AirGate 4G Wi-Fi

INSTRUCTION MANUAL V1.1x B

NOVUS

We Measure, We Control, We Record

ANATEL

CE

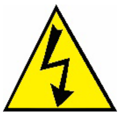
UK CA

1 SAFETY ALERTS

The symbols below are used throughout this manual to draw the user's attention to important information regarding safety and use of the device.

CAUTION

Read the manual fully before installing and operating the device.



CAUTION OR HAZARD

Risk of electric shock.

ATTENTION

Material sensitive to static charge. Check precautions before handling.

Safety recommendations must be followed to ensure user safety and to prevent damage to the device or system. If the device is used in a manner other than that specified in this manual, the safety protections may not be effective.

1.1 INTERFERENCE ISSUES

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

2 INTRODUCTION

AirGate 4G Wi-Fi has a unique and flexible platform that allows remote access to industrial automation networks. This device enables wireless data connectivity over public and private cellular networks with 2G/3G/4G technology and access to legacy network with Modbus RTU over RS485 networks and several protocols over TCP/IP and RS232.

AirGate 4G Wi-Fi has two SIM cards inputs, allowing the use of up to two cellular network operators (one of them acting as failover), two LAN ports (one port that can be used as both LAN and WAN - for fixed Internet with mobile failover) and two digital inputs and two digital outputs for alarm applications. Also has a Wi-Fi 802.11 b/g/n interface for access point with equipment that has Wi-Fi connectivity.

The device supports 9 to 48 VDC supply voltage and has a reverse polarity protection mechanism for added reliability. It is an advanced choice for M2M wireless applications with reliable data transmission capabilities.

2.1 FEATURES AND BENEFITS

INDUSTRIAL INTERNET ACCESS

- Wireless mobile broadband 2G / 3G / 4G connection
- Remote access to SCADA system for industrial automation
- Reduce high costs for on-site maintenance

DESIGNED FOR INDUSTRIAL USAGE

- Power input range 9 to 48 VDC
- Industrial designed for harsh environment
- Compact metal casing for easy mounting

SECURE AND RELIABLE REMOTE CONNECTION

- Connection manager ensure seamless communication
- Support multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

EASY TO USE AND EASY TO MAINTAIN

- User-friendly web interface for human interaction
- Easy configuration for deployment
- Support 3rd party remote management cloud

2.2 MECHANICAL SPECIFICATIONS

AirGate 4G Wi-Fi has the following dimensions: 106 mm x 106 mm x 40 mm (excluding antenna).

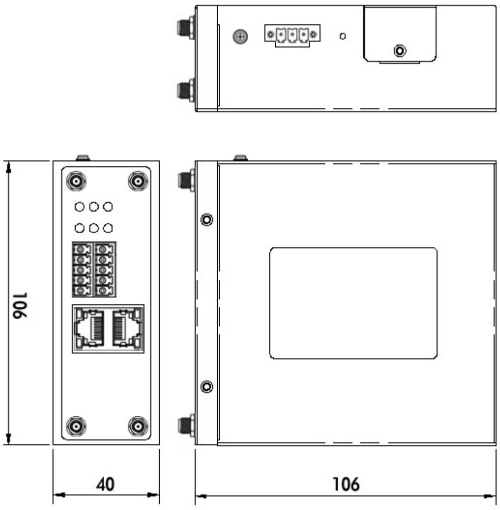


Figure 1 – AirGate 4G Wi-Fi Dimension

2.3 PACKAGE CHECKLIST

AirGate 4G Wi-Fi package contains:

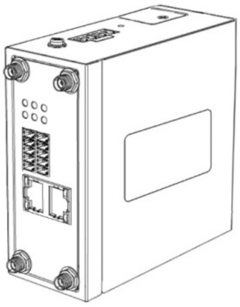
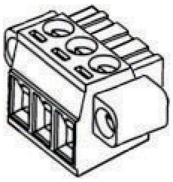
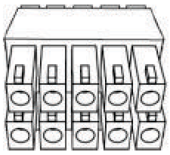
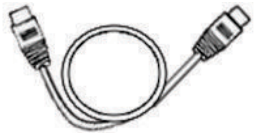
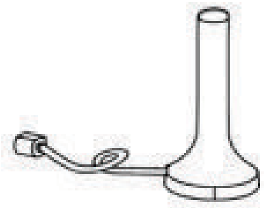
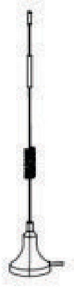
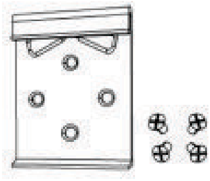
			
AirGate 4G Wi-Fi	**1 Power Supply Connector**	**1 Connector for serial ports and digital inputs and outputs**	**1 Ethernet Cable**
			
1 Cellular Antenna	**2 Wi-Fi Antennas**	**1 DIN Rail mounting kit**	

Table 1 – Required Items

AirGate 4G Wi-Fi contains the following optional accessory items:

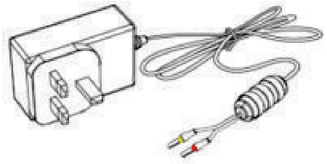
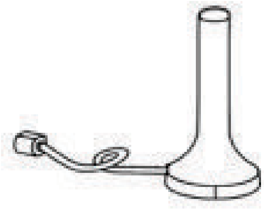
	
Power Supply	**Cellular Antenna**

Table 2 – Optional items

3 INSTALLATION

3.1 DEVICE OVERVIEW

3.1.1 FRONT PANEL

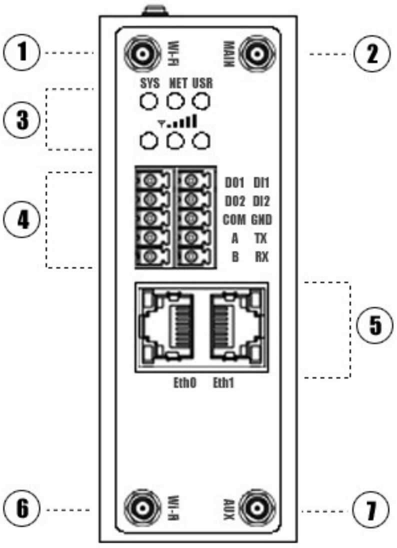


Figure 2 – Front panel

In the front panel, **AirGate 4G Wi-Fi** has the following items:

1. Wi-Fi antenna connector
2. MAIN cellular antenna connector
3. LED indicator
4. Serial ports and digital inputs and digital outputs (DIDO) connector
5. Ethernet port
6. Wi-Fi antenna connector
7. AUX cellular antenna connector

3.1.2 LEFT SIDE PANEL

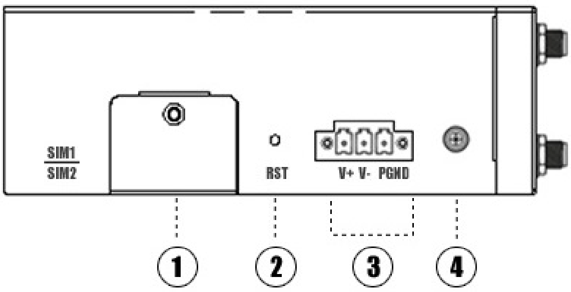


Figure 3 – Left side

In the left side panel, **AirGate 4G Wi-Fi** has the following items:

1. SIM card slot
2. Reset button
3. Power connector
4. Grounding stud

3.2 LED INDICATOR

NAME	COLOR	STATUS	DESCRIPTION
SYS	Green	Slow blinking (500 ms duration)	System booting.
		Fast blinking	Operating normally.
		Off	Power is off.
NET	Green	On	Register to highest priority network service (depend on Radio, e.g., Radio support LTE as Highest priority network).
		Fast blinking (500 ms duration)	Register to non-highest priority network service (depend on Radio, e.g., Radio support LTE as Highest priority network, then WCDMA and GPRS is non-highest priority network).
		Off	Register failed.
USR: SIM	Green	On	Router is trying cellular connection with SIM1.
		Fast blinking (250 ms duration)	Router is trying cellular connection with SIM2.
		Off	No SIM detected.
USR: Wi-Fi	Green	On	Wi-Fi is enabled but without data transmission.
		Blinking	Wi-Fi is enabled and transmitting data.
		Off	Wi-Fi is disabled or failed to boot.
Signal Strength Indicator 📶	Green	On / 3 LED light up	Signal strength (21-31) is high.
		On / 2 LED light up	Signal strength (11-20) is medium.
		On / 1 LED light up	Signal strength (1-10) is low.
		Off	No signal.

Table 3 – LED indicator

3.3 ETHERNET PORT INDICATOR

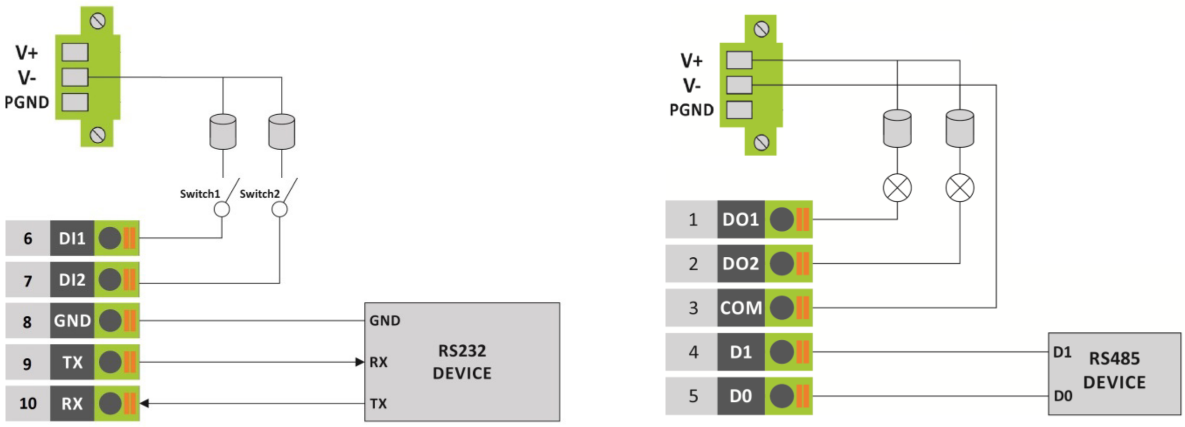
NAME	COLOR	STATUS	DESCRIPTION
Link indicator	Green	On	Connection is established.
		Blinking	Data is being transmitted.
		Off	Connection is not established.
	Yellow	Not used for this device model.	

Table 4 – Ethernet port indicator

3.4 CONNECTOR PIN DEFINITION

3.4.1 SERIAL PORTS & DIDO

Erro! Fonte de referência não encontrada. shows the RS232, the RS485, and the DIDO connections:



Digital input and RS232 connection

Digital output and RS485 connection

Figure 4 – AirGate 4G Wi-Fi connections

Erro! Fonte de referência não encontrada. shows the connector pins numbering:

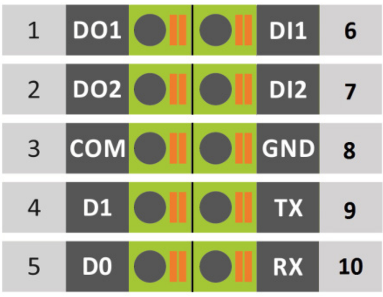


Figure 5 – Connectors

PIN	RS232	RS485	DI	DO	DIRECTION
1	--	--	--	DO1	Router ⟶ Device
2	--	--	--	DO2	Router ⟶ Device
3	--	--	--	COM	--
4	--	D1	--	--	Router ⟷ Device
5	--	D0	--	--	Router ⟷ Device
6	--	--	DI1	--	Router ⟵ Device
7	--	--	DI2	--	Router ⟵ Device
8	GND	--	--	--	--
9	TX	--	--	--	Router ⟶ Device
10	RX	--	--	--	Router ⟵ Device

Table 5 – Serial ports & DIDO

Table 7 shows the RS485 signals:

D1	D	D+	B	Bidirectional line of data.	Terminal 4
D0	$\overline{D}$	D-	C	Inverted bidirectional line of data.	Terminal 5
C GND				Optional link that improves communication performance.	Terminal 8

Table 6 – RS485 signals

3.4.2 POWER INPUT

The figure below shows the power input connections:

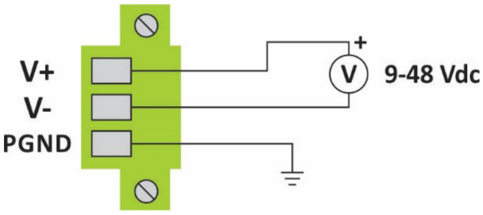


Figure 6 – Power input

PIN	DESCRIPTION
V+	Positive
V-	Negative
PGND	GND

Table 7 – Power input

3.5 RESET BUTTON

Table 9 shows the RESET button functions:

FUNCTION	ACTION
Reboot	Press the RST button for up to 3 seconds while device is operating.
Factory reset	Press the RST button until all LEDs flash. After that, you must manually restart the device.

Table 8 – Reset button

3.6 SIM CARD

To insert or remove a SIM card in **AirGate 4G Wi-Fi**, you must do the following:

1. Ensure that the device is not being electrically powered.
2. Use a Phillips screwdriver to remove the protective cover from the device.
3. Insert the SIM card into the SIM socket.
4. Replace the protective cover.

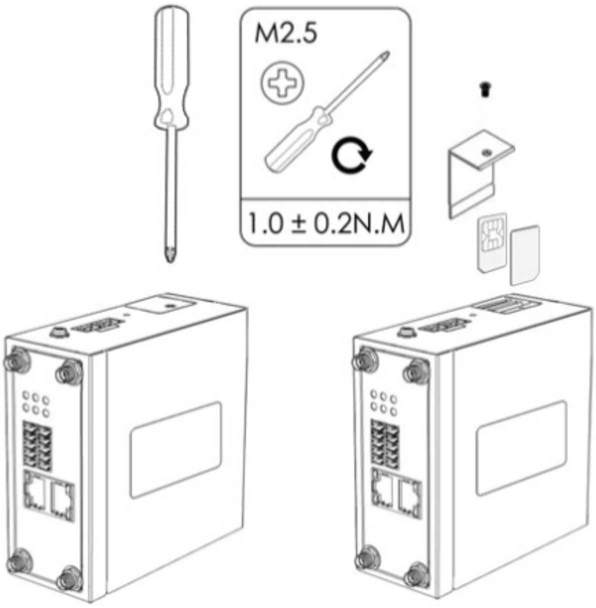


Figure 7 – Inserting SIM card

3.7 ANTENNAS

AirGate 4G Wi-Fi supports four antennas: two on Wi-Fi connectors for Wi-Fi functionality, one on MAIN connector and one on AUX connector, both for cellular connection.

Wi-Fi connectors are used to receive and transmit data wirelessly and their antennas should always be used together. The MAIN connector is used to receive and transmit data via cellular antenna. The AUX connector, in turn, is used to improve signal strength and depends on using an antenna on the MAIN connector to work.

How to connect the cellular antenna to the MAIN and AUX connectors of the device:

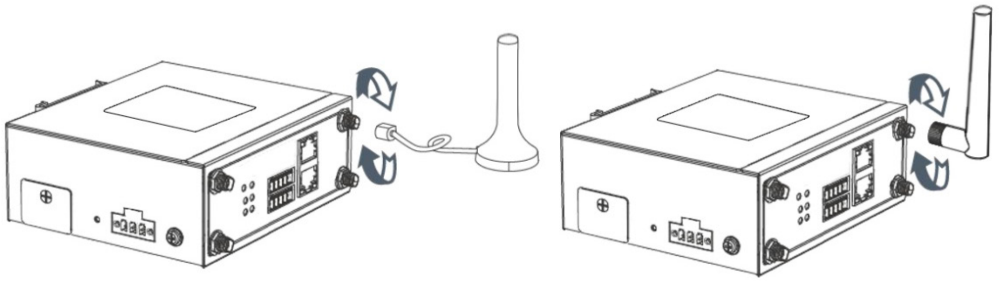


Figure 8 – Cellular antenna

How to connect the Wi-Fi antenna to the Wi-Fi connector of the device:

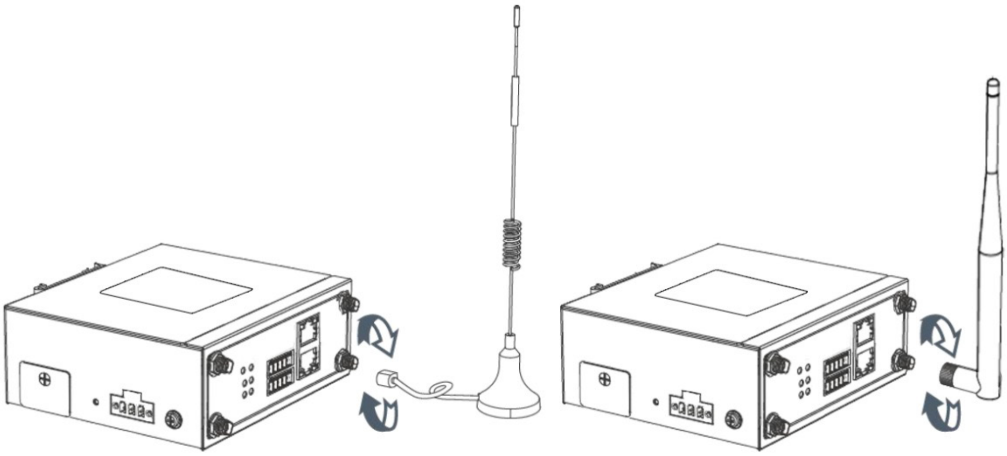


Figure 9 – Wi-Fi antenna

3.8 DIN RAIL

To mount the DIN rail kit, you must do the following:

1. Use four M3x6 flat head Phillips screws to fix the DIN rail kit to the device.
2. Insert the handle of the DIN rail bracket.
3. Press the device into the DIN rail until the bracket snaps into place.

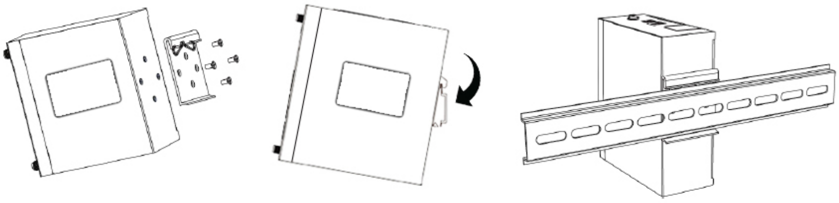


Figure 10 –DIN rail mounting

3.9 PROTECTIVE GROUNDING INSTALLATION

To install the grounding protection, you must do the following:

1. Remove the grounding screw.
2. Connect the grounding wire ring of the housing to the grounding pin.
3. Tighten the bolt screw.

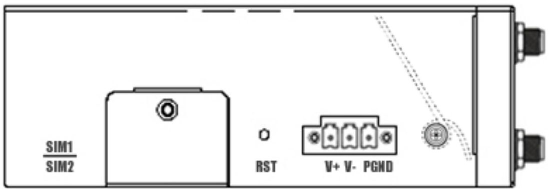


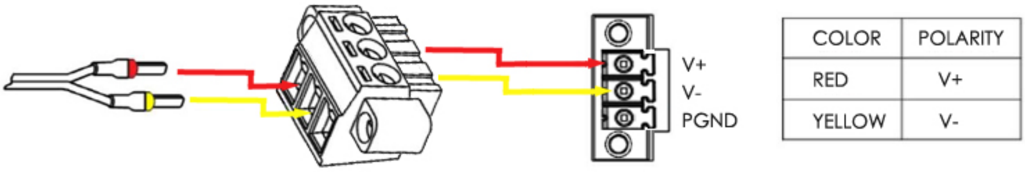
Figure 11 – Protective grounding

It is recommended that the device be grounded when installed.

3.10 POWER SUPPLY INSTALLATION

To install the power supply, you must do the following:

1. Remove the pluggable connector from the device.
2. Then loosen the screws for the locking flanges as needed.
3. Connect the wires of the power supply to the terminals.



COLOR	POLARITY
RED	V+
YELLOW	V-

Figure 12 – Power supply installation

3.11 TURN ON THE DEVICE

To turn the device, you must do the following:

1. Connect one end of the Ethernet cable to the device LAN port and the other end to the computer's LAN port.
2. Connect the AC source to a power source.
3. The device is ready for use when the SYS LED is flashing.

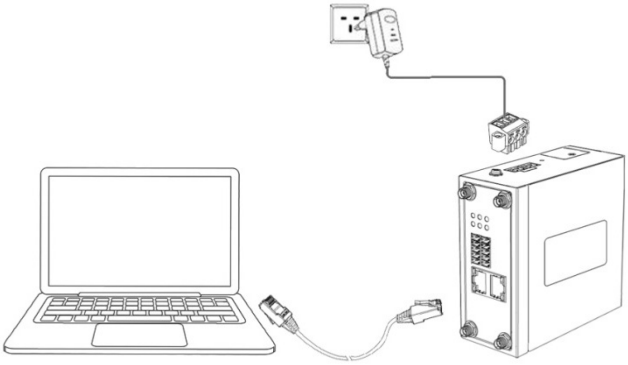


Figure 13 – Turning on the device

4 ACCESS TO WEB PAGE

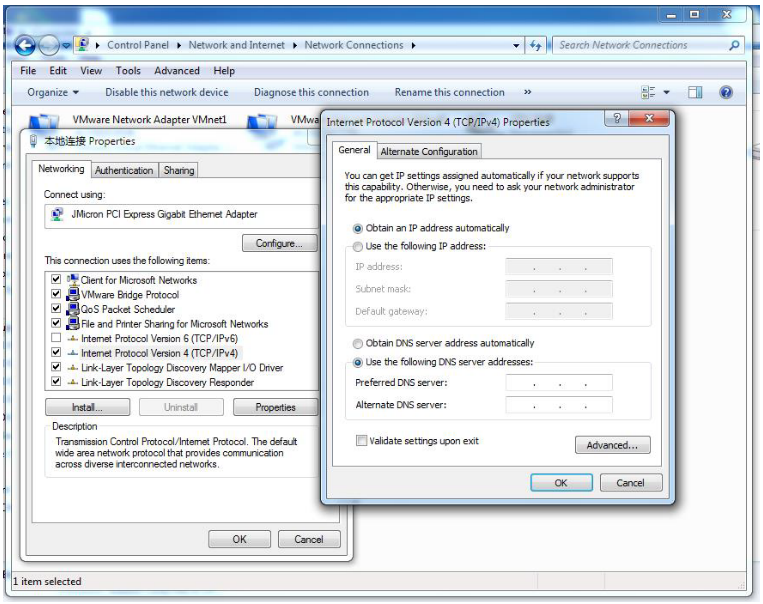
4.1 PC CONFIGURATION

AirGate 4G Wi-Fi has a DHCP server that will automatically assign an IP address to the user's computer. In some cases, it will be necessary to change the computer's network settings to accept the router's IP address. You can also manually configure the IP address.

The sections below provide information on setting up an IP for **AirGate 4G Wi-Fi** and how to make the first access to the device's web interface.

4.1.1 SET AN IP ADDRESS AUTOMATICALLY

You can set the device to automatically obtain an IP by following these steps:



Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
File Edit View Tools Advanced Help
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
VMware Network Adapter VMnet1
VMwa
本地连接 Properties
Networking Authentication Sharing
Configure...
Install... Uninstall Properties
OK Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General Alternate Configuration
Advanced...
OK Cancel
1 item selected

Connect using:
JMicron PCI Express Gigabit Ethernet Adapter

This connection uses the following items:
☑ Client for Microsoft Networks
☑ VMware Bridge Protocol
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

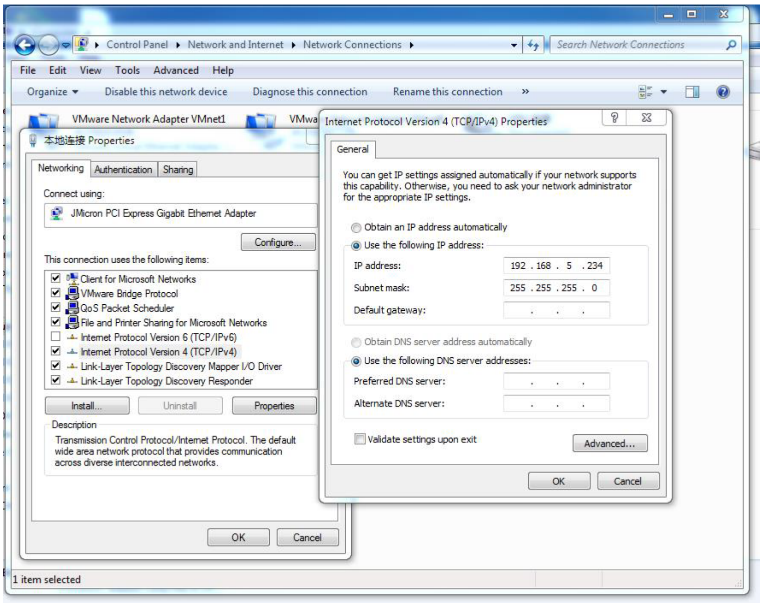
Figure 14 –Set an IP address automatically

Select **Start » Control Panel » Network Connections**. Right click **Local Area Connection** and select **Properties** to open the configuration dialog box for Local Area Connection. Select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP configuration window.

On the General tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to complete TCP/IP configuration.

4.1.2 SET AN STATIC IP ADDRESS

You can set your device to manually obtain an IP by following these steps:



Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
File Edit View Tools Advanced Help
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
VMware Network Adapter VMnet1
VMwa
本地连接 Properties
Networking Authentication Sharing
Configure...
Install... Uninstall Properties
OK Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Advanced...
OK Cancel
1 item selected

Connect using:
JMicron PCI Express Gigabit Ethernet Adapter

This connection uses the following items:
☑ Client for Microsoft Networks
☑ VMware Bridge Protocol
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 5 . 234
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Figure 15 – Set a static IP address

Click **Use the following IP address** to assign a static IP manually within the same subnet of the router.

Default Gateway and **DNS Server** are not necessary if PC not routing all traffic go through router.

4.2 FACTORY DEFAULT SETTINGS

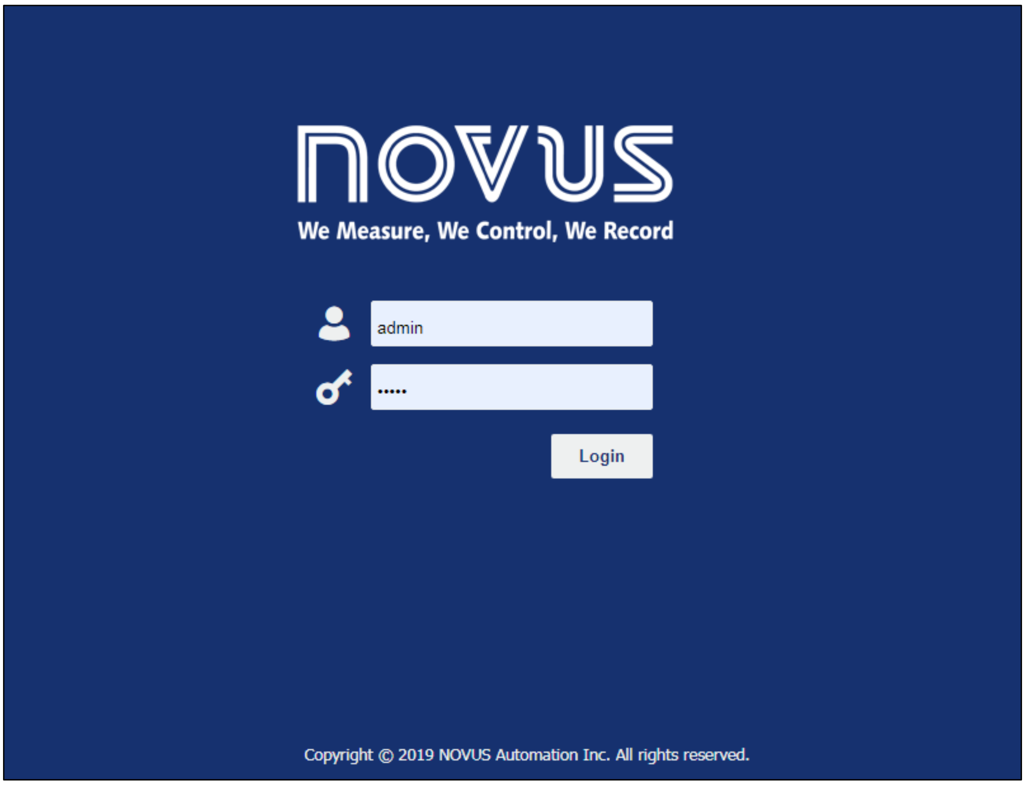
AirGate 4G Wi-Fi can be set up via a web page. The Graphical User Interface (GUI), presented in the LOGIN TO WEB PAGE section, allows you to manage and configure the device. During the first router configuration, the following default settings should be used:

- Username: **admin**
- Password: **admin**
- LAN IP Address: **192.168.5.1** (Eth0 ~ Eth1 as LAN mode)
- DHCP Server: **Enabled**

4.3 LOGIN TO WEB PAGE

To access **AirGate 4G Wi-Fi** setup page, you must open a web browser on your computer (Google Chrome or Internet Explorer are recommended) and enter IP 192.168.5.1 in the address bar.

After that, just use the same username and password (admin / admin) to access device settings.



admin

•••••

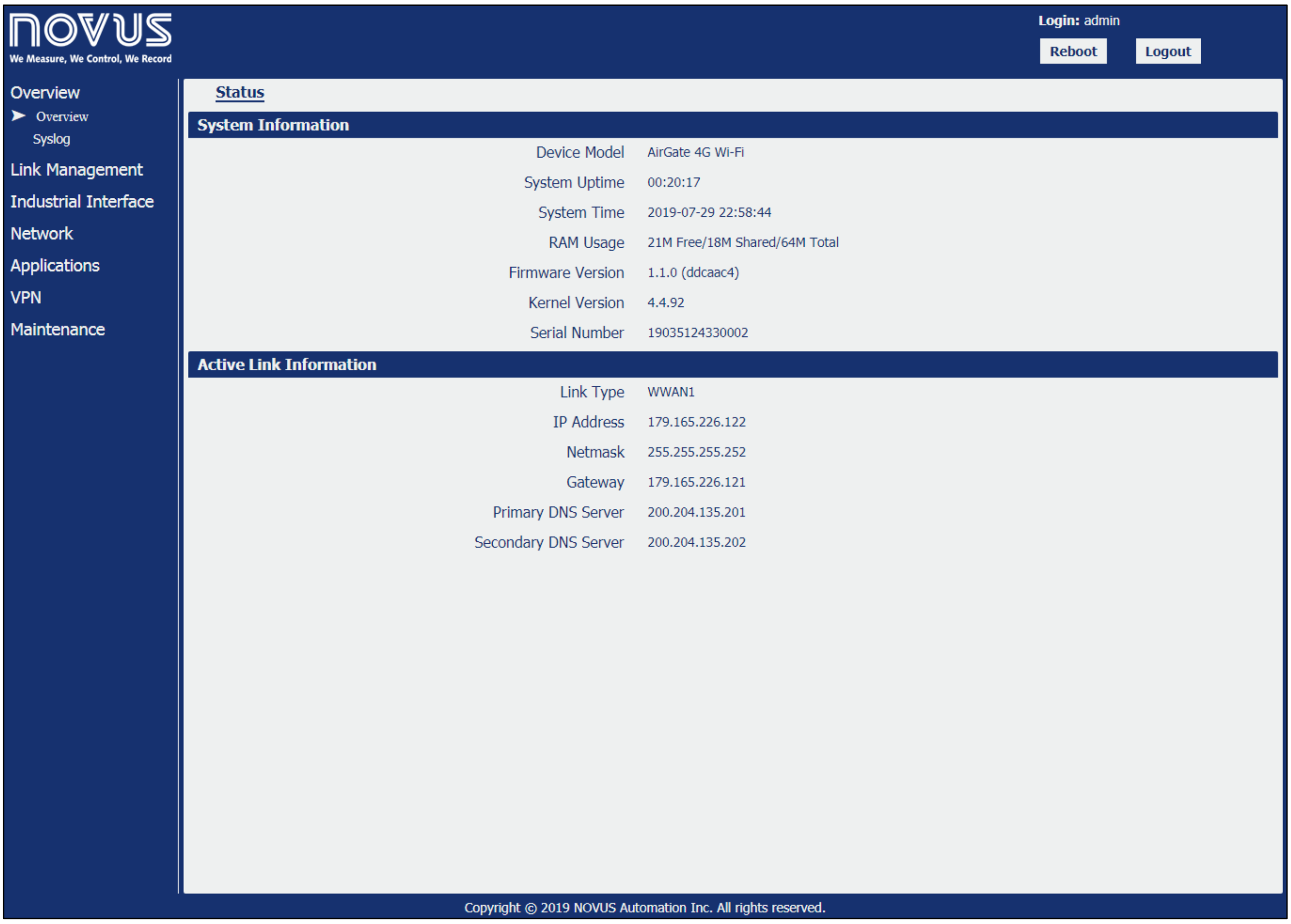
Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 16 – Login to Web page

5 WEB INTERFACE

5.1 WEB INTERFACE

AirGate 4G Wi-Fi router Web interface is divided into two sections: In the left pane is the main navigation menu and on the right is the content area for each page.



System Information

Device Model	AirGate 4G Wi-Fi
System Uptime	00:20:17
System Time	2019-07-29 22:58:44
RAM Usage	21M Free/18M Shared/64M Total
Firmware Version	1.1.0 (ddcaac4)
Kernel Version	4.4.92
Serial Number	19035124330002

Active Link Information

Link Type	WWAN1
IP Address	179.165.226.122
Netmask	255.255.255.252
Gateway	179.165.226.121
Primary DNS Server	200.204.135.201
Secondary DNS Server	200.204.135.202

Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 17 – Home page

The navigation menu may contain fewer sections than shown here depending on which options are installed in your device.

5.1.1 WEB PAGE BUTTONS

The **AirGate 4G Wi-Fi** configuration page contains the following buttons:

Figure 18 – Reboot and Logout buttons

- **Reboot:** Allows you to reboot the router.
- **Logout:** Allows you to logout the page.

Figure 19 – Save and Apply buttons

- **Save:** Allows you to save the settings applied to the current page.
- **Apply:** Allows you to apply the changes immediately made to the current page.

Figure 20 – Close button

- **Close:** Allows you to exit without changing the configuration on the current page.

5.2 OVERVIEW

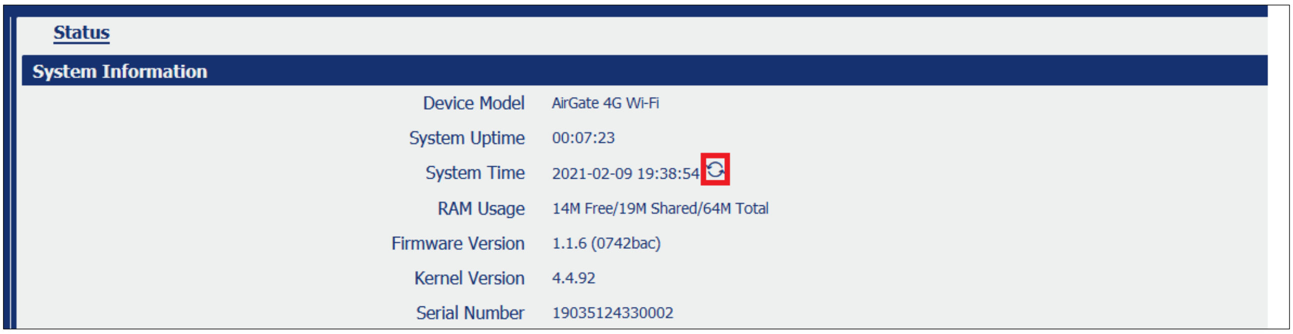
This section displays general information about the device and the system log files obtained by it.

5.2.1 STATUS

This tab allows displays information about the system and the current **AirGate 4G Wi-Fi** connection.

5.2.1.1 SYSTEM INFORMATION

This parameter group displays information about the system. Except for the time format, which supports time zone setting (see section SYSTEM → GENERAL), none of them are configurable.



Status

System Information

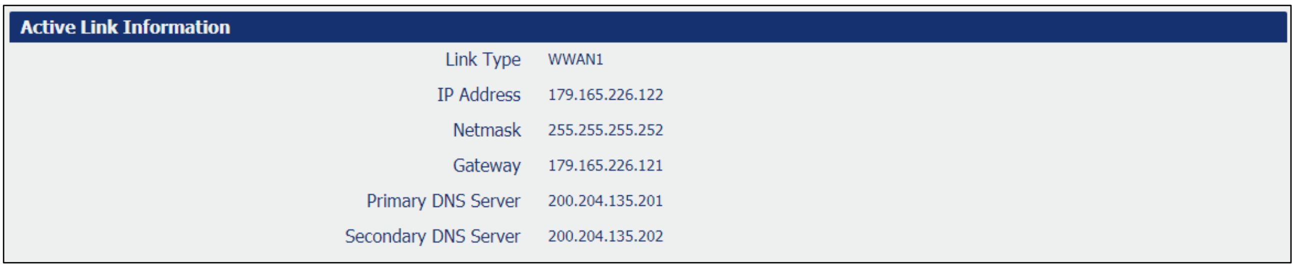
Device Model	AirGate 4G Wi-Fi
System Uptime	00:07:23
System Time	2021-02-09 19:38:54 ⟳
RAM Usage	14M Free/19M Shared/64M Total
Firmware Version	1.1.6 (0742bac)
Kernel Version	4.4.92
Serial Number	19035124330002

Figure 21 – System information

- **Device Module:** Displays the router model name.
- **System Uptime:** Displays the duration the system has been up in hours, minutes, and seconds.
- **System Time:** Displays the current date and time. The button ⟳ allows you to instantly synchronize the routers clock with the computers clock.
- **RAM Usage:** Displays the RAM capacity and the available RAM memory.
- **Firmware Version:** Displays the current firmware version of router.
- **Kernel Version:** Displays the current kernel version of router.
- **Serial Number:** Display the router serial number.

5.2.1.2 ACTIVE LINK INFORMATION

This parameter group provides information about the active **AirGate 4G Wi-Fi** connection, which can be configured throughout the next chapters.



Active Link Information

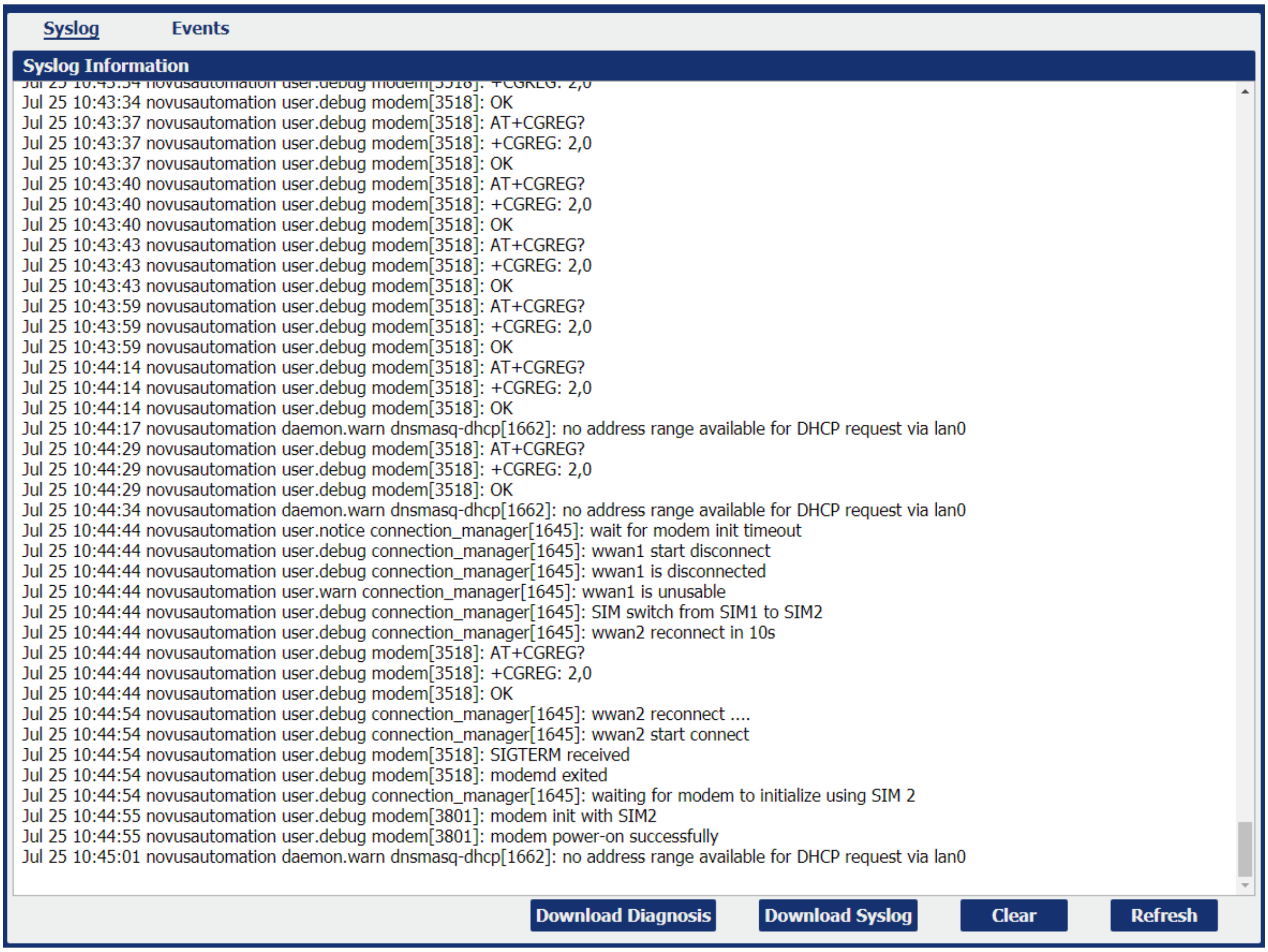
Link Type	WWAN1
IP Address	179.165.226.122
Netmask	255.255.255.252
Gateway	179.165.226.121
Primary DNS Server	200.204.135.201
Secondary DNS Server	200.204.135.202

Figure 22 – Active link information

- **Link Type:** Displays the current interface for Internet access.
- **IP Address:** Displays the IP address assigned to this interface.
- **Netmask:** Displays the subnet mask of this interface.
- **Gateway:** Displays the gateway of this interface.
- **Primary DNS Server:** Displays the primary DNS server of this interface.
- **Secondary DNS Server:** Displays the secondary DNS server of this interface.

5.2.2 SYSLOG

This feature allows you to view device system log data.



```
Jul 25 10:43:34 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:34 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:37 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:37 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:37 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:40 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:40 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:40 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:43 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:43 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:43 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:59 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:59 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:59 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:14 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:14 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:14 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:17 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
Jul 25 10:44:29 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:29 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:29 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:34 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
Jul 25 10:44:44 novusautomation user.notice connection_manager[1645]: wait for modem init timeout
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan1 start disconnect
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan1 is disconnected
Jul 25 10:44:44 novusautomation user.warn connection_manager[1645]: wwan1 is unusable
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: SIM switch from SIM1 to SIM2
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan2 reconnect in 10s
Jul 25 10:44:44 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:44 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:44 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: wwan2 reconnect ....
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: wwan2 start connect
Jul 25 10:44:54 novusautomation user.debug modem[3518]: SIGTERM received
Jul 25 10:44:54 novusautomation user.debug modem[3518]: modemd exited
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: waiting for modem to initialize using SIM 2
Jul 25 10:44:55 novusautomation user.debug modem[3801]: modem init with SIM2
Jul 25 10:44:55 novusautomation user.debug modem[3801]: modem power-on successfully
Jul 25 10:45:01 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
```

Figure 23 – Syslog

- **Download Diagnosis:** Allows you to download the diagnosis file for analysis. This function will create a compressed file with extension .en. The information, however, is confidential and, if necessary, must be sent to NOVUS Technical Support.
- **Download Syslog:** Allows you to download the complete syslog since last reboot.
- **Clear:** Allows you to clear the current page syslog.
- **Refresh:** Allows you to reload the current page.

5.3 LINK MANAGEMENT

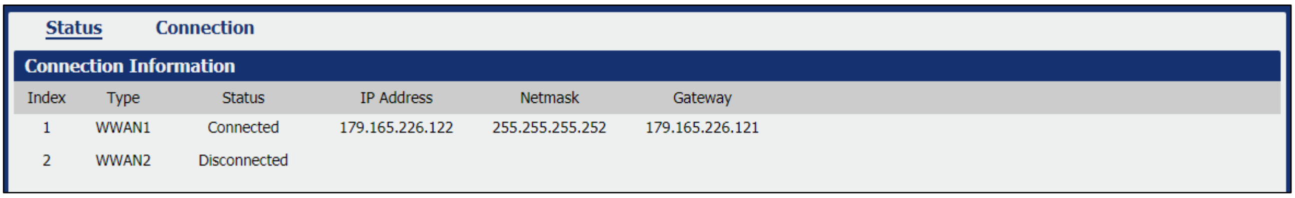
This section allows you to view information about device connection setup and management.

5.3.1 CONNECTION MANAGER

This tab allows you to view and manage the information of each connection configured for the device.

5.3.1.1 CONNECTION MANAGER → STATUS

This parameter group allows you to view information about the connections configured for the device. Each connection can be individually created, configured, or removed in the CONNECTION MANAGER → CONNECTION tab.



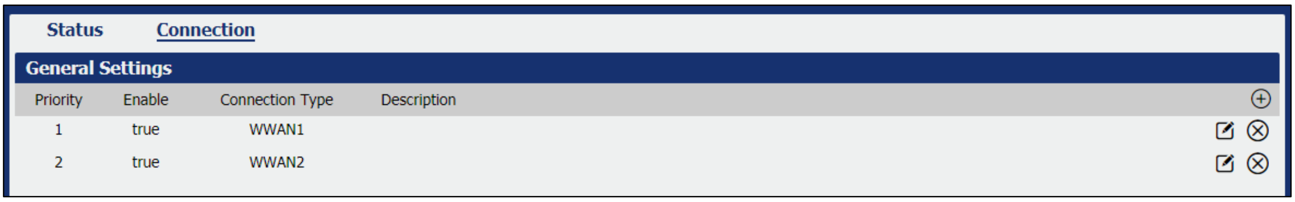
Index	Type	Status	IP Address	Netmask	Gateway
1	WWAN1	Connected	179.165.226.122	255.255.255.252	179.165.226.121
2	WWAN2	Disconnected			

Figure 24 – Connection information

- **Type:** Displays the connection interface.
- **Status:** Displays the connection status of this interface.
- **IP Address:** Displays the IP address of this interface.
- **Netmask:** Displays the netmask of this interface.
- **Gateway:** Displays the gateway of this interface. This is used for routing packets to remote networks.

5.3.1.2 CONNECTION MANAGER → CONNECTION

This parameter group allows you to add or delete connections, as well as edit parameters for connections previously created for the device.



Priority	Enable	Connection Type	Description	⊕
1	true	WWAN1		✎ ⊗
2	true	WWAN2		✎ ⊗

Figure 25 – Connection: General settings

This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new priority interface.

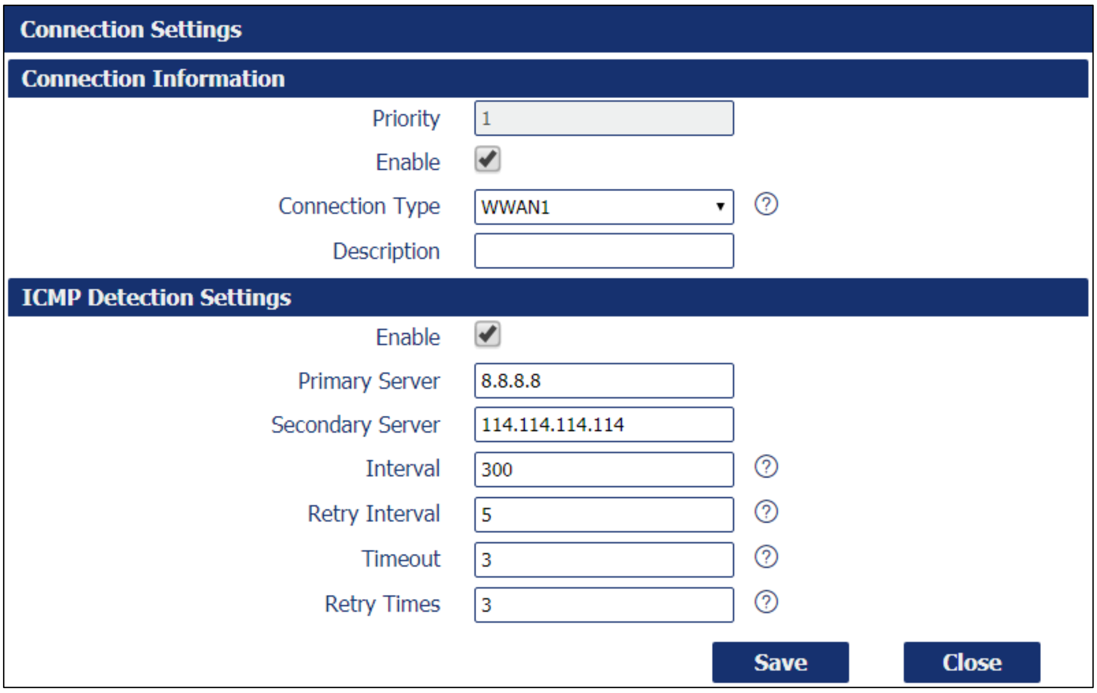
✎ **Button:** Allows you to edit current interface settings.

⊗ **Button:** Allows you to delete current interface settings.

This group displays the following parameters:

- **Priority:** Displays the priority list of default routing selection. The order of priorities will be defined by the order of creation of each connection, respecting the limit of three connections.
- **Enable:** Displays the connection enable status. Enabled connections will be displayed as "True" and disabled connections will be displayed as "False".
- **Connection Type:** Displays the name of this interface.
- **Description:** Displays the description of this connection.

As you can see in the figure below, you can create a new connection by clicking the ⊕ button.



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WWAN1
Description	

ICMP Detection Settings

Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 26 – Connection settings

GENERAL SETTINGS

This parameter group allows you to define the general connection settings.

- **Priority:** Displays current index on priority list. The order of priority will be defined by the connections creation order and cannot be manually changed.
- **Enable:** Allows you to enable or disable the connection.
- **Connection Type:** Allows you to define the connection type: "WWAN1", "WWAN2" or "WAN". It is recommended to specify the SIM1 operator link as "WWAN1" and the SIM2 operator link as "WWAN2".
- **Description:** Allows you to define a description for the connection.

ICMP DETECTION SETTINGS

This parameter group allows you to define the ICMP (Internet Control Message Protocol) protocol operation. The ICMP protocol is used to manage information about errors founded when a message is sent.

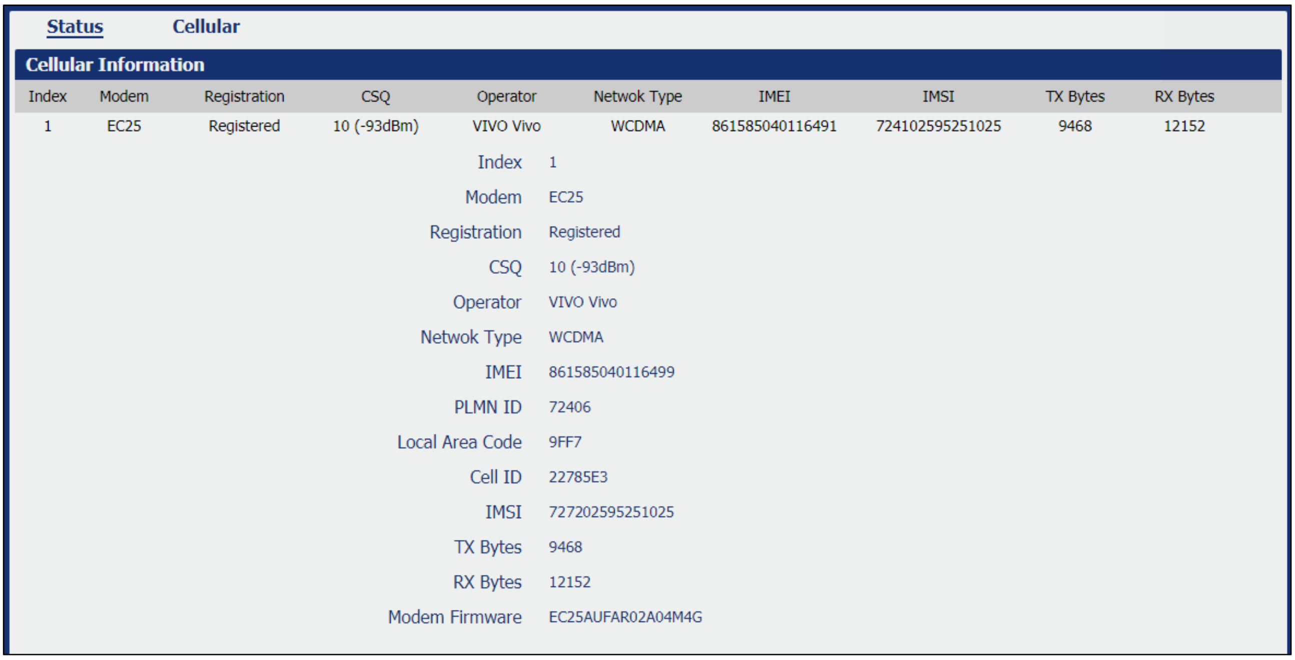
- **Enable:** Allows you to enable detection of link connection status based on pings to a specified IP address.
- **Primary Server:** Allows you to enter the primary IP address that pings will be sent to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g., 8.8.8.8).
- **Secondary Server:** Allows you to enter the secondary IP address that pings will be sent to, when the primary server is ping failed, router would try to ping the secondary server.
- **Interval:** Allows you to enter the duration of each ICMP detection (in seconds). 1 to 1800 second interval is allowed
- **Retry Interval:** Allows you to enter the interval in seconds between each ping if no packets have been received. 1 to 300 second retry interval is allowed.
- **Timeout:** Allows you to enter a timeout period, in seconds, for the response of received pings to determine ICMP detection failures. 1 to 10 seconds timeout is allowed.
- **Retry Times:** Allows you to specify the retry times for ICMP detection. 1 to 10 seconds retry times is allowed.

5.3.2 CELLULAR

This tab allows you to view and manage the SIM card information for the device.

5.3.2.1 CELLULAR → STATUS

This parameter group allows you to view information about cellular connections configured for the device. Each cellular connection can be individually created, configured, or removed on the CELLULAR → CELLULAR tab.



Cellular Information

Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	10 (-93dBm)	VIVO Vivo	WCDMA	861585040116491	724102595251025	9468	12152

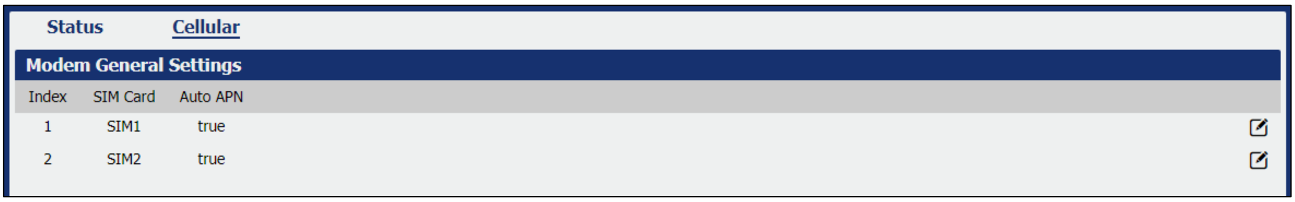
Index	1
Modem	EC25
Registration	Registered
CSQ	10 (-93dBm)
Operator	VIVO Vivo
Netwok Type	WCDMA
IMEI	861585040116499
PLMN ID	72406
Local Area Code	9FF7
Cell ID	22785E3
IMSI	727202595251025
TX Bytes	9468
RX Bytes	12152
Modem Firmware	EC25AUFAR02A04M4G

Figure 27 – Cellular information

- **Modem:** Displays the module of the modem used by this WWAN interface.
- **Registration:** Displays the registration status of SIM card.
- **CSQ:** Displays the signal strength of the carrier network.
- **Operator:** Displays the wireless network provider.
- **Network Type:** Displays the network type: "LTE" (Long Term Evolution), "UMTS" (Universal Mobile Telecommunications Service) or "CDMA" (Code Division Multiple Access).
- **IMEI:** Displays the IMEI (International Mobile Electronic Identifier). Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases, this will be blank.
- **PLMN ID:** Displays the current PLMN (Public Land Mobile Network) ID, including MCC (Mobile County Code), MNC (Mobile Network Code), LAC (Location Area Code) and Cell ID (Cell Identification).
- **Local Area Code:** Displays the location area code of the SIM card.
- **Cell ID:** Displays the Cell ID of the SIM card location.
- **IMSI:** International Mobile Subscriber Identity, as read from the SIM. This is the user's network subscription.
- **TX Bytes:** Displays the total bytes transmitted since the time the device was connected. **AirGate 4G Wi-Fi** router would record this data with same SIM card. Reboot would not erase this data.
- **RX Bytes** Displays the total bytes received since the time the device was connected. **AirGate 4G Wi-Fi** router would log this data with same SIM card. Reboot would not erase this data.
- **Modem Firmware:** Displays firmware version of the module used by the connection.

5.3.2.2 CELLULAR → CELLULAR

This parameter group allows you to configure the SIM cards parameters. **AirGate 4G Wi-Fi** supports up to two individually configured SIM cards for 2G, 3G or 4G connection.



Modem General Settings

Index	SIM Card	Auto APN
1	SIM1	true
2	SIM2	true

Figure 28 – Modem general settings

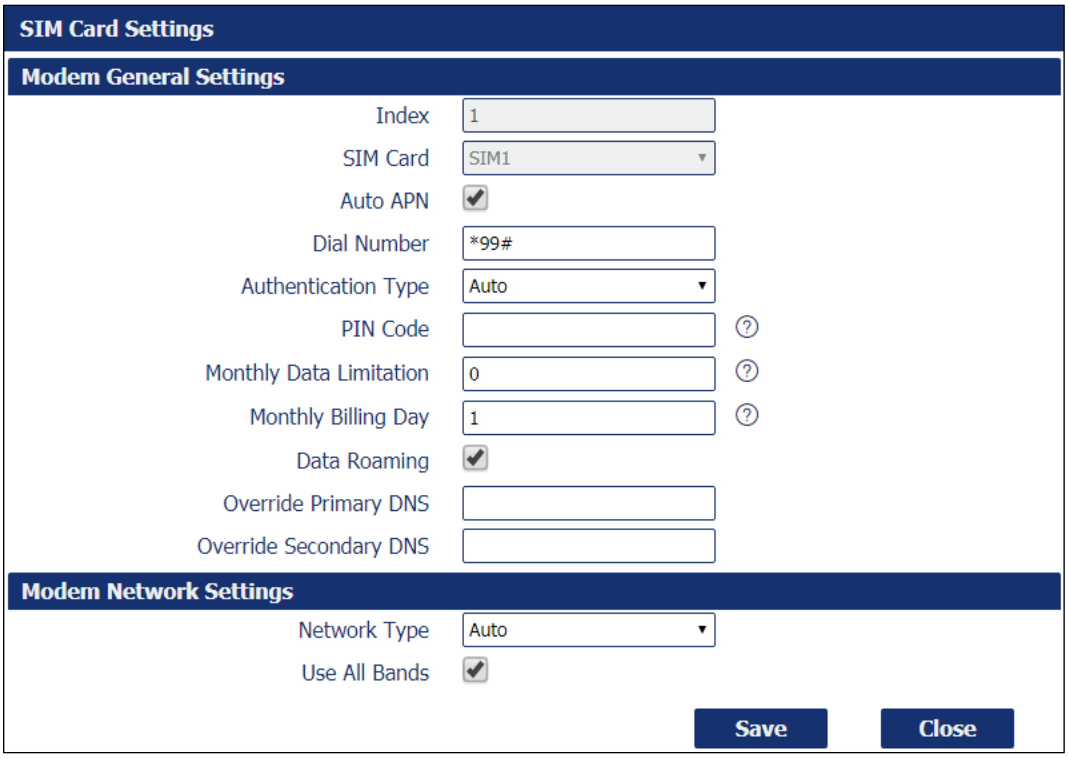
This parameter group has the following button:

✎ **Button:** Allows you to edit the settings of the selected SIM card.

This group displays the following parameters:

- **SIM Card:** Displays the SIM card support on this device.
- **Auto APN:** Displays the status of auto APN function.

As you can see in the figure below, you can edit a SIM card setting by clicking the ✎ button.



SIM Card Settings

Modem General Settings

Index	1
SIM Card	SIM1 ▾
Auto APN	☑
Dial Number	*99#
Authentication Type	Auto ▾
PIN Code	?
Monthly Data Limitation	0 ?
Monthly Billing Day	1 ?
Data Roaming	☑
Override Primary DNS	
Override Secondary DNS	

Modem Network Settings

Network Type	Auto ▾
Use All Bands	☑

Figure 29 – SIM card settings

SIM CARD GENERAL SETTINGS

- **SIM Card:** Displays the current SIM card settings.
- **Auto APN:** Allows you to enable auto checking the Access Point Name provided by the carrier.
- **APN:** You must manually add the APN to be used by the selected SIM card if **Auto APN** is disabled.
- **Username:** You must manually add the APN user to be used by the selected SIM card if **Auto APN** is disabled.
- **Password:** You must manually add the APN password to be used by the selected SIM card if **Auto APN** is disabled.
- **Dial Number:** Allows you to enter the dial number of the carrier.
- **Authentication Type:** Allows you to define the authentication method used by the carrier: "Auto", "PAP" (Password Authentication Protocol) or "CHAP" (Challenge Handshake Authentication Protocol).
- **PIN Code:** Allows you to enter a 4-8 characters PIN code to unlock the SIM.
- **Monthly Data Limitation:** Allows you to enter the data total amount for SIM card. SIM card switchover when data reach limitation. There is no limitation if set to "0".
- **Monthly Billing Day:** Allows you to enter the date of renew data amount every month. This parameter must remain disabled if set to "0".
- **Data Roaming:** Allows you to enable or disable the data roaming function on the router.
- **Override Primary DNS:** Allows you to enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS:** Allows you to enter the secondary DNS server will override the automatically obtained DNS.

SIM CARD NETWORK SETTINGS

- **Network Type:** Allows you to define the network type: "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only" or "4G First".
- **Use All Bands:** Allows you to enable all bands selection or choose specified bands. Otherwise, you can manually select the bands to be used.

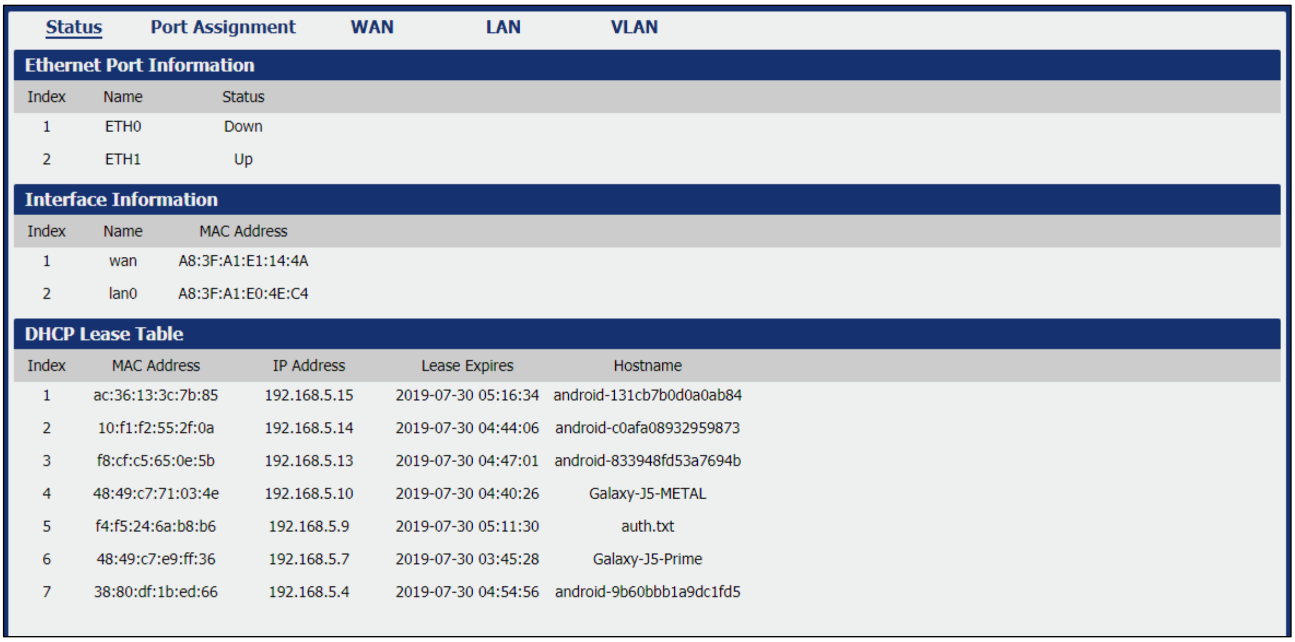
5.3.3 ETHERNET

This tab allows you to view and manage the information of Ethernet connection for the device.

5.3.3.1 ETHERNET → STATUS

This parameter group allows you to view general information about the device's Ethernet connection, such as the connection status of the Ethernet ports and the MAC address of the configured Ethernet interfaces.

As seen below, the IP addresses assigned by the DHCP server will be presented in a table. This table, created automatically by the DHCP server, is intended to store the IP address and MAC address of the receiving device - which will prevent the same IP from being delivered to the same device. Thus, the displayed lease period refers to the lease time of the IP addresses assigned to each device by the DHCP server.



Ethernet Port Information

Index	Name	Status
1	ETH0	Down
2	ETH1	Up

Interface Information

Index	Name	MAC Address
1	wan	A8:3F:A1:E1:14:4A
2	lan0	A8:3F:A1:E0:4E:C4

DHCP Lease Table

Index	MAC Address	IP Address	Lease Expires	Hostname
1	ac:36:13:3c:7b:85	192.168.5.15	2019-07-30 05:16:34	android-131cb7b0d0a0ab84
2	10:f1:f2:55:2f:0a	192.168.5.14	2019-07-30 04:44:06	android-c0afa08932959873
3	f8:cf:c5:65:0e:5b	192.168.5.13	2019-07-30 04:47:01	android-833948fd53a7694b
4	48:49:c7:71:03:4e	192.168.5.10	2019-07-30 04:40:26	Galaxy-J5-METAL
5	f4:f5:24:6a:b8:b6	192.168.5.9	2019-07-30 05:11:30	auth.txt
6	48:49:c7:e9:ff:36	192.168.5.7	2019-07-30 03:45:28	Galaxy-J5-Prime
7	38:80:df:1b:ed:66	192.168.5.4	2019-07-30 04:54:56	android-9b60bbb1a9dc1fd5

Figure 30 – Ethernet status

ETHERNET PORT INFORMATION

- **Name:** Displays the port physical connected states: "ETH0" or "ETH1".
- **Status:** Displays the status of the Ethernet port: If enabled, its status will be "Up". If disabled, its status will be "Down".

INTERFACE INFORMATION

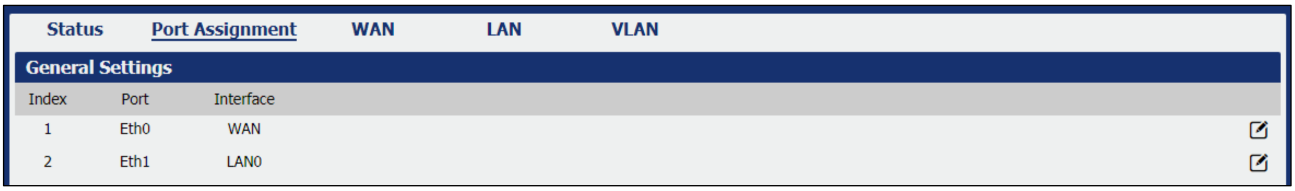
- **Name:** Displays the identification name of the Ethernet interface.
- **MAC Address:** Displays the MAC address of the Ethernet interface.
- **IP Address:** Displays the IP address of the Ethernet interface.

DHCP LEASE TABLE

- **MAC Address:** Displays the MAC address assigned to the device.
- **IP Address:** Displays the IP address assigned to the device.
- **Lease Expires:** Displays the lease time of the IP address assigned by the DHCP server.
- **Hostname:** Displays the hostname assigned to the device.

5.3.3.2 ETHERNET → PORT ASSINGMENT

This group of parameters allows you to edit the Ethernet ports of the device. **AirGate 4G Wi-Fi** supports up to two individually configured Ethernet ports.



Index	Port	Interface	
1	Eth0	WAN	✎
2	Eth1	LAN0	✎

Figure 31 – Port assignment

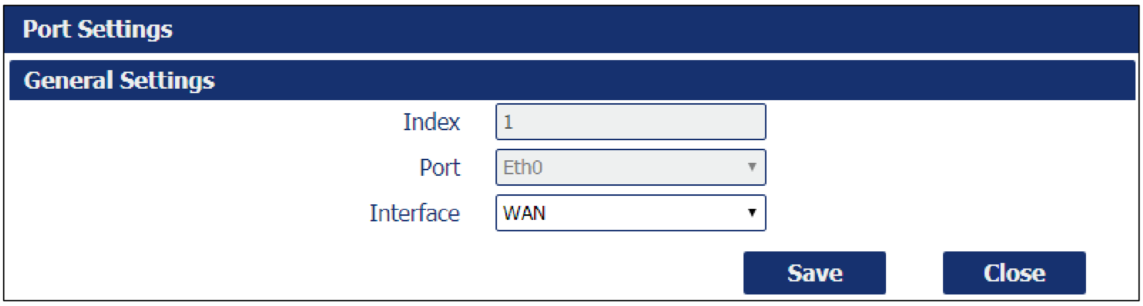
This parameter group has the following button:

✎ **Button:** Allows you to edit the settings of the selected Ethernet port.

This group displays the following parameters:

- **Port:** Displays the port states and numbers of this device: "ETH0" or "ETH1".
- **Interface:** Displays the interface configured for the Ethernet port: "LAN0", "LAN1" or "WAN".

As you can see in the figure below, you can edit the Ethernet port setting by clicking the ✎ button.



Index: 1

Port: Eth0

Interface: WAN

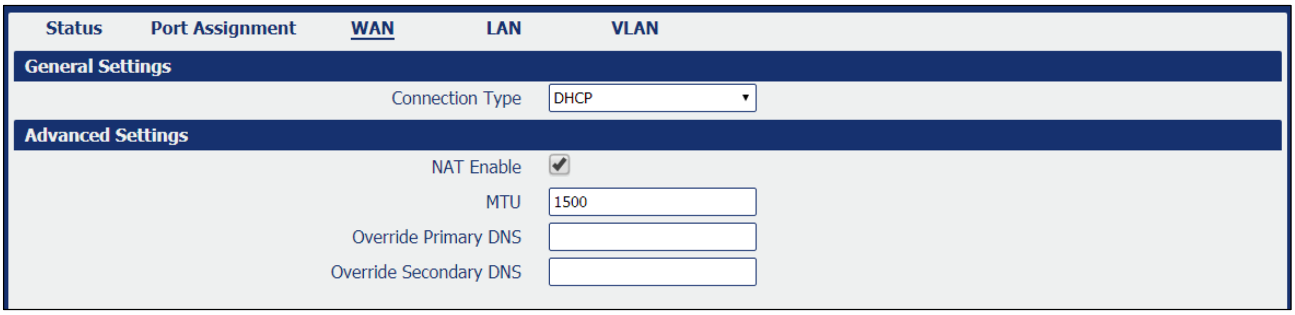
Figure 32 – Ethernet port settings

- **Port:** Displays the Ethernet port name configured.
- **Interface:** Allows you to configure an interface to the Ethernet port: "LAN0", "LAN1" or "WAN".

To be able to configure an interface as WAN, a configured LAN interface must already exist.

5.3.3.3 ETHERNET → WAN

This group of parameters allows you to edit the settings of the WAN (Wide Area Network) connection, used to cover a larger area, as opposed to the LAN (Local Area Network) connection.



Connection Type: DHCP

NAT Enable: ☑

MTU: 1500

Override Primary DNS:

Override Secondary DNS:

Figure 33 – WAN configuration: DHCP

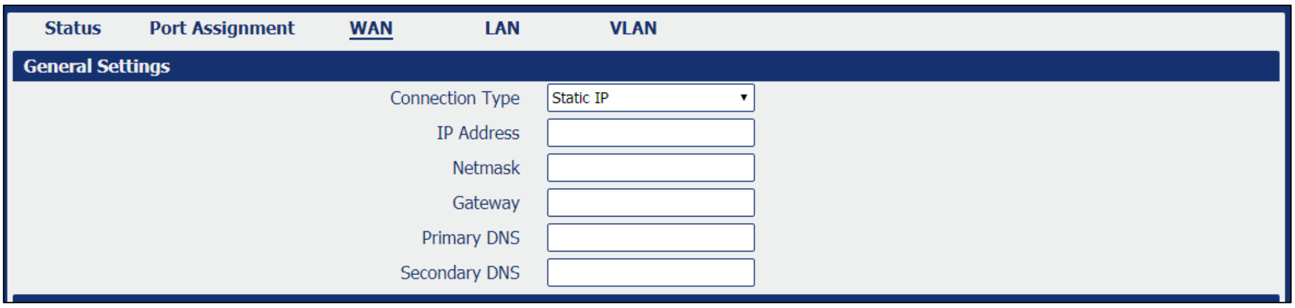
GENERAL SETTINGS

- **Connection Type:** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case, "DHCP", which will allow the external DHCP server to assign an IP address to this device.

ADVANCED SETTINGS

- **NAT Enable:** Allows you to enable or disable NAT (Network Address Translation).
- **MTU:** Allows you to define the maximum transmission device. In most cases you should leave the default value of 1024.
- **Override Primary DNS:** Allows you to enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS:** Allows you to enter the secondary DNS server will override the automatically obtained DNS.

If the **Connection Type** parameter is set to "Static IP", the following parameters will be displayed:



General Settings

Connection Type: Static IP

IP Address:

Netmask:

Gateway:

Primary DNS:

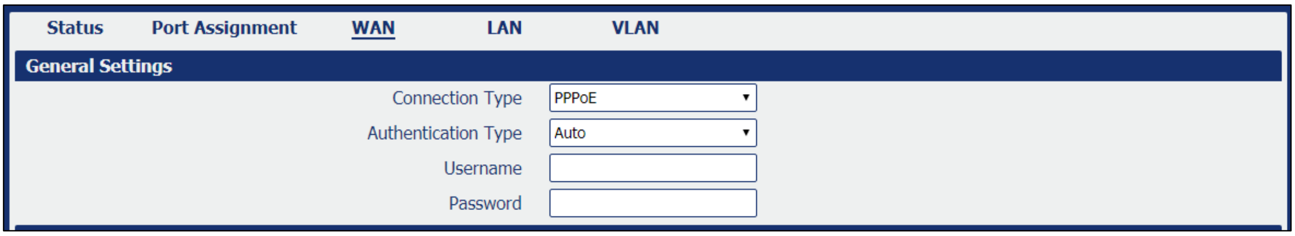
Secondary DNS:

Figure 34 – WAN configuration: Static IP

- **Connection Type** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case, "Static IP" will allow you to manually configure the IP.
- **IP Address:** Allows you to enter an IP address to be used for the WAN connection.
- **Netmask:** Allows you to enter a netmask to be used for the WAN connection.
- **Gateway:** Allows you to enter a gateway to be used for the WAN connection.
- **Primary DNS:** Allows you to enter a primary DNS to be used for the WAN connection.
- **Secondary DNS:** Allows you to enter a secondary DNS to be used for the WAN connection.

The **Advanced Settings** section parameters are the same as above and must be filled in the same way.

If the **Connection Type** parameter is set to "PPPoE" (Point-to-Point Protocol over Internet), the following parameters will be displayed:



General Settings

Connection Type: PPPoE

Authentication Type: Auto

Username:

Password:

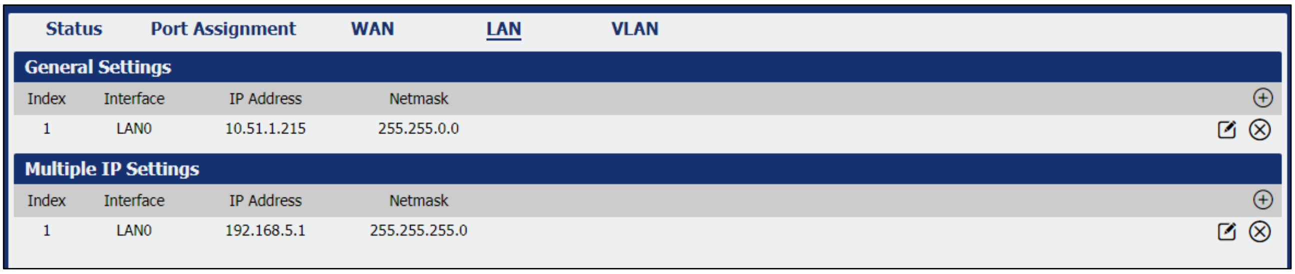
Figure 35 – WAN configuration: PPPoE

- **Connection Type:** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case, "PPPoE".
- **Authentication Type:** Allows you to define the type of authentication to be used by the WAN connection: "Auto", "PAP" (Password Authentication Protocol) or "CHAP" (Challenge Handshake Authentication Protocol).
- **Username:** Allows you to enter a username to be used by the WAN connection.
- **Password:** Allows you to enter a password to be used by the WAN connection.

The **Advanced Settings** section parameters are the same as above and must be filled in the same way.

5.3.3.4 ETHERNET → LAN

This group of parameters allows you to define the settings of the LAN (Local Area Network) connection, a local area network designed for smaller areas, as opposed to the WAN (Wide Area Network) connection.



General Settings

Index	Interface	IP Address	Netmask	⊕
1	LAN0	10.51.1.215	255.255.0.0	✎ ⊗

Multiple IP Settings

Index	Interface	IP Address	Netmask	⊕
1	LAN0	192.168.5.1	255.255.255.0	✎ ⊗

Figure 36 – LAN settings

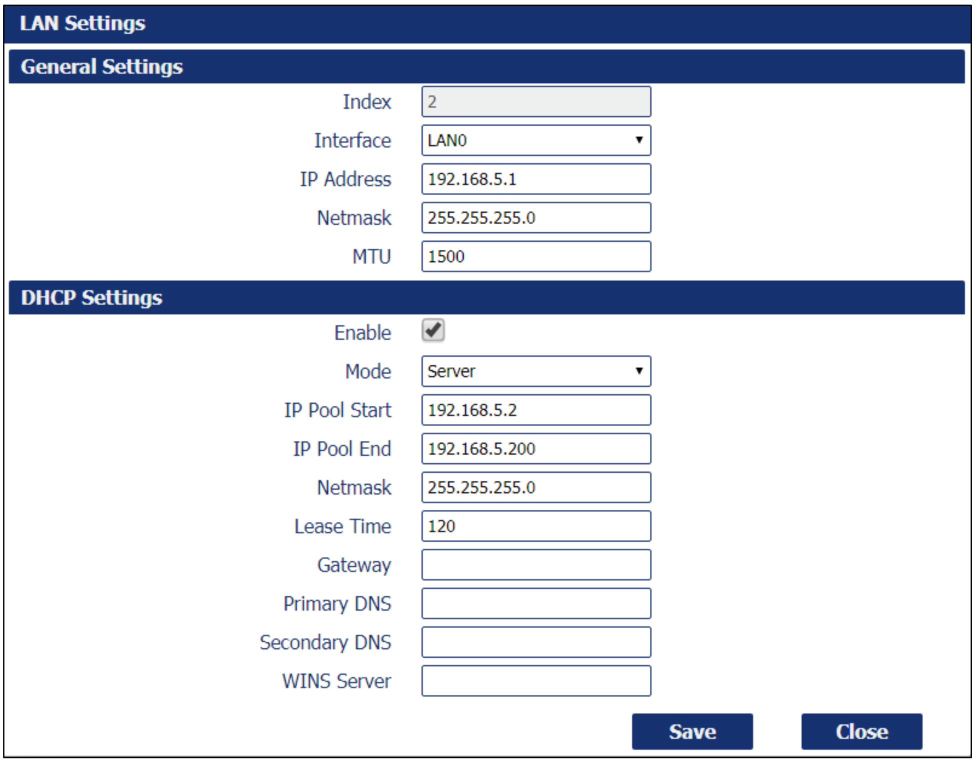
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new LAN connection.

✎ **Button:** Allows you to edit the current LAN connection settings.

⊗ **Button:** Allows you to delete the current LAN connection settings.

As you can see in the figure below, you can create a new LAN setting by clicking the ⊕ button.



LAN Settings

General Settings

Index	2
Interface	LAN0 ▾
IP Address	192.168.5.1
Netmask	255.255.255.0
MTU	1500

DHCP Settings

Enable	☑
Mode	Server ▾
IP Pool Start	192.168.5.2
IP Pool End	192.168.5.200
Netmask	255.255.255.0
Lease Time	120
Gateway	
Primary DNS	
Secondary DNS	
WINS Server	

Figure 37 – LAN settings

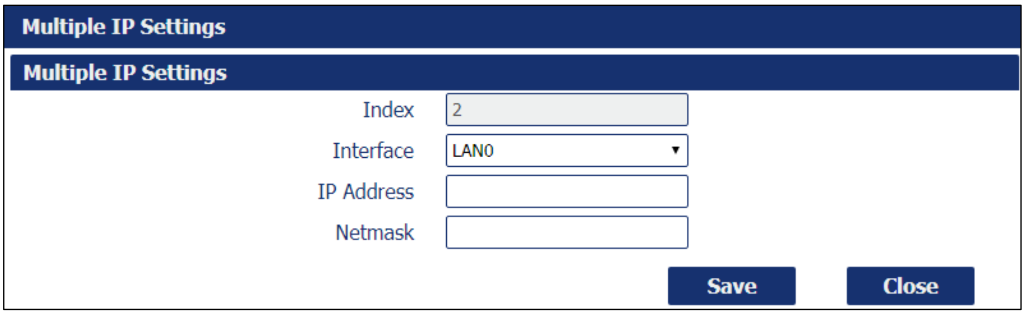
GENERAL SETTINGS

- **Interface:** Allows you to select the configure LAN port of this subnet.
- **IP Address:** Allows you to enter LAN IP address for this interface.
- **Netmask:** Allows you to enter the netmask for this subnet.
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

DHCP SETTINGS

- **Enable:** Allows you to enable or disable the DHCP feature of the current LAN port.
- **Mode:** Allows you to select the DHCP working mode: "Server" or "Relay".
- **Relay Server:** Allows you to enter the IP address of DHCP relay server.
- **IP Pool Start:** External LAN devices connected to this device will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.
- **IP Pool End:** External LAN devices connected to this device will be assigned IP address in this range when DHCP is enabled. This is the end of the pool of IP addresses.
- **Netmask:** Subnet mask of the IP address obtained by DHCP clients from DHCP server.
- **Lease Time:** The lease time of the IP address obtained by DHCP clients from DHCP server.
- **Gateway:** The gateway address obtained by DHCP clients from DHCP server.
- **Primary DNS:** Primary DNS server address obtained by DHCP clients from DHCP server.
- **Secondary DNS:** Secondary DNS server address obtained by DHCP clients from DHCP server.
- **WINS Server:** Windows Internet Naming Service obtained by DHCP clients from DHCP server.

As you can see in the figure below, you can create multiple IP settings by clicking the ⊕ button.



Multiple IP Settings

Multiple IP Settings

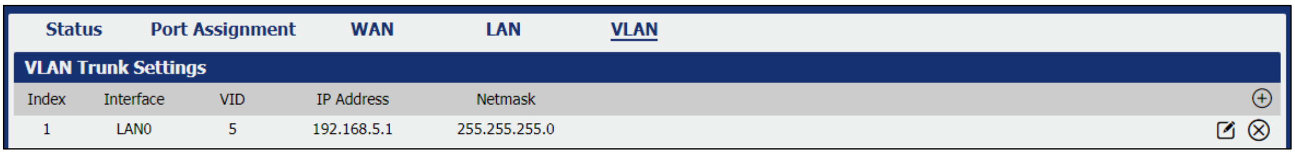
Index	2
Interface	LAN0
IP Address	
Netmask	

Figure 38 – Multiple IP settings

- **Interface:** Allows you to define a LAN port to be created.
- **IP Address:** Allows you to define an IP address for this network.
- **Netmask:** Allows you to define a netmask to be used.

5.3.3.5 ETHERNET → VLAN

This parameter group defines the VLAN (Virtual LAN) connection settings, a virtual local area network that enables physical network segmentation and grouping of multiple machines according to specific criteria.



VLAN Trunk Settings

Index	Interface	VID	IP Address	Netmask	⊕
1	LAN0	5	192.168.5.1	255.255.255.0	✎ ⊗

Figure 39 –VLAN Trunk settings

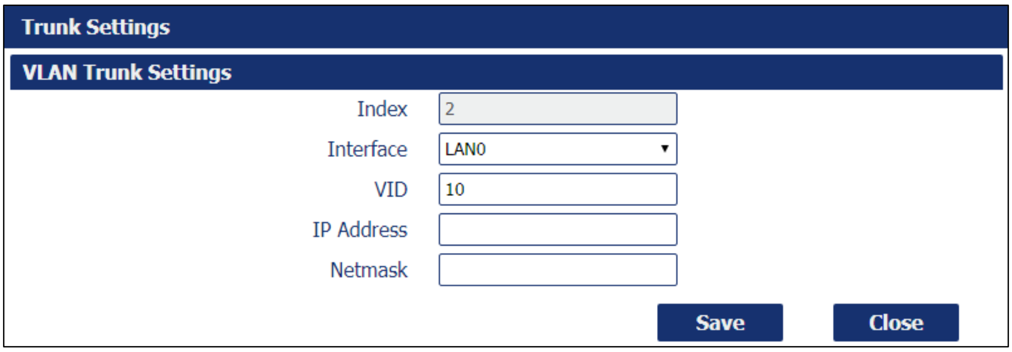
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new VLAN connection.

✎ **Button:** Allows you to edit the current VLAN connection.

⊗ **Button:** Allows you to delete the current VLAN connection.

As you can see in the figure below, you can create a new VLAN connection by clicking the ⊕ button.



Trunk Settings

VLAN Trunk Settings

Index	2
Interface	LAN0
VID	10
IP Address	
Netmask	

Figure 40 – Create a new VLAN connection

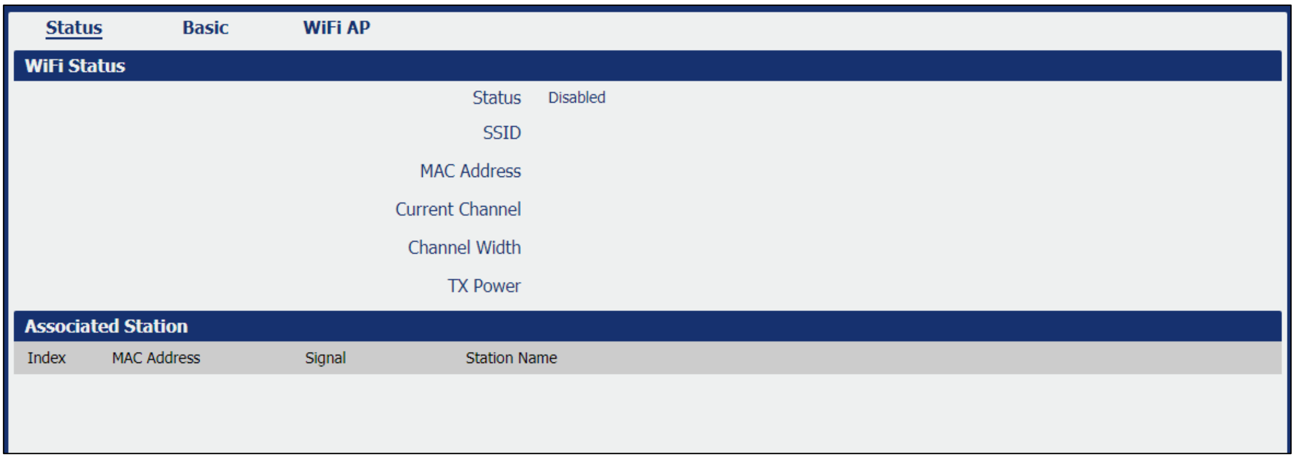
- **Interface:** Allows you to select the LAN port for VLAN trunk.
- **VID:** Allows you to define the VLAN ID for VLAN trunk.
- **IP Address:** Allows you to enter IP address for this VLAN trunk.
- **Netmask:** Allows you to enter subnet mask for this VLAN trunk.

5.3.4 WI-FI

This section allows you to view and manage information about the Wi-Fi connection and how the Wi-Fi interface works.

5.3.4.1 WI-FI → STATUS

This parameter group allows you to view information about the Wi-Fi connection and computers connected to the Wi-Fi network. In the section WI-FI → BASIC it is possible to define the operation mode of the Wi-Fi connection and to configure the other parameters.



Status	Disabled
SSID	
MAC Address	
Current Channel	
Channel Width	
TX Power	

Index	MAC Address	Signal	Station Name

Figure 41 – Wi-Fi status

WI-FI STATUS

- **Status:** Displays the Wi-Fi connection status.
- **SSID:** Display the SSID (Service Set Identifier), that is, the identifier name assigned to the Wi-Fi connection.
- **MAC Address:** Displays the MAC address of the Wi-Fi connection.
- **Current Channel:** Displays the current channel of the Wi-Fi connection.
- **Channel Width:** Displays the current width of the Wi-Fi connection.
- **TX Power:** Displays TX power (in dBm) as configured for the Wi-Fi connection.

ASSOCIATED STATION

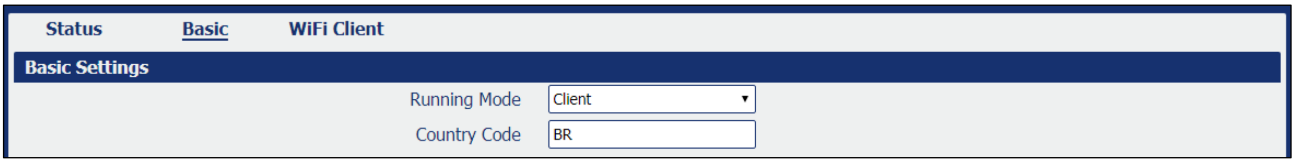
- **MAC Address:** Displays the MAC address of the device connected to the Wi-Fi network.
- **Signal:** Displays the quality of the Wi-Fi signal obtained by the computer connected to the network.
- **Station Name:** Displays the name of the workstation connected to the Wi-Fi network.

5.3.4.2 WI-FI → BASIC

This parameter group allows you to configure how the Wi-Fi connection of the device works. **AirGate 4G Wi-Fi** can be configured to function as a Wi-Fi Client or as a Wi-Fi Access Point, but does not support both configurations simultaneously.

If the device is configured as "Access Point", proceed to chapter WI-FI → WI-FI AP.

If the device is configured as "Client", proceed to the chapter WI-FI → WI-FI CLIENT.



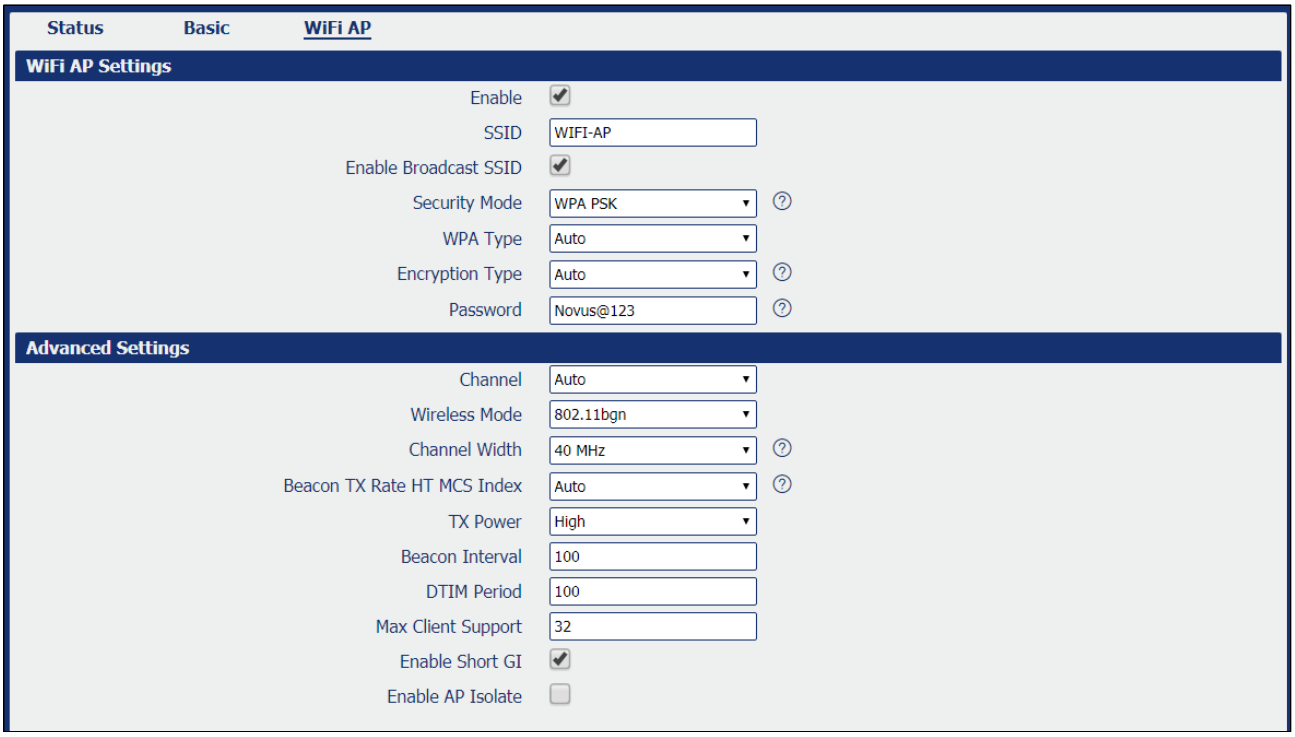
Running Mode	Client ▾
Country Code	BR

Figure 42 – Basic settings

- **Running Mode:** Allows you to select the running mode of Wi-Fi connection: "Access Point" or "Client".
- **County Code:** Allows you to enter the country where the device is located.

5.3.4.3 WI-FI → WI-FI AP

This parameter group allows you to edit the Wi-Fi access point settings of the device.



WiFi AP Settings

Enable	☑
SSID	WIFI-AP
Enable Broadcast SSID	☑
Security Mode	WPA PSK
WPA Type	Auto
Encryption Type	Auto
Password	Novus@123

Advanced Settings

Channel	Auto
Wireless Mode	802.11bgn
Channel Width	40 MHz
Beacon TX Rate HT MCS Index	Auto
TX Power	High
Beacon Interval	100
DTIM Period	100
Max Client Support	32
Enable Short GI	☑
Enable AP Isolate	□

Figure 43 – Wi-Fi Access Point

WI-FI AP SETTINGS

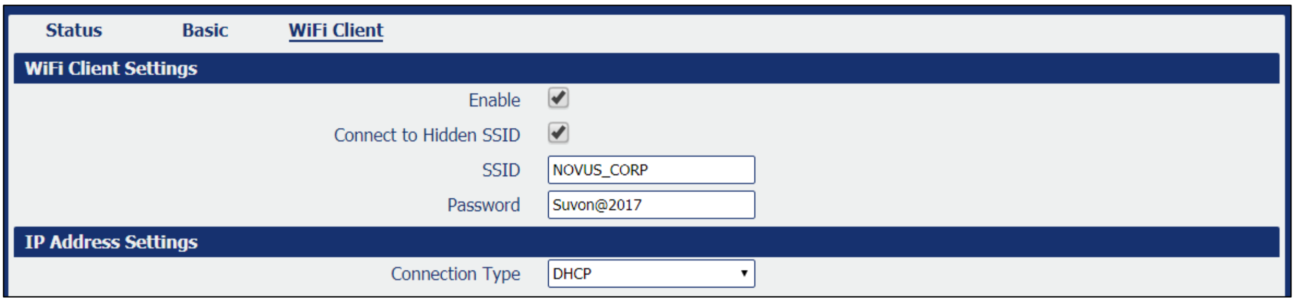
- **Enable:** Allows you to enable or disable the Wi-Fi interface.
- **SSID:** Allows you to define the SSID (Service Set Identifier), that is, the identifier name assigned to the Wi-Fi connection. Devices connected to the **AirGate 4G Wi-Fi** Wi-Fi access will identify the Access Point by this SSID.
- **Enable Broadcast SSID:** Allows you to enable or disable the SSID broadcast. When this function is disabled, other wireless devices cannot find the SSID, and users must enter the SSID manually.
- **Security Mode:** Allows you to select the connection security mode: "None", "WEP" or "WPA PSK".
- **WPA Type:** Allows you to select the WPA connection: "Auto", "WPA" or "WPA2".
- **Encryption Type:** Allows you to select the connection encryption type: "Auto", "TKIP" or "CCMP". Because these options depend on the authentication method selected, some options will not be available.
- **Password:** Allows you to enter the pre-shared key of WEP/WPA encryption.

ADVANCED SETTINGS

- **Channel:** Allows you to select the Wi-Fi channel to be transmitted. If there are other Wi-Fi devices in the area, **AirGate 4G Wi-Fi** should be set to a different channel than the other access points. Channels available for selection depend on the selected Band.
- **Wireless Mode:** Allows you to select the Wi-Fi 802.11 mode: "B", "G" or "N". Available selections depend on selected Band.
- **Chanel Width:** Allows you to select the width of the Wi-Fi channel. 20 MHz will limit the channel to 20 MHz wide; 20/40 MHz will enable the use of a 40 MHz wide channel when available.
- **Beacon TX Rate HT MCS Index:** Modulation and Coding Scheme, the MCS modulation coding table is a representation proposed by 802.11n to characterize the communication rate of the WLAN. The MCS takes the factors affecting the communication rate as the columns of the table and uses the MCS index as a row to form a rate table.
- **TX Power:** Allows you to select the transmission power for the access point: "High", "Medium" or "Low".
- **Beacon Interval:** Allows you to enter the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.
- **DTIM Period:** Allows you to enter the delivery traffic indication message period and the router AP will multicast the data according to this period.
- **Max Client Support:** Allows you to enter the maximum number of clients to access when the router is configured as access point.
- **Enable Short GI:** Allows you to enable or disable Short GI (guard interval), providing a long buffer time for signal delay.
- **Enable AP Isolate:** Allows you to enable or disable access point isolate. The route will isolate all connected wireless devices.

5.3.4.4 WI-FI → WI-FI CLIENT

This parameter group allows you to edit the Wi-Fi Client mode settings of the device.



WiFi Client Settings

Enable ☑

Connect to Hidden SSID ☑

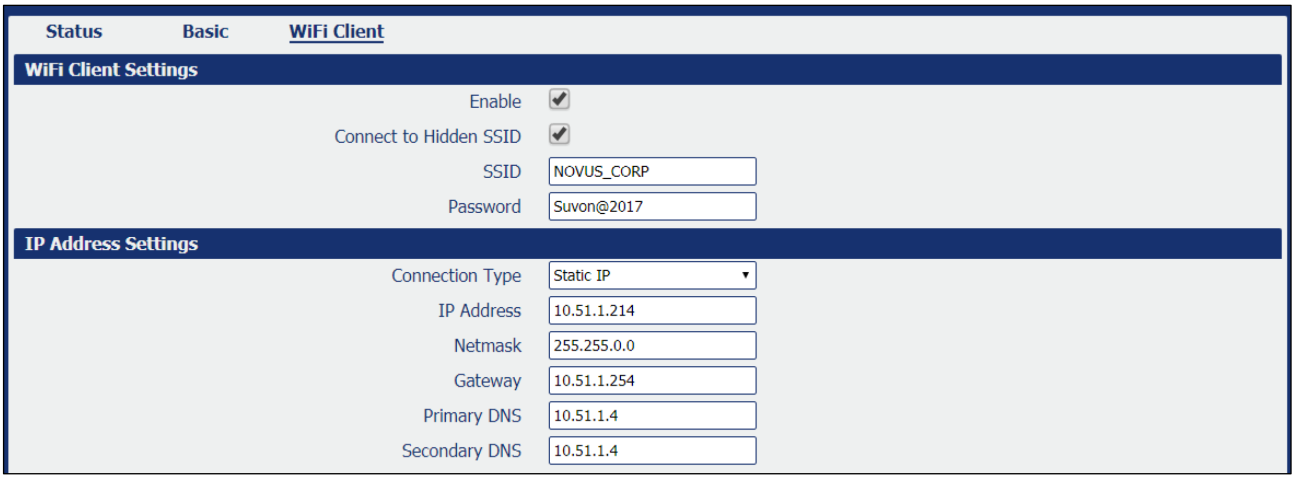
SSID: NOVUS_CORP

Password: Suvon@2017

IP Address Settings

Connection Type: DHCP

Figure 44 – Wi-Fi client: DHCP



WiFi Client Settings

Enable ☑

Connect to Hidden SSID ☑

SSID: NOVUS_CORP

Password: Suvon@2017

IP Address Settings

Connection Type: Static IP

IP Address: 10.51.1.214

Netmask: 255.255.0.0

Gateway: 10.51.1.254

Primary DNS: 10.51.1.4

Secondary DNS: 10.51.1.4

Figure 45 – Wi-Fi client: Static IP

WI-FI CLIENT SETTINGS

- **Enable:** Allows you to enable or disable the Wireless interface.
- **Connect to Hidden SSID:** Allows you to enable or disable connect to hidden SSID.
- **SSID:** Allows you to enter the password of external access point.
- **Password:** Allows you to enter the password of external access point.

IP ADDRESS SETTINGS

- **Connection Type:** Allows you to select the connection type: "DHCP Client" or "Static IP".
- **IP Address:** Allows you to enter the static address for this interface. It must be on the same subnet as the gateway.
- **Netmask:** Allows you to define the netmask to be assigned by the gateway.
- **Gateway:** Allows you to enter the IP address of the gateway.
- **Primary DNS:** Allows you to enter the primary DNS server, which will override the automatically obtained DNS.
- **Secondary DNS:** Allows you to enter the secondary DNS server, which will override the automatically obtained DNS.

5.4 INDUSTRIAL INTERFACE

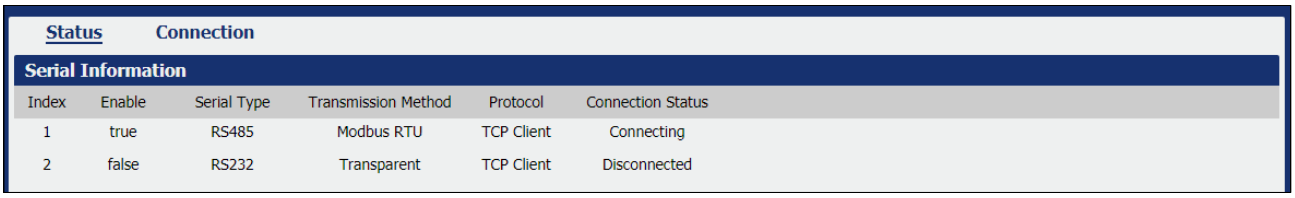
This section shows information about configuring RS232 and RS485 interfaces and device digital input and output.

5.4.1 SERIAL

This section shows information about configuring RS232 and RS485 interfaces and device digital input and output.

5.4.1.1 SERIAL → STATUS

This parameter group allows you to view information about device serial interfaces.



Serial Information

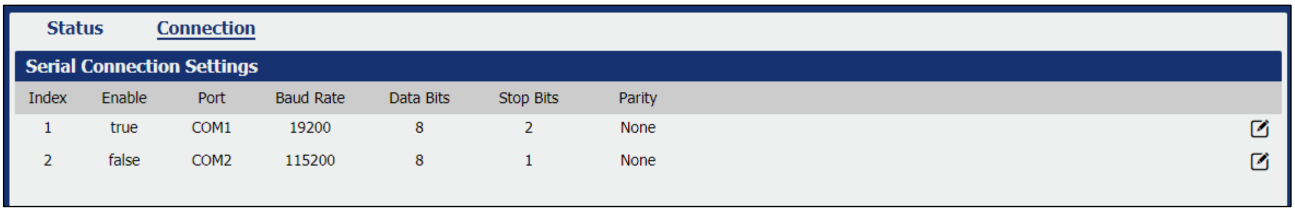
Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	true	RS485	Modbus RTU	TCP Client	Connecting
2	false	RS232	Transparent	TCP Client	Disconnected

Figure 46 – Serial information

- **Enable:** Displays the interface serial status.
- **Serial Type:** Displays the serial type of the COM port.
- **Transmission Method:** Displays the transmission method of the serial port.
- **Protocol:** Displays the protocol of the serial port.
- **Connection Status:** Displays the connection status of the serial port.

5.4.1.2 SERIAL → CONNECTION

This parameter group allows you to view information about device COM port connections.



Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity	
1	true	COM1	19200	8	2	None	✎
2	false	COM2	115200	8	1	None	✎

Figure 47 – Serial connection settings

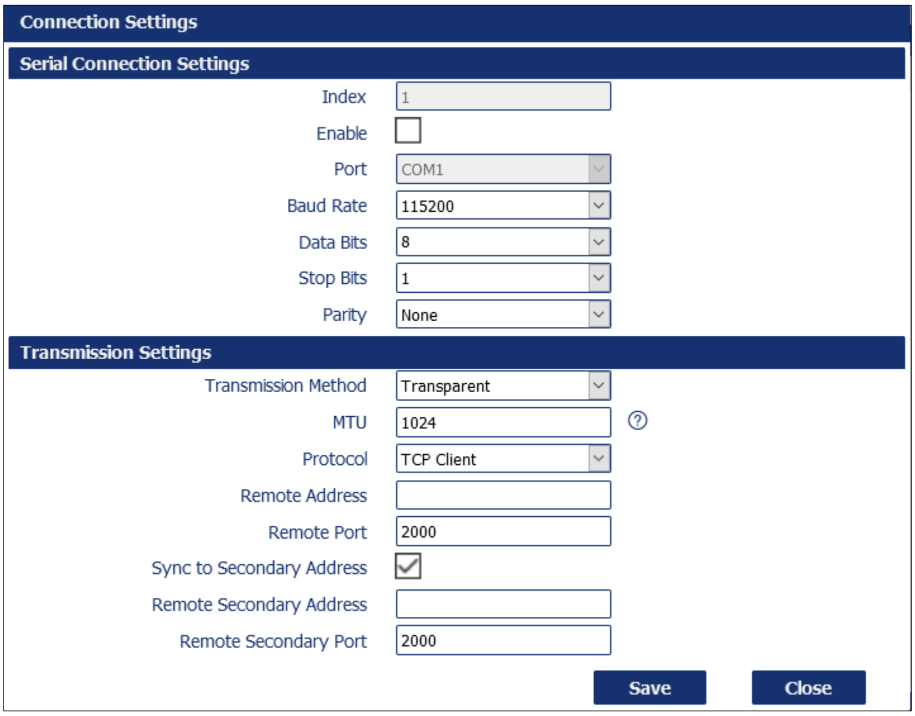
This parameter group has the following buttons:

✎ **Button:** Allows you to edit the settings of the serial port.

This group displays the following parameters:

- **Enable:** Displays the connection status of the serial port.
- **Port:** Displays the serial type of the serial port.
- **Baud Rate:** Displays the Baud Rate set for the serial port.
- **Data Bits:** Displays the data bits set for the serial port.
- **Stop Bits:** Displays the stop bits set for the serial port.
- **Parity:** Displays the parity set for the serial port.

As you can see in the figure below, you can edit the settings of the selected serial port by clicking the ✎ button.



Connection Settings

Serial Connection Settings

Index: 1

Enable: □

Port: COM1

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: None

Transmission Settings

Transmission Method: Transparent

MTU: 1024

Protocol: TCP Client

Remote Address:

Remote Port: 2000

Sync to Secondary Address: ☑

Remote Secondary Address:

Remote Secondary Port: 2000

Figure 48 – Serial port connection settings

SERIAL CONNECTION SETTINGS

- **Enable:** Allows you to enable or disable the serial port.
- **Port:** Displays the serial type of the serial port.
- **Baud Rate:** Allows you to define the Baud Rate for the serial port: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to define the data bits set for the serial port. Select the values from 7 or 8.
- **Stop Bits:** Allows you to define the stop bits for the serial port. Select the values from 1 or 2.
- **Parity:** Allows you to define the parity for the serial port: "None", "Even" or "Odd".

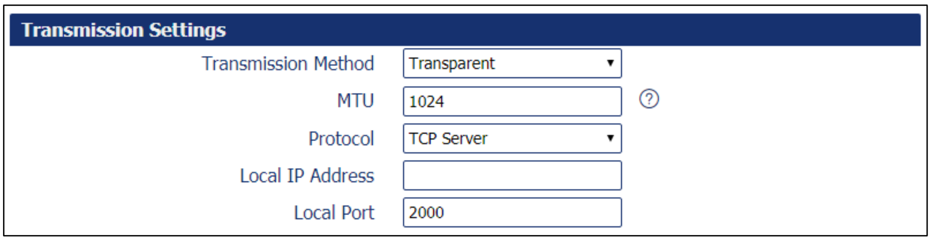
TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "TCP Client".

- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Client".
- **Remote IP Address:** Allows you to enter the IP address of the remote server.
- **Remote Port:** Allows you to enter the port number of the remote server.
- **Sync To Secondary Address:** Allows you to enable or disable a second remote server for data transmission.
- **Remote Secondary Address:** Allows you configure the IP address of the second remote server.
- **Remote Secondary Port:** Allows you configure the port number of the second remote server.

TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "TCP Server".



Transmission Settings

Transmission Method: Transparent

MTU: 1024

Protocol: TCP Server

Local IP Address:

Local Port: 2000

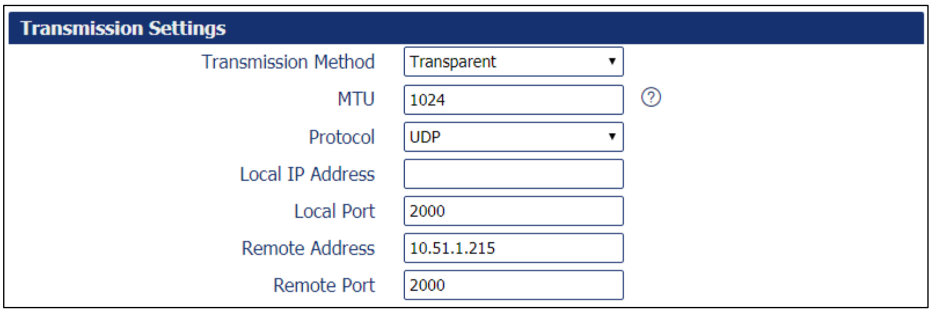
Figure 49 – TCP Server protocol

- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.

- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Server".
- **Local IP Address:** Allows you to enter the IP address of the local endpoint.
- **Local Port:** Displays the port number assigned to the serial IP port on which communications will take place.

TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "UDP".



Transmission Settings

Transmission Method	Transparent ▾
MTU	1024
Protocol	UDP ▾
Local IP Address	
Local Port	2000
Remote Address	10.51.1.215
Remote Port	2000

Figure 50 – UDP Protocol

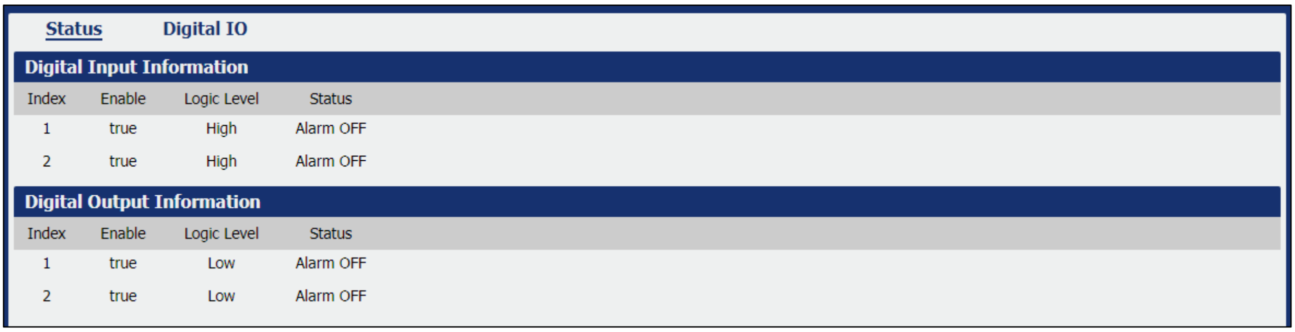
- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Server".
- **Local IP Address:** Allows you to enter the IP address of the local endpoint.
- **Local Port:** Displays the port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address:** Allows you to enter the IP address of the remote server.
- **Remote Port:** Allows you to enter the port number of the remote server.

5.4.2 DIGITAL I/O

This section allows you to configure digital input and output parameters. The digital input can be used to trigger alarms. The digital output, in turn, can be used to control the slave device by means of the digital signal. This control can be performed remotely via SMS or via a MQTT command.

5.4.2.1 DIGITAL I/O → STATUS

This parameter group allows you to view digital input and output information.



Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

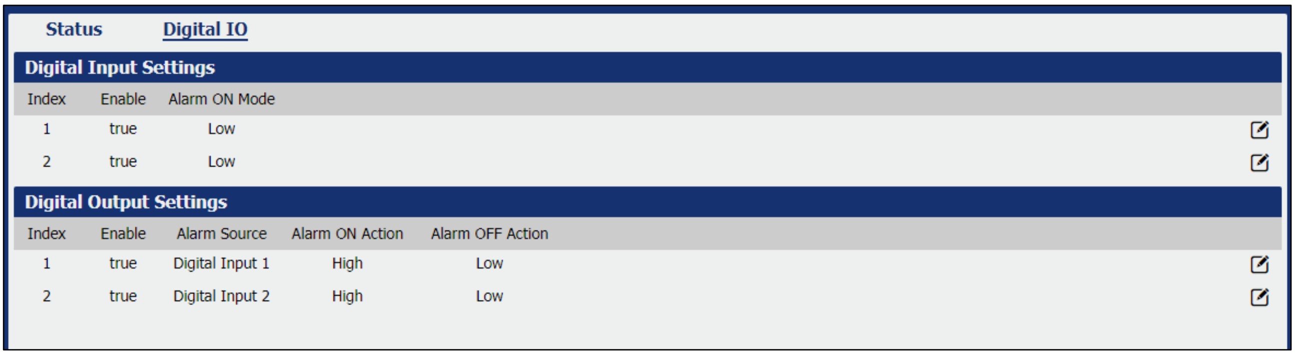
Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 51 – Digital input and output status

- **Enable:** Displays the status of current digital IO function.
- **Logic Level:** Displays the electrical level of digital IO port.
- **Status:** Displays the alarm status of digital IO port.

5.4.2.2 DIGITAL I/O → DIGITAL I/O

This parameter group allows you to configure the digital input and output.



Digital Input Settings

Index	Enable	Alarm ON Mode	
1	true	Low	✎
2	true	Low	✎

Digital Output Settings

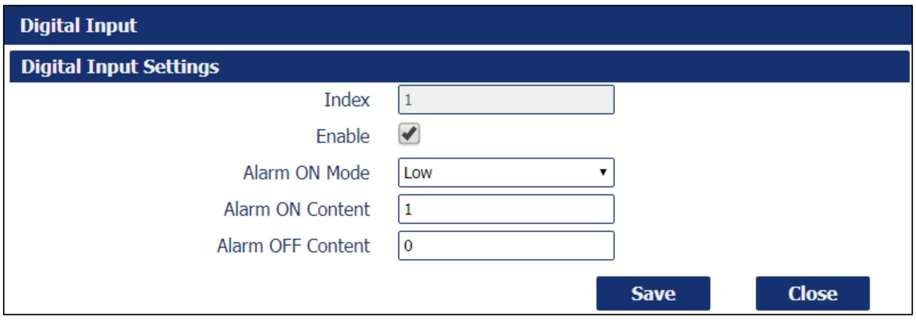
Index	Enable	Alarm Source	Alarm ON Action	Alarm OFF Action	
1	true	Digital Input 1	High	Low	✎
2	true	Digital Input 2	High	Low	✎

Figure 52 – Digital IP settings

This parameter group has the following buttons:

✎ **Button:** Allows you to edit the settings of the digital input or output selected.

As you can see in the figure below, you can edit the settings of the selected digital input by clicking the ✎ button.


Digital Input

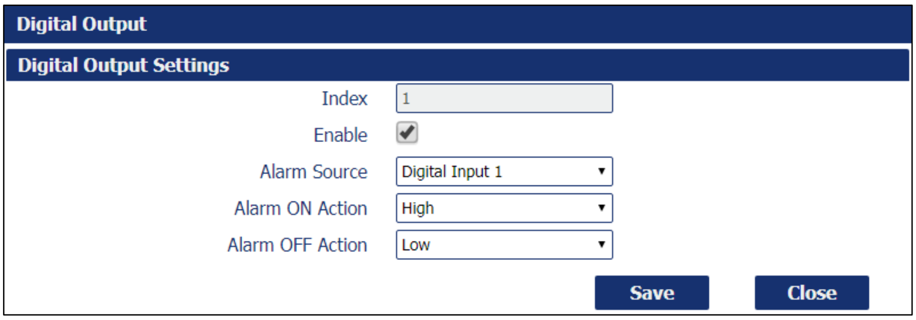
Digital Input Settings

Index	1
Enable	☑
Alarm ON Mode	Low ▾
Alarm ON Content	1
Alarm OFF Content	0

Figure 53 – Digital input settings

- **Enable:** Allows you to enable or disable the digital input function.
- **Alarm ON Mode:** Allows you to select the electrical level to trigger alarm: "Low" or "High".
- **Alarm ON Content:** Allows you to specify the alarm on content to be sent out via SMS message.
- **Alarm OFF Content:** Allows you to specify the alarm off content to be sent out via SMS message.

As you can see in the figure below, you can edit the settings of the selected digital output by clicking the ✎ button.


Digital Output

Digital Output Settings

Index	1
Enable	☑
Alarm Source	Digital Input 1 ▾
Alarm ON Action	High ▾
Alarm OFF Action	Low ▾

Figure 54 – Digital output settings

- **Enable:** Allows you to enable or disable the digital output function.
- **Alarm Source:** Allows you to select the alarm source: "Digital Input 1", "Digital Input 2", "SMS", "MQTT" or "Modbus Alarm". The digital output triggers the related action when there is alarm comes from a Digital Input or a SMS, or when satisfying a Modbus Alarm condition.
- **Alarm ON Action:** Allows you to select the alarm action when ON: "High", "Low" or "Pulse". "High" means high electrical level output. "Low" means low electrical level output. "Pulse" will generate a square wave as specified in the pulse mode parameters when triggered.
- **Alarm OFF Action:** Allows you to select the alarm action when OFF: "High", "Low" or "Pulse". "High" means high electrical level output. "Low" means low electrical level output. "Pulse" will generate a square wave as specified in the pulse mode parameters when triggered.
- **Pulse Width:** This parameter is available when select "Pulse" option in the **Alarm ON Action** or **Alarm OFF Action** parameters. The selected digital output channel will generate a square wave as specified in the pulse mode parameters.

5.5 NETWORK

This section shows information about Firewall, Router, VRRP (Virtual Routing Redundancy Protocol), and IP Passthrough settings.

5.5.1 FIREWALL

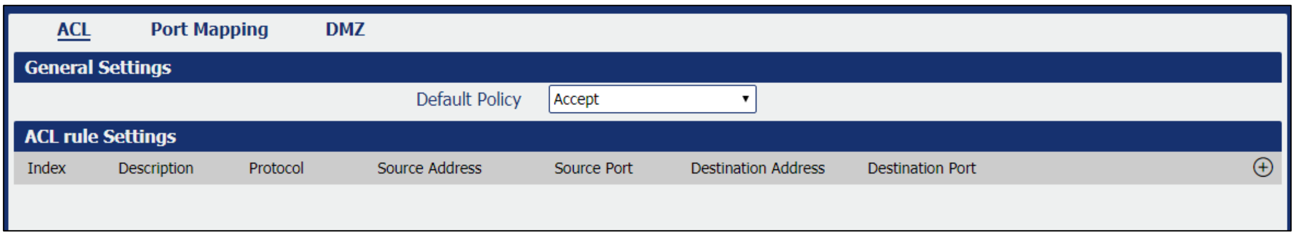
This section allows you to view and manage device firewall information.

Firewall rules are security rules, sets to implement control over users, applications, or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.

5.5.1.1 FIREWALL → ACL

This parameter group allows you to view information about firewall access control policies.

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.



Default Policy: Accept

Index	Description	Protocol	Source Address	Source Port	Destination Address	Destination Port

Figure 55 – Firewall: ACL

This parameter group hast the following buttons:

⊕ **Button:** Allows you to create a new access control list (ACL).

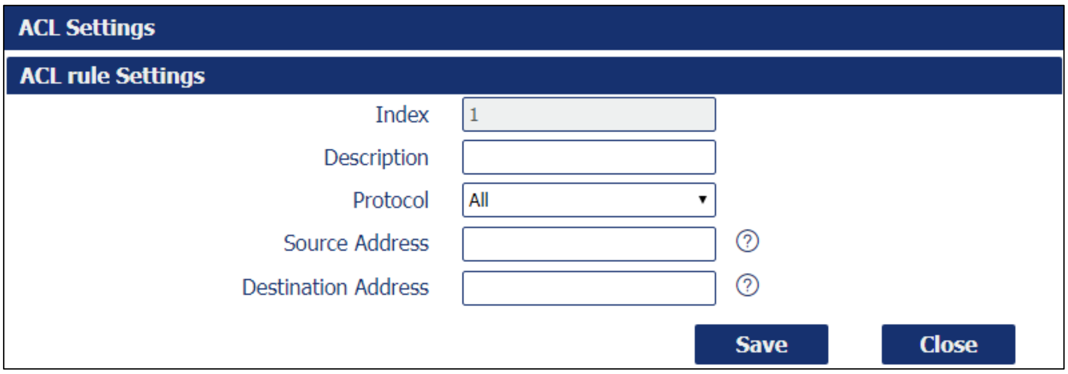
✎ **Button:** Allows you to edit the selected access control list.

⊗ **Button:** Allows you to delete the selected access control list.

This group displays the following parameter:

- **Default Policy:** Allows you to select the firewall default policy: "Accept" or "Drop". The packets which are not included in the access control list will be processed by the default filter policy.

As you can see in the figure below, you can create a new access control list by clicking the ⊕ button.



Index: 1

Description:

Protocol: All

Source Address:

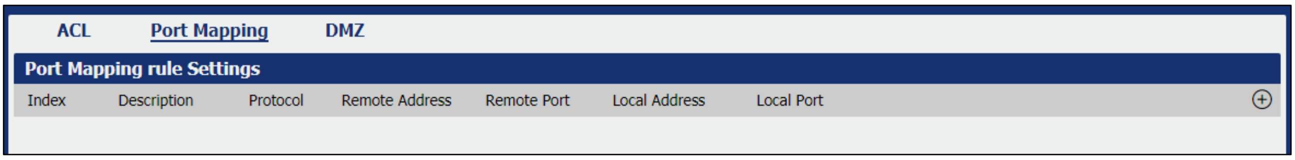
Destination Address:

Figure 56 – ACL rule settings

- **Description:** Allows you to enter a description for the rule to be created.
- **Protocol:** Allows you to select the protocol to be used: "All" (Any protocol number), "TCP", "UDP", "TCP & UDP" or "ICMP".
- **Source Address:** Allows you to enter a specific host IP address or a range of IP addresses via bitmask.
- **Destination Address:** Allows you to enter a specific IP address or a range of IP addresses via bitmask.

5.5.1.2 FIREWALL → PORT MAPPING

This parameter group allows you to view information about the firewall port mapping.



Port Mapping rule Settings

Index	Description	Protocol	Remote Address	Remote Port	Local Address	Local Port

Figure 57 –Figure 561 – Port mapping

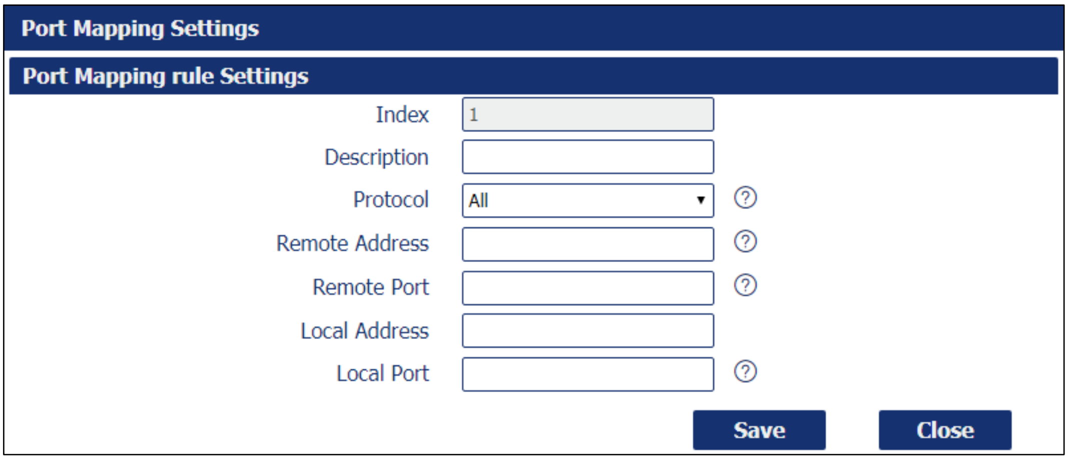
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new port mapping rule.

✎ **Button:** Allows you to edit a selected rule.

⊗ **Button:** Allows you to delete a selected rule.

As you can see in the figure below, you can create a new port mapping rule by clicking the ⊕ button.



Port Mapping Settings

Port Mapping rule Settings

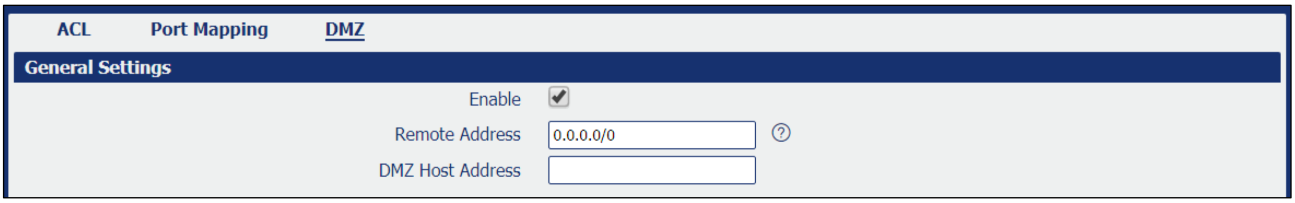
Index: 1
Description:
Protocol: All
Remote Address:
Remote Port:
Local Address:
Local Port:

Figure 58 – Port mapping rule settings

- **Description:** Allows you to enter a description for the rule to be created.
- **Protocol:** Allows you to select the protocol to be used: "All" (Any protocol number), "TCP" or "UDP".
- **Remote Address:** Allows you to enter a WAN IP address that is allowed to access the device.
- **Remote Port:** Allows you to enter the external port number range for incoming requests.
- **Local Address:** Allows you to define the LAN address of a device connected to one of the **AirGate 4G Wi-Fi** interfaces. Inbound requests will be forwarded to this IP address.
- **Local Port:** Allows you to define the LAN port number range used when forwarding to the destination IP address.

5.5.1.3 FIREWALL → DMZ

This parameter group allows you to configure a Demilitarized Zone (DMZ) for the device.



General Settings

Enable: ☑
Remote Address: 0.0.0.0/0
DMZ Host Address:

Figure 59 – DMZ

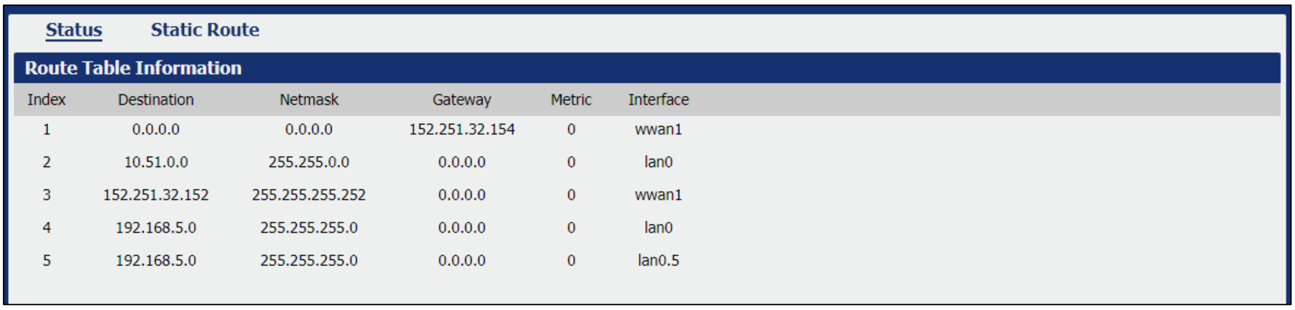
- **Enable:** Allows you to enable or disable DMZ function.
- **Remote Address:** Allows, if configured, optionally restricting DMZ access to the specified WAN IP address only. If set to 0.0.0.0/0, DMZ will be open for all WAN IP addresses.
- **DMZ Host Address:** Allows you to set a WAN IP address that will have access to all entries except for the ports defined during port forwarding setup.

5.5.2 ROUTE

This tab allows you to view and manage device data routing information.

5.5.2.1 ROUTE → STATUS

This parameter group allows you to view information about the configured routes for the device.



Route Table Information

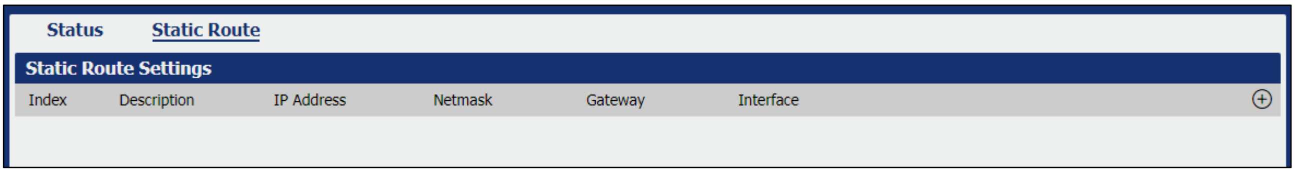
Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	152.251.32.154	0	wwan1
2	10.51.0.0	255.255.0.0	0.0.0.0	0	lan0
3	152.251.32.152	255.255.255.252	0.0.0.0	0	wwan1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0.5

Figure 60 – Route table information

- **Destination:** Displays the destination of this routing traffic.
- **Netmask:** Displays the subnet mask of this routing.
- **Gateway:** Displays the gateway of this interface. The gateway is used for routing packets to remote networks.
- **Metric:** Displays the metric value of this interface.
- **Interface:** Displays the outbound interface of this route.

5.5.2.2 ROUTE → ROUTE TABLE INFORMATION

This parameter group allows you to configure routes for the device. Static Routing refers to a manual method of setting up routing between networks.



Static Route Settings

Index	Description	IP Address	Netmask	Gateway	Interface	⊕

Figure 61 – Static route settings

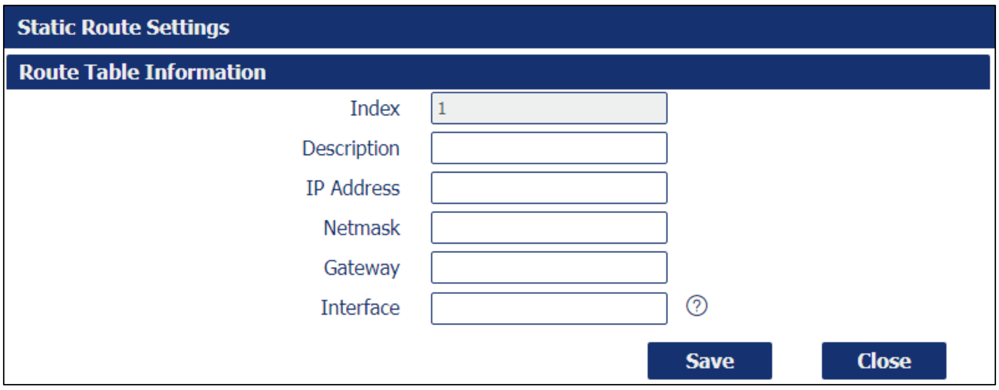
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new route for the device.

✎ **Button:** Allows you to edit the settings of the selected route.

⊗ **Button:** Allows you to delete the selected route.

As you can see in the figure below, you can create a new route by clicking the ⊕ button.



Static Route Settings

Route Table Information

Index	1
Description	
IP Address	
Netmask	
Gateway	
Interface	

Figure 62 – Static route settings

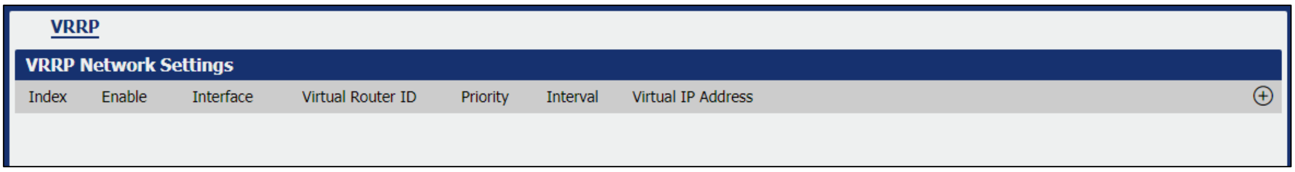
- **Description:** Allows you to enter the description of current static route rule.
- **IP Address:** Allows you to enter the IP address of the destination network.
- **Netmask:** Allows you to enter the subnet mask of the destination network.
- **Gateway**: Allows you to enter the IP address of the local gateway.
- **Interface**: Allows you to define the interface to be used.

5.5.3 VRRP

This tab allows you to view and manage information about the virtual router redundancy protocol.

The VRRP (*Virtual Router Redundancy Protocol*) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.



VRRP

VRRP Network Settings

Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address	⊕

Figure 63 – VRRP

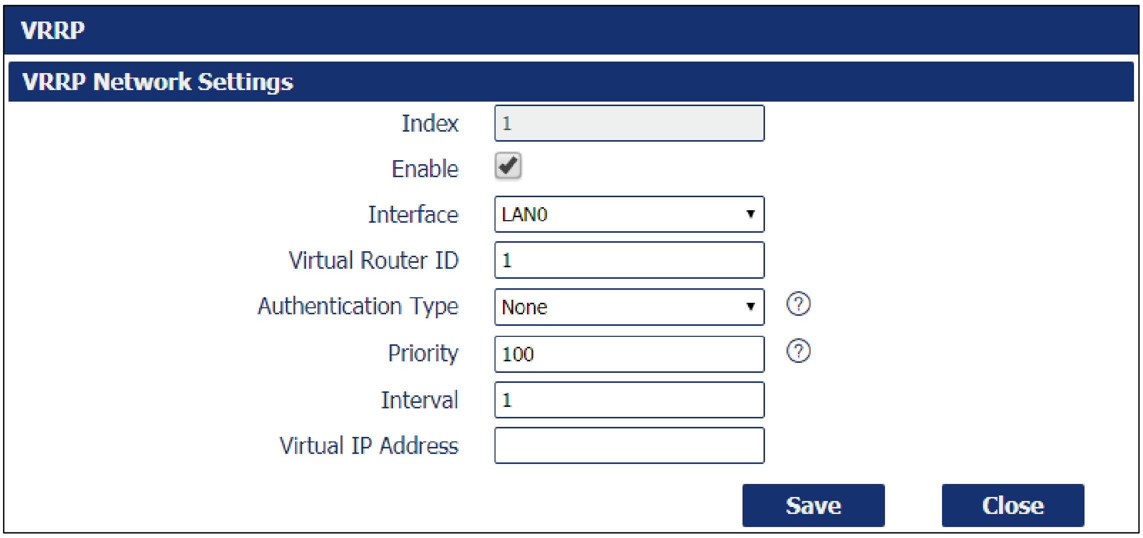
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new VRRP.

✎ **Button:** Allows you to edit the settings of the selected VRRP.

⊗ **Button:** Allows you to delete the selected VRRP.

As you can see in the figure below, you can create a new VRRP by clicking the ⊕ button.



VRRP

VRRP Network Settings

Index	1
Enable	☑
Interface	LAN0 ▾
Virtual Router ID	1
Authentication Type	None ▾ ⓘ
Priority	100 ⓘ
Interval	1
Virtual IP Address	

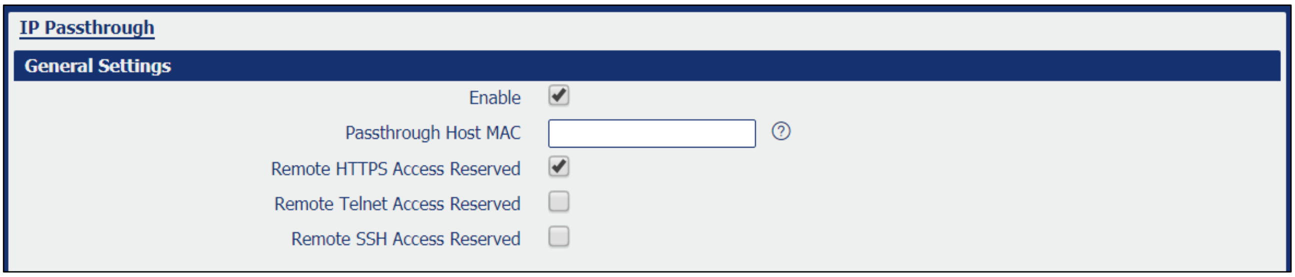
Figure 64 – VRRP network settings

- **Enable:** Allows you to enable or disable the VRRP.
- **Interface:** Allows you to select the virtual router interface.
- **Virtual Router ID:** Allows you to define the user-defined virtual router ID. Range: 1-255.
- **Authentication Type:** Allows you to select the authentication type for VRRP: "None" or "PASS".
- **Password:** If "PASS" option is selected in the **Authentication Type** parameter, allows you to set a password for the VRRP network.
- **Priority:** Allows you to define a VRRP priority range. Range: 1-254 (a bigger number indicates a higher priority).
- **Interval:** Allows you to define the heartbeat package transmission time interval between routers in the virtual IP group. Range: 1-255.
- **Virtual IP Address:** Allows you to enter the virtual IPP address of virtual gateway.

5.5.4 IP PASSTHROUGH

This parameter group allows you to manage information about IP Passthrough mode.

P Passthrough mode disables NAT (Network Address Translation) and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of NAT to make the router "transparent" in the communication process.



IP Passthrough

General Settings

Enable	☑
Passthrough Host MAC	
Remote HTTPS Access Reserved	☑
Remote Telnet Access Reserved	□
Remote SSH Access Reserved	□

Figure 65 – IP Passthrough

- **Enable:** Allows you to enable or disable IP passthrough.
- **Passthrough Host MAC:** Allows you to enter the MAC of passthrough host to receive the WAN IP address.
- **Remote HTTPS Access Reserved:** Allows you to enable or disable remote HTTPS access.
- **Remote Telnet Access Reserved:** Allows you to enable or disable remote Telnet access.
- **Remote SSH Access Reserved:** Allows you to enable or disable remote SSH access.

5.6 APPLICATIONS (NATIVE APPLICATIONS)

This section provides a list of standard **AirGate 4G Wi-Fi** applications. These applications are native to the device and cannot be removed. **AirGate 4G Wi-Fi** does, however, have applications that can be installed to improve the use of the device and that can be viewed in the APPLICATIONS chapter of this manual.

5.6.1 DDNS

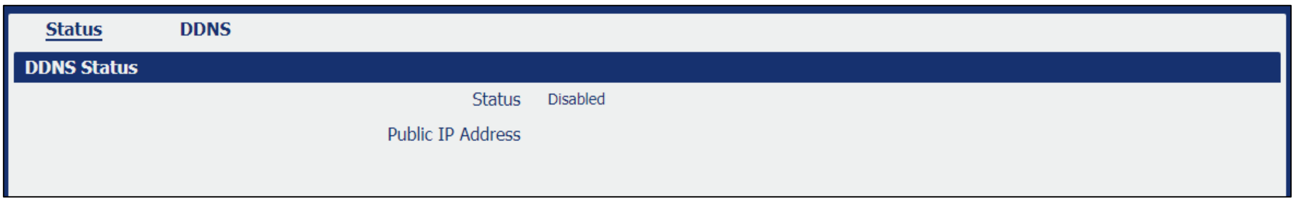
This tab allows you to view and manage information about DDNS.

DDNS is a system that allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time to make it possible to establish connections to that machine without the need to always track the actual IP addresses.

Several providers offer Dynamic DNS services (DDNS), free or for a charge.

5.6.1.1 DDNS → STATUS

This parameter group allows you to view information about the device DDNS.



DDNS Status

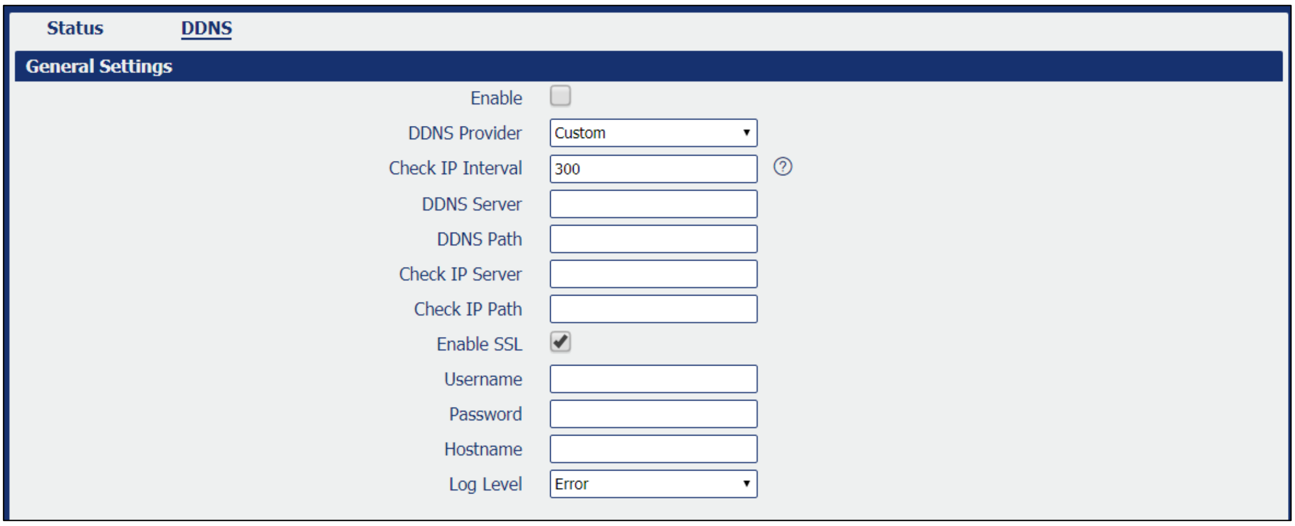
Status	Disabled
Public IP Address	

Figure 66 – DDNS status

- **Status:** Displays the DDNS status.
- **Public IP Address:** Displays the public IP address assigned to DDNS.

5.6.1.2 DDNS → DDNS

This parameter group allows you to manage the DDNS settings.



General Settings

Enable	☐
DDNS Provider	Custom
Check IP Interval	300
DDNS Server	
DDNS Path	
Check IP Server	
Check IP Path	
Enable SSL	☑
Username	
Password	
Hostname	
Log Level	Error

Figure 67 – DDNS settings

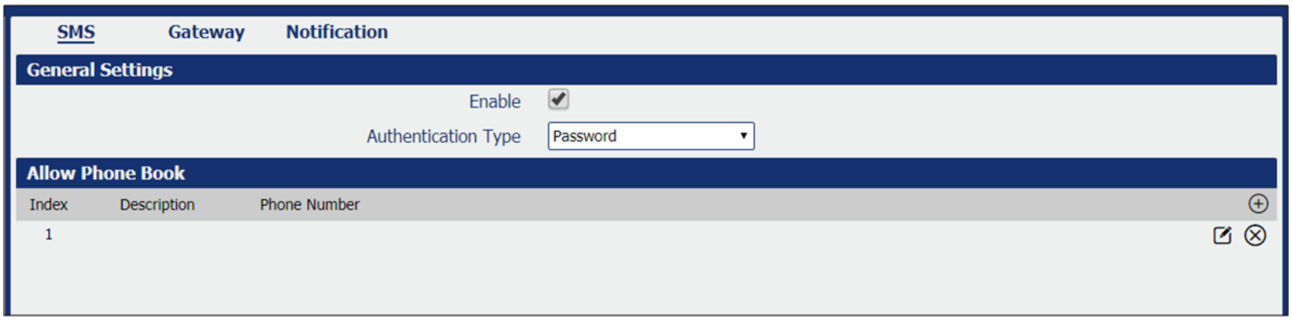
- **Enable:** Allows you to enable or disable DDNS service.
- **DDNS Provider:** Allows you to DDNS provider to be used: "DynDNS", "no-ip", "3322" or "custom".
- **Check IP Interval:** Allows you to enter the interval, in minutes (30 to 86400). The modem will update the Dynamic DNS server of its carrier assigned IP address.
- **DDNS Server:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to set the Internet address to communicate Dynamic DNS information.
- **DDNS Path:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to set the DDNS path for custom type.
- **Check IP Server:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to check the IP server.
- **Check IP Path:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to check the IP path.
- **Enable SSL:** Allows you to enable or disable SSL service for the connection.
- **Username:** Allows you to enter the username used when setting up the account. Used to login to the Dynamic DNS service.
- **Password:** Allows you to enter the password associated with the account.
- **Hostname:** Allows you to enter the hostname associated with the account.
- **Log Level:** Allows you to select the log output level: "None", "Debug", "Notice", "Info" or "Error".

5.6.2 SMS

This tab allows you to enable and configure SMS sending. SMS allows user to send the SMS to control the router or get the running status of the router.

5.6.2.1 SMS → SMS

This parameter group allows you to enter contacts that can send SMS commands or get status from the router.



SMS Gateway Notification

General Settings

Enable ☑

Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number
1		

Figure 68 – Sending SMS

This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new number to the phone book.

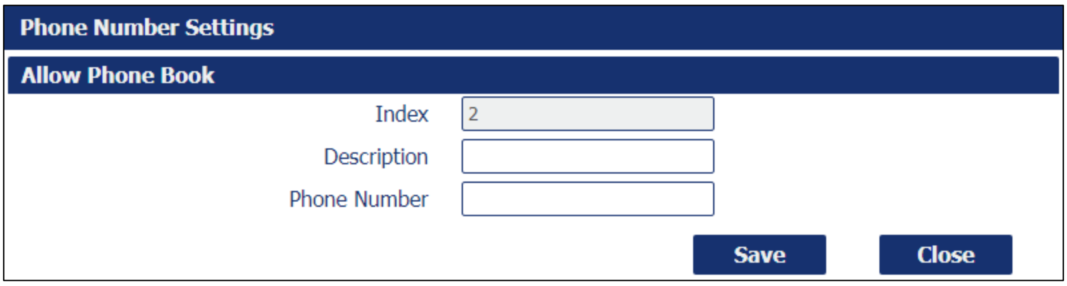
✎ **Button:** Allows you to edit the settings of the phone number selected.

⊗ **Button:** Allows you to delete the phone number selected.

This group displays the following parameters:

- **Enable:** Allows you to enable or disable SMS sending.
- **Authentication Type:** Allows you to define the authentication type for the SMS function: "None" or "Password".

As you can see in the figure below, you can create a new phone number by clicking the ⊕ button. You can add up to 20 contacts.



Phone Number Settings

Allow Phone Book

Index: 2

Description:

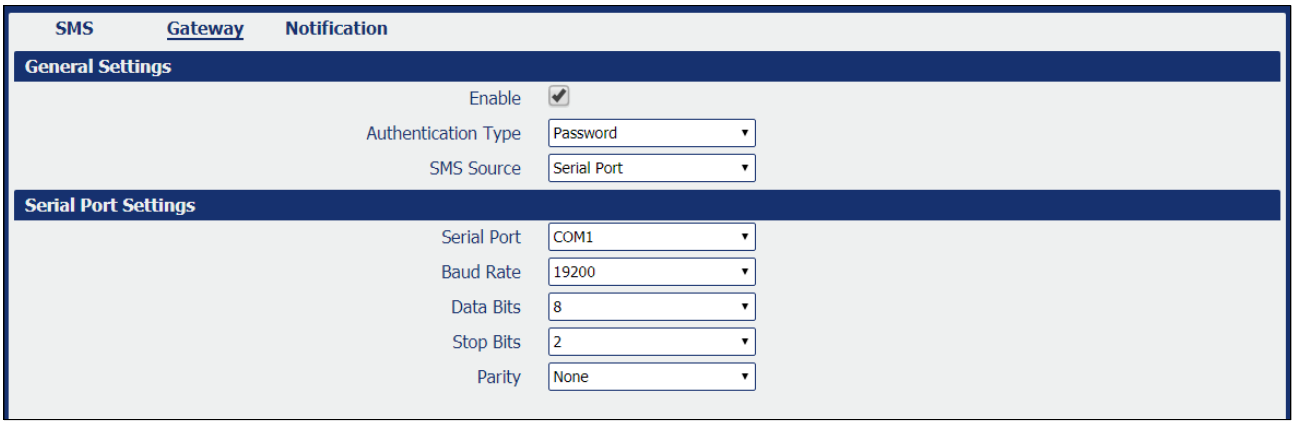
Phone Number:

Figure 69 – Phone number

- **Description:** Allows you to enter a description for the number to be created.
- **Phone Number:** Allows you to add a phone number.

5.6.2.2 SMS → GATEWAY

This parameter group allows you to send SMS messages by using a valid syntax from serial device or Ethernet device.



General Settings

Enable ☑

Authentication Type: Password

SMS Source: Serial Port

Serial Port Settings

Serial Port: COM1

Baud Rate: 19200

Data Bits: 8

Stop Bits: 2

Parity: None

Figure 70 – Gateway settings

GENERAL SETTINGS

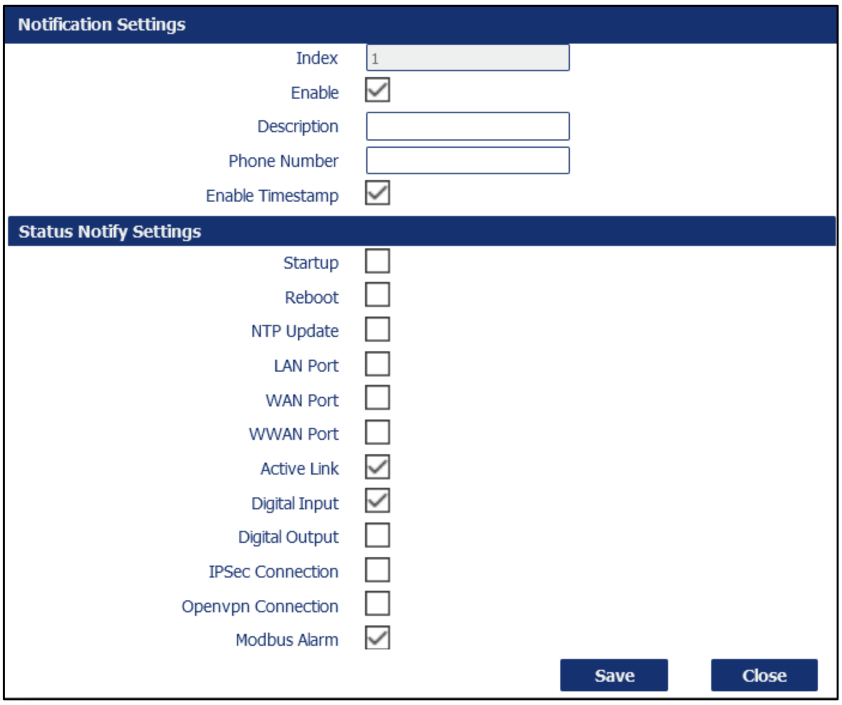
- **Enable:** Allows you to enable or disable SMS gateway.
- **Authentication Type:** Allows you to define an authentication type for SMS gateway: "None" or "Password".
- **SMS Source:** Allows you to define a valid syntax: "Serial Port" or "HTTP(S) GET/POST".

SERIAL PORT SETTINGS

- **Serial Port:** Allows you to select the serial port: COM1 or COM2.
- **Baud Rate:** Allows you to select the serial port Baud Rate: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to select the data bits values: 7 to 8.
- **Stop Bits:** Allows you to select the serial port stop bits: 1 or 2.
- **Parity:** Allows you to select the serial port parity: "None", "Even" or "Odd".

5.6.2.3 SMS → NOTIFICATION

This parameter group allows sending SMS notification to the pre-setting phone number when some of router status changed. You can set up to 10 alarm notifications.



Notification Settings

Index: 1

Enable ☑

Description:

Phone Number:

Enable Timestamp ☑

Status Notify Settings

Startup □

Reboot □

NTP Update □

LAN Port □

WAN Port □

WWAN Port □

Active Link ☑

Digital Input ☑

Digital Output □

IPSec Connection □

Openvpn Connection □

Modbus Alarm ☑

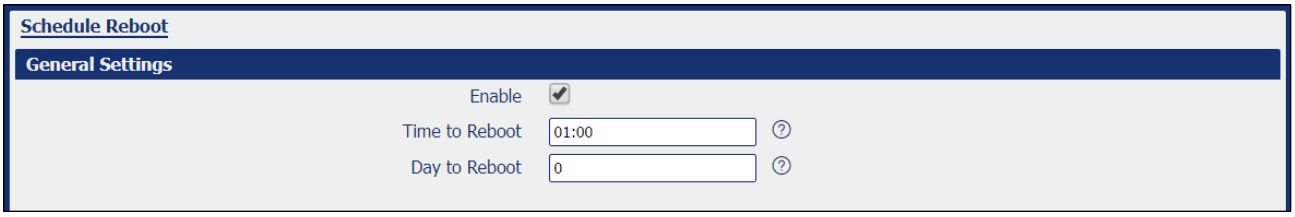
Figure 71 – Notification channel settings

- **Enable:** Allows you to enable or disable alarm notification.
- **Description:** Allows you to add the description for notification channel.
- **Phone Number:** Allows you to add a pre-setting phone number to receive the notification.

- **Enable Timestamp:** Allows you to enable or disable the timestamp that goes the SMS.
- **Startup:** Allows you to send a SMS notification to the pre-setting phone number when system startup.
- **Reboot:** Allows you to enable notification e-mails to be sent whenever the system is rebooted.
- **NTP Update:** Allows you to send a SMS notification to the pre-setting phone number when system startup.
- **LAN Port Status:** Allows you to send a SMS notification to the pre-setting phone number when LAN port status changed.
- **WAN Port Status:** Allows you to send a SMS notification to the pre-setting phone number when WAN port status changed.
- **WWAN Port Status:** Allows you to send a SMS notification to the pre-setting phone number when WWAN port status changed.
- **Active Link Status:** Allows you to send a SMS notification to the pre-setting phone number when active link status changed.
- **Digital Input Status:** Allows you to send a SMS notification to the pre-setting phone number when DI status changed
- **Digital Output Status:** Allows you to send a SMS notification to the pre-setting phone number when DO status changed.
- **IPsec Connection Status:** Allows you to send a SMS notification to the pre-setting phone number when IPsec connection status changed.
- **OpenVPN Connection Status:** Allows you to send a SMS notification to the pre-setting phone number when OpenVPN Connection Status changed.
- **Modbus Alarm:** Allows you to send an SMS notification whenever a Modbus alarm configured as "Event Notification" is detected. For more information on how to configure a Modbus alarm, see the MODBUS ALARM section of this manual.

5.6.3 SCHEDULE REBOOT

This tab allows you to define the time for router reboot itself.



Schedule Reboot

General Settings

Enable ☑

Time to Reboot 01:00

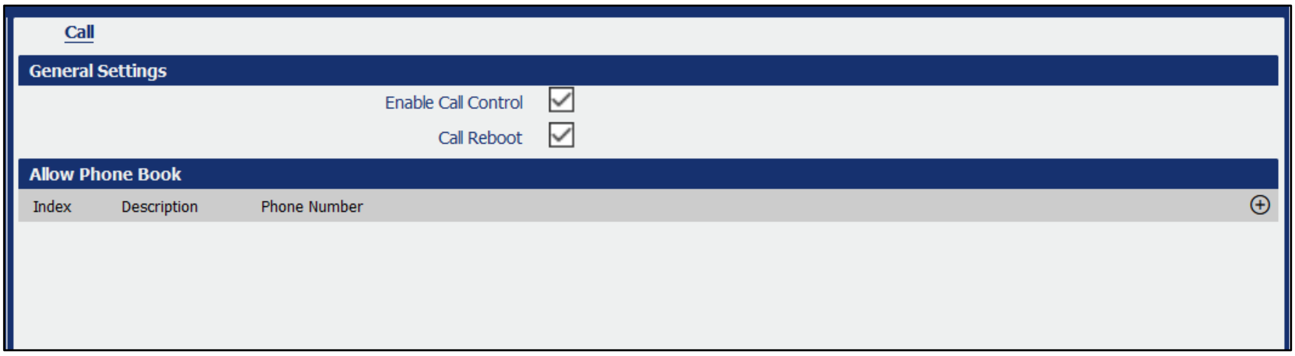
Day to Reboot 0

Figure 72 – Schedule reboot

- **Enable:** Allows you to enable or disable schedule reboot feature.
- **Time to Reboot:** Allows you to enter the time of each day to reboot device. Format: HH(00-23):MM(00-59).
- **Day to Reboot:** Allows you to enter the day of each month to reboot device. 0 means every day.

5.6.4 CALL

This feature allows you to reboot the router when making a phone call to the router.



Call

General Settings

Enable Call Control ☑

Call Reboot ☑

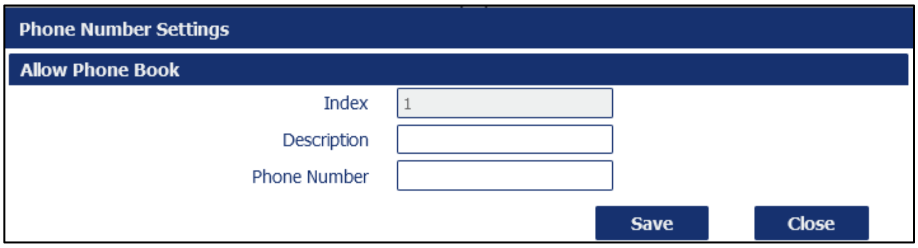
Allow Phone Book

Index	Description	Phone Number

Figure 73 – Enable function "Call"

- **Enable call control:** Allows you to enable or disable the restart control by phone call.
- **Call reboot:** Allows you to enable or disable router restart.

You can add up to 20 phone contacts.



Phone Number Settings

Allow Phone Book

Index 1

Description

Phone Number

Figure 74 – Adding Phone Numbers

- **Description:** Allows you to add a description to the phone number.
- **Phone Number:** Allows you to configure a number for the restart command.

5.7 VPN

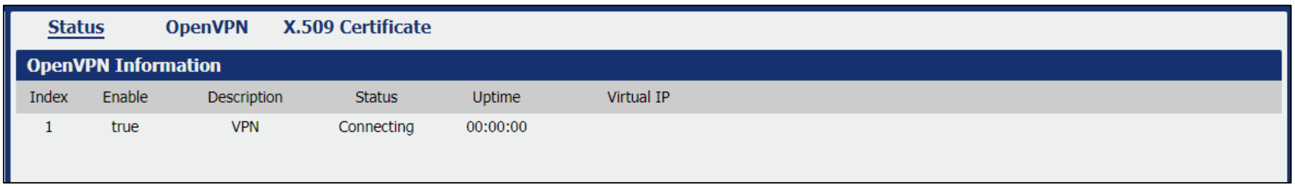
This section allows you to define VPN settings.

5.7.1 OpenVPN

OpenVPN is an open-source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

5.7.1.1 OpenVPN → STATUS

This parameter group allows you to view the OpenVPN status. Each OpenVPN can be individually created, configured, or removed in the OpenVPN → OpenVPN tab.



OpenVPN Information

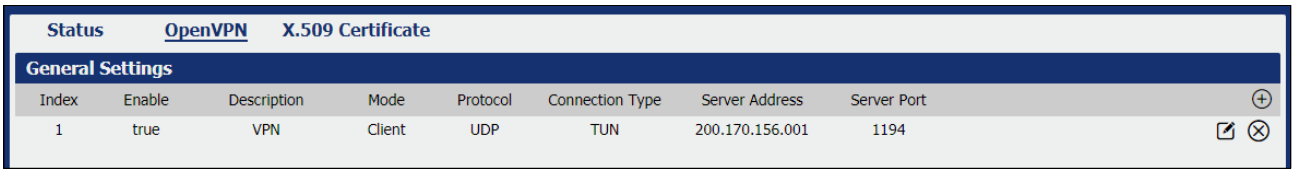
Index	Enable	Description	Status	Uptime	Virtual IP
1	true	VPN	Connecting	00:00:00	

Figure 75 – OpenVPN

- **Enable:** Displays current OpenVPN settings is enable or disable.
- **Status:** Displays the current VPN connection status.
- **Uptime:** Displays the connection time since VPN is established.
- **Virtual IP:** Displays the virtual IP address obtain from remote side.

5.7.1.2 OpenVPN → OpenVPN

This parameter group allows you to configure the OpenVPN.



General Settings

Index	Enable	Description	Mode	Protocol	Connection Type	Server Address	Server Port	⊕
1	true	VPN	Client	UDP	TUN	200.170.156.001	1194	✎ ⊗

Figure 76 – OpenVPN settings

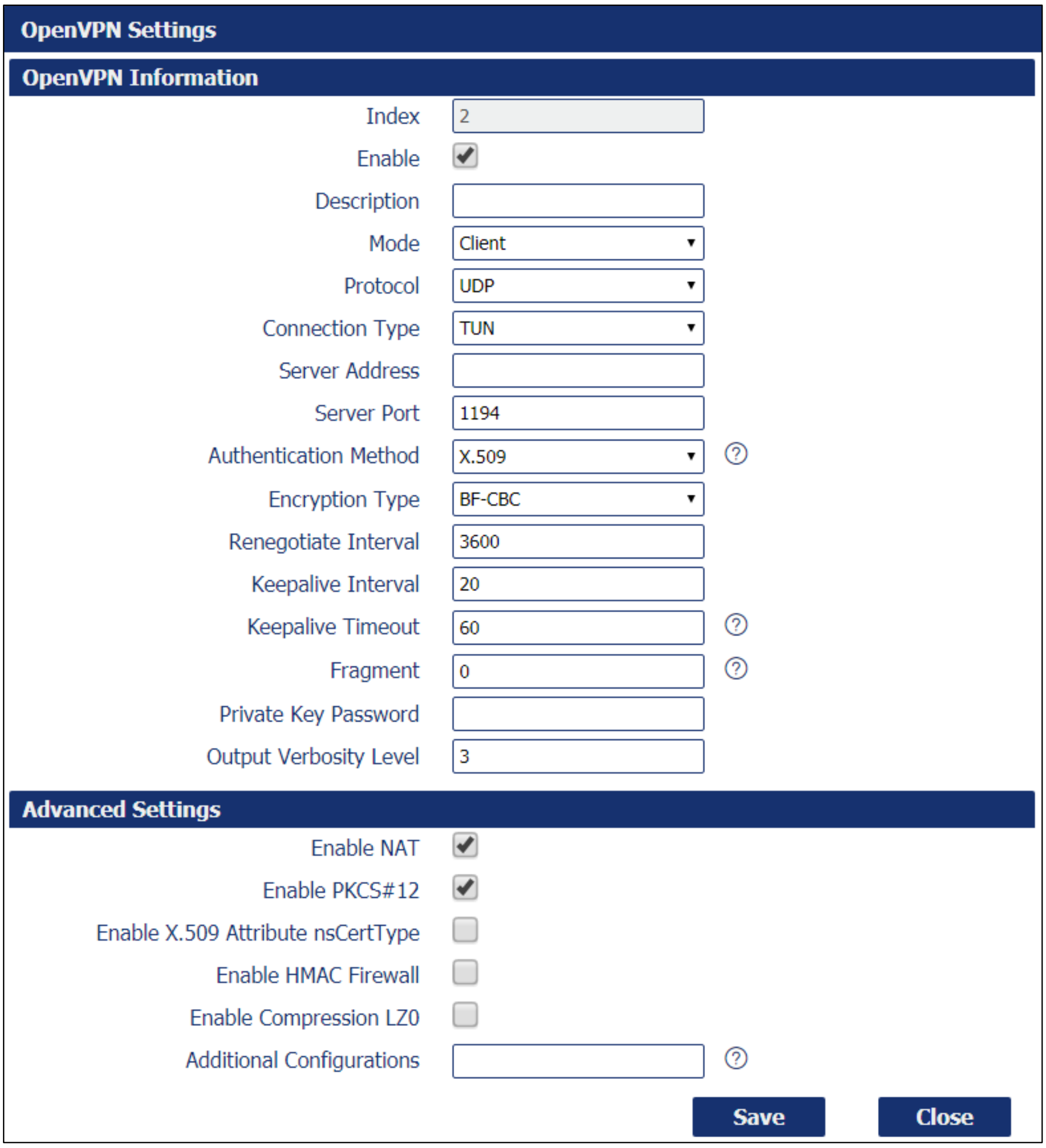
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new OpenVPN.

✎ **Button:** Allows you to edit the settings of the selected OpenVPN.

⊗ **Button:** Allows you to delete the selected OpenVPN.

As you can see in the figure below, you can create a new OpenVPN by clicking the ⊕ button.



OpenVPN Settings

OpenVPN Information

Index	2
Enable	☑
Description	
Mode	Client ▾
Protocol	UDP ▾
Connection Type	TUN ▾
Server Address	
Server Port	1194
Authentication Method	X.509 ▾ ⓘ
Encryption Type	BF-CBC ▾
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60 ⓘ
Fragment	0 ⓘ
Private Key Password	
Output Verbosity Level	3

Advanced Settings

Enable NAT	☑
Enable PKCS#12	☑
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZO	□
Additional Configurations	ⓘ

Figure 77 – OpenVPN settings

- **Enable:** Allows you to enable or disable OpenVPN tunnel.
- **Description:** Allows you to Enter a description for this OpenVPN tunnel.
- **Mode:** Allows you to define a mode for the OpenVPN tunnel: "Client" or "P2P".
- **Protocol:** Allows you to define a protocol for the OpenVPN tunnel: "UDP" or "TCP Client".
- **Connection Type:** Allows you to define a connection type for the OpenVPN tunnel: "TUN" or "TAP". The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.
- **Server Address:** Allows you to Enter the IP address or domain of remote server
- **Server Port:** Allows you to Enter the negotiate port on OpenVPN server
- **Authentication Method:** Allows you to define an authentication method for the OpenVPN tunnel: "X.509", "Pre-shared", "Password" or "X.509 and Password".
- **Encryption Type:** Allows you to define an encryption type for the OpenVPN tunnel: "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" or "AES-256 -CBC".
- **Username:** Allows you to enter the username for authentication when selection from "Password" or "X.509 And Password".
- **Password:** Allows you to enter the password for authentication when selection from "Password" or "X.509 And Password".
- **Local IP Address:** Allows you to enter the local virtual IP address when select "P2P" mode.
- **Remote IP Address:** Allows you to enter the remote virtual IP address when select "P2P" mode.
- **Local Netmask:** Allows you to enter the local netmask when select "TAP" connection type.
- **TAP Bridge:** Allows you to select the specified LAN that bridge with OpenVPN tunnel when select "TAP" connection type.
- **Renegotiate Interval:** Allows you to enter the renegotiate interval if connection is failed.
- **Keep Alive Interval:** Allows you to enter the keep alive interval to check the tunnel is active or not.

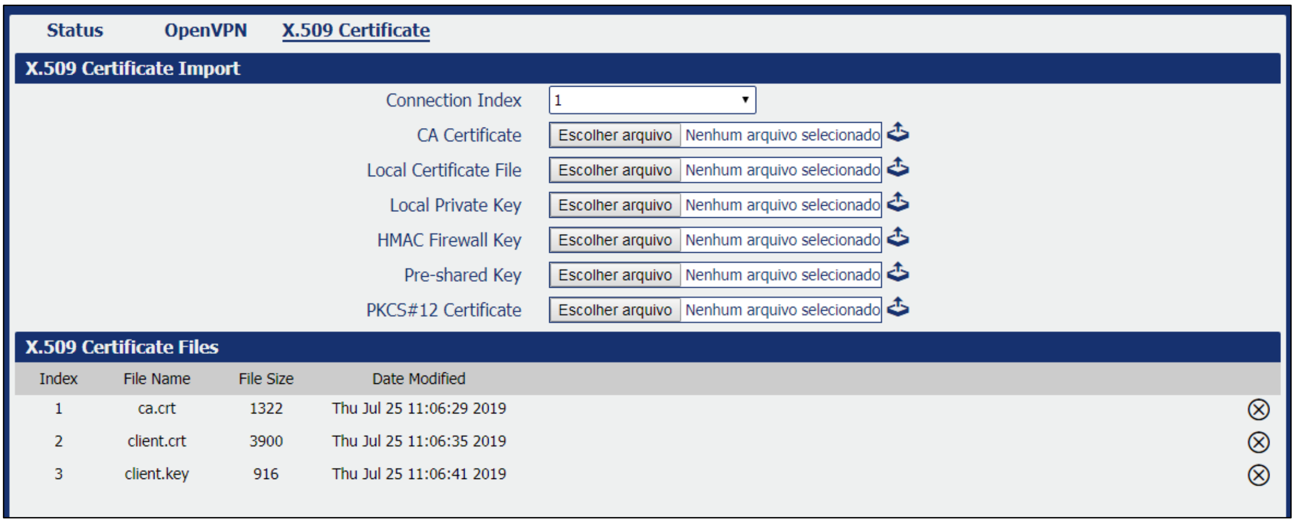
- **Keep Alive Timeout:** Allows you to enter the keep alive timeout, once connection is failed it will trigger the OpenVPN reconnect.
- **Fragment:** Allows you to enter the fragment size. 0 means disable
- **Private Key Password:** Allows you to enter the private key password for authentication when selection from "X.509" or "X.509 And Password".
- **Output Verbosity Level:** Allows you to enter the level of the output log and values.

AVANCED SETTINGS

- **Enable NAT:** Allows you to enable or disable NAT.
- **Enable PKCS#12:** Allows you to enable or disable PKCS#12. It is an exchange of digital certificate encryption standard, used to describe personal identity information.
- **Enable X.509 Attribute nsCertType:** Require that peer certificate be signed with an explicit nsCertType designation of "server".
- **Enable HMAC Firewall:** Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.
- **Enable Compression LZO:** Allows you to enable or disable compress the data.
- **Additional Configurations:** Allows you to enter some other options of OpenVPN in this field. Each expression can be separated by a ";".

5.7.1.3 OpenVPN → X.509 CERTIFICATE

This parameter group allows you to add certificates to the device.



X.509 Certificate Import

Connection Index: 1
CA Certificate: Escolher arquivo Nenhum arquivo selecionado
Local Certificate File: Escolher arquivo Nenhum arquivo selecionado
Local Private Key: Escolher arquivo Nenhum arquivo selecionado
HMAC Firewall Key: Escolher arquivo Nenhum arquivo selecionado
Pre-shared Key: Escolher arquivo Nenhum arquivo selecionado
PKCS#12 Certificate: Escolher arquivo Nenhum arquivo selecionado

X.509 Certificate Files

Index	File Name	File Size	Date Modified	
1	ca.crt	1322	Thu Jul 25 11:06:29 2019	⊗
2	client.crt	3900	Thu Jul 25 11:06:35 2019	⊗
3	client.key	916	Thu Jul 25 11:06:41 2019	⊗

Figure 78 – Certificate files

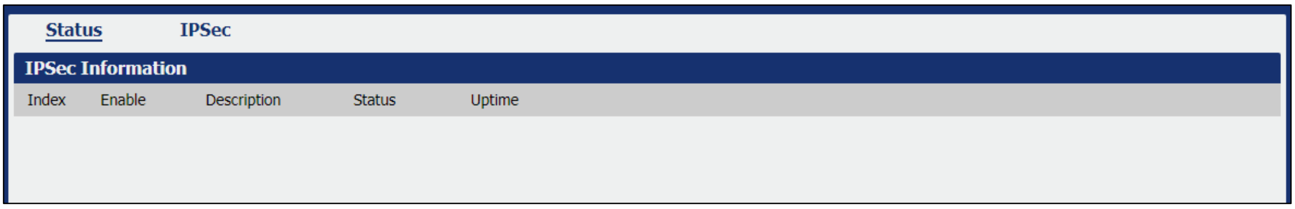
- **Connection Index:** Displays the current connection index for OpenVPN channel.
- **CA Certificate:** Allows you to import CA certificate file.
- **Local Certificate File:** Allows you to import local certificate file.
- **Local Private Key:** Allows you to import local private key file.
- **HMAC Firewall Key:** Allows you to import HMAC firewall key file.
- **Pre-shared Key:** Allows you to import the pre-shared key file.
- **PKCS#12 Certificate:** Allows you to import PKCS#12 certificates.

5.7.2 IPsec

IPsec facilitates configuration of secured communication tunnels. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are created using the ESP (Encapsulating Security Payload) protocol.

5.7.2.1 IPsec → STATUS

This section allows you to view IPsec status.



IPSec Information

Index	Enable	Description	Status	Uptime

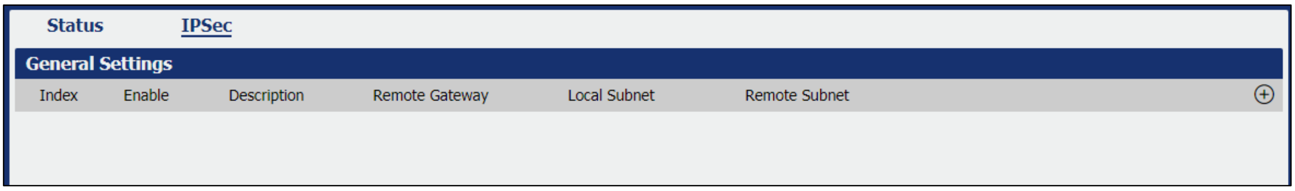
Figure 79 – IPsec status

- **Enable:** Displays current IPsec settings is enable or disable.
- **Description:** Displays the description of current VPN channel.
- **Status:** Displays the current VPN connection status.

- **Uptime:** Displays the connection time since VPN is established.

5.7.2.2 IPsec → IPsec

This section allows you to create or configure IPsec.



Status IPSec

General Settings

Index	Enable	Description	Remote Gateway	Local Subnet	Remote Subnet	⊕

Figure 80 –IPsec: general settings

This parameter group has the following buttons:

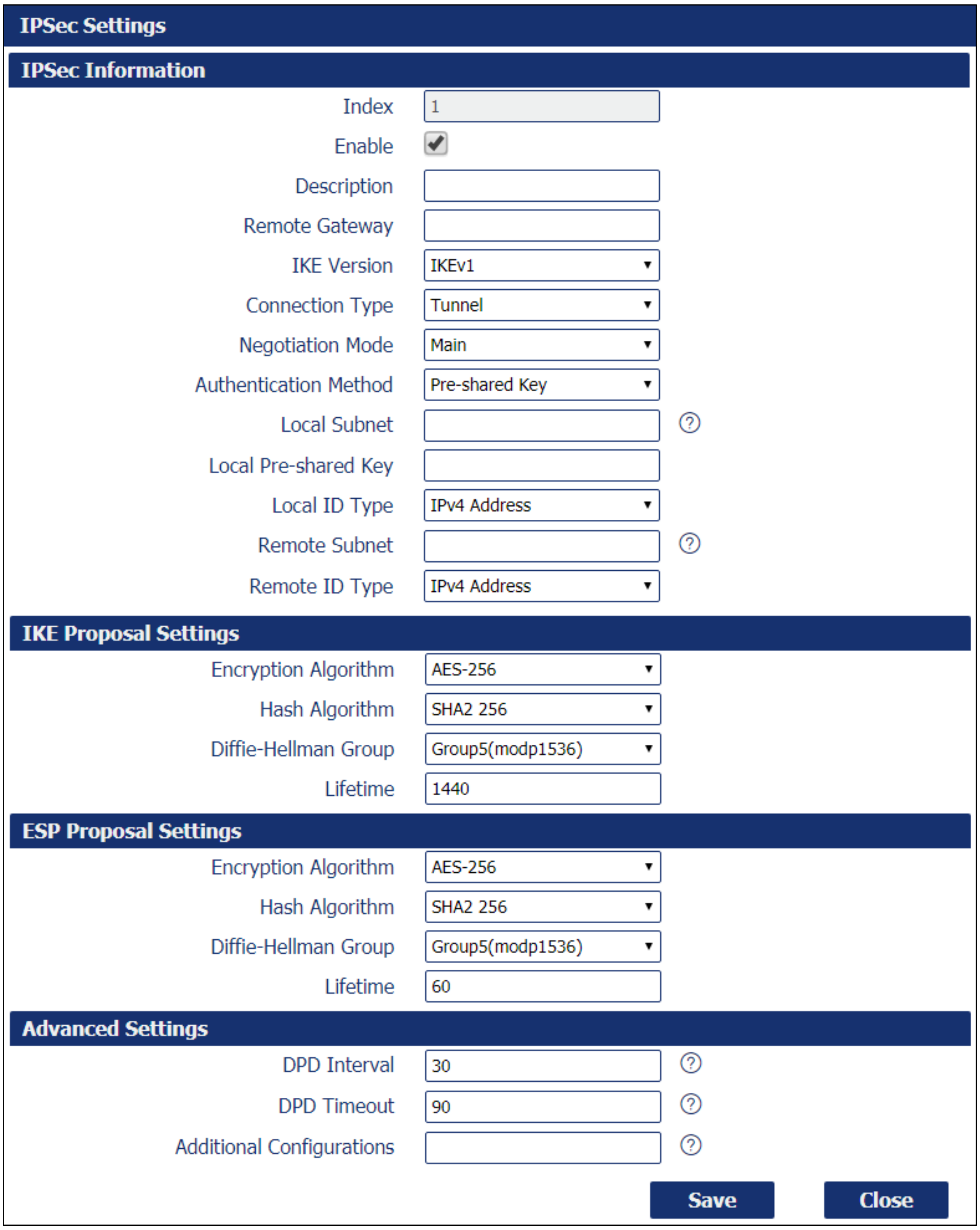
⊕ **Button:** Allows you to add a new IPsec.

✎ **Button:** Allows you to edit the settings of the selected IPsec.

⊗ **Button:** Allows you to delete the selected IPsec.

.

As you can see in the figure below, you can create a new IPsec by clicking the ⊕ button.



IPSec Settings

IPSec Information

Index	1
Enable	☑
Description	
Remote Gateway	
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key
Local Subnet	
Local Pre-shared Key	
Local ID Type	IPv4 Address
Remote Subnet	
Remote ID Type	IPv4 Address

IKE Proposal Settings

Encryption Algorithm	AES-256
Hash Algorithm	SHA2 256
Diffie-Hellman Group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption Algorithm	AES-256
Hash Algorithm	SHA2 256
Diffie-Hellman Group	Group5(modp1536)
Lifetime	60

Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 81 – IPsec settings

GENERAL SETTINGS

- **Enable:** Allows you to enable or disable IPsec.
- **Description:** Allows you to enter a description for this IPsec VPN tunnel.
- **Remote Gateway:** Allows you to enter an IP address for the remote tunnel.
- **IKE Version:** Allows you to select an IKE (Internet Key Exchange) version: "IKEv1" or "IKEv2".
- **Connection Type:** Allows you to select the connection type: "Tunnel" or "Transport".
  - **Tunnel:** In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications.
  - **Transport:** In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact since the IP header is neither modified nor encrypted.
- **Negotiation Mode:** Allows you to select a negotiation mode: "Main" or "Aggressive".
- **Authentication Method:** Allows you to select an authentication method: "Pre-Shared Key" or "Pre-Shared Key and XAuth".
- **Local Subnet:** Allows you to enter the IP address with mask if a network beyond the local LAN will be sending packets through the tunnel. The remote subnet and Local subnet addresses must not overlap.
- **Local Pre-Shared Key:** Allows you to enter the pre-shared key which matches the remote endpoint.
- **Local ID Type:** Allows you to enter the local endpoint's identification. The identifier can be a host name or an IP address.

- **Identity XAuth:** Allows you to enter Xauth identity after "Pre-shared Key and Xauth" on authentication Method is enabled.
- **Password XAuth:** Allows you to enter Xauth password "Pre-shared Key and Xauth" on authentication Method is enabled.
- **Remote Subnet:** Allows you to enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address. The remote subnet and local subnet addresses must not overlap.
- **Remote ID Type:** Allows you to enter the authentication address of the remote endpoint.

IKE PROPOSAL SETTINGS

- **Encryption Algorithm (IKE):** Allows you to select the encryption algorithm: "3DES AES-128", "AES-192" or "AES-256".
- **Hash Algorithm (IKE):** Allows you to select the hash algorithm: "MD5", "SHA1", "SHA2 256", "SHA2 384" or "SHA2 512".
- **Diffie-Hellman Group (IKE):** Allows you to select the Diffie-Hellman method: "Negotiate (None)", "768 (Group 1)", "1024 (Group 2)", "1536 (Group 5)" or "2048 (Group 14)".
- **Lifetime (IKE):** How long a particular instance of a connection should last, from successful negotiation to expiry.

ESP PROPOSAL SETTINGS

- **Encryption Algorithm (ESP):** Allows you to select the encryption algorithm: "3DES AES-128", "AES-192" or "AES-256".
- **Hash Algorithm (ESP):** Allows you to select the hash algorithm: "MD5", "SHA1", "SHA2 256", "SHA2 384" or "SHA2 512".
- **Diffie-Hellman Group (ESP):** Allows you to select the Diffie-Hellman method: "Negotiate (None)", "768 (Group 1)", "1024 (Group 2)", "1536 (Group 5)" or "2048 (Group 14)".
- **Lifetime (ESP):** How long a particular instance of a connection should last, from successful negotiation to expiry.

ADVANCED SETTINGS

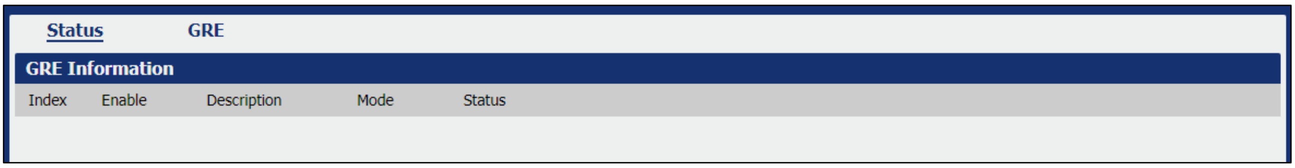
- **DPD Interval:** Allows you to enter the interval after which DPD is triggered if no IPsec protected packets is received from the peer.
- **DPD Timeout:** Allows you to enter the remote peer probe response timer.
- **Additional Configurations:** Allows you to enter some other options of IPsec in this field. Each expression can be separated by a ";".

5.7.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets to route other protocols over IP networks. It is a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

5.7.3.1 GRE → STATUS

This parameter group allows you to view the GRE protocol status.



GRE Information

Index	Enable	Description	Mode	Status

Figure 82 – GRE status

- **Enable:** Displays current GRE settings is enable or disable.
- **Description:** Displays the description of current VPN channel.
- **Mode:** Displays the current VPN mode.
- **Status:** Displays the current VPN connection status.

5.7.3.2 GRE → GRE

This parameter group allows you to create or configure the GRE protocol.

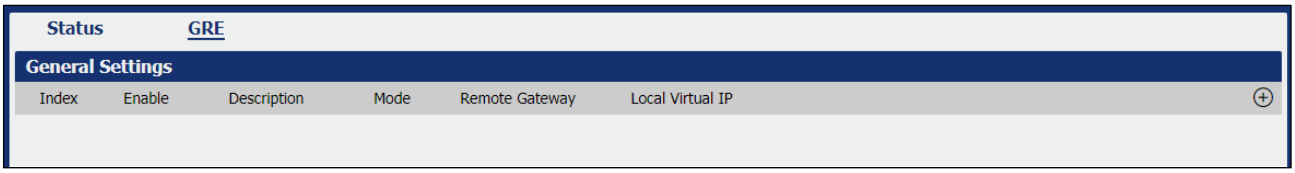


Figure 83 –Figure 80 – GRE settings

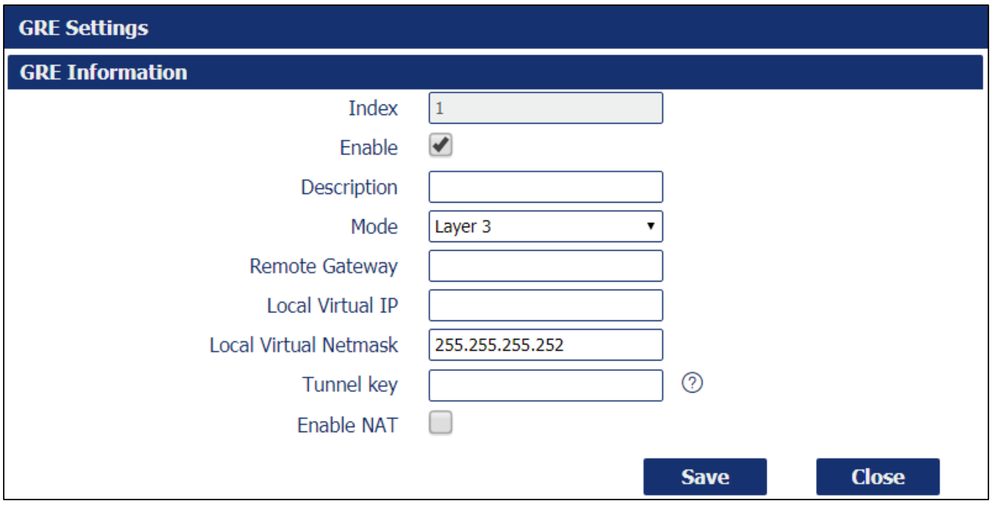
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new GRE.

Button: Allows you to edit the settings of the selected GRE.

⊗ **Button:** Allows you to delete the selected GRE.

As you can see in the figure below, you can create a GRE by clicking the ⊕ button.



GRE Settings

GRE Information

Index	1
Enable	☑
Description	
Mode	Layer 3
Remote Gateway	
Local Virtual IP	
Local Virtual Netmask	255.255.255.252
Tunnel key	
Enable NAT	□

Figure 84 – GRE information

- **Enable:** Allows you to enable or disable GRE.
- **Description:** Allows you to enter the description of current VPN channel.
- **Mode:** Allows you to specify the running mode of GRE: "Layer 2" or "Layer 3".
- **Remote Gateway:** Allows you to enter the remote IP address of peer GRE tunnel.
- **Local Virtual IP:** Allows you to enter the local virtual netmask of GRE tunnel.
- **Local Virtual Netmask:** Allows you to enter the local virtual netmask of GRE tunnel.
- **Tunnel Key:** Allows you to enter the authentication key of GRE tunnel.
- **Enable NAT:** Allows you to enable or disable NAT.
- **Bridge Interface:** Allows you to specify the bridge interface work with Layer 2 mode.

5.8 MAINTENANCE

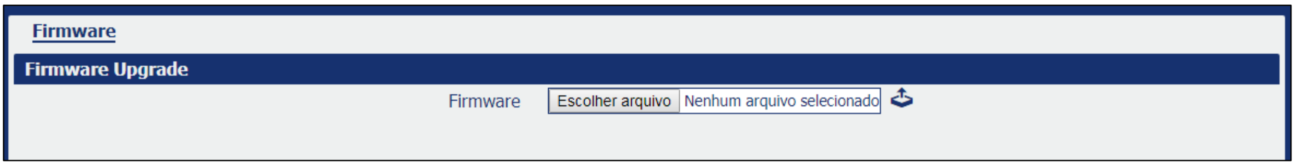
This section allows you to configure device maintenance settings.

5.8.1 UPGRADE

When new versions of **AirGate 4G Wi-Fi** firmware become available, the user can manually update their device by uploading a package.

The device will need to be manually rebooted once the upload is complete, leaving **AirGate 4G Wi-Fi** out of service for approximately 1 minute.

It is important to have a stable power source and ensure that power to the Fusion is not interrupted during a firmware upgrade.



Firmware

Firmware Upgrade

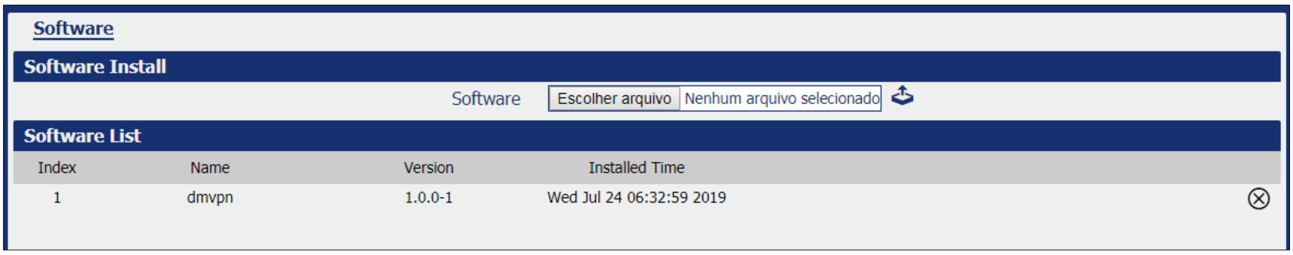
Firmware: Escolher arquivo | Nenhum arquivo selecionado ⇪

Figure 85 – Upgrade

5.8.2 SOFTWARE

When new versions of **AirGate 4G Wi-Fi** software with new features become available, the user can manually update their device by uploading a package. You can also uninstall new device features.

The device will need to be manually restarted after a package has been uploaded or some functionality has been uninstalled, leaving **AirGate 4G Wi-Fi** out of service for approximately 1 minute.



Software

Software Install

Software: Escolher arquivo | Nenhum arquivo selecionado ⇪

Software List

Index	Name	Version	Installed Time	
1	dmvpn	1.0.0-1	Wed Jul 24 06:32:59 2019	⊗

Figure 86 – Software

This parameter group has the following buttons:

⇪ **Button:** Allows you to upload a new update package.

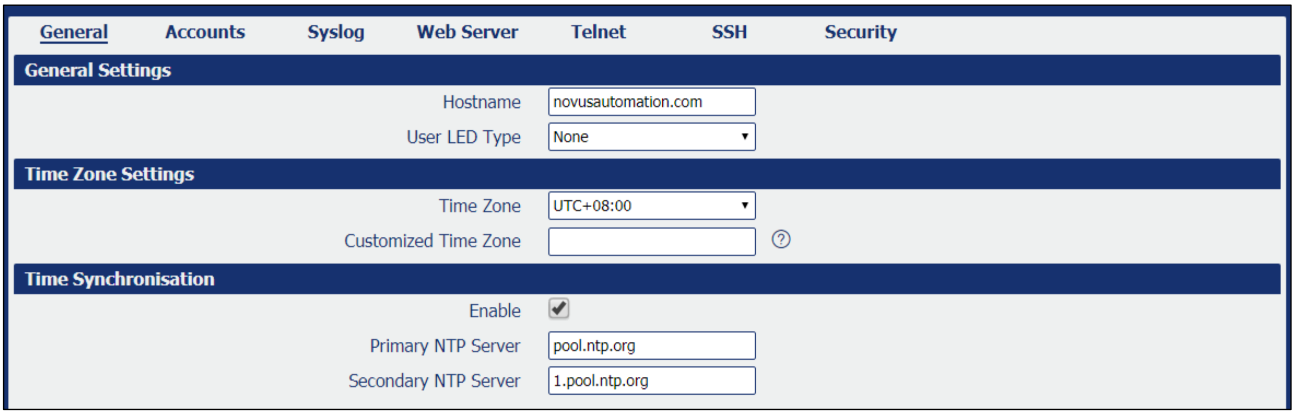
⊗ **Button:** Allows you to delete an update package.

5.8.3 SYSTEM

This tab allows you to configure the device.

5.8.3.1 SYSTEM → GENERAL

This parameter group allows you to define the general settings.



General Settings

Hostname: novusautomation.com

User LED Type: None

Time Zone Settings

Time Zone: UTC+08:00

Customized Time Zone:

Time Synchronisation

Enable: ☑

Primary NTP Server: pool.ntp.org

Secondary NTP Server: 1.pool.ntp.org

Figure 87 – System

GENERAL SETTINGS

- **Hostname:** Allows you to define the router name, which might be used to identify the IPsec local ID.
- **User LET Type:** Allows you to define the LED behavior: "None", "SIM" or "WiFi".

TIME ZONE SETTINGS

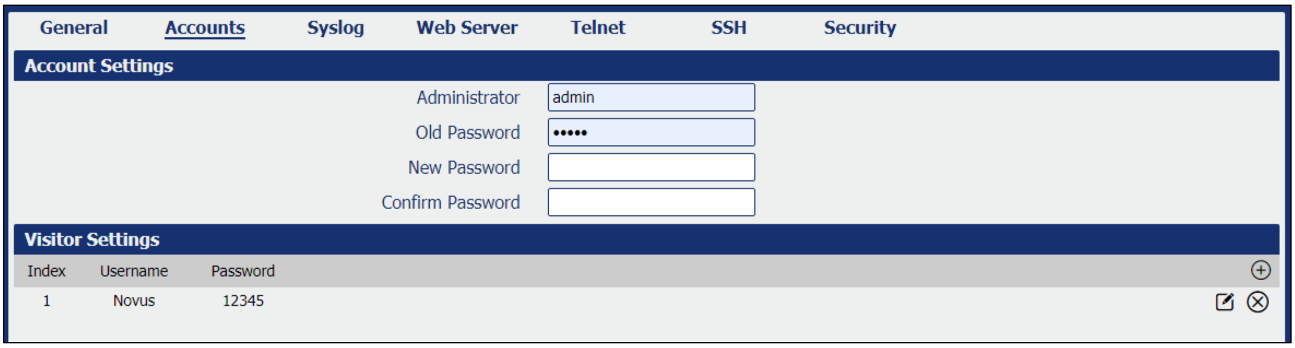
- **Time Zone:** Allows you to define the time zone where the device is in use.
- **Customized Time Zone:** Allows you to define a customized zone where the device is in use.

TIME SYNCHRONISATION

- **Enable (NTP Client):** If enabled, allows the NTP client to synchronize the device clock over the network when using a time server (NTP Server).
- **Primary NTP Server:** Allows you to enter the IP address (or host name) of the primary time server.
- **Secondary NTP Server:** Allows you to Enter the IP address (or host name) of the secondary time server.

5.8.3.2 SYSTEM → ACCOUNTS

This parameter group allows you to define user settings linked to the device.



Account Settings

Administrator: admin

Old Password: •••••

New Password:

Confirm Password:

Visitor Settings

Index	Username	Password
1	Novus	12345

Figure 88 – Account settings

ACCOUNT SETTINGS

- **Administrator:** Displays the name of current administrator, default as "admin".
- **Old Password:** Allows you to enter the old password of administrator.
- **New Password:** Allows you to enter the new password of administrator.
- **Confirm Password:** Allows you to confirm the new password of administrator.

VISITOR SETTINGS

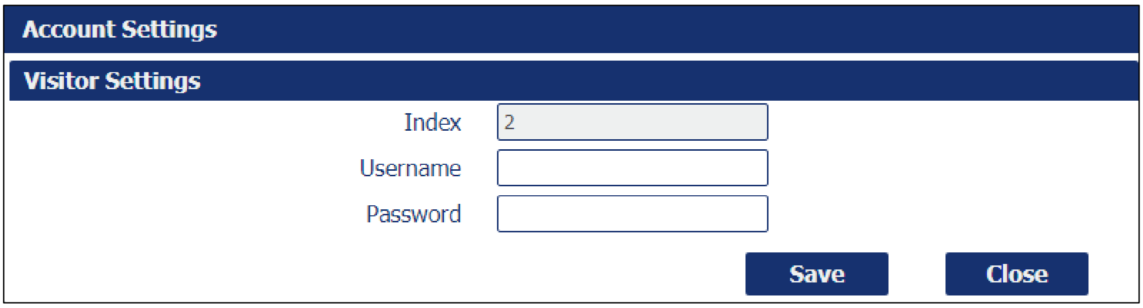
This parameter group hast the following buttons:

⊕ **Button:** Allows you to add a new visitor.

✎ **Button:** Allows you to edit the settings of the selected visitor.

⊗ **Button:** Allows you to delete the selected visitor.

As you can see in the figure below, you can create a new visitor by clicking the ⊕ button.



Account Settings

Visitor Settings

Index: 2

Username:

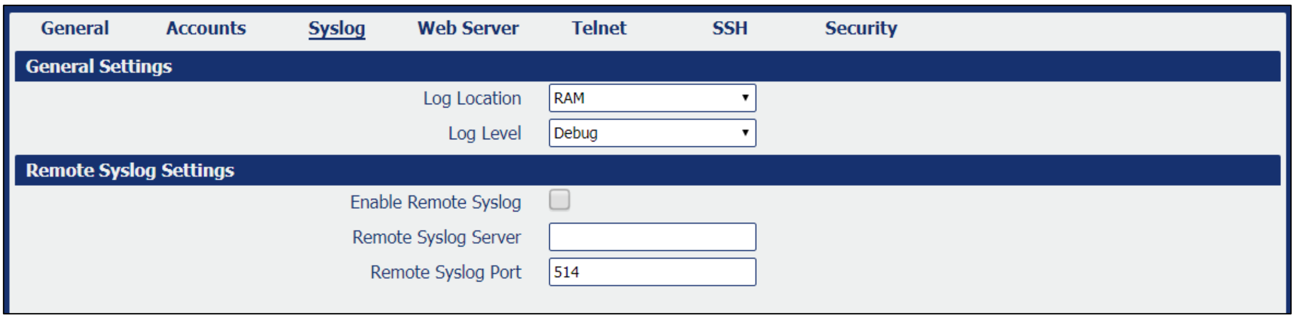
Password:

Figure 89 – Visitor settings

- **Username:** Allows you to enter a username for the visitor.
- **Password:** Allows you to define a password for the visitor account.

5.8.3.3 SYSTEM → SYSLOG

This parameter group allows you to analyze stored system log settings.



General Settings

Log Location: RAM

Log Level: Debug

Remote Syslog Settings

Enable Remote Syslog: □

Remote Syslog Server:

Remote Syslog Port: 514

Figure 90 – Syslog

GENERAL SETTINGS

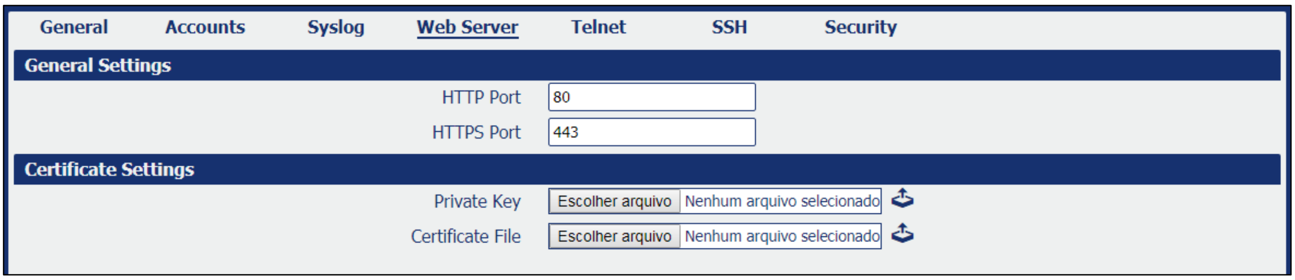
- **Log Location:** Allows you to select the log store location: "RAM" or "Flash".
- **Log Level:** Allows you to select the log output level: "Debug", "Notice", "Info", "Warning" or "Error".

REMOTE SYSLOG SETTINGS

- **Enable Remote Syslog:** Allows you to enable or disable remote syslog connection.
- **Remote Syslog Server:** Allows you to enter the IP address of remote syslog server.
- **Remote Syslog Port:** Allows you to enter the port for remote syslog server listening.

5.8.3.4 SYSTEM → WEB SERVER

This parameter group allows you to define HTTPS connection settings.



General Settings

HTTP Port: 80

HTTPS Port: 443

Certificate Settings

Private Key: Escolher arquivo Nenhum arquivo selecionado

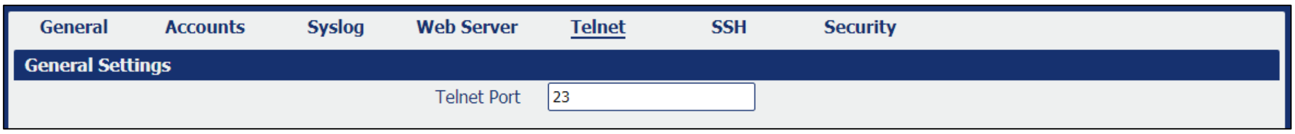
Certificate File: Escolher arquivo Nenhum arquivo selecionado

Figure 91 – Web Server

- **HTTP Port:** Allows you to enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.
- **HTTPS Port:** Allows you to enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.
- **Private Key:** Allows you to import private Key file for HTTPS connection.
- **Certificate File:** Allows you to import certificate file for HTTPS connection.

5.8.3.5 SYSTEM → TELNET

This parameter group allows you to define the Telnet port.



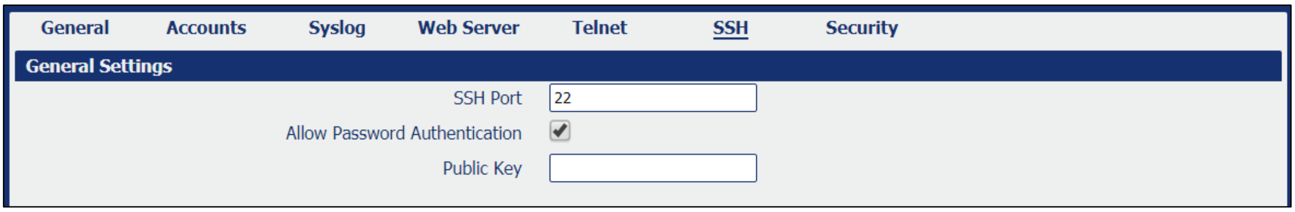
Telnet Port: 23

Figure 92 – Telnet

- **Telnet Port:** Allows you to enter the port for telnet access. A well-known port for HTTP is port 23.

5.8.3.6 SYSTEM → SSH

This parameter group allows you to enable and configure SSH.



SSH Port: 22

Allow Password Authentication: ☑

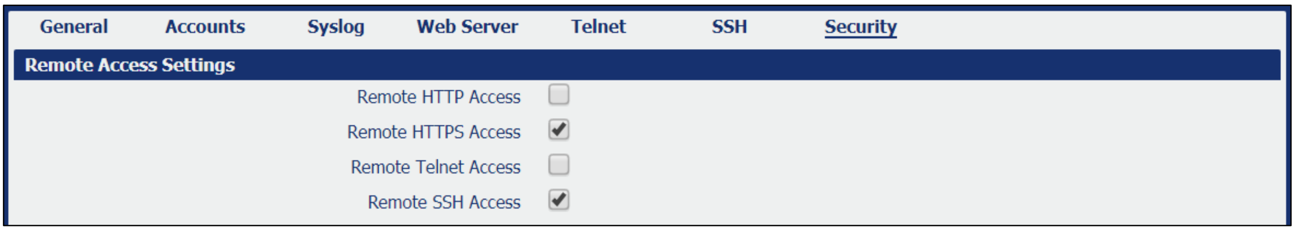
Public Key:

Figure 93 – SSH

- **SSH Port:** Allows you to enter the port for SSH access. A well-known port for HTTP is port 22.
- **Allow Password Authentication:** Allows you to enable or disable SSH authentication.
- **Public Key:** Allows you to enter the public Key SSH authentication.

5.8.3.7 SYSTEM → SECURITY

This parameter group allows you to enable or disable security settings for remote access.



Remote HTTP Access: □

Remote HTTPS Access: ☑

Remote Telnet Access: □

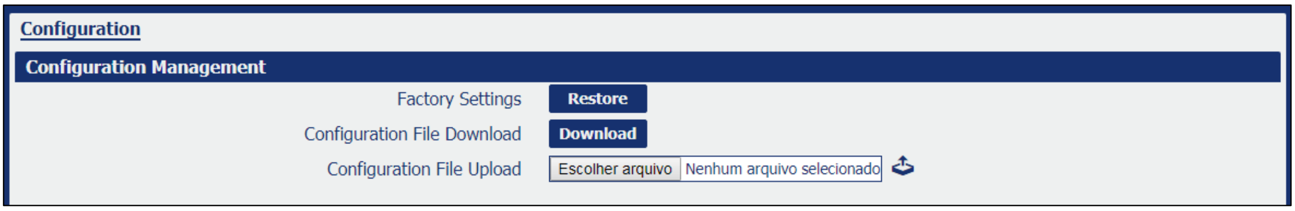
Remote SSH Access: ☑

Figure 94 – Security

- **Remote HTTP Access:** Allows you to allow remote HTTP access.
- **Remote HTTPS Access:** Allows you to allow remote HTTPS access.
- **Remote Telnet Access:** Allows you to allow remote Telnet access.
- **Remote SSH Access:** Allows you to allow remote SSH access.

5.8.4 CONFIGURATION

This tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the **AirGate 4G Wi-Fi** router to a file, you can import these previously saved configuration settings to the **AirGate 4G Wi-Fi** router as well.



Configuration Management

Factory Settings

Configuration File Download

Configuration File Upload: Nenhum arquivo selecionado

Figure 95 – Configuration

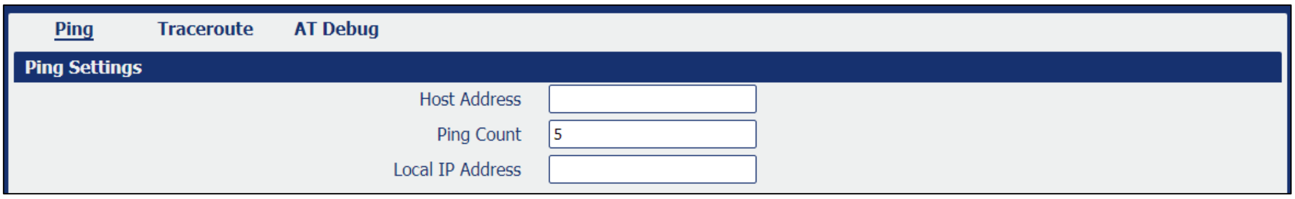
- **Factory Settings:** Click the **Restore** button allows you to reset the device to factory default settings.
- **Configuration File Download:** Click the **Download** button allows you to download the configuration file from **AirGate 4G Wi-Fi** router.
- **Configuration File Upload:** Allows you to import a previously saved configuration file.

5.8.5 DEBUG TOOLS

This tab allows you to configure debug tools.

5.8.5.1 DEBUG TOOLS → PING

This parameter group allows you to configure the tool to perform ping commands.



Ping Settings

Host Address:

Ping Count: 5

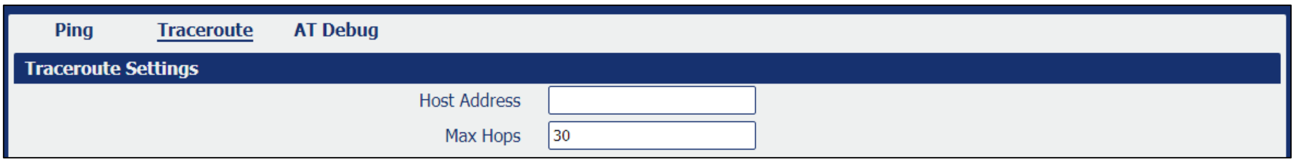
Local IP Address:

Figure 96 – Ping

- **Host Address:** Allows you to enter a host IP address or domain name for ping.
- **Ping Count:** Allows you to enter the ping times.
- **Local IP Address:** Allows you to enter the ping source IP address or leave it blank.

5.8.5.2 DEBUG TOOLS → TRACEROUTE

This parameter group allows you to configure Traceroute, whose purpose is to test the path taken by the package to its destination.



Traceroute Settings

Host Address:

Max Hops: 30

Figure 97 – Traceroute

- **Host Address:** Allows you to enter a host IP address or domain name for traceroute.
- **Max Hops:** Allows you to enter the max hops for traceroute.

6 APPLICATIONS

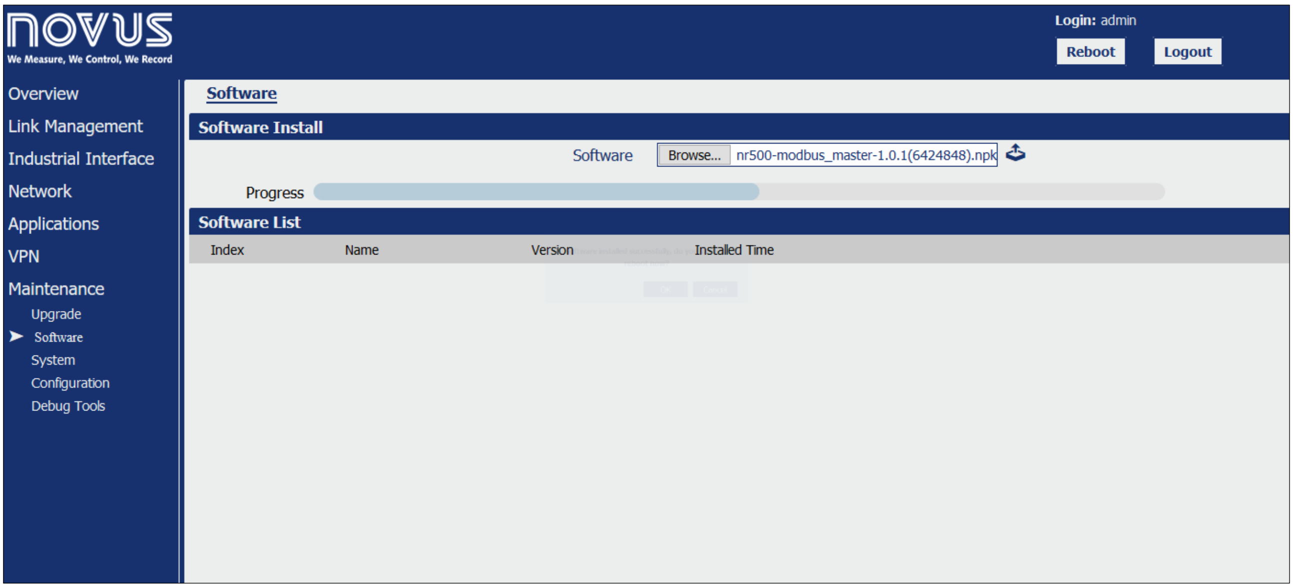
AirGate 4G Wi-Fi is compatible with multiple applications, although it allows up to 5 applications at a time. If you need to install a new application after this limit has been reached, you will need to uninstall a previously installed application.

6.1 INSTALLING AND REMOVING APPLICATIONS

Before you can configure any of the applications mentioned in this chapter, you must install it on the device. To do so, access the **Maintenance** option, located in the menu on the left of the web interface, and then click on **Software**. In the **Software Install** section, click the **Browse** button, and select the npk file for the application to be installed.

The npk files are available on the product page of the **NOVUS** website.

You must click on the ⇪ icon to upload the selected file and start the installation process:

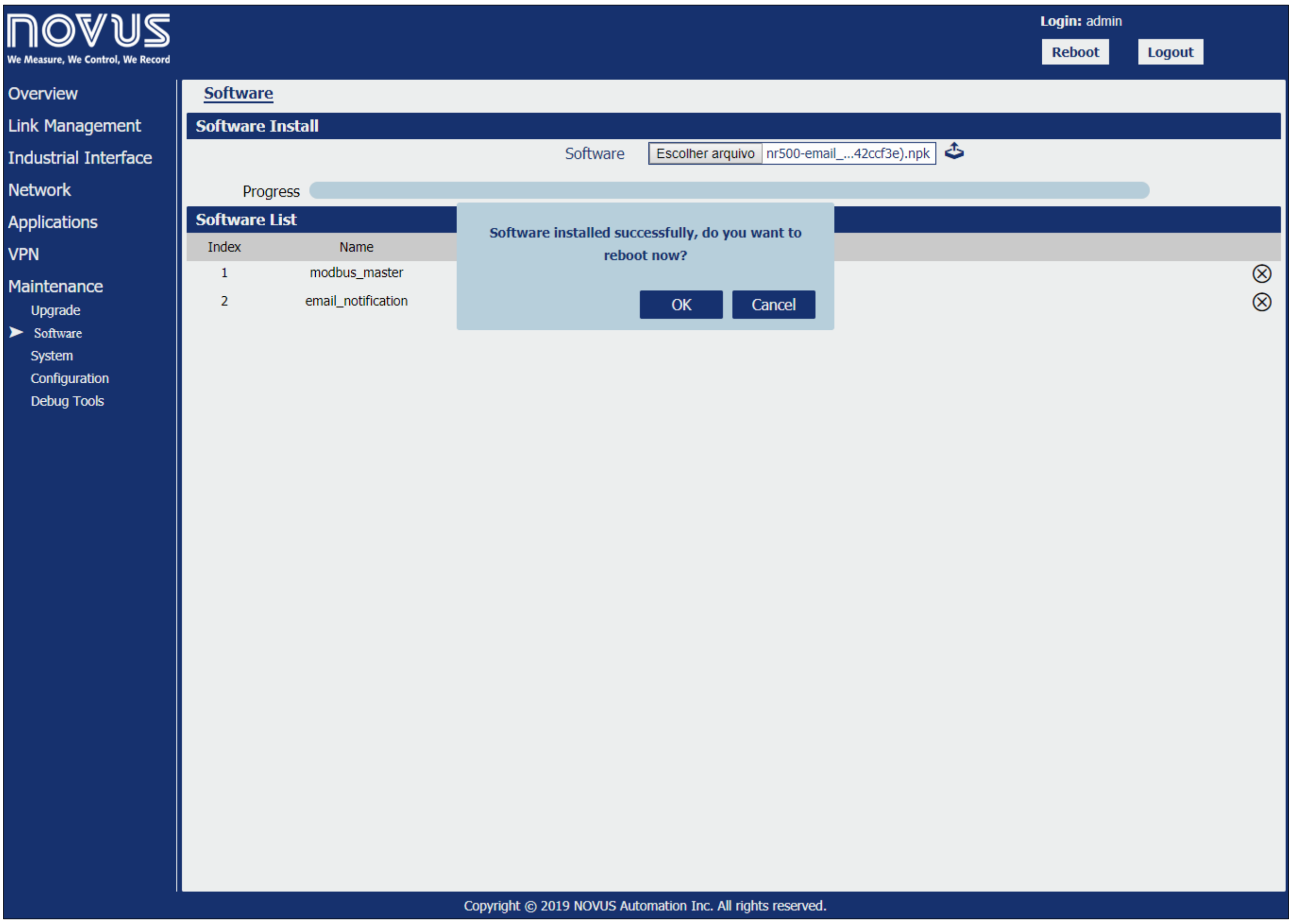


Software: Browse... nr500-modbus_master-1.0.1(6424848).npk

Progress

Figure 98 –Installing an application

A progress bar will appear at the bottom of the section. When the installation is complete, the device will display the following pop-up:



Software: Escolher arquivo nr500-email_...42ccf3e).npk

Progress

Index	Name
1	modbus_master
2	email_notification

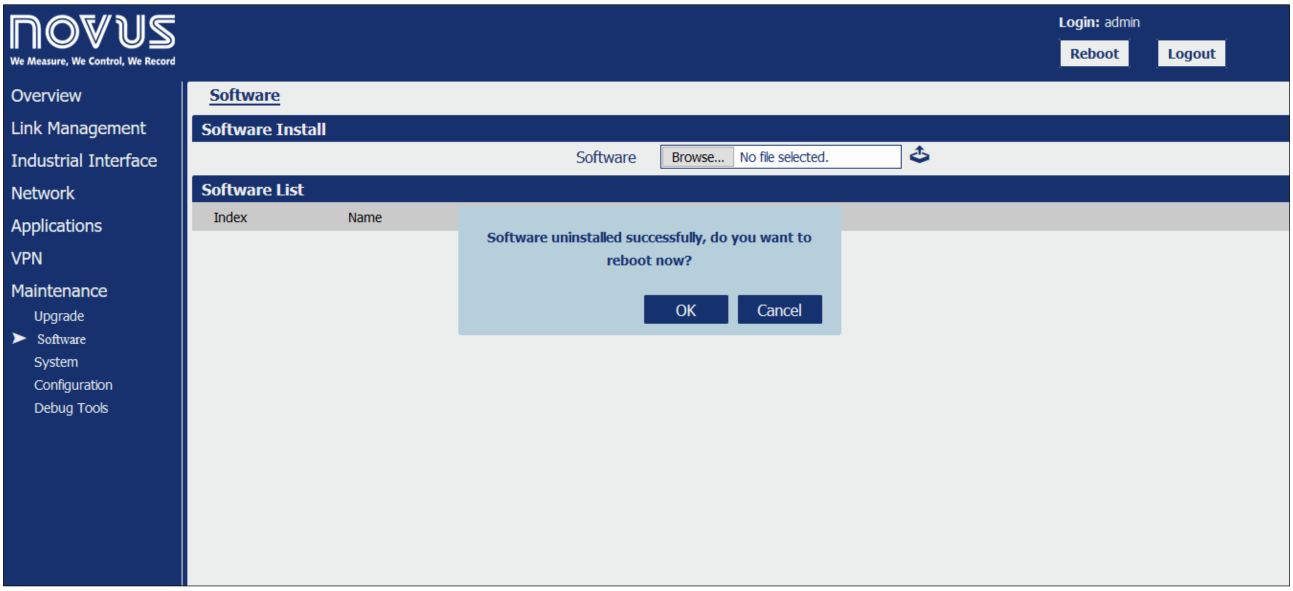
Software installed successfully, do you want to reboot now?

Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 99 – Application successfully installed

When the installation is complete, click **Ok** and wait for **AirGate 4G Wi-Fi** to restart. Once this happens, the application will be available for use.

To remove a previously installed application, you must click on the ⊗ button located next to the application in the **Software List** section. When the uninstallation is complete, the device will display the following pop-up:



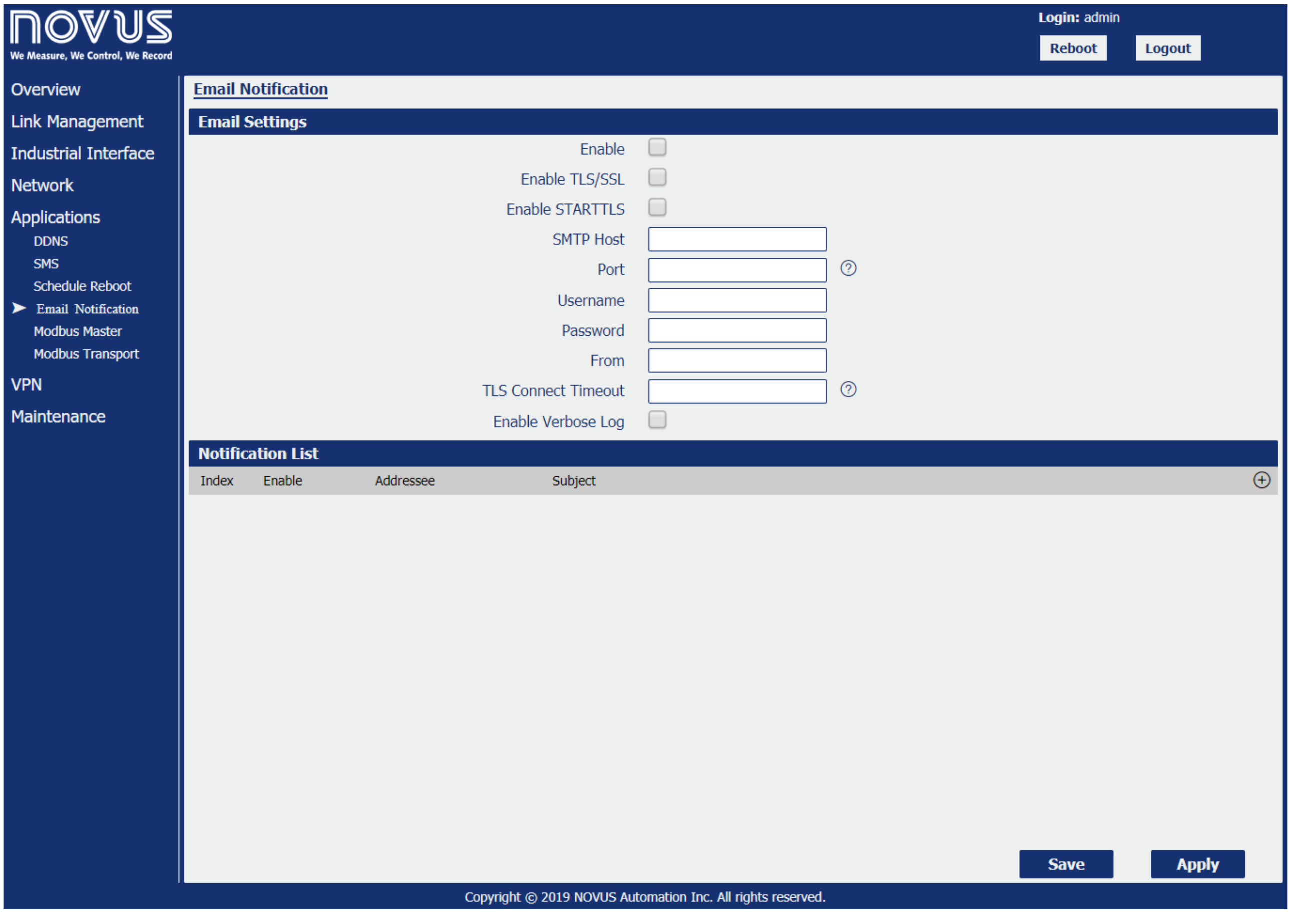
Software uninstalled successfully, do you want to reboot now?

Figure 100 – Application successfully uninstalled

Just click **Ok** and wait for **AirGate 4G Wi-Fi** to restart.

6.2 "EMAIL NOTIFICATION" APPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, it can be configured via the **AirGate 4G Wi-Fi** web interface. Access the **Applications** option, located on the left menu, and then click on **Email Notification**, as shown below:



Email Notification

Email Settings

Enable □
Enable TLS/SSL □
Enable STARTTLS □
SMTP Host
Port
Username
Password
From
TLS Connect Timeout
Enable Verbose Log □

Notification List

Index	Enable	Addressee	Subject

Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 101 – Configuring the email sending

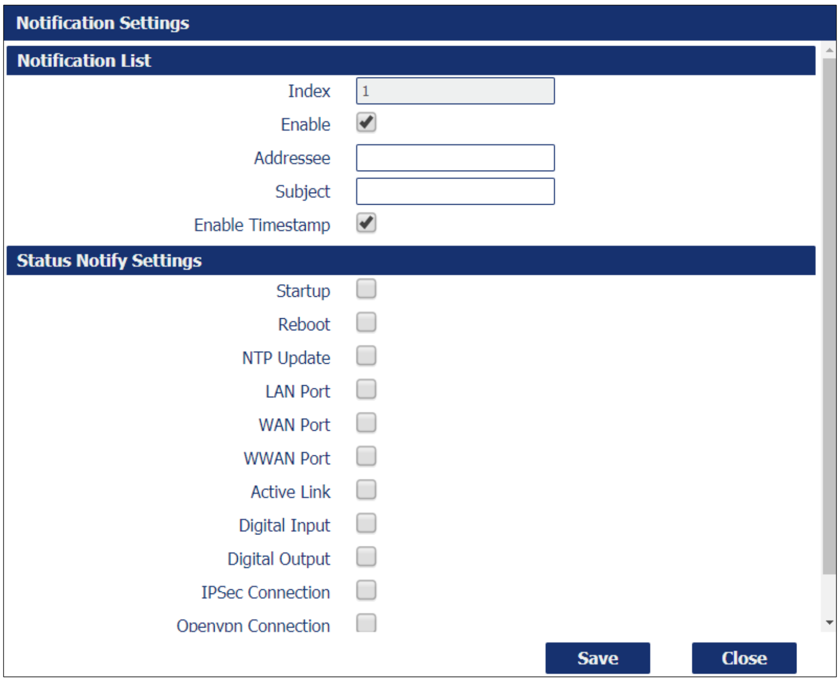
This application is compatible with **AirGate 4G Wi-Fi** firmware version 1.1.4.

6.2.1 EMAIL SETTINGS

These parameters allow you to configure the email service and the email account to be used by the application:

- **Enable:** Allows you to enable the email notification.
- **Enable TLS/SSL:** Allows you to enable the security in the transport layer (TLS) of communication with the SMTP server.
- **Enable STARTTLS:** Allows you to enable the use of the STARTTLS command at the beginning of the communication with the SMTP server.
- **SMTP Host:** Allows you to enable the insertion of the SMTP server address.
- **Port:** Allows you to insert the communication port with the SMTP server. By default, most SMTP servers can provide up to three ports:
  - **Port 25:** Port used without any type of transport layer security. By default, it should be used when **Enable TLS/SSL** and **Enable STARTTLS** are not selected. Since data send through port is unprotected, the use is not recommended.
  - **Port 465:** Port used with TLS/SSL protocol. By default, it should be used when only the **Enable TLS/SSL** option is selected.
  - **Port 587:** Port used with the TLS protocol established after sending the STARTTLS command. By default, it should be used when only **Enable STARTTLS** is selected.
- **Username:** Allows you to enter the username of the email account to be used.
- **Password:** Allows you to enter the password for the email account to be used.
- **From:** Allows you to enter the email address of the account to be used.
- **TLS Connect Timeout:** Allows you to configure the TLS connection timeout.
- **Enable Verbose Log:** Allows you to enable a detailed log in the message body of the outgoing emails.

Once the configuration parameters have been filled, click the **Save** button, located in the right corner of the screen. Then, you must enter the information of the email accounts that should receive the notifications, as well as the conditions that generate these emails. To do so, click on the ⊕ button, located on the right corner of the **Notification List** section, and then fill in the following fields:



Notification Settings

Notification List

Index 1

Enable ☑

Addressee

Subject

Enable Timestamp ☑

Status Notify Settings

Startup □

Reboot □

NTP Update □

LAN Port □

WAN Port □

WWAN Port □

Active Link □

Digital Input □

Digital Output □

IPSec Connection □

Openvpn Connection □

Figure 102 – Notification list

6.2.1.1 NOTIFICATION LIST

These parameters allow you to define the subject and email address to be included in the notification list, as well as enabling or disabling other settings.

- **Enable:** Allows you to enable the sending of email notifications to the configured address.
- **Address:** Allows you to enter the email address to receive the notifications.
- **Subject:** Allows you to insert the subject of the emails to be sent to this address.
- **Enable Timestamp:** Allows you to write in the email notification of the timestamp at the moment the condition of notification is triggered.

6.2.1.2 STATUS NOTIFY SETTINGS

These parameters allow you to define the situations in which notifications will be sent.

- **Startup:** Enables notification emails to be sent every time the system is booted.
- **Reboot:** Enables notification emails to be sent every time the system is rebooted.
- **NTP Update:** Enables notification emails to be sent every time the internal clock is updated from an NTP server.
- **LAN Port:** Enables notification emails to be sent every time a LAN port is connected or disconnected through an Ethernet output.
- **WAN Port:** Enables notification emails to be sent every time a WAN port is connected or disconnected through an Ethernet output.
- **WWAN Port:** Enables notification emails to be sent every time a WWAN port is connected or disconnected through the 4G interface.
- **Active Link:** Enables notification emails to be sent every time an active link is connected or disconnected through a WAN or WWAN port.
- **Digital Input:** Enables notification emails to be sent every time there is a change in the logical level of one of the digital inputs.
- **Digital Output:** Enables notification emails to be sent every time there is a change in the logical level of any of the digital outputs.
- **IPsec Connection:** Enables notification emails to be sent every time a VPN connection with IPsec is established.
- **OpenVPN Connection:** Enables notification emails to be sent whenever a VPN connection to OpenVPN is established.
- **Modbus Alarm:** Enables notification emails to be sent each time a Modbus alarm is detected. For more information on configuring a Modbus alarm for sending notification emails, see section EMAIL ACCOUNT SETUP from this chapter.

6.2.2 EMAIL ACCOUNT SETUP

Different email servers have different security policies. Depending on the server, additional settings may be required in the email account so that **AirGate 4G Wi-Fi** can send email from it. Below are the settings required to send email through two different servers: Gmail and Yahoo.

Other servers may require other settings to allow sending email from third-party applications.

6.2.2.1 GMAIL

To send email through a Gmail account, you must allow access through less secure applications. This can be done through the Google account security menu, which can be accessed from the following link: https://myaccount.google.com/security?gar=1.

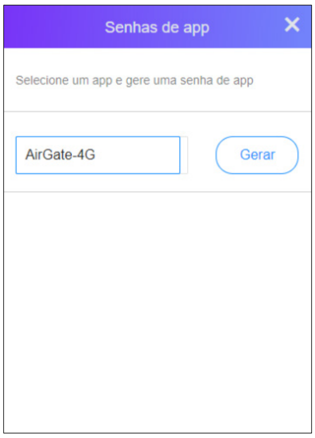
Alternatively, you can also access this menu through a Google page by clicking the **Manage Your Google Account** option and then selecting the **Security** option from the menu on the left.

Once on the **Security** menu, simply find the **Less secure app access** option and click **Enable access (not recommended)**. Then click on the button that appears on the screen, so that the warning "Allow less secure applications: ENABLED" is shown

6.2.2.2 YAHOO

To send emails through a Yahoo account, you must create an alternative password for access through third-party applications. Once the Yahoo account to be used is open, simply click on the user's profile photo, located in the top right corner of the screen, and then on **Account Information**. Then select the **Account Security** option, located in the menu on the left.

Once on the **Security** menu, you must select the **Manage app passwords** option, click **Select your application**, and enter a name for the **AirGate 4G Wi-Fi** application. Then, just click **Generate**, as shown below:



Senhas de app

Selecione um app e gere uma senha de app

AirGate-4G

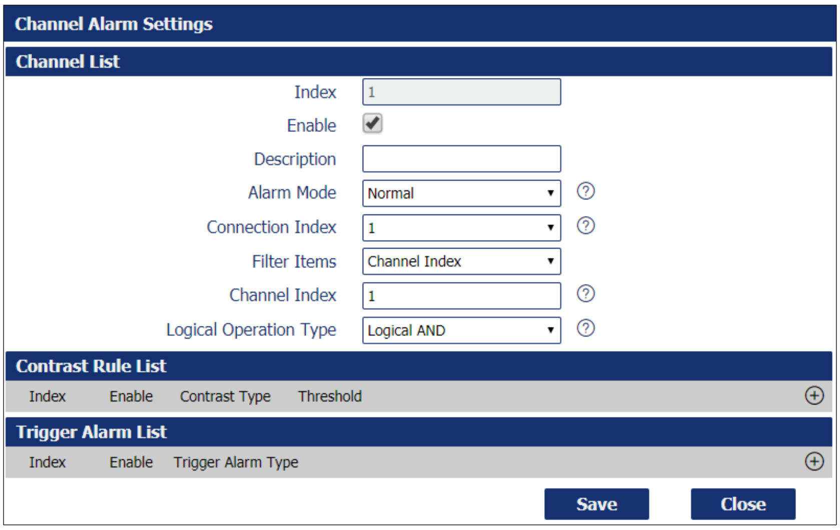
Figure 103 – Yahoo settings

After saving the password generated by Yahoo, click **Done**. This password must be used on the **AirGate 4G Wi-Fi** web interface to set up the email account in the **Password** field.

6.2.2.3 AIRGATE 4G WI-FI CONFIGURATION EXAMPLE

This section provides an example of how to configure the **AirGate 4G Wi-Fi** email notification process. In this case, the sending of notification emails will be performed through an Outlook email account and notifications for Modbus alarm and initialization will be activated. Thus, in the first part of this example a Modbus alarm will be configured for one of the registers read by the Modbus master. In the second part, email notification will be configured.

For this example, **AirGate 4G Wi-Fi** has been previously configured as Modbus master for reading registers from a Modbus slave (see "MODBUS MASTER" APPLICATION section of this chapter). Thus, to set up an alarm, simply click on **Applications** and then click on **Modbus Master**. Once this is done, click on **Modbus Alarm** and then click on the button ⊕, located in the upper right corner of the section. You can then configure Modbus Alarm, as shown below:



Channel Alarm Settings

Channel List

Index	1
Enable	☑
Description	
Alarm Mode	Normal
Connection Index	1
Filter Items	Channel Index
Channel Index	1
Logical Operation Type	Logical AND

Contrast Rule List

Index	Enable	Contrast Type	Threshold

Trigger Alarm List

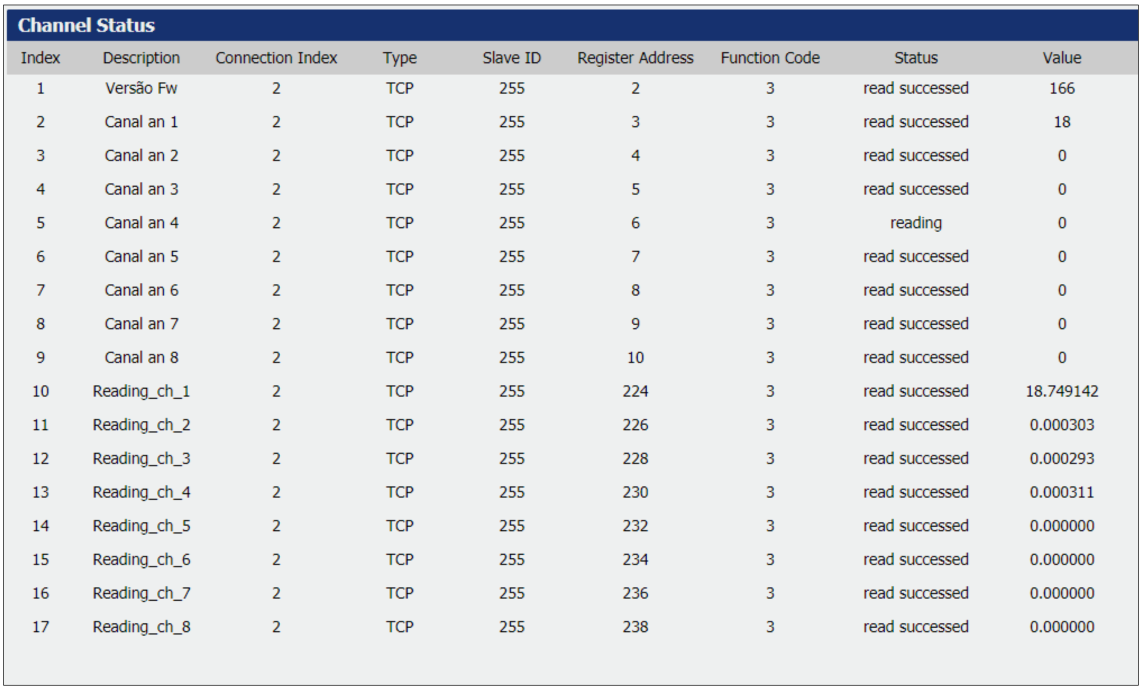
Index	Enable	Trigger Alarm Type

Figure 104 – Configuring a Modbus alarm

You must add an alarm description in the **Description** field and select the "Normal" option in the **Alarm Mode** parameter. After that, in the **Connection Index** parameter, choose the connection number for the Modbus slave to be read. Under **Filter Items**, select the "Register Address" option and enter the address value of the register to which an alarm is to be associated.

In the **Contrast Rule List** section, click the ⊕ button to add the condition that should create the alarm. Then, in the **Alarm Trigger List** section, click the ⊕ button to define the alarm settings to be created. In this screen, you must select the **Event Notification** parameter and, in **Alarm ON Content**, write the message to be sent in the body of the email when the alarm is triggered. Under **Alarm OFF Content**, write the message to be sent when the alarm condition is no longer met. You can use indexers to write these messages.

In this example an alarm will be created for a setup where **AirGate 4G Wi-Fi** is reading registers from a Modbus slave via TCP. The list of registers read can be seen in the picture below:

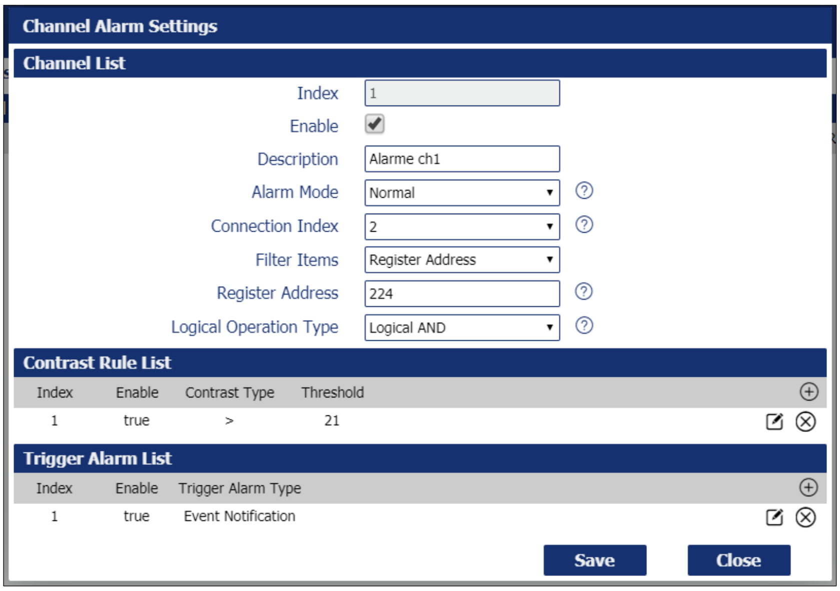


Channel Status

Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	Status	Value
1	Versão Fw	2	TCP	255	2	3	read successed	166
2	Canal an 1	2	TCP	255	3	3	read successed	18
3	Canal an 2	2	TCP	255	4	3	read successed	0
4	Canal an 3	2	TCP	255	5	3	read successed	0
5	Canal an 4	2	TCP	255	6	3	reading	0
6	Canal an 5	2	TCP	255	7	3	read successed	0
7	Canal an 6	2	TCP	255	8	3	read successed	0
8	Canal an 7	2	TCP	255	9	3	read successed	0
9	Canal an 8	2	TCP	255	10	3	read successed	0
10	Reading_ch_1	2	TCP	255	224	3	read successed	18.749142
11	Reading_ch_2	2	TCP	255	226	3	read successed	0.000303
12	Reading_ch_3	2	TCP	255	228	3	read successed	0.000293
13	Reading_ch_4	2	TCP	255	230	3	read successed	0.000311
14	Reading_ch_5	2	TCP	255	232	3	read successed	0.000000
15	Reading_ch_6	2	TCP	255	234	3	read successed	0.000000
16	Reading_ch_7	2	TCP	255	236	3	read successed	0.000000
17	Reading_ch_8	2	TCP	255	238	3	read successed	0.000000

Figure 105 – Register list

The Modbus alarm created will be triggered whenever the value read from the register of address 224 exceeds the value of 21. The following alarm settings will be used for this:



Channel Alarm Settings

Channel List

Index	1
Enable	☑
Description	Alarme ch1
Alarm Mode	Normal
Connection Index	2
Filter Items	Register Address
Register Address	224
Logical Operation Type	Logical AND

Contrast Rule List

Index	Enable	Contrast Type	Threshold
1	true	>	21

Trigger Alarm List

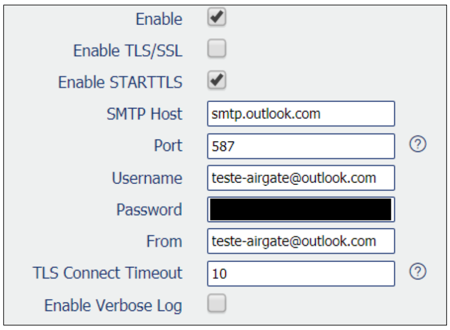
Index	Enable	Trigger Alarm Type
1	true	Event Notification

Figure 106 – Alarm condition

The following message will be sent by email during an alarm condition: "Value read in $CHANNEL_DESC ($VALUE), address register $REGISTER_ADDER, is in alarm condition". This message makes use of indexers, which will be replaced with information from the Modbus register cited.

The message to be sent when the register is no longer in alarm condition has only replaced the final part of the previous message with "not in alarm condition".

After adding the alarm parameters, simply click **Save** and then **Apply**. Once the Modbus alarm has been configured, you need to configure the email notification parameters. To do this, click on **Applications**, located on the left menu, and then click on **Email Notification**. On the following screen, fill in the data of the email that will be used to send the message, as in the example below:



Enable	☑
Enable TLS/SSL	□
Enable STARTTLS	☑
SMTP Host	smtp.outlook.com
Port	587
Username	teste-airgate@outlook.com
Password	[redacted]
From	teste-airgate@outlook.com
TLS Connect Timeout	10
Enable Verbose Log	□

Figure 107 – Email settings

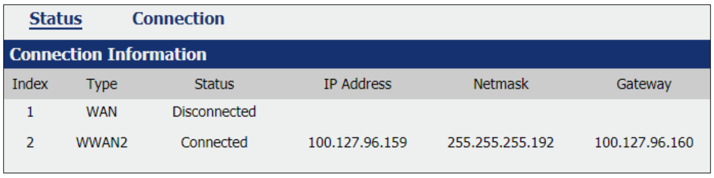
If another email provider is used, you must know the address of the SMTP server to fill in the above information. If **Enable STARTTLS** is selected, most servers support port 587. As explained above, for some email services, additional account settings may be required to enable sending email from **AirGate 4G Wi-Fi**. In this example with Outlook, none were required.

You should then add the email accounts that will receive the notifications. Simply click the ⊕ button located in the **Notification List** section to add an email address, the email subject, and the notification conditions. In this example, the address that receives the notifications will be the same as the one that sends them. The conditions **Startup** and **Modbus Alarm** have been chosen.

After adding these settings, you must click **Save** and then **Apply**.

At this point, the sending of notification emails in case of Modbus alarms and **AirGate 4G Wi-Fi** initialization is configured. Before testing sending notification emails, it is important to verify that the **AirGate 4G Wi-Fi** is connected to the Internet by clicking **Link Management** and then **Connection Manager**.

In the **Connection Information** section, the **Status** column should display the message "Connected" for at least one of the connections shown, as in the figure below:

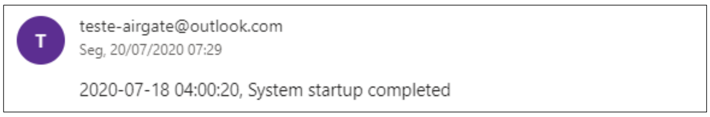


Connection Information

Index	Type	Status	IP Address	Netmask	Gateway
1	WAN	Disconnected			
2	WWAN2	Connected	100.127.96.159	255.255.255.192	100.127.96.160

Figure 108 – **AirGate 4G Wi-Fi** connection status

Once the **AirGate 4G Wi-Fi** is connected, you will need to reboot your device by clicking the **Reboot** button located in the upper right corner of the web interface. After the device initialization, you can check the notification for its initialization in the email inbox, as shown below:



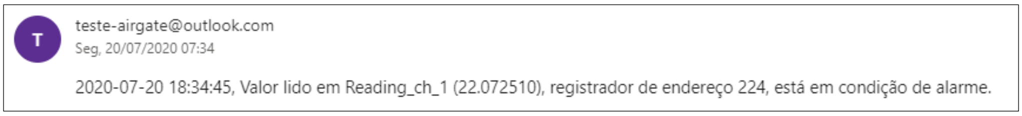
teste-airgate@outlook.com

Seg, 20/07/2020 07:29

2020-07-18 04:00:20, System startup completed

Figure 109 – Startup notification email

The email received corresponds to the **Startup** notification condition configured earlier. Similarly, once the **AirGate 4G Wi-Fi** reads the 224 address register from the Modbus slave and the read value is in the specified alarm condition (greater than 21), another notification email will be received, as shown in the figure below:



teste-airgate@outlook.com

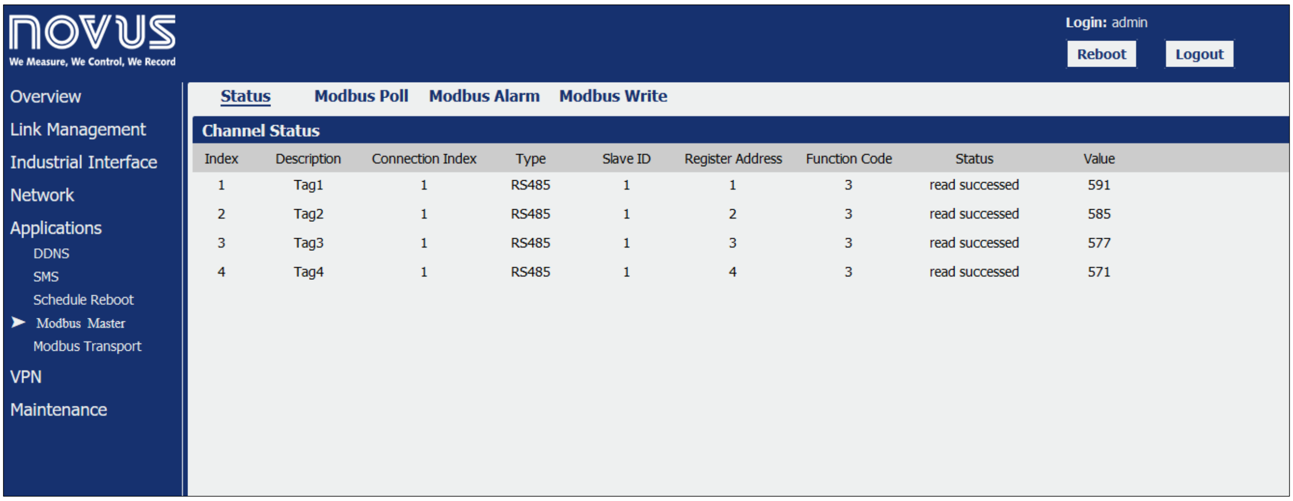
Seg, 20/07/2020 07:34

2020-07-20 18:34:45, Valor lido em Reading_ch_1 (22.072510), registrador de endereço 224, está em condição de alarme.

Figure 110 – Register notification email

6.3 "MODBUS MASTER" APPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, it can be configured via the **AirGate 4G Wi-Fi** web interface. Access the **Applications** option, located on the left menu, and then click on **Modbus Master**, as shown below:



Channel Status

Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	Status	Value
1	Tag1	1	RS485	1	1	3	read successed	591
2	Tag2	1	RS485	1	2	3	read successed	585
3	Tag3	1	RS485	1	3	3	read successed	577
4	Tag4	1	RS485	1	4	3	read successed	571

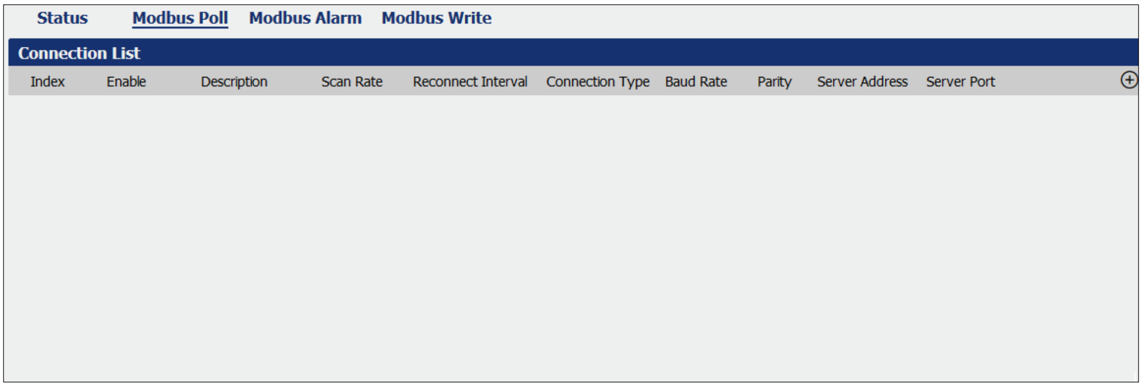
Figure 111 – Modbus Master application

This feature allows you to read the slave values of a Modbus network. The network can be either RTU over RS485 and RS232 or Modbus TCP (Server).

This application is compatible with **AirGate 4G Wi-Fi** firmware version 1.1.4.

6.3.1 MODBUS POLL

Modbus Poll allows you to create and configure a network of slaves.



Connection List

Index	Enable	Description	Scan Rate	Reconnect Interval	Connection Type	Baud Rate	Parity	Server Address	Server Port

Figure 112 – Configuring a slave network

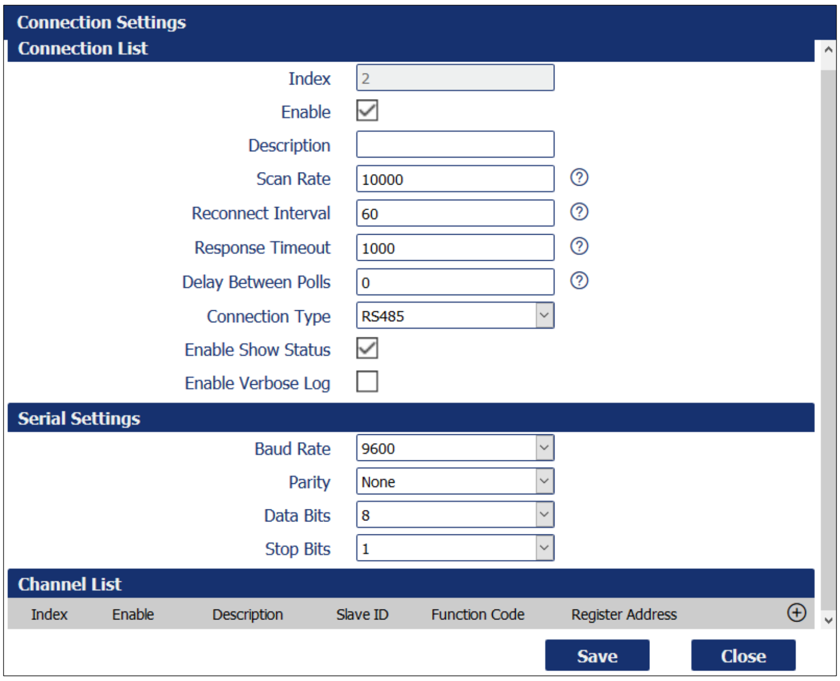
This parameter group has the following buttons:

Button ⊕**:** Allows you to add a new network.

Button ✎**:** Allows you to edit the settings of the selected network.

Button ⊗**:** Allows you to delete the selected network.

As you can see in the picture below, you can create a new configuration by clicking the button ⊕:



Connection Settings

Connection List

Index	2
Enable	☑
Description	
Scan Rate	10000
Reconnect Interval	60
Response Timeout	1000
Delay Between Polls	0
Connection Type	RS485
Enable Show Status	☑
Enable Verbose Log	□

Serial Settings

Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1

Channel List

Index	Enable	Description	Slave ID	Function Code	Register Address

Figure 113 – Connection settings

6.3.1.1 CONNECTION SETTINGS

- **Enable:** Allows you to enable a connection. A connection already created can be configured, but not enabled.
- **Description:** Allows you to insert a description for the connection to be created. For the correct connection to the **NOVUS Cloud**, do not use space, dot, dash, or other special characters in this field. Examples allowed: SPN1200, SP_N1200.
- **Scan Rate:** Allows you to set the slaves reading rate. Range: 100 ~3600000 ms. It is recommended to use a higher rate according to the number of slaves.
- **Reconnect Interval:** Allows you to set the reconnect time. Range: 1~600 s.
- **Response Timeout:** Allows you to set the time the device waits for a response. Range: 20~10000 ms.
- **Delay Between Polls:** Allows you to set the time between commands. Range: 0~10000 ms.
- **Connection Type:** Allows you to set the type of connection: RS232, RS485 or TCP.
- **Enable Show Status:** Allows the connection status to be shown on the status screen.
- **Enable Verbose Log:** Allows you to display a detailed log.

6.3.1.2 SERIAL SETTINGS RS485 / RS232

- **Baud Rate:** Allows you to set the Baud Rate to be used: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Parity:** Allows you to set the parity to be used: "None", "Even" or "Odd".
- **Data bits:** Allows you to define the data bits. Only selectable 8.
- **Stop bits:** Allows you to set the number of stop bits: 1 or 2.

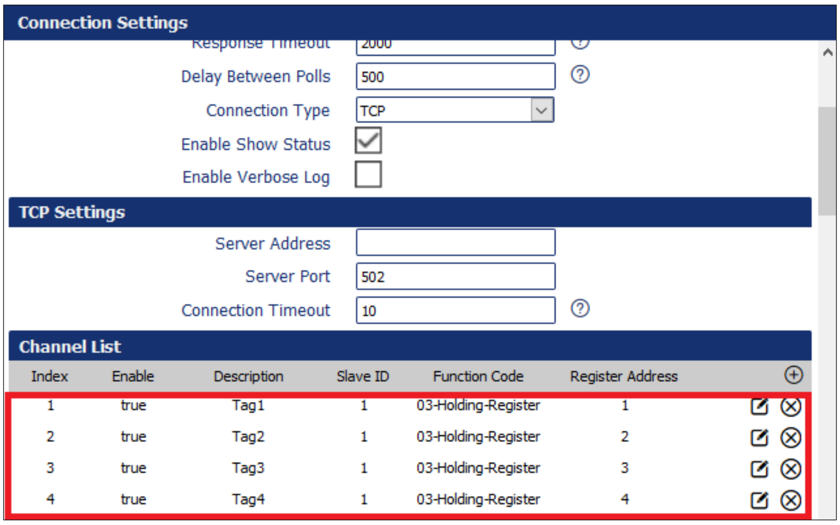
6.3.1.3 SERIAL SETTINGS TCP

- **Server Address:** Allows you to set the IP address of the slave to be read.
- **Server Port:** Allows you to set the server port. By default, port 502.
- **Connection Timeout:** Allows you to set the connection time between 1 and 30 s.

6.3.1.4 CHANNEL LIST

This section allows you to configure the Modbus registers that will be read on each connection. Up to 65 addresses are allowed per connection.

To add a new register, click the button ⊕. Once this is done, you can edit the parameters of this register by clicking the ✎ button or delete it by clicking the ⊗ button, as shown below:



Response Timeout: 2000

Delay Between Polls: 500

Connection Type: TCP

Enable Show Status: ☑

Enable Verbose Log: □

Server Address:

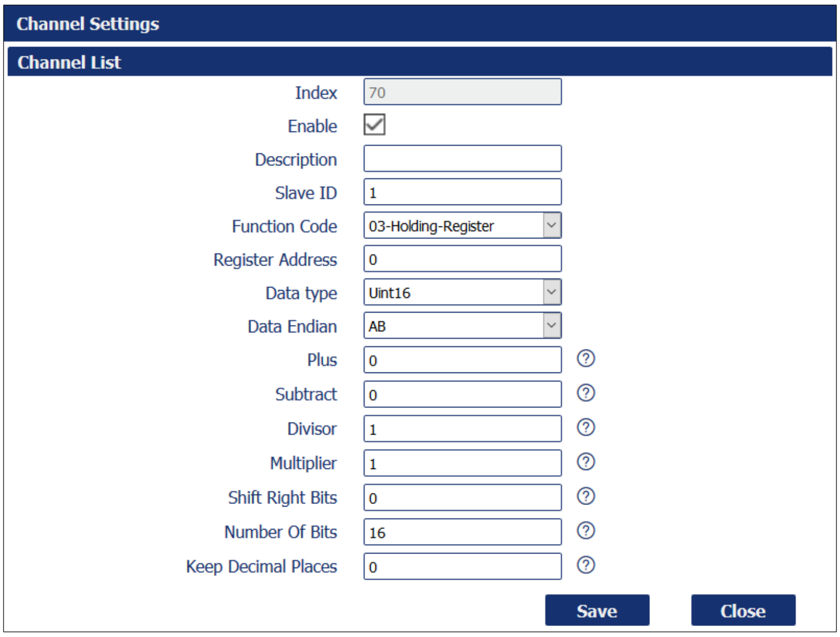
Server Port: 502

Connection Timeout: 10

Index	Enable	Description	Slave ID	Function Code	Register Address
1	true	Tag1	1	03-Holding-Register	1
2	true	Tag2	1	03-Holding-Register	2
3	true	Tag3	1	03-Holding-Register	3
4	true	Tag4	1	03-Holding-Register	4

Figure 114 – Register list

You must set the following parameters to set up a new register:



Index: 70

Enable: ☑

Description:

Slave ID: 1

Function Code: 03-Holding-Register

Register Address: 0

Data type: Uint16

Data Endian: AB

Plus: 0

Subtract: 0

Divisor: 1

Multiplier: 1

Shift Right Bits: 0

Number Of Bits: 16

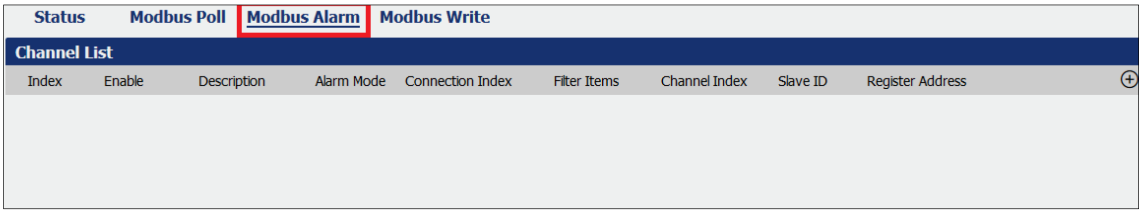
Keep Decimal Places: 0

Figure 115 – Adding a new register

- **Enable:** Allows you to enable a channel. A channel already created can be configured, but not enabled.
- **Description:** Allows you to insert a description for the connection to be created. For the correct connection to the **NOVUS Cloud**, do not use space, dot, dash, or other special characters in this field. Examples allowed: SPN1200, SP_N1200.
- **Slave ID:** Allows you to identify which network slave will be read from the register.
- **Function Code:** Allows you to define the function code to be used: 01-Coil-Status, 02-Input-Status, 03-Holding-register, or 04-Input-Registers.
- **Register Address:** Allows you to define the address of the register to be read.
- **Data type:** Allows you to define the data type: Unit 16, Int16, Unit 32, Float or RAW.
- **Data endian:** Allows you to define the bytes storage mode: AB (most significant at the beginning / big-endian) or BA (less significant at the beginning / little-endian).
- **Plus:** Allows you to add some value to the value read by the register. Range: 0~32767.
- **Subtract:** Allows you to subtract some value from the value read by the register. Range: 0~32767.
- **Split:** Allows you to divide any value by the value read from the register. Default Range: 0~32767.
- **Multiplier:** Allows you to multiply some value by the value read from the register. By default, 1. Range: 0~32767.
- **Shift right bits**: Allows you to set the number of bits to be shifted to the right. Range: 0~31.
- **Number of bits:** Allows you to set the number of bits to be read from the register (right to left). Range: 0~16.
- **Keep Decimal Places:** Allows you to set the number of decimal places to be kept by the recorder. Range: 0~5.

6.3.2 MODBUS ALARM

Modbus Alarm allows you to create alarms for Modbus variables read by the device. You can set up to 100 Modbus alarms.



Index	Enable	Description	Alarm Mode	Connection Index	Filter Items	Channel Index	Slave ID	Register Address	⊕

Figure 116 – Setting an alarm

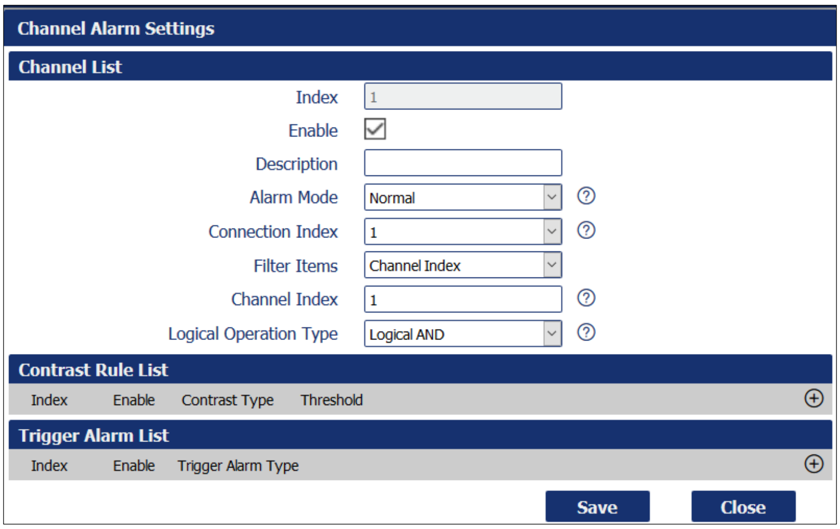
This parameter group has the following buttons:

Button ⊕: Allows you to add a new alarm.

Button ✎: Allows you to edit the settings of the selected alarm.

Button ⊗: Allows you to delete the selected alarm.

As you can see in the picture below, you can create a new alarm by clicking the button ⊕:



Channel Alarm Settings

Channel List

Index	1
Enable	☑
Description	
Alarm Mode	Normal
Connection Index	1
Filter Items	Channel Index
Channel Index	1
Logical Operation Type	Logical AND

Contrast Rule List

Index	Enable	Contrast Type	Threshold	⊕

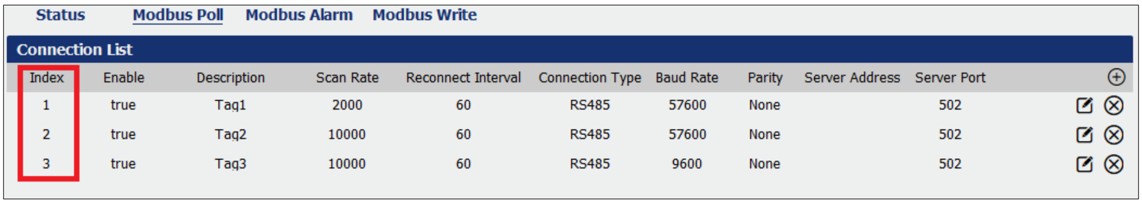
Trigger Alarm List

Index	Enable	Trigger Alarm Type	⊕

Figure 117 – Creating an alarm

CHANNEL LIST

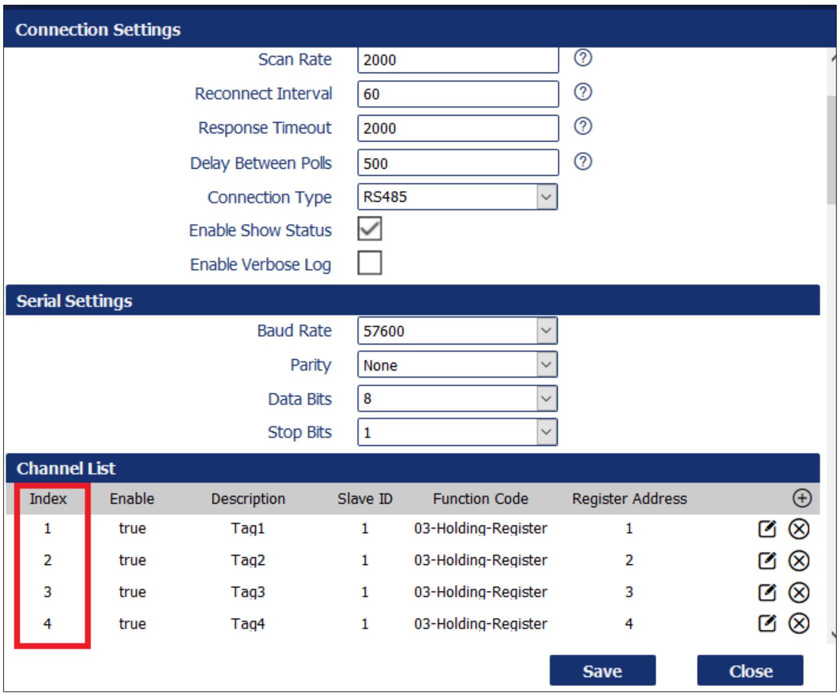
- **Enable:** Allows you to enable an alarm.
- **Description:** Allows you to enter a description for the alarm.
- **Alarm mode:** Allows you to set the alarm mode: "Normal", "Continuous" or "Every Time". If you select the "Normal" option, the alarm will be triggered once, indicating that you have exceeded the configured condition. If you select the "Continuous" option, the alarm will remain active if the alarm condition is true. If you select the "Every Time" option, the alarm will be activated whenever the alarm condition is true.
- **Connection Index:** Allows you to define the order in which the connection will be displayed in the Modbus Poll index. If 3 different connections are configured, for example, it will be necessary to define the order between them, as shown in the figure below:



Index	Enable	Description	Scan Rate	Reconnect Interval	Connection Type	Baud Rate	Parity	Server Address	Server Port	⊕
1	true	Tag1	2000	60	RS485	57600	None		502	✎ ⊗
2	true	Tag2	10000	60	RS485	57600	None		502	✎ ⊗
3	true	Tag3	10000	60	RS485	9600	None		502	✎ ⊗

Figure 118 – Order of alarms

- **Filter Items:** Allows defining other criteria to select alarms: Channel Index, Slave ID, or Register Address.
- **Channel Index:** Allows setting an index for the registers. Registers can be configured within each connection. The registers will receive a key figure for the creation order. When an index is selected, it is oriented through the index assigned to each register, as shown in the figure below:



Connection Settings

Scan Rate: 2000

Reconnect Interval: 60

Response Timeout: 2000

Delay Between Polls: 500

Connection Type: RS485

Enable Show Status: ☑

Enable Verbose Log: □

Serial Settings

Baud Rate: 57600

Parity: None

Data Bits: 8

Stop Bits: 1

Channel List

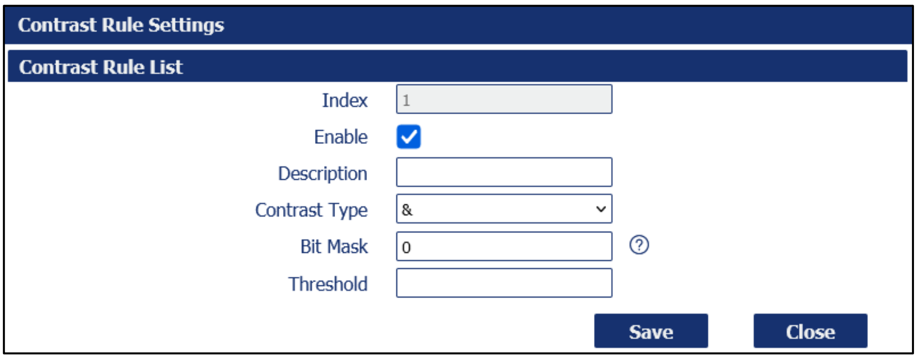
Index	Enable	Description	Slave ID	Function Code	Register Address
1	true	Tag1	1	03-Holding-Register	1
2	true	Tag2	1	03-Holding-Register	2
3	true	Tag3	1	03-Holding-Register	3
4	true	Tag4	1	03-Holding-Register	4

Figure 119 – Register index

- **Logical Operation Type:** Allows you to define the type of operation: AND or. If the "AND" option is selected, all alarm conditions must be met at the same time. If the "OR" option is selected, only the conditions defined in the parameters below must be met.

6.3.2.1 CONTRAST RULE LIST

When the button is selected, it allows you to create trigger conditions for the selected alarm. You can configure up to 6 rules.



Contrast Rule Settings

Contrast Rule List

Index: 1

Enable: ☑

Description:

Contrast Type: &

Bit Mask: 0

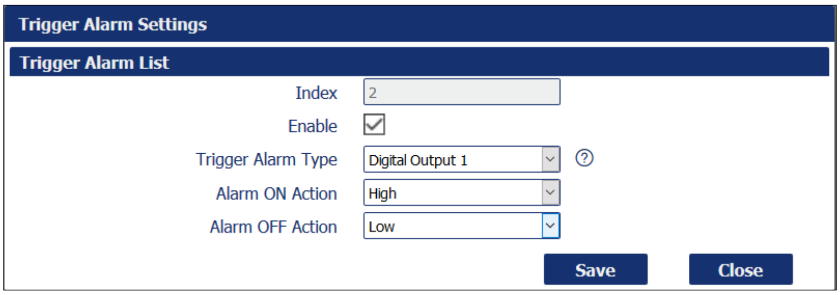
Threshold:

Figure 120 – Configuring a rule

- **Enable:** Allows you to enable the configured rule.
- **Contrast Type:** Allows you to define the type of rule to be applied:
  - **>:** Alarm greater than the configured value.
  - **<:** Alarm less than the configured value.
  - **=:** Alarm equal to the configured value.
  - **!=:** Alarm different than the configured value.
  - **>=:** Alarm greater than or equal to the configured value.
  - **<=:** Alarm less than or equal to the configured value.
  - **&=:** Alarm AND. **AirGate 4G Wi-Fi** does an AND operational logic with the value entered in the **BitMask** field. If the result equals the value in the **Threshold** field, the alarm is satisfied.
  - **|=:** Alarm OR. **AirGate 4G Wi-Fi** does an OR operational logic with the value entered in the **BitMask** field. If the result equals the value in the **Threshold** field, the alarm is satisfied.
  - **^=:** Alarm XOR. **AirGate 4G Wi-Fi** does an XCOR operational logic with the value entered in the **BitMask** field. If the result equals the value in the **Threshold** field, the alarm is satisfied.
- **BitMask:** Allows you to define a comparison value for the operational logics AND, OR, and XOR.
- **Threshold:** Allows you to configure a comparison value for the alarm.

6.3.2.2 TRIGGER ALARM LIST

This section allows you to define the actions for each selected alarm. You can configure up to 3 actions for each alarm.



Trigger Alarm Settings

Trigger Alarm List

Index: 2

Enable: ☑

Trigger Alarm Type: Digital Output 1

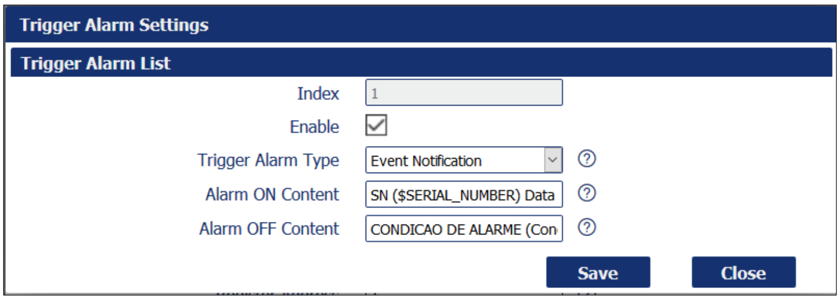
Alarm ON Action: High

Alarm OFF Action: Low

Figure 121 – Trigger list

- **Enable:** Allows you to enable the configured action.
- **Trigger Alarm Type:** Allows you to select the type of alarm trigger: "Digital Output 1", "Digital Output 2", "Event Notification" or "SMS". If "Digital Output" is selected, the action of the digital output must be configured for the alarm condition on and off.
- **Alarm ON Action:** Allows you to select an action for alarm activation: "High", "Low" or "Pulse".
- **Alarm OFF Action:** Allows you to select an alarm disable action: "High", "Low" or "Pulse".

If the "Event Notification" option of the **Trigger Alarm Type** parameter is selected, SMS, email and SNMP trap alarm can be assigned.



Trigger Alarm Settings

Trigger Alarm List

Index: 1

Enable: ☑

Trigger Alarm Type: Event Notification

Alarm ON Content: SN ($SERIAL_NUMBER) Data

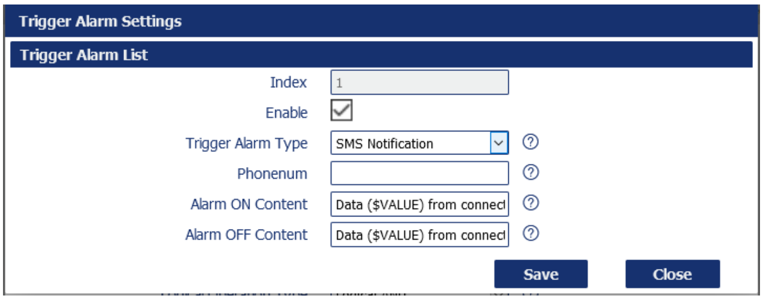
Alarm OFF Content: CONDICAO DE ALARME (Con

Figure 122 – Configuring a trigger

Each of these events must be configured in its own tab, selecting as Modbus Alarm. In this section, you can define the information for each alarm message. The options are:

- **$SERIAL_NUMBER:** Device serial number.
- **$DATE:** Date and time according to the time configured in the system (AirGate).
- **$VALUE:** Value of the channel that caused the alarm.
- **$CONNECTION_INDEX:** Index number of the connection where the alarm occurred.
- **$CONNECTION_DESC:** String configured in the **Description** parameter of the connection in alarm.
- **$CHANNEL_INDEX:** Index number of the channel in which the alarm occurred.
- **$CHANNEL_DESC:** String configured in the **Description** parameter of the channel where the alarm occurred.
- **$SLAVE_ID:** Number of the slave that caused the alarm.
- **$REGISTER_ADDER:** Number of the register that caused the alarm.
- **$FUNC_CODE:** Function as configured in the channel in alarm. Example: "func_code 3" represents the "03-Holding-register" setting.
- **$ALARM_INDEX:** Number of the activated alarm index.
- **$ALARM_DESC:** Description of the activated alarm.
- **$CONDITION:** Condition of the activated alarm.

The alarm notification text can be configured by the user and, if desired, have all the above items. If you select the "SMS" option of the Trigger Alarm Type parameter, you can assign SMS alarms to phone groups.



Trigger Alarm Settings

Trigger Alarm List

Index: 1

Enable: ☑

Trigger Alarm Type: SMS Notification

Phonenum:

Alarm ON Content: Data ($VALUE) from connect

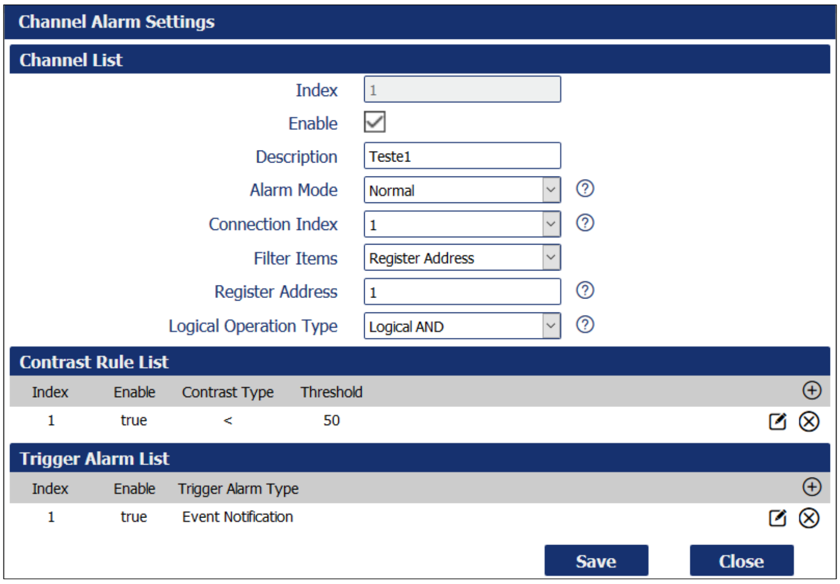
Alarm OFF Content: Data ($VALUE) from connect

Figure 123 – Trigger type

- **Enable:** Allows you to enable or disable the alarm.
- **Phonenum**: Allows you to add multiple phone numbers, which must be separated by commas.
- **Alarm ON Content:** Allows you to set the message information for when the alarm is triggered.

- **Alarm OFF Content:** Allows you to set the message information for when the alarm is deactivated.

The example below shows the configuration of an alarm:



Channel Alarm Settings

Channel List

Index	1
Enable	☑
Description	Teste1
Alarm Mode	Normal
Connection Index	1
Filter Items	Register Address
Register Address	1
Logical Operation Type	Logical AND

Contrast Rule List

Index	Enable	Contrast Type	Threshold
1	true	<	50

Trigger Alarm List

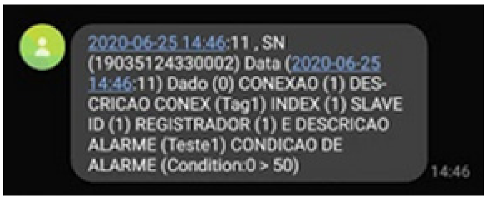
Index	Enable	Trigger Alarm Type
1	true	Event Notification

Figure 124 – Alarm example

In this example, you should follow these steps:

1. Set up an alarm to monitor the register number 1 of connection 1.
2. Create a rule to trigger the alarm if the value read on the recorder is less than 50.
3. In the **Trigger Alarm Type** parameter, select the option "Event notification".
4. In the **Alarm ON Content** parameter, enter the following string: SN ($SERIAL_NUMBER) Date ($DATE) Data ($VALUE) CONNECT ($CONNECTION_INDEX) DESCRIPTION CONNECT ($CONNECTION_DESC) INDEX ($CHANNEL_INDEX) SLAVE ID ($SLAVE_ID) REGISTER ($REGISTER_ADDER) AND ALARM DESCRIPTION ($ALARM_DESC) ALARM CONDITION: $CONDITION)

This will allow all the information about this alarm to be sent. In this example, an SMS notification was used:



2020-06-25 14:46:11 , SN (19035124330002) Data (2020-06-25 14:46:11) Dado (0) CONEXAO (1) DESCRICAO CONEX (Tag1) INDEX (1) SLAVE ID (1) REGISTRADOR (1) E DESCRICAO ALARME (Teste1) CONDICAO DE ALARME (Condition:0 > 50)

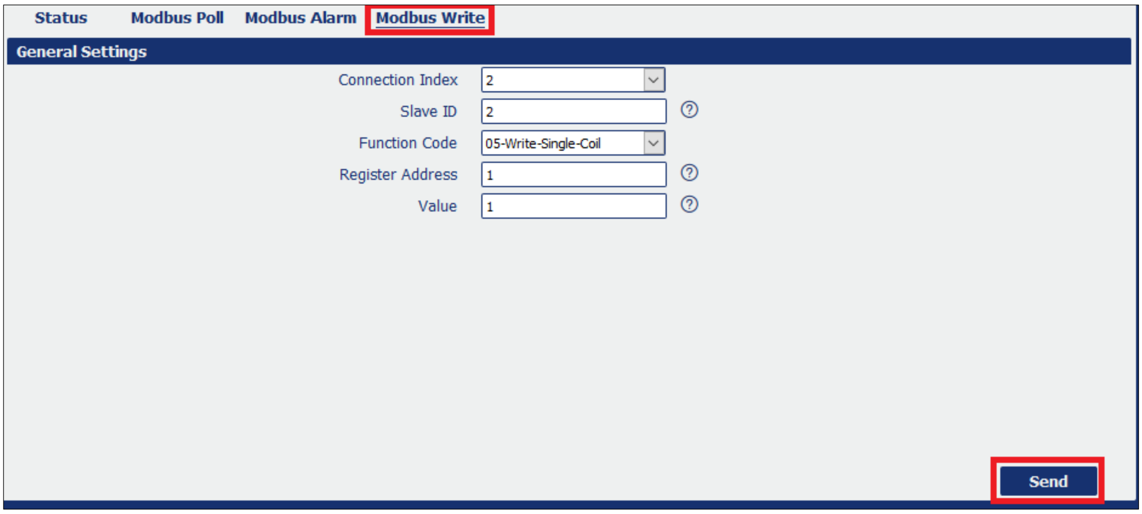
14:46

Figure 125 – SMS example

To send an SMS, you must select the "Modbus Alarm" notification in the SMS application.

6.3.3 MODBUS WRITE

Modbus Alarm allows you to write to registers. You can write to a single register at a time.



Connection Index: 2

Slave ID: 2

Function Code: 05-Write-Single-Coil

Register Address: 1

Value: 1

Figure 126 – Modbus Write

- **Connection Index:** Allows you to define the index of the connection where you want to write. You can configure up to 3 different connections.
- **Slave ID:** Allows you to define the address of the slave to write to. Range: 1~255.
- **Function Code:** Allows you to define the write command: 05-Write-Single-Coil or 06-Write-Single-Register.
- **Register Address:** Allows you to define the address of the register to write to.
- **Value:** Allows you to define the value to be written in the register.

Once the settings are made, you must click the **Send** button.

6.4 "MODBUS TRANSPORT" APPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, **AirGate 4G Wi-Fi** can be configured to send data read by Modbus and will allow it to be transported via three protocols: TCP-Client, MQTT and FTP.

Thus, after the registers reading has been configured through the Modbus Master application (see section "MODBUS MASTER" APPLICATION), it will be necessary to configure the protocol responsible for transporting this information. To do this, access the **AirGate 4G Wi-Fi** web interface, locate the **Applications** option on the left menu, and then click **Modbus Transport**, as shown below:

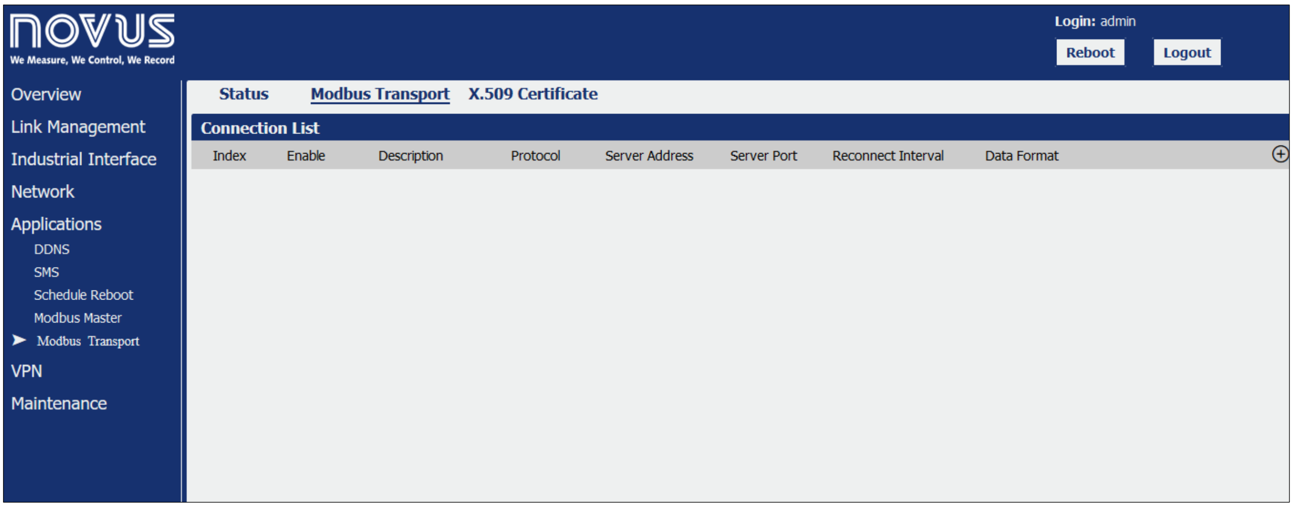
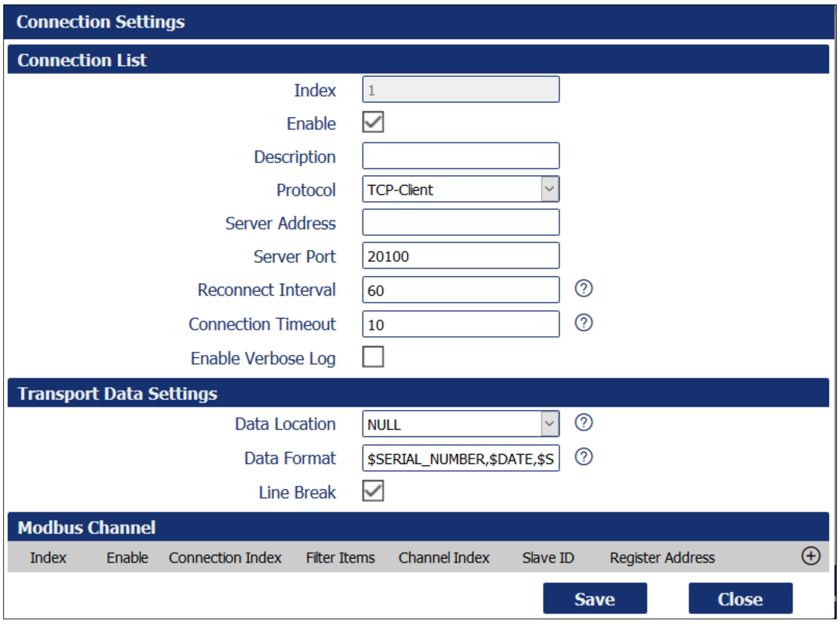


Figure 127 – Modbus Transport

Once you have done this, click on the ⊕ button to open the configuration screen and select the protocol you want to use in the **Protocol** parameter:



Connection Settings

Connection List

Index: 1

Enable: ☑

Description:

Protocol: TCP-Client

Server Address:

Server Port: 20100

Reconnect Interval: 60

Connection Timeout: 10

Enable Verbose Log: □

Transport Data Settings

Data Location: NULL

Data Format: $SERIAL_NUMBER,$DATE,$S

Line Break: ☑

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 128 – Configuring Modbus Transport

The option to transport data using the **TCP-Client** protocol is configured by default, but the settings and functionalities of this window vary according to the protocol selected, as shown in the following sections.

6.4.1 TCP-CLIENT

The default setting was displayed in the figure above. This protocol has the following parameters:

6.4.1.1 CONNECTION SETTINGS

- **Enable:** Allows you to enable a connection. A connection already created can be configured, but not enabled.
- **Description:** Allows you to enter a description.
- **Protocol:** Allows you to select the protocol to be used. In this case, TCP-Client.
- **Server Address:** Allows you to define the server address to which the data will be sent.
- **Server Port:** Allows you to define the server port to which the data will be sent.
- **Reconnect Interval:** Allows you to define the reconnection time with the server. Configurable between 1 and 60s.
- **Connection Timeout:** Allows you to define the connection timeout with the server. Configurable between 1 and 30s.

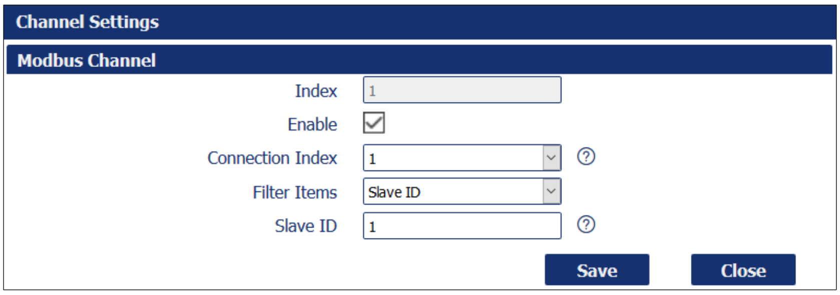
- **Enable Verbose Log:** Allows you to display a detailed log.

6.4.1.2 TRANSPORT DATA SETTINGS

- **Data Location:** Allows you to set the data location mode. This parameter acts when there is a failure in sending data (network connection failure, for example). When the connection is re-established, the data of this period will have the treatment configured as selected below:
  - **NULL:** The data will be discarded.
  - **RAM:** The data will be stored in RAM but lost after restarting the device.
  - **Flash:** The data will be stored in Flash memory and retained even after restarting the device.
- **Data Format:** Allows you to set the data display mode. Like the Modbus alarm configuration (see MODBUS ALARM section of this chapter), the device allows you to decide which information to transmit:
  - **$SERIAL_NUMBER:** Device serial number.
  - **$DATE:** Date and time according to the time configured in the system (AirGate).
  - **$VALUE:** Value of the channel that caused the alarm.
  - **$CONNECTION_INDEX:** Index number of the connection where the alarm occurred.
  - **$CONNECTION_DESC:** String configured in the **Description** parameter of the connection in alarm.
  - **$CHANNEL_INDEX:** Index number of the channel in which the alarm occurred.
  - **$CHANNEL_DESC:** String configured in the **Description** parameter of the channel where the alarm occurred.
  - **$SLAVE_ID:** Number of the slave that caused the alarm.
  - **$REGISTER_ADDER:** Number of the register that caused the alarm.
  - **$FUNC_CODE:** Function as configured in the channel in alarm. Example: "func_code 3" represents the "03-Holding-register" setting.
  - **$TRANSPORT_INDEX:** Index number of the connection where the transport is taking place.
  - **$TRANSPORT_DESC:** String configured in the **Description** parameter of the connection where the transport is taking place.
- **Line Break:** Allows you to enable the break of lines during the sending of information.

6.4.1.3 MODBUS CHANNEL

By clicking the ⊕ button in this section, you can define Modbus Master data to be sent in the CSV file, as shown in the figure below:



Channel Settings

Modbus Channel

Index: 1

Enable: ☑

Connection Index: 1

Filter Items: Slave ID

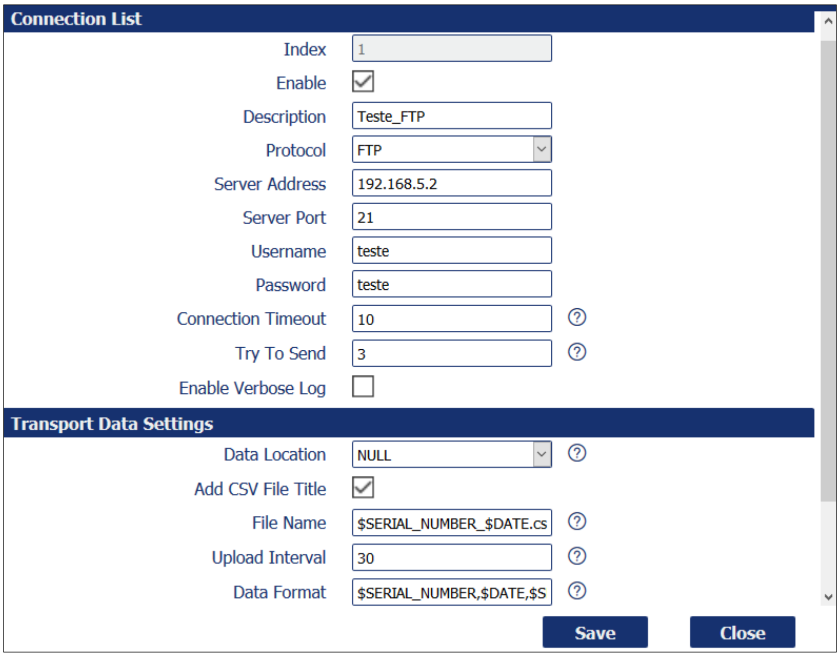
Slave ID: 1

Figure 129 – Configuring the data to be sent (1)

- **Enable:** Allows you to enable a Modbus channel to transport data.
- **Connection Index:** Allows you to define the index of the connection from which to send the data.
- **Filter Items:** Allows you to filter the type of data to be sent: "Channel Index", "Slave ID" or "Register Address".
  - **Channel Index:** When choosing this option, you must enter the channel of the Modbus connection that will send the data. If the field is left blank, the device will send all the data of this connection.
  - **Slave ID:** When choosing this option, you must enter the address of the slave that will send the data. All the registers of this slave will be transported.
  - **Register Address:** When choosing this option, you must enter the address of the register that will send the data.

6.4.2 FTP

The **FTP** transport functionality allows you to transfer the data downloaded in **Modbus Master** to a configured server. To do this, as in the case of the **TCP-Client** protocol presented in the previous section, you must click the ⊕ button on the Modbus Transport configuration screen, as shown in the figure below:



Connection List

Index	1
Enable	☑
Description	Teste_FTP
Protocol	FTP
Server Address	192.168.5.2
Server Port	21
Username	teste
Password	teste
Connection Timeout	10
Try To Send	3
Enable Verbose Log	□

Transport Data Settings

Data Location	NULL
Add CSV File Title	☑
File Name	$SERIAL_NUMBER_$DATE.cs
Upload Interval	30
Data Format	$SERIAL_NUMBER,$DATE,$S

Figure 130 – Configuring FTP protocol

6.4.2.1 CONNECTION SETTINS

- **Enable:** Allows you to enable a connection. A connection already created can be configured, but not enabled.
- **Description:** Allows you to enter a description.
- **Protocol:** Allows you to select the protocol to be used. In this case, TCP-Client.
- **Server Address:** Allows you to define the server address to which the data will be sent.
- **Server Port:** Allows you to define the server port to which the data will be sent. The default port is 21.
- **Username:** Allows you to enter the name of the configured user in the server.
- **Password:** Allows you to enter the password of the configured user in the server.
- **Connection Timeout:** Allows you to define the connection timeout with the server. Configurable between 1 and 30s.
- **Try to Send:** If the sending fails, it allows you to define the number of times the device will try to send again. Configurable between 1 and 5 attempts.
- **Enable Verbose Log:** Enables the display of a detailed log.

6.4.2.2 TRANSPORT DATA SETTINGS

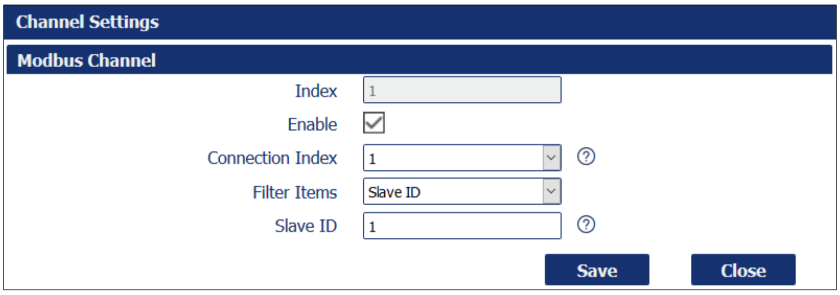
- **Data Location:** Allows you to set the data location mode. This parameter acts when there is a failure in sending data (network connection failure, for example). When the connection is re-established, the data of this period will have the treatment configured as selected below:
  - **NULL:** The data will be discarded.
  - **RAM:** The data will be stored in RAM but lost after restarting the device. Storage capacity: Up to 5000 data.
  - **Flash:** The data will be stored in Flash memory and retained even after restarting the device. Storage capacity: Up to 5000 data.

  This storage is exclusive for data transport and cannot be accessed by other interfaces. The memory is circular. Therefore, the oldest data will be overwritten when the limit is reached.
- **Add CSV file title:** Allows you to add the title of the parameters to be sent in the CSV file.
- **File Name:** Allows you to insert a name for the file. You can define a name to identify your CSV file. You can write a message and/or add information about the device. The characters supported in this parameter are: " ","-", "_", "$", ".", 0~9, a~z, A~Z. You can add the device features described below:
  - **$SERIAL_NUMBER:** Serial number of the device that is sending the data to the server.
  - **$DATE:** Date and time of sending data to the server.
  - **$TRANSPORT_INDEX:** Index number of the transport connection.
  - **$TRANSPORT_DESC:** Description of the transport connection.
- **Upload Interval:** Allows you to define the interval period with which the device uploads the CSV file to the destination server. Configurable between 1 and 86400s.
- **Data Format:** Like the Modbus alarm configuration, it allows you to decide which information will be transmitted:
  - **$SERIAL_NUMBER:** Device serial number.

- **$DATE:** Date and time according to the time configured in the system (AirGate).
- **$VALUE:** Value of the channel that caused the alarm.
- **$CONNECTION_INDEX:** Index number of the connection where the alarm occurred.
- **$CONNECTION_DESC:** String configured in the **Description** parameter of the connection in alarm.
- **$CHANNEL_INDEX:** Index number of the channel in which the alarm occurred.
- **$CHANNEL_DESC:** String configured in the **Description** parameter of the channel where the alarm occurred.
- **$SLAVE_ID:** Number of the slave that caused the alarm.
- **$REGISTER_ADDER:** Number of the register that caused the alarm.
- **$FUNC_CODE:** Function as configured in the channel in alarm. Example: "func_code 3" represents the "03-Holding-register" setting.
- **$TRANSPORT_INDEX:** Index number of the connection where the transport is taking place.
- **$TRANSPORT_DESC:** String configured in the **Description** parameter of the connection where the transport is taking place.

6.4.2.3 MODBUS CHANNEL

By clicking the ⊕ button in this section, you can define Modbus Master data to be sent in the CSV file, as shown in the figure below:



Channel Settings

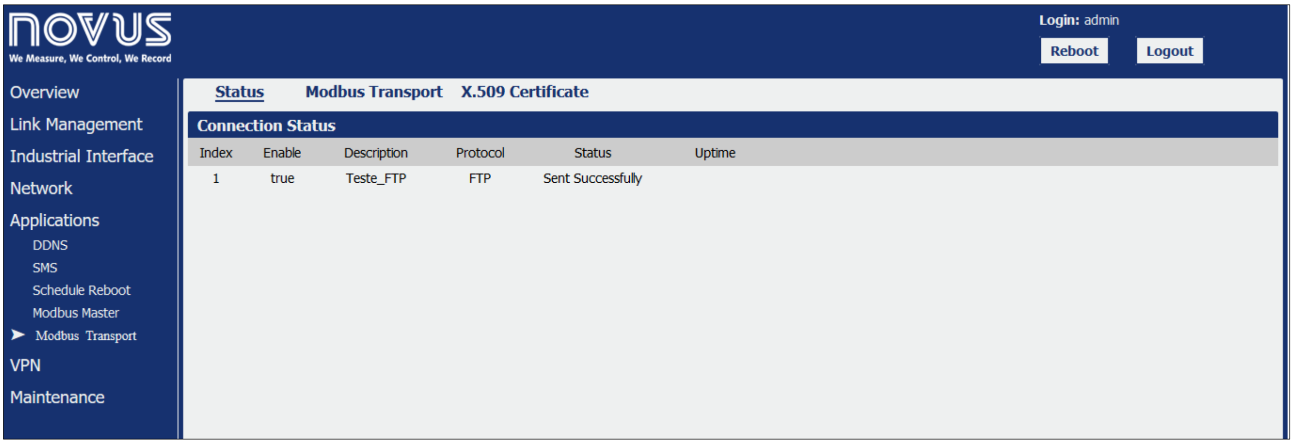
Modbus Channel

Index	1
Enable	☑
Connection Index	1
Filter Items	Slave ID
Slave ID	1

Figure 131 – Configuring the data to be sent (1)

- **Enable:** Allows you to enable a Modbus channel to transport data.
- **Connection Index:** Allows you to define the index of the connection from which to send the data.
- **Filter Items:** Allows you to filter the type of data to be sent: "Channel Index", "Slave ID" or "Register Address".
  - **Channel Index:** When choosing this option, you must enter the channel of the Modbus connection that will send the data. If the field is left blank, the device will send all the data of this connection.
  - **Slave ID:** When choosing this option, you must enter the address of the slave that will send the data. All the registers of this slave will be transported.
  - **Register Address:** When choosing this option, you must enter the address of the register that will send the data

After configuring the FTP protocol, you can check the sending status in the main menu of the **Modbus Transport** application, as shown in the figure below:



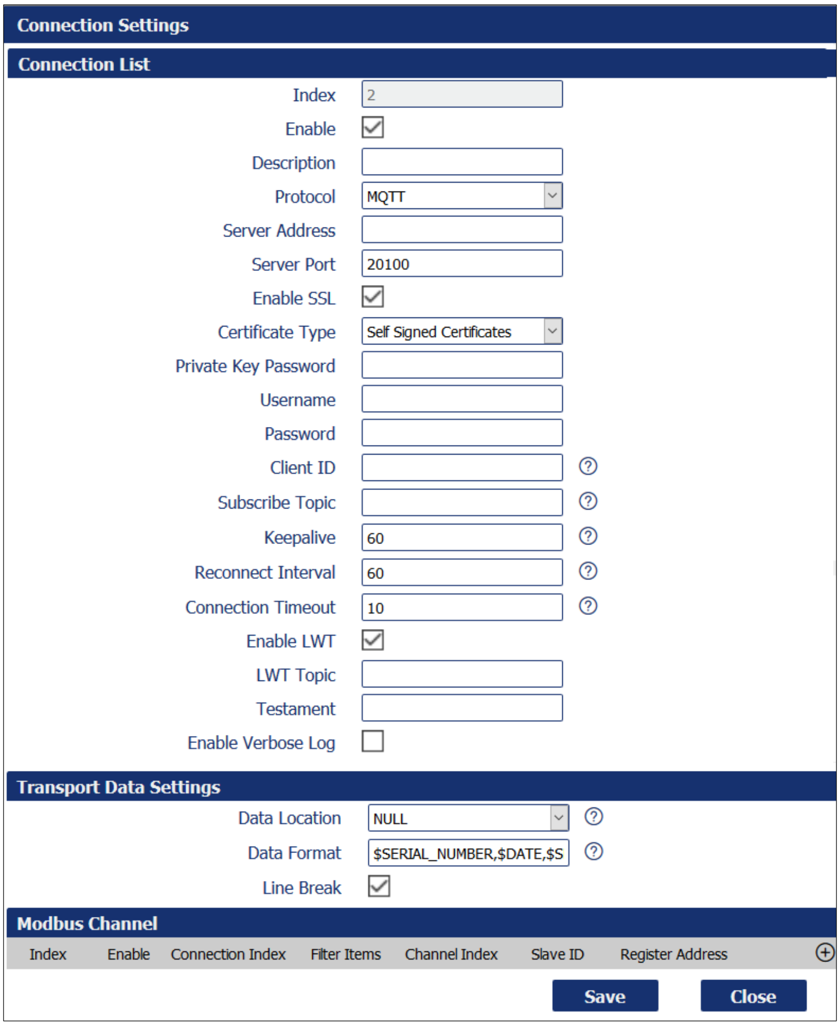
Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true	Teste_FTP	FTP	Sent Successfully	

Figure 132 – Checking the status

6.4.3 MQTT

The **MQTT** transport functionality allows you to transfer the data downloaded in **Modbus Master**. The device can connect to an internal Broker or send the data to platforms in the cloud. To do so, as in the case of **TCP-Client** and **FTP** protocols presented in the previous section, you must click the ⊕ button on the Modbus Transport configuration screen, as shown below:



Connection Settings

Connection List

Index: 2

Enable: ☑

Description:

Protocol: MQTT

Server Address:

Server Port: 20100

Enable SSL: ☑

Certificate Type: Self Signed Certificates

Private Key Password:

Username:

Password:

Client ID:

Subscribe Topic:

Keepalive: 60

Reconnect Interval: 60

Connection Timeout: 10

Enable LWT: ☑

LWT Topic:

Testament:

Enable Verbose Log: □

Transport Data Settings

Data Location: NULL

Data Format: $SERIAL_NUMBER,$DATE,$S

Line Break: ☑

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 133 – Configuring MQTT protocol

6.4.3.1 CONNECTION LIST

- **Server Address:** Allows you to enter the server address of the MQTT connection.
- **Server Port:** Allows you to enter the server port to which the data will be sent. The default port for MQTT is 1883; for MQTTS, 8883.
- **Enable SSL:** If enabled, allows you to add security certificates to the device.
  - **Certificate Type:** Allows you to select the type of security certificate to be added to the device: "Self-Signed Certificates" or "CA Certificate Only".
  - **Private Key Password:** Allows you to enter the private key of the device.
- **Username:** Allows you to enter the user of the server to which the data is being transferred.
- **Password:** Allows you to enter the password of the user of the server to which the data is being transferred.
- **Client ID:** Allows you to enter a client ID. When the parameter is left blank, **AirGate 4G Wi-Fi** will automatically fill in the serial number of the device.
- **Subscribe Topic:** Allows you to enter the device subscription topic.
- **Keepalive:** Allows you to enter the maximum time interval for the MQTT connection to remain active. Configurable between 1 and 86400s.
- **Reconnect Interval:** Allows you to enter the reconnection interval with the server. Configurable between 1 and 600s.
- **Connection Timeout:** Allows you to enter the connection timeout with the server.
- **Enable LWT:** If enabled, allows you to send a last message/warning when **AirGate 4G Wi-Fi** is unintentionally disconnected from the server.
  - **LWT Topic:** Allows you to write your last publication.
  - **Testament:** Allows you to write the message to be sent before the user is disconnected.
- **Enable Verbose Log:** Enables the display of a detailed log.

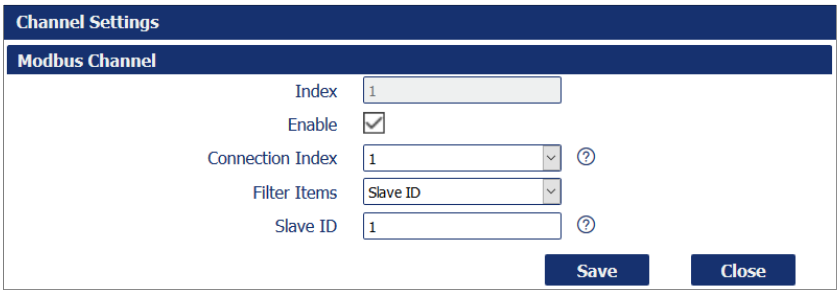
The interval for publishing information via MQTT depends on the **Scan Rate** parameter, available in the MODBUS PULL section.

6.4.3.2 TRANSPORT DATA SETTINGS

- **Data Location:** Allows you to set the data location mode. This parameter acts when there is a failure in sending data (network connection failure, for example). When the connection is re-established, the data of this period will have the treatment configured as selected below:
  - **NULL:** The data will be discarded.
  - **RAM:** The data will be stored in RAM but lost after restarting the device.
  - **Flash:** The data will be stored in Flash memory and retained even after restarting the device.
- **Data Format:** Allows you to set the data display mode. Like the Modbus alarm configuration (see MODBUS ALARM section of this chapter), the device allows you to decide which information to transmit:
  - **$SERIAL_NUMBER:** Device serial number.
  - **$DATE:** Date and time according to the time configured in the system (AirGate).
  - **$VALUE:** Value of the channel that caused the alarm.
  - **$CONNECTION_INDEX:** Index number of the connection where the alarm occurred.
  - **$CONNECTION_DESC:** String configured in the **Description** parameter of the connection in alarm.
  - **$CHANNEL_INDEX:** Index number of the channel in which the alarm occurred.
  - **$CHANNEL_DESC:** String configured in the **Description** parameter of the channel where the alarm occurred.
  - **$SLAVE_ID:** Number of the slave that caused the alarm.
  - **$REGISTER_ADDER:** Number of the register that caused the alarm.
  - **$FUNC_CODE:** Function as configured in the channel in alarm. Example: "func_code 3" represents the "03-Holding-register" setting.
  - **$TRANSPORT_INDEX:** Index number of the connection where the transport is taking place.
  - **$TRANSPORT_DESC:** String configured in the **Description** parameter of the connection where the transport is taking place.
- **Line Break:** Allows you to enable the break of lines during the sending of information.

6.4.3.3 MODBUS CHANNEL

By clicking the ⊕ button in this section, you can define Modbus Master data to be sent in the CSV file, as shown in the figure below:



Channel Settings

Modbus Channel

Index: 1

Enable: ☑

Connection Index: 1

Filter Items: Slave ID

Slave ID: 1

Figure 134 – Configuring the data to be sent (3)

- **Enable:** Allows you to enable a Modbus channel to transport data.
- **Connection Index:** Allows you to define the index of the connection from which to send the data.
- **Filter Items:** Allows you to filter the type of data to be sent: "Channel Index", "Slave ID" or "Register Address".
  - **Channel Index:** When choosing this option, you must enter the channel of the Modbus connection that will send the data. If the field is left blank, the device will send all the data of this connection.
  - **Slave ID:** When choosing this option, you must enter the address of the slave that will send the data. All the registers of this slave will be transported.
  - **Register Address:** When choosing this option, you must enter the address of the register that will send the data.

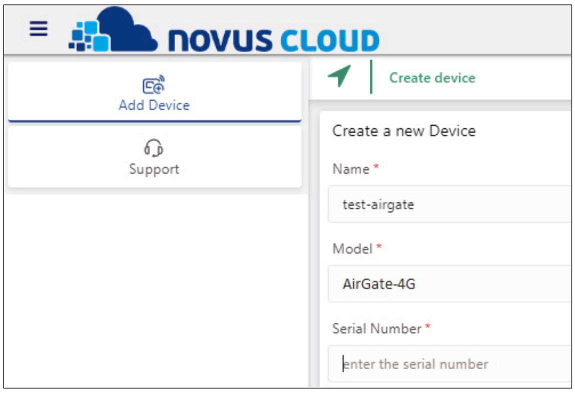
6.4.3.4 CLOUD PLAFTORM CONNECTION

AirGate 4G Wi-Fi can be configured to send data by Modbus to cloud platforms. The device must have been configured to read Modbus registers in Modbus Master mode (see section "MODBUS MASTER" APPLICATION). Once this has been done, you can connect to the following platforms:

- **NOVUS Cloud**
- AWS
- Google Cloud

NOVUS CLOUD

To establish communication between **AirGate 4G Wi-Fi** and **NOVUS Cloud**, the device must be configured on the platform. Access the **NOVUS Cloud** account to be used. At the top of the page, click on **Add Device** and enter a name for the device to be added (in this case, "AirGate-4G").



Create a new Device

Name *: test-airgate

Model *: AirGate-4G

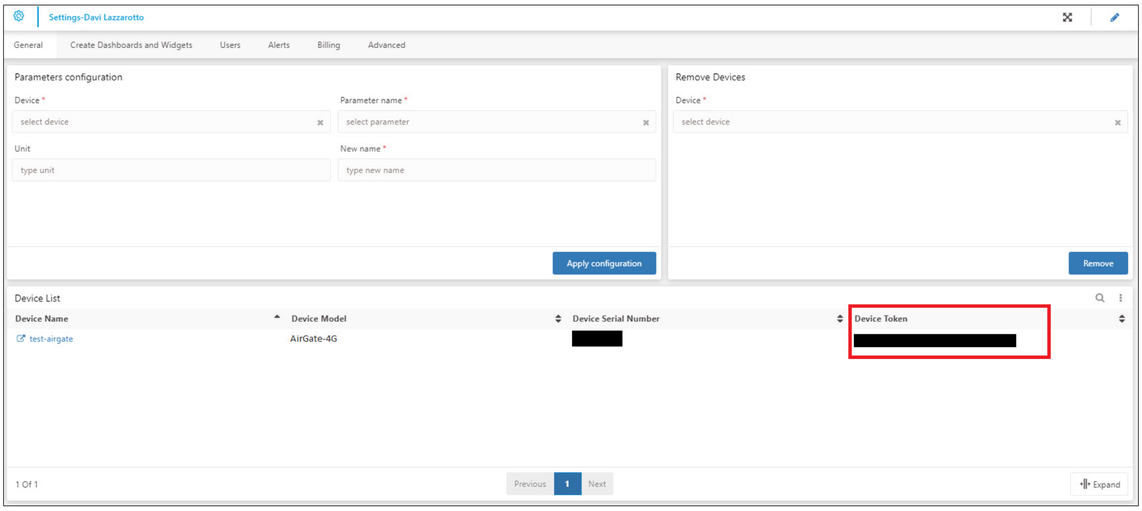
Serial Number *: enter the serial number

Figure 135 – Adding a device to the **NOVUS Cloud**

To obtain the **AirGate 4G Wi-Fi** serial number, you must access its web interface, click on **Overview,** and find the serial number in the **System Information** section. Copy and paste this serial number into the **NOVUS Cloud** interface.

By clicking on **Create Device**, the **NOVUS Cloud** will automatically add the device to the cloud platform (this process may take a few minutes). Once the device has been created in the cloud, its name will appear in the left column.

Once this has been done, you should click on **Settings**. On the screen that appears, you can see the created device in the table in the **Device List** section. To configure the **AirGate 4G Wi-Fi** connection, you must copy the Token showed there:



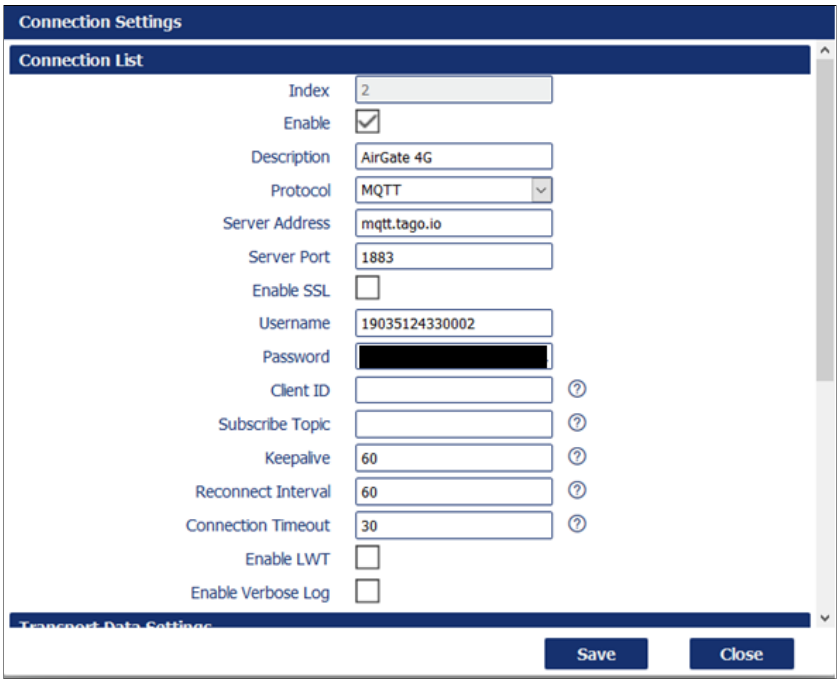
Device List

Device Name	Device Model	Device Serial Number	Device Token
test-airgate	AirGate-4G	[redacted]	[redacted]

1 Of 1

Figure 136 – Device Token

Once the device has been registered to the cloud, you can configure your connection via the **AirGate 4G Wi-Fi** web interface. Click on **Applications**, located in the menu on the left, and **Modbus Transport**. Then, at the top of the screen, select the **Modbus Transport** option and click the ⊕ button, located in the top right corner, to add a connection:



Connection Settings

Connection List

Index: 2
Enable: ☑
Description: AirGate 4G
Protocol: MQTT
Server Address: mqtt.tago.io
Server Port: 1883
Enable SSL: □
Username: 19035124330002
Password: [redacted]
Client ID:
Subscribe Topic:
Keepalive: 60
Reconnect Interval: 60
Connection Timeout: 30
Enable LWT: □
Enable Verbose Log: □

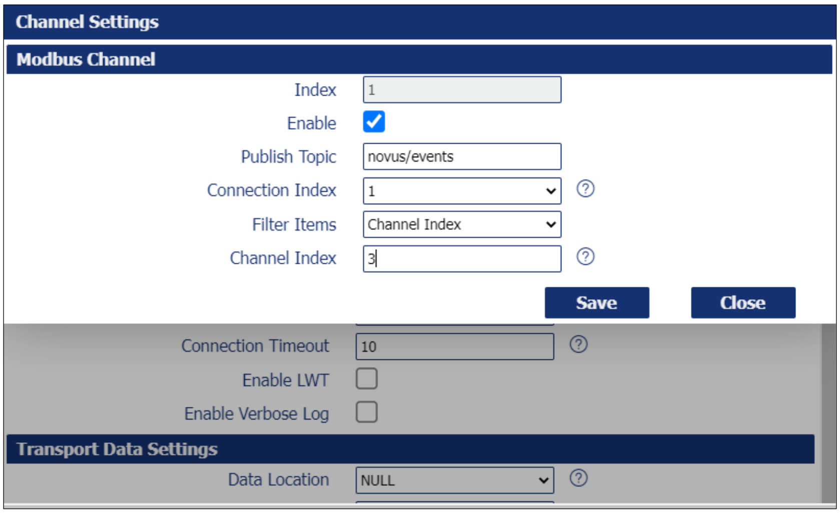
Figure 137 – Adding a new connection

In the **Username** field, you must enter the device serial number, as shown in the example above. In the **Password** field, you must enter the Token created by **NOVUS Cloud** for the device created. Then scroll down and, under **Transport Data Settings**, select the RAM option, so that when there is a connection failure, the data will be saved in a queue in the **AirGate 4G Wi-Fi** internal RAM and sent when the connection is restored.

In the **Data Format** field, write the desired format of each message sent to the cloud using the indexers. The indexer you have chosen should be in quotation marks. For the cloud platform to recognize the data sent, you must fill in the following:

[{ "variable" : "$CHANNEL_DESC", "value" : $VALUE }]

Finally, you must add the Modbus registers whose values you want to send to the **NOVUS Cloud**. To do this, below **Modbus Channel**, you must click on the ⊕ button, located on the right. In the menu that opens, fill in the MQTT publishing topic with "NOVUS/events". Under **Connection Index**, select the connection referring to the Modbus slave that contains the desired registers. To send data from a specific register, select the option **Register Address** under **Filter Items** and enter the register address:



Channel Settings

Modbus Channel

Index: 1
Enable: ☑
Publish Topic: novus/events
Connection Index: 1
Filter Items: Channel Index
Channel Index: 3

Connection Timeout: 10
Enable LWT: □
Enable Verbose Log: □

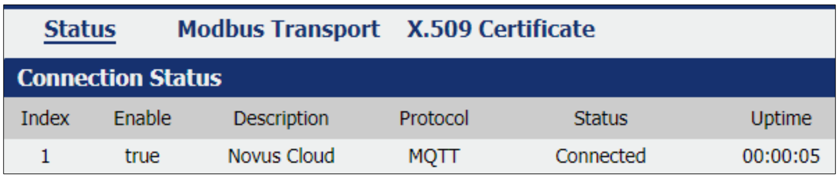
Transport Data Settings

Data Location: NULL

Figure 138 – Configuring a channel

Under **Filter Items**, you can configure other criteria to define how the Modbus registers to be sent are selected. In addition, other registers can be added to the send list by clicking on the ⊕ button located below **Modbus Channel** and filling in the send parameters again. When all desired Modbus registers are selected, click **Save** and then **Apply**.

To check if the connection has been successfully established, click on **Status**, located at the top of the screen. When **AirGate 4G Wi-Fi** establishes the connection to the **NOVUS Cloud**, the **Status** column of this connection shows the message "Connected". If the **Status** column shows the message "Connecting", you can click on **Status** to update the status of the table.



Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true	Novus Cloud	MQTT	Connected	00:00:05

Figure 139 – **NOVUS Cloud** status connection

Once the **AirGate 4G Wi-Fi** is connected to the **NOVUS Cloud**, you can view the values of Modbus registers read directly from the **NOVUS Cloud**. To do so, you must click on the registered device name in the left column. On the interface that opens, you can create widgets to show the values sent by **AirGate 4G Wi-Fi** by selecting a widget to insert in the dashboard.

Then, in the configuration menu, select as "Device" the device created in the cloud platform and as "Variable" the Modbus channel name given when setting up **AirGate 4G Wi-Fi** as Modbus master. After clicking **Save**, the values for this Modbus channel should appear in the widget.

You can insert several Modbus channels into the same widget, as shown in the picture below:

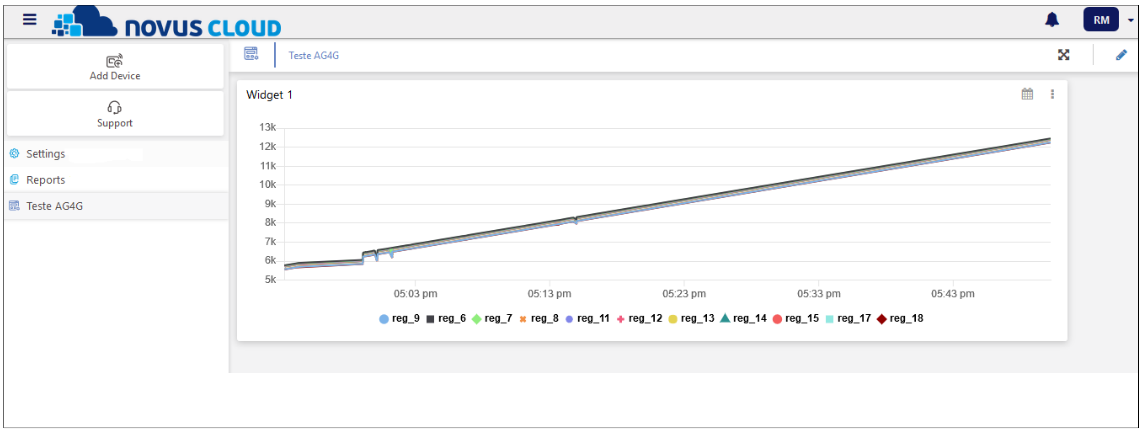


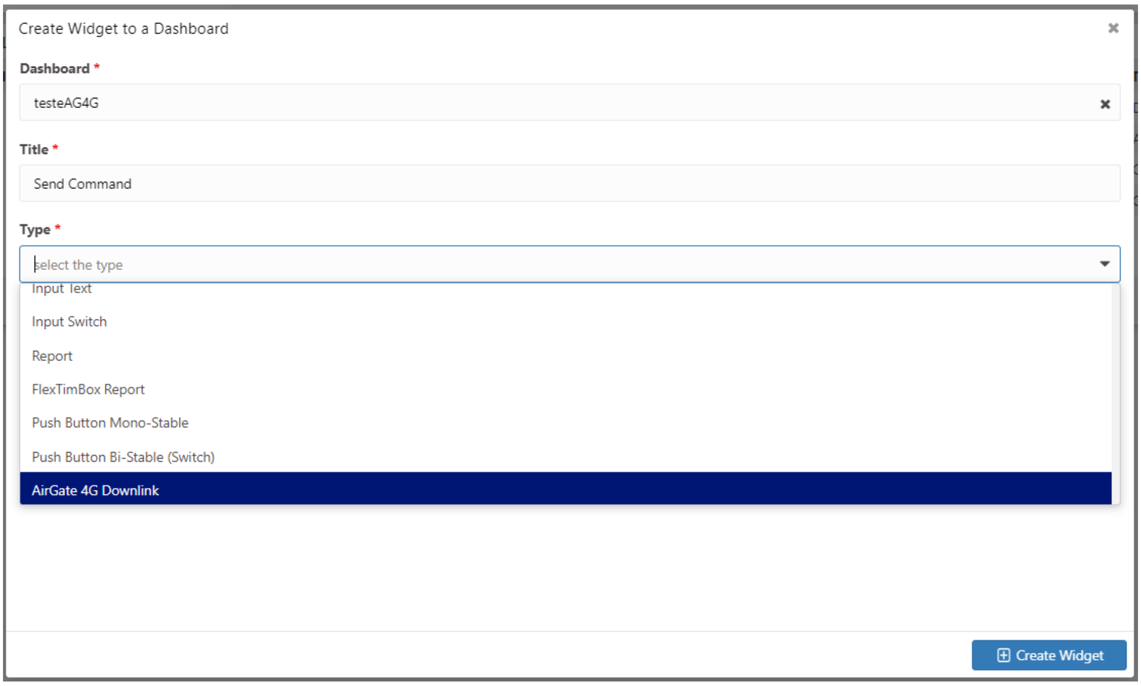
Figure 140 – Widget example

Summarizing the steps of this configuration:

- In the **NOVUS Cloud** account, add the device from the serial number.
- In the **AirGate 4G Wi-Fi** web interface, under **Modbus Transport**, configure the MQTT connection between **AirGate 4G Wi-Fi** and **NOVUS Cloud** by using the Token generated by **NOVUS Cloud**.
- Next, format the message, add the Modbus registers to be sent and configure the MQTT publishing topic.
- Check the connection status to the **NOVUS Cloud**.
- In the **NOVUS Cloud** account, add widgets to the device dashboard and perform its configuration to allow viewing the data of the desired channels.

WIDGET FOR WRITING TO MODBUS DEVICES (GATEWAY MODE)

It is possible to send Modbus write commands to slaves connected to **AirGate 4G Wi-Fi**. To do this, simply add the "AirGate 4G Downlink" widget to the custom dashboard, as shown in the figure below:



Create Widget to a Dashboard

Dashboard * testeAG4G

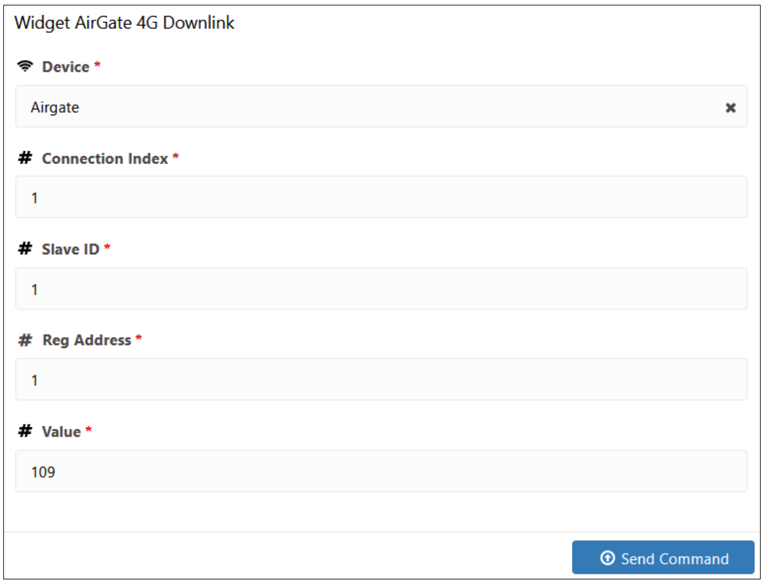
Title * Send Command

Type * select the type

Figure 141 – Widget downlink

The Widget should appear on the dashboard where it was included. To send commands to the devices, enter the address of the device in question and the value to be sent. The value sent must always be entered as an integer.

The value to be sent in the Widget will depend on the interpretation of the slave device that will receive the information. If the user wants to write the value 10.9 in the Setpoint register of a slave device and the configuration of this register has a decimal place, for example, the value 109 must be entered in the Widget's **Value** field and then click on the **Send Command** button so that the correct value can be written, as shown in the figure below:



Widget AirGate 4G Downlink

Device *

Airgate

Connection Index *

1

Slave ID *

1

Reg Address *

1

Value *

109

Figure 142 – Widget downlink

The parameters **Connection Index**, **Slave ID**, and **Register Address** are taken from the **AirGate 4G Wi-Fi** configuration itself and can be seen on the **Status** page of the Modbus Poll application.

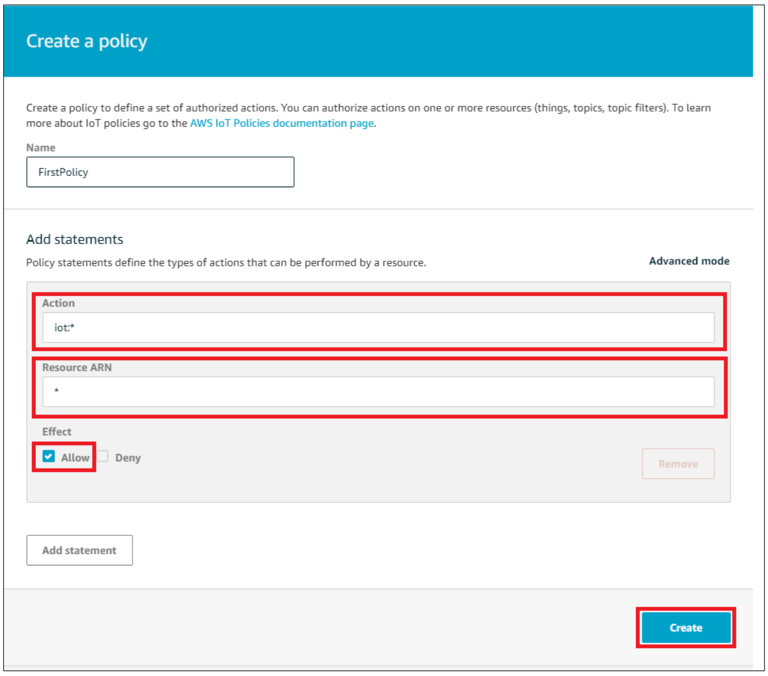
AWS

Just like configuring a device in the **NOVUS Cloud**, the first step is to create the device on the cloud platform. You must access the AWS account and select the IoT Core service. First you need to create a policy that defines the permissions that **AirGate 4G Wi-Fi** will have on the AWS account to be used.

In this example you will create a policy that allows the **AirGate 4G Wi-Fi** to access all features of the AWS IoT Core service. Since the same policy can be used for multiple things in the AWS account, the policy creation step only needs to be executed once if multiple devices are to be registered in the AWS account.

To do this, you need to click on **Protect** and then on **Policies**. Then click on **Create**, located in the top right corner, and then enter a name for the policy. To configure the permissions for this policy, you must fill in the following settings:

- **Action**: iot:*
- **Resource ARN**: *
- **Effect**: Allow



Create a policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the AWS IoT Policies documentation page.

Name

FirstPolicy

Add statements

Policy statements define the types of actions that can be performed by a resource.

Action

iot:*

Resource ARN

*

Effect

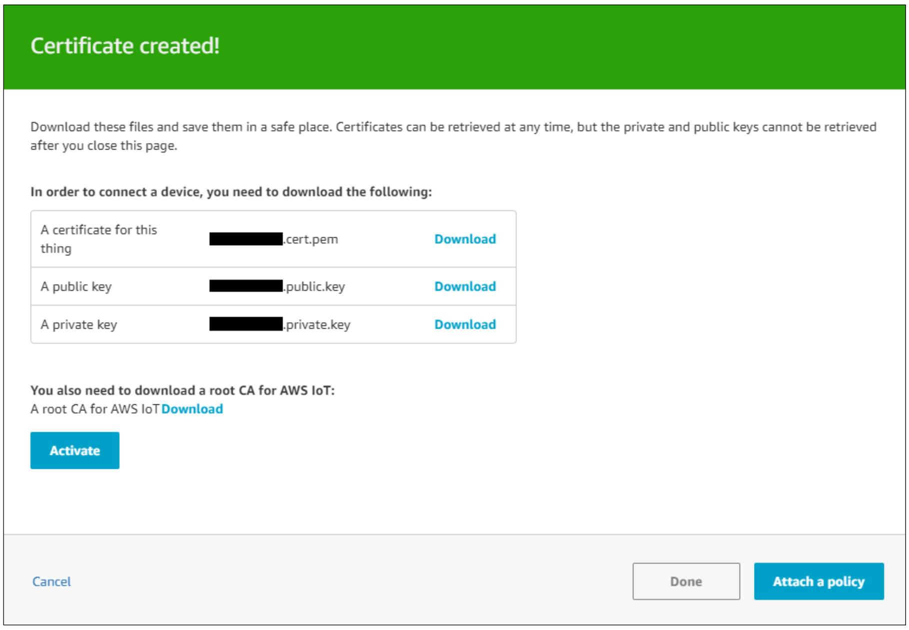
☑ Allow □ Deny

Figure 143 – Creating a policy

The next step is to create something in the AWS account that the **AirGate 4G Wi-Fi** will connect to. To do this, in the menu on the left, you must click on **Manage** and then on **Things**. In the top right corner, click on **Create** and then on **Create a single thing**, assign a name to your thing and, if desired, define a type, a group, and the attributes of that thing. Then click on **Next**.

To create a certificate for that thing, click on **Create certificate**. Alternatively, you can use an existing certificate for authentication on the AWS platform by clicking on **Create a thing** without a certificate and then add the certificate. However, this document assumes you have chosen the first option.

After creating the certificate, you should download the certificate, the public key, and the private key of that thing. It is also necessary to download the AWS root CA unless this is not the first AWS thing being created and the CA has been downloaded previously. To do this simply click on the **Download** link below "You also need to download a root CA for AWS IoT".



Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

A certificate for this thing	[redacted].cert.pem	Download
A public key	[redacted].public.key	Download
A private key	[redacted].private.key	Download

You also need to download a root CA for AWS IoT:
A root CA for AWS IoT Download

Figure 144 – Certificate created

As shown in the figure above, you can download different "Amazon Root CA". Clicking on **Download** the desired certificate will open a new tab, which will display the certificate in text format. You must save this text in a text file and, returning to the previous tab, where the certificate was created, click on **Attach a policy**. On the screen that opens, select the policy that was previously created and finally click on **Register the thing**.

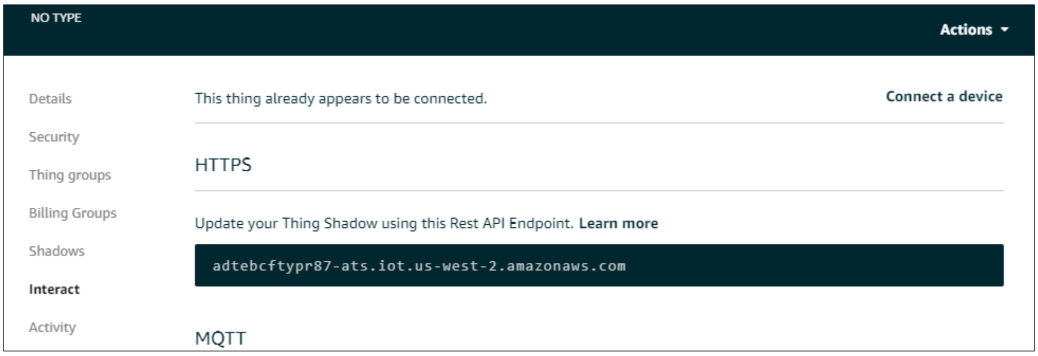
You can create certificates and attach policies to a thing after it has been created. To do so, simply click on **Manage** and on **Things**, located on the menu on the left of the screen. Then click on the checkbox for the created thing and, on the left menu, click on **Security**.

To create a certificate, simply click on **Create Certificate** and then download the certificate and the public and private keys.

To attach the policy to the **Security** menu, simply click on the certificate to be used. Then click on **Actions**, in the upper right corner, and then on **Attach Policy**. Finally, select the desired policy and click on **Attach**.

The last step on the AWS platform is to activate the certificate. In the **Security** menu of the thing created, click on the certificate created and then on **Actions** and **Activate**.

Once the thing is registered in the AWS account and with a certificate and a policy attached, you can configure **AirGate 4G Wi-Fi** to communicate with the cloud. To do so, open the **AirGate 4G Wi-Fi** web interface. Then click on **Applications** and **Modbus Transport**. At the top of the screen, click **Modbus Transport** and then add a connection by clicking the ⊕ button. Then add a description for the connection, indicate the server port as 8883 and select the Enable SSL option. Select the MQTT protocol and leave the certificate type as **Self Signed Certificates**. To get the server address, just access the AWS account and, in the IoT Core service, click on **Manage** and then on **Things**, selecting the thing created during this example. Then click on **Interact** and copy the address shown below "HTTPS", as shown in the figure below:



This thing already appears to be connected.

HTTPS

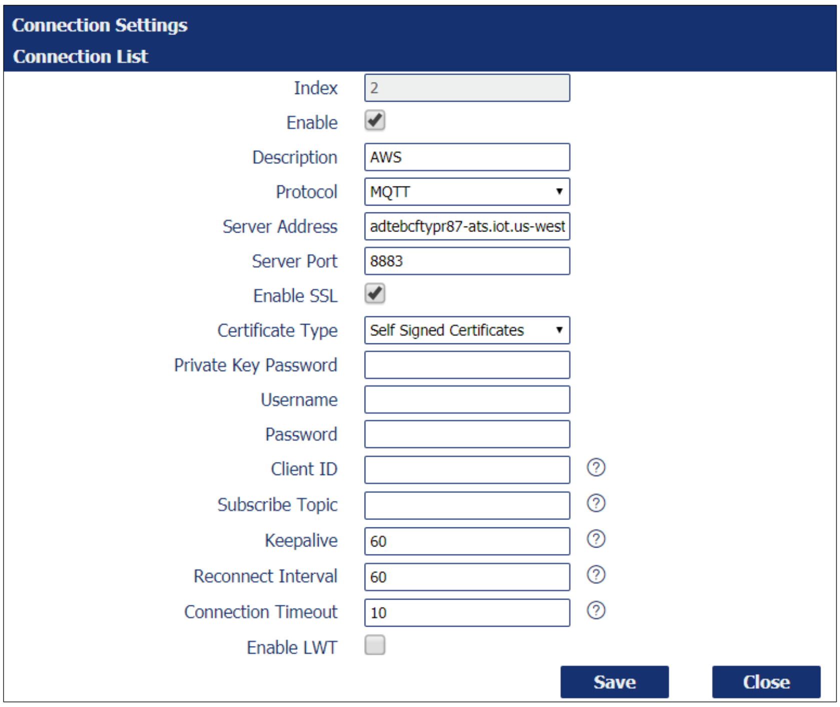
Update your Thing Shadow using this Rest API Endpoint. Learn more

```
adtebcftypr87-ats.iot.us-west-2.amazonaws.com
```

MQTT

Figure 145 – Connection server address

In the **AirGate 4G Wi-Fi** web interface, you must paste this address into the **Server Address** parameter of the connection, as shown in the figure below:



Connection Settings

Connection List

Index	2
Enable	☑
Description	AWS
Protocol	MQTT
Server Address	adtebcftypr87-ats.iot.us-west
Server Port	8883
Enable SSL	☑
Certificate Type	Self Signed Certificates
Private Key Password	
Username	
Password	
Client ID	
Subscribe Topic	
Keepalive	60
Reconnect Interval	60
Connection Timeout	10
Enable LWT	□

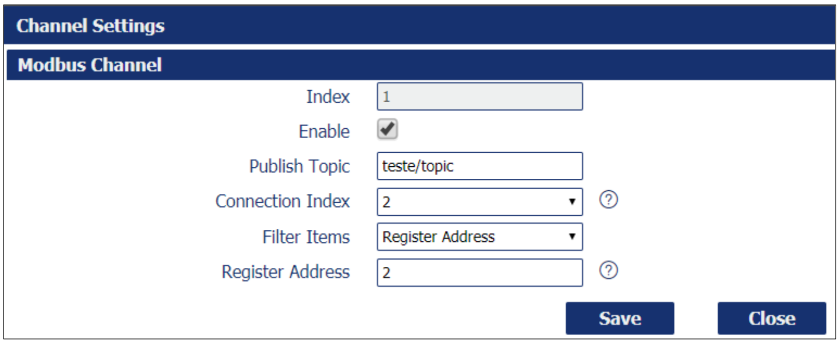
Figure 146 – Entering the server connection

Then scroll down and under **Transport Data Settings**, under **Data Location**, select the RAM option so that when there is a connection failure, the data is saved in a queue in the **AirGate 4G Wi-Fi** internal RAM and sent when the connection is restored.

In the **Data Format** field, with the help of the indexers, write the desired format of each message sent to the cloud. In this example, the following format will be used:

Valor : $VALUE

Finally, you must add the Modbus registers whose values you wish to send to the AWS platform. To do this, in the **Modbus Channel** section, you must click the ⊕ button. In the menu that opens, fill in the MQTT topic that you want to publish and, in **Connection Index**, select the connection referring to the Modbus slave that contains the desired registers. To send data from a specific register, select the option "Register Address" under **Filter Items** and enter the register address:



Channel Settings

Modbus Channel

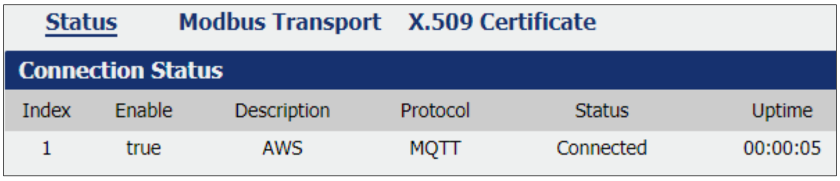
Index	1
Enable	☑
Publish Topic	teste/topic
Connection Index	2
Filter Items	Register Address
Register Address	2

Figure 147 – Modbus channel settings

If desired, you can set other criteria to determine how to select the Modbus registers to be sent in **Filter Items**. In addition, other registers can be added to the send list by clicking on the ⊕ button in the **Modbus Channel** section and filling in the send parameters again. When all the desired Modbus registers are selected, click **Save**.

Finally, it is necessary to add the certificates created on the AWS platform regarding that thing. To do this, click on **X.509 Certificate** at the top of the screen and select the connection index for the MQTT connection that was created. Then upload the CA certificate, the certificate, and the device private key by clicking on **Choose File** and select the corresponding files downloaded during the creation of the certificate of the thing on the AWS platform. You must repeat the process for each of the three files. Once the files are uploaded on **AirGate 4G Wi-Fi**, click **Apply**.

To check if the connection has been successfully established, click on **Status**, located at the top of the screen. When **AirGate 4G Wi-Fi** establishes the connection to the **NOVUS Cloud**, the **Status** column of this connection shows the message "Connected". If the **Status** column shows the message "Connecting", you can click on **Status** to update the status of the table.



Connection Status

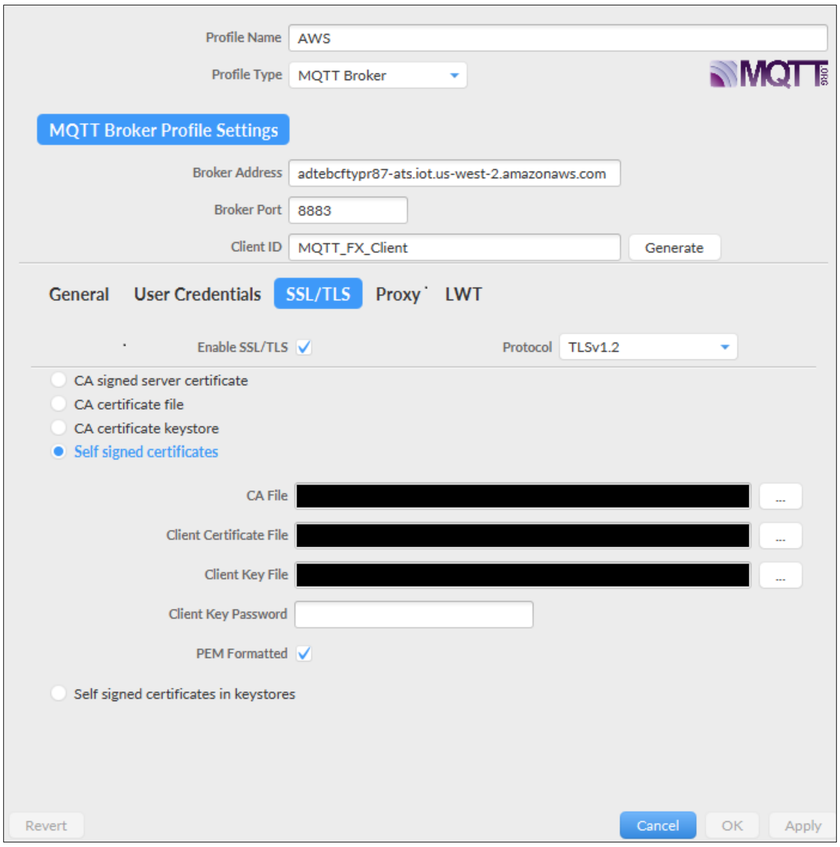
Index	Enable	Description	Protocol	Status	Uptime
1	true	AWS	MQTT	Connected	00:00:05

Figure 148 – AWS connection status

Once **AirGate 4G Wi-Fi** is connected to the cloud, you can verify that the data for the selected recorders is being correctly sent when using an MQTT client to subscribe to the topic the device is publishing. In this example, MQTT.fx v.1.7.1 software will be used as MQTT client.

To configure MQTT.fx connection to AWS, click on the gear next to **Connect**, located in the top left corner of the screen. On the screen that opens, fill in a name for the profile and choose the option "MQTT Broker" in the parameter **Profile Type**. In the **MQTT Broker Profile Settings** section, place the same broker address used for **AirGate 4G Wi-Fi MQTT** connection configuration, previously filled in the **Server Address** field of the device web interface. Enter 8883 for the broker port number and leave the value automatically filled in by MQTT.fx for the "Client ID".

Then, enter the "SSL/TLS" menu, select the **Enable SSL/TLS** option, select the **Self Signed Certificates** option, and find the same CA, certificate, and client private key files used in **AirGate 4G Wi-Fi**. Next, select the **PEM Formatted** option and click **OK**.



Profile Name: AWS

Profile Type: MQTT Broker

MQTT Broker Profile Settings

Broker Address: adtebcftypr87-ats.iot.us-west-2.amazonaws.com

Broker Port: 8883

Client ID: MQTT_FX_Client

Enable SSL/TLS ✓

Protocol: TLSv1.2

○ CA signed server certificate

○ CA certificate file

○ CA certificate keystore

● Self signed certificates

CA File: [redacted]

Client Certificate File: [redacted]

Client Key File: [redacted]

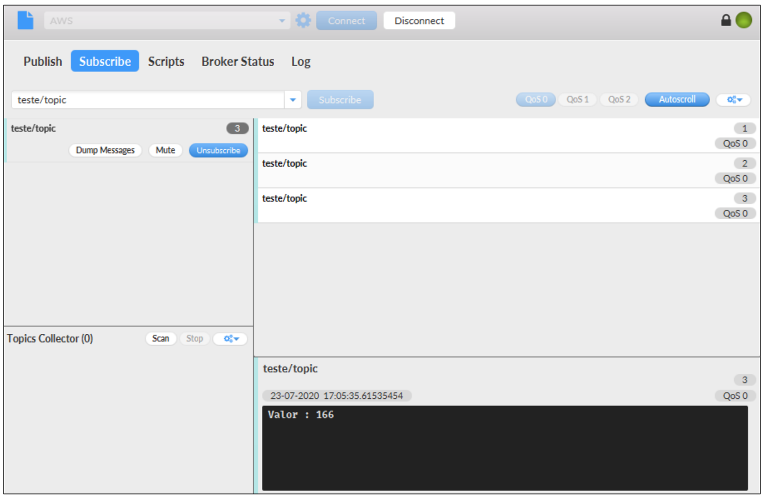
Client Key Password:

PEM Formatted ✓

○ Self signed certificates in keystores

Figure 149 – Configuring MQTT.fx

Then click **Connect** and wait for MQTT.fx to establish a connection with AWS. When this happens, the software will display a lock with a green circle on the right of the screen. To observe the data stream, you must subscribe to the topic that **AirGate 4G Wi-Fi** is publishing. To do so, enter the **Subscribe** menu and enter the topic that **AirGate 4G Wi-Fi** is publishing. By clicking the **Subscribe** button, all messages published by **AirGate 4G Wi-Fi** should appear on the screen, following the formatting you set during configuration.



teste/topic 3

teste/topic 1 QoS 0

teste/topic 2 QoS 0

teste/topic 3 QoS 0

teste/topic 3

23-07-2020 17:05:35.61535454 QoS 0

```
Valor : 166
```

Figure 150 – Device topic

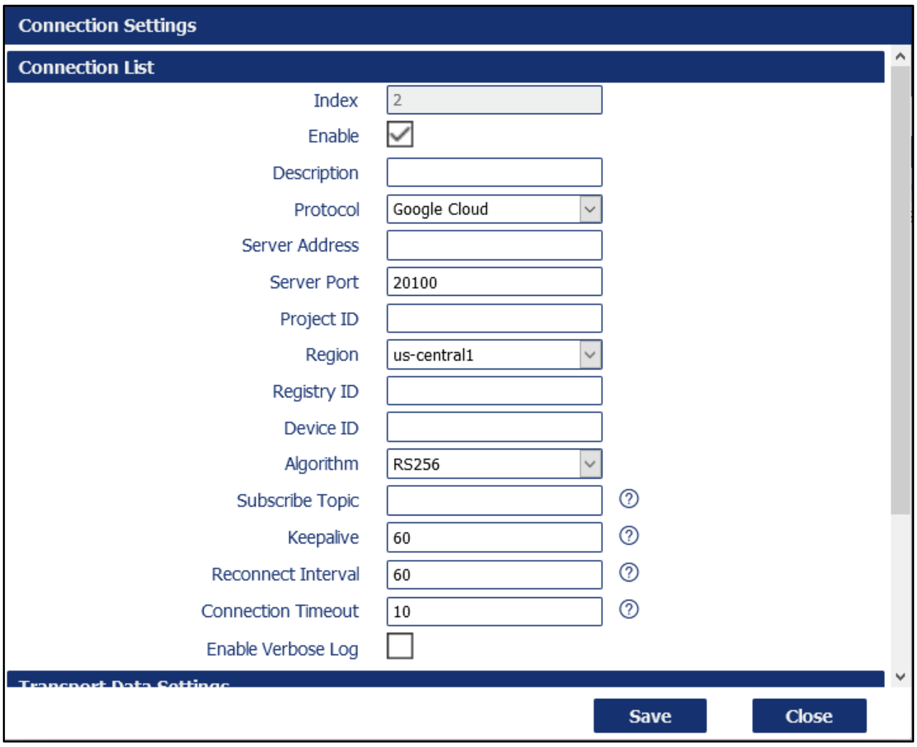
At this point you can make sure that the **AirGate 4G Wi-Fi** is sending data to the AWS account and process it in any way you wish.

Summarizing the steps of this configuration:

- On the AWS account, create a policy to allow access to the IoT Core service.
- Create something with a certificate.
- Attach the policy to the certificate.
- Activate the certificate.
- On the **AirGate 4G Wi-Fi** web interface, in Modbus Transport, configure the MQTT connection between **AirGate 4G Wi-Fi** and AWS.
- Format the message, add the Modbus registers to be sent, and configure the MQTT posting topic.
- Upload the AWS generated certificate files on **AirGate 4G Wi-Fi**.
- Check the AWS connection status.
- In MQTT.fx software, configure the connection to AWS using the same parameters and certificate files as **AirGate 4G Wi-Fi**.
- Finally, subscribe to MQTT and view messages sent by **AirGate 4G Wi-Fi** to AWS.

6.4.4 GOOGLE CLOUD

If you connect the device to **Google Cloud**, you can transfer the data downloaded in the **Modbus Master** to it. To do so, as in the case of **TCP-Client**, **FTP** and **MQTT** protocols, presented earlier, you must click the button on the **Modbus Transport** configuration screen, as shown in the figure below:



Index	2
Enable	☑
Description	
Protocol	Google Cloud
Server Address	
Server Port	20100
Project ID	
Region	us-central1
Registry ID	
Device ID	
Algorithm	RS256
Subscribe Topic	
Keepalive	60
Reconnect Interval	60
Connection Timeout	10
Enable Verbose Log	□

Figure 151 – Configuring Google Cloud

6.4.4.1 CONNECTION SETTINS

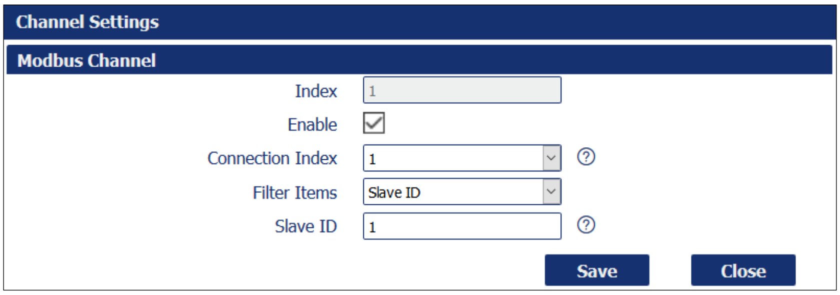
- **Server Address:** Allows you to enter the connection server address.
- **Server Port:** Allows you to enter the port of the server to which the data will be sent. Default port: 20100.
- **Project ID:** Allows you to enter the project ID. This parameter must be the same as the one configured in the **Google Cloud**.
- **Region:** Allows you to select which region is closest to where the device is installed. This parameter must be the same as the one configured in Google Cloud.
- **Register ID:** Allows you to insert a register ID. This parameter must be the same as the one configured in the **Google Cloud**.
- **Device ID:** Allows you to insert a device ID. This parameter must be the same as the one configured in the **Google Cloud**.
- **Algorithm:** Allows you to select the signature algorithm of the device. This parameter must be the same as the one configured in the **Google Cloud**.
- **Subscribe Topic:** Allows you to enter the subscription topic of the device.
- **Keepalive:** Allows you to enter the maximum time interval for the connection to remain active. Configurable between 1 and 86400s.
- **Reconnect Interval:** Allows you to enter the reconnection interval with the server. Configurable between 1 and 600s.
- **Connection Timeout:** Allows you to enter the maximum time to wait for a broker to respond. Configurable between 1 and 30 s.
- **Enable LWT:** If enabled, allows you to send a last message/warning when **AirGate 4G Wi-Fi** is unintentionally disconnected from the server.
  - **LWT Topic:** Allows you to write your last publication.
  - **Testament:** Allows you to write the message to be sent before the user is disconnected.
- **Enable Verbose Log:** Enables the display of a detailed log.

6.4.4.2 TRANSPORT DATA SETTINGS

- **Data Location:** Allows you to set the data location mode. This parameter acts when there is a failure in sending data (network connection failure, for example). When the connection is re-established, the data of this period will have the treatment configured as selected below:
  - **NULL:** The data will be discarded.
  - **RAM:** The data will be stored in RAM but lost after restarting the device.
  - **Flash:** The data will be stored in Flash memory and retained even after restarting the device.
- **Data Format:** Allows you to set the data display mode. Like the Modbus alarm configuration (see MODBUS ALARM section of this chapter), the device allows you to decide which information to transmit:
  - **$SERIAL_NUMBER:** Device serial number.
  - **$DATE:** Date and time according to the time configured in the system (AirGate).
  - **$VALUE:** Value of the channel that caused the alarm.
  - **$CONNECTION_INDEX:** Index number of the connection where the alarm occurred.
  - **$CONNECTION_DESC:** String configured in the **Description** parameter of the connection in alarm.
  - **$CHANNEL_INDEX:** Index number of the channel in which the alarm occurred.
  - **$CHANNEL_DESC:** String configured in the **Description** parameter of the channel where the alarm occurred.
  - **$SLAVE_ID:** Number of the slave that caused the alarm.
  - **$REGISTER_ADDER:** Number of the register that caused the alarm.
  - **$FUNC_CODE:** Function as configured in the channel in alarm. Example: "func_code 3" represents the "03-Holding-register" setting.
  - **$TRANSPORT_INDEX:** Index number of the connection where the transport is taking place.
  - **$TRANSPORT_DESC:** String configured in the **Description** parameter of the connection where the transport is taking place.
- **Line Break:** Allows you to enable the break of lines during the sending of information.

6.4.4.3 MODBUS CHANNEL

By clicking the ⊕ button in this section, you can define Modbus Master data to be sent in the CSV file, as shown in the figure below:



Channel Settings

Modbus Channel

Index: 1

Enable: ☑

Connection Index: 1

Filter Items: Slave ID

Slave ID: 1

Figure 152 – Configuring the data to be sent (3)

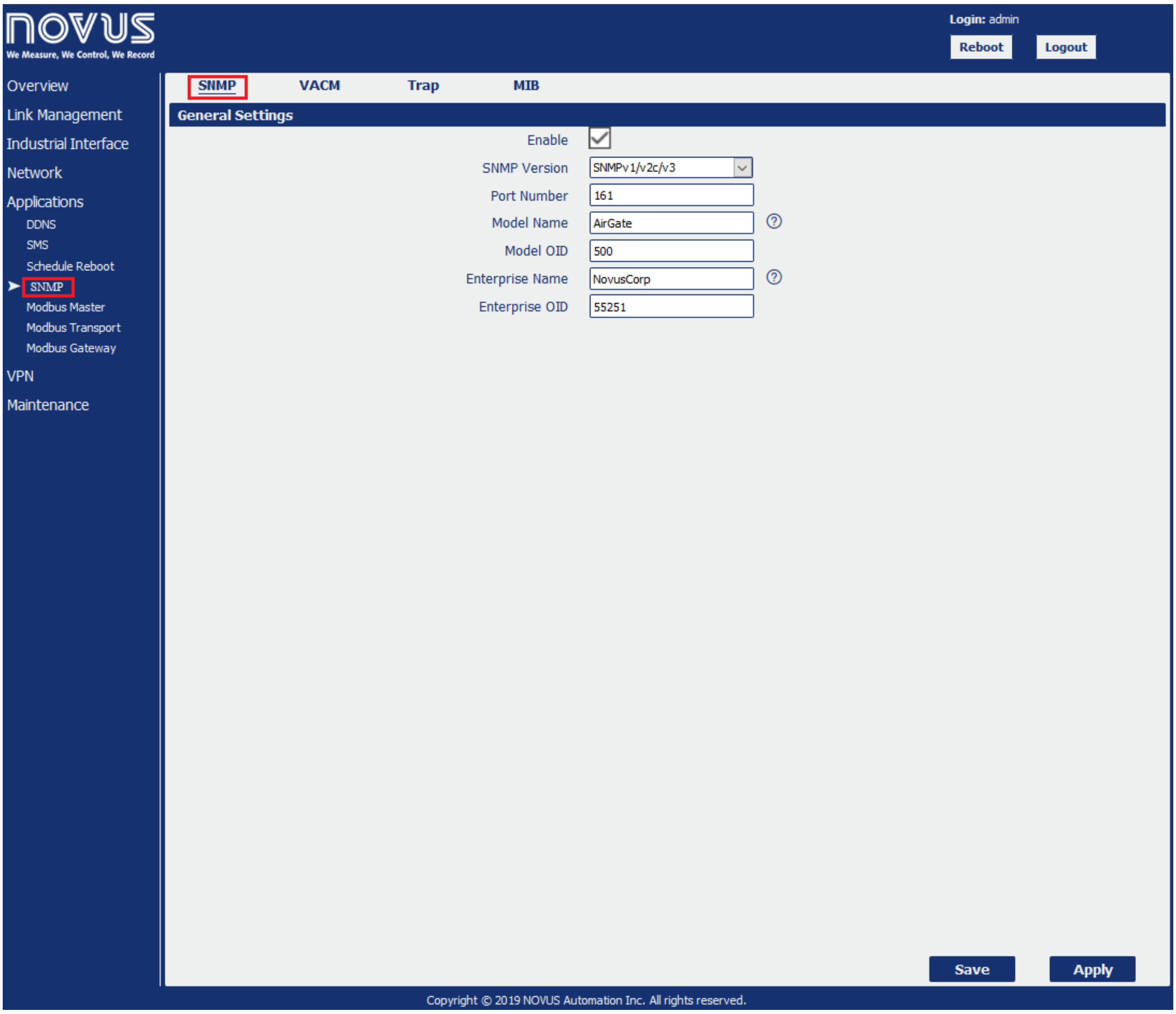
- **Enable:** Allows you to enable a Modbus channel to transport data.
- **Connection Index:** Allows you to define the index of the connection from which to send the data.
- **Filter Items:** Allows you to filter the type of data to be sent: "Channel Index", "Slave ID" or "Register Address".

- **Channel Index:** When choosing this option, you must enter the channel of the Modbus connection that will send the data. If the field is left blank, the device will send all the data of this connection.
- **Slave ID:** When choosing this option, you must enter the address of the slave that will send the data. All the registers of this slave will be transported.
- **Register Address:** When choosing this option, you must enter the address of the register that will send the data

6.5 "SNMP" APPPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, you can use the SNMP protocol to access and manage **AirGate 4G Wi-Fi** information (You cannot access the data of the communication interfaces through this protocol). The application also allows you to send alarm notifications of router events.

To configure it, you must access the **AirGate 4G Wi-Fi** web interface, locate the **Applications** option on the left menu and then click on **SNMP**, as shown below:



General Settings

Enable	☑
SNMP Version	SNMPv1/v2c/v3
Port Number	161
Model Name	AirGate
Model OID	500
Enterprise Name	NovusCorp
Enterprise OID	55251

Figure 153 – SNMP

Once this is done, you must configure the following parameters:

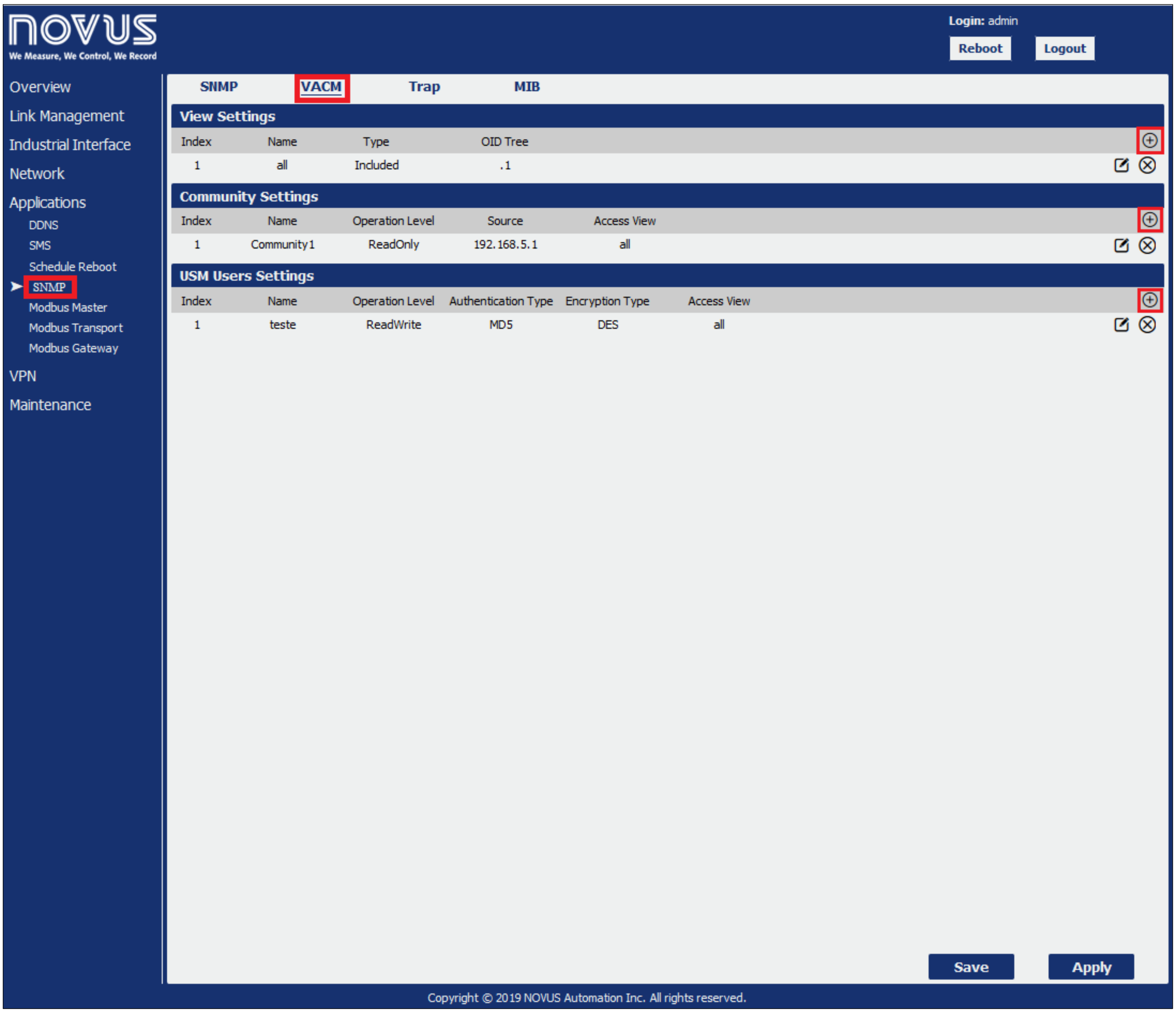
- **Enable:** Allows you to enable the functionality of the protocol.
- **SNMP Version:** Allows you to select the version of the protocol to be used: SNMPv1/v2/v3 or SNMPv3.
- **Port Number:** Allows you to insert the communication port with the SNMP protocol. By default, port 161.
- **Model Name:** Allows you to insert the name of the MIB file model to be used. Do not use space or reserved keywords such as "router", "operation" and "notification".
- **Model OID:** Allows you to insert the Object Identifier (OID) model. By default, 500.
- **Enterprise Name:** Allows you to insert the company name of the MIB tree. Do not use space or reserved keywords such as "router", "operation" and "notification".
- **Enterprise OID:** Allows you to insert the Object Identifier (OID) of the company. By default, 55251.

Once the parameters have been configured, you must click on **Apply**.

This application is compatible with **AirGate 4G Wi-Fi** firmware version 1.1.4.

6.5.1 VACM

VACM settings allow you to select different sets of permissions for users according to criteria set by the **AirGate 4G Wi-Fi** administrator.



View Settings

Index	Name	Type	OID Tree
1	all	Included	.1

Community Settings

Index	Name	Operation Level	Source	Access View
1	Community1	ReadOnly	192.168.5.1	all

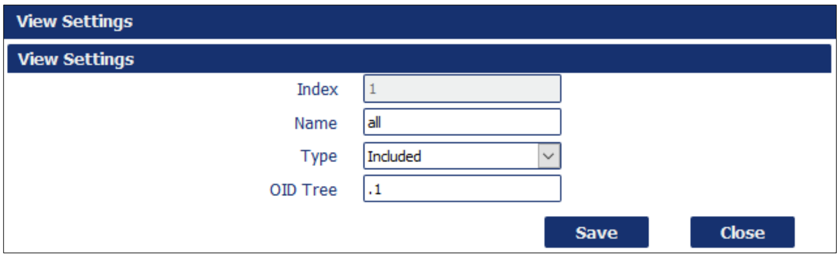
USM Users Settings

Index	Name	Operation Level	Authentication Type	Encryption Type	Access View
1	teste	ReadWrite	MD5	DES	all

Figure 154 – VACM

6.5.1.1 VIEW SETTINGS

You must click on the button ⊕, located on the right of the screen, as shown in the previous picture, to access the display settings of this section:



Index	1
Name	all
Type	Included
OID Tree	.1

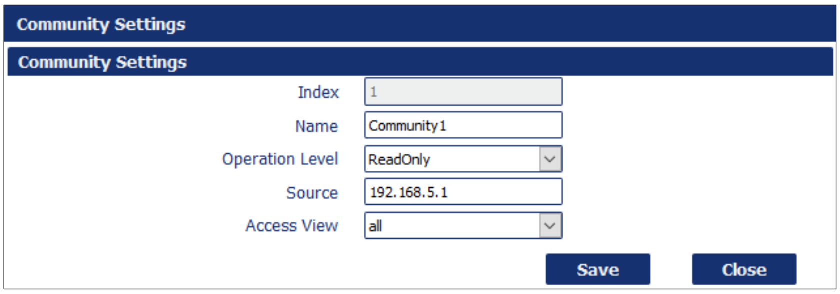
Figure 155 – View VACM settings

- **Index:** Filled in according to the configuration of each user. Up to 08 users can be configured.
- **Name:** Allows you to define a name for the access parameter.
- **Type:** Allows you to define the Object Identifier (OID): "Included" (Including the level of the tree configured in parameter **OID Tree**) or "Excluded" (Excluding the level of the tree configured in parameter **OID Tree**).
- **OID Tree:** Allows you to define from which level of the tree the user configured will have access.

After creating the first configuration and returning to the VACM settings screen, you can click the button ✎ to edit the selected configuration. Clicking the button ⊗, in turn, allows you to delete the selected setting.

6.5.1.2 COMMUNITY SETTINGS

You must click on the button ⊕, located on the right of the screen, as shown in the previous picture, to access the community settings:



Community Settings

Community Settings

Index	1
Name	Community1
Operation Level	ReadOnly
Source	192.168.5.1
Access View	all

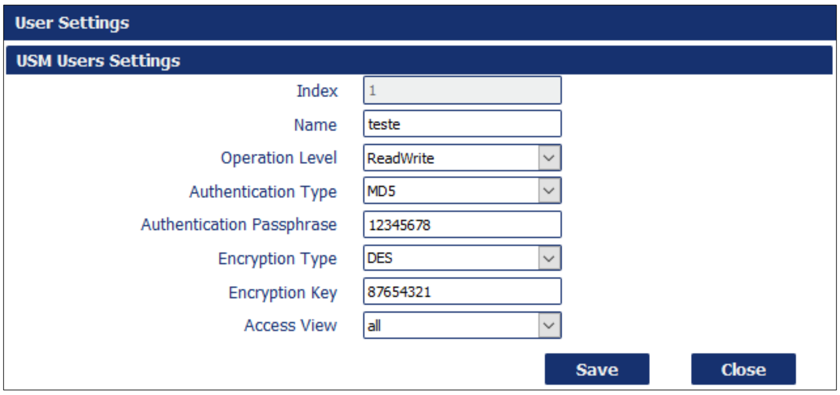
Figure 156 – Community settings

- **Index:** Filled in according to the configuration of each community. Up to 04 communities can be configured.
- **Name:** Allows you to define a name for the community.
- **Operation Level:** Allows you to define the operation level of the community: "ReadOnly" or "ReadWrite".
- **Source:** Allows you to define the IP address that will access the **AirGate 4G Wi-Fi** settings.
- **Access View:** Allows you to define the view access level. Any option previously configured can be selected in the **View Settings** section (see section VIEW SETTINGS of this chapter).

After creating the first configuration and returning to the VACM settings screen, you can click the button ✎ to edit the selected community. Clicking the button ⊗, in turn, allows you to delete the selected community.

6.5.1.3 USM USER SETTINGS

You must click on the button ⊕, located on the right of the screen, as shown in the previous picture, to access the user settings:



User Settings

USM Users Settings

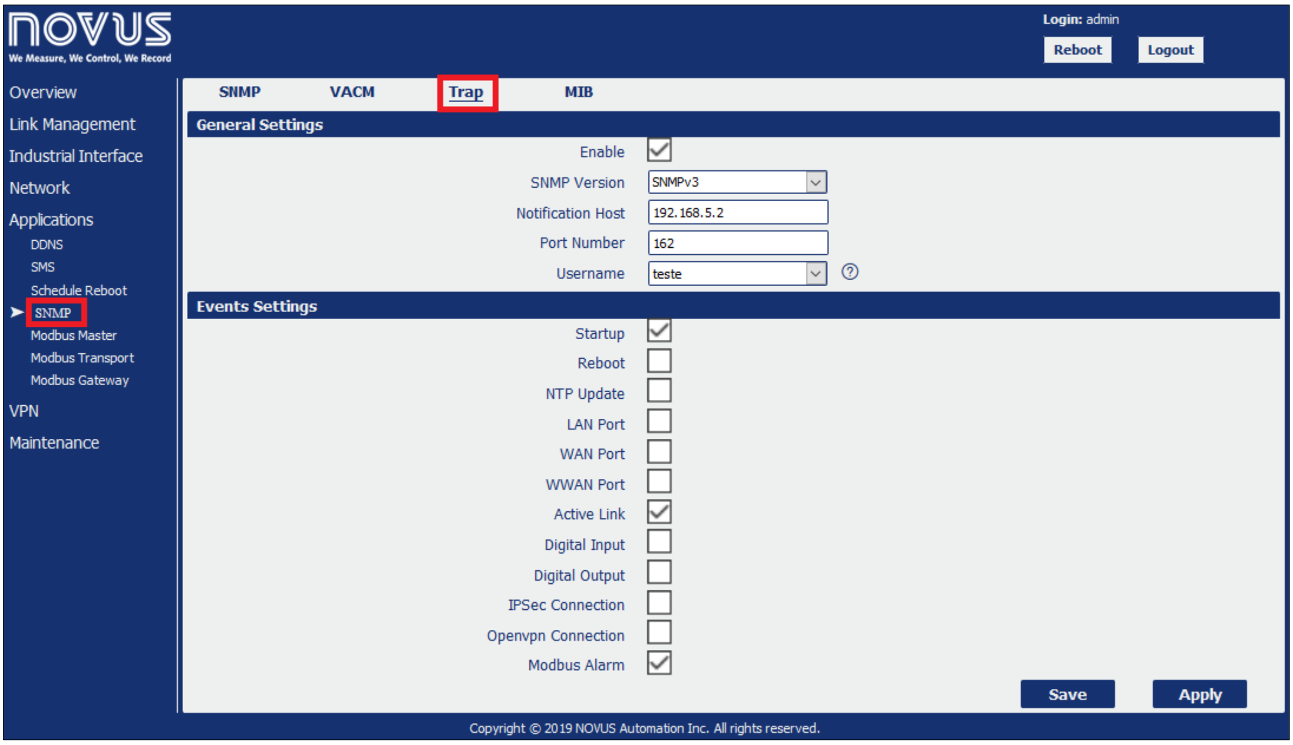
Index	1
Name	teste
Operation Level	ReadWrite
Authentication Type	MD5
Authentication Passphrase	12345678
Encryption Type	DES
Encryption Key	87654321
Access View	all

Figure 157 – User settings

- **Index:** Filled in according to each user's configuration. Up to 04 users can be configured.
- **Name:** Allows you to define a name for the user.
- **Operation Level:** Allows you to select the user's operation level: "ReadOnly" or "ReadWrite".
- **Authentication Type:** Allows you to select the user's security authentication level: None, MD5, SHA, SHA256 or SHA 512.
- **Authentication Passphrase:** Allows you to define the authentication password.
- **Encryption Type:** Allows you to select the type of encryption to be used: DES or AES.
- **Encryption Key:** Allows you to define the encryption key.
- **Access View:** Allows you to define the view access level. Any option previously configured can be selected in the **View Settings** section (see section VIEW SETTINGS of this chapter).

6.5.2 TRAP NOTIFICATION

This SNMP protocol notification feature allows you to send **AirGate 4G Wi-Fi** event notifications to a predetermined server



General Settings

Enable	☑
SNMP Version	SNMPv3
Notification Host	192.168.5.2
Port Number	162
Username	teste

Events Settings

Startup	☑
Reboot	□
NTP Update	□
LAN Port	□
WAN Port	□
WWAN Port	□
Active Link	☑
Digital Input	□
Digital Output	□
IPSec Connection	□
Openvpn Connection	□
Modbus Alarm	☑

Figure 158 – Trap notification

6.5.2.1 GENERAL SETTINGS

- **Enable:** Allows you to enable the Trap notification sending settings.
- **SNMP Version:** Allows you to select the version of the protocol to be used: SNMPv1, SNMPv2c or SNMPv3.
- **Host Notification:** Allows you to define the address of the server to which the Trap notifications will be redirected.
- **Port Number:** Allows you to define the communication port with the SNMP Trap protocol. By default, port 162.
- **Username:** Allows you to select one of the users configured in the **USM Users Settings** section (see USM USER SETTINGS section of this chapter).

6.5.2.2 EVENTS SETTINGS

This group of parameters allows you to define the situations in which notifications will be sent.

- **Startup:** Enables Trap notification to be sent every time the system is booted.
- **Reboot:** Enables Trap notification to be sent every time the system is rebooted.
- **NTP Update:** Enables Trap notification to be sent every time the internal clock is updated from an NTP server.
- **LAN Port:** Enables Trap notification to be sent every time a LAN port is connected or disconnected through an Ethernet output.
- **WAN Port:** Enables Trap notification to be sent every time a WAN port is connected or disconnected through an Ethernet output.
- **WWAN Port:** Enables Trap notification to be sent every time a WWAN port is connected or disconnected through the 4G interface.
- **Active Link:** Enables Trap notification to be sent every time an active link is connected or disconnected through a WAN or WWAN port.
- **Digital Input:** Enables Trap notification to be sent every time there is a change in the logical level of one of the digital inputs.
- **Digital Output:** Enables Trap notification to be sent every time there is a change in the logical level of any of the digital outputs.
- **IPsec Connection:** Enables Trap notification mails to be sent every time a VPN connection with IPsec is established.
- **OpenVPN Connection:** Enables Trap notification to be sent whenever a VPN connection to OpenVPN is established.
- **Modbus Alarm:** Enables Trap notification to be sent each time a Modbus alarm is detected. For more information on configuring a Modbus alarm for sending Trap notification, see the MODBUS ALARM section of this manual. For more information on using and configuring the SNMP protocol, see section CONFIGURING SNMP AND MG MIBBROWSER SOFTWARE of this manual.

6.5.3 MIB (MANAGEMENT INFORMATION BASE)

The Management Information Base (MIB) is the set of managed objects that aims to include all the information needed for the management of the router's network.

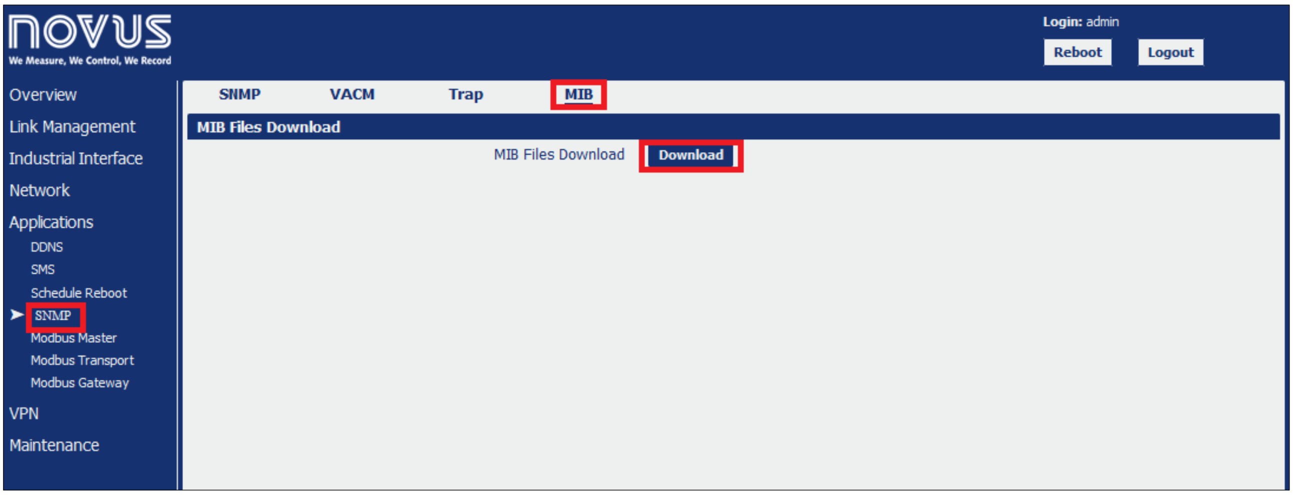


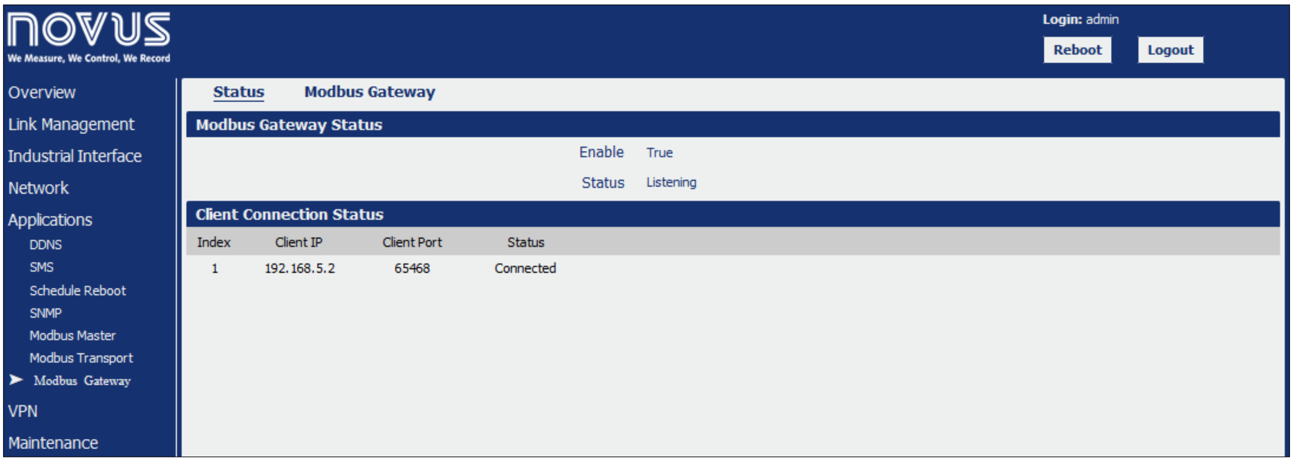
Figure 159 – MIB files

The **AirGate 4G Wi-Fi** MIB files can be downloaded via the **Download** button on this page, as shown above.

The files will be in the zip file **snmp-mibs.tar.gz**.

6.6 "MODBUS GATEWAY" APPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, can be configured through the **AirGate 4G Wi-Fi** web interface. Access the **Applications** option, located on the left menu, and then click **Modbus Gateway**, as shown in the figure:



Modbus Gateway Status

Enable: True

Status: Listening

Client Connection Status

Index	Client IP	Client Port	Status
1	192.168.5.2	65468	Connected

Figure 160 – Modbus Gateway application

Modbus Gateway allows the device to transmit data from serial ports via TCP Client protocol. This application is compatible with **AirGate 4G Wi-Fi** firmware version 1.1.4.

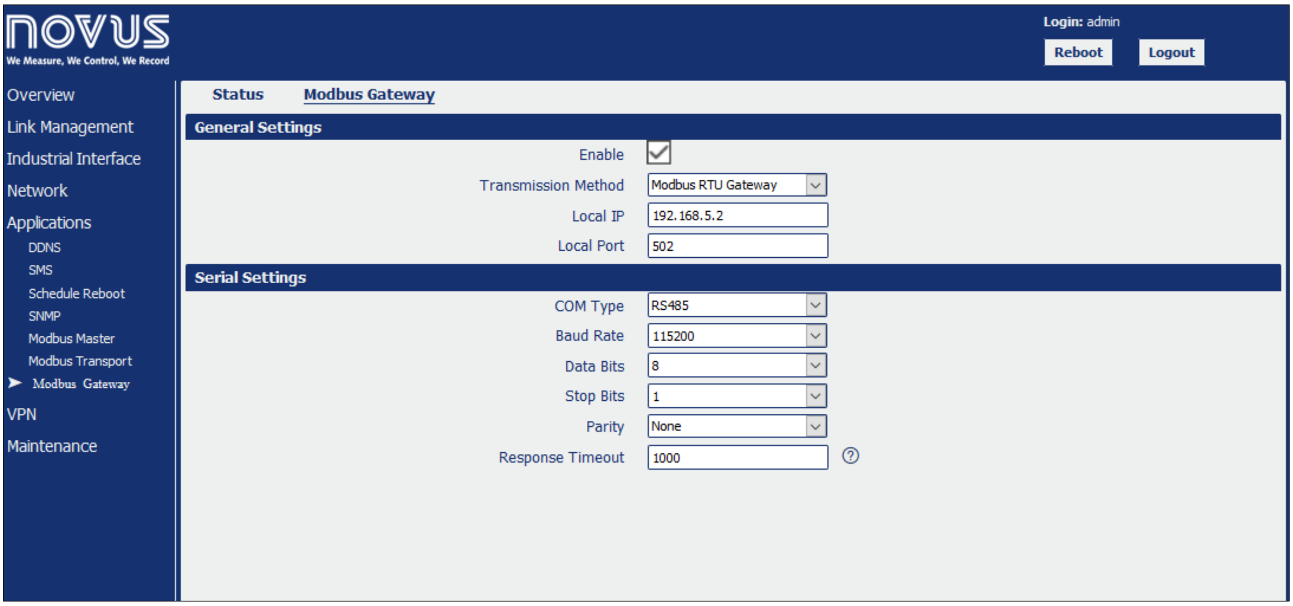
STATUS

- **Enable:** Shows the protocol status: "True" when enabled and "False" when disabled.
- **Status:** Shows **AirGate 4G Wi-Fi** status: "Listening" when listening to the network and waiting for client requests and "Binding" when waiting for requests from a configured local IP.

CLIENT CONNECTION STATUS

The **AirGate 4G Wi-Fi** shows the list of clients connected to the device and searching for serial port information via Gateway mode.

6.6.1 MODBUS GATEWAY



General Settings

Enable: ☑

Transmission Method: Modbus RTU Gateway

Local IP: 192.168.5.2

Local Port: 502

Serial Settings

COM Type: RS485

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: None

Response Timeout: 1000

Figure 161 – Configuring Modbus Gateway

6.6.1.1 GENERAL SETTINGS

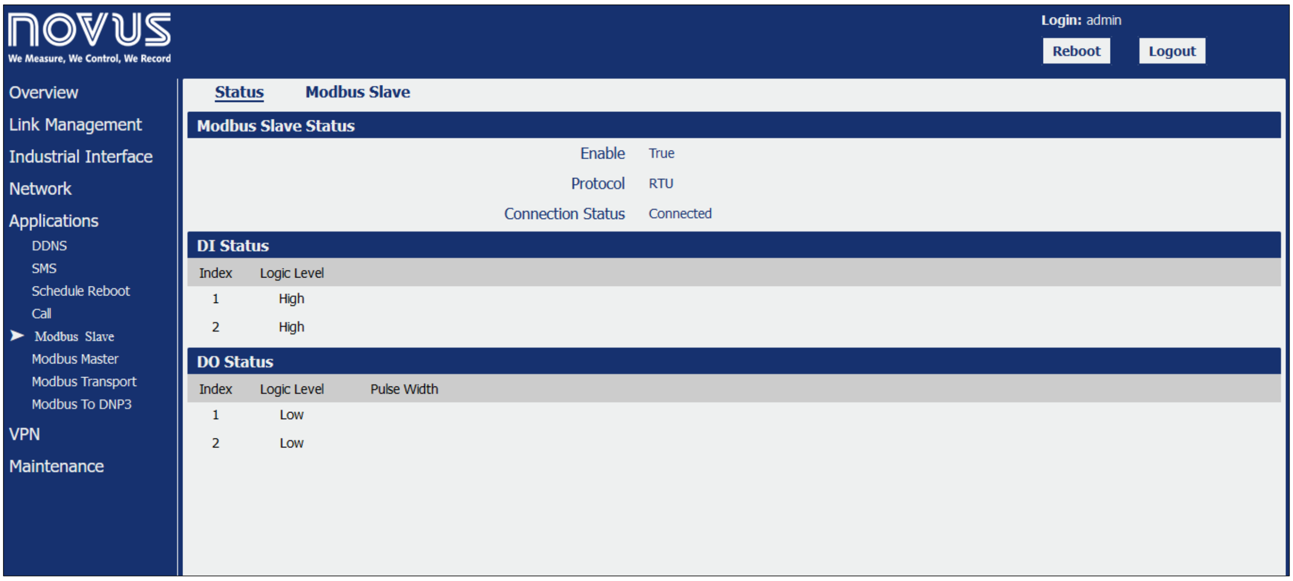
- **Enable:** Allows you to enable or disable the gateway mode settings.
- **Transmission Method:** Allows you to select the serial port transmission method: Modbus RTU Gateway or Modbus ASCII Gateway.
- **Local IP:** Allows you to configure the IP address of the local endpoint. The parameter can be left blank, suggesting that any IP can access the **AirGate 4G Wi-Fi**.
- **Local Port:** Displays the port number assigned to the serial IP port on which communications will occur.

6.6.1.2 SERIAL SETTINGS

- **COM Type:** Allows you to select the COM port type with which the **AirGate 4G Wi-Fi** will travel the data.
- **Baud Rate:** Allows you to select the Baud Rate of the serial port: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to select the data bits of the serial port: Values of 7 or 8.
- **Stop Bits:** Allows you to select the Stop Bits of the serial port: Values of 1 or 2.
- **Parity:** Allows you to select the serial port parity: "None", "Even" or "Odd".
- **Response Timeout:** Allows you to select the response time during the connection.

6.7 "MODBUS GATEWAY" APPLICATION

Once the application has been installed as described in the INSTALLING AND REMOVING APPLICATIONS section, can be configured through the **AirGate 4G Wi-Fi** web interface. Access the **Applications** option, located on the left menu, and then click **Modbus Slave**, as shown in the figure below:



Modbus Slave Status

Enable True

Protocol RTU

Connection Status Connected

DI Status

Index	Logic Level
1	High
2	High

DO Status

Index	Logic Level	Pulse Width
1	Low	
2	Low	

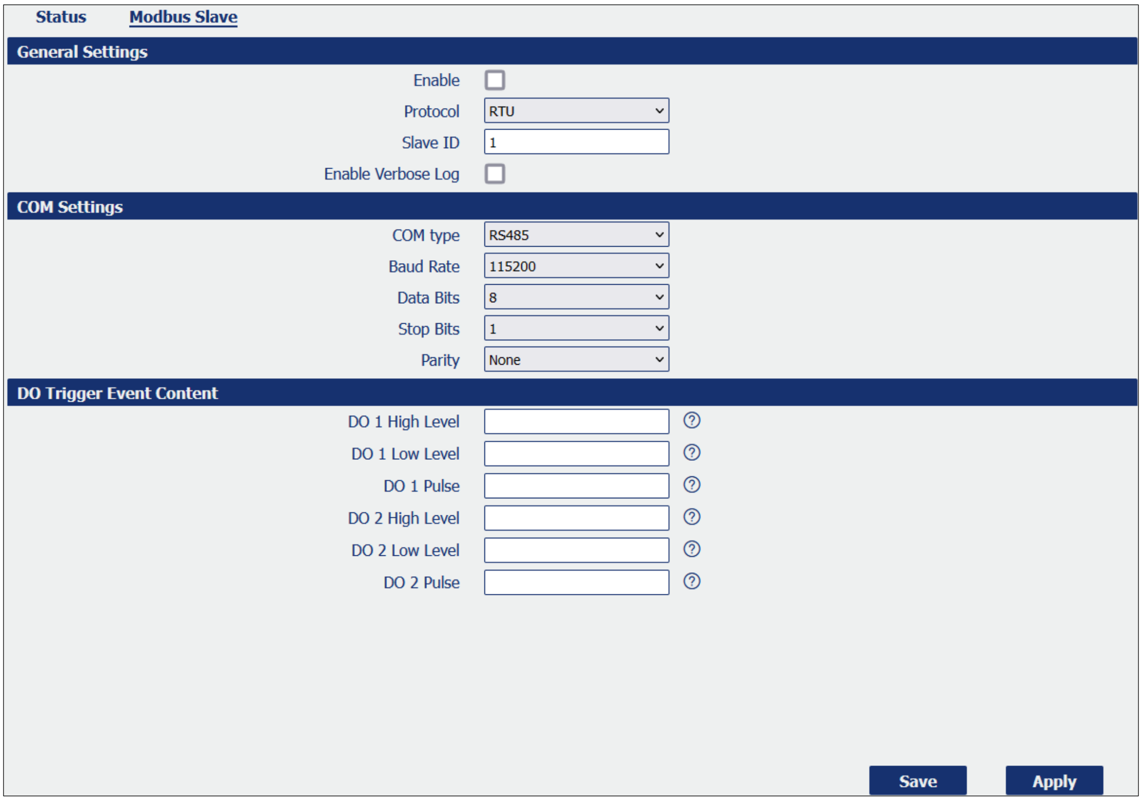
Figure 162 – Modbus slave

This application allows **AirGate 4G Wi-Fi** to act as a Modbus slave, making the input and output registers available for external audit. The connection can be RTU over RS485 and RS232 or Modbus-TCP.

This application is compatible with **AirGate 4G Wi-Fi** firmware version 1.1.6.

6.1.1 MODBUS SLAVE

Modbus Slave allows you to configure **AirGate 4G Wi-Fi** as a slave.



General Settings

Enable □

Protocol RTU

Slave ID 1

Enable Verbose Log □

COM Settings

COM type RS485

Baud Rate 115200

Data Bits 8

Stop Bits 1

Parity None

DO Trigger Event Content

DO 1 High Level

DO 1 Low Level

DO 1 Pulse

DO 2 High Level

DO 2 Low Level

DO 2 Pulse

Figure 163 – Configuring Modbus Slave

6.7.1.1 GENERAL SETTINGS

- **Enable:** Allows you to enable **AirGate 4G Wi-Fi** slave mode. The mode may already be configured but disabled.
- **Protocol:** Allows you to define the protocol: TCP/IP or RTU.
- **Slave ID:** Allows you to identify the network slave whose register will be read.
- **Enable Verbose Log:** Enables the display of a detailed log.

6.7.1.2 TCP SETTINGS

- **Local IP:** Allows you to set the IP address.
- **Local Port:** Allows you to define the server port. By default, port 502.

6.7.1.3 COM SETTINGS

- **COM Type:** Allows you to define a connection type: RS232 or RS485.
- **Baud Rate:** Allows you to define the Baud Rate to be used: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to define the data bits. Only 8 is selectable.
- **Stop Bits:** Allows you to define the Stop Bits: 1 or 2.
- **Parity:** Allows you to define the parity to be used: "None", "Even" or "Odd".

6.7.1.4 DO TRIGGER EVENT CONTENT

Each of the digital output events can be linked to different device services, such as SMS, MQTT, and email notification. In this section you can define the content of each message, according to the digital output status. The options are:

- **DO 1 High Level:** Allows you to define a description for the message to be displayed when digital output 1 is at high level. To see the types of description allowed for this parameter, see the section below.
- **DO 1 Low Level:** Allows you to define a description for the message to be displayed when digital output 1 is at low level. To see the types of description allowed for this parameter, see the section below.
- **DO 1 Pulse:** Allows you to define a description for the message to be displayed when digital output 1 is in pulse mode. To see the types of description allowed for this parameter, see the section below.
- **DO 2 High Level:** Allows you to define a description for the message to be displayed when digital output 2 is at high level. To see the types of description allowed for this parameter, see the section below.
- **DO 2 Low Level:** Allows you to define a description for the message to be displayed when digital output 2 is at low level. To see the types of description allowed for this parameter, see the section below.
- **DO 2 Pulse:** Allows you to define a description for the message to be displayed when digital output 2 is in pulse mode. To see the types of description allowed for this parameter, see the section below.

DESCRIPTION TYPE:

You can define the following types of descriptions for the messages to be displayed during events involving the digital outputs:

- **$DI_INDEX:** Displays the digital input index if it is linked to a digital output.
- **$DATE:** Displays the event timestamp.
- **$SERIAL_NUMBER:** Displays the device serial number.
- **$DEVICE_MODEL:** Displays the device model.
- **$FIRMWARE_VERSION:** Displays the device firmware version.
- **$SYSTEM_UPTIME:** Display the system timestamp.
- **$LINK_TYPE:** Displays the connection type configured for Internet access.
- **$IP_ADDRESS:** Displays the IP address configured for the router.
- **$MODEM_MODEL:** Displays the modem module used by the connection.
- **$CSQ:** Displays the signal strength of the network operator linked to the SIM card.
- **$OPERATOR:** Displays the network operator.
- **$NETWORK_TYPE:** Displays the name of the currently 2G/3G/4G technology: "LTE" (Long Term Evolution), "UMTS" (Universal Mobile Telecommunications Service) or "CDMA" (Code Division Multiple Access).
- **$IMEI:** Displays the IMEI (International Mobile Equipment Identifier) number of the SIM card being used. Depending on the network operator and the technology used, activation by the network operator may be required. In some cases, this parameter will remain blank.
- **$PLMN_ID:** Displays the PLMN (Public Land Mobile Network) ID, including MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Location Area Code) and CI (Cell Identification).
- **$LOCAL_AREA_CODE:** Displays the SIM card location area code.
- **$CELL_ID:** Displays the SIM card ID.
- **$IMSI:** Displays the IMSI (International Mobile Electronic Identifier) read by the SIM card.
- **$MODEM_FIRMWARE:** Displays the firmware version of the module used by the connection.

7 TUTORIALS

This chapter presents tutorials that show how to configure different features of the **AirGate 4G Wi-Fi**.

7.1 RS232: TRANSPARENT MODE WITH TCP CLIENT

This tutorial shows how to configure and use the Transparent mode of the RS232 interface with **AirGate 4G Wi-Fi** configured as TCP Client.

7.1.1 TOPOLOGY

You can use the following topology:

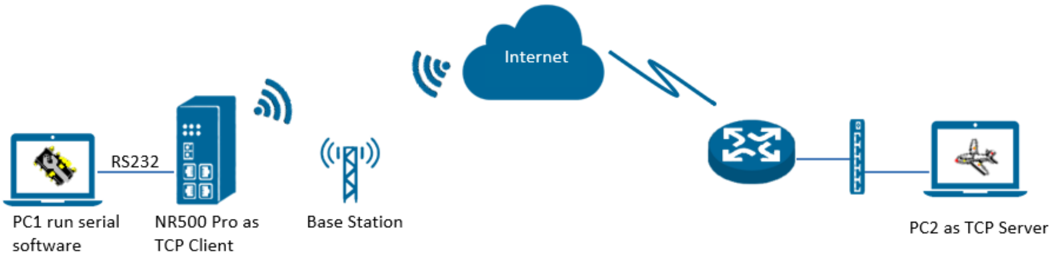


Figure 164 – RS232: Transparent mode

1. **AirGate 4G Wi-Fi** runs as TCP Client and connect to Internet with SIM card.
2. PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through **AirGate 4G Wi-Fi** with TCP transparent mode.
3. PC2 runs as TCP server and assume it can get the Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg can receive the data from TCP Client side.

7.1.2 RS232 CABLE

Follow figure below to make the RS232 cable:

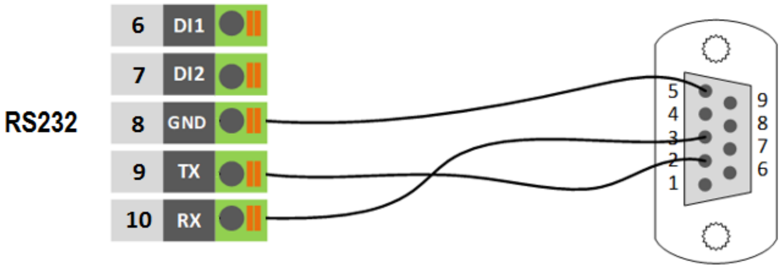


Figure 165 – RS232 Cable

Table 10 shows the connector pins:

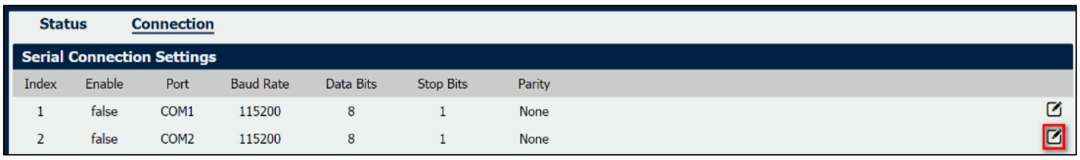
PIN	RS232	RS485	DI	DO	DIRECTION
6	--	--	DI1	--	Router ← Device
7	--	--	DI2	--	Router ← Device
8	GND	--	--	--	--
9	TX	--	--	--	Router → Device
10	RX	--	--	--	Router ← Device

Table 9 – RS232 connector pins

7.1.3 CONFIGURATION

7.1.3.1 RS232 CONFIGURATION

To configure RS232 interface, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Industrial Interface** > **Serial** > **Connection** > **Index 2**. To perform the interface configuration, just click on the COM2 edit button.

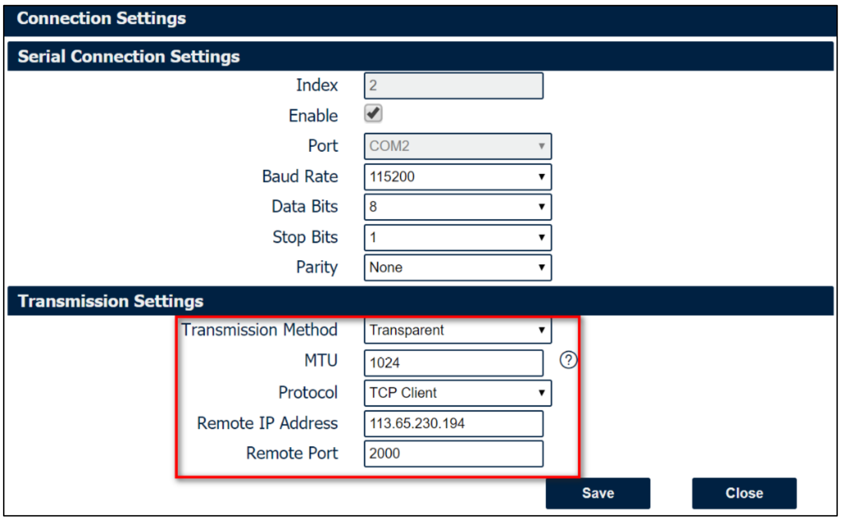


Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Figure 166 – RS232 configuration

To enable RS232 configuration, you must select the protocol as "TCP Client" and enter the server IP address and server port. Then click **Save**.



Connection Settings

Serial Connection Settings

Index: 2
Enable: ☑
Port: COM2
Baud Rate: 115200
Data Bits: 8
Stop Bits: 1
Parity: None

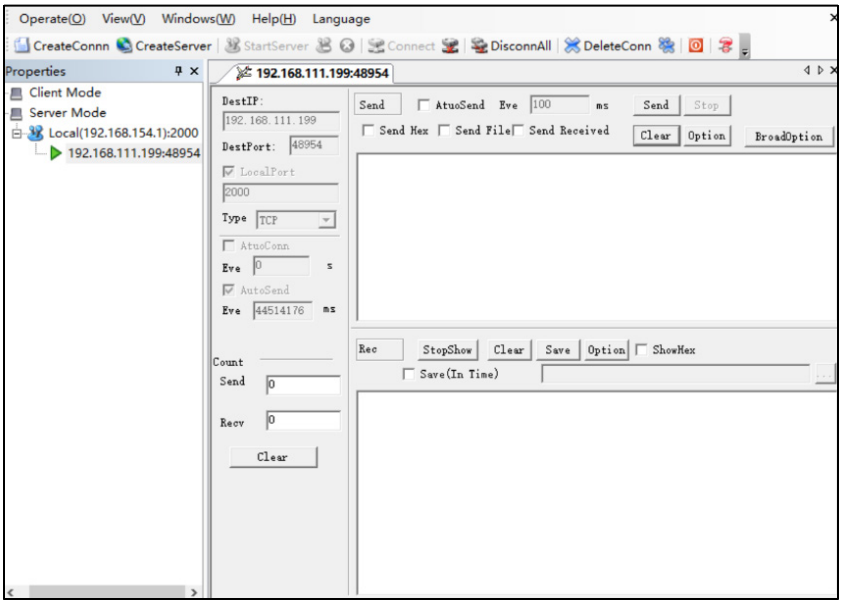
Transmission Settings

Transmission Method: Transparent
MTU: 1024
Protocol: TCP Client
Remote IP Address: 113.65.230.194
Remote Port: 2000

Figure 167 – Transmission configurations

7.1.3.2 TCP SERVER CONFIGURATION

To configure TCP server, you must run the TCP Software "TCPUDPDbg" on server PC2. **AirGate 4G Wi-Fi** will connect to the TCP Server automatically.



Operate(O) View(V) Windows(W) Help(H) Language
CreateConnn CreateServer StartServer Connect DisconnAll DeleteConn
Properties
Client Mode
Server Mode
Send
Stop
Clear
Option
BroadOption
Rec
StopShow
Save
Count

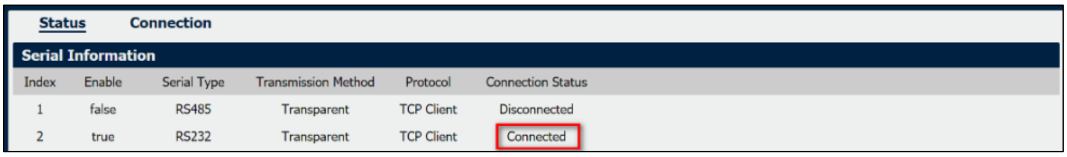
Local(192.168.154.1):2000
192.168.111.199:48954

DestIP: 192. 168. 111. 199
DestPort: 48954
☑ LocalPort 2000
Type TCP
□ AtuoConn
Eve 0 s
☑ AutoSend
Eve 44514176 ms
Send 0
Recv 0

□ AtuoSend Eve 100 ms
□ Send Hex □ Send File □ Send Received
□ ShowHex
□ Save(In Time)

Figure 168 – TCPUDPDDbg Software

In the **AirGate 4G Wi-Fi** Web Interface, go to **Industrial Interface** > **Serial** > **Status** > **Serial Information** > **Index2**. It will show the connection status.



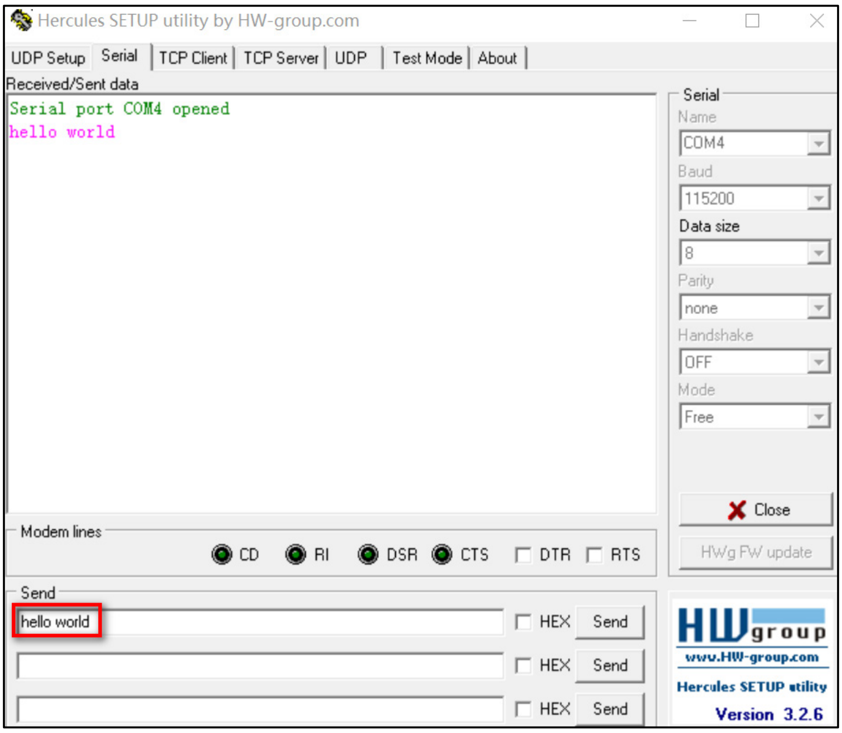
Serial Information

Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	false	RS485	Transparent	TCP Client	Disconnected
2	true	RS232	Transparent	TCP Client	Connected

Figure 169 – RS232 status connection

7.1.4 TEST

To perform a test, run serial software "Hercules" on PC1 and send the data "hello world".



Hercules SETUP utility by HW-group.com

Received/Sent data

```
Serial port COM4 opened
hello world
```

Serial

Name: COM4

Baud: 115200

Data size: 8

Parity: none

Handshake: OFF

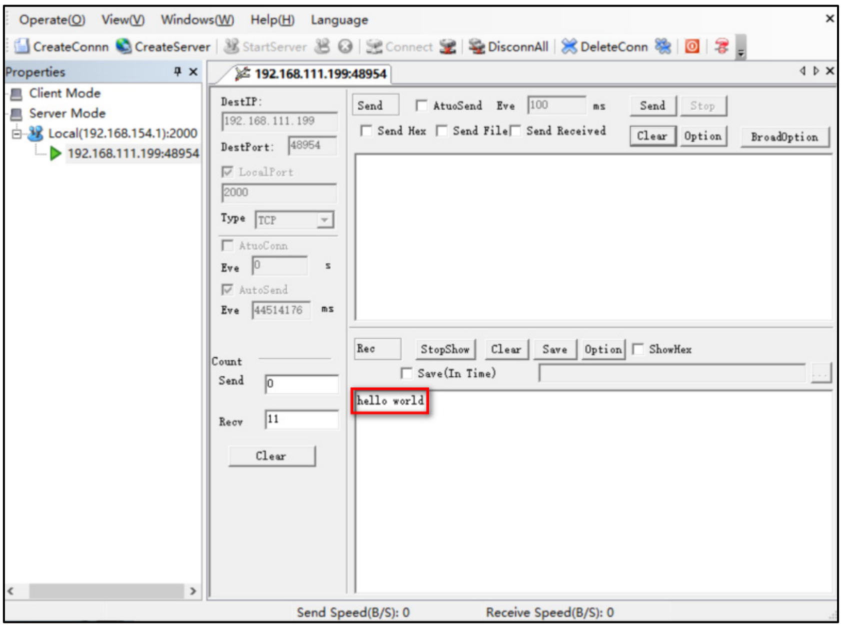
Mode: Free

Modem lines: ● CD ● RI ● DSR ● CTS □ DTR □ RTS

Send: hello world □ HEX Send

Figure 170 – RS232 test

TCP Server side can receive the data "hello world", as shown in figure below. Test successfully.



Client Mode

Server Mode

Local(192.168.154.1):2000

192.168.111.199:48954

DestIP: 192.168.111.199

DestPort: 48954

☑ LocalPort: 2000

Type: TCP

□ AtuoConn Eve 0 s

☑ AutoSend Eve 44514176 ms

Count

Send: 0

Recv: 11

hello world

Send Speed(B/S): 0 Receive Speed(B/S): 0

Figure 171 – RS232 test result

7.2 RS485: TRANSPARENT MODE WITH TCP CLIENT

This tutorial shows how to configure and use the Transparent mode of the RS485 interface with **AirGate 4G Wi-Fi** configured as TCP Client.

7.2.1 TOPOLOGY

You can use the following topology:

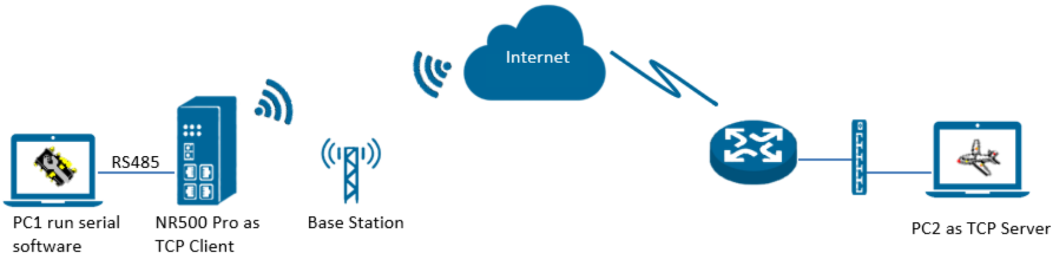


Figure 172 – RS485: Transparent mode

1. **AirGate 4G Wi-Fi** runs as TCP Client and connect to Internet with SIM card.
2. PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through **AirGate 4G Wi-Fi** with TCP transparent mode.
3. PC2 runs as TCP server and assume it can get the Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg can receive the data from TCP Client side.

7.2.2 RS485 CABLE

Follow figure below to make the RS485 cable:

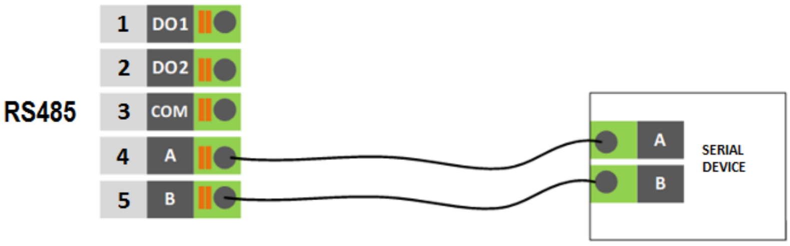


Figure 173 – RS485 Cable

Table 11 shows the connector pins:

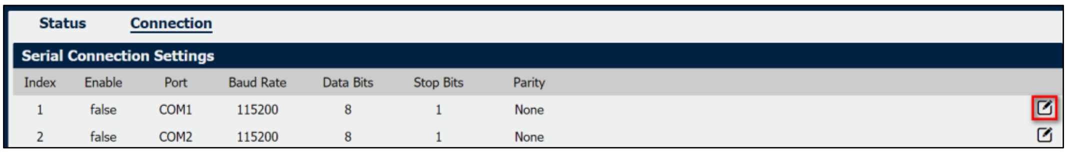
PIN	RS232	RS485	DI	DO	DIRECTION
1	--	--	--	DO1	Router → Device
2	--	--	--	DO2	Router → Device
3	--	--	--	COM	--
4	--	D1	--	--	Router ↔ Device
5	--	D0	--	--	Router ↔ Device

Table 10 – RS485 connector pins

7.2.3 CONFIGURATION

7.2.3.1 RS485 CONFIGURATION

To configure RS485 interface, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Industrial Interface** > **Serial** > **Connection** > **Index 1**. To perform the interface configuration, just click on the COM1 edit button.



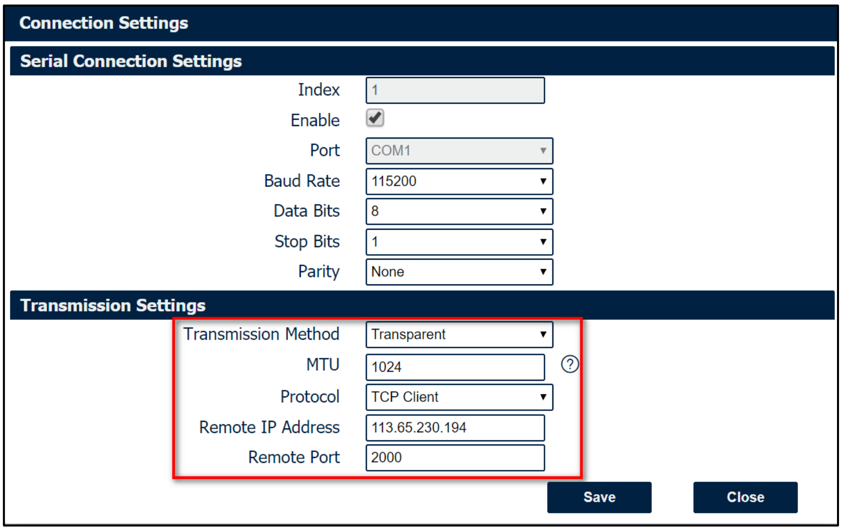
Status Connection

Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Figure 174 – RS485 configuration

To enable RS485 configuration, you must select the protocol as "TCP Client" and enter the server IP address and server port. Then click **Save.**



Connection Settings

Serial Connection Settings

Index	1
Enable	☑
Port	COM1
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None

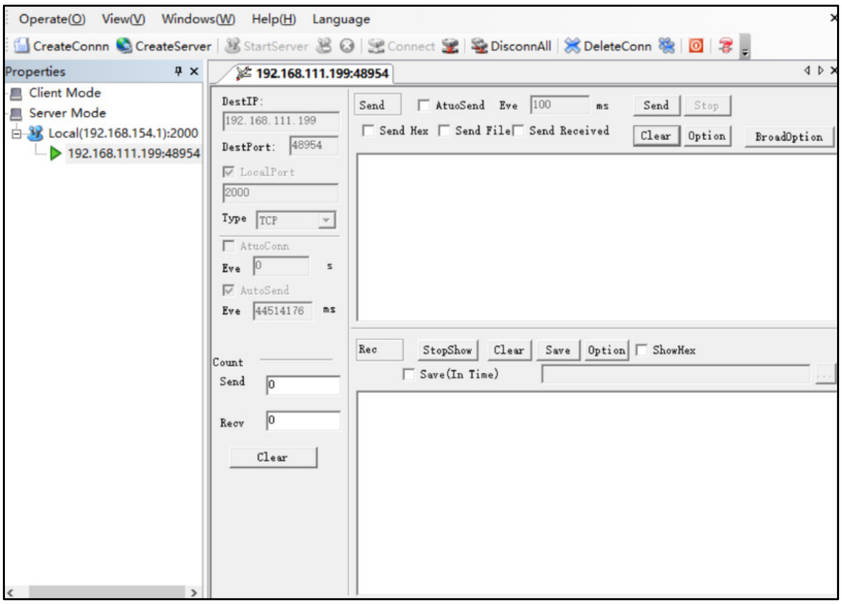
Transmission Settings

Transmission Method	Transparent
MTU	1024
Protocol	TCP Client
Remote IP Address	113.65.230.194
Remote Port	2000

Figure 175 – Transmission configurations

7.2.3.2 TCP SERVER CONFIGURATION

To configure TCP server, you must run the TCP Software "TCPUDPDbg" on server PC2. **AirGate 4G Wi-Fi** will connect to the TCP Server automatically.

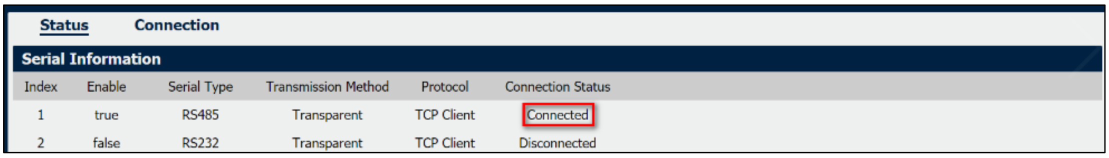


192.168.111.199:48954

DestIP:	192. 168. 111. 199
DestPort:	48954
☑ LocalPort	2000
Type	TCP
□ AtuoConn	
Eve	0 s
☑ AutoSend	
Eve	44514176 ms
Count	
Send	0
Recv	0

Figure 176 – TCPUDPDDbg Software

In the **AirGate 4G Wi-Fi** Web Interface, go to **Industrial Interface > Serial > Status > Serial Information > Index1**. It will show the connection status.



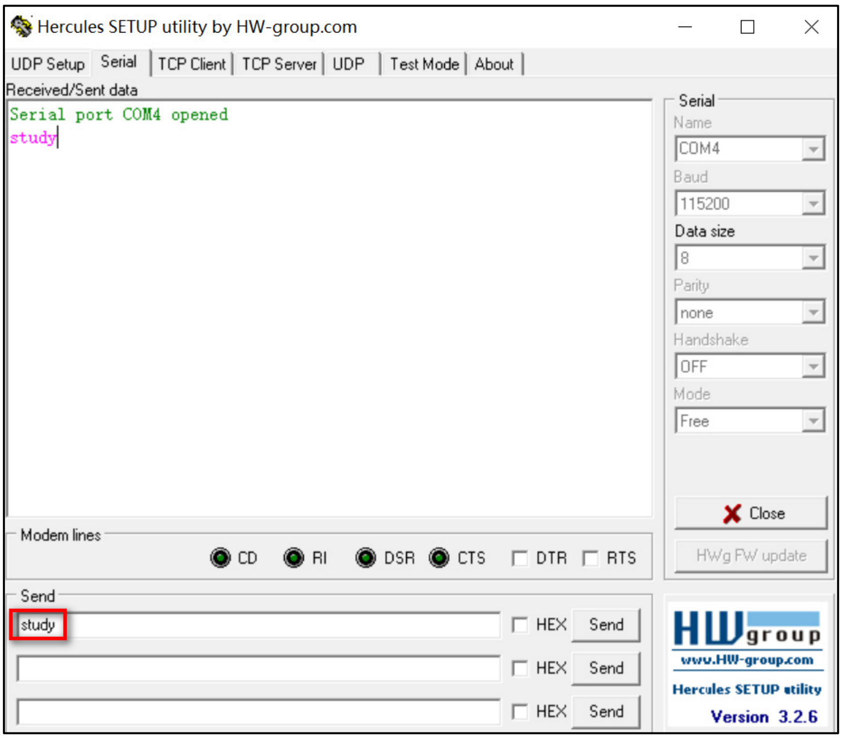
Serial Information

Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	true	RS485	Transparent	TCP Client	Connected
2	false	RS232	Transparent	TCP Client	Disconnected

Figure 177 – RS485 status connection

7.2.4 TEST

To perform a test, run serial software "Hercules" on PC1 and send the data "study".



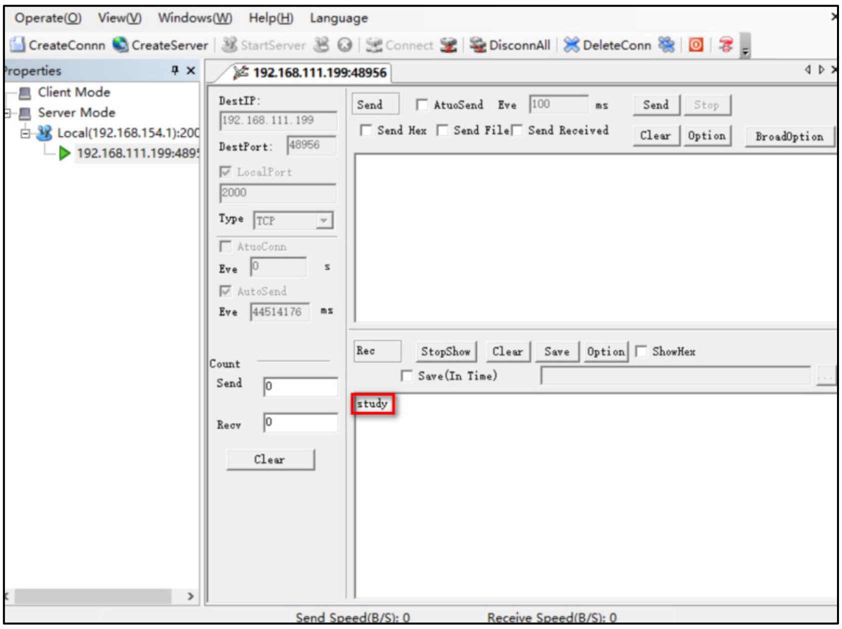
Serial port COM4 opened
study

Serial
Name: COM4
Baud: 115200
Data size: 8
Parity: none
Handshake: OFF
Mode: Free

Send: study

Figure 178 – RS485 test

TCP Server side can receive the data "study", as shown in figure below. Test successfully.



DestIP: 192. 168. 111. 199
DestPort: 48956
☑ LocalPort 2000
Type TCP
□ AtuoConn
Eve 0 s
☑ AutoSend
Eve 44514176 ms

□ AtuoSend Eve 100 ms
□ Send Hex □ Send File □ Send Received
□ ShowHex
□ Save(In Time)

Count
Send 0
Recv 0

study

Send Speed(B/S): 0 Receive Speed(B/S): 0

Figure 179 – RS485 test result

7.3 OPENVPN CERTIFICATES GENERATED

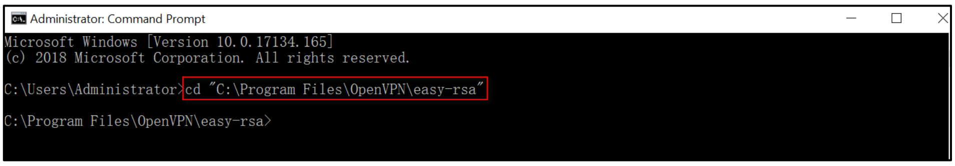
This tutorial shows how to generate certificates needed to use OpenVPN.

7.3.1 OpenVPN SOFTWARE INSTALLED

You must download the OpenVPN software, located at http://openvpn.net/index.php, and install it on a Windows computer.

7.3.2 CERTIFICATES GENERATED

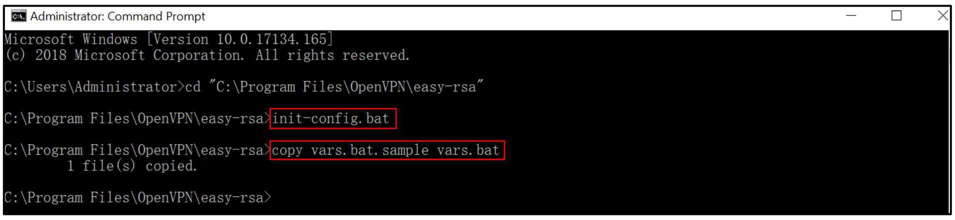
To generate a certificate, you must run as an administrator the Windows command prompt and type the following **cd** command to **"C:\Program Files\OpenVPN\easy-rsa"**, as shown in the figure below:



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 180 – cd "C:\Program Files\OpenVPN\easy-rsa" command

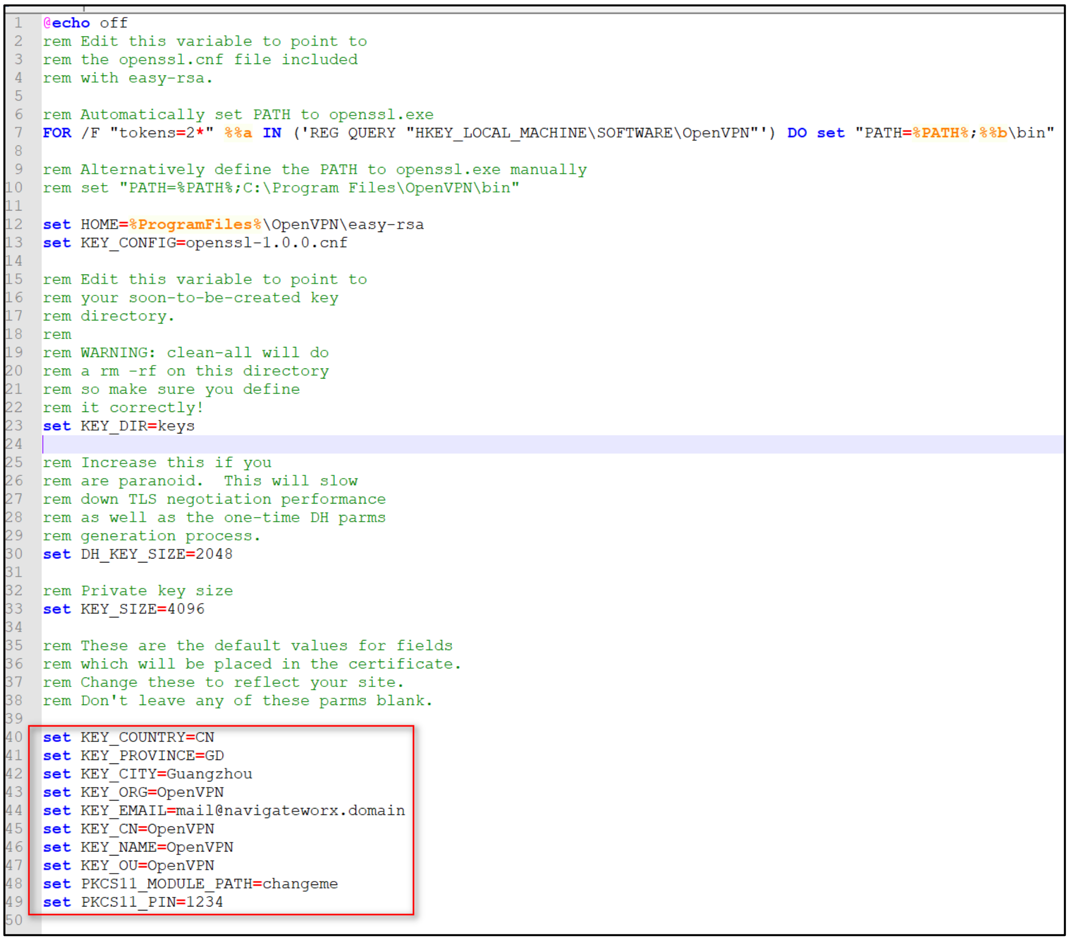
Then run the **init-config.bat** command to copy the configuration files to **vars.bat** (this command will overwrite both the previous **vars.bat** file and the **openssl.cnf** files).



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config.bat

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 181 – init-config.bat command

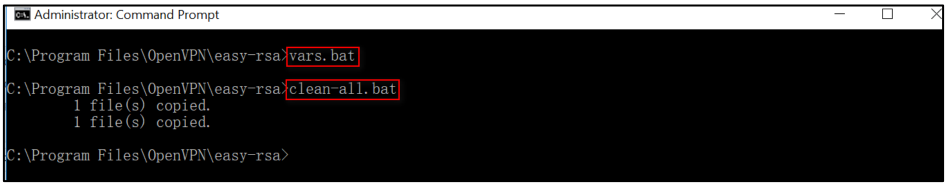
Edit the **vars.bat file** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL, KEY_CN, KEY_NAME, KEY_OU, PKCS11_MODULE_PATH and PKCS11_PIN parameters (parameters must be entered without space):



```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

rem Automatically set PATH to openssl.exe
FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"

rem Alternatively define the PATH to openssl.exe manually
rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@navigateworx.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Figure 182 – Editing the parameters

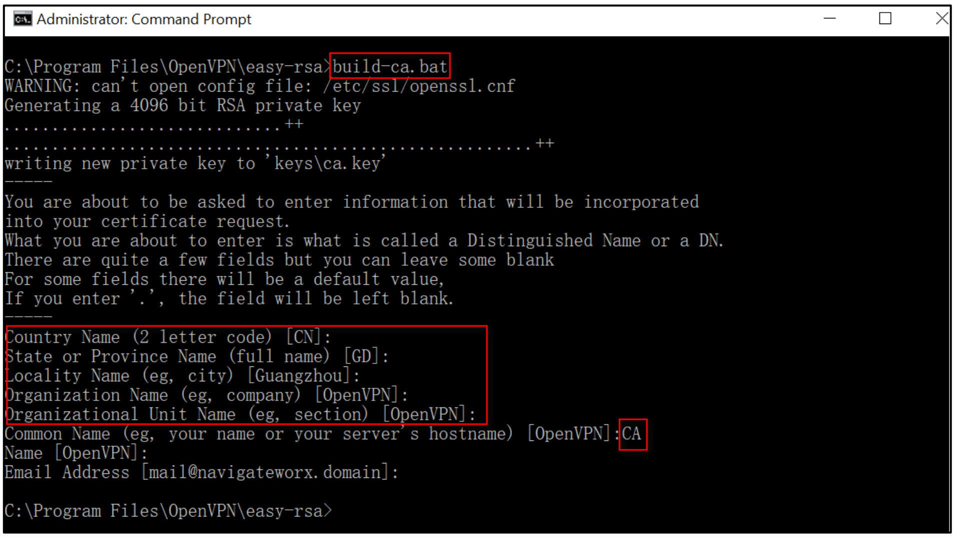
Run the **vars.bat** and **clean-all.bat** commands, as shown in the figure below, to initialize the environment:



```
C:\Program Files\OpenVPN\easy-rsa>vars.bat

C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 183 – vars.bat and clean-all.bat commands

The **build-ca.bat** command will build the certificate authority (CA) and the private key via the interactive openssl command.

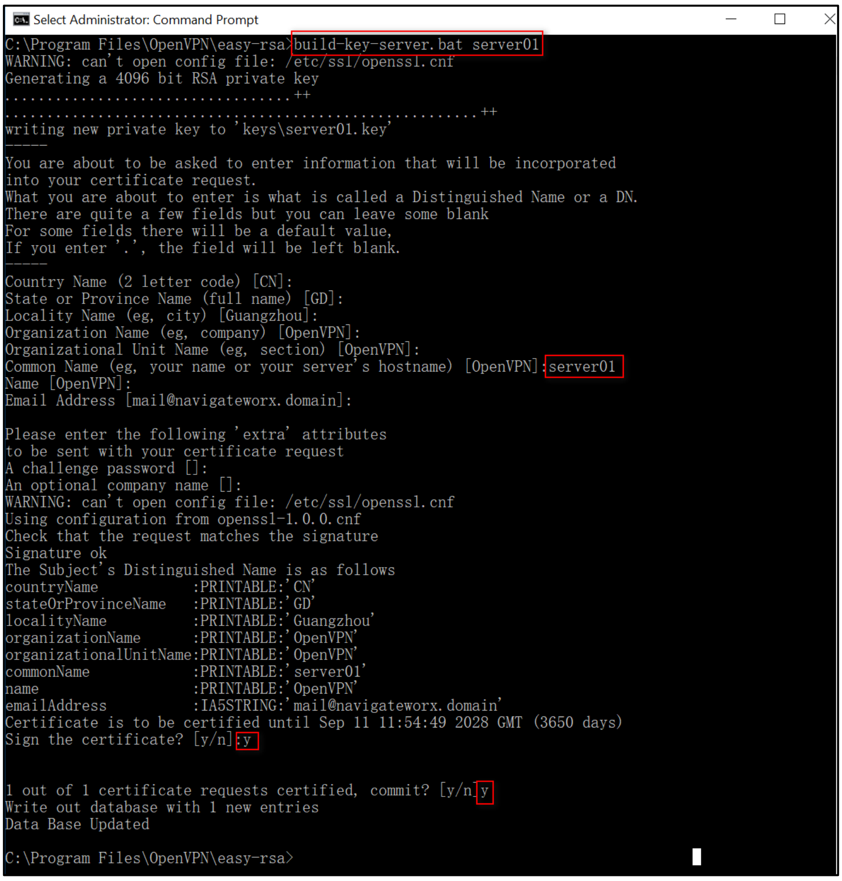


```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
............................++
......................................................++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:CA
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 184 – build-ca.bat command

In the sequence above, most of the parameters show the values configured in the **vars.bat file**. The only parameter to be filled in must be the Common Name parameter, as shown in figure above.

After that, you need to generate a certificate and private key for the server by using the **build-key-server.bad server01** command. When the information to be inserted in the **Common Name** parameter is requested, insert **server01**.

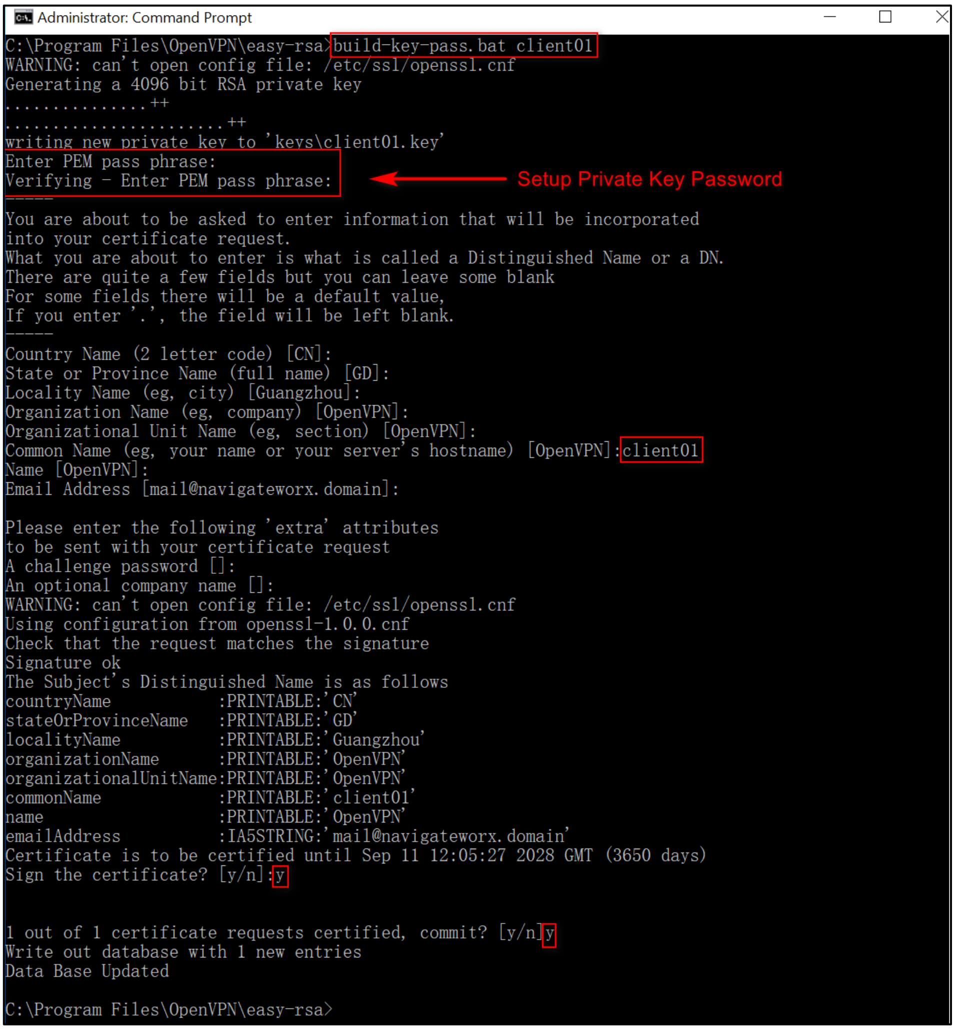


```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
..................................++
.......................................................++
writing new private key to 'keys\server01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:server01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'server01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@navigateworx.domain'
Certificate is to be certified until Sep 11 11:54:49 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 185 – build-key-server.bat server01 command

In the **build-key-server.bat server01** command, **server01** is the file name of the certificate (the name of the private key and the public key).

The next step involves generating the client's certificate and private key when using the **build-key-pass.bat client01** command. You will need to use the key authentication in the OpenVPN client configuration. When the information to be inserted in the **Common Name** parameter is requested, insert **client01**.



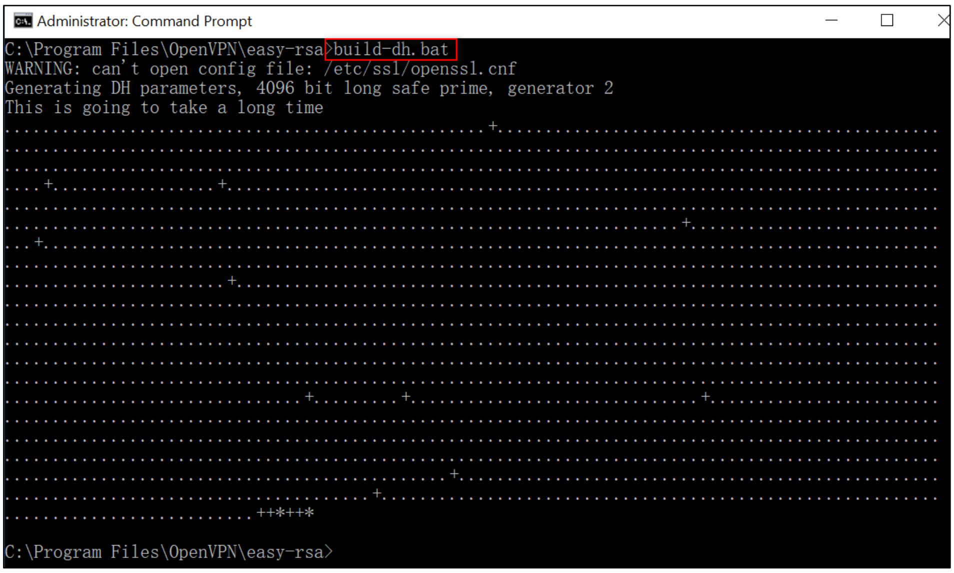
```
C:\Program Files\OpenVPN\easy-rsa>build-key-pass.bat client01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
................++
........................++
writing new private key to 'keys\client01.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:client01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'client01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@navigateworx.domain'
Certificate is to be certified until Sep 11 12:05:27 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Setup Private Key Password

Figure 186 – build-key-pass.bat client01 command

In the **build-key-pass.bat client01** command, **client01** is the file name of the certificate (the name of the private key and the public key). **You must use a unique name for each client.**

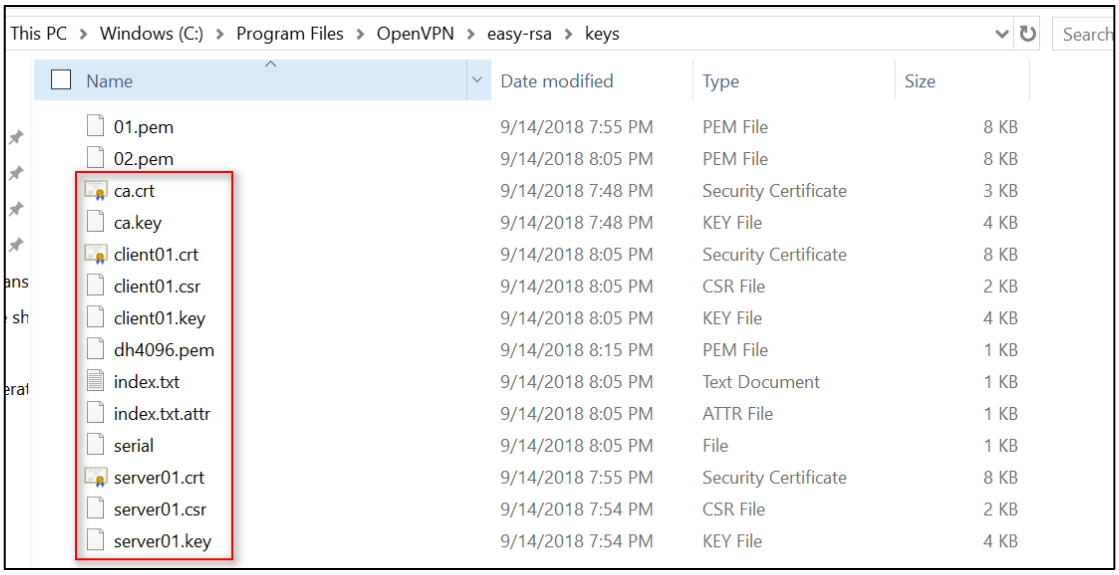
After that, generate Diffie Hellman parameters.



```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating DH parameters, 4096 bit long safe prime, generator 2
This is going to take a long time
..................................................+..............................................
.................................................................................................
.................................................................................................
....+.................+..........................................................................
.................................................................................................
......................................................................+..........................
...+.............................................................................................
.................................................................................................
.......................+.........................................................................
.................................................................................................
.................................................................................................
.................................................................................................
.................................................................................................
.................................................................................................
...............................+.........+..............................+........................
.................................................................................................
.................................................................................................
.................................................................................................
..............................................+..................................................
......................................+..........................................................
..........................++*++*

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 187 – Diffie Hellman parameters

Once the certificates had been generated, you can check them out on path **C:\Program Files\OpenVPN\easy-rsa\keys.**



This PC > Windows (C:) > Program Files > OpenVPN > easy-rsa > keys

Name	Date modified	Type	Size
01.pem	9/14/2018 7:55 PM	PEM File	8 KB
02.pem	9/14/2018 8:05 PM	PEM File	8 KB
ca.crt	9/14/2018 7:48 PM	Security Certificate	3 KB
ca.key	9/14/2018 7:48 PM	KEY File	4 KB
client01.crt	9/14/2018 8:05 PM	Security Certificate	8 KB
client01.csr	9/14/2018 8:05 PM	CSR File	2 KB
client01.key	9/14/2018 8:05 PM	KEY File	4 KB
dh4096.pem	9/14/2018 8:15 PM	PEM File	1 KB
index.txt	9/14/2018 8:05 PM	Text Document	1 KB
index.txt.attr	9/14/2018 8:05 PM	ATTR File	1 KB
serial	9/14/2018 8:05 PM	File	1 KB
server01.crt	9/14/2018 7:55 PM	Security Certificate	8 KB
server01.csr	9/14/2018 7:54 PM	CSR File	2 KB
server01.key	9/14/2018 7:54 PM	KEY File	4 KB

Figure 188 – List of certificates

7.4 OPENVPN WITH X.509 CERTIFICATE

This tutorial shows how to configure OpenVPN with a X.509 certificate.

7.4.1 TOPOLOGY

You can use the following topology:

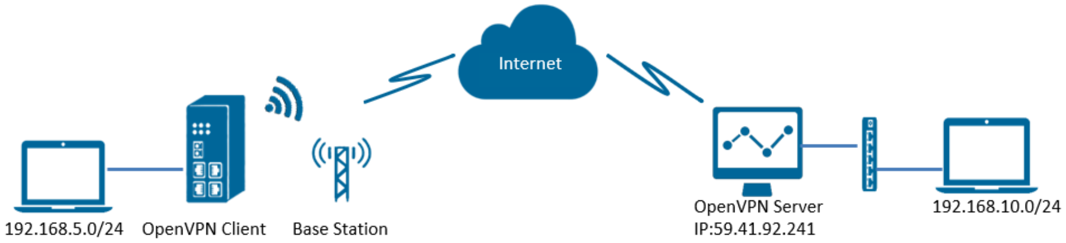


Figure 189 – OpenVPN with X.509 certificate

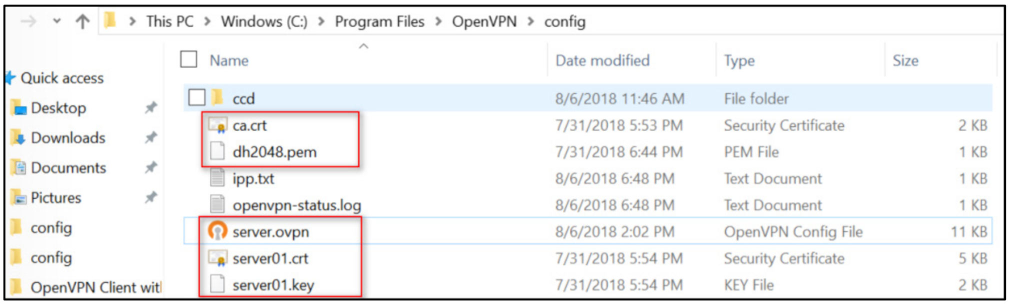
1. **AirGate 4G Wi-Fi** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the subnet can Ping each other successfully.

7.4.2 CONFIGURATION

7.4.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

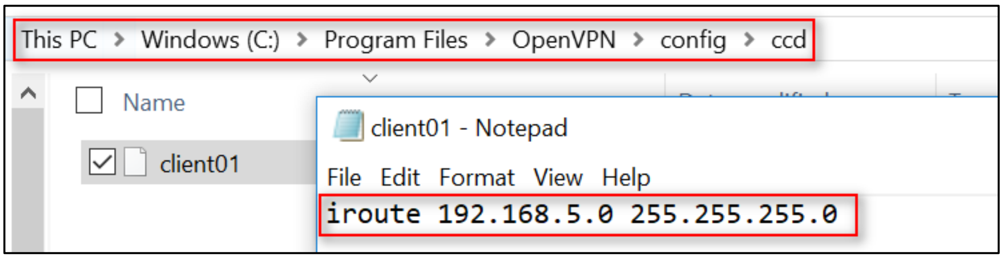
Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:


This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ccd	8/6/2018 11:46 AM	File folder	
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
ipp.txt	8/6/2018 6:48 PM	Text Document	1 KB
openvpn-status.log	8/6/2018 6:48 PM	Text Document	1 KB
server.ovpn	8/6/2018 2:02 PM	OpenVPN Config File	11 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

Figure 190 – OpenVPN configuration

After that, you must create a "ccd" folder, rename it ("client01" is the common name), rename it without suffix and configure it according to figure below:


This PC > Windows (C:) > Program Files > OpenVPN > config > ccd

```
iroute 192.168.5.0 255.255.255.0
```

Figure 191 – Client01 file

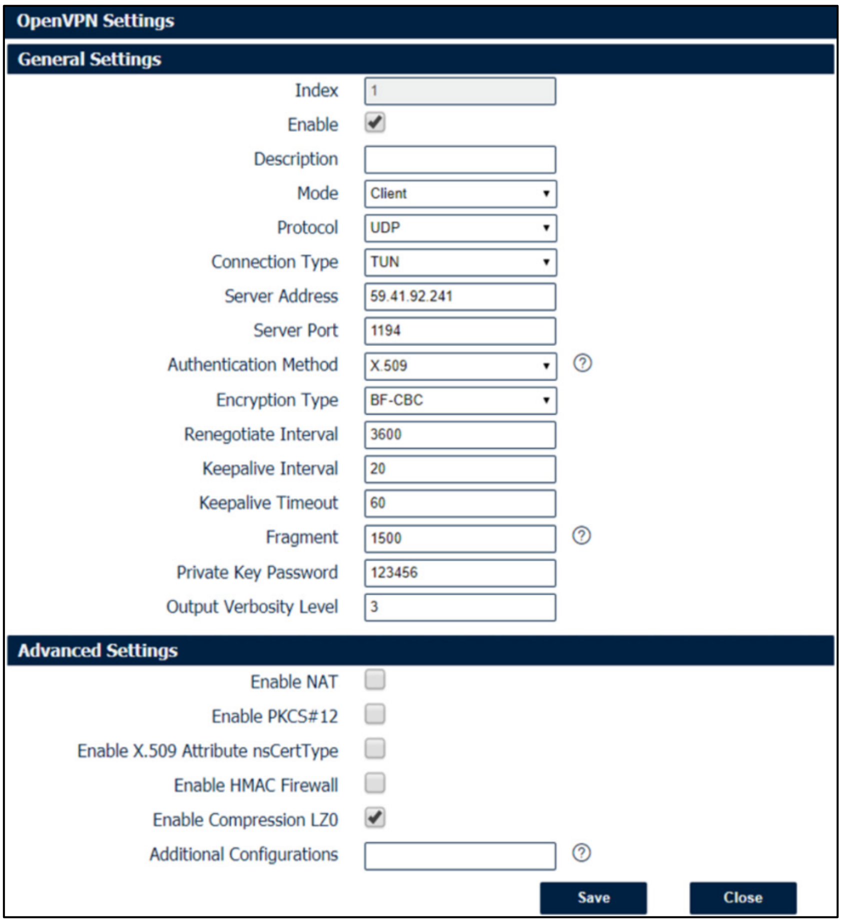
After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key  # This file should be kept secret
```

```
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

7.4.2.2 CLIENT CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

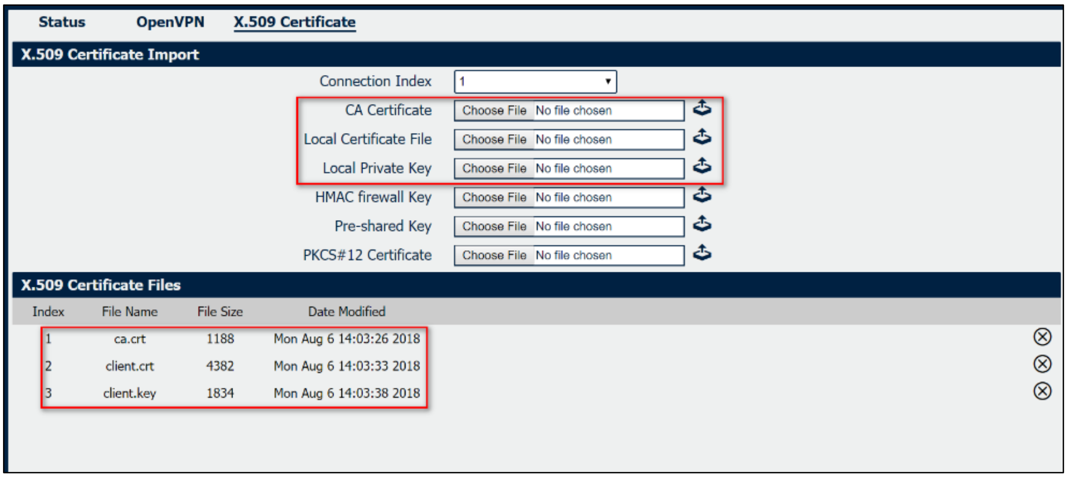
Advanced Settings

Enable NAT	□
Enable PKCS#12	□
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZO	☑
Additional Configurations	

Figure 192 – OpenVPN configuration

Click **Save > Apply**.

Once you have set up OpenVPN, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

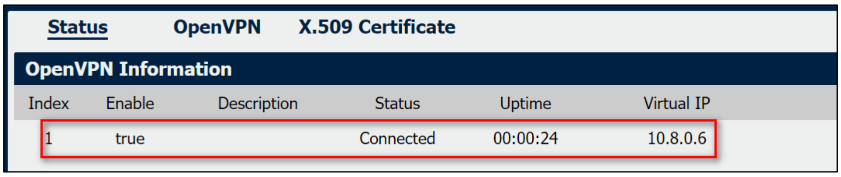
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified	
1	ca.crt	1188	Mon Aug 6 14:03:26 2018	⊗
2	client.crt	4382	Mon Aug 6 14:03:33 2018	⊗
3	client.key	1834	Mon Aug 6 14:03:38 2018	⊗

Figure 193 – Certificate import

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



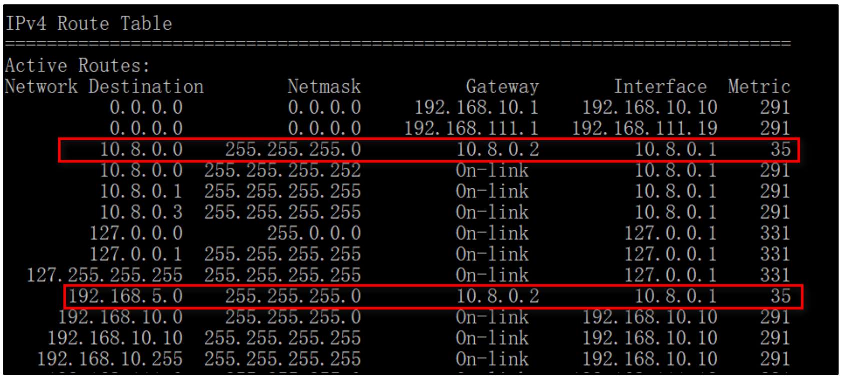
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:24	10.8.0.6

Figure 194 – OpenVPN connection status

7.4.3 ROUTE TABLE

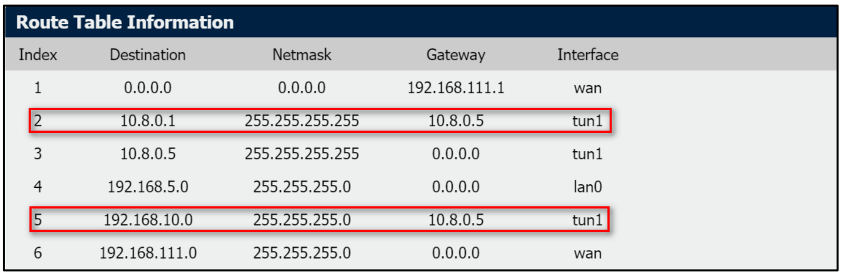
Figure below shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.8.0.0    255.255.255.0         10.8.0.2         10.8.0.1     35
         10.8.0.0  255.255.255.252          On-link         10.8.0.1    291
         10.8.0.1  255.255.255.255          On-link         10.8.0.1    291
         10.8.0.3  255.255.255.255          On-link         10.8.0.1    291
        127.0.0.0        255.0.0.0          On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link        127.0.0.1    331
      192.168.5.0    255.255.255.0         10.8.0.2         10.8.0.1     35
     192.168.10.0    255.255.255.0          On-link    192.168.10.10    291
    192.168.10.10  255.255.255.255          On-link    192.168.10.10    291
   192.168.10.255  255.255.255.255          On-link    192.168.10.10    291
```

Figure 195 – Route table of OpenVPN server

Figure below shows a route table of the OpenVPN client for reference:



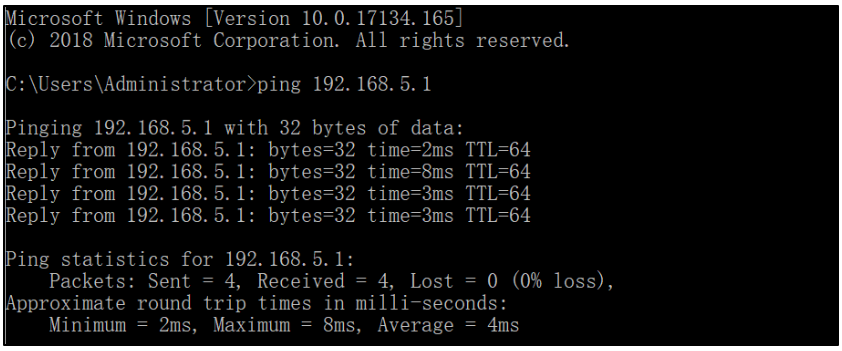
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.10.0	255.255.255.0	10.8.0.5	tun1
6	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 196 – Route table of OpenVPN client

7.4.4 TEST

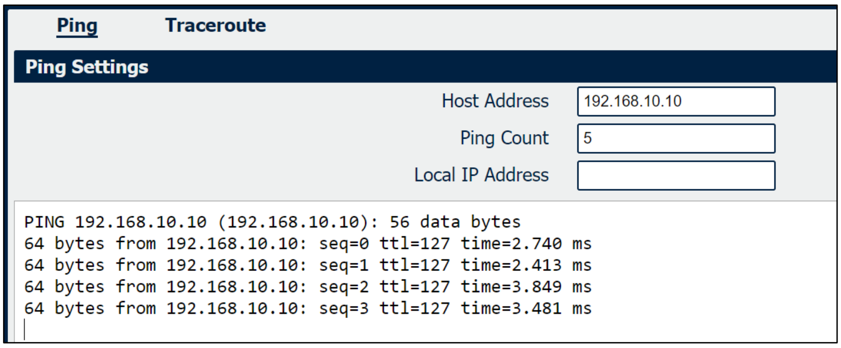
To perform a test, you must enable CMD and Ping from OpenVPN Server to LAN of OpenVPN client.



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=2ms TTL=64
Reply from 192.168.5.1: bytes=32 time=8ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

Figure 197 – Prompt

After that, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from OpenVPN client to OpenVPN Server.



Ping Settings

Host Address: 192.168.10.10

Ping Count: 5

Local IP Address:

```
PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: seq=0 ttl=127 time=2.740 ms
64 bytes from 192.168.10.10: seq=1 ttl=127 time=2.413 ms
64 bytes from 192.168.10.10: seq=2 ttl=127 time=3.849 ms
64 bytes from 192.168.10.10: seq=3 ttl=127 time=3.481 ms
```

Figure 198 – Ping

Test successfully.

7.5 OPENVPN CLIENT WITH PRE-SHARED KEY

This tutorial shows how to configure OpenVPN with a pre-shared key.

7.5.1 TOPOLOGY

You can use the following topology:

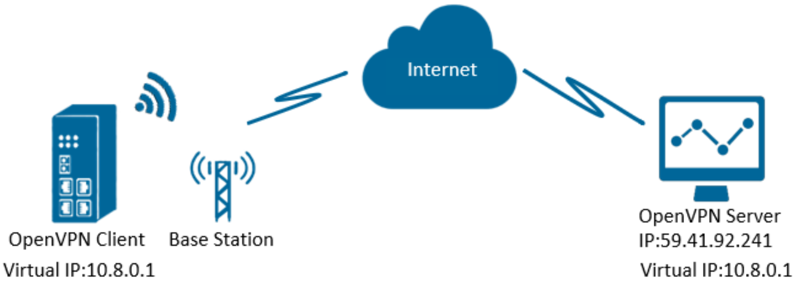


Figure 199 – OpenVPN with pre-shared key

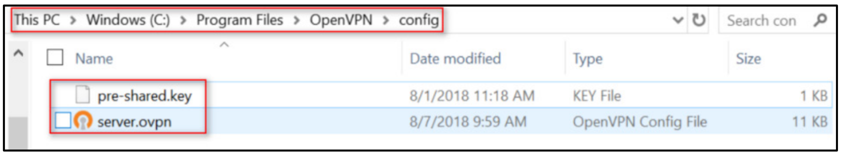
1. **AirGate 4G Wi-Fi** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. This is a point-to-point application.

7.5.2 CONFIGURATION

7.5.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Search con

Name	Date modified	Type	Size
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB
server.ovpn	8/7/2018 9:59 AM	OpenVPN Config File	11 KB

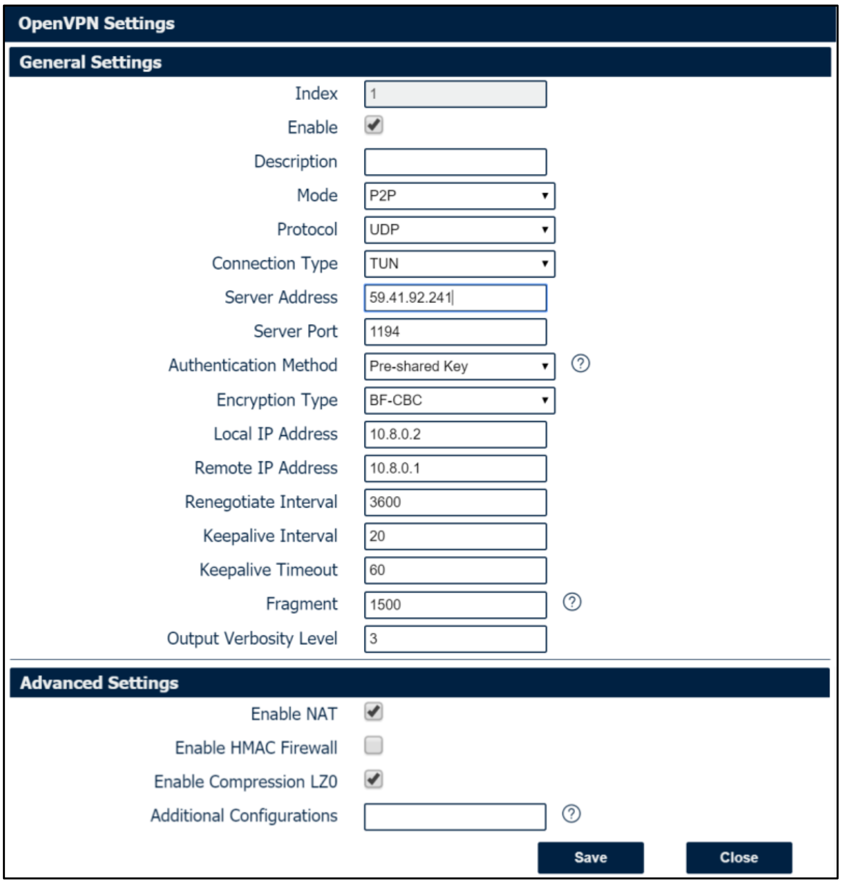
Figure 200 – OpenVPN folder

After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
proto udp
dev tun
tun-mtu 1500
fragment 1500
ifconfig 10.8.0.1 10.8.0.2
keepalive 10 120
secret pre-shared.key
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

7.5.2.2 CLIENT CONFIGURATION

To configure a PC as a client, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

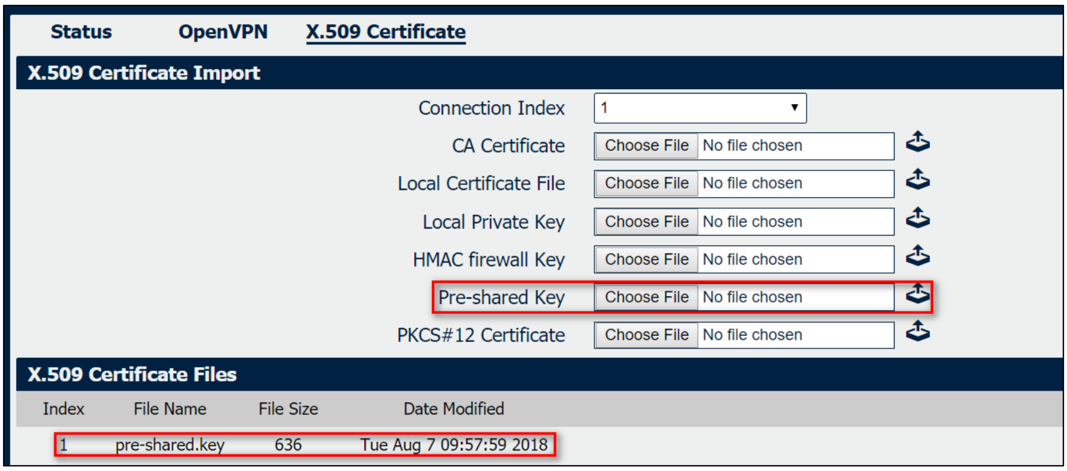
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

Figure 201 – OpenVPN settings

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

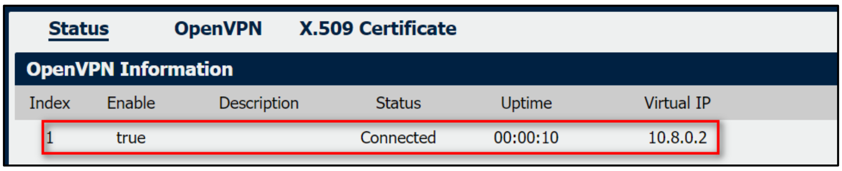
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	pre-shared.key	636	Tue Aug 7 09:57:59 2018

Figure 202 – Pre-shared key

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



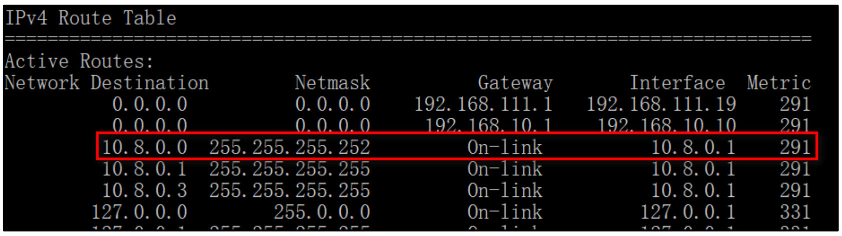
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:10	10.8.0.2

Figure 203 – OpenVPN status connection

7.5.3 ROUTE TABLE

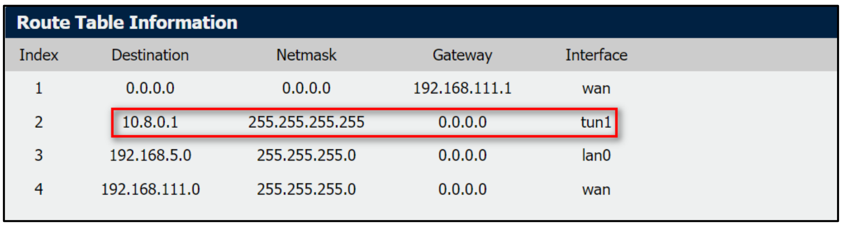
Figure below shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1  192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10    291
         10.8.0.0  255.255.255.252         On-link         10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link         10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link         10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
```

Figure 204 – Server route table information

Figure below shows a route table of the OpenVPN client for reference:



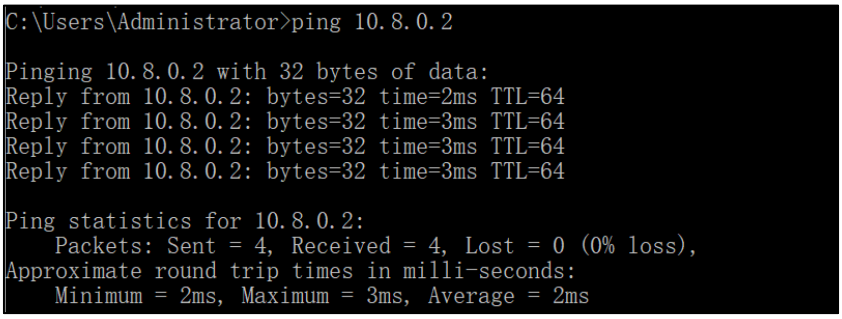
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 205 – Client route table information

7.5.4 TEST

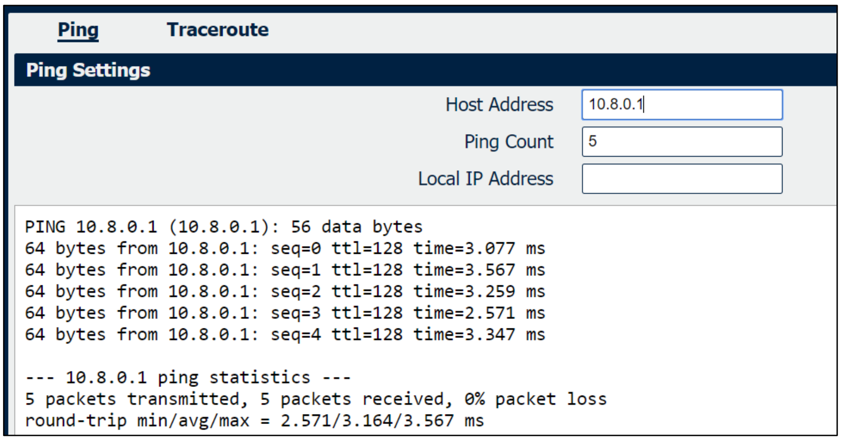
To perform a test, you must enable CMD and Ping from OpenVPN Server to LAN of OpenVPN client.



```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 206 – CMD

After that, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from OpenVPN client to OpenVPN Server.



Ping Settings

Host Address: 10.8.0.1

Ping Count: 5

Local IP Address:

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=3.077 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.567 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=3.259 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=2.571 ms
64 bytes from 10.8.0.1: seq=4 ttl=128 time=3.347 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.571/3.164/3.567 ms
```

Figure 207 – Ping

Test successfully.

.

7.6 OPENVPN CLIENT WITH USERNAME AND PASSWORD

This tutorial shows how to configure OpenVPN with a username and password.

7.6.1 TOPOLOGY

You can use the following topology:

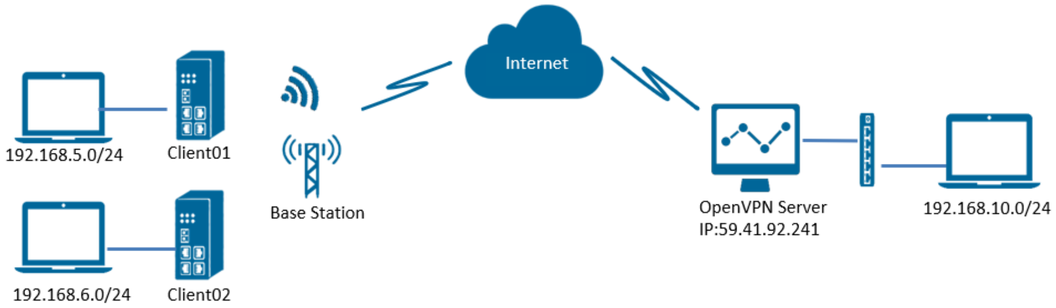


Figure 208 – OpenVPN with username and password

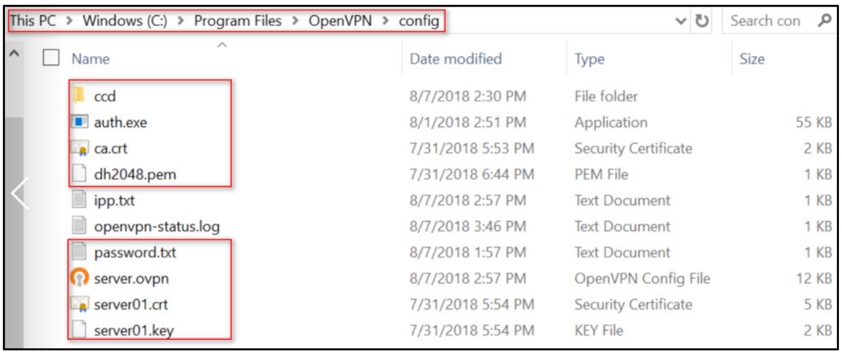
1. Two **AirGate 4G Wi-Fi** run as OpenVPN Client01 and Client02 with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client. Client01 can ping Client02 successfully and vice versa.

7.6.2 CONFIGURATION

7.6.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:

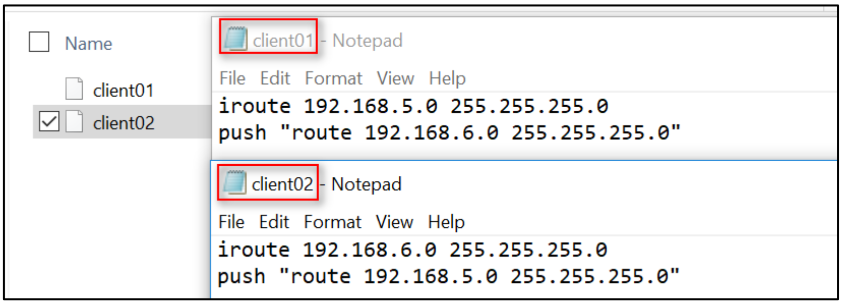


This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ccd	8/7/2018 2:30 PM	File folder	
auth.exe	8/1/2018 2:51 PM	Application	55 KB
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
ipp.txt	8/7/2018 2:57 PM	Text Document	1 KB
openvpn-status.log	8/7/2018 3:46 PM	Text Document	1 KB
password.txt	8/7/2018 1:57 PM	Text Document	1 KB
server.ovpn	8/7/2018 2:57 PM	OpenVPN Config File	12 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

Figure 209 – OpenVPN folders

After that, two new notepads must be created inside the "ccd" folder, renamed it without suffix (using the default names "client01" and "client02") and configured according to figure below:



☐ Name

client01

☑ client02

client01 - Notepad

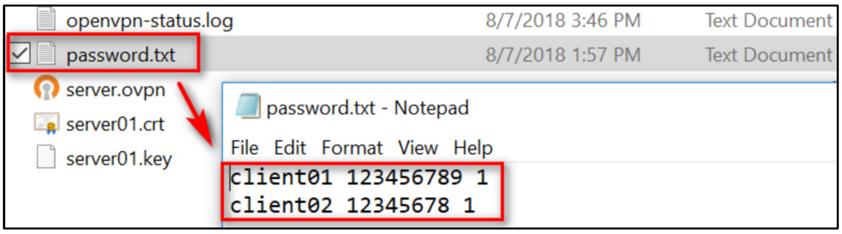
```
iroute 192.168.5.0 255.255.255.0
push "route 192.168.6.0 255.255.255.0"
```

client02 - Notepad

```
iroute 192.168.6.0 255.255.255.0
push "route 192.168.5.0 255.255.255.0"
```

Figure 210 – Client01 and client02 configuration files

It will also be necessary to create a "password.txt" file, which will include the contents of figure below, presented as follows: **common name > password > 1 or 0 (1 = enable / 0 = disable)**.



openvpn-status.log 8/7/2018 3:46 PM Text Document
password.txt 8/7/2018 1:57 PM Text Document
server.ovpn
server01.crt
server01.key

password.txt - Notepad

```
client01 123456789 1
client02 12345678 1
```

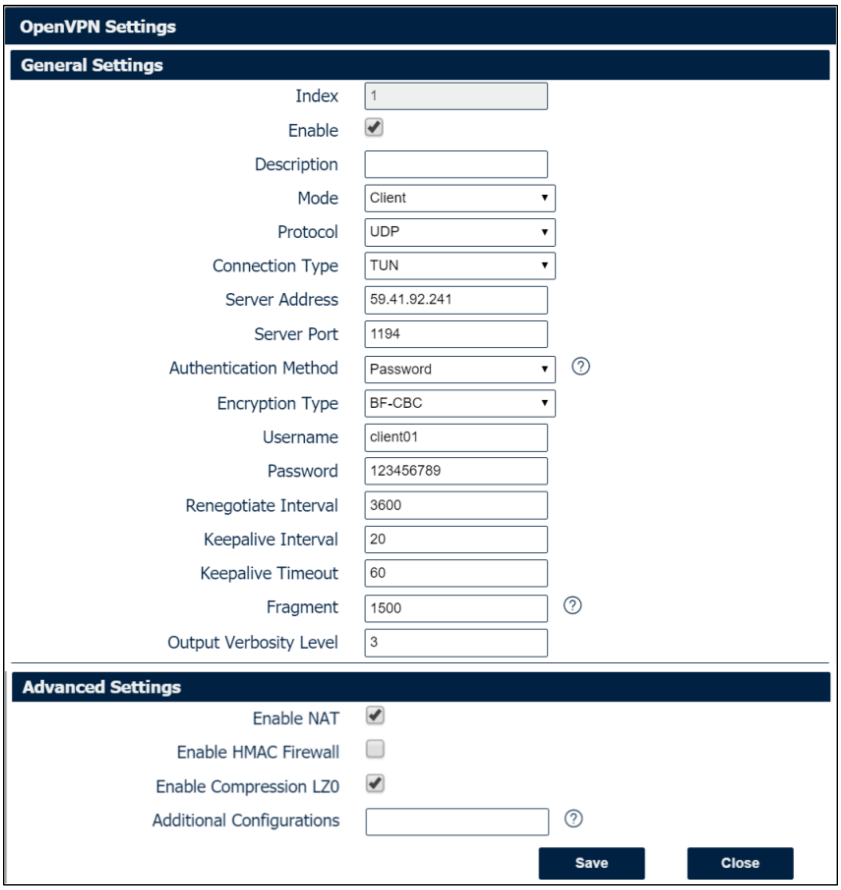
Figure 211 – Password configuration

After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
mode server
port 1194
proto udp
client-cert-not-required
username-as-common-name
auth-user-pass-verify auth.exe via-env
script-security 3 system
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key  # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
route 192.168.6.0 255.255.255.0
client-to-client
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

7.6.2.2 CLIENT01 CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Client ▾
Protocol	UDP ▾
Connection Type	TUN ▾
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Password ▾
Encryption Type	BF-CBC ▾
Username	client01
Password	123456789
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

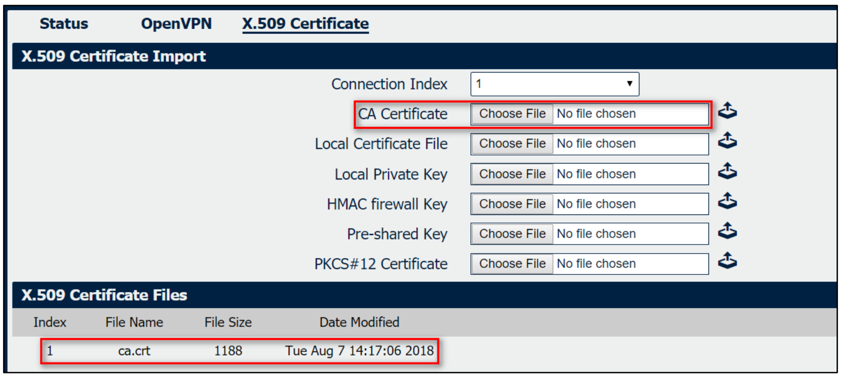
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	☐
Enable Compression LZO	☑
Additional Configurations	

Figure 212 – OpenVPN configuration

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

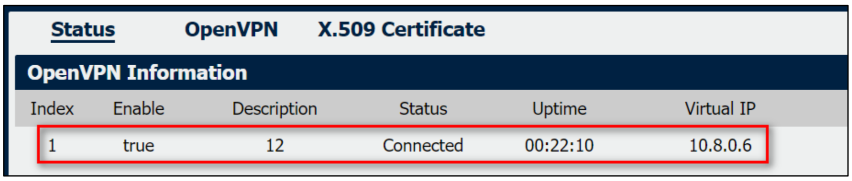
Connection Index	1 ▾
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 14:17:06 2018

Figure 213 – CA certificate import

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



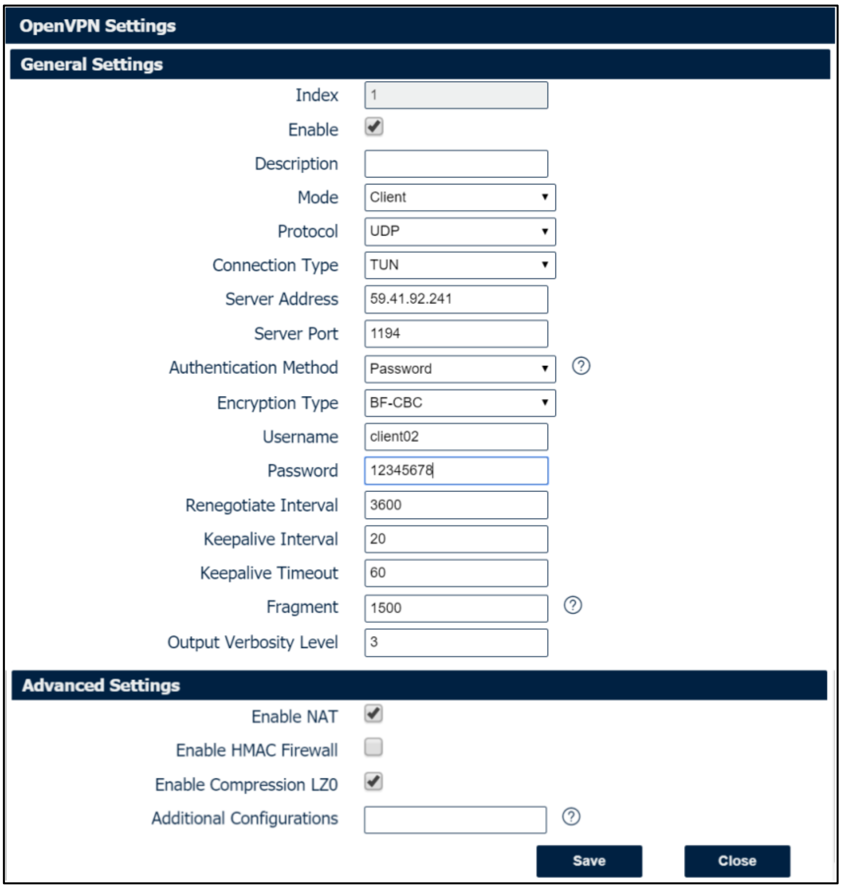
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	12	Connected	00:22:10	10.8.0.6

Figure 214 – OpenVPN status connection

7.6.2.3 CLIENT02 CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Password
Encryption Type	BF-CBC
Username	client02
Password	12345678
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

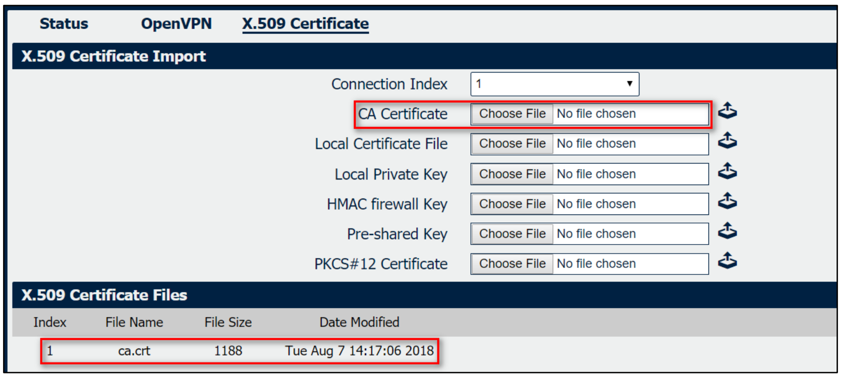
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	☐
Enable Compression LZ0	☑
Additional Configurations	

Figure 215 – OpenVPN configuration

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

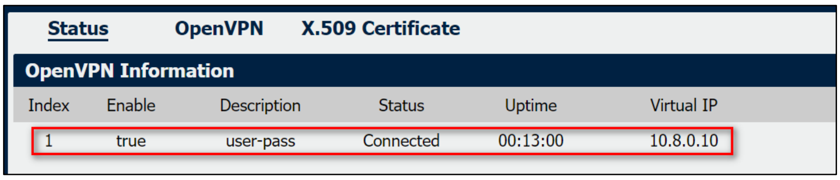
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 14:17:06 2018

Figure 216 – X.509 certificate: CA certificate

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



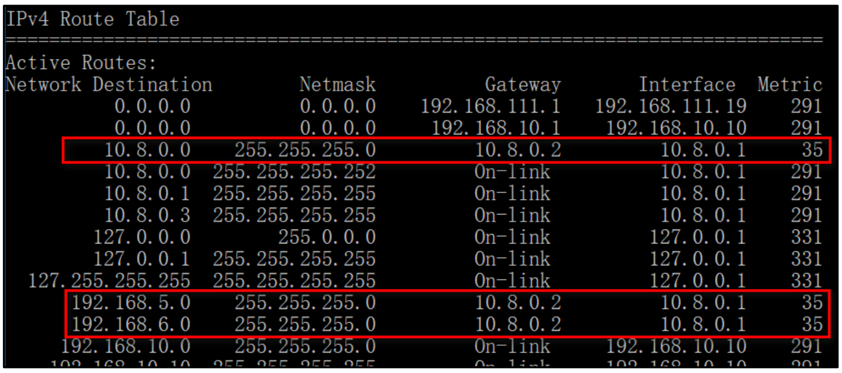
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	user-pass	Connected	00:13:00	10.8.0.10

Figure 217 – OpenVPN connection status

7.6.3 ROUTE TABLE

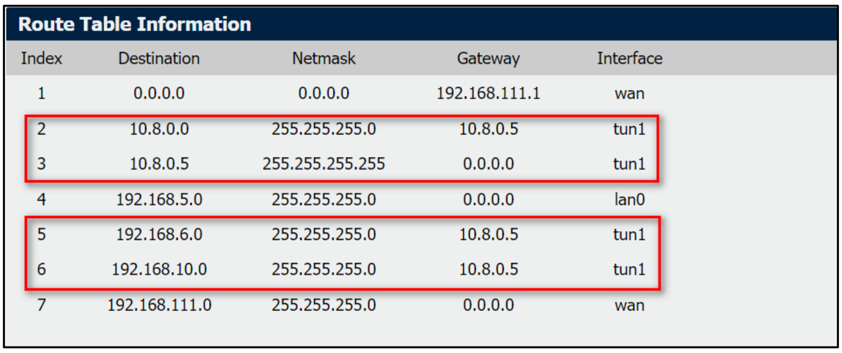
Figure below shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
         10.8.0.0    255.255.255.0         10.8.0.2         10.8.0.1     35
         10.8.0.0  255.255.255.252         On-link          10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link          10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link          10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.5.0    255.255.255.0         10.8.0.2         10.8.0.1     35
      192.168.6.0    255.255.255.0         10.8.0.2         10.8.0.1     35
     192.168.10.0    255.255.255.0         On-link     192.168.10.10    291
    192.168.10.10  255.255.255.255         On-link     192.168.10.10    291
```

Figure 218 – OpenVPN server route table

Figure below shows a route table of the Client01 for reference:

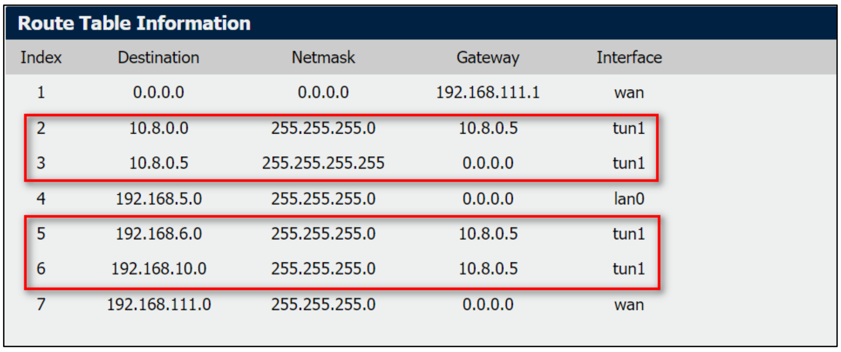


Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 219 – Client01 route table

Figure below shows a route table of the Client02 for reference:



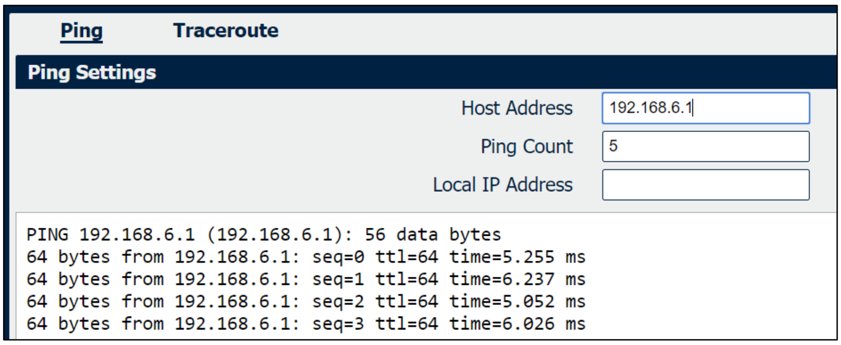
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 220 – Client02 route table

7.6.4 TEST

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and ping from Client01 to Cliente02:



Ping Settings

Host Address: 192.168.6.1

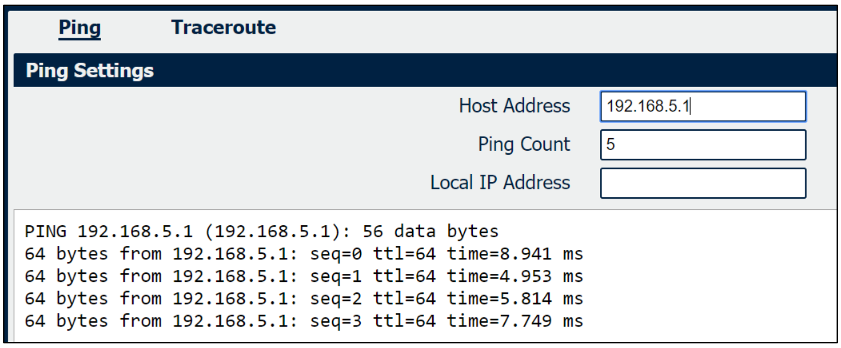
Ping Count: 5

Local IP Address:

```
PING 192.168.6.1 (192.168.6.1): 56 data bytes
64 bytes from 192.168.6.1: seq=0 ttl=64 time=5.255 ms
64 bytes from 192.168.6.1: seq=1 ttl=64 time=6.237 ms
64 bytes from 192.168.6.1: seq=2 ttl=64 time=5.052 ms
64 bytes from 192.168.6.1: seq=3 ttl=64 time=6.026 ms
```

Figure 221 – Ping from Client01 to Client02

After that, Ping from Client02 to Cliente01 as below:



Host Address: 192.168.5.1

Ping Count: 5

Local IP Address:

```
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: seq=0 ttl=64 time=8.941 ms
64 bytes from 192.168.5.1: seq=1 ttl=64 time=4.953 ms
64 bytes from 192.168.5.1: seq=2 ttl=64 time=5.814 ms
64 bytes from 192.168.5.1: seq=3 ttl=64 time=7.749 ms
```

Figure 222 – Ping from Client02 to Client01

Test successfully.

7.7 OPENPNV WITH TAP AND PRE-SHARED KEY UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TAP and pre-shared key under P2P mode.

7.7.1 TOPOLOGY

You can use the following topology:

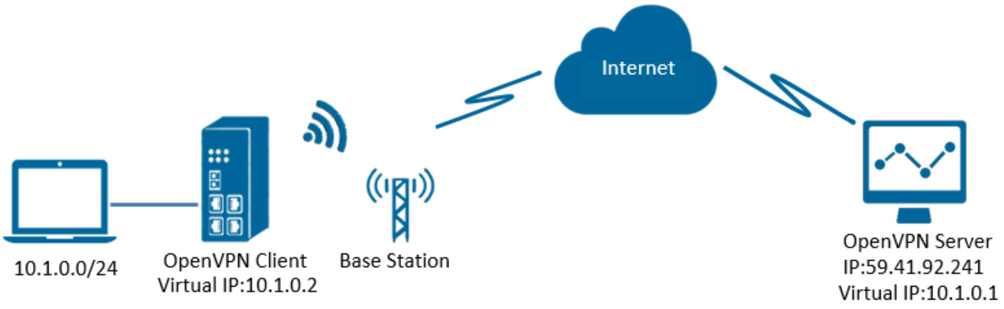


Figure 223 – OpenVPN with TAP and pre-shared key

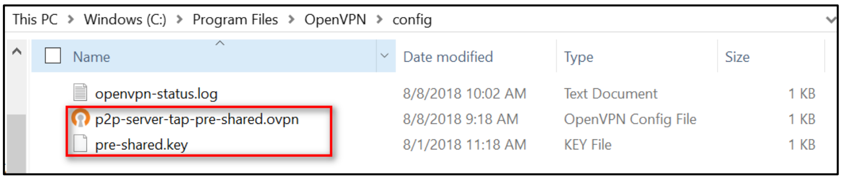
1. **AirGate 4G Wi-Fi** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. Also, server can Ping LAN PC device and vice versa.

7.7.2 CONFIGURATION

7.7.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:


This PC › Windows (C:) › Program Files › OpenVPN › config

Name	Date modified	Type	Size
openvpn-status.log	8/8/2018 10:02 AM	Text Document	1 KB
p2p-server-tap-pre-shared.ovpn	8/8/2018 9:18 AM	OpenVPN Config File	1 KB
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB

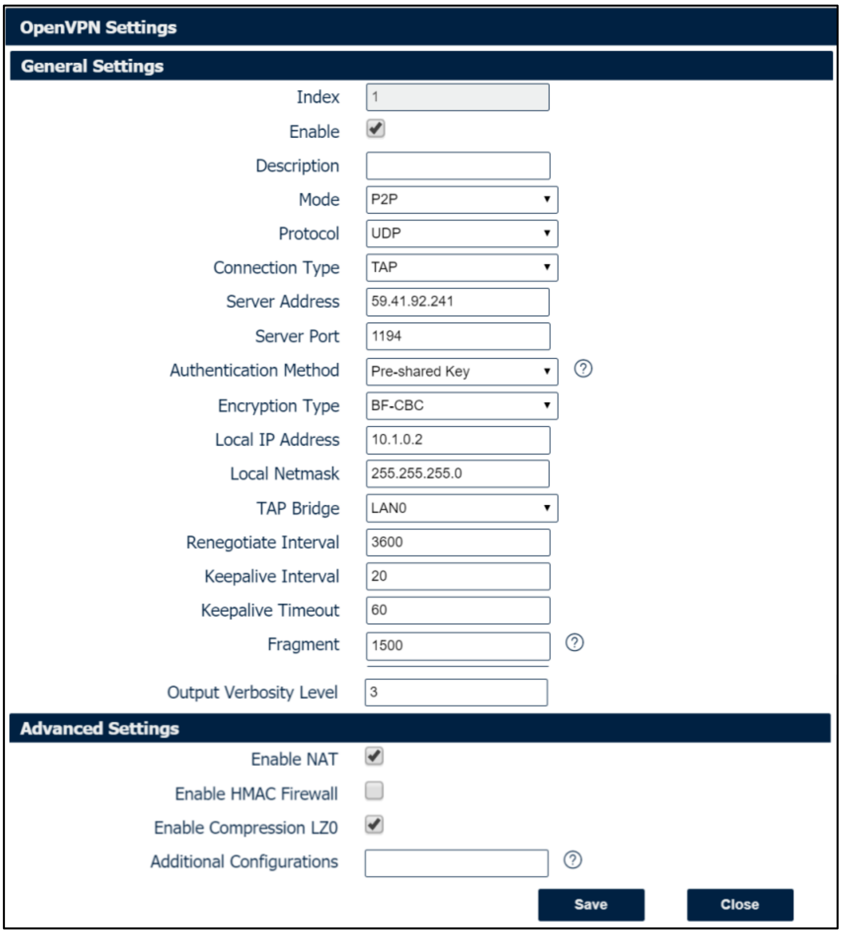
Figure 224 – OpenVPN folder

After that, just run the file **p2p-server-tap-pre-shared.ovpn** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
secret pre-shared.key   # None TLS Mode
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

7.7.2.2 CLIENT CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN** > **OpenVPN** > **OpenVPN** > **General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TAP
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC
Local IP Address	10.1.0.2
Local Netmask	255.255.255.0
TAP Bridge	LAN0
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

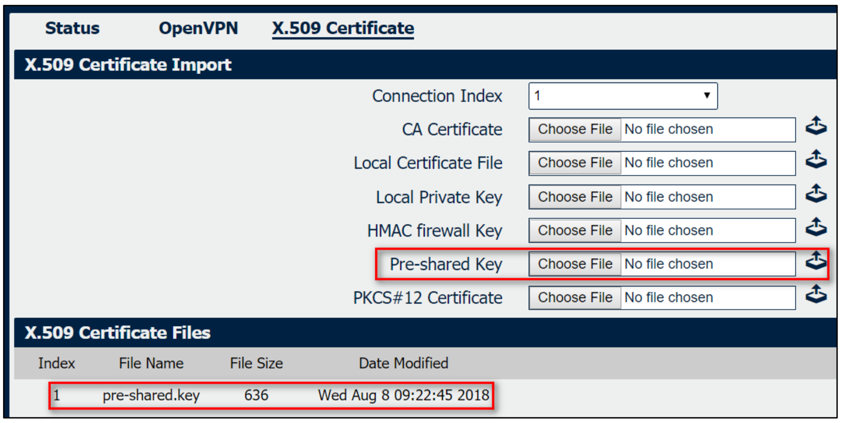
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	☐
Enable Compression LZ0	☑
Additional Configurations	

Figure 225 – OpenVPN settings

Click **Save** > **Apply**.

After that, go to **VPN** > **OpenVPN** > **X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

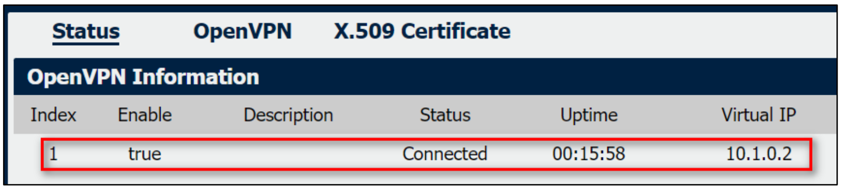
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	pre-shared.key	636	Wed Aug 8 09:22:45 2018

Figure 226 – Pre-shared key

Route had connected to OpenVPN server. Go to **VPN** > **OpenVPN** > **Status** to check the connection status.



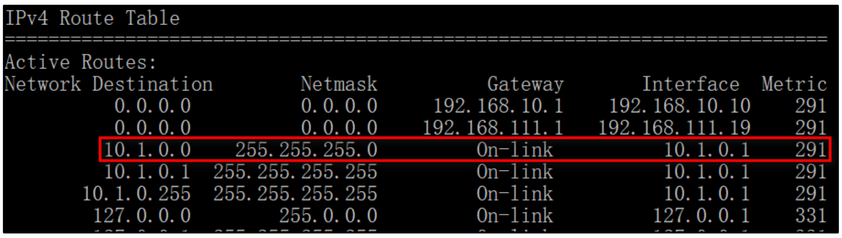
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:15:58	10.1.0.2

Figure 227 – OpenVPN connection status

7.7.3 ROUTE TABLE

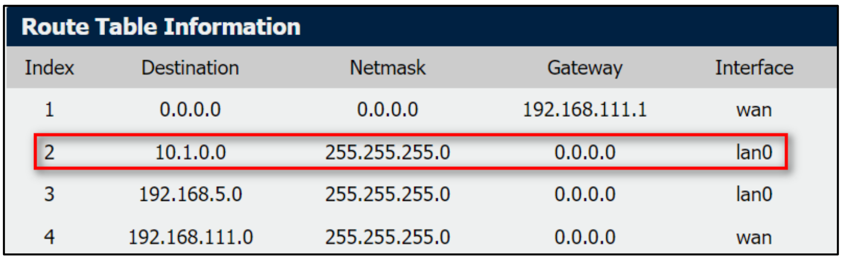
Figure below shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1    291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1    291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Figure 228 – OpenVPN server route table

Figure below shows a route table of the client for reference:



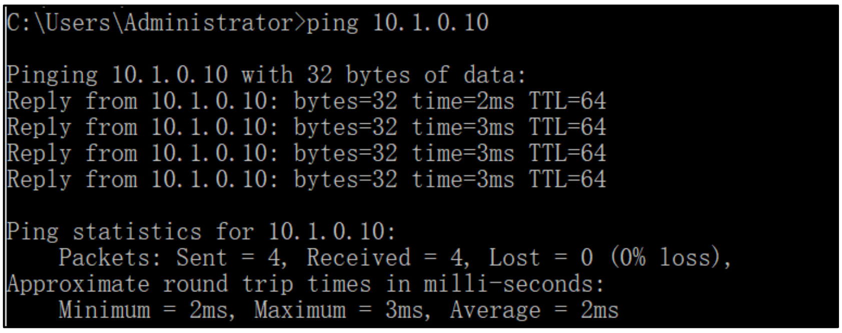
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 229 – Client route table

7.7.4 TEST

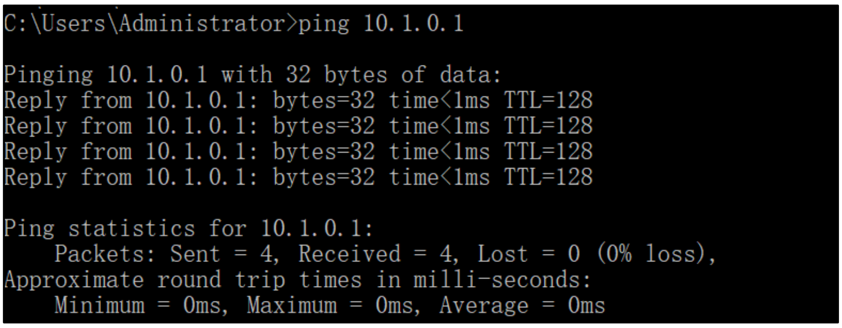
Enable CMD and Ping from PC to the LAN device of the router.



```
C:\Users\Administrator>ping 10.1.0.10

Pinging 10.1.0.10 with 32 bytes of data:
Reply from 10.1.0.10: bytes=32 time=2ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64

Ping statistics for 10.1.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 230 – CMD

After that, Ping from LAN device of the router to PC.



```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 231 – Ping

Test successfully.

7.8 OPENVPN WITH TAP UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TAP and under P2P mode.

7.8.1 TOPOLOGY

You can use the following topology:

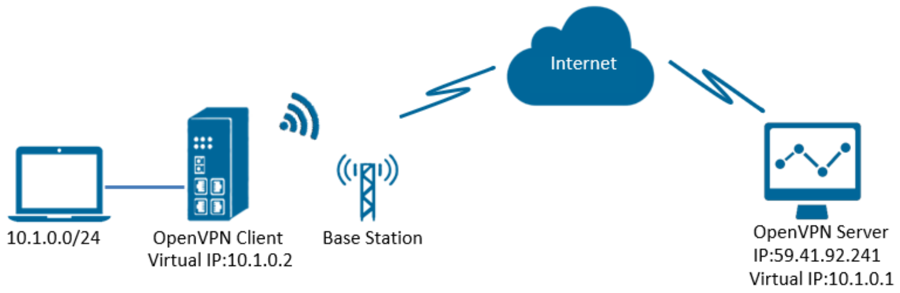


Figure 232 – OpenVPN with TAP under P2P

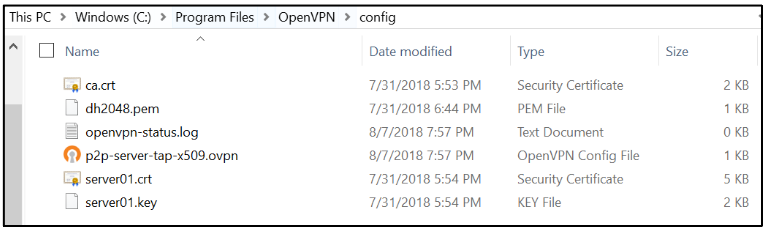
1. **AirGate 4G Wi-Fi** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. Also, Server can ping LAN PC device and vice versa.

7.8.2 CONFIGURATION

7.8.2.1 PC CONFIGURATION

To configure the computer, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB
p2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

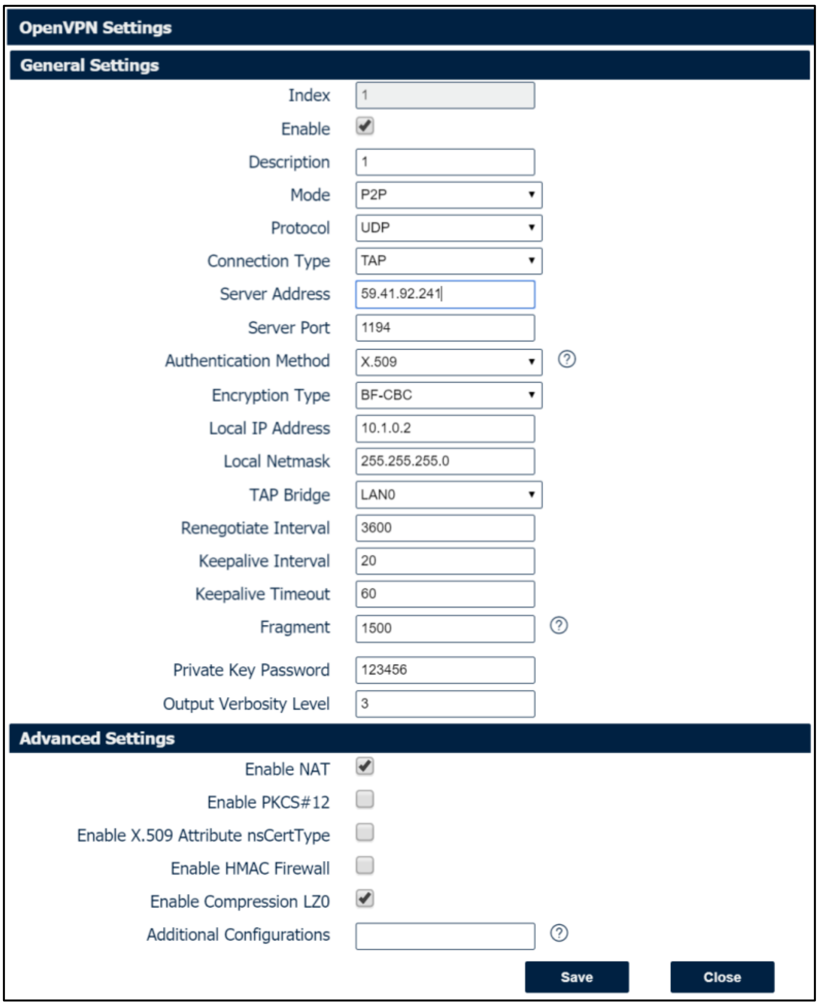
Figure 233 – OpenVPN configuration

After that, just run the file **p2p-server-tap-x.509.ovpn** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
```

7.8.2.2 ROUTER CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN** > **OpenVPN** > **OpenVPN** > **General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	1
Mode	P2P
Protocol	UDP
Connection Type	TAP
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Local IP Address	10.1.0.2
Local Netmask	255.255.255.0
TAP Bridge	LAN0
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

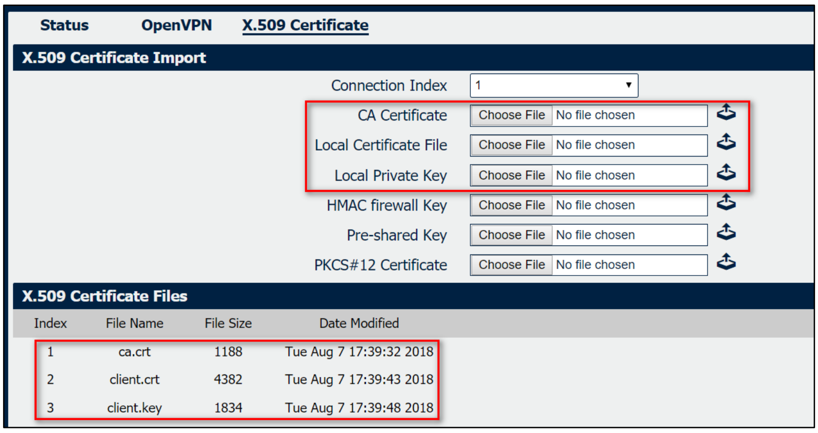
Advanced Settings

Enable NAT	☑
Enable PKCS#12	□
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZO	☑
Additional Configurations	

Figure 234 – OpenVPN configuration

Click **Save** > **Apply**.

After that, go to **VPN** > **OpenVPN** > **X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

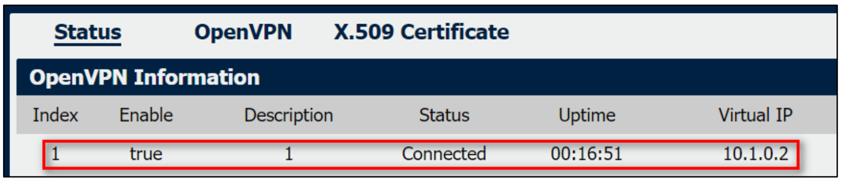
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 17:39:32 2018
2	client.crt	4382	Tue Aug 7 17:39:43 2018
3	client.key	1834	Tue Aug 7 17:39:48 2018

Figure 235 – X.509 certificates

Route had connected to OpenVPN server. Go to **VPN** > **OpenVPN** > **Status** to check the connection status.



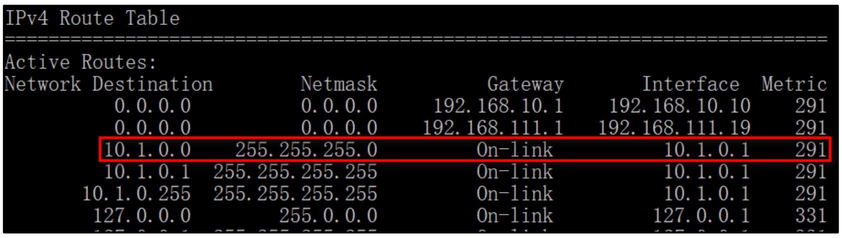
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	1	Connected	00:16:51	10.1.0.2

Figure 236 – OpenVPN status connection

7.8.3 ROUTE TABLE

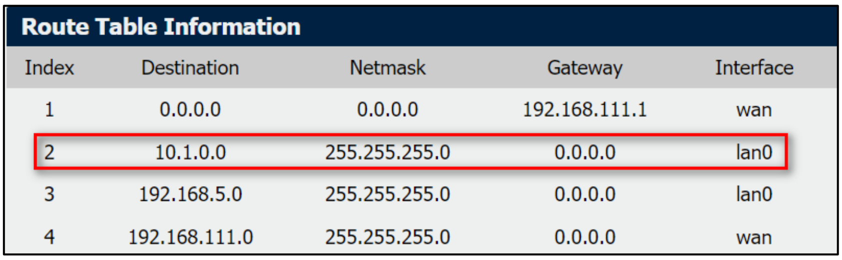
Figure below shows a route table of the PC for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1    291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1    291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Figure 237 – PC route table

Figure below shows a route table of the router for reference:



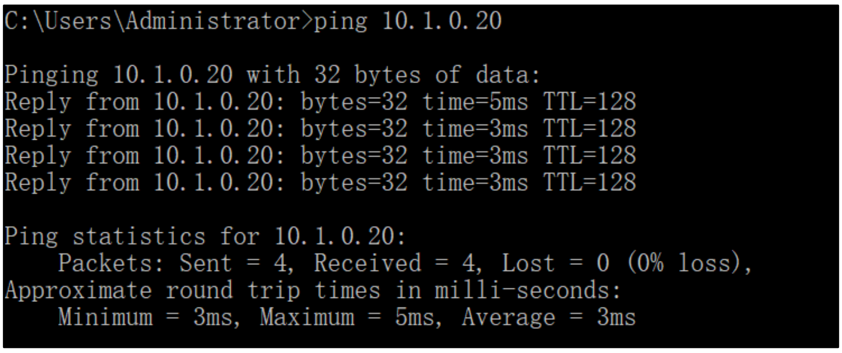
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 238 – Router table

7.8.4 TEST

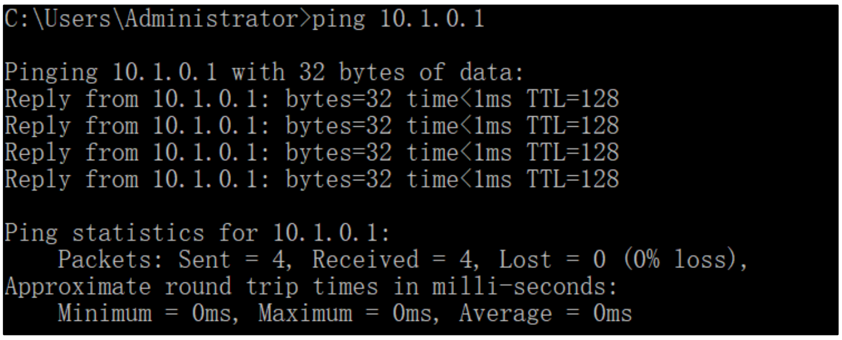
Enable CMD and Ping from PC side to LAN device of router.



```
C:\Users\Administrator>ping 10.1.0.20

Pinging 10.1.0.20 with 32 bytes of data:
Reply from 10.1.0.20: bytes=32 time=5ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128

Ping statistics for 10.1.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

Figure 239 – CMD

After that, ping from LAN device of router to PC side.



```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 240 – Ping

Test successfully.

7.9 OPENVPN WITH TUN CERTIFICATE UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TUN and under P2P mode.

7.9.1 TOPOLOGY

You can use the following topology:

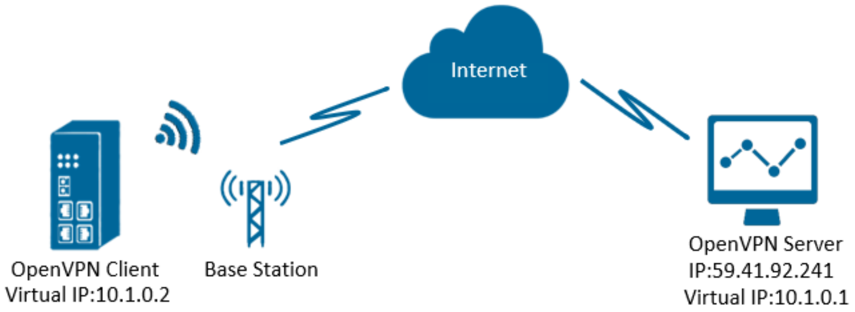


Figure 241 – OpenVPN with TUN under P2P mode

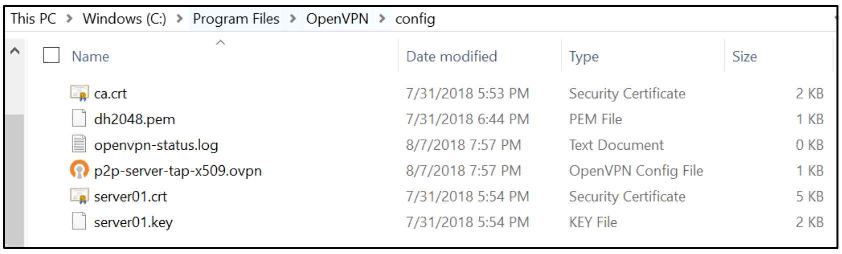
1. **AirGate 4G Wi-Fi** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can Ping each other successfully.

7.9.2 CONFIGURATION

7.9.2.1 PC CONFIGURATION

To configure the computer, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:


This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB
p2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

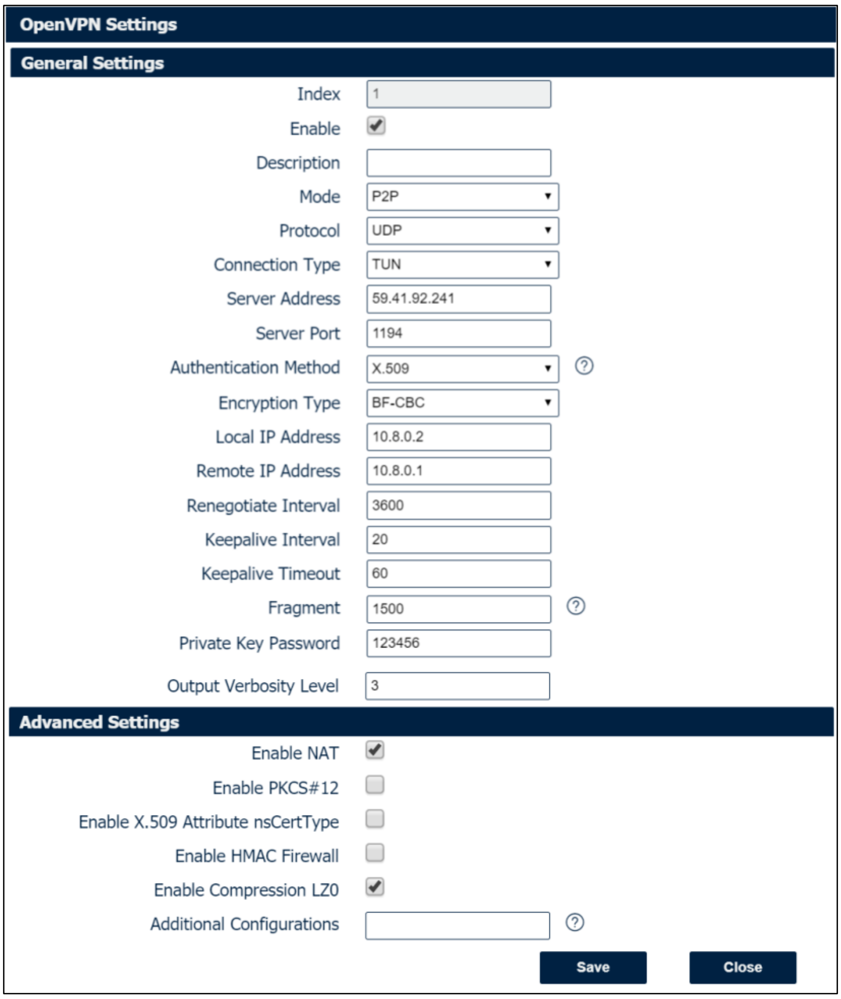
Figure 242 – OpenVPN configuration

After that, just run the file **p2p-server-tun-x.509** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tun
# tun
ifconfig 10.8.0.1 10.8.0.2
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

7.9.2.2 ROUTER CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

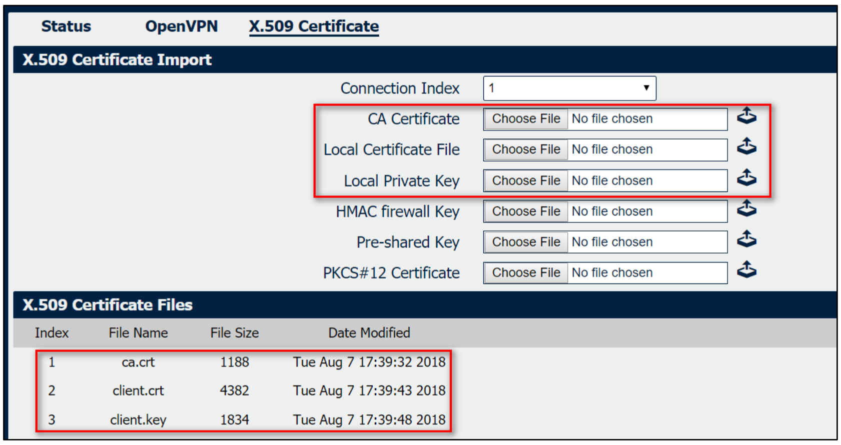
Advanced Settings

Enable NAT	☑
Enable PKCS#12	☐
Enable X.509 Attribute nsCertType	☐
Enable HMAC Firewall	☐
Enable Compression LZ0	☑
Additional Configurations	

Figure 243 – OpenVPN settings

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

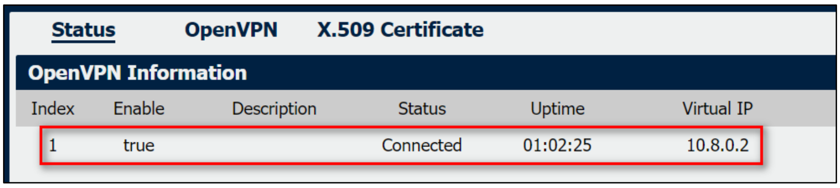
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 17:39:32 2018
2	client.crt	4382	Tue Aug 7 17:39:43 2018
3	client.key	1834	Tue Aug 7 17:39:48 2018

Figure 244 – Certificate import

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



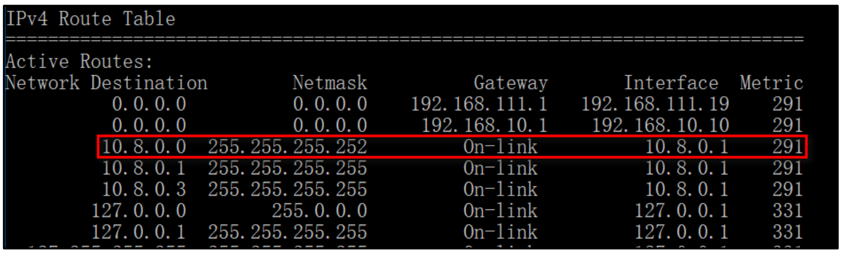
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	01:02:25	10.8.0.2

Figure 245 – OpenVPN status connection

7.9.3 ROUTE TABLE

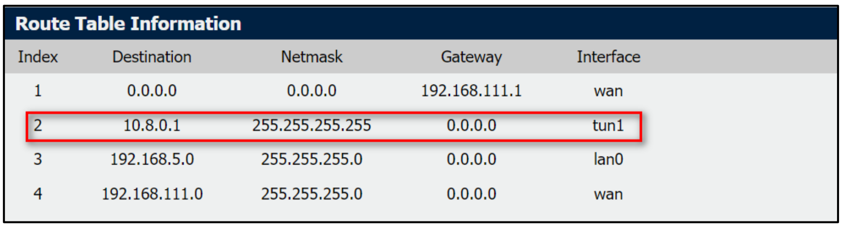
Figure below shows a route table of the PC for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1  192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10    291
         10.8.0.0  255.255.255.252         On-link          10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link          10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link          10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
```

Figure 246 – PC route table

Figure below shows a route table of the router for reference:



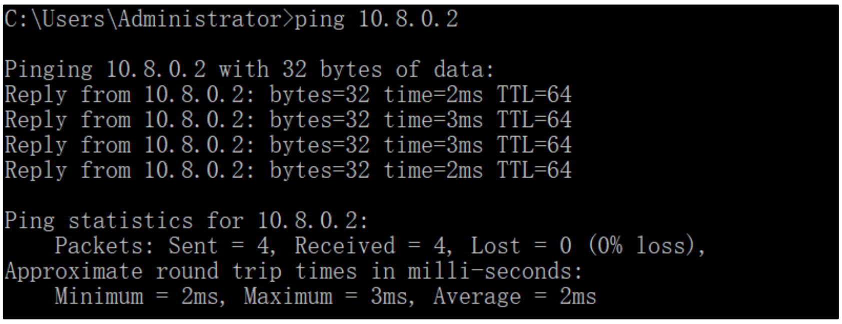
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 247 – Route table

7.9.4 TEST

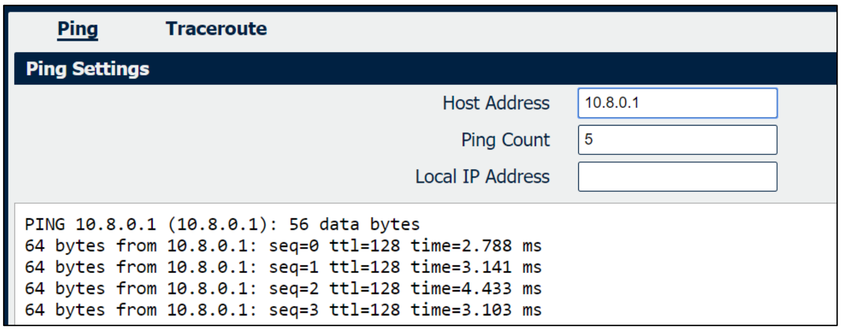
Enable CMD and Ping from PC side to router side.



```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 248 – CMD

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from router side to PC side.



Ping Settings

Host Address	10.8.0.1
Ping Count	5
Local IP Address	

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=2.788 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.141 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=4.433 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=3.103 ms
```

Figure 249 – Ping

Test successfully.

7.10 IPSEC: PRE-SHARED KEY WITH CISCO ROUTER

This tutorial shows how to configure IPsec with pre-shared key with Cisco router.

7.10.1 TOPOLOGY

You can use the following topology:

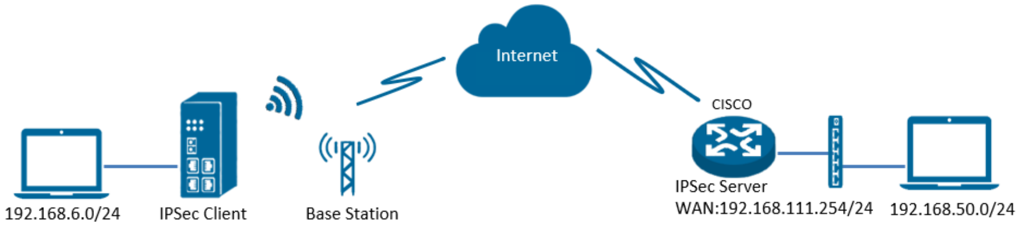


Figure 250 – IPsec topology

1. **AirGate 4G Wi-Fi** runs as IPsec Client with any kind of IP, which can ping IPsec server IP successfully.
2. Cisco router runs as IPsec Server with a static public IP.
3. IPsec tunnel is established between **AirGate 4G Wi-Fi** and Cisco router.

7.10.2 CONFIGURATION

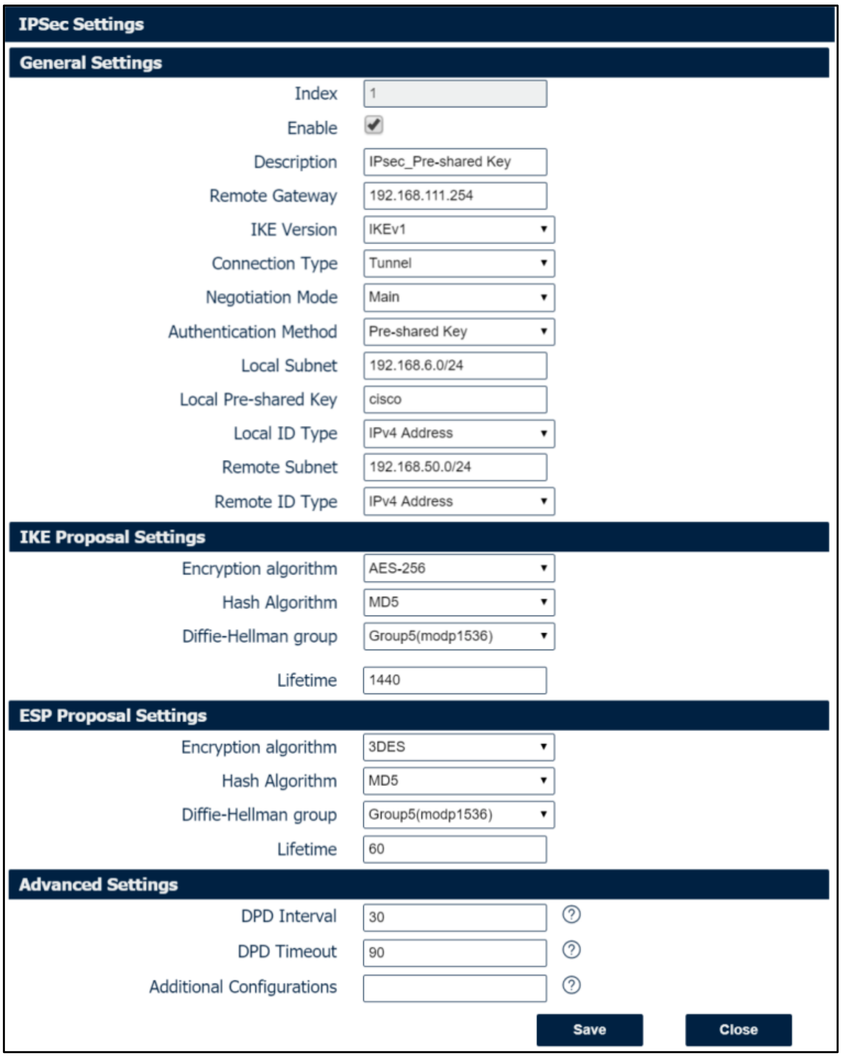
7.10.2.1 SERVER CONFIGURATION

Login to Cisco router and setting like below:

```
cisco2811#show running-config
Building configuration...
Current configuration : 3071 bytes
!
version 12.4
hostname cisco2811
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
!
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO

end
cisco2811#
```

7.10.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	IPv4 Address
Remote Subnet	192.168.50.0/24
Remote ID Type	IPv4 Address

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

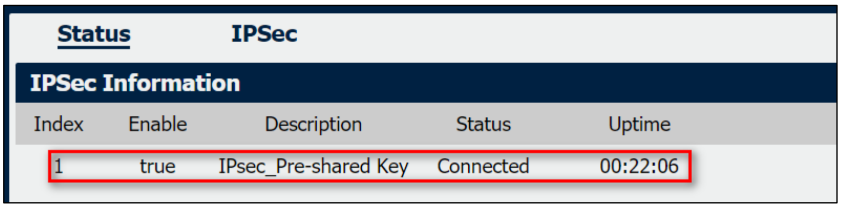
Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 251 – IPsec settings

Click **Save > Apply**. IPsec had been connected successfully. After that, go to **VPN > IPsec > Status** to check the connection status.



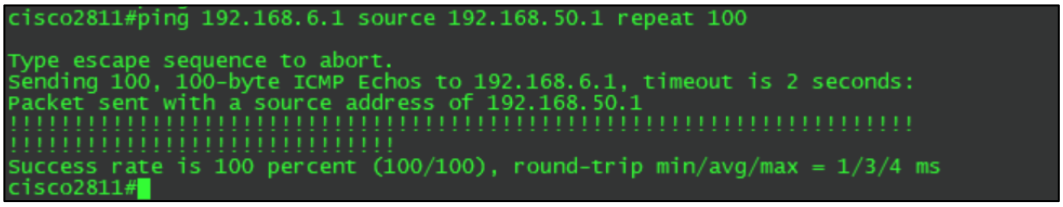
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Figure 252 – IPsec status connection

7.10.3 TEST

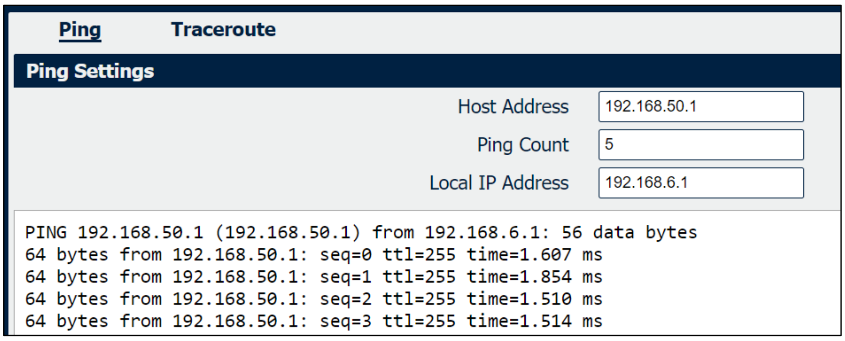
Ping from Cisco router to **AirGate 4G Wi-Fi**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 253 – Cisco test

Ping from **AirGate 4G Wi-Fi** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 254 – AirGate 4G Wi-Fi test

Test successfully.

7.11 IPSEC: FQDN WITH CISCO ROUTER

This tutorial shows how to configure IPsec_FQDN with Cisco router.

7.11.1 TOPOLOGY

You can use the following topology:

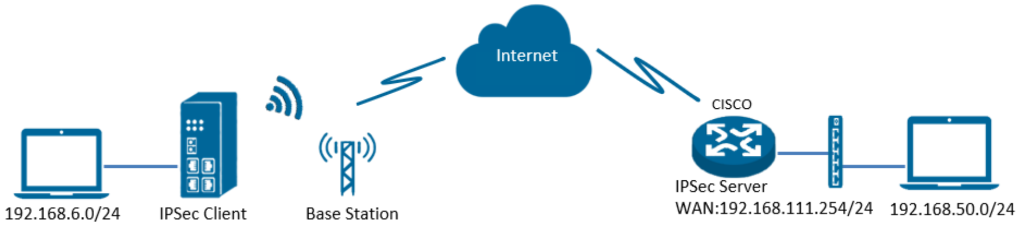


Figure 255 – IPsec topology

1. **AirGate 4G Wi-Fi** runs as IPsec Client with any kind of IP, which can ping IPsec server IP successfully.
2. Cisco router runs as IPsec Server with a static public IP.
3. IPsec tunnel is established between **AirGate 4G Wi-Fi** and Cisco router.

7.11.2 CONFIGURATION

7.11.2.1 SERVER CONFIGURATION

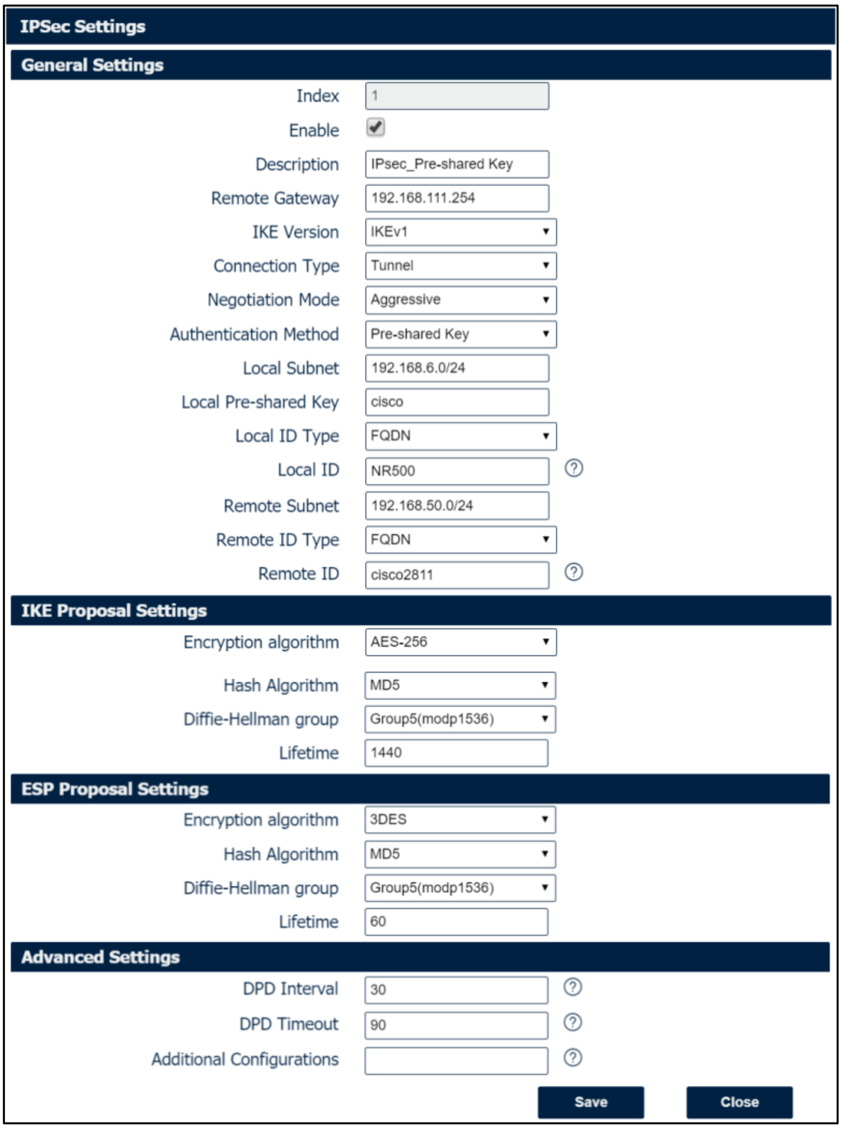
Login to Cisco router and setting like below:

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
ip cef
!
ip name-server 192.168.111.1
ip address-pool local
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password cisco
 set aggressive-mode client-endpoint fqdn NR500
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
```

```
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
!
end
cisco2811#
```

7.11.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Aggressive
Authentication Method	Pre-shared Key
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	FQDN
Local ID	NR500
Remote Subnet	192.168.50.0/24
Remote ID Type	FQDN
Remote ID	cisco2811

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

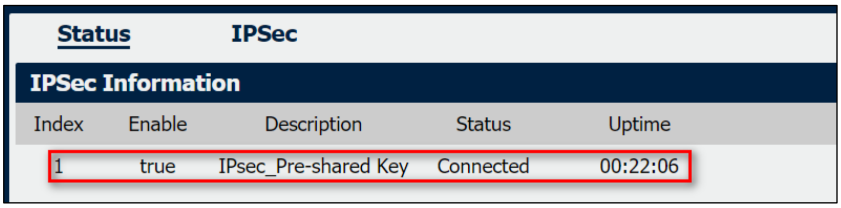
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 256 – IPsec settings

Click **Save > Apply**.

IPsec had been connected successfully. Go to **VPN > IPsec > Status** to check the connection status.



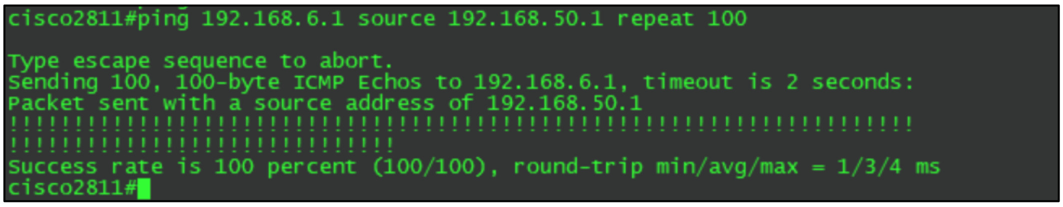
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPSec_Pre-shared Key	Connected	00:22:06

Figure 257 – IPsec status connection

7.11.3 TEST

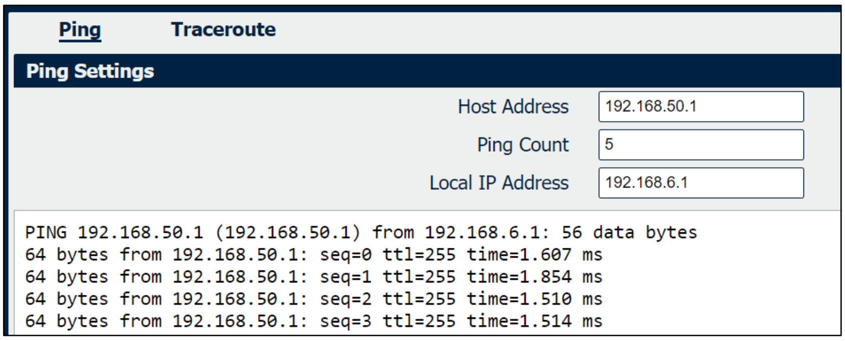
Ping from Cisco router to **AirGate 4G Wi-Fi**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 258 – IPsec test

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G Wi-Fi** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 259 – IPsec test

Test successfully.

7.12 IPSEC: PRE-SHARED KEY AND XAUTH WITH CISCO ROUTER

This tutorial shows how to configure IPsec_pre-shared key and Xauth with Cisco router.

7.12.1 TOPOLOGY

You can use the following topology:

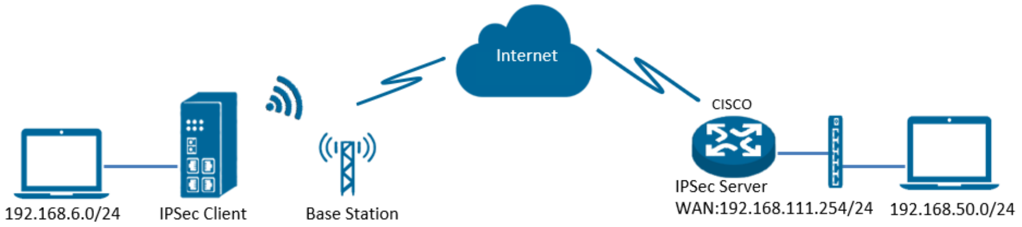


Figure 260 – IPsec topology

1. **AirGate 4G Wi-Fi** runs as IPsec Client with any kind of IP, which can ping IPsec server IP successfully.
2. Cisco router runs as IPsec Server with a static public IP.
3. IPsec tunnel is established between **AirGate 4G Wi-Fi** and Cisco router.

7.12.2 CONFIGURATION

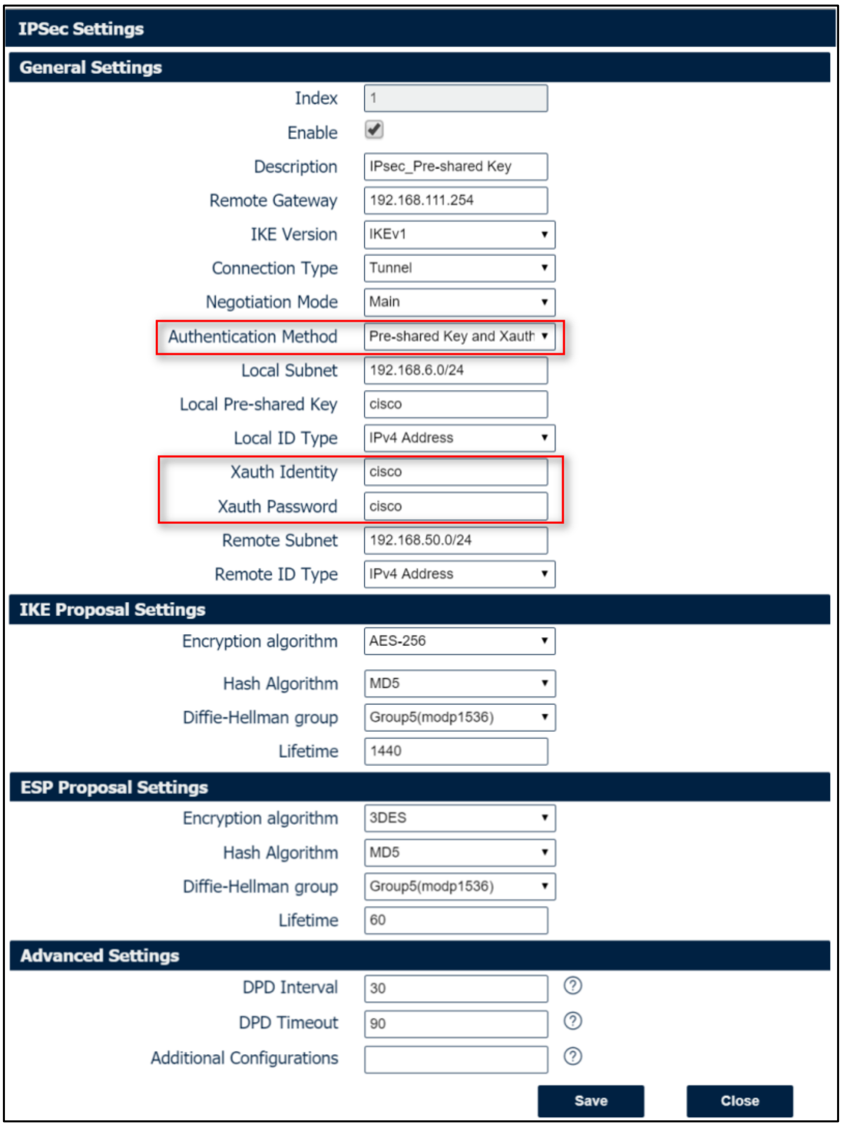
7.12.2.1 SERVER CONFIGURATION

Login to Cisco router and setting like below:

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
aaa new-model
aaa authentication login local
!
aaa session-id common
dot11 syslog
ip source-route
!
ip cef
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol

interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!!
line con 0
line vty 5 15
 exec-timeout 5 2
end
```

7.12.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN** > **IPsec** > **IPsec** > **General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key and Xauth
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	IPv4 Address
Xauth Identity	cisco
Xauth Password	cisco
Remote Subnet	192.168.50.0/24
Remote ID Type	IPv4 Address

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

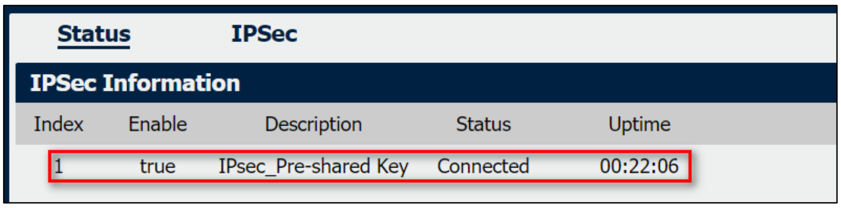
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 261 – IPsec settings

Click **Save** > **Apply**.

IPsec had been connected successfully. Go to **VPN** > **IPsec** > **Status** to check the connection status.



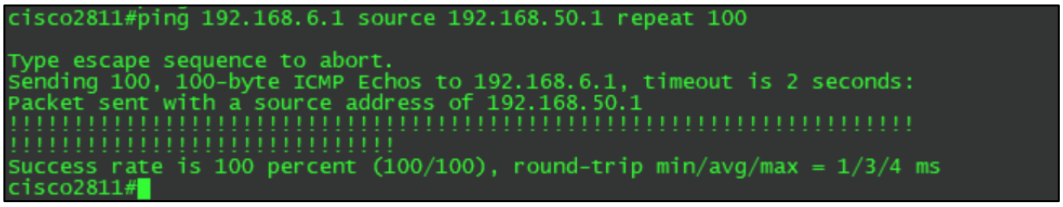
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Figure 262 – IPsec status connection

7.12.3 TEST

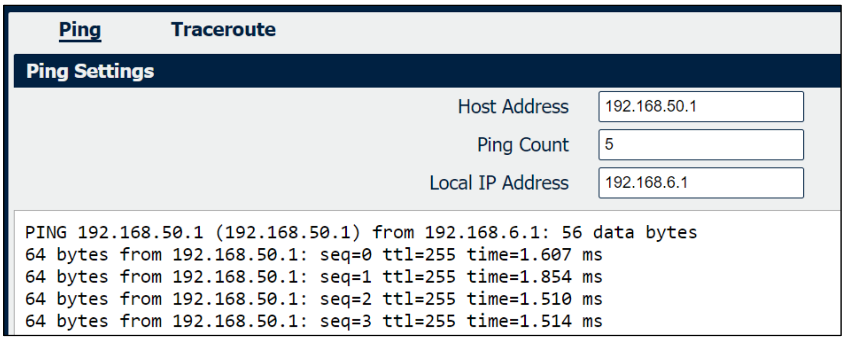
Ping from Cisco router to **AirGate 4G Wi-Fi**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 263 – Cisco test

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G Wi-Fi** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1
Ping Count: 5
Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 264 – AirGate 4G Wi-Fi test

Test successfully.

7.13 IPSEC: FQDN, PRE-SHARED KEY AND XAUTH WITH CISCO ROUTER

This tutorial shows how to configure IPSec_FQDN_Pre shared key and Xauth with Cisco router.

7.13.1 TOPOLOGY

You can use the following topology:

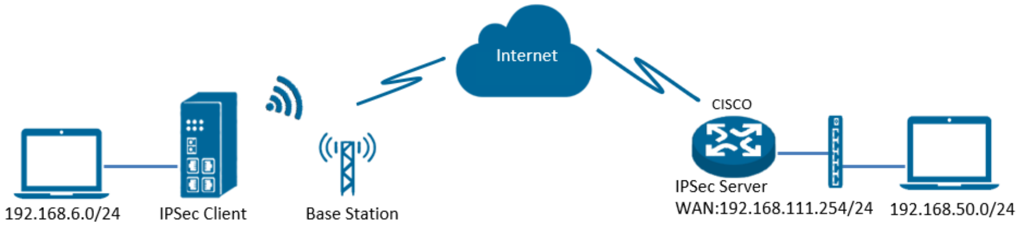


Figure 265 – IPsec topology

1. **AirGate 4G Wi-Fi** runs as IPsec Client with any kind of IP, which can ping IPsec server IP successfully.
2. Cisco router runs as IPsec Server with a static public IP.
3. IPsec tunnel is established between **AirGate 4G Wi-Fi** and Cisco router.

7.13.2 CONFIGURATION

7.13.2.1 SERVER CONFIGURATION

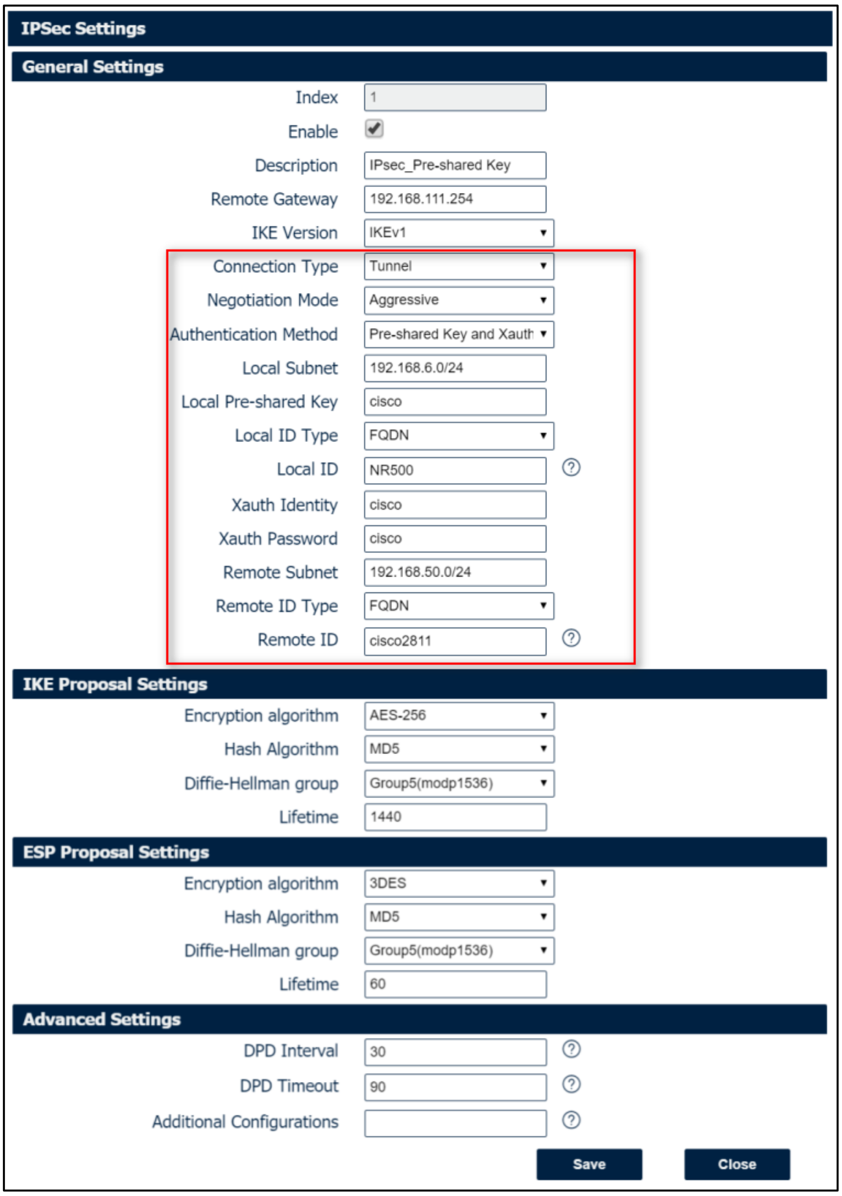
Login to Cisco router and setting like below:

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.!
aaa new-model
!
aaa authentication login LOGIN local
!
aaa session-id common
!
ip name-server 192.168.111.1
ip address-pool local
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password ken
 set aggressive-mode client-endpoint fqdn cisco2811
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
```

```
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
line con 0
line vty 5 15
end
```

7.13.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Aggressive
Authentication Method	Pre-shared Key and Xauth
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	FQDN
Local ID	NR500
Xauth Identity	cisco
Xauth Password	cisco
Remote Subnet	192.168.50.0/24
Remote ID Type	FQDN
Remote ID	cisco2811

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

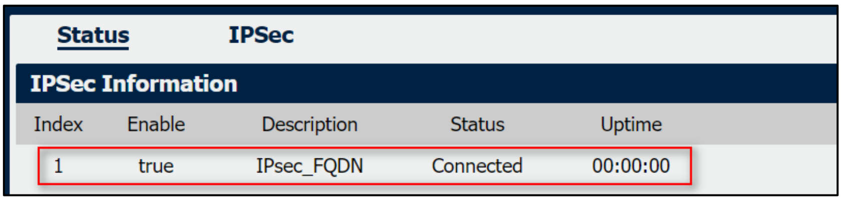
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 266 – IPsec settings

Click **Save > Apply**.

IPsec had been connected successfully. Go to **VPN > IPsec > Status** to check the connection status.



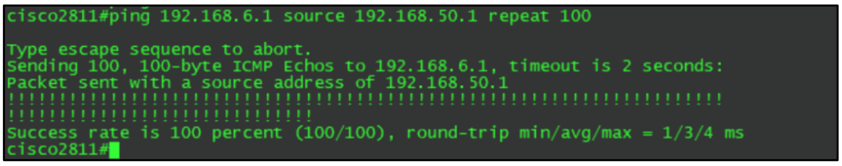
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_FQDN	Connected	00:00:00

Figure 267 – IPsec status connection

7.13.3 TEST

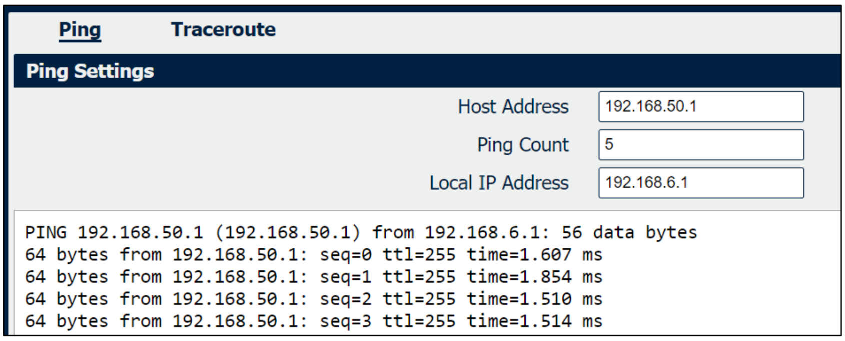
Ping from Cisco router to **AirGate 4G Wi-Fi**, LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 268 – Cisco terminal

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G Wi-Fi** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 269 – AirGate 4G Wi-Fi test

Test successfully.

7.14 CELLULAR SETTING

This tutorial shows how to configure cellular settings.

7.14.1 TOPOLOGY

You can use the following topology:

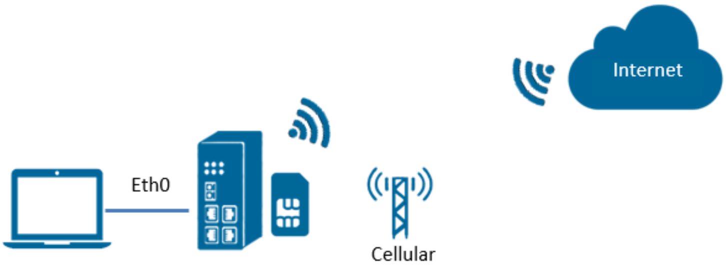
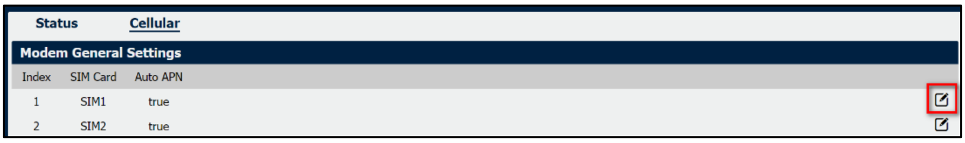


Figure 270 – Cellular connection topology

1. Specify WWAN1 as primary link and **AirGate 4G Wi-Fi** pro access cellular network via SIM card (WWAN1).
2. ETH0 works as LAN interface and enable DHCP server, allocate IP to the end PC.

7.14.2 CELLULAR SETTING

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Link Management > Cellular > Cellular**. After that, just click on the SIM1 connection edit button:

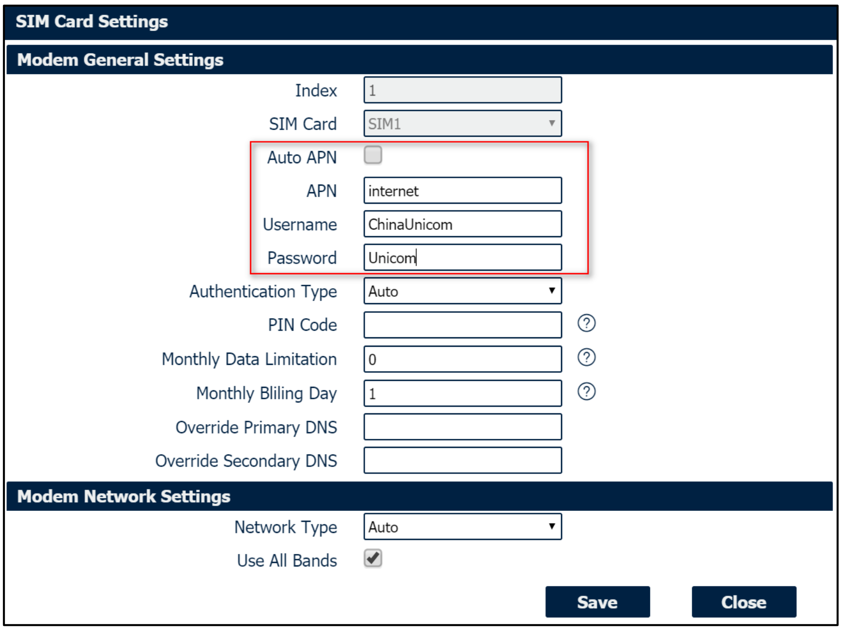


Modem General Settings

Index	SIM Card	Auto APN
1	SIM1	true
2	SIM2	true

Figure 271 – Cellular connection settings

Setup the APN, Username and Password of the SIM card, please also setup the PIN if the SIM work with the PIN code and left the other parameters as default.



SIM Card Settings

Modem General Settings

Index	1
SIM Card	SIM1
Auto APN	☐
APN	internet
Username	ChinaUnicom
Password	Unicom
Authentication Type	Auto
PIN Code	
Monthly Data Limitation	0
Monthly Bliling Day	1
Override Primary DNS	
Override Secondary DNS	

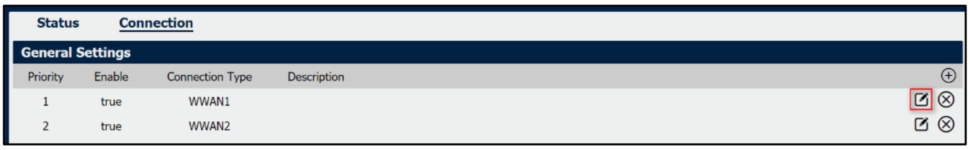
Modem Network Settings

Network Type	Auto
Use All Bands	☑

Figure 272 – SIM card settings

Click **Save** > **Apply**.

Go to Link **Management** > **Connection Manager** > **Connection**. Click the **Edit button** of WWAN1.

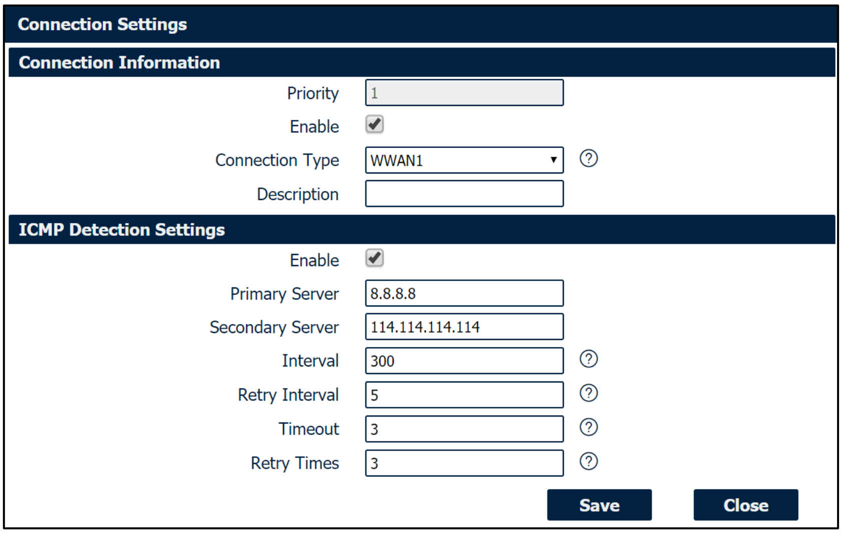


General Settings

Priority	Enable	Connection Type	Description
1	true	WWAN1	
2	true	WWAN2	

Figure 273 – WWAN1 connection

Setup the parameters of WWAN1 as below:



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WWAN1
Description	

ICMP Detection Settings

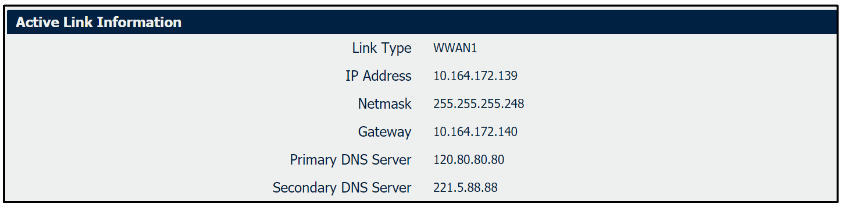
Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 274 – IPsec status connection

Click **Save** > **Apply**.

7.14.3 TEST

Go to **Overview** > **Overview** > **Active Link Information**. The router had been got the IP information for ISP.

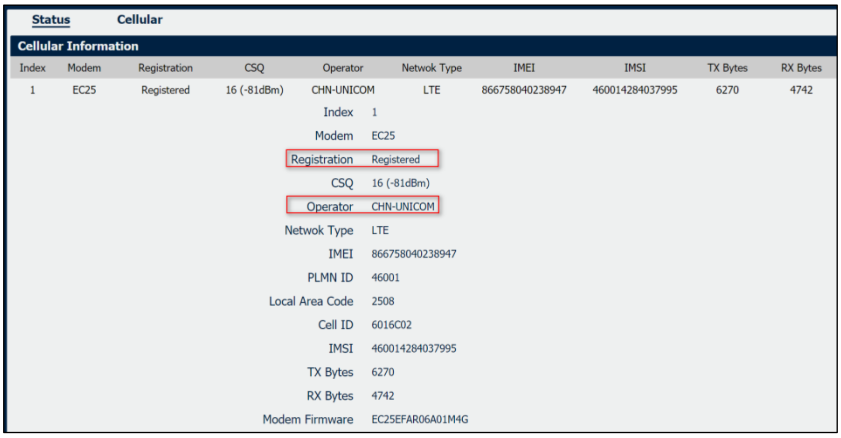


Active Link Information

Link Type	WWAN1
IP Address	10.164.172.139
Netmask	255.255.255.248
Gateway	10.164.172.140
Primary DNS Server	120.80.80.80
Secondary DNS Server	221.5.88.88

Figure 275 – IPsec status connection

Go to **Link Management** > **Cellular** > **Status** to check the registration information.



Cellular Information

Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	16 (-81dBm)	CHN-UNICOM	LTE	866758040238947	460014284037995	6270	4742

Index	1
Modem	EC25
Registration	Registered
CSQ	16 (-81dBm)
Operator	CHN-UNICOM
Netwok Type	LTE
IMEI	866758040238947
PLMN ID	46001
Local Area Code	2508
Cell ID	6016C02
IMSI	460014284037995
TX Bytes	6270
RX Bytes	4742
Modem Firmware	EC25EFAR06A01M4G

Figure 276 – Cellular status

7.15 ETHERNET SETTING

This tutorial shows how to configure Ethernet settings.

7.15.1 TOPOLOGY

You can use the following topology:

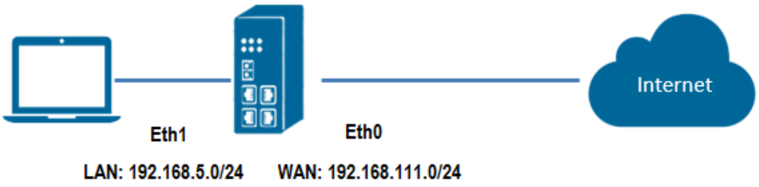


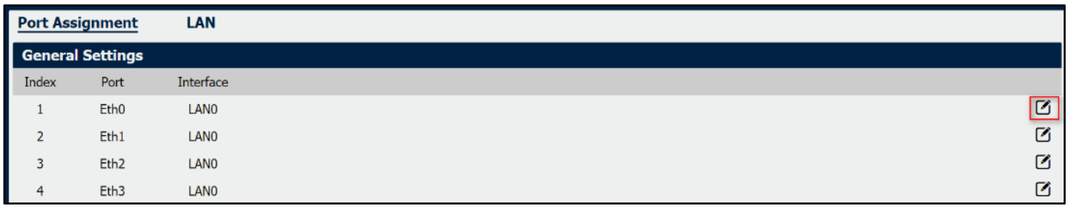
Figure 277 – Ethernet connection topology

1. Specify ETH0 port as WAN port and **AirGate 4G Wi-Fi** communicate with Internet via WAN link.
2. ETH1 works as LAN interface and enable DHCP server, allocate IP to the end PC.

7.15.2 CONFIGURATION

7.15.2.1 ETHERNET CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Link Management>Ethernet>Port Assignment.** After that, just click the **Edit button** of Eth0.

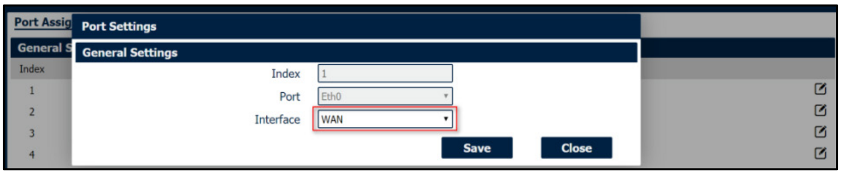


General Settings

Index	Port	Interface
1	Eth0	LAN0
2	Eth1	LAN0
3	Eth2	LAN0
4	Eth3	LAN0

Figure 278 – Eth0 port configuration

Assigned the port ETH0 as WAN, like below:



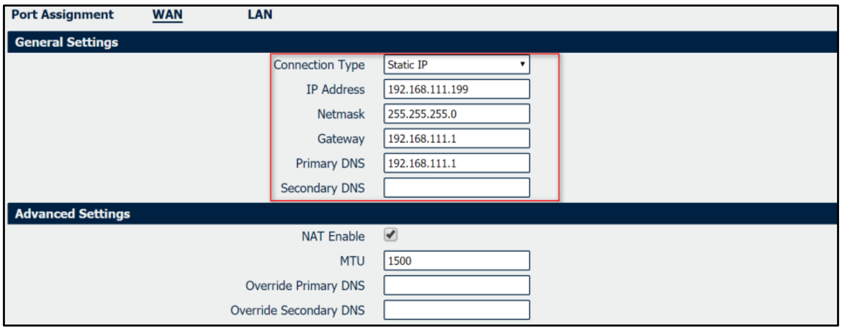
General Settings

Index: 1
Port: Eth0
Interface: WAN

Figure 279 – Eth0 interface

Click **Save > Apply**.

Go to **Industrial Interface > Ethernet > Status > WAN**, specify the Connection Type as "Static IP" and configure the IP information, setting like below:



General Settings

Connection Type: Static IP
IP Address: 192.168.111.199
Netmask: 255.255.255.0
Gateway: 192.168.111.1
Primary DNS: 192.168.111.1
Secondary DNS:

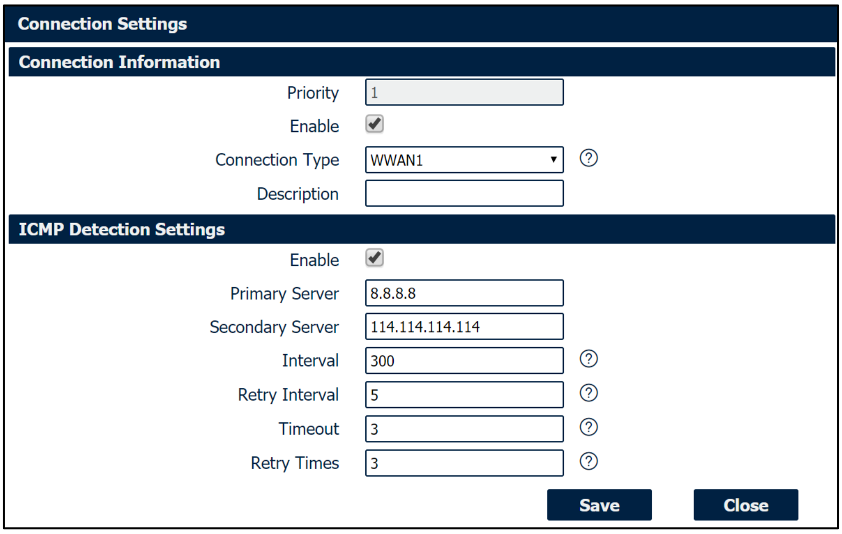
Advanced Settings

NAT Enable: ☑
MTU: 1500
Override Primary DNS:
Override Secondary DNS:

Figure 280 – WWAN1 connection

AirGate 4G Wi-Fi also supports DHCP and PPPoE connection types. In this example, however, the static IP configuration is used.

Click **Save > Apply**.



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WWAN1
Description	

ICMP Detection Settings

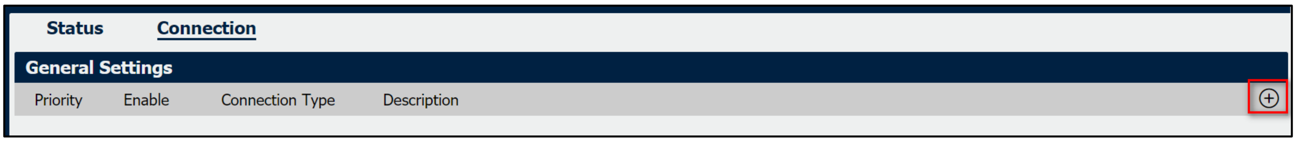
Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 281 – Ethernet settings

Click **Save > Apply**.

7.15.2.2 PRIMARY CONNECTION CONFIGURATION

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Link Management > Connection Manager > Connection**, delete the WWAN1 and WWAN2, then click **Save > Apply**. After that, add the "WAN" link as below picture:

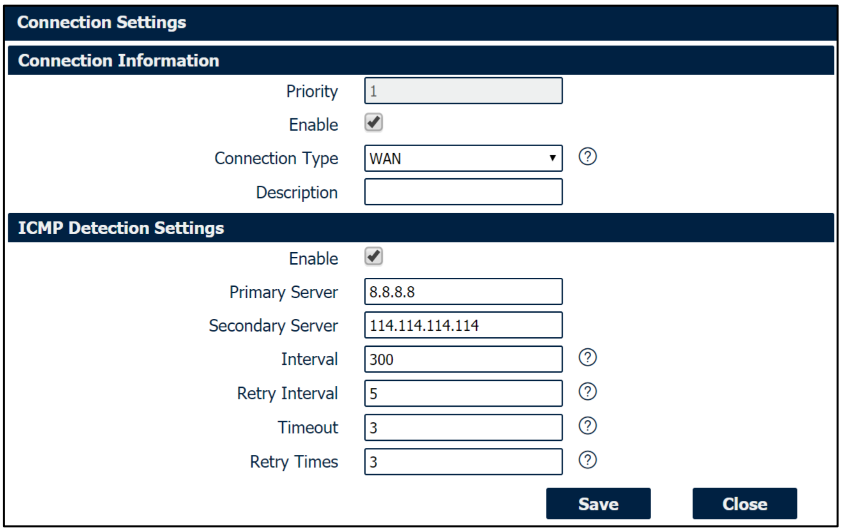


General Settings

Priority	Enable	Connection Type	Description

Figure 282 – Primary link settings

Configure the WAN parameters as below:



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WAN
Description	

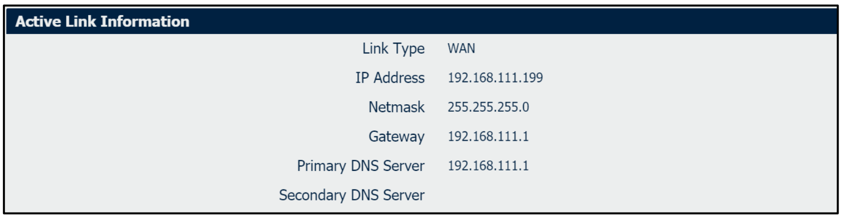
ICMP Detection Settings

Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 283 – WAN parameters

7.15.3 TEST

You must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Overview > Status > Active Link Information**.

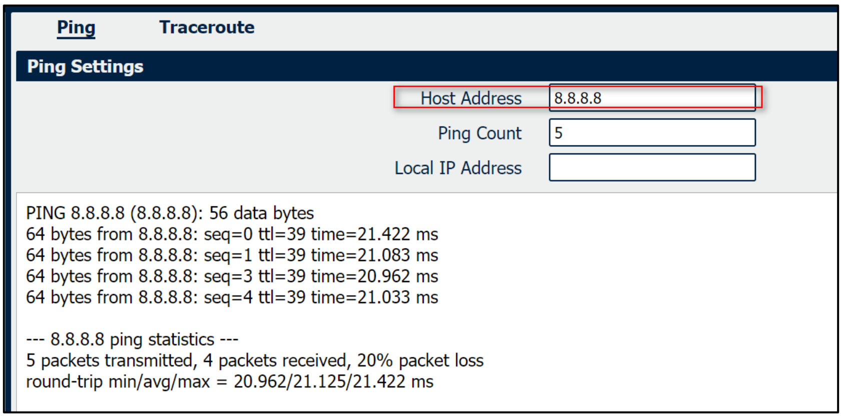


Active Link Information

Link Type	WAN
IP Address	192.168.111.199
Netmask	255.255.255.0
Gateway	192.168.111.1
Primary DNS Server	192.168.111.1
Secondary DNS Server	

Figure 284 – WAN status connection

After that, you must go to **Maintenance > Debug Tool > Ping.** Router can ping "8.8.8.8" successfully.



Host Address: 8.8.8.8

Ping Count: 5

Local IP Address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=39 time=21.422 ms
64 bytes from 8.8.8.8: seq=1 ttl=39 time=21.083 ms
64 bytes from 8.8.8.8: seq=3 ttl=39 time=20.962 ms
64 bytes from 8.8.8.8: seq=4 ttl=39 time=21.033 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 20.962/21.125/21.422 ms
```

Figure 285 – Ethernet configuration test

7.16 DIGITAL INPUT CONFIGURATION

This tutorial shows how to configure the digital input.

7.16.1 TYPICAL APPLICATION DIAGRAM

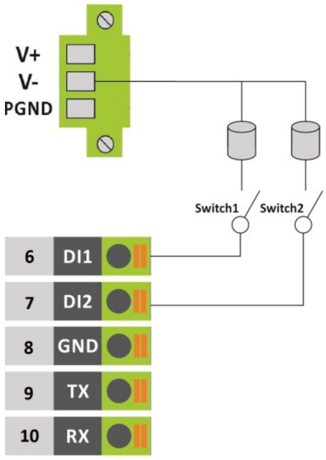
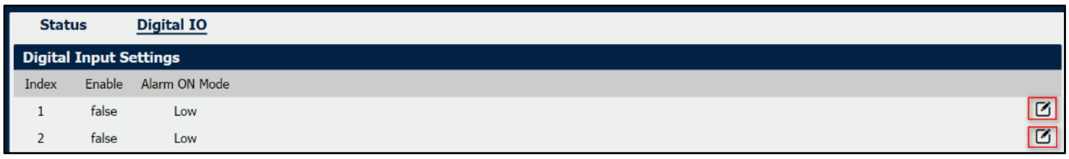


Figure 286 – Typical application diagram

7.16.2 DIGITAL INPUT CONFIGURATION

Go to **Industrial Interface > Digital IO > Digital IO > Digital Input Settings** and click the **Edit button** of DI1 and DI2.

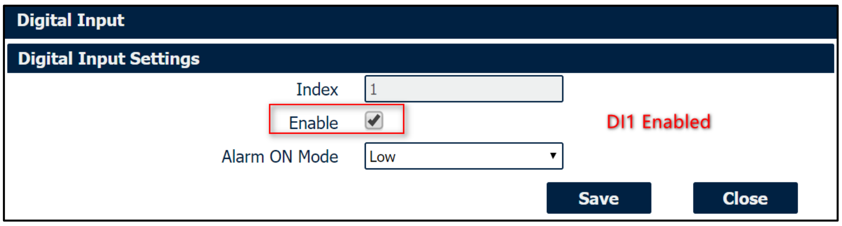


Digital Input Settings

Index	Enable	Alarm ON Mode
1	false	Low
2	false	Low

Figure 287 – Digital input settings

Enable DI1 and DI2, as shown in the figures below:



Digital Input

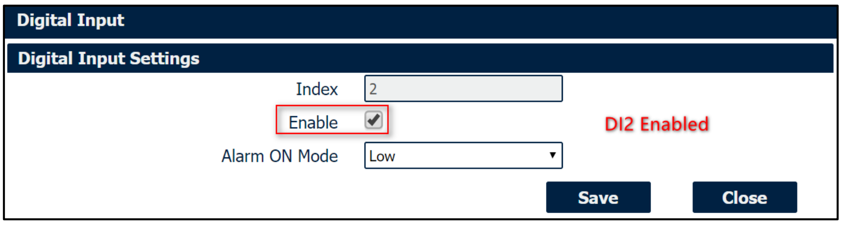
Digital Input Settings

Index: 1

Enable ☑ DI1 Enabled

Alarm ON Mode: Low

Figure 288 – DI1



Digital Input

Digital Input Settings

Index: 2

Enable ☑ DI2 Enabled

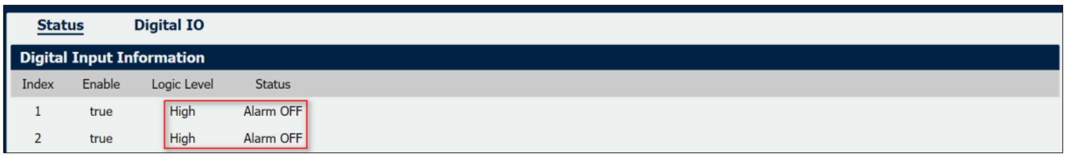
Alarm ON Mode: Low

Figure 289 – DI2

Click **Save > Apply**.

7.16.3 TEST

Go to **Industrial Interface > Digital IO > Status > Digital Input Information** to check the default DI1 and DI2 status like below:

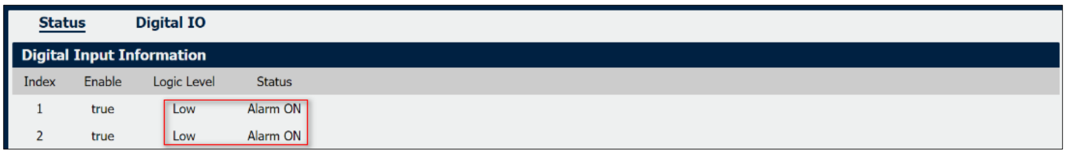


Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Figure 290 – Digital input information

Switch on (short to V-) for both DI1 and DI2, to check again the status of DI1 and DI2, like below:



Status Digital IO

Digital Input Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Figure 291 – Logical level

- "Logic Level" changed from "High" to "Low".
- "Status" changed from "Alarm OFF" to "Alarm ON".

Test successfully

7.17 DIGITAL OUTPUT CONFIGURATION

This tutorial shows how to configure the digital output.

7.17.1 TYPICAL APPLICATION DIAGRAM

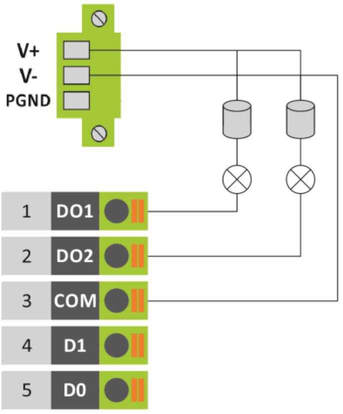
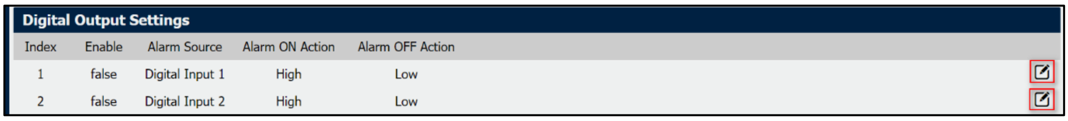


Figure 292 – Typical application diagram

7.17.2 DIGITAL OUTPUT CONFIGURATION

Go to **Industrial Interface > Digital IO > Digital IO > Digital Output Settings**. After that, click the **Edit button** of DO1 and DO2.

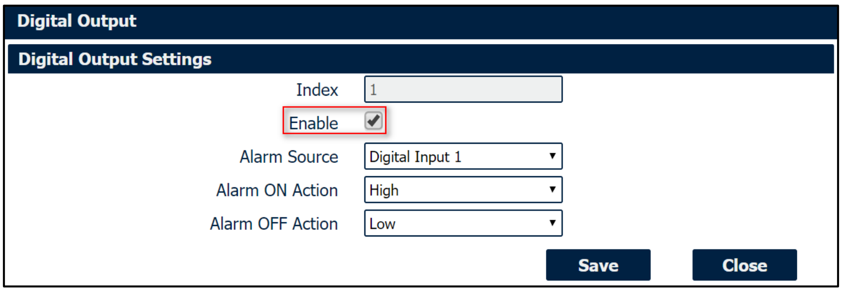


Digital Output Settings

Index	Enable	Alarm Source	Alarm ON Action	Alarm OFF Action
1	false	Digital Input 1	High	Low
2	false	Digital Input 2	High	Low

Figure 293 – Digital output settings

Enable DO1 and DO2, like below:

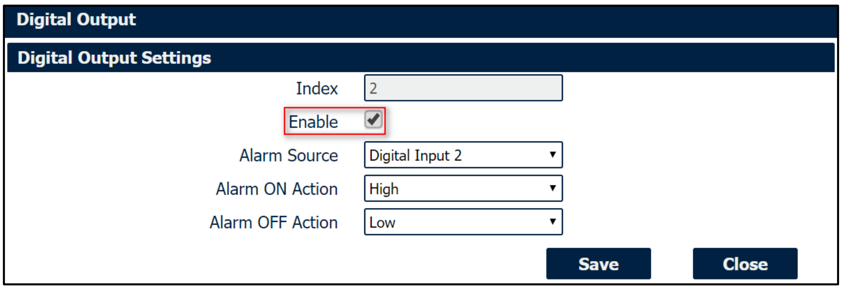


Digital Output

Digital Output Settings

Index	1
Enable	☑
Alarm Source	Digital Input 1
Alarm ON Action	High
Alarm OFF Action	Low

Figure 294 – DI1



Digital Output

Digital Output Settings

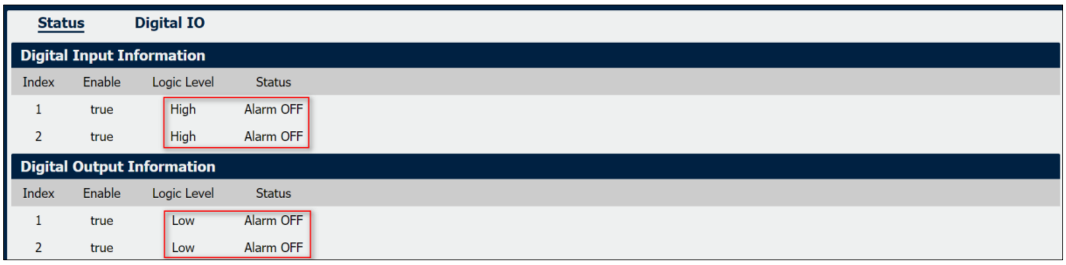
Index	2
Enable	☑
Alarm Source	Digital Input 2
Alarm ON Action	High
Alarm OFF Action	Low

Figure 295 – DI2

Click **Save > Apply**.

7.17.3 TEST

Go to **Industrial Interface > Digital IO > Status**, to check the default DI1, DI2, DO1 and DO2 status like below:



Status Digital IO

Digital Input Information

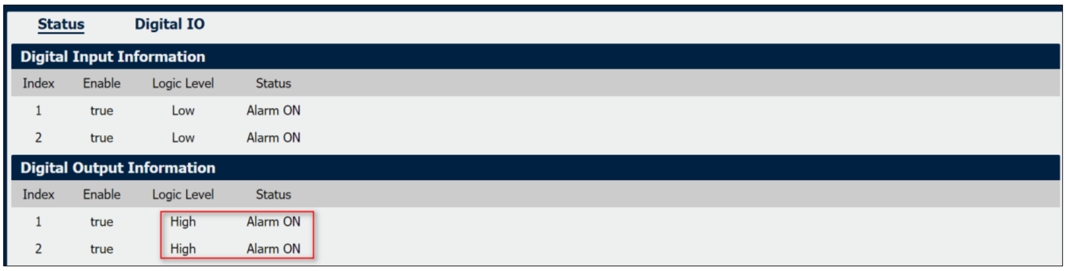
Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 296 – Digital and output status

Switch on (short to V-) for both DI1 and DI2, DO1 and DO2 will receive the trigger signal from D11 and DI2, the LED will become ON and the DO status like below:



Status Digital IO

Digital Input Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Digital Output Information

Index	Enable	Logic Level	Status
1	true	High	Alarm ON
2	true	High	Alarm ON

Figure 297 – Digital output test

- "Logic Level" changed from "High" to "Low".
- "Status" changed from "Alarm OFF" to "Alarm ON".

Test successfully.

7.18 SMS CONTROL

This tutorial contains information about configuring and using the SMS control function.

7.18.1 TOPOLOGY

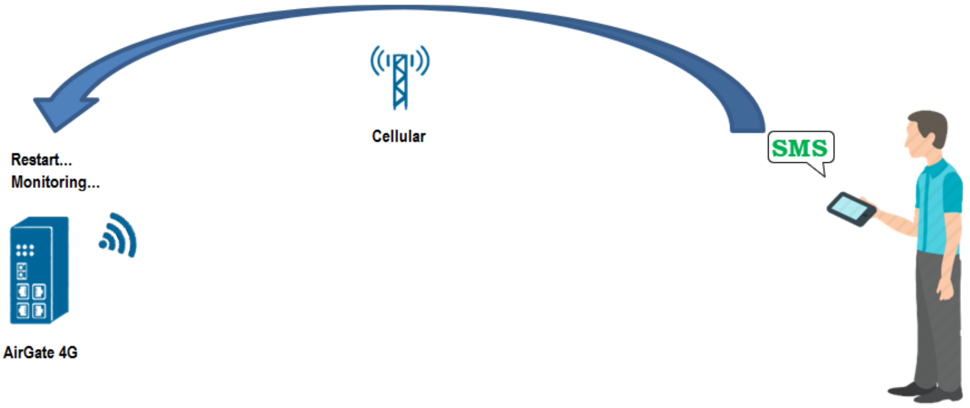


Figure 298 – SMS

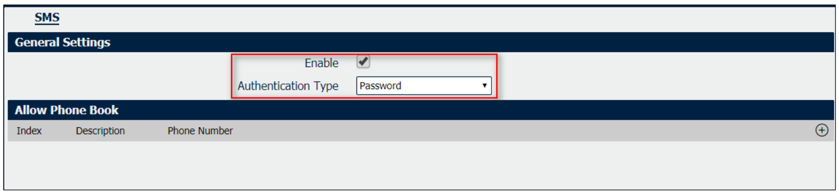
1. **AirGate 4G Wi-Fi** router dial up successfully with a SIM card.
2. Engineer sends SMS to the router with Special SMS Command to control **AirGate 4G Wi-Fi** router restart or configure **AirGate 4G Wi-Fi** router.

Special SMS Command means the router CLI Command. The engineer will send the SMS with CLI Command to control or monitoring the router.

7.18.2 CONFIGURATION

7.18.2.1 AIRGATE 4G WI-FI CONFIGURATION

Go to **Applications > SMS**, SMS control function is enabled by default settings.



SMS

General Settings

Enable ☑

Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number

Figure 299 – SMS configuration

It is also necessary to define the type of authentication ("Password", which will allow sending an SMS command with user and password, or "None") and register a phone number, which must be added to the phone book.

AirGate 4G Wi-Fi only receive the SMS message from the special phone number on the phone book.

7.18.2.2 SMS COMMAND

AUTHENTICATION TYPE: PASSWORD

The following commands are allowed:

1. **admin$admin$enable$enable$version** // send SMS to check the firmware version

The first "admin" means the router username. The second "admin" means the router password. "enable" means to send the CLI Command of "enable mode". "version" is the CLI command under enable mode.

2. **admin$admin$config$config$set syslog info** // send SMS to set router syslog to info level

The first "admin" means the router username. The second "admin" means the router password. "config" means to send the CLI Command of "config mode". "set syslog level info" is the CLI command under config mode.

You also can send SMS with **multiple** CLI Commands, like below:

3. **admin$admin$enable$enable$version;show active_link** // send SMS to check firmware version and link information together
4. **admin$admin$config$config$set syslog location ram;set syslog level info** // send SMS to set syslog location and syslog level
5. **admin$admin$doctl$DO 1 ON** // send command to enable digital output 1
6. **admin$admin$doctl$DO 2 ON** // send command to enable digital output 2
7. **admin$admin$doctl$DO 1 OFF** // send command to disable digital output 1
8. **admin$admin$doctl$DO 2 OFF** // send command to disable digital output 2

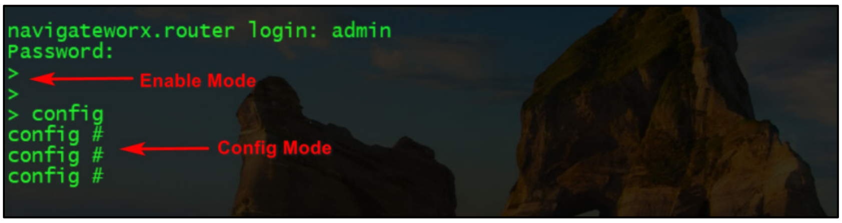
AUTHENTICATION TYPE: NONE

The following commands are allowed:

1. enable$version
2. config$set syslog level info
3. enable$version;show active_link
4. config$set syslog location ram;set syslog level info
5. doctl$DO 1 ON // send command to enable digital output 1.
6. doctl$DO 2 ON // send command to enable digital output 2.
7. doctl$DO 1 OFF // send command to disable digital output 1.
8. doctl$DO 2 OFF // send command to disable digital output 2.

7.18.3 CLI COMMAND

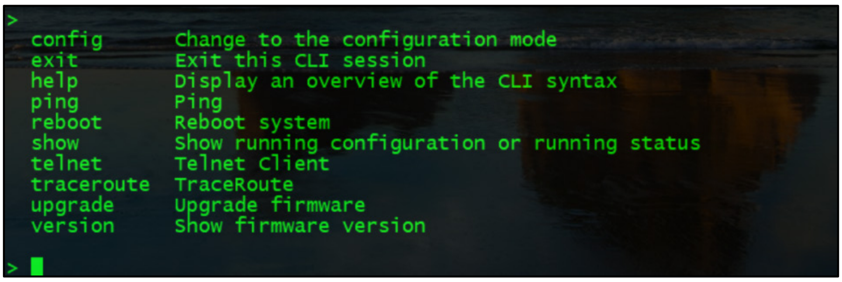
Telnet to the router to check the CLI command under "enable mode" or "config mode". When telnet to the router successfully, the character ">" means that the router under "enable mode".
When enter CLI command "config", the router will go into "config mode".



```
navigateworx.router login: admin
Password:
>
>
> config
config #
config #
config #
```

Figure 300 – Telnet Terminal

Enter the "?" or keyboard "Tab", then we can see what CLI command could be set in the next. Like in the figure below:

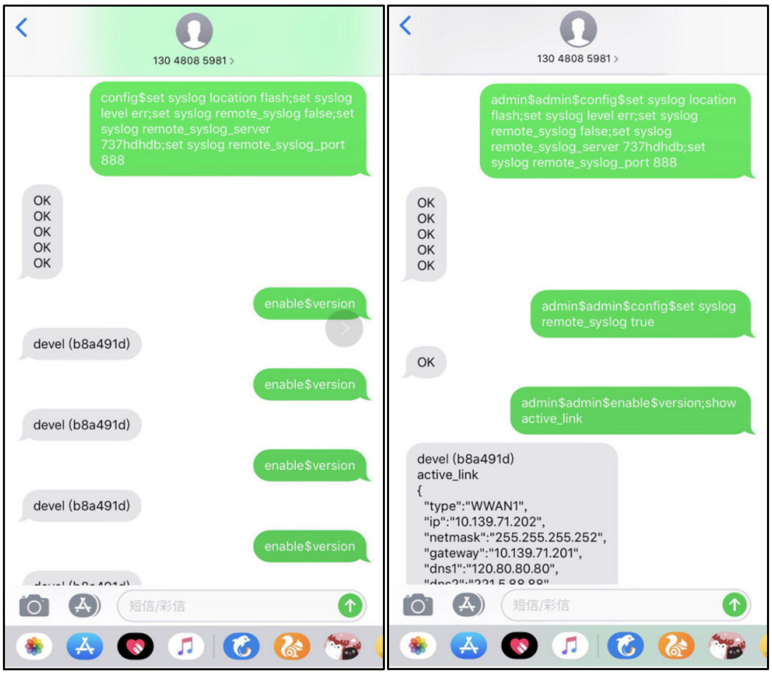


```
>
  config      Change to the configuration mode
  exit        Exit this CLI session
  help        Display an overview of the CLI syntax
  ping        Ping
  reboot      Reboot system
  show        Show running configuration or running status
  telnet      Telnet Client
  traceroute  TraceRoute
  upgrade     Upgrade firmware
  version     Show firmware version

> 
```

Figure 301 – Auto complete

7.18.4 TEST

Figure below presents results of a test for reference:



```
config$set syslog location flash;set syslog level err;set syslog remote_syslog false;set syslog remote_syslog_server 737hdhdb;set syslog remote_syslog_port 888

OK
OK
OK
OK
OK

enable$version

devel (b8a491d)

enable$version

devel (b8a491d)

enable$version

devel (b8a491d)

enable$version
```

```
admin$admin$config$set syslog location flash;set syslog level err;set syslog remote_syslog false;set syslog remote_syslog_server 737hdhdb;set syslog remote_syslog_port 888

OK
OK
OK
OK
OK

admin$admin$config$set syslog remote_syslog true

OK

admin$admin$enable$version;show active_link

devel (b8a491d)
active_link
{
  "type":"WWAN1",
  "ip":"10.139.71.202",
  "netmask":"255.255.255.252",
  "gateway":"10.139.71.201",
  "dns1":"120.80.80.80",
```

Figure 302 – SMS

7.19 SMS EVENT (DIDO)

This tutorial contains information about configuring and using the SMS control function.

7.19.1 TOPOLOGY

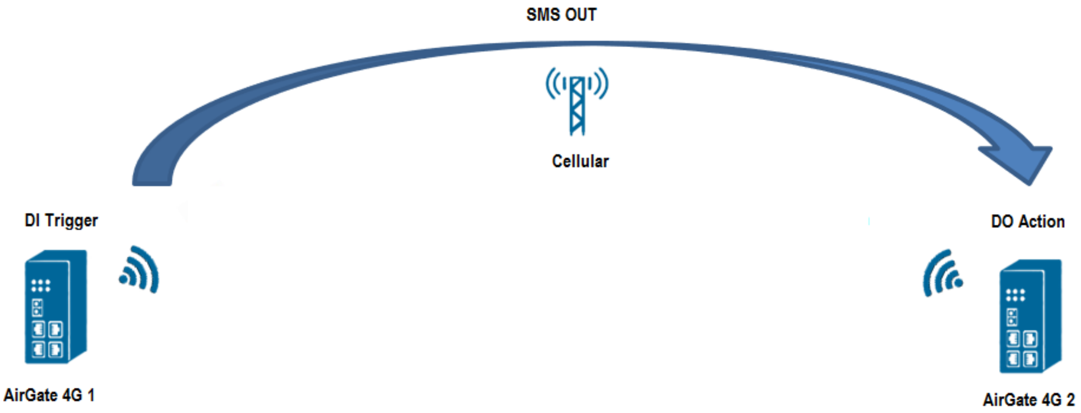


Figure 303 – SMS

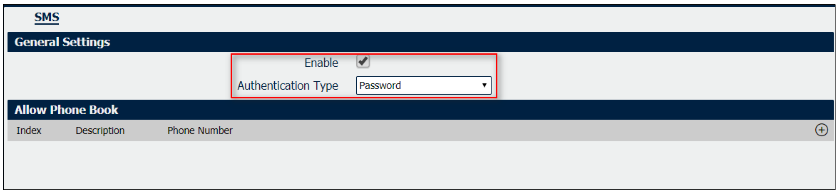
1. **AirGate 4G Wi-Fi** 1 dial up successfully with SIM card and Phone No:13265900210.
2. **AirGate 4G Wi-Fi** 2 dial up successfully with SIM card and Phone No:13265143432.
3. Trigger the DI status changed on Router 1 to make it send out the Pre-set special SMS command to Router 2.

Router 2 receives the special SMS command and controls DO on or off.

7.19.2 CONFIGURATION

7.19.2.1 AIRGATE 4G WI-FI 1 CONFIGURATION

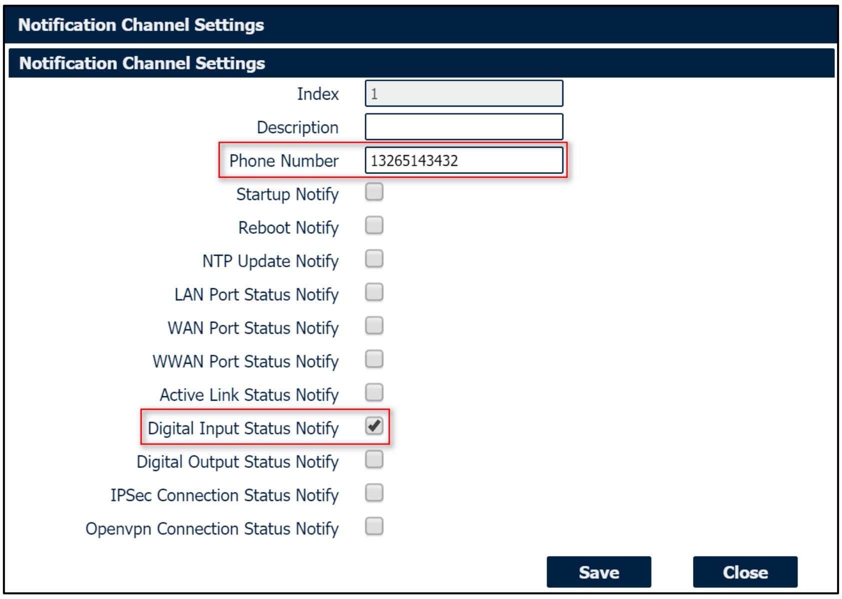
To configure router 1, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Applications** > **SMS** and enable SMS function.



Enable ☑
Authentication Type: Password

Figure 304 – SMS configuration

After that, go to **Applications** > **SMS** > **Notification,** specify the phone number of router 2 to receive the special SMS content from router 1 and enable DI status notify, like below:



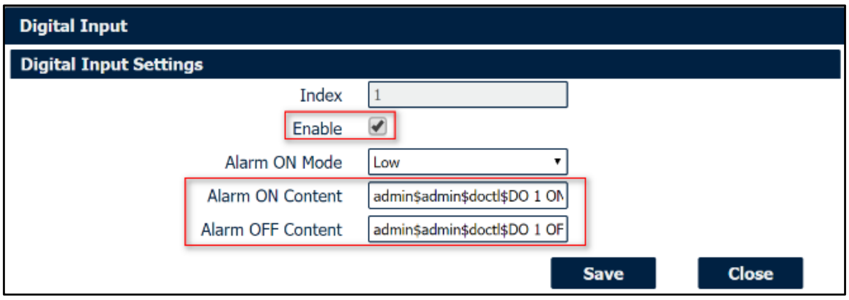
Index: 1
Description:
Phone Number: 13265143432
Startup Notify ☐
Reboot Notify ☐
NTP Update Notify ☐
LAN Port Status Notify ☐
WAN Port Status Notify ☐
WWAN Port Status Notify ☐
Active Link Status Notify ☐
Digital Input Status Notify ☑
Digital Output Status Notify ☐
IPSec Connection Status Notify ☐
Openvpn Connection Status Notify ☐

Figure 305 – Digital input status notification

Digital Input Status Notify parameter content is defined according to **Alarm ON/OFF Content** parameter. If **Alarm ON/OFF Content** is empty, then router will send out default content, like "Digital input 1/2 alarm on/off".

Click **Save** > **Apply**.

Go to **Industrial Interface > Digital IO > Digital Input Settings**, to specify the special content of Alarm ON and OFF, like below:



Digital Input

Digital Input Settings

Index	1
Enable	☑
Alarm ON Mode	Low
Alarm ON Content	admin$admin$doctl$DO 1 ON
Alarm OFF Content	admin$admin$doctl$DO 1 OF

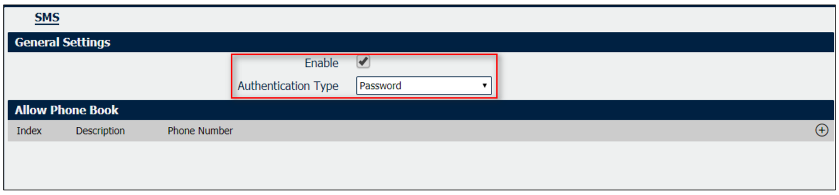
Figure 306 – Alarm content

The special SMS content to control DO on and off like below:

- **DO ON:** admin$admin$doctl$DO 1/2 ON
- **DO OFF:** admin$admin$doctl$DO 1/2 OFF
- **Format:** <username>$<password>$<control command>$<DO> <DO_index> <ON/OFF>

7.19.2.2 AIRGATE 4G WI-FI 2 CONFIGURATION

To configure router 1, you must open the Web Interface of **AirGate 4G Wi-Fi** and go to **Applications > SMS.** SMS control function is already enabled.



SMS

General Settings

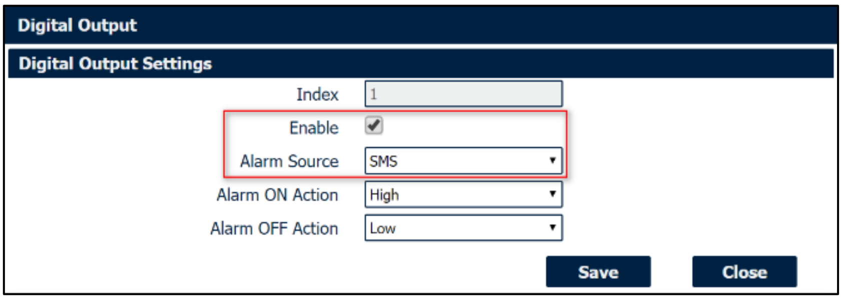
Enable	☑
Authentication Type	Password

Allow Phone Book

Index	Description	Phone Number

Figure 307 – Router 2: SMS sending

After that, go to **Industrial Interface > Digital IO > Digital Output Settings**, to specify the Alarm Source from SMS, like below:



Digital Output

Digital Output Settings

Index	1
Enable	☑
Alarm Source	SMS
Alarm ON Action	High
Alarm OFF Action	Low

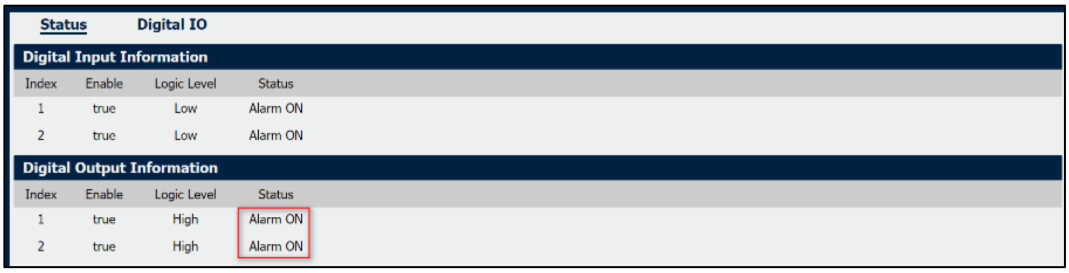
Figure 308 – Digital output settings

Click **Save > Apply**.

7.19.3 TEST

DI activated, send the special SMS to router 2. DO of Router 2 will be ON or OFF after received the special SMS from router 1.

7.19.3.1 TRIGGER ON STATUS



Status Digital IO

Digital Input Information

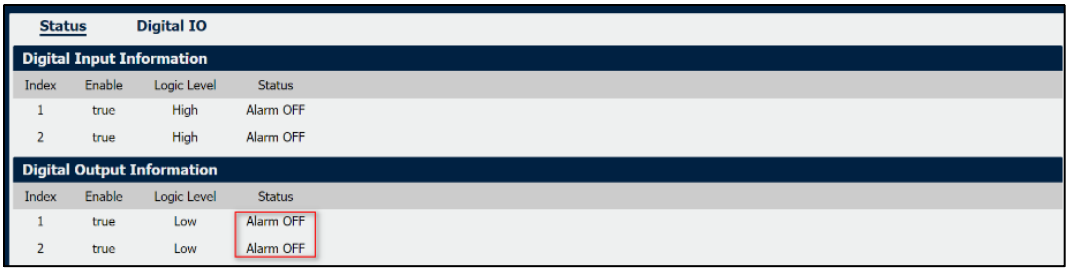
Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Digital Output Information

Index	Enable	Logic Level	Status
1	true	High	Alarm ON
2	true	High	Alarm ON

Figure 309 – On status

7.19.3.2 TRIGGER OFF STATUS



Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

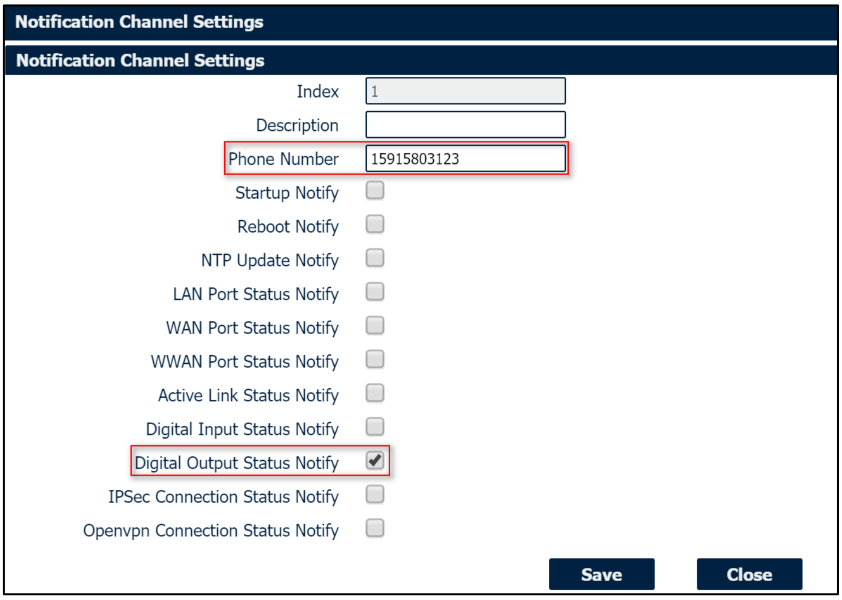
Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 310 – Off Status

Test successfully.

7.19.4 DO STATUS TO MOBILE PHONE

DO status on router 2 could be send to the special phone number, configuration like below. Go to **Applications > SMS > Notification**, specify the phone number to receive the DO status and enable DO status notify.



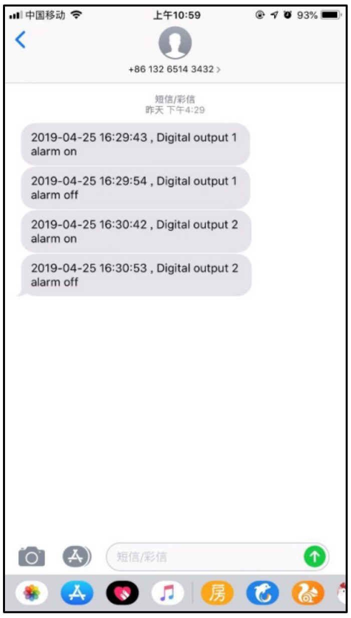
Notification Channel Settings

Notification Channel Settings

Index	1
Description	
Phone Number	15915803123
Startup Notify	□
Reboot Notify	□
NTP Update Notify	□
LAN Port Status Notify	□
WAN Port Status Notify	□
WWAN Port Status Notify	□
Active Link Status Notify	□
Digital Input Status Notify	□
Digital Output Status Notify	☑
IPSec Connection Status Notify	□
Openvpn Connection Status Notify	□

Figure 311 – Digital output configuration

Click **Save > Apply**.
DO status was sent to the mobile phone.



2019-04-25 16:29:43 , Digital output 1 alarm on

2019-04-25 16:29:54 , Digital output 1 alarm off

2019-04-25 16:30:42 , Digital output 2 alarm on

2019-04-25 16:30:53 , Digital output 2 alarm off

Figure 312 – SMS

7.20 MODBUS MASTER

This tutorial contains information on how to configure and use the Modbus Master application.

7.20.1 TOPOLOGY

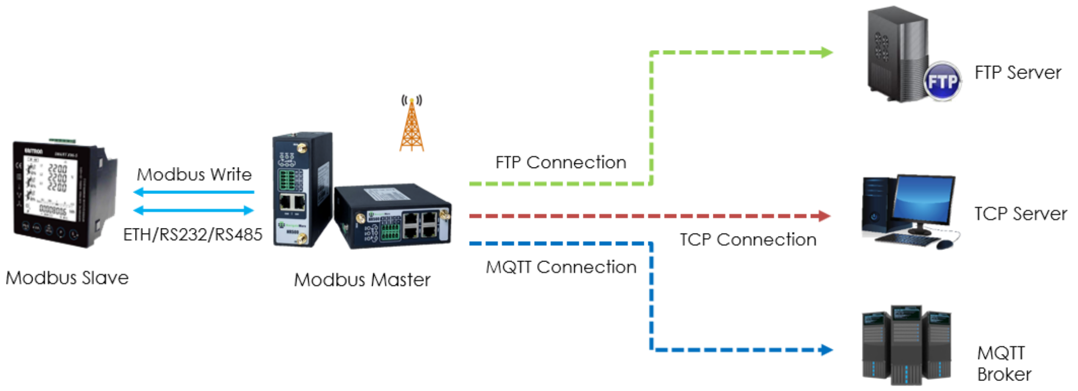


Figure 313 – Topology

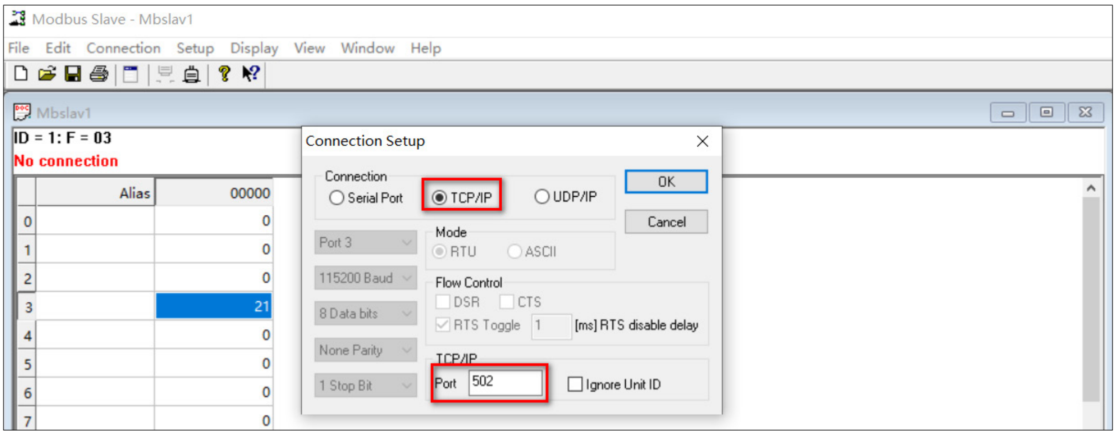
1. Configured as Modbus Master, the **AirGate 4G Wi-Fi** connects to the Modbus Slave via Ethernet, RS232 interface or RS485 interface.
2. The device searches Modbus Slave Modbus data and sends it to the remote management center via TCP, FTP or MQTT.
3. Still configured as Modbus Master, **AirGate 4G Wi-Fi** writes the register value to the Modbus Slave.

In this context, the connection type has been set to TCP, which means that the **AirGate 4G Wi-Fi** will connect to the Modbus Slave and read the value through the Ethernet port, although the process is also possible through the RS232 or RS485 serial port.

7.20.2 TRANSPORT VIA TCP

7.20.2.1 CONFIGURATION ON MODBUS SLAVE

In this example, the software "Modbus Slave" was used to simulate the final device (Modbus Slave device). The **TCP Port** parameter was set to "502", the **Slave ID** parameter was set to "1" and the **Function** parameter was set to "03-Holding Register (4x)", as shown below:



ID = 1: F = 03
No connection

	Alias	00000
0		0
1		0
2		0
3		21
4		0
5		0
6		0
7		0

Connection Setup

Connection: ○ Serial Port ● TCP/IP ○ UDP/IP

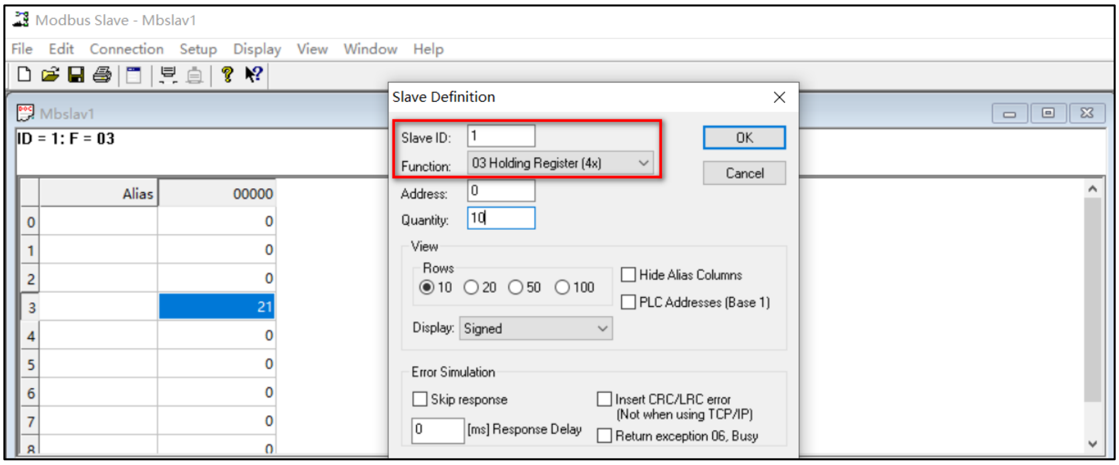
Port 3
115200 Baud
8 Data bits
None Parity
1 Stop Bit

Mode: ● RTU ○ ASCII

Flow Control: □ DSR □ CTS ☑ RTS Toggle 1 [ms] RTS disable delay

TCP/IP: Port 502 □ Ignore Unit ID

Figure 314 – Connection configuration (1)



ID = 1: F = 03

	Alias	00000
0		0
1		0
2		0
3		21
4		0
5		0
6		0
7		0
8		0

Slave Definition

Slave ID: 1
Function: 03 Holding Register (4x)
Address: 0
Quantity: 10

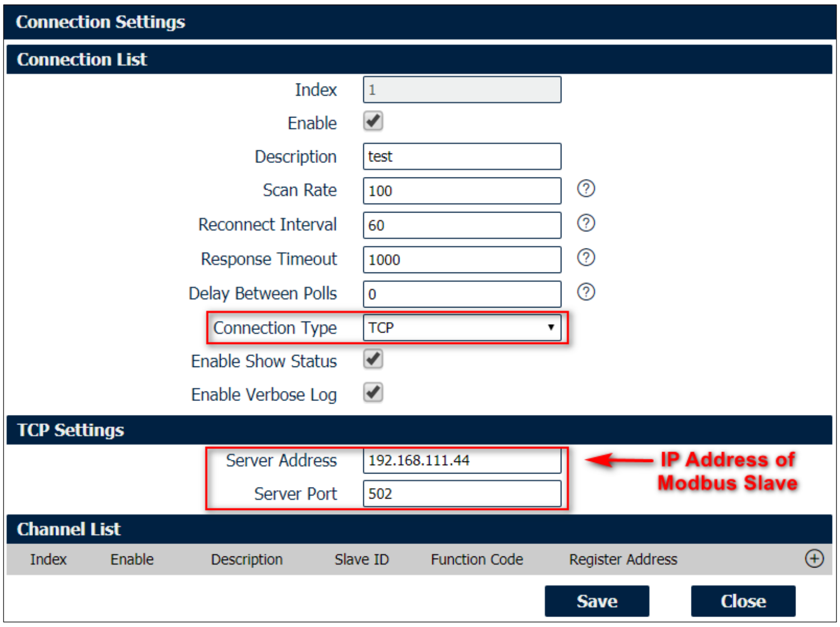
View
Rows: ● 10 ○ 20 ○ 50 ○ 100
□ Hide Alias Columns
□ PLC Addresses (Base 1)
Display: Signed

Error Simulation
□ Skip response
□ Insert CRC/LRC error (Not when using TCP/IP)
0 [ms] Response Delay
□ Return exception 06, Busy

Figure 315 – Connection configuration (2)

7.20.2.2 CONFIGURATION ON MODBUS POLL

To perform a configuration via Modbus Poll, you must open the **AirGate 4G Wi-Fi** web interface and follow the path **Application > Modbus Master > Modbus Poll**. Once this is done, it is necessary to add a new connection, specify the **Connection Type** parameter as "TCP" and configure the TCP connection in the **TCP Settings** section, so that it is possible to connect to the Modbus slave, as shown in the figure below:



Connection Settings

Connection List

Index	1
Enable	☑
Description	test
Scan Rate	100
Reconnect Interval	60
Response Timeout	1000
Delay Between Polls	0
Connection Type	TCP
Enable Show Status	☑
Enable Verbose Log	☑

TCP Settings

Server Address	192.168.111.44
Server Port	502

IP Address of Modbus Slave

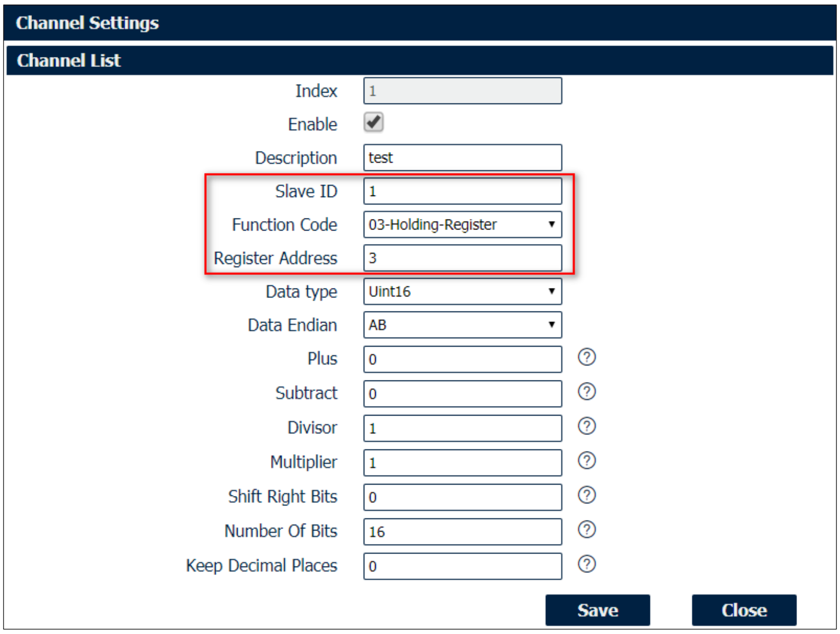
Channel List

Index	Enable	Description	Slave ID	Function Code	Register Address

Figure 316 – Configuring a connection via Modbus Poll (1)

Then click **Save > Apply**.

After that, it is necessary to access the **Channel List** section, configure the **Slave ID** parameter as "1", the **Function Code** parameter as "03-Holding Register" and the **Register Address** parameter as "3", as shown below:



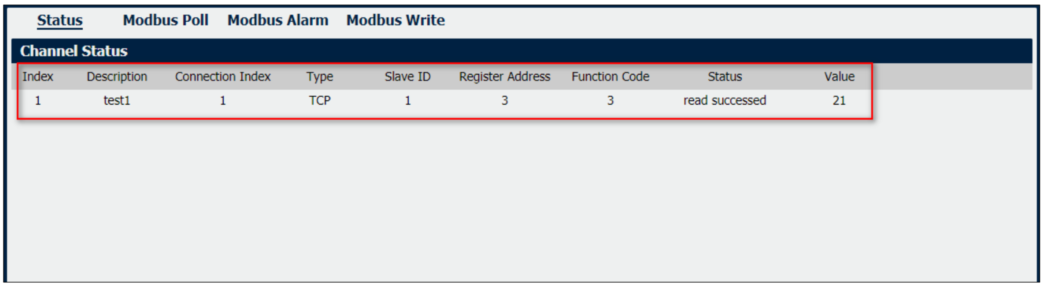
Channel Settings

Channel List

Index	1
Enable	☑
Description	test
Slave ID	1
Function Code	03-Holding-Register
Register Address	3
Data type	Uint16
Data Endian	AB
Plus	0
Subtract	0
Divisor	1
Multiplier	1
Shift Right Bits	0
Number Of Bits	16
Keep Decimal Places	0

Figure 317 – Configuring a connection via Modbus Poll (2)

Then click **Save > Apply** and follow the path **Application > Modbus Master > Status** to verify that the router has successfully read the value of the Modbus slave:



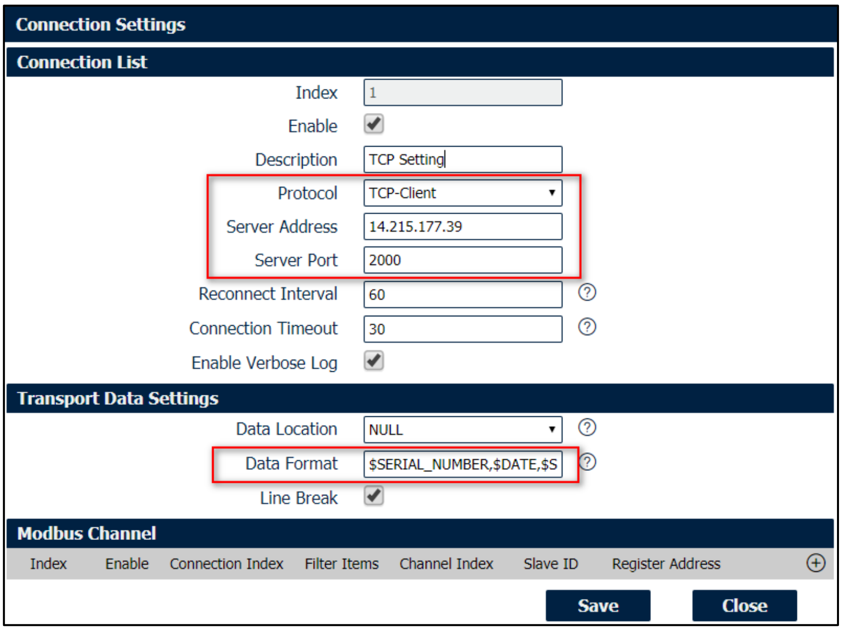
Channel Status

Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	Status	Value
1	test1	1	TCP	1	3	3	read successed	21

Figure 318 – Value successfully read

7.20.2.3 CONFIGURATION ON MODBUS TRANSPORT

To perform a configuration via Modbus Transport, you must open the **AirGate 4G Wi-Fi** web interface and follow the path **Application > Modbus Transport > Modbus Transport**. Once this is done, it is necessary to add a new connection, inform the protocol to be used in the **Protocol** parameter, inform the TCP server IP address in the **Server Address** parameter and the port to send the data to the remote TCP server in the **Server Port** parameter, as shown in the figure below:



Connection Settings

Connection List

Index	1
Enable	☑
Description	TCP Setting
Protocol	TCP-Client
Server Address	14.215.177.39
Server Port	2000
Reconnect Interval	60
Connection Timeout	30
Enable Verbose Log	☑

Transport Data Settings

Data Location	NULL
Data Format	$SERIAL_NUMBER,$DATE,$S
Line Break	☑

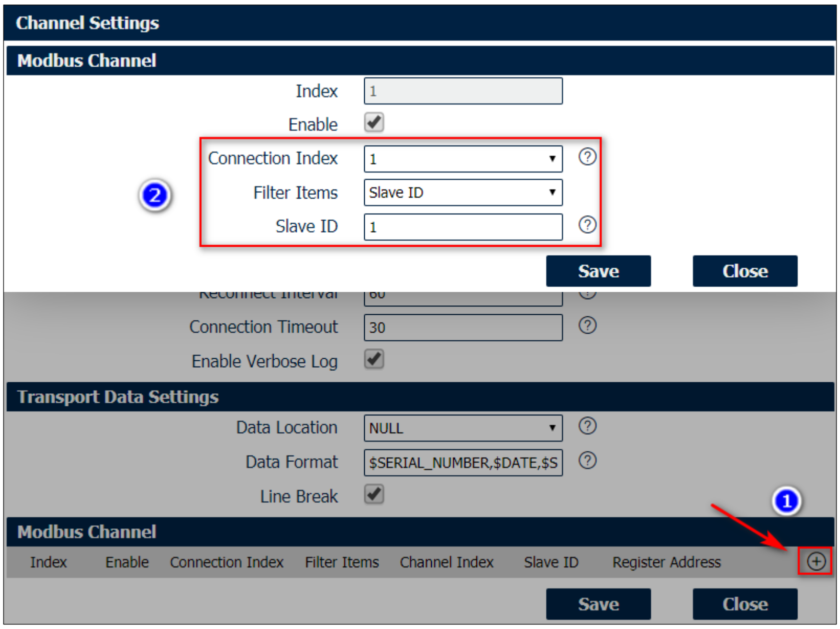
Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 319 – Configuring a connection via Modbus Transport (1)

In the **Data Format** parameter, you can enter the desired format or set it as default.

The **Modbus Channel** parameter must then be enabled. The Modbus Master will select the value sent to the remote TCP server from the Modbus slave.



Channel Settings

Modbus Channel

Index	1
Enable	☑
Connection Index	1
Filter Items	Slave ID
Slave ID	1

Connection Timeout	30
Enable Verbose Log	☑

Transport Data Settings

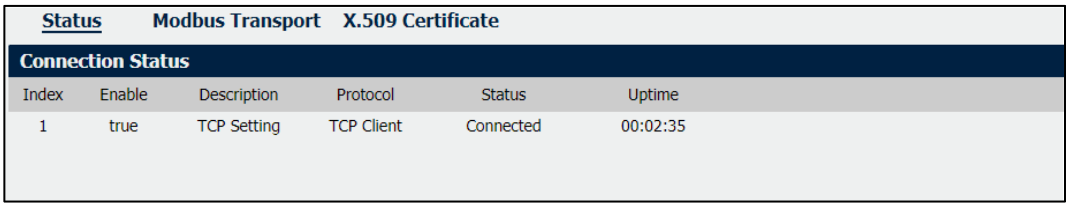
Data Location	NULL
Data Format	$SERIAL_NUMBER,$DATE,$S
Line Break	☑

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 320 – Configuring a connection via Modbus Transport (2)

Once this is done, just click **Save > Save > Apply** and go to **Application > Modbus Transport > Status** to check if the device has successfully connected to the remote server via TCP protocol:

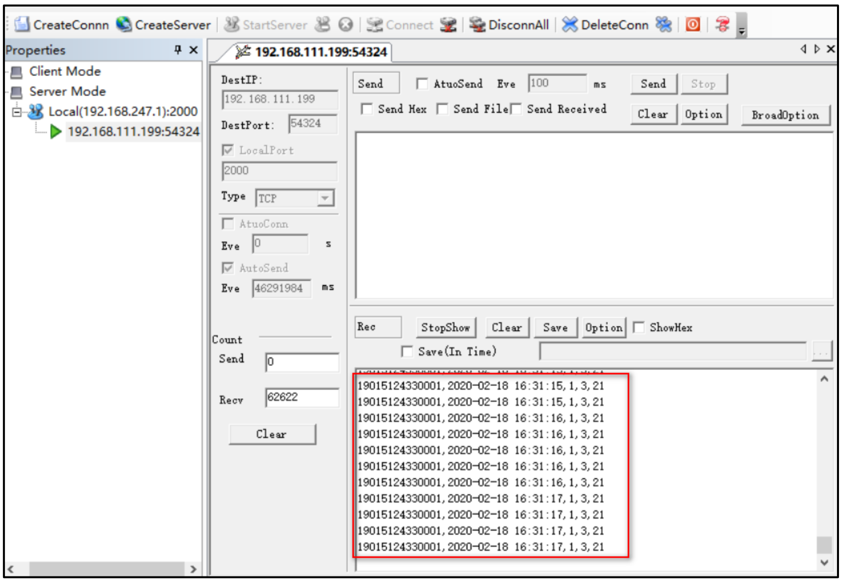


Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true	TCP Setting	TCP Client	Connected	00:02:35

Figure 321 – TCP connection status

In this example, the remote TCP server received the data successfully, as shown in the figure below:



DestIP: 192.168.111.199
DestPort: 54324
☑ LocalPort 2000
Type TCP
□ AtuoConn
Eve 0 s
☑ AutoSend
Eve 46291984 ms
□ AtuoSend Eve 100 ms
□ Send Hex □ Send File □ Send Received
Rec
□ ShowHex
□ Save(In Time)
Count
Send 0
Recv 62622

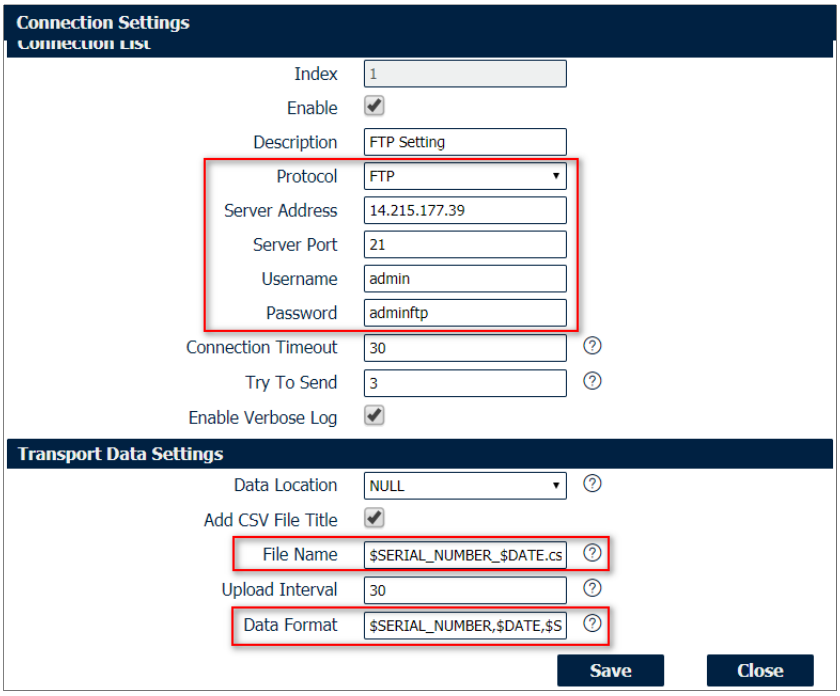
```
19015124330001,2020-02-18 16:31:15,1,3,21
19015124330001,2020-02-18 16:31:15,1,3,21
19015124330001,2020-02-18 16:31:16,1,3,21
19015124330001,2020-02-18 16:31:16,1,3,21
19015124330001,2020-02-18 16:31:16,1,3,21
19015124330001,2020-02-18 16:31:16,1,3,21
19015124330001,2020-02-18 16:31:16,1,3,21
19015124330001,2020-02-18 16:31:17,1,3,21
19015124330001,2020-02-18 16:31:17,1,3,21
19015124330001,2020-02-18 16:31:17,1,3,21
19015124330001,2020-02-18 16:31:17,1,3,21
```

Figure 322 – TCP server receiving data

7.20.3 TRANSPORT VIA FTP

To configure the device to perform data transport via FTP, you must observe the CONFIGURATION ON MODBUS SLAVE and CONFIGURATION ON MODBUS POLL sections of this chapter.

Once this is done, you must open the **AirGate 4G Wi-Fi** web interface and follow the path **Application > Modbus Transport > Modbus Transport**. Then it is necessary to add a new connection, inform the protocol to be used in the **Protocol** parameter, inform the FTP server IP address in the **Server Address** parameter, the port to send the data to the FTP server in the **Server Port** parameter and the user and password in the **Username** and **Password** parameters, as shown in the figure below:



Connection Settings

Connection List

Index	1
Enable	☑
Description	FTP Setting
Protocol	FTP
Server Address	14.215.177.39
Server Port	21
Username	admin
Password	adminftp
Connection Timeout	30
Try To Send	3
Enable Verbose Log	☑

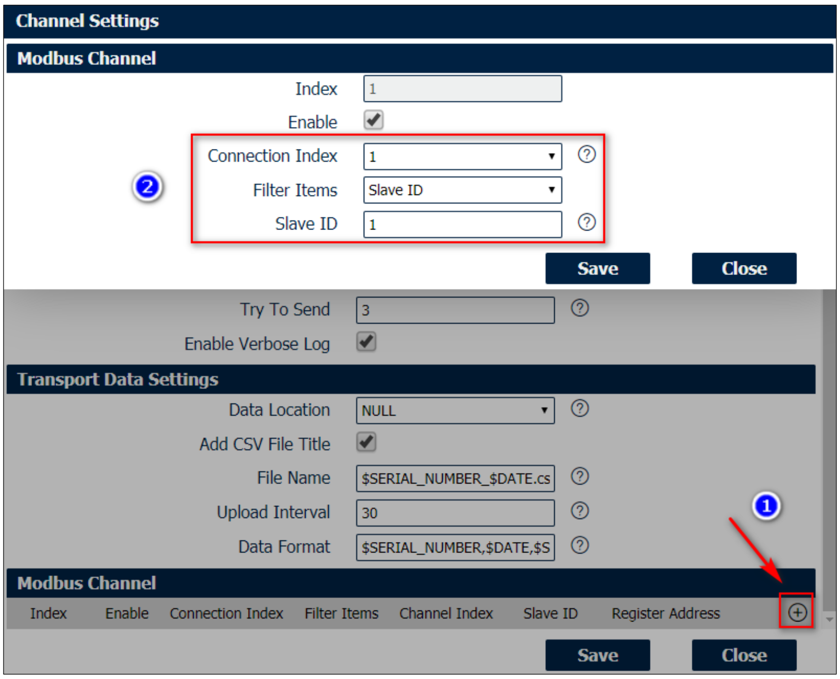
Transport Data Settings

Data Location	NULL
Add CSV File Title	☑
File Name	$SERIAL_NUMBER_$DATE.cs
Upload Interval	30
Data Format	$SERIAL_NUMBER,$DATE,$S

Figure 323 – Configuring a connection via FTP (1)

In the **File Name** and **Data Format** parameters, you can enter the desired format or set it as default.

Next, the **Modbus Channel** parameter must be enabled. The Modbus Master will select the value sent to the remote FTP server from the Modbus slave.



Channel Settings

Modbus Channel

Index	1
Enable	☑
Connection Index	1
Filter Items	Slave ID
Slave ID	1

Try To Send	3
Enable Verbose Log	☑

Transport Data Settings

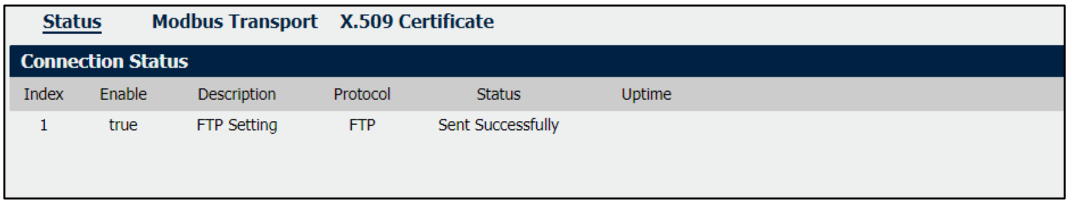
Data Location	NULL
Add CSV File Title	☑
File Name	$SERIAL_NUMBER_$DATE.cs
Upload Interval	30
Data Format	$SERIAL_NUMBER,$DATE,$S

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 324 – Configuring a connection via FTP (2)

Once this is done, simply click **Save > Save > Apply** and proceed to **Application > Modbus Transport > Status** to verify that the device has successfully connected to the remote server via FTP protocol:

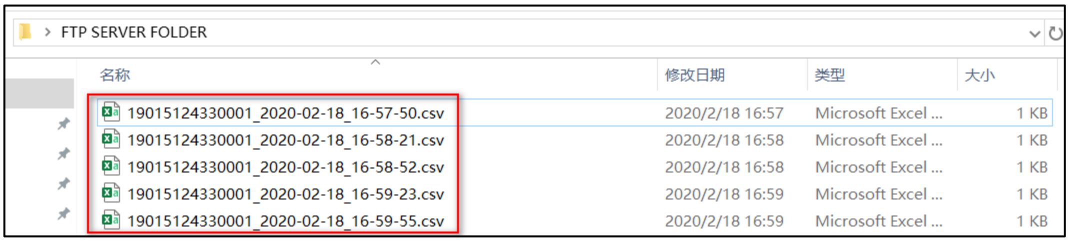


Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true	FTP Setting	FTP	Sent Successfully	

Figure 325 – FTP status connection

In this case, the remote FTP server received the data successfully, as shown in the figure below:



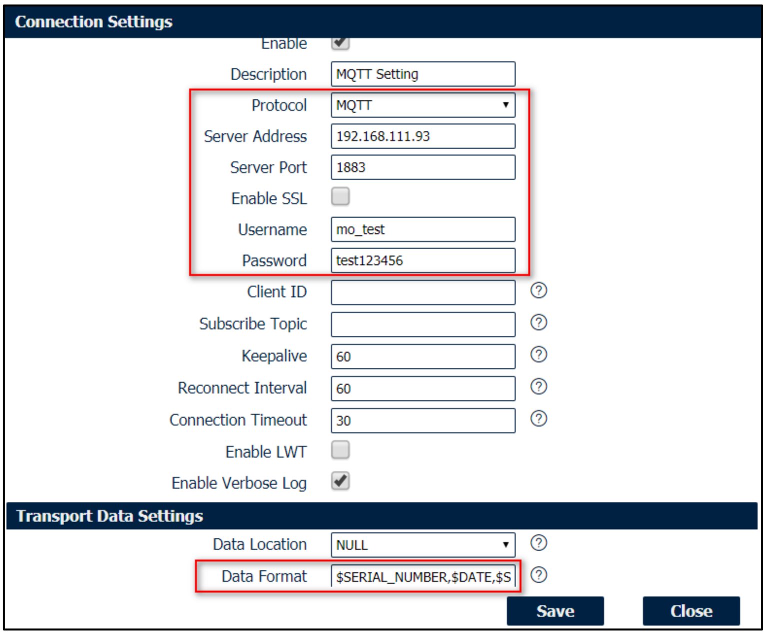
名称	修改日期	类型	大小
19015124330001_2020-02-18_16-57-50.csv	2020/2/18 16:57	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-58-21.csv	2020/2/18 16:58	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-58-52.csv	2020/2/18 16:58	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-59-23.csv	2020/2/18 16:59	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-59-55.csv	2020/2/18 16:59	Microsoft Excel ...	1 KB

Figure 326 – FTP server receiving data

7.20.4 TRANSPORT VIA MQTT

To configure the device to perform data transport via FTP, you must observe the CONFIGURATION ON MODBUS SLAVE and CONFIGURATION ON MODBUS POLL sections of this chapter.

Once this is done, you must open the **AirGate 4G Wi-Fi** web interface and follow the path **Application > Modbus Transport > Modbus Transport**. Then it is necessary to add a new connection, inform the protocol to be used in the **Protocol** parameter, the IP address of the MQTT Broker in the **Server Address** parameter, the port to send the data to the FTP server in the **Server Port** parameter and the user and password in the **Username** and **Password** parameters, as shown in the figure below:



Connection Settings

Enable ☑

Description: MQTT Setting

Protocol: MQTT

Server Address: 192.168.111.93

Server Port: 1883

Enable SSL □

Username: mo_test

Password: test123456

Client ID:

Subscribe Topic:

Keepalive: 60

Reconnect Interval: 60

Connection Timeout: 30

Enable LWT □

Enable Verbose Log ☑

Transport Data Settings

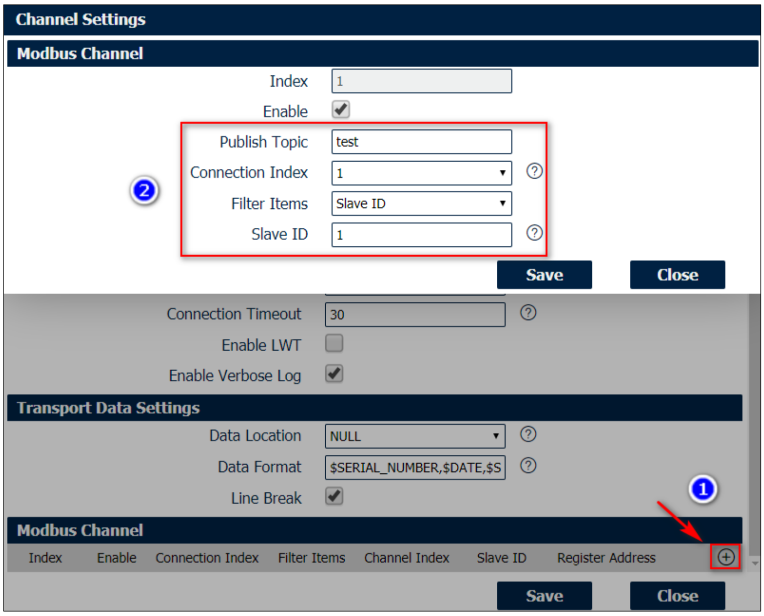
Data Location: NULL

Data Format: $SERIAL_NUMBER,$DATE,$S

Figure 327 – Configuring a connection via MQTT (1)

In the **Data Format** parameter, you can enter the desired format or set it as default.

Once this is done, you need to access the **Channel List** section and configure the **Publish Topic** parameter so that the MQTT Broker can publish the data.



Channel Settings

Modbus Channel

Index: 1

Enable ☑

Publish Topic: test

Connection Index: 1

Filter Items: Slave ID

Slave ID: 1

Connection Timeout: 30

Enable LWT □

Enable Verbose Log ☑

Transport Data Settings

Data Location: NULL

Data Format: $SERIAL_NUMBER,$DATE,$S

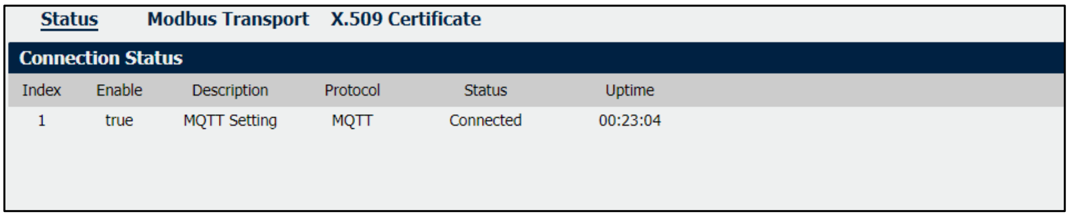
Line Break ☑

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Figure 328 – Configuring a connection via MQTT (2)

Once this is done, just click **Save > Save > Apply** and go to **Application > Modbus Transport > Status** to check if the device has successfully connected to the MQTT Broker:

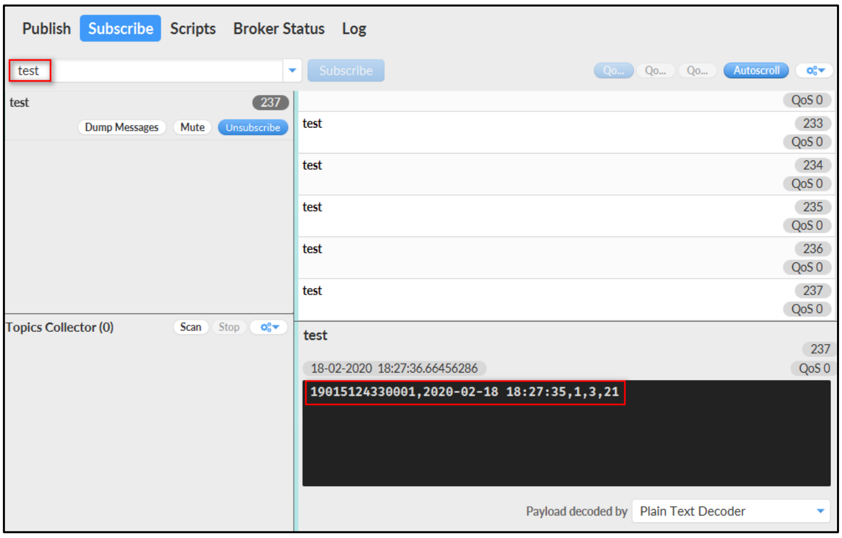


Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true	MQTT Setting	MQTT	Connected	00:23:04

Figure 329 – MQTT connection status

You need to run the MQTT Client (MQTT Subscriber) to access the topic you just published:



test

test 237

test 233 QoS 0

test 234 QoS 0

test 235 QoS 0

test 236 QoS 0

test 237 QoS 0

test 237

18-02-2020 18:27:36.66456286 QoS 0

```
19015124330001,2020-02-18 18:27:35,1,3,21
```

Payload decoded by Plain Text Decoder

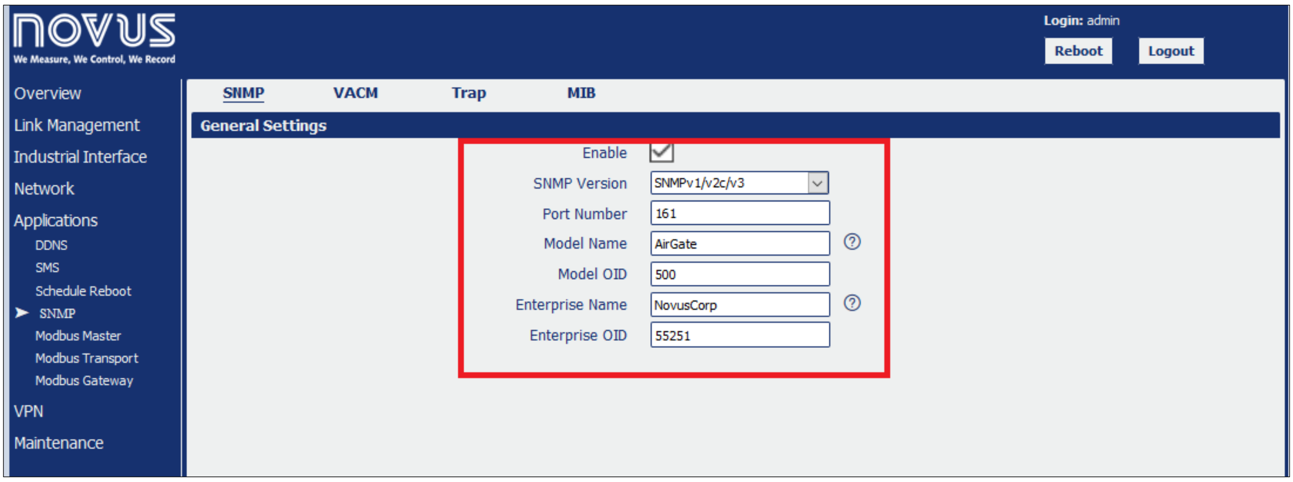
Figure 330 – MQTT client

7.21 CONFIGURING SNMP AND MG MIBBROWSER SOFTWARE

This tutorial contains information on how to configure SNMP protocol and MG MibBrowser software.

7.21.1 CONFIGURING AIRGATE 4G WI-FI

To configure the SNMP protocol, you must open the **AirGate 4G Wi-Fi** web interface, locate the **Applications** option on the left menu, and then click on **SNMP**, as shown in the figure below:



General Settings

Enable ☑

SNMP Version: SNMPv1/v2c/v3

Port Number: 161

Model Name: AirGate

Model OID: 500

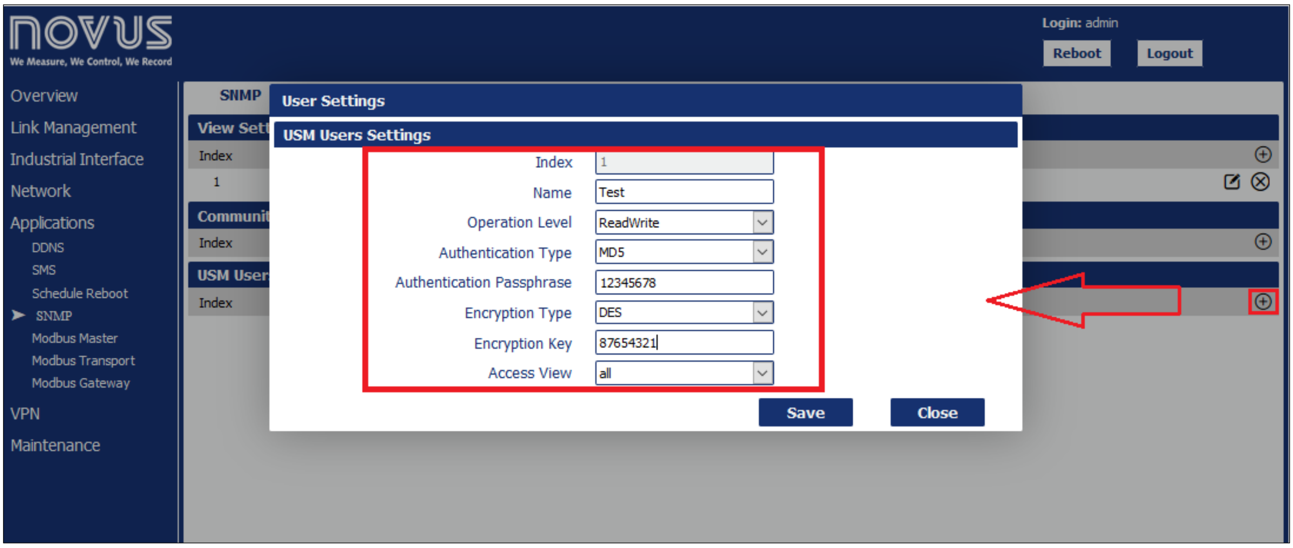
Enterprise Name: NovusCorp

Enterprise OID: 55251

Figure 331 – Configuring SNMP

After that, click **Save** > **Apply** and follow the path **Applications** > **SNMP** > **VACM**, using the default settings in the **View Settings** section and ignoring the community settings.

In the **USM Users Settings** section, apply the following settings:



User Settings

USM Users Settings

Index: 1

Name: Test

Operation Level: ReadWrite

Authentication Type: MD5

Authentication Passphrase: 12345678

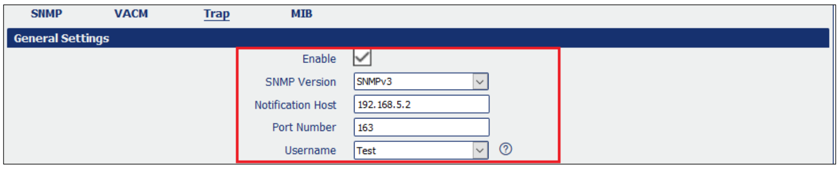
Encryption Type: DES

Encryption Key: 87654321

Access View: all

Figure 332 – Configuring a USM user

Once the configuration is done, click **Save** > **Apply** and follow the path **Applications** > **SNMP** > **Trap** to enable the sending of Traps and insert the IP of the destination computer, responsible for receiving the notifications. You must use the port as configured in the auxiliary software.



General Settings

Enable ☑

SNMP Version: SNMPv3

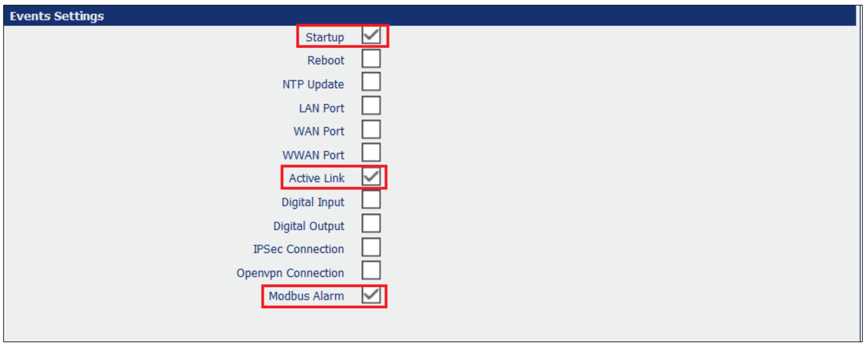
Notification Host: 192.168.5.2

Port Number: 163

Username: Test

Figure 333 – Configuring a Trap

You must select the event notifications to be received via Trap:



Events Settings

Startup ☑

Reboot □

NTP Update □

LAN Port □

WAN Port □

WWAN Port □

Active Link ☑

Digital Input □

Digital Output □

IPSec Connection □

Openvpn Connection □

Modbus Alarm ☑

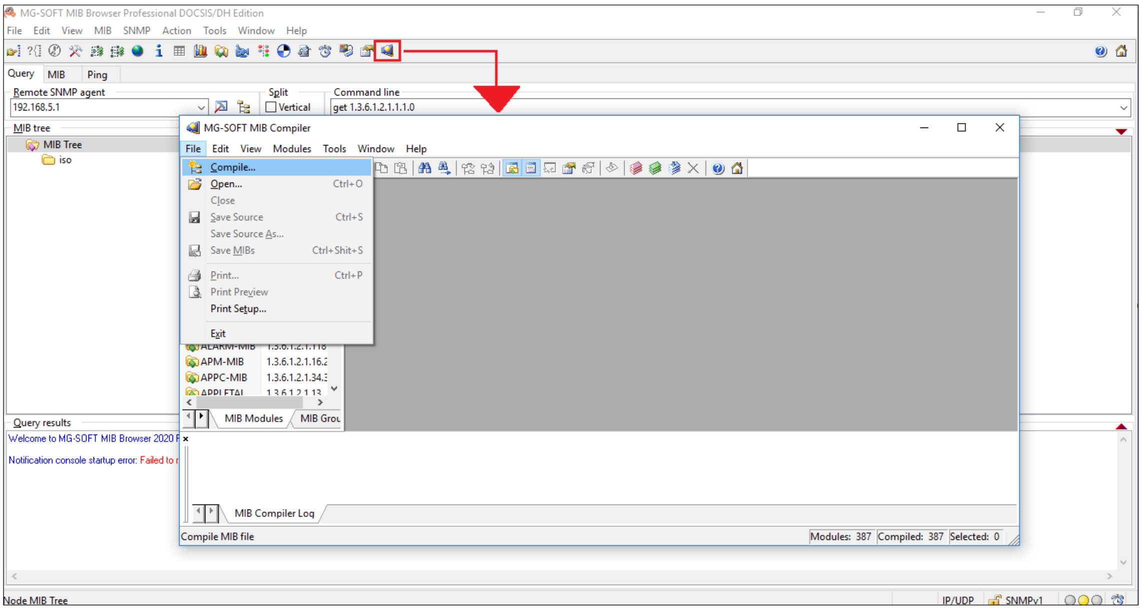
Figure 334 – Event notifications

Then click **Save > Apply** and follow the path **Applications > SNMP > MIB** to download the MIB files, unzipping the folder on your computer.

7.21.2 CONFIGURING "MG MibBrowser" SOFTWARE

After unpacking the browser package, you must install all the files indicated in the MG MibBrowser software installer.

In the MG-SOFT MIB Browser folder, you must open the **MIB Browser** shortcut. Then, in the software interface, click the button indicated below to open the **MIB Compiler**:



Remote SNMP agent: 192.168.5.1

Command line: get 1.3.6.1.2.1.1.1.0

ALARM-MIB	1.3.6.1.2.1.118
APM-MIB	1.3.6.1.2.1.16.2
APPC-MIB	1.3.6.1.2.1.34.3
APPLETAL	1.3.6.1.2.1.13

Welcome to MG-SOFT MIB Browser 2020 P

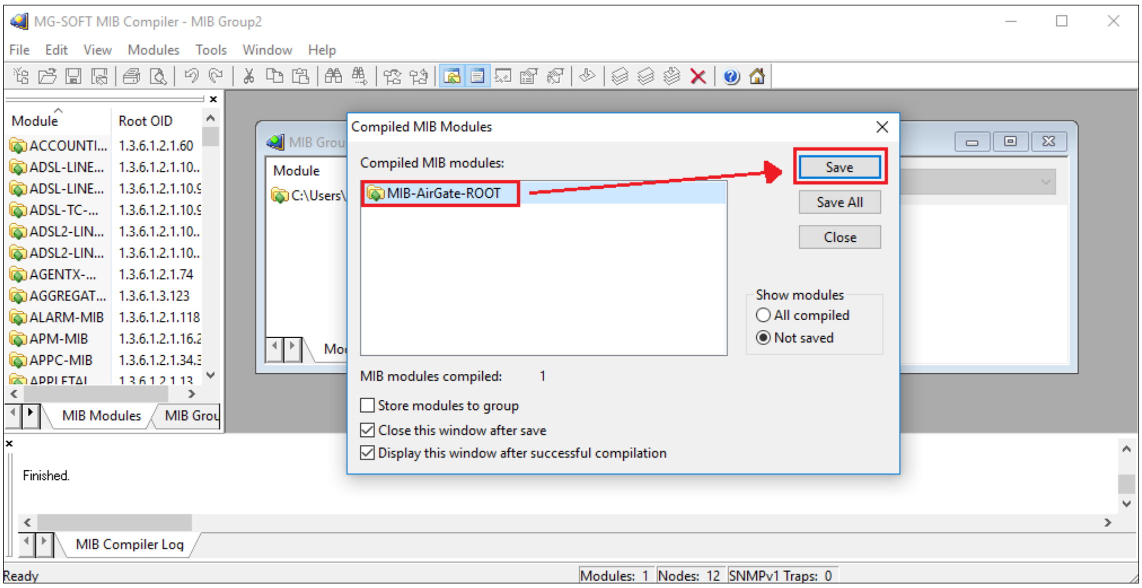
Notification console startup error: Failed to r

Compile MIB file

Modules: 387 Compiled: 387 Selected: 0

Figure 335 – MIB compiler

After that, click **File** > **Compile** and then select the MIB files "SNMP-ROOT.mib", "SNMO-TRAP.mib" and "SNMP-VALUES.mib" downloaded from **AirGate 4G Wi-Fi**. When the compilation process is over, click **Save** and again **Save** to integrate MIB into the software library:



Module	Root OID
ACCOUNTI...	1.3.6.1.2.1.60
ADSL-LINE...	1.3.6.1.2.1.10..
ADSL-LINE...	1.3.6.1.2.1.10.9
ADSL-TC-...	1.3.6.1.2.1.10.9
ADSL2-LIN...	1.3.6.1.2.1.10..
ADSL2-LIN...	1.3.6.1.2.1.10..
AGENTX-...	1.3.6.1.2.1.74
AGGREGAT...	1.3.6.1.3.123
ALARM-MIB	1.3.6.1.2.1.118
APM-MIB	1.3.6.1.2.1.16.2
APPC-MIB	1.3.6.1.2.1.34.3
APPLETAL	1.3.6.1.2.1.13

Module: C:\Users\

Compiled MIB modules:

MIB-AirGate-ROOT

Show modules
○ All compiled
● Not saved

MIB modules compiled: 1

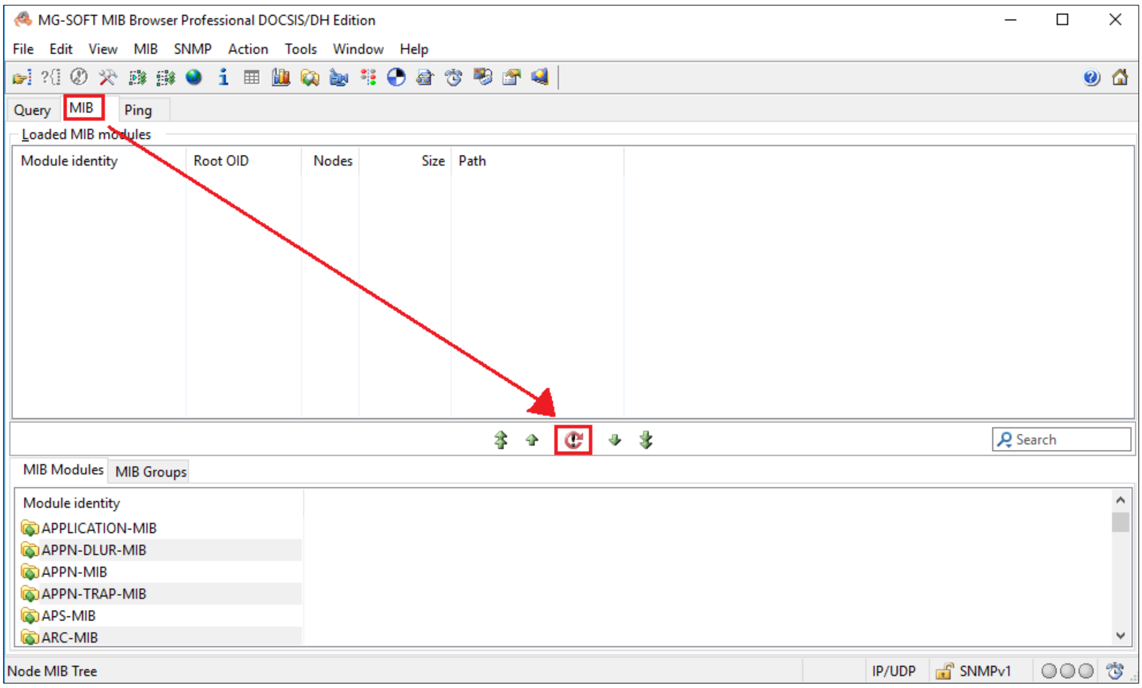
☐ Store modules to group
☑ Close this window after save
☑ Display this window after successful compilation

Finished.

Ready Modules: 1 Nodes: 12 SNMPv1 Traps: 0

Figure 336 – Saving compiled files

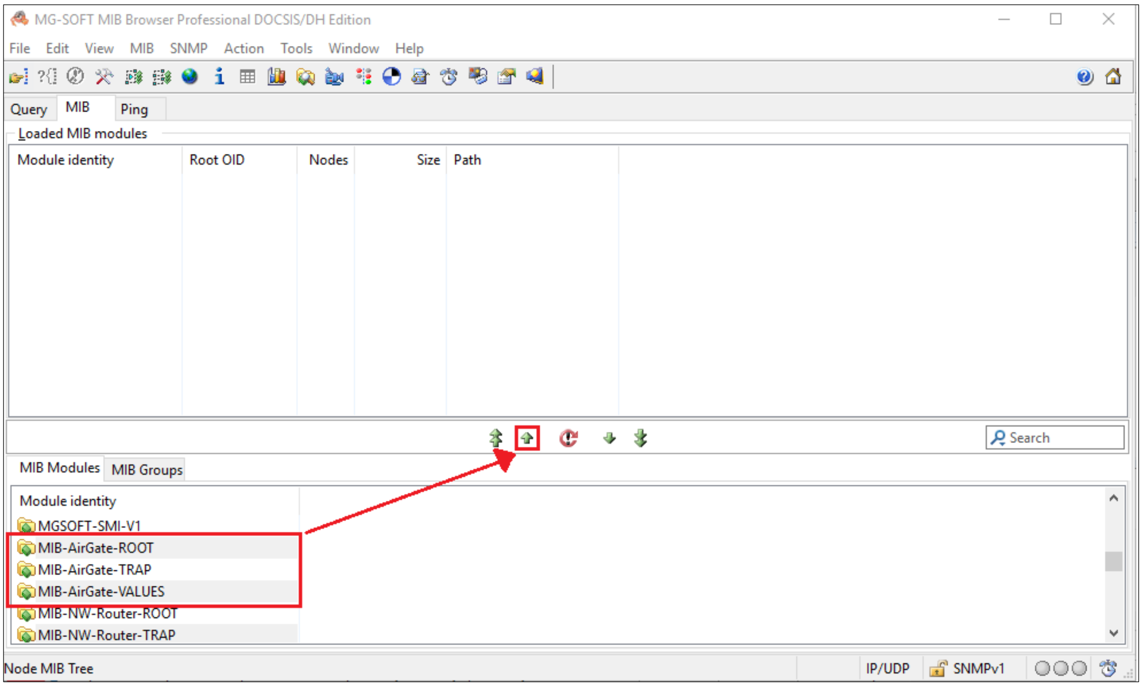
After the compilations are done, you must return to the MibBrowser software, click on **MIB** and then on the update button to update the library MIB files, as shown in the figure below:


MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
Query MIB Ping
Loaded MIB modules
Module identity Root OID Nodes Size Path
Search
MIB Modules MIB Groups
Node MIB Tree
IP/UDP SNMPv1

Module identity
APPLICATION-MIB
APPN-DLUR-MIB
APPN-MIB
APPN-TRAP-MIB
APS-MIB
ARC-MIB

Figure 337 – Updating the library

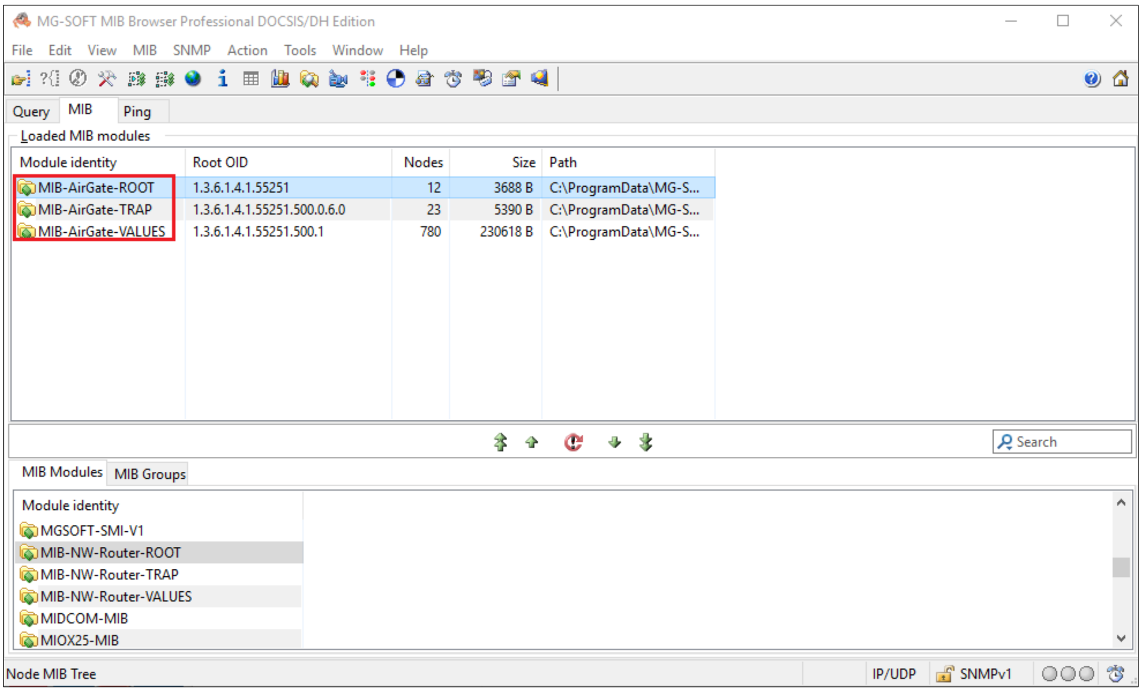
Next, browse the **AirGate 4G Wi-Fi** files in the list of **MIB Modules** and click the button as shown below to load them into the software:


MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
Query MIB Ping
Loaded MIB modules
Module identity Root OID Nodes Size Path
Search
MIB Modules MIB Groups
Node MIB Tree
IP/UDP SNMPv1

Module identity
MGSOFT-SMI-V1
MIB-AirGate-ROOT
MIB-AirGate-TRAP
MIB-AirGate-VALUES
MIB-NW-Router-ROOT
MIB-NW-Router-TRAP

Figure 338 – Uploading files

The MIB files will be displayed as follows:


MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
Query MIB Ping
Loaded MIB modules

Module identity	Root OID	Nodes	Size	Path
MIB-AirGate-ROOT	1.3.6.1.4.1.55251	12	3688 B	C:\ProgramData\MG-S...
MIB-AirGate-TRAP	1.3.6.1.4.1.55251.500.0.6.0	23	5390 B	C:\ProgramData\MG-S...
MIB-AirGate-VALUES	1.3.6.1.4.1.55251.500.1	780	230618 B	C:\ProgramData\MG-S...

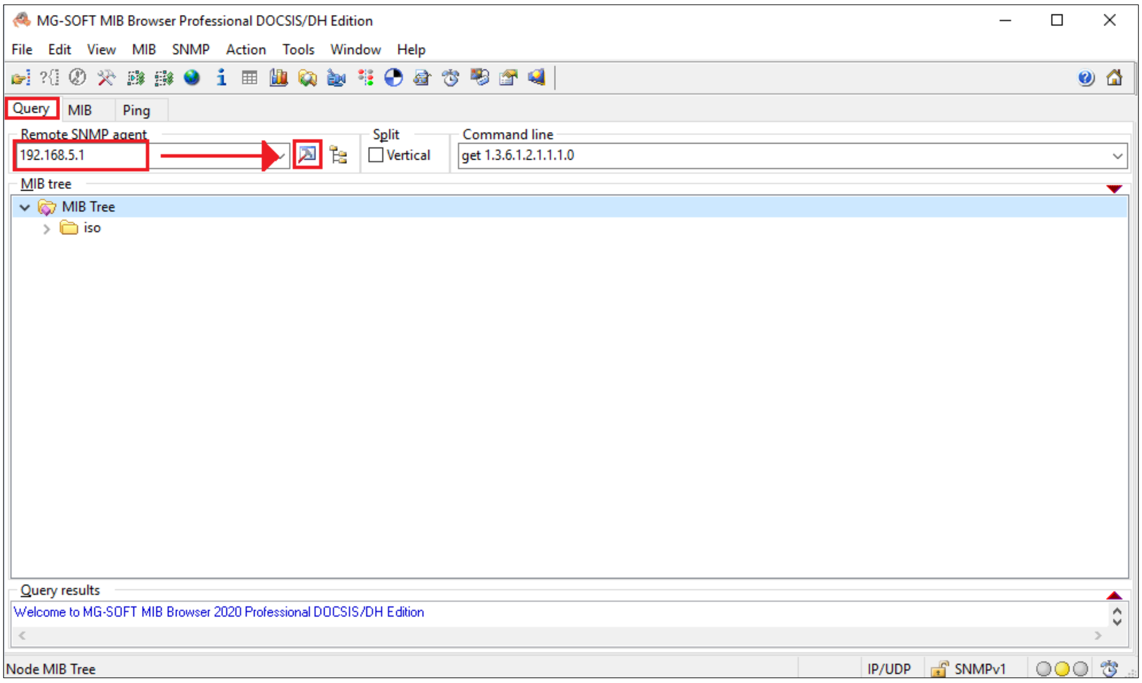
Search
MIB Modules MIB Groups

Module identity
MGSOFT-SMI-V1
MIB-NW-Router-ROOT
MIB-NW-Router-TRAP
MIB-NW-Router-VALUES
MIDCOM-MIB
MIOX25-MIB

Node MIB Tree
IP/UDP
SNMPv1

Figure 339 – Viewing the files

After uploading the files, click **Query**, select the **AirGate 4G Wi-Fi IP** address (in this case 192.168.5.1) and then click the preferences button of the protocol:


MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
Query MIB Ping

Remote SNMP agent: 192.168.5.1

Split: □ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

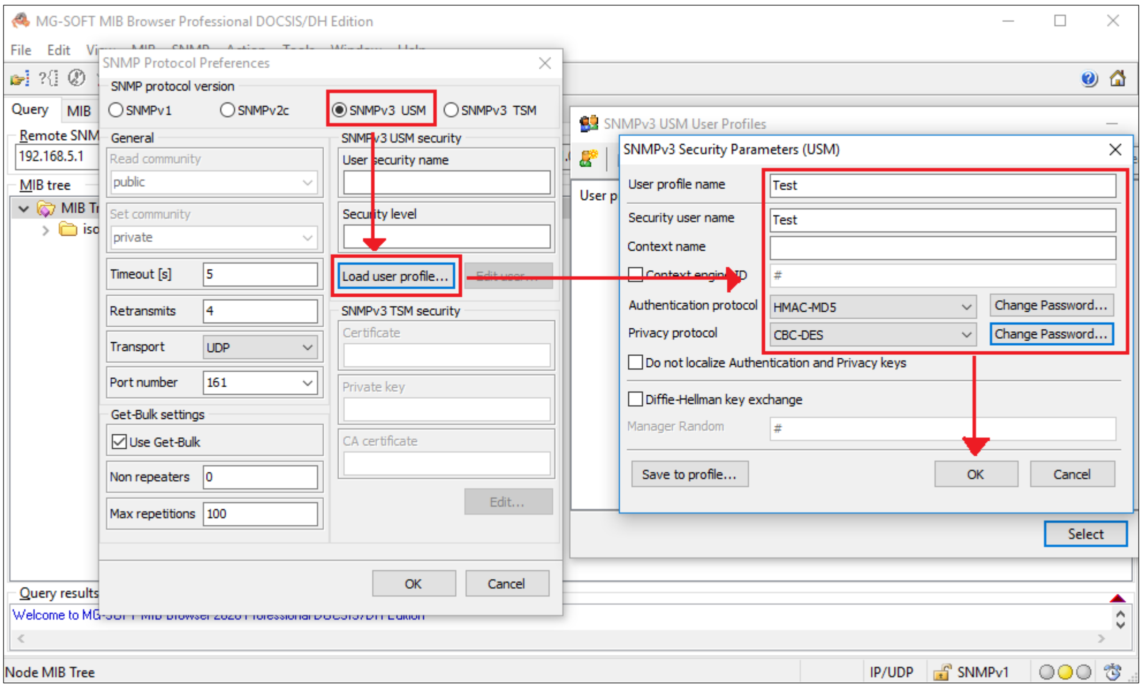
MIB tree
MIB Tree
iso
Query results

Welcome to MG-SOFT MIB Browser 2020 Professional DOCSIS/DH Edition

Node MIB Tree
IP/UDP
SNMPv1

Figure 340 – Query

In the preferences window, you must select the **SNMPv3 USM** protocol. In the **Load user profile** parameter, add the user settings as configured in the **USM Users Settings** section (see the USM USER SETTINGS section of the APPLICATIONS chapter).



SNMP protocol version: ○ SNMPv1 ○ SNMPv2c ● SNMPv3 USM ○ SNMPv3 TSM

General: Read community: public; Set community: private; Timeout [s]: 5; Retransmits: 4; Transport: UDP; Port number: 161

Get-Bulk settings: ☑ Use Get-Bulk; Non repeaters: 0; Max repetitions: 100

SNMPv3 Security Parameters (USM)

User profile name: Test

Security user name: Test

Context name:

□ Context engine ID: #

Authentication protocol: HMAC-MD5

Privacy protocol: CBC-DES

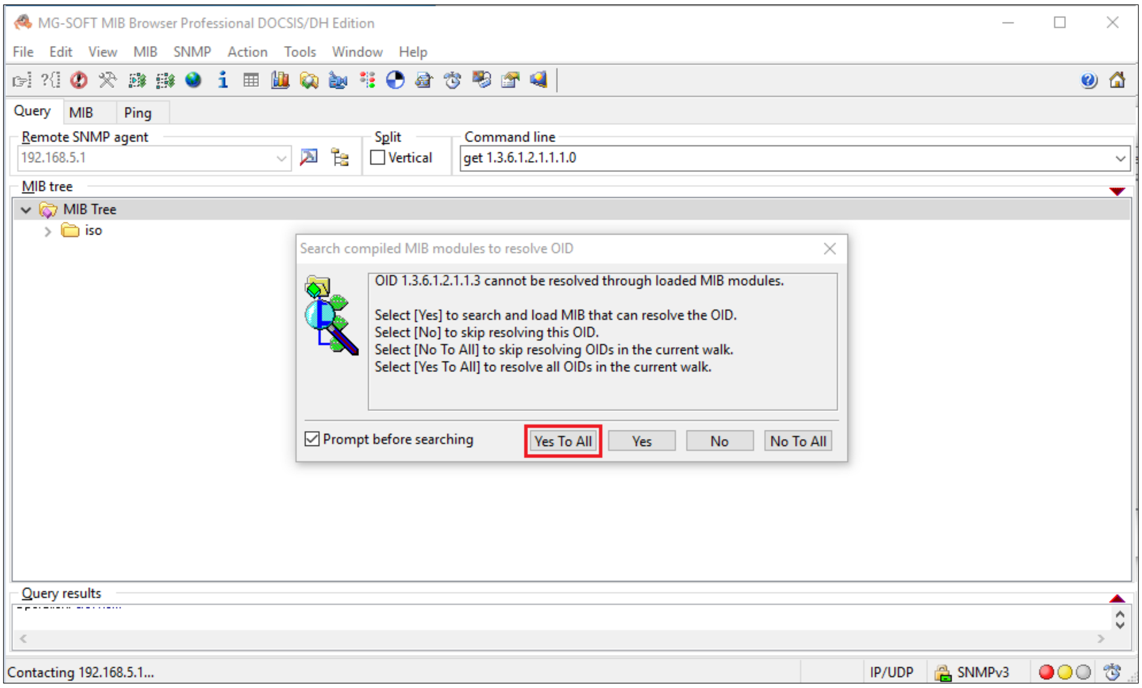
□ Do not localize Authentication and Privacy keys

□ Diffie-Hellman key exchange

Manager Random: #

Figure 341 – Configuring the user profile (1)

Once you have done this, click **Yes to All**:



MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
Query MIB Ping
MIB Tree
iso
Search compiled MIB modules to resolve OID
Yes To All
Yes
No
No To All
IP/UDP
SNMPv3

Remote SNMP agent: 192.168.5.1

Split: □ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

OID 1.3.6.1.2.1.1.3 cannot be resolved through loaded MIB modules.

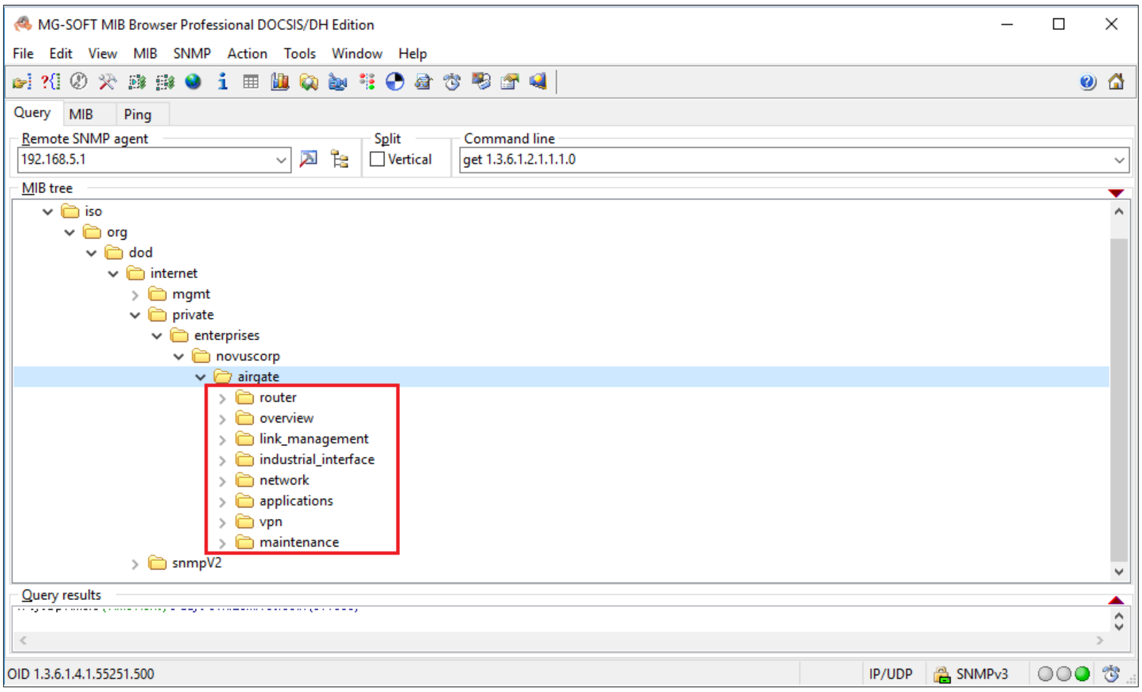
Select [Yes] to search and load MIB that can resolve the OID.
Select [No] to skip resolving this OID.
Select [No To All] to skip resolving OIDs in the current walk.
Select [Yes To All] to resolve all OIDs in the current walk.

☑ Prompt before searching

Contacting 192.168.5.1...

Figure 342 – Configuring the user profile (2)

At the end of this process, you will be able to access the **AirGate 4G Wi-Fi** menu:



Remote SNMP agent: 192.168.5.1

Command line: get 1.3.6.1.2.1.1.1.0

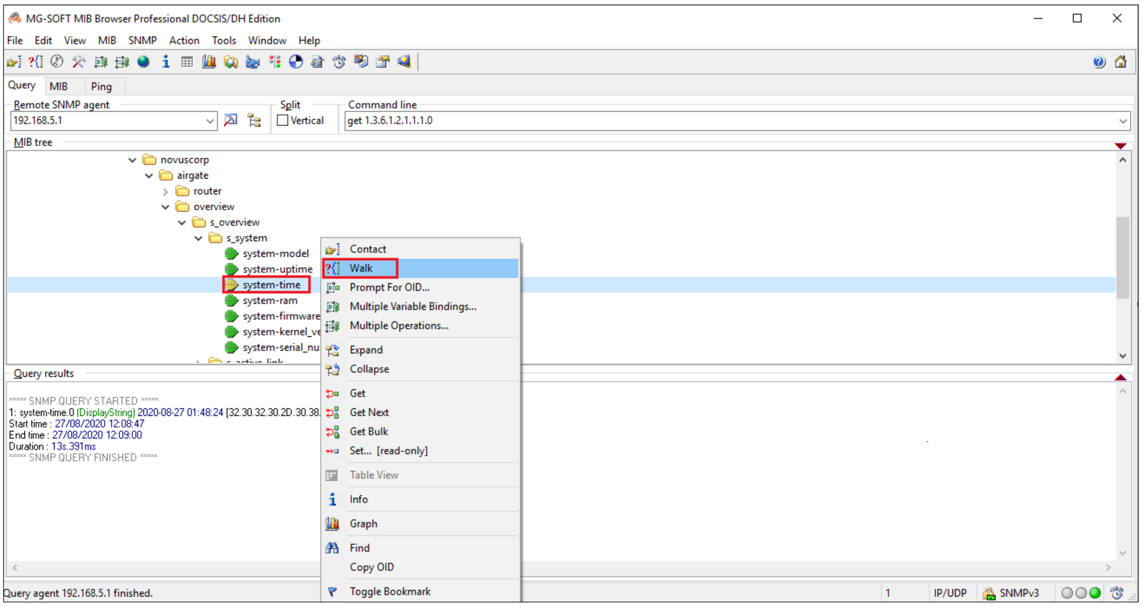
OID 1.3.6.1.4.1.55251.500

Figure 343 – Device menu

7.21.3 TEST

7.21.3.1 MONITORING THE ROUTER STATYS

To check the **System Time** parameter of the router, you must navigate to the **system-time** option of the software and right click on it, selecting the **Walk** option, as shown below:



Remote SNMP agent: 192.168.5.1

Command line: get 1.3.6.1.2.1.1.1.0

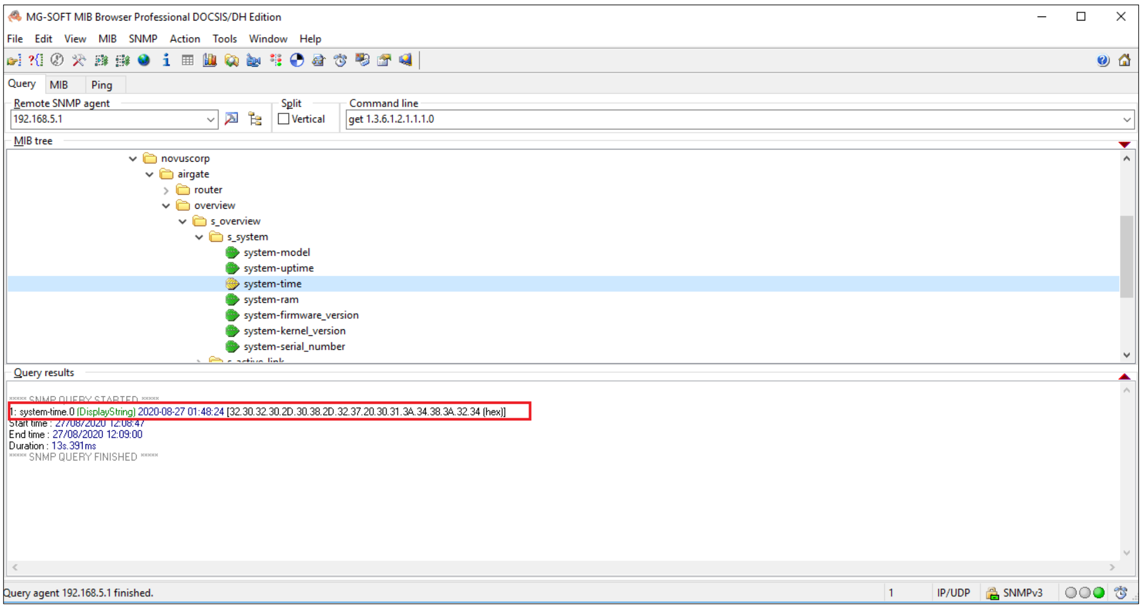
Query results

```
***** SNMP QUERY STARTED *****
1: system-time.0 (DisplayString) 2020-08-27 01:48:24 [32.30.32.30.2D.30.38.
Start time : 27/08/2020 12:08:47
End time : 27/08/2020 12:09:00
Duration : 13s.391ms
***** SNMP QUERY FINISHED *****
```

Query agent 192.168.5.1 finished.

Figure 344 – System date and time **(1)**

Once this is done, it will be possible to view the system information, made available by the router:



Remote SNMP agent: 192.168.5.1

Command line: get 1.3.6.1.2.1.1.1.0

Query results

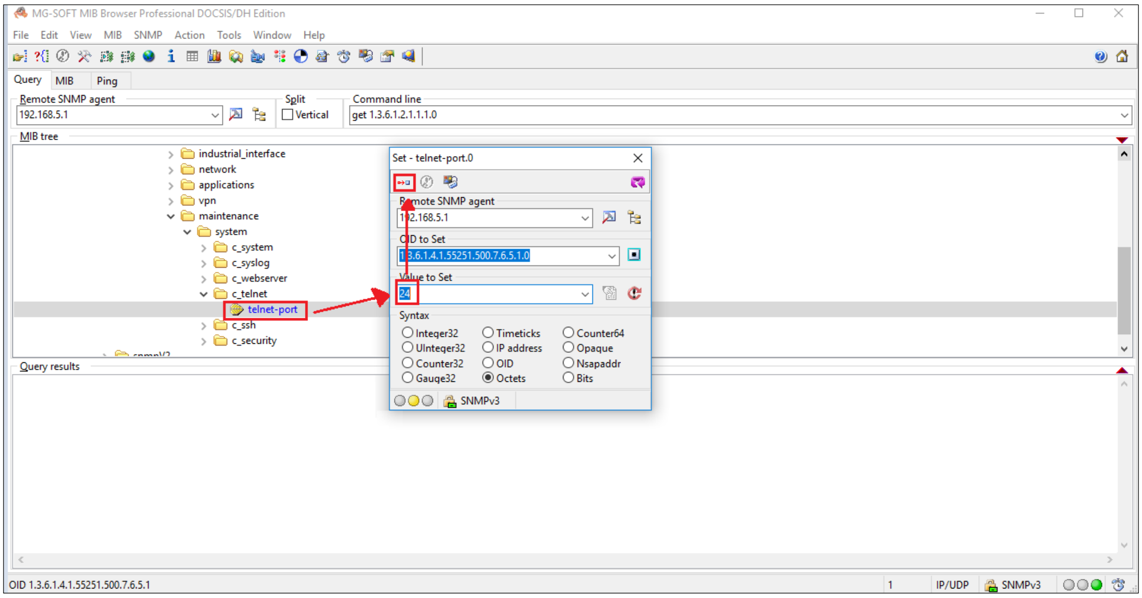
```
***** SNMP QUERY STARTED *****
1: system-time.0 (DisplayString) 2020-08-27 01:48:24 [32.30.32.30.2D.30.38.2D.32.37.20.30.31.3A.34.38.3A.32.34 (hex)]
Start time : 27/08/2020 12:08:47
End time : 27/08/2020 12:09:00
Duration : 13s.391ms
***** SNMP QUERY FINISHED *****
```

Query agent 192.168.5.1 finished.

Figure 345 – System date and time **(2)**

7.21.3.2 CONTROLLING THE ROUTER

To modify the configuration port of the Telnet protocol, you must navigate to the **telnet-port** option of the software and right click on it, selecting the **Set** option. After that, configure the port to 24 and send to the router:



Remote SNMP agent: 192.168.5.1

Split: □ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

Set - telnet-port.0

Remote SNMP agent: 192.168.5.1

OID to Set: 1.3.6.1.4.1.55251.500.7.6.5.1.0

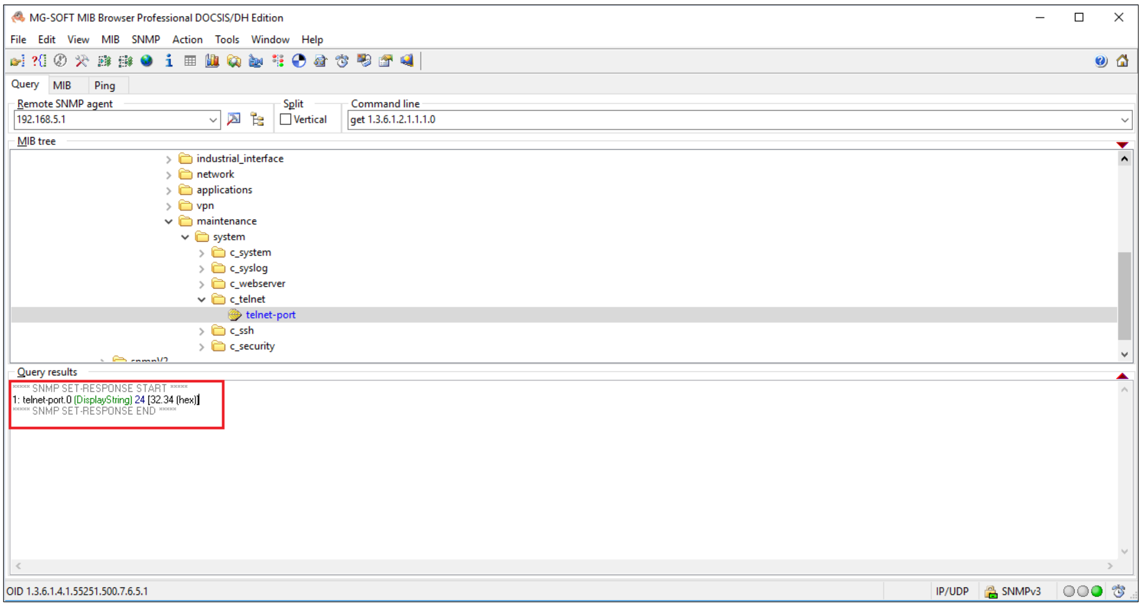
Value to Set: 24

Syntax:
○ Integer32 ○ Timeticks ○ Counter64
○ UInteger32 ○ IP address ○ Opaque
○ Counter32 ○ OID ○ Nsapaddr
○ Gauge32 ● Octets ○ Bits

OID 1.3.6.1.4.1.55251.500.7.6.5.1

Figure 346 – Configuring the Telnet protocol (1)

You can check if the data sending was successful in the screen below:



Remote SNMP agent: 192.168.5.1

Split: □ Vertical

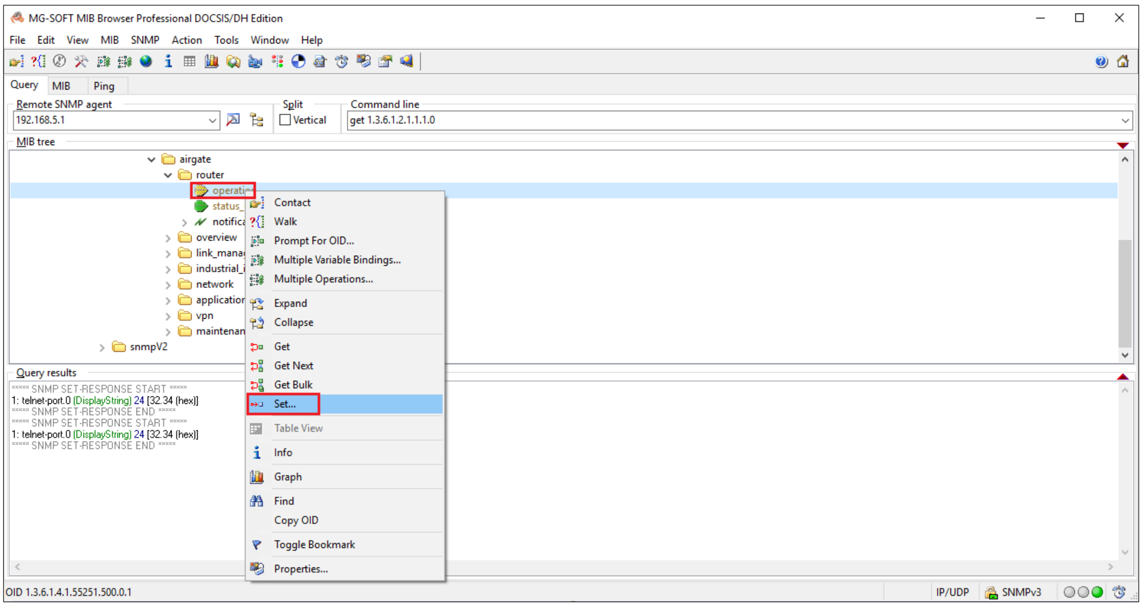
Command line: get 1.3.6.1.2.1.1.1.0

```
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
```

OID 1.3.6.1.4.1.55251.500.7.6.5.1

Figure 347 – Configuring the Telnet protocol (2)

After sending the configuration, you must click **Save** and **Apply**. To do so, you must navigate to the **Operation** option, then right-click on it and select the **Set** option:



Remote SNMP agent: 192.168.5.1

Split: □ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

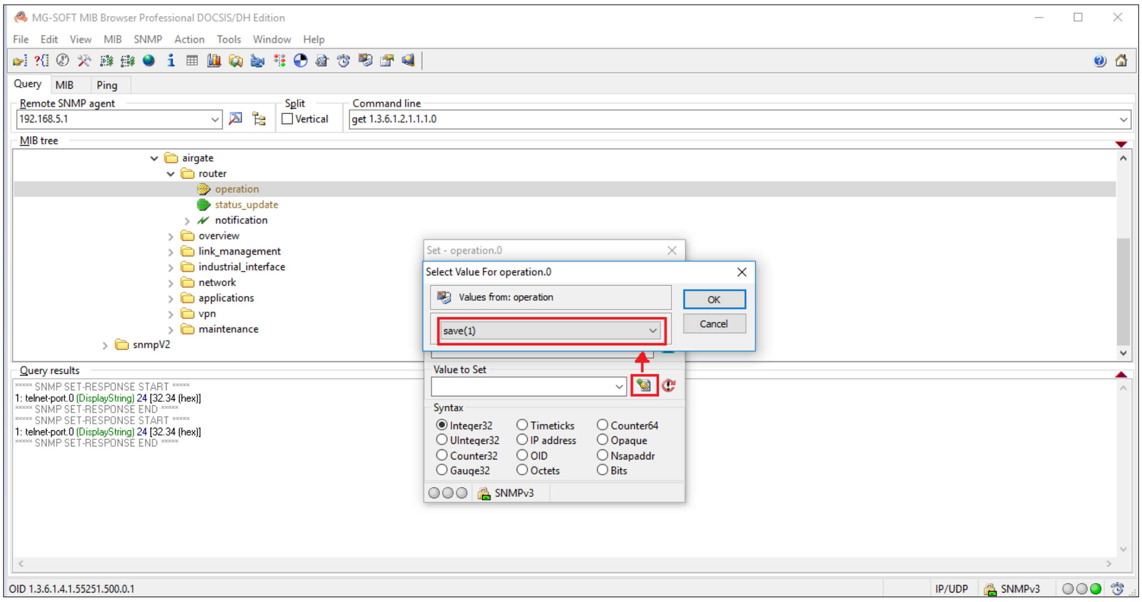
Query results

```
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
```

OID 1.3.6.1.4.1.55251.500.0.1

Figure 348 – Applying a configuration (1)

Next, click on the button indicated in the figure below, select the **Save** option and click **Ok** to send the configuration to the router. Then, repeat the same operation, but selecting the **Apply** option:



Remote SNMP agent: 192.168.5.1

Split: □ Vertical

Command line: get 1.3.6.1.2.1.1.1.0

Select Value For operation.0

Values from: operation

save(1)

Value to Set:

Syntax: ● Integer32 ○ Timeticks ○ Counter64 ○ UInteger32 ○ IP address ○ Opaque ○ Counter32 ○ OID ○ Nsapaddr ○ Gauge32 ○ Octets ○ Bits

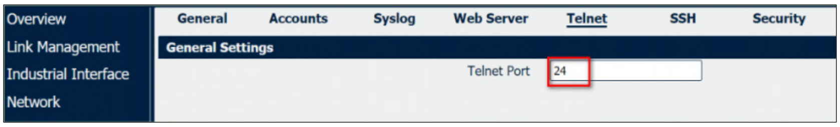
Query results

```
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
```

OID 1.3.6.1.4.1.55251.500.0.1

Figure 349 – Applying a configuration (2)

After that, in the web interface of the device, you can check if the Telnet protocol port was set to 24:



General Settings

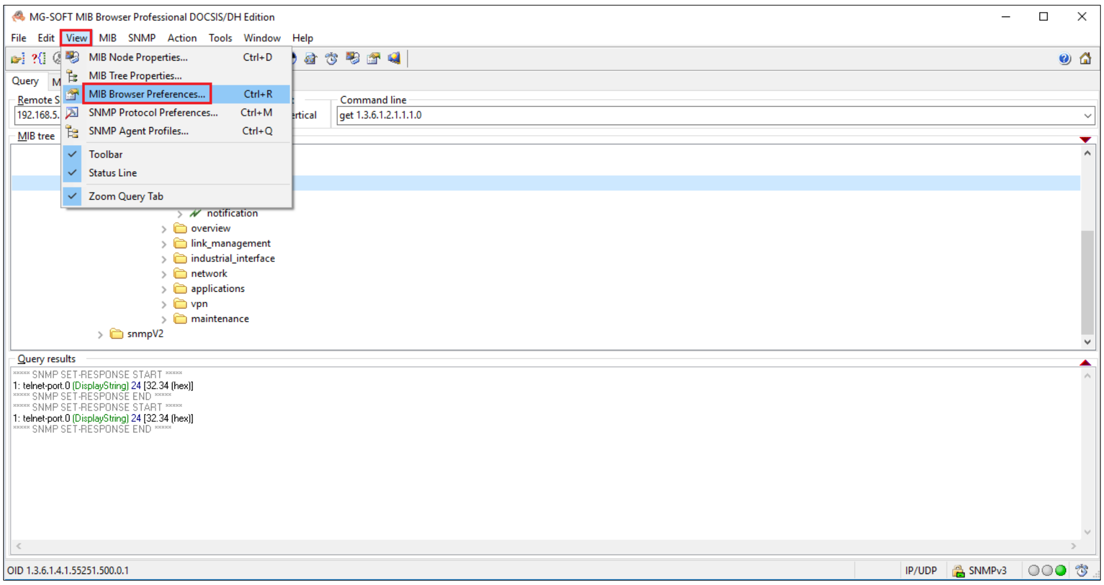
Telnet Port: 24

Figure 350 – Telnet protocol in the web interface

The test was successfully performed.

7.21.3.3 SNMP TRAP NOTIFICATION

To perform SNMP Trap tests, you must configure the UDP transport and select port 163, as shown in the next two figures below:


MG-SOFT MIB Browser Professional DOCSIS/DH Edition
File Edit View MIB SNMP Action Tools Window Help
MIB Node Properties... Ctrl+D
MIB Tree Properties...
MIB Browser Preferences... Ctrl+R
SNMP Protocol Preferences... Ctrl+M
SNMP Agent Profiles... Ctrl+Q
Toolbar
Status Line
Zoom Query Tab
Query
Remote S
MIB tree
Command line
notification
overview
link_management
industrial_interface
network
applications
vpn
maintenance
snmpV2
Query results
IP/UDP
SNMPv3

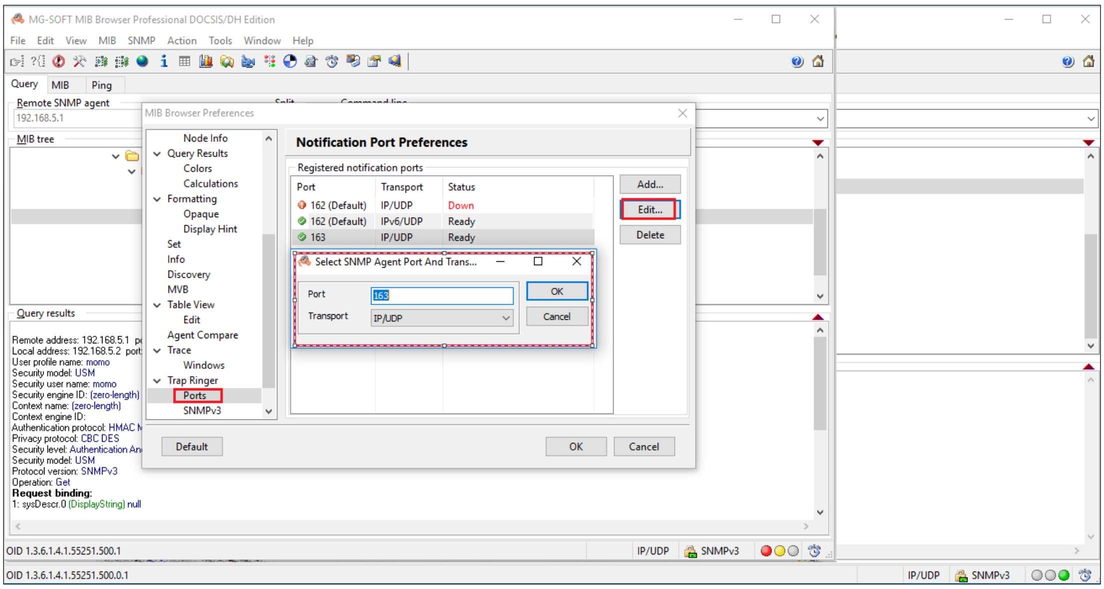
192.168.5.

get 1.3.6.1.2.1.1.1.0

```
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: telnet-port.0 (DisplayString) 24 [32.34 (hex)]
***** SNMP SET-RESPONSE END *****
```

OID 1.3.6.1.4.1.55251.500.0.1

Figure 351 – Configuring UDP transport (1)



192.168.5.1

Port	Transport	Status
162 (Default)	IP/UDP	Down
162 (Default)	IPv6/UDP	Ready
163	IP/UDP	Ready

Port: 163

Transport: IP/UDP

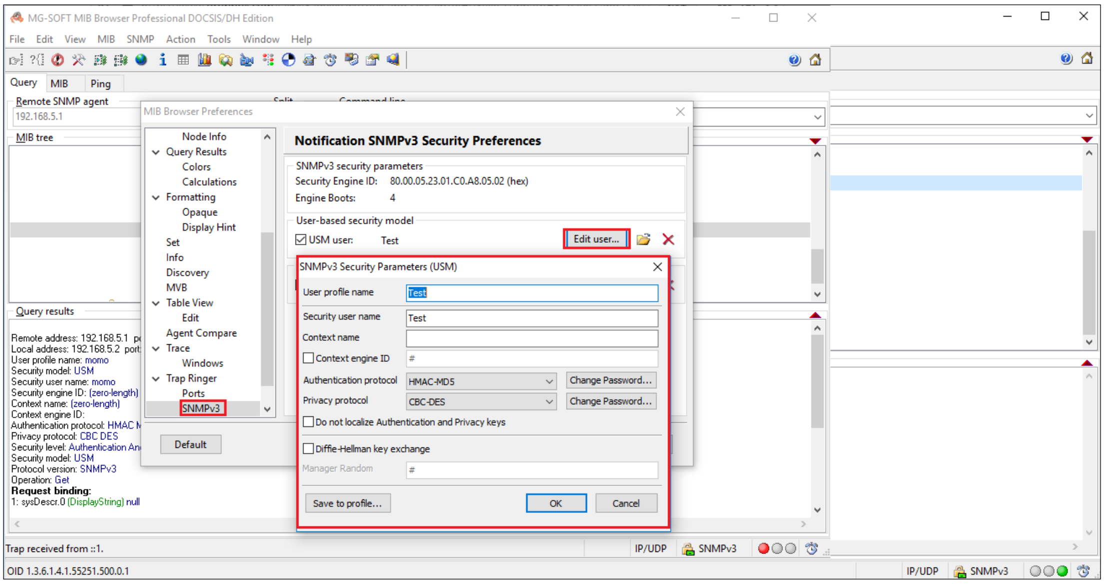
```
Remote address: 192.168.5.1  p
Local address: 192.168.5.2  port
User profile name: momo
Security model: USM
Security user name: momo
Security engine ID: (zero-length)
Context name: (zero-length)
Context engine ID:
Authentication protocol: HMAC M
Privacy protocol: CBC DES
Security level: Authentication An
Security model: USM
Protocol version: SNMPv3
Operation: Get
Request binding:
1: sysDescr.0 (DisplayString) null
```

OID 1.3.6.1.4.1.55251.500.1

OID 1.3.6.1.4.1.55251.500.0.1

Figure 352 – Configuring UDP transport (2)

After configuring the port, you must add the user settings as configured in the **USM Users Settings** section (see the USM USER SETTINGS section of the APPLICATIONS chapter).



192.168.5.1

Security Engine ID: 80.00.05.23.01.C0.A8.05.02 (hex)

Engine Boots: 4

☑ USM user: Test

User profile name: Test

Security user name: Test

Context name:

□ Context engine ID: #

Authentication protocol: HMAC-MD5

Privacy protocol: CBC-DES

□ Do not localize Authentication and Privacy keys

□ Diffie-Hellman key exchange

Manager Random: #

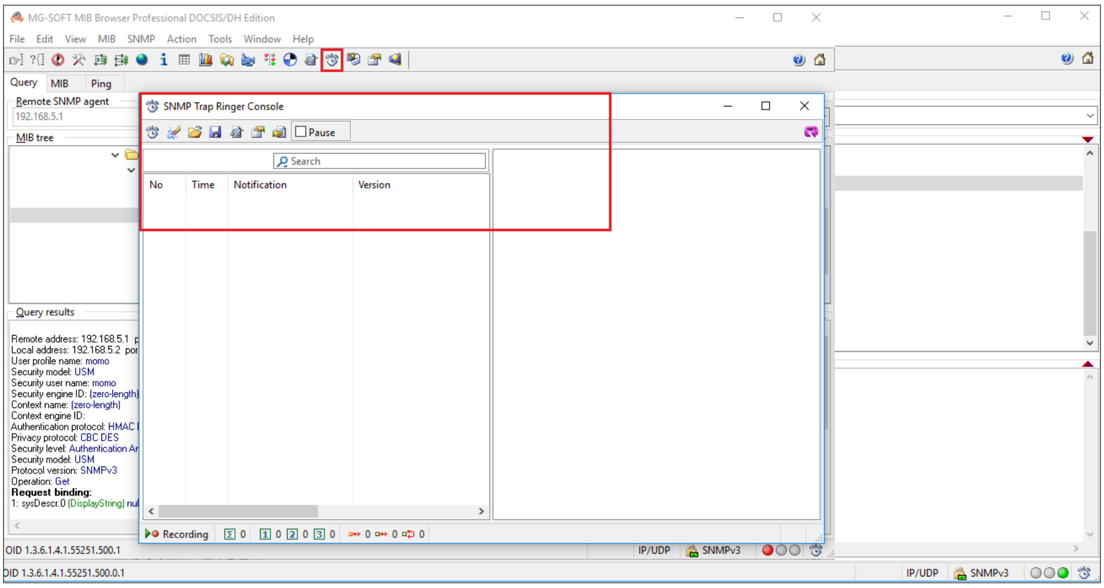
```
Remote address: 192.168.5.1  p
Local address: 192.168.5.2  port
User profile name: momo
Security model: USM
Security user name: momo
Security engine ID: (zero-length)
Context name: (zero-length)
Context engine ID:
Authentication protocol: HMAC M
Privacy protocol: CBC DES
Security level: Authentication An
Security model: USM
Protocol version: SNMPv3
Operation: Get
Request binding:
1: sysDescr.0 (DisplayString) null
```

Trap received from ::1.

OID 1.3.6.1.4.1.55251.500.0.1

Figure 353 – User settings

After that, open the **SNMP Trap Ringer Console**:



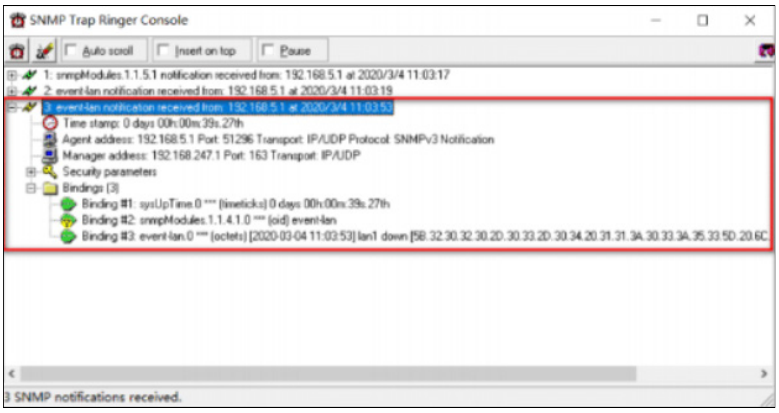
Remote address: 192.168.5.1 p
Local address: 192.168.5.2 por
User profile name: momo
Security model: USM
Security user name: momo
Security engine ID: (zero-length)
Context name: (zero-length)
Context engine ID:
Authentication protocol: HMAC
Privacy protocol: CBC DES
Security level: Authentication Ar
Security model: USM
Protocol version: SNMPv3
Operation: Get
Request binding:
1: sysDescr.0 (DisplayString) nul

OID 1.3.6.1.4.1.55251.500.1

OID 1.3.6.1.4.1.55251.500.0.1

Figure 354 – SNMP Trap Ringer Console (1)

You should wait until the router sends a Trap notification:



```
1: snmpModules.1.1.5.1 notification received from: 192.168.5.1 at 2020/3/4 11:03:17
2: event-lan notification received from: 192.168.5.1 at 2020/3/4 11:03:19
3: event-lan notification received from: 192.168.5.1 at 2020/3/4 11:03:53
    Time stamp: 0 days 00h:00m:39s.27th
    Agent address: 192.168.5.1 Port: 51296 Transport: IP/UDP Protocol: SNMPv3 Notification
    Manager address: 192.168.247.1 Port: 163 Transport: IP/UDP
    Security parameters
    Bindings (3)
        Binding #1: sysUpTime.0 *** (timeticks) 0 days 00h:00m:39s.27th
        Binding #2: snmpModules.1.1.4.1.0 *** (oid) event-lan
        Binding #3: event-lan.0 *** (octets) [2020-03-04 11:03:53] lan1 down [5B.32.30.32.30.2D.30.33.2D.30.34.20.31.31.3A.30.33.3A.35.33.5D.20.6C
3 SNMP notifications received.
```

Figure 355 – SNMP Trap Ringer Console (2)

The test was successfully performed.

7.22 MODBUS SLAVE

This tutorial contains information on how to configure Modbus Slave.

7.22.1 TOPOLOGY

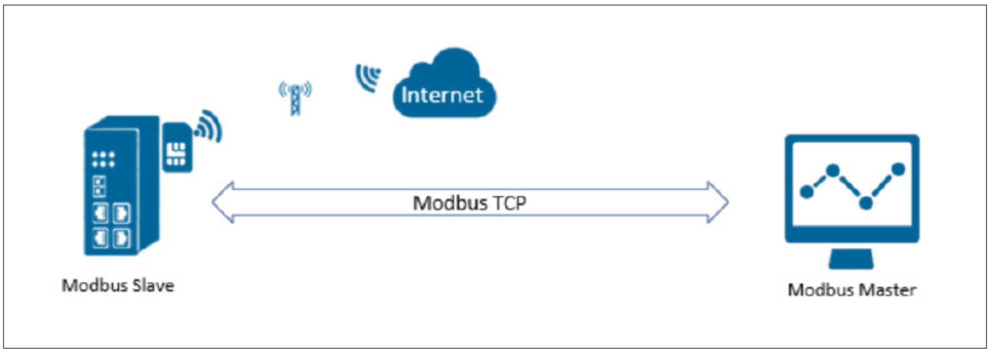


Figure 356 – Topology

1. **AirGate 4G Wi-Fi** operates as a Modbus slave with a static public IP address and a SIM card.
2. The Modbus Master connects to the AirGate 4G Wi-Fi router (Modbus Slave) via a TCP connection.
3. The Modbus master reads the status of the Digital IO and controls DO.

For this tutorial, it is necessary to run the "Modbus Poll" application to simulate a Modbus master.

7.22.2 REGISTER TABLE (IO DIGITAL)

INDEX	ITEM	FUNCTION	WRITE FUNCTION	ADDRESS (DECIMAL)	QUANTITY	VALUE
1	Digital Input 1	02 Input Status	Null	13800	1	0 – Low 1 – High
2	Digital Input 2	02 Input Status	Null	13801	1	0 – Low 1 – High
3	Digital Output 1	01 Coil Status	05/15	13802	1	0 – Low 1 – High
4	Digital Output 1	01 Coil Status	05/15	13803	1	1 – Pulse
5	Digital Output 2	01 Coil Status	05/15	13804	1	0 – Low 1 – High
6	Digital Output 2	01 Coil Status	05/15	13805	1	1 – Pulse
7	DO1 Pulse Width	03 Holding Registers	06/16	13806	1	Default: 500 (ms) Range: 1~1000
8	DO2 Pulse Width	03 Holding Registers	06/16	13807	1	Default: 500 (ms) Range: 1~1000

Table 11 – Register table

7.22.3 EXAMPLES

READ DI1 HIGH LEVEL

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	QUANTITY
Tx	01 90	00 00	00 06	01	02	35 E8	00 01

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	BYTE LENGHT	VALUE
Rx	01 90	00 00	00 04	01	02	01	01

Table 12 – Example 1

READ THE VALUE FROM 2 REGISTERS (DI1 AND DI1 HIGH LEVEL)

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	QUANTITY
Tx	01 91	00 00	00 06	01	02	35 E8	00 02

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	BYTE LENGHT	VALUE
Rx	01 91	00 00	00 04	01	02	01	03

Table 13 – Example 2

READ DO STATUS (DO1 OUTPUT LOW LEVEL)

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	QUANTITY
Tx	04 81	00 00	00 06	01	01	35 EA	00 01

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	BYTE LENGHT	VALUE
Rx	04 81	00 00	00 04	01	01	01	00

Table 14 – Example 3

CONTROL DO1 OUTPUT HIGH LEVEL

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Tx	07 29	00 00	00 06	01	05	35 EA	FF 00

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Rx	07 29	00 00	00 06	01	05	35 EA	FF 00

Table 15 – Example 4

CONTROL DO1 OUTPUT LOW LEVEL

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Tx	07 30	00 00	00 06	01	05	35 EA	00 00

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Rx	07 30	00 00	00 06	01	05	35 EA	00 00

Table 16 – Example 5

CONTROL DO1 PULSE OUTPUT

MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Tx	07 31	00 00	00 06	01	05	35 EB	FF 00

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Rx	07 31	00 00	00 06	01	05	35 EB	FF 00

Table 17 – Example 6

CHANGE PULSE OUTPUT LENGHT– 500 ms

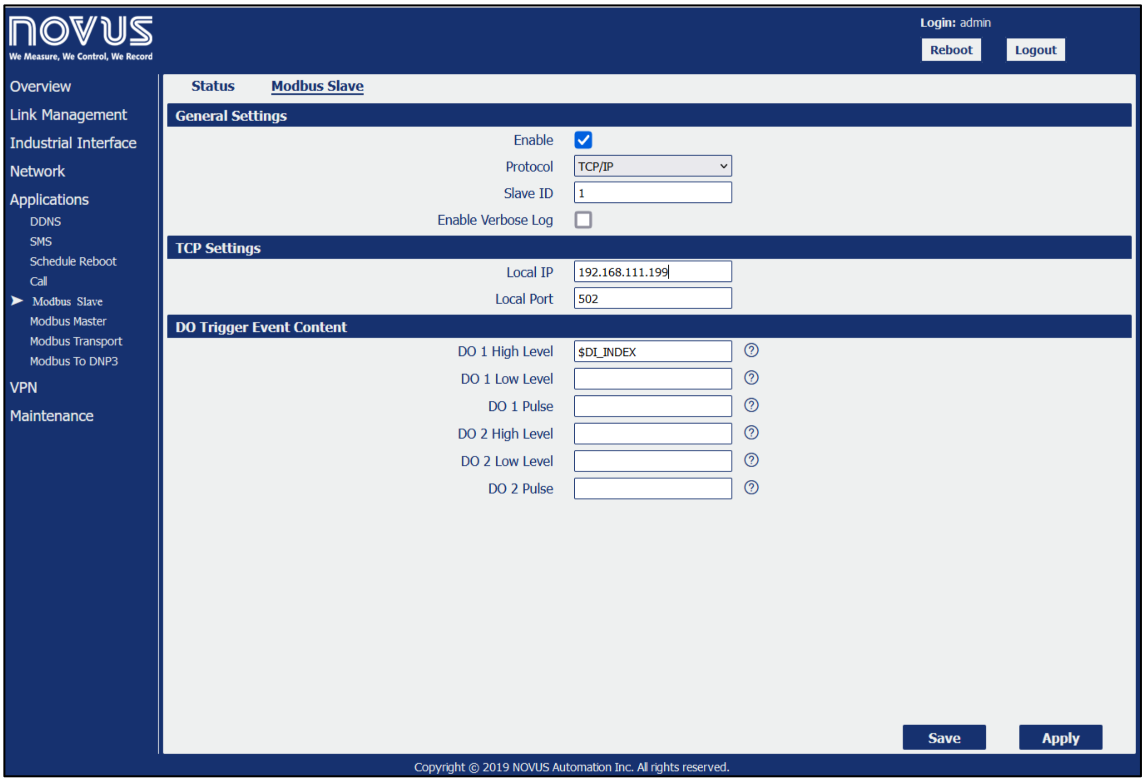
MASTER	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Tx	07 2C	00 00	00 06	01	06	35 EE	01 F4

SLAVE	TRANSACTION ID	PROTOCOL ID	DATA LENGHT	SLAVE ID	FUNCTION CODE	ADDRESS	VALUE
Rx	07 2C	00 00	00 06	01	06	35 EE	01 F4

Table 18 – Example 7

7.22.4 SETTINGS

1. Go to **Application** > **Modbus Slave**, enable Modbus Slave function, as shown in the figure below:



General Settings

Enable ☑

Protocol TCP/IP

Slave ID 1

Enable Verbose Log □

TCP Settings

Local IP 192.168.111.199

Local Port 502

DO Trigger Event Content

DO 1 High Level $DI_INDEX

DO 1 Low Level

DO 1 Pulse

DO 2 High Level

DO 2 Low Level

DO 2 Pulse

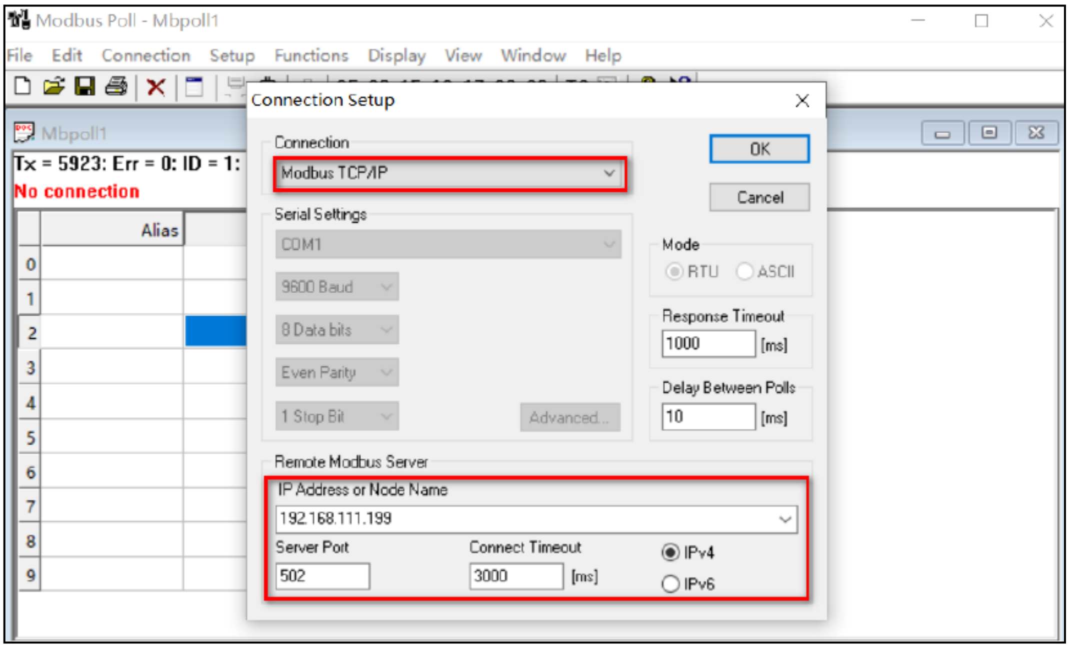
Figure 357 – Configuring the function

2. Click **Save** > **Apply**.

7.22.5 TEST

7.22.1.1 READ DIGITAL INPUT STATUS

1. Run "Modbus Poll" software to connect to **AirGate 4G Wi-Fi** (Modbus Slave) (Path: **Connection > Connect**):



Tx = 5923: Err = 0: ID = 1:
No connection

Connection Setup

Connection: Modbus TCP/IP

Serial Settings: COM1, 9600 Baud, 8 Data bits, Even Parity, 1 Stop Bit

Mode: ○ RTU ○ ASCII

Response Timeout: 1000 [ms]

Delay Between Polls: 10 [ms]

Remote Modbus Server

IP Address or Node Name: 192.168.111.199

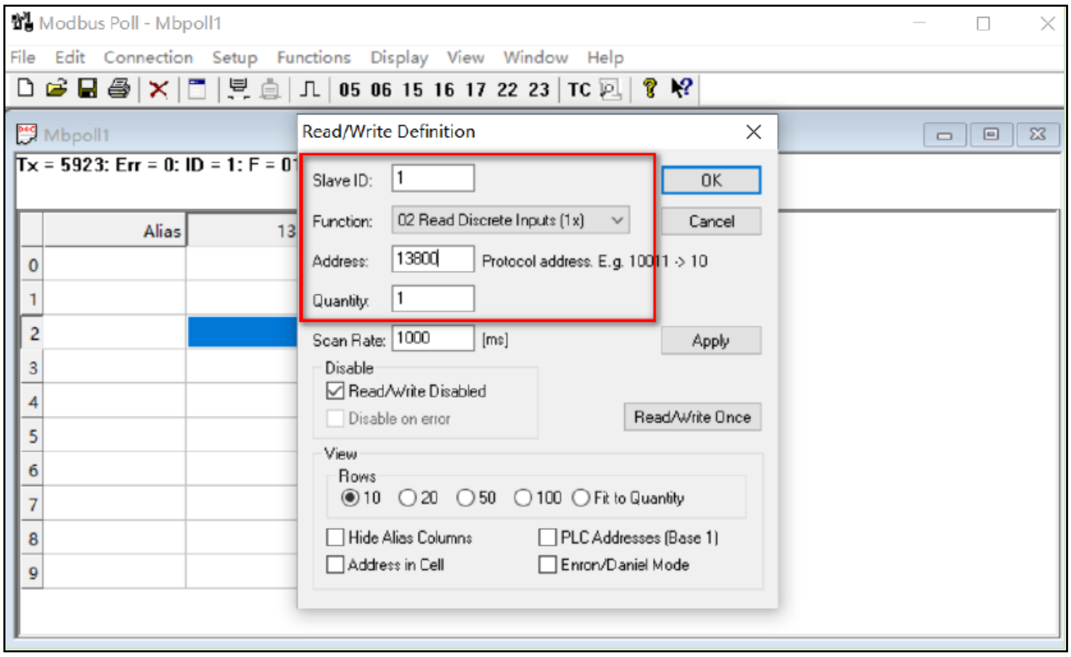
Server Port: 502

Connect Timeout: 3000 [ms]

● IPv4
○ IPv6

Figure 358 – Connection

Follow the path **Setup > Read/Write Definition**:



Tx = 5923: Err = 0: ID = 1: F = 0

Read/Write Definition

Slave ID: 1

Function: 02 Read Discrete Inputs (1x)

Address: 13800 Protocol address. E.g. 10011 -> 10

Quantity: 1

Scan Rate: 1000 [ms]

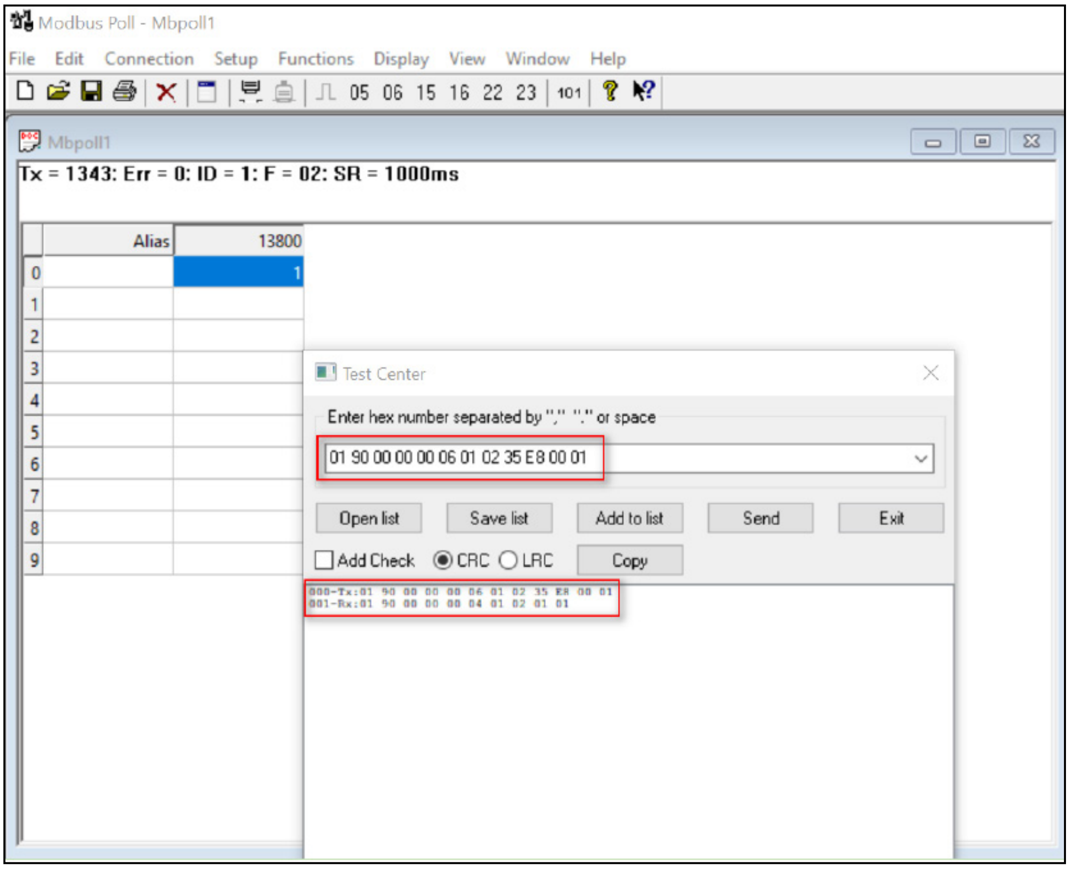
Disable
☑ Read/Write Disabled
□ Disable on error

View
Rows
● 10 ○ 20 ○ 50 ○ 100 ○ Fit to Quantity

□ Hide Alias Columns □ PLC Addresses (Base 1)
□ Address in Cell □ Enron/Daniel Mode

Figure 359 – Read/Write Definition

2. Send a command to read DI1 status (Path: **Functions > Test Center**):



Tx = 1343: Err = 0: ID = 1: F = 02: SR = 1000ms

	Alias	13800
0		1
1		
2		
3		
4		
5		
6		
7		
8		
9		

Enter hex number separated by "," "." or space

01 90 00 00 00 06 01 02 35 E8 00 01

□ Add Check ● CRC ○ LRC

```
000-Tx:01 90 00 00 00 06 01 02 35 E8 00 01
001-Rx:01 90 00 00 00 04 01 02 01 01
```

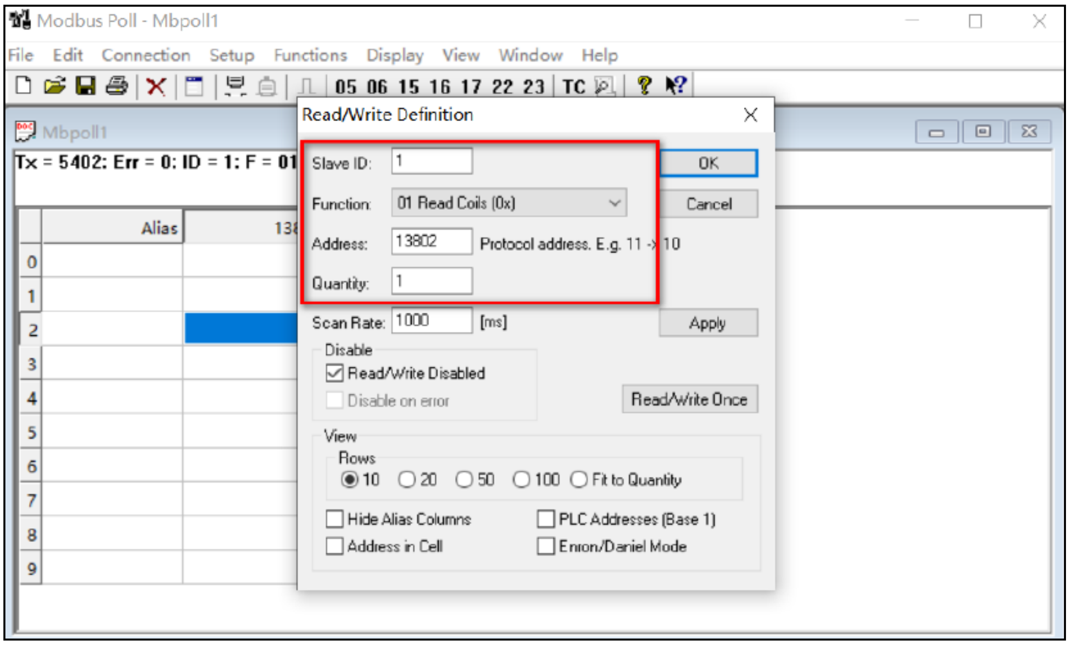
Figure 360 – Sending a command

The response from the Value field is "01"', the DI1 status is "High". Test run successfully.

For information about the "Tx" and "Rx" commands, see the register table in this section.

7.22.1.2 READ DIGITAL OUTPUT STATUS

1. Set **Function Code** field as "01", **Address** field as "13802" and **Quantity** field as "1" (Path: **Setup > Read/Write Definition**):



Tx = 5402: Err = 0: ID = 1: F = 01

Read/Write Definition

Slave ID: 1

Function: 01 Read Coils (0x)

Address: 13802 Protocol address. E.g. 11 -> 10

Quantity: 1

Scan Rate: 1000 [ms]

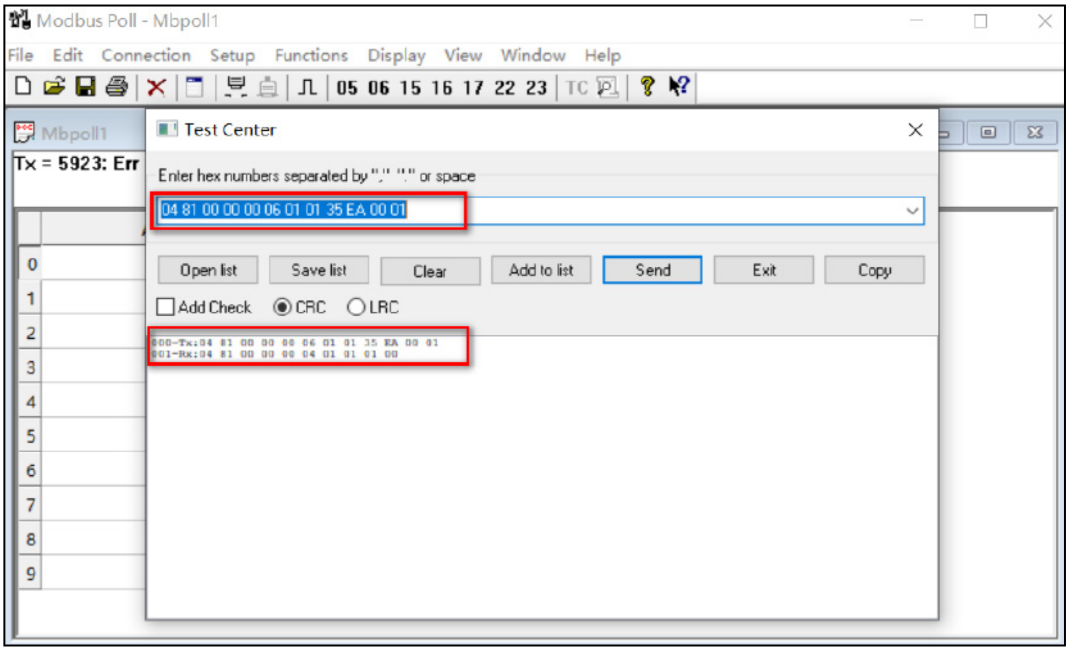
Disable
☑ Read/Write Disabled
□ Disable on error

View
Rows
● 10 ○ 20 ○ 50 ○ 100 ○ Fit to Quantity

□ Hide Alias Columns □ PLC Addresses (Base 1)
□ Address in Cell □ Enron/Daniel Mode

Figure 361 – Read/Write Definition

2. Send a command to read DI1 status (Path: **Functions > Test Center**):



Tx = 5923: Err

Enter hex numbers separated by "," "." or space

04 81 00 00 00 06 01 01 35 EA 00 01

□ Add Check ● CRC ○ LRC

```
000-Tx:04 81 00 00 00 06 01 01 35 EA 00 01
001-Rx:04 81 00 00 00 04 01 01 01 00
```

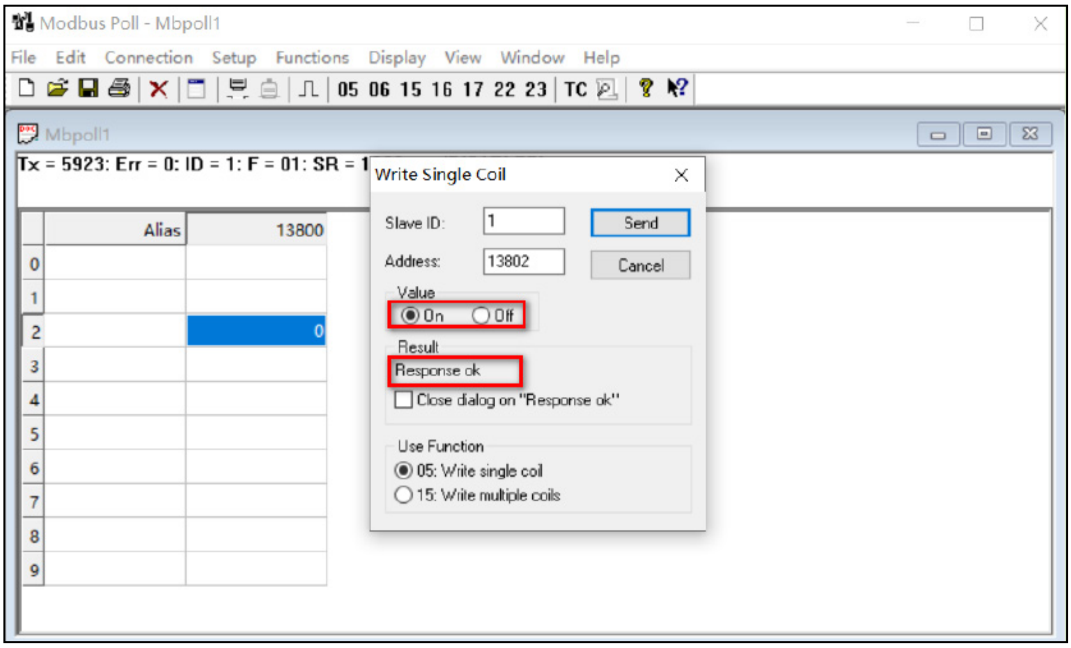
Figure 362 – Sending a command

The response from the Value field is "00"', the DO1 status is "Low". Test run successfully.

For information about the "Tx" and "Rx" commands, see the register table in this section.

7.22.1.3 CONTOL DIGITAL OUTPUT

1. Go to **Functions > 05: Write Single Coils** to change DO status from "0" to "1":



Tx = 5923: Err = 0: ID = 1: F = 01: SR = 1

	Alias	13800
0		
1		
2		0
3		
4		
5		
6		
7		
8		
9		

Slave ID: 1

Address: 13802

Value: ● On ○ Off

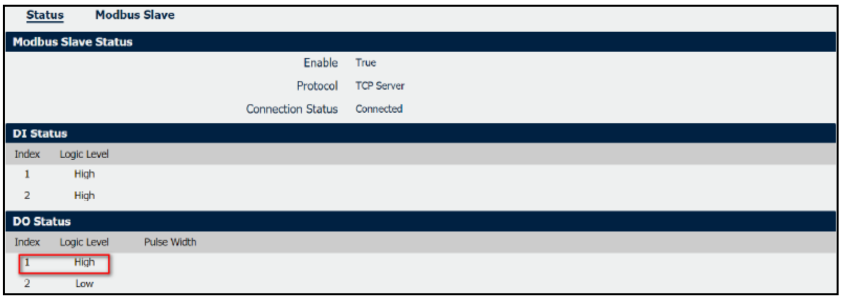
Result: Response ok

□ Close dialog on "Response ok"

Use Function: ● 05: Write single coil ○ 15: Write multiple coils

Figure 363 – Write Single Coil

2. Go to **Application > Modbus Slave > DO Status**. The **DO Logic Level** field changed to High".



Modbus Slave Status

Enable True

Protocol TCP Server

Connection Status Connected

DI Status

Index	Logic Level
1	High
2	High

DO Status

Index	Logic Level	Pulse Width
1	High	
2	Low	

Figure 364 – DO Logic level

Test run successfully.

7.23 MODBUS FOR DNP3

This tutorial contains information on how to configure Modbus for DNP3.

7.23.1 TOPOLOGY

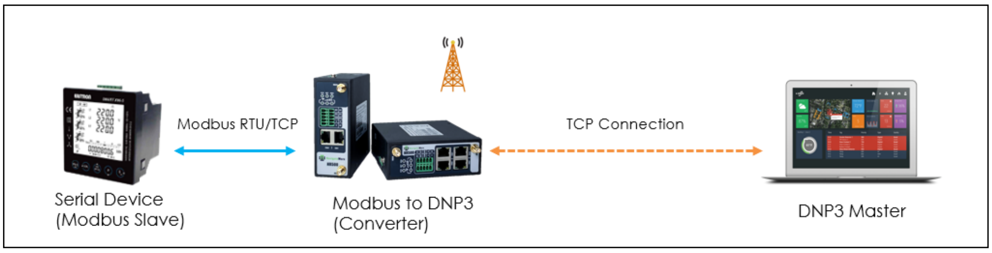


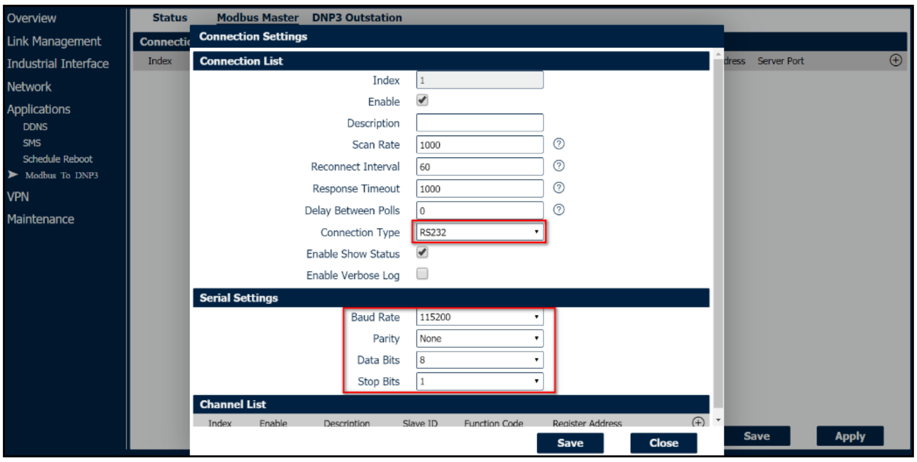
Figure 365 – Topology

1. **AirGate 4G Wi-Fi** operates as Modbus to DNP3 converter. Operates as Modbus master and DNP3 external station.
2. A serial device supports the Modbus protocol and acts as Modbus Slave. It is connected to the **AirGate 4G Wi-Fi** router via serial port or Ethernet port.
3. **AirGate 4G Wi-Fi** router polls the Modbus data from the end device (Modbus Slave). After that it sends the data to the remote DNP3 Master.

7.23.2 SETTINGS

7.23.1.1 AIRGATE 4G WI-FI SETTINGS

1. Go to **Application** > **Modbus to DNP3 > Modbus Master** and specify serial settings to connect the router to the Modbus slave via the R232 interface.



Connection Settings

Connection List

Index	1
Enable	☑
Description	
Scan Rate	1000
Reconnect Interval	60
Response Timeout	1000
Delay Between Polls	0
Connection Type	RS232
Enable Show Status	☑
Enable Verbose Log	☐

Serial Settings

Baud Rate	115200
Parity	None
Data Bits	8
Stop Bits	1

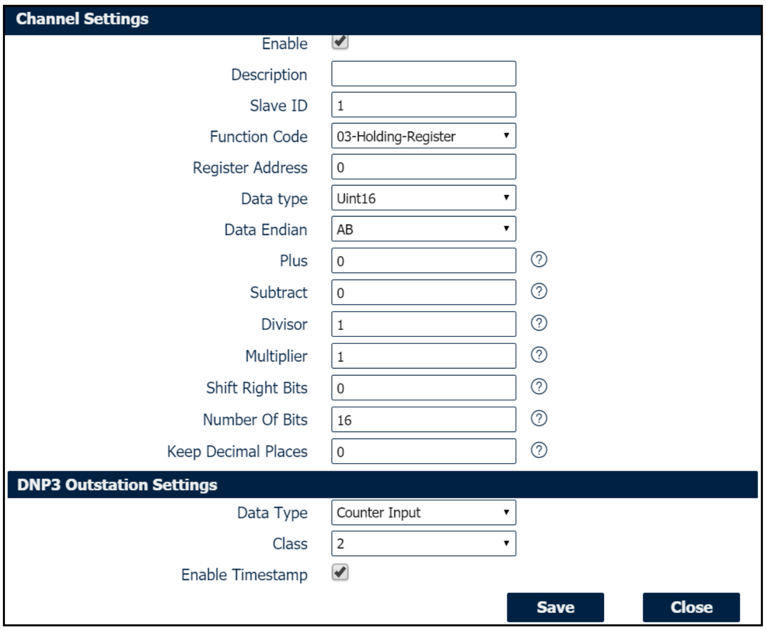
Channel List

Index	Enable	Description	Slave ID	Function Code	Register Address

Save Close

Figure 366 – Function settings

2. Go to **Application** > **Modbus to DNP3 > Modbus Master > Channel List** and specify the settings for the Modbus master and DNP3 data type:



Channel Settings

Enable	☑
Description	
Slave ID	1
Function Code	03-Holding-Register
Register Address	0
Data type	Uint16
Data Endian	AB
Plus	0
Subtract	0
Divisor	1
Multiplier	1
Shift Right Bits	0
Number Of Bits	16
Keep Decimal Places	0

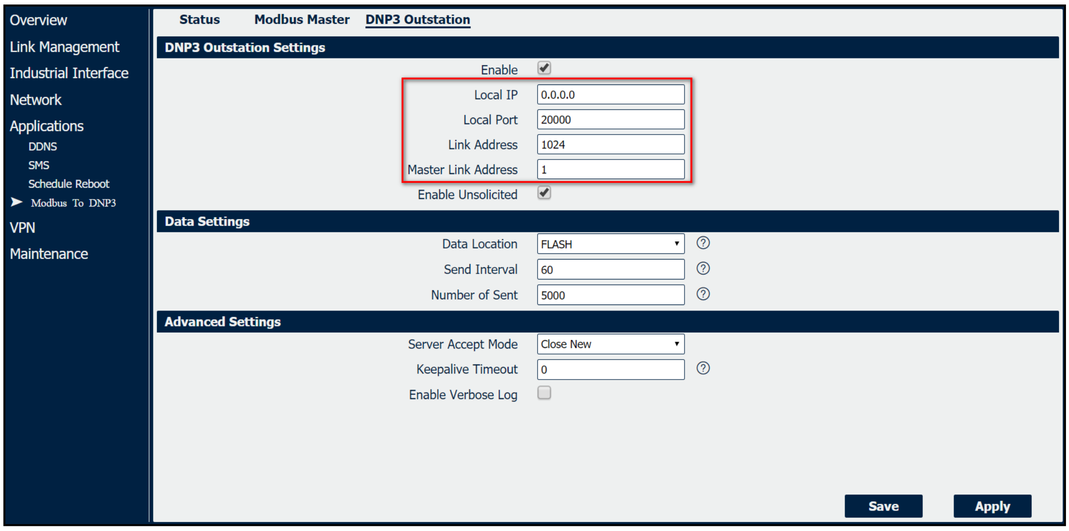
DNP3 Outstation Settings

Data Type	Counter Input
Class	2
Enable Timestamp	☑

Save Close

Figure 367 – Channel list

3. Go to **Application** > **Modbus to DNP3 > DNP3 Outstation** and specify the settings of the external DNP3 station:



DNP3 Outstation Settings

Enable ☑

Local IP 0.0.0.0

Local Port 20000

Link Address 1024

Master Link Address 1

Enable Unsolicited ☑

Data Settings

Data Location FLASH

Send Interval 60

Number of Sent 5000

Advanced Settings

Server Accept Mode Close New

Keepalive Timeout 0

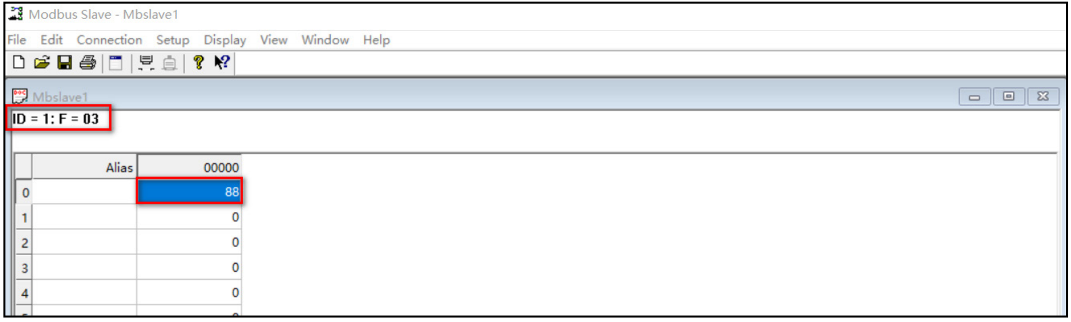
Enable Verbose Log □

Figure 368 – DNP3 external station

4. Click **Save** > **Apply**.

7.23.1.2 MODBUS SLAVE SETTINGS

1. Set **ID Slave** parameter as "1", **Function Code** parameter as "03" and "88" value in "0" register:

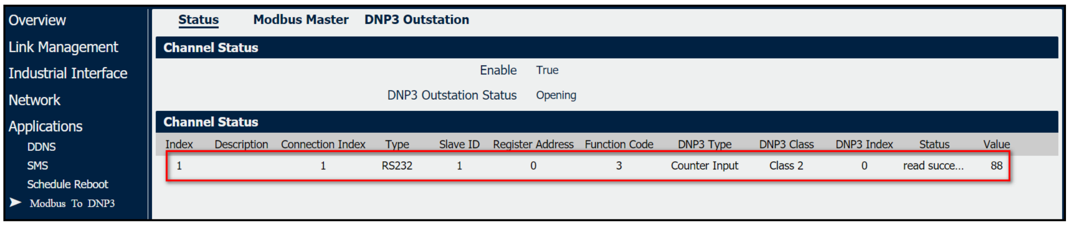


ID = 1: F = 03

	Alias	00000
0		88
1		0
2		0
3		0
4		0

Figure 369 – Modbus slave settings

2. **AirGate 4G Wi-Fi** has successfully polled the data from the Modbus slave:



Channel Status

Enable True

DNP3 Outstation Status Opening

Channel Status

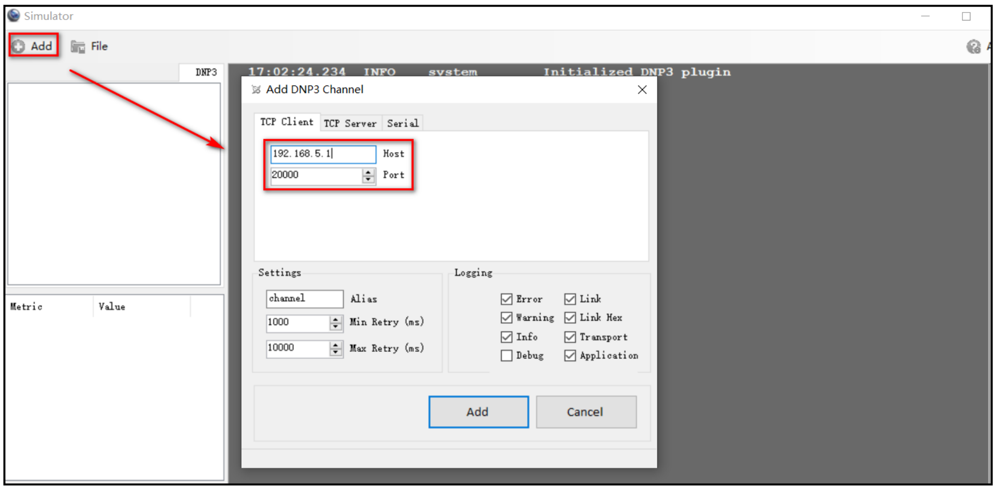
Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	DNP3 Type	DNP3 Class	DNP3 Index	Status	Value
1		1	RS232	1	0	3	Counter Input	Class 2	0	read succe...	88

Figure 370 – Modbus slave data

7.23.3 TEST

Use the DNP3 simulator "OpenDNP3" to perform the tests.

1. Run DNP3 simulator and enter the IP address and port number to connect to the **AirGate 4G Wi-Fi (DNP3 External Station)**:



```
17:02:24.234  INFO    system          Initialized DNP3 plugin
```

Add DNP3 Channel — TCP Client

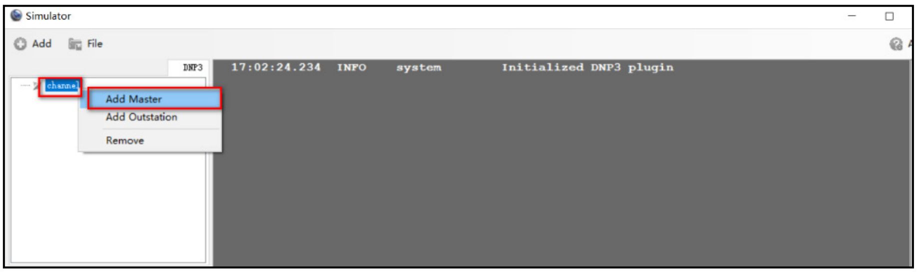
Host: 192.168.5.1
Port: 20000

Settings
Alias: channel
Min Retry (ms): 1000
Max Retry (ms): 10000

Logging
☑ Error ☑ Link
☑ Warning ☑ Link Hex
☑ Info ☑ Transport
□ Debug ☑ Application

Figure 371 – Filling the fields

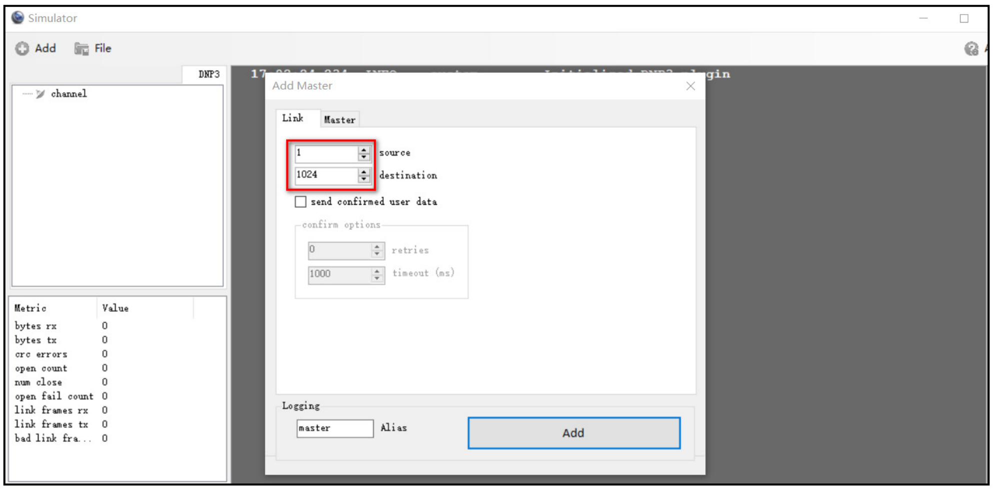
2. Click **Channel > Add Master**:



```
17:02:24.234  INFO    system          Initialized DNP3 plugin
```

Figure 372 – Add master

3. Specify the address of the DNP3 master to match the **AirGate 4G Wi-Fi (DNP3 External Station)** settings:



Add Master — Master

source: 1
destination: 1024
□ send confirmed user data

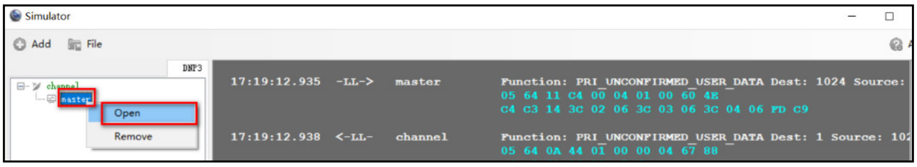
confirm options
retries: 0
timeout (ms): 1000

Logging
Alias: master

Metric	Value
bytes rx	0
bytes tx	0
crc errors	0
open count	0
num close	0
open fail count	0
link frames rx	0
link frames tx	0
bad link fra...	0

Figure 373 – Specify the address

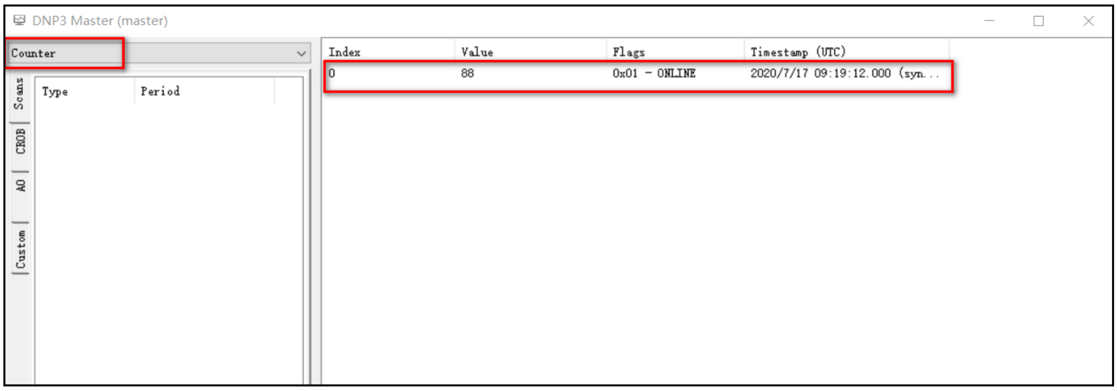
4. Click **Master > Open**:



```
17:19:12.935  -LL->   master          Function: PRI_UNCONFIRMED_USER_DATA Dest: 1024 Source:
                                      05 64 11 C4 00 04 01 00 60 4E
                                      C4 C3 14 3C 02 06 3C 03 06 3C 04 06 FD C9

17:19:12.938  <-LL-   channel         Function: PRI_UNCONFIRMED_USER_DATA Dest: 1 Source: 102
                                      05 64 0A 44 01 00 00 04 67 88
```

Figure 374 – Open master

5. Select the date type as "Counter". So, you can see that the data has been sent from **AirGate 4G Wi-Fi** to the DNP3 master successfully:



Index	Value	Flags	Timestamp (UTC)
0	88	0x01 - ONLINE	2020/7/17 09:19:12.000 (syn...

Figure 375 – See data

6. Test run successfully.

7.24 CONTROL AND READING OF DIGITAL OUTPUTS VIA MQTT

This tutorial contains information on how to configure and use MQTT for the digital and Modbus outputs.

This tutorial is compatible with the Modbus Master application (see "MODBUS MASTER" APPLICATION section).

7.24.1 TOPOLOGY

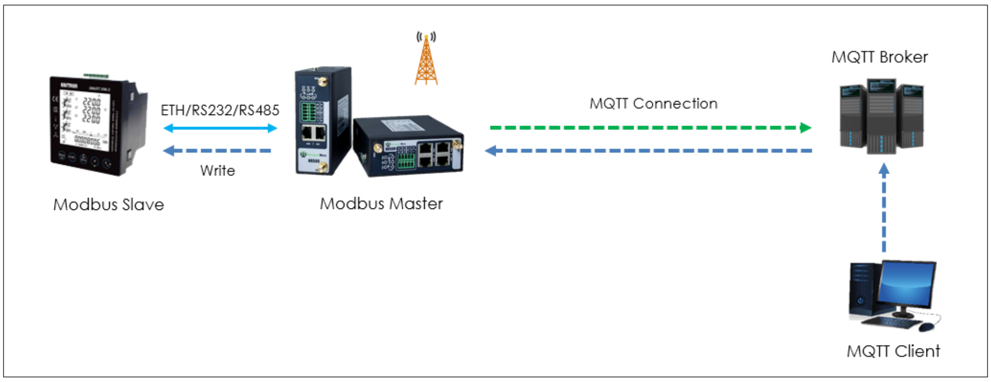


Figure 376 – Topology

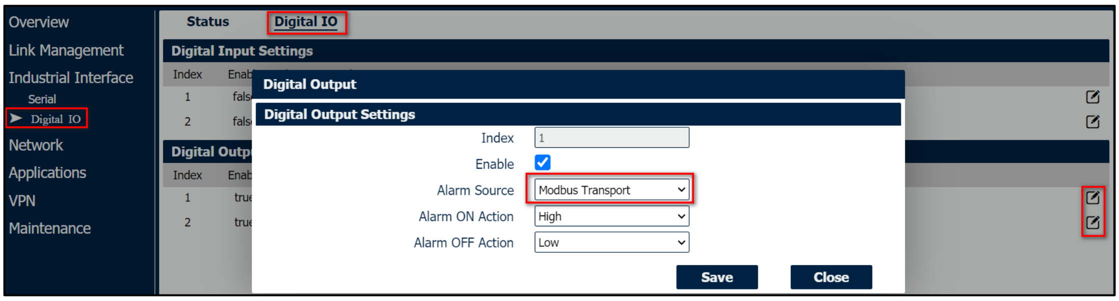
1. **AirGate 4G Wi-Fi** operates as Modbus Master and connects to the Modbus slave via the Ethernet, RSS232 or RS485 interfaces.
2. **AirGate 4G Wi-Fi** operates as the MQTT Client and connects to the MQTT Broker.
3. Another MQTT Client connects to the MQTT Broker and sends the commands to control the digital output and write to the slave device.

Para este tutorial, é ser necessário configurar o tipo de conexão como "RS232", o que significa que o dispositivo se conectará ao escravo Modbus via RS232. Isso também funciona com a RS485 e a porta Ethernet.

7.24.2 MQTT FOR DIGITAL OUTPUT

7.24.2.1 CONFIGURING AIRGATE 4G WI-FI

1. Go to **Industrial Interface** > **Digital IO**, enable the digital output function and set the **Alarm Source** parameter as **Modbus Transport**, as shown in the image below:



Digital Output

Digital Output Settings

Index 1

Enable ☑

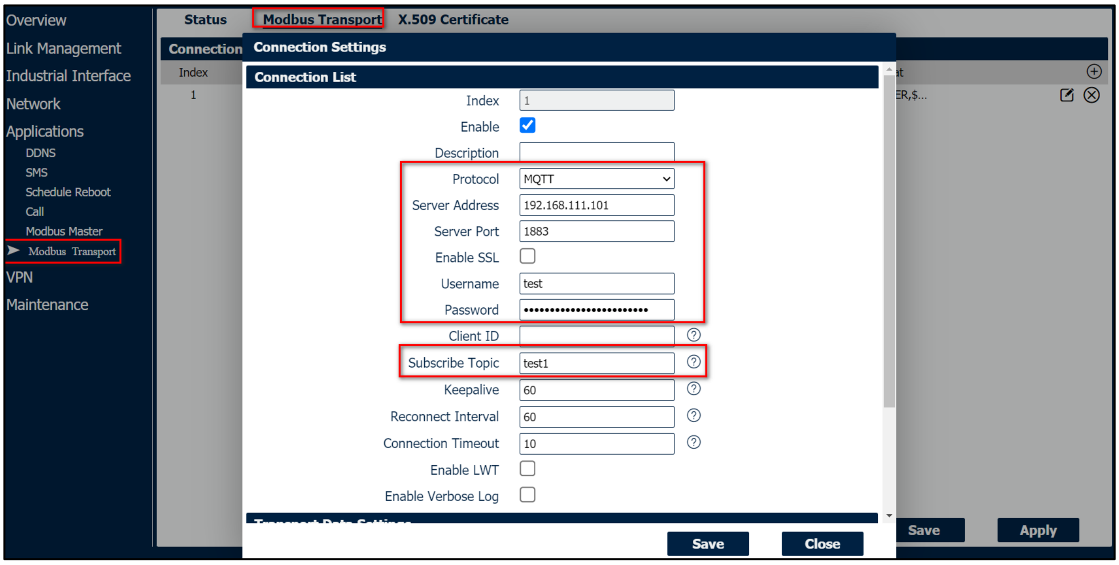
Alarm Source Modbus Transport

Alarm ON Action High

Alarm OFF Action Low

Figure 377 – Digital output settings

2. Click **Save** > **Apply**.
3. Go to **Applications** > **Modbus Transport** to specify the MQTT parameters to make the router connect to the MQTT Broker and set the Subscription topic to "test1". Leave the other parameters with the default settings.



Connection Settings

Connection List

Index 1

Enable ☑

Description

Protocol MQTT

Server Address 192.168.111.101

Server Port 1883

Enable SSL ☐

Username test

Password ••••••••••••••••••••••••

Client ID

Subscribe Topic test1

Keepalive 60

Reconnect Interval 60

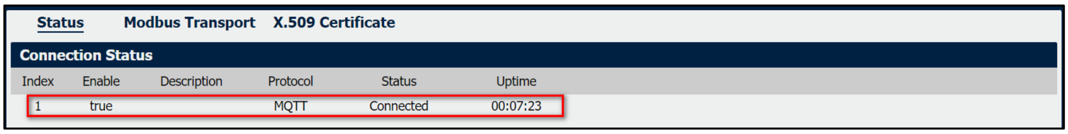
Connection Timeout 10

Enable LWT ☐

Enable Verbose Log ☐

Figure 378 – Application settings

4. Click **Save > Apply**.
5. The router has connected successfully to the MQTT Broker:



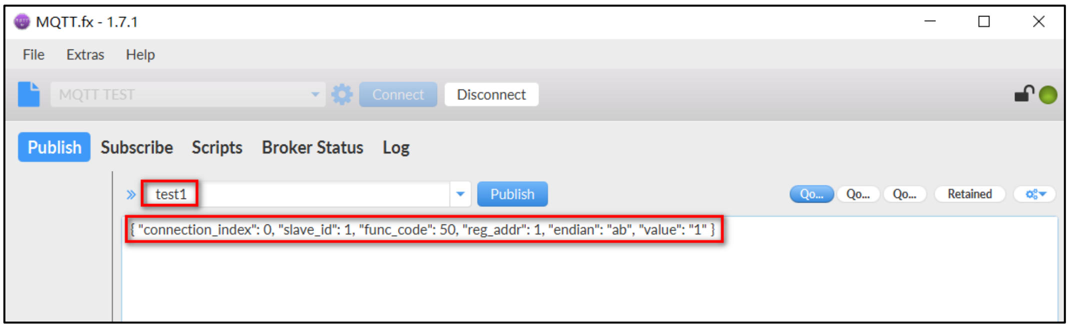
Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true		MQTT	Connected	00:07:23

Figure 379 – MQTT Broker: Connection status

7.24.2.2 TEST

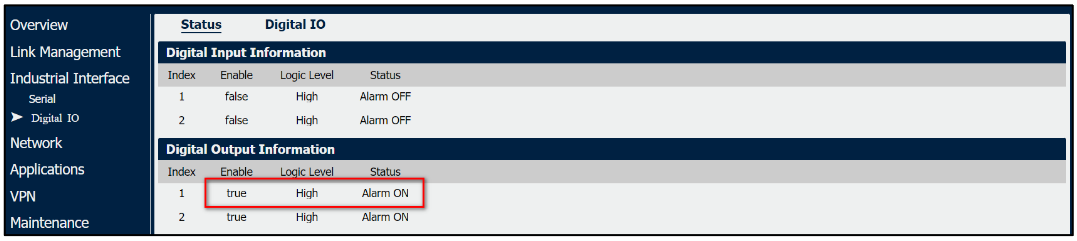
1. Run the MQTT Client on the computer, connect to the MQTT Broker, publish to the Publish topic as "test1" and send the command to the router to control the digital output:



{ "connection_index": 0, "slave_id": 1, "func_code": 50, "reg_addr": 1, "endian": "ab", "value": "1" }

Figure 380 – Publish topic

2. Test run successfully:



Digital Input Information

Index	Enable	Logic Level	Status
1	false	High	Alarm OFF
2	false	High	Alarm OFF

Digital Output Information

Index	Enable	Logic Level	Status
1	true	High	Alarm ON
2	true	High	Alarm ON

Figure 381 – Test run successfully

The commands are explained below:

1. Command to turn on digital output 1:
{ "connection_index": 0, "slave_id": 1, "func_code": 50, "reg_addr": 1, "endian": "ab", "value": "1" }

2. Command to turn off digital output 1:
{ "connection_index": 0, "slave_id": 1, "func_code": 50, "reg_addr": 1, "endian": "ab", "value": "0" }

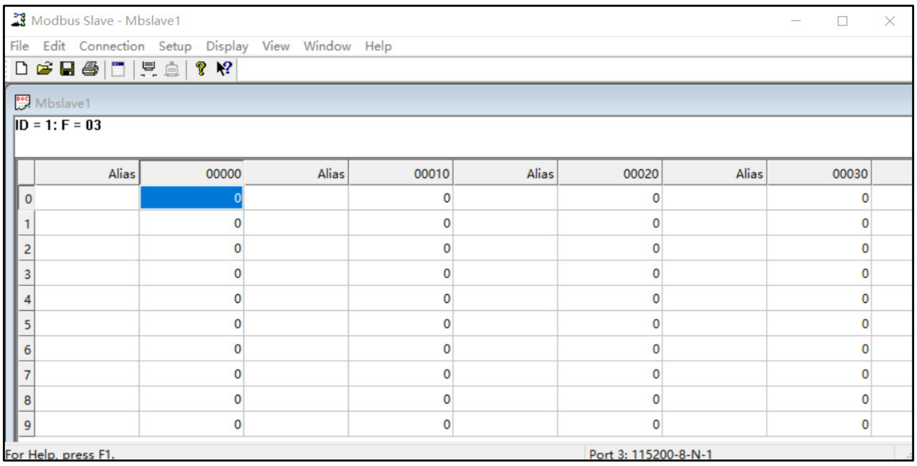
3. Command to turn on digital output 2:
{ "connection_index": 0, "slave_id": 1, "func_code": 50, "reg_addr": 2, "endian": "ab", "value": "1" }

4. Command to turn off digital output 2:
{ "connection_index": 0, "slave_id": 1, "func_code": 50, "reg_addr": 2, "endian": "ab", "value": "0" }

7.24.3 MQTT FOR MODBUS

7.24.3.1 MODBUS SLAVE SETTINGS

You must use the "Modbus Slave" software to simulate the end device (slave Modbus device) and specify the following parameters: **Slave ID:** 1; **Function Code:** 03-Holding-Register.



ID = 1: F = 03

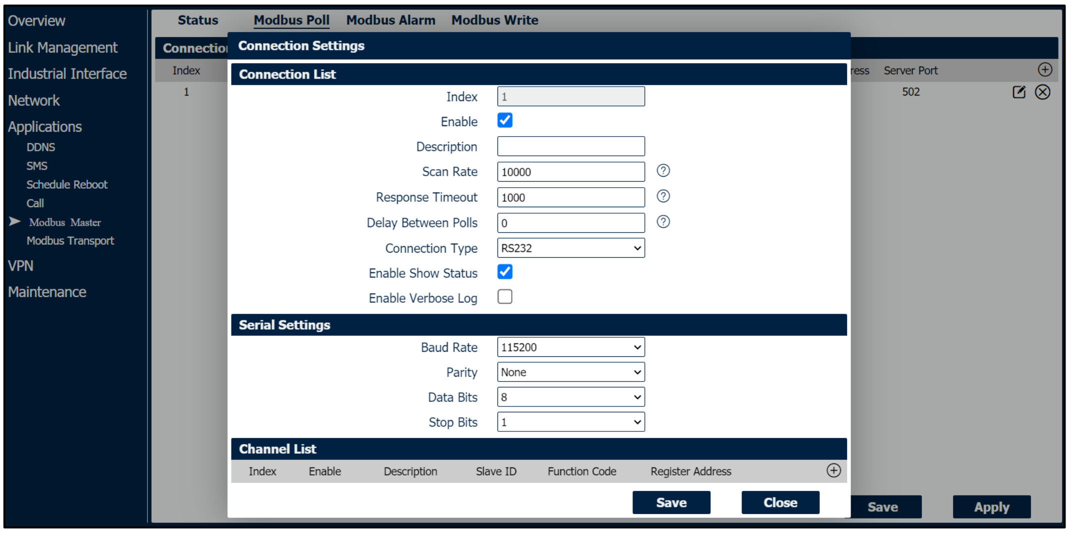
	Alias	00000	Alias	00010	Alias	00020	Alias	00030
0		0		0		0		0
1		0		0		0		0
2		0		0		0		0
3		0		0		0		0
4		0		0		0		0
5		0		0		0		0
6		0		0		0		0
7		0		0		0		0
8		0		0		0		0
9		0		0		0		0

For Help, press F1. Port 3: 115200-8-N-1

Figure 382 – Modbus slave settings

7.24.3.2 AIRGATE 4G WI-FI SETTINGS

1. Go to **Applications** > **Modbus Master** > **Modbus Poll** and specify the Modbus settings for connecting the device to the slave, as shown in the figure below:



Connection Settings

Connection List

Index: 1

Enable: ☑

Description:

Scan Rate: 10000

Response Timeout: 1000

Delay Between Polls: 0

Connection Type: RS232

Enable Show Status: ☑

Enable Verbose Log: □

Serial Settings

Baud Rate: 115200

Parity: None

Data Bits: 8

Stop Bits: 1

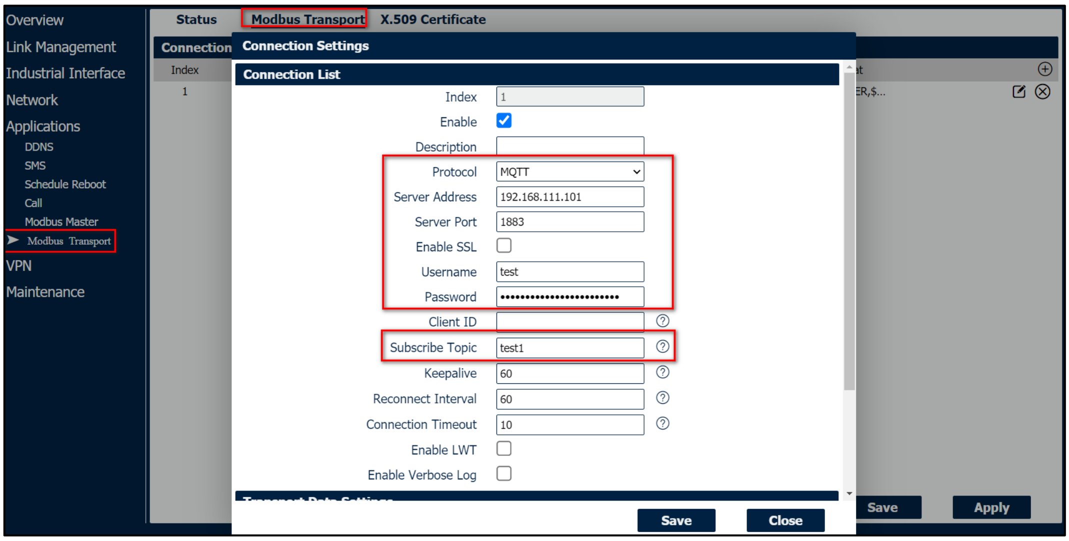
Channel List

Index	Enable	Description	Slave ID	Function Code	Register Address

Figure 383 – Connection settings

2. Click **Save** > **Apply**.

3. Go to **Applications > Modbus Transport** to specify the MQTT parameters to make the router connect to the MQTT Broker and set the Subscription topic to "test1". Leave the other parameters with the default settings.



Connection Settings

Connection List

Index: 1

Enable: ☑

Description:

Protocol: MQTT

Server Address: 192.168.111.101

Server Port: 1883

Enable SSL: □

Username: test

Password: ••••••••••••••••••••••••

Client ID:

Subscribe Topic: test1

Keepalive: 60

Reconnect Interval: 60

Connection Timeout: 10

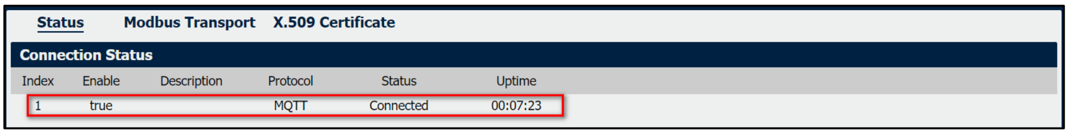
Enable LWT: □

Enable Verbose Log: □

Figure 384 – Modbus Transport

4. Click **Save** > **Apply**.

5. The router has connected to the MQTT Broker successfully:



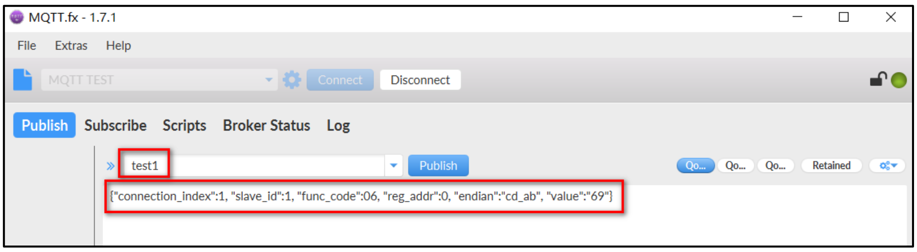
Connection Status

Index	Enable	Description	Protocol	Status	Uptime
1	true		MQTT	Connected	00:07:23

Figure 385 – MQTT connection

7.24.3.3 TEST

1. Run the MQTT Client on the computer, connect to the MQTT Broker, publish to the Publish topic as "test1" and send the command to the router to control the digital output:

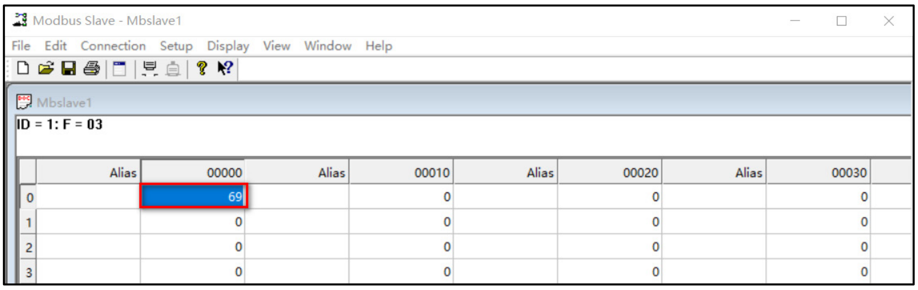


test1

```
{"connection_index":1, "slave_id":1, "func_code":06, "reg_addr":0, "endian":"cd_ab", "value":"69"}
```

Figure 386 – Test run successfully (1)

2. Test performed successfully. It was possible to send the command via MQTT to control the slave device:



ID = 1: F = 03

	Alias	00000	Alias	00010	Alias	00020	Alias	00030
0		69		0		0		0
1		0		0		0		0
2		0		0		0		0
3		0		0		0		0

Figure 387 – Test run successfully (2)

Control command to set the value to 69 to save 1 and register the address 0 as an example:
{"connection_index":1, "slave_id":1, "func_code":06, "reg_addr":0, "endian":"cd_ab", "value":"69"}

8 TROUBLESHOOTING

NO SIGNAL

Phenomenon: AirGate 4G Wi-Fi modem status shows no signal.

Possible Reason:

- Antenna installation is wrong.
- Modem failure.

Solution:

- Check the operation of the LTE antenna or replace it with a new one.
- In the LINK MANAGEMENT section, confirm that modem has been detected correctly.

CANNOT DETECT SIM CARD

Phenomenon: AirGate 4G Wi-Fi cannot detect SIM card even though the cellular connection has no connection problems.

Possible Reason:

- SIM card damage.
- SIM card with poor contact.

Solution:

- Replace SIM card.
- Reinstall SIM card.

SINAL FRACO

Phenomenon: No signal or weak signal device.

Possible Reason:

- Antenna installation is wrong.
- Area signal weak.

Solution:

- Check and reconnect the antenna.
- Contact the telecommunications company to confirm the existence of signal problems.
- Replace the actual antenna with a more powerful antenna.

IPsec VPN ESTABLISHED, BUT LAN TO LAN CANNOT COMMUNICATE

Phenomenon: IPsec VPN established, but LAN to LAN cannot communicate.

Possible Reason:

- Both networks do not match the selected traffic.
- IPsec second phase (ESP) settings do not match.

Solution:

- Check both network settings.
- Check IPsec second phase (ESP) setting.

FORGET ROUTER PASSWORD

Phenomenon: User forgot device login password.

Possible Reason:

User has changed the password.

Solution:

After initializing the router, press the RESET button for 3 to 10 seconds. The router will need to be rebooted manually and will return to factory default settings (username/password: **admin**/**admin**).

9 COMMAND LINE INTERFACE

Command-line interface (CLI) is a software interface that provides another configurable way to set parameters on the router. You can use Telnet or SSH connect the router for CLI input.

9.1 AIRGATE 4G WI-FI CLI ACCESS

```
login novusautomation.router: admin
Password: admin
>
```

9.2 CLI REFERENCE COMMANDS

```
>?
config          Switch to configuration mode
exit            Exit this CLI session
help            View an overview of CLI syntax
ping            Ping
reboot          Reboot the system
show            Show running configuration or running status
telnet          Telnet client
traceroute      Traceroute
upgrade         Firmware update
version         Show firmware version
```

Example:

```
> version
1.0.0 (1017.4)

> show wifi
wifi
{
  "status":"Ready",
  "mac":"a8: 3f: a1: e0: ab: 81",
  "ssid":"NR500-WAN",
  "channel":"6",
  "width":"40 MHz",
  "txpower":"20,00 dBm"
}

> ping www.baidu.com
PING www.baidu.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms
64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms
64 bytes from 14.215.177.38: seq=2 ttl=54 time=10.073 ms
64 bytes from 14.215.177.38: seq=3 ttl=54 time=10.031 ms
64 bytes from 14.215.177.38: seq=4 ttl=54 time=10.347 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.031/10.312/10.826 ms
>
```

9.3 HOW TO CONFIGURE THE CLI

CONTEXT SENSITIVE HELP

[?] Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring, and a subsequent repeat of the key will display possible completions.

[enter] Auto-completes, syntax-checks then executes a command. If there is a syntax error, then offending part of the command line will be highlighted and explained.

[space] Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS

[CTRL-A] Move to the start of the line

[CTRL-E] Move to the end of the line.

[up] Move to the previous command line held in history.

[down] Move to the next command line held in history.

[left] Move the insertion point left one character.

[right] Move the insertion point right one character.

DELETION KEYS

[CTRL-C] Delete and abort the current line

[CTRL-D] Delete the character to the right on the insertion point.

[CTRL-K] Delete all the characters to the right of the insertion point.

[CTRL-U] Delete the whole line.

[backspace] Delete the character to the left of the insertion point.

ESCAPE SEQUENCES

!! Substitute the last command line.

!N Substitute the Nth command line (absolute as per 'history' command).

!-N Substitute the command line entered N lines before (relative).

10 TECHNICAL SPECIFICATIONS

CHARACTERISTICS	AIRGATE 4G WI-FI
Cellular Interface	Frequency bands: • **4G LTE:** LTE FDD: 2100 (B1) / 1900 (B2) / 1800 (B3) / 1700 (B4) / 850 (B5) / 2600 (B7) / 900 (B8) / 700 (B28) MHz LTE TDD: 2300 (B40) MHz • **3G UMTS**: 2100 (B1) / 1900 (B2) / 850 (B5) / 900 (B8) MHz • **2G GSM**: 1900 (B2) / 1800 (B3) / 850 (B5) / 900 (B8) MHz
	Data transfer rate: • **4G LTE**: LTE FDD: Max 150 Mbps (DL) / Max 50 Mbps (UL) LTE TDD: Max 130 Mbps (DL) / Max 30 Mbps (UL) • **3G UMTS**: DC-HSDPA: Max 42 Mbps (DL) HSUPA: Max 5.76 Mbps (UL) WCDMA: Max 384 Kbps (DL) / Max 384 Kbps (UL) • **2G GSM**: EDGE: Max 296 Kbps (DL) / Max 236.8 Kbps (UL) GPRS: Max 107 Kbps (DL) / Max 85.6 Kbps (UL)
	2 x SMA female antenna connectors.
	2 x SIM (3.0 V and 1.8 V).
Wi-Fi Interface	• Standards: 802.11 b/g/n, 300 Mbps • 2 x RP-SMA male antenna connector • Support Wi-Fi Access Point and Client modes • Security: WEP, WPA and WPA2 encryption • Encryption: TKIP and CCMP
Ethernet Interface	• Standards: IEEE 802.3, IEEE 802.3u • 2 x ports 10/100 Mbps, RJ45 connector • 1 x WAN interface (configurable on Web GUI interface) • 1.5KV magnetic isolation protection
Serial Interface	• 1 x RS232 (3 pin): TX, RX, GND • 1 x RS485 (2 pin): D1, D0 • Baud Rate: 300 bps to 115.200 bps • 15 KV ESD protection
Digital Input and Digital Output	• 2 x Digital Inputs • 2 x Digital Outputs • Isolation: 3 KVDC or 2 KVrms • Absolute maximum VDC: 36 VCC • Absolute maximum ADC: 100 mA
Wi-Fi Antenna	Wi-Fi Magnet Antenna, 3 Meters Long, 2.412-2.483 GHz, 7 dBi, Φ 29×220 mm.
Cellular Antenna	4G / 3G / 2G Magnet Antenna, 3 Meters Long, 698-960 / 1710-2700 MHz, 2.5 dBi, Φ 29×112 mm.
LED	• 1 x SYS • 1 x NET • 1 x USR • 3 x RSSI
Software	• Network protocols: TCP, UDP, DHCP, ICMP, PPPoE, HTTP, HTTPS, DNS, VRRP, NTP • VPN: IPsec, GRE, OpenVPN, DMVPN • Policy: RIPv1 / RIPv2 / OSPF / BGP (optional) • Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL • Serial Port: TCP, UDP • Management: Web Interface
Power Supply	• Connector: 3-pin 3.5 mm female socket with lock. • Input voltage range: 9 to 48 VDC. • Power consumption: ○ Idle: 100 mA @ 12 V.

	○ Data Link: 400 mA (peak) @ 12 V.
Dimension	106 mm x 106 mm x 40 mm (excluding antenna).
Mounting	DIN rail mounting.
Environmental	• Operation temperature: -40 to 60 °C (-40 to 140 °F) • Storage temperature: -40 to 85 °C (-40 to 185 °F) • Operation humidity: 5 to 95 % non-condensing
Housing	Metal. 300 g.
Protection	IP30
Electromagnetic Compatibility	• **EMI**: EN 55032:2012 Class B • **EMS**: ○ IEC 61000-4-2 ESD: Level 4 ○ IEC 61000-4-3 RS: Level 3 ○ IEC 61000-4-4 EFT: Level 3 ○ IEC 61000-4-5 Surge: Level 3 ○ IEC 61000-4-6 CS: Level 3
Certifications	CE Mark UKCA Anatel (07661-19-12560) RoHS

Table 19 – Technical Specifications

10.1 CERTIFICATIONS

RoHS

NOVUS Automation declares and certifies that all of their products are designed and fabricated in compliance with the requirements of Directive 2011/65/EU (EU RoHS 2) of The European Parliament and of the Council of the 8th of June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (EEE) and the amendment (EU) 2015/863/EU.

CE Mark / UKCA

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

ANATEL

This device is homologated by ANATEL, according to the regulated procedures for conformity assessment of telecommunications devices, and meets the technical requirements applied.
This equipment is not subject to the protection from harmful interference and may not cause interference with duly authorized systems.
For more information, see the ANATEL website www.anatel.gov.br.

NORMA CISPR 22

In a domestic environment, this product may cause interference, which may require that the user take appropriate measures to minimize the interference.

11 WARRANTY

Warranty conditions are available on our website www.novusautomation.com/warranty.