IVT2600 Series

User Manual

Manual Version: V1.00

Revision History

Version	Firmware Version	Revision	Release Date	Author
V1.00		First release		

Disclaimer and Safety Warnings

Copyright Statement

©2024 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.
No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).
The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements

unv uniarch are trademarks or registered trademarks of Uniview.
All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will Uniview be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.
The following are necessary measures for the network security of your device:

- **Change default password and set strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Contents

1 Device Login

1.1 Login Preparation

Please complete the installation properly by referring to the quick guide, and then connect power to start the device.

You can manage the device and perform maintenance operations using a web browser.

The following takes Windows 10 as an example.

Preparation Before Web Login

- The device is operating properly.
- The client computer is connected to the device via network.
- You have the required permissions.
- For better display effects, a high resolution monitor is recommended.

1.2 Web Login

The device's static IP address may vary depending on the network interface. For GE1-GE4 network interfaces, the default IP is 192.168.2.30. For GE5-GE20, the default IP is 192.168.1.30.

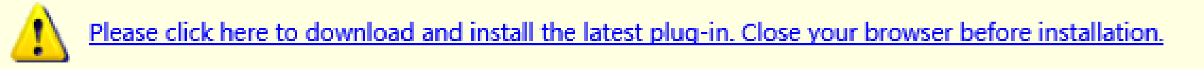
By default, DHCP is enabled on the device. If a DHCP server is configured, the device IP may be assigned dynamically by the DHCP server, be sure to use the actual IP address to log in.

Follow the steps below to log in:

1. Enter the device's IP address in address bar, and then press **Enter**.

2. Download the plugin.

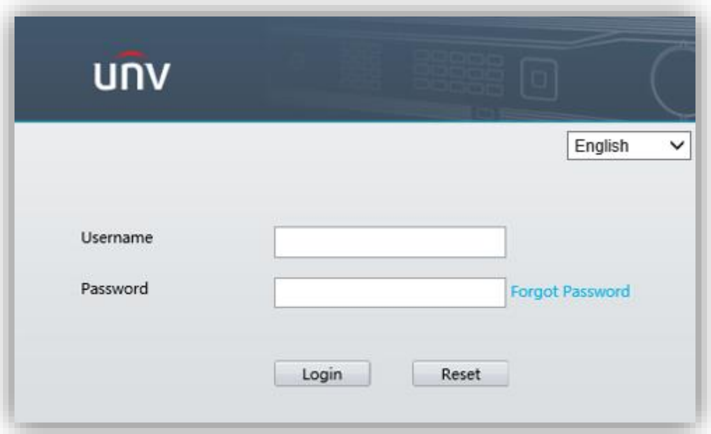
- For first-time use, you may be prompted to install the plugin for live view. Be sure to close all Web browsers before you start the installation. Follow on-screen instructions to complete the installation, and then restart the Web browser as administrator and log in.



Please click here to download and install the latest plug-in. Close your browser before installation.

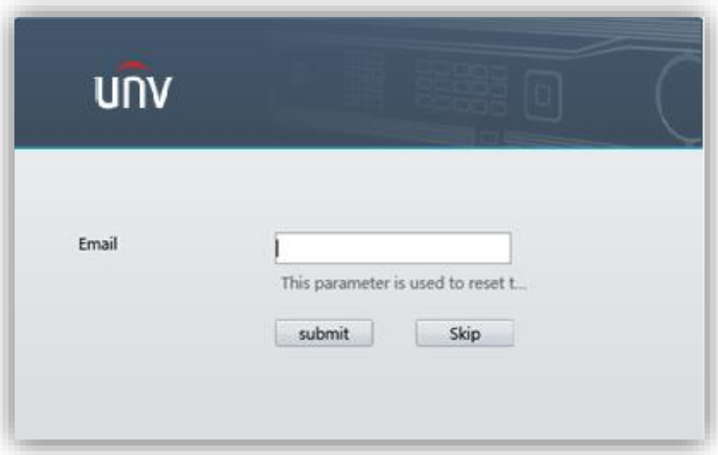
3. Enter the username and password, and then click Login.

- The default username/password is **admin/123456**.
- To clear the username and password, click **Reset**.

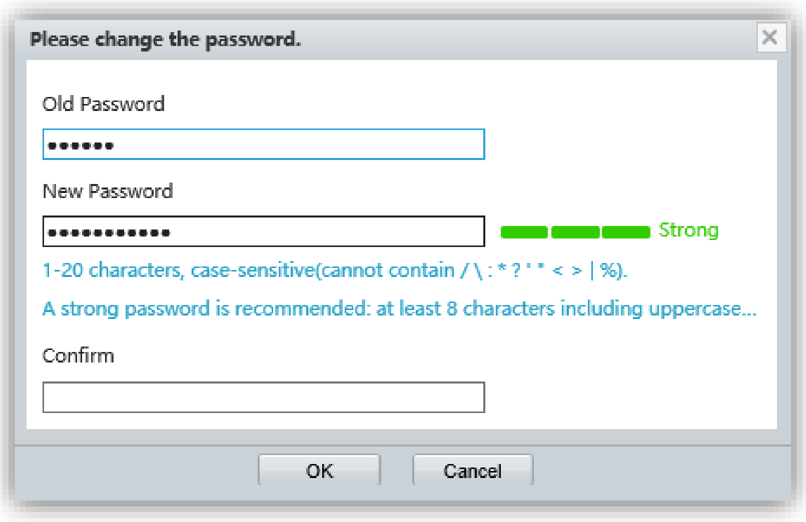


4. After the first-time login, you are prompted to fill in an email address.

- Fill in your email address. The email address can be used to reset the device password if you forgot the password.



- To change the password or email address, see the User section.
- You may also submit an email address later in User after login as admin.
- If you forgot the login password, click Forgot Password on the login page to reset the password.
- You will be prompted to set a strong password (see figure below).



Please change the password.

Old Password

••••••

New Password

•••••••••••• 🟩🟩🟩 Strong

1-20 characters, case-sensitive(cannot contain / \ : * ? ' " < > | %).

A strong password is recommended: at least 8 characters including uppercase...

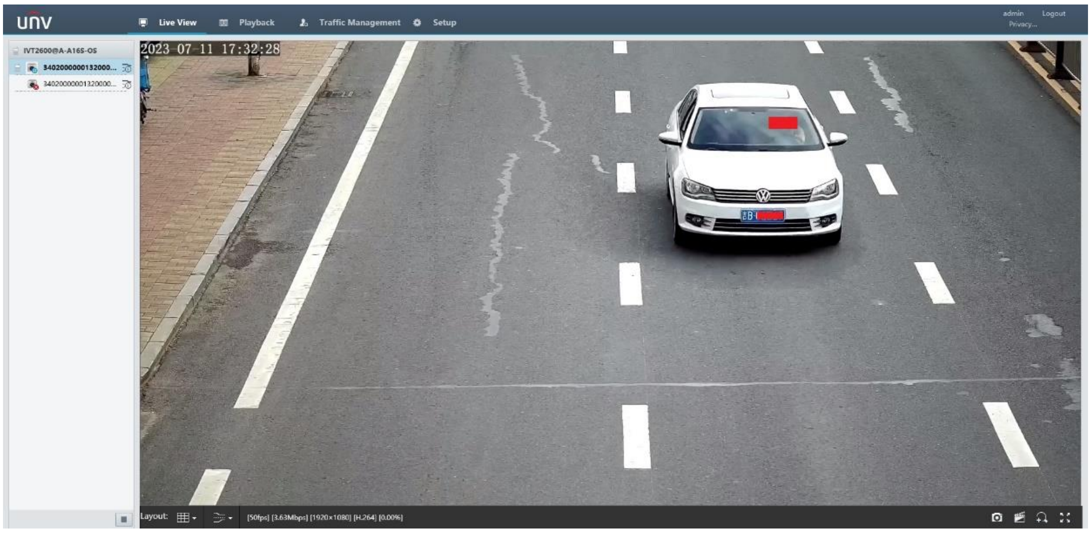
Confirm

2 Live View

2.1 Live View

View the live video from a camera in the client window.

The live view page appears after login. Double-click a camera in the left-side resource tree to start its live video. Or, drag the camera to the live view window on the right side to start its live video.



NOTE!

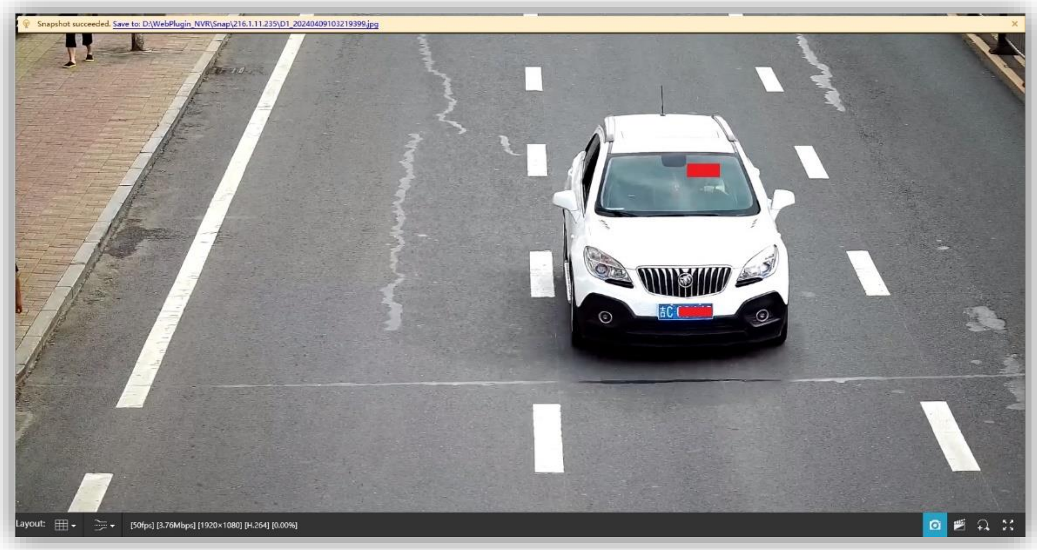
The actual live view operations supported may vary depending on the device model.

Table 2-1 Live View Control Toolbar

Parameter	Description
Layout class ▦ ▾	Set the window layout. ● Currently only 1-window layout is supported.
① ②	Set the live video stream type. ● Choosing ① will play the main stream of the camera. ● Choosing ② will play the sub stream of the camera.
[25fps] [3.88Mbps] [1920×1080] [H.264] [0.00%]	Frame rate/bitrate/resolution/compression format/packet loss rate
📷	Snapshot: Capture an image of the live video playing on the client. The storage location of snapshots is configured in Local Parameters.
🎬 🎬	Start/stop local recording. The storage location of local recordings is configured in Local Parameters.
🔍 🔍	Enable/disable digital zoom. See Digital Zoom.
⛶	Press **Esc** to exit full screen mode.

2.1.1 Snapshot

1. During live view, click 📷 in the live view toolbar to capture an image and save it to the set path (displayed on the top of image).

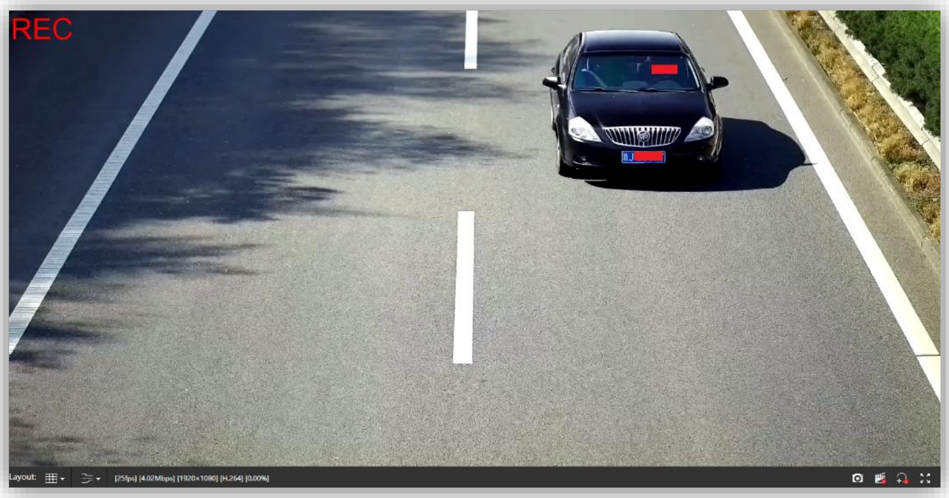


Snapshot succeeded. Save to: D:\WebPlugin_NVR\Snap\216.1.11.235\D1_20240409103219399.jpg

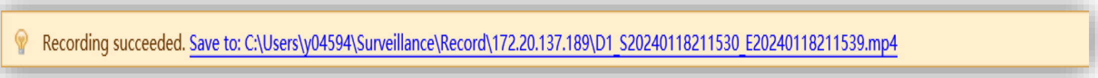
Layout: [50fps] [3.76Mbps] [1920×1080] [H.264] [0.00%]

2.1.2 Local Recording

1. During live view, click in the live view toolbar to start recording the live video. A red “REC” flashes in the top left corner, as shown below.

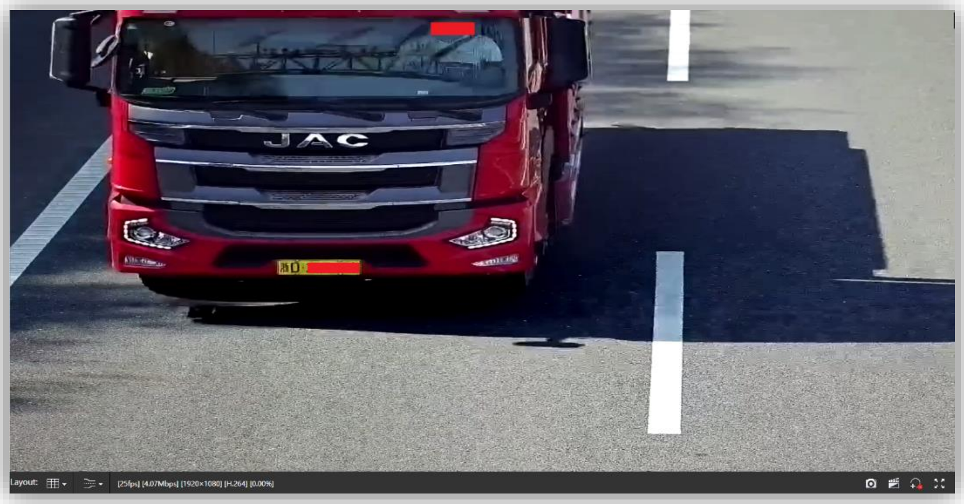


3. Click to stop recording and save the recording to the set path (shown on the top of the window).


Recording succeeded. Save to: C:\Users\y04594\Surveillance\Record\172.20.137.189\D1_S20240118211530_E20240118211539.mp4

2.1.3 Digital Zoom

1. During live view, click in the live view toolbar to enable digital zoom. The figure below shows a digitally zoomed image.

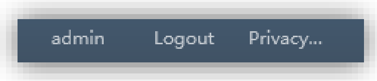


2. View the magnified area

- Click anywhere on the image, and then scroll the mouse wheel to zoom in. Drag the mouse to magnify other parts of the image. Right-click to restore the image.
- Click anywhere on the image, and then drag downwards to specify a rectangle area. The image in the rectangle area is magnified. Drag the area to magnify other parts of the image. Right-click to restore the image.
- Click to disable digital zoom.

2.2 User Information

View the information displayed in the top right corner, as shown below.



admin: Current user.

Logout: Click to log out. A confirmation message will appear.

Privacy Policy: Click to read the privacy policy.

3 Playback

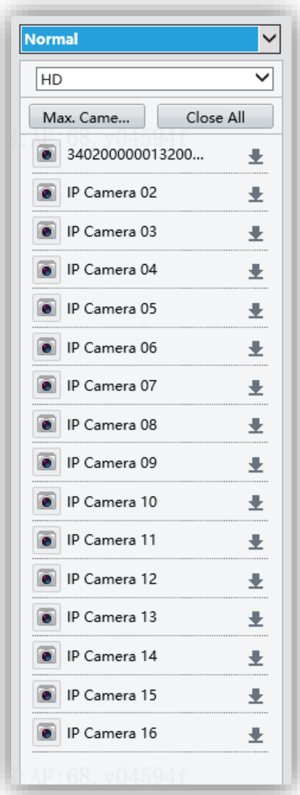
3.1 Recording Playback

NOTE!

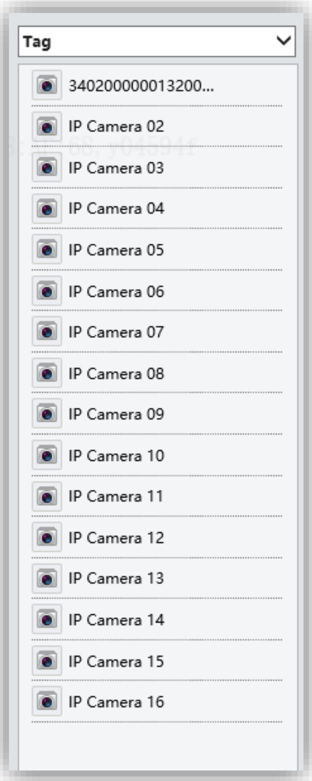
Before searching recordings, make sure storage resource has been configured on the device.

Recording playback supports normal playback and tag playback. You can switch on the resource tree.

Normal playback:

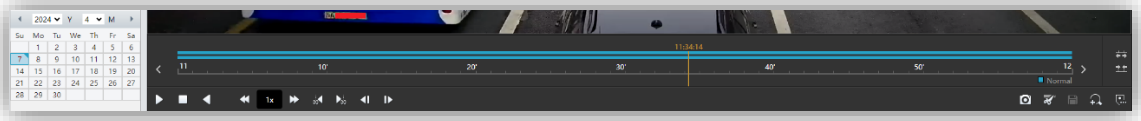


Tag playback:



Follow the steps to search recordings of a camera:

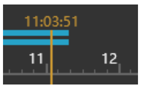
- Step 1: Click to select the camera in the list.
- Step 2: View the recording status on the calendar or on the playback toolbar.



- Step 3: Double-click on the blue progress bar, and then click the play button to start playback.

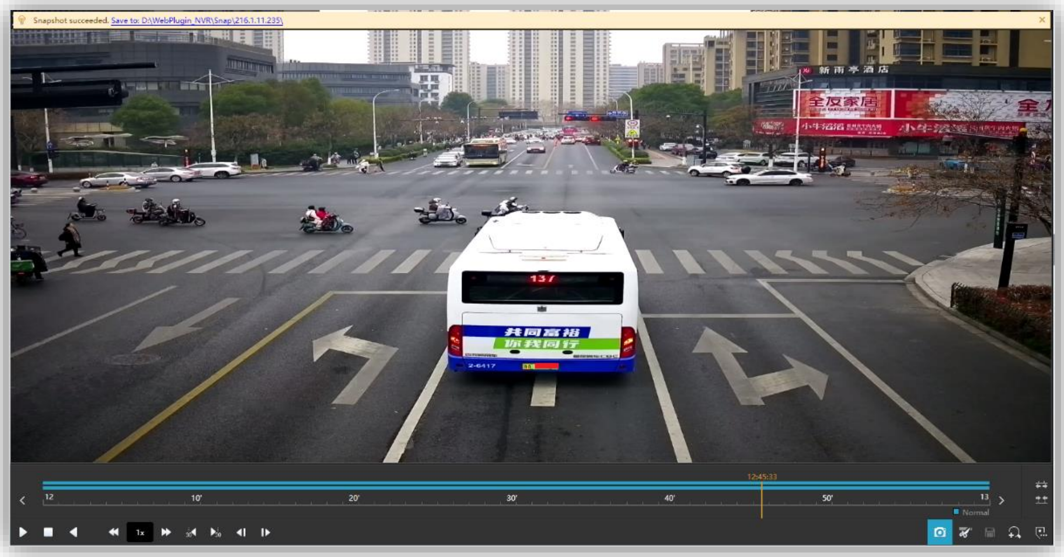
Playback Control Toolbar

Parameter	Description
▶ ⏸ ◀ ⏸ ■	Play/pause the video. Rewind/pause the video. Stop: Stop playback.
⏪ 1x ⏩	Set the playback speed. ⏪: Decrease speed 1x: Current speed

Parameter	Description
	⏩: Increase speed
30◀ ▶30	Forward/rewind 30s. 30◀: Click to rewind 30s ▶30: Click to forward 30s
◀‖ ‖▶	Rewind/forward by frame ◀‖: Rewind the video by one frame ‖▶: Forward the video by one frame.
📷	Snapshot: Capture an image of the recording playing on the client. ● The storage location of snapshots is configured in Local Parameters.
✂ ✂ 💾	Start/stop clipping video and save the video clip. ● You can save and download a selected area.
🔍 🔍	Enable/disable digital zoom. See Digital Zoom.
🏷	Add a custom tag for tag playback.
⇹ ⇼	Zoom in/out on the scale. You may also zoom in or out on the scale by scrolling the mouse wheel.
< >	Click to play the previous or next recording.
	The blue part on the bar means saved recording; the black part on the bar means unsaved recording. You can drag the yellow playhead to skip to the part of the video you want to view.

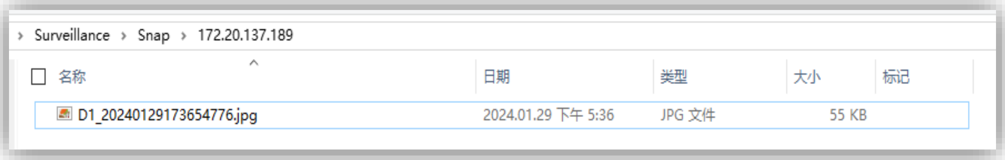
3.1.1 Snapshot

1. Select the desired camera in the list and start playback. During playback, click 📷 in the playback toolbar to capture an image and save it to the set path, as shown below.



Snapshot succeeded. Save to: D:\WebPlugin_NVR\Snap\216.1.11.235\

Click the link to open the folder saving the image.

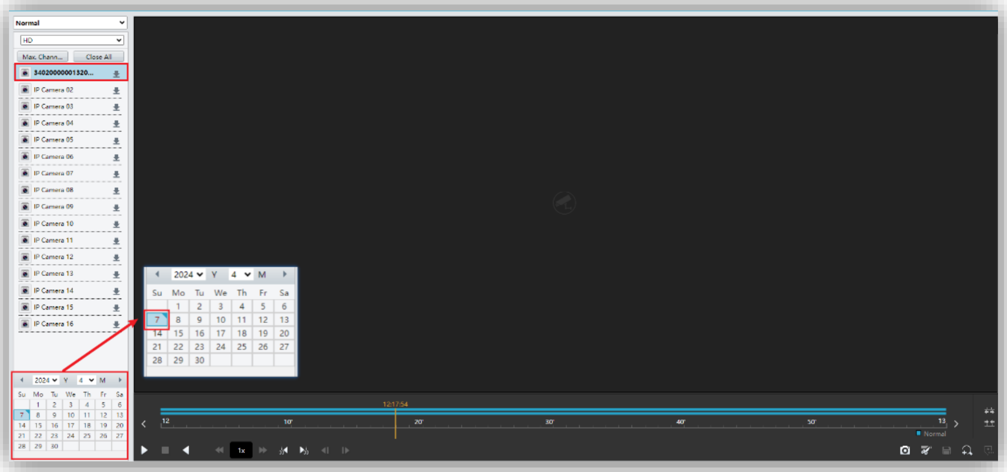


› Surveillance › Snap › 172.20.137.189

□ 名称	日期	类型	大小	标记
D1_20240129173654776.jpg	2024.01.29 下午 5:36	JPG 文件	55 KB	

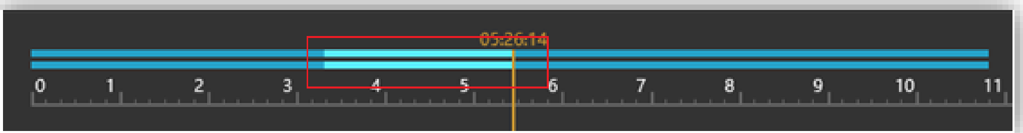
3.1.2 Clip and Download

1. Click a camera in the left-side list to view its recording status on the calendar. The following example describes how to clip and download recordings of 2024-01-29).

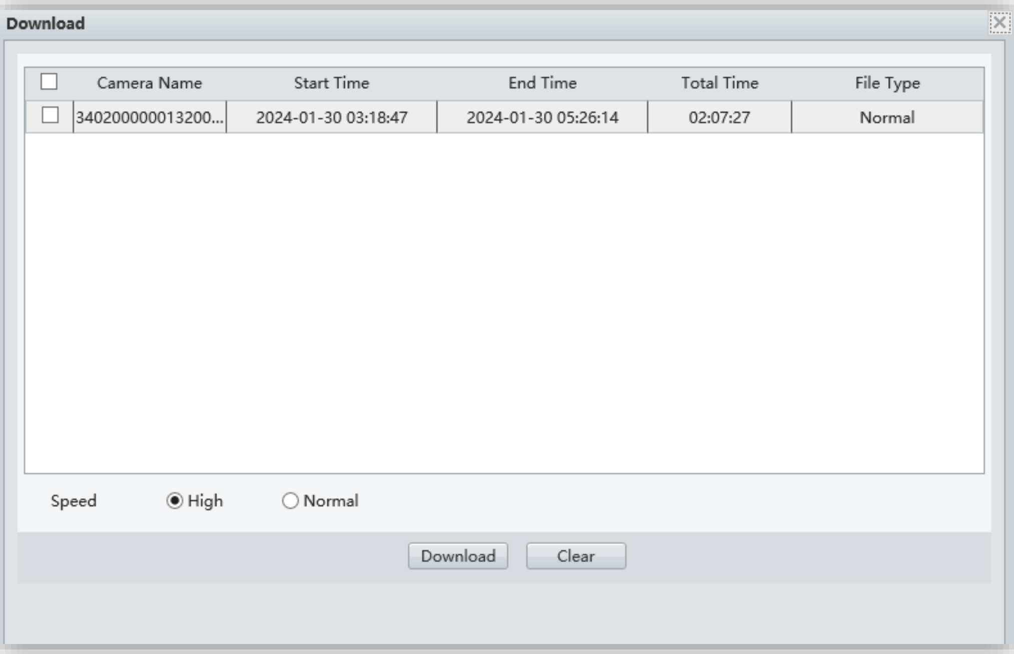


2. Click on the blue timeline to specify the start time of the recording you want to clip, and then click on the playback toolbar; click on the blue timeline to specify the end time of the recording you want to

clip, and then click on the playback toolbar. The specified part shows a lighter color on the time line.



3. Click in the playback toolbar, and then you can download the clipped recordings in the dialog box as shown below.

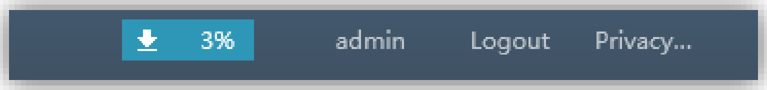


Download

□	Camera Name	Start Time	End Time	Total Time	File Type
□	340200000013200...	2024-01-30 03:18:47	2024-01-30 05:26:14	02:07:27	Normal

Speed ● High ○ Normal

- Select the recordings to download, and then click **Download**.
- The download progress is displayed in the top right corner, as shown below.



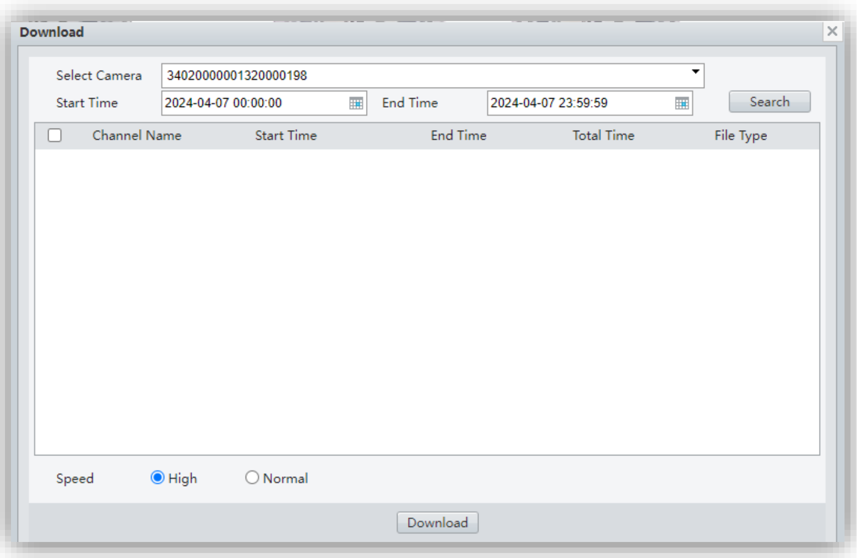
3.1.3 Digital Zoom

The operations are the same as that in the live view toolbar. See 2.1.3 Digital Zoom.

3.2 Recording Download

3.2.1 Recording Search and Download

1. Select a camera in the list, and then click ⬇ to download the recording of the selected camera.



Download

Select Camera 34020000001320000198

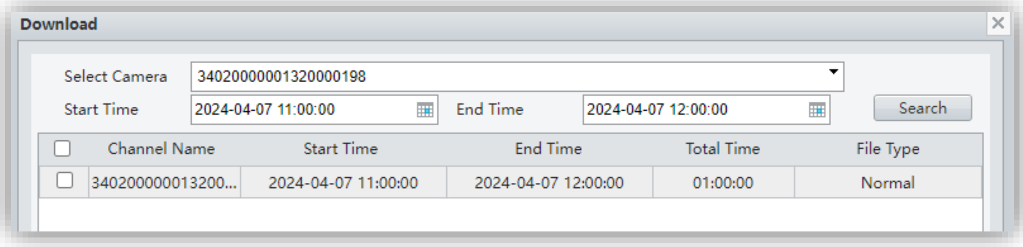
Start Time 2024-04-07 00:00:00 End Time 2024-04-07 23:59:59 Search

□	Channel Name	Start Time	End Time	Total Time	File Type

Speed ● High ○ Normal

Download

2. Set the start time and end time for the recording, and then click **Search**. The list below shows the corresponding recording, for example, 2024-04-07 11:00:00 to 2024-04-07 12:00:00.



Download

Select Camera 34020000001320000198

Start Time 2024-04-07 11:00:00 End Time 2024-04-07 12:00:00 Search

□	Channel Name	Start Time	End Time	Total Time	File Type
□	340200000013200...	2024-04-07 11:00:00	2024-04-07 12:00:00	01:00:00	Normal

3. Select the checkbox for the recording to download, choose high-speed download, and then click **Download**.
   - For the download progress display, see step 3 in Clip and Download.
   - Click download progress to view the detailed download information.

4 Traffic Management

NOTE!

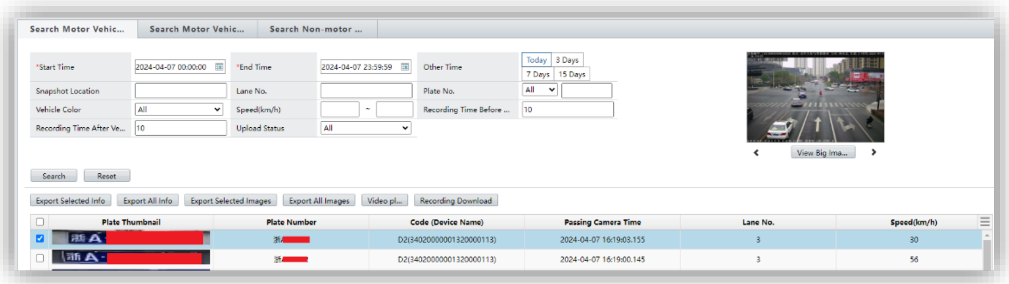
- Before searching photos, check that the cameras have been added to the device, and image storage space has been configured.
- Before searching photos, check that images captured by the cameras can be uploaded to the server, and the network is normal.

- Checkpoint motor vehicle search searches records of passing vehicles captured by cameras. Interval motor vehicle search searches for records of passing vehicles in a speed measurement interval. Non-motor vehicle search searches for records of non-motor vehicles captured by cameras.
- Violation vehicle search searches for violation vehicle info. Checkpoint motor vehicle search does not search for violation info.

4.1 Image Search

4.1.1 Checkpoint Motor Vehicle Search

1. Go to **Traffic Management** > **Search Image** > **Search Motor Vehicle in Checkpoint**. The page is as shown below.



*Start Time: 2024-04-07 00:00:00

*End Time: 2024-04-07 23:59:59

Other Time: Today | 3 Days | 7 Days | 15 Days

Snapshot Location:

Lane No.:

Plate No.: All

Vehicle Color: All

Speed(km/h): ~

Recording Time Before ...: 10

Recording Time After Ve...: 10

Upload Status: All

	Plate Thumbnail	Plate Number	Code (Device Name)	Passing Camera Time	Lane No.	Speed(km/h)
☑	浙A[redacted]	浙[redacted]	D2(34020000001320000113)	2024-04-07 16:19:03.155	3	30
□	浙A-[redacted]	浙[redacted]	D2(34020000001320000113)	2024-04-07 16:19:00.145	3	56

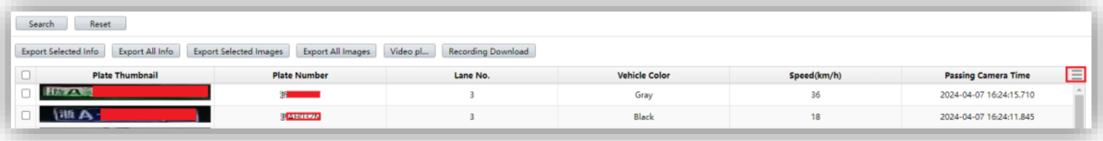
Table 4-1-1 Parameter Configuration Descriptions

Parameter	Description
Start Time/End Time	Set a time range for image searching.
Other Time	Options are Today, Last 3 days, Last 7 days, and Last 15 days. Today means the current day; last 3, 7, and 15 days mean the search time range from the past 2, 6, and 14 days to the current day, respectively.
Snapshot Location	Used to search images of a specified camera ID.
Lane No.	Used to search images of a specified lane ID.
Plate No.	By default, all plate numbers will be searched. You may specify a plate number to search a specific vehicle.
Vehicle Color	Choose a vehicle color to search vehicles.
Speed	Enter a speed range to search vehicles.
Recording Time Before Vehicle Pass-thru (s) Recording Time After Vehicle Pass-thru (s)	The start and end time of vehicle passing recording. Defaults to 10 seconds.
Upload Status	Image upload status. For example, to search uploaded images only, select Uploaded.

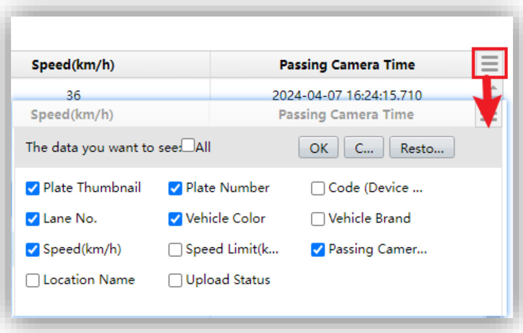
Parameter	Description
Search/Reset	Query: Click to search images that meet the search criteria. Reset: Click to reset the search criteria to the initial status.
Export Selected Info	Click to export the selected images with image information to the vehicle query.csv file and save the file to the PC.
Export All Info	Click to export all the retrieved images with image information to the vehicle query.csv file and save the file to the PC.
Export Selected Images	Click to export the selected images in the list to the PC.
Export All Images	Click to export all the retrieved images to the PC.
Playback/Download	Recording playback: Select an image in the list, and then click the play button to play the video 10s before and after the snapshot time. The **Recording Time Before Vehicle Pass-thru** and **Recording Time After Vehicle Pass-thru** parameters determine the video length.
View Big Image	Click to view the large image and image information.
☰	Click to personalize the items displayed on the image list. See Customize Columns.

4.1.2 Customize Columns

1. Go to **Traffic Management** > **Search Traffic Data** > **Search Motor Vehicle in Checkpoint** > **Search Motor Vehicle in Checkpoint**. Click ☰.



☐	Plate Thumbnail	Plate Number	Lane No.	Vehicle Color	Speed(km/h)	Passing Camera Time
☐	[redacted]	浙[redacted]	3	Gray	36	2024-04-07 16:24:15.710
☐	[redacted]	浙[redacted]	3	Black	18	2024-04-07 16:24:11.845

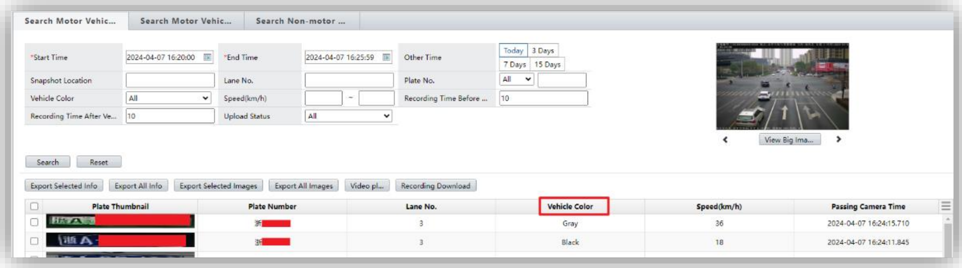


Speed(km/h)	Passing Camera Time
36	2024-04-07 16:24:15.710

The data you want to see: ☐All

☑ Plate Thumbnail ☑ Plate Number ☐ Code (Device ...
☑ Lane No. ☑ Vehicle Color ☐ Vehicle Brand
☑ Speed(km/h) ☐ Speed Limit(k... ☑ Passing Camer...
☐ Location Name ☐ Upload Status

2. Select items you want to display on the image list, for example, if "the color of car" is selected, this item will be displayed on the image list.

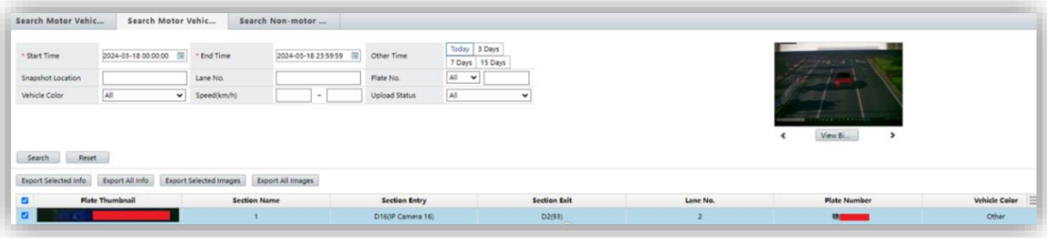


*Start Time	2024-04-07 16:20:00	*End Time	2024-04-07 16:25:59	Other Time	Today 3 Days 7 Days 15 Days
Snapshot Location		Lane No.		Plate No.	All
Vehicle Color	All	Speed(km/h)	~	Recording Time Before ...	10
Recording Time After Ve...	10	Upload Status	All		

□	Plate Thumbnail	Plate Number	Lane No.	Vehicle Color	Speed(km/h)	Passing Camera Time
□	[redacted]	浙[redacted]	3	Gray	36	2024-04-07 16:24:15.710
□	[redacted]	浙[redacted]	3	Black	18	2024-04-07 16:24:11.845

4.1.3 Interval Motor Vehicle Search

1. Go to **Traffic Management** > **Search Traffic Data** > **Search Motor Vehicle in Checkpoint** > **Search Motor Vehicle in Interval**. The page is as shown below.



* Start Time	2024-03-18 00:00:00	* End Time	2024-03-18 23:59:59	Other Time	Today 3 Days 7 Days 15 Days
Snapshot Location		Lane No.		Plate No.	All
Vehicle Color	All	Speed(km/h)	~	Upload Status	All

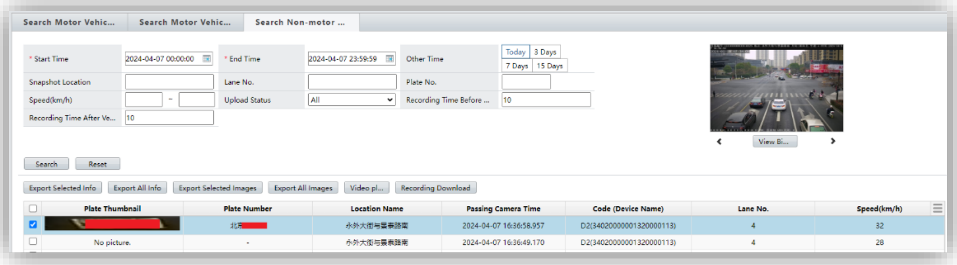
☑	Plate Thumbnail	Section Name	Section Entry	Section Exit	Lane No.	Plate Number	Vehicle Color
☑	[redacted]	1	D16(IP Camera 16)	D2(93)	2	[redacted]	Other

NOTE!

See the table in Section 4.1.1 for configuration descriptions.

4.1.4 Non-motor Vehicle Search

1. Go to **Traffic Management** > **Search Traffic Data** > **Search Motor Vehicle in Checkpoint** > **Search Non-motor Vehicle**. The page is as shown below.



* Start Time	2024-04-07 00:00:00	* End Time	2024-04-07 23:59:59	Other Time	Today 3 Days 7 Days 15 Days
Snapshot Location		Lane No.		Plate No.	
Speed(km/h)	~	Upload Status	All	Recording Time Before ...	10
Recording Time After Ve...	10				

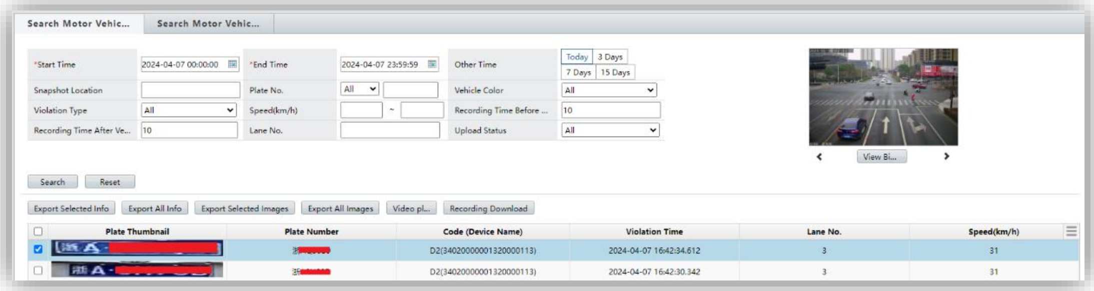
□	Plate Thumbnail	Plate Number	Location Name	Passing Camera Time	Code (Device Name)	Lane No.	Speed(km/h)
☑	[redacted]	北[redacted]	永外大街与景泰路南	2024-04-07 16:36:58.957	D2(34020000001320000113)	4	32
□	No picture.	-	永外大街与景泰路南	2024-04-07 16:36:49.170	D2(34020000001320000113)	4	28

NOTE!

See the table in Section 4.1.1 for configuration descriptions.

4.1.5 Violation Motor Vehicle Search

1. Go to **Traffic Management** > **Search Motor Vehicle with Violations** > **Search Motor Vehicle with Violations**. The page is as shown below.



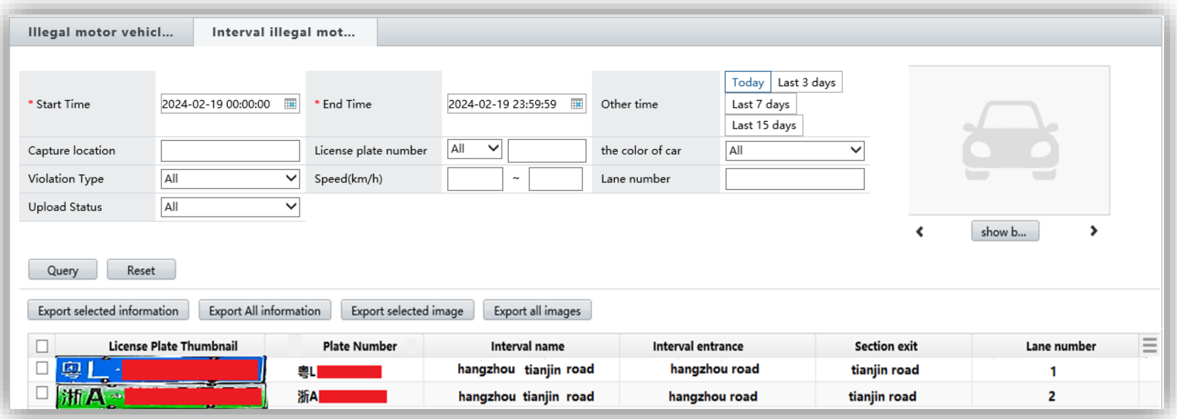
*Start Time	2024-04-07 00:00:00	*End Time	2024-04-07 23:59:59	Other Time	Today 3 Days 7 Days 15 Days
Snapshot Location		Plate No.	All	Vehicle Color	All
Violation Type	All	Speed(km/h)	~	Recording Time Before ...	10
Recording Time After Ve...	10	Lane No.		Upload Status	All

□	Plate Thumbnail	Plate Number	Code (Device Name)	Violation Time	Lane No.	Speed(km/h)
☑	浙A-[redacted]	浙[redacted]	D2(34020000001320000113)	2024-04-07 16:42:34.612	3	31
□	浙A-[redacted]	浙[redacted]	D2(34020000001320000113)	2024-04-07 16:42:30.342	3	31

NOTE!

See the table in Section 4.1.1 for configuration descriptions.

4.1.6 Interval Violation Motor Vehicle Search



* Start Time	2024-02-19 00:00:00	* End Time	2024-02-19 23:59:59	Other time	Today Last 3 days Last 7 days Last 15 days
Capture location		License plate number	All	the color of car	All
Violation Type	All	Speed(km/h)	~	Lane number	
Upload Status	All				

□	License Plate Thumbnail	Plate Number	Interval name	Interval entrance	Section exit	Lane number
□	粤L-[redacted]	粤L[redacted]	hangzhou tianjin road	hangzhou road	tianjin road	1
□	浙A[redacted]	浙A[redacted]	hangzhou tianjin road	hangzhou road	tianjin road	2

NOTE!

See the table in Section 4.1.1 for configuration descriptions.

4.2 Violation Determination

4.2.1 Interval Speed Measurement

1. Interval Configuration

1. Go to **Traffic Management** > **Violation Determination** > **Section Speed Measurement**. The page is as shown below.

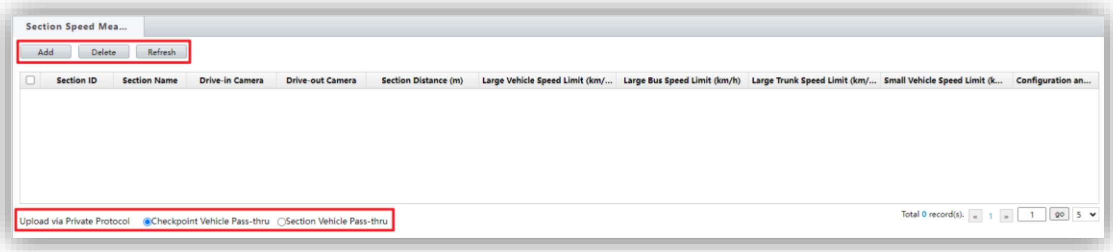

Section Speed Mea...
Add
Delete
Refresh
Section ID
Section Name
Drive-in Camera
Drive-out Camera
Section Distance (m)
Large Vehicle Speed Limit (km/...
Large Bus Speed Limit (km/h)
Large Trunk Speed Limit (km/...
Small Vehicle Speed Limit (k...
Configuration an...
Upload via Private Protocol
●Checkpoint Vehicle Pass-thru
○Section Vehicle Pass-thru
Total 0 record(s).
1
go
5

Table 4-2-1 Parameter Configuration Description

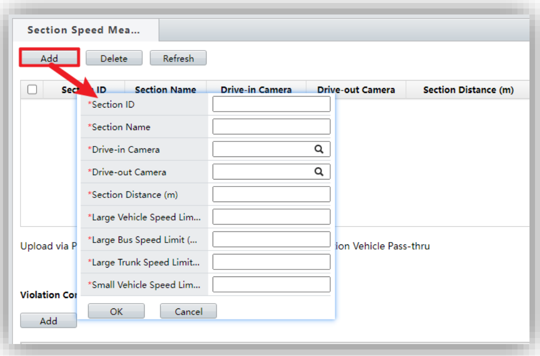
Parameter	Description
Add	Click **Add** to fill in interval information. See Table 4-2-2.  Section Speed Mea... Add Delete Refresh Section ID Section Name Drive-in Camera Drive-out Camera Section Distance (m) *Section ID *Section Name *Drive-in Camera *Drive-out Camera *Section Distance (m) *Large Vehicle Speed Lim... *Large Bus Speed Limit (... *Large Trunk Speed Limit... *Small Vehicle Speed Lim... OK Cancel Upload via P ion Vehicle Pass-thru Violation Co Add
Delete	Select the interval to delete, and then click **Delete**.
Refresh	Click to refresh the interval list.
Upload via Private Protocol	Checkpoint Vehicle Pass-thru: The uploaded images are vehicles passing a checkpoint. Interval Vehicle Pass-thru: The uploaded images are vehicles passing a road section.

Table 4-2-2 Parameter Configuration Description

Parameter	Description
Interval ID	Enter an ID for the interval.
Interval Name	Interval name. Enter a name as needed.
Drive-in Camera	Camera that captures approaching vehicles in interval speed measurement.
Drive-out Camera	Camera that captures departing vehicles in interval speed measurement.

Parameter	Description
Interval Distance (m)	Length of the interval for speed measurement.
Large Vehicle Speed Limit (km/h)	Speed limit for large vehicles. It is considered speeding if the average speed of a vehicle within the interval exceeds the limit.
Large Bus Speed Limit (km/h)	Speed limit for large buses. It is considered speeding if the average speed of a vehicle within the interval exceeds the limit.
Large Trunk Speed Limit (km/h)	Speed limit for large trucks. It is considered speeding if the average speed of a vehicle within the interval exceeds the limit.
Small Vehicle Speed Limit (km/h)	Speed limit for small vehicles. It is considered speeding if the average speed of a vehicle within the interval exceeds the limit.

2. Click **Save** when you complete the configuration.

2. Violation Configuration

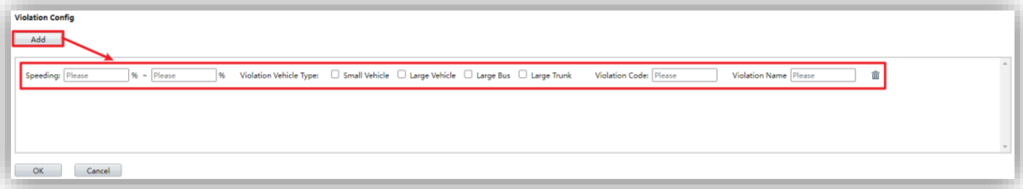

Violation Config
Add
Speeding: Please % ~ Please %
Violation Vehicle Type: □ Small Vehicle □ Large Vehicle □ Large Bus □ Large Trunk
Violation Code: Please
Violation Name Please
OK
Cancel

Table 4-2-3 Parameter Configuration Description

Parameter	Description
Speeding	Speeding percentage range. When the speeding value falls within the set range, the corresponding violation code will be output.
Violation Vehicle Type	Violation vehicle type. Choose the type(s) as needed.
Violation Code/Name	A violation code and violation name that will be output when the speeding value falls in a set speeding percentage range.

2. Click **Save** when you complete the configuration.

4.3 Image Composition

4.3.1 Add Violation

1. Go to **Traffic Management** > **Image Composite** > **Violation Type Association**. The page is as shown below.

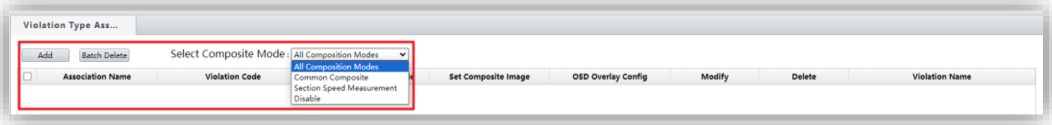


Table 4-3-1 Parameter Configuration Description

Parameter	Description
Add	Click **Add** to add a composition mode. See the table below for

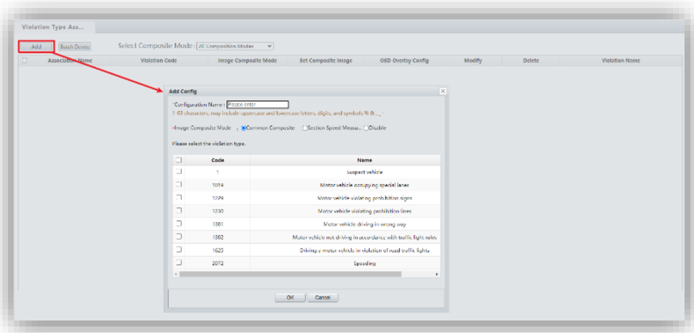
Parameter	Description
	configuration description.  Select Composite Mode : All Composition Modes Association Name / Violation Code / Image Composite Mode / Set Composite Image / OSD Overlay Config / Modify / Delete / Violation Name *Configuration Name : Please enter 1-63 characters, may include uppercase and lowercase letters, digits, and symbols % & , _ - *Image Composite Mode : ● Common Composite ○ Section Speed Measu... ○ Disable Please select the violation type. □ Code — Name □ 1 — Suspect vehicle □ 1019 — Motor vehicle occupying special lanes □ 1229 — Motor vehicle violating prohibition signs □ 1230 — Motor vehicle violating prohibition lines □ 1301 — Motor vehicle driving in wrong way □ 1302 — Motor vehicle not driving in accordance with traffic light rules □ 1625 — Driving a motor vehicle in violation of road traffic lights □ 2072 — Speeding
Delete	Select composition mode(s) in the list and then click **Delete**.
Select Composition Mode	All composition modes: When this mode is selected, the list shows all the image composition modes without differentiation. Common synthesis: When this mode is selected, the list shows the common composition mode. Interval velocity measurement: When this mode is selected, the list shows interval speed measurement mode. Do not enable composition: When this mode is selected, the list shows that image composition is disabled.

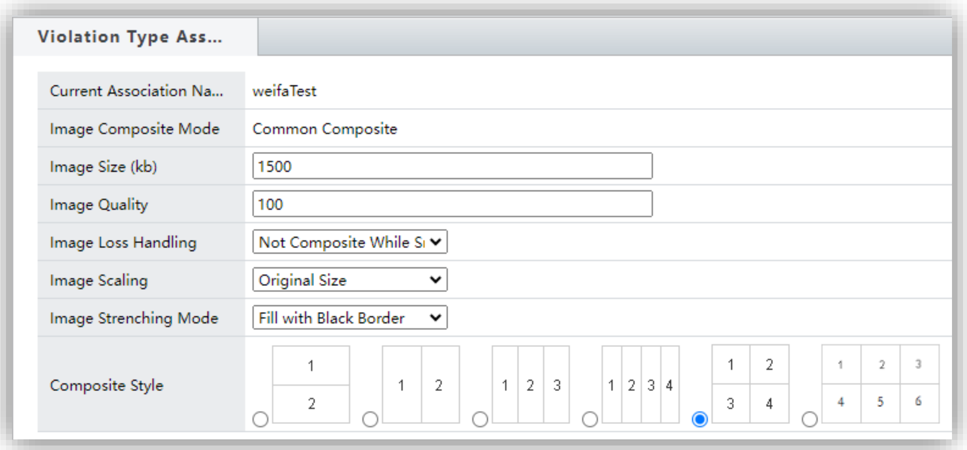
Table 4-3-2 Parameter Configuration Description

Parameter	Description
Configuration Name	Enter the violation type name.
Image Composition Mode	Three composition modes are available: Common synthesis: Used for common violations. Interval velocity measurement: Used for interval speeding violations. Do not enable composition: Choosing this mode will disable image composition.
Violation Types	Select the corresponding violation code(s) according to the current composition mode.

2. Click **Save** when you complete the configuration.

4.3.2 Image Composition Configuration

1. In the composition mode list, click ⚙ under image composition configuration. A page as shown below appears.

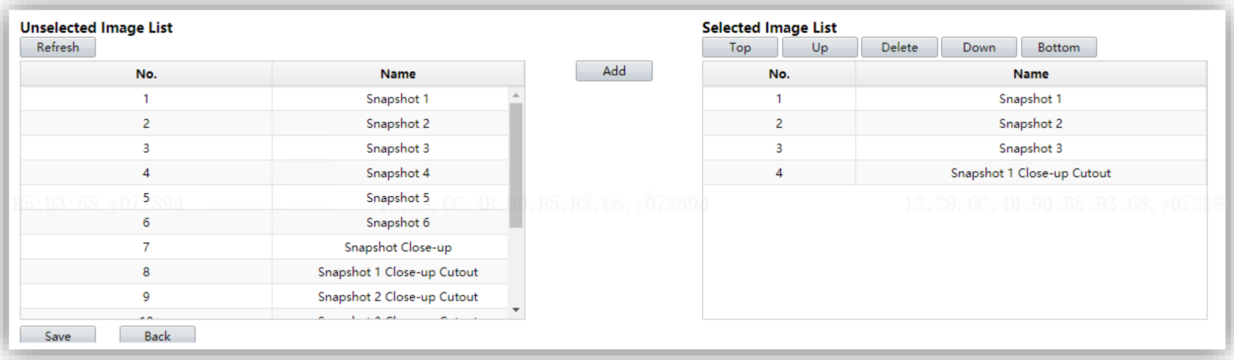


Violation Type Ass...

Current Association Na...	weifaTest
Image Composite Mode	Common Composite
Image Size (kb)	1500
Image Quality	100
Image Loss Handling	Not Composite While Si
Image Scaling	Original Size
Image Strenching Mode	Fill with Black Border
Composite Style	○ ○ ○ ○ ● ○

- Configure Image Composition Parameters

Parameter	Description
Current Violation Name	Violation name.
Image Composition Mode	Shows the current image composition mode.
Image Size (KB)	The default is 1500KB. You can modify the setting as needed. The range is 100-4096.
Image Quality	The default is 100. Keep the default setting unless modification is required.
Snapshot Loss Handling	Continue Image Composition: Image composition will continue if a snapshot is missing. The missing snapshot will be displayed as black. Cancel Image Composition: Image composition will be cancelled if a snapshot is missing.
Size of Composite Image	Total Size of Snapshots: After composition, the image resolution will be added based on the resolution of the individual snapshots. Size of One Snapshot: After composition, the image resolution remains the same as the resolution of the individual snapshots.
Image Stretching Mode	Black Padding: After composition, if the resolutions of the closeup image is different from the resolution of the individual snapshots, the excess parts will be filled with black. Stretch: After composition, if the resolution of the closeup image is different from the resolution of the individual snapshots, the closeup image will be stretched so its resolution will be the same as the resolution of the individual snapshots.
Composition Style	Six options are available. Choose as needed. For the meaning of the numbers, please see the Selected Image List in the figure below.



Unselected Image List

No.	Name
1	Snapshot 1
2	Snapshot 2
3	Snapshot 3
4	Snapshot 4
5	Snapshot 5
6	Snapshot 6
7	Snapshot Close-up
8	Snapshot 1 Close-up Cutout
9	Snapshot 2 Close-up Cutout

Selected Image List

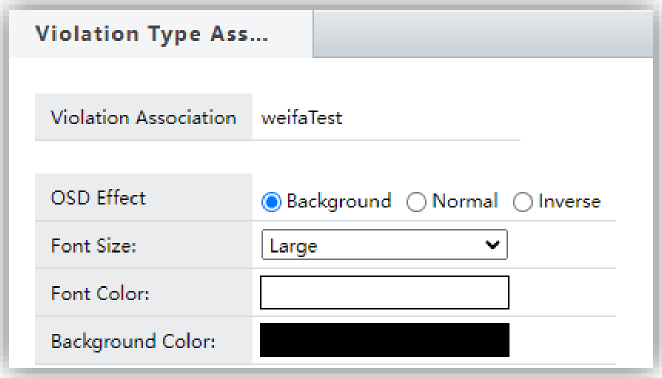
No.	Name
1	Snapshot 1
2	Snapshot 2
3	Snapshot 3
4	Snapshot 1 Close-up Cutout

- Configure image list:

Parameter	Description
Unselected Image List	Choose images to be used for composition. ● To select **Snapshot Close-up**, make sure **Vehicle Closeup** is selected at **Smart** > **Snapshot Handling** > **Photo of Violation**). This requirement is unnecessary for other options.
Add	Click to add the selected images to the right-side list.
Selected Image List	Shows the selected images that will be used in image composition style. ● The numbers (No.) in the selected picture list correspond to the numbers in the composition style. ● The number of selected images must match the number of images in the selected composition style.
Top/Up/Delete/Down/Bottom set	Perform the following operations to the selected images. Top set: Select a number and then click this button to set the image to the top of the list. Up: Select a number and then click this button to move the image upward. Delete: Select a number and then click this button to remove the image from the list. Down: Select a number and then click this button to move the image downward. Bottom set: Select a number and then click this button to set the image to the bottom of the list.

4.3.3 OSD Overlay Configuration

1. After you complete the configuration of image composition, click ⚙ under OSD overlay configuration to open the page as shown below.



Violation Type Ass...

Violation Association	weifaTest
OSD Effect	● Background ○ Normal ○ Inverse
Font Size:	Large
Font Color:	
Background Color:	■

- Configure the parameters by referring to the table below.

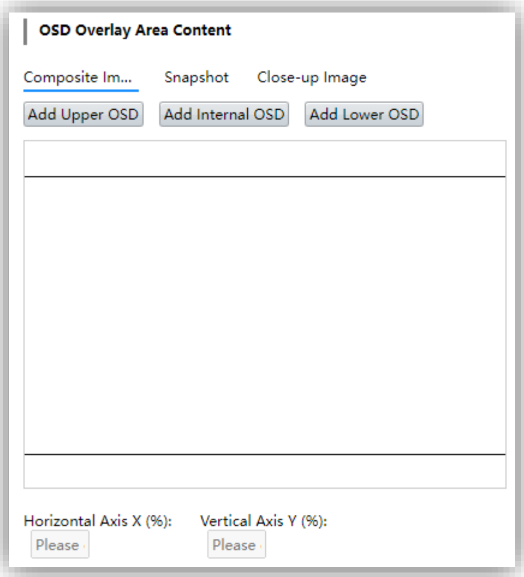
Parameter	Description
Violation Name	Shows the violation type name.
OSD Effect	Three options. Choose as needed.
Font Size	OSD font size.
Font Color	OSD font color.
Background Color	Click to choose a background color for the OSD. This parameter is effective when **OSD Effect** is set to **Background**.

2. Click **Save** when you complete the configuration.

NOTE!

You can configure OSD for composite image, snapshot image (original image), and closeup image. The following takes composite image as an example.

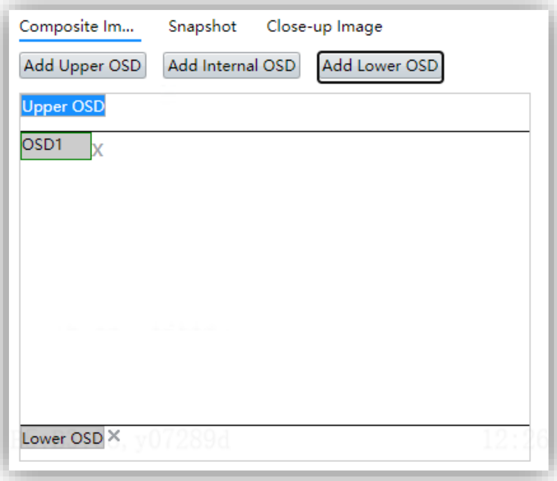
1. Configure the OSD position, as shown below.



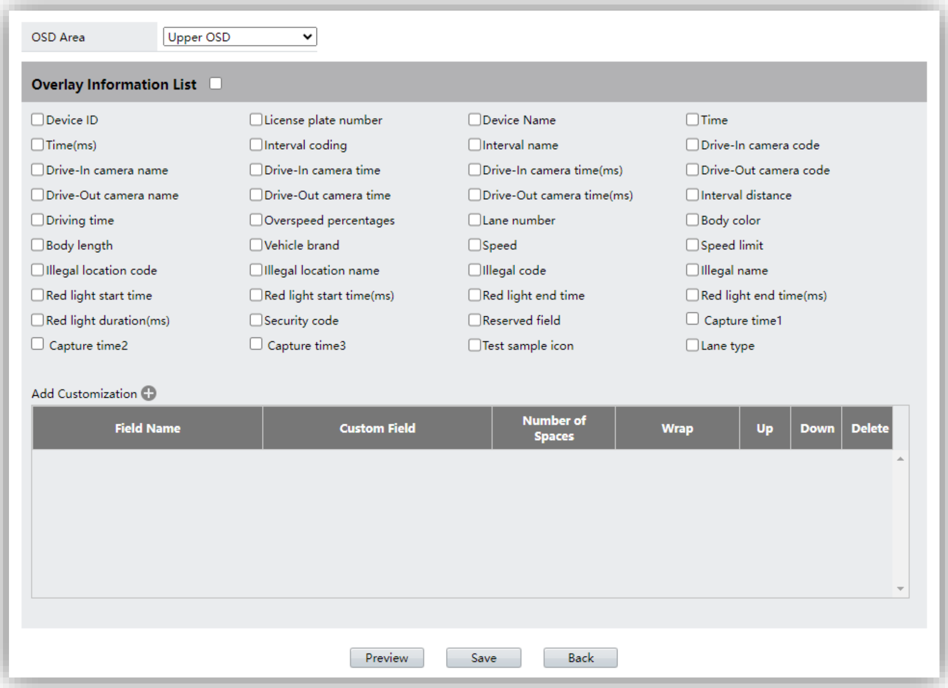
OSD Overlay Area Content

- Configure the parameters by referring to the table below.

Parameter	Description
Add Upper OSD	Click this button to display OSD above the image. See "The upper OSD" in the figure below. Only one OSD is allowed.
Add Internal OSD	Click this button to display OSD inside the image. See "OSD1" in the figure below. Up to four OSDs are allowed.
Add Lower OSD	Click this button to display the OSD below the image. See "The below OSD" in the figure below. Only one OSD is allowed.
Horizontal Axis X (%) Horizontal Axis Y (%)	These two parameters are used to adjust the position of OSDs inside the image. You may also drag the OSDs to change their positions.



2. After completing the configuration of OSD overlay, configure OSD content. The page is as shown below.



OSD Area: Upper OSD

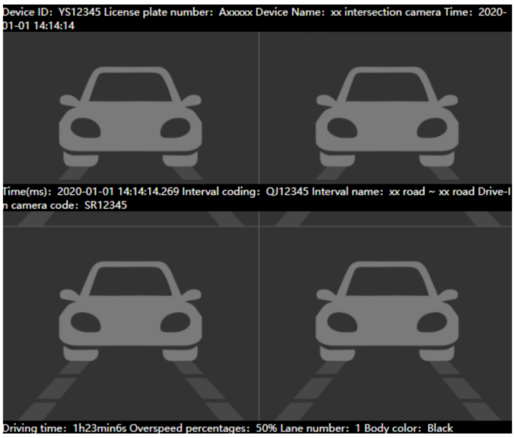
Overlay Information List □

□Device ID	□License plate number	□Device Name	□Time
□Time(ms)	□Interval coding	□Interval name	□Drive-In camera code
□Drive-In camera name	□Drive-In camera time	□Drive-In camera time(ms)	□Drive-Out camera code
□Drive-Out camera name	□Drive-Out camera time	□Drive-Out camera time(ms)	□Interval distance
□Driving time	□Overspeed percentages	□Lane number	□Body color
□Body length	□Vehicle brand	□Speed	□Speed limit
□Illegal location code	□Illegal location name	□Illegal code	□Illegal name
□Red light start time	□Red light start time(ms)	□Red light end time	□Red light end time(ms)
□Red light duration(ms)	□Security code	□Reserved field	□ Capture time1
□ Capture time2	□ Capture time3	□Test sample icon	□Lane type

Add Customization ⊕

Field Name	Custom Field	Number of Spaces	Wrap	Up	Down	Delete

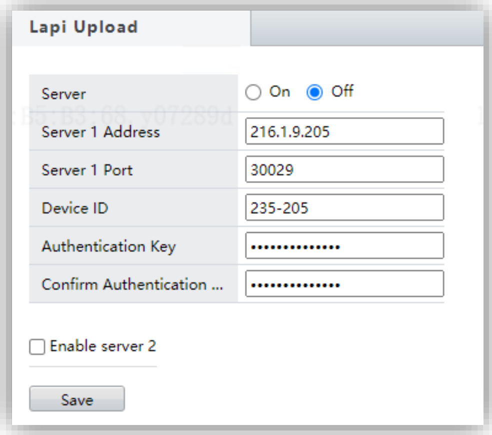
- Configure the parameters by referring to the table below.

Parameter	Description
OSD Area	Choose the OSD area. Upper OSD: The OSD content will be displayed in the **Upper OSD** area. Internal OSD: The OSD content will be displayed in the **Internal OSD** area. The number of internal OSDs is determined by the number of internal OSDs added. Below OSD: The OSD content will be displayed in the **Below OSD** area.
Overlay Information List	Select the OSD content to be displayed in the corresponding OSD area.
Add Customization	Click to add a custom field. Up to four custom fields are allowed.
Field Name	Field name of the corresponding OSD.
Custom Field	By default, it is empty. The actual OSD is the field value, not the field name.
Number of Spaces	Range: 1-10. Number of spaces allowed before the next OSD.
Wrap	Range: 1-3. Number of lines allowed before the next OSD.
Up	Click to move the OSD up.
Down	Click to move the OSD down.
Delete	Click to delete the OSD.
Preview/Save/Back	Preview: Preview the configured OSD, as shown below:  Device ID：YS12345 License plate number：Axxxxx Device Name：xx intersection camera Time：2020-01-01 14:14:14 Time(ms)：2020-01-01 14:14:14.269 Interval coding：QJ12345 Interval name：xx road ~ xx road Drive-In camera code：SR12345 Driving time：1h23min6s Overspeed percentages：50% Lane number：1 Body color：Black Save: Save the current settings on the page. Cancel: Discard the current settings and return to the previous page.

4.4 Image Upload

4.4.1 Upload via LAPI Protocol

1. To upload images via the LAPI protocol, go to **Traffic Management** > **Picture Upload** > **LAPI Upload**. The page is as shown below.



Lapi Upload

Server	○ On ● Off
Server 1 Address	216.1.9.205
Server 1 Port	30029
Device ID	235-205
Authentication Key	••••••••••••••
Confirm Authentication ...	••••••••••••••

□ Enable server 2

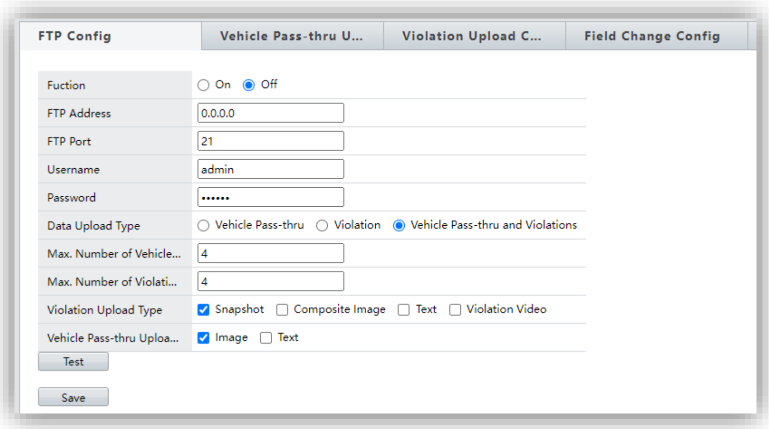
- Configure the parameters by referring to the table below.

Parameter	Description
Server	Select **On** to enable image upload via LAPI.
Server Address	Enter the server address.
Server Port	Enter numbers as needed.
Device ID	Enter the device ID configured on the server.
Authentication Key/Confirm Authentication Key	Enter the key configured on the server.
Enable server 2	Server 2 is disabled by default. To enable image upload to a second server, select the checkbox to enable this function. Other settings are similar to that for Server 1.

4.4.2 FTP Upload

1. Basic Configuration for FTP Upload

1. To upload images and videos to the FTP server via FTP, go to **Traffic Management** > **Picture Upload** > **FTP Protocol Upload**. The page is as shown below.



Fuction	○ On ● Off
FTP Address	0.0.0.0
FTP Port	21
Username	admin
Password	••••••
Data Upload Type	○ Vehicle Pass-thru ○ Violation ● Vehicle Pass-thru and Violations
Max. Number of Vehicle...	4
Max. Number of Violati...	4
Violation Upload Type	☑ Snapshot □ Composite Image □ Text □ Violation Video
Vehicle Pass-thru Uploa...	☑ Image □ Text

- Configure the parameters by referring to the table below.

Parameter	Description
Function	Select **On** to enable image upload via FTP.
FTP Address	FTP server address.
FTP Port	Default is 21. Generally this setting requires no modification.
Username	Username used to access the FTP server.
Password	Password used to access the FTP server.
Data Upload Type	Choose the types of data to be uploaded to the FPT server: Passing a car: Upload only passing vehicle images. Violation of regulations: Only upload violation images. Passing a car and violation of regulations: Upload both passing vehicle images and violation images.
Max. Number of Vehicle Pass-thru Snapshots	Maximum number of passing vehicle images that can be uploaded.
Max. Number of Violation Images	Maximum number of violation images that can be uploaded.
Violation Upload Type	Choose the type(s) of violation data to be uploaded to the FTP server: Snapshot: Upload snapshots of violation vehicles. Composite Image: Upload composition images. Text: Upload text information of the corresponding snapshots and composition images. Violation Video: Upload violation videos of violation vehicles. See Violation Video Upload for more information.
Vehicle Pass-thru Upload Type	Choose the type(s) of passing vehicle data to be uploaded to the FPT server: Snapshot: Upload images of passing vehicles. Text: Upload text information of passing vehicles.
Test	Click this button to test if the FTP server is online.

2. FTP Upload Path, Text and Text Content Configuration

1. Follow the steps below to configure upload for passing vehicles.

NOTE!

The steps for configuring upload for passing vehicles and violation vehicles are the same, both require you to configure the upload path. This section only describes how to configure upload for passing vehicles.

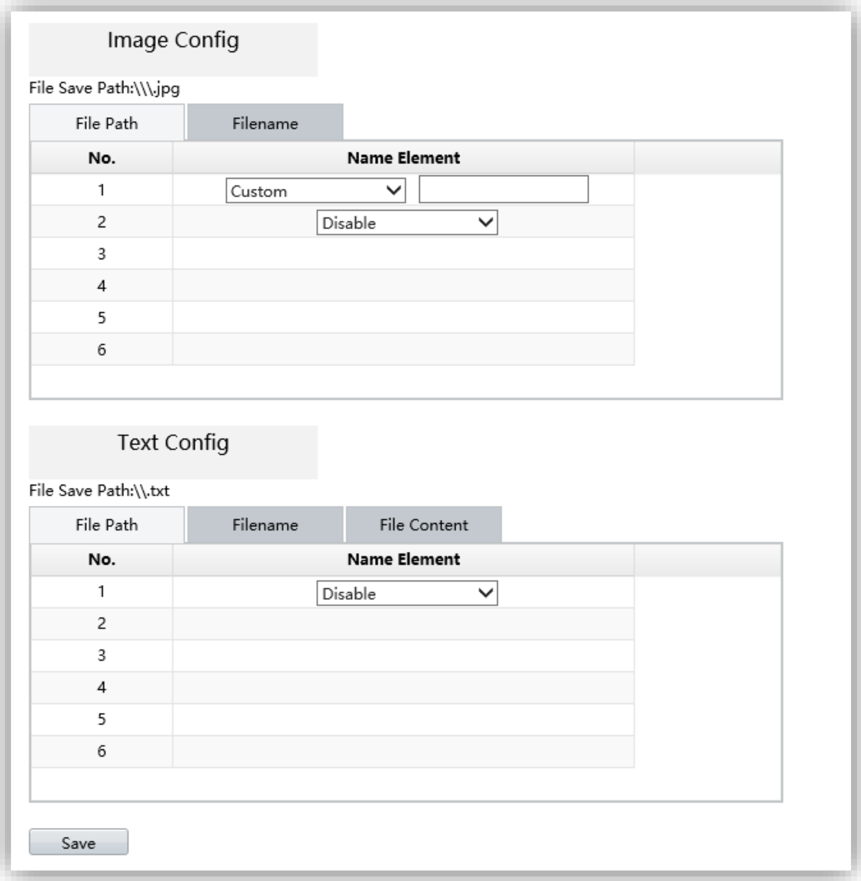


Image Config

File Save Path:\\\.jpg

No.	Name Element
1	Custom
2	Disable
3	
4	
5	
6	

Text Config

File Save Path:\\.txt

No.	Name Element
1	Disable
2	
3	
4	
5	
6	

- Configure the parameters by referring to the table below.

Parameter	Description
Image Config	
File Path-No.	Up to 6 levels of directories can be created to store images.
File Path-Naming Element	Filename in the file path. You can choose multiple elements from the list.
Filename-Naming Element	Name of the uploaded file. You can choose multiple elements from the list.
Text Config	
File Path-No.	Up to 6 levels of directories can be created to store text.

Parameter	Description
File Path-Naming Element	Filename in the path of the text. You can choose multiple elements from the list.
Filename-Naming Element	Name of the uploaded text file. You can choose multiple elements from the list.
File Content-Naming Element	Content of the uploaded text file. You can choose multiple elements from the list.

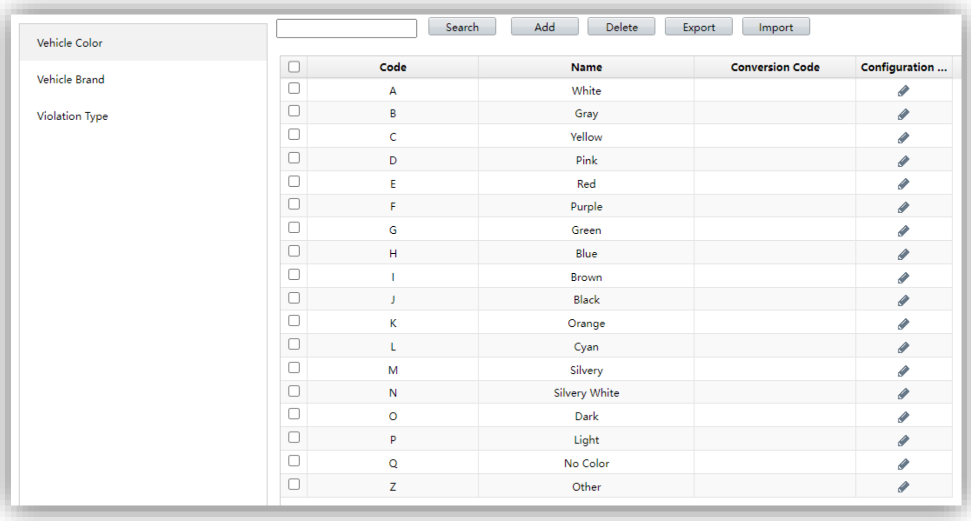
2. After you complete upload configuration for passing vehicles, continue to configure upload for violation vehicles._

3. Text Conversion Configuration

NOTE!

This section takes Vehicle Color as an example to describe how to configure text conversion. The configuration steps for other fields are similar.

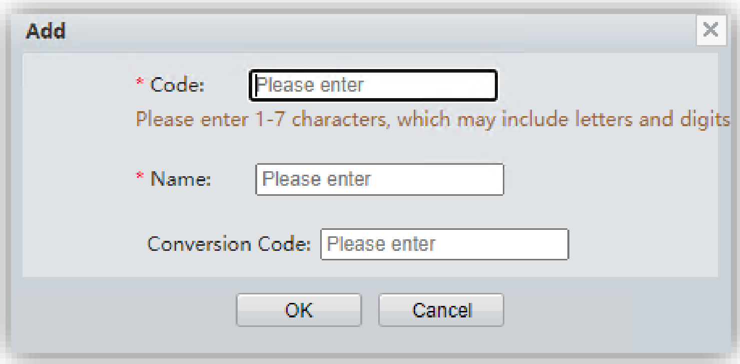
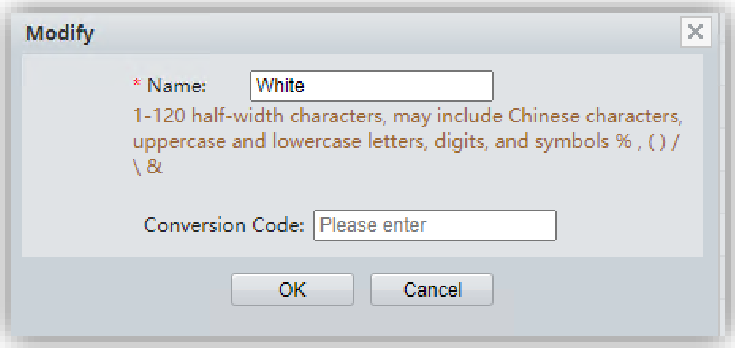
1. Refer to the figure below to configure field conversion for FTP upload.



□	Code	Name	Conversion Code	Configuration ...
□	A	White		✎
□	B	Gray		✎
□	C	Yellow		✎
□	D	Pink		✎
□	E	Red		✎
□	F	Purple		✎
□	G	Green		✎
□	H	Blue		✎
□	I	Brown		✎
□	J	Black		✎
□	K	Orange		✎
□	L	Cyan		✎
□	M	Silvery		✎
□	N	Silvery White		✎
□	O	Dark		✎
□	P	Light		✎
□	Q	No Color		✎
□	Z	Other		✎

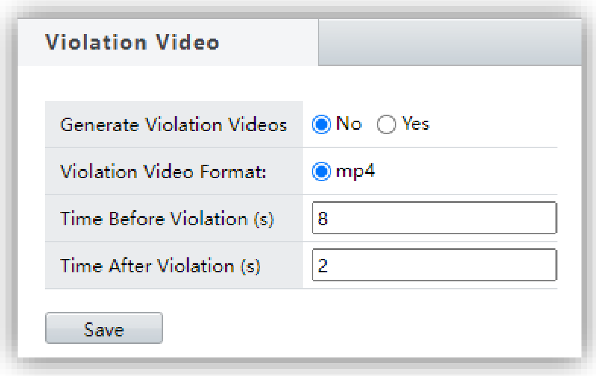
- Configure the parameters by referring to the table below.

Parameter	Description
Search box	Enter keywords to search for the desired fields.
Query	Enter a keyword in the search box, and then click this button to search for fields containing the keyword you entered.
Add	Click the **Add** button to add a field, as shown below:

Parameter	Description
	 Add * Code: Please enter Please enter 1-7 characters, which may include letters and digits * Name: Please enter Conversion Code: Please enter OK Cancel Code: Enter a code consisting of 1-7 characters (digits and letters) for the new field. Name: Enter a name for the new field. Conversion coding: Enter a code consisting of 1-7 characters (digits and letters). Configure this item only when required.
Delete	Select the fields you want to delete, and then click this button to delete them.
Export	Export all the fields on the current page to a table.
Import	Import a table containing the required fields. This function allows you to modify fields in batches.
Modify	Click ✎ to modify the field information.  * Name: White 1-120 half-width characters, may include Chinese characters, uppercase and lowercase letters, digits, and symbols % , ( ) / \ &

4.4.3 Violation Video Upload

1. Go to **Traffic Management** > **Picture Upload** > **Violation Video** to configure violation video upload.



Violation Video

Generate Violation Videos	● No ○ Yes
Violation Video Format:	● mp4
Time Before Violation (s)	8
Time After Violation (s)	2

- Configure the parameters by referring to the table below.

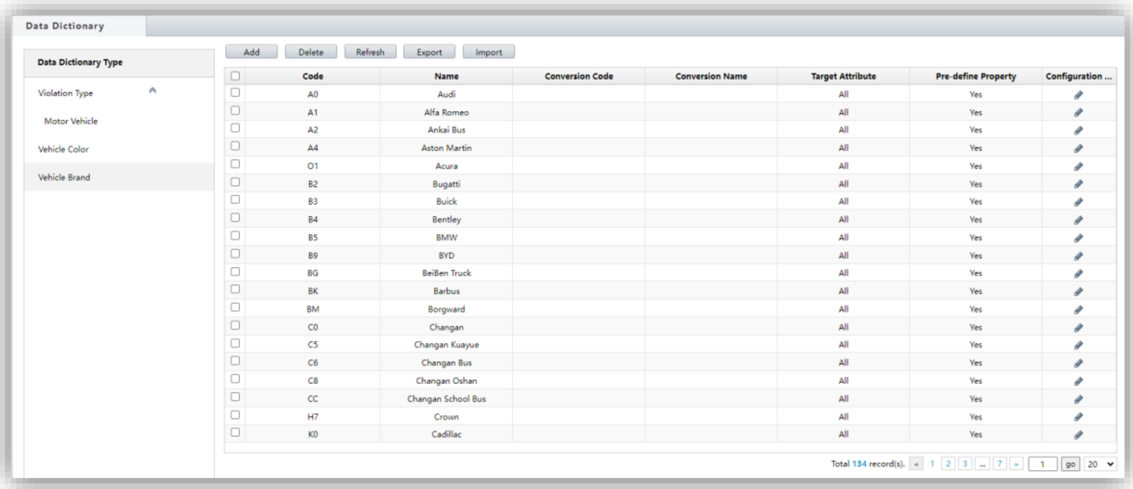
Parameter	Description
Generate Violation Videos	To upload violation videos, select **Yes**.
Violation Video Format	The default format is .mp4. Keep the default setting.
Time Before Violation (s) Time After Violation (s)	Used to configure the length of passing vehicle recordings. The default recording start time is 8 seconds before the violation time; the default recording end time is 2 seconds after the violation time. The actual violation time is determined by the violation time configured on the camera.

4.5 Data Dictionary

NOTE!

This section describes data field configuration by taking violation type as an example. For the modification of other fields, please refer to the descriptions of body color configuration.

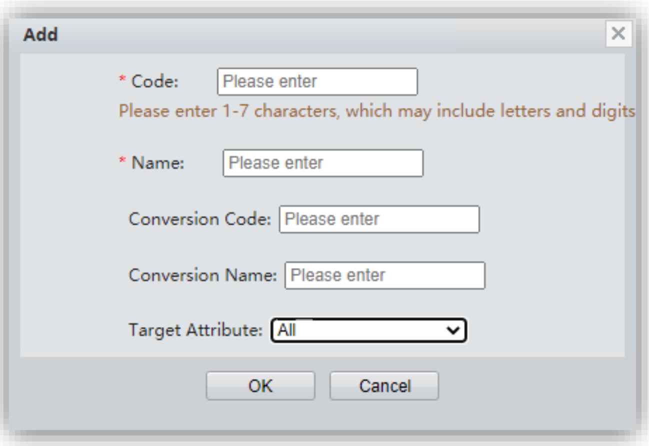
1. After completing image upload configuration, if you want to add or modify certain fields, you can go to **Traffic Management** > **Picture Upload** > **Data Dictionary**.

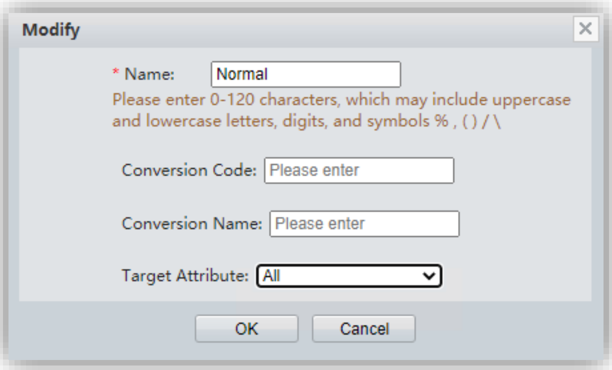


□	Code	Name	Conversion Code	Conversion Name	Target Attribute	Pre-define Property	Configuration ...
□	A0	Audi			All	Yes	✎
□	A1	Alfa Romeo			All	Yes	✎
□	A2	Ankai Bus			All	Yes	✎
□	A4	Aston Martin			All	Yes	✎
□	O1	Acura			All	Yes	✎
□	B2	Bugatti			All	Yes	✎
□	B3	Buick			All	Yes	✎
□	B4	Bentley			All	Yes	✎
□	B5	BMW			All	Yes	✎
□	B9	BYD			All	Yes	✎
□	BG	BeiBen Truck			All	Yes	✎
□	BK	Barbus			All	Yes	✎
□	BM	Borgward			All	Yes	✎
□	C0	Changan			All	Yes	✎
□	C5	Changan Kuayue			All	Yes	✎
□	C6	Changan Bus			All	Yes	✎
□	C8	Changan Oshan			All	Yes	✎
□	CC	Changan School Bus			All	Yes	✎
□	H7	Crown			All	Yes	✎
□	K0	Cadillac			All	Yes	✎

Total 134 record(s). « 1 2 3 ... 7 » 1 go 20

- Configure the parameters by referring to the table below.

Parameter	Description
Add	Click the **Add** button to add a field, as shown below:  Add * Code: Please enter Please enter 1-7 characters, which may include letters and digits * Name: Please enter Conversion Code: Please enter Conversion Name: Please enter Target Attribute: All OK Cancel Code: Enter a code consisting of 1-7 characters (digits and letters) for the new field. Name: Enter a name for the new field. Conversion coding: Enter a code consisting of 1-7 characters (digits and letters). Configure this item only when required. Conversion name: Enter a name for name conversion. Configure this item only when required.
Delete	Select the fields you want to delete, and then click this button to delete them.
Refresh	Click to refresh the page.
Export	Export all the fields on the current page to a table.
Import	Import a table containing the required fields. This function allows you to modify fields in batches.

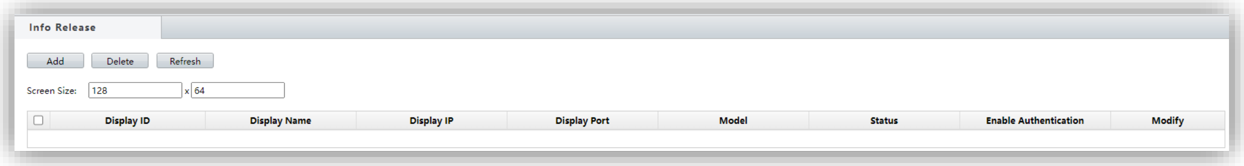
Parameter	Description
Modify	Click ✎ to modify the field information.  Modify * Name: Normal Please enter 0-120 characters, which may include uppercase and lowercase letters, digits, and symbols % , ( ) / \ Conversion Code: Please enter Conversion Name: Please enter Target Attribute: All

2. Click **Save** when you complete the configuration.

4.6 Information Release

4.6.1 Add Display

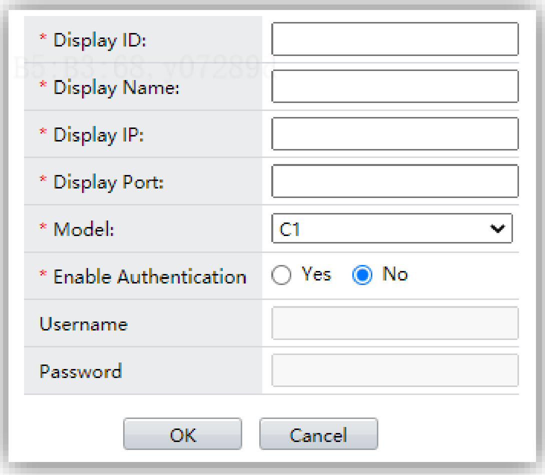
1. Go to **Traffic Management** > **Info Release** > **Info Release**. The page is as shown below.



Info Release

Screen Size: 128 x 64

- Configure the parameters by referring to the table below.

Parameter	Description
Add	Click the **Add** button to add a field, as shown below:  * Display ID: * Display Name: * Display IP: * Display Port: * Model: C1 * Enable Authentication ○ Yes ● No Username Password Display ID: Enter a code for the display.

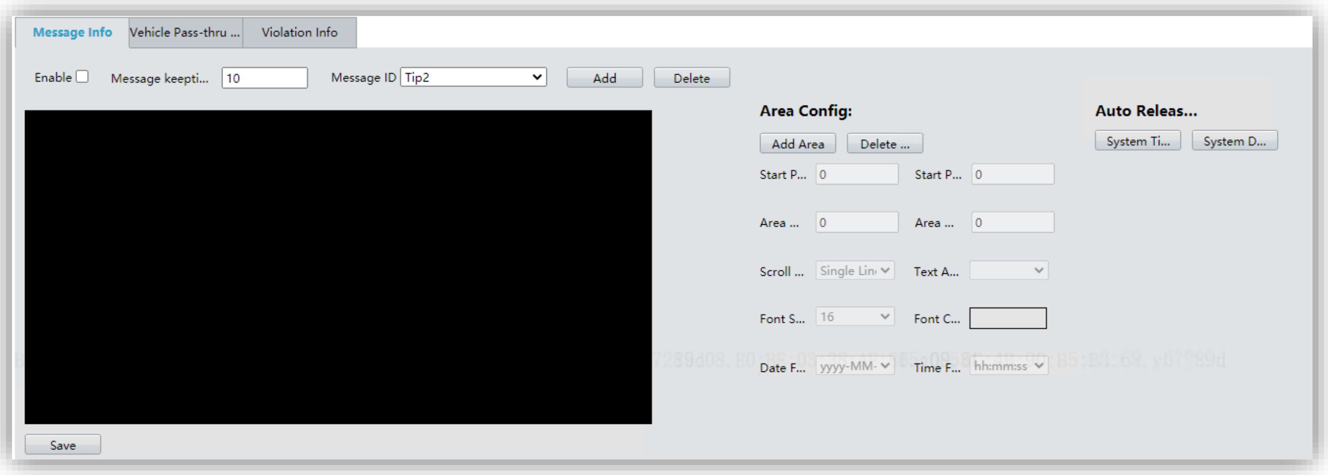
Parameter	Description
	Display Name: Enter a name for the display. Display IP: Enter the IP address of the display. Display Port: Enter 5884 as the port number. Model: Choose C1 or C4 according to the actual model of the display. Enable Authentication: Defaults to No. After enabling authentication, you need to enter the correct username and password. Username/Password: These fields are required when **Need Authentication** is enabled.
Delete	Select the display to delete, and then click **Delete**.
Refresh	Click to refresh the settings.
Display Size	Set according to the actual size of the display.
Display List	Shows information about the added displays, including online/offline status.

4.6.2 Configure Message Info Release

NOTE!

- Priority level for releasing information: violation info > vehicle pass-thru info > message info.
- Info release requires the display to be online.

1. The message info page is as shown below.



Enable □

Message keepti... 10

Message ID Tip2

Start P... 0

Start P... 0

Area ... 0

Area ... 0

Scroll ... Single Lin

Text A...

Font S... 16

Font C...

Date F... yyyy-MM-

Time F... hh:mm:ss

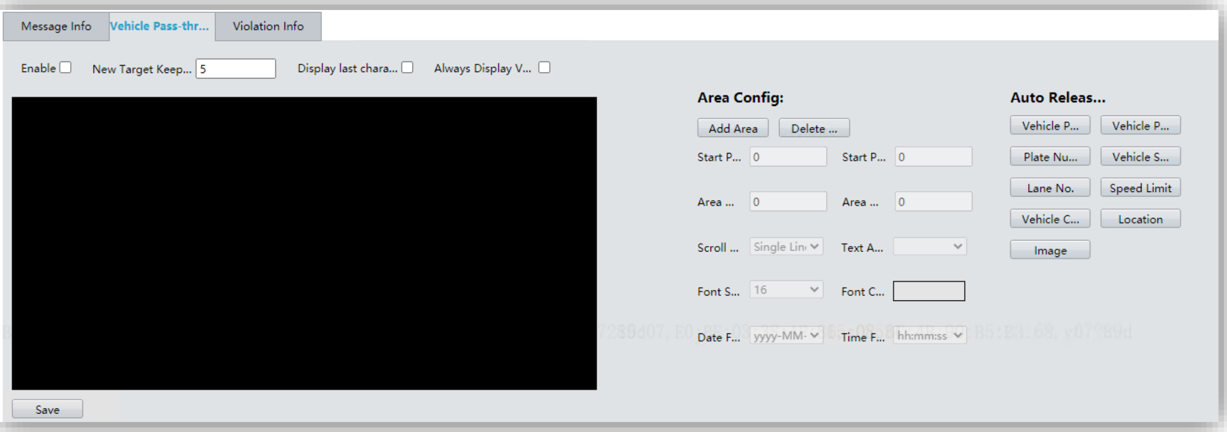
- Configure the parameters by referring to the table below.

Parameter	Description
Enable	Select the checkbox to enable releasing message info.
Message Keeptime (s)	Length of time message info will be displayed when there is no vehicle pass-thru info or violation info.
Message ID	Up to four message info can be added. You can select the message info from the list.
Add/Delete	Click **Add** to add message info. Up to four can be added.
Preview area (black)	Preview the info to be released.
Area Config	
Add Area	Click to add an area. The added area appears in the preview area on the left side. The size of the added area is limited by the area width and height. ● You can set area contents by selecting **Auto Release Field**, or enter information manually.
Delete Area	Select the area you want to delete, and then click this button to delete it.
Starting Point X/Y	Select an area to show its coordinates. You can modify the area by changing the coordinates. ● The coordinates that you can input are subject to the screen size.
Area Width/Height	Select an area to show its width and height. You can change the width and height of the area manually. ● The coordinates that you can input are subject to the screen size.
Scroll Mode	Four options: **Single Line**: Displays one line; the extra part will not be displayed. **Single Line&Scroll Left**: Displays one line, and will scroll from right to left to display the extra part. **Not Auto Wrap in Multiple Lines**: Displays multiple lines without wrapping automatically. **Auto Wrap in Multiple Lines**: Displays multiple lines and wraps automatically (recommended)
Text Alignment	Keep center aligned.
Font Size	Choose the desired font size.
Font Color	Choose the desired font color.
Date Format	Choose the desired date format.
Time Format	Choose the desired time format.

Parameter	Description
Automatically released fields	
System Time	Click to display the system time in the current area.
System Date	Click to display the system date in the current area.

4.6.3 Configure Vehicle Pass-thru Info Release

1. Configure vehicle pass-thru info release. The page is as shown below.



Message Info | Vehicle Pass-thr... | Violation Info

Enable ☐ New Target Keep... 5 Display last chara... ☐ Always Display V... ☐

Area Config:

Add Area | Delete ...

Start P... 0 Start P... 0

Area ... 0 Area ... 0

Scroll ... Single Lin Text A...

Font S... 16 Font C...

Date F... yyyy-MM- Time F... hh:mm:ss

Auto Releas...

Vehicle P... | Vehicle P... | Plate Nu... | Vehicle S... | Lane No. | Speed Limit | Vehicle C... | Location | Image

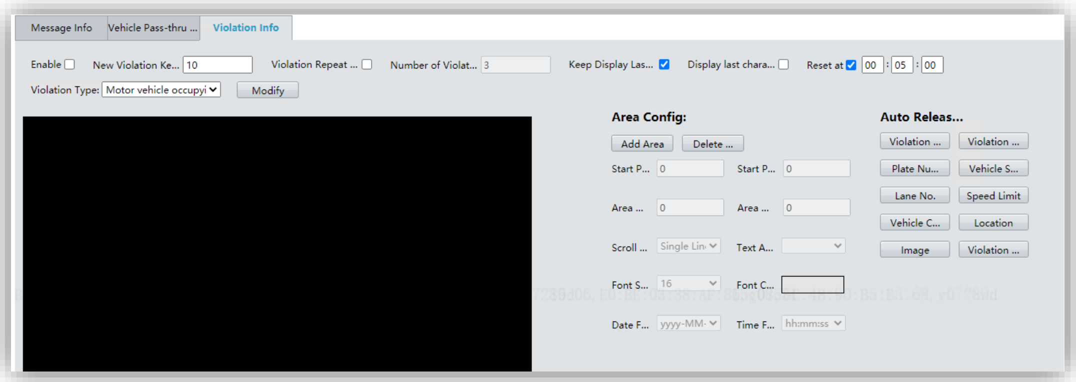
Save

- Configure the parameters by referring to the table below.

Parameter	Description
Enable	Select the checkbox to enable releasing passing vehicle info.
New Target Keeptime (s)	The length of time that each passing vehicle will be displayed on the screen, if there's no violation vehicle info. If there are new violation vehicles, violation vehicle info will be released first.
Display last character of plate number as *	Displays the last character of the license plate as *.
Always Display Vehicle Pass-thru	Continues to displaying the last passing vehicle if there are no other passing vehicles.
Area Config	See descriptions of area configuration in Configure Message Info Release.
Auto Release Field	Choose the fields to be released automatically. Text fields: time of passing vehicle, date of passing vehicle, plate number, vehicle speed, lane ID, speed limit, vehicle body color, location, direction. Image fields: Release images of passing vehicles.

4.6.4 Configure Violation Information Release

1. Configure violation information. The page is as shown below.



Enable □ New Violation Ke... 10 Violation Repeat ... □ Number of Violat... 3 Keep Display Las... ☑ Display last chara... □ Reset at ☑ 00 : 05 : 00

Violation Type: Motor vehicle occupyi

Start P... 0 Start P... 0

Area ... 0 Area ... 0

Scroll ... Single Lin Text A...

Font S... 16 Font C...

Date F... yyyy-MM- Time F... hh:mm:ss

- Configure the parameters by referring to the table below.

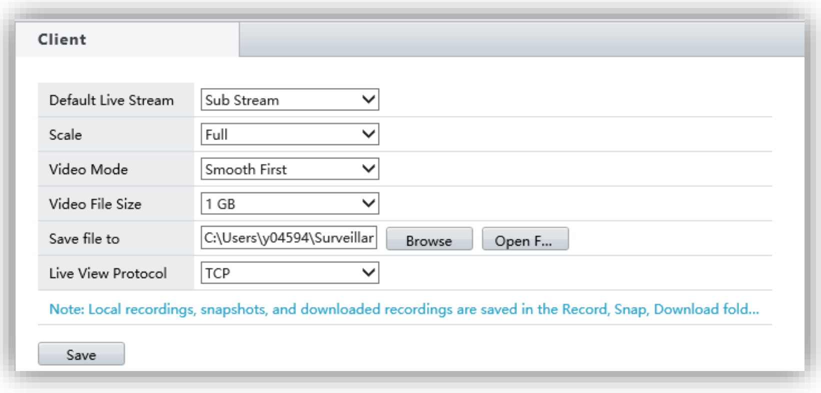
Parameter	Description
Enable	Select the checkbox to enable releasing violation info.
New Violation Keeptime (s)	Length of time that violation info will be released.
Violation Repeat Display Number of Violation Repeat Displays	When selected, the corresponding number of latest violation records will be displayed. For example, if the number is set to 5, then the five latest violation records will be displayed. Passing vehicle information and message info will not be displayed.
Keep Display Last Violation	When selected, only the latest violation record will be displayed. This parameter and **Violation Repeat Display** cannot be enabled at the same time.
Display last character of violation plate number as *	When selected, the last character of the license plate will be displayed as *; otherwise, the complete license plate will be displayed.
Reset at	When configured, the displayed contents will be cleared regularly according to the set time. If releasing message info is disabled, the screen will remain blank until there is new passing vehicle or violation data.
Violation Type and Modification	1) Click the **Modify** button to display violation types. After you select a violation type, violations of the corresponding type will be displayed on the screen. Otherwise, violations of the corresponding type will not be displayed. Up to 12 violation types can be selected. 2) You can click the drop-down list to view the selected violation types.
Area Config	See descriptions of area configuration in Configure Message Info Release.

Parameter	Description
Auto Release Field	Choose the fields to be released automatically. Text fields: violation time, violation date, plate number, vehicle speed, lane ID, speed limit, car body color, location, direction, violation type. Image fields: Release images of passing vehicles.

5 Setup

5.1 Local Settings

1. Go to **Setup** > **Local Config**. The page is as shown below.



Default Live Stream	Sub Stream
Scale	Full
Video Mode	Smooth First
Video File Size	1 GB
Save file to	C:\Users\y04594\Surveillar
Live View Protocol	TCP

Note: Local recordings, snapshots, and downloaded recordings are saved in the Record, Snap, Download fold...

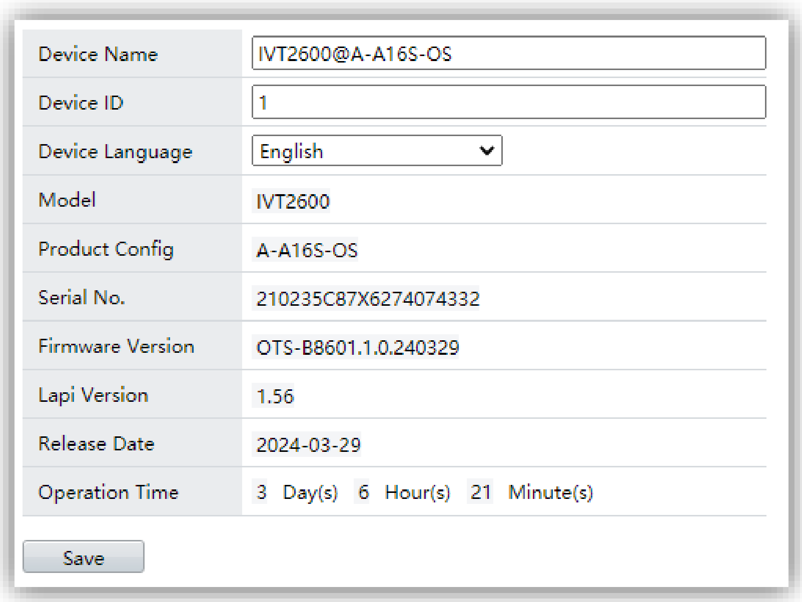
- Configure the parameters by referring to the table below.

Parameter	Description
Default Live Stream	Choose the main stream or the sub stream as the default live video stream.
Display Ratio	Choose the video display mode in the live view window: **Original** or **Full**.
Video Mode	Choose **Fluency Priority** or **Real Time Priority**.
Video File Size	The maximum size of a local recording file. If the size is set to 1GB, when the recording size exceeds 1GB, another recording file will be created.
Save File To	Path to save snapshots and recordings. ● Click **Browse** to browse the computer and specify the storage location. ● Click **Open Folder** to access the folder containing the saved files.
Live View Protocol	Protocol used to transport media streams to the client. Choose **TCP** or **UDP**.

5.2 System Configuration

5.2.1 Basic Configuration

1. Go to **Setup** > **System** > **Basic Config** to view the basic information of the device. No configuration is required on the page.

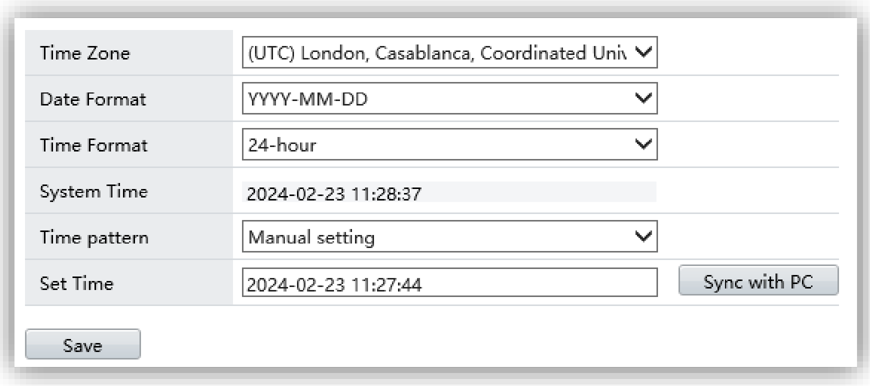


Device Name	IVT2600@A-A16S-OS
Device ID	1
Device Language	English
Model	IVT2600
Product Config	A-A16S-OS
Serial No.	210235C87X6274074332
Firmware Version	OTS-B8601.1.0.240329
Lapi Version	1.56
Release Date	2024-03-29
Operation Time	3 Day(s) 6 Hour(s) 21 Minute(s)

5.2.2 Time Configuration

1. Time Configuration

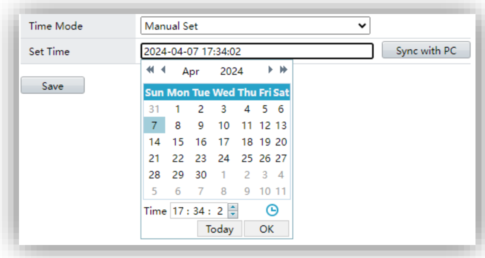
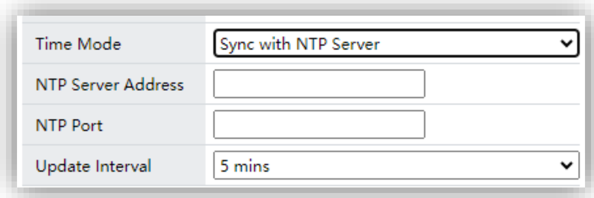
1. Go to **Setup** > **System** > **Time** > **Time**. The page is as shown below.



Time Zone	(UTC) London, Casablanca, Coordinated Univ	
Date Format	YYYY-MM-DD	
Time Format	24-hour	
System Time	2024-02-23 11:28:37	
Time pattern	Manual setting	
Set Time	2024-02-23 11:27:44	Sync with PC

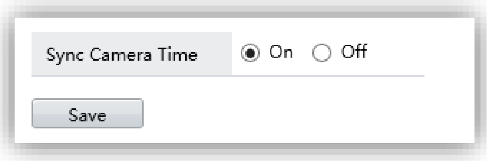
- Configure the parameters by referring to the table below.

Parameter	Description
Time Zone	Choose your local time zone.
Date Format	Choose a date format.
Time Format	Choose a time format.

Parameter	Description
System Time	Configure the device’s system time.
Time Mode/Set Time	Three options: **Set Manually**: You can enter the time manually, or click **Sync with PC** to synchronize the device’s system time with that of the PC.  Time Mode: Manual Set Set Time: 2024-04-07 17:34:02 Time 17 : 34 : 2 Sync with PC Save Apr 2024 Sun Mon Tue Wed Thu Fri Sat Today OK **Sync with NTP Server:** Sync time with the NTP server.  Time Mode: Sync with NTP Server NTP Server Address: NTP Port: Update Interval: 5 mins ● **NTP Server Address:** Enter the NTP server address. ● **NTP Port**: Enter the NTP server port, which usually is 123. ● **Update Interval:** Interval for updating time. For example, if you set it to 5 minutes, the device will perform time synchronization with the NTP server every 5 minutes. GPS Time Sync: Currently not applicable and can be ignored.

2. Time Sync

1. The time sync page is as shown below.



Sync Camera Time: ◉ On ○ Off

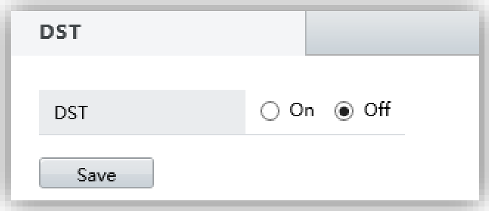
- Configure the parameters by referring to the table below.

Parameter	Description
Sync Camera Time	Sync the device’s time to the connected cameras to keep the camera time consistent with that of the device. ● Uniview/ONVIF: The device syncs time to cameras connected via UNV or Onvif when the function is enabled; it then

Parameter	Description
	continues to sync time regularly every 30 minutes until this function is disabled. Additionally, the device will sync time when cameras are added or go online. ● GB: The device will sync time only when the function is enabled or when cameras are added or go online. ● For cameras connected via Onvif and other protocols, you need to choose **Sync with Management Platform** (Onvif) and **Sync with Management Platform** (non-Onvif) on the camera side, respectively (**Settings** > **System** > **Time**). ● If the camera side is configured to sync with an NTP server, then it is unnecessary to enable **Sync Camera Time** on the device (IVT-2600).

5.2.3 Daylight Saving Time (DST)

1. Some regions adopt daylight saving time (DST). To enable DST, select **On**.



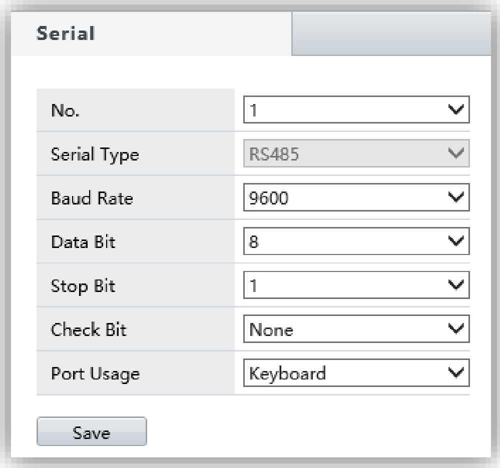
DST

DST ○ On ● Off

2. Click **Save** when you complete the configuration.

5.2.4 Serial Port Configuration

1. Go to **Setup** > **System** > **Serial**. The page is as shown below.



Serial

No.	1
Serial Type	RS485
Baud Rate	9600
Data Bit	8
Stop Bit	1
Check Bit	None
Port Usage	Keyboard

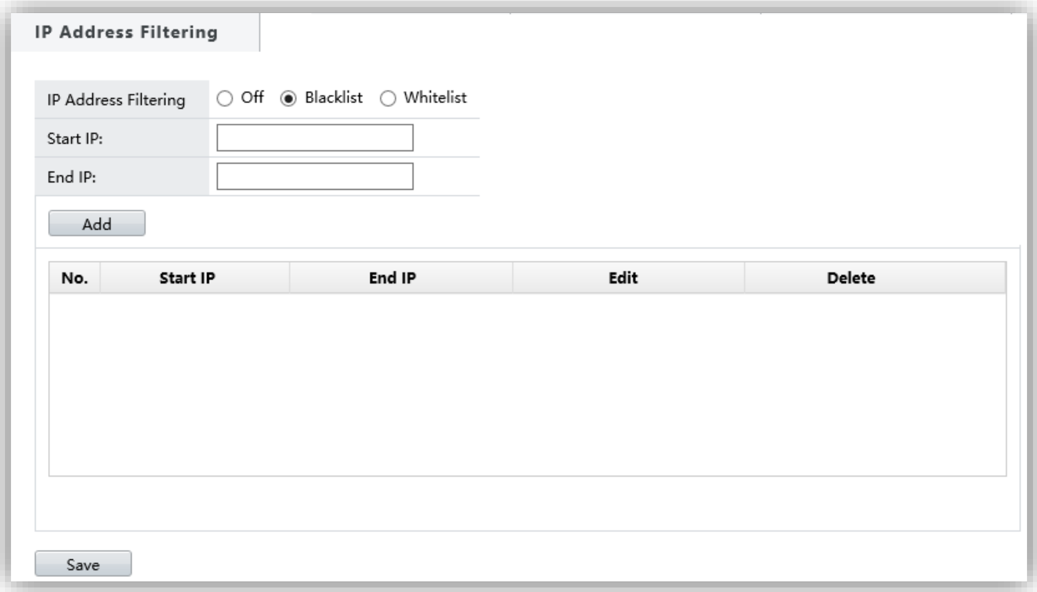
- Configure the parameters by referring to the table below.

Parameter	Description
Serial Port No.	Serial port ID. You may configure two.
Serial Type	Fixed to RS485.
Baud Rate	Data transmission speed (bits per second). The higher the value, the faster the transmission speed, and the shorter the transmission distance. It is recommended to use the default value.
Data Bit	The number of data bits (in bits) actually contained in a group of data packets. It is recommended to use the default value.
Stop Bit	Indicates the end of a data transmission. It is recommended to use the default value.
Check Bit	Used to check whether the received data bits are erroneous. You may choose **Odd** or **Even**.
Port Usage	Fixed to **Keyboard**.

5.2.5 Security Configuration

1. IP Address Filtering

1. Use IP address filtering to forbid or allow certain PCs to access the device. Go to **Setup** > **System** > **Security** > **IP Address Filtering**. The page is as shown below.



IP Address Filtering	○ Off ● Blacklist ○ Whitelist
Start IP:	
End IP:	

No.	Start IP	End IP	Edit	Delete

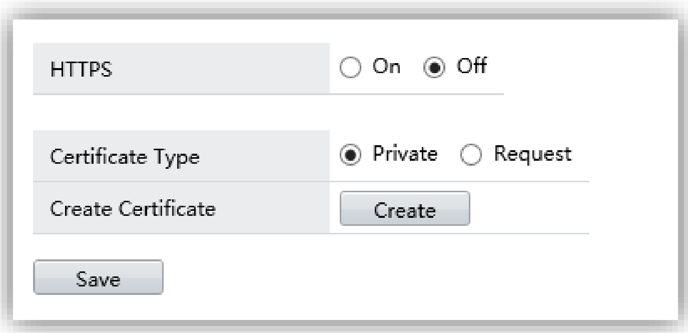
- Configure the parameters by referring to the table below.

Parameter	Description
IP Address Filtering	Choose a filtering mode: Off: Any PC can have access to the device (if network connection is normal).

Parameter	Description
	Blocklist: Add malicious IP addresses to the blocklist. PCs with IP addresses on the blocklist will be prohibited from accessing the device. Allowlist: Add trusted IP addresses to the allowlist. Only PCs with IP addresses on the allowlist will be allowed to access the device.
Start IP and End IP	Specifies the IP address range that is allowed or prohibited to access the device. For example: The start IP is 192.168.0.8, the end IP is 192.168.0.9, and the IP address filtering mode is set to allowlist, then only PCs with 192.168.0.8 and 192.168.0.9 have access to the device; PCs will other IP addresses have no access to the device.
Add	Set the start IP and end IP, and then click **Add** to add the IP range to the IP address filtering list.

2. HTTPS

1. HTTPS added SSL (Secure Socket Layer) to HTTP to enhance the security of information transmission through encryption and authentication.



HTTPS ○ On ● Off

Certificate Type ● Private ○ Request

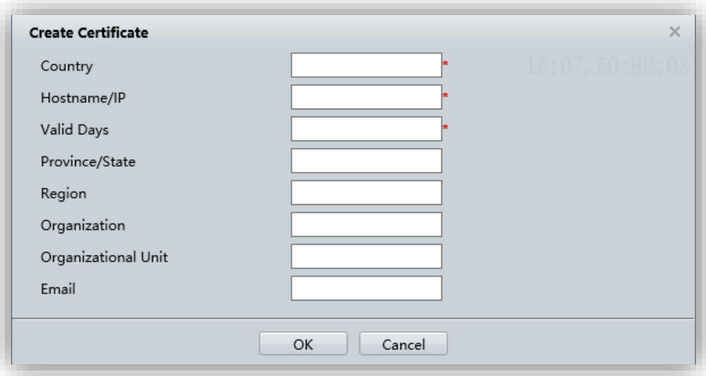
Create Certificate

- Configure the parameters by referring to the table below.

Parameter	Description
HTTPS	Click **On** to enable HTTPS.
Certificate Type	Choose a certificate type: Private certificate: Click Create to create a certificate that will be used for HTTPS request. Request: Import the signed certificate for HTTPS request.

2. A certificate is a digital file that uniquely represents an individual and a resource on the Internet. It enables secure and confidential communication between two entities. You can either create a self-signed certificate or import an existing certificate.

● Create a self-signed certificate: Suitable for low security scenes. A self-signed certificate is issued by an untrusted Certificate Authority (CA). It is usually created, issued, and signed by a company or a software developer.



Create Certificate

Country *

Hostname/IP *

Valid Days *

Province/State

Region

Organization

Organizational Unit

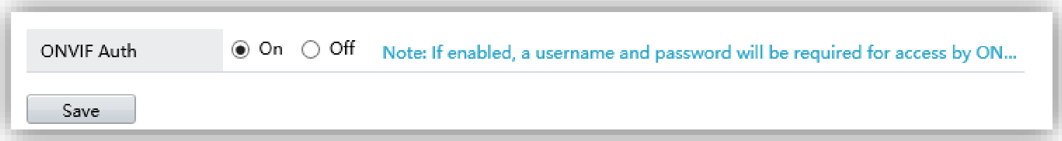
Email

- Configure the parameters by referring to the table below.

Parameter	Description
Country	Enter the two-character country code, for example, CN for China.
Hostname/IP	Enter the device's IP address or domain name.
Province/State	Enter the complete province name.
Region	Enter the complete city name.
Organization	Enter the organization name.
Organizational Unit	Enter the unit name.
Email	Enter a valid email address of the contact.

3. ONVIF Authentication

1. To enable authentication for Onvif access to the device, go to **Setup** > **System** > **Security** > **ONVIF Auth**. The page is as shown below.



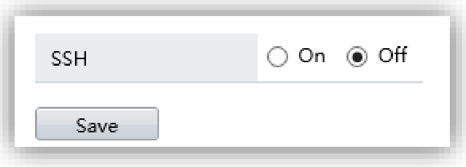
ONVIF Auth ● On ○ Off Note: If enabled, a username and password will be required for access by ON...

- Configure the parameters by referring to the table below.

Parameter	Description
ONVIF Auth	When enabled, a username and password will be required for access by Onvif.

4. SSH

1. SSH is used to enable or disable background debugging. It is recommended to keep the default setting.



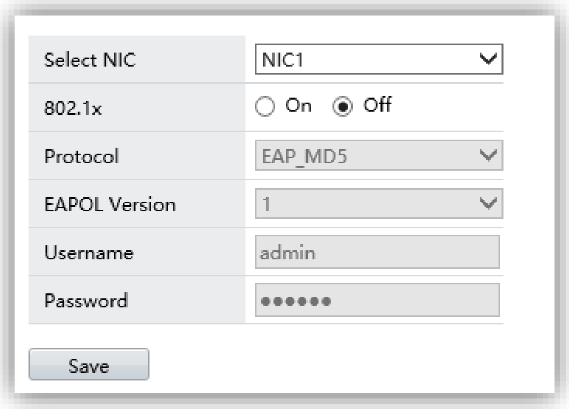
SSH	○ On ● Off

5. 802.1x

NOTE!

802.1x is an access control protocol used when devices connect to a switch-based network. In environments with high security requirements, devices need to undergo access authentication and control when connecting to the network. The 802.1x protocol can enhance network security by allowing only the authenticated devices to access the network.

1. Go to **Setup** > **System** > **Security** > **802.1x**. The page is as shown below.



Select NIC	NIC1
802.1x	○ On ● Off
Protocol	EAP_MD5
EAPOL Version	1
Username	admin
Password	••••••

2. Click **On** to enable 802.1x.

3. Choose a protocol type. The device must pass the authentication via the specified protocol before it can communicate with the network.

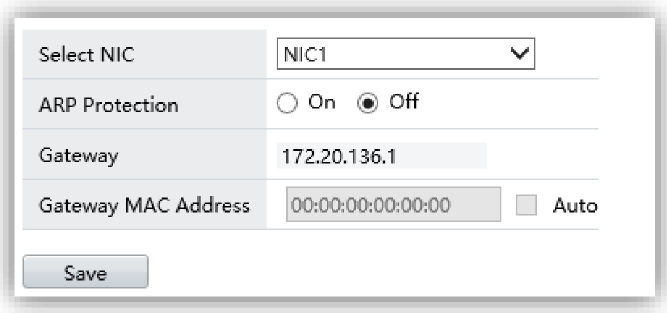
- Choose EAPOL version in accordance with the protocol version on the network switch (EAP overLANs).
- Enter the username and password of the device, and confirm the password.

6. ARP Protection

NOTE!

ARP attacks are carried out by spoofing IP and MAC addresses to manipulate the Address Resolution Protocol (ARP). These attacks primarily occur within local area networks (LANs). Configure APR protection so that the device will verify the physical address of the source of requests, thereby protecting itself from ARP spoofing attacks.

1. Go to **Setup** > **System** > **Security** > **ARP Protection**. The page is as shown below.



Select NIC	NIC1
ARP Protection	○ On ● Off
Gateway	172.20.136.1
Gateway MAC Address	00:00:00:00:00:00 □ Auto

2. Choose a network card, and then click **On** to enable this function.
3. Enter the gateway's physical address (MAC address).
4. Click **Save** when you complete the configuration.

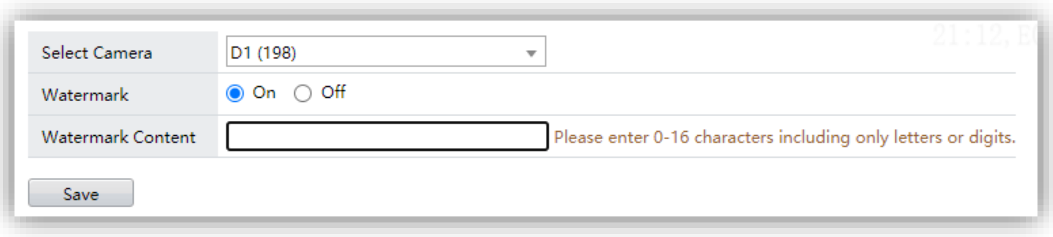
7. Watermark

Use watermark to embed custom encryption information in video contents to prevent video tampering.

NOTE!

- Currently this function is available only to cameras added via the private protocol. It is not available to cameras added via Onvif and GB28181.
- To view the watermark content, you need to download EZPlayer from Uniview official website.

1. Go to **Setup** > **System** > **Security** > **Watermark**.



Select Camera	D1 (198)
Watermark	● On ○ Off
Watermark Content	Please enter 0-16 characters including only letters or digits.

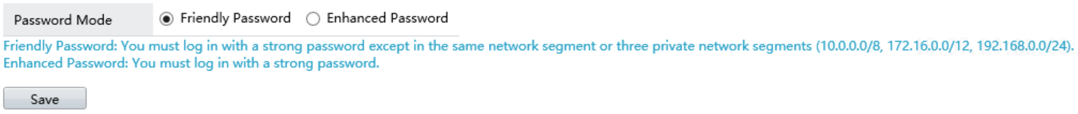
2. Select the camera for which you want to enable watermark, and enable watermark.
3. Enter the watermark content.
4. Click **Save** when you complete the configuration.

8. Password Mode

NOTE!

Weak passwords are not allowed in enhanced password mode. Likewise, you cannot switch to enhanced password mode if the current password is weak.

1. Go to **Setup** > **System** > **Security** > **Password Mode**. The page is as shown below.


Password Mode ● Friendly Password ○ Enhanced Password

Friendly Password: You must log in with a strong password except in the same network segment or three private network segments (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24).
Enhanced Password: You must log in with a strong password.

- Configure the parameters by referring to the table below.

Parameter	Description
Friendly Password	A strong password is required except when the PC client is in the same network segment as the NVR or in one of the three private network segments (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24).
Enhanced Password	A strong password is required in all conditions.

5.3 Network Configuration

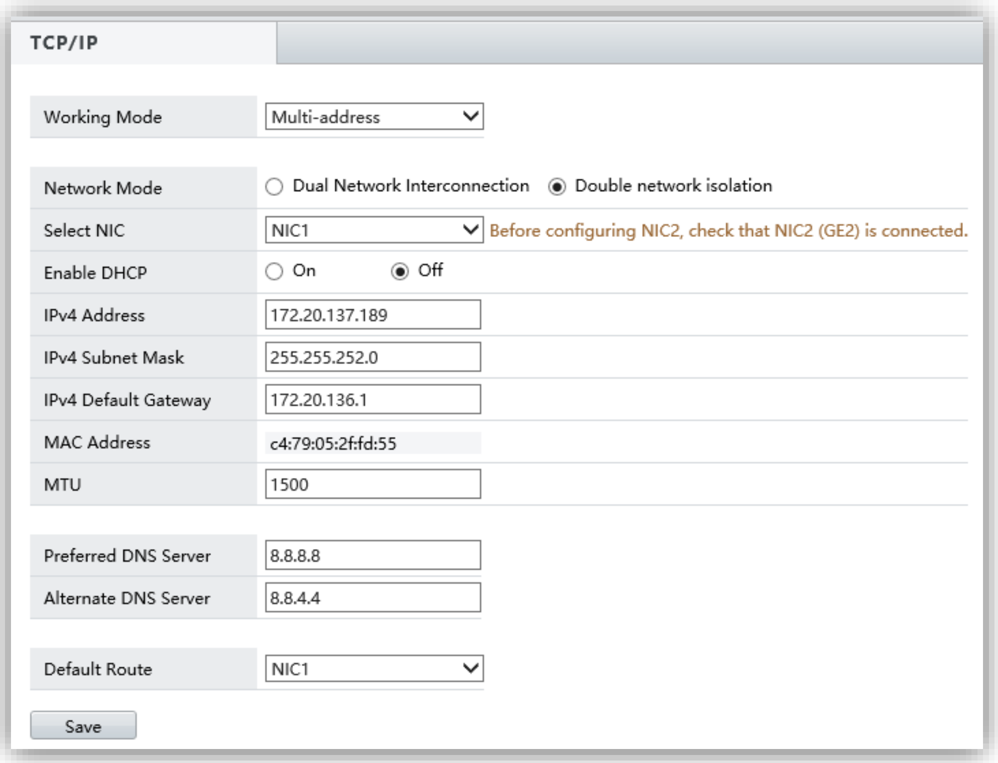
5.3.1 TCP/IP

NOTE!

Dual network isolation refers to the dual-IP mode; dual network interconnection refers to the single-IP mode.

1. IPv4 Settings

1. Go to **Setup** > **Network** > **TCP/IP**. The page is as shown below.



TCP/IP

Working Mode	Multi-address
Network Mode	○ Dual Network Interconnection ● Double network isolation
Select NIC	NIC1 Before configuring NIC2, check that NIC2 (GE2) is connected.
Enable DHCP	○ On ● Off
IPv4 Address	172.20.137.189
IPv4 Subnet Mask	255.255.252.0
IPv4 Default Gateway	172.20.136.1
MAC Address	c4:79:05:2f:fd:55
MTU	1500
Preferred DNS Server	8.8.8.8
Alternate DNS Server	8.8.4.4
Default Route	NIC1

A. Select **Dual Network Interconnection**, and then choose the corresponding network interface. Take NIC1 as an example.

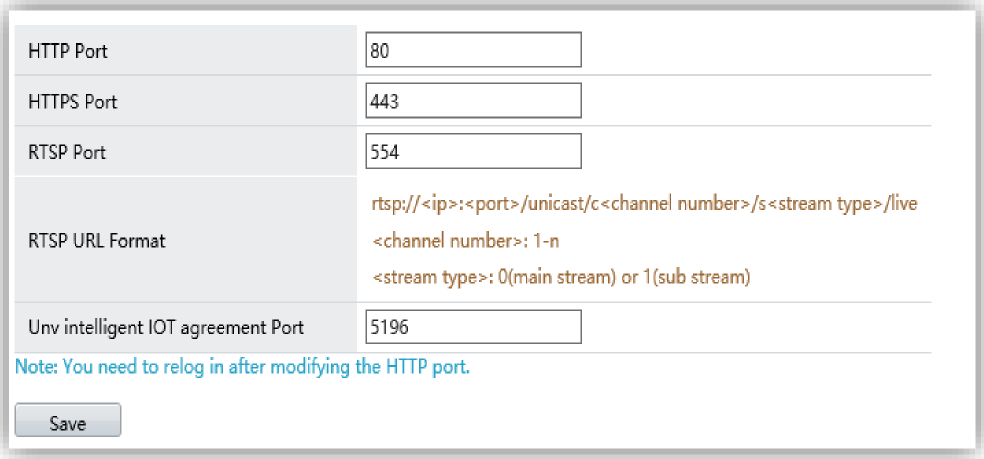
B. Disable DHCP, and then configure IPv4 address, subnet mask, and default gateway. Make sure that the IPv4 address is unique on the network.

C. Keep the default settings for other parameters.

5.3.2 Port

NOTE!

- If the HTTP port conflicts, a message indicating “Port conflict. Please reenter.” will appear.
- The following ports are reserved for special purposes and are not allowed: 23, 81, 82, 85, 3260, 49152.



HTTP Port	80
HTTPS Port	443
RTSP Port	554
RTSP URL Format	rtsp://<ip>:<port>/unicast/c<channel number>/s<stream type>/live <channel number>: 1-n <stream type>: 0(main stream) or 1(sub stream)
Unv intelligent IOT agreement Port	5196

Note: You need to relog in after modifying the HTTP port.

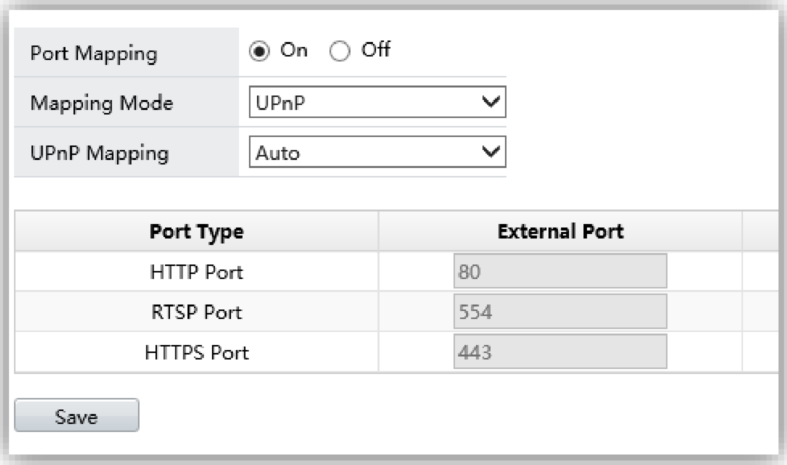
1. Go to **Setup** > **Network** > **Port** to configure ports.
2. Use the default settings. If a port entered is already in use, try another port.
   - HTTP port and HTTPS port: After changing these two ports, you need to append the new port to the address entered in the address bar when logging in using a web browser. For example: If the HTTP port has been changed to 88, you need to enter http://192.168.1.30:88.
   - RTSP port: Multimedia streaming port. Set a usable port.

3. Click **Save** to when you complete the configuration.

5.3.3 Port Mapping

The device is usually connected to the LAN port of the router. If the device is on the LAN and it is necessary to access the device from the Internet, port mapping is required.

1. Go to **Setup** > **Network** > **Port Mapping**, select **On** to enable port mapping.
2. Choose a mapping mode.
   - UPnP



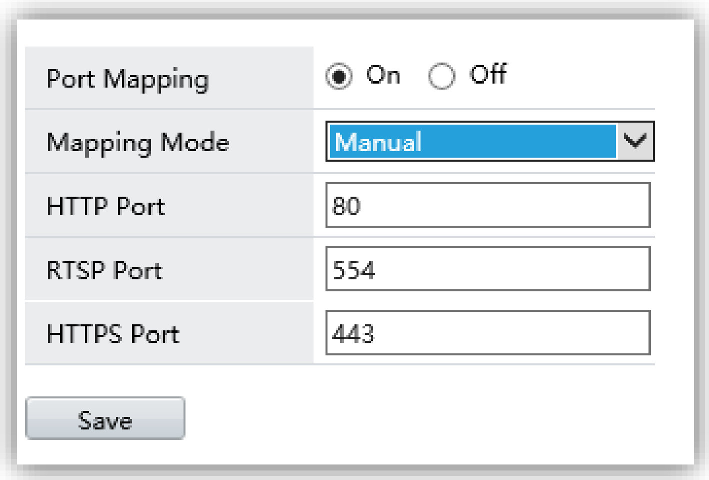
Port Mapping	● On ○ Off
Mapping Mode	UPnP
UPnP Mapping	Auto

Port Type	External Port
HTTP Port	80
RTSP Port	554
HTTPS Port	443

➢ Auto: The device automatically negotiates ports with the router, and when UPnP is enabled on the router, ports are opened to enable communication between the intranet and the external network. When disabled, the NAT gateway releases the ports. If a port is occupied, the device will automatically try another port to initiate the mapping request to ensure that the port is available.

- ➢ Specify port: When specifying a port, it is important to ensure that the specified port is available, otherwise, the mapping will not take effect. The NAT gateway opens a fixed port, and the mapping relationship always exists regardless of whether the connection is present. Simply fill in the mapping port number to open the port.

- Manual



Port Mapping ● On ○ Off

Mapping Mode: Manual

HTTP Port: 80

RTSP Port: 554

HTTPS Port: 443

➢ The device automatically acquires the external IP, configures and fills in the external port.

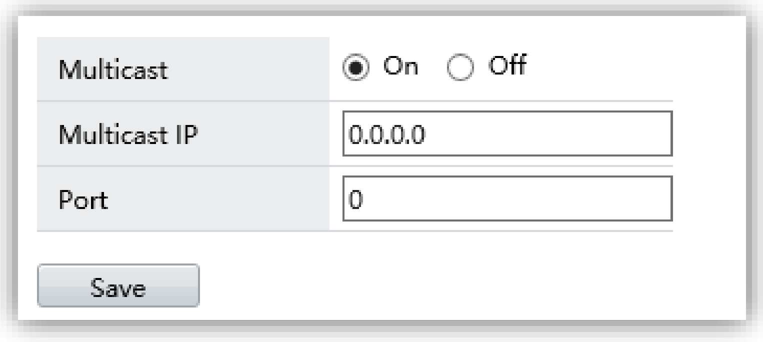
➢ If the configured external port is already in use, the **Status** column will indicate that the port mapping is not effective.

4. Click **Save** when you complete the configuration.

5.3.4 Multicast

After multicast is configured, third-party players can request the camera to send RTP multicast media streams through the RTSP protocol.

1. Go to **Setup** > **Network** > **Multicast**, select **On** to enable multicast.



Multicast ● On ○ Off

Multicast IP: 0.0.0.0

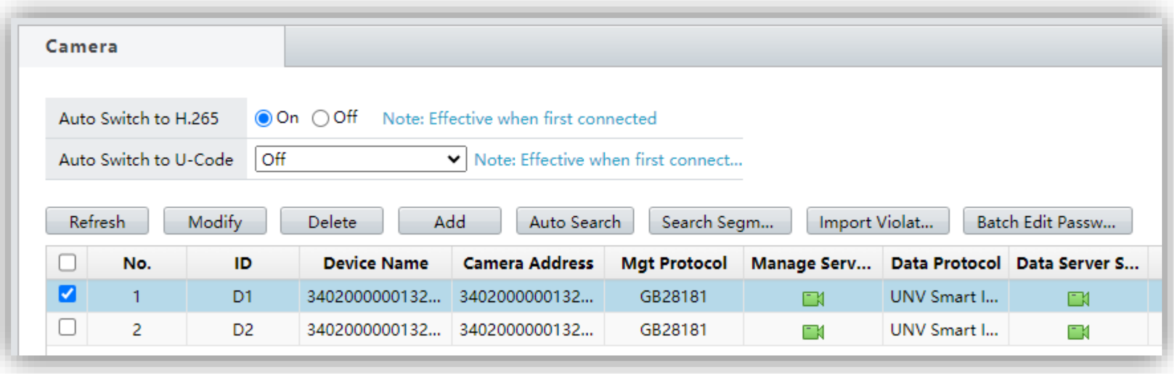
Port: 0

2. Set the multicast address and port number (the multicast address range is 224.0.1.0-239.255.255.255, and the port number range is 0-65535).
3. Click **Save** when you complete the configuration.

5.4 Camera Configuration

5.4.1 IPC Configuration

1. Go to **Setup** > **Camera Config** > **Camera**. The page is as shown below.



Camera

Auto Switch to H.265 ● On ○ Off Note: Effective when first connected

Auto Switch to U-Code Off Note: Effective when first connect...

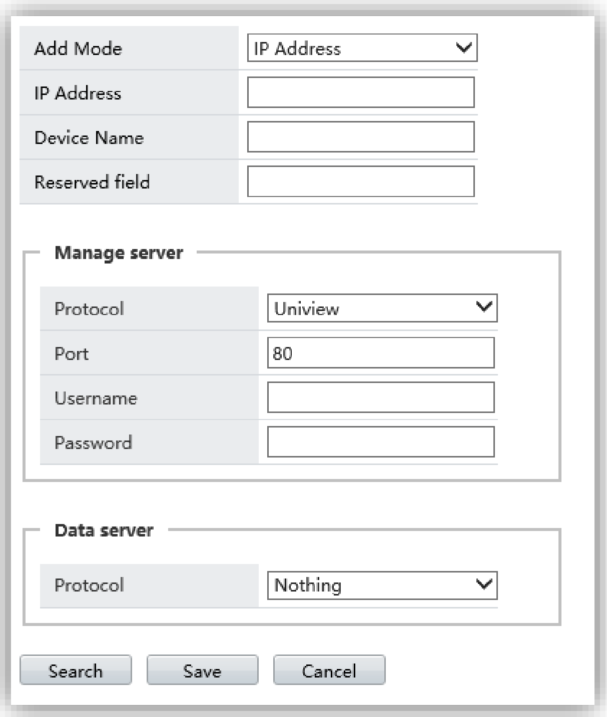
Refresh | Modify | Delete | Add | Auto Search | Search Segm... | Import Violat... | Batch Edit Passw...

☐	No.	ID	Device Name	Camera Address	Mgt Protocol	Manage Serv...	Data Protocol	Data Server S...
☑	1	D1	3402000000132...	3402000000132...	GB28181	📹	UNV Smart I...	📹
☐	2	D2	3402000000132...	3402000000132...	GB28181	📹	UNV Smart I...	📹

- Configure the parameters by referring to the table below.

Parameter	Description
Auto Switch to H.265	This function is disabled by default. When enabled, the camera will automatically switch the compression format to H.265 when connected for the first time.
Auto Switch to U-Code	Consistent with the default setting on the camera.~~Keep the default setting.~~ Remarks: U-Code utilizes deep encoding optimization technology to achieve extreme compression while ensuring video quality. With U-Code, it is possible to watch high-definition videos with 1 Mbps bitrate. It boasts four key highlights: low bitrate, high image quality, ease of use, and compatibility.
Refresh	Click to refresh the list.
Modify	Modify the parameters of the selected camera.
Delete	Delete the selected cameras.
Add	Click to add a camera manually. See Add.
Auto Search	Click to discover cameras on the LAN. See Auto Search.
Search Segment	Click to discover cameras on a specified network segment. See Auto Search.
Import Violation Sign Image	If a violation sign image is configured in image composition, this configuration can be used to import the violation sign image and add it to composition images. It is not recommended to configure this parameter.

- How to add cameras



Add Mode	IP Address
IP Address	
Device Name	
Reserved field	

Manage server

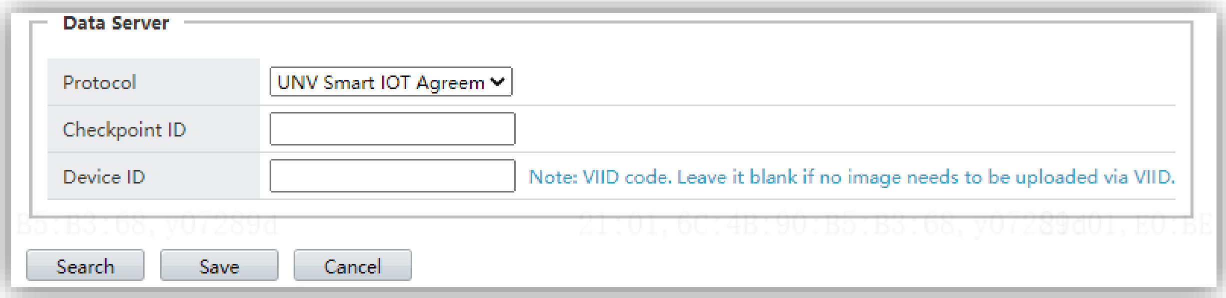
Protocol	Uniview
Port	80
Username	
Password	

Data server

Protocol	Nothing

1. In the IP Address field, enter the camera's IP address.
2. In the Device Name field, enter a device name for the camera.
3. Choose a protocol.
   - Uniview
     1. Enter the port number. The default is 80.
     2. Configure the username and password (username/password used to log in to the camera).
   - GB28281
     1. Set the channel ID, which should be consistent with the device ID configured on the management server.
     2. Choose TCP or UDP as the transport protocol.
     3. Enter the password. The password should be consistent with the password configured on the management server.
   - ONVIF
     1. Enter the port number. The default is 80.
     2. Configure the username and password (username/password used to log in to the camera).

4. Choose the data server.



Data Server

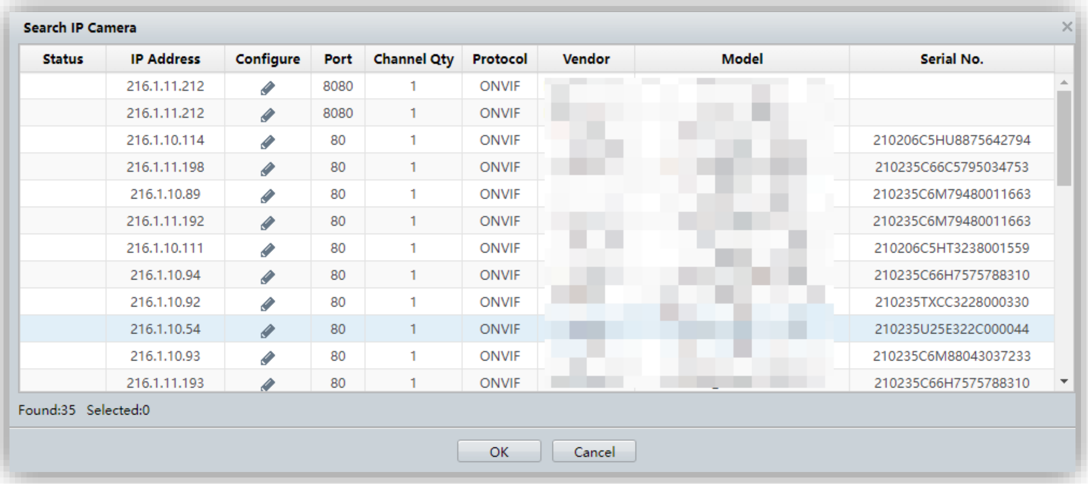
Protocol	UNV Smart IOT Agreem
Checkpoint ID	
Device ID	

Note: VIID code. Leave it blank if no image needs to be uploaded via VIID.

- IMOS
  1. Set the checkpoint code, which should be consistent with the checkpoint ID configured on the camera's photo server.
  2. Device ID needs no configuration.
- LAPI
  1. Configure the device code, which should be consistent with the camera.

5. Click **Save** to add the camera.

- Auto Search

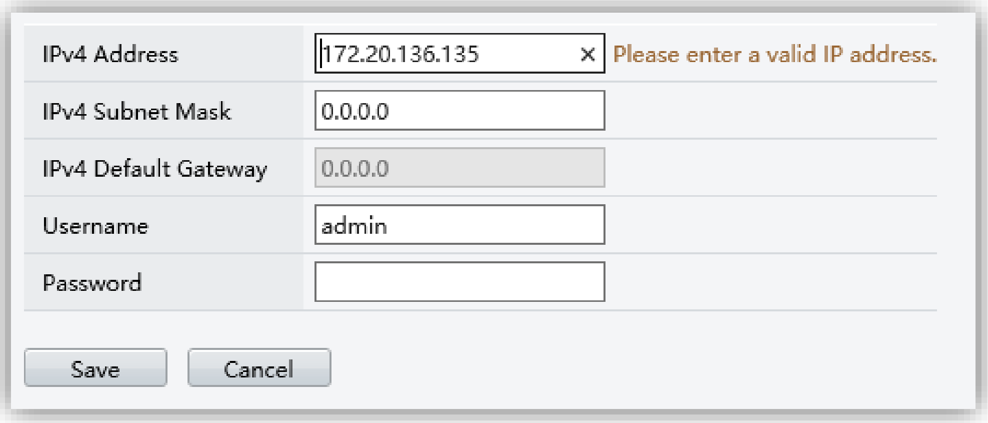


Search IP Camera

Status	IP Address	Configure	Port	Channel Qty	Protocol	Vendor	Model	Serial No.
	216.1.11.212	✎	8080	1	ONVIF	[redacted]	[redacted]	
	216.1.11.212	✎	8080	1	ONVIF	[redacted]	[redacted]	
	216.1.10.114	✎	80	1	ONVIF	[redacted]	[redacted]	210206C5HU8875642794
	216.1.11.198	✎	80	1	ONVIF	[redacted]	[redacted]	210235C66C5795034753
	216.1.10.89	✎	80	1	ONVIF	[redacted]	[redacted]	210235C6M79480011663
	216.1.11.192	✎	80	1	ONVIF	[redacted]	[redacted]	210235C6M79480011663
	216.1.10.111	✎	80	1	ONVIF	[redacted]	[redacted]	210206C5HT3238001559
	216.1.10.94	✎	80	1	ONVIF	[redacted]	[redacted]	210235C66H7575788310
	216.1.10.92	✎	80	1	ONVIF	[redacted]	[redacted]	210235TXCC3228000330
	216.1.10.54	✎	80	1	ONVIF	[redacted]	[redacted]	210235U25E322C000044
	216.1.10.93	✎	80	1	ONVIF	[redacted]	[redacted]	210235C6M88043037233
	216.1.11.193	✎	80	1	ONVIF	[redacted]	[redacted]	210235C66H7575788310

Found:35 Selected:0

1. Select the camera you want to add, and then click ✎ to edit camera information.

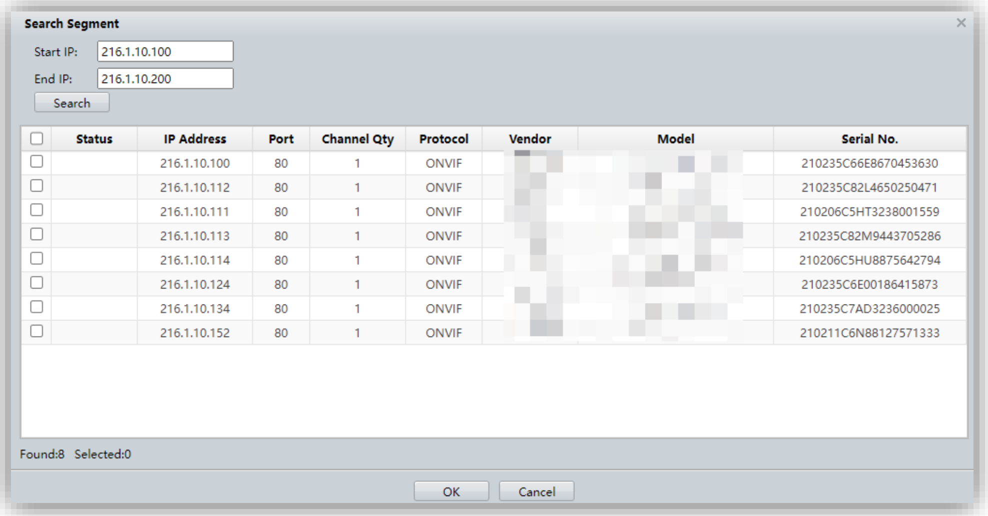


IPv4 Address	172.20.136.135 ✕ Please enter a valid IP address.
IPv4 Subnet Mask	0.0.0.0
IPv4 Default Gateway	0.0.0.0
Username	admin
Password	

- Enter the subnet mask. Enter the username and password that are used to log in to the camera.

2. Click **Save** when you complete the configuration.
3. Select the checkbox for the camera you just edited, and then click **OK** to add the camera.

- Search Segment



Search Segment

Start IP: 216.1.10.100

End IP: 216.1.10.200

□	Status	IP Address	Port	Channel Qty	Protocol	Vendor	Model	Serial No.
□		216.1.10.100	80	1	ONVIF	[redacted]	[redacted]	210235C66E8670453630
□		216.1.10.112	80	1	ONVIF	[redacted]	[redacted]	210235C82L4650250471
□		216.1.10.111	80	1	ONVIF	[redacted]	[redacted]	210206C5HT3238001559
□		216.1.10.113	80	1	ONVIF	[redacted]	[redacted]	210235C82M9443705286
□		216.1.10.114	80	1	ONVIF	[redacted]	[redacted]	210206C5HU8875642794
□		216.1.10.124	80	1	ONVIF	[redacted]	[redacted]	210235C6E00186415873
□		216.1.10.134	80	1	ONVIF	[redacted]	[redacted]	210235C7AD3236000025
□		216.1.10.152	80	1	ONVIF	[redacted]	[redacted]	210211C6N88127571333

Found:8 Selected:0

1. Set the network segment you want to search, and then click **Search**.

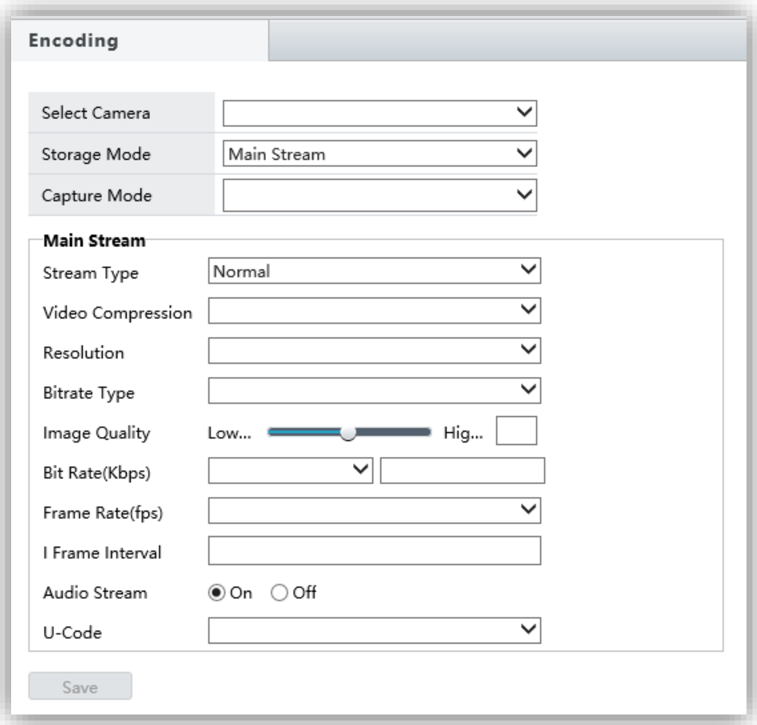
2. Select the cameras to add, and then click **OK** to add the camera. If a camera is offline, click the **Modify** button for the camera to change the username and password.

5.4.2 Encoding Parameters

NOTE!

The encoding parameters configured on the NVR will be synced to the camera.

1. Go to **Setup** > **Camera Config** > **Encoding**.



Encoding

Select Camera	
Storage Mode	Main Stream
Capture Mode	

Main Stream

Stream Type	Normal
Video Compression	
Resolution	
Bitrate Type	
Image Quality	Low... Hig...
Bit Rate(Kbps)	
Frame Rate(fps)	
I Frame Interval	
Audio Stream	● On ○ Off
U-Code	

- Configure the parameters by referring to the table below.

Parameter	Description
Select Camera	Choose the camera to configure.
Storage Mode	Choose main stream or sub stream.
Main stream (take the main stream as an example; the sub stream is similar)	
Stream Type	Keep the default setting.
Video Compression	Choose H.264 or H.265. Usually the default setting is applicable.
Resolution	Choose camera resolution. Usually the default setting is applicable.
Image Quality	Keep the default setting.
Bit Rate	Keep the default setting.
Frame Rate	Keep the default setting.
I Frame Interval	The larger the I-frame interval, the less noticeable the breathing effect becomes. It is recommended to keep the default setting.
Audio Stream	Not applicable to traffic cameras. Please ignore this parameter.

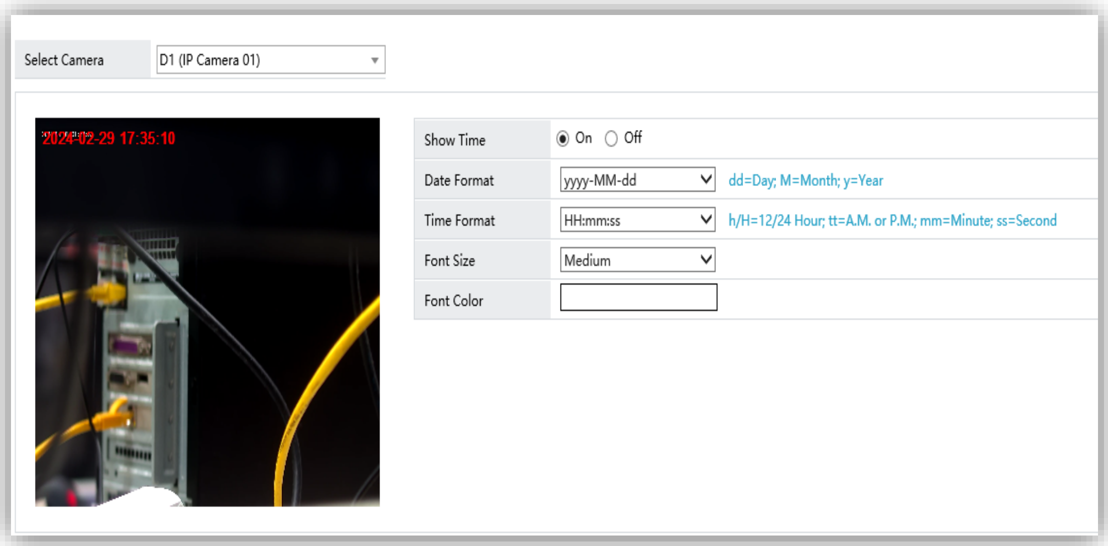
5.4.3 OSD Configuration

NOTE!

The OSD configured on the NVR will be synced to the camera.

1. To configure live view OSD, go to **Setup** > **Camera Config** > **Basic**.

- OSD Configuration



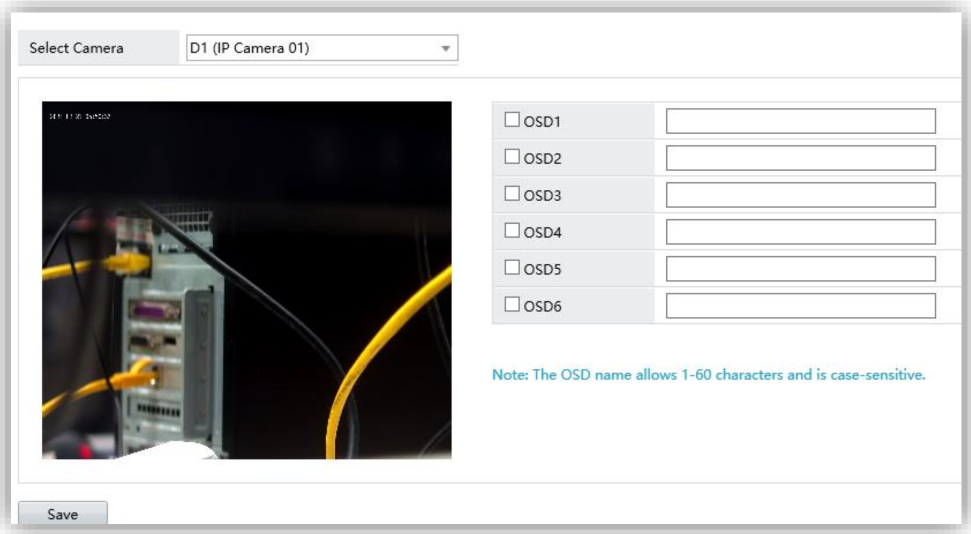
Select Camera	D1 (IP Camera 01)

Show Time	● On ○ Off	
Date Format	yyyy-MM-dd	dd=Day; M=Month; y=Year
Time Format	HH:mm:ss	h/H=12/24 Hour; tt=A.M. or P.M.; mm=Minute; ss=Second
Font Size	Medium	
Font Color		

1. Choose the camera, and click **On** to enable **Show Time**.
2. Configure the date format, time format, font size, and font color.
3. Click **Save** when you complete the configuration.

- OSD

1. Click **OSD Content**.



Select Camera	D1 (IP Camera 01)

□ OSD1	
□ OSD2	
□ OSD3	
□ OSD4	
□ OSD5	
□ OSD6	

Note: The OSD name allows 1-60 characters and is case-sensitive.

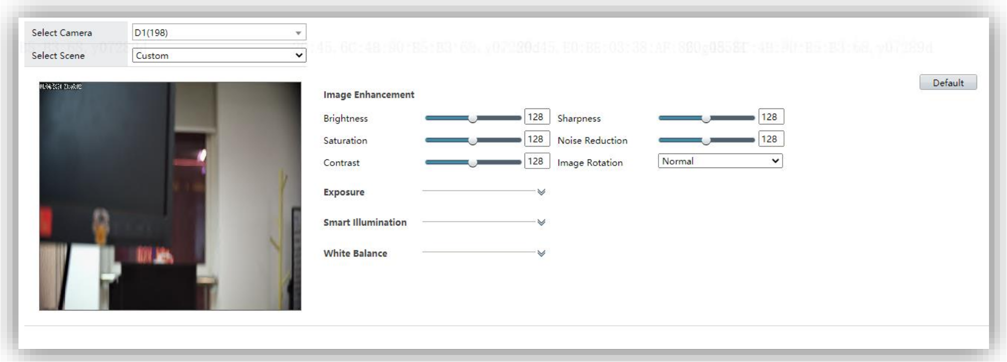
2. Select the checkbox for OSD1, and then configure the OSD in the right-side field. Up to six OSDs are allowed.
3. Click **Save** when you complete the configuration.

5.4.4 Image Settings

NOTE!

The image settings configured on the NVR will be synced to the camera.

Configure image settings of the camera on the page as shown below.



Select Camera: D1(198)

Select Scene: Custom

Image Enhancement

Brightness: 128

Saturation: 128

Contrast: 128

Sharpness: 128

Noise Reduction: 128

Image Rotation: Normal

1. Select the camera you want to configure.
2. Configure brightness, saturation, contrast, sharpness, noise reduction, image mirroring. Generally, the default settings can meet requirements. Do not change the settings randomly; otherwise, video and snapshots may be affected.
   - Parameter descriptions -- Image enhancement:

     Brightness: The higher the value, the brighter the image.

     Saturation: The higher the value, the more vibrant the colors of the picture; the lower the value, the opposite.

     Contrast: The higher the value, the brighter the bright areas and the darker the dark areas.

     Sharpness: The higher the value, the stronger the sense of jagged edges in the objects in the picture.

     Noise Reduction: The higher the value, the better the noise reduction effect, but it will affect the image clarity.

     Image Rotation: Rotate the image as needed.
   - Parameter descriptions - Exposure parameters

     IMPORTANT! Do not change the exposure settings randomly. If it is necessary to change the settings, consult a professional first.
   - Parameter descriptions - White balance

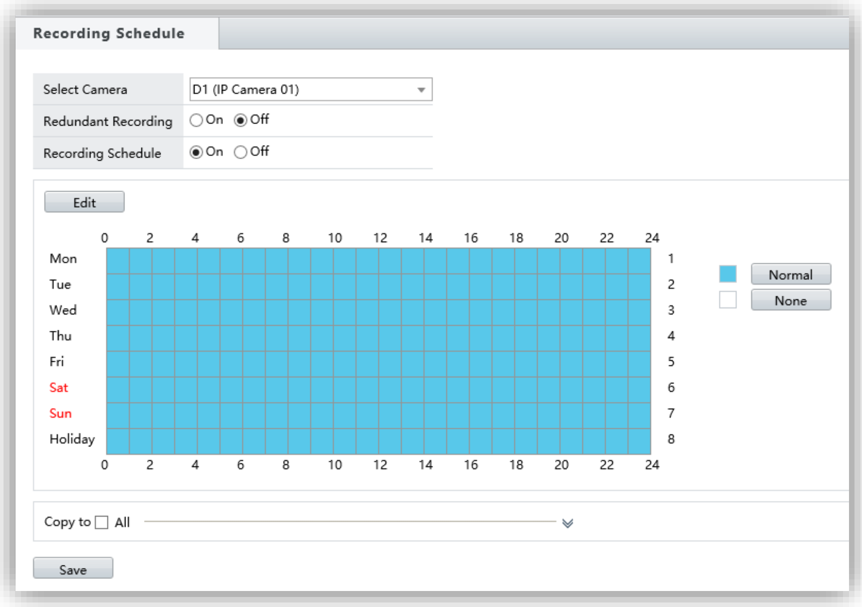
     IMPORTANT! Do not change the white balance settings randomly. If it is necessary to change the settings, consult a professional first.
3. The settings are saved automatically.

5.4.5 Edit Schedule

NOTE!

Generally, the default schedule can meet requirements. If it is necessary to modify the schedule, please refer to the descriptions below.

1. Go to **Setup** > **Camera Config** > **Schedule**. The page is as shown below.



Recording Schedule

Select Camera	D1 (IP Camera 01)
Redundant Recording	○ On ● Off
Recording Schedule	● On ○ Off

Copy to □ All

- Configure the parameters by referring to the table below.

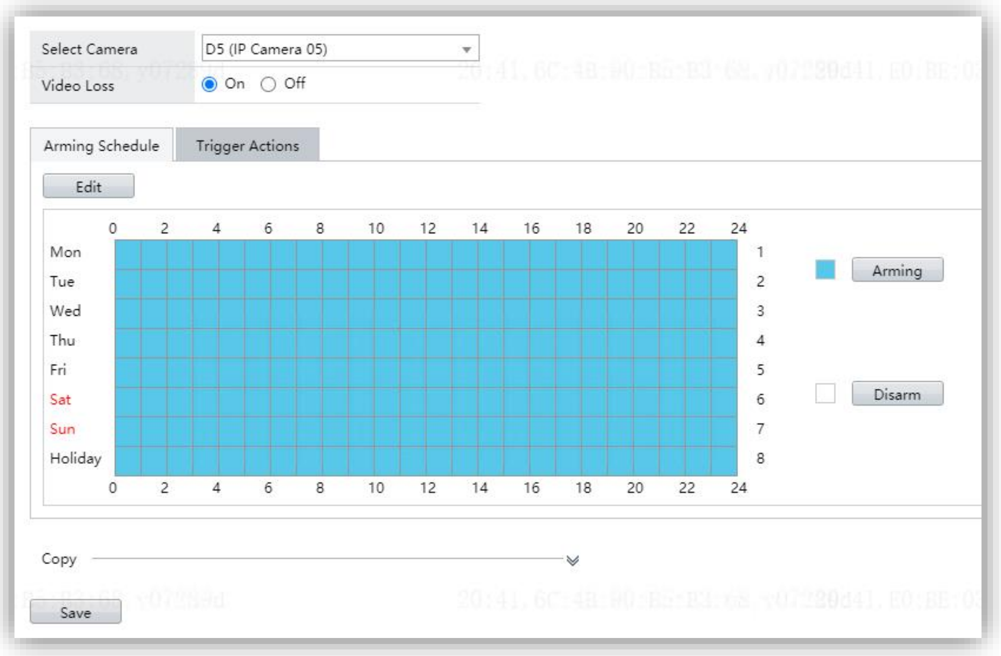
Parameter	Description
Select Camera	Select the target camera you want to configure.
Redundant Recording	When enabled, an extra copy of recordings will be saved on the redundant disk. You need to configure a redundant disk in disk management first.
Recording Schedule	This setting is enabled by default. When enabled, live video of the camera will be recorded.
Edit	You can configure the recording schedule for week days (Monday to Sunday) and for holidays, by hours or by day.
Copy To	This setting allows you to copy the schedule settings of the current day to other day(s).

5.4.6 Video Loss

NOTE!

Generally, the default settings can meet requirements. If it is necessary to modify the settings, please refer to the descriptions below.

1. Go to **Setup** > **Camera Config** > **Video Loss**. The page is as shown below.



Select Camera: D5 (IP Camera 05)

Video Loss: ● On ○ Off

1. Select the camera.
2. Enable video loss (video loss is enabled by default).

- Arming schedule
  1. Click **Edit** to edit the arming schedule. You can configure an arming schedule for week days (Monday to Sunday) and for holidays. By default, a 24H arming schedule is enabled for video loss detection.
  2. Copy the arming schedule of the current day to other days of the week.
- Alarm linkage
  1. Select linkage actions. Options include alarm output, alarm-triggered recording, and alarm-triggered snapshot.

  Note: It is required to connect an external alarm device for alarm output.

  2. Click **Save**.
  3. Click **Save** when you complete the configuration of video loss and linkage actions.

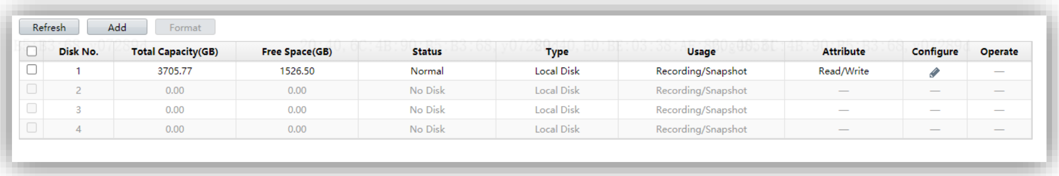
5.5 Disk Configuration

5.5.1 Disk Management

NOTE!

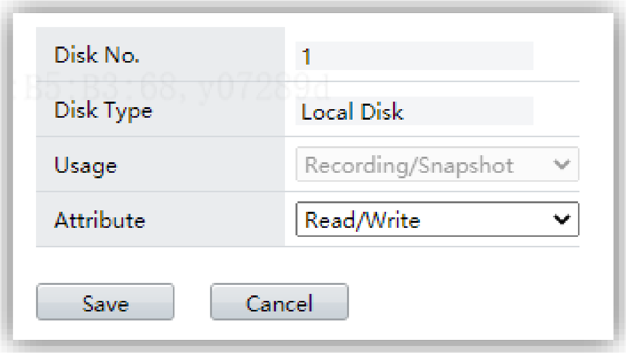
- Generally, the default settings can meet disk management requirements.
- To change the settings, please refer to the steps below.

1. Go to **Setup** > **Hard Disk** > **Hard Disk**. The page is as shown below.



□	Disk No.	Total Capacity(GB)	Free Space(GB)	Status	Type	Usage	Attribute	Configure	Operate
□	1	3705.77	1526.50	Normal	Local Disk	Recording/Snapshot	Read/Write	✎	—
□	2	0.00	0.00	No Disk	Local Disk	Recording/Snapshot	—	—	—
□	3	0.00	0.00	No Disk	Local Disk	Recording/Snapshot	—	—	—
□	4	0.00	0.00	No Disk	Local Disk	Recording/Snapshot	—	—	—

2. Click ✎ to edit the settings of the hard disk, as shown below.



Disk No.	1
Disk Type	Local Disk
Usage	Recording/Snapshot
Attribute	Read/Write

- Choose read/write permission, and then click **Save**.

  CAUTION: This configuration will affect video and image storage.

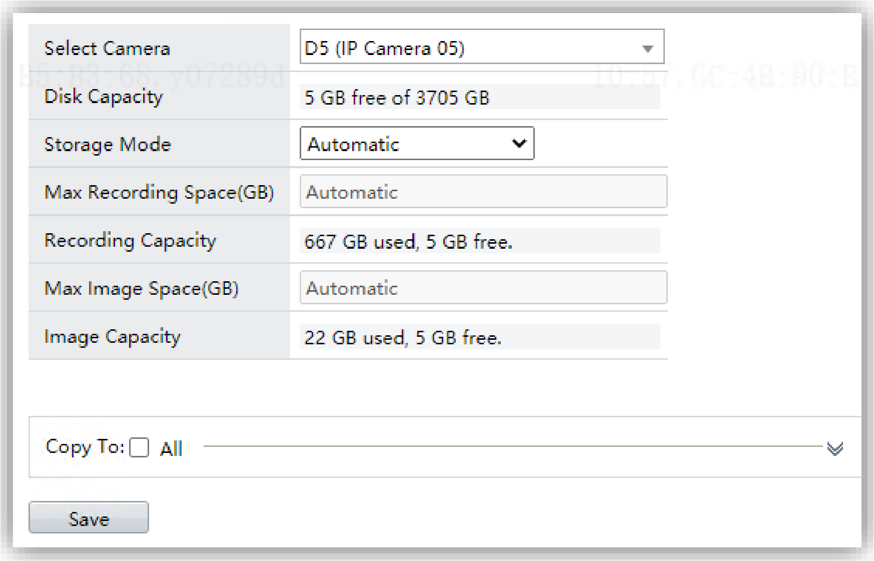
3. Click **Save** when you complete the configuration.

5.5.2 Capacity Configuration

NOTE!

Generally, the default settings can meet requirements. If it is necessary to change the settings, refer to the descriptions below.

1. To configure image and recording storage, follow the steps below.



Select Camera	D5 (IP Camera 05)
Disk Capacity	5 GB free of 3705 GB
Storage Mode	Automatic
Max Recording Space(GB)	Automatic
Recording Capacity	667 GB used, 5 GB free.
Max Image Space(GB)	Automatic
Image Capacity	22 GB used, 5 GB free.

Copy To: □ All

2. Choose the camera.

3. Choose the storage mode.

- Automatic

  1. The device automatically allocates recording space and image space for the camera; no manual configuration is required.

- Custom

  1. Configure recording space manually. The storage days allowed will be displayed.

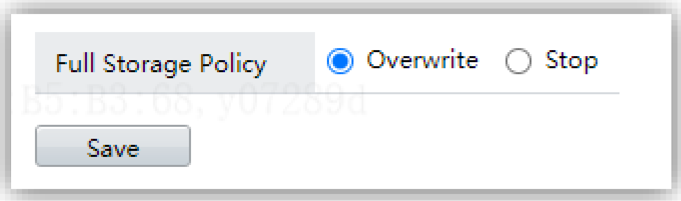
  2. Configure image space manually. The storage days allowed will be displayed.

4. Click **Copy to** to copy the current settings to other cameras.

5. Click **Save** when you complete the configuration.

5.5.3 Advanced Configuration

1. Go to **Setup** > **Hard Disk** > **Advanced Config** to configure storage policy for recording storage and image storage.



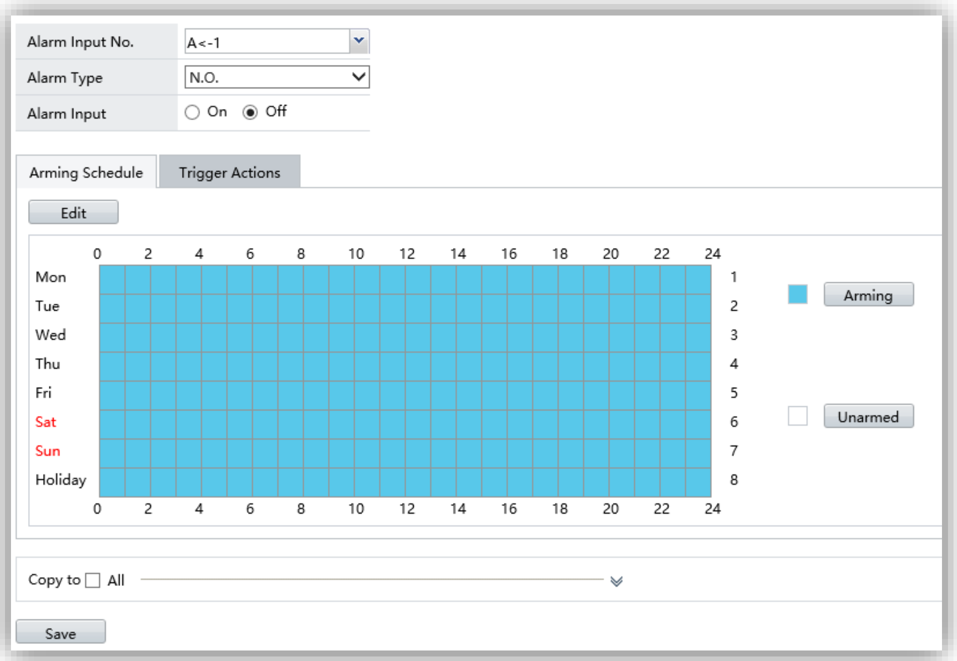
Full Storage Policy ● Overwrite ○ Stop

2. It is recommended to keep the default setting (Overwrite).

5.6 Alarm Configuration

5.6.1 Alarm Input

1. Go to **Setup** > **Alarm Config** > **Alarm Input**. The page is as shown below.



Alarm Input No.	A<-1
Alarm Type	N.O.
Alarm Input	○ On ● Off

Copy to □ All

2. Choose the alarm input number (the corresponding external interface connected to an alarm input device).
3. Choose the alarm type.
4. Select **On** to enable alarm input (default setting is **Off**).

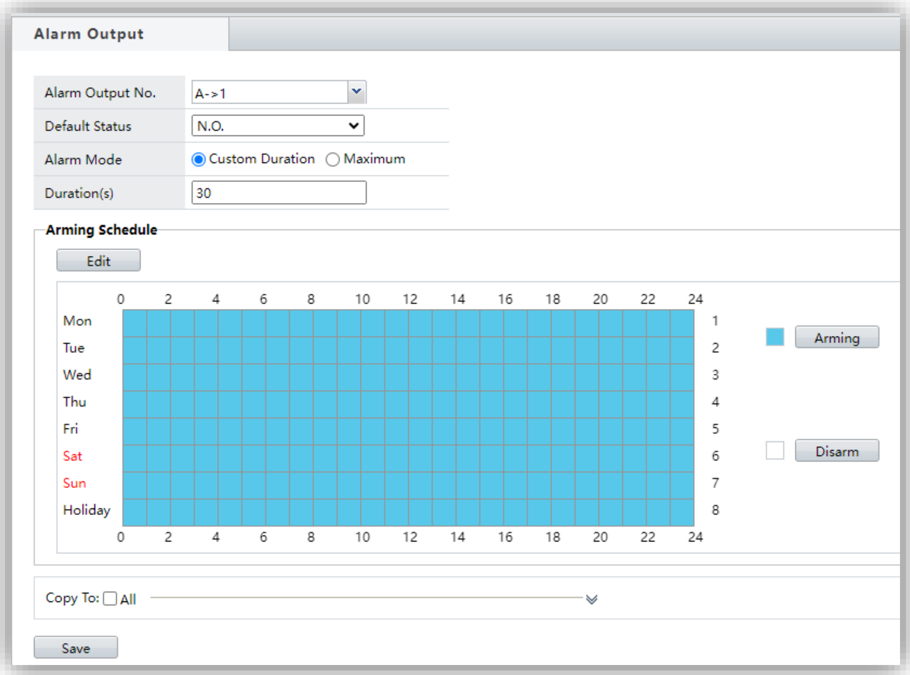
- Arming schedule
  1. Click **Edit** to edit the arming schedule. You can configure arming schedule for week days (Monday to Sunday) and for holidays.
  2. Copy the arming schedule of the current day to other days of the week or to holiday.
- Alarm linkage
  1. Select linkage actions. Options include alarm output, alarm-triggered recording, and alarm-triggered snapshot.

  Note: It is required to connect an external alarm device to implement alarm output.

  2. Click **Save** when you complete the configuration.
  3. Click **Save** when you complete the configuration of video loss and linkage actions.

5.6.2 Alarm Output

1. Go to **Setup** > **Alarm Config** > **Alarm Output**. The page is as shown below.



Alarm Output

Alarm Output No.	A->1
Default Status	N.O.
Alarm Mode	● Custom Duration ○ Maximum
Duration(s)	30

Arming Schedule

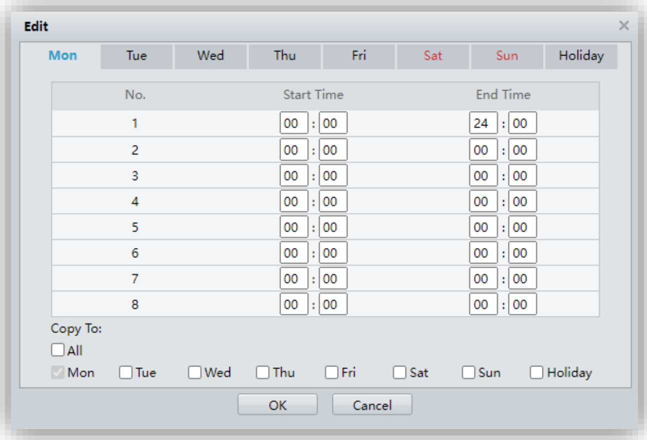
Copy To: □ All

2 Choose the alarm output number.

3. Choose the default status (N.O. or N.C.) as the alarm trigger condition.

4. Choose an alarm mode by choosing custom duration or maximum duration. This parameter sets the length of time that the alarm continues after the condition for triggering the alarm output has ended.

- Arming schedule



Edit

No.	Start Time	End Time
1	00 : 00	24 : 00
2	00 : 00	00 : 00
3	00 : 00	00 : 00
4	00 : 00	00 : 00
5	00 : 00	00 : 00
6	00 : 00	00 : 00
7	00 : 00	00 : 00
8	00 : 00	00 : 00

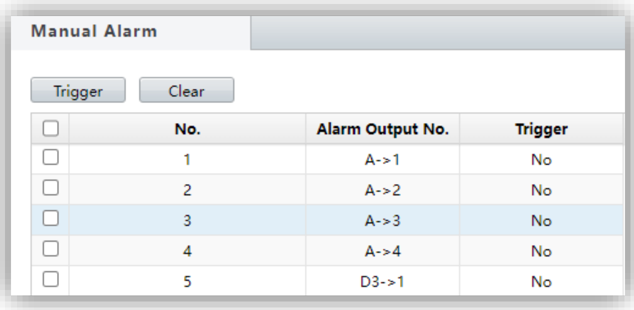
Copy To:
□ All
☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □ Holiday

1. Click **Edit** button, and then set the arming schedule from Monday to Sundays and for holiday.

2. Use **Copy To** to copy the settings of the current day to other days.

5.6.3 Manual Alarm

1. Go to Setup > Alarm Config > Manual Alarm. The page is as shown below.



Manual Alarm

Trigger | Clear

□	No.	Alarm Output No.	Trigger
□	1	A->1	No
□	2	A->2	No
□	3	A->3	No
□	4	A->4	No
□	5	D3->1	No

2. Select alarm output number(s) in the list, and then click **Trigger** to trigger alarm output, or click **Clear** to clear alarm output.

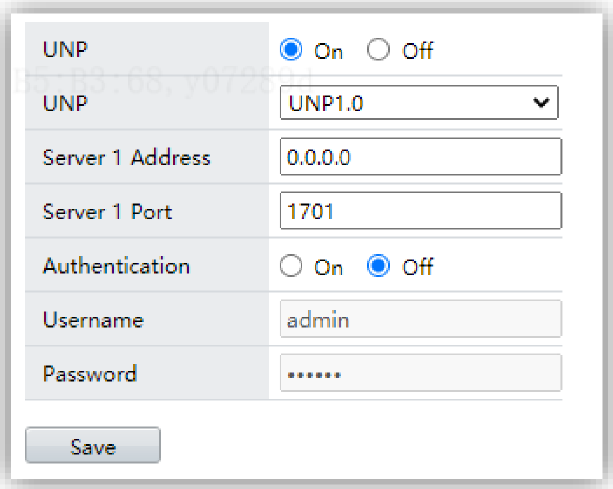
Note: Change the on/off status of alarm input will automatically trigger manual alarm. It is the current policy.

5.7 Platform Configuration

5.7.1 UNP

If GAP or firewall is configured on the network, you can connect the network via UNP.

1. Go to Setup > Platform > UNP. The page is as shown below.



UNP	● On ○ Off
UNP	UNP1.0
Server 1 Address	0.0.0.0
Server 1 Port	1701
Authentication	○ On ● Off
Username	admin
Password	••••••

Save

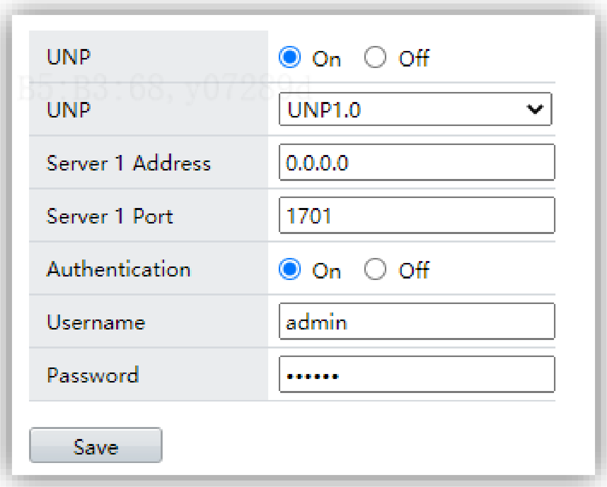
2. Enable UNP. The device's IP address is assigned by the UNP server.

3. Choose the UNP mode as needed.

- UNP1.0

A. Enter the UNP server address.

B. If the UNP server requires authentication, select On to enable authentication, and then enter the username and password.



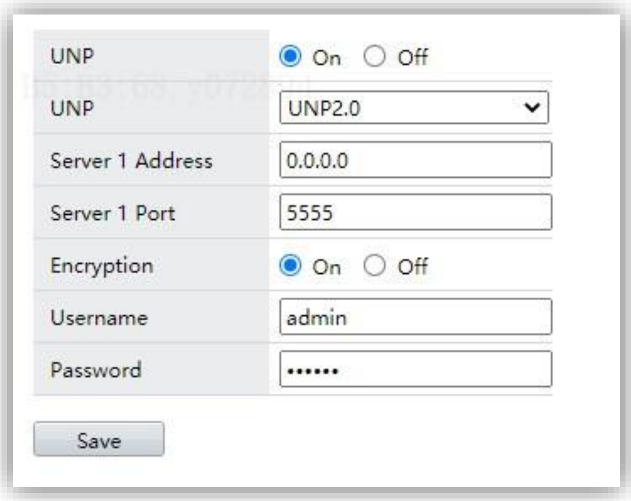
UNP	● On ○ Off
UNP	UNP1.0
Server 1 Address	0.0.0.0
Server 1 Port	1701
Authentication	● On ○ Off
Username	admin
Password	••••••

- UNP2.0

A. Enter the UNP server address.

B. Authentication is enabled by default. Enter the username and password.

C. Enable encryption to enhance data security.



UNP	● On ○ Off
UNP	UNP2.0
Server 1 Address	0.0.0.0
Server 1 Port	5555
Encryption	● On ○ Off
Username	admin
Password	••••••

4. Click Save when you complete the configuration.

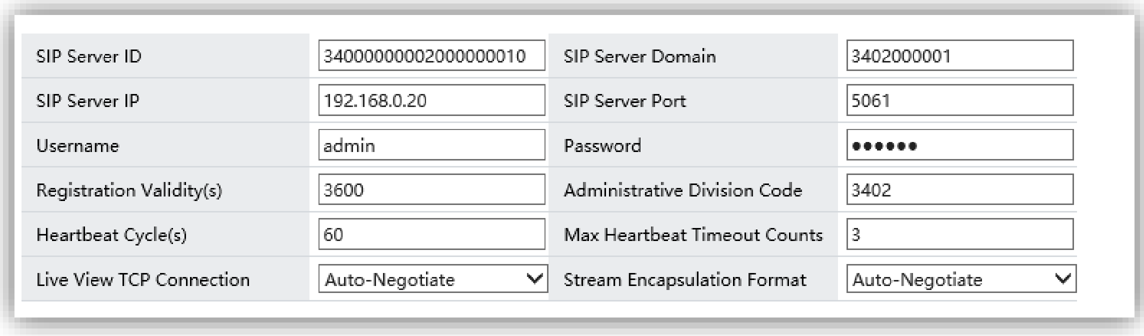
5.7.2 GB28281

1. To register the NVR to the upper platform, go to Setup > Platform > GB28281.

2. Enable the service.

3. Configure GB28181 server parameters and GB28181 local parameters.

- GB28181 server configuration

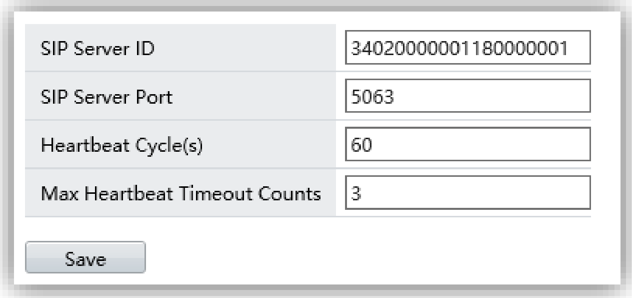


SIP Server ID	34000000002000000010	SIP Server Domain	3402000001
SIP Server IP	192.168.0.20	SIP Server Port	5061
Username	admin	Password	••••••
Registration Validity(s)	3600	Administrative Division Code	3402
Heartbeat Cycle(s)	60	Max Heartbeat Timeout Counts	3
Live View TCP Connection	Auto-Negotiate	Stream Encapsulation Format	Auto-Negotiate

Configure the parameters by referring to the table below.

Parameter	Description
SIP Server ID	The inter-domain domain ID obtained by the upper platform, for example, 34020000002001001060.
SIP Server Domain	Keep the default setting, which mainly indicates the area code (1-8 digits) and industry code (9-10 digits).
SIP Server IP	VM server IP.
SIP Server Port	SIP port of GB28181 on the VM platform, for example, 5061.
Username/Password	Authentication information required when adding the device on the VM platform. Set the username and password as needed.
Other Parameters	Keep the default settings. No modification is necessary.

- GB28181 local configuration



SIP Server ID	34020000001180000001
SIP Server Port	5063
Heartbeat Cycle(s)	60
Max Heartbeat Timeout Counts	3

Configure the parameters by referring to the table below.

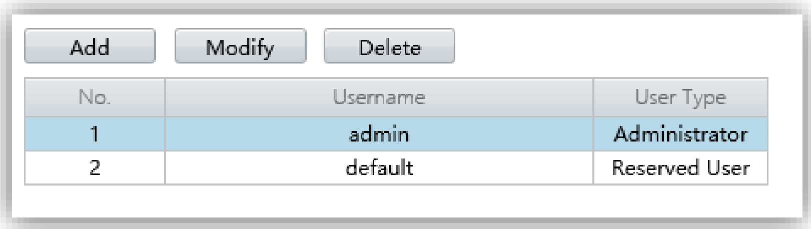
Parameter	Description
SIP Server ID	1-20 digits or letters (case-sensitive).
SIP Server Port	Range: [1-65535]. Default: 5063. Keep the default setting.
Other Parameters	Keep the default settings. No modification is necessary.

4. Click **Save** when you complete the configuration.

5.8 User Configuration

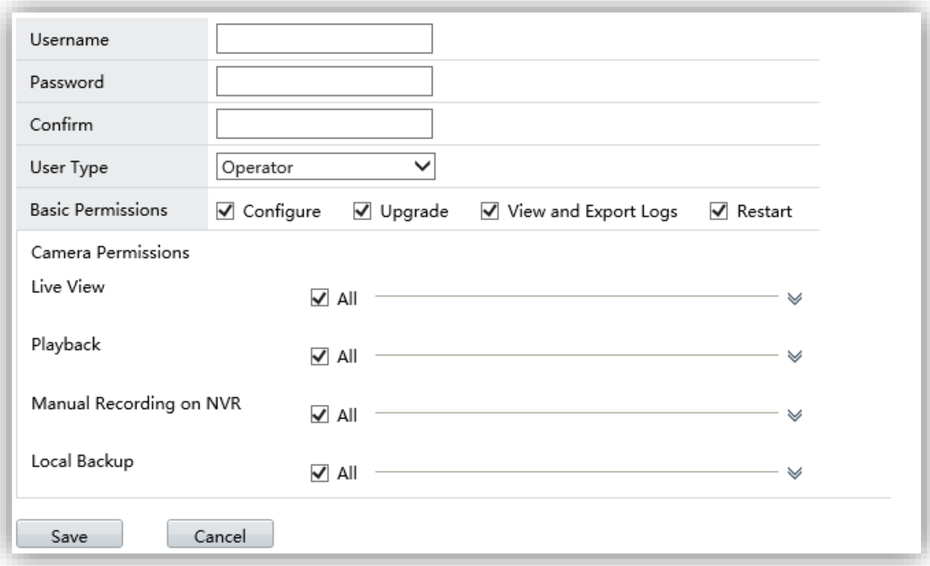
5.8.1 User Configuration

1. To change a user password or add users, go to **Setup** > **User** > **User**. The page is as shown below.



No.	Username	User Type
1	admin	Administrator
2	default	Reserved User

2. Click **Add** to add a user, set username and password for the user, and set permissions for the user, as shown below.



Username	
Password	
Confirm	
User Type	Operator
Basic Permissions	☑ Configure ☑ Upgrade ☑ View and Export Logs ☑ Restart

Camera Permissions

Live View ☑ All

Playback ☑ All

Manual Recording on NVR ☑ All

Local Backup ☑ All

3. For an existing user, you can select its username and then click **Edit** to change the password and permissions.

   Remarks: The admin is the system user and its permissions cannot be modified. Only the login password and email address (used for resetting password) can be modified.

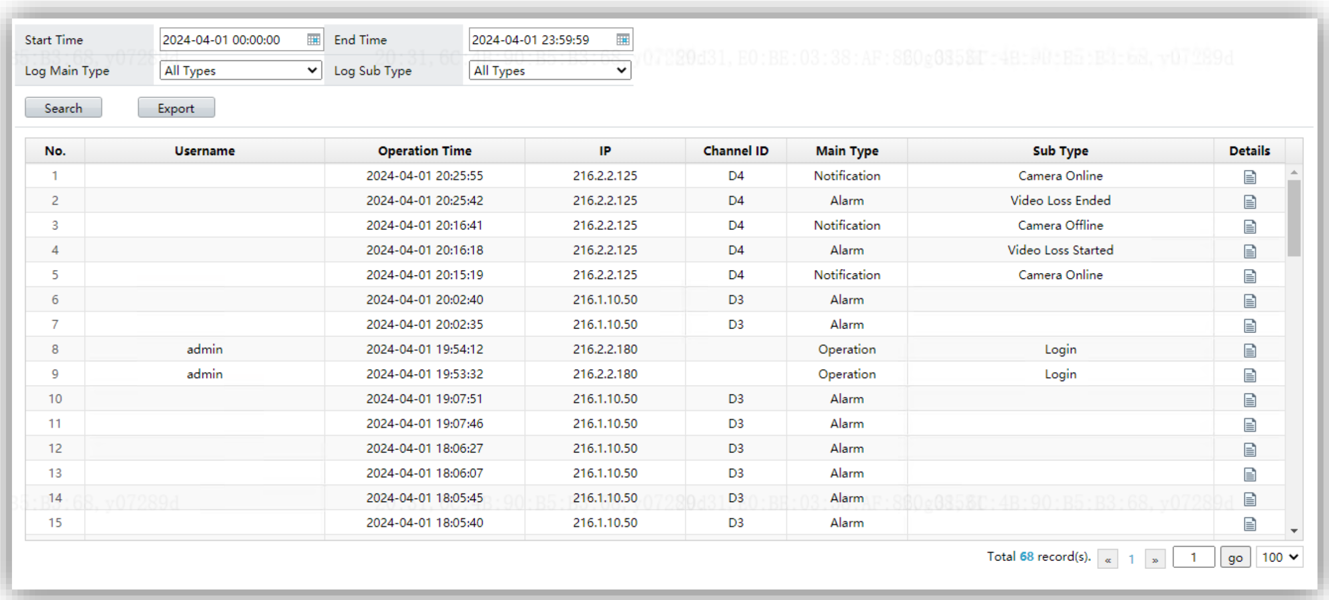
4. Click **Save** when you complete the configuration.

5.9 System Maintenance

5.9.1 Log Search

Search logs of operations performed by other users.

1. Go to **Setup** > **Maintenance** > **Search Logs**. The page is as show below.



Start Time	2024-04-01 00:00:00	End Time	2024-04-01 23:59:59
Log Main Type	All Types	Log Sub Type	All Types

No.	Username	Operation Time	IP	Channel ID	Main Type	Sub Type	Details
1		2024-04-01 20:25:55	216.2.2.125	D4	Notification	Camera Online	🗎
2		2024-04-01 20:25:42	216.2.2.125	D4	Alarm	Video Loss Ended	🗎
3		2024-04-01 20:16:41	216.2.2.125	D4	Notification	Camera Offline	🗎
4		2024-04-01 20:16:18	216.2.2.125	D4	Alarm	Video Loss Started	🗎
5		2024-04-01 20:15:19	216.2.2.125	D4	Notification	Camera Online	🗎
6		2024-04-01 20:02:40	216.1.10.50	D3	Alarm		🗎
7		2024-04-01 20:02:35	216.1.10.50	D3	Alarm		🗎
8	admin	2024-04-01 19:54:12	216.2.2.180		Operation	Login	🗎
9	admin	2024-04-01 19:53:32	216.2.2.180		Operation	Login	🗎
10		2024-04-01 19:07:51	216.1.10.50	D3	Alarm		🗎
11		2024-04-01 19:07:46	216.1.10.50	D3	Alarm		🗎
12		2024-04-01 18:06:27	216.1.10.50	D3	Alarm		🗎
13		2024-04-01 18:06:07	216.1.10.50	D3	Alarm		🗎
14		2024-04-01 18:05:45	216.1.10.50	D3	Alarm		🗎
15		2024-04-01 18:05:40	216.1.10.50	D3	Alarm		🗎

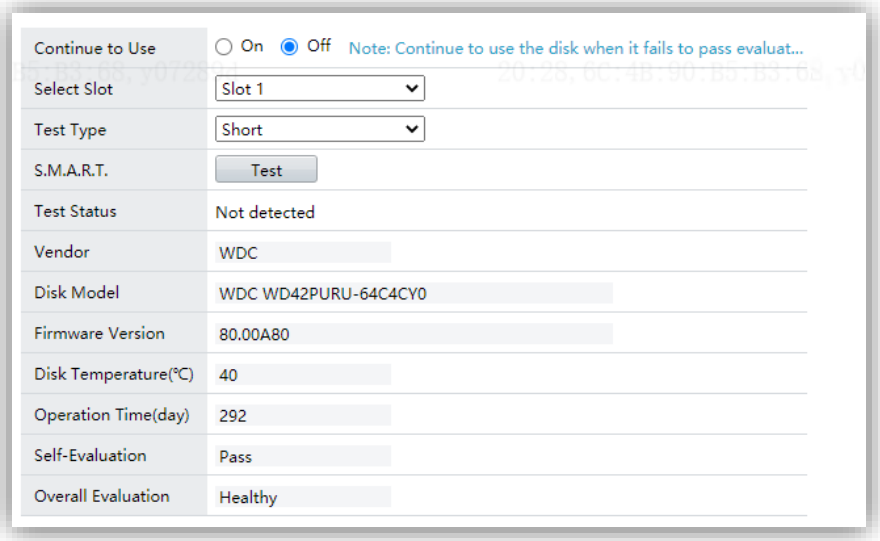
Total 68 record(s).

2. Set the time range for the logs you want to search.
3. Set the main type and sub type of logs, and then click **Search**.
4. To export search results to a file, click **Export**.

5.9.2 S.M.A.R.T. Test

- S.M.A.R.T. Test

1. Go to **Setup** > **Maintenance** > **HDD** > **S.M.A.R.T. Test**. The page is as shown below.



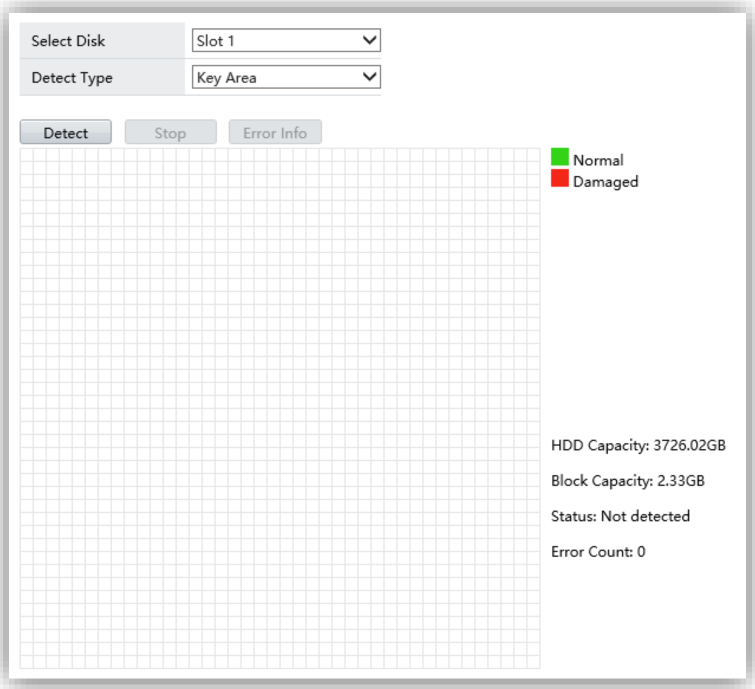
Continue to Use	○ On ● Off Note: Continue to use the disk when it fails to pass evaluat...
Select Slot	Slot 1
Test Type	Short
S.M.A.R.T.	Test
Test Status	Not detected
Vendor	WDC
Disk Model	WDC WD42PURU-64C4CY0
Firmware Version	80.00A80
Disk Temperature(℃)	40
Operation Time(day)	292
Self-Evaluation	Pass
Overall Evaluation	Healthy

2. Select the disk slot and test type, and then click **Test** to start the test. The test status shows the progress.
3. When the test is complete, the **Self-Evaluation** and **Overall Evaluation** fields show the test result.
   - If the test status is normal, the disk can be used properly.
   - To continue using the disk if the test result is abnormal, select **On** for **Continue to Use**.

     Caution: Continuing to use an unhealthy hard disk will pose a significant risk.

- Bad Sector Detection

1. Go to **Setup** > **Maintenance** > **HDD** > **Bad Sector Detect**. The page is as shown below.



Select Disk: Slot 1

Detect Type: Key Area

🟩 Normal

🟥 Damaged

HDD Capacity: 3726.02GB

Block Capacity: 2.33GB

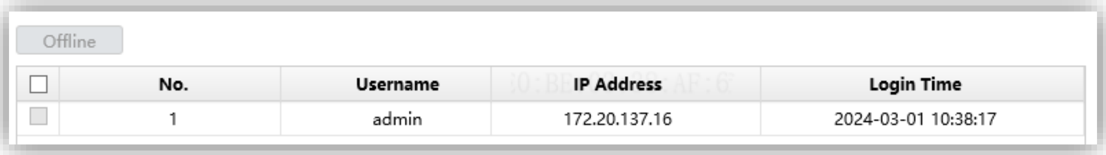
Status: Not detected

Error Count: 0

2. Select the disk slot and detection type, and then click **Detect** to start detection.
3. When the detection is complete, you can click **Error Info** to view error information (if any).

5.9.3 Online User

1. Force a logged-in user to log out by selecting the user and then clicking **Offline**.



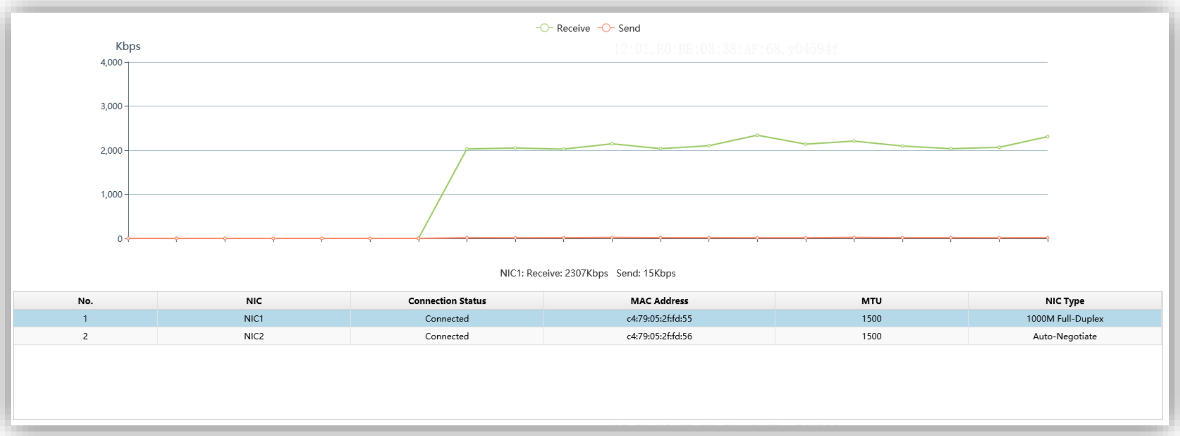
□	No.	Username	IP Address	Login Time
□	1	admin	172.20.137.16	2024-03-01 10:38:17

2. You can view the logged-in user's IP and login time.

5.9.4 Network Information

- Network Traffic

1. View the traffic information of each network card to determine if live video or image data are uploaded or received correctly.



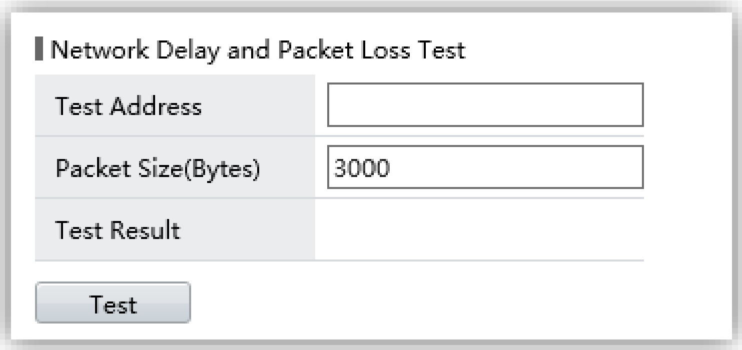
NIC1: Receive: 2307Kbps Send: 15Kbps

No.	NIC	Connection Status	MAC Address	MTU	NIC Type
1	NIC1	Connected	c4:79:05:2f:fd:55	1500	1000M Full-Duplex
2	NIC2	Connected	c4:79:05:2f:fd:56	1500	Auto-Negotiate

- Network Test

1. Go to **Setup** > **Maintenance** > **Network Info** > **Net Detect**. The page is as shown below.

- Packet loss test

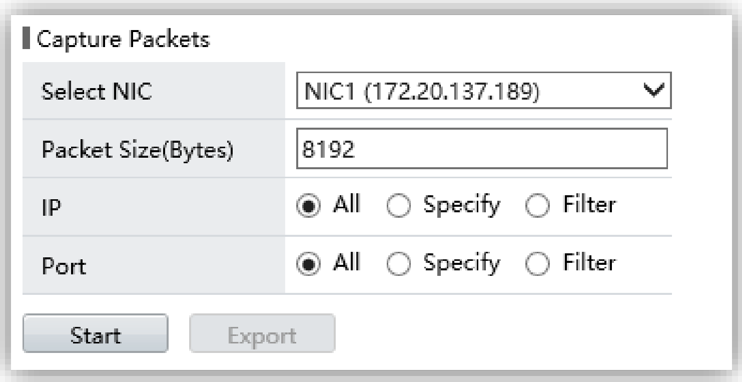


Network Delay and Packet Loss Test

Test Address	
Packet Size(Bytes)	3000
Test Result	

1. Enter the target IP address to perform packet loss test. The test result will be displayed when the test is completed.

- Packet Capture



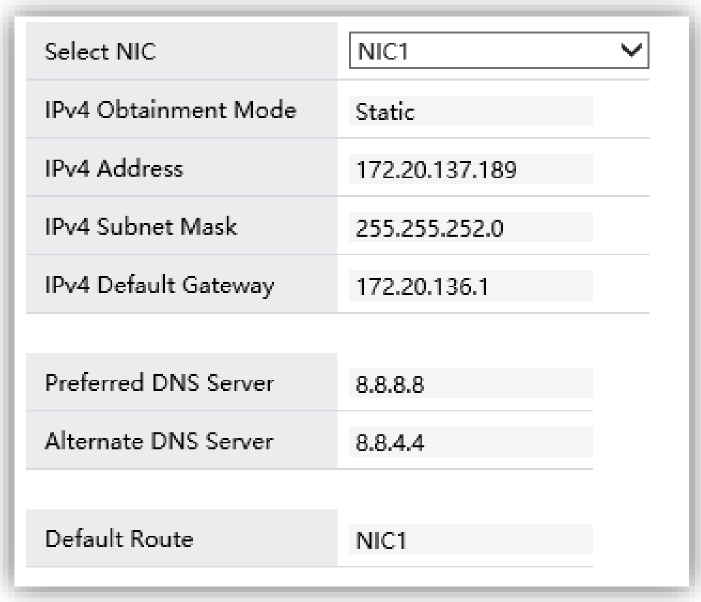
Capture Packets

Select NIC	NIC1 (172.20.137.189)
Packet Size(Bytes)	8192
IP	● All ○ Specify ○ Filter
Port	● All ○ Specify ○ Filter

1. Select the NIC.
2. Set the packet size.
3. Set the IP address and port number and then click **Start**.
4. When the capture is complete, click **Export** to export the captured packets.

- Network Test

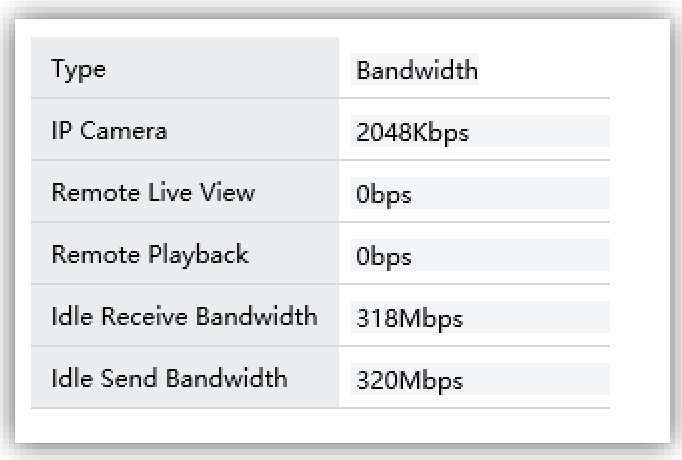
  View the network status of the NIC.



Select NIC	NIC1
IPv4 Obtainment Mode	Static
IPv4 Address	172.20.137.189
IPv4 Subnet Mask	255.255.252.0
IPv4 Default Gateway	172.20.136.1
Preferred DNS Server	8.8.8.8
Alternate DNS Server	8.8.4.4
Default Route	NIC1

- Network Resource Statistics

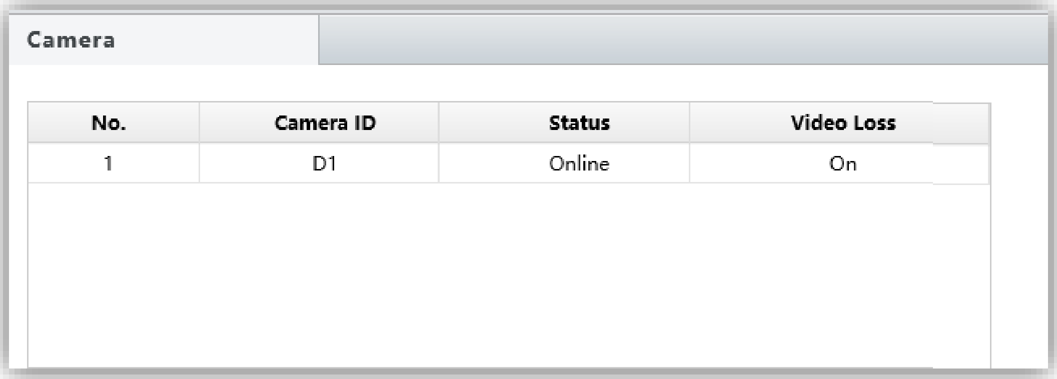
  View information about the current network resources.



Type	Bandwidth
IP Camera	2048Kbps
Remote Live View	0bps
Remote Playback	0bps
Idle Receive Bandwidth	318Mbps
Idle Send Bandwidth	320Mbps

5.9.5 Channel Status

View the status of the current camera.

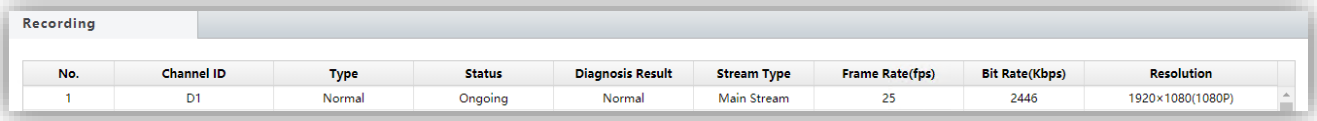


Camera

No.	Camera ID	Status	Video Loss
1	D1	Online	On

5.9.6 Recording Status

View the recording status of the current camera.



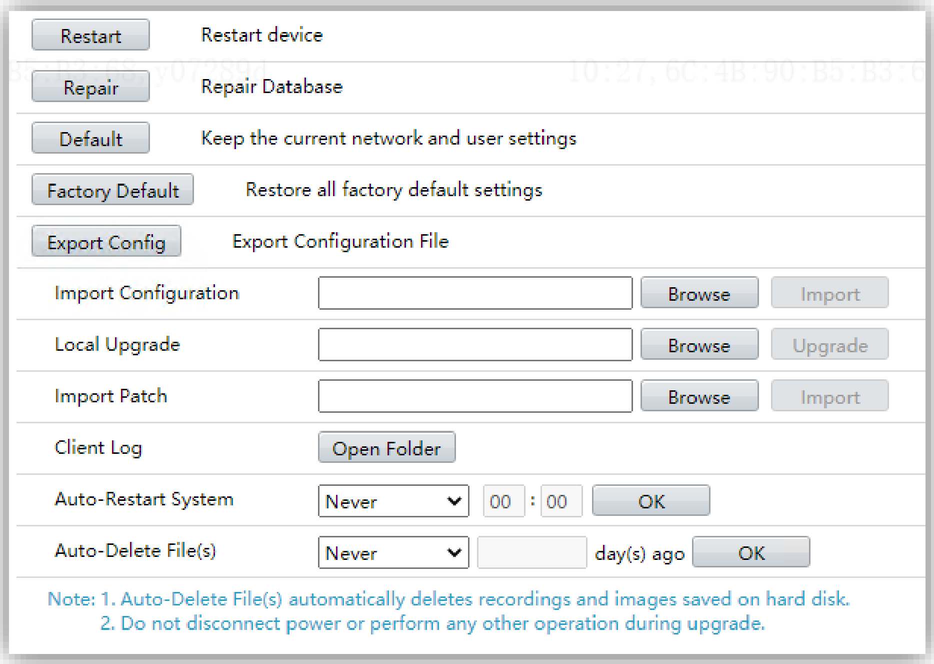
Recording

No.	Channel ID	Type	Status	Diagnosis Result	Stream Type	Frame Rate(fps)	Bit Rate(Kbps)	Resolution
1	D1	Normal	Ongoing	Normal	Main Stream	25	2446	1920×1080(1080P)

5.9.7 System Maintenance

- System Maintenance

  1. Go to Setup > Maintenance > Maintenance > Maintenance. The page is as shown below.



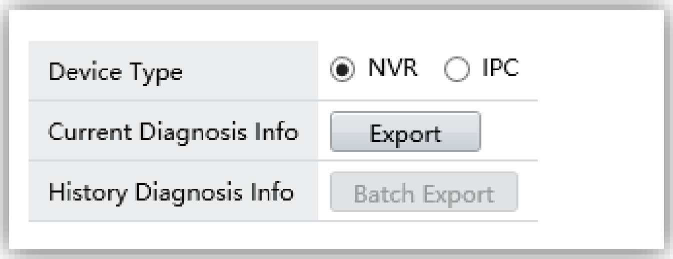
Restart	Restart device		
Repair	Repair Database		
Default	Keep the current network and user settings		
Factory Default	Restore all factory default settings		
Export Config	Export Configuration File		
Import Configuration		Browse	Import
Local Upgrade		Browse	Upgrade
Import Patch		Browse	Import
Client Log	Open Folder		
Auto-Restart System	Never 00 : 00	OK	
Auto-Delete File(s)	Never day(s) ago	OK	

Note: 1. Auto-Delete File(s) automatically deletes recordings and images saved on hard disk.
2. Do not disconnect power or perform any other operation during upgrade.

Configure the parameters by referring to the table below.

Parameter	Description
Restart	Restart the device.
Repair	Repair the database with one click.
Default	Restore all default settings except network and user settings.
Factory Default	Restore all default settings. Note: Clicking **Default** or **Factory Default** will not delete recordings and operation logs.
Export	Export configuration file for troubleshooting or backup.
Import	Import configuration file to restore the environment.
Local Upgrade	Perform a local upgrade to the device version using a **program.bin** file or a .zip file. Caution: During upgrade, do not disconnect power or perform any other operations.
Import patch	Import a **.patch** file. The device will restart after the import.
Client Log	Open the folder containing the client logs.
Auto-Restart System	The default setting is **Never**. You can enable this function and set the auto restart time.
Auto-Delete File(s)	The default setting is **Never**. You can enable this function and set the auto deletion time. Note: When Auto-Delete File(s) is enabled, the system will automatically delete videos and images saved on the hard disk.

- Diagnostic Info



Device Type	● NVR ○ IPC
Current Diagnosis Info	Export
History Diagnosis Info	Batch Export

1. Go to **Setup** > **Maintenance** > **Maintenance** > **Diagnosis Info**. The page is as shown below.

Configure the parameters by referring to the table below.

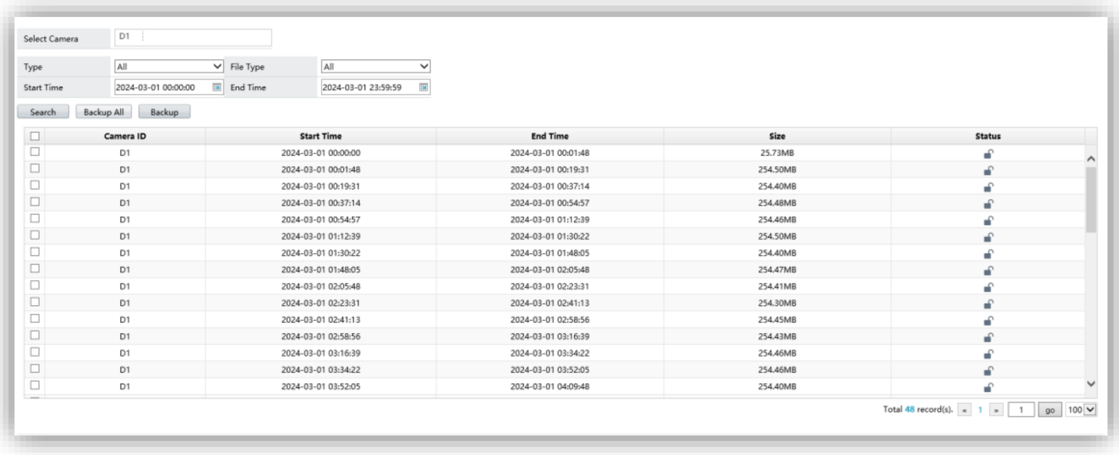
Parameter	Description
Device Type	Choose the type of device you want to export diagnostic information: NVR or IPC.
Current Diagnosis Info	Click **Export** to collect and export diagnostic information immediately.

History Diagnosis Info	You need to select one or more items in the list to activate the button.

5.10 Recording Backup

5.10.1 Recording Backup

1. Go to **Setup** > **Backup** > **Recording Backup** > **Recording Backup**. The page is as shown below.



Select Camera	D1
Type	All
File Type	All
Start Time	2024-03-01 00:00:00
End Time	2024-03-01 23:59:59

□	Camera ID	Start Time	End Time	Size	Status
□	D1	2024-03-01 00:00:00	2024-03-01 00:01:48	25.73MB	🔓
□	D1	2024-03-01 00:01:48	2024-03-01 00:19:31	254.50MB	🔓
□	D1	2024-03-01 00:19:31	2024-03-01 00:37:14	254.40MB	🔓
□	D1	2024-03-01 00:37:14	2024-03-01 00:54:57	254.48MB	🔓
□	D1	2024-03-01 00:54:57	2024-03-01 01:12:39	254.46MB	🔓
□	D1	2024-03-01 01:12:39	2024-03-01 01:30:22	254.50MB	🔓
□	D1	2024-03-01 01:30:22	2024-03-01 01:48:05	254.40MB	🔓
□	D1	2024-03-01 01:48:05	2024-03-01 02:05:48	254.47MB	🔓
□	D1	2024-03-01 02:05:48	2024-03-01 02:23:31	254.41MB	🔓
□	D1	2024-03-01 02:23:31	2024-03-01 02:41:13	254.30MB	🔓
□	D1	2024-03-01 02:41:13	2024-03-01 02:58:56	254.45MB	🔓
□	D1	2024-03-01 02:58:56	2024-03-01 03:16:39	254.43MB	🔓
□	D1	2024-03-01 03:16:39	2024-03-01 03:34:22	254.46MB	🔓
□	D1	2024-03-01 03:34:22	2024-03-01 03:52:05	254.46MB	🔓
□	D1	2024-03-01 03:52:05	2024-03-01 04:09:48	254.40MB	🔓

Total 48 record(s).

2. Select the camera.

3. Select the recording type, type, event type, and file type.

4. Select the start time and end time.

5. Click **Search**. The search results are displayed. Select the recordings you want to back up and then click **Backup**; or click **Backup All** to back up all the recordings.