 Cellular Signal.....	52

3. Network	53
3.1 WAN & Uplink	53
3.1.1 Physical Interface	53
3.1.2 Connection Setup	54
3.1.2.1 3G/4G WAN Connection Setup	54
3.1.2.2 Ethernet WAN Connection Setup	65
3.1.2.2.1 Static IP	67
3.1.2.2.2 Dynamic IP	67
3.1.2.2.3 PPPoE	68
3.1.2.2.4 PPTP	69
3.1.2.2.5 L2TP	71
3.1.2.3 Wi-Fi WAN Connection Setup	72
3.1.3 Load Balance	75
3.2 LAN & VLAN	79
3.2.1 Ethernet LAN	79
3.2.2 VLAN	81
3.2.3 DHCP Server	90
3.3 Wi-Fi	97
3.3.1 Wi-Fi Module One	97
3.3.2 Wi-Fi Module Two	108
3.3.3 Wireless Client List	117
3.3.4 Advanced Configuration	118
3.3.5 Wi-Fi as WAN	120
3.4 IPv6	125

3.5 Port Forwarding	133
3.5.1 Configuration.....	133
3.5.2 Virtual Server & Virtual PC	133
3.5.3 Special AP & ALG	136
3.5.4 DMZ & Pass Through	139
3.6 Routing	140
3.6.1 Static Routing	140
3.6.2 Dynamic Routing.....	142
3.6.3 Routing Information.....	147
3.7 DNS & DDNS	150
3.8 QoS	153
4. Serial Port.....	159
4.1 Bus & Protocol.....	159
4.1.1 Port Configuration	159
4.1.2 Virtual COM	159
5. User Rule	167
5.1 Scheduling.....	167
5.2 User	169
5.2.1 User List	169
5.2.2 User Profile	169
5.2.3 User Group	172
5.3 Grouping.....	174
5.4 External Servers	176

5.5 Certificate	179
5.5.1 Configuration.....	179
5.5.2 My Certificate	181
5.5.3 Trusted Certificate.....	183
5.5.4 Issued Certificate.....	187
6. Security	189
6.1 VPN	189
6.1.1 IPSec	189
6.1.2 OpenVPN	199
6.1.3 L2TP.....	211
6.1.4 PPTP	217
6.1.5 GRE.....	222
6.1.6 EoGRE.....	224
6.2 Firewall.....	228
6.2.1 Packet Filter	228
6.2.2 URL Blocking.....	232
6.2.3 Content Filter.....	234
6.2.4 MAC Control	237
6.2.5 Application Filter	238
6.2.6 IPS.....	242
6.2.7 Options	245
6.3 Authentication	247
6.3.1 Hotspot Services	247
6.3.2 MAC Authentication.....	250

7. Service.....	253
7.1 Cellular Toolkit	253
7.1.1 Data Limit.....	253
7.1.2 SMS	254
7.1.3 SIM PIN	259
7.1.4 USSD	262
7.1.5 Network Scan	264
7.2 Event Handling	266
7.2.1 Configuration.....	266
7.2.2 Managing Events.....	273
7.2.3 Notifying Events	276
7.3 Location Tracking.....	279
7.3.1 GNSS.....	279
7.3.2 Track Viewer	282
7.4 Power Control	286
8. Administration.....	287
8.1 Remote Management	287
8.1.1 Command Script.....	287
8.1.2 TR-069	290
8.1.3 SNMP	293
8.1.4 Telnet & SSH	302

8.2 System Operation	305
8.2.1 Password & MMI	305
8.2.2 System Information	308
8.2.3 System Time	309
8.2.4 System Log	316
8.2.5 Backup & Restore	319
8.2.6 Reboot & Reset	319
8.3 FTP	321
8.3.1 Server Configuration	321
8.3.2 User Account	322
8.4 Diagnostic	324
8.4.1 Packet Analyzer	324
8.4.2 Diagnostic Tools	326
Appendix	328
Appendix A – GPL Written Offer	328
Appendix B – Product handling	333
Appendix C – BEAM Warranty Terms and Conditions	334
Appendix D – Compliance	335

Overview

This manual provides the information users need to set up, configure, and operate the MG400.

Target readers

This document is intended for system integrators and experienced hardware installers who understand telecommunications and networking terminology.

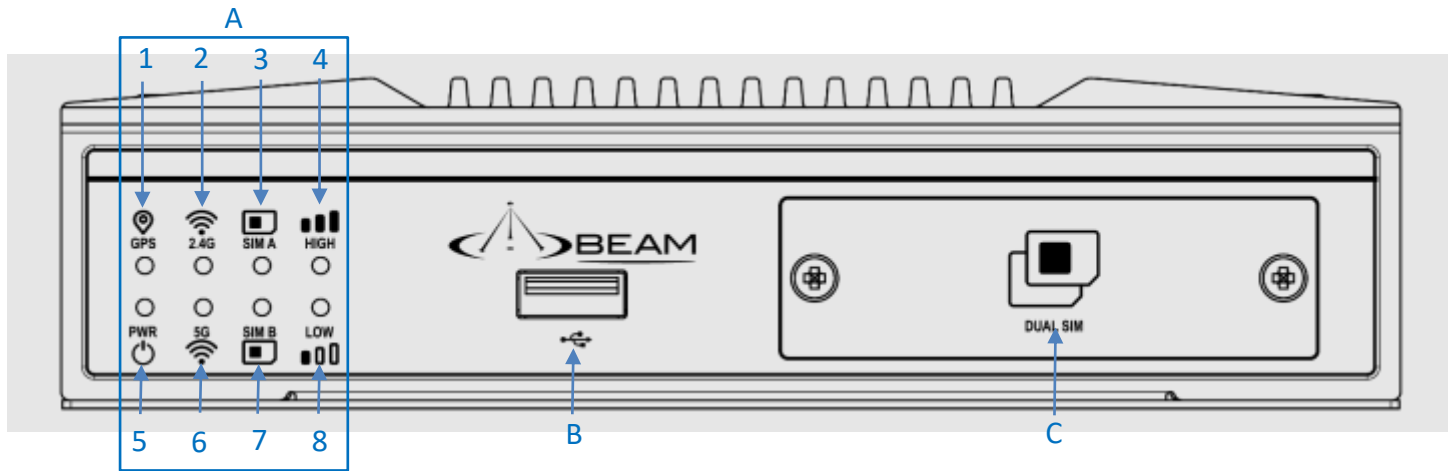
1 Introduction

1.1 Standard package contents

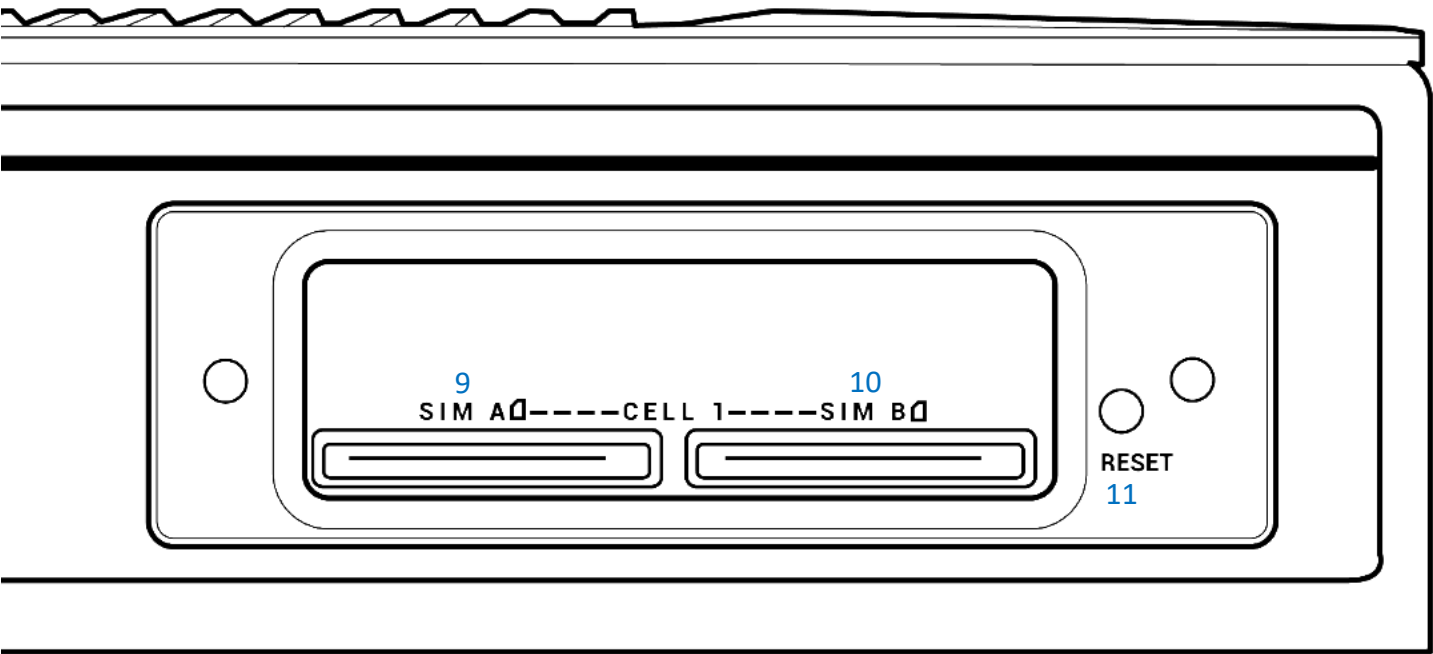
- 1 x MG400 LTE Gateway
- 2 x Wi-Fi antenna
- 2 x LTE antenna
- 1 x 8PIN Terminal block
- 1 x AC power adapter with AU plug
- 1 x Fused DC power cable with IGN (ignition wire)
- 2 x Mounting bracket
- 1 x Screw bag (Zinc grounding screw x 1, Black screw x 3)
- 1 x Quick Start Guide
- 1 x Spare device label

1.2 MG400 overview

1.2.1 Front panel

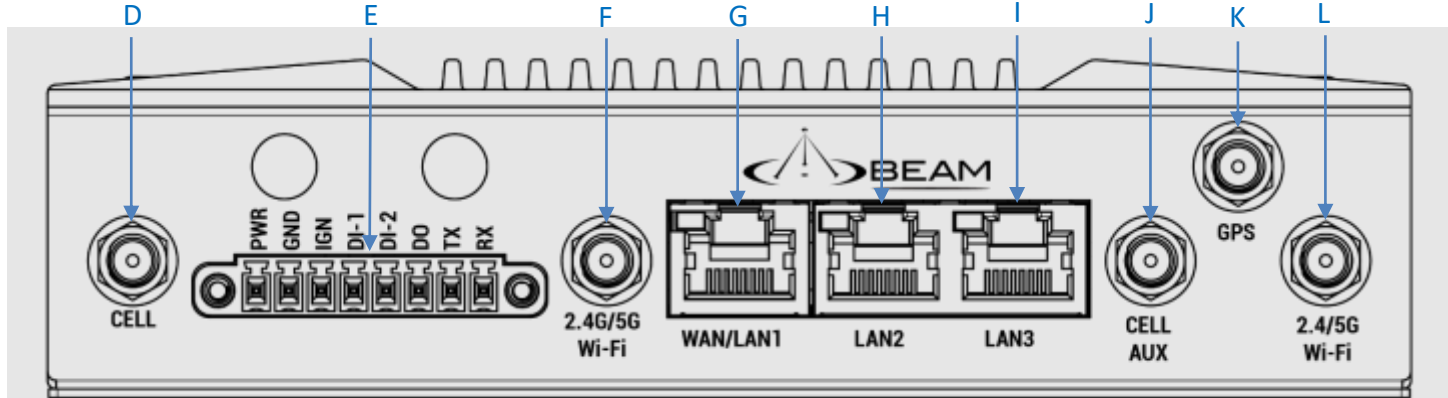


#	Description	Notes
A	Status LED	Indicates the MG400 status
B	USB PORT	Connect a USB memory stick.
C	SIM CARD SLOT	Covers 2 x SIM slots and the reset button.
1	GPS	Connect a active GPS antenna. OFF: GPS function is disabled, GPS antenna is disconnected, or there is no GPS signal. Steady ON: GPS signal is locked. Flashing: the MG400 is searching for GPS signal, no GPS lock
2	2.4G Wi-Fi	OFF: 2.4GHz Wi-Fi is disabled. Steady ON: 2.4G Wi-Fi is enabled. Fast Flashing: Data is transferring through 2.4G Wi-Fi.
3	SIM A in use	OFF: SIM card A is not inserted or not used for 3G/4G connection. ON: SIM card A is inserted and active.
4	LTE signal high	ON: 3G/4G network is connected, signal strength is at high level $\geq 50\%$
5	Power	OFF: MG400 is powered OFF or in standby mode. Steady ON: MG400 is in working mode. Slow Flashing: Firmware is upgrading, or MG400 is in Delay OFF mode Fast Flashing: Firmware is upgrading, or MG400 is in recovery mode.
6	5G Wi-Fi	OFF: 5G Wi-Fi is disabled. Steady ON: 5G Wi-Fi is enabled. Fast Flashing: Data is transferring through 5G Wi-Fi.
7	SIM B in use	OFF: SIM card B is not inserted or not used for 3G/4G connection. ON: SIM card B is inserted and active.
8	LTE signal low	ON: 3G/4G network is connected, signal strength is at low level $< 50\%$



#	Description	Notes
9	SIM A	For 2FF, mini SIM
10	SIM B	For 2FF, mini SIM
11	Reset Button	Reset the MG400 to factory default settings by holding the reset button down for at least 6 seconds then release.

1.2.2 Back panel



#	Description	Notes
D	LTE antenna port main	Connect LTE antenna. If only one antenna being used, ensure it is connected to this port.
E	Terminal block	<p>Connect Terminal block. The Terminal Block provides the following:</p> <p>PWR (Power): supports 9V – 36V DC power input.</p> <p>GND (Ground): Terminal for ground wire connection.</p> <p>IGN (Ignition): Terminal used to connect to the ignition sense wire of a vehicle.</p> <p>DI-1 (Digital Input 1): Trigger voltage (high): 5V to 30V. Trigger voltage (low): 0V to 2.0V.</p> <p>DI-2 (Digital Input 2): Trigger voltage (high): 5V to 30V. Trigger voltage (low): 0V to 2.0V.</p> <p>DO (Digital Output): Voltage (Relay mode): Depends on power input voltage, maximum voltage is 36V.</p> <p>TX (Transmit): serial (RS-232) connectivity for transmit data.</p> <p>RX (Receive): serial (RS-232) connectivity for receive data.</p>
F	Wi-Fi antenna port	Connect Wi-Fi antenna
G	WLAN/LAN1 port (RJ45)	Connect RJ45 cable for WAN/LAN connection
H	LAN2 port (RJ45)	Connect RJ45 cable for LAN connection
I	LAN3 port (RJ45)	Connect RJ45 cable for LAN connection
J	LTE antenna port AUX	Connect LTE antenna
K	GPS antenna port	Connect GPS antenna*
L	Wi-Fi antenna port	Connect Wi-Fi antenna

* The GNSS Antenna is an optional accessory that is not included in the standard package. If you intend to use the provided GNSS function, please purchase an active GPS antenna and install it to the corresponding SMA connector in advance.

1.3 Installation

1.3.1 System requirement

- For installation of the MG400, 1 x Philips-head screwdriver size 1 (not supplied) is required.
- For configuration, a PC with a working Ethernet network adapter and a web browser is needed.
- An active 3G/4G SIM card, or two SIM cards if you plan to use the SIM failover feature.

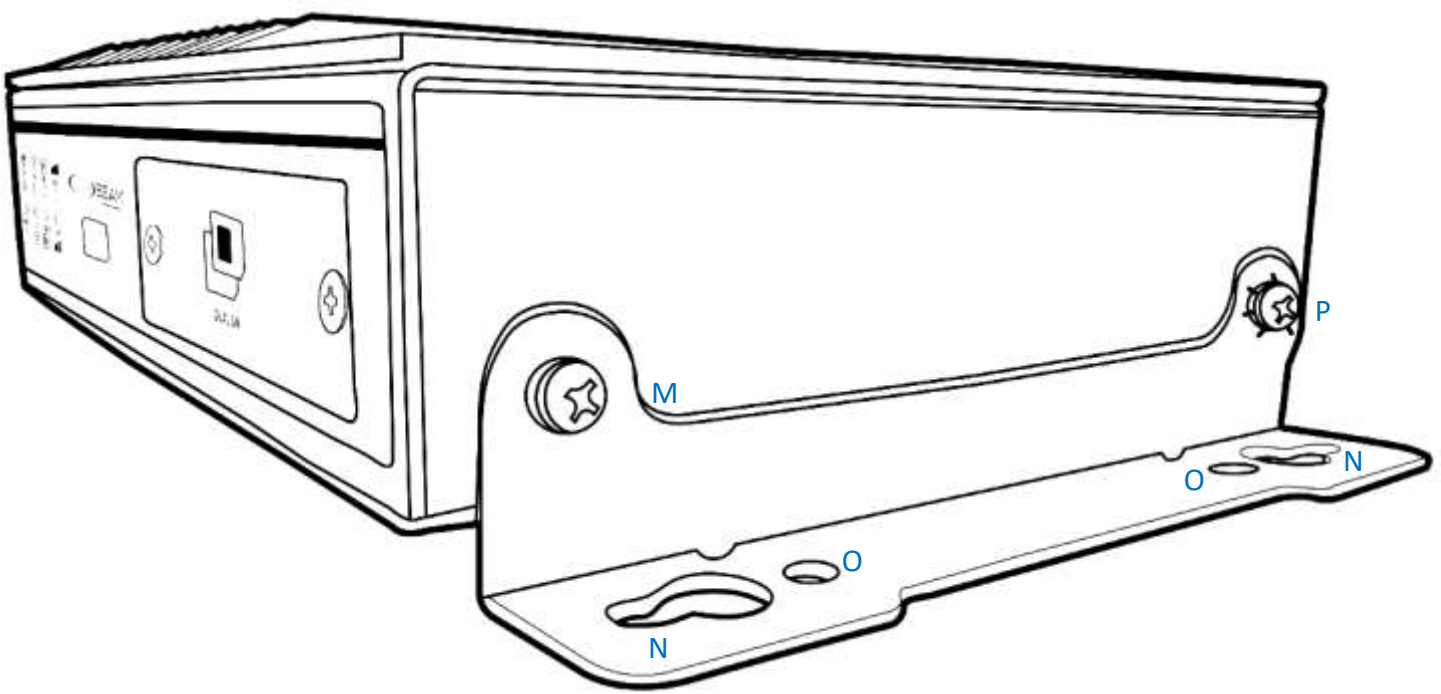
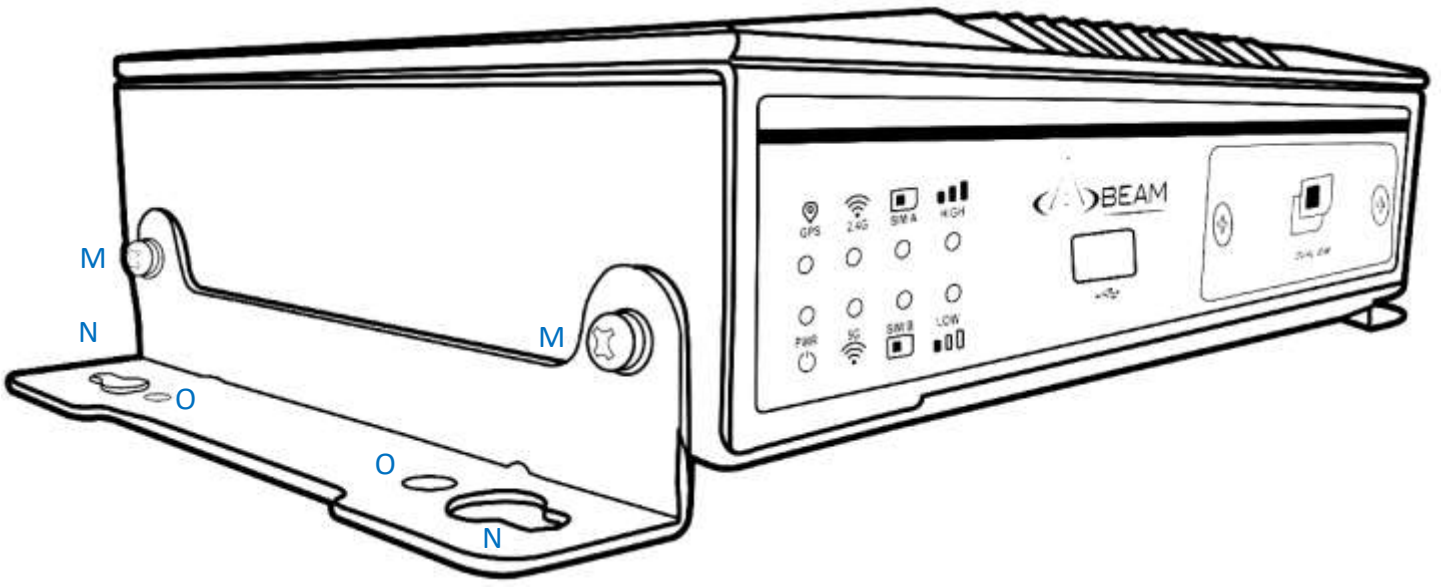
1.3.2 Hardware installation

1.3.2.1 Important notes on installation

- The MG400 can be powered by the AC power adapter shipped with the MG400, or 12Vdc / 24Vdc vehicle power.
- The top cover / heatsink of the MG400 can be hot in operation. Before servicing, power OFF the MG400, and leave it for a while to cool down.
- No serviceable parts inside the MG400. It is not recommended to open the case and service the unit yourself. If there is any hardware issue, please contact support at Beam.

1.3.2.2 Mounting the unit

The MG400 can be installed on a flat surface or mounted on a wall. The MG400 comes with mounting brackets that allow mounting for mobile and fixed positioning.



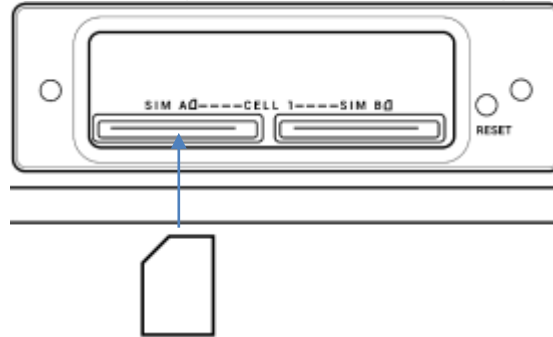
#	Description	Notes
M	Black screw	Screw the mounting brackets to the MG400.
N	Screw holes for flat surface installation	
O	Screw holes for flat surface installation	
P	Zinc screw for grounding (Earth) point	Screw the mounting brackets and grouding (Earth) cable to the MG400.

1.3.2.3 Inserting the SIM cards

Warning – Before changing or inserting a SIM card, ensure that the unit is powered OFF. As electrostatic discharge (ESD) may happen, do not touch the SIM card's metal connectors.

Step 1: Using a Philips-head screwdriver size 1, unscrew 2x screws on SIM cover and remove the cover.

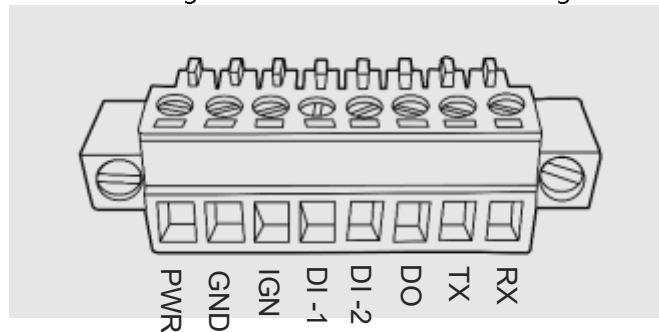
Step 2: Insert the SIM card(s) into the SIM slots. To eject an inserted SIM card, push it and release.



Step 3: Screw the SIM cover back to its original position.

1.3.2.4 Connecting terminal block

The MG400 accepts DC input power in the range of 9V to 36V. Follow the image below for the correct polarity.



Following table showing the PIN definitions and specifications.

PIN#	Description	Notes
1	PWR	9V – 36V DC power input.
2	GND	Terminal for ground wire connection.
3	IGN	Terminal used to connect to the ignition sense wire of a vehicle.
4	DI-1	Trigger voltage (high): - 5V to 30V. Trigger voltage (low): - 0V to 2.0V.
5	DI-2	Trigger voltage (high): - 5V to 30V. Trigger voltage (low): - 0V to 2.0V.
6	DO	Voltage (Relay mode): Depends on power input voltage, maximum voltage is 36V.
7	TX	Serial (RS-232) connectivity for transmit data.
8	RX	Serial (RS-232) connectivity for receive data.

1.3.2.5 Connecting Ethernet ports

The MG400 features 3x RJ45 10/100/1000 Mbps Ethernet ports with auto-MDIX. WAN/LAN1 port by factory default is configured as LAN port. However, it can be configured to work as WAN port, refer to WAN & Uplink section for details.

1.4 Connecting PC to MG400

1.4.1 Connecting via Wi-Fi

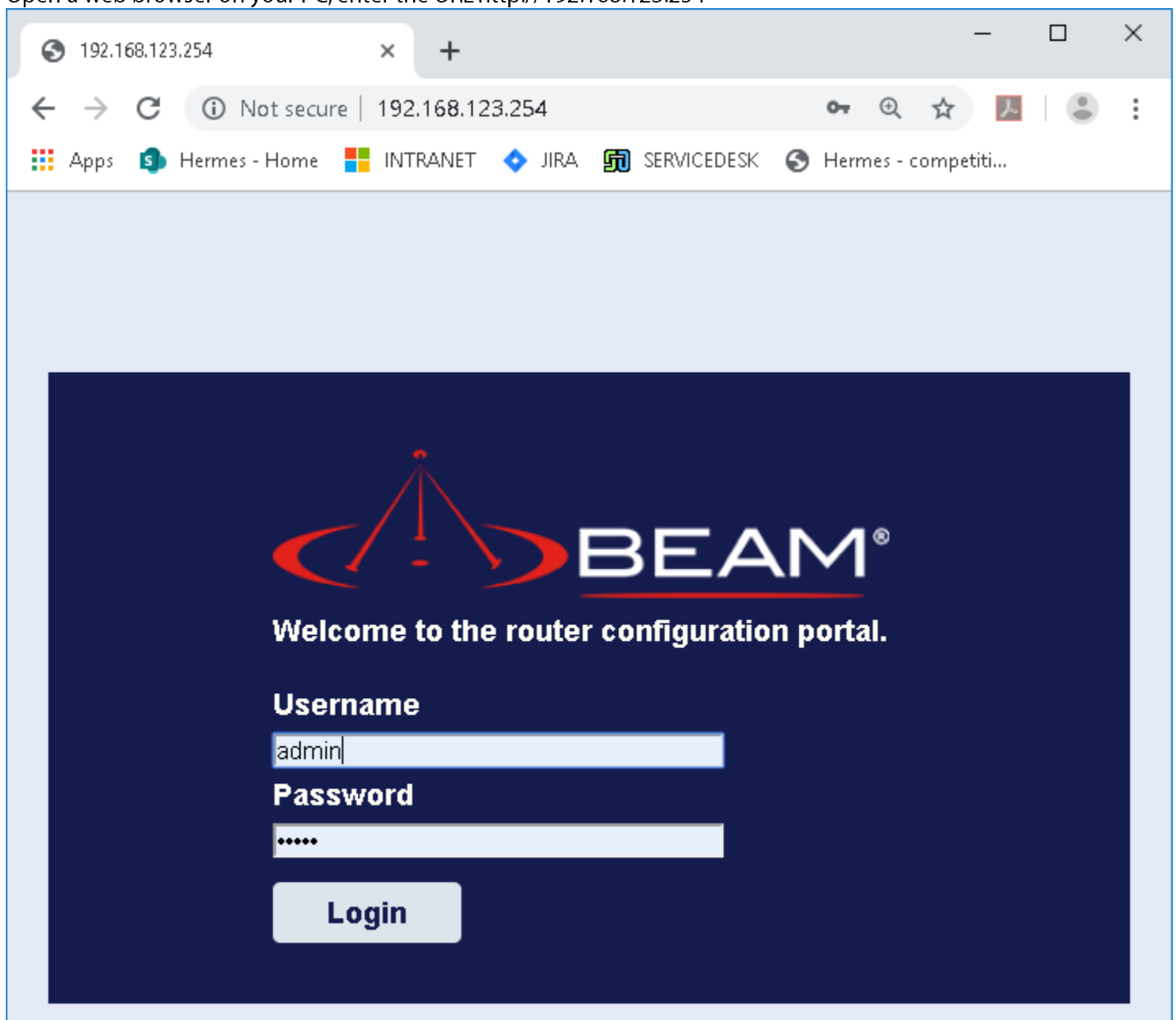
Using your PC, connect to the SSID labelled “BEAM_2.4GHz_XXXX”, where “XXXX” is four randomly generated numbers. The unique SSID and password for the wireless networks is printed on the MG400 label and Spare device label. Continue to the “Accessing the web GUI” section.

1.4.2 Connecting via Ethernet cable

Connect a standard straight-through Ethernet cable to your PC and the other end to any of the LAN ports on the back panel of the MG400. Continue to the “Accessing the web GUI” section.

1.4.3 Accessing the web GUI


Open a web browser on your PC, enter the URL <http://192.168.123.254>



Enter the:
Default Username: admin
Default Password: admin

To log-out the MG400, click top right [LOGOUT](#)

Upon your first login, the 1st page is the Setup Wizard page. You can use the Setup Wizard to configure the Administrator password, Time Zone, Wi-Fi SSID & password, APN settings. Click Next for the next page.

 **Setup Wizard**

Setup Wizard will guide you through some basic configuration.

- ▶ **Step 1.** Administrator Password.
- ▶ **Step 2.** Time Zone.
- ▶ **Step 3.** Wi-Fi Module.
- ▶ **Step 4.** APN Setting.
- ▶ **Step 5.** Setup Summary.
- ▶ **Step 6.** Complete.

[[Start](#) > Admin Password > Time Zone > Wi-Fi > APN > Summary > Complete]

[Next >](#)

On the **Administrator Password** page, type in a new password for the MG400 login. Then click Next for the next page.

Step 1. Administrator Password

▶ New Password

▶ Confirm New Password

< Back

[Start > Admin Password > Time Zone > Wi-Fi > APN > Summary > Complete]

Next >

The **Time Zone** page has the option to select Time Zone. Manual time zone setting is available down the bottom of drop-down list. Click Next for the next page.

Step 2. Time Zone

▶ Time Zone

(GMT+10:00) Canberra, Melbourne, Sydney ▼

< Back

[Start > Admin Password > Time Zone > Wi-Fi > APN > Summary > Complete]

Next >

The **Wi-Fi Module One** page is for the 2.4GHz Wi-Fi Module settings. Click Next for the next page.

Step 3. Wi-Fi Module One

▶ Network ID(SSID)

BEAM_2.4GHz_0704

▶ Wi-Fi System

802.11b/g/n Mixed ▼

▶ Authentication

WPA2-PSK ▼

▶ Encryption

AES ▼

▶ Preshared Key

utbiwt6eANAAH

▶ Wi-Fi Module

☒ Enable

< Back

[Start > Admin Password > Time Zone > **Wi-Fi** > APN > Summary > Complete]

Next >

The **Wi-Fi Module Two** page is for the 5GHz Wi-Fi Module settings. Click Next for the next page.

Step 3. Wi-Fi Module Two

▶ Network ID(SSID)

BEAM_5GHz_0704

▶ Wi-Fi System

802.11 a/n/ac Mixed ▼

▶ Authentication

WPA2-PSK ▼

▶ Encryption

AES ▼

▶ Preshared Key

utbiwt6eANAAH

▶ Wi-Fi Module

☒ Enable

< Back

[Start > Admin Password > Time Zone > **Wi-Fi** > APN > Summary > Complete]

Next >

On the **APN Setting** page, for each SIM card there are 2x options. One option is Telstra with APN automatically filled. The other option is Manual, where the APN needs to be manually typed in. Click Next for the next page.

Step 4. APN Setting

▶ SIM-A

APN

Telstra ▼

telstra.internet

▶ SIM-B

APN

Manual ▼

< Back

[Start > Admin Password > Time Zone > Wi-Fi > **APN** > Summary > Complete]

Next >

Check the settings in the **Setup Summary** page. Click Apply to confirm settings. The MG400 will then reboot. After the reboot is complete, the **Dashboard** page (see Section 2.1 Dashboard) will be shown after login.

Step 5. Setup Summary

Please confirm the information below.

[Time Zone Settings]

Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
-----------	--

[Wi-Fi Module One Settings]

Wi-Fi Module	Enable
SSID	BEAM_2.4GHz_1534
Authentication	WPA2-PSK
Encryption	AES

[Wi-Fi Module Two Settings]

Wi-Fi Module	Enable
SSID	BEAM_5GHz_1534
Authentication	WPA2-PSK
Encryption	AES

[APN Settings]

SIMA	
SIMB	

< Back

[Start > Admin Password > Time Zone > Wi-Fi > APN > **Summary** > Complete]

Apply

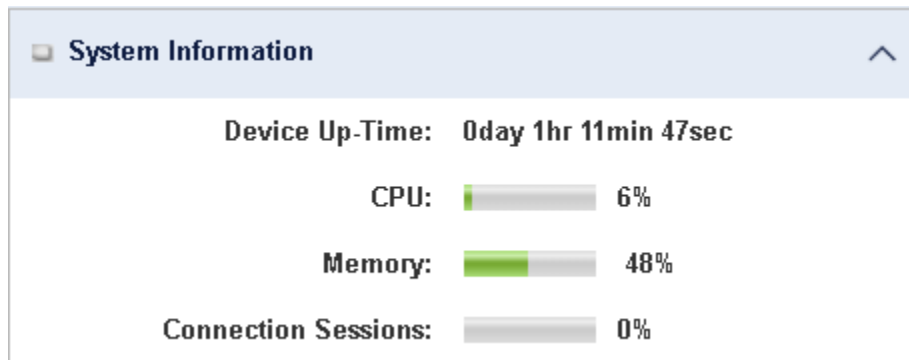
2. Status

2.1 Dashboard

Navigate to the **Status** -> **Dashboard** tab.

The **Dashboard** page shows system information & history, and the Network Interface status.

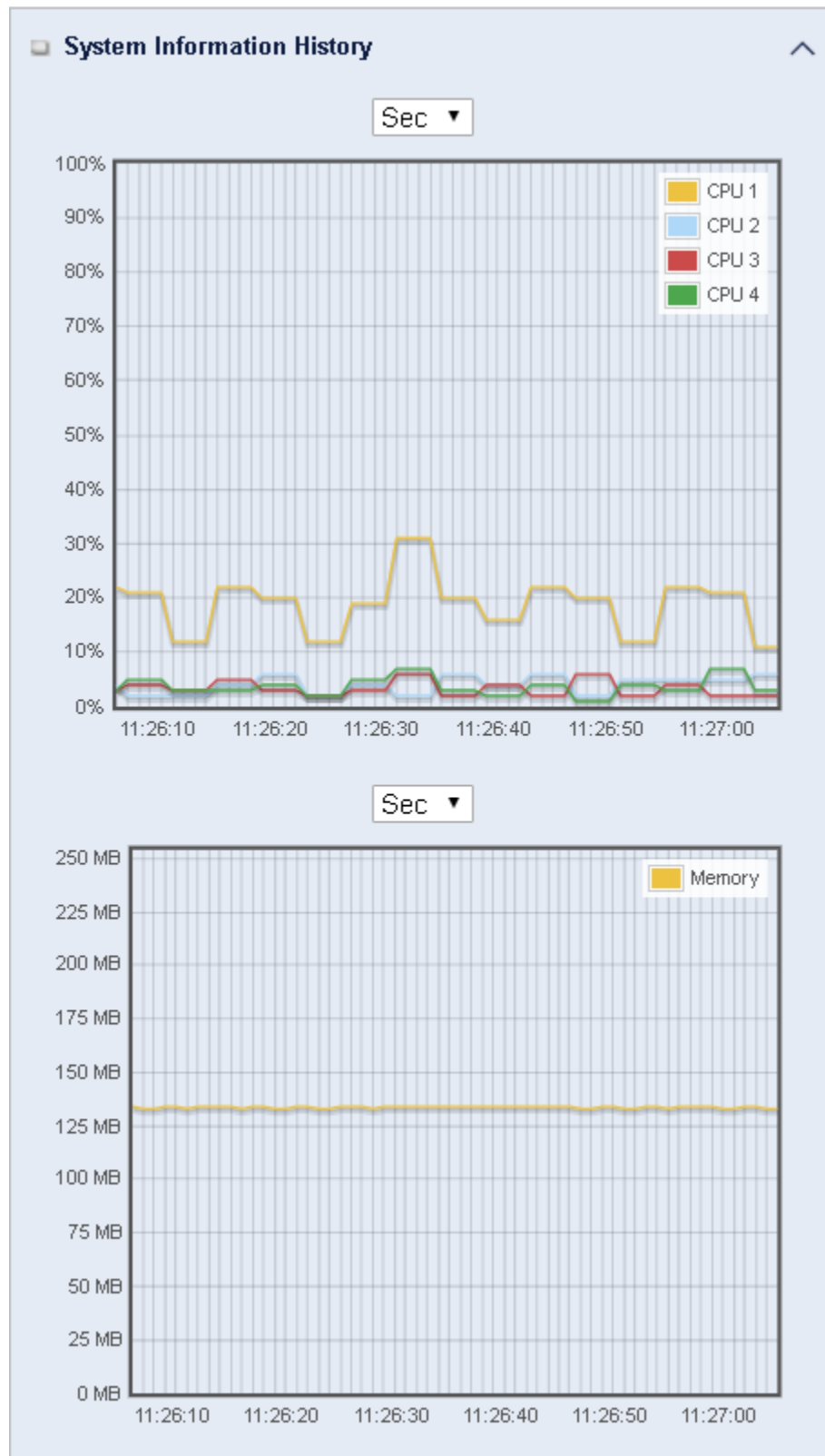
The System Information window shows the MG400 Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.



The Network Interface Status window shows statistic information for each network interface of the MG400. The statistic information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.

Network Interface Status					
Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	25 (MB)	7 (MB)	27 (KB)	3 (KB)
eth2.1	Ethernet	22 (MB)	4 (MB)	27 (KB)	3 (KB)
br0	Ethernet	22 (MB)	4 (MB)	27 (KB)	3 (KB)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
usbnet0	3G/4G	3 (MB)	3 (MB)	1 (KB)	136 (Bytes)

The System Information History window shows the statistic graphs for the CPU and memory.



2.2 Network

2.2.1 WAN & Uplink

Navigate to the **Status** -> **Network** -> **WAN & Uplink** tab.

The WAN & Uplink page shows the WAN network status, LAN network status, 3G/4G modem status and interface traffic statistics. The display will be refreshed every five seconds.

WAN interface IPv4 Network Status window shows status information for IPv4 network.

WAN Interface IPv4 Network Status										
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	NAT	22.224.145.161	255.255.255.252	22.224.145.162	10.4.149.70, 10.5.133.45	N/A	Connected 0 day 1:02:38	Edit
WAN-2		Disable								Edit
WAN-3		Disable								Edit
WAN-4		Disable								Edit

WAN interface IPv4 Network Status		
Item	Value setting	Description
ID	System generated.	Displays corresponding WAN interface WAN IDs.
Interface	System generated.	Displays the type of WAN physical interface. It can be Ethernet, 3G/4G, or Wi-Fi Uplink.
WAN Type	System generated.	Displays the method which public IP address is obtained from your ISP. It can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
Network Type	System generated.	Displays the network type for the WAN interface(s). It can be NAT, Routing, Bridge, or IP Pass-through.
IP Addr.	System generated.	Displays the public IP address obtained from your ISP for Internet connection. Default setting is 0.0.0.0 if left unconfigured.
Subnet Mask	System generated.	Displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default setting is 0.0.0.0 if left unconfigured.
Device	System generated.	Displays the MG400 IP address obtained from your ISP for Internet connection. Default setting is 0.0.0.0 if left unconfigured.
DNS	System generated.	Displays the IP address of DNS server obtained from your ISP for Internet connection. Default setting is 0.0.0.0 if left unconfigured.
MAC Address	System generated.	Displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	System generated.	Displays the connection status of the MG400 to your ISP. Status are connected or disconnected.
Action	Buttons.	This area provides functional buttons.

Renew button allows you to force the MG400 to request an IP address from the DHCP server. Note: Renew button is available when DHCP WAN Type is used and WAN connection is disconnected.

Release button allows you to force the MG400 to clear its IP address setting to disconnect from DHCP server. Note: Release button is available when DHCP WAN Type is used and WAN connection is connected.

Connect button allows you to manually connect the MG400 to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to Edit button in Network > WAN & Uplink > Internet Setup) and WAN connection status is disconnected.

Disconnect button allows you to manually disconnect the MG400 from the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to Edit button in Network > WAN & Uplink > Internet Setup) and WAN connection status is connected.

The **WAN Interface IPv6 Network Status** window shows IPv6 WAN connection status.

WAN Interface IPv6 Network Status						
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1		Disable				Edit

WAN interface IPv6 Network Status		
Item	Value setting	Description
ID	System data.	Displays corresponding WAN interface WAN IDs.
Interface	System data.	Displays the type of WAN physical interface. It can be Ethernet, 3G/4G, etc.
WAN Type	System data.	Displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from Network > IPv6 > Configuration.
Link-local IP Address	System data.	Displays the LAN IPv6 Link-Local address.
Global IP Address	System data.	Displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	System data.	Displays the connection status. The status can be connected, disconnected and connecting.
Action	Button	This area provides functional buttons. Edit Button when pressed, web-based utility will take you to the IPv6 configuration page. (Network > IPv6 > Configuration.)

LAN Interface Network Status window shows IPv4 and IPv6 information of LAN network.

LAN Interface Network Status						
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action	
192.168.123.254	255.255.255.0	fe80::250:18ff:fe21:f270	/64	00:50:18:21:F2:70	<input type="button" value="Edit IPv4"/> <input type="button" value="Edit IPv6"/>	

LAN Interface Network Status		
Item	Value setting	Description
IPv4 Address	System data.	Displays the current IPv4 IP Address of the MG400. This is also the IP Address you use to access Router's Web -based Utility.
IPv4 Subnet Mask	System data.	Displays the current mask of the subnet.
IPv6 Link-local Address	System data.	Displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address you use to access Router's Web -based Utility.
IPv6 Global Address	System data.	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	System data.	Displays the LAN MAC Address of the MG400.
Action	Buttons.	This area provides functional buttons. Edit IPv4 Button when press, web-based utility will take you to the Ethernet LAN configuration page. (Network > LAN & VLAN > Ethernet LAN tab). Edit IPv6 Button when press, web-based utility will take you to the IPv6 configuration page. (Network > IPv6 > Configuration.)

The **3G/4G Modem Status List** show the interface, card information, link status, signal strength and network name. Click the Detail button for more information.

3G/4G Modem Status List ^					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	EP06	Connected	67% (-71dBm)	Telstra Mobile Telstra (LTE+)	<button>Detail</button>

3G/4G Modem Status List		
Item	Value setting	Description
Physical Interface	System data.	Displays the type of WAN physical interface.
Card Information	System data.	Displays the vendor's 3G/4G modem model name.
Link Status	System data.	Displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	System data.	Displays the 3G/4G wireless signal level.
Network Name	System data.	Displays the name of the service network carrier.
Refresh	System data.	Click the Refresh button to renew the information.
Action	Button.	This area provides functional buttons. Detail button when press, a window of Modem Information will appear. They are the Modem Information, SIM Status, Service Information, Signal Strength / Quality and Error Messages.

Following is the Modem Information window.

Modem Information							
Interface	Module Name	IMEI/MEID	HW Version	FW Version	Temperature	Band List	
3G1	EP06	868186040077040	E	EP06ELAR03A07M4G	39	3G Band1 (2100MHz) Band3 (1800MHz) Band5 (850MHz) Band8 (900MHz) LTE Band1 (2100MHz) Band3 (1800MHz) Band5 (850MHz) Band7 (2600MHz) Band8 (900MHz) Band20 (800MHz) Band28 (700MHz) Band32 (1500MHz) Band38 (2600MHz) Band40 (2300MHz) Band41 (2500MHz)	
SIM Status							
SIM	PIN Code Status	PIN / PUK Code Remaining Times		IMSI	SMSC	MSISDN	
SIM-A	Ready	3 / 10		505013504590689	+61418706700	N/A	
Service Information							
Operator	MCC	MNC	Service Type	Band	LAC	TAC	Cell ID
Telstra Mobile Telstra	505	1	LTE	Band 28	N/A	309E	81B200D
CS / PS Register Status			PS Attached Status		Roaming Status		
Registered / Registered			Attached		Not Roaming		
Signal Strength and Quality							
RSSI	RSRP	RSRQ	SINR		RSCP	EcIo	
-67	-100	-14	10		N/A	N/A	

SCC Signal Information				
Band	RSSI	RSRP	RSRQ	SINR
Band 3	-76	-102	-17	9
Error Message				
Profile Index	Error Description			
1	N/A			

Interface Traffic Statistics window displays the interfaces total transmitted packets.

Interface Traffic Statistics				
ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	95.91	71.37	<button>Reset</button>
WAN-2	Ethernet	0	0	<button>Reset</button>
WAN-3	WiFi Module One	0	0	<button>Reset</button>
WAN-4	-	-	-	

Interface Traffic Statistics			
Item	Value setting	Description	
ID	System data.	Displays corresponding WAN interface WAN IDs.	
Interface	System data.	Displays the type of WAN physical interface. It can be Ethernet, 3G/4G, Wi-Fi Module One, Wi-Fi Module Two.	
Received Packets (Mb)	System data.	Displays the downstream packets (Mb). It is reset when the MG400 is rebooted.	
Transmitted Packets (Mb)	System data.	Displays the upstream packets (Mb). It is reset when the MG400 is rebooted.	
Action	Buttons.	Click the Reset button to clear the entire statistic and reset counter to 0 Mb.	

2.2.2 LAN & VLAN

Navigate to the **Status > Network > LAN & VLAN** tab.

The Client List shows the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each MG400 that is connected to the MG400.

LAN Client List				
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.123.148	WR-LT034	E4-B9-7A-1B-D4-35	00:12:30

LAN Client List		
Item	Value setting	Description
LAN Interface	System data.	Client record of LAN Interface.
IP Address	System data.	Client record of IP Address Type and the IP Address.
Host Name	System data.	Client record of Host Name.
MAC Address	System data.	Client record of MAC Address.
Remaining Lease Time	System data.	Client record of Remaining Lease Time.

2.2.3 Wi-Fi

Navigate to the **Status > Network > Wi-Fi** tab.

The Wi-Fi page shows the Wi-Fi Module One and Two AP list. Wi-Fi Module One is for 2.4GHz Wi-Fi, while Module Two is for 5GHz Wi-Fi. The Edit tab under Action provide access to configuration of the Wi-Fi module.

The Wi-Fi Virtual AP List shows all the virtual AP information on each Wi-Fi module. The Edit button allows for quick configuration changes.

Wi-Fi Module One Virtual AP List								
Op. Band	ID	Wi-Fi Enable	Op. Mode	SSID	Channel	Wi-Fi System	Auth.&Security	MAC Address
2.4G	VAP-1	<input checked="" type="checkbox"/>	AP Router	MG400_2.4G	Auto(11)	b/g/n Mixed	WPA2-PSK(AES)	00:50:18:21:F2:70
2.4G	VAP-2	<input type="checkbox"/>	AP Router	default	Auto(11)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:20:F2:70

[Edit](#) [QR Code](#)

[Edit](#) [QR Code](#)

Wi-Fi Virtual AP List		
Item	Value setting	Description
Wi-Fi Enable	System data.	Displays whether the VAP wireless signal is enabled or disabled.
Op. Band	System data.	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	System data.	Displays the ID of VAP.
Wi-Fi Enable	System data.	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	System data.	The Wi-Fi Operation Mode of VAP. It can be AP Router, WDS Only and WDS Hybrid.
SSID	System data.	Displays the network ID of VAP.
Channel	System data.	Displays the wireless channel used.
Wi-Fi System	System data.	The Wi-Fi System of VAP.
Auth. & Security	System data.	Displays the authentication and encryption type used.
MAC Address	System data.	Displays MAC Address of VAP.
Action	Buttons.	Click the Edit button to make a quick access to the Wi-Fi configuration page. (Network > Wi-Fi > Configuration tab) The QR Code button allows you to generate QR code for quick connect to the VAP by scanning the QR code.

The **Wi-Fi Uplink Status** shows all information of connected Wi-Fi uplink network on each Wi-Fi module.

WiFi Module One Uplink Status							
SSID	BSSID	Channel	Security	RSSI0	RSSI1	Rate	Action
Only_For_Monkey	00:00:00:00:00:00	1	WPA2-PSK(AES)	0	0	0	Edit

Wi-Fi Module One Uplink Status		
Item	Value setting	Description
SSID	System data.	Displays the network ID of VAP.
BSSID	System data.	Displays the BSSID for the connected wireless network.
Channel	System data.	Displays the wireless channel being used.
Security	System data.	Displays the authentication and encryption setting for the Wi-Fi uplink connection.
RSSI0, RSSI1	System data.	Displays the Rx sensitivity on each radio path.
Rate	System data.	Displays the link rate (Mbps) for the Wi-Fi uplink connection.
Action	Button.	Click the Edit button to make a quick access to the Wi-Fi uplink configuration page. (Network > WAN & Uplink > Internet Setup tab)

The **Wi-Fi IDS Status** shows the quantities of authentication, association, and other frames.

Wi-Fi Module One IDS Status								
Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	Reset

Wi-Fi IDS Status			
Item	Value setting	Description	
Authentication Frame	System data.	Displays the receiving Authentication Frame count.	
Association Request Frame	System data.	Displays the receiving Association Request Frame count.	
Re-association Request Frame	System data.	Displays the receiving Re-association Request Frame count.	
Probe Request Frame	System data.	Displays the receiving Probe Request Frame count.	
Disassociation Frame	System data.	Displays the receiving Disassociation Frame count.	
Deauthentication Frame	System data.	Displays the receiving Deauthentication Frame count.	
EAP Request Frame	System data.	Displays the receiving EAP Request Frame count.	
Malicious Data Frame	System data.	Displays the number of receiving unauthorized wireless packets.	
Action	Button.	Click the Reset button to clear the entire statistic and reset counter to 0.	

The Wi-Fi Traffic Statistic shows all the received and transmitted packets on each Wi-Fi module.

Wi-Fi Module One Traffic Statistics				
Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	0	0	<button>Reset</button>
2.4G	VAP-2	0	0	<button>Reset</button>

Wi-Fi Traffic Statistic			
Item	Value setting	Description	
Op. Band	System data.	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.	
ID	System data.	Displays the VAP ID.	
Received Packets	System data.	Displays the number of received packets.	
Transmitted Packets	System data.	Displays the number of transmitted packets.	
Action	Buttons.	Click the Reset button to clear individual VAP statistics.	

2.2.4 DDNS

Navigate to the **Status > Network > DDNS** tab.

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

DDNS Status List				
Host Name	Provider	Effective IP	Last Update Status	Last Update Time
<button>Refresh</button>				

DDNS Status		
Item	Value Setting	Description
Host Name	System data.	Displays the name you enter to identify DDNS service provider.
Provider	System data.	Displays the DDNS server of DDNS service provider.
Effective IP	System data.	Displays the public IP address of the MG400.
Last Update Status	System data.	Displays whether the last update of the MG400 public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	System data.	Displays time stamp of the last update of public IP address to the DDNS server.
Refresh	Button.	The refresh button allows you to force the display to refresh information.

2.3 Security

2.3.1 VPN

Navigate to the **Status > Security > VPN** tab.

The VPN page shows status of all the VPN technologies, including IPSec Tunnel, OpenVPN Server, OpenVPN Client, L2TP Server, L2YP Client, PPTP Server and PPTP Client.

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

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

IPSec Tunnel Status		
Item	Value setting	Description
Tunnel Name	System data.	Displays the tunnel name you have entered.
Tunnel Scenario	System data.	Displays the Tunnel Scenario.
Local Subnets	System data.	Displays the Local Subnets.
Remote IP/FQDN	System data.	Displays the Remote IP/FQDN.
Remote Subnets	System data.	Displays the Remote Subnets.
Conn. Time	System data.	Displays the connection time for the IPSec tunnel.
Status	System data.	Displays the Status of the VPN connection. The status displays are Connected, Disconnected, waiting for traffic, and Connecting.
Edit	Button.	Click on Edit Button to change IPSec setting, web-based utility will take you to the IPSec configuration page. (Security > VPN > IPSec tab)

The OpenVPN Server/Client Status shows the status and statistics for the OpenVPN connection from the server side or client side.

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

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

OpenVPN Client Status							
<div>EditDetail</div>							
ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status

OpenVPN Client Status		
Item	Value setting	Description
OpenVPN Client Name	System data.	Displays the Client name you have entered for identification.
Interface	System data.	Displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	System data.	Displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	System data.	Displays the Remote Subnet.
TUN/TAP Read (Bytes)	System data.	Displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write (Bytes)	System data.	Displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read (Bytes)	System data.	Displays the TCP/UDP Read Bytes of OpenVPN Client.
TCP/UDP Write (Bytes)	System data.	Displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	System data.	Displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	System data.	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected or Disconnected.

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

L2TP Server Status						<div>Edit</div>	<div>^</div>
ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status	

L2TP Server Status		
Item	Value setting	Description
User Name	System data.	Displays the username for the connection.
Remote IP	System data.	Displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	System data.	Displays the IP address assigned to the connected L2TP client.
Remote Call ID	System data.	Displays the L2TP client Call ID.
Conn. Time	System data.	Displays the connection time for the L2TP tunnel.
Status	System data.	Displays the Status of each of the L2TP client connection. The status displays Connected, Disconnect, Connecting
Edit	Button.	Click on Edit Button to change L2TP server setting, web-based utility will take you to the L2TP server page. (Security > VPN > L2TP tab)

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

L2TP Client Status		
Item	Value setting	Description
Client Name	System data.	Displays Name for the L2TP Client.
Interface	System data.	Displays the WAN interface with which the MG400 will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	System data.	Displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	System data.	Displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Device/Remote Subnet	System data.	Displays the specified IP address of the MG400 used to connect to the L2TP server –the default MG400. Or another specified subnet if the MG400 is not used to connect to the L2TP server –the remote subnet.
Conn. Time	System data.	Displays the connection time for the L2TP tunnel.
Status	System data.	Displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit	Button.	Click on Edit Button to change L2TP client setting, web-based utility will take you to the L2TP client page. (Security > VPN > L2TP tab)

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

PPTP Server Status Edit					
ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time Status

PPTP Server Status		
Item	Value setting	Description
User Name	System data.	Displays the username for the connection.
Remote IP	System data.	Displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	System data.	Displays the IP address assigned to the connected PPTP client.
Remote Call ID	System data.	Displays the PPTP client Call ID.
Conn. Time	System data.	Displays the connection time for the PPTP tunnel.
Status	System data.	Displays the Status of each of the PPTP client connection. The status displays Connected, Disconnect, and Connecting.
Edit	Button.	Click on Edit Button to change PPTP server setting, web-based utility will take you to the PPTP server page. (Security > VPN > PPTP tab)

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

PPTP Client Status		
Item	Value setting	Description
Client Name	System data.	Displays Name for the PPTP Client.
Interface	System data.	Displays the WAN interface with which the MG400 will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	System data.	Displays the IP address assigned by Virtual IP server of PPTP server.
Remote IP/FQDN	System data.	Displays the PPTP Server's Public IP address (the WAN IP address) or FQDN.
Default Device / Remote Subnet	System data.	Displays the specified IP address of the MG400 used to connect to the internet to connect to the PPTP server –the default MG400. Or another specified subnet if the MG400 is not used to connect to the PPTP server – the remote subnet.
Conn. Time	System data.	Displays the connection time for the PPTP tunnel.
Status	System data.	Displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit	Button.	Click on Edit Button to change PPTP client setting, web-based utility will take you to the PPTP server page. (Security > VPN > PPTP tab)

2.3.2 Firewall

Navigate to the Status > Security > Firewall Status Tab.

The **Firewall** page shows firewall status, including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and Options. The display will refresh automatically every five seconds.

The Packet Filters window shows the packet filter applied to the MG400, including the filter rule, IP addresses, date and time information.

Packet Filters		Edit		
Activated Filter Rule	Detected Contents	IP	Time	

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

Note: Enable Packet Filter Log Alert, navigate to Security > Firewall > Packet Filter tab. Enable Log Alert and save the setting.

The URL Blocking Status window displays the URL block rule, IP and time.

URL Blocking

Edit

Activated Blocking Rule

Blocked URL

IP

Time

URL Blocking Status		
Item	Value setting	Description
Activated Blocking Rule	System data.	This is the URL Blocking Rule name.
Blocked URL	System data.	This is the logged packet information.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note:
Enable Log Alert, navigate to Security > Firewall > URL Blocking tab. Enable Log Alert and save the setting.

The **Web Content Filter Status** window shows the filters rules based on web content.

Web Content Filters Edit				
Activated Filter Rule	Detected Contents		IP	Time
Web Content Filter Status				
Item	Value setting	Description		
Activated Filter Rule	System data.	Logged packet of the rule name. String format.		
Detected Contents	System data.	Logged packet of the filter rule. String format.		
IP	System data.	Logged packet of the Source IP. IPv4 format.		
Time	System data.	Logged packet of the Date Time. Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")		

Note: Enable Web Content Filter Log Alert, navigate to Security > Firewall > Web Content Filter Tab. Enable Log Alert and save the setting.

The MAC Control Status window shows the MAC filter status.

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

Note: Ensure MAC Control Log Alert, navigate to Security > Firewall > MAC Control tab. Enable Log Alert and save the setting.

The **Application Filters** window shows the application filter status.

Application Filters		Edit		
Filtered Application Category	Filtered Application Name		IP	Time

Application Filters Status

Item	Value setting	Description
Filtered Application Category	System data.	The name of the Application Category being blocked.
Filtered Application Name	System data.	The name of the Application being blocked.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Enable Application Filter Log Alert, navigate to **Security > Firewall > Application Filter** tab. Enable Log Alert and save the setting.

The **IPS Firewall Status** window shows the IPS Firewall status.

IPS		Edit		
Detected Intrusion			IP	Time

IPS Firewall Status

Item	Value setting	Description
Detected Intrusion	System data.	This is the intrusion type of the packets being blocked.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Enable IPS Log Alert, navigate to **Security > Firewall > IPS** tab. Enable Log Alert and save the setting.

The Firewall Options Status window shows the Firewall Options that are applied to the MG400.

Options

Edit

^

Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management
Disable	Enable	Disable	Disable

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

Note: Enable Firewall Options Log Alert, navigate to **Security > Firewall > Options** tab. Enable Log Alert and save the setting.

2.4 Administration

2.4.1 Remote Management

Navigate to the Status > Administration > Remote Management tab.

The Remote Management page shows the status for managing remote network devices. The type of management available are SNMP and TR-069. The display will refresh automatically every five seconds.

The SNMP Link Status window shows the status of current active SNMP connections.

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

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

The **SNMP Trap Information** window shows the trap level, time and trap event.

SNMP Trap Information		
Trap Level	Time	Trap Event

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

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

TR-069 Status
Link Status
Off

TR-069 Status

Item	Value setting	Description
Link Status	System data.	Displays the current connection status with the TR-068 server. The connection status is either on when the MG400 connects with the TR-068 server or Off when disconnected.

2.4.2 Log Storage

Navigate to the Status > Administration > Log Storage tab.

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

Storage Information					
Device Select	Device Description	Usage	File System	Speed	Status
Refresh					

2.4.3 GNSS

Navigate to the Status > Administration > GNSS tab.

The **GNSS** page shows GPS and location information.

The GNSS Information window shows the status for current GNSS positioning information for the MG400.

GNSS Information						
Condition	No. of Satellites	Satellites ID / Signal Strength (dBm)	Position (Lat, Long)	Altitude (meters)	True Course	Ground Speed (km/h)
Not Fixed						
Refresh						

The available GNSS information includes GNSS Condition, No. of Satellites, Satellites ID / Signal Strength, Position (Lat., Long.), Altitude (meters), True Course, and the equivalent Ground Speed (km/h).

2.5 Usage

2.5.1 Connection Records

Navigate to the Status > Usage > Connection Records tab.

The **Connection Records** window shows the connections records to from LAN IP to WAN IP.

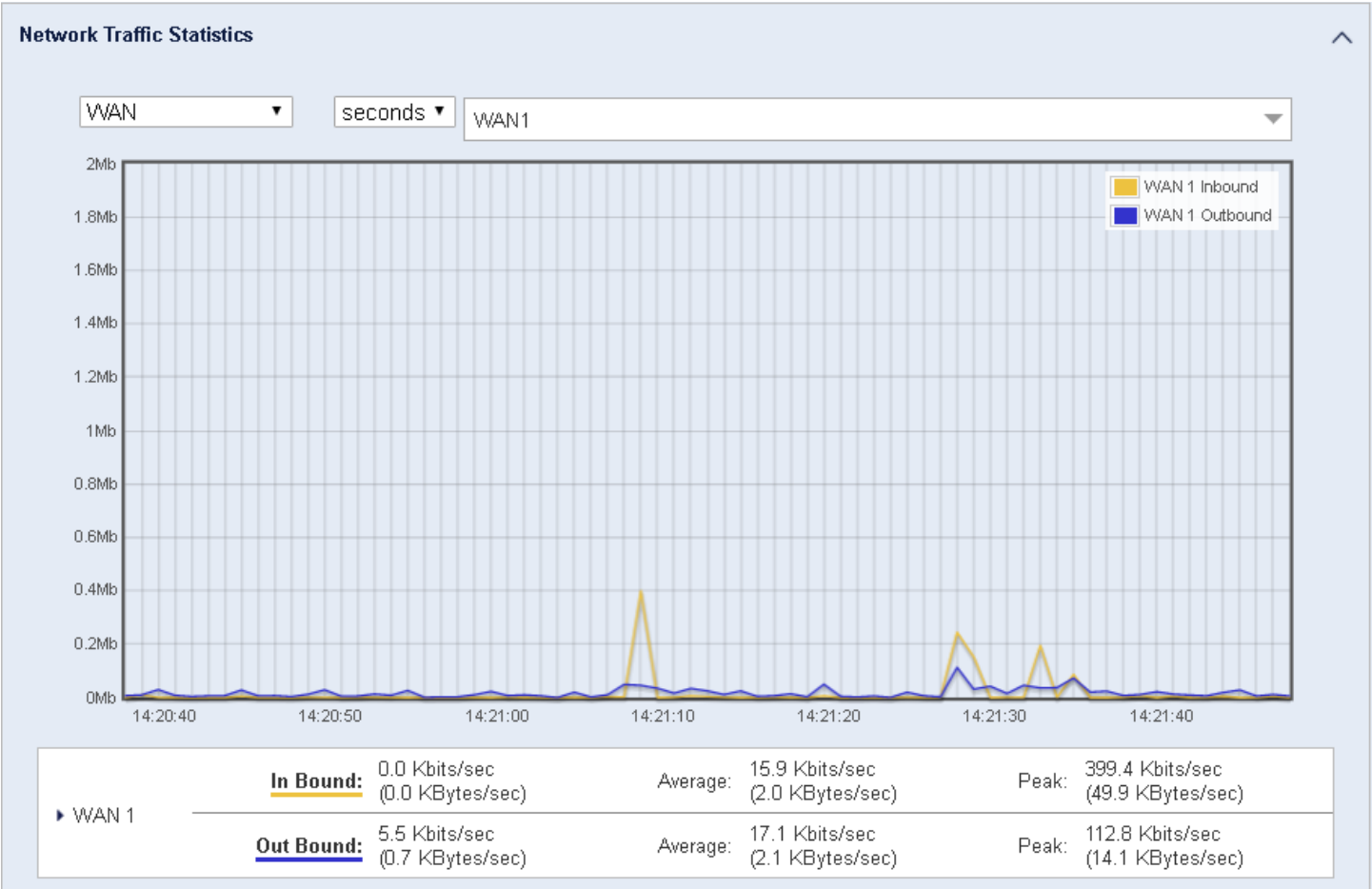
<input type="checkbox"/> Internet Surfing List (58 entries) <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="First"/> <input type="button" value="Last"/> <input type="button" value="Export (.xml)"/> <input type="button" value="Export (.csv)"/>					
<input type="button" value="Refresh"/>					
User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	TCP	192.168.123.148:52443		40.100.151.226:443	2019/07/18 14:18~
	TCP	192.168.123.148:52442		40.100.151.226:443	2019/07/18 14:18~

Internet Surfing Statistic		
Item	Value setting	Description
Previous	Button	Click the Previous button; you will see the previous page of the track list.
Next	Button	Click the Next button; you will see the next page of the track list.
First	Button	Click the First button; you will see the first page of the track list.
Last	Button	Click the Last button; you will see the last page of the track list.
Export (.xml)	Button	Click the Export (.xml) button to export the track list to an xml file.
Export (.csv)	Button	Click the Export (.csv) button to export the track list to a csv file.
Refresh	Button	Click the Refresh button to refresh the track list.

2.5.2 Network Traffic

Navigate to the Status > Usage > Network Traffic tab.

The **Network Traffic** window shows network traffic statistics. WAN, LAN, Wi-Fi Module One and Wi-Fi Module Two can be selected from the drop-down list.



2.5.3 Login Info

Navigate to the Status > Usage > Login Info.

The **Login Info** window shows the administrator login records.

Device Manager Login Statistics Previous Next First Last Export (.xml) Export (.csv)				
Refresh				
User Name	Protocol Type	IP Address	Info	Duration Time
admin	HTTP	192.168.123.148	Admin	2019/06/12 00:35~
admin	HTTP	192.168.123.148	Admin	2019/07/18 11:12~
admin	HTTP	192.168.123.148	Admin	2019/07/18 11:40~
admin	HTTP	192.168.123.148	Admin	2019/07/18 14:01~


Device Manager Login Statistic		
Item	Value setting	Description

Previous	Button	Click the Previous button; you will see the previous page of the login information.
Next	Button	Click the Next button; you will see the next page of the login information.
First	Button	Click the First button; you will see the first page of the login information.
Last	Button	Click the Last button; you will see the last page of the login information.
Export (.xml)	Button	Click the Export (.xml) button to export the login information to an xml file.
Export (.csv)	Button	Click the Export (.csv) button to export the login information to a csv file.
Refresh	Button	Click the Refresh button to refresh the login information.

2.5.4 Hotspot Usage

Navigate to the Status > Usage > Portal Usage tab.

The **Hotspot Usage** windows displays hotspot service user statistics.

 Hotspot Services User Statistics Previous Next First Last Refresh ^						
User Name	Status	Create Time	Remaining Lease Time	Time Used	Expiration Time	User Level

Hotspot Services User Login Statistics

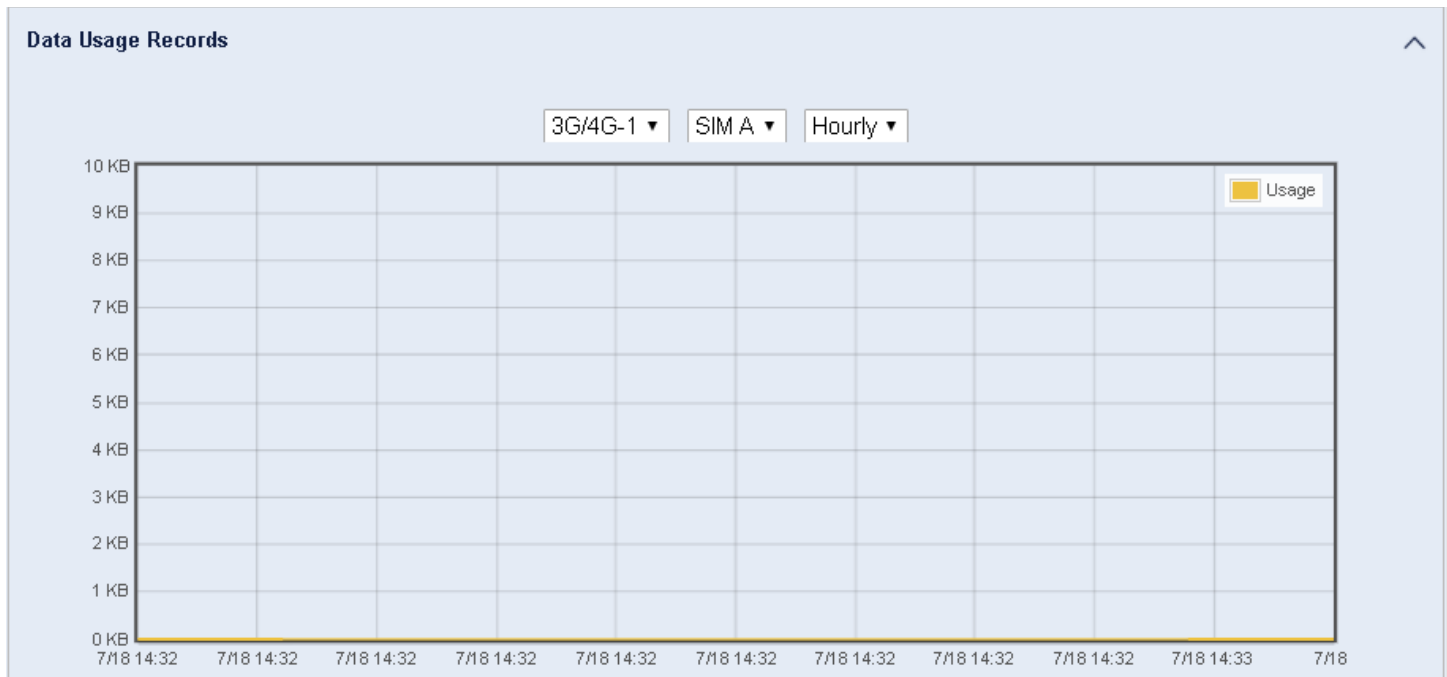
Item	Value setting	Description
------	---------------	-------------

User Name	System data.	Displays the User Name of user account created in User Rule > User > User Profile.
Status	System data.	Displays the Status of user account about logging Hotspot Services. Online for the users who have logged in to the Hotspot Services; Offline for the users who have already signed out.
Create Time	System data.	Displays the Create Time that user account created.
Remaining Lease Time	System data.	Displays the Remaining Lease Time of the user account. If the remaining time is zero, the corresponding user account can't be use for login Hotspot Services anymore. If the Lease Time of user account is empty, the remaining lease time field is shown empty. It means that the user account can be used all the time.
Time Used	System data.	Displays the Time Used since the user login to the Hotspot Services.
Expiration Time	System data.	Displays the Expiration Time of the user account. Tells the user what time the user account will be useless (expired). If the Lease Time of user account is empty, the expiration time field is also empty. It means that the user account can be used all the time (no expiry).
User Level	System data.	Displays the User Level of the user account. It can be Admin, Staff, Guest, and Passenger.
Previous	Button.	Click the Previous button; you will see the previous page of login statistics.
Next	Button.	Click the Next button; you will see the next page of login statistics.
First	Button.	Click the First button; you will see the first page of login statistics.
Last	Button.	Click the Last button; you will see the last page of login statistics.
Refresh	Button.	Click the Refresh button to refresh the login statistics.

2.5.5 Cellular Usage

Navigate to the Status > Usage > Cellular Usage tab.

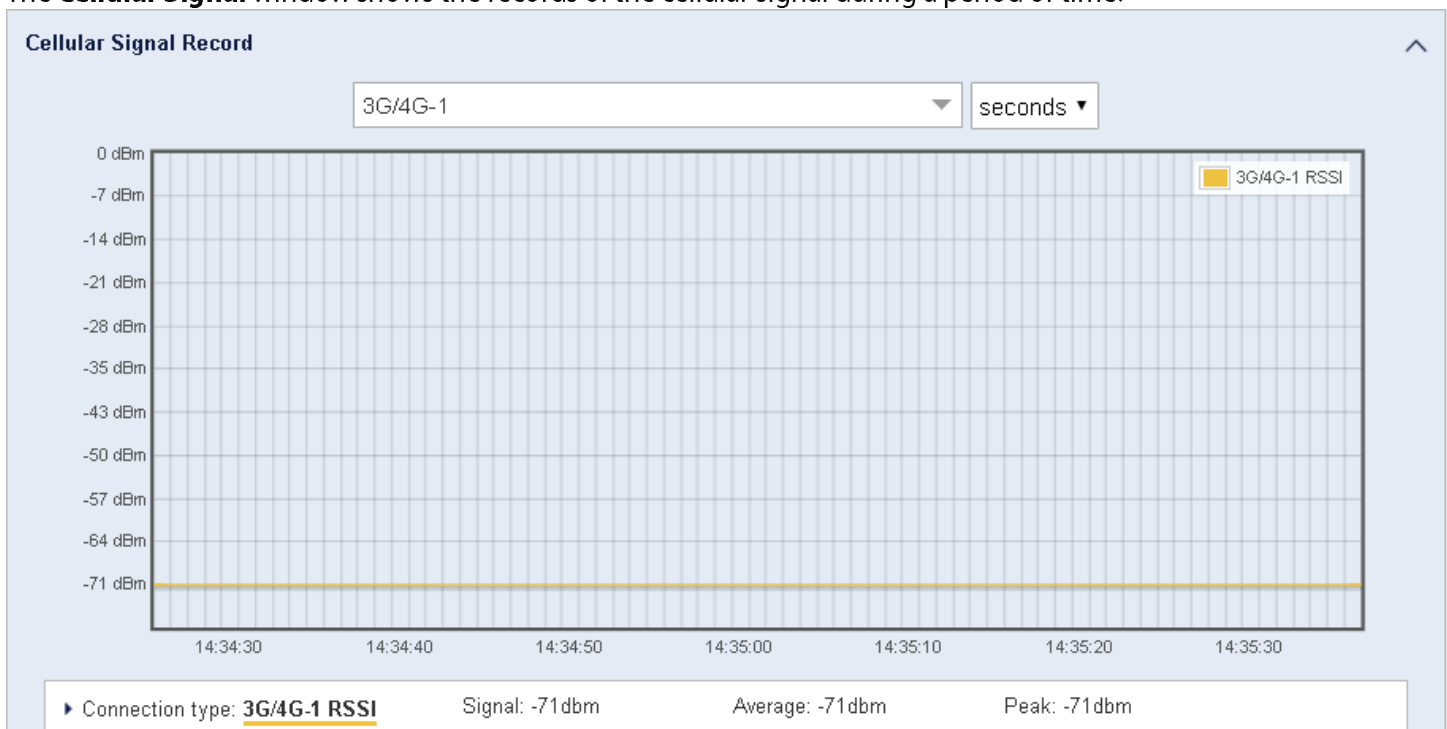
The **Cellular Usage** window shows Data Usage Records on the cellular network. SIM A and SIM B can be selected in the drop-down menu. The cellular data usage can be accumulated per hour or per day. To enable the recording of cellular usage, go **Service -> Cellular Toolkit -> Data limit** page, and add a usage profile.



2.5.6 Cellular Signal

Navigate to the Status > Statistics & Reports > Cellular Signal tab.

The **Cellular Signal** window shows the records of the cellular signal during a period of time.



3. Network

3.1 WAN & Uplink

3.1.1 Physical Interface

Navigate to the Network > WAN & Uplink > Physical Interface tab.

The **Physical Interface List** window shows the configuration on the physical WAN interface and provides the Edit button. Click Edit to access the **Interface Configuration** window.

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

The **Interface Configuration** window provides Physical Interface Settings (3G/4G, Ethernet, Wi-Fi Module One, Wi-Fi Module Two). For WAN-2, WAN-3 and WAN-4, operation mode can be always on, failover or disable. VLAN tagging can be enabled with VLAN ID 1 – 4095 by manually typing in.

Interface Configuration (WAN - 1)	
Item	Setting
Physical Interface	3G/4G
Operation Mode	Always on
VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="0"/> (1-4095)
<div>Save Undo</div>	

Interface Configuration		
Item	Value setting	Description
Physical Interface	A mandatory field. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be 3G/4G, Ethernet or Wi-Fi Module.
Operation Mode	A mandatory field.	<p>Disable and Failover options are available. Select Always on to make this WAN always active. Select Disable to disable this WAN interface. Select Failover to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the first or second WAN interface to failover from.</p> <p>Note: for WAN-1, only Always on option is available.</p>
VLAN Tagging	An optional setting.	<p>Check Enable box to enter tag value provided by your ISP. Otherwise uncheck the box. Value Range: 1 - 4095.</p> <p>Note: This feature is NOT available for 3G/4G WAN connection.</p>

3.1.2 Connection Setup

Navigate to the Network > WAN & Uplink > Connection Setup tab.

The **Connection Setup** window provides the logical settings on WAN connection. Click Edit to show the detail settings. The detail settings are subject to the WAN type.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<button>Edit</button>

3.1.2.1 3G/4G WAN Connection Setup

For 3G/4G WAN, the 1st window in detail settings is the **Internet Connection Configuration** window which shows 3G/4G as the WAN Type.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	3G/4G ▼

The WAN Type Configuration shows the preferred SIM card, Auto Flight Mode, SIM Switch Policy settings.

3G/4G WAN Type Configuration

Item	Setting
▶ Preferred SIM Card	SIM-A First ▼ Failback : <input type="checkbox"/> Enable
▶ Auto Flight Mode	<input type="checkbox"/> Enable
▶ SIM Switch Policy	Policy Setting

3G/4G Connection Configuration

Item	Value setting	Description
WAN Type	Mandatory field. Default setting: 3G/4G.	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only 3G/4G is available.
Preferred SIM Card	Mandatory field. Default setting: SIM-A First . Failback is unchecked by default.	<p>Choose which SIM card you want to use for the connection. When SIM-A First or SIM-B First is selected, it means the connection is built first by using SIM A/SIM B. And if the connection is failed, it will change to the other SIM card and try to dial again, until the connection is up.</p> <p>When SIM-A only or SIM-B only is selected, it will try to connect only using the SIM card you select.</p> <p>When Failback is checked, it means if the connection is not successful using the main SIM you select, it will failback to the main SIM and try to establish the connection periodically.</p> <p>Note 1: For the product with single SIM design, only SIM-A Only option is available.</p> <p>Note 2: Failback is available only when SIM-A First or SIM-B First is selected.</p>
Auto Flight Mode	Disabled by default.	<p>Check the Enable box to activate the function.</p> <p>By default, if you disable the Auto Flight Mode, the cellular module will always occupy a physical channel with cellular tower. It can get data connection instantly and receive managing SMS all the time on required.</p> <p>If you enable the Auto Flight Mode, the MG400 will pop up a message "Flight mode will cause cellular function to be disabled when the data session is offline.", and it will put the cellular module into flight mode and disconnect from the cellular tower. In addition, whenever the cellular module is going to be used for data connection to back up the failed primary connection, the cellular module will be active to connect with cellular tower and get the data connection for use, it takes few more seconds.</p> <p>Note: Keep it unchecked unless your cellular ISP asks the connected device to enable the Auto Flight Mode.</p>

The **Policy Setting** pop up window provides the settings on Failed connection times, RSSI Monitor, Network Service signal loss time and Roaming Service timeout.

Policy Setting

Item	Setting
Failed connection	<input type="text" value="0"/> (1-10) times
RSSI Monitor	<input type="checkbox"/> Enable Threshold: - <input type="text" value="0"/> (-90~-113 dBm)
Network Service	<input type="checkbox"/> Enable Loss LTE signal: <input type="text" value="0"/> (1~30 minutes)
Roaming Service	<input type="checkbox"/> Enable Timeout: <input type="text" value="0"/> (1~30 minutes)

Save

The **Connection with SIM-A / SIM-B Card** windows shows the Network Type, Dial-Up Profile, APN and other related settings.

Connection with SIM-A Card ^

Item	Setting
▶ Network Type	Auto ▾
▶ Dial-Up Profile	Manual-configuration ▾
▶ APN	<input type="text"/>
▶ IP Type	IPv4 ▾
▶ PIN Code	<input type="text"/> (Optional)
▶ Dial Number	<input type="text"/> (Optional)
▶ Account	admin (Optional)
▶ Password (Optional)
▶ Authentication	Auto ▾
▶ IP Mode	Dynamic IP ▾
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Roaming	<input type="checkbox"/> Enable

Connection with SIM-A/-B Card		
Item	Value setting	Description
Network Type	Mandatory field. Default setting: Auto.	Select Auto to register a network automatically, regardless of the network type. Select 3G only to register the 3G network only. Select LTE only to register the LTE network only.

Connection with SIM-A/-B Card		
Item	Value setting	Description
Dial-Up Profile	Mandatory field. Default setting: Manual-configuration.	<p>Enter the type of dial-up profile for your 3G/4G network. It can be Manual-configuration, APN Profile List, or Auto-detection.</p> <p>Select Manual-configuration to set APN (Access Point Name), Dial Number, Account, and Password to what your carrier provides.</p> <p>Select APN Profile List to set more than one profile to dial up in turn, until the connection is established. It will pop up a new field, please Navigate to Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List for details.</p> <p>Select Auto-detection to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database.</p> <p>Note 1: You are highly recommended to select the Manual or APN Profile List to enter the network for your subscription. Your ISP always provides such network settings for the subscribers.</p> <p>Note 2: If you select Auto-detection, it is likely to connect to the wrong network or fail to find a valid APN for your ISP.</p>
APN	Mandatory field. String format: any text.	Enter the APN you want to use to establish the connection. This is a mandatory field setting if you select Manual-configuration as dial-up profile scheme.
IP Type	Mandatory field. Default setting: IPv4.	Enter the IP type of the network service provided by your 3G/4G network. It can be IPv4 , IPv6 , or IPv4/6 .
PIN code	Optional field. String format: interger.	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Dial Number, Account, Password	Optional field. String format: any text.	Enter the optional Dial Number , Account , and Password settings if your ISP provides such settings to you. Note: These settings are only displayed when Manual-configuration is selected.
Authentication	Mandatory field. Default setting: Auto.	<p>Select PAP (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server.</p> <p>Select CHAP (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server.</p> <p>When Auto is selected, it means it will authenticate with the server either PAP or CHAP.</p>

Connection with SIM-A/-B Card		
Item	Value setting	Description
IP Mode	Mandatory field. Default setting: Dynamic IP.	<p>When Dynamic IP is selected, it means it will get all IP configurations from the carrier's server and set to the MG400 directly.</p> <p>If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to Static IP mode and fill in all parameters that required, such as IP address, subnet mask and device.</p> <p>Note: IP Subnet Mask is Mandatory field., and make sure you have the right configuration. Otherwise, the connection may get issues.</p>
Primary DNS	Optional field. String format: IP address (IPv4 type).	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Secondary DNS	Optional field. String format : IP address (IPv4 type).	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Roaming	Disabled by default.	<p>Check the box to establish the connection even the registration status is roaming, not in-home network.</p> <p>Note: It may cost more due to additional charges if the connection is under roaming.</p>

When **Dial-Up Profile** selects **APN Profile List**, the **Connection with SIM-A / SIM-B Card window** changes as following.

Connection with SIM-A Card

Item	Setting
▶ Network Type	Auto
▶ Dial-Up Profile	APN Profile List
▶ IP Type	IPv4
▶ PIN Code	<input type="text"/> (Optional)
▶ IP Mode	Dynamic IP
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Roaming	<input type="checkbox"/> Enable

Connection with SIM-A/-B Card		
Item	Value setting	Description
Network Type	Mandatory field. Default setting: Auto.	Select Auto to register a network automatically, regardless of the network type. Select 3G only to register the 3G network only. Select LTE only to register the LTE network only.
Dial-Up Profile	Mandatory field. Default setting: Manual-configuration.	Enter the type of dial-up profile for your 3G/4G network. It can be Manual-configuration , APN Profile List , or Auto-detection . Select Manual-configuration to set APN (Access Point Name), Dial Number , Account , and Password per your carrier provides. Select APN Profile List to set more than one profile to dial up in turn, until the connection is established. It will pop up a new field, please Navigate to Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List for details. Select Auto-detection to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database. Note 1: You are highly recommended to select the Manual or APN Profile List to enter the network for your subscription. Your ISP always provides such network settings for the subscribers. Note 2: If you select Auto-detection , it is likely to connect to the wrong network or fail to find a valid APN for your ISP.
IP Type	Mandatory field. Default setting: IPv4.	Enter the IP type of the network service provided by your 3G/4G network. It can be IPv4 , IPv6 , or IPv4/6 .
PIN code	Optional field. String format: interger.	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Dial Number, Account, Password	Optional field. String format: any text.	Enter the optional Dial Number , Account , and Password settings if your ISP provides such settings to you. Note: These settings are only displayed when Manual-configuration is selected.
IP Mode	Mandatory field. Default setting: Dynamic IP.	When Dynamic IP is selected, it means it will get all IP configurations from the carrier's server and set to the MG400 directly. If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to Static IP mode and fill in all parameters that required, such as IP address, subnet mask and device. Note: IP Subnet Mask is Mandatory field., and make sure you have the right configuration. Otherwise, the connection may get issues.
Primary DNS	Optional field. String format: IP address (IPv4 type).	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.

Connection with SIM-A/-B Card		
Item	Value setting	Description
Secondary DNS	Optional field. String format : IP address (IPv4 type).	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Roaming	Disabled by default.	Check the box to establish the connection even the registration status is roaming, not in-home network. Note: It may cost additional charges if the connection is under roaming.

The **SIM-A APN Profile List** shows the APN Profiles that have been applied to the MG400.

SIM-A APN Profile List
Add
Delete

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

APN Profile List
Add
Delete

SIM-A APN Profile Configuration

Item	Setting
▶ Profile Name	<input type="text" value="Profile-1"/>
▶ APN	<input type="text"/>
▶ IP Type	<input type="text" value="IPv4"/>
▶ Account	<input type="text" value="admin"/> (Optional)
▶ Password	<input type="password" value="....."/> (Optional)
▶ Authentication	<input type="text" value="Auto"/>
▶ Priority	<input type="text"/>
▶ Profile	<input type="checkbox"/> Enable

Secondary DNS

SIM-A/-B APN Profile Configuration		
Item	Value setting	Description
Profile Name	Default setting: Profile-x. String format: any text.	Enter the profile name you want to describe for this profile.
APN	String format: any text.	Enter the APN you want to use to establish the connection.

IP Type	Mandatory field. Default setting: IPv4.	Enter the IP type. It can be IPv4 , IPv6 , or IPv4/6 .
Account	String format: any text.	Enter the Account you want to use for the authentication. Value Range: 0 - 53 characters.
Password	String format: any text.	Enter the Password you want to use for the authentication.
Authentication	Mandatory field. Default setting: Auto.	Select the Authentication method for the 3G/4G connection. It can be Auto , PAP , CHAP , or None .
Priority	Mandatory field. String format: integer.	Enter the value for the dialing-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number. Value Range: 1 - 16.
Profile	Enabled by default.	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to restore what you just configure back to the previous setting.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

The **3G/4G Connection Common Configuration** window shows the configuration on 3G/4G connection.

3G/4G Connection Common Configuration

Item	Setting
▶ Connection Control	Auto-reconnect ▼
▶ Time Schedule	(0) Always ▼
▶ MTU Setup	<input type="checkbox"/> Enable
▶ IP Passthrough (Cellular Bridge)	<input type="checkbox"/> Enable Fixed MAC : <input type="text"/>
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ IGMP	Disable ▼
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

3G/4G Connection Common Configuration		
Item	Value setting	Description
Connection Control	Default setting: Auto-reconnect .	When Auto-reconnect is selected, it means it will try to keep the Internet connection on all the time whenever the physical link is connected. When Connect-on-demand is selected, it means the Internet connection will be established only when detecting data traffic.

		<p>When Connect Manually is selected, it means you need to click the Connect button to dial up the connection manually. Please Navigate to Status > Network > WAN & Uplink tab for details.</p> <p>Note: If the WAN interface serves as the primary one for another WAN interface in Failover role (and vice versa), the Connection Control parameter will not be available on both WANs as the system need to set it to "Auto-reconnect"</p>
Maximum Idle Time	Optional field. Default setting: 600 (seconds).	<p>Enter the maximum Idle time setting to disconnect the internet connection when the connection idle time is out. Value Range: 300 - 86400. Note: This field is available only when Connect-on-demand or Connect Manually is selected as the connection control scheme.</p>
Time Schedule	Mandatory field. Default setting: (0) Always is selected.	<p>When (0) Always is selected, it means this WAN is under operation all the time. Once you set another schedule rule, there will be other options to select. Please Navigate to User Rule > Scheduling for details.</p>
MTU Setup	Optional field. Uncheck by default.	<p>Check the Enable box to enable the MTU (Maximum Transmission Unit) limit and enter the MTU for the 3G/4G connection. MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1200 - 1500.</p>
IP Pass-through (Cellular Bridge)	Disabled by default. String format for Fixed MAC: MAC address, e.g. 00:50:18:aa:bb:cc	<p>When Enable box is checked, it means the MG400 will directly assign the WAN IP to the first connected local LAN client. However, when an optional Fixed MAC is filled-in a non-zero value, it means only the client with this MAC address can get the WAN IP address.</p> <p>Note: When the IP Pass-through is on, NAT and WAN IP Alias will be unavailable until the function is disabled again.</p>
NAT	Check by default.	<p>Uncheck the box to disable NAT (Network Address Translation) function.</p>
IGMP	Default setting: Disable .	<p>Select Auto to enable IGMP function. Check the Enable box to enable IGMP Proxy.</p>
WAN IP Alias	Unchecked by default. String format: IP address (IPv4 type).	<p>Check the box to enable WAN IP Alias and fill in the IP address you want to assign.</p>

The **Network Monitoring Configuration** window provides the configuration on network monitoring.

Network Monitoring Configuration ^

Item	Setting
▶ Network Monitoring Configuration	<input checked="" type="checkbox"/> Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	<input checked="" type="checkbox"/> Enable
▶ Query Interval	<input type="text" value="5"/> (seconds)
▶ Latency Threshold	<input type="text" value="3000"/> (ms)
▶ Fail Threshold	<input type="text" value="5"/> (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

Network Monitoring Configuration		
Item	Value setting	Description
Network Monitoring Configuration	Optional field. Box is checked by default.	Check the Enable box to activate the network monitoring function.
Checking Method	Optional field. DNS Query is set by default.	Choose either DNS Query or ICMP Checking to detect WAN link. With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With ICMP Checking, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.
		Query Interval defines the transmitting interval between two DNS Query or ICMP checking packets.
Loading Check	Optional field. Box is checked by default.	Check the Enable box to activate the loading check function. Enable Loading Check allows the MG400 to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.
		Latency Threshold defines the tolerance threshold of responding time.
		Fail Threshold specifies the threshold of disconnection before the router recognize the WAN link down status. Enter several

		detecting disconnection times to be the threshold before disconnection is acknowledged.
Target 1	Optional Setting. Default setting: DNS1.	Target 1 specifies the first target of sending DNS query/ICMP request. DNS1: set the primary DNS to be the target. DNS2: set the secondary DNS to be the target. Device: set the Current device to be the target. Other Host: enter an IP address to be the target.
Target 2	Optional Setting. Default setting: None.	Target 2 specifies the second target of sending DNS query/ICMP request. None: no second target is required. DNS1: set the primary DNS to be the target. DNS2: set the secondary DNS to be the target. Device: set the Current device to be the target. Other Host: enter an IP address to be the target.
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the settings.

3.1.2.2 Ethernet WAN Connection Setup

To select WAN/LAN1 RJ45 port as the Ethernet WAN connection port, in Physical **Interface configuration** window, select Ethernet.

Interface Configuration (WAN - 2)

Item	Setting
▶ Physical Interface	Ethernet ▼
▶ Operation Mode	Always on ▼
▶ VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="0"/> (1-4095)

Save

Undo

Interface Configuration		
Item	Value setting	Description
Physical Interface	WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be 3G/4G, Ethernet or Wi-Fi Module.
Operation Mode	A Need to select setting.	<p>Define the operation mode of the interface.</p> <p>Select Always on to make this WAN always active.</p> <p>Select Disable to disable this WAN interface.</p> <p>Select Failover to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch Failover from.</p> <p>(Note: for WAN-1, only Always on option is available.)</p>
VLAN Tagging	Optional setting.	<p>Check Enable box to enter tag value provided by your ISP. Otherwise uncheck the box.</p> <p>Value Range: 1 - 4095.</p> <p>Note: This feature is NOT available for 3G/4G WAN connection.</p>
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the settings.

To edit the Ethernet WAN connection setup, click Edit on WAN-2.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<button>Edit</button>
WAN-2	Ethernet	Always on	Dynamic IP	<button>Edit</button>

The WAN Type drop-down list provides 5 WAN types: Static IP, Dynamic IP, PPPoE, PPTP and L2TP.

Internet Connection Configuration (WAN - 2)	
Item	Setting
▶ WAN Type	Dynamic IP ▼

Following the descriptions for those 5 WAN types:

- Static IP: Select this option if ISP provides a fixed IP to you when you subscribe the service.
- Dynamic IP: The WAN IP address is assigned from a DHCP server.
- PPP over Ethernet: Also known as PPPoE. This WAN type is widely used for ADSL connection.
- PPTP: WAN connection via **Point to Point Tunnelling Protocol**.
- L2TP: WAN connection via **Layer 2 Tunnelling Protocol**.

3.1.2.2.1 Static IP

Following the example of setting the Ethernet WAN type to static IP.

Internet Connection Configuration (WAN - 2)

Item	Setting
▶ WAN Type	Static IP ▼

Static IP WAN Type Configuration

Item	Setting
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	255.255.255.0 (/24) ▼
▶ WAN Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/> (Optional)

Static IP WAN Type Configuration		
Item	Value setting	Description
WAN IP Address	Mandatory field.	Enter the WAN IP address given by your Service Provider.
WAN Subnet Mask	Mandatory field.	Enter the WAN subnet mask given by your Service Provider.
WAN Device	Mandatory field.	Enter the WAN device IP address given by your Service Provider.
Primary DNS	Mandatory field.	Enter the primary WAN DNS IP address given by your Service Provider.
Secondary DNS	Optional field.	Enter the secondary WAN DNS IP address given by your Service Provider.

3.1.2.2.2 Dynamic IP

Following the example of setting the Ethernet WAN type to Dynamic IP.

Internet Connection Configuration (WAN - 2)

Item	Setting
▶ WAN Type	Dynamic IP ▼

Dynamic IP WAN Type Configuration

Item	Setting
▶ Host Name	<input type="text"/> (Optional)
▶ ISP Registered MAC Address	<input type="text" value="admin"/> <input type="button" value="Clone"/> (Optional)

Dynamic IP WAN Type Configuration

Item	Value setting	Description
Host Name	Optional field	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	Optional field	Enter the MAC address that you have registered with your service provider. Or Click the Clone button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to Internet.

3.1.2.2.3 PPPoE

Following the example of setting the Ethernet WAN type to PPPoE.

Internet Connection Configuration (WAN - 2)

Item	Setting
▶ WAN Type	<input type="text" value="PPPoE"/>

PPPoE WAN Type Configuration

Item	Setting
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Connection Control	<input type="text" value="Auto-reconnect"/>
▶ Service Name	<input type="text"/> (Optional)
▶ Assigned IP Address	<input type="text"/> (Optional)

PPPoE WAN Type Configuration		
Item	Value setting	Description
PPPoE Account	Mandatory field.	Enter the PPPoE Username provided by your Service Provider.
PPPoE Password	Mandatory field.	Enter the PPPoE password provided by your Service Provider.
Primary DNS	Optional field.	Enter the IP address of Primary DNS server.
Secondary DNS	Optional field.	Enter the IP address of Secondary DNS server.
Connection Control	Mandatory field.	<p>Three options:</p> <ol style="list-style-type: none"> 1. Auto-reconnect. It is for automatically connect when connection establish after a disconnect. 2. Connect-on-demand. When data transfers between LAN and WAN, connection establishes. When traffic idle time reaches the value of preset maximum idle time, connection disconnect. <p>Manually. Connection and disconnection by manual control.</p>
Service Name	Optional field.	Enter the service name if your ISP requires it.
Assigned IP Address	Optional field.	Enter the IP address assigned by your Service Provider.

3.1.2.2.4 PPTP

Following the example of setting the Ethernet WAN type to PPTP.

Internet Connection Configuration (WAN - 2) ^

Item	Setting
▶ WAN Type	PPTP ▼

PPTP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address / Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="password"/>
▶ Connection ID	<input type="text"/> (Optional)
▶ Connection Control	Auto-reconnect ▼
▶ MTU Setup	<input type="checkbox"/> Enable
▶ MPPE	<input type="checkbox"/> Enable

PPTP WAN Type Configuration		
Item	Value setting	Description
IP Mode	Mandatory field.	<p>Select either Static or Dynamic IP address for PPTP Internet connection.</p> <ul style="list-style-type: none"> When Static IP Address is selected, you will need to enter the WAN IP Address, WAN Subnet Mask, and WAN Device. <ul style="list-style-type: none"> WAN IP Address (Mandatory field.): Enter the WAN IP address given by your Service Provider. WAN Subnet Mask (Mandatory field.): Enter the WAN subnet mask given by your Service Provider. WAN Device (Mandatory field.): Enter the WAN device IP address given by your Service Provider. When Dynamic IP is selected, there are no above settings required.
Server IP Address/Name	Mandatory field.	Enter the PPTP server name or IP Address.
PPTP Account	Mandatory field.	Enter the PPTP username provided by your Service Provider.
PPTP Password	Mandatory field.	Enter the PPTP connection password provided by your Service Provider.
Connection ID	Optional field.	Enter a name to identify the PPTP connection.
Connection Control	Mandatory field.	<p>Three options:</p> <ol style="list-style-type: none"> Auto-reconnect. It is for automatically connect when connection establish after a disconnect. Connect-on-demand. When data transfers between LAN and WAN, connection establishes. When traffic idle time

		reaches the value of preset maximum idle time, connection disconnect.
		5. Manually. Connection and disconnection by manual control.
MPPE	Optional field.	Select Enable to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

3.1.2.2.5 L2TP

Following the example of setting the Ethernet WAN type to L2TP.

Internet Connection Configuration (WAN - 2) ^

Item	Setting
▶ WAN Type	L2TP ▾

L2TP WAN Type Configuration ^

Item	Setting
▶ IP Mode	Dynamic IP Address ▾
▶ Server IP Address / Name	<input type="text"/>
▶ L2TP Account	<input type="text"/>
▶ L2TP Password	<input type="password"/>
▶ Connection Control	Auto-reconnect ▾
▶ MTU Setup	<input type="checkbox"/> Enable
▶ Service Port	User-defined ▾ <input type="text" value="1702"/>
▶ MPPE	<input type="checkbox"/> Enable

L2TP WAN Type Configuration		
Item	Value setting	Description
IP Mode	Mandatory field.	<div>Select either Static or Dynamic IP address for L2TP Internet connection.</div> <ul style="list-style-type: none">When Static IP Address is selected, you will need to enter the WAN IP Address, WAN Subnet Mask, and WAN Device.<ul style="list-style-type: none">WAN IP Address (Mandatory field.): Enter the WAN IP address given by your Service Provider.WAN Subnet Mask (Mandatory field.): Enter the WAN

		subnet mask given by your Service Provider.
		<ul style="list-style-type: none"> ■ WAN Device (Mandatory field.): Enter the WAN device IP address given by your Service Provider. ● When Dynamic IP is selected, there are no above settings required.
Server IP Address/Name	Mandatory field.	Enter the L2TP server name or IP Address.
L2TP Account	Mandatory field.	Enter the L2TP username provided by your Service Provider.
L2TP Password	Mandatory field.	Enter the L2TP connection password provided by your Service Provider.
Connection Control	Mandatory field.	<p>Three options:</p> <ol style="list-style-type: none"> 6. Auto-reconnect. It is for automatically connect when connection establish after a disconnect. 7. Connect-on-demand. When data transfers between LAN and WAN, connection establishes. When traffic idle time reaches the value of preset maximum idle time, connection disconnect. <p>Manually. Connection and disconnection by manual control.</p>
Service Port	Mandatory field.	<p>Enter the service port that the Internet service.</p> <p>There are three options can be selected:</p> <ul style="list-style-type: none"> ● Auto: Port will be automatically assigned. ● 1701 (For Cisco): Set service port to port 1701 to connect to CISCO server. ● User-defined: Enter a service port provided by your Service Provider.
MPPE	Optional field	Select Enable to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

3.1.2.3 Wi-Fi WAN Connection Setup

To select 2.4GHz / 5GHz Wi-Fi connection as the Ethernet WAN connection, in Physical **Interface configuration** window, select **Wi-Fi Module One** for 2.4GHz, or **Wi-Fi Module Two** for 5GHz.

Interface Configuration (WAN - 3)

Item	Setting
Physical Interface	WiFi Module One ▼
Operation Mode	Always on ▼
VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="0"/> (1-4095)

Save

Undo

Internet Connection Configuration (WAN - 3)

Item Setting

▶ WAN Type Uplink ▼

Internet Connection Configuration

Item	Value setting	Description
WAN Type	Mandatory field. Default setting: Uplink .	From the dropdown box, select Internet connection method for Wi-Fi Uplink Connection. Only Uplink is available.

Wi-Fi Uplink WAN Type Configuration

Item Setting

▶ Connect to AP default-Ch#1-Open (None) Scan

▶ Network Type NAT Mode ▼

▶ IP Mode Dynamic IP ▼

▶ Host Name (Optional)

▶ Connection Control Connect-on-demand ▼

▶ Maximum Idle Time 600 (seconds)

▶ Fast Roaming ☐ Enable Signal Threshold 40 %

▶ Fast Roaming Channels N/A ▼ N/A ▼ N/A ▼

Wi-Fi Uplink WAN Type Configuration

Item	Value setting	Description
Connect to AP	System data.	Display the information of the AP for connecting. You can Click the Scan button and select an AP for the uplink network. Besides, you can also create uplink profile(s) for ease of connecting to an available Uplink network. Refer to Network > Wi-Fi > Uplink Profile tab.
Network Type	Mandatory field. Default setting: NAT Mode.	Select the expected network type for the Wi-Fi Uplink connection. It can be NAT Mode, or NAT Disable. When NAT Mode is selected, the NAT function is activated on the

		Wireless Uplink connection; When NAT Disable is selected, the NAT function is deactivated on the Wireless Uplink connection, and it can function as a router with manually configured routing setting.
IP Mode	Mandatory field. Default setting: Dynamic IP.	Enter the IP mode for the wireless uplink Interface. It can be Dynamic IP or Static IP . When Dynamic IP is selected, the MG400 will request a IP from the Uplink Network as the IP for the uplink interface ; When Static IP is selected, you need to manually configure the IP address settings for the uplink interface. The settings include IP address, subnet mask, device, and primary/secondary DNS.
Connection Control	Mandatory field.	There are three connection modes. <ul style="list-style-type: none"> • Auto-reconnect (Always on) enables the router to always keep the Internet connection on. • Connect-on-demand enables the router to automatically re-establish Internet connection as soon as you attempt to access the Internet. Internet connection will be disconnected when it has been idle for a specified idle time. • Connect Manually allows you to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.
Maximum Idle Time	Optional field. Default value: 600 (seconds).	Enter the maximum Idle time setting to disconnect the internet connection when the connection idle timed out. Value Range: 300 - 86400. Note: This field is available only when Connect-on-demand or Connect Manually is selected as the connection control scheme.
Fast Roaming	Optional field. Unchecked is selected by default.	Click the Enable checkbox to activate the fast roaming function. In addition, you can also enter a threshold value for changing from one AP to another near-by AP. The default threshold value is 40%. Value Range: 30 - 60%.
Fast Roaming Channels	Optional field. Default setting: System data.	You can enter up to three channels for Wi-Fi Uplink fast roaming function. If you don't enter any channel, the Wi-Fi uplink will just operate on original connection channel.

Click **Scan** button, from **Wireless AP List**, enter the **Security Key**, then click **Apply** to start the connection.

Wireless AP List							^
SSID	BSSID	Channel	Mode	Security	Signal Strength	Action	
2Fly4Awifi_2G	b0:4e:26:d5:96:3b	5	b/g/n Mixed	WPA2-PSK(AES)	7%	Security Key: <input type="text"/>	<input type="button" value="Apply"/>
Beam-KB2	ee:fa:bc:35:ea:ee	6	b/g Mixed	WPA2-PSK(AES)	2%	Security Key: <input type="text"/>	<input type="button" value="Apply"/>
Area51	f0:9f:c2:71:4e:bc	6	b/g/n Mixed	WPA2-PSK(AES)	39%	Security Key: <input type="text"/>	<input type="button" value="Apply"/>

3.1.3 Load Balance

Navigate to the Network > WAN & Uplink > Load Balance tab.

The **Load Balance** window provides the settings on load balance on multiple WAN connection.

There are three options for load balance: By Smart Weight, By Specific Weight, and By User Policy. You can select one of the options according to application requirement and network status. The strategies are explained as below.

By Smart Weight

With the By Smart Weight strategy, the MG400 will take the line speed settings of all WAN interfaces specified in Physical Interface configuration page as default ratio for data transfer. Based on the ratio of packet bytes passing different WAN interfaces in 5 minutes, the system will decide how many sessions will be transferred via each WAN interface for next period. You may take it as a fast approach to maximize the bandwidth utilization of multiple WAN interfaces in MG400.

Configuration		^
Item	Setting	
▶ Load Balance	<input checked="" type="checkbox"/> Enable	
▶ Load Balance Strategy	<input type="text" value="By Smart Weight"/>	
		<input type="button" value="Save"/> <input type="button" value="Undo"/>

By Specific Weight

When you select the By Specific Weight strategy, you need to set up the ratio of WAN-1/WAN-2 as sessions sent ratio. Total ratio come together should be 100%. Device's traffic control process will operate routing adequately based on the dedicated weights ratio on each WAN interface.

Weight Definition

WAN ID	Weight	Action
WAN - 1	100 %	<button>Edit</button>
WAN - 2	0 %	<button>Edit</button>
WAN - 3	0 %	<button>Edit</button>

Save

Undo

Weight Definition		
Item	Value setting	Description
WAN ID	NA	The Identifier for each available WAN interface.
Weight	Mandatory field. Set with bandwidth ratio of each WAN by default.	Enter the weight ratio for each WAN interface. Initially, the bandwidth ratio of each WAN is set by default. Value Range: 1 - 99. Note: The sum of all weights can't be greater than 100%.
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to restore what you just configure back to the previous setting.

By User Policy

When the By User Policy strategy is selected, it allows you to mapping Source IP, Destination IP, or Destination Port to an assigned WAN interface. The IP address can be a single IP, or a subnet or IP range. Destination port can be a single port or port range. You can set the mapping with IP address and leave others just left as Any/ All. Moreover, you can also set protocol as TCP, UDP or both.

Configuration

Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By User Policy

User Policy List
Add
Delete

ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions
Save Undo						

User Policy Configuration

Item	Setting
Source IP Address	Any
Destination IP Address	Any
Destination Port	All
Protocol	Both
WAN Interface	WAN - 1
Policy	<input type="checkbox"/> Enable
Save	
Save Undo	

User Policy Configuration		
Item	Value setting	Description
Source IP Address	Mandatory field. Default setting: Any .	Four options can be selected: Any: No specific Source IP is provided. The traffic may come from any source Subnet: Enter the Subnet for the traffics come from the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24.

User Policy Configuration		
Item	Value setting	Description
		IP Range: Enter the IP Range for the traffics come from the IPs Single IP: Enter a unique IP Address for the traffics come from the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.
Destination IP Address	Mandatory field. Default setting: Any .	Five options can be selected: Any: No specific destination IP is provided. The traffic may come to any destination. Subnet: Enter the Subnet for the traffics come to the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. IP Range: Enter the IP Range for the traffics come to the IPs Single IP: Enter a unique IP Address for the traffics come to the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101. Domain Name: Enter the domain name for the traffics come to the domain
Destination Port	Mandatory field. Default setting: All .	Four options can be selected: All: No specific destination port is provided. Port Range: Enter the Destination Port Range for the traffics Single Port: Enter a unique destination Port for the traffics Well-known Applications: Select the service port of well-known application defined in dropdown list.
Protocol	Mandatory field. Default setting: Both .	Three options can be selected. They are Both , TCP , and UDP .
WAN Interface	Mandatory field. Default setting: WAN-1 .	You can select the interface that traffic should go. Note that the WAN interface dropdown list will only show the available WAN interfaces.
Policy	Unchecked by default.	Check the Enable checkbox to activate the policy rule.
Save	Button	Click the Save button to save the configuration
Undo	Button	Click the Undo button to restore what you just configure back to the previous setting.

3.2 LAN & VLAN

This section provides the configuration of LAN and VLAN.

3.2.1 Ethernet LAN

Navigate to the Network > LAN & VLAN > Ethernet LAN tab.

The **Ethernet LAN** window provides the settings on load Ethernet LAN port.

Configuration	
Item	Setting
▶ IP Mode	Static IP
▶ LAN IP Address	<input type="text" value="192.168.123.254"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>

Configuration		
Item	Value setting	Description
IP Mode	System data.	It shows the LAN IP mode for the MG400 according to the related configuration. Static IP: If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. Dynamic IP: If all the available WAN interfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	Mandatory field. Default setting: 192.168.123.254	Enter the local IP address of the MG400. The network device(s) on your network need to use the LAN IP address of the MG400 as their Default Device. You can change it if necessary. Note: It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.
Subnet Mask	Mandatory field. Default setting: 255.255.255.0 (/24)	Select the subnet mask for the MG400 from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of the MG400, so there are maximum 253 clients allowed in LAN network. Value Range: 255.0.0.0 (/8) - 255.255.255.252 (/30).

The MG400 provides the LAN IP alias function for some special management consideration. You can add additional LAN IP for the MG400, and access to the MG400 with the additional IP.

Additional IP
Add
Delete
^

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action
<div> Save Undo </div>						

Additional IP Configuration
^
x

Item	Setting
▶ Name	<input type="text"/>
▶ Interface	lo ▼
▶ IP Address	<input type="text"/>
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Enable	<input type="checkbox"/>
<div> Save </div>	
<div> Save Undo </div>	

Configuration		
Item	Value setting	Description
Name	Optional field.	Enter the name for the alias IP address.
Interface	Mandatory field. Default setting: lo.	Enter the Interface type. It can be lo or br0.
IP Address	Optional field. Default setting: 192.168.123.254.	Enter the addition IP address for the MG400.
Subnet Mask	Mandatory field. Default setting: 255.255.255.0 (/24)	<p>Select the subnet mask for the MG400 from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of the MG400, so there are maximum 253 clients allowed in LAN network.</p> <p>Value Range: 255.0.0.0 (/8) - 255.255.255.255 (/32).</p>
Save	Button.	Click the Save button to save the configuration.

3.2.2 VLAN

Navigate to the Network > LAN & VLAN > VLAN tab.

The **VLAN** window provides the settings on VLAN.

Two VLAN types can be set up in the MG400: **Port-based VLAN** and **Tag-based VLAN**.

See following for the **Port-based VLAN** setting.

Configuration

Item	Setting
▶ VLAN Types	Port-based ▼
▶ System Reserved VLAN ID	Start ID <input type="text" value="1"/> (1-4091) ~ End ID <input type="text" value="5"/>

Configuration		
Item	Value setting	Description
VLAN Type	Default setting: Port-based.	<p>Select the VLAN type that you want to adopt for organizing user local subnets.</p> <p>Port-based: Port-based VLAN allows you to add rule for each LAN port, and you can do advanced control with its VLAN ID.</p> <p>Tag-based: Tag-based VLAN allows you to add VLAN ID, select member and DHCP Server for this VLAN ID. Navigate to Tag-based VLAN List table.</p>
System Reserved VLAN ID	Default setting: 1 - 5.	<p>Enter the VLAN ID range that is reserved for the system operation. For the Port-based/Tag-based VLAN grouping, only use the ID outside the reserved range.</p> <p>Value Range: 1 - 4091.</p>

Port-based VLAN List
Add
Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	<input checked="" type="checkbox"/>	Edit

Apply
Inter VLAN Group Routing

By clicking **Detail**, you can check the port members in the existed setting.

VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID
<p>▶ Port Members:</p> <p>▶ Port: Port-2, Port-3</p> <p>▶ 2.4G: VAP-1, VAP-2, VAP-3, VAP-4, VAP-5, VAP-6, VAP-7, VAP-8</p> <p>▶ 5G: VAP-1, VAP-2, VAP-3, VAP-4, VAP-5, VAP-6, VAP-7, VAP-8</p>						

By clicking **Add**, you can add a Port-based VLAN rule. By clicking **Edit**, you can edit an existed rule.

×

Port-based VLAN Configuration

Item	Setting
▶ Name	LAN
▶ VLAN ID	Native VLAN
▶ VLAN Tagging	Disable
▶ NAT / Bridge	NAT
▶ Port Members	Port: <input checked="" type="checkbox"/> Port-2 <input checked="" type="checkbox"/> Port-3 2.4G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8 5G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8
▶ LAN to Join	<input type="checkbox"/> Enable <input type="text" value="DHCP 1"/>
▶ WAN & WAN VID to Join	<input type="text" value="All WANs"/> <input type="text" value="None"/>
▶ LAN IP Address	192.168.123.254
▶ Subnet Mask	255.255.255.0 (/24)
▶ DHCP Server / Relay	Server
▶ DHCP Server Name	DHCP 1
▶ IP Pool	Starting Address <input type="text" value="192.168.123.100"/> Ending Address <input type="text" value="192.168.123.200"/>

✕

▶ Subnet Mask 255.255.255.0 (/24) ▼

▶ DHCP Server / Relay Server ▼

▶ DHCP Server Name DHCP 1

▶ IP Pool Starting Address 192.168.123.100 Ending Address 192.168.123.200

▶ Lease Time 900 seconds

▶ Domain Name (Optional)

▶ Primary DNS (Optional)

▶ Secondary DNS (Optional)

▶ Primary WINS (Optional)

▶ Secondary WINS (Optional)

▶ Gateway (Optional)

▶ Enable ☒

IP Fixed Mapping Rule List Add Delete

MAC Address	IP Address	Enable	Actions

Save

Port-based VLAN Configuration (part-I)

Item	Value setting	Description
Name	Cannot be modified.	Define the Name of this rule. It has a default text and cannot be modified.
VLAN ID	Mandatory field.	Define the VLAN ID number, range is 1-4094.
VLAN Tagging	Default setting: Disable.	The rule is activated per VLAN ID and Port Members configuration when Enable is selected. The rule is activated per Port Members configuration when Disable is selected.
NAT / Bridge	Default setting: NAT.	Select NAT mode or Bridge mode for the rule.

Port-based VLAN Configuration (part-I)		
Item	Value setting	Description
Port Members	These boxes are unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule.
LAN to Join	Disabled by default.	Check the Enable box and select one of the defined DHCP Server for the List to define the DHCP server for the VLAN group. If you enabled this function, all the rest settings will be greyed out, not required to configured manually.
WAN & WAN VID to Join	Default setting: All WANs.	Select which WAN or All WANs that allows Internet access. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	Mandatory field.	Assign an IP Address for the DHCP Server that the rule used, this IP address is a device IP.
Subnet Mask	Default setting: 255.255.255.0 (/24).	Select a Subnet Mask for the DHCP Server.
DHCP Server /Relay	Default setting: Server.	Define the DHCP Server type. There are three types you can select: Server , Relay , and Disable . Relay : Select Relay to enable DHCP Relay function for the VLAN group, and you only need to fill the DHCP Server IP Address field. Server : Select Server to enable DHCP Server function for the VLAN group, and you need to enter the DHCP Server settings. Disable: Select Disable to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP Relay only)	Mandatory field.	If you select Relay type of DHCP Server, assign a DHCP Server IP Address that the MG400 will relay the DHCP requests to the assigned DHCP server.
DHCP Option 82 (for DHCP Relay only)	Optional Setting.	If you select Relay type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
DHCP Server Name	Mandatory field.	Define name of the DHCP Server for the specified VLAN group.
IP Pool	Mandatory field.	Define the IP Pool range. There are Starting Address and Ending Address fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of IP pool.
Lease Time	Mandatory field. Default setting is 86400 (seconds).	Define a period of time for an IP Address that the DHCP Server leases to a new device.
Domain Name	String format can be any text.	The Domain Name of this DHCP Server. Value Range: 0 - 31 characters.
Primary DNS	IPv4 format.	The Primary DNS of this DHCP Server.

Port-based VLAN Configuration (part-I)

Item	Value setting	Description
Secondary DNS	IPv4 format.	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format.	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format.	The Secondary WINS of this DHCP Server.
Device	IPv4 format.	The MG400 of this DHCP Server.
Enable	Default setting: unchecked.	Click Enable box to activate this rule.
Save	Button.	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

Port-based VLAN Configuration (part-II)

Item	Value setting	Description
WAN & WAN VID to Join	Default setting: All WANs.	Select which WAN or All WANs that allows Internet access. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	Mandatory field.	Assign an IP Address for the DHCP Server that the rule used, this IP address is a device IP.
Subnet Mask	Default setting: 255.255.255.0(/24).	Select a Subnet Mask for the DHCP Server.
DHCP Server /Relay	Default setting: Server.	Define the DHCP Server type. There are three types you can select: Server , Relay , and Disable . Relay : Select Relay to enable DHCP Relay function for the VLAN group, and you only need to fill the DHCP Server IP Address field. Server : Select Server to enable DHCP Server function for the VLAN group, and you need to enter the DHCP Server settings. Disable : Select Disable to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP Relay only)	Mandatory field.	If you select Relay type of DHCP Server, assign a DHCP Server IP Address that the MG400 will relay the DHCP requests to the assigned DHCP server.
DHCP Option 82 (for DHCP Relay only)	Optional Setting.	If you select Relay type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
DHCP Server Name	Mandatory field.	Enter the name of the DHCP Server for the specified VLAN group.

Port-based VLAN Configuration (part-II)

Item	Value setting	Description
IP Pool	Mandatory field.	Define the IP Pool range. There are Starting Address and Ending Address fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of IP pool.
Lease Time	Mandatory field.	Define a period for an IP Address that the DHCP Server leases to a new device. By default, the lease time is 86400 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server. Value Range: 0 - 31 characters.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Device	IPv4 format	The MG400 of this DHCP Server.
Enable	Disabled by default.	Click Enable box to activate this rule.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

Mapping Rule Configuration

Item	Value setting	Description
MAC Address	Mandatory field.	Define the MAC Address target that the DHCP Server wants to match.
IP Address	Mandatory field.	Define the IP Address that the DHCP Server will assign. If there is a request from the MAC Address filled in the above field, the DHCP Server will assign this IP Address to the client whose MAC Address matched the rule.
Enable	Disabled by default.	Click Enable box to activate this rule.
Save	Button	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

Click **Inter VLAN Group Routing** button to access the **VLAN Group Internet Access Definition** pop up window.

Inter VLAN Group Routing		
Item	Value setting	Description
VLAN Group Internet Access Definition	All boxes are checked by default.	<p>By default, all boxes are checked means all VLAN ID members can access WAN interface.</p> <p>If uncheck a certain VLAN ID box, it means the VLAN ID member can't access Internet anymore.</p> <p>Note: VLAN ID 1 is available always; it is the default VLAN ID of LAN rule. The other VLAN IDs are available only when they are enabled.</p>
Inter VLAN Group Routing	Disabled by default.	<p>Click the expected VLAN IDs box to enable the Inter VLAN access function.</p> <p>By default, members in different VLAN IDs can't access each other.</p> <p>The MG400 supports up to 4 rules for Inter VLAN Group Routing. For example, if ID_1 and ID_2 are checked, it means members in VLAN ID_1 can access members of VLAN ID_2, and vice versa.</p>
Save	Button	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

87 of 335
©2019 BEAM

Configuration

Item	Setting
▶ VLAN Type	Tag-based ▼
▶ System Reserved VLAN ID	Start ID <input type="text" value="1"/> (1-4091) ~ End ID <input type="text" value="5"/>

Tag-based VLAN List
Add
Delete

VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions	
Native VLAN	<input checked="" type="checkbox"/>	Port: <input checked="" type="checkbox"/> Port-1 <input checked="" type="checkbox"/> Port-2 <input checked="" type="checkbox"/> Port-3 2.4G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8 5G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8		DHCP 1			Edit Select

Press **Add** button to add a new rule.

Tag-based VLAN Configuration

Item	Setting
▶ VLAN ID	<input type="text" value="0"/>
▶ Internet Access	<input checked="" type="checkbox"/> Enable
▶ Port Members	Port: <input type="checkbox"/> Port-1 <input type="checkbox"/> Port-2 <input type="checkbox"/> Port-3 2.4G: <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8 5G: <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8
▶ Bridge Interface	DHCP 1 ▼

Save

Tag-based VLAN Configuration (Part-I)

Item	Value setting	Description
VALN ID	Mandatory field.	Define the VLAN ID number, that is outside the system reserved range. Value Range: 1 - 4095.
Internet Access	Enabled by default.	Click Enable box to allow the members in the VLAN group access to internet.
Port Members	Disabled by default.	Check the LAN port box(es) to join the VLAN group. Check the VAP box(es) to join the VLAN group.
Bridge Interface	Default setting: DHCP 1.	Select a predefined DHCP Server, a New to define a new DHCP server for these members of this VLAN group.
Save	Button.	Click Save button to save the configuration. Note: After clicking Save button, always click Apply button to apply the settings.

If you select New to create a new DHCP server setting for the VLAN group, you will need to set up the following configuration.

► Bridge Interface	New ▼
► IP Address	<input type="text"/>
► Subnet Mask	255.255.255.0 (/24) ▼
► DHCP Relay	<input type="checkbox"/> Enable & Server IP : <input type="text"/>
► WAN Interface	WAN - 1 ▼
► DHCP Relay Option 82	<input type="checkbox"/> Enable
Save	

Tag-based VLAN Configuration (part-II)

Item	Value setting	Description
IP Address	Mandatory field.	Assign an IP Address for the DHCP Server that the rule used, this IP address is a device IP.
Subnet Mask	Default setting: 255.255.255.0(/24).	Select a Subnet Mask for the DHCP Server.
DHCP Relay	Disabled by default.	Check the box to enable the DHCP Relay function for the VLAN group, and you only need to fill the DHCP Server IP Address field.
WAN Interface	Default setting: WAN-1.	Select which WAN interface that allows Internet access.
DHCP Option 82	Optional Setting.	If you select Relay type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
Save	Button	Click the Save button to save the configuration

After the configuration is applied, the configured tag-based VLAN group information will be displayed in the following window.

Tag-based VLAN Summary		^
Port	VLAN IDs	
Port1	Native VLAN	
Port2	Native VLAN	
Port3	Native VLAN	

3.2.3 DHCP Server

Navigate to the Network > LAN & VLAN > DHCP Server tab.

The DHCP Server setting allows you to create and customizes DHCP Server policies to assign IP Addresses to the MG400 on the local area network (LAN).

The MG400 allows you to customize your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group), and it supports up to a maximum of 4 policy sets.

DHCP Server ListAddDeleteDHCP Client List

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	900		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	EditFixed Mapping

When Add button is applied, DHCP Server Configuration pop up window will appear.

×

DHCP Server Configuration

Item	Setting
▶ DHCP Server Name	<input type="text" value="DHCP 2"/>
▶ LAN IP Address	<input type="text" value="192.168.2.254"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>
▶ IP Pool	<div>Starting Address: <input type="text"/></div> <div>Ending Address: <input type="text"/></div>
▶ Lease Time	<input type="text" value="86400"/> seconds
▶ Domain Name	<input type="text"/> (Optional)
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Primary WINS	<input type="text"/> (Optional)
▶ Secondary WINS	<input type="text"/> (Optional)
▶ Gateway	<input type="text"/> (Optional)
▶ Server	<input type="checkbox"/> Enable

DHCP Server Configuration		
Item	Value setting	Description
DHCP Server Name	Enter text string. Mandatory field.	Enter the DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	IPv4 format. Mandatory field.	The LAN IP Address of this DHCP Server.
Subnet Mask	Default setting: 255.0.0.0 (/8)	The Subnet Mask of this DHCP Server.
IP Pool	IPv4 format. Mandatory field.	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.

DHCP Server Configuration		
Item	Value setting	Description
Lease Time	Numeric string format. Mandatory field. Default value: 86400 seconds	The Lease Time of this DHCP Server. Value Range: 300 - 604800 seconds.
Domain Name	String format can be any text.	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format.	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format.	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format.	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format.	The Secondary WINS of this DHCP Server.
Device	IPv4 format.	The MG400 of this DHCP Server.
Server	Disabled by default.	Click Enable box to activate this DHCP Server.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

The MG400 allows you to create / edit mapping rule, customize your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** window will appear.

 Mapping Rule List

^ x

MAC Address	IP Address	Enable	Actions
-------------	------------	--------	---------

When the Add button is clicked, Mapping Rule Configuration pop up window will appear.

ing Rule List

✕

Mapping Rule Configuration

Item	Setting
▶ MAC Address	<input type="text"/>
▶ IP Address	<input type="text"/>
▶ Rule	<input type="checkbox"/> Enable

Server Option List

Mapping Rule Configuration		
Item	Value setting	Description

MAC Address	MAC Address string format. Mandatory field.	The MAC Address of this mapping rule.
IP Address	IPv4 format. Mandatory field.	The IP Address of this mapping rule.
Rule	Disabled by default.	Click Enable box to activate this rule.
Save	Button.	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

When the DHCP Client List button is clicked, the DHCP Client List window will appear.

DHCP Client List Copy to Fixed Mapping ^ x					
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.148	WR-LT034	E4:B9:7A:1B:D4:35	00:08:39	<input checked="" type="checkbox"/> Select

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

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


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

Configuration ^	
Item	Setting
▶ DHCP Server Options	<input type="checkbox"/> Enable

The MG400 supports up to a maximum of 99 option settings.

DHCP Server Option List Add Delete ^						
ID	Option Name	DHCP Server Select	Option Select	Type	Value	Enable Actions

When Add/Edit button is applied, DHCP Server Option Configuration pop up window will appear.



DHCP Server Option Configuration

Item	Setting
Option Name	<input type="text" value="Option 1"/>
DHCP Sever Select	<input type="text" value="DHCP 1"/>
Option Select	<input type="text" value="DHCP OPTION 66"/>
Type	<input type="text" value="Single IP Address"/>
Value	<input type="text"/>
Enable	<input type="checkbox"/> Enable

DHCP Server Option Configuration		
Item	Value setting	Description
Option Name	Enter text string. Mandatory field.	Enter the DHCP Server Option name. Enter a name that is easy for you to understand.
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
Option Select	Mandatory field. Default setting: Option 66.	Choose the specific option from the dropdown list. It can be Option 66, Option 72, Option 144, Option 42, Option 150, or Option 160. Option 42 for ntp server; Option 66 for tftp; Option 72 for www; Option 144 for url;
Type	Dropdown list of DHCP server option value's type	Each different options has different value types.
		66 Single IP Address
		Single FQDN
		72 IP Addresses List, separated by ","
		114 Single URL
		42 IP Addresses List, separated by ","
		150 IP Addresses List, separated by ","
		160 Single IP Address
Value	IPv4 format FQDN format IP list URL format	Should conform to Type :
		Type Value
		66 Single IP Address IPv4 format

DHCP Server Option Configuration				
Item	Value setting	Description		
	Mandatory field.		Single FQDN	FQDN format
		72	IP Addresses List, separated by “,”	IPv4 format, separated by “,”
		114	Single URL	URL format
Enable	Disabled by default.	Click Enable box to activate this setting.		
Save	Button	Click the Save button to save the setting.		
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.		

The MG400 supports up to a maximum of 6 DHCP Relay configurations.

☐ **DHCP Relay Configuration List**

ID	Agent Name	LAN interface	WAN interface	Server IP	DHCP Relay Option 82	Enable	Actions
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>							

When the Add/Edit button is clicked, the DHCP Relay Configuration pop up window will appear.

☐ **DHCP Relay Configuration**

Item	Setting
▶ Agent Name	<input type="text"/>
▶ LAN interface	<input type="text" value="LAN"/>
▶ WAN interface	<input type="text" value="WAN - 1"/>
▶ Server IP	<input type="text"/>
▶ DHCP OPTION 82	<input type="checkbox"/>
▶ Enable	<input type="checkbox"/>

DHCP Relay Configuration		
Item	Value setting	Description
Agent Name	Enter text string. Mandatory field.	Enter the DHCP Relay name. Enter a name that is easy for you to understand. Value Range: 1-64 characters.

LAN Interface	Mandatory field. Default setting: LAN.	Choose a LAN Interface for the dropdown list to apply with the DHCP Relay function.
WAN Interface	Mandatory field. WAN-1 is selected by default.	Choose a WAN Interface for the dropdown list to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
Server IP	Mandatory field. Default setting: null.	Assign a DHCP Server IP Address that the MG400 will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
DHCP OPTION 82	Disabled by default.	Click Enable box to activate DHCP OPTION 82 function. Option 82 is organized as a single DHCP option that contains circuit-ID information known by the relay agent. If the relayed DHCP server required the such information, you need to enable it, otherwise, just leave it as unchecked.
Enable	Disabled by default.	Click Enable box to activate this setting.
Save	Button.	Click the Save button to save the setting.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

3.3 Wi-Fi

3.3.1 Wi-Fi Module One

Navigate to the **Network > Wi-Fi > Wi-Fi Module One** tab.

For **Wi-Fi module One**, it is using 2.4GHz frequency for the Wi-Fi connection.

Basic Configuration	
Item	Setting
▶ Operation Band	2.4G Single Band ▼

2.4G Wi-Fi Configuration	
Item	Setting
▶ Wi-Fi Module	<input checked="" type="checkbox"/> Enable
▶ Channel	Auto ▼ <input checked="" type="radio"/> By AP Numbers <input type="radio"/> By Less Interference Current : 11
▶ Wi-Fi System	802.11b/g/n Mixed ▼
▶ Wi-Fi Operation Mode	AP Router Mode ▼
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	(0) Always ▼

Configuring Wi-Fi Settings		
Item	Value setting	Description
Wi-Fi Module	Enabled by default.	Check the Enable box to activate Wi-Fi function.
Channel	Mandatory field. Default setting: Auto.	<p>Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the Regulatory Domain.</p> <p>There are two available options when Auto is selected:</p> <ul style="list-style-type: none"> ● By AP Numbers The channel will be selected according to AP numbers (The less, the better). ● By Less Interference The channel will be selected according to interference. (The lower, the better).
Wi-Fi System	Mandatory field.	<p>Enter the preferred Wi-Fi System. The dropdown list of Wi-Fi system is based on IEEE 802.11 standard.</p> <ul style="list-style-type: none"> ● 2.4G Wi-Fi can select b, g and n only or mixed with each other.

		<ul style="list-style-type: none"> ● 5G Wi-Fi can select a, n and ac only or mixed with each other.
Wi-Fi Operation Mode	Mandatory field.	Enter the Wi-Fi Operation Mode according to your application. Navigate to the following table for AP Router Mode , WDS Only Mode , and WDS Hybrid Mode settings.
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.
VAP Isolation	Enabled by default.	Check the Enable box to activate this function. It means that stations which associates to different VAPs cannot communicate with each other.
Time Schedule	Mandatory field.	Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.

By default, VAP 1 is enabled and security key is required to connect to the MG400 wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default Wi-Fi key is printed on the MG400 label. It is created randomly and differs from devices. However, it is strongly recommended that you change the Wi-Fi key upon the 1st login to the MG400.

2.4G VAP List Add Delete ^								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	BEAM_2.4GHz_1534	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit <input type="checkbox"/> Select

Click **Add** / **Edit** button in the VAP List window to create or edit the settings for a VAP. A VAP Configuration window will appear.

For VAP 1:

VAP Configuration
^ x

Item	Setting
▶ VAP	VAP1 ▼
▶ SSID	MG400_2.4G
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK ▼
▶ Encryption	AES ▼
▶ Preshared Key	l4EGMKj0j0FJL
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

VAP Configuration		
Item	Value setting	Description
SSID	String format: Any text	Enter the SSID for the VAP, decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	Disabled by default.	Check this box and enter a limitation to limit the maximum number of client station. Disabled by default. It means no special limitation on the number of connected STAs.
Authentication	Mandatory field. VAP1: default setting WPA2-PSK; Others: default setting Open.	For security, there are several authentication methods supported. Client stations should provide the key when associate with the MG400.
		When Open is selected The check box named 802.1x shows up next to the dropdown list.
		<ul style="list-style-type: none"> ● 802.1x (Disabled by default) When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server. RADIUS Server IP (The default IP is 0.0.0.0) RADIUS Server Port (The default value is 1812) RADIUS Shared Key
		When Shared is selected The pre-shared WEP key should be set for authenticating.
		When Auto is selected

VAP Configuration		
Item	Value setting	Description
		<p>The MG400 will select Open or Shared by requesting of client automatically.</p> <p>The check box named 802.1x shows up next to the dropdown list.</p> <ul style="list-style-type: none"> ● 802.1x (Disabled by default) <p>When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA or WPA2 is selected</p> <p>They are implementation of IEEE 802.11i. WPA only had implemented part of IEEE 802.11i, owns the better compatibility.</p> <p>WPA2 had fully implemented 802.11i standard and owns the highest security.</p> <ul style="list-style-type: none"> ● RADIUS Server <p>The client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA / WPA2 is selected</p> <p>It has the same setting as WPA or WPA2. The client stations can associate with the MG400 via WPA or WPA2.</p>
		<p>When WPA-PSK or WPA2-PSK is selected</p> <p>It has the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.</p>
		<p>When WPA-PSK / WPA2-PSK is selected</p> <p>It has the same setting as WPA-PSK or WPA2-PSK. The client stations can associate with the MG400 via WPA-PSK or WPA2-PSK.</p>
		<p>Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you select.</p> <p>None</p> <p>It means that the MG400 is an open system without encrypting.</p> <p>WEP</p> <p>Up to 4 WEP keys can be set, and you need to select one as current key. The key type can set to HEX or ASCII.</p> <p>If HEX is selected, the key should consist of (0 to 9) and (A to F).</p> <p>If ASCII is selected, the key should consist of ASCII table.</p> <p>TKIP</p> <p>TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>AES</p> <p>The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p>
Encryption	Mandatory field. VAP1: default setting AES; Others: default setting None.	

VAP Configuration		
Item	Value setting	Description
		You are recommended to use AES encryption instead of any others for security. TKIP / AES TKIP / AES mixed mode. It means that the client stations can associate with the MG400 via TKIP or AES . Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. With default setting, stations which associates to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with the MG400 by scanning SSID.
Enable	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this VAP.
Save	Button	Click the Save button to save the current configuration.
Undo	Button	Click the Undo button to restore configuration to previous setting before saving.

For the **WDS Only mode**, the MG400 only bridges the connected wired clients to another WDS-enabled Wi-Fi device which the MG400 has associates with. It means no wireless clients can connect to the MG400 while WDS Only Mode is selected and enabled.

Wi-Fi Operation Mode

WDS Only Mode ▼

Green AP

☐ Enable

Time Schedule

(0) Always ▼

Scan Remote AP's MAC List

Scan

Remote AP MAC 1

Remote AP MAC 2

Remote AP MAC 3

Remote AP MAC 4

WDS Only Mode		
Item	Value setting	Description
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.

Time Schedule	Mandatory field.	Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.
Scan Remote AP's MAC List	System data.	Press the Scan button to scan the spatial AP information, and then select one from the AP list, the MAC of the selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1-4	Mandatory field.	Enter the remote AP's MAC manually, or via auto-scan approach, the MG400 will bridge the traffic to the remote AP when associates successfully.

2.4G VAP List
Add
Delete

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	MG400_2.4G	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Select

Save
Undo

VAP Configuration

Item	Setting
▶ VAP	VAP1 ▼
▶ SSID	MG400_2.4G
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK ▼
▶ Encryption	AES ▼
▶ Preshared Key	I4EGMKj0j0FJL
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

VAP Configuration		
Item	Value setting	Description
SSID	String format: Any text.	Enter the SSID for the VAP, decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID.

Max. STA	Disabled by default.	<p>Check this box and enter a limitation to limit the maximum number of client station.</p> <p>Disabled by default. It means no special limitation on the number of connected STAs.</p>
Authentication	<p>Mandatory field. VAP1: WPA2-PSK is selected be default; Others: Open is selected be default.</p>	<p>For security, there are several authentication methods supported. Client stations should provide the key when associate with the MG400.</p>
		<p>When Open is selected</p> <p>The check box named 802.1x shows up next to the dropdown list.</p> <ul style="list-style-type: none"> ● 802.1x (Disabled by default) <p>When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When Shared is selected</p> <p>The pre-shared WEP key should be set for authenticating.</p>
		<p>When Auto is selected</p> <p>The MG400 will select Open or Shared by requesting of client automatically.</p> <p>The check box named 802.1x shows up next to the dropdown list.</p> <ul style="list-style-type: none"> ● 802.1x (Disabled by default) <p>When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA or WPA2 is selected.</p> <p>WPA and WPA2 are implementations of IEEE 802.11i. WPA only had implemented part of IEEE 802.11i but owns the better compatibility. WPA2 had fully implemented 802.11i standard, and owns the highest security.</p> <p>RADIUS Server</p> <p>The client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA / WPA2 is selected.</p> <p>It has the same setting as WPA or WPA2. The client stations can associate with the MG400 via WPA or WPA2.</p>
		<p>When WPA-PSK or WPA2-PSK is selected.</p> <p>It has the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.</p>
		<p>When WPA-PSK / WPA2-PSK is selected.</p> <p>It has the same setting as WPA-PSK or WPA2-PSK. The client stations can associate with the MG400 via WPA-PSK or WPA2-PSK.</p>
Encryption	Mandatory field. VAP1: AES is	<p>Select a suitable encryption method and enter the required key(s).</p> <p>The available method in the dropdown list depends on the</p>

	selected be default; Others: None is selected be default.	<p>Authentication you select.</p> <p>None It means that the MG400 is an open system without encrypting.</p> <p>WEP Up to 4 WEP keys can be set, and you need to select one as the current key. The key type can set to HEX or ASCII. If HEX is selected, the key should consist of (0 to 9) and (A to F). If ASCII is selected, the key should consist of ASCII table.</p> <p>TKIP TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>AES The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. You are recommended to use AES encryption instead of any others for security.</p> <p>TKIP / AES TKIP / AES mixed mode. It means that the client stations can associate with the MG400 via TKIP or AES. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p>
STA Isolation	VAP1: Enabled by default; Others: unchecked by default.	<p>Check the Enable box to activate this function.</p> <p>With default setting, stations which have associates to the same VAP cannot communicate with each other.</p>
Broadcast SSID	VAP1: Enabled by default; Others: unchecked by default.	<p>Check the Enable box to activate this function.</p> <p>If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with the MG400 by scanning SSID.</p>
Enable	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this VAP.
Save	Button	Click the Save button to save the current configuration.
Undo	Button	Click the Undo button to restore configuration to previous setting before saving.

Under **WDS Only** mode, only VAP1 is available for further entering the required authentication and Encryption settings. Click **Edit** button in the VAP List window and a VAP Configuration window will appear for you to configure the required settings.

For the **WDS Hybrid** mode, the MG400 bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled Wi-Fi devices which the MG400 associates with.

Wi-Fi Operation Mode	WDS Hybrid Mode ▾
Lazy Mode	<input checked="" type="checkbox"/> Enable
Green AP	<input type="checkbox"/> Enable
VAP Isolation	<input checked="" type="checkbox"/> Enable
Time Schedule	(0) Always ▾

WDS Hybrid Mode		
Item	Value setting	Description
Lazy Mode	Enabled by default.	Check the Enable box to activate this function. When the function been enabled, the MG400 can auto-learn WDS peers without manually entering another AP's MAC address. But at least one of the APs need to fill remote AP MAC addresses.
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.
VAP Isolation	Enabled by default.	Check the Enable box to activate this function. By default, enabling it means that stations which associates to different VAPs cannot communicate with each other.
Time Schedule	Mandatory field.	Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.

Under **WDS Hybrid** mode, the VAP function is available and you can further enter the required VAP settings for connecting with wireless client devices.

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	MG400_2.4G	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>Edit</div> <div>Select</div>

2.4G VAP List

Add

Delete

Save

Undo

Click **Add** / **Edit** button in the VAP List window to create or edit the settings for a VAP. A VAP Configuration window will appear.

For VAP 1:

VAP Configuration
^ x

Item	Setting
▶ VAP	VAP1 ▼
▶ SSID	<input type="text" value="MG400_2.4G"/>
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK ▼
▶ Encryption	AES ▼
▶ Preshared Key	<input type="text" value="l4EGMKj0j0FJL"/>
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

VAP Configuration		
Item	Value setting	Description
SSID	String format: Any text.	Enter the SSID for the VAP. Decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	Disabled by default.	Check this box and enter a limitation to limit the maximum number of client station. Disabled by default. It means no special limitation on the number of connected STAs.
Authentication	Mandatory field. VAP1: WPA2-PSK is selected by default; Others: Open is selected by default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with the MG400.
		When Open is selected, the check box named 802.1x shows up next to the dropdown list.
		802.1x (Disabled by default.) - When 802.1x is enabled, the client stations will be authenticated by a RADIUS server. RADIUS Server IP (The default IP is 0.0.0.0) RADIUS Server Port (The default value is 1812) RADIUS Shared Key
		When Shared is selected. The pre-shared WEP key should be set for authenticating.
		When Auto is selected. The MG400 will select Open or Shared by requesting of client

VAP Configuration		
Item	Value setting	Description
		<p>automatically.</p> <p>The check box named 802.1x shows up next to the dropdown list.</p> <ul style="list-style-type: none"> ● 802.1x (Disabled by default) <p>When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA or WPA2 is selected.</p> <p>WPA and WPA2 are implementations of IEEE 802.11i. WPA only had implemented part of IEEE 802.11i but owns the better compatibility. WPA2 had fully implemented 802.11i standard and has the highest security.</p> <p>RADIUS Server</p> <p>The client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA / WPA2 is selected.</p> <p>It has the same setting as WPA or WPA2. The client stations can associate with the MG400 via WPA or WPA2.</p>
		<p>When WPA-PSK or WPA2-PSK is selected.</p> <p>It has the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.</p>
		<p>When WPA-PSK / WPA2-PSK is selected.</p> <p>It has the same setting as WPA-PSK or WPA2-PSK. The client stations can associate with the MG400 via WPA-PSK or WPA2-PSK.</p>
Encryption	<p>Mandatory field.</p> <p>VAP1: default setting AES is selected be default;</p> <p>Others: default setting None.</p>	<p>Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you select.</p> <p>None</p> <p>It means that the MG400 is an open system without encrypting.</p> <p>WEP</p> <p>Up to 4 WEP keys can be set, and you need to select one as current key. The key type can set to HEX or ASCII.</p> <p>If HEX is selected, the key should consist of (0 to 9) and (A to F).</p> <p>If ASCII is selected, the key should consist of ASCII table.</p> <p>TKIP</p> <p>TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>AES</p> <p>The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>You are recommended to use AES encryption instead of any others for</p>

VAP Configuration		
Item	Value setting	Description
		security. TKIP / AES TKIP / AES mixed mode. It means that the client stations can associate with the MG400 via TKIP or AES . Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. With default setting, stations which have associates to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with the MG400 by scanning SSID.
Enable	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this VAP.
Save	Button.	Click the Save button to save the current configuration.
Undo	Button.	Click the Undo button to restore configuration to previous setting before saving.

3.3.2 Wi-Fi Module Two

Navigate to the **Network > Wi-Fi > Wi-Fi Module Two** tab.

For **Wi-Fi module Two**, it is using 5GHz frequency for the Wi-Fi connection.

Basic Configuration	
Item	Setting
▶ Operation Band	5G Single Band ▼

5G Wi-Fi Configuration	
Item	Setting
▶ Wi-Fi Module	<input checked="" type="checkbox"/> Enable
▶ Channel	Auto ▼ <input checked="" type="radio"/> By AP Numbers <input type="radio"/> By Less Interference Current : 161
▶ Wi-Fi System	802.11 a/n/ac Mixed ▼
▶ Wi-Fi Operation Mode	AP Router Mode ▼
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	(0) Always ▼

Configuring Wi-Fi Settings		
Item	Value setting	Description
Wi-Fi Module	Enabled by default.	Check the Enable box to activate Wi-Fi function.
Channel	Mandatory field. Default setting: Auto.	<p>Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the Regulatory Domain.</p> <p>There are two available options when Auto is selected:</p> <ul style="list-style-type: none"> ● By AP Numbers The channel will be selected according to AP numbers (The less, the better). ● By Less Interference The channel will be selected according to interference. (The lower, the better).
Wi-Fi System	Mandatory field.	<p>Enter the preferred Wi-Fi System. The dropdown list of Wi-Fi system is based on IEEE 802.11 standard.</p> <ul style="list-style-type: none"> ● 2.4G Wi-Fi can select b, g and n only or mixed with each other. ● 5G Wi-Fi can select a, n and ac only or mixed with each other.
Wi-Fi Operation Mode	Select from the list.	<p>Enter the Wi-Fi Operation Mode according to your application.</p> <p>Navigate to the following table for AP Router Mode, WDS Only Mode, and WDS Hybrid Mode settings.</p>
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.
VAP Isolation	Enabled by default.	<p>Check the Enable box to activate this function.</p> <p>With the default setting, stations which have associates to different VAPs cannot communicate with each other.</p>
Time Schedule	Mandatory field.	<p>Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always.</p> <p>If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.</p>

5G VAP List

AddDelete

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	BEAM_5GHz_1534	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>Edit</div> <div><input type="checkbox"/> Select</div>

Save

Undo

Click **Add** / **Edit** button in the VAP List window to create or edit the settings for a VAP. A VAP Configuration window will appear.

For example, for VAP 2:

VAP Configuration ^ x

Item	Setting
▶ VAP	VAP2 ▼
▶ SSID	<input type="text" value="default"/>
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	<input type="text" value="Open"/> ▼ 802.1x <input type="checkbox"/> Enable
▶ Encryption	<input type="text" value="None"/> ▼
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input type="checkbox"/>
▶ Enable	<input type="checkbox"/>

VAP Configuration		
Item	Value setting	Description
SSID	String format: Any text.	Enter the SSID for the VAP. Decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	Disabled by default.	Check this box and enter a limitation to limit the maximum number of client station. Disabled by default. It means no special limitation on the number of connected STAs.
Authentication	Mandatory field. VAP1: default setting WPA2-PSK; Others: default setting Open.	For security, there are several authentication methods supported. Client stations should provide the key when associate with the MG400.
		When Open is selected. The check box named 802.1x shows up next to the dropdown list.
		<ul style="list-style-type: none">● 802.1x (Disabled by default) When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server. RADIUS Server IP (The default IP is 0.0.0.0) RADIUS Server Port (The default value is 1812) RADIUS Shared Key
		When Shared is selected. The pre-shared WEP key should be set for authenticating.
		When Auto is selected.

VAP Configuration		
Item	Value setting	Description
		<p>The MG400 will select Open or Shared by requesting of client automatically.</p> <p>The check box named 802.1x shows up next to the dropdown list.</p> <ul style="list-style-type: none"> ● 802.1x (Disabled by default) <p>When 802.1x is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA or WPA2 is selected.</p> <p>They are implementation of IEEE 802.11i. WPA has implemented as part of IEEE 802.11i and has better compatibility.</p> <ul style="list-style-type: none"> ● RADIUS Server <p>The client stations will be authenticated by RADIUS server.</p> <p>RADIUS Server IP (The default IP is 0.0.0.0)</p> <p>RADIUS Server Port (The default value is 1812)</p> <p>RADIUS Shared Key</p>
		<p>When WPA / WPA2 is selected.</p> <p>It has the same setting as WPA or WPA2. The client stations can associate with the MG400 via WPA or WPA2.</p>
		<p>When WPA-PSK or WPA2-PSK is selected.</p> <p>It has the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.</p>
		<p>When WPA-PSK / WPA2-PSK is selected.</p> <p>It has the same setting as WPA-PSK or WPA2-PSK. The client stations can associate with the MG400 via WPA-PSK or WPA2-PSK.</p>
Encryption	<p>Mandatory field.</p> <p>VAP1: default setting AES;</p> <p>Others: default setting None.</p>	<p>Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you select.</p> <p>None</p> <p>It means that the MG400 is an open system without encrypting.</p> <p>WEP</p> <p>Up to 4 WEP keys can be set, and you need to select one as current key. The key type can set to HEX or ASCII.</p> <p>If HEX is selected, the key should consist of (0 to 9) and (A to F).</p> <p>If ASCII is selected, the key should consist of ASCII table.</p> <p>TKIP</p> <p>TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>AES</p> <p>The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.</p> <p>You are recommended to use AES encryption instead of any others for security.</p>

VAP Configuration		
Item	Value setting	Description
		TKIP / AES TKIP / AES mixed mode. It means that the client stations can associate with the MG400 via TKIP or AES . Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. With default setting, stations which have associates to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with the MG400 by scanning SSID.
Enable	VAP1: Enabled by default; Others: unchecked by default.	Check the Enable box to activate this VAP.
Save	Button.	Click the Save button to save the current configuration.
Undo	Button.	Click the Undo button to restore configuration to previous setting before saving.

For the **WDS Only mode**, the MG400 only bridges the connected wired clients to another WDS-enabled Wi-Fi device which the MG400 has associates with. It means no wireless clients can connect to the MG400 while WDS Only Mode is selected and enabled.

5G Wi-Fi Configuration

Item	Setting
Wi-Fi Module	<input checked="" type="checkbox"/> Enable
Channel	Auto By AP Numbers By Less Interference Current : 0
Wi-Fi System	802.11 a/n/ac Mixed
Wi-Fi Operation Mode	WDS Only Mode
Green AP	<input type="checkbox"/> Enable
Time Schedule	(0) Always
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

WDS Only Mode		
Item	Value setting	Description
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.
Time Schedule	Mandatory field.	Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.
Scan Remote AP's MAC List	System data.	Press the Scan button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1-4	Mandatory field.	Enter the remote AP's MAC manually, or via auto-scan approach, the MG400 will bridge the traffic to the remote AP when associates successfully.

5G VAP List								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	BEAM_5GHz_6221	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Select

Under **WDS Only** mode, only VAP1 is available for further entering the required authentication and Encryption settings. Click **Edit** button in the VAP List window and a VAP Configuration window will appear for you to configure the required settings.

VAP Configuration
^ x

Item	Setting
▶ VAP	VAP1 ▼
▶ SSID	BEAM_5GHz_6221
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK ▼
▶ Encryption	AES ▼
▶ Preshared Key	l4EGMKj0j0FJL
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

For the detail description about VAP configuration, please refer to the description stated in AP-Router section.

For the **WDS Hybrid** mode, the MG400 bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled Wi-Fi devices which the MG400 associates with.

▶ Wi-Fi Operation Mode	WDS Hybrid Mode ▼
▶ Lazy Mode	<input checked="" type="checkbox"/> Enable
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	{0} Always ▼

WDS Hybrid Mode

Item	Value setting	Description
Lazy Mode	Enabled by default.	Check the Enable box to activate this function. With the function been enabled, the MG400 can auto-learn WDS peers without manually entering another AP's MAC address. But at least one of the APs needs to be filled with remote AP MAC addresses.
Green AP	Disabled by default.	Check the Enable box to activate Green AP function.

VAP Isolation	Enabled by default.	Check the Enable box to activate this function. With the default setting, stations which have associates to different VAPs cannot communicate with each other.
Time Schedule	Mandatory field.	Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.
Scan Remote AP's MAC List	Available when Lazy Mode disabled.	Press the Scan button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1-4	Available when Lazy Mode disabled.	Enter the remote AP's MAC manually, or via auto-scan approach, the MG400 will bridge the traffic to the remote AP when associates successfully.

5G VAP List Add Delete ^								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	BEAM_5GHz_6221	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit <input type="checkbox"/> Select
Save Undo								

Under **WDS Hybrid** mode, the VAP function is available and you can further enter the required VAP settings for connecting with wireless client devices.

Click **Add** / **Edit** button in the VAP List window to create or edit the settings for a VAP. A VAP Configuration window will appear.

For VAP 1:

VAP Configuration
^ x

Item	Setting
▶ VAP	VAP1 ▼
▶ SSID	BEAM_5GHz_6221
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK ▼
▶ Encryption	AES ▼
▶ Preshared Key	l4EGMKj0j0FJL
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

3.3.3 Wireless Client List

Navigate to the **Network > Wi-Fi > Wireless Client List** tab.

The **Wireless Client List** page shows the information of wireless clients which are associates with the MG400.

Select Module One or Two from the following Target Wi-Fi window.

Target Wi-Fi
^

Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼
▶ Multiple AP Names	All ▼

Target Configuration		
Item	Value setting	Description
Module Select	Mandatory field.	Select the Wi-Fi module to check the information of connected clients. For those single Wi-Fi module products, this option is hidden.
Operation Band	Mandatory field.	Enter the intended operation band for the Wi-Fi module.

		<p>This setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for you to choose according to his network environment.</p> <p>Under such situation, you can enter which operation band is suitable for the application.</p>
Multiple AP Names	Mandatory field. Default setting is All.	Enter the VAP to show the associates client's information in the following Client List. By default, All VAP is selected.

The Client list shows the client information of the Wi-Fi module selected.

Client List									
IP Address Configuration & Address	Host Name	MAC Address	Mode	Rate	RSSI0	RSSI1	Signal	Interface	
<div>Refresh</div>									

Target Configuration		
Item	Value setting	Description
IP Address Configuration & Address	System data.	It shows the Client's IP address and the deriving method. Dynamic means the IP address is derived from a DHCP server. Static means the IP address is a fixed one that is self-filled by client.
Host Name	System data.	It shows the host name of client.
MAC Address	System data.	It shows the MAC address of client.
Mode	System data.	It shows what kind of Wi-Fi system the client used to associate with the MG400.
Rate	System data.	It shows the data rate between client and the MG400.
RSSI0, RSSI1	System data.	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	System data.	The signal strength between client and the MG400.
Interface	System data.	It shows the VAP ID that the client associates with.
Refresh	System data.	Click the Refresh button to update the Client List immediately.

3.3.4 Advanced Configuration

Navigate to the **Network > Wi-Fi > Advanced Configuration** tab.

The **Target Wi-Fi** window provides the selection of Module One and Two.

Target Wi-Fi	
Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼

Target Configuration		
Item	Value setting	Description
Module Select	Mandatory field.	Select the Wi-Fi module to check the information of connected clients.
Operation Band	Mandatory field.	Enter the intended operation band for the Wi-Fi module. This setting is fixed and cannot be changed once the module is integrated into the product.

Advanced Configuration
^

Item	Setting
▶ Regulatory Domain	(1-13)
▶ Beacon Interval	<input type="text" value="100"/> Range: (1~1000 msec)
▶ DTIM Interval	<input type="text" value="3"/> Range: (1~255)
▶ RTS Threshold	<input type="text" value="2347"/> Range: (1~2347)
▶ Fragmentation	<input type="text" value="2346"/> Range: (256~2346)
▶ WMM	<input checked="" type="checkbox"/> Enable
▶ Short GI	<input type="text" value="400ns"/>
▶ TX Rate	<input type="text" value="Best"/>
▶ RF Bandwidth	<input type="text" value="Auto"/>
▶ Transmit Power	<input type="text" value="100%"/>
▶ WIDS	<input type="checkbox"/> Enable

Advanced Configuration		
Item	Value setting	Description
Regulatory Domain	This value is determined by the region of sale.	It limits the available radio channel of the MG400. The permissible channels depend on the Regulatory Domain .
Beacon Interval	Default setting: 100.	It shows the time interval between each beacon packet broadcasted. The beacon packet contains SSID, Channel ID and Security setting.

Advanced Configuration		
Item	Value setting	Description
DTIM Interval	Default setting: 3.	A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast message. When the MG400 has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	Default setting: 2347.	RTS (Request to send) Threshold means when the packet size is over the setting value, then active RTS technique. RTS/CTS is a collision avoidance technique. It means RTS never activated when the threshold is set to 2347.
Fragmentation	Default setting: 2346.	Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference at the limits of RF coverage.
WMM	Enabled by default.	WMM (Wi-Fi Multimedia) can help control latency and jitter when transmitting multimedia content over a wireless connection.
Short GI	Default setting: 400ns.	Short GI (Guard Interval) is defined to set the sending interval between each packet. Note that lower Short GI could increase not only the transition rate but also error rate.
TX Rate	Default setting: Best.	It means the data transition rate . When Best is selected, the MG400 will choose a proper data rate according to signal strength .
RF Bandwidth	Default setting: Auto.	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	Default setting: 100%.	Normally the wireless transmitter operates at 100% power. Alter the transmit power to control the Wi-Fi coverage .
5G Band Steering	Disabled by default.	When the client station is associated with the 2.4G Wi-Fi, the MG400 will send the client to 5G Wi-Fi automatically if the client is available to access the 5G Wi-Fi band.
WIDS	Disabled by default.	The WIDS (Wireless Intrusion Detection System) will analyze all packets and make a statistic table in Wi-Fi status. Navigate to Status > Network > Wi-Fi tab for detailed WIDS status.
Save	Button.	Click the Save button to save the current configuration.
Undo	Button.	Click the Undo button to restore configuration to previous setting before saving.

3.3.5 Wi-Fi as WAN

Navigate to the **Network > Wi-Fi > Uplink Profile** tab for configuring the Uplink Profile page.

The Setting window provides the settings on the Wi-Fi as WAN.

Setting ^

Item	Setting
▶ Profile	<input type="checkbox"/> Enable
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼
▶ Priority	<input checked="" type="radio"/> By Signal Strength <input type="radio"/> By User-defined
▶ Current Profile	

Setting Item	Value setting	Description
Profile	Mandatory field. Unchecked by default.	Check the Enable box to activate the profile function. It is available only when the selected Wi-Fi module is configured at Wi-Fi Uplink mode.
Module Select	Mandatory field.	Select the Wi-Fi module to check or configure the expected uplink profile(s). For those single Wi-Fi module products, this option is hidden.
Operation Band	Mandatory field.	Enter the intended operation band for the Wi-Fi module. This setting is fixed and cannot be changed once the module is integrated into the MG400 product. However, there are some module with selectable band for you to choose according to his network environment. Under such situation, you can enter which operation band is suitable for the application.
Priority	Mandatory field. By Signal Strength is selected by default.	Enter the network selection methodology for connecting to an available wireless uplink network. It can be By Signal Strength or By User-defined priority. When By Signal Strength is selected, the MG400 will try to connect to the available uplink network whose wireless signal strength is the strongest. When By User-defined is selected, the MG400 will try to connect to the available uplink network whose priority is the highest (1 is the highest priority, and 16 is the lowest priority).
Current Profile	System data.	After enabling Profile and connecting by a certain uplink profile, the profile name will be displayed.

Note: to apply the defined Uplink profile(s) for the MG400 to find a best fit profile for connecting to a certain uplink network, you need to **Enable** the Profile auto-connect function (Refer to **Network > Wi-Fi > (Module One/ Module Two) Wi-Fi Configuration** tab).

☐ Profile List

ID	Profile Name	SSID	Channel	Authentication	Encryption	MAC Address	Signal Strength	Priority	Enable	Actions
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>										

The Profile List shows the settings for the created uplink profiles. The information includes Profile Name, SSID, Channel, Authentication, Encryption, MAC Address, Signal Strength, Priority, and Enable.

When Add button is applied, Profile Configuration window will appear.

Profile Configuration

Item	Setting
Profile Name	<input type="text"/>
Network ID (SSID)	<input type="text"/> <input type="button" value="Scan"/>
Channel	Auto ▾
Authentication	Open ▾
Encryption	None ▾
MAC Address	<input type="text"/>
Priority	16 ▾
Enable	<input checked="" type="checkbox"/>

×

↑

Profile Configuration		
Item	Value setting	Description
Profile Name	Enter text string. Mandatory field.	Enter a profile name for the uplink network specified below. It is a name that is easy for you to understand. Value Range: 1 - 64 characters.
Network ID (SSID)	String format: Any text. Enabled by default.	Enter the SSID for the VAP and decide whether to broadcast the SSID or not. The SSID is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations

		can associate with the MG400 by scanning SSID.
Channel	Mandatory field. Default setting: Auto.	<p>Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the Regulatory Domain.</p> <p>There are two available options when Auto is selected:</p> <ul style="list-style-type: none"> ● By AP Numbers The channel will be selected according to AP numbers (The less, the better). ● By Less Interference The channel will be selected according to interference. (The lower, the better).
Authentication	Mandatory field. Default setting: Open.	<p>Enter the authentication method for connecting with the uplink network. It can be Open, Shared, WPA-SPK, or WPA2-PSK.</p> <p>When Open is selected, the preshared WEP key could be set for authentication;</p> <p>When Shared is selected, the preshared WEP key should be set for authentication;</p> <p>When WPA-PSK or WPA2-PSK is selected, the TKIP or AES preshared key should be set for authentication;</p>
Encryption	Mandatory field. Default setting: None.	<p>Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you select.</p> <p>None It means that the MG400 is open system without encrypting.</p> <p>WEP Up to 4 WEP keys can be set, and you need to select one as current key. The key type can set to HEX or ASCII. If HEX is selected, the key should consist of (0 to 9) and (A to F). If ASCII is selected, the key should consist of ASCII table.</p> <p>TKIP TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters.</p> <p>AES The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. You are recommended to use AES encryption instead of any others for security.</p>
MAC Address	MAC Address string Format Mandatory field.	Enter the MAC Address of the access point (with the Network ID) to be connected to.
Priority	Optional Setting. Default setting: 16.	Enter a priority setting for the uplink profile when the By User-defined methodology is selected. The priority value can be 1 - 16. 1 is the highest priority, and 16 is the lowest priority).
Enable	Enabled by default.	Click the Enable box to activate this profile.
Save	Button.	Click the Save button to save the configuration.

Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.
------	---------	--

You can click the **Scan** button to get the available wireless networks around the MG400, then select one as the uplink network.

When the **Scan** button is applied, **Wireless AP List** will appear after few seconds.

When you select an AP from the AP list, the channel, SSID, Authentication, Encryption, and MAC address will be automatically filled into the profile, you need to enter a key for the uplink connection, if required.

3.4 IPv6

The IPv6 page allows you to set the IPv6 connection type to access the IPv6 network. The MG400 supports various types of IPv6 connection on WAN-1, including Static IPv6, DHCPv6, and PPPoEv6.

Static IPv6

Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default device address, and IPv6 DNS.

DHCPv6

DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client has then to resend a request to renew the IPv6 address.

PPPoEv6

PPPoEv6 in IPv6 does the same function as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters based on PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other required parameters to automatically configure the client.

Navigate to the Network > IPv6 > Configuration Tab.

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

IPv6 Configuration	
Item	Setting
▶ IPv6	<input type="checkbox"/> Enable
▶ WAN Connection Type	IPv6 ▼

IPv6 Configuration		
Item	Value setting	Description
IPv6	Disabled by default.	Check the Enable box to activate the IPv6 function.
WAN Connection Type	Mandatory field. Default setting: DHCPv6.	<p>Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity via WAN-1 Interface.</p> <p>Select Static IPv6 when your ISP provides you with a set IPv6 addresses.</p> <p>Select DHCPv6 when your ISP provides you with DHCPv6 services.</p> <p>Select PPPoEv6 when your ISP provides you with PPPoEv6 account settings.</p> <p>Note: The available WAN connection types can be different, depending on the Interface type of WAN-1.</p>

For the **Static IPv6 WAN Type Configuration**, configuration can be set up via following window.

Static IPv6 WAN Type Configuration
^

Item	Setting
▶ IPv6 Address	<input type="text"/>
▶ Subnet Prefix Length	<input type="text"/>
▶ Default Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

Static IPv6 WAN Type Configuration		
Item	Value setting	Description
IPv6 Address	Mandatory field.	Enter the WAN IPv6 Address for the router.
Subnet Prefix Length	Mandatory field.	Enter the WAN Subnet Prefix Length for the router.
Default Device	Mandatory field.	Enter the WAN Default Device IPv6 address.
Primary DNS	Optional field.	Enter the WAN primary DNS Server.
Secondary DNS	Optional field.	Enter the WAN secondary DNS Server.
MLD Snooping	Disabled by default.	Enable/Disable the MLD Snooping function.

LAN Configuration window provides the Global Address setting.

LAN Configuration
^

Item	Setting
▶ Global Address	<input type="text"/> /64
▶ Link-local Address	fe80::250:18ff:fe21:f270

Then Navigate to **Address Auto-configuration** for setting LAN environment.

Address Auto-configuration ^

Item	Setting
▶ Auto-configuration	<input checked="" type="checkbox"/> Enable
▶ Auto-configuration Type	Stateless ▾
▶ Router Advertisement Lifetime	<input type="text" value="200"/> (seconds)

If above setting is configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

For the **HCPv6 WAN Type Configuration**, configuration can be set up via following window.

DHCPv6 WAN Type Configuration ^

Item	Setting
▶ DNS	<input checked="" type="radio"/> From Server <input type="radio"/> Specific DNS
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

DHCPv6 WAN Type Configuration		
Item	Value setting	Description
DNS	Default setting: From Server.	Select the [Specific DNS] option to active Primary DNS and Secondary DNS. Then fill the DNS information.
Primary DNS	Can not modified by default.	Enter the WAN primary DNS Server.
Secondary DNS	Can not modified by default.	Enter the WAN secondary DNS Server.
MLD	Disabled by default.	Enable/Disable the MLD Snooping function.

LAN Configuration window provides the Global Address setting.

LAN Configuration		^
Item	Setting	
▶ Global Address		
▶ Link-local Address	fe80::250:18ff:fe21:f270	

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

Then Navigate to **Address Auto-configuration** for setting LAN environment.

Address Auto-configuration		^
Item	Setting	
▶ Auto-configuration	<input checked="" type="checkbox"/> Enable	
▶ Auto-configuration Type	Stateless ▾	
▶ Router Advertisement Lifetime	200 (seconds)	
		Save Undo

If above setting is configured, click the **Save** button to save the configuration, and click **Reboot** button to reboot the router.

For the **PPPoEv6 WAN Type Configuration**, configuration can be set up via following window.

PPPoEv6 WAN Type Configuration	
Item	Setting
▶ Account	<input type="text"/>
▶ Password	<input type="password"/>
▶ Service Name	<input type="text"/>
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

PPPoEv6 WAN Type Configuration		
Item	Value setting	Description
Account	Mandatory field.	Enter the Account for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 - 45 characters.
Password	Mandatory field.	Enter the Password for setting up PPPoEv6 connection. If you want more information, please contact your ISP.
Service Name	Mandatory field.	Enter the Service Name for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 - 45 characters.
Connection Control	Fixed value.	The value is Auto-reconnect (Always on).
MTU	Mandatory field.	Enter the MTU for setting up PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 1280 - 1492.
MLD Snooping	Disabled by default.	Enable/Disable the MLD Snooping function.

LAN Configuration window provides the Global Address setting.

LAN Configuration	
Item	Setting
Global Address	
Link-local Address	fe80::250:18ff:fe21:f270

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

Then Navigate to **Address Auto-configuration** for setting LAN environment.

If above setting is configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

Address Auto-configuration	
Item	Setting
Auto-configuration	<input checked="" type="checkbox"/> Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	<input type="text" value="200"/> (seconds)

Address Auto-configuration		
Item	Item	Item
Auto-configuration	Disabled by default.	Check to enable the Auto configuration feature.
Auto-configuration Type	Can only be selected when Auto-configuration is enabled. Default setting: Stateless.	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select Stateless to manage the Local Area Network to be SLAAC + RDNSS Router Advertisement Lifetime (Mandatory field.): Enter the Router Advertisement Lifetime (in seconds). 200 is set by default. Value Range: 0 - 65535. Select Stateful to manage the Local Area Network to be Stateful (DHCPv6).

		IPv6 Address Range (Start) (Mandatory field.): Enter the start IPv6 Address for the DHCPv6 range for your local computers. 0100 is set by default. Value Range: 0001 - FFFF.
		IPv6 Address Range (End) (Mandatory field.): Enter the end IPv6 Address for the DHCPv6 range for your local computers. 0200 is set by default. Value Range: 0001 - FFFF.
		IPv6 Address Lifetime (Mandatory field.): Enter the DHCPv6 lifetime for your local computers. 36000 is set by default. Value Range: 0 - 65535.
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to cancel the settings.

If above setting is configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

3.5 Port Forwarding

3.5.1 Configuration

Navigate to the Network > Port Forwarding > Configuration tab.

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

NAT Loopback ^

Item	Setting
▶ NAT Loopback	<input checked="" type="checkbox"/> Enable

Configuration		
Item	Item	Item
NAT Loopback	Enabled by default.	Check the Enable box to activate this NAT function.
Save	Button.	Click the Save button to save the settings.
Undo	Button.	Click the Undo button to cancel the settings

3.5.2 Virtual Server & Virtual PC

Navigate to the Network > Port Forwarding > Virtual Server & Virtual PC tab.

Enable **Virtual Server / Virtual Computer** in the following window.

Configuration ^

Item	Setting
▶ Virtual Server	<input checked="" type="checkbox"/> Enable
▶ Virtual Computer	<input checked="" type="checkbox"/> Enable

Configuration		
Item	Item	Item
Virtual Server	Disabled by default.	Check the Enable box to activate this port forwarding function.
Virtual Computer	Enabled by default.	Check the Enable box to activate this port forwarding function.

Click **Add** button to add a new **Virtual Server**.

Virtual Server List Add Delete									
ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Type in the server information.

Virtual Server Rule Configuration

Item	Setting
▶ WAN Interface	<input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4
▶ Server IP	<input type="text"/>
▶ Source IP	<input type="text" value="Any"/>
▶ Protocol	<input type="text" value="TCP(6) & UDP(17)"/>
▶ Public Port	<input type="text" value="Single Port"/> <input type="text"/>
▶ Private Port	<input type="text" value="Single Port"/> <input type="text"/>
▶ Time Schedule	<input type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

Save

×

↑

↑

Virtual Server Rule Configuration		
Item	Value setting	Description
WAN Interface	Mandatory field. Default setting is ALL.	<p>Define the selected interface to be the packet-specifying interface of the MG400.</p> <p>If the packets to be filtered are coming from WAN-x, then select WAN-x for this field.</p> <p>Select ALL for packets coming into the MG400 from any interface.</p> <p>It can be selected WAN-x box when WAN-x enabled.</p> <p>Note: The available check boxes (WAN-1 - WAN-4) depend on the number of WAN interfaces for the product.</p>
Server IP	Mandatory field.	This field is to enter the IP address of the interface selected in the WAN Interface setting above.
Source IP	Mandatory field. Default setting is Any.	<p>This field is to enter the Source IP address.</p> <p>Select Any to allow the access coming from any IP addresses.</p> <p>Select Specific IP Address to allow the access coming from an IP address.</p> <p>Select IP Range to allow the access coming from a specified range of IP address.</p>
Protocol	Mandatory field. Default setting is TCP & UDP.	<p>When "ICMPv4" is selected.</p> <p>It means the option "Protocol" of packet filter rule is ICMPv4.</p> <p>Apply Time Schedule to this rule, otherwise leave it as Always. (refer to Scheduling setting under User Rule)</p> <p>Then check Enable box to enable this rule.</p>
		<p>When "TCP" is selected.</p> <p>It means the option "Protocol" of packet filter rule is TCP.</p> <p>Public Port selected a predefined port from Well-known Service, and Private Port is the same with Public Port number.</p> <p>Public Port is selected Single Port and enter a port number, and Private Port can be set a Single Port number.</p> <p>Public Port is selected Port Range and enter a port range, and Private Port can be selected Single Port or Port Range.</p> <p>Value Range: 1 - 65535 for Public Port, Private Port.</p>
		<p>When "UDP" is selected.</p> <p>It means the option "Protocol" of packet filter rule is UDP.</p> <p>Public Port selected a predefined port from Well-known Service, and Private Port is the same with Public Port number.</p> <p>Public Port is selected Single Port and enter a port number, and Private Port can be set a Single Port number.</p> <p>Public Port is selected Port Range and enter a port range, and Private Port can be selected Single Port or Port Range.</p> <p>Value Range: 1 - 65535 for Public Port, Private Port.</p>
		<p>When "TCP & UDP" is selected.</p> <p>It means the option "Protocol" of packet filter rule is TCP and UDP.</p>

	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 enter a port number, and Private Port can be set a Single Port number. Public Port is selected Port Range and enter a port range, and Private Port can be selected Single Port or Port Range. Value Range: 1 - 65535 for Public Port, Private Port.
	When "GRE" is selected. It means the option "Protocol" of packet filter rule is GRE.

The MG400 allows you to customize your Virtual Computer rules. It supports up to a maximum of 20 rule-based **Virtual Computer** sets.

Virtual Computer List

AddDelete

ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

Save

Undo

When Add button is applied, Virtual Computer Rule Configuration window will appear.

AN Interface

Server IP

Source IP

Protocol

Public Port

Private Port

Time Schedule

Enable

Actions

Virtual Computer Rule Configuration

Global IP	Local IP	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save

Undo

Virtual Computer Rule Configuration		
Item	Value setting	Description
Global IP	Mandatory field.	This field is to enter the IP address of the WAN IP.
Local IP	Mandatory field.	This field is to enter the IP address of the LAN IP.
Enable	System data.	Then check Enable box to enable this rule.
Save	System data.	Click the Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

3.5.3 Special AP & ALG

Special AP

The Special AP feature allows you to request the MG400 open a pre-defined service ports for incoming packets to pass

SIP ALG

Navigate to the Network > Port Forwarding > Special AP & ALG tab.

Configuration	
Item	Setting
▶ Special AP	<input checked="" type="checkbox"/> Enable
▶ ALG Enable	<input checked="" type="checkbox"/> SIP ALG

Special AP List

Add

Delete

ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
<div>SaveUndo</div>						

137 of 335
©2019 BEAM

Special AP Rule Configuration
^ x

Item	Setting
▶ WAN Interface	<input checked="" type="checkbox"/> ALL <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4
▶ Trigger Port	Port : <input style="width: 150px;" type="text"/> Popular Applications : User-defined ▼
▶ Incoming Ports	<input style="width: 200px;" type="text"/>
▶ Time Schedule	(0) Always ▼
▶ Rule	<input type="checkbox"/>

Save

Save
Undo

IP Translation Configuration		
Item	Value setting	Description
WAN Interface	Mandatory field. Default setting: All.	Check the interface box(es) to apply the Special AP rule. By default, All is checked, and the Special AP rule will be applied to all WAN interfaces.
Trigger Port	Mandatory field. Default setting: User-defined.	Enter the expected trigger port (or port range) if User-defined is selected in the dropdown list. If you select a popular application from the dropdown list, the corresponding trigger port(s) and incoming ports will be selected automatically. Value Range: 1 - 65535.
Incoming Ports	Mandatory field.	Enter the expected Incoming ports if User-defined is selected in the Trigger Port dropdown list. If you select a popular application from the dropdown list, the corresponding incoming ports will be selected automatically. Value Range: 1 - 65535; It can be a single port, multiple ports separated by ",", or port range.
Time Schedule	Mandatory field Default setting: (0) Always.	Apply Time Schedule to this rule, otherwise leave it as Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.
Rule	Disabled by default.	Check the Enable box to activate the special AP rule.
Save	Button.	Click the Save button to save the settings.

3.5.4 DMZ & Pass Through

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

The DMZ function allows you to ask the MG400 pass through all normal packets to the DMZ host behind the NAT device only when these packets are not expected to receive by applications in the MG400 or by other client hosts in the Intranet. Certainly, the DMZ host is also protected by the MG400 firewall. Activate the feature and enter the DMZ host with a host in the Intranet when needed.

Navigate to the Network > Port Forwarding > DMZ & Pass Through tab.

The **Configuration** window allows you to enable **DMZ and Pass Through**.

Configuration

Item	Setting
DMZ	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4 DMZ Host : <input type="text"/>
Pass Through Enable	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP

Save

Undo

Configuration		
Item	Value setting	Description
DMZ	Mandatory field. Default setting is ALL.	<p>Check the Enable box to activate the DMZ function</p> <p>Define the selected interface to be the packet-specifying interface of the MG400, and fill in the IP address of Host LAN IP in DMZ Host field</p> <p>.</p> <p>If the packets to be filtered are coming from WAN-x, then select WAN-x for this field.</p> <p>Select ALL for packets coming into the router from any interfaces.</p> <p>It can be selected WAN-x box when WAN-x enabled.</p> <p>Note: The available check boxes (WAN-1 - WAN-4) depend on the number of WAN interfaces for the product.</p>
Pass Through Enable	Enabled by default.	<p>Check the box to enable the pass-through function for the IPSec, PPTP, and L2TP.</p> <p>With the pass-through function enabled, the VPN hosts behind the MG400 still can connect to remote VPN servers.</p>
Save	Button.	Click the Save button to save the settings.
Undo	Button.	Click the Undo button to cancel the settings

3.6 Routing

3.6.1 Static Routing

Navigate to the **Network > Routing > Static Routing** tab.

From the Configuration window IPv4 and IPv6 Static Routing can be enabled.

Configuration		
Item	Setting	
▶ IPv4 Static Routing	<input checked="" type="checkbox"/> Enable	
▶ IPv6 Static Routing	<input checked="" type="checkbox"/> Enable	

Static Routing		
Item	Value setting	Description
Static Routing	Disabled by default	Check the Enable box to activate this function.

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

IPv4 Static Routing Rule List Add Delete							
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

The MG400 allows you to customize your static routing rules. It supports up to a maximum of 64 rule sets. When **Add** button is applied, **Static Routing Rule Configuration** window will appear, while the Edit button at the end of each static routing rule can allow you modify the rule.

IPv4 Static Routing Rule Configuration

Item	Setting
Destination IP	<input type="text"/>
Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>
Gateway IP	<input type="text"/>
Interface	<input type="text" value="Auto"/>
Metric	<input type="text"/>
Rule	<input type="checkbox"/> Enable

Save

IPv4 Static Routing		
Item	Value setting	Description
Destination IP	IPv4 Format Mandatory field.	Enter the Destination IP of this static routing rule.
Subnet Mask	Default setting 255.255.255.0 (/24).	Enter the Subnet Mask of this static routing rule.
Device IP	IPv4 Format Mandatory field.	Enter the MG400 IP of this static routing rule.
Interface	Default setting: Auto.	Select the Interface of this static routing rule. It can be Auto, or the available WAN / LAN interfaces.
Metric	Numeric String Format. Mandatory field.	The Metric of this static routing rule. Value Range: 0 - 255.
Rule	Disabled by default.	Click Enable box to activate this rule.
Save	NA	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

☐ IPv6 Static Routing Rule List

AddDelete

ID	Destination IP	Prefix Length	Gateway IP	Interface	Metric	Enable	Actions
<div>SaveUndo</div>							

IPv6 Static Routing Rule Configuration

Item	Setting
Destination IP	<input type="text"/>
Prefix Length	<input type="text"/>
Gateway IP	<input type="text"/>
Interface	WAN-1 ▼
Metric	<input type="text"/>
Rule	<input type="checkbox"/> Enable

Save

IPv6 Static Routing		
Item	Value setting	Description
Destination IP	IPv6 Format. Mandatory field.	Enter the Destination IP of this static routing rule.
Prefix Length	Mandatory field.	Enter the WAN Subnet Prefix Length for the router.
Device IP	IPv6 Format. Mandatory field.	Enter the MG400 IP of this static routing rule.
Interface	Default setting: Auto.	Select the Interface of this static routing rule. It can be Auto, or the available WAN / LAN interfaces.
Metric	Numeric String Format Mandatory field.	The Metric of this static routing rule. Value Range: 0 - 255.
Rule	Disabled by default.	Click Enable box to activate this rule.
Save	Button.	Click the Save button to save the configuration
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

3.6.2 Dynamic Routing

RIP Scenario

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

OSPF Scenario

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

BGP Scenario

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

Navigate to the Network > Routing > Dynamic Routing tab.

The RIP configuration window allows you to enable RIP protocol.

RIP Configuration ^

Item	Setting
▶ RIP Enable	Disable ▼

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

The RIPng configuration window allows you to enable RIPng.

RIPng Configuration ^

Item	Setting
▶ RIPng	<input type="checkbox"/> Enable

RIPng Configuration		
Item	Value setting	Description
RIPng Enable	Disabled by default.	Check Enable to activate RIPng protocol.

OSPF Configuration

The OSPF configuration setting allows you to enable OSPF protocol.

OSPF Configuration

Item	Setting
▶ OSPF	<input checked="" type="checkbox"/> Enable
▶ Router ID	<input type="text"/>
▶ Authentication	None ▼
▶ Backbone Subnet	<input type="text"/>

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

Create / Edit OSPF Area Rules

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

OSPF Area List

Add

Delete

ID	Area Subnet	Area ID	Enable	Actions
----	-------------	---------	--------	---------

When Add button is applied, OSPF Area Rule Configuration window will appear.

OSPF Area Configuration

Item

Setting

▶ Area Subnet

▶ Area ID

▶ Area

☐ Enable

Save

OSPF Area Configuration		
Item	Value setting	Description
Area Subnet	Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) Mandatory field.	The Area Subnet of this router on OSPF Area List.
Area ID	IPv4 Format Mandatory field.	The Area ID of this router on OSPF Area List.
Area	Disabled by default.	Click Enable box to activate this rule.
Save	System data.	Click the Save button to save the configuration

The **OSPF6 Configuration** allows you to enable OSPF6 protocol.

OSPF6 Configuration

Item

Setting

▶ OSPF6

☐ Enable

RIPng Configuration		
Item	Value setting	Description
OSPF6 Enable	Disabled by default.	Check Enable to activate OSPF6 protocol.

The BGP configuration setting allows you to enable BGP protocol.

BGP Network Configuration		
Item	Value setting	Description
BGP	Disabled by default.	Check the Enable box to activate the BGP protocol.
ASN	Numeric String Format Mandatory field.	The ASN Number of this router on BGP protocol. Value Range: 1 - 4294967295.
Router ID	IPv4 Format. Mandatory field.	The Router ID of this router on BGP protocol.

<div> <div>BGP Network List</div> <div>Add</div> <div>Delete</div> </div>			
ID	Network Subnet	Enable	Actions

BGP Network Configuration

Item

Setting

▶ Network Subnet

IP :


▶ Network

☐ Enable

Save

Item	Value setting	Description
Network Subnet	IPv4 Format Mandatory field.	The Network Subnet of this router on BGP Network List. It composes of entered the IP address in this field and the selected subnet mask.
Network	Disabled by default.	Click Enable box to activate this rule.
Save	System data.	Click the Save button to save the configuration

146 of 335
©2019 BEAM

 **BGP Neighbor List**
Add
Delete
^

ID	Neighbor IP	Remote ASN	Enable	Actions
<div> Save Undo </div>				

When Add button is applied, BGP Neighbour Configuration window will appear.

BGP Neighbor Configuration
×

Item	Setting
▶ Neighbor IP	<input type="text"/>
▶ Remote ASN	<input type="text"/>
▶ Neighbor	<input type="checkbox"/> Enable
<div> Save </div>	
<div> Save Undo </div>	

BGP Neighbour Configuration		
Item	Value setting	Description
Neighbor IP	IPv4 Format. Mandatory field.	The Neighbor IP of this router on BGP Neighbor List.
Remote ASN	Numeric String Format. Mandatory field.	The Remote ASN of this router on BGP Neighbor List. Value Range: 1 - 4294967295.
Neighbor	Disabled by default.	Click Enable box to activate this rule.
Save	System data.	Click the Save button to save the configuration

3.6.3 Routing Information

Navigate to Network > Routing > Routing Information Tab.

Routing Table ^				
Destination IP	Subnet Mask	Gateway IP	Metric	Interface
22.224.87.244	255.255.255.252	0.0.0.0	0	WAN-1
192.168.123.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo
0.0.0.0	0.0.0.0	22.224.87.246	0	WAN-1

Routing Table		
Item	Value setting	Description
Destination IP	System data.	Routing record of Destination IP. IPv4 Format.
Subnet Mask	System data.	Routing record of Subnet Mask. IPv4 Format.
Device IP	System data.	Routing record of Device IP. IPv4 Format.
Metric	System data.	Routing record of Metric. Numeric String Format.
Interface	System data.	Routing record of Interface Type. String Format.

IPv6 Routing Table ^			
Destination	Next Hop	Metric	Interface
::1/128	::	0	lo
fe80::/128	::	0	lo
fe80::/128	::	0	lo
fe80::/128	::	0	lo

IPv6 Routing Table		
Item	Value setting	Description
Destination IP	System data.	Routing record of Destination IP. IPv6 Format.
Next Hop	System data.	Routing record of Next Hop IP. IPv6 Format.
Metric	System data.	Routing record of Metric. Numeric String Format.
Interface	System data.	Routing record of Interface Type. String Format.

Policy Routing Information				
Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-
<div>Refresh</div>				

Policy Routing Information		
Item	Value setting	Description
Policy Routing Source	System data.	Policy Routing of Source. String Format.
Source IP	System data.	Policy Routing of Source IP. IPv4 or IPv6 Format.
Destination IP	System data.	Policy Routing of Destination IP. IPv4 or IPv6 Format.
Destination Port	System data.	Policy Routing of Destination Port. String Format.
WAN Interface	System data.	Policy Routing of WAN Interface. String Format.

3.7 DNS & DDNS

Navigate to the **Network > DNS & DDNS** Tab.

The Dynamic DNS setting allows you to setup Dynamic DNS feature.

Dynamic DNS	
Item	Setting
▶ DDNS	<input checked="" type="checkbox"/> Enable
▶ IPv6	<input type="checkbox"/> Enable
▶ WAN Interface	WAN-1 ▼
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ User Name / E-Mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

DDNS (Dynamic DNS) Configuration

Item	Value setting	Description
DDNS	Disabled by default.	Check the Enable box to activate this function.
WAN Interface	Default setting: WAN 1.	Select the WAN Interface IP Address of the MG400.
Provider	DynDNS.org (Dynamic) is set by default.	Select your DDNS provider of Dynamic DNS. It can be DynDNS.org (Dynamic), DynDNS.org, NO-IP.com, etc.
Host Name	Enter text string. Mandatory field.	Your registered host name of Dynamic DNS. Value Range: 0 - 63 characters.
User Name / E-Mail	Enter text string. Mandatory field.	Enter your username or E-mail address of Dynamic DNS.
Password / Key	Enter text string. Mandatory field.	Enter your Password or Key of Dynamic DNS.

DNS redirect can be enabled via following window.

DNS Redirect ^

Item	Setting
► DNS Redirect	<input checked="" type="checkbox"/> Enable

DNS Redirect Configuration		
Item	Value setting	Description
DNS Redirect	Disabled by default.	Check the Enable box to activate this function.

If you enable the DNS Redirect function, you need to enter the redirect rules. According to the rules, the MG400 can redirect the traffic that matched the DNS to corresponding pre-defined IP address.

☐ Redirect Rule ^

ID	Mapping Rule	Condition	Description	Enable	Action
----	--------------	-----------	-------------	--------	--------

When Add button is applied, Redirect Rule window will appear.

☐ Redirect Rule ^ x

Item	Setting						
Mapping Rule	<table><thead><tr><th>Domain Name</th><th>IP</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr><tr><td colspan="2">(* for Any)</td></tr></tbody></table>	Domain Name	IP	<input type="text"/>	<input type="text"/>	(* for Any)	
Domain Name	IP						
<input type="text"/>	<input type="text"/>						
(* for Any)							
Condition	<div>Always ▼</div>						
Description	<input type="text"/>						
Enable	<input type="checkbox"/> Enable						

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

3.8 QoS

When you want to add a new QoS rule or edit one already existed, the "QoS Rule Configuration" window shows up for you to configure. The parameters in a rule include the applied WAN interfaces, the dedicated host group based on MAC address or IP address, the dedicated kind of service packets, the system resource to be distributed, the corresponding control function for your specified resource, the packet flow direction, the sharing method for the control function, the integrated time schedule rule and the rule activation.

Navigate to the **Network > QoS** Tab.

In Configuration window, two options in QoS Types: Software and Hardware. Following for the settings when Software is selected.

Configuration ^

Item	Setting
▶ QoS Types	<div style="display: inline-block; border: 1px solid #ccc; padding: 2px 5px;">Software ▼</div> <div style="display: inline-block; margin-left: 10px;"> <input checked="" type="checkbox"/> Enable </div>
▶ Flexible Bandwidth Management	<div style="display: inline-block;"> <input type="checkbox"/> Enable </div>

Configuration		
Item	Value Setting	Description
QoS Type	Select types. Disabled by default.	Select the QoS Type: Software, Hardware. The default QoS type is set to Software .
Flexible Bandwidth Management	Disabled by default.	Click Enable box to activate the Flexible Bandwidth Management function.
Save	System data.	Click the Save button to save the settings.

In System Resource Configuration window, two options for type of System Queue: Priority Queues and Bandwidth Queue.

System Resource Configuration ^

Item	Setting
▶ Type of System Queue	<div style="display: inline-block; border: 1px solid #ccc; padding: 2px 5px;">Priority Queues ▼</div> <div style="display: inline-block; margin-left: 10px;"> <input type="text" value="6"/> (1~6) </div>
▶ WAN Interface	<div style="display: inline-block; border: 1px solid #ccc; padding: 2px 5px;">WAN - 1 ▼</div>

System Resource Configuration		
Item	Value Setting	Description
Type of System Queue	Mandatory field. Bandwidth Queue, and 6 is the default value.	Define the system queues that are available for the QoS settings. The supported type of system queues are Bandwidth Queue and Priority Queues. Value Range: 1 - 6.
WAN Interface	Default setting: WAN-1.	Select the WAN interface and then the following WAN Interface Resource window will show the related resources for configuration. <ul style="list-style-type: none"> Bandwidth of Upstream / Downstream Enter total upload / download bandwidth of the selected WAN. Value Range: For Gigabit Ethernet: 1-1024000Kbps, or 1-1000Mbps; For Fast Ethernet: 1-102400Kbps, or 1-100Mbps; For 3G/4G: 1-153600Kbps, or 1-150Mbps. Total Connection Sessions Enter total connection sessions of the selected WAN. Value Range: 1 - 10000.

When Priority Queues is selected, bandwidth settings in WAN Interface Resource are grey out.

WAN Interface Resource

Item	Setting
▶ Bandwidth of Upstream	50 Mbps
▶ Bandwidth of Downstream	100 Mbps
▶ Total Connection Sessions	30000 (1~100000)

When Bandwidth Queue is selected, queue number can be set from 1 to 6.

System Resource Configuration

Item	Setting
▶ Type of System Queue	Bandwidth Queue 6 (1~6)
▶ WAN Interface	WAN - 1

Upstream and Downstream bandwidth can be configured.

WAN Interface Resource

Item	Setting
▶ Bandwidth of Upstream	<input type="text" value="50"/> <input type="text" value="Mbps"/>
▶ Bandwidth of Downstream	<input type="text" value="100"/> <input type="text" value="Mbps"/>
▶ Total Connection Sessions	<input type="text" value="30000"/> (1~100000)

System Resource Configuration		
Item	Value Setting	Description
Type of System Queue	Mandatory field. Bandwidth Queue, and 6 is the default value.	Define the system queues that are available for the QoS settings. The supported type of system queues are Bandwidth Queue and Priority Queues. Value Range: 1 - 6.
WAN Interface	Default setting: WAN-1.	Select the WAN interface and then the following WAN Interface Resource window will show the related resources for configuration. <ul style="list-style-type: none"> Bandwidth of Upstream / Downstream Enter total upload / download bandwidth of the selected WAN. Value Range: For Gigabit Ethernet:1-1024000Kbps, or 1-1000Mbps; For Fast Ethernet: 1-102400Kbps, or 1-100Mbps; For 3G/4G: 1-153600Kbps, or 1-150Mbps. Total Connection Sessions Enter total connection sessions of the selected WAN. Value Range: 1 - 10000.

QoS Rule List

Interface Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>								

After enabled the QoS function and configured system resources, you need to further specify some QoS rules for provide better service on the interested traffics. The MG400 supports up to a maximum of 128 rule based QoS rule sets.

QoS Rule List

Interface Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>								

When Add button is applied, QoS Rule Configuration window will appear.

Flexible Bandwidth Management

☐ Enable

QoS Rule Configuration

Item	Setting
> Interface	All WANs ▾
> Group	Src. MAC Address ▾ <input type="text"/>
> Service	All ▾
> Resource	Bandwidth ▾
> Control Function	Set MINR & MAXR ▾ <input type="text"/> --- <input type="text"/> Mbps ▾
> QoS Direction	Outbound ▾
> Time Schedule	(0) Always ▾
> Rule Enable	<input type="checkbox"/> Enable

QoS Rule List

AddDeleteClearRestartSave

QoS Rule Configuration		
Item	Value setting	Description
Interface	Mandatory field. Default setting: All WANs.	Enter the WAN interface to apply the QoS rule. Select All WANs or a certain WAN-n to filter the packets entering to or leaving from the interface(s).
Group	Mandatory field. Default setting: Src. MAC Address.	<p>Enter the Group category for the QoS rule. It can be Src. MAC Address, IP, or Host Name.</p> <p>Select Src. MAC Address to prioritize packets based on MAC;</p> <p>Select IP to prioritize packets based on IP address and Subnet Mask;</p> <p>Select Host Name to prioritize packets based on a group of a pre-configured group of hosts from the dropdown list. If the dropdown list is empty, ensure if any group is pre-configured.</p> <p>Note: The required host groups need to be created in advance and corresponding QoS checkbox in the Multiple Bound Services field is checked before the Host Group option become available. Refer to User Rule > Grouping > Host Grouping.</p>
Service	Mandatory field.	Enter the service type of traffics that need to be applied with the QoS

	<p>Default setting: All.</p>	<p>rule. It can be All, DSCP, TOS, User-defined Service, or Well-known Service.</p> <p>Select All for all packets.</p> <p>Select DSCP for DSCP type packets only.</p> <p>Select TOS for TOS type packets only. You need to select a service type (Minimize-Cost, Maximize-Reliability, Maximize-Throughput, or Minimize-Delay) from the dropdown list as well.</p> <p>Select User-defined Service for user-defined packets only. You need to define the port range and protocol as well.</p> <p>Select Well-known Service for specific application packets only. You need to select the required service from the dropdown list as well.</p>
Resource, and Control Function	<p>Mandatory field.</p>	<p>Enter the Resource Type and corresponding Control function for the QoS rule. The available Resource options are Bandwidth, Connection Sessions, Priority Queues, and DiffServ Codepoints.</p> <p>Bandwidth: Select Bandwidth as the resource type for the QoS Rule, and you need to assign the min rate, max rate and rate unit as the bandwidth settings in the Control Function / Set MINR & MAXR field.</p> <p>Connection Sessions: Select Connection Sessions as the resource type for the QoS Rule, and you need to assign supported session number in the Control Function / Set Session Limitation field.</p> <p>Priority Queues: Select Priority Queues as the resource type for the QoS Rule, and you need to enter a priority queue in the Control Function / Set Priority field.</p> <p>DiffServ Code Points: Select DiffServ Code Points as the resource type for the QoS Rule, and you need to select a DSCP marking from the Control Function / DSCP Marking dropdown list.</p>
QoS Direction	<p>Mandatory field. Default setting: Outbound.</p>	<p>Enter the traffic flow direction for the packets to apply the QoS rule. It can be Outbound, Inbound, or Both.</p> <p>Outbound: Select Outbound to prioritize the traffics going to the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a source group.</p> <p>Inbound: Select Inbound to prioritize the traffics coming from the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a destination group.</p> <p>Both: Select both to prioritize the traffics passing through the specified</p>

		interface, both Inbound and Outbound are considered. Under such situation, the hosts specified in the Group field can be a source or destination group.
Sharing Method	Mandatory field. Default setting: Group Control.	Enter the preferred sharing method for how to apply the QoS rule on the selected group. It can be Individual Control or Group Control. Individual Control: If Individual Control is selected, each host in the group will have its QoS service resource as specified in the rule. Group Control: If Group Control is selected, all the group hosts share the same QoS service resource.
Time Schedule	Mandatory field. Default setting: (0) Always.	Apply Time Schedule to this rule; otherwise leave it as (0) Always. (refer to User Rule > Scheduling > Configuration settings)
Rule Enable	Disabled by default.	Click Enable box to activate this QoS rule.
Save	Button.	Click the Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

4. Serial Port

4.1 Bus & Protocol

4.1.1 Port Configuration

Navigate to the Serial Port > Bus & Protocol > Port Configuration tab.

The Edit button in Configuration window allows you configure serial port parameters including the operation mode being "Virtual COM" or disabled, the interface, the baud rate, the data bit length, the stop bit length, the flow control, and the parity.

Serial Port Definition
^

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

Save Undo

Port Configuration Window		
Item	Value setting	Description
Serial Port	System data.	Displays the serial port ID of the serial port.
Operation Mode	Disabled by default.	Displays the current selected operation mode for the serial interface.
Interface	Default setting: RS-232 .	Select the physical interface type for connecting to the access device(s) with the same interface specification.
Baud Rate	Default setting: 19200 .	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	Default setting: 8 .	Select 8 or 7 for data bits.
Stop Bits	Default setting: 1 .	Select 1 or 2 for stop bits.
Flow Control	Default setting: None .	Select None / RTS, CTS / DTS, DSR for Flow Control in RS-232 mode.
Parity	Default setting: None .	Select None / Even / Odd for Parity bit.
Edit	Button.	Click Edit button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

4.1.2 Virtual COM

Navigate to the **Serial Port > Bus & Protocol > Virtual COM** tab.

Operation Configs

Serial	Operation	Listen	Trust	Max	Connection	Connection Idle	Alive Check	Enable	Action
Port	Mode	Port	Type	Connection	Control	Timeout	Timeout		
SPort-0	Disable	N/A	N/A	N/A	N/A	N/A	N/A	<input type="checkbox"/>	Edit

Virtual COM setting window enables you to connect a COM port device to the Internet. It allows you to transfer serial data remotely. Operation mode includes TCP Client, TCP Server, UDP, and RFC2217.

Following an example of setting the TCP Client mode.

Operation Configs

Serial	Operation Mode	Listen Port	Trust Type	Max	Connection	Connection Idle	Alive Check	Enable	Action
Port				Connection	Control	Timeout	Timeout		
SPort-0	TCP Client	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable TCP Client Mode Window

Item	Value setting	Description
Operation Mode	Mandatory field.	Select TCP Client .
Connection Control	Default setting: Always on .	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	Default setting: 0.	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	Default setting: 0.	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.

Type in settings in Data Packing window.

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

Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	0 (0~1024)	0 (Hex) <input type="checkbox"/>	0 (Hex) <input type="checkbox"/>	0 (0~1000ms)

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

Setup Host IP / FQDN

Legal Host IP/ FQDN Definition (for TCP Client operation mode)					
ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	Edit
2		4001	SPort-0	<input type="checkbox"/>	Edit
3		4001	SPort-0	<input type="checkbox"/>	Edit
4		4001	SPort-0	<input type="checkbox"/>	Edit

Host IP / FQDN		
Item	Value setting	Description
To Remote Host	Mandatory field.	Press Edit button to enter IP address or FQDN of the remote TCP server to transmit serial data.
Remote Port	Mandatory field. Default setting: 4001.	Enter the TCP port number. This is the listen port of the remote TCP server. Value Range: 1 - 65535.
Serial Port	Default setting: SPort-0.	Apply the TCP server connection for a selected serial port. Up to 4 TCP servers can be configured at the same time for each serial port.
Definition Enable	Disabled by default.	Check the Enable box to enable the TCP server configuration.

Configure the MG400 as a TCP Server.

Operation Configs									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Server ▼	4001 (1~65535)	Allow All ▼	1	Always on ▼	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable TCP Server Mode Window		
Item	Value setting	Description
Operation Mode	Mandatory field.	Select TCP Server mode.
Listen Port	Default setting: 4001.	Indicate the listening port of TCP connection. Value Range: 1 - 65535.
Trust Type	Default setting: Allow All .	Choose Allow All to allow any TCP clients to connect. Otherwise choose Specific IP to limit certain TCP clients.
Max Connection	Default setting: 1.	Set the maximum number of concurrent TCP connections. Up to 128 simultaneous TCP connections can be established. Value Range: 1 - 128.
Connection Idle Timeout	Default setting: 0.	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	Default setting: 0.	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	Disabled by default.	Check the Enable box to activate the corresponding serial port in specified operation mode.

Type in Data Packing parameters.

Data Packing (for TCP Client, TCP Server and UDP operation mode)				
Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	0 (0~1024)	0 (Hex) <input type="checkbox"/> Enable	0 (Hex) <input type="checkbox"/> Enable	0 (0~1000ms)
<div>Save Undo</div>				

Data Packing Configuration		
Item	Value setting	Description
Data Buffer	Optional Setting.	Enter the data buffer length for the serial port.

Length	Default value is 0.	Value Range: 0 - 1024.
Delimiter Character 1	Optional Setting. Default value is 0.	Check the Enable box to activate the Delimiter character 1 and enter the Hex code for it. Value Range: 0x00 - 0xFF.
Delimiter Character 2	Optional Setting. Default value is 0.	Check the Enable box to activate the Delimiter character 2 and enter the Hex code for it. Value Range: 0x00 - 0xFF.
Data Timeout Transmit	Optional Setting. Default value is 0.	Enter the data timeout interval for transmitting serial data through the port. By default, it is set to 0 and the timeout function is disabled. Value Range: 0 - 1000ms.
Save	Button.	Click the Save button to save the configuration
Undo	Button	Click Undo to cancel the settings.

Setup TCP Clients for TCP Server Access.

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	Edit
2			<input type="checkbox"/>	Edit
3			<input type="checkbox"/>	Edit
4			<input type="checkbox"/>	Edit

Enter TCP Clients Window		
Item	Value setting	Description
Host	Mandatory field.	Enter the IP address range of allowed TCP clients.
Serial Port	Disabled by default.	Check the box to select the rule for the Serial Port.
Definition Enable	Disabled by default.	Check the Enable box to enable the rule.

Following the settings of enabling the UDP mode.

Operation Configs									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	UDP	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable UDP Mode Window		
Item	Value setting	Description
Operation Mode	Mandatory field.	Select UDP mode.
Listen Port	Default setting: 4001.	Indicate the listening port of UDP connection. Value Range: 1 - 65535
Enable	Disabled by default.	Check the Enable box to activate the corresponding serial port in specified operation mode.

Enter Data Packing Parameters

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

Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	<input style="width: 50px;" type="text" value="0"/> (0~1024)	<input style="width: 50px;" type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input style="width: 50px;" type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input style="width: 50px;" type="text" value="0"/> (0~1000ms)

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

Setup the remote UDP host.

Legal Host IP Definition (for UDP operation mode)					
ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	Edit
2		4001	SPort-0	<input type="checkbox"/>	Edit
3		4001	SPort-0	<input type="checkbox"/>	Edit
4		4001	SPort-0	<input type="checkbox"/>	Edit

Enter Remote UDP hosts Window		
Item	Value setting	Description
Host	Mandatory field.	Press Edit button to enter IP address range of remote UDP hosts.
Remote Port	Default value is 4001.	Indicate the UDP port of peer UDP hosts. Value Range: 1 - 65535
Serial Port	Default setting: SPort-0.	Apply the UDP hosts for a selected serial port. Up to 4 UDP servers can be configured at the same time for each serial port.
Definition Enable	Disabled by default.	Check the Enable box to enable the rule.

Following the settings of enabling RFC-2217 mode.

Operation Configs							
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout
SPort-0	RFC-2217	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)
							<input type="checkbox"/> Edit

Enable RFC-2217 Mode Window		
Item	Value setting	Description
Operation Mode	Mandatory field.	Select RFC-2217 mode.
Listen Port	Default setting: 4001.	Indicate the listening port of RFC-2217 connection. Value Range: 1 - 65535
Trust Type	Default setting: Allow All .	Choose Allow All to allow any clients to connect. Otherwise choose Specific IP to limit certain clients.
Connection Idle Timeout	Default setting: 0.	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	Default setting: 0.	Enter the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive check

Timeout		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	Disabled by default.	Check the Enable box to activate the corresponding serial port in specified operation mode.

Enter Data Packing Parameters.

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

Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	<input type="text" value="0"/> (0~1024)	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (0~1000ms)

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

Enter Remote Host for Access

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	<input type="button" value="Edit"/>
2			<input type="checkbox"/>	<input type="button" value="Edit"/>
3			<input type="checkbox"/>	<input type="button" value="Edit"/>
4			<input type="checkbox"/>	<input type="button" value="Edit"/>

Enter RFC-2217 Clients for Access Window		
Item	Value setting	Description
Host	Mandatory field.	Enter the IP address range of allowed clients.
Serial Port	Disabled by default.	Check the box to Enter the rule for selected Serial Port.
Definition Enable	Disabled by default.	Check the Enable box to enable the rule.

5. User Rule

5.1 Scheduling

Navigate to the User Rule > Scheduling > Configuration tab.

☐ Time Schedule List

^

ID	Rule Name	Actions
<input type="button" value="Save"/> <input type="button" value="Refresh"/>		

Button description		
Item	Value setting	Description
Add	Button.	Click the Add button to configure time schedule rule.
Delete	Button.	Click the Delete button to delete selected rule(s).
Save	Button.	Click the Save button to save the configuration.
Refresh	Button.	Refresh the Time Schedule List.

When Add button is applied, Time Schedule Configuration and Time Period Definition windows will appear.

Time Schedule Configuration

Item	Setting
Rule Name	<input type="text"/>
Rule Policy	<div>Inactivate</div> the Selected Days and Hours Below.

Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --	<input type="text"/>	<input type="text"/>
2	-- choose one --	<input type="text"/>	<input type="text"/>
3	-- choose one --	<input type="text"/>	<input type="text"/>
4	-- choose one --	<input type="text"/>	<input type="text"/>
5	-- choose one --	<input type="text"/>	<input type="text"/>
6	-- choose one --	<input type="text"/>	<input type="text"/>
7	-- choose one --	<input type="text"/>	<input type="text"/>
8	-- choose one --	<input type="text"/>	<input type="text"/>

Save

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 every day 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.
Save	System data.	Click Save to save the settings.

5.2 User

You can manage user account in this section, including user list, user profile and user group.

5.2.1 User List

Navigate to the User Rule > User > User List tab.

User List displays the username, user level, membership group name, IP address, on-line status and activity status in User List & Status window.

User List & Status

AddDeleteRefresh

User Name	User Level	Group Name	IP Address	On-line Status	Enable	Actions
-----------	------------	------------	------------	----------------	--------	---------

When **Add** button is pressed, the **User Profile Configuration** window will pop up as follows,

User NameUser LevelGroup NameIP AddressOn-line StatusEnableActions

User Profile Configuration

Item	Setting
User Name	admin
Password
User Level	Admin
Lease Time	(seconds)
Idle Timeout	(seconds)
Group to	
Profile	<input checked="" type="checkbox"/> Enable

Save

See following 5.2.2 User Profile section for the details.

5.2.2 User Profile

Navigate to the User Rule > User > User Profile tab.

User Profile Configuration

Item	Setting
▶ User Name	<input type="text" value="admin"/>
▶ Password	<input type="password" value="....."/>
▶ User Level	<input type="text" value="Admin"/>
▶ Lease Time	<input type="text"/> (seconds)
▶ Idle Timeout	<input type="text"/> (seconds)
▶ Group to	<input type="text"/>
▶ Profile	<input checked="" type="checkbox"/> Enable

Save

User Profile Configuration		
Item	Value setting	Description
User Name	Enter text string. Mandatory field.	Enter the name of user account.
Password	Enter text string. Mandatory field.	Enter the password of user account.
User Level	Default setting: Admin. Mandatory field.	Select a User Level for the account. There are 4 available levels for you to select, including "Admin", "Staff", "Guest" and "Passenger" . Admin level of account can allow the user to configure the MG400 with fully control ability. Staff level of can access both the Intranet resources and the Internet resources. Guest level account can use limited bandwidth to access Internet. Passenger level of user account is for mobile users to use the MG400 to access the Internet. He will use fair and average bandwidth utilization with other passengers.
Lease Time	Any integer. Optional field.	Enter the lease time (in seconds) for the user account to login the MG400. The MG400 will log out the user if the user has logged in longer than the Lease Timeout.
Idle Time	Number format can be any integer number. Optional field.	Enter the idle time (in seconds) for the user account. The MG400 will logout the user account if the user is idle for the time longer than the Idle Timeout.
Group to	Enter text string. Optional field.	Enter a group name if the user would like to collect the user in a certain user group.
Profile	Enabled by default.	Check the Enable box to activate the user profile.

	Mandatory field.	
Save	Button.	Click the Save button to save the settings.

Navigate to the User Rule > User > User Group tab.

<div> <div>User Group List</div> <div> <div>Add</div> <div>Delete</div> <div>Refresh</div> </div> </div>					
ID	Group Name	User Member List	Bound Services	Enable	Actions

User Group Configuration

Item	Setting
▶ Group Name	<input type="text"/>
▶ Multiple User Members	<input type="button" value="Choice"/>
▶ Multiple Bound Services	<input type="checkbox"/> X-Auth <input type="checkbox"/> NAS <input type="checkbox"/> RADIUS <input type="checkbox"/> VPN
▶ QoS & BWM Property	<input type="button" value="Individual Control ▼"/> Set MINR : <input type="text"/> MAXR : <input type="text"/> <input type="button" value="Mbps ▼"/>
▶ Policy Routing Property	Routing Interface : <input type="button" value="WAN-1 ▼"/>
▶ Group	<input checked="" type="checkbox"/> Enable

Save

Undo

User Profile Configuration		
Item	Value setting	Description
Group Name	Enter text string. Mandatory field.	Enter the name of user group. Value Range: at least 1 character, 'A' - 'Z', 'a' - 'z', and '0' - '9' are valid;
Multiple user Members	System data.	Click the Choice button to select multiple user accounts to join the group.
Multiple Bound Services	System data.	Check the available service box(es) to bind with the user group. So, the bound service can use the group object or all user account objects in the group.
QoS & BWM Property	Mandatory field. Default setting: Individual Control.	Enter the preferred sharing method for how to apply a QoS rule on the selected group, and define the guaranteed and limited bandwidth usage for the group It can be Individual Control or Group Control. Individual Control: If Individual Control is selected, each user in the group will have its QoS service resource as specified in the rule. Group Control: If Group Control is selected, the entire user group shares the same QoS service resource.
Policy Routing Property	Mandatory field. Default setting: WAN-1.	Enter the routing interface. All packets from the group members will be routed via the specified interface.
Group	Enabled by default. Mandatory field.	Check the Enable box to activate the user group.
Save	Button.	Click the Save button to save the settings.
Undo	Button.	Click the Undo button to cancel the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

5.3 Grouping

Navigate to the User Rule > Grouping > Host Grouping tab.

The Grouping function allows you to make group for some services, such as QoS, Firewall, and Communication Bus.

Host Group List
Add
Delete
^

ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions
Refresh						

When Add button is applied, Host Group Configuration window will pop up.

Host Group Configuration
×

Item	Setting
▶ Group Name	<input type="text"/>
▶ Group Type	IP Address-based ▼
▶ Member to Join	<input type="text"/> Join
▶ Member List	
▶ Bound Services	<input type="checkbox"/> Firewall <input type="checkbox"/> QoS
▶ Group	<input type="checkbox"/> Enable

Save

Host Group Configuration		
Item	Value setting	Description
Group Name	Enter text string. Mandatory field.	Enter a group name for the rule. It is a name that is easy for you to understand.
Group Type	Default setting: IP Address-based. Mandatory field.	<p>Select the group type for the host group. It can be IP Address-based, MAC Address-based, or Host Name-based.</p> <p>When IP Address-based is selected, only IP address can be added in Member to Join.</p> <p>When MAC Address-based is selected, only MAC address can be added in Member to Join.</p> <p>When Host Name-based is selected, only host name can be added in Member to Join.</p>
Member to Join	System data.	<p>Add the members to the group in this field.</p> <p>You can enter the member information as specified in the Member Type above and press the Join button to add.</p> <p>Only one member can be added at a time. You need to add the members to the group one by one.</p>
Member List	System data.	This field will indicate the hosts (members) contained in the group.
Bound Services	Disabled by default.	Binding the services that the host group can be applied. If you enable the Firewall, the produced group can be used in firewall service. Same as by enable QoS, or other available service types.
Group	Disabled by default.	Check the Enable checkbox to activate the host group rule. So that the group can be bound to selected service(s) for further configuration.
Save	Button.	Click Save to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

5.4 External Servers

Navigate to the User Rule > External Servers tab.

The External Server page allows you to add external servers.

External Server List
Add
Delete
^

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

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

External Server Configuration
^
x

Item	Setting
▶ Server Name	<input type="text"/>
▶ Server Type	<div>Email Server ▼</div> <div>User Name: <input type="text"/></div> <div>Password: <input type="password"/></div>
▶ Server IP/FQDN	<input type="text"/>
▶ Server Port	<input type="text" value="25"/>
▶ Server	<input checked="" type="checkbox"/> Enable
Save	
Refresh	

External Server Configuration		
Item	Value setting	Description
Sever Name	Enter text string. Mandatory field.	Enter the server name. Enter a name that is easy for you to understand.
Server Type	Mandatory field.	Enter the Server Type of the external server and enter the required settings for the accessing the server.
		Email Server (Mandatory field.): When Email Server is selected, Username, and Password are also required. Username (String format: any text) Password (String format: any text) RADIUS Server (Mandatory field.): When RADIUS Server is selected, the following settings are also required.

Primary:
 Shared Key (String format: any text)
 Authentication Protocol (Default setting: CHAP.)
 Session Timeout (Default setting: 1)
 The values need to be between 1 and 60.
 Idle Timeout: (Default setting: 1)
 The values need to be between 1 and 15.
 Secondary:
 Shared Key (String format: any text)
 Authentication Protocol (Default setting: CHAP.)
 Session Timeout (Default setting: 1.)
 The values need to be between 1 and 60.
 Idle Timeout: (Default setting: 1.)
 The values need to be between 1 and 15.
 Active Directory Server (Mandatory field.):
 When Active Directory Server is selected, Domain setting is also required.
 Domain (String format: any text)
 LDAP Server (Mandatory field.):
 When LDAP Server is selected, the following settings are also required.
 Base DN (String format: any text)
 Identity (String format: any text)
 Password (String format: any text)
 UAM Server (Mandatory field.):
 When UAM Server is selected, the following settings are also required.
 Login URL (String format: any text)
 Shared Secret (String format: any text)
 NAS/Device ID (String format: any text)
 Location ID (String format: any text)
 Location Name (String format: any text)
 TACACS+ Server (Mandatory field.):
 When TACACS+ Server is selected, the following settings are also required.
 Shared Key (String format: any text)
 Session Timeout (String format: any number)
 The values need to be between 1 and 60.
 SCEP Server (Mandatory field.):
 When SCEP Server is selected, the following settings are also required.
 Path (String format: any text, default setting: cgi-bin.)
 Application (String format: any text, default setting: pkiclient.exe is filled.)
 FTP(SFTP) Server (Mandatory field.):
 When FTP(SFTP) Server is selected, the following settings are also required.
 Username (String format: any text)
 Password (String format: any text)
 Protocol (Select FTP or SFTP)
 Encryption (Select Plain, Explicit FTPS or Implicit FTPS)
 Transfer mode (Select Passive or Active)

Server IP/FQDN Mandatory field.

Enter the IP address or FQDN used for the external server.

Server Port	Mandatory field.	<p>Enter the Port used for the external server. If you select a certain server type, the default server port number will be set.</p> <p>Email Server, default setting: 25;</p> <p>Syslog Server, default setting: 514;</p> <p>For RADIUS Server, default setting: 1812, 1823;</p> <p>For Active Directory Server, default setting: 389;</p> <p>For LDAP Server, default setting: 389;</p> <p>For UAM Server, default setting: 3990, 4990;</p> <p>For TACACS+ Server, default setting: 49;</p> <p>For SCEP Server, default setting: 80;</p> <p>For FTP(SFTP) Server, default setting: 21;</p> <p>Value Range: 1 - 65535.</p>
Account Port	Mandatory field. Default setting: 1813.	<p>Enter the accounting port used if you select external RADIUS server.</p> <p>Value Range: 1 - 65535.</p>
Server	Enabled by default.	Click Enable to activate this External Server.
Save	Button.	Click Save to save the settings.
Refresh	Button.	Click the Refresh button to refresh the external server list.

5.5 Certificate

5.5.1 Configuration

Navigate to the User Rule > Certificate > Configuration tab.

The configuration setting allows you to create Root Certificate Authority (CA) and enable Simple Certificate Enrolment Protocol (SCEP).

The **Root CA** can be generated in the **Root CA** window.

Root CA Generate					
ID	Name	Subject	Issuer	Vaild To	Action

When **Generate** button is clicked, **Root CA Certificate Configuration** window will pop up. Please fill in the name, key, subject name and validity period.

Configuration

Root CA Certificate Configuration

Item	Setting
▶ Name	<input type="text"/>
▶ Key	Key Type : RSA ▼ Key Length : 512-bits ▼ Digest Algorithm : MD5 ▼
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> E-mail : <input type="text"/>
▶ Validity Period	20-years ▼

Save

Root CA Certificate Configuration		
Item	Value setting	Description
Name	Enter text string. Mandatory field.	Enter the Root CA Certificate name. It will be a certificate file name.
Key	Mandatory field.	This field is to enter the key attribute of certificate. Key Type to set public-key cryptosystems. It only supports RSA now. Key Length to set the size measured in bits of the key used in a cryptographic algorithm. Digest Algorithm to set identifier in the signature algorithm identifier of certificates
Subject Name	Mandatory field.	This field is to enter the information of certificate. Country (C) is the two-letter ISO code for the country where your organization is located. State (ST) is the state where your organization is located. Location (L) is the location where your organization is located. Organization (O) is the name of your organization. Organization Unit (OU) is the name of your organization unit. Common Name (CN) is the name of your organization. Email is the email of your organization. It need to be email address style.
Validity Period	Mandatory field.	This field is to enter the validity period of certificate.
Save	Button.	Click Save to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

SCEP can be enabled in the **SCEP Configuration** window.

SCEP Configuration

Item	Setting
▶ SCEP	<input type="checkbox"/> Enable
▶ Automatically re-enroll aging certificates	<input type="checkbox"/> Enable

Save

Undo

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

5.5.2 My Certificate

Navigate to the User Rule > Certificate > My Certificate tab.

The Local Certificate List shows all generated certificates by the root CA for the MG400. And it also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the MG400.

<div>Local Certificate List</div> <div>AddImportDelete</div>					
ID	Name	Subject	Issuer	Vaild To	Actions

When **Add** button is applied, **Local Certificate Configuration** window will pop up. Please fill in name, key, subject name, extra attributes and SCEP Enrolment.

NameSubjectIssuerVaild ToActions

Local Certificate Configuration

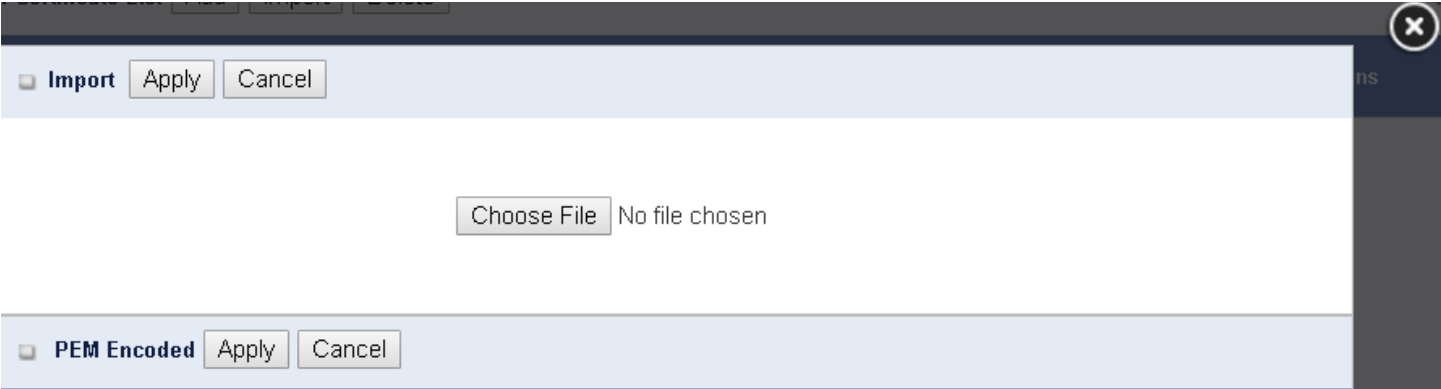
Item	Setting
Name	<div></div> Self-signed : <input type="checkbox"/>
Key	Key Type : <div>RSA</div> Key Length : <div>1024-bits</div> Digest Algorithm : <div>SHA-1</div>
Subject Name	<div>Country(C) : <div></div>State(ST) : <div></div>Location(L) : <div></div></div> <div>Organization(O) : <div></div>Organization Unit(OU) : <div></div></div> <div>Common Name(CN) : <div></div>E-mail : <div></div></div>
Extra Attributes	<div>Challenge Password: <div></div></div> <div>Unstructured Name: <div></div></div>
SCEP Enrollment	<div>Enable: <input type="checkbox"/>SCEP Server: <div>--- Option ---</div><div>Add Object</div></div> <div>CA Certificate: <div></div>CA Encryption Certificate: <div>--- Option ---</div>(Optional)</div> <div>CA Identifier: <div>admin</div>(Optional)</div>

Save

Local Certificate Configuration		
Item	Value setting	Description
Name	Enter text string. Mandatory field.	Enter a certificate name. It will be a certificate file name If Self-signed is checked, it will be signed by root CA. If Self-signed is not checked, it will generate a certificate signing request (CSR).
Key	Mandatory field.	This field is to enter the key attributes of certificate. Key Type to set public-key cryptosystems. Currently, only RSA is supported. Key Length to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. Digest Algorithm to set identifier in the signature algorithm

		identifier of certificates. It can be MD5/SHA-1.
Subject Name	Mandatory field.	<p>This field is to enter the information of certificate.</p> <p>Country (C) is the two-letter ISO code for the country where your organization is located.</p> <p>State (ST) is the state where your organization is located.</p> <p>Location (L) is the location where your organization is located.</p> <p>Organization (O) is the name of your organization.</p> <p>Organization Unit (OU) is the name of your organization unit.</p> <p>Common Name (CN) is the name of your organization.</p> <p>Email is the email address of your organization. It needs to be email address setting only.</p>
Extra Attributes	Mandatory field.	<p>This field is to enter the extra information for generating a certificate.</p> <p>Challenge Password for the password you can use to request certificate revocation in the future.</p> <p>Unstructured Name for additional information.</p>
SCEP Enrollment	Mandatory field.	<p>This field is to enter the information of SCEP.</p> <p>If you want to generate a certificate signing request (CSR) and then signed by SCEP server online, you can check the Enable box.</p> <p>Select a SCEP Server to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to User Rule > External Server > External Server. You may click Add Object button to generate, and the settings are the same as those defined in Section 3.4 External Server.</p> <p>Select a CA Certificate to identify which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates.</p> <p>Select an optional CA Encryption Certificate, if it is required, to identify which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates.</p> <p>Fill in optional CA Identifier to identify which CA could be used for signing certificates.</p>
Save	Button.	Click the Save button to save the configuration.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

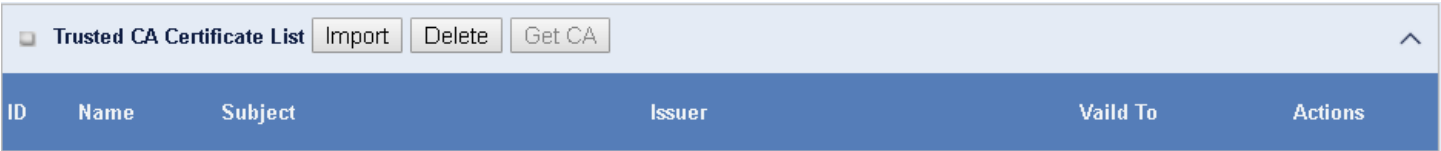
When Import button is applied, an Import window will pop up. You can import a certificate file, or directly paste a PEM encoded string as a certificate.



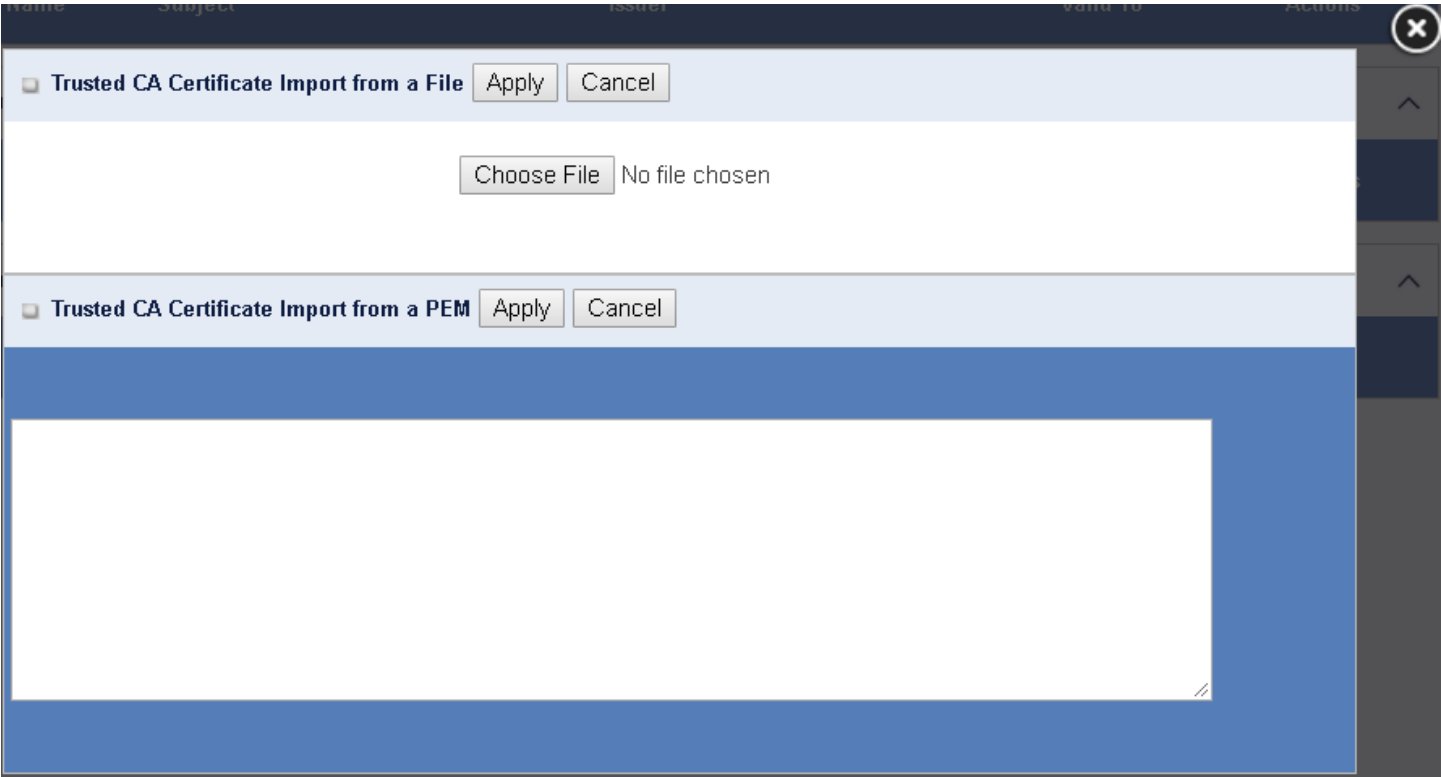
Import		
Item	Value setting	Description
Import	Mandatory field.	Select a certificate file from your computer and click the Apply button to import the specified certificate file to the MG400.
PEM Encoded	Enter text string. Mandatory field.	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the Apply button to import the specified certificate to the MG400.
Apply	Button.	Click the Apply button to import the certificate.
Cancel	Button.	Click the Cancel button to discard the import operation and the window will return to the My Certificates page.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

5.5.3 Trusted Certificate
Navigate to User Rule > Certificate > Trusted Certificate tab.

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



When Import button is clicked, a Trusted CA import window will pop up. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.



Trusted CA Certificate List		
Item	Value setting	Description
Import from a File	Mandatory field.	Select a CA certificate file from your computer and click the Apply button to import the specified CA certificate file to the MG400.
Import from a PEM	Enter text string. Mandatory field.	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string, and click the Apply button to import the specified CA certificate to the MG400.
Apply	Button.	Click the Apply button to import the certificate.
Cancel	Button.	Click the Cancel button to discard the import operation and the window will return to the Trusted Certificates page.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

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

If SCEP is enabled (User Rule > Certificate > Configuration page), you can click Get CA button, the Get CA Configuration window will appear.

ame

Subject

Issuer

Vaild To

Actions

Get CA Configuration

Item

Setting

▶ SCEP Server

--- Option --- ▼

Add Object

▶ CA Identifier

admin

(Optional)

Save

Get CA Configuration		
Item	Value setting	Description
SCEP Server	Mandatory field.	Select a SCEP Server to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to User Rule > External Server > External Server. You may click Add Object button to generate.
CA Identifier	Enter text string.	Fill in optional CA Identifier to identify which CA could be used for signing certificates.
Save	System data.	Click Save to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

Trusted Client Certificate can be imported from **Trusted Client Certificate List** window.

Trusted Client Certificate List

Import

Delete

^

ID

Name

Subject

Issuer

Vaild To

Actions

When Import button is clicked, a Trusted Client Certificate Import window will appear. You can import a certificate file, or directly paste a PEM encoded string as the certificate.

Trusted Client Certificate Import from a File

ApplyCancel

Choose FileNo file chosen

Trusted Client Certificate Import from a PEM

ApplyCancel

Trusted Client Certificate List Item	Value setting	Description
Import from a File	Mandatory field.	Select a certificate file from your computer and click the Apply button to import the specified certificate file to the MG400.
Import from a PEM	Enter text string. Mandatory field.	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the Apply button to import the specified certificate to the MG400.
Apply	Button.	Click the Apply button to import certificate.
Cancel	Button.	Click the Cancel button to discard the import operation and the window will return to the Trusted Certificates page.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

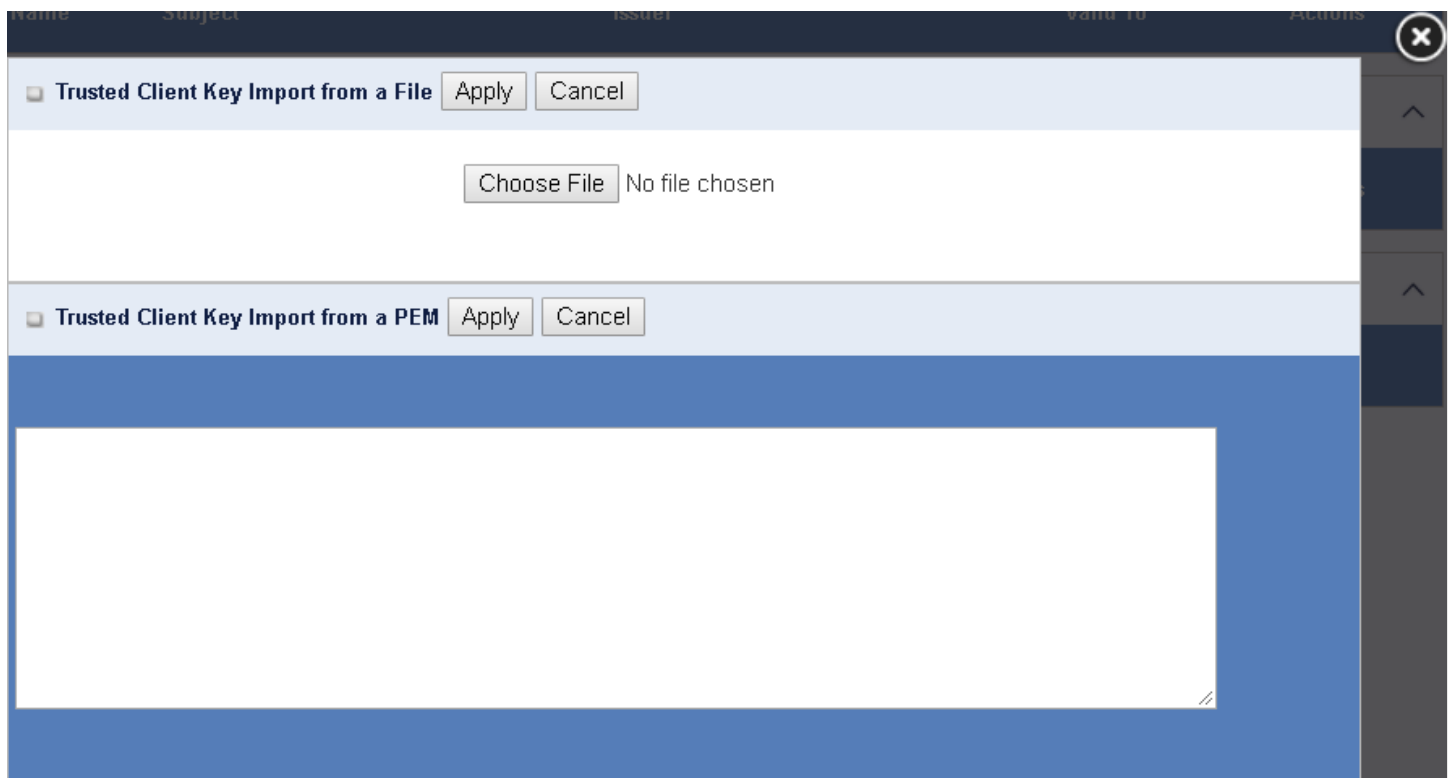
Trusted Client Key can be imported via following **Trusted Client Key List**.

Trusted Client Key List

ImportDelete

ID	Name	Actions
----	------	---------

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



Trusted Client Key List		
Item	Value setting	Description
Import from a File	Mandatory field.	Select a certificate key file from your computer and click the Apply button to import the specified key file to the MG400.
Import from a PEM	Enter text string. Mandatory field.	This is an alternative approach to import a certificate key. You can directly fill in (Copy and Paste) the PEM encoded certificate key string, and click the Apply button to import the specified certificate key to the MG400.
Apply	Button.	Click the Apply button to import the certificate key.
Cancel	Button.	Click the Cancel button to discard the import operation and the window will return to the Trusted Certificates page.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

5.5.4 Issued Certificate

Navigate to the User Rule > Certificate > Issued Certificate tab.

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the MG400, you can issue the request via Issued Certificate page and allow Root CA sign it. There are two approaches to issue a certificate. One is from a CSR file importing from the managing PC and another is copy-paste the CSR codes in device's web-based utility, and then click on the "Sign" button.

If the MG400 signs a CSR successfully, the "Signed Certificate View" window will show the resulted certificate contents. In addition, a "Download" button is available for you to download the certificate to a file in the

managing PC.

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

Import and Issue Certificate

Certificate Signing Request (CSR) Import from a File

Sign

Choose File No file chosen

Certificate Signing Request (CSR) Import from a PEM

Sign

Certificate Signing Request (CSR) Import from a File		
Item	Value setting	Description
Certificate Signing Request (CSR) Import from a File	Mandatory field.	Select a certificate signing request file for your computer for importing to the MG400.
Certificate Signing Request (CSR) Import from a PEM	Enter text string. Mandatory field.	Enter (copy-paste) the certificate signing request PEM encoded certificate to the MG400.
Sign	Button.	When root CA exists, click the Sign button sign and issue the imported certificate by root CA.

6. Security

6.1 VPN

6.1.1 IPSec

Navigate to the Security > VPN > IPSec tab.

There are four scenarios:

Site to Site: You need to setup remote device IP and subnet of device at each site. After the IPSec tunnel established, hosts which connect to both devices can communicate with each other through the tunnel.

Site to Host: Site to Host is suitable for tunnelling between clients in a subnet and an application server (host).

Host to Site: On the contrast, for a single host to access the resources located in an intranet, the Host to Site scenario can be applied.

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

The Configuration window allow you to enable IPSec.

Configuration		^
Item	Setting	
▶ IPSec	<input checked="" type="checkbox"/> Enable	
▶ Max. Concurrent IPSec Tunnels	16	

Configuration Window		
Item	Value setting	Description
IPsec	Disabled by default.	Click the Enable box to enable IPSec function.
Max. Concurrent IPSec Tunnels	System data.	The maximum number of simultaneous IPSec tunnel connection is 16.

The Dynamic VPN Server List shows the existed VPN rule.

Dynamic VPN List Add Delete Refresh ^					
ID	Tunnel Name	Interface	Connected Client	Enable	Action

When Add / Edit button is clicked, a series of configuration windows will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition.

Tunnel Configuration

Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	<input type="text" value="Dynamic IPSec1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Tunnel Scenario	<input type="text" value="Tunnel Mode"/>
▶ Encapsulation Protocol	<input type="text" value="ESP"/>
▶ IKE Version	<input type="text" value="v1"/>

Local & Remote Configuration

Item	Setting
▶ Local Subnet	<input type="text" value="192.168.123.0"/>
▶ Local Netmask	<input type="text" value="255.255.255.0(24)"/>

Authentication

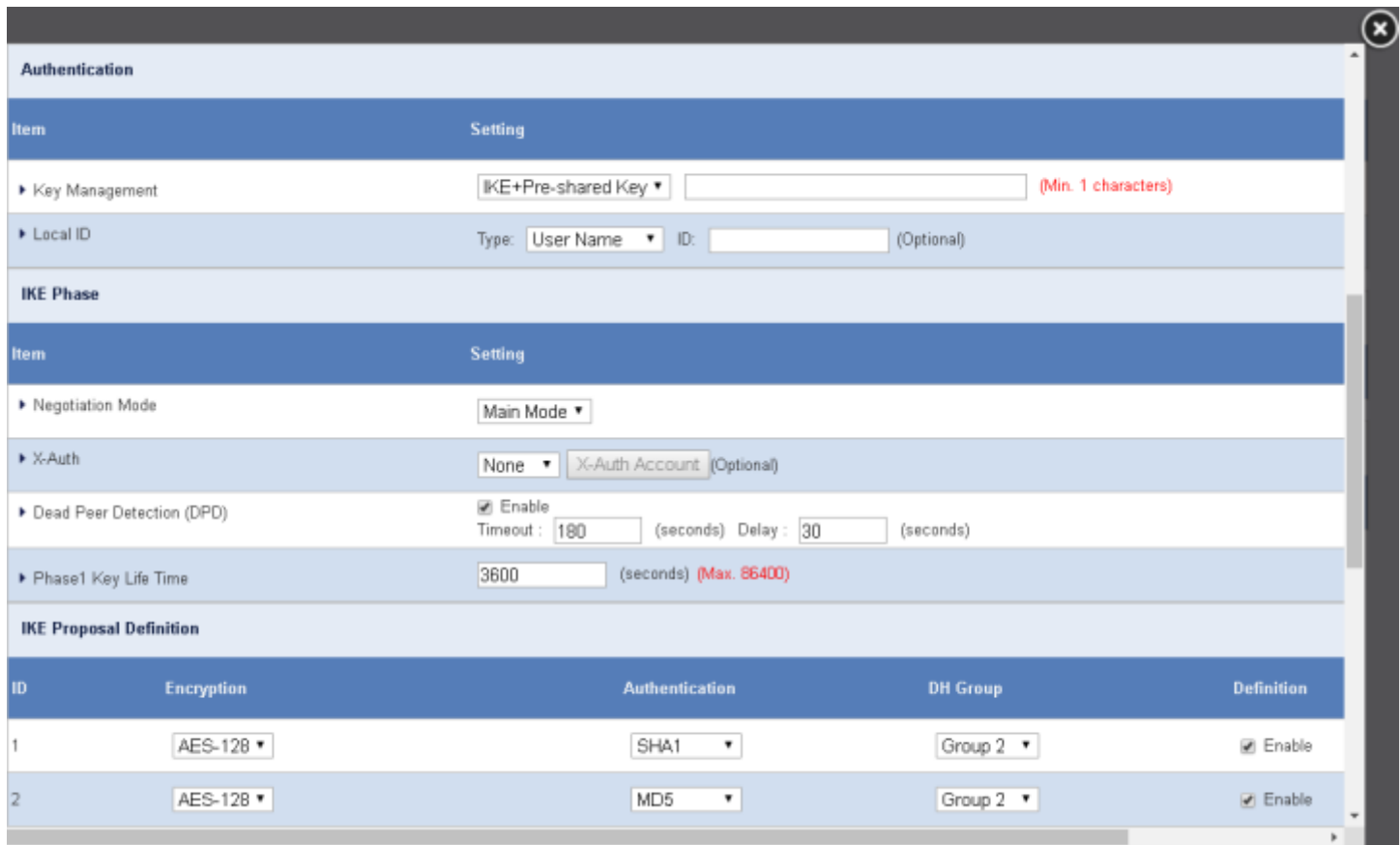
Item	Setting
------	---------

Tunnel Configuration Window

Item	Value setting	Description
Tunnel	Disabled by default.	Check the Enable box to activate the Dynamic IPSec VPN tunnel.
Tunnel Name	Mandatory field. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 19 characters.
Interface	Mandatory field. Default setting: WAN 1.	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	Mandatory field. Default setting: Tunnel Mode.	Select the Dynamic IPSec tunneling scenario. It can be Tunnel Mode or Transport Mode.
Encapsulation Protocol	Mandatory field. Default setting: ESP.	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.
IKE Version	Mandatory field. Default setting: v1.	Enter the IKE version for this IPSec tunnel.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

Local & Remote Configuration Window

Item	Value setting	Description
Local Subnet	Mandatory field.	Enter the Local Subnet IP address.
Local Netmask	Mandatory field.	Enter the Local Subnet Mask.



The screenshot shows the 'Authentication' configuration window. It is divided into several sections: 'Authentication', 'IKE Phase', and 'IKE Proposal Definition'. The 'Authentication' section includes fields for 'Key Management' (set to 'IKE+Pre-shared Key'), 'Local ID' (with a dropdown for 'Type' set to 'User Name' and an 'ID' field), and 'X-Auth' (set to 'None'). The 'IKE Phase' section includes 'Negotiation Mode' (set to 'Main Mode'), 'Dead Peer Detection (DPD)' (checked, with 'Timeout' at 180 seconds and 'Delay' at 30 seconds), and 'Phase1 Key Life Time' (set to 3600 seconds). The 'IKE Proposal Definition' section is a table with two rows, each representing a proposal with its own encryption, authentication, and DH group settings.

Authentication				
Item	Setting			
Key Management	IKE+Pre-shared Key			(Min. 1 characters)
Local ID	Type: User Name	ID:		(Optional)
IKE Phase				
Item	Setting			
Negotiation Mode	Main Mode			
X-Auth	None	X-Auth Account		(Optional)
Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable	Timeout: 180	(seconds)	Delay: 30 (seconds)
Phase1 Key Life Time	3600	(seconds)		(Max. 86400)
IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-128	SHA1	Group 2	<input checked="" type="checkbox"/> Enable
2	AES-128	MD5	Group 2	<input checked="" type="checkbox"/> Enable

Authentication Configuration Window


Item	Value setting	Description
Key Management	Mandatory field. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. IKE+Pre-shared Key: you need to set a key (8 - 32 characters).
Local ID	Optional field	Enter the Local ID for this IPSec tunnel to authenticate. Select User Name for Local ID and enter the username. The username may include but can't be all numbers . Select FQDN for Local ID and enter the FQDN. Select user@FQDN for Local ID and enter the user@FQDN. Select Key ID for Local ID and enter the Key ID (English alphabet or number).
Remote ID	Optional field	Enter the Remote ID for this IPSec tunnel to authenticate. Select User Name for Remote ID and enter the username. The username may include but can't be all numbers . Select FQDN for Local ID and enter the FQDN.

		Select user@FQDN for Remote ID and enter the user@FQDN. Select Key ID for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

IKE Phase Window		
Item	Value setting	Description
Negotiation Mode	Default setting: Main Mode.	Enter the Negotiation Mode for this IPSec tunnel. Select Main Mode or Aggressive Mode.
X-Auth	Default setting: None.	Enter the X-Auth role for this IPSec tunnel. Select Server, Client, or None. Selected None no X-Auth authentication is required. Selected Server the MG400 will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client account. Selected Client the MG400 will be an X-Auth client. Enter username and Password to be authenticated by the X-Auth server device. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
Dead Peer Detection (DPD)	Default setting: Timeout is 180s, and Delay is 30s	Click Enable box to enable DPD function. Enter the Timeout and Delay time in seconds. Value Range: 0 - 999 seconds for Timeout and Delay.
Phase1 Key Life Time	Mandatory field. Default setting: 3600s.	Enter the Phase1 Key Lifetime. Value Range: 30 - 86400.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

IKE Proposal Definition Window		
Item	Value setting	Description
IKE Proposal Definition	Mandatory field.	Enter the Phase 1 Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256.
		Enter the Authentication method. It can be None / MD5 / SHA1 / SHA2-256.
		Enter the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18.
		Check Enable box to enable this setting
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

IPSec tunnel can be added via the IPSec Tunnel List window.



When Add/Edit button is applied, a series of configuration windows will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. Tunnel details for both local and remote VPN devices need to be configured.

Tunnel Configuration

Item

Setting

▶ Tunnel

☐ Enable

▶ Tunnel Name

▶ Interface

▶ Tunnel Scenario

▶ Tunnel TCP MSS

(64~1500 Bytes)

▶ Encapsulation Protocol

▶ IKE Version

Local & Remote Configuration

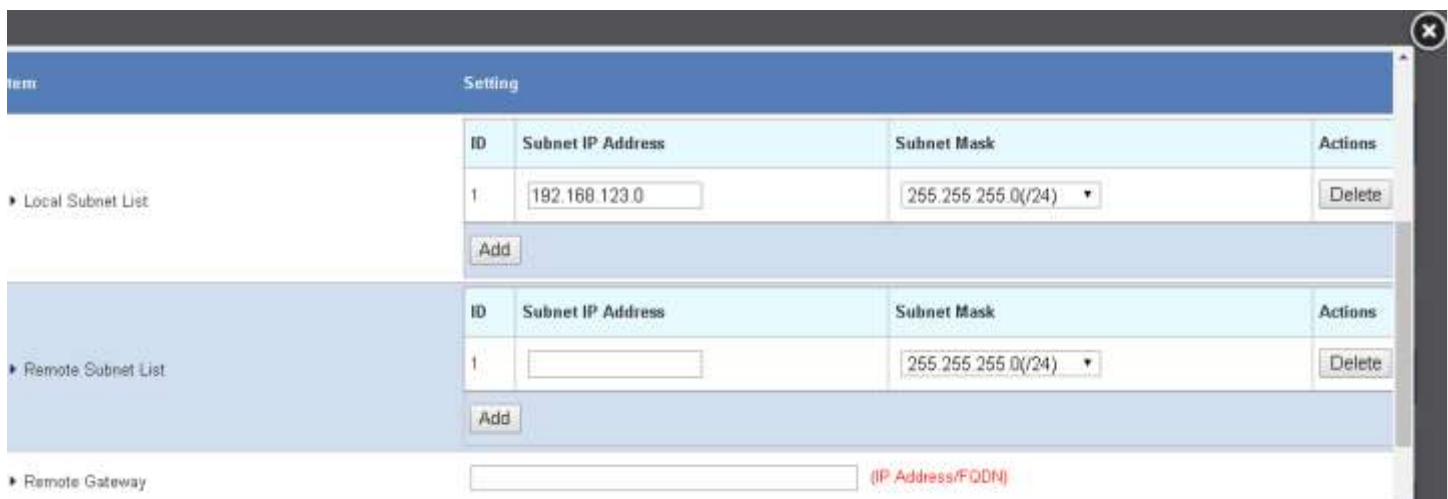
Item

Setting

▶ Local Subnet List

ID	Subnet IP Address	Subnet Mask	Actions
1	<input type="text" value="192.168.123.0"/>	<input type="text" value="255.255.255.0(/24)"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>			

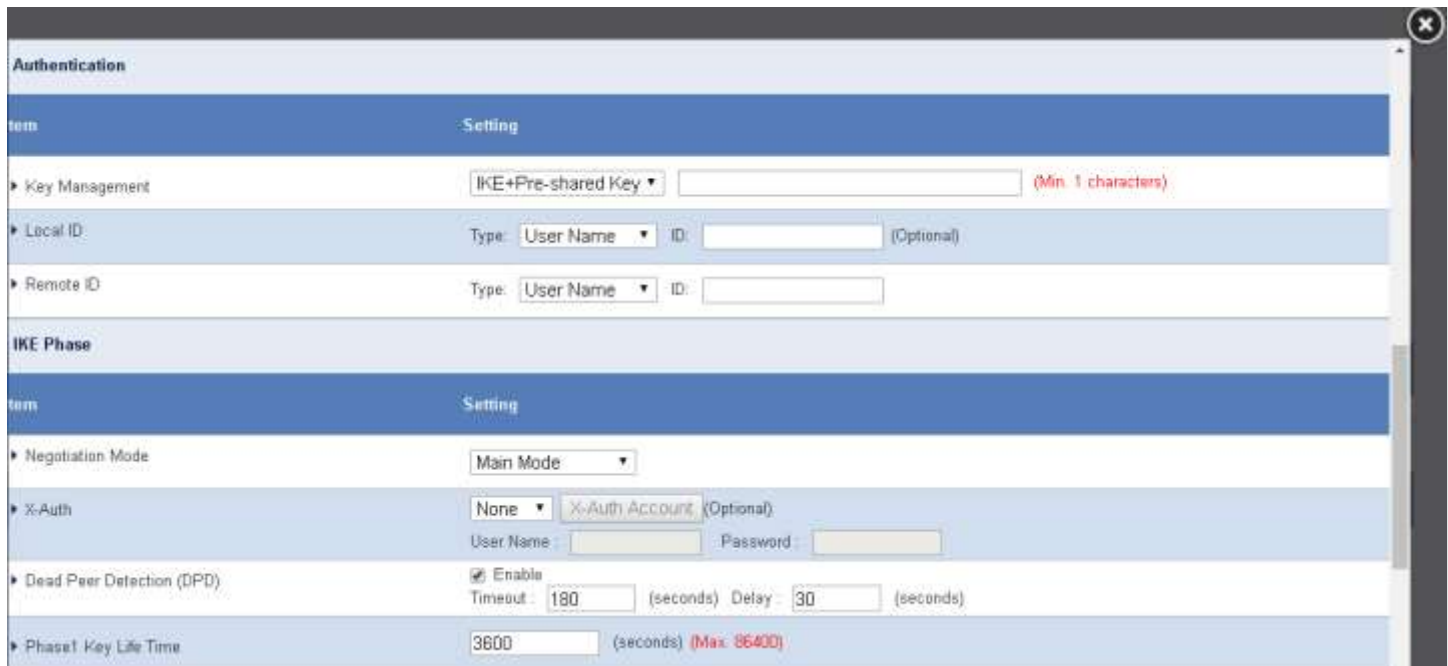
Tunnel Configuration Window		
Item	Value setting	Description
Tunnel	Disabled by default.	Check the Enable box to activate the IPSec tunnel.
Tunnel Name	Mandatory field. String format can be any text.	Enter a tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 19 characters.
Interface	Mandatory field. Default setting: WAN 1.	Select the interface on which IPSec tunnel is to be established. It can be the available WAN and LAN interfaces.
Tunnel Scenario	Mandatory field. Default setting: Site to site.	Select an IPSec tunneling scenario from the dropdown box for your application. Select Site-to-Site, Site-to-Host, Host-to-Site, or Host-to-Host. If LAN interface is selected, only Host-to-Host scenario is available. With Site-to-Site or Site-to-Host or Host-to-Site, IPSec operates in tunnel mode. The difference among them is the number of subnets. With Host-to-Host, IPSec operates in transport mode.
Tunnel TCP MSS	Optional field. Default setting: Auto.	Select from the dropdown box to define the size of Tunnel TCP MSS. Select Auto, and all devices will adjust this parameter automatically. Select Manual, and enter an expected value for Tunnel TCP MSS. Value Range: 64 - 1500 bytes.
Encapsulation Protocol	Mandatory field. Default setting: ESP.	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.
IKE Version	Mandatory field. Default setting: v1.	Enter the IKE version for this IPSec tunnel. Select v1 or v2.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.



The screenshot shows a configuration window with a title bar and a close button. It contains three main sections: 'Local Subnet List', 'Remote Subnet List', and 'Remote Gateway'. Each section has a table with columns for ID, Subnet IP Address, Subnet Mask, and Actions. The 'Local Subnet List' table has one entry with ID 1, Subnet IP Address 192.168.123.0, and Subnet Mask 255.255.255.0. The 'Remote Subnet List' table has one entry with ID 1, Subnet IP Address, and Subnet Mask 255.255.255.0. The 'Remote Gateway' section has a text input field and a label '(IP Address/FQDN)'.

Local & Remote Configuration Window		
Item	Value setting	Description
Local Subnet List	Mandatory field.	Enter the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet.

		<p>Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available.</p> <p>Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available.</p> <p>Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.</p>
Remote Subnet List	Mandatory field.	<p>Enter the Remote Subnet IP address and Subnet Mask.</p> <p>Click the Add or Delete button to add or delete Remote Subnet setting.</p>
Remote Device	<p>Mandatory field.</p> <p>Format can be a ipv4 address or FQDN.</p>	Enter the Remote Device.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.
Local Subnet List	Mandatory field.	<p>Enter the Local Subnet IP address and Subnet Mask.</p> <p>Click the Add or Delete button to add or delete a Local Subnet.</p> <p>Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available.</p> <p>Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available.</p> <p>Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.</p>
Remote Subnet List	Mandatory field.	<p>Enter the Remote Subnet IP address and Subnet Mask.</p> <p>Click the Add or Delete button to add or delete Remote Subnet setting.</p>
Remote Device	<p>Mandatory field.</p> <p>Format can be a ipv4 address or FQDN.</p>	Enter the Remote Device.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.



Authentication Configuration Window

Item	Value setting	Description
Key Management	Mandatory field. Pre-shared Key, 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. IKE+Pre-shared Key: User needs to set a key (8 - 32 characters). IKE+X.509: User needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and User Rule > Certificate in web-based utility.
Local ID	Optional field	Enter the Local ID for this IPSec tunnel to authenticate. Select Username for Local ID and enter the username. The username may include but can't be all numbers . Select FQDN for Local ID and enter the FQDN. Select user @FQDN for Local ID and enter the user @FQDN. Select Key ID for Local ID and enter the Key ID (English alphabet or number).
Remote ID	Optional field	Enter the Remote ID for this IPSec tunnel to authenticate. Select username for Remote ID and enter the username. The username may include but can't be all numbers . Select FQDN for Local ID and enter the FQDN. Select user@FQDN for Remote ID and enter the user@FQDN. Select Key ID for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

IPSec Phase Window		
Item	Value setting	Description
Phase1 Key Life Time	Mandatory field. Default value : 28800s.	Enter the Phase2 Key Lifetime in second. Value Range: 30 - 86400.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

1

AES-128 ▼

SHA1 ▼

Group 2 ▼

Enable

2

AES-128 ▼

MD5 ▼

Group 2 ▼

Enable

3

DES ▼

SHA1 ▼

Group 2 ▼

Enable

4

AES-128 ▼

SHA1 ▼

Group 2 ▼

Enable

IPSec Phase

Item

Setting

► Phase2 Key Life Time

28800

(seconds) (Max: 86400)

IPSec Proposal Definition

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

Save

IPSec Proposal Definition Window		
Item	Value setting	Description
IPSec Proposal Definition	Mandatory field.	Enter the Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256. Note: None is available when Encapsulation Protocol is set as AH.
		Enter the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Note: None and SHA2-256 are available only when Encapsulation Protocol is set as ESP; they are not available for AH Encapsulation.
		Enter the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18.
		Click Enable to enable this setting.
Save	Button.	Click Save to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.1.2 OpenVPN

Navigate to the Security > VPN > OpenVPN tab.

There are two OpenVPN connection scenarios. They are the TAP and TUN scenarios. The product can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the MG400 as a Server or Client, you need to enter which type of OpenVPN connection scenario is to be adopted.

OpenVPN TUN Scenario

The term "TUN" mode is referred to routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers.

OpenVPN TAP Scenario

The term "TAP" is referred to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access to the resources in LAN. If you want to offer remote access to the entire remote LAN for VPN client(s), you need to **setup OpenVPN in "TAP" bridge mode.**

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

OpenVPN can be enabled in Configuration window, and select an expected configuration, either server or client, for the MG400 to operate.

Configuration ^

Item	Setting
▶ OpenVPN	<input checked="" type="checkbox"/> Enable
▶ Server / Client	Server ▼

Configuration		
Item	Value setting	Description
OpenVPN	Disabled by default.	Check the Enable box to activate the OpenVPN function.
Server/ Client	Default setting: Server Configuration.	When Server is selected, as the name indicated, server configuration will be displayed below for further setup. When Client is selected, you can enter the client settings in another client configuration window.

If **Server** is selected, an OpenVPN Server Configuration window will appear. OpenVPN Server Configuration window allows you to enable the OpenVPN server function. The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.

OpenVPN Server Configuration

Item	Setting
▶ OpenVPN Server	<input type="checkbox"/> Enable
▶ Protocol	TCP ▼
▶ Port	4430
▶ Tunnel Scenario	TUN ▼
▶ Authorization Mode	TLS ▼ CA Cert.: ▼ Server Cert.: ▼ Please set the Certificate.
▶ Server Virtual IP	10.8.0.0
▶ DHCP-Proxy Mode	<input checked="" type="checkbox"/> Enable
▶ IP Pool	Starting Address: ~ Ending Address:
▶ Gateway	
▶ Netmask	255.255.255.0(/24) ▼
▶ Redirect Default Gateway	<input type="checkbox"/> Enable
▶ Encryption Cipher	Blowfish ▼
▶ Hash Algorithm	SHA-1 ▼
▶ LZO Compression	Adaptive ▼
▶ Persist Key	<input checked="" type="checkbox"/> Enable
▶ Persist Tun	<input checked="" type="checkbox"/> Enable
▶ Advanced Configuration	Edit

Save Undo

OpenVPN Server Configuration

Item	Value setting	Description
OpenVPN Server	Disabled by default.	Click the Enable to activate OpenVPN Server functions.
Protocol	Mandatory field.	Define the selected Protocol for connecting to the OpenVPN Server.

	Default setting: TCP.	<ul style="list-style-type: none"> • 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.
Port	Mandatory field. Default setting: 4430.	Enter the Port for connecting to the OpenVPN Server. Value Range: 1 - 65535.
Tunnel Scenario	Mandatory field. Default setting: TUN.	Enter the type of Tunnel Scenario for connecting to the OpenVPN Server. It can be TUN for TUN tunnel scenario or TAP for TAP tunnel scenario.
Authorization Mode	Mandatory field. Default setting: TLS.	Enter the authorization mode for the OpenVPN Server. <ul style="list-style-type: none"> • TLS ->The OpenVPN will use TLS authorization mode, and the following items CA Cert., Server Cert. and DH PEM will be displayed. CA Cert. could be generated in Certificate. Refer to User Rule > Certificate > Trusted Certificate. Server Cert. could be generated in Certificate. Refer to User Rule > Certificate > My Certificate. • Static Key ->The OpenVPN will use static key (pre-shared) authorization mode, and the following items Local Endpoint IP Address, Remote Endpoint IP Address and Static Key will be displayed. Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.
Local Endpoint IP Address	Mandatory field.	Enter the virtual Local Endpoint IP Address of this OpenVPN device. Value Range: The IP format is 10.8.0.x, the range of x is 1-254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	Mandatory field.	Enter the virtual Remote Endpoint IP Address of the peer OpenVPN device. Value Range: The IP format is 10.8.0.x, the range of x is 1-254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	Mandatory field.	Enter the Static Key . Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	Mandatory field.	Enter the Server Virtual IP . Value Range: The IP format is 10.y.0.0, the range of y is 1-254. Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.
DHCP-Proxy Mode	Mandatory field. Enabled by default.	Check the Enable box to activate the DHCP-Proxy Mode . Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	Mandatory field.	Enter the virtual IP pool setting for the OpenVPN server. You need to enter the Starting Address and Ending Address as the IP address pool for the OpenVPN clients.

		Note: IP Pool will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Device	Mandatory field.	Enter the MG400 setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Note: Device will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Netmask	Default setting: select one.	Enter the Netmask setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Value Range: 255.255.255.0/24 (only support class C) Note_1: Netmask will be available when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled). Note_2: Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Device	Optional field. Disabled by default.	Check the Enable box to activate the Redirect Default Device function.
Encryption Cipher	Mandatory field. Default setting: Blowfish.	Enter the Encryption Cipher from the dropdown list. It can be Blowfish/AES-256/AES-192/AES-128/None .
Hash Algorithm	Default setting: SHA-1.	Enter the Hash Algorithm from the dropdown list. It can be SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable .
LZO Compression	Default setting: Adaptive.	Enter the LZO Compression scheme. It can be Adaptive/YES/NO/Default .
Persis Key	Optional field. Enabled by default.	Check the Enable box to activate the Persis Key function.
Persis Tun	Optional field. Enabled by default.	Check the Enable box to activate the Persis Tun function.
Advanced Configuration	System data.	Click the Edit button to enter the Advanced Configuration setting for the OpenVPN server. If the button is clicked, Advanced Configuration will be displayed below.
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the changes and return to last page.

When the Edit button in Advanced Configuration is clicked, an OpenVPN Server Advanced Configuration window will appear.

OpenVPN Server Advanced Configuration
×

Item	Setting
▶ TLS Cipher	None
▶ TLS Auth. Key	<input type="text"/> (Optional)
▶ Client to Client	<input checked="" type="checkbox"/> Enable
▶ Duplicate CN	<input checked="" type="checkbox"/> Enable
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	0
▶ Tunnel UDP MSS-Fix	<input type="checkbox"/> Enable
▶ CCD-Dir Default File	<input type="text"/>
▶ Client Connection Script	<input type="text"/>
▶ Additional Configuration	<input type="text"/>

Save
Undo

OpenVPN Server Advanced Configuration		
Item	Value setting	Description
TLS Cipher	Mandatory field. Default setting: TLS-RSA-WITH-AES128-SHA.	Enter the TLS Cipher from the dropdown list. It can be None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA . Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	Optional field. String format: any text.	Enter the TLS Auth. Key. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Client to Client	Enabled by default.	Check the Enable box to enable the traffics among different OpenVPN Clients. Note: Client to Client will be available only when TLS is chosen in Authorization Mode
Duplicate CN	Enabled by default.	Check the Enable box to activate the Duplicate CN function. Note: Duplicate CN will be available only when TLS is chosen in Authorization Mode
Tunnel MTU	Mandatory field. Default setting: 1500.	Enter the Tunnel MTU. Value Range: 0 - 1500.

Tunnel UDP Fragment	Mandatory field. Default setting: 1500.	Enter the Tunnel UDP Fragment. By default, it is equal to Tunnel MTU . Value Range: 0 - 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	Optional field. Disabled by default.	Check the Enable box to activate the Tunnel UDP MSS-Fix Function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	Optional field. String format: any text.	Enter the CCD-Dir Default File. Value Range: 0 - 256 characters.
Client Connection Script	Optional field. String format: any text.	Enter the Client Connection Script. Value Range: 0 - 256 characters.
Additional Configuration	Optional field. String format: any text.	Enter the Additional Configuration. Value Range: 0 - 256 characters.

If **Client** is selected, the configuration window will be changed as below. The **OpenVPN Client List** window appear.

Configuration

Item	Setting
▶ OpenVPN	<input checked="" type="checkbox"/> Enable
▶ Server / Client	Client ▼
▶ OpenVPN Configuration file	<input type="checkbox"/> Enable <button>Upgrade</button>

OpenVPN Configuration		
Item	Value setting	Description
OpenVPN Configuration file	Optional field. Disabled by default.	Click the Enable box to activate the OpenVPN Client configuration via a pre-defined configuration file. You need to further click the Upgrade button to upload the configuration from a .ovpn file. If you enabled this function, you can't add any OpenVPN clients manually.

OpenVPN Client List
Add
Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	HAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions
<div> Save Undo </div>														

When Add button is clicked, OpenVPN Client Configuration window will pop up. It allows you to enter the required parameters for setting up an OpenVPN VPN client.

OpenVPN Client Configuration

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

Save

OpenVPN Client Configuration

Item	Value setting	Description
OpenVPN Client Name	Mandatory field.	The OpenVPN Client Name will be used to identify the client in the tunnel list. Value Range: 1 - 32 characters.
Interface	Mandatory field. Default setting: WAN-1.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	Mandatory field. Default setting: TCP.	Define the Protocol for the OpenVPN Client. <ul style="list-style-type: none"> • Select TCP ->The OpenVPN will use TCP protocol, and Port will be set as 443 automatically. • Select UDP -> The OpenVPN will use UDP protocol, and Port will be set as 1194 automatically.

Port	Mandatory field. Default setting: 443.	Enter the Port for the OpenVPN Client to use. Value Range: 1 - 65535.
Tunnel Scenario	Mandatory field. Default setting: TUN.	Enter the type of Tunnel Scenario for the OpenVPN Client to use. It can be TUN for TUN tunnel scenario or TAP for TAP tunnel scenario.
Remote IP/FQDN	Mandatory field.	Enter the Remote IP/FQDN of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	Optional field. Disabled by default.	Check the Enable box to activate remote subnet function and enter 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	Optional field. Disabled by default.	Check the Enable box to activate the Redirect Internet Traffic function.
NAT	Optional field. Enabled by default.	Check the Enable box to activate the NAT function.
Authorization Mode	Mandatory field. Default setting: TLS.	Enter the authorization mode for the OpenVPN Server. <ul style="list-style-type: none"> • TLS ->The OpenVPN will use TLS authorization mode, and the following items CA Cert., Client Cert. and Client Key will be displayed. CA Cert. could be selected in Trusted CA Certificate List. Refer to User Rule > Certificate > Trusted Certificate. Client Cert. could be selected in Local Certificate List. Refer to User Rule > Certificate > My Certificate. Client Key could be selected in Trusted Client key List. Refer to User Rule > Certificate > Trusted Certificate. • Static Key ->The OpenVPN will use static key authorization mode, and the following items Local Endpoint IP Address, Remote Endpoint IP Address and Static Key will be displayed.
Local Endpoint IP Address	Mandatory field.	Enter the virtual Local Endpoint IP Address of this OpenVPN device. Value Range: The IP format is 10.8.0.x, the range of x is 1-254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	Mandatory field.	Enter the virtual Remote Endpoint IP Address of the peer OpenVPN device. Value Range: The IP format is 10.8.0.x, the range of x is 1-254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	Mandatory field.	Enter the Static Key . Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	Default setting: Blowfish.	Enter the Encryption Cipher. It can be Blowfish/AES-256/AES-192/AES-128/None .
Hash Algorithm	Default setting: SHA-1.	Enter the Hash Algorithm. It can be SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable .

When Edit button in Advanced Configuration is clicked, an OpenVPN Client Configuration window will appear.

208 of 335
©2019 BEAM

OpenVPN Advanced Client Configuration

Item	Value setting	Description
TLS Cipher	Mandatory field. TLS-RSA-WITH-AES128-SHA is selected by default.	Enter the TLS Cipher from the dropdown list. It can be None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA . Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	Optional field. String format: any text.	Enter the TLS Auth. Key for connecting to an OpenVPN server, if the server required it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	Optional field.	Enter the user account for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Password	Optional field.	Enter the Password for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Bridge TAP to	Default setting: VLAN 1.	Enter the setting of "Bridge TAP to" to bridge the TAP interface to a certain local network interface or VLAN. Note: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
Firewall Protection	Disabled by default.	Check the box to activate the Firewall Protection function. Note: Firewall Protection will be available only when NAT is enabled.
Client IP Address	Default setting: Dynamic IP.	Enter the virtual IP Address for the OpenVPN Client. It can be Dynamic IP/ Static IP .
Tunnel MTU	Mandatory field. Default setting: 1500.	Enter the value of Tunnel MTU. Value Range: 0 - 1500.
Tunnel UDP Fragment	Default setting: 1500.	Enter the value of Tunnel UDP Fragment. Value Range: 0 - 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	Disabled by default.	Check the Enable box to activate the Tunnel UDP MSS-Fix function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	Disabled by default.	Check the Enable box to activate the nsCerType Verification function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	Default setting: 3600.	Enter the time interval of TLS Renegotiation Time. Value Range: -1 - 86400.
Connection	Default setting: -1.	Enter the time interval of Connection Retry. The default -1 means that it is no need to execute connection retry.

Retry(seconds)		Value Range: -1 - 86400, and -1 means no retry is required.
DNS	Default setting: Automatically.	Enter the setting of DNS. It can be Automatically/ Manually .
Additional Configuration	Optional field.	Enter optional configuration string here. Up to 256 characters is allowable. Value Range: 0 - 256characters.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.1.3 L2TP

Navigate to the Security > VPN > L2TP tab.

Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. The MG400 can behave as a L2TP server and a L2TP client both at the same time.

L2TP Server: **Static IP or FQDN for clients are needed to create L2TP tunnels.**

L2TP Client: This is for devices in remote offices with Dynamic IP.

The **Configuration** window allows the users to enable L2TP.

Configuration	
Item	Setting
▶ L2TP	<input checked="" type="checkbox"/> Enable
▶ Client/Server	Server ▼

Enable L2TP Window		
Item	Value setting	Description
L2TP	Disabled by default.	Click the Enable box to activate L2TP function.
Client/Server	Mandatory field.	Enter the role of L2TP. Select Server or Client role your device will take. Below are the configuration windows for L2TP Server and for L2TP Client.

When Server is selected, the L2TP server Configuration window will appear.

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<input checked="" type="checkbox"/> Enable
▶ Interface	All WANs ▼
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text"/> (Min. 1 characters)
▶ Server Virtual IP	192.168.10.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	17
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▼
▶ Service Port	1701

L2TP Server Configuration		
Item	Value setting	Description
L2TP Server	Disabled by default.	When click the Enable box. It will active L2TP server.
Interface	Mandatory field. Default setting: All WANs.	Select the interface on which L2TP tunnel is to be established. It can be the available WAN interfaces.
L2TP over IPSec	Disabled by default.	When click the Enable box. It will enable L2TP over IPSec and need to fill in the Pre-shared Key (8-32 characters).
Server Virtual IP	Mandatory field.	Enter the L2TP server Virtual IP. It will set as this L2TP server local virtual IP.
IP Pool Starting Address	Mandatory field. Default setting: 10.	Enter the L2TP server starting IP of virtual IP pool. It will set as the starting IP which assign to L2TP client. Value Range: 1 - 254.
IP Pool Ending Address	Mandatory field. Default setting: 17.	Enter the L2TP server ending IP of virtual IP pool. It will set as the ending IP which assign to L2TP client. Value Range: \geq Starting Address, and $<$ (Starting Address + 8) or 254.
Authentication Protocol	Mandatory field.	Select single or multiple Authentication Protocols for the L2TP server with which to authenticate L2TP clients. Available authentication protocols are PAP / CHAP / MS-CHAP / MS-CHAP v2.
MPPE Encryption	Mandatory field.	Enter whether to support MPPE Protocol. Click the Enable box to enable MPPE and from dropdown box to select 40 bits / 56 bits / 128 bits. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP / CHAP options will not be available.
Service Port	Mandatory field.	Enter the Service Port which L2TP server use. Value Range: 1 - 65535.

L2TP Server Status
Refresh

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

L2TP Server Status		
Item	Value setting	Description
L2TP Server Status	System data.	Displays the Username, Remote IP, Remote Virtual IP, and Remote Call ID of the connected L2TP clients. Click the Refresh button to renew the L2TP client information.

User accounts can be added via the **User Account List** window.

User Account List
Add
Delete

ID	User Name	Password	Enable	Actions
Save Undo				

User Account List Window		
Item	Value setting	Description
User Account List	Maximum of 10 user accounts.	This is the L2TP authentication user account entry. You can create and add accounts for remote clients to establish L2TP VPN connection to the MG400. Click Add button to add user account. Enter Username and password. Then check the enable box to enable the user. Click Save button to save new user account. The selected user account can permanently be deleted by clicking the Delete button. Value Range: 1 - 32 characters.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

When add is clicked, User Name, Password can be typed in into the **User Account Configuration** window.

User Account Configuration

User Name	Password	Account
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable
Save		
Save Undo		

For Client mode, select Client in Client/Server.

Configuration ^

Item	Setting
L2TP	<input checked="" type="checkbox"/> Enable
Client/Server	Client ▾

When **Client** is selected, **L2TP Client Configuration** window will appear.

L2TP Client Configuration ^

Item	Setting
L2TP Client	<input checked="" type="checkbox"/> Enable

L2TP Client Configuration		
Item	Value setting	Description
L2TP Client	Disabled by default.	Check the Enable box to enable L2TP client role of the MG400.

L2TP Client can be added via following L2TP Client List & Status window.

L2TP Client List & Status

AddDeleteRefresh

^

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

SaveUndo

When Add/Edit button is applied, a series of configuration windows will appear. You can add up to 8 Clients.

L2TP Client Configuration

Item	Setting
▶ Tunnel Name	<input style="width: 100%;" type="text" value="L2TP #1"/>
▶ Interface	<input style="width: 100%;" type="text" value="WAN1"/>
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input style="width: 100px;" type="text"/> (Min. 1 characters)
▶ Remote LNS IP/FQDN	<input style="width: 100%;" type="text"/>
▶ MTU	<input style="width: 100%;" type="text" value="1500"/>
▶ Remote LNS Port	<input style="width: 100%;" type="text" value="1701"/>
▶ User Name	<input style="width: 100%;" type="text" value="admin"/>
▶ Password	<input style="width: 100%;" type="password" value="*****"/>
▶ Tunneling Password (Optional)	<input style="width: 100%;" type="password"/>
▶ Remote Subnet	<input style="width: 100%;" type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ NAT before Tunneling	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input style="width: 50px;" type="text" value="Auto"/> <div style="display: flex; align-items: center;"> Interval <input style="width: 50px;" type="text" value="30"/> seconds Max. Failure Time <input style="width: 50px;" type="text" value="6"/> times </div>
▶ Service Port	<input style="width: 50px;" type="text" value="Auto"/> <input style="width: 50px;" type="text" value="0"/>
▶ Tunnel	<input type="checkbox"/> Enable

L2TP Client Configuration		
Item	Value setting	Description
Tunnel Name	Mandatory field.	Enter the tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 32 characters.
Interface	Mandatory field.	Define the selected interface to be the used for this L2TP tunnel (WAN-1 is available only when WAN-1 interface is enabled). The same applies to other WAN interfaces (e.g. WAN-2).
L2TP over IPSec	Disabled by default.	Check the Enable box to activate L2TP over IPSec, and further enter a Pre-shared Key (8-32 characters).
Remote LNS IP/FQDN	Mandatory field.	Enter the public IP address or the FQDN of the L2TP server.
MTU	Mandatory field. Default setting: 1500.	Enter the MTU. Value Range: 0 - 1500.
Remote LNS Port	Mandatory field.	Enter the Remote LNS Port for this L2TP tunnel.

	Default setting: 1701.	Value Range: 1 - 65535.
User Name	Mandatory field.	Enter the User Name for this L2TP tunnel to be authenticated when connect to L2TP server. Value Range: 1 - 32 characters.
Password	Mandatory field.	Enter the Password for this L2TP tunnel to be authenticated when connect to L2TP server.
Tunneling Password (Optional)	Optional Setting.	Enter the Tunneling Password for this L2TP tunnel to authenticate.
Remote Subnet	Mandatory field.	Enter the remote subnet for this L2TP tunnel to reach L2TP server. The Remote Subnet format need to be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of L2TP VPN server. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security device at L2TP client peer. If you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default device setting for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peer, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flow of any packets from the L2TP client peer. Certainly, those packets come through the L2TP VPN tunnel.
Authentication Protocol	Mandatory field. Disabled by default.	Enter one ore multiple Authentication Protocol for this L2TP tunnel. Available authentication methods are PAP / CHAP / MS-CHAP / MS-CHAP v2.
MPPE Encryption	Disabled by default. Optional field.	Enter whether L2TP server supports MPPE Protocol. Click the Enable box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP / CHAP options will not be available.
NAT before Tunneling	Mandatory field. Disabled by default.	Enter whether NAT is required or not for this L2TP tunnel.
LCP Echo Type	Default setting: Auto.	Enter the LCP Echo Type for this L2TP tunnel. It can be Auto, User-defined, or Disable. Auto: the system sets the Interval and Max. Failure Time. User-defined: enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. Disable: disable the LCP Echo. Value Range: 1 - 99999 for Interval Time, 1-999 for Failure Time.
Service Port	Mandatory field.	Enter the Service Port for this L2TP tunnel to use. It can be Auto, (1701) for Cisco), or User-defined. Auto: The system determines the service port. 1701 (for Cisco): The system use port 1701 for connecting with CISCO L2TP Server. User-defined: Enter the service port. The default value is 0. Value Range: 0 - 65535.

6.1.4 PPTP

Navigate to the Security > VPN > PPTP tab.

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

PPTP Server: **Static IP or FQDN is required for clients to create PPTP tunnels.**

PPTP Client: Suitable for devices with dynamic IP.

Navigate to Security > VPN > PPTP tab.

The Configuration window allows you to create and configure PPTP tunnels.

Configuration	
Item	Setting
PPTP	<input checked="" type="checkbox"/> Enable
Client/Server	Server ▼

Enable PPTP Window		
Item	Value setting	Description
PPTP	Disabled by default.	Click the Enable box to activate PPTP function.
Client/Server	Mandatory field.	Enter the role of PPTP. Select Server or Client role your device will take. Below are the configuration windows for PPTP Server and for Client.

When Server in the Client/Server field is selected, the PPTP server configuration window will appear.

PPTP Server Configuration	
Item	Setting
PPTP Server	<input checked="" type="checkbox"/> Enable
Interface	All WANs ▼
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▼

PPTP Server Configuration Window		
Item	Value setting	Description
PPTP Server	Unchecked by default.	Check the Enable box to enable PPTP server role of the MG400.
Interface	Mandatory field. Default setting: All WANs.	Select the interface on which PPTP tunnel is to be established. It can be the available WAN interfaces.
Server Virtual IP	Mandatory field. Default setting: 192.168.0.1	Enter the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	Mandatory field. Default value is 10.	This is the PPTP server's Virtual IP DHCP server. You can enter the first IP address for the subnet from which the PPTP client's IP address will be assigned. Value Range: 1 - 254.
IP Pool Ending Address	Mandatory field. Default value is 17.	This is the PPTP server's Virtual IP DHCP server. You can enter the last IP address for the subnet from which the PPTP client's IP address will be assigned. Value Range: >= Starting Address, and < (Starting Address + 8) or 254.
Authentication Protocol	Mandatory field. Disabled by default.	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols are PAP / CHAP / MS-CHAP / MS-CHAP v2.
MPPE Encryption	Mandatory field. Disabled by default.	Enter whether to support MPPE Protocol. Click the Enable box to enable MPPE and from dropdown box to select 40 bits / 56 bits / 128 bits. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP / CHAP options will not be available.

The **PPTP Server Status** window shows username, remote IP, and other info of the PPTP connection.

PPTP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

PPTP Server Status Window		
Item	Value setting	Description
PPTP Server Status	System data.	Displays the Username, Remote IP, Remote Virtual IP, and Remote Call ID of the connected PPTP clients. Click the Refresh button to renew the PPTP client information.

User Account List window allows you to add user accounts.

User Account List Add Delete				
ID	User Name	Password	Enable	Actions
Save Undo				

User Account List Window		
Item	Value setting	Description
User Account List	Maximum of 10 accounts	<p>This is the PPTP authentication user account entry. You can create and add accounts for remote clients to establish PPTP VPN connection to the MG400. Click Add button to add your account. Enter Username and password. Then check the enable box to enable the user.</p> <p>Click Save button to save new user account.</p> <p>The selected user account can permanently be deleted by clicking the Delete button.</p> <p>Value Range: 1 - 32 characters.</p>

User Name, Password and Account enabling can be configure in **User Account Configuration** window.

User Account Configuration

User Name	Password	Account
<input type="text"/>	<input type="password"/>	<input type="checkbox"/> Enable
<input type="button" value="Save"/>		
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

When Client is selected in Client/Server, a series of PPTP Client Configuration windows will appear.

Configuration

Item	Setting
► PPTP	<input checked="" type="checkbox"/> Enable
► Client/Server	<input type="button" value="Client"/> ▼

PPTP Configuration		
Item	Value setting	Description
PPTP	Disabled by default.	Check the Enable box to enable PPTP.
Client/Server	Client or Server.	Select Client or Server mode.

Create/Edit PPTP Client

PPTP Client Configuration

Item	Setting
► PPTP Client	<input checked="" type="checkbox"/> Enable

PPTP Client Configuration		
Item	Value setting	Description
PPTP Client	Disabled by default.	Check the Enable box to enable PPTP client role of the MG400.

PPTP Client can be added in PPTP Client List & Status window.

PPTP Client List & Status

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>								

When Add/Edit button is applied, a series PPTP Client Configuration will appear.

PPTP Client Configuration

Item	Setting
Tunnel Name	<input type="text" value="PPTP #1"/>
Interface	<input type="text" value="WAN1"/>
Remote IP/FQDN	<input type="text"/>
MTU	<input type="text" value="1500"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="****"/>
Remote Subnet	<input type="text"/>
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable
NAT before Tunneling	<input type="checkbox"/> Enable
LCP Echo Type	<input type="text" value="Auto"/>
	Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
Tunnel	<input type="checkbox"/> Enable

PPTP Client Configuration Window

Item	Value setting	Description
Tunnel Name	Mandatory field.	Enter the tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 32 characters.
Interface	Mandatory field. Default setting: WAN1.	Define the selected interface to be the used for this PPTP tunnel (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. WAN-2).
Remote IP/FQDN	Mandatory field. Format can be an IPv4 address or FQDN.	Enter the public IP address or the FQDN of the PPTP server.
MTU	Mandatory field.	Enter the MTU.

	Default setting: 1500.	Value Range: 0 - 1500.
User Name	Mandatory field.	Enter the User Name for this PPTP tunnel to be authenticated when connect to PPTP server. Value Range: 1 - 32 characters.
Password	Mandatory field.	Enter the Password for this PPTP tunnel to be authenticated when connect to PPTP server.
Remote Subnet	Mandatory field.	<p>Enter the remote subnet for this PPTP tunnel to reach PPTP server. The Remote Subnet format need to be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security device at PPTP client peer.</p> <p>If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default device setting for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flow of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel.</p>
Authentication Protocol	Mandatory field. Disabled by default.	Enter one ore multiple Authentication Protocol for this PPTP tunnel. Available authentication methods are PAP / CHAP / MS-CHAP / MS-CHAP v2.
MPPE Encryption	Optional field. Disabled by default.	Enter whether PPTP server supports MPPE Protocol. Click the Enable box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP / CHAP options will not be available.
NAT before Tunneling	Mandatory field. Disabled by default.	Enter whether NAT is required or not for this PPTP tunnel.
LCP Echo Type	Default setting: Auto.	<p>Enter the LCP Echo Type for this PPTP tunnel. It can be Auto, User-defined, or Disable.</p> <p>Auto: the system sets the Interval and Max. Failure Time.</p> <p>User-defined: enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times.</p> <p>Disable: disable the LCP Echo.</p> <p>Value Range: 1 - 99999 for Interval Time, 1-999 for Failure Time.</p>
Tunnel	Disabled by default.	Check the Enable box to enable this PPTP tunnel.
Save	Button.	Click Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.1.5 GRE

Navigate to the Security > VPN > GRE tab.

Generic Routing Encapsulation (GRE) is a tunnelling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

To setup a GRE tunnel, each peer needs to setup its global IP as tunnel IP and fill in the other's global IP as remote IP.

The Configuration window allows you to enable the GRE Tunnel.

Configuration	
Item	Setting
GRE Tunnel	<input checked="" type="checkbox"/> Enable
Max. Concurrent GRE Tunnels	32

Enable GRE Window

Item	Value setting	Description
GRE Tunnel	Disabled by default.	Click the Enable box to enable GRE function.
Max. Concurrent GRE Tunnels	System data.	The maximum number of simultaneous GRE tunnel connection is 32.

GRE Tunnel can be added in following **GRE Tunnel List** window.

GRE Tunnel List Add Delete										
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions
<div> Save Undo </div>										

When Add/Edit button is clicked, the GRE Rule Configuration window will pop up.

GRE Rule Configuration

Item	Setting
Tunnel Name	GRE #1
Interface	WAN1
Tunnel IP	IP: MASK: -- select one -- (Optional)
Remote IP	
MTU	
Key	(Optional)
TTL	
Remote Subnet	
Tunnel	<input type="checkbox"/> Enable

Save

GRE Rule Configuration Window		
Item	Value setting	Description
Tunnel Name	Mandatory field.	Enter a tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 9 characters.
Interface	Mandatory field. Default setting: WAN 1.	Select the interface on which GRE tunnel is to be established. It can be the available WAN and LAN interfaces.
Tunnel IP	Optional field.	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	Mandatory field.	Enter the Remote IP address of remote GRE tunnel device. Normally this is the public IP address of the remote GRE device.
MTU	Mandatory field. Default setting: Auto (value zero or blank).	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to Auto (value '0' or blank), the router selects the best MTU for best Internet connection performance. Value Range: 0 - 1500.
Key	Optional field.	Enter the Key for the GRE connection. Value Range: 0 - 9999999999.
TTL	Mandatory field.	Enter TTL hop-count value for this GRE tunnel. Value Range: 1 - 255.
Remote Subnet	Mandatory field.	Enter the remote subnet for this GRE tunnel. The Remote Subnet format need to be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of GRE server peer. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the security device at GRE client peer.

If you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default device setting for the GRE client peer, all packets, including the Internet accessing of GRE client peer, will go through the established GRE tunnel. That means the remote GRE server peer controls the flow of any packets from the GRE client peer. Certainly, those packets come through the GRE tunnel.		
Tunnel	Disabled by default.	Check Enable box to enable this GRE tunnel.
Save	Button.	Click Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.1.6 EoGRE

Navigate to the Security > VPN > EoGRE tab.

Ethernet over GRE (EoGRE) is a tunnel protocol that enables tunnelling of layer 2 packets encapsulated in a GRE header over IP core networks.

The Configuration window allows to enable EoGRE Tunnel.

Configuration		^
Item	Setting	
▶ EoGRE Tunnel	<input checked="" type="checkbox"/> Enable	
▶ Max. Concurrent EoGRE Tunnels	4	

Enable GRE Window		
Item	Value setting	Description
EoGRE Tunnel	Disabled by default.	Click the Enable box to enable EoGRE function.
Max. Concurrent EoGRE Tunnels	System data.	The maximum number of simultaneous EoGRE tunnel connections is 4.

EoGRE Tunnel can be added in EoGRE Tunnel List window.

EoGRE Tunnel List Add Delete ^									
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Enable	Actions
Save Undo									

When the Add button is clicked, following EoGRE Rule Configuration window will pop up.

EoGRE Rule Configuration

Item	Setting
▶ Tunnel Name	<input type="text" value="EoGRE #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Tunnel IP	IP: <input type="text"/> MASK: <input type="text" value="-- select one --"/> (Optional)
▶ Remote IP	<input type="text"/>
▶ MTU	<input type="text"/> (Optional)
▶ Key	<input type="text"/> (Optional)
▶ TTL	<input type="text"/> (Optional)
▶ Port-based VLAN ID Interface	<input type="text" value="None"/>
▶ Tunnel	<input type="checkbox"/> Enable

☐ TAG ID List

ID	TAG ID	MTU	VLAN ID Interface	Enable

EoGRE Rule Configuration Window		
Item	Value setting	Description
Tunnel Name	Mandatory field.	Enter a tunnel name. Enter a name that is easy for you to identify. Value Range: 1 - 8 characters.
Interface	Mandatory field. Default setting: WAN 1.	Select the interface on which EoGRE tunnel is to be established. It can be the available WAN interfaces.
Tunnel IP	Optional field.	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	Mandatory field.	Enter the Remote IP address of remote EoGRE tunnel device. Normally this is the public IP address of the remote EoGRE device.
MTU	Optional field.	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1 - 1500.
Key	Optional field.	Enter the Key for the EoGRE connection. Value Range: 0 - 4294967295.

TTL	Optional field.	Enter TTL hop-count value for this GRE tunnel. Value Range: 1 - 255.
Port-based VLAN ID Interface	Mandatory field. Default setting: None.	Select a Port-based VLAN ID for aggregating its traffic to the EoGRE tunnel. It can be None, or all available Port –based VLAN IDs. For creating the Port-based VLAN ID, refer to Network > LAN & VLAN > VLAN. If VLAN type is tag based VLAN, it will be grayed out. You can also aggregate tag based VLAN group to an EoGRE tunnel with entering additional TAG ID listing below.
Tunnel	Disabled by default.	Check Enable box to enable this EoGRE tunnel.
Save	Button.	Click Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

In addition, to aggregate Tag-based VLAN traffic to an EoGRE tunnel, you need to create a TAG ID List for the tunnel. Up to 40 TAG IDs can be defined for a tunnel, each TAG can be regard as a sub-tunnel.

When Add/Edit button is applied in following TAG ID List window, the TAG ID Configuration window will appear.

☐ TAG ID List

ID	TAG ID	MTU	VLAN ID Interface	Enable
TAG ID Configuration				
Item	Setting			
▶ TAG ID	<input type="text"/>			
▶ MTU	<input type="text"/> (Optional)			
▶ Tag-based VLAN ID Interface	<input type="text" value="None"/>			
▶ Enable	<input type="checkbox"/>			
<input type="button" value="Save"/>				
<input type="button" value="Save"/>				

TAG ID Configuration Window		
Item	Value setting	Description
TAG ID	Mandatory field.	Enter a Tag ID that is going to be bound to a specified Tag-based VLAN ID. Value Range: 1 - 4094.

MTU	Optional field.	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1 - 1500 and shouldn't be greater than that of the EoGRE Tunnel.
Tag-based VLAN ID Interface	Mandatory field. None is selected by default.	Select a Tag-based VLAN ID on which EoGRE tunnel is to be established. It can be None, or all available Tag –based VLAN IDs. If VLAN type is port based VLAN, it will be grayed out. For creating the Port-based VLAN ID, refer to Network > LAN & VLAN > VLAN.
Enable	Unchecked by default.	Check Enable box to enable this TAG rule.
Save	Button.	Click Save button to save the settings.

6.2 Firewall

The firewall menu includes Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and firewall options.

6.2.1 Packet Filter

Navigate to the Security > Firewall > Packet Filter tab.

"Packet Filter" function allows you to define some filtering rules for incoming and outgoing packets.

Packet Filters can be enabled in following Configuration Window.

Configuration	
Item	Setting
▶ Packet Filters	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	<input type="checkbox"/> Log Alert

Configuration Window		
Item	Value setting	Description
Packet Filter	Disabled by default.	Check the Enable box to activate Packet Filter function
Black List / White List	Deny those match the following rules is set by default.	When Deny those match the following rules is selected, as the name suggest, packets specified in the rules will be blocked - blacklisted. In contrast, with Allow those match the following rules, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	Disabled by default.	Check the Enable box to activate Event Log.

Packet Filter Rules can be added in Packet Filter List window. The MG400 supports up to a maximum of 20 filter rule sets.

Packet Filter List											
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable Actions
<div> <input type="button" value="Add"/> <input type="button" value="Delete"/> </div>											
<div> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="MAC Level"/> </div>											

When **Add** button is applied, **Packet Filter Rule Configuration** window will pop up.

Packet Filter Rule Configuration

Item	Setting
▶ Rule Name	<input style="width: 150px;" type="text" value="Rule1"/>
▶ From Interface	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any ▼</div>
▶ To Interface	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any ▼</div>
▶ Source IP	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any ▼</div>
▶ Destination IP	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any ▼</div>
▶ Source MAC	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any ▼</div>
▶ Protocol	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Any(0) ▼</div>
▶ Source Port	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">User-defined Service ▼</div> <div style="border: 1px solid #ccc; width: 40px; height: 15px; display: inline-block; margin: 0 5px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 15px; display: inline-block;"></div>
▶ Destination Port	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">User-defined Service ▼</div> <div style="border: 1px solid #ccc; width: 40px; height: 15px; display: inline-block; margin: 0 5px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 15px; display: inline-block;"></div>
▶ Time Schedule	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">(0) Always ▼</div>
▶ Rule	<input type="checkbox"/> Enable

Save

Packet Filter Rule Configuration		
Item	Value setting	Description
Rule Name	Enter text string. Mandatory field.	Enter a packet filter rule name. Enter a name that is easy for you to remember. Value Range: 1 - 30 characters.
From Interface	Mandatory field. Default setting: Any.	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. Or VLAN-1 to WAN then select VLAN-1 for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select Any to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.

To Interface	Mandatory field. Default setting: Any.	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. Or VLAN-1 to WAN then select WAN for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select Any to filter packets leaving the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
Source IP	Mandatory field. Default setting: Any.	This field is to enter the Source IP address. Select Any to filter packets coming from any IP addresses. Select Specific IP Address to filter packets coming from an IP address. Select IP Range to filter packets coming from a specified range of IP address. Select IP Address-based Group to filter packets coming from a pre-defined group. Note: group need to be pre-defined before this option become available. Refer to User Rule > Grouping > Host grouping. You may also access to create a group by the Add Rule shortcut button.
Destination IP	Mandatory field. Default setting: Any.	This field is to enter the Destination IP address. Select Any to filter packets that are entering to any IP addresses. Select Specific IP Address to filter packets entering to an IP address entered in this field. Select IP Range to filter packets entering to a specified range of IP address entered in this field. Select IP Address-based Group to filter packets entering to a pre-defined group selected. Note: group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host grouping. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting window.
Source MAC	Mandatory field. Default setting: Any.	This field is to enter the Source MAC address. Select Any to filter packets coming from any MAC addresses. Select Specific MAC Address to filter packets coming from a MAC address. Select MAC Address-based Group to filter packets coming from a pre-defined group selected. Note: group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host grouping. You may also access to create a group by the Add Rule shortcut button.
Protocol	Mandatory field. Default setting: Any (0).	For Protocol, select Any to filter any protocol packets Then for Source Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range. Then for Destination Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range. Value Range: 1 - 65535 for Source Port, Destination Port. For Protocol, select ICMPv4 to filter ICMPv4 packets For Protocol, select TCP to filter TCP packets

		<p>Then for Source Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range.</p> <p>Then for Destination Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range.</p> <p>Value Range: 1 - 65535 for Source Port, Destination Port.</p> <p>For Protocol, select UDP to filter UDP packets</p> <p>Then for Source Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range.</p> <p>Then for Destination Port, select a predefined port dropdown box when Well-known Service is selected, otherwise select User-defined Service and enter a port range.</p> <p>Value Range: 1 - 65535 for Source Port, Destination Port.</p> <p>For Protocol:</p> <p>select GRE to filter GRE packets.</p> <p>select ESP to filter ESP packets.</p> <p>select SCTP to filter SCTP packets.</p> <p>select User-defined to filter packets with specified port number. Then enter a port number in Protocol Number box.</p>
Time Schedule	Mandatory field.	<p>Apply Time Schedule to this rule, otherwise leave it as Always.</p> <p>If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.</p>
Rule	Disabled by default.	Click Enable box to activate this rule then save the settings.
Save	Button.	Click Save to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

When **MAC Level** button is clicked, the **Configuration** window for MAC Control and **MAC Control Rule List** window will appear.

Mac Control can be enabled in the following **Configuration** window.

Configuration

Item	Setting
▶ MAC Control	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input checked="" type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.123.148(WR-LT034) ▼ <button>Copy to</button>

MAC Control rule can be added in **MAC Control Rule List** window.

MAC Control Rule List
Add
Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
----	-----------	-------------	--------------------	--------	---------

When **Add** button is clicked, following **MAC Control Rule Configuration** window will appear.

MAC Control Rule Configuration
X

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always ▼	<input type="checkbox"/>

Save

6.2.2 URL Blocking

Navigate to the **Security > Firewall > URL Blocking** tab.

"URL Blocking" function allows you to define blocking or allowing rules for incoming and outgoing Web request packets. With defined rules, device can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords.

URL Blocking can be enabled in following Configuration window.

Configuration
^

Item	Setting
▶ URL Blocking	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	<input checked="" type="checkbox"/> Enable

Configuration		
Item	Value setting	Description
URL Blocking	Disabled by default.	Check the Enable box to activate URL Blocking function.
Black List / White List	Default setting: Deny those match the following rules.	Enter the URL Blocking Policy, either Blacklist or White List. Black List: When Deny those match the following rules is selected, as the name suggest, the matched Web request packets will be blocked. White List: When Allow those match the following rules is selected, the

URL Blocking Rule can be added in following **URL Blocking Rule List** window. The MG400 supports up to a maximum of 20 URL blocking rule sets.

When Add button is applied, the URL Blocking Rule Configuration window will pop up.

URL Blocking Rules Configuration		
Item	Value setting	Description
Rule Name	Enter text string. Mandatory field.	Enter an URL Blocking rule name. Enter a name that is easy for you to understand.

URL Blocking Rules Configuration		
Item	Value setting	Description
Source IP	Mandatory field. Default setting: Any.	<p>This field is to enter the Source IP address.</p> <ul style="list-style-type: none"> • 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. • Select IP Address-based Group to filter packets coming from a pre-defined group selected. Note: group need to be pre-defined before this option become available. Refer to User Rule > Grouping > Host grouping.
Source MAC	Mandatory field. Default setting: Any.	<p>This field is to enter the Source MAC address.</p> <ul style="list-style-type: none"> • Select Any to filter packets coming from any MAC addresses. • Select Specific MAC Address to filter packets coming from a MAC address entered in this field. • Select MAC Address-based Group to filter packets coming from a pre-defined group selected. Note: group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host grouping.
URL / Domain Name / Keyword	Mandatory field. Supports up to a maximum of 10 Keywords in a rule by using the delimiter “;”.	<p>Enter URL, Domain Name, or Keyword list for URL checking.</p> <ul style="list-style-type: none"> • In the Black List mode, if a matched rule is found, the packets will be dropped. • In the White List mode, if a matched rule is found, the packets will be accepted and the others which don't match any rule will be dropped.
Destination Port	Mandatory field. Default setting: Any.	<p>This field is to enter the Destination Port number.</p> <ul style="list-style-type: none"> • Select Any to filter packets going to any Port. • Select Specific Service Port to filter packets going to a specific Port entered in this field. • Select Port Range to filter packets going to a specific range of Ports entered in this field.
Time Schedule Rule	Mandatory field.	<p>Apply a specific Time Schedule to this rule; otherwise leave it as (0) Always.</p> <p>If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.</p>
Rule	Disabled by default.	Click the Enable box to activate this rule.
Save	Button.	Click the Save button to save the settings.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.2.3 Content Filter

Navigate to the **Security > Firewall > Content Filter** tab.

Content Filter can block HTML requests with some specific extension file names, like ".exe", ".bat" (applications), "mpeg" (video), and so on. It also blocks HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.

Configuration ^	
Item	Setting
▶ Content Filters	<input checked="" type="checkbox"/> Enable
▶ Popular File Extension List	<input checked="" type="checkbox"/> Cookie <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> ActiveX
▶ Log Alert	<input checked="" type="checkbox"/> Enable

Web Content Filters		
Item	Value setting	Description
Content Filter	Disabled by default.	Check the Enable box to activate this content filter function.
Popular File Extension List	Mandatory field.	Check the Cookie box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword "Cookie:" .
	Disabled by default.	Check the Java box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword "js" , ".class" , ".jar" , ".jsp" , ".java" , ".jse" , ".jcm" , ".jtk" , or ".jad" .
Log Alert	Disabled by default.	Check the ActiveX box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword ".ocx" , ".cab" , ".ole" , ".olb" , ".com" , ".vbs" , ".vrm" , or ".viv" .
		If one of the matching rules is found, the packets with http header will be dropped.
Log Alert	Disabled by default.	Check the Enable box to activate Event Log.

Content Filter Rule can be added in the following Content Filter List. The MG400 supports up to a maximum of 20 filter rule sets.

Content Filter List Add Delete ^						
ID	Rule Name	Source IP	Source MAC	User-defined File Extension List	Time Schedule	Enable Actions
<div> Save Undo </div>						

When Add button is clicked, Content Filter Configuration window will pop up.

Setting
✕

Content Filter Configuration

Item	Setting
▶ Rule Name	<input style="width: 100%;" type="text" value="Rule1"/>
▶ Source IP	<input style="width: 100%;" type="text" value="Any"/>
▶ Source MAC	<input style="width: 100%;" type="text" value="Any"/>
▶ User-defined File Extension List (Use ; to Concatenate)	<input style="width: 100%;" type="text"/>
▶ Time Schedule	<input style="width: 100%;" type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

Content Filter Configuration		
Item	Value setting	Description
Rule Name	Enter text string. Mandatory field.	Enter a content filter rule name that is easy for you to understand.
Source IP	Mandatory field. Default setting: Any.	<p>Enter the Source IP address to apply with the content filter rule. It can be Any, Specific IP Address, IP Range, or IP Address-based Group. 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.</p> <p>Select IP Range to filter packets coming from a specified range of IP address entered in this field.</p> <p>Select IP Address-based Group to filter packets coming from a pre-defined group selected.</p> <p>Note: Group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host Grouping Tab. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting window.</p>
Source MAC	Mandatory field. Default setting: Any.	<p>Enter the Source MAC address to apply with the content filter rule. Select Any to filter packets coming from any MAC addresses. Select Specific MAC Address to filter packets coming from a MAC address entered in this field.</p> <p>Select MAC Address-based Group to filter packets coming from a pre-defined group selected.</p>

		Note: Group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host Grouping Tab. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting window.
User-defined File Extension List (Use ; to Concatenate)	Mandatory field.	Enter file extension list for the content filter rule. It supports up to a maximum of 10 file extensions in a rule by using the delimiter ";" . If a matching rule is found, the packets with http header will be dropped.
Time Schedule	Mandatory field. Default setting: (0).	Apply Time Schedule to this rule, otherwise leave it as Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.
Rule	Disabled by default.	Click the Enable box to activate this rule.
Save	Button.	Click the Save button to save the configuration.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.2.4 MAC Control

Navigate to the Security > Firewall > MAC Control tab.

"MAC Control" function allows you to assign the MG400 accessibility based on client devices MAC addresses. When the you want to reject the traffic from some client devices with specific MAC addresses, he can make use of the Blacklist configuration.

The MAC control setting allows you to create and customizes MAC address policies to allow or reject packets with specific source MAC address.

Configuration

Item	Setting
▶ MAC Control	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input checked="" type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.123.148(WR-LT034) ▼ <button>Copy to</button>

Configuration Window		
Item	Value setting	Description
MAC Control	Disabled by default	Check the Enable box to activate the MAC filter function
Black List / White List	Default setting: Deny MAC Address Below.	When Deny MAC Address Below is selected, as the name suggest, packets specified in the rules will be blocked – blacklisted. In contrast, with Allow

		MAC Address Below, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	Disabled by default	Check the Enable box to activate to activate Event Log.
Known MAC from LAN PC List	System data.	Select a MAC Address from LAN Client List. Click the Copy to copy the selected MAC Address to the filter rule.

MAC Control Rules can be added in MAC Control Rule List. The MG400 supports up to a maximum of 20 filter rule sets.

☐ **MAC Control Rule List**

^

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
----	-----------	-------------	--------------------	--------	---------

When **Add** button is applied, **Filter Rule Configuration** window will appear.

MAC Control Rule Configuration
×

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	<input type="text" value="(0) Always"/> ▼	<input type="checkbox"/>

MAC Control Rule Configuration		
Item	Value setting	Description
Rule Name	Enter text string. Mandatory field.	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	MAC Address string Format. Mandatory field.	Enter the Source MAC Address to filter rule.
Time Schedule	Mandatory field.	Apply Time Schedule to this rule; otherwise leave it as (0) Always. If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab
Enable	Disabled by default.	Click Enable box to activate this rule, and then save the settings.
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the settings.

6.2.5 Application Filter


Navigate to the Security > Firewall > Application Filter tab.

Application Filter function can allow or deny the passing of Internet protocol packets. It supports the application filters for various Internet chat software, P2P download, Proxy, and video streaming.


Configuration ^	
Item	Setting
▶ Application Filter	<input checked="" type="checkbox"/> Enable
▶ Log Alert	<input checked="" type="checkbox"/> Enable

Application Filters		
Item	Value setting	Description
Application Filter	Disabled by default.	Check the Enable box to activate this application filter function.
Log Alert	Disabled by default.	Check the Enable box to activate Event Log.

Application Filter Rules can be added in the Application filter List. The MG400 supports up to a maximum of 20 filter rule sets.

<div>  Application Filter List <input type="button" value="Add"/> <input type="button" value="Delete"/> ⬆ </div>						
Rule Name	Source IP	Source MAC	Application	Time Schedule	Enable	Actions

When Add button is applied, Filter Rule Configuration window will appear.



Application Filter Rule Configuration

Item	Setting
▶ Rule Name	<input type="text" value="Rule1"/>
▶ Source IP	<input type="text" value="Any"/>
▶ Source MAC	<input type="text" value="Any"/>
▶ Chat Software	<input type="checkbox"/> QQ <input type="checkbox"/> Skype <input type="checkbox"/> Aliww <input type="checkbox"/> Line
▶ P2P Software	<input type="checkbox"/> BT(BitTorrent, BitSpirit, BitComet) <input type="checkbox"/> HTTP Multiple Thread Download
▶ Streaming	<input type="checkbox"/> MMS <input type="checkbox"/> RTSP
▶ Time Schedule	<input type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

Application Filter Rule Configuration		
Item	Value setting	Description
Rule Name	Enter text string. Mandatory field.	Enter an application filter rule name that is easy for you to understand.
Source IP	Mandatory field. Default setting: Any.	<p>Enter the Source IP address to apply with the application filter rule. It can be Any, Specific IP Address, IP Range, or IP Address-based Group. 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.</p> <p>Select IP Range to filter packets coming from a specified range of IP address entered in this field.</p> <p>Select IP Address-based Group to filter packets coming from a pre-defined group selected.</p> <p>Note: Group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host Grouping Tab. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting window.</p>
Source MAC	Mandatory field. Default setting: Any.	<p>Enter the Source MAC address to apply with the application filter rule. Select Any to filter packets coming from any MAC addresses. Select Specific MAC Address to filter packets coming from a MAC address entered in this field.</p> <p>Select MAC Address-based Group to filter packets coming from a pre-defined group selected.</p> <p>Note: Group need to be pre-defined before this selection become available. Refer to User Rule > Grouping > Host Grouping Tab. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting window.</p>
Chat Software	All boxes are unchecked by default.	Check the box(es) to activate the application filter function you want on this rule.
P2P Software	All boxes are unchecked by default.	<p>Check the box(es) to activate the application filter function you want on this rule.</p> <p>The available P2P applications include BT, and HTTP Multiple Thread Download.</p>
Streaming	All boxes are unchecked by default.	<p>Check the box(es) to activate the application filter function you want on this rule.</p> <p>The available streaming applications include MMS, and RTSP.</p>
Time Schedule	Mandatory field. Default setting: (0) Always.	<p>Apply Time Schedule to this rule; otherwise leave it as (0) Always.</p> <p>If the dropdown list is empty, ensure Time Schedule is pre-configured. Refer to User Rule > Scheduling > Configuration tab.</p>
Rule	Disabled by default.	Click the Enable box to activate this rule.
Save	Button.	Click the Save button to save the configuration.
Back	Button.	When the X button is clicked, the window will return to the Application Filter Configuration page.

6.2.6 IPS

Navigate to the Security > Firewall > Application Filter tab.

Intrusion Prevention System (IPS) is network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it. You can enable the IPS function and check the listed intrusion activities when needed. You can also enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.

Configuration		^
Item	Setting	
► IPS	<input checked="" type="checkbox"/> Enable	
► Log Alert	<input checked="" type="checkbox"/> Enable	

Configuration Window		
Item	Value setting	Description
IPS	Disabled by default.	Check the Enable box to activate IPS function.
Log Alert	Disabled by default.	Check the Enable box to activate to activate Event Log.

The **Intrusion Prevention** window allows you to enable intrusion prevention rules.

Intrusion Prevention



Item	Setting		
▶ SYN Flood Defense	<input type="checkbox"/> Enable	<input type="text" value="300"/>	Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable	<input type="text" value="300"/>	Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable	<input type="text" value="300"/>	Packets/second (10~10000)
▶ Port Scan Defense	<input type="checkbox"/> Enable	<input type="text" value="200"/>	Packets/second (10~10000)
▶ Block Land Attack	<input type="checkbox"/> Enable		
▶ Block Ping of Death	<input type="checkbox"/> Enable		
▶ Block IP Spoof	<input type="checkbox"/> Enable		
▶ Block TCP Flag Scan	<input type="checkbox"/> Enable		
▶ Block Smurf	<input type="checkbox"/> Enable		
▶ Block Traceroute	<input type="checkbox"/> Enable		
▶ Block Fraggle Attack	<input type="checkbox"/> Enable		
▶ ARP Spoofing Defense	<input type="checkbox"/> Enable	<input type="text" value="300"/>	Packets/second (10~10000)
<div>Save Undo</div>			

Setup Intrusion Prevention Rules

Item	Value setting	Description
SYN Flood Defense	Mandatory field. Disabled by default. Traffic threshold, default setting: 300.	Click Enable box to activate this intrusion prevention rule and enter the traffic threshold in this field.
UDP Flood Defense		Click Enable box to activate this intrusion prevention rule and enter the traffic threshold in this field.
ICMP Flood Defense		Click Enable box to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000.

Port Scan Defection	Mandatory field. Disabled by default. Traffic threshold, default setting: 200.	Click Enable box to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000.
Block Land Attack	Disabled by default.	Click Enable box to activate this intrusion prevention rule.
Block Ping of Death		
Block IP Spoof		
Block TCP Flag Scan		
Block Smurf		
Block Traceroute		
Block Fraggle Attack		
ARP Spoofing Defence	Mandatory field. Disabled by default. Traffic threshold, default setting: 300.	Click Enable box to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000.
Save	Button	Click Save to save the settings.
Undo	Button	Click Undo to cancel the settings.

6.2.7 Options

Navigate to the Security > Firewall > Options tab.

The Firewall Options window allows you to modify the behaviour of the firewall and to enable Remote Router Access Control.

Firewall Options		
Item	Setting	
▶ Stealth Mode	<input type="checkbox"/> Enable	
▶ SPI	<input checked="" type="checkbox"/> Enable	
▶ Discard Ping from WAN	<input type="checkbox"/> Enable	

Firewall Options		
Item	Value setting	Description
Stealth Mode	Disabled by default.	Check the Enable box to activate the Stealth Mode function
SPI	Enabled by default.	Check the Enable box to activate the SPI function
Discard Ping from WAN	Disabled by default.	Check the Enable box to activate the Discard Ping from WAN function

Specific IP addresses can be assigned in the Remote Administrator Host Definition window.

Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
2	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
5	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
<div>Save Undo</div>							

Remote Administrator Host Definition		
Item	Value setting	Description
Protocol	HTTP is set by default.	Select HTTP or HTTPS method for router access.
IP	Mandatory field.	This field is to enter 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. An IP address entered in this field and a selected Subnet Mask to compose the subnet.
Service Port	Default setting: 80 for HTTP. Default setting: 443 for HTTPS.	This field is to enter a Service Port to HTTP or HTTPS connection. Value Range: 1 - 65535.
Enabling the rule	Disabled by default.	Click Enable box to activate this rule.
Save	Button.	Click Enable box to activate this rule then save the settings.
Undo	Button.	Click Undo to cancel the settings

6.3 Authentication

6.3.1 Hotspot Services

Navigate to the Security > Authentication > Hotspot Services tab.

The Hotspot Services function provides the Web Portal which asks guests or passengers to pass the authentication process before they can access the Internet via the MG400. Two options on the

External Web Portal

For external Web Portal, you need to enter external RADIUS (Remote Authentication Dial in User Service) server and external UAM (Universal Access Method) server.

Before enabling the external Hotspot Services function, please Navigate to **[User Rule]-[External Server]** to setup external server objects, like RADIUS server and UAM server. Then return to configure Hotspot Services function back in this page to specific WAN Interface, select external Authentication Server and UAM Server from the pre-defined external server object list.

Internal Web Portal

You will only select "Internal RADIUS Server" option for your authentication. The account database can be an embedded database, an external AD database or an external LDAP database. However, the UAM server is not necessary for this case and that the Hotspot Services Web site is embedded in the MG400.

Hotspot Services Configuration ^

Item	Setting
▶ Hotspot Services	<input type="checkbox"/> Enable
▶ WAN Interface	WAN-1 ▼
▶ DHCP Server	DHCP-1 ▼
▶ Web Portal	Internal ▼
▶ Customize login page	<div style="display: flex; justify-content: space-between; align-items: center;"> <div> Download Default CSS and Logo Download Current CSS and Logo </div> <div> Choose File No file chosen </div> <div> Upload CSS and Logo files </div> </div>
▶ MAC Whitelist (Separated by ,)	
▶ Walled-Garden Hosts (Separated by ;)	
▶ Walled-Garden domains (Separated by ;)	
▶ Authentication Server	<div style="display: flex; justify-content: space-between;"> Internal RADIUS Server ▼ Embedded DataBase ▼ </div>
<div style="display: flex; justify-content: center; gap: 10px;"> Save Refresh </div>	

Hotspot Services Configuration		
Item	Value setting	Description
Hotspot Services	Disabled by default.	Check the Enable box to activate the Hotspot Services function.
WAN Interface	Mandatory field. Default setting: WAN-1.	Enter a WAN Interface for the authenticated clients or hosts. All the traffics coming from the hosts will be directed to the specified WAN interface.
DHCP Server	Mandatory field. Default setting: DHCP.	It can be DHCP-1 - DHCP-4, if you configured the corresponding DHCP servers in Network > LAN & VLAN > DHCP Server . If DHCP-1 is selected, you connected to the physical LAN port which

		bound the DHCP-1 server, will be re-directed to a login page when accessing the Internet.
Web Portal	Mandatory field. Default setting: Internal.	<p>Enter which kind of authentication server is to be used for Hotspot Services function. It can be Internal, External, or Terms and Conditions Only, and depends on the product specification. Not all products with internal option.</p> <p>When External is selected, there is no Customize login page to be configured, but you need to enter external UAM Server and Authentication Server for authentication.</p> <p>When Internal is selected, you need to enter an Authentication Server and the portal login page can be edited in Customize login page.</p>
Customize login page	System data.	<p>Customize login page is available only when Internal, or Terms and Conditions Only Web Portal is selected.</p> <p>Click the Download Default CSS and Logo button to download the default CSS file and Logo of login page for the internal authentication server.</p> <p>You can edit the CSS file or Logo downloaded from above buttons and upload them by Upload CSS and Logo files button.</p>
MAC Whitelist (Separated by ,)	Optional setting.	<p>Enter a MAC whitelist for the client devices that will not be subjected to the Hotspot Services authentication function.</p> <p>The MAC(s) filled in this field can access Internet directly, instead of been re-direct to the login page.</p>
Walled-Garden Hosts (Separated by ;)	Optional setting.	<p>Enter the host IP(s) for the MG400 that will not be subjected to the Hotspot Services authentication function.</p> <p>The IP(s) filled in this field can access Internet directly, instead of been re-direct to the login page.</p>
Walled-Garden domains (Separated by ;)	Optional setting.	<p>Enter the domain name(s) for the MG400 that will not be subjected to the Hotspot Services authentication function.</p> <p>The domain names(s) filled in this field can access Internet directly, instead of been re-direct to the login page.</p>
Authentication Server	Mandatory field.	<p>Select the type of authentication server and corresponding user database.</p> <p>If Web Portal is Internal, the Internal RADIUS Server is used to authentication by default, and there are three databases you can choose.</p> <p>When Embedded DataBase is selected, the login IDs and Passwords are created in Serial Port > User > User Profile tab.</p> <p>When External LDAP is selected, the login IDs and passwords are from an external LDAP server. Please enter it as well.</p> <p>When External AD is selected, the login IDs and passwords are from an external AD server. Please enter it as well.</p> <p>If Web Portal is External, the External RADIUS Server is used to authentication by default, you need to enter the external RADIUS</p>

		server. The external radius server can be added by pressing Add Object button directly or added in User Rule > External Server > External Server tab.
Save	Button.	Click the Save button to save changes
Refresh	Button.	Click the Refresh button to refresh current page

6.3.2 MAC Authentication

Navigate to the Security > Authentication > MAC Authentication tab.

The MG400 supports MAC authentication function. When the MAC Authentication function is enabled, the traffic from the specified interface(s) will be applied with the MAC Authentication. The MG400 will interact with the RADIUS server and provide the corresponding information for authentication process.

Configuration

Item	Setting
Mac Authentication	<input type="checkbox"/> Enable
Radius Server	<div> <div>--- Option --- ▼</div> <div>Add Object</div> </div>
LAN Interface	<input type="checkbox"/> LAN
Client Connection Idle Time	<input type="text"/> (20 - 6000 Seconds)

Configuration		
Item	Value setting	Description
MAC Authentication	Disabled by default.	Check the Enable box to activate the MAC Authentication function.
Radius Server	Mandatory field.	Enter an external RADIUS server for authentication. When the MAC Authentication is enabled, the MG400 sends out the connecting client's information to the RADIUS server for authentication.
LAN Interface	Mandatory field.	Select the network interface(s) to apply the MAC Authentication function. It can be LAN or VLAN(s) (port-based). At least, one interface should be selected. Note: DON'T choose the interface which RADIUS server in it.
Client Connection Idle Time	Mandatory field.	Enter the idle time (in seconds) for a client connection. If a client didn't access network for the specified idle time period, its authentication will be invalidated consequently.

The User List shows the existed users. You can create, edit, delete, or even search with a certain key and filter function to quick access to the information.

User List

Filter by

None

Add

Delete

admin

Filter

Previous

Next


^

ID	Nickname	User Name	Password	Actions
----	----------	-----------	----------	---------

Save

Refresh

User List		
Item	Value setting	Description
Nickname	System data.	Displays the nickname for the user.
User Name	System data.	Displays the MAC address for the user.
Password	System data.	Displays the password for the user.
Add	System data.	Add information of new device authentication.
Delete	System data.	Delete information of exists device authentication.
Filter	System data.	Search information of exists device authentication.
Previous	System data.	Navigation Button of authentication list.
Next	System data.	Navigation Button of authentication list.


User Configuration

×

Item	Setting
Nickname	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>

User List		
Item	Value setting	Description
Nickname	Mandatory field. String format can be any text.	Enter a nickname for the user that is easy for user to understand. Value Range: 1 - 64 characters.
User Name	Mandatory field. MAC address format.	Enter the MAC address for the user. Value Range: 0 - 17 characters, MAC format with ':' or '-'.
Password	Mandatory field. String format can be any text (max. 64 characters).	Enter the password for the user.
Save	Button.	Click the Save button to save changes.
Refresh	Button.	Click the Refresh button to update the User Configuration window.

7. Service

7.1 Cellular Toolkit

7.1.1 Data Limit

Navigate to the Service > Cellular Toolkit > Data Limit tab.

The MG400 can be configured to monitor cellular data usage and take actions if required. When data limit is configured, if data usage reaches limited quota, the MG400 can be set to drop the cellular data connection.

If Data Limit feature is enabled, all history of cellular data usage can be viewed at **Status > Usage > Cellular Usage** tab.

3G/4G Data Limit Profile List Add Delete							
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable Action
1	3G/4G SIM A	Telstra	1 Days	Thu Jul 18 2019 00:00:00 GMT+1000	100GB	<input type="checkbox"/>	<input checked="" type="checkbox"/> Edit Select

When Add button is clicked, 3G/4G Data Limit Profile Configuration window will pop up. You can create up to four data limit profiles.

3G/4G Data Limit Profile List Add Delete

3G/4G Data Usage Profile Configuration

Item	Setting
▶ SIM Select	3G/4G ▼ SIM A ▼
▶ Carrier Name	<input type="text"/>
▶ Cycle Period	Days ▼ <input type="text"/>
▶ Start Date	2019 ▼ / July ▼ / 22 ▼
▶ Data Limitation	<input type="text"/> KB ▼
▶ Connection Restrict	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable

Save

3G/4G Data Limit Profile Configuration		
Item Setting	Value setting	Description
SIM Select	Default setting: 3G/4G-1 and SIM A .	Choose a cellular interface (3G/4G-1 or 3G/4G-2), and a SIM card bound to the selected cellular interface to configure its data limit profile.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	Default setting: Days .	The first box has three types for cycle period. They are Days , Weekly and Monthly . Days : For per Days cycle periods, you need to further enter the number of days in the second box. Value Range : 1 - 90 days. Weekly, Monthly : The cycle period is one week or one month.
Start Date	System data.	Enter the date to start measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be incorrect.
Data Limitation	System data.	Enter the allowable data limitation for the defined cycle period.
Connection Restrict	Disabled by default.	Check the Enable box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Disabled by default.	Check the Enable box to activate the data limit profile.
Save	Button.	Click the Save button to save changes.

7.1.2 SMS

Navigate to the Service > Cellular Toolkit > SMS tab.

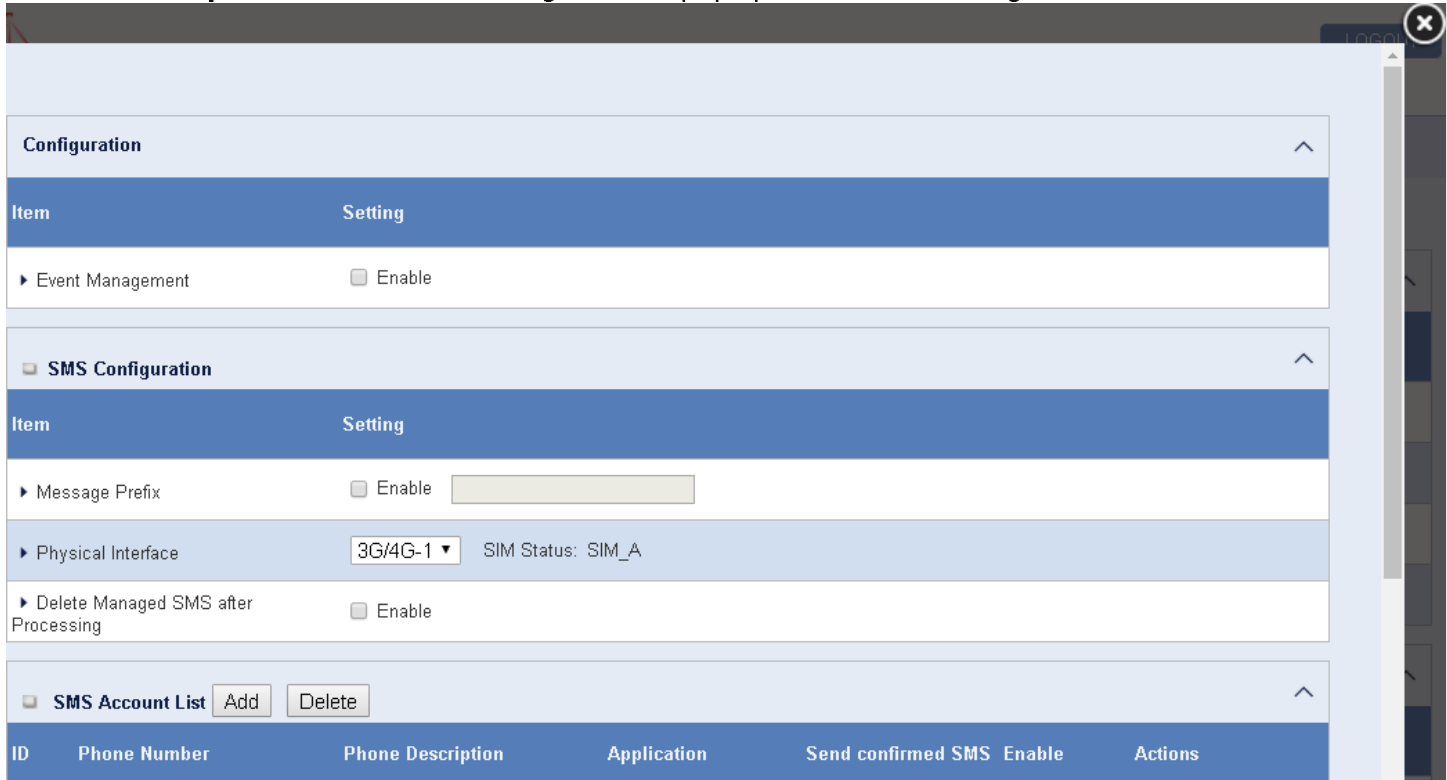
You can send SMS text messages or browse received SMS messages.

Configuration
SMS Setup
Managing Events Setup
Notifying Events Setup

Item	Setting
Physical Interface	3G/4G-1 ▼
SMS	<input checked="" type="checkbox"/> Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▼
SMS Space	<input type="checkbox"/> Enable & Keep Available Space <input type="text"/> (1-10)

Configuration Item	Value setting	Description
Physical Interface	Default setting: 3G/4G-1.	Choose a cellular interface (3G/4G-1 or 3G/4G-2) for the following SMS function configuration.
SMS	Enabled by default.	This is the SMS switch. If the box checked that the SMS function enable, if the box unchecked that the SMS function disable.
SIM Status	System data.	Depend on currently SIM status. The possible value will be SIM_A or SIM_B.
SMS Storage	Default setting: SIM Card Only.	This is the SMS storage location. Currently the option only SIM Card Only.
SMS Space	Disabled by default.	Check the Enable box and enter a number (1-10) for message count to reserve some available storage space and prevent it from run out of storage. The oldest message(s) will be deleted when the SMS storage is going to full.
Undo	Button.	Click Undo to cancel the settings

When **SMS Setup** button is clicked, following windows pop up for the detail settings.



Configuration

Item	Setting
▶ Event Management	<input type="checkbox"/> Enable

SMS Configuration

Item	Setting
▶ Message Prefix	<input type="checkbox"/> Enable <input type="text"/>
▶ Physical Interface	<input type="text" value="3G/4G-1"/> SIM Status: SIM_A
▶ Delete Managed SMS after Processing	<input type="checkbox"/> Enable

SMS Account List

ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions
----	--------------	-------------------	-------------	--------------------	--------	---------

SMS Summary window Shows the numbers of **Unread SMS**, **Received SMS**, **Sent SMS**, **Remaining SMS**, and provide the access to create **new SMS**, **SMS Inbox** and **SMS Sent Folder**.



SMS Summary

Item	Setting
▶ Unread SMS	0
▶ Received SMS	1
▶ Sent SMS	0
▶ Remaining SMS	29

SMS Summary		
Item	Value setting	Description
Unread SMS	System data.	If SIM card insert to router first time, unread SMS value is zero. When received the new SMS but didn't read, this value plus one.
Received SMS	System data.	This value record the existing SMS numbers from SIM card, when received the new SMS, this value plus one.

Sent SMS	System data.	This value record the number of outgoing SMS, when sent one SMS, this value plus one.
Remaining SMS	System data.	This value is SMS capacity minus received SMS, when received the new SMS, this value minus one.
New SMS	Button.	Click New SMS button, a New SMS window appears. You can set the SMS setting from this window.
SMS Inbox	Button.	Click SMS Inbox button, a SMS Inbox List window appears. You can read or delete SMS, reply SMS or forward SMS from this window.
SMS Sent Folder	Button.	Click SMS Sent Folder button, a SMS Sent Folder window appears. You can read or delete SMS, reply SMS or forward SMS from this window.
Save	Button.	Click the Save button to save changes.
Refresh	Button.	Click the Refresh button to update the SMS summary immediately.

When **New SMS** button is clicked, you can create the content for a new SMS.

New SMS
Send

Item

Setting

Receivers

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

Text Message

Length of Current Input : 0

Result

New SMS		
Item	Value setting	Description
Receivers	System data.	Write the receivers to send SMS. You need to add the semicolon and compose multiple receivers that can group send SMS.
Text Message	System data.	Write the SMS context to send SMS. The router supports up to a maximum of 1023 character for SMS context length.
Send	System data.	Click the Send button, above text message will be sent as a SMS.
Result	System data.	If SMS has been sent successfully, it will show Send OK, otherwise Send Failed will be displayed.

When **SMS Inbox** button is clicked, **SMS Inbox List** window will appear and show the received SMS.

You can read, delete, reply and forward SMS from this window.

SMS Inbox List

Refresh

Delete

Close

Previous


1

Next

ID	From Phone Number	Timestamp	SMS Text Preview	Actions
1	+61421922649	2019/07/21 18:11:16	Hey j. Hop.....	<div>Detail</div> <div></div> <div>Reply</div> <div>Forward</div>

SMS Inbox List		
Item	Value setting	Description
ID	System data.	The number of SMS.
From Phone Number	System data.	Sender List (Phone Number) for the received SMS.
Timestamp	System data.	What time the SMS is received.
SMS Text Preview	System data.	Preview the SMS text. Click the Detail button to read a certain message.
Action	Buttons.	Click the Detail button to read the SMS detail; Click the Reply / Forward button to reply/forward SMS. Besides, you can check the box, and then click the Delete button to delete the checked SMS.
Refresh	Buttons.	Refresh the SMS Inbox List.
Delete	Buttons.	Delete the SMS for all checked box from Action.
Close	Buttons.	Close the Detail SMS Message window.

When **SMS Sent Folder** button is clicked, the **SMS Sent Folder** window shows the SMS been sent.

<div>  SMS Sent Folder <div> Delete Close Previous 0 ▼ Next </div> </div>				
ID	Receivers	Timestamp	SMS Text Preview	Actions

SMS Sent Folder		
Item	Value setting	Description
ID	System data.	The number of SMS.
Receivers	System data.	Receiver list for the sent SMS.
Timestamp	System data.	What time the SMS is sent.
SMS Text Preview	System data.	Preview the SMS text. Click the Detail button to read a certain message.
Action	Disabled by default.	Click the Detail button to read the SMS detail. Besides, you can check the box(es), and then click the Delete button to delete the checked record(s).
Delete	Button.	Delete the SMS for all checked box from Action.
Close	Button.	Close the Detail SMS Message window.
Close	Buttons.	Close the Detail SMS Message window.

7.1.3 SIM PIN

Navigate to the Service > Cellular Toolkit > SIM PIN tab.

The MG400 allows you to activate and manage PIN code on a SIM card through its web GUI.

With the Configuration window, it allows you to enable or disable SIM lock (which means protected by PIN code) or change PIN code.

Configuration

Item	Setting
▶ Physical Interface	3G/4G-1 ▼
▶ SIM Status	SIM-A Not insert
▶ SIM Selection	SIM-A ▼ <input type="button" value="Switch"/>

Configuration Window		
Item	Value setting	Description
Physical Interface	Default setting: 3G/4G-1 .	Choose a cellular interface (3G/4G-1 or 3G/4G-2) to change the SIM PIN setting for the selected SIM Card.
SIM Status	System infomation.	<p>Indication for the selected SIM card and the SIM card status. The status could be Ready, Not Insert, or SIM PIN.</p> <p>Ready -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code.</p> <p>Not Insert -- No SIM card is inserted in that SIM slot.</p> <p>SIM PIN -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. That SIM card is still at locked status.</p>
SIM Selection	Default setting : SIM-A	<p>Select the SIM card for further SIM PIN configuration. Press the Switch button, then the router will switch SIM card to another one. After that, you can configure the SIM card.</p>

The PUK Function window is only activated for configuration if that SIM card is locked by PUK code. It means that SIM card is locked and needs additional PUK code to unlock.

☐ **PUK function**

Item	Setting
▶ PUK status	PUK unlock.
▶ Remaining times	N/A
▶ PUK Code	<input type="text"/> (8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)

PUK Function Window		
Item	Value setting	Description
PUK status	PUK Unlock / PUK Lock.	Indication for the PUK status. The status could be PUK Lock or PUK Unlock . As mentioned earlier, the SIM card will be locked by PUK code after too many trials of failure PIN code. In this case, the PUK Status will turns to PUK Lock . In a normal situation, it will display PUK Unlock .
Remaining times	Depend on SIM card.	Represent the remaining trial times for the PUK unlocking. Note : DO NOT make the remaining times down to zero, it will damage the SIM card FOREVER! Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	Mandatory field.	Fill in the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	Mandatory field.	Fill in the New PIN Code (4~8 digits) for the SIM card. You need to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	Button	Click the Save button to apply the setting.

See following window for the enable or Disable PIN code (password) function and change PIN code function.

☐ **SIM function**

^

Item	Setting
▶ PIN Lock	<input checked="" type="checkbox"/> Enable PIN Code: <input type="text"/> (4~8 digits)
▶ Remaining times	N/A

SIM function Window		
Item Setting	Value setting	Description
SIM lock	Depend on SIM card.	Click the Enable button to activate the SIM lock function. For the first time you want to enable the SIM lock function, you need to fill in the PIN code as well, and then click Save button to apply the setting.
Remaining times	Depend on SIM card.	Represent the remaining trial times for the SIM PIN unlocking.
Save	Button.	Click the Save button to apply the setting.
Change PIN Code	Button.	Click the Change PIN code button to change the PIN code (password). If the SIM Lock function is not enabled, the Change PIN code button is disabled. In the case, if you still want to change the PIN code, you need to enable the SIM Lock function first, fill in the PIN code, and then click the Save button to enable. After that, you can click the Change PIN code button to change the PIN code.

When Change PIN Code button is clicked, the following window will appear.

Item	Setting
▶ Current PIN Code	<input type="text"/> (4~8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)
▶ Verified New PIN Code	<input type="text"/> (4~8 digits)

Apply Cancel


Item	Value Setting	Description
Current PIN Code	Mandatory field.	Fill in the current (old) PIN code of the SIM card.
New PIN Code	Mandatory field.	Fill in the new PIN Code.
Verified New PIN Code	Mandatory field.	Confirm the new PIN Code again.
Apply	Button.	Click the Apply button to change the PIN code with specified new PIN code.
Cancel	Button.	Click the Cancel button to cancel the changes and keep current PIN code.

Note: If you change the PIN code for a certain SIM card, you need to also change the corresponding PIN code specified in the Network > WAN & Uplink > Connection Setup > Internet Connection List > Edit > Connection with SIM-A / SIM-B. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

7.1.4 USSD

Navigate to the Service > Cellular Toolkit > USSD tab.

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid call-back service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network.

 Configuration

Item	Setting
▶ Physical Interface	<div>3G/4G-1 ▼</div> <div>SIM Status: SIM_A</div>

Configuration Item	Value setting	Description
Physical Interface	Default setting: 3G/4G-1.	Choose a cellular interface (3G/4G-1 or 3G/4G-2) to configure the USSD setting for the connected cellular service (identified with SIM_A or SIM_B).
SIM Status	System information.	Show the connected cellular service (identified with SIM_A or SIM_B).

The **USSD Profile List** window allows you to customize your USSD profile. It supports up to a maximum of 35 USSD profiles.

USSD Profile List
Add
Delete
^

ID	Profile Name	USSD Command	Comments	Actions
----	--------------	--------------	----------	---------

When Add button is applied, USSD Profile Configuration window will appear.

USSD Profile Configuration
Save
×

Item	Setting
▶ Profile Name	<input type="text"/>
▶ USSD Command	<input type="text"/>
▶ Comments	<input type="text"/>

USSD Profile Configuration		
Item	Value setting	Description
Profile Name	Mandatory field.	Enter a name for the USSD profile.
USSD Command	Mandatory field.	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad "0~9", "*", and "#". The USSD commands are highly related to the cellular service, please check with your service provider for the details.
Comments	Optional field.	Enter a brief comment for the profile.

USSD Request can be **send**, **clear** or **cancel** in the following window.

USSD Request
Send
Clear
Cancel

Item	Setting
▶ USSD Profile	--- Option --- ▼
▶ USSD Command	<input type="text"/>

Save
Refresh

USSD Request		
Item	Value setting	Description
USSD Profile	Mandatory field.	Select a USSD profile name from the dropdown list.
USSD Command	Mandatory field.	The USSD Command string of the selected profile will be shown here.
USSD Response	System Information.	Click the Send button to send the USSD command, and the USSD Response window will appear. You will see the response message of the corresponding service, receive the service SMS.

7.1.5 Network Scan

Navigate to the Service > Cellular Toolkit > Network Scan tab.

Configuration

Item	Setting
▶ Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
▶ Network Type	Auto ▼
▶ Scan Approach	Auto ▼

Save

Configuration		
Item	Value setting	Description
Physical Interface	Default setting: 3G/4G-1.	Choose a cellular interface (3G/4G-1 or 3G/4G-2) for the network scan function.
SIM Status	System information.	Show the connected cellular service (identified with SIM_A or SIM_B).
Network Type	Default setting: Auto.	Specify the network type for the network scan function. It can be Auto, 2G Only, 2G prefer, 3G Only, 3G prefer, or LTE Only. When Auto is selected, the network will be register automatically; If the prefer option is selected, network will be register for your option first;

		If the only option is selected, network will be register for your option only.
Scan Approach	Default setting: Auto.	When Auto is selected, cellular module register automatically. If the Manually option is selected, a Network Provider List window appears. Press Scan button to scan for the nearest base stations. Select (check the box) the preferred base stations then click Apply button to apply settings.
Save	Button.	Click Save to save the settings.

7.2 Event Handling

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the MG400 or change the setting / status of the specific functionality of the MG400. On receiving the managing event, the MG400 will act to change the functionality, collect the required status for administration, and change the status of a certain connected field bus device simultaneously.

The **notifying events** are the events that related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event generated from the connected sensor, or a certain connected field bus device for alerting you something happened with SMS message, Email, and SNMP Trap, etc.

7.2.1 Configuration

Navigate to the **Service > Event Handling > Configuration** tab.

Configuration	
Item	Setting
▶ Event Management	<input type="checkbox"/> Enable

Configuration Item	Value setting	Description
Event Management	Disabled by default	Check the Enable box to activate the Event Management function.

To use the SMS management function, you need to configure some settings in the following **SMS Configuration** window first.

SMS Configuration	
Item	Setting
▶ Message Prefix	<input type="checkbox"/> Enable <input type="text"/>
▶ Physical Interface	<input type="text" value="3G/4G-1"/> SIM Status: SIM_A
▶ Delete Managed SMS after Processing	<input type="checkbox"/> Enable

SMS Configuration		
Item	Value setting	Description
Message Prefix	Disabled by default.	Click the Enable box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you need to enter the prefix behind the checkbox. The received managing events SMS needs to have the designated prefix as an initial identifier , then corresponding handlers will become effective for further processing .
Physical Interface	Default setting: 3G/4G-1.	Choose a cellular interface (3G/4G-1 or 3G/4G-2) to configure the SMS management setting.
SIM Status	System data.	Show the connected cellular service (identified with SIM_A or SIM_B).
Delete Managed SMS after Processing	Disabled by default.	Check the Enable box to delete the received managing event SMS after it has been processed.

Setup the SMS Account for managing the MG400 through the SMS. It supports up to a maximum of 5 accounts.

SMS Account List Add Delete ^						
ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.

SMS Account Configuration ×

Item	Setting
▶ Phone Number	Specific Number ▼ <input type="text"/>
▶ Phone Description	<input type="text"/>
▶ Application	<input type="checkbox"/> Event Trigger <input type="checkbox"/> Notify Handle
▶ Send confirmed SMS	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable

Save

SMS Account Configuration		
Item	Value setting	Description
Phone Number	Mobile phone number format. Mandatory field.	Select the Phone number policy from the drop list, and Enter a mobile phone number as the SMS account identifier if required. It can be Specific Number, or Allow Any. If Specific Number is selected, you need to enter the phone number as the SMS account identifier. Value Range: -1 - 32 digits.
Phone Description	Any text. Optional field.	Enter brief description for the SMS account.
Application	Mandatory field.	Enter the application type. It could be Event Trigger, Notify Handle, or both. If the Phone Number policy is Allow Any, the Noftify Handle will be unavailable.
Send confirmed SMS	Optional field. Disabled by default.	Click Enable box to active the SMS response function. The MG400 will send a confirmed message back to the sender whenever it received a SMS managing event. The confirmed message is like following format: "Device received a SMS with command xxxxx."
Enable	Disabled by default.	Click Enable box to activate this account.
Save	Button.	Click the Save button to save the configuration.

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

Email Service List Add Delete ^				
ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.

Email Service Configuration ×

Item	Setting
▶ Email Server	<input type="text" value="--- Option ---"/>
▶ Email Addresses	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

Save

Email Service Configuration

Item	Value setting	Description
Email Server	--- Option ---	Select an Email Server profile from External Server setting for the email account setting.
Email Addresses	Internet E-mail address format Mandatory field.	Enter the Destination Email Addresses.
Enable	Disabled by default.	Click Enable box to activate this account.
Save	Button.	Click the Save button to save the configuration

Setup the Digital Input (DI) Profile rules. It supports up to 10 profiles.

<input type="checkbox"/> Digital Input (DI) Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/> ^								
ID	DI Profile Name	Description	DI Source	Continues Update Status	Normal Level	Signal Active Time (s)	Enable	Actions

When **Add** button is applied, the **Digital Input (DI) Profile Configuration** window will appear.

☐ **Digital Input (DI) Profile Configuration**
×

Item	Setting
▶ DI Profile Name	<input type="text"/>
▶ Description	<input type="text"/>
▶ DI Source	<input type="text" value="ID1"/>
▶ Continues Update Status	<input type="checkbox"/> Enable & Update Interval <input type="text" value="2"/> (2~86400 seconds)
▶ Normal Level	<input type="text" value="Low"/>
▶ Signal Active Time	<input type="text" value="1"/> (seconds)
▶ Profile	<input checked="" type="checkbox"/> Enable

Digital Input (DI) Profile Configuration		
Item	Value setting	Description
DI Profile Name	String format. Mandatory field.	Enter the DI Profile Name. Value Range: -1 - 32 characters.
Description	Any text. Optional field.	Enter a brief description for the profile.
DI Source	Default setting: ID1.	Enter the DI Source. It could be ID1 or ID2.
Continues Update Status	Disabled 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 MG400 will send repeated notify events for each check interval. Value Range: 2 - 86400 seconds. Note : To prevent receiving too much notify event for the same situation, you can adjust the check interval to a proper one for your application.
Normal Level	Default setting: Low.	Enter the Normal Level. It could be Low or High.
Signal Active Time	Numeric String format. Mandatory field.	Enter 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 Value Range: 1 - 10 seconds.
Profile	Disabled by default.	Click Enable box to activate this profile setting.
Save	Button.	Click the Save button to save the configuration.

Setup the Digital Output (DO) Profile rules. It supports up to 10 profiles.

<div> <input type="checkbox"/> Digital Output (DO) Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/> ^ </div>								
ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable Actions

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** window will appear.

Digital Output (DO) Profile Configuration

Item	Setting
DO Profile Name	<input type="text"/>
Description	<input type="text"/>
DO Source	ID1 ▾
Normal Level	Low ▾
Total Signal Period	<input type="text" value="10"/> (ms)
Repeat & Counter	<input type="checkbox"/> Enable & Counter: <input type="text" value="0"/>
Duty Cycle	<input type="text"/> (%)
Profile	<input checked="" type="checkbox"/> Enable

Save

Digital Output (DO) Profile Configuration		
Item	Value setting	Description
DO Profile Name	String format. Mandatory field.	Enter the DO Profile Name. Value Range: -1 - 32 characters.
Description	Any text. Optional field.	Enter brief description for the profile.
DO Source	Default setting: ID1.	Enter the DO Source. It could be ID1.
Normal Level	Default setting: Low.	Enter the Normal Level. It could be Low or High.
Total Signal Period	Numeric String format Mandatory field.	Enter the Total Signal Period. Value Range: 10 - 10000 ms.
Repeat & Counter	Default setting: Disabled.	Check the Enable box to activate the repeated Digital Output, and enter the repeat times. Value Range: 0 - 65535.
Duty Cycle	Numeric String format Mandatory field.	Enter the Duty Cycle for the Digital Output. Value Range: 1 -100 %.
Profile	Disabled by default.	Click Enable box to activate this profile setting.
Save	Button.	Click the Save button to save the configuration.

Setup the Remote Host Profile. It supports up to 10 profiles.

☐ Remote Host List

^

ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions
----	-----------	---------	---------------	-------------	----------------	----------------	--------	---------

You can click the Add / Edit button to configure the profile.

Remote Host Configuration
×

Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>

Remote Host Configuration		
Item	Value setting	Description
Host Name	String format. Mandatory field.	Enter the Remote Host profile name. Value Range: -1 - 64 characters.
Host IP	Mandatory field. IP Address format.	Enter the IP address for the Remote Host. IPv4 Format.
Protocol Type	Mandatory field. Default setting: TCP.	Enter the protocol to access the Remote Host. It could be TCP or UDP.
Port Number	Mandatory field.	Enter the Port number for accessing the Remote Host. Value Range: 1 - 65535.
Prefix Message	String format. Optional Setting.	Enter the Prefix Message string as pre-defined identification for accessing the remote host, if required. Value Range: -1 - 64 characters.
Suffix Message	String format. Optional Setting.	Enter the Suffix Message string as pre-defined identification for accessing the remote host, if required. Value Range: -1 - 64 characters.
Enable	Disabled by default.	Click Enable box to activate this profile setting.
Save	Button.	Click the Save button to save the configuration.

7.2.2 Managing Events

Navigate to the **Service > Event Handling > Managing Events** tab.

Managing Events allows you to define the rule between event trigger, handlers and response.

Configuration

Item	Setting
Managing Events	<input type="checkbox"/> Enable

Configuration		
Item	Value setting	Description
Managing Events	Disabled by default.	Check the Enable box to activate the Managing Events function.

Setup the Managing Event rules. It supports up to 128 rules.

Managing Event List

AddDelete

ID	Event Name	Event	Trigger Type	Description	Enable	Actions
----	------------	-------	--------------	-------------	--------	---------

SaveUndo

When Add or Edit button is clicked, the Managing Event Configuration window will appear.

Managing Event Configuration

Item

Setting

▶ Event Name

▶ Event

None

None

None

▶ Trigger Type

Period

▶ Interval

0

(0~86400 seconds)

▶ Description

▶ Action

☐ Network Status

☐ WAN

☐ LAN&VLAN

☐ WiFi

☐ NAT

☐ Firewall

☐ VPN

☐ GRE

☐ System Manage

☐ Administration

☐ Digital Output

☐ Remote Host

▶ Managing Event

☒ Enable

Save

Undo

Managing Event Configuration		
Item	Value setting	Description
Event	Default setting: None.	<p>Enter the Event type (SMS, SNMP Trap, or Digital Input) and an event identifier / profile. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simultaneously (AND relation).</p> <p>The supported Event types could be: SMS: Select SMS and fill the message in the textbox to as the trigger condition for the event; SNMP: Select SNMP Trap and fill the message in the textbox to enter</p>

		SNMP Trap Event; Digital Input: Select Digital Input and a DI profile you define to enter a certain Digital Input Event;
Trigger Type	Default setting: Period.	Enter the type of event trigger, either Period or Once. Period: Select Period and enter 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	Default setting: 0.	Enter the repeatedly event trigger time interval. Value Range: 0 -86400 seconds.
Description	String format: any text.	Enter a brief description for the Managing Event.
Action	All box is unchecked by default.	Enter Network Status, or at least one rest action to take when the expected event is triggered. Network Status: Select Network Status Checkbox to get the network status as the action for the event; LAN&VLAN: Select LAN&VLAN Checkbox and the interested sub-items (Port link On/Off), the MG400 will change the settings as the action for the event; Wi-Fi: Select Wi-Fi Checkbox and the interested sub-items (Wi-Fi radio On/Off), the MG400 will change the settings as the action for the event; NAT: Select NAT Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the MG400 will change the settings as the action for the event; Firewall: Select Firewall Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the MG400 will change the settings as the action for the event; VPN: Select VPN Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the MG400 will change the settings as the action for the event; GRE: Select GRE Checkbox and the interested sub-items (GRE Tunnel On/Off), the MG400 will change the settings as the action for the event; System Manage: Select System Manage Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the MG400 will change the settings as the action for the event; Administration: Select Administration Checkbox and the interested sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the MG400 will change the settings as the action for the event; Digital Output: Select Digital Output checkbox and a DO profile you define as the action for the event; Remote Host: Select Remote Host checkbox and a Remote Host profile you define as the action for the event;
Managing	Disabled by default.	Click Enable box to activate this Managing Event setting.

Event		
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to restore what you just configure back to the previous setting.

7.2.3 Notifying Events

Navigate to the **Service** > **Event Handling** > **Notifying Events** tab.


Notifying Events Setting allows you to define the rules between event trigger and handlers.

Configuration		^
Item	Setting	
▶ Notifying Events	<input checked="" type="checkbox"/> Enable	

Configuration		
Item	Value setting	Description
Notifying Events	Disabled by default.	Check the Enable box to activate the Notifying Events function.

Create / Edit Notifying Event Rules

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.

<div>  Notifying Event List <div> Add Delete </div> </div>								^
ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

When **Add** or **Edit** button is applied, the **Notifying Event Configuration** window will appear.

Notifying Event Configuration

Item	Setting
▶ Event Name	<input type="text"/>
▶ Event	<div>None ▼ None ▼ None ▼</div>
▶ Trigger Type	Period ▼
▶ Interval	<input type="text" value="0"/> (0~86400 seconds)
▶ Description	<input type="text"/>
▶ Action	<div><input type="checkbox"/> Digital Output <input type="checkbox"/> SMS <input type="checkbox"/> Syslog <input type="checkbox"/> SNMP Trap (Only Support v1 and v2c) <input type="checkbox"/> Email Alert <input type="checkbox"/> Remote Host</div>
▶ Time Schedule	(0) Always ▼
▶ Notifying Events	<input checked="" type="checkbox"/> Enable
<div>Save</div>	
<div>Undo</div>	

Notifying Event Configuration

Item	Value setting	Description
Event	Default setting: None.	<p>Enter the Event type and corresponding event configuration. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simultaneously (AND relation).</p> <p>The supported Event Type could be:</p> <p>Digital Input: Select Digital Input and a DI profile you define to enter a certain Digital Input Event;</p> <p>Power Change: Select Power Change and a trigger condition to enter the event on a certain power source.</p> <p>WAN: Select WAN and a trigger condition to enter a certain WAN Event;</p> <p>LAN&VLAN: Select LAN&VLAN and a trigger condition to enter a</p>

		<p>certain LAN&VLAN Event;</p> <p>Wi-Fi: Select Wi-Fi and a trigger condition to enter a certain Wi-Fi Event;</p> <p>DDNS: Select DDNS and a trigger condition to enter a certain DDNS Event;</p> <p>Administration: Select Administration and a trigger condition to enter a certain Administration Event;</p> <p>Data Usage: Select Data Usage, the SIM Card (Cellular Service) and a trigger condition to enter a certain Data Usage Event;</p>
Description	String format: any text.	Enter a brief description for the Notifying Event.
Action	All box is unchecked by default.	<p>Enter at least one action to take when the expected event is triggered.</p> <p>Digital Output: Select Digital Output checkbox and a DO profile you define as the action for the event;</p> <p>SMS: Select SMS, and the MG400 will send out a SMS to all the defined SMS accounts as the action for the event;</p> <p>Syslog: Select Syslog and select/unselect the Enable Checkbox to as the action for the event;</p> <p>SNMP Trap: Select SNMP Trap, and the MG400 will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event;</p> <p>Email Alert: Select Email Alert, and the MG400 will send out an Email to the defined Email accounts as the action for the event;</p> <p>Remote Host: Select Remote Host checkbox and a Remote Host profile you define as the action for the event;</p>
Time Schedule	Default setting: (0) Always.	Select a time scheduling rule for the Notifying Event.
Notifying Events	Disabled by default.	Click Enable box to activate this Notifying Event setting.
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to restore what you just configure back to the previous setting.

7.3 Location Tracking

7.3.1 GNSS

Navigate to the **Service>Location Tracking> GNSS** tab.

Configuration

Item	Setting
▶ GNSS	<input checked="" type="checkbox"/> Enable
▶ GNSS Type	GPS ▾
▶ GNSS Message Types	<input checked="" type="checkbox"/> RMC
▶ Data to Storage	<div> <input type="checkbox"/> Enable Select Device: Internal ▾ </div> <div>Interval: <input type="text" value="5"/> (s)</div> <div>Data format: <input type="text" value="RAW"/> ▾</div> <div>Data file name: <input type="text" value="RAW_YYYYMMddhhmm"/></div> <div>Split file: <input type="checkbox"/> Enable Size: <input type="text" value="200"/> KB ▾</div> <div> <input type="button" value="Download log file"/> <input type="button" value="Delete log file"/> </div>

GNSS Configuration

Item	Value setting	Description
GNSS Enable	Disabled by default.	Check Enable box to activate GNSS functions.
GNSS Type	Non-selectable.	GPS is the only option.
GNSS Message Types	These box is unchecked by default.	<p>Select one or more GNSS Message Types that you want to use for transmitting or recording GPS data.</p> <p>There are many sentences in the NMEA standard for selecting, GGA, GLL, GSA, GSV, RMC and VTG. ALL Other includes DTM, GNS, GRS, GST, ZDA, and GBS sentences.</p> <p>Only select the type you need, otherwise it will consume unnecessary network bandwidth.</p> <p>Note: The supported message type is hardware dependent.</p>
SBAS	Disabled by default.	<p>Check Enable box to activate satellite-based augmentation system (SBAS).</p> <p>Note: Some devices do not support this function.</p>
Data to Storage	Disabled by default.	<ul style="list-style-type: none"> ● Enable (Disabled by default) Check Enable box to activate data to storage function. ● Select Device (Mandatory field.) Select Internal or External device to store log data. ● Interval (Mandatory field.) Enter the time interval between two continuous data logs. By default, 5 second is set. Value Range: 5 - 60 seconds.

- **Data Format** (Mandatory field.)
Select data format (RAW, or GPX) to store.
- **Data file name** (Mandatory field.)
Define file name to store.
- **Split Enable**
Check Enable box to activate file splitting function.
- **Split Size& Unit**
Define file size and unit for log file. By default, 200 KB is defined.
Value Range: >= 10KB (Minimum file size is 10 KB).
- **Download log file**
Select a log file and Click **Download log file** to download through Web GUI. If the log format which is specified to download is GPX, we will convert standard GPX format for used.

The Remote Host List window allows you to customize your rules for sending NMEA data to specific IP address and Port. The router supports up to 10 rules.

☐ Remote Host List

^

ID	Host Name	Host IP	Protocol Type	Port Number	Interval(s)	MAC Address Message	Prefix Message	Suffix Message	Enable	Actions
<input type="button" value="Save"/> <input type="button" value="Undo"/>										

When **Add** button is applied, **Remote Host Configuration** window will appear.

Configuration

Remote Host Configuration

Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Interval(s)	<input type="text" value="1"/>
▶ MAC Address Message	<input checked="" type="checkbox"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>

Save

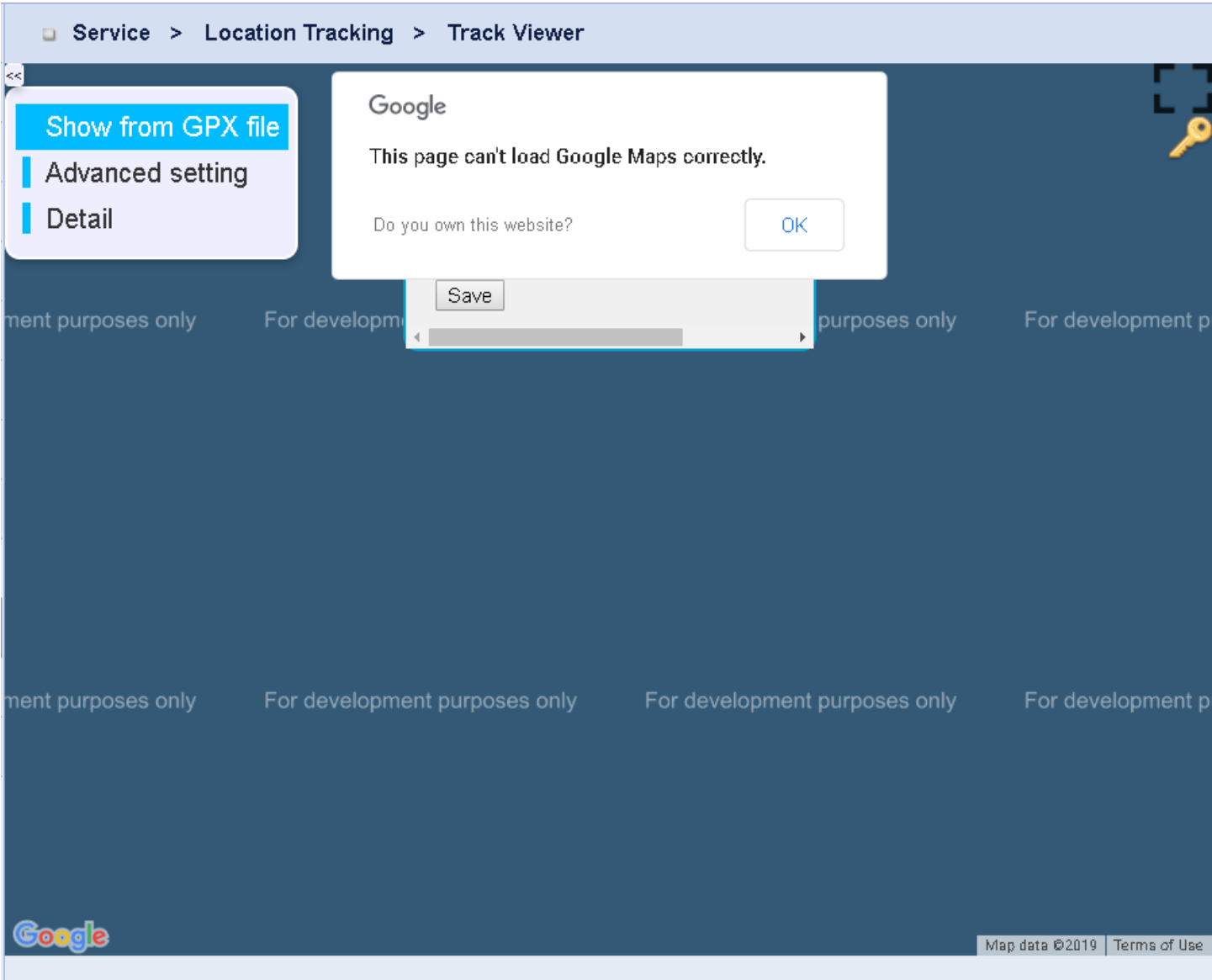
Remote Host Configuration		
Item	Value setting	Description
Host Name	String format: any text	Enter the host name for the designated remote host. Value Range: -1 - 64 characters.
Host IP	Mandatory field.	Enter the IP Address of remote host. It will be use as destination IP for sending NMEA packets.
Protocol Type	Default setting: TCP.	Enter the Protocol (TCP or UDP) to use for sending NMEA packets.
Port Number	Mandatory field.	Enter a Port Number as destination port for sending NMEA packets. Value Range: 1 - 65535.
Interval(s)	Mandatory field.	Enter the time interval (seconds) between two NMEA packets. Value Range: 1 -255 seconds.
Prefix Message	String format: any text.	Enter optional prefix string with specific information if your backend server can recognize. For example, you can input the IMEI code of the MG400 here, and then your backend server can recognize this GPS data is sent from the MG400. You can also leave this field blank.
Suffix Message	String format: any text.	Enter optional suffix string with specific information if your backend server can recognize.

Enable	Disabled by default.	Check Enable box to activate this remote host rule.
Save	Button.	Click the Save button to save the configuration.

7.3.2 Track Viewer

Navigate to the Service > Location Tracking > Track Viewer tab.

Track Viewer allows you to see the track in Google Maps from GPX file recorded by GNSS. In addition, when GNSS is enabled, current position will also be displayed in Track Viewer.



When you use Track Viewer for the first time, UI will request Google Maps API key from you.

Google Maps API key		
Item	Value setting	Description
Google Maps API Key	An optional setting.	<p>The Track Viewer function is implemented with Google Maps JavaScript API, and it requires authentication for further operation. If you don't have Google Maps API key, click the link at [Get a key] to get a key from Google. Paste API key on the text box, and then click Save.</p> <p>You can choose to remain it empty and then click X directly. It allows you use the map temporarily. The key icon on the right top will appear until you input the API key.</p>

If you enter the valid key, the key input window and key icon on the right top side will disappear. If you enter an invalid key, UI will prompt the message and request you to change the value of the API key.

If Google Maps API key remains empty and clicks "Save", you can load and use Google Maps normally. However, we can't guarantee the number of loading times you can reach if you don't input the API key.

Track Viewer lists following items in the side bar.

General Functions		
Item	Value setting	Description
Current Track	System data.	<p>Show current position and current track on the map. Update interval is 5 seconds.</p> <p>If GNSS is disabled, Current Track button will be hidden.</p>
Show from GPX file	System data.	Show the track from the GPX file. It can choose the file from either internal or external storage.
Advanced setting	System data.	You can set track color, line width, minimum distance, and API key here.
Detail	System data.	Select the Detail function to show a time-speed graph and information of the track.

When Current Track button is clicked, then the following window will appear.

The bus icon indicates the current position of the MG400 (or the vehicle that equipped with the MG400). Current track is drawn from the time page was loaded to current time.

In order to show track from a GPX File, click Show from GPX file button, then the following window will appear.

☒ **Show from GPX file**

Item	Setting
From	<input checked="" type="radio"/> Internal <input type="radio"/> External
GPX file	<div> <div></div> <div></div> </div>

Show from GPX file		
Item	Value setting	Description
From	Mandatory field. Internal is selected by default.	Enter the storage where the GPX file located. It can be Internal or External , it depends on the storage setting in GNSS page. Note: External is disabled when no USB flash drive is detected.
GPX file	Mandatory field.	Select the expected GPX file from the dropdown list.

When Advanced setting button is clicked then applied window will appear.

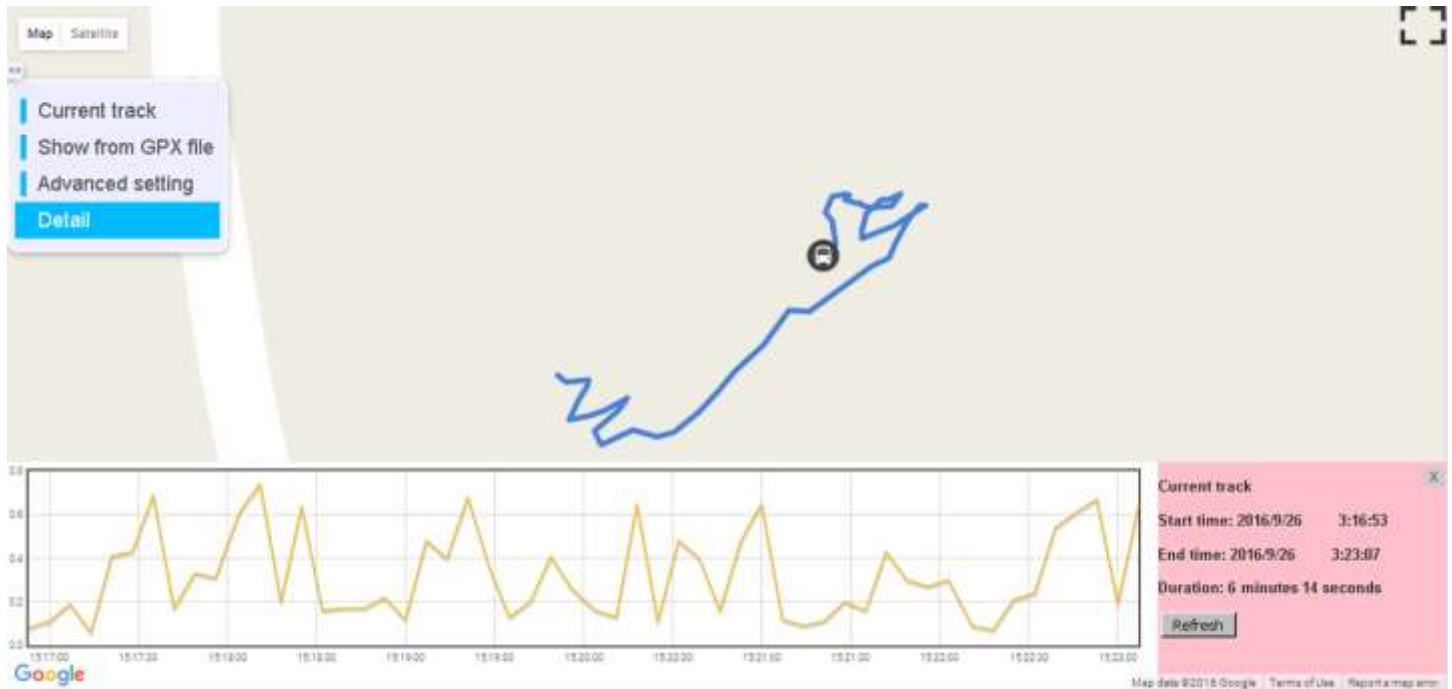
☒ **Advanced setting**

Item	Setting
Track color	<div> <div></div> <div>#0000FF</div> </div>
Line width	<div> <div>5</div> <div>(1-32)</div> </div>
Minimum distance	<div> <div>10</div> <div>m (0-100)</div> </div>
API Key	<div> <div></div> <div>Change</div> </div>

Advanced Setting		
Item	Value setting	Description
Track color	Mandatory field. Default setting: #0000FF.	Change the color of the track. The default value is #0000FF (Blue). Format: #000000 / #0000 / color names e.g. #0000FF, #00F, blue
Line width	Mandatory field. Default setting: 5.	Change the line width of the track. Range is from 1 to 32.

Minimum Distance	Mandatory field. Default setting: 10.	Set the minimum distance between two continuous points. Range is from 0 to 100. When the number is larger, the redundant points are eliminated and the number of points on the map becomes less.
Change	Button.	Click the Change button to modify Google Maps API key.



When Detail button is clicked, then the following window will appear.



Detail Item	Value setting	Description
File name	System data.	Show the file name of current used GPX file. Showing the text Current Track if the map loads current track instead of GPX file.
Start time	System data.	Show the time of the start position. Time format depends on locale.
End time	System data.	Show the time of the end position. Time format depends on locale.
Duration	System data.	Show the time difference between Start time and End time. Format: ? years ? months ? days ? hours ? minutes ? seconds, hide the unit when '?'==0
Refresh	System data.	Only showing the button when the map loads current track. Click Refresh button to refresh the information of the track and update the time-speed graph immediately.
Time-speed graph	System data.	When mouse is over the curve in time-speed graph, the small text box will show the locale time and speed in that point and the yellow car icon will locate on the position at that timestamp in the map. When you click the mouse on the point of curve in time-speed graph, it will set the centre point of the map to that position.

7.4 Power Control

Navigate to Service > Power Control Tab.


Configuration


Item	Setting
▶ Ignition Sense	<input type="checkbox"/> Enable
▶ Shutdown Timer	<input type="text" value="0"/> (0~240 minutes)
▶ Voltage Sense	<input type="checkbox"/> Enable
▶ Shutdown Voltage Threshold	<input type="text" value="9"/> (volts) (Range:9V-36V)

Save

Undo

Configuration		
Item	Value setting	Description
Ignition Sense	Disabled by default.	Click Enable box to activate this Ignition Sense function. By default, the function is disabled, and the MG400 will be always ON when Power Source is attached.
Shutdown Timer	Number format : any number between 0 and 240. Default setting: 0.	Enter a shutdown timer (0-240 minutes) to shutdown the power of the MG400 after the engine has been stopped '0' means the MG400 will never been shutdown even if ignition is removed (ACC OFF). Value Range: 0 - 240.
Voltage Sense	Disabled by default.	Click Enable box to activate this Voltage Sense function. If the function is enabled, when input voltage is under the specified threshold value, the MG400 will be shut down when ACC is OFF, no matter shutdown timer is due or not.
Shutdown Voltage Threshold	Optional field.	Enter a threshold voltage to shut down the MG400 when low battery power situation happens.
Save	Button.	Click the Save button to save the configuration.
Undo	Button.	Click the Undo button to restore what you just configure back to the previous setting.

8. Administration

8.1 Remote Management

8.1.1 Command Script

Navigate to the Administration > Command Script > Configuration tab.

Command script configuration is the application that allows you to setup the pre-defined configuration in plain text style and apply configuration on start-up.

Configuration

Item	Setting
▶ Command Script	<input type="checkbox"/> Enable
▶ Backup Script	Via Web UI
▶ Upload Script	Via Web UI
▶ Script Name	<input type="text"/>
▶ Version	<input type="text"/>
▶ Description	<div></div>
▶ Update time	

Configuration		
Item	Value setting	Description
Command Script	Disabled by default.	Check the Enable box to activate the Command Script function.
Backup Script	Button.	Click the Via Web UI button to backup or upload the existed command script in a .txt file. You can enter the script file name in Script Name below.
Upload Script	Button.	Click the Via Web UI button to Upload the existed command script from a specified .txt file.
Script Name	Optional field. Any valid file name.	Enter a script file name for script backup or display the selected upload script file name. Value Range: 0 - 32 characters.
Version	Optional field. Any string.	Enter the version number for the applied Command script. Value Range: 0 - 32 characters.
Description	Optional field.	Enter a short description for the applied Command script.

	Any string.	
Update time	System data.	It records the upload time for last command script upload.

☐ **Command Script Editor**

0 / 65280

You can edit the plain text configuration settings in the configuration window as above.

Plain Text Configuration		
Item	Value setting	Description
Clean	Button.	Clean text area. (You should click Save button to further clean the configuration already saved in the system.)
Save	Button.	Save configuration.

The supported plain text configuration items are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configure with **STARTUP** command. For those configurations without corresponding Linux command set to configure, you can configure them with proprietary command set.

Configuration Content		
Key	Value setting	Description
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	Mandatory field.	Enter the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the Protocol for the OpenVPN Client. <ul style="list-style-type: none"> • Select TCP or TCP /UDP ->The OpenVPN will use TCP protocol, and Port will be set as 443 automatically. • Select UDP -> The OpenVPN will use UDP protocol, and Port will be set

		as 1194 automatically.
OPENVPN_PORT	Mandatory field.	Enter the Port for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Enter the Remote IP/FQDN of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Enter the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Enter the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Enter the LZO Compression algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Enter the authorization mode for the OpenVPN tunnel. <ul style="list-style-type: none"> • TLS ->The OpenVPN will use TLS authorization mode, and the following items CA Cert., Client Cert. and Client Key needs to enter as well.
OPENVPN_CA_CERT	Mandatory field.	Enter the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	Mandatory field.	Enter the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	Mandatory field.	Enter the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Enter the extra options setting for the OpenVPN client.
IP_ADDR1	Ip	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With ICMP Query, the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Enter an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Enter the time interval for between two DNS Query or ICMP checking packets.
STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo "startup done" > /tmp/demo

The MG400 accepts Telnet CLI commands. You can use the proprietary telnet command "txtConfig" and related action items to perform the plain system configuration.

The command format is: txtConfig (action) [option]

Action	Option	Description
clone	Output file	Duplicate the configuration content from database and stored as a configuration file. (ex: txtConfig clone /tmp/config) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the "Backup" plain text configuration.
commit	An existing file	Commit the configuration content to database. (ex: txtConfig commit /tmp/config)
enable	NA	Enable plain text system config. (ex: txtConfig enable)
disable	NA	Disable plain text system config. (ex: txtConfig disable)
run_immediately	NA	Apply the configuration content that has been committed in database. (ex: txtConfig run_immediately)
run_immediately	An existing file	Assign a configuration file to apply. (ex: txtConfig run_immediately /tmp/config)

8.1.2 TR-069

Navigate to the Administration > Remote Management > TR-069 tab.

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end user devices, like the MG400. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer provided equipment (CPE) and Auto Configuration Servers (ACS). The Security Device is such CPE.

Configuration	
Item	Setting
▶ TR-069	<input type="checkbox"/> Enable
▶ Interface	WAN-1 ▼
▶ Data model	ACS Cloud Data Model ▼
▶ ACS URL	<input type="text"/>
▶ ACS UserName	<input type="text"/>
▶ ACS Password	<input type="password"/>
▶ Connection Request Port	8099
▶ Connection Request UserName	<input type="text"/>
▶ Connection Request Password	<input type="password"/>
▶ Inform	<input checked="" type="checkbox"/> Enable Interval 300
▶ Certification Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: ▼

TR-069		
Item	Value setting	Description
TR-069	Disabled by default.	Check the Enable box to activate TR-069 function.
Interface	Default setting: WAN-1.	When you finish set network WAN-1 - WAN-n, you can choose WAN-1 - WAN-n When you finish set Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface just like "IPSec #1"
Data Model	Default setting: ACS Cloud Data Model.	Select the TR-069 data model for the remote management. Standard: the ACS Server is a standard one, which is fully comply with TR-069. ACS Cloud Data Model: Select this data model if you intend to use Cloud ACS Server to manage the deployed devices.
ACS URL	Mandatory field.	You can ask ACS manager provide ACS URL and manually set
ACS Username	Mandatory field.	You can ask ACS manager provide ACS username and manually set

ACS Password	Mandatory field.	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	Mandatory field. Default setting: 8099.	You can ask ACS manager provide ACS Connection Request Port and manually set Value Range: 0 - 65535.
ConnectionRequest UserName	Mandatory field.	You can ask ACS manager provide ACS Connection Request Username and manually set
ConnectionRequest Password	Mandatory field.	You can ask ACS manager provide ACS Connection Request Password and manually set
Inform	Enabled by default. Default setting: 300.	When the Enable box is checked, the MG400 (CPE) will periodically send inform message to ACS Server according to the Interval setting. Value Range: 0 - 86400 for Inform Interval.
Certification Setup	Default setting: default.	You can leave it as default or select an expected certificate and key from the drop down list. Refer to User Rule > Certificate Section for the Certificate configuration.

STUN Settings ^

Item	Setting
▶ STUN	<input checked="" type="checkbox"/> Enable
▶ Server Address	<input style="width: 150px;" type="text"/>
▶ Server Port	<input style="width: 60px;" type="text" value="3478"/> (1~65535)
▶ Keep Alive Period	<input style="width: 60px;" type="text" value="0"/> (0~65535)second(s)

STUN Settings Configuration		
Item	Value setting	Description
STUN	Enabled by default	Check the Enable box to activate STUN function.
Server Address	String format: any IPv4 address It is an optional item.	Enter the IP address for the expected STUN Server.
Server Port	Optional field. Default setting: 3478.	Enter the port number for the expected STUN Server. Value Range: 1 - 65535.
Keep Alive Period	Optional field. Default setting: 0.	Enter the keep alive time period for the connection with STUN Server. Value Range: 0 - 65535.
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the modifications.

8.1.3 SNMP

Navigate to the Administration > Remote Management > SNMP tab.

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give you the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

The MG400 supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIV1 and SMIV2, SNMPv2-TM and SNMPv2-MIB, and AMIB (a Proprietary MIB)

Configuration ^

Item	Setting
▶ SNMP Enable	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WAN
▶ WAN Interface	All WANs ▾
▶ Supported Versions	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> v3
▶ SNMP Port	161
▶ Limited Remote Access IP	Specific IP Address ▾
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable

SNMP Item	Value setting	Description
SNMP Enable	Disabled by default.	Select the interface for the SNMP and enable SNMP functions. When Check the LAN box, it will activate SNMP functions and you can access SNMP from LAN side; When Check the WAN box, it will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	Mandatory field. Default setting: ALL WANs.	Enter the WAN interface that a remote SNMP host can access to the MG400. By default, All WANs is selected, and there is no limitation for the WAN interface.
Supported Versions	Mandatory field. Disabled by default.	Select the version for the SNMP When Check the v1 box. It means you can access SNMP with version 1. When Check the v2c box. It means you can access SNMP with version 2c. When Check the v3 box. It means you can access SNMP with version 3.
SNMP Port	String format: any port number. The default SNMP port is 161. Mandatory field.	Enter the SNMP Port. You can fill in any port number. While you need to ensure the port number is not to be used. Value Range: 1 - 65535.
Limited Remote Access IP	String format: any IPv4 address. It is an optional item.	Enter the Remote Access IP for WAN and check the box to enable it as well. Select Specific IP Address, and fill in a certain IP address. It means only this IP address can access SNMP from LAN/WAN side. Select IP Range, and fill in a range of IP addresses. It means the IP address within specified range can access SNMP from LAN/WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
Undo	Button.	Click Undo to cancel the modifications.

The **Multiple Community List** window allows you to customize your access control. The router supports up to 10 community sets.

☐ **Multiple Community List**

⤴

ID	Community	Enable	Actions
----	-----------	--------	---------

When Add button is applied, Multiple Community Rule Configuration window will pop up.

Multiple Community Rule Configuration

Item	Setting
Community	<div>Read Only</div>
Enable	<div><input checked="" type="checkbox"/> Enable</div>

Save

Multiple Community Rule Configuration		
Item	Value setting	Description
Community	Mandatory field. String format: any text. Default setting: Read Only.	Enter this version 1 or version v2c user’s community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	Enabled by default	Click Enable to enable this version 1 or version v2c user.
Save	Button.	Click the Save button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show “Click on save button to apply your changes” to remind you to click main page Save button.
Back	Button.	Click the X button to return to last page.

The **User Privacy List** window allows you to customize your access control. The router supports up to 128 user Privacy sets.

User Privacy List

AddDelete

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions
----	-----------	----------	----------------	------------	--------------	-------------	-----------	-------------------	--------	---------

When Add button is clicked, User Privacy List window will pop up.

Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="password"/>
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Mode	noAuthNoPriv ▼
▶ Privacy Key	<input type="password"/>
▶ Authority	Read ▼
▶ OID Filter Prefix	<input type="text" value="1"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

User Privacy Rule Configuration		
Item	Value setting	Description
User Name	Mandatory field. String format: any text.	Enter the User Name. Value Range: 1 - 32 characters.
Password	String format: any text.	When your Privacy Mode is authNoPriv or authPriv, you need to enter the Password for this user. Value Range: 8 - 64 characters.
Authentication	Default setting: None.	When your Privacy Mode is authNoPriv or authPriv, you need to enter the Authentication types for the user. Select the authentication types MD5/ SHA-1 to use.
Encryption	Default setting: None.	When your Privacy Mode is authPriv, you need to enter the Encryption protocols for the user. Select the encryption protocols DES / AES to use.
Privacy Mode	Default setting: noAuthNoPriv.	Enter the Privacy Mode for the user. Select the noAuthNoPriv. You do not use any authentication types and encryption protocols. Select the authNoPriv. You need to enter the Authentication and Password. Select the authPriv. You need to enter the Authentication, Password, Encryption and Privacy Key.
Privacy Key	String format: any text.	When your Privacy Mode is authPriv, you need to enter the Privacy Key (8 - 64 characters) for the user.
Authority	Default setting: Read.	Enter the user's Authority that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	The default value is 1. Mandatory field. String format: any legal OID.	The OID Filter Prefix restricts access for the user to the sub-tree rooted at the given OID. Value Range: 1 - 2080768.
Enable	Enabled by default.	Click Enable to enable the rule for this user.
Save	Button.	Click the Save button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind you to click main page Save button.

The Trap Event Receiver List window allows you to customize your trap event receiver. The router supports up to 4 Trap Event Receiver sets.

<input type="checkbox"/> Trap Event Receiver List <input type="button" value="Add"/> <input type="button" value="Delete"/> ^											
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable Actions

When Add button is applied, Trap Event Receiver Rule Configuration window will appear.

Trap Event Receiver Rule Configuration

Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	<input type="text" value="v1"/>
▶ Community Name	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

Save

Trap Event Receiver Rule Configuration		
Item	Value setting	Description
Server IP	Mandatory field. String format: any IPv4 address or FQDN.	Enter the trap Server IP or FQDN. The DUT will send trap to the server IP/FQDN.
Server Port	String format: any port number. The default SNMP trap port is 162. Mandatory field.	Enter the trap Server Port. You can fill in any port number. But you need to ensure the port number is not to be used. Value Range: 1 - 65535.
SNMP Version	Default setting: v1.	Select the version for the trap. Selecting v1 or v2c will display a smaller configuration window containing five settings. If v3 is selected, six additional configuration settings will be included in the configuration window.
Community Name	Mandatory field for SNMP Version v1 and v2c. String format: any text.	Enter the Community Name for this version 1 or version v2c trap. Value Range: 1 - 32 characters.
User Name	Mandatory field for SNMP Version v3. String format: anytext	Enter the User Name for this version 3 trap. Value Range: 1 - 32 characters.
Password	Mandatory field for SNMP Version v3. String format: anytext	When your Privacy Mode is authNoPriv or authPriv, you need to enter the Password for this version 3 trap. Value Range: 8 - 64 characters.
Privacy Mode	Mandatory field for SNMP Version v3. Default setting: noAuthNoPriv	Specify the Privacy Mode for this version 3 trap. Select noAuthNoPriv if you do not use any authentication types and encryption protocols. If authNoPriv is selected, you need to specify the Authentication and Password. If authPriv is selected, you need to specify the Authentication, Password, Encryption and Privacy Key.
Authentication	Mandatory field for SNMP Version v3 Default setting: None	When your Privacy Mode is authNoPriv or authPriv, you need to enter the Authentication types for this version 3 trap. Select the authentication types MD5/ SHA-1 to use.
Encryption	Mandatory field for SNMP Version v3	When your Privacy Mode is authPriv, you need to enter the Encryption protocols for this version 3 trap. Select the encryption protocols DES / AES to use.

	Default setting: None	
Privacy Key	Mandatory field for SNMP Version v3 String format: any text	When your Privacy Mode is authPriv, you need to enter the Privacy Key (8 - 64 characters) for this version 3 trap.
Enable	Enabled by default.	Click Enable to enable this trap receiver.
Save	System data.	Click the Save button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" to remind you to click main page Save button.

When you select v2c, the configuration window is the same as for v1.

When you select v3, the configuration window will provide more setting items for the version 3 Trap.

SNMP MIB-2 System
^

Item	Setting
▶ sysContact	<input type="text"/>
▶ sysLocation	<input type="text"/>

SNMP MIB-2 System Configuration		
Item	Value setting	Description
sysContact	Optional Setting. String format: any text.	Enter the contact information forMIB-2 system. Value Range: 0 - 64 characters.
sysLocation	Optional Setting. String format: any text.	Enter the location information forMIB-2 system. Value Range: 0 - 64 characters.

If you use some private MIB, you need to fill the enterprise name, number and OID in the following **Options** window.

Options ^

Item	Setting
▶ Enterprise Name	<input type="text" value="Default"/>
▶ Enterprise Number	<input type="text" value="12823"/>
▶ Enterprise OID	1.3.6.1.4.1. <input type="text" value="12823.4.4.9"/>

Options Item	Value setting	Description
Enterprise Name	The default value is Default. Mandatory field. String format: any text	Enter the Enterprise Name for the private MIB. Value Range: 1 - 10 characters, and only string with A-Z, a-z, 0-9, '-', '_'.
Enterprise Number	The default value is 12823. (Default Enterprise Number) Mandatory field. String format: any number.	Enter the Enterprise Number for the private MIB. Value Range: 1 -2080768.
Enterprise OID	The default value is 1.3.6.1.4.1.12823.4.4.9 (Default Enterprise OID) Mandatory field. String format: any legal OID.	Enter the Enterprise OID for the private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number need to be identical with the enterprise number.
Save	Button.	Click the Save button to save the configuration and apply your changes to SNMP functions.
Undo	Button.	Click the Undo button to cancel the settings.

8.1.4 Telnet & SSH

Navigate to the Administration > Remote Management > Telnet & SSH tab.

The Telnet & SSH setting allows you to access the MG400 through the traditional Telnet or SSH Telnet program. Before you can telnet (login) to the MG400, please configure the related settings and password. The password

management part allows you to set root password for logging telnet and SSH.

Configuration

Save

Undo

Item	Setting
Telnet	<div>LAN <input checked="" type="checkbox"/> Enable</div> <div>WAN <input type="checkbox"/> Enable (WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/>)</div> <div></div> <div>Service Port <input type="text" value="23"/></div>
SSH	<div>LAN <input type="checkbox"/> Enable</div> <div>WAN <input type="checkbox"/> Enable (WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/>)</div> <div></div> <div>Service Port <input type="text" value="22"/></div>

Configuration Item	Value setting	Description
Telnet	The LAN Enable box is checked by default. By default Service Port is 23.	Check the Enable box to activate the 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.
SSH	The LAN Enable box is checked by default. 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.
Save	Button.	Click Save to save the settings
Undo	Button.	Click Undo to cancel the settings

Password Management

Save

Undo

Item	Setting
root	<div>Old Password : <input type="text"/></div> <div>New Password : <input type="text"/></div> <div>New Password Confirmation : <input type="text"/></div>

Configuration		
Item	Value setting	Description
root	String: any text but no blank character. The default password for telnet is 'wirelessm2m'.	Type old password and enter new password to change root password. Note_1: You are highly recommended to change the default telnet password with you before the MG400 is deployed. Note_2: If you have trouble for the default password for previous FW version, please check the corresponding User Manual to get the correct one.
Save	Button.	Click Save to save the settings.
Undo	Button.	Click Undo to cancel the settings.

8.2 System Operation

8.2.1 Password & MMI

Navigate to the Administration > System Operation > Password & MMI tab.

Host Name window allows you to setup / change the host name of the MG400.

Host Name

Item

Setting

▶ Host Name

Save

Undo

Username Configuration		
Item	Value setting	Description
Host Name	Optional field.	Enter the host name of the MG400.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

Username window allows you to change the web based MMI login account to access the MG400.

Username

Item

Setting

▶ Username

admin

Modify

▶ New Username

▶ Password

Save

Undo

Username Configuration		
Item	Value setting	Description
Username	The default Username for web-based MMI is 'admin'.	Display the current MMI login account (Username).
New Username	String: any text.	Enter new Username to replace the current setting.
Password	String: any text.	Enter current password to verify if you have the permission to change the username setting.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

Password window allows you to change the web based MMI login password for the MG400 access.

Password
^

Item	Setting
▶ Old Password	<input type="password"/>
▶ New Password	<input type="password"/>
▶ New Password Confirmation	<input type="password"/>

Save

Undo

Password Configuration		
Item	Value setting	Description
Old Password	String: any text. The default password for web-based MMI is 'admin'.	Enter the old password.
New Password	String: any text.	Enter new password.
New Password Confirmation	String: any text.	Enter new password again to confirm.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

MMI window provides the Web GUI access configurations.

MMI ^

Item	Setting
▶ Login	Password-Guessing Attack & MAX: <input type="text" value="3"/> (times)
▶ Login Timeout	<input checked="" type="checkbox"/> Enable <input type="text" value="600"/> (seconds)
▶ GUI Access Protocol	<input type="text" value="http/https"/> ▼
▶ HTTPs Certificate Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: <input type="text"/> Key: <input type="text"/>
▶ HTTP Compression	<input type="checkbox"/> gzip <input type="checkbox"/> deflate
▶ HTTP Binding	<input checked="" type="checkbox"/> DHCP 1
▶ System Boot Mode	<input type="text" value="Normal Mode"/> ▼

MMI Configuration		
Item	Value setting	Description
Login	Default setting: 3 (times).	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, a 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, default setting 300.	Check the Enable box to activate the auto logout function and enter the maximum idle time as well. Value Range: 30 - 65535.
GUI Access Protocol	Default setting: http/https.	Select the protocol that will be used for GUI access. It can be http/https, http only, or https only.
HTTPs Certificate Setup	Default is selected by default.	If the https Access Protocol is selected, the HTTPs Certificate Setup option will be available for further configuration. You can leave it as default or select a expected certificate and key from the drop down list. Refer to User Rule > Certificate Section for the Certificate configuration.
HTTP Compression	Disabled by default.	Check the box (gzip, or deflate) if any compression method is preferred.
HTTP Binding	Optional field. DHCP-1 is checked by default.	Select the DHCP Server to bind with http access.
System Boot Mode	Normal Mode is selected by default.	Select the system boot mode that will be adopted to boot up the MG400. Normal Mode: It takes longer boot up time, with complete firmware image check during the MG400 booting. Fast Mode: It takes shorter boot up time, without checking the firmware image during the MG400 booting. Quick Mode: It takes the shortest boot up time, without checking the firmware image and creating the internal database for User/Group/Hotspot Services functions. Note: Use Quick Mode with care, once selected, the User/Group/Hotspot Services function will become non-functional.
Save	Button.	Click Save button to save the settings.
Undo	Button.	Click Undo button to cancel the settings.

8.2.2 System Information

Navigate to the Administration > System Operation > System Information tab.

System Information window displays the MG400 information.

System Information ^	
Item	Setting
▶ Model Name	MG400
▶ Kernel Version	2.6.36
▶ FW Version	0CLD1G0.J41_e41.0CLD_07081700
▶ System Time	Mon, 22 Jul 2019 14:00:39 +1000
▶ Device Up-Time	0day 2hr 28min 4sec
<div>Refresh</div>	



System Information		
Item	Value setting	Description
Model Name	System data.	Displays the model name of this product.
Device Serial Number	System data.	Displays the serial number of this product.
Kernel Version	System data.	Displays the Linux kernel version of the product
FW Version	System data.	Displays the firmware version of the product
Memory Usage	System data.	Displays the percentage of the MG400 memory utilization.
System Time	System data.	Displays the current system time.
Device Up-Time	System data.	Displays the statistics for the MG400 up-time since last boot up.
Refresh	System data.	Click the Refresh button to update the system Information immediately.

8.2.3 System Time

Navigate to the Administration > System Operation > System Time tab.

The System Time Configuration window provides auto-synchronized and manual setup for you to setup the system time for the MG400. The time supported synchronization methods can be Time Server, Manual, PC, Cellular Module, or GPS Signal. Select the method first, and then configure rest settings.

When Time Server is selected in synchronization method field, the system time will synchronize automatically to the time server.


System Time Configuration


Item	Setting
▸ Synchronization method	Time Server ▼
▸ Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney ▼
▸ Auto-synchronization	Time Server: <input type="text"/> Available Time Servers (RFC-868): Auto ▼
▸ Daylight Saving Time	<input type="checkbox"/> Enable
▸ NTP Service	<input type="checkbox"/> Enable
▸ Synchronize immediately	Active

System Time Information		
Item	Value setting	Description
Synchronization method	Mandatory field. Default setting: Time Server.	Select the Time Server as the synchronization method for the system time.
Time Zone	Mandatory field. Default setting: GMT+00 :00.	Select a time zone where the MG400 locates.
Auto-synchronization	Mandatory field. Default setting: Auto.	Enter the IP or FQDN for the NTP time server you expect, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	It is an optional item. Disabled by default.	Check the Enable button to activate the daylight saving function. When you enabled this function, you need to enter the start date and end date for the daylight-saving time duration.
NTP Service	It is an optional item. Disabled by default.	Check the Enable button to activate the NTP Service function. When you enable this function, the MG400 can provide NTP server service for its local connected devices.
Synchronize immediately	Button.	Click the Active button to synchronize the system time with specified time server immediately.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Click the Refresh button to update the system time immediately.

When Manual is selected in Synchronization method, the system time will follow the manual setting.

System Time Configuration

Item	Setting
Synchronization method	Manual
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
Daylight Saving Time	<input type="checkbox"/> Enable
Set Date & Time Manually	<div>2019 / July / 26 (Year/Month/Day)</div> <div>11 : 12 : 17 (Hour:Minute:Second)</div>
NTP Service	<input type="checkbox"/> Enable

Save

Refresh

System Time Information		
Item	Value setting	Description

Synchronization method	Mandatory field. Default setting: Time Server.	Select the Manual as the synchronization method for the system time. It means you need to set the Date & Time manually.
Time Zone	Mandatory field. Default setting: GMT+00 :00.	Select a time zone where the MG400 locates.
Daylight Saving Time	It is an optional item. Disabled by default	Check the Enable button to activate the daylight saving function. When you enabled this function, you need to enter the start date and end date for the daylight-saving time duration.
Set Date & Time Manually	It is an optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
NTP Service	It is an optional item. Disabled by default.	Check the Enable button to activate the NTP Service function. When you enable this function, the MG400 can provide NTP server service for its local connected devices.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Refresh the System Time Configuration window.

When PC is selected in Synchronization method, the system time will follow the PC time.

System Time Configuration

Item	Setting
Synchronization method	PC
NTP Service	<input type="checkbox"/> Enable
Synchronize immediately	Active

Save Refresh

System Time Information		
Item	Value setting	Description
Synchronization method	Mandatory field. Default setting: Time Server.	Select PC as the synchronization method for the system time to allow system to synchronize its date and time to the time of the administration PC.
NTP Service	It is an optional item. Disabled by default.	Check the Enable button to activate the NTP Service function. When you enable this function, the MG400 can provide NTP server service for its local connected devices.
Synchronize immediately	Button.	Click the Active button to synchronize the system time with specified time server immediately.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Click the Refresh button to update the system time immediately.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Refresh the System Time Configuration window.

When Cellular Module is selected in Synchronization method, the system time will follow the Cellular network time.

System Time Configuration

Item	Setting
Synchronization method	Cellular Module
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
NTP Service	<input type="checkbox"/> Enable
Synchronize immediately	Active

Save Refresh

System Time Information		
Item	Value setting	Description
Synchronization method	Mandatory field. Default setting: Time Server.	Select Cellular Module as the synchronization method for the system time to allow system to synchronize its date and time to the time provided from the connected mobile ISP. Note: this option is only available for the product with Cellular WAN interface.
Time Zone	Mandatory field. Default setting: GMT+00 :00.	Select a time zone where the MG400 locates.
NTP Service	It is an optional item. Disabled by default.	Check the Enable button to activate the NTP Service function. When you enable this function, the MG400 can provide NTP server service for its local connected devices.
Synchronize immediately	Button.	Click the Active button to synchronize the system time with specified time server immediately.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Click the Refresh button to update the system time immediately.
Synchronization method	Mandatory field. Default setting: Time Server.	Select Cellular Module as the synchronization method for the system time to allow system to synchronize its date and time to the time provided from the connected mobile ISP. Note: this option is only available for the product with Cellular WAN interface.

Synchronize with GPS Time Service

When GPS signal is selected in Synchronization method, the system time will follow the GPS satellite time.

System Time Configuration

Item	Setting
Synchronization method	GPS Signal
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney
NTP Service	<input type="checkbox"/> Enable
Synchronize immediately	Active

Save

Refresh

System Time Information		
Item	Value setting	Description
Synchronization method	Mandatory field. Time Server is selected by	Select GPS Signal as the synchronization method for the system time to allow system to synchronize its date and time to the time provided from the GNSS service.

	default.	Note: this option is only available for the product with GNSS interface.
Time Zone	Mandatory field. Default setting: GMT+00 :00.	Select a time zone where the MG400 locates.
NTP Service	It is an optional item. Disabled by default.	Check the Enable button to activate the NTP Service function. When you enable this function, the MG400 can provide NTP server service for its local connected devices.
Synchronize immediately	Button.	Click the Active button to synchronize the system time with specified time server immediately.
Save	Button.	Click the Save button to save the settings.
Refresh	Button.	Click the Refresh button to update the system time immediately.
Synchronization method	Mandatory field. Default setting: Time Server.	Select Cellular Module as the synchronization method for the system time to allow system to synchronize its date and time to the time provided from the connected mobile ISP. Note: this option is only available for the product with Cellular WAN interface.

8.2.4 System Log

Navigate to the Administration > System Operation > System Log tab.

View button is for you to view log history on the MG400. Email Now button enables you to send instant Email with system log.

System Log

ViewEmail Now

Web Log List

PreviousNextFirstLastDownloadClear

Time	Log
Jul 26 08:37:28	BusyBox(csm lib) v1.3.2
Jul 26 08:37:28	kernel: klogd started: BusyBox v1.3.2 (2019-07-04 12:50:21 CST)(csm lib)

Web Log List Window		
Item	Value setting	Description
Time column	System data.	Displays event time stamps
Log column	System data.	Displays Log messages
Previous	Button.	Click the Previous button to move to the previous page.
Next	Button.	Click the Next button to move to the next page.
First	Button.	Click the First button to jump to the first page.
Last	Button.	Click the Last button to jump to the last page.
Download	Button.	Click the Download button to download log to your PC in tar file format.
Clear	Button.	Click the Clear button to clear all log.
Back	Button.	Click the Back button to return to the previous page.

Web Log Type Category window allows you to select the type of events to be logged and displayed in the Web Log List Window as described in the previous section.

Item

Setting

Web Log Type Category

☒ System

☒ Attacks

☒ Drop

☒ Login message

☐ Debug

Web Log Type Category Setting Window		
Item	Value setting	Description
System	Enabled by default.	Check to log system events and to display in the Web Log List window.
Attacks	Enabled by default.	Check to log attack events and to display in the Web Log List window.
Drop	Enabled by default.	Check to log packet drop events and to display in the Web Log List window.
Login message	Enabled by default.	Check to log system login events and to display in the Web Log List window.
Debug	Disabled by default.	Check to log debug events and to display in the Web Log List window.

Email Alert window allows you to select the type of events to be logged and sent to a destined Email address.

☐ Enable

Server: --- Option --- ▼ Add Object

E-mail Addresses:

Subject:

Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Email Alert Setting Window		
Item	Value setting	Description
Enable	Disabled by default.	Check Enable box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	Button	Select an email server from the Server dropdown list to send Email. If none has been available, click the Add Object button to create an outgoing Email server.
E-mail address	String: email format.	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ';' Enter the Email address in the format of 'myemail@domain.com'.
Subject	String: any text.	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Disabled by default.	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Syslog window allows you to select the type of event to be logged and sent to a Syslog server.

☐ Enable

Server: --- Option --- ▼ Add Object

Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Syslog Setting Window		
Item	Value Setting	Description
Enable	Disabled by default.	Check Enable box to activate the Syslog function, and send event logs to a syslog server
Server	Button.	Select one syslog server from the Server dropdown box to send event log to. If none has been available, click the Add Object button to create a system log server. You may also add a system log server from the User Rule > External Server > External Server tab.
Log type category	Disabled by default.	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

Log to Storage window allows you to select the type of events to be logged and stored in internal or external storage.

☐ Enable
 Select Device:
 Log file name:
 Split file: ☐ Enable Size: KB
 Interval: ☐ Enable (1 ~ 10080 Minutes)
 Max Records: (5~10000)

 Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Log to Storage Setting Window		
Item	Value setting	Description
Enable	Disabled by default.	Check to enable sending log to storage.
Select Device	Default setting: Internal.	Select internal or external storage.
Log file name	Disabled by default.	Enter log file name to save logs in designated storage.
Split file Enable	Disabled by default.	Check enable box to split file whenever log file reaching the specified limit.
Split file Size	Default setting: 200 KB.	Enter the file size limit for each split log file. Value Range: 10 - 1000.
Interval Enable	Disabled by default	Check enable box to enable the log interval setting.
Log Interval	Default setting: 1440 minute.	Enter the log interval setting. Value Range: 1 - 10080 Minute.
Max Records	Default setting: 3000 minute.	Enter the maximum number of records to be stored in the log storage. Value Range: 5 - 10000.
Log type category	Disabled by default.	Check which type of logs to send: System, Attacks, Drop, Login message, Debug
Download log file	System data.	Click the Download log file button to download log files to a log.tar file.
Clear Logs	System data.	Click the Clear logs button to delete the log files from the storage.

8.2.5 Backup & Restore

Navigate to the Administration > System Operation > Backup & Restore tab.



FW Backup & Restore
^

Item	Setting
▶ FW Upgrade	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Via Web UI ▼</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">FW Upgrade</div> </div>
▶ Module FW Upgrade	<div style="border: 1px solid #ccc; padding: 2px 10px;">FW Upgrade</div>
▶ Backup Configuration Settings	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Download ▼</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Via Web UI</div> </div>
▶ Auto Restore Configuration	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <input type="checkbox"/> Enable </div> <div style="display: flex; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px;">Save Conf.</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Clean Conf.</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Conf. Info.</div> </div> </div>

FW Backup & Restore		
Item	Value setting	Description
FW Upgrade	Default setting: Via Web UI.	If new firmware is available, click the FW Upgrade button to upgrade the MG400 firmware via Web UI, or Via Storage. After clicking on the “FW Upgrade” command button, you need to enter the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on the MG400. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”
Module FW Upgrade	Button	Upgrade Cellular module FW via Web UI.
Backup Configuration Settings	Default setting: Download.	You can backup or restore the MG400 configuration settings by clicking the Via Web UI button. Download: for backup the MG400 configuration to a config.bin file. Upload: for restore a designated configuration file to the MG400. Via Web UI: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	Disabled by default.	Check the Enable button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the Save Conf. button or clicking the Clean Conf. button to erase the stored customized configuration.

8.2.6 Reboot & Reset

Navigate to the Administration > System Operation > Reboot & Reset tab.

 **System Operation**


Item	Setting
▶ Reboot	<div>Now ▼</div> <div>Reboot</div>
▶ Reset to Default	<div>Reset</div>

Save

System Operation Window		
Item	Value setting	Description
Reboot	Default setting: Now.	<p>Click the Reboot button to reboot the MG400 immediately or on a pre-defined time schedule.</p> <p>Now: Reboot immediately</p> <p>Time Schedule: Select a pre-defined auto-reboot time schedule rule to reboot the MG400 automatically. To define a time schedule rule, Navigate to User Rule > Scheduling > Configuration tab.</p>
Reset to Default	Button.	Click the Reset button to reset the MG400 configuration to its default value.

8.3 FTP

8.3.1 Server Configuration

Navigate to the Administration > FTP > Server Configuration tab.

This section allows you to setup the embedded FTP and SFTP server for retrieving the log files.

☐ **FTP Server Configuration**


^

Item	Setting
▶ FTP	<input checked="" type="checkbox"/> Enable
▶ FTP Port	<input type="text" value="21"/>
▶ Timeout	<input type="text" value="300"/> second(s)(60-7200)
▶ Max. Connections per IP	<input type="text" value="2"/>
▶ Max. FTP Clients	<input type="text" value="5"/>
▶ PASV Mode	<input type="checkbox"/> Enable
▶ Port Range of PASV Mode	<input type="text" value="50000"/> ~ <input type="text" value="50031"/>
▶ Auto Report External IP in PASV Mode	<input type="checkbox"/> Enable
▶ ASCII Transfer Mode	<input type="checkbox"/> Enable
▶ FTPS(FTP over SSL/TLS)	<input type="checkbox"/> Enable

Configuration Item	Value setting	Description
FTP	Disabled by default.	Check Enable box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. Note: The embedded FTP Server is only for log downloading, so no write permission is implemented for user file upload to the storage.
FTP Port	Default setting: Port 21.	Enter a port number for FTP connection. The MG400 will listen for incoming FTP connections on the specified port. Value Range: 1 - 65535.
Timeout	Default setting: 300.	Enter the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max.	Default setting: 2.	Enter the maximum number of clients from the same IP address for

Connections per IP		the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	Default setting: 5	Enter the maximum number of clients for the FTP connection. Up to 32 clients is supported.
PASV Mode	Optional setting.	Check the Enable box to activate the support of PASV mode for an FTP connection from FTP clients.
Port Range of PASV Mode	Default Setting: 50000 - 50031.	Enter the port range to allocate for PASV style data connection. Value Range: 1024 - 65535.
Auto Report External IP in PASV Mode	Optional setting.	Check the Enable box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting.	Check the Enable box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting.	Check the Enable box to activate the support of secure connections via SSL/TLS.

The **SFTP Server** can be enable and configured in the following window.


SFTP Server Configuration

Save

^

Item	Setting
▶ SFTP	<input type="checkbox"/> Enable via <input type="checkbox"/> LAN via <input type="checkbox"/> WAN (<input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/>) <div></div>
▶ SFTP Port	22

Configuration Item	Value setting	Description
SFTP	Disabled by default.	Check Enable box to activate the embedded SFTP Server function. Furthermore, you can check the granted interface(s) for the SFTP connection, via LAN, WAN, or both. <ul style="list-style-type: none"> With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Default setting: 22	Enter a port number for SFTP connection. The MG400 will listen for incoming SFTP connections on the specified port. Value Range: 1 - 65535.

8.3.2 User Account

Navigate to the Administration > FTP > User Account tab.

This section allows you to setup your accounts for logging to the embedded FTP and SFTP server to retrieve

the interested fog files.

User Account List

AddDelete

ID	User Name	Password	Directory	Permission	Enable	Actions
<div>Refresh</div>						

When **Add** button is applied, **User Account Configuration window** will appear.

User Account Configuration

Save

Item	Setting
▶ User Name	<input type="text" value="admin"/>
▶ Password	<input type="password" value="....."/>
▶ Directory	<div>Browse</div>
▶ Permission	<div>Read/Write ▼</div>

Configuration Item	Value setting	Description
User Name	String: non-blank string.	Enter the user account for login to the FTP server. Value Range: 1 - 15 characters.
Password	String: no blank.	Enter the user password for login to the FTP server.
Directory	Button.	Select a root directory after user login.
Permission	Default setting: Read/Write.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no write permission is implemented for user file upload to the storage, even Read/Write option is selected.

8.4 Diagnostic

8.4.1 Packet Analyzer

Navigate to the Administration > Diagnostic > Packet Analyzer tab.

The Packet Analyzer can capture packets per your settings. You can enter interfaces to capture packets and filter by setting rule. Ensure the log storage is available (external USB Storage), otherwise Packet Analyzer cannot be enabled.

Configuration

Item	Setting
▶ Packet Analyzer	<input type="checkbox"/> Enable
▶ File Name	<input type="text"/>
▶ Split Files	<input type="checkbox"/> Enable File Size : <input type="text" value="200"/> <input type="text" value="KB"/>
▶ Packet Interfaces	<div> <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4 </div> <div> <input type="checkbox"/> ASY <input type="text" value="Binary Mode"/> </div> <div> 2.4G : <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 </div> <div> 5G : <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8 </div>

Configuration		
Item	Value setting	Description
Packet Analyzer	Disabled by default.	Check Enable box to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	Optional field. Blank is set by default, and the default file name is <Interface>_<Date>_<index> .	Enter the file name to save the captured packets in log storage. If Split Files option is also enabled, the file name will be appended with an index code " _<index> ". The extension file name is .pcap .
Split Files	Optional field. The default value of File Size is 200 KB.	Check enable box to split file whenever log file reaching the specified limit. If the Split Files option is enabled, you can further enter the File Size and Unit for the split files. Value Range: 10 - 99999. NOTE: File Size cannot be less than 10 KB
Packet Interfaces	Optional field.	Define the interface(s) that Packet Analyzer should work on. At least, one interface is required, but multiple selections are also accepted.

The supported interfaces can be:

- **WAN:** When the WAN is enabled at **Physical Interface**, it can be selected here.
- **ASY:** This means the serial communication interface. It is used to capture packets appearing in the **Serial Port**. Therefore, it can only be selected when specific serial port protocol, like Modbus, is enabled. Select **Binary mode** or **String mode** for the serial interface.
- **VAP:** This means the virtual AP. When Wi-Fi and VAP are enabled, it can be selected here.

After you enable the Packet Analyzer function on specific Interface(s), you can further setup some filter rules to capture the packets which matched the rules.

Capture Filters

Item

Setting

▶ Filter

☐ Enable

▶ Source MACs

▶ Source IPs

▶ Source Ports

▶ Destination MACs

▶ Destination IPs

▶ Destination Ports

Save

Undo

Capture Fitters		
Item	Value setting	Description
Filter	Optional setting.	Check Enable box to activate the Capture Filter function.
Source MACs	Optional setting.	<p>Define the filter rule with Source MACs, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they need to be separated with “;”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.</p>
Source IPs	Optional setting.	<p>Define the filter rule with Source IPs, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they need to be separated with “;”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.</p>
Source Ports	Optional setting.	<p>Define the filter rule with Source Ports, which means the source port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they need to be separated with “;”, e.g. 80; 53 Value Range: 1 - 65535.</p>
Destination MACs	Optional setting.	<p>Define the filter rule with Destination MACs, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they need to be separated with “;”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.</p>
Destination IPs	Optional setting.	<p>Define the filter rule with Destination IPs, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they need to be separated with “;”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.</p>
Destination Ports	Optional setting.	<p>Define the filter rule with Destination Ports, which means the destination port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they need to be separated with “;”, e.g. 80; 53 Value Range: 1 - 65535.</p>

8.4.2 Diagnostic Tools

Navigate to the Administration > Diagnostic > Diagnostic Tools tab.

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools for you to check WAN connectivity.

Diagnostic Tools

Item	Setting
▶ Ping Test	Host IP: <input type="text"/> Outer Interface: <input type="text" value="Auto"/> LAN Source: <input type="text" value="Default"/> <input type="button" value="Ping"/>
▶ Tracert Test	Host IP: <input type="text"/> Interface: <input type="text" value="Auto"/> <input type="text" value="UDP"/> <input type="button" value="Tracert"/>
▶ Speed Test	Interface: <input type="text" value="Auto"/> mode: <input type="text" value="DL+UL"/> <input type="checkbox"/> SSL <input type="button" value="Test"/>
▶ Wake on LAN	<input type="text"/> <input type="button" value="Wake up"/>
<input type="button" value="Save"/>	

Diagnostic Tools		
Item	Value setting	Description
Ping Test	Optional Setting.	This allows you to enter an IP / FQDN, the Outer interface (auto, WAN, LAN, or VLAN), and LAN source (default, LAN, or VLAN) as well, so system will try to ping the specified device to test whether it is alive after clicking on the Ping button. A test result window will appear beneath it.
Tracert Test	Optional setting.	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost, and the route cannot be evaluated. First, you need to enter an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), and by default, it is UDP. Then, system will try to trace the specified host to test whether it is alive after clicking on Tracert button. A test result window will appear beneath it.
Speed Test	Optional setting.	This allows you to do a quick speed test for verifying the connectivity on specific interface.
Wake on LAN	Optional setting.	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can enter the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the Wake up command button.
Save	Button.	Click the Save button to save the configuration.

Appendix

Appendix A – GPL Written Offer

This product incorporates open source software components covered by the terms of third-party copyright notices and license agreements contained below.

GPSTabel

Version 1.4.4

Copyright (C) 2002-2005 Robert Lipe<robertlipe@usa.net>

GPL License: <https://www.gpsbabel.org/>

Curl

Version 7.19.6

Copyright (c) 1996-2009, Daniel Stenberg, <daniel@haxx.se>.

MIT/X derivate License: <https://curl.haxx.se/>

OpenSSL

Version 1.0.2m

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

GPL License: <https://www.openssl.org/>

brctl - ethernet bridge administration

Stephen Hemminger <shemminger@osdl.org>

Lennert Buytenhek <buytenh@gnu.org>

version 1.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings

Stephen Hemminger<shemminger@osdl.org>

Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>

version iproute2-ss050330

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent

Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>

version 0.7

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program

Alexander V. Lukyanov <lav@yars.free.net>

version:4.5.x

Copyright (c) 1996-2014 by Alexander V. Lukyanov (lav@yars.free.net)

dnsmasq - A lightweight DHCP and caching DNS server.

Simon Kelley <simon@thekelleys.org.uk>

version:2.72

dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay

Version: 2.0.0-b8

GPLv2

<http://www.dest-unreach.org/socat/>

LibModbus

Version: 3.0.3

LGPL v2

<http://libmodbus.org/news/>

LibIEC60870

GPLv2

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

<https://sourceforge.net/projects/mrts/>

Openswan

Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

<https://www.openswan.org/>

Opennhp

Version: v0.14.1

OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332
and Cisco IOS extensions.

Project homepage: <http://sourceforge.net/projects/opennhp>

Git repository: git://opennhp.git.sourceforge.net/gitroot/opennhp

LICENSE

OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for
additional details.

OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and
GPLv2+ licenses. See libev/LICENSE for additional details.

OpenNHRP links to c-ares. c-ares is licensed under the MIT License.

<https://sourceforge.net/projects/opennhp/>

IPSec-tools

Version: v0.8

No GPL be written

<http://ipsec-tools.sourceforge.net/>

PPTP

Version: pptp-1.7.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

<http://pptpclient.sourceforge.net/>

PPTPServ

Version: 1.3.4

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. <http://poptop.sourceforge.net/>

L2TP

Version: 0.4

Copying All software included in this package is Copyright 2002 Roaring Penguin Software Inc. You may distribute it under the terms of the GNU General Public License (the "GPL"), Version 2, or (at your option) any later version.

<http://www.roaringpenguin.com/>

L2TPServ

Version: v 1.3.1 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

<http://www.xelerance.com/software/xl2tpd/>

Mpstat: from sysstat, system performance tools for Linux

Version: 10.1.6

Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server

Version: 0.53.1

Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.

Version: 5.9

Copyright: (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet Gateway Device) which provide NAT traversal services to any UPnP enabled client on the network.

Version: 1.7

Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for Hotspot Services (UAM) and 802.1X access provisioning.

Version: 1.3.0

Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

Version: 1.11.3

Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.

Version: 2.4

Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems

Version: 3.3.11

Copyright: (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers

Version: 2007_365

Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation

Version: 0.9.8

Copyright: (C) 2010-2012 Andrew Nayenko

NTFS_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.

Version: 2009.4.4

Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72: a release of MySQL, a dual-license SQL database server

Version: 5.1.72

Copyright: (c) 2000, 2013, Oracle and/or its affiliates

FreeRadius: a high performance and highly configurable RADIUS server

Version: 2.1.12

Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

Linux IPv6 Router Advertisement Daemon – radvd

Version: V 1.15

Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>

BSD License: <http://www.litech.org/radvd/>

WIDE-DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients, servers, and relay agents.

Version: 20080615

Copyright (C) 1998-2004 WIDE Project.

BSD License: <https://sourceforge.net/projects/wide-dhcpv6/>

Python version 2.7.12

This Python distribution contains no GNU General Public Licensed (GPLed) code so it may be used in proprietary projects just like prior Python distributions. There are interfaces to some GNU code but these are entirely optional

OpenPAM Radula

This software was developed for the FreeBSD Project by ThinkSec AS and Network Associates Laboratories, the Security Research Division of Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

ISC DHCP Version 4.3.5

Copyright (c) 2004-2016 by Internet Systems Consortium, Inc. ("ISC")

Appendix B – Product handling

Do handle, install and connect the MG400 and its accessories with care.

Installation, configuration and decommissioning should be performed by trained professional only.

Do install the MG400 in a dust-free place with ventilation.

Humidity range of the MG400 is 10% ~ 95% (non-condensing). Do not operate the MG400 beyond this range or expose to liquid.

Do not operate the MG400 beyond operating temperature range (-30°C to +70°C).

Before decommissioning, do check and follow local regulations for disposal of electronic products.

For DC power source applications, before connecting power, check the output voltage and rated current of the power source. Output voltage should be 9-36V DC. Output current minimum 2.5A at 9V.

The MG400 may getting warm during normal use. Do not touch the top heat sink.

Appendix C – BEAM Warranty Terms and Conditions

Please visit following web page for the latest warranty terms and conditions.

<https://beamcommunications.com/support/service-warranty/beam-warranty-conditions>.

Appendix D – Compliance

The MG400 complies with the following standards.

EMC: EN 55032, ETSI EN 301 489-1, ETSI EN 301 489-17, EN 301489-52

Radio: ETSI EN 300 328, ETSI EN 301 893, AS/ ACIF S042.1& AS/CA S042.4

Safety: AS/NZS 2772.2, IEC62368