



VAJRAVEGHA MOBILITY PVT. LTD.

VVM 401 4G IoT GATEWAY

USER MANUAL

Version 1.1

15th September 2023

Table of Contents

Introduction and Key Features	3
Supported Protocols	4
Gateway Ports and Connectors	5
Basic Connection and Setup	7
Configuration and Settings via web portal	9
Home Page	10
Network Settings	12
MQTT Settings	15
RS-485 and RS-232 Settings	17
Modbus Settings	18
MQTT JSON Format	20
SD Card	21
RTC Calibration	22
General Settings	23
Additional Information, Customisation and Contact Details	24

Introduction

Dear user, thank you for your purchase. Now experience seamless connectivity and advanced control with the VVM401 4G IoT Gateway. Whether you need secure data transmission, real-time monitoring, or efficient control, the VVM401 has you covered. Its versatile features make it a powerful solution for a wide range of applications.



Key Features

- **Secure IoT Cloud Connectivity:** Connect seamlessly to IoT cloud platforms via 4G LTE, Ethernet, or Wi-Fi, ensuring your data is transmitted securely.
- **Compatibility with All Indian Telecom Operators:** The VVM401 is compatible with frequency bands of all Indian telecom operators, ensuring reliable network connectivity.
- **Modbus RTU Master over Isolated RS485:** Easily integrate with various industrial devices using Modbus RTU master over isolated RS485.
- **Modbus TCP/IP Client over Ethernet:** Efficiently communicate with other devices and systems using Modbus TCP/IP client over Ethernet.
- **Secure MQTT Connectivity:** Ensure data security with secure MQTT connectivity, a robust protocol for IoT communication.
- **Convenient Web Portal Configuration:** Effortlessly configure your gateway through a user-friendly web portal over Wi-Fi, simplifying setup and management.
- **Data Telemetry in Standard JSON Format:** Receive data in a standardized JSON format with timestamps, making it easy to process and analyze.
- **Micro SD Card for Local Data Backup:** Store critical data locally with the Micro SD card support, ensuring data redundancy and reliability.
- **SMS alerts:** Receive SMS alerts at prescribed time intervals to stay informed about important events or conditions.
- **Firmware Over-The-Air (OTA) Updates:** Keep your gateway up to date with OTA updates via Wi-Fi, eliminating the need for manual firmware updates.
- **Versatile Data Acquisition:** Benefit from 4 digital isolated inputs for versatile data acquisition, suitable for various sensing and monitoring applications.
- **Compact DIN Mount Enclosure:** The VVM401 comes in a compact DIN mount enclosure with dimensions of 135x110x55mm, making it easy to install in various environments.

Supported Protocols

Modbus RTU:

Modbus RTU is a protocol designed for serial communication between master and slave devices. It employs a compact binary format for data exchange between devices. To ensure data reliability, Modbus RTU appends a cyclic redundancy check (CRC) checksum to commands/data.

Modbus TCP/IP:

Modbus TCP/IP is a Client Server protocol used for network communication over TCP/IP networks, typically connecting via port 502. Unlike Modbus RTU, it doesn't require calculating a checksum because lower network layers already provide checksum protection.

MQTT / MQTTS (Message Queuing Telemetry Transport):

MQTT is a lightweight publish/subscribe messaging protocol used for machine-to-machine (M2M) and Internet of Things (IoT) applications. It's ideal for remote connections with a focus on minimal code footprint and efficient use of network bandwidth.

HTTP/HTTPS (Hyper Text Transfer Protocol):

HTTP is the foundational protocol of the World Wide Web. It defines how messages are structured and transmitted. It also specifies the actions that web servers and browsers should take in response to various commands, facilitating data exchange on the internet.

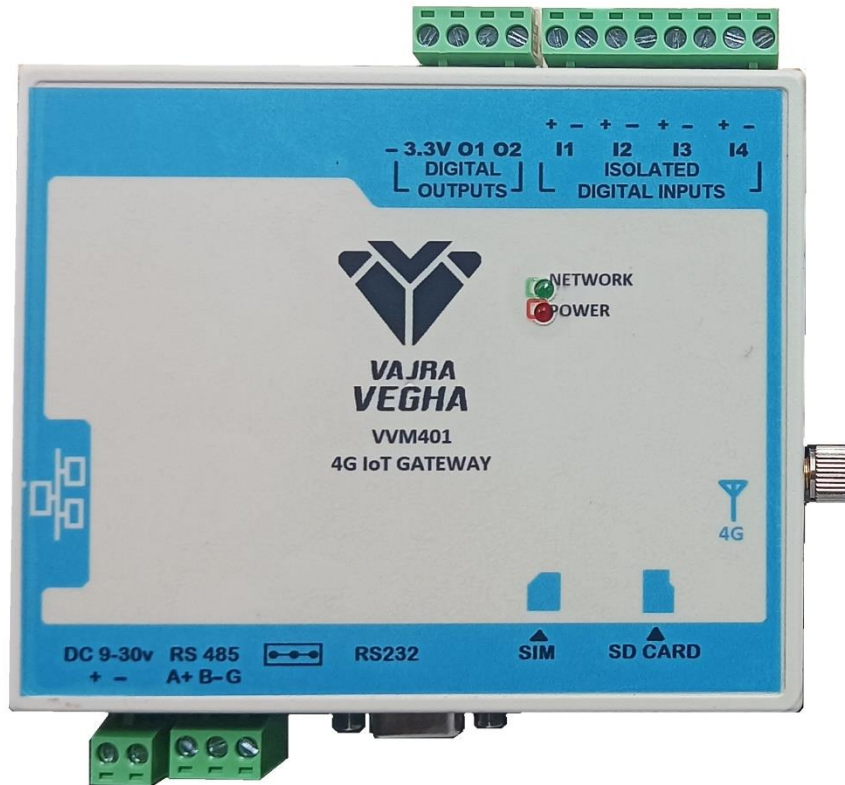
DHCP (Dynamic Host Configuration Protocol):

DHCP is employed on TCP/IP networks to automate the assignment of IP addresses and network configuration parameters to connected devices. A DHCP server dynamically allocates IP addresses, simplifying network management.

ICMP (Internet Control Message Protocol):

ICMP, commonly associated with the "Ping" utility, is a network administration protocol used to test the reachability of hosts on an Internet Protocol (IP) network. ICMP can also be utilized for secure network troubleshooting and diagnostics.

VVM 401 4G IoT Gateway Ports and Connectors



Gateway Ports and Connectors

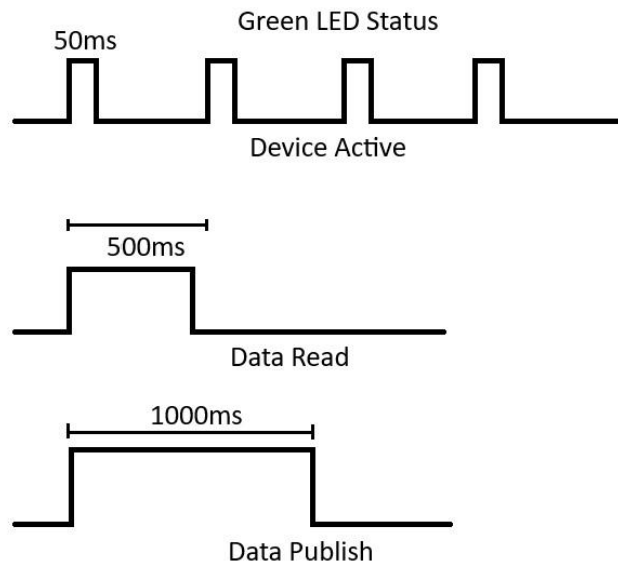
On-board Ports and Connectors:

1. Power Input Connector: DC 9v to 30v SMPS Power Supply Input
2. RS-485 Port: 1.5kV Isolated RS-485 Input Port for Modbus RTU or transparent mode or any other proprietary protocol
3. Rs-232 Port: Isolated Rs-232 Port for transparent mode or any other proprietary protocol.
Note: Either RS-485 or RS-232 will work at a time depending on the jumper selection between both the ports. When jumper is to the left, RS-485 is active and when jumper is to the right, RS-232 is active
4. SIM Slot: Nano SIM card slot. Spring type push to insert type connector
5. SD Card Slot: Micro SD Card slot for data logging. Maximum 16GB Support. SD Card is optional
6. 4G Antenna Connector: Connect the LTE Antenna provided here.
Note: It is recommended to connect the antenna before power on to avoid damage to the LTE chipset
7. Ethernet Port: Connect an RJ-45 Cable to the network switch / router. This port can be used either in Modbus TCP / IP Mode or Internet gateway mode. When the network gateway is selected to Ethernet instead of 4G or Wi-Fi, the Modbus TCP/IP mode cannot be used.

8. Digital Inputs: 4 different isolated 5v Digital Inputs can be applied at I1, I2, I3 and I4. Ensure correct polarity!
9. The default gateway has two non-isolated 3.3v compatible output pins. Contact us for client specific configuration of these pins.

LED Status:

1. Red LED is for Power
2. Green LED is for Device Monitoring and Network Status. Constant blinking (50msec pulse every second) indicates that the device is functioning properly. A half second LED blink pulse indicates that the device is reading data from the connected devices and a one second blink pulse indicates that the device is publishing data to the cloud.



Gateway Connection and Setup



Please read carefully below instructions on how to make the necessary connections for the VVM401 device based on the wiring diagram. Please note that these steps should be performed externally according to the indications provided in the diagram:

Nano SIM Card:

Carefully insert the Nano SIM card into its designated slot, aligning it as per the enclosure orientation diagram.

SD Card:

Insert a micro SD card into the designated slot on the VVM401 device, following the orientation shown in the enclosure diagram. This is for device data logging and is optional.

4G Antenna:

Attach the 4G antenna to the corresponding port on the VVM401 device as illustrated in the wiring diagram. Connect the antenna before turning the device ON.

RS485 / RS232:

Modes Supported are Modbus RTU over RS485 or Transparent RS485 / RS232. Select jumpers for either RS485 or RS232

Ethernet Cable:

Connect one end of an Ethernet cable to the RJ45 port on the VVM401 device as shown in the diagram. Connect the other end to Network Switch / Router / PLC / Modbus Server. Ethernet port can be configured either as gateway mode or Modbus TCP/IP Mode.

Power Adapter (9-30V VDC):

Connect the SMPS Power Supply with proper polarity to the VVM401 device. Ensure that the voltage supply matches the specified range of 9-30V DC as indicated in the diagram. **DO NOT TURN ON THE SMPS YET!**

Steps before powering on the gateway

The gateway provides a web portal for configuration which can be accessed through local Wi-Fi. Before powering the gateway please follow these steps:

Configure a WiFi Router or a Mobile Access Point (Hotspot) with **SSID "iotgateway"** and the **Password "iot@1234"** These are the default credentials which can later be changed. Ensure both the gateway and the router / hotspot is within local Wi-Fi range.

Powering the Gateway: Connect the DC power supply to the gateway and switch it on. You will see the power LED indicator turn ON.

Using the Web Portal for VVM401 Configuration

Option A: Connecting to the Access Point

Once the access point is configured and gateway is powered on, the device will search for the access point and connect to it.

Once the gateway is connected to the hotspot, find the device's IP address from your router or hotspot settings. Connect a laptop or mobile to the same network, open the browser and enter the IP address that was allocated to the gateway.

If you are using a Windows / Linux operating system on the laptop, you can enter "vvm401_product_id_number.local" in the web browser's address bar. Replace "product_id_number" with your specific product ID number (e.g., http://vvm_1234.local , where VVM_1234 is the product ID). This feature is not available for Android mobiles, so mobiles must enter the actual IP address instead of the Domain Name address.

Option B: Using the VVM401 Hotspot

The second method involves using the VVM401 gateway hotspot. This method is to be used only when a router or a mobile hotspot is unavailable for the gateway to connect to. In this scenario the gateway creates its own WiFi access point (hotspot) to which a Mobile or Laptop can connect via Wi-Fi for configuration.

Note: This is not an Internet hotspot and is only used for gateway configuration .

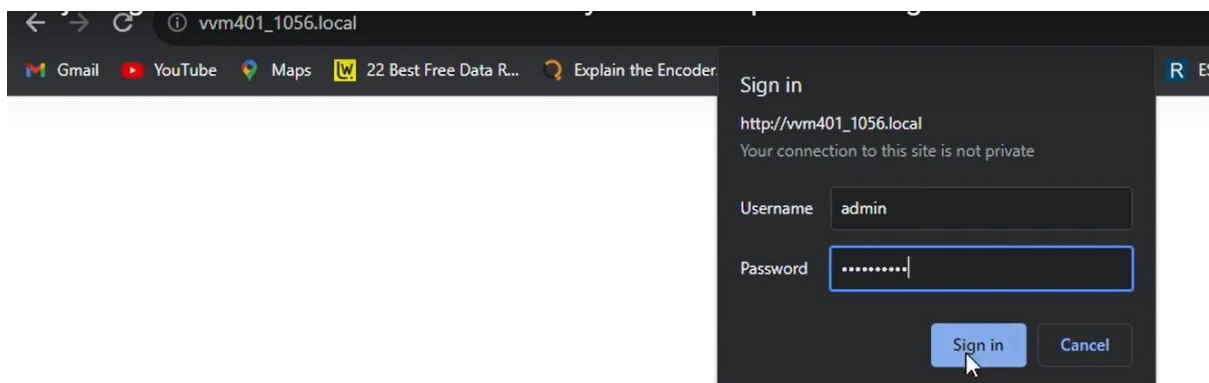
Using a laptop or a mobile, search for a Wi-Fi network with the SSID "VVM401_product_id_number" (e.g., "VVM401_1234"). The password is provided separately to the client.

Connect to this network.

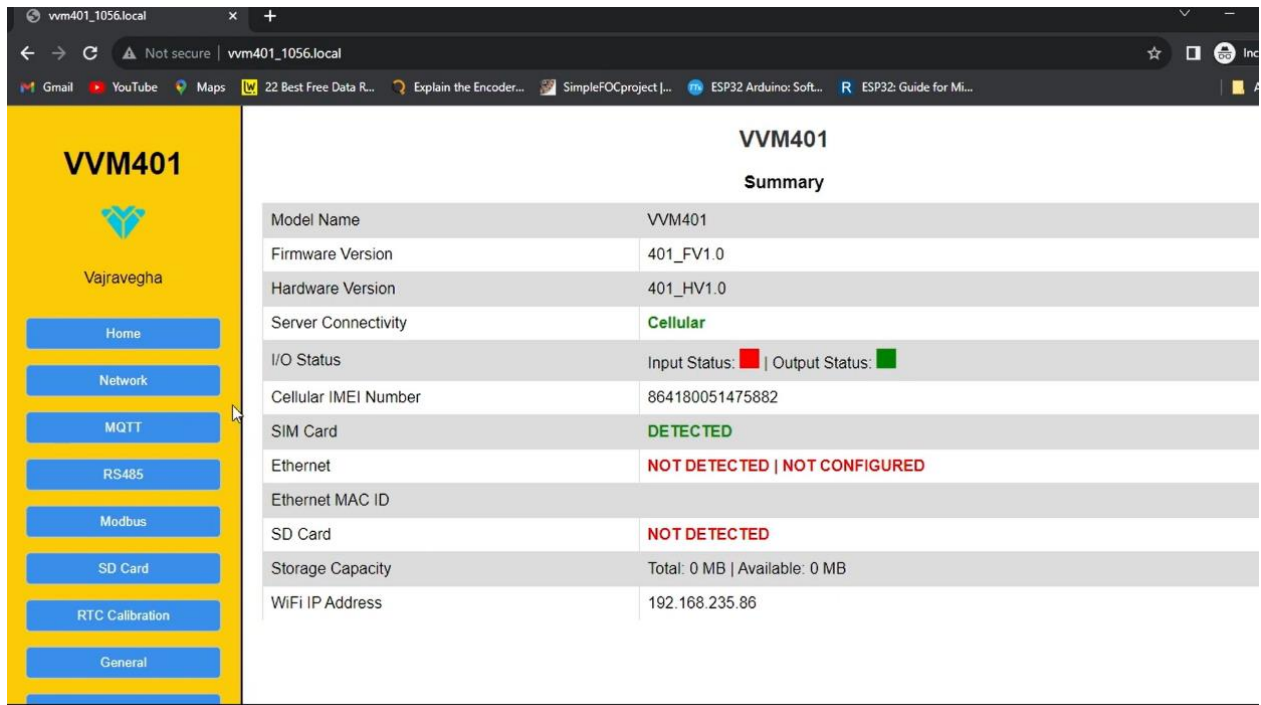
Open a web browser and enter "**192.168.4.1**" in the address bar

Login Window:

A login window will appear; enter the default SSID "**admin**" and password "**admin@1234**"



Home Page



VVM401	
Summary	
Model Name	VVM401
Firmware Version	401_FV1.0
Hardware Version	401_HV1.0
Server Connectivity	Cellular
I/O Status	Input Status: ■ Output Status: ■
Cellular IMEI Number	864180051475882
SIM Card	DETECTED
Ethernet	NOT DETECTED NOT CONFIGURED
Ethernet MAC ID	
SD Card	NOT DETECTED
Storage Capacity	Total: 0 MB Available: 0 MB
WiFi IP Address	192.168.235.86

If the username and password are correct, you will gain access to the web portal.

The home page will display a summary of the device's general information, providing you with an overview of its configuration.

Model Name: Displays the model name as VVM401

Firmware Version: Displays the current firmware version

Hardware Version: Displays the current hardware version

Server Connectivity: Displays one of the following options: Cellular, Ethernet, or Wi-Fi based on the current Gateway connectivity status

Note: The Home Page refreshes automatically every 10 seconds.

I/O Status:

Input Status: Indicator is green if input is detected from RS485/RS232 for more than one minute; otherwise, its red

Output Status: Indicator is green if output data is published to MQTT for more than one minute; otherwise, its red

Cellular IMEI Number: Displays the IMEI number of the SIM card

Sim Card Status: Displays in green colour if a SIM card is detected; otherwise in red

Ethernet Status: Displays "Detected" in green if Ethernet is detected; otherwise in red. (If Ethernet is detected, specify whether it is configured as TCP/IP or for internet)

Ethernet MAC ID: Displays the Ethernet MAC ID if Ethernet is detected; otherwise blank

SD Card Status: Displays in green if the storage device (Micro SD card) is detected; otherwise in red. SD Card is optional and is only for data logging.

Storage Capacity: Displays the total backup memory and available memory of the SD Card

Wi-Fi IP Address: If the device is connected to the internet via Wi-Fi, the IP address allotted to the gateway is displayed.

Network Settings

Select Gateway:

Network Settings

Select Gateway: (Current Value Cellular)

Cellular

Submit

(If Ethernet gateway is selected, Modbus TCP/IP will be disabled)

SMS Settings

Field	Current Value	Change Value
Enter Receiver Phone Number for SMS Alerts (ex: +91xxxxxxxxx):		<input type="text"/> Submit
Enter SMS Duration in Hours:		<input type="text"/> Submit

In the "Select Gateway" section, you can choose how data will be transferred to the MQTT server. There are three options in the drop-down menu: **Cellular, Ethernet, or Wi-Fi.**

The default value is "Cellular," meaning data will be transferred to MQTT via 4G LTE.

If "Ethernet," is selected, the Internet source will be through the Ethernet connection. Note that if Ethernet gateway is selected, Modbus TCP will be disabled.

If "Wi-Fi" is selected, the Internet source will be the WiF router / Access Point to which the gateway is connected to

After selecting the gateway, click "Submit" to apply the changes.

SMS Settings:

In the "SMS Settings" section, you can configure SMS alerts.

Enter the phone number for SMS alerts, ensuring you add the country code before the 10-digit number (e.g., +91xxxxxxxxx). You can also specify the SMS alert duration in hours, with the default value set to one hour. When this duration is reached, the JSON message transmitted to the MQTT server will also be sent as an SMS notification.

Wi-Fi Credentials:

Field	Current Value	Change Value
GatewaySSID	iotgateway	<input type="text" value="iotgateway"/> <input type="button" value="Submit"/>
GatewayPwd	iot@1234	<input type="text" value="iot@1234"/> <input type="button" value="Submit"/>

Ethernet Type: (Current Value DHCP)

The "Wi-Fi Credentials" section allows you to set your Wi-Fi network information.

You can enter your new SSID (Wi-Fi network name) and password.

The default values are "iotgateway" for SSID and "iot@1234" for the password.

Ensure the SSID and password are correctly entered, as incorrect values can result in connectivity issues or difficulty accessing the web configuration page.

IMPORTANT: Ensure that the special character apostrophe (') is not present in the credentials or other fields else the Web page may not be displayed correctly.

Ethernet Settings:

In the "Ethernet Settings" section, you can configure Ethernet connectivity.

You can select the Ethernet type as either "DHCP" or "Static IP." The default value is "DHCP," which means the device will automatically obtain an IP address from the network.

If "Static IP" is selected, additional fields will appear, allowing you to specify the IPv4 address, subnet mask, default gateway, and DNS server manually.

Default values for these settings are typically as follows: IPv4 address (192.168.0.10), subnet mask (255.255.255.0), default gateway (192.168.0.1), and DNS server (192.168.0.1).

It's important to note that changes made in this section will be reflected after restarting the module.

Field	Current Value	Change Value
IPv4 Address	192.168.0.10	<input type="text"/> <input type="button" value="Submit"/>
Subnet Mask	255.255.255.0	<input type="text"/> <input type="button" value="Submit"/>
Default Gateway	192.168.0.1	<input type="text"/> <input type="button" value="Submit"/>
DNS Server	192.168.0.1	<input type="text"/> <input type="button" value="Submit"/>

Note: Whenever changes are made, consider restarting the module using the "Restart" button in the "General" tab to ensure the new settings take effect.

MQTT Settings

MQTT Settings

Vajravegha Server Clients Server Current Value **clientServer**

MQTT Server	broker.hivemq.com	<input type="text"/>	<input type="button" value="Submit"/>
MQTTPort ((1883: MQTT , 8883: MQTTS. Upload CA Certificate for 8883. NOTE: Currently, Ethernet Gateway supports only plain MQTT port 1883))	1883	<input type="text"/>	<input type="button" value="Submit"/>
Topic Name	VVM401Data	<input type="text"/>	<input type="button" value="Submit"/>
User Name		<input type="text"/>	<input type="button" value="Submit"/>

In the "**MQTT Settings**" section, you can configure MQTT connectivity based on your requirements. You have two options: "**Vajravegha Server**" or "**Client Server**." The default value is "Client Server."

Client Server: If you choose "Client Server," you can enter the following fields:

MQTT Server: Specify the MQTT server's broker name either in Domain Name or IP Address format

MQTT Port: Set the MQTT port number. Default is 1883 for plain MQTT and 8883 for MQTT over SSL

Note: Currently Ethernet Gateway only supports plain MQTT not MQTTS

Username and Password (if any): Enter the MQTT server username and password if present.

Password		<input type="text"/>	<input type="button" value="Submit"/>
MQTT Publish Time Interval in Minutes (1 minute min)	1	<input type="text"/>	<input type="button" value="Submit"/>

CA Certificate Upload

<input type="button" value="Choose File"/> No file chosen	<input type="button" value="File upload!"/>
---	---

Topic Name: Topic name of the data to be published

MQTT Publish Time Interval (in minutes): Define the time interval at which MQTT data will be published. The default value is 1 minute.

Default MQTT values:

MQTT server is a public broker: "broker.hivemq.com."

MQTT port: 1883.

Topic Name: VVM401Data

Publish time interval: 1 minute.

Clients can enter their own broker details here instead of the default values.

For secured MQTT data transfer, you can:

Type the broker address.

Enter "8883" in the MQTT port field.

Provide a username and password, if required.

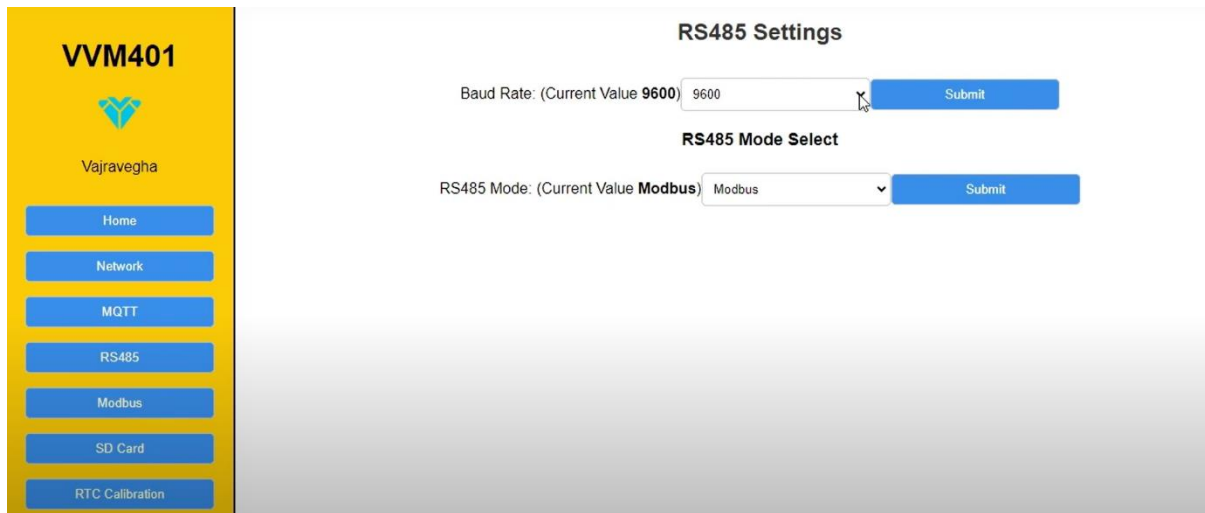
If you are using MQTT over a secure connection (MQTTS), you need to upload your CA certificate. Click on "Choose File," select the CA certificate file, and upload it. CA certificates are used by the device to verify the authenticity of the server before publishing the data. CA certificates are compulsory if you wish to publish data to SaaS providers such as AWS-IoT, Azure, etc.

Vajravegha Server:

If you plan to use "Vajravegha Server," please contact us for the configuration. We can provide secure MQTT data transmission and Dashboard visualization based on your specific needs. This option will be customized according to your requirement.

RS485 / RS232 Settings

In the "RS485 Settings" section, you have two drop-down sections for configuring the RS485 communication parameters:



The screenshot displays the VVM401 web interface. On the left is a yellow sidebar with the Vajravegha logo and a list of navigation buttons: Home, Network, MQTT, RS485, Modbus, SD Card, and RTC Calibration. The main content area is titled 'RS485 Settings' and contains two configuration sections. The first section, 'RS485 Settings', features a text input field for 'Baud Rate' with the current value '9600' and a blue 'Submit' button. The second section, 'RS485 Mode Select', features a dropdown menu for 'RS485 Mode' with the current value 'Modbus' and a blue 'Submit' button.

1. Baud Rate Selection:

This drop-down allows you to choose the desired baud rate for RS485 communication. Baud rate determines the speed at which data is transmitted over the RS485 interface.

The available baud rates are: 9600 (Default), 19200, 38400, 57600, 115200

Use lower baud rates for noisy communication lines.

2. RS485 Mode Selection:

Modbus Mode (Default): This mode is suitable for applications where the RS485 communication follows the Modbus protocol. It allows for structured communication with Modbus-compatible devices.

Transparent Serial Mode: In this mode, the RS485 or RS232 communication is transparent, meaning data is sent and received as-is, without specific protocol interpretation by the gateway.

The default mode is "Modbus Mode," which is commonly used for industrial applications requiring structured communication with Modbus devices. However, if you need a more generic serial communication without protocol interpretation, you can select "Transparent Serial Mode."

Note: Select either RS485 or RS232 by the jumper setting in between

Modbus Settings

Modbus RTU Configuration:

Modbus Settings

Modbus RTU Modbus TCP Select Modbus Type Current Value **TCP** (If Ethernet gateway is selected, Modbus TCP/IP will be disabled)

Initial Register	0	<input type="text"/>	<input type="button" value="Submit"/>
Number of Registers to be Read (50 Registers Max)	10	<input type="text"/>	<input type="button" value="Submit"/>
From Slave ID	1	<input type="text"/>	<input type="button" value="Submit"/>
To Slave ID (10 Slaves Max)	2	<input type="text"/>	<input type="button" value="Submit"/>

Modbus Mode: Modbus RTU or Modbus TCP/IP. Default value: Modbus RTU

Initial Register: This field allows you to set the starting register address from which data will be read using the Modbus RTU protocol. The default value is 1.

Number of Registers to be Read: Specify the number of registers you want to read in a single Modbus request. The default value is 4, but you can change it according to your data retrieval requirements. Maximum 50 16-bit registers can be read at a time.

From Slave ID and To Slave ID: Modbus RTU typically involves communication with multiple devices or slaves. The "From Slave ID" and "To Slave ID" fields help you define the range of slave IDs with which you want to communicate. The default "From Slave ID" and "To Slave ID" is 1. Maximum 10 slaves can be read from at a time.

Function Code (1:Coils, 2:Di Inputs, 3:Holding Reg., 4:Input Reg.)	1	<input type="text"/>	<input type="button" value="Submit"/>
--	---	----------------------	---------------------------------------

Select Data Format

Data Format: (Current Value **16bit**)

16bit

Transfer Format (For 32-bit Float only)

Transfer Format: (Current Value **Low Word First**)

High Word First

Function Codes: Modbus RTU uses function codes to specify the type of request being made (e.g., read, write, etc.). The default function code is 3, which corresponds to reading multiple holding registers. 1: Coils, 2: Discrete Inputs, 3: Holding Registers, 4: Input Registers

Data Format: You can choose between 16-bit register format and 32-bit data format based on the Modbus device's data format. Though default Modbus register size is 16 bits, pair of registers can be combined together for a single 32-bit IEEE float format. The default is 32-bit.

Transfer Format: This setting determines whether the high word or low word is transmitted first in 32 bit data format. The default is "High Word First." Check your slave device format settings. This field is not valid for 16 bit data format setting.

Modbus RTU Limits: Keep in mind that in Modbus RTU mode, you can connect a maximum of 10 slaves, and for each slave, you can read a maximum of 50 registers.

Modbus TCP Configuration: This configuration is used to read data from Modbus TCP/IP Servers / Slaves.

Following parameters will be same for Modbus RTU as well as Modbus TCP/IP and functioning will be as described in the Modbus RTU Section above:

Initial Register, Number of Registers, Function Code, Data Format and Transfer Format

Number of Servers (min. 1 & max. 5):		
<input type="text" value="1"/>		
<input type="button" value="Submit"/>		
(Current Value 1)		
IP Address 1	192.168.0.5	<input type="text"/> <input type="button" value="Submit"/>
IP Address 2		<input type="text"/> <input type="button" value="Submit"/>
IP Address 3		<input type="text"/> <input type="button" value="Submit"/>
IP Address 4		<input type="text"/> <input type="button" value="Submit"/>

Server IP addresses are present instead of Slave Addresses in Modbus TCP/IP

Number of Servers to be Read: This dropdown allows you to specify the number of Modbus TCP servers you want to communicate with, with a maximum of 5 servers. You can enter the IP addresses of these servers.

Note: If Ethernet is selected as the gateway, then Modbus TCP/IP will be disabled

MQTT JSON Format

The data received from Modbus devices are parsed into standard JSON message before publishing to the broker. The topic name can be set in the MQTT Section Tab.

JSON Text Format:

```
{"DevID":"VVM401_1056","TS":1696403795,"S1_0":10,"S1_1":20,"S1_2":30,"S1_3":40,"DI1":1,"DI2":1,"DI3":1,"DI4":1}
```

where

DevID indicates Unique Device ID of the gateway

TS indicates Unix Timestamp

S1_0 indicates Slave 1 Register 1 and 10 is the value read from the slave

S1_1 indicates Slave 1 Register 2 and 20 is the value read from the slave

S1_2 indicates Slave 1 Register 3 and 30 is the value read from the slave

S1_3 indicates Slave 1 Register 4 and 40 is the value read from the slave

S2_0 indicates Slave 2 Register 1

S2_1 indicates Slave 2 Register 2

S2_2 indicates Slave 2 Register 3

etc.

The register type whether holding, input, coils etc needs to be set in the Modbus Section Tab

DI1 indicates Digital Input 1 Data

DI2 indicates Digital Input 2 Data

DI3 indicates Digital Input 3 Data

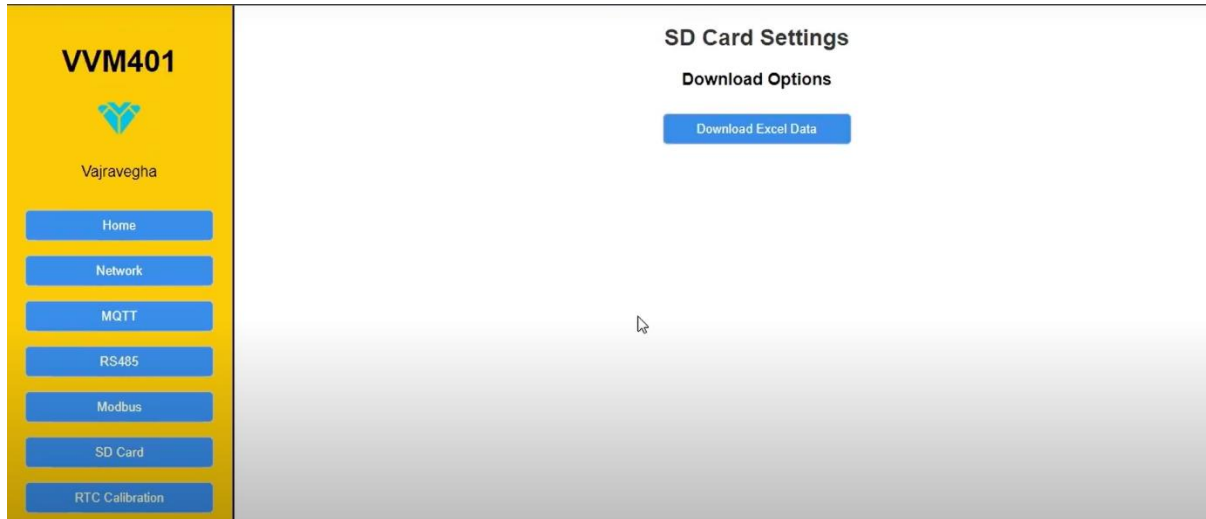
DI4 indicates Digital Input 4 Data

All Digital Inputs are active low, so when no signal is present on the DI, 1 is transmitted and when 5v is present 0 is transmitted

SD Card

In the "SD Card" section, you can manage, and access data stored on the SD card within the VVM401 device.

Download Option for Excel CSV Data:



The "Download" option allows you to retrieve data that has been saved to the SD card in CSV format. This is a valuable feature for data retrieval and analysis.

Data Saving to SD Card: Before data is published to the MQTT server, it is saved to the SD card. The frequency of data saving to the SD card is determined by the MQTT Publish Time Interval, which you can configure in the "MQTT Settings" section. For example, if you set the MQTT Publish Time Interval to 5 minutes, the data will be saved to the SD card every 5 minutes.

CSV Data: The downloaded data will be in CSV format, which is widely used for data analysis and reporting.

On the home page summary, you can readily check the status of the SD card. If the SD card is detected and functioning correctly, it will show 'DETECTED' in green colour.

RTC Calibration

RTC Calibration

If variation in time observed, click on the RTC Calibration button below.

RTC CURRENT TIMESTAMP

2023-10-04 13:31:25

Calibrate RTC

In the "RTC Calibration" section, you can manage and calibrate the Real-Time Clock (RTC) of the VVM401 device. The RTC is crucial for accurate timestamping of events and data.

Current RTC Timestamp:

This section displays the current RTC time stamp, which represents the device's current date and time. It's important to have an accurate RTC time for various applications that rely on precise timing and scheduling.

Calibrate Button:

If you observe any variation or discrepancy in the RTC time compared to the actual time, you can use the "Calibrate" button to correct it.

Calibration Options:

When you click on the "Calibrate" button, it will open a dialog box that allows you to select the correct date, time, and UTC time zone. Here's how you can configure it:

Correct Date and Time: Select the current date and time, which should be accurate according to your reference source (e.g., an atomic clock or other reliable timekeeping method).

UTC Time Zone: For India, the UTC time zone is typically +5.30. This value represents the offset from Coordinated Universal Time (UTC) to the local time zone.

Submitting Calibration:

After selecting the correct date, time, and UTC time zone, click the "Submit" button. The VVM401 device will then use these values to calibrate its RTC.

Alert Message:

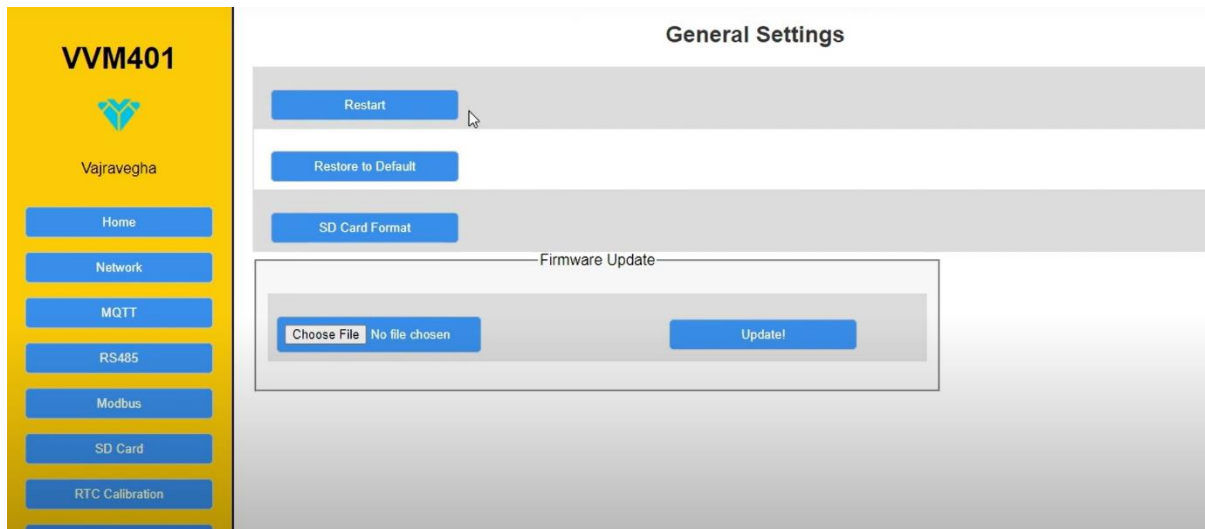
Upon successful RTC calibration, you will receive an alert message confirming that the RTC has been configured properly. This message indicates that the device's internal clock is now synchronized with the accurate time and date.

Importance of RTC Calibration:

RTC calibration is essential for ensuring that events and data recorded by the VVM401 device are accurately timestamped. In applications where precise timing is critical, such as data logging or event scheduling, having an accurate RTC is crucial for reliable operation.

General Settings

In the "General Settings" section, you can access essential options for managing and configuring the VVM401 device. This section provides control over critical device functions.



1. Restart Button:

The "Restart" button is used to restart the VVM401 module. Clicking this button initiates a device reboot. You will receive an alert message on the webpage confirming whether the module has been successfully restarted. It's essential to note that after making any changes to the configuration settings on the webpage, you should restart the module to apply those changes.

2. Restore to Default Button:

The "Restore to Default" button allows you to reset all configuration settings to their default values. Each section within the device has default values, and this button helps you revert the device to its factory settings. All default values are specified in the corresponding sections mentioned earlier in the datasheet. This option is useful if you need to start fresh or undo any customizations. This feature is protected with a unique password provided to the client. You must enter the correct password to initiate a Restore to Default".

3. SD Card Format Button:

The "SD Card Format" button is used to format the SD card. Formatting the SD card will result in the deletion of all data stored on it. It's important to exercise caution when using this option, as it is irreversible. If you need to clear the SD card and remove all data, this is the function to use. This feature is protected with a unique password provided to the client. You must enter the correct password to initiate a SD Card Format.

4. Firmware Update Button:

The "Firmware Update" feature is used to upgrade the firmware of the VVM401 device. Firmware updates are crucial for improving device functionality, security, and compatibility.

Password Protection: This feature is protected with a unique password provided to the client. You must enter the correct password to initiate a firmware update.

Important Note: During a firmware update, it's important not to refresh the webpage or navigate to another page until the update is completed. Once the firmware is updated to the new version, you should refresh the page to verify the device's firmware details.

Sign-Out

Click on this tab to safely sign out from the web page

Additional Customisation

We can provide additional customisation such as additional Analog and Digital Outputs, LoRa node connectivity, IoT Cloud Dashboard. Contact us in case of any business or technical enquiry.

Contact Us:

Vajravegha Mobility Pvt Ltd, Mumbai

info@vv-mobility.com

www.vv-mobility.com

Ph: +91-8850627350, +91-9511233885