4G Router

Quick Start Guide

V1.0.0

Zhejiang Dahua Vision Technology Co., Ltd

Foreword

General

This manual introduces the structure and configuration of the 4G router (hereinafter referred to as "the Device").

Models

DH-WM4700-O

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
TIPS	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
NOTE	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2019

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure that the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not dissemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy operation.

Table of Contents

1 Product Introduction

The appearance of DH-WM4700-O 4G router is shown in Figure 1-1 and Figure 1-2.

Figure 1-1 Front panel

Table 1-1 Front panel description

Indicator	Status	Description
Wi-Fi	On	Wi-Fi is enabled.
	Off	Wi-Fi is not enabled.
WAN	On/flash	● On: WAN port is connected. ● Flash: Data transmission is in progress.
	Off	WAN port is disconnected.
Local network	On/flash	● On: Network port is connected. ● Flash: Data transmission is in progress.
	Off	Network port is disconnected.
Signal strength indicator	One light on	Weak signal strength (less than -90 dbm).
	Two lights on	Medium signal strength (-70 dbm to -90 dbm).
	Three lights on	Strong signal strength (more than -70 dbm).
SIM	On	SIM/UIM card is identified.
	Off	SIM/UIM card is not identified.
Online	On	The Device is connected to the network.
	Off	The Device is disconnected to the network.
SIM/UIM	-	For inserting SIM/UIM card.
System	Flash	The system is running normally.
	Off	The system is abnormal.
Power	On	Power supply to the Device is normal.
	Off	The Device is not powered on or during shutdown by timing switch.

Figure 1-2 Rear Panel

Table 1-2 Rear panel description

Indicator	Description
ANT-M	External 4G main antenna.
Power	Connector for power adapter.
Reset	Restore factory default button. Press and hold the button for about 10 seconds until all lights are off. And the Device can be reset to the factory default.
Console	Serial port for debugging. Baud rate is 115200 bps.
ANT-A	External 4G backup antenna.
Local Network	Four 100 M LAN port for local network access.
WAN	One 100 M WAN port for Internet access.
WIFI	External Wi-Fi antenna.

2 Product Configuration

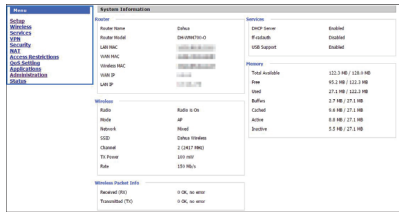
Before you configure the Device, make sure that:

- Connect the LAN port of the Device to the PC with network cable, and then power on the Device.
- The network of the PC is set to automatic access mode.

Step 1 Open the browser, enter IP address of the Device (the default IP is 192.168.1.110) and then press Enter key.

The **System Information** interface is displayed. See Figure 2-1.

Figure 2-1 System information

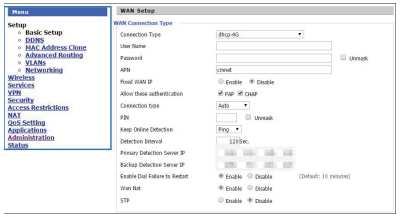


Step 2 In the left navigation menu, click **Setup**, and then enter the login account and password.

The **Basic Setup** interface is displayed. See Figure 2-2.

The account is admin and password is admin by default.

Figure2-2 Basic setup



Step 3 (Optional) In **WAN Setup** section, configure WAN parameters. See Table 2-1.

- Only the private network card needs to be configured, and the ordinary mobile card does not need to be configured to automatically access the Internet.
- Only certain parameters are described, and the rest parameters can be configured according to the actual situation.

Table 2-1 WAN parameter configuration

Parameter	Description
Connetion Type	Select the connection type for 4G dial-up access. The default choice is **dhcp-4g** or **3G/UMTS/4G/LTE**.
User Name	Enter the private network information provided by the operator, including user name, password and APN.
Password	
APN	
Keep Online Detection	Select online detection mode. The default mode to detect IP is **Ping**, but it is suitable only for public network. If there is no private network server IP, select **None**.
Primary Detection Server IP	Modified to the private network server IP.
Backup Detection Server IP	When **Keep Online Detection** is set to **None**, you do not need to set **Primary Detection Server IP** and **Backup Detection Server IP**.

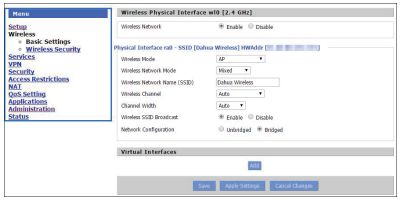
Step 4 In **Network Setup** section, configure router IP.

Figure 2-3 Network setup

Step 5 Configure wireless network name.

1) In the left navigation menu, click **Wireless**.
   The **Wireless Basic Settings** interface is displayed. See Figure 2-4.

Figure2-4 Wireless basic settings

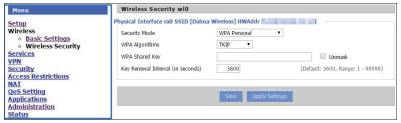


2) Enter **Wireless Network Name (SSID)**, and then click **Save**.

Step 6 Configure wireless network password

1) In the left navigation menu, select **Wireless > Wireless Security**.
2) Select **Security Mode** as **WPA Personal**.
   The **Wireless Security** interface is displayed. See Figure 2-5.

Figure2-5 Wireless security

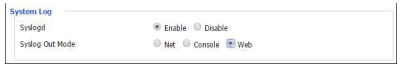


3) In **WPA Shared Key** box, set wireless network password, and then click **Save**.

Step 7 Configure system log.

1) In the left navigation menu, select **Service** to go to service management interface.
2) In **System Log** section, enable system log, and select **Syslog Out mode** as **Web**.

Figure2-6 System log



3) Click **Save** to finish configuration.
4) Select **Status > WebLog** to view logs.
   - Click **Backup** to back up logs.
   - Click **Refresh** to refresh logs.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**
   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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.

FCC Statement

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
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.
FCC 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 minimum distance 20cm between the radiator& your body.

Note : 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.

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. **Enable Whitelist**
   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
9. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
10. **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.
11. **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.
12. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
13. **Network Log**
    Due to the limited storage capacity of the equipment, 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.
14. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment 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.

Zhejiang Dahua Vision Technology Co., Ltd
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, **310053** P.R. China
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com