Wireless Bridge

Quick Start Guide

V1.0.1

Foreword

General

This manual introduces the installation, functions and operations of the wireless bridge (hereinafter referred to as "the Device"). Read carefully before using the device, 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
V1.0.1	Updated the image and description of the indicator light, and the device connection.	June 2022
V1.0.0	First release.	December 2020

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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

⚠

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

⚠

Store the device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the device 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 device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not leave outdoor models of the device hanging in the air or facing outwards when installing onto poles that are on top of buildings.

⚠

- Do not place the device in a place exposed to sunlight or near heat sources.
- Put the device 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 device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm^2 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 device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Outdoor models of the device must be securely installed on poles or brackets that are perpendicular to the ground. Make sure the entire surface of the device and all its related components are covered with anti-oxidation coating (such as rust preventive paint), and that the

installation site and height of the device meet the requirements of the plan.

- Install outdoor models of the device on top of buildings where there is little to no direct sunlight to avoid the device becoming overheated. Make sure to take all necessary measures to protect the device.
- Face the side with the Ethernet port downwards, and arrange the wires in a downward direction when installing outdoor models of the device.

Operation Requirements

⚠ WARNING

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.

⚠

- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.

Maintenance Requirements

⚠ WARNING

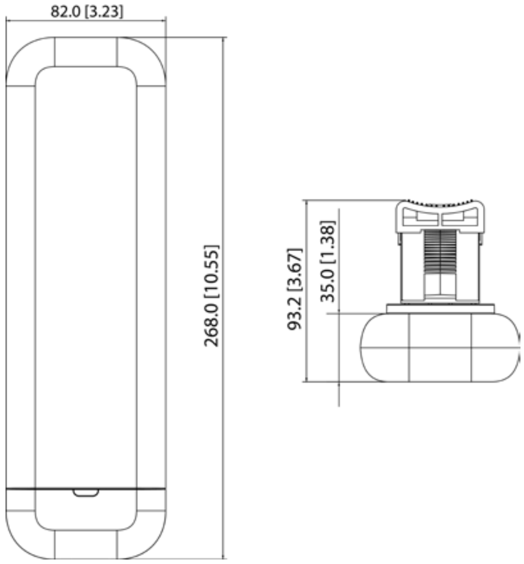
- This is a waterproof device for outdoors use. Do not disassemble it unless necessary.
- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

1 Device Structure

1.1 Dimensions

Figure 1-1 Dimensions (Unit: mm [inch])



1.2 Structure

1.2.1 Indicator Light

Figure 1-2 Indicator light

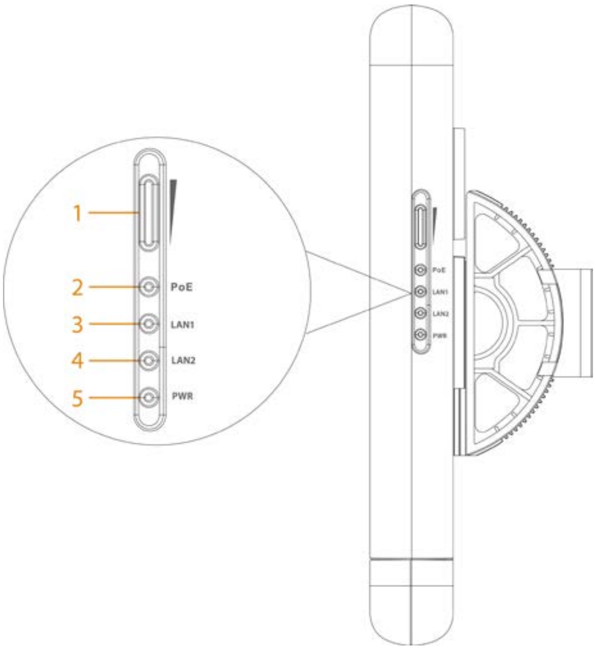


Table 1-1 Description of indicator light

No.	Name	Status	Description
1	LED 1/LED 2/LED 3 (Received signal strength indicator)	Off	Not connected to any devices.
		On	● Client: ◇ LED 1, LED 2, LED 3 are on: strong wireless signal. ◇ LED 1, LED 2 are on, and LED 3 is off: medium wireless signal. ◇ LED 1 is on, and LED 2 and LED 3 are off: weak wireless signal. You need to adjust the direction or position between bridges. ● Access Point: All LED1, LED2 and LED3 are on.
2	PoE indicator light	Off	PoE OUT function is disabled.
		On	PoE OUT function is enabled.
3	LAN 1 indicator light	Off	The port is not properly connected.
		Flicker	Wireless data transmission is in progress.
		On	The port is properly connected.
4	LAN 2 indicator light	Off	The port is not properly connected.
		Flicker	Wireless data transmission is in progress.
		On	The port is properly connected.
5	Power indicator light	Off	Power supply is abnormal.
		On	Power supply is normal.

1.2.2 Port and Button

Figure 1-3 Port and button

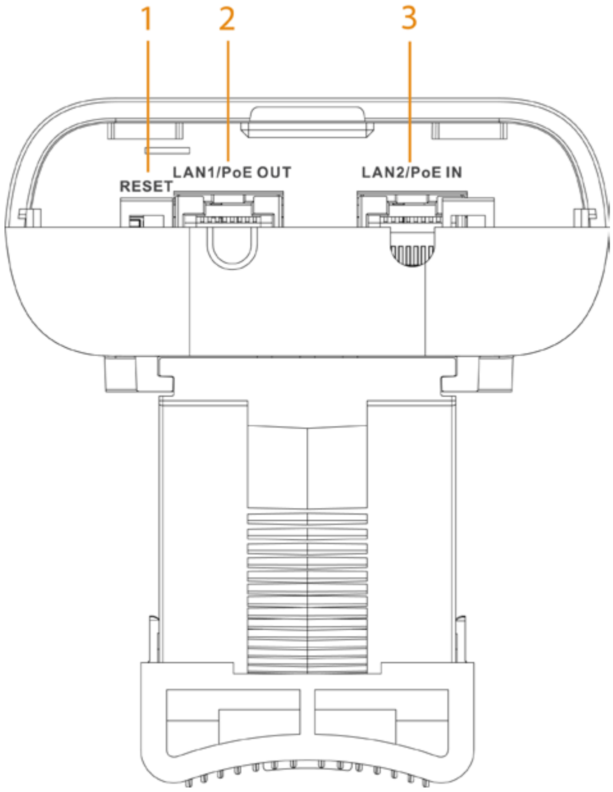


Table 1-2 Description of port/button

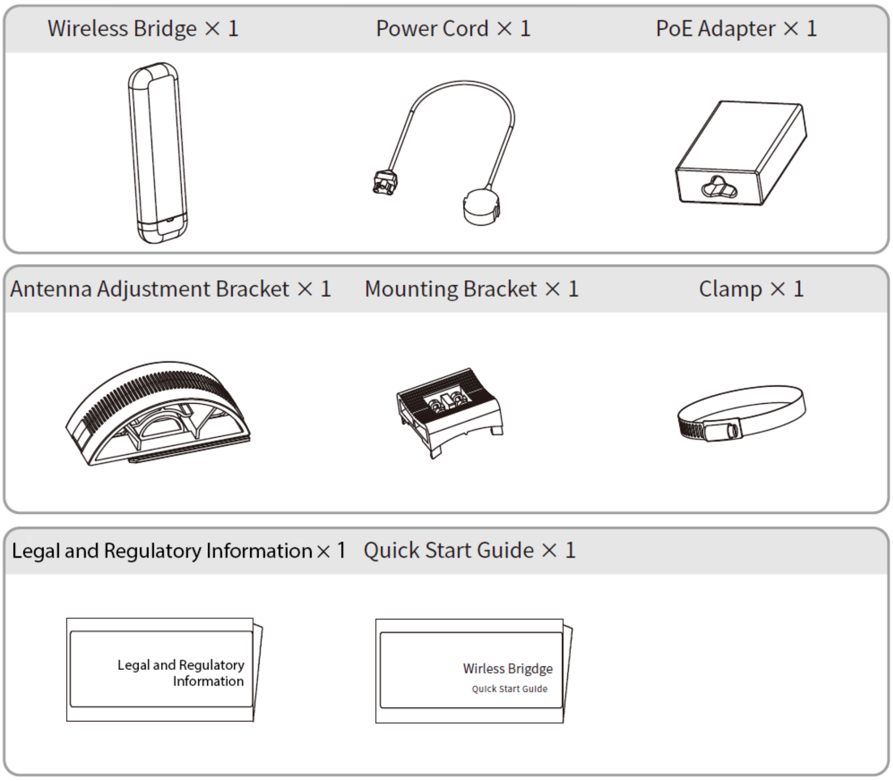
No.	Name	Description
1	RESET	After the Device is powered on for 1 minute, press and hold Reset button for about 5 seconds and then release it. If the indicator light is on and off again, the Device is restored to factory settings.
2	LAN1/PoE OUT	Ethernet data transmission port and PoE power output port, which can be connected to terminal device such as IPC or speed dome.
3	LAN2/PoE IN	PoE power input port/data transmission reuse port: The PoE power supply adapter or PoE switch can be connected to supply power to device.

2 Installation and Connection

2.1 Packing List

For tools or accessories not listed, please purchase them as needed.

Figure 2-1 Packing list

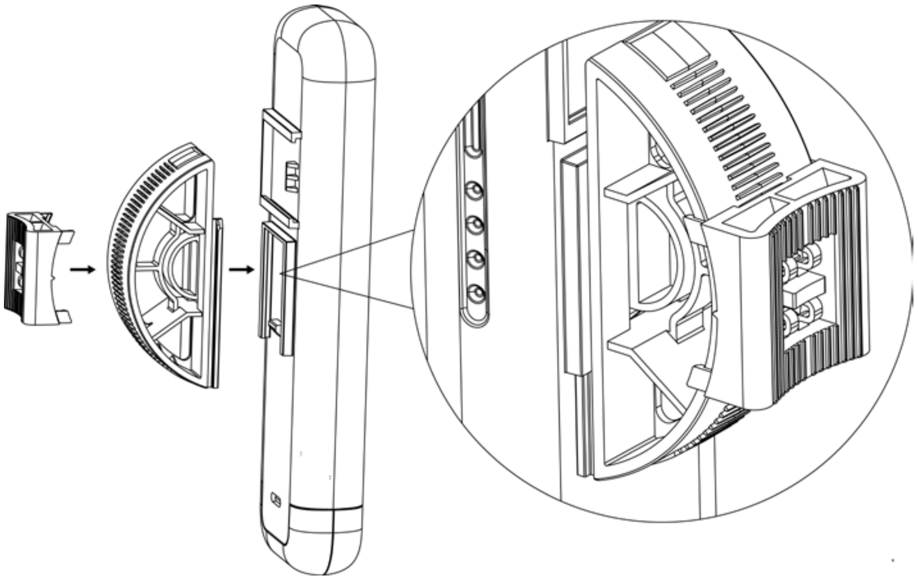


2.2 Device Installation

2.2.1 Vertical Installation

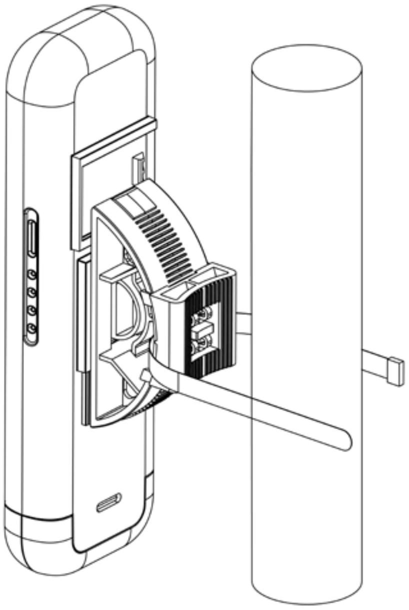
Step 1 Put the mounting bracket into the vertical slot on the back of the Device.

Figure 2-2 Vertical installation of the bridge



Step 2 After crossing the mounting bracket on the back of the Device with clamp, fix the Device to the mounting rod and tighten the clamp.

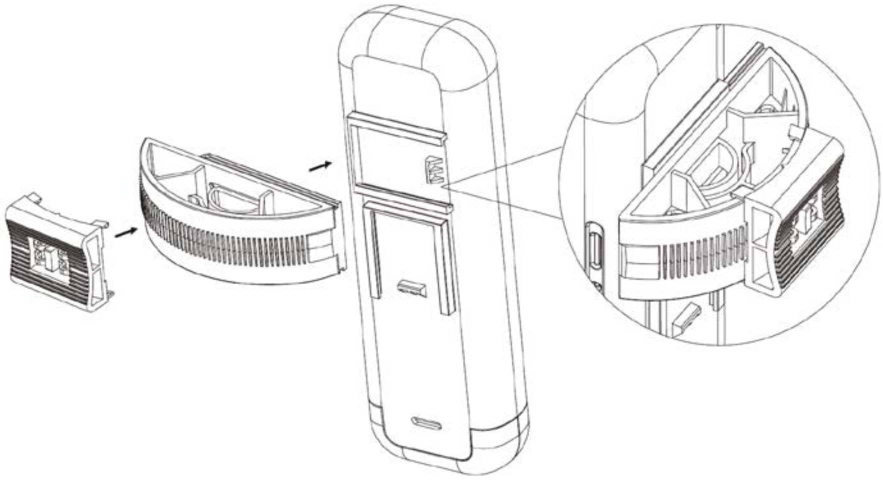
Figure 2-3 Fixing the bridge



2.2.2 Horizontal Installation

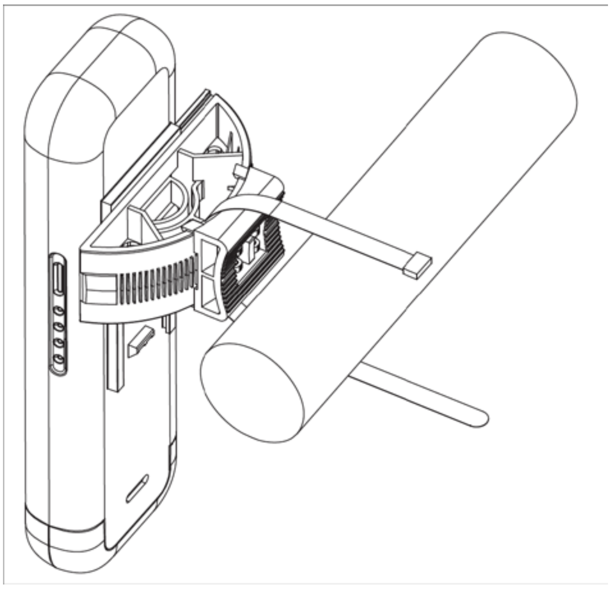
Step 1 Put the mounting bracket into the horizontal slot on the back of the Device.

Figure 2-4 Horizontal installation of the bridge



Step 2 After crossing the mounting bracket on the back of the Device with clamp, fix the Device to the mounting rod and then tighten the clamp.

Figure 2-5 Fixing the bridge

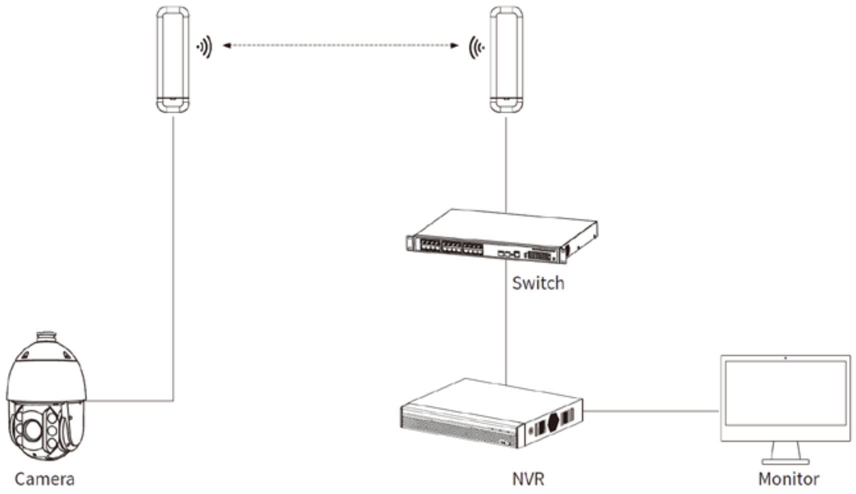


2.3 Device Connection

2.3.1 Connection Mode

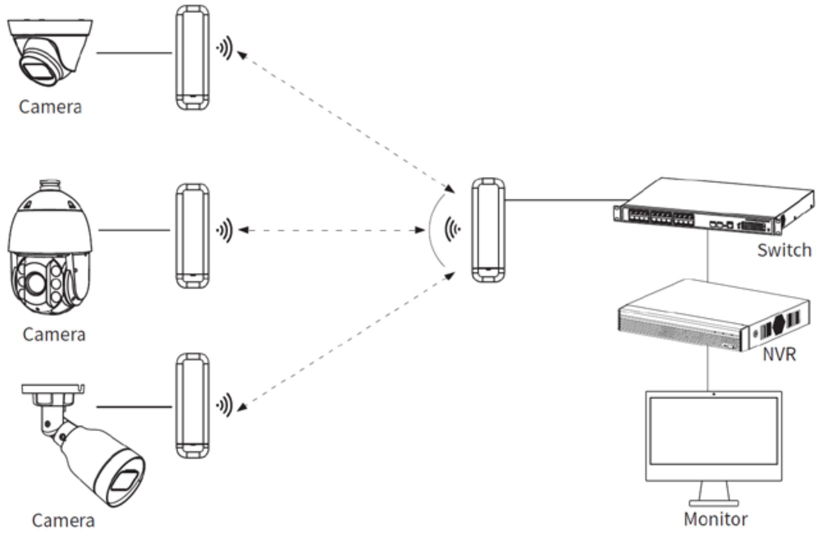
Point to Point

Figure 2-6 Point-to-point connection



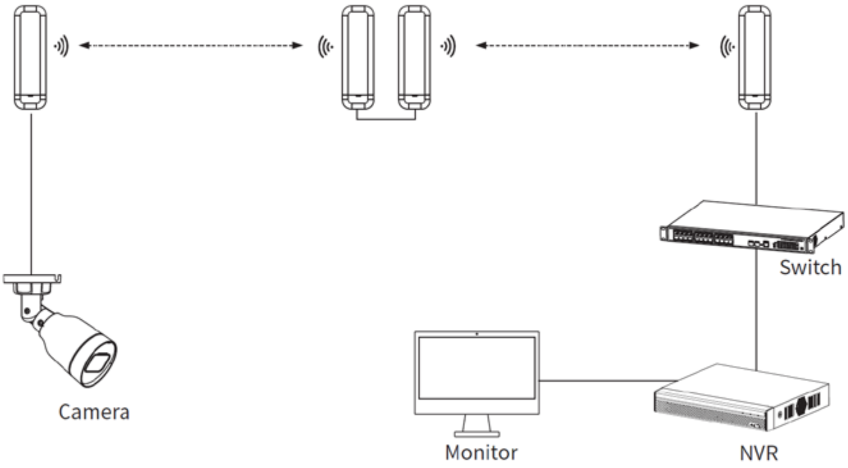
Point to Points

Figure 2-7 Point-to-points connection



Back to Back

Figure 2-8 Back-to-back connection

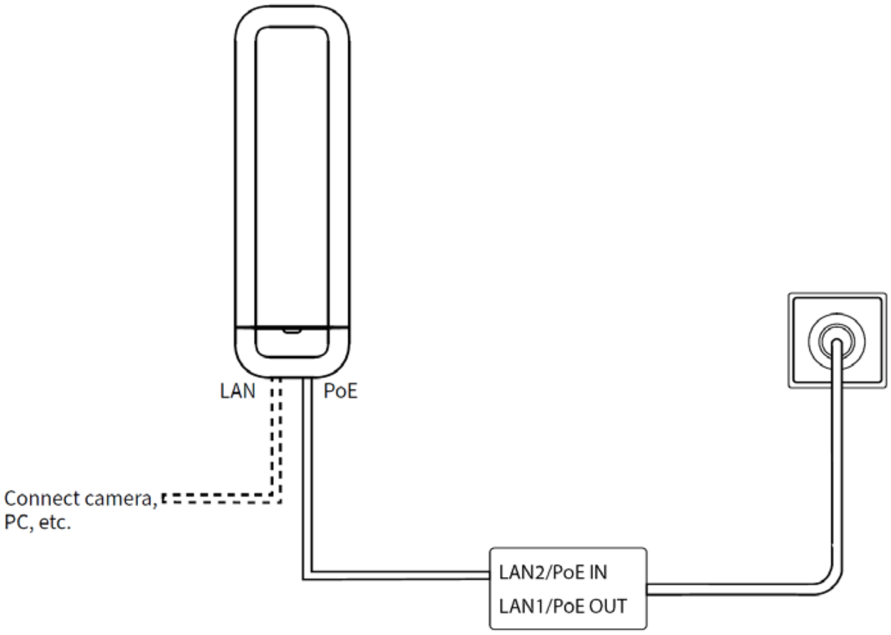


2.3.2 Connecting the Device

Step 1 Connect the PoE ports of power supply and of wireless device with cable.

Step 2 Connect the LAN port of wireless device, and the LAN port of peripheral device such as camera or PC with cable.

Figure 2-9 Device connection



3 Basic Configuration

3.1 Device Initialization

You need to initialize the Device for first-time use or after it is restored to factory settings.

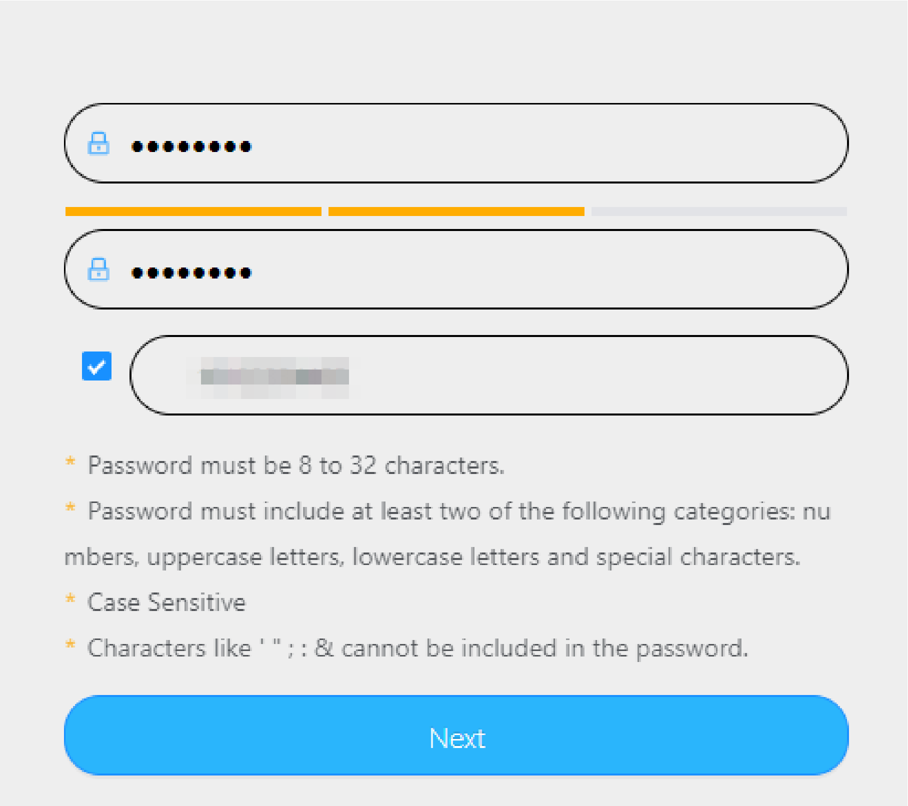
- For Device safety, keep your login password well after initialization, and change it regularly.
- When initializing the Device, keep the PC IP address and device IP address in the same network, or connect to the hotspot of the Device through Wi-Fi. The SSID of the Wi-Fi is the last six digits of WB_admin2.4GHz_SN.

Step 1 Open the browser, enter device IP address (192.168.1.36 by default under wired management, and 192.168.177.36 by default under 2.4G Hz Wi-Fi management) in the address bar, and then press the Enter key.

Step 2 Read the **Software License Agreement**, select **I have read and agree to all the terms**, and then click **OK**.

Step 3 Set the login password of admin account.

Figure 3-2 Password settings



••••••••

••••••••

☑

* Password must be 8 to 32 characters.

* Password must include at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters.

* Case Sensitive

* Characters like ' " ; : & cannot be included in the password.

Step 4 Click **Next**, and then finish initialization.

3.2 Device Login

You can log in to the device web interface through browser.

Prerequisites

- You need to initialize the device before logging in to the web interface.
- When logging in, keep the PC IP and device IP in the same network.

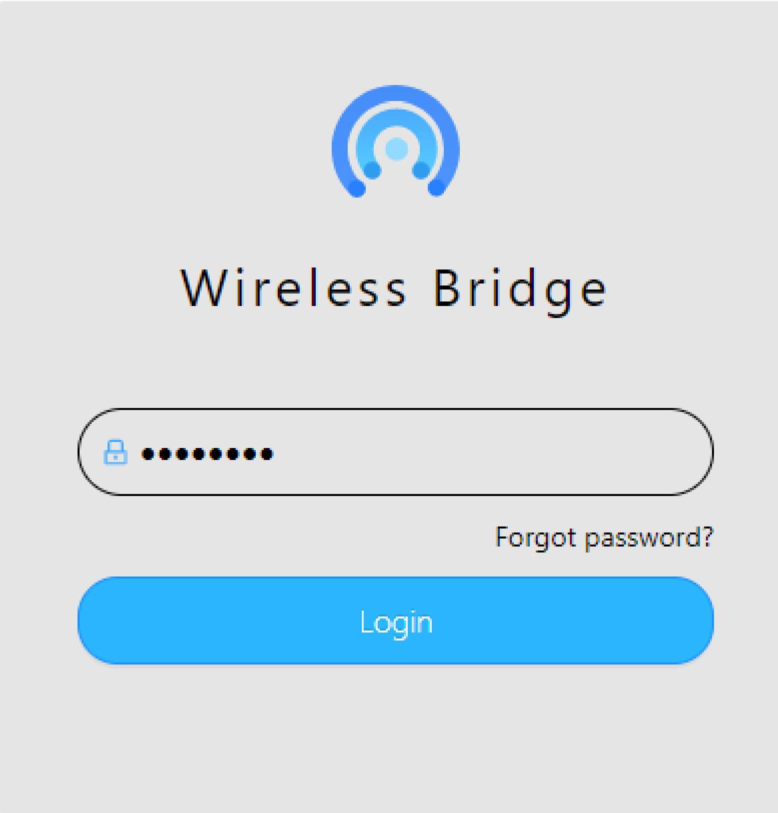
Procedure

Step 1 Open browser, enter the IP address of the device (192.168.1.36 by default under wired management, and 192.168.177.36 by default under 2.4G Hz Wi-Fi management) in the address bar and then press Enter.

Step 2 Enter the username and password.

The default username is admin, and the password is the one that you set while initializing the device.

Figure 3-3 Logging in to web



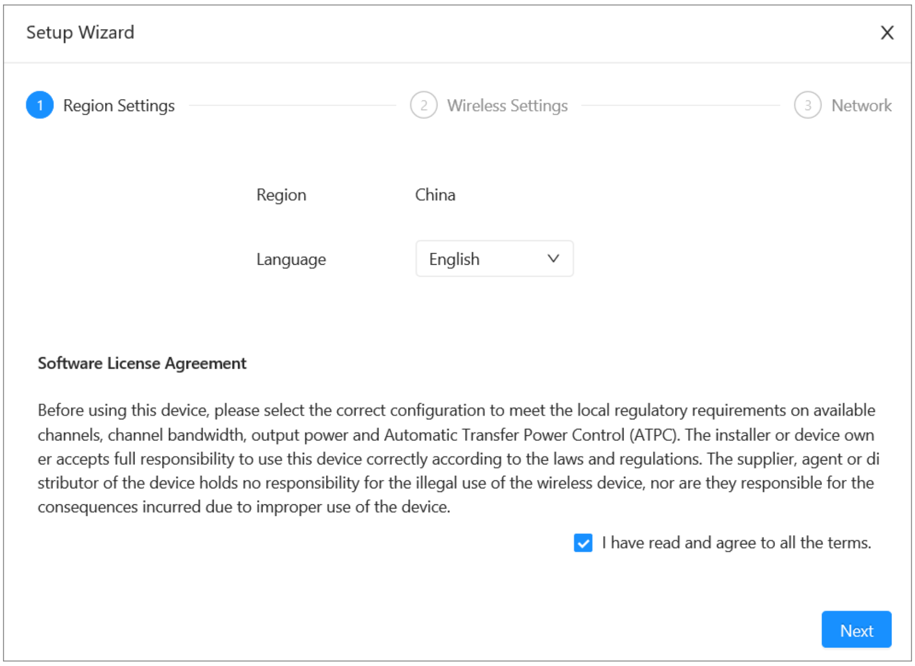
Step 3 Click **Login**

3.3 Setup Wizard

Follow the prompt to complete the setup wizard when logging in to the web for the first time.

Step 1 On the **Region Settings** page, set region and language, select **I have read and agree to all the terms**, and then click **Next**.

Figure 3-4 Region settings



Setup Wizard ✕

1 Region Settings — 2 Wireless Settings — 3 Network

Region China

Language English ∨

Software License Agreement

Before using this device, please select the correct configuration to meet the local regulatory requirements on available channels, channel bandwidth, output power and Automatic Transfer Power Control (ATPC). The installer or device own er accepts full responsibility to use this device correctly according to the laws and regulations. The supplier, agent or di stributor of the device holds no responsibility for the illegal use of the wireless device, nor are they responsible for the consequences incurred due to improper use of the device.

☑ I have read and agree to all the terms.

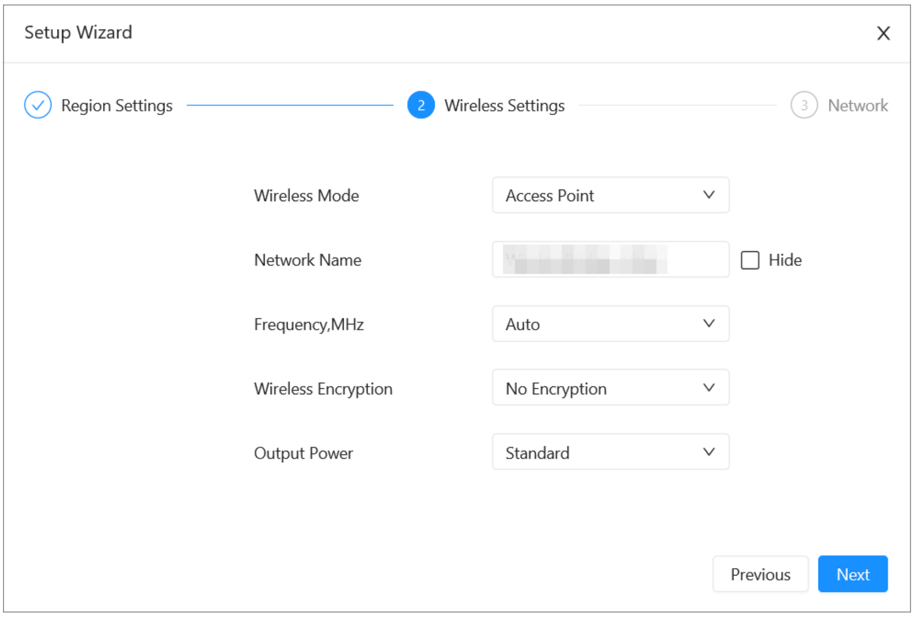
Next

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

⚠

If there are more than one access points, set different frequency for each of them to avoid interference.

Figure 3-5 Access point settings



Setup Wizard ✕

✓ Region Settings — 2 Wireless Settings — 3 Network

Wireless Mode Access Point ∨

Network Name [redacted] □ Hide

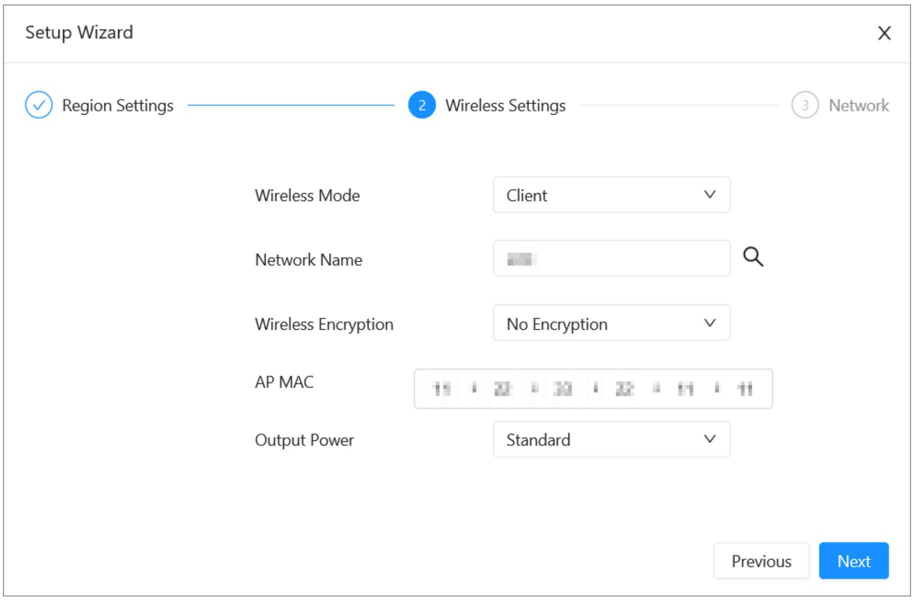
Frequency,MHz Auto ∨

Wireless Encryption No Encryption ∨

Output Power Standard ∨

Previous Next

Figure 3-6 Client settings



Setup Wizard

Wireless Mode: Client

Network Name: [redacted]

Wireless Encryption: No Encryption

AP MAC: [redacted]

Output Power: Standard

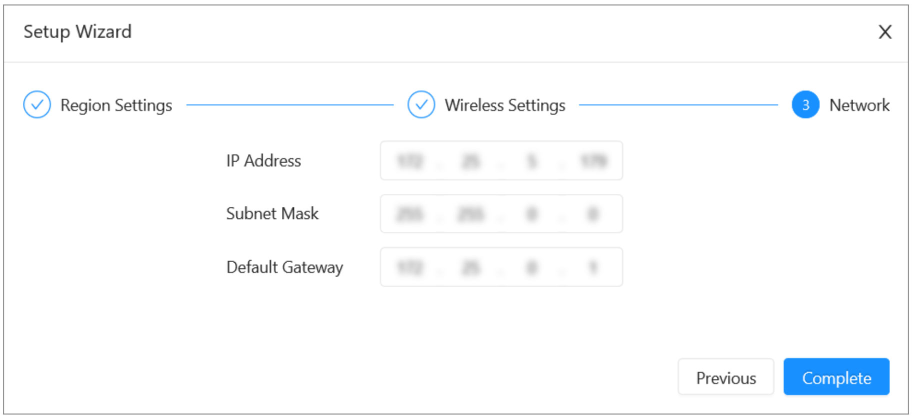
Table 3-1 Description of wireless setting

Parameter	Description
Wireless Mode	Two modes are available: **Access Point** and **Client**. 📖 ● We recommend you set devices connected to PC to **Access Point** mode, and devices connected to camera to **Client** mode. ● In the same LAN, make sure that the access point device and the responding client device have the same network name, frequency, encryption type, wireless password and output power.
Network Name	Control access to the wireless network. Click 🔍 to search for the network name of the surrounding wireless network, and then connect to the corresponding wireless network as needed. 📖 Only devices with the same network name can communicate with each other and establish a LAN.
Frequency	The center frequency of the carrier. The left and right offset of the center frequency is the channel bandwidth. If there are more than one access point devices, set different frequency for each of them to avoid interference.
Wireless Encryption	Select an encryption method as needed. 📖 The devices to be paired must have the same wireless encryption method, otherwise they will not be paired.
Encryption Type	
Wireless Password	Set the wireless password of the device. 📖 The devices to be paired must have the same wireless password, otherwise they will not be paired.

Parameter	Description
AP MAC	By specifying the MAC address of the pairing access point, the client can only be connected to the specific access point.
Output Power	Change the distance of effective wireless transmission by adjusting the mode of the output power. Transmission power can be sequentially increased from **Eco Mode**, **Standard**, and **High Performance**.

Step 3 Change the IP address of the device to make sure that IP addresses in the same LAN do not conflict, and then click **Complete**.

Figure 3-7 Network management



Setup Wizard

IP Address [redacted]

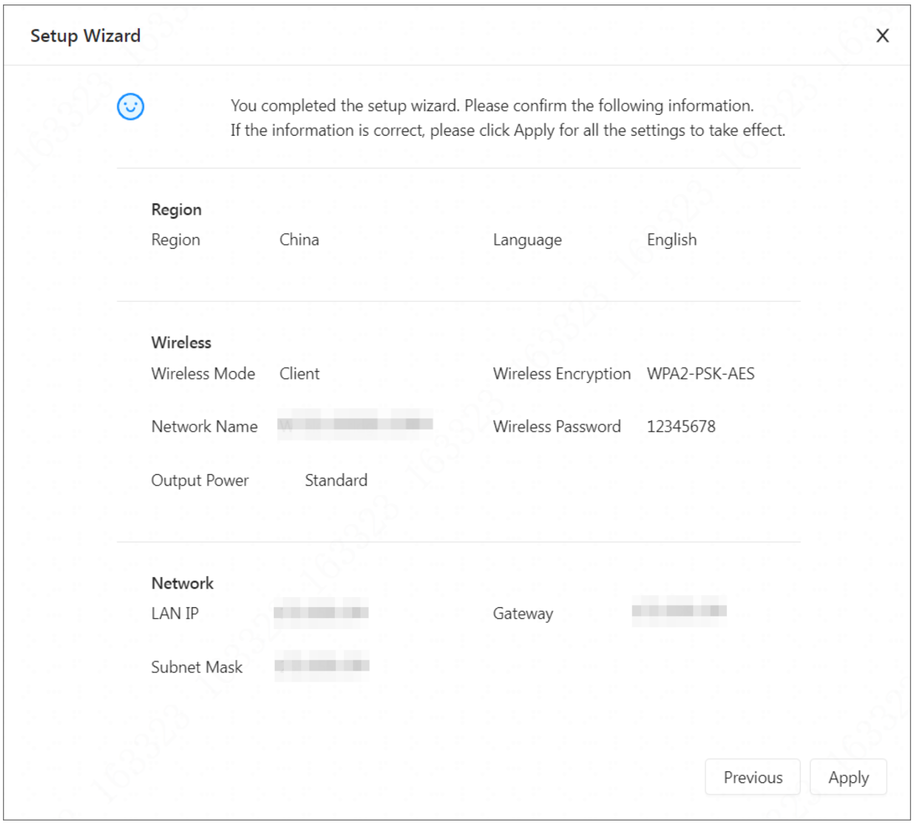
Subnet Mask [redacted]

Default Gateway [redacted]

Step 4 Click **Apply** to apply the setup wizard.

If you want to modify the configured information, click **Previous**.

Figure 3-8 Setup wizard



Setup Wizard

You completed the setup wizard. Please confirm the following information.
If the information is correct, please click Apply for all the settings to take effect.

Region

Region	China	Language	English

Wireless

Wireless Mode	Client	Wireless Encryption	WPA2-PSK-AES
Network Name	[redacted]	Wireless Password	12345678
Output Power	Standard		

Network

LAN IP	[redacted]	Gateway	[redacted]
Subnet Mask	[redacted]		

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 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.