SD6200

WebUI User Manual and Safety Information

About This Manual

Thank you for choosing this mobile device. To keep your device in its best condition, please read this manual and keep it for future reference.

Notice

This manual has been designed with the utmost care to ensure the accuracy of its content. However, all statements, information and recommendations contained therein do not constitute a warranty of any kind, either expressed or implied. Please refer to *For Your Safety* to be sure to use your phone properly and safely.

Disclaimer

Images and screenshots used in this manual may differ from the actual product. Content in this manual may differ from the actual product or software.

Trademarks

Other trademarks and trade names are the property of their respective owners.

Version No.: R1.0

Edition Time: June 22 2018

Getting Started 5

Know Your OBD2 (On-Board Diagnostic) Device 5
Status LED Indicator 6
Reset the OBD2 Device 7
Restart the OBD2 Device 7
Installing the micro-SIM Card. 8

Installing your OB2 Device 10

Manage Your OBD2 Device and Settings 12

Connect Devices to Your OBD2 Device's Wi-Fi 12
Connect a wireless device manually 12

Use Your OBD2 Device 13

4G Mobile Hotspot Configuration Page 13

Security Credentials 14

Manage Wi-Fi 14

View Connected Devices 14
Set Maximum Number of Connected Devices 15
Add / removed Devices 17

Security 18

Change Wi-Fi Network Name and Password. 18
Change 4G Mobile Hotspot Configuration Page Access Settings 19
Change Wi-Fi Security Types 20
Configure Data Network Options 21

Advanced Settings 23

Manage Wi-Fi 23

Change Advanced Settings 24

View WAN Information 24
Enable Port Mapping 24
Enable MAC/ IP/Port Filtering 24
Configure APN details 25

Troubleshooting 27

Compatible vehicles 28

Working Voltage 28

Specifications 29

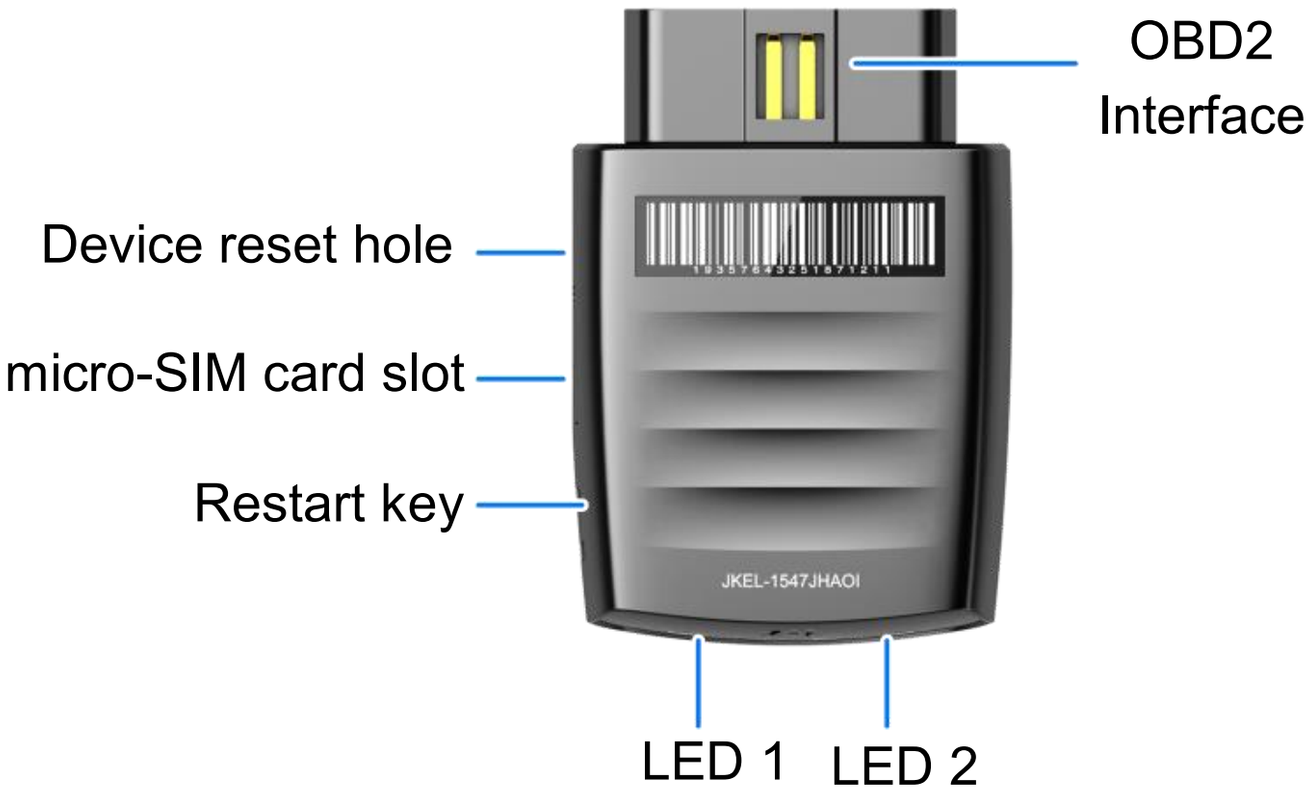
Regulatory and Safety Information 30

Warranty 33

Getting Started

Know Your OBD2 (On-Board Diagnostic) Device

Your OBD2 device enables you to create a Wi-Fi network in your vehicle. You can use that Wi-Fi network to connect your smartphone and other Wi-Fi capable devices to your network provider's mobile broadband network and connect to the Internet.



Status LED Indicator

LED INDICATOR	LED STATUS
LED 1 (Power)	Green blinking
The device is being powered by the internal battery	
LED 1 (Power)	Green solid
The device is being powered by the vehicle	
LED 2 (Signal)	Red solid
The device is on but is not connected to the cellular network	
LED 2 (Signal)	Green solid
The device is connected to the 4G network but no data is being transferred	
LED 2 (Signal)	Green blinking
The device is connected to the 4G LTE network and data is being transferred	

Reset the OBD2 Device

You can reset the OBD2 device to the factory setting on the OBD2 device or the 4G Mobile Hotspot configuration page. (This is useful if you have lost your Admin Login for the 4G Mobile Hotspot configuration page.)

NOTE:

If you reset the modem to factory settings, all your customizations will be lost. If you want to keep them, save them before doing the reset, and then restore them afterward. Note: When you reset the OBD2 device, any currently connected devices will lose access and will have to be reconnected after the OBD2 device restarts.

On the OBD2 device:

Insert a pin into **Reset hole** and hold for about 3 seconds until the LED1 indicator turns red.

After the device has reset, reconnect Wi-Fi devices.

On the 4G Mobile Hotspot configuration page:

- Log in as Administrator.
- Select **Settings > Device Settings**.
- Select **Reset**.

Restart the OBD2 Device

You can restart the OBD2 device by pressing the restart key.

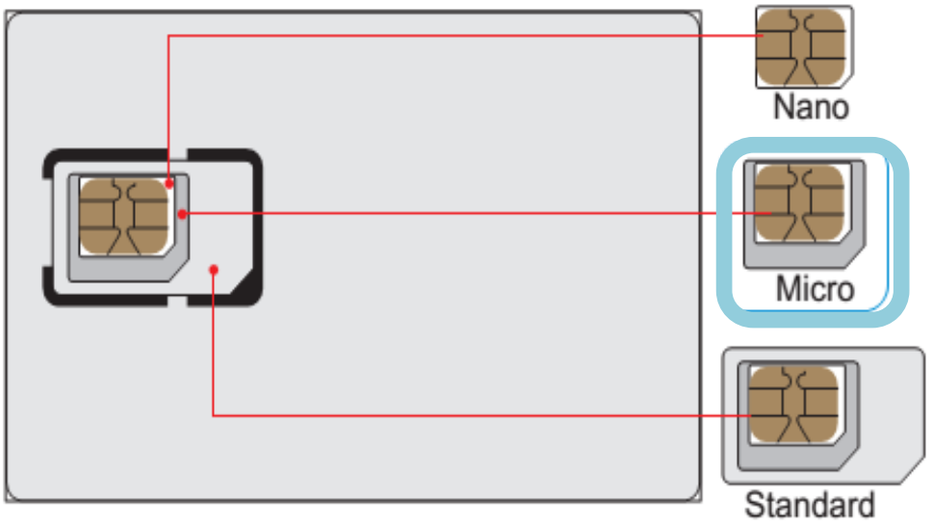
Installing the micro-SIM Card.

1. Insert the tip of the tray eject tool to eject the SIM card tray.

2. Place the micro-SIM card on the tray with the gold-colored contacts facing down and slide the tray back into place.

WARNING!

To avoid damage to the device, do not use any non-standard micro-SIM card cut from a card. You can get a standard micro-SIM card from your service provider.



This device uses a Micro-SIM card Only.

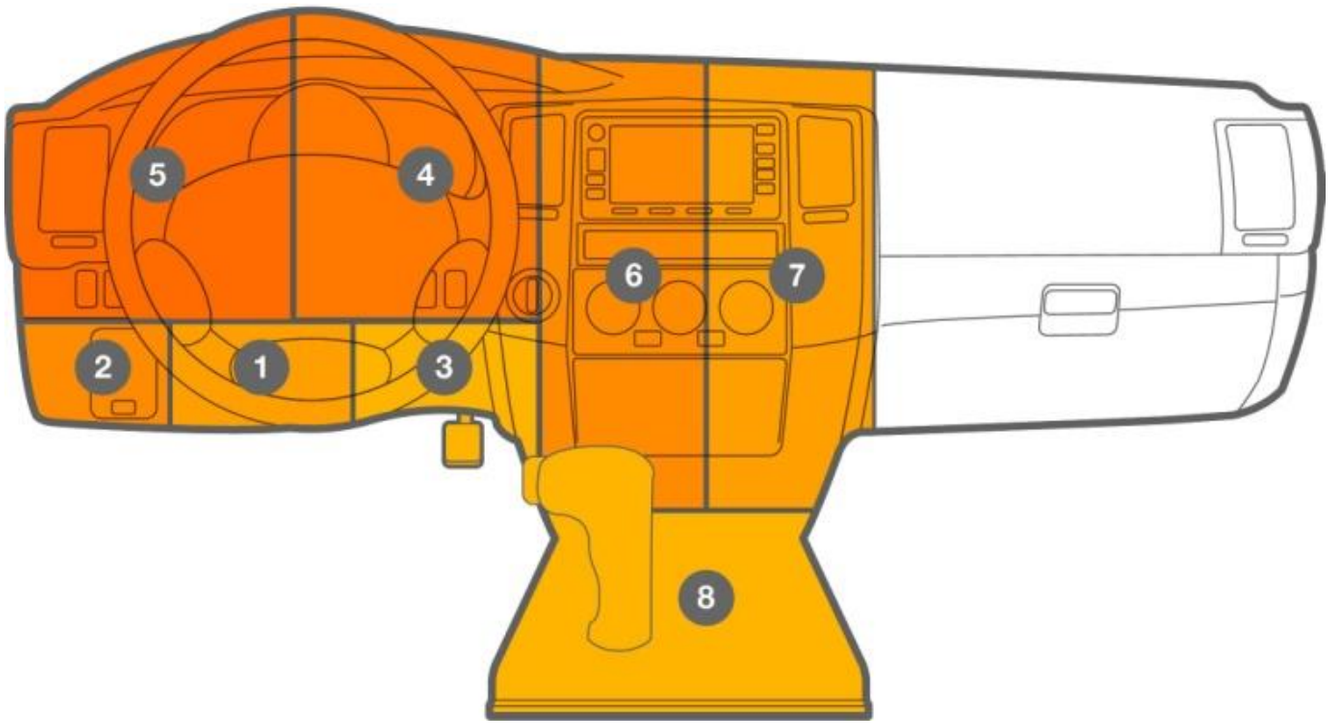
Installing your OB2 Device

- Make sure your vehicle is parked outside in a safe location and the engine is turned off.
- Connect your OBD2 device into the OBD connector port (**or into the extension cable if it is required – not included**). Ensure that your OBD2 device is connected in the correct direction.

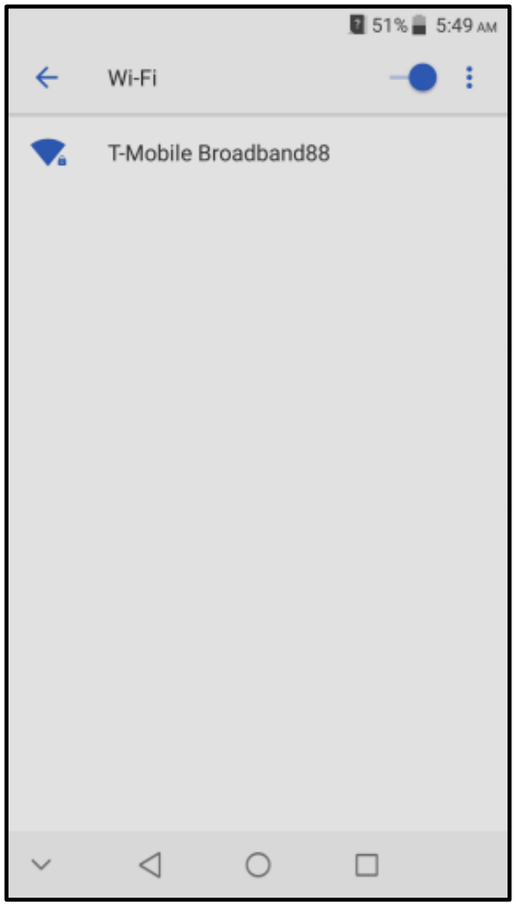
NOTE:

Gently insert your OBD2 device as to avoid damage to the device.

- OBD interface connect with OBD connector on your vehicle to power on your OBD2 device. The OBD (On-Board Diagnostics) connector is usually located on or under the dash, on the driver's side. Other possible locations are at the center console area or inside the glove compartment.



- Start your vehicle’s engine and let it run for at least 30 seconds.
- Once powered up, your OBD2 device automatically searches for and connects to your network provider’s mobile broadband network.
- Connect your smartphone or other WPS-enabled devices to your network.
    - Use your normal Wi-Fi application on the client to search for the available wireless network.



    - Select the Wi-Fi network name.
    - Input the Wi-Fi network password, as it displays on the label on your OBD2 device.
- Launch your browser to surf the Internet.

Manage Your OBD2 Device and Settings

You can use the 4G Mobile Hotspot configuration page to manage your OBD2 device and change settings.

NOTE:

To personalize the OBD2 device and change settings, use a Wi-Fi enabled device to connect to the OBD2 device and then use a browser to display the 4G Mobile Hotspot configuration page (**http://192.168.0.1**).

Log in as Administrator to make changes. (The default Admin Login is: **admin**).

Connect Devices to Your OBD2 Device's Wi-Fi

You can connect up to 10 wireless devices such as smartphones, laptops, tablets, digital cameras, printers, gaming consoles, and digital picture frames to your OBD2 device's Wi-Fi network. (See *Set maximum number of connected devices* for instructions on setting connections for the Wi-Fi network.)

You can connect a wireless device to your Wi-Fi network by typing the Wi-Fi password.

Connect a wireless device manually

To connect a wireless device to your OBD2 device's Wi-Fi network, see *Connect to the Internet*.

Use Your OBD2 Device

This chapter describes the main features of the web interfaces for managing your OBD2 device.

4G Mobile Hotspot Configuration Page

You must be logged in as Administrator to change settings and view detailed information.

- Default homepage URL — (**http://192.168.0.1**)
- Default Administrator Login — **admin**

To log in as Administrator:

1. On the 4G Mobile Hotspot configuration page, place your cursor in the **Password** field and type **admin** (the default login).

2. Select **Login**.

Security Credentials

The OBD2 device uses two passwords:

- **Wi-Fi password** —used to authenticate wireless devices to your mobile hotspot network. It is unique to your mobile hotspot and can be found printed on a label on the mobile hotspot. If you want to change the Wi-Fi password, see Change Wi-Fi Network Name and Password on page 12.
- **Admin Login** — used to log into the 4G Mobile Hotspot configuration page as Administrator. You must be logged in as Administrator to use certain features and to make changes to your OBD2 device settings. The default Admin Login is admin. The Admin Login can be changed to 4–32 characters.

You can change these passwords on the 4G Mobile Hotspot configuration page (**http://192.168.0.1**).

Manage Wi-Fi

View Connected Devices

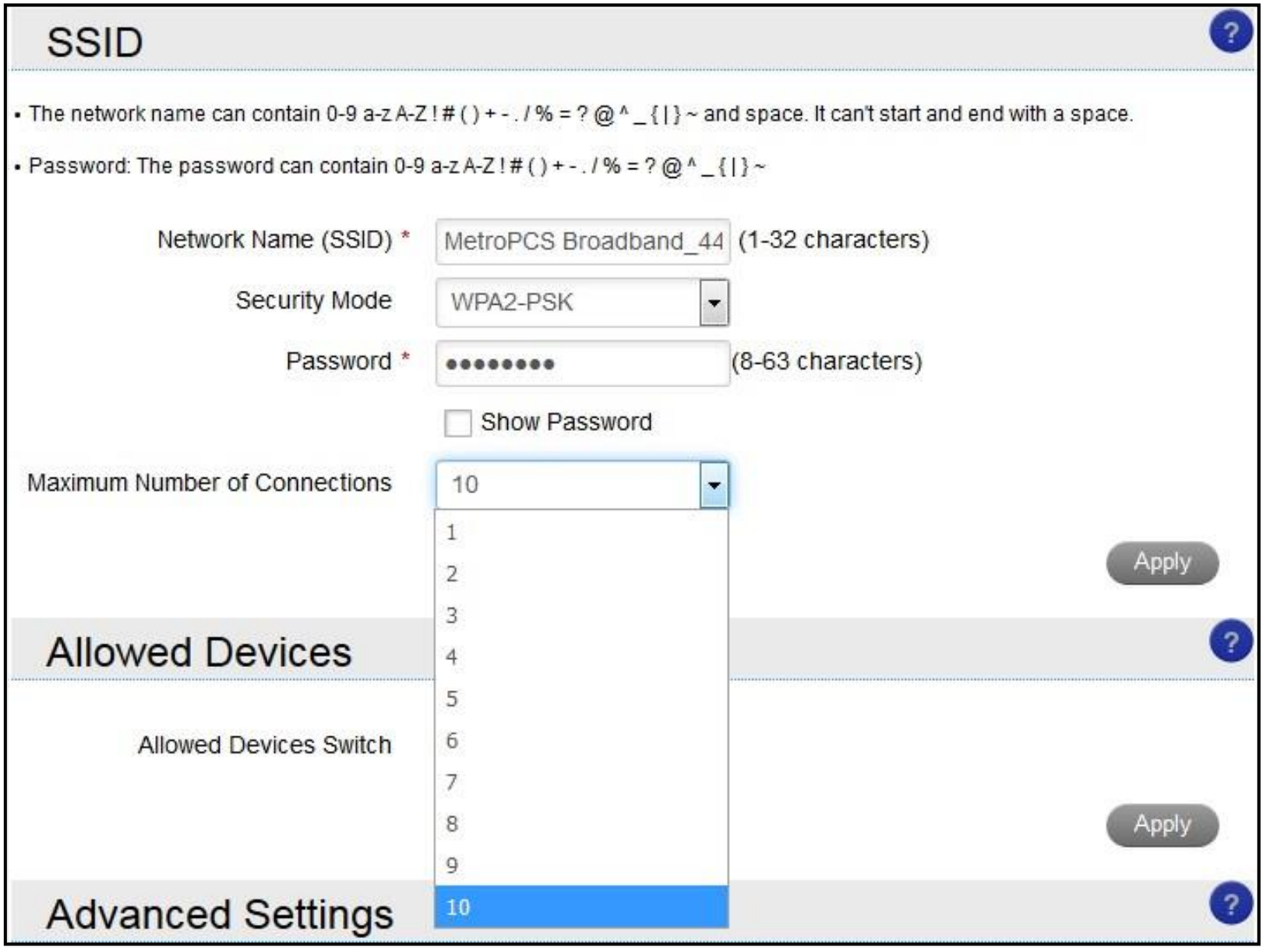
You can view a list of devices connected to your OBD2 device on the 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Home**. A list of devices Connected to the Wi-Fi network appears in the **Connected Devices** section. You can view the IP and MAC addresses of the devices.

Set Maximum Number of Connected Devices

You can connect up to 10 wireless devices to your OBD2 device. You can customize the number of devices from the 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Settings**.
- In the **SSID** section, select drop-down box beside **Maximum Number of connections** to set the number of connections available for the Wi-Fi network.



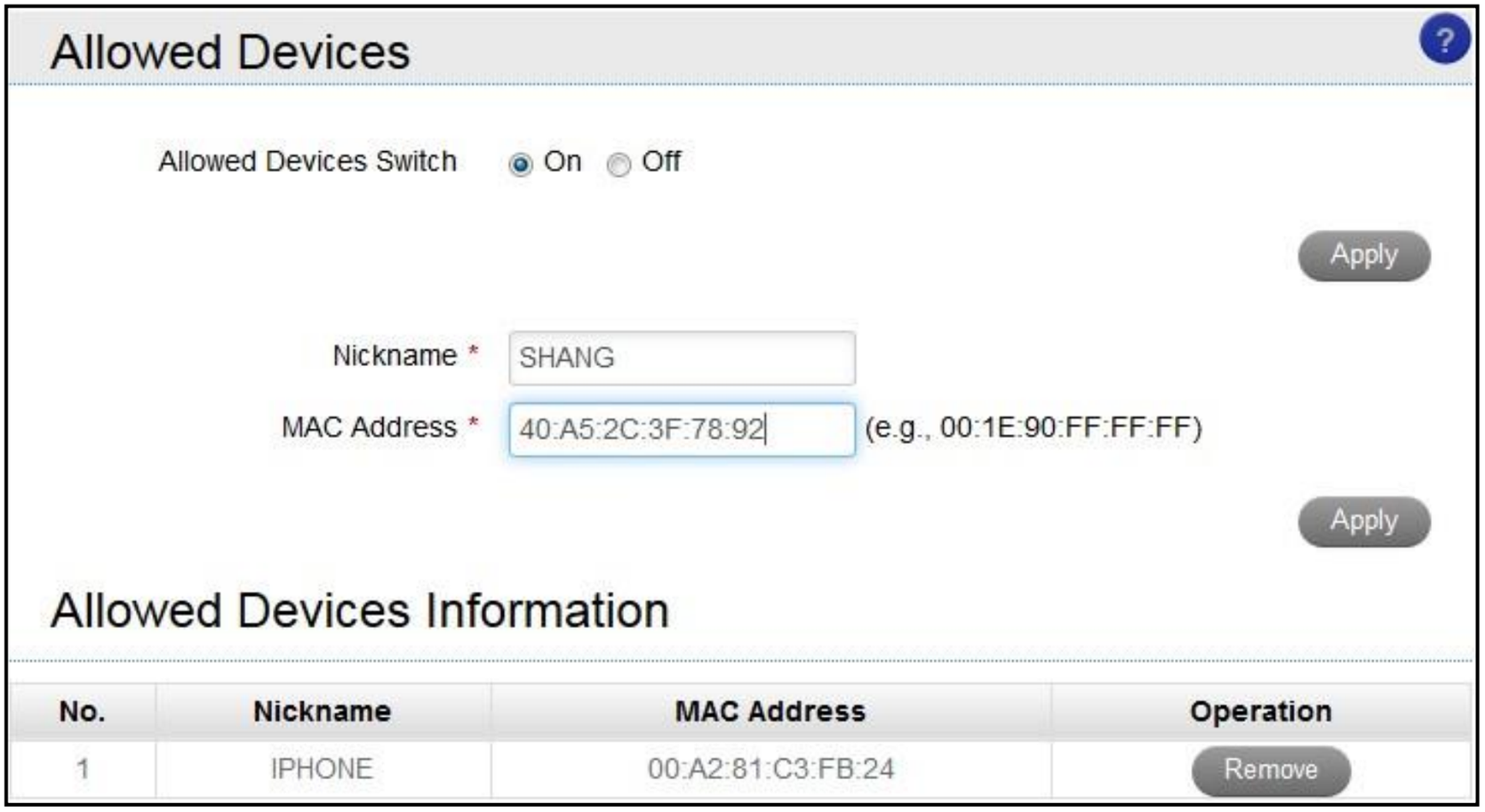
- Select **Apply.**

Add / removed Devices

You can prevent other device from connecting to the OBD2 device, only the MAC address listed in the **Allowed Devices Information** section can access your OBD2 device. You can add / remove a device from the 4G Mobile Hotspot configuration page.

To add a device:

- Log in as Administrator.
- Select **Settings > Wi-Fi Settings**.
- Set **Allowed Devices Switch** to **On** and select **Apply**.
- Enter the **Nickname** and **MAC Address**.
- Select **Apply.**



To remove a device:

- Log in as Administrator.
- Select **Settings > Wi-Fi Settings**.

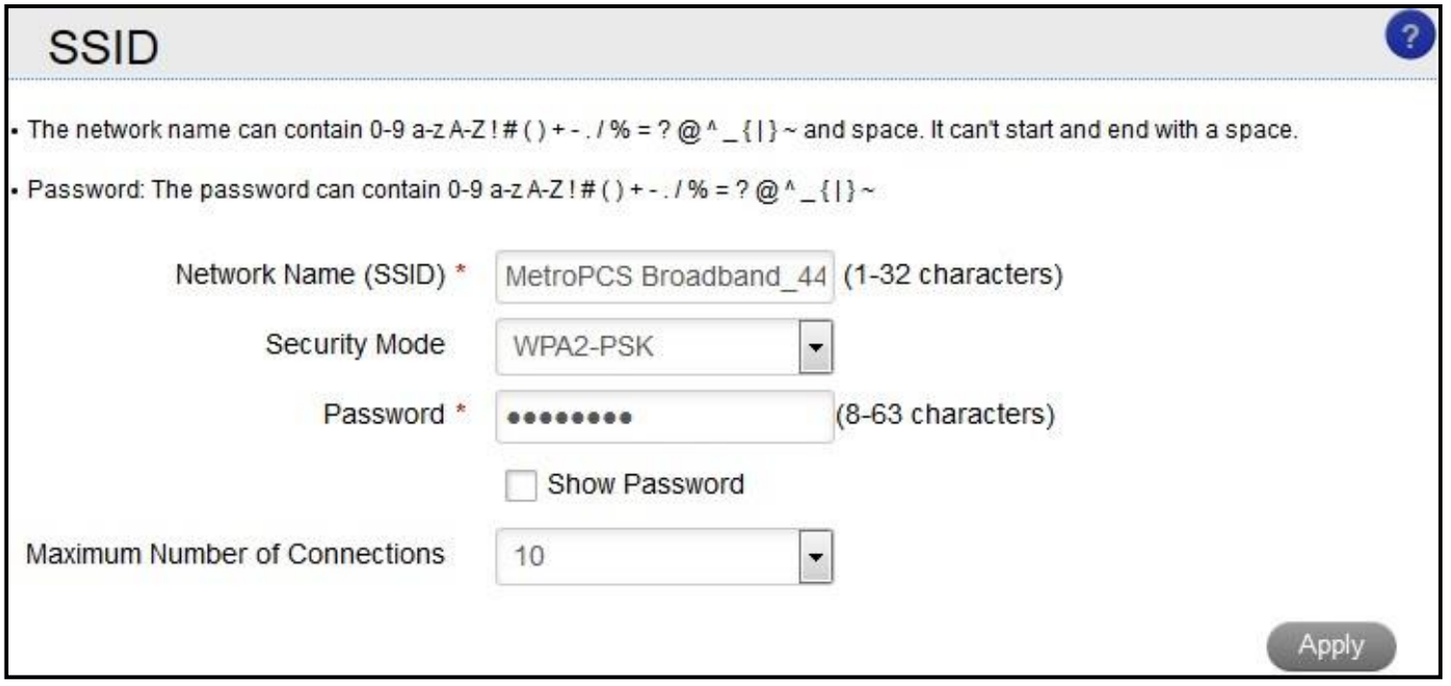
Select **Remove** next to the device in the **Add / removed Devices** section.

Security

Change Wi-Fi Network Name and Password.

You can customize the network name and password for the Wi-Fi network from the 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Settings > Wi-Fi Settings**.
- Change the Wi-Fi network name and / or password in the **SSID** section.



- **Select Apply**

NOTE:

If you changed the Wi-Fi network name or password, all connected devices will be disconnected and must reconnect.

Change 4G Mobile Hotspot Configuration Page Access Settings

You can customize the Admin Login used to access 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Settings > Device Settings**.

- If desired, change the Admin Login (maximum 32 characters).
- Select **Apply**.

NOTE:

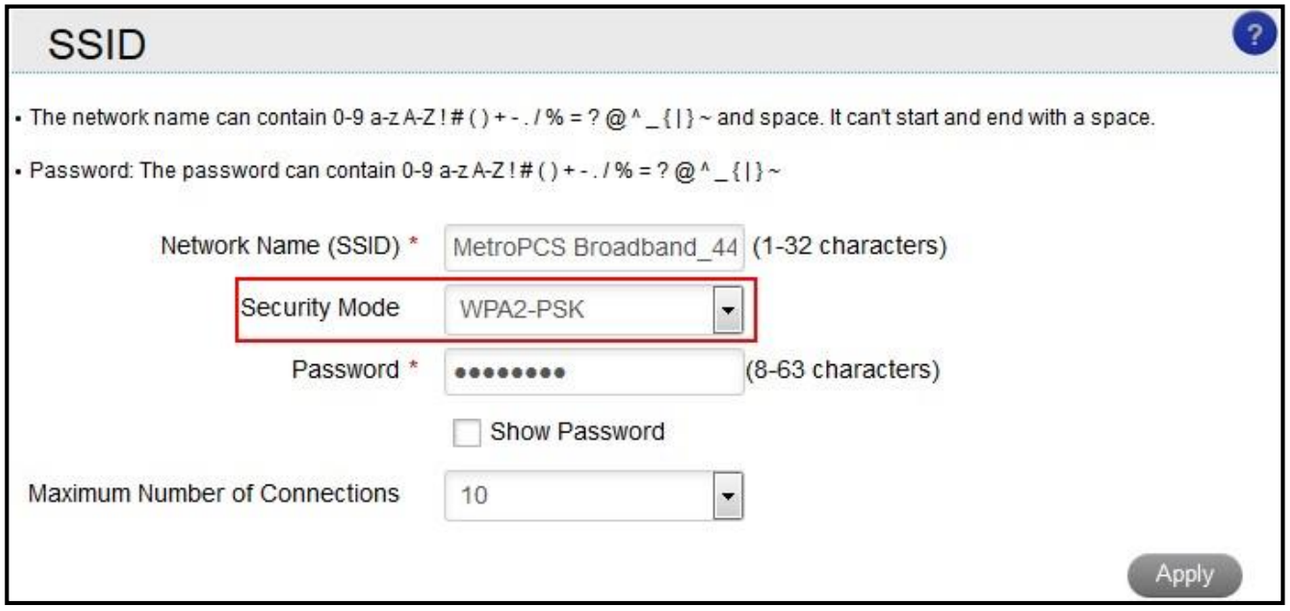
If you forget the Admin login, you need to perform a hardware reset.

Change Wi-Fi Security Types

You can set the OBD2 device's Wi-Fi security types from the 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Settings > Wi-Fi Settings**.
- Select the desired security types for the Wi-Fi network. (It is recommended that you use WPA2-PSK whenever possible.)
- The **Security Type** (the most common mode) are:

  - WPA2-PSK --other users can access your OBD2 device only if they enter the correct password (default)
  - WPA-PSK/WPA2-PSK-- WPA Pre-Shared Key (WPA-PSK).
  - SHARED-- Shared Key Authentication, a type of WEP Encryption.
  - OPEN--Not recommended. Anyone can access your Wi-Fi network without a password and you are responsible for charges incurred.

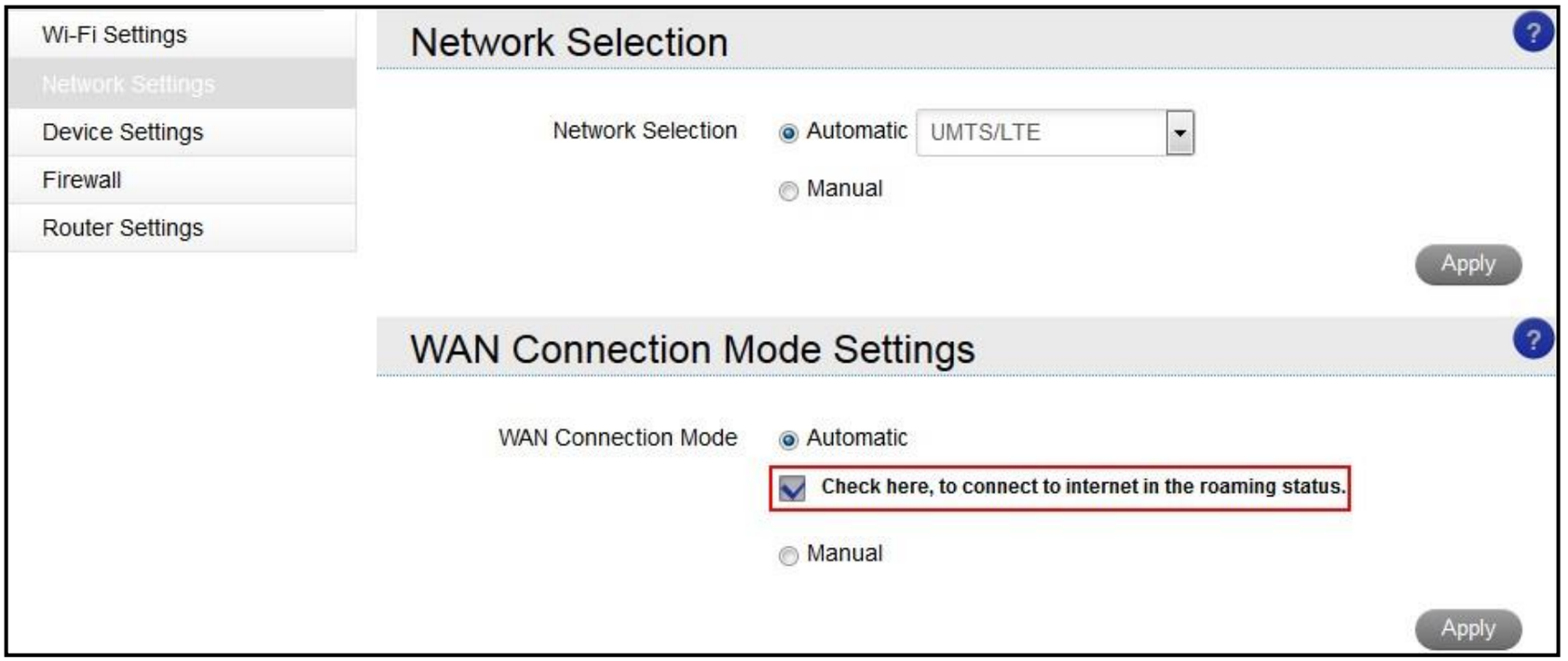


- Select **Apply**.
- Reconnect your Wi-Fi devices, if necessary, using the new Wi-Fi credentials.

Configure Data Network Options

You can set WAN connection mode and choose whether to allow the OBD2 device to be used when roaming internationally, from the 4G Mobile Hotspot configuration page.

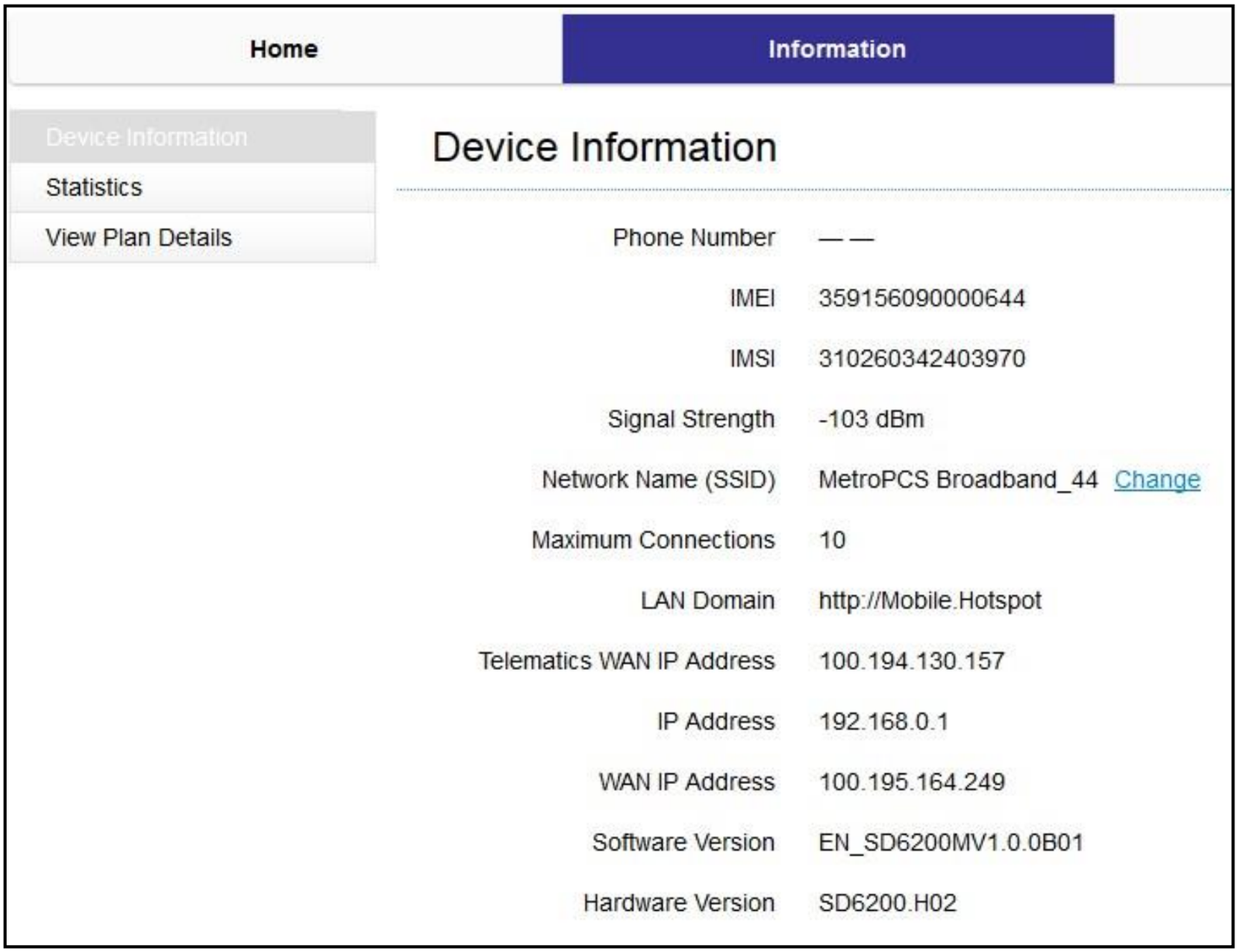
- Log in as Administrator.
- Select **Settings > Network Settings**.
- Choose the appropriate option:
  - To access the Internet in automatic or manual mode, select **Automatic** / **Manual** in **WAN Connection Mode Settings** section, and select **Apply**.
  - To enable / disable international roaming, check or uncheck the box under **Automatic** in **WAN Connection Mode Settings** section, and select **Apply**.



View details

You can view details about your OBD2 device, such as the wireless number, data usage (not accurate for billing purposes), hardware version, and IMEI from the 4G Mobile Hotspot configuration page.

- Log in as Administrator.
- Select **Information**.



Advanced Settings

This chapter provides information on how to configure advanced settings for various aspects of the device such as Wi-Fi settings, WAN settings, router settings, etc.

Manage Wi-Fi

Set Wi-Fi Network Mode

To configure the Wi-Fi network mode:

- On the 4G Mobile Hotspot page, log in as Administrator.
- Select **Settings** > **Wi-Fi Settings**.
- Select the desired option in the **Advanced Settings** section.

Network Mode -- The WLAN protocol being used. The recommended value depends on the band range selected and then select **Apply**.:

- 802.11 b/g/n
- 802.11 b only
- 802.11 g only
- 802.11 b/g

Change Advanced Settings

View WAN Information

At the top right of 4G Mobile Hotspot configuration page, you can view network information, such as the active network, connection status, signal strength, etc.

Enable Port Mapping

If your computer hosts a server, you can enable port mapping so that other users can access the server.

To enable port mapping:

- On the 4G Mobile Hotspot configuration page, log in as Administrator.
- Select **Settings > Firewall**.
- Select **Enable** beside Port Mapping Settings. The Port Mapping list will appear.
- Incoming traffic is forwarded to specific ports and devices on your network (using their local IP addresses).
- Identify the ports to forward--Enter the port forwarding information (the IP address, the Port range, the Protocol and the comment), then select **Apply**.

Caution: Port mapping creates a security risk. When not required, port mapping should be disabled.

Enable MAC/ IP/Port Filtering

You can enable or disable the MAC/IP/Port Filtering feature as needed to block certain Internet traffic. If this setting is enabled, you can then choose whether traffic is **Accepted** or **Dropped** by default by selecting the appropriate option from the Default Policy dropdown.

To enable port filtering:

- On the 4G Mobile Hotspot configuration page, log in as Administrator.
- Select **Settings**.
- Select **Firewall** > **Port Filtering** tab.
- Select the Default Policy:

Accepted– Internet traffic is allowed by default. Only traffic from the selected applications will be blocked from accessing the internet. Traffic is identified by port numbers. Some applications are pre-defined. You can define additional applications by clicking the "**Add Custom Application**" button, but you need to know details of the traffic used and generated by the applications you wish to define. In particular, you need to know the port numbers and the protocol (TCP, UDP) used by outgoing traffic.

Dropped – Internet traffic is blocked by default. Only traffic from the selected pre-defined or custom applications can access the internet.

Select **Apply**.

Configure APN details

The APN is checked to determine the type of network connection to establish.

Your OBD2 device comes preconfigured with the APN (Access Point Name) for AT&T.

To add an APN for another network:

- On the 4G Mobile Hotspot configuration page, log in as Administrator.
- Select **Settings** > **Network Settings**.
- Select **Manual** in the **APN** section.
- Select **Add New**.

In the blank line, enter the profile name, APN (obtained from your carrier).

Select the network **Authentication** mode. The options are:

- None (default)
- CHAP
- PAP

Enter the Username and Password, if these are required for the wireless network.

Click **Apply**.

To select the APN entry to use:

From the drop-down box beside **Profile Selection**, select the desired APN to use.

To remove an APN entry:

Select the APN you want to remove and select **Delete**.

Enable DMZ

In a DMZ (demilitarized zone) network configuration, a computer runs outside the firewall in the DMZ. This computer intercepts incoming Internet traffic, providing an extra layer of protection for the rest of the network.

To enable DMZ and designate a computer to screen incoming traffic:

- On the 4G Mobile Hotspot configuration page, log in as Administrator.
- Select **Settings > Firewall**.
- Select **Enable** beside DMZ in **DMZ Settings** section.
- In the DMZ IP Address field, enter the IP address of the computer you want to have in the DMZ.
- Select **Apply**.

Set Router options

- To set the OBD2 device's LAN options:
- On the 4G Mobile Hotspot configuration page, log in as Administrator.
- Select **Settings > Router Settings**.
- Enter the desired information in each section.
- If the DHCP Server is enabled, it automatically assigns an IP address to each device on the network and manages their configuration information.
- Select **Apply**.

Troubleshooting

Problem	Suggested Solution
Cannot establish the Wi-Fi connection between your device and client.	• Refresh network list and select the correct SSID. • Check the IP address to make sure your client can obtain an IP address automatically in the Internet protocol (TCP/IP) properties. • Type the correct network key (Wi-Fi password) when you connect to your OBD2 device.
The client connected to the device cannot access the Internet.	• Make sure your micro-SIM card is available. • Ensure that the roaming status is turned on. Once turned on and your OBD2 device connected to mobile network, the LED2 indicator turns green. Select **Settings** > **Network Settings > WAN Connection Mode Settings** on the 4G Mobile Hotspot configuration page to check the box under **Automatic**. • Contact your service provider.
Cannot visit the 4G Mobile Hotspot configuration page.	• Enter the correct address. The default address is http://192.168.0.1. • Only use one network adapter in your PC. • Do not use any proxy server.

About the password	• Select **Settings** > **Wi-Fi Settings** on the 4G Mobile Hotspot configuration page to check the Wi-Fi Network password or check the label on the device to get them. • If you changed the password and forgot the new password, you need to reset the device to the factory default settings.

Compatible vehicles

Electric cars and other vehicles, like heavy duty trucks, motorcycles and ATVs, are not compliant with your OBD2 device.

Working Voltage

Your device is a Wi-Fi hotspot without a battery. The power is supplied through the vehicle's OBD II connector port. The voltage range is from 9V to 16V. If the OBD II voltage drops to 11.5V, your device will go into Protection mode to ensure that the car battery remains capable of restarting.

Mode	Average current (mA)
Power Saving	10.5
LTE network searching	61.3
LTE MAX power (maximum transmission power)	B2@maxpower=298 B4@maxpower=305 B5@maxpower=322 B12@maxpower=300

Specifications

Mechanical specifications

Dimensions	75.2mm*52.2mm*28.2mm

Supported RF bands

Technology	Bands
LTE	Band 2 Band 4 Band 5 Band 12
UMTS/HSPA+	Band 2 Band 4

Regulatory and Safety Information

To the Owner

- Operating your device may interfere with medical devices such as hearing aids and pacemakers. Please always keep them more than 20 centimeters away from such medical devices when they are powered on. Stop using your device if necessary. Consult a physician or the manufacturer of the medical device before using your device.
- Be aware of the usage limitation when using your device at places such as oil warehouses or chemical factories, where there are explosive gases or explosive products being processed. Stop using your device if required.
- The use of electronic transmitting devices is forbidden in aircrafts, at petrol stations and in hospitals. Please observe and obey all warning signs and Stop using your device in these conditions.
- Store your device out of the reach of little children. Your device may cause injury if used as a toy.
- Do not touch the metallic parts of your device. Otherwise it will affect your device's performance.

Using Your Device

- Please use original accessories or accessories that are authorized. Using any unauthorized accessories may affect your device' s performance and violate related national regulations about telecom terminals.
- Avoid using your device near or inside metallic structures or establishments that can emit electromagnetic waves. Otherwise it may influence signal reception.
- Your device is not waterproof. Please keep it dry and store in a shady and cool place.
- Do not use your device immediately after a sudden temperature change. In such case, it will produce dew inside and outside your device, so don't use it until it becomes dry.
- Handle your device carefully. Do not drop, bend or strike it. Otherwise your device will be damaged.
- No dismantling by non-professionals and only qualified technicians can undertake repair work.

- Operating temperature range of-10°C ~ +55°C and humidity range of 5% ~ 95% are recommended.

Radio Frequency (RF) Energy

This device meets the government's requirements for exposure to radio waves.
This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government:
FOR MOBILE DEVICE USAGE (>20 cm/low power)
Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.
FCC ID: 2APQU-SD6200.

FCC Compliance
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.
Caution: Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
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, 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: The country code selection is for non-U.S. models only and is not available to all U.S. models. Per FCC regulation, all Wi-Fi products marketed in the U.S. must be fixed to U.S.

Warranty

Consumer Limited Warranty

KONNECTONE (“Seller”) offers you a limited warranty that the enclosed product or products (the “Product”) will be free from defects in material and workmanship for a period that expires one year from the date of sale of the Product to you, provided that you are the original end-user purchaser of the Product and provided that your purchase was made from a supplier authorized by the Seller. Transfer or resale of a Product will automatically terminate warranty coverage with respect to that Product. This limited warranty is not transferable to any third party, including but not limited to any subsequent purchaser or owner of the Product. This limited warranty is applicable to end users in the United States.

Seller will, at its sole and absolute discretion, either repair or replace a Product (which unit may use refurbished parts of similar quality and functionality) if found by Seller to be defective in material or workmanship, or if Seller determines that it is unable to repair or replace such Product, Seller will refund the purchase price for such Product, provided that the subject Product (i) is returned to a Seller authorized service center within the one year warranty period, and (ii) is accompanied by a proof of purchase in the form of a bill of sale or receipted invoice which evidences that the subject Product is within the one year warranty period. After the one-year warranty period, you must pay all shipping, parts and labor charges. In the event that the product is deemed un-repairable or has been removed from the list of products supported by the Seller, you will only be liable for shipping and labor charges.

This limited warranty does not cover and is void with respect to the following: (i) any Product which has been improperly installed, repaired, maintained or modified; (ii) any Product which has been subjected to misuse (including any Product used in conjunction with hardware electrically or mechanically incompatible or used with accessories not approved by Seller), abuse, accident, physical damage, abnormal operation, improper handling, neglect, exposure to fire or liquid; (iii) any Product operated outside published maximum ratings; (iv) cosmetic damage; (v) any Product on which warranty stickers or Product serial numbers have been removed, altered, or rendered illegible; (vi) cost of installation, removal or reinstallation; (vii) signal reception problems (unless caused by defects in material and workmanship); (viii) damage the result of fire, flood, other natural disasters or acts which are not the fault of Seller and which the Product is not specified to tolerate, including damage caused by mishandling, shipping and blown fuses; (ix) consumables (such as fuses); or (x) any Product which has been opened, repaired, modified or altered by anyone other than Seller or a Seller authorized service center.

USE ONLY SELLER APPROVED ACCESSORIES WITH SELLER DEVICES. USE OF ANY UNAUTHORIZED ACCESSORIES MAY BE DANGEROUS AND WILL INVALIDATE THE DEVICE WARRANTY IF SAID ACCESSORIES CAUSE DAMAGE OR A DEFECT TO THE DEVICE. SELLER SPECIFICALLY DISCLAIMS LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, PUNITIVE, EXEMPLARY,

1. AGGRAVATED, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE OF ANY KIND WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, UNANTICIPATED BENEFITS OR REVENUE, ANTICIPATED PROFITS ARISING OUT OF USE OF OR INABILITY TO USE ANY PRODUCT (FOR EXAMPLE, WASTED AIRTIME CHARGES DUE TO THE MALFUNCTION OF A PRODUCT) OR CONTRIBUTION OR INDEMNITY IN RESPECT OF ANY CLAIM RELATED TO A PRODUCT. REPAIR OR REPLACEMENT OF A DEFECTIVE PRODUCT OR REFUND OF THE PURCHASE PRICE RELATING TO A DEFECTIVE PRODUCT, AS PROVIDED UNDER THIS WARRANTY, ARE YOUR SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE LIMITED WARRANTY, AND SUBJECT TO THIS WARRANTY, THE PRODUCTS ARE APPROVED AND ACCEPTED BY YOU “AS IS”. SELLER MAKES NO OTHER WARRANTIES, REPRESENTATIONS OR CONDITIONS OF ANY KIND, ORAL OR WRITTEN, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OR ANY IMPLIED WARRANTY OR CONDITION ARISING OUT OF TRADE USAGE OR OUT OF A COURSE OF DEALING OR COURSE OF PERFORMANCE. NO DEALER, DISTRIBUTOR, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATION OR ADDITION TO THIS WARRANTY.
2. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, or allow limitations on how long an implied warranty lasts, so the above limitations or exclusions may
3. not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.
4. For warranty service information, please call the following telephone number: 1-800-617-5065.
5. IMPORTANT: Please provide warranty information (proof of purchase) to KONNECTONE in order to receive warranty service at no charge. If the warranty has expired on the device, charges may apply.