

Wireless Bridge

Quick Start Guide

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (*https://www.hikvision.com*). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE

OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Preface

Applicable Models

This manual is applicable to the DS-3WF Series wireless bridge.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

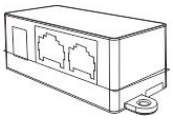
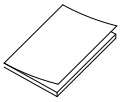
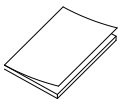
Chapter 1 Introduction

The 2.4 GHz wireless bridge (hereinafter referred to as the device) is used for long-distance wireless connection, which is suited for outdoor video security and transmission between sites in the same LAN.

1.1 Packing List

Please check if there is any damage of the package first. According to the packing list, make sure no item is lost. After checking all the items included, you can continue to install the device.

Table 1-1 Packing List

Item	Quantity	Item	Quantity	Item	Quantity
 Wireless Bridge	× 2	 PoE Injector	× 2	 Power Adapter	× 2
 Cable Tie	× 4	 Quick Start Guide	× 1	 Regulatory Compliance and Safety Information	× 1

1.2 Interface/Button

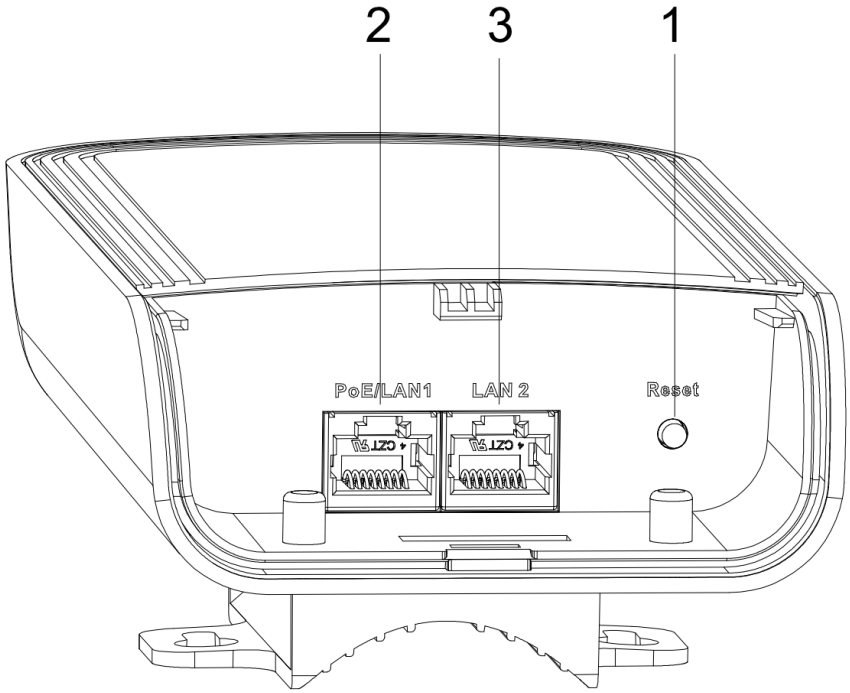


Figure 1-1 Device Interface/Button

Table 1-2 Device Interface/Button Description

No.	Interface/Button	Description
1	Reset	Long press for 4 seconds to restore to factory settings.
2	PoE/LAN 1	The 10/100 Mbps adaptive RJ45 port, also can be used as a PoE port.
3	LAN 2	The 10/100 Mbps adaptive RJ45 port.

1.3 Indicator

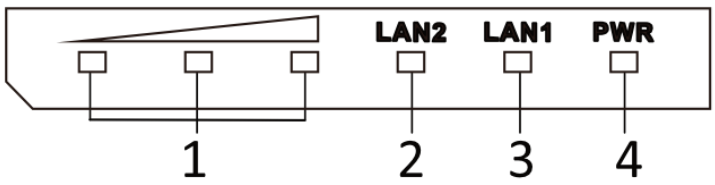
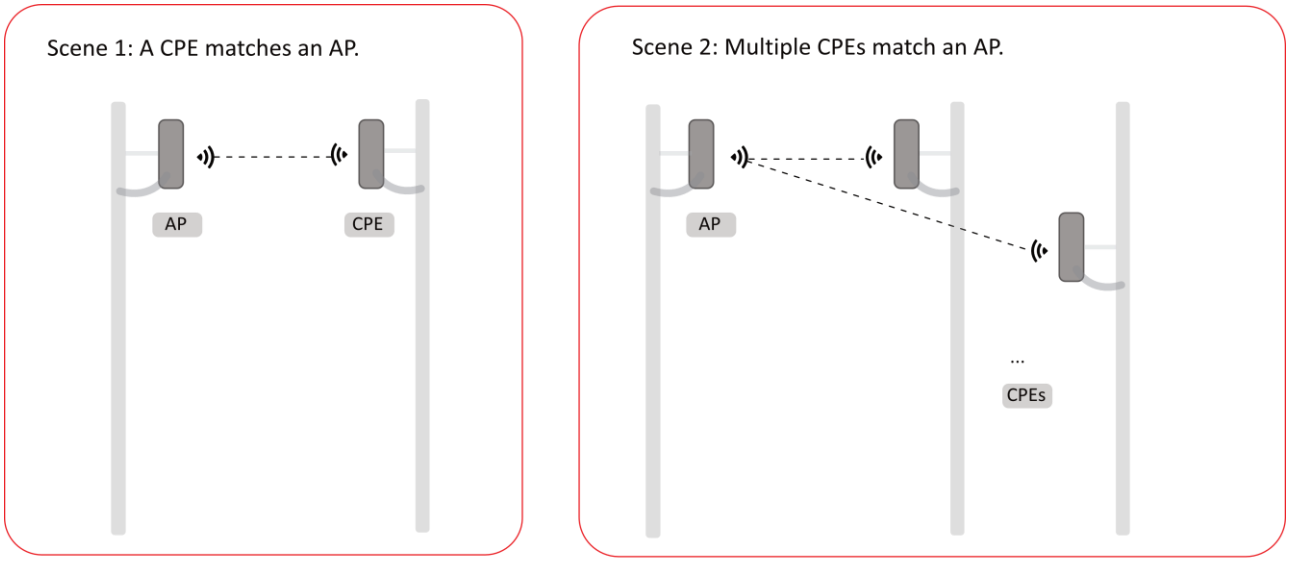


Figure 1-2 Device Indicator

Table 1-3 Device Indicator Description

No.	Indicator	Description	
1	Signal Strength Indicator	Solid on	The devices are matched. ● Solid red, yellow, and green: The wireless signal is strong. ● Solid red and yellow, unlit green: The wireless signal is normal. ● Solid red, unlit yellow and green: The wireless signal is weak. Please adjust the position and direction of the device.
		Unlit	The devices are not matched.
2/3	LAN 1/LAN 2 Indicator	Solid Green	The port is connected.
		Flashing Green	The port is transmitting data. The faster the indicator flashes, the greater the transmission rate is.
		Unlit	The port is disconnected or connection is abnormal.
4	Power Indicator	Solid Green	The device is powered on normally.
		Unlit	No power supply connected or power supply is abnormal.

1.4 Application Scene



The CPE will connect to the AP when its SSID matches that of the AP. The AP's SSID should be unique.

Figure 1-3 Application Scene

Chapter 2 Installation & Connection

2.1 Preparation for Installation

To avoid device damage or personal injury caused by improper usage of the device, please follow the preparations below.

- Use the attached power adapter and PoE injector to power the device.
- The distance between the AP and the CPE should be less than the suggested distance to secure transmission rate.
- Make sure the water-proof cover is installed.
- Protect the power adapter and PoE injector from rain. It is suggested to put them into a waterproof case or keep them in a dry place.
- It is suggested to manage the gap between cover and device with fluid dispensing.
- Install the device in the place where the maintenance personnel can operate easily.
- The devices should be installed face to face and the max. angle of deviation is 30°.
- Disconnect the power supply when you have the device serviced.
- The temperature of the cover area will be high when the device is working. In the circumstances, only personnel with relevant professional knowledge, such as installation and maintenance personnel, are allowed to operate the device.

2.2 Pole-Mounted Installation

Mount the device on the pole with a diameter of 40 to 100 mm using the attached cable ties.

Step 1 Thread the cable ties into the installation holes at the back of the device.

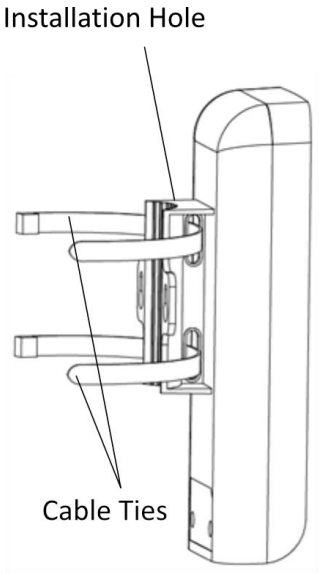


Figure 2-1 Thread Cable Ties

Step 2 Fix and fasten the cable ties on the pole.

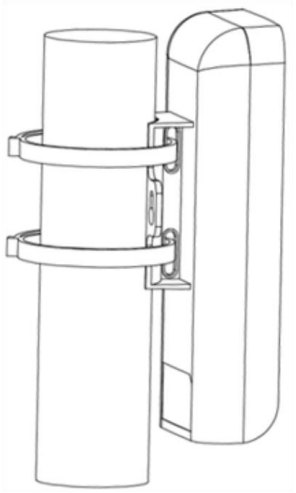


Figure 2-2 Fix Device

Note

Adjust the direction of the device manually to keep the device installed vertically.

2.3 Device Connection

Based on the actual situations, the device can be set to work in the AP mode or CPE mode. Refer to ***Chapter 4 Remote Management*** for detailed configuration of the device working scene. After the working scene of the device is decided, you can connect the device according to the following wiring diagrams.

Note

- Use the attached power adapter and PoE injector to power on the device.
- The PoE injector must be connected to an earthed socket outlet.
- The device should be paired with another device of the same model or another compatible wireless bridge.

2.3.1 AP Connection

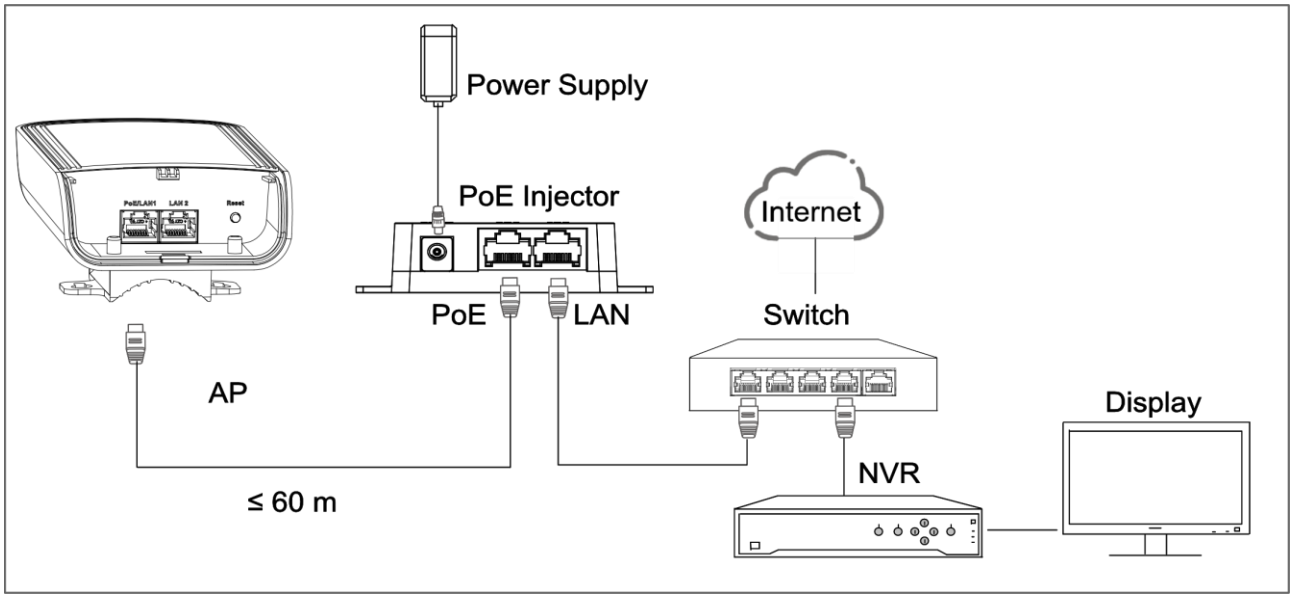


Figure 2-3 AP Connection

2.3.2 CPE Connection

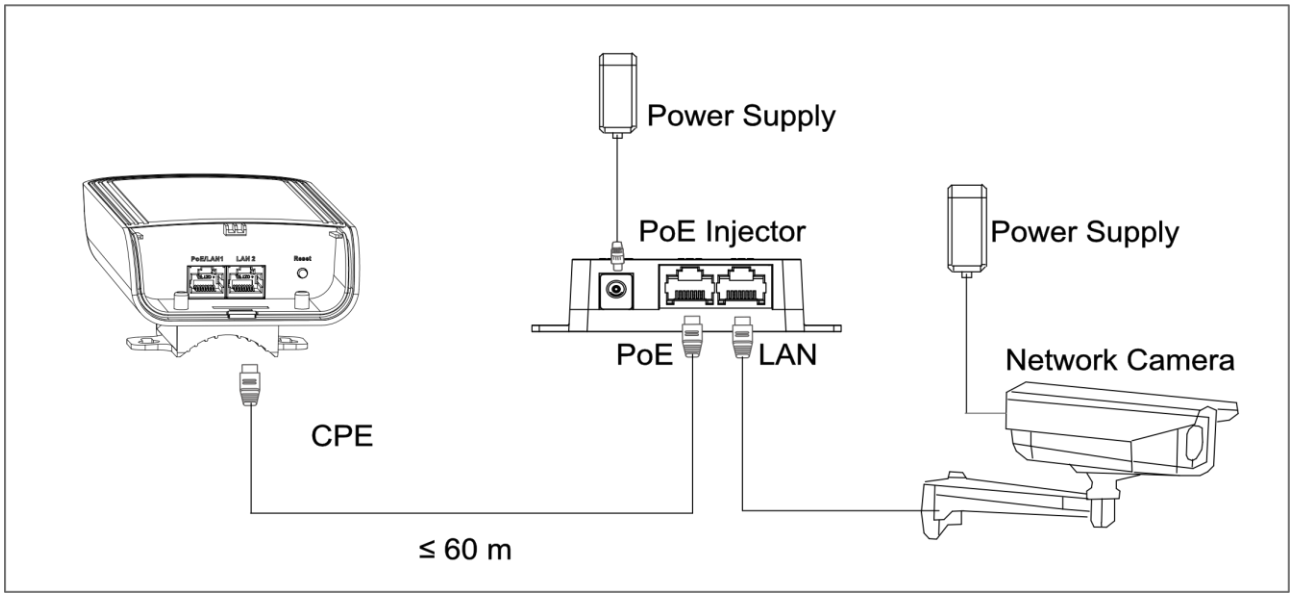


Figure 2-4 CPE Connection

See ***1.3 Indicator*** for details after device connection, to check device working status, network connection, and signal strength.

Chapter 3 Activation

For the first-time access, you need to activate the device by setting a password. The device can be activated and managed via multiple tools, such as web browser, iVMS-4200 client, SADP software, and HikCentral Professional clients. The following part introduces the activation steps of the device on the web browser and on the iVMS-4200 client. For the activation steps of the device on other tools, please refer to the corresponding user manuals in ***Chapter 4 Remote Management***.

Note

- The password strength of the device can be automatically checked. We highly recommend you to change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of the following categories: uppercase letters, lowercase letters, numbers, and special characters) in order to increase the security of your product.
- We recommend you to change your password regularly, especially in the high security system. Changing the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.36
- Default user name: admin

3.2 Activation Using Web Browser

Before you start:

- Make sure the device is powered on and connected to the network correctly.
- Make sure the device is in the same network segment with that of the PC.

Step 1 Open the web browser.

Step 2 Enter the default IP address of the device in the address bar of the web browser.

Step 3 Press **Enter** key.

Step 4 Set **Password**.

Step 5 Read and agree with the disclaimer and select **Country/Region Code**.

Step 6 Click **OK** to finish the activation.

3.3 Activation Using iVMS-4200 Client

Before you start:

- Make sure you have downloaded the latest iVMS-4200 client from the official website.
- Make sure the device is powered on and connected to the network correctly.
- Make sure the device is in the same network segment with that of the PC.

Step 1 Run the iVMS-4200 client.

Step 2 Go to **Device Management→Device**.

Step 3 Click **Online Device** to show the online devices.

The searched online devices are displayed in the list.

Step 4 Select the inactive device and click **Activate**.

Step 5 Create a password and confirm the password.

Step 6 Click **OK**.

Step 7 Click **Add**, and set relevant parameters to add the device to the client.

Step 8 Read and agree with the disclaimer and select **Country/Region Code**.

Step 9 Click **OK** to finish the activation.

Chapter 4 Remote Management

After the device activation, you can manage the device remotely using the web browser, iVMS-4200 client, SADP software, and HikCentral Professional clients.

4.1 Web Browser Operations

Scan the QR code below for detailed guidance.



Figure 4-1 Web User Manual

4.2 iVMS-4200 Client Operations

Scan the QR code below for detailed guidance.



Figure 4-2 iVMS-4200 Client User Manual

4.3 SADP Software Operations

Scan the QR code below for detailed guidance.



Figure 4-3 SADP Software User Manual

4.4 HikCentral Professional Operations

Scan the QR code below for detailed guidance.

Figure 4-4 HikCentral Professional Web Client User Manual

Figure 4-5 HikCentral Professional Control Client User Manual

Figure 4-6 HikCentral Professional Mobile Client Function List


See Far, Go Further