Intelligent Entrance ANPR Camera

User Manual

Legal Information

About this Document

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

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

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

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

Contents

Chapter 1 Introduction

1.1 Introduction

Intelligent Entrance ANPR Camera (hereinafter referred to as device) integrates multiple functions including video collection, smart video compression, network transmission, etc. It can be used with other devices (vehicle detector or barrier gate) to realize vehicle management and control, light supplement, capture, etc.

It can be widely applied in normal entrance and exit, toll station, and entrance and exit of underground parking lot.

1.2 Key Feature

- Adopts advanced video compression with high compression ratio and flexible operation.
- Captures pictures of the passing vehicles in entrance and exit via video detection, IO coil trigger, RS-485 trigger, etc.
- Capture and recognition via vehicle direction and license plate type.
- Remote control of barrier gate, including opening, closing, locking, and unlocking barrier gate.
- Supplement light control according to brightness condition or time schedule.

Note

The functions vary with different models. The actual product prevails.

Chapter 2 Activation and Login

2.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via SADP software, web browser, and iVMS-4200 Client.

Note

Refer to the user manual of iVMS-4200 Client for the activation via client software.

2.1.1 Default Information

Device default information are as follows.

- Default IP address: 192.168.1.64
- Default port: 8000
- Default user name: admin

2.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the devices over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (***https://www.hikvision.com/***), and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Enter a new password (admin password) and confirm the password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And

we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

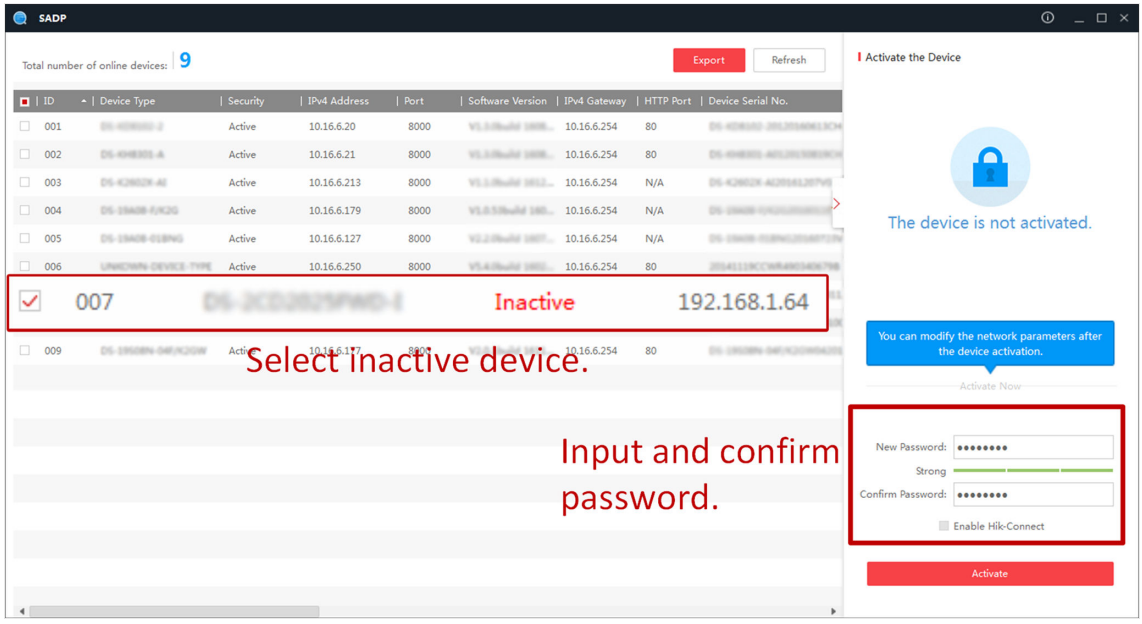

Figure 2-1 Activate via SADP

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

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Enter the admin password and click **Modify** to activate your IP address modification.

2.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer connect to the same LAN.

Steps

1. Change the IP address of your computer to the same network segment as the device.
2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
3. Create and confirm the admin password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

2.2 Login

You can log in to the device via web browser for further operations such as live view and local configuration.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
2. **Optional:** Select the other languages from the drop-down list on the upper right corner of the interface to switch the language.
3. Enter **User Name** and **Password**.
4. Click **Login**.
5. Click **Plugin Download** on the upper right corner of the interface to download and install the plugin for your web browser. Follow the installation prompts to install the plugin.
6. Reopen the web browser after the installation of the plugin and repeat steps 1 to 3 to log in.
7. **Optional:** Click **Logout** on the upper right corner of the interface to log out of the device.

Chapter 3 Capture Configuration

3.1 Quick Configuration

3.1.1 Set Basic Parameters

When the I/O coils have been laid and the device has been connected to trigger capture in the site, you can set the basic parameters in quick configuration to realize capture quickly.

Before You Start
The device position has been adjusted.

Steps
1. Go to **Quick Configuration → Basic Configuration** .

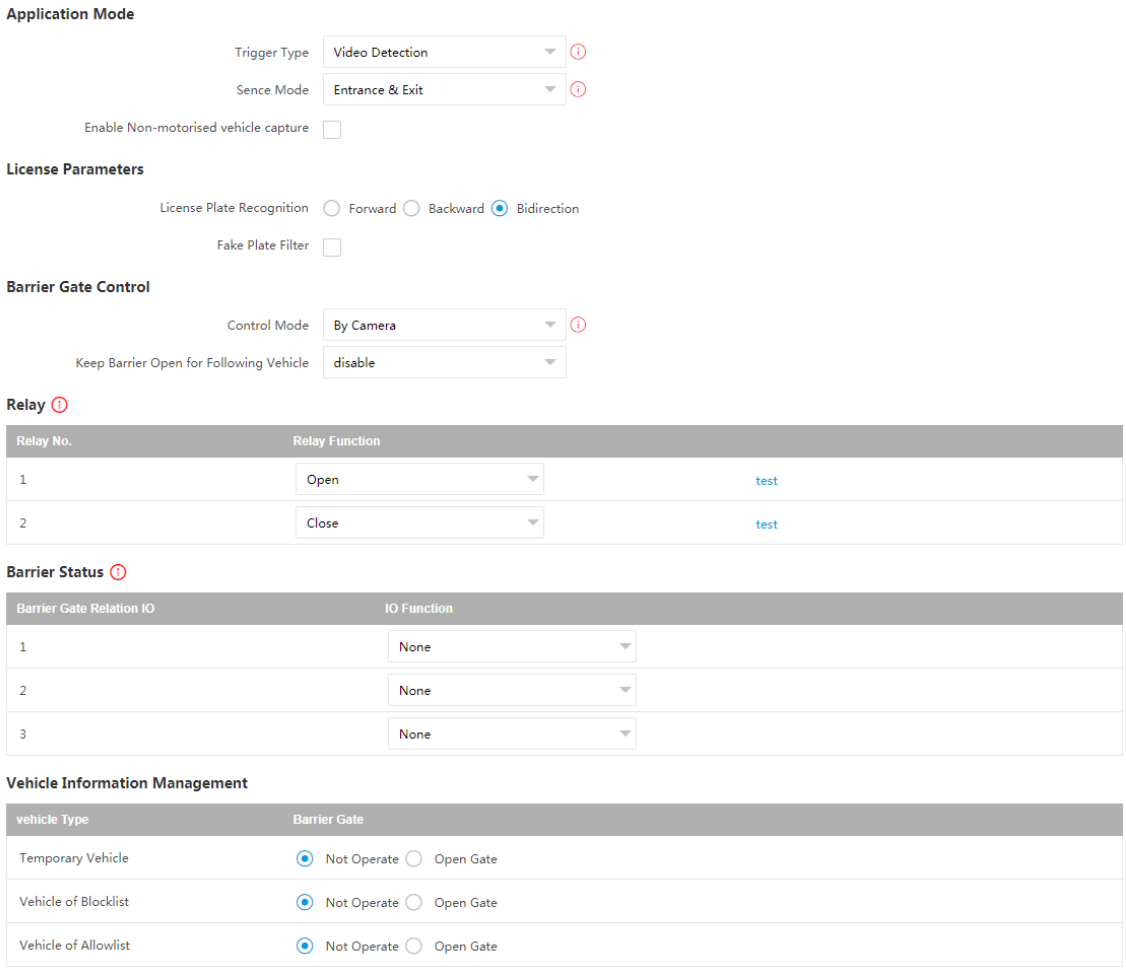

Figure 3-1 Set Basic Parameters

2. Set **Application Mode** parameters.

1) Select **Trigger Type**.

Video Detection

Select it to trigger capture by video stream detection.

I/O Coil

Select it to trigger capture by external device such as the vehicle detector and radar.

Radar Mixed Traffic

Select it to detect the driving direction in mixed traffic scene with two radars.

Note

If you select this type, one **Forward Radar** and one **Backward Radar** should be set.

2) Set the following parameters as required.

Scene Mode

Select a scene mode as required. Select **Toll Gate** when there are many large-sized vehicles and vehicle heads are not captured completely. Select **Underground Parking Entrance & Exit** in low light environment. Select **Entrance & Exit** in other scenes.

Enable Non-motorised Vehicle Capture

Check to identify and capture non-motor vehicles in the scene.

I/O Trigger Defaults Status

Capture is triggered according to the level signal status. If you select **Falling Edge**, the device will trigger capture at the moment that the high level falls to low level. If you select **Rising Edge**, the device will trigger capture at the moment that the low level rises to high level.

Linked I/O No.

The I/O No. linked under I/O coil mode. When the coil detects that there is a vehicle passing, a rising or falling edge signal is sent to the linked I/O of the device to trigger capture.

Forward/Backward Radar

Radar Mixed Traffic shall be used with one forward radar and one backward radar. Select the corresponding I/O No.

3. Set **License Parameters**.

License Plate Recognition

- Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
- Select **Backward** when license plates of vehicles from the leaving direction need to be recognized.
- Select **Bidirection** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.

Fake Plate Filter

After you enable this function, if it is identified as a fake license plate, the device will not output the captured picture and license plate information, and the barrier gate will not be opened.

4. Set **Barrier Gate Control** parameters.

Control Mode

- Select **By Camera** in single camera scene (no control software) and allowlist scene in which the camera controls the barrier gate in advance according to the set passing rules in **Vehicle Information Management**.
- Select **By Platform** in the scene in which the entry permissions are controlled by the software.
- Select **By Mixed**, and the platform control and camera control are effective simultaneously. It is applicable to the scene in which different vehicle passing permissions are managed by software and camera. E.g., the software controls the passing of blocklist vehicles and temporary vehicles, and the camera controls the passing of allowlist vehicles and controls the barrier gate in advance for allowlist vehicles.

Keep Barrier Open for Following Vehicle

After you enable this function, the barrier gate keeps open when the device detects following vehicles are passing. The barrier gate will close after the following vehicles pass.

5. Select **Relay Function** as needed.

Note

The supported number of relays varies with different models. Relay 1 corresponds to the 1A and 1B of the terminal. Relay 2 corresponds to the 2A and 2B of the terminal.

6. Select **IO Function** for the corresponding barrier gate related I/O. The device will upload barrier gate status information for convenient exit and entrance management.

Note

- If the device only have one I/O interface, and the trigger type is **I/O Coil**, the barrier status cannot be configured.
- If the trigger type is **Radar Mixed Traffic** and the forward radar and backward radar are selected, the corresponding barrier gate related I/O function cannot be configured. E.g., the forward radar is IO1 and the backward radar is IO2. Then the barrier gate related IO1 and IO2 functions cannot be configured.

7. **Optional:** Select the barrier gate operations for temporary vehicles, vehicles of blocklist, and vehicles of allowlist in **Vehicle Information Management**.

What to do next

Click **Next** to set image adjustment parameters.

3.1.2 Adjust Image

You can adjust the positions of the lane line, lane right limit, and trigger line, and adjust the lens if the lens is vari-focal lens.

Steps

1. Go to **Quick Configuration → Image Adjustment** .

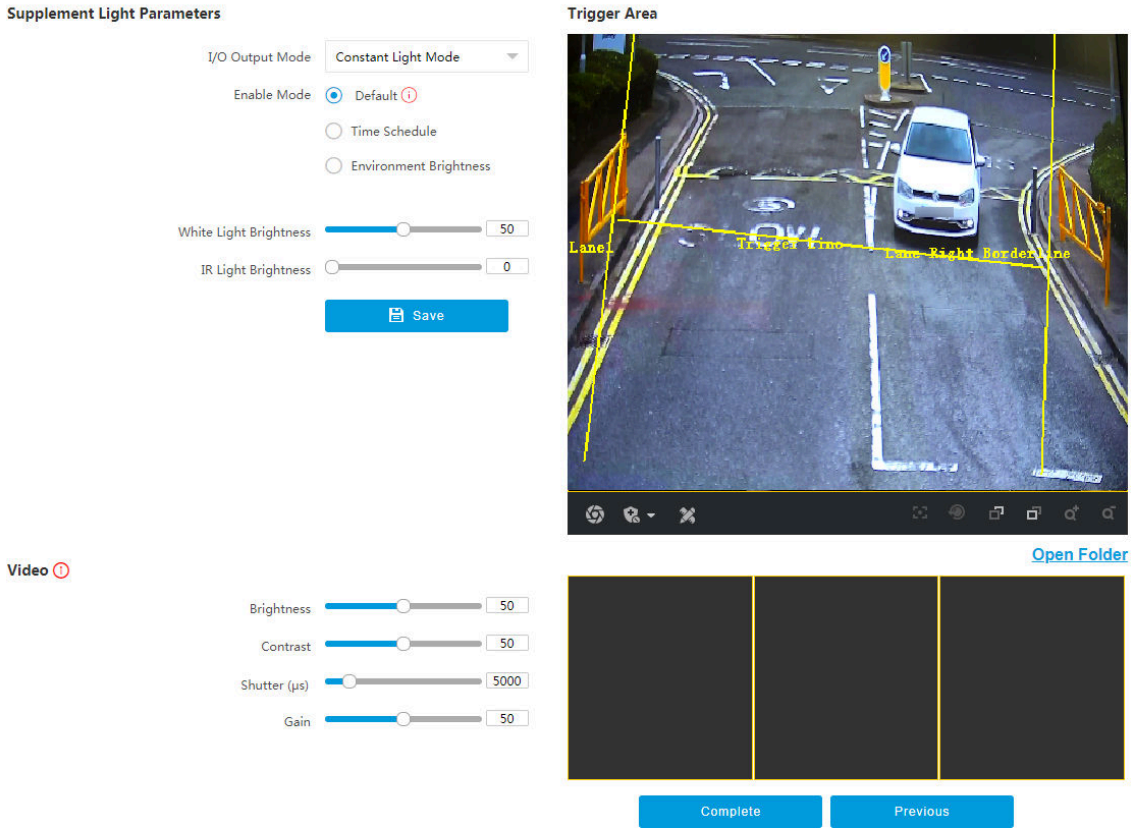

Figure 3-2 Adjust Image

2. Set **Supplement Light Parameters**.

I/O Output Mode

Constant Light Mode: The supplement light is constantly on to supplement light for the scene.

Enable Mode

Default

The default status of the supplement light depends on the device models.

Time Schedule

Select it when you want the constant light to be enabled during fixed time period. Set the start time and end time.

Environment Brightness

Select it when you want the constant light to be controlled by detecting the surroundings brightness automatically. Set the brightness threshold. The higher the threshold is, the harder the constant light can be enabled.

White Light Brightness/IR Light Brightness

Drag the slider to adjust the brightness, or enter the value in the text field. The higher the brightness is, the more the light will be supplemented.

Note

The actual functions may vary with different models. The actual device prevails.

3. Set **Video** parameters.

Note

You can adjust the video parameters according to the prompt on the interface.

Brightness

Adjust the average brightness and the reference value of the image. When the image is overexposed, the brightness will be reduced. When the image is too dark, the brightness will be enhanced.

Contrast

In the case of underexposure or overexposure, the brightness of the image may be limited to a small range, and you will see a blurred image. Contrast adjusts the level and permeability of the image. The screen blinding can be appropriately raised, and the dark place can be appropriately lowered.

Shutter

Shutter refers to a single frame exposure time, in microseconds. If you need to increase the light intensity, you can increase the shutter value; if you need to reduce the light intensity coming in, lower the shutter value.

Gain

It is used to limit the upper limit of image signal amplification. It is recommended to increase the scene of insufficient illumination. Increasing the signal gain can improve the brightness of the picture, and the noise will also be amplified by the gain. You are recommended to reduce the scenario with a strong point light source to prevent overexposure of the point light source.

4. Adjust lines on the live view image.
   1) Select the lane line, right border line, or trigger line.
   2) Drag the endpoints to adjust the position and length of the line, or drag the line to adjust its position.

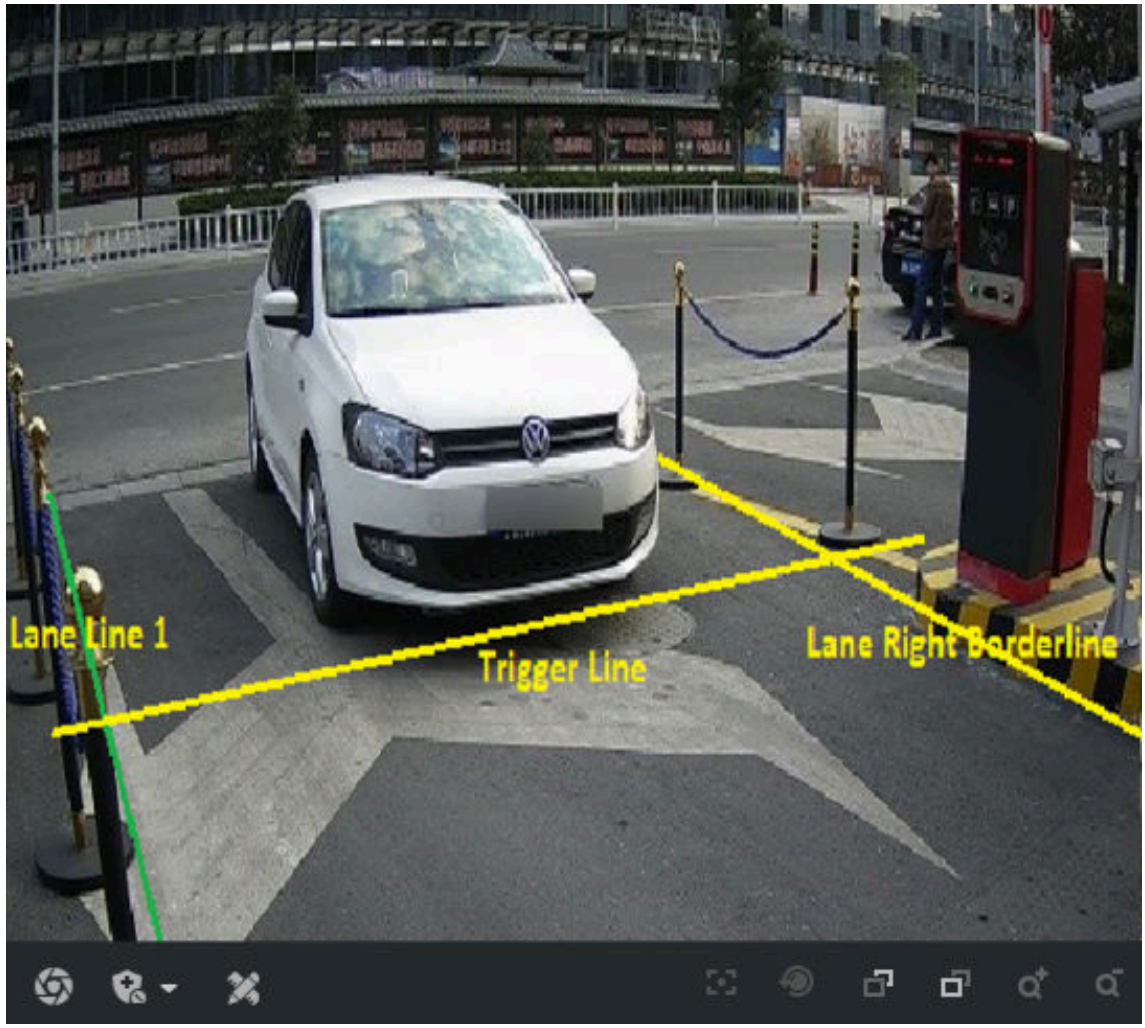

Figure 3-3 Adjust Lines

5. **Optional:** You can click the icons under the live view image to do corresponding operations.

Table 3-1 Image Adjustment Icon Description

Icon	Description
	Click it to capture a picture.
	• **Level 1 Arming** can only connect one client or web. The uploaded pictures will not be stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming. • **Level 2 Arming** can connect three clients or webs. The pictures will be uploaded to the client/web, and stored in the storage card. • **Disarming** is to cancel the alarm status or real-time picture.

Icon	Description
	Click it to measure the license plate pixel. Click it again to disable the measurement.
	Click it to realize one-touch focus. Click it again to restore to the initial status.
	Click it to realize lens initialization.
	Focus +. Hold it to view distant objects clearly, while nearby objects will be blurred.
	Focus -. Hold it to view nearby objects clearly, while distant objects will be blurred.
	Zoom +. Hold it to zoom in the image.
	Zoom -. Hold it to zoom out the image.
Open Folder	Click it to open the saving path of captured pictures.

6. Click **Complete** to finish the quick configuration.

3.2 Detailed Configuration

3.2.1 Set Application Mode

If you want to trigger capture of the passing vehicle information at the entrance or exit, set the application mode.

Before You Start

The device has been installed at the specific location, and the lens has been debugged.

Steps

1. Go to **Configuration → Capture → Application Mode** .

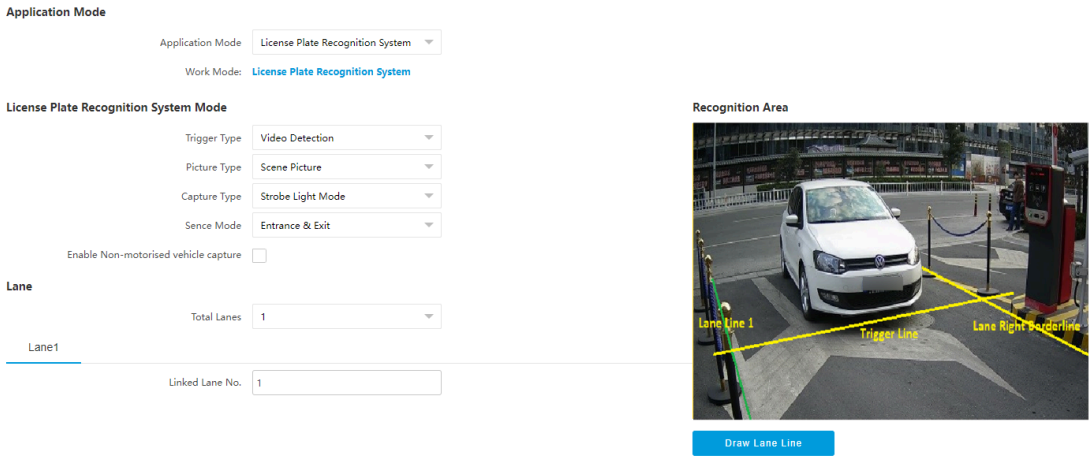

Figure 3-4 Set Application Mode

2. Select **Trigger Type**.

   Video Detection

   Select it to trigger capture by video stream detection.

   I/O Coil

   Select it to trigger capture by external device such as the vehicle detector and radar.

   Radar Mixed Traffic

   Select it to detect the driving direction in mixed traffic scene with two radars.

   Note

   If you select this type, one **Forward Radar** and one **Backward Radar** should be set.

3. Select **Picture Type**.

   Scene Picture

   One scene picture and one license plate picture will be captured.

   Scene Picture + Close-up Picture

   One scene picture, one license plate picture, and one close-up picture will be captured.

4. Set the following parameters as required.

   Scene Mode

   Select a scene mode as required. Select **Toll Gate** when there are many large-sized vehicles and vehicle heads are not captured completely. Select **Underground Parking Entrance & Exit** in low light environment. Select **Entrance & Exit** in other scenes.

   Enable Non-motorised Vehicle Capture

   Check to identify and capture non-motor vehicles in the scene.

   I/O Trigger Defaults Status

Capture is triggered according to the level signal status. If you select **Falling Edge**, the device will trigger capture at the moment that the high level falls to low level. If you select **Rising Edge**, the device will trigger capture at the moment that the low level rises to high level.

Linked I/O No.

The I/O No. linked under I/O coil mode. When the coil detects that there is a vehicle passing, a rising or falling edge signal is sent to the linked I/O of the device to trigger capture.

Forward/Backward Radar

Radar Mixed Traffic shall be used with one forward radar and one backward radar. Select the corresponding I/O No.

5. Click **Draw Lane Line** to draw the lines.
   1) Select the lane line, right border line, or trigger line.
   2) Drag the endpoints to adjust the position and length of the line, or drag the line to adjust its position.
   3) Click **OK** to save the settings.

Note

It is recommended to draw the trigger line at the position which is 1/3 to 1/4 of the lane line. The license plate number height pixel should be between 25 to 35 pixels at the capture position.

6. Click **Save**.

3.2.2 Set Capture Parameters

Set License Plate Recognition Parameters

When there are vehicles of different types passing from different directions, set the license plate recognition parameters.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → License Parameters** .

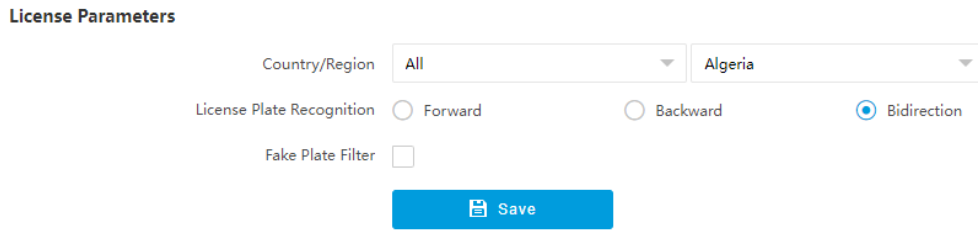

Figure 3-5 Set License Plate Recognition Parameters

2. Set **Country/Region** according to the actual needs.
3. Set the following parameters.

   License Plate Recognition

   - Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
   - Select **Backward** when license plates of vehicles from the leaving direction need to be recognized.
   - Select **Bidirection** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.

   Fake Plate Filter

   After you enable this function, if it is identified as a fake license plate, the device will not output the captured picture and license plate information, and the barrier gate will not be opened.
4. Click **Save**.

Set Supplement Light Parameters

Supplement light can enhance the image stabilization and adjust the brightness and color temperature. It can supplement light at night or when the light is dim.

Steps

Note

Only when the constant light is connected, can the set parameters take effect.

1. Go to **Configuration → Capture → Capture Parameters → Supplement Light Parameters** .

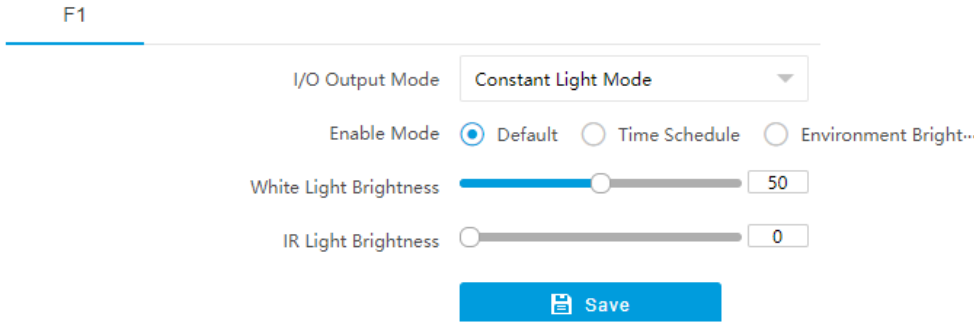

Figure 3-6 Set Supplement Light Parameters

2. Select **I/O Output Mode** as **Constant Light Mode**.
3. Set the supplement light parameters according to actual conditions.

   Enable Mode

   Default

   The default status of the supplement light depends on the device models.

   Time Schedule

   Select it when you want the constant light to be enabled during fixed time period. Set the start time and end time.

   Environment Brightness

   Select it when you want the constant light to be controlled by detecting the surroundings brightness automatically. Set the brightness threshold. The higher the threshold is, the harder the constant light can be enabled.

   White Light Brightness/IR Light Brightness

   Drag the slider to adjust the brightness, or enter the value in the text field. The higher the brightness is, the more the light will be supplemented.

   Note

   The actual functions may vary with different models. The actual device prevails.

4. Click **Save**.

Set Vehicle Feature Parameters

Set vehicle feature parameters when you need to capture the passing vehicle according to the vehicle features.

Steps

Note

Some models do not support vehicle features recognition. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Vehicle Feature** .
2. Check the vehicle features to be recognized.
3. Click **Save**.

Set Image Encoding Parameters

If the captured pictures are not clear, set the resolution of the captured pictures and the picture size.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Image Encoding and Composition** .

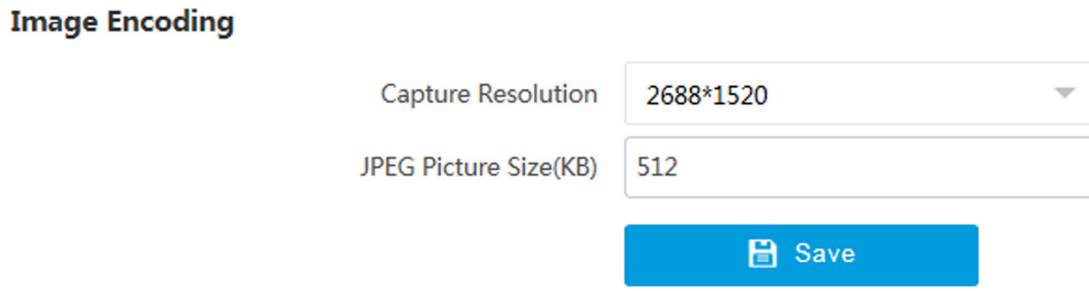

Figure 3-7 Set Image Encoding Parameters

2. Select **Capture Resolution**.
3. Enter **JPEG Picture Size**.
4. Click **Save**.

Set Capture Overlay

If you want to overlay information on the captured pictures, set capture overlay.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Text Overlay** .
2. Check **Capture Picture Overlay**.

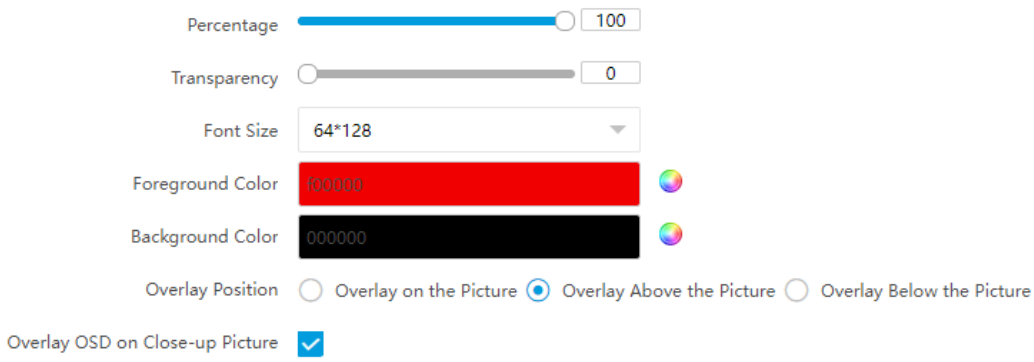

Figure 3-8 Set Capture Overlay

3. Set the percentage, front size, color, overlay position, etc.

   Percentage

   It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

   Overlay OSD on Close-up Picture

   Check it to overlay the OSD information on the close-up pictures.

4. Select the overlay information from the list.

   Note

   The overlay information varies with different models. The actual device prevails.

5. Set the overlay information.

Type	You can edit the type.
Overlay Information	For some information types, you can edit the detailed information.
Overlay Position	Check it, and the current information will be displayed from a new line.
Space	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
Line Break Characters	Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
/	Adjust the display sequence of the overlay information.

6. Click **Save**.

3.3 View Real-Time Picture

You can view the real-time captured pictures and license plate information.

Steps

Note

The supported functions vary with different models. The actual device prevails.

1. Go to **Live View → Real-Time Capture** .
2. Click **Arming**.
3. Select an item from the list, and you can view the capture scene picture and recognized license plate information.

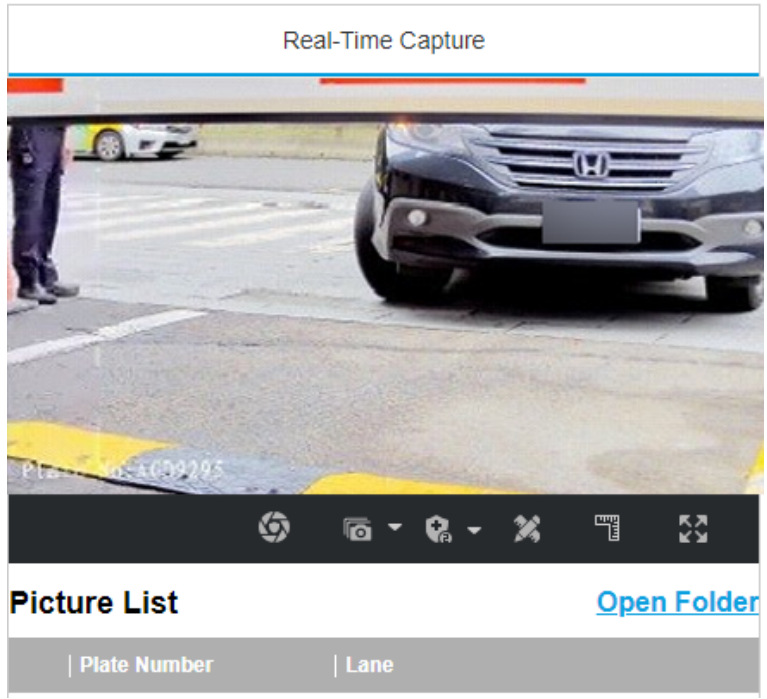

Figure 3-9 Real-Time Picture

4. **Optional:** You can also do the following operations.

/ /	• **Level 1 Arming** can only connect one client or web. The uploaded pictures will not be stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming. • **Level 2 Arming** can connect three clients or webs. The pictures will be uploaded to the client/web, and stored in the storage card. • **Disarming** is to cancel the alarm status or real-time picture.
	Click it to measure the license plate pixel. Click it again to disable the measurement.
	Click it to enable the ruler to measure the license plate.
	Click it to enable manual capture.

	Click it to set continuous capture parameters and the device will capture pictures according to the set interval. • **Capture Times**: Up to five pictures can be captured per continuous capture. • **Interval**: Up to four intervals can be set, and the default interval is 100 ms.
	Display the images in full screen mode.
Open Folder	Open the saving path of captured pictures.

Chapter 4 Peripheral Device Linkage

4.1 Set Barrier Gate Linkage

If a barrier gate has been connected to the device, you can link barrier gate to realize the control and management of the vehicles at the entrance or exit.

4.1.1 Set Allowlist and Blocklist

Set allowlist and blocklist if you want to control the passing vehicles at the entrance or exit via the barrier gate.

Before You Start

- Connect the barrier gate to the relay output interface of the device.
- Install the storage card, and ensure the storage status is normal.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Allowlist and Blocklist** .
2. Add an allowlist or blocklist.
   1) Click **Add**.
   2) Set **License Plate Number** and **Card No.**, and select the list type.
   3) **Optional:** If you want to control vehicles during fixed time period, enable **Time Settings**, and set the effective start time and end time.

      Note

      Time settings is only available for the allowlist vehicles.
   4) Click **OK**.

      Note

      Wait for 15 minutes to let the added allowlist or blocklist write into the storage. Do not reboot the device during the process.

   The information of the added vehicles in the allowlist or blocklist will be listed below.

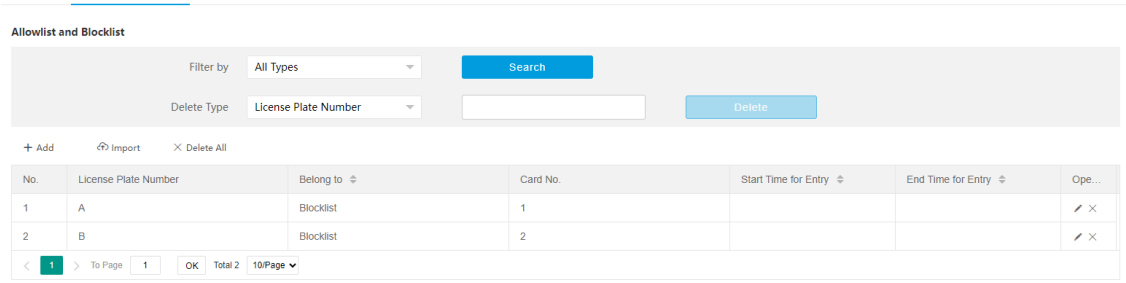

Figure 4-1 Set Allowlist and Blocklist

3. You can search, modify, delete, or import the allowlist and blocklist.

Search Select the search type, or enter the keywords. Click **Search**. The searched vehicle information will be listed below.

Modify Select an item from the list, and click . Modify the information, and click **OK**.

Delete
- Select the delete type, or enter the keywords. Click **Delete** to delete the lists of the same type.
- Select an item from the list, and click × to delete the item.
- Click **Delete All** to delete all the lists.

Import
a. Click **Import**.
b. Click **Download Template**, and save the template.
c. Open the template, edit the information, and save it.
d. Click **Import** again.
e. Click **Browse** to select the edited template.
f. Click **Import** to import the information to the device.

4.1.2 Control Barrier Gate

Link the barrier gate to realize the control and management of the vehicles at the entrance or exit.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Barrier Gate** .

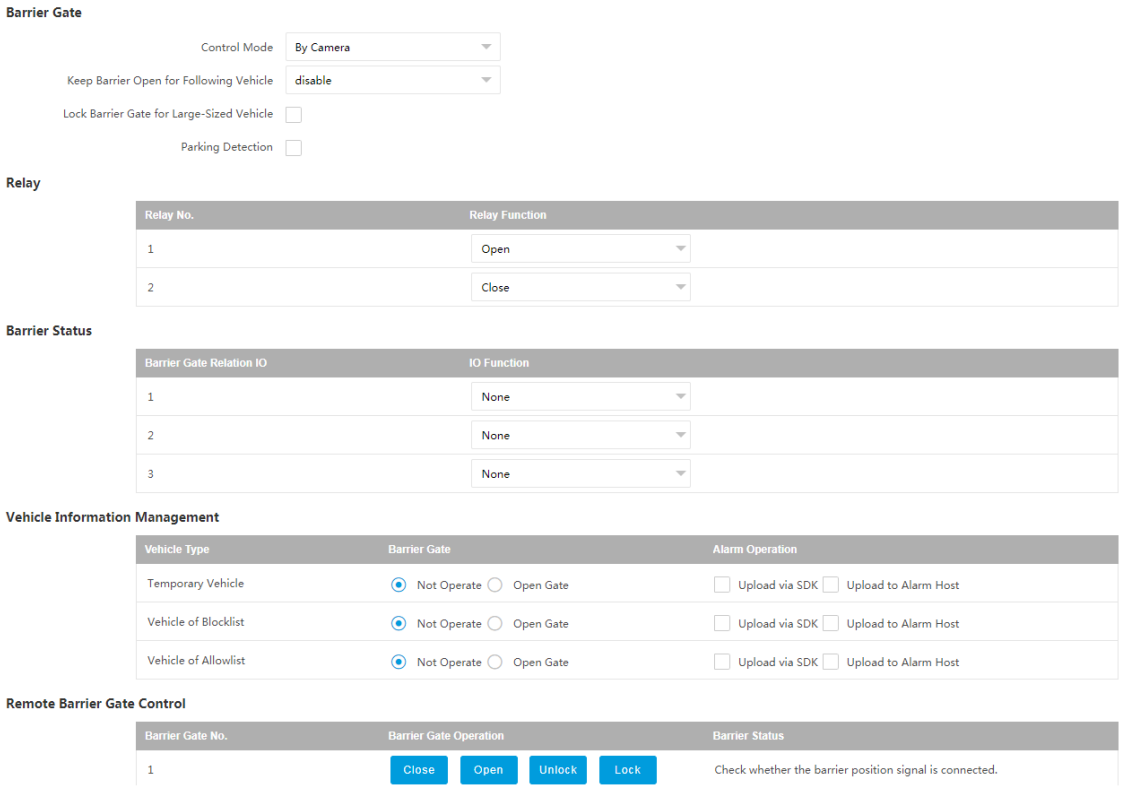

Figure 4-2 Control Barrier Gate

2. Set **Barrier Gate** parameters.

Control Mode

- Select **By Camera** in single camera scene (no control software) and allowlist scene in which the camera controls the barrier gate in advance according to the set passing rules in **Vehicle Information Management**.
- Select **By Platform** in the scene in which the entry permissions are controlled by the software.
- Select **By Mixed**, and the platform control and camera control are effective simultaneously. It is applicable to the scene in which different vehicle passing permissions are managed by software and camera. E.g., the software controls the passing of blocklist vehicles and temporary vehicles, and the camera controls the passing of allowlist vehicles and controls the barrier gate in advance for allowlist vehicles.

Keep Barrier Open for Following Vehicle

After you enable this function, the barrier gate keeps open when the device detects following vehicles are passing. The barrier gate will close after the following vehicles pass.

Lock Barrier Gate for Large-Sized Vehicle

Enable the function and set **Barrier Gate Rising Time**. If a large-sized vehicle is passing, the barrier gate will be locked during the set time.

Parking Detection

Enable the function and set **Judgment Time**. If a vehicle has been parked for a duration longer than the set judgment time, the parking information will be upload.

3. Set the relay function.

Note

The supported number of relays varies with different models. Relay 1 corresponds to the 1A and 1B of the terminal. Relay 2 corresponds to the 2A and 2B of the terminal.

4. Select **IO Function** for the corresponding barrier gate related I/O. The device will upload barrier gate status information for convenient exit and entrance management.

Note

- If the device only have one I/O interface, and the trigger type is **I/O Coil**, the barrier status cannot be configured.
- If the trigger type is **Radar Mixed Traffic** and the forward radar and backward radar are selected, the corresponding barrier gate related I/O function cannot be configured. E.g., the forward radar is IO1 and the backward radar is IO2. Then the barrier gate related IO1 and IO2 functions cannot be configured.

5. Set the barrier gate operation and alarm operation for the temporary vehicles, vehicles in the blocklist, and vehicles in the allowlist in **Vehicle Information Management**.

Upload via SDK

Check **Upload via SDK** to arm and upload the vehicle information to the arming terminal via SDK.

Upload to Alarm Host

If the device has been connected to the alarm device, check **Upload to Alarm Host**. When the barrier gate is open, the alarm device will be triggered to alarm.

6. **Optional:** You can click **Close**, **Open**, **Unlock**, or **Lock** to control the barrier gate remotely.

Note

The functions of remote control of barrier gate vary with different models. The actual device prevails.

7. Click **Save**.

4.1.3 Set Wiegand Parameters

The device can get access to the access control system or other system supporting Wiegand protocols to send data in the entrance and exit scenes.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Wiegand Parameters** .
2. Check **Enable**.

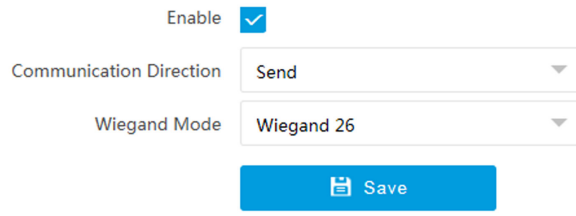

Figure 4-3 Set Wiegand Parameters

3. Select **Communication Direction**.

   Send

   The barrier gate can be connected to the device via Wiegand 26, Wiegand 34, Wiegand 72, or Wiegand sha1 26 protocol.

4. Select **Wiegand Mode**.

   Wiegand 26

   It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 8 digits) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 26 protocol.

   Wiegand 34

   It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 10 digits) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 34 protocol.

   Wiegand 72

   It is a non-standard Wiegand protocol. The device will get the card No. (up to 9 characters only including 0 to 9, uppercase, or lowercase can be sent) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 72 protocol.

   Wiegand sha1 26

   It is a non-standard Wiegand protocol. The captured license plate number will be encrypted via sha1. The last low 24 bits after encryption will be get as the data bits. The high 12-bit parity check bits will be added before the highest bit. The low 12-bit parity check bits will be added after the lowest bit. The bit stream composed with 26 bits will be sent to the access control system or other system supporting Wiegand protocols.

5. Click **Save** to save the settings.

Chapter 5 Live View and Local Configuration

5.1 Live View

5.1.1 Start/Stop Live View

Click ▶ to start live view. Click ■ to stop live view.

5.1.2 Select Image Display Mode

Click to select an image display mode.

5.1.3 Select Window Division Mode

Click to select a window division mode.

5.1.4 Select Stream Type

Click to select the stream type. It is recommended to select the main stream to get the high-quality image when the network condition is good, and select the sub-stream to get the fluent image when the network condition is not good enough.

Note

The supported stream types vary with different models. The actual device prevails.

5.1.5 Capture Picture Manually

You can capture pictures manually on the live view image and save them to the computer.

Steps

1. Click to capture a picture.
2. **Optional:** Click **Configuration → Local → Picture and Clip Settings** to view the saving path of snapshots in live view.

5.1.6 Record Manually

You can record videos manually on the live view image and save them to the computer.

Steps

1. Click to start live view.
2. Click to start recording.
3. Click to stop recording.
4. **Optional:** Click **Configuration → Local → Record File Settings** to view the saving path of record files.

5.1.7 Start/Stop Two-Way Audio

The device supports two-way audio with terminals, such as computers.

Before You Start

The device is equipped with an audio input interface and audio output interface, which support connecting with the corresponding devices, such as microphones and loudspeakers.

Steps

Note

The function varies with different models. The actual device prevails.

1. Select a window to start two-way audio.
2. Click to start live view.
3. Click to start two-way audio.

   When speaking at the PC end, you can hear the voice at the device end and vice versa.
4. Click to stop two-way audio.

5.1.8 Enable/Disable Audio

Enable the audio if necessary after connecting an audio input device under the audio & video stream. Click to enable and adjust it. Click again to disable this function.

Note

The function varies with different models. The actual device prevails.

5.1.9 Enable Digital Zoom

You can enable digital zoom to zoom in a certain part of the live view image.

Steps

1. Click to start live view.
2. Click to enable digital zoom.
3. Place the cursor on the live view image position which needs to be zoomed in. Drag the mouse rightwards and downwards to draw an area.

The area will be zoomed in.

4. Click any position of the image to restore to normal image.
5. Click to disable digital zoom.

5.1.10 Enable Regional Focus

Steps

1. Click .
2. Drag the cursor from the upper left corner to the lower right corner to select the area that needs to be focused.

Result

The selected area is focused.

5.1.11 Select Video Mode

Set the video mode when adjusting the device focus during construction.

Click and select when the device is running normally.

5.2 PTZ Operation

Click **Live View**. Click and click to show the PTZ control panel.

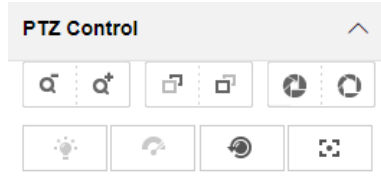

Figure 5-1 Control Panel

Table 5-1 Button Description

Button	Description
/	Zoom + and Zoom - • Hold to zoom in the scene. • Hold to zoom out the scene.
/	Focus + and Focus -

Button	Description
	• Hold under the manual focus mode to make near objects become clear and distant objects become vague. • Hold to make distant objects become clear and near objects become vague.
/	Iris + and Iris – • Hold to increase the iris diameter when in a dark environment. • Hold to decrease the iris diameter when in a bright environment.
	Lens Initialization It is applicable to devices with motorized lenses. You can use this function when overcoming image blurs caused by overtime zooming or focusing.
	Auxiliary Focus It is applicable to devices with motorized lenses. Use this function to focus the lens automatically and make images become clear.

Note

Other unmentioned buttons are reserved buttons.

5.3 Local Configuration

Go to **Configuration → Local** to set the live view parameters and change the saving paths of videos, captured pictures, scene pictures, etc.

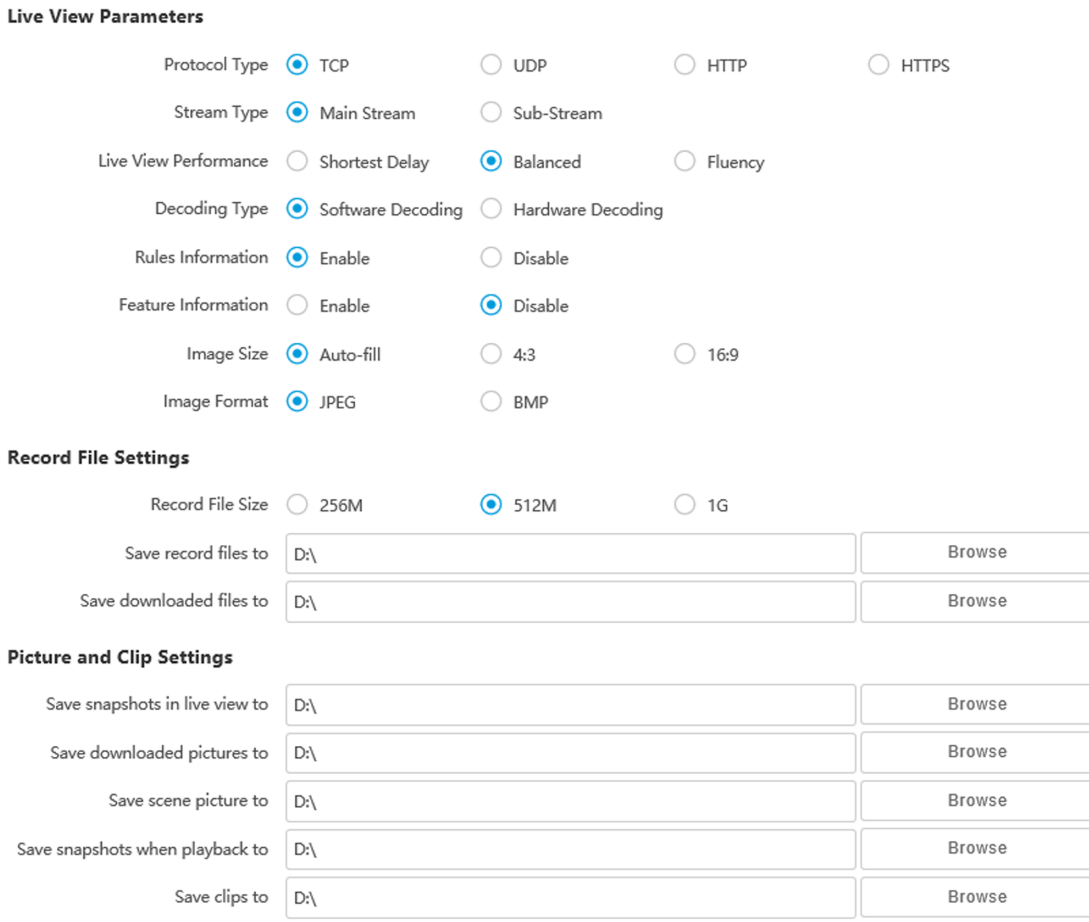

Figure 5-2 Local Configuration

Protocol Type

Select the network transmission protocol according to the actual needs.

TCP

Ensures complete delivery of streaming data and better video quality, but the real-time transmission will be affected.

UDP

Provides real-time audio and video streams.

HTTP

Gets streams from the device by a third party client.

HTTPS

Gets streams in https format.

Stream Type

Main Stream

Select it to get the high-quality image when the network condition is good.

Sub-Stream

Select it to get the fluent image when the network condition is not good enough.

Live View Performance

Shortest Delay

The video is real-time, but its fluency may be affected.

Balanced

Balanced mode considers both the real time and fluency of the video.

Fluency

When the network condition is good, the video is fluent.

Decoding Type

Software Decoding

Decode via software. It takes up more CPU resources but provides images with better quality when it compares to the hardware decoding.

Hardware Decoding

Decode via GPU. It takes up less CPU resources but provides images with worse quality when it compares to the software decoding.

Rules Information

If you enable this function, tracking frames will be displayed on the live view interface when there are vehicles passing.

Feature Information

Enable it to display feature information of the target on the live view image.

Image Size

The display ratio of the live view image.

Image Format

The saving format of manually captured images.

Record File Size

Select the packed size of the manually recorded video files. After the selection, the max. record file size is the value you selected.

Save record files to

Set the saving path of the manually recorded video files.

Save downloaded files to

Set the saving path of the download files.

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Save downloaded pictures to

Set the saving path of the downloaded pictures.

Save scene picture to

Set the saving path of the captured pictures in **Live View → Real-Time Capture** .

Save snapshots when playback to

Set the saving path of the manually captured pictures in playback mode.

Save clips when playback to

Set the saving path of the clips in playback mode.

Chapter 6 Playback

You can search, play back, and download videos that stored on the storage card.

Steps

1. Click **Playback**.
2. Select a channel.
3. Select a date.
4. Click **Search**.
5. Click ▶ to start playback.
6. **Optional:** You can also do the following operations.

Set playback time	• Drag the time bar to the target time and click ▶ to play the video. • Click the current time point showed above the time bar and enter the target time point in the popup window. Click **OK** and click ▶ to play the video.
Capture image	Click 📷 to capture an image.
Clip record	Click ✂ / ✂ to start/stop clipping the record.
Play back in single frame	Click ⏭ once to play back the video in one frame.
Download record	a. Click ⬇ . b. Select the start time and end time. c. Click **Search**. d. Check record files that need to be downloaded. e. Click **Download**.
Stop playback	Click ■ to stop playback.
Slow forward	Click « to slow down the playback.
Fast forward	Click » to speed up the playback.
Digital zoom	Click 🔍 to enable digital zoom. Click 🔍 to disable digital zoom.
Adjust volume	Click 🔊 to enable volume.

Chapter 7 Record and Capture

7.1 Set Storage Path

7.1.1 Set Memory Card

If you want to store the files to the memory card, make sure you insert and format the memory card in advance.

Before You Start
Insert the memory card to the device.

Steps
1. Go to **Configuration → Storage → Storage Management → HDD Management** .

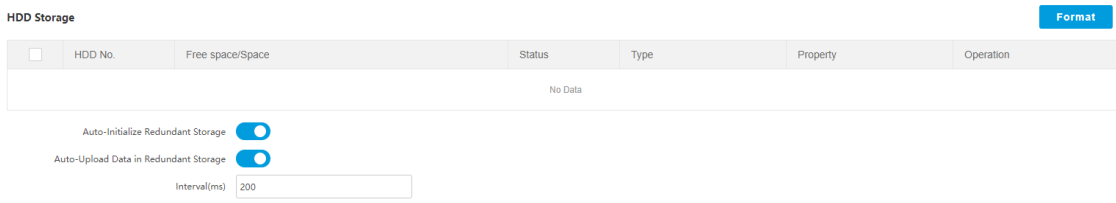

Figure 7-1 Set Memory Card

2. Format the memory card in two ways.
   - Check the memory card, and click **Format** to format it manually.

     Note

     For the newly installed memory card, you need to format it manually before using it normally.
   - If you want to format the memory card automatically when the card is abnormal, check **Auto-Initialize Redundant Storage**.
3. **Optional:** If the device has been connected to the platform, and you want to upload the memory card information automatically, check **Auto-Upload Data in Redundant Storage** and set **Interval** to upload.
4. Click **Save**.

7.1.2 Set FTP

Set FTP parameters if you want to upload the captured pictures to the FTP server.

Before You Start
Set the FTP server, and ensure the device can communicate normally with the server.

Steps

1. Go to **Configuration → Network → Data Connection → FTP** .

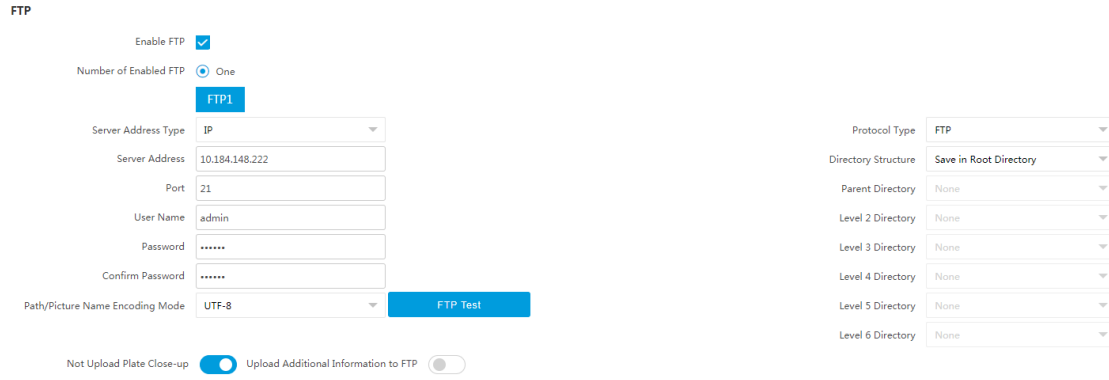

Figure 7-2 Set FTP

2. Check **Enable FTP**.
3. Select **Number of Enabled FTP**.

Note

You can only enable one FTP.

4. Set FTP Parameters.
   1) Select **Sever Address Type** and enter corresponding information.
   2) Enter **Port**.
   3) Enter **User Name**, **Password**, and confirm the password.
   4) Select **Protocol Type**.
   5) Select **Directory Structure**.

Note

You can customize the directory structure according to your needs.

5. Select **Path/Picture Name Encoding Mode**.

   UTF-8

   UNICODE encoding.

6. **Optional:** Enable upload functions.

   Not Upload Plate Close-up

   The close-up pictures of a license plate will not be uploaded.

   Upload Additional Information to FTP

   Add related information when uploading data to the FTP server.

7. **Optional:** Click **FTP Test** to check the FTP server.
8. Set naming rules and separators according to the actual needs.
9. **Optional:** Edit **OSD information** which can be uploaded to the FTP server with the pictures to make it convenient to view and distinguish the data.
10. Click **Save**.

7.1.3 Set SDK Listening

The SDK listening can be used to receive the uploaded information and pictures of the device arming alarm.

Before You Start

The listening service has been enabled for the SDK listening, and the network communication with the device is normal.

Steps

1. Go to **Configuration → Network → Data Connection → SDK Listening** .

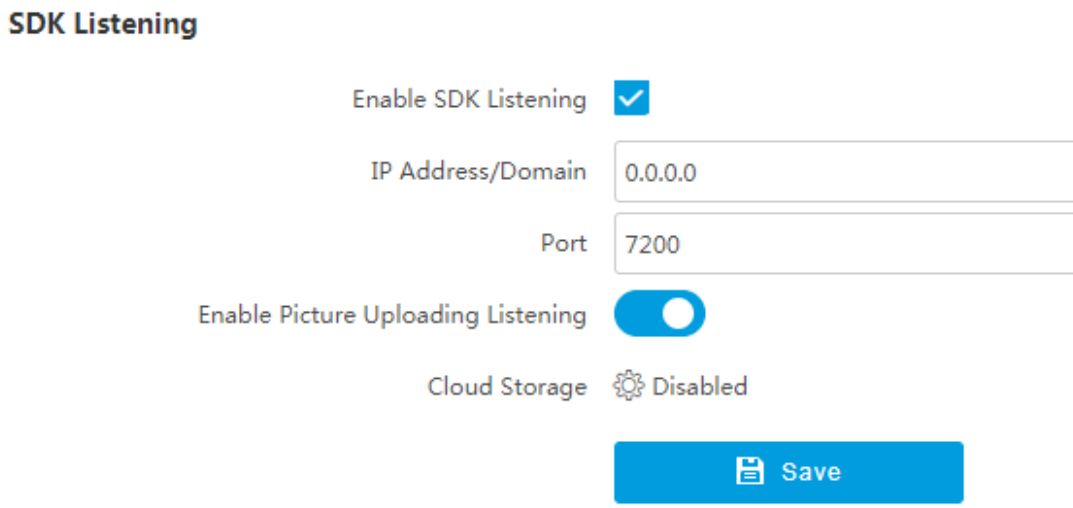

Figure 7-3 Set SDK Listening

2. Check **Enable SDK Listening**.
3. Set **IP Address/Domain** and **Port** if you need to upload the alarm information and pictures.
4. **Optional:** Enable the picture uploading listening if you need to upload image information.
5. **Optional:** If you want to save the alarm information and pictures to the cloud storage, click ⚙ to set **Cloud Storage**. Refer to ***Set Cloud Storage*** for details.
6. Click **Save**.

7.1.4 Set Arm Host

The device can upload the captured pictures via the arm host.

Steps

Note

For level 1 arm, the pictures can be uploaded normally. If uploading failed, the device will upload again. For level 2 arm, the pictures will be uploaded once. No more upload if uploading failed. For level 3 arm, pictures will not be uploaded.

1. Go to **Configuration → Network → Data Connection → Arm Upload** .

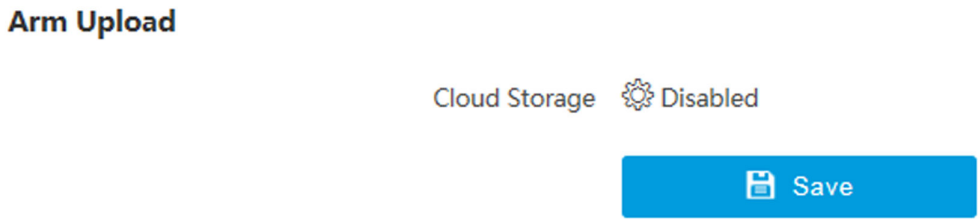

Figure 7-4 Set Arm Host

2. Click ⚙ to set **Cloud Storage**. Refer to ***Set Cloud Storage*** for details.
3. Click **Save**.

7.1.5 Set ISAPI Listening

ISAPI listening and SDK listening are mutually exclusive protocols. If you enable the picture uploading listening, the device will transmit images via the SDK listening. If not, the device will upload images via ISAPI protocol after the ISAPI parameters are set.

Before You Start

The listening service has been enabled for the ISAPI host, and the network communication with the device is normal.

Steps

1. Go to **Configuration → Network → Data Connection → ISAPI Listening** .

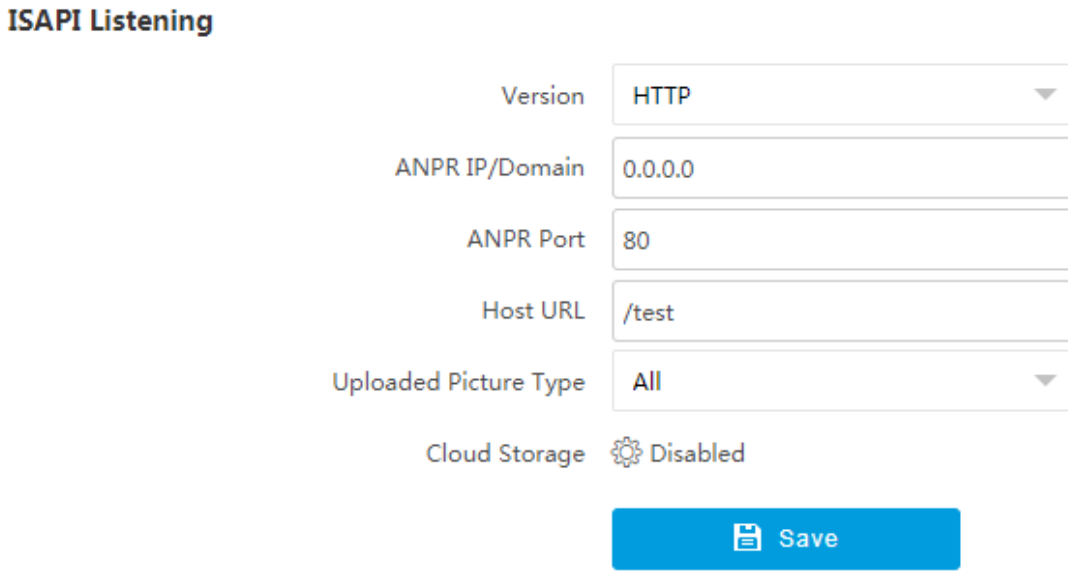

Figure 7-5 Set ISAPI Listening

2. Set **ANPR IP/Domain**, **ANPR Port**, and **Host URL**.
3. Set **Uploaded Picture Type**.
4. **Optional:** If you want to save the alarm information and pictures to the cloud storage, click ⚙ to set **Cloud Storage**. Refer to ***Set Cloud Storage*** for details.
5. Click **Save**.

7.1.6 Set Cloud Storage

Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

- Arrange the cloud storage server.
- You have enabled level 1 arm in **Live View → Real-Time Capture** .

Steps

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .

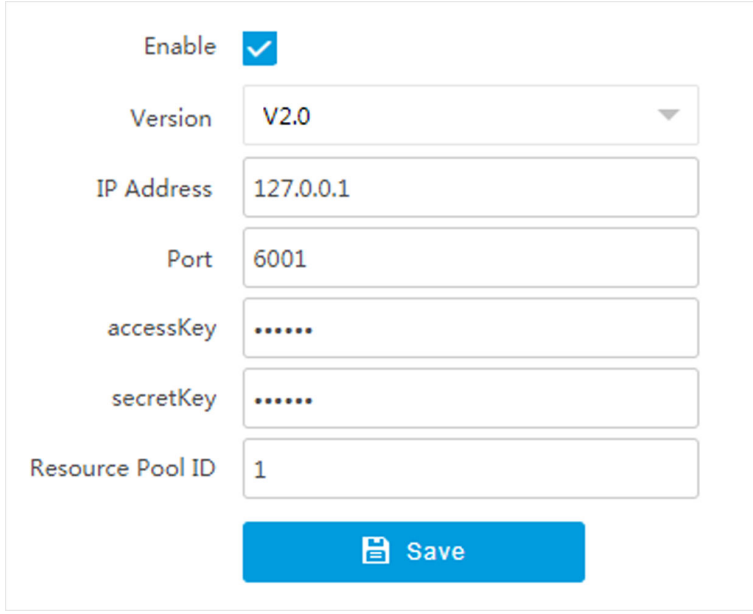

Figure 7-6 Set Cloud Storage

2. Check **Enable**.
3. Select **Version**.

V1.0
a. Enter **IP Address** and **Port**
b. Enter **User Name** and **Password**.
c. Enter **Cloud Storage ID** according to the server storage area No.

V2.0
a. Enter **IP Address** and **Port**
b. Enter **accessKey** and **secretKey**.
c. Enter **Resource Pool ID** according to the server storage area No. of uploading pictures.

4. Click **Save**.

7.2 Set Quota

Set the video and picture ratio in the storage.

Before You Start
Install the memory card.

Steps
1. Go to **Configuration → Storage → Storage Management → HDD Management → HDD Quota** .
2. Set **Capture Quota Ratio** and **Video Quota Ratio** according to the actual needs.

Note
The percentage sum of the capture and video quota ratio should be 100%.

3. Click **Save**.

What to do next
Format the memory card after the settings.

7.3 Set Record Schedule

Set record schedule to record video automatically during configured time periods.

Before You Start
Install the storage card.

Steps
1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. **Optional:** Enable the recording overwriting.
   When the storage is full, the earliest videos will be overwritten.
3. Enable the record schedule.

Figure 7-7 Set Record Schedule

4. Select **Record Type**.
5. Drag the cursor on the time bar to set a recording time.

Note

Up to 8 time periods can be set on a time bar.

6. Adjust the recording time.
   - Click a set recording period and enter the start time and end time in the pop-up window.

- Drag two ends of the set recording period bar to adjust the length.
- Drag the whole set recording period bar and relocate it.

7. **Optional:** Delete recording periods.
   - Click a set recording period and click **Delete** in the pop-up window.
   - Click a set recording period and click **Delete** on the record configuration interface.
8. **Optional:** Click to copy set recordings to other days.
9. Click **Save**.

Result

The device will only record at the set periods.

Chapter 8 Encoding and Display

8.1 Set Video Encoding Parameters

Set video encoding parameters to adjust the live view and recording effect.

- When the network signal is good and the speed is fast, you can set high resolution and bitrate to raise the image quality.
- When the network signal is bad and the speed is slow, you can set low resolution, bitrate, and frame rate to guarantee the image fluency.
- When the network signal is bad, but the resolution should be guaranteed, you can set low bitrate and frame rate to guarantee the image fluency.
- Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space. Third stream is offered for customized usage.

Steps

Note

The supported parameters vary with different models. The actual device prevails.

1. Go to **Configuration → Video → Video Encoding → Video Encoding** .
2. Set the parameters for different streams.

   Stream Type

   Video stream and video & audio stream are selectable.

   Bitrate

   Select relatively large bitrate if you need good image quality and effect, but more storage spaces will be consumed. Select relatively small bitrate if storage requirement is in priority.

   Frame Rate

   It is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

   Resolution

   The higher the resolution is, the clearer the image will be. Meanwhile, the network bandwidth requirement is higher.

   SVC

Scalable Video Coding (SVC) is an extension of the H.264/AVC and H.265 standard. Enable the function and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is variable, 6 levels of video quality are selectable. The higher the video quality is, the higher requirements of the network bandwidth.

Profile

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to device models.

I Frame Interval

It refers to the number of frames between two key frames. The larger the I frame interval is, the smaller the stream fluctuation is, but the image quality is not that good.

Video Encoding

The device supports multiple video encoding types, such as H.264, H.265, and MJPEG. Supported encoding types for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate, and image quality.

3. Click **Save**.

8.2 Set Image Parameters

You can adjust the image parameters to get clear image.

Steps

Note

The supported parameters may vary with different models. The actual device prevails.

1. Go to **Configuration → Video → Camera Parameter → Camera Parameter** .

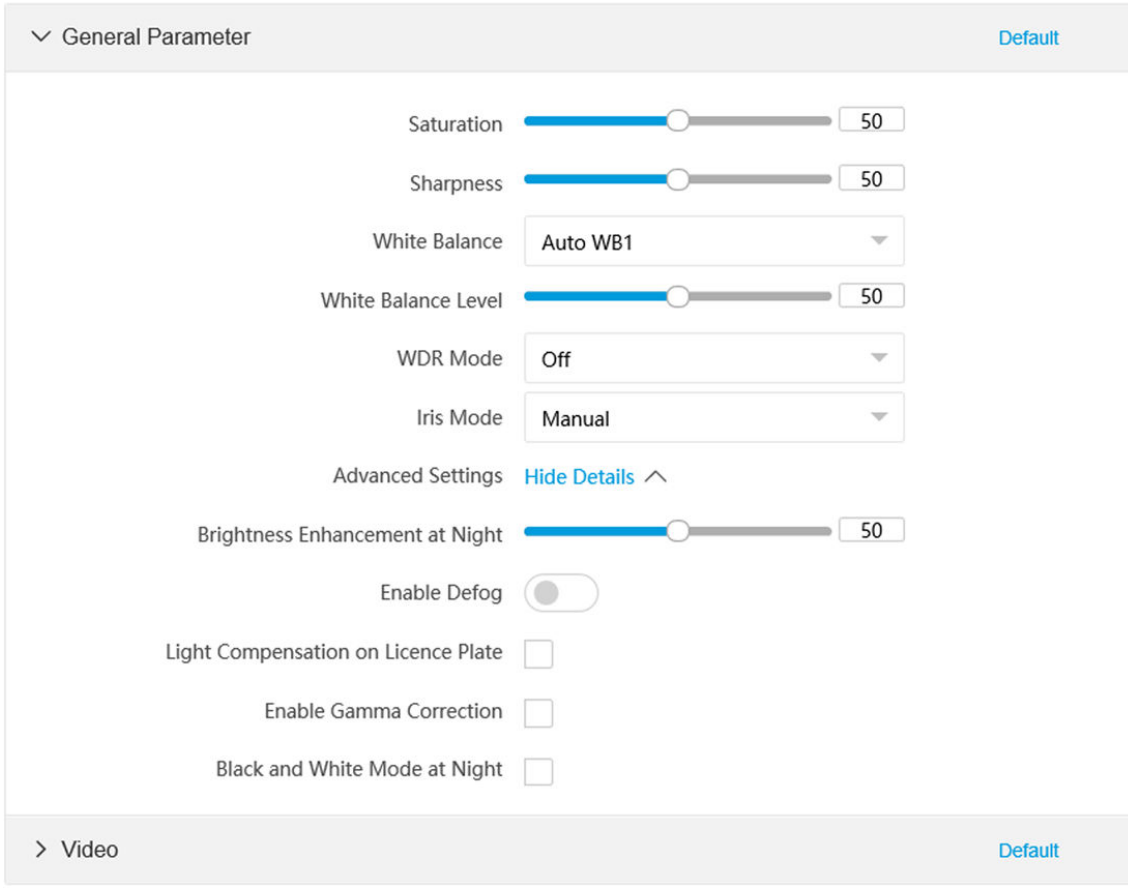

Figure 8-1 Set Image Parameters

2. Set the camera parameters.

Note

Click **Default** to reset parameters.

General Parameter

Saturation

It refers to the colorfulness of the image color.

Sharpness

It refers to the edge contrast of the image.

White Balance

It is the white rendition function of the device used to adjust the color temperature according to the environment.

WDR Mode

Wide Dynamic Range (WDR) can be used when there is a high contrast of the bright area and the dark area of the scene.

Select **WDR Switch** and set corresponding parameters according to your needs.

On

Set **WDR Level**. The higher the level is, the higher the WDR strength is.

Time

Enable WDR according to the set time period and level.

Brightness

Set **Light Threshold** and **WDR Level**. When the brightness reaches the threshold, WDR will be enabled.

Iris Mode

Select the iris mode as manual or auto.

Brightness Enhancement at Night

The scene brightness will be enhanced at night automatically.

Enable Defog

Enable defog to get a clear image in foggy days.

Light Compensation on License Plate

Check it. The plate brightness compensation can be realized, and various light supplement conditions can be adapted via setting license plate expectant brightness and supplement light correction coefficient. The higher the sensitivity is, the easier this function can be enabled.

Enable Gamma Correction

The higher the gamma correction value is, the stronger the correction strength is.

Black and White Mode at Night

When ICR is in night mode, you can check it to keep the video in black and white mode.

Video

Brightness

It refers to the brightness the image.

Contrast

It refers to the contrast of the image. Set it to adjust the levels and permeability of the image.

Shutter

If the shutter speed is quick, the details of the moving objects can be displayed better. If the shutter speed is slow, the outline of the moving objects will be fuzzy and trailing will appear.

Gain

It refers to the upper limit value of limiting image signal amplification. It is recommended to set a high gain if the illumination is not enough, and set a low gain if the illumination is enough.

3D DNR

Digital Noise Reduction (DNR) reduces the noise in the video stream.

In **Normal Mode**, the higher the **3D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

In **Expert Mode**, set **Spatial Intensity** and **Time Intensity**. If the space domain intensity is too high, the outline of the image may become fuzzy and the details may lose. If the time domain intensity is too high, trailing may appear.

2D DNR

The higher the **2D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

Slow Shutter

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure. The higher **Slow Shutter Level** is, the slower the shutter speed is.

Video Standard

Select the video standard according to the actual power supply frequency.

3. **Optional:** Click **Capture Test** to check the image.

8.3 Set ICR

ICR adopts mechanical IR filter to filter IR in the day to guarantee the image effect, and to remove the IR filter at night to guarantee full-spectrum rays can get through the device.

Steps

1. Go to **Configuration → Capture → Capture Images → ICR** .
2. Select **ICR Mode**.

Auto Switch	Switches to ICR mode automatically at night or in dark light conditions.
Manual Switch	Switches to the day or night manually.
Scheduled Switch	Set day/night mode, start time, and end time to switch to ICR mode only during the set time period. **Note** The four start times and end times cannot be the same. At least one minute interval should be set.
No Switch	Disable ICR mode.

3. Click **Save**.

8.4 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resources to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video encoding type. ROI is supported when the video encoding type is H.264 or H.265.

Steps

1. Go to **Configuration → Video → Video Encoding → ROI** .

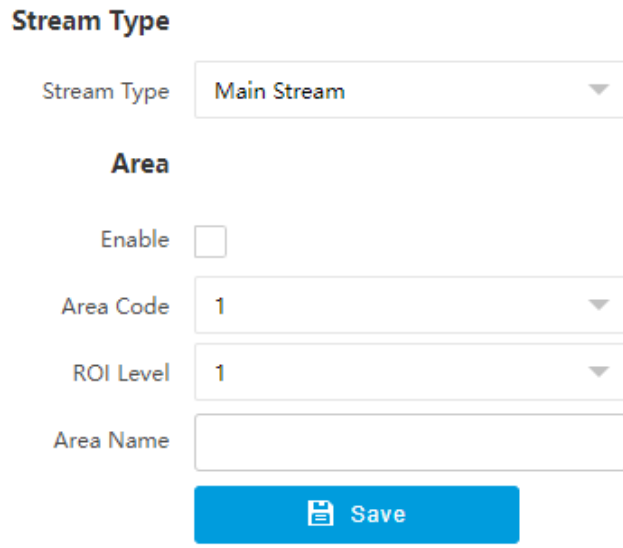

Figure 8-2 Set ROI

2. Select **Stream Type**.
3. Set ROI region.
   1) Check **Enable**.
   2) Select **Area Code**.
   3) Click **Draw Area**.
   4) Drag the mouse on the live view image to draw the fixed area.
   5) Select the fixed area that needs to be adjusted and drag the mouse to adjust its position.
   6) Click **Stop Drawing**.
4. Enter **Area Name** and select **ROI Level**.

Note

The higher the ROI level is, the clearer the image of the detected area is.

5. Click **Save**.
6. **Optional:** Select other area codes and repeat the steps above if you need to draw multiple fixed areas.

8.5 Set OSD

You can customize OSD information on the live view.

Steps

1. Go to **Configuration → Video → Text Overlay on Video → Text Overlay on Video** .

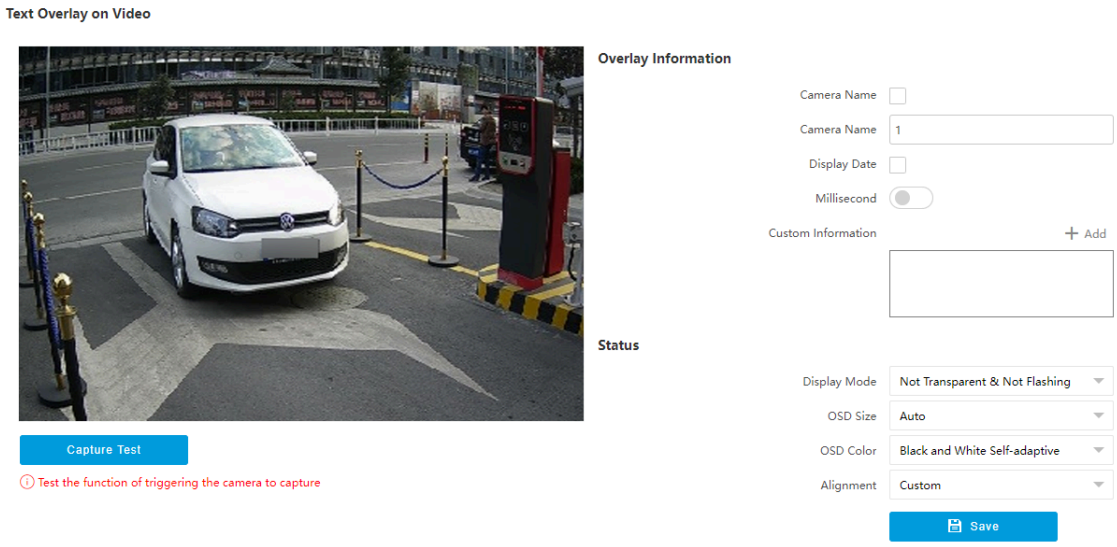

Figure 8-3 Set OSD

2. Set display contents.
   1) Check **Camera Name**.
   2) Enter **Camera Name**.
   3) Check **Display Date**, and set the time and date format.
   4) Enable **Millisecond** according to your needs.
3. **Optional:** Click **Add** and enter information if you want to add custom information.

Note

Up to 6 items of custom information can be added.

4. Set display properties (font, color, etc.).
5. Select **Alignment**.

Note

If you select **Align Left** or **Align Right**, set **Min. Horizontal Margin** and **Min. Vertical Margin**.

6. Drag the red frames on the live view image to adjust the OSD positions.

7. Click **Save**.

Result

The set OSD will be displayed in live view image and recorded videos.

8.6 Enable Regional Exposure

Enable regional exposure to expose partial area of the live view image.

Steps

1. Go to **Configuration → Video → Video Encoding → BLC** .
2. Check **Enable**.
3. Drag the mouse to draw an area in the live view image.
   The drawn area will be exposed.
4. Click **Save**.

Chapter 9 Network Configuration

9.1 Set IP Address

IP address must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Network Parameters → Network Interface** .

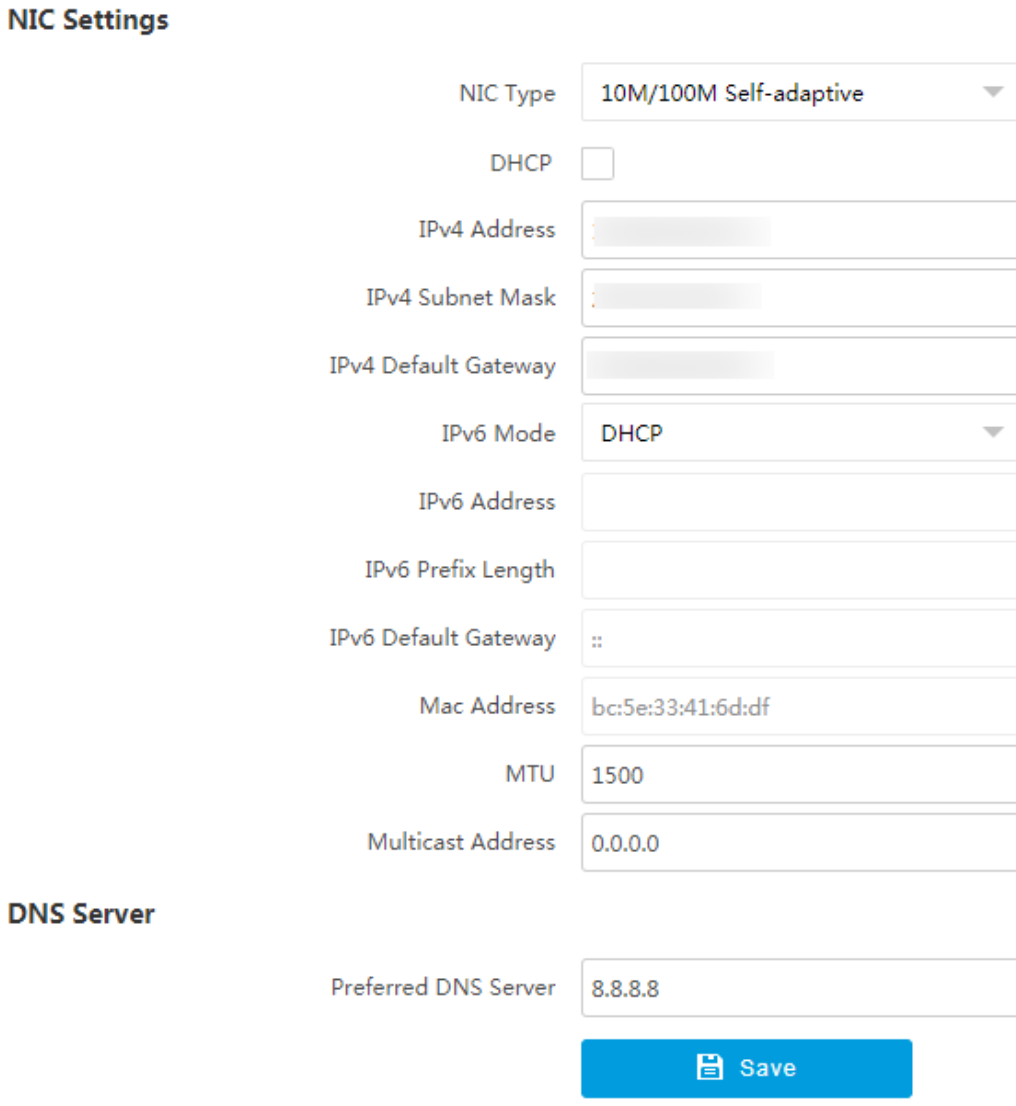

Figure 9-1 Set IP Address

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two modes are available.

DHCP

The device automatically gets the IP parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IP parameters manually. Enter **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast Address

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting the IP address of the multicast host, you can send the source data efficiently to multiple receivers.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** properly if needed.

9.2 Connect to Platform

9.2.1 Connect to ISUP Platform

ISUP (EHome) is a platform access protocol. The device can be remotely accessed via this platform.

Before You Start

- Create the device ID on ISUP platform.
- Ensure the device can communicate with the platform normally.

Steps

1. Go to **Configuration → Network → Data Connection → ISUP** .

Figure 9-2 Connect to ISUP Platform

2. Check **Enable ISUP**.
3. Select **Protocol Version**.
4. Select **Address Type**.
5. Enter **Sever IP Address**, **Server Port**, and **Device ID**.

Note

You need to enter **Key** if you select **Protocol Version** as **v5.0**.

6. Click **Save**.

7. **Optional:** View **Register Status**.

What to do next
When the registration status shows online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

9.2.2 Connect to OTAP

The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information.

Before You Start
Ensure the device can communicate with the platform normally.

Steps
1. Go to **Configuration → Network → Data Connection → OTAP** .
2. Check **Enable**.

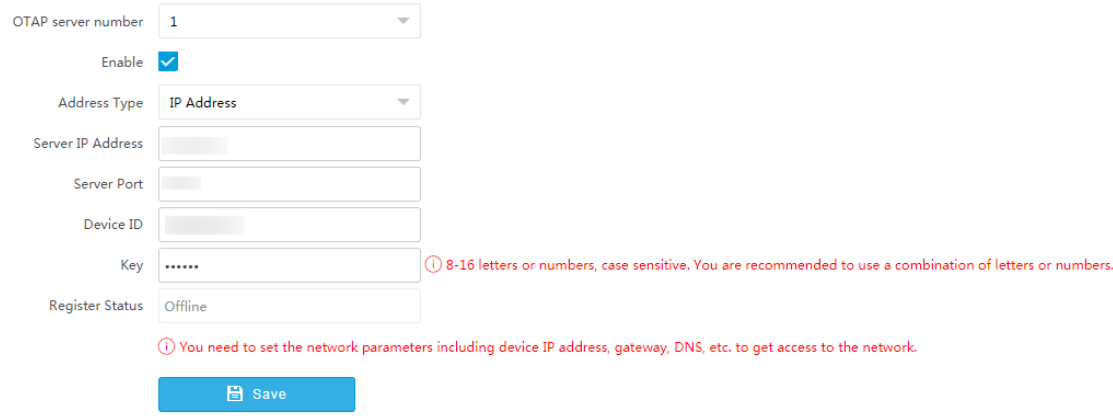

Figure 9-3 Connect to OTAP

3. Set corresponding parameters.

Note

The device ID should be the same with the added one on the OTAP platform.

4. Click **Save**.

What to do next
When the registration status is online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

9.2.3 Connect to Hik-Connect

The device can be remotely accessed via Hik-Connect.

Before You Start

- Connect the device to the Internet.
- Set the IP address, subnet mask, gateway, and DNS server of the LAN.
- OTAP connection is disabled.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Configuration → Network → Data Connection → Hik-Connect Platform** .
2. Check **Enable Hik-Connect Platform**.

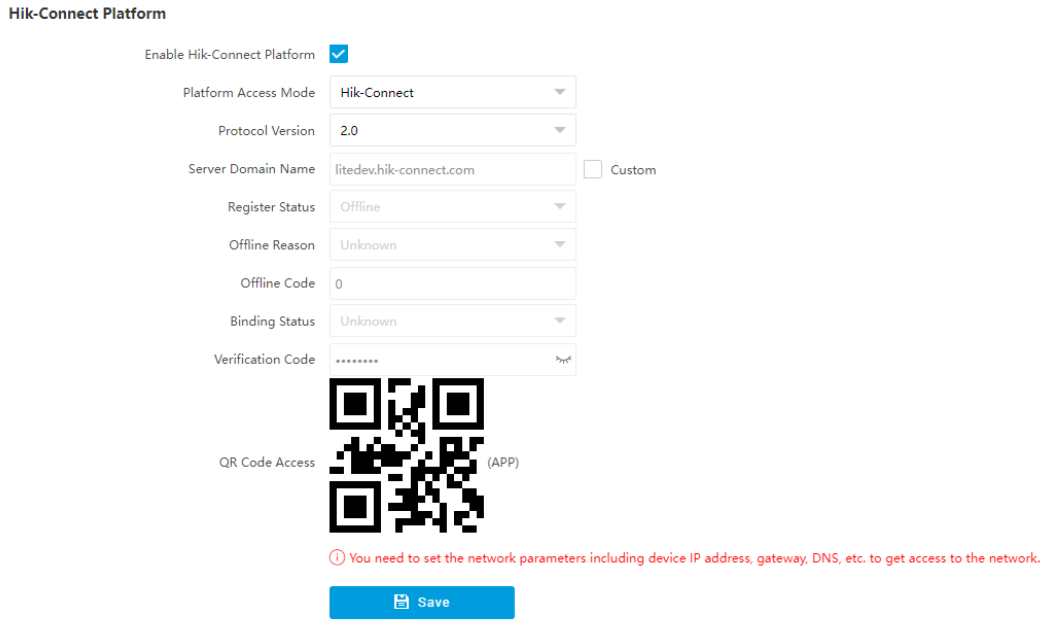

Figure 9-4 Connect to Hik-Connect

3. Select **Protocol Version**.
4. **Optional:** If you have allocated a custom server, check **Custom** and enter the custom **Server Domain Name**.
5. Add the device to Hik-Connect.

Set a verification code to add the device to Hik-Connect

a. Enter a custom **Verification Code** used to add the device.

Caution

The verification code should be 6 letters or numbers, case sensitive. You are recommended to use a combination of letters or numbers.

b. Click **Save**.

c. Get and install Hik-Connect application by the following ways.

- Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
- Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
- Scan the QR code below to download the application.

Figure 9-5 Hik-Connect

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

d. Start the application and register a user account to log in.
e. Add device by the serial No. on the device body and the verification code.

Scan the QR code on the interface to add the device to Hik-Connect

a. Get and install Hik-Connect application according to the ways above.
b. Scan the QR code on the interface with the Hik-Connect application, and add the device to Hik-Connect.

Note

The verification information has been included in the QR code, so you do not need to enter the verification code.

Note

Refer to the user manual of Hik-Connect application for details.

9.3 Set DDNS

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to for details.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

1. Go to **Configuration → Network → Network Parameters → DDNS** .

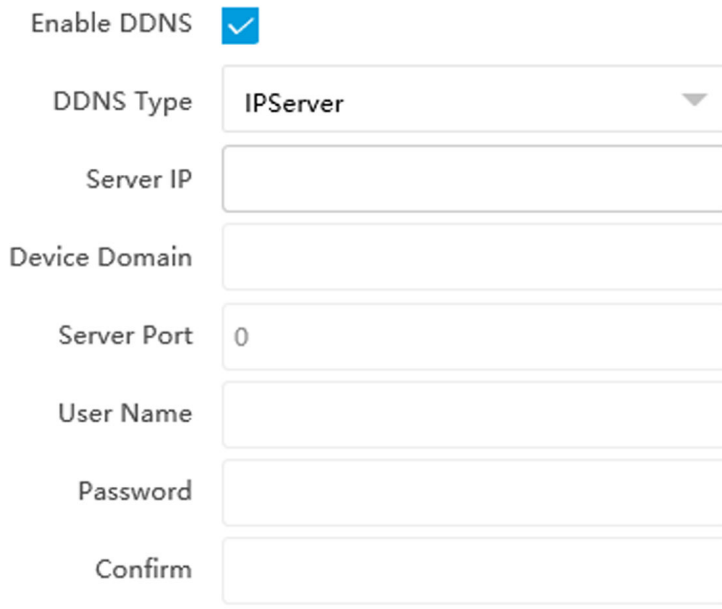

Figure 9-6 Set DDNS

2. Check **Enable DDNS**.
3. Enter the server address and other information.
4. Click **Save**.
5. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client software manual for specific adding methods.

9.4 Set SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration → Network → Network Parameters → SNMP** .
2. Check **Enable SNMPv1**/**Enable SNMP v2c**/**Enable SNMPv3**.

Note

- The SNMP version you select should be the same as that of the SNMP software.
- Use different versions according to the security levels required. SNMP v1 is not secure and SNMP v2 requires password for access. SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Set the SNMP parameters.
4. Click **Save**.

9.5 Set Port

The device port can be modified when the device cannot access the network due to port conflicts.

Go to **Configuration → Network → Network Parameters → Port** for port settings.

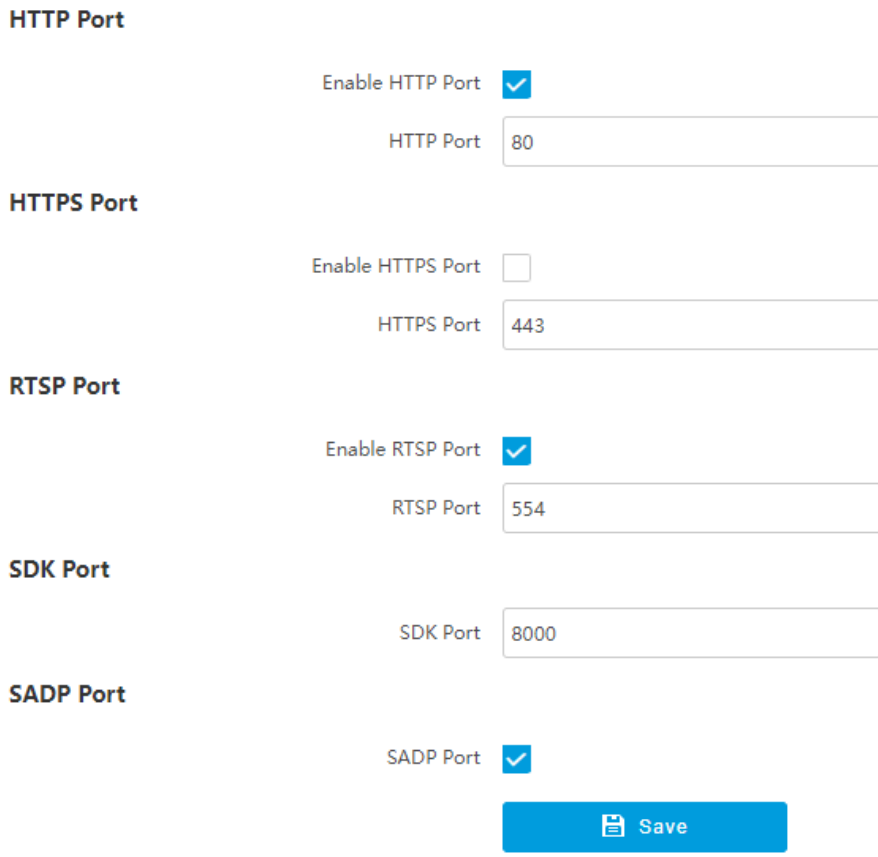

Figure 9-7 Set Port

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

Set the HTTPS for accessing the browser. Certificate is required when accessing.

RTSP Port

It refers to the port of real-time streaming protocol.

SDK Port

It refers to the port through which the client adds the device.

SADP Port

It refers to the port through which the SADP software searches the device.

Note

- After editing the port, access to the device via new port.
- Reboot the device to take the new settings into effect.
- The supported ports vary with different models. The actual device prevails.

Chapter 10 Serial Port Configuration

10.1 Set RS-485

Set RS-485 parameters if the device has been connected to a vehicle detector or other RS-485 devices.

Before You Start
The corresponding device has been connected via the RS-485 serial port.

Steps

Note
The number of available RS-485 serial port varies with different models.

1. Go to **Configuration → System → System Settings → Serial Port → RS-485** .
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

   Note
   The parameters should be same with those of the connected device.
3. Set **Work Mode**.

   Transparent Channel

   Select it when the other peripheral devices are connected to the RS-485 serial port of the device for communication transmission.
4. Click **Save**.

10.2 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port, or peripheral devices have been connected.

Before You Start
The debugging device has been connected via the RS-232 serial port.

Steps
1. Go to **Configuration → System → System Settings → Serial Port → RS-232** .
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

   Note
   The parameters should be same with those of the connected device.
3. Select **Work Mode**.

   Console

Select it when you need to debug the device via RS-232 serial port.

Transparent Channel

Select it, and the network command can be transmitted to RS-232 control command via the RS-232 serial port.

Narrow Bandwidth Transmission

Reserved.

4. Click **Save**.

Chapter 11 Exception Alarm

Set exception alarm when the network is disconnected, the IP address is conflicted, etc.

Steps

Note

The supported exception types vary with different models. The actual device prevails.

1. Go to **Configuration → Event → Alarm Linkage → Exception** .
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

Chapter 12 Safety Management

12.1 Manage User

The administrator can add, modify, or delete other accounts, and grant different permissions to different user levels.

Steps

1. Go to **Configuration → System → User Management → User List** .
2. Select **Password Level**.

   The password level of the added user should conform to the selected level.
3. Add a user.
   1) Click **Add**.
   2) Enter **User Name** and select **Type**.
   3) Enter **Admin Password**, **New Password**, and confirm the password.

   Caution

   To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

   4) Assign remote permission to users based on needs.

   User

   Users can be assigned permission of viewing live video and changing their own passwords, but no permission for other operations.

   Operator

   Operators can be assigned all permission except for operations on the administrator and creating accounts.

   5) Click **OK**.
4. **Optional:** You can do the following operations.

Change the password and permission	Click ✎ to change the password and permission.
Delete the user	Click 🗑 to delete the user.

12.2 Set IP Address Filtering

You can set the IP addresses allowable and not allowable to access the device.

Steps

1. Go to **Configuration → System → Security → Security Settings** .
2. Check **Enable IP Address Filtering**.

3. Set **Filtering Mode**.

   Blocklist Mode

   The added IP addresses are not allowed to access the device.

   Allowlist Mode

   The added IP addresses are allowed to access the device.

4. Click **Add**, enter the IP address, and click **OK**.

   Note

   The IP address only refers to the IPv4 address.

5. **Optional:** Edit, delete, or clear the added IP addresses.
6. Click **Save**.

12.3 Enable User Lock

To raise the data security, you are recommended to lock the current IP address.

Steps

1. Go to **Configuration → System → Security → Security Service → Software** .
2. Enable user lock.
3. Click **Save**.

Result

When the times you entered incorrect passwords have reached the limit, the current IP address will be locked automatically.

12.4 Set HTTPS

12.4.1 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Parameters → HTTPS** .
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **OK**.

Result

The device will install the self-signed certificate by default.

12.4.2 Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **Configuration → Network → Network Parameters → HTTPS** .
2. Select **Create certificate request first and continue the installation**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Hostname/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Import certificate to the device.
   - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
   - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
7. Click **Save**.

12.5 Set SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **Configuration → System → Security → Security Service → Software** .
2. Disable **SSH Service**.
3. Click **Save**.

12.6 Set RTSP Authentication

You can improve network access security by setting RTSP authentication.

Steps

1. Go to **Configuration → System → Security → Security Settings** .
2. Select **RTSP Authentication**.

   digest

   The device only supports digest authentication.

   digest/basic

   The device supports digest or basic authentication.
3. Click **Save**.

12.7 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration → System → Security → Security Service → Timeout Logout** .
2. Enable timeout logout for static page.
3. Set **Max. Timeout**.
4. Click **Save**.

Result

When the page static time exceeds the set time, the device will automatically log out.

12.8 Set Password Validity Period

You can improve network access security by setting password validity period.

Steps

1. Go to **Configuration → System → Security → Security Service → Password Validity Period** .
2. Select **Validity Type**.
   - Select **Permanent**. The password will be permanently valid.
   - Select **Daily** and set **Password Expiry Time**. It will prompt you that the password is expired according to the set password expiry time, and you need to set the new password.
3. Click **Save**.

Chapter 13 Maintenance

13.1 View Device Information

Basic Information and Algorithms Library Version

Go to **Configuration → System → System Settings → Basic Information** to view the basic information and algorithms library version of the device.
You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

Device Status

Go to **Configuration → System → System Settings → Device Status** to view the status of the current device.

13.2 Log

13.2.1 Enable System Log Service

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events. Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you are recommended to save the logs on a log server.

Steps

1. Go to **Configuration → System → Security → Security Service → Log Audit Service** .
2. Enable system log service.
3. Enter **IP Address** and **Port** of the log server.
4. Click **Save**.

Result

The device will upload the security audit logs to the log server regularly.

13.2.2 Search Log

Log helps to locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log Search** .
2. Set search conditions.

3. Click **Search**.

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files to your computer.

13.3 Upgrade

Upgrade the system when you need to update the device version.

Before You Start

- Update the plugin before upgrade.
- Prepare the upgrade file. If the upgrade file is a compressed package, it needs to be decompressed into the .dav format.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Upgrade** .
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.

Note

The upgrade process will take 1 to 10 minutes. Do not cut off the power supply.

Result

The device will reboot automatically after upgrade.

13.4 Reboot

When the device needs to be rebooted, reboot it via the software instead of cutting off the power directly.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Device Maintenance** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

13.5 Restore Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Device Maintenance** .
2. Select the restoration mode.
   - Click **Restore** to restore the parameters except the IP address, subnet mask, gateway, and port No. to the default settings.
   - Click **Restore Factory Settings** to restore all the parameters to the factory settings.
3. Click **OK**.

13.6 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select **Sync Mode**.

   NTP Synchronization

   Select it to synchronize the device time with that of the NTP server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

   Manual Synchronization

   Select it to synchronize the device time with that of the computer. Set time manually, or check **Sync. with computer time**.

   SDK

   If the remote host has been set for the device, select it to synchronize time via the remote host.

   ONVIF

   Select it to synchronize time via the third-party device.

   No

   Select it to disable time synchronization.

   All

   Select it, and you can select any mode above.

   Note

   The time synchronization modes vary with different models. The actual device prevails.

4. Click **Save**.

13.7 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → DST** .
2. Check **Enable DST**.
3. Set **Start Time**, **End Time**, and **DST Bias**.
4. Click **Save**.

13.8 Debug

Note

The debug configurations below are only provided to debug the device by the professionals.

13.8.1 Debug Device

You can enable the functions to debug the device.

Steps

1. Go to **Configuration → Capture → Advanced → System Service** .
2. Check the debug information according to your needs.

   Note

   The supported parameters vary with different models. The actual device prevails.

   Enable Algorithm POS Information Debug

   The algorithm POS information will be overlaid on the playback image when you play back the video with the dedicated tool.
3. Click **Save**.

13.8.2 Vehicle Capture and Recognition Service

Set the vehicle capture and recognition service to debug the device.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Vehicle Capture and Recognition Service** .

2. Check the service(s) according to your needs.

Note

The supported services vary with different models. The actual device prevails.

multiProtocolUpload Enabled

The captured information will upload to all the connected platforms (such as the FTP, arm host, listening, etc.) without priority.

noPlateFilter Enabled

The vehicles without license plates will not be captured.

Filter Checkpoint Capture of Same Vehicle

It is used to debug the device with the same vehicle. When the same vehicle is triggered many times during a short period in the scene, the checkpoint pictures of the vehicle will not be captured.

3. Click **Save**.

13.9 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Data Export** .
2. Click **Export** after **Configuring Parameters**.
3. Set an encryption password, confirm the password, and click **OK**.

Note

The password is used for importing the configuration file of the current device to other devices.

4. Select the saving path, and enter the file name.
5. Click **Save**.

13.10 Import Configuration File

Import the configuration file of another device to the current device to set the same parameters.

Before You Start

Save the configuration file to the computer.

Steps

Caution

Importing configuration file is only available to the devices of the same model and same version.

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Advanced Settings → Data Import** .
2. Select **Importing Method**.

Note

If you select **Import Part**, check the parameters to be imported.

3. Click **Browse** to select the configuration file.
4. Click **Import**.
5. Enter the password which is set when the configuration file is exported, and click **OK**.
6. Click **OK** on the popup window.

Result

The parameters will be imported, and the device will reboot.

13.11 Export Debug File

The technicians can export the debug file to troubleshoot and maintain the device.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Data Export** .
2. Click **Export** after **Debug File**.
3. Select the saving path, and enter the file name.
4. Click **Save**.

13.12 Export Diagnosis Information

The technicians can export the diagnosis information to troubleshoot and maintain the device.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Data Export** .
2. Click **Export** after **Diagnosis Information**.
3. Select the saving path, and enter the file name.
4. Click **Save**.


See Far, Go Further