# IPC-C26E
# WiFi Active Alarm Camera

## Quick Installation Guide

**V1.0.4**

Dahua Technology Co., Ltd

# 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. | January 2019 |
| 2 | V1.0.1 | Revised for North America | July 2019 |
| 3 | V1.0.2 | Updated Feature Content | January 2020 |
| 4 | V1.0.3 | Added SD Card | January 2020 |
| 5 | V1.0.4 | Addedd DMSS Instructions | June 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.

## FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference;
- This device must accept any interference received, including interference that may cause undesired operation.

## FCC compliance：

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Legal Notices

### Copyright

### Trademarks

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

# 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 Overview

The IPC-C26EN WiFi Active Alarm camera is a component of the Dahua WiFi series. The camera offers Passive IR motion detection and is capable of sounding a siren and turning on a spotlight when an intruder is detected. This device is compatible with Dahua NVRs and with the DMSS mobile application. The IPC-C26EN is certified to the IP65 Ingress Protection standard, making it the ideal camera for indoor and outdoor surveillance at homes and small retail or dining establishments.

The key features of this camera are:

**WiFi Capability**

The IPC-C26EN operates on the IEEE802.11b/g/n networks using the 2.4 GHz band. The camera has an internal dual antennae offering reliable performance.

**Active Alarm**

The camera includes a passive infrared (PIR) detector that detects motion without drawing attention to the camera. When motion is detected, the camera can be programmed to sound a siren and turn on an integrated spotlight.

## 1.1 Camera Components
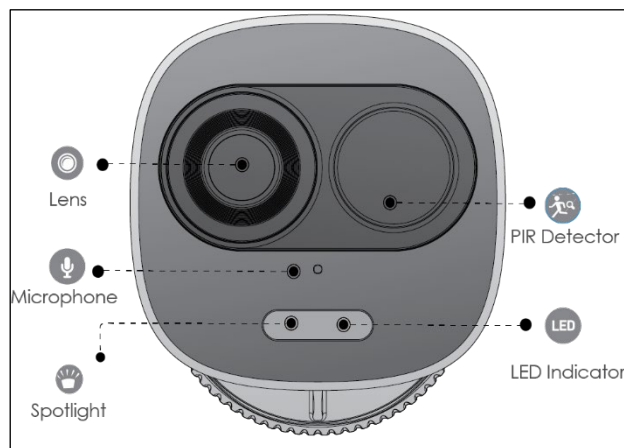
Figure 1-1: IPC-C26E Front Detail
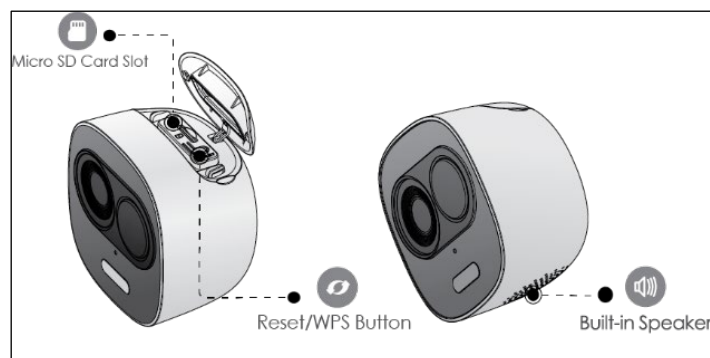
Figure 1-2: IPC-C26E Top and Bottom Detail

Note:
- Use the pry bar included in the packaging to open the top panel to access the Reset/WPS Button and the SD Card slot.
- Press the Reset/WPS button to enable WPS.
- Press the Reset/WPS button for 10 seconds to reset the device to the factory settings.

# 1.2 LED Indicators

| LED Indicator Light | Device Status |
|---|---|
| Off | <ul><li>Powered off.</li><li>Rebooting after reset.</li></ul> |
| Steady Red | Device malfunction. Try resetting the camera (see 'Camera Overview' for details) and repeating the setup. |
| Flashing Red | Network connection failed. Try resetting the camera (see 'Camera Overview' for details) and repeating the setup. |
| Flashing Green | Waiting for network connection. |
| Steady Green | Operating normally. |
| Alternating Flashing Red/Green | Firmware updating. |

# 2 Installing the Camera

The camera ships with all the components to mount the camera to a wall. Before installing the camera consider the following:

- Review the "Installation Tips" section to help you choose an ideal mounting location.
- Decide whether to run the cables through the wall or along the wall.

## 2.1 Installation Tips

To ensure the best possible wireless performance, it is recommended to keep the following installation tips in mind when choosing a location for the camera:

- Place the camera as close to your Wi-Fi router or access point as possible.
- Reduce the number of obstructive materials between the camera and the router or access point. Concrete, brick, metal and wood are the most common materials in your house that can cause poor signal strength.
- The camera uses the 2.4 GHz band exclusively. Most new routers support both 2.4 GHz and 5GHz bands. It is recommended to use other WiFi devices on the 5 GHz band when possible to ensure the 2.4 GHz band is not overcrowded.
- Other electronic devices such as microwaves, TVs, cordless phones, and baby monitors can cause signal interference. It is recommended to install the camera as far away from these devices as possible.
- Point the camera where there is the least amount of obstructions, for example trees and branches.
- Install the camera where vandals cannot easily reach.
- This camera is rated for outdoor use. Installation in a sheltered location is recommended.

## 2.2 Unpacking

This equipment should be unpacked and handled with care. If an item appears to have sustained damage during shipping, notify the shipper immediately.

Verify that all the parts listed below are included. If an item is missing, contact customer support or your local representative.

The original packing carton is the safest container to transport the unit, in the event the unit must be returned for service. Retain the carton and all shipping material for future use.

## 2.3 Parts List
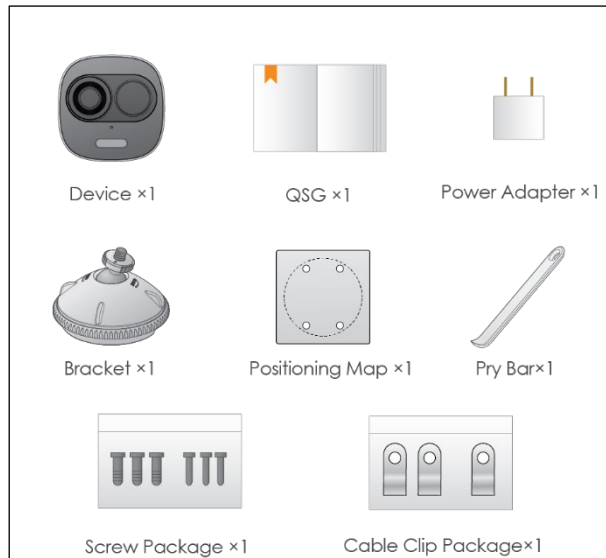


Figure 2-1: IPC-C26E Package Contents

## 2.4 Inserting an SD Card
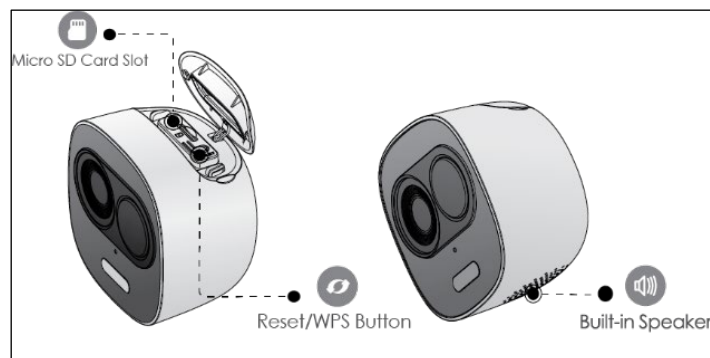


1. Use the pry bar included in the packaging to open the top panel to access the Reset/WPS Button and the SD Card slot.
2. Insert the SD card into the slot and gently push until it clicks into place.
3. Replace the cover and ensure it is secure.
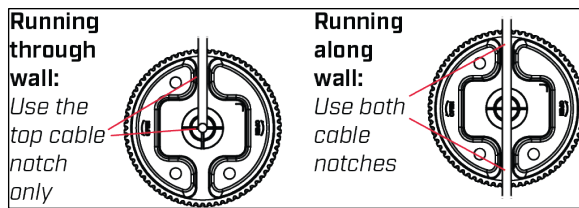
## 2.5 Mounting the Camera to a Wall

1. Attach the wall mount to the back of the camera.
2. Twist the wall mount cover counterclockwise to separate it from the base.
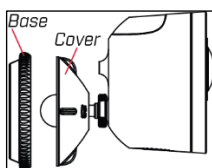


3. Set the base of the wall mount in the desired mounting position with the TOP indicator pointing up.
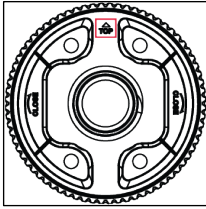
4. Mark holes for screws and cables through the mounting base.
5. Drill holes where marked. If required, insert the included drywall anchors (4×).
6. (OPTIONAL) For a cleaner installation, you may wish to run the camera cable through the cable notches on the back on the wall mount:
   ● If you are running the cable through the wall, feed it through the top cable notch, then through the cable hole you drilled in the mounting surface.
   ● If running the cable along the wall, feed the cable through both cable notches.



7. Secure the wall mount base to the mounting surface using the provided screws (4×).
8. Twist the wall mount cover clockwise onto the base. Adjust the angle of the camera before fully tightening the wall mount cover.
9. (OPTIONAL) If you run the cables along the wall, you may use the included cable guides with the cable guide screws and optional drywall anchors as needed.
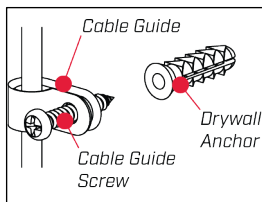


10. Connect the included USB power adapter to the camera cable and connect to a nearby power outlet.

# 3 Connecting to the DMSS App

1. Connect the mobile device to the same 2.4 GHz WiFi network that used for the camera.
2. Install the free DMSS mobile app from the Apple App Store or from the Google Play Store.
3. Tap the DMSS icon to open the app. Tap Enter to setup the app.
   **Note:** Ensure your mobile device is connected to the same 2.4 GHz WiFi network that will be used with for the camera. The camera does not work with 5 GHz WiFi networks.
4. Select the country or area from which you are accessing the app.
5. Tap Skip to continue setup.

## 3.1.1 Adding the Camera

Before adding the camera to DMSS, check the camera's Web interface to obtain the following information:

- Camera IP or Domain Address
- Port

1. Tap the Plus icon on the Home Screen. Then tap IP/ Domain.
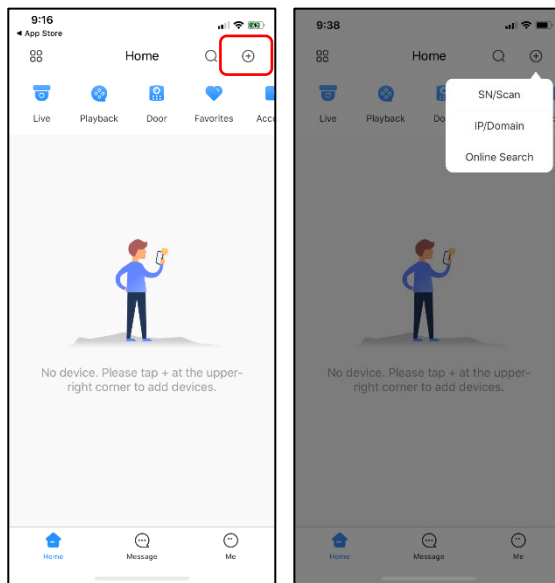


2. Tap Wireless Camera.
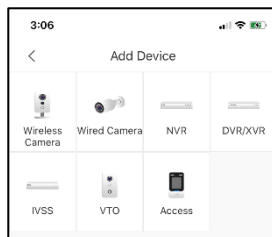


3. Type the following information for the camera: IP Address or the complete Domain Address, Device Name, Username and Password.
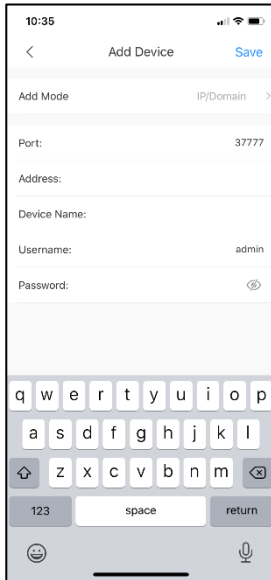
4. Tap Save to save the device information and to display live video from the device.

## 3.1.2 Configuring Alarms

1. Tap the three dots (…) to the right of the camera. Then, Tap Device Details.
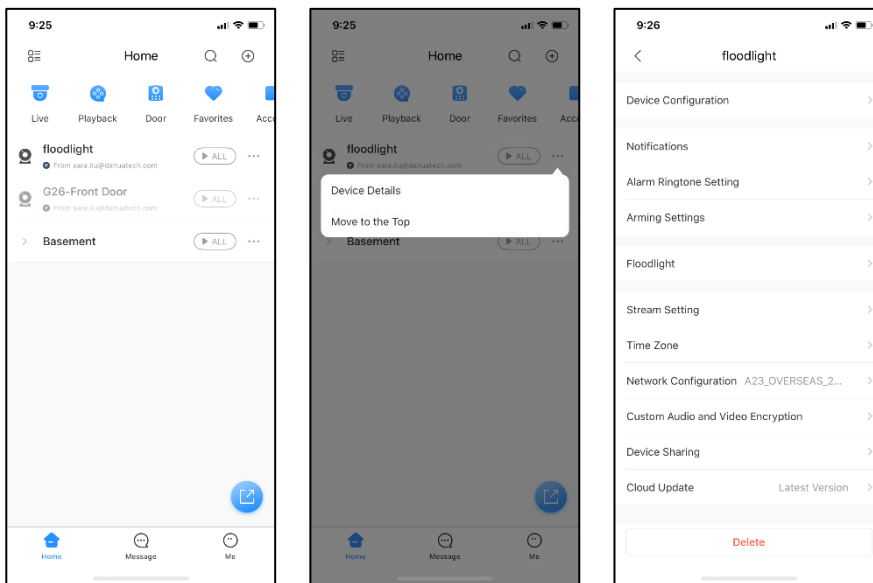


2. Tap Notifications and then tap the Alarm Notification switch to activate.
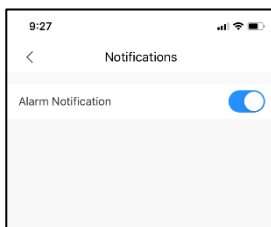


3. Tap the Left Arrow to return to Device Details.
4. Tap Alarm Ringtone Setting to link an alarm trigger with an audible sound.
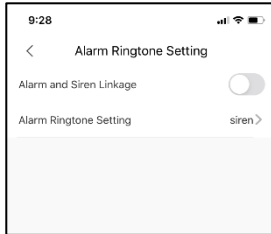
a) Tap the Alarm and Siren Linkage switch to activate.

b) Tap Alarm Ringtone Setting to set the sound for the siren.

c) Tap the Left arrow twice to return to Device Settings.

5. Tap Arming Settings.
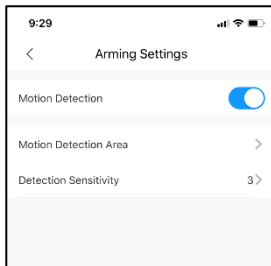


a) Tap the Motion Detection switch to activate motion detection on the camera.

b) Tap Motion Detection Area. The app displays the live scene overlaid by a grid. By default, the app enables motion detection for the entire scene.
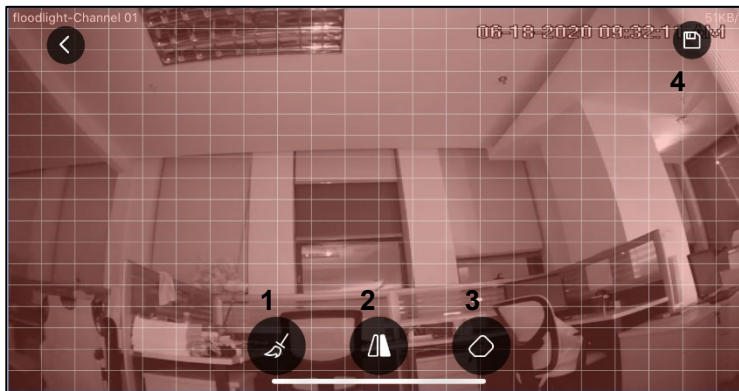


c) To define discrete areas of the scene for motion detection, tap the Default (2) button to clear the grid.

d) Drag your finger through the grid to define the separate areas.

e) To clear the defined areas, tap the Erase (1) button.

f) To save the defined areas, tap the Save (4) button, then tap OK to accept the motion detection areas.

g) Tap the Left arrow to return to Arming Settings.

h) Tap Detection Sensitivity to set the motion detection sensitivity. Tap a button for the desired sensitivity (1 through 5), then tap Save.
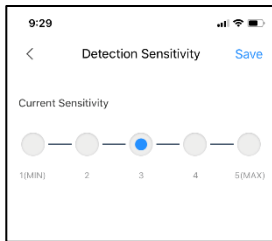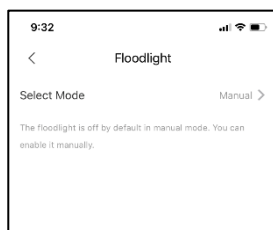


i) Tap the Left Arrow twice to return to the Home screen.

# 3.1.3 Configuring the External Light

1. Tap the three dots (…) to the right of the camera. Then, Tap Device Details.
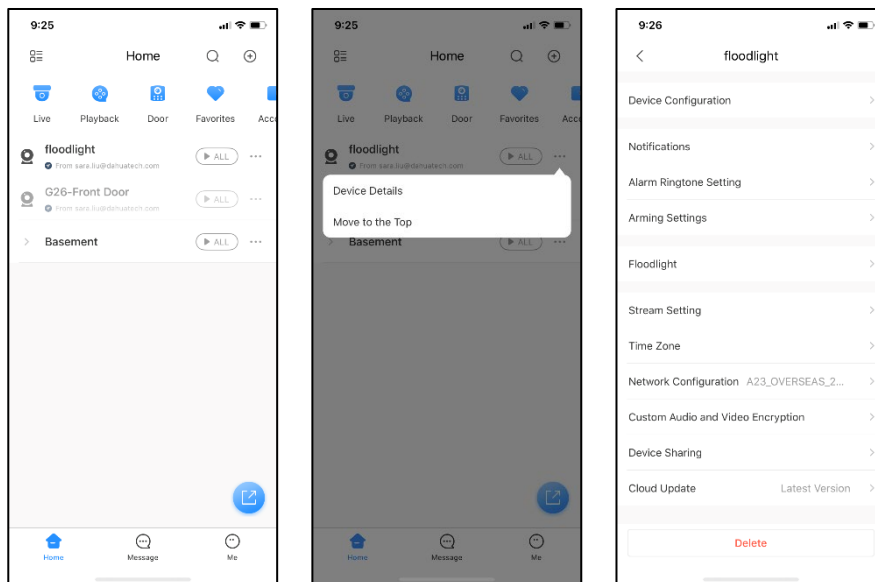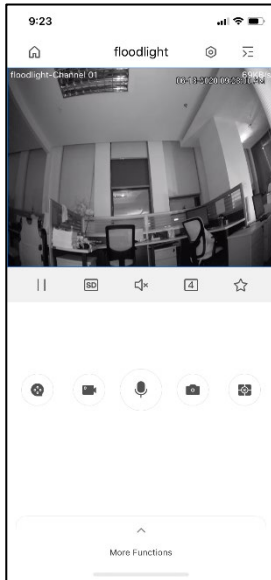


2. Tap Light, and then tap Select Mode.



3. Select one of the light settings:
   - Manual: user must turn on the floodlight.
   - Automatic: the camera determines when to turn on the floodlight.

# 3.1.4 Turning on the Light or Siren

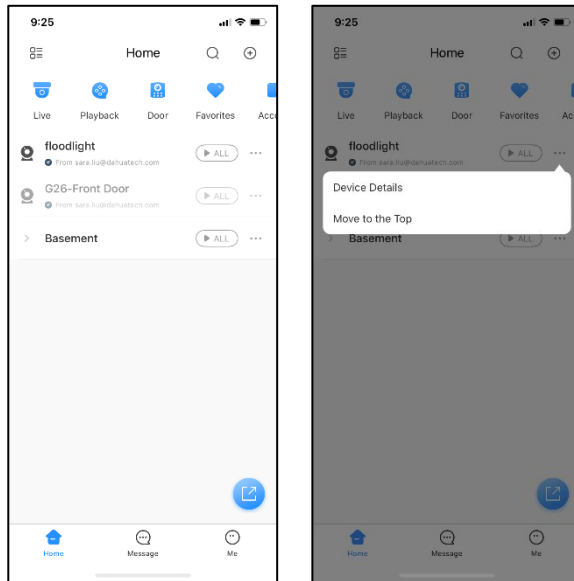1. Tap More Functions, located at the bottom of the Live View screen.

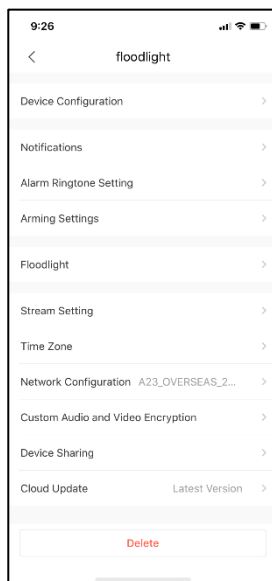2. Tap the Bell icon to activate the siren and tap the Light icon to activate the floodlight.



3. Tap the icon again to stop the siren or to turn off the floodlight.
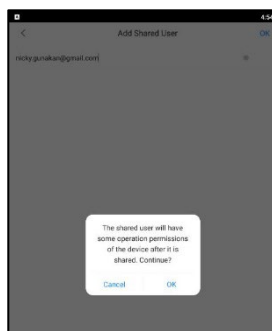
# 3.1.5 Sharing the Camera

1. Tap Home.
2. Tap the three dots (…) to the right of the camera to share. Then, Tap Device Details.



3. Tap Device Sharing.



4. Tap the Plus icon.
5. Type the target DMSS account and click OK.

# **4** Troubleshooting

| Issue | Solution |
|---|---|
| Cannot setup camera | ● Ensure you are using a 2.4GHz Wi-Fi network to configure the camera. The camera does not work with 5GHz networks.<br>● Ensure your mobile device is within 1 ft (30 cm) of the camera during setup. |
| No Picture/Signal | ● Ensure the LED indicator on the camera is glowing steady green. See 'LED Behavior' section for details if otherwise.<br>● Ensure the camera is properly connected to power using the included USB power adapter.<br>● Try repositioning the camera, router, or both to improve signal strength. |
| Picture is not clear | ● Check the camera lens for dirt, dust, spiderwebs. Clean the lens with a soft, clean cloth.<br>● Remove the vinyl cover on the camera lens. |
| No audio | ● Ensure audio function on camera is turned on.<br>● Ensure audio is turned up on viewing device. |
| The warning light is not switching on automatically | ● Ensure that you have enabled and configured white light deterrence. |
| The siren is not switching on automatically | ● The camera siren cannot switch on automatically. You can control the camera siren manually using the Dahua DMSS app. |

**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