

# **Electronic Shelf Label AP Station DHI- ESL-AP-A**

User's Manual



V1.0.0

# Foreword

## General











This manual introduces the installation, functions and operations of the Electronic Shelf Label (ESL) AP Station (hereinafter referred to as "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

## Model










DHI-ESL-AP-A

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Description
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>ESD PROTECTION</b>	Indicates electrostatic sensitive equipment.
 <b>WARNING ELECTRIC SHOCK</b>	Indicates high voltage danger.
 <b>LASER RADIATION</b>	Indicates strong laser radiation.
 <b>FAN WARNING</b>	Indicates dangerous moving parts, please stay away from moving fan blades.
 <b>WARNING MECHANICAL INJURY</b>	Indicates that equipment parts will cause mechanical wounding to people.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## General Icons

Icon	Meaning
	View icon. View the configurations.
	Search icon. Search the entered keywords.
 or 	Delete icon. Delete the configurations.
 or 	Edit icon. Change the configurations.
 or 	Refresh icon.
	Enable/disable icon. Enable/disable the functions.
*	Required parameters.

## Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2023

## 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.

375697 da hua 2023-07-21

# 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, comply with the guidelines when using it, and keep the manual safe for future reference.

## Transportation Requirements



- Transport the Device under the allowed humidity and temperature conditions.
- Use a factory package or same-quality material for packaging when transporting the Device.

## Storage Requirements



Store the Device under the allowed humidity and temperature conditions.

## Operation Requirements



Use the Device under the allowed humidity and temperature conditions.

## Maintenance Requirements

### **WARNING**

- Only use the wire assembly (power cable) that complies with the regulations in this area and use it within its rated specifications.
- Only use the standard power adapter of the Device, otherwise the user will be responsible for personnel injury or device damage.
- Use the power supply that meets the requirements of SELV (Safety Extra Low Voltage) and supply power in accordance with the rated voltage of (IEC60065) or (IEC60950-1 compliant with Limited Power Source). Note that the power supply requirements are subject to the Device label.



- Prevent liquids from splashing or dripping on the Device.
- Do not press hard, vibrate violently, or soak the Device.
- The grounding terminal on the Device must be well grounded to improve the anti-interference capability of the Device.

# Table of Contents

<b>Foreword</b> .....	<b>1</b>
<b>Important Safeguards and Warnings</b> .....	<b>1</b>
<b>1 Introduction</b> .....	<b>1</b>
1.1 Introduction .....	1
1.2 Features.....	1
1.3 Specifications.....	1
<b>2 Structure</b> .....	<b>3</b>
2.1 Appearance.....	3
2.2 Ports.....	3
<b>3 Installation</b> .....	<b>5</b>
3.1 Unpacking the Box.....	5
3.2 Preparations before Installation.....	5
3.3 Tools.....	6
3.4 Wall Mount .....	6
3.5 Ceiling Mount.....	7
3.6 Power Supply.....	7
3.6.1 By PoE Switch.....	7
3.6.2 By PoE Power Adapter.....	7
<b>4 Configuration</b> .....	<b>9</b>
4.1 Log in to Management Background of AP Station .....	9
4.1.1 If the LAN can automatically assign IP, the AP station can directly connect to the switch	9
4.1.2 If the IP address of the LAN is static, the PC direct connection to the AP station is required for the first access to AP station background.....	9
4.2 Set Static IP of AP Station.....	10
4.3 Set Server Address.....	11
<b>5 FAQ</b> .....	<b>12</b>
Appendix 1 <b>Cybersecurity Recommendations</b> .....	<b>13</b>

# 1 Introduction

## 1.1 Introduction

Not only is the Electronic Shelf Label (ESL) AP Station the core of the ESL transmission system, but it is the data transceiver and transfer device between the ESL and the background. As a Bluetooth /Wi-Fi dual-mode indoor wireless base station, the AP station gives full play to its advantages such as superior extensibility, wide coverage, convenient installation, high security and outstanding stability. Cooperating with ESLs, it can quickly realize the change of commodity prices. Besides, it plays a significant role in improving the efficiency of picking, reducing costs and more. It has proven its unmatched performance in the wide application in supermarkets, retail stores and other fields.

## 1.2 Features

- Superior extensibility: one AP station can manage up to 5,000 ESLs, which has more stable performance with multi-AP load balancing.
- Wide coverage: one AP station covers an indoor area of up to 700 square meters, and the coverage diameter is up to 40 meters in the accessible indoor environment.
- Convenient installation: supports the following functions: plug and play, AP station automatic network access, cloud automatic activation, ESL automatic access, and more convenient Bluetooth management.
- Superior security and stability: AES encryption technology contributes to impeccable protection for information and privacy security.
- Intelligent system: supports smooth roaming in the wireless environment, and ESLs can automatically search compatible AP stations. It is equipped with advanced technologies such as load balancing and frequency hopping.

## 1.3 Specifications

Table 1-1 Specifications

Specifications	Details	Descriptions
Structure Material	Casing Material	ABS Plastic
	Indicator Cover	Translucent PC
Dimensions and Weight	Dimensions	180 mm × 180 mm × 33 mm (7.09" × 7.09" × 1.30")
	Gross Weight	780 g (1.72 lb)

Specifications	Details	Descriptions
	Net Weight	500 g (1.10 lb)
CPU	CPU Main Frequency	775 MHz
	Chip Solution	Gaotong 9563
Memory	Memory	16 M Flash+128 M Ram
Wireless	Bluetooth Communication Method	BLE Private Protocol
	Bluetooth Module	4
	Bluetooth Transmission Speed	Up: 1 Mbps Down: 1 Mbps
	Transmission Frequency	7 dBm
	Antenna Gain	3 dBi
	Antenna Characteristics	4-Channel Omnidirectional Antenna
	Wi-Fi Standard	2.4 GHZ+5 GHz
	Wi-Fi Frequency	802.11 b/g/n/ac
	Wi-Fi Transmission Speed	1167 Mbps
Wired and Functions	Ethernet Module	Connection Rate 1,000M (self-adaptive)
	Auto-negotiation	Yes
	Auto-turning	Yes
	DHCP	Yes



# 2 Structure

## 2.1 Appearance

Figure 2-1 Appearance



## 2.2 Ports

Figure 2-2 Descriptions of AP station ports



Table 2-1 Descriptions of AP station ports

No.	Name	Functions
1	ETH	PoE Port
2	Reset	Reset key. Press the key to reboot the system. Long Press the key for over 5 seconds to reset the system to factory settings.
3	Status LED	Solid on: normal connection Blink: data is being transmitted...

# 3 Installation

## 3.1 Unpacking the Box

When receiving the Device from the transportation company, refer to the following checklist to check the package. If you find device damage or component loss, contact the after-sales service.

Table 3-1 Checklist


No.	Item	Description	
1	Overall packing	Appearance	Obvious damage
		Packaging	Accidental impact
		Components	Complete or not
2	Main body	Appearance	Obvious damage
		Model	Whether consistent with the order contract
		Labels on the Device	Whether the labels are torn off  Do not tear off and discard the labels. Or the warranty to this Device will be compromised. You might be asked to provide the serial number of this Device when you call the after-sales service.

Table 3-2 Packing list



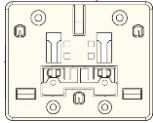



Name	Quantity
AP station	1
Network cable	1
Desktop PoE power supply	1
Power cable	1
Square ceiling hanging plate	1
Plastic expansion tube	4
Cross pan head self-tapping screw	4
Cross pan head screw	2
M3 Hex nut	2

## 3.2 Preparations before Installation

- During the Device installation, the installation personnel must take necessary safety measures to ensure personal safety.
- Do not place the Device and installation tools on the pedestrian passage, otherwise the Device may be damaged.
- The Device supports ceiling and wall mount. Please check the bearing capacity of ceiling and wall before installation to ensure safety.

## 3.3 Tools

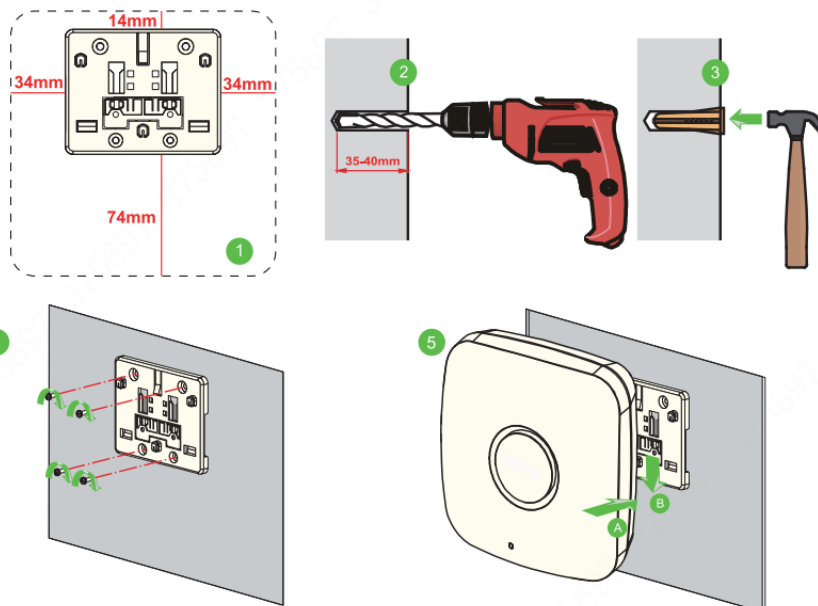
Table 3-3 Tools

Name	Image	Name	Image
Phillips screwdriver		Claw hammer	
Mounting plate		Ladder	
Electric drill		Marker	

## 3.4 Wall Mount

1. According to the dimensions shown in the figure, use a marker to mark the location of holes to be drilled.
2. Select a 6mm drill bit, and drill holes with a depth of 35-40 mm according to the marked location.
3. Use a claw hammer to knock three expansion screw sleeves into the holes and secure them tightly.
4. Align the mounting holes of the mounting plate with the expansion screw sleeves, and use three self-tapping screws to install the mounting plate on the wall.
5. Align the mounting holes at the back of the Device with the mounting screws on the mounting plate, hang the Device, and gently pull the Device in place in the outlet direction of the network cable to finish the installation.

Figure 3-1 Installation

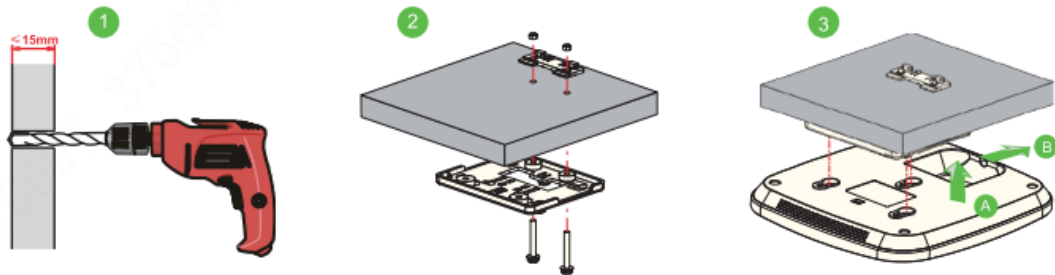


Before installing the Device on the mounting plate, connect the network cable, otherwise the network cable cannot be connected after the installation.

## 3.5 Ceiling Mount

1. Remove the ceiling, select a 4mm drill bit, and use an electric drill to drill two holes in the ceiling between which the spacing is 35 mm.
2. Use a locking slider to fasten the sheet metal mounting plate and the ceiling, that is, place the mounting plate and locking slider on two different sides of the ceiling, and then fasten them with screws.
3. Align the mounting holes at the back of the Device with the mounting screws on the mounting plate, hang the Device, and gently pull the Device in place in the outlet direction of the network cable to finish the installation.

Figure 3-2 Installation diagram



- After the installation is complete, the AP station needs to be connected to the network cable that can automatically get the IP address to ensure Internet access.
- When powered on, the AP station can automatically connect the surrounding ESLs and synchronize with the system after the Internet access.

## 3.6 Power Supply

### 3.6.1 By PoE Switch

The AP station uses PoE switch direct connection for power supply. Use a network cable to connect the network port of the AP station and the network port of the PoE switch to realize data and power transmission.

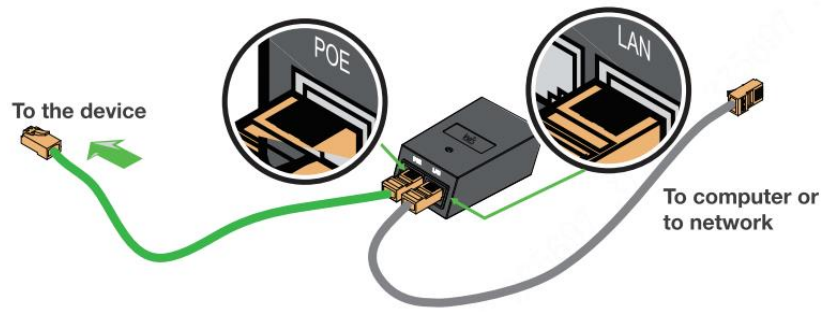
Figure 3-3 Connection between PoE switch and AP station



### 3.6.2 By PoE Power Adapter

The AP station uses a PoE power adapter for power supply. Power on the original PoE power adapter, and use a network cable to connect the PoE port of the power adapter to the network port of the AP station (the distance should be no more than 100 m). Then connect the LAN port on the power adapter to the site network equipment, such as a switch or router, to achieve data transmission.

Figure 3-4 Connection between PoE power adapter and AP station



Please use the original PoE power adapter. If you need to use other brands of adapters or PoE switches, please communicate with the service provider in advance.

# 4 Configuration

## 4.1 Log in to Management Background of AP Station

### 4.1.1 If the LAN can automatically assign IP, the AP station can directly connect to the switch

By default, the AP station uses DHCP to get an IP address. Connect the AP station to a network with a DHCP server to get an IP address. There are two ways to view the AP station IP:

Method 1: Use Wimanager (IP scanning tool) to scan for an IP address.

Step 1 Connect the PC and the AP station in the same network segment.

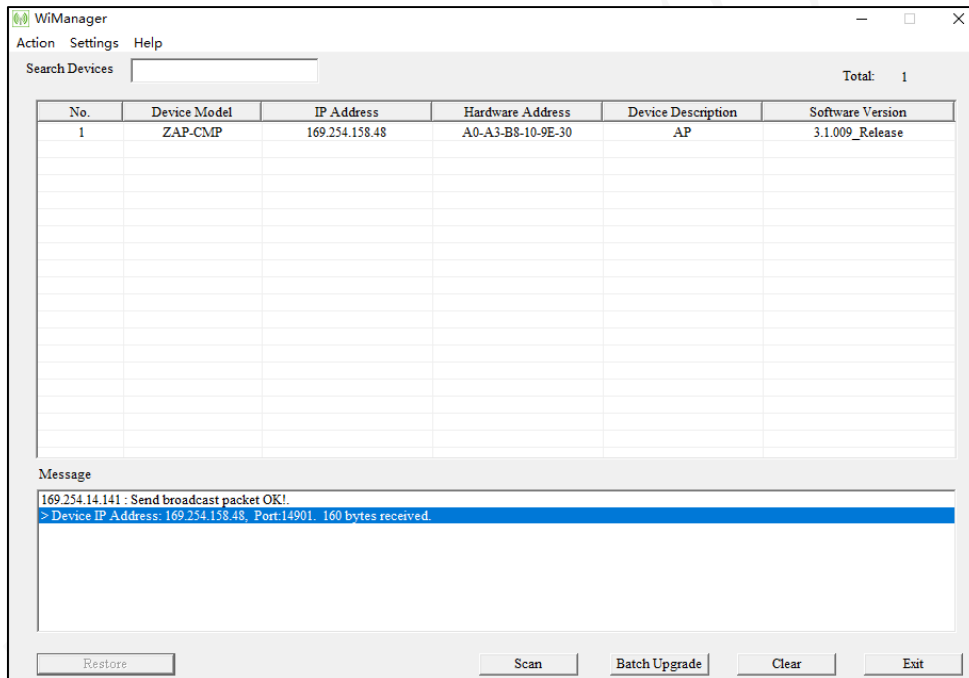
Step 2 Double-click **Wimanager.exe** to open the scanning software.

Step 3 Click **Scan** to get IP addresses of the AP station in the same network segment.



Please contact the installation service personnel to get Wimanager.

Figure 4-1 Get IP address



Method 2: Based on the MAC address of the AP station (viewed on the back of the AP station), confirm the IP address on the DHCP server (usually the gateway device) which assigns IP addresses. After getting the IP address of the AP station, enter it in the browser to access the background management system with its login password (Admin369).

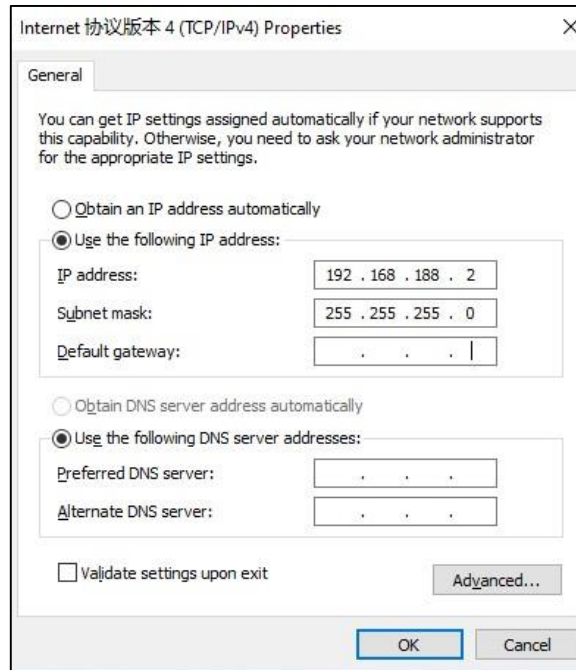
### 4.1.2 If the IP address of the LAN is static, the PC direct connection to the AP station is required for the first access to AP station background

The default IP address of a new AP station is 192.168.188.1. If you have used it before, please reset the AP station first:

Step 1 Remove the PoE power module and insert the plug into the socket. Connect the PoE port of the PoE power module to the network port of the AP station, and connect the LAN port of the PoE module to the PC.

Step 2 Set the IP address and subnet mask of the PC to 192.168.188.2 and 255.255.255.0 respectively, as shown in the following figure.

Figure 4-2 Set IP address



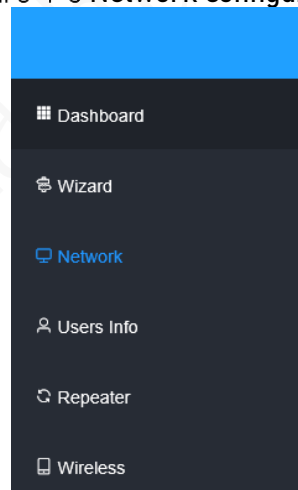
Step 3 Enter 192.168.188.1 in the browser of the PC to log in to the AP station management background.

## 4.2 Set Static IP of AP Station

If the LAN IP address is automatically assigned by DHCP, ignore this part. If the server address is a domain name, the DNS address is required to be configured:

Step 1 After entering the website, click **Network** in the left status bar.

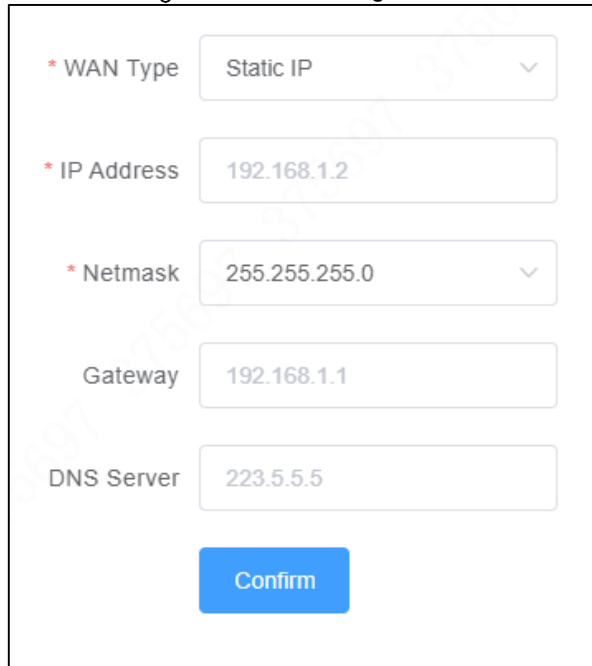
Figure 4-3 Network configuration



Step 2 For **WAN Type**, select **Static IP** in the drop-down list. For **IP Address**, enter an IP address.



Figure 4-4 IP configuration



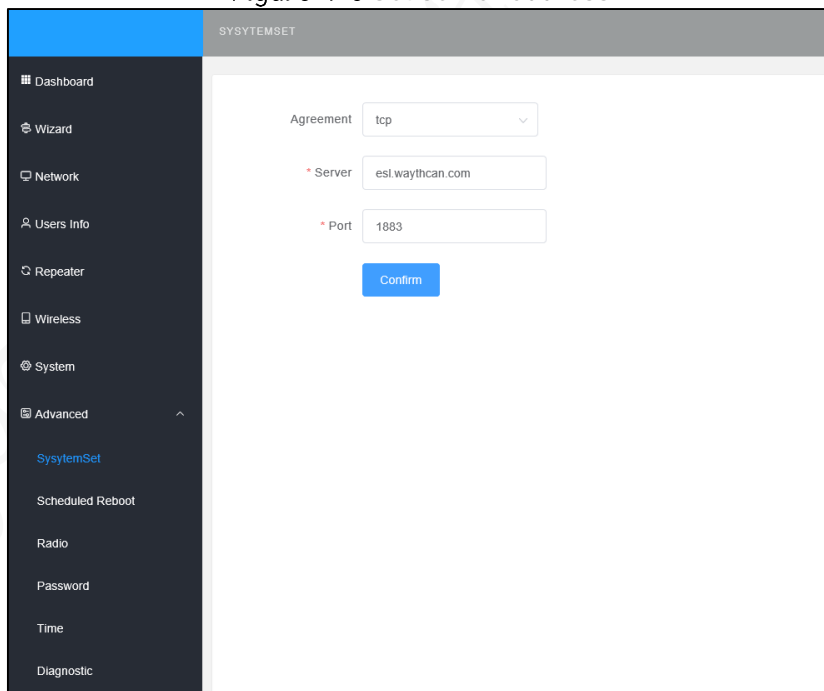
A screenshot of a web interface for IP configuration. It features five input fields: 'WAN Type' (Static IP), 'IP Address' (192.168.1.2), 'Netmask' (255.255.255.0), 'Gateway' (192.168.1.1), and 'DNS Server' (223.5.5.5). A blue 'Confirm' button is located at the bottom.

Step 3 Click **Confirm** to save the configurations.

## 4.3 Set Server Address

Select **Advanced > SystemSet** in the left status bar. For **Server**, enter the server address and click **Confirm** to save the configuration.

Figure 4-5 Set server address



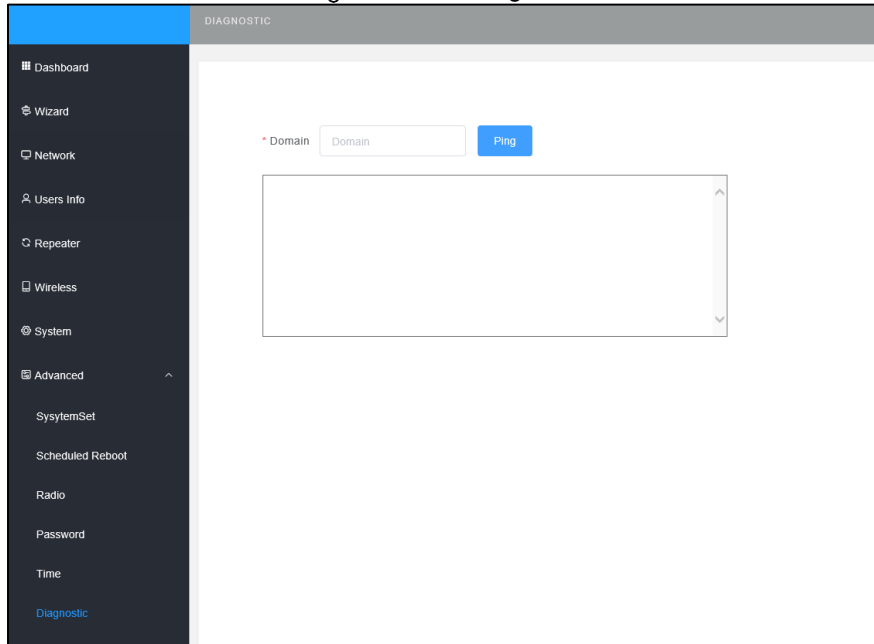
A screenshot of the 'SYSTEMSET' configuration page. The left sidebar shows a menu with 'Advanced' expanded to 'SystemSet'. The main content area has three fields: 'Agreement' (tcp), '\* Server' (esl.waythcan.com), and '\* Port' (1883). A blue 'Confirm' button is at the bottom.

# 5 FAQ

Use the background detection tool to check whether the network connection of the server is normal.

- In the left status bar, select **Advanced > Diagnostic**.
- Enter the IP address and click **Ping** to check whether the network connection is normal.

Figure 5-1 IP diagnosis



**The AP station fails to be connected due to the unavailable port 1833.**

- Solution: The network is connected but the server cannot be connected. Check whether port 1833 is available.

**Check whether there is a DNS address when configuring a static IP address (if not, domain name resolution will be affected).**

- Solution: If the server address is a domain name, the static IP address must be configured with a DNS address.

**The indicator is not on after the AP station is connected.**

- Solution: Check whether the network cable is properly connected (for details, see 2.2 Ports).

**Reset the AP station.**

- Solution: When the AP station is powered on, long press the **Reset** button for 8 seconds to complete the reset.

# 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.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [overseas@dahuatech.com](mailto:overseas@dahuatech.com) | Fax: +86-571-87688815 | Tel: +86-571-87688883