



Smart On-Street ANPR 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

Smart On-Street ANPR 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






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

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
 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.

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.
- The power source should meet limited power source or PS2 requirements according to IEC 60950-1 or IEC 62368-1 standard.

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.

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.
- 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

Chapter 1 Introduction	1
1.1 Product Introduction	1
1.2 Key Feature	1
Chapter 2 Activation and Login	2
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
Chapter 3 Parking Space Detection	5
3.1 Set Parking Parameters	5
3.2 Set Parking Space Indicator	6
3.3 Set Allowlist and Blocklist	6
3.4 Set Capture Parameters	8
3.4.1 Set Flash Light Parameters	8
3.4.2 Set Picture Composition	9
3.4.3 Set Capture Overlay	10
3.4.4 Set Image Encoding Parameters	11
3.5 View Real-Time Picture	12
Chapter 4 Live View and Local Configuration	14
4.1 Live View	14
4.1.1 Start/Stop Live View	14
4.1.2 Select Image Display Mode	14
4.1.3 Select Stream Type	14
4.1.4 Capture Picture Manually	14
4.1.5 Record Manually	14

4.1.6 Enable Digital Zoom	15
4.2 Local Configuration	15
Chapter 5 Storage	17
5.1 Set FTP	17
5.2 Set Listening Host	18
5.3 Set Cloud Storage	18
Chapter 6 Encoding and Display	20
6.1 Set Video Encoding Parameters	20
6.2 Set Image Parameters	21
6.3 Set ICR	24
6.4 Set ROI	24
6.5 Set OSD	26
Chapter 7 Network Configuration	28
7.1 Set IP Address	28
7.2 Connect to ISUP Platform	30
7.3 Set DDNS	31
7.4 Set Port	31
Chapter 8 Serial Port Configuration	33
8.1 Set RS-485	33
8.2 Set RS-232	33
Chapter 9 Exception Alarm	35
Chapter 10 Safety Management	36
10.1 Manage User	36
10.2 Enable User Lock	36
10.3 Set HTTPS	37
10.3.1 Create and Install Self-signed Certificate	37
10.3.2 Install Authorized Certificate	37
10.4 Set SSH	38

Chapter 11 Maintenance	39
11.1 View Device Information	39
11.2 Enable System Log Service	39
11.3 Upgrade	39
11.4 Reboot	40
11.5 Restore Parameters	40
11.6 Synchronize Time	40
11.7 Set DST	41
11.8 Export Parameters	41
11.9 Import Configuration File	41
11.10 Export Debug File	42
Appendix A. Communication Matrix and Device Command	43

Chapter 1 Introduction

1.1 Product Introduction

Embedded with camera and radar, Smart On-Street ANPR Camera (hereinafter referred to as "device") adopts advanced deep-learning algorithm and integrates radar detection to realize the road side parking spaces capture. It supports license plate recognition and vehicle entry and exit detection.

The device supports the scenes of parallel parking, reverse parking, and pulling-in-head parking, applicable to the outdoor road side parking space management widely.

1.2 Key Feature

- Embedded with HD camera. Dual detection via video and radar.
- Adopts energy-saving LED indicator with high brightness and low consumption to indicate seven colors.
- Vehicle entry and exit detection, and license plate recognition.
- Supports short lens applicable to wider scenes.
- Supports hand-in-hand network cascade allocation.

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 client software.



Refer to the user manual of client software 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.

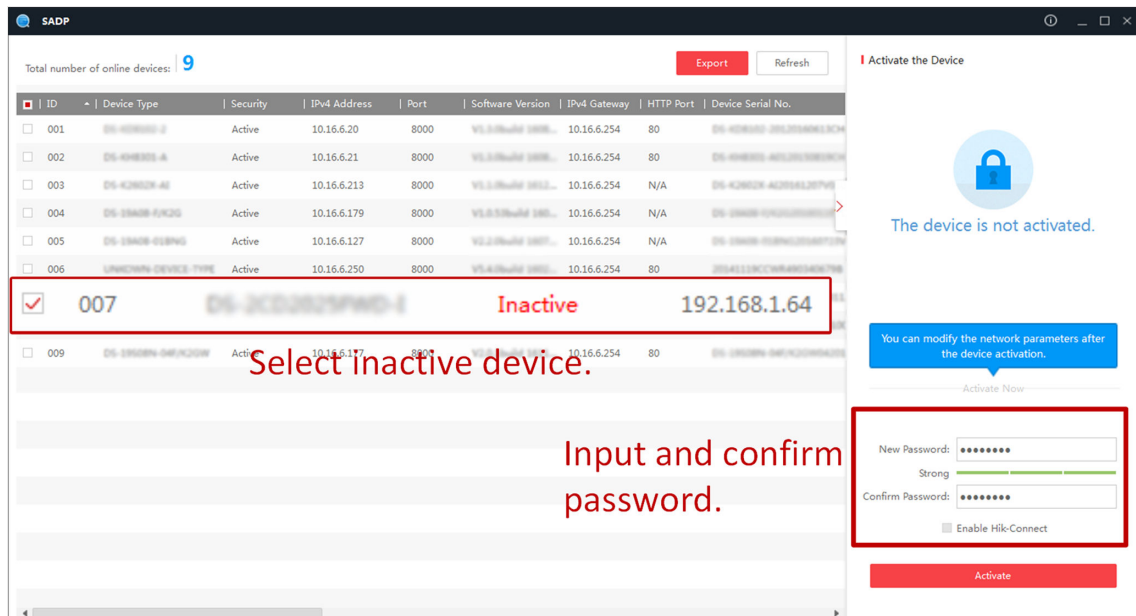


Figure 2-1 Activate via SADP

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. 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 Parking Space Detection

3.1 Set Parking Parameters

Set parking parameters to detect the parking status of the parking space, and capture license plates.

Steps

1. Go to **Configuration** → **Device Configuration** → **Smart Analysis** .

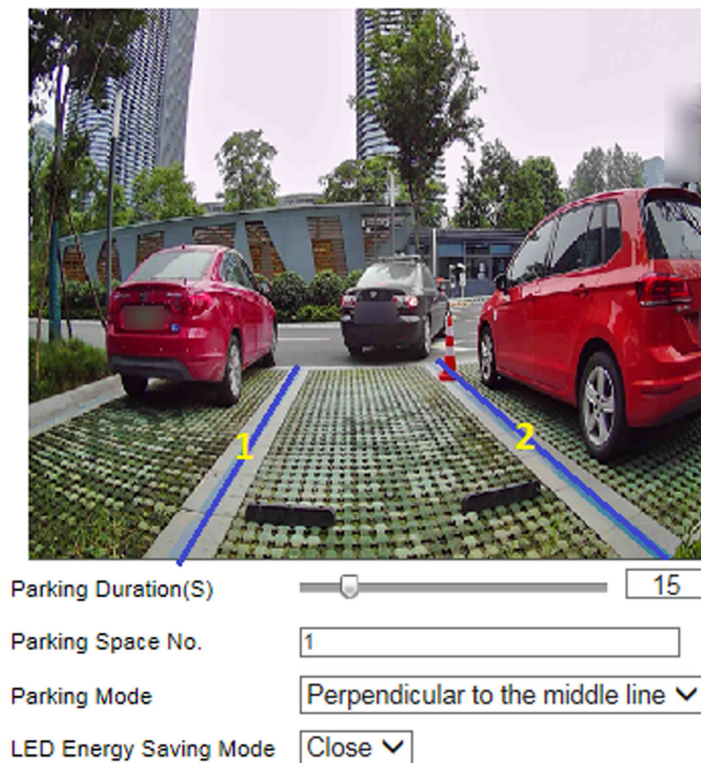


Figure 3-1 Set Parking Parameters

2. Adjust the lane lines on the live view image to make them overlap with the parking space lines in the actual scene.
3. Set the parameters below.

Parking Duration

The capture will be triggered after the set duration.

Parking Space No.

The No. will be overlaid on the captured pictures.

Parking Mode

Select the parking mode according to the actual scene.

One word parallel

Parallel parking.

Perpendicular to the middle line

Backing into a parking space or pulling in head.

LED Energy Saving Mode

It is used to control the supplement light. If you enable the mode, only when the vehicle is being parked into or driven out of the parking space, will the supplement light be enabled.

4. Click **Save**.

3.2 Set Parking Space Indicator

Set the parking space indicator to indicate different colors for different parking status.

Before You Start

Set the detection lanes of the parking space.

Steps

1. Go to **Configuration → Device Configuration → Parking Space Indicator → Parking Space Indicator** .

The screenshot shows the 'Parking Space Indicator Parameters' configuration page. It includes a dropdown for 'Indicator Control Mode' set to 'Internal Indicator'. Below is a table for 'Parking Space Status' with columns for 'Enable', 'Indicator Flicker', and 'Indicator Color'. The 'Absent' status is set to 'Yes' for enable, 'No' for flicker, and 'Green' for color. The 'Occupied' status is set to 'Yes' for enable, 'No' for flicker, and 'Red' for color. There is also a checkbox for 'Vehicle Entry Alarm' which is currently unchecked.

Parking Space Status	Enable	Indicator Flicker	Indicator Color
Absent	Yes	No	Green
Occupied	Yes	No	Red

Vehicle Entry Alarm

Figure 3-2 Set Parking Space Indicator

2. Select **Indicator Control Mode**.

3. Set **Indicator Flicker** and **Indicator Color** for different parking space status.

4. **Optional:** Check **Vehicle Entry Alarm**.

The indicator will flicker the set color for the occupied parking status when the vehicle is entering into the parking space.

5. Click **Save**.

3.3 Set Allowlist and Blocklist

You can set the parking lock linked allowlist and blocklist to control the parking.

Before You Start

- Connect the parking lock to the RS-485 interface of the device.
- Install the storage media, and ensure the storage status is normal.

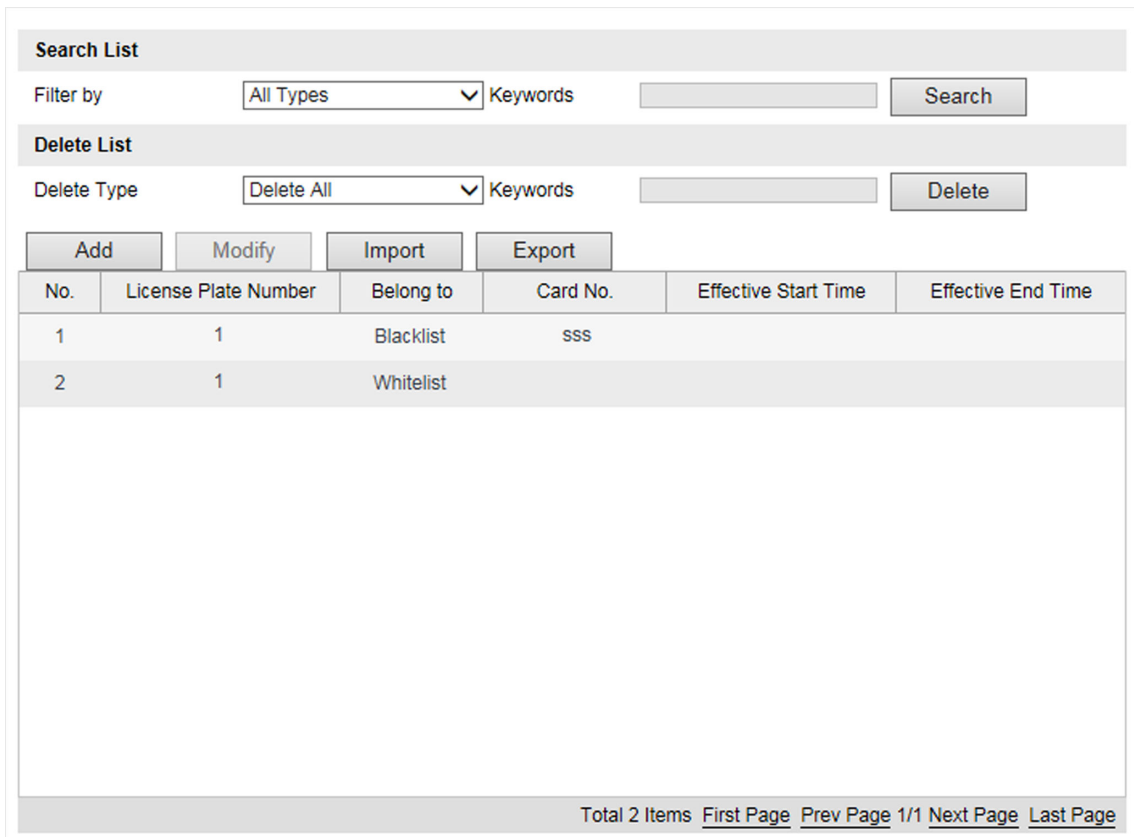
Steps

1. Go to **Configuration → Device Configuration → Capture Parameters → Blocklist/Allowlist** .
2. Add a 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 in the table.



The screenshot shows a web interface for managing vehicle lists. It includes a 'Search List' section with a dropdown for 'Filter by' (set to 'All Types') and a 'Keywords' search field. Below that is a 'Delete List' section with a dropdown for 'Delete Type' (set to 'Delete All') and a 'Keywords' search field. A row of buttons includes 'Add', 'Modify', 'Import', and 'Export'. The main part of the interface is a table with the following data:

No.	License Plate Number	Belong to	Card No.	Effective Start Time	Effective End Time
1	1	Blacklist	sss		
2	1	Whitelist			

At the bottom right of the table area, there is a summary: 'Total 2 Items' followed by navigation links: 'First Page', 'Prev Page 1/1', 'Next Page', and 'Last Page'.

Figure 3-3 Set Allowlist and Blocklist

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

- Search** Select the search type, or enter the keywords. Click **Search**. The searched vehicle information will be listed in the table.
- Edit** Select an item from the list, and click **Edit**. Edit the information, and click **OK**.
- Delete** Select the deleting type, or enter the keywords. Click **Delete**.
- Import**
- Click **Import**.
 - Click **Download Template**, and save the template.
 - Open the template, edit the information, and save it.
 - Click **Import** again.
 - Click to select the edited template.
 - Click **Import** to import the information to the device.

3.4 Set Capture Parameters

3.4.1 Set Flash Light Parameters

Flash light can enhance the image stabilization and adjust the brightness and color temperature. You can use flash light to supplement light at night or when the light is dim.

Steps



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

- Go to **Configuration** → **Device Configuration** → **Capture Parameters** → **Flash Light Parameters** .

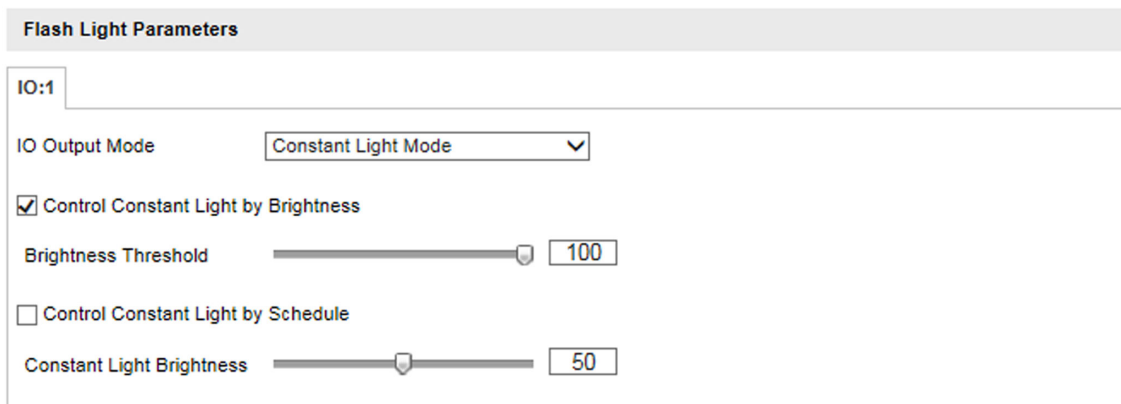


Figure 3-4 Set Flash Light Parameters

- Set constant light control mode and other parameters.
 - Check **Control Constant Light by Brightness** when you want the constant light to be controlled by detecting the surroundings brightness automatically. Set **Brightness Threshold**. The higher the threshold is, the harder the constant light can be enabled.

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

 **Note**

Controlling constant light by brightness and schedule conflict with each other.

3. Set Constant Light Brightness.

 **Note**

The higher the brightness is, the more the light will be supplemented.

4. Click Save.

3.4.2 Set Picture Composition

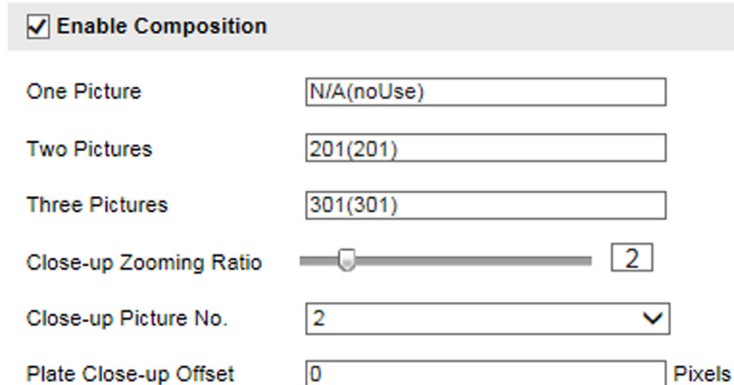
You can enable the picture composition to composite several pictures into one to make it convenient to view the violation captured pictures.

Steps

 **Note**

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

1. Go to Configuration → Device Configuration → Capture Parameters → Image Composition .



<input checked="" type="checkbox"/> Enable Composition	
One Picture	N/A(noUse)
Two Pictures	201(201)
Three Pictures	301(301)
Close-up Zooming Ratio	2
Close-up Picture No.	2
Plate Close-up Offset	0 Pixels

Figure 3-5 Set Picture Composition

- 2. Check Enable Composition.**
- 3. Set composition types for different picture quantities.**
- 4. Set other composition parameters.**

Close-up Zooming Ratio

The higher the value is, the larger the close-up is.

Close-up Picture No.

It is the picture where the close-up comes from.

Plate Close-up Offset

The default value is 0, which is recommended to be adopted. The device can capture close-up pictures according to the set offset when no license plate is recognized.

5. Click **Save**.


3.4.3 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 → Single Picture Overlay**.
2. Check **Capture Picture Overlay**.


Capture Picture Overlay



Percentage:

Font Size: ▼

Foreground Color: 

Background Color: 

Overlay on the Picture


Overlay Above the Picture

Overlay Below the Picture

Overlay Number Zeroizing

Overlay Plate Close-up

(Single Captured Picture Only)

 Hint: Test the function of triggering the camera to capture.

Overlay Information List Select All

Location: Device No.: Parking Space No.: Capture Time:

Plate No.: Parking Space Status:

Type	Overlay Information	Overlay Position	Space	Line Break Characters

Figure 3-6 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.



The overlay information may vary 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.

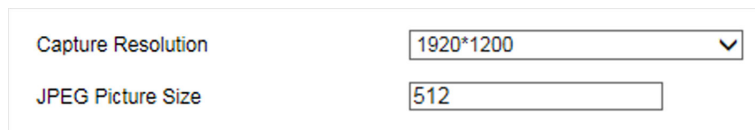
6. Click **Save**.

3.4.4 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	1920*1200
JPEG Picture Size	512

Figure 3-7 Set Image Encoding Parameters

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

3.5 View Real-Time Picture

You can view the real-time captured pictures and information of the captured vehicles.

Steps

1. Go to **Live View** → **Live Traffic Statistics** .
2. Select the captured picture from the picture list, and you can view the capture scene picture and the captured license plate picture.

The screenshot displays the real-time picture interface. On the left, there are two small images: the top one shows the rear of a red car with a blurred license plate, and the bottom one shows a close-up of the license plate. To the right is a larger scene picture showing a red car, a black car, and another red car on a street with green-paved lanes. Below the images are controls for 'Capture' and 'Continuous Capture'. A status bar at the bottom of the image area shows 'Armed.' and various settings like 'Level 1 A', 'Measuring I', 'Closing me', 'Enable Rule', 'Disable Rul', and 'Open Folder'.

Picture List

No.	Capture Time	Lane No.	Plate Color	License Plate No.	Speed	Illegal Type	Vehicle No.	Directory
9		1					59	
8		1					58	
7		1					57	
6		1					56	
5		1					55	

Traffic Light Status

Lane 1 (N/A)	Lane 2 (N/A)	Lane 3 (N/A)	Lane 4 (N/A)
--------------	--------------	--------------	--------------

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.

- Click **Measuring license plate** to measure the license plate pixel. After the measurement, click **Closing measurement**.
- Click **Enable Ruler** to enable ruler when measuring the license plate. After the measurement, click **Disable Ruler**.
- 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 on the right of **Continuous Capture** to set the continuous capture parameters. After the configuration, click **Continuous Capture** to capture pictures.

Capture Times

Up to five times are supported.



Continuous Capture Intervals

Up to four intervals are supported. You can set the time of each interval.





Chapter 4 Live View and Local Configuration

4.1 Live View

4.1.1 Start/Stop Live View

Click  to start live view. Click  to stop live view.

4.1.2 Select Image Display Mode

Click     to display the image in 4:3/16:9/original/self-adaptive display mode.

4.1.3 Select Stream Type

Click [Main Stream](#) / [Sub-Stream](#) / [Third Stream](#) 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. The third stream is the custom stream.



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

4.1.4 Capture Picture Manually

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




Steps

1. Click  to start live view.
2. Click  to capture a picture.
3. **Optional:** Click **Configuration** → **Local Configuration** to view the saving path of snapshots in live view.

4.1.5 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 Configuration** to view the saving path of record files.


4.1.6 Enable Digital Zoom

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

Steps

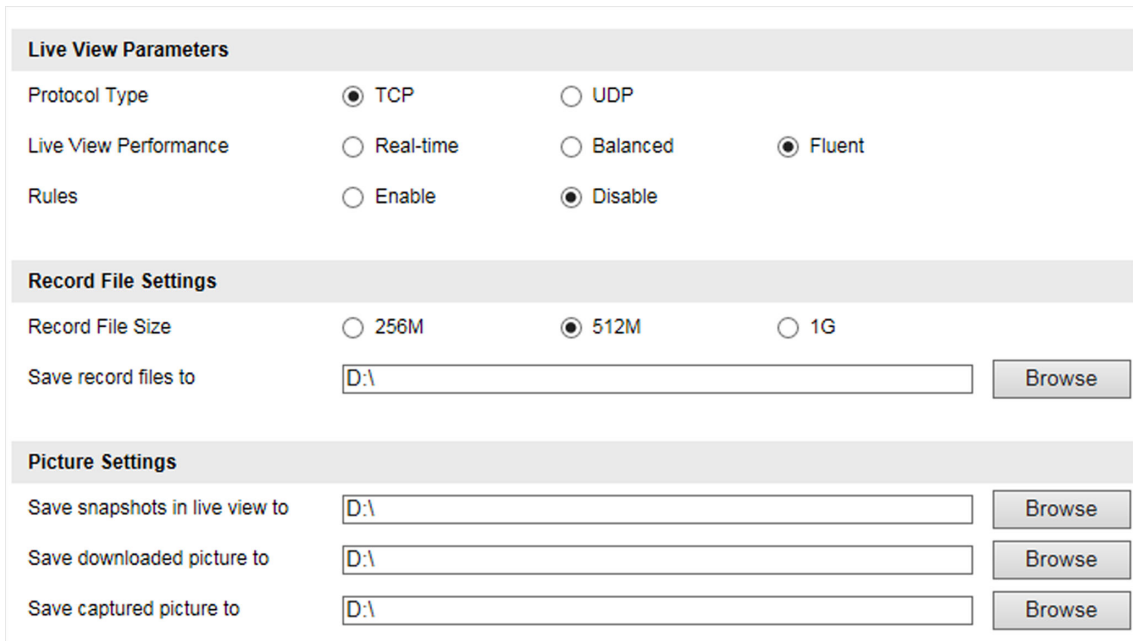
1. Click  to start live view.
2. Click  to enable digital zoom.
3. Place the cursor on the live view image position which needs to be zoomed in. Drag the mouse rightwards and downwards to draw an area.

The area will be zoomed in.

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

4.2 Local Configuration

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



The screenshot shows a configuration interface with three main sections:

- Live View Parameters:**
 - Protocol Type: TCP, UDP
 - Live View Performance: Real-time, Balanced, Fluent
 - Rules: Enable, Disable
- Record File Settings:**
 - Record File Size: 256M, 512M, 1G
 - Save record files to:
- Picture Settings:**
 - Save snapshots in live view to:
 - Save downloaded picture to:
 - Save captured picture to:

Figure 4-1 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, yet the real-time transmission will be affected.

UDP

Provides real-time audio and video streams.

Live View Performance

Real-Time

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.

Fluent

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

Rules

If you enable rules, the colored rectangles will display on the live view image when the motion detection is triggered.

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 for the manually captured pictures in live view mode.

Save downloaded picture to

Set the saving path for the downloaded pictures.

Save captured picture to

Set the saving path for the captured pictures in **Live View → Live Traffic Statistics** .

Chapter 5 Storage

5.1 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** .

Figure 5-1 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**.

5.2 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 → TCP/IP** .

ANPR IP Address:	<input type="text" value="0.0.0.0"/>
ANPR Port:	<input type="text" value="80"/>
Listening Host IP:	<input type="text" value="0.0.0.0"/>
Listening Host Port No.:	<input type="text" value="7200"/>
Enable Uploading Picture...	<input type="checkbox"/>

Figure 5-2 Set Listening Host

2. Set **ANPR IP Address/Domain** and **ANPR Port** if you need to upload the alarm information and pictures.
3. Set **Listening Host IP** and **Listening Host Port No.**, and check **Enable Uploading Picture while Listening** if you need to upload the alarm information and pictures.



Note

ANPR and listening conflict with each other. When you enable listening host, pictures will be uploaded via listening host in priority. When you disable listening and have set ANPR IP address and port, pictures will be uploaded via ANPR protocol.

4. Click **Save**.

5.3 Set Cloud Storage

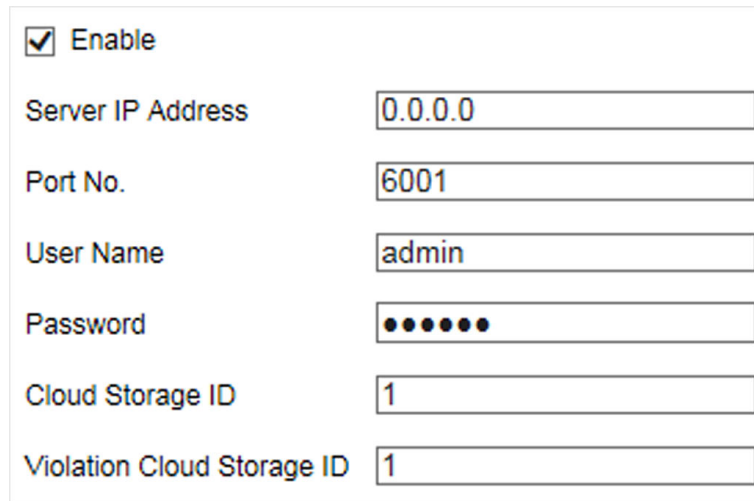
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

- Arrange the cloud storage server.
- You have enabled level 1 arm in **Live View → Live Traffic Statistics** .

Steps

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



The screenshot shows a configuration form for Cloud Storage. It includes a checkbox for 'Enable' which is checked. Below it are several input fields: 'Server IP Address' with the value '0.0.0.0', 'Port No.' with '6001', 'User Name' with 'admin', 'Password' with seven dots, 'Cloud Storage ID' with '1', and 'Violation Cloud Storage ID' with '1'.

Figure 5-3 Set Cloud Storage

2. Check **Enable**.
3. Set the server parameters.
 - 1) Enter **Server IP Address** and **Port No.**
 - 2) Enter **User Name** and **Password**.
 - 3) Enter the ID according to the storage area No. of the server.
4. Click **Save**.

Chapter 6 Encoding and Display

6.1 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.

Max. 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.

Encoding Complexity

Under the same bitrate, the higher the encoding complexity is, the higher the image quality is, and the higher the requirement of the network bandwidth is.

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**.

6.2 Set Image Parameters

You can adjust the image parameters to get clear image.

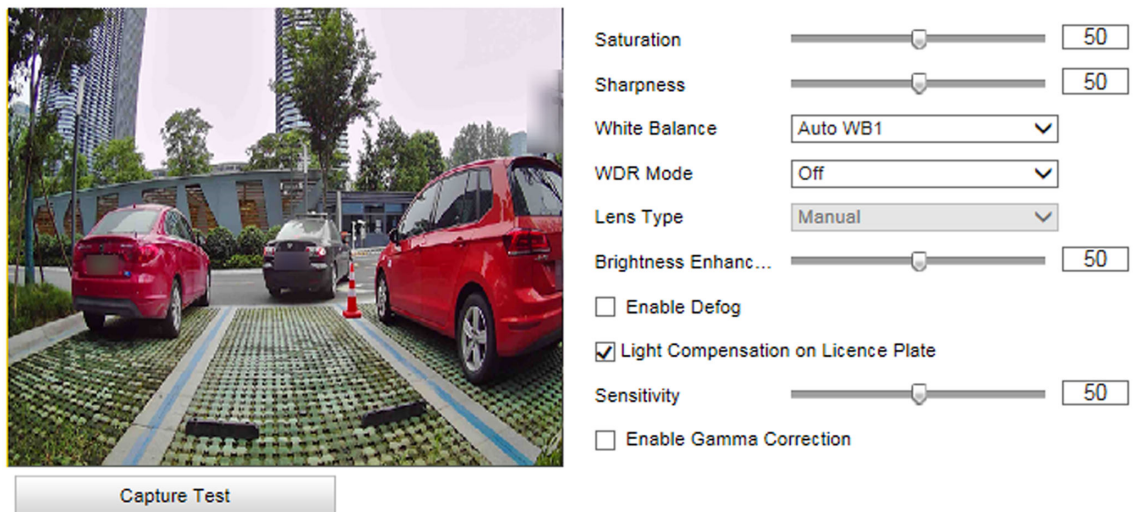
Steps



Note

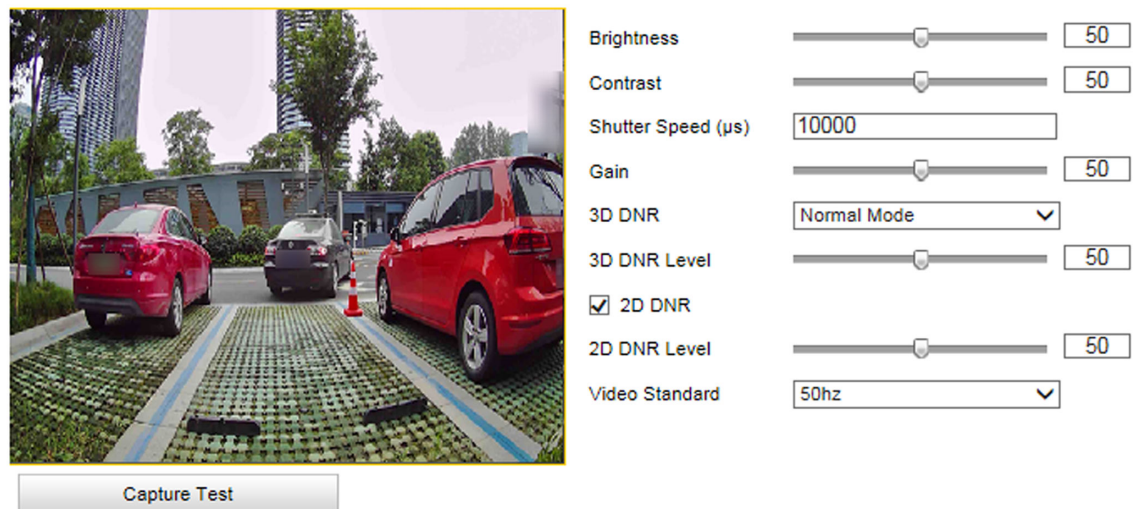
The supported parameters may vary with different models. The actual device prevails.

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



Hint: Test the function of triggering the camera to capture.

Figure 6-1 Set General Parameters



Hint: Test the function of triggering the camera to capture.

Figure 6-2 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.

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 spatial 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.

Video Standard

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

6.3 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**.

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.
Do not switch	Disable ICR mode.

3. Click **Save**.

6.4 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** .

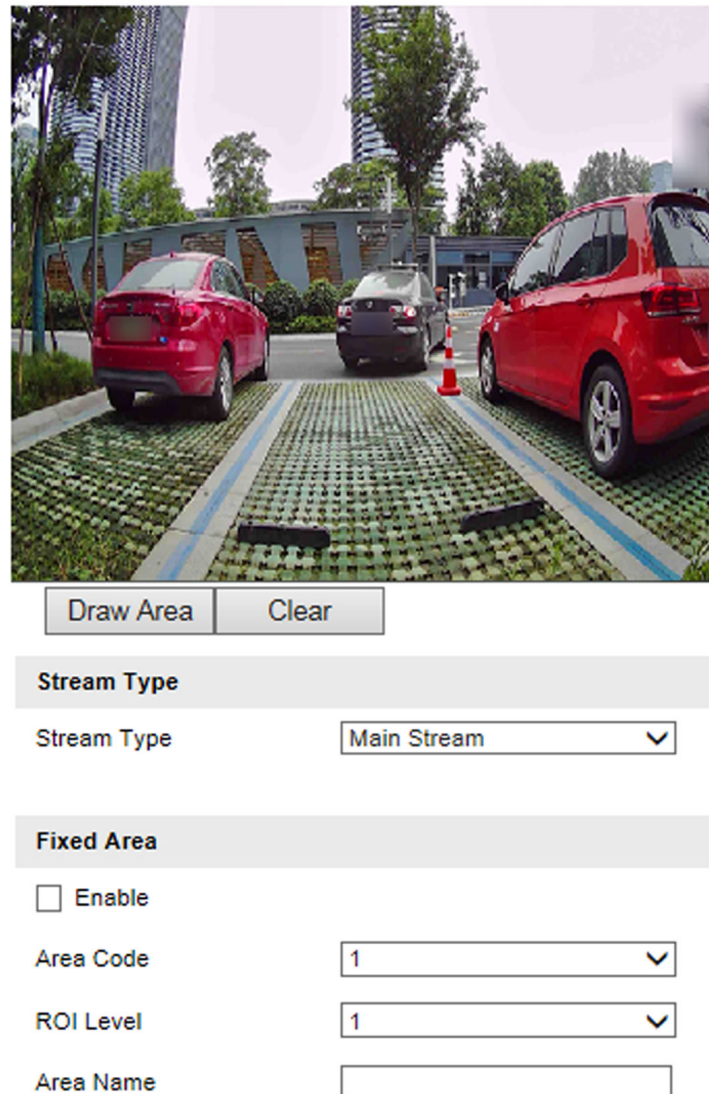


Figure 6-3 Set ROI

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.

6.5 Set OSD

You can customize OSD information on the live view.

Steps

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

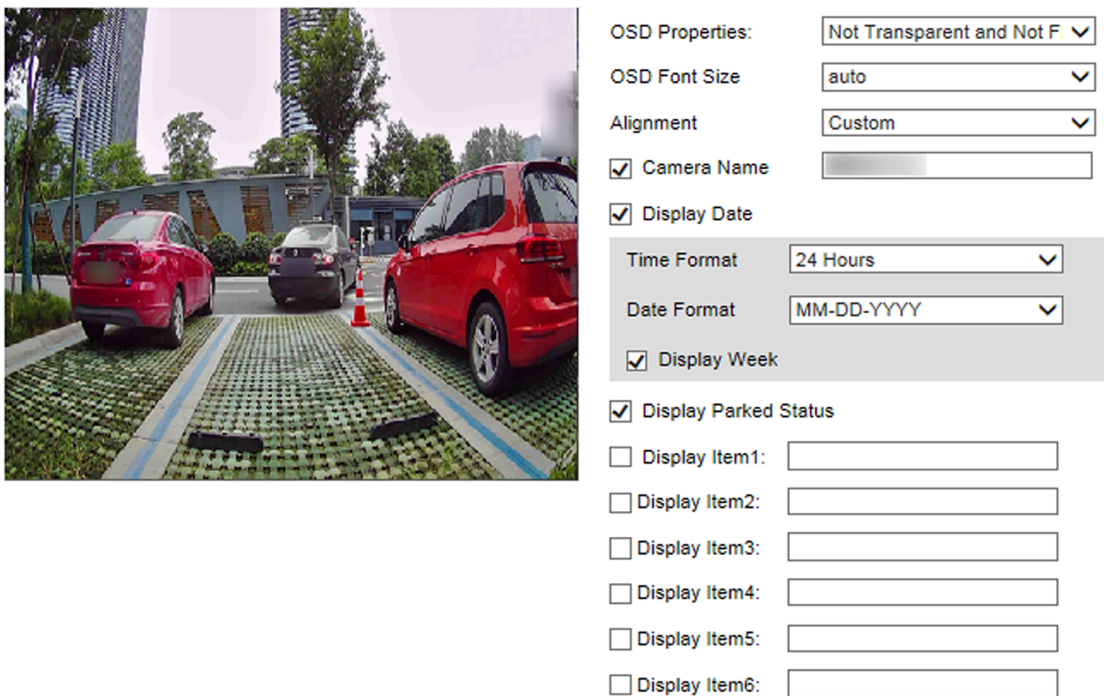


Figure 6-4 Set OSD

2. Set OSD property, font size, alignment, etc.
3. **Optional:** Set the display content.
 - 1) Check **Camera Name** and enter the name.
 - 2) Check **Display Date**, and set the time and date format.
 - 3) Check **Display Week**.
 - 4) Check **Display Parked Status**.
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 7 Network Configuration

7.1 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** → **TCP/IP** for parameter settings.

The screenshot shows a configuration window titled "NIC Parameters". It contains the following fields and values:

NIC Parameters	
NIC Type	10M/100M/1000M Self-adaptive
<input type="checkbox"/> Auto-Obtain	
IPv4 Address	10.10.113.152
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.10.113.254
IPv6 Mode	Auto-Obtain
IPv6 Address	
IPv6 Default Gateway	::
IPv6 Subnet Mask	
MAC Address	68:ed:bc:11:ba:0e
MTU	1500
Multicast Address	

Figure 7-1 Set IP Address

NIC Type

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

IPv4

Two IPv4 modes are available.

Auto-Obtain

The device automatically gets the IPv4 parameters from the network if you check **Auto-Obtain**. 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 auto-obtain.

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 Announcement

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

 **Note**

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

Auto-Obtain

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 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 Server** properly if needed.

7.2 Connect to ISUP Platform

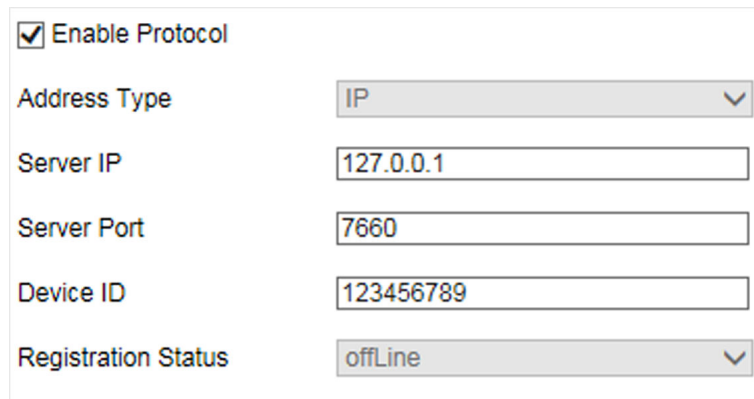
ISUP is a platform access protocol. The device can be remotely accessed via ISUP platform.

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** .



The screenshot shows a configuration form with the following fields:

<input checked="" type="checkbox"/> Enable Protocol	
Address Type	IP
Server IP	127.0.0.1
Server Port	7660
Device ID	123456789
Registration Status	offLine

Figure 7-2 Connect to ISUP Platform

2. Check **Enable Protocol**.

3. Select **Address Type**.

Domain Name

When the server is in extranet, and the IP address is dynamic, you can select it.

IP

When the server IP address is static, you can select it.

4. Enter the parameters below.

Server IP

Enter the static IP address of ISUP platform.

Server Port

The default value is 7660.

Device ID

The ID of the device registered on the ISUP platform. If you leave it empty, the device will be logged in to the platform with serial No.

5. Click **Save**.

7.3 Set DDNS

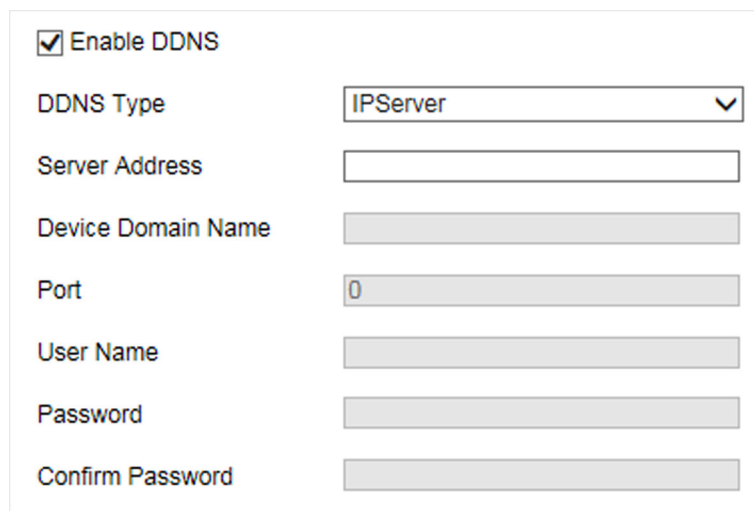
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

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 Password	

Figure 7-3 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.

7.4 Set Port

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

Caution

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.

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

Figure 7-4 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.

Chapter 8 Serial Port Configuration

8.1 Set RS-485

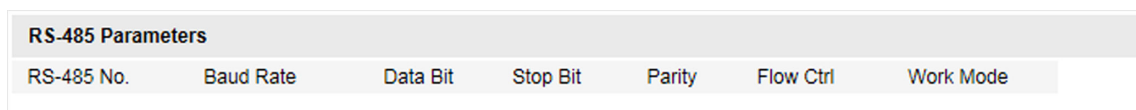
Set RS-485 parameters if the device needs to be connected to other peripheral devices controlled by RS-485 serial port.

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 Port Parameters** .



RS-485 Parameters						
RS-485 No.	Baud Rate	Data Bit	Stop Bit	Parity	Flow Ctrl	Work Mode

Figure 8-1 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 **Work 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.

4. Click **Save**.

8.2 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port.

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 Port Parameters** .
2. Click **Advanced Settings**.

RS-232 Parameters	
Baud Rate	115200 bps <input type="button" value="v"/>
Data Bit	8 <input type="button" value="v"/>
Stop Bit	1 <input type="button" value="v"/>
Parity	<input type="button" value="v"/>
Flow Ctrl	<input type="button" value="v"/>
Working Mode	Console <input type="button" value="v"/>
Advanced Settings	

Figure 8-2 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.

Narrowband

Reserved.

5. Click Save.

Chapter 9 Exception Alarm

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

Steps

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

Enable	Exception Type	Notify Surveillance Center	Trigger Alarm Output	Alarm Dwell Time (s)
<input type="checkbox"/>	Network Disconnected			
<input type="checkbox"/>	IP Address Conflicted			

Figure 9-1 Set Exception Alarm

2. Check the exception type to be alarmed.
3. Click **Save**.

Chapter 10 Safety Management

10.1 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 **User Type**.
 - 3) Enter **Admin Password, 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**.



Note

The administrator can add up to 15 user accounts.

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

10.2 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.

10.3 Set HTTPS

10.3.1 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.

10.3.2 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**.

10.4 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** → **Port** .
2. Uncheck **SSH Port**.
3. Click **Save**.

Chapter 11 Maintenance

11.1 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 device status.

11.2 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 syslog**.
3. Enter **IP** and **Port** of the log server.
4. Click **Save**.

Result

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

11.3 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.

11.4 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.

11.5 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 **Default** to restore all the parameters to the factory settings.
3. Click **OK**.

11.6 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**.



Note

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

4. Click **Save**.

11.7 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**.

11.8 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 Configuration File**.
2. Click **Export**.
3. Set a 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**.

11.9 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



Caution

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 Configuration File**.
 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. Enter the password which is set when the configuration file is exported, and click **OK**.
5. Click **Import**.
6. Click **OK** on the popup window.

Result

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

11.10 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**.
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.

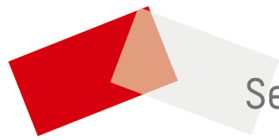


Figure A-1 Communication Matrix

Scan the QR code below to get the device command.



Figure A-2 Device Command



See Far, Go Further