



Guidance Terminal

User Manual

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.

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 Introduction.....	1
1.1 Product Introduction.....	1
1.2 Key Features.....	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 and Logout.....	4
Chapter 3 Parking Camera Management.....	5
3.1 Set Application Mode.....	5
3.2 Manage Channel	5
3.2.1 Set IP Camera	5
3.2.2 Set Interaction Parameters	6
3.3 Set Parking Space Detection Area.....	7
3.4 Set Parking Space Indicator.....	8
Chapter 4 Live View and Local Configuration	10
4.1 Live View	10
4.1.1 Start/Stop Live View.....	10
4.1.2 Divide Window and Switch Page	10
4.1.3 Select Stream Type.....	10
4.1.4 Capture Manually.....	11
4.1.5 Record Manually	11
4.1.6 Enable/Disable Audio	11
4.1.7 Enable Digital Zoom	11
4.1.8 Display in Full Screen	12
4.2 Local Configuration	12
Chapter 5 Storage Settings	15
5.1 Set Storage Path.....	15

5.1.1 Format Disk	15
5.1.2 Set Quota	15
5.1.3 Detect HDD.....	16
5.2 Set Record Schedule.....	16
5.3 Set Holiday	18
Chapter 6 Record and Playback	20
Chapter 7 Encoding and Display	21
7.1 Set Video Encoding Parameters.....	21
7.2 Set Image Parameters	22
7.3 Set OSD.....	23
Chapter 8 Network Configuration.....	25
8.1 Set Internal IP.....	25
8.2 Set External IP	26
8.3 Set DDNS	27
8.4 Set Port.....	27
8.5 Set Static Router.....	29
8.6 Connect to Platform.....	29
8.6.1 Connect to SDK.....	29
8.6.2 Connect to ISUP	30
8.6.3 Connect to HTTP	32
8.6.4 Set Cloud Storage.....	32
8.6.5 Set Remote Host	34
Chapter 9 Data Management	37
9.1 Set Picture and Video Export Rule	37
9.2 Search Data	37
9.3 View Parking Space Status	38
Chapter 10 Alarm Configuration	39
10.1 Set Alarm Output	39
10.2 Set Exception Alarm	40
Chapter 11 Safety Management	41
11.1 Manage User	41

11.2 Set HTTPS	41
11.2.1 Install Authorized Certificate	41
11.2.2 Create and Install Self-signed Certificate.....	42
11.3 Set SSH	42
11.4 Set Log Server.....	42
11.5 Set Timeout Logout.....	43
Chapter 12 Maintenance	44
12.1 View Device Information.....	44
12.2 Synchronize Time	44
12.3 Set RS-485	45
12.4 Set RS-232	45
12.5 Reboot.....	46
12.6 Restore Parameters	46
12.7 Restore Database	46
12.8 Export Parameters	46
12.9 Import Parameters.....	47
12.10 Upgrade.....	47
12.11 Search Log	48
12.12 View System Status	48
12.13 Reserved Parameters	48
12.14 Set Other Parameters	48

Chapter 1 Introduction

1.1 Product Introduction

Guidance terminal (hereinafter referred to as device), based on the ARM processor, is a remarkable intelligent management system used for underground garage. Adopting the advanced parking guidance and find my car system, the guidance terminal is capable of connecting multiple parking cameras to realize parking space detection, license plate recognition, guidance screen information control, video storage, playback, etc.

The guidance terminal is widely used in the parking lot of the community, business center and hotels. It greatly shortens the parking time and vehicle searching time of customers, and improves the utilization of the spare parking spaces.

1.2 Key Features

- Supports access to dual-lens parking cameras or single-lens parking cameras.
- Supports Hikvision PoE power supply for parking cameras.
- Supports TPM cascade and data upload.
- Supports IP address automatic allocation.
- HDD slots with large capacity distributed storage, storing recordings up to 30 days.

Chapter 2 Activation and Login

2.1 Activation

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



Note

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

2.1.1 Default Information

Device default information are as follows.

- Default IP address: P: 192.168.254.1, G: 192.168.1.64
- Default user name: admin

2.1.2 Activate via SADP

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

Before You Start

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

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

Steps

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



Caution

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

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

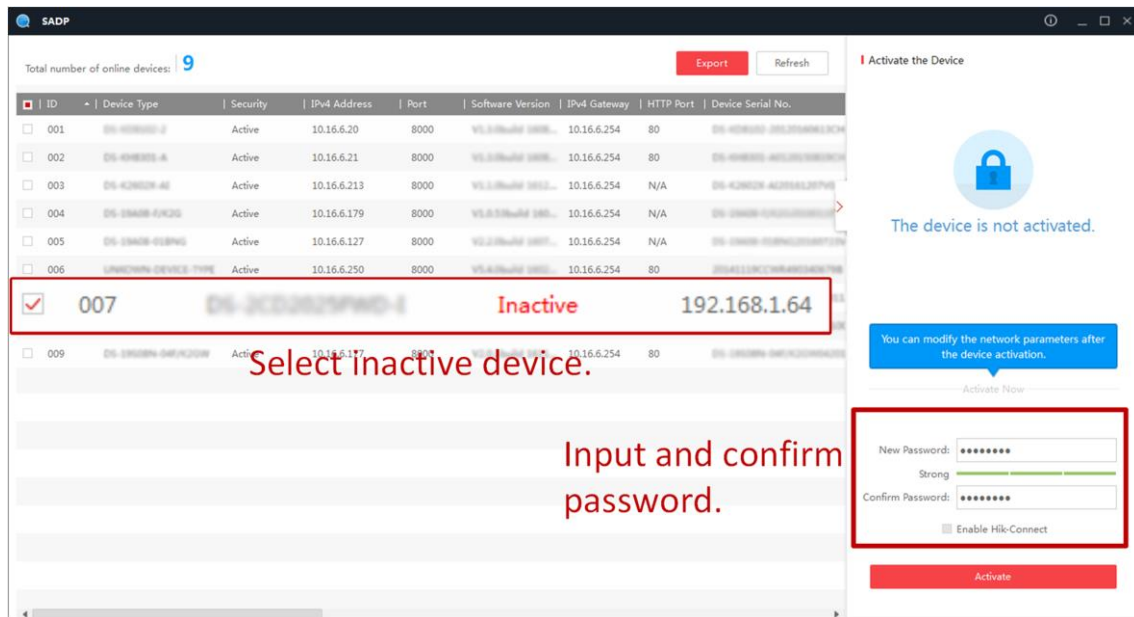


Figure 2-1 Activate via SADP

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

5. Modify IP address of the device.

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

2.1.3 Activate via Web Browser

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

Before You Start

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

Steps

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



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 and Logout

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

Before You Start

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

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
2. Enter **User Name** and **Password**.
3. Click **Login**.
4. Download and install appropriate plug-in for your web browser. Follow the installation prompts to install the plug-in.
5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 3 to login.
6. Optional: Click **Logout** on the upper right corner of the interface to log out of the device.

Chapter 3 Parking Camera Management

After parking cameras are added to the device, the real-time monitoring and management of parking spaces can be achieved after configuration.

3.1 Set Application Mode

Set the application mode according to the on-site camera model.

Steps



The number of accessible channels and supported functions may vary in different modes.

1. Go to **Param Config > System > Application Mode > Application Mode**.

Application Mode

Application Mode Note: after switching mode, the parameter will be reset

Channel Analysis Enable... ☐ Note: after switching mode, Will disconnect links that do not support analysis algorithm channels

 Save

Figure 3-1 Application Mode

2. Set **Application Mode** as **IPC Mode**.
3. Check **Channel Analysis Enabled Mode**, and then only the channels that support analysis algorithm will be displayed.
4. Click **Save**.



Reboot the device to take the settings into effect.

3.2 Manage Cameras

3.2.1 Set Parking Camera

When you connect parking cameras to the device, the device will automatically recognize and activate the cameras with its own activation password if they are not activated, and adjust the

camera's network segment to the network segment of the device. After configuration, you can view or set the camera information.

Before You Start

Connect the camera to the device.

Steps

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

Note

- When no parking camera is connected, the status of each channel is offline.
 - If the camera is activated via the device, the camera password is the same as the device activation password. If the camera has already been activated before connecting to the device, the default password is recommended or keep it the same as the device activation password.
 - The number of accessible parking cameras (number of channels displayed) varies by device models. The actual device shall prevail.
-

2. View the IP camera information, including camera name, IP address, status, etc.
3. Optional: You can also do the following operations.

Edit Edit the added camera IP address.

Reboot Reboot the online camera.

Access Directly Access the online camera.

3.2.2 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**.

Camera	[D1] Camera 01()
Interaction Mode	Normal Mode 

 Copy to...

 Save

Figure 3-2 Set Interaction Parameters

2. Select the camera.

3. Select the interaction mode.
 - Normal Mode: The device can tell the camera status via the camera's stream, and it can record and live view images and receive image data.
 - Data Receiving Mode: The device only can receive image data, but it cannot record or live view the camera.
4. Optional: You can click **Copy to...** and check channels to copy the set parameters to those selected channels.
5. Click **Save**.

3.3 Set Parking Space Detection Area

You can set the parking space detection areas according to the actual scenario for parking space management and monitoring.

Before You Start

Add the camera.

Step

1. Go to **Param Config > Parking Settings > Parking Space Settings > Parking Space Settings**.

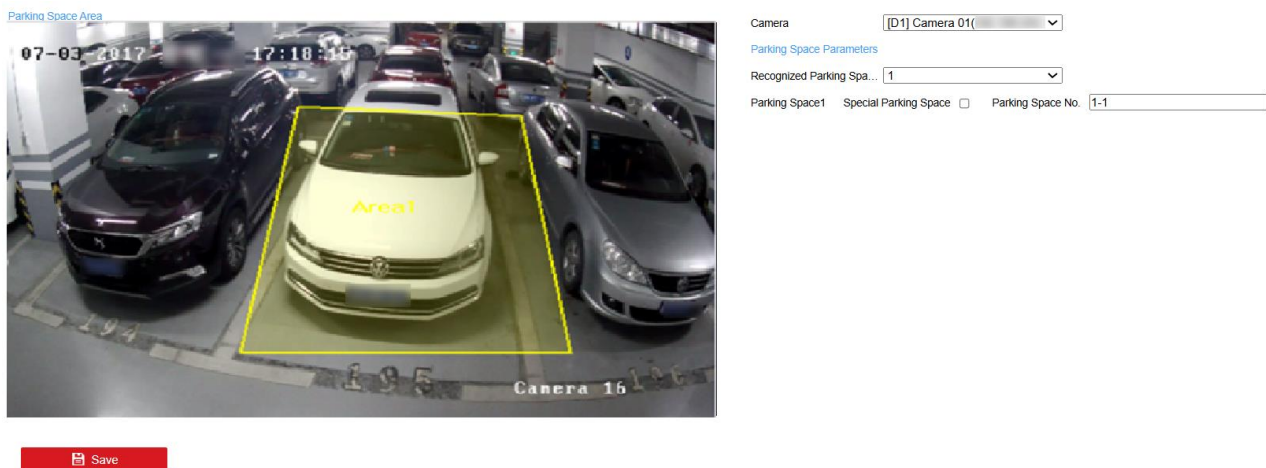


Figure 3-3 Set Parking Space Detection Area

2. Select the camera.
3. Set the parking space parameters.
 - 1) Select the number of the **Recognized Parking Space(s)** from the drop-down list.

Note

The selectable value may vary with camera model.

- 2) Optional: Check **Special Parking Space** if the space is a special space.

Note

The indicator light color of special spaces has the highest priority.

3) Enter **Parking Space No.** in the text filed.

Note

Parking space No. only allows \$, #, -, letters, and digits.

4. Draw parking spaces. The quadrilaterals appear in the image according to the number of spaces you set.

1) Click a quadrilateral, and drag corners of the quadrilateral to adjust the shape, or drag the quadrilateral to adjust the location.

2) Repeat step 1) to set more quadrilaterals.

5. Click **Save**.

3.4 Set Parking Space Indicator

The indicator displays the status of the parking space, and different colors stand for different status. You can select the indicator and the color of different status.

Before You Start

Add the camera.

Steps

1. Go to **Param Config > Parking Settings > Parking Space Indicator > Parking Space Indicator**.

Parking Space Indicator

Camera

Indicator Control Mode

Parking Space1

Indicator Source

Parking Space Status	Enable	Indicator Flicker	Indicator Color
Occupied	Yes	No	Red
Unoccupied	Yes	No	Green
Driving on the Lane Line	No	No	Yellow
Special Parking Space	No	No	Blue

Figure 3-4 Set Parking Space Indicator

2. Select the camera.
3. Set **Indicator Control Mode** on your demand.

Internal Indicator

The parking space status is informed via the internal indicator of the device. When all the detected parking spaces are occupied, the indicator turns to the occupied color; when the detected parking spaces are not all occupied, the indicator remains the unoccupied color.

External Indicator

The parking space status is informed via the external indicator connected to the device. After the connection, power up the device and the external indicator will start the self-test by indicating red, green, and blue respectively.



Note

If the self-test fails, check the cable connection.

Internal & External Indicator

The internal and external indicators work at the same time. You can respectively set the indicator to inform the status of each parking space.

4. Set the indicator parameters for different parking space status.
 - 1) Optional: Select **Indicator Source**.
 - 2) Enable or disable the indication for different parking space status.

Unoccupied

The parking space is free.

Occupied

The parking space is occupied by a vehicle.



Note

If you select **Internal Indicator** or **External Indicator**, occupied status means all the detected parking spaces are occupied, and unoccupied status means not all the detected parking spaces are occupied. E.g., three parking spaces are detected. When the three spaces are all occupied, the indicator will display the color you set for the occupied status. When two spaces are occupied and one space is unoccupied, the indicator remains the color you set for the unoccupied status.

Over Line

A vehicle occupied two parking spaces.

Special Parking Space

The parking space is specified to a certain vehicle.

- 3) Select **Indicator Flicker** and **Indicator Color** for different parking space status.
5. Optional: Click **Copy to...** to copy the settings to other cameras.
6. Click **Save**.

Chapter 4 Live View and Local Configuration

4.1 Live View

4.1.1 Start/Stop Live View

Start/stop the live view of cameras.

Start Live View

Click **Live View**, and double-click the camera list on the left side 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 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, click the camera list on the left side of the live view interface to stop live view.

Click  to stop all live view.

4.1.2 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 the page and view the camera live view of all pages.

4.1.3 Select Stream Type

To select the stream type, click  /  in the channel list, or hover over  /  on the bottom of the live view interface. It is recommended to select the main stream to get the high-quality image when the network condition is good, and select the sub-stream to get the fluent image when the network condition is not good enough.

4.1.4 Capture Manually

Capture live view pictures and save them to your computer.

Steps

1. Click **Live View**.
2. Start the live view of the camera.
3. Click .
4. View captured pictures.



Go to **Param Config > Local > Capture and Clip Settings** for the saving path of snapshots in live view.

4.1.5 Record Manually

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

Steps

1. Click  to start live view.
2. Double-click the camera name to start the live view.
3. Click  to start recording.
4. Click  to stop recording.



Go to **Param Config > Local > Record File** to view the saving path of record files.

4.1.6 Enable/Disable Audio

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

4.1.7 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.

4.1.8 Display in Full Screen

You can display the live view image in full screen.
On the **Live View** interface, click  to display the live view image in full screen.
Press **Esc** on the keyboard to exit the full screen mode.

4.2 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

Rendering Engine

☐ D3D9
☒ D3D11

Record File

Record File Size

☐ 256M
☒ 512M
☐ 1G

Save record files to

Save downloaded files when playb...

Capture and Clip Settings

Save snapshots in live view to

Save snapshots when playback to

Save clips when playback to

Save

Figure 4-1 Local Configuration



The parameters vary with device model. The actual device prevails.

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 engine as needed.

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 5 Storage Settings

5.1 Set Storage Path

5.1.1 Format Disk

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

Steps



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

1. Go to **Param Config > Storage > Storage Management > HDD Management**.

[illegible]

Figure 5-1 Manage HDD

2. Check the HDD No. needs to be formatted.
3. Click **Format**. After formatting, the device can start recording according to the record schedule.

5.1.2 Set Quota

Set the picture ratio in the storage.

Before You Start

Format the HDD.

Steps

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



Note

The picture quota takes effect when the record schedule is enabled.

3. Click **Save**.

5.1.3 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.

5.2 Set Record Schedule

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

Before You Start

Install and format the storage media (like HDD).

Steps

1. Go to **Param Config > Storage > Schedule Settings > Recording Schedule**.

Recording Schedule

Camera

[D1] Camera 01()

Record Status

Not Recording

☒ Enable

CMR

✕ Delete

🗑 Delete All

Open All

Advanced

0 2 4 6 8 10 12 14 16 18 20 22 24

Mon.

0 2 4 6 8 10 12 14 16 18 20 22 24

Tue.

0 2 4 6 8 10 12 14 16 18 20 22 24

Wed.

0 2 4 6 8 10 12 14 16 18 20 22 24

Thu.

0 2 4 6 8 10 12 14 16 18 20 22 24

Fri.

0 2 4 6 8 10 12 14 16 18 20 22 24

Sat.

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

📄 Copy to...

💾 Save

CMR

Motion Detection

ALARM

Figure 5-2 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.

Motion Detection

During the set time period, when a moving object in the set detection area is detected, the camera will start recording automatically.

4. Set the recording time.

- 1) Click **Open All** to enable all-day recording of all the dates, or 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.

- 2) Adjust the recording type and time.

- Click a set recording period, and you can edit the recording type.

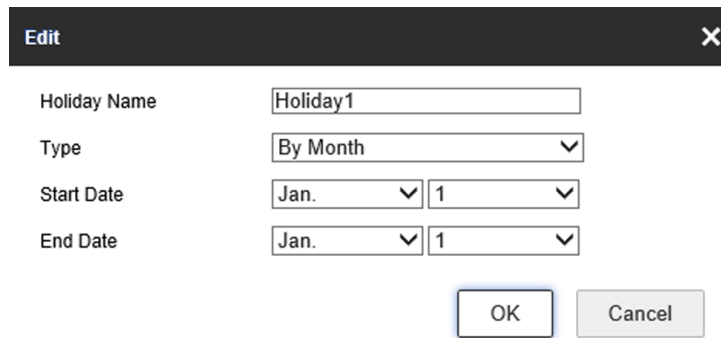
- Click a set recording period, enter the start time and end time in the pop-up window, and click **Save**.
- Drag two ends of the set recording period bar to adjust the length.
- Drag the whole set recording period bar and relocate it.
- 3) Optional: To delete the recording period, choose one way to delete it.
 - 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.
- 4) Click the icon  that appears on the right side of the timeline, copy the same time to other weeks, and click **OK**.
- 5. Optional: Click **Advanced** to set the camera record parameters.
 - Record Audio**
Enable the function to record audio.
 - Pre-record Time**
The time to start recording before the scheduled time.
 - Post-record**
The time to stop recording after the scheduled time.
 - Stream Type**
Select the recording stream type. The main stream offers higher video quality with larger recording files, while the sub-stream provides lower video quality with smaller file sizes.
 - 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.
- 6. Optional: Click **Copy to...**, check the camera(s), and click **OK**.
- 7. Click **Save**.

5.3 Set Holiday

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

Steps

1. Go to **Param Config > Storage > Advanced Settings > Holiday**.
2. Check the holiday date to set.
3. Set the holiday parameters.
 - 1) Click .



Edit [X]

Holiday Name:

Type:

Start Date:

End Date:

Figure 5-3 Set Holiday

- 2) Set **Holiday Name**, **Type**, **Start Date**, and **End Date**.
- 3) Click **OK**.
4. Optional: Repeat the previous step to set other holidays.

 Note

The holiday time of the same type cannot overlap.

5. Click **Save**.

Chapter 6 Record and Playback

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

Steps

1. Click **Playback**.
2. Select the camera.
3. Select the file date, and click **Search**.
4. Select the playback time.
 - Drag time bar and put the yellow line at the time point that you need.
 - Enter the specific time at **Set Playback Time**.
5. Click ► to play back the file.
6. Optional: During playback, you can also do the following operations.

Table 6-1 Button Description

	Pause		Play back the record files frame by frame.
	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.
	Reverse.		Enable/disable audio.
	Full screen.		Clip the recorded video.
	Digital zoom.		

Note

For the captured picture of playback saving path, refer to **Save snapshots when playback to** in **Param Config > Local > Capture and Clip Settings**.

Chapter 7 Encoding and Display

7.1 Set Video Encoding Parameters

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

Steps

- 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.

1. Go to **Param Config > Video & Audio > Video**.

Camera	[D1] Camera 01(	▼
Stream Type	Main Stream(Normal)	▼
Video Type	Video	▼
Resolution		▼
Bitrate Type	Constant Bitrate	▼
Image Quality	Highest	▼
Frame Rate		▼ fps
Max. Bitrate		Kbps
Video Encoding	H.264	▼

 Copy to...

 Save

Figure 7-1 Video Settings

Note

Video configuration is to set the parking space camera encoding parameters. The actual device prevails.

2. Select the 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. 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.

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.

7.2 Set Image Parameters

Set image parameters to adjust brightness and contrast.

Steps

1. Go to **Param Config > Image > Display Settings**.

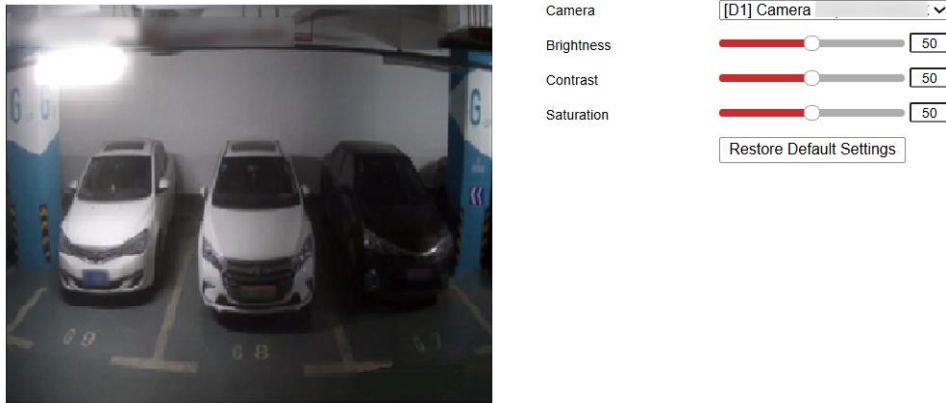


Figure 7-2 Display Settings

2. Select the camera.
3. Adjust the parameters to obtain clear images.

Brightness

Set the max. brightness of the image. Lower it appropriately if it is overexposed during daytime, and do not adjust at night.

Contrast

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

Saturation

It refers to the colorfulness of the image color. The larger the value, the more vivid the image.

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

7.3 Set OSD

You can customize OSD information on the live view.

Steps

1. Go to **Param Config > Image > OSD Settings**.

Camera [D1] Camera 01

☒ Display Name

☒ Display Date

☒ Display Week

Camera Name Camera 01

Time Format 24-hour

Date Format MM-DD-YYYY

Text Overlay

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

Copy to... Save

Figure 7-3 OSD Settings

2. Select the camera.
3. Set the display content according to actual needs.
 - 1) Check **Display Name**, and enter the camera name.
 - 2) Check **Display Date**, and set the time and date format.
 - 3) Check **Display Week**.
4. Optional: Check the text overlay No. and enter contents according to your needs.

Note

Up to 8 text overlays are allowed. The actual effect displayed on the live view image may vary with camera model.

5. Optional: To copy the settings to other cameras, click **Copy to...**, and check the camera(s).
6. Click **Save**.

Result

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

Chapter 8 Network Configuration

8.1 Set Internal IP Address

The internal network is for self-adaptive network interfaces on the device panel. The default IP address is 192.168.254.1. Only cameras with IP addresses in this subnet can connect to the device.

Steps

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

Figure 8-1 Set Internal IP Address

2. Select **NIC Type** according to the actual network.
3. Set the network parameters.
 - Check **Auto** to get the IP address automatically if the network supports distributing the IP address automatically.
 - Manually enter IP address, subnet mask, gateway, MTU, and other parameters.

Note

- The internal IP address and the device on the internal network segment should be set to the same network segment, and it must be set to a different network segment from the external IP address.
- **MTU** stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
- Set the DNS server if you need to visit the device with domain access.

4. Optional: Set the IPv6 parameters as needed.

5. Enable **NAT** if devices such as computers connected to the external G2 network interface need to access cameras connected to the internal G1 network interface.
6. Click **Save**.

8.2 Set External IP Address

The external network is set for the IP address of the G2 network interface on the device panel, and it mainly communicates with the external network (platform, remote host, etc.).

Steps

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

Figure 8-2 Set External IP Address

2. Select **NIC Type** according to the actual network.
3. Set the network information.
 - Check **Auto** to get the IP address automatically if the network supports distributing the IP address automatically.
 - Manually enter IP address, subnet mask, gateway, and other parameters.

Note

- The network segment of external IP address should be different from that of the internal IP address.
- **MTU** stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
- Set the DNS server if you need to visit the device with domain access.

4. Optional: Set the IPv6 parameters as needed.

5. Click **Save**.

8.3 Set DDNS

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

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters.
- 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 8-3 Set DDNS

2. Select **DDNS Type** according to the registered type.
3. Enter the server information and **Domain Name**.
4. Click **Save**.

What to do next

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

8.4 Set Port

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



Caution

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

Go to **Param Config > Network > Basic Settings > Port** for port settings. Click **Save** after finished

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.

Service Port

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



Note

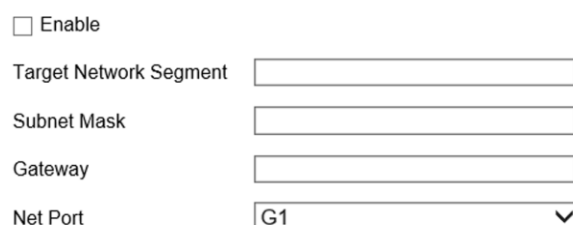
- Certain ports need to reboot after edited to take the new settings into effect.
 - When the device cannot edit the port No. via access Web due to port conflicts, you can connect the device to your computer and edit via SADP software.
-

8.5 Set Static Router

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

Steps

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



☐ Enable

Target Network Segment

Subnet Mask

Gateway

Net Port

Figure 8-4 Set 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 G1, set the G1 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 G2, set the G2 as a static router, and the external IP address will serve as the gateway.
6. Click **OK**.

Note

You can delete or edit the added router.

8.6 Connect to Platform

8.6.1 Connect to SDK

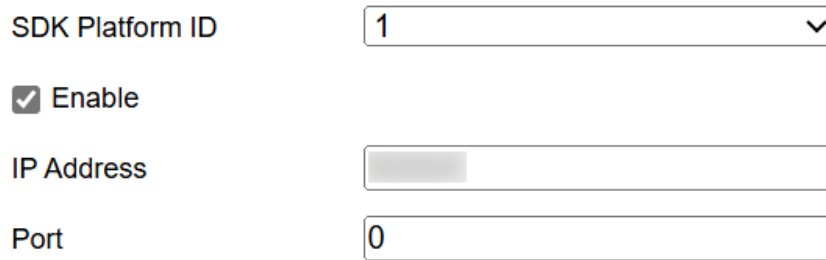
SDK is the platform access protocol. You can connect the device to the SDK platform to upload picture data and alarm information.

Before You Start

- Set the platform server first.
- Make sure that the network communication between the device and the platform is normal.

Steps

1. Go to **Platform Settings > Remote Host Connection > SDK**.



SDK Platform ID 1

☒ Enable

IP Address

Port 0

Figure 8-5 Connect to SDK Platform

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



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

5. Click **Save**.

What to do next

Click **Param Config > Platform Settings > Upload to Remote Host**, select **Upload Protocol** as **SDK Protocol**, and set the related parameters.

8.6.2 Connect to ISUP

ISUP is a platform access protocol. You can connect the device to the ISUP platform to realize live view and data management via the 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 8-6 Connect to ISUP Platform

2. Select **ISUP Platform ID**.
3. Check **Enable**.
4. Select protocol **Version**.

Note

Functions vary with different protocol versions.

5. Enter ISUP **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 shows online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

What to do next

Click **Param Config** > **Platform Settings** > **Upload to Remote Host**, select **Upload Protocol** as **ISUP**, and set the related parameters.

8.6.3 Connect to HTTP

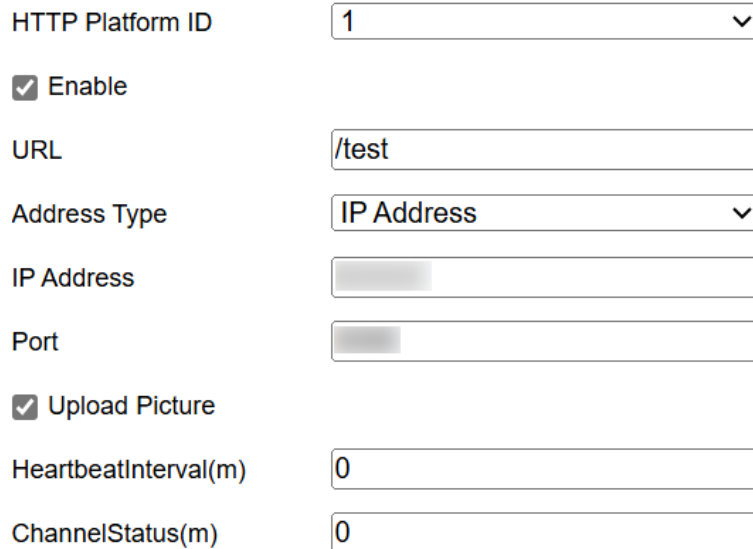
You can connect the device to HTTP platform to upload the pictures and alarm data to the remote host platform.

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
☒ Enable	
URL	/test
Address Type	IP Address
IP Address	
Port	
☒ Upload Picture	
HeartbeatInterval(m)	0
ChannelStatus(m)	0

Figure 8-7 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. Check **Upload Picture**, and set the upload interval of heartbeat and channel status.
7. Click **Save**.

What to do next

Click **Param Config > Platform Settings > Upload to Remote Host**, select **Upload Protocol** as **HTTP Protocol**, and set the related parameters.

8.6.4 Set Cloud Storage

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

Before You Start

- Arrange the cloud storage server.
- The **Picture Upload Mode** has been set to **Cloud Storage** under **Param Config > Platform Settings > Upload to Remote Host > Remote Host**, and **Picture Server ID** has been set.

Steps

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

Cloud Storage

IP Address

Port

Cloud Storage Server Parameters

Protocol Version

Central Management Port

User Name

Password

Storage Pool ID

Save

Figure 8-8 Set Cloud Storage

2. Select the cloud storage server ID.

Note

- The ID is the **Picture Server ID** that you set in **Param Config > Platform Settings > Upload to Remote Host > Remote Host**.
 - The parameters may vary with device model. The actual device shall prevail.
-

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

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.

User Name and Password

User name and password of the cloud storage server.

Bucket name

Set the storage pool name.

access_key

Key to access the cloud storage server.

secret_key

Key to encrypt the data uploaded to the cloud storage server.

5. Click **Save**.

8.6.5 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 the remote host.

Param Config

Upload Protocol	SDK Protocol
SDK Platform ID	1
Upload Strategy	Latest Data Priority
Data Type	0 Selected, Total 0
License Plate Color	11 items are selected.
Upload History Data	Disable
Upload No-Plate Data	Enable
Interval (ms)	50
Timeout (ms)	5000
Waiting For Upload Resp...	Disable
Upload Traffic Statistics P...	Disable
Picture Upload Mode	Direct Upload
Enable SDK Start Chann...	☒
Enable Passthrough data	☐

Figure 8-9 Set Remote Host

Note

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

3. Select **Upload Protocol** and the corresponding platform ID according to the actual communication protocol.
 - **HTTP Protocol**: select this mode when communicating via HTTP protocol.
 - **ISUP**: select this mode when communicating via ISUP protocol.
 - **SDK Protocol**: select this mode when communicating via SDK protocol.
 4. Set access parameters.
-

Note

The supported parameters may vary with device model. The actual device shall prevail.

Upload Strategy

Set the data upload method.

Data Type

Select the data type to upload to the remote host.

Note

The supported data type may vary with device model. The actual device shall prevail.

License Plate Color

Select the license plate color to upload.

Upload History Data

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

Upload No-Plate Data

Enable it to upload vehicle without license plate data to the remote host.

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 history data and uploaded according to history data rule.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Waiting For Upload Respond

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



Note

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

Picture Upload Mode

In SDK protocol, only **Direct Upload** is available; In ISUP protocol, only **Cloud Storage** is available; In HTTP protocol, **Cloud Storage** and **Direct Upload** are available.

- **Direct Upload**: The device uploads data to the platform directly.
- **Cloud Storage**: The device uploads data to the cloud storage server to generate a URL, then uploads the URL and alarm information to the platform. This requires you to set **Picture Server ID** as needed.

Enable SDK Start Channel No.

Enable it for compatibility with different versions of SDK protocol platforms. Disable it for platforms that don't support analogue signal channel No. reservation.

Enable Passthrough data

When enabled, alarm data that the device does not support processing will be directly uploaded to the platform.

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

1) Set **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 history 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**.

6. Click **Save**.

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

Chapter 9 Data Management

9.1 Set Picture and Video Export Rule

You can set the naming and path of the pictures and videos to be exported, and back them up to the set path on your computer.

Steps

1. Set the picture export rule.
 - 1) Go to **Param Config > Backup Settings > Web Backup > Web Backup Settings**.
 - 2) Enter the name, path, and other information of the picture and video, and click **OK**.
 - 3) Set the parameters below.

Replacement Characters

Set the replacement characters when the license plate is not recognized.

Random Number Digits

After random number digits are 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.

- 4) 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

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

9.2 Search Data

You can search the traffic data according to the camera channel, including license plate No. and parking space No.

Before you start

Traffic data has been stored normally.

Steps

1. Go to **Data Search > Traffic Data Search**.
2. Select time and other search conditions.



There must be less than 7 days between start time and end time.

3. Click **Search**.

The device will display the search result.

Start Time: 2025-03-12 00:00:00 End Time: 2025-03-17 23:59:59 Data Type: Parking Space Detecti Camera: Select

Search Export

License Plate Number: Parking Space No.: License Plate Color: Select Vehicle Status in Park...: -- All --

Remote Host: -- All --

No.	License Plate ...	License Pla...	Chan...	Capture Time	Parking Spac...	Logical Parking S...	Vehicle Status in Park...	Parking over ...	Remote Ho...	Remote Ho...	Details
1	unknown	Others	18	2025-03-12 01:14:55.392	2-4	3	Occupied	no	No need to s...	No need to s...	Details
2	unknown	Others	18	2025-03-12 01:15:01.016	2-4	3	Unoccupied	no	No need to s...	No need to s...	Details
3	unknown	Others	18	2025-03-12 08:07:59.113	2-4	3	Occupied	no	No need to s...	No need to s...	Details
4	unknown	Others	18	2025-03-12 08:08:04.729	2-4	3	Unoccupied	no	No need to s...	No need to s...	Details
5	unknown	Others	18	2025-03-12 10:14:13.498	2-4	3	Occupied	no	No need to s...	No need to s...	Details
6	unknown	Others	18	2025-03-12 10:14:19.371	2-4	3	Unoccupied	no	No need to s...	No need to s...	Details
7	unknown	Others	18	2025-03-12 10:48:38.616	2-4	3	Occupied	no	No need to s...	No need to s...	Details
8	unknown	Others	18	2025-03-12 10:48:44.756	2-4	3	Unoccupied	no	No need to s...	No need to s...	Details

20 Total 348 Item(s) 1/18

Figure 9-1 Search Data

- Click **Details** to view the vehicle pictures, videos, and other details.
- Optional: Click **Export** to export the selected data information to the specified path.

Note

- If the exporting failed, please add the IP address of the channel as a trusted site in the browser.
- To set the saving path, refer to [9.1 Set Picture and Video Export Rule](#).

9.3 View Parking Space Status

You can view the occupancy status, license plate number, indicator color, etc. of the detected parking spaces.

Before You Start

Traffic data has been stored normally.

Steps

- Click **Status**.
The status of the parking spaces monitored by the connected camera is displayed:
 - Green indicates the space is available, and red indicates the space is occupied.
 - Each channel allows up to 3 parking spaces. Blank means no parking space exits.
- Click a parking space to view the vehicle information and image on the right side. You can double-click the image to enlarge it, and double-click again to return it to the original size.

Chapter 10 Alarm Configuration

10.1 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**.

Alarm Output No. IP Address

Default Status Triggering Status

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon.	[Blue bar]												
Tues.	[Blue bar]												
Wed.	[Blue bar]												
Thur.	[Blue bar]												
Fri.	[Blue bar]												
Sat.	[Blue bar]												
Sun.	[Blue bar]												

Figure 10-1 Set Alarm Output

2. Select **Alarm Output No.**, and edit **Alarm Name**.

3. Select **Delay**.

The device will send out alarm output signal for the set time.

4. Click **Arming Schedule** to set the arming schedule.

Note

To enable all-day recording of all the date (7 × 24), click **Open All**. Refer to [5.2 Set Record Schedule](#) for details.

5. Optional: Click **Manual Alarm** to enable manual alarm output. Set according to the actual needs.



Note

You need to click **Clear Alarms** to stop the alarm manually after you click **Manual Alarm**. Set it as needed.

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

10.2 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.

3. Set the linkage method.
 - When an event occurs, if you need to upload alarm information to the platform that the device has been connected to, check **Notify Surveillance Center**.
 - When an event occurs, if you need to report the alarm information to the connected monitoring interface, check **Full Screen Monitoring**.
 - When an event occurs, if you need to trigger an alarm by the external alarm device connected to the alarm output interface, select **Trigger Alarm Output**.
4. Click **Save**.

Chapter 11 Safety Management

11.1 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 that you create a strong password of your own choosing in order to increase the security of your product. Change the password of your account regularly.

1. Go to **Param Config > System > User Management > User Management**.
2. Add a user.
 - 1) Click **Add**.
 - 2) Enter the user name, password, and other information in the popup window.
 - 3) Enter **Admin Password**.
 - 4) Click **OK**.
3. Optional: You can also do the following operations.

Delete the User	Select a user, and click Delete to delete the user.
Edit the User Information	Click the user name of the added user, and click Edit to edit the user information.
View online user	Click Online User , and click Refresh to view online user information, including username, type, IP address, and user operation time.

11.2 Set HTTPS

11.2.1 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, Domain Name/IP**, etc., and click **OK**.
4. 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.

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

What to do next

Enter <https://device> IP address (e.g., 192.168.1.64): HTTPS port e.g., 443) in the browser, press Enter, and follow the prompts to download and install the certificate before logging into the device.

11.2.2 Create and Install Self-signed Certificate

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

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, Domain Name/IP**, etc., and click **OK**.
5. Check **Enable**.
6. Click **Save**.

What to do next

Enter <https://device> IP address (e.g., 192.168.1.64): HTTPS port e.g., 443) in the browser, press Enter, and follow the prompts to download and install the certificate before logging into the device.

11.3 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**.

11.4 Set Log Server

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. Due to limited storage space, you are recommended to save the logs on a log server.

Steps



Note

The function may vary with device model. The actual device shall prevail.

1. Go to **Param Config > System > Security > Security Service > Log Audit Service**.
2. Check **Enable the Syslog 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.

11.5 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Param Config > System > Security > Security Enhancement**.
2. Check **Enable Timeout Logout for Static Page**.
3. Set **Session Expired Time (min)**.
4. Click **Save**.

Result

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

Chapter 12 Maintenance

12.1 View Device Information

Go to **Param Config > System > System Settings > Basic Information** to view the device basic information, including device model, software version, etc.

You can edit **Device Name**. The device No. is used to control the device, and the default value is recommended.

12.2 Synchronize Time

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

Steps



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.



NTP Time Sync. is available only when the communication between the device and the NTP server is normal.

Manual Time Sync.

Select it to synchronize the device time with that of the computer. You can 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.

4. Click **Save**.

12.3 Set RS-485

Set RS-485 parameters if the device needs to be connected to a RS-485 device.

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**.
2. Select the channel.
3. 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.
-

4. Click **Save**.

12.4 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 > RS232**.
2. Set RS-232 parameters including baud rate, data bit, etc. according to the connected peripheral devices.

Note

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

3. Select **Control Mode**.

Transparent Channel

For the data transmission of peripheral devices.

Control Panel (By Parameter)

For the serial port debugging of the device.

4. Click **Save**.

12.5 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**.
2. Click **Reboot**.
3. Click **OK** to reboot the device.

Reboot

When checked, the device will reboot automatically in every 2 a.m.

Reboot Without HDD

The device will reboot after no HDD is detected.

12.6 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**.

12.7 Restore Database

You can restore the database if database exception occurs.

Go to **Param Config > System > System Maintenance > Upgrade & Maintenance > Restore Database**., and click **Restore** to restore the database.

12.8 Export Parameters

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

Before You Start

Add the trusted site.

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**.

12.9 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



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.

12.10 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.



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

Result

The device will reboot automatically after upgrade.

12.11 Search Log

You can search logs to troubleshoot problems.

Before You Start

HDD storage is normal.

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.

12.12 View System Status

Go to **Param Config > System Status > Server Status\Status** to view the server status and the connected camera status.

Server Status

- **Working Status:** View the system time, working time, mainboard temperature, cabinet door status, and GPS device status.

Camera Status

- **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.

12.13 Reserved Parameters

The reserved parameters are only for technical personnel to debug.

12.14 Set Other Parameters

You can set the device arming level, camera time synchronization threshold, etc.

Before You Start

Ensure the parking cameras are connected.

Steps

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

Arming Level	Level 1
Camera Time Synchroniz...	Enable
Camera Time Sync. Thre...	2
Pre-record (s)	4
Post-record (s)	6
Longest Recording Time (s)	60
Cabinet Door Name	Equipment Cabinet Door
Cabinet Door No.	12345

Figure 12-1 Set Working Mode

2. Select **Arming Level**.

Note

- 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.
-

3. Select **Camera Time Synchronization**.

4. Set **Camera Time Sync. Threshold**, and the camera will synchronize time if the set threshold is exceeded.

5. Set record time parameters.

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.

6. Enter **Cabinet Door Name** and **Cabinet Door No.** based on the actual cabinet door connected to the device.

7. Click **Save**.



See Far, Go Further