Panoramic Fisheye Network Camera

Quick Start Guide

V1.0.1

Dahua Technology USA Inc.

Foreword

General

This manual offers reference material and general information about the basic operation, maintenance, and troubleshooting for a Dahua Network Camera. Read, follow, and retain the following safety instructions. Heed all warning on the unit and in the operating instructions before operating the unit. Keep this guide for future reference.

Safety Instructions

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

Signal Words	Meaning
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.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	June 2019
2	V1.0.1	Revised for North America	January 2020

Privacy Protection Notice

As the device user or data controller, you may collect personal data such as face images, fingerprints, license plate number, email address, phone number, GPS location and other sensitive or private information. You must ensure that your organization is in compliance with local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact

About the Guide

- This user guide has been compiled with great care and the information it contains has been thoroughly reviewed and verified.
- The text was complete and correct at the time of printing. This guide may be periodically updated to reflect changes to the product or to correct previous information and the content of this guide can change without notice.
- If you encounter an error or have any questions regarding the contents of this guide, contact customer service for the latest documentation and supplementary information.
- Dahua accepts no liability for damage resulting directly or indirectly from faults, incompleteness, or discrepancies between this guide and the product described. Dahua is not liable for any loss caused by installation, operation, or maintenance inconsistent with the information in this guide.
- All the designs and software are subject to change without prior written notice. The product updates may cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- Video loss is inherent to all digital surveillance and recording devices; therefore Dahua cannot be held liable for any damage that results from missing video information. To minimize the occurrence of lost digital information, Dahua recommends multiple, redundant recording systems, and adoption of backup procedure for all data.
- All trademarks, registered trademarks and the company names in the Guide 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.
- Contact the supplier or customer service if you encounter any issue while using this unit.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it well for future reference.

Installation and Maintenance Professionals Requirements

- All installation and maintenance professionals must have adequate qualifications or experiences to install and maintain CCTV systems and electric apparatus, and to work above the ground. The professionals must have the following knowledge and operation skills:
- Basic knowledge and installation of CCTV systems.
- Basic knowledge and operation skills of low voltage wiring and low voltage electronic circuit wire connection.
- Basic knowledge and operation skills of electric apparatus installation and maintenance in hazardous sites.

Power Requirements

- Install the unit in accordance with the manufacturer's instructions and in accordance with applicable local codes.
- All installation and operation must conform to your local electrical safety codes.
- Do not overload outlets and extension cords, which may cause fire or electrical shock.
- Do not place the camera near or in a place where the camera may contact overhead power lines, power circuits, or electrical lights.
- Ensure power conforms to SELV (Safety Extra Low Voltage) and that the limited power source is rated AC 24V as specified in IEC60950-1. (Power supply requirement is subject to the device label).
- All input/output ports are SELV circuits. Ensure that SELV circuits are connected only to other SELV circuits.
- Ground the unit using the ground connection of the power supply to protect the unit from damage, especially in damp environments.
- Please install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Protect the plug and power cord from foot traffic, being pinched, and its exit from the unit.
- Do not attempt to service the unit. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified personnel.

- If the unit is damaged and requires service, unplug the unit from the main AC power supply and from the PoE supply and refer to qualified service personnel. Damage may include, but is not limited to:
  - The power supply cord or plug is damaged.
  - Liquid has spilled in or on the unit.
  - An object has fallen on the unit.
  - The unit has been dropped and the housing is damaged.
  - The unit displays a marked change in performance.
  - The unit does not operate in the expected manner when the user correctly follows the proper operating procedures.
- Ensure a service technician uses replacement parts specified by the manufacturer, or that have the same characteristics as the original parts. Unauthorized parts may cause fire, electrical shock, or other hazards. Dahua is not liable for any damage or harm caused by unauthorized modifications or repairs.
- Perform safety checks after completion of service or repairs to the unit.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Incorporate a readily accessible disconnect device in the building installation wiring for quick power disconnect to the camera.
- Dahua assumes no liability or responsibility for any fire or electrical shock caused by improper handling or installation.

Application Environment Requirements

- Please use the device within the allowed humidity (<95%RH) and altitude (<3000m).
- Transport, use, and store the unit within the specified temperature and humidity range.
- Do not place the unit in a wet, dusty, extremely hot or an extremely cold environment; and avoid environments with strong electromagnetic radiation or unstable lighting.
- Do not use the device in the corrosive environment such as high salt fog area (sea, beach and coastal area), acid gas environment and chemical plants.
- Do not use the device in applications with strong vibrations such as in boats and vehicles.
- Never push objects of any kind into this unit through openings as they may touch dangerous voltage points or cause a short circuit that may result in fire or electrical shock. Take care to not spill any liquid on the unit.
- If your installation environment is subjected to one of the conditions above, contact our sales staff to purchase cameras intended for the particular environment.
- Please don’t install the device near the place with heat source, such as radiator, heater, stove or other heating equipment, which is to avoid fire.
- Do not aim the lens at an intense radiation source (such as the sun, a laser, and molten steel for example) to avoid damage to the thermal detector.
- Use the factory default package or material with equal quality to pack the device when transporting.

Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the unit. This part of the unit is hot and may cause a burn.
- Do not open or dismantle the device; there are no components that a user can fix or replace. Opening the unit may cause water leakage or expose components to direct light. Contact the manufacturer or a qualified service representative to service the camera or to replace a component, including the desiccant.
- Dahua recommends the use of a thunder-proof device in concert with the unit.
- Do not touch the CCD or the CMOS optic sensor. Use a blower to clean dust or dirt on the lens surface. Use a dry cloth dampened with alcohol and gently wipe away any dust on the lens.
- Use a dry soft cloth to clean the unit's housing. If the unit is particularly dusty, use water to dilute a mild detergent, apply the diluted detergent to a soft cloth, then gently clean the device. Finally, use a dry cloth to wipe the unit dry. Do not use a volatile solvent like alcohol, benzene, or thinner; or use a strong detergent with abrasives, which may damage the surface coating or reduce the working performance of the unit.
- Do not touch or wipe a dome cover during installation, this cover is an optical device. Refer to the following methods clean the dome cover:
- Stained with dirt: Use an oil-free soft brush or blower to gently remove the dirt.
- Stained with grease or fingerprints: Use a soft cloth to wipe gently the water droplet or the oil from the dome cover. Then, use an oil-free cotton cloth or paper soaked with alcohol or detergent to clean the lens from the center of the dome to outside. Change the cloth several times to ensure the dome cover is clean.

 WARNING

- Modify the default password after login.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Internal and external ground connection should be stable.
- Do not supply power via the Ethernet connection (PoE) when power is already supplied via the power connector.
- Disconnect power before device maintenance and overhaul. It is prohibited to open the cover with power on in an explosive environment.
- Please contact the local dealer or the nearest service center if the device fails to work normally, please don't dismantle or modify the device.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

- **Change Passwords and Use Strong Passwords**
  - The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.
- **Update Firmware**
  - As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

Recommendations to improve your network security

- **Change Passwords Regularly**
  - The length should be greater than 8 characters;
  - Include at least two types of characters; character types include upper and lower case letters, numbers, and symbols;
  - Do not use an account name or the account name in reverse order;
  - Do not use sequential characters, such as 123, abc, etc.;
  - Do not use repeated characters, such as 111, aaa, etc.;
- **Change Default HTTP and TCP Ports**
  - Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
  - These ports can be changed to any set of numbers between 1025 and 65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.
- **Update Firmware and Client Software**
  - Keep your network-enabled equipment (such as NVRs, DVRs, IP cameras, 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.
  - Download and use the latest version of client software.
- **Enable HTTPS/SSL**
  - Set up an SSL Certificate and enable HTTPS to encrypt all communication between your devices and recorder.
- **Enable IP Filter**
  - Enable the IP filter to prevent unauthorized access to the system.

- **Change ONVIF Password**
  - Older IP camera firmware does not automatically change the ONVIF password when the system credentials are changed. Update the camera's firmware to the latest revision or manually change the ONVIF password.
- **Forward Only Ports You Need**
  - Forward only the HTTP and TCP ports that are requited. Do not forward a wide range of numbers to the device. Do not DMZ the device's IP address.
  - Do not forward any ports for individual cameras if they are all connected to a recorder on site. Simply forward the NVR port.
- **Disable Auto-Login on SmartPSS**
  - Disable the Auto-Login feature on SmartPSS installed on a computer that is used by multiple people. Disabling auto-login prevents users without the appropriate credentials from accessing the system.
- **Use a Different Username and Password for SmartPSS**
  - Do not a username/password combination that you have in use for other accounts, including social media, bank account, or email in case the account is compromised. Use a different username and password for your security system to make it difficult for an unauthorized user to gain access to the IP system.
- **Limit Features of Guest Accounts**
  - Ensure that each user has rights to features and functions they need to perform their job.
- **Disable Unnecessary Services and Choose Secure Modes**
  - Turn off specific services, such as SNMP, SMTP, and UPnP, to reduce network compromise from unused services.
  - It is recommended to 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 a mailbox server.
  - FTP: Choose SFTP and use strong passwords.
  - AP hotspot: Choose WPA2-PSK encryption mode and use strong passwords.
- **Multicast**
  - Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast. Deactivate this feature if not in use to enhance network security.
- **Check the Log**
  - The information stored in the network log file is limited due to the equipment's limited storage capacity. Enable the network log function to ensure that the critical logs are synchronized to the network log server if saving log files is required.
  - Check the system log if you suspect that someone has gained unauthorized access to the system. The system log shows the IP addresses used to login to the system and the devices accessed.
- **Physically Lock Down the Device**
  - Perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement access control permission and key management to prevent unauthorized personnel from accessing the equipment.

- **Connect IP Cameras to the PoE Ports on the Back of an NVR**
  - Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.
- **Isolate NVR and IP Camera Network**
  - Ensure that the network for the NVR and IP cameras should not be the same network as a public computer network. Separate networks prevent unauthorized users accessing the same network the security system.
- **Secure Auditing**
  - Check online users regularly to ensure unauthorized accounts are not logged in to a device.
  - Check the equipment log to access the IP addresses used to login to devices and their key operations.

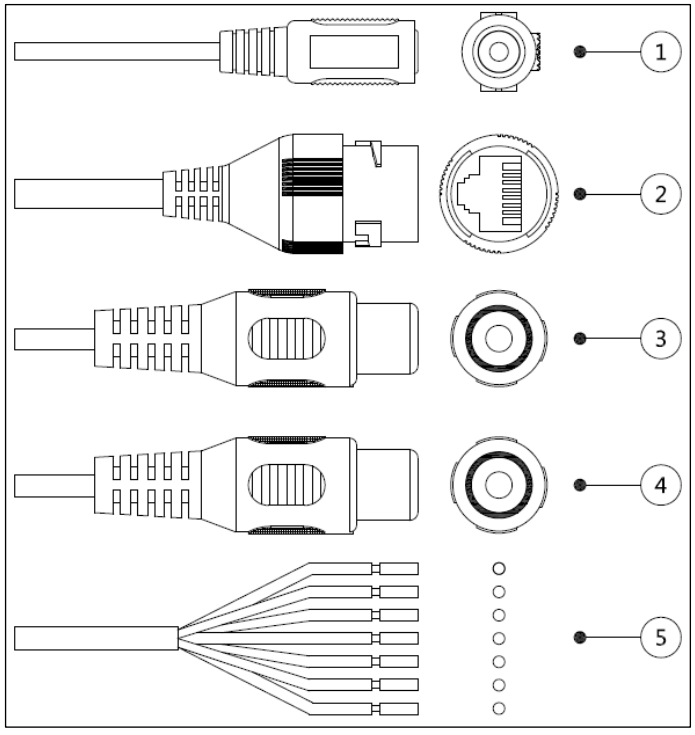
Table of Contents

1 Introduction

Dahua Fisheye Cameras provide detailed panoramic views in a compact, low-profile design. The progressive-scan sensor combined with a fisheye lens provide a high-quality 360° panoramic view without blind spots, making the camera the ideal solution for wide and open areas, such as airports, shopping malls and banks. The camera offers Analytics+ functions at the edge – performing complex real-time perimeter people counting and queue management. The IP67 environmental protection rating and the IK10 vandal resistance ensure the camera operates in the harshest environments.

1.1 Cables

- Cable type might vary with device.
- Waterproof all cable joints with insulating and waterproof tape to avoid short circuit and water damage.



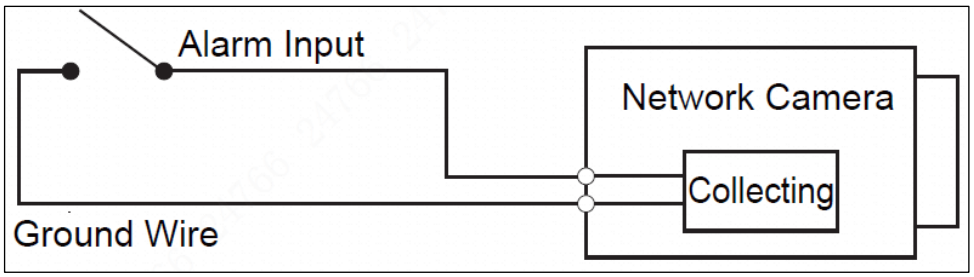
No.	**Port Name**	**Description**
1	12 VDC Power Input	Please be sure to supply power as instructed in the Guide.
2	Ethernet Port	Connects to network with network cable. ● Provides power to the device with PoE.
3	Audio Input	Connects to sound-pick-up device to receive audio signal.
4	Audio Output	Connects to speaker to output audio signal.
5	Alarm I/O	Includes alarm signal input and output ports.

1.2 Alarm Wiring

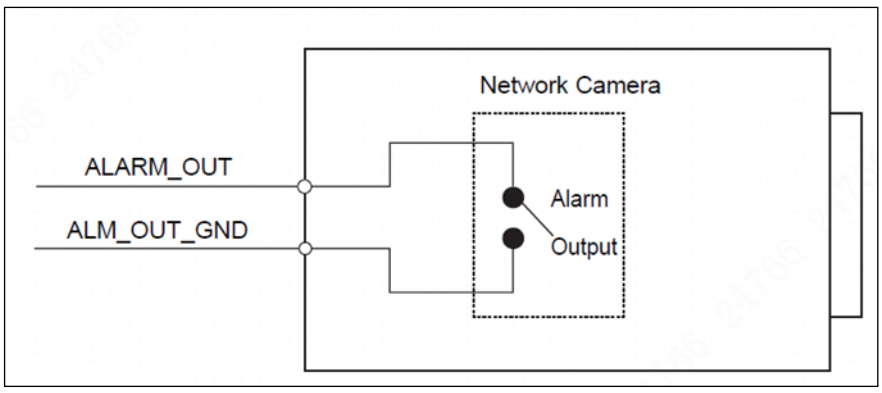
No.	Connector name	Description
1	ALARM_OUT1	Alarm output port 1 outputs alarm signal to alarm device. When connecting to alarm device, only the ALARM_OUT 1 port and ALARM_OUT_GND 1 port with the same number can be used together.
2	ALM_OUT_GND1	
3	ALARM_IN1	Alarm input port 1 receives the switch signal of external alarm source.
4	ALARM_IN2	Alarm input port 2 receives the switch signal of external alarm source.
5	ALM_IN_GND	Alarm input GND.
6	ALARM_OUT2	Alarm output port 2 outputs alarm signal to alarm device. When connecting to alarm device, only the ALARM_OUT 2 port and ALARM_OUT_GND 2 port with the same number can be used together.
7	ALM_OUT_GND2	

1.3 Connecting Alarm Input/Output

1. Connect alarm input device to the alarm input end of the I/O port. Device collects different states of alarm input port when the input signal is idling and being grounded. Device collects logic "1" when input signal connecting to 3.3V or idling; device collects logic "0" when input signal being grounded.



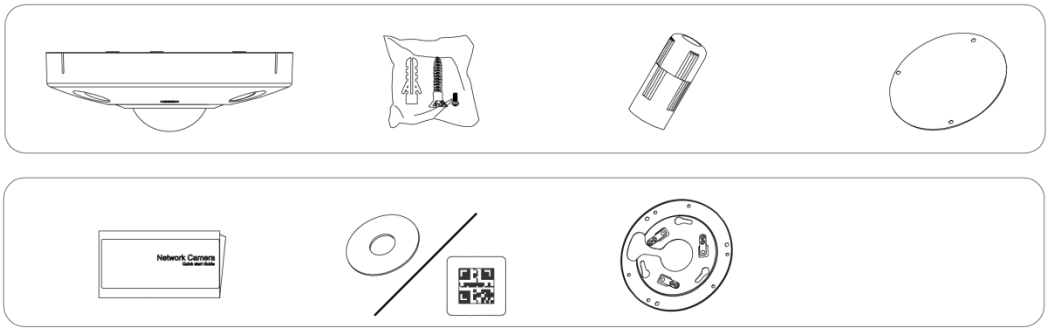
2. Connect alarm output device to the alarm output end of the I/O port. The alarm output is relay switch output, which can only connect to NO alarm devices. The ALARM_OUT port and the ALM_OUT_GND port with the same number constitute a switch for alarm output, see Figure 1-3. The switch is open normally and closes when there is alarm output.



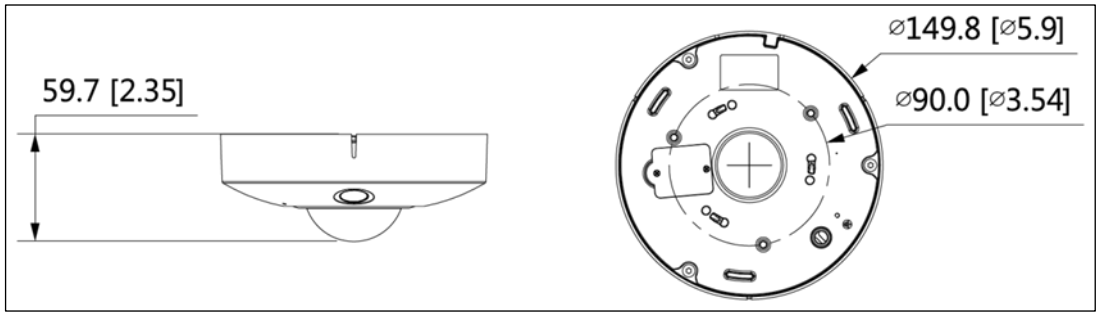
3. Log in web interface, and configure alarm input and alarm output in alarm setting.
    - The alarm input in the web interface is corresponding to the alarm input end of the I/O port. There will be high level and low level alarm signal generated by the alarm input device when alarm occurs, set the input mode to NO if the signal is high level and to NC if the signal is low level.
    - The alarm output in the web interface is corresponding to the alarm output end of the device, which is also the alarm output end of the I/O port.

2 Installation

- The tools required for the installation including electric drill are not provided in the packing.
- The operation manual and related tool are contained in the disk or the QR code, and the actual packing shall prevail.

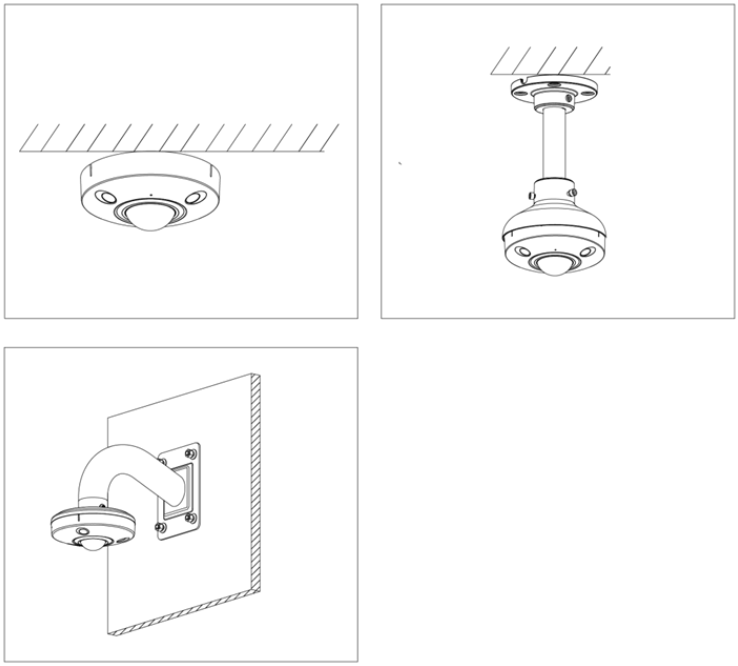


2.1 Dimensions



2.2 Mounting Methods

The fisheye camera can be mounted in several different ways:

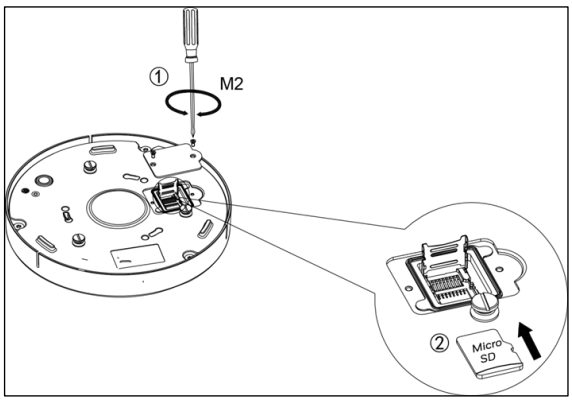


2.3 Preparing the Installation

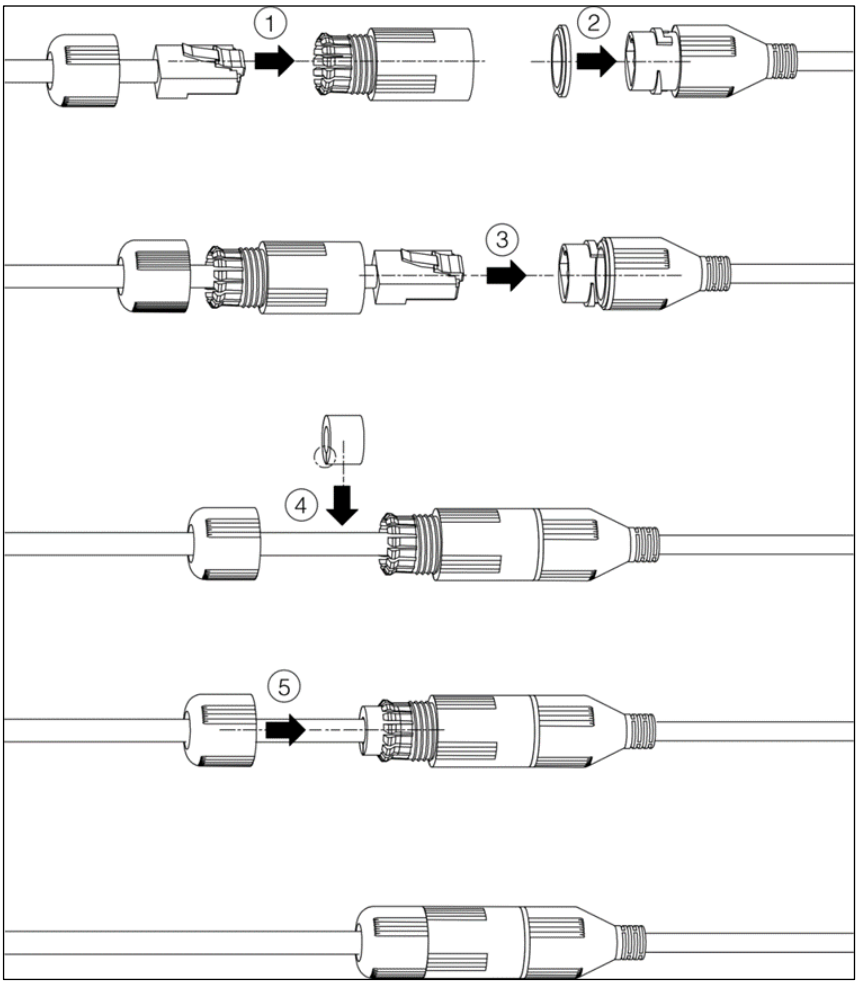
- Make sure the mounting surface is strong enough to hold at least three times the total weight of camera and mounting hardware.
- Ensure the camera is properly grounded. The grounding connection (M2.5 screw) is located next to the cable exit hole on the back of the bottom cover.

2.4 Installing a SD Card

1. Disconnect power to the camera.
2. Remove the panel on the bottom of the camera.
3. Lift the cover from the SD card slot.
4. Gently insert the SD card into the slot until it clicks in place.
5. Lower the cover.
6. Replace the panel.
7. Press the Reset button for 10 seconds to reset the device.

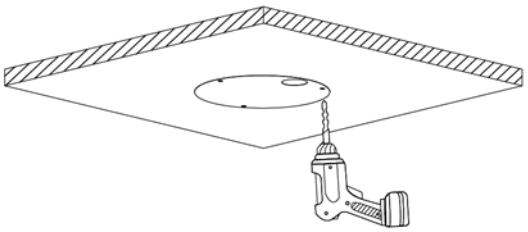


2.5 Using the Waterproof Ethernet Connection

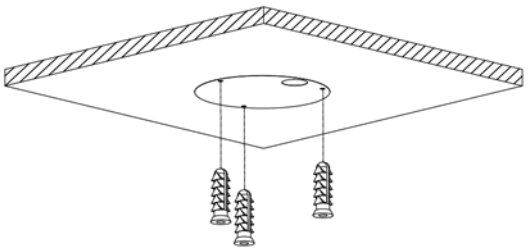


2.6 Mounting to a Ceiling

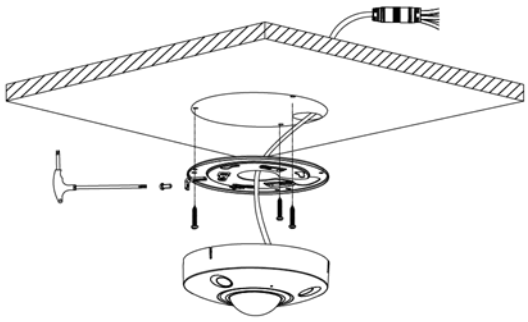
1



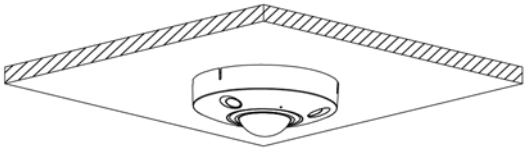
2



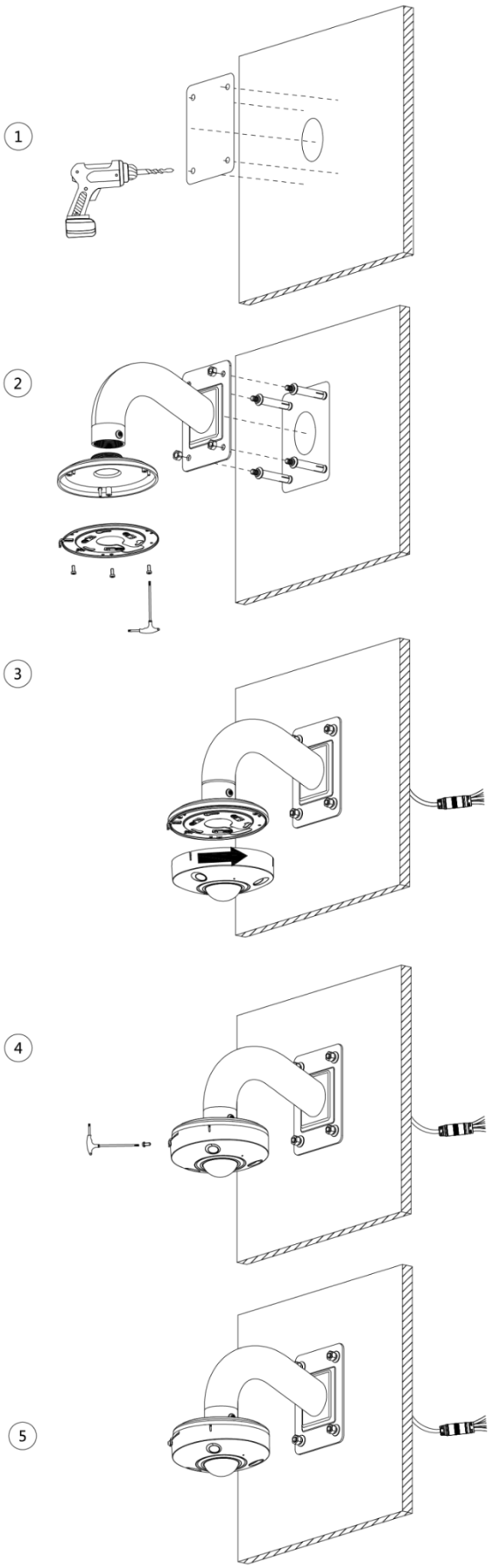
3



4



2.7 Mounting to a Wall



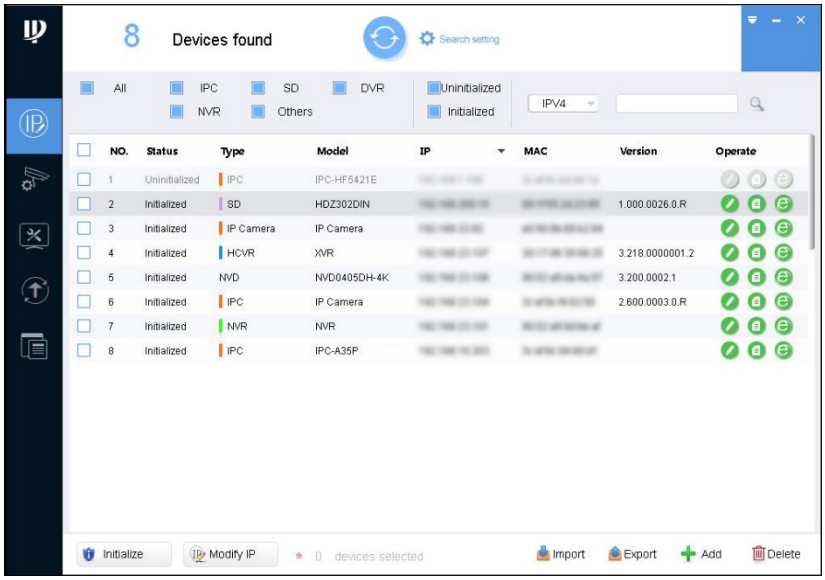
3 Network Configuration

Device initialization and IP setting can be finished with the "ConfigTool" or in web interface.

- Device initialization is available on select models, and it is required at first use and after device is being reset.
- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stays in the same network segment.
- Planning useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

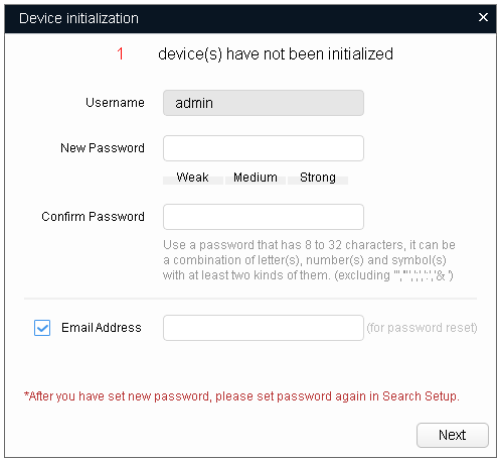
3.1 Initializing the Device

1. Double-click "ConfigTool.exe" to open the tool.
2. Click the IP Icon.



3. Click Search Setting.
4. Enter the start IP and end IP of the network segment in which you want to search devices, and then click OK. All the devices found in the network segment are listed.
5. Select one or several devices with status Uninitialized, and then click Initialize.

6. Select the appropriate devices and click Initialize.

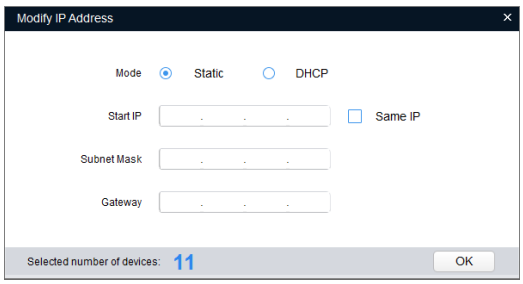


7. Set and confirm the password of the devices, and then enter a valid email address. Click Next.
8. Select the options according to your needs and then click OK.
9. Click Finish.

3.2 Modifying a Device IP Address

- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batch.
- Modifying IP addresses in batch is available only when the corresponding devices have the same login password.

1. Follow steps 1 through in the section above to initializing the device and to search for devices in your network segment. Ensure the username and password are the same as set during the device initialization.
2. Select the devices whose IP addresses need to be modified, and then click Modify IP.



3. Select Static mode and enter start IP, subnet mask, and gateway.
   - IP addresses of multiple devices will be set to the same if you select Same IP.
   - If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select DHCP.
4. Click Ok.

3.3 Logging into the Web Interface

1. Open the browser, enter the IP address of the device in the address bar, and press Enter. Follow the instructions to finish the settings.
2. Enter user name and password in the login box, and then click Login.
3. For first time login, Click Here to Download Plugin and install the plugin as instructed.

Dahua Technology USA

23 Hubble
Irvine, CA 92618

Tel: (949) 679-7777
Fax: (949) 679-5760

Support: 877-606-1590

Sales: sales.usa@dahuatech.com

Support: support.usa@dahuatech.com