Wireless Bridge (DH-WB5-8AC-20 Series)

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

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.

Important Safeguards and Warnings

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

Transportation Requirements

Please transport the product within the permissible humidity and temperature ranges.

Storage Requirements

Please store the product within the permissible humidity and temperature ranges.

Installation Requirements

DANGER

- It is strictly prohibited to connect the device after the power adapter has been powered on. Please connect the power adapter and the device while the power is off.
- Strictly follow local electrical safety standards to ensure the environmental voltage is stable and meets the equipment's power requirements.
- Personnel working at heights must wear safety helmets and use safety harnesses, taking appropriate protective measures to ensure personal safety.

WARNING

- Do not place or install the device in direct sunlight or near heat-generating equipment.
- Do not install the device in the humid, dusty, or smoky environments.
- Install the device in a well-ventilated location and do not block the ventilation openings of the device.
- Use the adapter or power supply provided by the product manufacturer.
- Use a power supply that meets the SELV (Safety Extra-Low Voltage) requirements and complies with the rated voltage specified by GB8898 (IEC60950) or GB4943.1 (IEC60950-1) for Limited Power Source. Refer to the product label for specific power supply requirements.
- Do not provide two or more power sources to the device simultaneously, as this may cause damage or pose a safety risk.
- Connect Class I structure products to an outlet with a protective grounding connection.
- Ensure that the device is properly grounded (using copper wires with a cross-sectional area not less than 2.5 mm^2, with a ground resistance of <4Ω).
- Install voltage stabilizers and lightning protectors as needed, depending on the power supply and surrounding environmental conditions.

- When installing the product, ensure there is sufficient clearance around the device for proper heat dissipation. The sides should have at least 10 cm of clearance, and the top should have at least 10 cm of clearance.
- The installation must allow for easy access to the power plug and appliance coupler to safely disconnect the power supply to the product.

Operation Requirements

- Do not disassemble the equipment.
- The equipment should only be used within the rated input and output ranges.
- Before operating the equipment, please check if the power supply is correct.
- When disconnecting cables, power off the equipment first to avoid personal injury.
- Do not unplug the power cord from the equipment while the adapter is powered on.

WARNING

- Operating this equipment in residential environments may cause radio interference.
- Do not disassemble the equipment.
- Use the equipment only within the rated input and output ranges.
- Before operating the equipment, ensure the power supply is correct.
- When disconnecting cables, power off the equipment to prevent personal injury.
- Do not unplug the power cord from the equipment while the adapter is powered on.
- Ensure the equipment is connected to protective earth before connecting to power.
- Ensure the product is properly grounded by skilled technicians (including connecting the ground conductor to the building ground and verifying the protective grounding of the outlet).

- Use the product within the allowable humidity and temperature ranges.
- Do not drip or splash liquids on the equipment, and make sure no liquid-filled items are placed on the equipment to prevent liquid from entering the device.
- Operating temperature range:-30°C to +70°C.
- Do not obstruct the product's ventilation openings with objects such as newspapers, tablecloths, or curtains.
- Do not place any open flame sources, such as lit candles, on the product.

Maintenance Requirements

- Please use the product within the permissible humidity and temperature range.

Table of Contents

Foreword....I
Important Safeguards and Warnings....III
1 Product Overview....3
1.1 Product Introduction....3
1.2 Product Features....3
1.3 Interface Buttons and Indicator Light Status....3
2 Equipment Installation....6
2.1 Installation diagram....6
2.2 Schematic diagram of connection....6
3 Basic Configuration....7
3.1 Logging into the Device....7
3.2 Setup Wizard....8
3.3 Connection Settings....10
4 FAQ....11
Appendix 1 Security Commitment and Recommendation....12

1 Product Overview

1.1 Product Overview

This product is a high-performance, high-speed outdoor long-distance wireless bridge, which has the characteristics of long transmission distance, strong penetration ability and strong anti-interference ability.

1.2 Product Features

- Integrated 25dBi dual-polarized dish antenna, up to 20 km.
- Support both 48V standard PoE and DC 12V power supply.
- Support intelligent channel analysis, automatic optimal channel selection, the maximum speed is 867Mbps.
- The product supports universal relay mode and AP mode, and the user application scenarios are more extensive.

1.3 Interface Buttons and Indicator Light Status

Figure 1-1

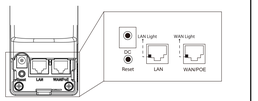


Figure 1-2

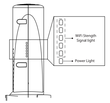


Table 1-3 Interface Descriptions

Interface Label	Description
RST	long press for 6-10 seconds to restore factory settings.
LAN	10/100/1000 Mbps
WAN	10/100/1000 Mbps PoE 48V power input
DC	DC 12V 1.5A power input

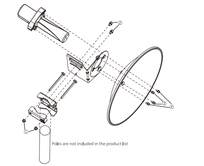
Table 1-4 Indicator Light Status

Indicator Light Status	Description
WiFi Strength Signal light	Constant light bars: Wi-Fi connection strength
LAN Indicator Light	Constant light: Connected; Flashing: Connected and data is being transmitted.
WAN Indicator Light	Constant light: Connected; Flashing: Connected and data is being transmitted.
Power Indicator Light	Constant light: The device is powered up

2 Equipment Installation

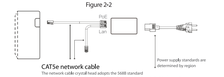
2.1 Installation diagram

Figure 2-1



2.2 Schematic diagram of connection

Figure 2-2



Product Specifications:	Operating frequency	5.150GHz-5.850GHz
	Transmit power	<29dBm(It depends on the region)
	Power supply	12V DC, 48V PoE or customized 24VPoE
	Power consumption	<12W

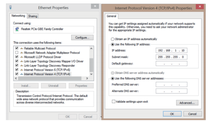
3 Basic Configuration

3.1 Logging into the Device

Step 1 Connect via wired connection: The computer used for the setup must have a wired network card with its TCP/IP properties set to an IP address within the same network segment as the default IP address on the device's label. For example, if the default IP is 192.168.1.36, the network card can be set to 192.168.1.10.

Figure 3-1 Look at the wired connection

Figure 3-2 Set up your computer's network card



Step 2 Open the browser, enter the default IP address of the wireless device (192.168.1.36) in the address bar, and then press the [Enter] key. For the first login, the user needs to set a login password. The initial password is admin123. After setting the new password, click "OK" to enter the setup wizard.

3.2 Setup Wizard

Step 1 After setting the password for the bridge in the data center, you will be automatically redirected to the setup wizard page, and click Next to enter the quick setting page.

Step 2 Choose the internal network connection method. The default is GHCP. Based on your usage, you can click the drop-down menu to change the connection method.

Figure 3-3 Internal network connection method

Internal network connection method:

- If you want the bridge to assign IP addresses internally between bridges, choose [GHCP Address]. The bridge with the largest MAC address will automatically assign dynamic IP addresses to the other bridges.
- If you want the IP address to be assigned by a third-party router, select [DHCP].
- If you already have pre-configured network addresses for the devices, select [Static Address].

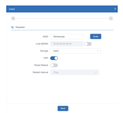
Step 3 For the Wi-Fi configuration page, set the Wi-Fi parameters, and click Next to complete the setup wizard.

Figure 3-4 Setting Wi-Fi Parameters

Step 4 For the bridge on the Client side. After setting the password for the camera-side bridge, the setting wizard page will be automatically redirected, and click Next to enter the quick setting page.

Step 5 Set the relay Wi-Fi parameters. Click "Search" and select the Wi-Fi emitted by the AP end from the scan results. Fill in the same parameters, then click "Next" to complete the setup wizard.

Figure 3-5 Setting Relay Wi-Fi Parameters



- Locking BSSID: When multiple SSIDs are present, locking the BSSID allows you to specify the master bridge connected to the MAC address.
- Point-to-point transmission: Generally, it should be enabled, but when using third-party Wi-Fi intermediaries, it is recommended to disable this option.

Step 6 Configure the intranet settings according to the actual usage, click Next, switch to trunk mode, and wait for the device to restart.

Figure 3-6 Trunk Intranet Settings

3.3Connection Settings

Use the web configuration for connection. After completing the connection, the results will be displayed as follows.

Figure 3-7 Access Point End

Figure 3-8 Client End:

4 FAQ

1.Forgot the login password?

Restore the device to factory settings by pressing and holding the Reset button on the device for more than 10 seconds, then release it. The device will automatically restart and return to its factory settings.

2.Unable to log into the device management page via web?

Try the following solutions:

- **Method 1** Check if the computer's IP address and the device are on the same network segment. Ensure it has not been manually set to another network segment.
- **Method 2** Reset the device to factory default settings and reconnect.
- **Method 3** Verify that the device's address (192.168.1.36) is not being used by another device on the network.
- **Method 4** Check the computer and network cable for any issues. It is recommended to use unshielded CatSe twisted-pair cable.

3.Forgot the wireless network password?

Follow these steps to troubleshoot:

Step 1: Connect the device using an Ethernet cable.

Step 2: Log into the web management page and click on "Wireless Settings."

4.Unable to connect between the two bridges?

Try the following solutions:

- **Method 1** Check for obstacles between the bridges, such as trees, high-voltage power lines, or buildings. Try raising the bridge or relocating it.
- **Method 2** Check if the link is disconnected. You can check the LAN and WAN indicator lights on the bridges to see if they are connected.

Appendix 1 Security Commitment and Recommendation

Dahua attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited:to:

1. Account Management

1.1 Use complex 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: 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 repeating characters, such as 111, aaa, etc.

1.2 Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

1.3 Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

1.4 Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

1.5 Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

2. Service Configuration

2.1 Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2.2 Encrypted transmission of audio and video

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

2.3 Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

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

2.4 Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

3. Network Configuration

3.1 Enable Allow list

It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

3.2 MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3.3 Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;According to the actual network needs, partition the network; if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation; Stabilish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

It is recommended to check online users regularly to identify illegal users.

4.2 Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

4.3 Configure network log

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

5. Software Security

5.1 Update firmware in time

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. Physical protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING ASMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO. LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, p.R. China Website: www.dahuasecurity.com Postcode: 310053
Email: dhoverseas@dhvisiontech.com Tel:+86-571-87688888 28933188