Mobile Enforcement Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

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

Symbol Conventions

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

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

Contents

Chapter 1 Product Introduction 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 Network Configuration 5

3.1 Set IP Address 5

3.2 Dial-up 6

3.3 Set Wi-Fi 7

3.4 Set Wi-Fi AP 8

3.5 Set DDNS 10

3.6 Set Port 11

3.7 Set Integration Protocol 11

Chapter 4 Camera Management 12

4.1 Add IP Camera 12

4.2 Set Camera 14

4.2.1 Set Camera Parameters 14

4.2.2 Set Interaction Parameters 15

4.2.3 Set Camera Connection Mode 15

4.3 Add Traffic Radar 17

Chapter 5 Mobile Enforcement Configuration 18

5.1 Set Road Name Overlay 18

5.2 Set Secondary Stopped Vehicle Parameters 18

5.3 Set Satellite Positioning 19

5.4 Set Vehicle Deployment 21
5.5 Set Capture Parameters 22
5.5.1 Set Picture Composition 22
5.5.2 Set Single Picture Overlay 24
5.5.3 Set Composite Picture Overlay 26
5.5.4 Set Camera Matching 28
5.6 Set Violation Dictionary 29
Chapter 6 Live View and Local Configuration 31
6.1 Live View 31
6.1.1 Start/Stop Live View 31
6.1.2 Divide Window and Switch Page 31
6.1.3 Select Stream Type 31
6.1.4 Capture Manually 32
6.1.5 Record Manually 32
6.1.6 Enable/Disable Audio 32
6.1.7 Enable Digital Zoom 32
6.1.8 Display in Full Screen 33
6.2 PTZ Control 33
6.2.1 PTZ Control Panel 33
6.2.2 Set Preset 34
6.3 Local Configuration 34
Chapter 7 Storage 38
7.1 Format Disk 38
7.2 Set Quota 38
7.3 Detect HDD 38
7.4 Set Holiday 39
Chapter 8 Record and Playback 40
8.1 Set Recording Schedule 40

8.2 Play Back Video 41
8.3 Backup 42
8.3.1 Back up Video 42
8.3.2 Back up Clipped Video 43
Chapter 9 Encoding and Display 44
9.1 Set Video Encoding Parameters 44
9.2 Set Audio Encoding Parameters 45
9.3 Set Image Parameters 45
9.4 Set OSD 46
Chapter 10 Platform Connection 47
10.1 Set Remote Host 47
10.2 Set FTP 52
10.3 Connect to SDK Platform 55
10.4 Connect to ISUP Platform 55
10.5 Connect to HTTP Platform 56
10.6 Set Cloud Storage 57
Chapter 11 Alarm Congifuration 60
11.1 Set Alarm Input 60
11.2 Set Alarm Output 61
11.3 Set Exception Alarm 62
11.4 Set Camera Capture Alarm 63
Chapter 12 Data Management 65
12.1 View Real-Time Data 65
12.2 Search Data 65
12.3 Back up Data 66
12.3.1 Back up to Local 66
12.3.2 Back up to USB 66
Chapter 13 Safety Management 68

13.1 Manage User 68
13.2 Set HTTPS 68
13.2.1 Install Authorized Certificate 68
13.2.2 Create and Install Self-signed Certificate 69
13.3 Set IP Address Filtering 69
13.4 Set SSH 70
13.5 Enable System Log Service 70
13.6 Set Session Expired Time 70
Chapter 14 Maintenance 71
14.1 View Device Information 71
14.2 View System Status 71
14.3 Synchronize Time 71
14.4 Set RS-485 72
14.5 Set RS-232 73
14.6 Set DST 73
14.7 Reboot 73
14.8 Restore Parameters 74
14.9 Restore Database 74
14.10 Export Parameters 74
14.11 Import Parameters 75
14.12 Upgrade 75
14.13 Search Log 75
14.14 Export Debugging Log 76
14.15 Reserved Parameters 76
14.16 Set Startup Mode 76

Chapter 1 Product Introduction

Mobile enforcement video recorder (hereinafter referred to as device) can be connected with intelligent emergency vehicle lighting, positioning system lite, manual controller, LCD monitor, etc to realize mobile enforcement. It supports local video storage, dial-up, wireless network transmission, satellite positioning, remote control, and light supplement, meeting the demand of all-day enforcement. It is widely applied to police vans, special vehicles, emergency scenes, etc. It provides a complete solution for traffic violation enforcement, security protection, emergency commanding, and other monitoring projects.

Chapter 2 Activation and Login

2.1 Activation

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

Note

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

2.1.1 Default Information

The device default information is shown as below.

- 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 device over the LAN.

Before You Start

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

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

Steps

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

   Caution

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

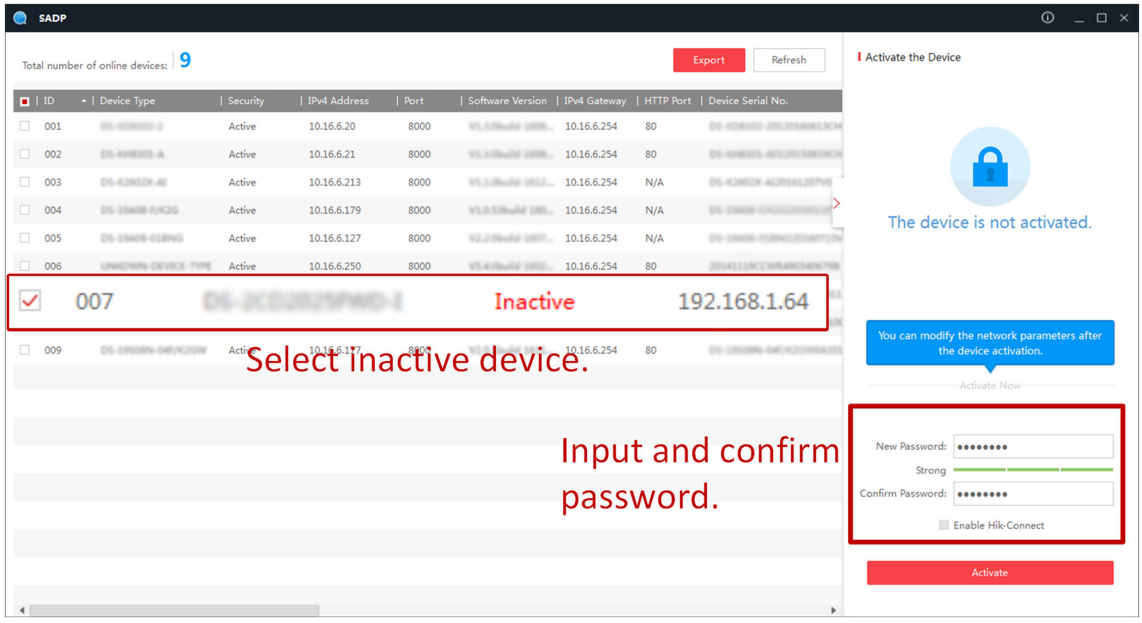

Figure 2-1 Activate via SADP

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

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP** (Dynamic Host Configuration Protocol).
   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 are in the LAN with the same network segment.

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 Network Configuration

3.1 Set IP Address

Set the IP address of the network interface on the device panel. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Steps

1. Go to **Param Config → Network → Basic Settings → TCP/IP** .

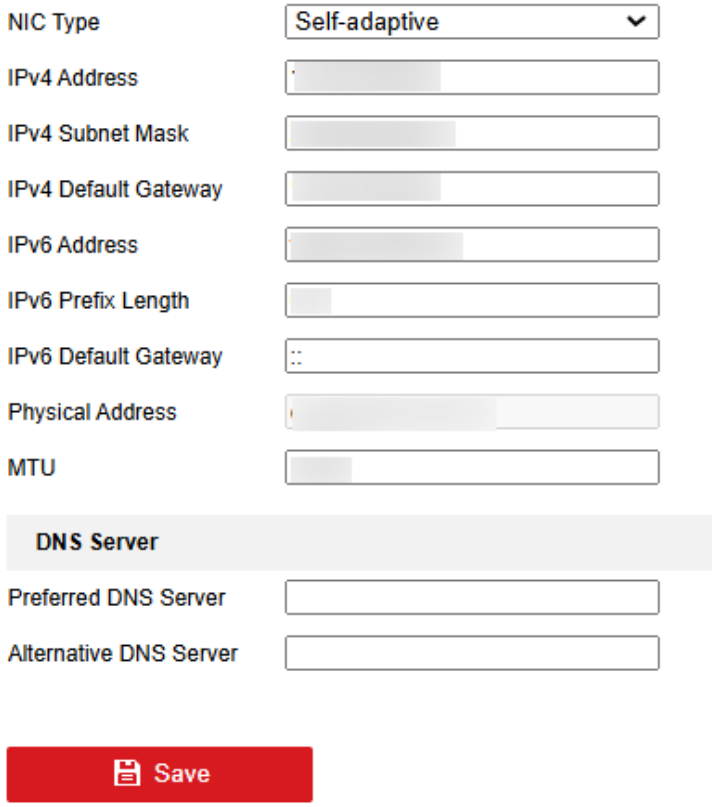

Figure 3-1 Set IP Address

2. Select **NIC Type** according to the actual network.
3. Enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.

Note

MTU stands for the maximum transmission unit in the network.

4. **Optional:** Set DNS Server if remote domain name access is needed.
5. Click **Save**.

3.2 Dial-up

Set the dial-up parameters if you want to connect the device to the network via a SIM card.

Before You Start

The device has a dial-up module and a SIM card has been installed.

Steps

1. Go to **Param Config → Network → Basic Settings → Wireless Dial** .
2. Click **Dial-up Parameters**.
3. Check **Enable**.

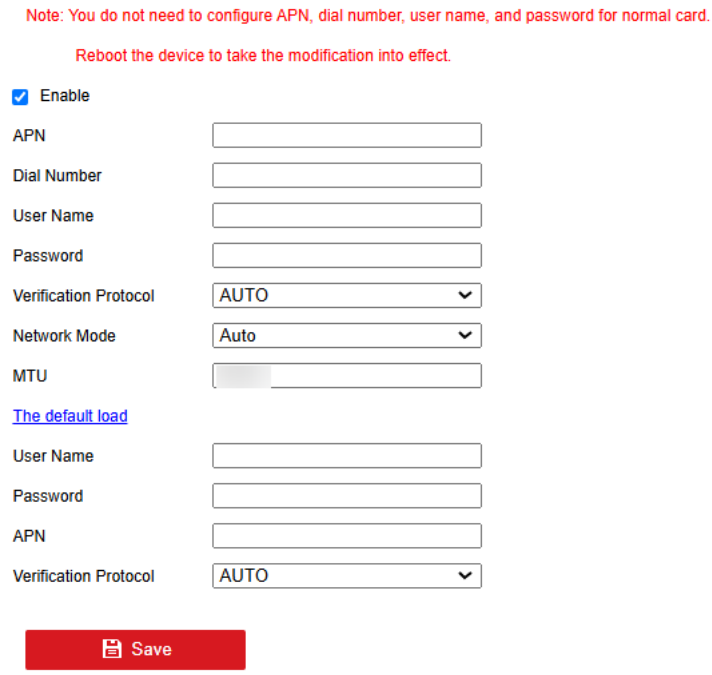

Figure 3-2 Set Dial-up Parameters

4. Set dial-up parameters.
   - When you connect the device to the normal network, you do not need to set the dial-up parameters.
   - When you connect the device to the private network, set the dial number, user name, password and APN information according to the SIM card information.
5. Select **Network Mode** according to the actual needs.

   Auto-Search and Auto-Switch

   The device will search and switch the network mode automatically.

   3G/4G

   Connecting the device via 3G/4G dial-up.
6. Set **MTU**.

Note

The MTU is the maximum payload length for a particular transmission media.

7. Click **Save**.

What to do next

Reboot the device to take the settings into effect. After reboot, you can click **Dial-up Status** to view the dial-up status.

3.3 Set Wi-Fi

Set Wi-Fi parameters if you want to connect the device to the network via Wi-Fi.

Steps

Note

Wi-Fi and Wi-Fi AP functions conflict with each other. You can only enable one.

1. Go to **Param Config → Network → Advanced Settings → Wi-Fi** .
2. Click **Wi-Fi Configuration**.

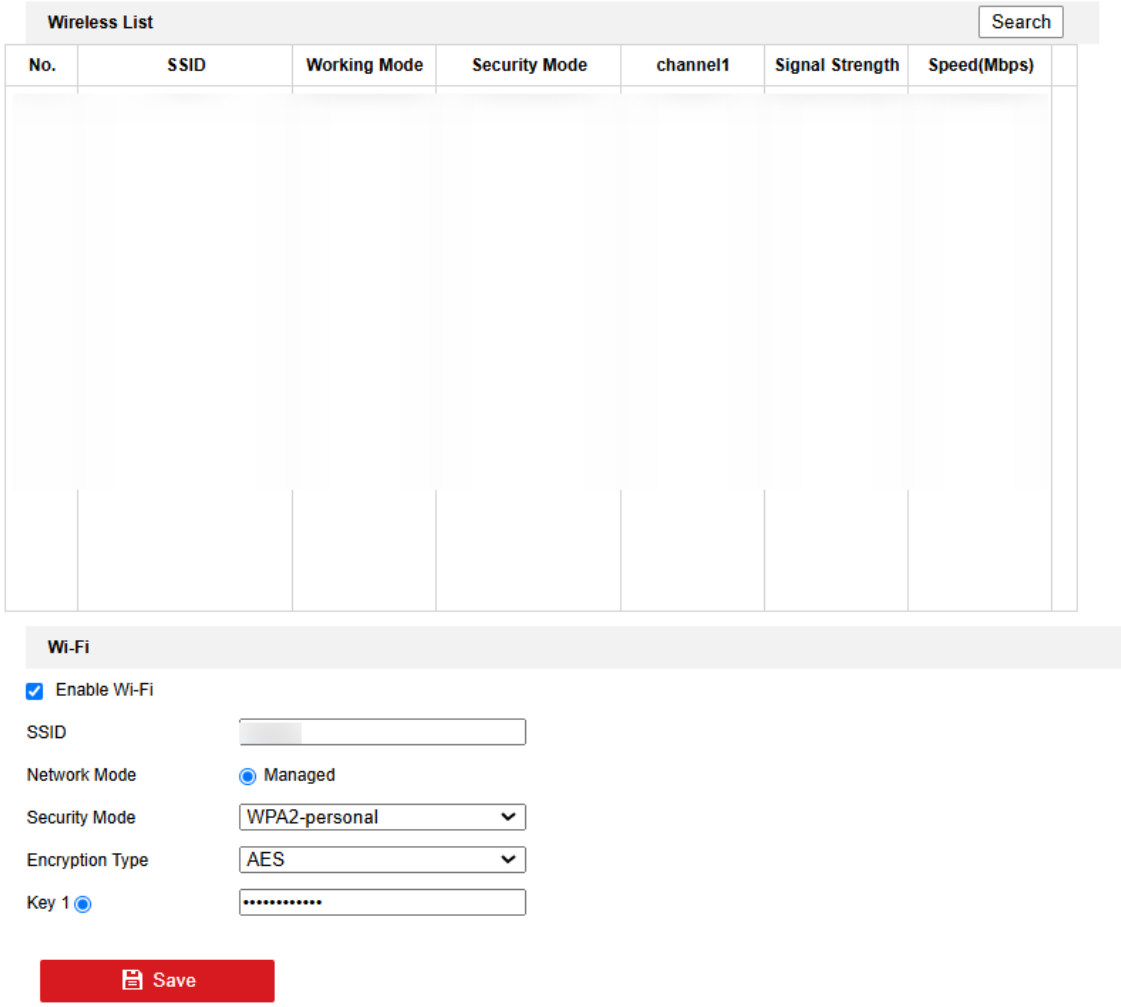

Figure 3-3 Set Wi-Fi

3. Click **Search** and select Wi-Fi to connect in the Wi-Fi list.
4. Check **Enable Wi-Fi**.
5. Select **Security Mode** and **Encryption Type** according to the actual needs.
6. Enter **Key**.
7. Click **Save**.
8. **Optional:** Click **Wi-Fi Status** to view the Wi-Fi connection status.

3.4 Set Wi-Fi AP

The device can be set as a hotspot to share network to other devices.

Steps

Note

Wi-Fi and Wi-Fi AP functions conflict with each other. You can only enable one.

1. Go to **Param Config → Network → Advanced Settings → Wi-Fi AP** .
2. Check **Enable Wi-Fi AP**.

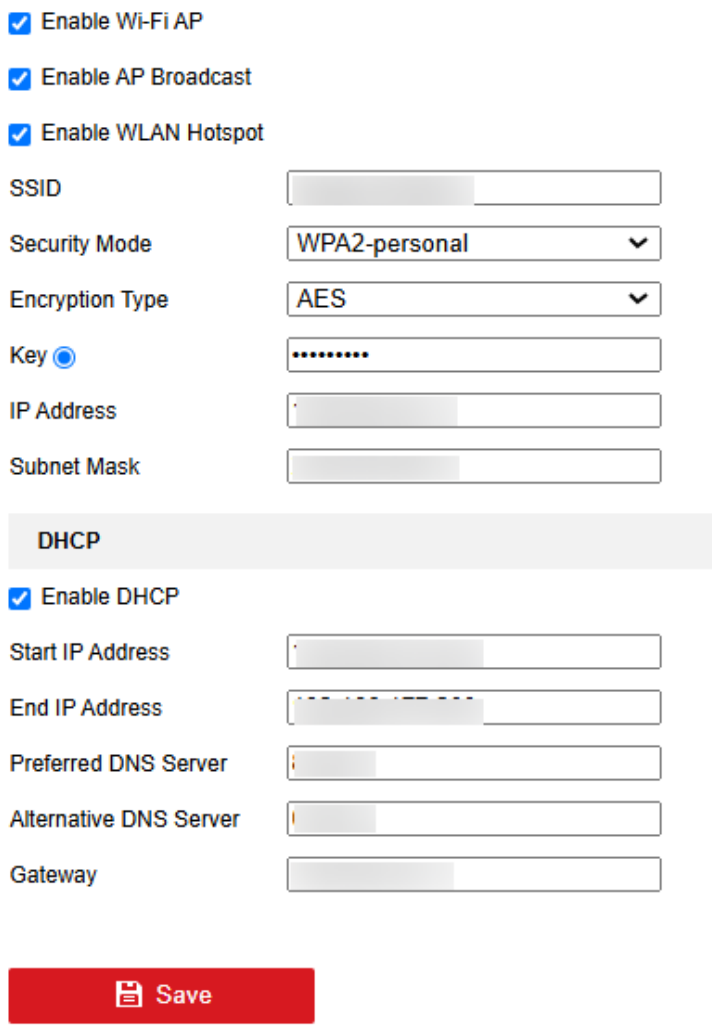

Figure 3-4 Set Wi-Fi AP

3. Enable AP broadcast or WLAN hotspot.

   Enable AP Broadcast

   Once enabled, other devices are able to detect the SSID of the device.

   Enable WLAN Hotspot

   Enable it to share the device network. Other devices can access to the device Wi-Fi AP.
4. Set Wi-Fi hotspot parameters.

1) Enter **SSID** (hotspot name).
2) Select **Security Mode** and **Encryption Type**.
3) Set **Key**.

5. Check **Enable DHCP**, and enter IP addresses and gateway from the address pool that allows automatic obtaining.

Note

The Wi-Fi AP IP address and the device IP address should be in different network segments.

6. **Optional:** Set DNS server address if you need to visit the device with domain name.
7. Click **Save**.

3.5 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 ports are 80, 8000, and 554.

Steps

1. Go to **Param Config → Network → Basic Settings → DDNS** .

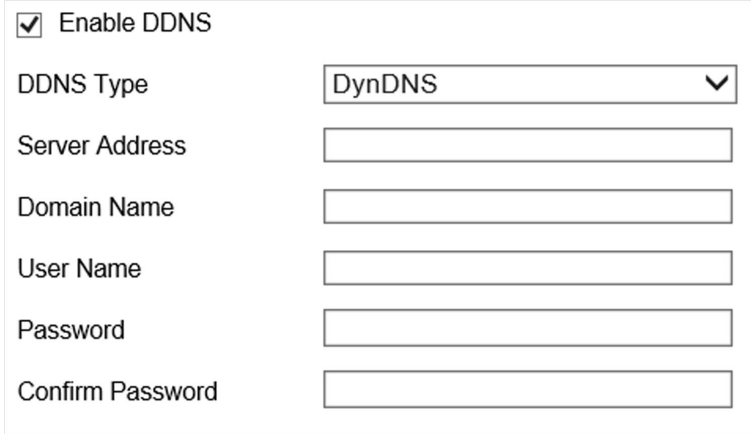

Figure 3-5 Set DDNS

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

What to do next

Enter the domain name in the browser address bar to access the device.

3.6 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 **Param Config → Network → Basic Settings → Port** for port settings. Click **Save** after finishing settings.

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.

HTTPS Port

It refers to the port of encrypted transmission and identity authentication protocol.

Server Port

It refers to the port to connect to client for obtain network protocol control and set device parameters.

Note

- Certain ports need to reboot after edited to take the new settings into effect.
- When the device cannot edit the port No. via access Web due to port conflicts, you can connect the device to your computer and edit via SADP software.

3.7 Set Integration Protocol

If you want to use the device as an ONVIF server, you can enable this function.

Steps

1. Go to **Param Config → Network → Advanced Settings → Integration Protocol** .
2. Check **Enable ONVIF**.
3. Click **Save**.

Chapter 4 Camera Management

4.1 Add IP Camera

Add IP cameras to the device to get the video stream.

Before You Start

Set the network properly to guarantee the device and the cameras can be communicated normally.

Steps

1. Go to **Param Config → System → Camera Management → IP Camera** .

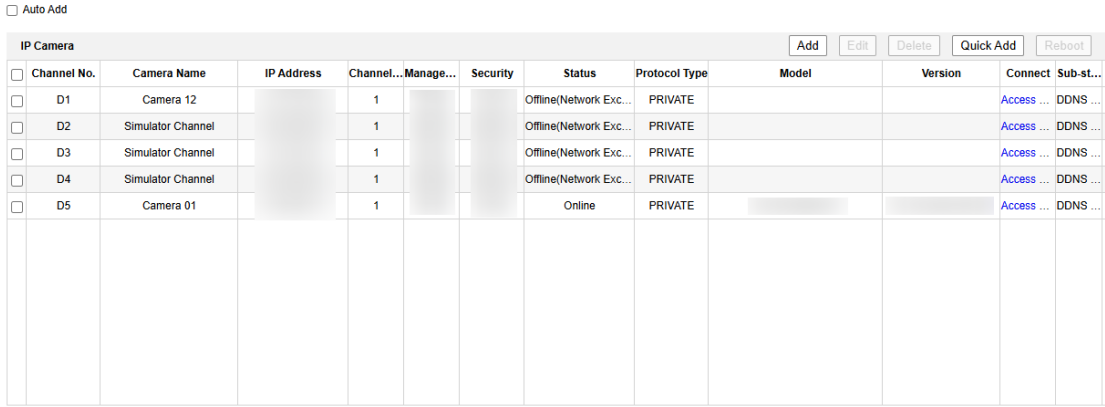

Figure 4-1 Add IP Camera

2. Add IP cameras via the following 3 methods.
   - Auto Add: For the network positioning system which has been connected to the PTZ interface of the device, and the IP cameras which have been connected to the IPC interfaces of the device, you can check **Auto Add** to add them automatically.
   - Quick Add: It is applicable to the cameras adopting PRIVATE protocol.
     a. Click **Quick Add**. The cameras in the same network segment with the device will be displayed.
     b. Check the camera(s) that need to be added, enter the corresponding user name and password, and click **OK**.

     Note

     You can check cameras that have the same user name and password to add in batch.
   - Manual Add:

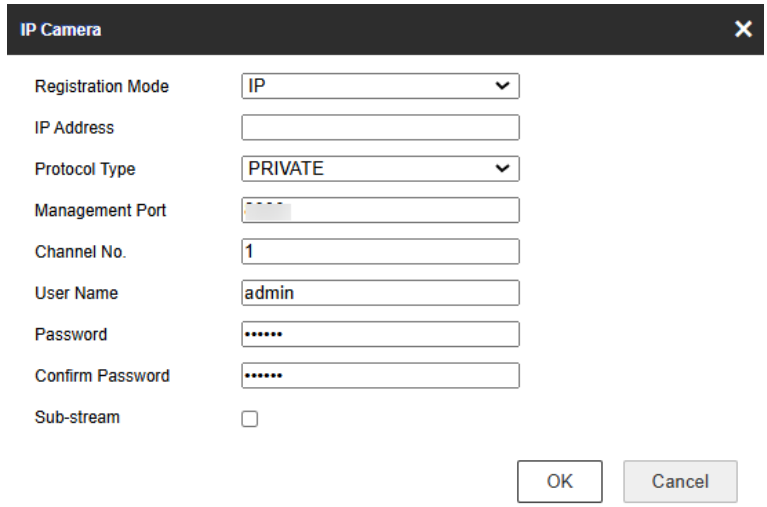

Figure 4-2 Manual Add

a. Click **Add**.
b. Select **Registration Mode**.
c. Enter the camera information.

Protocol Type

Select **PRIVATE** for Hikvision cameras. Select **ONVIF** for the third-party cameras. Select **RTSP** for the cameras getting stream from stream media.

Management Port

The protocol management port. Log in to the camera to get the corresponding protocol port.

Channel No.

For the multi-channel cameras, enter the channel No. to get streams. The No. is 1 for the single-channel cameras by default.

d. Enter **User Name**, **Password**, and confirm the password.
e. If you want the camera to get stream via sub-stream, check **Sub-stream**.
f. Click **OK**.

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

Edit	Edit the added camera Information.
Delete	Delete the added camera.
Reboot	Reboot the online camera.
Access Directly	Access to the online camera directly.

4.2 Set Camera

4.2.1 Set Camera Parameters

You can set camera parameters for easy management.

Steps

1. Go to **Param Config → System → Camera Management → Camera Parameter** .

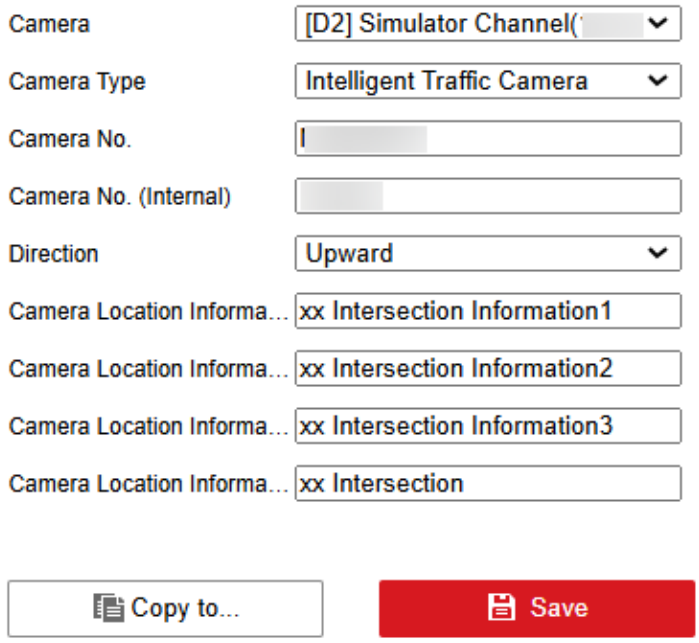

Figure 4-3 Set Camera Parameters

2. Select a camera.
3. Select **Camera Type**.

Note

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

Camera for Video Surveillance (Not Capture)

Select it when the device only monitor the camera live view image without receiving the pictures captured by the cameras.

Intelligent Traffic Camera

Select it when the device needs to receive the pictures captured by the cameras.

Ray camera

Select it when the radar-assisted cameras are connected to the device.

4. Set **Camera No.**, **Camera No. (Internal)**, and **Camera Location Information**.
5. Select **Direction** according to the driving direction.
6. **Optional:** Click **Copy to...** to copy the settings to other channels.
7. Click **Save**.

4.2.2 Set Interaction Parameters

Set interaction parameters to control the interaction data between the camera and the device.

Before You Start
Add the camera.

Steps
1. Go to **Param Config → System → Camera Management → Interactive Settings** .
2. Select a camera.
3. Select an interaction mode.

   Normal Mode

   You can realize the live view of the camera image, control the video recording, receive the capture data of the camera, and judge the camera online status via the device.

   Data Receiving Mode

   You can only receive the capture data of the camera, but you cannot record or preview the images.
4. **Optional:** Click **Copy to...** to copy the settings to other channels.
5. Click **Save**.

4.2.3 Set Camera Connection Mode

You can set the camera under the listening mode or arming mode.

Before You Start
Ensure the connected camera supports violation capture function.

Steps
1. Go to **Param Config → Advanced Settings → Other Settings → Other Settings** .

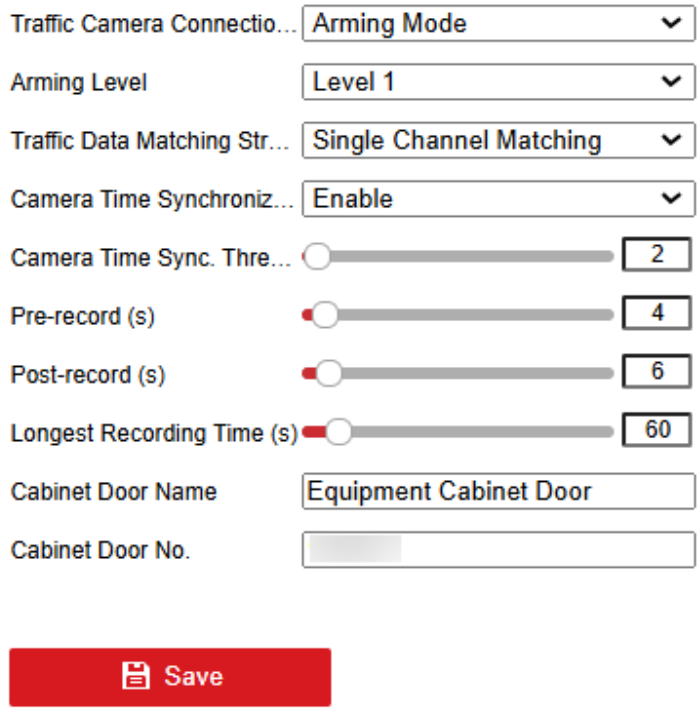

Figure 4-4 Set Camera Connection Mode

2. Set the parametes below.

Traffic Camera Connection Mode

Arming Mode

The device actively connects to the camera and receives images after the camera login via the device.

Listening Mode

The connection between the camera and the device should be created on the camera. Set the camera to the listening upload mode, and the device can receive the uploaded date from the camera.

Arming Level

- Level 1 arming can only connect 1 client or web. Level 2 arming can connect 3 clients or webs. Level 3 arming can connect 5 clients or webs.
- The device supports to set level 1, level 2 and level 3 arming simultaneously. The level 1 arming uploads first.

Traffic Data Matching Strategy

It is valid only when the connection mode is listening mode. Select it according to the number of camera channels. For example, if the connected camera is a multi-channel camera in listening mode, you can select **Multi-Channel Matching**.

Camera Time Synchronization

You can enable the function to synchronize the camera time with the device time. Set **Camera Time Sync. Threshold**. The device will synchronize the camera time according to the set threshold to ensure its time is consistent with the device time.

Pre-record

The time to record before the violation recording start time.

Post-record

The time to record after the violation recording end time.

Longest Recording Time

The longest recording time of violation recording.

3. Enter the name and No. of the cabinet door according to the actual connected cabinet of the device.
4. Click **Save**.

4.3 Add Traffic Radar

You can add traffic radars to the device.

Steps

1. Go to **Param Config → System → Camera Management → Traffic Radar** .
2. Click **Add**.
3. Enter **IP Address**, **Port**, and **Associated Channel**.
4. Click **OK**.
5. **Optional:** You can also do the following operations.

Edit	Edit the added radar Information.
Delete	Delete the added radar.

Chapter 5 Mobile Enforcement Configuration

5.1 Set Road Name Overlay

Import the road name file to locate the road and overlay the road name on the enforcement videos and captured images.

Before You Start

Contact the technical support to get the road name tool and make the road name file. Save the road name file to the computer.

Steps

1. Go to **Param Config → Advanced Settings → Other Settings → Road Name Config** .

Figure 5-1 Set Road Name Overlay

2. Click **Browse** to select the road name file from the computer, and click **Import** to import it to the device.
3. **Optional:** Check **Enable auto Related Road Name**, and the device will compare the location information actually gotten from the embedded positioning module with that in the road name file to locate the road name.
4. Select **Camera No.** to overlay the road name on the enforcement videos and captured images of the selected camera(s).
5. Click **Save**.

5.2 Set Secondary Stopped Vehicle Parameters

You can enable the function to recognize and capture the secondary stopped vehicle violations.

Steps

Note

You need to set the function when using the device with a pad or the third-party platform. You do not need to set the function when using the device with TPC platform.

1. Go to **Param Config → Advanced Settings → Other Settings → Secondary Stopped Vehicle** .
2. Check **Enable**.

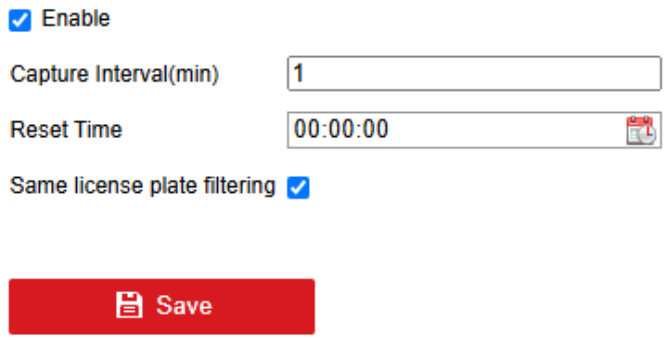

Figure 5-2 Set Secondary Stopped Vehicle Parameters

3. Set the parameters below.

   Capture Interval

   During the set interval, the device will not capture the secondary stopped vehicle violation of the same vehicle.

   Reset Time

   Set the time to clear the stopped vehicle violation every day. The captured data before the set time will not operate the secondary stopped vehicle comparison, and the captured data after the set time will operate the secondary stopped vehicle comparison.

   Same license plate filtering

   Disable it to capture violations of the stopped vehicle with the same license plate repeatedly. Enable it to capture once for the repeated violations of the stopped vehicle with the same license plate.
4. Click **Save**.

5.3 Set Satellite Positioning

Set satellite positioning to get the specific location of the device, synchronize time with the satellite, or trigger speed limit alarm.

Steps

1. Go to **Param Config → Advanced Settings → Other Settings → Position Settings** .
2. Click **Location Configuration**.

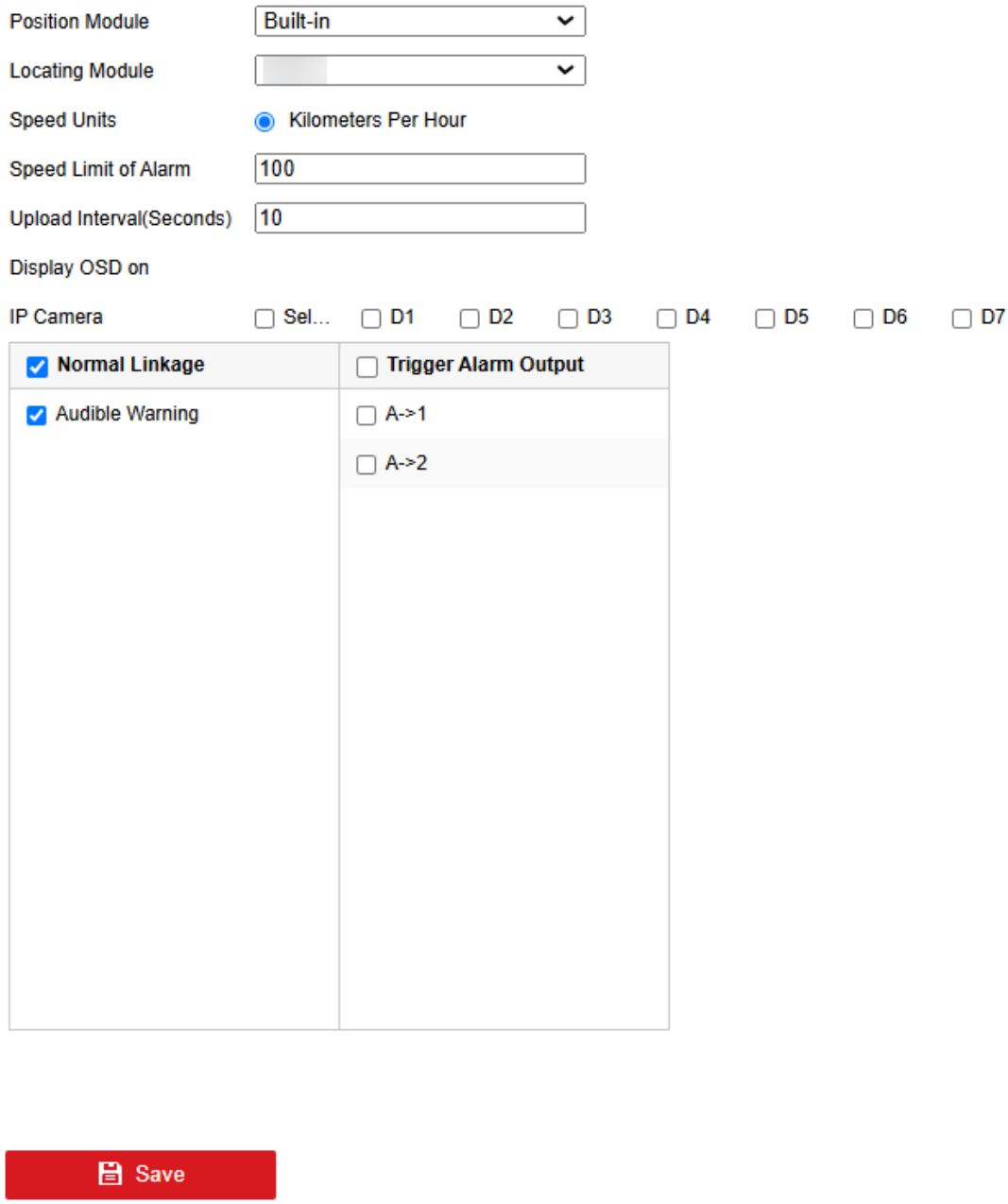

Figure 5-3 Set Satellite Positioning

3. Select **Speed Units** and enter **Speed Limit of Alarm**.

   When the speed of the vehicle installed with the device is higher than the set value, the selected alarm linkage will be triggered.

4. Enter **Upload Interval**.

   The device will upload the positioning information to the connected platform according to the set interval.

5. Select the camera(s) to overlay the positioning information.
6. Select the linkage action (**Audible Warning**) for the speeding alarm, and the alarm output channel(s).
7. Click **Save**.
8. **Optional:** Click **Location Status** to view the positioning status.

5.4 Set Vehicle Deployment

You can add blocklist and allowlist vehicles to the device to realize vehicle deployment.

Steps

1. Go to **Param Config → Advanced Settings → Vehicle Deployment → Vehicle Deployment** .

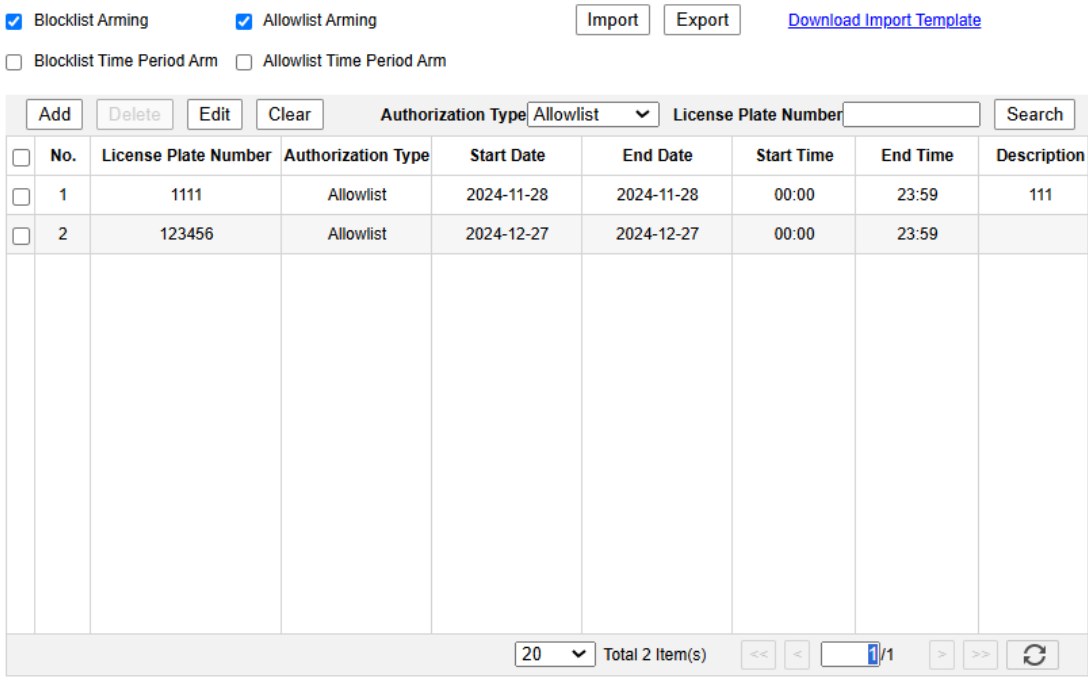

Figure 5-4 Vehicle Deployment

2. Check **Blocklist Arming** or **Allowlist Arming**.
3. **Optional:** Check **Blocklist Time Period Arm** or **Allowlist Time Period Arm** to set specific arming time periods.

Note

After enabling the two functions, you can set the arming time period while adding an item, and the arming will be performed within the set time period. Otherwise, the arming will be performed all day long.

Example

If you check **Blocklist Time Period Arming** and set the arming time period between 8:00 and 9:00, the arming will be performed between the set time period. If you don't check **Blocklist Time Period Arming**, the arming will be performed all day long by default even though you set the time period while adding the item.

4. Add arming vehicles.

Batch Import	a. Click **Download Import Template** to download the import template and fill in relevant information. b. Click **Import**. Click **Browse** to select the file from the computer, and click **Import** to import the file to the device.
Manual Add	a. Select **Authorization Type**. b. Click **Add**. c. Enter **License Plate Number**, and set the specific date and time. d. Click **OK**.

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

Search Data	Click **Search** after selecting **Authorization Type** or entering the license plate number to view relevant data.
Edit Data	Check the item to be edited and click **Edit** to edit this item.
Delete Data	Check the item(s) to be deleted and click **Delete** to delete the item(s).
Export Data	Check the item(s) to be exported and click **Export** to export the data to the computer.

5.5 Set Capture Parameters

5.5.1 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

1. Go to **Param Config → Picture Settings → Picture Composition** .
2. Select a camera and enable the function.

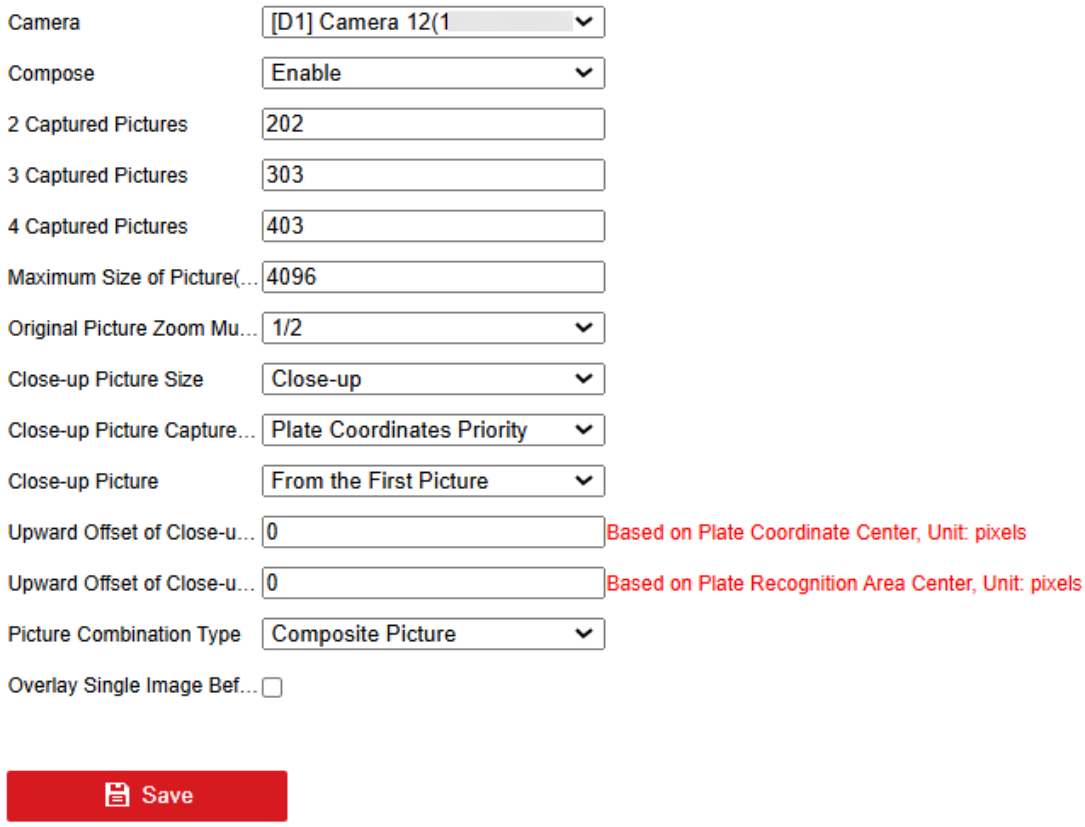

Figure 5-5 Set Picture Composition

3. Set composition types for different picture quantities.
4. Set other composition parameters.

Maximum Size of Picture

The max. size of the composite picture.

Original Picture Zoom Multiple

The zooming multiple for the pictures to be composed.

Close-up Picture Size

It is recommended to select **Panorama** for the large scene.

Close-up Picture Capture Strategy

If the camera can recognize the license plate coordinates, you're recommended to select **Plate Coordinates Priority** to recognize the close-up pictures according to the license plate coordinates. If the camera cannot recognize the license plate coordinates, you're recommended to select **Forced Plate Recognition Area** to recognize the close-up pictures.

Close-up Picture

The camera may collect multiple continuous captured pictures for the same target. Select the No. of the picture from which the close-up picture will be snapshot.

Upward Offset of Close-up Center

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.

Picture Composition Type

If you select **Composite & Original & Close-up Picture**, an original picture and a close-up picture will be saved in addition to the composite picture. You can select **Original Picture Information** to save the selected No. of the original pictures. If you select **merge And Transparent**, all the original pictures will be saved in addition to the composite picture.

Overlay Single Image Before Composition

Enable the function to overlay characters on the single pictures before composition.

5. **Optional:** Click **Copy to** to copy the settings to other channels.
6. Click **Save**.

5.5.2 Set Single Picture Overlay

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

Before You Start

Go to **Param Config → System → Camera Management → Camera Parameter** to select **Camera Type** as **Intelligent Traffic Camera**.

Steps

1. Go to **Param Config → Picture Settings → Single Overlay** .
2. Select the single picture channel.
3. Enable **Text Overlay**.

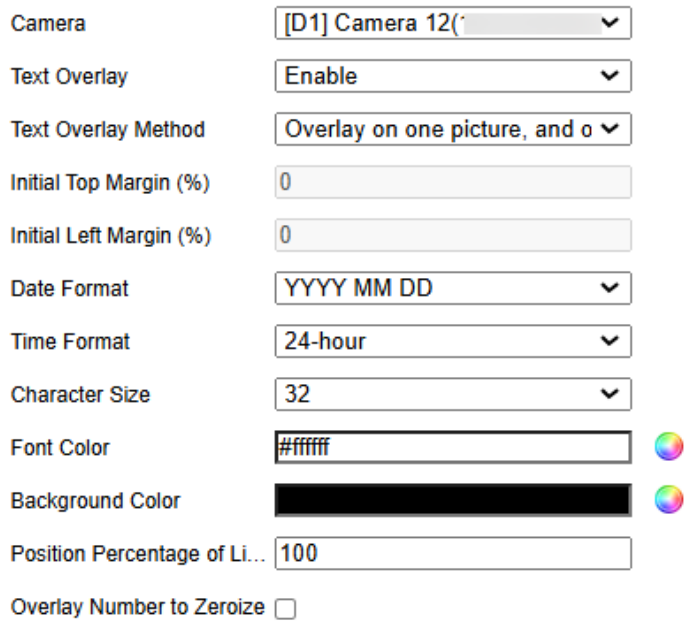

Figure 5-6 Set Single Picture Overlay

4. Select **Text Overlay Method** according to your needs.
5. Set the other parameters.

   Initial Top/Left Margin

   The parameters are available when you select to overlay information inside the picture. It is the percentage that the overlaid information will start from the top/left of the picture. For example, if you set the percentage to 50, the overlaid information will start from half of the picture width and height.

   Background Color

   Set the background color of the overlaid information when you select to overlay information outside the picture.

   Position Percentage of Line Break

   Set the percentage that the overlaid information will start from a new line. For example, if you set the percentage to 90, the overlaid information will start from a new line if the content has already occupied 90% of the picture width from the left.

   Overlay Number of Zeroize

   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.
6. Select the overlay information from the list.

Note

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

7. Set the overlay information.

View Original Type	You can view the default overlay information.
Set Overlay Type	You can edit the type.
Set Space number	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
Set 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.

8. Click **Save**.

5.5.3 Set Composite Picture Overlay

If you want to overlay information on the composite pictures, set composite picture overlay.

Before You Start

Go to **Param Config → System → Camera Management → Camera Parameter** to select **Camera Type** as **Intelligent Traffic Camera**.

Steps

1. Go to **Param Config → Picture Settings → Composite Overlay** .
2. Select the composite picture channel.
3. Enable **Text Overlay**.

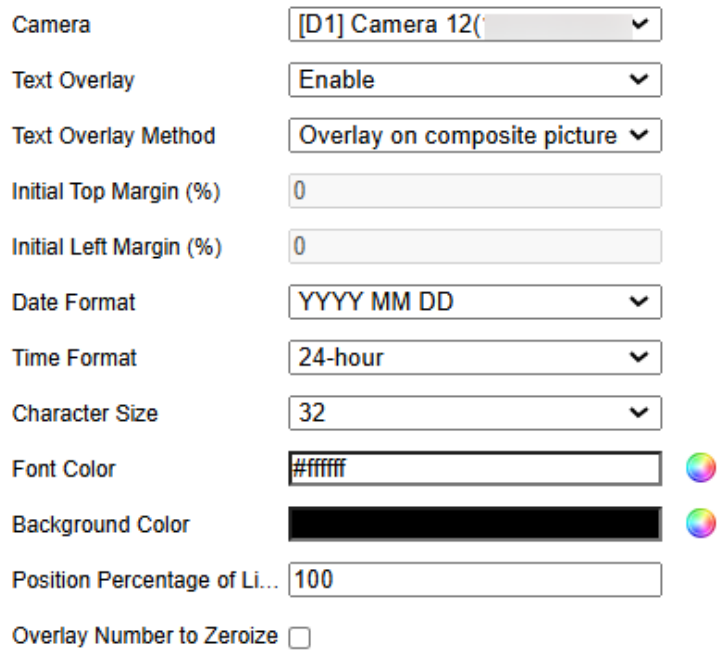

Figure 5-7 Set Composite Picture Overlay

4. Select **Text Overlay Method** according to your needs.
5. Set the other parameters.

   Initial Top/Left Margin

   The parameters are available when you select to overlay information inside the picture. It is the percentage that the overlaid information will start from the top/left of the picture. For example, if you set the percentage to 50, the overlaid information will start from half of the picture width and height.

   Background Color

   Set the background color of the overlaid information when you select to overlay information outside the picture.

   Position Percentage of Line Break

   Set the percentage that the overlaid information will start from a new line. For example, if you set the percentage to 90, the overlaid information will start from a new line if the content has already occupied 90% of the picture width from the left.

   Overlay Number of Zeroize

   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.
6. Select the overlay information from the list.

Note

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

7. Set the overlay information.

View Original Type	You can view the default overlay information.
Set Overlay Type	You can edit the type.
Set Space number	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
Set 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.

8. Click **Save**.

5.5.4 Set Camera Matching

The checkpoint data of different channels can be combined via camera matching to make it convenient to view the data.

Before You Start

The combined cameras should be installed at the adjacent locations and connected to the same device.

Steps

1. Go to **Param Config → Advanced Settings → Camera Matching → Camera Matching** .

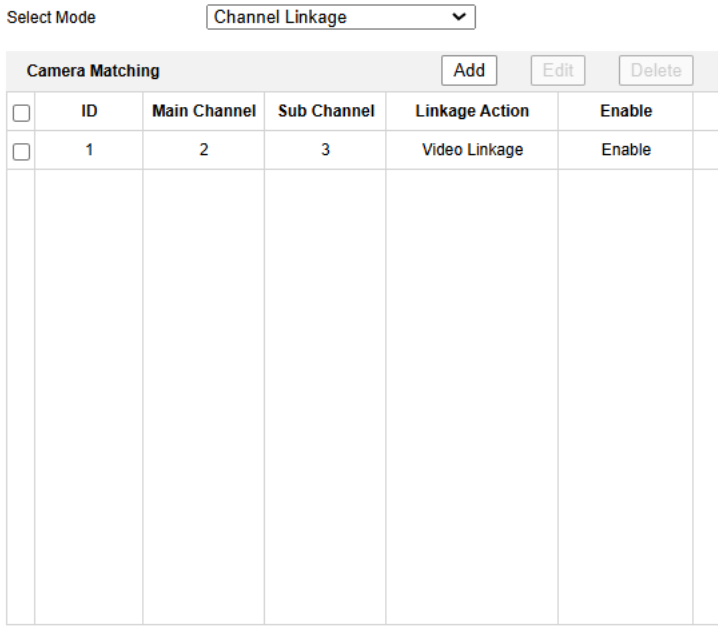

Figure 5-8 Set Camera Matching

2. Select mode as **Channel Linkage**.
3. Click **Add**.
4. Check **Enable**.
5. Select **Linkage Action** as **Video Linkage**.

   The vehicle will be linked according to the license plate.
6. Set the main and sub-channels.

   Note

   If the data of the main and sub-channels match, the pictures of the sub-channel will be combined to the main channel, and only the combined data (including 2 pictures) of the main channel will be displayed in picture search.
7. Click **OK**.
8. **Optional:** You can also do the following operations.

Edit Data	Check the item to be edited and click **Edit** to edit this item.
Delete Data	Check the item(s) to be deleted and click **Delete** to delete the item(s).

5.6 Set Violation Dictionary

Violation dictionary defines corresponding codes of violation types, and it is convenient for violation recognition.

Steps

1. Go to **Param Config → Dictionary Settings** .
2. Select a violation type.
3. Check the data and click **Edit** to edit the code.
4. **Optional:** You can also do the following operations.

Add Click **Add** to add custom acts and codes.

Delete Check the added data and click **Delete** to delete the data.

Note

The default data in the dictionary cannot be deleted.

Reset Click **Reset** to restore the dictionary to the factory settings, and all the custom data will be cleared.

Chapter 6 Live View and Local Configuration

6.1 Live View

6.1.1 Start/Stop Live View

Start/stop the live view of cameras.

Start Live View

Double-click the camera in the camera list on the left side of the live view interface to start a camera live view.

Note

If you want to display a camera live view in a specific split window, please select the split window first, and then double-click the camera to start live view. The display window is only set for once, and you need to set it again when you start live view next time.

Click to start all live view.

Stop Live View

When the camera starts live view, double-click the camera in the camera list on the left side of the live view interface to stop live view.
Click to stop all live view.

6.1.2 Divide Window and Switch Page

Select window division if you need to switch the single or multi-window live view mode, and view the camera live view of all pages via switching the page.

Divide Window

Click to select the live view window division mode according to the actual needs.

Switch Page

When the number of divided windows is less than the cameras, click ← and → to switch page and view the camera live view of all pages.

6.1.3 Select Stream Type

The device supports the dual-stream technology, including a main stream and a sub-stream. The main stream stands for a high-resolution and high bit rate stream, mainly used for storing

recordings. The sub-stream stands for a low-resolution and low bit rate stream, mainly used for bandwidth-saving network transmission.

Click / in the channel list to select the stream type.

6.1.4 Capture Manually

Capture live view pictures and save them to your computer.

Steps

1. Click **Live View**.
2. Double click the channel name on the left to enable live view.
3. Click .
4. Name and save the captured pictures.

Note

Go to **Param Config → Local** to view the saving path of snapshots in live view.

6.1.5 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:** Go to **Param Config → Local** to view the saving path of record files.

6.1.6 Enable/Disable Audio

Enable the audio if necessary after relevant configuration of a connected audio input device.

Click to enable and adjust the audio. Click the icon again to mute the audio.

6.1.7 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.

6.1.8 Display in Full Screen

You can display the live view image in full screen.

On **Live View** interface, click to display the live view image in full screen.

Press **esc** on the keyboard to exit the full screen mode.

6.2 PTZ Control

6.2.1 PTZ Control Panel

If a PTZ camera is connected to the device ,you can click **Live View** and control PTZ cameras via PTZ control panel.

Note

- PTZ control panels may vary with the camera models. The actual device prevails.
- PTZ camera supports power-down memory. After PTZ camera suddenly loses power or reboots, it can automatically go back to the former position.

Table 6-1 Buttons Description

Icon	Description	Icon	Description
	Direction buttons		Auto-scan button
	Zoom -		Zoom +
	Focus +		Focus -
	Iris +		Iris -
	Display the PTZ control panel		Hide the PTZ control panel
	Control the PTZ speed		Auxiliary focus
	Menu	/	/

Note

Other functions are reserved.

6.2.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click .

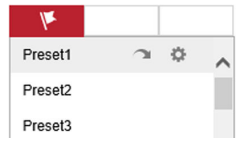

Figure 6-1 Set Preset

2. Operate the direction buttons of PTZ control to adjust PTZ to the desired position, and adjust the focus, zoom, etc., to get the desired scene.
3. Select the preset to set.
4. **Optional:** You can also do the following operations.

   Click Set preset according to prompt.

   Click Call the preset, then PTZ will turn to the set direction.

6.3 Local Configuration

Go to **Param Config → Local** to set the live view parameters.

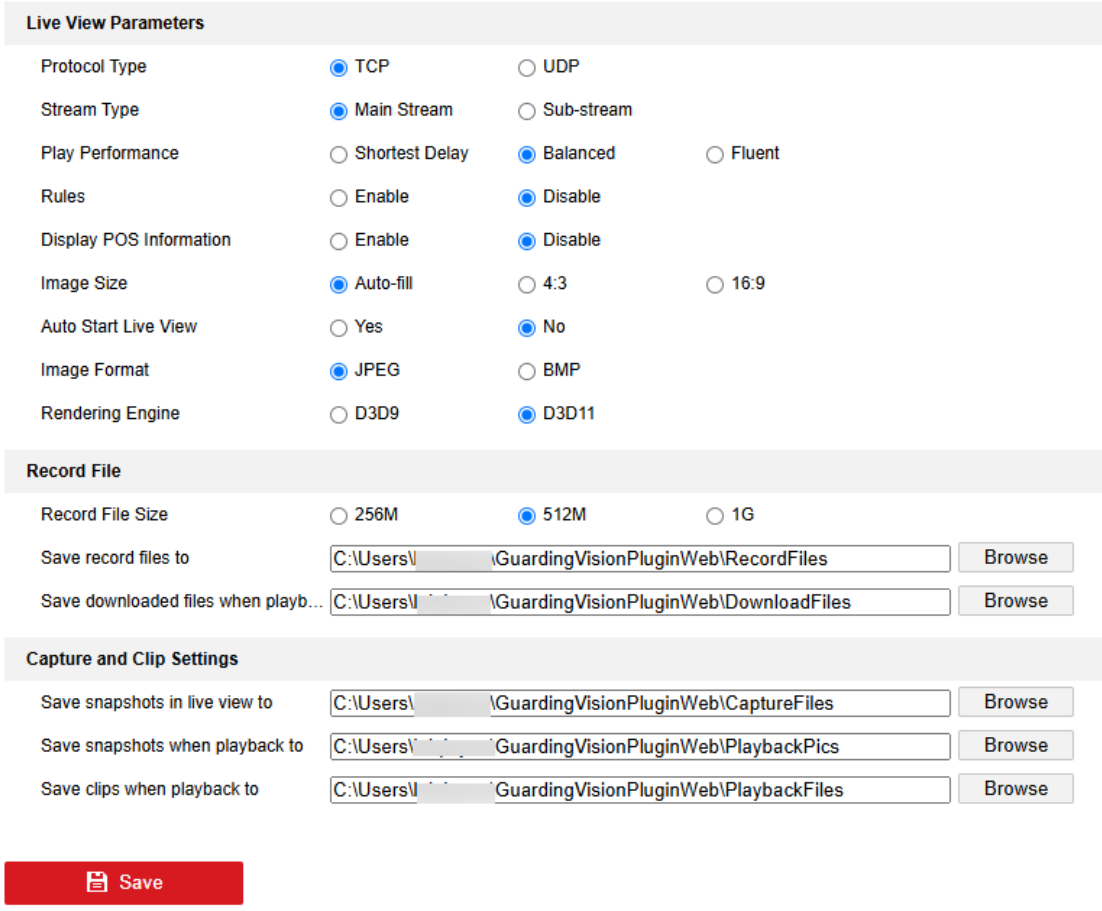

Figure 6-2 Local Configuration

Protocol Type

TCP

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

UDP

Provides real-time audio and video streams.

Stream Type

The stream type decides the definition of live view image.

Main Stream

Provides the best resolution and frame rate the device can do.

Sub-stream

Provides comparatively low resolution options.

Play Performance

Shortest 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.

Fluent

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

Rules

If you select **Enable**, set rule information will be displayed on the live view interface.

Display POS Information

If you select **Enable**, the POS information of the capture camera will be displayed on the live view interface.

Image Size

Select according to your needs.

Auto Start Live View

If you select **Yes**, you can view the camera live view image after login the browser. If you select **No**, you need to start live view manually after login the device.

Image Format

Set the saving format of captured pictures.

JPEG

The picture will be compressed.

BMP

The picture will not be compressed.

Rendering Engine

Select the rendering API of the browser. D3D9 uses fixed rendering pipeline. D3D11 uses programmable graphics pipeline, in which the shader replaces the traditional fixed rendering pipeline to improve visual effects and enhance the picture quality.

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 in live view interface.

Save downloaded files when playback to

Set the saving path for the downloaded files in playback mode.

Save snapshots in live view to

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

Save snapshots when playback to

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

Save clips when playback to

Set the saving path for the clips in playback mode.

Chapter 7 Storage

7.1 Format Disk

Format the disk when the storage is abnormal or a new disk is installed.

Steps

Caution

Formatting the disk will cause the disk data loss. Back up the data first.

1. Go to **Param Config → Storage → Storage Management → HDD Management** .
2. Check the HDD No. needs to be formatted.
3. Click **Format**.

7.2 Set Quota

Set the picture ratio in the storage.

Steps

1. Go to **Param Config → Storage → Storage Management → Picture Quota** .
2. Set the capacity for saving picture according to the actual needs.
3. Click **Save**.

7.3 Detect HDD

Detect HDD regularly to avoid data loss due to HDD damage.

Steps

1. Go to **Param Config → Storage → Storage Management → HDD Detection** .

S.M.A.R.T. Detection	Detect and report on various indicators of reliability in the hopes of anticipating failures.
Bad Sector Test	Detect the block capacity of the HDD.

2. Select **HDD No.** and **Self-test Type**, and click **Start Detecting**.

Result

Decide whether to use the HDD any more according to the detection result. If there are too many bad sectors, change the HDD in time.

7.4 Set Holiday

Set holiday for special days that alarms will not be triggered.

Steps

1. Go to **Param Config → Storage → Advanced Settings → Holiday** .

Holiday Settings — The periods of holiday cannot be overlapped.

Enable	No.	Holiday Name	Type	Start Date	End Date	Edit
☐	1	Holiday1	By Month	1.Jan.	1.Jan.	
☐	2	Holiday2	By Month	1.Jan.	1.Jan.	
☐	3	Holiday3	By Month	1.Jan.	1.Jan.	
☐	4	Holiday4	By Month	1.Jan.	1.Jan.	
☐	5	Holiday5	By Month	1.Jan.	1.Jan.	
☐	6	Holiday6	By Month	1.Jan.	1.Jan.	
☐	7	Holiday7	By Month	1.Jan.	1.Jan.	
☐	8	Holiday8	By Month	1.Jan.	1.Jan.	
☐	9	Holiday9	By Month	1.Jan.	1.Jan.	
☐	10	Holiday10	By Month	1.Jan.	1.Jan.	
☐	11	Holiday11	By Month	1.Jan.	1.Jan.	
☐	12	Holiday12	By Month	1.Jan.	1.Jan.	
☐	13	Holiday13	By Month	1.Jan.	1.Jan.	

Save

Figure 7-1 Set Holiday

2. Check the holiday date to set.
3. Set the holiday parameters.
   1) Click .
   2) Set **Holiday Name**, **Type**, **Start Date** and **End Date**.
   3) Click **OK**.
4. **Optional:** Repeat the previous step to set other holidays.
5. Click **Save**.

Chapter 8 Record and Playback

8.1 Set Recording Schedule

Set recording schedule if you need the camera to record automatically according to the set schedule.

Before You Start
Install and format the storage media.

Steps
1. Go to **Param Config → Storage → Schedule Settings → Recording Schedule** .

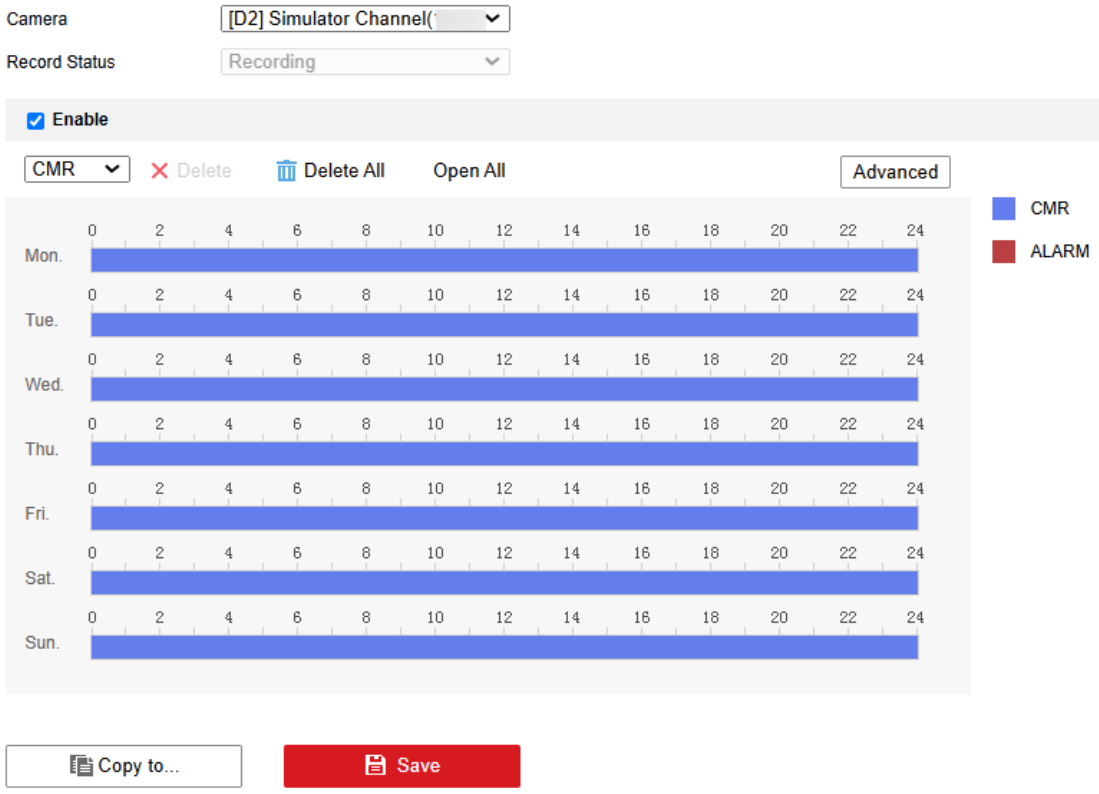

Figure 8-1 Set Recording Schedule

2. Select the camera.
3. Check **Enable**, and select the record type.

CMR

The camera will start recording automatically during the set time period, and stop recording automatically outside the set time period.

ALARM

During the set time period, when the capture alarm is triggered, the camera will start recording automatically.

4. **Optional:** Click **Advanced** to set the camera record parameters.

Record Audio

Enable the function to record audio.

Redundant Recording

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

Pre-record Time

The time to start recording before the scheduled time.

Post-record

The time to stop recording after the scheduled time.

Video Expiry Date

Automatically delete video files after the scheduled time. **0** means that video files won't be deleted, but will be automatically overwritten after enabled overwritten record.

5. Drag the cursor on the time bar to set a recording time.

Note

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

6. Adjust the recording time.
   - Click **Open All** to enable all-day recording of all the date.
   - Click a set recording period and enter the start time and end time in the pop-up window.
   - Drag two ends of the set recording period bar to adjust the length.
   - Drag the whole set recording period bar and relocate it.
7. **Optional:** Delete recording periods.
   - Click a set recording period and click **Delete** in the pop-up window.
   - Click a set recording period and click **Delete** on the record configuration interface.
   - Click **Delete All** to delete all the recording schedule.
8. **Optional:** Click to copy set recordings to other days.
9. **Optional:** Click **Copy to...**, check the camera, and click **OK**.
10. Click **Save**.

8.2 Play Back Video

You can play back the record files saved in the storage media (HDD, etc.).

Steps

1. Click **Playback**.
2. Select a camera.
3. Select the file date, and click **Search**.
   - Drag time bar and put the yellow line at the time point that you need.

- Enter the specific time at **Set Playback Time**.

4. Click ▶ to play back the file.
5. **Optional:** You can also do the following operations.

⏸	Pause		Start playback for selected camera.
	Split the playback window, and play back multiple cameras simultaneously.	■	Stop playback for selected camera.
	Fast forward.		Slow forward.
	Stop playback for all cameras.		Capture pictures.
	Reversed.		Enable/disable audio.
	Full screen.	-	-

Note

- For the captured picture of playback saving path, refer to **Save snapshots when playback to** in **Param Config → Local** .
- Operations and buttons vary with different models. The actual device prevails.

8.3 Backup

8.3.1 Back up Video

Download videos to a local path.

Steps

1. Click **Playback**.
2. Click .
3. Select **Camera**.
4. Select download type.
   - If you need to search video by date, select **Download by Date**, and select the date.
   - If you need to search video by file type, select **Download by File**, and select file type and search time.
5. Select **File Type**.
6. Click **Search**.
7. Check videos to download and click **Download**.
8. For the video saving path, refer to **Save downloaded files when playback to** in **Param Config → Local** .

8.3.2 Back up Clipped Video

Clip videos and save them to a local path.

Steps

1. Click **Playback**.
2. Select a camera and date.
3. Click **Search**.
4. Play the video.
5. Drag time bar to the clip start time and click to start clipping.
6. Drag time bar to the clip end time and click to stop clipping.
7. Go to **Param Config → Local** to view the saving path of video clips.

Chapter 9 Encoding and Display

9.1 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 **Param Config → Video & Audio → Video** .
2. Select a camera.
3. Set the parameters for different streams.

Stream Type

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.

Video Type

Select the video type to video & audio when you need taping while recording. Select video when you only need record.

Note

The device only supports audio can select video & audio. The actual device prevails.

Resolution

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

Bitrate Type and Max. Bitrate

Select the bitrate type to constant or variable. Constant bitrate means that the stream is compressed and transmitted at a comparatively fixed bitrate. Variable bitrate means that the device automatically adjust the bitrate under the set **Max. Bitrate**.

Image Quality

When bitrate type is variable, you can select video quality according to actual needs. The higher the video quality is, the higher requirements of the network bandwidth.

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.

Video Encoding

The device supports multiple video encoding types. 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.

4. **Optional:** Click **Copy to** to copy the settings to other channels.
5. Click **Save**.

9.2 Set Audio Encoding Parameters

When the target platform or the device does not support the initial audio encoding mode, you can switch the audio encoding mode.

Before You Start

The device supports embedded audio or the audio peripherals have been connected to the device.

Steps

1. Go to **Param Config → Video & Audio → Audio** .
2. Select **Audio Encoding**.

Note

The selected audio encoding mode should be consistent with that of the embedded audio or peripherals.

3. Click **Save**.

9.3 Set Image Parameters

Set image parameters to adjust brightness and contrast.

Steps

1. Go to **Param Config → Image → Display Settings** .
2. Select a camera.
3. Set the parameters to obtain clear images.

Brightness

The brightness of the image.

Contrast

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

Saturation

The colorfulness of the image color.

Hue

Select the range to adapt to the display.

4. **Optional:** Click **Restore Default Settings** to restore parameters to the default status.

9.4 Set OSD

You can customize OSD information on the live view.

Steps

Note

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

1. Go to **Param Config → Image → OSD Settings** .
2. Select a camera.
3. Enter **Camera Name**, and select **Time Format** and **Date Format**.
4. Check **Display Name**, **Display Date**, and **Display Week** according to actual needs.
5. **Optional:** Check the text overlay No. and enter contents according to your needs.
6. Drag the red frame overlaid on the live view image to adjust the OSD information positions.
7. Click **Save**.

Result

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

Chapter 10 Platform Connection

10.1 Set Remote Host

Set remote host when the device needs to transmit data to the central control platform.

Before You Start

Set the remote host, and ensure the device can communicate normally with the remote host.

Steps

1. Go to **Param Config → Platform Settings → Upload to Remote Host** .
2. Select a remote host.

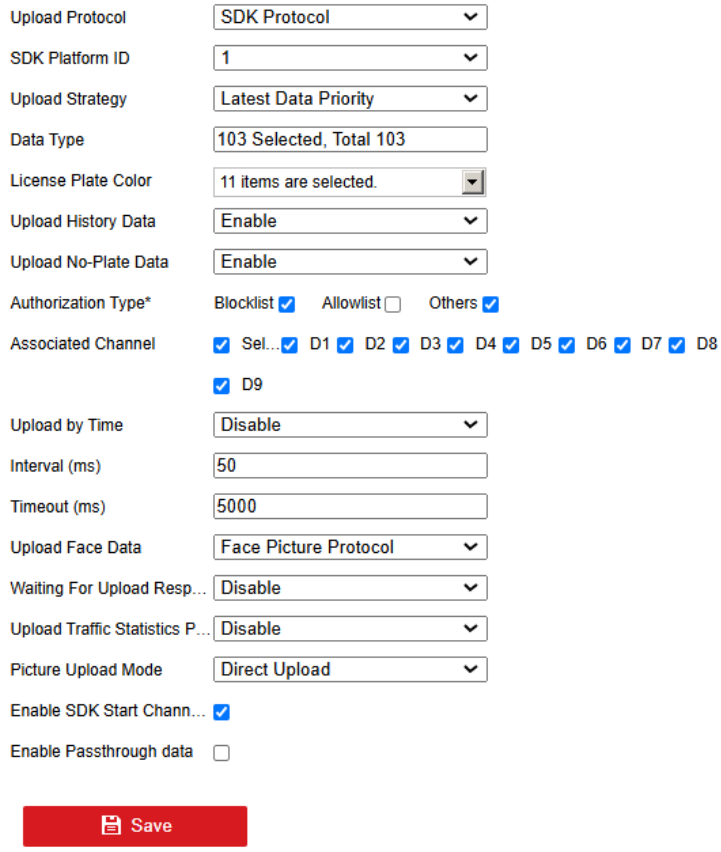

Figure 10-1 Set Remote Host

Note

The supported number of remote hosts varies with different devices. The actual interface prevails.

3. If you select **Upload Protocol** as **SDK Protocol**, follow the steps below.

1) Select **SDK Platform ID** according to the actual communication protocol.
2) Select **Upload Strategy** as **Latest Data Priority**.
3) Click the text field behind **Data Type** to check the upload data type(s) and select specific upload data.
4) Set the parameters below.

Upload History Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. When enabled, historical data will be uploaded again.

Upload No-Plate Data

Upload data of vehicles without license plates to the remote host.

Authorization Type

Upload the armed blocklist or allowlist vehicle information set in **Param Config → Advanced Settings → Vehicle Deployment → Vehicle Deployment** to the remote host. Select **Others** for the vehicle types except the blocklist or allowlist vehicle type.

Associated Channel

Select the channel(s) to upload data. The interface will show the max. number of channels allowed by the device. You can go to **Param Config → System → Camera Management → IP Camera** to view the corresponding camera(s).

Upload by Time

When enabled, data will be uploaded within the time period between the set upload start time and the set upload end time. Two time periods are supported. Select **Time Type**. The device time when the picture is captured and the actual time when the picture is captured may be different. If you select **Device Time**, the captured pictures at the device time during the set time period will be uploaded to the platform. If you select **Capture Time**, the captured pictures at the actual capture time during the set time period will be uploaded to the platform.

Interval

The interval between 2 data uploads.

Timeout

When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as historical data and uploaded according to historical data rule.

Upload Face Data

The device will upload the face pictures data according to the face picture protocol used by the camera. For the platform not supporting face picture protocol, you can select **License Plate Protocol** to guarantee the captured pictures can be uploaded to the platform.

Waiting For Upload Respond

When enabled, if the platform does not respond to the data, it means data upload is failed.

Note

The function is effective only when the platform supports upload response.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Picture Upload Mode

Direct Upload means to upload the captured pictures and alarm information to the platform directly.

Enable SDK Start Channel No.

You can enable the function to make SDK protocol platforms of different versions compatible. Disable the function for the platform not supporting the analog signal channel No. reservation.

Enable Passthrough data

Enable the function to upload the alarm data which cannot be handled by the device to the platform host directly.

4. If you select **Upload Protocol** as **ISUP**, follow the steps below.

1) Select **ISUP platform ID** according to the actual communication protocol.
2) Click the text field behind **Data Type** to check the upload data type(s) and select specific upload data.
3) Set the parameters below.

Upload History Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. When enabled, historical data will be uploaded again.

Upload No-Plate Data

Upload data of vehicles without license plates to the remote host.

Authorization Type

Upload the armed blocklist or allowlist vehicle information set in **Param Config → Advanced Settings → Vehicle Deployment → Vehicle Deployment** to the remote host. Select **Others** for the vehicle types except the blocklist or allowlist vehicle type.

Associated Channel

Select the channel(s) to upload data. The interface will show the max. number of channels allowed by the device. You can go to **Param Config → System → Camera Management → IP Camera** to view the corresponding camera(s).

Upload by Time

When enabled, data will be uploaded within the time period between the set upload start time and the set upload end time. Two time periods are supported. Select **Time Type**. The device time when the picture is captured and the actual time when the picture is captured may be different. If you select **Device Time**, the captured pictures at the device time during

the set time period will be uploaded to the platform. If you select **Capture Time**, the captured pictures at the actual capture time during the set time period will be uploaded to the platform.

Interval

The interval between 2 data uploads.

Timeout

When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as historical data and uploaded according to historical data rule.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Picture Upload Mode

Enable cloud storage and set **Picture Server ID** to upload the captured pictures to the cloud storage server to generate URL, and then upload URL and alarm information to the platform.

Enable SDK Start Channel No.

You can enable the function to make SDK protocol platforms of different versions compatible. Disable the function for the platform not supporting the analog signal channel No. reservation.

5. If you select **Upload Protocol** as **HTTP Protocol**, follow the steps below.

1) Select **HTTP Platform ID** according to the actual communication protocol.
2) Click the text field behind **Data Type** to check the upload data type(s) and select specific upload data.
3) Set the parameters below.

Upload History Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. When enabled, historical data will be uploaded again.

Upload No-Plate Data

Upload data of vehicles without license plates to the remote host.

Authorization Type

Upload the armed blocklist or allowlist vehicle information set in **Param Config → Advanced Settings → Vehicle Deployment → Vehicle Deployment** to the remote host. Select **Others** for the vehicle types except the blocklist or allowlist vehicle type.

Associated Channel

Select the channel(s) to upload data. The interface will show the max. number of channels allowed by the device. You can go to **Param Config → System → Camera Management → IP Camera** to view the corresponding camera(s).

Upload by Time

When enabled, data will be uploaded within the time period between the set upload start time and the set upload end time. Two time periods are supported. Select **Time Type**. The device time when the picture is captured and the actual time when the picture is captured may be different. If you select **Device Time**, the captured pictures at the device time during the set time period will be uploaded to the platform. If you select **Capture Time**, the captured pictures at the actual capture time during the set time period will be uploaded to the platform.

Interval

The interval between 2 data uploads.

Timeout

When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as historical data and uploaded according to historical data rule.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Picture Upload Mode

Direct Upload

Upload the captured pictures and alarm information to the platform directly.

Cloud Storage

Enable cloud storage and set **Picture Server ID** to upload the captured pictures to the cloud storage server to generate URL, and then upload URL and alarm information to the platform.

Enable SDK Start Channel No.

You can enable the function to make SDK protocol platforms of different versions compatible. Disable the function for the platform not supporting the analog signal channel No. reservation.

6. Click **Data Upload Config** to set the relevant parameters.

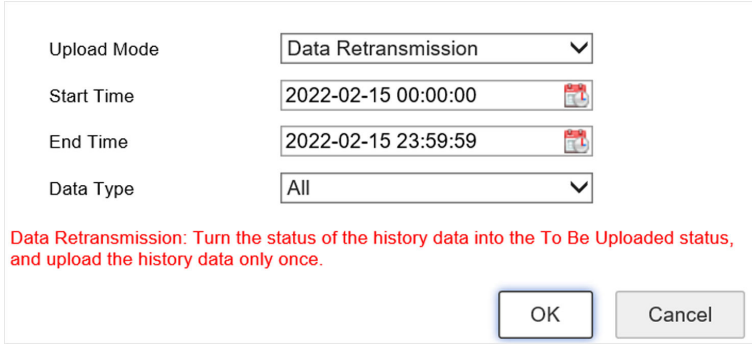

Figure 10-2 Set Data Upload

1) Select **Upload Mode**.

Data Retransmission

Change the status of the historical data into the To Be Uploaded status, and upload the historical data only once.

History Data Priority

Upload the historical data in the To Be Uploaded first.

Disable

Change the status of the historical data into the Not to Be Uploaded status, and do not upload these data.

2) Set **Start Time** and **End Time**.
3) Select **Data Type**.
4) Click **OK**.

7. Click **Save**.
8. **Optional:** Repeat the above steps if you need to set another remote host.

10.2 Set FTP

Set FTP parameters if you want to upload the captured pictures or recordings 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 **Param Config → Platform Settings → FTP Upload** .

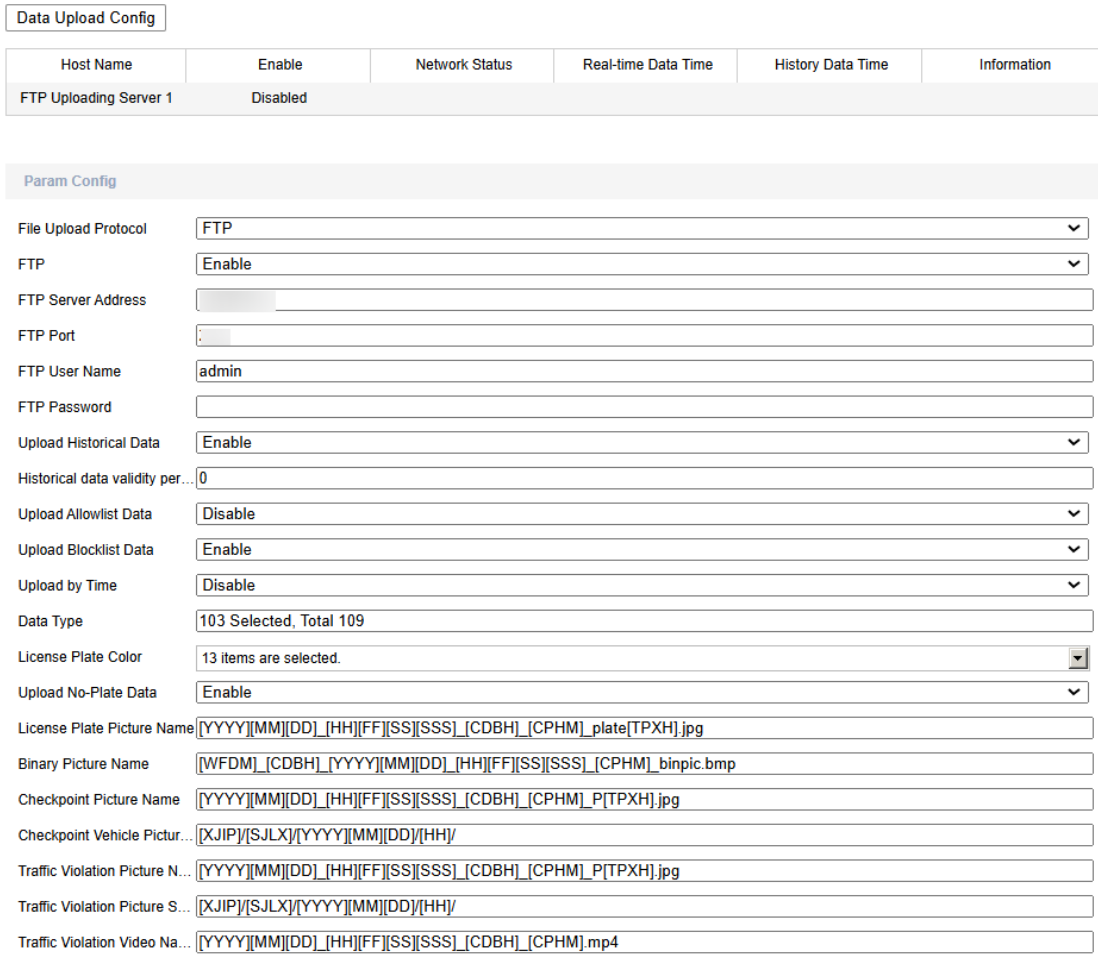

Figure 10-3 Set FTP

2. Select a FTP server.
3. Select **File Upload Protocol**.

Note

If you select **SFTP**, the files will be transmitted via encryption mode to guarantee security.

4. Set FTP parameters.
   1) Enable the FTP.
   2) Enter **FTP Server Address**, **FTP Port**, **FTP User Name**, and **FTP Password**.
5. Set upload parameters.

Upload Historical Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. After this function has been enabled, historical data will be uploaded again.

Upload Allowlist Data

Upload the information of allowlist vehicles set in **Param Config → Advance Settings → Vehicle Deployment → Vehicle Deployment** .

Upload Blocklist Data

Upload the information of blocklist vehicles set in **Param Config → Advance Settings → Vehicle Deployment → Vehicle Deployment** .

Upload by Time

After this function has been enabled, data will be uploaded within the time period between the set uploading start time and the set uploading end time.

Upload No-Plate Data

Upload data of vehicles without license plates to the FTP server.

6. Select **License Plate Color** and **Data Type**.
7. Edit the names and paths of the captured pictures or videos according to the actual needs.
8. Click **Data Upload Config** to set relevant parameters.

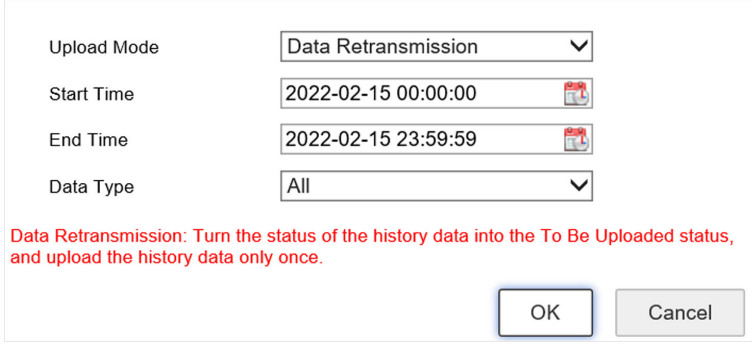

Figure 10-4 Set Data Upload

1) Select **Upload Mode**.

Data Retransmission

Change the status of the historical data into the To Be Uploaded status, and upload the historical data only once.

History Data Priority

Upload the historical data in the To Be Uploaded first.

Disable

Change the status of the historical data into the Not to Be Uploaded status, and do not upload these data.

2) Set **Start Time** and **End Time**.
3) Select **Data Type**.
4) Click **OK**.

9. Click **Save**.
10. **Optional:** Repeat the above steps to set another FTP.

10.3 Connect to SDK Platform

SDK is the platform access protocol. You can connect the device to the SDK platform to realize live view and data management via the platform.

Before You Start

Set the platform server first. Guarantee the network communication between the device and the platform is normal.

Steps

1. Go to **Param Config → Platform Settings → Remote Host Connection → SDK** .

Figure 10-5 Connect to SDK Platform

2. Select **SDK Platform ID**.
3. Check **Enable**.
4. Enter **IP Address** and **Port** of the device.

Note

The IP address and port should be consistent with those added on the platform.

5. Click **Save**.

10.4 Connect to ISUP Platform

ISUP 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 **Param Config → Platform Settings → Remote Host Connection → ISUP** .

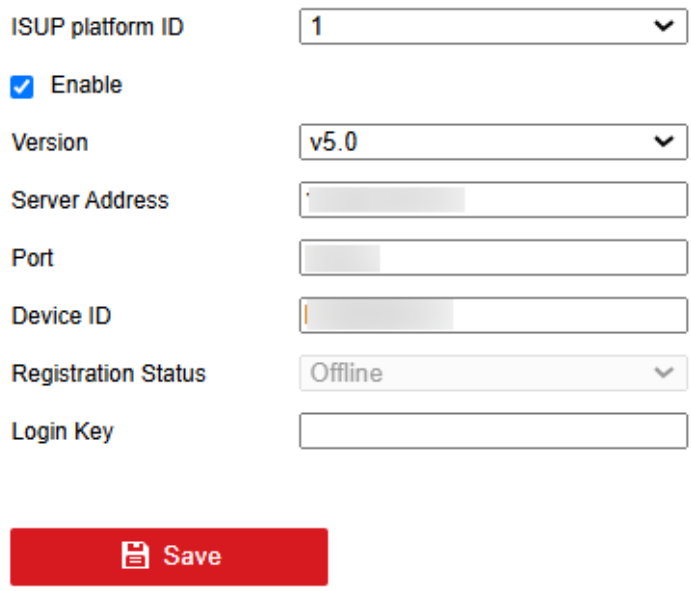

Figure 10-6 Connect to ISUP Platform

2. Select **ISUP platform ID**.
3. Check **Enable**.
4. Select **Version**.
5. Enter **Server Address**, **Port**, and **Device ID**.

Note

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

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

Note

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

10.5 Connect to HTTP Platform

You can connect the device to HTTP platform to upload the pictures and alarm data to the remote host platform.

Before You Start

The network communication between the device and the platform is normal.

Steps

1. Go to **Param Config → Platform Settings → Remote Host Connection → HTTP** .

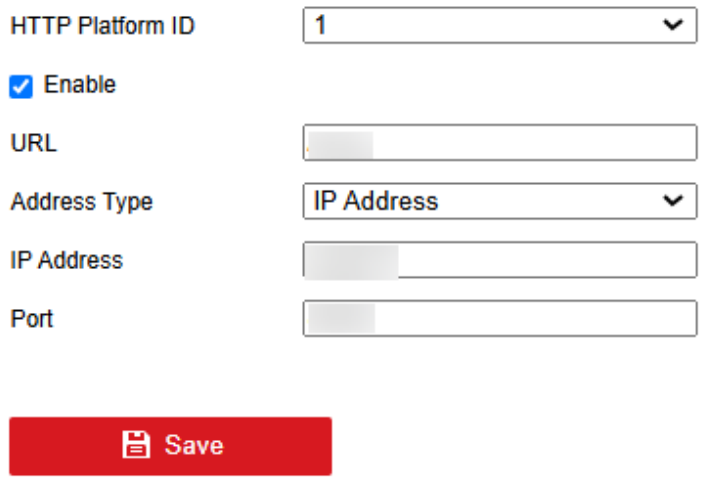

Figure 10-7 Connect to HTTP Platform

2. Select **HTTP Platform ID**.
3. Check **Enable**.
4. Set **URL** of the platform.
5. Select **Address Type** and set the corresponding parameters.
6. Click **Save**.

10.6 Set Cloud Storage

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

Before You Start

Arrange the cloud storage server.

Steps

1. Go to **Param Config → Platform Settings → Remote Host Connection → Cloud Storage** .

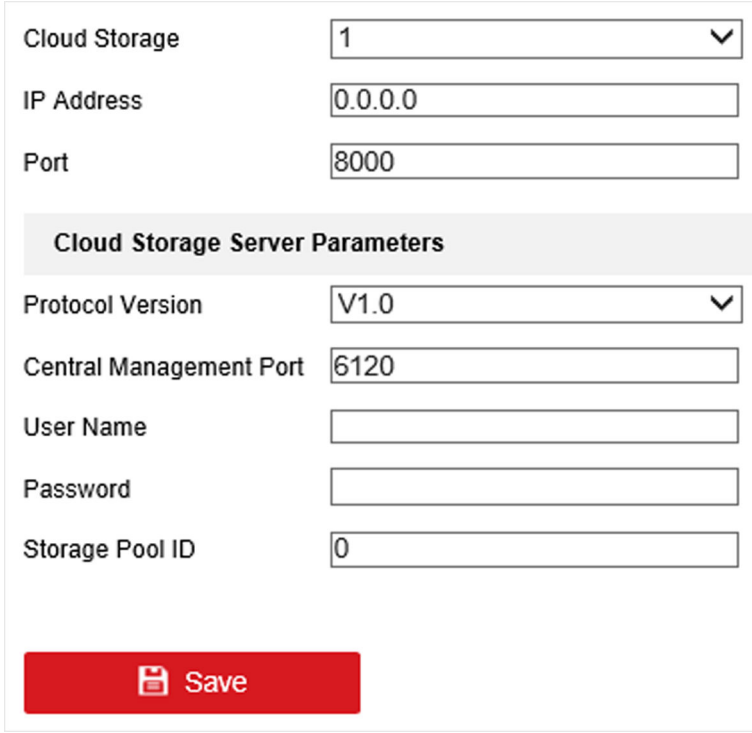

Figure 10-8 Set Cloud Storage

2. Select **Cloud Storage**.
3. Enter **IP Address** and **Port** of the cloud storage server.
4. Set cloud storage server parameters.

Protocol Version

Protocol version of the cloud storage server.

Note

The cloud storage server parameters vary with different protocol versions. The actual interface prevails.

Central Management Port

Central management HTTP port of the cloud storage server.

Storage Pool ID

Storage pool ID of uploaded files on the cloud storage server. Set it when you select **Protocol Version** as **V1.0/V2.0**.

User Name and Password

User name and password of the cloud storage server.

access_key

Key to access the cloud storage server. Set it when you select **Protocol Version** as **V2.0/V3.0**.

secret_key

Key to encrypt the data uploaded to the cloud storage server. Set it when you select **Protocol Version** as **V2.0/V3.0**.

5. Click **Save**.

Chapter 11 Alarm Congifuration

11.1 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Param Config → Event → Basic Event → Alarm Input** .

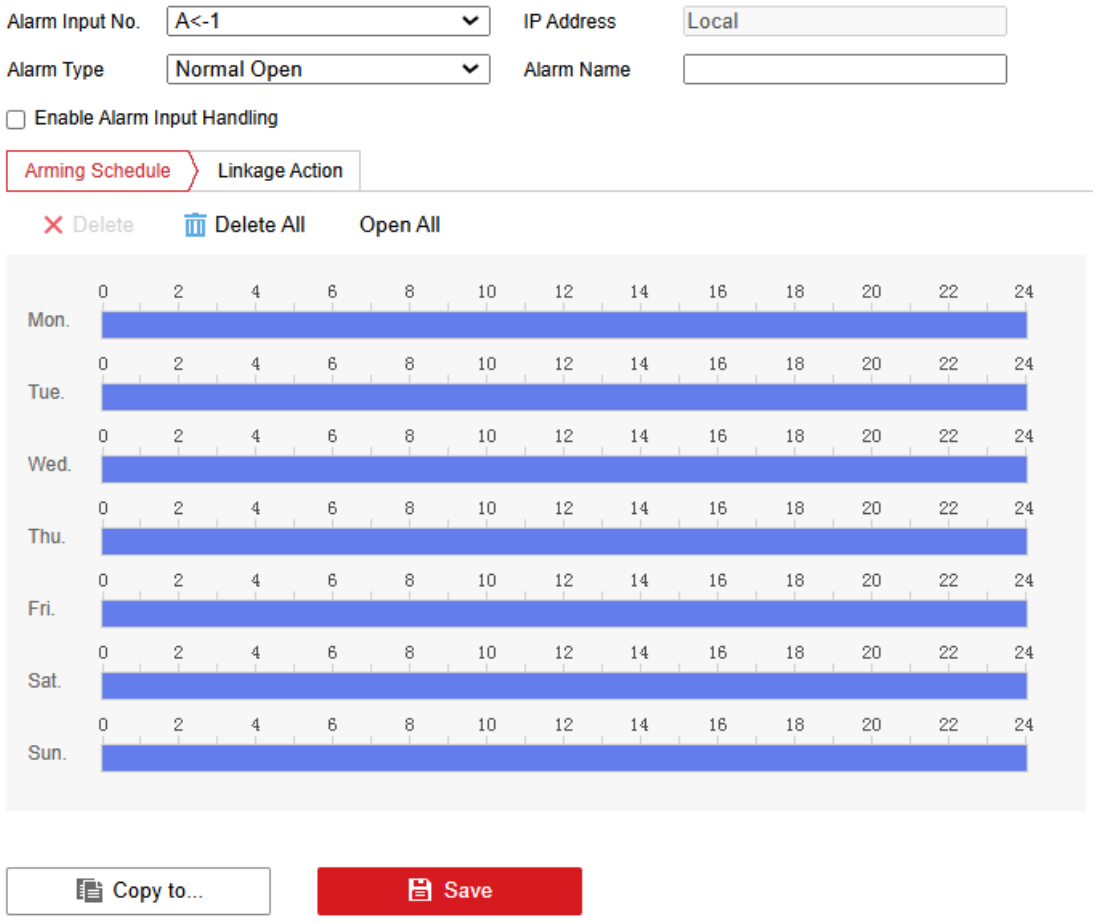

Figure 11-1 Set Alarm Input

2. Select **Alarm Input No.** and edit **Alarm Name**.

Note

If you select **Alarm Input No.** as **A<-1(Cabinet Door Alarm)** or **A<-2(Cabinet Door Alarm)** (options vary with different models), please go to **Param Config → Advanced Settings → Other Settings → Other Settings** to set **Cabinet Door Name** and **Cabinet Door No.**.

3. Select **Alarm Type** according to the alarm device type.
4. **Optional:** Check **Enable Alarm Input Handling**.

   If you enable the function, after the external connected alarm device alarms, it will trigger the camera to capture or record.
5. Refer to ***Set Recording Schedule*** for setting **Arming Schedule**.
6. Set **Linkage Action**.
   1) Select **Normal Linkage**.

      Audible Warning

      Generate an audible warning when an event occurs.

      Notify Surveillance Center

      Upload the alarm information to the surveillance center.

      Full Screen Monitoring

      Display the image from the alarm channel in full screen.
   2) Select the alarm output channel(s) to link the connected external alarm devices to trigger alarms when alarms occur.
   3) Select the channel(s) to start recording automatically when alarms occur.
   4) Select the PTZ linkage channel and the corresponding preset, patrol, or pattern No. to execute the selected PTZ actions when alarms occur.
7. **Optional:** Click **Copy to...** to copy the settings to other alarm input channels.
8. Click **Save**.

11.2 Set Alarm Output

Set alarm output to realize linkage alarm via external alarm device when the event occurs.

Before You Start

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Param Config → Event → Basic Event → Alarm Output** .

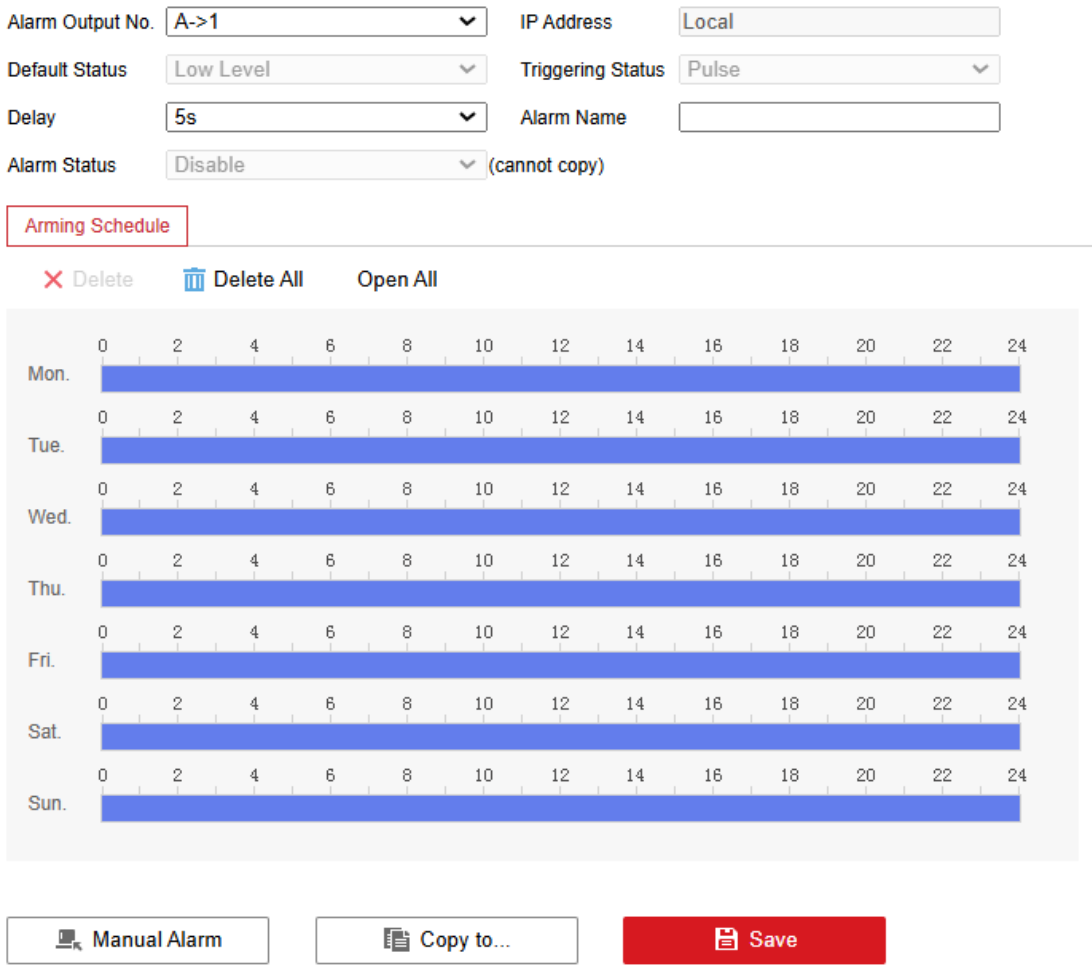

Figure 11-2 Set Alarm Output

2. Select **Alarm Output No.** and edit **Alarm Name**.
3. Select **Delay**.

   The device will disable alarm output signal after the set time. If you select **Manual**, you need to disable alarm output manually.
4. Refer to ***Set Recording Schedule*** for setting **Arming Schedule**.
5. Click **Manual Alarm** to enable manual alarm output. Set according to the actual needs.
6. **Optional:** Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

11.3 Set Exception Alarm

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

Steps

1. Go to **Param Config → Event → Basic Event → Exception** .
2. Select **Exception Type**.

   HDD Full

   The HDD storage is full.

   HDD Error

   Error occurs in HDD.

   Network Cable Disconnected

   The device is offline.

   IP Address conflicted.

   The IP address of current device is same as that of other device in the network.

   Illegal Login

   Incorrect user name or password is entered.

   Record/Capture Exception

   Exception occurs in record/capture.

   Vehicle Blocklist

   When vehicles in blocklist detected, alarm will be triggered.

   Vehicle Allowlist

   When vehicles in allowlist detected, alarm will be triggered.
3. Refer to for setting linkage method.
4. Click **Save**.

11.4 Set Camera Capture Alarm

For the device containing alarm output interfaces, when the connected cameras capture pictures, the alarm output interfaces will output relay signals to link the external alarm devices to alarm.

Before You Start

Make sure the external alarm device has been connected to the alarm output interface of the device.

Steps

1. Go to **Param Config → Event → Basic Event → The camera snaps the alarm** .
2. Check **Enable**.

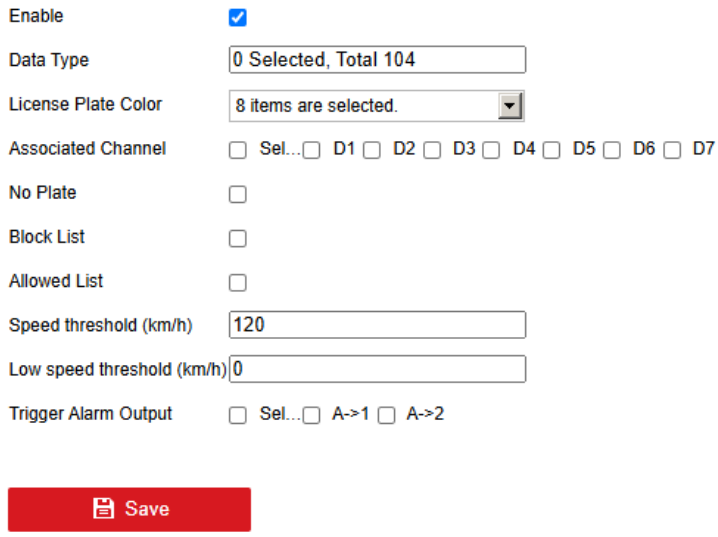

Figure 11-3 Set Camera Capture Alarm

3. Select the triggering conditions of the capture alarms. You can select **Data Type**, **License Plate Color**, **No Plate**, **Block List**, or **Allow List** according to your needs.

Note

If multiple triggering conditions are selected, only when all the selected conditions are satisfied, the capture alarm will be triggered.

4. Select **Associated Channel** to trigger the capture alarm.
5. **Optional:** If you select speeding or low-speed driving as the data type, set **Speed threshold** (the allowed max. speed) and **Low speed threshold** (the allowed min. speed).
6. Select the alarm output channel(s).
7. Click **Save**.

Chapter 12 Data Management

12.1 View Real-Time Data

The device supports viewing captured violation information in real time.

Steps

1. Click **Real-Time Data**.
2. View the data.

View the vehicle violation detailed information	Check the data row, and the left side of the interface will display the vehicle violation detailed information.
View the vehicle violation picture information	Click **Picture** to view the vehicle violation picture information.

12.2 Search Data

You can search the traffic data of the connected cameras.

Steps

1. Click **Data Search**.
2. Click the data type to search.
   - **Traffic Data Search**: Search the checkpoint data, violation data, traffic incident data, evidence capture data, etc.
   - **Traffic Parameters Statistics**: Search the lane traffic flow data.

   Note

   You need to enable **Traffic Parameter Statistics** in **Param Config → Advanced Settings → Other Settings → Traffic Parameters Statistics** .
3. Set **Start Time** and **End Time**.

   Note

   The time span between the start time and the end time cannot exceed 7 days.
4. Set the search conditions.
5. Click **Search/Statistics**.

   The searched result will be displayed.
6. Click **Details** after the data to view detailed information, pictures, video clips, etc.
7. **Optional:** After the data have been searched, click **Export** to export the selected data information to the set path.

Note

Make sure the IP address of the camera has been added as a trusted site before exporting the data.

12.3 Back up Data

12.3.1 Back up to Local

You can back up the data of the device to your computer.

Before You Start

Search the data to back up.

Steps

1. Set the data export rule.
   1) Go to **Param Config → Backup Settings → Web Backup → Web Backup Settings** .
   2) Enter the name, saving path, and other information of the picture and video.

      Note

      After the random number digits have been set, pictures with the same name will be automatically numbered. The upper limit of the number is the maximum number of the random number digits.

   3) Click **Save**.
2. Set the device IP address as a trusted site in the security settings of the browser.
3. Search the data, refer to ***Search Data*** for details.
4. Click **Export** to select export type and export the data to your computer.

Result

Data will be backed up as the set name in the set path.

12.3.2 Back up to USB

The device supports automatically backing up the data to the USB.

Before You Start

Connect a USB to the device.

Steps

1. Go to **Param Config → Backup Settings → Local Backup → USB Backup Settings** .
2. Click **USB Backup Settings**.
3. Enable USB backup.
4. Select **Backup Period** and **Start Time**.

- **Real-Time Backup**: Automatically back up the data only once after the data have been saved at the set time.
- **Backup Every Day**: Automatically back up the data once a day at the set time.

5. Select **Data Type** to backup.
6. Enter the picture backup naming rule and saving path.
7. Click **Save**.

   Pictures will be backed up with the set name in the set path.
8. **Optional:** Click **USB Backup Status** to view the backup status.

Chapter 13 Safety Management

13.1 Manage User

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

Before You Start
Set the administrator password when you first use the device to ensure a normal working.

Steps

Caution
It is highly recommended to create a strong password of your own choosing in order to increase the security of your product.

1. Go to **Param Config → System → User Management → User Management** .
2. Click **Add**.
3. Set the user name, password, and other information in the popup window.
4. Click **OK**.
5. **Optional:** You can also do the following operations.

Delete User	Select the added user and click **Delete** to delete the user.
Edit User Information	Select the added user and click **Edit** to edit the user information.
View Online User	Click **Online User** to view the online users.

13.2 Set HTTPS

13.2.1 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 **Param Config → Network → Advanced Settings → HTTPS** .
2. Select **Create the certificate request first and continue the installation.** and click **Create**.
3. Follow the prompt to enter **Country/Region**, **Domain Name/IP**, **Password**, and other parameters.
4. Click **OK**
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.

Note

Certification of certificates issued by Certification Authority may incur costs.

6. Import certificate to the device.
   - Click **Browse** to select the certificate and click **Setup** to import the certificate to the device.
   - Select **Signed certificate is available, start the installation directly.**. Click **Browse** to select the certificate and click **Setup** to import the certificate to the device.
7. Click **Save**.

13.2.2 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 **Param Config → Network → Advanced Settings → HTTPS** .
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain Name/IP**, **Effective Period**, and other parameters.
5. Click **OK**.
6. Click **Save**.

13.3 Set IP Address Filtering

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

Steps

1. Go to **Param Config → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Set **IP Address Filter Type**.

   Prohibit

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

   Allow

   The added IP addresses are allowed to access the device.
4. Click **Add**, enter the IP address, and click **OK**.

   Note

   The IP address only refers to the IPv4 address.
5. **Optional:** Edit, delete, or clear the added IP addresses.
6. Click **Save**.

13.4 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 **Param Config → System → Security → Security Service** .
2. Uncheck **Enable SSH**.
3. Click **Save**.

13.5 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 **Param Config → System → Security Service → Log Audit Service** .
2. Enable system log service.
3. Enter **IP Address** and **Port** of the log server.
4. Click **Save**.

Result

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

13.6 Set Session Expired Time

If you log out of the device or the device is disconnected, and then log in to the device within the set session expired time, you will enter into the page which you logged out from the last time automatically.

Steps

1. Go to **Param Config → System → Security → Security Enhancement** .
2. Enable timeout logout for static page.
3. Enter **Session Expired Time**.
4. Click **Save**.

Chapter 14 Maintenance

14.1 View Device Information

Go to **Param Config → System → System Settings → Basic Information** to view the device basic information.

You can edit **Device Name** and **Device No.** It is recommended to reserve the default value.

14.2 View System Status

View the device status and the connected camera status.

Device Status

Go to **Param Config → System Status → Server Status** to view the status below.

- **Working Status**: View the system time, working time, device running status, cabinet door status, and satellite time sync. status.
- **Net Port Status**: View the connection status of all the network interfaces on the device.
- **Bandwidth usage status**: View the overall bandwidth, idle bandwidth, the IP addresses and occupied bandwidth of the live view channels, and the IP addresses and occupied bandwidth of the playback channels.

Camera Status

Go to **Param Config → System Status → Status** to view the status below.

- **Traffic Flow Statistics**: View the traffic flow statistics of the selected camera.
- **Front-End Device Status**: View the name and status of the selected camera.
- **Camera Management Status**: View the login and arming status of the selected camera.

14.3 Synchronize Time

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

Steps

Note

Time sync. mode varies with different models. The actual interface prevails.

1. Go to **Param Config → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select the time sync. mode.

   NTP Time Sync.

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.

Note

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

Manual Time Sync.

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

GPS Time Sync.

Select it to synchronize the device time with that of the GPS. It is high-efficiency and less error.

SDK Time Sync.

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

4. Click **Save**.

14.4 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 **Param Config → System → System Settings → Serial Port** .

RS485

No.	Baud Rate	Data Bit	Stop Bit	Verification	Flow Control
1	9600	8	2	None	None

Figure 14-1 Set RS-485

2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, **Verification** and **Flow Control**.

Note

- Flow control can control the process of data transmission and avoid data loss.
- When you select hardware flow control, you need to ensure the cable connection. It is recommended to select software flow control if the cable connection is restricted.

3. Click **Save**.

14.5 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 **Param Config → System → System Settings → Serial Port** .
2. Select COM port according to the connected peripheral devices.

   Note
   Do not need to select COM port if the device only has one RS-232.
3. **Optional:** Edit **Baud Rate**, **Data Bit** and **Stop Bit**.
4. Select **Control Mode**.

   Transparent Channel

   For the data transmission of peripheral devices.

   Control Panel(By Parameter)

   For the serial port debugging of the device.
5. Click **Save**.

14.6 Set DST

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

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

14.7 Reboot

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

Steps
1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Reboot** .
2. Select the reboot mode.
   - Click **Reboot** to reboot the device directly.

- Check **Reboot** to reboot the device at 2 a.m. every day automatically.
- Check **Reboot Without HDD** to reboot the device when no HDD is detected.

3. Click **OK**.

14.8 Restore Parameters

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

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Restore Default Settings** .
2. Select the restoration mode.
   - Click **Restore** to restore the parameters except the IP parameters and platform parameters to the default settings.
   - Click **Default** to restore all the parameters to the factory settings.
3. Click **OK**.

14.9 Restore Database

When an exception occurs, you can restore the database if you have backed up the database before.

Before You Start

Make sure you have backed up the database before.

Steps

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Restore Database** .
2. Click **Restore**.
3. Click **OK**.

14.10 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 **Param Config → System → System Maintenance → Upgrade & Maintenance → Export Parameters** .
2. Click **Device Parameters**.
3. Select the saving path and enter the file name.
4. Click **Save**.

14.11 Import Parameters

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

Before You Start
Save the file that needs to be imported to the computer.

Steps

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

1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Import Parameters** .
2. Click **Browse** to import the configuration file.
3. Click **Import**.

Result

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

14.12 Upgrade

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

Before You Start
Prepare the upgrade file.

Steps
1. Go to **Param Config → System → System Maintenance → Upgrade & Maintenance → Upgrade** .
2. Click **Browse** and 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.

14.13 Search Log

You can search logs to troubleshoot problems.

Steps

1. Go to **Param Config → System → System Maintenance → Log Search** .
2. Set the search conditions.
3. Click **Search**.
   The log information will be displayed in the list.
4. **Optional:** Click **Export** to export the logs to the computer.

14.14 Export Debugging Log

Save and export debugging logs.

Steps

Note

This function is only available to professionals.

1. Go to **Param Config → Advanced Settings → Debugging Log → Debugging Log** .
2. Enable **Save Log**.
3. Select **Log Type**.
4. Click **Save**.
5. **Optional:** To export logs for a specified time period, set **Start Time** and **End Time**, and click **Export**.

14.15 Reserved Parameters

The reserved parameters are for technical personnel debugging only.

14.16 Set Startup Mode

Set the startup mode of the device.

Before You Start

Wire the power cord of the device properly.

Steps

1. Go to **Param Config → Advanced Settings → Other Settings → Startup** .
2. Select **Low voltage protection**.

Note

- Select **Battery** or **UPS** according to the power supply mode. If you select **Disable**, low voltage protection is disabled.
- When the device power voltage is lower than **Current Battery Voltage**, the device will shut down automatically, no matter what type of startup/shutdown mode you selected.

3. Select **Auto Work Type**.

Halt Delay

After the vehicle powers off, the device will automatically shut down after the set **Delay Time**.

Auto Working

Set the time period during which the device will start up/shut down automatically. Refer to ***Set Recording Schedule*** for details.

Note

Up to two time periods are allowed for each day and the time periods cannot overlap with each other.

4. Click **Save**.

See Far, Go Further

UD41351B