



Mobile Intelligent Panoramic Positioning System

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction	1
1.1 Product Introduction	1
1.2 Key Feature	1
Chapter 2 Activation and Login	2
2.1 Activation	2
2.1.1 Default Information	2
2.1.2 Activate via SADP	2
2.1.3 Activate via Web Browser	3
2.2 Login	4
Chapter 3 Network Configuration	5
3.1 Set IP Address	5
3.2 Set Port	8
3.3 Set IEEE 802.1X	9
3.4 Set DDNS	10
3.5 Set SNMP	11
3.6 Data Connection	12
3.6.1 Set FTP	12
3.6.2 Set Arming Host	14
3.6.3 Set SDK Listening	15
3.6.4 Set ISAPI Listening	16
3.6.5 Set Integration Protocol	17
Chapter 4 Application Mode Configuration	18
4.1 Set Road Maintenance	18
4.2 Vehicle Arming	19
4.2.1 Set Vehicle Arming	19
4.2.2 Set Face Parameters	21

4.3 Checkpoint Capture	25
4.3.1 Set Checkpoint Capture	25
4.3.2 Set Face Parameters	27
4.4 Stopped Vehicle Capture	27
4.4.1 Set Stopped Vehicle Capture	27
4.4.2 Set Face Parameters	29
Chapter 5 Face Picture Library	30
5.1 Manage Face Picture Library	30
5.2 Add Face Picture	31
5.3 Import Face Pictures in Batch	33
5.4 Search Face Picture	33
Chapter 6 Capture Parameters Configuration	35
6.1 Set License Plate Recognition Parameters	35
6.2 Set Feature Parameters	35
6.3 Set Violation Dictionary	36
6.4 Set Information Overlay	36
6.4.1 Set Single Picture Overlay	36
6.4.2 Set Composite Picture Overlay	38
6.5 Set Image Encoding Parameters	40
6.6 Set Picture Composition	41
6.7 Set Capture Schedule	42
6.8 Advanced Configuration	43
6.8.1 System Service	43
Chapter 7 View Real-Time Picture	44
Chapter 8 Live View and Local Configuration	48
8.1 Live View	48
8.1.1 Switch Channel Composition Mode	48
8.1.2 Start/Stop Live View	49

8.1.3 Select Image Display Mode	49
8.1.4 Select Window Division Mode	49
8.1.5 Select Stream Type	50
8.1.6 Capture Picture Manually	50
8.1.7 Record Manually	50
8.1.8 Enable Digital Zoom	50
8.1.9 Enable 3D Positioning	51
8.1.10 Select Video Mode	51
8.2 Set Snapshot Mode	51
8.3 Local Configuration	51
Chapter 9 PTZ Control	55
9.1 PTZ Control Panel	55
9.2 Set Preset	56
9.3 Set Patrol Scan	58
9.4 Set Pattern Scan	59
9.5 Enable Proportional Pan	59
9.6 Set Park Action	60
9.7 Set Scheduled Task	61
9.8 Clear Configuration	61
Chapter 10 Record and Capture	63
10.1 Set Storage Path	63
10.1.1 Set Storage Card	63
10.1.2 Set Cloud Storage	64
10.2 Set Record Schedule	65
10.3 Set Snapshot Schedule	67
10.4 Search Picture	67
10.5 Playback	68
Chapter 11 Encoding and Display	70

11.1 Set Camera Parameters	70
11.2 Set OSD	73
11.3 Set Video Encoding Parameters	75
11.4 Set ROI	76
Chapter 12 Event and Alarm	78
12.1 Exception Alarm	78
12.2 Set Email Event	78
Chapter 13 Safety Management	79
13.1 Manage User	79
13.2 Enable User Lock	79
13.3 Set SSH	80
13.4 Prohibit PING	80
13.5 Enable System Log Service	80
13.6 Set Timeout Logout	81
13.7 Set Password Validity Period	81
13.8 Set SDK Protocol Authentication Mode	81
13.9 Set RTSP Authentication	82
13.10 Set IP Address Filtering	82
13.11 Set HTTPS	82
13.11.1 Create and Install Self-signed Certificate	82
13.11.2 Install Authorized Certificate	83
Chapter 14 Maintenance	84
14.1 View Device Information	84
14.2 Synchronize Time	84
14.3 Set DST	85
14.4 Set RS-485	85
14.5 Set RS-232	86
14.6 Reboot	86

14.7 Restore Parameters	87
14.8 Export Parameters	87
14.9 Export Debug File	87
14.10 Export Diagnosis Information	88
14.11 Upgrade	88
14.12 Export Violation Type File	88
14.13 Import Violation Code File	89
14.14 Import Configuration File	89
14.15 Search Log	90
14.16 Enable Log According to Module	90
14.17 Enable Maintenance Service	90

Chapter 1 Introduction

1.1 Product Introduction

Panoramic positioning system (hereinafter referred to as "device" or "PTZ camera") is an intelligent PTZ camera integrating functions like image processing, intelligent analysis, storage, satellite positioning, and wireless transmission. It can be widely used in mobile monitoring and common road monitoring scenes.

1.2 Key Feature



Product features vary with different models. The actual device prevails.

- 4 MP 1/1.8" CMOS sensor, ultra-low illumination night imaging, shooting clearer.
- 360° (2 × 180°) panoramic view.
- High resolution for image encoding.
- Several types of road disease information detection.
- 4 MP PTZ camera, 23× optical zoom.
- IR illumination helps to capture high quality images in dim light environment.
- Adopts all-weather design, high-strength aluminum alloy casting housing.

Chapter 2 Activation and Login

2.1 Activation

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



Note

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

2.1.1 Default Information

The device default information is shown as below.

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

2.1.2 Activate via SADP

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

Before You Start

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

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

Steps

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



Caution

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

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

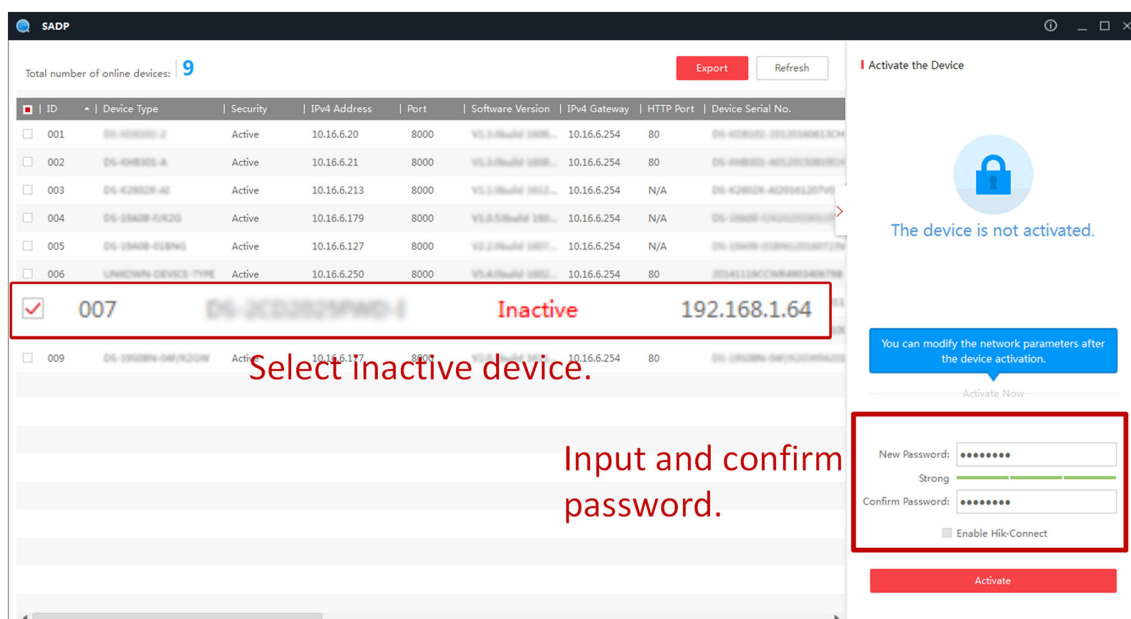


Figure 2-1 Activate via SADP

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

5. Modify IP address of the device.

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

2.1.3 Activate via Web Browser

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

Before You Start

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

Steps

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



Caution

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

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

2.2 Login

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

Before You Start

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

Steps

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

Chapter 3 Network Configuration

3.1 Set IP Address

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

Steps



Note

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

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

NIC Settings

NIC Type	Auto
DHCP	☐
IPv4 Address	
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	
IPv6 Mode	DHCP
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	
MTU	1500
Multicast Address	

DNS Server

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

Save

Figure 3-1 Set IP Address

2. Set network parameters.

NIC Type

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

IPv4

Two modes are available.

DHCP

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



Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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



Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

Multicast Address

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

DNS

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

3. Click **Save**.

3.2 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.

The screenshot displays a configuration interface for various network ports. It is organized into sections for each port type, with an 'Enable' checkbox and a text input field for the port number.

Port Type	Enable	Port Number
HTTP Port	☒	80
HTTPS Port	☐	443
RTSP Port	☒	554
SDK Port		8000
SADP Port	☒	
SDK over TLS Port	☐	8433

Figure 3-2 Set Port

HTTP Port

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

HTTPS Port

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

RTSP Port

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

SDK Port

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

SADP Port

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

SDK over TLS Port

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



Note

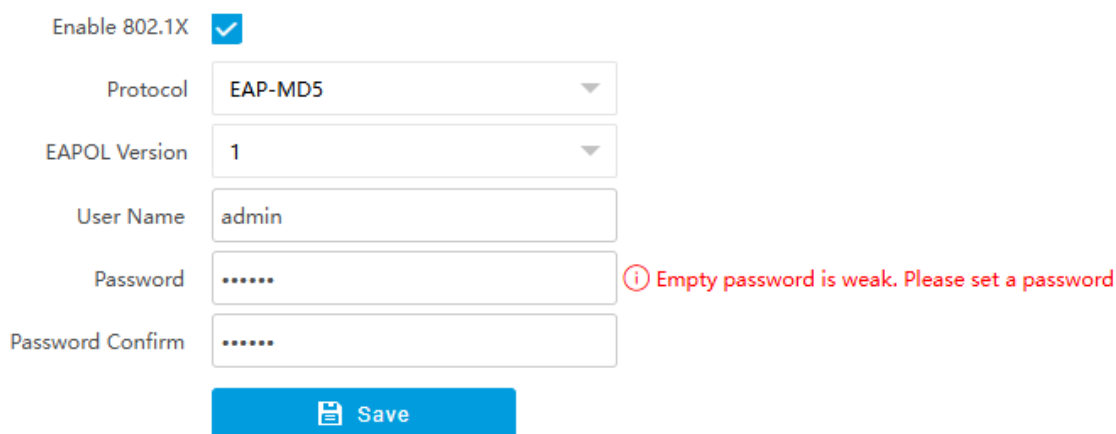
- After editing the port, access to the device via the new port.
 - Reboot the device to bring the new settings into effect.
 - The supported ports vary with different models. The actual device prevails.
-

3.3 Set IEEE 802.1X

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

Steps

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



Enable 802.1X ☒

Protocol EAP-MD5

EAPOL Version 1

User Name admin

Password ⓘ Empty password is weak. Please set a password

Password Confirm

 Save

Figure 3-3 Set IEEE 802.1X

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

Protocol

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**.

3.4 Set DDNS

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

Before You Start

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

Steps

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

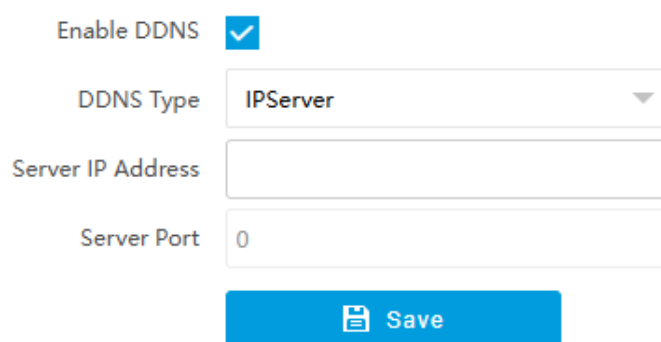


Figure 3-4 Set DDNS

2. Check **Enable DDNS**.
3. Select **DDNS Type**, and set corresponding parameters.

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. |

3.5 Set SNMP

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

Before You Start

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

Steps

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

The screenshot displays the SNMP configuration interface, organized into three main sections: **SNMP v1/v2c**, **SNMP v3**, and **SNMP Other Settings**.

SNMP v1/v2c section includes:

- Enable SNMPv1**: A checkbox that is currently unchecked.
- Enable SNMPv2c**: A checkbox that is currently unchecked.
- Read SNMP Community**: A text input field containing the value "public".
- Write SNMP Community**: A text input field containing the value "private".
- Trap Address**: A text input field with a blurred value.
- Trap Port**: A text input field with a blurred value.
- Trap Community**: A text input field containing the value "public".

SNMP v3 section includes:

- Enable SNMPv3**: A checkbox that is currently unchecked.
- Read UserName**: A text input field.
- Security Level**: Three radio buttons: "Authentication and not Encryption" (unchecked), "Not Authentication or Encryption" (checked), and "Authentication and Encryption" (unchecked).
- Authentication Algorithm**: Two radio buttons: "MD5" (checked) and "SHA" (unchecked).
- Authentication Password**: A text input field with masked characters (dots) and a "Show/Hide" icon.
- Encryption Algorithm**: Two radio buttons: "DES" (unchecked) and "AES" (unchecked).
- Encryption Password**: A text input field with masked characters (dots) and a "Show/Hide" icon.
- Write UserName**: A text input field.
- Security Level**: Three radio buttons: "Authentication and not Encryption" (unchecked), "Not Authentication or Encryption" (checked), and "Authentication and Encryption" (unchecked).
- Authentication Algorithm**: Two radio buttons: "MD5" (checked) and "SHA" (unchecked).
- Authentication Password**: A text input field with masked characters (dots) and a "Show/Hide" icon.
- Encryption Algorithm**: Two radio buttons: "DES" (unchecked) and "AES" (unchecked).
- Encryption Password**: A text input field with masked characters (dots) and a "Show/Hide" icon.

SNMP Other Settings section includes:

- SNMP Port**: A text input field with a blurred value.

At the bottom of the form is a blue button with a save icon and the text "Save".

Figure 3-5 Set SNMP

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



Note

- The SNMP version you select should be the same as that of the SNMP software.
- Use different versions according to the security levels required. 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.

3.6 Data Connection

3.6.1 Set FTP

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

Before You Start

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

Steps

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

FTP

Enable FTP ☒

Number of Enabled FTP ☒ One ☐ Two

FTP1

Server Address Type

Server Address

Port

User Name

Password

Confirm Password

Path/Picture Name Encoding Mode **FTP Test**

Connection Mode

Not Upload Plate Close-up ☐ Upload Face Picture ☐

Upload Additional Information to FTP ☐ Upload CSV Vehicle Passing Statistic... ☐

Protocol Type

Directory Structure

Parent Directory

Level 2 Directory

Level 3 Directory

Level 4 Directory

Level 5 Directory

Level 6 Directory

Figure 3-6 Set FTP

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

Note

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

4. Set FTP parameters.

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

Note

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

5) Select **Directory Structure**.

Note

You can customize the directory structure according to your needs.

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

UTF-8

UNICODE encoding.

7) Select **Connection Mode**.

Transitory Connection

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

Persistent Connection

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

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

Note

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

Not Upload Plate Close-up

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

Upload Face Picture

Upload face close-up pictures to the FTP server.

Upload Additional Information to FTP

Add related information when uploading data to the FTP server.

Upload CSV Vehicle Passing Statistics Information to FTP

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

6. **Optional:** Click **FTP Test** to check the FTP server.

7. Set naming rules and separators according to the actual needs.



Note

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

8. **Optional:** Edit **OSD Information** which can be uploaded to the FTP server with the pictures to make it convenient to view and distinguish the data.
9. Click **Save**.

3.6.2 Set Arming Host

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

Steps



Note

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

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

Protocol Type ☒ License Plate Alarm

Cloud Storage  Disabled

 Save

Figure 3-7 Set Arming Host

2. Select **Protocol Type**.



Note

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

License Plate Alarm

Uploads arming alarm images of the license plate.

3. **Optional:** If you want to save the alarm information and pictures to the cloud storage, click  to set **Cloud Storage**. Refer to **Set Cloud Storage** for details.
4. Click **Save**.

3.6.3 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** .

Enable SDK Listening ☒

Listening Host IP Address/Domain

Listening Host Port

Enable SDK Listening ☐

Protocol Type ☒ License Plate Alarm

Cloud Storage Disabled

Save

Figure 3-8 Set SDK Listening

2. Enable 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:** The device will transmit images via the SDK listening if you enable the picture uploading listening.
5. Select **Protocol Type**.



Note

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

License Plate Alarm

Uploads arming alarm images of the license plate.

6. **Optional:** If you want to save the alarm information and pictures to the cloud storage, click  to set **Cloud Storage**. Refer to [Set Cloud Storage](#) for details.
7. Click **Save**.

3.6.4 Set ISAPI Listening

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

Before You Start

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

Steps

1. Go to **Configuration → Network → Data Connection → ISAPI Listening**.
2. Enable the ISAPI listening.

Enable ISAPI Listening

☒

Version

HTTP

Host IP Address/Domain Name

Host Port

Host URL

Heartbeat Interval (s)

0



Uploaded Picture Type Control

All

Authentication Mode

None

Cloud Storage

 Disabled

 Save

Figure 3-9 Set ISAPI Listening

3. Set **Host IP Address/Domain Name**, **Host Port**, and **Host URL**.

4. Enter **Heartbeat Interval**.



Note

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

5. Select **Uploaded Picture Type Control**.

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



Note

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

7. **Optional:** If you want to save the alarm information and pictures to the cloud storage, click ⚙️ to set **Cloud Storage**. Refer to [Set Cloud Storage](#) for details.

8. Click **Save**.

3.6.5 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.

Chapter 4 Application Mode Configuration

4.1 Set Road Maintenance

The device supports setting road maintenance parameters to detect conditions and abnormal conditions of the road.

Steps

1. Go to **Configuration → Capture → Application Mode**.
2. Select **Trigger Mode** as **Road Maintenance**.

Trigger Mode

Trigger Mode

Road Maintenance

Work Mode

Capture Configuration

Lens

Lens 1

Road Damage Detection

Maintenance Type

☒ Pothole

☒ Alligator Cracking

☒ Pitted Skin

☒ Longitudinal Cracking

☐ Road Signage

☒ Waterlogging

☒ Patching

☒ Transverse Cracking

☒ Manhole Frame Difference

Sensitivity

50

Other Settings

Overlay Target Frame

☒

Recognize Road Distress

☒

Min. Speed Threshold (km/h)

5

Max. Speed Threshold (km/h)

120

Lane Width(cm)

328

Construction Height (cm)

184

Horizontal Distance (cm)

1600

Horizontal Field Angle (°)

81

Vertical Field Angle (°)

44

Figure 4-1 Set Road Maintenance

3. Select **Lens**.
4. Select **Maintenance Type** and set **Sensitivity**.
5. Set the following parameters.

Overlay Target Frame

Enable it, and the target to be captured on the picture will be overlaid with a target frame.

Recognize Road Distress

Enable it and set **Min. Speed Threshold** and **Max. Speed Threshold**. The camera will capture violation behaviors of vehicles driven at speeds within the speed range.

6. Set **Lane Width**, **Construction Height**, **Horizontal Distance**, **Horizontal Field Angle**, and **Vertical Field Angle** according to the actual condition.
7. Click **Draw Lane Line** to adjust the lane lines and shielded region according to the actual scene, and click **OK**.



Note

- The selected road damage detection types will not take effect in the shielded region.
- You can check **Stop Live View** to stop live view of the scene, or check **Start Live View** to start live view of the scene.

-
8. Click **Save**.

Result

In the road maintenance mode, go to **Configuration → Local** and enable **Rule Information**. Then the rule frame will be overlaid on the video image when the target to be captured is detected.

4.2 Vehicle Arming

4.2.1 Set Vehicle Arming

Set vehicle arming to arm vehicles according to the scene and capture the violations.

Steps

1. Go to **Configuration → Capture → Application Mode**.
2. Select **Trigger Mode** as **Vehicle Arming**.
3. Click **Vehicle Arming**.

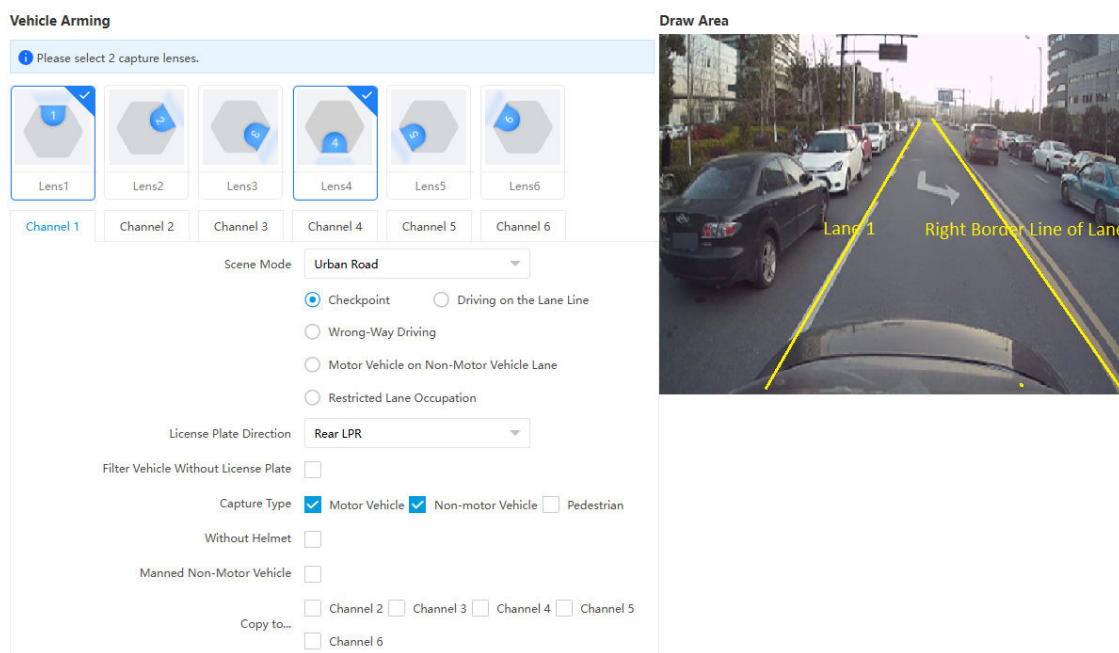


Figure 4-2 Vehicle Arming

4. Select two capture lenses.
5. Click the corresponding channel of the selected lens, and set vehicle arming parameters.

Scene Mode

Select the scene according to the actual condition. The supported parameters are different according to the selected scene. Select the violation type(s) to be detected according to your needs.

License Plate Direction

Select **Front LPR** when license plates of vehicles from the approaching direction need to be recognized. Select **Rear LPR** when license plates of vehicles from the leaving direction need to be recognized.

Filter Vehicle Without License Plate

Enable the function to filter the capture results of vehicles without license plates.

Number of Captured Violation Picture(s)

If you have selected violation capture type(s), select the number of pictures to capture the violations.

Capture Type

Select the target types to be captured.

Without Helmet

If you have enabled non-motor vehicle detection and capture, you can enable **Without Helmet** to detect and capture the violation of not wearing helmet for the non-motor vehicle driver. Set **Number of Without Helmet Captures**.

Manned Non-Motor Vehicle

If you have enabled non-motor vehicle detection and capture, you can enable **Manned Non-Motor Vehicle** to detect and capture the violation of manned non-motor vehicle. Set **Number of Manned Non-Motor Vehicle Captures**.

6. Adjust the lane lines and right border line according to the actual scene on the right of the interface.
7. **Optional:** Select the other channel(s) to copy the same settings.
8. Click **Save**.

4.2.2 Set Face Parameters

If you need the device to capture the face pictures appeared in the detection area and upload them to the platform, set face detection.

Steps

1. Go to **Configuration → Capture → Application Mode**.
2. Select **Trigger Mode** as **Vehicle Arming**.
3. Click **Face Parameters**. Enable **Face Capture**.

Algorithm Parameters

Face Capture ☒

Capture Range (Frame) 50

Capture Times 1

Detection Sensitivity 3

Capture Threshold 20

Generation Speed 3

Enable Face Picture Exposure ☒

Exposure Duration(s)

Smart Information

Enable Information Overlay on Picture ☒

Enable Video Information Overlay ☒

Upload Face Picture Only ☐

Number of Areas

Number of Pupil Distance Frames

Number of Rule Areas

Number of Shielded Areas

Human Face Picture Matting

Face Close-up Picture Cutting Ratio ☐ Small ☒ Medium ☐ Large

Face Picture Comparison

Enable Face Picture Comparison ☒

Face Picture Comparison Threshold 80

Figure 4-3 Set Face Parameters

4. Set algorithm parameters.

Capture Range (Frame)

Set the frame interval of every capture during the process that the face appears in the detection area and disappears from the area. The face picture with the highest quality rating will be captured.

Capture Times

Set the capture times of the same face picture during the process that the face appears in the detection area and disappears from the area.

Detection Sensitivity

Set the face detection sensitivity. If there are many mistaken face captures, adjust the sensitivity smaller. If there are many missing face captures, adjust the sensitivity larger.

Capture Threshold

Set the face capture rating threshold. Only the face picture larger than or equaling to the threshold can be captured.

Generation Speed

Set the generation speed of the face target appearing in the detection area. The larger the speed is, the more quickly the target can be generated.

Enable Face Picture Exposure

Enable the function and set **Exposure Duration**. When the face is recognized, the detected face area will be exposed partially for the set duration to raise the brightness of the area.

5. Set smart information.

Enable Information Overlay on Picture

Check it to overlay the detection rectangle on the face appeared in the captured scene picture.

Enable Video Information Overlay

Check it to overlay the detection rectangle on the face appeared in the video.



Note

You need to enable rule information in **Configuration → Local** before enabling video information overlay.

Upload Face Picture Only

If you check it, only the close-up face picture will be uploaded to the platform. Otherwise, both the scene picture and close-up face picture will be uploaded to the platform.

6. Set face picture matting parameters.

Face Close-up Picture Cutting Ratio

Put the cursor on the selection to view the cutting effect. Select the face close-up picture cutting ratio according to the actual needs.

7. Set face picture comparison parameters if you want to compare the captured face pictures with those in the face picture library to match the person information.



Note

Set the face picture library before enabling the function. Refer to ***Face Picture Library*** for details.

1) Check **Enable Picture Comparison**.

2) Set **Face Picture Comparison Threshold**.

When the similarity between the captured face picture and the face picture in the face picture library exceeds the set threshold, alarm will be triggered and the captured face picture will be uploaded to the platform. You can view the captured face picture and information, capture scene picture, similarity, and the face picture in the face picture library.

8. Draw the face detection areas.

- 1) Select **Number of Pupil Distance Frames**, **Number of Rule Areas**, and **Number of Shielded Areas**.

 Note

If you select **0** for **Number of Shielded Areas**, the shielded area function will be disabled.

- 2) If the default face detection area does not fit the current scene, click **Draw Area** to adjust the pupil distance rectangle, rule area, and shielded areas on the right of the interface. You can double click the live view image to adjust in full screen.

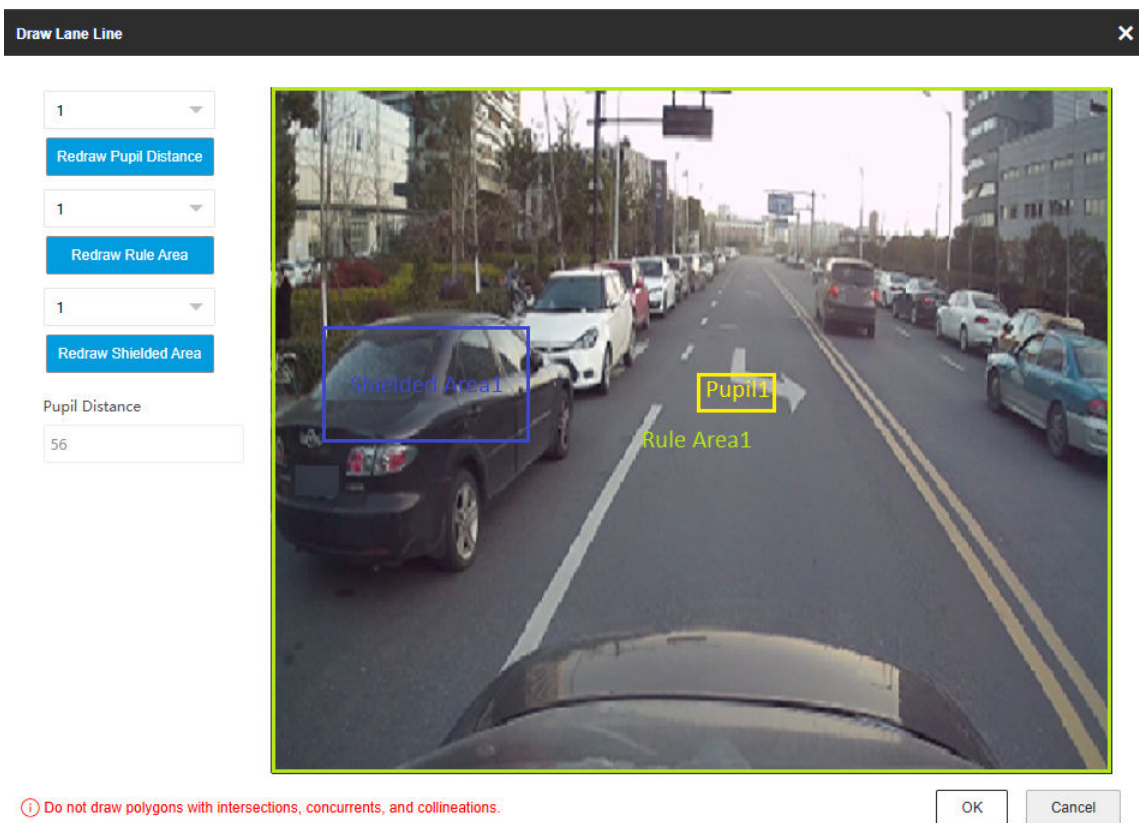


Figure 4-4 Draw Area

 Note

- You can click the PTZ buttons to adjust the visual angle and lens.
- You can click **Live View** to start the live view, or click **Stop Live View** to stop the live view.
- Do not draw polygons with intersections, concurrents, and collineations.

Redraw pupil distance	Pupil distance refers to the distance between the pupils of both eyes. Draw to set the value. The recommended value is 40.
-----------------------	--

	a. Select the pupil distance frame No. b. Click Redraw Pupil Distance. c. Drag the mouse to draw the pupil distance frame.  Note Pupil distance must be set, or the face picture cannot be captured.
Redraw rule area	a. Select the rule area No. b. Click Redraw Rule Area. c. Click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to finish.  Note The rule area is recommended to occupy 1/2 of the live view image, and not more than 2/3 of the live view image.
Redraw shielded area	a. Select the shielded area No. b. Click Redraw Shielded Area. c. Click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to finish.  Note The faces detected in the shielded area will not be captured. Up to four shielded areas can be set.

9. Click **Save**.

4.3 Checkpoint Capture

4.3.1 Set Checkpoint Capture

In checkpoint capture mode, you can enable two channels to capture the moving vehicles and recognize license plates in the visual angle.

Steps

1. Go to **Configuration → Capture → Application Mode**.
2. Select **Trigger Mode** as **Checkpoint Capture**.
3. Click **Checkpoint Capture**.
4. Enable **Checkpoint Capture**.

Checkpoint Capture

Checkpoint Capture ☒ Enable

Please select 2 capture lenses.


Lens1


Lens2


Lens3


Lens4


Lens5


Lens6

Number of Captures

Filter Vehicle Without License Plate ☒

Capture Type ☒ Motor Vehicle ☒ Non-motor Vehicle ☐ Pedestrian

Without Helmet ☒

Number of Without Helmet Captures

Manned Non-Motor Vehicle ☒

Number of Manned Non-Motor Vehicle Captures

Figure 4-5 Checkpoint Capture

- 5. Select two capture lenses.
- 6. Set checkpoint capture parameters.

Number of Captures

Select the number of pictures to capture.

Filter Vehicle Without License Plate

Enable the function to filter the capture results of vehicles without license plates.

Capture Type

Select the target types to be captured.

Without Helmet

If you have enabled non-motor vehicle detection and capture, you can enable **Without Helmet** to detect and capture the violation of not wearing helmet for the non-motor vehicle driver. Set **Number of Without Helmet Captures**.

Manned Non-Motor Vehicle

If you have enabled non-motor vehicle detection and capture, you can enable **Manned Non-Motor Vehicle** to detect and capture the violation of manned non-motor vehicle. Set **Number of Manned Non-Motor Vehicle Captures**.

7. Optional: You can click **Front Lens** or **Rear Lens** to switch the lens on the right of the interface to view the live view image of corresponding lens.

8. Click **Save**.

4.3.2 Set Face Parameters

The configuration is same with the face parameters configuration in vehicle arming mode. You can refer to **Set Face Parameters** for details.

4.4 Stopped Vehicle Capture

4.4.1 Set Stopped Vehicle Capture

The device can detect the stopped vehicles and capture pictures via a front and a rear lens.

Steps

- 1.** Go to **Configuration → Capture → Application Mode**.
- 2.** Select **Trigger Mode** as **Stopped Vehicle Capture**.
- 3.** Click **Stopped Vehicle Capture**.
- 4.** Select the camera.
 - **Camera Module:**
 - a. Select **License Plate Direction**. Select **Front LPR** when license plates of vehicles from the approaching direction need to be recognized. Select **Rear LPR** when license plates of vehicles from the leaving direction need to be recognized.
 - b. Click the PTZ buttons to adjust the lens to the scene to be detected. Operate the focusing, zooming, and iris to adjust an appropriate visual angle and clear image.
 - c. Draw the LPR area. Adjust the area on the live view image, or click **Redraw LPR Area** to redraw the area.
 - d. Click **Capture Close Shot** to capture a close-up picture manually. The picture will be stored to the storage card in priority. If no storage card is installed, the picture will be uploaded to the set platform.

Stopped Vehicle Capture

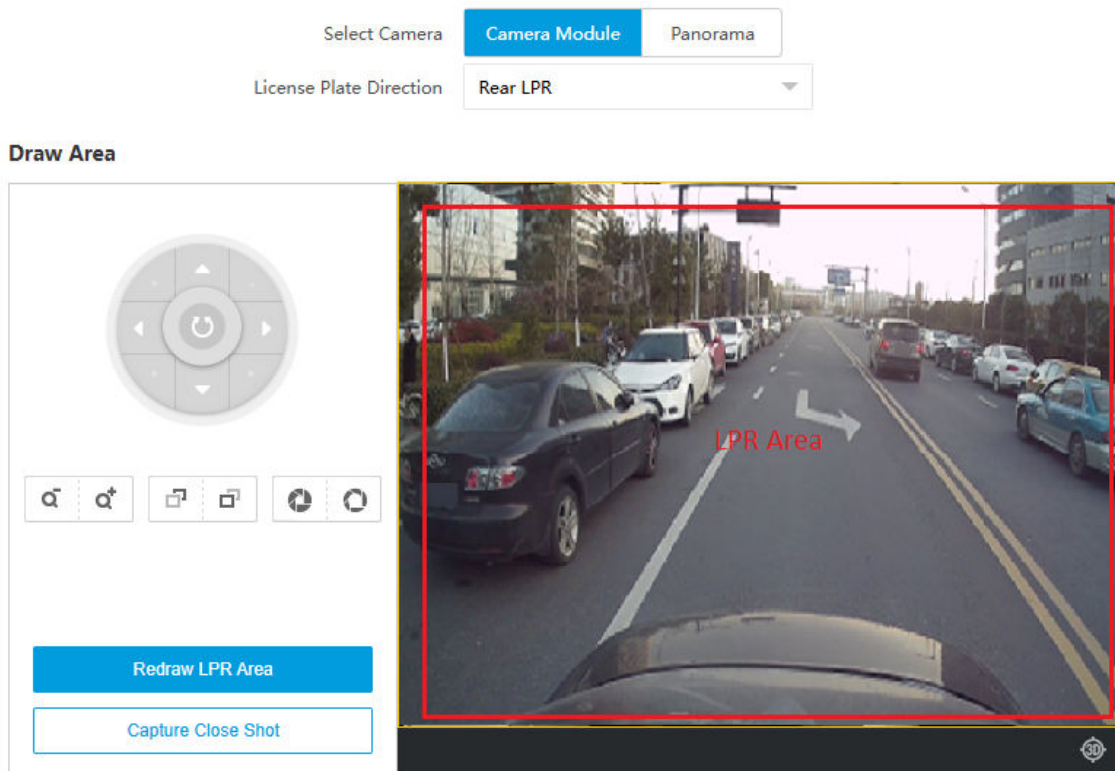


Figure 4-6 Camera Module

- Panorama:

- Enable **Stopped Vehicle Capture**.
- Set the capture parameters.

Filter Vehicles in Parking Spaces

Enable the function and the vehicles parking in the parking spaces will not be captured.

Filter Vehicles Outside Traffic Lanes

Enable the function and the vehicles parking outside the lane will not be captured.

Mounting Mode

Select the mounting mode of the two lenses which is used to capture the stopped vehicle violation.

Side Mounting Capture Mode

If you have selected **Side Mounting of Lens** for the mounting mode, select the capture mode of side mounting. If the two right side lenses are used to capture, select **Right Side Capture**. If the two left side lenses are used to capture, select **Left Side Capture**. You can refer to **Lens Direction** diagram for the positions of the lenses.



Note

Capture can be triggered only when the front and rear lenses recognize the same license plates.

Stopped Vehicle Capture

Select Camera

Stopped Vehicle Capture ☒ Enable

Filter Vehicles in Parking Spaces ☒ Enable

Filter Vehicles Outside Traffic Lanes ☒ Enable

Mounting Mode ☐ Center Mounting of Lens ☒ Side Mounting of Lens

Side Mounting Capture Mode ☒ Right Side Capture ☐ Left Side Capture

Lens Direction

Right Front	Right Rear

! In matched capture mode, capture can be triggered only when the front and rear lenses recognize the same license plates.

Figure 4-7 Panorama

- 5. Optional:** You can click **Front Lens** or **Rear Lens** to switch the lens on the right of the interface to view the live view image of corresponding lens.
- 6.** Click **Save**.

4.4.2 Set Face Parameters

The configuration is same with the face parameters configuration in vehicle arming mode. You can refer to **Set Face Parameters** for details.

Chapter 5 Face Picture Library

5.1 Manage Face Picture Library

You can manage face picture libraries.

Before You Start

- Install the storage media. Click **Configuration → Storage → Storage Management → HDD Management → HDD Quota** to set **Face Picture Library Quota**. Reboot the device after the face picture library partition is formatted for the first time.
- After the storage media is formatted, reboot the device to check if the face picture library quota is normal.
- Enable face capture and face picture comparison in **Configuration → Capture → Application Mode**, or **Face Picture Library** interface will not appear. If the interface still disappears after you have enabled face capture and face picture comparison, refresh the web page or reboot the device.

Steps

1. Click **Face Picture Library**.
2. Click **+** on the left of the interface to add a face picture library.
3. Enter **Face Picture Library Name**, and click **OK**.
4. Check **Enable** to enable the added face picture library.

The added face picture libraries will be listed on the left. Up to 10 libraries can be added.

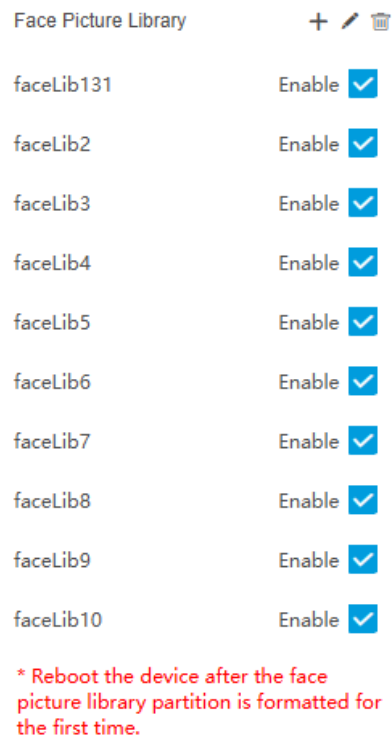


Figure 5-1 Added Face Picture Library

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

- Edit name** Select a face picture library, and click to edit its name.
- Delete added library** Select a face picture library, and click to delete it.

5.2 Add Face Picture

You can add face pictures one by one to a face picture library.

Steps

1. Click **Face Picture Library**.
2. Select an enabled face picture library.
3. Click **Add**.

Add face info

Name

Gender

Male

ID Type

Officer ID

ID No.

Face Picture

Select File

Delete Device Pictures

No

OK

Cancel

Figure 5-2 Add Face Picture to Library

4. Set **Name**, **Gender**, **ID Type**, and **ID No.**
5. Click **Select File**, and select a face picture from the computer to add to the library.



Note

- The added face picture size cannot exceed 1 M.
 - Only the face picture in the format of .jpg can be added.
6. **Optional:** If you want to delete the backup face picture in the device local storage after it is added to the library and modeled successfully to protect data security, select **Delete Device Pictures** as **Yes**.
7. Click **OK**, and added face pictures will be listed on the interface.

Face Picture Library

faceLib1

Enable

faceLib2

Enable

faceLib3

Enable

faceLib4

Enable

faceLib5

Enable

faceLib6

Enable

faceLib7

Enable

faceLib8

Enable

faceLib9

Enable

faceLib10

Enable

Name

Gender

ID Type

ID No.

Modeling Status

1

faceLib1

Male

Officer ID

123456

Success

Total 11 item(s)

Prev Page

1

Next Page

Go

Page

Go

Figure 5-3 Face Picture List

8. Optional: Edit or delete the added face picture.

- Select the added face picture, and click **Modify** to edit the information.
- Select the added face picture, and click **Delete** to delete it.

5.3 Import Face Pictures in Batch

You can import face pictures from the computer to the library manually in batch.

Steps

1. Click **Face Picture Library**.
2. Select a face picture library.
3. Click **Import**.
4. Check items according to the actual needs, and click **OK**.
 - **Whether to delete device local image after successful image import?**
Enable it to delete the backup face picture in the device local storage after it is added to the library and modeled successfully.
 - **Prompt immediately when importing and modeling failed?**
Enable it, and you will receive prompts immediately when importing or modeling the face pictures failed.
 - **Whether to report the result of importing?**
Enable it and the device will report the importing result.
5. Select the file folder storing the face pictures, and click **OK**.



Note

- The imported face picture should be named as "name_gender_cardID.jpg". Here the gender should be 1/2 to stand for the male/female gender respectively. E.g., Jim_1_1234567890.jpg. If the face picture name does not conform to the requirement, the device will recognize the face picture file name as the person name to import.
 - Only the face picture in the format of .jpg can be imported.
 - Up to 50,000 face pictures can be imported to a face picture library.
-
6. Check the importing information in the popup window, and click **OK**.
 7. **Optional:** Edit or delete the face picture information.
 - Select the imported face picture, and click **Modify** to edit the information.
 - Select the imported face picture, and click **Delete** to delete it.

5.4 Search Face Picture

You can search face pictures in the face picture library.

Steps

1. Click **Face Picture Library**.
2. Select a face picture library.

3. Set the search conditions such as **Name**, **Gender**, and **ID No.**
4. Click **Search**, and the face picture(s) conforming to the search conditions will be listed on the interface.

Chapter 6 Capture Parameters Configuration

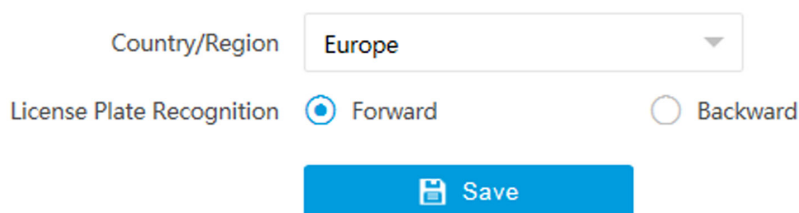
6.1 Set License Plate Recognition Parameters

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 → License Parameters**.

License Parameters



Country/Region Europe

License Plate Recognition ☒ Forward ☐ Backward

Save

Figure 6-1 Set License Plate Recognition Parameters

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

6.2 Set Feature Parameters

Set non-motor vehicle and pedestrian feature parameters in the application modes of vehicle arming and checkpoint capture.

Before You Start

Set the application mode as vehicle arming or checkpoint capture.

Steps

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

Helmet Detection

Enable it to detect the violation that the non-motor vehicle driver not wearing helmet. Set the detection sensitivity at daytime and night.

Manned Non-Motor Vehicle Detection

Enable it to detect the violation that the non-motor vehicle is carrying other persons except the driver. Set the detection sensitivity.

3. Click **Save**.

6.3 Set Violation Dictionary

Violation dictionary defines corresponding codes of violation types. You can set the violation code, violation type, and violation description in this section. The default parameters are recommended.

Steps

1. Go to **Configuration → Capture → Capture Parameters → Violation Dictionary**.
2. Set **Violation Code**, **Violation Type**, and **Violation Behavior** description according to the actual needs.
3. **Optional**: Click **Default** to restore the parameters to the default settings.
4. Click **Save**.

Result

The violation code and description will be displayed on the captured picture when the corresponding violation happens.

6.4 Set Information Overlay

6.4.1 Set Single Picture Overlay

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

Steps

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

Percentage 100

Transparency 0

Time Format 24-hour

Date Format YYYY-MM-DD

Font Size 16 x 32

Foreground Color fffffff

Background Color 000000

Overlay Position ☐ Overlay on the Picture ☐ Overlay Above the Picture ☒ Overlay Below the Picture

Overlay Number Zeroizing ☒

Overlay Plate Close-up ☐

Overlay OSD on Close-up Picture ☐

Copy to... ☐ Violation Single ☐ Violation Composition

Figure 6-2 Set Single Picture Overlay

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

Percentage

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

Transparency

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

Overlay Number Zeroizing

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

Overlay Plate Close-up

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

Overlay OSD on Close-up Picture

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

5. **Optional:** Check the other channel(s) to copy the same settings.

6. Select the overlay information from the list.



Note

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

7. Set the overlay information.

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

8. Click Save.

6.4.2 Set Composite Picture Overlay

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

Steps

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

Percentage 100

Transparency 0

Time Format 24-hour

Date Format YYYY-MM-DD

Font Size 16 x 32

Foreground Color fffffff

Background Color 000000

Overlay Position ☐ Overlay on the Picture ☐ Overlay Above the Picture ☒ Overlay Below the Picture

Composite Picture Capture Time First

Copy to... ☐ Checkpoint Single ☐ Violation Single

Figure 6-3 Set Composite Picture Overlay

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

Percentage

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

Transparency

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

Composite Picture Capture Time

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

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



Note

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

7. Set the overlay information.

View Default Type	You can view the default overlay information.
Set Type	You can edit the type.
Set Overlay Information	For some information types, you can edit the detailed information.
Set Overlay Position	If you check it, the current information will be displayed from a new line.

Set Space	Edit the number of space between the current information and the next one from 0 to 255. 0 means there is no space.
Set Line Break Characters	Edit the number of characters from 0 to 100 between the current information line and the previous information line. 0 means no line break.
Adjust overlay sequence	Click ^ / v to adjust the display sequence of the overlay information.

8. Click **Save**.

6.5 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**.

Image Encoding

Capture Resolution	2688*1520
Close-up Picture Resolution	2688*1520
Picture Size (KB)	512
Picture EXIF Format Transmission	☒

Figure 6-4 Set Image Encoding Parameters

2. Select **Capture Resolution**.
3. Select **Close-up Picture Resolution**.
4. Set the parameters.

Picture Size

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

Picture EXIF Format Transmission

The captured pictures will be transmitted in the EXIF format.

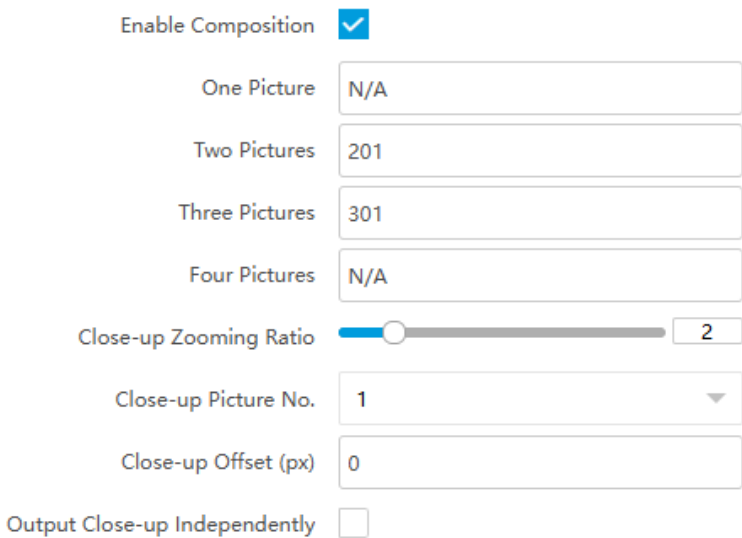
5. Click **Save**.

6.6 Set Picture Composition

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

Steps

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



Enable Composition	☒
One Picture	N/A
Two Pictures	201
Three Pictures	301
Four Pictures	N/A
Close-up Zooming Ratio	<input type="range" value="2"/>
Close-up Picture No.	1
Close-up Offset (px)	0
Output Close-up Independently	☐

Figure 6-5 Set Picture Composition

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

Close-up Zooming Ratio

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

Close-up Picture No.

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

Close-up Offset

The default value is 0, which is recommended to be adopted. The device can capture close-up pictures according to the set offset when no license plate is recognized.

5. **Optional:** Check **Output Close-up Independently** to output close-up pictures independently when the picture composition is not enabled.



Note

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

6. Click **Save**.

6.7 Set Capture Schedule

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

Steps

1. Go to **Configuration → Capture → Capture Parameters → Scheduled Capture**.
2. Check **Enable Scheduled Capture**.
3. Set **Picture Format**, **Resolution**, **Picture Quality**, **Capture Interval**, and **Capture Channel**.
4. Set the capture schedule according to the actual needs.

Enable Scheduled Capture ☒

Picture Format JPEG

Resolution 2688*1520

Picture Quality Low

Capture Interval 5 sec

Capture Channel Channel1

Edit Schedule Time Scheduled Delete

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon														
Tue														
Wed														
Thu														
Fri														
Sat														
Sun														

 Scheduled

Save

Figure 6-6 Set Capture Schedule

5. Adjust the time period.
 - Click on the selected time period, and enter the desired value. Click **Save**.
 - Click on the selected time period. Drag the both ends to adjust the time period.
6. **Optional:** Click  to copy the same settings to other days.
7. Click **OK**.
8. Click **Save**.

6.8 Advanced Configuration



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

6.8.1 System Service

You can enable the functions to debug the device.

Steps

1. Go to **Configuration → Capture → Advanced → System Service**.
2. Enable the functions according to your needs.

Enable Algorithm POS Information Debug

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

Enable Positioning Frame Debug

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

Enable Closed Positioning Frame

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

Priority Mode

If you enter 0, the device will capture pictures only when the recognized license plates by the front and rear lens for stopped vehicle capture are the same. If you enter 1, the device will capture pictures when the front and rear lens recognize license plates for stopped vehicle capture and the license plate numbers are not required to be the same.

Filter Checkpoint Capture of Same Vehicle

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

3. Click **Save**.

Chapter 7 View Real-Time Picture

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

Before You Start

Enable and set the corresponding application mode.

Steps

1. Go to **Live View** → **Real-Time Capture** .
2. Select the arming level.
 -  : 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.
 -  : Level 2 arming can connect three clients or webs. The pictures will be uploaded to the client/web, and stored in the storage card.
 -  : Disable the real-time capture function.
3. Click **Arming** and you can view the capture scene picture and recognized information about the captured license plates and face pictures.

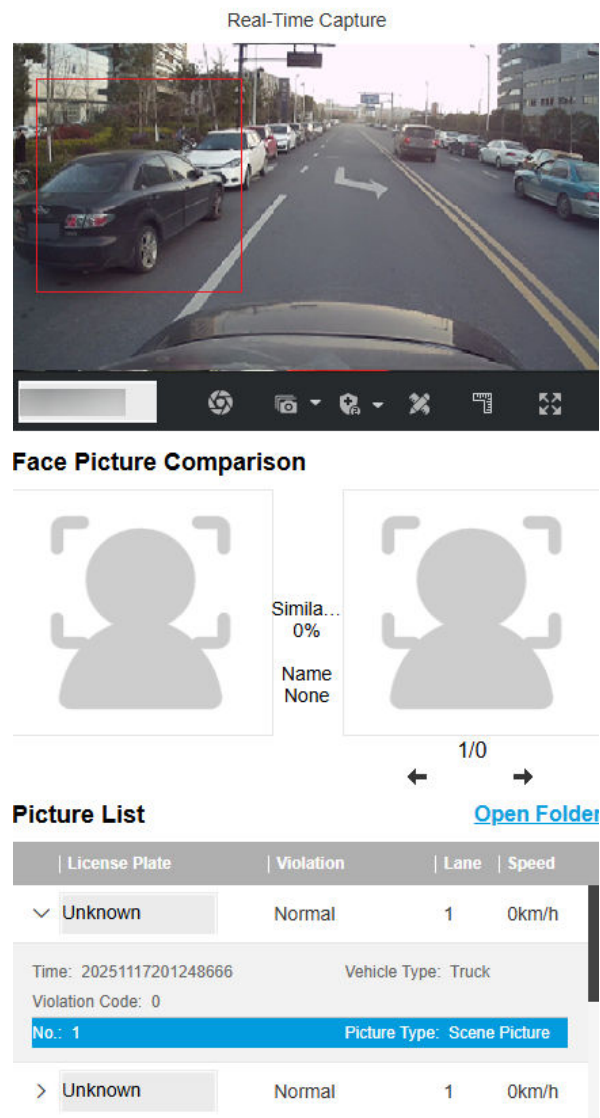


Figure 7-1 Real-Time Capture (Vehicle Capture)

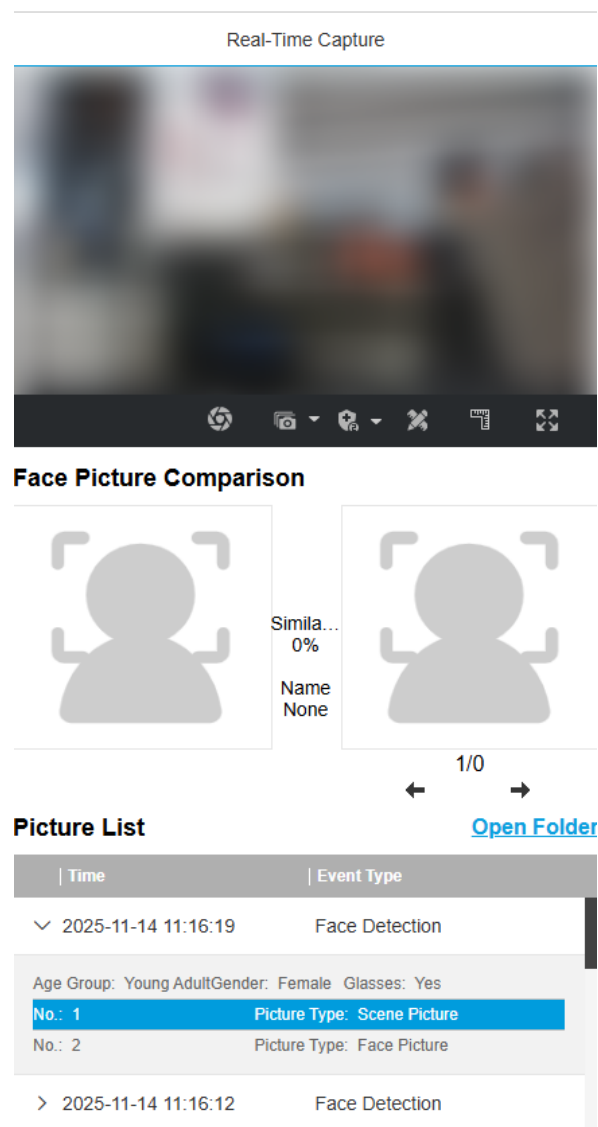


Figure 7-2 Real-Time Capture (Face Picture Capture)

- For the captured vehicle, you can view the captured license plate number, lane, and speed. You can also expand the menu in the picture list to view the captured time, vehicle type, and picture type. View the scene picture on the upper window.
- For the captured face picture, you can view the captured time and event type. You can also expand the menu in the picture list to view the detailed information, such as the age, gender, glasses wearing status, the scene picture, and the close-up face picture. If you have enabled face comparison function, you can view the similarity between the captured face picture and the face picture in the face picture library, and the captured face picture and the face picture in the face picture library in the **Face Picture Comparison** area. You can click ← / → to view the more pictures.

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



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



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



Click it to enable manual capture.



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

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.



Display the images in full screen mode.

**Open
Folder**

Open the saving path of captured pictures.

Chapter 8 Live View and Local Configuration

8.1 Live View

8.1.1 Switch Channel Composition Mode

The device supports one module, two stitching channels, and two single channels for running algorithm. You can switch the composition mode of the channels according to the installation mode of the device.

Steps

1. Click **Live View**.
2. View the live view images of the current mode.

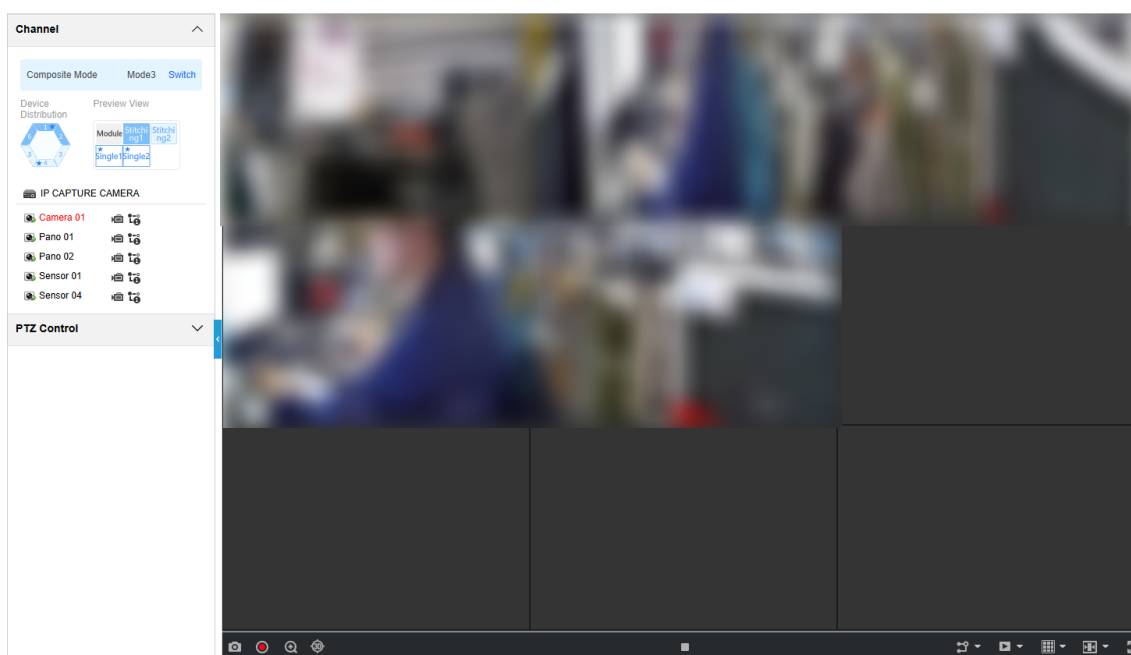


Figure 8-1 Live View

3. Click **Switch** to select other composition modes according to the installation mode of the device.

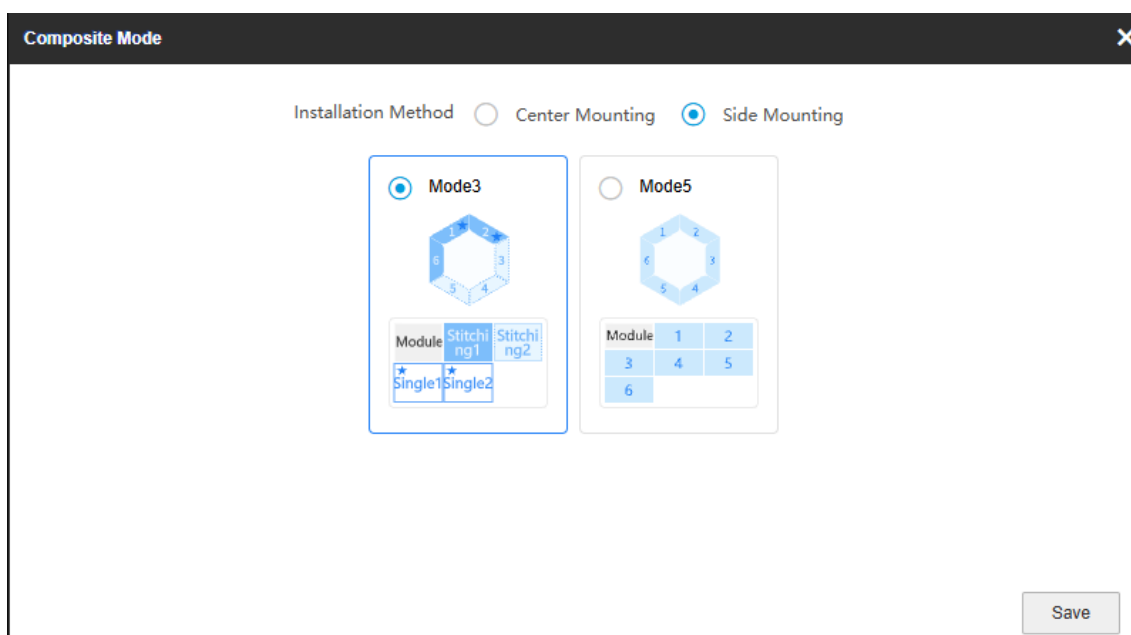


Figure 8-2 Switch Channel Composition Mode

Example

You can select the stitching mode 3 or non-stitching mode 5. For stitching mode 3, channel 1, 2, and 6 will compose a stitching channel 1 (dark blue colored) to show a panoramic view; and channel 3, 4, and 5 will compose another stitching channel 2 (light blue colored) to show a panoramic view. The two channels marked with five-pointed stars are the two single channels for running algorithm. For non-stitching mode 5, all the channels are working independently.

4. Click **Save**, and follow the prompt to reboot the device to take the settings into effect.

8.1.2 Start/Stop Live View

Double click the corresponding channel in the channel list to start/stop live view of a single channel. Click  to start live view of all the channels. Click  to stop live view of all the channels.

8.1.3 Select Image Display Mode

Click  to select an image display mode.

8.1.4 Select Window Division Mode

Click  to select a window division mode.

8.1.5 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.

8.1.6 Capture Picture Manually

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

Steps

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

8.1.7 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.

8.1.8 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.

8.1.9 Enable 3D Positioning

You can enable 3D positioning to select an area of the live view image and move it to the center of the image to zoom in and view the details.

Steps

1. Click .

The icon will change to , which means the 3D positioning is enabled.

2. Click anywhere of the image, and the lens will move the image center to the point.

- Hold the left button of the mouse to draw a rectangular area to the lower/upper right of the image, and then the lens will move the image center to the area and zoom in.
- Hold the left button of the mouse to draw a rectangular area to the upper/lower left of the image, and then the lens will move the image center to the area and zoom out.

3. Click  to disable the 3D positioning.

8.1.10 Select Video Mode

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

Click  and select  when the device is running normally.

8.2 Set Snapshot Mode

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

- Enable **Snapshot**. 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.
- Disable **Snapshot**. 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.

8.3 Local Configuration

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

 Note

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

Live View Parameters

Protocol Type

☒ TCP

☐ UDP

☐ HTTP

☐ HTTPS

Stream Type

☒ Main Stream

☐ Sub-Stream

Live View Performance

☐ Shortest Delay

☒ Balanced

☐ Fluency

Decoding Type

☒ Software Decoding

☐ Hardware Decoding

Rules Information

☐ Enable

☒ Disable

Feature Information

☐ Enable

☒ Disable

Image Size

☒ Auto-fill

☐ 4:3

☐ 16:9

Image Format

☒ JPEG

☐ BMP

Rendering Engine

☐ D3D9

☒ D3D11

Record File Settings

Record File Size

☐ 256M

☒ 512M

☐ 1G

Save record files to

C:\Users\ \PluginWeb\RecordFiles

Browse

Save downloaded files to

C:\Users\ \PluginWeb\DownloadFiles

Browse

Picture and Clip Settings

Save snapshots in live view to

C:\Users\ \PluginWeb\CaptureFiles

Browse

Save downloaded pictures to

C:\Users\ \PluginWeb\ViewPics

Browse

Save scene pictures to

C:\Users\ \PluginWeb\ScenePics

Browse

Save snapshots when playback to

C:\Users\ \PluginWeb\PlaybackPics

Browse

Save clips when playback to

C:\Users\ \PluginWeb\PlaybackFiles

Browse

Figure 8-3 Local Configuration

Protocol Type

Select the network transmission protocol according to the actual needs.

TCP

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

UDP

Provides real-time audio and video streams.

HTTP

Gets streams from the device by a third party client.

HTTPS

Gets streams in https format.

Stream Type

Main Stream

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

Sub-Stream

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

Live View Performance

Shortest Delay

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

Balanced

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

Fluency

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

Decoding Type

Software Decoding

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

Hardware Decoding

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

Rules Information

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

Feature Information

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

Image Size

The display ratio of the live view image.

Image Format

The saving format of manually captured images.

Rendering Engine

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

Record File Size

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

Save record files to

Set the saving path of the manually recorded video files.

Save downloaded files to

Set the saving path of the download files.

Save snapshots in live view to

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

Save downloaded pictures to

Set the saving path of the downloaded pictures.

Save scene picture to

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

Save snapshots when playback to

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

Save clips when playback to

Set the saving path of the clips in playback mode.

Chapter 9 PTZ Control

9.1 PTZ Control Panel

Click **Live View**. Expand the PTZ control panel on the left of the interface.

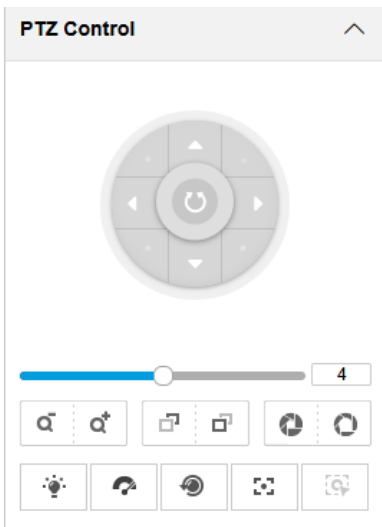


Figure 9-1 PTZ Control Panel

 Note

The PTZ supports power-off memory. When the device is suddenly cut off power or restarted normally, it can automatically return to the position before the power cut or reboot.

The button descriptions are as follows:

Table 9-1 Button Description

Button	Description
	Hold the direction buttons to pan/tilt the device. Click  , and the device keeps panning. Click it again to stop panning.
	Adjust the PTZ speed.
	Zoom + and Zoom - • Hold  to zoom in the scene. • Hold  to zoom out the scene.
	Focus + and Focus -

Button	Description
	- Hold  under the manual focus mode to make near objects become clear and distant objects become vague. - Hold  to make distant objects become clear and near objects become vague.
 / 	Iris + and Iris – - Hold  to increase the iris diameter when in a dark environment. - Hold  to decrease the iris diameter when in a bright environment.
	Light Enable/Disable the supplement light manually.
	Wiper Click the icon to clear the lens.
	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.

9.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click  .

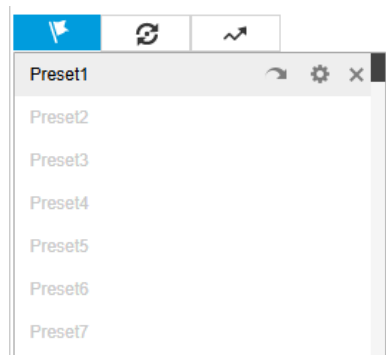


Figure 9-2 Set Preset

- 2. Operate the direction buttons of the PTZ control panel to turn the PTZ to the desired position.
- 3. Select the preset to be set.
- 4. Click  to save the settings.
- 5. **Optional:** You can call, reset, and delete the preset.

- Call preset** Click  , and the PTZ will turn to the set position.
- Reset preset** Operate the PTZ and click  to reset the preset.
- Delete preset** Click  to delete the PTZ position information corresponding to the preset.

- 6. **Optional:** Some presets are predefined with special commands. You can only click  to call them.

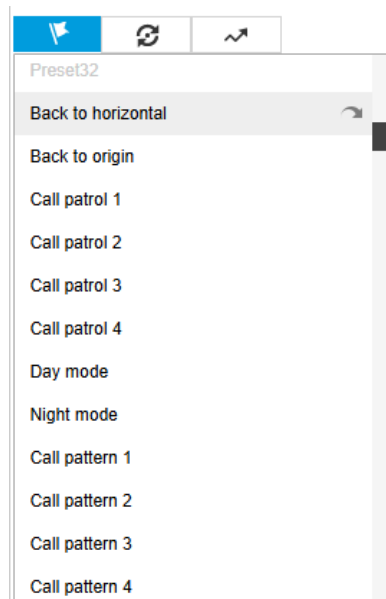


Figure 9-3 Special Presets

9.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

Before You Start

Set two or more presets.

Steps

1. Click .
2. Click  of a patrol path.
3. Click  to add the presets.

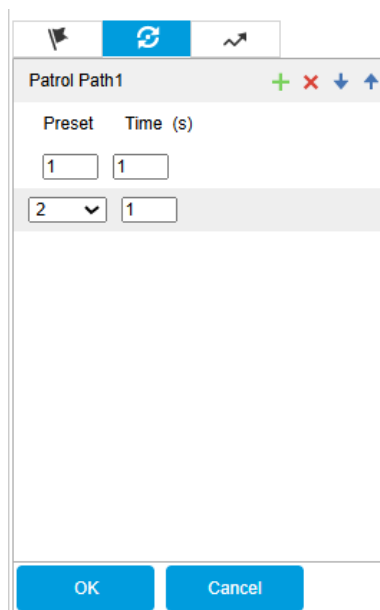


Figure 9-4 Set Patrol Scan

- 1) Select **Preset**.
- 2) Enter **Time**, which is the duration of the device on one patrol point.
- 3) Click **OK**.
- 4) Repeat the above steps to add more presets.



Note

- At least 2 presets need to be added in one patrol path.
- Up to 32 presets can be added in one patrol path.
- You can click   to adjust the preset sequence, or click  to delete the added preset.

4. Optional: Other operations.

Start/stop patrol Click  /  to start/stop patrol.

Delete patrol path Click  to delete the whole patrol path.

9.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

1. Click , and select a pattern scan path.

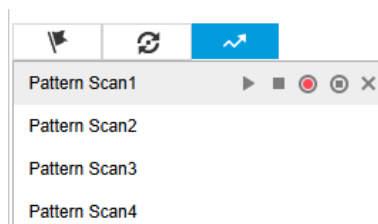


Figure 9-5 Set Pattern Scan

2. Click  to start recording the pattern scan.
3. Click PTZ control buttons as needed.
4. Click  to stop recording and save the pattern scan path.
5. **Optional:** Other operations.

Start/stop pattern scan Click  /  to start/stop pattern scan.

Delete pattern scan Click  to delete the pattern scan path.

9.5 Enable Proportional Pan

The device supports setting proportional pan. In the keyboard control mode, the device pans or tilts adaptively according to the zoom speed. When there is a higher zoom speed, the pan/tilt speed will be reduced automatically. When there is a lower zoom speed, the pan/tilt speed will be increased automatically.

Steps

1. Go to **Configuration → PTZ → PTZ → Basic Settings**.

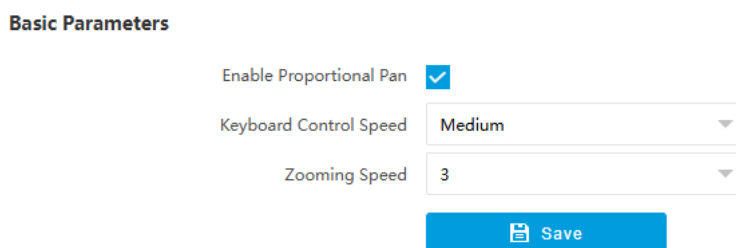


Figure 9-6 Enable Proportional Pan

2. Check **Enable Proportional Pan**.

3. Set the parameters.

Keyboard Control Speed

The higher the level is, the faster the device pans or tilts.

Zooming Speed

The higher the value is, the faster the zooming speed is.

4. Click **Save**.

9.6 Set Park Action

You can set a certain action or return to a certain position that the PTZ needs to perform when it does not receive a control signal within the park time.

Before You Start

Set the desired action mode. For example, if you need to realize pattern scan, set the pattern scan first.

Steps

 Note

Scheduled task is prior to park action. When these two functions are set at the same time, only the scheduled task function takes effect.

1. Go to **Configuration → PTZ → PTZ → Park Action**.

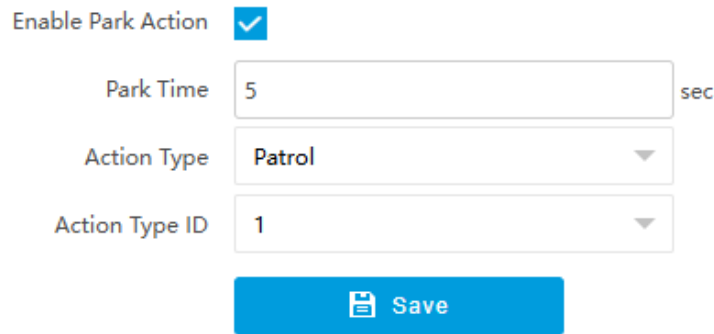


Figure 9-7 Set Park Action

2. Check **Enable Park Action**.

3. Set **Park Time** as the inactivity time of the PTZ before it starts the park actions.

4. Select **Action Type**.

 Note

Action type may vary with different models. Please refer to the actual product.

5. Set **Action Type ID**.

6. Click **Save**.

9.7 Set Scheduled Task

You can set the device to perform a certain task during a certain period.

Steps

1. Go to **Configuration → PTZ → PTZ → Scheduled Task**.
2. Enable scheduled task.
3. Enter **Park Time**.

During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.

4. Select **Task Type** and the corresponding No. Set the schedule.

Advanced

Enable Scheduled Task ☒

Park Time s

Scheduled Tasks

Task Type Preset 1 Delete

Day	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Save

Legend:
Disable
Patrol
Pattern
Preset
Reboot Dome

Figure 9-8 Set Scheduled Task



Note

The configuration method is same with that of recording schedule. Refer to [Set Record Schedule](#) for details.

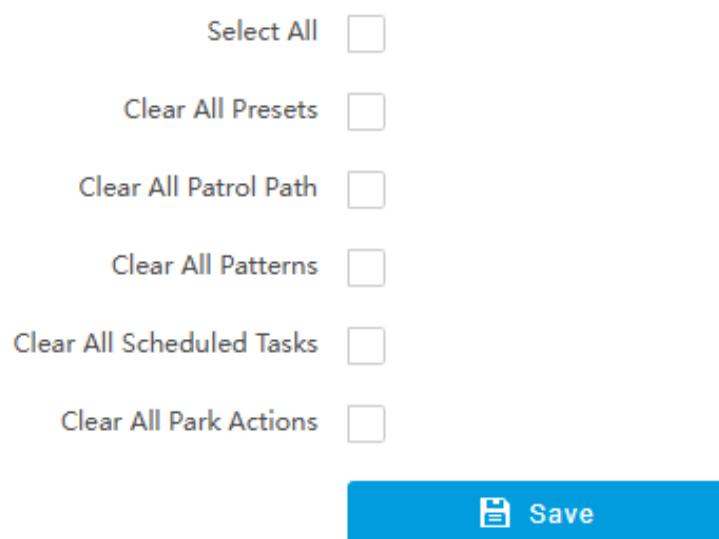
5. Click **Save**.

9.8 Clear Configuration

You can clear the set presets, patrols, patterns, privacy masks, scheduled tasks, and park action.

Steps

1. Go to **Configuration** → **PTZ** → **PTZ** → **Clear Config**.



The screenshot displays a configuration interface with the following elements:

- Four checkboxes are arranged in a vertical column on the left, each with a corresponding label to its right:
 - ☐ Select All
 - ☐ Clear All Presets
 - ☐ Clear All Patrol Path
 - ☐ Clear All Patterns
- Below these, there are two more labels with checkboxes to their right:
 - Clear All Scheduled Tasks ☐
 - Clear All Park Actions ☐
- At the bottom right, there is a blue rectangular button with a white floppy disk icon and the text "Save".

Figure 9-9 Clear Configuration

2. Check the configuration(s) to clear according to the actual needs.
3. Click **Save**.

Chapter 10 Record and Capture

10.1 Set Storage Path

10.1.1 Set Storage Card

If you want to store the files to the storage card, make sure you have installed and formatted the storage card in advance.

Before You Start

Install the storage card to the device.

Steps

Note

- For storage card used for the first time, you need to partition the quota and format it manually before using it normally. After the storage card is formatted, the former content in the storage card will be cleared and the storage will be partitioned according to the set quota ratios.
- If the storage card already has files, back up important files before formatting it.

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

HDD Storage

Format

☐	HDD No.	Free Space/Space	Status	Type	Property	Operation
No Data						

Auto-Initialize Redundant Storage ☒

Auto-Upload Data in Redundant Storage ☒

Interval(ms) 200

HDD Quota

Picture Capability(MB) 0

Video Capability(MB) 0

Face Picture Library Capacity (MB) 0

Capture Quota Ratio(%) 20

Video Quota Ratio(%) 50

Face Picture Library Quota (%) 30

Save

Figure 10-1 Set Storage Card

2. Set Capture Quota Ratio, Video Quota Ratio, and Face Picture Library Quota according to the actual needs.

Note

- The percentage sum of the capture, video, and face picture library quota ratios should be 100%.
- Reboot the device after the face picture library partition is formatted for the first time.

3. Check the storage card, and click **Format** to format it manually.



Note

You can click  to format the specific storage partition.

4. Enable other functions according to your needs.

Auto-Initialize Redundant Storage

Enable the function to format the storage card automatically when the card is abnormal.
Reboot the device to take the settings into effect.

Auto-Upload Data in Redundant Storage

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

5. Click **Save**.

10.1.2 Set Cloud Storage

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

Before You Start

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



Note

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

Steps

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

Enable ☒

Version

Server IP Address

Port

Access Key

Secret Key

Resource Pool ID

 Save

Figure 10-2 Set Cloud Storage

2. Check **Enable**.

3. Select **Version**.

- V1.0**
 - a. Enter **Server IP Address** and **Port**.
 - b. Enter **User Name** and **Password**.
 - c. Enter **Cloud Storage ID** and **Violation Cloud Storage ID** according to the server storage area No.
- V2.0**
 - a. Enter **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**.

10.2 Set Record Schedule

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

Before You Start

Install the storage card.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule**.
2. Select **Record Stream** and **Record Channel**.
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

Record Channel: Channel1

Enable Overwritten Recording: ☒

Enable Storing Expiration: ☒

Expired Time (day): 7

Enable Record Schedule: ☒

Record Configuration

Record Type: Scheduled

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon														
Tue														
Wed														
Thu														
Fri														
Sat														
Sun														

Scheduled

Figure 10-3 Set Record Schedule

5. Select **Record Type**.
6. 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.

7. 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.
8. **Optional:** Delete recording periods.
- Click a set recording period and click **Delete** in the pop-up window.
 - Click a set recording period and click **Delete** on the record configuration interface.
9. **Optional:** Click to copy set recordings to other days.

10. Click **Save**.

Result

The device will only record at the set periods.

10.3 Set Snapshot Schedule

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

Before You Start

Install the storage card.

Steps

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

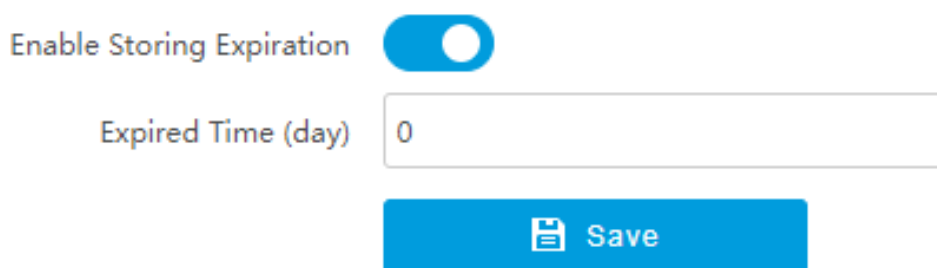


Figure 10-4 Set Snapshot Schedule

2. Enable storing expiration.

3. Set **Expired Time**.

4. Click **Save**.

Result

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

10.4 Search Picture

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

Before You Start

Install the storage card, and ensure the storage status is normal.

Steps

1. Click **Picture**.

2. Set search conditions.



Note

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

3. Click **Search**.

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



Note

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

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

Download pictures	Check picture(s) and click Download to save them to local. The downloaded picture(s) will be marked as "Downloaded". You can go to Configuration → Local to check the saving path.
View picture details	Click Live View to view the picture details, such as the license plate number, vehicle type, etc.

10.5 Playback

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

Steps

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

Set playback time	Drag the time bar to the target time and click  to play the video.
Capture image	Click  to capture an image.
Clip record	Click  /  to start/stop clipping the record.
Play back in single frame	Click  once to play back the video in one frame.
Download record	a. Click . b. Select the start time and end time. c. Click Search. d. Check record files that need to be downloaded. e. Click Download.
Stop playback	Click  to stop playback.
Slow forward	Click  to slow down the playback.

Fast forward

Click  to speed up the playback.

Digital zoom

Click  to enable digital zoom.

Click  to disable digital zoom.

Chapter 11 Encoding and Display

11.1 Set Camera Parameters

If the image quality is poor, you can set camera parameters to adjust image features.

Steps

1. Go to **Configuration → Video → Camera Parameters → Camera Parameters**.
2. Select the camera module or other channels.



Note

- The supported parameters for the camera module and single channels are different.
- You can click **Default** to restore the parameters to default settings.

-
3. Set camera module parameters.

- 1) Set the image adjustment parameters.

Brightness

The brightness of the image.

Contrast

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

Saturation

The colorfulness of the image color.

Sharpness

The edge contrast of the image.

- 2) Set the exposure parameters.

Exposure Mode

Auto

The aperture, shutter, and gain values will be adjusted automatically according to the brightness of the environment. You can set **Maximum Aperture Limit**, **Minimum Aperture Limit**, **Maximum Shutter Limit**, **Minimum Shutter Limit**, **Limit Gain**, and **Low Illumination Digital Shutter** for better exposure effect.

Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values will be adjusted automatically according to the brightness of the environment.

Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values will be adjusted automatically according to the brightness of the environment.

- 3) Set the focus parameters.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under the auto mode, reduce light sources in the image and avoid flashing lights.

Manual

You can adjust the focus manually on the live view page.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus will not change when the scene changes.

Minimum Focusing

If the distance between the scene and lens is shorter than the **Minimum Focusing**, the lens will not focus.

- 4) Set the day/night switch parameters.

Day/Night Switch

Daytime/Nighttime

The system will be switched to the day or night mode.

Auto

The device will switch automatically between the day mode and the night mode according to the illumination.

Schedule

The device will switch to the day mode according to the set **Start Time** and the **End Time**.

- 5) Set backlight parameters.

BLC Area

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. Backlight Compensation (BLC) can lighten up the object in the front to make it clear.

WDR

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

HLC

High Light Compression (HLC) function stands for highlight compensation. The camera detects the strong spots (the over-exposure portion of image), and then reduces the brightness of the strong spots to improve the overall image quality.

- 6) Select **White Balance** mode according to the environment.

- 7) Set the image enhancement parameters.

Digital Noise Reduction

It is used to reduce the image noise and improve the image quality. Enable the function and set **DNR Level** to control the noise reduction degree. The higher the level is, the stronger the reduction degree is.

Defog Mode

You can enable the function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

EIS

Enable the function to increase the stability of video image by using jitter compensation technology.

- 8) Set the video adjustment parameters.

Video Standard

You can set **Video Standard** according to the video system in your country.

- 9) Set other parameters.

Lens Initialization

It is used to reset lens when long time zooming or focusing results in the blurred image.

Zoom Limit

You can set the maximum value of zooming.

4. Set other single channel parameters.

General

Saturation

It refers to the colorfulness of the image color.

Sharpness

It refers to the edge contrast of the image.

White Balance

It is the white rendition function of the device used to adjust the color temperature according to the environment. Set **White Balance Level**.

Brightness Enhancement at Night

The scene brightness will be enhanced at night automatically.

Enable 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.

Enable Gamma Correction

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

Video

Brightness

The brightness of the image.

Contrast

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

Shutter

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

Gain

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

Hue Range

Select the range to adapt to the display.

3D DNR

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

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

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

2D DNR

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

Video Standard

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

5. Optional: Click **Capture Test** to test the image effect.

11.2 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** .
2. Select the camera module or other single channels.

Overlay Information

Camera Name ☒

Camera Name

Display Date ☒

Time Format

Date Format

Display Week ☒

Millisecond ☐

Custom Information

Status

Display Mode

OSD Size

OSD Color

Alignment

Figure 11-1 Set OSD

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



Note

Up to 6 items of custom information can be added.

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



Note

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

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

Result

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

11.3 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. Select a channel.
3. Set the parameters.

Stream Type

Select the stream type according to your needs.



Note

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

Bitrate

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

Frame Rate

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

Resolution

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

SVC

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

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

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

Profile

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

I Frame Interval

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

Video Encoding

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

4. Click **Save**.

11.4 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**.
2. Select the camera module or other single channels.

Stream Type

Stream Type Main Stream (Scheduled) ▼

Fixed Area

Enable ☒

Area No. 1 ▼

ROI Level 1 ▼

Area Name

 Save

Figure 11-2 Set ROI

3. Select **Stream Type**.
4. Set ROI region.
 - 1) Check **Enable**.
 - 2) Select **Area No.**
 - 3) Click **Draw Area**.
 - 4) Drag the mouse on the live view image to draw a fixed area.
 - 5) Select the fixed area that needs to be adjusted and drag the mouse to adjust its position.
5. Select **ROI Level** and enter **Area Name**.



Note

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

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

Chapter 12 Event and Alarm

12.1 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 → Incident → Alarm Linkage → Exception** .
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

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

Chapter 13 Safety Management

13.1 Manage User

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

Steps

1. Go to **Configuration → System → User Management → User List**.
2. Select **Password Level**.

The password level of the added user should conform to the selected level.

3. Add a user.
 - 1) Click **Add**.
 - 2) Enter **User Name** and select **User Type**.
 - 3) Enter **Admin Password**, **New Password**, and confirm the password.



Caution

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

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

User

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

Operator

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

- 5) Click **OK**.

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

Change the password and permission Click  to change the password and permission.

Delete the user Click  to delete the user.

13.2 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.

13.3 Set SSH

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

Steps

1. Go to **Configuration → System → Security → Security Service → Software**.
2. Enable or disable **SSH Service**, and set **SSH Port** if you enable the function.
3. Click **Save**.

13.4 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**.

13.5 Enable System Log Service

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

Steps

1. Go to **Configuration → System → Security → Security Service → Log Audit Service**.
2. Enable system log service.
3. Enter **IP Address** and **Port** of the log server.
4. Click **Save**.

Result

The device will upload the security audit logs to the log server regularly.

13.6 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

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

Result

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

13.7 Set Password Validity Period

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

Steps

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

13.8 Set SDK Protocol Authentication Mode

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

Steps

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



Note

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

3. Click **Save**.
-

13.9 Set RTSP Authentication

You can improve network access security by setting RTSP authentication.

Steps

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

digest

The device only supports digest authentication.

3. Click **Save**.

13.10 Set IP Address Filtering

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

Steps

1. Go to **Configuration → System → Security → Security Settings**.
2. 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**.

13.11 Set HTTPS

13.11.1 Create and Install Self-signed Certificate

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

Steps

1. Go to **Configuration → Network → Network Parameters → HTTPS**.
2. Select **Create Self-signed Certificate**.

3. Click **Create**.
4. Follow the prompt to enter **Country/Region, Domain/IP, Validity**, and other parameters.
5. Click **OK**.

Result

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

13.11.2 Install Authorized Certificate

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

Steps

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

Chapter 14 Maintenance

14.1 View Device Information

Basic Information and Algorithms Library Version

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

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

Device Status

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

14.2 Synchronize Time

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

Steps

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

NTP Time Sync.

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

Manual 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.

PTP Time Sync.

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

No

Select it to disable time synchronization.

All

Select it, and you can select any mode above.

4. Click **Save**.

14.3 Set DST

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

Steps

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

14.4 Set RS-485

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

Before You Start

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

Steps



Note

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

-
1. Go to **Configuration → System → System Settings → Serial Port → RS-485**.
 2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.



Note

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

-
3. Set **Work Mode**.

Application Trigger

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

Transparent Channel

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

4. Click **Save**.

14.5 Set RS-232

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

Before You Start

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

Steps

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



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

3. Select **Work Mode**.



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

Console

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

Transparent Channel

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

Narrow Bandwidth Transmission

Reserved.

4. Click **Save**.

14.6 Reboot

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

Steps

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



Note

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

14.7 Restore Parameters

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

Steps

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

14.8 Export Parameters

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

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Export Data** .
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**.

14.9 Export Debug File

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

Steps

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

14.10 Export Diagnosis Information

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

Steps

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

14.11 Upgrade

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

Before You Start

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

Steps

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



Note

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

Result

The device will reboot automatically after upgrade.

14.12 Export Violation Type File

You can export the violation type file to check the violation types of the vehicles.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Advanced Settings → Violation Code** .
2. Click **Export**.
3. Select the saving path and enter the file name.
4. Click **Save**.

14.13 Import Violation Code File

Violation codes define the violation behaviors to make it convenient to recognize the violations. You can import the violation codes to define the violation behaviors quickly.

Before You Start

Save the violation code file to the computer.

Steps



Note

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

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance → Advanced Settings → Violation Code**.
 2. Click **Browse** to select the violation code file.
 3. Click **Import**.
-



Note

The importing process will take 1 to 5 minutes. Do not power off.

What to do next

Reboot the device to take the settings into effect.

14.14 Import Configuration File

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

Before You Start

Save the configuration file to the computer.

Steps



Caution

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

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



Note

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

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

6. Click **OK** on the popup window.

Result

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

14.15 Search Log

Log helps to locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log Search** .
2. Set search conditions.
3. Click **Search**.

The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files to your computer.

14.16 Enable Log According to Module

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

Steps

1. Go to **Configuration → System → Maintenance → Debug → Log** .
2. Check the module(s) according to your needs.
3. **Optional:** If you want to disable the log automatically, you can enable **Disable Log Automatically**.
4. Click **Save**.

14.17 Enable Maintenance Service

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

Steps

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

Maintenance Service

Enable Maintenance Service ☒

Agent Settings

Address Type: IPv4 Address

IPv4 Address:

Port:

Client Identifier Type: Custom

Client Identifier:

Authentication Information

User Name: admin

Password:

Heartbeat Cycle(s): 120

End Time: 2024-04-10 06:17:17

Status: Offline

Protocol Settings

+ Add

No.	Name	Protocol Type	Client Target IP Address	Client Target Port	Max. Number of Simultaneous Accesses via Client	Operation
1	SSH	TCP			5	

Figure 14-1 Maintenance Service

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

User Name/Password

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

Heartbeat Cycle(s)

You are recommended to keep the default value.

End Time

The camera will disconnect with the platform server when reaching the set end time.

5. Set protocol parameters.
- 1) Click **Add** to add a protocol.
 - 2) Set the corresponding parameters of the protocol.



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

6. Click **Save**.

What to do next

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



See Far, Go Further