



Incident Detection Server

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 Production Introduction	1
1.2 Key Feature	1
1.3 Running Environment	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 Basic Operation	5
3.1 Set IP Address	5
3.2 Set Static Router	7
3.3 Manage Camera	8
3.3.1 Add Organization	8
3.3.2 Add Camera	9
3.3.3 Search Added Camera	11
3.4 Set Remote Host	11
3.4.1 Set Upload Strategy	15
Chapter 4 Traffic Incident Detection	17
4.1 Set Camera Parameters	17
4.2 Set Violation Incident Detection	17
4.2.1 Set Smart Analysis Parameters	17
4.2.2 Set Scene	20
4.2.3 Set Preset Scene	20
4.2.4 Set Violation Incident	22

4.2.5 Set Scene Patrol	29
4.3 Set VQD	30
4.4 Set Detection Parameters	31
4.4.1 Set License Plate Recognition Parameters	31
4.4.2 Set Evidence Code	31
4.4.3 Set Picture Composition	31
4.4.4 Set Text Overlay	32
Chapter 5 Data Management	35
5.1 View Statistics Result	35
5.2 View Real-Time Data	35
5.3 Search Traffic Data	36
5.4 View Traffic Flow Statistics	37
5.5 Back up Data	38
5.5.1 Back up to Local Storage	38
5.5.2 Back up to USB	38
Chapter 6 Live View and Local Configuration	40
6.1 Live View	40
6.1.1 Start/Stop Live View	40
6.1.2 Select Window Division Mode	40
6.1.3 Manual Evidence Capture	40
6.1.4 Capture Manually	41
6.1.5 Record Manually	42
6.1.6 Display in Full Screen	42
6.2 PTZ Control Panel	42
6.3 Local Configuration	43
Chapter 7 Network Configuration	46
7.1 Connect to Platform	46
7.1.1 Connect to SDK Platform	46

7.1.2 Connect to HTTP Platform	46
7.2 Set DDNS	47
7.3 Set Port	48
7.4 Set ONVIF	48
Chapter 8 Record and Playback	49
8.1 Set Storage Path	49
8.1.1 Format Disk	49
8.1.2 Set FTP	49
8.1.3 Set Cloud Storage	51
8.2 Set Quota	53
8.3 Enable Record	53
8.4 Playback	53
8.5 Backup	54
Chapter 9 Serial Port Configuration	55
9.1 Set RS-485	55
9.2 Set RS-232	55
Chapter 10 Safety Management	56
10.1 Manage User	56
10.2 Install Authorized Certificate	56
10.3 Create and Install Self-signed Certificate	57
10.4 Set SSH	57
10.5 Enable System Log Service	58
Chapter 11 Maintenance	59
11.1 View Device Information	59
11.2 View Running Status	59
11.3 View Audio/Video Parameters	59
11.4 Log	59
11.4.1 Search Log	59

11.4.2 Export Debugging Log	59
11.5 Upgrade	60
11.6 Reboot	60
11.7 Restore Parameters	61
11.8 Synchronize Time	61
11.9 Synchronize Camera Time	61
11.10 Set DST	62
11.11 Export Parameters	62
11.12 Import Parameters	62
11.13 Reserved Parameters	63

Chapter 1 Introduction

1.1 Production Introduction

Incident detection server, the multiple-channel video analysis device, provides multiple functions, including real-time smart detection of incidents and traffic parameters collection. It can capture the detected incidents, and recognize license plates. It is widely applied in cities, highways, tunnels, etc.

1.2 Key Feature

- Box cameras and speed domes are connectable to detect traffic events and collect traffic parameters.
- Rack-mounted 1U chassis design, convenient to be placed in the cabinet of machine room.
- Supports multiple events detection, such as congestion, parking, wrong-way driving, etc.
- Supports multiple traffic parameters collection, such as vehicle type, lane flow, speed, space headway, time headway, etc.
- Supports zooming capture of illegal parking and patrol detection of multiple scenes when a speed dome is connected.
- Supports operation via web browser.
- Supports customizing specific events detection.



Note

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

1.3 Running Environment

- Browser: Chrome 80 and above versions recommended.
- Resolution: 1366 × 768 and above.

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.

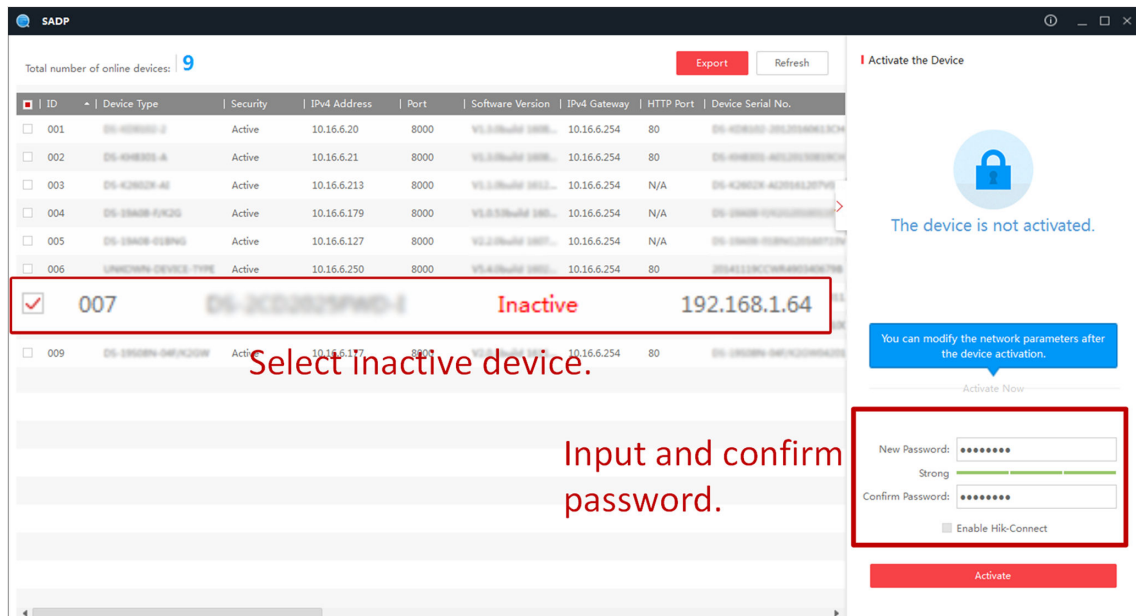


Figure 2-1 Activate via SADP

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 Basic Operation

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

1. Go to **System** → **Network Settings** → **TCP/IP** .
2. Select a network card.

Network Card 1

Network Card 2

NIC Type

10M/100M/1000M Auto

DHCP

IPv4 Address

IPv4 Subnet Mask

IPv4 Default Gateway

IPv6 Address

IPv6 Prefix Length

IPv6 Default Gateway

::

Mac Address

MTU

DNS Server

Preferred DNS Server

Alternate DNS Server

Save

Figure 3-1 Set IP Address

3. Select **NIC Type** according to the actual network.
4. Set relevant network parameters.
 - Enable **DHCP** to get the IPv4 and IPv6 addresses automatically if the network supports distributing the IP addresses automatically.
 - Manually enter the IPv4 and IPv6 parameters and the MTU according to the actual network conditions.



Note

- The network segments of different network cards should be different.
- **MTU** stands for the maximum transmission unit in the network.
- Set **DNS Server** if remote domain name access is needed.

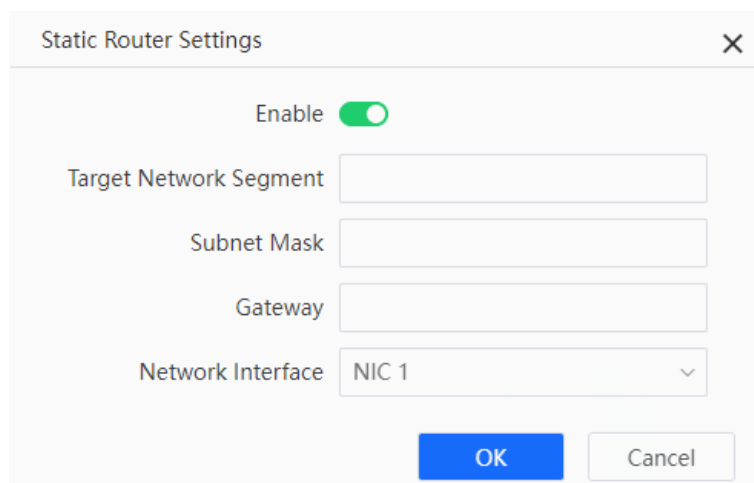
5. Click **Save**.

3.2 Set Static Router

Set a static router for access across network segments. The device will transmit data as a router.

Steps

1. Go to **System → Network Settings → Static Router**.
2. Click **Add** to add a static router.



The image shows a 'Static Router Settings' dialog box. It has a title bar with a close button (X). Inside, there is an 'Enable' toggle switch which is turned on (green). Below this are four input fields: 'Target Network Segment', 'Subnet Mask', 'Gateway', and 'Network Interface'. The 'Network Interface' field is a dropdown menu currently showing 'NIC 1'. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 3-2 Add Static Router

3. Enable the function.
4. Enter **Target Network Segment**, **Subnet Mask**, and **Gateway**.



Note

Set the gateway according to the selected network interface.

5. Select the network interface that needs external communication for routing.
 - When you need other network segments to access the connected camera through the NIC 1, set the NIC 1 as a static router, and the internal IP address will serve as the gateway.
 - When you need to upload data to other network segments through the NIC 2, set the NIC 2 as a static router, and the external IP address will serve as the gateway.
6. Click **OK**.



Note

The device supports deleting or editing the added router.

7. **Optional:** Select the added static router, click **Edit** to edit the parameters, or click **Delete** to delete it.

3.3 Manage Camera

3.3.1 Add Organization

Add organizations before adding cameras.

Steps

1. Click **Resource Management**.
2. Click **Add** on the left side of the interface.
3. Select **Upper-Level Organization**, and enter **Organization Name**.

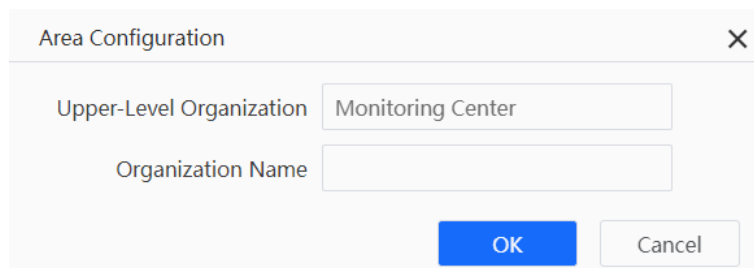


Figure 3-3 Add Organization

Example

For example, if the upper-level organization is Monitoring Center and the organization name is Park 1, then Park 1 belongs to Monitoring Center.

4. Click **OK**.
5. **Optional:** Repeat the above steps to add more organizations.
6. **Optional:** You can also do the following operations.

Edit Organization Name	Click Edit on the left side of the interface, select Upper-Level Organization , change Organization Name , and then click OK .
Delete Organization	Select the organization you want to delete, and click Delete .



Note

The root organization cannot be deleted.

3.3.2 Add Camera

Add cameras before managing and analyzing data.



- If a camera supports multi-stream, multi-stream is supported only when it is added via a private protocol, otherwise the camera only supports main stream for preview and recording.
 - Up to 4 cameras can be added.
-

Quick Add

If cameras need to be added via the parameters such as the default protocol and the port, it is recommended to use quick add.

Before You Start

Connect the device to the camera via the network interface.

Steps

1. Click **Resource Management**.
 2. Select the target organization on the left side.
 3. Click **Quick Add**.
 4. Check the camera that needs to be added, enter the corresponding user name and password, and click **OK**.
-



You can check cameras that have the same user name and password to add in batch.

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

Edit	Edit the added camera information.
Delete	Delete the added camera.
Scene Configuration	Click to reach Smart Traffic Settings → Param Config interface quickly to set the corresponding parameters.

Manual Add

Add manually if you need to customize the access protocol or port.

Before You Start

- Connect cameras to the device via the network interface.
- Add an organization.

Steps

1. Click **Resource Management**.

- 2. Select the target organization on the left side.
- 3. Click **Add Channel**.

IP Camera

Upper-Level Organization

Monitoring Center

Camera Name

IPC-1

Stream Type

Main Stream

IP Address

Protocol Type

PRIVATE

Management Port

8000

Channel No.

1

User Name

admin

Password

.....

Confirm

.....

Camera Type

Box Camera

OK

Cancel

Figure 3-4 Manual Add

- 4. Enter **Camera Name**.
- 5. Select **Stream Type**.
- 6. Enter the camera IP address, port, user name, password, and other information.

 Note

Channel No. is only used to select the access channel when multiple channel devices are accessed. For example, if you want to access a camera with 5 channels, you can select Channel 2 to access the camera, and then enter 2 for **Channel No.**

- 7. Select **Protocol Type** of the added camera.

 Note

The device and the camera should both support the selected protocol type.

- 8. Click **OK**.
- 9. **Optional:** You can also do the following operations.

Edit	Edit the added camera IP address.
Delete	Delete the added camera.
Scene Configuration	Click to reach Smart Traffic Settings → Param Config interface quickly to set the corresponding parameters.

Batch Add

Add cameras in batch by importing a .xls file from local.

Steps

1. Click **Resource Management**.
2. Click **Download Template** to save the template to your computer.
3. Open the template, enter the camera information as required, and save the file.
4. Click **Import**, and click **Browse** to select the target .xls file.
5. Click **OK**.

Result

The cameras in the file are added in batch and displayed in the list.



Note

To edit based on the added camera information, click **Export** to save the added camera information to your computer, and modify it to the target camera information, and then import in batch.

3.3.3 Search Added Camera

After adding camera(s), you can set conditions to search the added camera(s).

Before You Start

Add camera(s) first.

Steps

1. Click **Resource Management**.
2. Set **Camera Name**, **Display IP Address**, and **Camera Location Information Description**.
3. **Optional:** You can click **Reset** to reset the search conditions.
4. Click **Search**.

Result

The searched result will be displayed on the interface.

3.4 Set Remote Host

Set remote host when the device needs to transmit data to the central control platform.

Before You Start

Set the remote host, and ensure the device can communicate normally with the remote host.

Steps

1. Go to **Platform Settings → Upload Config**.

2. Select a remote host.

Param Config

Upload Protocol

SDK Protocol

SDK Platform ID

1

Upload Strategy

Upload Latest Data in Priority

Upload Data Type

19 item(s) selected. Total 19 item(s)

Upload Historical Data

☒

Upload by Time Period

☐

Upload Interval (ms)

50

Upload Timeout (ms)

5000

Waiting For Upload Respond

☐

Upload Traffic Statistics Parameters

☐

Enable Cloud Storage

☐

Upload VQD Data

☐

Save

Figure 3-5 Set Remote Host

 Note

The supported number of remote hosts varies with different devices. The actual interface prevails.

3. If you select **Upload Protocol** as **SDK Protocol**, follow the steps below.
- 1) Select **SDK Platform ID** according to the actual communication protocol.
 - 2) Select **Upload Strategy** as **Upload Latest Data Priority**.
 - 3) Click the text field behind **Upload Data Type** to check the upload data type(s) and select specific upload data.
 - 4) Set the parameters below.

Upload Historical Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. When enabled, historical data will be uploaded again.

Upload by Time Period

When enabled, data will be uploaded within the time period between the set upload start time and the set upload end time. Two time periods are supported. Select **Time Type**. The device time when the picture is captured and the actual time when the picture is captured

may be different. If you select **Device Time**, the captured pictures at the device time during the set time period will be uploaded to the platform. If you select **Capture Time**, the captured pictures at the actual capture time during the set time period will be uploaded to the platform.

Upload Interval

The interval between 2 data uploads.

Upload Timeout

When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as historical data and uploaded according to historical data rule.

Waiting For Upload Respond

When enabled, if the platform does not respond to the data, it means data upload is failed.



Note

The function is effective only when the platform supports upload response.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Enable Cloud Storage

Enable cloud storage and set **Picture Server ID** to upload the remote host data to the cloud storage.



Note

- Only certain devices in specific protocol support cloud storage settings. The actual interface prevails.
 - Enabling cloud storage and uploading VQD data conflict with each other. You can only enable one function.
-

Upload VQD Data

You can enable the function to upload the VQD (video quality analysis) data to the connected platform.



Note

Enabling cloud storage and uploading VQD data conflict with each other. You can only enable one function.

4. If you select **Upload Protocol** as **HTTP Protocol**, follow the steps below.

- 1) Select **HTTP Platform ID** according to the actual communication protocol.
- 2) Click the text field behind **Upload Data Type** to check the upload data type(s) and select specific upload data.
- 3) Set the parameters below.

Upload Historical Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. When enabled, historical data will be uploaded again.

Upload by Time Period

When enabled, data will be uploaded within the time period between the set upload start time and the set upload end time. Two time periods are supported. Select **Time Type**. The device time when the picture is captured and the actual time when the picture is captured may be different. If you select **Device Time**, the captured pictures at the device time during the set time period will be uploaded to the platform. If you select **Capture Time**, the captured pictures at the actual capture time during the set time period will be uploaded to the platform.

Upload Interval

The interval between 2 data uploads.

Upload Timeout

When the upload time of a single piece of data exceeds the set time, the data will be automatically saved as historical data and uploaded according to historical data rule.

Upload Traffic Statistics Parameters

Upload traffic statistics of each channel.

Enable Cloud Storage

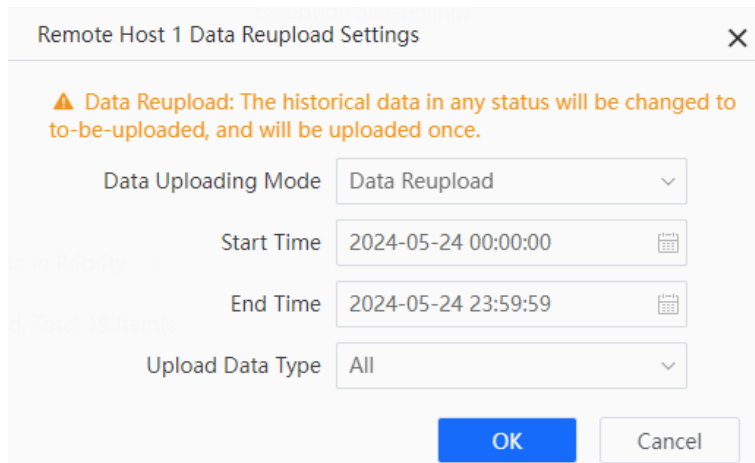
Enable cloud storage and set **Picture Server ID** to upload the remote host data to the cloud storage.



Note

Only certain devices in specific protocol support cloud storage settings. The actual interface prevails.

5. Click **Data Upload Control** to set the relevant parameters.



The dialog box titled "Remote Host 1 Data Reupload Settings" contains the following fields and controls:

- Data Uploading Mode:** A dropdown menu with "Data Reupload" selected.
- Start Time:** A date and time picker showing "2024-05-24 00:00:00".
- End Time:** A date and time picker showing "2024-05-24 23:59:59".
- Upload Data Type:** A dropdown menu with "All" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

An orange warning message at the top states: "Data Reupload: The historical data in any status will be changed to to-be-uploaded, and will be uploaded once."

Figure 3-6 Data Upload Control

- 1) Select **Data Uploading Mode**.

Data Reupload

Change the status of the historical data into the To Be Uploaded status, and upload the historical data only once.

Upload Historical Data in Priority

Upload the historical data in the To Be Uploaded first.

Disable

Change the status of the historical data into the Not to Be Uploaded status, and do not upload these data.

- 2) Set **Start Time** and **End Time**.
- 3) Select **Upload Data Type**.
- 4) Click **OK**.
- 6. Click **Save**.
- 7. **Optional:** Repeat the above steps if you need to set another remote host.

3.4.1 Set Upload Strategy

Enable the data to be filtered to filter the target information and capture pictures not to be uploaded.

Steps

- 1. Go to **Platform Settings → Host Parameters → Upload Strategy** .

Vehicle

Filter Construction Vehicle

Filter Police Vehicle

Filter Bus

Pedestrian

Filter Constructor

Construction

Report Once on Construction Day

Roadblock

Report Once on Roadblock Day

Upload Schedule

Upload Schedule

MonTueWedThuFriSatSun

Up to 8 time periods can be set for each day.

Copy to...

No.	Start Time	End Time	Event Type	Opera...
1	00:00	23:59	Congestion, Stopped Vehicle, Wrong-Way Driving, Pedestrian, Fallen Object, Smo...	
+ Add				

Save

Figure 3-7 Set Upload Strategy

- 2. Enable the corresponding vehicle and pedestrian targets to be filtered.
- 3. Set construction and roadblock upload strategy.
Report Once on Construction Day

If you enable the function, on construction day, only the first item of construction incident data will be uploaded to the platform to filter other repeated data.

Report Once on Roadblock Day

If you enable the function, on roadblock day, only the first item of roadblock incident data will be uploaded to the platform to filter other repeated data.

4. Set the schedule to upload the selected incident types to the platform.

- 1) Enable **Upload Schedule**.
- 2) Select a day, and click **Add** to add a time period.
- 3) Set **Start Time** and **End Time** of the period, and select **Event Type** to be uploaded during the period.
- 4) Repeat the steps above to add more time periods.
- 5) **Optional:** You can click  to delete the time period.
- 6) **Optional:** You can click **Copy to...** to copy the settings of one day to the selected other day(s).



Note

- Up to 8 time periods can be set for each day.
- The time periods in one day cannot overlap with each other.
- The incident data can be uploaded to the platform via SDK or FTP.

5. Click **Save**.

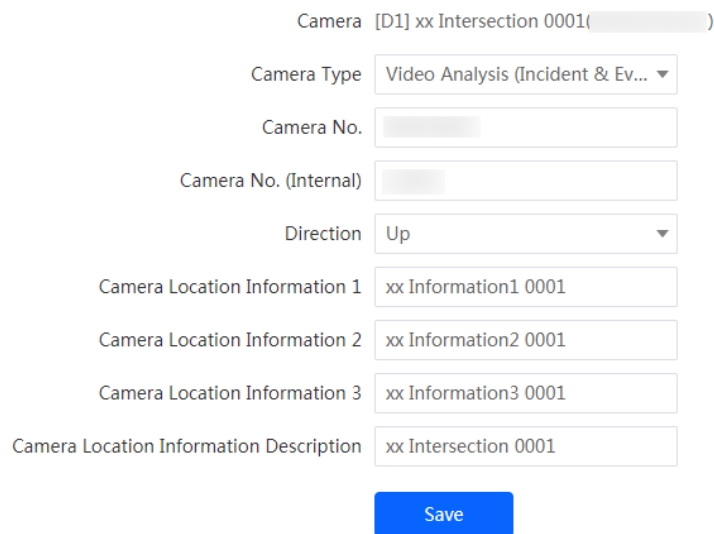
Chapter 4 Traffic Incident Detection

4.1 Set Camera Parameters

You can set camera parameters for easy management.

Steps

1. Go to **Smart Traffic Settings → Param Config → Camera Parameters**.



The screenshot shows a web form for configuring camera parameters. At the top, there is a label 'Camera' followed by a text input field containing '[D1] xx Intersection 0001' and a dropdown arrow. Below this are several fields: 'Camera Type' with a dropdown menu showing 'Video Analysis (Incident & Ev...'; 'Camera No.' with a text input field; 'Camera No. (Internal)' with a text input field; 'Direction' with a dropdown menu showing 'Up'; 'Camera Location Information 1' with a text input field containing 'xx Information1 0001'; 'Camera Location Information 2' with a text input field containing 'xx Information2 0001'; 'Camera Location Information 3' with a text input field containing 'xx Information3 0001'; and 'Camera Location Information Description' with a text input field containing 'xx Intersection 0001'. At the bottom right of the form is a blue 'Save' button.

Figure 4-1 Set Camera Parameters

2. Select a camera.
3. Select **Camera Type**.



Select **Video Analysis** for the incident detection, incident evidence capture, or traffic statistics.

4. Set **Camera No.**, **Camera No. (Internal)**, and **Camera Location Information**.
5. Select **Direction** according to the vehicle passing direction.
6. **Optional:** Click **Copy to...** to copy the settings to other channels.
7. Click **Save**.

4.2 Set Violation Incident Detection

4.2.1 Set Smart Analysis Parameters

Set the smart analysis parameters to get the violation evidence information quickly and effectively.

Steps

1. Go to **Smart Traffic Settings → Param Config → VCA** .

Camera [D1] xx Intersection 0001()

Mounting Height (m) 6

Distance Between Lower Boundary of Vis... 24

Stopped Vehicle Evidence Record Mode Whole Process ▾

Overlay Rectangle on Incident Picture ☒

Overlay Rectangle on Distant-View Capture ☒

Filter Interval for Stopped Vehicle Captur... 60

Force Recognize Initial Plate ☐

Force Recognize Last Plate ☐

Overlay Target Rectangle on Stream ☒

Debug Mode ☒

Start Time of Day 06:00

End Time of Day 17:59

Scene Self-Adaptation ☐

Scene Reset Delay 180 (s)

Construction Area Filter Mode ☐

Incident Time Analysis Stream Time ▾

Copy to... Save

Figure 4-2 Set Smart Analysis Parameters

2. Select a camera.
3. Set **Mounting Height** and **Distance Between Lower Boundary of Visual Area to Vertical Pole** according to the camera actual installation location.
4. Set the parameters below.

Stopped Vehicle Evidence Record Mode

Select **Whole Process** to record the whole process of stopped vehicle.

Overlay Rectangle on Incident Picture

Enable the function, and the targets appearing in the captured pictures will be overlaid with rectangles.

Overlay Rectangle on Distant-View Capture

Enable the function, and the targets appearing in the distant-view captured pictures will be overlaid with rectangles.

Filter Interval for Stopped Vehicle Capture of the Same Plate

During the set time interval, if the stopped vehicles with the same license plate number are captured repeatedly by the same camera, the captured data will be saved only once.

Force Recognize Initial Plate

Enable the function, and the license plate number of the target vehicle will be recognized during the initial capture.

Force Recognize Last Plate

Enable the function, and the license plate number of the target vehicle will be recognized during the last capture.

Overlay Target Rectangle on Stream

Enable the function, and the detected targets will be overlaid with rectangles on the stream.

Debug Mode

Enable the debug mode, and the videos will be overlaid with POS information for the professionals to debug the device.

Start Time of Day

The start time of the smart analysis.

End Time of Day

The end time of the smart analysis.

Scene Self-Adaptation

Enable the function, and the algorithm will generate the lane lines in the area according to the actual scene automatically.

Scene Reset Delay

If a speed dome is added, you can set the parameter. After the scene for incident detection is set, if the scene is changed, the speed dome will restore to the set scene after the delay time.

Construction Area Filter Mode

Enable the function, and the data collection and analysis will not be done for the area recognized as a construction area.

Incident Time Analysis

Select the incident capture to output according to **Device Time** or **Stream Time**. When analyzing via stream time failed, the incident capture will be output according to the device time by default.

5. Optional: Click **Copy to...** to copy the settings to other channels.

6. Click **Save**.

4.2.2 Set Scene

Set the scene capture parameters.

Before You Start

If the channel is a speed dome, set the preset scene first.

Steps

1. Go to **Smart Traffic Settings → Param Config → Incident Rule** .

Camera [D2] xx Intersection 0002()

Scene	Scene Mode	Direction	Scene Name	Scene No.
Scene1	High Speed	Up	Preset Scene1	1

Figure 4-3 Set Scene

2. Select the camera and scene.



Scene is only available for the speed dome.

3. Select **Scene Mode** according to the actual environment.

4. Select **Direction** of the device.



Up refers to the driving direction away from the device. Down refers to the driving direction closing to the device.

5. Enter **Scene Name**.

6. Click **Save**.

4.2.3 Set Preset Scene

The position information such as scenes, focal length, focus, etc. can be saved in the preset scene to let the PTZ return to a certain scene quickly, convenient for the event detection in different scenes.

Steps



Only the speed dome supports preset scene configuration.

1. Go to **Smart Traffic Settings → Param Config → Scene Parameters** .



Figure 4-4 Set Preset Scene



Note

After entering the interface, the PTZ is locked automatically. During the locked period, only the current operator can control the PTZ to prevent the other PTZ movement from interfering the configuration. After the auto lock is released, you can click **Lock** to lock it again.

2. Select the speed dome channel and **Scene**.
3. Click the direction buttons and lens control buttons to adjust the live view image to the needed scene.
4. Click **Set Current Scene** to set the current scene as the preset scene.
5. **Optional:** Enable stopped vehicle capture and set corresponding parameters.
 - 1) Enable **Capture Illegal Parking**.
 - 2) **Optional:** Enable **Capture No Plate Vehicle** when you need to capture the vehicles without license plates.



Note

The function is only available for the captured close view pictures. When you set all the captured pictures as distant view ones, no matter you check it or not, the vehicles without license plates will be detected.

- 3) Set the parameters below.

Number of Captured Picture(s)

The number of the captured pictures for stopped vehicle detection.

Plate Matching Ratio

When the plate matching ratio of vehicles exceeds the set value, the vehicles with the license plates will be judged as the same one, and the violation of the vehicle will only be captured once.

- 4) Click **Captured Picture Settings** to set the capture interval and picture type.

Capture Interval

The time interval between two captured pictures.

Picture Type

In order to guarantee the license plate recognition result, set at least one close view picture.

When the illegal parking is detected, the device will capture pictures according to the set picture No. and interval.

6. Optional: Click **Copy to Scene** and select the scene(s) to copy the same settings.

7. Click **Save**.

8. Optional: Repeat the steps above to set more preset scenes.



Note

When the device lens deviates from the preset scene, you can click **Go to Current Scene** to return to the preset scene quickly.

4.2.4 Set Violation Incident

The device supports multiple violation incidents detection. After the incident rule configuration, the device will detect and capture the incidents according to the set rules automatically.

Before You Start

Set the scene first.

Steps

1. Go to **Smart Traffic Settings → Param Config → Incident Rule**.



Figure 4-5 Set Incident Detection

2. Select the camera and scene.



Note

Scene is only available for the speed dome.

3. Check the incident(s) to be detected and set the corresponding parameters.



Note

The supported incidents vary with different scene modes. The actual device prevails. The supported parameters vary with different models. The actual device prevails.

Table 4-1 Incident Description

Incident Type	Parameters Description
Congestion	The motor vehicles are queuing and the roads are blocked. Check it and set the corresponding parameters. • Vehicle Dwell Time in Area: Click Configuration to set the vehicle dwell times in different areas. If the vehicle dwells in the area for more than the set duration, the congestion incident will be uploaded. • Duration: When the congestion status lasts for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident. • Filter Time: The violation capture during the set filter time will be judged as the violation capture of the same target. In this case, only one captured picture will be uploaded. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions. • Duplicate Alarm Before Canceling Congestion: Check it to enable repeated alarm data reporting until the vehicle evacuation is achieved.
Driving on Lane Line	The motor vehicle is driven out of the lane and over the solid lane line. Check it and set Capture Sensitivity. The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Lane Change	Most part of the vehicle body crosses over the lane line and enters into another lane. Check it and set Capture Sensitivity. The higher the

Incident Type	Parameters Description
	sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Wrong-Way Driving	The vehicle is driven in the direction opposite to the guidance direction of the lane. Check it and set the corresponding parameters. • Duration: When the vehicle is driven in the direction opposite to the guidance direction of the lane at the detection area for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Vehicle Overstay	Some certain number of motor vehicles overstay at the linked areas. Check it and set the corresponding parameters. • Min. Number of Vehicle to Trigger Overstay Detection: The number of vehicles allowed to stay at the linked areas. If the number of vehicles exceeds the set value, vehicle overstay incident will be triggered and uploaded. • Duration: When the vehicle stays at the detection area or lane line for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Stopped Vehicle	The motor vehicle stops at the positions where parking is forbidden. Check it and set the corresponding parameters.

Incident Type	Parameters Description
	• Long Range Target Frame: When the vehicle with violation incident is far away from the lens, the target frame will appear on the live view image to mark the vehicle position. • Duration: When the vehicle is parking at the detection area or lane line for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident. • Filter Time: The violation capture during the set filter time will be judged as the violation capture of the same target. In this case, only one captured picture will be uploaded. • The Degree of Congestion: When the vehicle density in the detection area or lane line exceeds the set threshold, no picture will be captured or uploaded. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
U-Turn	The motor vehicle makes a U-turn at the intersection where U-turn or left turn is forbidden. Check it and set Capture Sensitivity. The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Motor Vehicle on Non-Motor Vehicle Lane	The motor vehicle is driven on the non-motor vehicle lane. Check it and set Duration. When the motor vehicle occupies the non-motor vehicle lane for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident.
Traffic Accident	To detect the incident of traffic accident between two vehicles. Check it and set the corresponding parameters. • Alarm Under Construction: Construction may be judged as a traffic accident and alarmed by mistake. Disable the function to not to alarm if the road segment is in construction status to filter the mistaken alarms. If you enable the function, construction will also be judged as a traffic accident to trigger alarms. It is disabled by default. • Duration: When the incident lasts for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident.

Incident Type	Parameters Description
	• Filter Time: The violation capture during the set filter time will be judged as the violation capture of the same target. In this case, only one captured picture will be uploaded. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions. • Parking Interval Between Two Vehicles: If the parking time between two vehicles at one position is longer than the set value, it is not judged as a traffic accident and no incident alarm will be triggered.
Single Vehicle Breakdown	To detect the incident of single vehicle breakdown. Check it and set the corresponding parameters. • Alarm Under Construction: Construction may be judged as the single vehicle breakdown and alarmed by mistake. Disable the function to not to alarm if the road segment is in construction status to filter the mistaken alarms. If you enable the function, construction will also be judged as the single vehicle breakdown to trigger alarms. It is disabled by default. • Duration: When the incident lasts for a time period longer than the set duration, the vehicle will be judged as a vehicle with violation incident. • Filter Time: The violation capture during the set filter time will be judged as the violation capture of the same target. In this case, only one captured picture will be uploaded. • Capture Sensitivity: The higher the sensitivity is, the more possible it is for the detection target to be recognized as the vehicle with violation incidents. If the value is too high, detection mistakes may occur. If the value is too low, detection loopholes may occur. Therefore, it's recommended that the value should be set reasonably according to the actual conditions.
Flow	To detect the traffic flow. Check it and set the corresponding parameters. • Report Time: The camera data statistics and uploading will be done every the set time. • Flow Distance: It refers to the distance from the flow trigger line 1 to flow trigger line 2, which is used to calculate the average speed.

The enabled incident types will display in the list of **Lane Linkage**, **Area Linkage**, and **Associated Masked Area** automatically according to the detection needs or capability permissions.

4. **Optional:** Copy the incident parameters to the other camera(s).
- 1) Click  of the incident.
 - 2) Select the parameter(s) to be copied.
 - 3) Select the camera(s) to copy the same settings.
 - 4) Click **OK**.
5. Click **Draw Area** to draw the lane lines, detection areas, and shielded areas. Click **OK**.



Note

- Draw the areas and lane lines first, and then you can check the incident types in the list of **Lane Linkage** and **Area Linkage**.
- If you check **Background Mode**, you can draw on the live view image. If you uncheck it, you can draw on the image snapshot.

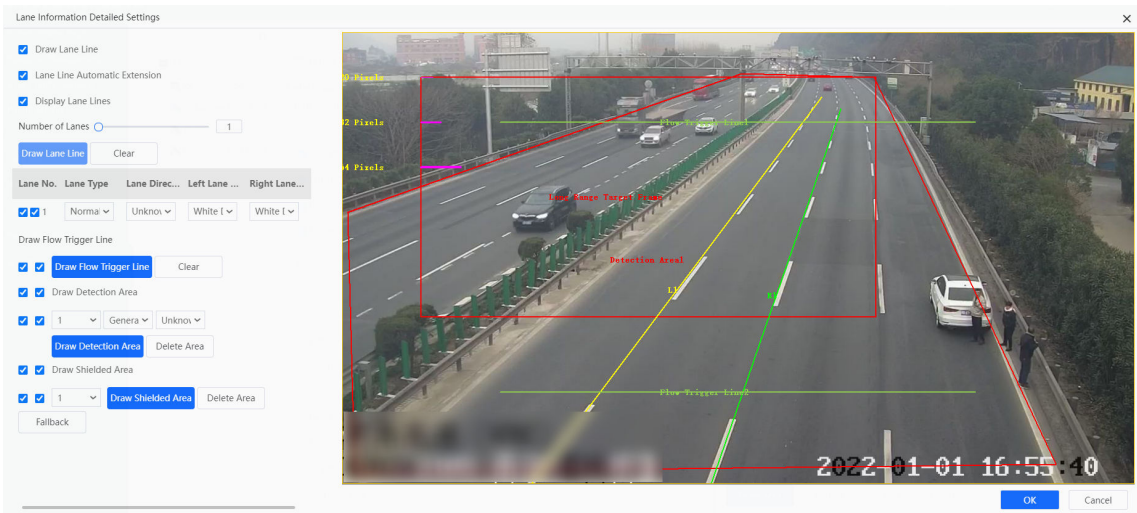


Figure 4-6 Draw Lane Lines and Areas

Table 4-2 Drawing Instructions

Draw Lane Line	a. A lane line is displayed by default. If you need to add lane lines, add Number of Lanes to activate the Draw Lane Line button, and a row of lane property items will be added. b. Click Draw Lane Line, and one lane line will be added on the image. Drag the line to adjust its position, or select the two ends of the line and drag to adjust the lane line direction according to the actual scene. c. Set Lane Type, Lane Direction, Left Lane Line Type, and Right Lane Line Type. The selected lane type is the associated condition to judge the violation incident. d. Reduce Number of Lanes to delete the newly drawn lane line and its lane property.
----------------	---

	e. Click Clear to clear all the drawn lane lines, but the lane property list will not be influenced. f. If there are too many lines on the image, which influences the live view, you can uncheck Lane Line Automatic Extension and Display Lane Lines to hide the drawn lines.
Draw Flow Trigger Line	a. Click Draw Flow Trigger Line, and two flow trigger lines will display on the image. b. Drag the line to adjust its position, or select the two ends of the line and drag to adjust the line direction according to the actual scene. c. Uncheck to hide the drawn flow trigger lines. Click Clear to clear all the drawn flow trigger lines.
Draw Detection Area	a. Select the area No., area type, and area direction from the drop-down list. The area type defines the area usage, which is the associated condition to judge the violation incident. b. Click Draw Detection Area, and click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area. c. Uncheck to hide the drawn areas. Select the area No. and click Delete Area to delete the drawn detection areas of the selected No.
Draw Shielded Area	a. Select the area No. from the drop-down list. b. Click Draw Shielded Area, and click the left button of the mouse to draw a rectangular or polygonal frame, and then click the right button of the mouse to save the area. c. Uncheck to hide the drawn areas. Select the area No. and click Delete Area to delete the drawn shielded areas of the selected No.



Note

You can click **Fallback** to return to the previous operation.

6. Check the violation incident(s) to be enabled in the list of **Lane Linkage** and **Area Linkage**.

7. **Optional:** For the speed dome, click **Copy to Scene** to copy the same settings to the other scene(s).

Copy scene For the speed dome, click **Copy to Scene** to copy the same settings to the other scene(s).

Copy channel Click **Copy to...** to copy the same settings to the other camera(s). If you check **Copy the frame coordinates of the drawn area.**, the drawn area rules will also be copied to the selected camera(s).

8. Click **Save**.

4.2.5 Set Scene Patrol

You can set the scene patrol schedule to make the device monitor the preset scene in patrol during the set period.

Before You Start

Only the speed dome supports scene patrol. Ensure at least two preset scenes have been set.

Steps

1. Go to **Smart Traffic Settings → Param Config → Scene Auto-Switch**.

Camera [D2] xx Intersection 0002(1 :)

Enable Schedule ☒

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	[Blue bar from 0 to 24]												
Tue	[Blue bar from 0 to 24]												
Wed	[Blue bar from 0 to 24]												
Thu	[Blue bar from 0 to 24]												
Fri	[Blue bar from 0 to 24]												
Sat	[Blue bar from 0 to 24]												
Sun	[Blue bar from 0 to 24]												

Figure 4-7 Set Scene Patrol

2. Select the speed dome camera.
3. Check **Enable Schedule**.
4. 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.

5. Adjust the recording time.
 - Drag two ends of the set recording period bar to adjust the length.
 - Drag the whole set recording period bar and relocate it.
6. **Optional:** Delete recording periods.
 - Click a set recording period and click **Delete**.

- Click **Delete All** to delete all the recording periods.

7. **Optional:** Click  to copy set recordings to other days.

8. Click **Save**.

4.3 Set VQD

You can set VQD (Video Quality Diagnosis) and enable alarm.

Steps

1. Go to **Smart Traffic Settings → Param Config → VQD**.

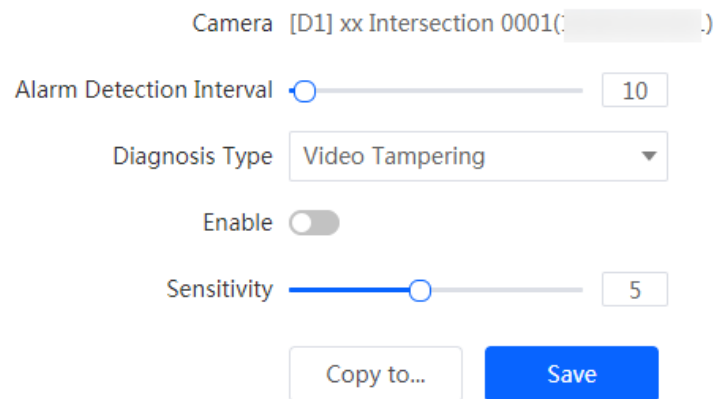


Figure 4-8 Set VQD

2. Select a camera.
3. Set **Alarm Detection Interval**.
4. Select **Diagnosis Type**, and enable it.
5. Set **Sensitivity**.

Sensitivity

The higher the sensitivity, the more possible to detect the video quality problems. But too high sensitivity will result in more false detection. So set it reasonably to guarantee the detection accuracy.

6. **Optional:** Click **Copy to...** to copy the same settings to other camera(s).
7. Click **Save**.

Result

If video tampering or blurred image is detected, the alarm will be triggered every set interval.

4.4 Set Detection Parameters

4.4.1 Set License Plate Recognition Parameters

Select the license plate recognition country/region.

Steps

1. Go to **Capture → Capture Parameters → License Parameters** .
2. Select **Country/Region** according to the actual needs.
3. Click **Save**.

4.4.2 Set Evidence Code

Evidence codes define various violation types. Through setting evidence codes, different captured evidences can be easily managed.

Steps

1. Go to **System → System Settings → Dictionary Settings** .
2. View the traffic evidence type and code.
3. **Optional:** Edit or reset the evidences.

Edit Select the captured evidence item from the list and click **Edit** to edit its code.

Reset Click **Reset All** to restore the dictionary data to the factory settings.

4.4.3 Set Picture Composition

You can composite the captured multiple pictures to one picture to upload and store.

Steps

1. Go to **Smart Traffic Settings → Param Config → Picture Composition** .

Camera [D1] xx Intersection 0001()

Composition ☒

Composition Mode of 2 Pics 2 Pics: Left to Right 1 by 1(202)

Composition Mode of 3 Pics 3 Pics: Up to Down 1 by 1(301)

Composition Mode of 4 Pics 4 Pics: Up 2, Down 2(403)

Picture Quality 80

Figure 4-9 Set Picture Composition

2. Select a camera.
3. Enable picture composition.
4. Select the composition mode of 2/3/4 pictures.
5. Set **Picture Quality**.
6. **Optional:** Click **Copy to...** to copy the same settings to other camera(s).
7. Click **Save**.

4.4.4 Set Text Overlay

You can overlay the information such as the intersection, lane No., license plate number, etc. on the captured pictures.

Steps

1. Go to **Smart Traffic Settings → Param Config → Text Overlay** .

Camera [D1] xx Intersection 0001()

Enable Overlay Info ☒

Text Overlay on Picture Mode

Overlay Content

Initial Top Margin (%)

Initial Left Margin (%)

Character Size

Character Color 

Background Color 

Space number

Position Percentage of Line Break (%)

Figure 4-10 Set Text Overlay

- 2. Select a camera.
- 3. Enable overlay information.
- 4. Set the text overlay parameters.

Text Overlay on Picture Mode

Select the position to overlay the text.

Overlay Content

Click the text filed to check the overlaid information, and click **OK**.

Initial Top Margin

Set the top coordinate from which the text begins to overlay.

Initial Left Margin

Set the left coordinate from which the text begins to overlay.

Space Number

Set the number of space after between two overlaid items. For example, if you set it as 1, the adjacent overlaid items will be separated with one space.

Position Percentage of Line Break

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.



Note

If the overlaid information exceeds the overlay area, the excess content will not be displayed.

5. **Optional:** Click **Copy to...** to copy the same settings to other camera(s).

6. Click **Save**.

Chapter 5 Data Management

5.1 View Statistics Result

Click **System Home Page** to view the incident overview, today's incident proportion statistics, today's incident quantity, incident number trend this month, incident(s) in an hour, the top 10 camera alarms, and the top 5 exception alarms.

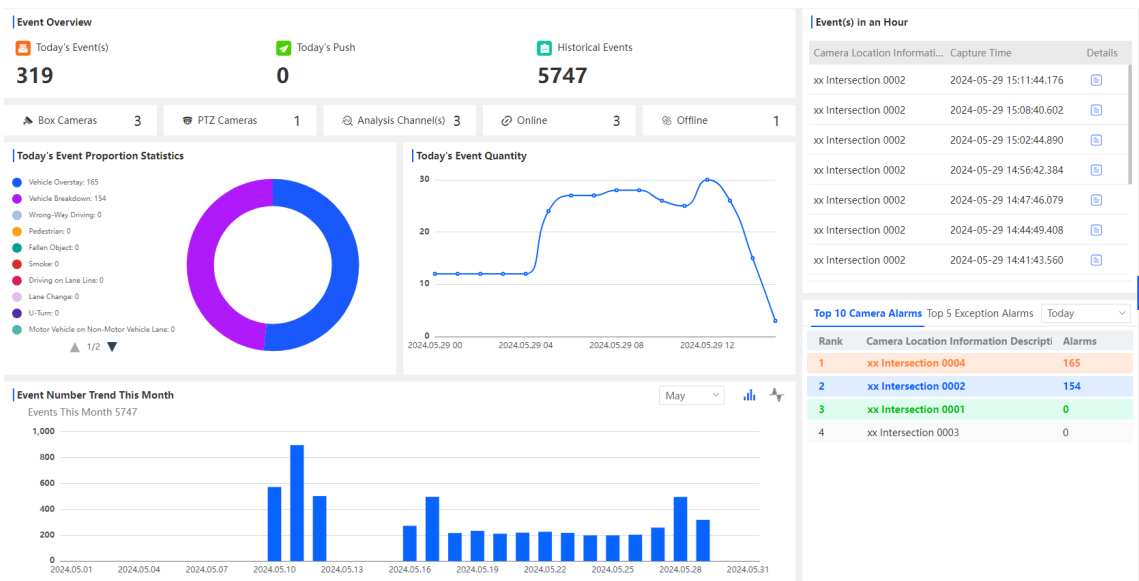


Figure 5-1 View Statistics Result

For incident(s) in an hour, you can click  to view the incident details, including the captured image, camera location, capture time, lane/area, incident type, and license plate picture.

5.2 View Real-Time Data

The device supports viewing captured incident information in real time.

Steps

1. Click **Live View**.
2. Check the data item from the real-time list, and the lower left side of the interface will display the incident detailed information.

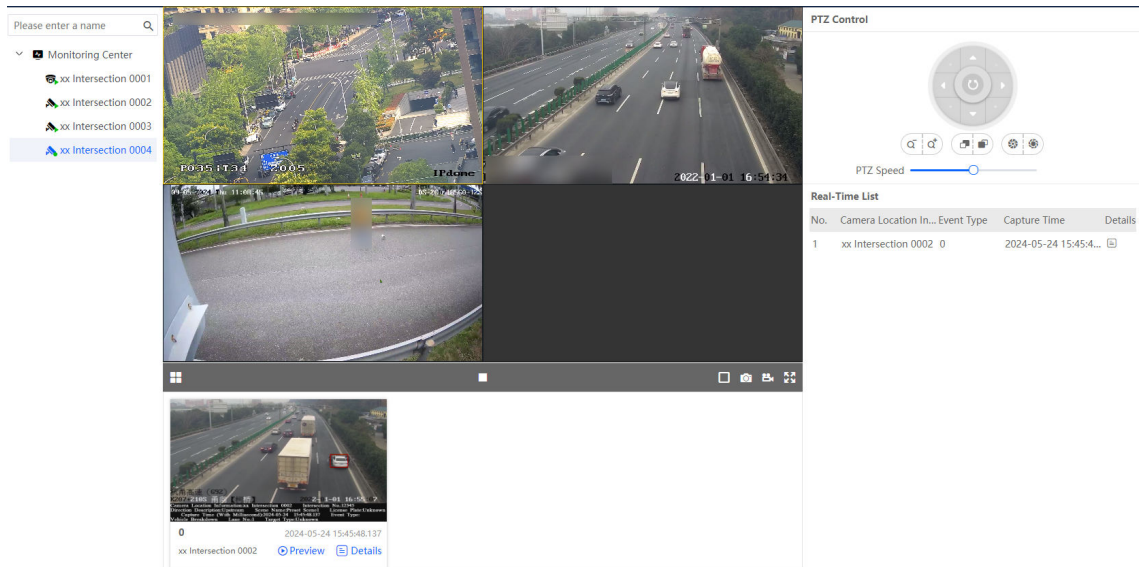


Figure 5-2 Live View

3. You can do the following operations.

- Preview the incident video**

Click **Preview** to preview the incident video.
- View detailed information**

Click **Details** on the lower left side of the interface or click in the real-time list to view the corresponding captured incident picture and detailed information.

5.3 Search Traffic Data

You can search the traffic data of the connected cameras by searching data.

Steps

1. Go to **Data Search** → **Traffic Data Search**.
2. Select a camera.
3. Set **Start Time** and **End Time**.



Note

The time span between the start time and the end time cannot exceed 30 days.

4. Set the search conditions.
5. Click **Search**.

The searched result will be displayed.
6. Click after the data to view detailed information, pictures, video clips, etc.



Note

You can set the recording parameters in **System → System Settings → Other Settings**.

Traffic Camera Time Synchronization

After enabling the function, the device will synchronize the camera time after the set **Camera Time Sync. Threshold** to make the camera time consistent with the device time.

Pre-record

The time period before the violation recording.

Post-record

The time period after the violation recording.

Longest Recording Time

The longest recording time of one piece of violation video.

-
7. **Optional:** After the data has been searched, you can export the selected data information to the set path in two ways.
- On **Details** interface, click **Export**, select the export type, and click **OK** to export the data.
 - On **Traffic Data Search** interface, check the incident items from the list, click **Export**, select the export type, and click **OK** to export the data.



Note

- Make sure the IP address of the camera has been added as a trusted site before exporting the data.
 - You can set the exported data names and saving paths. Refer to [***Back up to Local Storage***](#) for details.
-

5.4 View Traffic Flow Statistics

You can view the traffic flow statistics of the specific time period via data search.

Steps

1. Go to **Data Search → Traffic Parameters Statistics**.
2. Select a camera.
3. Set **Start Time** and **End Time**.
4. Set **Statistics Cycle** and **Lane No.** according to the actual needs.
5. Click **Search**.
6. **Optional:** After the data has been searched, click **Export** to export the data information to the set path.

5.5 Back up Data

5.5.1 Back up to Local Storage

You can back up the data of the device to your computer.

Steps

1. Set the data export rule.
 - 1) Go to **System → System Settings → Web Backup Settings**.
 - 2) Set the name, saving path, and other information of the pictures and videos.



Note

After the random number digits have been set, pictures with the same name will be automatically numbered. The upper limit of the number is the maximum number of the random number digits.

- 3) Click **Save**.
2. Set the device IP address as a trusted site in the security settings of the browser.
3. Search the data. Refer to ***Search Traffic Data*** for details.
4. On **Traffic Data Search** interface, check the data to be exported and click **Export** to select export type and export the data to your computer.

Result

Data will be backed up as the set name in the set path.

5.5.2 Back up to USB

The device supports automatically backing up the data to the USB.

Before You Start

Connect a USB to the device.

Steps

1. Go to **System → System Settings → USB Backup**.
2. Click **USB Backup Parameters**.
3. Enable USB backup.

USB Backup Parameters | USB Backup Status

USB Backup

Enable USB Backup ☒

Backup Period: Real-Time Backup

Start Time: 2024-05-24 16:02:59

Upload Data Type

Event

- ☒ Unknown
- ☒ Congestion
- ☒ Stopped Vehicle
- ☒ Wrong-Way Driving
- ☒ Pedestrian
- ☒ Fallen Object
- ☒ Smoke
- ☒ Driving on Lane Line
- ☒ Lane Change
- ☒ U-Turn
- ☒ Motor Vehicle on Non-Motor Vehicle Lane
- ☒ Roadblock
- ☒ Construction
- ☒ Traffic Accident
- ☒ Emergency Lane Occupation
- ☒ Vehicle Breakdown
- ☒ Vehicle Overstay

Evidence Capture

- ☒ Parking on Urban Road
- ☒ Parking on Highway

Other

- ☐ Event Record
- ☐ Evidence Record
- ☐ Attached File

Figure 5-3 USB Backup

4. Select **Backup Period** and **Start Time**.
- **Real-Time Backup**: Automatically back up the data only once after the data have been saved at the set time.
 - **Backup Every Day**: Automatically back up the data once a day at the set time.
5. Select **Upload Data Type** to backup.
6. Set the file backup naming rule and saving path.
7. Click **Save**.
- Files will be backed up with the set name in the set path.
8. **Optional**: Click **USB Backup Status** to view the backup status.

Chapter 6 Live View and Local Configuration

6.1 Live View

6.1.1 Start/Stop Live View

Start/stop the live view of cameras.

Start Live View

Click **Live View**, and double click the camera from the left side list to start live view.



Note

If you want to display a camera live view in a specific divided window, select the divided window first, and then double click the camera to start live view. The display window is only set for once, and you need to set it again when you start live view next time.

Click  to start all live view.

Stop Live View

When the camera starts live view, double click the camera from the list on the left side of the live view interface to stop live view.

Click  to stop all live view.

6.1.2 Select Window Division Mode

Select window division if you need to switch the single or multi-window live view mode.

On the **Live View** interface, click  to select the live view window division mode according to the actual needs.

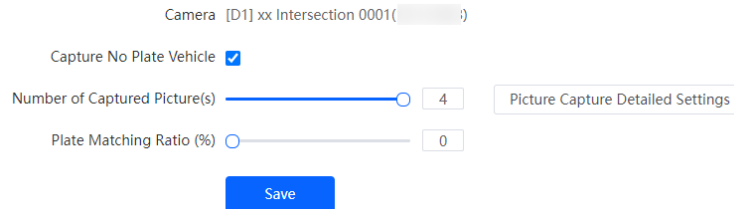
6.1.3 Manual Evidence Capture

For the speed dome, you can set the manual evidence capture parameters. Then when you capture the evidence pictures on the live view interface, the device will capture pictures according to the set rules.

Steps

1. Click **Live View**.
2. Select a speed dome camera.
3. Click , and drag on the image to capture evidence manually.
4. **Optional:** To adjust manual evidence capture parameters, perform the following steps.

- 1) Go to **Smart Traffic Settings → Param Config → Manual Evidence Capture** .
- 2) Select the speed dome camera.
- 3) Set the parameters below.



The screenshot shows a configuration window for a camera labeled 'Camera [D1] xx Intersection 0001()'. It contains three settings: 'Capture No Plate Vehicle' with a checked checkbox, 'Number of Captured Picture(s)' with a slider set to 4 and a numeric input field showing 4, and 'Plate Matching Ratio (%)' with a slider set to 0 and a numeric input field showing 0. A 'Picture Capture Detailed Settings' button is located to the right of the first two settings. A blue 'Save' button is at the bottom center.

Figure 6-1 Set Manual Evidence Capture Parameters

Capture No Plate Vehicle

If you enable the function, the vehicles without license plates will be captured.

Number of Captured Picture

The number of the captured pictures when you click  on the live view interface.

Plate Matching Ratio

When the plate matching ratio exceeds the set value, the vehicles with the license plates will be judged as the same one, and the events of the vehicle will only be captured once.

- 4) Click **Picture Capture Detailed Settings** to set the capture interval and picture type.

Capture Interval

The time interval between two captured pictures.

Picture Type

In order to guarantee the license plate recognition result, set at least one close-up picture.

- 5) Click **Save**.

6.1.4 Capture Manually

Capture live view pictures and save them to your computer.

Steps

1. Click **Live View**.
2. Double click the camera on the left to start live view.
3. Click  .
4. **Optional:** Name and save the captured pictures.
5. **Optional:** Go to **System → System Settings → Local** to view the saving path of snapshots in live view.

6.1.5 Record Manually

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

Steps

1. Click **Live View**.
2. Double click the camera on the left to start live view.
3. Click  to start recording.
4. Click  to stop recording.
5. **Optional:** Go to **System** → **System Settings** → **Local** to view the saving path of record files.

6.1.6 Display in Full Screen

On the **Live View** interface, click  to display the live view image in full screen.

Press **Esc** on the keyboard to exit the full screen mode.

6.2 PTZ Control Panel

Click **Live View** and control PTZ cameras via PTZ control panel.

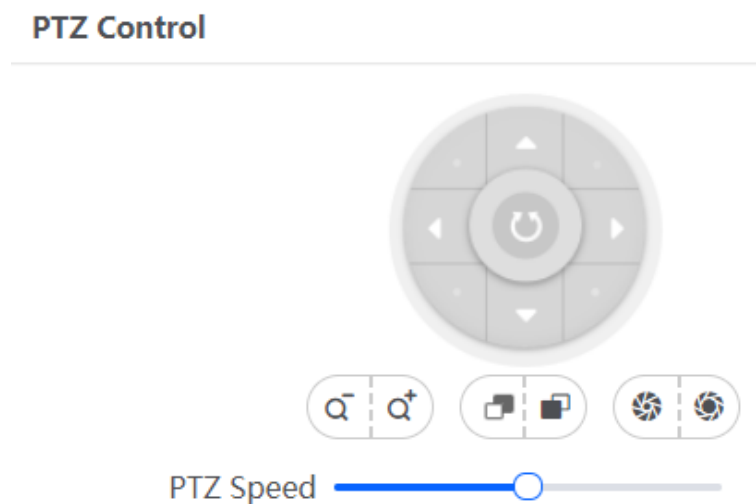


Figure 6-2 PTZ Control

Note

- PTZ camera supports power-down memory. After PTZ camera suddenly loses power or reboots, it can automatically go back to the former position.

The PTZ control buttons are described as follows.

Table 6-1 Buttons Description

Icon	Description
	Hold the direction buttons to rotate the camera horizontally and vertically. Click  to continue rotating horizontally, and click again to stop rotation.  Note The function may vary with models.
	Zoom -/Zoom + • Hold  to zoom in on the image. • Hold  to zoom out on the image.
	Focus -/Focus + • In manual focus mode, hold  to view nearby objects clearly, while distant objects will be blurred. • Hold  to view distant objects clearly, while nearby objects will be blurred.
	Iris -/Iris + • Hold  to increase aperture when the image is relatively dark. • Hold  to decrease aperture when the image is relatively bright.
	Control the PTZ speed.

6.3 Local Configuration

Go to **System** → **System Settings** → **Local** to set the parameters.

Live View Parameters

Protocol Type ☒ TCP ☐ UDP

Live View Performance ☐ Shortest Delay ☒ Balanced ☐ Fluency

Image Size ☒ Auto-fill ☐ 4:3 ☐ 16:9

Image Format ☒ JPEG ☐ BMP

Rules Information ☐

Display POS Information ☐

Record File Settings

Record File Size ☐ 256M ☒ 512M ☐ 1G

Save record files to

Save downloaded files to

Picture and Clip Settings

Save snapshots in live view to

Save snapshots when playback to

Save clips when playback to

Figure 6-3 Local Configuration

Protocol Type

TCP

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

UDP

Provides real-time audio and video streams.

Live View Performance

Shortest Delay

The video is real-time, but the video 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.

Image Size

Select according to your needs.

Image Format

Set the saving format of captured pictures.

JPEG

The picture will be compressed.

BMP

The picture will not be compressed.

Rules Information

When enabled, the configured rule information will be displayed on the live view interface.

Display POS Information

When enabled, the POS information of the capture camera will be displayed on the live view interface.

Record File Size

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

Save record files to

Set the saving path for the manually recorded video files in live view interface.

Save downloaded files to

Set the saving path for the downloaded files in playback mode.

Save snapshots in live view to

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

Save snapshots when playback to

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

Save clips when playback to

Set the saving path for the clips in playback mode.

Chapter 7 Network Configuration

7.1 Connect to Platform

7.1.1 Connect to SDK Platform

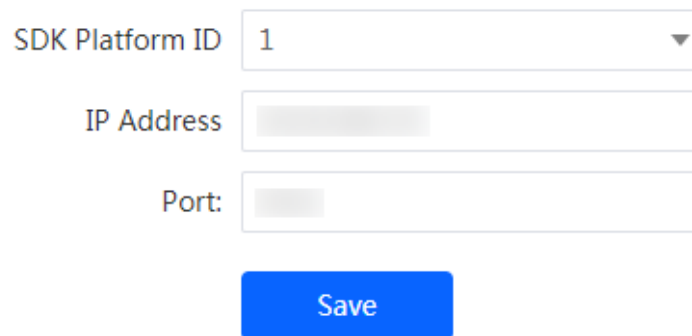
SDK is the platform access protocol. You can connect the device to the SDK platform to realize live view and data management via the platform.

Before You Start

Set the platform server first. Guarantee the network communication between the device and the platform is normal.

Steps

1. Go to **Platform Settings** → **Host Parameters** → **SDK** .



SDK Platform ID 1 ▼

IP Address

Port:

Save

Figure 7-1 Connect to SDK Platform

2. Select **SDK Platform ID**.
3. Enter **IP Address** and **Port** of the device.



Note

The IP address and port should be consistent with those added on the platform.

4. Click **Save**.

7.1.2 Connect to HTTP Platform

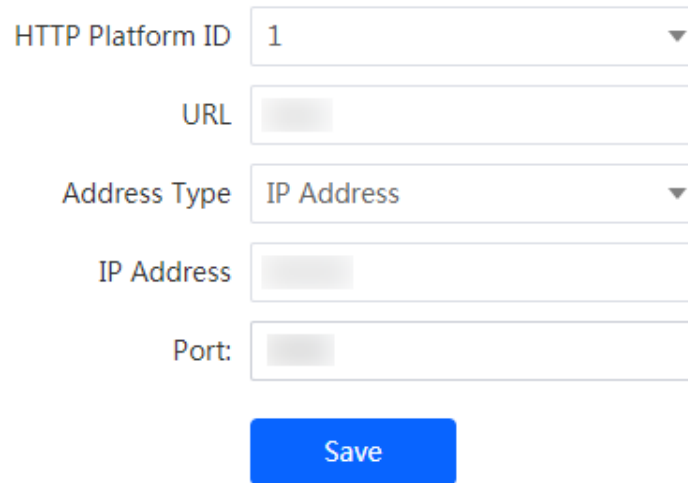
You can connect the device to HTTP platform to upload the pictures and alarm data to the remote host platform.

Before You Start

The network communication between the device and the platform is normal.

Steps

1. Go to **Platform Settings** → **Host Parameters** → **HTTP** .



The screenshot shows a configuration form for connecting to an HTTP platform. It includes five input fields: 'HTTP Platform ID' (a dropdown menu with '1' selected), 'URL' (a text box), 'Address Type' (a dropdown menu with 'IP Address' selected), 'IP Address' (a text box), and 'Port' (a text box). Below these fields is a blue 'Save' button.

Figure 7-2 Connect to HTTP Platform

2. Select **HTTP Platform ID**.
3. Set **URL** of the platform.
4. Select **Address Type** and set the corresponding parameters.
5. Click **Save**.

7.2 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 **System** → **Network Settings** → **DDNS** .
2. Enable DDNS.
3. Select **DDNS Type** according to the registration type.
4. Enter the server address and other information.
5. Click **Save**.

What to do next

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

7.3 Set Port

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



Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **System → Network Settings → Port** for port settings. Click **Save** after finishing settings.

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.

RTSP Port

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

HTTPS Port

It refers to the port of encrypted transmission and identity authentication protocol.

Server Port

It refers to the port to connect to client for obtain network protocol control and set device parameters.



Note

- Certain ports need to reboot after edited to take the new settings into effect.
 - When the device cannot edit the port No. via access Web due to port conflicts, you can connect the device to your computer and edit via SADP software.
-

7.4 Set ONVIF

If you want to use the device as an ONVIF server, you should enable this function.

Steps

1. Go to **System → Network Settings → Integration Protocol**.
2. Enable ONVIF.
3. Click **Save**.

Chapter 8 Record and Playback

8.1 Set Storage Path

8.1.1 Format Disk

Format the disk when the storage is abnormal or a new disk is installed.

Steps



Caution

Formatting the disk will cause the disk data loss. Back up the data first.

1. Go to **System → Storage Management → HDD Management** .
2. Check the HDD No. needs to be formatted.
3. Click **Format**.

8.1.2 Set FTP

Set FTP parameters if you want to upload the captured pictures or recordings 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 **Platform Settings → FTP Upload Settings** .
2. Select a FTP server.

FTP ☒

FTP Server Address

FTP Port

FTP User Name

FTP Password

Upload Historical Data ☒

MP4 Format Conversion for Videos ☐

Upload by Time ☐

Data Type

Upload No-Plate Data ☒

License Plate Picture Name

Event Picture Name

Event Picture Saving Path

Event Video Name

Event Video Saving Path

Evidence Picture Name

Evidence Picture Saving Path

Evidence Video Name

Evidence Video Saving Path

Attached File Name

Attached File Saving Path

Attached File Content

Figure 8-1 Set FTP

3. Set FTP parameters.

- 1) Enable the FTP.
- 2) Enter **FTP Server Address**, **FTP Port**, **FTP User Name**, and **FTP Password**.

4. Set upload parameters.

Upload Historical Data

Historical data refers to the data failed to be uploaded due to network disconnection or congestion. After this function has been enabled, historical data will be uploaded again.

MP4 Format Conversion for Videos

Enable the function to convert the format of incident videos to standard MP4 to upload to FTP.

Upload by Time

After this function has been enabled, data will be uploaded within the time period between the set uploading start time and the set uploading end time.

Upload No-Plate Data

Upload data of vehicles without license plates to the FTP server.

5. Select **Data Type**.
6. Set the file naming rule and saving path according to the actual needs.
7. Click **Data Upload Control** to set relevant parameters.

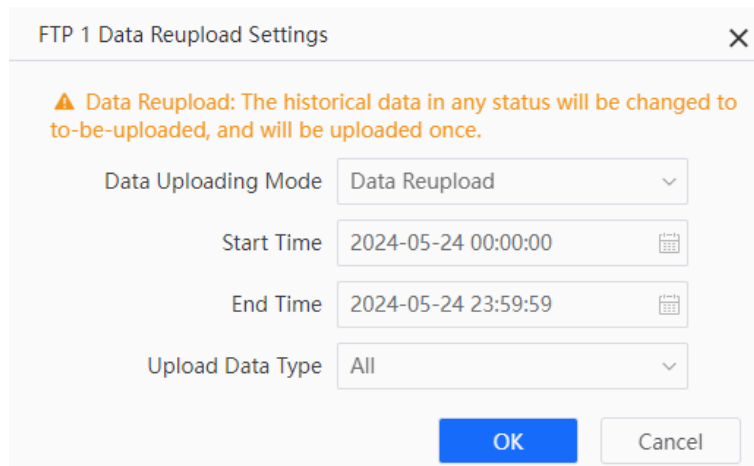


Figure 8-2 Data Upload Control

- 1) Select **Data Uploading Mode**.

Data Reupload

Change the status of the historical data into the To Be Uploaded status, and upload the historical data only once.

Upload Historical Data in Priority

Upload the historical data in the To Be Uploaded first.

Disable

Change the status of the historical data into the Not to Be Uploaded status, and do not upload these data.

- 2) Select **Start Time** and **End Time**.
- 3) Select **Upload Data Type**.
- 4) Click **OK**.

8. Optional: Repeat the above steps to set another FTP.

9. Click **Save**.

8.1.3 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.

Steps

1. Go to **Platform Settings → Host Parameters → Cloud Storage** .

The screenshot displays the 'Cloud Storage' configuration page. At the top, there are three input fields: 'Cloud Storage' with a dropdown menu showing '1', 'IP Address' with a text box, and 'Port' with a text box. Below these is a section header 'Cloud Storage Server Parameters' with a vertical bar to its left. Under this header are five more input fields: 'Protocol Version' with a dropdown menu showing 'V1.0', 'Central Management Port' with a text box, 'User Name' with a text box, 'Password' with a text box, and 'Storage Pool ID' with a text box showing '0'. At the bottom right of the form is a blue 'Save' button.

Figure 8-3 Set Cloud Storage

- 2. Select **Cloud Storage**.
- 3. Enter **IP Address** and **Port** of the cloud storage server.
- 4. Set cloud storage server parameters.

Protocol Version

Protocol version of the cloud storage server.



Note

The cloud storage server parameters vary with different protocol versions. The actual interface prevails.

Central Management Port

Central management HTTP port of the cloud storage server.

User Name/Password

User name and password of the cloud storage server.

Storage Pool ID

Storage pool ID of uploaded files on the cloud storage server.

5. Click **Save**.

8.2 Set Quota

Set the picture or video ratio in the storage.

Steps



Note

This function takes effect only when the recording schedule is enabled.

1. Go to **System → Storage Management → Picture Quota/Quota Set for Short Video** .
2. Set the capacity for saving picture or video according to the actual needs.
3. Click **Save**.

8.3 Enable Record

Enable all-day recording according to your needs.

Steps

1. Go to **System → Storage Management → Record Configuration** .
2. Select the camera.
3. Enable record.

The selected camera will start all-day recording.
4. **Optional:** To apply the same settings to other channels, click **Copy To...**, select the target channel(s), and click **OK**.
5. Click **Save**.

8.4 Playback

You can play back the record files saved in the storage media (HDD, etc.).

Steps

1. Click **Playback**.
2. Select the camera.
3. Select the file date, and click **Search**.
4. Drag the time bar and put the yellow line at the time point that you need.
5. Click  to play back the file.
6. **Optional:** You can also do the following operations.

	Pause.		Single frame.
	Divide the playback window, and play back multiple cameras simultaneously.		Stop playback for selected camera.
	Fast forward.		Slow forward.
	Stop playback for all cameras.		Capture pictures.
	Download.		Start clipping.
	Full screen.	-	-

Note

- For the captured picture of playback saving path, refer to **Save snapshots when playback to in System → System Settings → Local** .
- Operations and buttons vary with different models. The actual device prevails.

8.5 Backup

Download videos saved in the storage media (HDD, etc.) to a local path.

Steps

1. Click **Playback**.
2. Click .
3. Select download type.
 - To search video by date, select **Download by Time**, and set the start time and end time.
 - To search video by file type, select **Download by File**, set the search conditions, and click **Search**.
 - To download quickly, select **Quick Download**, select a camera, and set the pre-time and post-time, and download time.
4. Check videos to download and click **Download**.
5. For the video saving path, refer to **Save downloaded files when playback to in System → System Settings → Local** .

Chapter 9 Serial Port Configuration

9.1 Set RS-485

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

Before You Start

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

Steps

1. Go to **System → System Settings → Serial Port Parameters → RS485** .
2. Set **Baud Rate, Data Bit, Stop Bit**, etc.



Note

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

3. Click **Save**.

9.2 Set RS-232

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

Before You Start

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

Steps

1. Go to **System → System Settings → Serial Port Parameters → RS232** .
2. Set **Baud Rate, Data Bit, Stop Bit**, etc.



Note

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

3. Click **Save**.

Chapter 10 Safety Management

10.1 Manage User

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

Before You Start

Set the administrator password when you first use the device to ensure a normal working.

Steps



Caution

It is highly recommended to create a strong password of your own choosing in order to increase the security of your product.

1. Go to **System** → **System Settings** → **User Management** .
 2. Add a user.
 - 1) Click **Add**.
 - 2) Enter **User Name** and select **Level**.
 - 3) Enter **Admin Password**, **Password**, and confirm the password.
-



Caution

- Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.
 - 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 local and remote permissions to users based on needs.
 - 5) Click **OK**.
3. **Optional:** You can also do the following operations.
- | | |
|------------------------------|---|
| Delete User | Select the added user and click Delete to delete the user. |
| Edit User Information | Select the added user and click Edit to edit the user information. |

10.2 Install Authorized Certificate

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

Steps

1. Go to **System → Network Settings → HTTPS** .
2. Enable the function.
3. Select **Create the certificate request first and continue the installation.** and click **Create**.
4. Follow the prompt to enter **Country/Region, Domain/IP, Password**, and other parameters.
5. Click **OK**.
6. Click **Download** to download the certificate request and submit it to the trusted authority for signature.



Note

Certification of certificates issued by Certification Authority may incur costs.

7. Import certificate to the device.
 - Click **Browse** to select the certificate and click **Install** to import the certificate to the device.
 - Select **Signed certificate is available, start the installation directly**. Click **Browse** to select the certificate and click **Install** to import the certificate to the device.
8. Enable the function.
9. Click **Save**.

10.3 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 **System → Network Settings → HTTPS** .
2. Enable the function.
3. Select **Create Self-signed Certificate**.
4. Click **Create**.
5. Enter **Country/Region, Domain Name/IP, Validity**, and other parameters, and then click **OK**.
6. Enable the function.
7. Click **Save**.

10.4 Set SSH

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

Steps

1. Go to **System → System Settings → Security Service → Security Service** .
2. Enable or disable SSH, and set **SSH Port No.** if you enable the function.
3. Click **Save**.

10.5 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 **System → System Settings → 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.

Chapter 11 Maintenance

11.1 View Device Information

Go to **System → System Settings → Basic Information** to view the device basic information.
You can edit **Device Name** and **Device No.** It is recommended to reserve the default value.

11.2 View Running Status

Go to **System → System Maintenance → Running Status** to view the server running status, the number of online cameras, the number of current analysis channels, and the camera status such as the online status, resolution, frame rate, analysis status, etc.

11.3 View Audio/Video Parameters

Go to **Smart Traffic Settings → Param Config → Audio/Video** to view audio/video parameters of the selected camera.

11.4 Log

11.4.1 Search Log

You can search logs to troubleshoot problems.

Steps

1. Go to **System → System Maintenance → Log**.
2. Set the search conditions.
3. Click **Search**.
The log information will be displayed in the list.
4. **Optional:** Click **Export** to export the logs to the computer.

11.4.2 Export Debugging Log

Save and export debugging logs.

Steps



Note

This function is only available to professionals.

1. Click **System** → **System Maintenance** → **Debugging Log** .
2. Enable **Save** to save debugging logs.
3. Select **Type**.
4. Click **Save**.
5. **Optional:** To export logs for a specified time period, set **Start Time** and **End Time**, and click **Export**.

11.5 Upgrade

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

Before You Start

Prepare the upgrade file.

Steps

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



Note

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

Result

The device will upgrade and reboot automatically.

11.6 Reboot

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

Steps

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

11.7 Restore Parameters

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

Steps

1. Go to **System → System Maintenance → Upgrade & Maintenance → Default** .
2. Select the restoration mode.
 - Click **Restore** to restore the parameters except the IP parameters and platform parameters to the default settings.
 - Click **Restore Factory Settings** to restore the device to the factory settings.
3. Click **OK**.

11.8 Synchronize Time

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

Steps



Note

Time sync. mode varies with different models. The actual interface prevails.

1. Go to **System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select the time sync. mode.

NTP Time Sync.

Select it to synchronize the device time with that of the NTP server. Set **Server Address**, **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 Time Sync.

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

4. Click **Save**.

11.9 Synchronize Camera Time

It is recommended to synchronize the camera time when the camera time is inconsistent with the device time.

Steps

1. Go to **System → System Settings → Other Settings** .
2. Select **Traffic Camera Time Synchronization** as **Enable**.
3. Set the synchronization threshold.
4. Click **Save**.

Result

The device will synchronize the camera time if the difference between the camera time and the device time exceeds the threshold.

11.10 Set DST

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

Steps

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

11.11 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 **System → System Maintenance → Upgrade & Maintenance → Export Parameters** .
2. Click **Export**.
3. Select the saving path, and name the file.



Note

Please manually enter the ".bin" suffix for the file name.

4. Click **Save**.

11.12 Import Parameters

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 **System → System Maintenance → Upgrade & Maintenance → Import Parameters** .
2. Click **Browse** to select the configuration file.
3. Click **Import**.
4. Click **OK** on the popup window.

Result

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

11.13 Reserved Parameters

The reserved parameters in **System → System Settings → Custom Reserved Params** are for technical personnel debugging only.



See Far, Go Further