



Outdoor Parking Camera

User Manual

Initiatives on the Use of Video Products

Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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 Capture Configuration	5
3.1 Set Trigger Mode	5
3.1.1 Set Parking Space Mode	5
3.1.2 Set Area Mode	7
3.2 Set Capture Parameters	8
3.2.1 Set License Plate Recognition Parameters	8
3.2.2 Set Supplement Light Parameters	8
3.2.3 Set Capture Overlay	9
3.2.4 Set Image Encoding Parameters	10
3.3 View Real-Time Picture	10
Chapter 4 Live View and Local Configuration	12
4.1 Live View	12
4.1.1 Start/Stop Live View	12
4.1.2 Select Image Display Mode	12
4.1.3 Select Window Division Mode	12
4.1.4 Select Stream Type	12
4.1.5 Capture Picture Manually	12

4.1.6 Record Manually	13
4.1.7 Enable Digital Zoom	13
4.1.8 Select Video Mode	13
4.2 PTZ Operation	13
4.3 Local Configuration	15
Chapter 5 Storage	18
5.1 Set FTP	18
5.2 Set Listening Host	19
5.3 Set Arm Host	20
5.4 Set ISAPI Listening	20
5.5 Set Cloud Storage	21
Chapter 6 Encoding and Display	23
6.1 Set Video Encoding Parameters	23
6.2 Set Image Parameters	24
6.3 Set ROI	27
6.4 Enable Regional Exposure	28
6.5 Set OSD	28
Chapter 7 Network Configuration	30
7.1 Set IP Address	30
7.2 Connect to ISUP Platform	32
7.3 Set DDNS	33
7.4 Set Port	34
Chapter 8 Serial Port Configuration	36
8.1 Set RS-485	36
8.2 Set RS-232	36
Chapter 9 Safety Management	38
9.1 Manage User	38
9.2 Enable User Lock	38

9.3 Set HTTPS	39
9.3.1 Create and Install Self-signed Certificate	39
9.3.2 Install Authorized Certificate	39
9.4 Exception Alarm	40
9.5 Set SSH	40
9.6 Set RTSP Authentication	40
9.7 Set IP Address Filtering	40
9.8 Set Timeout Logout	41
9.9 Set Password Validity Period	41
Chapter 10 Maintenance	42
10.1 View Device Information	42
10.2 Enable System Log Service	42
10.3 Search Log	42
10.4 Upgrade	43
10.5 Reboot	43
10.6 Restore Parameters	43
10.7 Synchronize Time	44
10.8 Debug Device	45
10.9 Set DST	45
10.10 Export Parameters	45
10.11 Import Configuration File	45
10.12 Export Diagnosis Information	46
10.13 Export Debug File	46

Chapter 1 Introduction

1.1 Introduction

The outdoor parking camera (hereinafter referred to as "device") is applied in the parking guidance system to detect the parking status and parking space status. Integrated with the camera and the supplement light, the device can be widely applied in the outdoor parking lot, community dedicated lane, 4S automotive dealership, outdoor dedicated parking spaces, etc.

1.2 Key Feature

- Supports parking space status detection, parking space occupation detection, and parking over line detection.
- Built-in HD camera provides high quality imaging.
- Low illumination enables clear imaging at night.
- Built-in supplement light reduces construction and wiring costs.
- Supports to connect peripheral alarm devices.

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: 192.168.1.64
- 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.

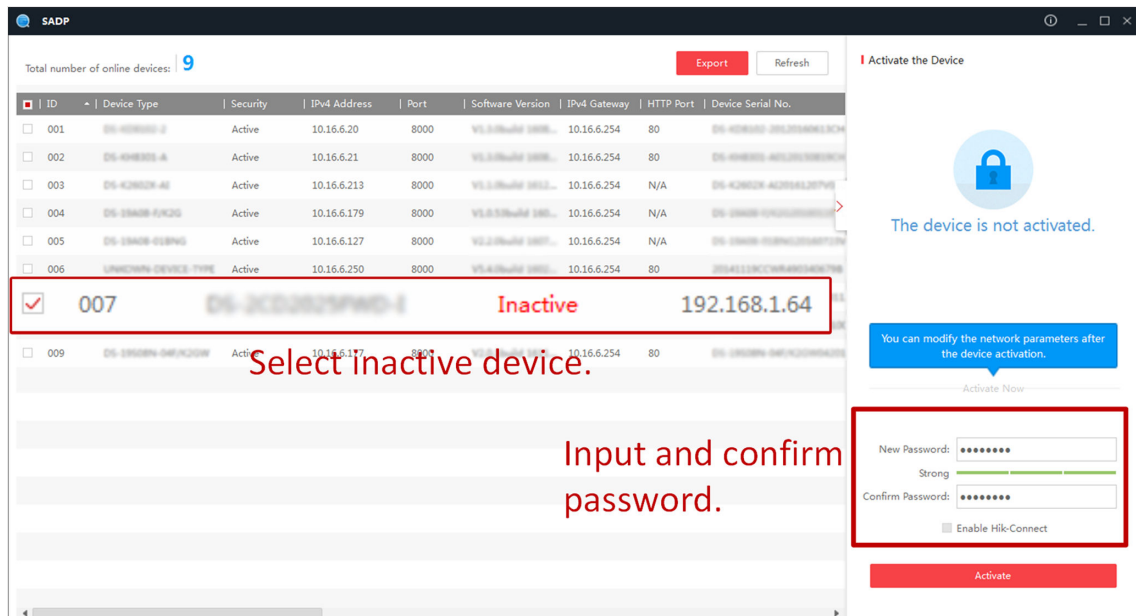


Figure 2-1 Activate via SADP

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.



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 Capture Configuration

3.1 Set Trigger Mode

After setting trigger mode, the device will capture pictures if the parking space status changes (a vehicle enters or exits), and the information will be uploaded with the captured pictures as well.

3.1.1 Set Parking Space Mode

Set parking space mode to detect the parking space occupation status.

Steps

1. Go to **Configuration → Capture → Application Mode → Trigger Mode**.

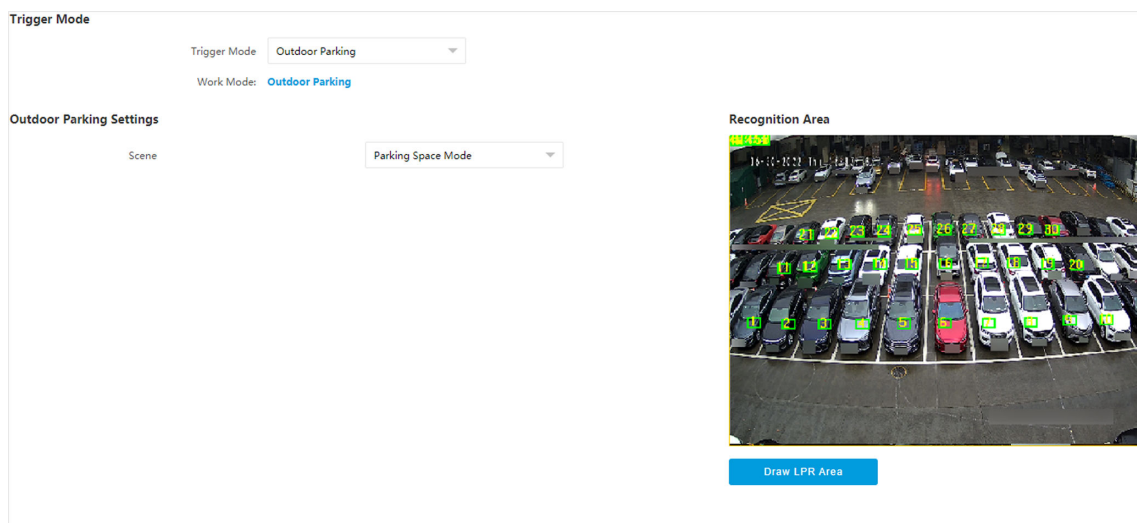


Figure 3-1 Set Parking Space Mode

2. Select **Scene** as **Parking Space Mode**.
3. Draw parking spaces.
 - 1) Click **Draw LPR Area**.
 - 2) Click **Mark Parking Space** and drag the parking space frame to the middle of the parking space.

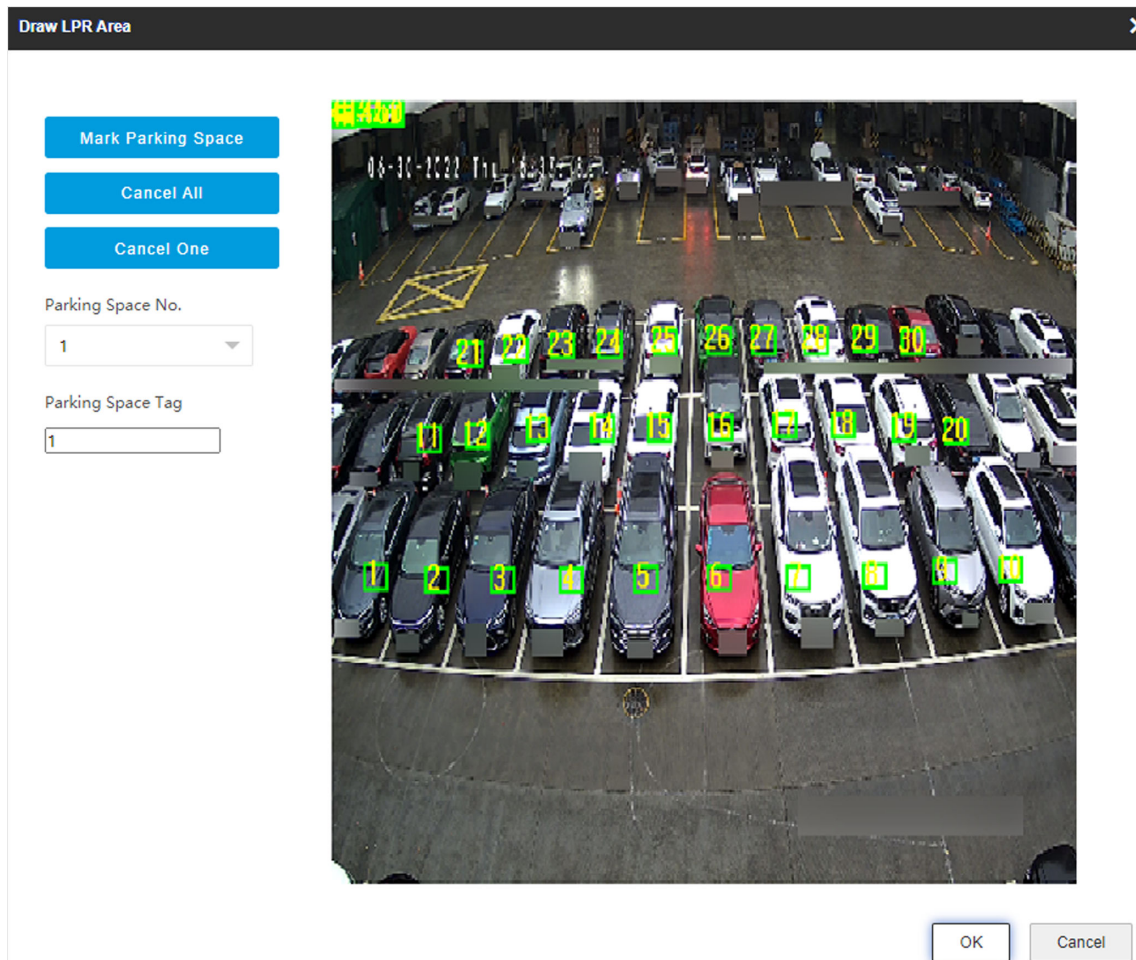


Figure 3-2 Mark Parking Spaces

3) Click **OK**.

4) **Optional**: Repeat the above steps to mark parking spaces that you want to detect.

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

Set Parking Space No. Select **Parking Space No.** and enter the parking space tag.

Cancel All Delete all the set parking space frames.

Cancel One Delete the latest set parking space frame.

5. Click **Save**.

Result

On the live view page, you can view the parking space status. If the parking space is available, the parking space frame will be green. If the parking space is occupied, the parking space frame will be red.

3.1.2 Set Area Mode

You can set detection area in the outdoor parking lot, community dedicated lane, outdoor dedicated parking spaces, and other scenes to detect the number of parked vehicles and parking space status.

Steps

1. Go to **Configuration → Capture → Application Mode → Trigger Mode**.

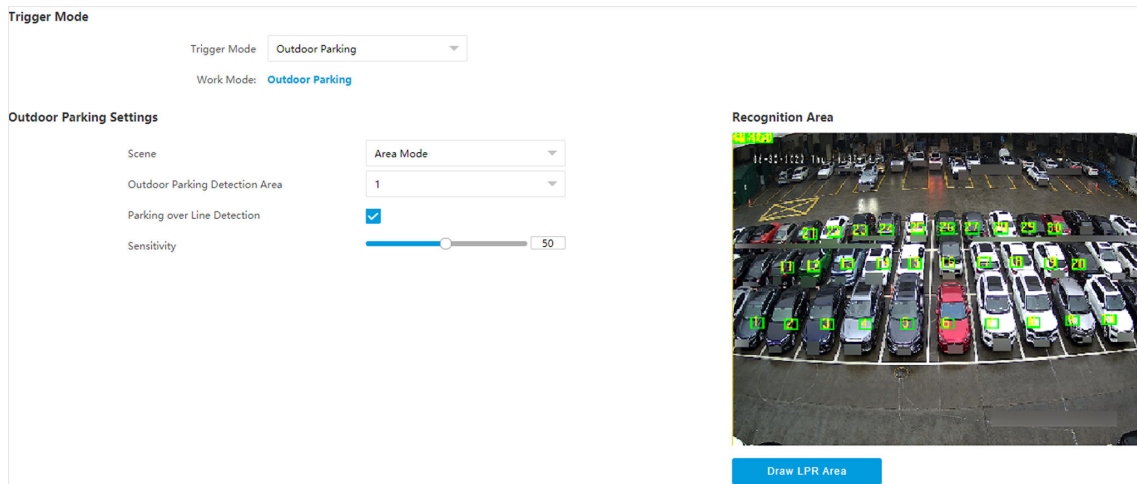


Figure 3-3 Set Area Mode

2. Select **Scene** as **Area Mode**.
3. Select **Outdoor Parking Detection Area**.
4. **Optional:** Check **Parking over Line Detection** and set **Sensitivity**.

Note

The higher the sensitivity is, the more easily the parking over line will be detected. But if it is too high, false detection would occur. Please set the sensitivity according to the actual needs.

If the vehicle is parked over line, the device will capture pictures, and the information of parking over line will be uploaded with the captured pictures as well.

5. Draw the detection area.
 - 1) Click **Draw LPR Area**.
 - 2) Select **Area Type** and adjust the detection area frame to match the actual detection area.
 - 3) Select **Parking Space Type** according to the actual scene.

Note

Click **Redraw Area** to delete the existing area.

- 4) Click **OK**.
6. Click **Save**.

3.2 Set Capture Parameters

3.2.1 Set License Plate Recognition Parameters

Select the belonged country/region of the license plates.

Steps

1. Go to **Configuration → Device Configuration → Capture Parameters → License Parameters** .



Figure 3-4 Set License Plate Recognition Parameters

2. Select **Country/Region**.
3. Click **Save**.

3.2.2 Set Supplement Light Parameters

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

Steps



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

1. Go to **Configuration → Capture → Capture Parameters → Supplement Light Parameters** .

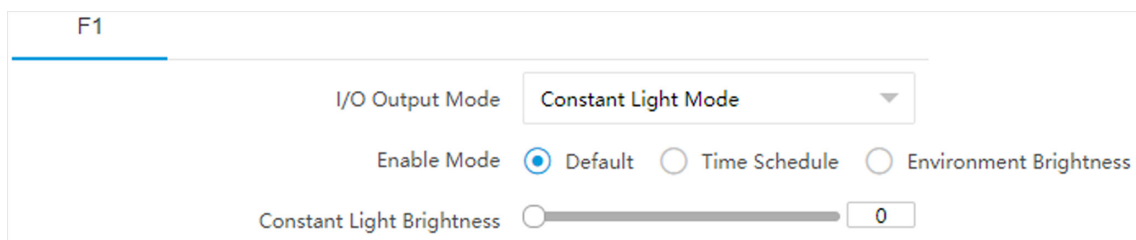


Figure 3-5 Set Supplement Light Parameters

2. Select the I/O output mode as **Constant Light Mode**.
3. Set the supplement light parameters according to actual conditions.

Enable Mode

Default

The usage of the supplement light is determined based on the license plate brightness in the scene.

Time Schedule

In this mode, **Begin Time** and **End Time** need to be set. The device enables the supplement light only during the set time range.

Environment Brightness

In this mode, **Threshold** needs to be set. When the brightness of the image reaches the set threshold, the supplement light is enabled automatically.

Constant Light Brightness

Set the brightness value according to actual needs.

4. Click **Save**.

3.2.3 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. Check **Capture Picture Overlay**.

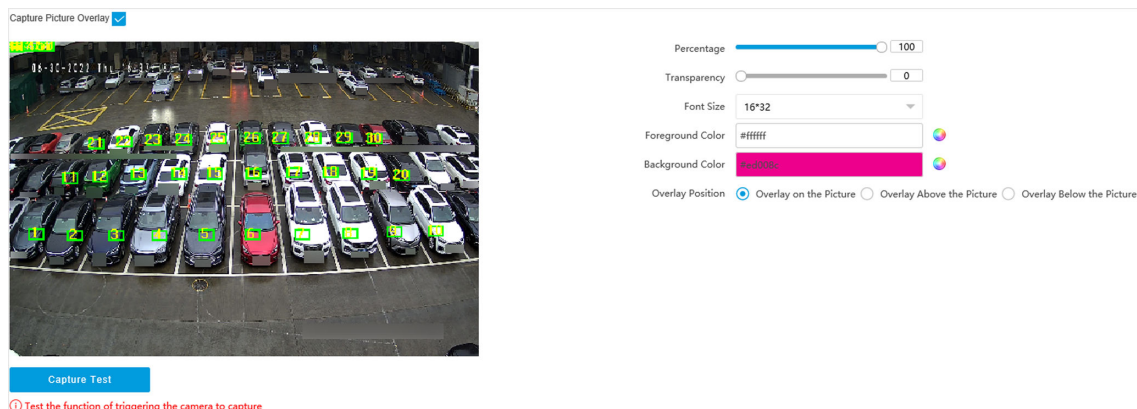


Figure 3-6 Set Capture Overlay

3. Set the capture overlay parameters.

Percentage

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

4. Select the overlay information from the list.



Note

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

5. Set the overlay information.

Type

You can edit the type.

Overlay Information	For some information types, you can edit the detailed information.
Overlay Position	Check it, and the current information will be displayed on a new line.
Space	Edit the number of spaces between the current information and the next one from 0 to 255. 0 means there is no space.
Line Break Characters	Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
	Adjust the display sequence of the overlay information.

6. Click **Save**.

3.2.4 Set Image Encoding Parameters

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

Steps

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

Image Encoding

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

Figure 3-7 Set Image Encoding Parameters

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

3.3 View Real-Time Picture

You can view the real-time captured pictures and license plate information.

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.

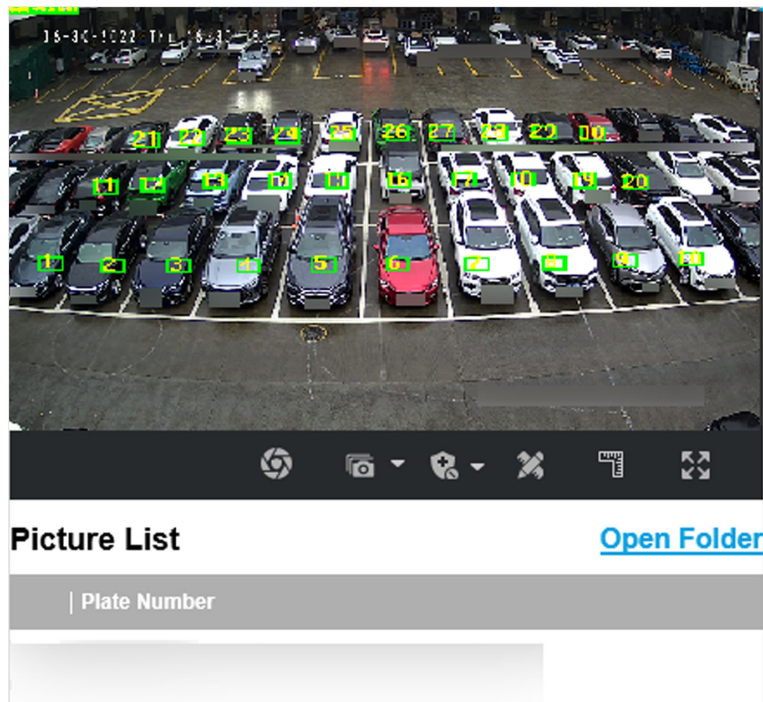


Figure 3-8 Real-Time Picture

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 4 Live View and Local Configuration

4.1 Live View

4.1.1 Start/Stop Live View

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

4.1.2 Select Image Display Mode

Click  to select an image display mode.

4.1.3 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.

4.1.4 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.

4.1.5 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.

4.1.6 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.

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 Select Video Mode

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

Click  and select  when the device is running normally.

4.2 PTZ Operation

Click **Live View**. Click  and click  to show the PTZ control panel.



Note

- The PTZ supports power-off memory. When the device is suddenly cut off power or restarted normally, it can automatically return to the position before the power cut or reboot.
 - The PTZ function varies with different models. The actual device prevails.
 - Other unmentioned buttons are reserved buttons.
-

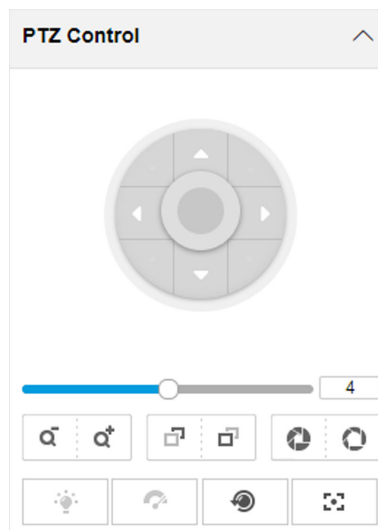


Figure 4-1 Control Panel

Table 4-1 Button Description

Button	Description
	Adjust the PTZ speed.
	Zoom + and Zoom - - Hold to zoom in the scene. - Hold to zoom out the scene.
	Focus + and Focus - - Hold under the manual focus mode to make near objects become clear and distant objects become vague. - Hold to make distant objects become clear and near objects become vague.
	Iris + and Iris - - Hold to increase the iris diameter when in a dark environment. - Hold to decrease the iris diameter when in a bright environment.
	Lens Initialization It is applicable to devices with motorized lenses. You can use this function when overcoming image blurs caused by overtime zooming or focusing.
	Auxiliary Focus

Button	Description
	It is applicable to devices with motorized lenses. Use this function to focus the lens automatically and make images become clear.

4.3 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 4-2 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 5 Storage

5.1 Set FTP

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

Before You Start

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

Steps

Note

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

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

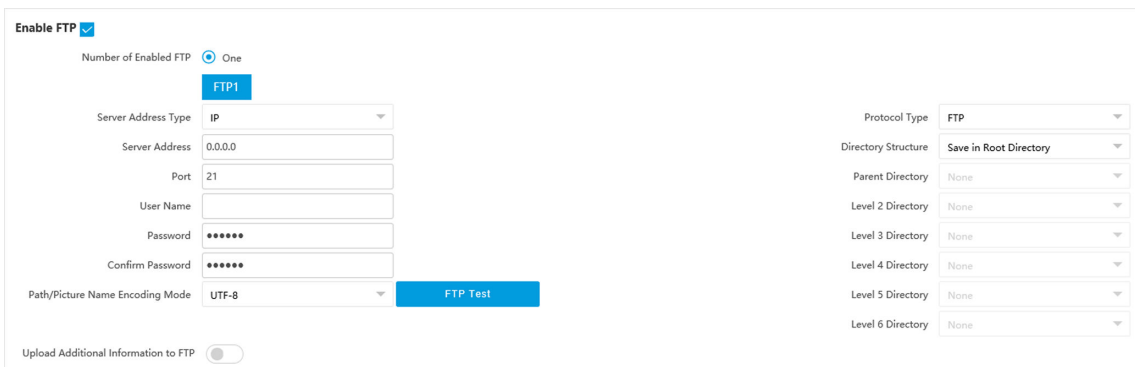


Figure 5-1 Set FTP

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.

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**.

5.2 Set Listening Host

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 5-2 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**.

5.3 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 5-3 Set Arm Host

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

5.4 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 5-4 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**.

5.5 Set Cloud Storage

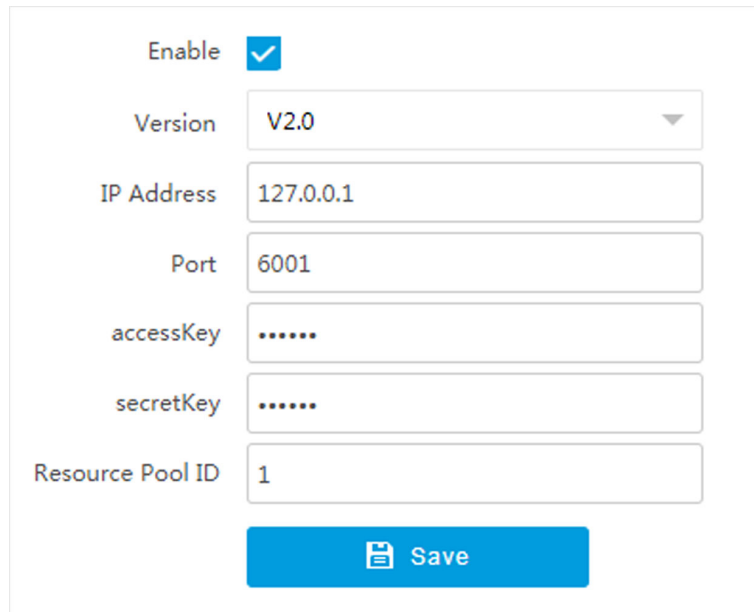
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

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 5-5 Set Cloud Storage

2. Check **Enable**.

3. Select **Version**.

V1.0 a. Enter **IP Address** and **Port**

b. Enter **User Name** and **Password**.

c. Enter **Cloud Storage ID** and **Violation Cloud Storage ID** according to the server storage area No.

V2.0 a. Enter **IP Address** and **Port**

b. Enter **accessKey** and **secretKey**.

c. Enter **Resource Pool ID** according to the server storage area No. of uploading pictures.

4. Click **Save**.

Chapter 6 Encoding and Display

6.1 Set Video Encoding Parameters

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

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

Steps



Note

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.



Note

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**.

6.2 Set Image Parameters

You can adjust the image parameters to get clearer images.

Steps



Note

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

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

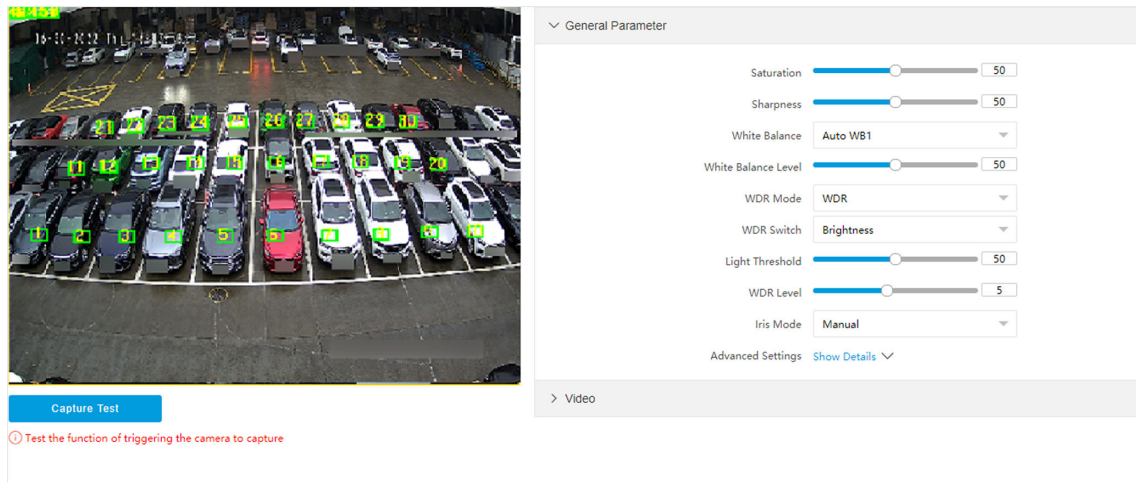


Figure 6-1 Set General Parameter

2. Set the parameters.

General Parameter

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.

In this mode, 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

Only manual iris mode is supported.

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.

Enable Gamma Correction

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

Video

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.

Hue Range

Select the range to adapt to the display.

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.

6.3 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**.

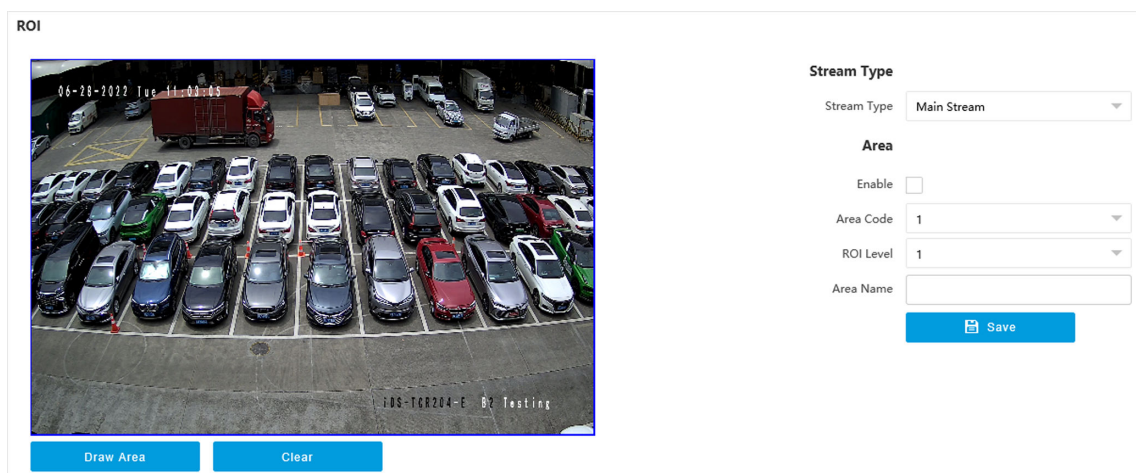


Figure 6-2 Set ROI

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.

6.4 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.



Figure 6-3 Enable Regional Exposure

4. Click **Save**.

6.5 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.

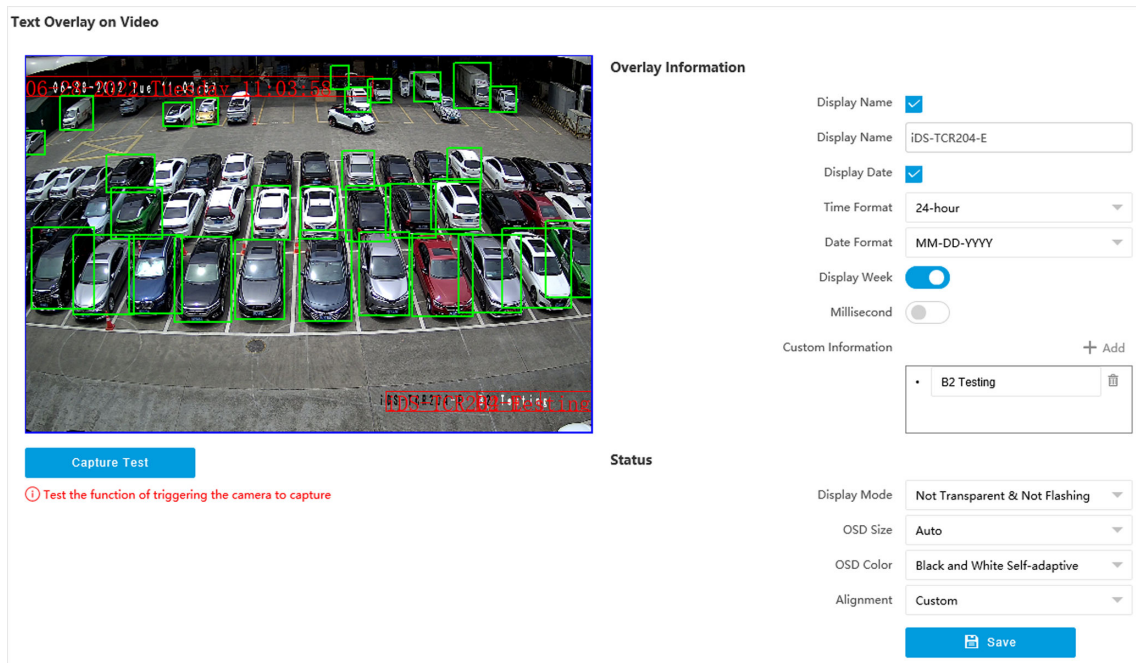


Figure 6-4 Set OSD

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 7 Network Configuration

7.1 Set IP Address

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

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

NIC Settings

NIC Type	Auto
DHCP	☐
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 7-1 Set IP Address

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.

7.2 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

Address Type

Server IP Address

Server Port

Device ID

Key

Register Status

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

Save

Figure 7-2 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.

7.3 Set DDNS

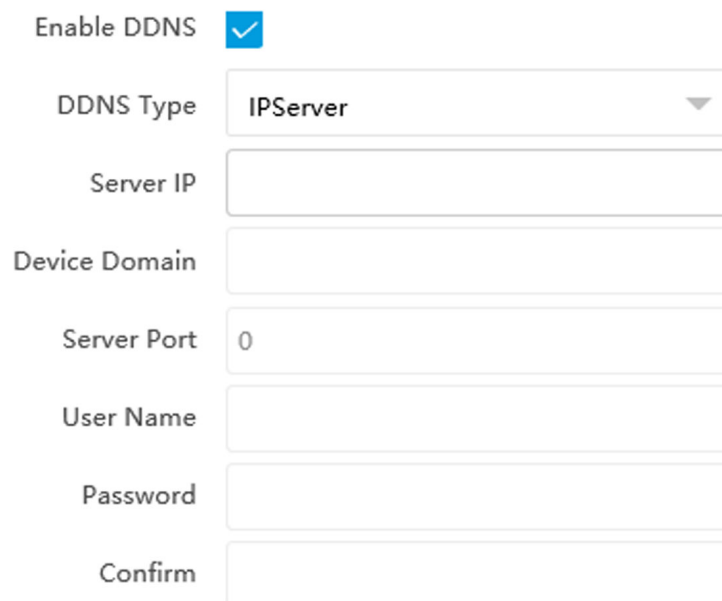
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to 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	0
User Name	
Password	
Confirm	

Figure 7-3 Set DDNS

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

- | | |
|---------------------------|--|
| By Browsers | Enter the domain name in the browser address bar to access the device. |
| By Client Software | Add domain name to the client software. Refer to the client software manual for specific adding methods. |

7.4 Set Port

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

Go to **Configuration → Network → Network Parameters → Port** for port settings.

The screenshot shows a web interface for configuring network ports. It is organized into five sections, each with an 'Enable' checkbox and a port number input field. At the bottom right is a blue 'Save' button.

Port Type	Enable	Port Number
HTTP Port	☒	80
HTTPS Port	☐	443
RTSP Port	☒	554
Server Port		8000
SADP Port	☒	

Figure 7-4 Set Port

HTTP Port

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

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.
 - The supported ports vary with different models. The actual device prevails.
-

Chapter 8 Serial Port Configuration

8.1 Set RS-485

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

Before You Start

The corresponding device has been connected via the RS-485 serial port.

Steps



Note

The number of available RS-485 serial port varies with different models.

1. Go to **Configuration → System → System Settings → Serial Port → RS-485**.

RS-485							
No.	Baud Rate	Data Bit	Stop Bit	Parity	Flow Control	Work Mode	
1	38400 bps	8	1	None	None	Application Trigger	
2	115200 bps	8	1	None	None	Application Trigger	
3	115200 bps	8	1	None	None	Application Trigger	

Figure 8-1 Set RS-485

2. Set **Baud Rate, Data Bit, Stop Bit**, etc.



Note

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

3. Set **Work Mode**.

Application Trigger

Select it when the signal trigger devices (such as radar) are connected to the RS-485 serial port of the device.

Transparent Channel

Select it when the other peripheral devices are connected to the RS-485 serial port of the device for communication transmission.

4. Click **Save**.

8.2 Set RS-232

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

Before You Start

The debugging device has been connected via the RS-232 serial port.

Steps

1. Go to **Configuration → System → System Settings → Serial Port → RS-232**.

RS-232						
No.	Baud Rate	Data Bit	Stop Bit	Parity	Flow Control	Work Mode
1	9600 bps	8	1	None	None	Transparent Channel

Figure 8-2 Set RS-232

2. Set **Baud Rate, Data Bit, Stop Bit**, etc.



Note

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

3. Select **Work Mode**.

Console

Select it when you need to debug the device via RS-232 serial port.

Transparent Channel

Select it, and the network command can be transmitted to RS-232 control command via the RS-232 serial port.

Narrow Bandwidth Transmission

Reserved.

4. Click **Save**.

Chapter 9 Safety Management

9.1 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.

9.2 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.

9.3 Set HTTPS

9.3.1 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.

9.3.2 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**.

9.4 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 Event** .
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

9.5 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**.

9.6 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**.

9.7 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**.



Note

The IP address only refers to the IPv4 address.

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

6. Click **Save**.

9.8 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.

9.9 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 10 Maintenance

10.1 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.

10.2 Enable System Log Service

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

Steps

1. Go to **Configuration → 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.

10.3 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.

10.4 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.



Note

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

Result

The device will reboot automatically after upgrade.

10.5 Reboot

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

Steps

1. Go to **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.

10.6 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.

10.7 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**.

10.8 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**.

10.9 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**.

10.10 Export Parameters

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

Steps

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



Note

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

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

10.11 Import Configuration File

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

Before You Start

Save the configuration file to the computer.

Steps



Caution

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

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



Note

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

3. Click **Browse** to select the configuration file.
4. 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.

10.12 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**.

10.13 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**.



See Far, Go Further