Vehicle Telematics 200 Series User Manual

VT200 Series

Version: 1.0

Revision History

Version	Data	Author	Description
1.0	2023-1-10	Sun Zhandong	Creation of the document

Chapter I Product Introduction and Preparation

1. Introduction

1.1 Overview

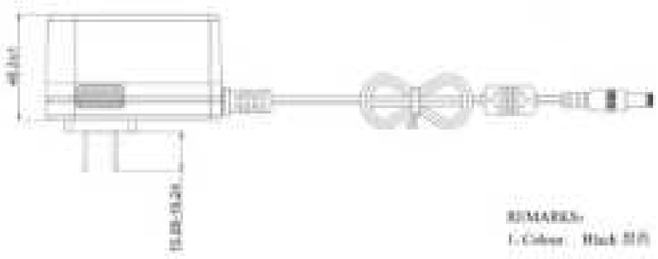
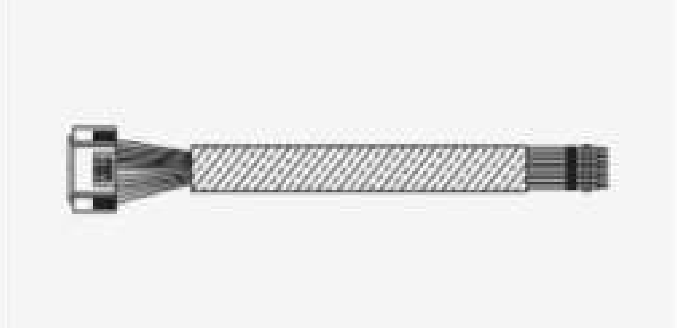
The VT200 series vehicle tracking gateway is an asset tracking product that features cost-effectiveness, rich interfaces and strong performance. It is suitable for industries such as logistics and transportation, engineering vehicle monitoring and so on. It offers precise positioning with GNSS, tracking and monitoring the status, history track, geofencing, abnormity alarm and other functions of vehicles and drivers, combined with the vehicle network cloud platform, can realize remote vehicle management, asset tracking, preventive maintenance, helping fleet operators save costs and improve efficiency. The device provides sub-models that support wireless network access of various speeds such as LTE CatM1, Cat1, Cat4, etc.

2. Start to use VT200

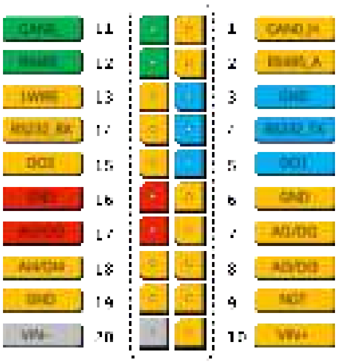
2.1 Check necessary accessories

Different accessories need to be ordered when purchasing the product. You can also purchase it yourself.

In order to help customers test and log in the equipment in the office, InHand provides test kits: 9-36V adapter or AC to DC 9~36V power supply, RS232 to USB as shown in the table below.

Product Name	MLFB	
DC 5.5*2.1mm Female Connector	ECON000047	
Power adapter 12V/2A	APWR000122/121	
20PIN All-in-one Test Cable	SCAB000381	

2.2 About VT200 interface



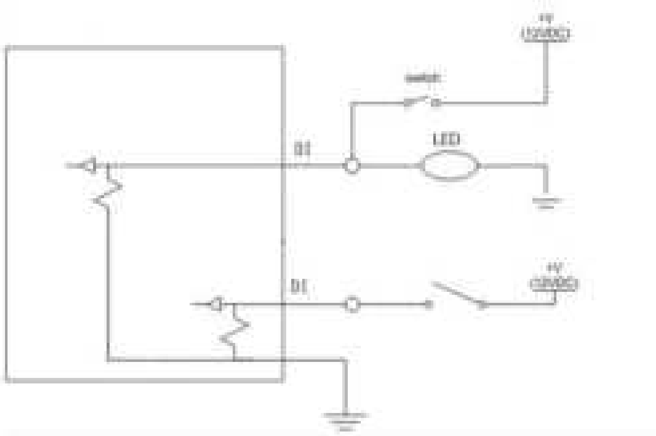
2.2.1 RS232 Serial Port

VT200， RS232 serial port is used for data transfer only, not for configuring the device. Configuration device requires USB-Type C. Connect the RS232_RX, RS232_TX, and GND of the VT310 to TXD, RXD, and GND of the DB-9 serial port welding-free interface . Use RS232 to USB cable to connect with DB-9 serial port surface welding port.

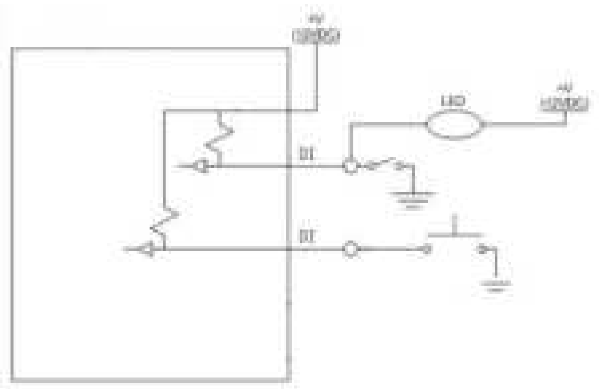
2.2.2 Digital Input (DI)

The DI can detect the switching value, such as whether the button is pressed or bounced, and whether the switch is on or off. The VT200 provides configurable pull-up. The DI has a default 10kΩ resistor pulled down to GND. When the DI is configured to pull up, there is a 20kΩ resistor pull up to the power supply voltage. When using DI, it is necessary to distinguish between pull-up and no pull-up.

When the DI has no pull-up power supply, the external circuit is connected as follows:

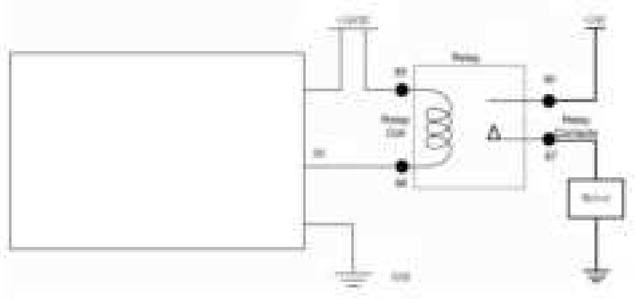


When the DI has a pull-up power supply, the external circuit is connected as follows:



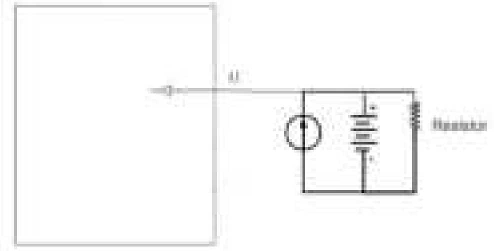
2.2.3 Digital Output (DO)

The DO can output DC voltage. The DO is an open-leakage output that supports a current of 300mA and usually works with relays.



2.2.4 Analog Input (AI)

The AI can detect DC voltage, and customers can directly access the analog quantity of voltage. External circuit is connected as follows:



2.2.5 1-Wire

The 1-Wire is usually used for small communication equipment, such as digital thermometers and iButton devices. Before use, the customer needs to connect the DQ pin (signal line) of the 1-Wire device to the VT200 PIN8, and connect the VDD and GND pins of the 1-Wire device to the GND of the VT310. The sensor is the less02b type. The following picture shows the water temperature detection wires of the 32 digital temperature sensor probe.

2.2.6 Ignition Sense

IGT(Ignition sense): IGT is used to connect to the Ignition switch of the vehicle. The VT310 can detect whether the connected vehicle is ignited. When using the 20PIN cable for testing, connect the IGT cable and V+ cables to DC power supply.

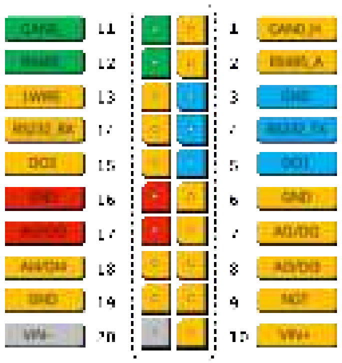
3. Start the VT200

After the customer completes the installation according to the above steps, the device can be started for debugging. The condition of the device can be told through the status indicator. To avoid consumption of battery power during transportation, the device is under transportation mode in the factory state. The VT200 needs to be activated by external power supply or the vehicle diagnostic interface.

3.1 Steps for usage

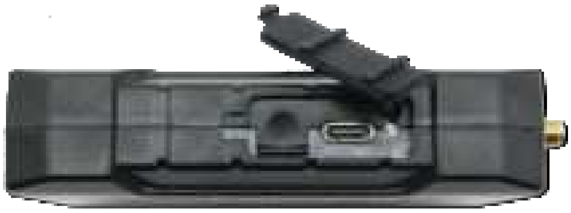
Steps:

1. Insert the 20PIN female head of P1 into the VT200;
2. Connect PIN20 CONN-X-V- and PIN10 CONN-X-V+ to the negative and positive poles of the power adapter respectively. PIN9 CONN-X-IGT and V + are both connected to the positive side of the power supply;

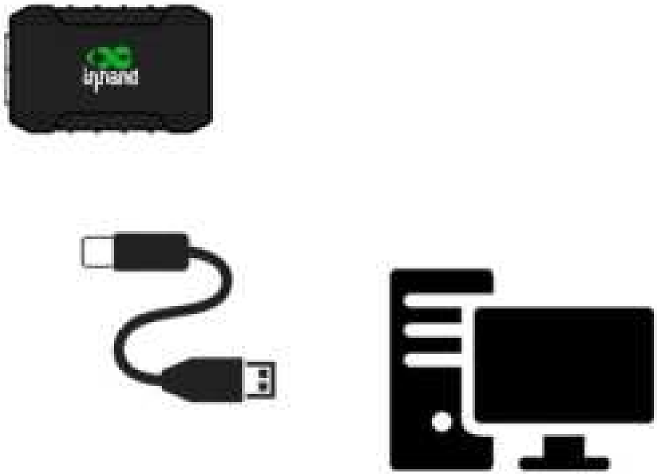


3. Use USB-Type C Debug and config VT200

4. Insert Micro-SIM card as shown with PIN request.Make sure that Micro-SIM card cut-off corner is pointing forward to slot.



5. After configuration, see “PC Connection (Windows)”, attach device top and bottom cover back. Download the configuration tool and connect the computer and VT200 with a USB Type C cable.



6. For external antenna models, please connect the 4G antenna to the ANT antenna interface of the device. The GNSS antenna is connected to the GNSS antenna interface of the device.

3.2 GNSS Status Light

Indicator Status	Function status
Long annihilation	The device is not started or the GNSS function is disabled.
Flash (frequency: 0.5Hz)	GNSS Time service succeeded GNSS delivery successful
Slow flash (frequency: 1Hz)	GNSS function enabled
Solid	Location success

3.3 Cellular Status Light

Indicator status	Function status
Long annihilation	The device is disabled or the dialing function is disabled.
Flash (frequency: 0.5Hz)	Dialed successfully
Slow flash (frequency: 1Hz)	Dialing enabled

Chapter II Login and Device Configuration

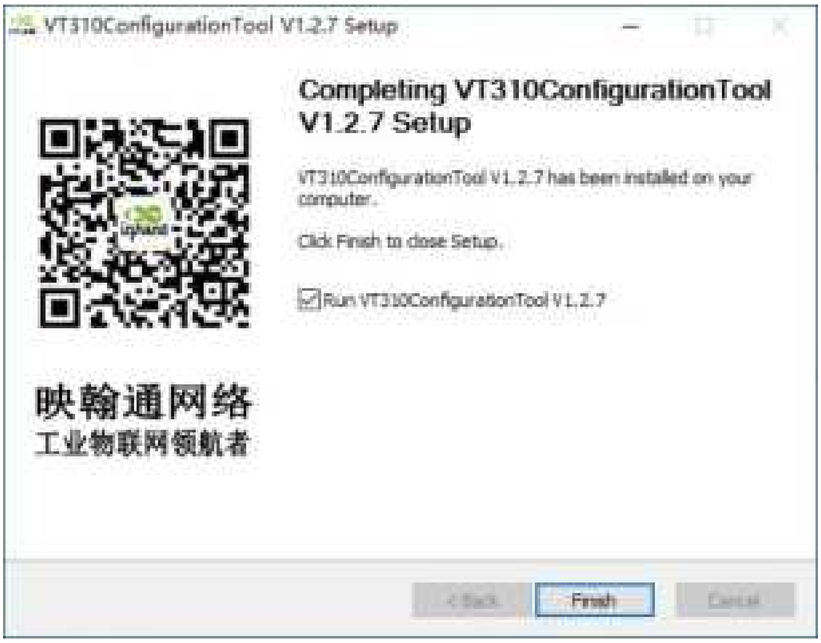
1. Install the Configuration Tool

The tool software supports the installation OS environment: **Windows 10** ;

Not support Windosw 7.

1.1 Download Configuration Tools

Enter the Download Center of InHand's Website, and download the tool from the Vehicle Gateway Part >>InVehicle T310 Tracker. Download the configuration tool installation package in the product documentation. Select the default path to complete the installation, as is shown below.



VT310ConfigurationTool V1.2.7 Setup

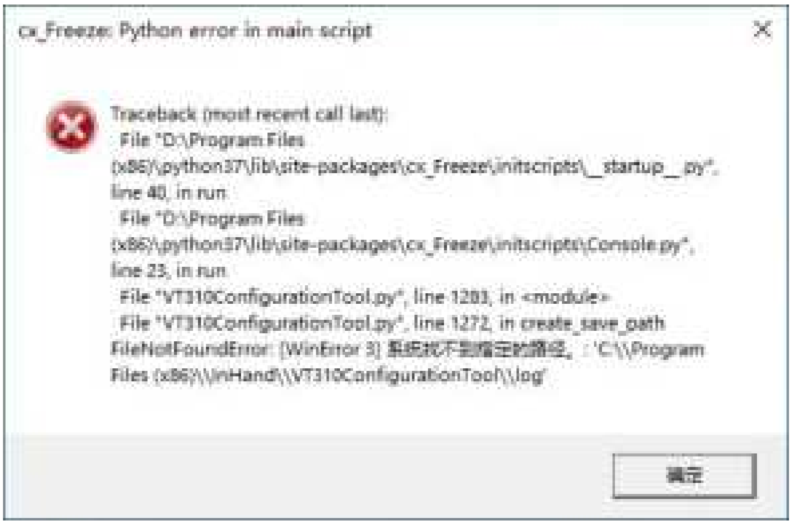
Completing VT310ConfigurationTool V1.2.7 Setup

VT310ConfigurationTool V1.2.7 has been installed on your computer.

Click Finish to close Setup.

☑ Run VT310ConfigurationTool V1.2.7

- If the following error occurs after installation, choose "Run as administrator" to open the software, as is shown below.

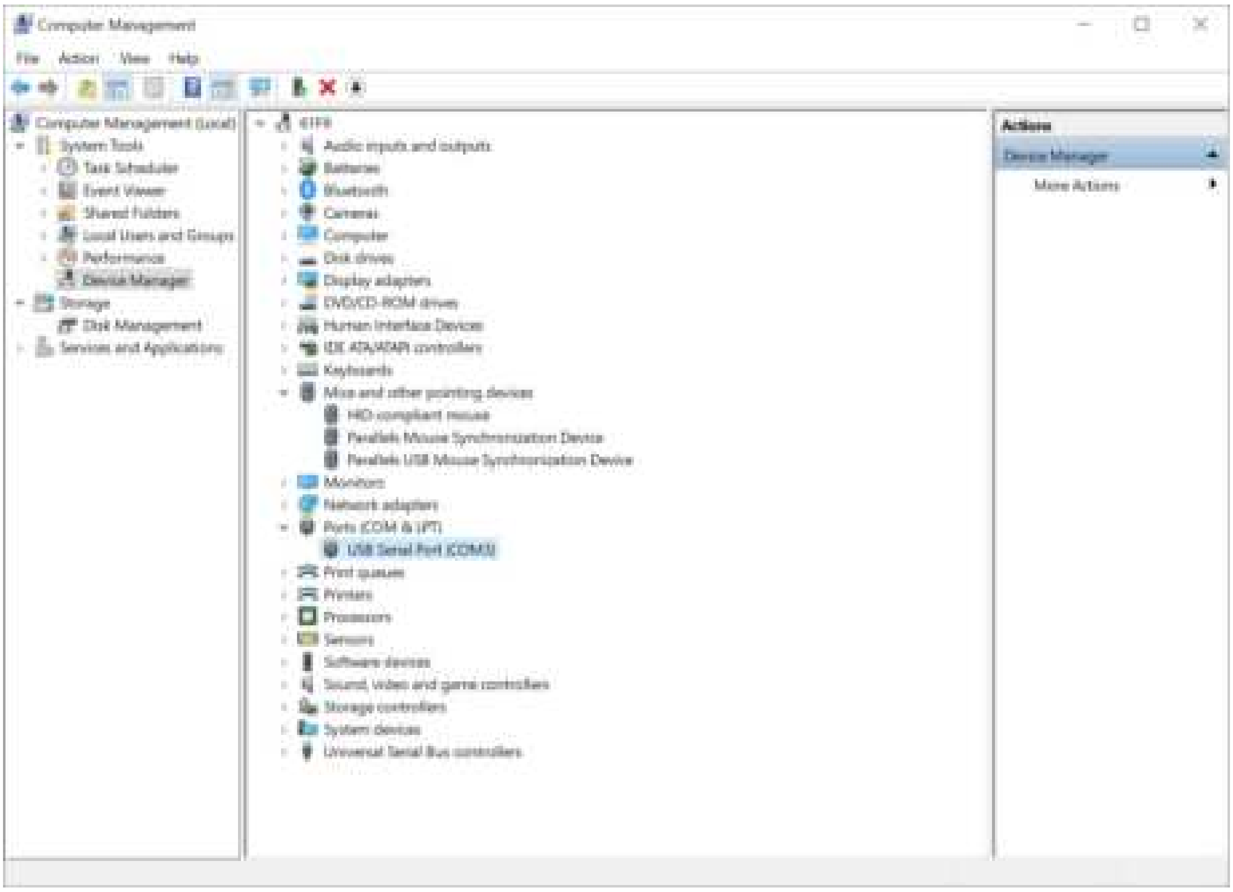


```
Traceback (most recent call last):
  File "D:\Program Files (x86)\python37\lib\site-packages\cx_Freeze\initscripts\__startup__.py", line 40, in run
  File "D:\Program Files (x86)\python37\lib\site-packages\cx_Freeze\initscripts\Console.py", line 23, in run
  File "VT310ConfigurationTool.py", line 1283, in <module>
  File "VT310ConfigurationTool.py", line 1272, in create_save_path
FileNotFoundError: [WinError 3] 系统找不到指定的路径。: 'C:\\Program Files (x86)\\inHand\\VT310ConfigurationTool\\log'
```

1.2 Search for the COM Port Number

Power the VT310 with an external adapter through the 26PIN all-in-one test cable. The VT310 is connected to the computer through a USB to serial port cable. If the GNSS or cellular light flickers, the device is started successfully.

Enter the device management page of the computer and observe the COM slogan in the "device manager"> "ports (COM and LPT)" of the computer, as is shown below.

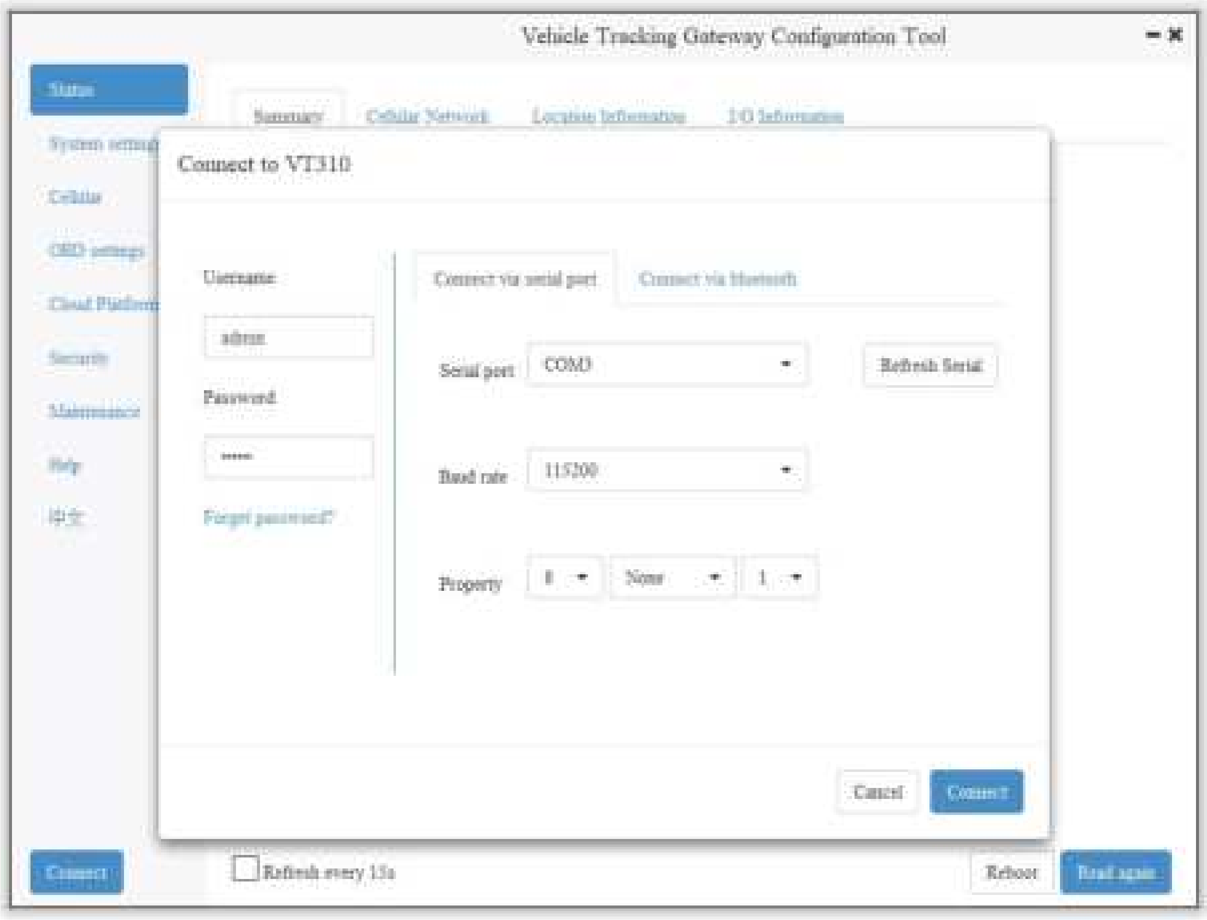


1.3 Login to the Device

The VT310 and VT320 software have the same functions and configuration methods.

Open the VT310 configuration tool . If an error message appears, open it as an administrator.

Click "Connect device", enter the user name and password (default: admin/123456), select the recorded serial port, baud rate (default: 115200), and click "connect", as is shown below.



Vehicle Tracking Gateway Configuration Tool

Connect to VT310

Username: admin

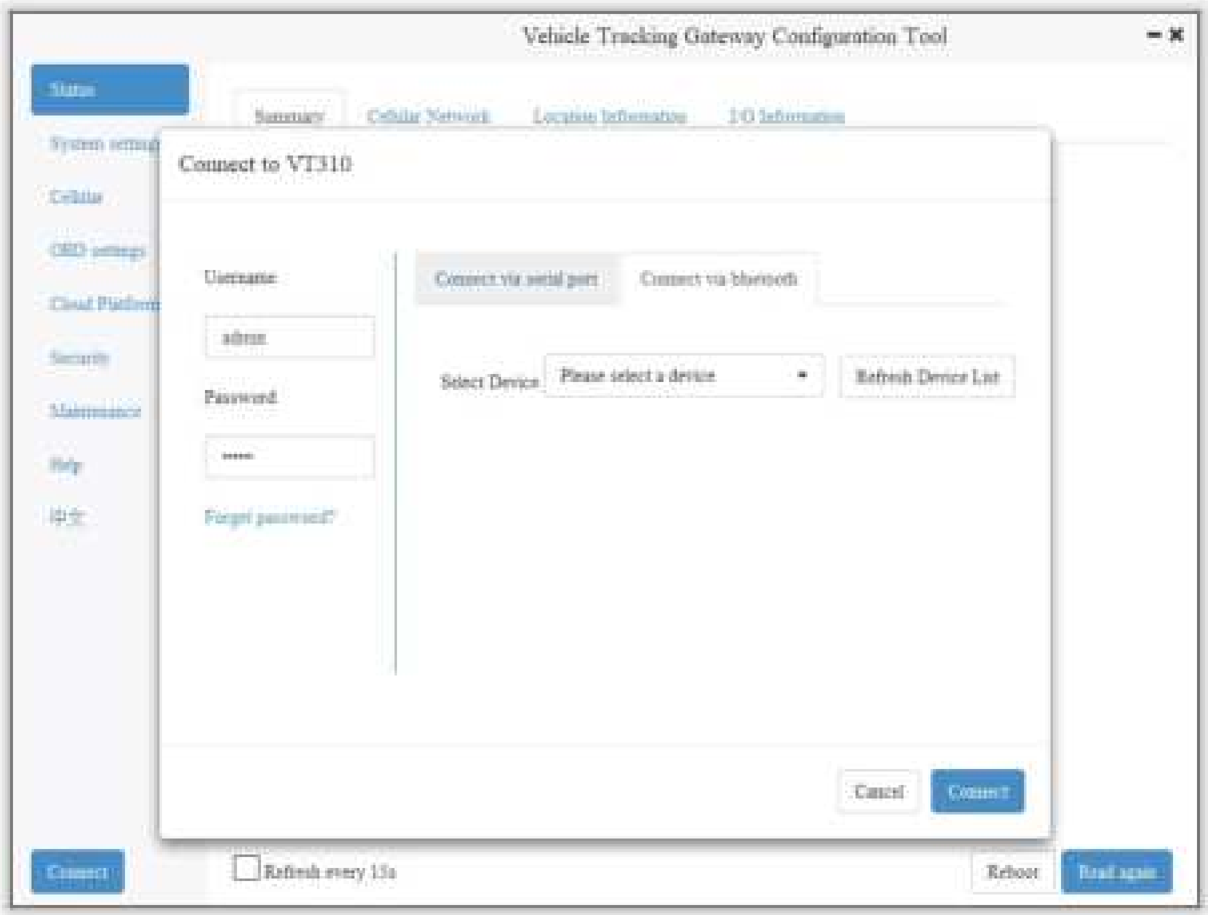
Password: ••••••

Serial port: COM3

Baud rate: 115200

Property: 8 None 1

You can also use computer Bluetooth (4.2 or above) to connect the device. Click "Connect device", enter the user name and password (default: admin/123456), select the Bluetooth device with the same name as the device SN (SN can be found on the device nameplate), and click Connect ", as is shown below.

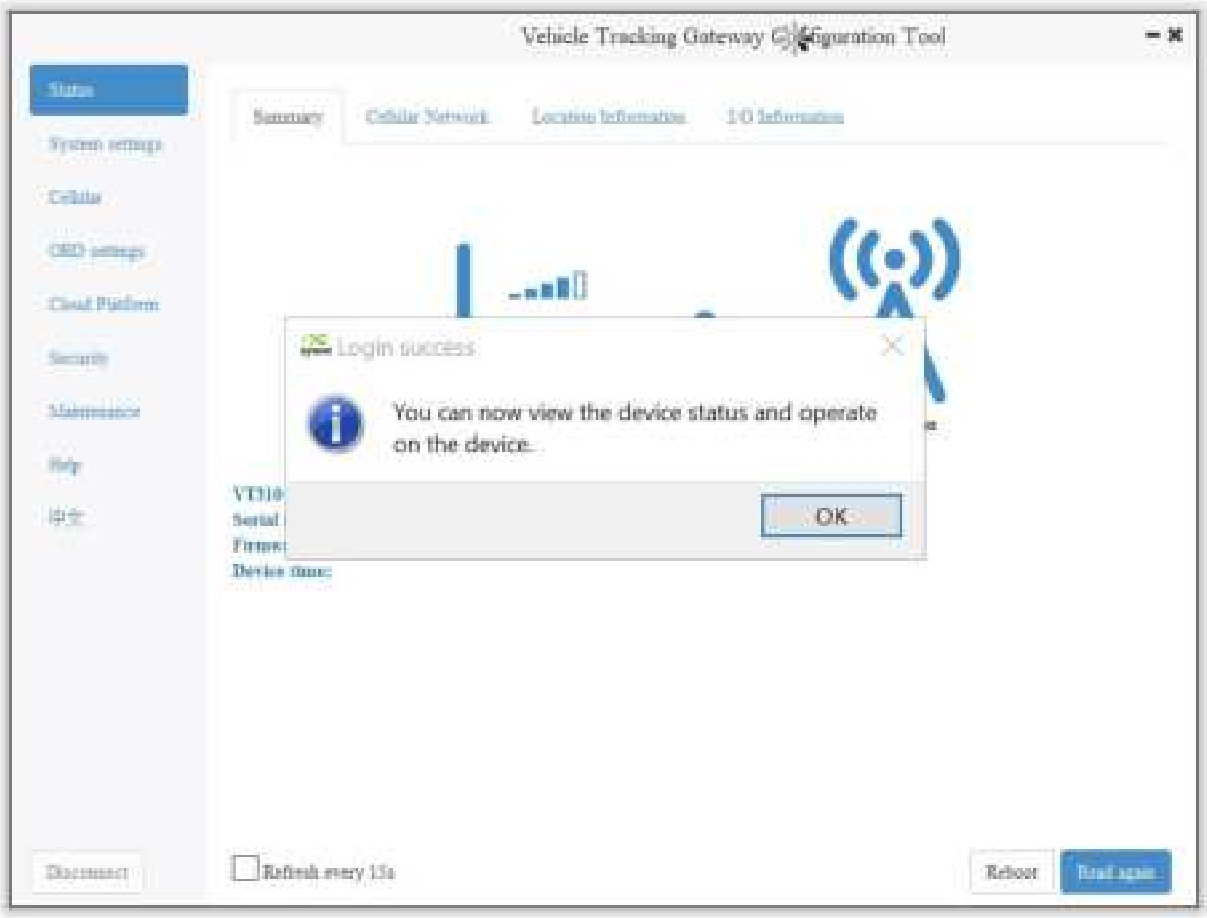


Username: admin

Password: *****

Select Device: Please select a device

In the dialog box that pops up, you can view the device status and perform operations on the device. Click OK to preview or modify the configuration, as is shown below.



Login success

You can now view the device status and operate on the device.

OK

Login succeeded

2. Inquire Status Information

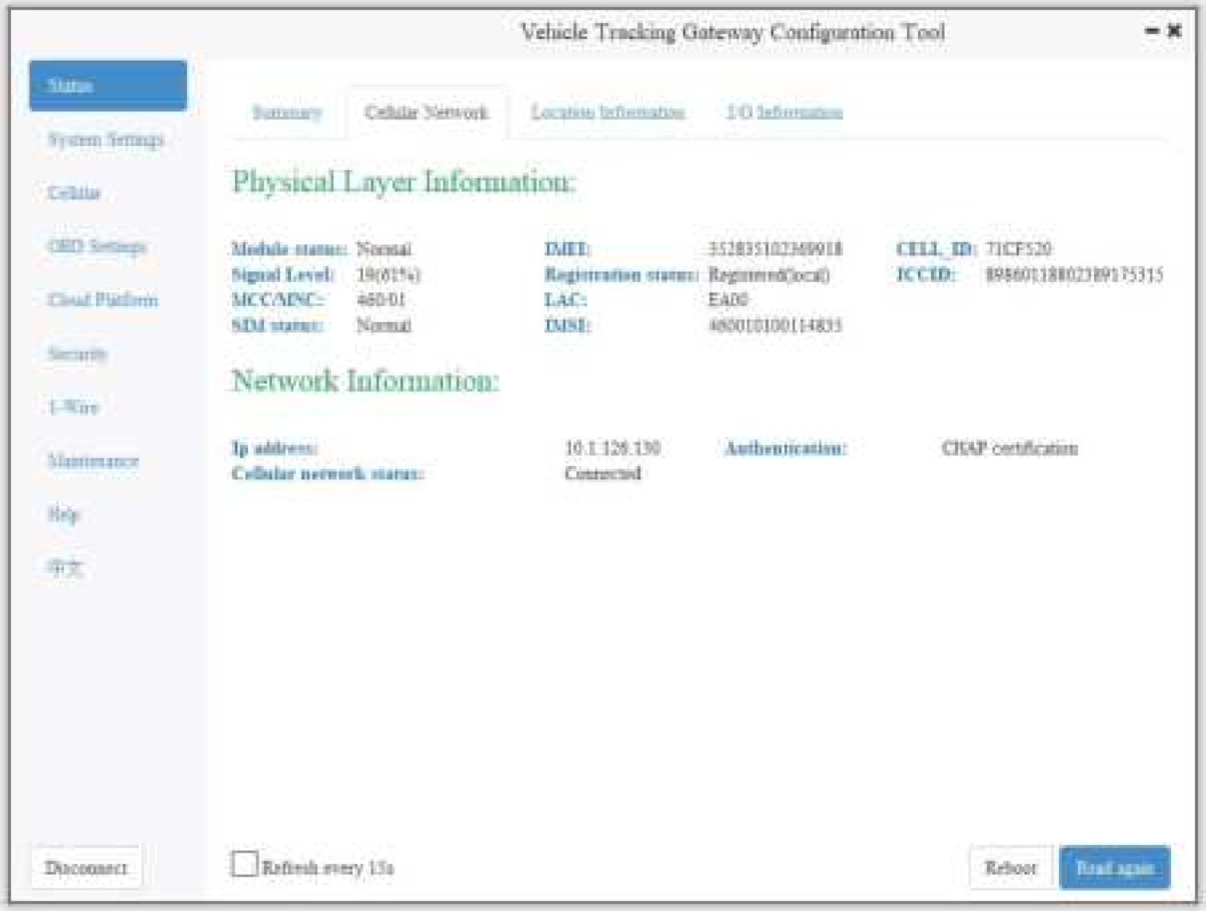
2.1 Mobile Network Parameters

On this page are mobile network link parameters, which are used mainly to check whether the wireless network link is normal. All parameters read when the SIM is not inserted are default parameters. After the device is connected to the Internet through the SIM card, it can obtain the IP address for data transmission. For configuration of mobile network parameters, please refer to Section 4 Configure the Cellular Network.

Parameter	Description

Signal value	Indicates the signal strength of the connected wireless network. Valid values: 0 to 31.
MCC/NMC	MCC (mobile country code), MNC (mobile network code), read from the SIM card
SIM card status	Normal/Unidentified
IMEI	The International Mobile device identification code (International Mobile Equipment Identity) is the built-in dialing module code of the vehicle gateway.
Registration	Registered/Not registered
LAC	LAC(Location area code) , obtain this parameter from the base station after dialing successfully
IMSI	IMSI(International Mobile Subscriber Identity) this parameter is read from the SIM card
CELL ID	This parameter is obtained from the base station after dialing successfully.
ICCID	The ID of the integrated circuit card is the SIM card number and ICCID (integrated circuit card identity). This parameter is read from the SIM card.
IP ADDRESS	After the dialing is successful, the carrier assigns the IP address of the

	network access.
Cellular status	Connected/Not connected
Authentication method	CHAP/PAP



Physical Layer Information:

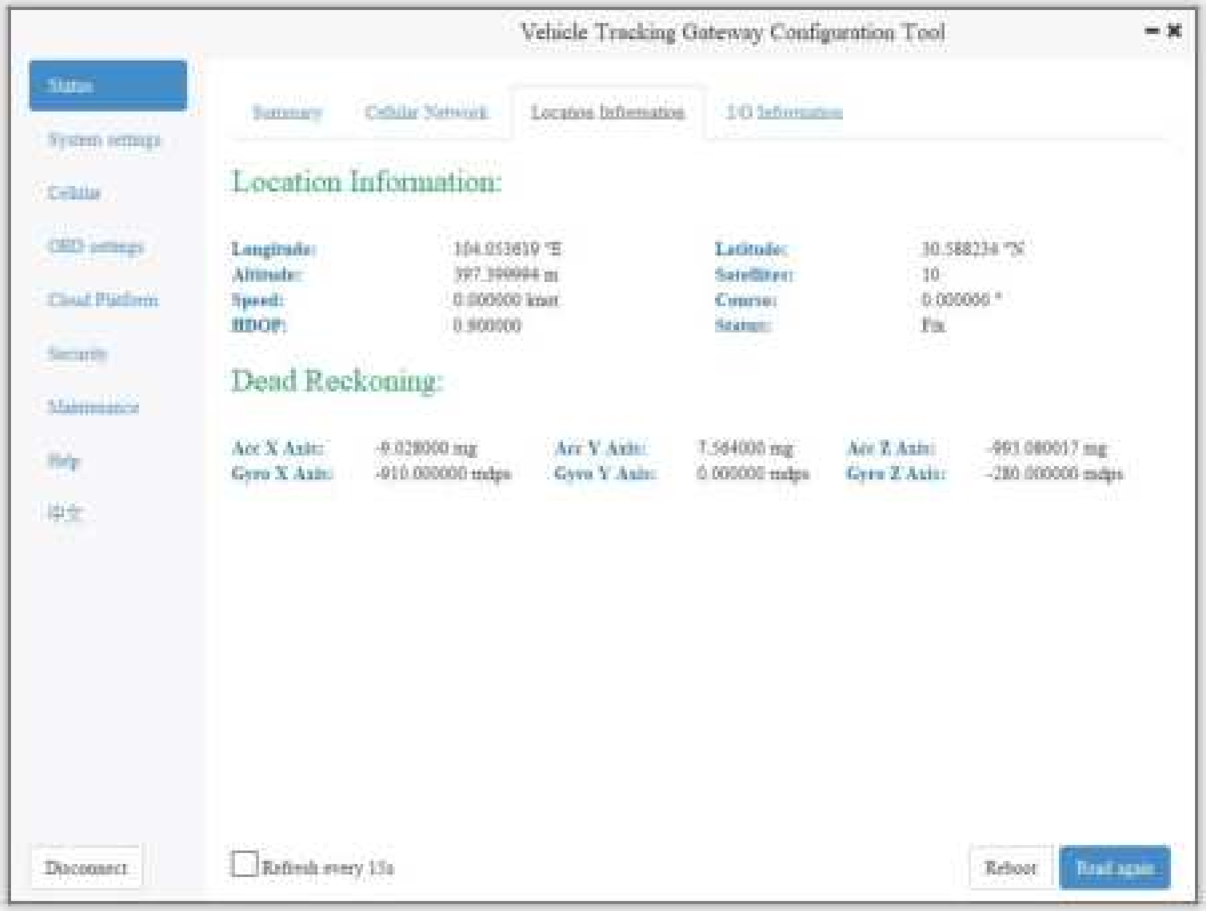
Module status: Normal
Signal Level: 19(61%)
MCC/MNC: 460-01
SIM status: Normal
IMEI: 352835102369918
Registration status: Registered(local)
LAC: EA00
IMSI: 460010100114835
CELL_ID: 71CF520
ICCID: 89860118802389175315

Network Information:

Ip address: 10.1.128.130
Cellular network status: Connected
Authentication: CHAP certification

2.2 Location Information

The location information page shows the latest parameters obtained by the GNSS module. It includes location information and related parameters of the inertial sensor. As is shown below.



Location Information:

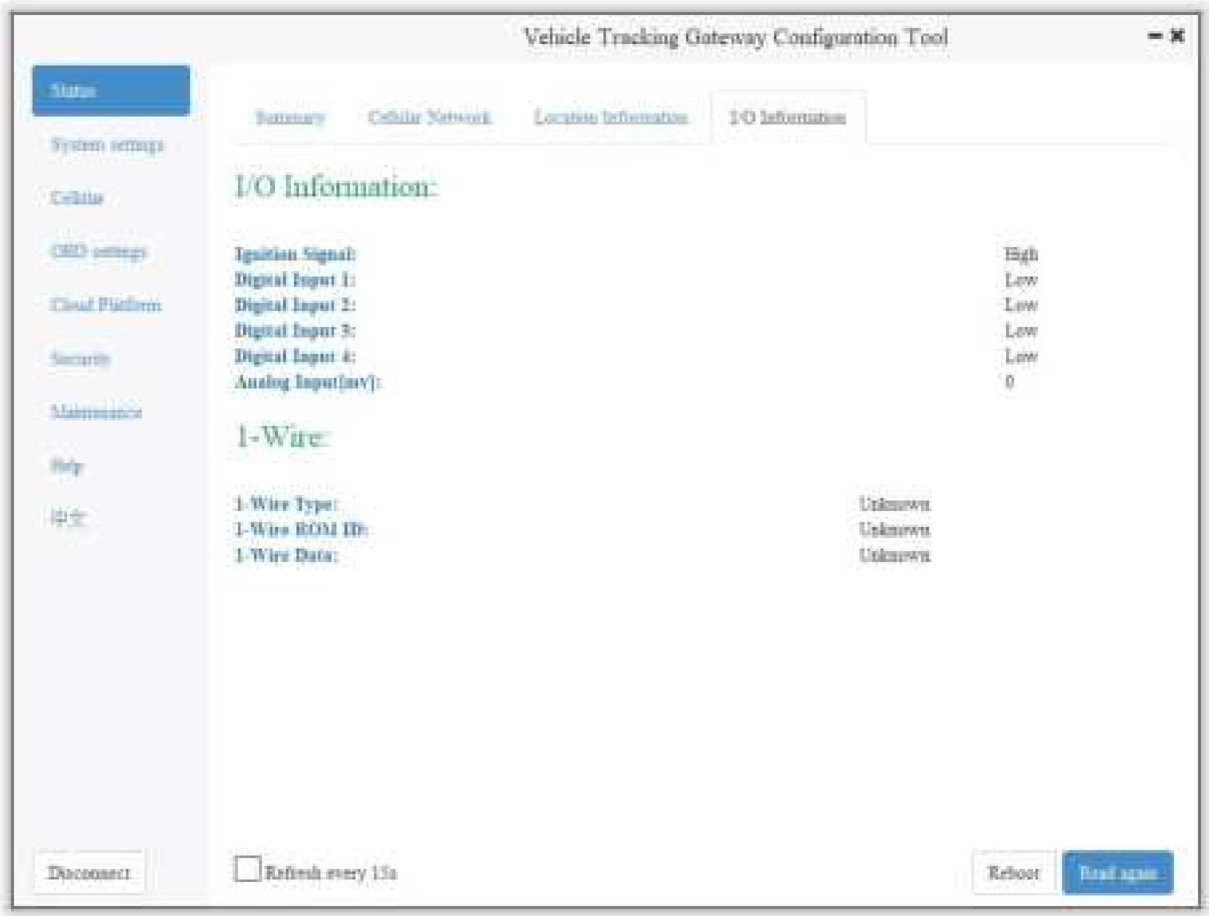
Longitude:	104.053619 °E	Latitude:	30.588234 °N
Altitude:	397.399994 m	Satellites:	10
Speed:	0.000000 knot	Course:	0.000000 °
HDOP:	0.900000	Status:	Fix

Dead Reckoning:

Acc X Axis:	-9.028000 mg	Acc Y Axis:	7.564000 mg	Acc Z Axis:	-993.080017 mg
Gyro X Axis:	-910.000000 mdps	Gyro Y Axis:	0.000000 mdps	Gyro Z Axis:	-280.000000 mdps

□ Refresh every 15s

2.3 I/O Information



I/O Information:

Ignition Signal: High
Digital Input 1: Low
Digital Input 2: Low
Digital Input 3: Low
Digital Input 4: Low
Analog Input(mv): 0

1-Wire:

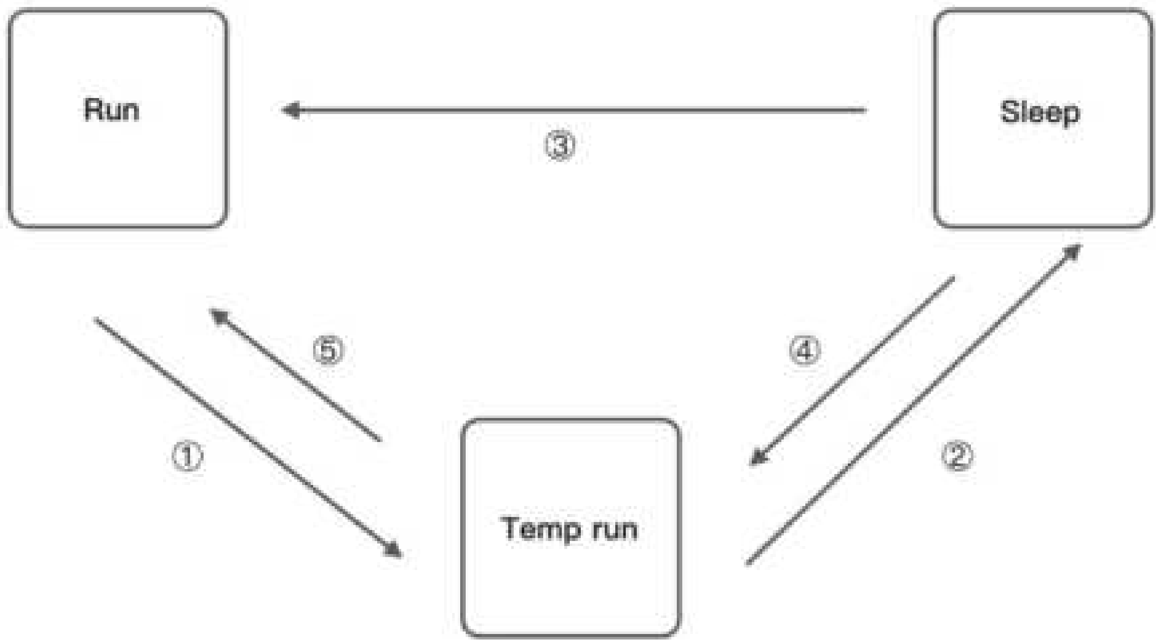
1-Wire Type: Unknown
1-Wire ROM ID: Unknown
1-Wire Data: Unknown

□ Refresh every 15s

3. System Settings

3.1 Sleep Mode

The sleep mode ensures the battery life after flameout, providing continuous guarantee for special environments. The state machine is as follows:



Description of the state machine:

Run, Sleep, and Temp run represent normal running status, sleep status, and temporary running status respectively.

① Corresponding to the state machine, the condition from Run to Temp run is that the power supply voltage is less than sleep voltage (6V by default) or IGT OFF (IGT needs to be enabled in the configuration), by default, the device continues to run for 15Stemp (for reporting information) and then enters Sleep;

② Corresponding to the state machine, the condition of entering Sleep from the Temp run is that after the device runs a wake-up runtime cycle in the Temp run or after the device runs Temp Run for 15s from run;

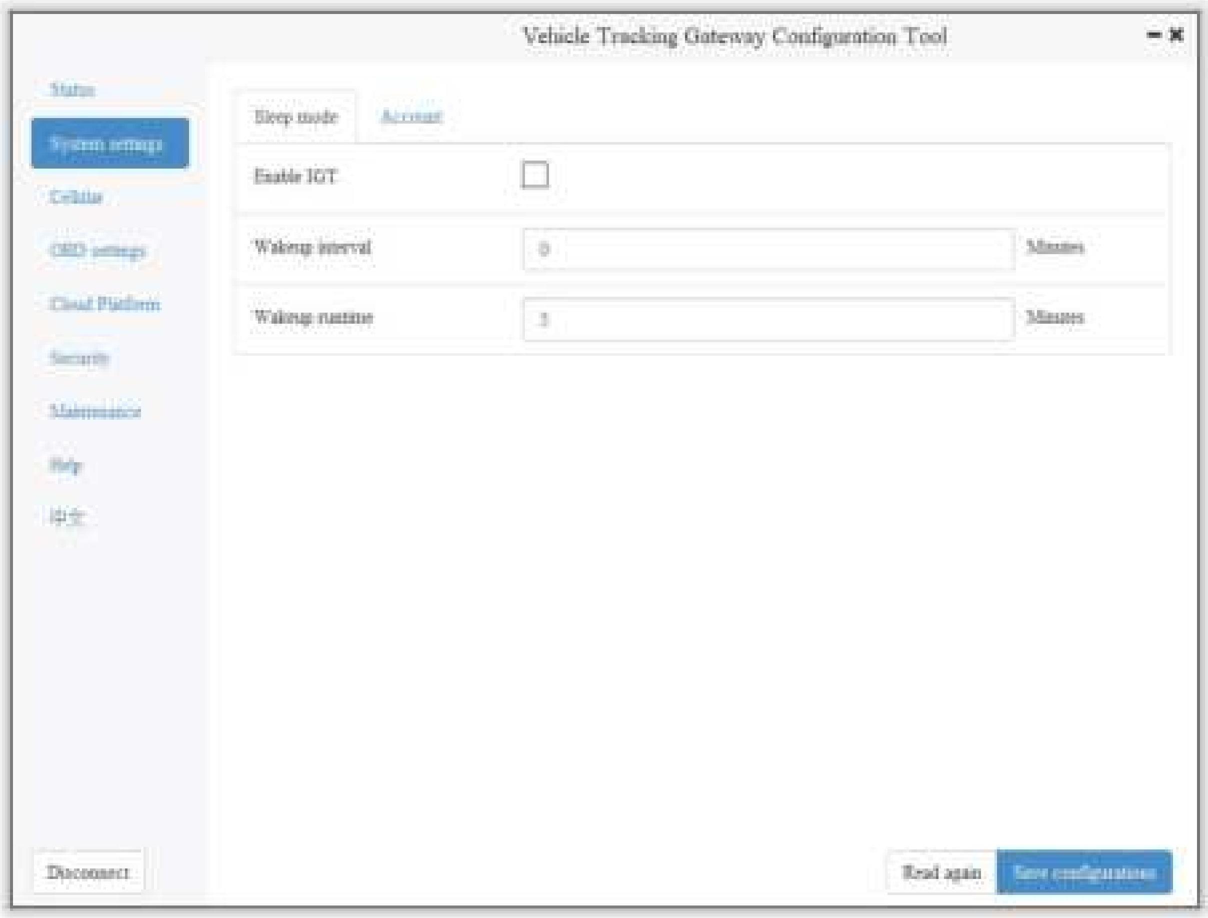
③ Corresponding to the state machine, the condition from Sleep to Run is that the power supply voltage is greater than Sleep voltage or IGT ON (IGT needs to be enabled in configuration);

④ Corresponding to the state machine, the condition of entering the Temp run from Sleep is that after the device runs a wake-up interval in Sleep;

⑤ Corresponding to the state machine, the condition from Temp run to Run is that the power supply voltage is greater than sleep voltage or IGT ON (IGT needs to be enabled in configuration);

Configure the sleep mode:

Parameter	Description
Enable IGT	After IGT is enabled, the device uses the IGT status as the condition for entering or exiting Sleep. The IGT status is not ticked by default.
Wake-up interval	The interval between the device automatically wakes up in Sleep, whose default value is 120 minutes.
Wake-up time	The interval between the time when the device enters the next Sleep, whose default value is 5 minutes.



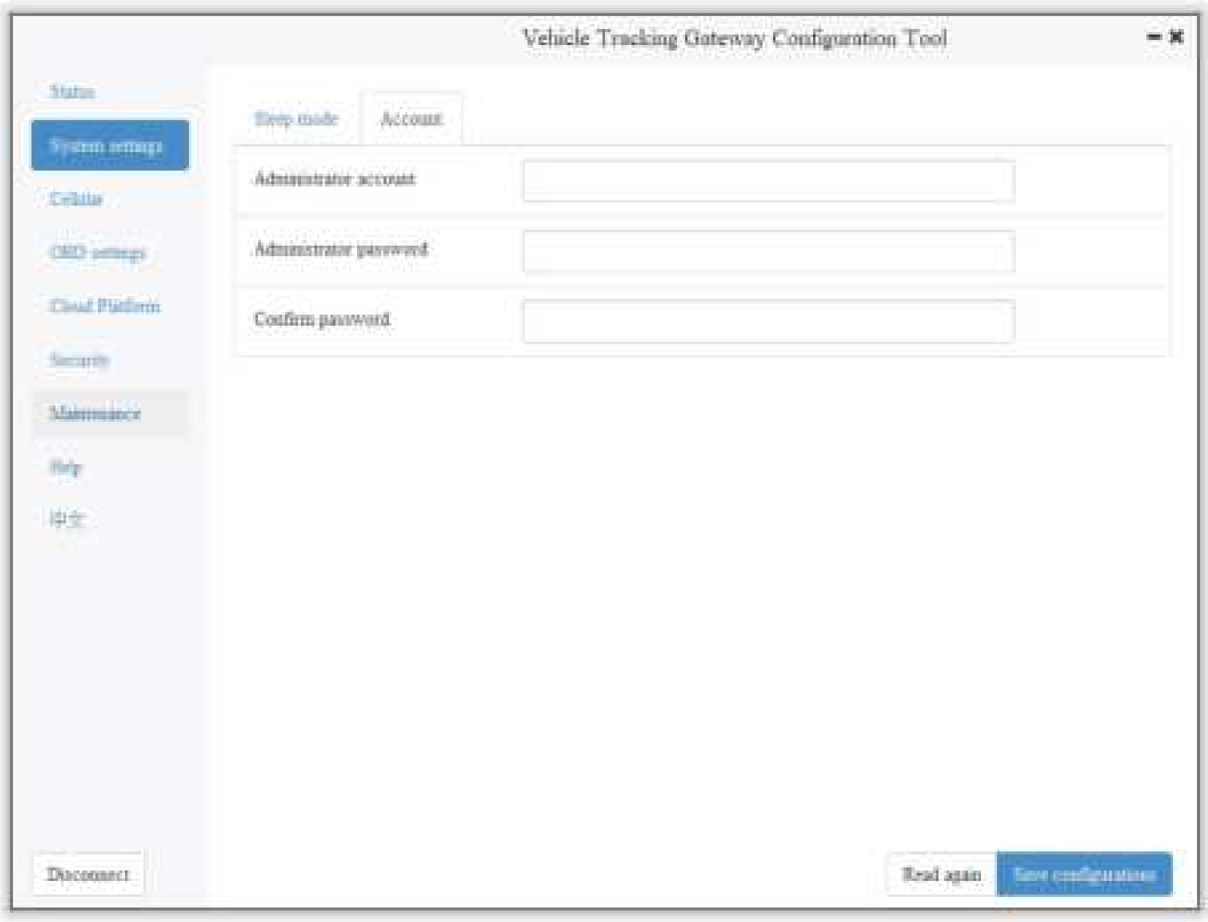
Enable IGT □

Wakeup interval 0 Minutes

Wakeup runtime 3 Minutes

3.2 Account Settings

This function allows the device administrator to modify the device administrator login information. The default administrator account is admin, password 123456. The device administrator can modify the configuration options if necessary. After the modification, the device prompts a restart. Click OK to restart the device and log in with the modified administrator account and password. As is shown below.



Administrator account

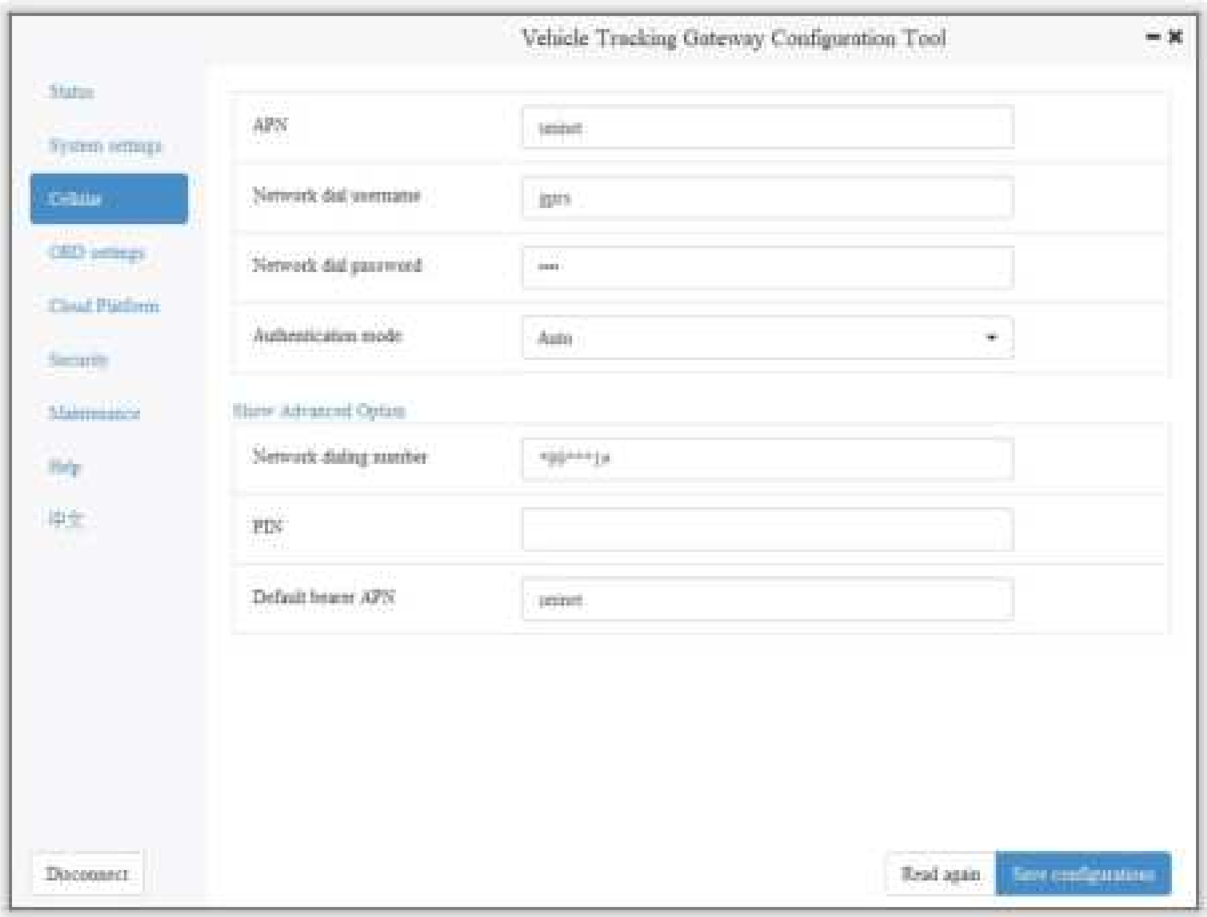
Administrator password

Confirm password

4. Configure the Cellular Network

Click "Cellular" to enter the configuration page. Generally, customers only need to configure "Network Access Point Name (APN)", "Network dialing user name", "Network dialing password" and "Authentication mode" and click "Save configuration". The device takes effect after restarting.

If the customer has special trial scenarios, click "Show Advanced Options" to see hidden configuration items. Configure the network dial number, PIN, and default host APN as needed. As is shown below.



APN: internet

Network dial username: gprs

Network dial password: ****

Authentication mode: Auto

Network dialing number: *99***1#

PIN:

Default bearer APN: internet

Parameter	Description
APN	This parameter is required when the APN private network is connected to the mobile network. Most public network service SIM cards do not authenticate APN when dialing.
Network dialing username	The default parameter is ″gprs″. When the private network is AAA certified, the mobile network operator needs to provide this parameter.
Network dialing password	The default parameter is “gprs”. This is required by the carrier during the AAA certification for the private network.

Authentication mode	Automatic/CHAP/PAP. This parameter is required when the private network is AAA certified. Automatic: take turns to use PAP and CHAP authentication to dial (pap authentication is used for the first power-on, if dialing fails, chap authentication is used for dialing again, and pap authentication is used for the next dialing, and so on. If the authentication mode is not automatic, but PAP or CHAP, use only PAP or CHAP authentication to dial.
Network dial number	The default parameter is * 99 *** 1#, which is required by mobile network operators.
PIN	PIN (Personal Identification Number) refers to the Personal Identification password of the SIM card. When the SIM card is enabled for PIN verification, does it fill in the corresponding PIN of the SIM card. This parameter is required for mobile network operators.
Default carrier APN	This parameter is provided by the carrier.

The default host setting is a function for special data transmission required by some carriers, which generally does not need configuration. If configuration is required, please inquire from your carrier.

5. Configuration of Vehicle Diagnostic Interface

The on-board diagnostic interface is the South interface of the tracker and the configuration option of the protocol.

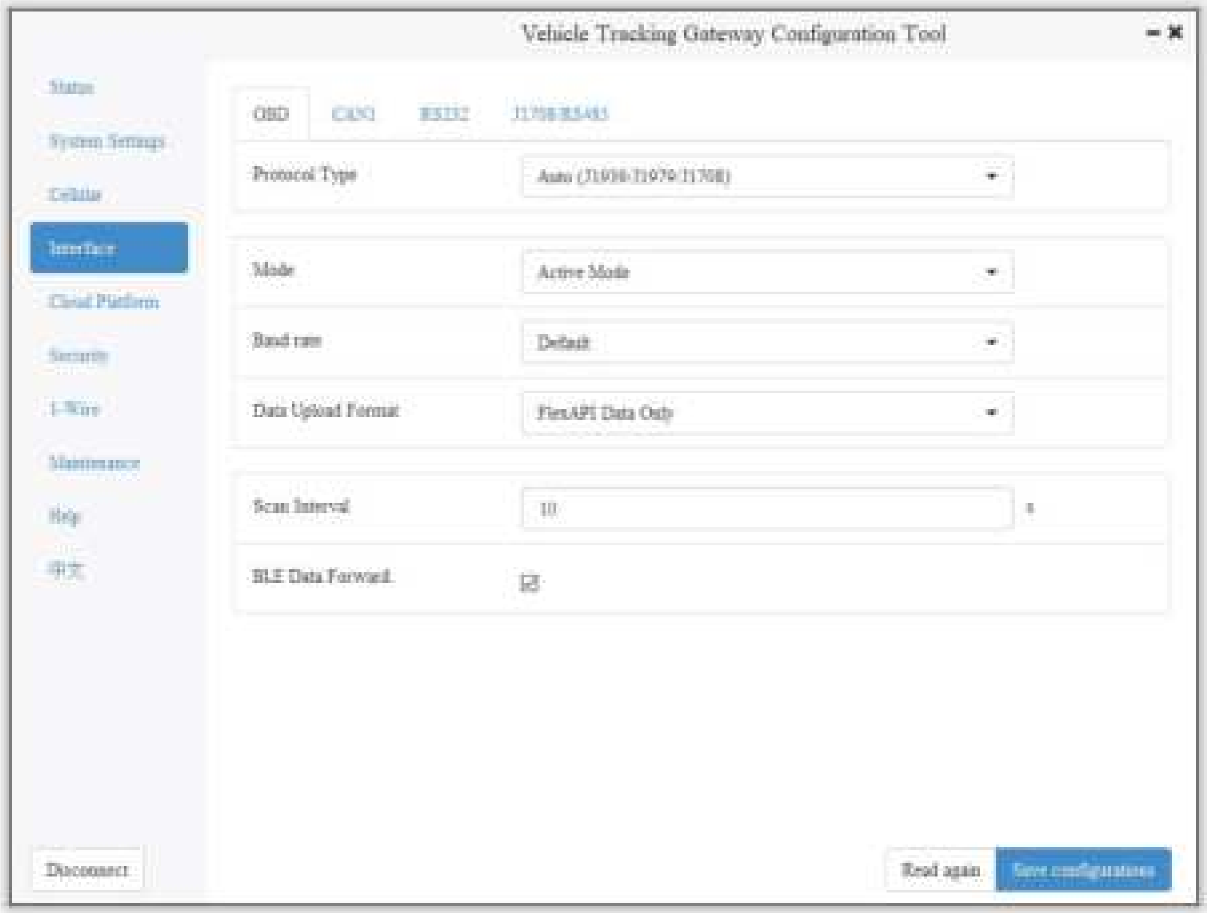
5.1 Configure ODB Interface

In the configuration tool, select OBD as the diagnostic protocol. The ODB protocol is the CAN2 interface and J1708 interface of the vehicle tracker.

	Parameter	Description	Others
Protocol Type	AUTO(J1939/J1979)	ODB CAN2 interface protocol, corresponding to physical layer PIN CAN_2L(PIN 12) and CAN_2H(PIN 25)	OBD default configuration
	AUTO(J1939/J1979/J1708)	When set to Auto mode, the vehicle tracker will poll the link and automatically poll and send the protocol data of the above four options for link testing. When receiving data packets of the corresponding	When Auto mode is used, the CAN1 and J1708 interfaces are enabled at the same time.

		protocol, the vehicle tracker will choose this protocol for communication.	
	J1939	ODB CAN2 interface protocol, corresponding to physical layer PIN CAN_2L(PIN 12) and CAN_2H(PIN 25)	
	J1939	ODB CAN2 interface protocol, corresponding to physical layer PIN CAN_2L(PIN 12) and CAN_2H(PIN 25)	
	J1708	J1708 interface protocol, corresponding to physical layer PIN J1708_ B(PIN13) and J1708_A (PIN 26)	
	Disable	Disable ODB CAN2 and J1708	
Mode	Active mode		
	Passive mode		
Baudrate	default		

	250K		
	500K		
Data Upload Format			
Scan Interval			
BLE Data Forward			



Protocol Type: Auto (J1939/J1979/J1708)

Mode: Active Mode

Baud rate: Default

Data Upload Format: FlexAPI Data Only

Scan Interval: 10 s

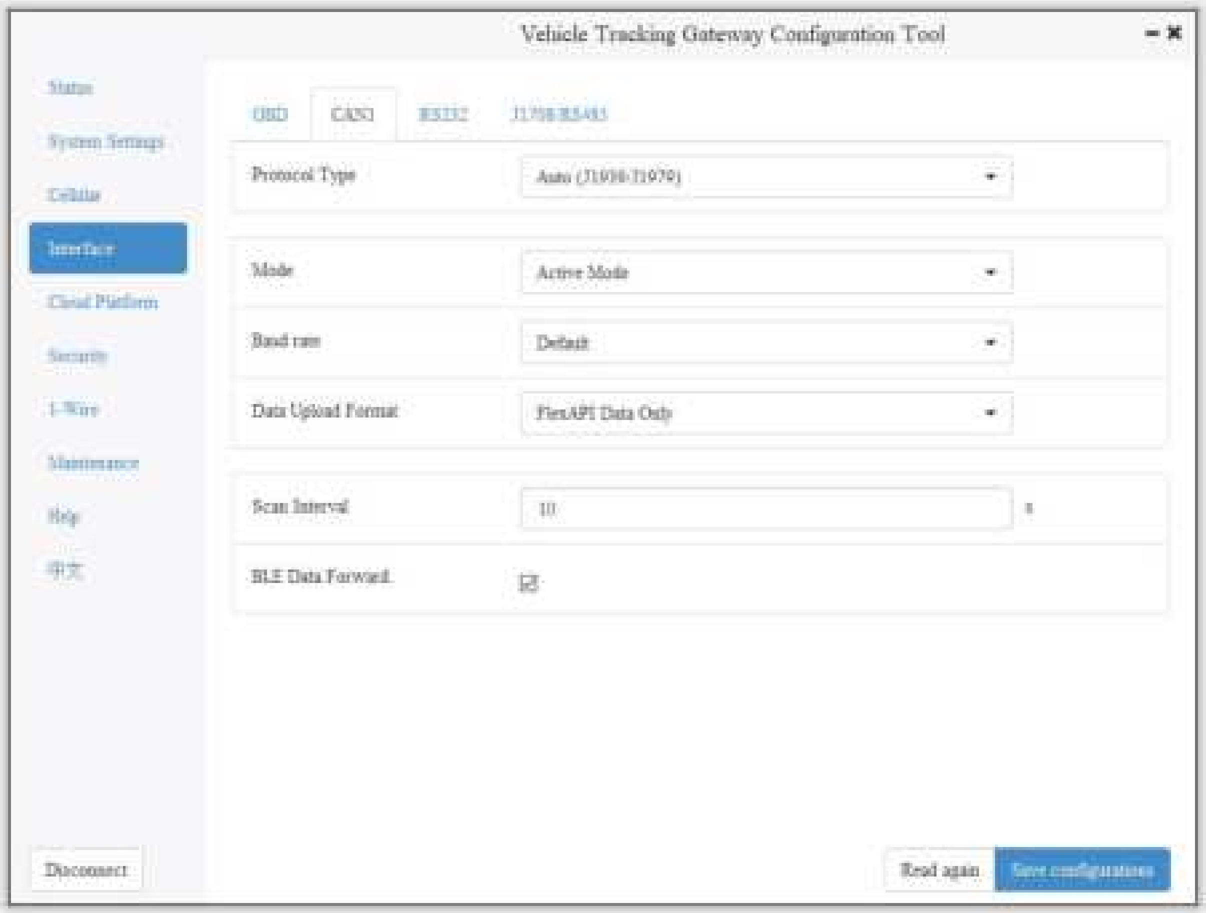
BLE Data Forward: ☑

5.2 Configure CAN1 Interface

In the configuration tool, select CAN1 as the diagnostic protocol and the CAN1 interface of the vehicle tracker.

	Parameter	Description	Others
Protocol Type	J1939/J1979	CAN1 interface protocol, corresponding to physical layer PIN CAN_1L(PIN 11) and CAN_1H(PIN 24)	CAN1 default configuration
	J1939	CAN1 interface protocol, corresponding to physical layer PIN CAN_1L(PIN 11) and CAN_1H(PIN 24)	
	J1939	CAN1 interface protocol, corresponding to physical layer PIN CAN_1L(PIN 11) and CAN_1H(PIN 24)	
	Disable	Disable CAN1	
Mode	Active mode		
	Passive mode		

Baudrate	default		
	250K		
	500K		
Data Upload Format			
Scan Interval			
BLE Data Forward			



Protocol Type: Auto (J1939/J1979)

Mode: Active Mode

Baud rate: Default

Data Upload Format: FlexAPI Data Only

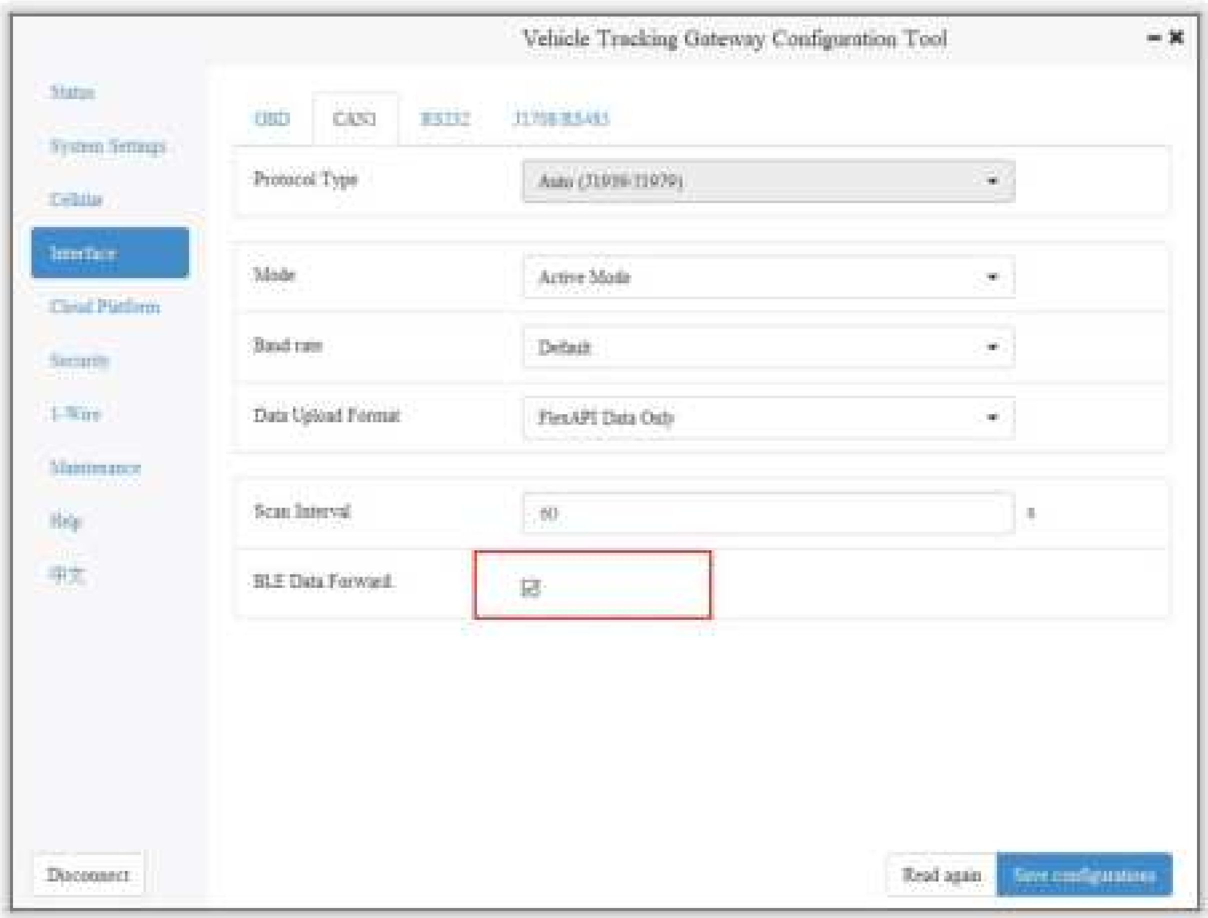
Scan Interval: 10 s

BLE Data Forward: ☑

- The function of CAN1 and OBD can be enabled at the same time.

5.3 How to use ELD?

After ELD is enabled, the data read by CAN, OBD and J1708 will be forwarded as Bluetooth notification.



Protocol Type: Auto (J1939/J1979)

Mode: Active Mode

Baud rate: Default

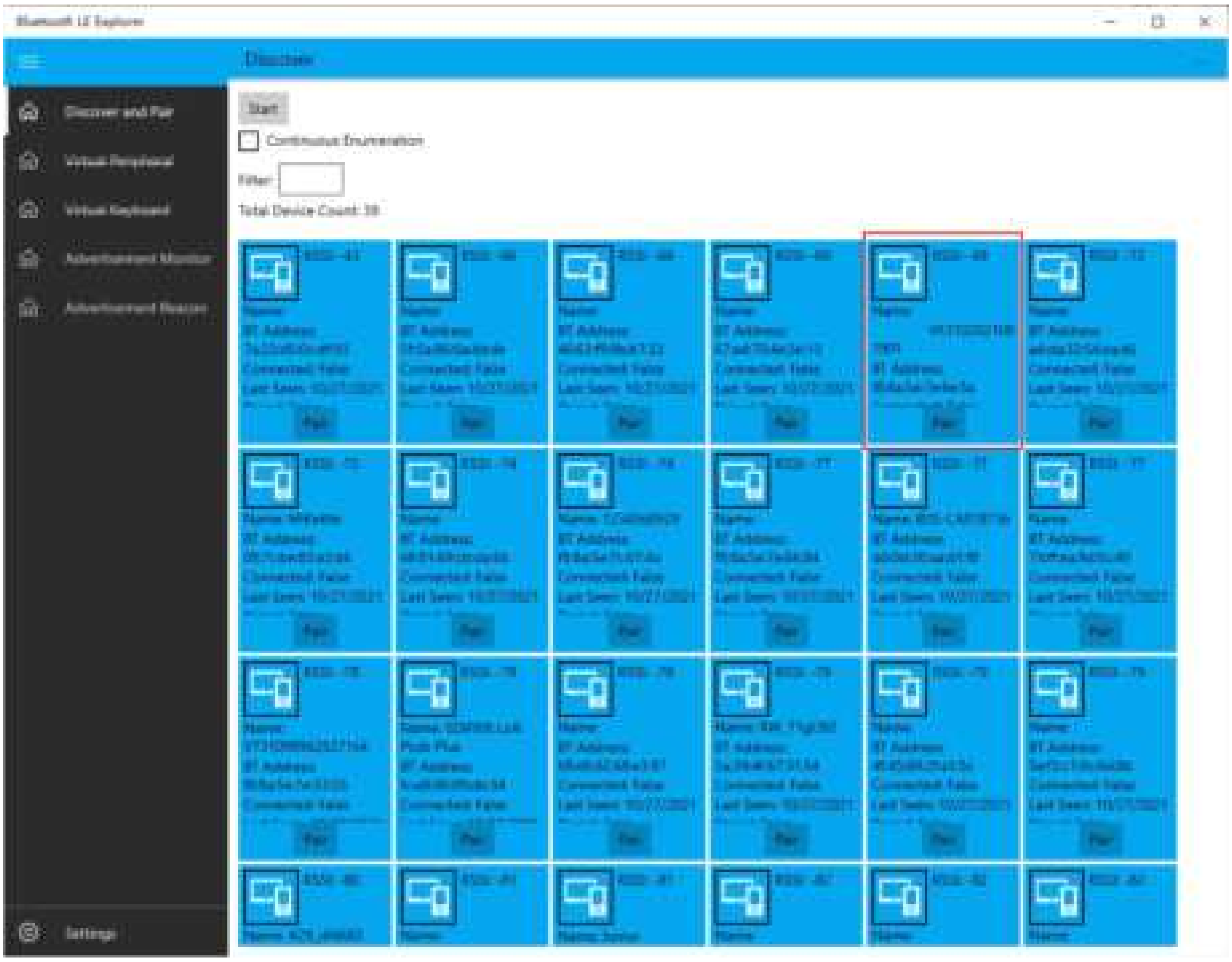
Data Upload Format: FlexAPI Data Only

Scan Interval: 60 s

BLE Data Forward: ☑

Download Bluetooth LE Explorer from the Microsoft Store to connect to VT.

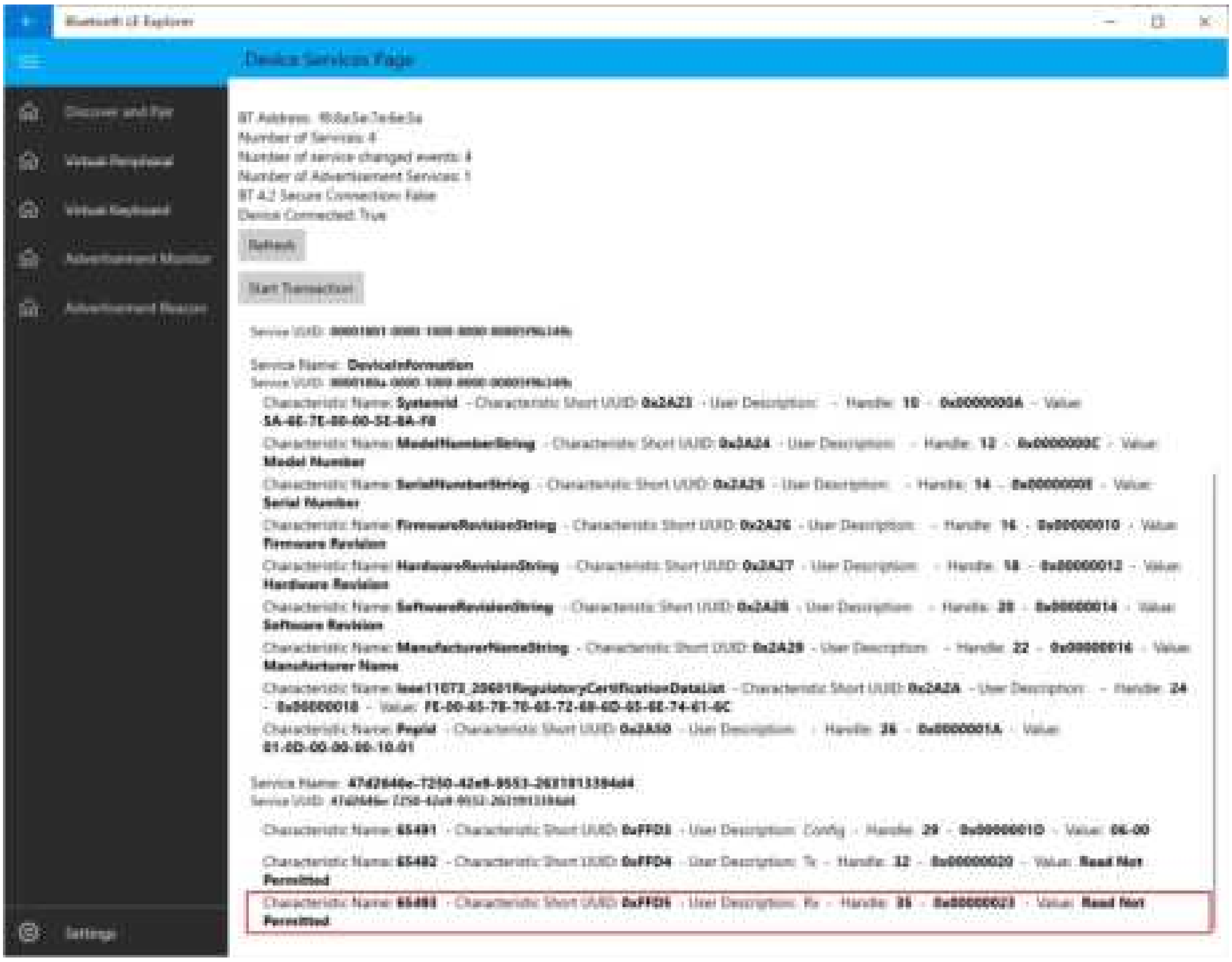
Click Start to search VT. The bluetooth name is the same as SN.



□ Continuous Enumeration

Total Device Count: 38

Then select the last one to read the Bluetooth notification.



BT Address: f8:8a:5e:7e:6e:5a
Number of Services: 4
Number of service changed events: 4
Number of Advertisement Services: 1
BT 4.2 Secure Connection: False
Device Connected: True

Service UUID: **00001801-0000-1000-8000-00805f9b34fb**

Service Name: **DeviceInformation**
Service UUID: **0000180a-0000-1000-8000-00805f9b34fb**

Characteristic Name: **SystemId** - Characteristic Short UUID: **0x2A23** - User Description: - Handle: **10** - **0x0000000A** - Value: **5A-6E-7E-00-00-5E-8A-F8**

Characteristic Name: **ModelNumberString** - Characteristic Short UUID: **0x2A24** - User Description: - Handle: **12** - **0x0000000C** - Value: **Model Number**

Characteristic Name: **SerialNumberString** - Characteristic Short UUID: **0x2A25** - User Description: - Handle: **14** - **0x0000000E** - Value: **Serial Number**

Characteristic Name: **FirmwareRevisionString** - Characteristic Short UUID: **0x2A26** - User Description: - Handle: **16** - **0x00000010** - Value: **Firmware Revision**

Characteristic Name: **HardwareRevisionString** - Characteristic Short UUID: **0x2A27** - User Description: - Handle: **18** - **0x00000012** - Value: **Hardware Revision**

Characteristic Name: **SoftwareRevisionString** - Characteristic Short UUID: **0x2A28** - User Description: - Handle: **20** - **0x00000014** - Value: **Software Revision**

Characteristic Name: **ManufacturerNameString** - Characteristic Short UUID: **0x2A29** - User Description: - Handle: **22** - **0x00000016** - Value: **Manufacturer Name**

Characteristic Name: **Ieee11073_20601RegulatoryCertificationDataList** - Characteristic Short UUID: **0x2A2A** - User Description: - Handle: **24** - **0x00000018** - Value: **FE-00-65-78-70-65-72-69-6D-65-6E-74-61-6C**

Characteristic Name: **PnpId** - Characteristic Short UUID: **0x2A50** - User Description: - Handle: **26** - **0x0000001A** - Value: **01-0D-00-00-00-10-01**

Service Name: **47d2646e-7250-42e8-9553-2631813394d4**
Service UUID: **47d2646e-7250-42e8-9553-2631813394d4**

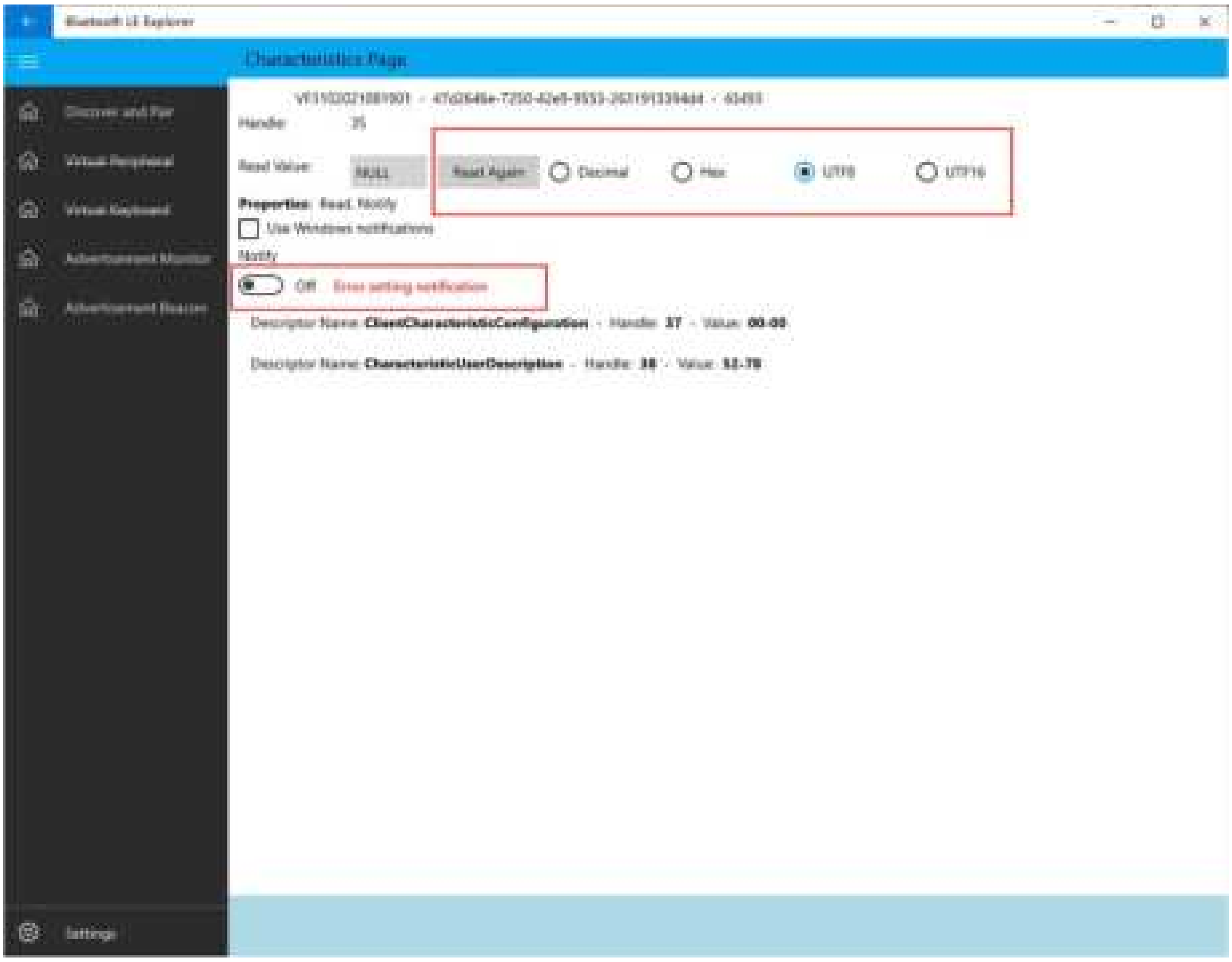
Characteristic Name: **65491** - Characteristic Short UUID: **0xFFD3** - User Description: Config - Handle: **29** - **0x0000001D** - Value: **06-00**

Characteristic Name: **65492** - Characteristic Short UUID: **0xFFD4** - User Description: Tx - Handle: **32** - **0x00000020** - Value: **Read Not Permitted**

Characteristic Name: **65493** - Characteristic Short UUID: **0xFFD5** - User Description: Rx - Handle: **35** - **0x00000023** - Value: **Read Not Permitted**

Turn on Notify (Ignore error messages). Bluetooth notification messages is in Read Value. Data format:

<ESN|VIN|SPEED|ODOMETER|ENGINEHOURS|RPM>



VT310202108?901 - 47d2646e-7250-42e9-9553-2631913394dd - 63493

Handle: 35

Read Value: NULL

○ Decimal ○ Hex ● UTF8 ○ UTF16

Properties: Read, Notify

□ Use Windows notifications

Notify

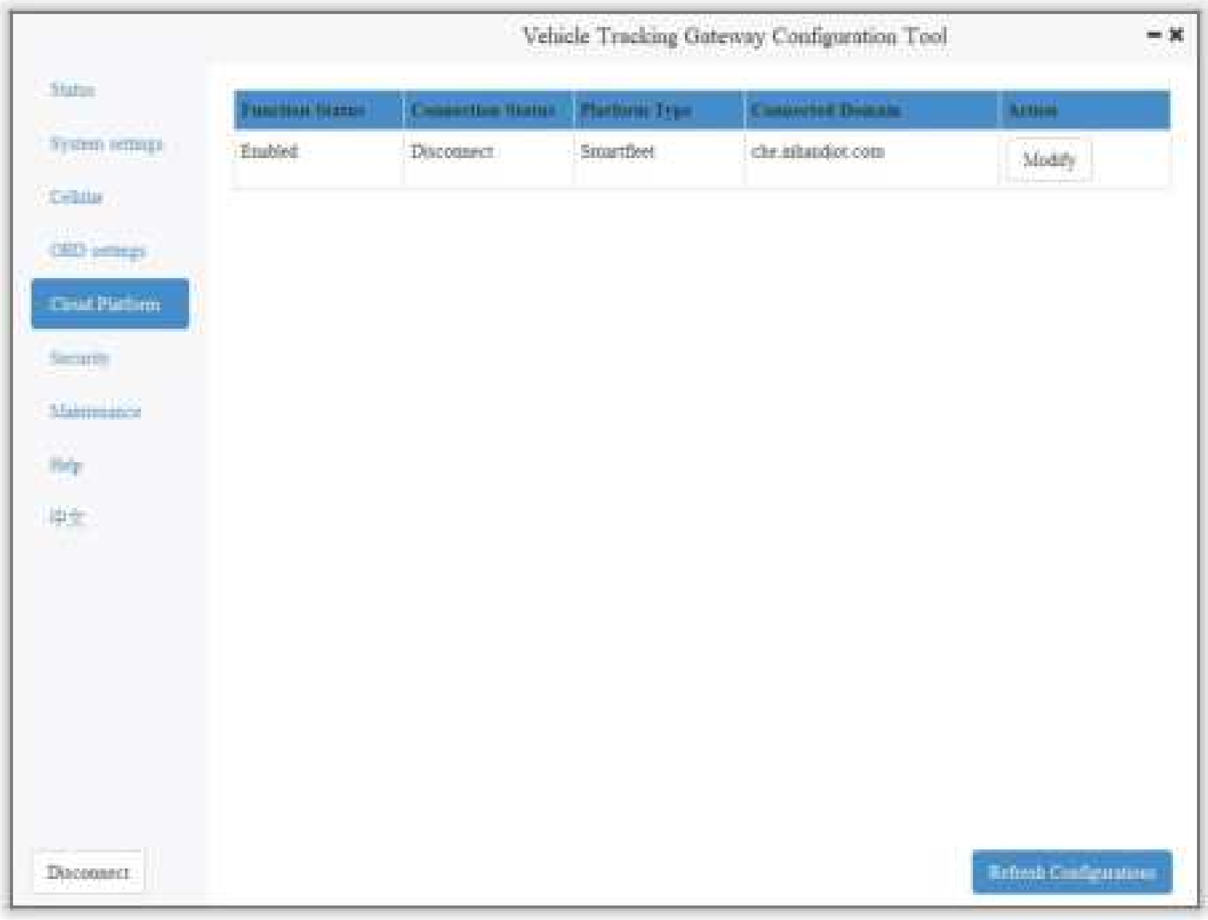
Off Error setting notification

Descriptor Name: ClientCharacteristicConfiguration - Handle: 37 - Value: 00-00

Descriptor Name: CharacteristicUserDescription - Handle: 38 - Value: 52-78

6. Configuration of the Cloud Platform

The configuration of the cloud platform is the North-direction interface and protocol configuration option of the vehicle tracker. The VT310 can only be connected to one cloud platform at a time. The configuration of the platform takes effect only after the device is restarted. Click "Platform" to enter the configuration page. Click "Modify" to enter the configuration page. As is shown below.



Function Status	Connection Status	Platform Type	Connected Domain	Action
Enabled	Disconnect	Smartfleet	che.inhandiot.com	Modify

6.1 SmartFleet Platform

The SmartFleet platform is a SaaS platform for the Internet of Vehicles market launched by InHand Networks. It mainly includes vehicle profile, alarms, driving behavior monitoring, statistical analysis of driving information, electronic fence and other functions. Through the visual user interface and simple operation, you can manage and monitor your hardware devices such as the InVehicle Gateway with speed and ease. Deployment in the cloud allows you to focus on your core business. Login address: https://che.inhandiot.com. For more information about the platform, please visit https://www.inhandnetworks.com and chat with us.

Cloud Platform >> Platform Type: SmartFleet,

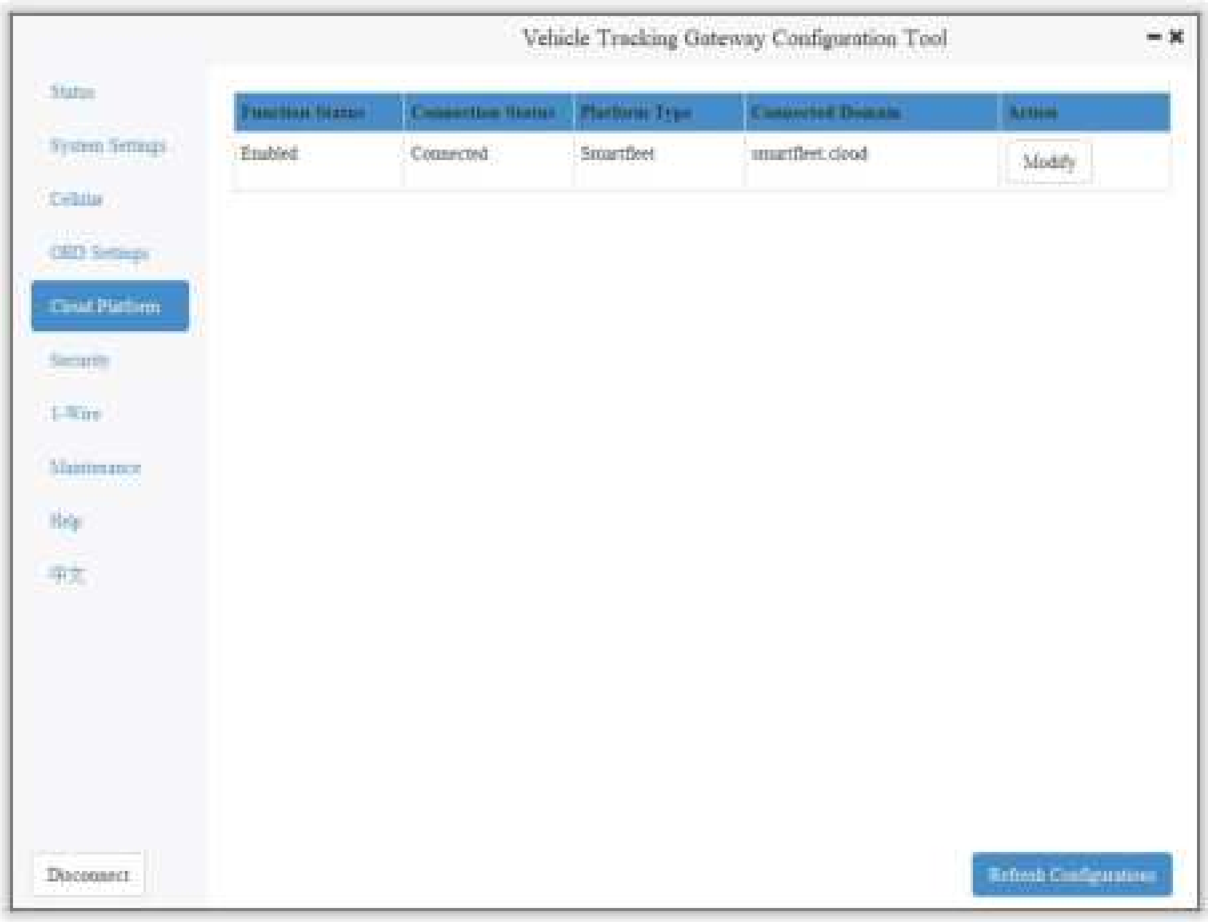
Cloud Platform >> Enable

Cloud Platform >> Domain name: smartfleet.cloud

Cloud Platform >> Account (Enter the platform's registered account)

Cloud Platform >> License Plate Number

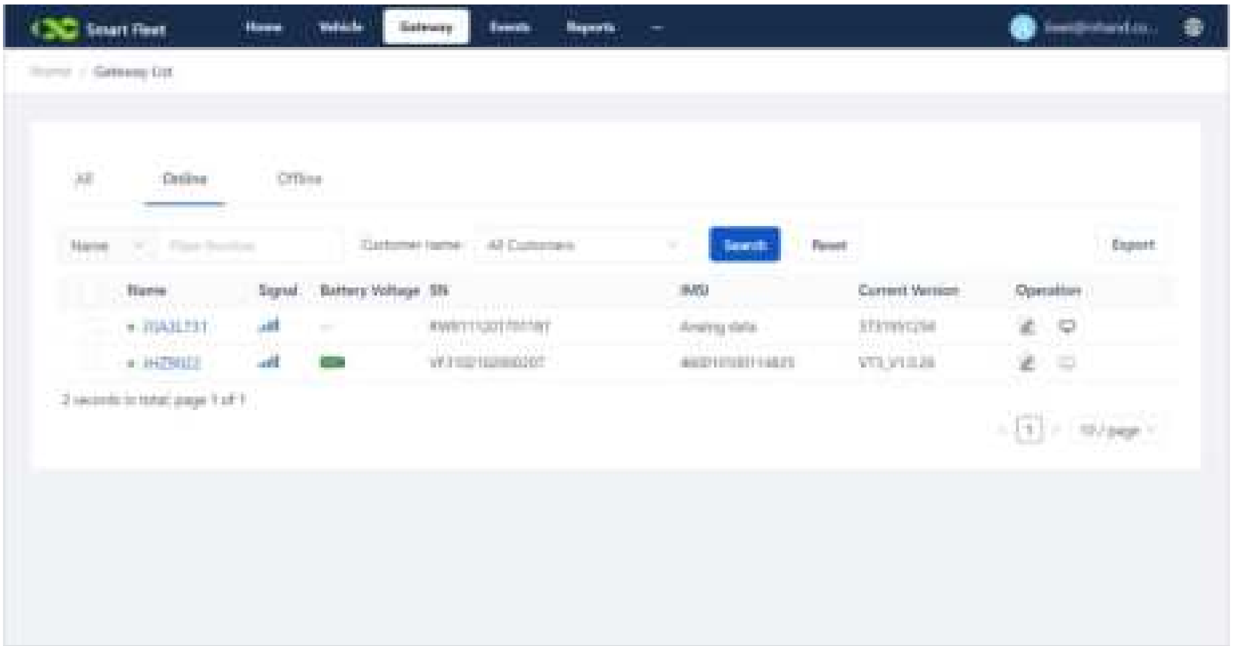
Click "Show Advanced Options" to show hidden configuration items. Configure the LBS reporting interval, traffic reporting interval, and heartbeat reporting interval as needed. The reporting interval is measured in seconds, as is shown below. Click "Save configuration" and restart the device. As is shown below.



Function Status	Connection Status	Platform Type	Connected Domain	Action
Enabled	Connected	Smartfleet	smartfleet.cloud	Modify

On the Cloud Platfrom homepage, view the link status of the platform. The link status is "linked". As is shown below.

Log in the platform and choose Gateways >> Gateway List. You can see if the vehicle tracker is online. As is shown below.



	Name	Signal	Battery Voltage	SN	IMSI	Current Version	Operation
	[illegible]		--	[illegible]	Analog data	[illegible]	
	[illegible]			[illegible]	[illegible]	[illegible]	

2 records in total, page 1 of 1

1 10 / page

6.2 Wialon Platform

Wialon has more than 18 years of best practice in software engineering in the area of GPS vehicle tracking and a team of talented specialists committed to the common goal. The community is united by continuous advancement of the proprietary products and five offices around the world – the headquarters and development center in Minsk and sales offices in Moscow, Boston, Dubai and Buenos Aires. Nowadays solutions by Gurtam take up about 36% of the CIS commercial carrier market and are actively expanding to Europe, the Middle East, the USA, South America, Africa and Australia, with even New Zealand market tapped. For more information, visit https://gurtam.com/en/wialon. To test the Wialon platform, you can contact manager Sun sunzd@inhand.com.cn for more support.

Cloud Platform >> Platform Type: Wialon,

Cloud Platform >> Enable

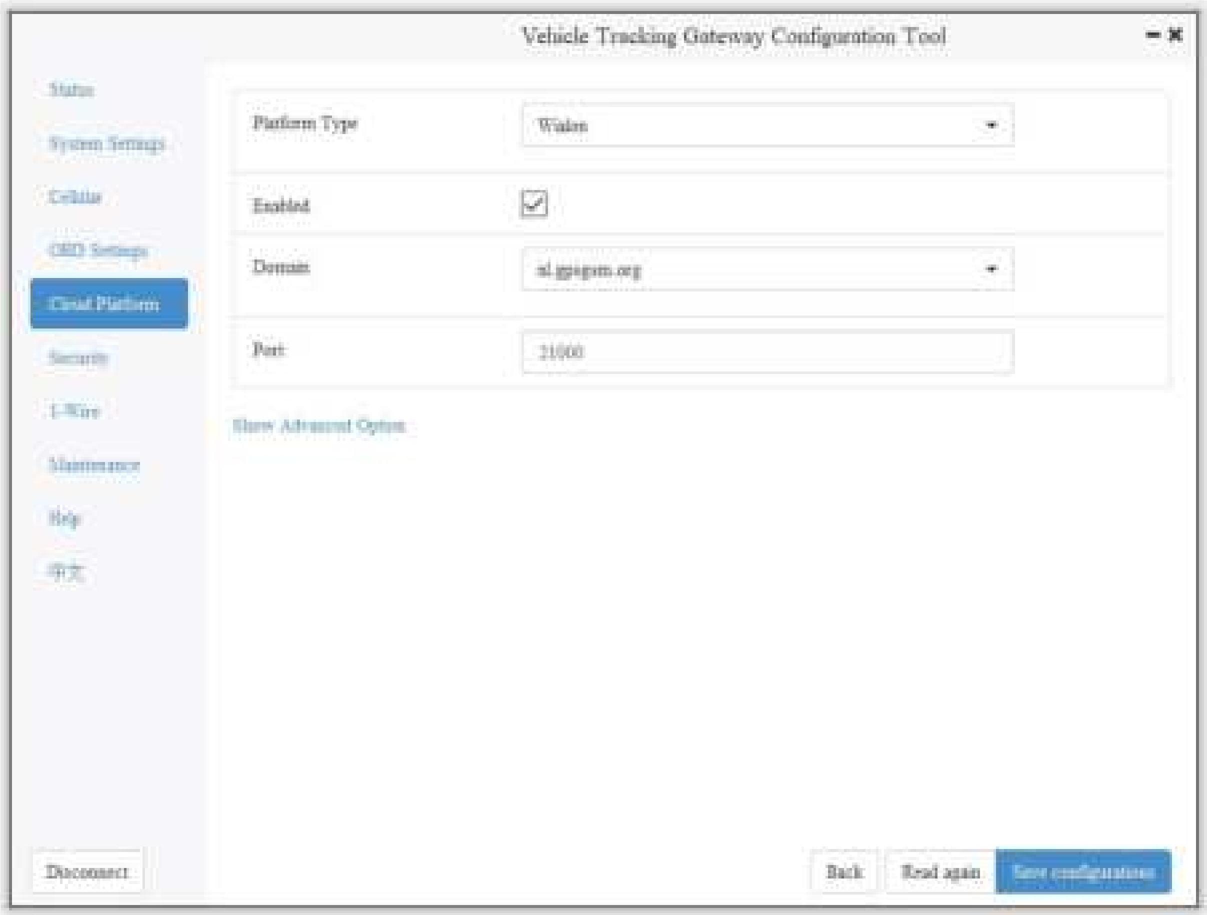
Cloud Platform >> Domain name: nlgpsgsm.rog

Cloud Platform >> Port : 21000

Cloud Platform >> Account （Enter the platform's registered account）

Cloud Platform >> License Plate Number

To adjust the reporting frequency, click "Show Advanced Options" to show hidden configuration items. Set the reporting interval reporting interval in seconds. As is shown in the following.



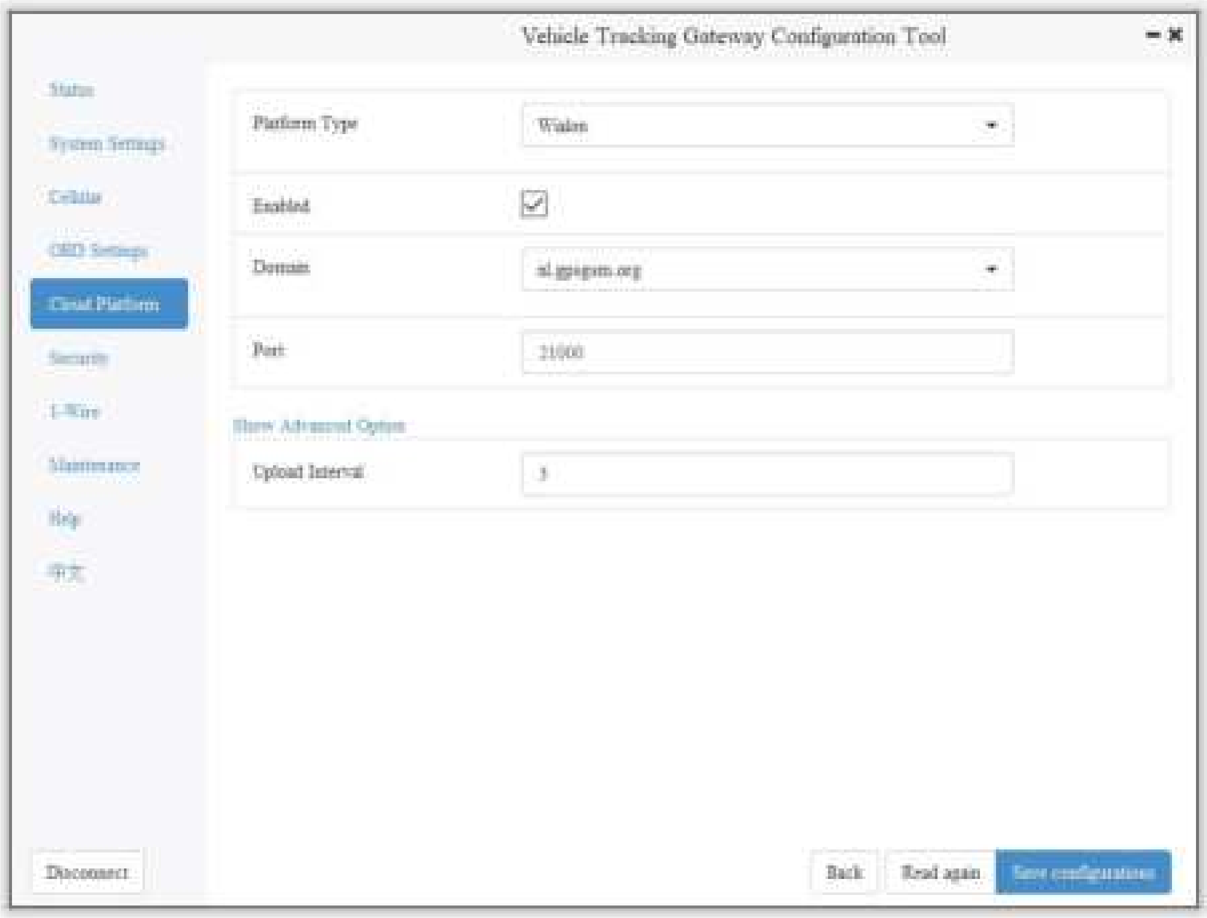
Platform Type: Wialon

Enabled: ☑

Domain: nl.gpsgsm.org

Port: 21000

If you have obtained an independent domain name provided by Wialon, enter the custom domain name and port number. As is shown below.



Vehicle Tracking Gateway Configuration Tool

Platform Type: Wialon

Enabled: ☑

Domain: nl.gpsgsm.org

Port: 21000

Show Advanced Option

Upload Interval: 3

6.2.1 Configuration on Wialon Platform

Platform website: https://hosting.wialon.com

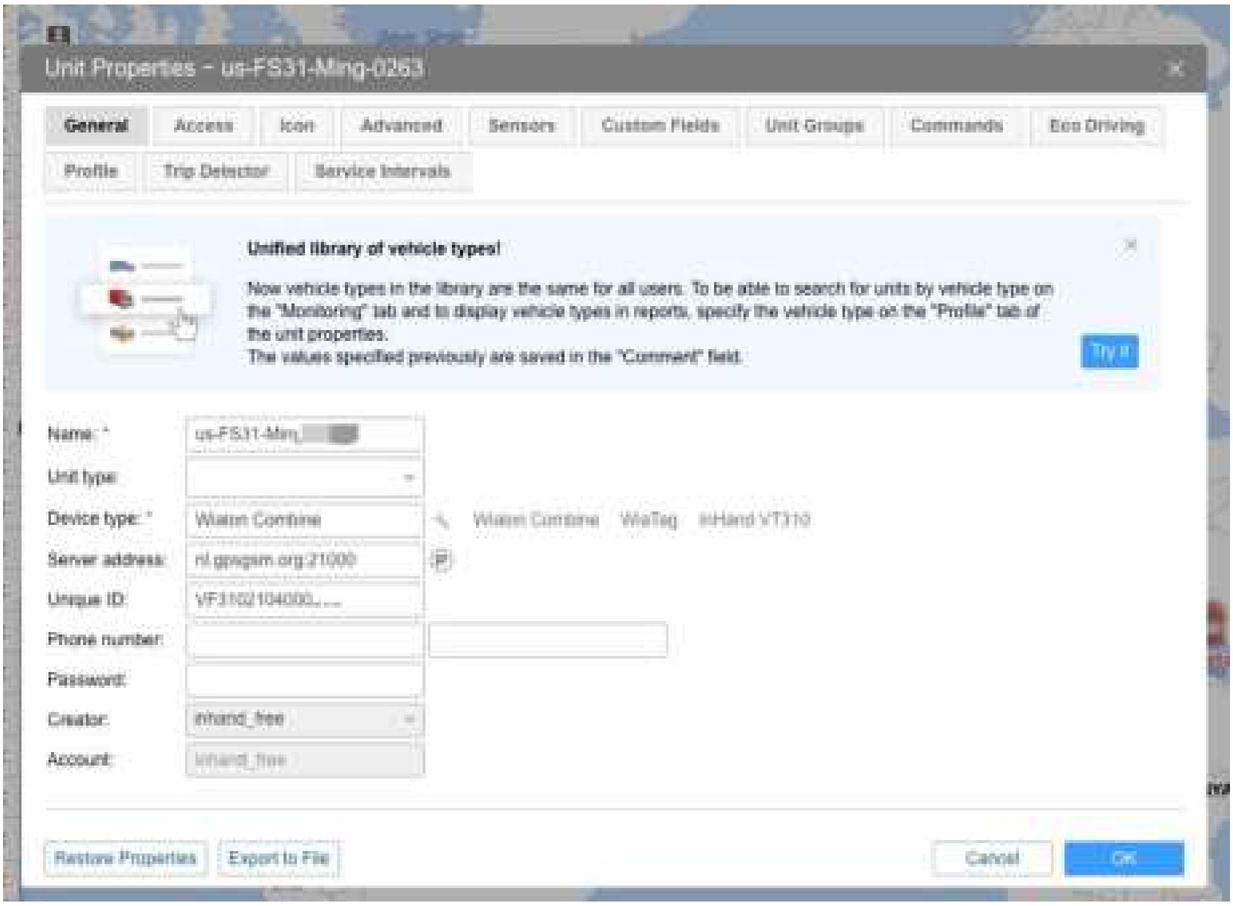
New devices:

The device configuration information is as follows:

- Name: Custom

- Device Type: Select "Wialon Combine"

- Special ID: Enter the device-specific serial number. View the serial number of the device or the serial number on the status page of the configuration tool. The information shown in the following figure is for example only.



Unified library of vehicle types!

Now vehicle types in the library are the same for all users. To be able to search for units by vehicle type on the "Monitoring" tab and to display vehicle types in reports, specify the vehicle type on the "Profile" tab of the unit properties.
The values specified previously are saved in the "Comment" field.

Name: *	us-FS31-Min[redacted]
Unit type:	
Device type: *	Wialon Combine — Wialon Combine WiaTag InHand VT310
Server address:	nl.gpsgsm.org:21000
Unique ID:	VF3102104000....
Phone number:	
Password:	
Creator:	inhand_free
Account:	inhand_free

6.2.2 View Data Uploaded by Devices

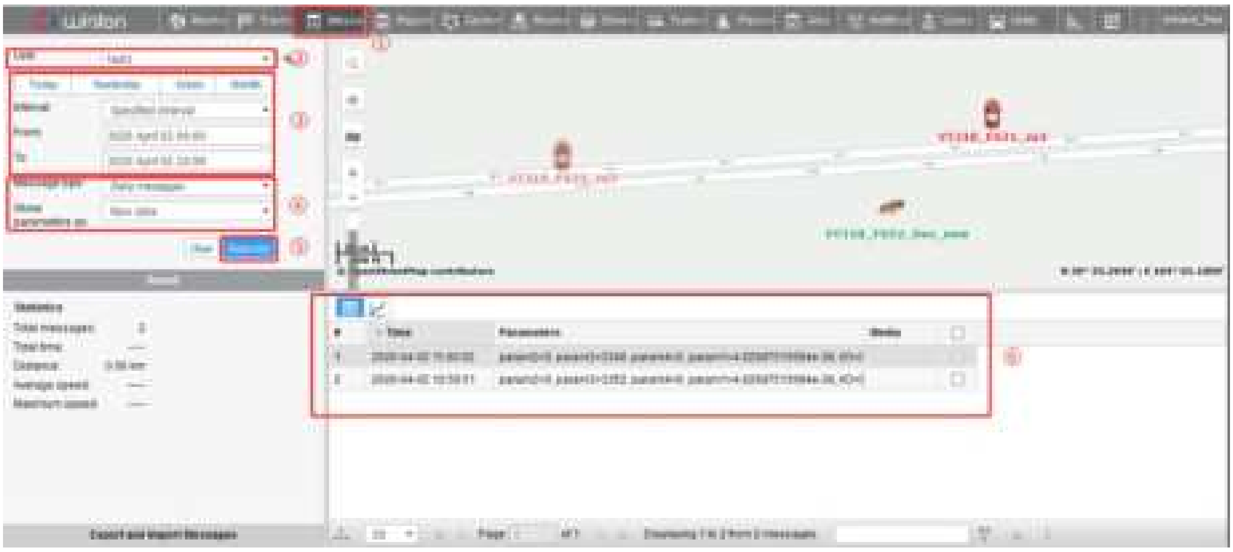
① Select "Message"

② Select the name of the target device to be viewed

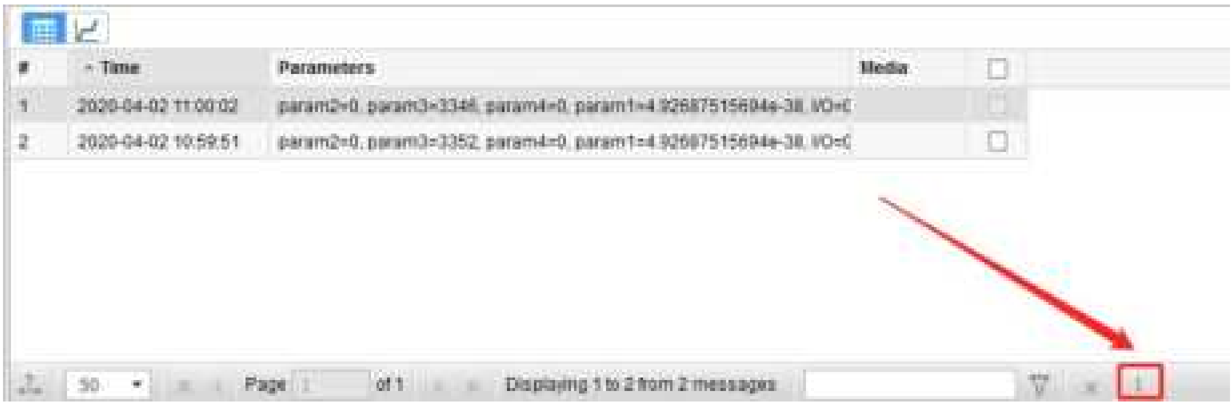
③ Select the time range of interest

④ Select the data type. Currently the colelcted I/O data is viewed through Raw Data

⑤ Click the "Execute" button to view the information of the target device at the position of ⑥, as is shown below.



Note: The information display of the target device can be selected by clicking the configuration method, as is shown below.



#	Time	Parameters	Media	□
1	2020-04-02 11:00:02	param2=0, param3=3346, param4=0, param1=4.92687515694e-38, I/O=(		□
2	2020-04-02 10:59:51	param2=0, param3=3352, param4=0, param1=4.92687515694e-38, I/O=(		□

50 Page 1 of 1 Displaying 1 to 2 from 2 messages

6.3 Azure IoT Hub

Azure IoT builds IoT applications that offer highly secure and reliable two-way communication between IoT applications and their managed devices. Azure IoT Center provides the back end of cloud hosting solutions, which can connect to almost any device. The solution is extended from the cloud to the edge through authentication, built-in device management, and extended configuration of each device. For more information, visit https://azure.microsoft.com/zh-cn/services/iot-hub

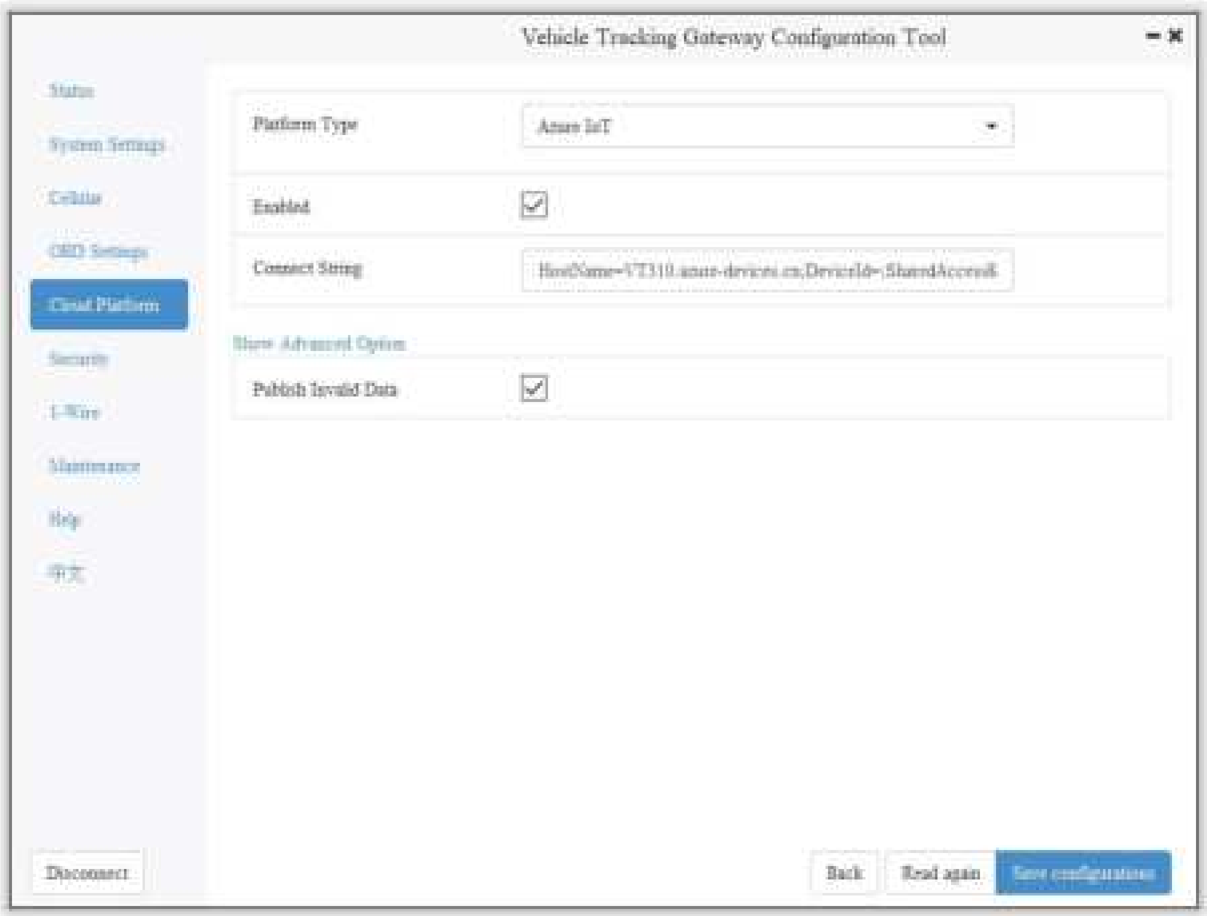
Cloud Platform >> Platform Type: Azure IoT

Cloud Platform >> Enable

Cloud Platform >> Connect String

The Connect String is created from Microsoft IoT platform. See in the next section.

To see invalid data, click "Show Advanced Options" to view hidden configuration items. Tick "Show Invalid Data", as is shown below.



Platform Type: Azure IoT

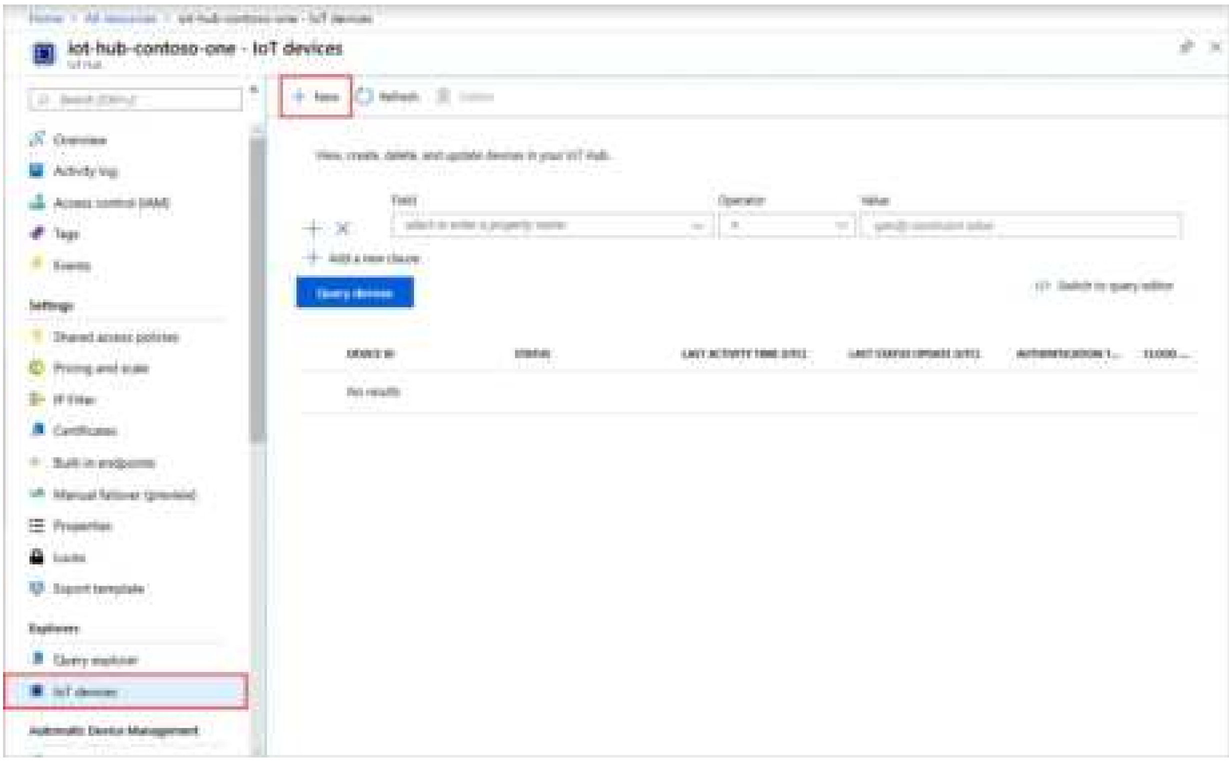
Enabled: ☑

Connect String: HostName=VT310.azure-devices.cn;DeviceId=;SharedAccessK

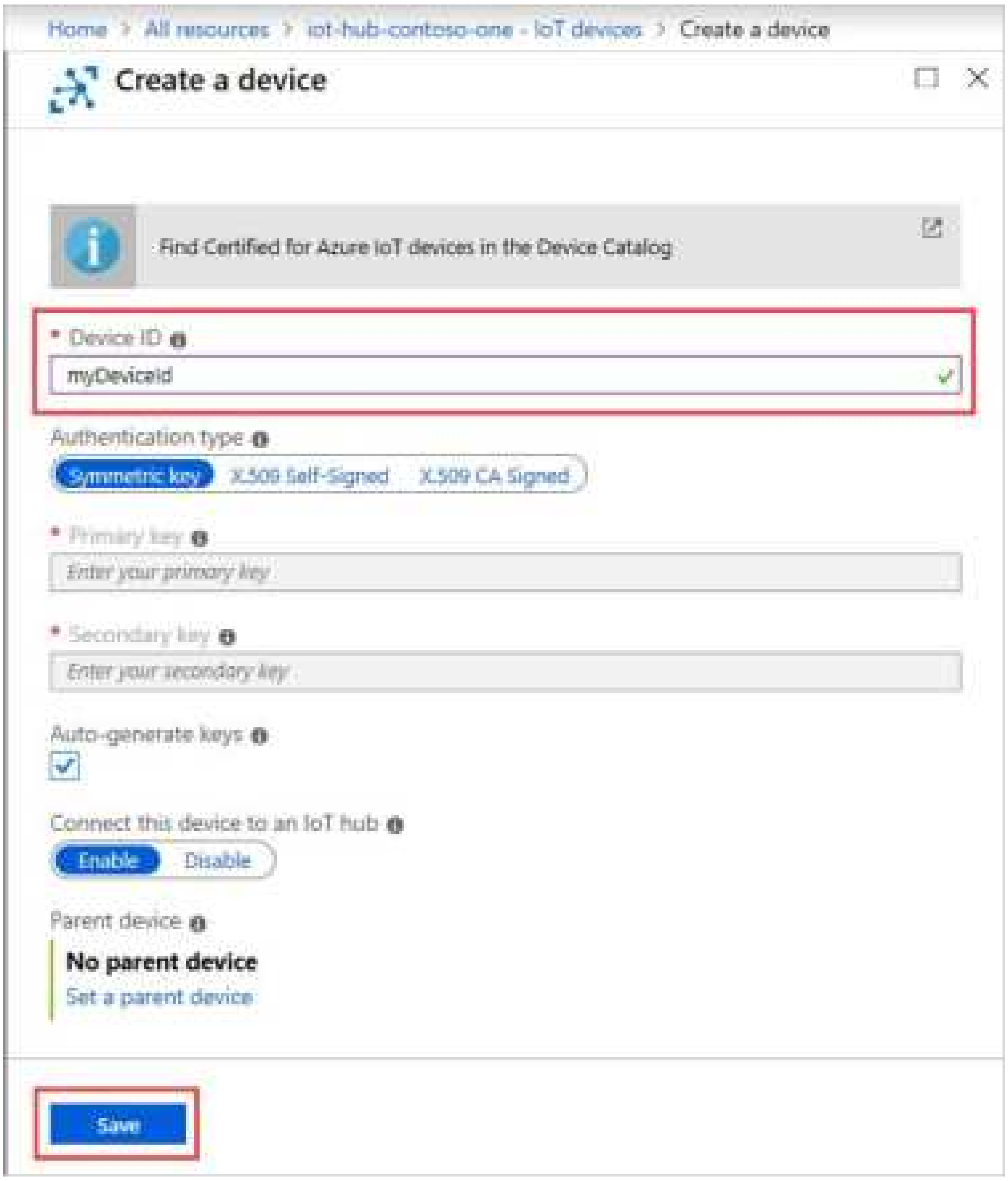
Publish Invalid Data: ☑

6.3.1 Configure Azure IoT Platform

1. Before configuring the Connect String, log in the Azure IoT platform to create a device. In the left-side navigation pane of the IoT Center, choose "IoT devices", and then select "New". As is shown below.



1. On the "Create a device" page, provide the name of the new device, such as myDeviceId, and then select "Save". This creates a device identifier for IoT Center. As is shown below.



Home > All resources > iot-hub-contoso-one - IoT devices > Create a device

Create a device

Find Certified for Azure IoT devices in the Device Catalog

* Device ID: myDeviceId

Authentication type: ● Symmetric key ○ X.509 Self-Signed ○ X.509 CA Signed

* Primary key: Enter your primary key

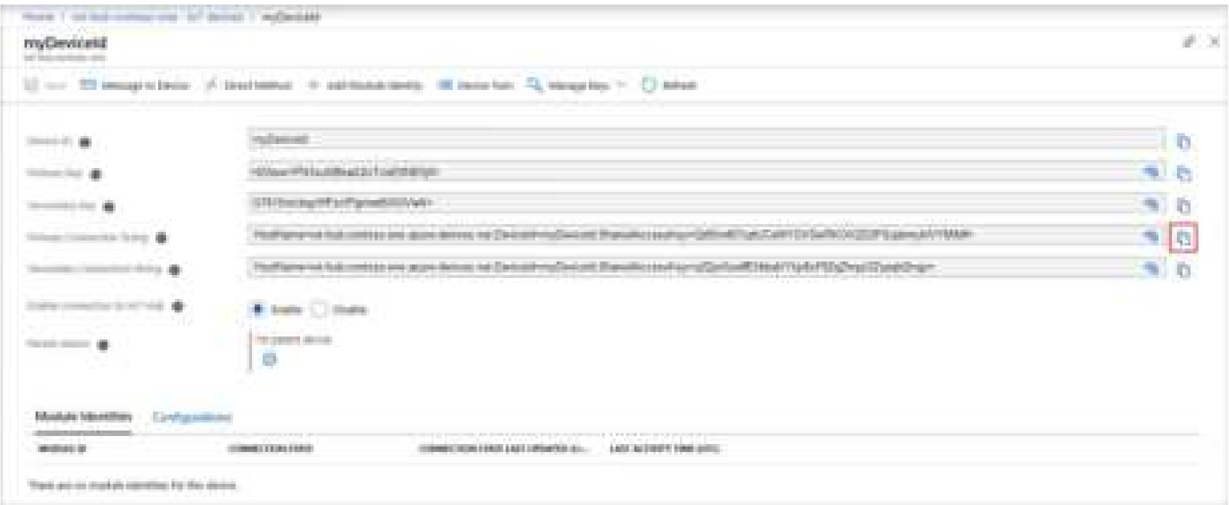
* Secondary key: Enter your secondary key

Auto-generate keys: ☑

Connect this device to an IoT hub: ● Enable ○ Disable

Parent device: No parent device

1. After creating the device, open the device in the "IoT devices" pane. Copy the "Primary Connection String" and later paste to the "Connection String" of the configuration tool ". As is shown below.



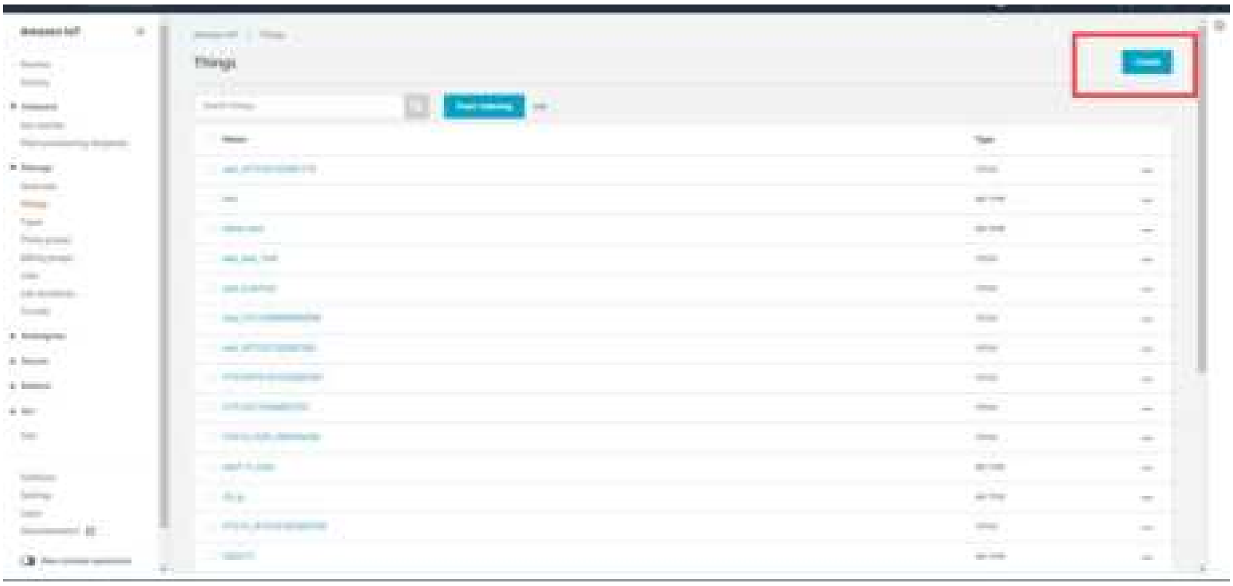
6.4 AWS IoT Platform

With the AWS IoT Core, you can connect your IoT devices to the AWS cloud without configuring or managing the server. The AWS IoT Core supports billions of devices and trillions of messages, and can process those messages before routing them to AWS terminal nodes and other devices with security and reliability. With the AWS IoT Core, your applications can track all devices and communicate with them anytime, even if those devices are not connected. Build your IoT applications with AWS services, so that you can collect, process and analyze data generated by connected devices and take action without managing any infrastructure. For more information, please visit https://aws.amazon.com/iot-core/.

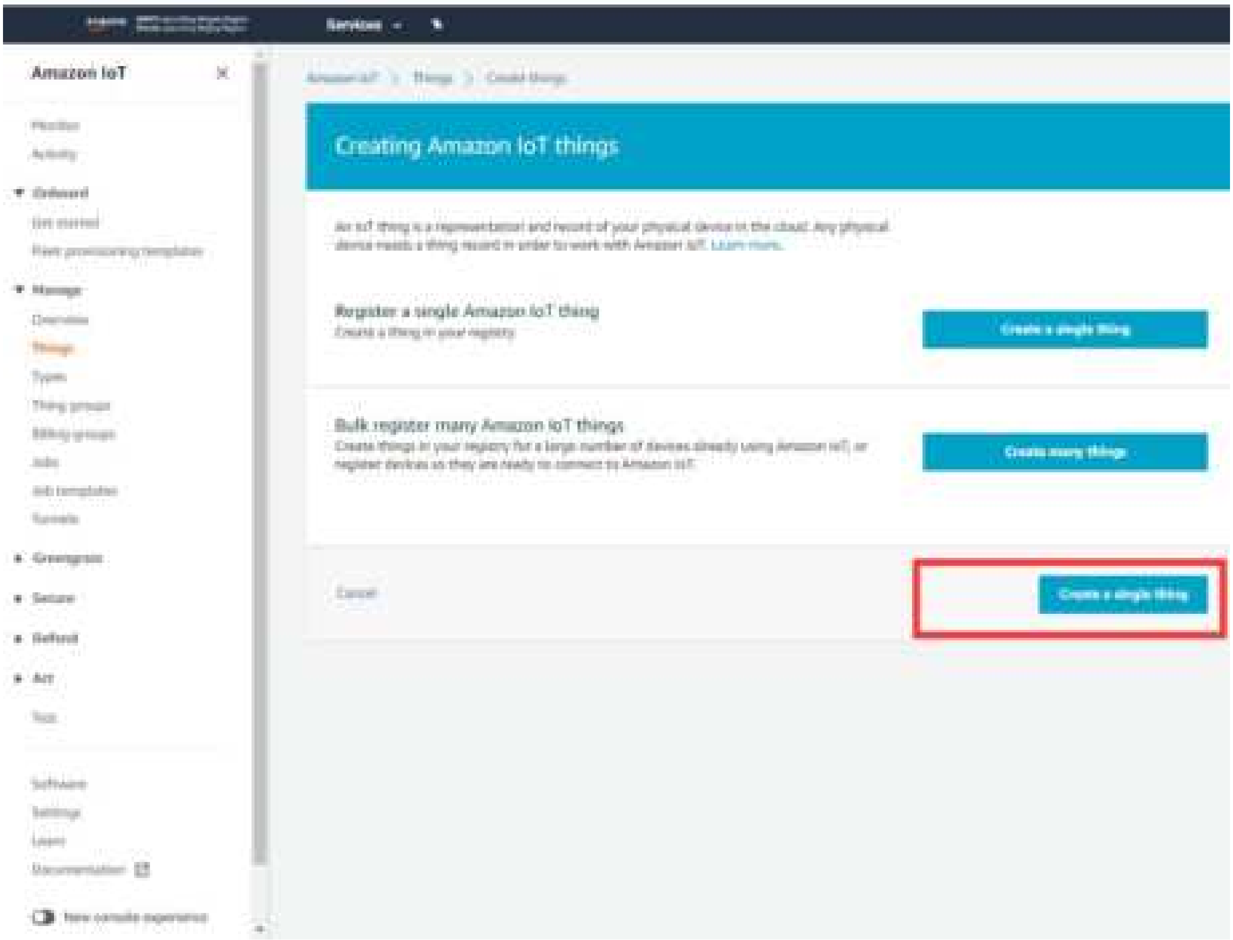
6.4.1 Configure AWS IoT Platform

Method 1: Creat A Thing for link

1. Go to the Amazon IoT console >> Things page, and click "Create", as is shown below.



Amazon IoT >> Things >> Create a single thing



Creating Amazon IoT things

An IoT thing is a representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with Amazon IoT. Learn more.

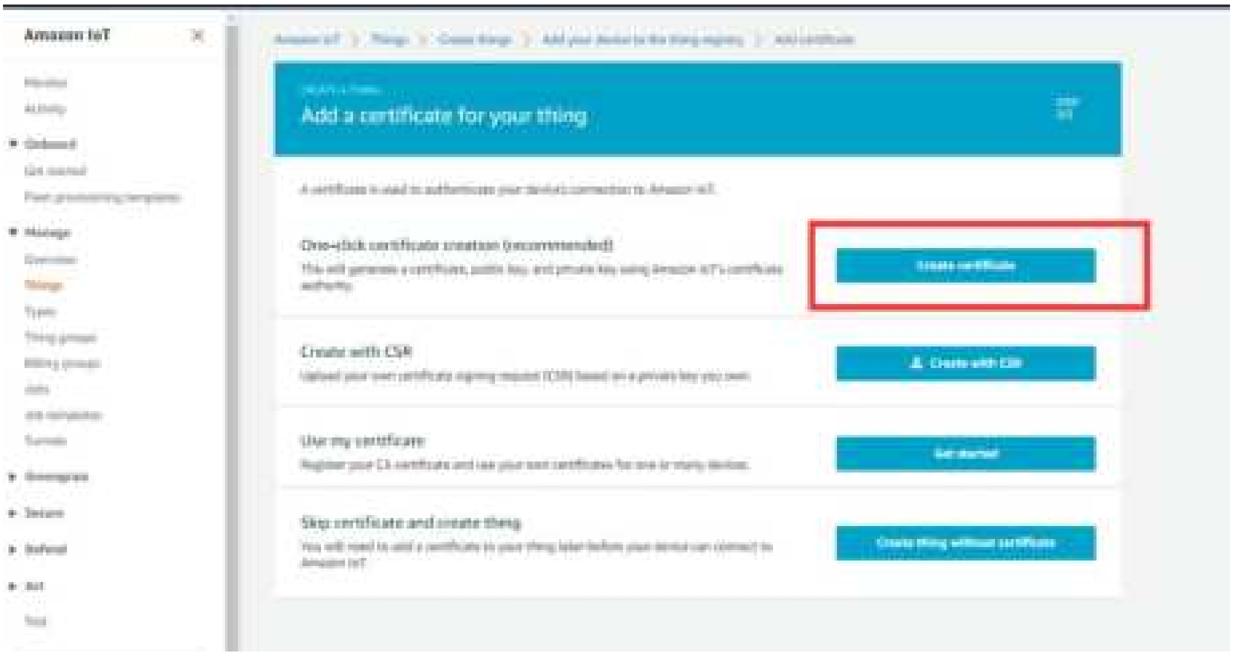
Register a single Amazon IoT thing

Create a thing in your registry

Bulk register many Amazon IoT things

Create things in your registry for a large number of devices already using Amazon IoT, or register devices as they are ready to connect to Amazon IoT.

Amazon IoT >> Things >> Create a single thing >> Add your device to the thing registry >> Add certificate On this page, create a certificate for the thing just created, as is shown below.



Add a certificate for your thing

A certificate is used to authenticate your device's connection to Amazon IoT.

One-click certificate creation (recommended)
This will generate a certificate, public key, and private key using Amazon IoT's certificate authority.

Create with CSR
Upload your own certificate signing request (CSR) based on a private key you own.

Use my certificate
Register your CA certificate and use your own certificates for one or many devices.

Skip certificate and create thing
You will need to add a certificate to your thing later before your device can connect to Amazon IoT.

1. Download certificate file

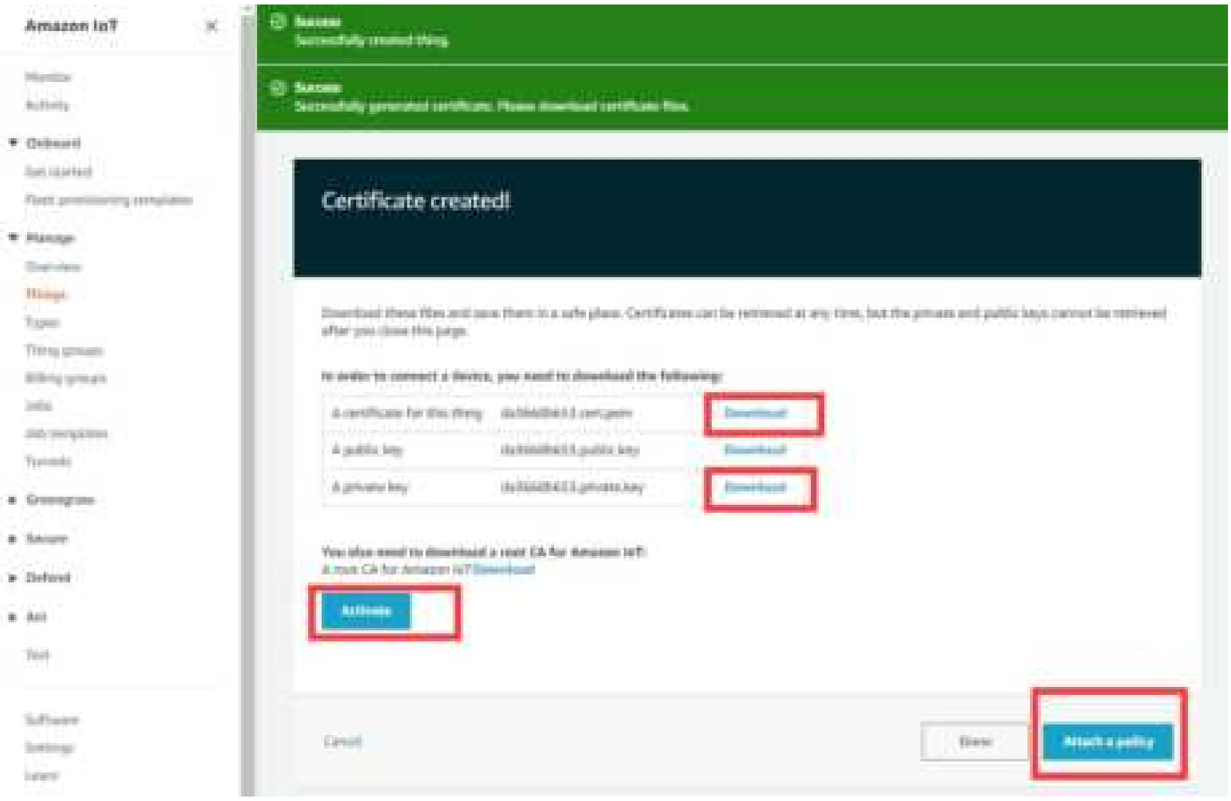
- Download certificate >> A certificate for the things >> Download the file format is as follows: ***.cert.pem;

- Download private >> A private key >> Download. The file format is: ***.private.key;

- AWS CA files have been download in the vehicle tracker, so you do not need to Download CA files. If you need to update, click "A root CA for Amazon IoT Download";

- Click "Activate" to activate the certificate of the thing;

- Click the "Attache a policy", enter additional policy page. As shown in the following illustration.


Success
Successfully created thing.

Success
Successfully generated certificate. Please download certificate files.

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:

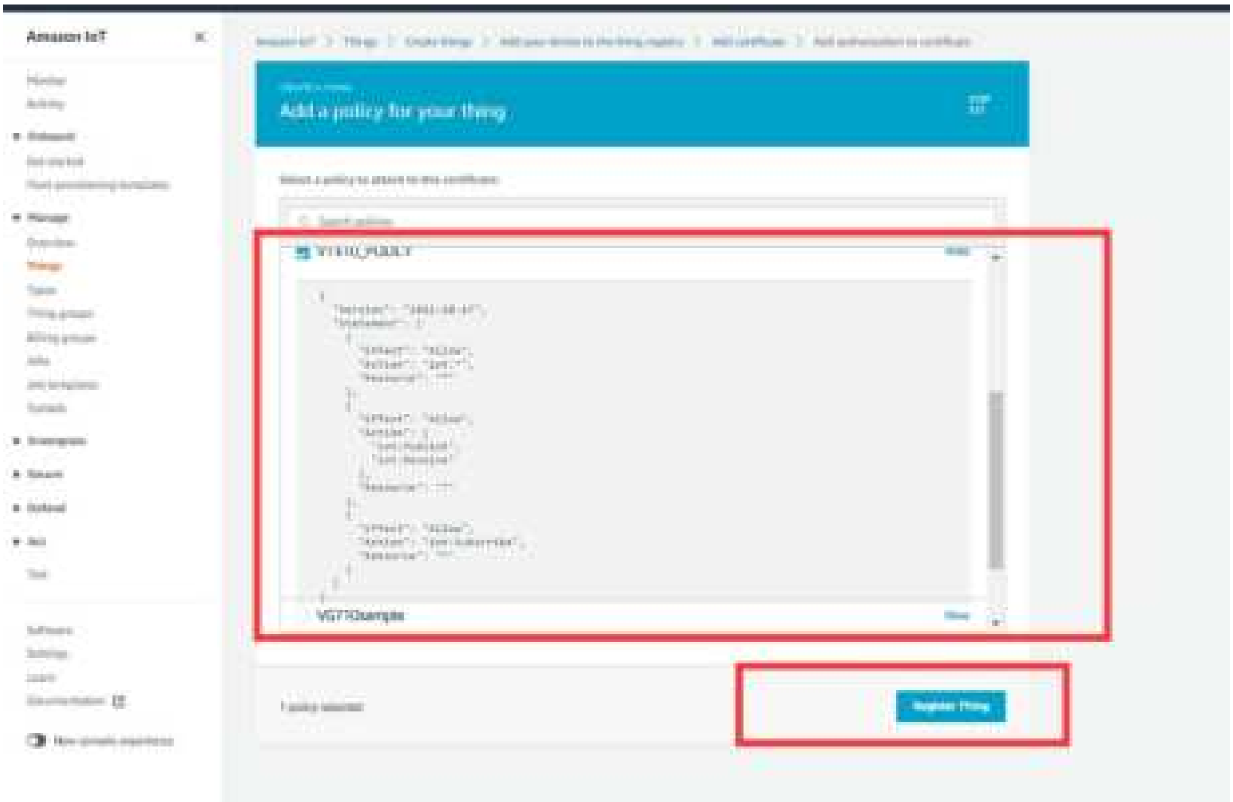
A certificate for this thing	[illegible].cert.pem	Download
A public key	[illegible].public.key	Download
A private key	[illegible].private.key	Download

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

Activate

Cancel   Done   Attach a policy

- On the "Attach a policy" page, config additional policy for the certificate and click "Register Thing" to register the item, as is shown below.


AWS IoT > Things > Create things > Add your device to the thing registry > Add certificate > Add authorization to certificate

Create a thing
Add a policy for your thing

Select a policy to attach to this certificate:

Search policies

VT410_POLICY   View

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Receive"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "*"
    }
  ]
}
```

VG710Example   View

1 policy selected   Register Thing

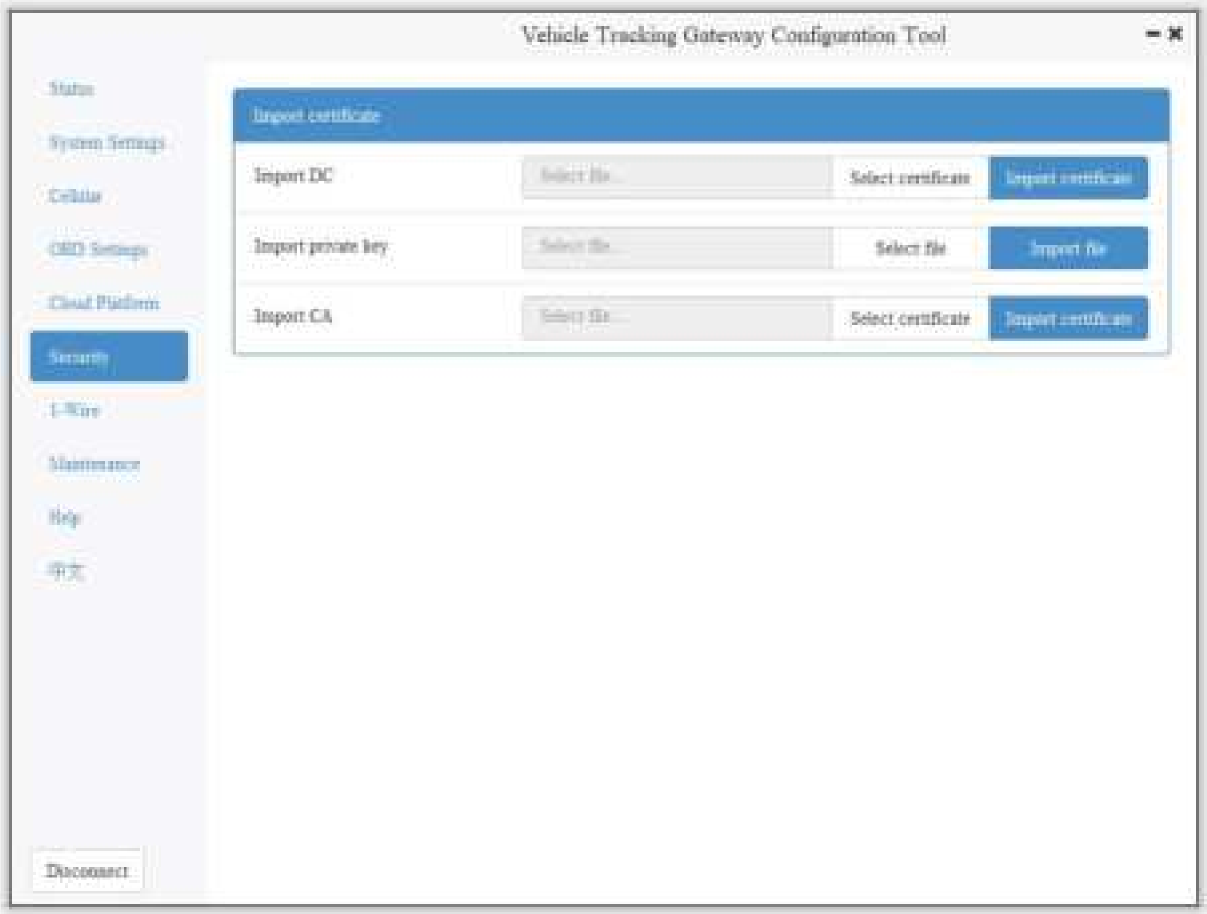
-

1. Use the configuration tool to import the certificate file to the tracker

- Security >> Import digital certificate >> Select a certificate (select the downloaded digital certificate ***.cert.pem in the displayed dialog box); click "Import certificate"

- Security>> Import private key certificate >> Select a file (select the downloaded digital certificate ***. private.key in the dialog box that appears); click "Import file";

- As the AWS CA files have been built into the vehicle tracker, there is no need to download them. If you need to update them, go to Security >> Import CA certificate >> Select a file (select the downloaded digital certificate ***. private.key in the dialog box that appears); click import certificate, as is shown below.



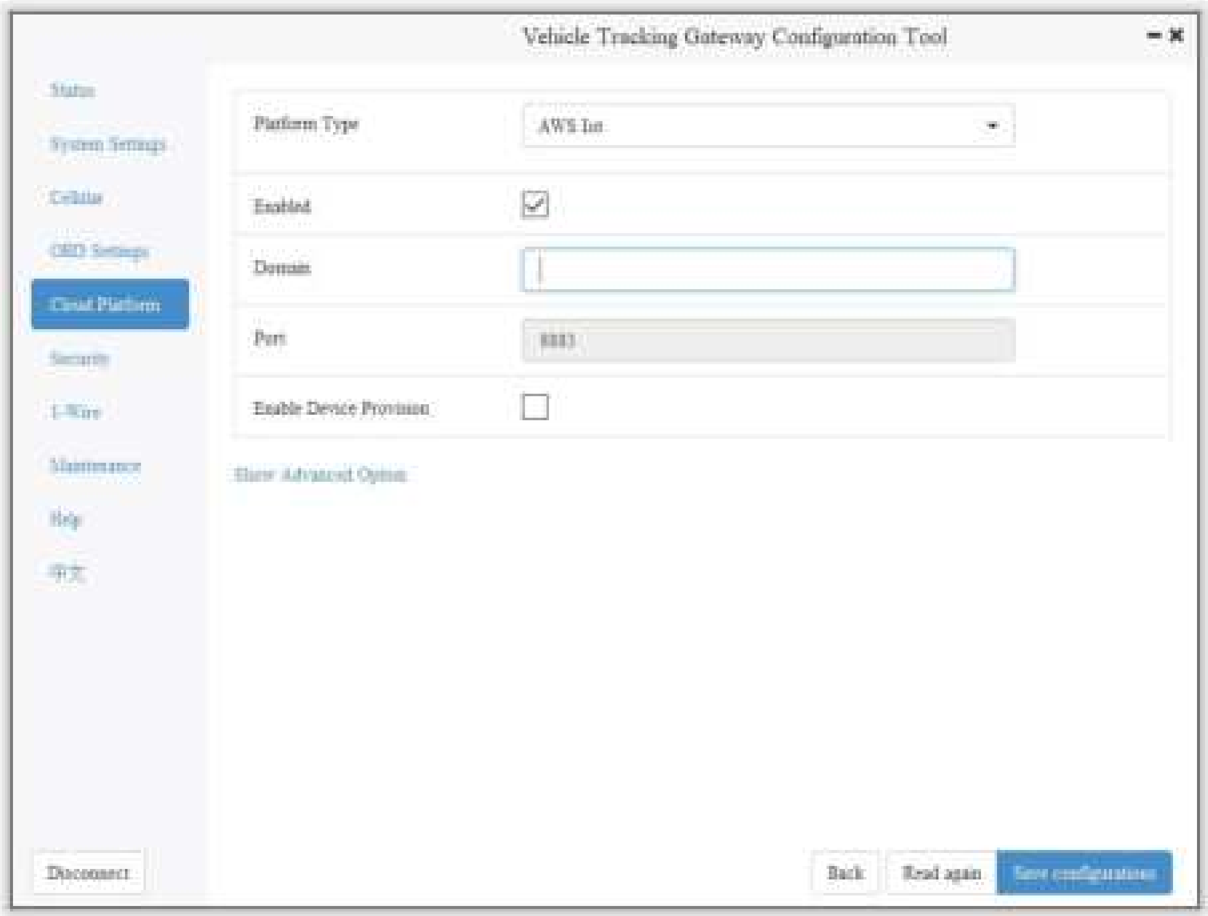
1. Enable AWS Platform

Cloud Platform >> Platform Type: AWS IoT

Cloud Platform >> Enable

Cloud Platform >> Domain name

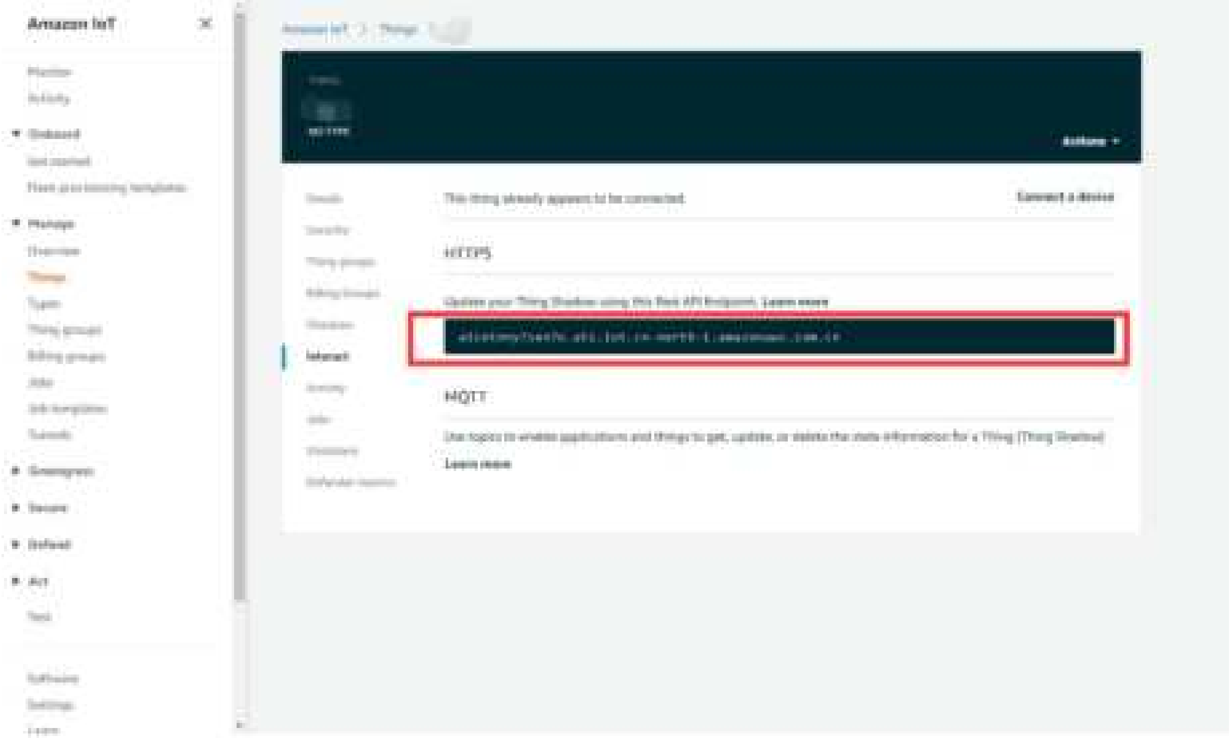
Cloud Platform >> Port: 8883



Vehicle Tracking Gateway Configuration Tool

Platform Type	AWS Iot
Enabled	☑
Domain	
Port	8883
Enable Device Provision	☐

“Cloud Platform >> Domain name” AWS IoT >> Things >> “Select the created things” >> Interact Copy this domain name paste to “Cloud Platform >> Domain name”



This thing already appears to be connected.

HTTPS

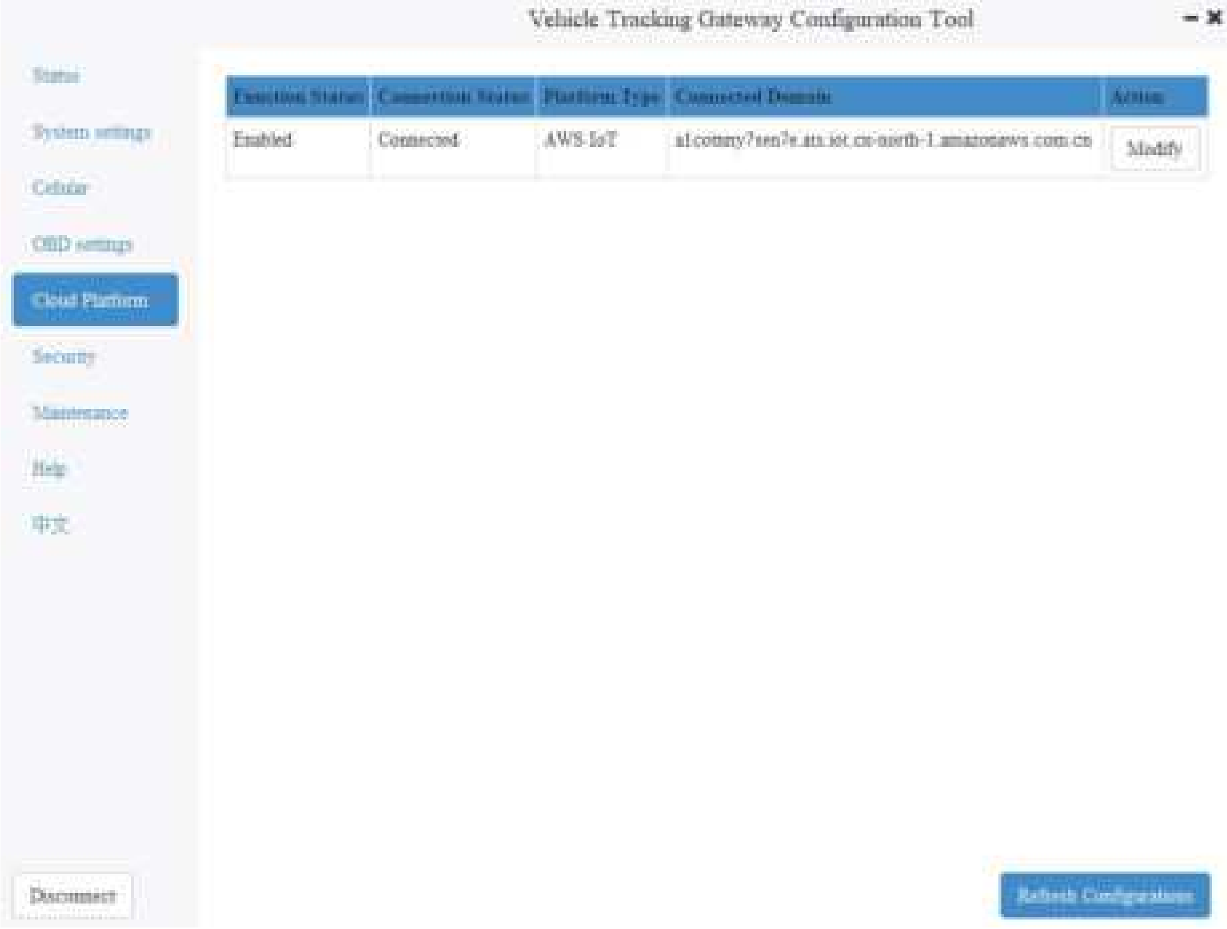
Update your Thing Shadow using this Rest API Endpoint. Learn more

[illegible]

MQTT

Use topics to enable applications and things to get, update, or delete the state information for a Thing (Thing Shadow)

Save the configuration and restart the device. On the Cloud Plateform Cloud Platform page, check the connection status:

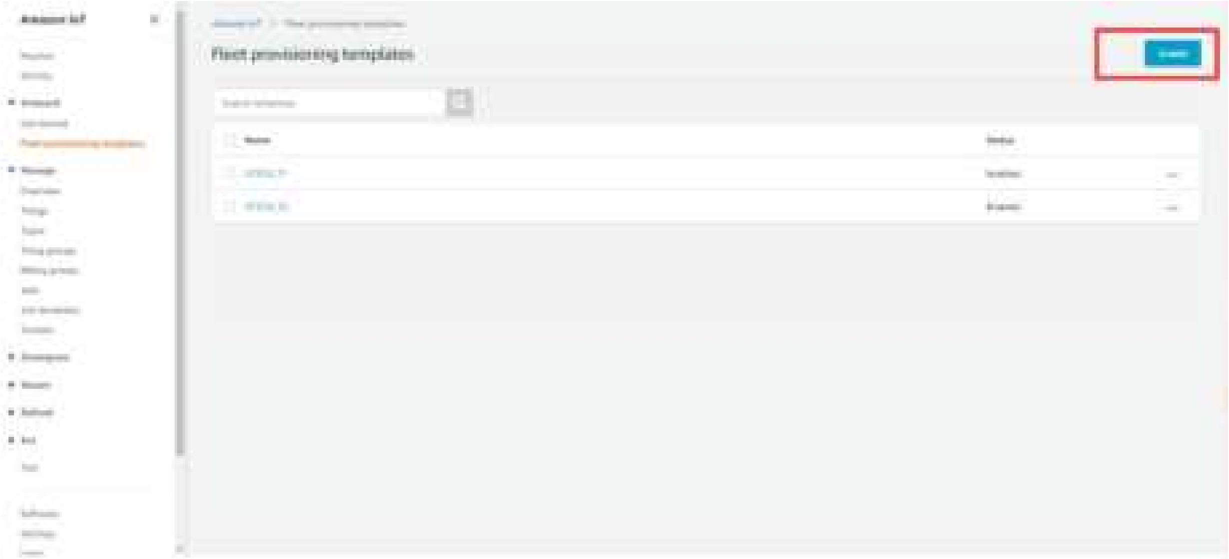


Function Status	Connection Status	Platform Type	Connected Domain	Action
Enabled	Connected	AWS-IoT	a1cotmny7sen7e.ats.iot.cn-north-1.amazonaws.com.cn	Modify

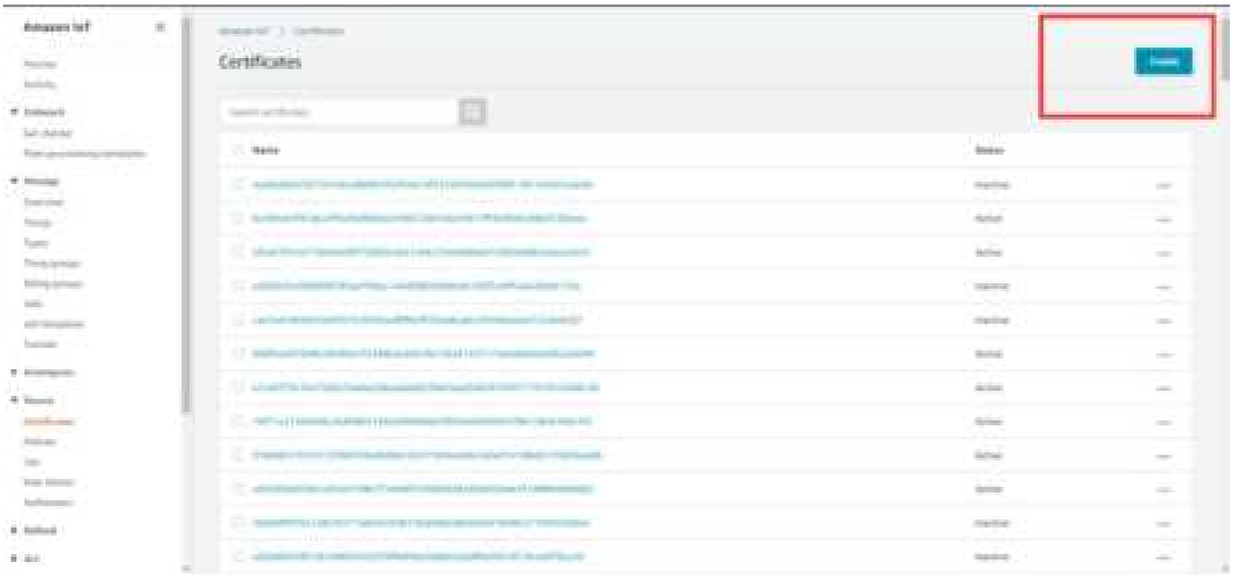
By default, invalid data is not reported. To report invalid data, tick "Report invalid data" in the advanced options. After that, the reported data value that does not exist is NULL, as is shown below.

Method 2: Create a provisioning template connection for AWS

1. Create a prefabricated templet: Amazon IoT >> Fleet provisioning templates >> Create, as is shown below.

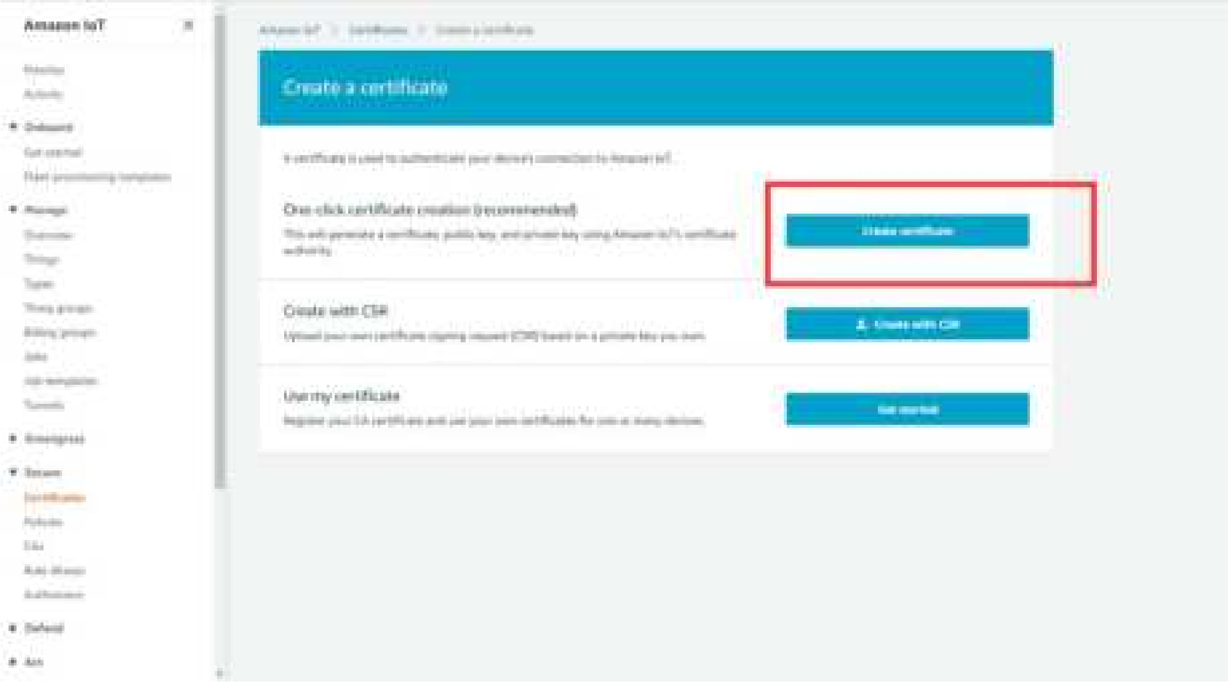


Creat Certificate: Amazon IoT >> Certificates



Amazon IoT >> Things >> Create a single things >> Add your device to the thing registry >> Add certificate

On this page, create a certificate for the thing just created, as is shown below.



Create a certificate

A certificate is used to authenticate your device's connection to Amazon IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using Amazon IoT's certificate authority.

Create with CSR

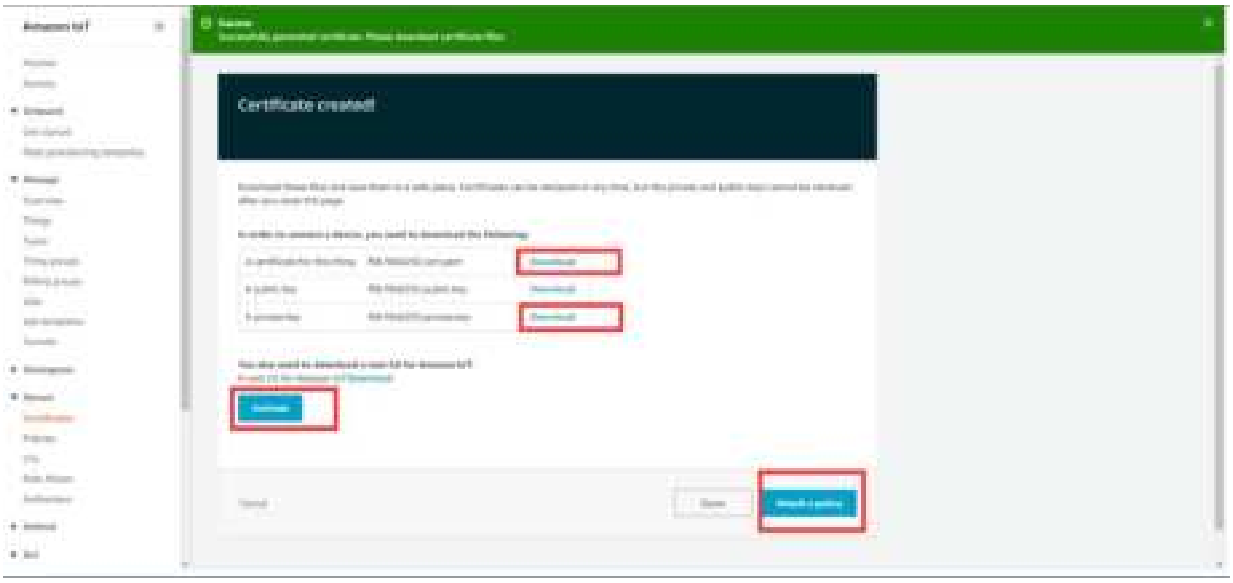
Upload your own certificate signing request (CSR) based on a private key you own.

Use my certificate

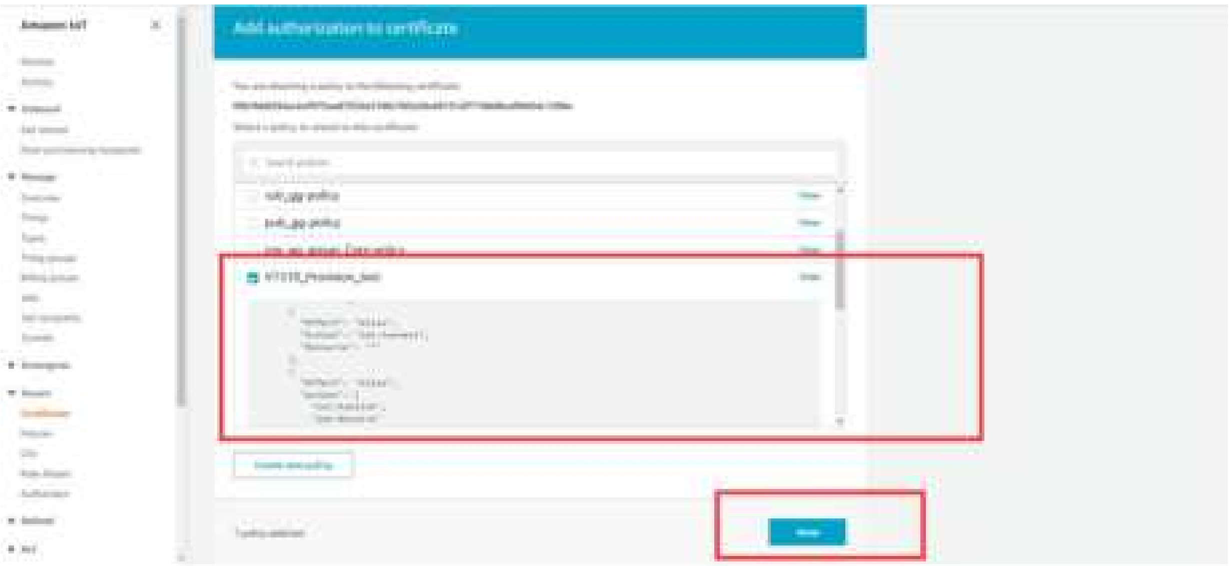
Register your CA certificate and use your own certificates for one or many devices.

1. Download a certificate file

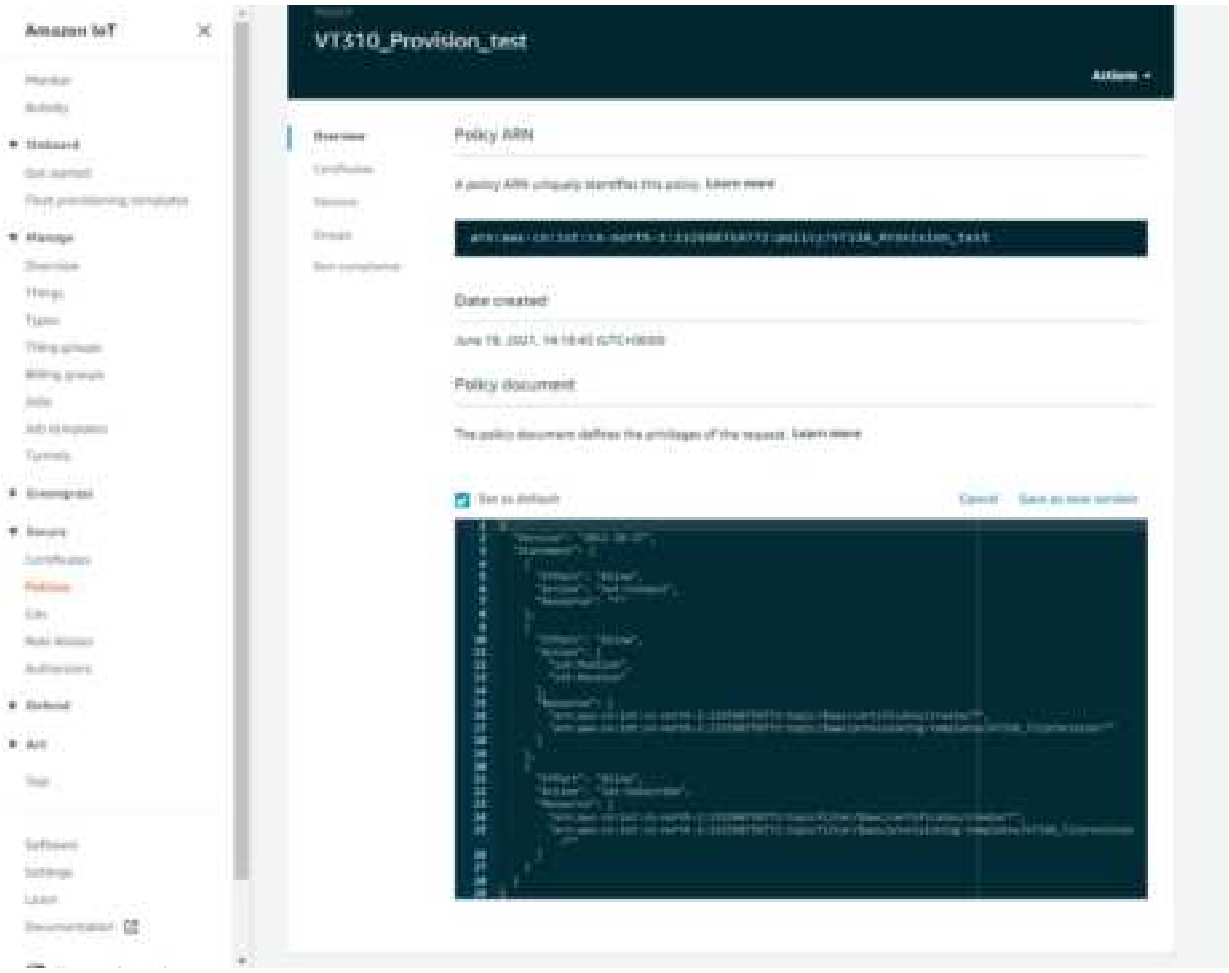
- Download a public key file >> A certificate for the things >> Download. The file format is ***.cert.pem;
- Download the private key file >> A private key >> Download. The file format is ***.private.key;
- As the AWS CA files have been built into the tracker, there is no need to download them. If you need to update, click“A root CA for Amazon IoT Download”;
- Click Activate to activate the certificate;
- Click the "Attach a policy", enter additional policy page, as is shown below.



- On the previous window, click "Activate" to enter the certificate list. Click "Done" and complete certification.



- On the previous window, click "Attach a policy" to enter the Amazon IoT >> Policy list to add a policy, as is shown below.

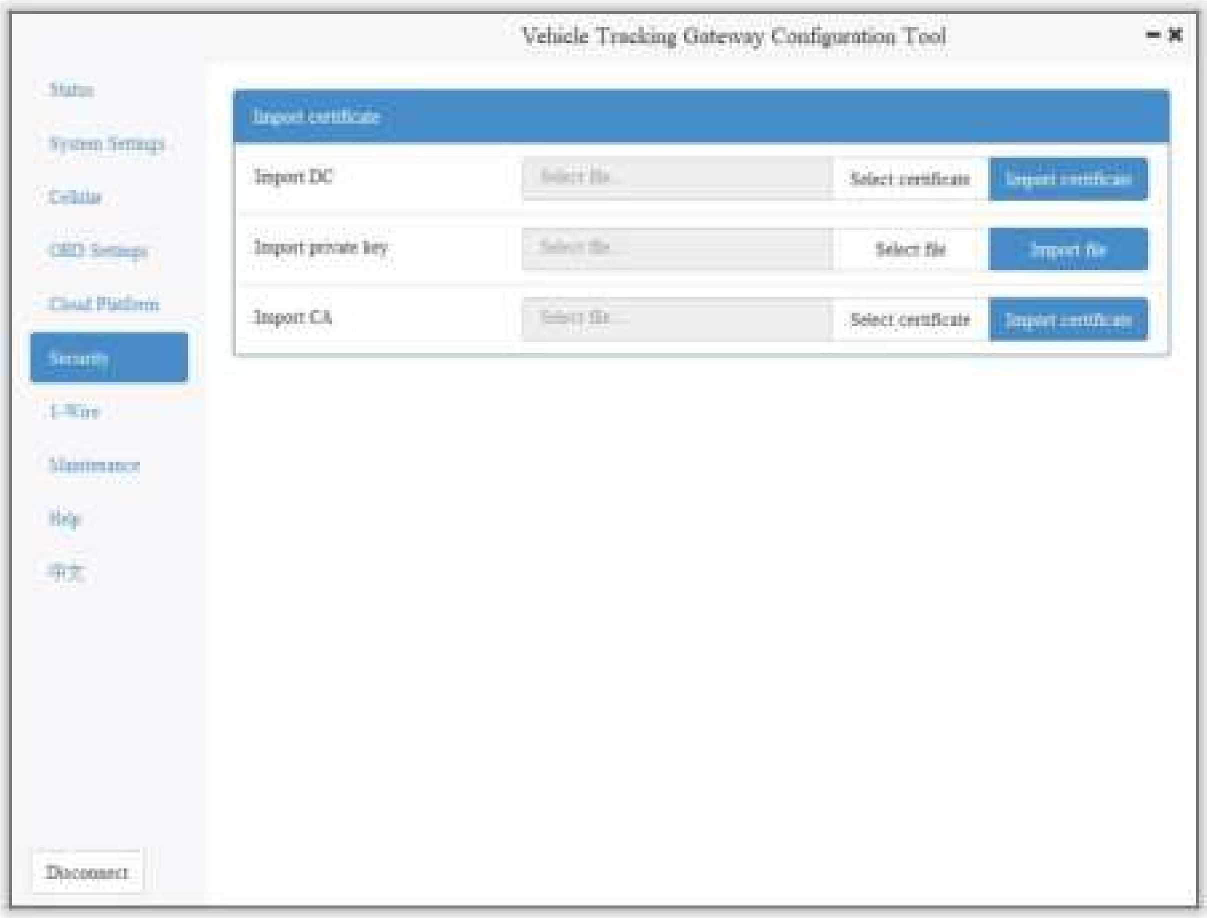


1. Use the configuration tool to import the certificate file to the vehicle tracker

- Security >> Import digital certificate >> Select a certificate (select the downloaded digital certificate ***.cert.pem in the displayed dialog box), click "Import certificate"

- Security >> Import private key certificate >> Select a file (select the downloaded digital certificate \\. private.key in the dialog box that appears); click "Import file";

- As the tracker already has a built-in AWS CA file, the CA file is not required. If you need to update the CA file, go to Security >> Import CA certificate >> Select a file (select the downloaded digital certificate ***.cert in the pop-up dialog box), click "Import certificate";



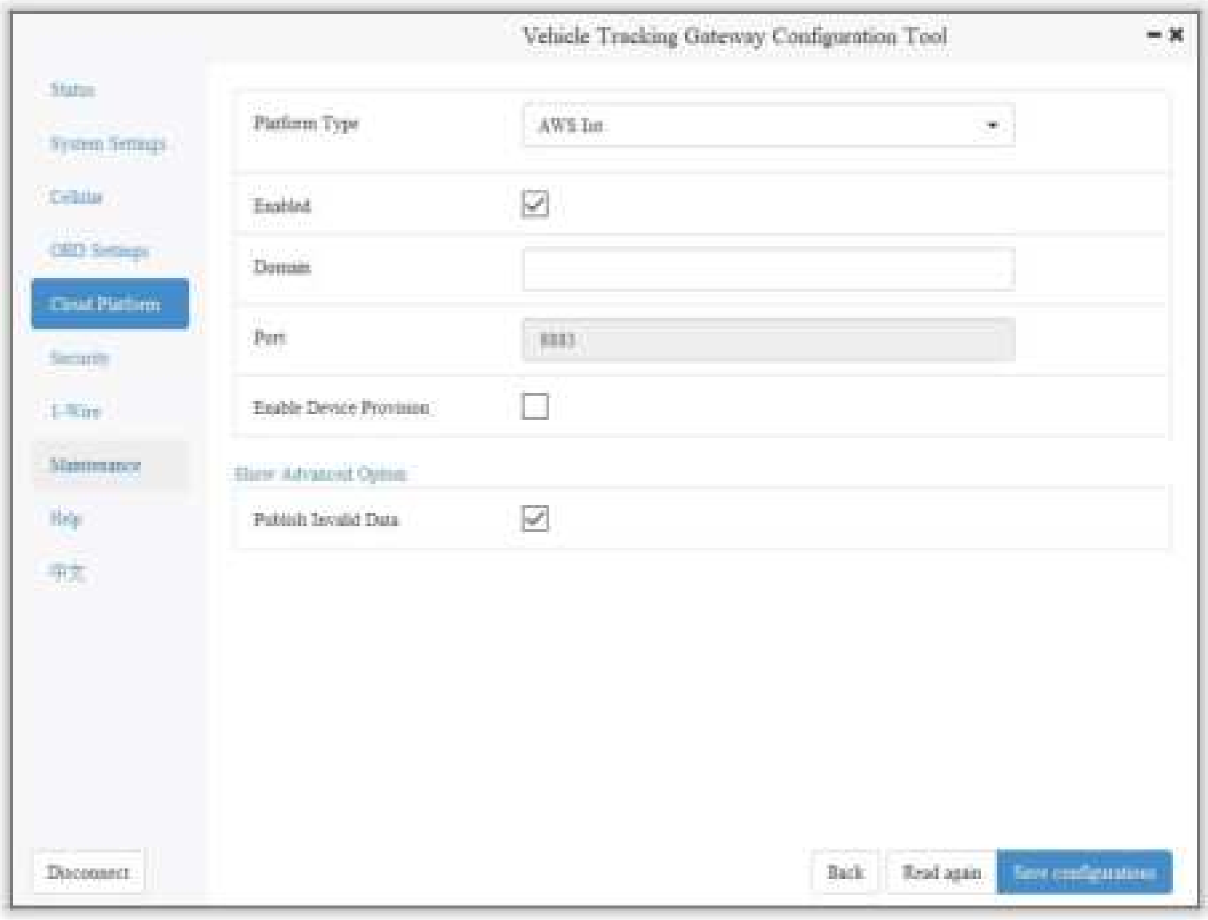
1. Enable AWS

Cloud Platform >> Platform Type: AWS IoT

Cloud Platform >> Enable

Cloud Platform >> Domain name

Cloud Platform >> Port : 8883



Platform Type: AWS Iot

Enabled: ☑

Domain:

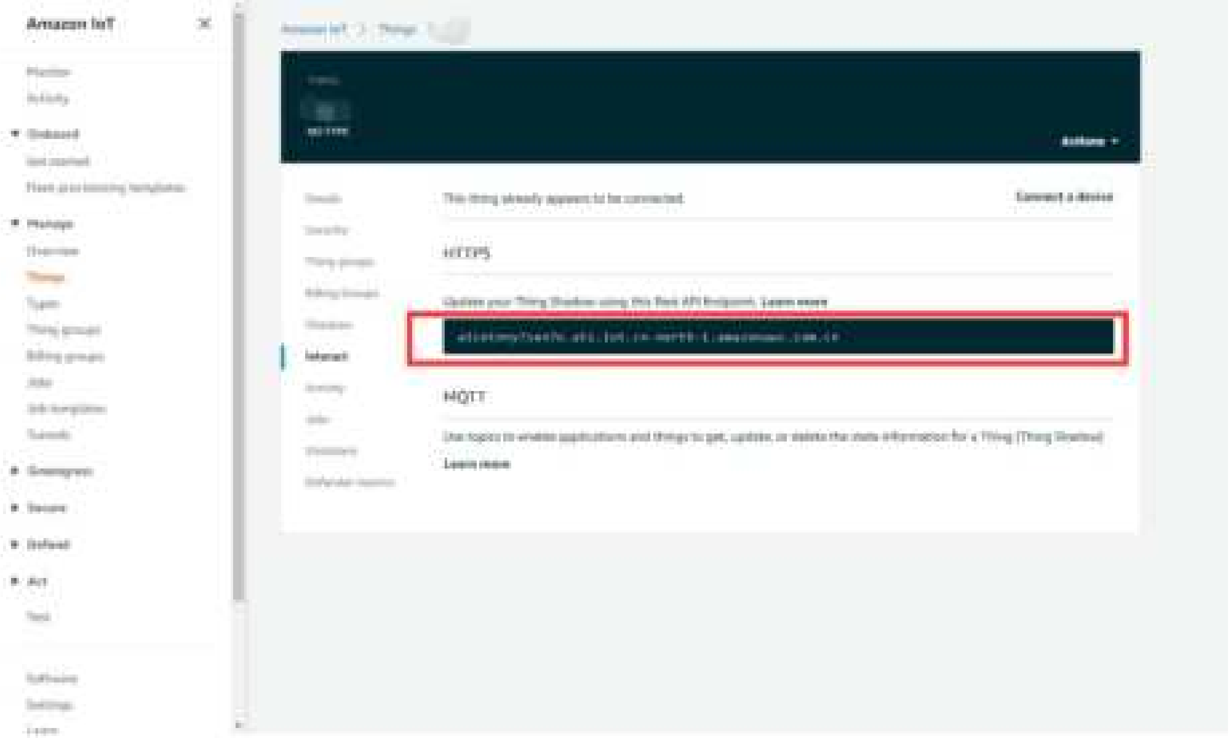
Port: 8883

Enable Device Provision: □

Publish Invalid Data: ☑

If you create a preset template on AWS, you need to enable device preset in the configuration tool. Tick to enable it, and enter the preset template name. The template name can be found in AWS IoT >>Fleet provisioning templates.

Copy the address in the AWS IoT >> Things >> “Select created things”>> Interact option. Enter the domain name on the AWS IoT page.



This thing already appears to be connected.

HTTPS

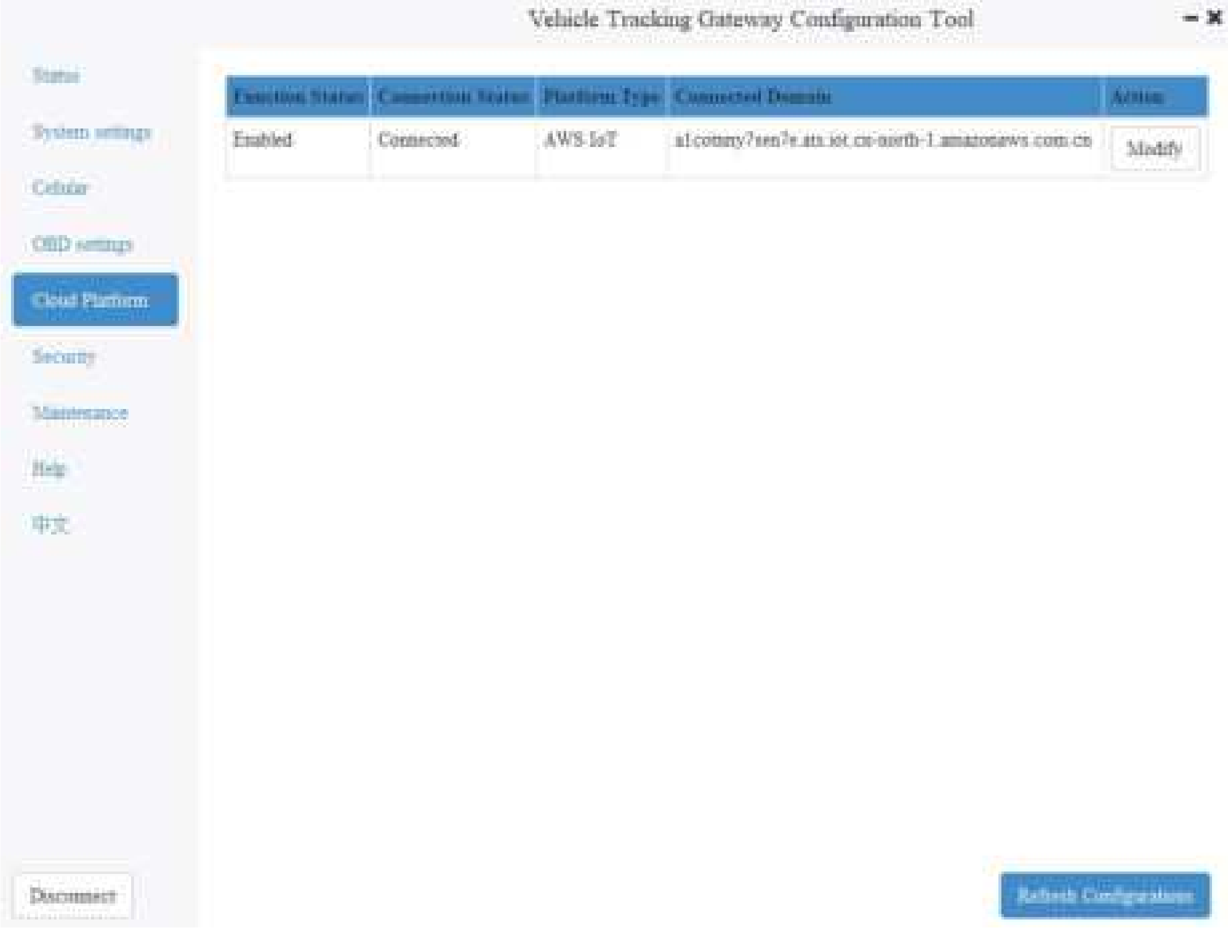
Update your Thing Shadow using this Rest API Endpoint. Learn more

```
[illegible].iot.cn-north-1.amazonaws.com.cn
```

MQTT

Use topics to enable applications and things to get, update, or delete the state information for a Thing (Thing Shadow)

Save the configuration and restart the device. On the Cloud Platform Cloud Platform page, check the connection status:

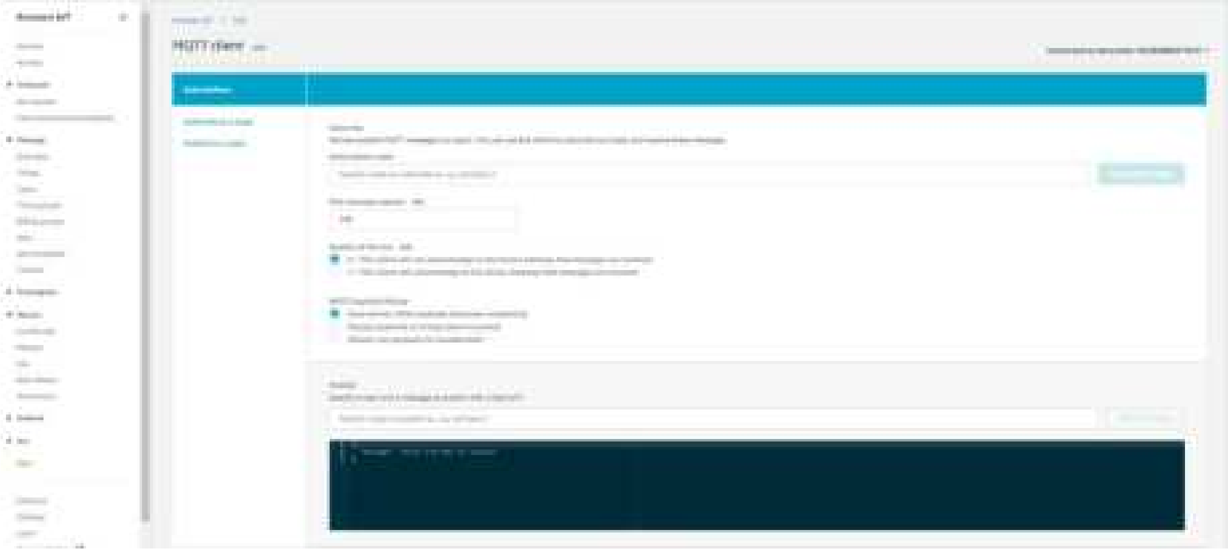


Function Status	Connection Status	Platform Type	Connected Domain	Action
Enabled	Connected	AWS IoT	a1comny7sen7e.ats.iot.cn-north-1.amazonaws.com.cn	Modify

6.4.2 Subscription and Publishing of AWS

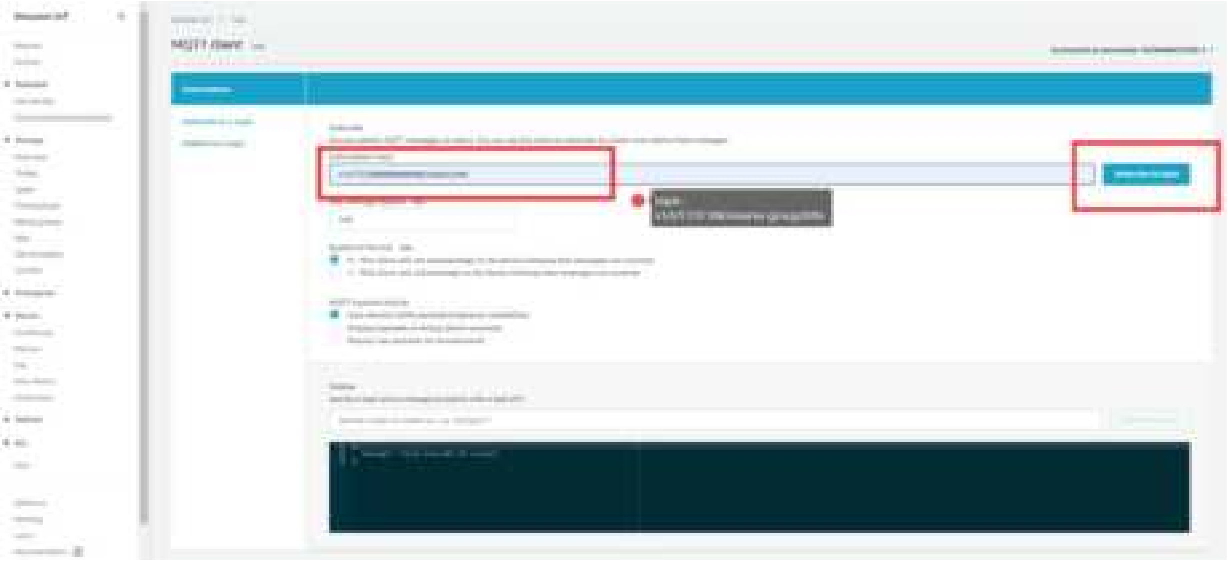
1. Subscribe to messages reported and published by VT310

Amazon IoT >> Test

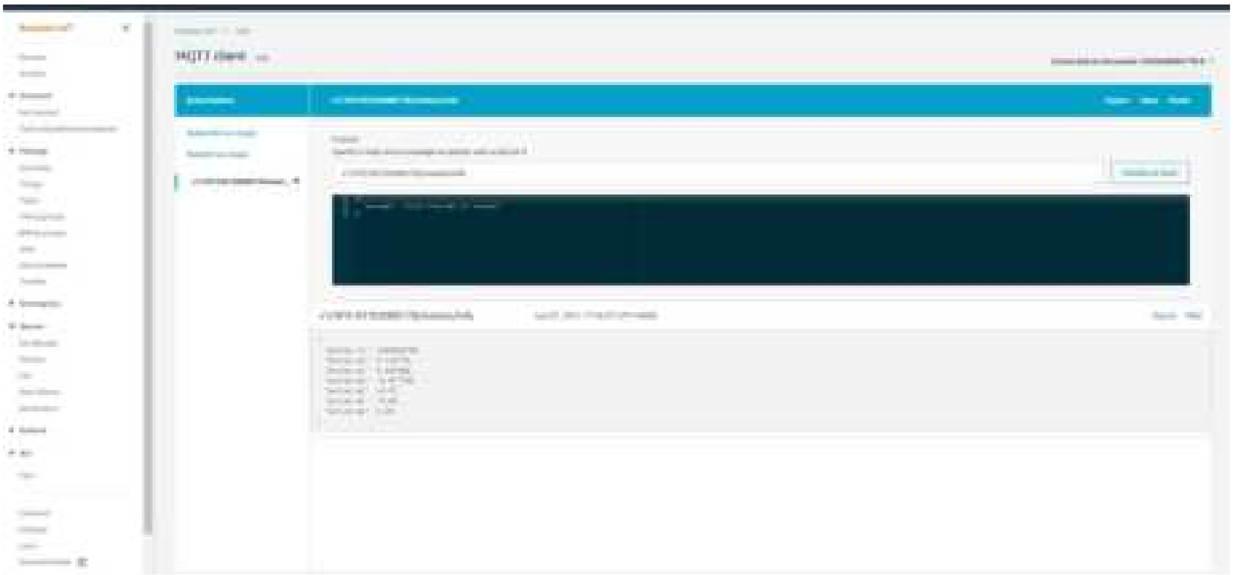


Amazon IoT >> Test >> enter the published topic in the Subscription topic text box, as is shown below.

For example: v1/VT310 SN/motion/info



By default, the VT310 reports messages from the retention groups of GNSS, Sysinfo, Motion, Cellular1, IO, and OBD. You only need to subscribe to topics to receive messages, as is shown below.



For more information, see API documentation.

《FlexAPI_over_MQTT_Reference_for_3rd_party_platform_VT310.pdf》

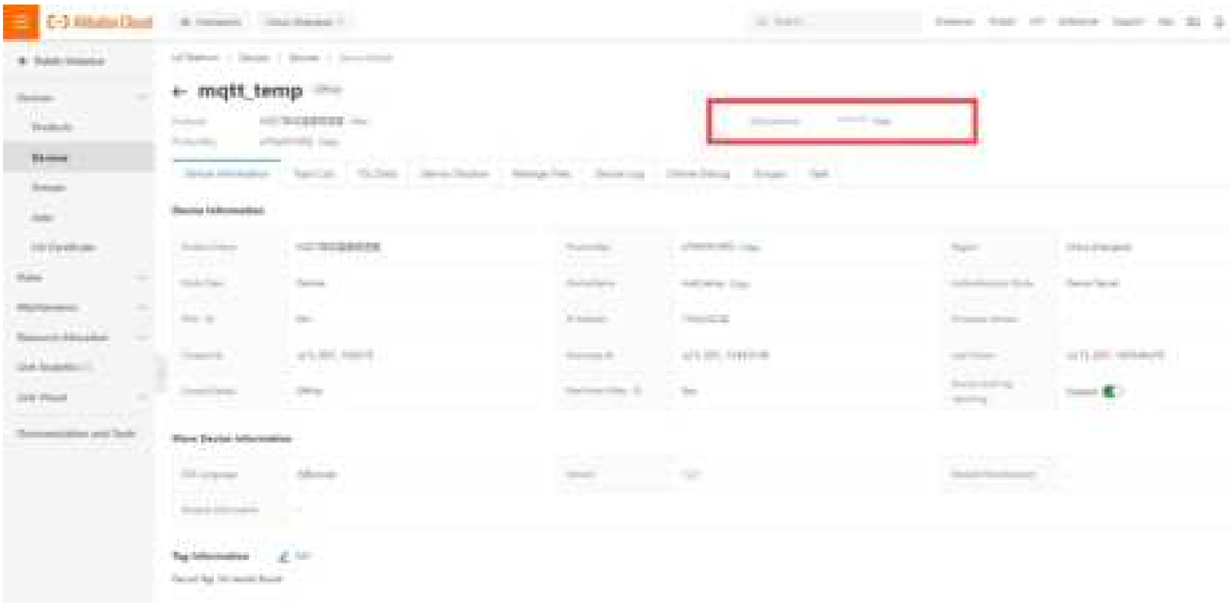
6.5 Aliyun IoT

The Alibaba Cloud Enterprise IoT platform provides fully-hosted instance services. It allows you to easily access and manage devices without building IoT infrastructure by yourself. It features low costs, high reliability, high performance, and easy operation and maintenance. With powerful data processing capabilities, it can better analyze and visualize device data. Real-time security threat detection ensures that each instance is secure and reliable. It is the first choice for each enterprise device to migrate to the cloud. For more information, visit the Alibaba Cloud product page. https://www.aliyun.com/product/iot.

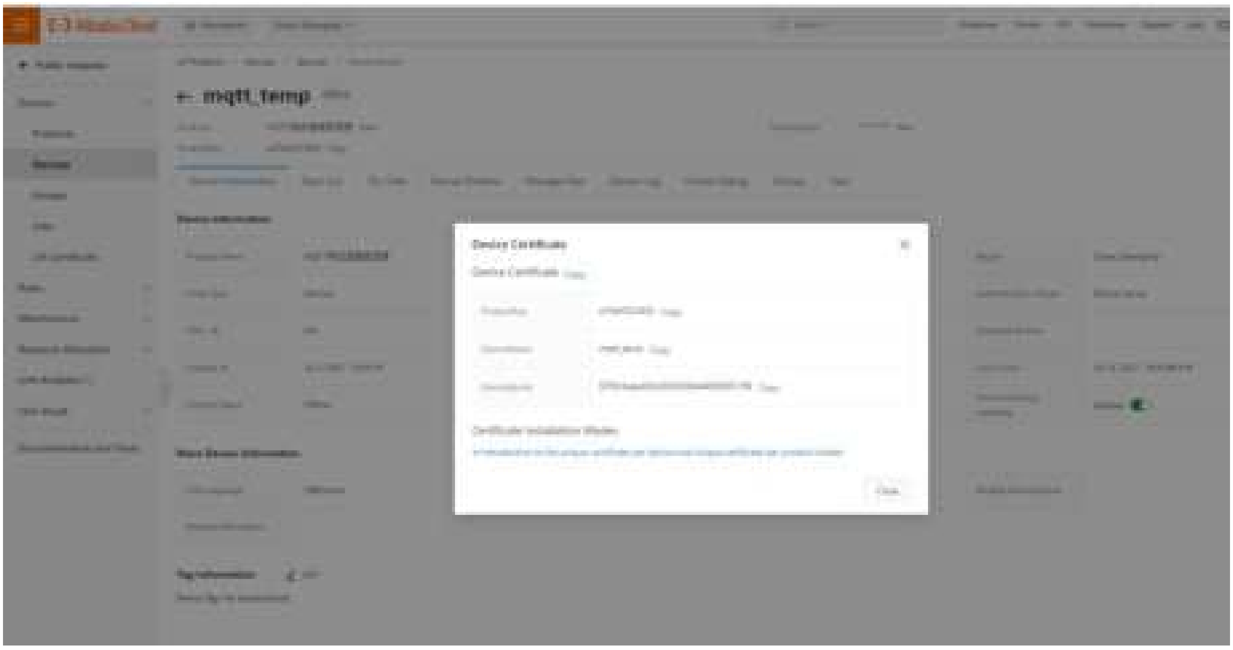
Method 1: One machine and one key

For more information: https://help.aliyun.com/document_detail/74006.html

1. Go to the Alibaba Cloud Console IoT Platfrom >> Device >> Devices >> Device Details. Create a Device and view the Device Secret, as is shown below.



The Device Certificate of the replication Device includes three parameters: Product Key, Device Name, and Device Secret, as is shown below.



1. Config Aliyun IoT

Cloud Platform >> Platform Type: Aliyun IoT

Cloud Platform >> Enable

Cloud Platform >> Device Name:

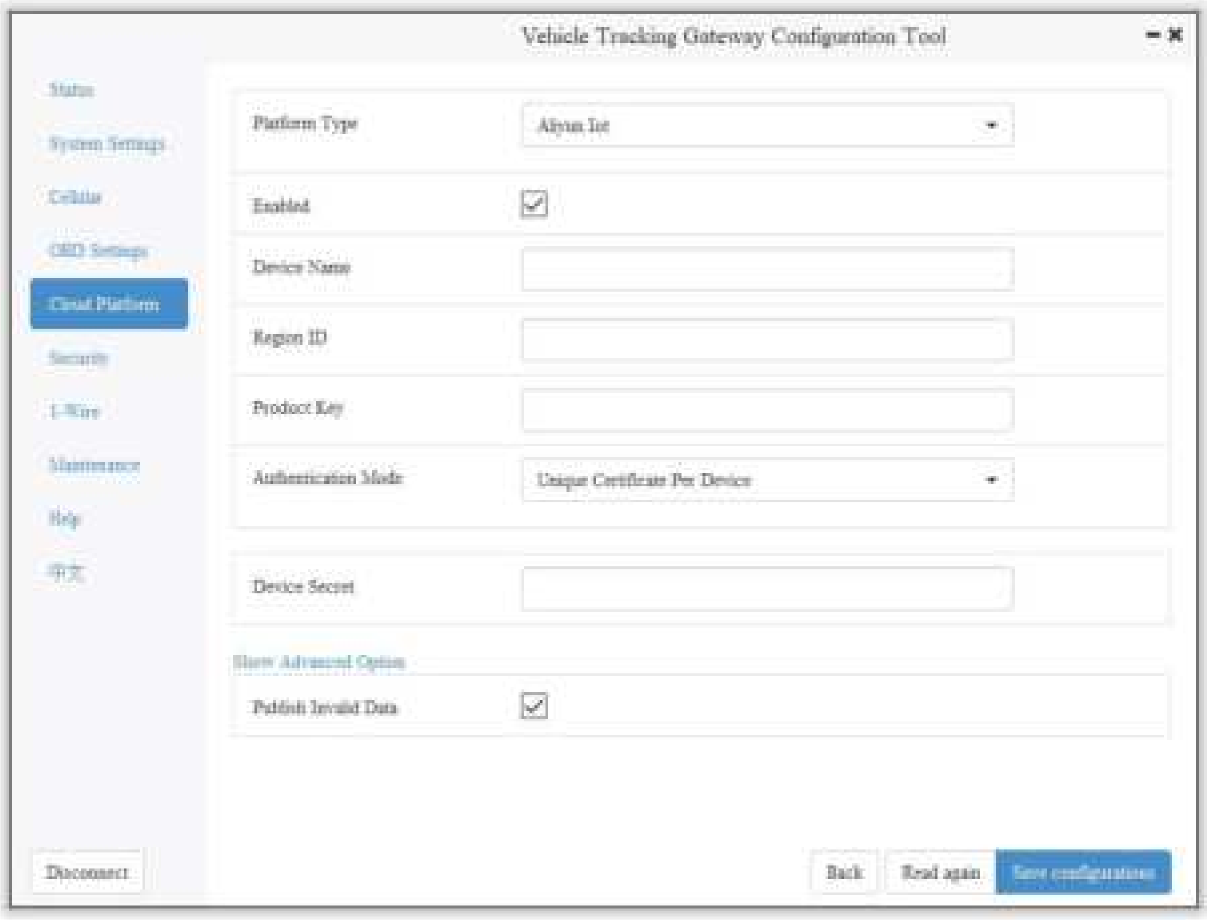
Cloud Platform >> Product Key

Cloud Platform >> Authentication Mode： Unique Certificate Per Device

Cloud Platform >> Device Secert

Tick to enable Secure Certification Mode: Unique Certificate Per Device/Unique Certificate Per Model

The three parameters from Alibaba Cloud ProductKey, DeviceName, and DeviceSecret. Enter the corresponding parameters in the configuration tool. In the upper-left corner of the IoT platform console, view the region where your service is located. For more information about the Region ID values, see Region and zone.



Platform Type: Aliyun Iot

Enabled: ☑

Device Name:

Region ID:

Product Key:

Authentication Mode: Unique Certificate Per Device

Device Secret:

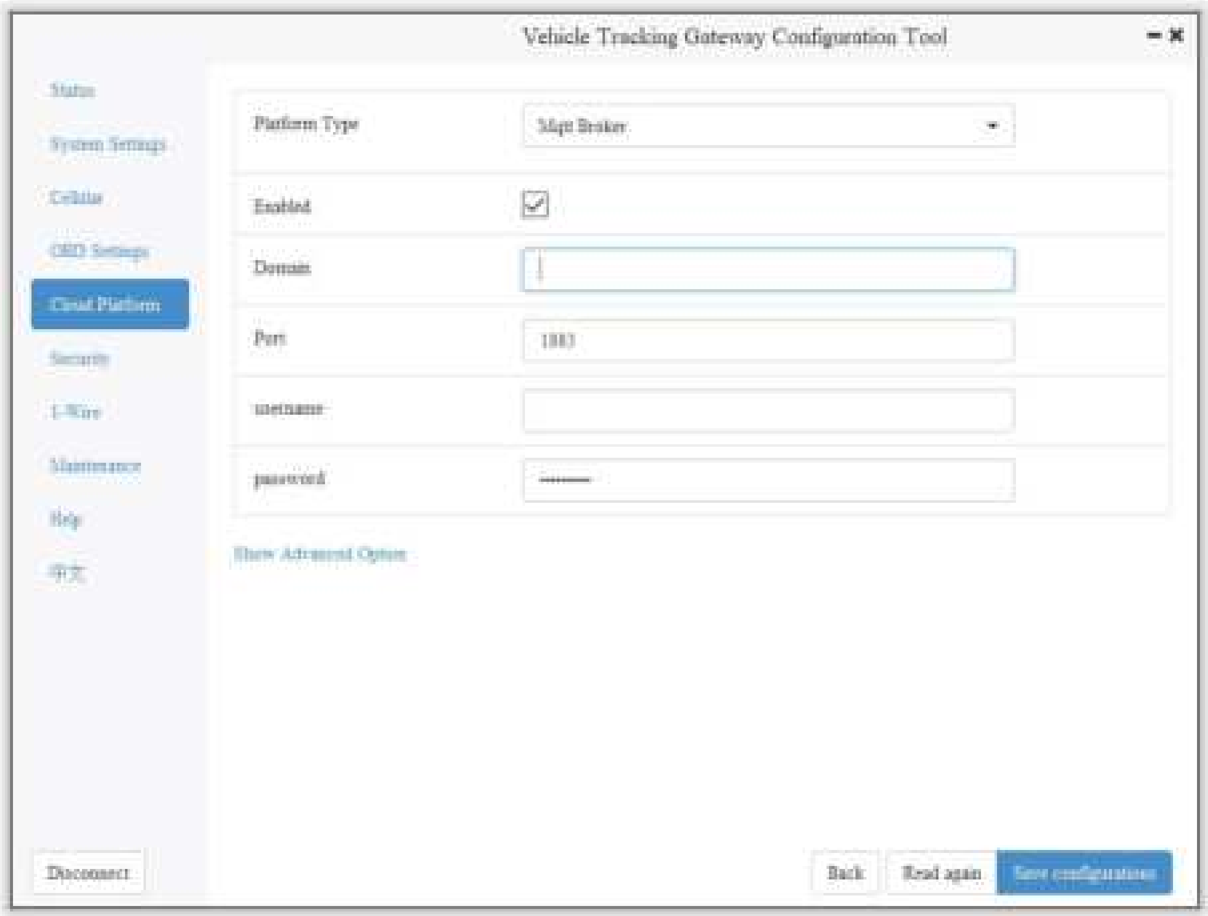
Publish Invalid Data: ☑

6.6 Configuration of MQTT Platform Link

MQ Telemetry Transport (MQTT) is a lightweight proxy-based message transmission protocol for Publishing/Subscribing. It is designed to be open, simple, lightweight, and easy to implement. These features make it suitable for restricted network environments, including but not limited to high-costs, low-bandwidth and unreliable networks. CPU and memory resources are limited for embedded devices. This protocol provides one-to-many message publishing and discoupling applications using the publish/subscribe message mode. It supports transmission of messages blocked by load content with TCP/IP. Open-source software that supports MQTT, such as ThingsBoard and EMQ, allows customers to develop their own IoT platforms.

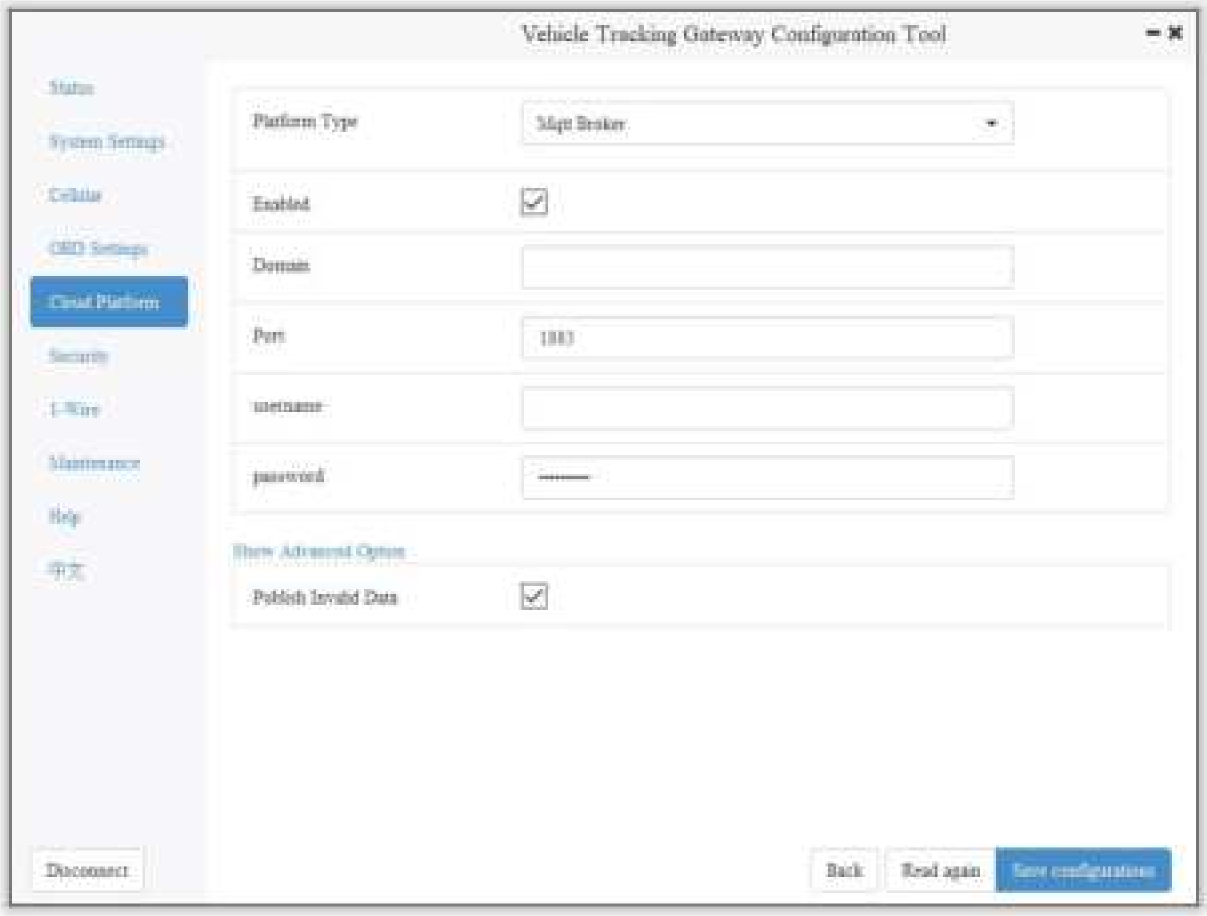
6.6.1 MQTT Broker

Cloud Platform >> Platform Type >> Mqtt Broker: Enable, configure domain name, port, username, and password ″. Click ″Save configuration″ and restart, as is shown below.



Platform Type	Mqtt Broker
Enabled	☑
Domain	
Port	1883
username	
password	••••••••

If you want to view invalid data, click ″Show Advanced Options″ to see hidden configuration items. Select ″Show invalid data″, as is shown below.



Platform Type: Mqtt Broker

Enabled: ☑

Domain:

Port: 1883

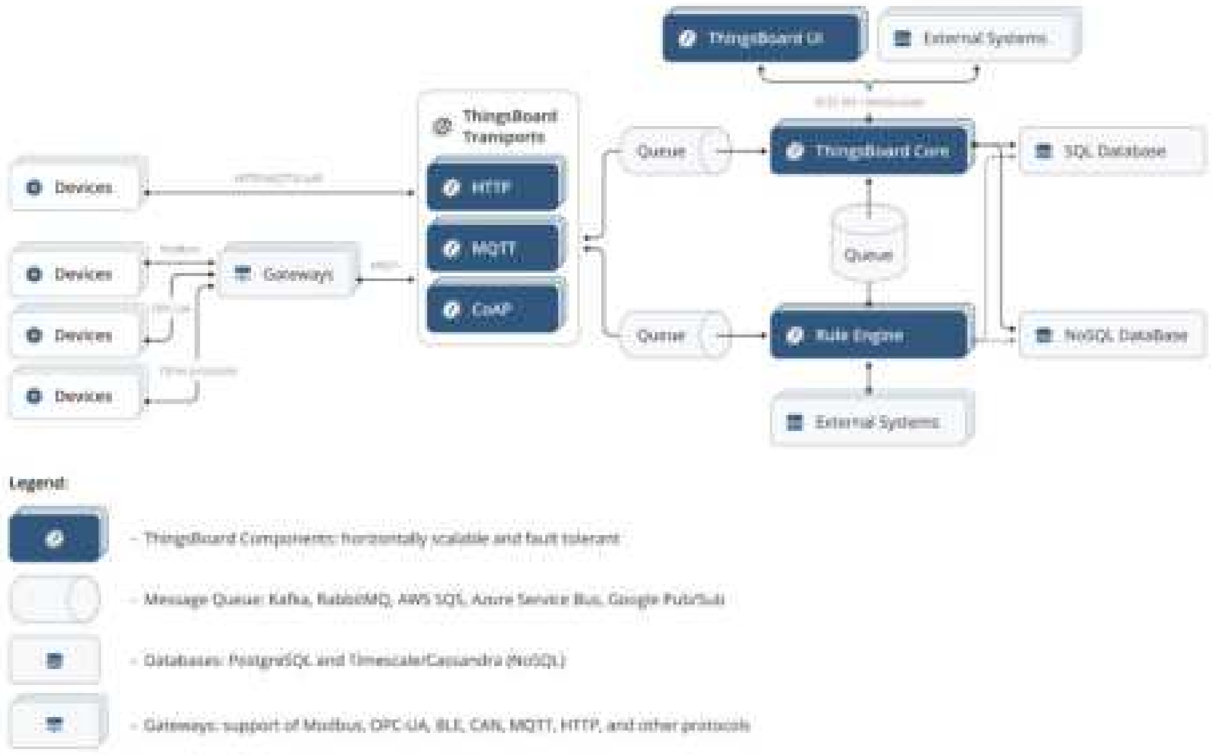
username:

password: ••••••••

Publish Invalid Data: ☑

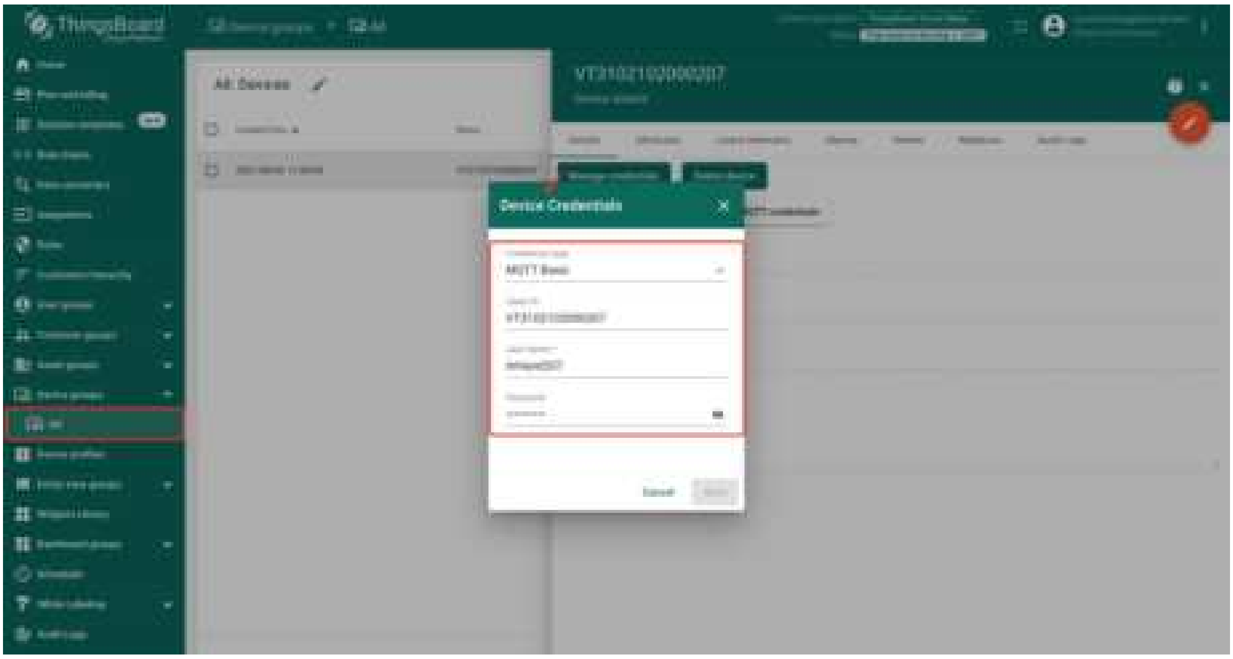
6.6.2 Configure ThingBoard Open-source IoT Platform

ThingsBoard is an open-source IoT platform where you can quickly develop, manage, and expand IoT projects. It is an open-source IoT platform for data collection, processing, visualization, and device management. It connects devices through the industry-standard IoT protocols - MQTT, CoAP, and HTTP, and supports cloud and local deployment. For more information, go to https://thingsboard.io.


ThingsBoard UI
External Systems
ThingsBoard Transports
HTTP
MQTT
CoAP
Devices
Devices
Devices
Devices
Gateways
Queue
ThingsBoard Core
SQL Database
Queue
Queue
Rule Engine
NoSQL DataBase
External Systems
Legend:
- ThingsBoard Components: horizontally scalable and fault tolerant
- Message Queue: Kafka, RabbitMQ, AWS SQS, Azure Service Bus, Google Pub/Sub
- Databases: PostgreSQL and Timescale/Cassandra (NoSQL)
- Gateways: support of Modbus, OPC-UA, BLE, CAN, MQTT, HTTP, and other protocols

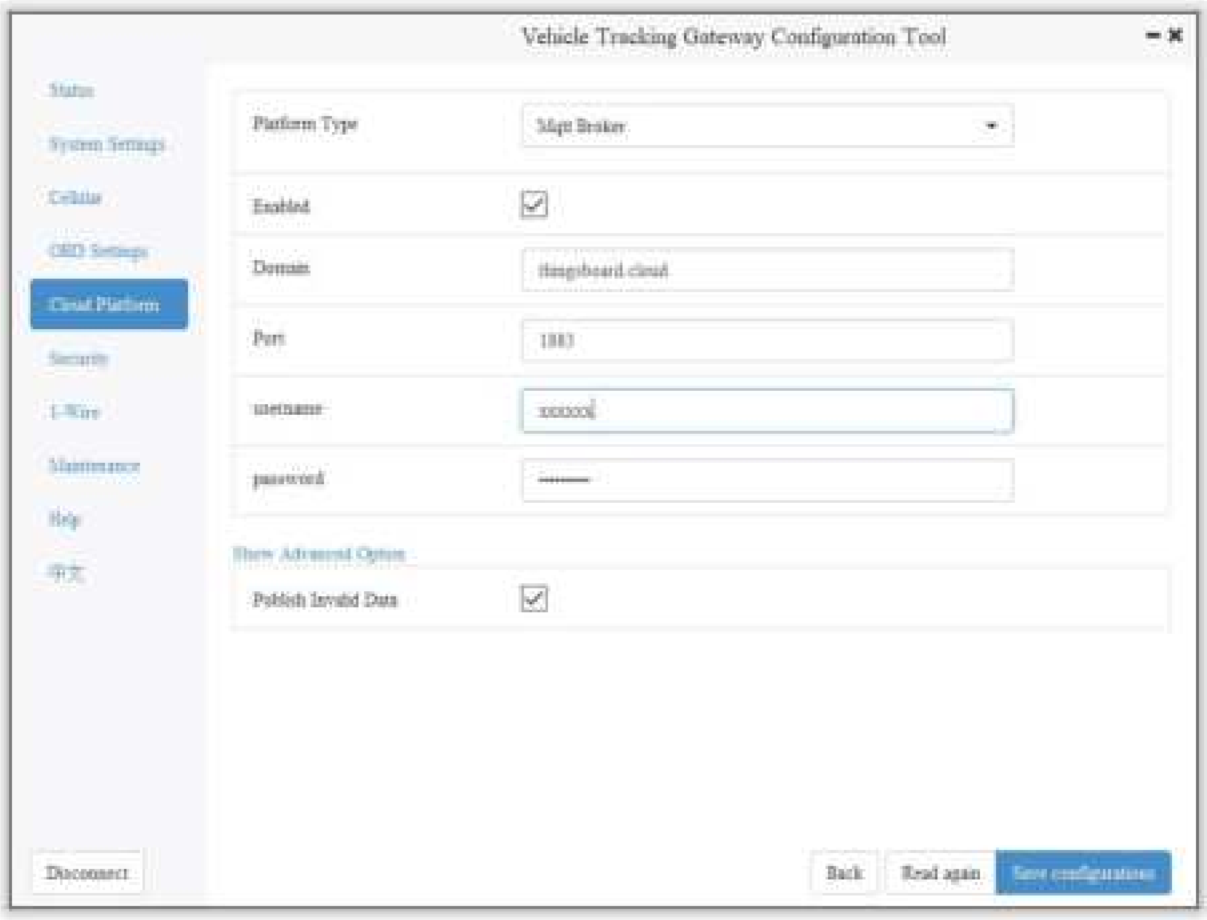
ThingsBoard Architecture

1. Register an account and add a device. After adding a device, use the open Device Device Credentials >> MQTT Basic to enter the Client ID, User Name, and Password parameters. For more information, visit https://thingsboard.io/docs/getting-started-guides.



Platform Device Parameters

1. In the configuration tool, enter the thingsboard.cloud, port number 1883, username User Name, Password, Password of the device parameters added by the platform.


Vehicle Tracking Gateway Configuration Tool

Platform Type: Mqtt Broker

Enabled: ☑

Domain: thingsboard.cloud

Port: 1883

username: xxxxxx

password: --------

Show Advanced Option

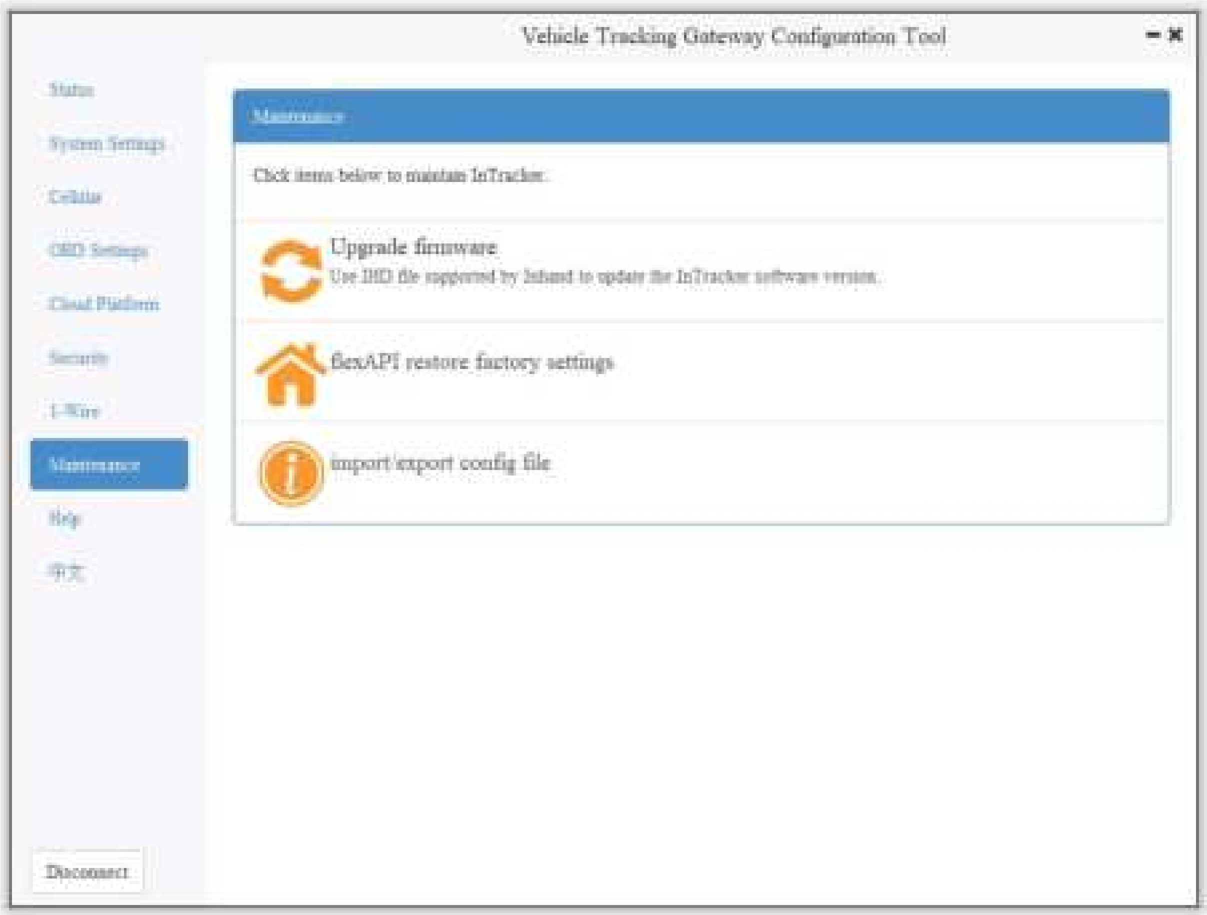
Publish Invalid Data: ☑

7. Maintenance

You can upgrade the firmware with the local upgrade configuration tool, xshell, or through OTA. OTA upgrading includes Alibaba Cloud standard OTA upgrading, SmartFleet platform OTA upgrading and FlexAPI upgrading. Now we will only introduce how to upgrade with local configuration tools. For more information about upgrading, please contact technical support of InHand Networks.

7.1 Firmware Upgrade

Step 1: Go to Maintenance >> Upgrade firmware, as is shown below:



Click items below to maintain InTracker.

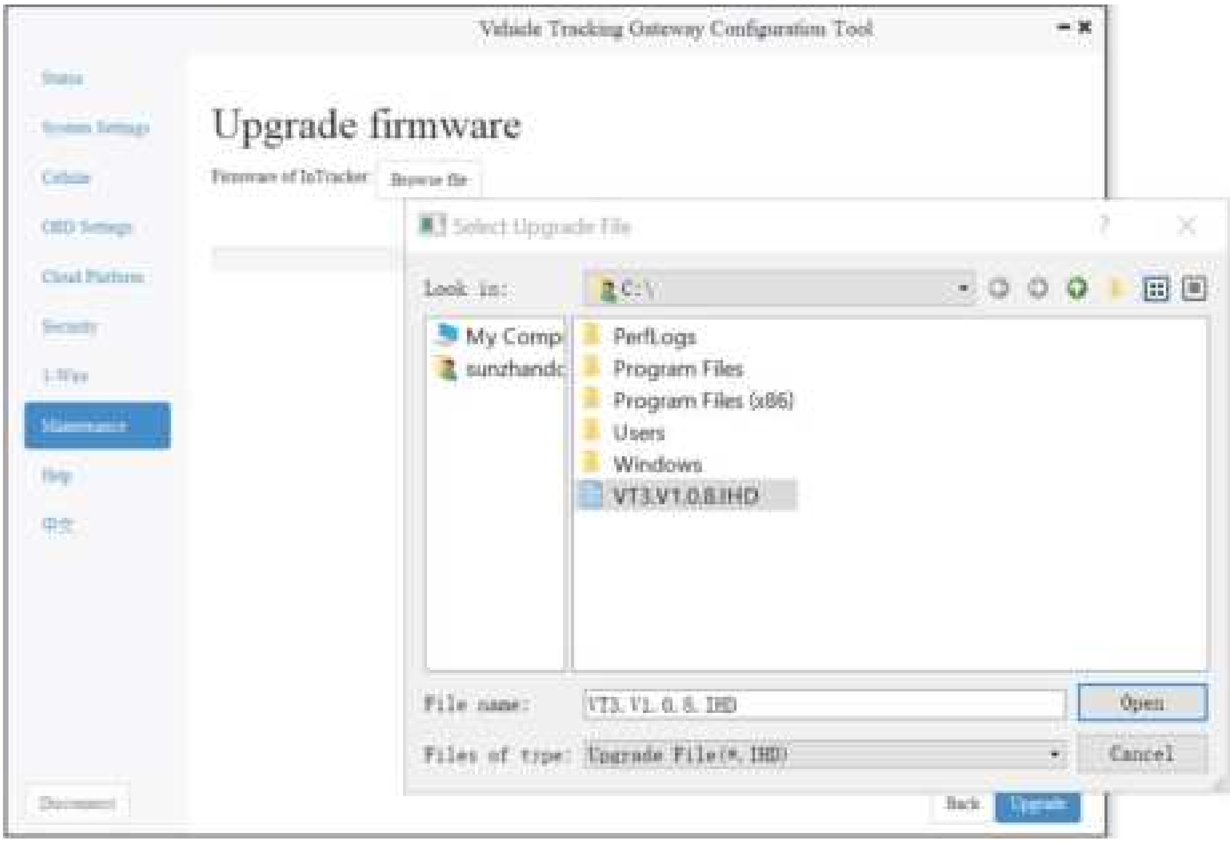
Upgrade firmware

Use IHD file supported by Inhand to update the InTracker software version.

flexAPI restore factory settings

import/export config file

Step 2: Click ″Browse file″ to select the firmware. Click ″Upgrade″ and wait for firmware installation, as is shown below:



Upgrade firmware

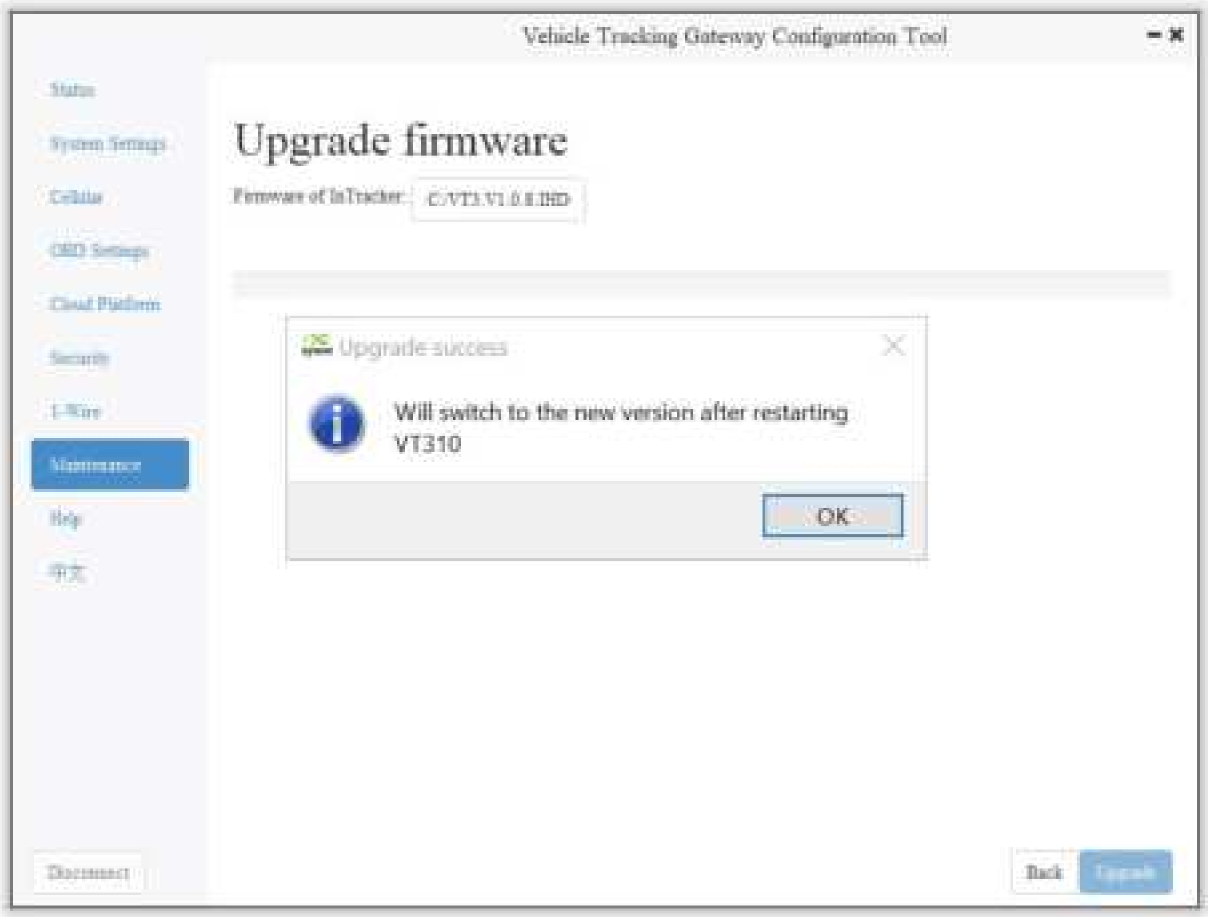
Firmware of InTracker

Look in: C:\

File name: VT3.V1.0.8.IHD

Files of type: Upgrade File(*.IHD)

When a prompt box says ″Will switch to the new version after restarting VT310″, new firmware has been imported successfully. Click ″Restart″ to upgrade the firmware.



Upgrade firmware

Firmware of InTracker: C:/VT3.V1.0.8.IHD

Upgrade success

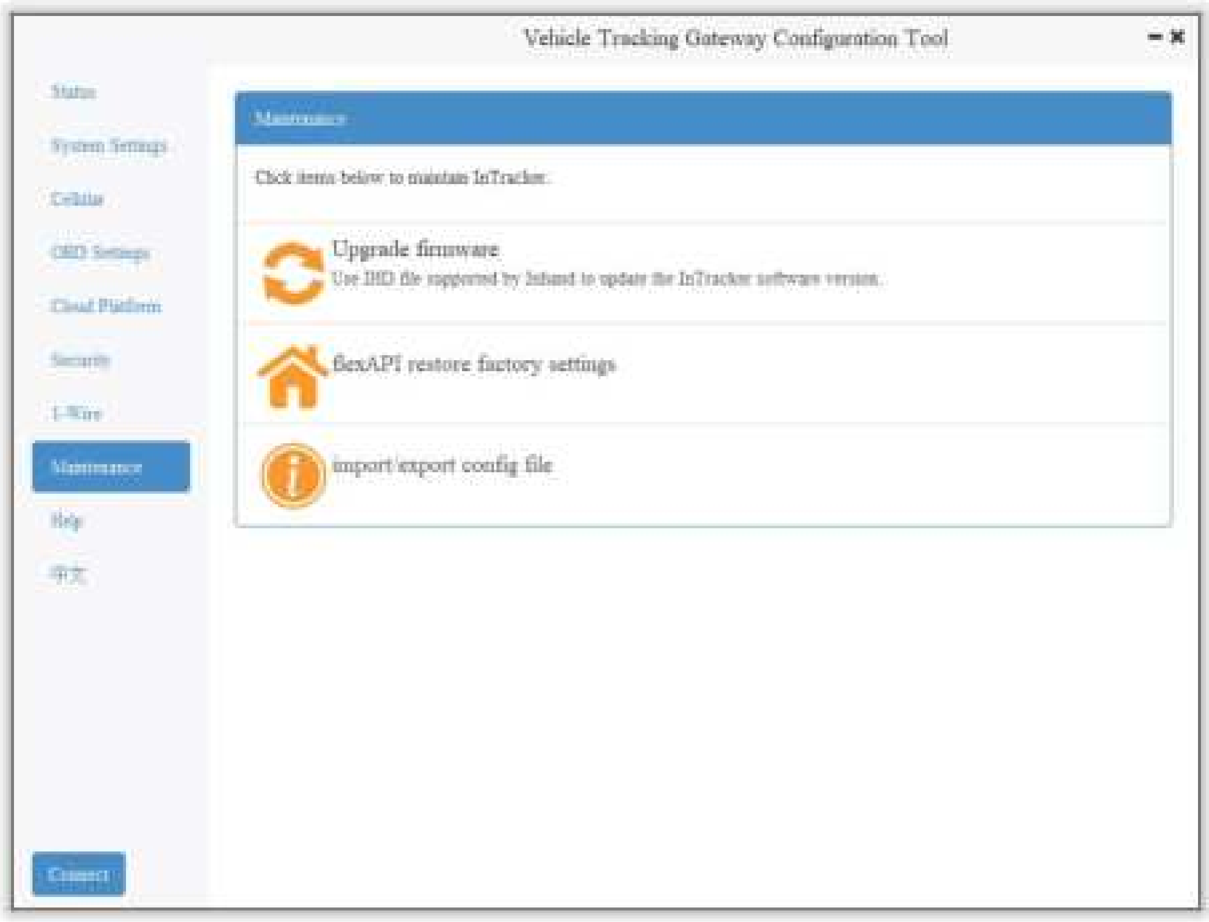
Will switch to the new version after restarting VT310

OK

Note: After the device is upgraded, restart the device and then configure it.

7.2 Restore Factory Settings of FlexAPI

Go to Maintenance >> FlexAPI restore factory settings to reset FlexAPI settings.



Click items below to maintain InTracker.

Upgrade firmware

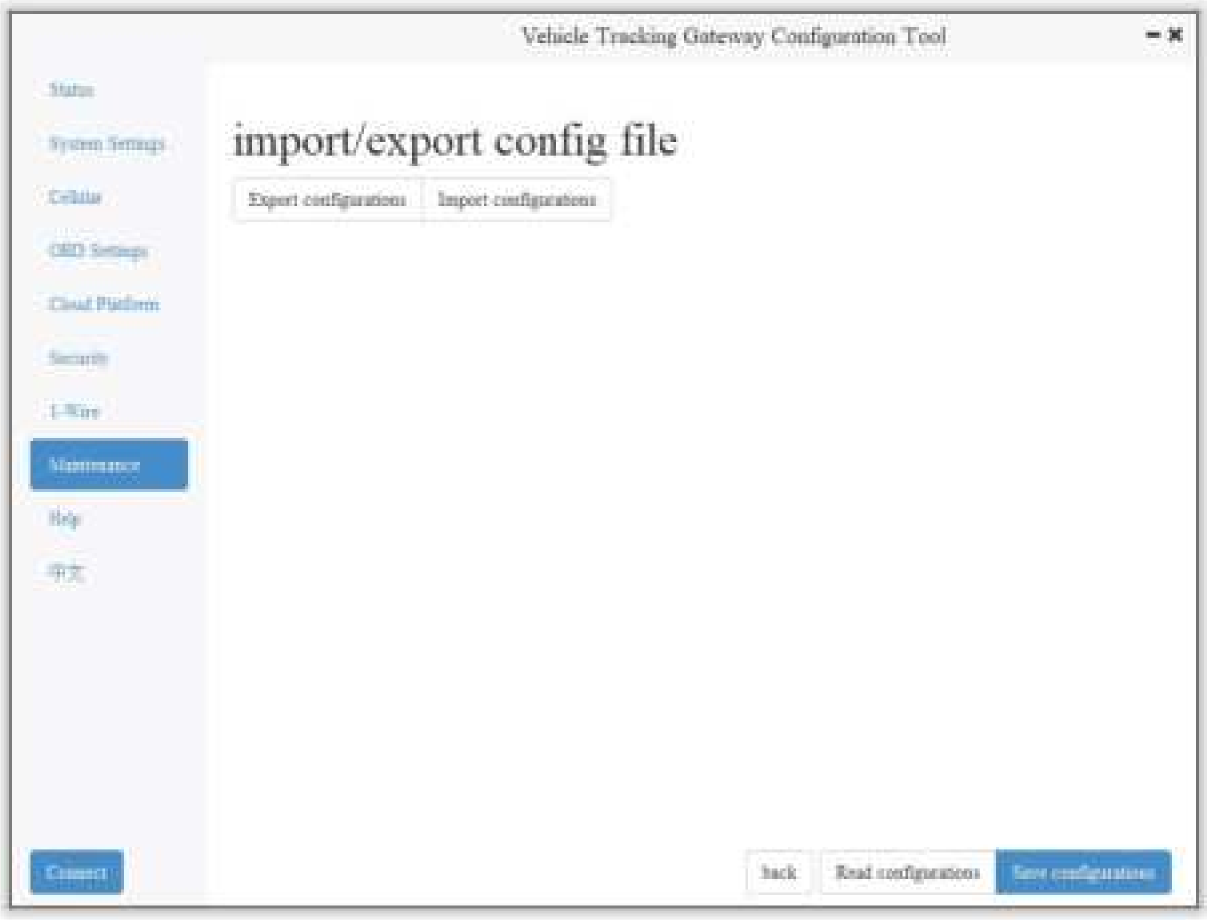
Use IHD file supported by Inhand to update the InTracker software version.

flexAPI restore factory settings

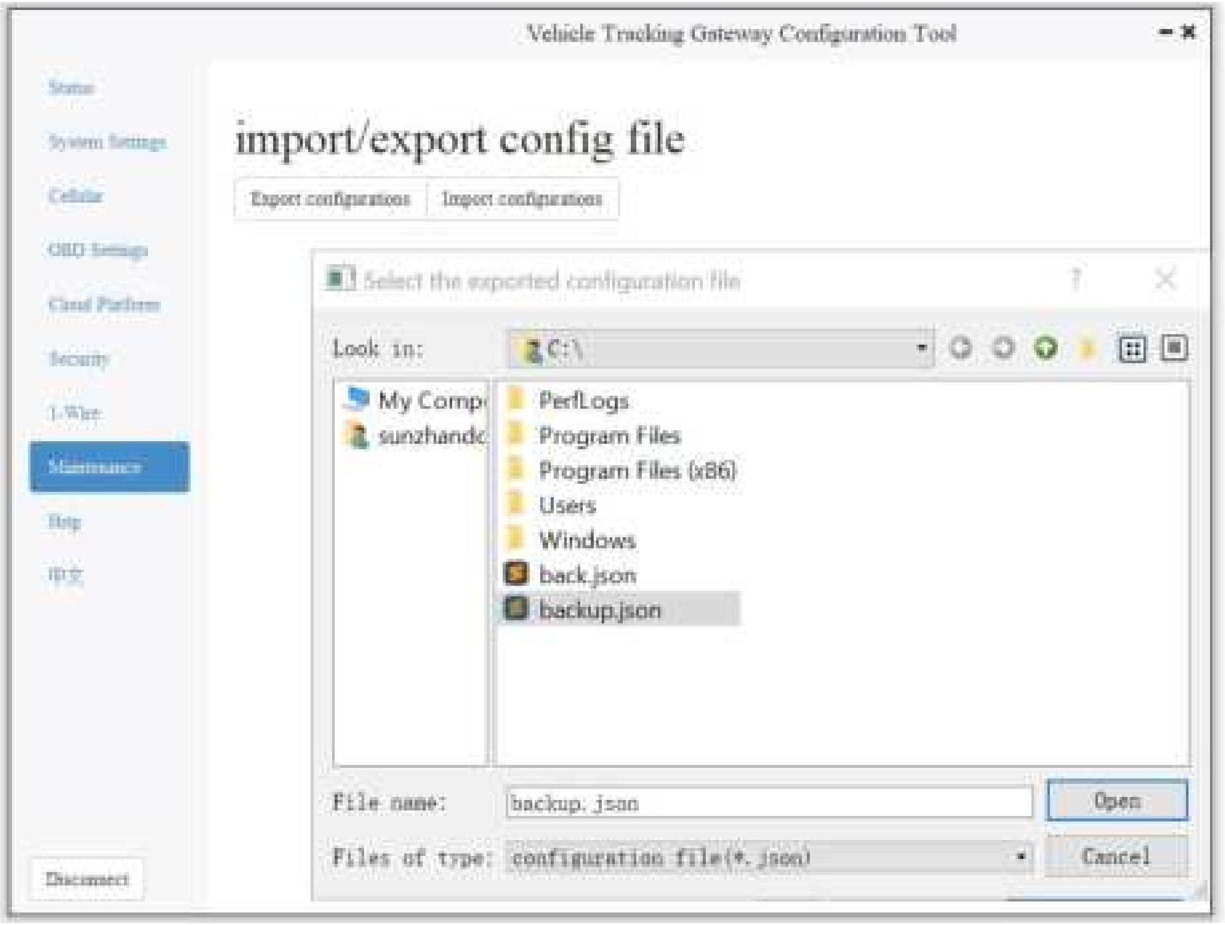
import/export config file

7.3 Import/Export Configuration

To back up and import configuration, go to Maintenance >> Import/export congifuration file, as is shown below. Click "Export configuration" to back up configuration, and click "Import configuration" to load the configuration file.



To back up configuration, click "Export configuration". The configuration tool can read device configuration and pop up file storage window. Enter the name of the backup file, and click "Open".

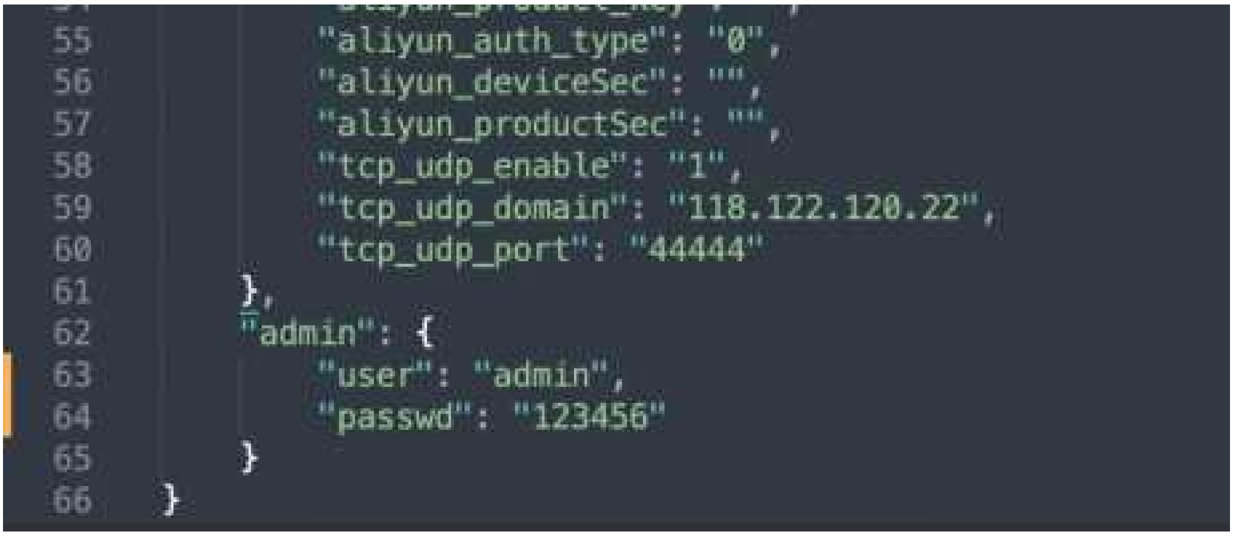


File name: backup.json

Files of type: configuration file(*.json)

In the exported configuration file, Username and Password are not available. If you hope to import the modified username and password to the new device, you can modify them in the exported file. Replace the admin characters with a new admin account, and input in the password of the new account. After the modified configuration file is saved, import it into the new device and restart the device. Log in the new device with the new admin account and password.

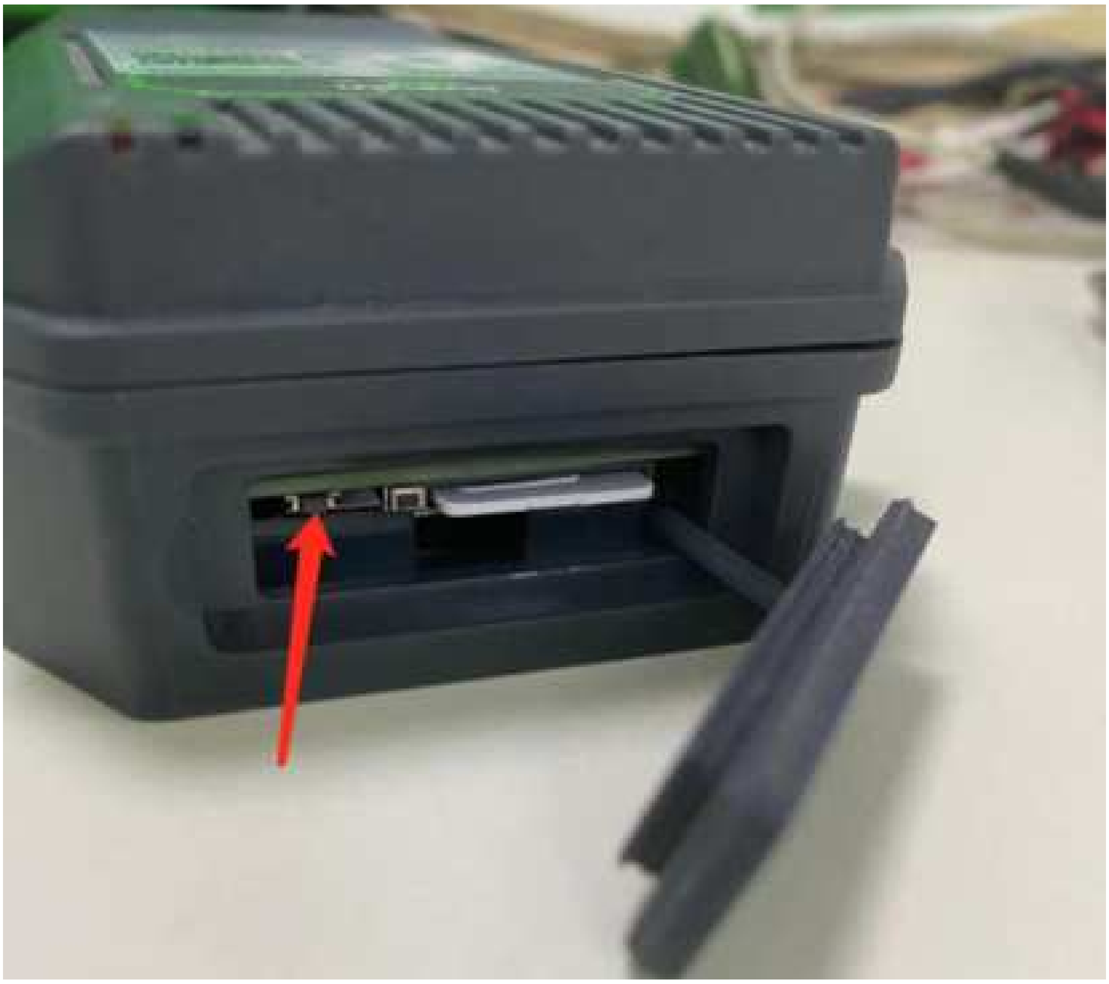
In the exported configuration file, Username and Password are not available. If you hope to import the modified username and password to the new device, you can add them in the exported configuration file. Enter your admin account in "" of "user:":"", and enter the password in "" of "passwd":"". After the modified configuration file is saved, import it into the new device and restart the device. Log in the new device with the new admin account and password.



```
        "aliyun_auth_type": "0",
        "aliyun_deviceSec": "",
        "aliyun_productSec": "",
        "tcp_udp_enable": "1",
        "tcp_udp_domain": "118.122.120.22",
        "tcp_udp_port": "44444"
    },
    "admin": {
        "user": "admin",
        "passwd": "123456"
    }
}
```

8. Restoration of the Default Account and Password for Hardware

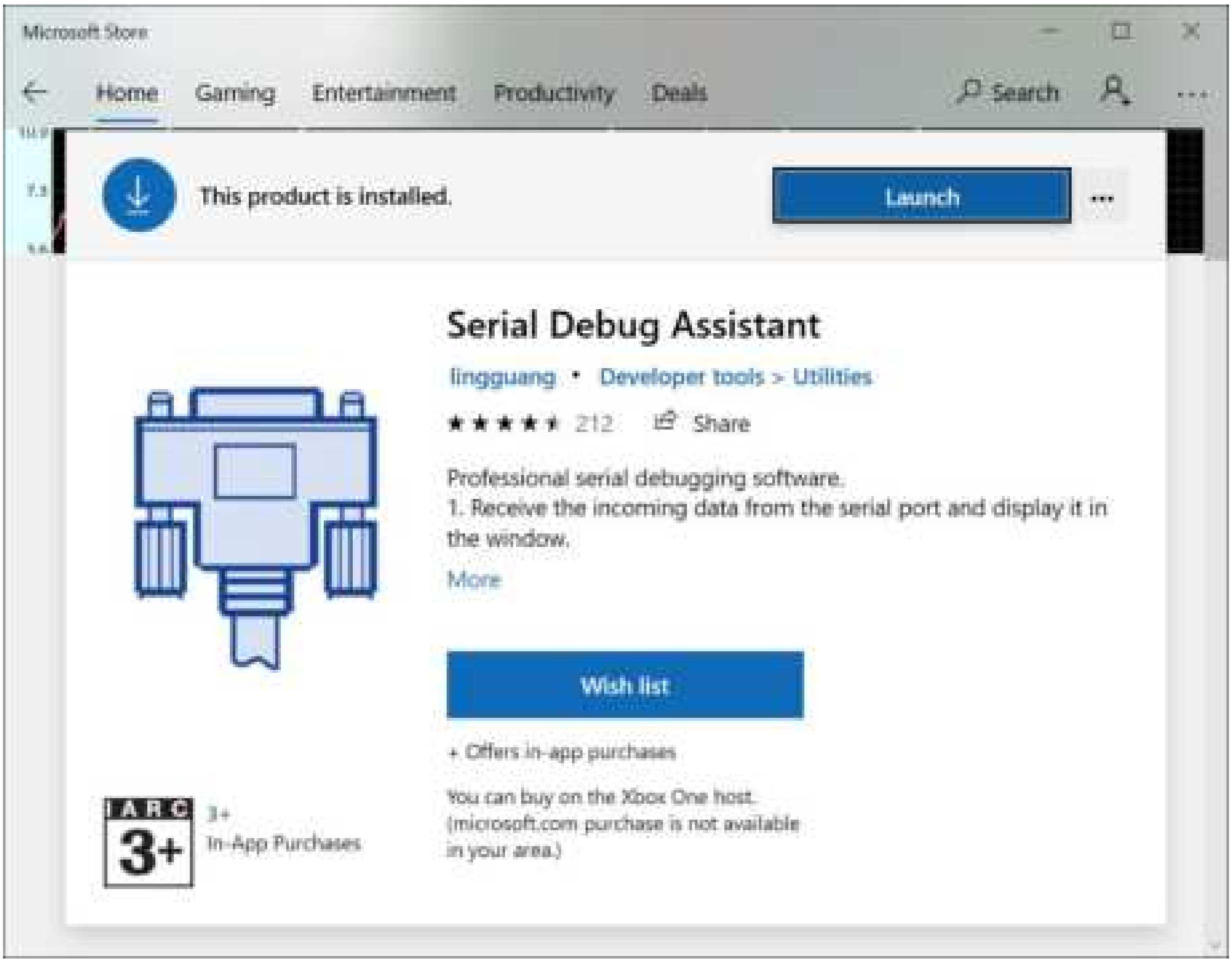
Because configuration usually involves the device certificate file, when the device is restored to the factory via hardware, only the username and password are restored to admin/123456. As is shown in the following picture, press the Reset button with a screwdriver or other tools for more than 8 seconds, and then loosen it.



ps: By double-clicking "Reset", you can restart the device when it goes wrong.

9. How to Get the Device Log

Make sure that the computer is connected to the VT310 through USB to serial port through configuration wire, and open a serial port connection tool such as the serial port debugging software. The software can be downloaded in Mircrosoft Store.



Microsoft Store

This product is installed.

Serial Debug Assistant

lingguang • Developer tools > Utilities

★★★★★ 212

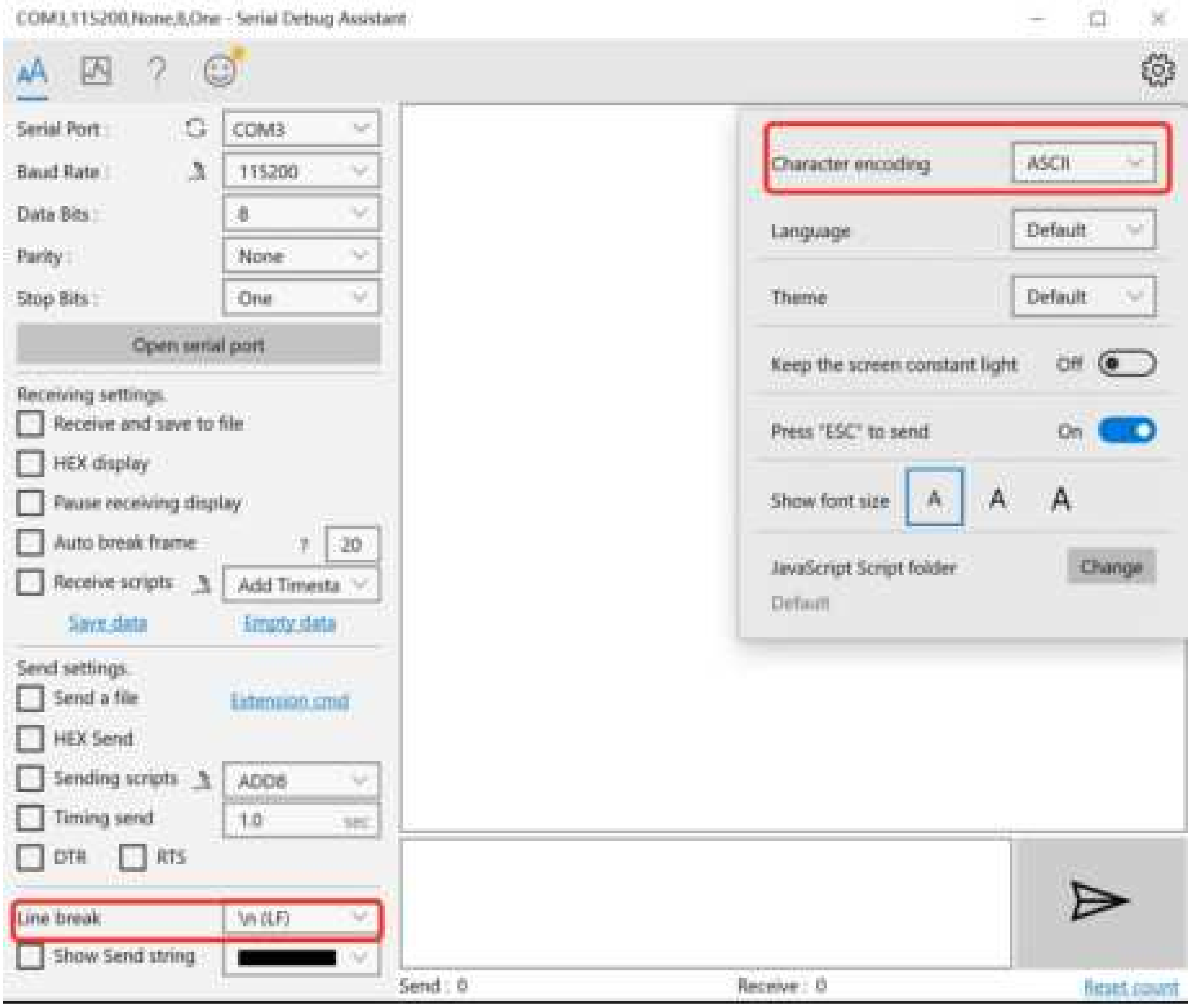
Professional serial debugging software.
1. Receive the incoming data from the serial port and display it in the window.

+ Offers in-app purchases

You can buy on the Xbox One host. (microsoft.com purchase is not available in your area.)

3+ In-App Purchases

1. Open the serial port debugging software and select the link serial port. The default baud rate of the serial port is 115200/8/n/1. Click "Open serial port". Note that the Character encoding mode (Character encoding) is ASCII, and the line break mode (Linet break) is \n(LF).



COM3,115200,None,8,One - Serial Debug Assistant

Serial Port : COM3

Baud Rate : 115200

Data Bits : 8

Parity : None

Stop Bits : One

Open serial port

Receiving settings

□ Receive and save to file

□ HEX display

□ Pause receiving display

□ Auto break frame ? 20

□ Receive scripts Add Timesta

Save data Empty data

Send settings

□ Send a file Extension cmd

□ HEX Send

□ Sending scripts ADD8

□ Timing send 1.0 sec

□ DTR □ RTS

Line break \n (LF)

□ Show Send string

Character encoding ASCII

Language Default

Theme Default

Keep the screen constant light Off

Press "ESC" to send On

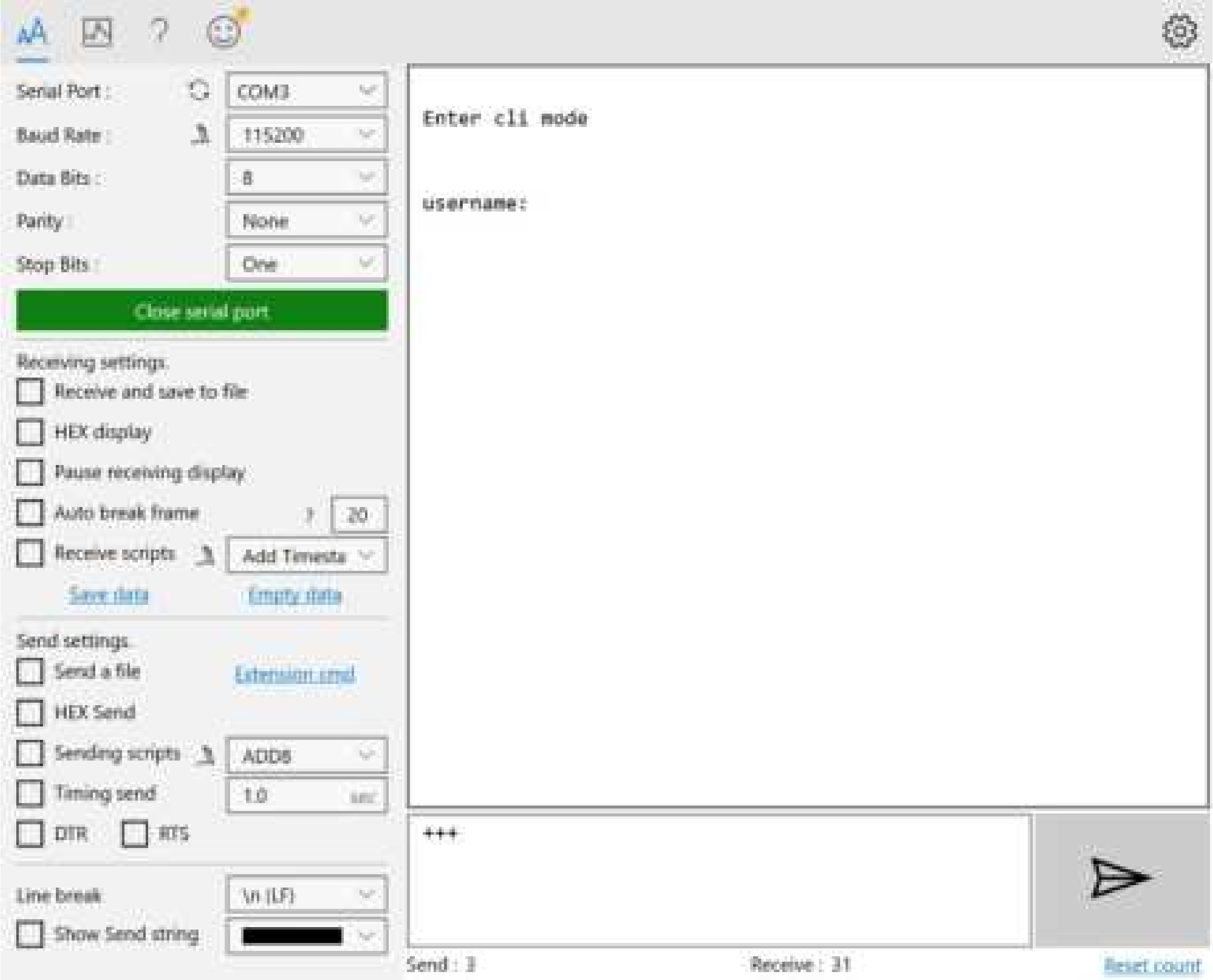
Show font size A A A

JavaScript Script folder Change

Default

Send : 0 Receive : 0 Reset count

1. Enter +++ in the content sending serial port to activate the CLI mode, as is shown below;



Serial Port : COM3

Baud Rate : 115200

Data Bits : 8

Parity : None

Stop Bits : One

Receiving settings

- □ Receive and save to file
- □ HEX display
- □ Pause receiving display
- □ Auto break frame 20
- □ Receive scripts Add Timesta

Send settings

- □ Send a file
- □ HEX Send
- □ Sending scripts ADD8
- □ Timing send 1.0
- □ DTR □ RTS

Line break \n (LF)

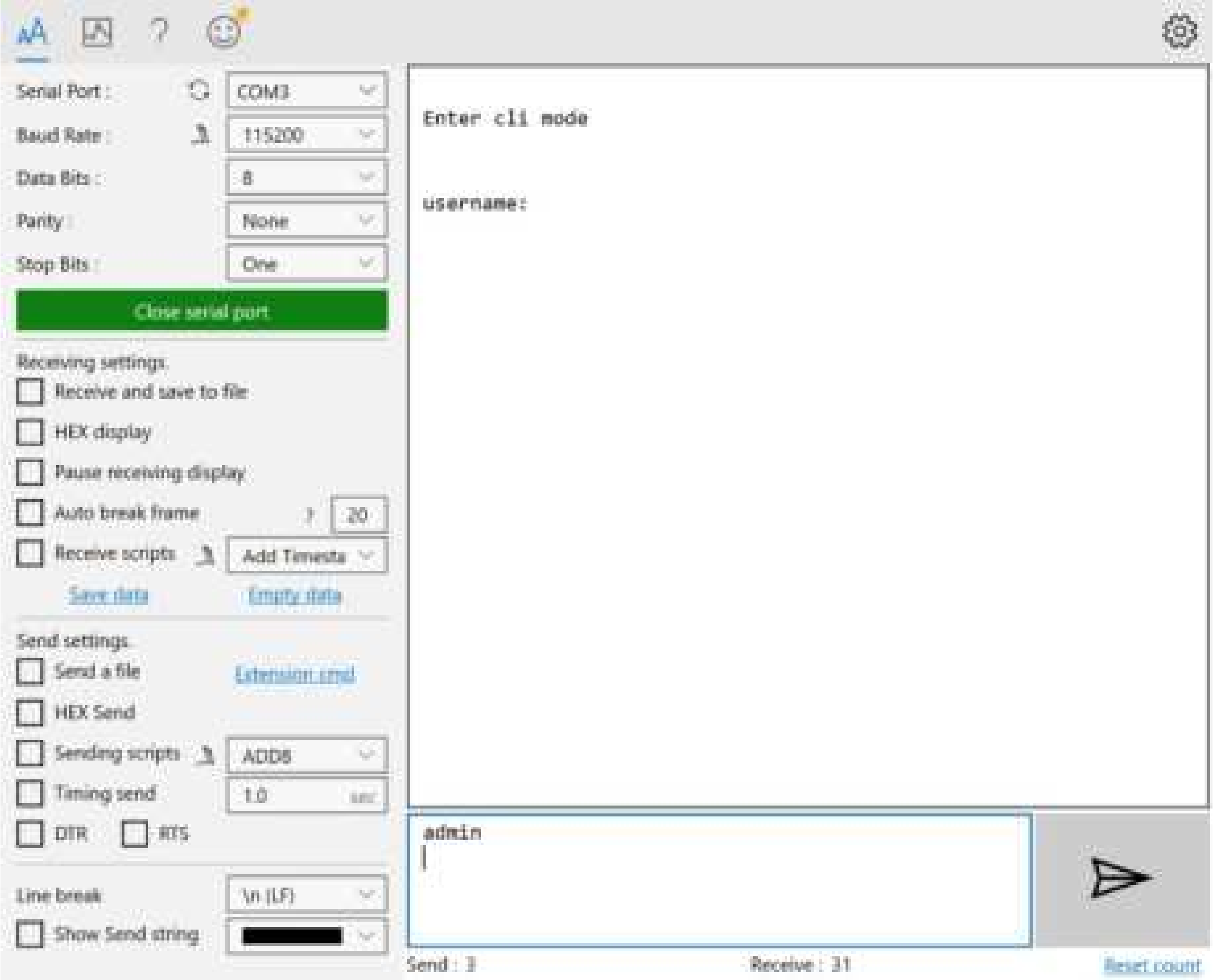
□ Show Send string

```
Enter cli mode


username:
```

```
+++
```

Send : 3 Receive : 31

Enter the Username admin (press the enter key), click "Send", enter the password 123456 (press the enter key), and click send to enter the command line mode.



Serial Port : COM3

Baud Rate : 115200

Data Bits : 8

Parity : None

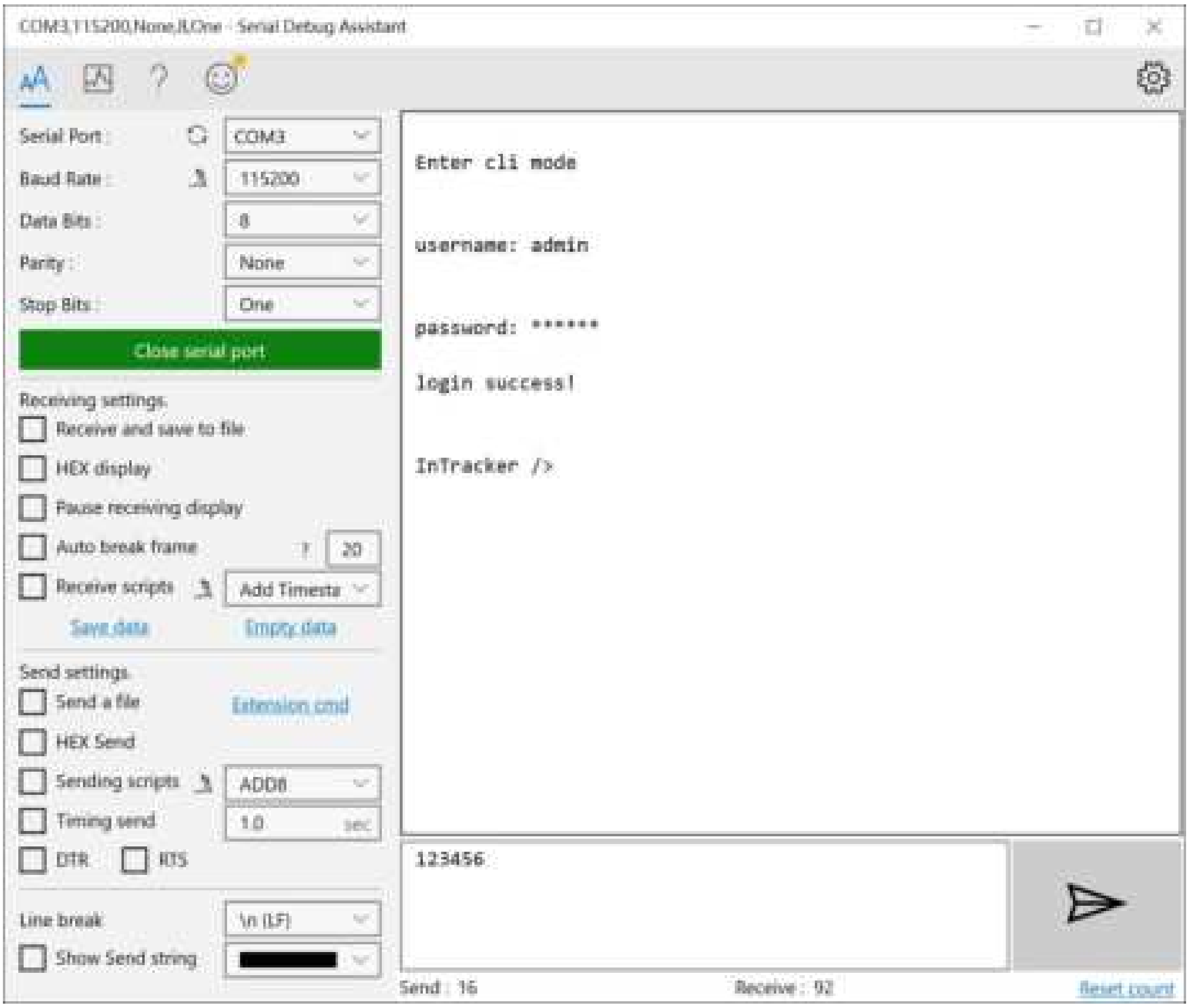
Stop Bits : One

```
Enter cli mode


username:
```

```
admin
```

Send : 3

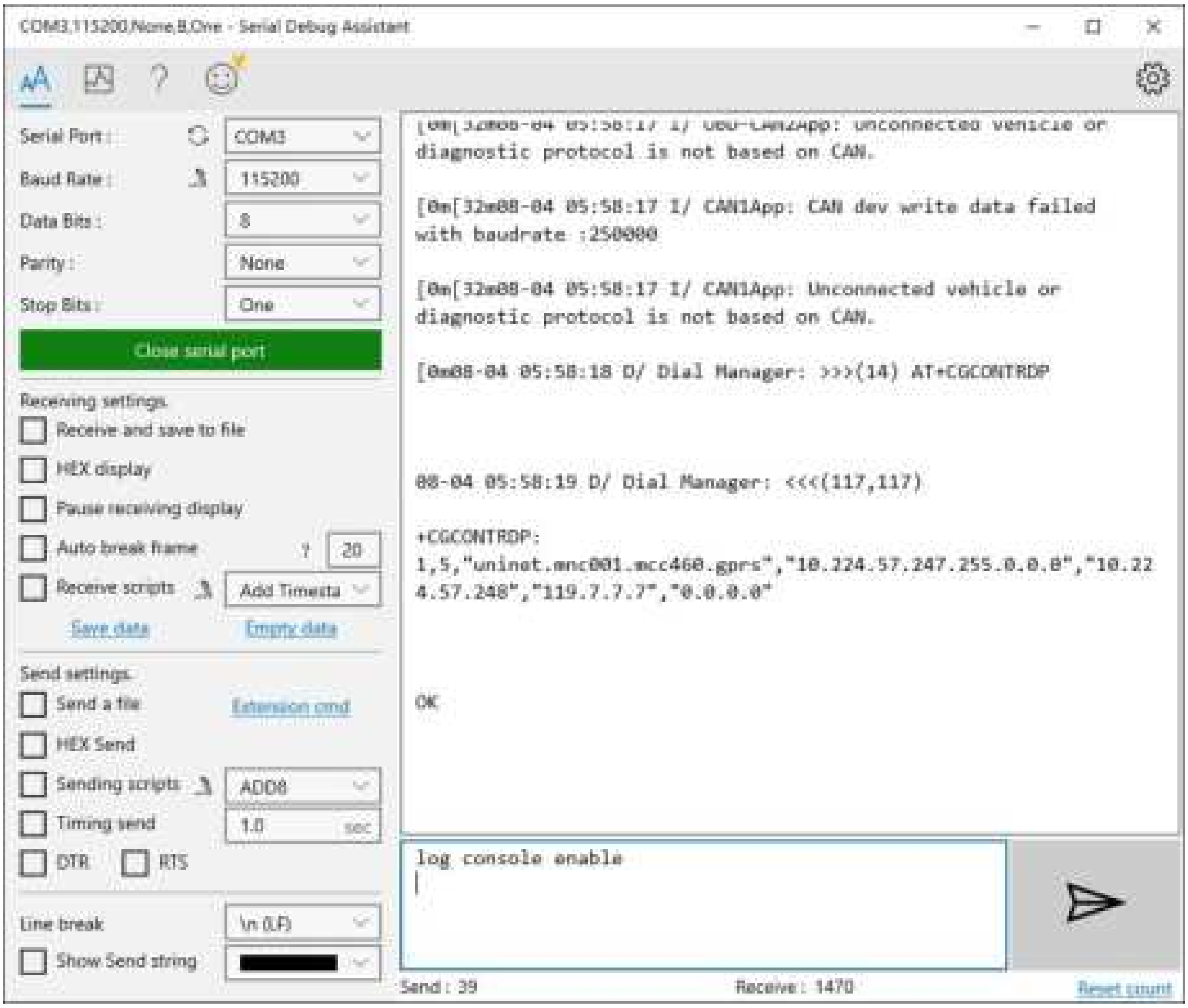
Receive : 31



```
Enter cli mode

username: admin

password: ******
login success!

InTracker />
```

```
123456
```

1. Enable the log function. In the send text box, enter “log console enable” (press the enter key) and click "Send". The following screenshot shows the log information in the receive window.



COM3,115200,None,8,One - Serial Debug Assistant

Serial Port : COM3
Baud Rate : 115200
Data Bits : 8
Parity : None
Stop Bits : One

Receiving settings
□ Receive and save to file
□ HEX display
□ Pause receiving display
□ Auto break frame ? 20
□ Receive scripts Add Timesta

Send settings
□ Send a file

□ HEX Send
□ Sending scripts ADD8
□ Timing send 1.0 sec
□ DTR □ RTS

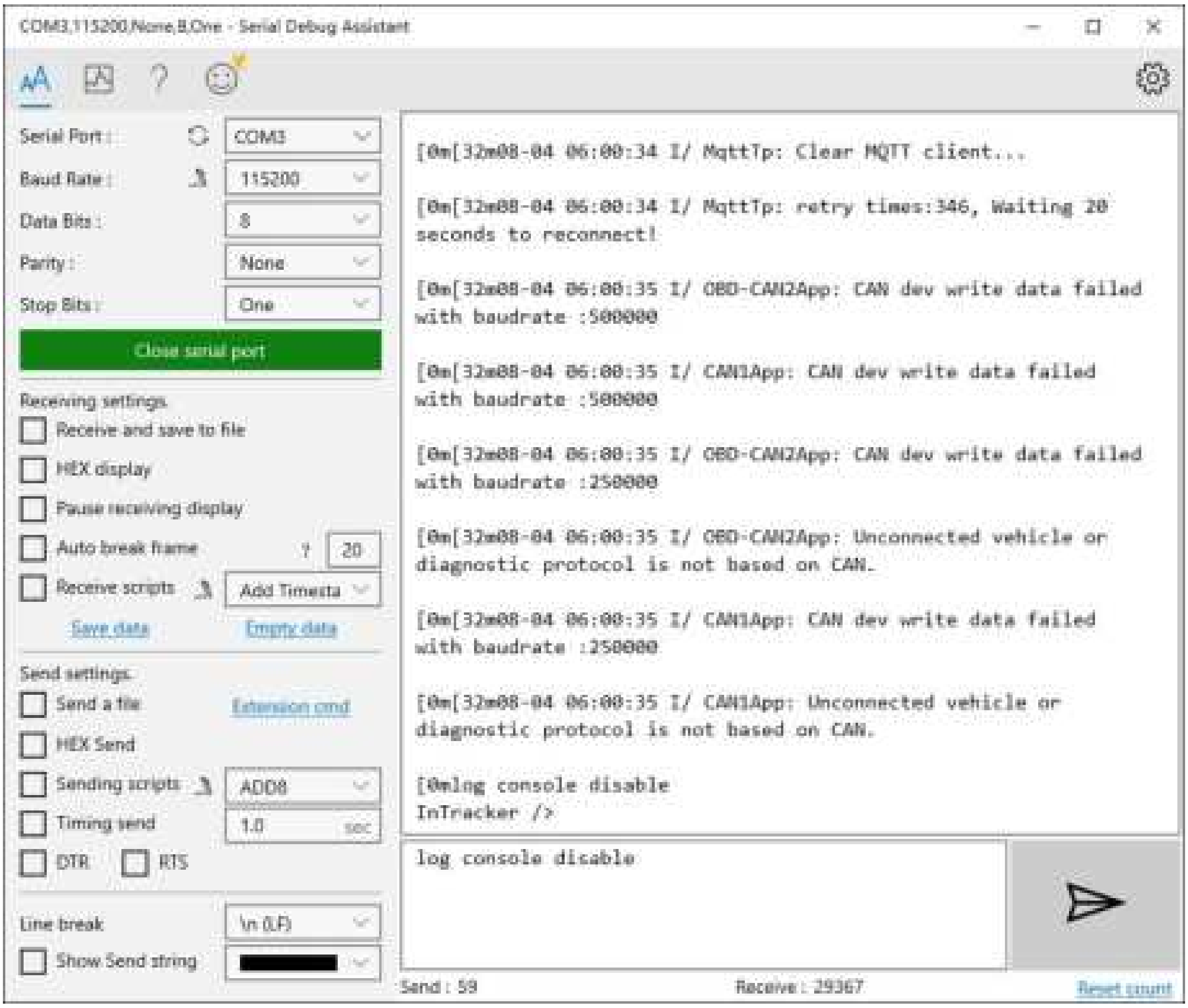
Line break \n (LF)
□ Show Send string

```
[0m[32m08-04 05:58:17 I/ OBD-CAN2App: Unconnected vehicle or
diagnostic protocol is not based on CAN.

[0m[32m08-04 05:58:17 I/ CAN1App: CAN dev write data failed
with baudrate :250000

[0m[32m08-04 05:58:17 I/ CAN1App: Unconnected vehicle or
diagnostic protocol is not based on CAN.

[0m08-04 05:58:18 D/ Dial Manager: >>>(14) AT+CGCONTRDP



08-04 05:58:19 D/ Dial Manager: <<<(117,117)

+CGCONTRDP:
1,5,"uninet.mnc001.mcc460.gprs","10.224.57.247.255.0.0.0","10.22
4.57.248","119.7.7.7","0.0.0.0"



OK
```

```
log console enable
```

Send : 39 Receive : 1470

1. Close log function, write “log console disable” (press the enter key) in the send text box and click ″Send″. The receive window stops receiving logs.



COM3,115200,None,8,One - Serial Debug Assistant

Serial Port : COM3

Baud Rate : 115200

Data Bits : 8

Parity : None

Stop Bits : One

Close serial port

Receiving settings

□ Receive and save to file

□ HEX display

□ Pause receiving display

□ Auto break frame ? 20

□ Receive scripts Add Timesta

Save data Empty data

Send settings

□ Send a file Extension cmd

□ HEX Send

□ Sending scripts ADD8

□ Timing send 1.0 sec

□ DTR □ RTS

Line break \n (LF)

□ Show Send string

```
[0m[32m08-04 06:00:34 I/ MqttTp: Clear MQTT client...

[0m[32m08-04 06:00:34 I/ MqttTp: retry times:346, Waiting 20
seconds to reconnect!

[0m[32m08-04 06:00:35 I/ OBD-CAN2App: CAN dev write data failed
with baudrate :500000

[0m[32m08-04 06:00:35 I/ CAN1App: CAN dev write data failed
with baudrate :500000

[0m[32m08-04 06:00:35 I/ OBD-CAN2App: CAN dev write data failed
with baudrate :250000

[0m[32m08-04 06:00:35 I/ OBD-CAN2App: Unconnected vehicle or
diagnostic protocol is not based on CAN.

[0m[32m08-04 06:00:35 I/ CAN1App: CAN dev write data failed
with baudrate :250000

[0m[32m08-04 06:00:35 I/ CAN1App: Unconnected vehicle or
diagnostic protocol is not based on CAN.

[0mlog console disable
InTracker />
```

```
log console disable
```

Send : 59 Receive : 29367 Reset count

1. If you need to link the configuration tool after exiting the serial port, write “exit” (press the enter key) in the send text box, click ″Send″ (used to exit the CLI mode), and then close the serial port. Or you wait for 180 seconds when the device automatically exits the CLI mode.

According to RSS-GEN section 6.8

For licence-exempt equipment with detachable antennas, the user manual shall also contain the following notice in a conspicuous location:

This radio transmitter 11594A-VT2FQ33 and 11594A-VT2FQ02 has been approved by

Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Antenna type and gain for HVIN:FQ33,FQ33-BAT,FQ02,FQ02-BAT

Ceramic Chip Antenna with maximum antenna gain 3.2dBi

Antenna type and gain for HVIN:FQ33-ANT,FQ33--ANT-BAT,FQ02-ANT,FQ02-ANT-BAT

Patch Antenna with maximum antenna gain 1.23dBi

Note: -ANT represents external antenna(Patch Antenna), without adding - ANT represents internal antenna(Ceramic Chip Antenna), - BAT represents internal battery, without adding - BAT represents no battery.

FCC STATEMENT

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device , pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment

off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure

The equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands is country dependent and firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

IC STATEMENT

This device complies with Industry Canada license-exempt RSS standard(s): Operation is subject to the following Two conditions:

(1) this device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation

of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareildoit accepter tout brouillage radioélectrique subi, même si le brouillage est

susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)

Avis d'Industrie Canada

Le présent appareil est conforme aux CNR d'industrie Canada applicables aux appareils radio exem pts de licence L'exploitation est autorisée aux deux conditions suivantes:

1) l'appareil ne doit pas produire de brouillage; et

2) l'utillsateur de l'appareil doit accepterbrouillage radioélectrique subi meme si le brouillage est susceptible d'encompromettre le fonctionnement. mauvais fonctionnement de l'appareil.

Cet appareil numériquie de la classe B est conforme à la norme NMB-003 du Canada.

CAN NMB-3 (B)

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.