



Parking Camera

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 Introduction	1
1.1 Introduction	1
1.2 Key Feature	1
Chapter 2 Activation and Login	2
2.1 Activation.....	2
2.1.1 Default Information	2
2.1.2 Activate via SADP	2
2.1.3 Activate via Web Browser	3
2.2 Login	4
Chapter 3 Parking Space Detection	5
3.1 Set Detection Rules	5
3.2 Set Parking Space Indicator.....	6
3.3 View Parking Space Status	8
3.4 Typical Application.....	8
3.4.1 Internal/External Indicator Application	8
3.4.2 Internal and External Indicator Application	10
3.4.3 Alternate Indicator Control Application	11
3.4.4 Special Parking Space Application	12
Chapter 4 Capture Configuration.....	13
4.1 Set Capture Parameters	13
4.1.1 Set Image Encoding Parameters.....	13
4.1.2 Set Capture Overlay	13
4.2 View Real-Time Picture	15
Chapter 5 Live View and Local Configuration	17
5.1 Live View.....	17
5.1.1 Start/Stop Live View	17
5.1.2 Select Image Display Mode	17
5.1.3 Select Window Division Mode	17
5.1.4 Select Stream Type.....	17

5.1.5 Capture Picture Manually	17
5.1.6 Record Manually	18
5.1.7 Enable Digital Zoom	18
5.1.8 Select Video Mode	18
5.2 Local Configuration	18
Chapter 6 Storage.....	22
6.1 Set FTP	22
6.2 Set SDK Listening	23
6.3 Set Arm Host	24
6.4 Set ISAPI Listening.....	25
6.5 Set Cloud Storage.....	25
Chapter 7 Encoding and Display	27
7.1 Set Video Encoding Parameters	27
7.2 Set Image Parameters	28
7.3 Set ROI	31
7.4 Enable Regional Exposure	32
7.5 Set OSD	32
Chapter 8 Network Configuration	35
8.1 Set IP Address	35
8.2 Connect to ISUP Platform	38
8.3 Set DDNS.....	39
8.4 Set Port	40
8.5 Set Bluetooth	41
Chapter 9 Alarm Configuration.....	43
9.1 Set Motion Detection.....	43
9.2 Exception Alarm.....	44
Chapter 10 Safety Management.....	46
10.1 Manage User	46
10.2 Enable User Lock	47
10.3 Set HTTPS	47
10.3.1 Create and Install Self-signed Certificate.....	47

10.3.2 Install Authorized Certificate	47
10.4 Set SSH	48
10.5 Set RTSP Authentication	48
10.6 Set IP Address Filtering	48
10.7 Set Timeout Logout	49
10.8 Set Password Validity Period	49
Chapter 11 Maintenance	50
11.1 View Device Information	50
11.2 Log	50
11.2.1 Enable System Log Service	50
11.2.2 Search Log	50
11.2.3 Search Security Audit Log	51
11.3 Upgrade	51
11.4 Reboot	52
11.5 Restore Parameters	52
11.6 Synchronize Time	52
11.7 Debug Device	53
11.8 Set DST	53
11.9 Export Parameters	54
11.10 Import Configuration File	54
11.11 Export Debug File	55
11.12 Export Diagnosis Information	55
A. Communication Matrix and Device Command	56

Chapter 1 Introduction

1.1 Introduction

The parking camera (hereinafter referred to as device) is applied in the parking guidance and find my car system to detect whether the parking space is occupied or not and recognize the license plate. It is integrated with the parking space status indicator which can indicates red, green, yellow, blue, cyan, and magenta colors. Red indicates the parking space is occupied, green indicates the parking space is available, and blue indicates the parking space is reserved.

The device can be widely applied in the environment with dark light, such as road, warehouse, underground garage, bar, garden, etc. to provide HD display.

1.2 Key Feature

- Supports ANPR, detection of the parking space status, and smart analysis of crossing over line, motion detection, etc.
- HD camera, applied in environment with low illumination such as underground garage.
- 3D noise reduction to guarantee clean and exquisite image.
- Smart detection of the parking space status, and smart analysis of crossing over line, motion detection, etc.
- Energy-saving LED with high brightness and low consumption.
- Speed recognition in second accuracy to indicate the parking space status in real time and provide accurate available parking space number.
- Network wiring with easy connection, installation, and maintenance.
- ROI encoding.
- Two RJ45 interfaces, supporting connecting cameras in series, and no power cord is needed.
- Dual-stream.
- Built-in iBeacon module, supporting indoor positioning and navigation with the help of APP. iOS or Android SDK is provided.

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: 192.0.0.64
- 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.

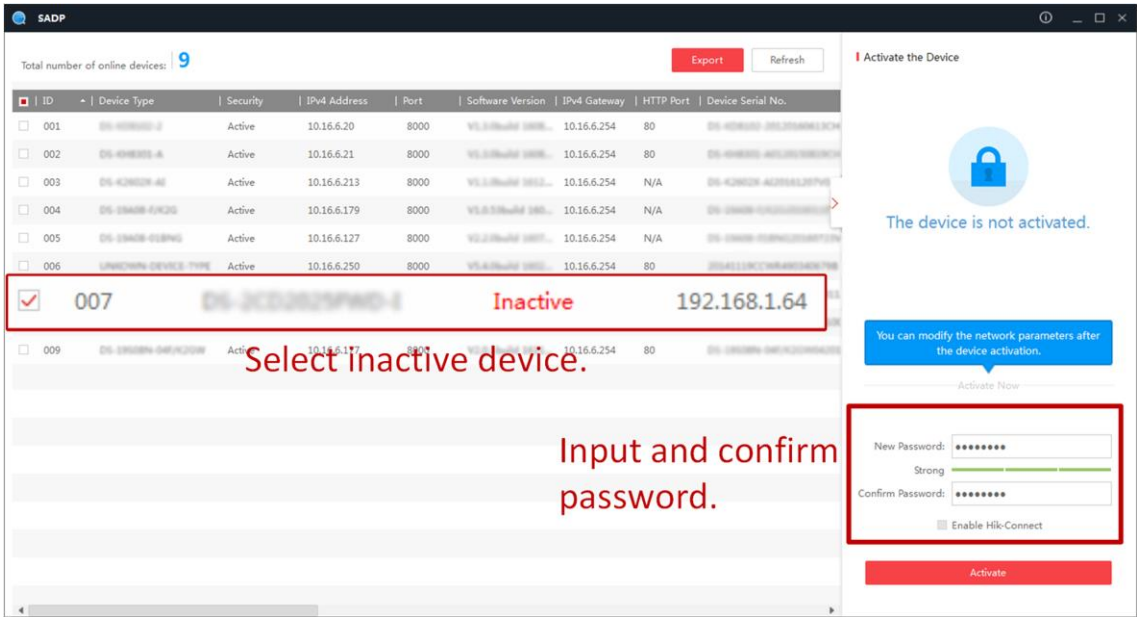
Before You Start

- 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.



2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
3. Create and confirm the admin password.

Caution

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

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

2.2 Login

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

Before You Start

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

Steps

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

Chapter 3 Parking Space Detection

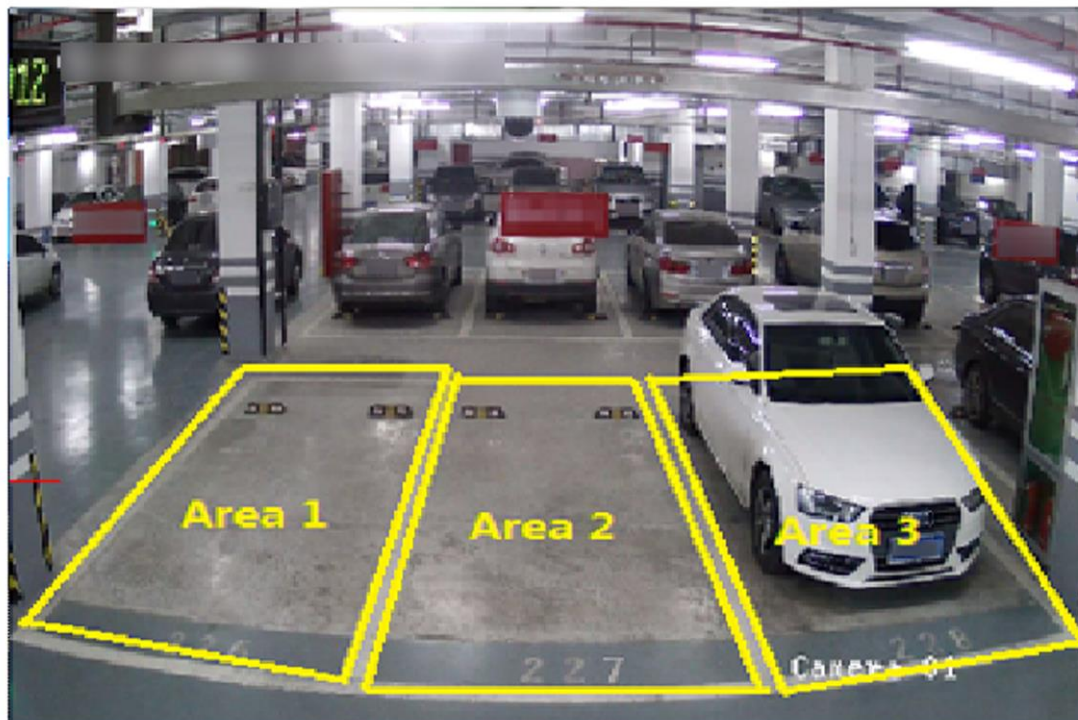
3.1 Set Detection Rules

To detect the parking spaces, you should enable the smart analysis and set the parameters of parking spaces.

Steps

1. Go to **Configuration** → **Capture** → **Smart Analysis** → **Analytics Parameters**

Parking Space Area



Channel Management	Channel 1	
Recognized Parking Space(s)	3	
Parking Space1	Parking Space2	Parking Space3
Parking Space No. 1		
Special Parking Space <input type="radio"/> Yes <input checked="" type="radio"/> No		

Figure 3-1 Smart Analysis

2. Optional: Select a channel.
3. Select the number of **Recognized Parking Space(s)**.

Note

The number may vary with different models.

According to the number of spaces you set, the quadrilateral(s) of the parking space area(s) will appear in the image.

4. Click the tab of the parking space No. to set the parameters.
 - 1) Enter **Parking Space No.**
 - 2) Click **Yes** if the parking space is a special parking space.
5. Adjust the parking space areas.
 - 1) Select a quadrilateral, and drag the vertices of the quadrilateral to adjust its shape, or drag the quadrilateral to adjust the position.
 - 2) Repeat the step above to adjust other areas.
6. Click **Save**.

3.2 Set Parking Space Indicator

The indicator indicates the parking space status. Different colors stand for different status. You can set the indicator colors and flashing status for different parking space status.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Parking Space Indicator**.

The screenshot displays the 'Parking Space Indicator' configuration page. At the top, 'Indicator Control Mode' is set to 'Internal Indicator'. Below this, the 'Parking Space Indicator Parameters' section contains a table with four rows: 'Occupied', 'Unoccupied', 'Over Line', and 'Special Parking Space'. Each row has three columns: 'Enable', 'Indicator Flicker', and 'Indicator Color'. The 'Enable' column has dropdown menus with 'Yes' or 'No' selected. The 'Indicator Flicker' column has dropdown menus with 'No' selected. The 'Indicator Color' column has dropdown menus with 'Red', 'Green', 'Yellow', and 'Blue' selected respectively. At the bottom, the 'Alternate Indicator Control Parameters' section has an 'Enable' checkbox (unchecked) and an 'IP Address' field with '0.0.0.0'.

Parking Space Status	Enable	Indicator Flicker	Indicator Color
Occupied	Yes	No	Red
Unoccupied	Yes	No	Green
Over Line	No	No	Yellow
Special Parking Space	No	No	Blue

Alternate Indicator Control Parameters

Enable ☐

IP Address 0.0.0.0

Figure 3-2 Set Parking Space Indicator

2. Select **Indicator Control Mode**.

Internal Indicator

The parking space status is informed via the internal indicator of the device.

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.

3. Set the indicator parameters for different parking space status.
 - 1) Optional: Select **Indicator Source** if you have selected **Internal & External Indicator** for **Indicator Control Mode**.
 - 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.
4. Optional: If there are symmetric parking spaces on both sides, and the distance between the device to the monitored parking space lines is too far, you can enable alternate indicator control and set the parameters.
 - 1) Check **Enable** of **Alternate Indicator Control Parameters**.
 - 2) Enter **IP Address** of the device on the opposite parking space.The current device can control the indicator of the device on the opposite parking space, and vice versa.
5. Click **Save**.

Note

For the detailed application of the different indicator control modes, refer to "Typical Application" for details.

3.3 View Parking Space Status

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

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Parking Space Status**.
2. View the parking space status.

Parking Space No.	Occupancy Status	License Plate Number	Indicator Flickering Status	Indicator Color
1	Unoccupied		No	Green
2	Unoccupied		No	Green
3	Unoccupied		No	Green
1	Unoccupied		No	Green
2	Unoccupied		No	Green
3	Unoccupied		No	Green

Figure 3-3 Parking Space Status

3.4 Typical Application

In this section, the typical applications of the internal indicator control mode, external indicator control mode, alternate indicator control mode, and special parking space will be illustrated.

3.4.1 Internal/External Indicator Application

Note

Here we take example of the scene in which a device monitors three parking spaces.

In internal/external indicator application, the indicator displays the color of occupied status when the three spaces are all occupied. The indicator displays the color of unoccupied status when any of the spaces is free. The indicator displays the color of over line when a parked vehicle occupies two spaces.

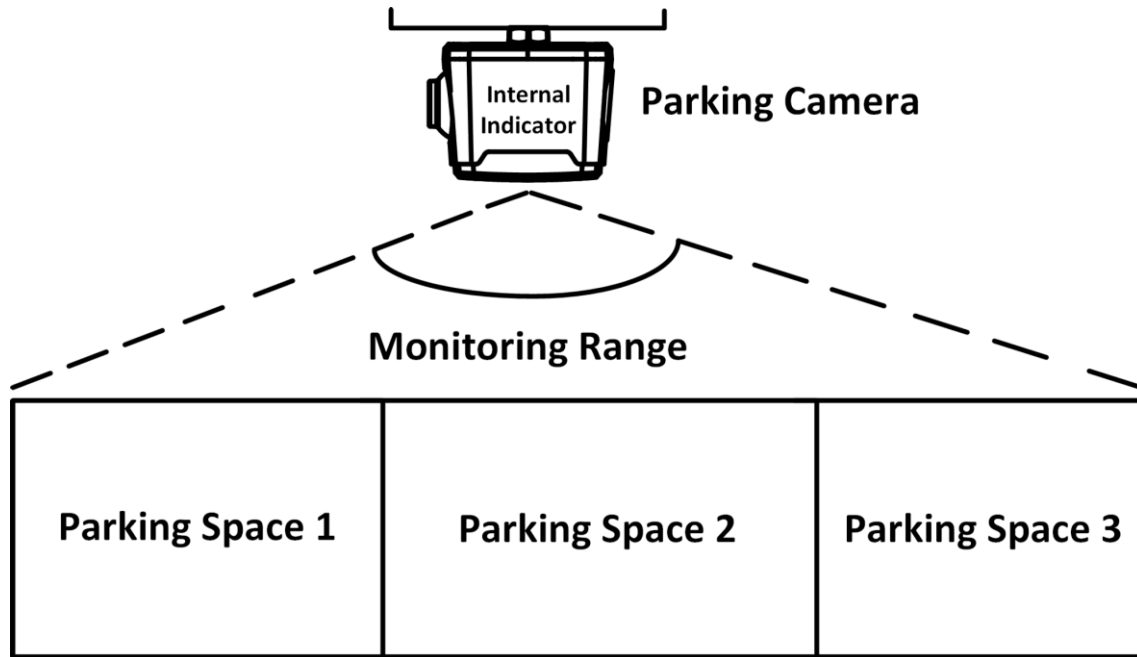


Figure 3-4 Internal Indicator Application

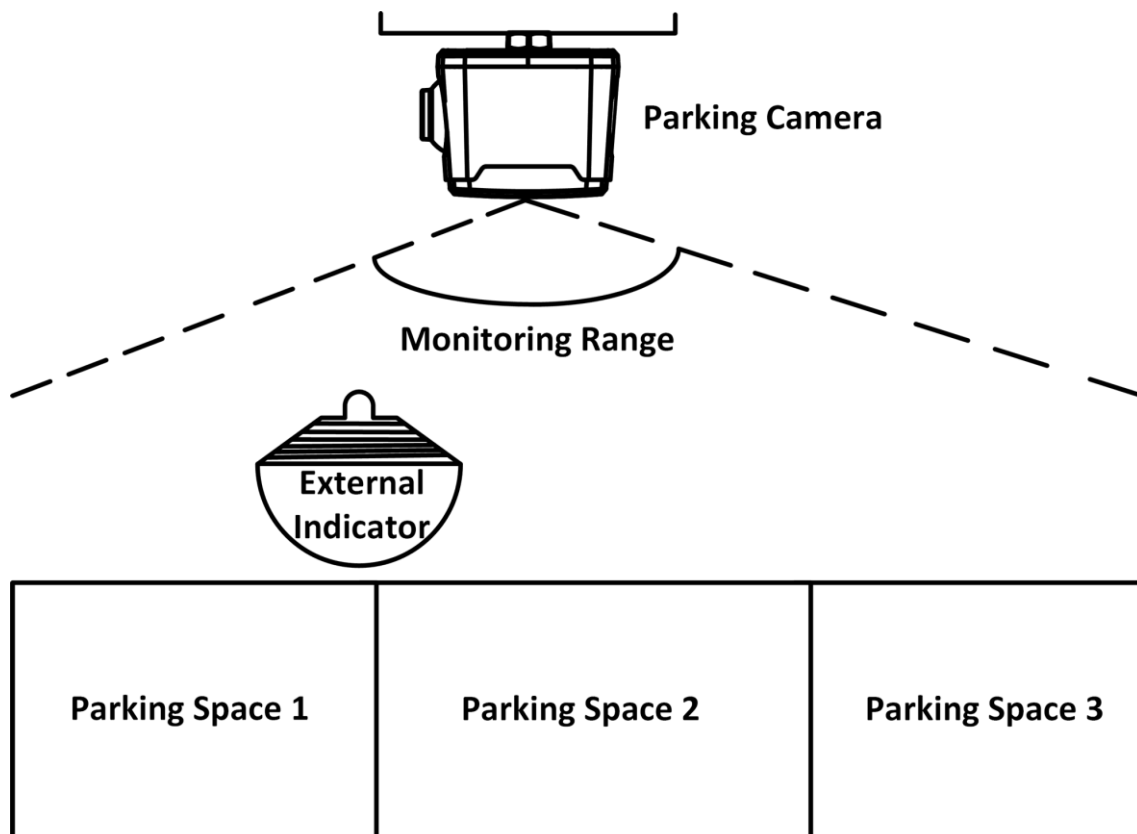


Figure 3-5 External Indicator Application

3.4.2 Internal and External Indicator Application

Note

Here we take example of the scene in which a device monitors three parking spaces.

In internal and external indicator application, the internal and external indicators work at the same time. All the indicators display the set colors for different parking space status. E.g., the parking camera A controls the internal indicator B, the external indicator 2 of parking camera A, and the external indicator 2 of parking camera B, and detects the status of the parking spaces B1 to B3. The parking camera B controls the internal indicator A, the external indicator 1 of parking camera A, and the external indicator 1 of parking camera B, and detects the status of the parking spaces A1 to A3, as shown below. After the settings, the external indicator 2 of parking camera A will display the different status of parking space B1, the internal indicator B will display the different status of parking space B2, and the external indicator 2 of parking camera B will display the different status of parking space B3. The external indicator 1 of parking camera A will display the different status of parking space A1, the internal indicator A will display the different status of parking space A2, and the external indicator 1 of parking camera B will display the different status of parking space A3.

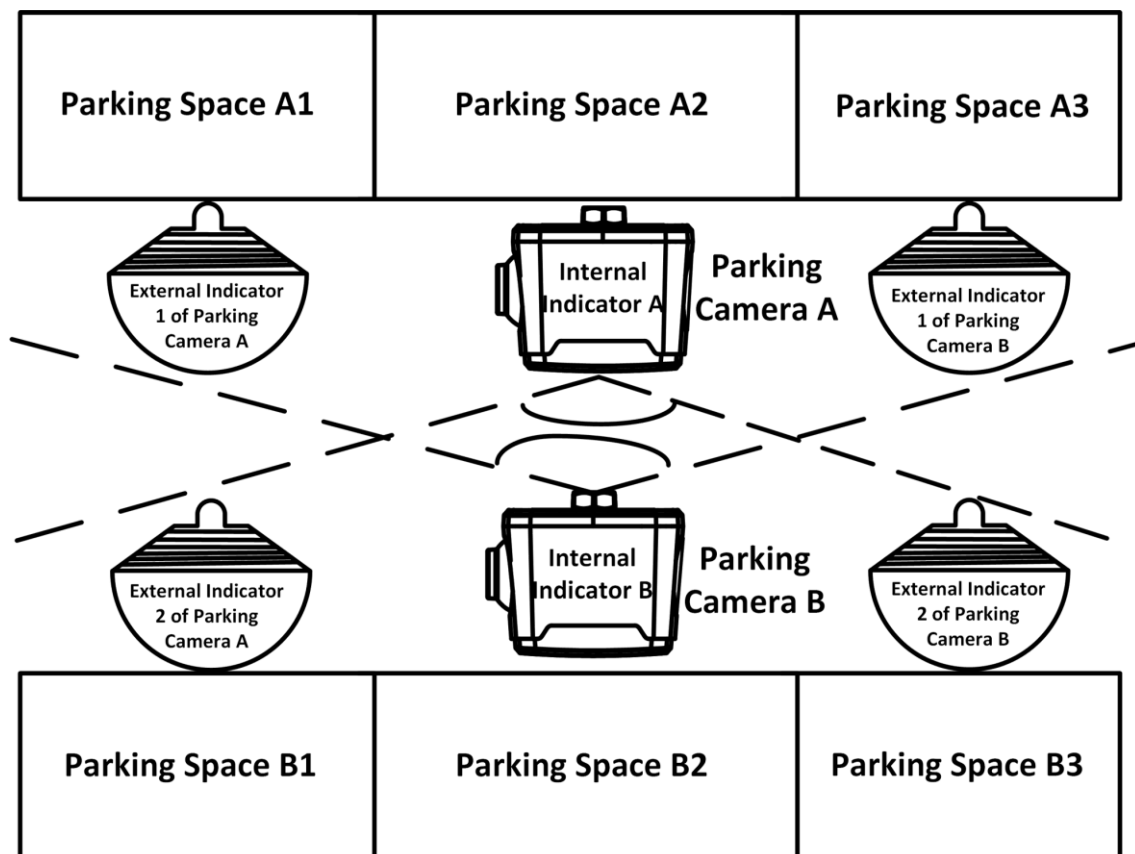


Figure 3-6 Internal and External Indicator Application

3.4.3 Alternate Indicator Control Application



Note

Here we take example of the scene in which two devices monitor six parking spaces.

The alternate indicator control is applicable to the parking lot where there are symmetric parking spaces on both sides, and the distance between the device to the monitored parking space lines is too far.

E.g., the parking camera A controls the indicator B and detects the status of the parking spaces B1 to B3, while the parking camera B controls the indicator A and detects the status of the parking spaces A1 to A3, as shown below. After the settings, the indicator A/B will display the color of occupied status when the parking spaces A1 to A3/B1 to B3 are all occupied. The indicator A/B will display the color of unoccupied status when any of the three spaces is free. The indicator A/B will display the color of over line when a parked vehicle occupies two spaces.

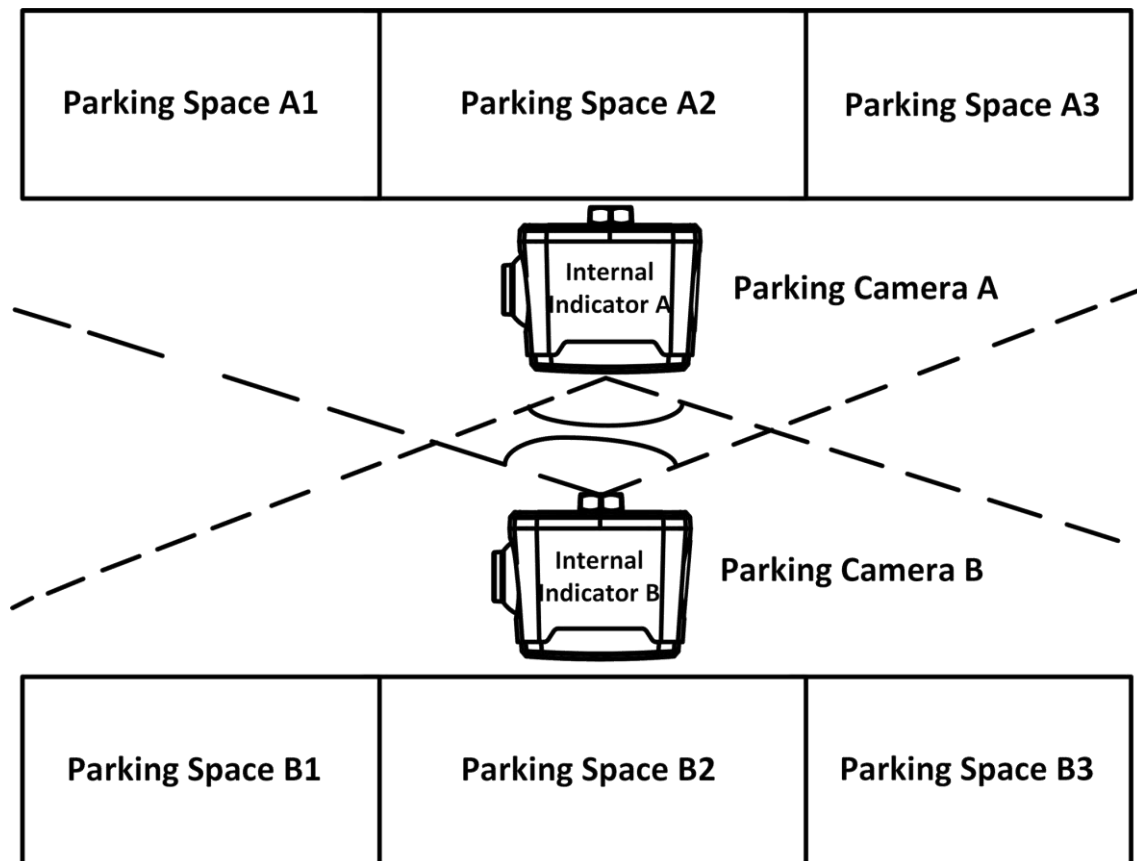


Figure 3-7 Alternate Indicator Control Application

3.4.4 Special Parking Space Application

Note

Here we take example of the scene in which a device monitors three parking spaces.

E.g., the parking space 1 is set as a special parking space in the monitoring range, and its status is indicated by the external indicator 1 connected to the device. Then the external indicator 1 will display the set color for the special parking space, and the occupied, unoccupied, or over-line status is invalid for the indicator.

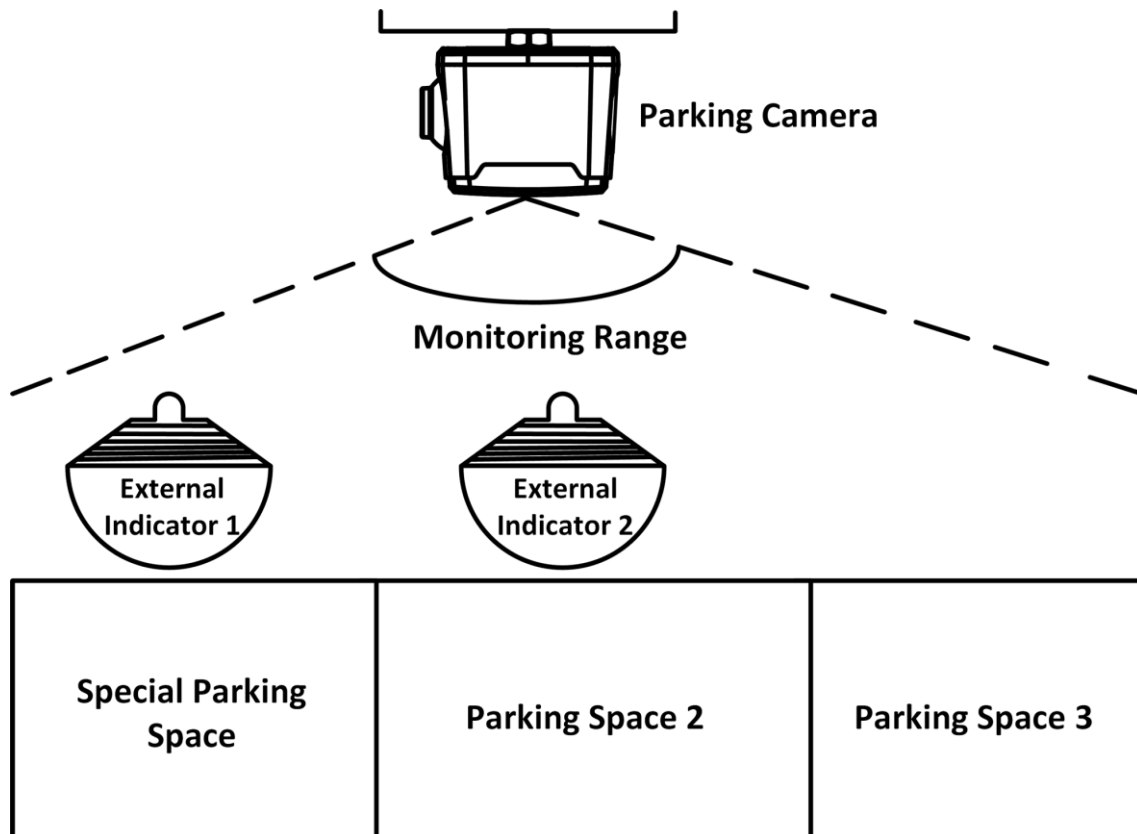


Figure 3-8 Special Parking Space Application

Chapter 4 Capture Configuration

4.1 Set Capture Parameters

4.1.1 Set Image Encoding Parameters

If the captured pictures are not clear, set the resolution of the captured pictures and the picture size.

Steps

1. Go to **Configuration** → **Capture** → **Capture Parameters** → **Picture Encoding and Composition**.

Image Encoding

Capture Resolution	2688*1520
JPEG Picture Size(KB)	512


 Save

Figure 4-1 Set Image Encoding Parameters

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

4.1.2 Set Capture Overlay

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

Steps

1. Go to **Configuration** → **Capture** → **Capture Parameters** → **Text Overlay**.
2. Click **Checkpoint Single**.
3. Check **Capture Picture Overlay**.

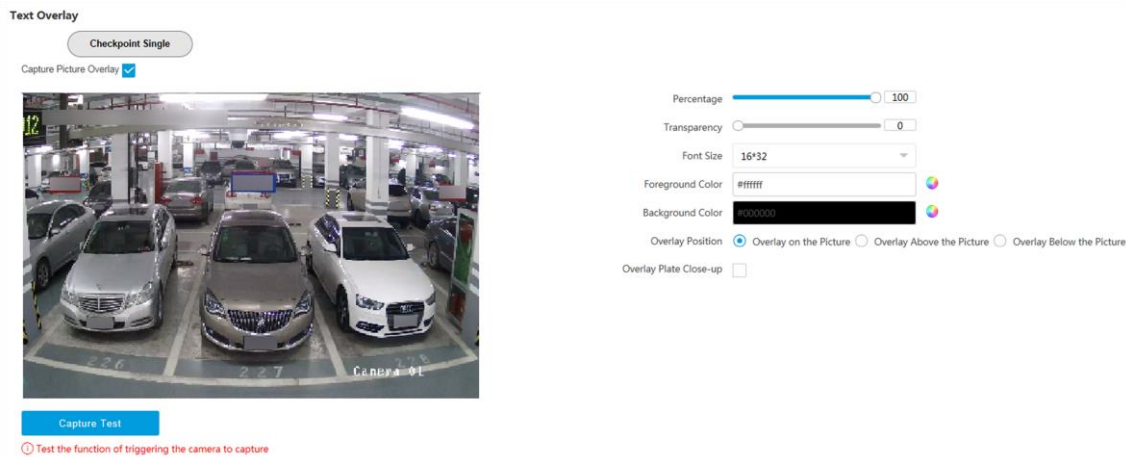


Figure 4-2 Set Capture Overlay

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

Percentage

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

Overlay Plate Close-up



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

5. Select the overlay information from the list.

Note

The overlay information may vary with different models. The actual device prevails.

6. Set the overlay information.

Type	You can edit the type.
Overlay Information	For some information type, you can edit the detailed information.
Overlay Position	If you select Overlay on the Picture , you can check it. Then the current information will be displayed from a new line.
Space	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
Line Break Characters	Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
Adjust overlay sequence	Click  /  to adjust the display sequence of the overlay information.

7. Click **Save**.

4.2 View Real-Time Picture

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

Steps

1. Go to **Live View** → **Real-Time Capture**.
2. Click **Arming**.
3. Select an item from the list, and you can view the capture scene picture and recognized license plate information.

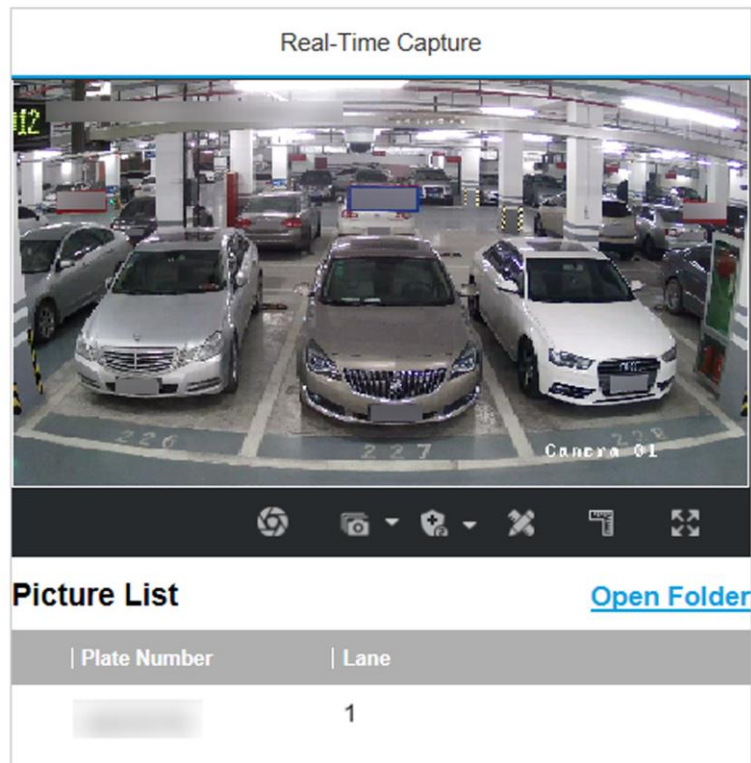


Figure 4-3 Real-Time Picture

4. Optional: You can also do the following operations.



- **Level 1 Arming** can only connect one client or web. The uploaded pictures will not be stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming.
- **Level 2 Arming** can connect three clients or webs. The pictures will be uploaded to the client/web, and stored in the storage card.
- **Disarming** is to cancel the alarm status or real-time picture.



Click it to measure the license plate pixel. Click it again to disable the measurement.



Click it to enable the ruler to measure the license plate.



Click it to enable manual capture.



Click it to set continuous capture parameters and the device will capture pictures according to the set interval.

- **Capture Times:** Up to five pictures can be captured per continuous capture.
- **Interval:** Up to four intervals can be set, and the default interval is 100 ms.



Display the images in full screen mode.



Open Folder

Open the saving path of captured pictures.


Chapter 5 Live View and Local Configuration

5.1 Live View

5.1.1 Start/Stop Live View

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

5.1.2 Select Image Display Mode

Click  to select an image display mode.

5.1.3 Select Window Division Mode


Click  to select a window division mode.



Note

For the dual-lens camera, you can select the 2 × 2 mode to show the images of both lens.

5.1.4 Select Stream Type

Click  to select the stream type. It is recommended to select the main stream to get the high-quality image when the network condition is good, and select the sub-stream to get the fluent image when the network condition is not good enough. The third stream is the custom stream.



Note

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

5.1.5 Capture Picture Manually

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


Steps

1. Click  to capture a picture.
2. Optional: Click **Configuration** → **Local** → **Picture and Clip Settings** to view the saving path of snapshots in live view.

5.1.6 Record Manually

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




Steps

1. Click  to start live view.
2. Click  to start recording.
3. Click  to stop recording.
4. Optional: Click **Configuration** → **Local** → **Record File Settings** to view the saving path of record files.

5.1.7 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.

5.1.8 Select Video Mode

Set the video mode when adjusting the device focus during construction.

Click  and select  when the device is running normally.

5.2 Local Configuration

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

Live View Parameters

Protocol Type

☒ TCP☐ UDP☐ HTTP☐ HTTPS

Stream Type

☒ Main Stream☐ Sub-Stream

Live View Performance

☐ Shortest Delay☒ Balanced☐ Fluency

Decoding Type

☒ Software Decoding☐ Hardware Decoding

Rules Information

☐ Enable☒ Disable

Feature Information

☐ Enable☒ Disable

Image Size

☒ Auto-fill☐ 4:3☐ 16:9

Image Format

☒ JPEG☐ BMP

Record File Settings

Record File Size

☐ 256M☒ 512M☐ 1G

Save record files to

D:\

Browse

Save downloaded files to

D:\

Browse

Picture and Clip Settings

Save snapshots in live view to

D:\

Browse

Save downloaded pictures to

D:\

Browse

Save scene pictures to

D:\

Browse

Save snapshots when playback to

D:\

Browse

Save clips when playback to

D:\

Browse

Figure 5-1 Local Configuration

Protocol Type

Select the network transmission protocol according to the actual needs.

TCP

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

UDP

Provides real-time audio and video streams.

HTTP

Gets streams from the device by a third party client.

HTTPS

Gets streams in https format.

Stream Type

Main Stream

Select it to get the high-quality image when the network condition is good.

Sub-Stream

Select it to get the fluent image when the network condition is not good enough.

Live View Performance

Shortest Delay

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

Balanced

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

Fluency

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

Decoding Type

Software Decoding

Decode via software. It takes up more CPU resources but provides images with better quality when it compares to the hardware decoding.

Hardware Decoding

Decode via GPU. It takes up less CPU resources but provides images with worse quality when it compares to the software decoding.

Rules Information

If you enable the rule information, tracking frames will be displayed on the live view interface when there are vehicles passing.

Feature Information

Enable it to display feature information of the target in the live view image.

Image Size

The display ratio of live view.

Image Format

The saving format of manually captured images.

Record File Size

Select the packed size of the manually recorded video files. After the selection, the max. record file size is the value you selected.

Save record files to

Set the saving path for the manually recorded video files.

Save downloaded files to

Set the saving path for the download files.

Save snapshots in live view to

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

Save downloaded pictures to

Set the saving path for the downloaded pictures.

Save scene picture to

Set the saving path of the captured pictures in **Live View** → **Real-Time Capture**.

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.

Chapter 6 Storage

6.1 Set FTP

Set FTP parameters if you want to upload the captured pictures to the FTP server.

Before You Start

Set the FTP server, and ensure the device can communicate normally with the server.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **FTP**.



Figure 6-1 Set FTP

2. Check **Enable FTP**.
3. Select **Number of Enabled FTP**.



Note

You can only enable one FTP.

4. Set FTP Parameters.
 - 1) Select **Sever Address Type** and enter corresponding information.
 - 2) Enter **Port**.
 - 3) Enter **User Name**, **Password**, and confirm the password.
 - 4) Select **Protocol Type**.
 - 5) Select **Directory Structure**.



Note

You can customize the directory structure according to your needs.

5. Select **Path/Picture Name Encoding Mode**.

GB2312

Chinese characters encoding.

UTF-8

UNICODE encoding.

6. Optional: Enable upload functions.



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

Not Upload Plate Close-up

The close-up pictures of a license plate will not be uploaded.

Upload Additional Information to FTP

Add related information when uploading data to the FTP server.

7. Optional: Click **FTP Test** to check the FTP server.
8. Set naming rules and separators according to the actual needs.
9. Optional: Edit **OSD information** which can be uploaded to the FTP server with the pictures to make it convenient to view and distinguish the data.
10. Click **Save**.

6.2 Set SDK Listening

The SDK listening can be used to receive the uploaded information and pictures of the device arming alarm.

Before You Start

The listening service has been enabled for the SDK listening, and the network communication with the device is normal.

Steps


1. Go to **Configuration** → **Network** → **Data Connection** → **SDK Listening**.

SDK Listening

IP Address/Domain

Port

Enable Picture Uploading Listening ☐

Cloud Storage  Disabled



 Save

Figure 6-2 Set SDK Listening

2. Set **IP Address/Domain** and **Port** if you need to upload the alarm information and pictures.
3. Optional: Enable the picture uploading listening if you need to upload image information.
4. Optional: If you want to save the alarm information and pictures to the cloud storage, click  to set **Cloud Storage**. Refer to [Set Cloud Storage](#) for details.
5. Click **Save**.

6.3 Set Arm Host

The device can upload the captured pictures via the arm host.

Steps

Note

For level 1 arm, the pictures can be uploaded normally. If uploading failed, the device will upload again. For level 2 arm, the pictures will be uploaded once. No more upload if uploading failed. For level 3 arm, pictures will not be uploaded.


1. Go to **Configuration** → **Network** → **Data Connection** → **Arm Upload**.

Arm Upload

Cloud Storage  Disabled

 Save

Figure 6-3 Set Arm Host

2. Click  to set **Cloud Storage**. Refer to [Set Cloud Storage](#) for details.
3. Click **Save**.

6.4 Set ISAPI Listening

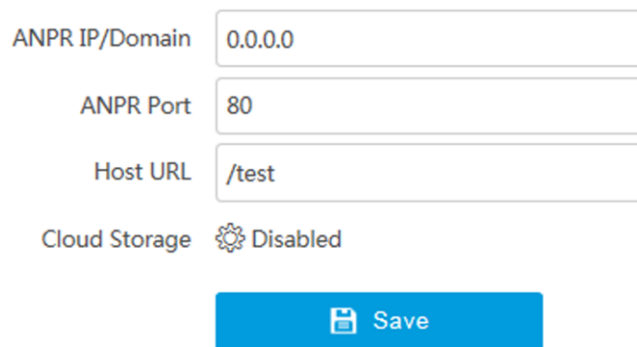
ISAPI listening and SDK listening are mutually exclusive protocols. If you enable the picture uploading listening, the device will transmit images via the SDK listening. If not, the device will upload images via ISAPI protocol after the ISAPI parameters are set.


Before You Start

The listening service has been enabled for the ISAPI host, and the network communication with the device is normal.

Steps


1. Go to **Configuration** → **Network** → **Data Connection** → **ISAPI Listening**.



ANPR IP/Domain	0.0.0.0
ANPR Port	80
Host URL	/test
Cloud Storage	 Disabled

Save

Figure 6-4 Set ISAPI Listening

2. Set **ANPR IP/Domain**, **ANPR Port**, and **Host URL**.
3. Optional: If you want to save the alarm information and pictures to the cloud storage, click  to set **Cloud Storage**. Refer to [Set Cloud Storage](#) for details.
4. Click **Save**.

6.5 Set Cloud Storage

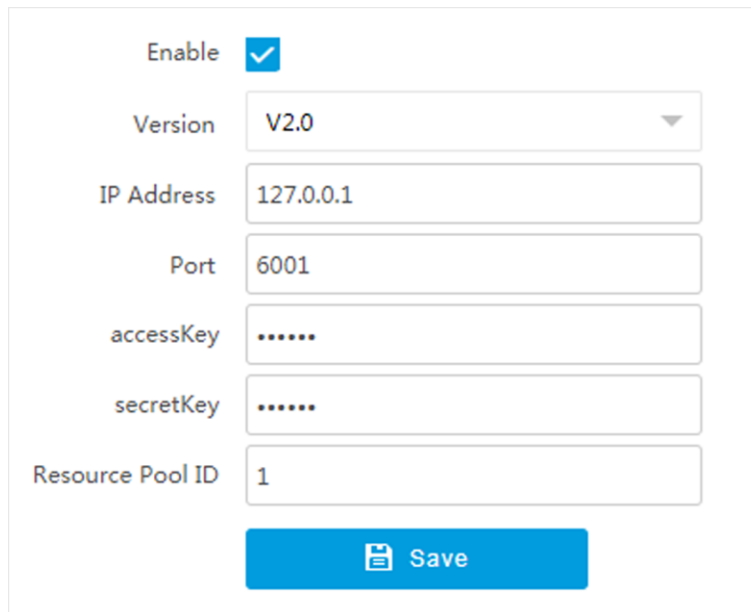
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

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

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **Cloud Storage**.



Enable ☒

Version

IP Address

Port

accessKey

secretKey

Resource Pool ID


 Save

Figure 6-5 Set Cloud Storage

2. Check **Enable**.
3. Select **Version**.

V1.0

1. Enter **IP Address** and **Port**
2. Enter **User Name** and **Password**.
3. Enter **Cloud Storage ID** and **Violation Cloud Storage ID** according to the server storage area No.

V2.0

1. Enter **IP Address** and **Port**
2. Enter **accessKey** and **secretKey**.
3. Enter **Resource Pool ID** according to the server storage area No. of uploading pictures.

4. Click **Save**.

Chapter 7 Encoding and Display

7.1 Set Video Encoding Parameters

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

- When the network signal is good and the speed is fast, you can set high resolution and bitrate to raise the image quality.
- When the network signal is bad and the speed is slow, you can set low resolution, bitrate, and frame rate to guarantee the image fluency.
- When the network signal is bad, but the resolution should be guaranteed, you can set low bitrate and frame rate to guarantee the image fluency.
- Main stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission. Sub-stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space. Third stream is offered for customized usage.

Steps



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

1. Go to **Configuration** → **Video** → **Video Encoding** → **Video Encoding**.
2. Set the parameters for different streams.

Stream Type

Select the stream type according to your needs.



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

Bitrate

Select relatively large bitrate if you need good image quality and effect, but more storage spaces will be consumed. Select relatively small bitrate if storage requirement is in priority.

Frame Rate

It is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Resolution

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

SVC

Scalable Video Coding (SVC) is an extension of the H.264/AVC and H.265 standard. Enable the function and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is variable, 6 levels of video quality are selectable. The higher the video quality is, the higher requirements of the network bandwidth.

Profile

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to device models.

I Frame Interval

It refers to the number of frames between two key frames. The larger the I frame interval is, the smaller the stream fluctuation is, but the image quality is not that good.

Video Encoding

The device supports multiple video encoding types, such as H.264, H.265, and MJPEG. Supported encoding types for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate, and image quality.

3. Click **Save**.

7.2 Set Image Parameters

You can adjust the image parameters to get clear image.

Steps



Note

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

1. Go to **Configuration** → **Video** → **Camera Parameter** → **Camera Parameter**.

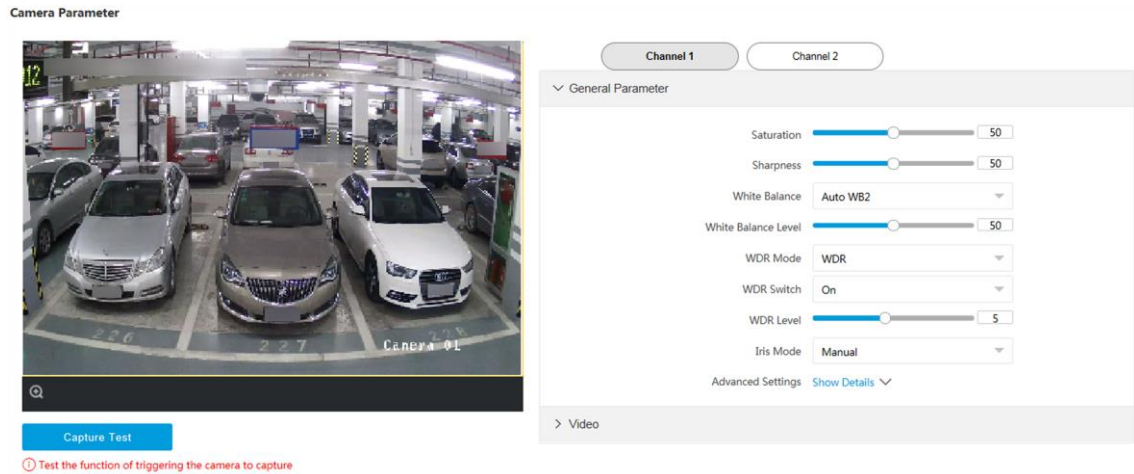


Figure 7-1 Set Image Parameters

- Optional: Select a channel.
- Adjust the parameters.

Saturation

It refers to the colorfulness of the image color.

Sharpness

It refers to the edge contrast of the image.

White Balance

It is the white rendition function of the device used to adjust the color temperature according to the environment.

WDR Mode

Wide Dynamic Range (WDR) can be used when there is a high contrast of the bright area and the dark area of the scene.

Select **WDR Switch** and set corresponding parameters according to your needs.

On

Set **WDR Level**. The higher the level is, the higher the WDR strength is.

Time

Enable WDR according to the time.

Brightness

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

Iris Mode

Select the iris mode as manual or auto.

Brightness Enhancement at Night

The scene brightness will be enhanced at night automatically.

Enable Defog

Enable defog to get a clear image in foggy days.

Light Compensation on License Plate

Check it. The light compensation on license plates can be realized, and various light supplement conditions can be adapted via setting license plate expectant brightness and supplement light correction coefficient. The higher the sensitivity is, the easier this function can be enabled.

Enable Gamma Correction

The higher the gamma correction value is, the stronger the correction strength is.

Brightness

It refers to the max. brightness of the image.

Contrast

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

Shutter

If the shutter speed is quick, the details of the moving objects can be displayed better. If the shutter speed is slow, the outline of the moving objects will be fuzzy and trailing will appear.

Gain

It refers to the upper limit value of limiting image signal amplification. It is recommended to set a high gain if the illumination is not enough, and set a low gain if the illumination is enough.

3D DNR

Digital Noise Reduction (DNR) reduces the noise in the video stream.

In **Normal Mode**, the higher the **3D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

In **Expert Mode**, set **Spatial Intensity** and **Time Intensity**. If the special intensity is too high, the outline of the image may become fuzzy and the details may lose. If the time intensity is too high, trailing may appear.

2D DNR

The higher the **2D DNR Level** is, the stronger the noise will be reduced. But if it is too high, the image may become fuzzy.

Video Standard

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

7.3 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resources to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video encoding type. ROI is supported when the video encoding type is H.264 or H.265.

Steps

1. Go to **Configuration** → **Video** → **Video Encoding** → **ROI**.

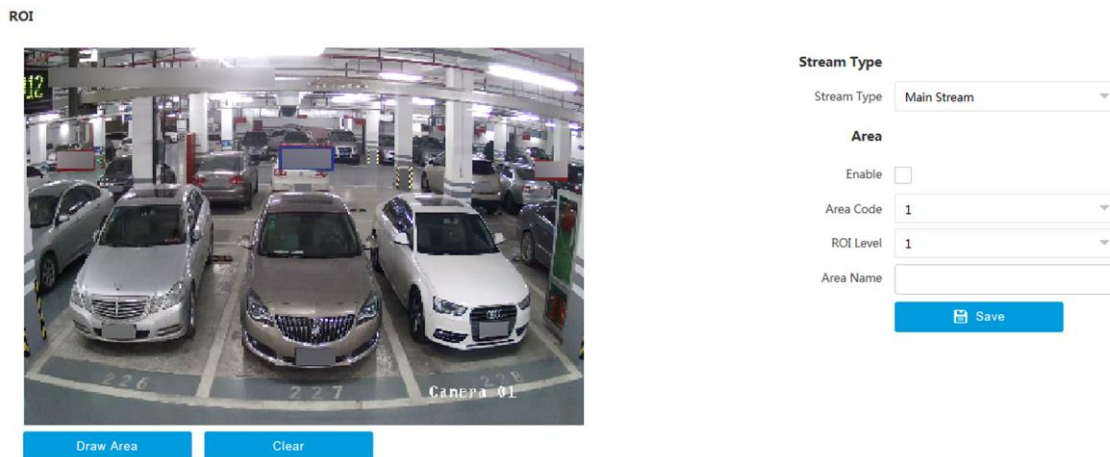


Figure 7-2 Set ROI

2. Select **Stream Type**.
3. Set ROI region.
 - 1) Check **Enable**.
 - 2) Select **Area Code**.
 - 3) Click **Draw Area**.
 - 4) Drag the mouse on the live view image to draw a fixed area.
 - 5) Select the fixed area that needs to be adjusted and drag the mouse to adjust its position.
4. Select **ROI Level** and enter **Area Name**.

Note

The higher the ROI level is, the clearer the image of the detected area is.

5. Click **Save**.
6. Optional: Select other area codes and repeat the steps above if you need to draw multiple fixed areas.

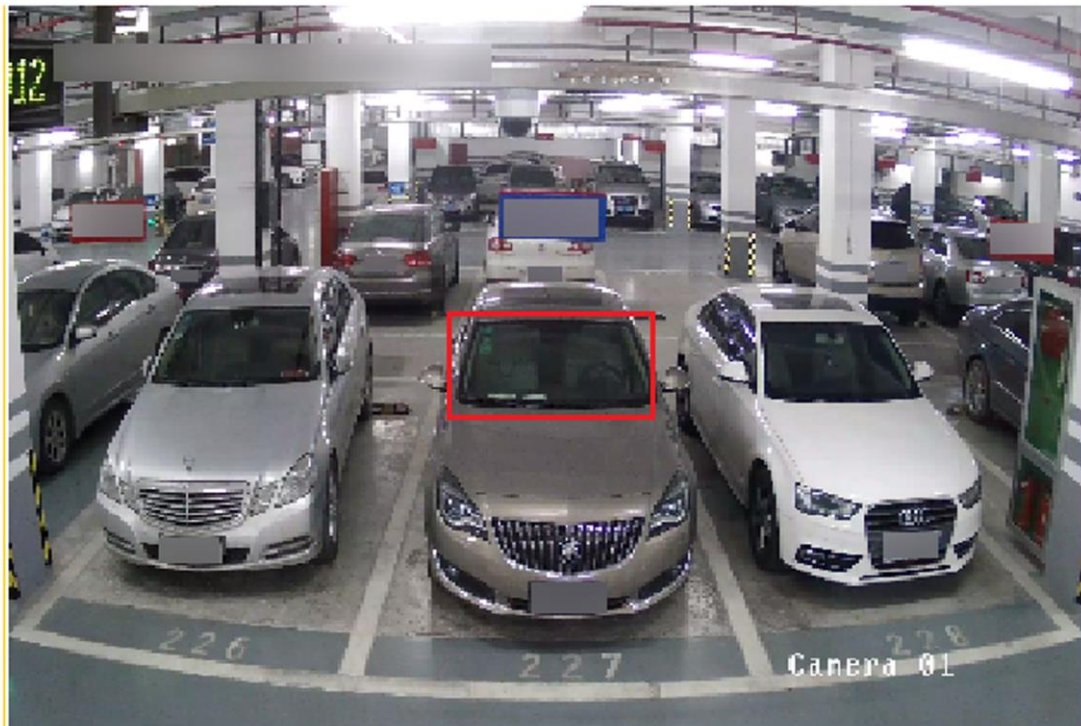
7.4 Enable Regional Exposure

Enable regional exposure to expose partial area of the live view image.

Steps

1. Go to **Configuration** → **Video** → **Video Encoding** → **Regional Exposure**.
2. Check **Enable**.
3. Drag the cursor to draw an area.
The drawn area will be exposed.

Regional Exposure



Enable ☒

 Save

Figure 7-3 Enable Regional Exposure

4. Click **Save**.

7.5 Set OSD

You can customize OSD information on the live view.

Steps

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

Note

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

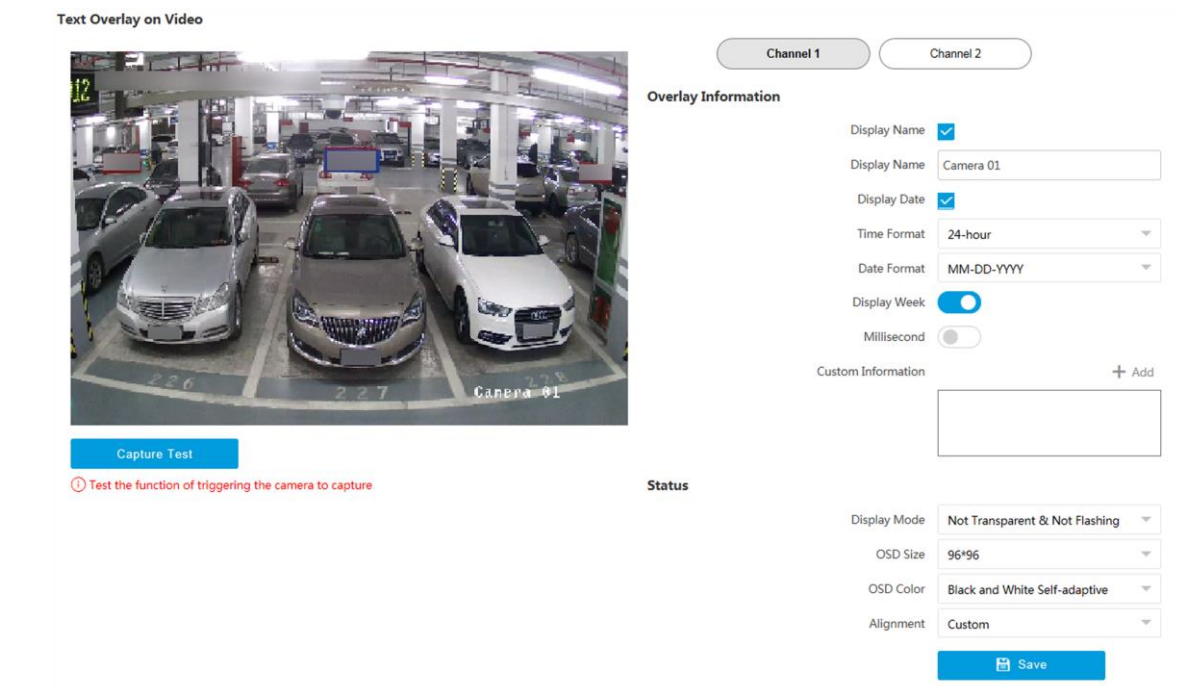


Figure 7-4 Set OSD

2. Optional: Select a channel.
3. Set display contents.
 - 1) Check **Display Name**.
 - 2) Enter **Display Name**.
 - 3) Check **Display Date**, and set the time and date format.
 - 4) Enable **Display Week** or **Millisecond** according to your needs.
4. Optional: Click **Add** and enter information if you want to add custom information.

Note

Up to 6 items of custom information can be added.

5. Set display properties (font, color, etc.).
6. Select **Alignment**.

Note

If you select **Align Left** or **Align Right**, set **Min. Horizontal Margin** and **Min. Vertical Margin**.

7. Drag the red frames on the live view image to adjust their positions.

8. Click **Save**.

Result

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

Chapter 8 Network Configuration

8.1 Set IP Address

IP address must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Steps



Note

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

1. Go to **Configuration** → **Network** → **Network Parameters** → **Network Interface**.

NIC Settings

NIC Type	Auto
DHCP	<input type="checkbox"/>
IPv4 Address	10.99.3.84
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.99.3.254
IPv6 Mode	DHCP
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	24:0f:9b:76:2b:53
MTU	1500
Multicast Address	0.0.0.0

DNS Server

Preferred DNS Server	10.1.7.77
----------------------	-----------

Save

Figure 8-1 Set IP Address

2. Set network parameters.

NIC Type

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

IPv4

Two modes are available.

DHCP

The device automatically gets the IP parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IP parameters manually. Enter **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**.

IPv6

Three IPv6 modes are available.

Route Advertisement

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



Note

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

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast Address

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting the IP address of the multicast host, you can send the source data efficiently to multiple receivers.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** properly if needed.

3. Click **Save**.

8.2 Connect to ISUP Platform

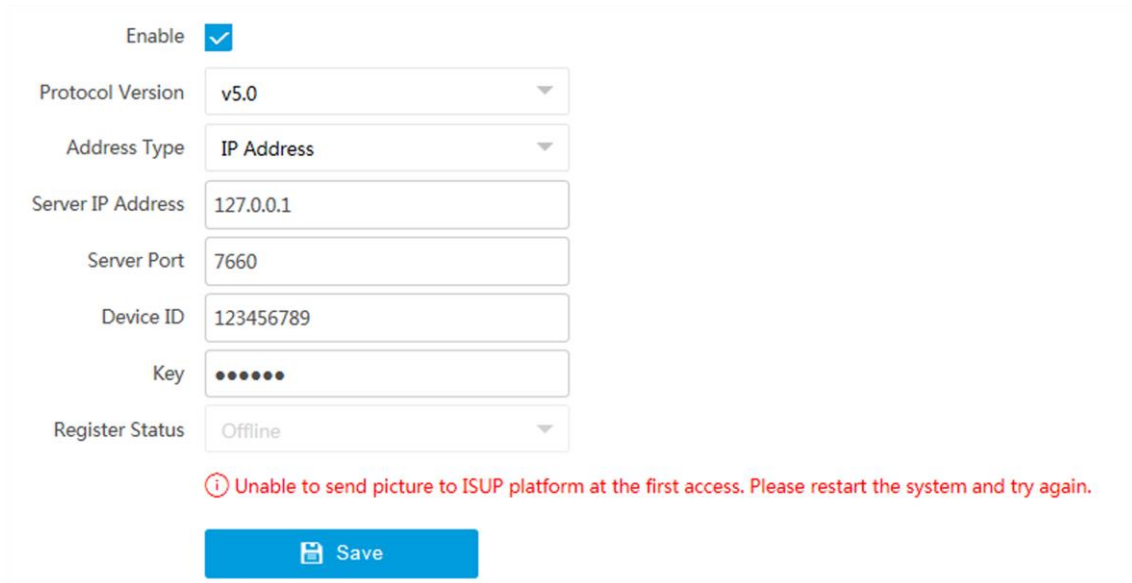
ISUP (EHome) is a platform access protocol. The device can be remotely accessed via this platform.

Before You Start

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

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **ISUP**.



Enable ☒

Protocol Version v5.0

Address Type IP Address

Server IP Address 127.0.0.1

Server Port 7660

Device ID 123456789

Key •••••

Register Status Offline

Unable to send picture to ISUP platform at the first access. Please restart the system and try again.

Save

Figure 8-2 Connect to ISUP Platform

2. Check **Enable**.
3. Select **Protocol Version**.
4. Select **Address Type**.
5. Enter **Sever IP Address**, **Server Port**, and **Device ID**.

Note

You need to enter **Key** if you select **Protocol Version** as **v5.0**.

6. Click **Save**.
7. Optional: View **Register Status**.

What to do next

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

8.3 Set DDNS

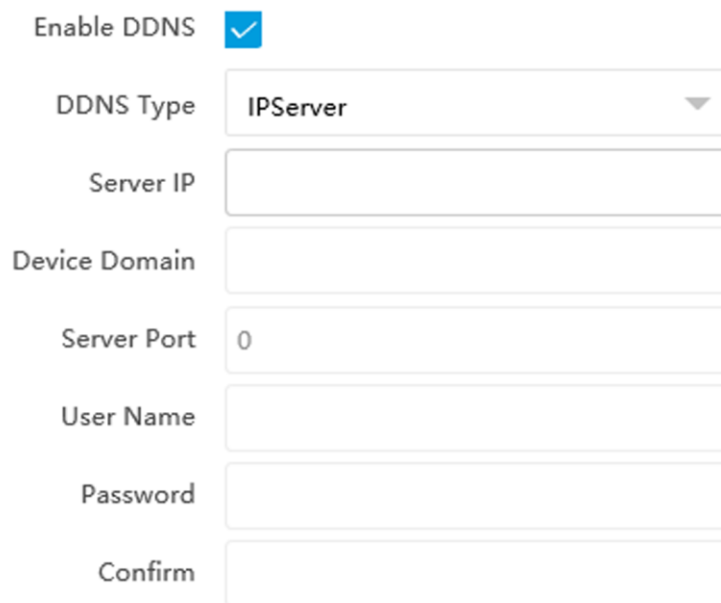
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to for details.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **DDNS**.



Enable DDNS ☒

DDNS Type IPServer ▼

Server IP

Device Domain

Server Port

User Name

Password

Confirm

Figure 8-3 Set DDNS

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

By Browsers

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

By Client Software

Add domain name to the client software. Refer to the client software manual for specific adding methods.

8.4 Set Port

The device port can be modified when the device cannot access the network due to port conflicts. Go to **Configuration** → **Network** → **Network Parameters** → **Port** for port settings.

The screenshot shows a web interface for configuring network ports. It is divided into five sections: HTTP Port, HTTPS Port, RTSP Port, Server Port, and SADP Port. Each section has an 'Enable' checkbox and a text input field for the port number. A blue 'Save' button is at the bottom right.

Port Type	Enable	Port Number
HTTP Port	<input checked="" type="checkbox"/>	80
HTTPS Port	<input type="checkbox"/>	443
RTSP Port	<input checked="" type="checkbox"/>	554
Server Port		8000
SADP Port	<input checked="" type="checkbox"/>	

Figure 8-4 Set Port

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

Set the HTTPS for accessing the browser. Certificate is required when accessing.

RTSP Port

It refers to the port of real-time streaming protocol.

Server Port

It refers to the port through which the client adds the device.

SADP Port

It refers to the port through which the SADP software searches the device.

Note

- After editing the port, access to the device via new port.
- Reboot the device to take the new settings into effect.

You can enable Bluetooth to upload the parking space information to the platform.

 Note

Some models do not support Bluetooth. The actual device prevails.

- [illegible]

Figure 8-5 Set Bluetooth

- ### Broadcast Time Interval

Rated Power

Transmitted Power

4. Set **Parking Lot ID**, **Parking Lot Floor Amount**, etc. according to the actual parking lot environment.

 Note

Enter the hex characters (0 to F) according to the corresponding standard of Bluetooth for the parking lot ID.

5. Click **Save**.

Chapter 9 Alarm Configuration

This section explains how to set the device to respond to alarm events, including motion detection and exceptions. These events can trigger the linkage methods, such as notifying the surveillance center.

9.1 Set Motion Detection

Motion detection detects the moving objects in the set surveillance area, and a series of actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Motion Detection**.
2. Optional: Select a channel.
3. Check **Enable Motion Detection** and **Enable Dynamic Analysis**.
4. Set the motion detection area.
 - 1) Click **Draw Area**.
 - 2) Drag the mouse on the live view to draw a motion detection area.
 - 3) Optional: Repeat the steps to draw more areas.
 - 4) Optional: Click **Clear All** to clear all the areas.
 - 5) Adjust **Sensitivity** of the motion detection.

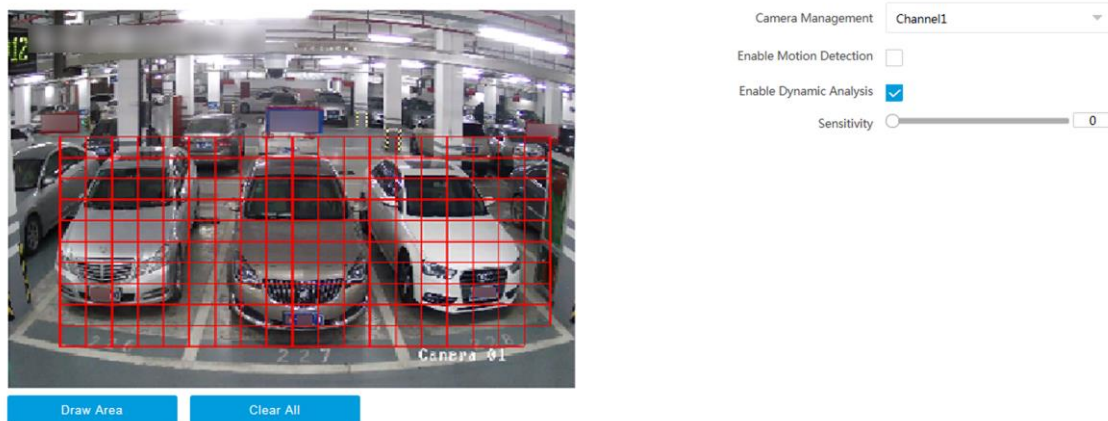



Figure 9-1 Set Motion Detection

5. Set the arming schedule for the motion detection.
 - 1) Drag the cursor on the time bar to set an arming time.

Note

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

- 2) Adjust the arming time.

- Click a set recording period and enter the start time and end time in the pop-up window.
 - Drag two ends of the set recording period bar to adjust the length.
 - Drag the whole set recording period bar and relocate it.
- 3) Optional: Delete arming periods.
- Click a set arming period and click **Delete** in the pop-up window.
 - Click a set arming period and click **Delete** on the arming schedule configuration interface.
- 4) Optional: Click  to copy the set arming schedule to other days.



The image shows the 'Arming Schedule' configuration interface. At the top, there is a dropdown menu set to 'Continuous' and a 'Delete' button. Below this is a grid showing the arming schedule for each day of the week (Mon through Sun). Each day has a horizontal bar representing the 24-hour period, with a legend indicating that the blue bar represents 'Continuous' arming. Each bar has a green copy icon at its end. At the bottom, there is a 'Linkage Method' section with a checkbox for 'Notify Surveillance Center' which is checked, and a 'Save' button.

Figure 9-2 Set Arming Schedule

6. Optional: Check **Notify Surveillance Center** to send an exception or alarm signal to the surveillance center when the motion detection occurs.
7. Click **Save**.

9.2 Exception Alarm

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

Steps

Note

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

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Exception**.
2. Select the exception type(s) and the linkage method.

3. Click **Save**.

Chapter 10 Safety Management

10.1 Manage User

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

Steps

1. Go to **Configuration** → **System** → **User Management** → **User List**.
2. Select **Password Level**.
The password level of the added user should conform to the selected level.
3. Add a user.
 - 1) Click **Add**.
 - 2) Enter **User Name** and select **Type**.
 - 3) Enter **Admin Password**, **New Password**, and confirm the password.



Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

- 4) Assign remote permission to users based on needs.

User


Users can be assigned permission of viewing live video and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

- 5) Click **OK**.
4. Optional: You can do the following operations.

Change the password and permission

Click  to change the password and permission.

Delete the user

Click  to delete the user.

10.2 Enable User Lock

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

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Enable the user lock function.
3. Click **Save**.

Result

When the times you entered incorrect passwords have reached the limit, the current IP address will be locked automatically.

10.3 Set HTTPS

10.3.1 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **OK**.

Result

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

10.3.2 Install Authorized Certificate

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

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create certificate request first and continue the installation**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Import certificate to the device.

- Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
- Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.

7. Click **Save**.

10.4 Set SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Disable **SSH Service**.
3. Click **Save**.

10.5 Set RTSP Authentication

You can improve network access security by setting RTSP authentication.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Settings**.
2. Select **RTSP Authentication**.

digest

The device only supports digest authentication.

digest/basic

The device supports digest or basic authentication.

3. Click **Save**.

10.6 Set IP Address Filtering

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

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Settings**.
2. Check **Enable IP Address Filtering**.
3. Set **Filtering Mode**.

Blocklist Mode

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

Allowlist Mode

The added IP addresses are allowed to access the device.

4. Click **Add**, enter the IP address, and click **OK**.



The IP address only refers to the IPv4 address.

5. Optional: Edit, delete, or clear the added IP addresses.
6. Click **Save**.

10.7 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Timeout Logout**.
2. Enable timeout logout for static page.
3. Set **Max. Timeout**.
4. Click **Save**.

Result

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

10.8 Set Password Validity Period

You can improve network access security by setting password validity period.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Password Validity Period**.
2. Select **Validity Type**.
 - Select **Permanent**. The password will be permanently valid.
 - Select **Daily** and set **Password Expiry Time**. It will prompt you that the password is expired according to the set password expiry time, and you need to set the new password.
3. Click **Save**.

Chapter 11 Maintenance

11.1 View Device Information

Basic Information and Algorithms Library Version

Go to **Configuration** → **System** → **System Settings** → **Basic Information** to view the basic information and algorithms library version of the device.

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

Device Status

Go to **Configuration** → **System** → **System Settings** → **Device Status** to view the device status and live view and arming status.

11.2 Log

11.2.1 Enable System Log Service

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events. Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you are recommended to save the logs on a log server.

Steps

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

11.2.2 Search Log

Log helps to locate and troubleshoot problems.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Log Search**.

2. Set search conditions.
3. Click **Search**.
The matched log files will be displayed on the log list.
4. Optional: Click **Export** to save the log files to your computer.

11.2.3 Search Security Audit Log

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.

Before You Start

Go to **Configuration** → **System** → **Security** → **Security Service** → **Log Audit Service** and enable system log service.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Security Audit Log**.
2. Set search conditions.
3. Click **Search**.
The matched log files will be displayed on the log list.
4. Optional: Click **Export** to save the log files to your computer.

11.3 Upgrade

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

Before You Start

Prepare the upgrade file. If the upgrade file is a compressed package, it needs to be decompressed into the .dav format.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Upgrade**.
2. Click **Browse** to 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.

11.4 Reboot

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

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Device Maintenance**.
2. Click **Reboot**.
3. Click **OK** to reboot the device.



Note

You can also click **Reboot** on the upper right corner of the page to reboot the device.

11.5 Restore Parameters

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

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Device Maintenance**.
2. Select the restoration mode.
 - Click **Restore**, and click **OK**. Then the parameters except the IP parameters and user parameters will be restored to the default settings.
 - Click **Restore Factory Settings** and click **OK** to restore all the parameters to the factory settings.

11.6 Synchronize Time

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

Steps

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

NTP Synchronization

Select it to synchronize the device time with that of the NTP server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

Manual Synchronization

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

SDK

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

ONVIF

Select it to synchronize time via the third-party device.

No

Select it to disable time synchronization.

All

Select it, and you can select any mode above.



Note

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

4. Click **Save**.

11.7 Debug Device

You can enable the function to debug the device.

Steps

1. Go to **Configuration** → **Capture** → **Advanced** → **System Service**.
2. Check the debug information according to your needs.

Enable Algorithm POS Information Debug

The algorithm POS information will be overlaid on the image.

3. Click **Save**.

11.8 Set DST

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

Steps

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

11.9 Export Parameters

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

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Data Export**.
2. Click **Export** after **Configuring Parameters**.
3. Set an encryption password, confirm the password, and click **OK**.



The password is used for importing the configuration file of the current device to other devices.

4. Select the saving path, and enter the file name.
5. Click **Save**.

11.10 Import Configuration File

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

Before You Start

Save the configuration file to the computer.

Steps



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

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Advanced Settings** → **Data Import**.
2. Select **Importing Method**.



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

3. Click **Browse** to select the configuration file.
4. Click **Import**.
5. Enter the password which is set when the configuration file is exported, and click **OK**.
6. Click **OK** on the popup window.

Result

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

11.11 Export Debug File

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

Steps

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

11.12 Export Diagnosis Information

The technicians can export the diagnosis information to troubleshoot and maintain the device.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Data Export**.
2. Click **Export** after **Diagnosis Information**.
3. Select the saving path, and enter the file name.
4. Click **Save**.

A. Communication Matrix and Device Command

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



Figure A-1 Communication Matrix

Scan the QR code below to get the device command.



Figure A-2 Device Command



See Far, Go Further