

Industrial 4G/5G Router

Quick Start Guide

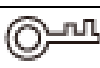


Foreword

This manual introduces the functions and operations of the industrial 4G/5G router (hereinafter referred to as "the Router"). Read carefully before using the Router, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Router, hazard prevention, and prevention of property damage. Read carefully before using the Router, and comply with the guidelines when using it.

Transportation Requirements



Transport the Router under allowed humidity and temperature conditions.

Storage Requirements



Store the Router under allowed humidity and temperature conditions.

Installation Requirements



WARNING

- Do not connect the power adapter to the Router while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Router.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.



- Do not place the Router in a place exposed to sunlight or near heat sources.
- Put the Router in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Do not connect the Router to two or more kinds of power supplies, to avoid damage to the Router.
- The Router is a class I electrical appliance. Make sure that the power supply of the Router is connected to a power socket with protective earthing.
- The Router must be grounded by a copper wire with a cross-sectional area of 2.5 mm² and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the Router and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the Router.
- When installing the Router, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operation Requirements



WARNING

- Do not disassemble the Router without professional instruction.
- Operate the Router within the rated range of power input and output.

- Make sure that the power supply is correct before use.
- Make sure the Router is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the Router while the adapter is powered on.



- Use the Router under allowed humidity and temperature conditions.
- Operating temperature: -40°C to $+75^{\circ}\text{C}$ (-40°F to $+167^{\circ}\text{F}$).
- This is a class B product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

Maintenance Requirements



WARNING

- Do not disassemble it unless necessary.
- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

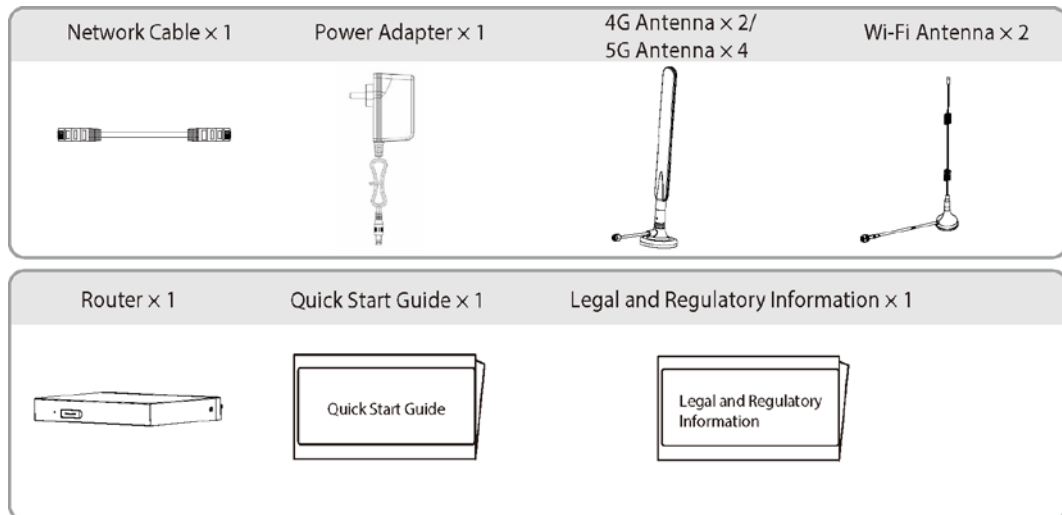
- ForewordI
- Important Safeguards and Warnings..... III
- 1 Overview 1
 - 1.1 Packing List..... 1
 - 1.2 Ports and Indicator Lights 1
 - 1.2.1 Front Panel..... 1
 - 1.2.2 Rear Panel..... 2
- 2 Basic Configuration 3
 - 2.1 Initialization 3
 - 2.2 Login 3
 - 2.3 Setup Wizard..... 3
- 3 FAQ 7
- Appendix 1 Cybersecurity Recommendations..... 8

1 Overview

1.1 Packing List

For tools or accessories not included in the packing list, purchase them as needed.

Figure 1-1 Packing list



1.2 Ports and Indicator Lights

1.2.1 Front Panel

Figure 1-2 Front panel (4G/5G router)

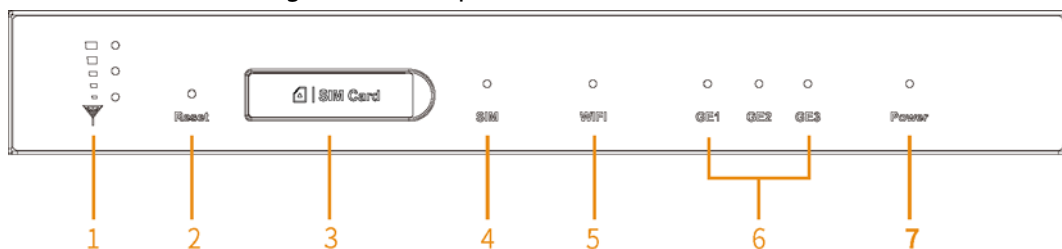


Table 1-1 Front panel description

No.	Name	Status	Description
1	Signal strength indicator light	One light on	Signal strength is weak.
		Two lights on	Signal strength is medium.
		Three lights on	Signal strength is strong.
2	Reset	—	To restore the Router to the factory settings, press and hold the reset button with a thin object for about 5 seconds until all the indicator lights come on and then go out.
3	SIM card slot	—	Insert nano SIM card.

No.	Name	Status	Description
4	SIM indicator light	On	SIM/UIM card is identified.
		Off	SIM/UIM card is not identified.
5	Wi-Fi	On	Wi-Fi is enabled.
		Off	Wi-Fi is not enabled.
6	GE1–GE3 indicator lights	On	Network port is connected.
		Flickering	Data transmission is in progress.
		Off	Network port is disconnected.
7	Power indicator light	On	The Router is powered on.
		Off	The Router is powered off.

1.2.2 Rear Panel

Figure 1-3 Rear panel (4G router)

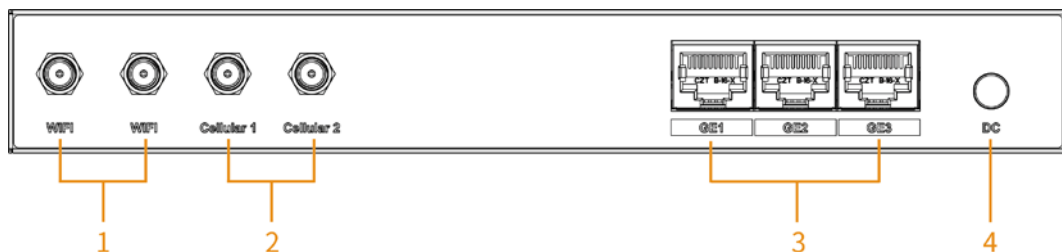


Figure 1-4 Rear panel (5G router)

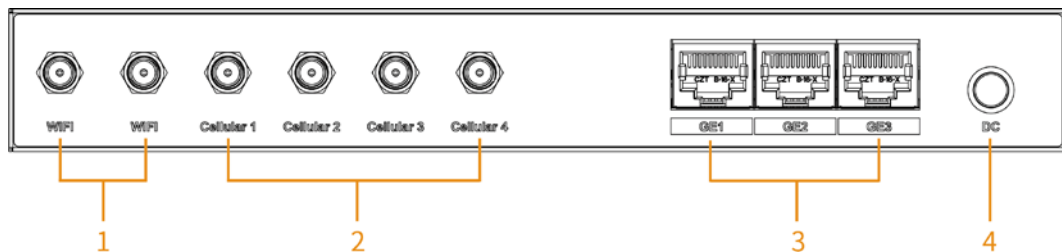


Table 1-2 Rear panel description

No.	Port	Description
1	Wi-Fi antenna SMA port	Connect Wi-Fi antennas.
2	Cellular antenna SMA port	Connect cellular antennas.
3	GE1	Ethernet port. It is WAN port by default and can be switched to LAN port through configuration.
	GE2 and GE3	Ethernet ports. They are LAN ports by default and can be switched to WAN ports through configuration.
4	Power port	Inputs 9–36 VDC power supply.

2 Basic Configuration

Initialize the Router and then log in to the webpage for more configurations.



- You need to initialize the Router for the first-time use or after it is restored to factory settings.
- For device security, keep the password safe after initialization and change it regularly.
- The default IP address of the Router is 192.168.1.110. When you initialize or log in to the Router, make sure that the Router and your computer are on the same network segment.

2.1 Initialization

Step 1 Open a browser, enter the default IP address of the Router, and then press the Enter key.

Step 2 Click **Explore**.

Step 3 Select **I have read and agree to the terms of the Software License Agreement and Privacy Policy**, and then click **OK**.

Step 4 Configure the password and email address.



The email address is used to reset the password. You can also reset the Router by pressing the reset button.

Step 5 Click **Next** to finish initialization.

2.2 Login

Step 1 Open IE browser, enter the IP address of the Router in the address bar, and then press Enter.

Step 2 Enter the password, and then click **Login**.



If you forget your password, click **Forgot password** on the login page to reset the password.

2.3 Setup Wizard

Step 1 When you log in to the webpage of the Router for the first time, follow the setup wizard to configure basic settings.

After you configure the basic settings at your first-time login, you can click  on the upper-right corner of the webpage to change the settings.

Step 2 Configure network settings, and then click **Next**.

Figure 2-1 Network settings

1 Network Settings — 2 WLAN — 3 Link Detection — 4 Complete

WAN Port List

☐	Port No.	Network Connection	IP Address	MAC	Status	Operation
☐	WAN1	DHCP			Disconnected	

- 1) Select a WAN port, click to change the network connection mode or click to delete the port.
- 2) Click **Add** to add more WAN ports, select the network connection mode, and then configure other parameters.

Figure 2-2 Add WAN port

Add

Port No.

Network Connection

Broadband Account

Broadband Password

[Forgot your password? Contact your br...](#)



- By default, there is a wired WAN port (GE1) whose network connection mode is DHCP.
- You can add up to 3 wired WAN ports on a Router.
- The 3 network ports on the Router can switch between WAN port and LAN port. The default multi-WAN mode is **Active/Standby**. You can change the mode in **Port**.
- You need to pay attention to the above points when you configure the uplink wired network. The cellular network is enabled by default with its priority level lower than WAN port. If you want to configure cellular network settings, go to **Cellular Network** after you complete the setup wizard.

Step 3 Configure WLAN settings, and then click **Next**.

- 1) Select **Same as the device login password** to make the passwords of 2.4G WLAN and

5G WLAN the same as the login password of the Router. Enable **Dual-band 2.4/5G** to use the same settings for both 2.4G and 5G. The end device will choose the one with the better signal.

2) Configure the name and power for 2.4 G WLAN and 5G WLAN.



- 2.4G WLAN uses the 2.4 GHz frequency band and 5G WLAN uses the 5 GHz band.
- You can select **High** (wall-penetrating) or **Low** for **Power**.

Figure 2-3 WLAN settings

Step 4 Configure settings for link detection, and then click **Next**.



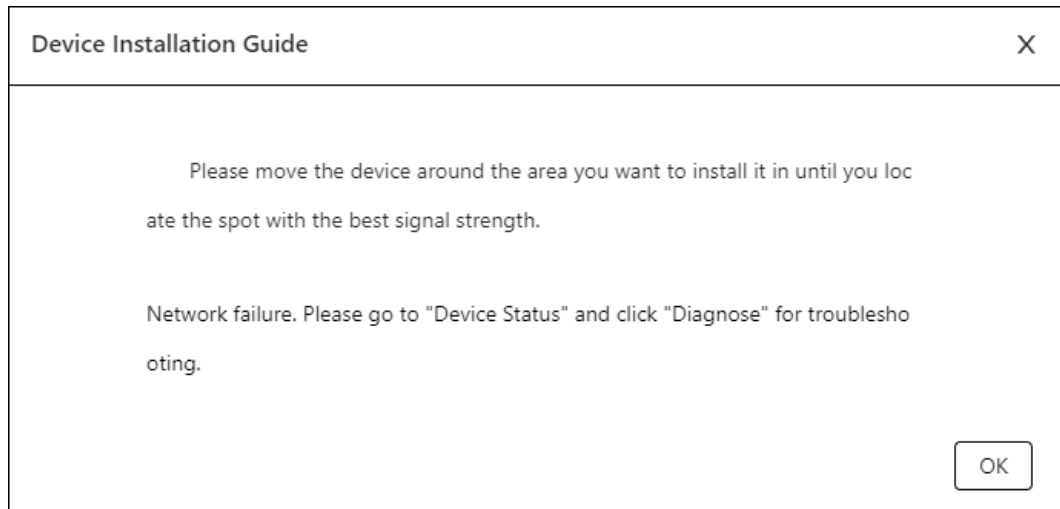
- The wired WAN port is prioritized for uplink network by default. After you enable link detection, the system automatically detects whether the WAN port or cellular network is reachable so that the router can switch to a working network.
- Before enabling link detection, make sure that the keep-alive address is valid.

Step 5 Click **OK**. Configuration is complete.

Step 6 Reconnect the Router to WLAN.

Step 7 Follow the installation guide to find a proper location for the Router.

Figure 2-4 Installation guide



3 FAQ

1. Failed to access the webpage of the Router.

- Restart the Router. Power off the Router and then power on it.
- If your computer is using a static IP, make sure your computer and the Router are on the same network segment or switch your computer to DHCP mode.
- Try again with other browsers.

2. The IPC and computer cannot access the network via the Router.

- Log in to the webpage of the Router, and then click **Device Status** to check whether the Router is connected to the network. If no, click **Diagnose** and then operate according to the on-screen instructions.
- If the Router uses the wired WAN port to access the network, consult your carrier to make sure the network connection of the WAN port is correct. If the Router uses the cellular network, go to **Port** to check whether the configured WAN port is connected, and whether **Priority Level 1** has been selected for cellular network. You can enable link detection in **Port > Link Detection**.
- If the IPC or computer cannot access the network via Wi-Fi, make sure that you are connecting to the correct Wi-Fi.
- If your computer is connected to the LAN port of the Router but cannot access the network, make sure your computer is using DHCP to obtain the IP address automatically.
- Log in to the webpage of the Router and then check whether you have configured the blocklist.
- If the issue remains after you tried the above troubleshooting steps, contact your Internet service provider.

3. Do not know how to restore the Router to factory settings.

- Method 1: After the Router is powered on for 1 minute, press and hold the reset button for about 5 seconds. When all the indicator lights come on and then go out, the Router has been restored to the factory default.
- Method 2: Log in to the webpage of the Router, and then go to **Advanced > Maintenance > Backup & Restore** to restore the Router to factory settings.

4. Failed to find the Wi-Fi signal of the Router.

Connect your computer to the LAN port of the Router using a network cable, log in to the webpage of the Router, click **WLAN** to check whether the WLAN network is enabled. If no, turn on the WLAN network and then use your computer and other devices to search for the Wi-Fi again.

5. Failed to detect the 5 GHz Wi-Fi signal.

Only devices compatible with 5 GHz can detect 5 GHz Wi-Fi signal. If you have enabled **Dual-band 2.4/5G**, the 2.4G WLAN and 5G WLAN will share the name by default. You can customize the 5 GHz WLAN network in **WLAN**.

6. Forgot the WLAN password.

Connect your computer to the LAN port of the Router using a network cable, log in to the webpage of the Router, and then click **WLAN** to reset the WLAN password.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing

the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.