

## About this Manua

Please use this user manual under the guidance of professionals

For products that support Wi-Fi or cellular data:  
(Marked with a "W", "GLT", "GLE", "GLF", "GE", "GT" or "GW" in the Part C of a product model.  
Product Model Example: Part A-Part B-Part C. Part C is optional.)

## FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**FCC compliance:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

## FCC Conditions

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

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

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

For products that do not support Wi-Fi or cellular data:

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**FCC Compliance:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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.

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

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

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The device should be used in compliance with local laws, electrical safety regulations, and fire prevention regulations.

Keep the device in original or similar packaging while transporting it.

The input voltage should conform to IEC60950-1 standard: SELV (Safety Extra Low Voltage) and the Limited Power Source. Refer to the appropriate documentation for detailed information.

DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.

Make sure the plug is properly connected to the power socket.

The installer and user are responsible for password and security configuration and its settings.

Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the local codes.

If the product does not work properly, please contact your dealer or the nearest service center. We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.

A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.

Please use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.

When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.

Do not expose the device to high electromagnetic radiation or dusty environments.

For indoor-only device, place it in a dry and well-ventilated environment.  
Do not aim the lens at the sun or any other bright light.  
Make sure the running environment meets the requirement of the device. The operating temperature shall be -10 °C to 40 °C (-14 °F to 104 °F), and the operating humidity shall be 90% or less (no condensing).

If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

Set up camera time manually for the first time access if the local time is not synchronized with that of the network. Visit the camera via Web browser/client software and go to time settings interface.

Make sure the device is firmly secured to any wall or ceiling mountings.  
Be sure that there is enough space to install the camera and accessories.  
Make sure that the device in the package is in good condition and all the assembly parts are included.





Make sure that the wall is strong enough to withstand at least 4 times the weight of the camera and the mount.

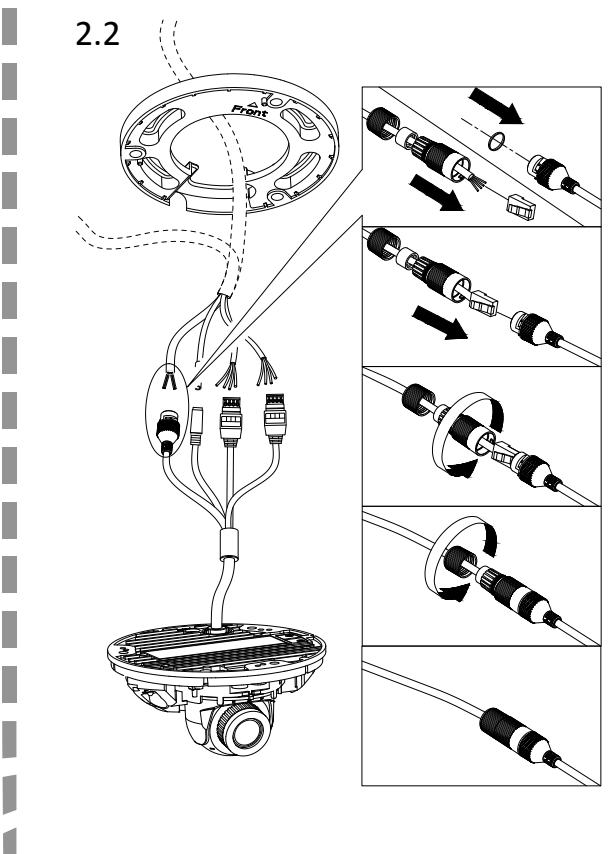
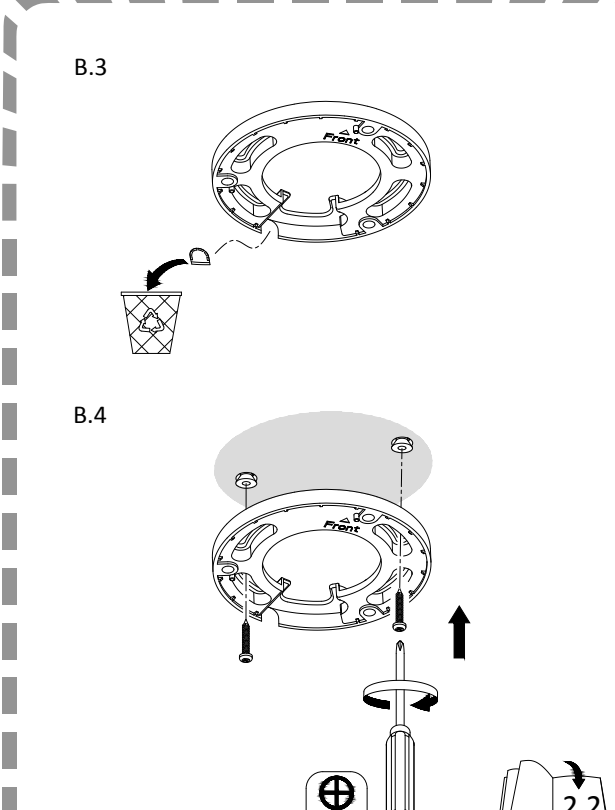
The standard power supply is 85 VAC to 245 VAC, or PoE (802.3at), please make sure your power supply matches with your camera.

Make sure that the power has been disconnected before you wire, install, or disassemble the device.

Make sure that no reflective surface is too close to the camera lens. The IR light from the camera may reflect back into the lens causing reflection.

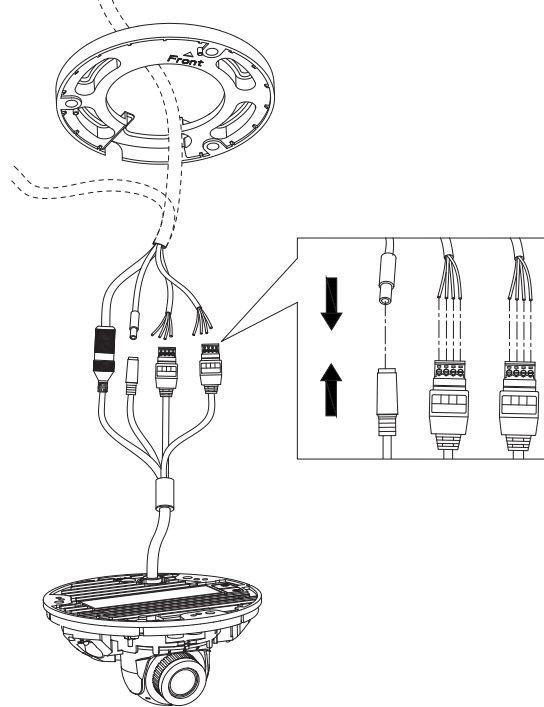
 **Notice**

-  Purchase separately
-  Not necessarily included accessory/  
Skip this step if not required.
-  Attention
-  Disposal

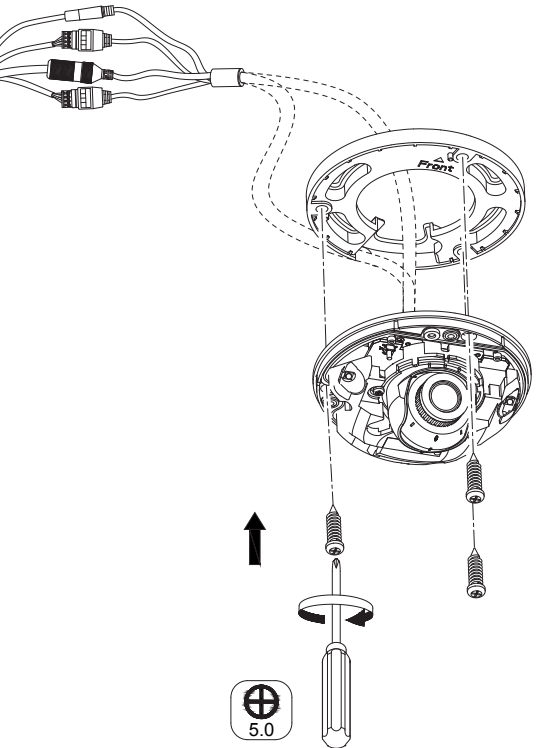




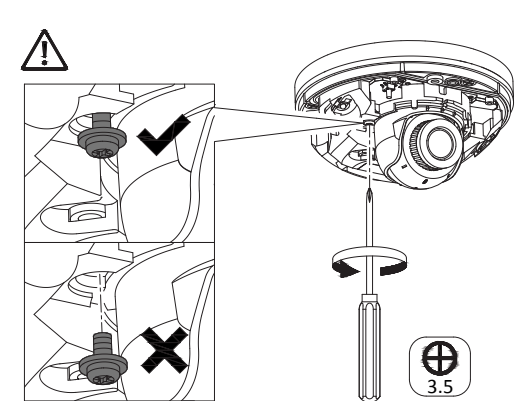
2.3



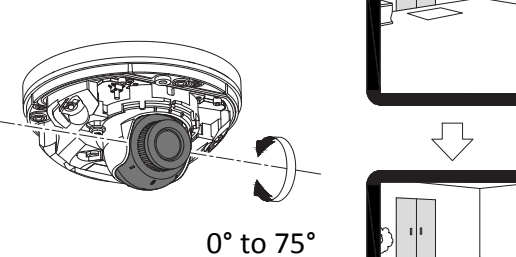
2.4



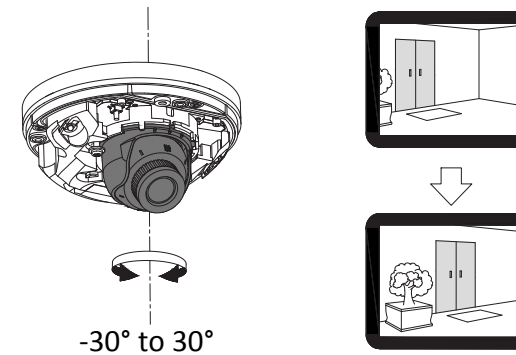
3.1



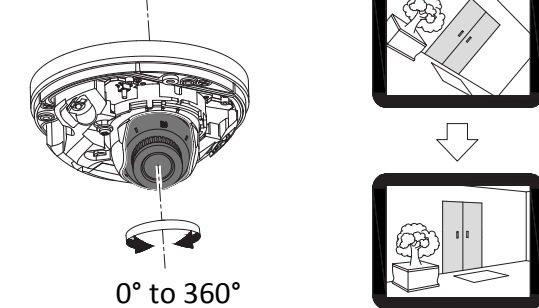
3.2



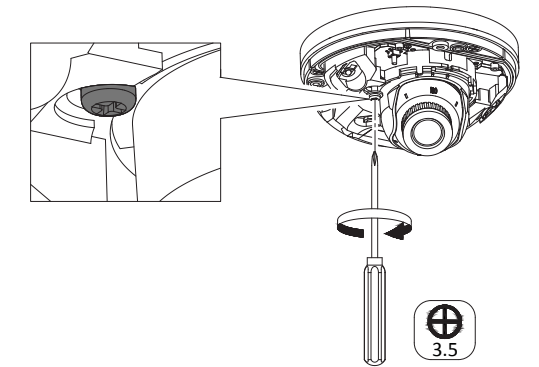
3.3



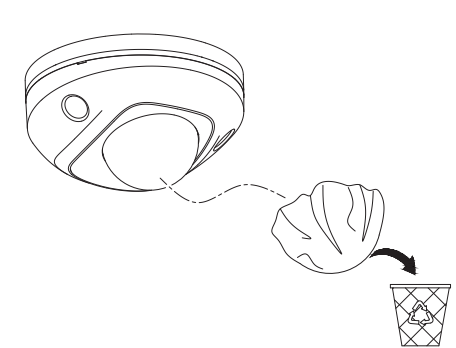
3.4



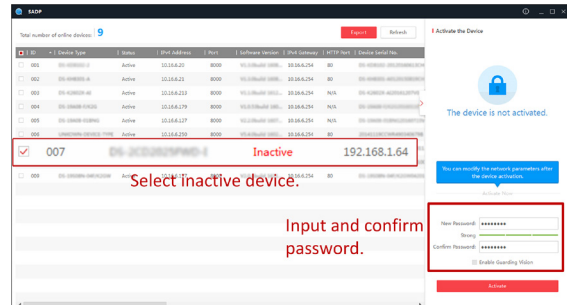
3.5



4.3



4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the camera.

- 1) Select the device.
- 2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

## 2 Visit Camera

This part introduces how to visit the camera via Web browser or client softwares.

### 2.1 Visit Camera via Web Browser

#### Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements.

Table 2-1 System Requirement

Operating System	Microsoft Windows XP and above version, Mac OS X 10.8 and above version
CPU	3.0 GHz or higher
RAM	1 GB or higher
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 8.0 and above version, Mozilla Firefox 30.0-51, Google Chrome 31.0-44, Safari 8.0+

#### Steps

1. Open the web browser.
2. Input IP address of the camera to enter the login interface.
3. Input user name and password.



**Note**

Illegal login lock is activated by default. If admin user performs 7 failed password attempts (5 attempts for user/operator), the IP address is blocked for 30 minutes.

If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.

4. Click **Login**.

5. Download and install appropriate plug-in for your web browser.

For IE based web browser, webcomponents and <sup>TM</sup> are optional. For non-IE based web browser, webcomponents, <sup>TM</sup>, VLC and MJPEG are optional.

### 2.2 Visit Camera via Guarding Expert

Add the camera to client software before further operation.

Refer to the *Guarding Expert Client Software User Manual* for detailed setting steps.

## 3 Operating via Mobile Client

Guarding Vision is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.



**Note**

Guarding Vision service should be supported by the camera.

### 3.1 Enable Guarding Vision Service on Camera

Guarding Vision service should be enabled on your camera before using the service.

You can enable the service through SADP software or web browser.

#### 3.1.1 Enable Guarding Vision Service via Web Browser

Follow the following steps to enable Guarding Vision Service via Web Browser.

#### Before You Start

You need to activate the camera before enabling the service.

#### Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Advanced Settings → Platform Access**
3. Select Platform Access Mode as Guarding Vision.
4. Check the checkbox of Enable.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.



**Note**

The verification code is required when you add the camera to Guarding Vision app.

7. Save the settings.

#### 3.1.2 Enable Guarding Vision Service via SADP Software

This part intruduce how to enable Guarding Vision service via SADP software of an activated camera.

#### Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check the checkbox of Enable Guarding Vision
4. Create a verification code or change the old verification code.



**Note**

The verification code is required when you add the camera to Guarding Vision app.

5. Click and read "Terms of Service" and "Privacy Policy".

6. Confirm the settings.

### 3.2 Set up Guarding Vision

#### Steps

1. Download and install the Guarding Vision app by searching "Guarding Vision" in App Store or <sup>TM</sup>.
2. Launch the app and register for a Guarding Vision user account.
3. Log in after registration.

### 3.3 Add Camera to Guarding Vision


#### Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Guarding Vision app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on the bottom of the camera or on the *Quick Start Guide* cover.



**Note**

If the QR code is missing or too blur to be recognized, you can

also add the camera by tapping the  and inputting the camera's serial number.

5. Input the verification code of your camera.



**Note**

- The required verification code is the code you create or change when you enabling Guarding Vision service on camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.

7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

**Wireless Connection**

Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)

**Wired Connection**

Connect the camera to the router with a network cable and tap **Connected** in the result interface.



**Note**

The router should be the same one that your mobile phone has connected to.

8. Tap **Add** button in the next interface to finish adding.

For detailed information, refer to the user manual of the Guarding Vision app.

### 3.4 Initialize the Memory Card

Memory card required initialization before saving recordings of the camera.

#### Steps

1. Check the memory card status by tapping on the **Storage Status** in the device settings interface.
2. If the memory card status displays as **Uninitialized**, tap to initialize it.  
The status change to **Normal** after successful initialization.

#### Result

You can then start recording any event triggered video in the camera such as motion detection.