



# **Entrance and Exit Capture Camera**

**User Manual**

## Initiatives on the Use of Video Products

### **Thank you for choosing Hikvision products.**

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

### **Please read the following initiatives carefully:**

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

## Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website ( <https://www.hikvision.com/> ).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

### Trademarks

**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.

### Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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

## Entrance and Exit Capture Camera User Manual

---

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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

## Regulatory Information

### 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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### FCC Conditions

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.

### EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: [www.recyclethis.info](http://www.recyclethis.info)



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: [www.recyclethis.info](http://www.recyclethis.info)

## **Industry Canada ICES-003 Compliance**

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

## Symbol Conventions

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

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

## Safety Instruction

### Regulatory Information

This is a class A product and may cause radio interference in which case the user may be required to take adequate measures.

### Laws and Regulations

Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.

### Power Supply

- Use of the product must be in strict compliance with the local electrical safety regulations.
- Use the power adapter provided by qualified manufacturer. Refer to the product specification for detailed power requirements.
- It is recommended to provide independent power adapter for each device as adapter overload may cause over-heating or a fire hazard.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device in the authorized way according to the description in the manual.
- To avoid electric shock, DO NOT directly touch exposed contacts and components once the device is powered up.
- DO NOT use damaged power supply devices (e.g., cable, power adapter, etc.) to avoid electric shock, fire hazard, and explosion.
- DO NOT directly cut the power supply to shut down the device. Please shut down the device normally and then unplug the power cord to avoid data loss.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Make sure the power supply has been disconnected if the power adapter is idle.
- Connect to earth before connecting to the power supply.

### Transportation, Use, and Storage

- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Store the device in dry, well-ventilated, corrosive-gas-free, no direct sunlight, and no heating source environment.
- Avoid fire, water, and explosive environment when using the device.
- Install the device in such a way that lightning strikes can be avoided. Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- Keep the device away from magnetic interference.
- Avoid device installation on vibratory surfaces or places. Failure to comply with this may cause device damage.
- DO NOT touch the heat dissipation component to avoid burns.

- DO NOT expose the device to extremely hot, cold, or humidity environments. For temperature and humidity requirements, see device specification.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- DO NOT touch the sharp edges or corners.
- To prevent possible hearing damage, DO NOT listen at high volume levels for long periods.

### **Installation**

The appropriate disconnecting device should be provided as part of the installation.

### **Maintenance**

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.
- If the device cannot work properly, contact the store you purchased it or the nearest service center. DO NOT disassemble or modify the device in the unauthorized way (For the problems caused by unauthorized modification or maintenance, the company shall not take any responsibility).
- Keep all packaging after unpacking them for future use. In case of any failure occurred, you need to return the device to the factory with the original packaging. Transportation without the original packaging may result in damage to the device and the company shall not take any responsibility.

### **Network**

- Please enforce the protection for the personal information and the data security as the device may be confronted with the network security problems when it is connected to the Internet. Contact us if network security risks occur.
- Please understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

### **Lens**

- DO NOT touch the lens with fingers directly in case the acidic sweat of the fingers erodes the surface coating of the lens.
- DO NOT aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the device.

### **Battery**

- DO NOT charge the battery continuously more than one week. Overcharging may shorten the battery life.
- Battery will discharge gradually if it is not used for a long time. It must be recharged before using.
- If the device contains dismountable battery, store the device and battery separately if it is not used.
- The battery must be charged and discharged every three months if it is not used, and recharged to 60% to 70% power percentage to store.

## Entrance and Exit Capture Camera User Manual

---

- The scrapped battery should be discarded in compliance with the local laws and regulations. If there are no corresponding laws or regulations, throw it in a hazardous trash can.
- DO NOT pierce the battery or shorten the electrodes, or it may cause explosion or fire hazard.
- DO NOT dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- CAUTION: Please use the specific battery supported by the device, or it may cause explosion. If the battery is damaged and needs to be changed, contact the device manufacturer or local distributor.
- If the device contains button battery, keep it far away from children.
- DO NOT expose the battery pack or battery combination to sunlight, fire, or similar overheated environment. DO NOT leave the battery in an extremely high temperature surrounding environment or subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children.

### **Data**

DO NOT disconnect the power during formatting, uploading, and downloading. Or files may be damaged.

# Contents

<b>Chapter 1 Introduction .....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Key Feature .....	1
<b>Chapter 2 Activation and Login .....</b>	<b>2</b>
2.1 Activation .....	2
2.1.1 Default Information .....	2
2.1.2 Activate via SADP .....	2
2.1.3 Activate via Web Browser .....	3
2.2 Login .....	4
<b>Chapter 3 Capture Configuration .....</b>	<b>5</b>
3.1 Quick Configuration .....	5
3.1.1 Set Basic Parameters .....	5
3.1.2 Adjust Image .....	5
3.2 Detailed Configuration .....	7
3.2.1 Set Application Mode .....	7
3.2.2 Set Capture Parameters .....	9
3.3 View Real-Time Picture .....	13
3.4 Search Picture .....	15
<b>Chapter 4 Peripheral Device Linkage .....</b>	<b>17</b>
4.1 Set Barrier Gate Linkage .....	17
4.1.1 Set Allowlist and Blocklist .....	17
4.1.2 Control Barrier Gate .....	19
4.2 Set LCD .....	20
4.3 Set Serial Port .....	23
4.3.1 Set RS-485 .....	23
4.3.2 Set RS-232 .....	23

<b>Chapter 5 Network Configuration</b> .....	<b>25</b>
5.1 Set IP Address .....	25
5.2 Connect to Platform .....	27
5.2.1 Connect to ISUP Platform .....	27
5.2.2 Connect to Guarding Vision .....	28
5.3 Set DDNS .....	29
5.4 Set IEEE 802.1X .....	30
5.5 Set Port .....	30
<b>Chapter 6 Record</b> .....	<b>32</b>
6.1 Set Storage Path .....	32
6.1.1 Set Memory Card .....	32
6.1.2 Set FTP .....	33
6.1.3 Set Listening Host .....	34
6.1.4 Set Cloud Storage .....	34
6.2 Set Quota .....	35
6.3 Set Record Schedule .....	36
6.4 Local Configuration .....	37
<b>Chapter 7 Encoding and Display</b> .....	<b>39</b>
7.1 Set Video Encoding Parameters .....	39
7.2 Set Image Parameters .....	40
7.3 Set ICR .....	43
7.4 Set ROI .....	43
7.5 Set OSD .....	45
<b>Chapter 8 Safety Management</b> .....	<b>47</b>
8.1 Manage User .....	47
8.2 Set IP Address Filtering .....	47
8.3 Enable User Lock .....	48
8.4 Set SSH .....	48

8.5 Set HTTPS .....	49
8.5.1 Create and Install Self-signed Certificate .....	49
8.5.2 Install Authorized Certificate .....	49
<b>Chapter 9 Maintenance .....</b>	<b>50</b>
9.1 View Device Information .....	50
9.2 Log .....	50
9.2.1 Enable System Log Service .....	50
9.2.2 Search Log .....	50
9.3 Upgrade .....	51
9.4 Reboot .....	51
9.5 Restore Parameters .....	51
9.6 Synchronize Time .....	52
9.7 Set DST .....	52
9.8 Export Parameters .....	53
9.9 Import Configuration File .....	53
9.10 Export Debug File .....	54
<b>Appendix A. Communication Matrix and Device Command .....</b>	<b>55</b>

# Chapter 1 Introduction

## 1.1 Introduction

Entrance and exit capture 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.
- Control of the external audio device to output voice via audio output interface.
- Offline and online voice play. After the license plate is recognized, voice will be played.

---

 **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.



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 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.



**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.





### 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. Enter **User Name** and **Password**.
3. Click **Login**.
4. Download and install appropriate plug-in for your web browser. Follow the installation prompts to install the plug-in.
5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 3 to login.
6. **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** .
2. If you need to modify the device IP address, enter **IP Address**, **Subnet Mask**, and **Default Gateway**.
3. Select **Scene Mode**.

#### 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** .
2. Adjust lens to meet the license plate with 120 to 180 pixels.

---

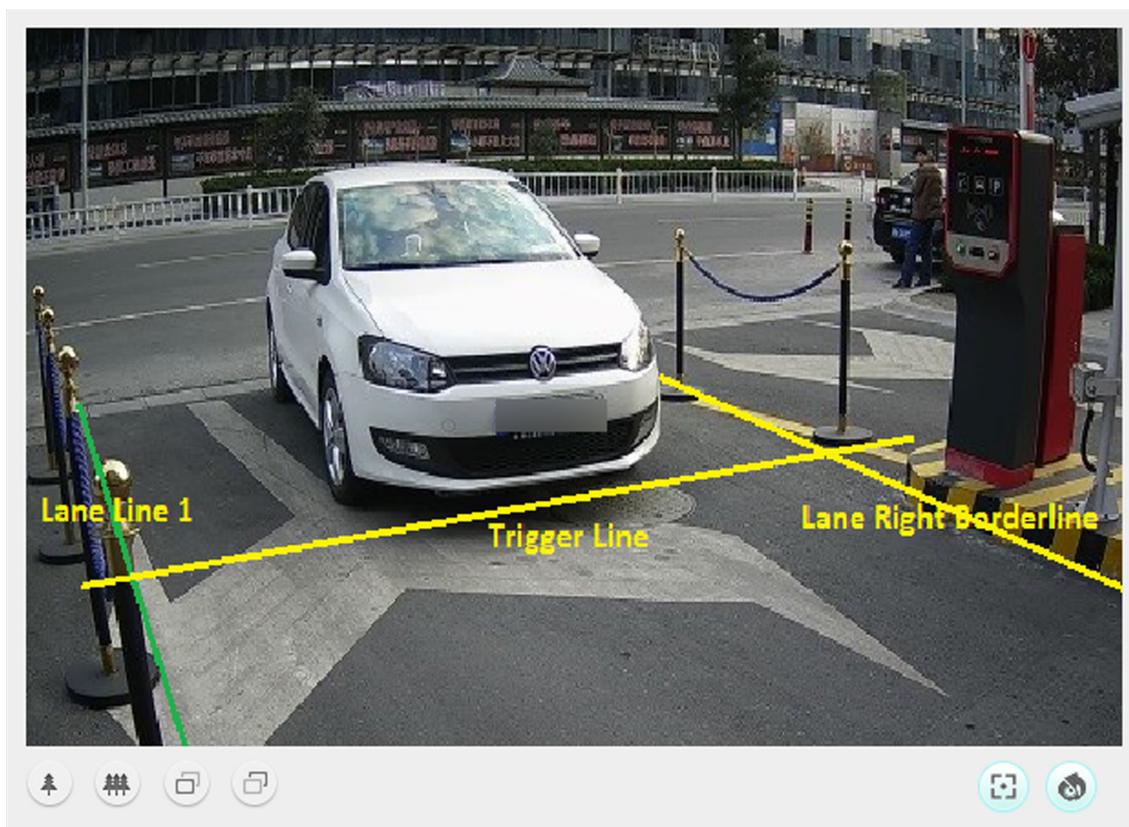
##### Note

- There are two ways to measure the license plate pixel. You can click **Measure Plate** on **Real-Time Picture** interface, and draw a frame on the license plate position to measure the pixel. Or measure the pixel with the Windows drawing tool.
  - The lens of some models are prime lens. Lens adjustment is not supported. The actual device prevails.
  - For some models, you need to adjust the focal lens and focus via the lens lever.
-

Icon	Function	Icon	Function
	Hold it to realize zoom +.		Hold it to realize focus -.
	Hold it to realize zoom -.		Click it to realize one-touch focus.
	Hold it to realize focus +.		Click it to initialize the lens, and all the parameters will restore to default.

### 3. Adjust lines.

- 1) Select the lane line, lane right limit, or trigger line.
- 2) Drag the endpoint to adjust the position and length of the line, or drag the line to adjust its position.
- 3) Click **Complete** to save the settings.



**Figure 3-1 Adjust Lines**

4. Test the capture effect. After the vehicle passed through the coils, click **Picture** and click **Search** to search the captured pictures. If pictures are captured, the adjustment is successful.

---

#### **Note**

If other trigger types are set in the site, refer to "Detailed Configuration" for details.

---

## 3.2 Detailed Configuration

### 3.2.1 Set Application Mode

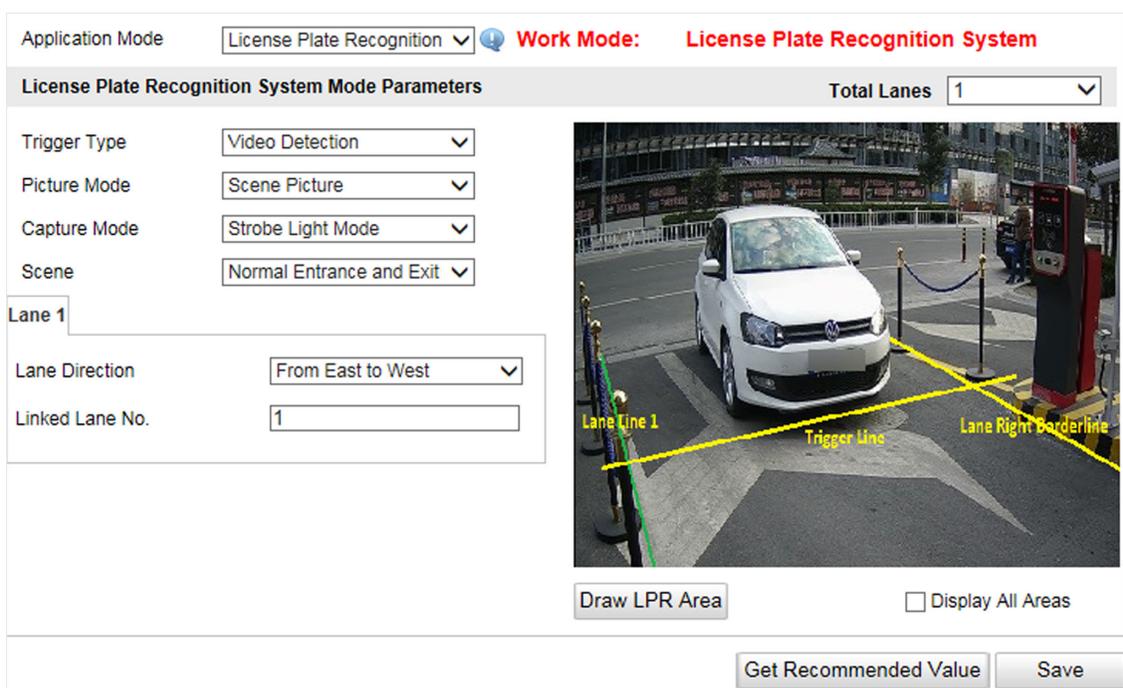
If you want to trigger capture of the passing vehicle information at the entrance or exit, set the application mode.

#### Before You Start

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

#### Steps

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



**Figure 3-2 Set Application Mode**

2. Click **Draw LPR Area** to draw the lines.

- 1) Check the lane line, lane right limit, or trigger line.
- 2) Drag the endpoint 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 pixel should be between 120 to 180 at the capture position.

3. Select **Trigger Type**.

- Video Detection** Select it when video recognition mode is applied at the site. The capture mode is **Strobe Light Mode**.
- I/O Coil** Select it when the device has been connected to I/O signal.
- RS485** Select it when the device has been connected to RS-485 devices.
- Radar Mixed Traffic** Select it when the device detects vehicles via coils, and only the license plates at the entrance need to be captured.



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



The trigger types vary with different models. The actual device prevails.

---

#### 4. Select **Picture Mode**.

- 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.

#### 5. Select **Scene**.

#### 6. Set **Lane Direction**, **Linked Lane No.**, and other parameters according to the selected trigger type.

##### **Lane Direction**

The license plates of the vehicles from the set detection will be captured.

##### **Linked Lane No.**

It is the corresponding lane No. of the trigger command.

##### **I/O Trigger Default 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.**

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.

##### **RS-485 Linked Camera No.**

It refers to the connected channel No. of the RS-485 serial port.

#### 7. 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

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



License Parameters

License Plate Recognition  Front Plate  Back Plate  Front And Back Plate

Country/Region

**Figure 3-3 Set License Plate Recognition Parameters**

2. When the trigger type is vehicle detection, select **License Plate Recognition**.
  - If only license plates of vehicles from unidirection need to be captured, select **Front Plate** or **Back Plate**.
  - If both the front and back license plates need to be captured, select **Front and Back Plate**.
3. Select **Country/Region**.
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



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

---

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

The screenshot shows a configuration window for 'I/O:1'. It contains the following elements:

- I/O Output Mode:** A dropdown menu set to 'Constant Light Mode'.
- Duty Ratio/Brightness:** A text input field containing '0' with a range indicator '[0-40]' to its right.
- Control Constant Light by Brightness:** An unchecked checkbox.
- Control Constant Light by Schedule:** An unchecked checkbox.
- White Light Brightness:** A slider control with a numeric input field set to '0'.
- IR Light Brightness:** A slider control with a numeric input field set to '0'.

**Figure 3-4 Set Supplement Light Parameters**

## 2. Set **Duty Ratio/Brightness**.

### **Duty Ratio/Brightness**

It is the time occupation of the high level in a certain period. The higher the duty ratio, the brighter the supplement light. High duty ratio will cut life span of the supplement light.

## 3. Set constant light control mode and other parameters.

**Control Constant Light by Brightness** Check 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.

**Control Constant Light by Schedule** Check it when you want the constant light to be enabled during fixed time period. Set the start time and end time.

**White Light Brightness/IR Light Brightness/Constant 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 supported functions 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.

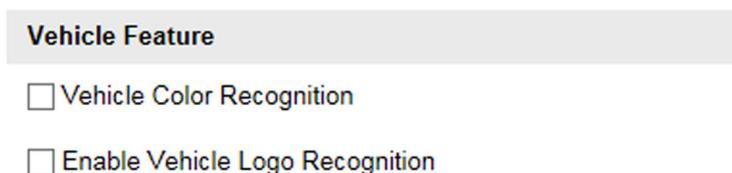
## Steps



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

---

1. Go to **Configuration → Device Configuration → Capture Parameters → Vehicle Feature** .



**Vehicle Feature**

Vehicle Color Recognition

Enable Vehicle Logo Recognition

**Figure 3-5 Set Vehicle Feature Parameters**

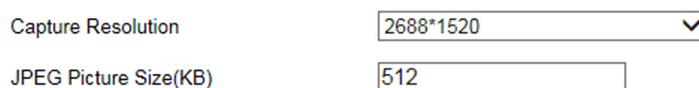
2. Check the vehicle features to be recognized.
3. Click **Save**.

## 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 → Device Configuration → Encoding and Storage → Image Encoding** .



Capture Resolution

JPEG Picture Size(KB)

**Figure 3-6 Set Image Encoding Parameters**

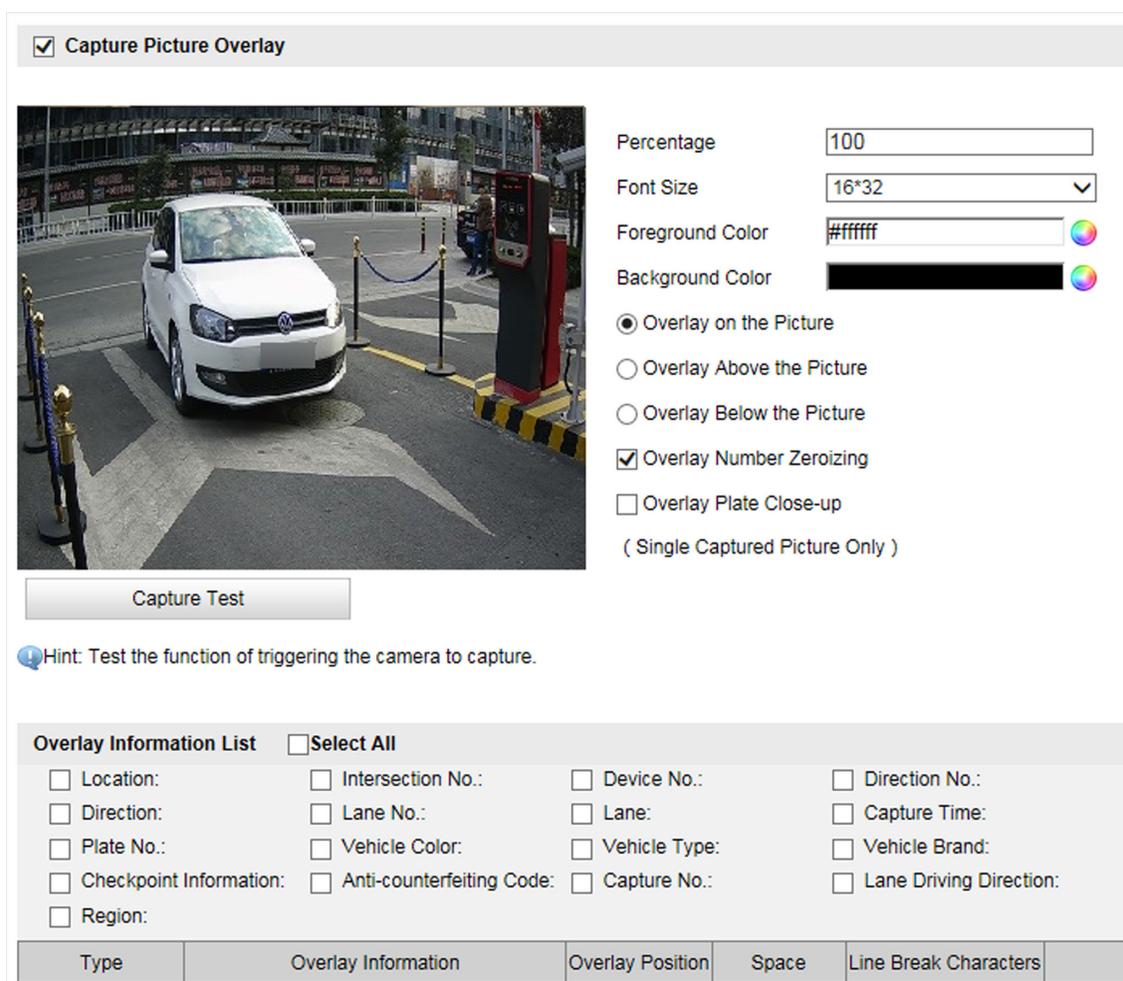
2. Select **Capture Resolution**.
3. Enter **JPEG Picture Size**.
4. Click **Save**.

## Set Capture Overlay

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

### Steps

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



**Figure 3-7 Set Capture Overlay**

3. Set the font size, color, overlay position, etc.

**Percentage**

It is the percentage that the overlaid information occupies on the picture.

**Overlay Number Zeroizing**

When the overlaid number digits are smaller than the fixed digits, 0 will be overlaid before the overlaid number. E.g., the fixed digits for lane No. is 2. If the lane No. is 1, 01 will be overlaid on the picture.

**Overlay Plate Close-up**

Check it, and a license plate close-up picture will be overlaid on the upper left corner of the captured picture.

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.

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

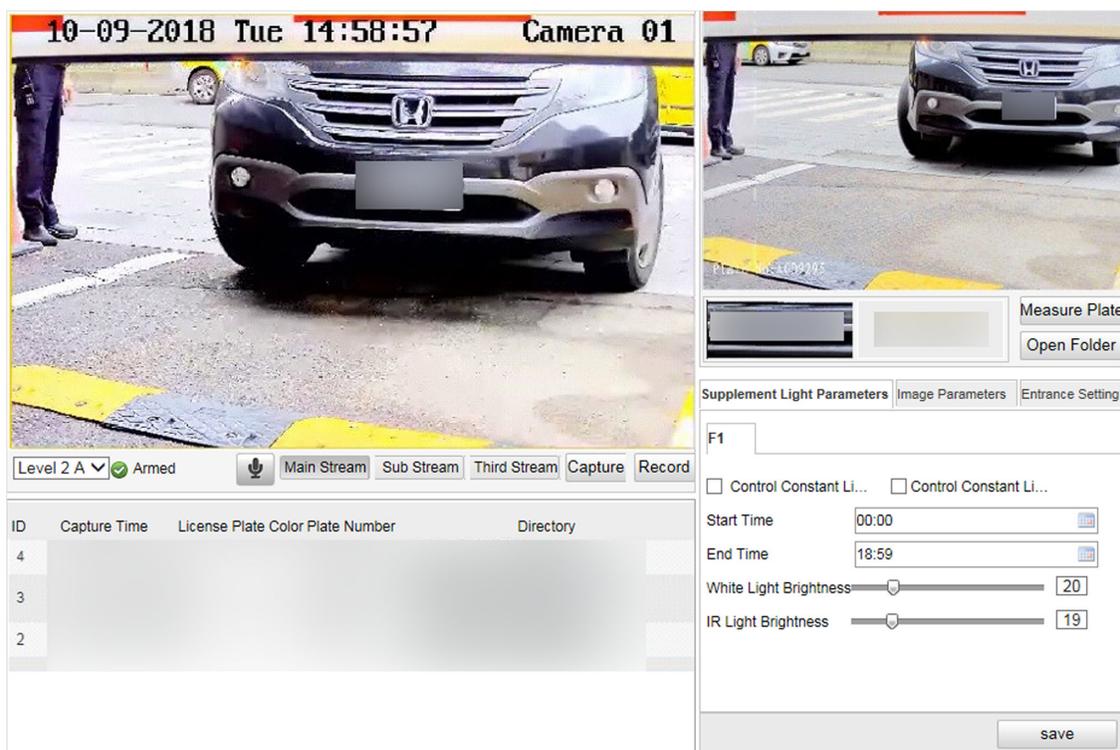
---

## Note

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

---

1. Click **Real-Time Picture**.
2. Select an item from the list, and you can view the capture scene picture and license plate picture.



**Figure 3-8 Real-Time Picture**

3. You can do the following operations on this interface.

- Select the arming mode. **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.
- Select the stream type. **Main Stream** is the HD stream, mainly used for record. **Sub-Stream** is the SD stream, mainly used for network transmission to save the bandwidth. **Third Stream**, independent from the main stream and sub-stream, is used for network transmission, and you can set different resolutions and bit rates.
- Click **Capture** to enable manual capture. The captured pictures will be saved in the set local path. Or you can click **Open Folder** to view the pictures.
- Click **Record** to enable manual record. The recorded videos will be saved in the set local path.
- If the computer and the device support built-in audio or have connected to an audio device, you can click to start two-way audio between the device and the computer.

**Note**

Some models do not support two-way audio. The actual device prevails.

- Click **Measure Plate** to measure the license plate pixel. After the measurement, click **Disable**.

- For the supplement light parameters settings, refer to "Set Flash Light Parameters" for details. For the image parameters settings, refer to "Set Video Parameters" for details. For the entrance settings, refer to "Set Barrier Gate Linkage" for details.

## 3.4 Search Picture

You can search the captured pictures stored in the storage card and export the pictures you need.

### Before You Start

Install the storage card, and ensure the storage status is normal.

### Steps

1. Click **Picture**.
2. Set the search conditions such as **Lane No.**, **Vehicle Type**, etc.



### Note

The search conditions vary with different models. The actual device prevails.

3. Click **Search**.

No.	File Name	File Date	File Size	Live View	Progress
1	20200411201119_000493_00_00_SC_D1	2020-04-11 20:11:19	259 KB		
2	20200411201119_000489_00_00_SC_D1	2020-04-11 20:11:19	208 KB		
3	20200411201119_000486_00_00_SC_D1	2020-04-11 20:11:19	161 KB		
4	20200411201119_000483_00_00_SC_D1	2020-04-11 20:11:19	137 KB		
5	20200411201121_000498_00_00_SC_D1	2020-04-11 20:11:21	259 KB		
6	20200411201122_000503_00_00_SC_D1	2020-04-11 20:11:22	259 KB		
7	20200411201122_000508_00_00_SC_D1	2020-04-11 20:11:22	259 KB		
8	20200411201122_000513_00_00_SC_D1	2020-04-11 20:11:22	259 KB		

**Figure 3-9 Search Picture**

The searched pictures information will be displayed in the picture list.

---

### **Note**

If you have set level 1 arming for the device, the captured pictures will not be saved in the storage card. Go to the saving path of scene pictures to view them. You can go to **Configuration → Local Configuration** to get the saving path.

---

**4. Optional:** Click  to preview the selected picture.

You can view the captured picture and the related information such as the capture time, lane No., license plate number, etc.

**5. Optional:** Check a picture or several pictures and click **Export Picture** to export it/them to the saving path you have set.

The downloaded picture(s) will be marked as "Downloaded". You can go to **Configuration → Local Configuration** to get the saving path of downloaded 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** → **Device Configuration** → **Entrances and Exits** → **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, check **Time Settings**, and set the effective start time and end time.
  - 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.

**Search List**

Filter by  Keywords

**Delete List**

Delete Type  Keywords

No.	License Plate Number	Belong to	Card No.	Effective Start Time	Effective End Time
1		Blocklist			
2		Allowlist			
3		Blocklist			
4		Allowlist			
5		Blocklist			
6		Allowlist			
7		Blocklist			
8		Allowlist			
9		Blocklist			
10		Allowlist			

Total 4897 Items [First Page](#) [Prev Page](#) 1/490 [Next Page](#) [Last Page](#)

**Figure 4-1 Set Allowlist and Blocklist**

3. You can search, modify, delete, import, or export 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**. Modify the information, and click **OK**.
- Delete**    Select the deleting type, or enter the keywords. Click **Delete**.
- 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  to select the edited template.  
               f. Click **Import** to import the information to the device.
- Export**    Click **Export** and select the saving path to export the allowlist or blocklist to the computer.

## 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** → **Device Configuration** → **Entrances and Exits** → **Entrance and Exit** .

Control Mode By Camera ▼

Keep Barrier Open for Following Vehicle Disable ▼

Lock Barrier Gate for Large-Sized Vehicle

**Relay**

Relay No.	Relay Function
1	Open ▼
2	Close ▼

**Vehicle Information Management**

Vehicle Type	Barrier Gate Operation	Alarm Operation
Temporary Vehicle	<input checked="" type="radio"/> No Operation <input type="radio"/> Open Barrier Gate	<input type="checkbox"/> Upload via SDK <input type="checkbox"/> Upload to Alarm Host
Vehicle in Blocklist	<input checked="" type="radio"/> No Operation <input type="radio"/> Open Barrier Gate	<input type="checkbox"/> Upload via SDK <input type="checkbox"/> Upload to Alarm Host
Vehicle in Allowlist	<input checked="" type="radio"/> No Operation <input type="radio"/> Open Barrier Gate	<input type="checkbox"/> Upload via SDK <input type="checkbox"/> Upload to Alarm Host

**Remote Control Barrier Gate**

Barrier Gate No.	Operation	Barrier Gate Status
1	<input type="button" value="Close"/> <input type="button" value="Open"/> <input type="button" value="Unlock"/> <input type="button" value="Lock"/>	Check if the rising or falling to position signal of the barrier gate is connected or not.

**Figure 4-2 Control Barrier Gate**

2. Select **Control Mode**.

#### By Camera

The barrier gate is controlled via the license plates recognized by the capture camera.

#### By Platform

The barrier gate is controlled via the platform which is connected to the capture camera.

---

#### **Note**

Connect the capture camera to the platform if you want to control the barrier gate by platform. It is recommended to select this mode.

3. Enable or disable the function of keeping barrier open for following vehicles.
4. **Optional:** Check **Lock Barrier Gate for Large-Sized Vehicle**.

---

### **Note**

Some models do not support this function. The actual device prevails.

---

5. 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.

---

6. Set the barrier gate operation and alarm operation for the temporary vehicles, vehicles in the blacklist, and vehicles in the allowlist.
    - Check **Upload via SDK** to arm and upload the vehicle information to the arming terminal via SDK.
    - If the device has been connected to the alarm device, check **Upload via Alarm Host**. When the barrier gate is open, the alarm device will be triggered to alarm.
  7. **Optional:** You can click the corresponding buttons to control the barrier gate remotely.
- 

### **Note**

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

---

8. Click **Save**.
- 

## 4.2 Set LCD

When the device is connected with a LCD, or equipped with a LCD, set the LCD parameters.

### **Before You Start**

If you want to play the media files, prepare the media files in the format of PNG, JPG, JPEG, BMP, or MP4. Ensure the size of a single file is smaller than 512 M.

### **Steps**

1. Go to **Configuration → Device Configuration → Entrances and Exits → LCD Settings** .

Control Mode  ▼

Time Format  ▼

Idle Title List

Row 1

Row 2

Passing Vehicle Title List

Row 1

Custom Content List

Row 1

Font Size  50

Fan Speed  ▼

Display Duration(s)

Software Version

Display Free Space

Enable Screen Brightness

Screen Brightness  0

Adjust by Period

No.	Start Time	End Time	Screen Brightness
1	<input type="text" value="11:00"/>	<input type="text" value="19:00"/>	<input type="range" value="0"/> 0

Loop Display Duration(s)  60

Loop Play Sequence

No.	Media File Name
-----	-----------------

**Figure 4-3 Set LCD**

**2. Select Control Mode and Time Format.**

**3. Set the display content.**

- 1) Click + to add a row of idle title, passing vehicle title, or custom content according to your needs.
- 2) Edit the content in the text filed of the corresponding row.
- 3) **Optional:** Click - to delete the row from the bottom to the top.
- 4) Set **Font Size** and **Display Duration**.

**Display Duration**

The duration from the end of displaying passing vehicle information to the start of displaying idle information.

**4. Optional:** If the device has been connected to the platform, you can check **Display Free Space** to display the number of the free parking spaces.

**5. Optional:** Set the screen brightness.

**Set the same brightness for the whole period**

For the scenes with stable brightness, you can check **Enable Screen Brightness**, and adjust **Screen Brightness**.

**Set different brightness for different periods**

- a. Check **Enable Screen Brightness**.
- b. Check **Adjust by Period**.
- c. Click **Add** one by one to add different time periods.
- d. Set **Start Time**, **End Time**, and **Screen Brightness** for different periods.

 **Note**

- You can click **Delete** to delete the time period from the bottom to the top.
- For the time period(s) out of the set period(s), the screen will keep the brightness set for the whole period.

**6. Optional:** Set the media files to be displayed on the screen.

- 1) Click **Import Media**.
- 2) Click **Browse** to select the media file.

---

 **Note**

If importing failed, try to disable the upload path of the browser.

- 3) Click **Import**.
- 4) If you want to display pictures in cycle, set **Loop Display Duration** to control the display duration of each picture.
- 5) Check the imported medium one by one to set **Loop Play Sequence**.

---

 **Note**

The medium checked first will be played in priority. All the media will be played one by one according to the set sequence.

- 6) **Optional:** Delete or search the imported media.

**Delete Single Medium**

Select a file, and click **Delete Single Medium**.

**Delete All Media**

Click **Delete All Media** to clear all the imported media.

**Search Media**

Reserved.

**7. Click Save.**

## 4.3 Set Serial Port

### 4.3.1 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

1. Go to **Configuration → Device Configuration → System Configuration → Serial Ports** .

RS-485 Parameters						
RS-485 No.	Baud Rate	Data Bit	Stop Bit	Parity	Flow Ctrl	Working Mode
1	38400	8	1	None	None	Application Mode Trigger

**Figure 4-4 Set RS-485**

2. Set **Baud Rate, Data Bit, Stop Bit**, etc.



#### Note

The parameters should be same with those of the connected device.

3. Select **Working Mode**.

#### Application Mode Trigger

Select it if the vehicle detector has been connected via the RS-485 serial port.

#### Transparent Transmission

Select it, and the network command can be transmitted to RS-485 control command via the RS-485 serial port.

#### LED Display

Select it when the LED display is connected to the device via RS-485 serial port.

4. Click **Save**.

### 4.3.2 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 corresponding device has been connected via the RS-232 serial port.

## Steps

1. Go to **Configuration → Device Configuration → System Configuration → Serial Ports**.
2. Click **Advanced Settings**.

RS-232 Parameters	
Baud Rate	115200 bps
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
Working Mode	Console

[Advanced Settings](#)

Figure 4-5 Set RS-232

3. Set **Baud Rate, Data Bit, Stop Bit**, etc.

---

### Note

The parameters should be same with those of the connected device.

---

4. Select **Working 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 Band**

Reserved.

5. Click **Save**.

## Chapter 5 Network Configuration

### 5.1 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** → **Device Configuration** → **System Configuration** → **Network Parameters** for parameter settings.

NIC Settings	
NIC Type	10M/100M/1000M Self-adaptive
<input type="checkbox"/> DHCP	
IPv4 Address	10.10.113.241
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.10.113.254
IPv6 Mode	DHCP
IPv6 Address	
IPv6 Default Gateway	::
IPv6 Subnet Mask	
Mac Address	54:c4:15:fb:c2:1c
MTU	1500
Multicast Address	

Figure 5-1 Set IP Address

#### NIC Type

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

#### IPv4

Two IPv4 modes are available.

#### DHCP

The device automatically gets the IPv4 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 IPv4 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 Default 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

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 Server** properly if needed.

## 5.2 Connect to Platform

### 5.2.1 Connect to ISUP Platform

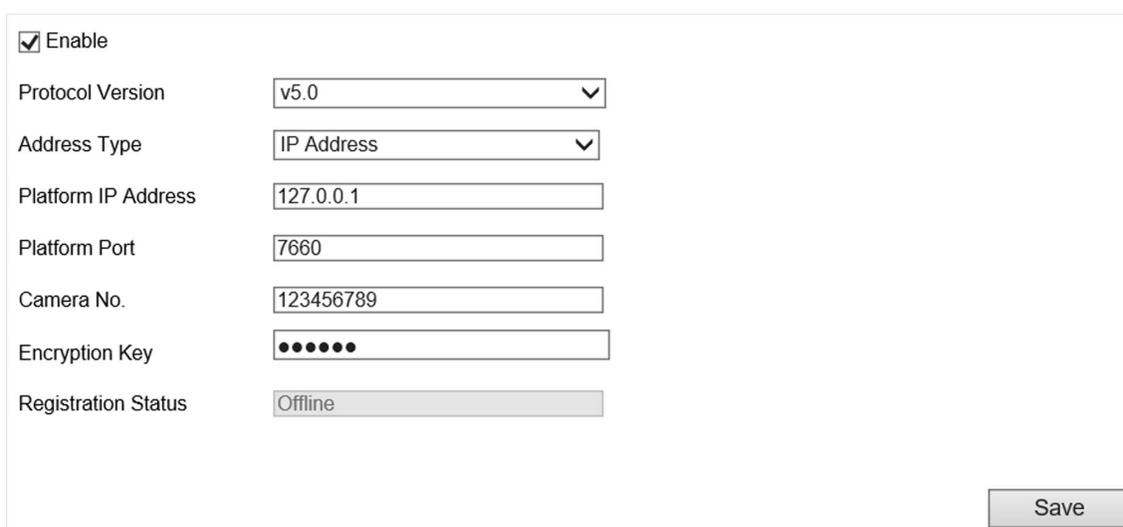
ISUP (EHome) is a platform access protocol. The device can be remotely accessed via this platform.

#### Before You Start

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

#### Steps

1. Go to **Configuration** → **Device Configuration** → **System Configuration** → **ISUP** .



<input checked="" type="checkbox"/> Enable	
Protocol Version	v5.0
Address Type	IP Address
Platform IP Address	127.0.0.1
Platform Port	7660
Camera No.	123456789
Encryption Key	••••••
Registration Status	Offline

Save

Figure 5-2 Connect to ISUP Platform

2. Check **Enable**.
3. Select **Protocol Version**.
4. Select **Address Type**.
5. Enter **Platform IP Address**, **Platform Port**, and **Camera No.**

---

#### Note

The camera No. should be the same with the added one on the ISUP platform.

---

6. **Optional:** Enter **Encryption Key** if you select **v5.0**.
7. Click **Save**.
8. **Optional:** View **Registration 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.

## 5.2.2 Connect to Guarding Vision

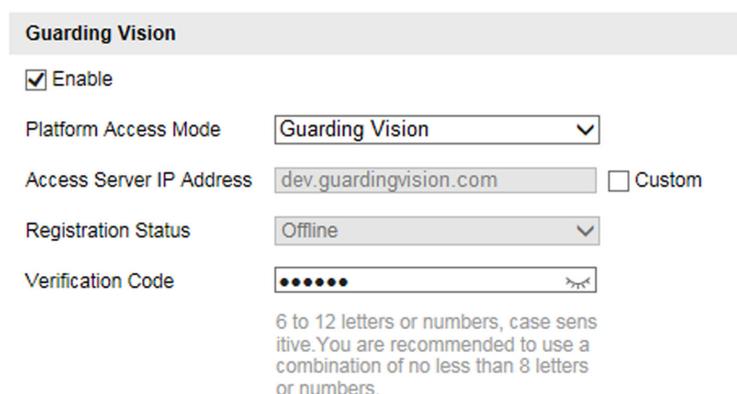
The device can be remotely accessed via Guarding Vision.

### Before You Start

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

### Steps

1. Go to **Configuration** → **Device Configuration** → **System Configuration** → **Guarding Vision** .
2. Check **Enable**.



**Guarding Vision**

Enable

Platform Access Mode

Access Server IP Address   Custom

Registration Status

Verification Code

6 to 12 letters or numbers, case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

**Figure 5-3 Connect to Guarding Vision**

3. Enter a customized **Verification Code**. You need to enter the code when adding the device in Guarding Vision.

---

 **Caution**

Valid security code range [6-12]. You are recommended to use an eight-bit or above combination of numbers, lowercase, and uppercase for the code.

4. Click **Save**.
5. Get Guarding Vision application from the following ways.
  - For computer user: Visit [dev.guardingvision.com](http://dev.guardingvision.com) .
  - For mobile phone user: Download Guarding Vision in App Store (iOS system) or Google Play™ (Android system).
6. Register an account and add the device to Guarding Vision.

---

 **Note**

Refer to the user manual of Guarding Vision for details.

---

## 5.3 Set DDNS

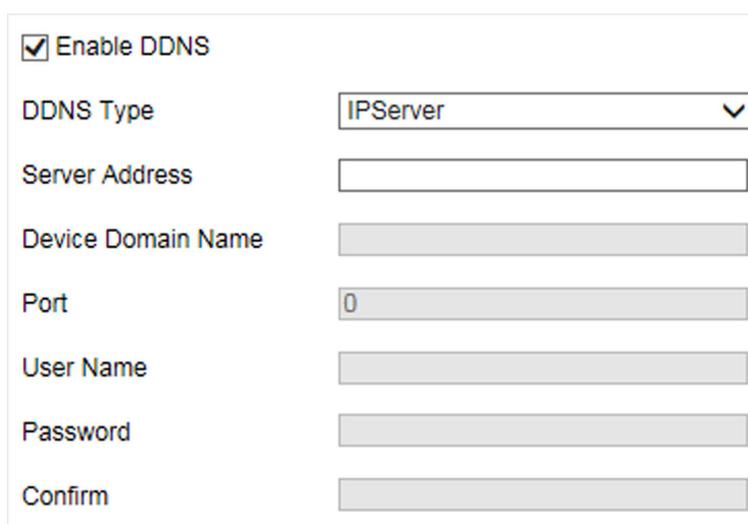
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

### 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 "Set IP Address" for details.
- Complete port mapping. The default port is 80, 8000, and 554.

### Steps

1. Go to **Configuration → Device Configuration → System Configuration → DDNS** .



<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	IPServer
Server Address	
Device Domain Name	
Port	0
User Name	
Password	
Confirm	

Figure 5-4 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.

## 5.4 Set IEEE 802.1X

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN/WLAN. When devices connect to the network with IEEE 802.1X standard, the authentication is needed.

### Steps

---



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

---

1. Go to **Configuration** → **Device Configuration** → **System Configuration** → **802.1X** .

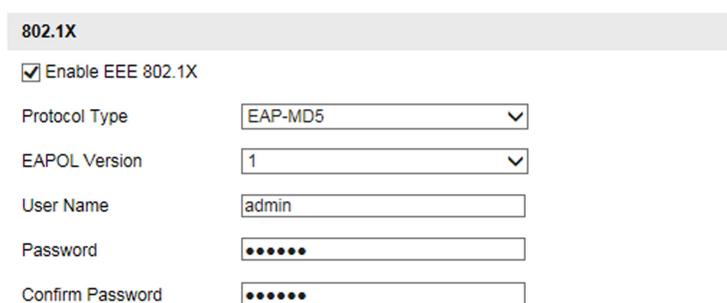


Figure 5-5 Set IEEE 802.1X

2. Check **Enable IEEE 802.1X**.
3. Select **Protocol Type** and **EAPOL Version**.

#### Protocol Type

If you use **EAP-MD5**, the authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Enter the user name and password for authentication.

#### EAPOL Version

The EAPOL version must be identical with that of the router or the switch.

4. Enter **User Name** and **Password** registered in the server.
5. Confirm the password.
6. Click **Save**.

## 5.5 Set Port

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

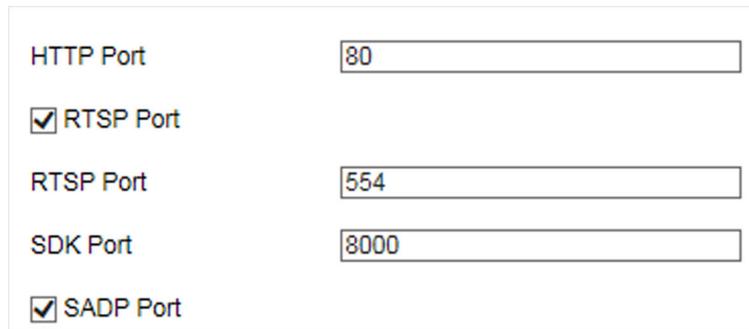
---



Do not modify the default port parameters at will, otherwise the device may be inaccessible.

---

Go to **Configuration** → **Device Configuration** → **System Configuration** → **Port** for port settings.



The screenshot shows a configuration window with the following settings:

HTTP Port	<input type="text" value="80"/>
<input checked="" type="checkbox"/> RTSP Port	
RTSP Port	<input type="text" value="554"/>
SDK Port	<input type="text" value="8000"/>
<input checked="" type="checkbox"/> SADP Port	

**Figure 5-6 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.

### **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.

## Chapter 6 Record

### 6.1 Set Storage Path

#### 6.1.1 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 → Device Configuration → Encoding and Storage → Storage Management**.

HDD No.	Capacity	Free space	Status	Type	Property	Progress
1	14.73GB	12.62GB	Normal	Local	R/W	

Auto-Initialize Redundant Storage  
 Auto-Upload Data in Redundant Storage

**HDD Quota**

Picture Capability:  MB  
 Video Capability:  MB  
 Capture Quota Ratio:  %  
 Video Quota Ratio:  %

Figure 6-1 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**.
  4. Click **Save**.

## 6.1.2 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** → **Device Configuration** → **Encoding and Storage** → **FTP** .

The screenshot shows the 'Upload to FTP' configuration interface. It includes a checked checkbox for 'Upload Additional Information to FTP'. The 'Enable FTP' section is set to 'Enable One'. Under the 'FTP1' section, the 'Server Address' is '192.168.1.201', 'Port' is '21', 'User Name' is 'test', and 'Password' and 'Confirm' are masked. Directory settings include 'Directory Structure' set to 'Save in Root Dire', and 'Parent Directory', 'Level 2 Directory', 'Level 3 Directory', and 'Level 4 Directory' all set to 'None'. There is also a 'Not Upload Plate Close-up' checkbox and a 'Test' button.

Figure 6-2 Set FTP

2. **Optional:** Check **Upload Additional Information to FTP**, and then the related information can be attached when uploading.
3. Enable the FTP server.
4. Set FTP parameters.
  - 1) Enter **Server Address** and **Port**.
  - 2) Enter **User Name** and **Password**, and confirm the password.
  - 3) Select **Directory Structure**.

---

### Note

If multiple directories are needed, you can customize the directory name.

5. **Optional:** Check **Not Upload Plate Close-up** if the license plate close-up pictures are not needed to upload.
6. Set the name rule and separator according to the actual needs.
7. **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.
8. Click **Save**.

### 6.1.3 Set Listening Host

The listening host 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 listening host, and the network communication with the device is normal.

#### Steps

1. Go to **Configuration → Device Configuration → System Configuration → Network Parameters** .

ANPR IP Address/Domain:	<input type="text" value="0.0.0.0"/>
ANPR Port:	<input type="text" value="80"/>
Listening Host IP Address:	<input type="text" value="0.0.0.0"/>
Listening Host Port:	<input type="text" value="7200"/>
Enable Picture Uploading ...	<input type="checkbox"/>

**Figure 6-3 Set Listening Host**

2. Set **ANPR IP Address/Domain** and **ANPR Port** if you need to upload the alarm information.
3. Set **Listening Host IP Address** and **Listening Host Port**, and check **Enable Picture Uploading Listening** if you need to upload pictures.
4. Click **Save**.

### 6.1.4 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 **Real-Time Picture**.

#### Steps

1. Go to **Configuration → Device Configuration → Encoding and Storage → Cloud Storage** .

<input type="checkbox"/> Enable	
Version	V1.0
Access Server IP Address	0.0.0.0
Port No.	6001
User Name	admin
Password	••••••
Cloud Storage ID	1
Violation Cloud Storage ID	1

**Figure 6-4 Set Cloud Storage**

2. Check **Enable**.
3. Set the server parameters.
  - 1) Select **Version**.
  - 2) Enter **Access Server IP Address** and **Port No.**
  - 3) Enter **accessKey** and **secretKey** of the resource pool.
  - 4) Enter the ID according to the storage area No. of the server.

---

 **Note**

Enter **User Name** and **Password** if you select **V1.0**.

---

4. Click **Save**.

## 6.2 Set Quota

Set the video and picture ratio in the storage.

### Before You Start

Install the memory card.

### Steps

1. Go to **Configuration → Device Configuration → Encoding and Storage → Storage Management**.
  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.

## 6.3 Set Record Schedule

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

### Before You Start

Install the memory card, and you are recommended to set the video quota ratio as not 0.

### Steps

1. Go to **Configuration → Device Configuration → Encoding and Storage → Record Schedule** .

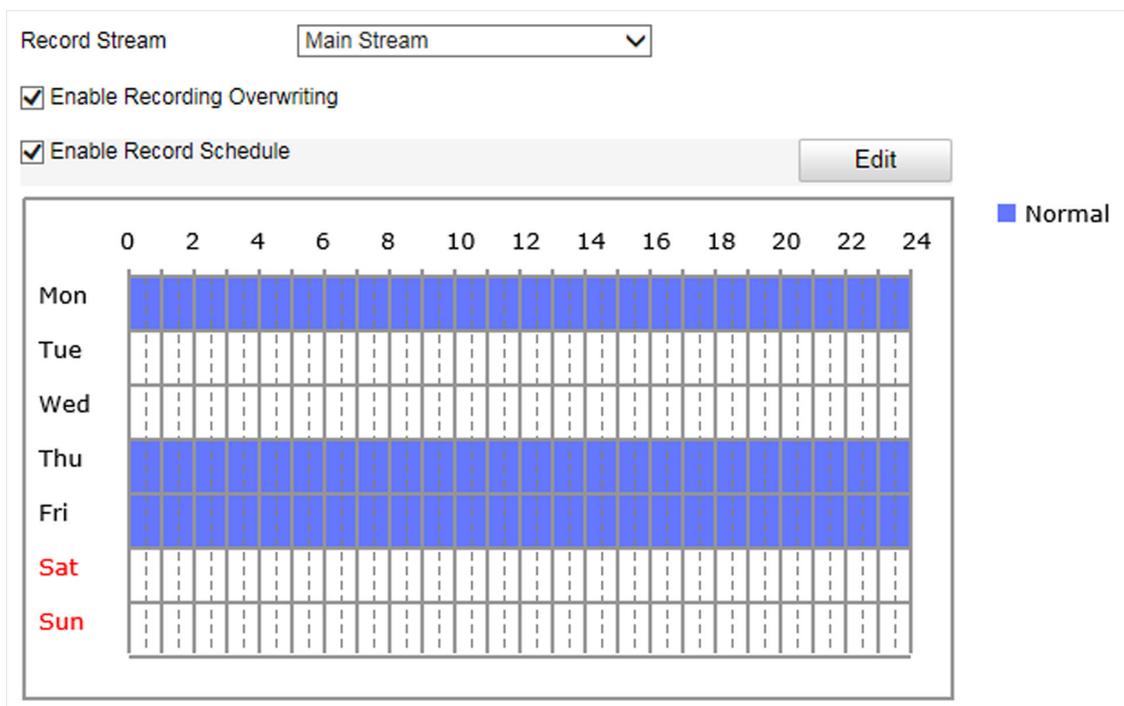


Figure 6-5 Set Record Schedule

2. **Optional:** Check **Enable Recording Overwriting**.

When the storage is full, the earliest videos will be overwritten.

3. Check **Enable Record Schedule**.

4. Click **Edit** to edit the record schedule.

- 1) Select **Customize**.

- 2) Set the start time and end time.

- 3) **Optional:** Select the other days and click **Copy** to copy the settings to other days.

- 4) Click **OK**.

5. Click **Save**.

## 6.4 Local Configuration

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

Live View Parameters			
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	
Live View Performance	<input type="radio"/> Least Delay	<input type="radio"/> Balanced	<input checked="" type="radio"/> Best Fluency
Rule Information	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Feature Information	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	

Record File Settings			
Record File Size	<input type="radio"/> 256M	<input checked="" type="radio"/> 512M	<input type="radio"/> 1G
Save record files to	<input type="text" value="D:\"/>		<input type="button" value="Browse"/>

Picture and Clip Settings			
Save snapshots in live view to	<input type="text" value="D:\"/>		<input type="button" value="Browse"/>
Save downloaded pictures to	<input type="text" value="D:\"/>		<input type="button" value="Browse"/>
Save scene picture to	<input type="text" value="D:\"/>		<input type="button" value="Browse"/>

**Figure 6-6 Local Configuration**

### Protocol

Select the network transmission protocol according to the actual needs.

#### TCP

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

#### UDP

Provides real-time audio and video streams.

### Live View Performance

#### Least Delay

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

#### Balanced

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

#### Best Fluency

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

### Rule Information

Reserved.

### **Feature Information**

Reserved.

### **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 for the manually recorded video 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 for the downloaded pictures.

### **Save scene picture to**

Set the saving path of the captured pictures in **Real-Time Picture** interface.



### **Note**

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

---

## Chapter 7 Encoding and Display

### 7.1 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

1. Go to **Configuration → Device Configuration → Encoding and Storage → 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**.

## 7.2 Set Image Parameters

You can adjust the image parameters to get clear image.

### Steps

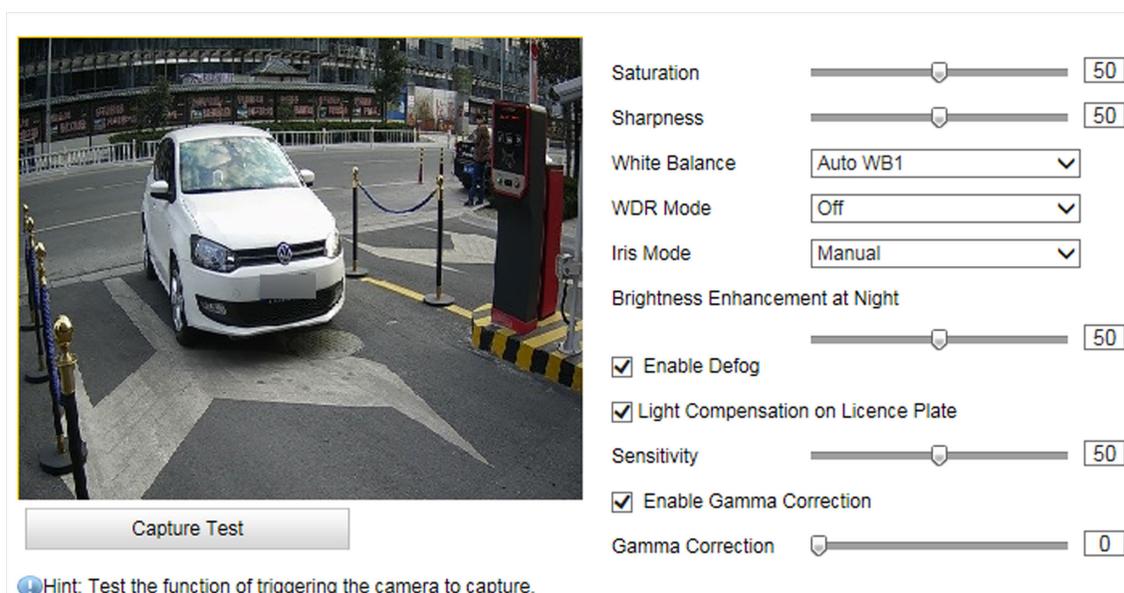


#### Note

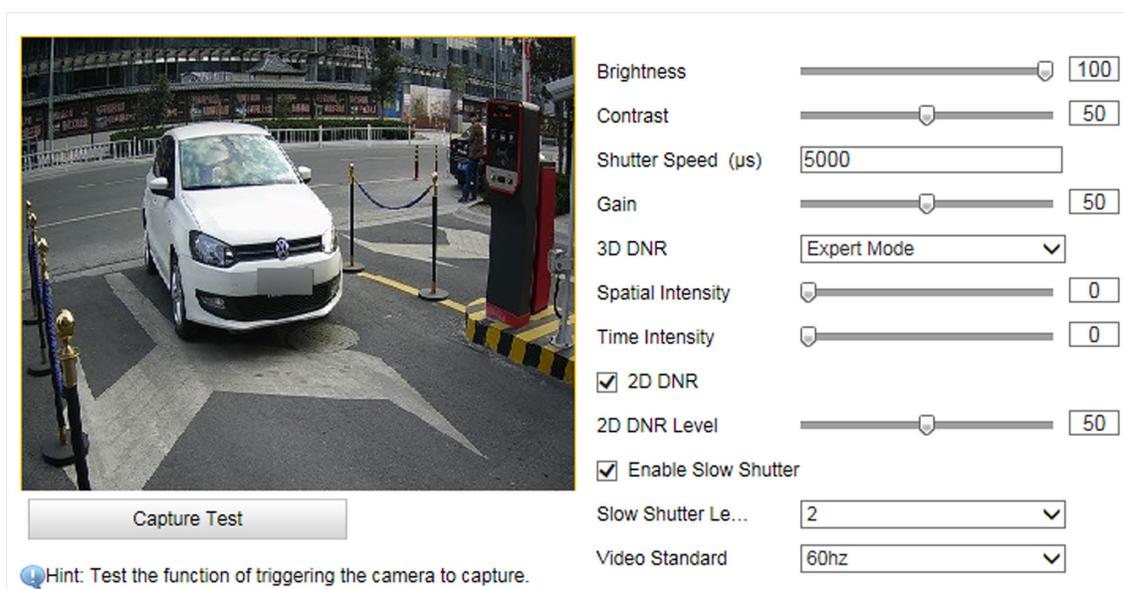
The supported parameters may vary with different models. The actual device prevails.

---

1. Go to **Configuration** → **Device Configuration** → **Image Parameters** → **General Parameters** / **Configuration** → **Device Configuration** → **Image Parameters** → **Video** .



**Figure 7-1 Set General Parameters**



**Figure 7-2 Set Video Image Parameters**

## 2. Adjust the parameters.

### 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 time.

#### **Brightness**

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

### **Iris Mode**

In **Auto** mode, the iris can adjust automatically according to the current light strength. In **Manual** mode, you need to adjust the iris manually.

### **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 light compensation on license plates 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.

### **Brightness**

It refers to the max. brightness of the image.

### **Contrast**

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

### **Shutter Speed**

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 special intensity is too high, the outline of the image may become fuzzy and the details may lose. If the time 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.

### Enable Slow Shutter

You can enable slow shutter to increase the exposure time and raise the photosensitivity. Then the image brightness can be raised in low illumination conditions.

### Video Standard

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

## 7.3 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** → **Device Configuration** → **Image Parameters** → **ICR**.
2. Select **ICR Mode**.

<b>Auto-switch</b>	Switches to ICR mode automatically at night or in dark light conditions.
<b>Manual Switch</b>	Switches to the day or night manually.
<b>Scheduled Switch</b>	Set day/night mode, start time, and end time to switch to ICR mode only during the set time period.
<b>Do not switch</b>	Disable ICR mode.

3. Click **Save**.

## 7.4 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** → **Device Configuration** → **Encoding and Storage** → **ROI** .

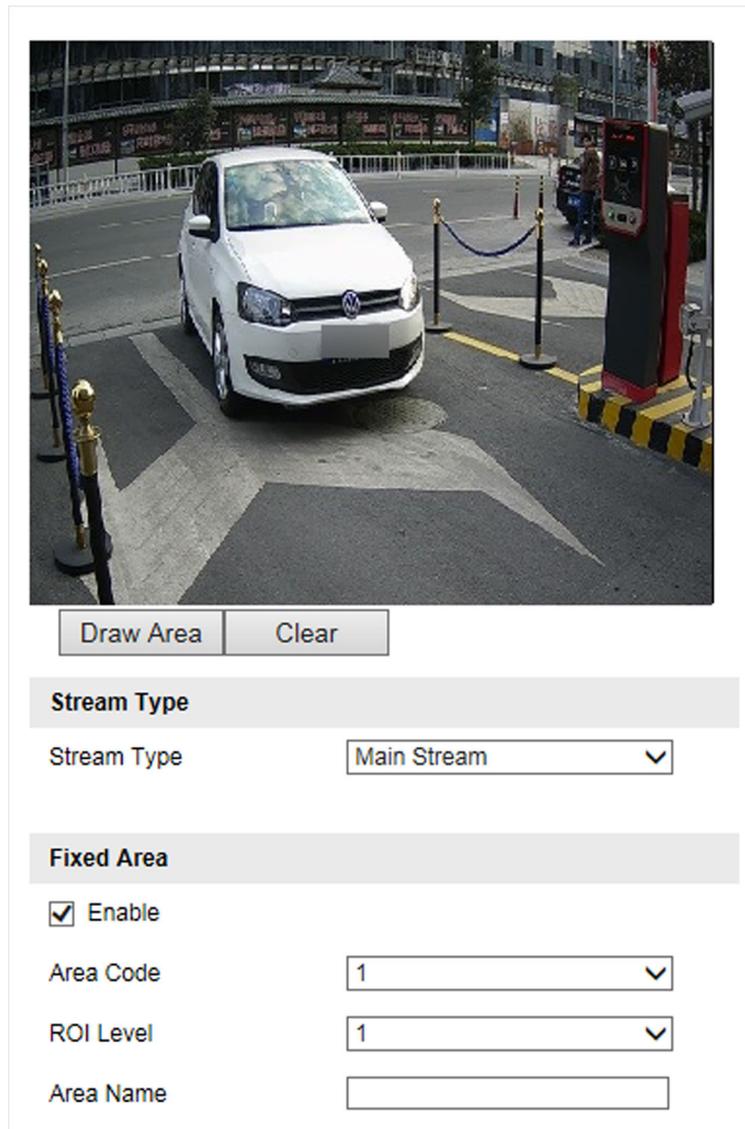


Figure 7-3 Set ROI

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.

## 7.5 Set OSD

You can customize OSD information on the live view.

### Steps

1. Go to **Configuration → Device Configuration → Text Overlay → OSD Settings**.

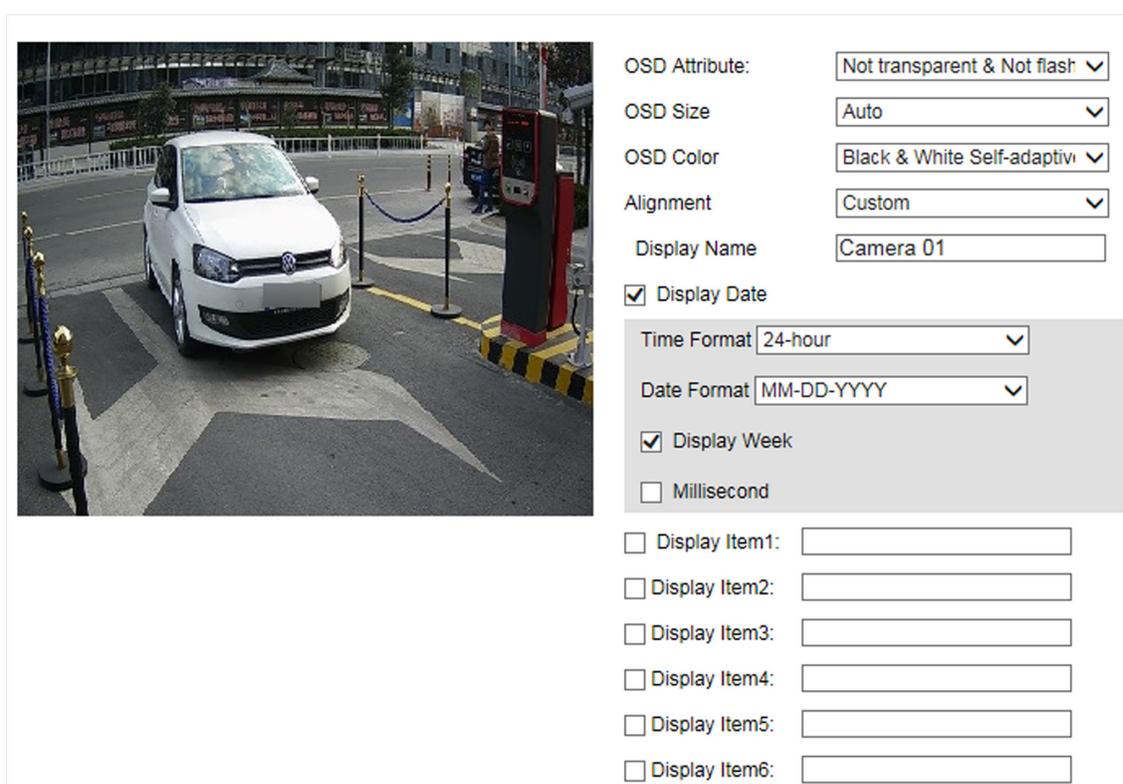


Figure 7-4 Set OSD

2. Set OSD attribute, size, color, etc.



### Note

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

3. Set the display content.
  - 1) Enter **Display Name**.
  - 2) Check **Display Date**, and set the time and date format.
  - 3) Check **Display Week** or **Millisecond**.
4. **Optional:** Check the display item(s) and enter the information in the text field(s).
5. Drag the red frames on the live view image to adjust the OSD positions.
6. Click **Save**.

### **Result**

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

## Chapter 8 Safety Management

### 8.1 Manage User

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

#### Steps

1. Go to **Configuration → Device Configuration → User Management** .
2. Add a user.
  - 1) Click **Add**.
  - 2) Enter **User Name** and select **Level**.
  - 3) Enter **Admin Password**, **Password**, and confirm the password.



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**.



The administrator can add up to 31 user accounts.

- 
3. You can do the following operations.
    - Select a user and click **Modify** to change the password and permission.
    - Select a user and click **Delete** to delete the user.

### 8.2 Set IP Address Filtering

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

#### Steps

1. Go to **Configuration → Device Configuration → System Configuration → Service** .
2. Check **Enable IP Address Filtering**.

### 3. Set **Filtering Mode**.

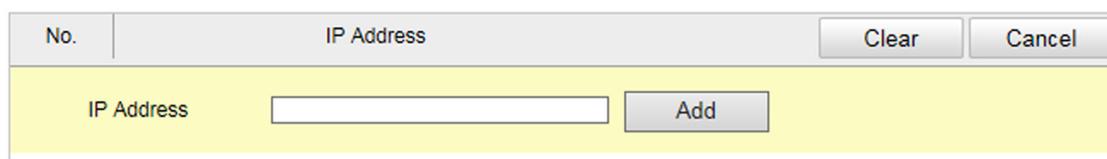
#### **Blocklist Mode**

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 **Add**.



No.	IP Address
-----	------------

Clear Cancel

IP Address  Add

**Figure 8-1 Set IP Address Filtering**

### 5. **Optional**: Edit, delete, or clear the added IP addresses.

### 6. Click **Save**.

## 8.3 Enable User Lock

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

#### **Steps**

1. Go to **Configuration → Device Configuration → System Configuration → Service** .
2. Check **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.

## 8.4 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 → Device Configuration → System Configuration → Service** .
2. Uncheck **Enable SSH Service**.
3. Click **Save**.

### 8.5 Set HTTPS

#### 8.5.1 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 → Device Configuration → System Configuration → HTTPS**.
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region, Hostname/IP, Validity**, and other parameters.
5. Click **OK**.

##### Result

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

#### 8.5.2 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 → Device Configuration → System Configuration → 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**.

## Chapter 9 Maintenance

### 9.1 View Device Information

#### Basic Information and Algorithms Library Version

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

### 9.2 Log

#### 9.2.1 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** → **Device Configuration** → **System Configuration** → **Service** .
2. Check **Enable System Log Service**.
3. Enter **IP Address** and **Port No.** of the log server.
4. Click **Save**.

##### Result

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

#### 9.2.2 Search Log

Log helps to locate and troubleshoot problems.

##### Steps

1. Click **Log**.
2. Set search conditions.

### 3. Click **Search**.

The matched log files will be displayed on the log list.

### 4. **Optional**: Click **Save Log** to save the log files to your computer.

## 9.3 Upgrade

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

### Before You Start

Prepare the upgrade file.

### Steps

1. Go to **Configuration → Device Configuration → System 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.

## 9.4 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 → Device Configuration → System Maintenance → Reboot** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

## 9.5 Restore Parameters

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

### Steps

1. Go to **Configuration → Device Configuration → System Maintenance → Default** .
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**.

### 9.6 Synchronize Time

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

#### Steps

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

#### NTP Synchronization

Select it to synchronize the device time with that of the NTP server. Set **Server Address**, **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**.

### 9.7 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 → Device Configuration → System Configuration → DST** .
2. Check **Enable DST**.

3. Set **Start Time**, **End Time**, and **DST Bias**.
4. Click **Save**.

### 9.8 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** → **Device Configuration** → **System Maintenance** → **Export Parameters** .
2. Click **Export Parameters**.
3. Set a password, and click **OK**.



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**.

### 9.9 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



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

1. Go to **Configuration** → **Device Configuration** → **System Maintenance** → **Import Config. File** .
2. Select **Importing Method**.



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

3. Click **Browse** to select the configuration file.
4. Enter the password of the device from which the configuration file is exported, and click **OK**.
5. Click **Import**.
6. Enter the admin password, and click **OK**.

#### Result

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

### 9.10 Export Debug File

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

#### Steps

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

## Appendix A. Communication Matrix and Device Command

Scan the QR code below to get the communication matrix of the device.



**Figure A-1 Communication Matrix**

Scan the QR code below to get the device command.



**Figure A-2 Device Command**

