

Smart Monitoring 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 Activation and Login 1
1.1 Activation 1
1.1.1 Default Information 1
1.1.2 Activate via SADP 1
1.1.3 Activate via Web Browser 2
1.2 Login 3
Chapter 2 Application Mode Configuration 4
2.1 Set Smart Monitoring Capture 4
2.2 Set Incident Detection 7
2.2.1 Set Violation and Incident Detection 8
2.2.2 Set Linked Lane Parameters 10
2.2.3 Draw Lane Lines and Detection Areas 11
2.2.4 Set Data Collection 13
2.3 Set License Plate Recognition System Capture 16
Chapter 3 Capture Parameters Configuration 20
3.1 Set License Plate Recognition Parameters 20
3.2 Set Supplement Light Parameters 20
3.3 Set Vehicle Feature Parameters 21
3.4 Set Body Picture Matting 22
3.5 Set Picture Composition 22
3.6 Set Information Overlay 23
3.6.1 Set Single Picture Overlay 23
3.6.2 Set Composite Picture Overlay 25
3.7 Set Image Encoding Parameters 27
3.8 Set Capture Schedule 28
3.9 Set Captured Image Parameters 29

3.10 Set ICR 30
3.11 Debug 31
3.11.1 Debug Device 31
3.11.2 Vehicle Capture and Recognition Service 32
3.11.3 Set Image Format 33
3.12 Set Barrier Gate Linkage 34
3.12.1 Set Allowlist and Blocklist 34
3.12.2 Control Barrier Gate 35
3.12.3 Set Wiegand Parameters 37
Chapter 4 View Real-Time Picture 39
Chapter 5 View Traffic Statistics 41
5.1 View Real-Time Traffic Statistics 41
5.2 View Traffic Flow Statistics 41
Chapter 6 Live View and Local Configuration 42
6.1 Live View 42
6.1.1 Start/Stop Live View 42
6.1.2 Select Image Display Mode 42
6.1.3 Select Window Division Mode 42
6.1.4 Select Stream Type 42
6.1.5 Capture Picture Manually 42
6.1.6 Record Manually 42
6.1.7 Start/Stop Two-Way Audio 43
6.1.8 Enable/Disable Audio 43
6.1.9 Enable Digital Zoom 43
6.1.10 Enable Regional Focus 44
6.1.11 Select Video Mode 44
6.2 PTZ Operation 44
6.3 Local Configuration 46

Chapter 7 Record and Capture 50
7.1 Set Storage Path 50
7.1.1 Set Storage Card 50
7.1.2 Set Quota 51
7.1.3 Set FTP 51
7.1.4 Set Cloud Storage 53
7.2 Set Record Schedule 54
7.3 Set Snapshot Schedule 56
7.4 Search Picture 56
7.5 Playback 57
Chapter 8 Encoding and Display 59
8.1 Set Video Encoding Parameters 59
8.2 Set Image Parameters 60
8.3 Set ROI 63
8.4 Set Privacy Mask 64
8.5 Enable Regional Exposure 65
8.6 Set OSD 66
Chapter 9 Network Configuration 68
9.1 Set IP Address 68
9.2 Set Port 71
9.3 Set IEEE 802.1X 72
9.4 Set DDNS 73
9.5 Set SNMP 73
9.6 Set QoS 75
9.7 Connect to Platform 75
9.7.1 Set Arm Host 75
9.7.2 Set SDK Listening 76
9.7.3 Set ISAPI Listening 77

9.7.4 Connect to ISUP Platform 79
9.7.5 Connect to OTAP 80
9.7.6 Connect to Hik-Connect 82
9.8 Set Integration Protocol 84
Chapter 10 Serial Port Configuration 85
10.1 Set RS-485 85
10.2 Set RS-232 86
Chapter 11 Event and Alarm 87
11.1 Exception Alarm 87
11.2 Set Email 87
11.3 Set Email Event 88
Chapter 12 Safety Management 90
12.1 Manage User 90
12.2 Enable User Lock 90
12.3 Set SSH 91
12.4 Prohibit PING 91
12.5 Enable System Log Service 91
12.6 Set Timeout Logout 92
12.7 Set Password Validity Period 92
12.8 Set SDK Protocol Authentication Mode 92
12.9 Set RTSP Authentication 93
12.10 Set IP Address Filtering 93
12.11 Set HTTPS 93
12.11.1 Create and Install Self-signed Certificate 93
12.11.2 Install Authorized Certificate 94
Chapter 13 Maintenance 95
13.1 View Device Information 95
13.2 Synchronize Time 95

13.3 Set DST 96
13.4 Reboot 96
13.5 Restore Parameters 97
13.6 Export Parameters 97
13.7 Export Debug File 97
13.8 Export Diagnosis Information 98
13.9 Upgrade 98
13.10 Import Configuration File 98
13.11 Log 99
13.11.1 Enable Log According to Module 99
13.11.2 Search Log 99
13.12 Enable Maintenance Service 100

Chapter 1 Activation and Login

1.1 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.

1.1.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.64
- Default user name: admin

1.1.2 Activate via SADP

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

Before You Start

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

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

Steps

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

   Caution

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

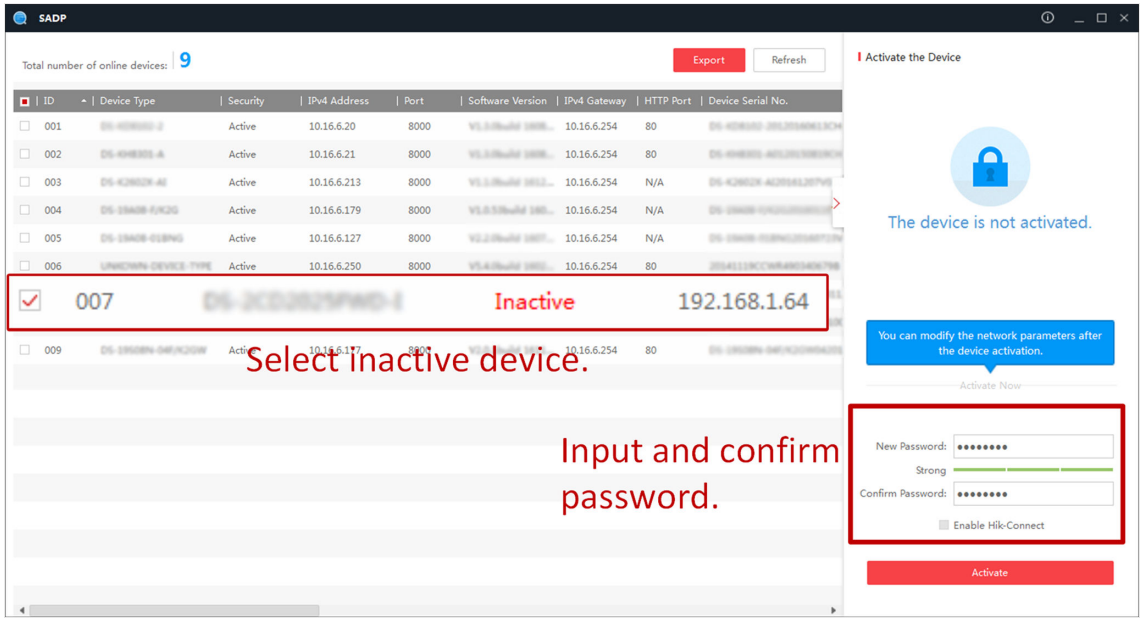


Figure 1-1 Activate via SADP

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

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

1.1.3 Activate via Web Browser

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

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

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

Caution

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

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

1.2 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 2 Application Mode Configuration

Note

- The supported application modes vary with different models. The actual device prevails.
- When you draw lane lines or detection areas on **Application Mode** interface:
  - You can enable **Display All Areas** to display all the lines and areas, convenient to view the effect of all the lines and areas. If you uncheck it, only the current selected lane will be displayed, convenient to draw the current lane.
  - You can enable **Small Target Detection** and draw the small target detection areas which are always set at the road distance to raise the detection effect of the distant targets.
  - The system will capture a picture and use it as the background. You can also enable **Video Background** to use the live view as the background.

Caution

You can click **Default** on **Application Mode** interface to restore all the set parameters to the default settings. Please operate with care.

2.1 Set Smart Monitoring Capture

The smart monitoring mode supports capturing motor vehicles, non-motor vehicles, and pedestrians via video triggering.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Application Mode** as **Smart Mode**.

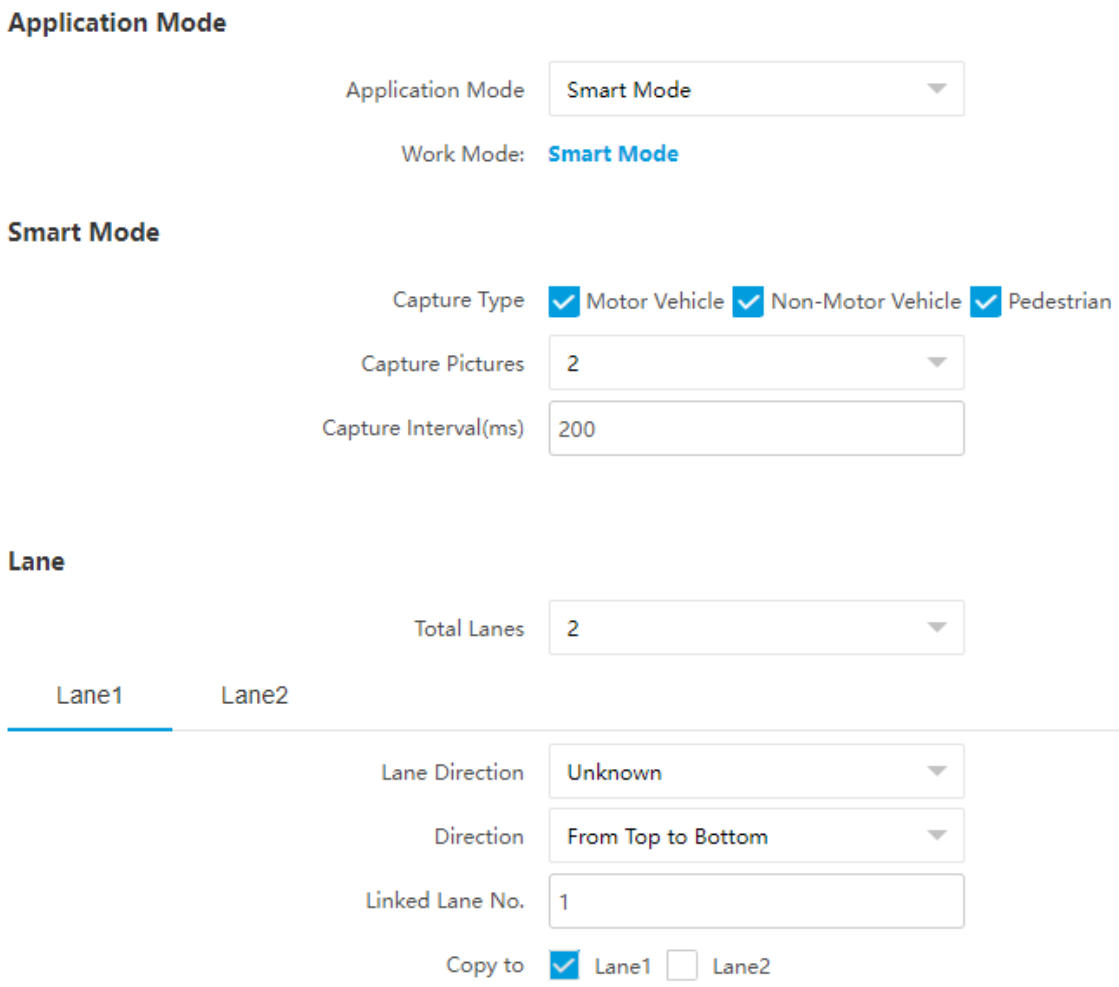


Figure 2-1 Set Smart Monitoring Capture

3. Set smart mode parameters.

Capture Type

Select the targets to be recognized and captured in the scene.

Capture Pictures

The number of captured picture(s).

Capture Interval

The time between the adjacent captures.

4. Set the lane parameters.

Total Lanes

The number of the total lane(s) in the scene.

Lane Direction

The guidance direction of the lane.

Direction

If you select **From Top to Bottom**, the targets from the approaching direction towards the device will be captured. If you select **From Bottom to Top**, the targets from the leaving direction away from the device will be captured. If you set the direction as **From Top to Bottom**, then the vehicle will be judged as wrong-way driving if it comes from bottom to top, and vice versa.

Linked Lane No.

The corresponding lane No. linked with the current lane. The lane No. will be overlaid on the captured picture.

Copy to

Check the other lane(s) to copy the same settings.

5. Draw lane lines.

1) Click **Draw Lane Line**.

Note

The system will capture a picture and use it as the background. You can also check **Video Background** to use the live view as the background.

2) Select the default lane lines, trigger line, and right border line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
3) **Optional:** Click **Redraw Lane Line** to redraw the lines.
4) Click **OK**.

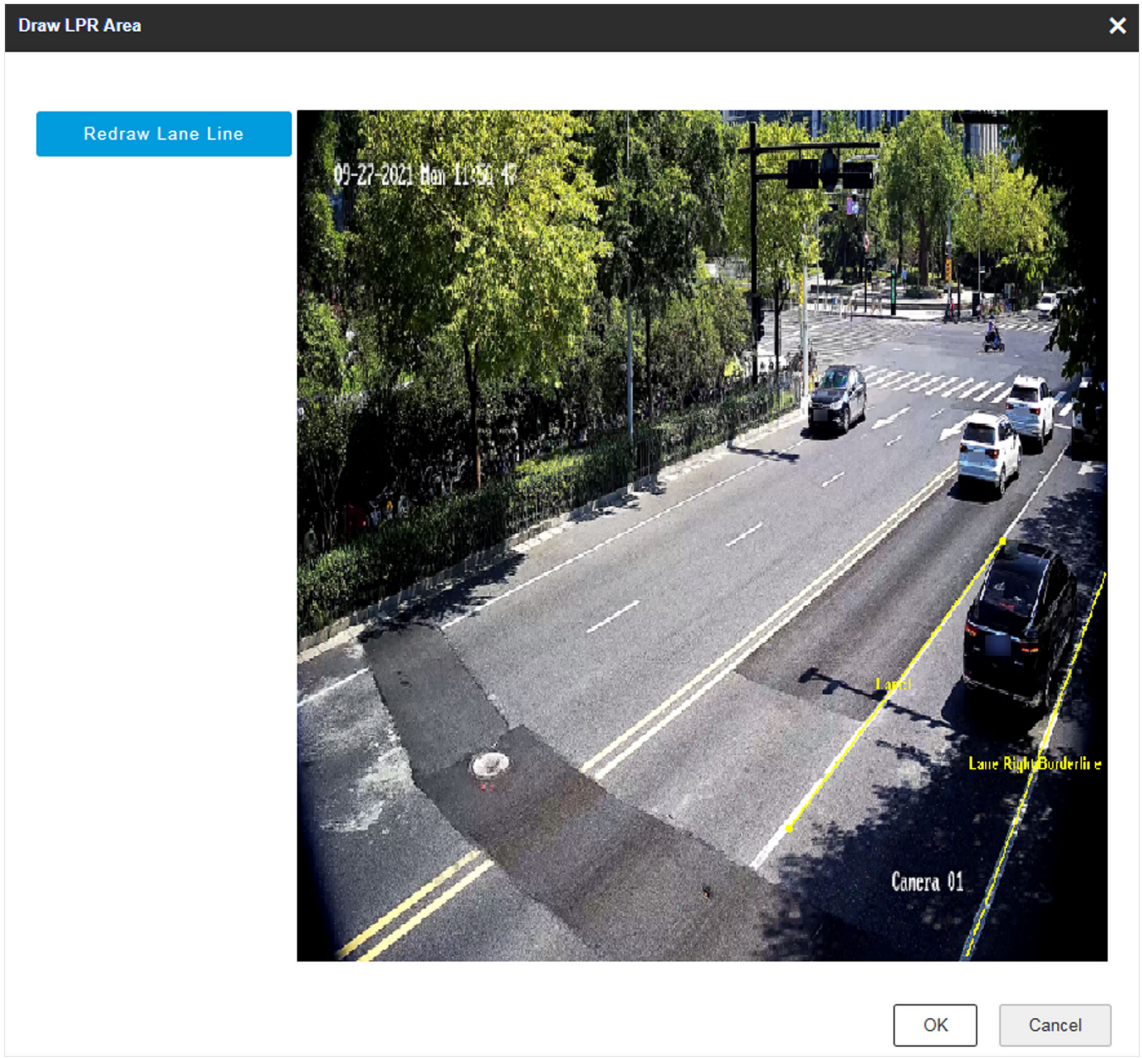


Figure 2-2 Draw Lane Line

6. Click **Save**.

2.2 Set Incident Detection

The device supports to capture various traffic incidents.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Application Mode** as **Event Detection**.
3. Click **Event Detection**.
4. Set the capture parameters.

Scene Mode

Select the scene according to the actual device installation environment.

Close Range Capture

Check it and set **Capture Interval**. The device will track the target until one more picture is captured in close distance according to the capture interval.

5. Set other parameters, and click **Save**. Refer to the chapters below for details.

2.2.1 Set Violation and Incident Detection

The device can capture pictures of the targets passing the checkpoint in the linked lanes according to the set rules.

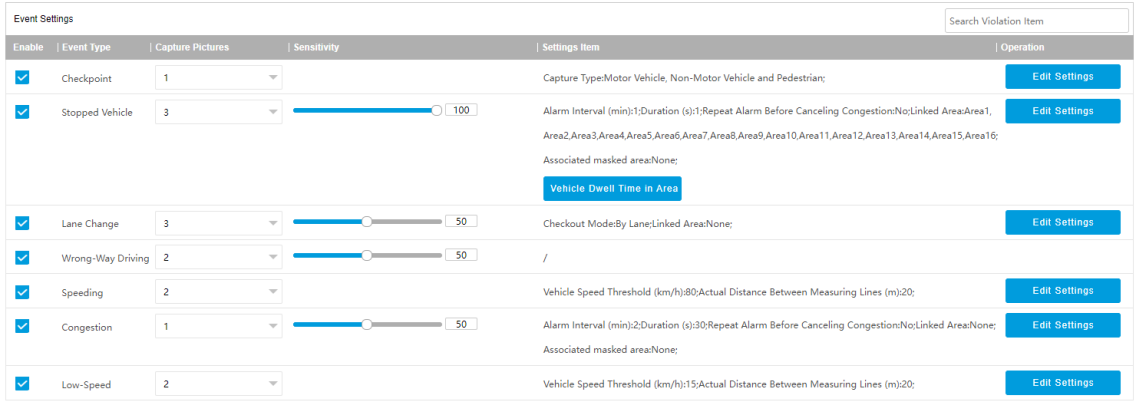


Figure 2-3 Capture Type

Note

For the violation or incident types supporting linked areas and associated masked areas, the enabled No. of the linked areas and associated masked areas should be different, or the linked areas cannot take effect.

Table 2-1 Capture Type Description

Capture Type	Parameters Description
Checkpoint	Check it and select the number of captured picture(s). Click **Edit Settings** to select **Capture Type**.
Stopped Vehicle	The motor vehicle stops at the positions where parking is forbidden. Check it, select the number of captured picture(s), and set **Sensitivity**. The higher the sensitivity is, the more easily the violation will be captured. Click **Edit Settings** to set the parameters below. • **Alarm Interval**: The interval between two alarms. • **Duration**: When the vehicle stops at the positions for more than the set duration, capture will be triggered.

Capture Type	Parameters Description
	• **Linked Area**: Check the lane area(s) to link to the violation detection. All the selected area(s) will apply the set duration. • **Associated Masked Area**: Check corresponding areas and violations or incidents occurred in those areas will not be detected. **Note** • You can also click **Vehicle Dwell Time in Area** to set the duration of each linked area independently. • When the device judges that the current lane is in congestion status, the stopped vehicles will not be captured.
Lane Change	Most part of the vehicle body crosses over the lane line and enters into another lane. Check it, select the number of captured picture(s), and set the sensitivity. Click **Edit Settings** to select **Checkout Mode**. • **By Lane**: Select it to detect the lane change in the set lane(s). • **By Area**: Select it to detect the lane change in the set area(s).
Wrong-Way Driving	The vehicle is driven in the direction opposite to the guidance direction of the lane. Check it, select the number of captured picture(s), and set the sensitivity.
Speeding	The motor vehicle is driven in the speed larger than the max. speed limit of the lane. Check it and select the number of captured picture(s). Click **Edit Settings** to set the parameters below. • **Vehicle Speed Threshold**: The max. speed limit. When the vehicle speed exceeds the value, speeding capture will be triggered. • **Actual Distance Between Measuring Lines**: The actual distance between the two measuring lines within which the vehicle speed is detected.
Congestion	The motor vehicles are queuing and the roads are blocked. Check it and select the number of captured picture(s), and set **Sensitivity**. The higher the sensitivity is, the more easily the congestion will be captured. Click **Edit Settings** to set the parameters below. • **Alarm Interval**: The interval between two alarms. • **Duration**: When the congestion lasts for more than the set duration, capture will be triggered. • **Repeat Alarm Before Canceling Congestion**: If you enable the function, alarms will be repeated before the congestion status is removed.

Capture Type	Parameters Description
	• **Linked Area**: Check the lane area(s) to link to the detection. • **Associated Masked Area**: Check corresponding areas and violations or incidents occurred in those areas will not be detected.
Low-Speed	The motor vehicle is driven in the speed lower than the min. speed limit. Check it and select the number of captured picture(s). Click **Edit Settings** to set the parameters below. • **Vehicle Speed Threshold**: The min. speed allowed. When the vehicle speed is lower than the value, low-speed capture will be triggered. • **Actual Distance Between Measuring Lines**: The actual distance between the two measuring lines within which the vehicle speed is detected.

Note

For the violation and incident types supporting linked areas, if you select linked area(s), select **Area Type** of the corresponding linked area.

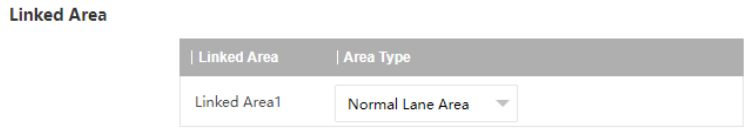


Figure 2-4 Set Linked Area Type

2.2.2 Set Linked Lane Parameters

You can set the properties and parameters of the linked lanes.

Steps

Note

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

1. Select **Total Lanes**.
2. Set the lane parameters.

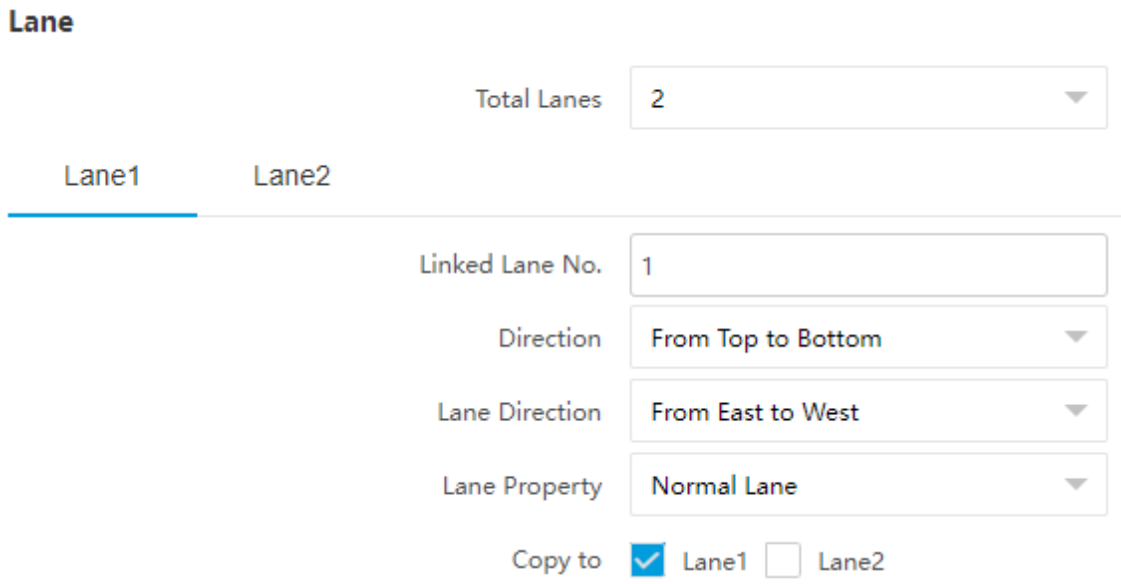


Figure 2-5 Set Lane Parameters

Linked Lane No.

The corresponding lane No. linked with the current lane. The lane No. will be overlaid on the captured picture.

Direction

If you select **From Top to Bottom**, the targets from the approaching direction towards the device will be captured. If you select **From Bottom to Top**, the targets from the leaving direction away from the device will be captured. If you set the direction as **From Top to Bottom**, then the vehicle will be judged as wrong-way driving if it comes from bottom to top, and vice versa.

Lane Direction

The guidance direction of the lane.

Lane Property

Select the current lane property according to its usage.

Copy to

Check the other lane(s) to copy the same settings.

3. Click **Save**.

2.2.3 Draw Lane Lines and Detection Areas

Draw lane lines and detection areas to detect and capture the violations or incidents in the linked areas.

Before You Start

Select the linked areas and associated masked areas if needed.

Steps

1. Click **Draw Lane Line**.
2. Select the lane.
3. Set **Lane Line Type** and **Right Border Line Type**.
4. Select the default lane lines, right border line, triggering line, and measuring lines, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.

> **Note**
>
> Measuring lines are available for speeding and low-speed detections.

5. **Optional:** Click **Draw Lane Line** to restore to the default drawing.
6. Select area and click **Draw Area**. Click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area.
7. **Optional:** Click **Draw Area** to delete the current area.
8. **Optional:** Check **Digital Zoom**, and drag the mouse on the live view image to zoom the area in. Uncheck it to exit from digital zoom.
9. Click **OK**.

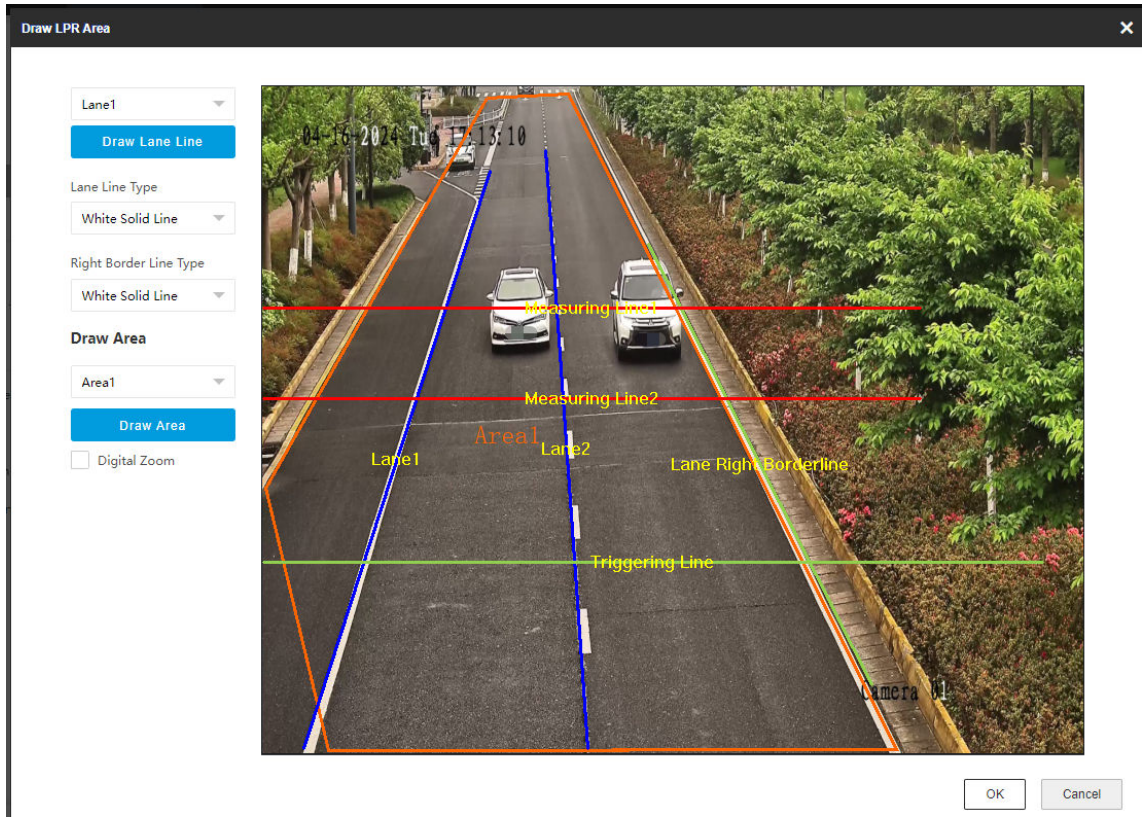


Figure 2-6 Draw Lane Lines and Detection Areas

2.2.4 Set Data Collection

The device supports to detect the traffic flow, POS, and other information.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Application Mode** as **Event Detection**.
3. Click **Data Collection**.
4. Set traffic flow detection parameters and traffic flow information overlay.

Set Traffic Flow Detection

Steps

1. Click **Traffic Flow Detection Settings**.

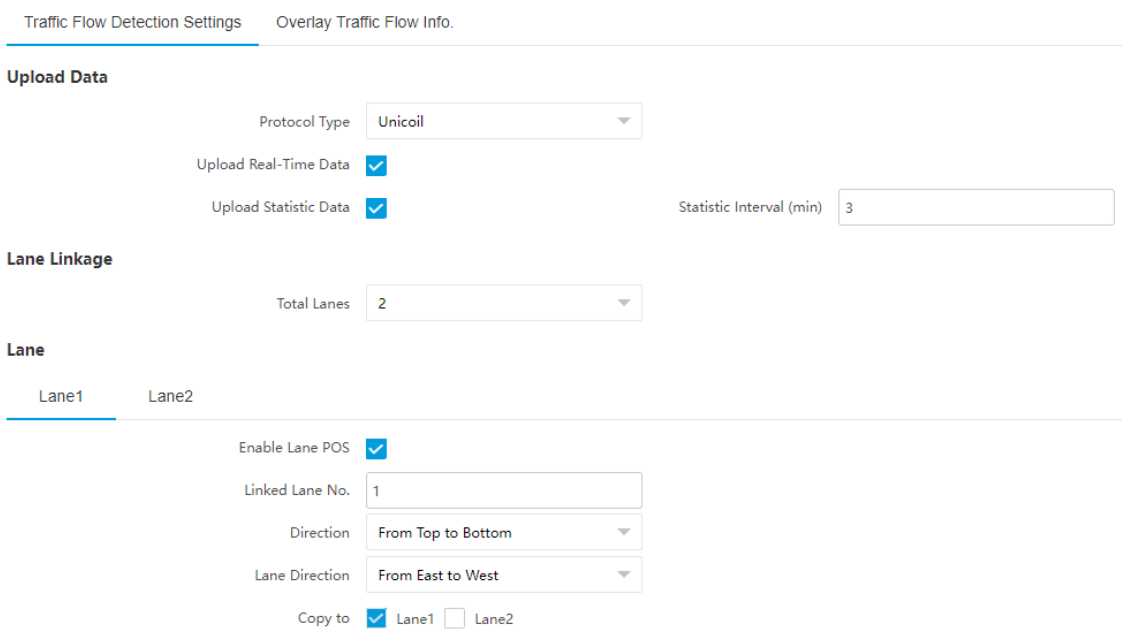


Figure 2-7 Set Traffic Flow Detection

2. Set the data upload parameters.

Protocol Type

Unicoil

One coil for each lane.

Double Coil

Two coils for each lane.

Upload Real-Time Data

The device will upload the real-time data to the server. The real-time data include road status, time, lane No., entrance/exit status, instantaneous speed, space headway, time headway, congestion traffic flow, driving direction, queue length, congestion level, and intersection dedicated data such as the signals when leaving the left turn line, right turn line, going straight line, and stop line at intersections (only supported for multi-coils protocol).

Upload Statistic Data

The device will upload the statistic data to the server according to the set **Statistic Interval**. The statistic data include lane No., traffic, average speed, traffic state, lane queue length, time interval of vehicle head, headway distance, lane space occupancy, lane time occupancy, average delay, and average number of stops.

3. Set the lane parameters.
   1) Select **Total Lanes**.
   2) Click the lane No.
   3) Check **Enable Lane POS** to enable the POS information (feature information) collection of the lane.
   4) Set other parameters.

      Linked Lane No.

      The corresponding lane No. linked with the current lane. The lane No. will be overlaid on the captured picture.

      Direction

      If you select **From Top to Bottom**, the targets from the approaching direction towards the device will be captured. If you select **From Bottom to Top**, the targets from the leaving direction away from the device will be captured. If you set the direction as **From Top to Bottom**, then the vehicle will be judged as wrong-way driving if it comes from bottom to top, and vice versa.

      Lane Direction

      The guidance direction of the lane.

   5) **Optional:** Check lane(s) to copy the parameters of the current lane to other lane(s).
4. Draw lane lines and virtual coil areas.
   1) Click **Draw Lane Line**.
   2) Select the lane.
   3) Select the default lane lines and right border line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
   4) **Optional:** Click **Draw Lane Line** to restore to the default drawing.
   5) Click **Draw Virtual Coil A/B/C...** to draw the virtual coil areas.

Note

- Click the left button of the mouse to locate the vertexes of the virtual coil area on the live view image, and click the right button of the mouse to finish the drawing.
- It is recommended that the virtual coil height is half of the small-sized vehicle length and the width is the lane width.
- The virtual coils should be set at the positions where the radar and video can both detect.

6) **Optional:** You can check **Virtual Coil Aided Drawing** and draw the coils of lane 1. Then the coils of the other lanes will be generated automatically.
7) **Optional:** Check **Digital Zoom**, and drag the mouse on the live view image to zoom the area in. Uncheck it to exit from digital zoom.
8) Click **OK**.

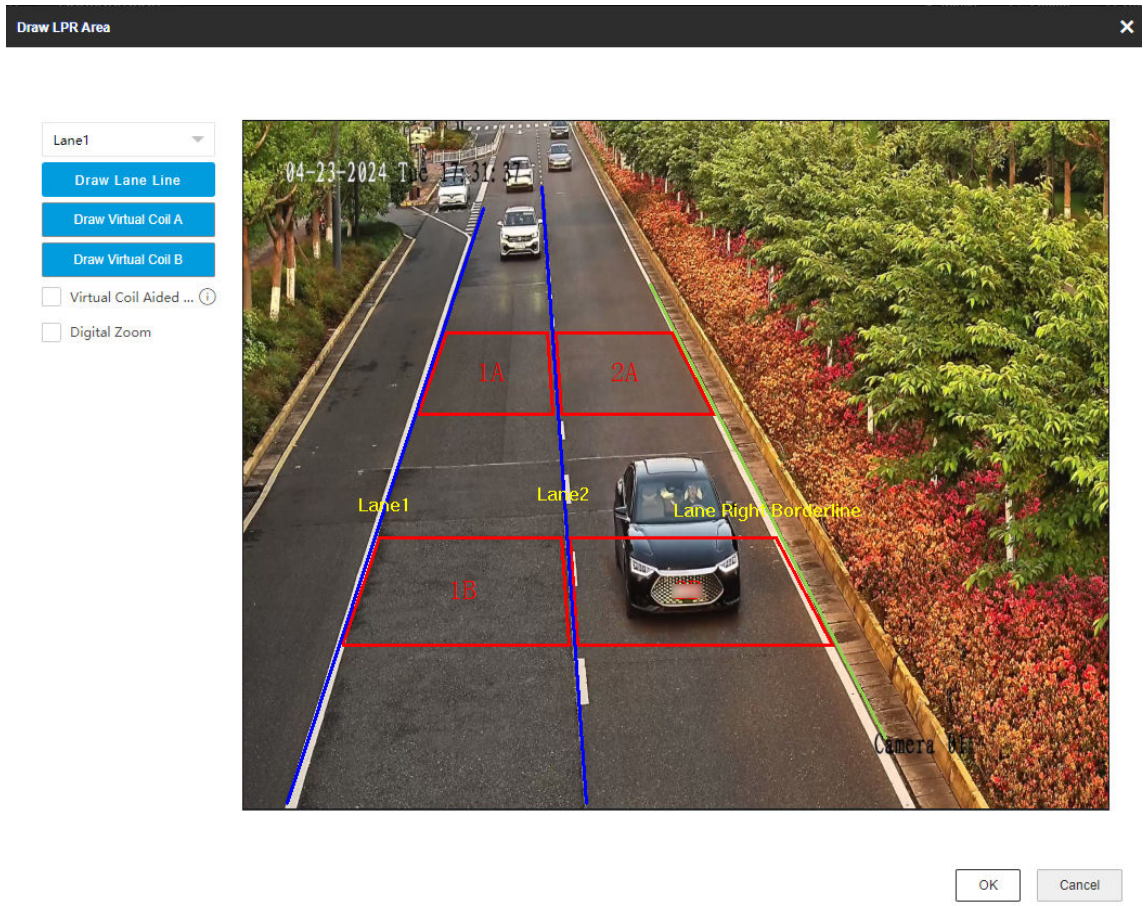


Figure 2-8 Draw Lane Lines and Virtual Coils Areas

5. Click **Save**.

Set Traffic Flow Information Overlay

Steps

1. Click **Overlay Traffic Flow Info.**

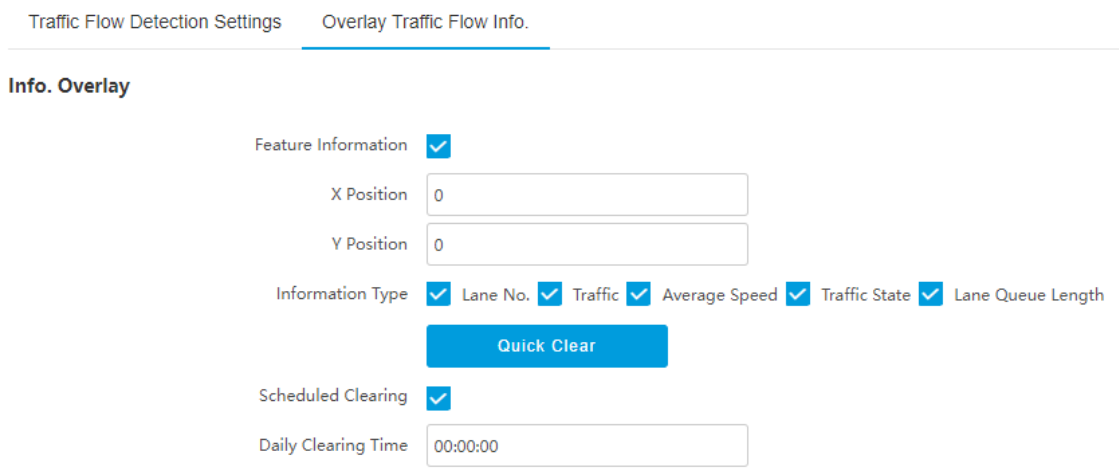


Figure 2-9 Set Traffic Flow Information Overlay

2. Set feature information overlay.
   1) Check **Feature Information** to overlay the feature information on the video stream and display on the live view image.
   2) Enter **X Position** and **Y Position** to display on the image.
   3) Select **Information Type** to overlay on the image.

Note

You can display the traffic flow (left turn flow, right turn flow, and going straight flow), and coil flow (coil 1 or coil 2 flow) on the live view image.

3. **Optional:** Clear the traffic flow statistics data if needed.
   - Click **Quick Clear** to clear all the traffic flow statistics data quickly.
   - If you want to clear the traffic flow statistics data at the fixed time daily, check **Scheduled Clearing** and set **Daily Clearing Time**.
4. Click **Save**.

2.3 Set License Plate Recognition System Capture

If you want to trigger capture of the passing vehicles and recognize the license plate numbers, set license plate recognition system capture.

Steps

1. Go to **Configuration → Capture → Application Mode** .
2. Select **Application Mode** as **License Plate Recognition System**.

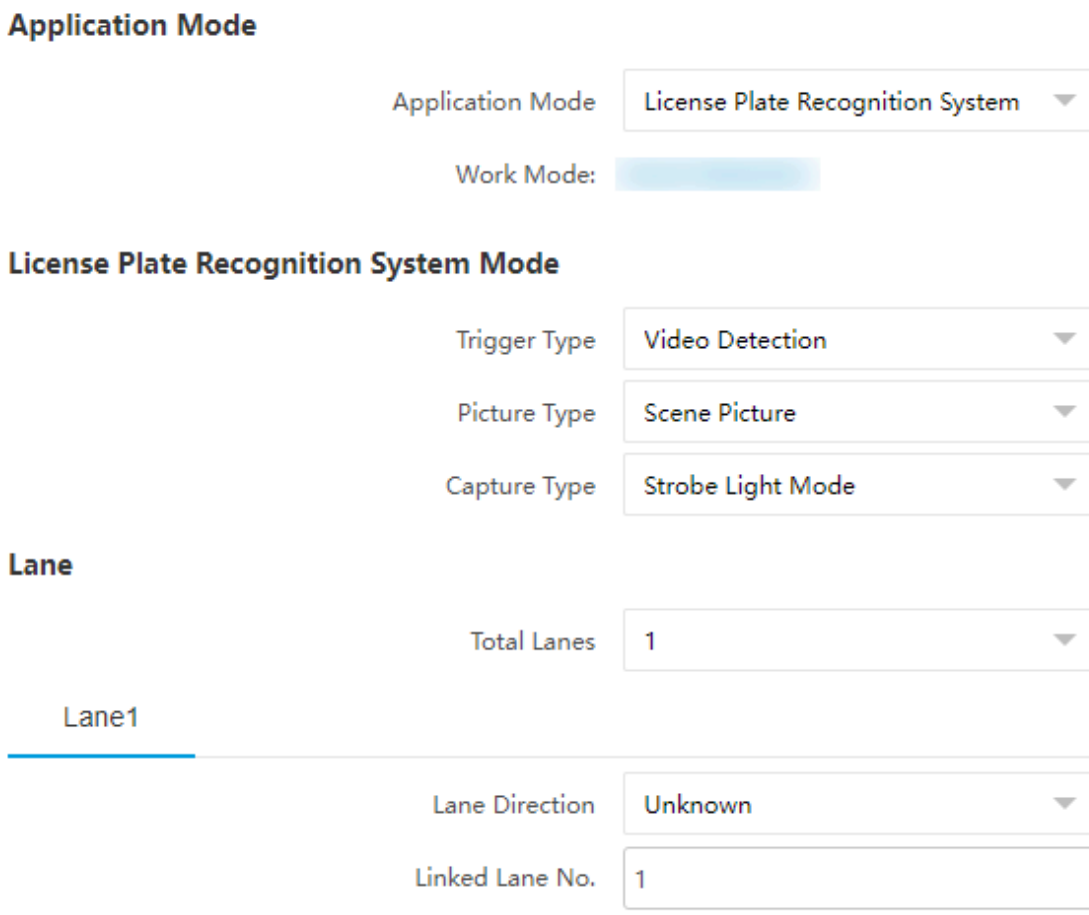


Figure 2-10 Set License Plate Recognition System

3. Select **Trigger Type**.

   Video Detection

   The passing vehicles will be recognized via videos. The capture mode is recommended as **Strobe Light Mode**.

   I/O Coil

   Select it when the device has been connected to I/O signal.

Note

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

4. Select **Picture Type**.

   Scene Picture

   Only one passing vehicle picture will be output.

5. Set the lane parameters.

   Total Lanes

The number of the total lane(s) in the scene.

Lane Direction

The guidance direction of the lane.

Linked Lane No.

The corresponding lane No. linked with the current lane. The lane No. will be overlaid on the captured picture.

6. Set I/O trigger parameters if you select **Trigger Type** as **I/O Coil**.

I/O Trigger Default Status

Capture is triggered according to the level signal status. If you select **Falling Edge**, the device will trigger capture at the moment that the high level falls to low level. If you select **Rising Edge**, the device will trigger capture at the moment that the low level rises to high level.

Linked I/O No.

When the coil detects that there is a vehicle passing, a rising or falling edge signal is sent to the linked I/O of the device to trigger capture.

7. Draw lane lines.
   1) Click **Draw Lane Line**.
   2) Select the default lane lines, trigger line, and right border line, and drag the two end points of the line or drag the whole line to adjust its position according to the actual scene.
   3) Click **OK**.

Note

It is recommended to draw the trigger line at the position which is 1/3 to 1/4 of the lane line. The license plate pixel should be between 120 to 180 at the capture position.



Figure 2-11 Draw Lane Line

8. Click **Save**.

Chapter 3 Capture Parameters Configuration

3.1 Set License Plate Recognition Parameters

When there are vehicles of different types passing from different directions, set the license plate recognition parameters.

Steps

Note

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

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

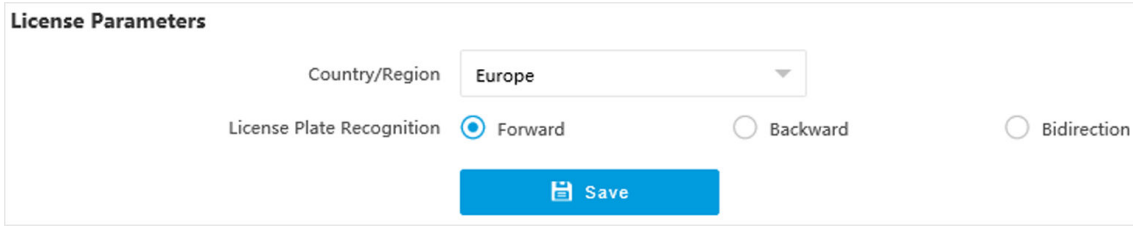


Figure 3-1 Set License Plate Recognition Parameters

2. Set **Country/Region** according to the actual needs.
3. Select **License Plate Recognition**.
   - Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
   - Select **Backward** when license plates of vehicles from the leaving direction need to be recognized.
   - Select **Bidirection** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.
4. Click **Save**.

3.2 Set Supplement Light Parameters

Supplement light can enhance the image stabilization and adjust the brightness and color temperature.

Steps

Note

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

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

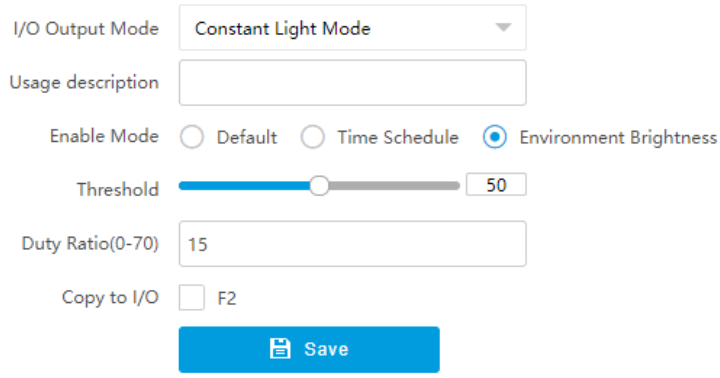


Figure 3-2 Set Supplement Light Parameters

2. Select the I/O and set the usage.

   I/O Output Mode

   Constant Light Mode

   The constant light supplements light for the scene.

   Usage Description

   Enter the usage description of the constant light.
3. Set the supplement light control mode.
   - Select **Default** to disable the supplement light.
   - Select **Time Schedule** when you want the supplement light to be enabled during a fixed time period. Set the start time and end time.
   - Select **Environment Brightness** when you want the supplement light to be controlled by detecting the surroundings brightness automatically. Set the brightness threshold. The higher the threshold is, the harder the supplement light can be enabled.
4. **Optional:** Select other I/O(s) to copy the same settings.
5. Click **Save**.

3.3 Set Vehicle Feature Parameters

Set vehicle feature parameters if you need to detect the vehicle features of the passing vehicle.

Steps

Note

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

1. Go to **Configuration → Capture → Capture Parameters → Vehicle Feature → Vehicle Feature** .
2. Check the motor and non-motor vehicle features that needed to be detected, and set the corresponding sensitivity.
3. Click **Save**.

3.4 Set Body Picture Matting

Set body picture matting first if you need to upload body and vehicle pictures to the platform.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Parameters → Vehicle Feature → Body Picture Matting** .
2. Check **Enable Body Picture Matting**.

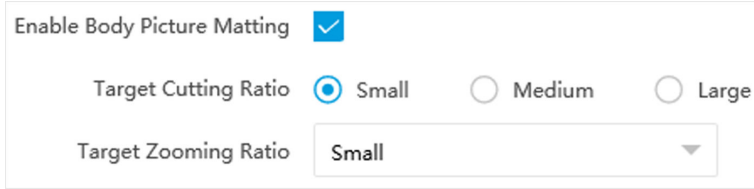


Figure 3-3 Set Body Picture Matting

3. Set body picture matting parameters according to the actual needs.
4. Click **Save**.

Result

If the device is level 1 armed, the matting pictures will be uploaded to this device directly. If the device is level 2 armed, the matting pictures will be saved to the SD/TF card and uploaded to a level 2 armed device.

3.5 Set Picture Composition

You can enable the picture composition to composite several pictures into one to make it convenient to view the violation captured pictures.

Steps

Note

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

1. Go to **Configuration → Capture → Capture Parameters → Image Encoding and Composition → Checkpoint Image Composition/Violation Picture Composition** .

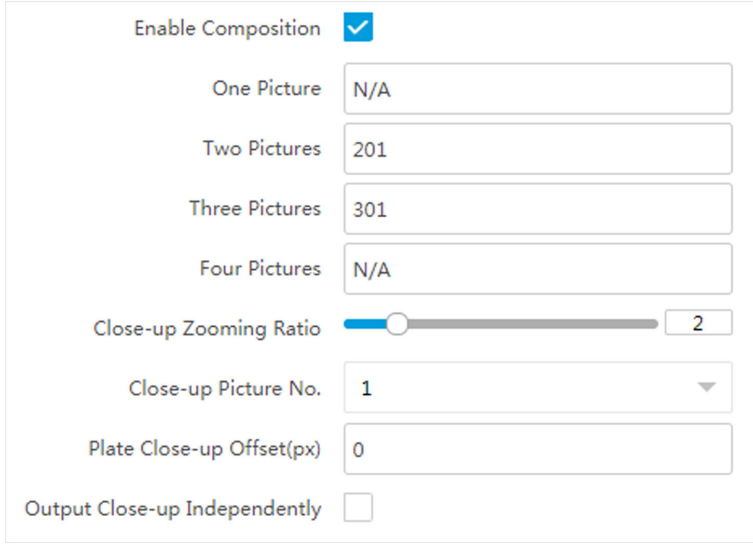


Figure 3-4 Set Picture Composition

2. Check **Enable Composition**.
3. Set composition types for different picture quantities.
4. Set other composition parameters.

   Close-up Zooming Ratio

   The higher the value is, the larger the close-up is.

   Close-up Picture No.

   It is the picture where the close-up comes from.

   Plate Close-up Offset

   The default value is 0, which is recommended to be adopted. The device can capture close-up pictures according to the set offset when no license plate is recognized.
5. **Optional:** Check **Output Close-up Independently** to output close-up pictures independently when the picture composition is not enabled.

   Note

   Enabling composition and outputting close-up independently functions conflict with each other. You can only enable one.
6. Click **Save**.

3.6 Set Information Overlay

3.6.1 Set Single Picture Overlay

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

Steps

Note

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

1. Go to **Configuration → Capture → Capture Parameters → Text Overlay** .
2. Select single picture channel.
3. Check **Capture Picture Overlay**.

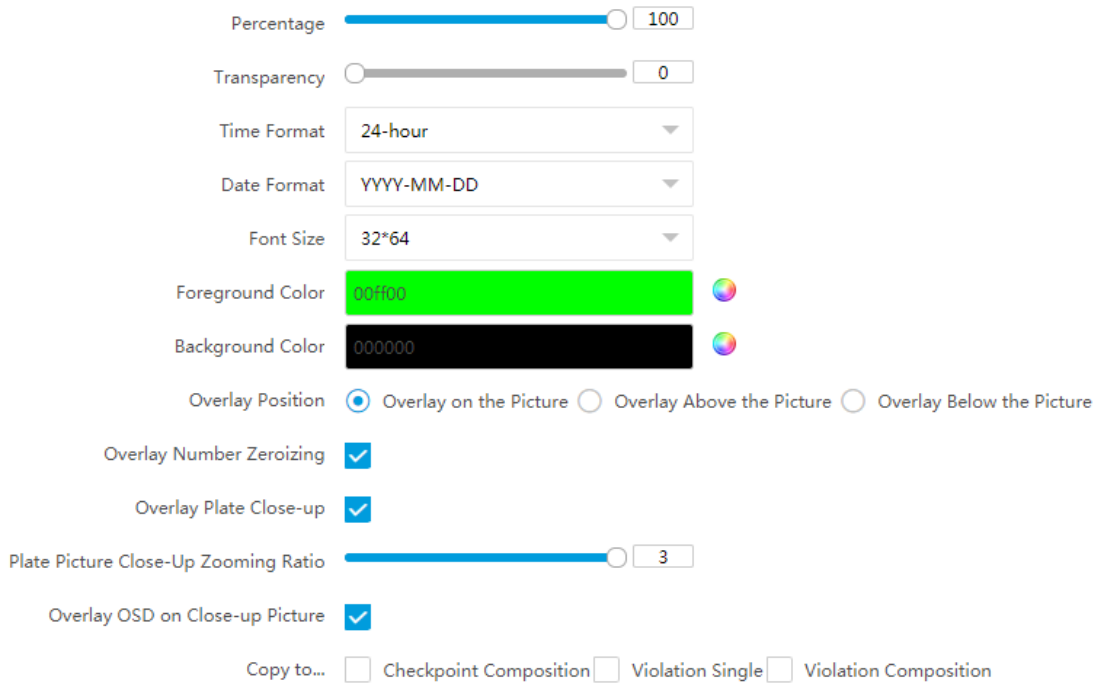


Figure 3-5 Set Single Picture Overlay

4. Set the percentage, front size, color, overlay position, etc.

Percentage

It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

Transparency

It is the condition of viewing the live view image through the overlaid information.

Overlay Number Zeroizing

When the overlaid number digits are smaller than the fixed digits, 0 will be overlaid before the overlaid number. E.g., the fixed digits for lane No. is 2. If the lane No. is 1, 01 will be overlaid on the picture.

Overlay Plate Close-up

Check it to overlay license plate close-up pictures on the captured pictures. Set **Plate Picture Close-Up Zooming Ratio** to adjust the close-up picture size.

Overlay OSD on Close-up Picture

Check it to overlay the OSD information on the close-up pictures.

5. **Optional:** Check the other channel(s) to copy the same settings.
6. Select the overlay information from the list.

Note

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

7. Set the overlay information.

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

8. Click **Save**.

3.6.2 Set Composite Picture Overlay

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

Steps

Note

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

1. Go to **Configuration → Capture → Capture Parameters → Text Overlay** .
2. Select composite picture channel.
3. Check **Capture Picture Overlay**.

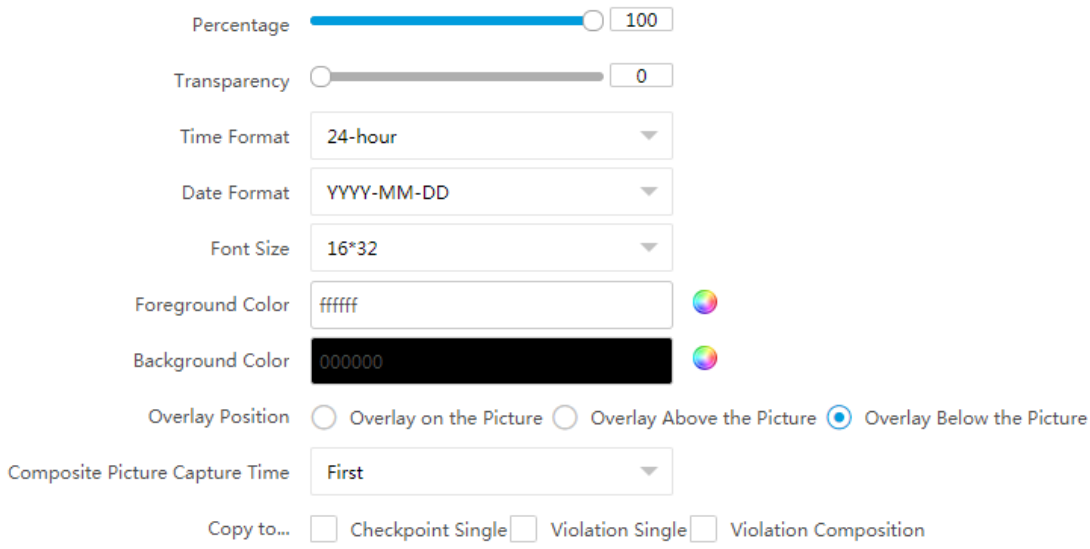


Figure 3-6 Set Composite Picture Overlay

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

   Percentage

   It is the percentage that the overlaid information occupies on the picture. For example, if you set the percentage to 50, the overlaid information in a row will occupy up to half of the image width, and the excess content will be overlaid from a new line.

   Transparency

   It is the condition of viewing the live view image through the overlaid information.

   Composite Picture Capture Time

   The capture time of the selected picture sequence will be overlaid on the composite picture.

5. **Optional:** Check the other channel(s) to copy the same settings.
6. Select the overlay information from the list.

   Note

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

7. Set the overlay information.

View Default Type	You can view the default overlay information.
Set Type	You can edit the type.
Set Overlay Information	For some information types, you can edit the detailed information.
Set Overlay Position	If you check it, the current information will be displayed from a new line.
Set Space	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.

Set Line Break Characters
Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.

Adjust overlay sequence
Click ^ / v to adjust the display sequence of the overlay information.

8. Click **Save**.

3.7 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 → Image Encoding and Composition → Image Encoding** .

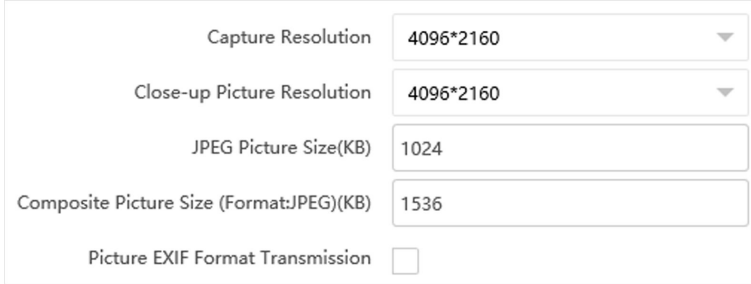


Figure 3-7 Set Image Encoding Parameters

2. Select **Capture Resolution**.
3. Select **Close-up Picture Resolution**.
4. Enter the picture size.

JPEG Picture Size

The size of the compressed captured picture. The actual size is related to the scene complexity.

Composite Picture Size

The size of the compressed composite picture. The actual size is related to the scene complexity.

Note

Only the device supporting picture composition supports composite picture size settings. The actual device prevails.

Picture EXIF Format Transmission

The captured pictures will be transmitted in the EXIF format.

5. Click **Save**.

3.8 Set Capture Schedule

You can set the schedule for the violation behavior capture or checkpoint capture if needed.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Capture Schedule** .
2. Click ✎ to set the capture schedule according to the actual needs.

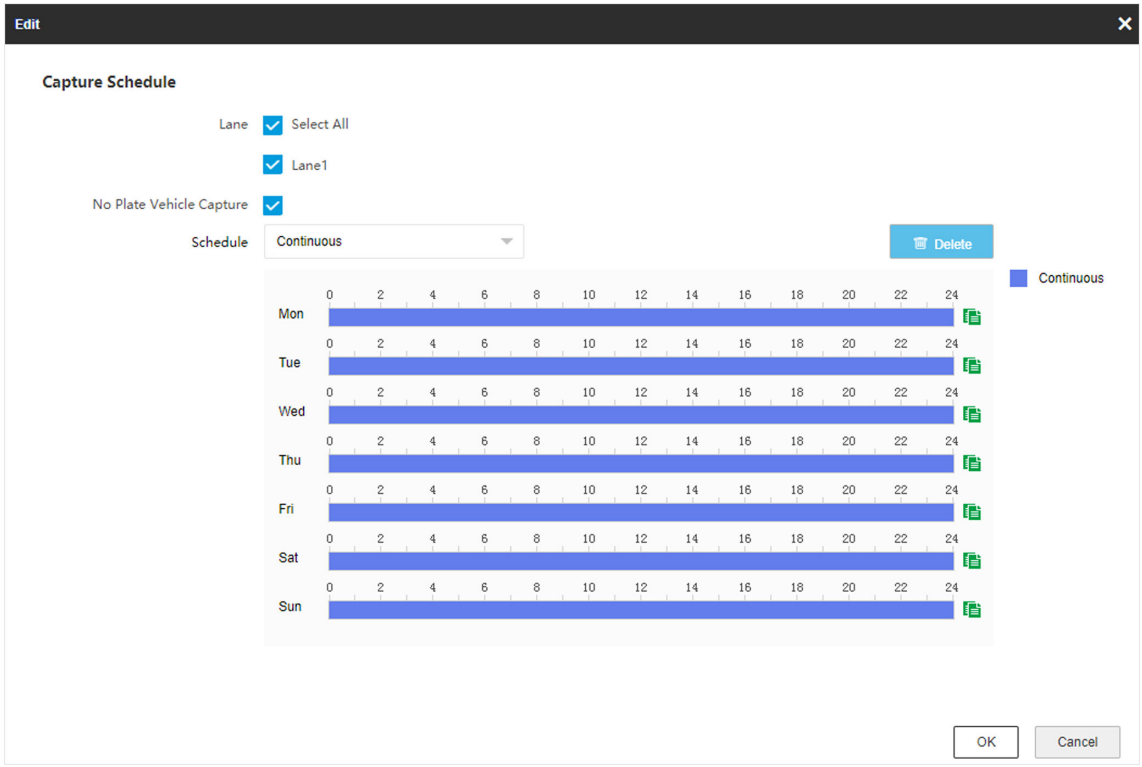


Figure 3-8 Set Capture Schedule

3. Select **Lane**.
4. **Optional:** Check **No Plate Vehicle Capture** according to the actual needs.
5. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
6. **Optional:** Click to copy the same settings to other days.
7. Click **OK**.
8. **Optional:** Check **Upload to Mailbox** to email the capture schedule to the user.
9. Click **Save**.

3.9 Set Captured Image Parameters

Set the parameters of captured images to raise the image quality.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Capture Images → Image Parameters** .

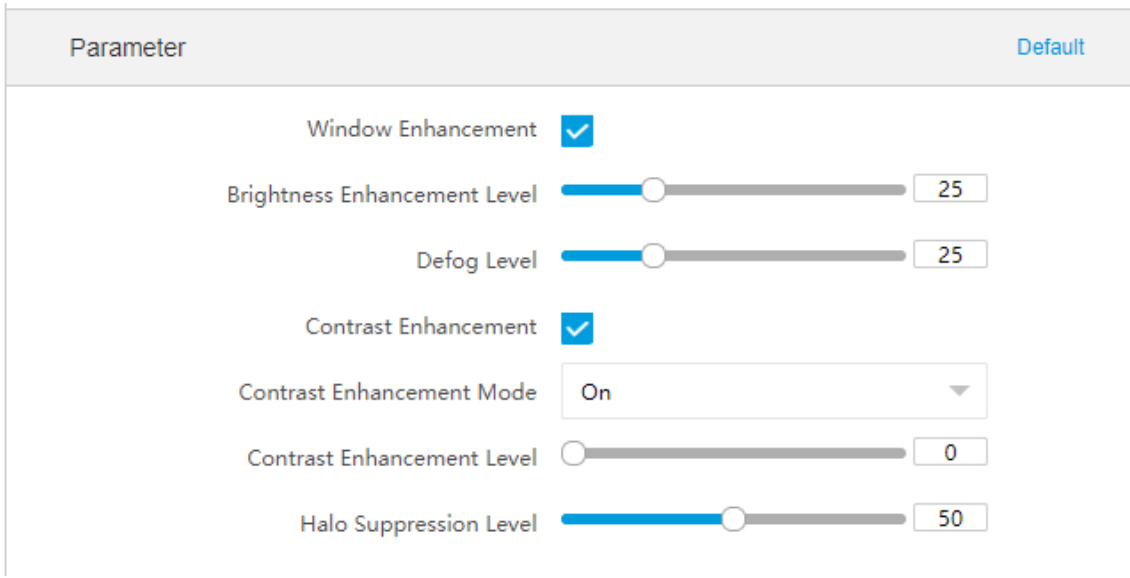


Figure 3-9 Set Captured Image Parameters

2. Set the captured image parameters.

Note

You can click **Default** to restore all the set parameters to the default settings.

Window Enhancement

In front light or back light scene, the flash light may not pass through the vehicle window, or the image effect of the window is bad caused by the light. In this condition, you can check **Window Enhancement**. The higher the **Brightness Enhancement Level** is, the brighter the window image is. The higher the **Defog Level** is, the better the permeability of the window image is.

Contrast Enhancement

Check **Contrast Enhancement** to capture clearer images. Select **Contrast Enhancement Mode**, and set corresponding parameters.

Contrast Enhancement Mode	Description
On	The contrast enhancement mode is always enabled.
Time	The contrast enhancement mode is enabled during the set start time and end time. In other time, it is disabled.
Brightness	The contrast enhancement mode is enabled according to the brightness of the surroundings. In this case, you can set **Brightness Level**.

Contrast Enhancement Level

The higher the level is, the more the contrast is enhanced.

Halo Suppression Level

Halo suppression is to suppress the halo of the vehicle headlights. The higher the level is, the more the halo is suppressed.

3.10 Set ICR

ICR adopts mechanical IR filter to filter IR in the day to guarantee the image effect, and to remove the IR filter at night to guarantee full-spectrum rays can get through the device.

Steps

Note

For the device supporting black and white mode at night, when the day-night mode is night, and **Black and White Mode at Night** has been enabled in **Configuration → Video → Camera Parameter → Camera Parameter → General Parameter** , the image displays as black and white. When **Black and White Mode at Night** is disabled, the image displays as color.

1. Go to **Configuration → Capture → Capture Images → ICR** .
2. Select **ICR Mode**.

Auto Switch	The ICR mode will switch to day or night mode automatically according to the surrounding light conditions. When the surrounding light is sufficient and higher than the set **Threshold**, the ICR mode will switch to day. When the surrounding light is insufficient and lower than the set **Threshold**, the ICR mode will switch to night.
Manual Switch	Select **Day-night Mode** to switch to the day or night manually.
Schedule Switch	Set **Day-night Mode**, **Start Time**, and **End Time** to switch to the day or night mode only during the set time period.

3. Click **Save**.

3.11 Debug

Note

The debug configurations below are only provided to debug the device by the professionals.

3.11.1 Debug Device

You can enable the functions to debug the device.

Steps

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

Note

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

Enable Algorithm POS Information Debug

The algorithm POS information will be overlaid on the playback image when you play back the video with the dedicated tool.

Enable Positioning Frame Debug

The positioning frames of vehicle bodies and license plates will be overlaid on the captured pictures.

Enable Closed Positioning Frame

The bottom lines of the positioning frames on the captured pictures will be displayed. The frames will be closed.

Enable LPR Area Frame

The LPR area frames on the captured pictures will be displayed.

Note

The function is only valid in the trigger modes of checkpoint single I/O and RS-485 radar, and manual capture. In these modes, the license plate may not be included in the LPR area, and the LPR rate is low. To solve the problem, you can enable the function to add a green frame on the captured picture to check whether the license plate is included in the LPR area.

LPR Area Frame Y-Direction Deviation

If the license plate is not included in the LPR area frame, adjust the LPR area frame position in the Y-direction by pixel. Enter the deviation pixel in the text field. The value = image height × (deviation distance/100). Set the value according to the actual needs. Range: -100% to 100%. The LPR area frame moves up if the value is negative, and it moves down if the value is positive.

Enable License Plate Frame

The license plate frames will be overlaid on the captured pictures.

Enable Multi-Way Upload

Data will be uploaded in multiple set ways simultaneously.

Enable Lane Line Debug

Check it to overlay lane lines on a captured picture.

3. Click **Save**.

3.11.2 Vehicle Capture and Recognition Service

Set the vehicle capture and recognition service to debug the device.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Vehicle Capture and Recognition Service** .
2. Click **Checkpoint Parameters** or **Violation Parameters** to set the corresponding parameters.
3. Check the service(s) according to your needs.

Note

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

Filter Checkpoint Capture of Same Vehicle

It is used to debug the device with the same vehicle. When the same vehicle is triggered many times during a short period in the scene, the checkpoint pictures of the vehicle will not be captured. Set **Effective Time of Filtering** to filter the vehicle during the set time.

Capture Frame Priority Mode

Check it to adopt license plate recognition results that processed by the single frame recognition algorithm.

Enable License Plate Supplementary Recognition

Check it and the device will enable license plate recognition algorithm again to re-recognize the unrecognized license plates.

Do Not Capture Reverse-driving Vehicle

The reverse-driving vehicles will not be captured. For example, if you need to capture the vehicles driven from the west to the east, enable the function and the vehicles driven from the east to the west will not be captured.

Enable SIRA Protocol

For the device supporting Middle East SIRA protocol, check it to enable the protocol. Then the license plates will be overlaid on the captured pictures according to the license plate types of the Middle East license plate recognition library.

Enable Video Electric Alarm Steering Flow

In video analysis E-police application mode, you can enable the function to make statistics about the traffic flow of left turn and right turn at the intersection and upload the statistics data to the connected platform.

Enable Non-Motor Vehicle Flow Statistics

Check it to enable the non-motor vehicle flow statistics.

Enable Statistics Integral Upload

The device will upload data at every integral minute according to the set time interval under the collection mode. For example, if the set time interval is 2, the device will upload data at 8:00:00, 8:02:00, 8:04:00, etc.

Filter Two-Wheelers Without License

Check it to not capture the two-wheelers without license plates.

Enable ANR

Enable ANR (Automatic Network Replenishment) to save the videos in the condition of network disconnection, and synchronize data after the network is recovered.

Add No. After Violation Type

The No. of the captured pictures will be added after the overlaid violation type on the pictures.

Filter Violation Capture of Motorcycle

The violation pictures of motorcycles will not be captured.

Disable Non-Motor Vehicle Speed Detection

The speeds of non-motor vehicles will not be detected.

VCA Alarm for Target Picture Matting

If target picture matting is enabled, the alarms will be triggered and the matted target pictures will be uploaded via VCA protocol.

4. Click **Save**.

3.11.3 Set Image Format

You can enable smartJPEG which can save the storage space without influencing the resolution.

Steps

1. Go to **Configuration → Capture → Advanced → Image Service** .
2. Check **smartJPEG**.
3. Set image quality according to your needs.

Note

The higher the value is, the better the image quality is.

4. **Optional:** Set **Expansion Ratio of License Plate Image** to expand the cutout scale of license plate image.
5. Click **Save**.

3.12 Set Barrier Gate Linkage

If a barrier gate has been connected to the device, you can link barrier gate to realize the control and management of the vehicles at the entrance or exit.

Note

The function is only supported for the application modes of smart mode and license plate recognition system. The actual device prevails.

3.12.1 Set Allowlist and Blocklist

Set allowlist and blocklist if you want to control the passing vehicles at the entrance or exit via the barrier gate.

Before You Start

- Connect the barrier gate to the relay output interface of the device.
- Install the storage card, and ensure the storage status is normal.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Allowlist and Blocklist** .
2. Add an allowlist or blocklist.
   1) Click **Add**.
   2) Set **License Plate Number** and **Card No.**, and select the list type.
   3) **Optional:** If you want to control allowlist vehicles during fixed time period, enable **Time Settings**, and set the effective start time and end time.
   4) Click **OK**.

   Note

   Wait for 15 minutes to let the added allowlist or blocklist write into the storage. Do not reboot the device during the process.

   The information of the added vehicles in the allowlist or blocklist will be listed below.

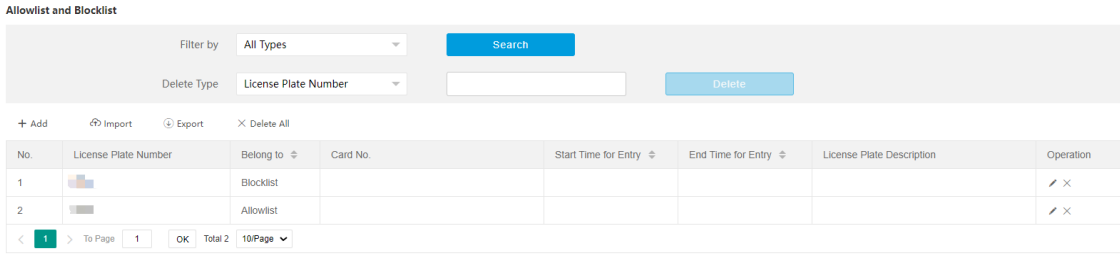


Figure 3-10 Set Allowlist and Blocklist

3. You can search, modify, delete, import, or export the allowlist and blocklist.

Search Select the search type, or enter the keywords. Click **Search**. The searched vehicle information will be listed below.

Modify Select an item from the list, and click . Modify the information, and click **OK**.

Delete
- Select the delete type, or enter the keywords. Click **Delete** to delete the lists of the same type.
- Select an item from the list, and click × to delete the item.
- Click **Delete All** to delete all the lists.

Import
a. Click **Import**.
b. Click **Download Template**, and save the template.
c. Open the template, edit the information, and save it.
d. Click **Import** again.
e. Click **Browse** to select the edited template.
f. Click **Import** to import the information to the device.

Export Click **Export** and select the saving path to export the allowlist or blocklist to the computer.

3.12.2 Control Barrier Gate

Link the barrier gate to realize the control and management of the vehicles at the entrance or exit.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Barrier Gate** .

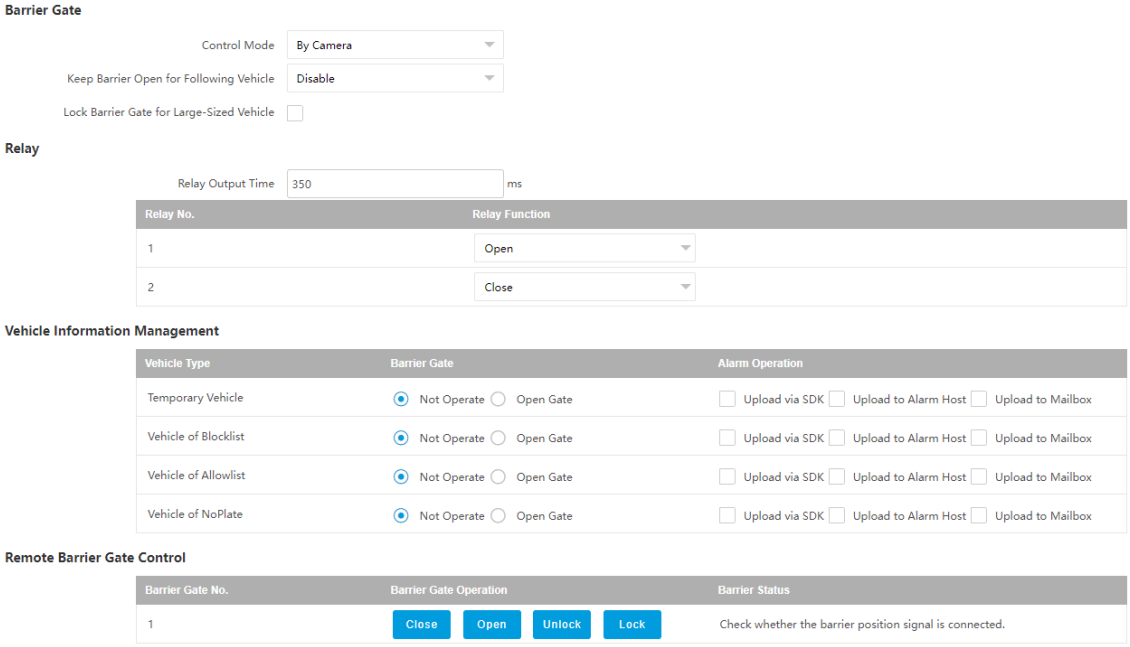


Figure 3-11 Control Barrier Gate

2. Set **Barrier Gate** parameters.

   Control Mode

   - Select **By Camera** in single camera scene (no control software) and allowlist scene in which the camera controls the barrier gate in advance according to the set passing rules in **Vehicle Information Management**.
   - Select **By Platform** in the scene in which the entry permissions are controlled by the software.
   - Select **By Mixed**, and the platform control and camera control are effective simultaneously. It is applicable to the scene in which different vehicle passing permissions are managed by software and camera. E.g., the software controls the passing of blocklist vehicles and temporary vehicles, and the camera controls the passing of allowlist vehicles and controls the barrier gate in advance for allowlist vehicles.

   Keep Barrier Open for Following Vehicle

   After you enable this function, the barrier gate keeps open when the device detects following vehicles are passing. The barrier gate will close after the following vehicles pass.

   Lock Barrier Gate for Large-Sized Vehicle

   Enable the function and set **Barrier Gate Rising Time**. If a large-sized vehicle is passing, the barrier gate will be locked during the set time.

3. Set the relay function.

Note

The supported number of relays varies with different models. Relay 1 corresponds to the 1A and 1B of the terminal. Relay 2 corresponds to the 2A and 2B of the terminal.

4. Set the barrier gate operation and alarm operation for the temporary vehicles, vehicles of the blocklist, vehicles of the allowlist, and vehicles without license plates.
   - Check **Upload via SDK** to arm and upload the vehicle information to the arming terminal via SDK.
   - If the device has been connected to the alarm device, check **Upload to Alarm Host**. When the barrier gate is open, the alarm device will be triggered to alarm.
   - Check **Upload to Mailbox** to email the vehicle information to the user.
5. **Optional:** You can click **Close**, **Open**, **Unlock**, or **Lock** to control the barrier gate remotely.

Note

The functions of remote control of barrier gate vary with different models. The actual device prevails.

6. Click **Save**.

3.12.3 Set Wiegand Parameters

The device can get access to the access control system or other system supporting Wiegand protocols to send data in the entrance and exit scenes.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Wiegand Parameters** .
2. Check **Enable**.

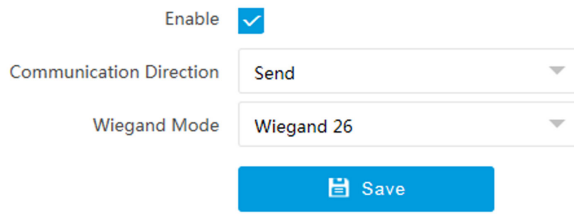


Figure 3-12 Set Wiegand Parameters

3. Select **Communication Direction**.

   Send

   The barrier gate can be connected to the device via Wiegand 26 or Wiegand 34 mode.
4. Select **Wiegand Mode**.

   Wiegand 26

   It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 8 digits) from the allowlist and blocklist related to the captured

license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 26 protocol.

Wiegand 34

It is applicable to all the access control projects. The device will get the card No. (pure numbers with no more than 10 digits) from the allowlist and blocklist related to the captured license plate number and send the card No. to the access control system or other system supporting Wiegand protocols via Wiegand 34 protocol.

5. Click **Save**.

Chapter 4 View Real-Time Picture

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

Steps

Note

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

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.

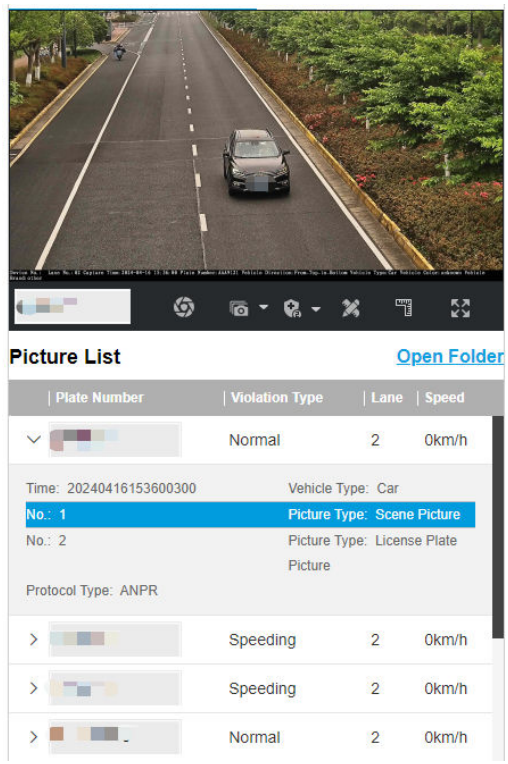


Figure 4-1 Real-Time Capture

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 View Traffic Statistics

5.1 View Real-Time Traffic Statistics

You can view the real-time traffic statistics if the device supports this function.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Traffic Parameters → Traffic Parameters** .
2. Check **Enable**.
3. Set **Interval**.
4. Go to **Live View → Traffic Statistics** to view real-time data.

5.2 View Traffic Flow Statistics

The device supports counting and uploading traffic follow data.

Steps

Note

This function varies with different models. The actual device prevails.

1. Go to **Configuration → Capture → Advanced → Traffic Parameters → TPS Parameters** .
2. Check **Enable**.
3. Set **Interval**.
4. Click **Save**.

Chapter 6 Live View and Local Configuration

6.1 Live View

6.1.1 Start/Stop Live View

Click ▶ to start live view. Click ■ to stop live view.

6.1.2 Select Image Display Mode

Click to select an image display mode.

6.1.3 Select Window Division Mode

Click to select a window division mode.

6.1.4 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 custom.

Note

The third stream varies with different models. The actual device prevails.

6.1.5 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 → Live View Parameters** and select **Image Format**.
3. **Optional:** Click **Configuration → Local → Picture and Clip Settings** to view the saving path of snapshots in live view.

6.1.6 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.

6.1.7 Start/Stop Two-Way Audio

The device supports two-way audio with terminals, such as computers.

Before You Start

The device is equipped with an audio input interface and audio output interface, which support connecting with the corresponding devices, such as microphones and loudspeakers.

Steps

Note

The function varies with different models. The actual device prevails.

1. Select a window to start two-way audio.
2. Click to start live view.
3. Click to start two-way audio.

   When speaking at the PC end, you can hear the voice at the device end and vice versa.
4. Click to stop two-way audio.

6.1.8 Enable/Disable Audio

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

Note

The function varies with different models. The actual device prevails.

6.1.9 Enable Digital Zoom

You can enable digital zoom to zoom in a certain part of the live view image.

Steps

1. Click to start live view.
2. Click to enable digital zoom.
3. Place the cursor on the live view image position which needs to be zoomed in. Drag the mouse rightwards and downwards to draw an area.

The area will be zoomed in.

4. Click any position of the image to restore to normal image.
5. Click to disable digital zoom.

6.1.10 Enable Regional Focus

Steps

Note

The function varies with different models. The actual device prevails.

1. Click .
2. Drag the cursor from the upper left corner to the lower right corner to select the area that needs to be focused.

Result

The selected area is focused.

6.1.11 Select Video Mode

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

Click and select when the device is running normally.

6.2 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.

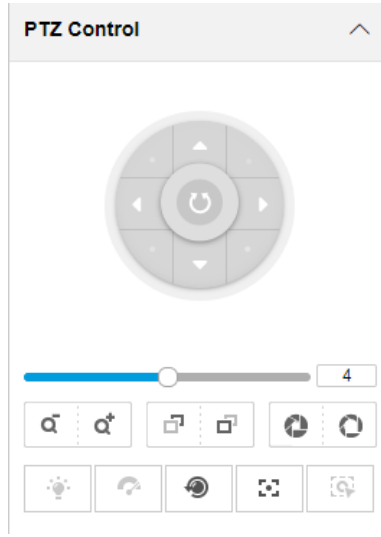


Figure 6-1 PTZ Control Panel

Table 6-1 Button Description

Button	Description
4	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.

6.3 Local Configuration

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

Note

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

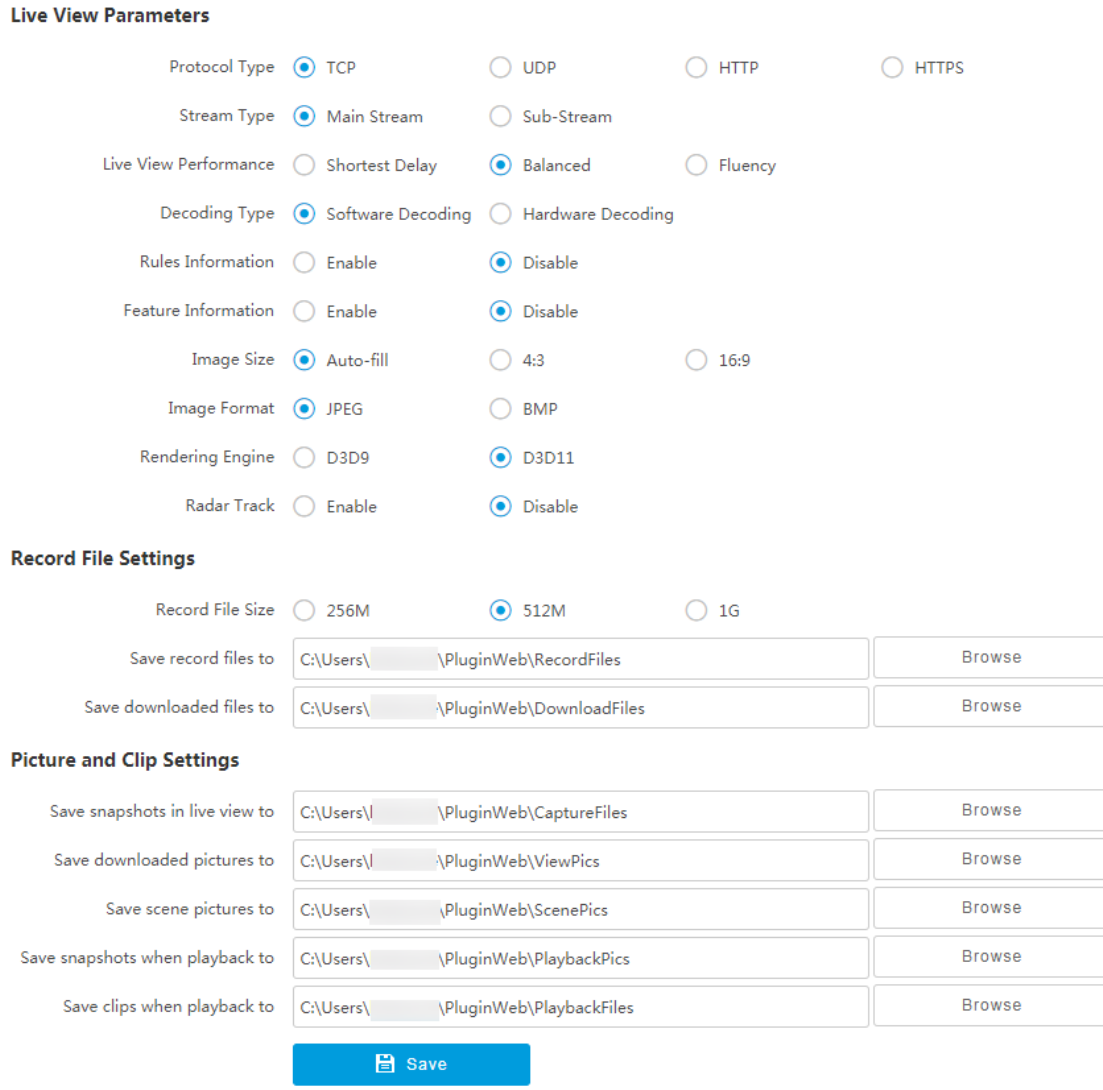


Figure 6-2 Local Configuration

Protocol Type

Select the network transmission protocol according to the actual needs.

TCP

Ensures complete delivery of streaming data and better video quality, but 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 this function, 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 on the live view image.

Image Size

The display ratio of the live view image.

Image Format

The saving format of manually captured images.

Rendering Engine

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

Radar Track

When the radar is connected, enable it to generate and overlay the radar tracks.

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 of the manually recorded video files.

Save downloaded files to

Set the saving path of the download files.

Save snapshots in live view to

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

Save downloaded pictures to

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

Save clips when playback to

Set the saving path of the clips in playback mode.

Chapter 7 Record and Capture

7.1 Set Storage Path

7.1.1 Set Storage Card

If you want to store the files to the storage card, make sure you insert and format the storage card in advance.

Before You Start
Insert the storage card to the device.

Steps
1. Go to **Configuration → Storage → Storage Management → HDD Management → HDD Storage** .

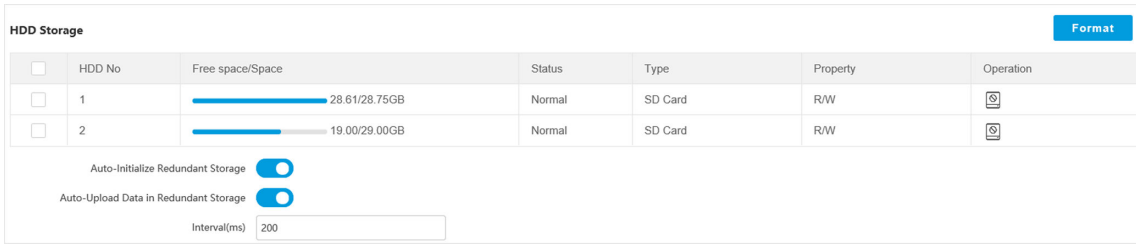


Figure 7-1 Set Storage Card

2. Format the storage card in two ways.
   - Check the storage card, and click **Format** to format it manually.

     Note

     For the newly installed storage card, you need to format it manually before using it normally.
   - If you want to format the storage card automatically when the card is abnormal, enable **Auto-Initialize Redundant Storage**.

     Note

     If you enable **Auto-Initialize Redundant Storage**, reboot the device to take the settings into effect.
3. **Optional:** If the device has been connected to the platform, and you want to upload the storage card information automatically, enable **Auto-Upload Data in Redundant Storage** and set the interval.
4. Click **Save**.

7.1.2 Set Quota

Set the video and picture ratio in the storage.

Before You Start
Install the storage card.

Steps
1. Go to **Configuration → Storage → Storage Management → HDD Management → HDD Quota** .

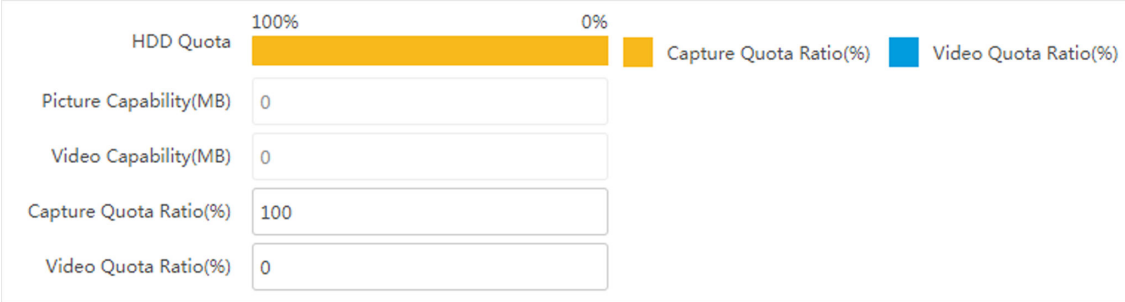


Figure 7-2 Set Quota

2. Set **Capture Quota Ratio** and **Video Quota Ratio** according to the actual needs.

Note
The percentage sum of the capture and video quota ratio should be 100 %.

3. Click **Save**.

What to do next
Format the storage card after the settings.

7.1.3 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** .

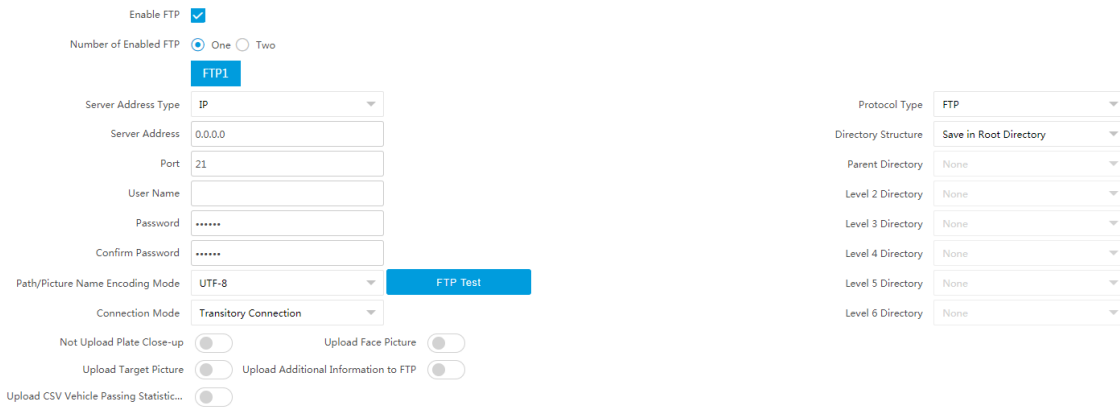


Figure 7-3 Set FTP

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

Note

You can only enable one FTP if the device does not support the violation capture. If more than one FTP is enabled, you should set upload data type for each FTP according to your needs.

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

Note

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

   5) Select **Directory Structure**.

Note

You can customize the directory structure according to your needs.

   6) Select **Path/Picture Name Encoding Mode**.

UTF-8

UNICODE encoding.

   7) Select **Connection Mode**.

Transitory Connection

The connection is temporarily made for one data transmission task. After this task, the connection will be broken.

Persistent Connection

The connection is made for long-term data transmission, which will be broken only when the device is disconnected from the FTP server.

5. **Optional:** Enable upload functions.

Note

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 Face Picture

Upload face close-up pictures to the FTP server.

Upload Target Picture

Upload the pictures of the target detection area to the FTP server.

Upload Additional Information to FTP

Add related information when uploading data to the FTP server.

Upload CSV Vehicle Passing Statistics Information to FTP

Upload the CSV vehicle passing statistics information to the FTP server.

6. **Optional:** Click **FTP Test** to check the FTP server.
7. Set naming rules and separators according to the actual needs.

Note

For the European version, select **Custom** and enter ***adr*** or ***ADR*** in the text field, and the ADR (Autorisation Dangerous Road) vehicle plate number will be added in the corresponding vehicle picture name.

8. **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.
9. Click **Save**.

7.1.4 Set Cloud Storage

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

Before You Start

- Arrange the cloud storage server.
- You have enabled level 1 arming in **Live View → Real-Time Capture** .

Note

The real-time capture should be used with dedicated platform.

Steps

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

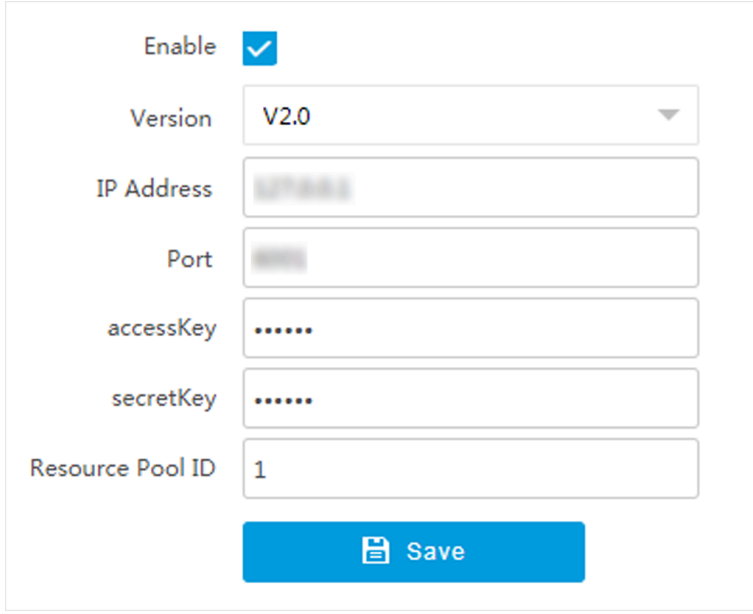


Figure 7-4 Set Cloud Storage

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**.

7.2 Set Record Schedule

Set record schedule to record video automatically during configured time periods.

Before You Start
Install the storage card.

Steps
1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. **Optional:** Enable the functions below according to your needs.

Enable Recording Overwriting

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

Enable Storing Expiration

Enable the function and set **Expired Time** for the recorded videos stored in the storage card. Beyond the time, the files will be overwritten.

3. Enable the record schedule.

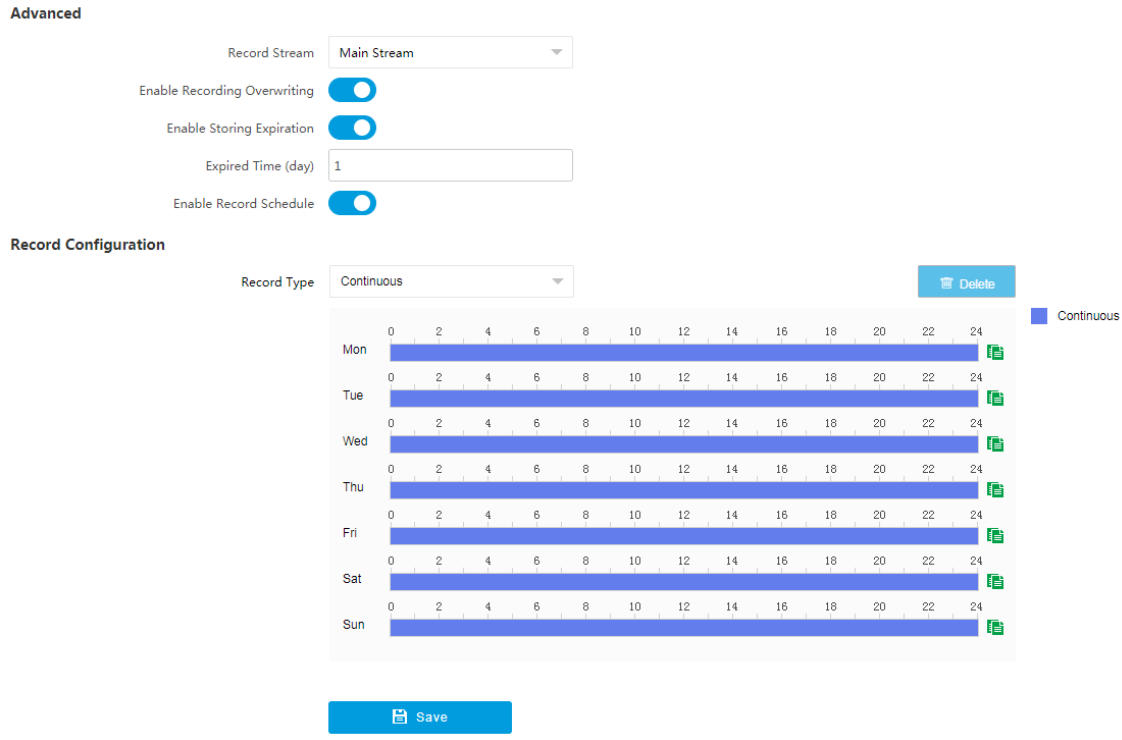


Figure 7-5 Set Record Schedule

4. Select **Record Type**.
5. Drag the cursor on the time bar to set a recording time.

Note

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

6. Adjust the recording time.
   - Click a set recording period and enter the start time and end time in the pop-up window.
   - Drag two ends of the set recording period bar to adjust the length.
   - Drag the whole set recording period bar and relocate it.
7. **Optional:** Delete recording periods.
   - Click a set recording period and click **Delete** in the pop-up window.
   - Click a set recording period and click **Delete** on the record configuration interface.
8. **Optional:** Click to copy set recordings to other days.
9. Click **Save**.

Result

The device will only record at the set periods.

7.3 Set Snapshot Schedule

You can enable storage expiration of the snapshots saved in the storage card.

Before You Start
Install the storage card.

Steps
1. Go to **Configuration → Storage → Schedule Settings → Snapshot Schedule** .

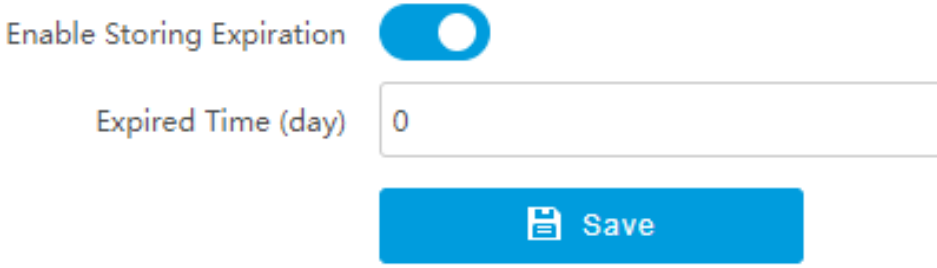


Figure 7-6 Set Snapshot Schedule

2. Enable storing expiration.
3. Set **Expired Time**.
4. Click **Save**.

Result

Beyond the set expired time, the snapshots saved in the storage card will be overwritten.

7.4 Search Picture

You can search the captured pictures stored in the storage card and export the pictures you need.

Before You Start
Install the storage card, and ensure the storage status is normal.

Steps
1. Click **Picture**.
2. Set search conditions.

Note

Search conditions vary with different models. The actual device prevails.

3. Click **Search**.

   The searched pictures information will be displayed in the picture list.

   Note

   If you have set level 1 arming for the device, the captured pictures will not be saved in the storage card. Go to the saving path of scene pictures to view them. You can go to **Configuration → Local** to check the saving path.

4. **Optional:** Check picture(s) and click **Download** to save them to local.

   The downloaded picture(s) will be marked as "Downloaded". You can go to **Configuration → Local** to check the saving path.

7.5 Playback

You can search, play back, and download videos that stored on the storage card.

Steps

1. Click **Playback**.
2. Select a channel.
3. Select a date.
4. Click **Search**.
5. Click ▶ to start playback.
6. **Optional:** You can also do the following operations.

Set playback time	• Drag the time bar to the target time and click ▶ to play the video. • Click the current time point showed above the time bar and enter the target time point in the popup window. Click **OK** and click ▶ to play the video.
Capture image	Click 📷 to capture an image.
Clip record	Click ✂ / ✂ to start/stop clipping the record.
Play back in single frame	Click ⏭ once to play back the video in one frame.
Download record	a. Click ⬇ . b. Select the start time and end time. c. Click **Search**. d. Check record files that need to be downloaded. e. Click **Download**.
Stop playback	Click ■ to stop playback.
Slow forward	Click « to slow down the playback.
Fast forward	Click » to speed up the playback.
Digital zoom	Click 🔍 to enable digital zoom.

	Click  to disable digital zoom.
Adjust volume	Click  to enable volume.

Chapter 8 Encoding and Display

8.1 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**.

8.2 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** .

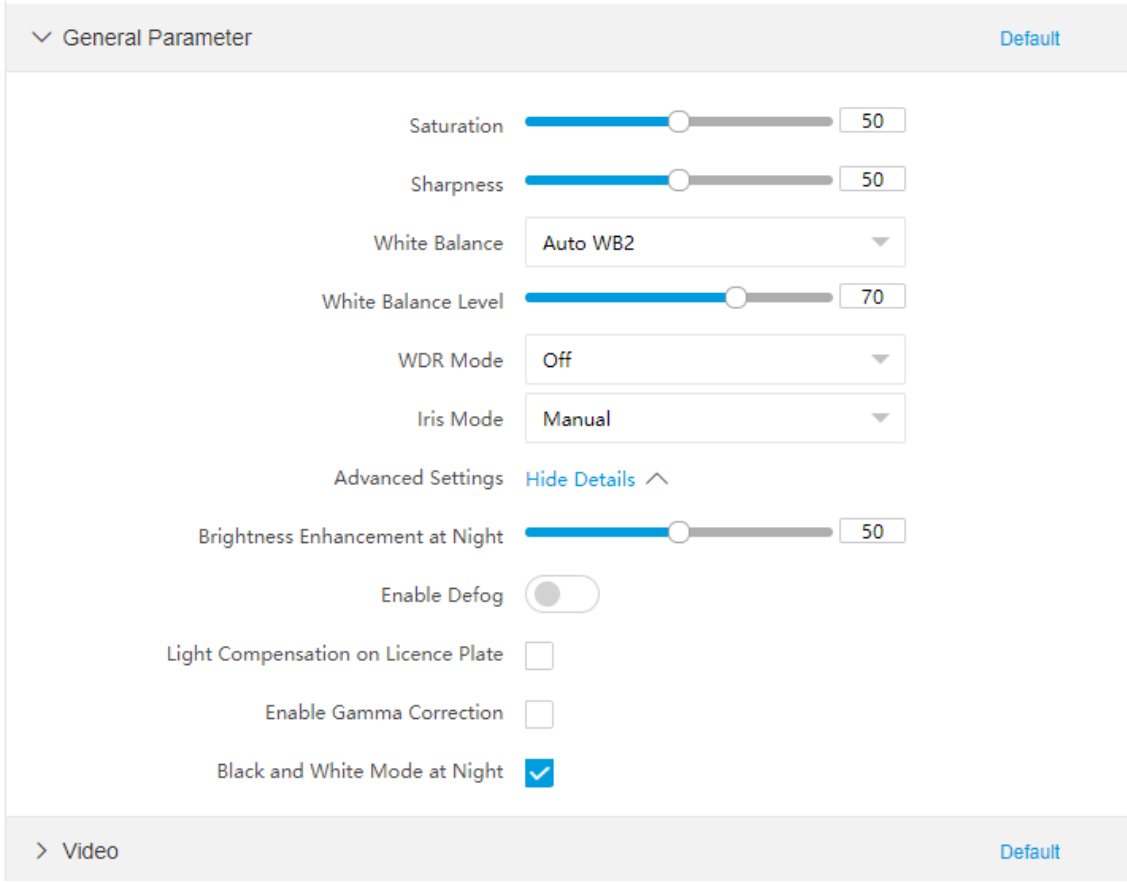


Figure 8-1 Set Image Parameters

2. Set the camera parameters.

Note

- The supported parameters vary with different models. The actual device prevails.
- You can click **Default** to restore the parameters to default settings.

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.

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 set time period and level.

Brightness

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

Iris Mode

Select the iris mode according to your needs.

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 plate brightness compensation 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.

Black and White Mode at Night

When ICR is in night mode, you can check it to keep the video in black and white mode at night.

Video

Brightness

It refers to the brightness 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 space domain intensity is too high, the outline of the image may become fuzzy and the details may lose. If the time domain 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.

Slow Shutter

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure. The higher **Slow Shutter Level** is, the slower the shutter speed is.

Video Standard

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

3. **Optional:** You can click under the live view image to enable digital zoom. Refer to ***Enable Digital Zoom*** for details.
4. **Optional:** Click **Capture Test** to check the image effect.

8.3 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** .

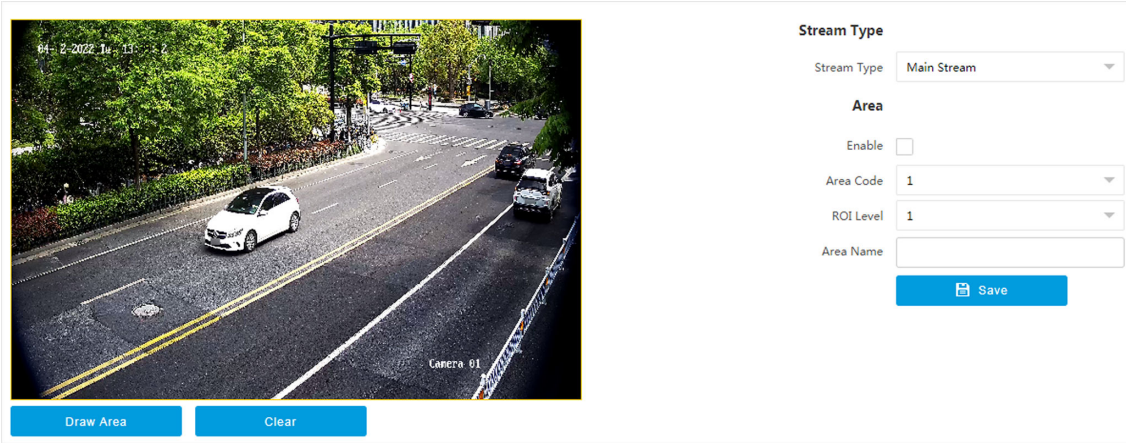


Figure 8-2 Set ROI

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.

8.4 Set Privacy Mask

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

Steps

1. Go to **Configuration → Video → Video Encoding → Privacy Mask** .

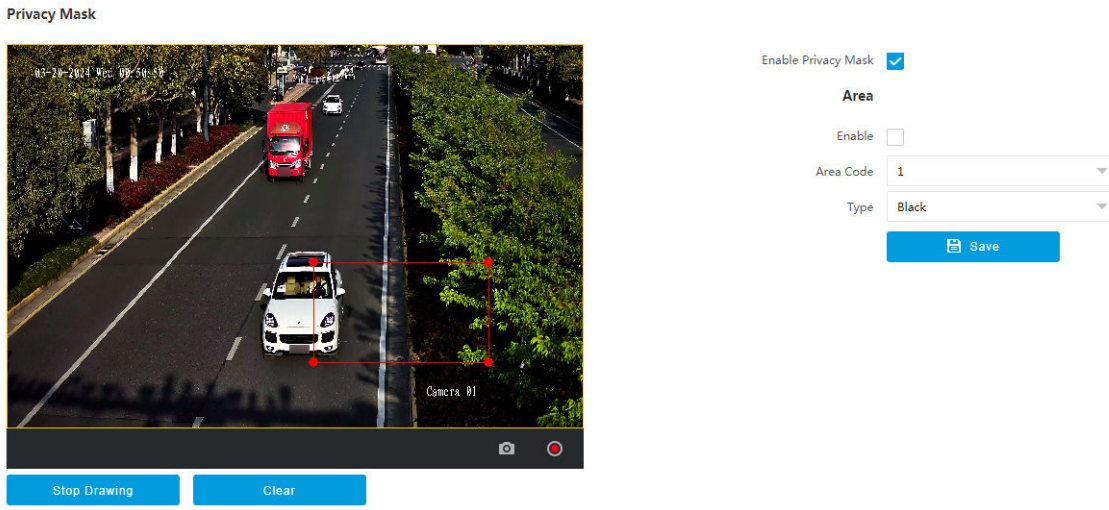


Figure 8-3 Set Privacy Mask

2. Check **Enable Privacy Mask**.
3. Enable the privacy mask area(s).
   1) Check **Enable**.
   2) Select **Area Code**.
   3) Select **Type**.
4. Draw the privacy mask area.
   1) Click **Draw Area**.
   2) In the live view image, drag the mouse to draw the privacy mask area of the selected area code.
   3) Click **Stop Drawing**.
   4) **Optional:** Click **Clear** to clear all the drawn areas.
5. **Optional:** Repeat step 3 and 4 to draw more privacy mask areas.

Note

Up to four privacy mask areas are supported.

6. Click **Save**.

8.5 Enable Regional Exposure

Enable regional exposure to adjust the brightness of the whole live view image according to the drawn partial area.

Steps

1. Go to **Configuration → Video → Video Encoding → BLC** .
2. Check **Enable**.
3. Drag the mouse to draw an area.

The brightness of the whole live view image will be adjusted according to the drawn area.

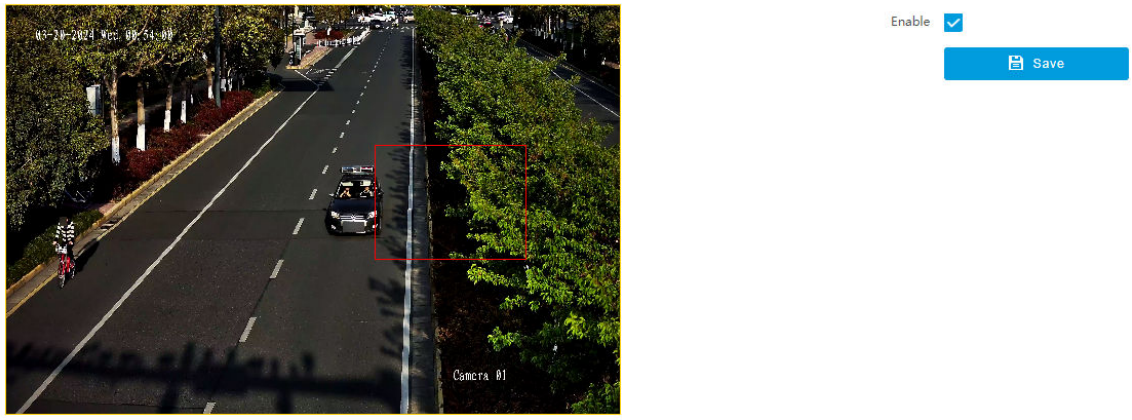


Figure 8-4 Enable Regional Exposure

4. Click **Save**.

8.6 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.

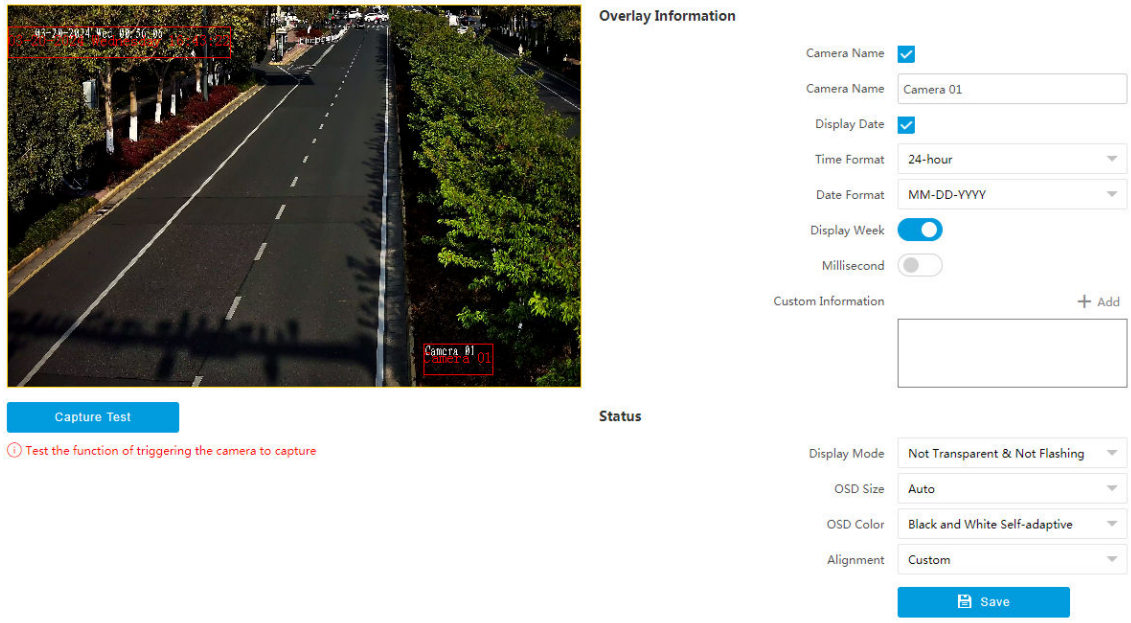


Figure 8-5 Set OSD

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

Note

Up to 6 items of custom information can be added.

4. Set display properties (size, color, etc.).
5. Select **Alignment**.

Note

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

6. Drag the red frames on the live view image to adjust their positions.
7. Click **Save**.

Result

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

Chapter 9 Network Configuration

9.1 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** .

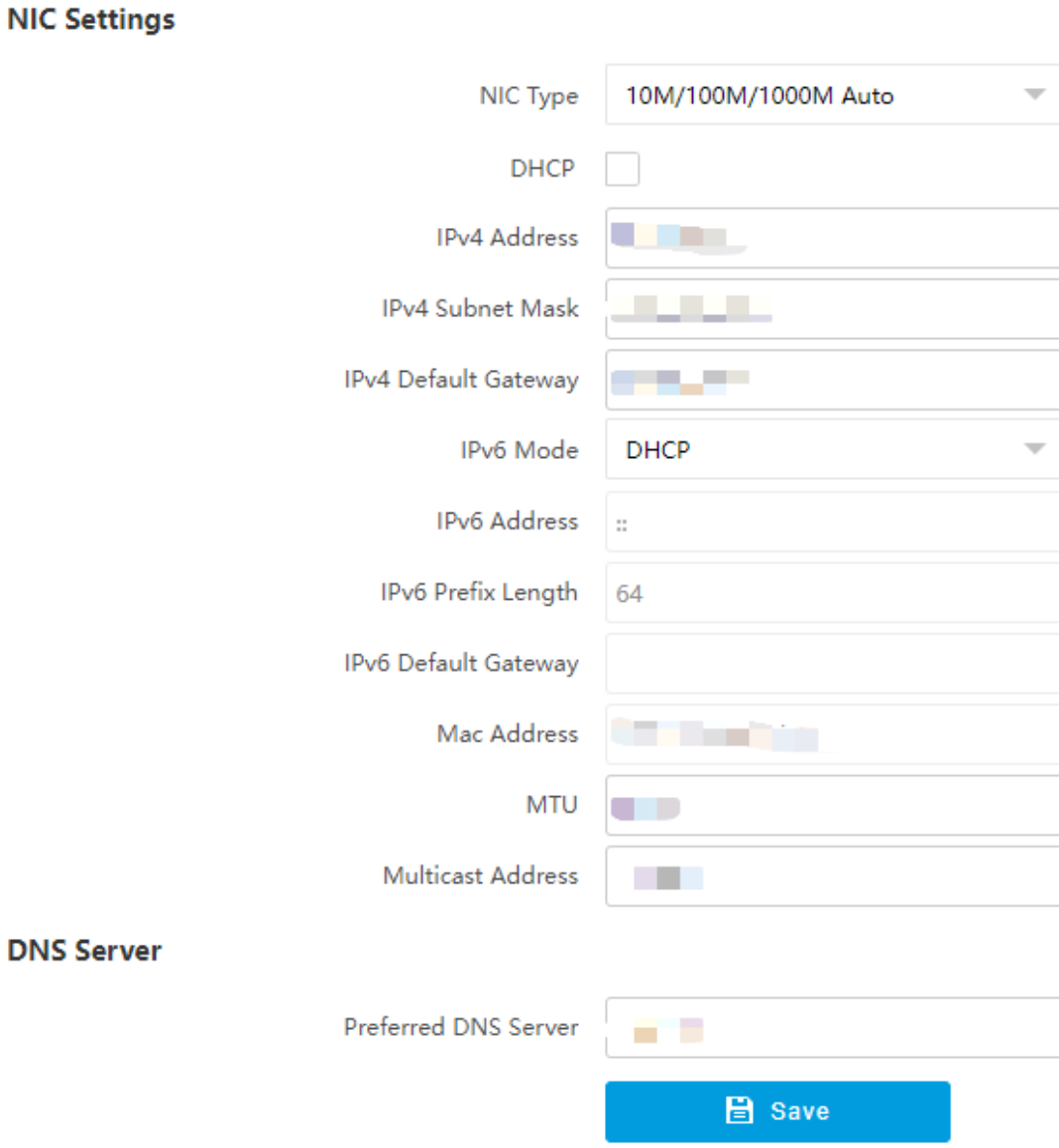


Figure 9-1 Set IP Address

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 Default 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

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**.

9.2 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.

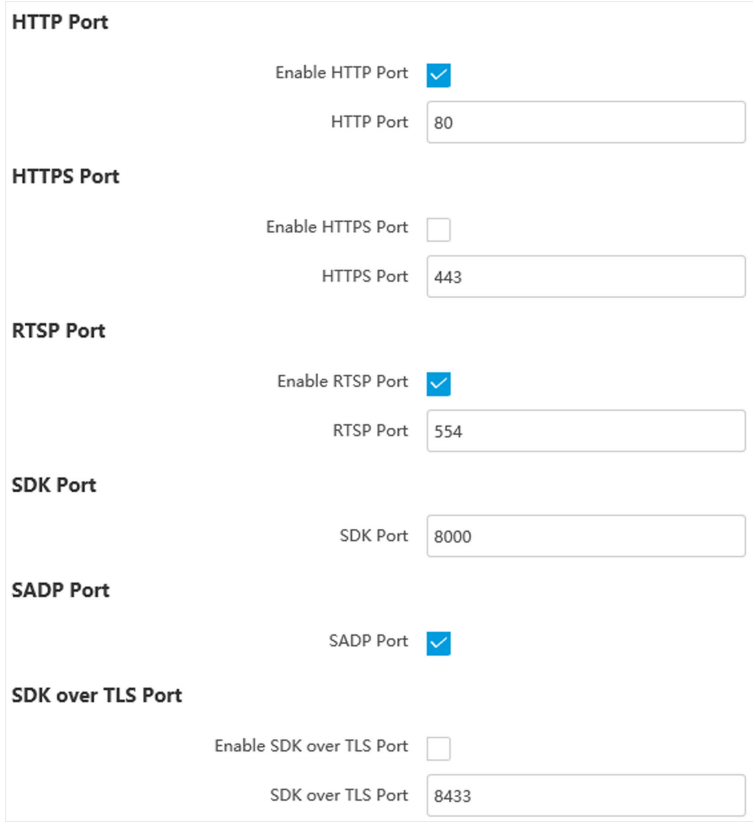


Figure 9-2 Set Port

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

It refers to the port through which the browser accesses the device, but certificate verification is needed.

RTSP Port

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

SDK 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.

SDK over TLS Port

It refers to the port that adopts TLS protocol over the SDK service, to provide safer data transmission.

Note

- After editing the port, access to the device via the new port.
- Reboot the device to bring the new settings into effect.
- The supported ports vary with different models. The actual device prevails.

9.3 Set IEEE 802.1X

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN/WLAN. When devices connect to the network with IEEE 802.1X standard, the authentication is needed.

Steps

1. Go to **Configuration → Network → Network Parameters → 802.1X** .

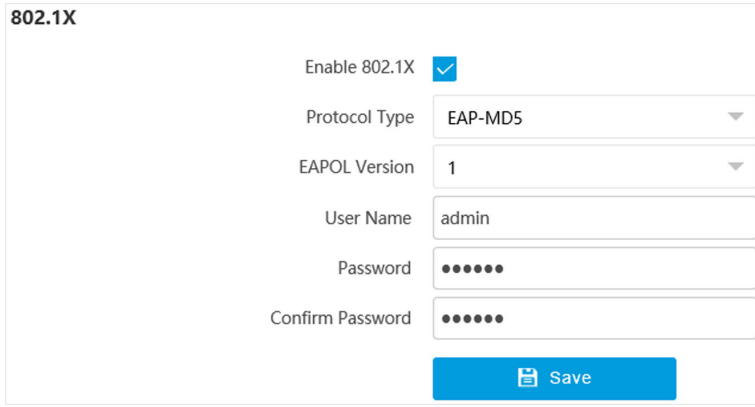


Figure 9-3 Set IEEE 802.1X

2. Check **Enable 802.1X**.
3. Select **Protocol Type** and **EAPOL Version**.

   Protocol Type

   The authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Enter the user name and password for authentication.

   EAPOL Version

   The EAPOL version must be identical with that of the router or the switch.
4. Enter **User Name** and **Password** registered in the server.
5. Confirm the password.
6. Click **Save**.

9.4 Set DDNS

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

Before You Start

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

Steps

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

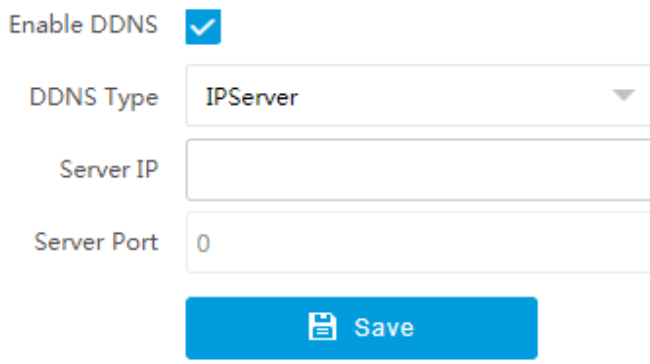


Figure 9-4 Set DDNS

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

Note

You can select **IPServer**, **DynDNS**, and **NO-IP** for the DDNS type.

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.

9.5 Set SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Download the SNMP software and manage to receive the device information via SNMP port.

Steps

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

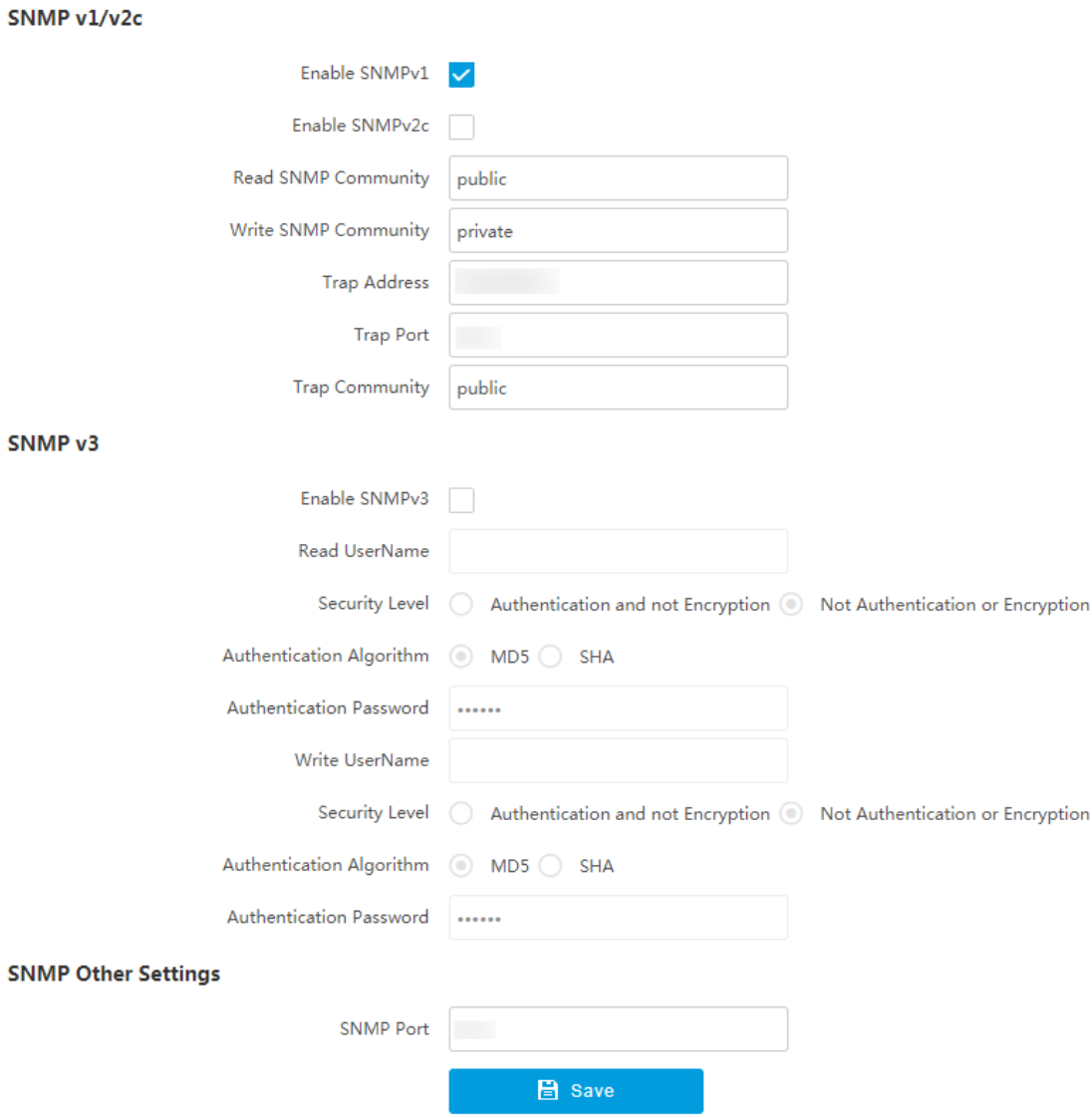


Figure 9-5 Set SNMP

2. Check **Enable SNMPv1/Enable SNMP v2c/Enable SNMPv3**.

Note

- The SNMP version you select should be the same as that of the SNMP software.
- Use different versions according to the security levels required. SNMP v1 is not secure and SNMP v2 requires password for access. SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Set the SNMP parameters.
4. Click **Save**.

9.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network devices such as routers and switches.

Steps

1. Go to **Configuration → Network → Network Parameters → QoS** .
2. Enable DSCP according to the actual needs and set the value.

   Note

   Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. Same settings need to be set in the router for configuration.

3. Click **Save**.

9.7 Connect to Platform

9.7.1 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** .

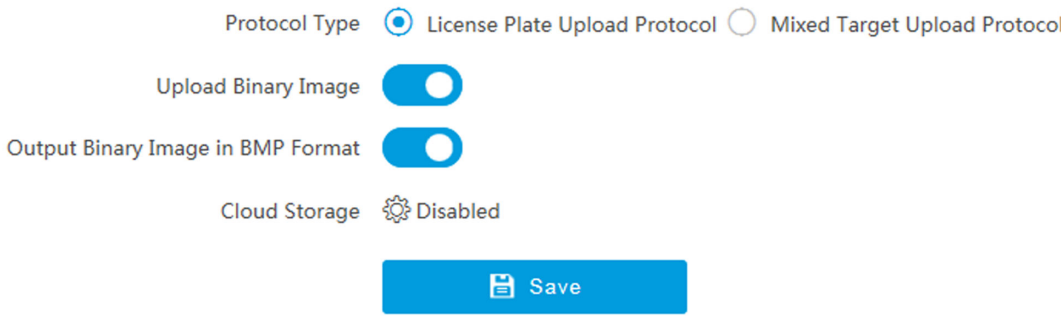


Figure 9-6 Set Arm Host

2. Select **Protocol Type**.

Note

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

License Plate Upload Protocol

Uploads arming alarm images of the license plate. You can enable **Upload Binary Image** if you need to upload binary images full of black or white pixel points. Enable **Output Binary Image in BMP Format** if you want to output images in this format.

Mixed Target Upload Protocol

Uploads images of multiple targets such as humans and vehicles. You can enable the body property to recognize clothes, bags, and other properties.

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**.

9.7.2 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** .

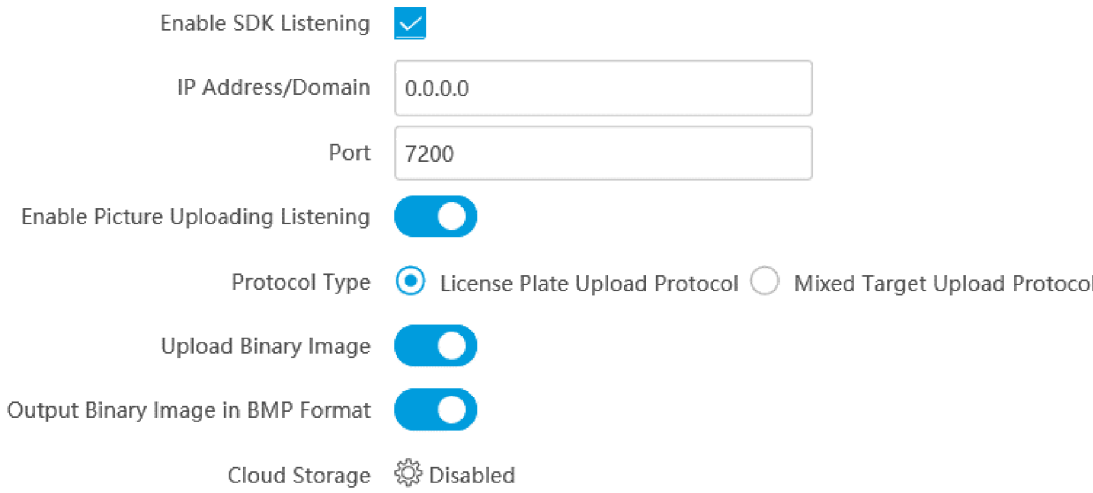


Figure 9-7 Set SDK Listening

2. Enable SDK listening.
3. Set **IP Address/Domain** and **Port** if you need to upload the alarm information and pictures.
4. **Optional:** The device will transmit images via the SDK listening if you enable the picture uploading listening.
5. Select **Protocol Type**.

Note

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

License Plate Upload Protocol

Uploads arming alarm images of the license plate. You can enable **Upload Binary Image** if you need to upload images which are full of black or white pixel points. Enable **Output Binary Image in BMP Format** if you want to output images in this format.

Mixed Target Upload Protocol

Uploads images of multiple targets such as humans and vehicles. You can enable the body property to recognize clothes, bags, and other properties.

6. **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.
7. Click **Save**.

9.7.3 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** .
2. Enable the ISAPI listening.

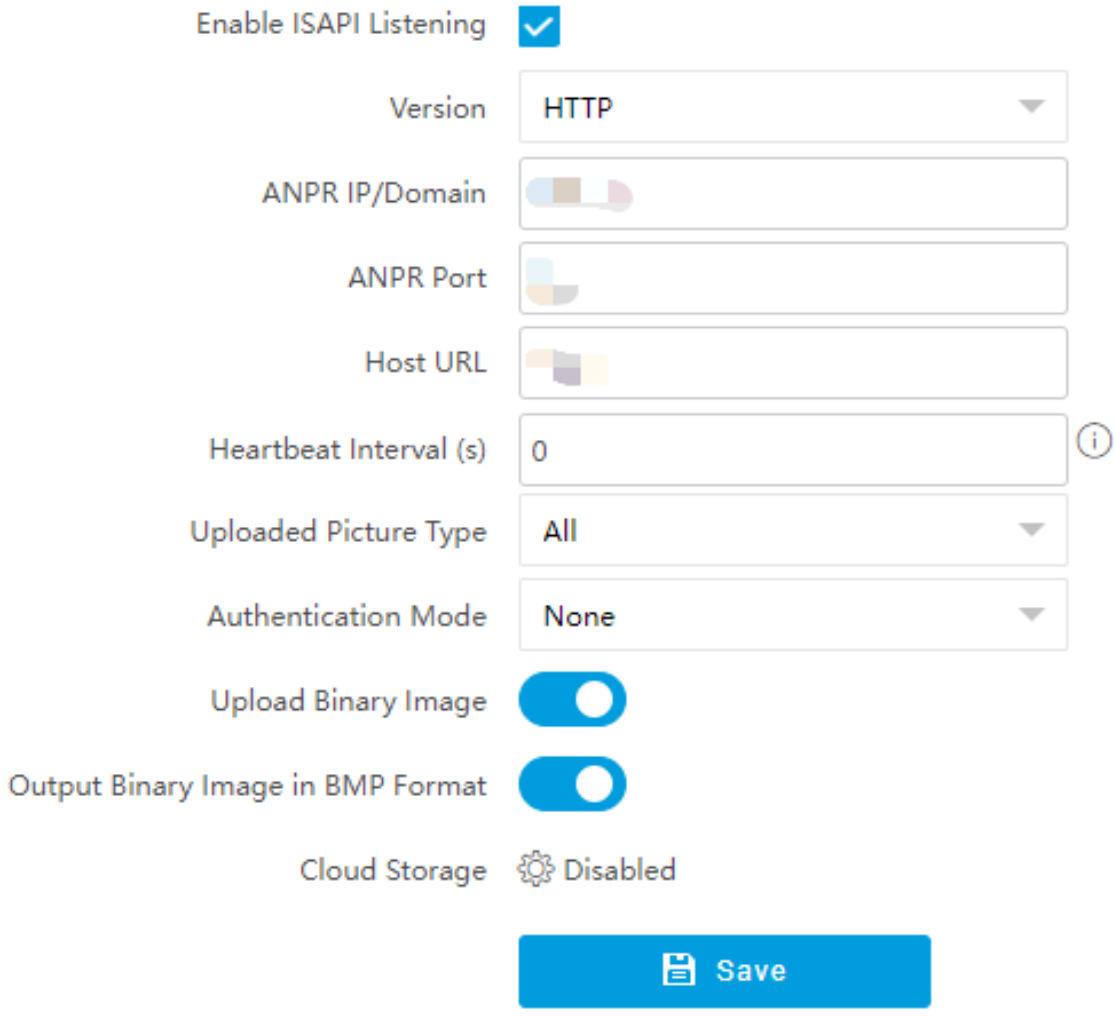


Figure 9-8 Set ISAPI Listening

3. Set **ANPR IP/Domain**, **ANPR Port**, and **Host URL**.
4. Enter **Heartbeat Interval**.

Note

If you set it as 0, the heartbeat is disabled.

5. Set **Uploaded Picture Type**.

6. Select **Authentication Mode** and set corresponding parameters to guarantee that only the authorized users can access the device.

Note

If you select **None**, the device will not verify the authentication condition of the access users. It is recommended to select an authentication mode to guarantee the device information security.

7. **Optional:** Enable **Upload Binary Image** if you need to upload images which are full of black or white pixel points.

Note

Enable **Output Binary Image in BMP Format** if you want to output images in this format.

8. **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.
9. Click **Save**.

9.7.4 Connect to ISUP Platform

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

Before You Start

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

Steps

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

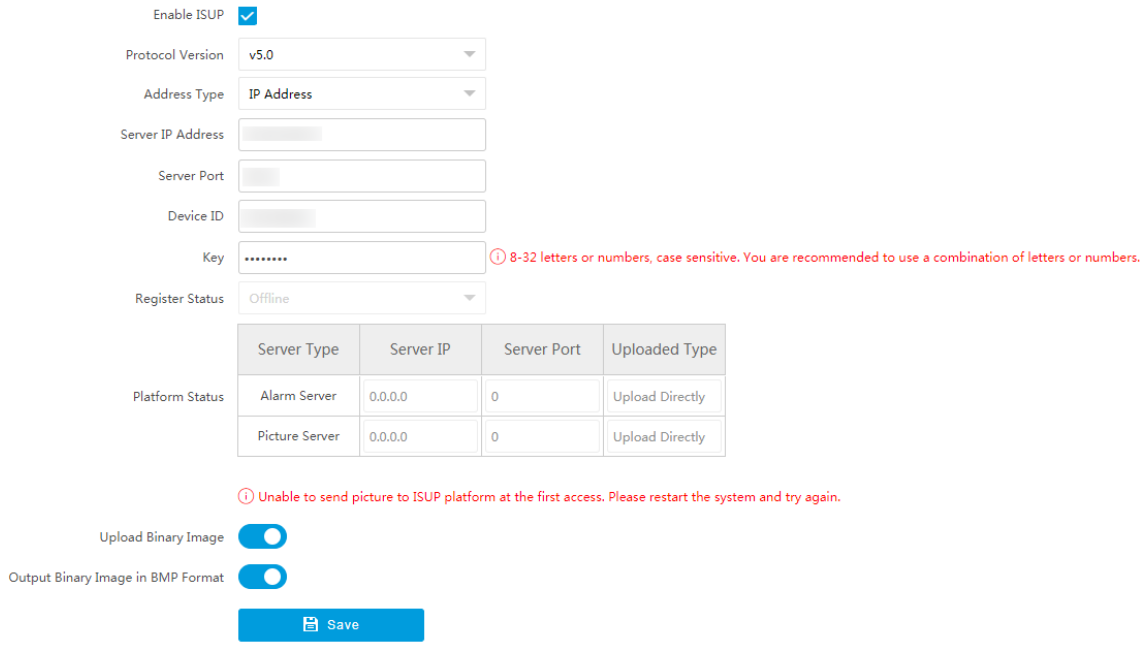


Figure 9-9 Connect to ISUP Platform

2. Check **Enable ISUP**.
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. **Optional:** For protocol **v5.0**, you can enable **Upload Binary Image** if you need to upload images which are full of black or white pixel points.

Note

Enable **Output Binary Image in BMP Format** if you want to output images in this format.

7. Click **Save**.

What to do next

When the registration status is online, you can manage the device via the platform or server.

9.7.5 Connect to OTAP

The device can be accessed to the ISC platform via OTAP protocol to realize live view, view incident information, manage the devices, etc. via the platform.

Before You Start

- Ensure the device can communicate with the platform normally.
- Disable the other platform accesses conflicting with OTAP.

Steps

1. Go to **Configuration → Network → Data Connection → OTAP** .
2. Select **Platform Access Mode** as **Private Deployment**.
3. Check **Enable**.

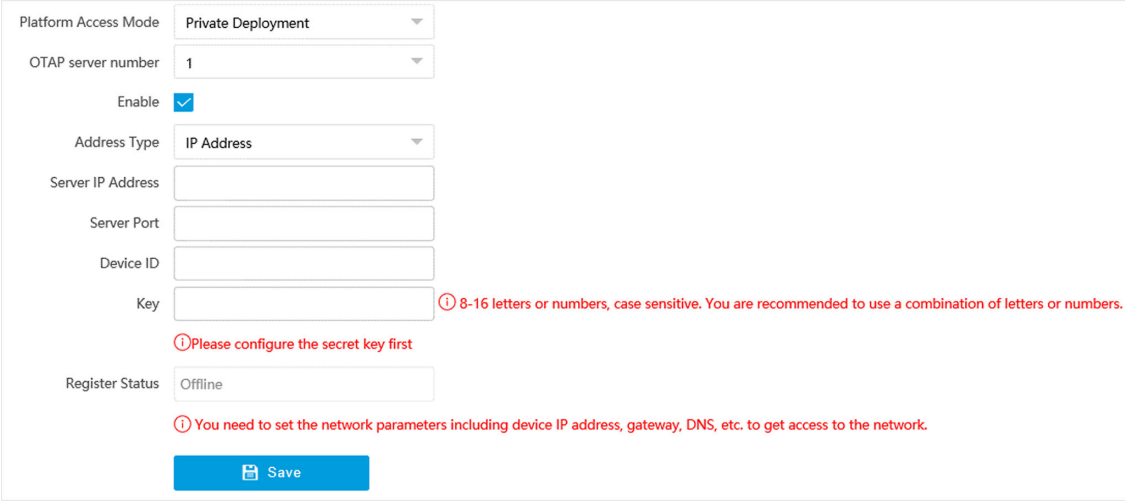


Figure 9-10 Connect to OTAP

4. Set corresponding parameters.

   Address Type

   Select the address type of the connected platform or server.

   Server IP Address/Server Domain Name

   The IP address or domain name of the connected platform or server.

   Server Port

   The port of the connected platform or server.

   Device ID

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

   Key

   Set a custom key to encrypt the data connection between the device and the platform or server.

5. Click **Save**.

What to do next

When the registration status is online, you can manage the device via the platform or server.

9.7.6 Connect to Hik-Connect

The device can be remotely accessed via Hik-Connect.

Before You Start

- Connect the device to the Internet.
- Set the IP address, subnet mask, gateway, and DNS server of the LAN.

Steps

Note

This function varies with different models. The actual device prevails.

1. Enable Hik-Connect in two ways.
   - Get access to Hik-Connect V2.0. Go to **Configuration → Network → Data Connection → OTAP** , and select **Platform Access Mode** as **Hik-Connect**. Check **Enable**.

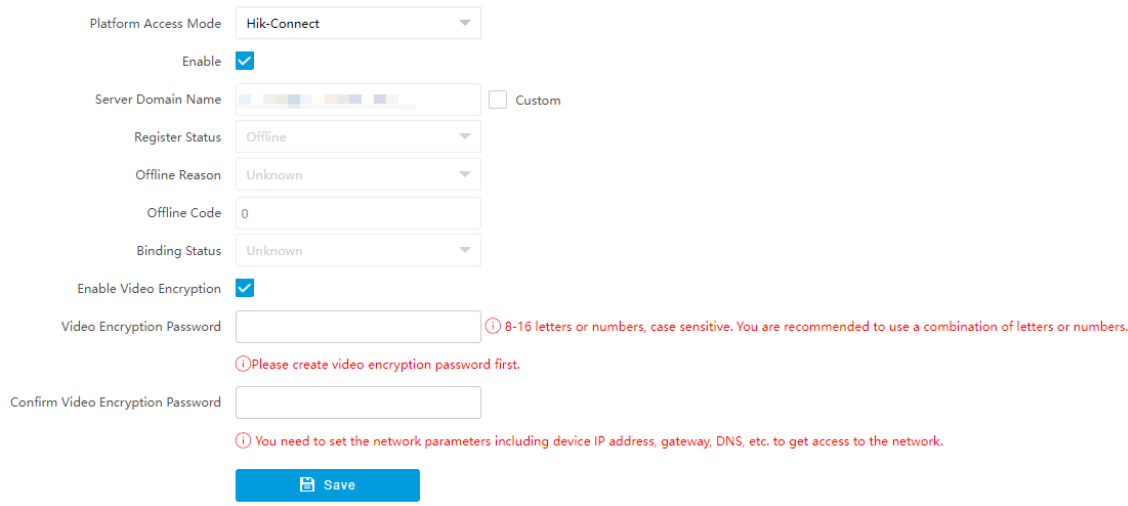


Figure 9-11 Connect to Hik-Connect (V2.0)

   - Get access to Hik-Connect V3.0. Go to **Configuration → Network → Data Connection → Hik-Connect Platform** . Check **Enable Hik-Connect Platform**.

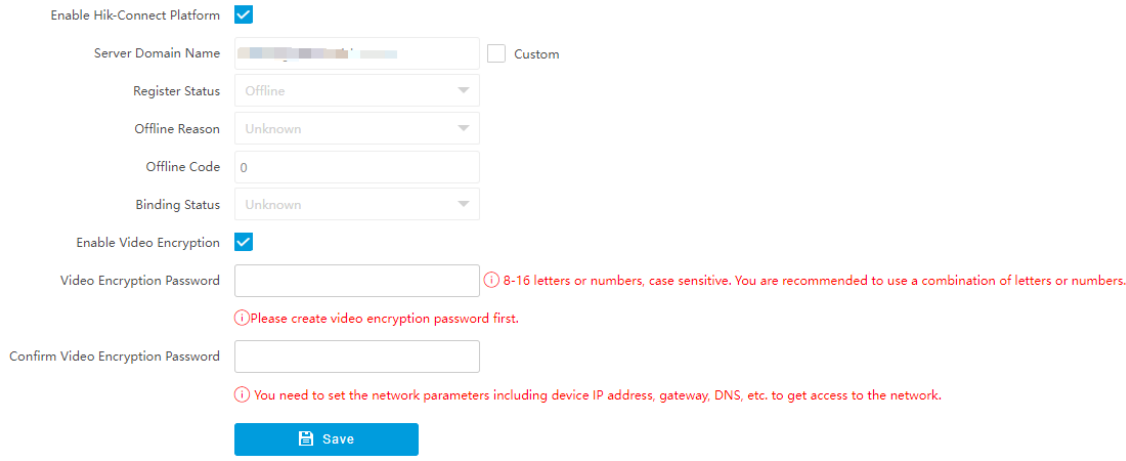


Figure 9-12 Connect to Hik-Connect (V3.0)

2. **Optional:** If you have allocated a custom server, check **Custom** and enter the custom **Server Domain Name**.
3. **Optional:** Check **Enable Video Encryption** and set **Video Encryption Password** to encrypt the videos transmission. Confirm the password.
4. Click **Save**.
5. Add the device to Hik-Connect.
   1) Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Figure 9-13 Hik-Connect

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

   2) Start the application and register a user account to log in.

3) Add device by the serial No. on the device body and the verification code.

Note

Refer to the user manual of Hik-Connect application for details.

9.8 Set Integration Protocol

You can connect the device via ONVIF protocol.

Steps

1. Go to **Configuration → Network → Data Connection → Integration Protocol** .
2. Check **Enable**.
3. Add a user.
   1) Click **Add**.
   2) Set user name, password, and user level, and confirm the password.
   3) Click **OK**.
   4) **Optional:** You can select the added user and click **Modify** to edit the user information, or click **Delete** to delete the user.
4. Click **Save**.

Result

Only the added users can access the device via ONVIF protocol.

Chapter 10 Serial Port Configuration

10.1 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** .

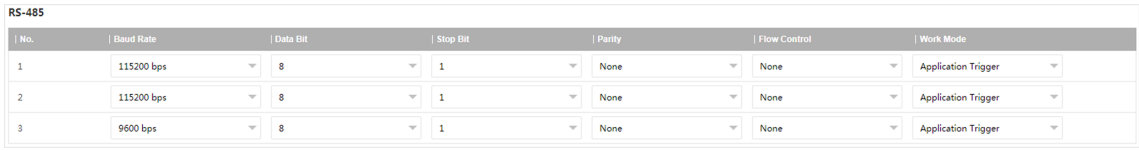


Figure 10-1 Set RS-485

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**.

Note

- The supported work modes vary with different models. The actual device prevails.
- You need to reboot the device after editing the work mode to take effect.

Application Trigger

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

Transparent Channel

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

GPS

Select it when a GPS device is connected to the RS-485 serial port of the device to receive positioning information.

Traffic Signal Controller Mode

Select it when a traffic signal controller is connected to the RS-485 serial port of the device for communication transmission.

4. Click **Save**.

10.2 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** .

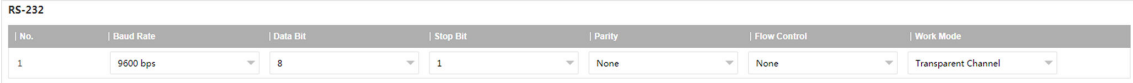


Figure 10-2 Set RS-232

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**.

Note

- The supported work modes vary with different models. The actual device prevails.
- You need to reboot the device after editing the work mode to take effect.

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 11 Event and Alarm

11.1 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**.

11.2 Set Email

When the email is enabled and set, the device will send an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the email function. Go to **Configuration → Network → Network Parameters → Network Interface** for DNS settings.

Steps

1. Go to **Configuration → Network → Data Connection → Email** .
2. Check **Enable Email**.

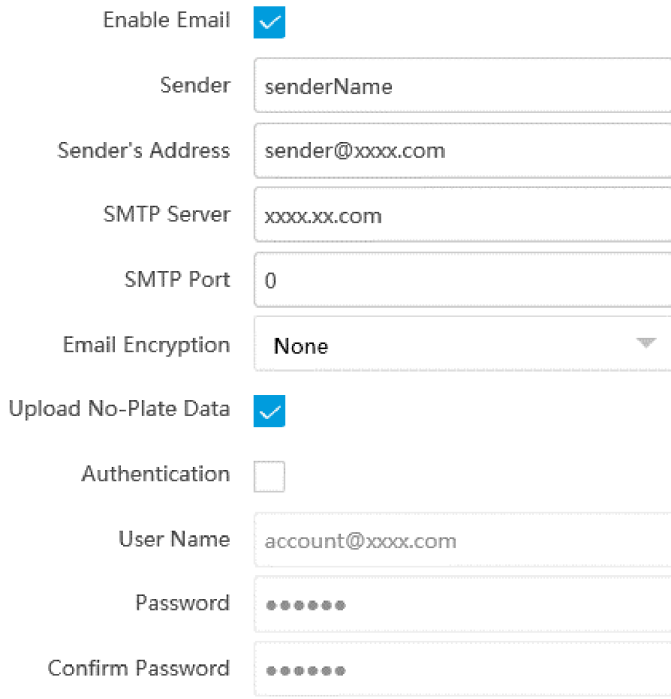


Figure 11-1 Set Email

3. Set email parameters.
   1) Enter the sender's email information, including **Sender**, **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) Select **Email Encryption**.

      None

      Emails are sent without encryption.

      TLS

      Emails are sent after being encrypted by TLS.
   3) **Optional:** If you want to upload no-plate data, check **Upload No-Plate Data**.
   4) **Optional:** If your email server requires authentication, check **Authentication** and enter your user name and password to log in to the server.
   5) Enter the receiver's information, including the receiver's name and address.
   6) **Optional:** Click **Test** to see if the function is well configured.
4. Click **Save**.

11.3 Set Email Event

When the set event occurs, the device can be set to send an email with alarm information to the user.

Before You Start

The email has been enabled and related email parameters have been configured.

Steps

1. Go to **Configuration → Event → Alarm Linkage → Email Event** .
2. Check **Enable** to trigger an email alarm.
3. Click **Save**.

Chapter 12 Safety Management

12.1 Manage User

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

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.

12.2 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. Check **Enable User Lock**.

3. Click **Save**.

Result

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

12.3 Set SSH

To raise network security, you are recommended to 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. Enable or disable **SSH Service**, and set **SSH Port** if you enable the function.
3. Click **Save**.

12.4 Prohibit PING

You can prohibit the external devices to operate network connection volume test to the current device.

Steps

1. Go to **Configuration → System → Security → Security Service → Software**
2. Enable **Prohibit PING**.
3. Click **Save**.

12.5 Enable System Log Service

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

Steps

1. Go to **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.

12.6 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.

12.7 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**.

12.8 Set SDK Protocol Authentication Mode

When you need to operate development integration or data collection via SDK protocol, you are recommended to enable SDK protocol authentication to enhance the information security.

Steps

1. Go to **Configuration → System → Security → Security Service → SDK Service Module** .
2. Select **SDK Protocol Authentication Mode**.

Note

You are recommended to select **Safety Mode**. In this mode, the device cannot be logged in via an invertible password of SDK protocol, which can enhance the information security.

3. Click **Save**.

12.9 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.
3. Click **Save**.

12.10 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**.

12.11 Set HTTPS

12.11.1 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.

12.11.2 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**.

Chapter 13 Maintenance

13.1 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.

13.2 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**.

Satellite Time

Select it to synchronize the device time with that of the satellite. Set **Interval**.

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.

PTP

Select it to synchronize time more accurately. Precision Time Protocol (PTP) is a protocol to synchronize clocks in a computer network, similar to NTP. NTP is accurate, under ten milliseconds. PTP, however, is accurate up to less than a microsecond and is measured in nanoseconds.

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**.

13.3 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**.

13.4 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.

13.5 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 select the parameters to be saved instead of being restored. Click **OK**. Then the parameters except the IP parameters, user parameters, and the saved parameters will be restored to the default settings.
   - Click **Restore Factory Settings** and click **OK** to restore all the parameters to the factory settings.
3. Click **OK**.

13.6 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**.

13.7 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**.

13.8 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**.

13.9 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.

13.10 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

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.

13.11 Log

13.11.1 Enable Log According to Module

You can enable the log according to the module for debugging.

Steps

Note

The function varies with different models. The actual device prevails.

1. Go to **Configuration → System → Maintenance → Debug → Log** .
2. Check the module(s) according to your needs.

Note

If you want to disable the log automatically, you can enable auto close log and set close time.

3. Click **Save**.

13.11.2 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.

13.12 Enable Maintenance Service

If you want to realize remote camera maintenance and debug via the platform server, enable maintenance service and set the access mode.

Steps

1. Go to **Configuration → System → Maintenance → Maintenance Service** .
2. Enable maintenance service.

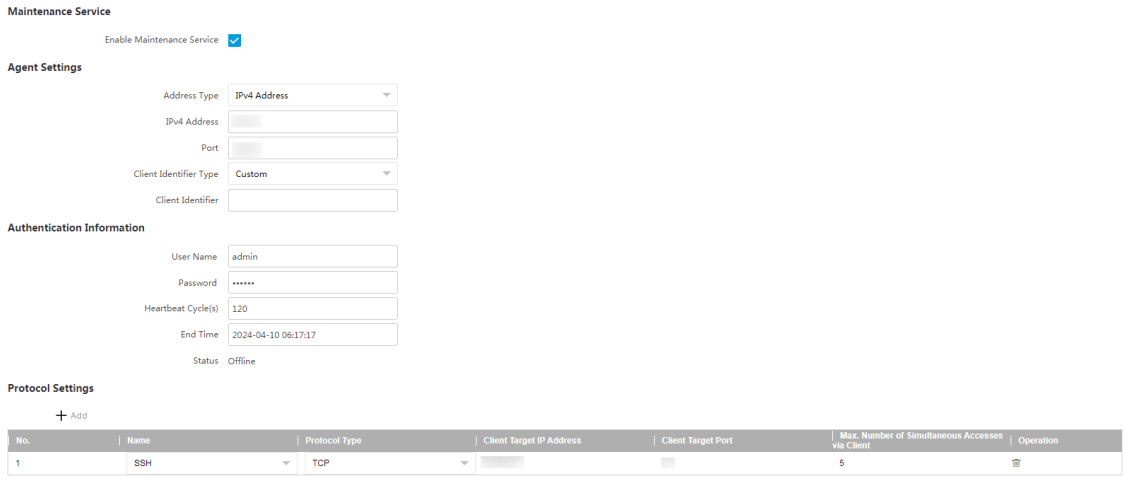


Figure 13-1 Maintenance Service

3. Set agent parameters.
   1) Select **Address Type**.
   2) Set the IP address/domain name and port of the agent.
   3) Select **Client Identifier Type** and set **Client Identifier** according to the actual supporting conditions of the camera. The identifier serves as a unique mark of the camera.
4. Set the authentication information.

   User Name/Password

   The user name and password of the camera for the authentication via the platform server access.

   Heartbeat Cycle(s)

   You are recommended to keep the default value.

   End Time

   The camera will disconnect with the platform server when reaching the set end time.
5. Set protocol parameters.
   1) Click **Add** to add a protocol.
   2) Set the corresponding parameters of the protocol.

Note

You can login and access up to 5 cameras (clients) simultaneously via HTTP or SSH protocol.

6. Click **Save**.

What to do next

After settings, refresh the interface and check the authentication status of the camera. If the status is online, you can access and debug the camera via the platform server.


See Far, Go Further