GTOR-4-3G

3G to Serial
Internet Object

User
Manuel

Klemsan®

TABLE OF CONTENTS

SECTION 4   **TECHNICAL SPECIFICATIONS**

FIGURES

GTOR-4-3G

3G to Serial
Internet
Object

**SECTION 1
GENERAL
INFORMATION**

SECTION 1 GENERAL INFORMATIONS

1.1 Proper Use and Safety Conditions

● Installation and connections should be established in accordance with the instructions set out in the manual by authorized persons. Unless the connection is built properly, device should not be operated.

● Before wiring the device up, make sure that energy is cut off

● Use a dry cloth to remove the dust from the device/clean the device. Avoid using alcohol, thinner or a corrosive material.

● Device should be engaged only after all the connections are made.

● Do not open the inside of the device. There are no parts which the users can intervene inside.

● Device should be kept away from humid, wet, vibrant and dusty environments.

> ⚠️ The manufacturing company may not be kept responsible for unfavorable incidents that arise out of the failure to follow the above cautions.

1.2 General Features

GTOR-4-3G is an Internet object that has gateway and logging capabilities that are running in client and server roles through the use of 3G infrastructure. It has Modbus RS385 serial interface. Thanks to the transparent operation type, it is possible to control and monitor serial devices with MODBUS or other protocols remotely. In addition, the configuration settings of device can be read and written via USB, JSON format or via SMS. GTOR-4-3G generally has the following features:

• Work in server or client roles
• Supports up to 9 remote connections
• Work with SIM cards that support and not support static IP
• Serial server or transparent operation capability
• at 3G speed data communications
• Basic configuration with SMS messages
• Modbus RTU, Modbus ASCII, Modbus TCP support
• Data logging feature
• Easy configuration via USB or Internet
• Access to all configuration functions, information, and log records with an open JSON Rest API
• Location feature
• Software update via USB

GTOR-4-3G

**3G to Serial
Internet
Object**

**SECTION 2
DEVICE
SPECIFICATIONS**

SECTION 2 DEVICE SPECIFICATIONS

2.1 Definitions on Device
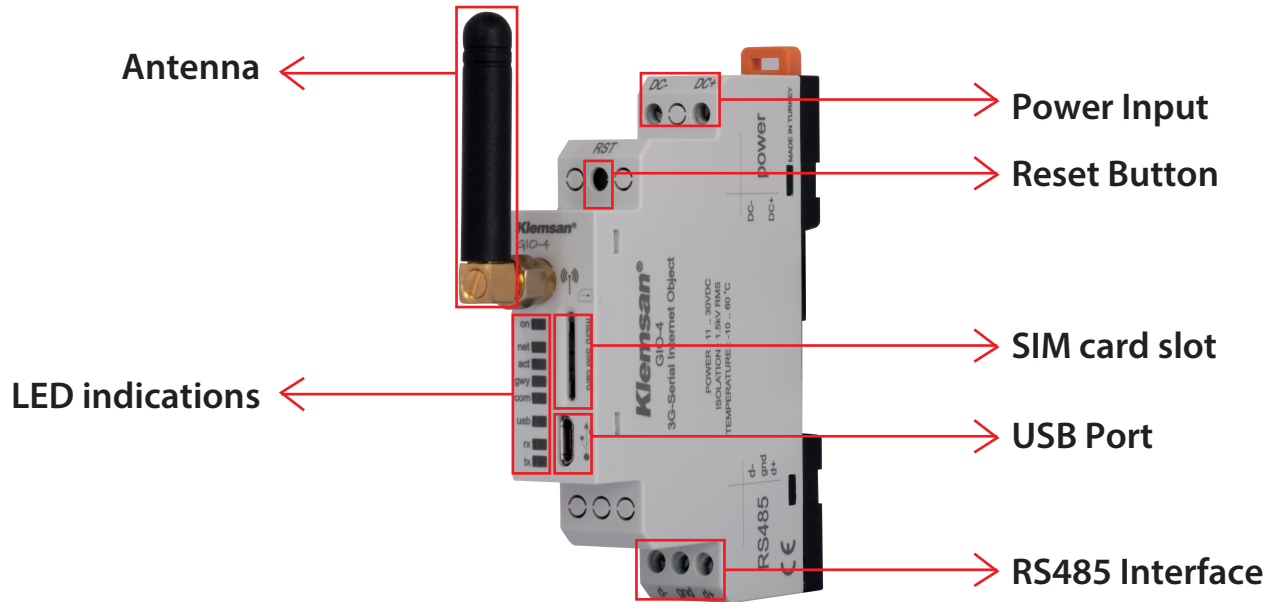
Figure 2-1 Definitions on Device

DC-,DC+ Input:

Device is powered on from DC-, DC+ input. 11 … 30V AC/DC must be applied. It has reverse voltage protection.

RST Button:

When pressed briefly (<5 sec) the device restarts. When pressed for a long time (≥ 5 sec), the device returns to the factory settings and starts again.

Micro SIM Card Slot:

This entry only supports micro SIM cards. A micro SIM card with an open PIN code must be installed on the device. If a micro SIM card is not inserted, or if a micro SIM card with a open PIN lock is not installed, it will not be able to connect to the GSM network.

Micro USB Port:

It is used to configuration, access product, production and runtime information, capture, delete, and update daily logs and to update the software of the device. It can be powered via the USB port, but the GSM functions will not be active to protect the USB port on the computer unless the main power connection is made.

NOTE: If it is fed from the main supply and USB port, the button will ignore all reset requests except the configuration and product information (production only) change.

If the device is only fed through the USB port, the button will ignore all reset requests except the configuration and product information (production only) and the supply of the main supply. When the device is powered up by USB, it is reset if the main supply is connected.

d+ - d- Input:

RS-485 connection is made from this input.

Antenna:

It is SMA type connection where external antenna connection is made.

ON LED (Red):

If the LED is on, the device's supply is from the DC-, DC+ input. Or the micro-USB cable is plugged into the device.

NET (Blue):

When connected to a 3G network, it remains on, and in other cases it remains off.

ACT (Blue):

•When the network is being dialed, it lights up to 200 milliseconds, goes out to 1800
 milliseconds

•When there is no data transfer, lights up to 1800 milliseconds, goes out to 200
 milliseconds

•When there is data transfer, it lights up to 125 milliseconds, goes out to 125 milliseconds

GWY (Green):

Indicates the status of the gateway service.

•   When the device is running in the server role, the gateway server is lit when it is connectable.

•   When the device is running in the server role, the gateway server turns on 50 milliseconds if it is not yet ready, it goes out to 450 milliseconds.

•   When the device is running in the client role, remains steady when connected to the server specified for the gateway.

•   If it is not connected to the server that is set for the gateway when it is running in the client role, it will turn on 50 milliseconds, goes out to 450 milliseconds.

•   If the RST button is pressed for more than 5 seconds, it turns on 250 milliseconds, goes out 250 milliseconds.

COM (Green):

Indicates the status of the communication service.

•   If it is running in the server role, the communication server remains steady when it is connected.

•   If it is running in the server role, the communication server turns on 50 milliseconds if it is not yet ready, it goes out to 450 milliseconds.

•   If it is running in the client role, it remains steady when connected to the server designated for communication.

•   If it is running in the client role, it will turn on 50 milliseconds, goes off to 450 milliseconds if it is not connected to the server specified for communication.

•   If the RST button is pressed for more than 5 seconds, it turns on 250 milliseconds, goes out 250 milliseconds.

USB (Yellow): When data transfer is via USB, it turns on 250 milliseconds, goes out 250 milliseconds.

RX,TX (Yellow):

When data is received from the RS-485, RX lights up; when it sends data to the RS-485, TX lights up, otherwise it remains off.

2.2 Micro SIM Replacement

While the SIM card is inserted and the device is switched on, if the SIM card is removed, the device will restart. In this case, the operation will continue as follow:

If no SIM card is inserted at the power on or the SIM lock is not deactivated,

• If there is no USB connection in the device, the device will be restarted until the SIM card is inserted in 1 minute intervals.

During this time, COMM and GWY LEDs will be on with 80% duty. The device can detect that the SIM card has been removed, but can not detect that it is inserted. Therefore, if the SIM card is inserted again in this process, the device will start to operate normally within 1 minute at the latest.

• If the device has a USB connection, the device will continue to operate. Configuration can be done and logs can be read but logging will not be done.

However, communication via USB will continue when requested.

GTOR-4-3G

3G to Serial
Internet
Object

**SECTION 3
FUNCTIONAL
SPECIFICATIONS**

SECTION 3 FUNCTIONAL SPECIFICATIONS

3.1 Operating Roles and Types

GTOR-4-3G can assume both server and client roles on a TCP connection. Regardless of the selected role, it can operate in 'Serial Master' or 'Transparent' mode.
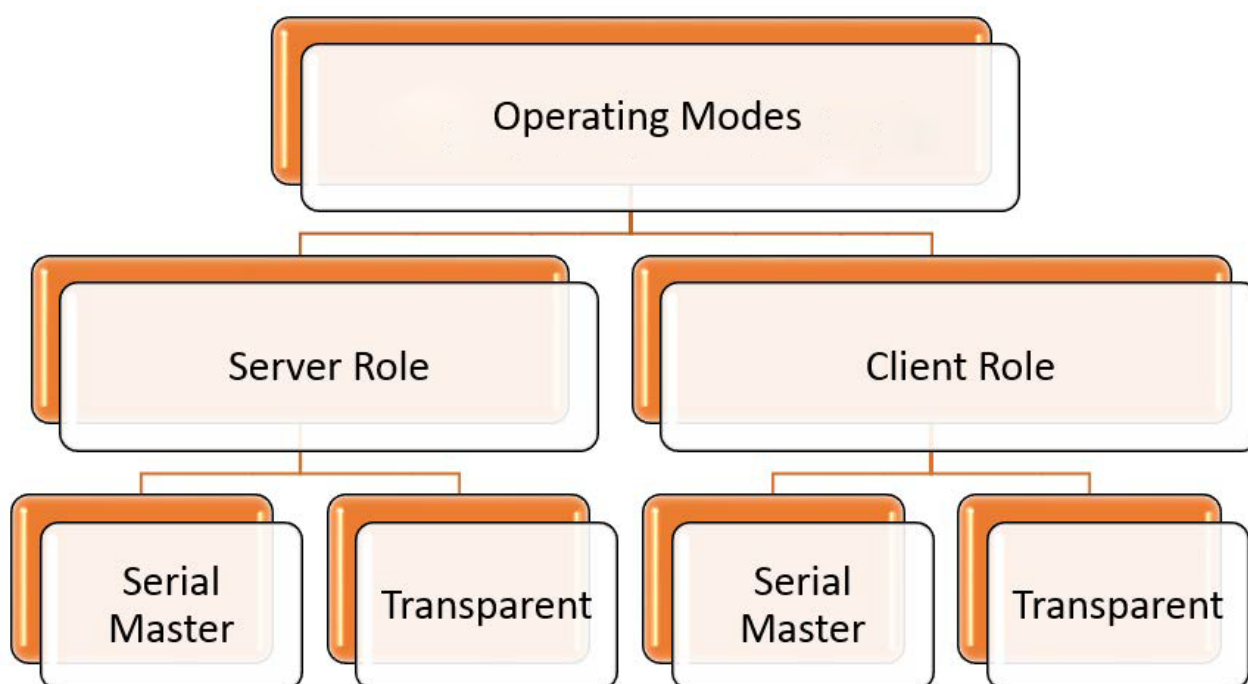
Figure 3-1 Operating Modes

3.1.1 Operating Roles

3.1.1.1 Server Role

While the device in the server role, it runs two servers on different ports for communication and gateway. It supports 1 communication connection (configuration, information and log reading) and 9 or 1 gateway connection according to the type of operation (Serial Master, Transparent). It has IP blocking feature. The IP blocking feature can be set on and off. Up to 3 permitted IP addresses can be entered if IP restriction is turned on. When a connection request is received from an unauthorized IP address, the connection is terminated and SIM card with a static IP is required.

Server Role Settings: The way of device works in the server role can be customized with the following parameters:

•**Gateway Listen Port:** The port that the gateway server will listen to. It should take a value between 1-65535.

•**Gateway IP Restriction:** It can be on or off. In the 'On' position, up to 3 allowed IPs can be entered. When a connection request is received from an unauthorized IP address, the connection is terminated.

•**Permitted Gateway IP Addresses:** When IP blocking is on, the connection requests are the IP addresses to be accepted. It supports up to 3 allowed IP addresses. (Client IP 1, Client IP 2, Client IP 3)

•**Configuration Listen Port:** The port that the communication server will listen to. It should take a value between 1-65535.

•**Configuration IP Restriction:** It can be on or off. In the 'On' position, up to 3 allowed IPs can be entered. When a connection request is received from an unauthorized IP address, the connection is terminated.

•**Permitted Configuration IP Addresses:** When IP blocking is on, the connection requests are the IP addresses to be accepted. It supports up to 3 allowed IP addresses. (Client IP 1, Client IP 2, Client IP 3)

3.1.1.2 Client Role

While the device in the client role, two clients run on different ports for communication (configuration, information and record reading) and gateway (queries to be forwarded to the serial line).

A SIM card with a static IP is not required. For both communication and gateway clients, up to 3 server addresses can be entered. It tries the entered servers with both clients, respectively, and connects to 1 of them. The server IPs and ports of communication and gateway clients may be different. After the communication and gateway connection are established, the device sends a data to identify itself to the server. Using this data, it can be checked whether the it is connected to the desired server.

Since the device is connected to the server, the information it contains consists of 4 bytes with 12 bytes total of 48 bytes. This information is as follows.
Information 1: Company Name (12 Bytes)
Information 2: Device model (12 Bytes)
Information 3: Device serial number (12 Bytes)
Information 4: Order number (12 Bytes)

Client Role Settings: The way of device works in the client role can be customized with the following parameters:

•   **Gateway Server Port:** The port to which the gateway client is connected. It should take a value between 1-65535.
•   **Gateway Server Addresses:** The addresses of the servers where the gateway client will attempt to connect in sequence. It supports up to 3 server addresses. A connection request to other addresses is not sent after it has connected to one of these addresses. (Server IP 1, Server IP 2, Server IP 3)
•   **Retry Interval:** If the device cannot connect to any server in the server list, it scans the server list from the beginning. The gateway retry interval is the time that it will wait before it rescans.
•   **Configuration Server Port:** The port to which the configuration client is connected. It should take a value between 1-65535.
•   **Configuration Server Addresses:** The addresses of the servers in which the configuration client will try to connect in turn. It supports up to 3 server addresses. A connection request to other addresses is not sent after you have connected to one of these addresses.(Server IP 1, Server IP 2, Server IP 3)
•   **Retry Interval:** If the device cannot connect to any server in the server list, it scans the server list from the beginning. The retry interval is the time it waits before resuming the scan.

3.1.2 Operating Types

3.1.2. 1 Serial Master Type

Supports up to 9 gateway connections (queries to be forwarded to the serial line). When the device works in the serial master type, it waits for a remote query and converts the incoming query to the protocol supported by the devices on the serial line, depending on the configuration. It requests the query from the serial line and transmits the response it received to the query type.
Serial Master Settings:

•**Request Timeout:** If a new query from the remote connection to the device does not reach until the request time-out period expires, it terminates the remote connection.

NOTE: If the device is running in client mode, it will attempt to reconnect with the server after this time is completed. Setting the query timeout to 60000 ms (1 minute) may cause problems with applications running on servers. The ideal determination of this period is as follows.
(For Client mode)
Query timeout = Communication frequency + 2 minutes

For instance
- In a system with a ModBus query per minute, the request timeout parameter must be set to
  1 minute + 2 minutes => 3 minutes.
- In a system with a ModBus query every 5 minutes, the request timeout should be set to
  5 minutes + 2 minutes => 7 minutes

•**Response Timeout:** It is the waiting time for each serial device to be responded in the MODBUS network of the device. If no response is received from the device in which the query was sent during this time, the next remote connection query is passed.

•**Convertion:** When the device is running as serial master, makes the following conversions on the remote and serial sides:
ModBus Gateway:
    -Modbus TCP - Modbus RTU: After the Modbus TCP query obtained from the remote connection has been verified, it is transmitted from the serial line by converting it to Modbus RTU query. After the Modbus RTU response received from the serial device is verified, it is converted to Modbus TCP and forwarded to the remote connection.
    -Modbus TCP - Modbus ASCII: After the Modbus TCP query received from the remote connection has been verified, it is transmitted from the serial line by converting it to the Modbus ASCII query. After the Modbus ASCII response received from the serial device is verified, it is converted to Modbus TCP and forwarded to the remote connection.
    -Modbus RTU - Modbus RTU: After the Modbus TCP query received from the remote connection has been verified, it is transmitted from the serial line by converting it to the Modbus ASCII query. After the Modbus ASCII response received from the serial device is verified, it is converted to Modbus TCP and forwarded to the remote connection.

-Modbus RTU - Modbus ASCII: The Modbus RTU (Modbus RTU over TCP) received from the remote connection has been verified and then transmitted to the Modbus ASCII query and passed through the serial line. Modbus ASCII response received from serial device is converted to Modbus RTU and then forwarded to remote connection.

    -Modbus ASCII - Modbus RTU: The Modbus ASCII (Modbus ASCII over TCP) received from the remote connection is verified and transmitted to the Modbus RTU query and forwarded from the serial line. After the Modbus RTU response received from the serial device is verified, it is converted to Modbus ASCII and forwarded to the remote connection.

-Modbus ASCII - Modbus ASCII: The Modbus ASCII (Modbus ASCII over TCP) received from the remote connection is verified and transmitted to the Modbus RTU query and forwarded from the serial line. After the Modbus RTU response received from the serial device is verified, it is converted to Modbus ASCII and forwarded to the remote connection.

Pass-through:

The data received from the remote connection is transmitted directly to the serial line, and the received response is forwarded directly to the remote connection without the protocol conversion and verification. This makes it possible for users to use their own local protocols or protocols that are not supported by device.

3.1.2.2 Transparent Type:

It supports 1 gateway connection (the connection to be transmitted to the serial line) while operating in transparent mode.

The query direction is negligible. The remote transmits data from the serial line to the remote connection on the serial line. In this type of operation, it can be considered as a virtual serial cable. In this way, any device with RS-485 connection is able to communicate over the Internet.

Transparent Settings:

•**Communication Timeout:** If no data flow occurs during the timeout period from the serial or remote connection, the remote connection will be terminated by the device.

•**Idle Character Count:** If the number of characters to wait after the last character has elapsed, the data is routed to the remote connection.

•**Max. package Byte Count:** When the data length from the serial line reaches the maximum packet length, the data is routed to the remote connection without waiting.

3.2 Serial Interface

The serial parameters of the device must be compatible with the devices in the serial line to which it is connected for correct data transfer.

Serial Settings: Supported serial settings are as follows:

•**Baud Rate:** Supports 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud rates.

•**Parite :** None, even and odd parity communication is supported.

•**Stop Bit :** 1 and 2 values are supported.

3.3 APN/SMS Settings

APN:

The settings of the APN defined by the SIM card inserted in the device are entered in this tab. If these settings are not set correctly, data communication will not occur.

APN Name: The gateway that provides the switch between the mobile network and the computer network to use. It has a maximum of 31 characters.
APN Username: Up to 31 characters.
APN Password: Up to 31 characters. This setting can only be changed via serial communication.

SMS:

Depending on the configuration, read the configuration data of the required device information and change some configuration data (server addresses and ports etc.) via SMS. SMS messages must be sent to the subscriber number of the SIM. The SMS feature can be on or off. It has ability to control phone number. The phone number control feature can be set on and off. Up to 3 allowed phone numbers can be entered if the phone number check is on. The commands from numbers other than those phone numbers are ignored.

SMS Communication: The SMS function can be on or off. In this case, the SMS features will not be available.
Service Number: The service number specified by the operator. Required for SMS functions to work.
Service Type: It is the type of service determined by the operator. Required for SMS functions to work.
Number Restriction Mode: The device may only be able to take into account messages received from the specified numbers (up to 3). This feature can be selected either on or off. If this feature is off, the device will consider each message as long as the SMS messages are correct. If this feature is turned on, it will only consider messages from the specified numbers.

3.4 Logging Settings

GTOR-4-3G has logging functionality as well as gateway functionality. Thanks to this feature, it is possible to perform continuous data monitoring even in situations where internet outages occur frequently.

The device will ask the user for up to 10 Modbus RTU or Modbus ASCII queries from the serial line with the period specified by the user. It records the datas received from the serial line by date and time. Received datas are kept in the non-volatile memory.

The query period can be between 1-60 minutes with a minute resolution. In this way, it is possible to keep up to 1440 records per day for each query. In the memory, it keeps a record of 7 days for each query. The oldest record will be automatically deleted when the recording of the 8. day is added.

NOTE: In order for the logging functions to be performed correctly, the device requires date and time information.

In order for the device to obtain the current date and time information, a valid NTP server address must be defined to the device during configuration. It only connects to the NTP server for one time only at boot time and updates the date and time information. It uses these current date and time values until the power is turned off. The date and time information is kept at UTC and must be converted to local time by the user. If a non-valid NTP server is defined, logging will not start because the device cannot update the date and time information.

Saved records, recording statistics and logging dates can be retrieved via USB and via internet in the JSON format. The records of the desired days and the records of the desired query can be deleted via the same interfaces.

NOT: Logging is a feature that can be turned on and off, but it can only be turned on when running in the serial master type. Logging functions cannot be used in transparent operation.

Logging Settings: The logging function can be managed with the following settings:

Serial Timeout(msec.): After the user-entered queries are sent to the serial line, it starts waiting for the response from the serial line again. The duration of time it will wait is determined by this parameter. It can be between 1000 milliseconds and 4000 milliseconds.

Query Period(min.): This parameter specifies the time interval during which the queries are sent to the serial line. When the period expires, all queries are sent in series one after the other and wait until the next period. It can be adjusted from 1 minute to 60 minutes.

NTP Server Address: The address of the time server that the device will use to update time and date information. Logging functions will not work if this address is not valid. (Örn: time.google.com)

NTP Server Port: The port number of the device to use to update time and date information. If this port number is not valid, the logging functions will not work. (rn: 123)

Only logging settings are not enough to start logging. Periodic queries that will be sent to the serial line must also be defined to the device.

Query Settings: The parameters required to add a new query are as follows:

Protocol: It can be selected as Modbus RTU or Modbus ASCII. Device will create its own queries according to the selected query type.

Slave Id: Modbus address of the serial device where the query is sent. It can be between 1-254.

Function: 1,2,3,4.

Address: Starting register address is selected. It can be set between 0-65535.

Quantity: It can be adjusted from 1 to 125.

GTOR-4-3G

3G to Serial
Internet
Object

SECTION 4
USER INTERFACE
PROGRAM
AND
CONFIGURATION
SETTINGS

SECTION 4 USER INTERFACE PROGRAM AND CONFIGURATIONSETTINGS

4.1 Required Installations for Configuration Software

This section will explain the setups necessary to configure the device via the

USB port. You can find the required files in the Klemsan website.

4.1.1 Installation of Gateway Master
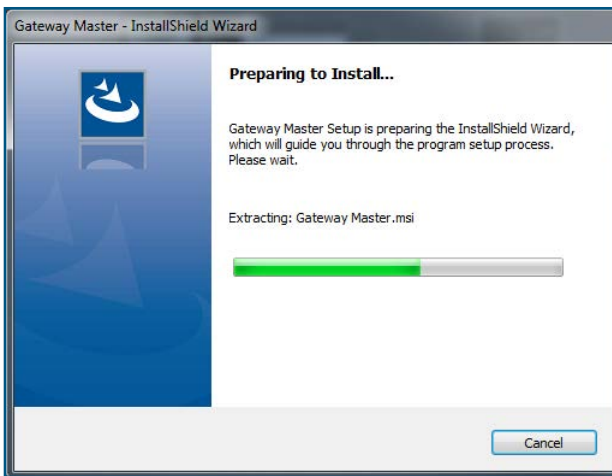
Figure 4-1 Setup-1
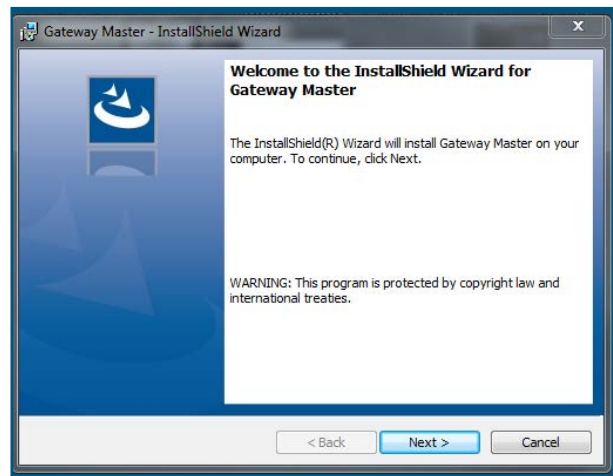
Figure 4-2 Setup-2
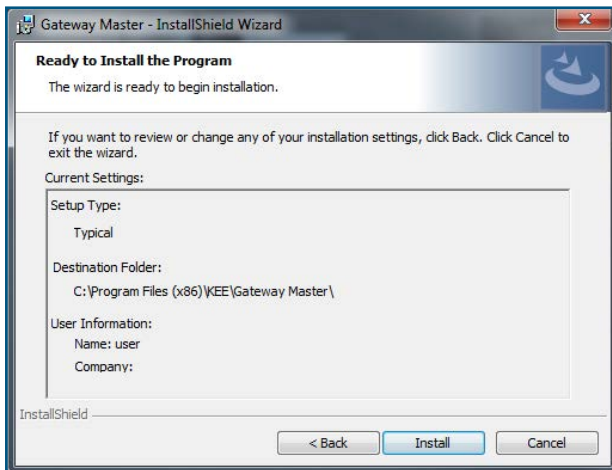
Figure 4-3 Setup-3
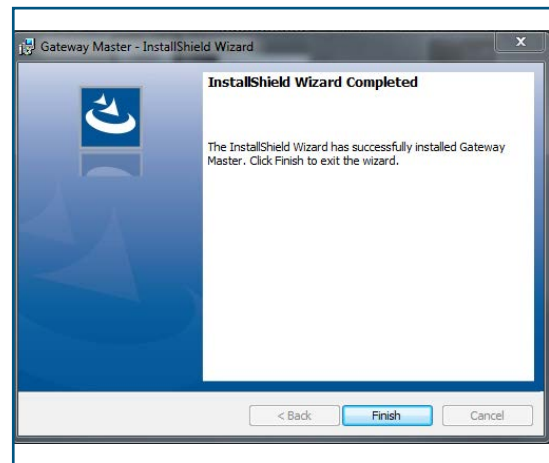
Figure 4-4 Setup-4

The setup wizard will display a list that summarizes the contents to be loaded. Installation is started by clicking "Next" button again. When the installation is finished, click "Finish" to complete the installation.

4.1.2 Installation of GTOR-4-3G USB Driver:

For USB Driver installation, the following screens will come up after program installation. By following the steps you can set up your driver.

Figure 4-5 Setup-5

Figure 4-6 Setup-6

When the installation is completed, by clicking the "Finish" button, the installation is completed and the Gateway Master is ready for use.

● The connection between the computer where the program is installed and the device should be connected with the Micro-USB cable.
● Then the configuration program should be run. The Configuration Program can be accessed from the Windows Start menu or from the desktop shortcut.
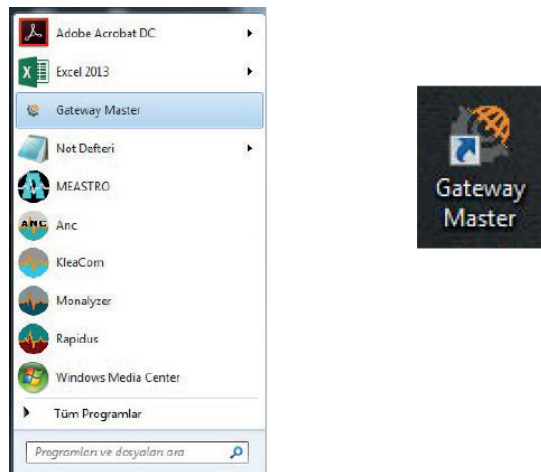
Figure 4-7 Configuration Program Shortcuts

4.2 Configuration Settings

Gateway Master can configure the device via micro-USB in serial or it can be configured in server/client roles over TCP / IP .
After the initial settings are made via USB, it can be configured with the 'Server' or 'Client' roles via the user interface program or via the RestAPI service in JSON format with SMS or HTTP protocol regardless of the Gateway Master program.
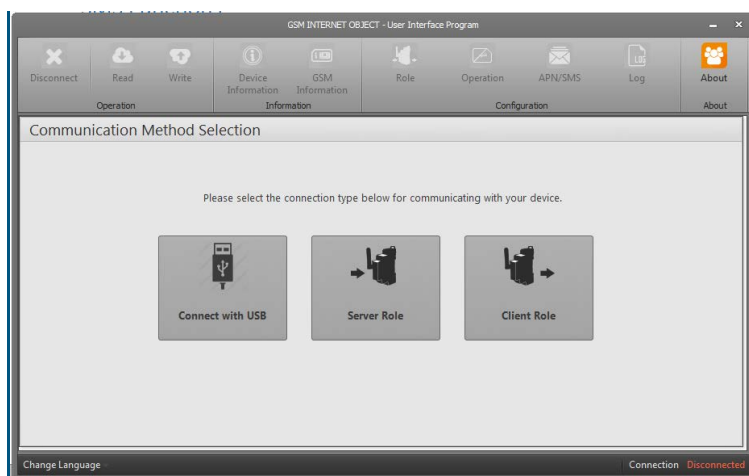
Figure 4-8 Connection Types

NOT: Once the device is connected to one of these options, press the 'Write' button to save the changes made.

4.2.1 Connect with USB

It is used to configure GTOR-4-3G , access product, production and working information, capture, delete, and update daily logs and to update the firmware. The device can be powered via the USB port, but the GSM functions will not be active to protect the USB port on the computer unless the main power connection is made.

•	It will restart and activate the GSM functions if the main power connection is made while the USB cable is connected.
•	If the main power connection is disconnected while feeding from both USB and the main line, it will restart from the beginning and will not activate the GSM functions. Under normal operating conditions, the connection will be recognized by the computer as a virtual COM port. In this way, users can easily send JSON Rest API queries to the device via their own software without the need for the Gateway Master.

NOT: When the USB interface is used for software update, the software provided by Klemsan must be used.

When the "Connect with USB" button is pressed, settings are read and written in series via micro-USB.

While the device is connected to PC via USB port, if the virtual port is not shown, virtual port list can be refreshed by pressing "Refresh" button.
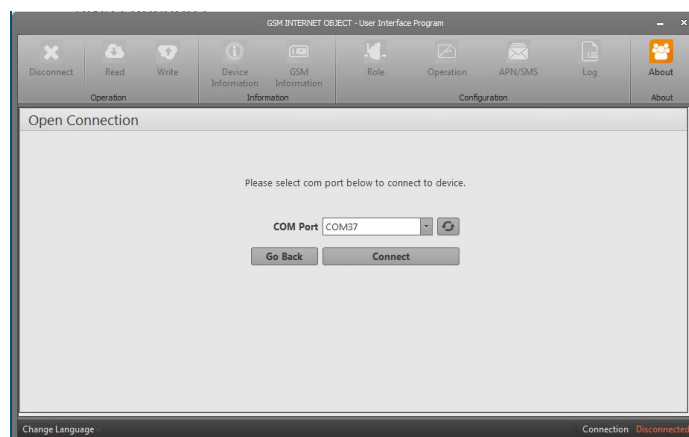
Figure 4-9 Virtual Serial Port

NOTE: USB connection must not be interrupted before the "Disconnect" button is pressed.

When is accessed via USB, the information and configuration settings become active.

4.2.1.1 Device Information

This tab contains information about the device. In the "Product Information" section, there is information about the product, in the "Production Information" section, there is production information about the production.
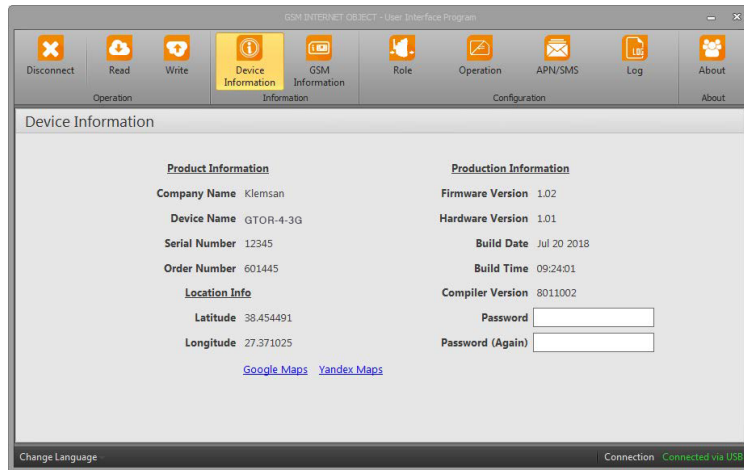
Figure 4-10 Device Information

4.2.1.2 GSM Information

This tab contains IMEI number, IP address and GSM Operator informations.
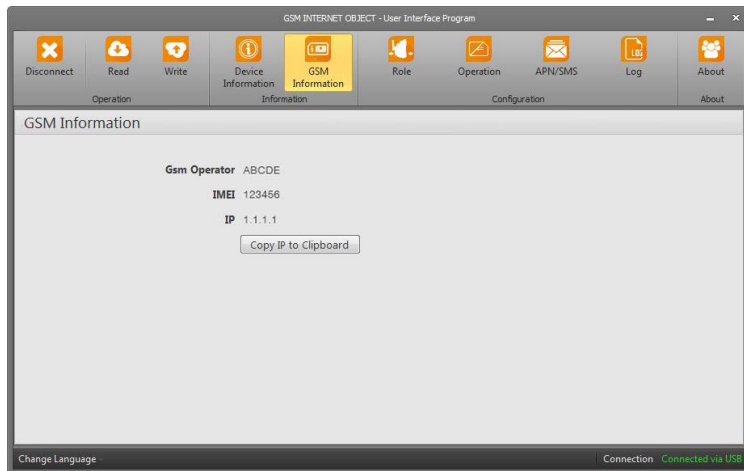
Figure 4-11 GSM Information

4.2.1.3 Role Settings

In this tab, the 'Role' settings that device will work are made. (Refer to 3.1.1.1 Server Role, 3.1.1.2 Client Role)
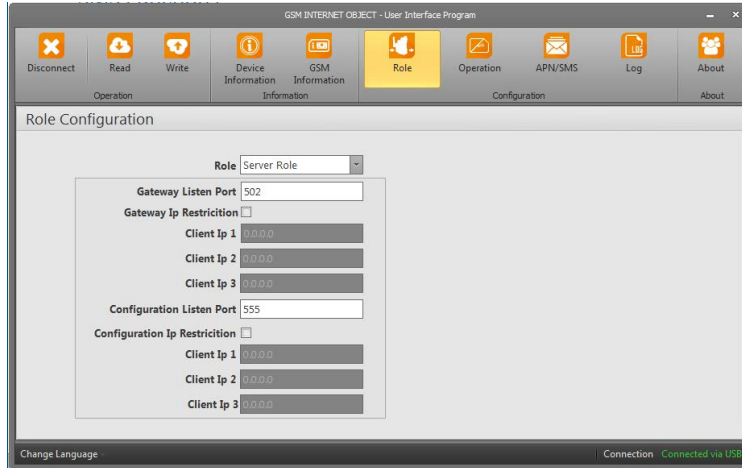
Figure 4-12 Server Role
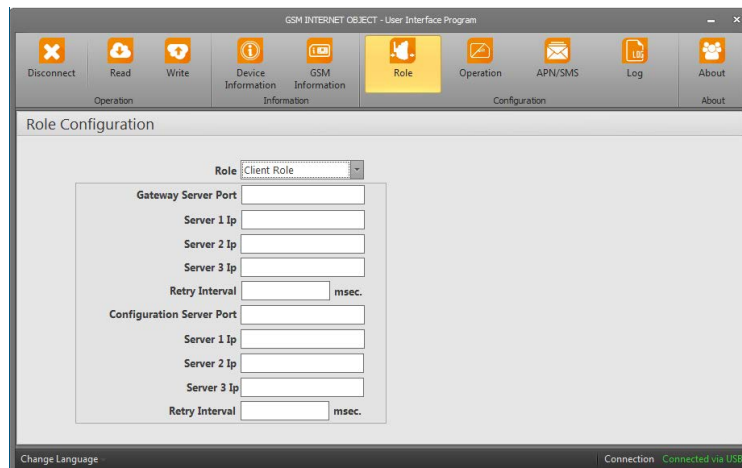
Figure 4-13 Client Role

4.2.1.4 Operation Settings

In this tab, operating modes and serial communication settings are configured. (Refer to 3.1.2.1 Serial Master Type , 3.1.2.2 Transparent Type, 3.2 Serial Interface)
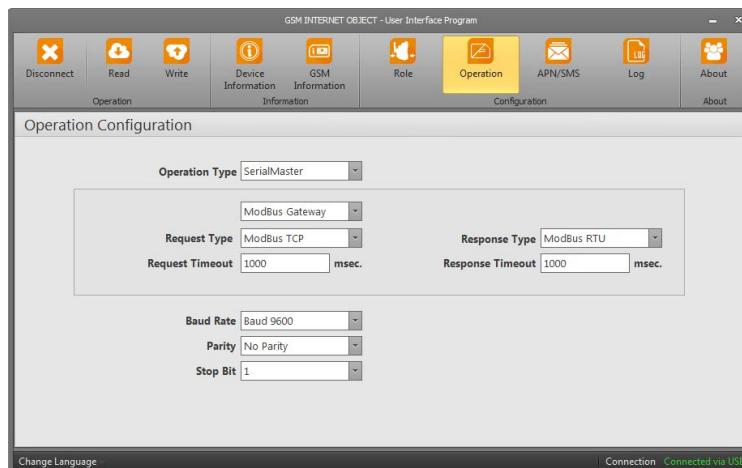
Figure 4-14 Serial Master
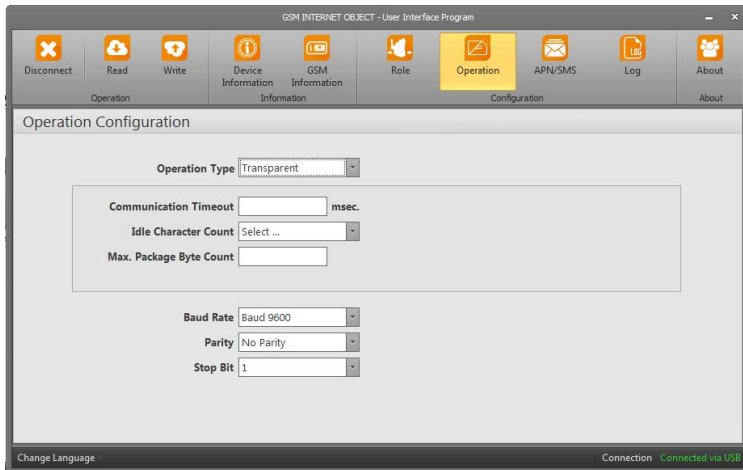
Figure 4-15 Transparent

4.2.1.5 APN/SMS Settings

In this tab, APN and SMS settings are configured. (Refer to 3.3 APN/SMS Settings)
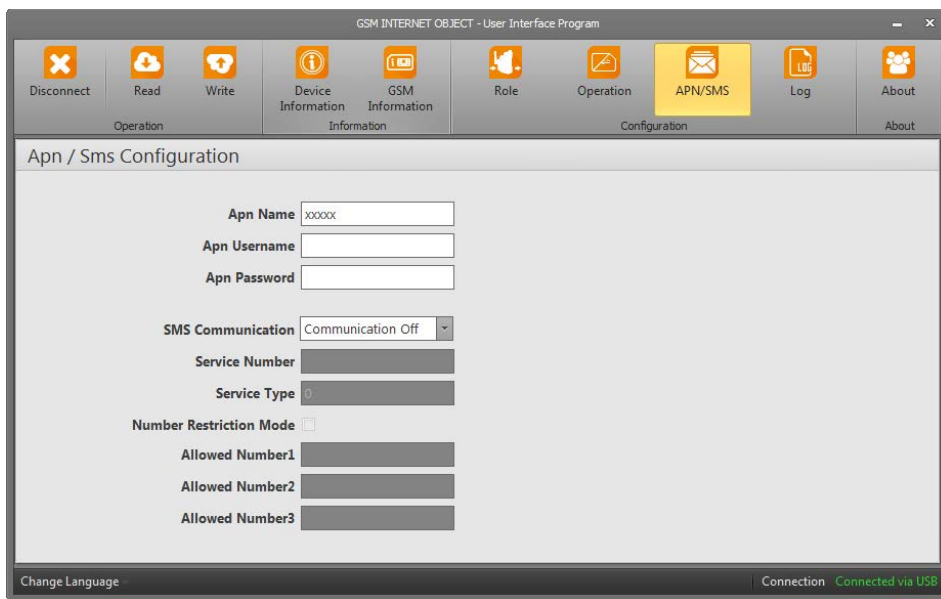
Figure 4-16 APN-SMS

4.2.1.6 LOG Settings

The logging function is activated under this menu. Timeout, query period, NTP server address and NTP server port are set under this menu. If a non-valid NTP server is defined, logging will not start because the device cannot update the date and time information.
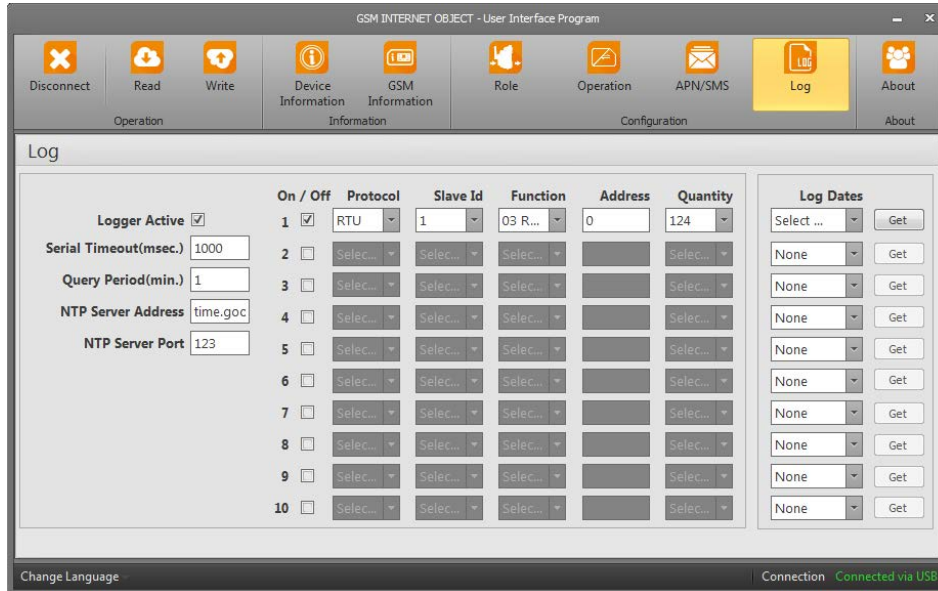
Figure 4-17 Log

To access the recorded logs, select the desired date under 'Log Dates' and press the 'Get' button. The following screen will then appear:
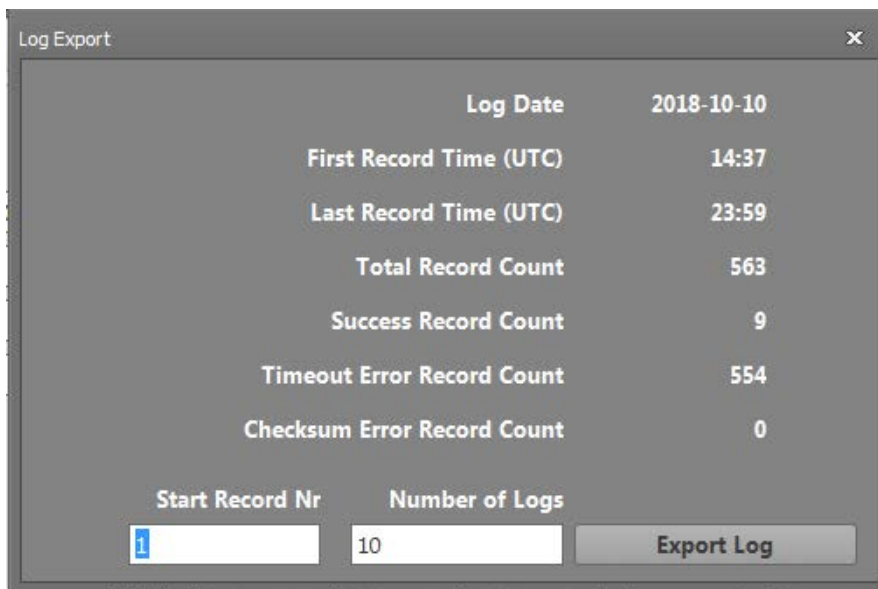
Figure 4-18 Export Log

This screen contains the log date, first and last recording time (UTC), total recors, number of successful and unsuccessful records. In order to export, the starting number of the logs and the number of logs are written and the required logs are saved in 'JSON' format by the 'Export Log' button.
The file is automatically created to include the device serial number, log number, date, and recorded file number information.

The file should be opened with Notepad.

For instance, file opened with Notepad will seem in the following format.

{"recordNo":4,"time":"08:58","state":"success","response":[1,3,4,249,14,194,65]}

RecordNo: Number of records.

Time: Shows the recording time.

State: Recording status

Response: Shows Slave ID, function, number of byte and data value (decimal)

The following steps should be followed in order to read "response" information in the file as a significant number.

---

1. The numbers in the file will be as follows.

1	3	4	87	82	191	65
			1.byte	2.byte	3.byte	4.byte

Slave ID

Function

Number of Byte
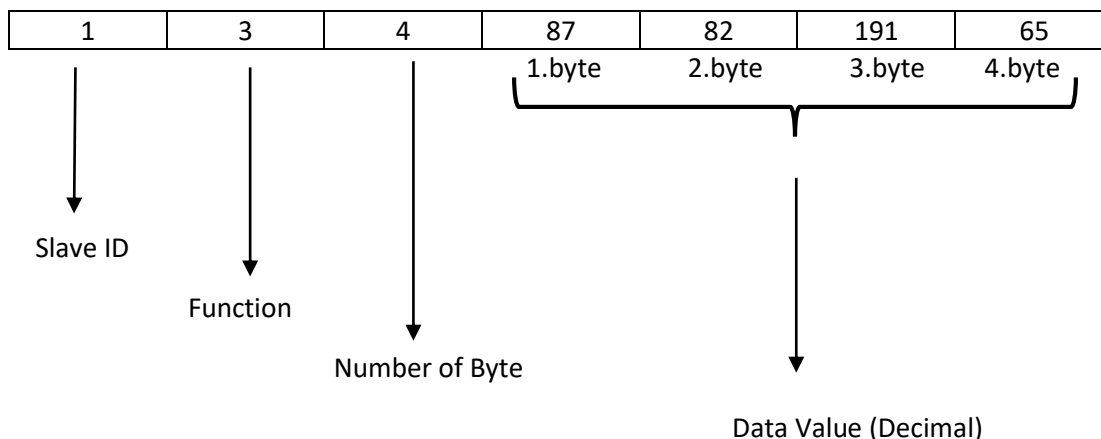
Data Value (Decimal)

2. The value of the data registered (decimal) must be converted to hexadecimal value. The following steps should be followed for this;

- The data value in the recorded file is decimal.

$(87)_{10}$	$(82)_{10}$	$(191)_{10}$	$(65)_{10}$

Decimal

- Decimal value must be converted to Hexadecimal form.

$(57)_{16}$	$(52)_{16}$	$(BF)_{16}$	$(41)_{16}$

Hexadecimal

- In the last step, the Hexadecimal value must be converted to the data type (integer, float, etc.) of the address held by the Log. For instance, the log value is set to float type. The number which is hexadecimal is converted to float type.

(Hex to Float) $(23.915205)_{float}$

NOTE: Numbers can be converted with conversion program.

4.2.2 Configuring with Server Role

After the settings of the SIM card to be used with the device are made, the same settings can also be accessed with the server role. The SIM card to be used must have a static IP. In addition, the default configuration port '555' or the user-specified port must be used. The default password is 'Pass'. After all the settings are done, the device settings are accessed by the 'Connect' button.
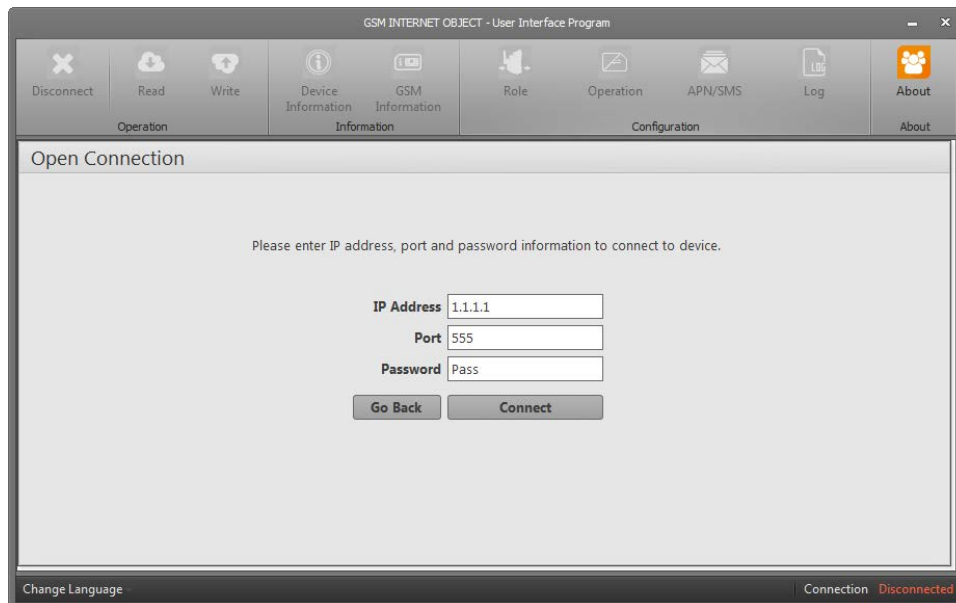
Figure 4-19 Configuration - Server Role

4.2.3 Configuring with Client Role

After the settings of the SIM card to be used with the device are made, the same settings can also be accessed with the client role. A SIM card with a static IP is not required. Predefined configuration port for the client role must be used. The serial number information of the product must be entered correctly. The default password is 'Pass'. After all the settings are done, the device settings are accessed by the 'Start Listen' button.
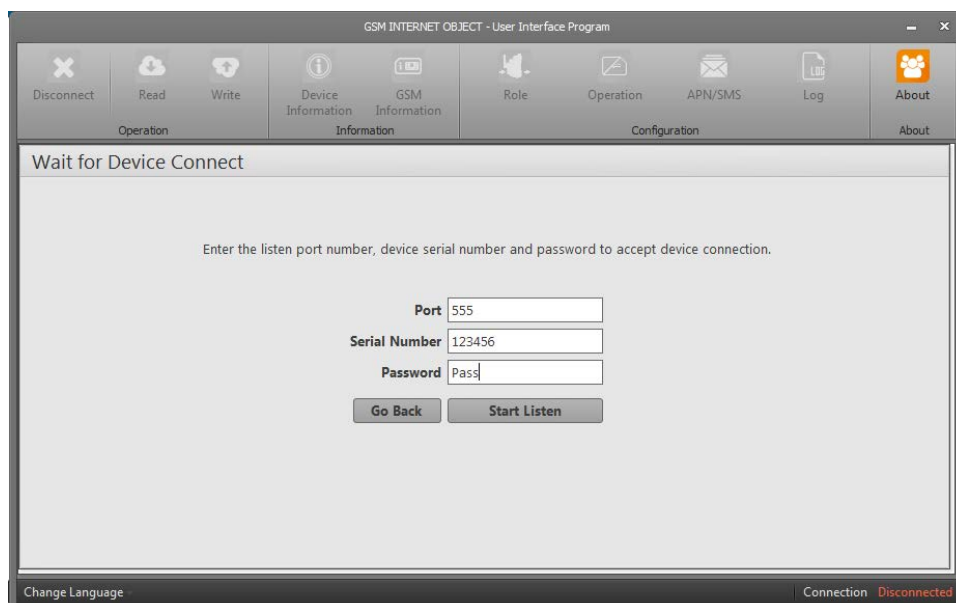
Şekil 4-20 Configuration - Client Role

4.2.4 Configuration with SMS

In order for the device to make sense of the SMS messages sent, the messages to be sent must be arranged in a specific format. At the beginning of the message, there must be a pre-defined password. After the password, a space and one of the valid commands must be written in <u>capital</u> letters.

[password] [Command] < variable value>

NOTE: In case of password error, the device ignores received SMS messages and does not send a reply. If the password is correct but the command is incorrect, it sends an "ERROR message. When assigning values, Turkish characters should not be used.

4.2.4.1 Valid Commands

1) INFO: This command must be used to get a summary of the current operating status. If the password is set to "password", the SMS message to be sent should be as follows:

```
password INFO
```

It will send different answers depending on its role.

Server Role: When the device working in the server role, it will reply in the following format.

```
ROLE: SERVER
IP: [IP of GTOR-4-3G ]
PORT: [Communication port of GTOR-4-3G ]
ALLOWED IPS:
<ALL>

<IP1>
<IP2>
<IP3>
```

If the IP blocking function is on under the "Configuration IP Restriction"; the allowed IPs (if entered) will be listed. If the IP blocking function is turned off, the word 'ALL' means that all IPs are allowed.

Example: In the server role, if the IP address is AAA.BBB.CCC.DDD, communication port 555, and the IP blocking function is off, it will give the following answer:

```
ROLE: SERVER
IP: AAA.BBB.CCC.DDD
PORT: 555
ALLOWED IPS:
ALL
```

Example: In the server role, if the IP address is AAA.BBB.CCC.DDD, communication port 555 and the IP blocking function is on and the allowed IPs are EEE.FFF.GGG.HHH and III.JJJ.KKK.LLL, it will give the following answer:

```
ROLE: SERVER
IP: AAA.BBB.CCC.DDD
PORT: 555
ALLOWED IPS:
EEE.FFF.GGG.HHH
III.JJJ.KKK.LLL
```

Client Role: When the device working in the client role, it will reply in the following format.

```
ROLE: CLIENT
SERVER IPS:
<IP1>
<IP2>
<IP3>
PORT: [Communication port of GTOR-4-3G ]
```

Under th SERVER IPS title; The server addresses to which the device will attempt to connect will be listed. (Server addresses with no value assigned will not be listed.)

Example: In the client role, if the communication port is 555 and the server IPs are EEE.FFF.GGG.HHH and III.JJJ.KKK.LLL, it will give the following answer:

```
ROLE: CLIENT
SERVER IPS:
EEE.FFF.GGG.HHH
III.JJJ.KKK.LLL
PORT: 555
```

2) SETALWIP: This command is only valid when the device is running in the server role and the IP blocking function is active. Enables the identification of IP addresses to be allowed to connect.

```
password SETALWIP [i] [IP]
```

The "i" parameter in this command refers to the area in which the IP value to be allowed is assigned. It should be one of the values 1, 2 and 3. "IP" is the IP address to be allowed.

Example: The following SMS message must be sent while the device in the server role and when the IP blocking function is turned on, if it is wanted to enter the EEE.FFF.GGG.HHH IP in the second field of the allowed IPs list:

```
password SETALWIP 2 EEE.FFF.GGG.HHH
```

It makes the necessary changes and approves the transaction with the following message:

```
OK
```

If the device is not in the server role, or the IP blocking function is turned off while device working in the server role it sends the following SMS message:

```
ERROR
```

3) SETSERVER: This command is only valid when the device working in the client role. It allows to determine which servers it will attempt to connect to while the device running in the client role.

```
password SETSERVER [i] [IP]
```

The "i" parameter in this command refers to the area in which the IP value to be allowed is assigned. It should be one of the values 1, 2 and 3. "IP" is the IP address to be allowed.

Example: The following SMS message must be sent while the device in the server role and when the IP blocking function is turned on, if it is wanted to enter the EEE.FFF.GGG.HHH IP in the third field of the allowed IPs list:

```
password SETSERVER 3 EEE.FFF.GGG.HHH
```

It makes the necessary changes and approves the transaction with the following message:

```
OK
```

If it is not in the client role, it sends the following SMS message:

```
ERROR
```

4) SETAPN: Used to change the access point name (APN).

```
password SETAPNUSER [apn user name]
```

Example: If you want to set the access point name 'user1', the following SMS message must be sent.

```
password SETAPNUSER user1
```

It makes the necessary changes and approves the transaction with the following message:
```
OK
```

5) SETAPNUSER: The user name for the access point is entered.

```
password SETAPNUSER [apn user name]
```

Example: If you want to set the access point user name "user1", the following SMS message must be sent.

```
password SETAPNUSER user1
```

It makes the necessary changes and approves the transaction with the following message:

```
OK
```

6) SETAPNPASS: The user password for the access point is entered.

```
password SETAPNPASS [apn user password]
```

Example: If you want to set the access point user password "pass1", the following SMS message must be sent.

```
password SETAPNPASS pass1
```

It makes the necessary changes and approves the transaction with the following message:

OK

7) RESTART: It is used to restart the device. The following message has to be sent:

```
password RESTART
```

When the device receives this message, it sends the following message and restarts after one second.

```
OK
```

8) SAVE: This command saves the changes made.

```
password SAVE
```

When the device receives this message, it sends the following message and restarts after one second.

```
OK
```

4.2.5 JSON RestAPI

It has the interface to read device information, read / write configuration data and read / delete record data without being dependent on any program. Using standard HTTP methods (GET, PUT, POST, DELETE), the requested data can be read or written in JSON format.

4.2.5.1 General Communication Settings

The device communicates with two different interfaces. These interfaces are remote connection and USB. Unless otherwise specified, all parameters in the document can be used for remote connection and communication via USB.

•Authentication:
The communication is secured with the "Basic" authentication algorithm. The user name is always "user". The user password is the password specified in the configuration.
•Mandatory HTTP header fields and values
        HTTP Method: GET | POST | PUT | DELETE
        HTTP Version: HTTP/1.1 | HTTP/2
        Server(Only available on remote connection): Host:
        AAA.BBB.CCC.DDD:PPP (IPAddress:PortNumber)

URL: The required data will be defined in the following pages of the document, depending on the topics.

Content Type: Content-Type: application/json

Authentication (Only available on remote connection): Authorization: Basic xxxxxxxxxxxx

•'Query succeed' answer:

It is the response that the query is correct.

Code 200: OK.

•'Query failed' answer:

It is the response that the query is incorrect.

Code 400 Bad Request: This error is run, if the non-valid request, the wrong content type, unsupported http method invalid the json parameter are sent.

Code 401 Unauthorized: This error is run if an incorrect user name / password is entered.

Code 404 Not Found: This error is run if the requested resource is not found.

4.2.5.2 Serial Communication Settings

This is the chapter where the functions enabling that serial communication data can be read and written are described.

•URL

/settings/serial

•Method:

GET | PUT

•Data Parameters

Baudrate: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Parity: "none" , "even" , "odd"

Stopbit: 1, 2

```
{
    "baudrate": 38400,
    "parity": "none",
    "stopBits": 1
}
```

4.2.5.3 Device Role Settings

This is the chapter where the functions enabling that device role data can be read and written are described. The device runs in server and client roles.

•URL

/settings/role

•Method:

GET | PUT

•Data Parameters

Server Role Parameters:

•gateway:
  port: 1-65535
  allowedIps: [AAA.BBB.CCC.DDD, EEE.FFF.GGG.HHH, III.JJJ.KKK.LLL]
  ipRestriction: true (Ip restrction on), false(Ip restriction off)
•communication:
  port: 1-65535
  allowedIps: [AAA.BBB.CCC.DDD, EEE.FFF.GGG.HHH, III.JJJ.KKK.LLL]
  ipRestriction: true (Ip restrction on), false(Ip restriction off)

Client Role Parameters:
•gateway:
  port: 1-65535
  remoteIps: [AAA.BBB.CCC.DDD, EEE.FFF.GGG.HHH, III.JJJ.KKK.LLL]
  retryInterval: 1000-600000
•communication:
  port: 1-65535
  remoteIps: [AAA.BBB.CCC.DDD, EEE.FFF.GGG.HHH, III.JJJ.KKK.LLL]
  retryInterval: 1000-600000

Server Role:

```
{
    "type": "server",
    "gateway": {
        "port": 502,
        "allowedIps": [
            "0.0.0.0",
            "0.0.0.0",
            "0.0.0.0"
        ],

"ipRestriction": false
    },
    "communication": {
        "port": 555,
        "allowedIps": [
            "0.0.0.0",
            "0.0.0.0",
            "0.0.0.0"
        ],

"ipRestriction": false
    }

}
```

Client Role:

```
{
    "type": "client",
    "gateway": {
        "port": 502,
        "remoteIps": [
            "0.0.0.0",
            "0.0.0.0",
            "0.0.0.0"
        ],

"retryInterval": 5000
    },
    "communication": {
        "port": 555,
        "remoteIps": [
            "0.0.0.0",
            "0.0.0.0",
            "0.0.0.0"
        ],

"retryInterval": 5000
    }

}
```

GTOR-4-3G

**3G to Serial
Internet Object**

SECTION 4 USER INTERFACE PROGRAM AND CONFIGURATIONSETTINGS

4.2.5.4 Device Operation Settings

This is the chapter where the functions enabling that device operation data can be read and written are described. The device runs in serial administrator and transparent operations.

•URL
/settings/operation
•Method:
GET | PUT
•Data Parameters
Serial Master Operation Parameters:

  type: "serial-master" (Operation Type)
  reqTimeout: 1000 - 600000 (Request Timeout)
  resTimeout: 1000 - 600000 (Response Timeout)
  conversion:
          "mtcp-mrtu" (Modbus TCP - Modbus RTU)
          "mtcp-mascii" (Modbus TCP - Modbus ASCII)
          "mrtu-mrtu" (Modbus RTU over TCP - Modbus RTU)
          "mrt-mascii" (Modbus RTU over TCP- Modbus ASCII)
          "mascii-mrtu" (Modbus RTU over TCP - Modbus ASCII)
          "mascii-mascii" (Modbus ASCII over TCP - Modbus ASCII)
          "pass-through"(transmission)

Transparent Operation Parameters:
  type:" transparent" (Operation Type)
  commTimeout: 1000 - 600000(Communication Timeout)
  serialIdleChar: 1, 2, 4, 8, 16, 32, 64, 128
  serialMaxPacketLength: 16 .. 1460

Serial Master Operation: Transparent Operation

```
{                                           {
    "type": "serial-master",                    "type": "transparent",
    "reqTimeout": 60000,                        "commTimeout": 60000,
    "resTimeout": 1000,                         "serialIdleChar": 4,
    "conversion": "mtcp-mrtu"                   "serialWaitValue": 1460
}                                           }
```

35

4.2.5.5 APN Settings

This is the chapter where the functions enabling that APN data can be read and written are described. This data can only be written via USB.

•URL
/settings/apn
•Method:
GET | PUT
•Data Parameters
apn: up to 32 characters
userName: up to 32 characters
password: up to 32 characters

```
{
     "apn": "apn",
     "userName": "user name",
     "password": "password"
}
```

4.2.5.6 SMS Settings

This is the chapter where the functions enabling that SMS data can be read and written are described.

•URL
/settings/sms
•Metod:
GET | PUT
•Data Parameters
status: true (turns on the SMS feature), false (turns off the SMS feature)
numberRestrictionMode: true (Turns on phone number restriction), false (Turns off phone number restriction)
allowedNumbers: ["","",""] (If the phone number restriction feature is on, these are the permitted numbers.)
serviceNumber: Service telephone number which depends on operator.
serviceType: Service type which depends on operator.

```
{
     "status": true,
     "numberRestrictionMode": false,
     "allowedNumbers": [
          "",
          "",
          ""
     ],
     "serviceNumber": "+905329010000",
     "serviceType": 145

}
```

4.2.5.7 Security Settings

This section describes the security-related functions.

•URL
/settings/security
•Method:
GET | PUT
•Data Parameters
password: up to 12 characters.

```
{
    "password": "password"
}
```

4.2.5.8 All Settings

In this section, it is explained all the data which can be read and written .

•URL
/settings
•Method:
GET | PUT
•Data Parameters
serial: Refer to 4.2.5.2
operation: Refer to 4.2.5.4
role: Refer to 4.2.5.3
apn: Refer to 4.2.5.5 (Can only be written via USB)
•sms: Refer to 4.2.5.6
security: Refer to 4.2.5.7

```
{
    "serial": {
        "baudrate": 38400,
        "parity": "none",
        "stopBits": 1
    },
    "operation": {
        "type": "serial-master",
        "reqTimeout": 60000,
        "resTimeout": 1000,
        "conversion": "mtcp-mrtu"
    },
```

```
    "role": {
        "type": "server",
        "gateway": {
            "port": 502,
            "allowedIps": [
                "0.0.0.0",
                "0.0.0.0",
                "0.0.0.0"
            ],
            "ipRestriction": false
        },
        "communication": {
            "port": 555,
            "allowedIps": [
                "0.0.0.0",
                "0.0.0.0",
                "0.0.0.0"
            ],
            "ipRestriction": false
        }
    },
    "apn": {
        "apn": "mgbs",
        "userName": "",
        "password": ""
    },
    "sms": {
        "status": true,
        "numberRestrictionMode": false,
        "allowedNumbers": [
            "",
            "",
            ""
        ],
        "serviceNumber": "+905329010000",
        "serviceType": 145
    },
    "security": {
        "password": "password"
    }
}
```

4.2.5.9 Product Information Functions

In this section, the functions to read the product information data are explained.

•URL
/info/product
•Method:
GET
•Data Parameters
companyName: Manufacturer name.
deviceName: Product name.
serialNumber: Product serial number.
orderNumber: Order number.

```
{
    "companyName": "Klemsan",
    "deviceName": "GTOR-4-3G ",
    "serialNumber": "00111111111",
    "orderNumber": "00000601445"

}
```

4.2.5.10 Production Information Functions

In this section, the production information datas are explained.

•URL
/info/production
•Metod:
GET
•Data Paremeters
firmwareVer: Firmware version
pcbVer: Hardware version
buildDate: Build date
buildTime: Buid time
compilerVer: Comlier version

```
{
    "firmwareVer": "1.00",
    "pcbVer": "1.00",
    "buildDate": "Mar 29 2018",
    "buildTime": "17:08:35",
    "compilerVer": 8011002

}
```

4.2.5.11 GSM Info Functions

This is the chapter where the functions enabling that GSM information data can be read are described.

•URL
/info/gsm

•Method:
GET

•Data parameters
imei: Up to 15 characters.
operator: Up to 15 characters.
ip: Up to 15 characters.

```
{
    "imei": "123456789",
    "operator": "abcd",
    "ip": "1.1.1.1"

}
```

4.2.5.12 Location Info Functions

This is the chapter where the functions enabling that location information data can be read are described. The device location is the position reported by the operator.

•URL
/info/location

•Method:
GET

•Data Parameters
latitude: Up to 11 characters.
longitude: Up to 11 characters.

```
{
    "latitude": "39.907246",
    "longitude": "32.750305"

}
```

4.2.5.13 All Device Info Functions

This is the chapter where the functions enabling that all of the information data can be read are described.

•URL
/info

•Method:
GET

•Data Parameters
product: Refer to 4.2.5.9
production: Refer to 4.2.5.10
gsm: Refer to 4.2.5.11
location: Refer to 4.2.5.12

```json
{
    "product": {
        "companyName": "Klemsan",
        "deviceName": "GTOR-4-3G ",
        "serialNumber": "00111111111",
        "orderNumber": "00000601445"
    },
    "production": {
        "firmwareVer": "1.00",
        "pcbVer": "1.00",
        "buildDate": "Apr 26 2018",
        "buildTime": "10:25:53",
        "compilerVer": 8011002
    },
    "gsm": {
        "imei": "123456789",
        "operator": "abcd",
        "ip": "1.1.1.1"
    },
    "location": {
        "latitude": "39.907246",
        "longitude": "32.750305"
    }

        }
```

4.2.5.14 Command Functions

This is the chapter where command functions are described.

•URL
/command
•Method:
POST
•Data Parameters
command: "save-config" (Allows the changed configuration to be saved to non-volatile memory)

```json
{
    "command": "save-config"
}
```

command: "restart" (The device is restarted)

```
{
    "command": "restart "
}
```

command: "return-config-to-default" (The device is reset)

```
{
    "command": "return-config-to-default "
}
```

4.2.5.15 General Logging Settings

This is the section that describes the functions allowing that log data is read, written and deleted. The logging functions have two different settings. The first one is the common settings for all the records and the second one is the settings for the queries.

4.2.5.15.1 Common Logging Settings

This is the section where functions allowing that common logging data are written are described.

•URL
/ settings/log
•Method:
POST
•Veri Parametreleri
ntpServerAddress: Up to 32 characters
ntpServerAddress: 1-65535
serialTimeout: 1000 - 4000
period:1-60

```
{
    "ntpServerAddress": "time.google.com",
    "ntpServerPort": 123,
    "serialTimeout": 1000,
    "period": 1
}
```

NOT: To be able to save the changes made in the non-volatile memory, a save command must be sent. Logging functions will be activated once the sent data has been saved.

Functions for deleting common logging data are as follows:

•URL
/ settings/log
•Method:
DELETE
•Data Parameters:
None

4.2.5.15.2 Logging Record Settings

This is the section where functions allowing that record settings are written are described.

•URL
/ settings/log/q[n] (n. query settings)

•Method:
POST

•Data Parameters
type: "mrtu", "mascii"

•slaveAddress: 1-254

•function: 1,2,3,4

•startingAddress: 0-65535

•numberOfPoints:1-125

```
{
    "type": "mascii",
    "slaveAddress": 5,
    "function": 2,
    "startingAddress": 10,
    "numberOfPoints": 100
}
```

NOT: To be able to save the changes made in the non-volatile memory, a save command must be sent. Logging functions will be activated once the sent data has been saved.

NOT: Once the sent data has been saved, the logging functions of the selected record will be inactive and all logging data of the selected record will be deleted.

•URL
/ settings/log/q[n] (n. query settings)

•Metod:
DELETE

•Data Parameters
None.

4.2.5.15.3 Logging Functions

This is the section where the functions enabling that logging date data is read are described.

•URL
/ log/dates/qn (n. query date)

•Method:
GET

•Data Parameters
dates: "yyyy-mm-dd"

```
{
    "dates": [
        "2018-04-19",
        "2018-04-26",
        "2018-04-27",
        "2018-04-30"
    ]
}
```

The functions of reading the statistics of logging data are as follows:

•URL
/log/q[n]/yyyy-mm-dd/stats (statistic record at yyyy-mm-dd of n. query.)

•Method:
GET

•Data Parameters
dates: "yyyy-mm-dd"

```
{
    "date": "2018-04-26",
    "recordCount": 320,
    "successCount": 320,
    "timeoutCount": 0,
    "checksumErrorCount": 0,
    "firstRecordTime": "08:45",
    "lastRecordTime": "15:11"
}
```

The functions of reading logging data are as follows:

•URL
/log/q[n]/[yyyy-mm-dd]/r[m] (n. interrogate air on yyyy-mm-dd m. record.)

•Metod:
GET

•Veri Parametreleri
recordNo: 1-1440
time: "hh:mm"
time: "success", "timeout", "checksum"
response: [...]

```
{
    "recordNo": 1,
    "time": "08:45",
    "state": "success",
    "response": [
        1,
        3,
        .
        .
        .
        0
    ]
}
```

The functions to delete all logging data are as follows:

•URL
/log

•Method:
DELETE

•Data Parameters
None

With this function it is allowed the logging data of the query to be deleted. All records, date information and statistics of the query are deleted.

•URL
/log/q[n] (n. query)

•Method:
DELETE

•Data Parameters
None

The following function ensures that all logging data on a specific date is deleted.

•URL
/log/q[n]/[yyyy-mm-dd] (data for yyyy-mm-dd of the n. query)

•Method:
DELETE

•Data Parameters
None

GTOR-4-3G

3G to Serial
Internet
Object

SECTION 5
TECHNICAL
SPECIFICATIONS

SECTION 5 TECHNICAL SPECIFICATIONS

Supply

Voltage ....11-30VDC from DC+ DC- terminals, or USB Port

Power Consumption........................ <1.2W

Working Temperature...................... -10…60 °C

Insulation... 1.5kV RMS

GSM Module Features

GPRS.. Max. 85.6Kbps (DL)/ Max. 85.6Kbps (UL)

EDGE.. Max.236.8Kbps (DL)/Max.236.8Kbps (UL)

GPRS/EDGE.. Multi-slot Class 12

Serial Communications

Device support for up to 64

Baudrate... 300 ... 115200

Stop Bit... 1,2

Parity... None, Even, Odd

Data... 8 Bit

Configuration

USB

SMS

JSON RestAPI

Suppoted Protocols

MODBUS TCP

MODBUS RTU over TCP
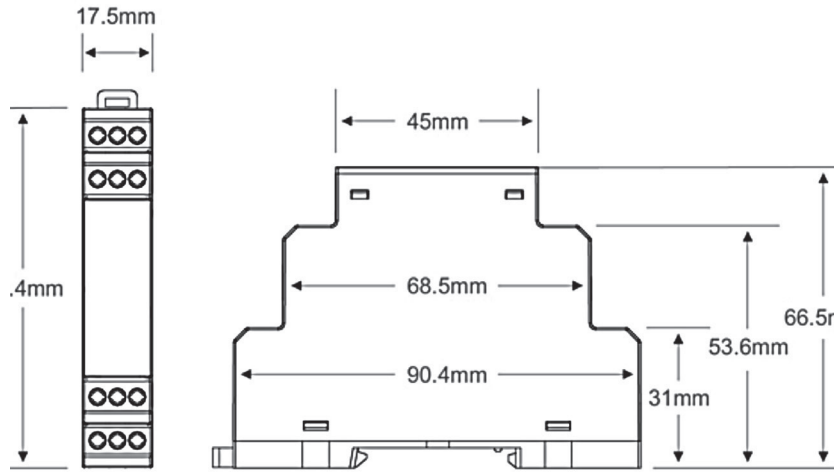
MODBUS ACII over TCP

Suppoted Roles

Server Role

Client Role

Operation Types

Serial Master

Transparent

Logging

7-days records (1 ... 60min),

Totally 100,800 records (1 minute resolution)

Şekil 5-1 Dimensions

Klemsan®