HIKVISION

Intelligent ANPR 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.

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.
ℹ **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

1.3 Download Plug-in 4

Chapter 2 Network Configuration 5

2.1 Set IP Address 5

2.2 Set Port 6

2.3 Set IEEE 802.1X 8

2.4 Set DDNS 9

2.5 Set mDNS 10

2.6 Set SNMP 10

2.7 Set QoS 12

2.8 Connect to Platform 12

2.8.1 Set Arm Host 12

2.8.2 Set SDK Listening 12

2.8.3 Set FTP 13

2.8.4 Set ISAPI Listening 15

2.8.5 Connect to ISUP Platform 16

2.8.6 Connect to OTAP 18

2.8.7 Connect to Hik-Connect 19

2.8.8 Set Integration Protocol 22

2.8.9 Set Cloud Storage 23

Chapter 3 Quick Configuration 24

3.1 Select Application Mode 24
3.2 Set Basic Parameters 25
3.3 Draw Lane Lines 29
3.4 Set Allowlist and Blocklist 31
Chapter 4 Entrance and Exit Configuration 33
4.1 Set Barrier Gate Linkage 33
4.1.1 Set Allowlist and Blocklist 33
4.1.2 Control Barrier Gate 34
4.1.3 Pass Control 37
4.2 Set Wiegand Parameters 39
4.3 Set Custom License Plate Mapping 40
4.4 Set LED Display 41
4.5 Set Voice Prompt 43
4.6 Set Main and Sub-Camera Mode 44
4.7 Peripheral Control 46
Chapter 5 Capture Configuration 50
5.1 Set Capture Parameters 50
5.1.1 Set License Plate Recognition Parameters 50
5.1.2 Set Vehicle Feature Parameters 51
5.1.3 Set Supplement Light Parameters 51
5.1.4 Set Capture Overlay 52
5.1.5 Set Image Encoding Parameters 54
5.1.6 Set Capture Schedule 55
5.2 Advanced Configuration 56
5.2.1 System Service 56
5.2.2 Vehicle Capture and Recognition Service 57
Chapter 6 View Real-Time Picture 59
Chapter 7 Live View and Local Configuration 62

7.1 Live View 62

7.1.1 Start/Stop Live View 62

7.1.2 Select Image Display Mode 62

7.1.3 Select Window Division Mode 62

7.1.4 Select Stream Type 62

7.1.5 Capture Picture Manually 62

7.1.6 Record Manually 62

7.1.7 Enable Digital Zoom 63

7.1.8 Start/Stop Two-Way Audio 63

7.1.9 Enable/Disable Audio 63

7.1.10 Select Video Mode 64

7.2 Set Snapshot Mode 64

7.3 PTZ Operation 64

7.4 Local Configuration 65

Chapter 8 Record and Capture 70

8.1 Set Storage Media 70

8.2 Set Record Schedule 71

8.3 Set Snapshot Schedule 73

Chapter 9 Playback 74

Chapter 10 Encoding and Display 75

10.1 Set Camera Parameters 75

10.2 Set OSD 78

10.3 Set Video Encoding Parameters 80

10.4 Set ROI 81

10.5 Set Privacy Mask 82

10.6 Enable Regional Exposure 83

Chapter 11 Event and Alarm 84

11.1 Exception Alarm 84

11.2 Set Email 84

11.3 Set Email Event 85

11.4 Set Motion Detection 85

Chapter 12 Safety Management 87

12.1 Manage User 87

12.2 Enable User Lock 88

12.3 Set SSH 88

12.4 Prohibit PING 89

12.5 Set SDK Protocol Authentication Mode 89

12.6 Set RTSP Authentication 89

12.7 Set Timeout Logout 89

12.8 Set Password Validity Period 90

12.9 Set IP Address Filtering 90

12.10 Set HTTPS 91

12.10.1 Create and Install Self-signed Certificate 91

12.10.2 Install Authorized Certificate 91

Chapter 13 Maintenance 92

13.1 View Device Information 92

13.2 Synchronize Time 92

13.3 Set DST 93

13.4 Set RS-485 94

13.5 Set RS-232 94

13.6 Download Debug Data 95

13.7 Search Log 96

13.8 Reboot 96

13.9 Restore Parameters 97

13.10 Export Parameters 97

13.11 Import Configuration File 97

13.12 Upgrade 98

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

Device default information are as follows.

- Default IP address: 192.168.1.64
- Default port: 8000
- Default user name: admin

1.1.2 Activate via SADP

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

Before You Start

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

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

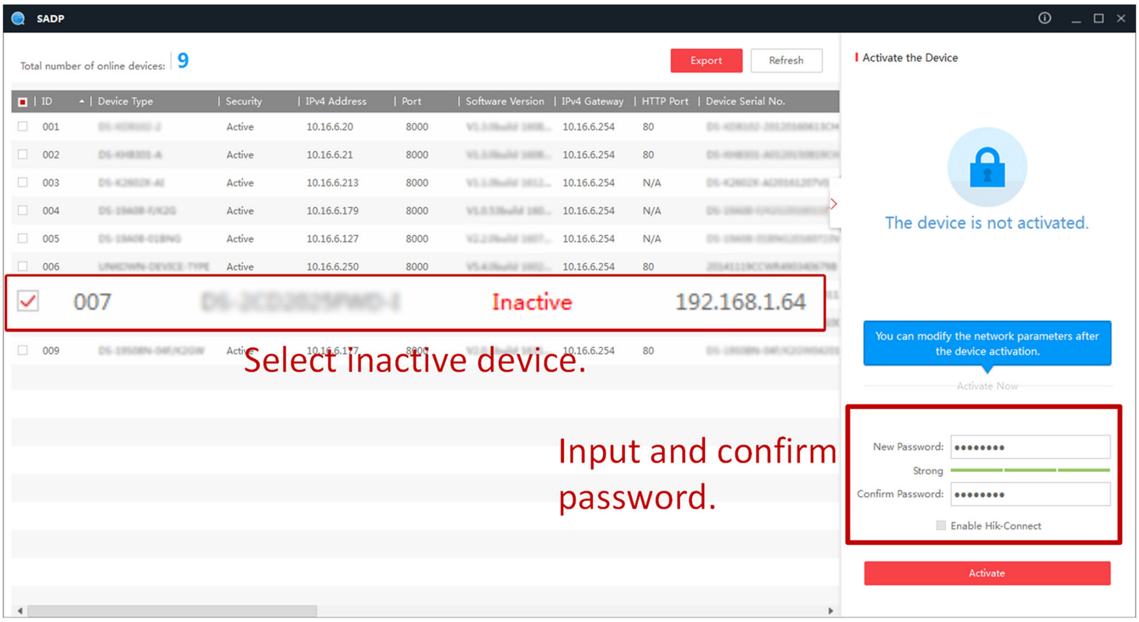
Steps

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

   Caution

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

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



SADP

Total number of online devices: 9

Export Refresh

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐	002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐	003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.168.1.64					
☐	009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Activate

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**.
   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 connect to the same LAN.

Steps

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

⚠ **Caution**

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

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

1.2 Login

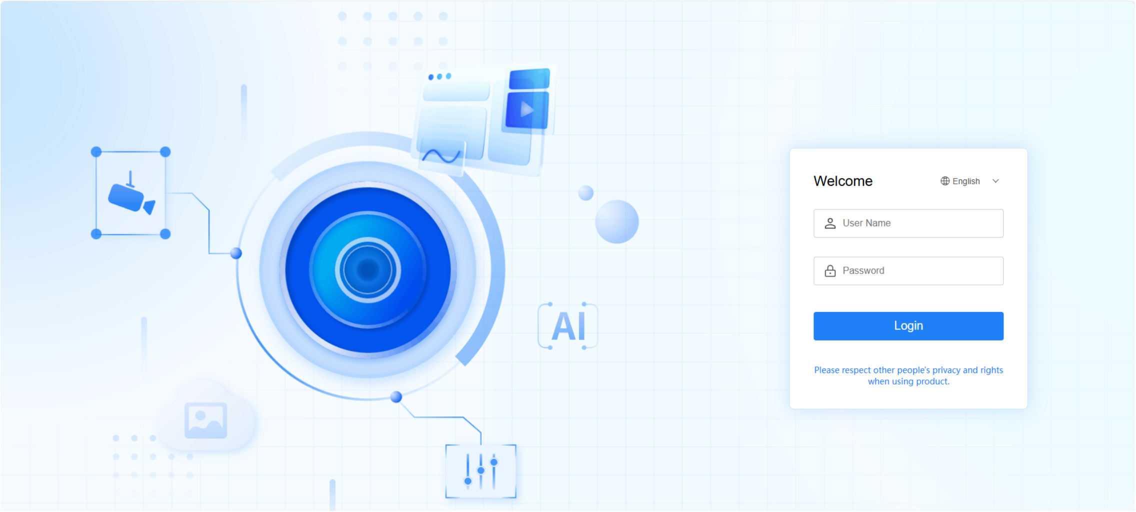
You can log in to the device via web browser for further operations such as live view and local configuration.

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.



Please respect other people's privacy and rights when using product.

Figure 1-2 Login

2. **Optional:** Select the other languages from the drop-down list on the upper right corner of the interface to switch the language.
3. Enter **User Name** and **Password**.
4. Click **Login**.

Note

- If live view failed, click on the upper right corner of the interface to download the plug-in and install it.
- Close the web browser to install the plug-in, or the installation may fail. If you still cannot realize live view after installing the plug-in, try to uninstall the plug-in and reinstall.

5. Reopen the web browser after the installation of the plugin and repeat steps 1 to 3 to log in.
6. **Optional:** Click on the upper right corner of the interface to log out of the device.

1.3 Download Plug-in

No plug-in mode is enabled by default. In no plug-in mode, the resolution of the live view image will be decreased and the live view may not be smooth. You can download and install plug-in to improve the live view condition.

In no-plug in mode, "No Plug-in Mode" prompt will appear on the upper right corner of the interface. You can click to download the plug-in. Close the browser to install the plug-in to the computer. Then access to the IP address of the device again, and the "No Plug-in Mode" prompt will disappear from the upper right corner of the interface.

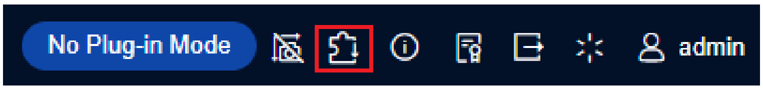


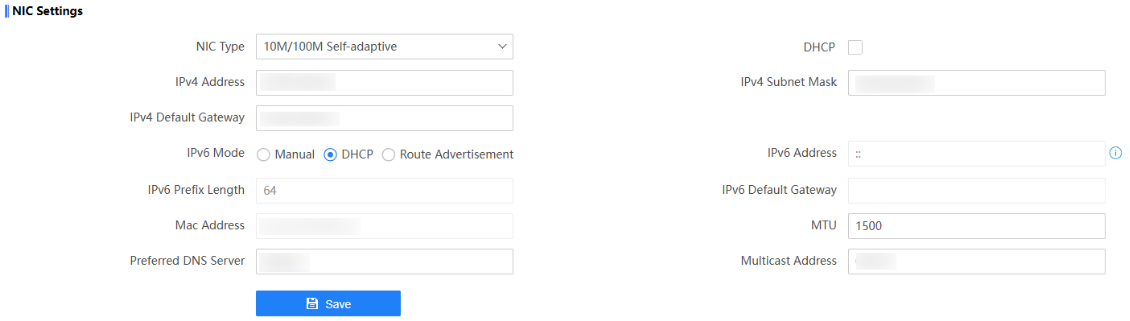
Figure 1-3 Download Plug-in

Chapter 2 Network Configuration

2.1 Set IP Address

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

Go to **Configuration → Network → Network Parameters → Network Interface** . Set the parameters and click **Save**.



NIC Settings

NIC Type	10M/100M Self-adaptive	DHCP	□
IPv4 Address	[redacted]	IPv4 Subnet Mask	[redacted]
IPv4 Default Gateway	[redacted]		
IPv6 Mode	○ Manual ● DHCP ○ Route Advertisement	IPv6 Address	::
IPv6 Prefix Length	64	IPv6 Default Gateway	
Mac Address	[redacted]	MTU	1500
Preferred DNS Server	[redacted]	Multicast Address	[redacted]

Figure 2-1 Set IP Address

NIC Type

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

IPv4

Two modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, 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 Address

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

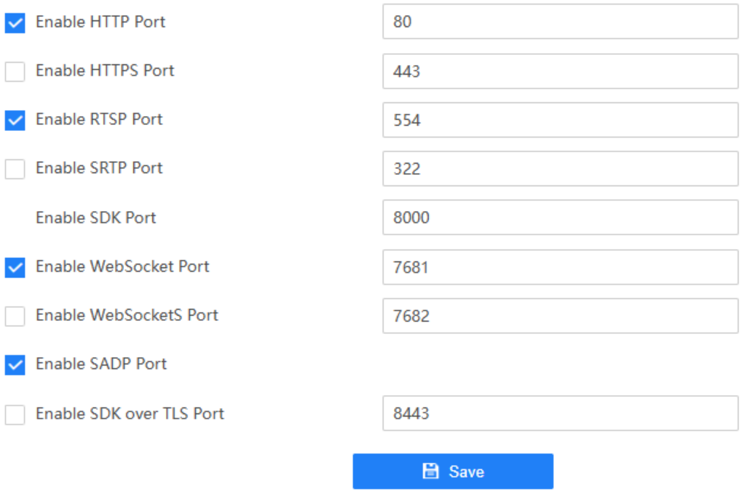
DNS

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

2.2 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.



☑ Enable HTTP Port	80
□ Enable HTTPS Port	443
☑ Enable RTSP Port	554
□ Enable SRTP Port	322
Enable SDK Port	8000
☑ Enable WebSocket Port	7681
□ Enable WebSocketS Port	7682
☑ Enable SADP Port	
□ Enable SDK over TLS Port	8443

Figure 2-2 Set Port

Enable 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 address bar for login.

Enable HTTPS Port

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

Enable RTSP Port

RTSP (Real-Time Streaming Protocol) is a communication protocol used to control servers that stream media content over the Internet. It helps in setting up and managing connections between devices for streaming audio or video. RTSP ensures that media players and servers can communicate smoothly, allowing users to play, pause, adjust volume, and perform other actions while streaming content.

Enable SRTP Port

SRTP (Secure Real-Time Transport Protocol) is an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features.

Enable SDK Port

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

Enable WebSocket Port

It refers to the full-duplex communication protocol port based on TCP. Enable the port for live view without plug-in.

Enable WebSocketS Port

It refers to the full-duplex communication protocol port based on TCP. Enable the port for live view without plug-in. It can only be accessed via certificate verification with high security.

Enable SADP Port

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

Enable 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 new port.
- Reboot the device to take the new settings into effect.
- The supported ports vary with different models. The actual device prevails.

2.3 Set IEEE 802.1X

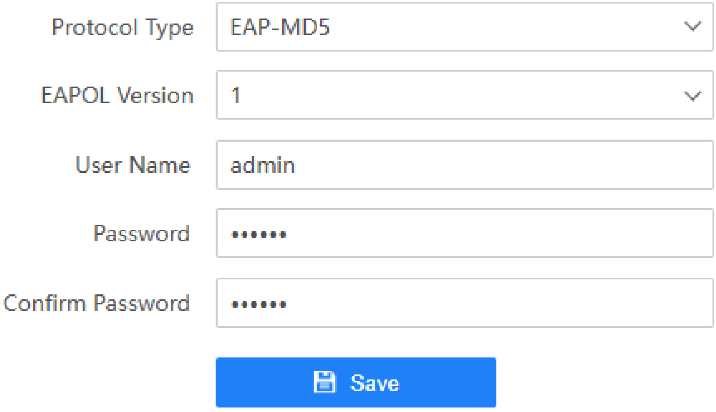
IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1X standard, the authentication is needed.

Steps

Note

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

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



Protocol Type: EAP-MD5

EAPOL Version: 1

User Name: admin

Password: ••••••

Confirm Password: ••••••

Figure 2-3 Set IEEE 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**.

2.4 Set DDNS

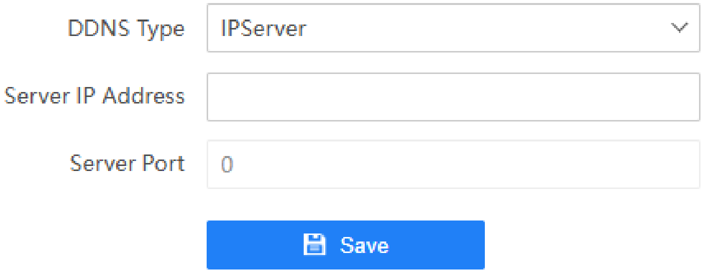
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

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** .
2. Enable DDNS.



DDNS Type: IPServer

Server IP Address:

Server Port: 0

Figure 2-4 Set 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.

2.5 Set mDNS

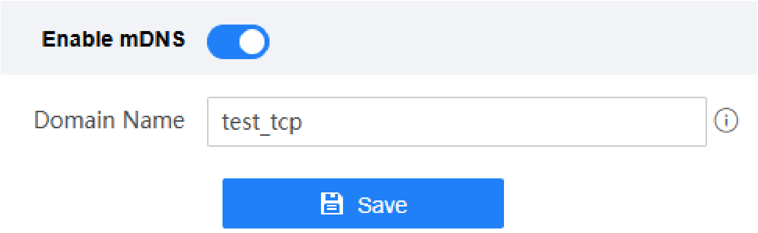
If multiple devices of the same type are deployed in the same LAN, you can enable mDNS and set a domain name with the environment identification. Then you can access to the devices quickly via the domain name instead of accessing via the specific IP addresses.

Before You Start

Ensure all the devices of the same type are in the same LAN.

Steps

1. Go to **Configuration → Network → Network Parameters → mDNS** .
2. Enable mDNS.



Enable mDNS

Domain Name: test_tcp

Figure 2-5 Set mDNS

3. Enter **Domain Name**.

Note

The domain name should start with a letter or digit and end with a letter. Only special characters "-_." are allowed. The length cannot exceed 63 bytes.

For example, you can enter "test_tcp".

4. Click **Save**.

What to do next

After setting the domain name, add ".local" suffix to access the device. For example, if the domain name is set as "test_tcp", you need to enter "test_tcp.local" to access to the device. If the domain name contains "." to form multi-level domain name, you should create a DNS server in addition to take the settings into effect.

2.6 Set SNMP

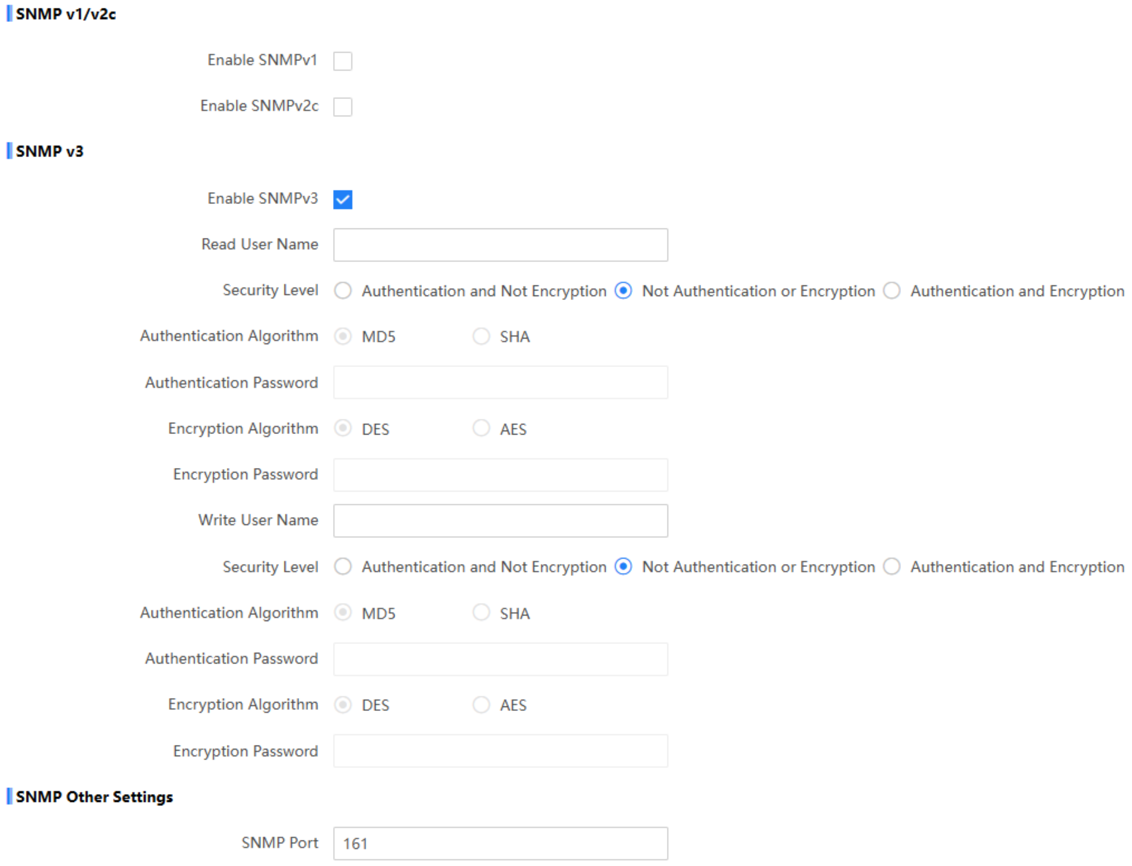
You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

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** .



SNMP v1/v2c

Enable SNMPv1 □

Enable SNMPv2c □

SNMP v3

Enable SNMPv3 ☑

Read User Name

Security Level ○ Authentication and Not Encryption ● Not Authentication or Encryption ○ Authentication and Encryption

Authentication Algorithm ○ MD5 ○ SHA

Authentication Password

Encryption Algorithm ○ DES ○ AES

Encryption Password

Write User Name

Security Level ○ Authentication and Not Encryption ● Not Authentication or Encryption ○ Authentication and Encryption

Authentication Algorithm ○ MD5 ○ SHA

Authentication Password

Encryption Algorithm ○ DES ○ AES

Encryption Password

SNMP Other Settings

SNMP Port 161

Figure 2-6 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. There exists information leakage using SNMP v1 or v2. You're recommended to use SNMP v3, which provides encryption and is safer. If you use v3, HTTPS protocol must be enabled.

3. Set the SNMP parameters.

Note

For SNMP v3, you need to set **Authentication Algorithm** and **Authentication Password**, and **Encryption Algorithm** and **Encryption Password**.

4. Click **Save**.

2.7 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**.

2.8 Connect to Platform

2.8.1 Set Arm Host

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

Steps

1. Go to **Configuration → Network → Data Connection → Arm Upload** .
2. Go to **Configuration → Network → Data Connection → Cloud Storage** to set the cloud storage parameters. Refer to ***Set Cloud Storage*** for details.
3. Click **Save**.

2.8.2 Set SDK Listening

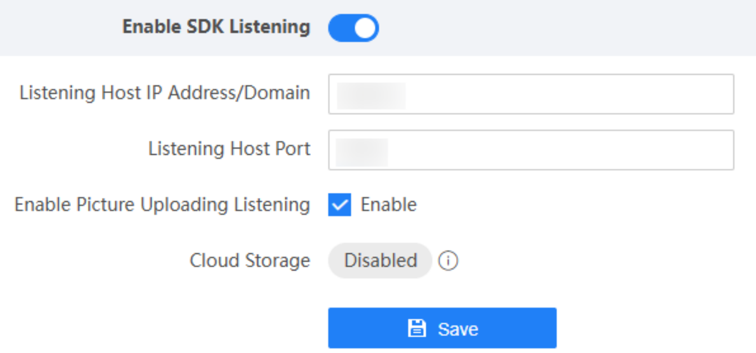
The SDK listening can be used to receive the uploaded information and pictures of the device arming alarm.

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** .
2. Enable SDK listening.



Enable SDK Listening ●

Listening Host IP Address/Domain

Listening Host Port

Enable Picture Uploading Listening ☑ Enable

Cloud Storage Disabled

Save

Figure 2-7 Set SDK Listening

3. Set **Listening Host IP Address/Domain** and **Listening Host Port** if you need to upload the alarm information and pictures.
4. **Optional:** Enable the picture uploading listening if you need to upload picture information.
5. **Optional:** If you want to save the alarm information and pictures to the cloud storage, go to **Configuration → Network → Data Connection → Cloud Storage** to set the cloud storage parameters. Refer to ***Set Cloud Storage*** for details.
6. Click **Save**.

2.8.3 Set FTP

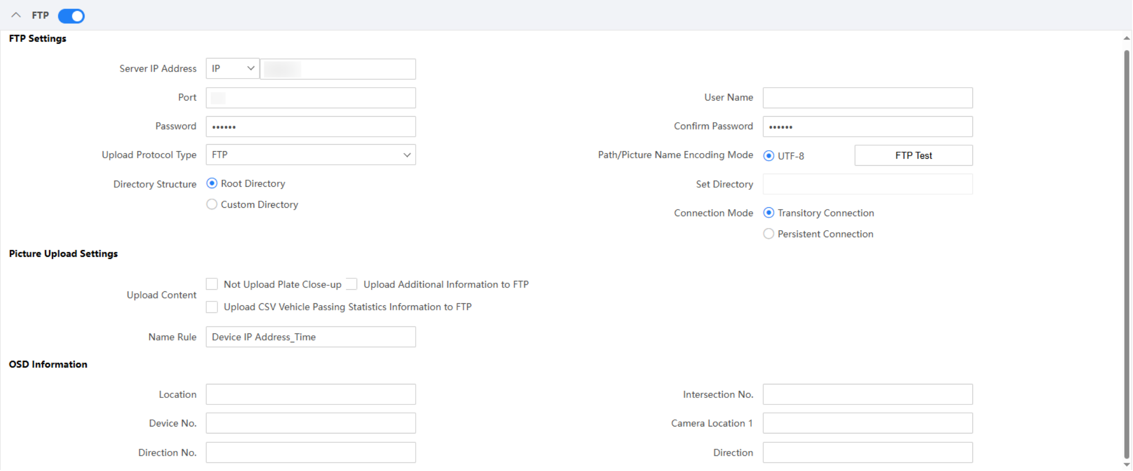
Set FTP parameters if you want to upload the captured pictures to the FTP server.

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** .
2. Enable the FTP server.



FTP

FTP Settings

Server IP Address	IP [redacted]		
Port	[redacted]	User Name	
Password	••••••	Confirm Password	••••••
Upload Protocol Type	FTP	Path/Picture Name Encoding Mode	● UTF-8 FTP Test
Directory Structure	● Root Directory ○ Custom Directory	Set Directory	
		Connection Mode	● Transitory Connection ○ Persistent Connection

Picture Upload Settings

Upload Content	□ Not Upload Plate Close-up □ Upload Additional Information to FTP □ Upload CSV Vehicle Passing Statistics Information to FTP
Name Rule	Device IP Address_Time

OSD Information

Location		Intersection No.	
Device No.		Camera Location 1	
Direction No.		Direction	

Figure 2-8 Set FTP

3. Set FTP Parameters.

   1) Select **Sever IP Address** type and enter corresponding information.

   2) Enter **Port**.

   3) Enter **User Name** and **Password**, and confirm the password.

   4) Select **Upload 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.

4. **Optional:** Enable upload functions.

   Not Upload Plate Close-up

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

   Upload Additional Information to FTP

Add related information when uploading data to the FTP server.

Upload CSV Vehicle Passing Statistics Information to FTP

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

5. **Optional:** Click **FTP Test** to check the FTP server.
6. Click the text filed of **Name Rule** to set the directory and separator for the file storage.
7. **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.
8. Click **Save**.

2.8.4 Set ISAPI Listening

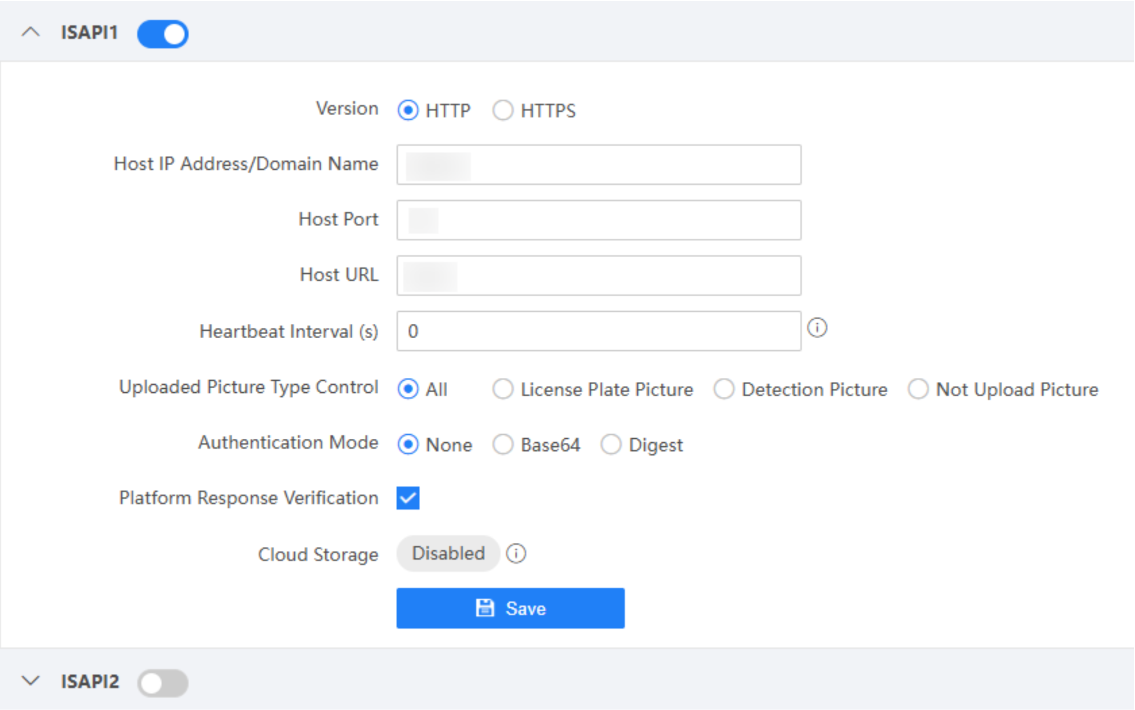
ISAPI listening and SDK listening are mutually exclusive protocols. If you enable the picture uploading listening, the device will transmit images via the SDK listening. If not, the device will upload images via ISAPI protocol after the ISAPI parameters are set.

Before You Start

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

Steps

1. Go to **Configuration → Network → Data Connection → ISAPI Listening** .
2. Enable **ISAPI1** or **ISAPI2**.



ISAPI1

Version ● HTTP ○ HTTPS

Host IP Address/Domain Name

Host Port

Host URL

Heartbeat Interval (s) 0

Uploaded Picture Type Control ● All ○ License Plate Picture ○ Detection Picture ○ Not Upload Picture

Authentication Mode ● None ○ Base64 ○ Digest

Platform Response Verification ☑

Cloud Storage Disabled

Figure 2-9 Set ISAPI Listening

3. Select **Version**.
4. Set **Host IP Address/Domain Name**, **Host Port**, and **Host URL**.
5. Set the parameters.

   Heartbeat Interval

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

   Uploaded Picture Type Control

   You can upload license plate pictures and detection pictures (the capture scene pictures), or do not upload pictures.

   Authentication Mode

   Only the authorized users can access the device. 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.

   Platform Response Verification

   Enable the function, and the device will get the platform response result.
6. **Optional:** If you want to save the alarm information and pictures to the cloud storage, go to **Configuration → Network → Data Connection → Cloud Storage** to set the cloud storage parameters. Refer to ***Set Cloud Storage*** for details.
7. Click **Save**.

2.8.5 Connect to ISUP Platform

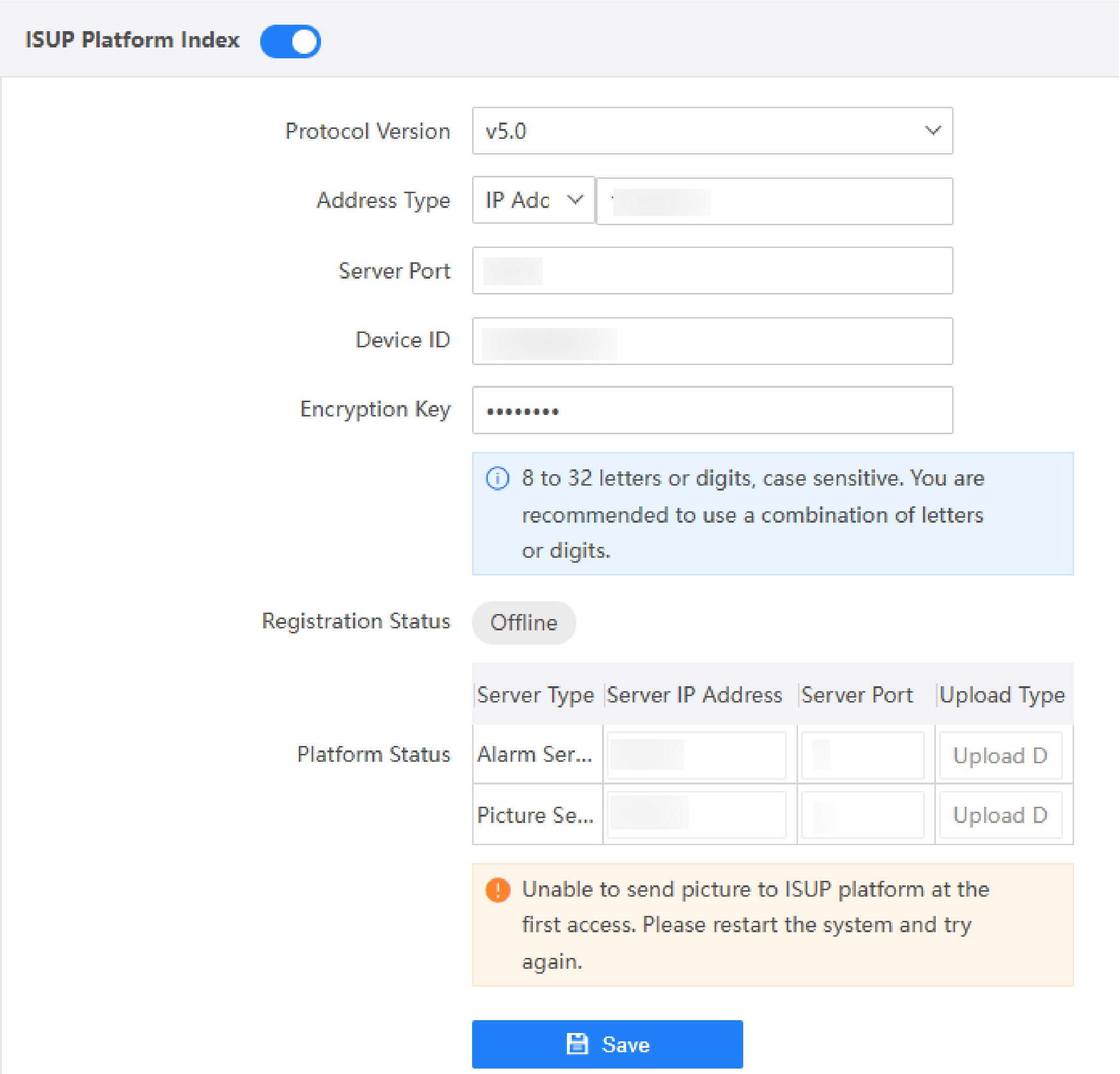
ISUP is a platform access protocol. The device can be remotely accessed via this platform.

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** .
2. Enable **ISUP Platform Index**.



ISUP Platform Index

Protocol Version: v5.0

Address Type: IP Adc

Server Port:

Device ID:

Encryption Key: ••••••••

ⓘ 8 to 32 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Registration Status: Offline

Platform Status:

Server Type	Server IP Address	Server Port	Upload Type
Alarm Ser...			Upload D
Picture Se...			Upload D

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

Figure 2-10 Connect to ISUP Platform

3. Select **Protocol Version**.
4. Select **Address Type** and enter IP address or domain name of the platform.
5. Enter **Server Port**, **Device ID**, and **Encryption Key**.

Note

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

6. Click **Save**.

What to do next

When the registration status shows online, you can add or manage the device via the platform software.

2.8.6 Connect to OTAP

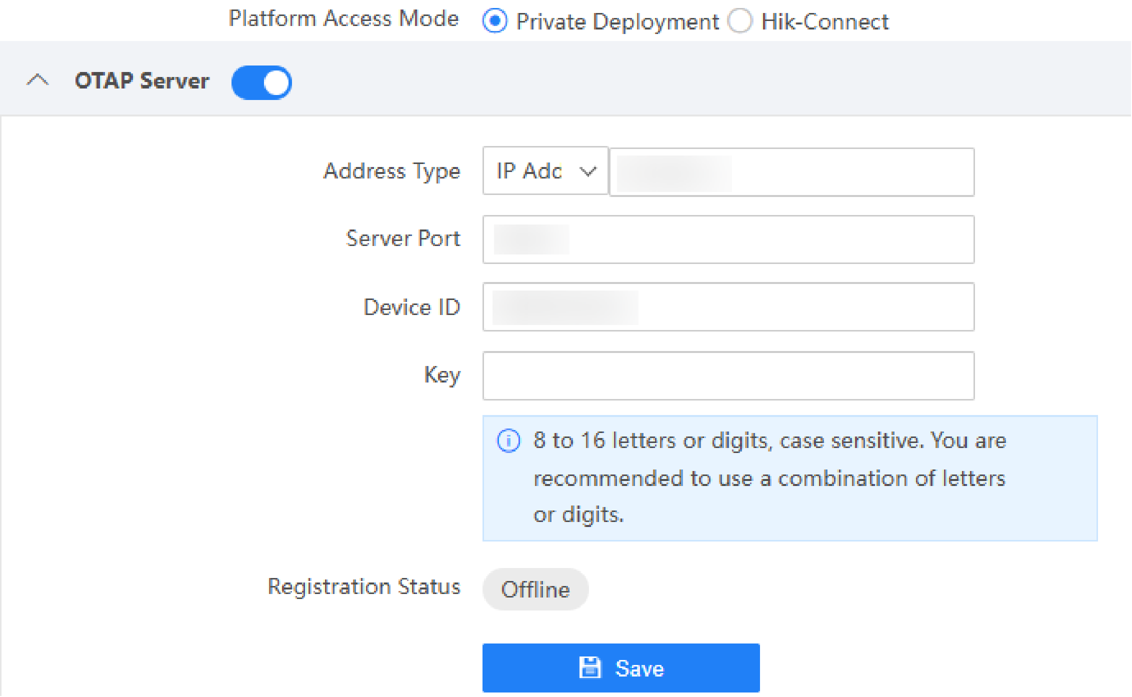
The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information.

Before You Start

- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- 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. Enable **OTAP Server**.



Platform Access Mode ● Private Deployment ○ Hik-Connect

OTAP Server

Address Type IP Adc

Server Port

Device ID

Key

ⓘ 8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Registration Status Offline

Figure 2-11 Connect to OTAP

4. Set corresponding parameters.

Address Type

Select the address type of the connected platform or server, and enter the IP address or domain name.

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 add or manage the device via the platform software.

2.8.7 Connect to Hik-Connect

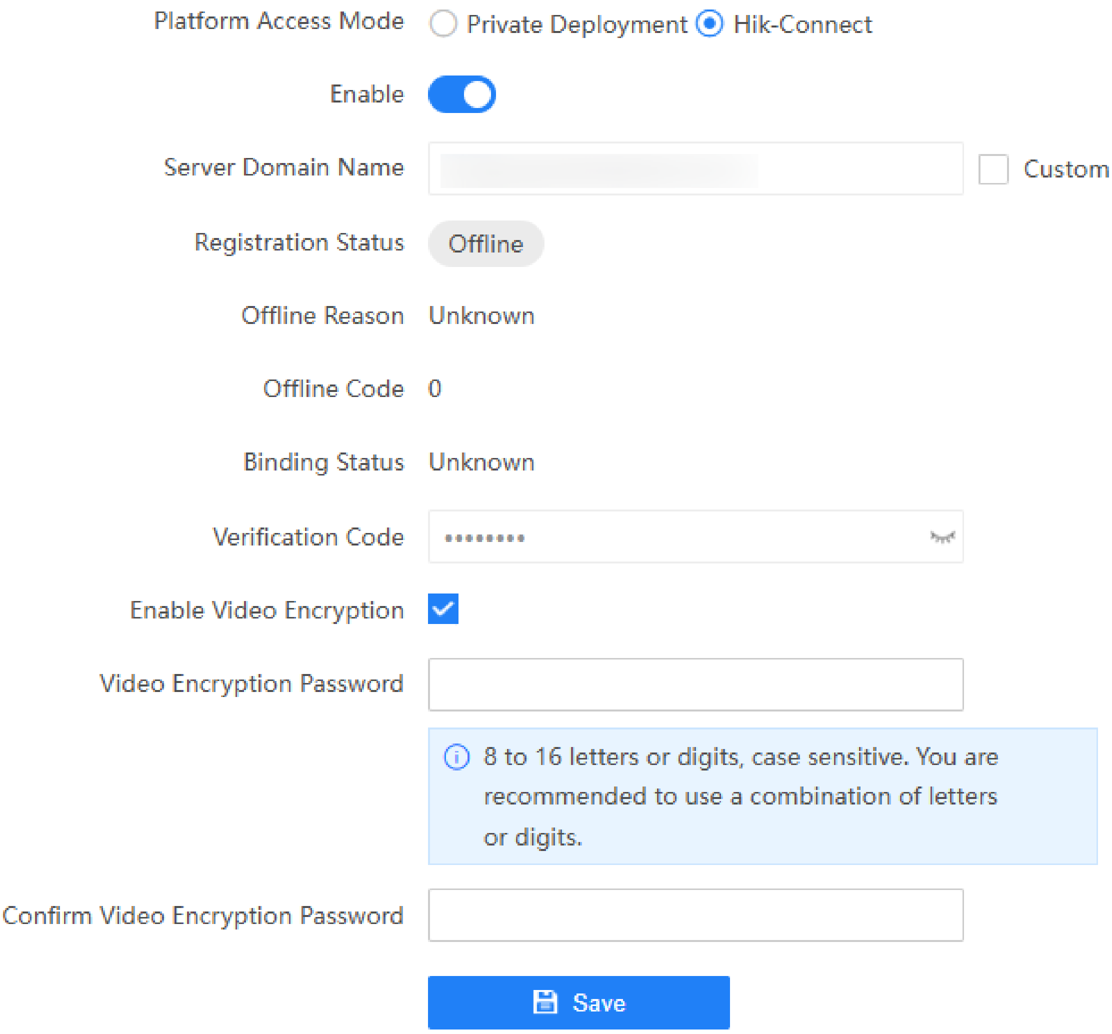
The device can be remotely accessed via Hik-Connect.

Before You Start

- Set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.
- OTAP connection is disabled.

Steps

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**. Enable the function.



Platform Access Mode ○ Private Deployment ● Hik-Connect

Enable

Server Domain Name [redacted] □ Custom

Registration Status Offline

Offline Reason Unknown

Offline Code 0

Binding Status Unknown

Verification Code ••••••••

Enable Video Encryption ☑

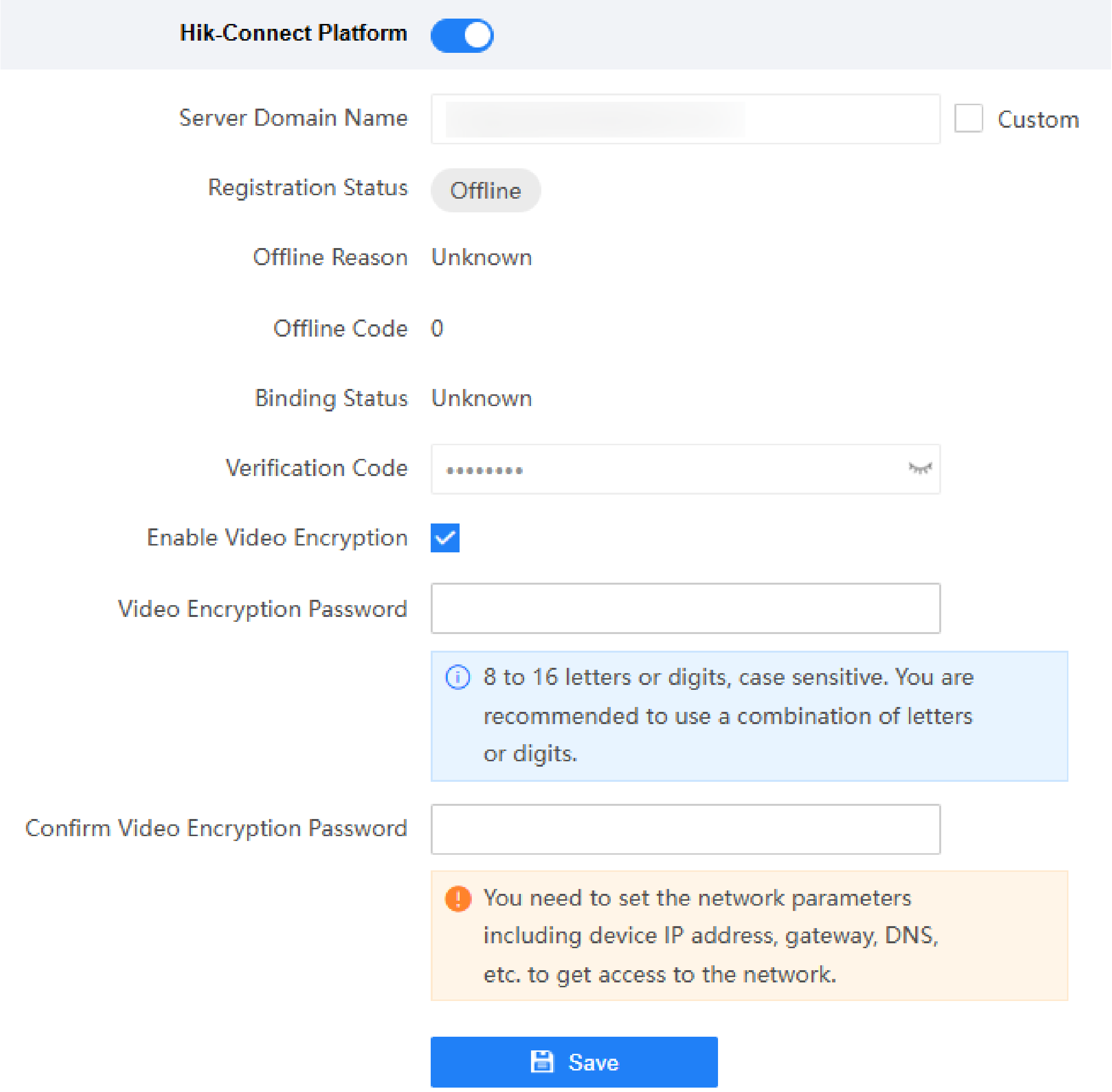
Video Encryption Password

8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Confirm Video Encryption Password

Figure 2-12 Connect to Hik-Connect (V2.0)

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



Hik-Connect Platform

Server Domain Name □ Custom

Registration Status: Offline

Offline Reason: Unknown

Offline Code: 0

Binding Status: Unknown

Verification Code: ••••••••

Enable Video Encryption ☑

Video Encryption Password

8 to 16 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

Confirm Video Encryption Password

You need to set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.

Figure 2-13 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. Enter a custom **Verification Code** used to add the device via **Hik-Connect**.

Caution

The verification code should be 6 letters or digits, case sensitive. You are recommended to use a combination of letters or digits.

4. **Optional:** Check **Enable Video Encryption** and set **Video Encryption Password** to encrypt the videos transmission. Confirm the password.
5. Click **Save**.
6. 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 → Installation & Maintenance Tools → Hikvision APP Store** .
   - Scan the QR code below to download the application.

Figure 2-14 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.

2.8.8 Set Integration Protocol

You can connect the device via ONVIF protocol.

Steps

1. Go to **Configuration → Network → Data Connection → Integration Protocol** .
2. Enable **ONVIF**.
3. Select **Authentication Mode**, and click **Save**.
4. Add a user.
   1) Click **Add**.
   2) Set user name, password, and user type, and confirm the password.
   3) Click **OK**.
   4) **Optional:** You can select the added user and click ✎ to edit the user information, or click 🗑 to delete the user.

Result

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

2.8.9 Set Cloud Storage

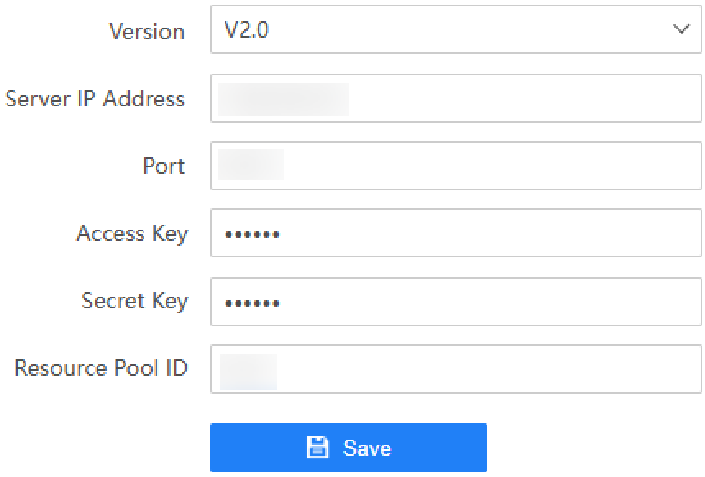
Cloud storage is a kind of network storage. It can be used as the extended storage to save the captured pictures.

Before You Start

- Arrange the cloud storage server.
- You have enabled listening or arming.

Steps

1. Go to **Configuration → Network → Data Connection → Cloud Storage** .
2. Enable **Cloud Storage**.



Version: V2.0

Server IP Address:

Port:

Access Key: ••••••

Secret Key: ••••••

Resource Pool ID:

Figure 2-15 Set Cloud Storage

3. Select **Version**.

V1.0

a. Enter **Server IP Address** and **Port**
b. Enter **User Name** and **Password**.
c. Enter **Cloud Storage ID** according to the server storage area No.

V2.0

a. Enter **Server IP Address** and **Port**
b. Enter **Access Key** and **Secret Key**.
c. Enter **Resource Pool ID** according to the server storage area No. of uploading pictures.

4. Click **Save**.

Chapter 3 Quick Configuration

3.1 Select Application Mode

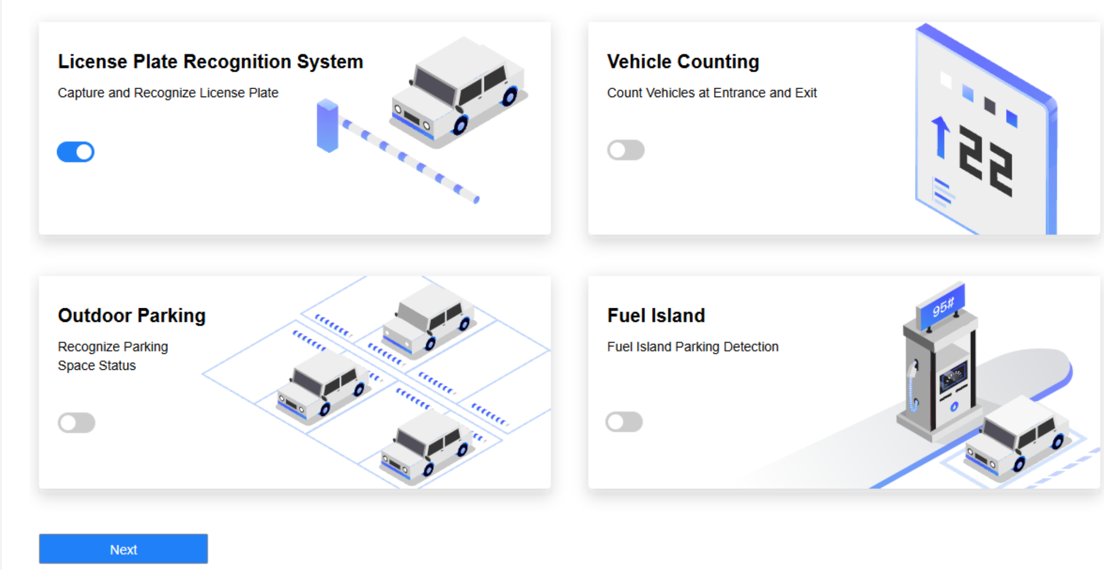
You can enable the application mode of the device according to the actual scene quickly.

Steps

Note

The function varies with different models. For some device models, you do not need to select the application mode. The actual device prevails.

1. Go to **Quick Configuration → Application Mode** .



License Plate Recognition System
Capture and Recognize License Plate
●

Vehicle Counting
Count Vehicles at Entrance and Exit
○

Outdoor Parking
Recognize Parking Space Status
○

Fuel Island
Fuel Island Parking Detection
○

Next

Figure 3-1 Select Application Mode

2. Enable an application mode according to the actual scene.

Note

You can only enable one application mode.

License Plate Recognition System

Select this mode to capture and recognize license plates at entrance or exit.

Vehicle Counting

Select this mode to count vehicles at entrance or exit.

Outdoor Parking

Select this mode to detect the outdoor parking space status and capture pictures when vehicles enter or exit from the parking spaces.

Fuel Island

Select this mode for the fuel island scene. The vehicle driver prepays the refueling fees via the APP before entering into the fuel island. When the vehicle enters into the corresponding parking space, the device will capture pictures with the license plate and upload the pictures to the platform. After refueling ends and the vehicle exits from the parking space, the device will capture pictures and upload the exiting records to the platform. Up to four parking spaces are supported. The left and right lanes of the parking space cannot be changed.

3. If you switch the application mode, click **OK** on the popup window to reboot the device and restore to default parameters to take the settings into effect.
4. Click **Next** to set basic parameters.

3.2 Set Basic Parameters

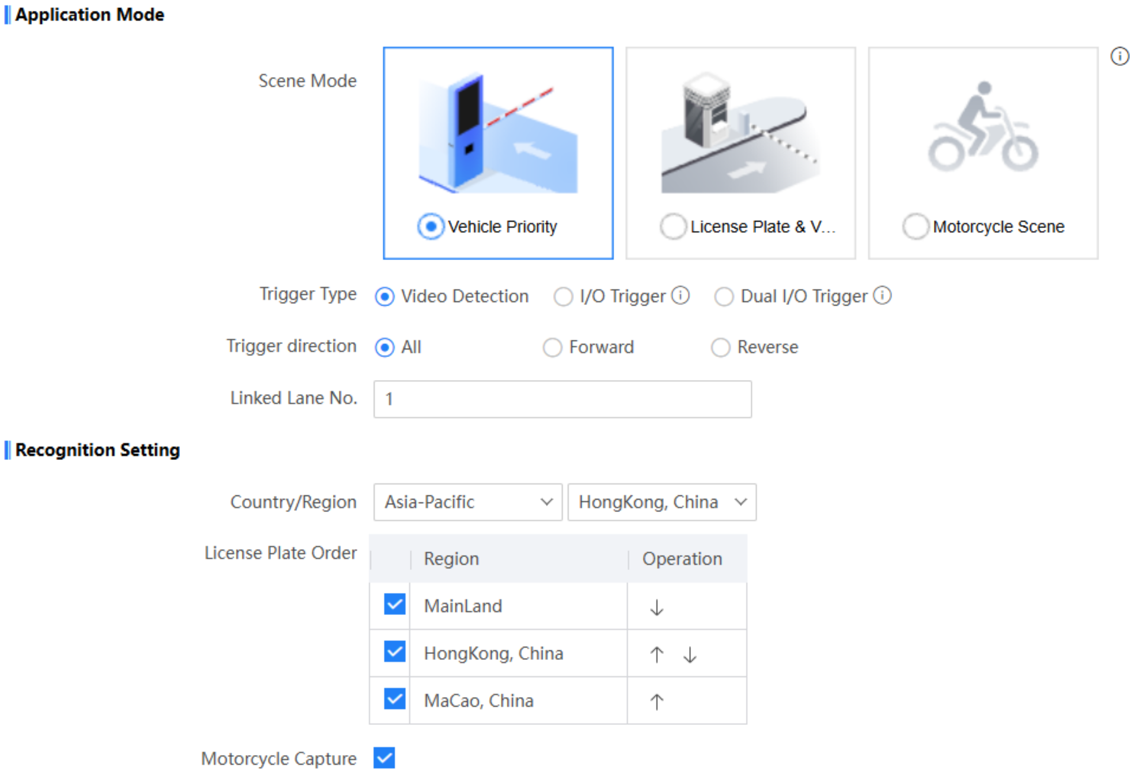
You can set the basic parameters in quick configuration to realize capture quickly.

Steps

Note

The interfaces and supported parameters may vary with different models. The actual interface prevails.

1. Go to **Quick Configuration → Basic Parameters** .



Application Mode

Scene Mode: ● Vehicle Priority ○ License Plate & V... ○ Motorcycle Scene

Trigger Type: ● Video Detection ○ I/O Trigger ○ Dual I/O Trigger

Trigger direction: ● All ○ Forward ○ Reverse

Linked Lane No.: 1

Recognition Setting

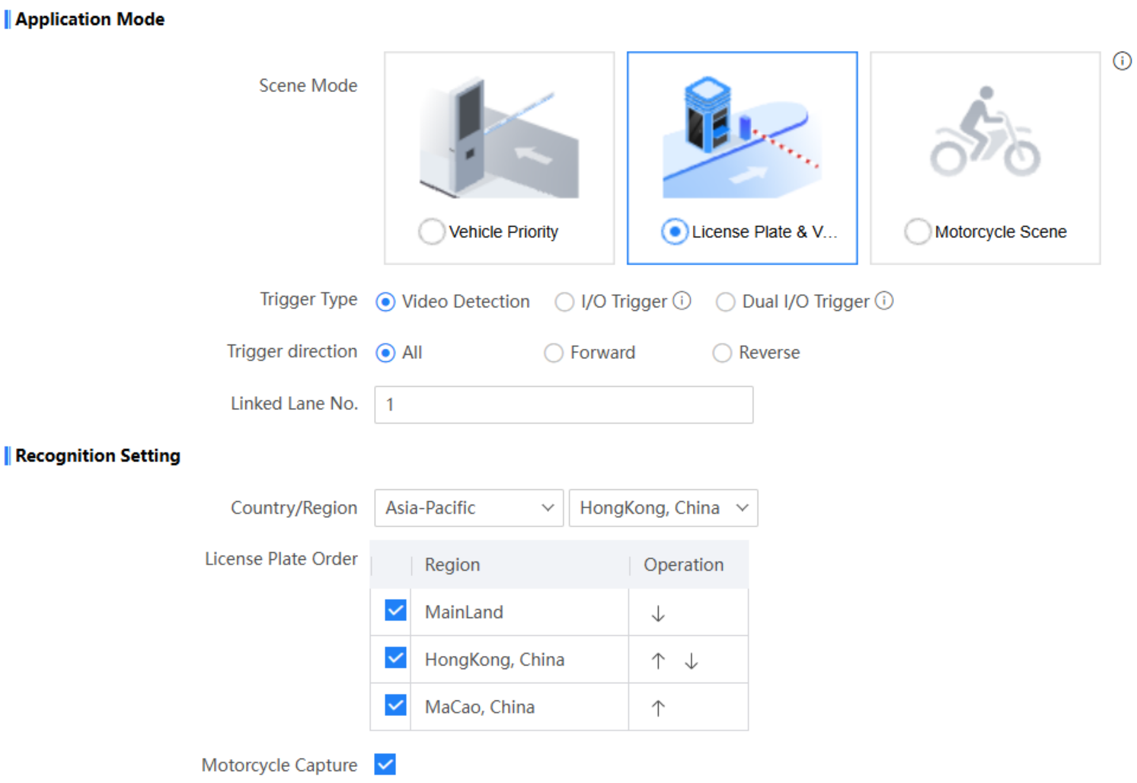
Country/Region: Asia-Pacific | HongKong, China

License Plate Order

	Region	Operation
☑	MainLand	↓
☑	HongKong, China	↑ ↓
☑	MaCao, China	↑

Motorcycle Capture ☑

Figure 3-2 Set Basic Parameters (Vehicle Priority)



Application Mode

Scene Mode: ○ Vehicle Priority ● License Plate & V... ○ Motorcycle Scene

Trigger Type: ● Video Detection ○ I/O Trigger ○ Dual I/O Trigger

Trigger direction: ● All ○ Forward ○ Reverse

Linked Lane No.: 1

Recognition Setting

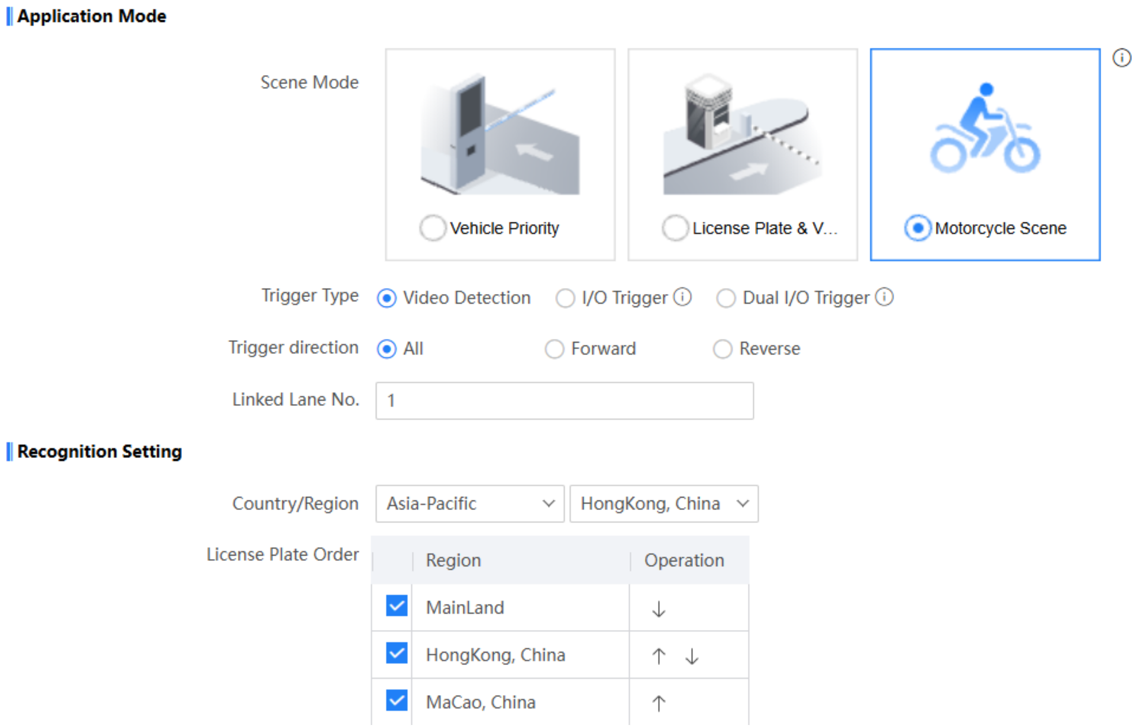
Country/Region: Asia-Pacific | HongKong, China

License Plate Order

	Region	Operation
☑	MainLand	↓
☑	HongKong, China	↑ ↓
☑	MaCao, China	↑

Motorcycle Capture ☑

Figure 3-3 Set Basic Parameters (License Plate & Vehicle)



Application Mode

Scene Mode: ○ Vehicle Priority ○ License Plate & V... ● Motorcycle Scene

Trigger Type: ● Video Detection ○ I/O Trigger ○ Dual I/O Trigger

Trigger direction: ● All ○ Forward ○ Reverse

Linked Lane No.: 1

Recognition Setting

Country/Region: Asia-Pacific | HongKong, China

License Plate Order

	Region	Operation
☑	MainLand	↓
☑	HongKong, China	↑ ↓
☑	MaCao, China	↑

Figure 3-4 Set Basic Parameters (Motorcycle Scene)

2. Set **Application Mode** parameters.

Scene Mode

Select the scene mode according to the actual scene.

- **Vehicle Priority**: The device installation height is 1.5 m with the available capture distance of 3 to 5 m.
- **License Plate & Vehicle**: The device installation height is 0.6 m with the available capture distance of 2 to 4 m.
- **Motorcycle Scene**: The device installation height is 1 to 1.5 m with the available capture distance of 1.5 m. The rear license plate of the motorcycle will be captured.

Trigger Type

Video Detection

Select it to trigger capture by video stream detection.

I/O Trigger

Select it to trigger capture by external device such as the vehicle detector and radar.

Dual I/O Trigger

Select it to detect the driving directions in mixed traffic scene with **Trigger I/O** and **Logic I/O**. You can click ⓘ to view the application scenario.

Trigger Direction

The parameter is available when you select **Trigger Type** as **Video Detection**.

- Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
- Select **Reverse** when license plates of vehicles from the leaving direction need to be recognized.
- Select **All** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.

Linked I/O No.

The parameter is available when you select **Trigger Type** as **I/O Trigger**. It refers to the I/O No. linked under I/O trigger mode. 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.

Trigger/Logic IO

The parameter is available when you select **Trigger Type** as **Dual I/O Trigger**. This trigger type shall be used with one trigger I/O and one logic I/O. Select the corresponding I/O No.

Linked Lane No.

The targets on the linked lane will be captured.

3. Select recognition parameters. Refer to ***Set License Plate Recognition Parameters*** for details.

Note

Enable **Motorcycle Capture** to enable non-motor vehicle capture. **Motorcycle Capture** is only available in **Video Priority** and **License Plate & Vehicle** scenes.

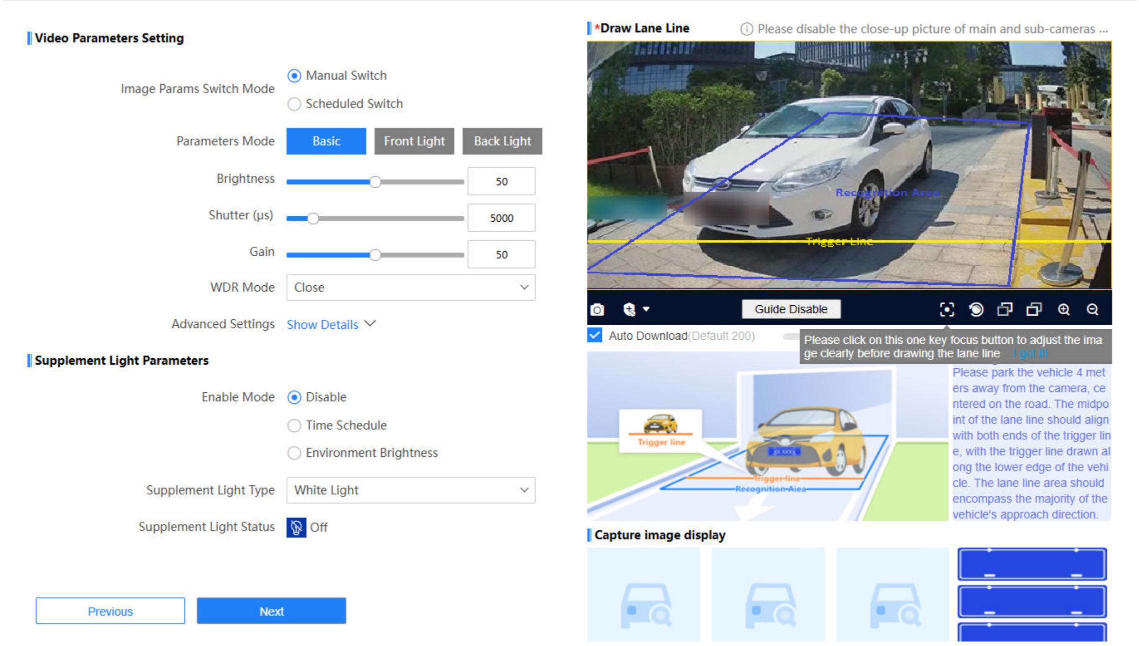
4. Click **Next** to draw lane lines.

3.3 Draw Lane Lines

You can set video parameters, supplement light parameters, and draw trigger line and recognition area.

Steps

1. Go to **Quick Configuration → Draw Lane Line** .



Video Parameters Setting

Image Params Switch Mode ● Manual Switch ○ Scheduled Switch

Parameters Mode: Basic | Front Light | Back Light

Brightness: 50

Shutter (μs): 5000

Gain: 50

WDR Mode: Close

Advanced Settings: Show Details

Supplement Light Parameters

Enable Mode ● Disable ○ Time Schedule ○ Environment Brightness

Supplement Light Type: White Light

Supplement Light Status: Off

Previous | Next

***Draw Lane Line**

ⓘ Please disable the close-up picture of main and sub-cameras ...

Guide Disable

☑ Auto Download(Default 200)

Please click on this one key focus button to adjust the image clearly before drawing the lane line I got it!

Please park the vehicle 4 meters away from the camera, centered on the road. The midpoint of the lane line should align with both ends of the trigger line, with the trigger line drawn along the lower edge of the vehicle. The lane line area should encompass the majority of the vehicle's approach direction.

Capture image display

Figure 3-5 Draw Lane Lines

2. Set video parameters. Refer to ***Set Camera Parameters*** for details.

3. Set supplement light parameters. Refer to ***Set Supplement Light Parameters*** for details.

4. Adjust the trigger line and recognition area on the live view image.

> **Note**
>
> For the device with vari-focal lens, disable the close-up picture of main and sub-cameras before adjusting the trigger line and recognition area.

1) Click ⊙ under the live view image to adjust the image clearly.
2) Refer to the drawing guide below the live view image on the interface.
3) Select the default trigger line and recognition area on the live view image. Adjust the positions and shapes according to the actual scene.

5. Optional: You can click the icons under the live view image to do corresponding operations.

Table 3-1 Icon Description

Icon	Description
📷	Click it to capture a picture, and the captured picture and recognized license plate picture will be displayed on the interface below the drawing guide.
🛡 / 🛡 / 🛡	• **Level 1 Arming**: Only the current computer can arm the device and receive the captured pictures in real time. The pictures will not be

Icon	Description
	stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming terminal. • **Level 2 Arming**: Up to 3 computers can arm the device and receive the captured pictures in real time. The pictures will be uploaded to level 2 arming terminal, and stored in the storage card. • **Disarming**: Disable the real-time capture function.
⊡	Click it to realize one-touch focus. Click it again to restore to the initial status.
◎	Click it to realize lens initialization.
⧉	Focus +. Hold it to view distant objects clearly, while nearby objects will be blurred.
⧉	Focus -. Hold it to view nearby objects clearly, while distant objects will be blurred.
⊕	Zoom +. Hold it to zoom in the image.
⊖	Zoom -. Hold it to zoom out the image.
Auto Download	In no plug-in mode, you can enable **Auto Download** to download the captured pictures to the computer directly. The latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically. The max. number of pictures in one compressed file depends on the selected **Number of Auto Captured Pictures** in **Configuration → Local** in no plug-in mode. If you disarm, the auto downloading will stop. You can view the downloading progress on the interface. The auto downloaded files will be saved to the default downloading directory of the browser in the format of .zip. You can go to the directory, decompress the file, and view the captured pictures. If you disable **Auto Download**, when you disarm, the dialogue box will pop up to prompt you if you need to download the arming captures. Click **OK** and the latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically.

Note

The supported icons vary with different models. The actual interface prevails.

6. Click **Next** to set allowlist and blocklist.

3.4 Set Allowlist and Blocklist

Barrier Gate Control

1. Go to **Quick Configuration → Allowlist and Blocklist → Barrier Gate Control** .
2. Select **Control Mode**.
   - **By Platform**: Select this mode in the scene in which the entry permissions are controlled by the software.
   - **By Camera**: Select this mode 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 **Configuration → Capture → Entrance and Exit → Pass Control** .
3. If you select **Control Mode** as **By Platform**, you can check **Enable Barrier Gate Control Offline** to control the barrier gate when the device is offline. Select **Barrier Gate Control When Platform Disconnection**. You can select to remain the barrier gate open or control the barrier gate by camera.
4. If you select **Control Mode** as **By Camera**, select the vehicle types to open the barrier gate and pass.

Note

You can refer to ***Control Barrier Gate*** and ***Pass Control*** for details.

Allowlist and Blocklist

You can refer to ***Set Allowlist and Blocklist*** for details.

Chapter 4 Entrance and Exit Configuration

Note

Entrance and exit configuration is available only when you enable **License Plate Recognition System** application mode.

4.1 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.

4.1.1 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 **Plate No.** and **Card No.**, and select the list type.
   3) **Optional:** If you want to control vehicles during fixed time period, enable **Time Settings**, and set the valid start time and end time.

      Note

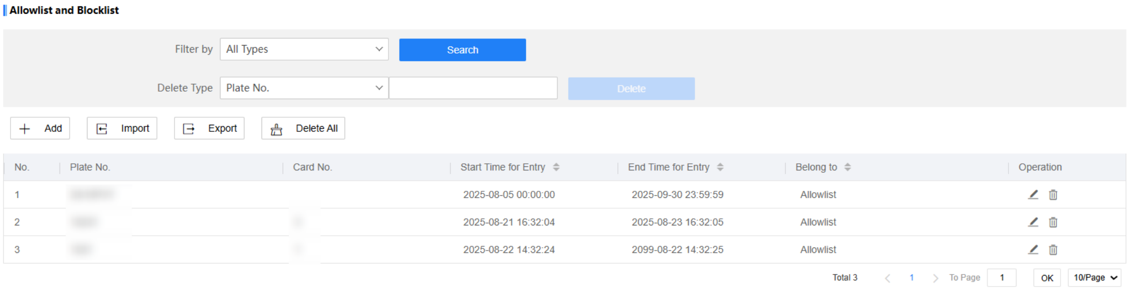
      Time settings is only available for the allowlist vehicles.

   4) Click **OK** to save the current settings and exit, or click **Save and Continue** to save the current settings and add other vehicles continuously.

      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.



Allowlist and Blocklist

Filter by: All Types — Search

Delete Type: Plate No. — Delete

No.	Plate No.	Card No.	Start Time for Entry	End Time for Entry	Belong to	Operation
1	[redacted]		2025-08-05 00:00:00	2025-09-30 23:59:59	Allowlist	✎ 🗑
2	[redacted]	[redacted]	2025-08-21 16:32:04	2025-08-23 16:32:05	Allowlist	✎ 🗑
3	[redacted]	[redacted]	2025-08-22 14:32:24	2099-08-22 14:32:25	Allowlist	✎ 🗑

Figure 4-1 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.

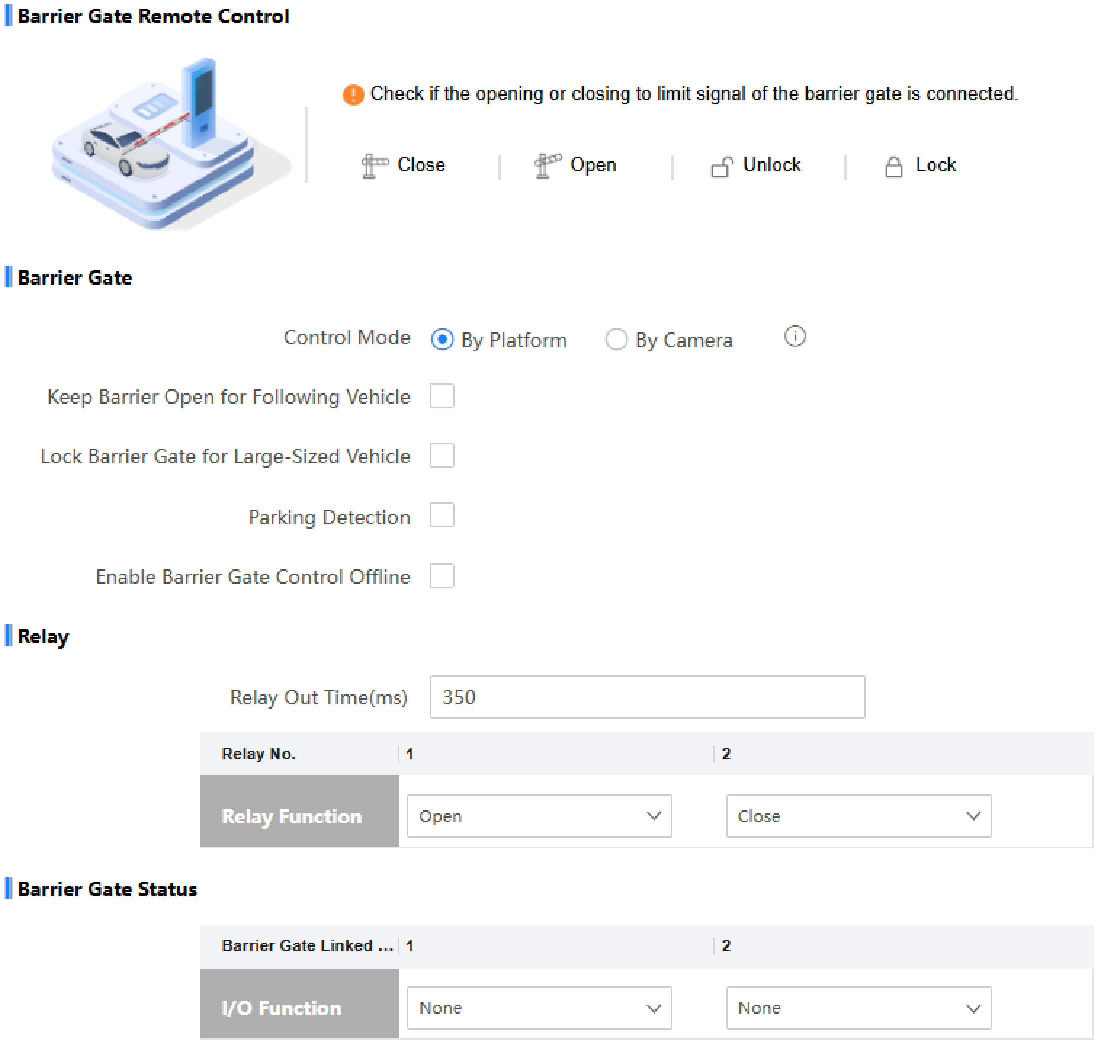
Export Click **Export**, and the list will be saved to the default downloading directory of the browser in the format of .xls.

4.1.2 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** .



Barrier Gate Remote Control

Check if the opening or closing to limit signal of the barrier gate is connected.

Close | Open | Unlock | Lock

Barrier Gate

Control Mode ● By Platform ○ By Camera

Keep Barrier Open for Following Vehicle □

Lock Barrier Gate for Large-Sized Vehicle □

Parking Detection □

Enable Barrier Gate Control Offline □

Relay

Relay Out Time(ms) 350

Relay No.	1	2
Relay Function	Open	Close

Barrier Gate Status

Barrier Gate Linked ...	1	2
I/O Function	None	None

Figure 4-2 Control Barrier Gate

2. Set **Barrier Gate** parameters.

   Control Mode

   - **By Platform**: Select this mode in the scene in which the entry permissions are controlled by the software.
   - **By Camera**: Select this mode 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 **Pass Control**.

   Keep Barrier Open for Following Vehicle

   Enable the function to keep the barrier gate 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 **Lock Duration**. If a large-sized vehicle is passing, the barrier gate will be locked during the set time.

Parking Detection

Enable the function and set **Judging Time**. If a vehicle has been parked for a duration longer than the set judging time, the parking information will be uploaded.

Enable Barrier Gate Control Offline

If you select **Control Mode** as **By Platform**, you can check **Enable Barrier Gate Control Offline** to control the barrier gate when the device is offline. Select **Barrier Gate Control When Platform Disconnection**. You can select to remain the barrier gate open or control the barrier gate by camera when the platform is disconnected.

3. Set **Relay** parameters.

   Relay Out Time

   Alarms will be output during the set time.

   Relay Function

   Select the functions of corresponding relays. Relay 1 corresponds to the 1A and 1B of the terminal. Relay 2 corresponds to the 2A and 2B of the terminal.

4. Select **I/O Function** for the corresponding barrier gate related I/O. The device will upload barrier gate status information for convenient entrance and exit management.

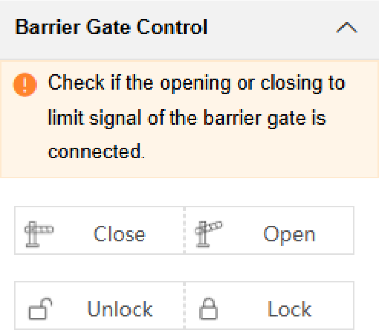
Note

- If the device only have one I/O interface, and the trigger type is **I/O Trigger**, the barrier status cannot be configured.
- If the trigger type is **Dual I/O Trigger** and the trigger I/O and logic I/O are selected, the corresponding barrier gate related I/O function cannot be configured. E.g., the trigger I/O is I/O 1 and the logic I/O is I/O 2. Then the barrier gate related I/O 1 and I/O 2 functions cannot be configured.

5. **Optional:** Click **Close**, **Open**, **Unlock**, or **Lock** in **Barrier Gate Remote Control** to control the barrier gate remotely.

Note

- Ensure the opening or closing to limit signal of the barrier gate is connected.
- You can also go to **Live View → Barrier Gate Control** to control the barrier gate remotely.



Barrier Gate Control

Check if the opening or closing to limit signal of the barrier gate is connected.

6. Click **Save**.

4.1.3 Pass Control

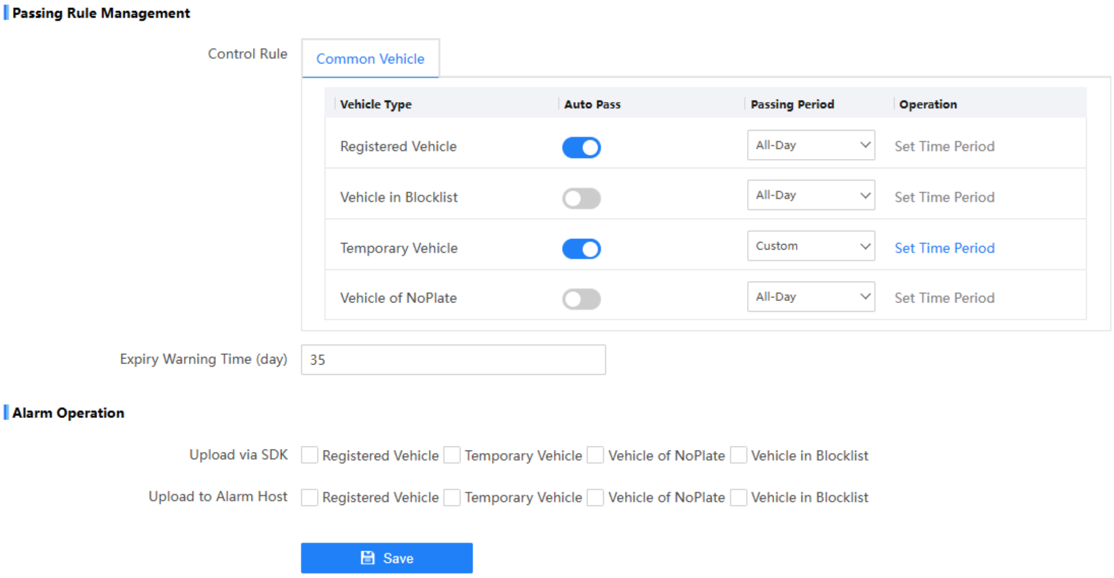
The camera can control the passing rules of different types of vehicles, and upload alarm information.

Before You Start

- Select the barrier gate control mode as **By Camera**. Refer to ***Control Barrier Gate*** for details.
- Set the allowlist and blocklist. Refer to ***Set Allowlist and Blocklist*** for details.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Pass Control** .



Passing Rule Management

Control Rule: Common Vehicle

Vehicle Type	Auto Pass	Passing Period	Operation
Registered Vehicle	●	All-Day	Set Time Period
Vehicle in Blocklist	○	All-Day	Set Time Period
Temporary Vehicle	●	Custom	Set Time Period
Vehicle of NoPlate	○	All-Day	Set Time Period

Expiry Warning Time (day): 35

Alarm Operation

Upload via SDK ☐ Registered Vehicle ☐ Temporary Vehicle ☐ Vehicle of NoPlate ☐ Vehicle in Blocklist

Upload to Alarm Host ☐ Registered Vehicle ☐ Temporary Vehicle ☐ Vehicle of NoPlate ☐ Vehicle in Blocklist

Figure 4-3 Pass Control

2. Set the passing rules for different types of vehicles.

1) Enable **Auto Pass** or not for vehicles in allowlist, vehicles in blocklist, temporary vehicles, and vehicles of no plates.
2) Set **Passing Period**.

All-Day

The corresponding type of vehicles can pass automatically all day.

Custom

The corresponding type of vehicles can pass automatically at the set time period. Click **Set Time Period** to set the auto passing time period of each day. Up to 5 passing periods can be set for each day. The setting method is same with setting capture schedule. Refer to ***Set Capture Schedule*** for details.

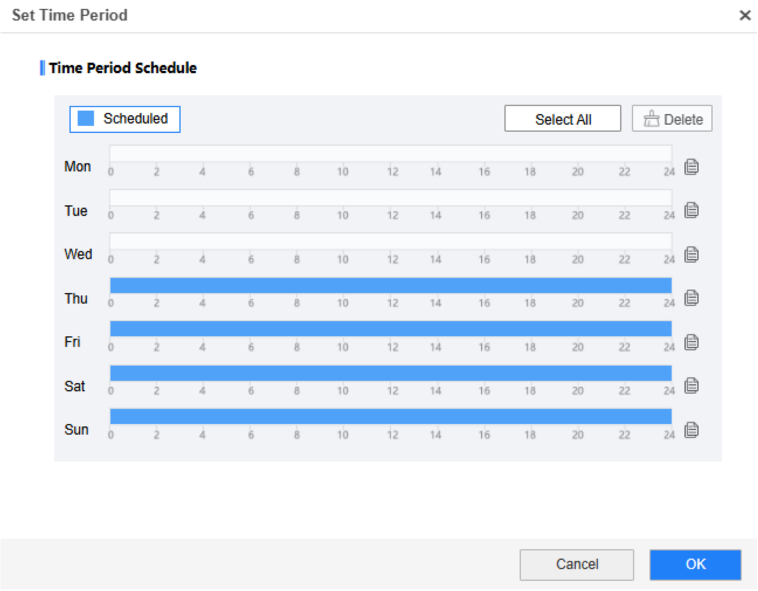


Figure 4-4 Set Custom Auto Passing Time Period

3) Set **Expiry Warning Time**. The set passing rule will expire after the set time.

Note

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

3. Select the vehicle type(s) of which the alarm information will be uploaded via SDK or to alarm host.

Upload via SDK

If the device has been connected to the platform, you can arm and upload the vehicle information to the arming terminal via SDK.

Upload to Alarm Host

If the device has been connected to the alarm device, when the barrier gate is open, the alarm device will be triggered to alarm.

4. Click **Save**.

4.2 Set Wiegand Parameters

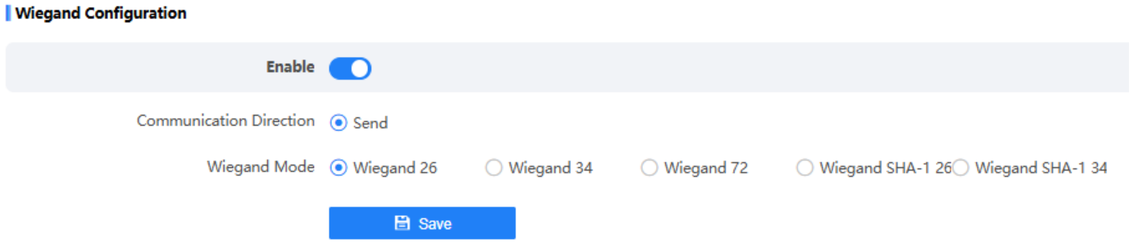
The device can get access to the access control system or other system supporting Wiegand protocols to send data in the entrance and exit scenes.

Steps

Note

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

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



Wiegand Configuration

Enable: On

Communication Direction: ● Send

Wiegand Mode: ● Wiegand 26 ○ Wiegand 34 ○ Wiegand 72 ○ Wiegand SHA-1 26 ○ Wiegand SHA-1 34

Figure 4-5 Set Wiegand Parameters

3. Select **Communication Direction**.

   Send

   The barrier gate can be connected to the device via Wiegand 26, Wiegand 34, Wiegand 72, or Wiegand sha1 26 protocol.

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.

   Wiegand 72

   It is a non-standard Wiegand protocol. The device will get the card No. (up to 9 characters only including 0 to 9, uppercase, or lowercase can be sent) 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 72 protocol.

Wiegand SHA-1 26

It is a data transmission format integrating Wiegand protocol and SHA-1 hash algorithm. This format increases SHA-1 hash value based on the standard Wiegand 26-bit data frame to raise the data security and integrity.

Wiegand SHA-1 34

It is a data transmission format integrating Wiegand protocol and SHA-1 hash algorithm. This format increases SHA-1 hash value based on the standard Wiegand 34-bit data frame to raise the data security and integrity.

5. **Optional:** If you select Wiegand SHA-1 26 or Wiegand SHA-1 34, you can enable MSB (Most Significant Bit) to verify the format and content of the data frame to raise the system security and stability.
6. Click **Save**.

4.3 Set Custom License Plate Mapping

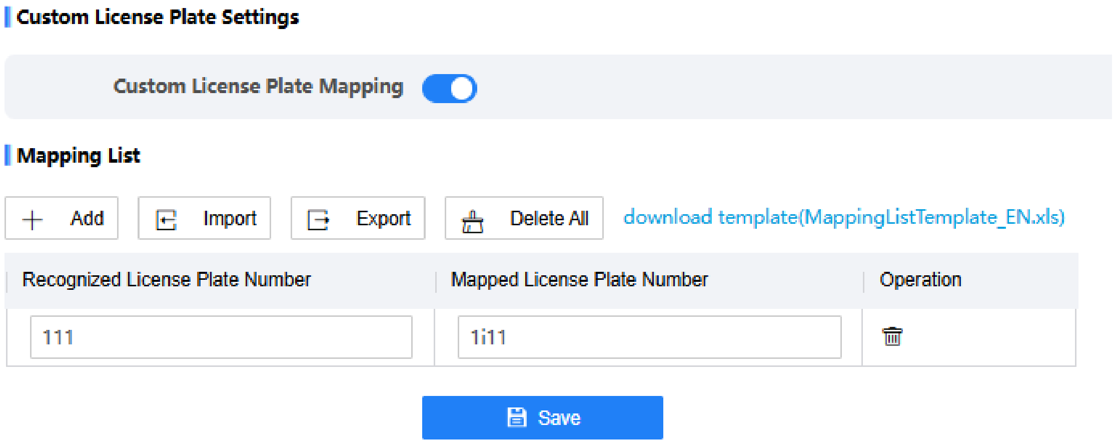
In some conditions, the recognized license plate number is inconsistent with the actual one. You can add the license plate mapping list to correct the recognized license plate number.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Mapping List** .
2. Enable **Custom License Plate Mapping**.
3. Add a mapping list.
   1) Click **Add** to add an item.
   2) Enter **Recognized License Plate Number** and **Mapped License Plate Number**.
   3) Click **Save**.

Note

Up to 64 items can be added.



Custom License Plate Settings

Custom License Plate Mapping ●

Mapping List

Add | Import | Export | Delete All | download template(MappingListTemplate_EN.xls)

Recognized License Plate Number	Mapped License Plate Number	Operation
111	1i11	🗑

Save

Figure 4-6 Add Mapping List

4. You can import, export, or delete the mapping list.

Delete
- Click 🗑 to delete the item.
- Click **Delete All** to delete all the lists.

Import
a. Click **download template**, and save the template.
b. Open the template, edit the information, and save it.
c. Click **Import**.
d. Select the edited template to import the mapping list in batch.

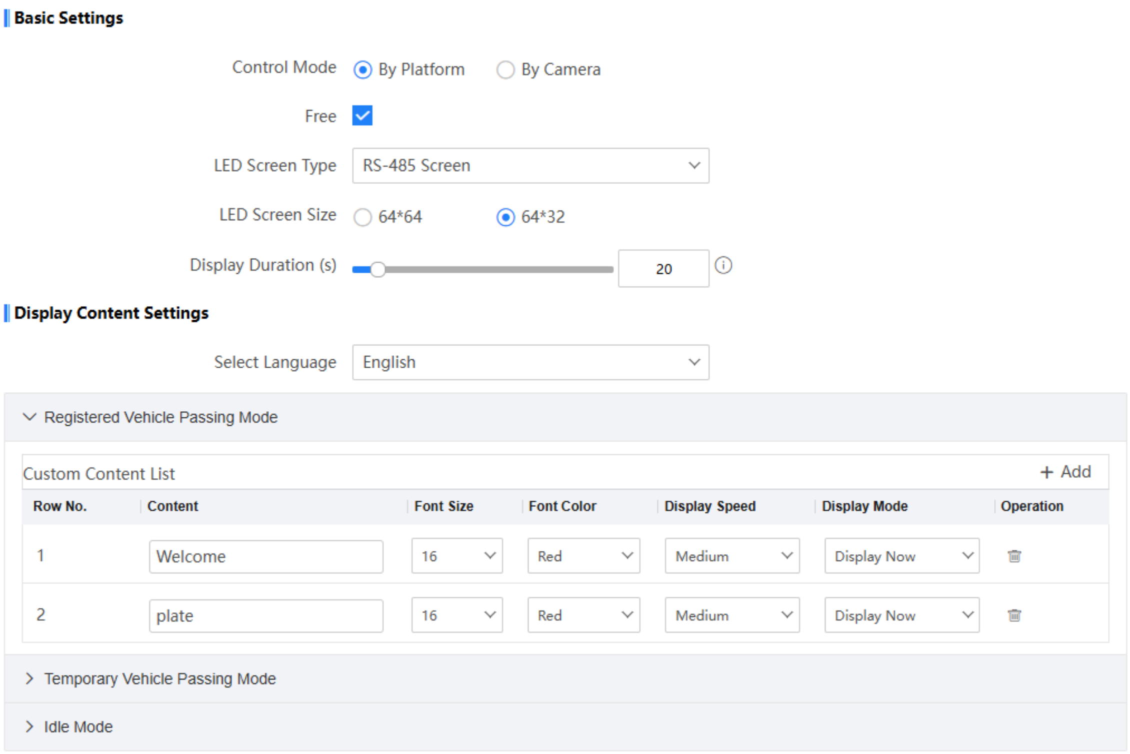
Export Click **Export**, and the mapping list will be saved to the default downloading directory of the browser in the format of .xls.

4.4 Set LED Display

When the device is connected with a LED display, or the device is equipped with a LED display, you can set the display information on the screen.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → LED Display Settings** .



Basic Settings

Control Mode ● By Platform ○ By Camera

Free ☑

LED Screen Type: RS-485 Screen

LED Screen Size ○ 64*64 ● 64*32

Display Duration (s): 20

Display Content Settings

Select Language: English

Registered Vehicle Passing Mode

Custom Content List + Add

Row No.	Content	Font Size	Font Color	Display Speed	Display Mode	Operation
1	Welcome	16	Red	Medium	Display Now	🗑
2	plate	16	Red	Medium	Display Now	🗑

Temporary Vehicle Passing Mode

Idle Mode

Figure 4-7 Set LED Display

2. Set the basic parameters.

Control Mode

- **By Platform**: Select this mode in the scene in which the entry permissions are controlled by the software.
- **By Camera**: Select this mode 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 **Pass Control**.

Free

Check it to enable the screen to display the content in idle mode. Set **Display Duration** which is the duration after displaying the content in vehicle passing mode and before displaying the content in idle mode.

LED Screen Type

If you select **Network Screen**, set the IP address and port No. of the screen.

Note

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

LED Screen Size

Select the LED screen size.

3. Set the display content in vehicle passing and idle modes.

1) Select the language.
2) Expand the menu of corresponding mode.
3) Click **Add** to add a content row.

Note

The supported display rows vary with different models. The actual device prevails.

4) Click the text field of content, select or enter the display content, and click **OK**.

Note

Use & to separate the content.

5) Set **Font Size**, **Font Color**, **Display Speed**, and **Display Mode**.
6) **Optional:** Click 🗑 to delete the row.

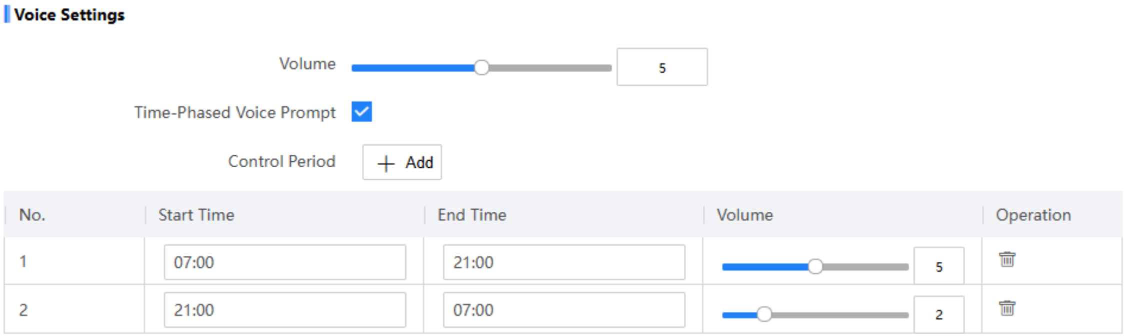
4. Click **Save**.

4.5 Set Voice Prompt

When the device is connected with a loudspeaker, or equipped with a loudspeaker, you can set the voice prompt.

Steps

1. Go to **Configuration → Capture → Entrance and Exit → Voice Prompt** .
2. Set voice prompt parameters.



Voice Settings

Volume: 5

Time-Phased Voice Prompt ☑

Control Period: + Add

No.	Start Time	End Time	Volume	Operation
1	07:00	21:00	5	🗑
2	21:00	07:00	2	🗑

Figure 4-8 Set Voice Prompt Parameters

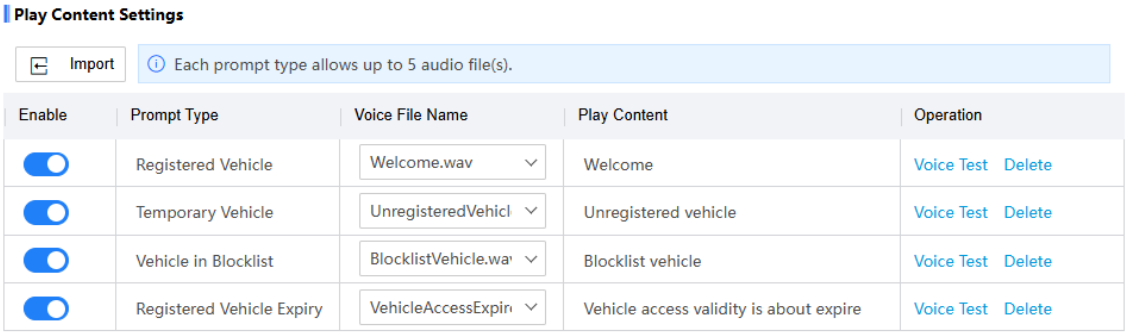
Volume

Adjust the voice volume.

Time-Phased Voice Prompt

Enable the function to play the voice prompt at fixed time period. Click **Add** to add a time period. Set **Start Time** and **End Time** of the time period, and adjust **Volume**. You can click 🗑 to delete the time period.

3. Import the voice prompt files.



Play Content Settings

Import

ⓘ Each prompt type allows up to 5 audio file(s).

Enable	Prompt Type	Voice File Name	Play Content	Operation
●	Registered Vehicle	Welcome.wav	Welcome	Voice Test Delete
●	Temporary Vehicle	UnregisteredVehicl	Unregistered vehicle	Voice Test Delete
●	Vehicle in Blocklist	BlocklistVehicle.wa	Blocklist vehicle	Voice Test Delete
●	Registered Vehicle Expiry	VehicleAccessExpir	Vehicle access validity is about expire	Voice Test Delete

Figure 4-9 Import Voice Prompt Files

1) Click **Import**.

2) Enter **Play Content**.

3) Select **Prompt Type** for the play content.

4) Click **Browse** to select the voice prompt file from the computer, and click **Import** to import it to the device.

5) Repeat the steps above to import more voice prompt files.

6) Enable the voice prompt(s).

7) **Optional:** Click **Voice Test** to test the actual voice prompt effect. Click **Delete** to delete it.

Note

- Each prompt type allows up to 5 audio file(s).
- Mono audio files in .wav format with 16-bit depth and 8 kHz sampling rate allowed.

4. Click **Save**.

4.6 Set Main and Sub-Camera Mode

In entrance and exit scenes, a main camera can be cooperated with a sub-camera to upload the captured pictures of the sub-camera to the connected platform.

Before You Start

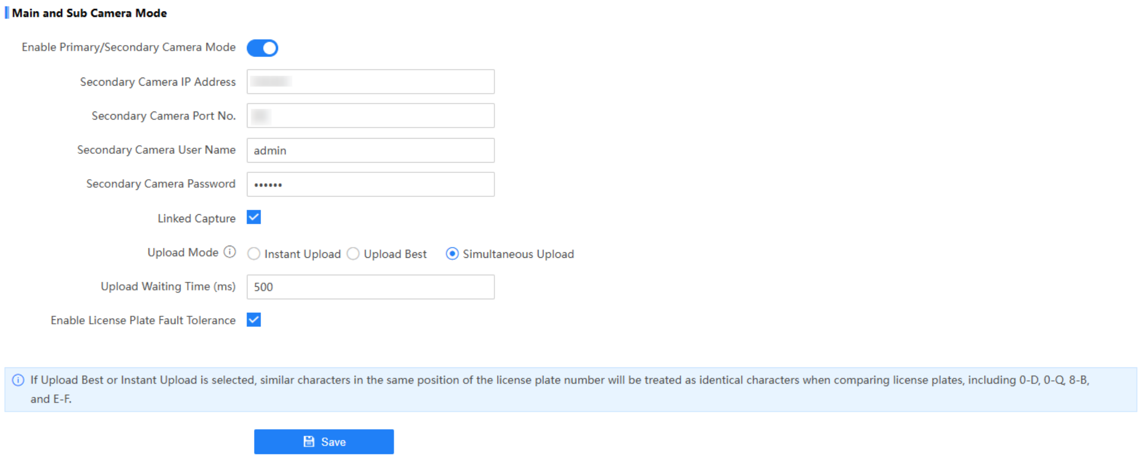
Disable the close-up picture capture of the main and sub-cameras before use.

Steps

Note

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

1. Go to **Configuration → Capture → Entrance and Exit → Main and Sub Camera Mode** .
2. Enable the function.



Main and Sub Camera Mode

Enable Primary/Secondary Camera Mode: on

Secondary Camera IP Address: [redacted]

Secondary Camera Port No.: [redacted]

Secondary Camera User Name: admin

Secondary Camera Password: ••••••

Linked Capture ☑

Upload Mode ○ Instant Upload ○ Upload Best ● Simultaneous Upload

Upload Waiting Time (ms): 500

Enable License Plate Fault Tolerance ☑

If Upload Best or Instant Upload is selected, similar characters in the same position of the license plate number will be treated as identical characters when comparing license plates, including 0-D, 0-Q, 8-B, and E-F.

Figure 4-10 Set Main and Sub-Camera Mode

3. Enter the IP address, port No., user name, and password of the sub-camera.
4. Enable **Linked Capture** to enable the sub-camera to capture pictures too.
5. Set other parameters.

Upload Mode

Instant Upload

Upload data immediately after capturing vehicles. The latter captured data will not be uploaded if the main/sub-camera (another camera) captures the same license plate during the upload waiting time. If a different license plate is captured, the data will be uploaded, and the waiting time will be reset.

Upload Best

After a vehicle is captured, if the main/sub-camera (another camera) captures the same license plate, the capture data with higher confidence will be uploaded. If no second capture within the waiting time, the previous data will be uploaded.

Simultaneous Upload

The captured data from the main/sub-camera will be uploaded via the main camera.

Note

If **Upload Best** or **Instant Upload** is selected, similar characters in the same position of the license plate number will be treated as identical characters when comparing license plates, including 0-D, 0-Q, 8-B, and E-F.

Upload Waiting Time

The time interval between two uploads.

Enable License Plate Fault Tolerance

Enable this function to enable fuzzy matching of license plates. The license plate color or state/province will not be matched. Up to 1 character will be matched fuzzily. For example, the license plate of a registered vehicle is 10-85538, but the recognized license plate is 10-85638. If license plate fault tolerance is enabled, the recognize license plate also belongs to the type of registered vehicle.

6. Click **Save**.

4.7 Peripheral Control

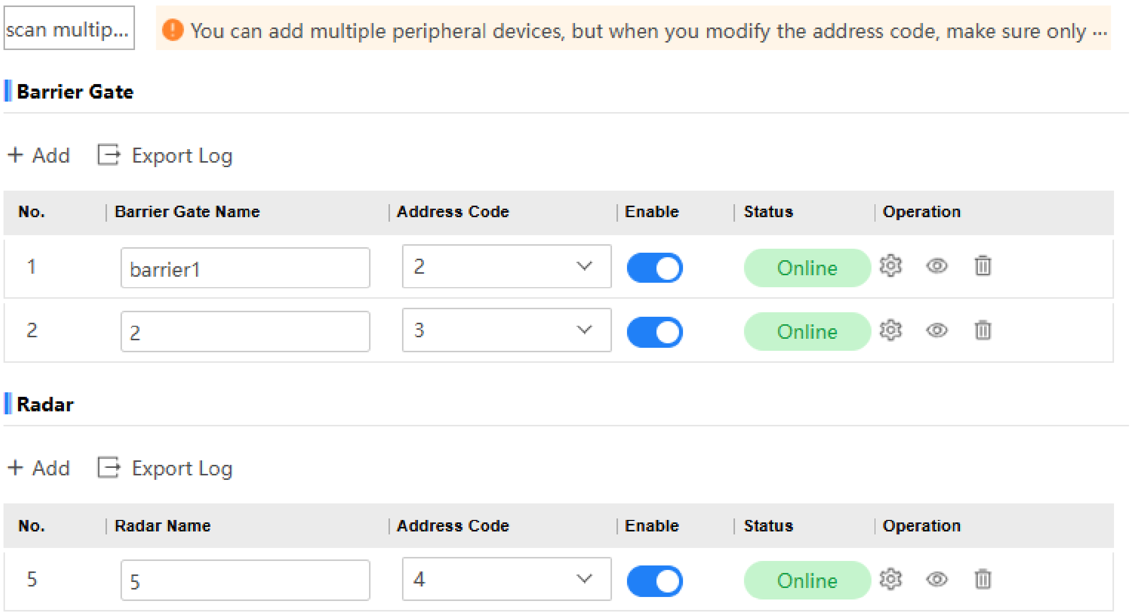
The device supports adding peripheral devices such as barrier gates and radars. You can edit the address codes, enable the peripheral devices, set the parameters, and export logs.

Steps

Note

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

1. Go to **Configuration → Capture → Entrance and Exit → Peripheral Control** .



scan multip...

You can add multiple peripheral devices, but when you modify the address code, make sure only ...

Barrier Gate

+ Add Export Log

No.	Barrier Gate Name	Address Code	Enable	Status	Operation
1	barrier1	2	●	Online	⚙ 👁 🗑
2	2	3	●	Online	⚙ 👁 🗑

Radar

+ Add Export Log

No.	Radar Name	Address Code	Enable	Status	Operation
5	5	4	●	Online	⚙ 👁 🗑

Figure 4-11 Peripheral Control

2. Click **Scan Multiple Peripheral Devices** to scan the connected peripheral devices of the current device.
3. Click **Add** to add a barrier gate or radar.
4. Edit the peripheral device name, select **Address Code**, and enable them.

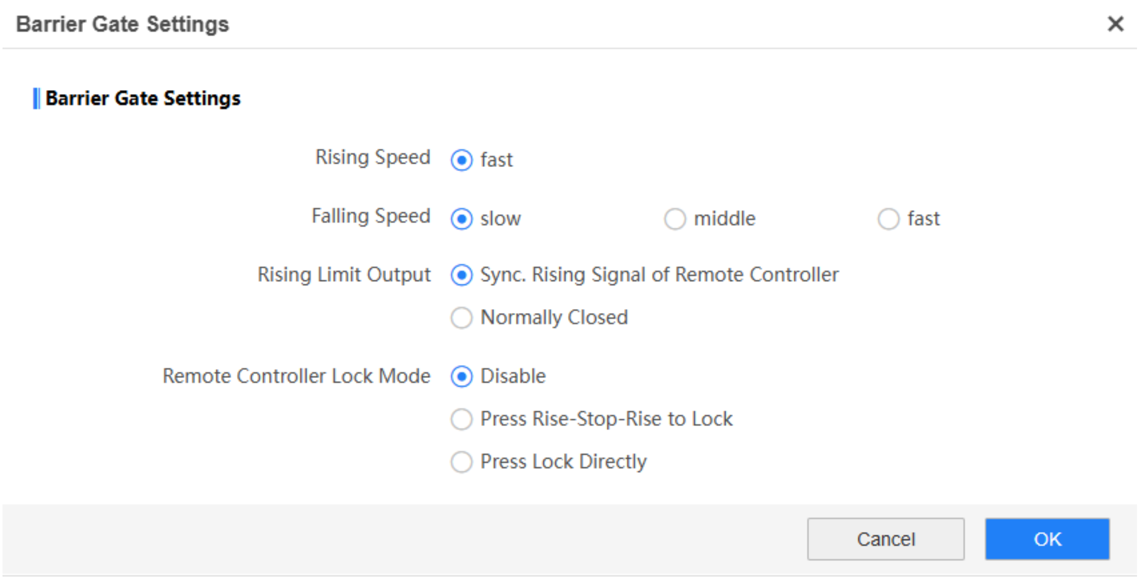
Note

You can add multiple peripheral devices, but when you modify the address code, make sure only peripheral device is connected.

Result: When the status shows online, the peripheral device is enabled successfully.

5. **Optional:** Other operations.

- Click ⚙ to set the barrier gate or radar parameters.



Barrier Gate Settings ✕

Barrier Gate Settings

Rising Speed ● fast

Falling Speed ● slow ○ middle ○ fast

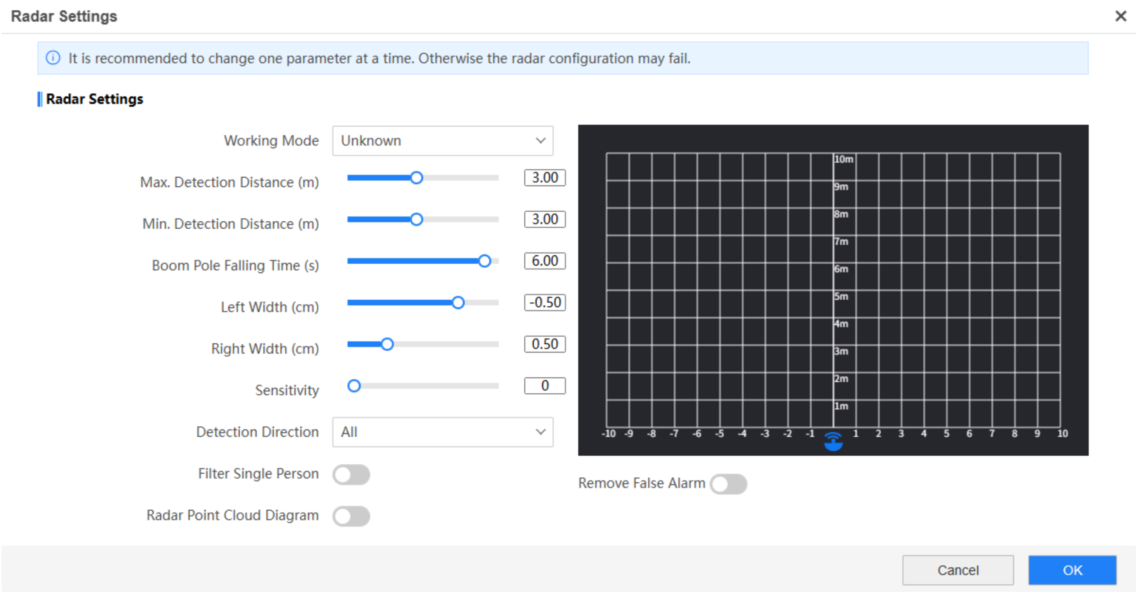
Rising Limit Output ● Sync. Rising Signal of Remote Controller ○ Normally Closed

Remote Controller Lock Mode ● Disable ○ Press Rise-Stop-Rise to Lock ○ Press Lock Directly

Figure 4-12 Set Barrier Gate Parameters

Table 4-1 Barrier Gate Parameters

Parameters	Description
Rising Limit Output	◦ **Sync. Rising Signal of Remote Controller**: To sync. the rising limit output of the barrier gate with the rising signal of the remote controller. ◦ **Normally Closed**: To disable rising limit output of the barrier gate.
Remote Controller Lock Mode	◦ **Disable**: To disable remote controller lock mode. ◦ **Press Rise-Stop-Rise to Lock**: To press Rise, Stop, and Rise buttons on the remote controller one by one to lock the barrier gate. ◦ **Press Lock Directly**: To press Lock button on the remote controller directly to lock the barrier gate.



Radar Settings

It is recommended to change one parameter at a time. Otherwise the radar configuration may fail.

Radar Settings

Working Mode: Unknown

Max. Detection Distance (m): 3.00

Min. Detection Distance (m): 3.00

Boom Pole Falling Time (s): 6.00

Left Width (cm): -0.50

Right Width (cm): 0.50

Sensitivity: 0

Detection Direction: All

Filter Single Person

Radar Point Cloud Diagram

Remove False Alarm

Figure 4-13 Set Radar Parameters

Table 4-2 Barrier Gate Parameters

Parameters	Description
Working Mode	Select the working mode according to the actual scene. ◦ **Trigger Mode**: The radar is used as a trigger radar. ◦ **Anti-Fall Single Boom Pole**: The radar is used as an anti-fall radar in the scene with a single boom pole. ◦ **Advertisement Boom Pole on Radar Left**: The radar is installed on the right of the advertisement boom pole. ◦ **Advertisement Boom Pole on Radar Right**: The radar is installed on the left of the advertisement boom pole.
Max./Min. Detection Distance	The max./min. distance that the radar can detect. The targets outside the max. distance or within the min. distance cannot be detected by the radar.
Boom Pole Falling Time	The waiting time between the time that the radar confirms there is no target in the detection range after the vehicle is passing totally and the time that the radar sends the command that the boom pole can fall down.
Left/Right Width	Set the horizontal range of the radar detection area.
Sensitivity	The higher the value, the easier to detect small targets. Adjust the value according to the actual scene. In mixed entrance and exit

Parameters	Description
	scenes, you're recommended to set relatively high sensitivity to avoid the boom pole from smashing vehicles or pedestrians.
Detection Direction	Select the radar detection direction according to the installation in the scene.
Filter Single Person	Enable the function, and when the radar detects a single person passing through the detection area, it will not send the command of rising the boom pole to the barrier gate.
Radar Point Cloud Diagram	Enable the function to view the radar detection area and the detected targets intuitively.
Remove False Alarm	Enable the function to filter the false alarms such as detecting other still objects as vehicles.

Note

It is recommended to change one parameter at a time. Otherwise the radar configuration may fail.

- Click 👁 to view the read back information of the barrier gate and radar.
- Click 🗑 to delete the added barrier gate or radar.
- Click **Export Log** to export the logs of the selected barrier gate or radar during the set start and end time.

Chapter 5 Capture Configuration

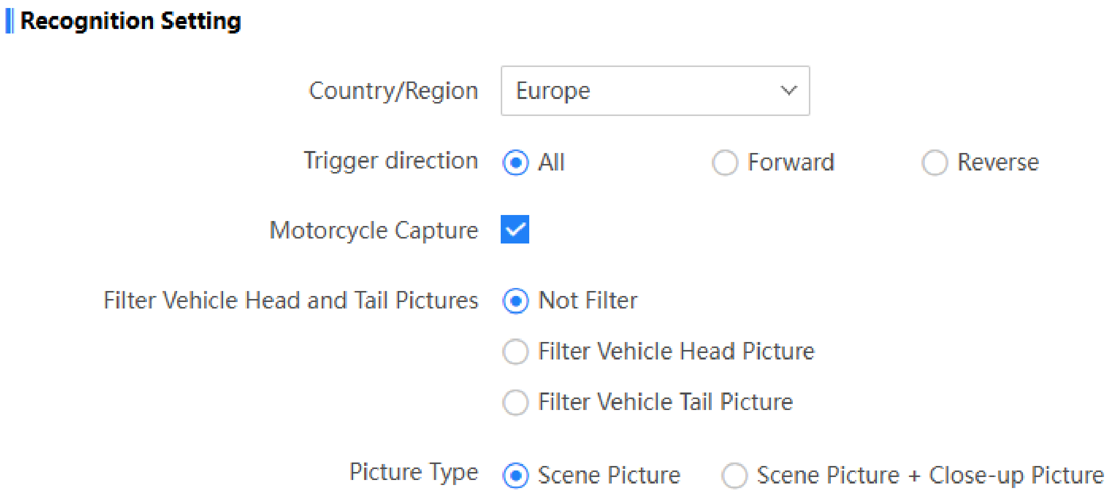
5.1 Set Capture Parameters

5.1.1 Set License Plate Recognition Parameters

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

Steps

1. Go to **Configuration → Capture → Capture Parameters → Recognition Setting → Recognition Setting** .



Recognition Setting

Country/Region: Europe

Trigger direction: ● All ○ Forward ○ Reverse

Motorcycle Capture: ☑

Filter Vehicle Head and Tail Pictures: ● Not Filter ○ Filter Vehicle Head Picture ○ Filter Vehicle Tail Picture

Picture Type: ● Scene Picture ○ Scene Picture + Close-up Picture

Figure 5-1 Set License Plate Recognition Parameters

2. Set the following parameters.

   Country/Region

   Select the country/region in which the license plates will be recognized. If you select HongKong (China) or MaCao (China), you can select the region(s) in which the license plates will be recognized. The license plates in the unselected region(s) will not be recognized. You can also click ↑ / ↓ to adjust the recognition order. The license plates in the upper region will be recognized in priority.

   Trigger Direction

- Select **Forward** when license plates of vehicles from the approaching direction need to be recognized.
- Select **Reverse** when license plates of vehicles from the leaving direction need to be recognized.
- Select **All** when license plates of vehicles from both the approaching direction and the leaving direction need to be recognized.

Motorcycle Capture

Enable the function to capture pictures of non-motor vehicles.

Filter Vehicle Head and Tail Pictures

- **Not Filter**: Both the vehicle head and tail pictures will be captured.
- **Filter Vehicle Head Picture**: The vehicle head pictures will not be captured.
- **Filter Vehicle Tail Picture**: The vehicle tail pictures will not be captured.

Picture Type

Select the captured picture type. The device supports capturing the scene picture, or the scene picture and the close-up picture.

3. Click **Save**.

5.1.2 Set Vehicle Feature Parameters

Set vehicle feature parameters when you need to capture the passing vehicle according to the vehicle features.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Recognition Setting → Vehicle Feature** .
2. Check the vehicle features to be recognized.
3. Click **Save**.

5.1.3 Set Supplement Light Parameters

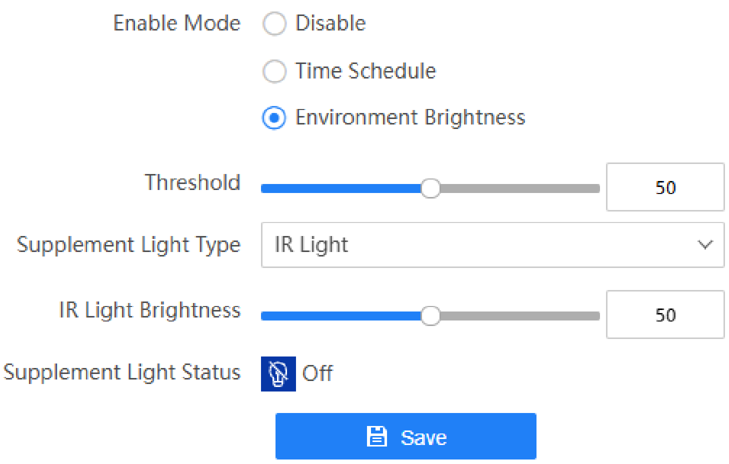
Supplement light can enhance the image stabilization and adjust the brightness and color temperature. It can supplement light at night or when the light is dim.

Steps

Note

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

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



Enable Mode ○ Disable
○ Time Schedule
● Environment Brightness

Threshold 50

Supplement Light Type IR Light

IR Light Brightness 50

Supplement Light Status Off

Figure 5-2 Set Supplement Light Parameters

2. Set the supplement light parameters according to actual conditions.

Enable Mode

Disable

Disable supplement light.

Time Schedule

Select it when you want the constant light to be enabled during fixed time period. Click **Time Schedule** to set the time periods to enable supplement light.

Environment Brightness

Select it when you want the constant light to be controlled by detecting the surroundings brightness automatically. Set the brightness threshold. The higher the threshold is, the harder the constant light can be enabled.

Supplement Light Type

Select IR light or white light.

Note

The supplement light types vary with different models. The actual device prevails.

White/IR Light Brightness

Drag the slider to adjust the brightness, or enter the value in the text field. The higher the brightness is, the more the light will be supplemented.

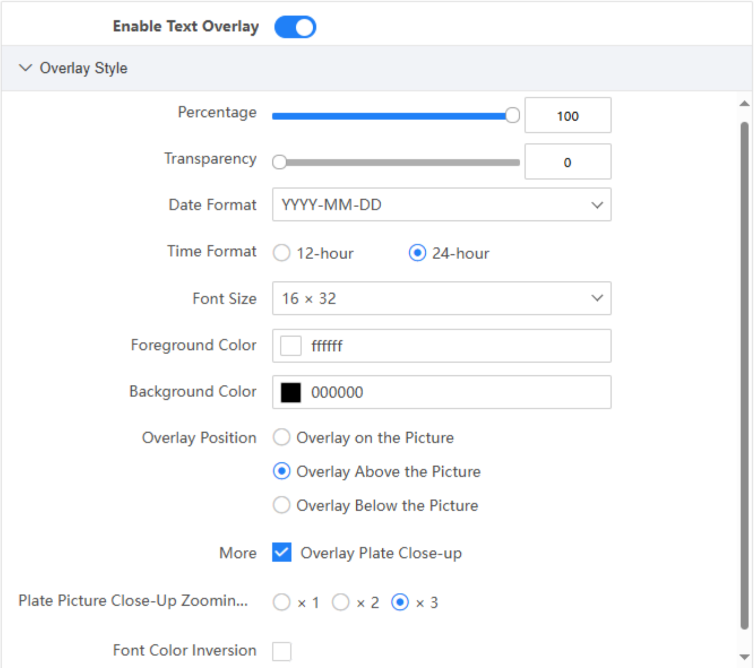
3. Click **Save**.

5.1.4 Set Capture Overlay

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

Steps

1. Go to **Configuration → Capture → Capture Parameters → Capture Overlay Configuration** .
2. Check **Enable Text Overlay**.
3. Set **Overlay Style**.



Enable Text Overlay ●

Overlay Style

Percentage 100

Transparency 0

Date Format YYYY-MM-DD

Time Format ○ 12-hour ● 24-hour

Font Size 16 × 32

Foreground Color □ ffffff

Background Color ■ 000000

Overlay Position ○ Overlay on the Picture ● Overlay Above the Picture ○ Overlay Below the Picture

More ☑ Overlay Plate Close-up

Plate Picture Close-Up Zoomin... ○ × 1 ○ × 2 ● × 3

Font Color Inversion □

Figure 5-3 Set Overlay Style

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.

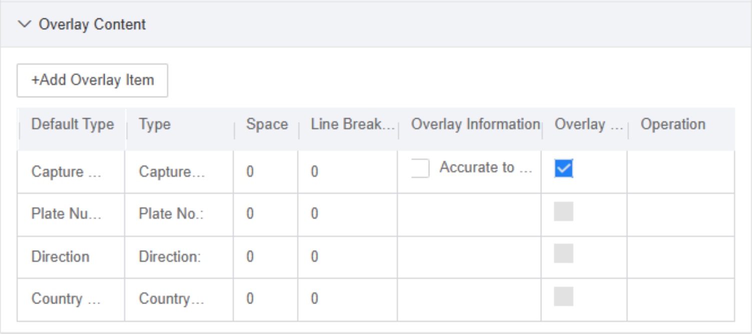
Overlay Plate Close-up

Enable the function to overlay a license plate close-up picture on the captured picture. Set **Plate Picture Close-Up Zooming Ratio** to adjust the close-up picture size.

Font Color Inversion

Enable the function to detect the gray level of the image overlaid position automatically. When the image color is dark, the overlaid characters will be displayed as white automatically. When the image color is light, the overlaid characters will be displayed as black automatically.

4. Set **Overlay Content**.



Default Type	Type	Space	Line Break...	Overlay Information	Overlay ...	Operation
Capture ...	Capture...	0	0	□ Accurate to ...	☑	
Plate Nu...	Plate No.:	0	0		□	
Direction	Direction:	0	0		□	
Country ...	Country...	0	0		□	

Figure 5-4 Set Single Picture Overlay Content

1) Click **Add Overlay Item** to select the information to overlay, and click **OK**.

Note

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

2) Set the parameters below.

- **Default Type**: You can view the default overlay information name. If you have edited the name, you can refer to the default name for the definition.
- **Type**: You can edit a custom overlay information name.
- **Space**: Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
- **Line Break Characters**: Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
- **Overlay Information**: For some information types, you can edit the detailed information.
- **Overlay Position**: If you check it, the current information will be displayed from a new line.
- **Operation**: You can click ↑ / ↓ to adjust the display sequence of the overlay information, or click 🗑 to delete the item.

5. Click **Capture Test** to test the information overlay effect.
6. Click **Save**.

5.1.5 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** .

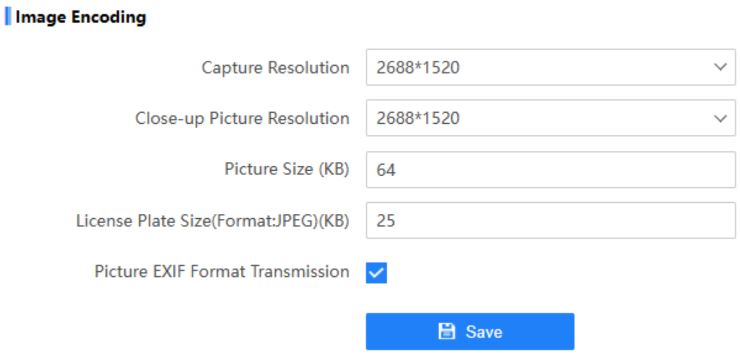


Image Encoding

Capture Resolution: 2688*1520

Close-up Picture Resolution: 2688*1520

Picture Size (KB): 64

License Plate Size(Format:JPEG)(KB): 25

Picture EXIF Format Transmission: ☑

Figure 5-5 Set Image Encoding Parameters

2. Set the parameters below.

   Capture Resolution

   Select the resolution of the captured scene picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

   Close-up Picture Resolution

   Select the resolution of the target close-up picture. When the picture size keeps the same, the higher the resolution, the more the picture will be compressed, and the slower the picture will be handled.

   Picture Size

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

   License Plate Size

   The size of the captured license plate close-up picture.

   Picture EXIF Format Transmission

   The captured pictures will be transmitted in the EXIF format.

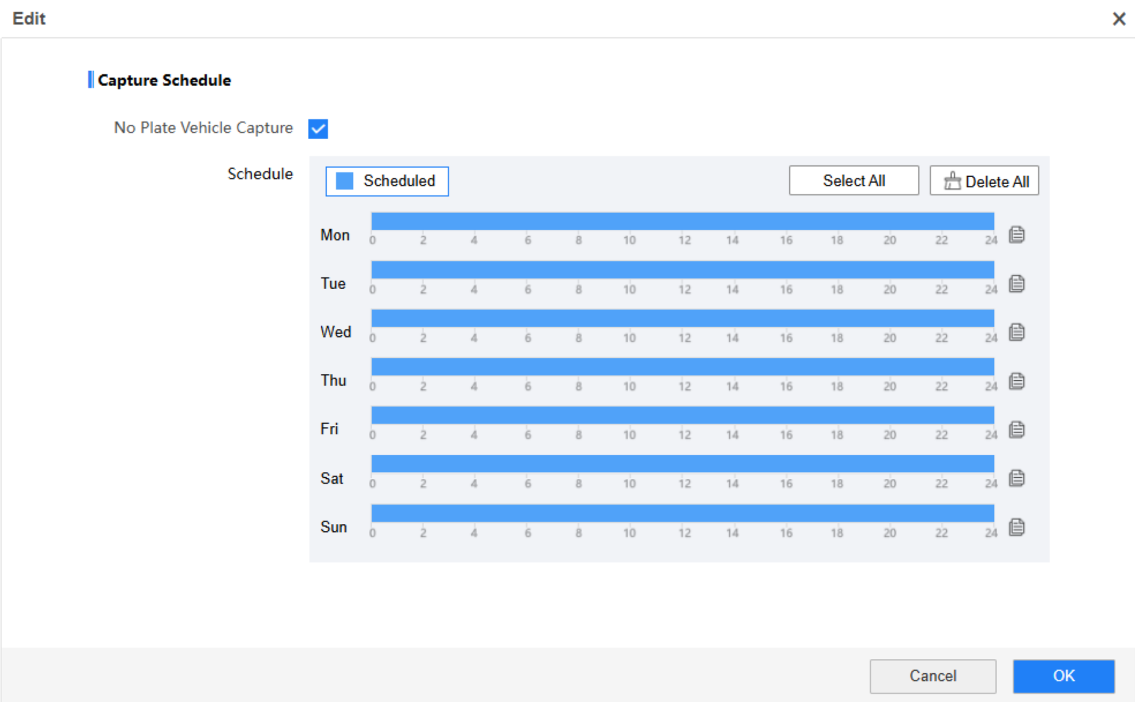
3. Click **Save**.

5.1.6 Set Capture Schedule

You can set the capture schedule of the device.

Steps

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



No Plate Vehicle Capture ☑

Figure 5-6 Set Capture Schedule

3. **Optional:** Enable **No Plate Vehicle Capture** to capture the vehicles without license plates if needed.
4. 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.
5. **Optional:** Click 🗐 to copy the same settings to other days.
6. Click **OK**.
7. **Optional:** Check **Upload to Mailbox** to email the capture schedule to the user.
8. Click **Save**.

5.2 Advanced Configuration

Note

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

5.2.1 System Service

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.

Show License Plate Frame

Enable the function to overlay license plate frames on the captured pictures.

Capture information debugging enable

Check to enable capture information debugging.

Enable Closed Positioning Frame

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

Capture Interval Enable

Check to enable parking vehicle detection. When there is parking vehicle detected, the device will capture pictures according to the set **Capture Interval Time**.

3. Click **Save**.

5.2.2 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. Check the service(s) according to your needs.

Note

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

Picture Upload

Time of Filtering Checkpoint Duplicate License Plates

It is used to debug the device with the same vehicle. When the same vehicle is triggered many times during the set time in the scene, the checkpoint pictures of the vehicle will not be captured.

Enable Vehicle Type Mapping

Enable the function, and when the device recognizes the vehicle types as shown in the figure left column below, the corresponding mapped vehicle type fields as shown in the figure right column below will be output for the OSD and the ANPR protocol message.

Table 5-1 Vehicle Type Mapping

Recognized Vehicle Type	Output Vehicle Type Field
Motorcycle	twoWheelVehicle
Mini bus, large bus, van	bus
Buggy, medium heavy truck	truck
SUV/MPV, pickup truck	vehicle

Slope Scene

Check **Enable Slope Scene** to enable the license plate recognition and capture in slope scenes.

Coil Triggered Capture

For I/O trigger and dual I/O trigger types, set the coil triggered capture parameters.

Coil Default Status

NO means the coils are enabled, and **NC** means the coils are disabled.

Capture Triggered Time

Select **Entry** to trigger capture when the vehicle is entering. Select **Exit** to trigger capture when the vehicle is exiting.

Focus Detection

Enable focus detection to detect the live view image. If the image is obscure, alarms will be triggered and uploaded to the platform or the connected terminal to prompt that the lens needs to be focused.

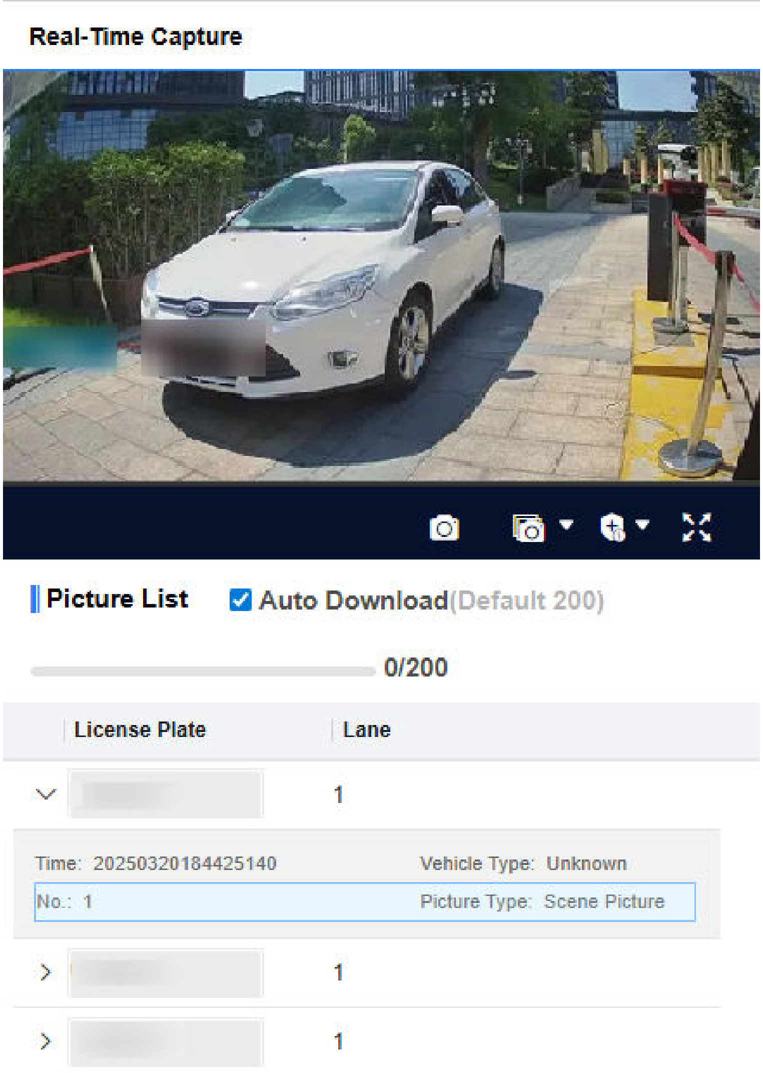
3. Click **Save**.

Chapter 6 View Real-Time Picture

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

Steps

1. Click **Live View**.
2. Click **Draw Lane Line** under the live view image, and adjust the detection area and trigger line according to the actual scene. Click **Save** to save the drawing.
3. Click **Arming** on the right **Real-Time Capture** window.
4. Select an item from the list, and you can view the capture scene picture and recognized license plate information.



Real-Time Capture

Picture List ☑ Auto Download(Default 200)

0/200

	License Plate	Lane
∨	[redacted]	1
	Time: 20250320184425140 No.: 1	Vehicle Type: Unknown Picture Type: Scene Picture
>	[redacted]	1
>	[redacted]	1

Figure 6-1 Real-Time Picture

5. **Optional:** Other operations.

/	• **Level 1 Arming**: Only the current computer can arm the device and receive the captured pictures in real time. The pictures will not be stored in the storage card. The pictures in the storage card will be uploaded to the level 1 arming terminal. • **Disarming**: Disable the real-time capture function.
	Click it to capture a picture manually.
	Click the arrow to set continuous capture parameters and then click the icon to enable continuous capture manually. The device will capture pictures according to the set interval.

	• **Trigger Channel**: If the camera has multiple channels, enter the channel No. to enable continuous capture. • **Waiting Time**: Set the interval between continuous captures when triggering continuous capture continuously. • **Capture Times**: Select the number of captured pictures per continuous capture. • **Interval**: Set the interval between each capture in the continuous capture. Up to four intervals can be set, and the default interval is 100 ms.
⛶	Click it to display the captured picture in full screen mode. Press **Esc** on the keyboard to exit from the full screen mode.
Open Folder	If the plug-in has been installed, the button will display on the interface. You can click it to open the saving path of captured pictures.
Auto Download	In no plug-in mode, you can enable **Auto Download** to download the captured pictures to the computer directly. The latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically. The max. number of pictures in one compressed file depends on the selected **Number of Auto Captured Pictures** in **Configuration → Local** in no plug-in mode. If you disarm, the auto downloading will stop. You can view the downloading progress on the interface. The auto downloaded files will be saved to the default downloading directory of the browser in the format of .zip. You can go to the directory, decompress the file, and view the captured pictures. If you disable **Auto Download**, when you disarm, the dialogue box will pop up to prompt you if you need to download the arming captures. Click **OK** and the latest captured pictures will be downloaded and compressed as a file in the format of .zip automatically.

Chapter 7 Live View and Local Configuration

7.1 Live View

7.1.1 Start/Stop Live View

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

7.1.2 Select Image Display Mode

Click ▣▾ to select an image display mode.

7.1.3 Select Window Division Mode

Click ▣▾ to select a window division mode.

7.1.4 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.

Note

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

7.1.5 Capture Picture Manually

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

Steps

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

7.1.6 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.

7.1.7 Enable Digital Zoom

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

Steps

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

   The area will be zoomed in.
4. Click any position of the image to restore to normal image.
5. Click ⊕ to disable digital zoom.

7.1.8 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.

7.1.9 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.

7.1.10 Select Video Mode

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

Click ▶▾ to select the normal mode when the device is running normally.

7.2 Set Snapshot Mode

Click **Live View**, and you can enable or disable snapshot mode on the upper right corner of the interface.

- ▣ : The snapshot mode is enabled. In this mode, only the image in the live view interface is in real-time streaming, and the live view images in other interfaces are just pictures. You can refresh the interfaces to refresh the pictures. For the conditions that the network is unstable, or the computer performance is not that good, you're recommended to enable snapshot mode to raise the operation efficiency.
- ▨ : The snapshot mode is disabled. All the live view images are in real-time streaming.

Note

Disable snapshot mode before drawing areas for cropping capture pictures, ROI, privacy mask, and regional exposure.

7.3 PTZ Operation

Click **Live View**. The **PTZ Control** menu is displayed on the left.

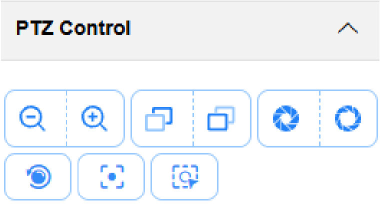


Figure 7-1 PTZ Control

Table 7-1 Button Description

Button	Description
⊕ / ⊖	Zoom + and Zoom -

Button	Description
	- Hold ⊕ to zoom in the scene. - Hold ⊖ to zoom out the scene.
⧉ / ⧉	Focus + and Focus - - Hold ⧉ 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 It is applicable to devices with motorized lenses. Use this function to focus the lens automatically and make images become clear.
⛶	Regional Auto Focus Click it and drag a rectangle on the live view image, and the area will be auto focused.

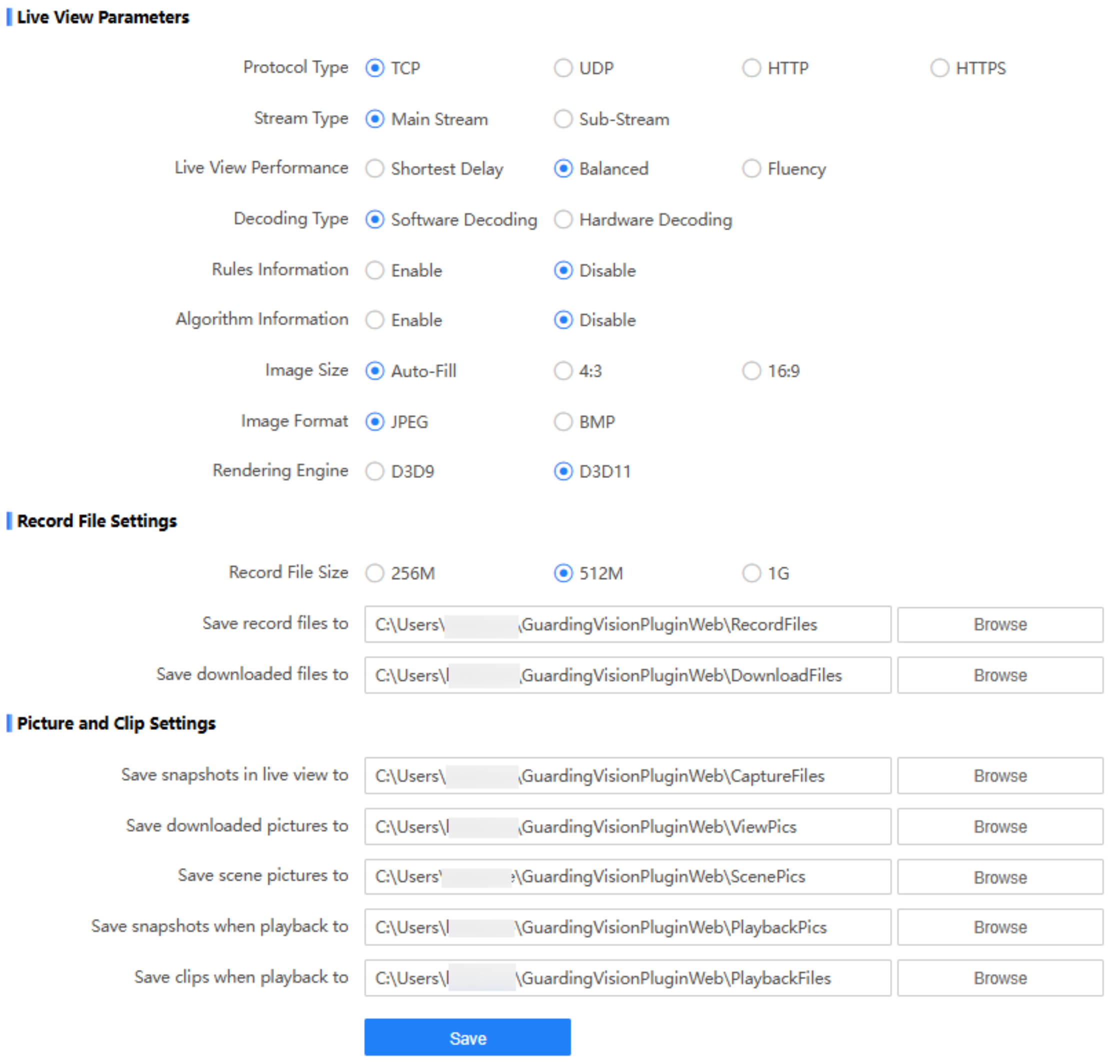
7.4 Local Configuration

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

Note

The interfaces in no plug-in mode and plug-in mode are different.

Local Configuration in Plug-in Mode



Live View Parameters

Protocol Type ● TCP ○ UDP ○ HTTP ○ HTTPS

Stream Type ● Main Stream ○ Sub-Stream

Live View Performance ○ Shortest Delay ● Balanced ○ Fluency

Decoding Type ● Software Decoding ○ Hardware Decoding

Rules Information ○ Enable ● Disable

Algorithm Information ○ Enable ● Disable

Image Size ● Auto-Fill ○ 4:3 ○ 16:9

Image Format ● JPEG ○ BMP

Rendering Engine ○ D3D9 ● D3D11

Record File Settings

Record File Size ○ 256M ● 512M ○ 1G

Save record files to C:\Users\[redacted]\GuardingVisionPluginWeb\RecordFiles Browse

Save downloaded files to C:\Users\[redacted]\GuardingVisionPluginWeb\DownloadFiles Browse

Picture and Clip Settings

Save snapshots in live view to C:\Users\[redacted]\GuardingVisionPluginWeb\CaptureFiles Browse

Save downloaded pictures to C:\Users\[redacted]\GuardingVisionPluginWeb\ViewPics Browse

Save scene pictures to C:\Users\[redacted]\GuardingVisionPluginWeb\ScenePics Browse

Save snapshots when playback to C:\Users\[redacted]\GuardingVisionPluginWeb\PlaybackPics Browse

Save clips when playback to C:\Users\[redacted]\GuardingVisionPluginWeb\PlaybackFiles Browse

Figure 7-2 Local Configuration in Plug-in Mode

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.

Algorithm 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.

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** .

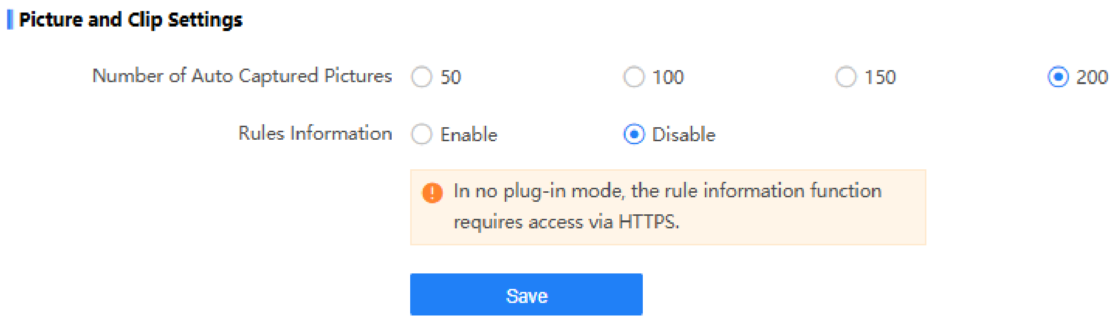
Save snapshots when playback to

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.

Local Configuration in No Plug-in Mode



Picture and Clip Settings

Number of Auto Captured Pictures ○ 50 ○ 100 ○ 150 ● 200

Rules Information ○ Enable ● Disable

In no plug-in mode, the rule information function requires access via HTTPS.

Figure 7-3 Local Configuration in No Plug-in Mode

Number of Auto Captured Pictures

Select the max. number of auto downloaded pictures in one compressed file in **Live View → Real-Time Capture** in no plug-in mode.

Rules Information

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

Note

In no plug-in mode, the rule information function requires access via HTTPS.

Chapter 8 Record and Capture

8.1 Set Storage Media

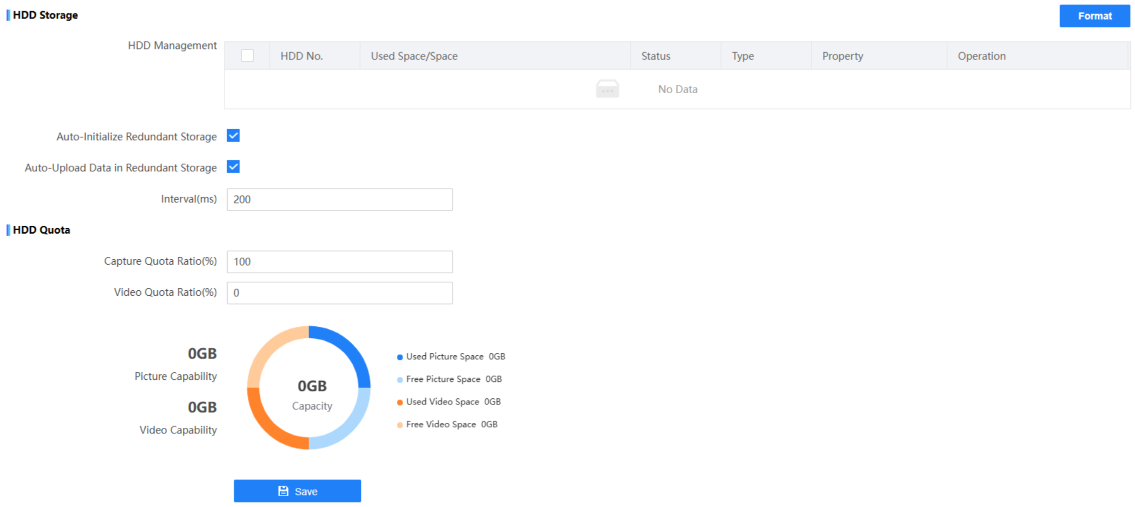
If you want to store the files to the storage media, make sure you install, format, and set the storage media in advance.

Before You Start

Install the storage media to the device.

Steps

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



HDD Storage

Format

HDD Management

□	HDD No.	Used Space/Space	Status	Type	Property	Operation
			No Data			

Auto-Initialize Redundant Storage ☑

Auto-Upload Data in Redundant Storage ☑

Interval(ms) 200

HDD Quota

Capture Quota Ratio(%) 100

Video Quota Ratio(%) 0

0GB Picture Capability

0GB Video Capability

0GB Capacity

Save

Figure 8-1 Set Storage Media

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

   Note

   For the newly installed storage media, you need to format it manually before using it normally.

   - If you want to format the storage media automatically when the media is abnormal, check **Auto-Initialize Redundant Storage**.
3. Set other parameters.

   Auto-Upload Data in Redundant Storage

   If the device has been connected to the platform, and you want to upload the storage media information automatically, enable the function and set the interval.
4. 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 %.

5. Click **Save**.

8.2 Set Record Schedule

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

Before You Start

Install the storage media.

Steps

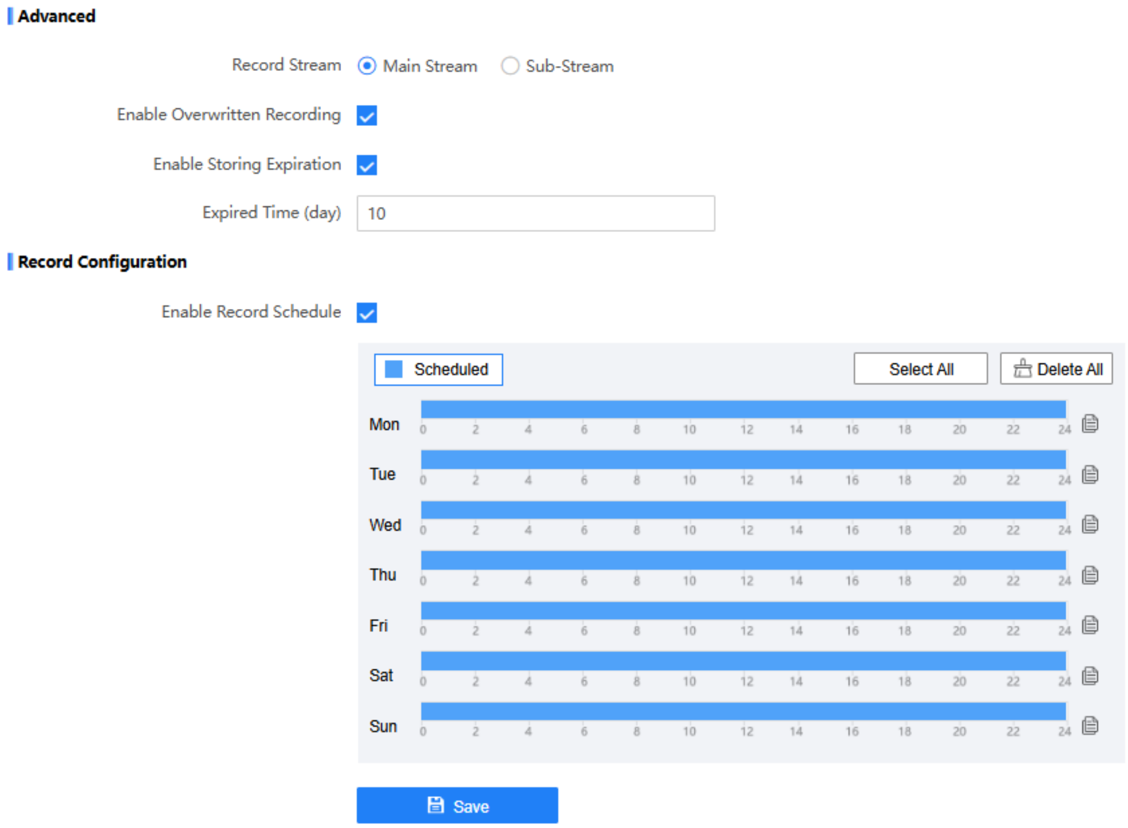
1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Select **Record Stream**.
3. **Optional:** Enable the functions below according to your needs.

   Enable Overwritten Recording

   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.
4. Enable the record schedule.



Advanced

Record Stream ● Main Stream ○ Sub-Stream

Enable Overwritten Recording ☑

Enable Storing Expiration ☑

Expired Time (day) 10

Record Configuration

Enable Record Schedule ☑

Figure 8-2 Set Record Schedule

5. Click **Select All** to enable the device to record the whole days. Or drag the cursor on the time bar to set a recording time.

Note

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

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 **Delete All** on the record configuration interface to delete all the schedules.
8. **Optional:** Click 🗐 to copy the settings to other days.
9. Click **Save**.

Result

The device will only record at the set periods.

8.3 Set Snapshot Schedule

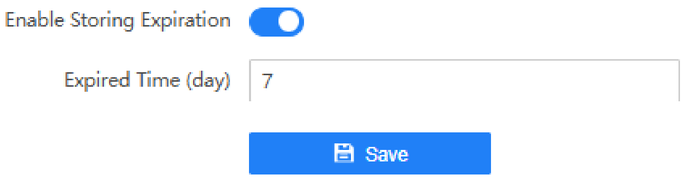
You can enable storage expiration of the snapshots saved in the storage media.

Before You Start

Install the storage media.

Steps

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



Enable Storing Expiration ●

Expired Time (day) 7

Figure 8-3 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 media will be overwritten.

Chapter 9 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.
   - Click ◎ to capture an image.
   - Click ✂ / ✂ to start/stop clipping the record.
   - 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**.
   - Click ■ to stop playback.
   - Click « to slow down the playback.
   - Click » to speed up the playback.
   - Click 🔍 / 🔍 to enable/disable digital zoom.
   - Click 🔇 to enable volume.

Chapter 10 Encoding and Display

10.1 Set Camera Parameters

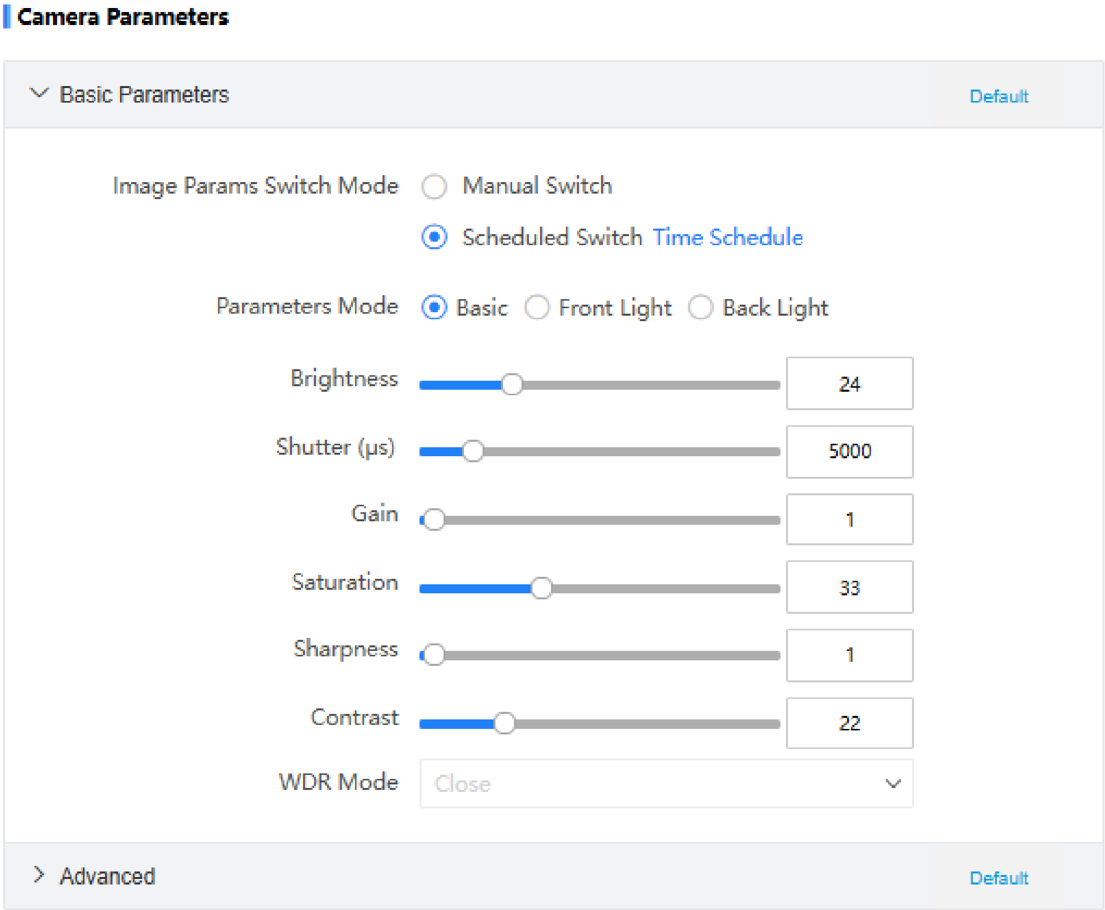
You can adjust the camera parameters to get clear image.

Steps

Note

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

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



Camera Parameters

Basic Parameters — Default

Image Params Switch Mode: ○ Manual Switch ● Scheduled Switch Time Schedule

Parameters Mode: ● Basic ○ Front Light ○ Back Light

Brightness: 24

Shutter (μs): 5000

Gain: 1

Saturation: 33

Sharpness: 1

Contrast: 22

WDR Mode: Close

Advanced — Default

Figure 10-1 Set Camera Parameters

2. Set the camera parameters.

Note

Click **Default** to reset parameters.

Basic Parameters

Image Params Switch Mode

- **Manual Switch**: The camera parameters set for the selected **Parameters Mode** will take effect.
- **Scheduled Switch**: Click **Time Schedule** to set the time periods during which the camera parameters set for the front light or back light mode take effect. Select the corresponding light, and drag the cursor on the time bar to set a time period. Up to 2 time periods can be set on a time bar totally. The camera parameters set for basic mode will take effect outside the set time periods of front light or back light.

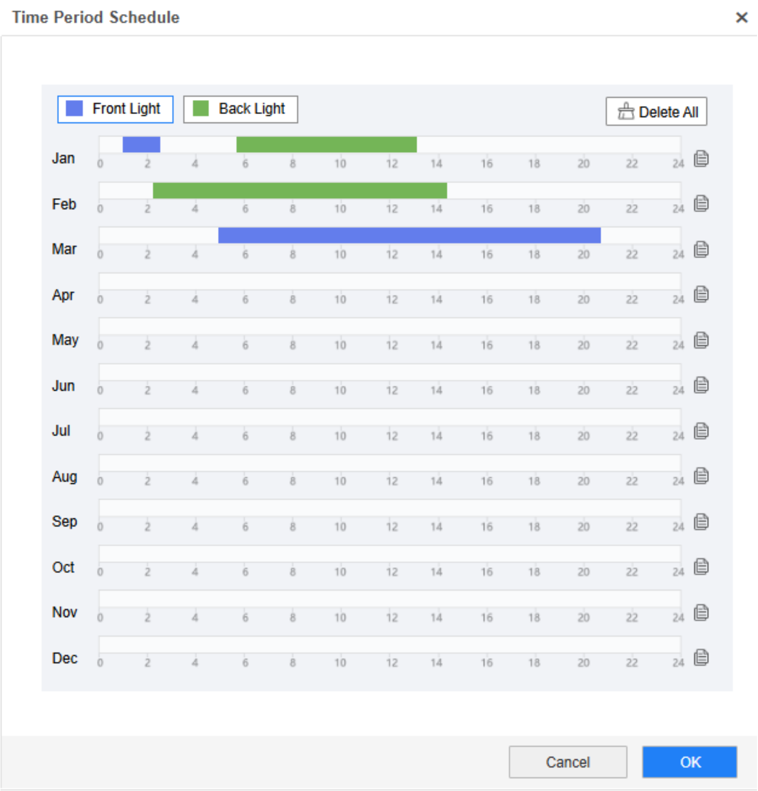


Figure 10-2 Set Time Schedule for Front or Back Light Mode

Parameters Mode

The supported camera parameters vary with different modes. Select a mode the set the corresponding parameters.

Brightness

It refers to the brightness 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.

Saturation

It refers to the colorfulness of the image color.

Sharpness

It refers to the edge contrast of the image.

Contrast

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

WDR Level

Wide Dynamic Range (WDR) can be used when there is a high contrast of the bright area and the dark area of the scene. When you select **Parameters Mode** as **Front Light** or **Back Light**, you can adjust the WDR level. The higher the level is, the higher the WDR strength is.

Advanced

White Balance

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

Hue Range

Select the range to adapt to the display.

Gamma Correction

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

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.

Brightness Enhancement at Night

The scene brightness will be enhanced at night automatically.

Plate Brightness Compensation

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.

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.

Defog

Enable defog to get a clear image in foggy days.

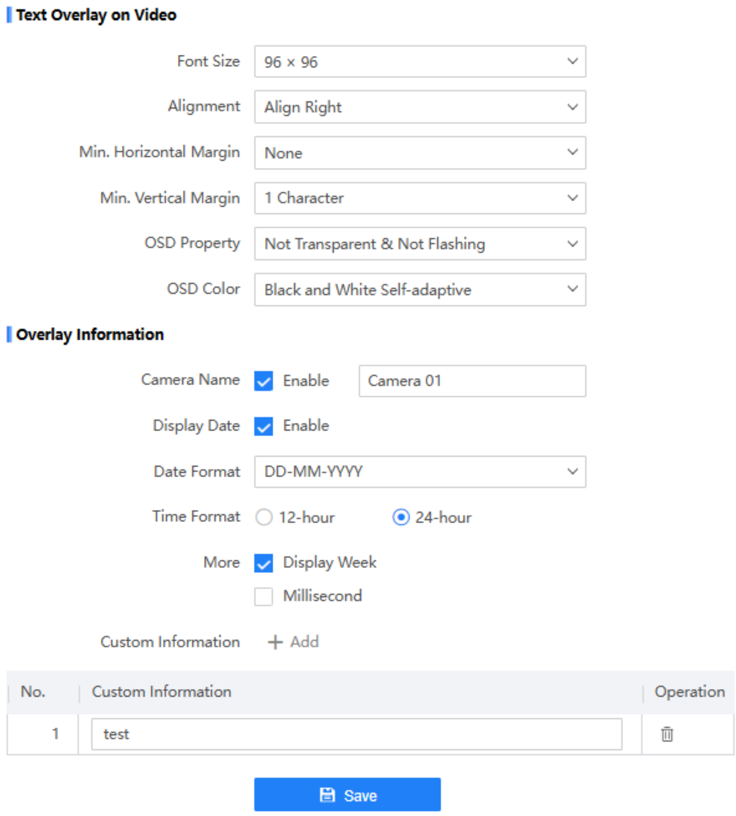
3. **Optional:** Click **Capture Test** to check the image.

10.2 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

Font Size: 96 × 96

Alignment: Align Right

Min. Horizontal Margin: None

Min. Vertical Margin: 1 Character

OSD Property: Not Transparent & Not Flashing

OSD Color: Black and White Self-adaptive

Overlay Information

Camera Name: ☑ Enable Camera 01

Display Date: ☑ Enable

Date Format: DD-MM-YYYY

Time Format: ○ 12-hour ● 24-hour

More: ☑ Display Week

□ Millisecond

Custom Information: + Add

No.	Custom Information	Operation
1	test	🗑

Figure 10-3 Set OSD

2. Set display properties (font, color, etc.).

   Alignment

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

3. Set display contents.

   1) Enable **Camera Name**, and enter the camera name.

   2) Enable **Display Date**, and set the time and date format.

   3) Enable **Display Week** or **Millisecond** according to your needs.

4. **Optional:** Click **Add** and enter information if you want to add custom information.

Note

Up to 6 items of custom information can be added.

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

Result

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

10.3 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.

   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**.

10.4 Set ROI

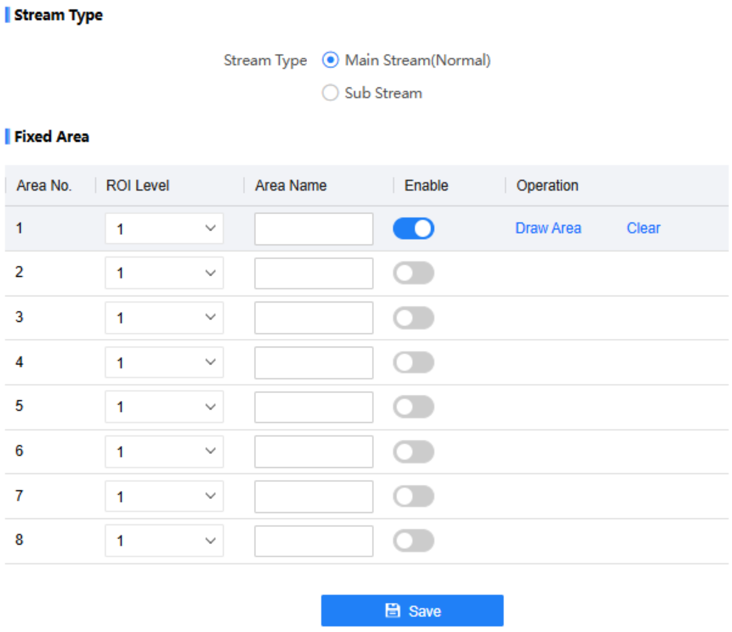
ROI (Region of Interest) encoding helps to assign more encoding resources to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

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** .



Stream Type

Stream Type ● Main Stream(Normal) ○ Sub Stream

Fixed Area

Area No.	ROI Level	Area Name	Enable	Operation
1	1		●	Draw Area Clear
2	1		○	
3	1		○	
4	1		○	
5	1		○	
6	1		○	
7	1		○	
8	1		○	

Figure 10-4 Set ROI

2. Select **Stream Type**.
3. Set ROI area.
    1) Enable the corresponding area.
    2) Select **ROI Level**.

    Note

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

    3) Enter **Area Name**.
    4) Click **Draw Area**.
    5) Drag the mouse on the live view image to draw the fixed area.
    6) Select the fixed area that needs to be adjusted and drag the mouse to adjust its position.
    7) Click **Stop Drawing**.
    8) Repeat the steps above to set more areas. Up to 8 areas are supported.
    9) **Optional:** If you want to delete the area, click **Clear** to delete.
4. Click **Save**.

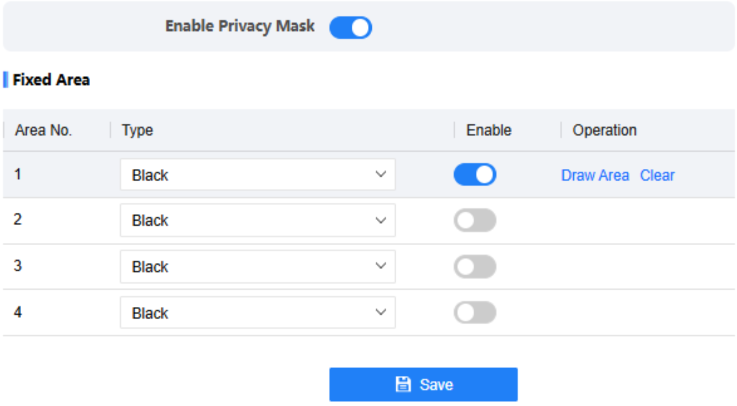
10.5 Set Privacy Mask

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** .

2. Enable privacy mask.



Enable Privacy Mask ●

Fixed Area

Area No.	Type	Enable	Operation
1	Black	●	Draw Area Clear
2	Black	○	
3	Black	○	
4	Black	○	

Figure 10-5 Set Privacy Mask

3. Set the privacy mask area.
   1) Enable the corresponding privacy mask area.
   2) Select **Type**.
   3) Click **Draw Area**.
   4) In the live view image, drag the mouse to draw the privacy mask area of the selected area No.
   5) Click **Stop Drawing**.
   6) Repeat the steps above to set more areas. Up to 4 areas are supported.
   7) **Optional:** If you want to delete the area, click **Clear** to delete.
4. Click **Save**.

10.6 Enable Regional Exposure

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

Steps

1. Go to **Configuration → Video → Video Encoding → BLC** .
2. Enable **Regional Exposure**.
3. Drag the mouse to draw an area in the live view image.

   The drawn area will be exposed.
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

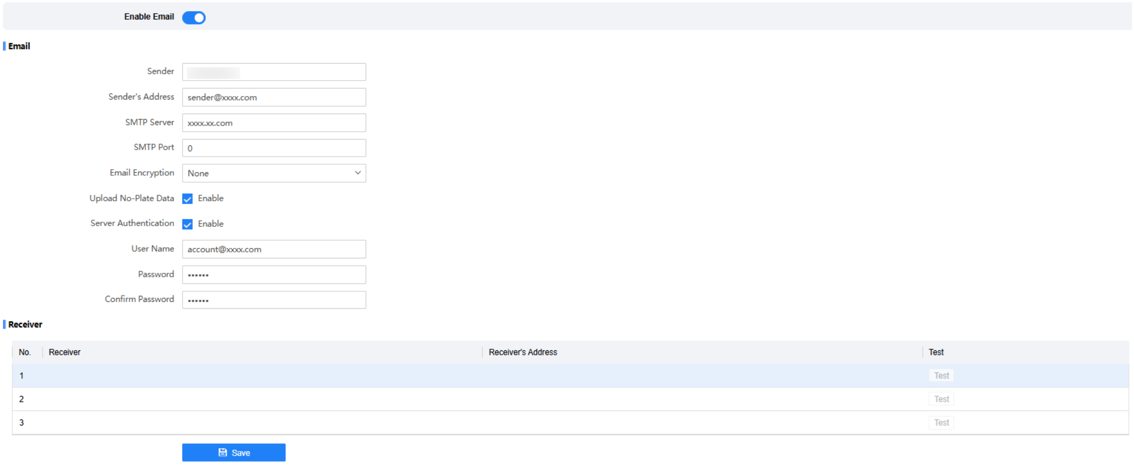
When the email is enabled and set, the device will send an email notification to all designated receivers if an alarm event is detected.

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. Enable Email.



Enable Email ●

Email

Sender	
Sender's Address	sender@xxxx.com
SMTP Server	xxxx.xx.com
SMTP Port	0
Email Encryption	None
Upload No-Plate Data	☑ Enable
Server Authentication	☑ Enable
User Name	account@xxxx.com
Password	••••••
Confirm Password	••••••

Receiver

No.	Receiver	Receiver's Address	Test
1			Test
2			Test
3			Test

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, enable **Upload No-Plate Data**.
4) **Optional:** If your email server requires authentication, enable **Server 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 test 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

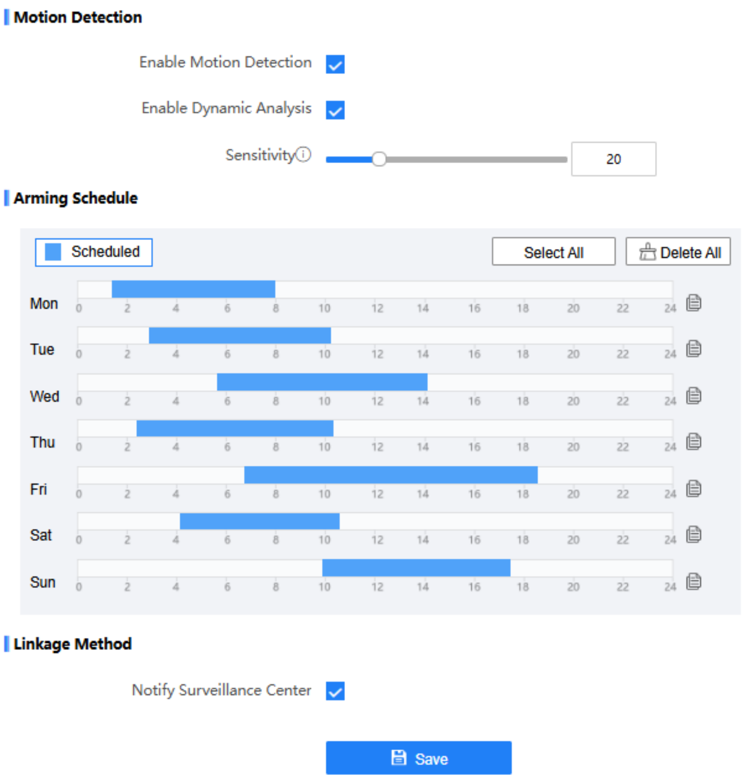
1. Go to **Configuration → Event → Alarm Linkage → Email Event** .
2. Enable linkage to trigger an email for login alarm.
3. Click **Save**.

11.4 Set Motion Detection

When motion detection alarm is set, once a motion event is detected, the device starts to record and the linkage action will be triggered.

Steps

1. Go to **Configuration → Event → Alarm Linkage → Motion Detection** .



Motion Detection

Enable Motion Detection ☑

Enable Dynamic Analysis ☑

Sensitivity 20

Arming Schedule

Linkage Method

Notify Surveillance Center ☑

Figure 11-2 Set Motion Detection

2. Check **Enable Motion Detection**.
3. Check **Enable Dynamic Analysis** if you want to mark the detected objects with green rectangles on the live view window.
4. Set **Sensitivity** for the motion detection.

Note

The sensitivity should be in multiple of 20.

5. Click **Draw Area**. Drag the mouse on the live view image to draw motion detection area(s).
6. Set arming schedule of motion detection. The method is same with that of setting record schedule. Refer to ***Set Record Schedule*** for details.
7. Check **Notify Surveillance Center** to send notification to the surveillance center when a motion event is detected.
8. Click **Save**.

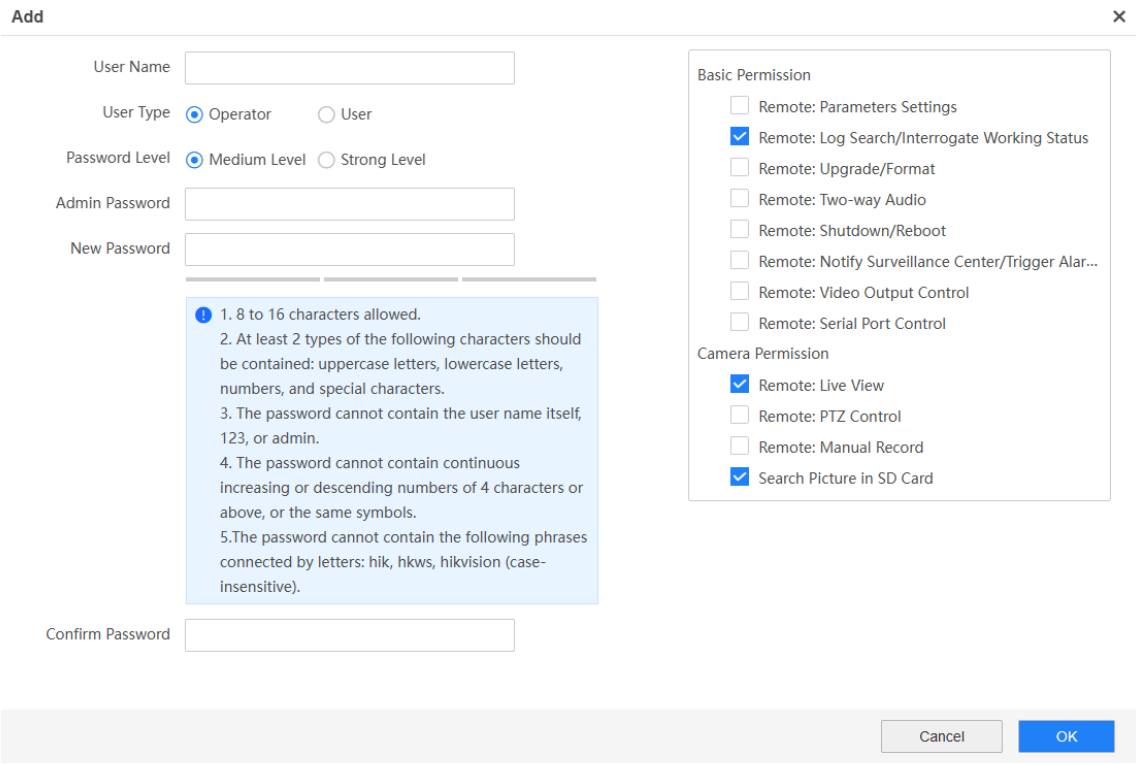
Chapter 12 Safety Management

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. Add a user.



Add

User Name

User Type ● Operator ○ User

Password Level ● Medium Level ○ Strong Level

Admin Password

New Password

1. 8 to 16 characters allowed.
2. At least 2 types of the following characters should be contained: uppercase letters, lowercase letters, numbers, and special characters.
3. The password cannot contain the user name itself, 123, or admin.
4. The password cannot contain continuous increasing or descending numbers of 4 characters or above, or the same symbols.
5.The password cannot contain the following phrases connected by letters: hik, hkws, hikvision (case-insensitive).

Confirm Password

Basic Permission

- □ Remote: Parameters Settings
- ☑ Remote: Log Search/Interrogate Working Status
- □ Remote: Upgrade/Format
- □ Remote: Two-way Audio
- □ Remote: Shutdown/Reboot
- □ Remote: Notify Surveillance Center/Trigger Alar...
- □ Remote: Video Output Control
- □ Remote: Serial Port Control

Camera Permission

- ☑ Remote: Live View
- □ Remote: PTZ Control
- □ Remote: Manual Record
- ☑ Search Picture in SD Card

Figure 12-1 Add User

1) Click **Add**.
2) Enter **User Name** and select **User Type**.
3) Select **Password Level**. The password level of the added user should conform to the selected level.
4) 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.

---

5) Assign remote permissions to users based on needs.

   User

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

   Operator

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

6) Click **OK**.

3. **Optional:** You can do the following operations.

Edit the user information	Click ✎ to edit the user information.
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. 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, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

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

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 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 → Authentication Settings** .
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**.

12.6 Set RTSP Authentication

You can improve network access security by setting RTSP authentication.

Steps

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

   digest

   The device only supports digest authentication.
3. Click **Save**.

12.7 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration → System → Security → Security Service → Login Management** .
2. Check **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.

12.8 Set Password Validity Period

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

Steps

1. Go to **Configuration → System → Security → Security Service → Login Management** .
2. Select **Password Validity Period**.
   - 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**.

12.9 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. 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**.

12.10 Set HTTPS

12.10.1 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.

12.10.2 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**, **Hostname/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

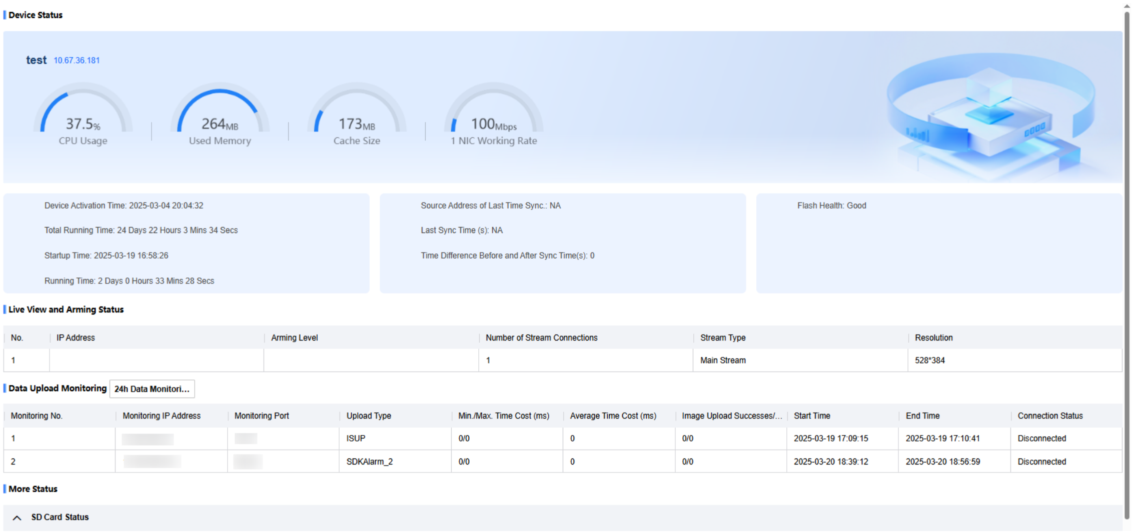
Basic Information and Algorithm Version

Go to **Configuration → System → System Settings → Basic Information** to view the basic information and algorithm 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, live view and arming status, data upload monitoring, and other status.



Device Status

test 10.67.36.181

37.5% CPU Usage

264MB Used Memory

173MB Cache Size

100Mbps 1 NIC Working Rate

Device Activation Time: 2025-03-04 20:04:32

Total Running Time: 24 Days 22 Hours 3 Mins 34 Secs

Startup Time: 2025-03-19 16:58:26

Running Time: 2 Days 0 Hours 33 Mins 28 Secs

Source Address of Last Time Sync.: NA

Last Sync Time (s): NA

Time Difference Before and After Sync Time(s): 0

Flash Health: Good

Live View and Arming Status

No.	IP Address	Arming Level	Number of Stream Connections	Stream Type	Resolution
1			1	Main Stream	528*384

Data Upload Monitoring 24h Data Monitori...

Monitoring No.	Monitoring IP Address	Monitoring Port	Upload Type	Min./Max. Time Cost (ms)	Average Time Cost (ms)	Image Upload Successes/...	Start Time	End Time	Connection Status
1	[redacted]	[redacted]	ISUP	0/0	0	0/0	2025-03-19 17:09:15	2025-03-19 17:10:41	Disconnected
2	[redacted]	[redacted]	SDKAlarm_2	0/0	0	0/0	2025-03-20 18:39:12	2025-03-20 18:56:59	Disconnected

More Status

SD Card Status

Figure 13-1 Device Status

For data upload monitoring, you can click **24h Data Monitoring**, and select the IP address of the picture upload server to view the data upload statistics in 24 hours. The statistics data will be cleared if the device is rebooted by default. You can enable **Flash Storage** and set **Flash Storage Days** to keep the statistics data not to be cleared when the device is rebooted within the set time.

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 → Sync Mode** .

2. Select **Time Zone**.
3. Select **Sync Mode**.

   NTP Time Sync.

   Select it to synchronize the device time with that of the NTP (Network Time Protocol) server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal. You can check **Enable Alternate NTP Server** to guarantee the stability and reliability of NTP time sync. Then set the IP address and port of the alternate NTP server, and set the interval of alternate NTP time sync. Click **Alternate NTP Test** to test if the connection between the device and the alternate server is normal.

   Manual Time Sync.

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

   SDK

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

   ONVIF

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

   No

   Select it to disable time synchronization.

   All

   Select it, and you can select any mode above.

   Note

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

4. Click **Save**.

13.3 Set DST

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

Steps

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

13.4 Set RS-485

Set RS-485 parameters if the device has been connected to a vehicle detector or other RS-485 devices.

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

Steps

Note

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

1. Go to **Configuration → System → System Settings → Serial Port → 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**.

   Transparent Channel

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

   LED Display

   Select it when the LED display is connected to the device via RS-485 serial port.

   License Plate Transmission

   Select it to transmit the recognized license plate information to the other peripheral devices via RS-485 serial port.
4. Click **Save**.

13.5 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port, or peripheral devices have been connected.

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

Steps

1. Go to **Configuration → System → System Settings → Serial Port → RS-232** .
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.

Note

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

3. Select **Work Mode**.

   Console

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

   Transparent Channel

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

   Narrow Bandwidth Transmission

   Reserved.

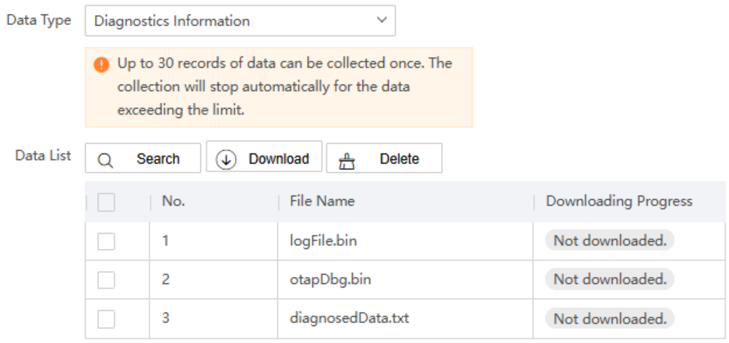
4. Click **Save**.

13.6 Download Debug Data

You can search and download the diagnostics information of the device to troubleshoot and maintain the device.

Steps

1. Go to **Configuration → System → Maintenance → Debug Data Download** .



Data Type: Diagnostics Information

Up to 30 records of data can be collected once. The collection will stop automatically for the data exceeding the limit.

Data List

□	No.	File Name	Downloading Progress
□	1	logFile.bin	Not downloaded.
□	2	otapDbg.bin	Not downloaded.
□	3	diagnosedData.txt	Not downloaded.

Figure 13-2 Download Debug Data

2. Select **Data Type**.

   Diagnostics Information

   The diagnostics information includes kernel, status, version information, etc.

Note

Up to 30 records of data can be collected once. The collection will stop automatically for the data exceeding the limit.

3. Click **Search** to search the data list.

4. Select the file(s) to be downloaded, and click **Download** to download the file(s). You can view the downloading progress.
5. **Optional:** Select the file(s) to be deleted, and click **Delete** to delete the file(s).

13.7 Search Log

Log helps to locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log Search** .
2. Set search conditions.
3. Click **Configuration** to select the logs to be searched according to modules or enable system log service.
   1) Select the module(s) from the dropdown list of **Enable According to Module**.
   2) Enable the functions below.

      Disable Log Automatically

      Enable the function to disable the log automatically, and set **Auto Disabling Time**.

      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. Enter **IP Address** and **Port** of the log server.
   3) Click **OK**.
4. Click **Search**.

   The matched log files will be displayed on the log list.
5. **Optional:** Click **Export** to save the log files to your computer.

13.8 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 → Upgrade & Maintenance → Device Maintenance** .
2. Click **Reboot**.
3. Click **OK** to reboot the device.

Note

You can also click on the upper right corner of the interface to reboot the device.

13.9 Restore Parameters

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

Steps

1. Go to **Configuration → Upgrade & Maintenance → Device Maintenance** .
2. Select the restoration mode.
   - Click **Restore** to restore the parameters except the IP address, subnet mask, gateway, and port No. to the default settings.
   - Click **Restore Factory Settings** to restore all the parameters to the factory settings.
3. Click **OK**.

13.10 Export Parameters

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

Steps

1. Go to **Configuration → Upgrade & Maintenance → Backup and Import Parameters** .
2. Click **Export** after **Configuration 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**.

13.11 Import Configuration File

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

Before You Start

Save the configuration file to the computer.

Steps

Caution

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

1. Go to **Configuration → Upgrade & Maintenance → Backup and Import Parameters** .
2. Select **Importing Method**.

Note

If you select **Import Part**, select **Partially Imported Information**.

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.

13.12 Upgrade

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

Before You Start

- Update the plugin before upgrade.
- Prepare the upgrade file in .dav format.

Steps

1. Go to **Configuration → Upgrade & Maintenance → Import Upgrade File** .
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.

Note

The upgrading process will take minutes. Do not power off the device. The device will restart automatically after upgrading. If the network condition is poor, it may take more time.

Result

The device will reboot automatically after upgrade.

See Far, Go Further

UD44282B