



Mobile Patrol ANPR System

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 External IP Address	5
3.2 Set Internal IP Address	6
3.3 Dial-up	7
3.4 Set Wi-Fi	8
3.5 Set Wi-Fi AP	9
3.6 Set DDNS	11
3.7 Set Port	12
3.8 Set Static Router	12
3.9 Share Network via USB Interface	13
Chapter 4 Camera Management	15
4.1 Check Camera Status	15
4.2 Set Camera Parameters	15
4.3 Set Other Parameters	16
Chapter 5 Mobile Enforcement Configuration	18
5.1 Set LPR Parameters	18
5.2 Enable Capture	18
5.3 Set Traffic Incident Rule	18
5.4 Set Manual Capture	19

5.5 Set Satellite Positioning	21
5.6 Set Vehicle Arming	22
5.7 Set Camera Brightness Control	23
5.8 Set Captured Picture	25
5.8.1 Set Picture Composition	25
5.8.2 Set Single Picture Overlay	26
5.8.3 Set Composite Picture Overlay	28
5.9 Set Violation Dictionary	29
5.10 Person Management	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 Local Configuration	33
Chapter 7 Storage	36
7.1 Format Disk	36
7.2 Set Quota	36
7.3 Set Holiday	36
Chapter 8 Record and Playback	38
8.1 Enable Recording	38
8.2 Play Back Video	38
8.3 Backup	39

8.3.1 Back up Video	39
8.3.2 Back up Clipped Video	39
Chapter 9 Encoding and Display	40
9.1 Set Video Encoding Parameters	40
9.2 Set Image Parameters	41
9.3 Set OSD	41
Chapter 10 Platform Connection	43
10.1 Set Remote Host	43
10.2 Set FTP	48
10.3 Connect to SDK Platform	51
10.4 Connect to ISUP Platform	51
10.5 Connect to HTTP Platform	52
10.6 Set Cloud Storage	53
Chapter 11 Data Management	56
11.1 View Real-Time Data	56
11.2 Search Data	56
11.3 Back up Data	56
11.3.1 Back up to Local	56
Chapter 12 Safety Management	58
12.1 Manage User	58
12.2 Set HTTPS	58
12.2.1 Install Authorized Certificate	58
12.2.2 Create and Install Self-signed Certificate	59
12.3 Set SSH	59
12.4 Enable System Log Service	59
12.5 Set Session Expired Time	60
Chapter 13 Maintenance	61
13.1 View Device Information	61

13.2 View System Status	61
13.3 Synchronize Time	61
13.4 Set RS-485	62
13.5 Set RS-232	62
13.6 Set DST	63
13.7 Reboot	63
13.8 Restore Parameters	63
13.9 Restore Database	64
13.10 Export Parameters	64
13.11 Import Parameters	64
13.12 Upgrade	65
13.13 Search Log	65
13.14 Export Debugging Log	66
13.15 Reserved Parameters	66
Appendix A. Port Information	67

Chapter 1 Product Introduction

Mobile Patrol ANPR System includes a mobile video recorder and several cameras. It can be installed on a vehicle, with handheld data processing terminals, to realize vehicle capture and ANPR, license plate comparison, driving records and vehicle locating, etc.

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.

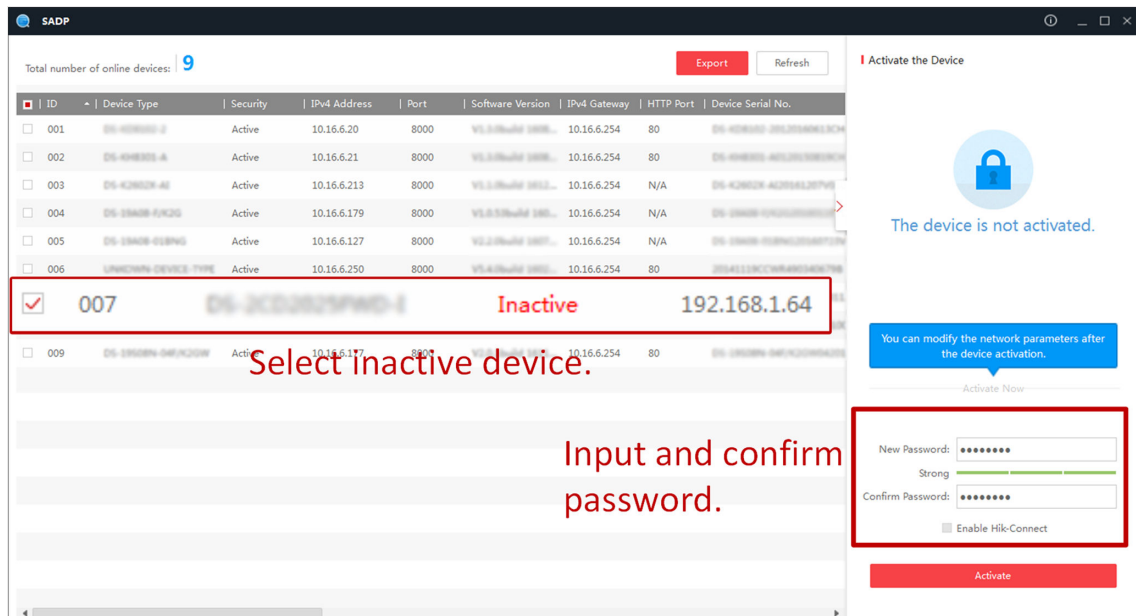


Figure 2-1 Activate via SADP

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 External IP Address

Set the external network mainly communicating with platform, remote host, etc.

Steps

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

NIC Type	Self-adaptive ▼
	☐ Auto
IPv4 Address	
IPv4 Subnet Mask	
IPv4 Default Gateway	
IPv6 Address	
IPv6 Prefix Length	64
IPv6 Default Gateway	
Physical Address	
MTU	1500
DNS Server	
Preferred DNS Server	
Alternative DNS Server	

 Save

Figure 3-1 Set External IP Address

2. Select **NIC Type** according to the actual network.
3. Set relevant network parameters.
 - Check **Auto** to get the IPv4 and IPv6 addresses automatically if the network supports distributing the IP addresses automatically.
 - Manually enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.



Note

- The network segment of external IP address should be different from that of the internal IP address.
- **MTU** stands for the maximum transmission unit in the network.
- Set **DNS Server** if remote domain name access is needed.

4. Click **Save**.

3.2 Set Internal IP Address

Set the internal network mainly used to connect to the camera.

Steps

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

NIC Type	Self-adaptive ▼ ☐ Auto
IPv4 Address	
IPv4 Subnet Mask	
IPv4 Default Gateway	
IPv6 Address	
IPv6 Prefix Length	64
IPv6 Default Gateway	::
Physical Address	
MTU	1500

Figure 3-2 Set Internal IP Address

2. Select **NIC Type** according to the actual network.

3. Set relevant network parameters.

- Check **Auto** to get the IPv4 and IPv6 addresses automatically if the network supports distributing the IP addresses automatically.
- Manually enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.



Note

- The internal IP address and the camera should be set to the same network segment, and it must be set to a different network segment from that of the external IP address.
- **MTU** stands for the maximum transmission unit in the network.

4. Click **Save**.

3.3 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 Communication Configuration**.
2. Click **Dial-up Parameters**.
3. Check **Enable**.

Note: You do not need to configure APN, dial number, user name, and password for normal card.

Reboot the device to take the modification into effect.

☒ Enable	
APN	
Dial Number	
User Name	
Password	
Security Mode	AUTO
Network Mode	Auto-Switch
MTU	1500
Dial-up Mode	QMI

Save

Figure 3-3 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-Switch

The device will switch the network mode automatically.

3G/4G Only

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.

3.4 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**.

Wireless List

Search

No.	SSID	Working Mode	Security Mode	channel1	Signal Strength	Speed(Mbps)
-----	------	--------------	---------------	----------	-----------------	-------------

Wi-Fi

☒ Enable Wi-Fi

SSID

Network Mode

☒ Managed

Security Mode

WPA2-personal

Encryption Type

AES

Key 1 ☒

.....

Save

Figure 3-4 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.

3.5 Set Wi-Fi AP

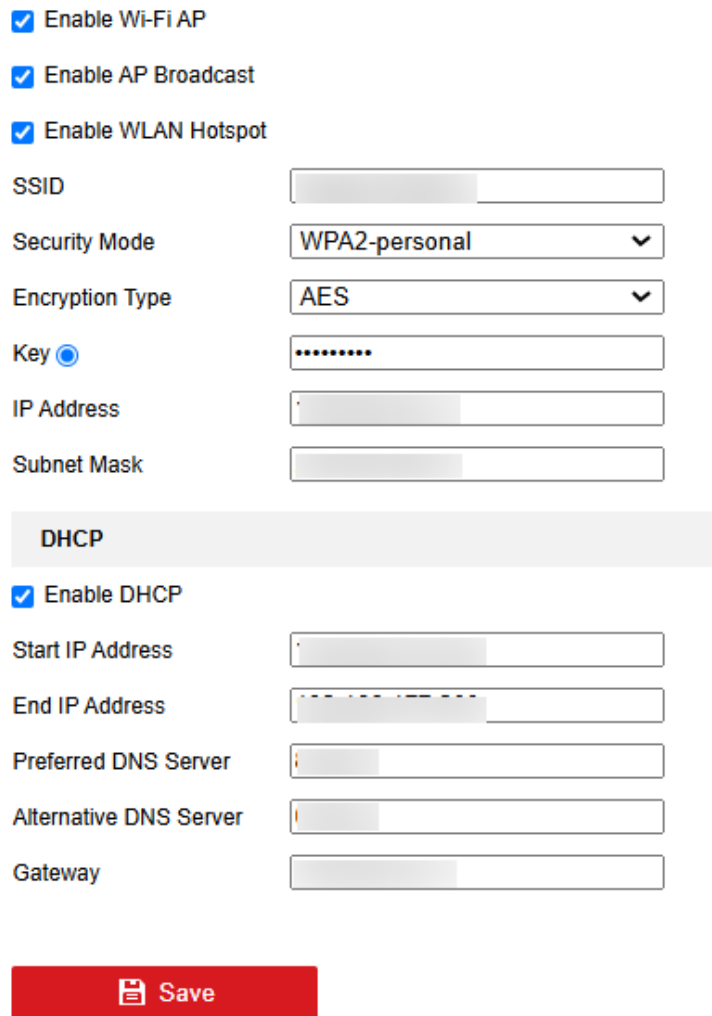
The device can be set as a hotspot to share network to other devices.

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**.



☒ Enable Wi-Fi AP

☒ Enable AP Broadcast

☒ Enable WLAN Hotspot

SSID

Security Mode

Encryption Type

Key ☒

IP Address

Subnet Mask

DHCP

☒ Enable DHCP

Start IP Address

End IP Address

Preferred DNS Server

Alternative DNS Server

Gateway

 Save

Figure 3-5 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**.

3.6 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**.

☒ Enable DDNS	
DDNS Type	DynDNS
Server Address	
Domain Name	
User Name	
Password	
Confirm Password	

Figure 3-6 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.

3.7 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

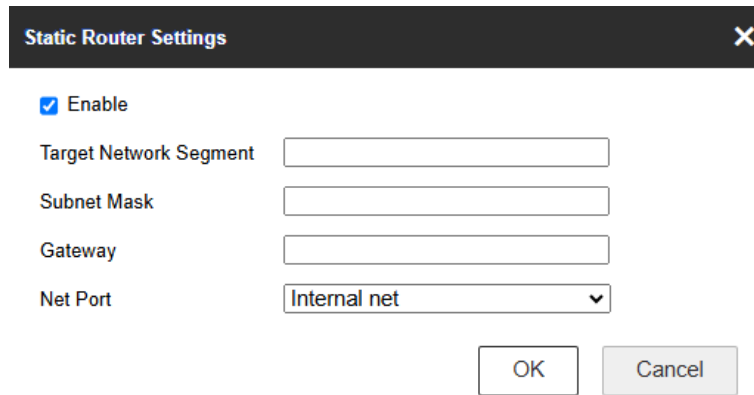
- Certain ports need to reboot after edited to take the new settings into effect.
 - When the device cannot edit the port No. via access Web due to port conflicts, you can connect the device to your computer and edit via SADP software.
-

3.8 Set Static Router

Set a static router for access across network segments. The device will transmit data as a router.

Steps

1. Go to **Param Config** → **Network** → **Basic Settings** → **Static Router** .
2. Click **Add** to add a static router.



The image shows a 'Static Router Settings' dialog box with a dark header bar containing the title and a close button (X). The main area is white and contains the following controls: a checked checkbox labeled 'Enable'; four input fields labeled 'Target Network Segment', 'Subnet Mask', 'Gateway', and 'Net Port'; and two buttons at the bottom right labeled 'OK' and 'Cancel'. The 'Net Port' field is a dropdown menu currently showing 'Internal net'.

Figure 3-7 Add Static Router

3. Check **Enable**.

4. Enter **Target Network Segment**, **Subnet Mask**, and **Gateway**.

 Note

Set the gateway according to the selected network interface.

5. Select the network interface that needs external communication for routing.

- When you need other network segments to access the connected camera through the internal network interface, select **Internal net** as a static router, and the internal IP address will serve as the gateway.
- When you need to upload data to other network segments through the external network interface, select **Outer net** as a static router, and the external IP address will serve as the gateway.

6. Click **OK**.

 Note

The device supports deleting or editing the added router.

7. **Optional:** You can select the added static router and click **Edit** to edit the router, or click **Delete** to delete the router.

3.9 Share Network via USB Interface

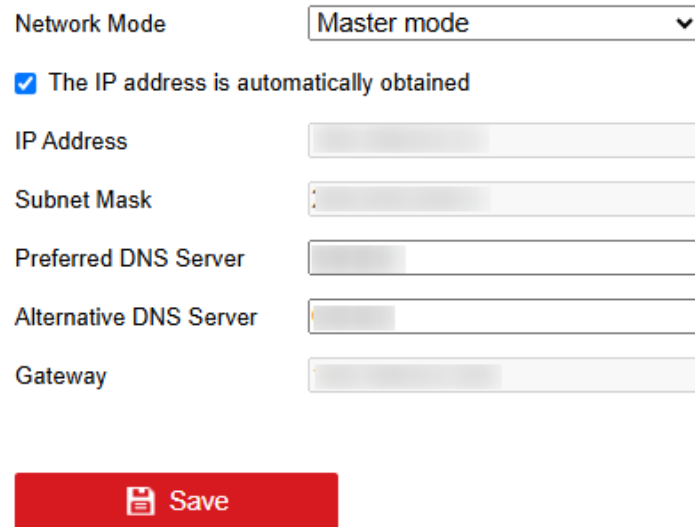
If you want to share the 4G network of the mobile video recorder to a portable code scanner, or vice versa, you can set the main and sub-mode of the USB interface on the mobile video recorder to realize network sharing.

Before You Start

Connect a portable code scanner to the USB interface of the mobile video recorder.

Steps

1. Go to **Param Config** → **Network** → **Advanced Settings** → **USB network** .



Network Mode Master mode

☒ The IP address is automatically obtained

IP Address

Subnet Mask

Preferred DNS Server

Alternative DNS Server

Gateway

 Save

Figure 3-8 Share Network via USB Interface

2. Select **Network Mode**, and set corresponding parameters.
 - **Master mode:** The mobile video recorder can use the 4G network of the connected portable code scanner. Check **The IP address is automatically obtained** and click **Save**, the mobile video recorder will obtain the IP address, subnet mask, and gateway automatically. If not, enter the IP address, subnet mask, gateway, etc. of the connected portable code scanner manually.
 - **Slave mode:** The portable code scanner can use the 4G network of the mobile video recorder. Enter **Local IP address** of the mobile video recorder manually, or check **Enable DHCP** to obtain the IP address automatically. Set **Start IP Address** and **End IP Address** of the portable code scanner in the same network segment with that of the mobile video recorder.

 Note

If you use slave mode, you need to enable **USB tethering** in  → **Network & internet** → **Hotspot & tethering** → **Hotspot & tethering** on the portable code scanner.

3. Click **Save**.

Chapter 4 Camera Management

4.1 Check Camera Status

Connect the cameras to the corresponding interfaces of the mobile video recorder. Go to **Param Config → System → Camera Management → Status** to view the camera status and information. Only when the camera is online, can it get streams and record videos normally.

IP Camera										Add	Edit	Delete	Quick Add	Reboot
☐ Channel...	Camera Name	IP Address	Channel No.	Managem...	Security	Status	Protocol Type	Model	Version	Connect	Operation			
☐ D1	Camera 01		1	8000	Weak	Online	PRIVATE			Access ...	Forgot Password			
☐ D2	Camera 02		1	8000	Weak	Online	PRIVATE			Access ...	Forgot Password			
☐ D3	Camera 03		1	8000	Weak	Online	PRIVATE			Access ...	Forgot Password			
☐ D4	Camera 04		1	8000	Weak	Online	PRIVATE			Access ...	Forgot Password			

Figure 4-1 Check Camera Status

4.2 Set Camera Parameters

You can set camera parameters for easy management.

Steps

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

Camera	[D1] Camera 01() ▼
Camera Type	Video Analysis Camera (Back- ▼
Camera No.	
Intersection No.(Internal)	
Direction	Upward ▼
Camera Location Informa...	xx Intersection Information1
Camera Location Informa...	xx Intersection Information2
Camera Location Informa...	xx Intersection Information3
Camera Location Informa...	

 Copy to...

 Save

Figure 4-2 Set Camera Parameters

2. Select a camera.
3. Select **Camera Type**.
4. Set **Camera No.**, **Intersection 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**.

4.3 Set Other Parameters

You can enable camera time synchronization and set other recording parameters.

Steps

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

The screenshot displays a configuration interface with the following elements:

- Camera Time Synchroniz...**: A dropdown menu currently set to **Enable**.
- Camera Time Sync. Thre...**: A slider control with a red indicator and a numeric input box showing **30**.
- Pre-record (s)**: A slider control with a red indicator and a numeric input box showing **4**.
- Post-record (s)**: A slider control with a red indicator and a numeric input box showing **6**.
- Longest Recording Time (s)**: A slider control with a red indicator and a numeric input box showing **60**.
- Save**: A prominent red button with a white floppy disk icon and the text **Save**.

Figure 4-3 Set Other Parameters

2. Set the parameters below.

Camera Time Synchronization

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

Pre-record

The time to record before the recording start time.

Post-record

The time to record after the recording end time.

Longest Recording Time

The longest recording time for one video.

3. Click **Save**.

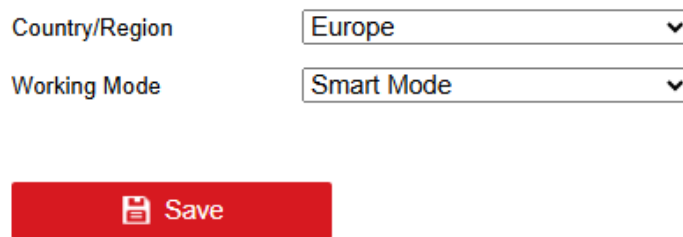
Chapter 5 Mobile Enforcement Configuration

5.1 Set LPR Parameters

You can switch the working mode of the mobile video recorder.

Steps

1. Go to **Param Config → Smart Traffic Settings → Capture Configuration → LPR Parameters** .



Country/Region	Europe ▼
Working Mode	Smart Mode ▼

Save

Figure 5-1 Set LPR Parameters

2. Select **Country/Region** in which the license plates are recognized.
3. Select **Working Mode**.

Smart Mode

The four channels all adopt checkpoint recognition algorithm to recognize the license plates.

Evidence Mode

The first and second channels adopt enforcement recognition algorithm to recognize the violation incidents. The third channel adopts checkpoint recognition algorithm to recognize the license plates. The fourth channel does not enable algorithm.

4. Click **Save**.

5.2 Enable Capture

Enable picture capture of the connected cameras.

Steps

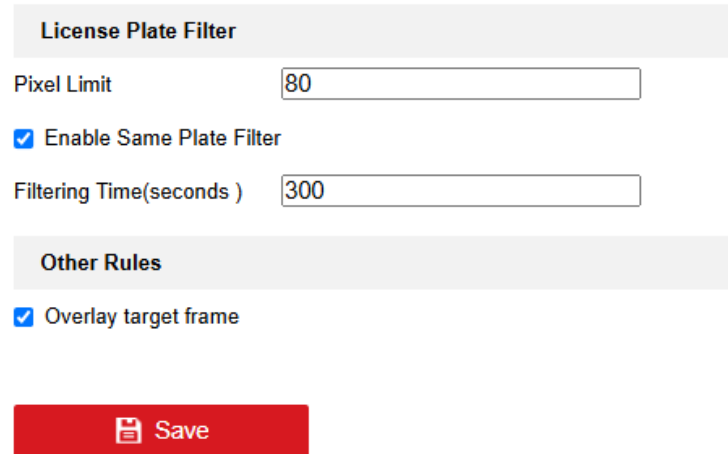
1. Go to **Param Config → Smart Traffic Settings → Capture Configuration → Enable Capture** .
2. Select the camera to enable capture.
3. Check **enable capture**.
4. Click **Save**.

5.3 Set Traffic Incident Rule

You can set the rules to capture traffic incidents.

Steps

1. Go to **Param Config → Smart Traffic Settings → Capture Configuration → Traffic Incident Rule** .



License Plate Filter

Pixel Limit

☒ Enable Same Plate Filter

Filtering Time(seconds)

Other Rules

☒ Overlay target frame

 Save

Figure 5-2 Set Traffic Incident Rule

2. Set traffic incident rules.

Pixel Limit

The license plates of which the pixels are lower than the set limit will be filtered.

Enable Same Plate Filter

When the same license plate is triggered many times during the set **Filtering Time** in the scene, the pictures of the vehicle will not be captured.

Overlay target frame

Enable the function to overlay target frame on the live view and captured pictures.

3. Click **Save**.

5.4 Set Manual Capture

You can enable manual capture to capture pictures by external physical button.

Before You Start

Connect the external physical button to the mobile video recorder.

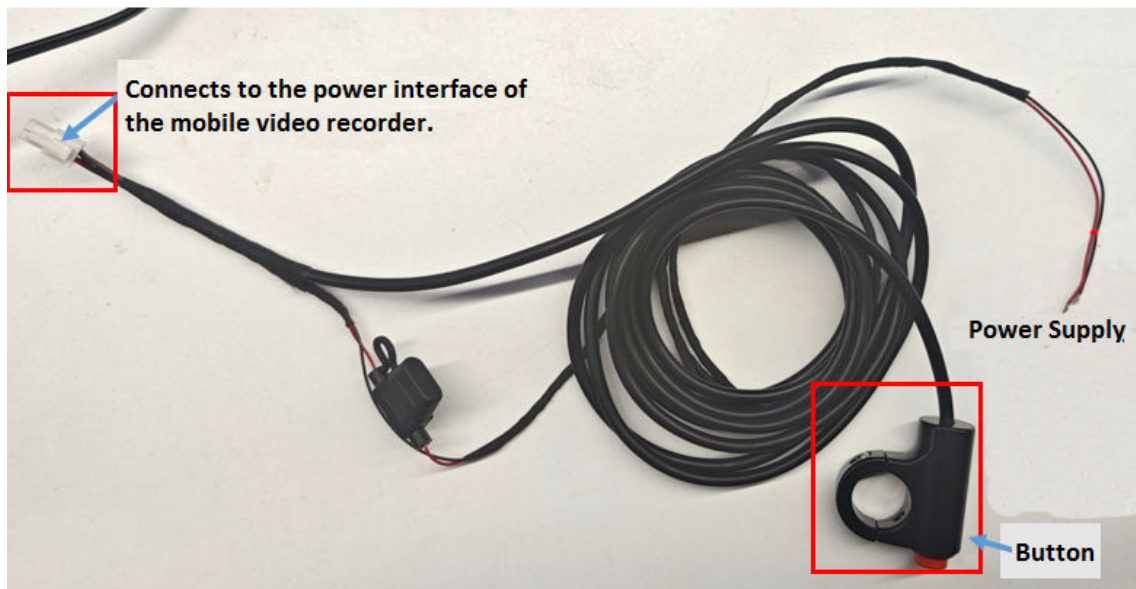


Figure 5-3 Connect External Physical Button

Note

The button is not provided with the product. You need to purchase the button if needed.

Steps

1. Go to **Param Config → Smart Traffic Settings → Capture Configuration → Manual capture** .

Enable	☒
Number of pictures before...	3
Number of pictures after t...	0
Capture Interval(seconds)	1

 Save

Figure 5-4 Set Manual Capture

2. Enable the function.
3. Set the parameters.

Number of pictures before trigger point

The trigger point refers to the point of triggering manual capture by double pressing the button. Set the number of captured pictures before triggering manual capture.

Number of pictures after the trigger point

The trigger point refers to the point of triggering manual capture by double pressing the button. Set the number of captured pictures after triggering manual capture.

Capture Interval

The time interval between two captured pictures.

4. Click **Save**.

What to do next

Double press the external physical button continuously and quickly to capture pictures.

5.5 Set Satellite Positioning

Set satellite positioning to get the specific location of the mobile video recorder, 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**.

Position Module	Built-in
Locating Module	GPS
Satellite Time Sync	☒ Enable
Speed Units	☒ Kilometers Per Hour ☐ Miles Per Hour
Speed Limit of Alarm	100
Blind Replacement(day)	2
Position Upload Interval(...)	10
IP Camera	☐ Sel... ☐ D1 ☐ D2 ☐ D3 ☐ D4

Figure 5-5 Set Satellite Positioning

3. **Optional:** Enable **Satellite Time Sync** to synchronize the time of the mobile video recorder with the satellite.
4. Select **Speed Units** and enter **Speed Limit of Alarm**.
When the speed of the vehicle installed with the mobile video recorder is higher than the set value, the alarm will be triggered.
5. Enter **Position Upload Interval**.
The mobile video recorder will upload the positioning information to the connected platform according to the set interval.
6. Select the camera(s) to overlay the positioning information.
7. Click **Save**.

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 | <ul style="list-style-type: none">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 | <ul style="list-style-type: none">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. |

5.7 Set Camera Brightness Control

You can enable supplement light and set corresponding parameters at night or in the dim scenes to raise the image quality.

Steps

1. Go to **Param Config → Smart Traffic Settings → Capture Configuration → Camera brightness Control**.

Supplement Light Control

Camera

[D1] Camera 01() ▼

Enable

☒

Supplement Light Brightn...

50

Enabled Time

17:00:00

Disabled Time

08:00:00

Exposure parameter configuration

Upper exposure time limit...

7000

Exposure time limit(us)

1

 Copy to...

 Save

Figure 5-7 Set Camera Brightness Control

2. Select a camera, and enable the function.
3. Set **Supplement Light Brightness**.
4. Set **Enabled Time** and **Disabled Time** during which the supplement light is enabled.

 Note

If you set the same **Enabled Time** and **Disabled Time**, the supplement light will not be enabled.

5. Set exposure parameters.

Upper exposure time limit

The upper limit of exposure time. Increase the exposure time appropriately when the environment is dim. Decrease the exposure time appropriately when the environment is bright.

Exposure time limit

The lower limit of exposure time. Increase the exposure time appropriately when the environment is dim. Decrease the exposure time appropriately when the environment is bright.

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

5.8 Set Captured Picture

5.8.1 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.

Camera	[D1] Camera 01()	
Compose	Enable	
2 Captured Pictures	Resolution: original picture resolu	
3 Captured Pictures	Resolution: original picture resolu	
4 Captured Pictures	Resolution: original picture resolu	
Maximum Size of Picture(...)	4096	
Copy Checkpoint Picture ...	Not Copy	
Copy Checkpoint Picture ...	Copy the First Picture	
Close-up Picture Size	Close-up	
Close-up Picture Capture...	Plate Coordinates Priority	
Close-up Picture	From the First Picture	
Upward Offset of Close-u...	0	Based on Plate Coordinate Center, Unit: pixels
Upward Offset of Close-u...	0	Based on Plate Recognition Area Center, Unit: pixels
Picture Combination Type	Composite Picture	

Copy to...
Save

Figure 5-8 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.

Copy Checkpoint Picture for Running the Red Light

Select whether to copy the checkpoint picture for the violation type of running the red light. If yes, select the picture sequence to copy.

Copy Checkpoint Picture for Other Traffic Violations

Select whether to copy the checkpoint picture for other traffic violations. If yes, select the picture sequence to copy.

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.

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

5.8.2 Set Single Picture Overlay

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

Steps

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

Camera	[D1] Camera 01() ▾
Text Overlay	Enable ▾
Text Overlay Method	Overlay on one picture, and ov ▾
Content	Camera Location Information Inte
Initial Top Margin (%)	0
Initial Left Margin (%)	0
Character Size	32 ▾
Font Color	#ffffff 
Background Color	 
Space number	4
Position Percentage of Li...	100

 Copy to...

 Save

Figure 5-9 Set Single Picture Overlay

4. Select **Text Overlay Method** according to your needs.
5. Click the text filed of **Content** to select the overlay information.
6. 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.

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.

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.

7. **Optional:** Click **Copy to** to copy the settings to other channels.

8. Click **Save**.

5.8.3 Set Composite Picture Overlay

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

Steps

1. Go to **Param Config → Picture Settings → Composite Overlay**.
2. Enable **Text Overlay**.

Camera	[D1] Camera 01()
Text Overlay	Enable
Text Overlay Method	Overlay on composite picture,
Content	Camera Location Information Inte
Initial Top Margin (%)	0
Initial Left Margin (%)	0
Character Size	32
Font Color	#ffffff
Background Color	
Space number	4
Position Percentage of Li...	100

 Save

Figure 5-10 Set Composite Picture Overlay

3. Select **Text Overlay Method** according to your needs.
4. Click the text filed of **Content** to select the overlay information.
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.

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.

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.

6. Click **Save**.

5.9 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.

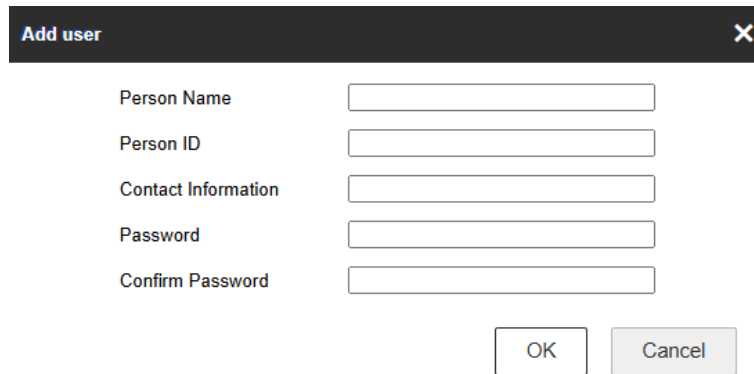
Reset Click **Reset** to restore the dictionary to the factory settings, and all the custom data will be cleared.

5.10 Person Management

You can add and manage the inspection personnel.

Steps

1. Go to **Param Config → Advanced Settings → Person Management → Person Management**.
2. Click **Add** to add a person.
 - 1) Enter **Person Name**, **Person ID** and **Contact Information**.
 - 2) Set **Password** for the person and confirm the password.
 - 3) Click **OK**.



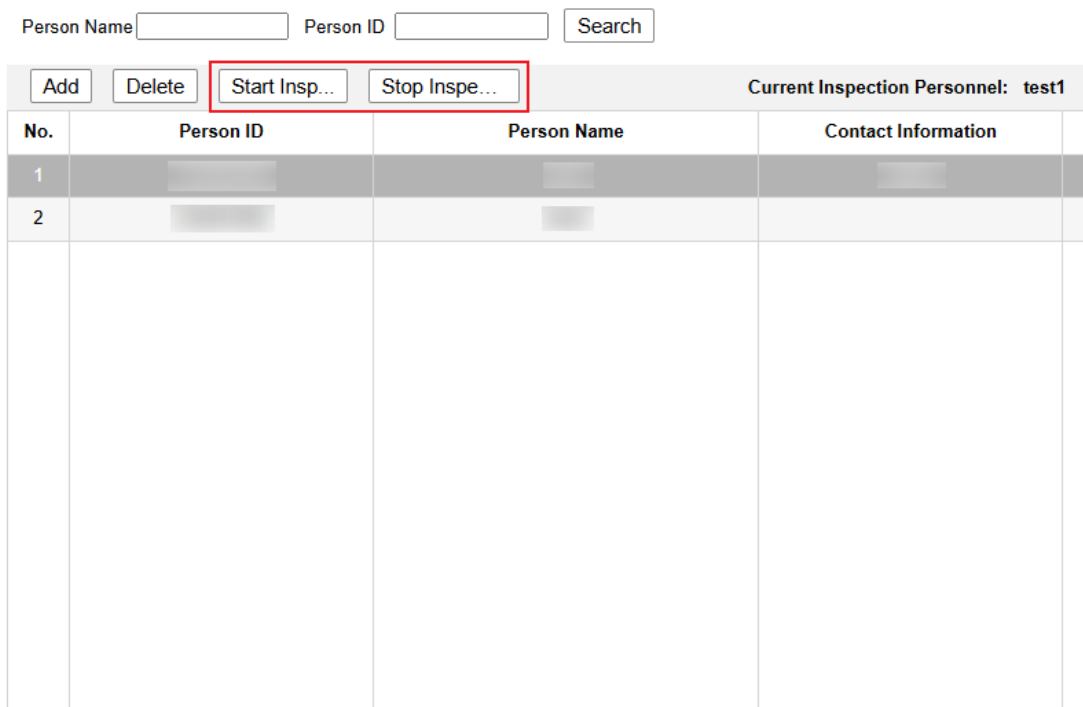
The 'Add user' dialog box is a dark-themed window with a close button (X) in the top right corner. It contains five input fields for user registration: 'Person Name', 'Person ID', 'Contact Information', 'Password', and 'Confirm Password'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Person Name	
Person ID	
Contact Information	
Password	
Confirm Password	

OK Cancel

Figure 5-11 Add Person

3. The added persons will be listed in the table. Select a person and click **Start Inspection** to start inspection. You can click **Stop Inspection** to stop inspection.



The main interface includes a search section at the top with 'Person Name' and 'Person ID' input fields and a 'Search' button. Below this is a table with columns: 'No.', 'Person ID', 'Person Name', and 'Contact Information'. The table contains two rows of data. Above the table, there are four buttons: 'Add', 'Delete', 'Start Insp...', and 'Stop Inspe...'. The 'Start Insp...' and 'Stop Inspe...' buttons are highlighted with a red rectangle. To the right of the table, it says 'Current Inspection Personnel: test1'.

Person Name Person ID Search

Add Delete Start Insp... Stop Inspe... Current Inspection Personnel: test1

No.	Person ID	Person Name	Contact Information
1			
2			

Figure 5-12 Start/Stop Inspection

4. **Optional:** You can do the following operations.
- Enter **Person Name** or **Person ID**, and click **Search** to search the person.
 - Select a person, and click **Delete** to delete the person.

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 Local Configuration

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

Live View Parameters			
Protocol Type	☒ TCP	☐ UDP	
Stream Type	☒ Main Stream	☐ Sub-stream	
Play Performance	☐ Shortest Delay	☒ Balanced	☐ Fluent
Rules	☐ Enable	☒ Disable	
Display POS Information	☐ Enable	☒ Disable	
Image Size	☒ Auto-fill	☐ 4:3	☐ 16:9
Auto Start Live View	☐ Yes	☒ No	
Image Format	☒ JPEG	☐ BMP	

Record File	
Record File Size	☐ 256M ☒ 512M ☐ 1G
Save record files to	D:\ Browse
Save downloaded files when playb...	D:\ Browse

Capture and Clip Settings	
Save snapshots in live view to	D:\ Browse
Save snapshots when playback to	D:\ Browse
Save clips when playback to	D:\ Browse

Figure 6-1 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.

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 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 Enable Recording

You can enable recording for the selected camera.

Before You Start

Install and format the storage media.

Steps

1. Go to **Param Config** → **Storage** → **Schedule Settings** → **Recording Schedule** .
2. Select a camera.
3. Check **Enable** to enable recording.
4. **Optional:** Click **Copy to** to enable recording for other cameras.
5. 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.

Steps

1. Go to **Param Config → Video → 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 Image Parameters

Set image parameters to adjust brightness and contrast.

Steps

1. Go to **Param Config → Image → Display Settings**.
2. Select a camera.
3. Check **Enable Image Flip** and select **Image Flip Style**. The camera supports center flip, left-right flip, and up-down flip.
4. **Optional:** Click **Restore Default Settings** to restore parameters to the default status.

9.3 Set OSD

You can customize OSD information on the live view.

Steps

1. Go to **Param Config → Image → OSD Settings**.
2. Select a camera.
3. Check **Display Name** or **Display Date** according to actual needs.
4. Enter **Camera Name**, and select **Time Format** and **Date Format**.
5. Drag the red frame overlaid on the live view image to adjust the OSD information positions.
6. **Optional:** Click **Copy to** to copy the settings to other channels.
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.

Upload Protocol	SDK Protocol	▼
SDK Platform ID	1	▼
Upload Strategy	Latest Data Priority	▼
Data Type	1 Selected, Total 1	
License Plate Color	8 items are selected.	▼
Upload History Data	Enable	▼
History Data Time range(...	0	
Upload No-Plate Data	Enable	▼
Upload by Time	Enable	▼
Start Time 1	00:00	
End Time 1	11:59	
Start Time 2	12:00	
End Time 2	23:59	
Time Type	Device Time	▼
Interval (ms)	50	
Timeout (ms)	5000	
Waiting For Upload Resp...	Disable	▼
Picture Upload Mode	Upload Picture Directly	▼

 Save

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 select the upload data type(s).
 - 4) Select **License Plate Color** to be recognized.

5) 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, the historical data within the set **History Data Time range** will be uploaded again.

Upload No-Plate Data

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

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.

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.

Picture Upload Mode

Upload Picture Directly

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.

Local URL

The device will generate URL for the pictures stored in the storage media and upload the picture URL and alarm information to the platform.

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 select the upload data type(s).

3) Select **License Plate Color** to be recognized.

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, the historical data within the set **History Data Time range** will be uploaded again.

Upload No-Plate Data

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

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.

Picture Upload Mode

Select **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 select the upload data type(s).

3) Select **Checkpoint Picture Upload Type**.

4) Select **License Plate Color** to be recognized.

5) 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, the historical data within the set **History Data Time range** will be uploaded again.

Upload No-Plate Data

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

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.

Picture Upload Mode

Upload Picture Directly

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.

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

Upload Mode: Data Retransmission

Start Time: 2022-02-15 00:00:00

End Time: 2022-02-15 23:59:59

Data Type: All

Data Retransmission: Turn the status of the history data into the To Be Uploaded status, and upload the history data only once.

OK Cancel

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** .

Data Upload Config

Host Name	Enable	Network Status	Real-time Data Time	History Data Time	Information
FTP Uploading Server 1	Disabled				

Param Config

FTP	Enable
FTP Server Address	
FTP Port	
FTP User Name	admin
FTP Password	
Upload Historical Data	Enable
Upload Allowlist Data	Disable
Upload Blocklist Data	Enable
Upload by Time	Disable
Data Type	1 Selected, Total 3
Checkpoint Detection Pict...	Enable
Checkpoint Vehicle Pictur...	Disable
License Plate Color	8 items are selected.
Upload No-Plate Data	Enable
License Plate Picture Name	[YYYY][MM][DD]_[HH][FF][SS][SSS]_[CDBH]_[CPHM]_plate.jpg
Checkpoint Picture Name	[YYYY][MM][DD]_[HH][FF][SS][SSS]_[CDBH]_[CPHM]_P[TPXH].jpg
Checkpoint Vehicle Pictur...	[XJIP]/[SJLX]/[YYYY][MM][DD]/[HH]/
Attached File Name	[YYYY][MM][DD]_[HH][FF][SS][SSS]_[CDBH]_[CPHM]_attachfile.ini
Attached File Saving Path	ATTACHFILE/[XJIP]/[YYYY][MM][DD]/[HH]/
Attached File Content	DataType=[SJLX][HCHH]PassTime=[YYYY]-[MM]-[DD] [HH]:[FF]:[SS][HCHH]PlateNum=[CPHM][HCHH]DeviceID=[XJBH][HCHH]

Figure 10-3 Set FTP

2. Select a FTP server.
3. Set FTP parameters.
 - 1) Enable the FTP.
 - 2) Enter **FTP Server Address**, **FTP Port**, **FTP User Name**, and **FTP Password**.
4. 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 Arming → Arming Management**.

Upload Blocklist Data

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

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 **Upload 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.

Upload No-Plate Data

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

5. Enable or disable **Checkpoint Detection Picture Upload** and **Checkpoint Vehicle Picture Upload** according to your needs.
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.

Upload Mode: Data Retransmission

Start Time: 2022-02-15 00:00:00

End Time: 2022-02-15 23:59:59

Data Type: All

Data Retransmission: Turn the status of the history data into the To Be Uploaded status, and upload the history data only once.

OK Cancel

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

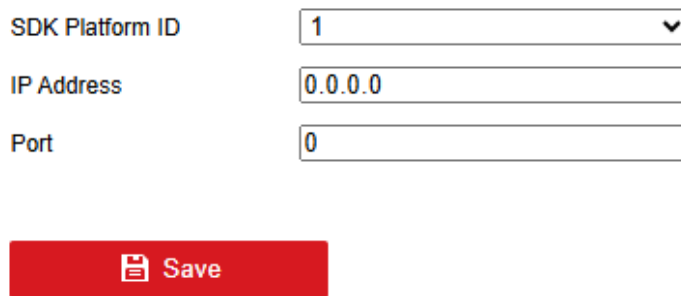
SDK is the platform access protocol. You can connect the device to the SDK platform to realize live view and data management via the platform.

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** .



SDK Platform ID	1
IP Address	0.0.0.0
Port	0

Save

Figure 10-5 Connect to SDK Platform

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



Note

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

4. 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** .

ISUP platform ID	1
☒ Enable	
Version	v5.0
Server Address	
Port	
Device ID	
Registration Status	Offline
Login Key	

 Save

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** .

HTTP Platform ID	1
URL	
Address Type	IP Address
IP Address	
Port	

 Save

Figure 10-7 Connect to HTTP Platform

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

The screenshot displays a configuration window for cloud storage. At the top, there are three fields: 'Cloud Storage' with a dropdown menu showing '1', 'IP Address' with a text input field, and 'Port' with a text input field. Below these is a section header 'Cloud Storage Server Parameters'. Under this header are five more fields: 'Protocol Version' with a dropdown menu showing 'V1.0', 'Central Management Port' with a text input field, 'User Name' with a text input field, 'Password' with a text input field, and 'Storage Pool ID' with a text input field showing '0'. At the bottom of the form is a red button with a floppy disk icon and the text 'Save'.

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 Data Management

11.1 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.

11.2 Search Data

You can search the traffic data of the connected cameras by searching data.

Steps

1. Click **Data Search** → **Traffic Data Search**.
2. Set **Start Time** and **End Time**.



The time span between the start time and the end time cannot exceed 7 days.

3. Set the search conditions.
4. Click **Search**.
The searched result will be displayed.
5. Click **Details** after the data to view detailed information, pictures, video clips, etc.
6. **Optional:** After the data has been searched, click **Export** to export the selected data information to the set path.



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

11.3 Back up Data

11.3.1 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.

Chapter 12 Safety Management

12.1 Manage User

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

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**. Enter the admin password to delete the user.

Edit User Information

Select the added user and click **Edit** to edit the user information.

12.2 Set HTTPS

12.2.1 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**.

12.2.2 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**.

12.3 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**.

12.4 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.

12.5 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 13 Maintenance

13.1 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.

13.2 View System 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.

13.3 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**.

SDK Time Sync.

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

EHome Time Sync

Select it to synchronize the device time with that of the EHome platform.

4. Click **Save**.

13.4 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 13-1 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**.

13.5 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**.

13.6 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**.

13.7 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**.

13.8 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**.

13.9 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**.

13.10 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**.

13.11 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.

13.12 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.

13.13 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.

13.14 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**.

13.15 Reserved Parameters

The reserved parameters in **Param Config → Advanced Settings → Custom Reserved Params → Global Parameters** are for technical personnel debugging only.

Appendix A. Port Information

For Mobile Patrol ANPR System The device will open the following network ports to provide corresponding services. The service names, ports, and functions are as follows:

- SADP Discovery: UDP 37020 (multicast 239.255.255.250), LAN device search.
- HTTPS Management: TCP 443, for parameter configuration and data query.



See Far, Go Further