Edge Storage Terminal

User's Manual



V1.0.1

Foreword

General

This manual introduces the installation, functions and operations of the 12-ch edge storage terminal (hereinafter referred to as "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated "Important Safeguards and Warnings".	August 2022
V1.0.0	First Release.	February 2022

Privacy Protection Notice

As the Device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between

the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the Device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirements



- Pack the Device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Transport the Device under allowed humidity and temperature conditions.

Storage Requirements



Store the Device under allowed humidity and temperature conditions.

Installation Requirements

 WARNING

- To avoid damage to the hard disk, the Device must be carefully installed in a horizontal position. The device must never be placed in an inclined or vertical position.
- Do not install the Device in locations where children are likely to be present.
- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- When using a laser beam device, avoid exposing the surface of the Device to laser beam radiation.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Device label.
- The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily

accessible location for emergency power cut-off.

- Operating temperature: –30 °C to +65 °C (–22 °F to +149 °F).
- The rated current of the Device is 5 A and the rated power is 60 W (for device with a 4 T HDD).
- The power and communication port of the Device can sustain a surge of±6 KV in common mode and±4 KV in differential mode. Extra surge protection is required when the Device is connected to a circuit with higher surge levels.
- To ensure heat dissipation, the gap between the Device and the surrounding area should not be less than 50 mm on the sides and 50 mm on top of the Device.
- A safety circuit breaker is designed on the connector of the Device to cut the power of the Device. Make sure the breaker can be easily operated during installation.
- Only applicable for use in altitudes below 2,000 meters.
- Only applicable for use in non-tropical climates.

Operation Requirements



WARNING

This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.



- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device.
- We recommend you use the Device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the Device.
- Do not block the ventilation near the Device.
- Do not vibrate, squeeze or immerse the Device in liquid.
- Ground the function earthing portion of the Device to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Prevent water from flowing into the Device during on-site installation to avoid the risk of damage.
- Do not place an open flame on the Device, such as a lit candle.
- The device is applicable for DC power supplies with the negative pole grounded.
- Replace unwanted batteries with new batteries of the same type and model. To prevent explosion, replace the battery with the correct model and dispose of the old ones as instructed.
- Do not expose the battery to extremely hot environments, such as direct sunlight and fire.

Maintenance Requirements



- Clean the Device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Power off the Device before maintenance.
- Clean the dust off the circuit board, connectors and the cabinet to avoid the device short circuiting due to dampness.
- Make sure the Device is properly grounded to avoid being damaged by static electricity or induced voltage.
- Do not plug in or unplug RS-232, RS-485 and other ports while the power is on to avoid damage to the ports.
- Do not expose the Device to heat sources and high temperature environments. Keep the area around the Device cabinet well-ventilated.
- Regularly inspect and perform maintenance on the Device.

Notes for HDD

HDD Requirements

⚠

Use HDDs and cables recommended by the manufacturer to avoid risks of abnormal device operations or unrecognized HDDs. We assume no responsibilities for losses caused by wrong HDDs or cables.

Table 1 Recommended models of new HDDs

Brand	Model	Capacity	Size (inch)
Seagate	ST1000VM002	1 T	3.5
Seagate	ST2000VM003	2 T	3.5
Seagate	ST4000VM000	4 T	3.5
Seagate	ST1000VX001	1 T	3.5
Seagate	ST2000VX003	2 T	3.5
Seagate	ST4000VX000	4 T	3.5
Seagate	ST6000VX0003	6 T	3.5

Temperature Requirements

- Temperature requirements vary with the configured total capacity of HDDs. Do not use them in an over-temperature environment; otherwise, the HDD service life will be affected.
  - ◇ –30°C to + 65°C: Applicable to the models with a total capacity of 1 T/2 T/4 T/8 T.
  - ◇ –30°C to + 50°C: Applicable to the models with a total capacity of 12 T.
  - ◇ –30°C to + 45°C: Applicable to the models with a total capacity of 16 T.
- If the Device is used at an ambient temperature≤ 0°C, a special heater for HDDs is also required when adding HDDs.

Table of Contents

Foreword I

Important Safeguards and Warnings III

Notes for HDD VI

1 Product Introduction 1

1.1 Overview 1

1.2 Functions 1

2 Appearance and Structure 3

2.1 Appearance 3

2.2 Front Panel 3

2.3 Rear Panel 4

3 Quick Configuration 6

3.1 Initializing the Device 6

3.2 Changing IP Address 7

3.3 Device Upgrade 7

3.4 Logging in to Webpage 7

4 Webpage Operations 8

4.1 Webpage Introduction 8

4.1.1 Recommended System Requirements 8

4.1.2 Login 8

4.1.3 Resetting Password 9

4.1.4 Webpage Functions 11

4.2 Live 11

4.2.1 Video and Picture 11

4.2.2 Video 12

4.2.3 Picture 13

4.3 Data Search 14

4.3.1 Searching for Vehicles 14

4.3.2 Searching for Recordings 16

4.4 Setting 18

4.4.1 ITC 18

4.4.1.1 Selecting Working Mode 18

4.4.1.2 Image Mosaic 18

4.4.1.2.1 Normal Combination 18

4.4.1.2.2 Related Composition 20

4.4.1.3 Measuring Section Speed 24

4.4.1.4 Setting Snapshot OSD 26
4.4.1.5 Automatic Network Recovery 28
4.4.1.6 Allowlist and Blocklist 29
4.4.1.6.1 Setting Allowlist 29
4.4.1.6.2 Setting Blocklist 31
4.4.1.7 Traffic Flow 31
4.4.1.8 Watermark Verification 31
4.4.1.8.1 Picture Verification 32
4.4.1.8.2 Video Verification 32
4.4.2 Network Settings 32
4.4.2.1 TCP/IP 33
4.4.2.2 Port 34
4.4.2.2.1 Port 34
4.4.2.2.2 ONVIF 34
4.4.2.3 Auto Registration 34
4.4.2.4 Flow Statistics 35
4.4.2.5 802.1x 36
4.4.2.6 Routing Settings 36
4.4.3 Remote Device 37
4.4.3.1 Remote Device 37
4.4.3.2 Device Search 39
4.4.3.3 Upgrading Remotely 41
4.4.4 Event Management 41
4.4.4.1 Setting Relay Activation 42
4.4.4.2 Abnormality 43
4.4.4.3 Testing Alarm I/O Output 44
4.4.5 Storage Management 44
4.4.5.1 Storage 45
4.4.5.1.1 Local Storage 45
4.4.5.1.2 Smart Info 45
4.4.5.2 FTP Storage 46
4.4.5.3 Recording 47
4.4.5.3.1 Record Control 47
4.4.5.3.2 Record Plan 48
4.4.5.4 Snapshot 49
4.4.6 System 50
4.4.6.1 General 50
4.4.6.1.1 General Settings 50

4.4.6.1.2 Date & Time 51
4.4.6.2 Local Setting 52
4.4.6.3 Account Management 52
4.4.6.3.1 Account 52
4.4.6.3.2 ONVIF User 54
4.4.6.4 Safety 55
4.4.6.4.1 System Service 55
4.4.6.4.2 HTTPS 56
4.4.6.4.3 Firewall 60
4.4.6.5 Default 60
4.4.6.6 Import/Export 60
4.4.6.7 Auto Maintain 61
4.4.6.8 System Update 61
4.4.7 System Information 62
4.4.7.1 Version Information 62
4.4.7.2 Log 62
4.4.7.2.1 System Log 62
4.4.7.2.2 Remote Log 63
4.4.7.3 Viewing Online User 63
4.4.7.4 Legal Information 63
4.5 Alarm 64
4.6 Logout 64
Appendix 1 Reference for Filling in Allowlist and Blocklist Template 65
Appendix 2 Cybersecurity Recommendations 68

1 Product Introduction

1.1 Overview

The Device is a high-performance outdoor edge storage device, which is used to receive videos and pictures collected by cameras. It integrates video management, data management, real-time storage, picture composition, and network switching.
The Device is widely used in various monitoring systems of roads and airport runways. It also provides multiple storage methods such as device storage, FTP storage, and platform storage.
The Device can work independently or form a stronger security surveillance network with multiple cameras, platforms, and professional video surveillance software.

1.2 Functions

Image Mosaic

- Combine several violation event pictures into one picture. The combination method can be flexibly configured to provide an effective basis for violation penalties, parking fee or illegal parking penalties.
- Overlay information such as license plate, parking space name, time, and location on the picture.

Storage

- Based on the configuration strategy of the user, store videos and pictures from the camera in the edge storage device through the network.
- Users can store picture files in the HDDs of the Device as required.
- Store pictures and associated records in the FTP server.
- Mass storage, up to 4 × 4 T HDDs.

History Search and Download

- Search for data by picture type, channel, plate, and other key words.
- Multiple users can download the search results at the same time.

Recording

- Record any channel on the Device, and store the records on the HDDs of the Device.
- All-day recording and multi-period timing recording.

Alarm

Set multiple-channel alarm input, output, and prompt message.

Network Management

- Manage the Device configuration and control permissions through Ethernet.
- Manage devices through the webpage.

Communication Ports

- RS-485 and RS-232 ports.
- 16 switching network ports, can be used as a switch.
- Two 1000 M network ports. The G2 network adapter and 8-channel 100 M network ports form a switching network.

2 Appearance and Structure

2.1 Appearance

Figure 2-1 Device appearance



2.2 Front Panel

Figure 2-2 Front panel

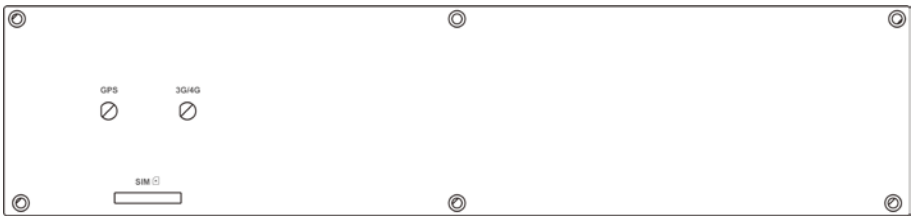


Table 2-1 Front panel ports

Port	Description
3G/4G	This antenna port can be used to enhance the signal when the Device is configured with the 3G/4G module.
GPS	This antenna port can be used when the Device is configured with the GPS module. Place the GPS antenna in an open area to enhance the signal when using it.
SIM	When the Device has 3G/4G module configured, you can insert the SIM card to use the 3G/4G function.

2.3 Rear Panel

Figure 2-3 Rear panel

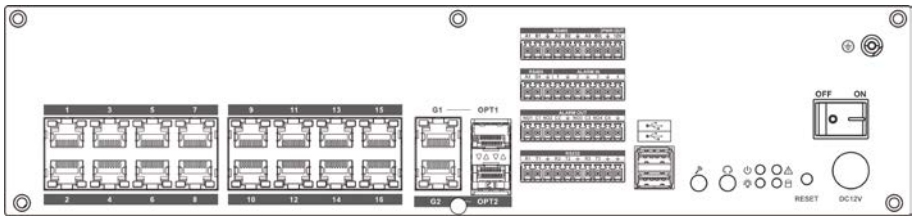


Table 2-2 Description of ports on rear panel

Port		Description
1–16	Network port	16 RJ-45 self-adaptive Ethernet ports. They are on the same network segment with G2.
G1/G2	Dual NICs port	Two 1000 Mbps Ethernet ports. They are physically separated, available for connecting to cameras and platforms on different network segments.
OPT1/OPT2	Optical port	Two 1000 M SFP optical fiber ports. OPT1 and G1, OPT2 and G2 are respectively on the same network segment.
	USB3.0 port	Connects with external USB storage devices. Reserved function.
	Audio input port	1-channel audio input port. Reserved function.
	Audio output port	1-channel audio output port. Reserved function.
	Power indicator	Displays the status of the power supply. Solid red means the Device is working normally.
	Operation indicator	Displays the operation status of the Device. • Solid green: The Device runs normally. • Flashes green: The Device is being upgraded.
	Alarm indicator	Displays the alarm status of the Device. • Solid red: The alarm is enabled. • Flashes red: The alarm is triggered.
	HDD status indicator	Displays the status of HDD. The indicator flashes green when the HDD is exchanging data.
	Ground port	This port must be grounded to improve device reliability. Otherwise, the Device will lose its lightning protection function.
	Power button	Turns on/off the Device.
RESET	Reset button	Restores the Device to factory defaults. Press and hold the button for more than 10 seconds when the Device is working, and the system configuration restores to factory defaults.
DC 12V	12 VDC power	Power port.

Figure 2-4 Ports on the middle of rear panel

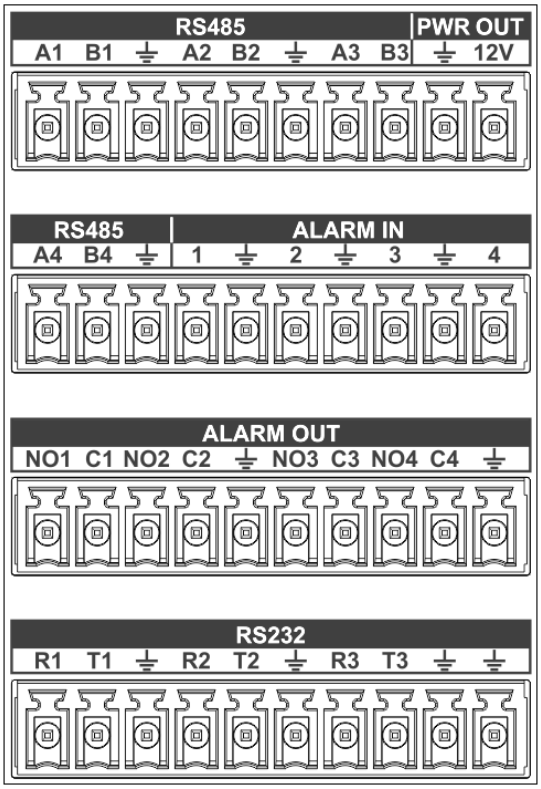


Table 2-3 Middle ports description

Port Name		Group	Description
PWR OUT	12 V	—	Power output port.
	⏚	—	Ground.
RS485	Four sets of RS-485 ports.	A1, B1	● A1, A2, A3, A4: RS-485_A port. ● B1, B2, B3, B4: RS-485_B port.
		A2, B2	
		A3, B3	
		A4, B4	
ALARM IN	4-channel alarm input port	1	Receives switch quantity signals from external alarm sources. ● 1, 2, 3, 4: alarm input ports. ● ⏚: alarm input ground terminal.
		2	
		3	
		4	
		⏚	
ALARM OUT	4-channel alarm output port	NO1, C1	Outputs alarm signals to external alarm devices that must have power supply. ● NO1, NO2, NO3, NO4: normally open alarm output ports. ● C1, C2, C3, C4: common alarm output ports.
		NO2, C2	
		NO3, C3	
		NO4, C4	
RS232	3 sets of RS-232 ports	R1, T1	● R1, R2, R3: RS-232 serial port receivers. ● T1, T2, T3: RS-232 serial port senders.
		R2, T2	
		R3, T3	

3 Quick Configuration

You can use the ConfigTool to quickly configure the Device, including initialization, system update and webpage login.

- The operation pages vary depending on different versions.
- Get the ConfigTool installation package from technical support and install it on your local computer.

3.1 Initializing the Device

You can initialize the Device, and cameras connected to the Device in batches through the ConfigTool.

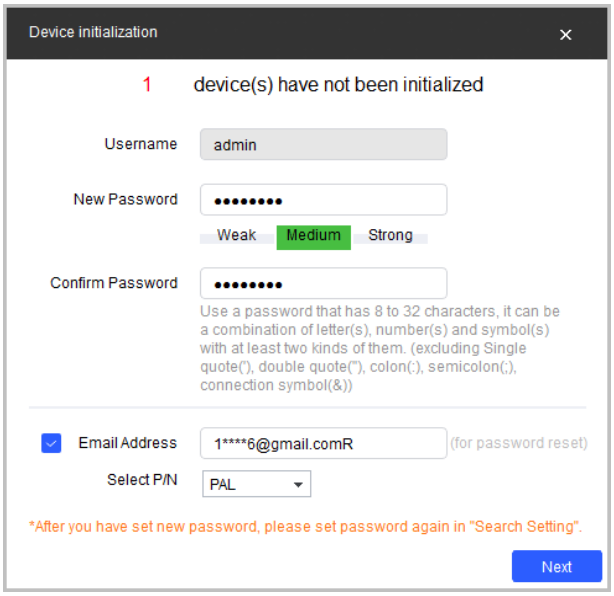
Uninitialized devices are not available for any operations and are displayed in gray on the Device list.

Step 1 Start the ConfigTool, and then click **Modify IP**.

The ConfigTool automatically searches for devices on the same network segment with the computer.

Step 2 Select a device to be initialized, and then click **Initialize**.

Figure 3-1 Device initialization



Step 3 Set and confirm the password, and enter an email for future password reset.

The pages are for reference only, and might differ from the actual page.

Step 4 Click **Initialize**, and the system starts initializing the Device.

is displayed for successful initialization, and is displayed for initialization failure. Click the icon to view details.

Step 5 Click **Finish**.

3.2 Changing IP Address

You can acquire and change the IP address of devices accessed through wired network. This section uses changing IP address with the ConfigTool as the example.

Step 1 Get the ConfigTool from technical support and install it on your local computer.

Step 2 Start the ConfigTool.

Step 3 Click **Modify IP**.

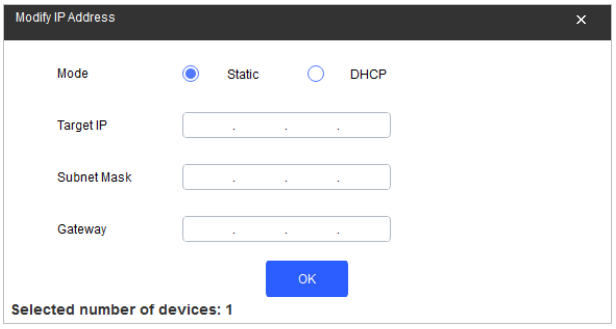
Step 4 Select the device(s) whose IP need(s) to be changed.

- Change one IP address: Click **Edit** corresponding to the device.
- Change IP addresses in batches: Select the devices, and then click **Batch Modify IP**.

Step 5 Set mode, IP, subnet mask and gateway.

Step 6 Click **OK**.

Figure 3-2 Change IP addresses in batches



3.3 Device Upgrade

Single upgrade and batch upgrade are supported.

Step 1 Start the ConfigTool.

Step 2 Click **Device Upgrade**.

Step 3 Select the Device to be updated.

- Update one by one: Click corresponding to the Device.
- Update in batches: Select multiple devices, and then click **Batch Upgrade**.

Step 4 Select the update file.

Step 5 Update the Device.

- Update one by one: Click to start updating.
- Update in batches: Click **OK** to start updating.

During update, if the Device is disconnected, as long as the ConfigTool stays on the update page, the upgrade will continue when the Device is reconnected.

3.4 Logging in to Webpage

On the **Modify IP** page, click **Web** corresponding to the Device, and then you are directed to the login page of the webpage. Enter the login username and password to log in.

4 Webpage Operations

You can access and manage connected devices, such as cameras and radars through the webpage of the Device.

The pages displayed in this section are for reference only, and might differ from the actual model.

4.1 Webpage Introduction

Log in to the webpage of the Device through a browser, on which you can operate on, configure and maintain the Device.

4.1.1 Recommended System Requirements

Table 4-1 Recommended system requirements

Component	Recommended System Requirements
Operating system	Windows 7 and later.
CPU	Intel core i3 and later.
Graphics card	Intel HD Graphics and later.
Memory	2 GB and bigger.
Monitor resolution	1024 × 768 and higher.
Browser	Internet Explorer 11, Chrome 41/33, and Firefox 49.

4.1.2 Login

- For first-time login or login after the Device is restored to factory defaults, initialization is required.
- Make sure that the IP address of the computer and that of the Device are on the same network segment. Otherwise, the initialization might fail.

Step 1 Set the IP address, subnet mask, and gateway of the computer and the Device.

- If there is no router on the network, assign an IP address on the same network segment.
- If there is a router on the network, set the corresponding gateway and subnet mask.

- The IP address of the Device cannot be set before logging in to the webpage on the computer.
- Based on the factory defaults, the IP address of G1 port is 192.168.1.108, and that of G2 port is 192.168.2.108.

Step 2 Enter ping *device IP address* in the cmd command window to check whether the network is

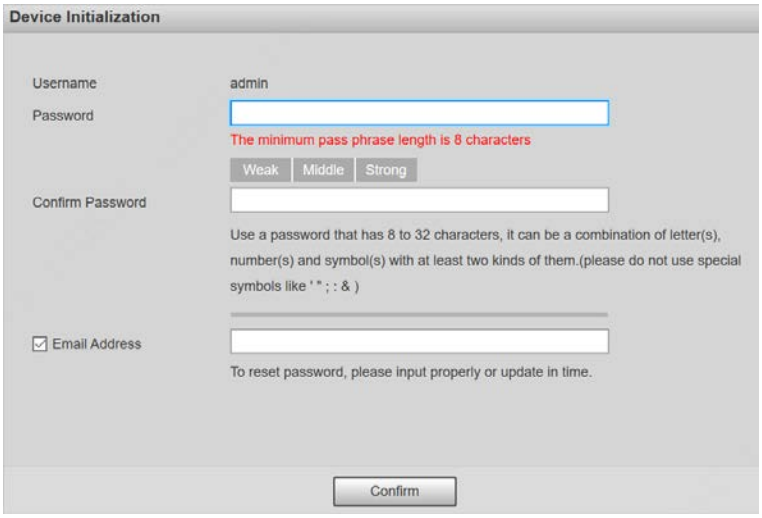
connected.

Step 3 Open the browser and enter the IP address of the Device, and then press Enter.

Step 4 Enter and confirm the password.

Change the password from **Setting** > **System** > **Account** > **Account** > **Username**. For details, see " Managing Users".

Figure 4-1 Device initialization



Step 5 Select **Email Address**, and then enter an email address.

The email address is used for resetting password.

Step 6 Click **Confirm**.

Step 7 Enter **Username** and **Password** on the login window, and then click **Login**.

The account will be locked for five minutes after five failed username or password attempts.

Step 8 On the **Live** page, click **Please click here to download and install the plug-in** to download and install the plug-in.

The **Live** page is normally displayed.

4.1.3 Resetting Password

When you forget the password, you can set a new password.

- You need to enter an email address during device initialization to receive the security code. Otherwise, password reset is not available. You can also change the email address from **Setting** > **System** > **Account** > **Account** > **Username**. For details, see "Managing Users".
- The password of a device can only be reset up to 10 times a day.
- You can only get two security codes for each QR code.
- Use the security code to reset the password within 24 hours after you receive it. Otherwise the security code will become invalid.

Step 1 Open the browser and enter the IP address of the Device, and then press Enter.

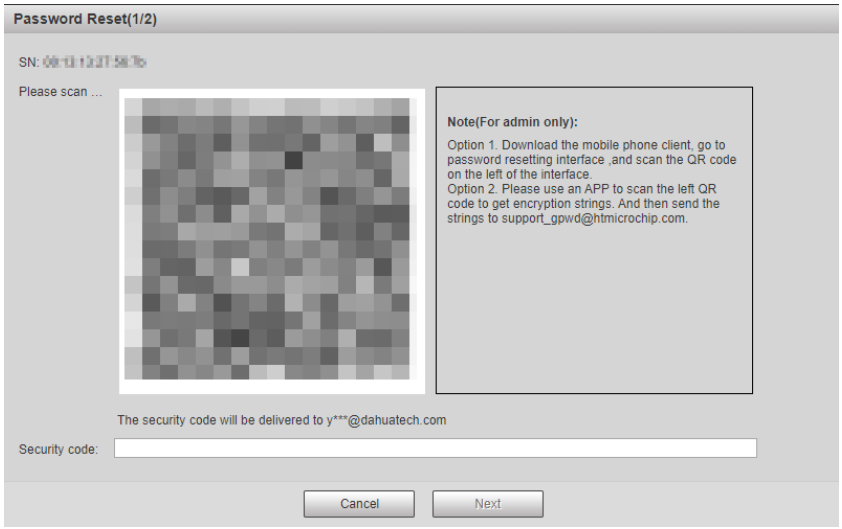
Step 2 Click **Forgot password?** on the login page, and then click **OK** in the pop-up window.

If Internet Explorer is used, **Stop running this script** is displayed. In this case, click **No** to continue to run the script.

Step 3 Scan the QR code, and the scan result will be sent to the reserved email.

Step 4 Send the received scan result to support_gpwd@htmicrochip.com through the reserved email address to get the security code.

Figure 4-2 Reset password (1)



Step 5 Enter the security code, and then click **Next**.

Step 6 Enter and confirm the new password.

Follow the password security prompt to set a password with a high security level.

Figure 4-3 Reset password (2)



Step 7 Click **OK**.

4.1.4 Webpage Functions

Figure 4-4 Tabs

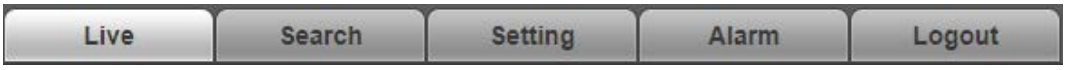


Table 4-2 Tab functions

Function	Content
Live	View the real-time videos and captures of the camera.
Search	Search for vehicles and recordings.
Setting	Configure intelligent traffic rules, the basic attributes of the Device, network settings, event management, storage management, system management, and view system information.
Alarm	Set alarm prompts.
Logout	Log out of the webpage.

The common buttons on the webpage are as follows.

Table 4-3 Common buttons

Button	Description
Default	Restores the parameter to the default value.
Refresh	Restores the parameter to the value saved last time.
Save	Saves current configurations.

4.2 Live

The **Live** page displays real-time videos of the connected cameras, real-time snapshots, and recognized plates.

4.2.1 Video and Picture

You can view the videos and snapshots of a channel and the details of captured vehicles.
Log in to the webpage, select **Live** > **Videos & Images**, and then click a channel.

Figure 4-5 Video and image



Table 4-4 Video/picture live view page description

No.	Module Name	Description
1	Channel	Select a channel for live view, and you can select to view live videos, pictures or both on the same page.
2	Live view	The real-time video of the selected channel.
3	Image window	Displays the snapshot of the recognized vehicle.
4	PTZ settings	Adjust the zoom, focus, iris and direction of the PTZ camera.
5	Image information	Displays the captured plate. You can select the upload type of pictures to the connected platform.
6	Event details	Displays the details of recognized violations.

4.2.2 Video

You can view the live video of multiple channels at the same time. Log in to the webpage, select **Live > Video**, and then click a channel, and the **Live** page of this channel is displayed. See Figure 4-6. The pane selected area on the page is the video window setting bar. See Figure 4-7. For icon description, see Table 4-5.

Figure 4-6 Live view

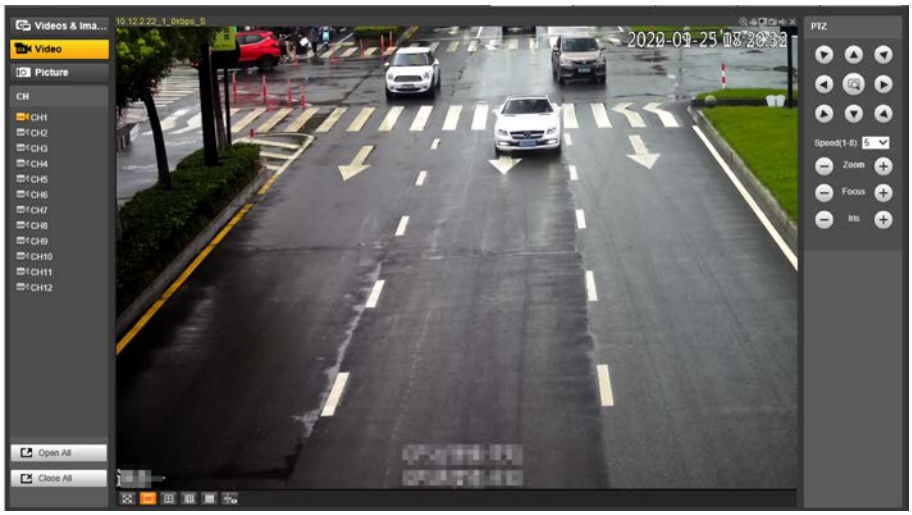


Figure 4-7 Video window setting bar



Table 4-5 Video window setting description

Icon	Name	Description
	Full screen	• Click the icon to switch to the full screen mode. • Double-click anywhere on the screen to exit the full screen.
	1 window	Default image display mode. Select any video channel in the list on the left side for live view directly in a single window.
	4 windows	Equally divide the live view window into 4, 9, and 16 windows. Live view channels and display positions can be customized. 1. Click a window to be set, and the border of this window turns green. 2. Select the channel number for live view in this window in the list on the left side. 3. Repeat the earlier steps for other windows until every window displays the required channel images.  Click **Open All** or **Close All** below the channel list to quickly open or close all channels, and the opened channels will be displayed in the order of channel numbers from left to right and top to bottom in the live view windows.
	9 windows	
	16 windows	
	Bounding box	Click the icon to display the smart tracks uploaded by the camera. Smart tracks such as non-motor vehicle and motor vehicle detection boxes are displayed on the video.  In **Setting** > **Add Camera** > **Add Camera**, select **RTSP** as the protocol type of main stream/sub stream of camera. The terminal device will not display smart track frames unless the address contains proto=Private3.

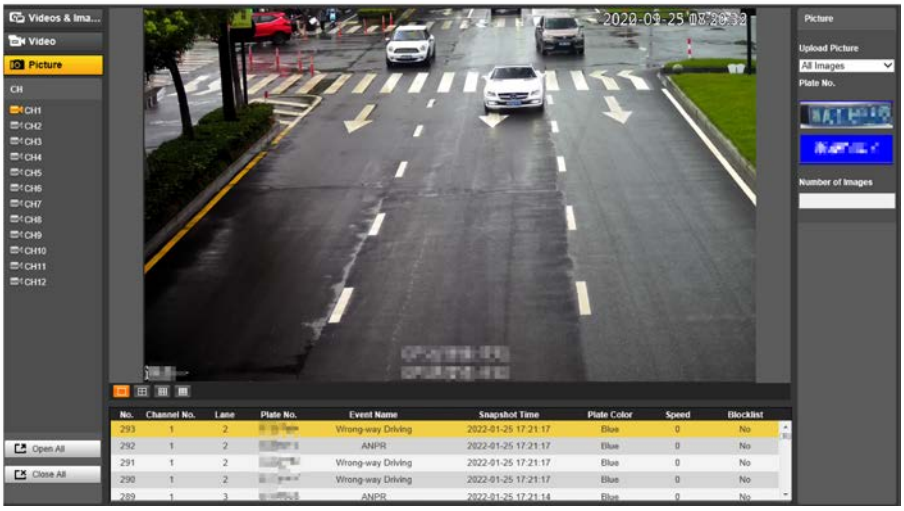
4.2.3 Picture

The live view of pictures of multiple channels at the same time is available. You can view details of captured vehicles.

Log in to the webpage, select **Live > Picture**, and then click a channel, and the **Picture** page of this channel is displayed.

See "4.2.1 Video and Picture" and "4.2.2 Video" for operations on this page.

Figure 4-8 Live view of picture



4.3 Data Search

You can set search conditions to search for vehicles or recordings, and set file or time as download type to download related data.

4.3.1 Searching for Vehicles

Step 1 Click **Search**, and then select **Vehicle**.

Step 2 Set vehicle search conditions.

1) Set basic parameters such as the period, channel and picture type.
2) Click **Advanced Options**, and then select detailed options as needed.

- When searching for records through plate numbers, fuzzy match is available.
- Multiple selections are available.

3) Select whether to only search for composed pictures and vehicles on the blocklist.

Step 3 Click **Search**.

Click a record on the list to view the picture on top.

Figure 4-9 Search for vehicles

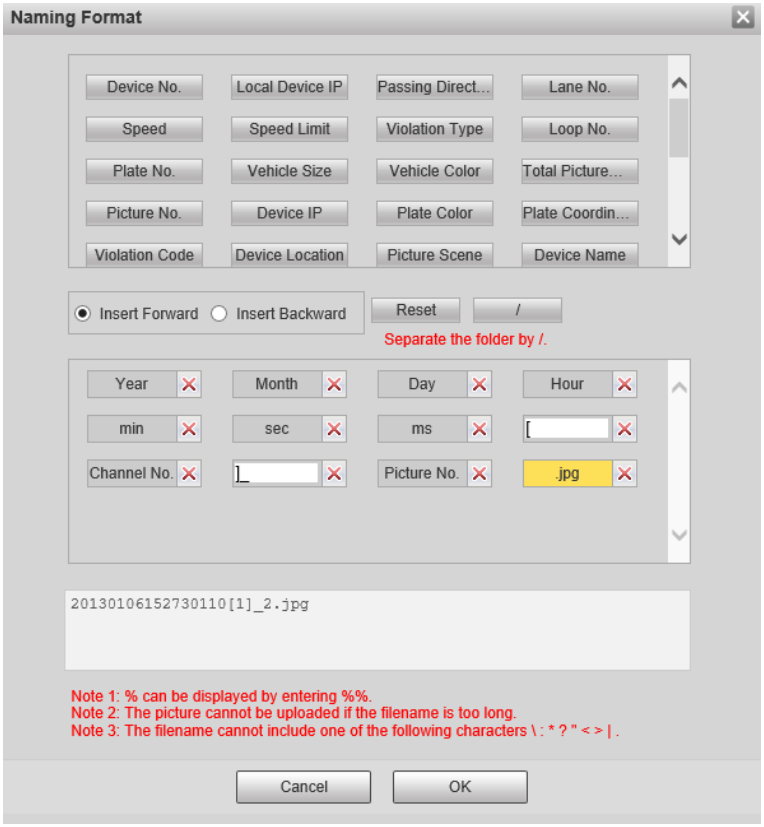


Step 4 Select the download type, and then click **Download**.

- **File**: Select one or more pictures to download from the search results.
- **Time**: Download all pictures taken during the set period.
- **Cutout Type**: Select the cutout type of pictures to be downloaded. When downloading pictures, the related cutout image will be separated and downloaded together.

Step 5 Click **Name Format for Downloaded Images**, click **Help** next to the corresponding picture type, and then customize the picture naming format in the pop-up window.

Figure 4-10 Picture naming format





You can add up to 76 items when setting the naming format.

Step 6 Select index number in the search results, and then click **Download**.

Step 7 Set the duration of **Record Linkage** and then download related records as needed.



Related records cannot be displayed until the camera and device are synchronized in time.

- Click **Open** to view the video. During playback, you can use the buttons on the progress bar to play, pause, stop, and quick play the video. During playback, the channel name, time, and other info of the record file are displayed in the video window.
- To download related records only, directly select index number in the search results, and then click **Download**.

4.3.2 Searching for Recordings

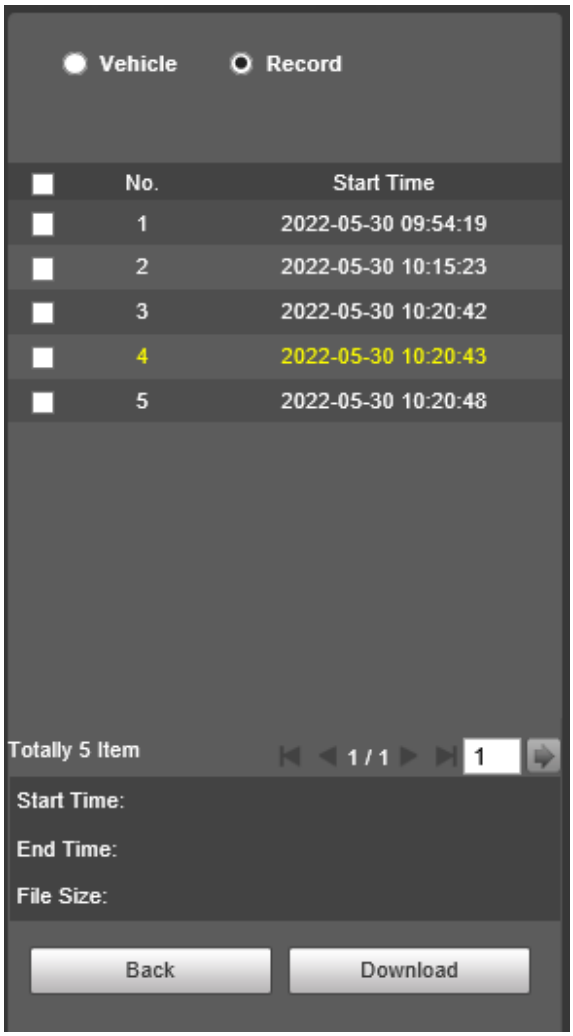
Step 1 Click **Search**, and then select **Record**.

Step 2 Set the query time and channel, and then click **Search**.



After the query time and channel are set, select **Time** in **Download Format**, and then click **Download** to directly download all recordings of the specified channel within this period.

Figure 4-11 Query results



Step 3 Double-click a query result to view the recording. Click the buttons on the play bar to control the playback.

Table 4-6 Description of playback buttons

Icon	Name
	Play/Pause
	Stop
	Slow down
	Speed up
	Play speed

Step 4 Select a recording, and then click **Download** to download the selected recording to local computer.

4.4 Setting

Set parameters of the Device, including intelligent traffic rules, network settings, remote devices, event management, storage management, system management, and system information, to realize functions such as image composition, speed measuring, network connection, data storage and alarm.

4.4.1 ITC

You can configure intelligent traffic parameters to provide functions such as image mosaic and OSD configuration.

4.4.1.1 Selecting Working Mode

Step 1 Select **Setting** > **ITC** > **Working Mode** > **Working Mode**.

Step 2 Select a **Scene Type**.

- **ANPR Image Composition**: Supports connecting with 12 cameras and receiving videos and snapshots from them. Image composition is available.
- **Video Access**: Supports connecting with 16 cameras and receiving videos and snapshots from them. Image composition is not available.

Step 3 Click **Save**.

The Device will restart after switching business types.

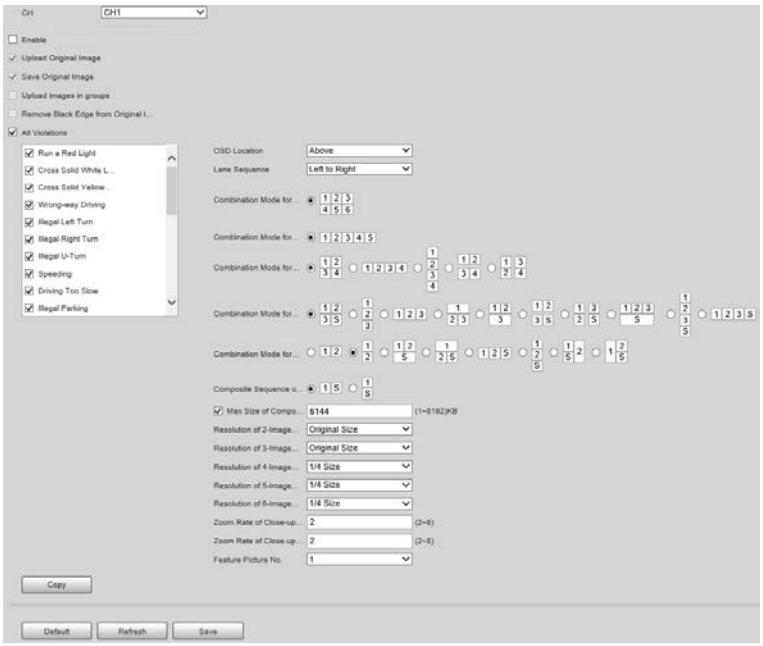
4.4.1.2 Image Mosaic

4.4.1.2.1 Normal Combination

Select violation types, set the combination sequence, picture size, and other parameters to form a picture combined with the information you set.

Step 1 Select **Setting** > **ITC** > **Snapshot Synthesis Config** > **Picture Synthesis**.

Figure 4-12 Picture synthesis



Step 2 Select a channel to be set in **CH** as required.

Step 3 Select **Enable** to enable image mosaic.

Step 4 Select **Upload Original Image** as required. If it is unselected, no original picture is uploaded in the corresponding channel on the live view page.

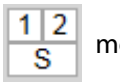
Step 5 Select **Upload images in groups**, original images will be temporarily saved and uploaded together with combined images. There is no time difference between the original image and combined image.

Step 6 Select **Remove Black Edge from Original Image** as required.

Step 7 Under **All Violations**, select the violation type to enable the combination.

Step 8 Set other parameters.

Table 4-7 Snapshot combination parameters

Parameter	Description
OSD Location	Select the location where OSD information is overlaid on the combination picture. Select **Above** or **Below**, or select **None** without OSD information overlay.
Combination Mode	Select the correspondence between sequence and location according to the picture sequence of 1→2.  means that the combination pictures are arranged in order from left to right and top to bottom. S means that there is a feature in the combination pictures, and it is the enlarged feature of a snapshot. The sequence can be switched at will. Take horizontal 12 as an example, you can delete the numbers and enter 21.

Parameter	Description
Max Size of Composite Image	Select it to enable picture size limit, and set the maximum number of KBs of combination pictures. It is selected by default.  When this function is enabled, the picture compression ratio setting is invalid. ● If it is selected, when the combination picture is larger than 6,144 KB, it will be automatically compressed to nearly 6,144 KB and displayed on the webpage. ● If it is not selected, when the combination picture is larger than 8,192 KB, it will be automatically stored in the HDD and will not be displayed on the webpage.
Resolution of X-Image Composite	Set the resolution of the combination picture according to the number of pictures.
Zoom Rate of Close-up Image for Large Vehicle	Set the feature multiple of big car and small car respectively. Value range: 2–8.
Zoom Rate of Close-up Image for Small Vehicle	
Feature Picture No.	Select the serial number of original pictures that require feature.

Step 9 Click **Copy** to copy the snapshot combination strategy to another channel in the pop-up window. After selection, click **Save**.

Step 10 Repeat the earlier steps, and select other channel numbers to set the combination method of other channels.

Step 11 Click **Save**.

4.4.1.2.2 Related Composition

Based on the selected scheme and matching method, you can link multiple channels, and compose or group the snapshots of the channels on the related composition page.

Prerequisites

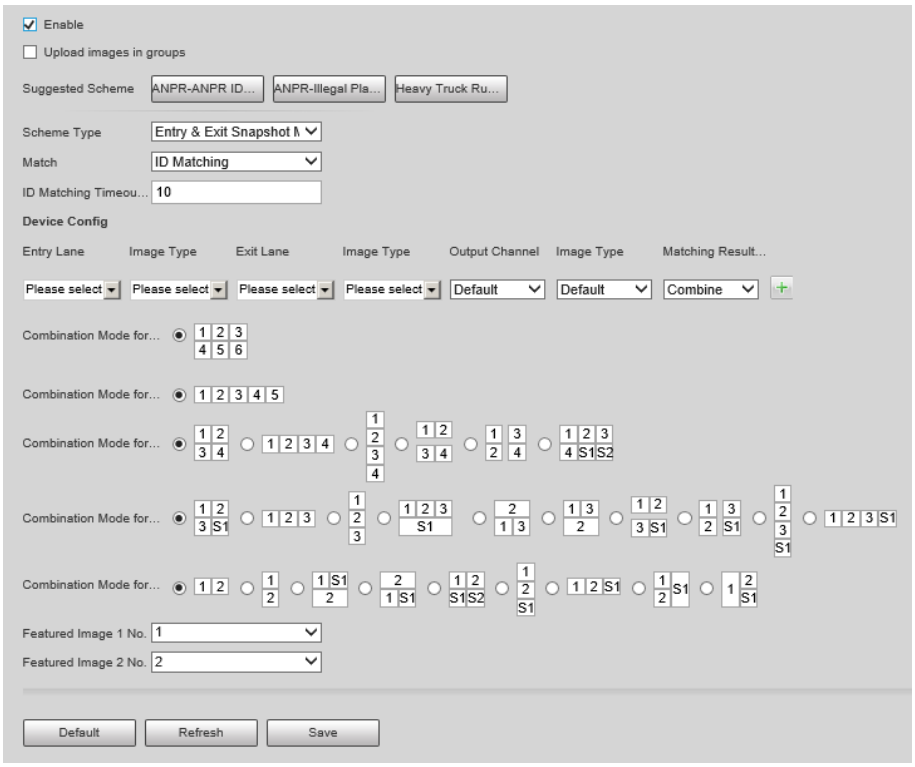
Related composition is only available when normal combination of the channels is enabled. For details, see "4.4.1.2.1 Normal Combination".

Procedure

Step 1 Select **Setting** > **ITC** > **Snapshot Synthesis Config** > **Related Composition**.

Step 2 Select **Enable** to enable the function.

Figure 4-13 Related composition



Step 3 Select scheme type.

- **Entry & Exit Snapshot Match**: The Device links and matches the snapshots captured in entry and exit channels. ID matching and plate matching are available.
- **Three Channels Matching**: The Device matches (ID matching) the snapshots of the entry and auxiliary channels, and then matches (plate matching) the snapshots of the entry and exit channels to link the three channels.
- **Multiple Channels Matching**: The Device links and matches snapshots of multiple channels. ID matching and plate matching are available.

Step 4 Select matching type and matching timeout duration.

Table 4-8 Composition method description

Parameters	Description
ID Matching	Suitable for composing snapshots of false-registered vehicles. Match snapshots of multiple cameras based on the same image ID.
By Plate No.	Match snapshots of multiple cameras based on the same plate.
ID First & License Plate Second	The Device matches (ID matching) the snapshots of the entry and auxiliary channels, and then matches (plate matching) the snapshots of the entry and exit channels to link the three channels. Only available when setting **Scheme Type** to **Three Channels Matching**.
ID Matching Timeout	The maximum waiting period for snapshot composition. When the time interval between the vehicle passing the front and back cameras exceeds the defined value, the Device does not compose snapshots.
Plate Matching Timeout	

Parameters	Description
Fuzzy Matching	Enable fuzzy match, set the valid period and auxiliary information such as plate color, vehicle color, lane and more. Multiple selections are available. After enabling fuzzy match, the Device searches for snapshots latest captured within the valid period and conform to selected auxiliary information items, and match them when plate matching failed. - Fuzzy match is only available when plate matching fails. - You need to configure the channels based on the capture sequence when enabling fuzzy match. For example, channels receive snapshots first are configured as entry channel, and later ones are exit channels.

Step 5 Configure matching scheme. Configure the input channel number, image type and output channel number and image type after matching. You also need to select image processing method from **Combine** and **Group**. This section uses matching of entry and exit lanes as an example.

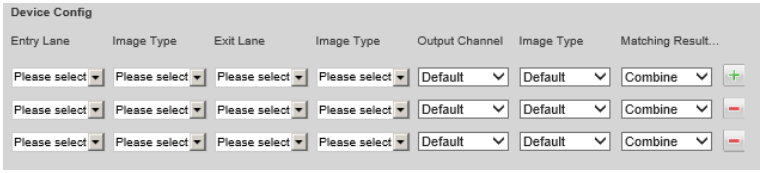
Table 4-9 Composition scheme

Config Items		Description
Drive-in Lane	Entry Lane	The channel number of the camera on drive-in lane. Multiple selections are available. When there are multiple cameras on drive-in lane to capture multiple lanes, you can select channels matching with output channels as needed.
	Image Type	Select picture type supported by related composition. Multiple selections are available.
Drive-out Lane	Exit Lane	The channel number of the camera on drive-out lane. Multiple selections are available. When there are multiple cameras on drive-out lane to capture multiple lanes, you can select channels matching with input channels as needed.
	Image Type	Select picture type supported by related composition. Multiple selections are available.
Output Channel	Output Channel	Select channel to output processed snapshots after successful match of drive-in and drive-out lanes. Default setting means that 1. If the picture type of entry lane is ANPR, and that of exit lane is violation, the processed image will be output through violation channel. 2. For other situations, the processed images are output through the channel of entry lane when successfully matched.

Config Items		Description
	Image Type	Select picture type for outputting processed snapshots after successful match of drive-in and drive-out lanes. Default setting means that 1. If the picture type of entry lane is ANPR, and that of exit lane is violation, the processed image is violation image. 2. For other situations, the processed images are output as the same picture type as entry lane when successfully matched.
	Matching Result Processing	The processing method for snapshots after successful match. ● Combination: Compose multiple snapshots to one. ● Group: Group multiple snapshots to one group.

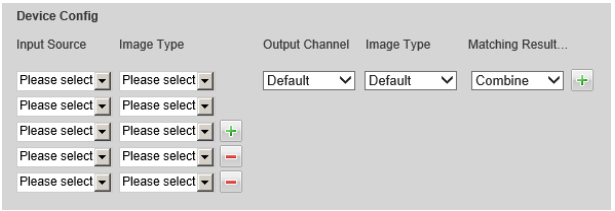
1. Matching scheme configuration is available for every matching method. Schemes are independent and cannot repeat.
2. You can configure up to eight schemes for each matching method.
   - Click + to add matching schemes.
   - Click − to delete matching schemes.

Figure 4-14 Composition scheme add/delete



3. When setting **Scheme Type** to **Multiple Channels Matching**, you can customize the number of channels (at most 6).
   - Click + to add matching schemes.
   - Click − to delete matching schemes.

Figure 4-15 Input source add/delete



Step 6 Set the composing sequence of multiple snapshots. For details, see Table 4-7.
Set the featured image number.

Step 7 Click **Save**.

Select an option from **Suggested Scheme** to automatically configure scheme type, matching type and matching scheme.

Table 4-10 Suggested scheme

Scheme	Scenes
ANPR-ANPR ID	Using ID matching to match and compose the snapshots of ANPR on the drive-in and drive-out lanes. The entry and exit lanes are channel 1 and channel 2 respectively by default. You can change it as needed.
ANPR-Illegal Plate	Using plate matching to match and compose the snapshots of ANPR on the drive-in lane and violations on the drive-out lane. The entry and exit lanes are channel 1 and channel 2 respectively by default. You can change it as needed.
Heavy Truck Running a Red Light	Using plate matching to match and compose the snapshots of ANPR on the drive-in lane and Run a Red Light on the drive-out lane. Enable fuzzy match for recognizing heavy truck plate. The entry and exit lanes are channel 1 and channel 2 respectively by default. You can change it as needed.

When setting **Matching Result Processing** to **Combine**, the number of original images cannot exceed 6.

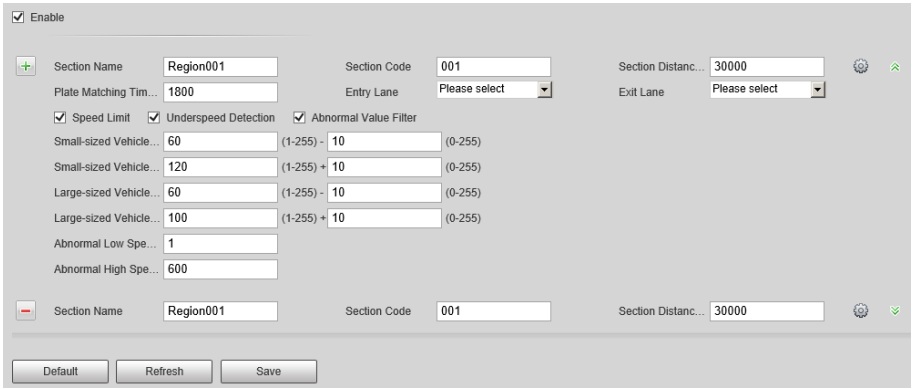
4.4.1.3 Measuring Section Speed

Set section distance, entry lane, exit lane, speed limit and other parameters, section speed measurement function can calculate the average speed of the vehicle based on the section distance and passing time. Compare with the defined speed limit, and compose the original images when the Device judges the vehicle is overspeed or underspeed.

Step 1 Select **Setting** > **ITC** > **Section Speed Measurement**.

Step 2 Select **Enable** to enable the function.

Figure 4-16 Section speed measurement



Step 3 Configure parameters.

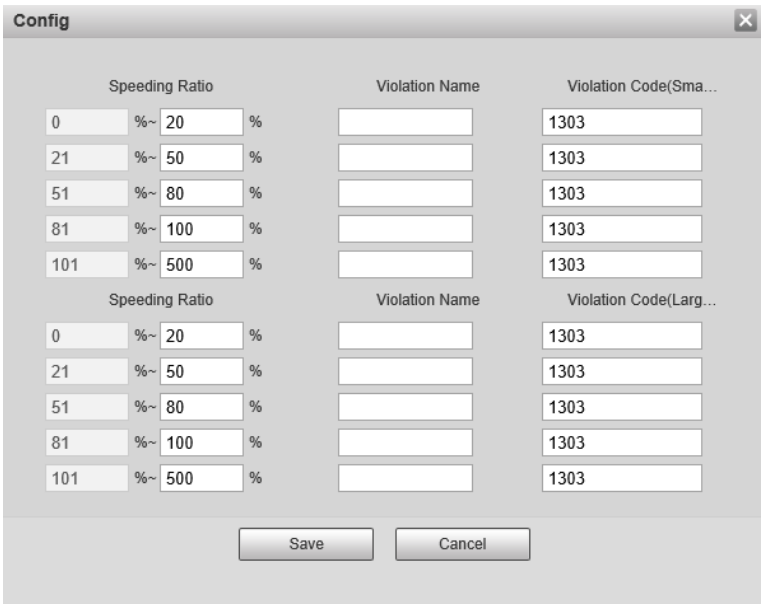
Table 4-11 Parameter description

Parameter	Description
Section Name	Set section name and code.
Section Code	
Section Distance	Enter the section distance (unit: m).

Parameter	Description
Plate Matching Timeout(s)	Set the plate matching timeout duration for snapshots captured by cameras on the entry and exit lanes when vehicle passes. The Device will not match images if the duration is exceeded. ● When only enabling overspeed detection (enabled by default), the duration must be longer than the time the vehicle needs to pass the section at the limited high speed. ● When enabling **Underspeed Detection**, the duration must be longer than the time the vehicle needs to pass the section at the limited low speed.
Entry Lane	The channel number of the camera on the section entry. Multiple selections are available. If there are multiple cameras, you can select multiple channels as needed.
Exit Lane	The channel number of the camera on the section exit. Multiple selections are available. If there are multiple cameras, you can select multiple channels as needed.
Speed Limit	Enable speed limit, and you can set speed limit for both large and small vehicles respectively.
Underspeed Detection	Enable the function to set the low speed limit and detect vehicles running at a speed lower than the defined value while passing the section.
Abnormal Value Filter	Enable the function to set the abnormal value, and the Device filters measuring results lower than the low speed limit or higher than the high speed limit.
Small-sized Vehicle Lowest Speed Limit	Consists of low speed limit and high speed limit. When the section speed is lower than the low speed limit, meaning the vehicle is underspeed, and higher means overspeed.
Small-sized Vehicle Highest Speed Limit	
Large-sized Vehicle Lowest Speed Limit	
Large-sized Vehicle Highest Speed Limit	
Abnormal Low Speed	The Device defines and filters the result that is lower than the defined value.
Abnormal High Speed	The Device defines and filters the result that is higher than the defined value.

Step 4 Click ⚙ to set the illegal name and code as needed.

Figure 4-17 Configure overspeed ratio



Step 5 Click **Save**.

The Device supports multiple groups of section speed measurement, and parameters of them are independently configured.

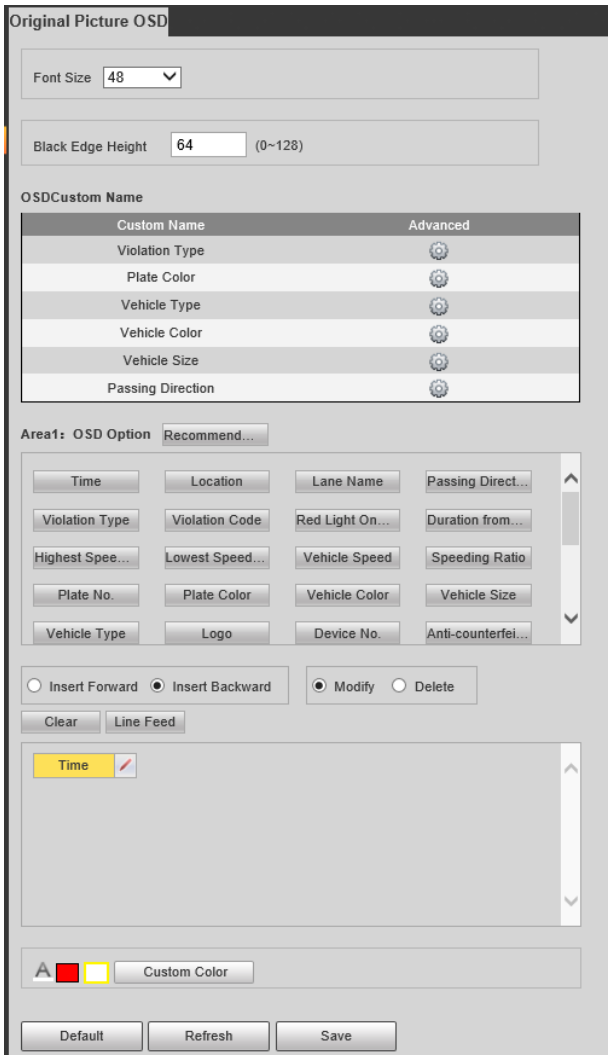
- Click + to add sections.
- Click − to delete sections.

4.4.1.4 Setting Snapshot OSD

You can set the OSD information of snapshots.

Step 1 Select **Setup** > **ITC** > **OSD** > **Orginal Picture OSD**.

Figure 4-18 Orginal Picture OSD



Step 2 Set **Front Size** and **Black Edge Height**.

Step 3 Select the information to be displayed on the picture in the **OSD Option** area.

Step 4 Set the sequence and line feed of OSD options. Click  to modify the prefix, suffix, and number of separators of each OSD option.

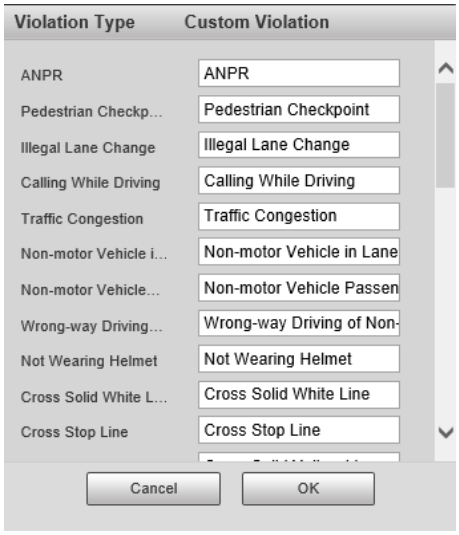
Click **Recommend Overlay** for quick configuration.

Step 5 Select font color as required, or click **Custom Color** to set the required font color.

Step 6 (Optional) Set **OSDCustom Name** as required. **Violation Type** is used as an example in this section.

1) Click **Advanced** corresponding to **Violation Type** .

Figure 4-19 Details of violation type parameters



2) Modify the parameters as required.
   For example, change the parameter **(Parking Space) Available** to **(Parking Space) Empty**, the OSD on the composite pictures for **(Parking Space) Available** will be overlaid as **(Parking Space) Empty**.
3) Click **OK**.

Step 7 Click **Save**.

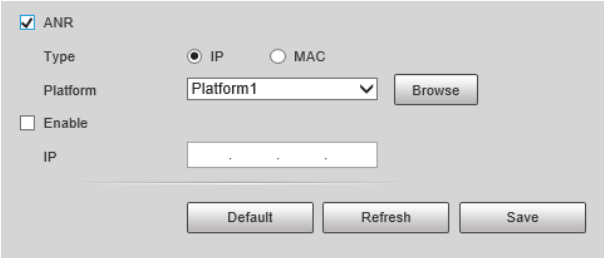
4.4.1.5 Automatic Network Recovery

Enable automatic network recovery (ANR). When the Device is disconnected from the platform and reconnected to it, the Device continues to upload the pictures during the offline period to the platform. You can select IP or MAC for **Type**.

Step 1 Select **Setting** > **ITC** > **ANR**.

Step 2 Select **ANR** to enable this function.

Figure 4-20 ANR



Step 3 Configure parameters.

Table 4-12 ANR parameters

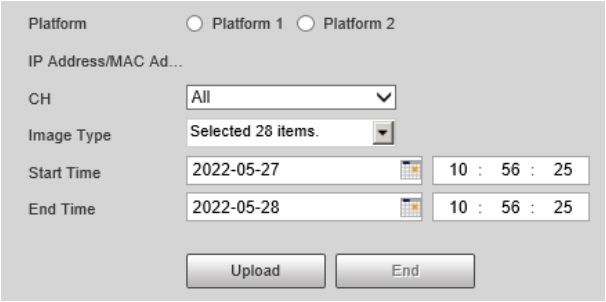
Parameter	Description
Type	Select the platform identification type. ● IP: The system identifies the upload platform through IP address. ● MAC: The system identifies the upload platform through MAC address.
Platform	Select a platform for transfer. Click **Browse** to search for the current online platforms.

Parameter	Description
IP/MAC address	Enter IP/MAC address. ● When IP is selected, enter the IP address of the platform for transfer. ● When MAC is selected, enter the MAC address of the platform for transfer.
Enable	Enable visualization to display platform label and upload time on the corresponding vehicle data list.

Step 4 Click **Save**.

Step 5 Click **Manual Upload** tab, select a target platform and enter its IP address, select a channel, picture type and time period to upload snapshots taken during the set period to the specified platform.

Figure 4-21 Manual upload



Step 6 Click **Upload**.

During the upload, click **End** to stop uploading.

4.4.1.6 Allowlist and Blocklist

Set the allowlist and blocklist of vehicles. Linked actions will be triggered when vehicles on the lists are detected.

- Allowlist: When vehicles on the allowlist are detected, the Device discards the captured vehicle violation pictures without any processing.
- Blocklist: When vehicles on the blocklist are detected, the Device triggers linked actions.

4.4.1.6.1 Setting Allowlist

You can set the allowlist of plate numbers. When vehicles in the allowlist are detected, the Device discards the captured vehicle violation pictures without any processing.

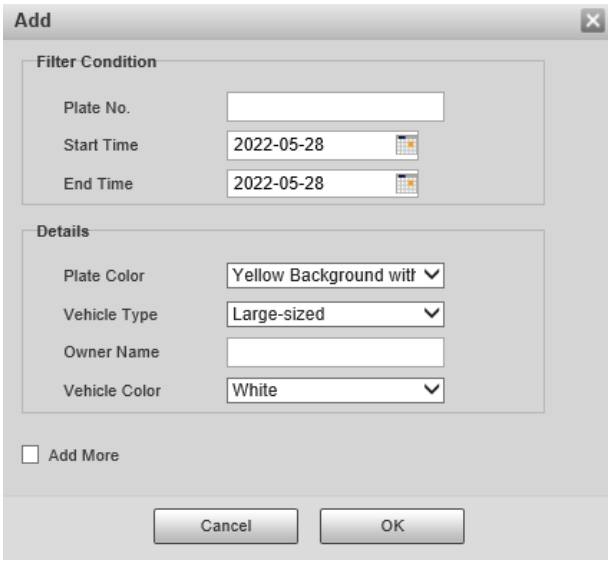
Procedure

Step 1 Select **Setting** > **ITC** > **Vehicle Blocklist/Allowlist** > **Allowlist**.

Step 2 Add allowlist.

- Add one by one.
  1. Click **Add**.
  2. Set filter conditions and detail info.

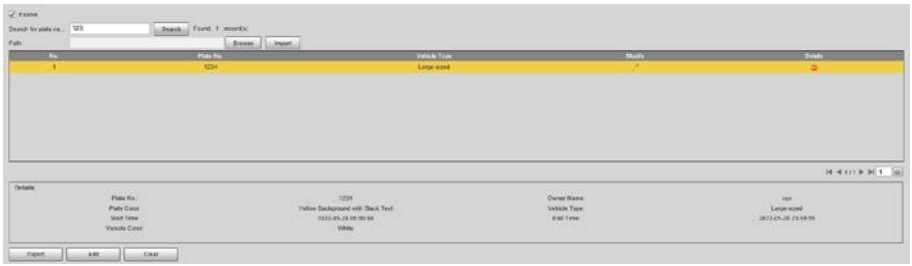
Figure 4-22 Add an item to the allowlist



3. Click **OK**. The allowlist is added successfully, and the added allowlist is displayed.

Select **Add More**, and click **OK** to save the added allowlist information and add more.

Figure 4-23 Allowlist



- Add in batches
  1. Click **Export** to download and fill in the allowlist template.
     See "Appendix 1 Reference for Filling in Allowlist and Blocklist Template" for how to fill in the corresponding number of plate color, plate type, vehicle color, and vehicle type.

Table 4-13 Allowlist import table

Begin Time	Cancel Time	Owner Of Car	Plate Color	Plate Number	Vehicle Color	Vehicle Type
2019/5/15 00:00	2019/5/15 23:59	Zhang San	1	Zhejiang A****	A	1

  2. Click **Browse**, and then select the allowlist table you want to import.
  3. Click **Import** to import the allowlist table, and then **Successfully imported** is displayed.

Related Operations

- Enter a several-digit field in the plate number, and click **Search** to search for plate numbers containing this field in the allowlist.
- Click  to modify allowlist parameters.

- Click  to delete a single allowlist.
- Click **Export**, and then select encryption if needed and then follow the prompts to save the allowlist.
- Click **Clear** to delete all allowlists.

4.4.1.6.2 Setting Blocklist

Set the blocklist of plate numbers. When vehicles in the blocklist are detected, the Device triggers the actions linked with the alarm.

Select **Setting** > **ITC** > **Vehicle Blocklist/Allowlist** > **Blocklist**. The setting of blocklist is similar to that of allowlist. See "4.4.1.6.1 Setting Allowlist" for details.

4.4.1.7 Traffic Flow

You can search for traffic flow data and view the real-time traffic flow.

Step 1 Select **Setting** > **ITC** > **Traffic Flow Statistics** > **Flow Query**.

Step 2 Set the time period and select a channel, and then click **Search**.

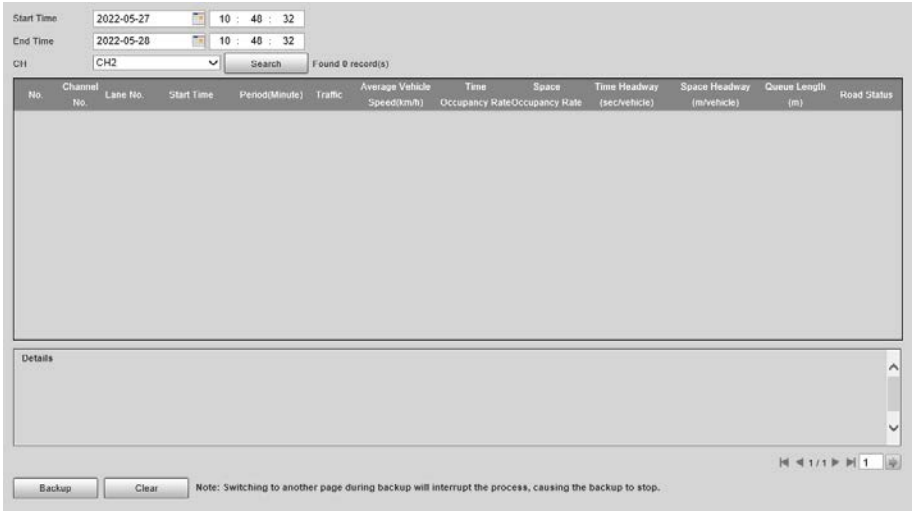
Select a record, and you can view the details at the bottom.

- Click **Backup** to save the results.
- Click **Clear** to delete all information.



- Switch to other pages during backup, and the backup will stop.
- **Clear** refers to delete all data from the database.

Figure 4-24 Search for traffic flow data



Step 3 Click **Flow Data** tab to view the flow data of the corresponding channel in real time.

4.4.1.8 Watermark Verification

You can verify whether the local pictures and videos were tampered with by checking the watermark.

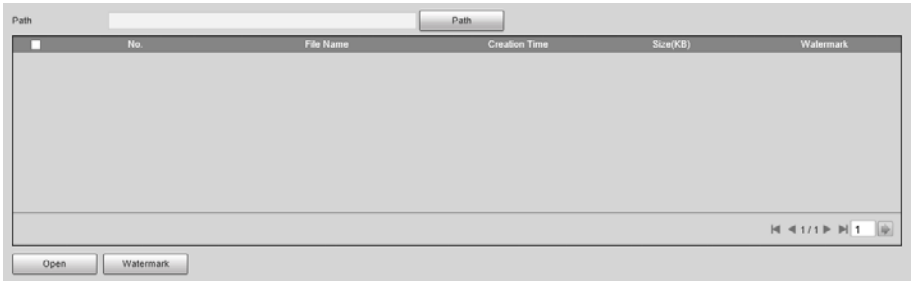
4.4.1.8.1 Picture Verification

You can verify whether the local pictures were tampered with.

Step 1 Select **Setting** > **ITC** > **Watermark** > **Picture**.

Step 2 Click **Path**, select the folder where the picture to be verified is located, and then click **OK**. All pictures in this folder directory are automatically displayed.

Figure 4-25 Picture watermark verification



Step 3 Select one or more pictures to be verified from the list, and then click **Watermark**. Check the verification results on the right side of the list.

- When the result is **Error**, the picture is tampered.
- When the result is **Normal**, the picture is not tampered.

Step 4 Click **Open** to open the selected picture.

4.4.1.8.2 Video Verification

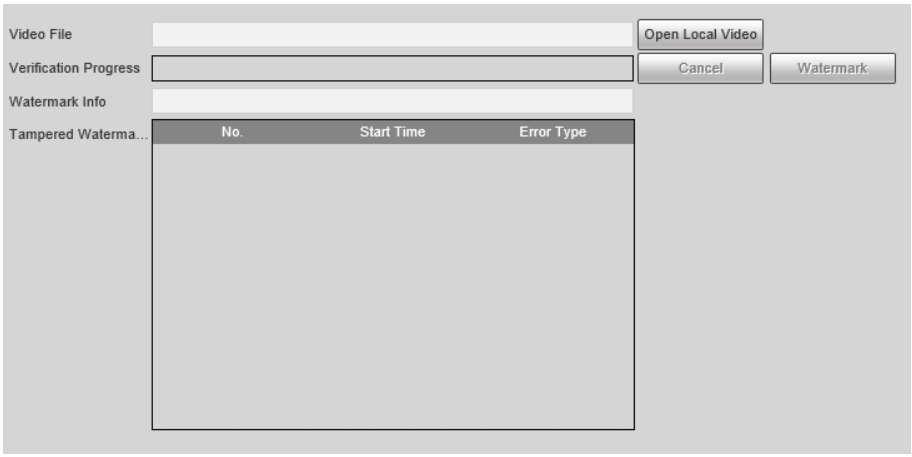
Verify whether the local records were tampered with.

Step 1 Select **Setting** > **ITC** > **Watermark** > **Video**.

Step 2 Click **Open Local Video**, select the record to be verified through the file path, and then click **Watermark** to check the verification results.

- If the video is verified to be authentic, the watermark you set is displayed next to **Watermark Info**.
- If the video is tampered, you can check the details next to **Tampered Watermark Info**.

Figure 4-26 Video



4.4.2 Network Settings

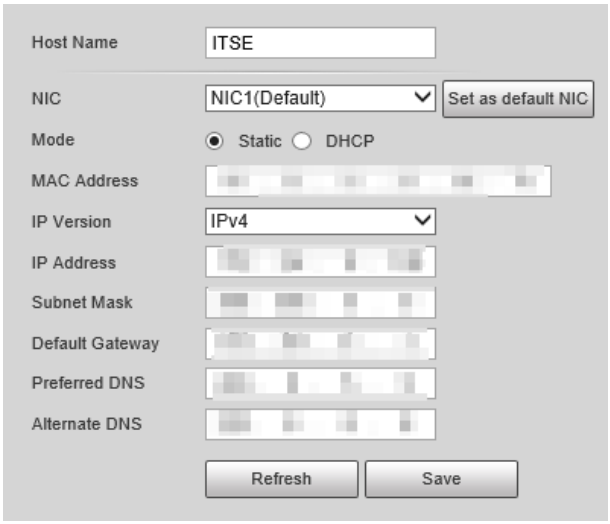
You can set the network parameters of the Device.

4.4.2.1 TCP/IP

You can set the IP address, DNS server and other parameters of the Device to make sure that the Device is connected to other devices on the network.

Step 1 Select **Setting** > **Network Settings** > **TCP/IP**.

Figure 4-27 TCP/IP



Step 2 Configure parameters.

Table 4-14 TCP/IP parameters

Parameter	Description
Host Name	Set the name of the current host, with a maximum length of 15 characters.
NIC	Dual Ethernet cards are supported. Select an Ethernet card and then click **Set as default NIC** to set it to the default.
Mode	Select a network mode. ● DHCP mode: Automatically obtains the IP address. The **IP Address**, **Subnet Mask**, and **Default Gateway** cannot be set when DHCP is enabled. You can check the current IP address regardless if the DHCP takes effect. ● Static mode: Manually set **IP Address**, **Subnet Mask**, and **Default Gateway**, and then click **Save**. The webpage will automatically go to the login page of the set IP address.
MAC Address	MAC address of the host, which cannot be modified.
IP Version	Only IPv4 is supported.
IP Address	Enter IP address.
Subnet Mask	Set a subnet mask as needed. The subnet prefix is a number in the range from 1 through 255. The subnet prefix identifies a specific network link and usually contains a hierarchical structure.
Default Gateway	Set a default gateway on the same network segment as the IP address as needed.
Preferred DNS	IP address of DNS.
Alternate DNS	IP address of the alternate DNS.

Step 3 Click **Save**.

4.4.2.2 Port

4.4.2.2.1 Port

You can set the information of the connected ports to access the Device through different protocols and configuration tools.

Step 1 Select **Setting** > **Network Settings** > **Port** > **Port**.

Step 2 Set the maximum number of clients accessing the Device at the same time (such as webpage and platform client) and each port value of the Device.

Figure 4-28 Port



Step 3 Click **Save**.

4.4.2.2.2 ONVIF

Enable ONVIF, and then network video products produced by different manufacturers can communicate with each other.

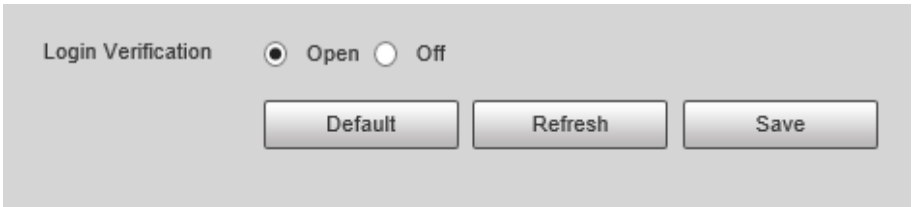
Login verification is required by default when ONVIF is enabled.

Step 1 Select **Setting** > **Network Settings** > **Port** > **ONVIF**.

Step 2 Select **Open** or **Off** as needed.

- By turning on ONVIF, login username and password are required when logging in through ONVIF
- Login verification is not required when turning off ONVIF.

Figure 4-29 ONVIF



Step 3 Click **Save**.

4.4.2.3 Auto Registration

Configure auto registration, and the current device location will be reported on automatically to the server specified by the user when the Device is connected to internet, so that the client software can

use the server to access the Device, and the server can perform operations such as live view, monitoring, and configuration of the parameters of the Device.

Step 1 Select **Setting** > **Network Settings** > **Register**.

Step 2 Select **Enable** to enable auto register, and then enter the address, port, and sub-device ID.

Figure 4-30 Auto registration

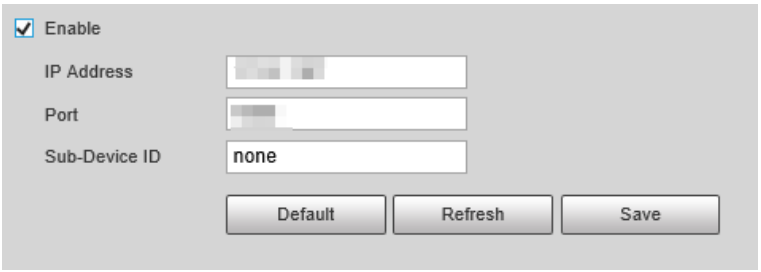


Table 4-15 Auto register parameters

Parameter	Description
IP Address	Server IP address or server domain that you want to register to.
Port	Port of the server for auto register.
Sub-Device ID	ID of the automatically registered device assigned by the server. Ensure that the ID of the automatically connected device is unique during configuration.

Step 3 Click **Save**.

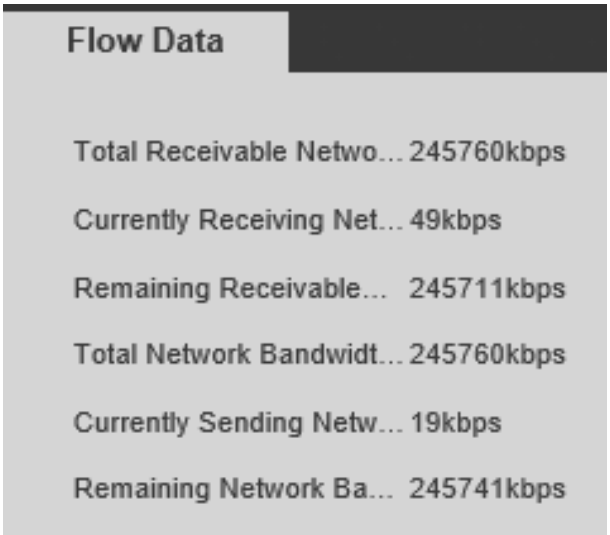
4.4.2.4 Flow Statistics

You can view the flow state of the Device, including flow receive ability, flow channel insert, flow receive remain, flow remote ability, flow remote live, and flow remote remain. Technicians can troubleshoot network problems according to the statistical data.

Select **Setting** > **Network Settings** > **Flow Data** > **Flow Data** to view flow statistics.

When **Remaining Receivable Network Bandwidth** and **Remaining Network Bandwith Can be Set** are negative numbers (in red), it means that these items have exceeded device performance limits, resulting in possible loss of some data and other problems. You can reduce the stream size, picture quality, or number of access channels to solve this problem.

Figure 4-31 Flow data



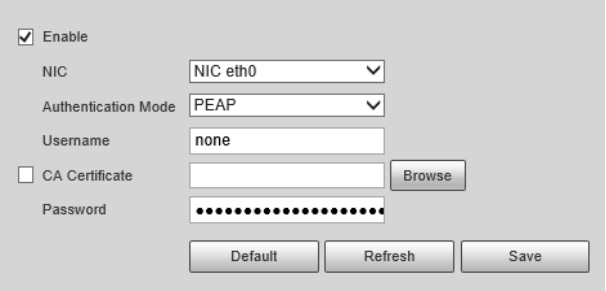
4.4.2.5 802.1x

802.1x is a port-based access control and authentication protocol, which can restrict unauthorized devices or users from accessing the LAN through the access port. When the switch in the network is configured with 802.1x, the Device also needs to be set to 802.1x, otherwise users cannot access the Device through the network.

Step 1 Select **Setting** > **Network Settings** > **802.1x**.

Step 2 Select **Enable**, and then select an Ethernet card. The 802.1x protocol of the NIC is enabled.

Figure 4-32 802.1x



Step 3 Leave the **Authentication Mode** as default, and then enter the username and password for authentication. The username must be the one authorized on the server side.

Step 4 Select **CA Certificate**, click **Browse** to select the CA certificate from local computer. Contact technical support to obtain the CA certificate.

Step 5 Click **Save**.

4.4.2.6 Routing Settings

The Device supports configuring routings for dual NICs, and accessing gateways of target network segments.

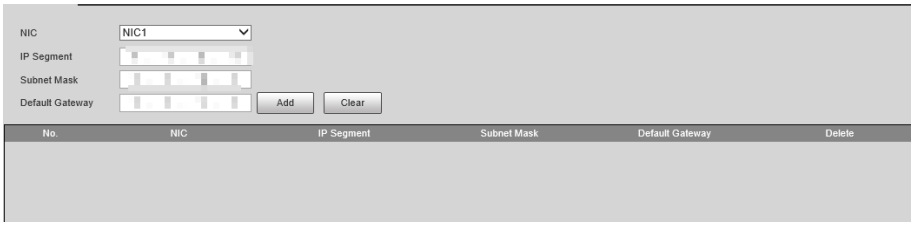
Step 1 Select **Setting** > **Network Settings** > **Route Settings**.

Step 2 Select Ethernet card and enter IP segment, subnet mask and default gateway.

Step 3 Click **Add**, **Save Succeeded** appears at the bottom and the routing is added to the list.

- Click to delete routing one by one.
- Click Clear to quickly delete all added routings.

Figure 4-33 Routing settings



4.4.3 Remote Device

Remote device (such as enforcement camera or IP camera) information will be displayed on the **Add Camera** page if any of such devices are in use. You can enable the remote device to work with the Device to capture the events.

4.4.3.1 Remote Device

You can add cameras to the Device.

Step 1 Select **Setting** > **Add Device** > **Add Device**.

Step 2 Enable channels.

- Select **Enable All Channels** to enable the remote device of all channels.
- After selecting a single channel, select **Enable** to enable the remote device of this channel.

Step 3 Set parameters.

Figure 4-34 Remote device

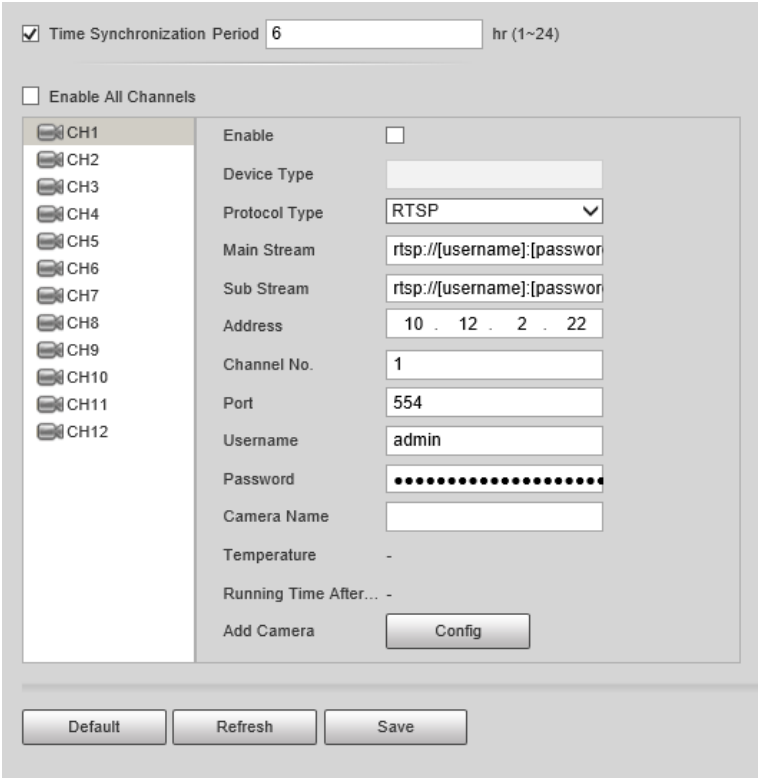


Table 4-16 Remote device parameters

Parameter	Description
Time Synchronization	Select to enable **Time Synchronization** to synchronize time with front-end equipment according to the set period.
Period	Set the timing period (hours).
Device Type	Display camera model.
Protocol Type	Select the protocol type of the Device, including private protocol, RTSP and ONVIF. • **RTSP**: Real Time Streaming Protocol, which defines how one-to-many applications effectively transmit multimedia data through the IP network. • **ONVIF**: A general protocol that defines information exchange between network video devices. • **Private Protocol**: Supports remotely operating on devices that work under the private protocol.
Main Stream Sub Stream	Set the address of main stream and sub stream of channels. The setting is available only when the protocol type is **RTSP**. When **RTSP** is selected as the protocol type, and the address contains proto=Private3, the terminal device can display smart track frames.
Address	Enter the IP address of the camera.
Channel NO.	Set the channel number to **1** for normal cameras and **1** or **2** for dual-channel cameras.

Parameter	Description
Port	• When the protocol type is RTSP, the port number is 554 by default. • When the protocol type is ONVIF, the port number is 80 by default.
Username	Enter the username and password of the remote device.
Password	
ONVIF User	Enter the username and password of ONVIF.  The setting is available only when the protocol type is **ONVIF**.
ONVIF Password	
Camera Name	It will be displayed in the channel name on the live view page after it is set.
Temperature	Display the current temperature of the Device.
Running Time After Power On	Display the running time of the Device.
Add Camera	Click **Config** to go to the setting page of the camera.

Step 4 Click **Save**.

4.4.3.2 Device Search

You can set search conditions to search for devices, and add the Devices to a channel.

- The search function on this page can only be used for devices on the same LAN.
- Only initialized devices can be added.

Step 1 Select **Setting** > **Add Camera** > **Search**.

Figure 4-35 Device search



Step 2 Multiple search modes are available on the **Search** page.

- Click **Search** to search for all devices on the same LAN.
- Select **IP Address** and enter the address, and then click **Search** to accurately search for devices with the IP address. Fuzzy search is supported.
- Select **IP Segment** and enter the network segment, and then click **Search** to search for all devices on the network segment.
- Select **MAC Address** and enter the address, and then click **Search** to accurately search for devices with the MAC address. Fuzzy search is supported.
- Select **Uninitialized** to view uninitialized devices on the list.

Step 3 (Optional) Select an uninitialized device, and then click **Initialize** to initialize it.

Step 4 Add devices.

1) Select the Device to be added from the list, and then click **Add**.
2) Enter the username and password of the Device.

Figure 4-36 Setting account



3) Set the channel number of remote device. Set the channel number to **1** for normal cameras and **1** or **2** for dual-channel cameras.
4) Click **Save**.

If the selected IP address already exists, there is a prompt showing whether to add repetitively. Select as required. If it is selected, the same IP address will be added repetitively. If it is unselected, only non-repetitive IP addresses are added. Click **Save**. Click **Cancel**, and no IP address is added.

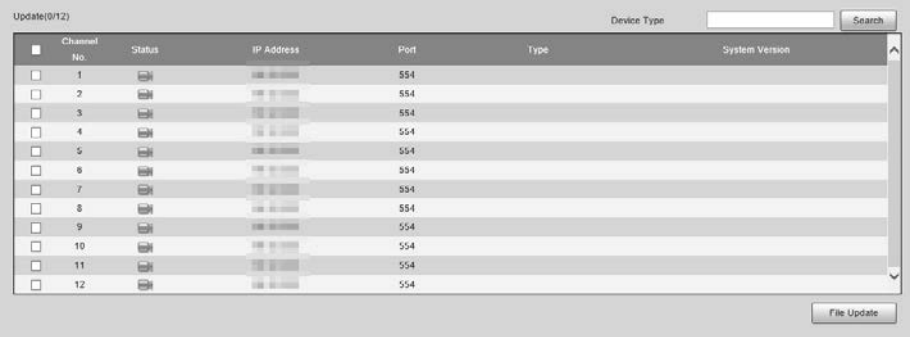
4.4.3.3 Upgrading Remotely

You can upgrade remote device.

Up to 4 devices can be upgraded at the same time.

Step 1 Select **Setting** > **Add Camera** > **Update**.

Figure 4-37 Upgrading remotely



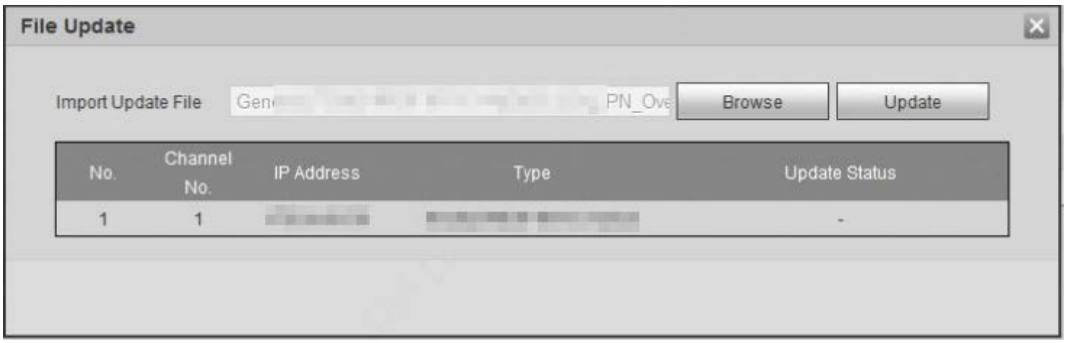
Step 2 Search for devices.

- Click **Search** to search for all connected devices.
- Enter the Device type, and then click **Search**, and the Device information that meets the search conditions is displayed.

Step 3 Select the Device to be upgraded, and then click **File Update**.

Only online upgrade is available, and the Device status is displayed as .

Figure 4-38 File Update



Step 4 Click **Browse**, follow the prompts to select a file, and then click **Update**.

4.4.4 Event Management

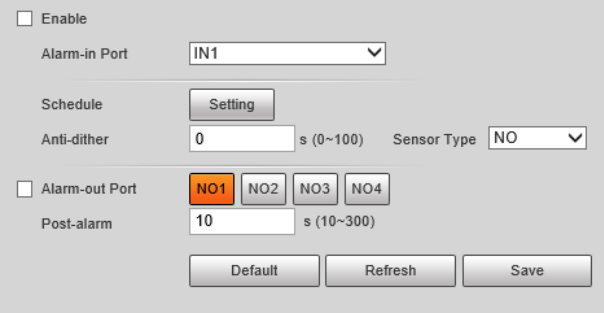
Before configuration, the alarm ports must be connected. See Figure 2-4 in "2.3 Rear Panel".

4.4.4.1 Setting Relay Activation

Set the input and output channel of alarms on the Device, and then when an alarm is triggered, the Device outputs the signal to the external device connected to the corresponding output channel, such as a buzzer.

Step 1 Select **Setting** > **Event** > **Alarm** > **Alarm**.

Figure 4-39 Alarm



Step 2 Select **Enable** to enable the relay-in for the current channel.

Step 3 Select the relay-in channel.

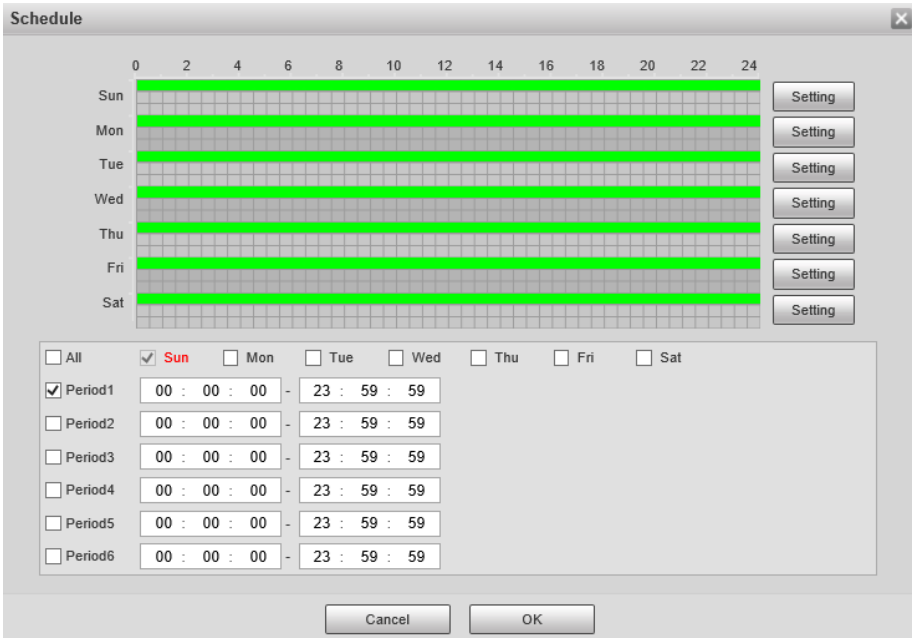
The settings in the subsequent steps are based on the current channel number. They will take effect after you click **Save**. If you switch the channel number before clicking **Save**, all settings for the current channel will not be effective.

Step 4 Set the relay-in arming and disarming periods.

The Device outputs alarm signals during armed periods.

1) Click **Setting**.
2) Set the arming and disarming periods.
   - Method 1: Press and hold the left mouse button, and directly drag to set the period on the timeline corresponding to Sunday to Saturday.
   - Method 2: Click **Setting** corresponding to Sunday to Saturday, and then select and set the arming and disarming periods. You can set up to six periods.

Figure 4-40 Period



3) Repeat the earlier steps to set the periods corresponding to other days.

4) Click **OK**.

Step 5 Set other parameters.

Table 4-17 Relay activation parameters

Parameter	Description
Anti-dither	Set the anti-dither duration to filter out false alarms.
Sensor Type	Select sensor type according to the connected relay-in device. ● Normally open: Effective for low level. ● Normally closed: Effective for high level.
Alarm-out Port	Optocoupler output. When enabled, the corresponding external device can be activated after an alarm goes off.
Pose-alarm	Set the duration of the output signal.

Step 6 Click **Save**.

Repeat the earlier steps to set other relay-in channel numbers.

4.4.4.2 Abnormality

Set relay-out for disk abnormal, illegal access, and security exception. Security exception includes web path blasting behavior, session connection overload, session ID blasting behavior, exhaustion of network connection resources, trusted environmental monitoring, abnormal program run, or username and password blasting behavior.

Step 1 Select **Setting** > **Event** > **Exception**.

Figure 4-41 Disk error



Figure 4-42 Illegal access

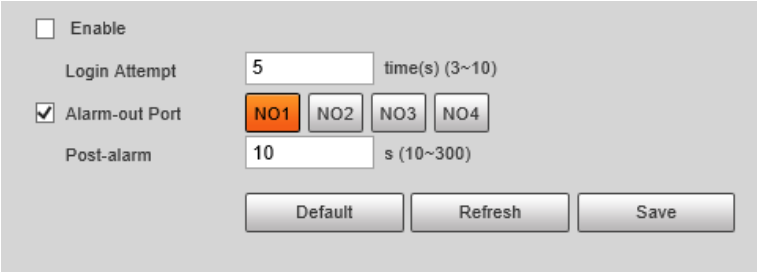
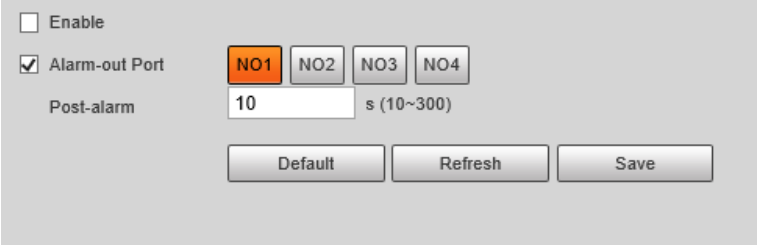


Figure 4-43 Security exception



Step 2 Select **Enable** to enable you to handle the corresponding abnormal events. **Event Type** is required in **Disk Error**.

Step 3 Configure parameters.

Table 4-18 Abnormality parameters

Parameter	Description
Event Type	Select an event type. You can select **No Disk** or **Low Disk Space**. The setting is required only when the **Disk Error** tab is selected.
Alarm-out Port	Select the checkbox to enable **Alarm-out Port**, and then select an alarm output channel. When an error occurs, the corresponding alarm output device will receive the signal and send an alarm.
Post-alarm	After the alarm ends, the relay-out will be extended for a period of time before stopping. The duration ranges from 10 s to 300 s.
Free Space	When the remaining capacity of the HDD is lower than this value, an alarm is triggered. The setting is required only when the event type is **Low Disk Space**.
Login Attempt	When the number of login errors exceeds this value, an alarm is triggered. The setting is required only when the **Illegal Access** tab is selected.

Step 4 Click **Save**.

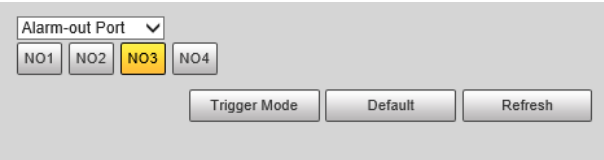
4.4.4.3 Testing Alarm I/O Output

Set alarm output parameters of the I/O page to test whether the alarm output is normal.

Step 1 Select **Setting** > **Event** > **Alarm I/O**.

Step 2 Select a channel number to enable alarm output.

Figure 4-44 Alarm I/O



Step 3 Click **Trigger Mode** to check whether the external alarm device normally triggers alarms.

4.4.5 Storage Management

Configure the storage method and location of pictures and records.

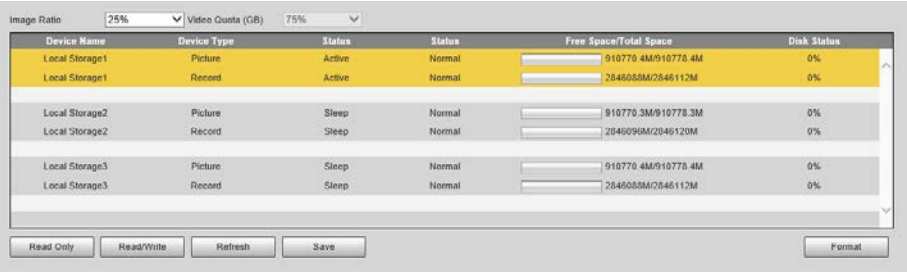
4.4.5.1 Storage

4.4.5.1.1 Local Storage

You can set the storage ratio of locally stored pictures and records, view the storage state, and set the HDD state.

Step 1 Select **Setting** > **Storage** > **Local Storage** > **Local Storage**.

Figure 4-45 Local Storage



Step 2 Select the container according to the storage ratio of pictures and records.

- The record container is automatically set with the change of the picture container.
- When the picture container is set to 0%, pictures cannot be stored. When the picture container is set to 100%, records cannot be stored.

Step 3 Click **Read Only** or **Read/Write** to set the read and write access to the HDDs of the Device.

Step 4 Click **Save**, and then restart the Device.

If the HDD are full, back up the data as required, and then click **Format** to clear the HDD.

4.4.5.1.2 Smart Info

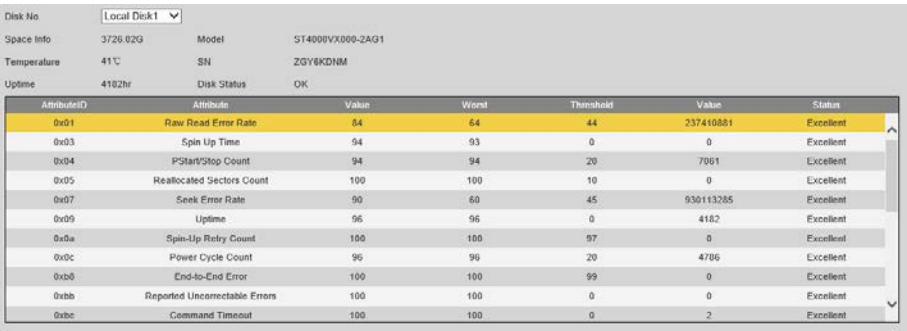
Smart (Self-Monitoring Analysis and Reporting Technology) is used to display automatic HDD detection results, discover and predict possible HDD problems in time.

When the health state is **Failure**, replace the HDD in time to avoid real-time data loss.

Step 1 Select **Setting** > **Storage** > **Local Storage** > **S.M.A.R.T**.

Step 2 Select **Disk No.** to check the related information and health state of the disk.

Figure 4-46 Smart info

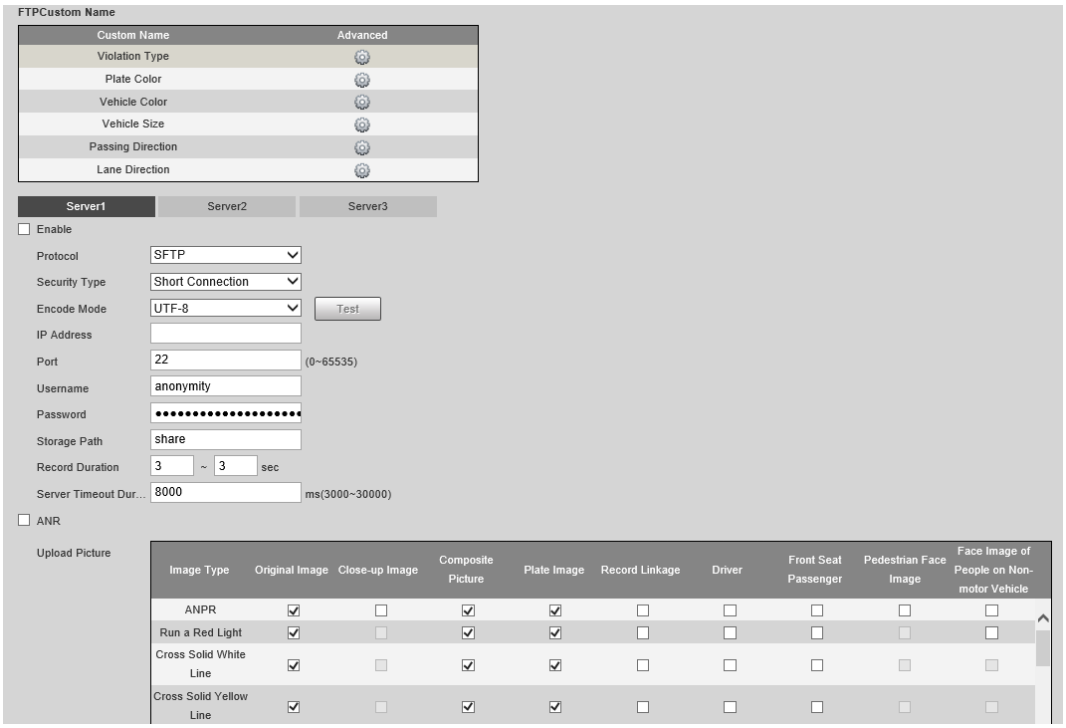


4.4.5.2 FTP Storage

Back up pictures to the FTP server for later viewing.

Step 1 Select **Setting** > **Storage** > **FTP Storage**.

Figure 4-47 FTP storage



Step 2 Click **FTP Storage**.

Step 3 (Optional) Set **FTP Custom Name** as required. Click  to modify the corresponding name.

Step 4 Select a server tab, and then select **Enable** to enable the storage function of this server.

Step 5 Configure parameters.

Table 4-19 FTP storage parameters

Parameter	Description
Protocol	Select a protocol. SFTP is recommended.
Security Type	• **Short Connection**: Connects with the FTP server when uploading each image and disconnect after upload completes. • **Long Connection**: The device stays connected with the FTP server.
Encode Mode	Select an encode mode. • **UTF-8**: International universal font library, with various languages. • **GB2312**: National standard font library, only with Chinese characters and some common foreign languages.
Test	Click **Test** to test whether the FTP server is successfully connected, and the corresponding test file will be generated according to the selected encode mode.
IP Address	The IP address of the FTP server.
Port	The port number of the FTP server, 22 by default.
Username	The username of the FTP server.

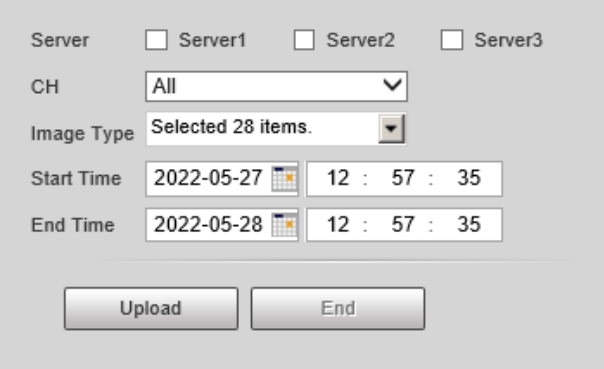
Parameter	Description
Password	The password of the FTP server.
Storage Path	The file storage path of the FTP server.
Related Video Time	Set the length of the video captured during a period before and after the time of event, in seconds.
Record Duration	Set the timeout duration of waiting for server response.
ANR	Select the checkbox. When the Device is disconnected from the FTP server and reconnected to it, the pictures during the offline period will continue to be uploaded.
Upload Picture	Select the original picture, mosaic picture, plate picture, related record, corresponding to the violation types to be uploaded to this server.
FTP Naming	Set the naming method of pictures and related videos respectively. • **Help**: The naming format window is prompted, on which you can select, insert and delete naming items. You can add up to 76 items. • **Restore**: Restore the default naming rules.
Name Each FTP	Select the checkbox, and three FTP naming rules can be separately configured.

Step 6 Click **Save**.

You can configure three FTP servers and repeat configuring the same violation type.

Step 7 Click **Manual Upload** tab, select a target server, a channel, picture type and time period to upload snapshots taken during the set period to the specified server.

Figure 4-48 Manual upload to server



Step 8 Click **Upload**.

During the upload, click **End** to stop uploading.

4.4.5.3 Recording

4.4.5.3.1 Record Control

You can set pack duration, record mode of each channel, and the recording method when the disk is full.

Step 1 Select **Setting** > **Storage** > **Record** > **Record Control**.

Step 2 Configure record control parameters.

Figure 4-49 Record control

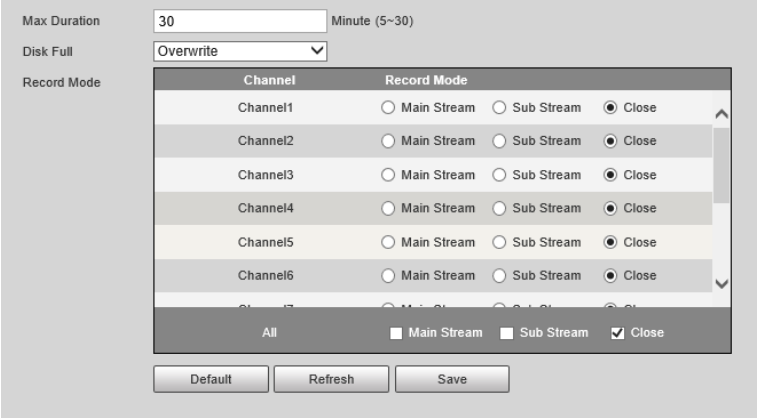


Table 4-20 Record control parameters

Parameter	Description
Max Duration	Set the duration of each record.
Disk Full	Select the recording method when the disk is full. ● Stop: If the current disk is full, recording and picture storage will be stopped. ● Overwrite: After the current disk is full, the oldest files will be circularly overwritten.
Record Mode	Set the record mode of each channel. ● **Main Stream**: Automatic recording in main stream mode according to the Record Plan. ● **Sub Stream**: Automatic recording in Sub Stream mode according to the Record Plan. ● **Close**: Recording is disabled. ● If **Sub Stream** is selected, enable **Sub Stream** for the camera. ● If **Close** is selected, videos of the corresponding channel cannot be queried on the data query page. ● To set the same record mode for all channels, select the record mode in the **All** area.

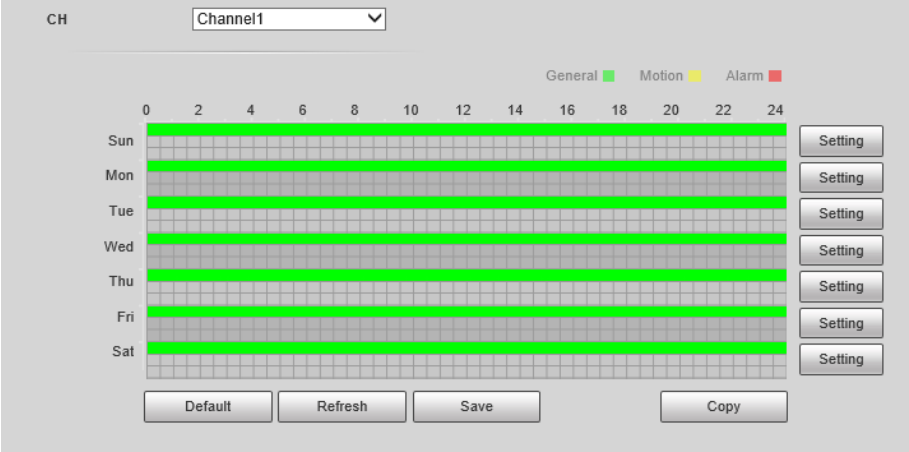
Step 3 Click **Save**.

4.4.5.3.2 Record Plan

You can set the time and type to enable recording for each channel.

Step 1 Select **Setting** > **Storage** > **Record** > **Schedule**.

Figure 4-50 Record plan

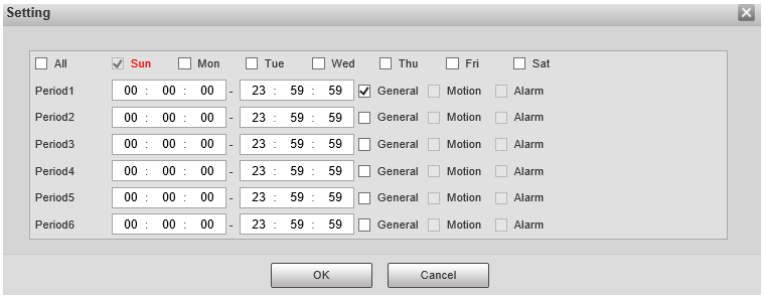


Step 2 Select a channel to set the record plan.

Step 3 Set the record plan periods. There are two setting methods.

- Click **Copy** to copy the record plan of the current channel to another channel.
- Only **General** is supported for record type now.
- Method 1: Press and hold the left mouse button, and directly drag to set the period on the timeline corresponding to Sunday to Saturday.
- Method 2: Click **Setting** on the right side of Sunday to Saturday. On the **Setting** page, select periods and record types, and then click **OK**. The **Schedule** tab is displayed.

Figure 4-51 Record time setting



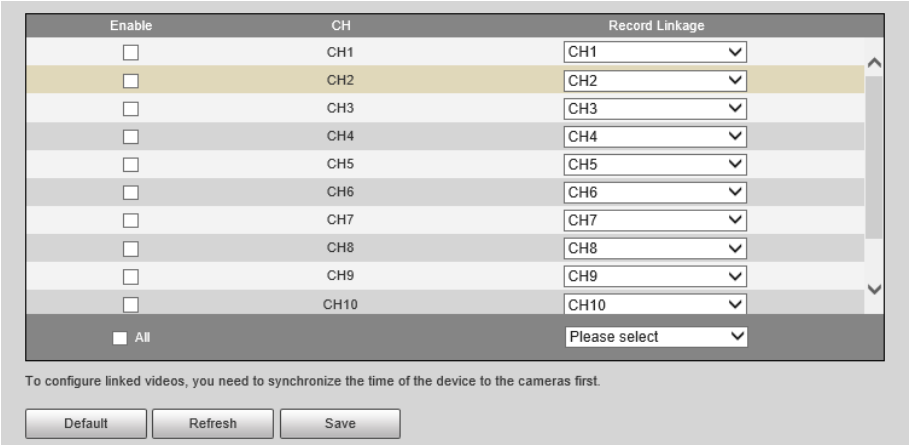
Step 4 Click **OK**.

4.4.5.4 Snapshot

You can enable channel snapshot, and then select the related record channel.

Step 1 Select **Setting** > **Storage** > **Snapshot**.

Figure 4-52 Snapshot settings



Step 2 Select **Enable** corresponding to the channel to enable snapshot.

Step 3 Set the related record of each channel.

- To set recording linkage for each channel separately, select channel number in **Record Linkage**.
- If recording linkage is not required, select **No linked videos**.

If all channels need to set the same related record, select **All** and set the linked record as required.

Step 4 Click **Save**.

4.4.6 System

4.4.6.1 General

You can configure display language, video standard, and also set the time and time zone of the Device.

4.4.6.1.1 General Settings

You can configure the Device No., video standard, and more.

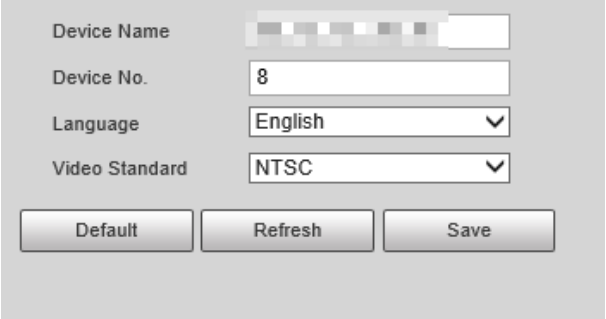
Step 1 Select **Setting** > **System** > **General** > **General**.

Step 2 Configure the parameters.

For **Video Standard**, **PAL** and **NTSC** are available.

- **PAL**: Much more common around the world, and can be found in most of Western Europe, Australia, China, and elsewhere.
- **NTSC**: Mostly limited to North America, parts of South America, Japan and the Philippines.

Figure 4-53 General



Step 3 Click **Save**.

4.4.6.1.2 Date & Time

You can configure date, time, time zone, and more of the Device.

Step 1 Select **Setting** > **System** > **General** > **Date & Time**.

Step 2 Configure the parameters.

Figure 4-54 Date & time



Table 4-21 Date & time parameters

Parameter	Description
Date Format	Select the date format. Three formats are available: **YYYY-MM-DD**, **MM-DD-YYYY** and **DD-MM-YYYY**.
Time Format	Only **24-Hour** is available.
Time Zone	The time zone where the Device locates.
System Time	The current time of the Device.
Sync PC	Sync the time of the Device with the time of the computer. Click **Sync PC**, and settings will immediately take effect.
DST	Select the **DST** (means daylight saving time) check box, set the **DST Type** by **Date** or by **Day**, and then configure the **Start Time** and **End Time** of DST.
Enable	Select **Positioning System** or **BeiDou** positioning system.

Parameter	Description
Time Synchronization	Select time synchronization mode. • **NTP**: Select the checkbox to enable **NTP** (network time protocol) time synchronization. In this case, you need to set the NTP server IP address, port, and time synchronization interval. • **Positioning System Time Synchronization**: Synchronize the time according to the positioning. In this case, you need to enable **Positioning** or **BeiDou** positioning first.

Step 3 Click **Save**.

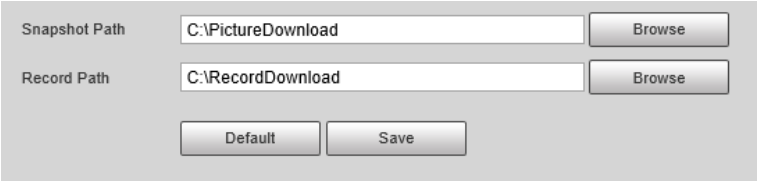
4.4.6.2 Local Setting

Configure the storage path of snapshots and videos.

Step 1 Select **Setting** > **System** > **Setting**.

Step 2 Click **Browse** to select the storage path of snapshots and videos respectively.

Figure 4-55 Local setting



Step 3 Click **Save**.

4.4.6.3 Account Management

You can add or delete users and user groups, assign permissions to new users and user groups, change password, and manage users and user groups.

4.4.6.3.1 Account

Managing Users

You can view user information, add or delete user(s), change user password, assign user permissions, restrict user login, and more.

- After the Device is initialized, the admin user generated by default has the highest permission. The admin user cannot be deleted, and its permissions cannot be changed.
- Users with **User** permission can change its own password, and change the password of other users.
- Users who have logged in cannot be deleted.

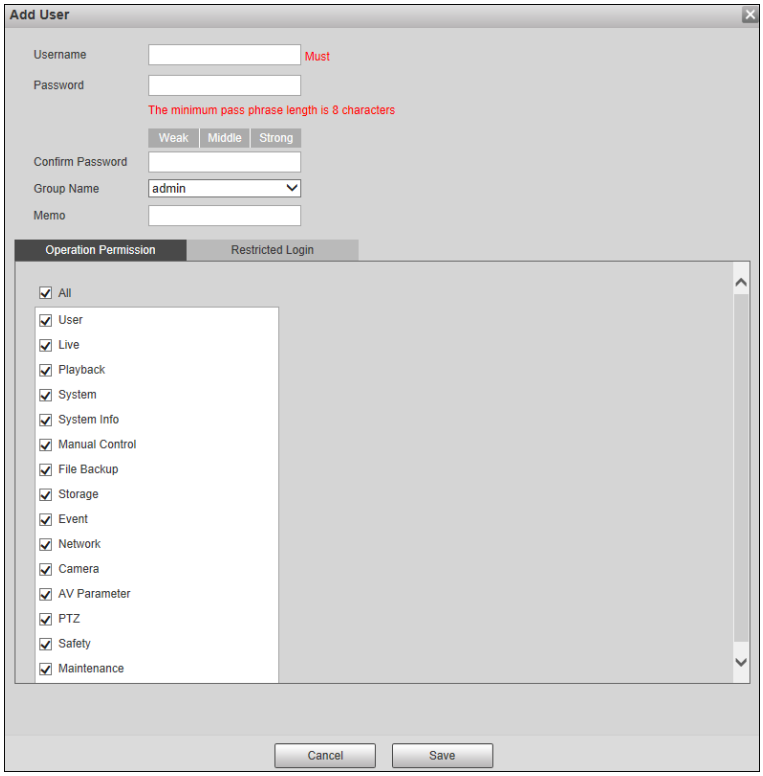
Procedure

Step 1 Select **Setting** > **System** > **Account** > **Account** > **Username**.

Step 2 Click **Add User**.

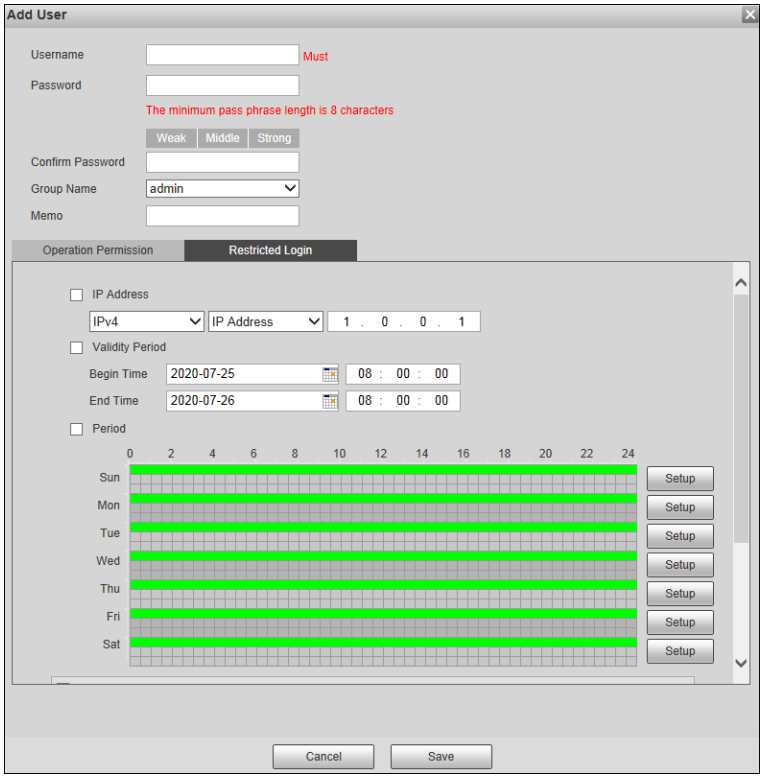
Step 3 Configure the user information including username, password, group name, memo, and operation permissions.

Figure 4-56 Add user



Step 4 Set login restrictions (if necessary), and then the restricted IP addresses or IP within the defined segment will be allowed to log in to the Device during the defined validity period and time.

Figure 4-57 Configure login restriction



Step 5 Click **Save**.

Related Operations

- Delete a user: Click to delete the corresponding user. Admin user cannot be deleted.

- Edit user information: Click corresponding to the user. You can edit the information such as username, password, email address, group name, and memo. Click **Save** to save the settings.
- Change password: On the **Modify User** page, select the **Modify Password** checkbox. Enter the old and new passwords, and confirm password. Click **Save** after configuration.

Managing User Groups

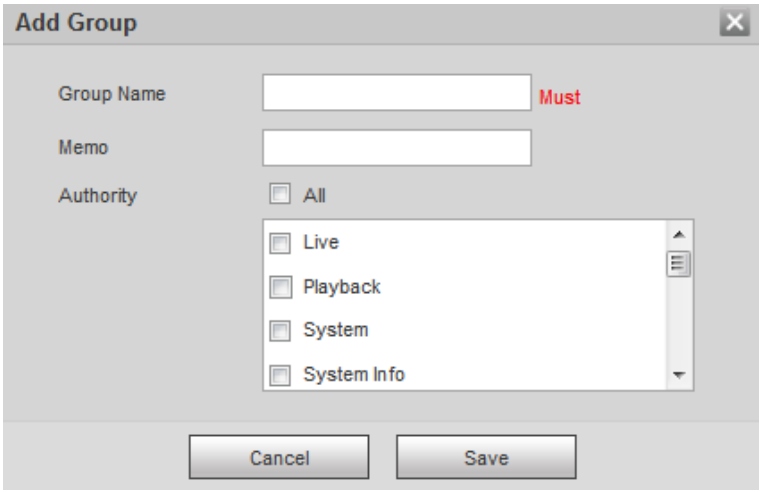
After the Device is initialized, two user groups, admin and user, are generated by default. You can also add or delete user group(s), and change user group password and permissions.

Step 1 Select **Setting** > **System** > **Account** > **Account** > **Group Name**.

Step 2 Add, modify, and delete user groups.

- Add a user group
  1. Click **Add Group**.
  2. Configure the **Group Name** and **Authority** of the group.

Figure 4-58 Add user group



  3. Click **Save**.

Click an added user group, and then you can view its permissions.

- Modify a user group
  1. Click .
  2. Modify the memo and permissions of the group.

Permission of admin user group cannot be deleted.

  3. Click **Save**.
- Delete a user group

Click to delete the selected user group. Admin and user groups cannot be deleted.

4.4.6.3.2 ONVIF User

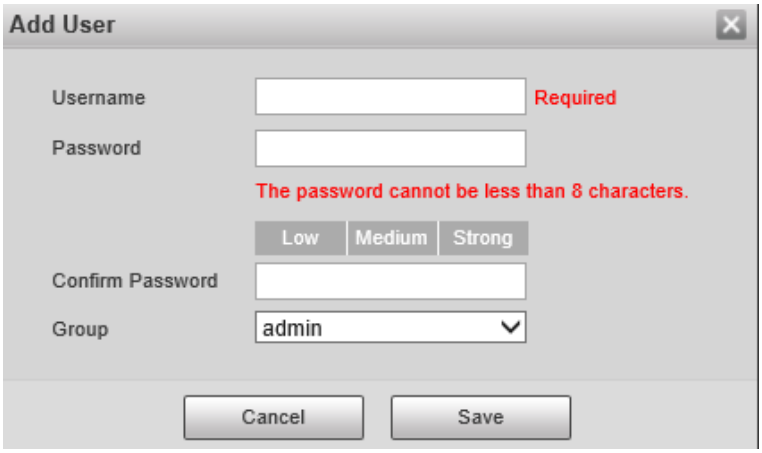
You can view ONVIF user information, add or delete ONVIF users, and change ONVIF user passwords.

Step 1 Select **Setting** > **System** > **Account** > **ONVIF User**.

Step 2 Add, modify, and delete an ONVIF user.

- Add user
  1. Click **Add User**.
  2. Configure user information such as username, password, and group name.

Figure 4-59 Add user



  3. Click **Save**.
- Modify user

  Click  to modify the information such as username, password, and group name.

  Group of admin user cannot be modified.
- Delete user

  Click  to delete the added user. Admin user cannot be deleted.

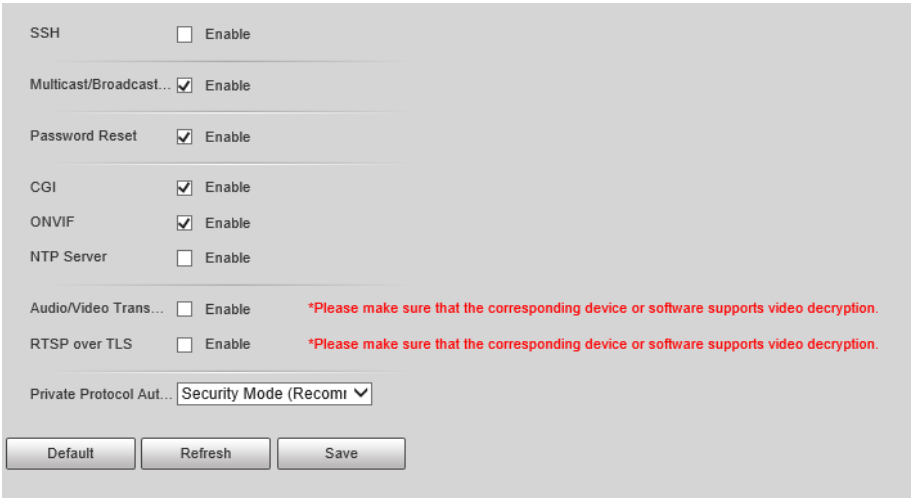
4.4.6.4 Safety

4.4.6.4.1 System Service

You can enable multiple system services to secure network safety.

Step 1 Select **Setting** > **System** > **Security** > **System Service**.

Figure 4-60 System service



Step 2 Enable the services as needed.

Table 4-22 Description of system service parameters

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is a method for secure remote login, providing secure access for users.
Multicast/Broadcast Search	Multicast identifies logical groups of computers group members. This allows a single message to be sent to the group. Broadcast allows all devices on the same network segment to see the same message.
Password Reset	Enable it so you can reset the password when you forgot your password.
CGI	The service is enabled by default. CGI is the interface between external applications and the web server, and devices can be accessed through this protocol.
ONVIF	The service is enabled by default. It allows network video products produced by different manufacturers to communicate with each other.
NTP Server	Select to enable time synchronization from the NTP server.
Audio/Video Transmission Encryption	Select the **Enable** checkbox to enable encryption during audio and video transmission. Make sure that the matched device or software supports video decryption function; otherwise, do not enable it.
RTSP over TLS	Enable this function to encrypt stream transmitted through standard protocol. We recommend you keep the function on.
Private Protocol Authentication Mode	Keep the recommended configuration.

Step 3 Click **Save**.

4.4.6.4.2 HTTPS

Prerequisites

- For first-time use of HTTPS or after changing device IP address, you need to create server certificate, and install root certificate.
- After creating server certificate, and installing root certificate, if you change a computer to log in to the webpage, then you need to download and install the root certificate again on the new computer or copy the downloaded root certificate on the new computer, and install it.

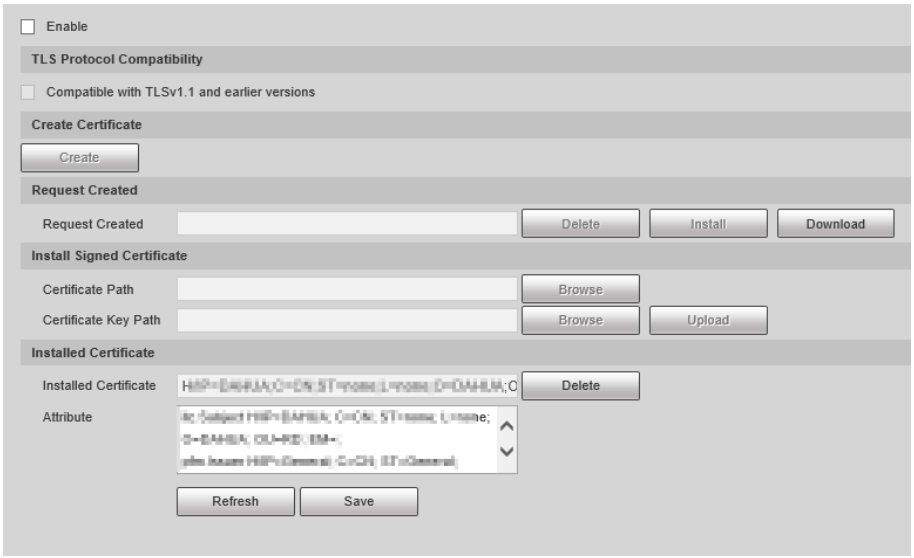
On the **HTTPS** page, users can make computer log in normally through HTTPS by creating certificate or uploading authenticated certificate. It can ensure security of communication data, and provide guarantee for user information, and device safety through reliable and stable technical approach.

Procedure

Step 1 Create certificate or upload the authenticated certificate.

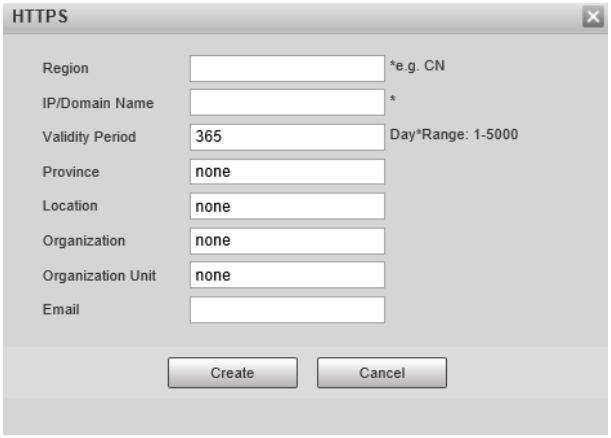
- **Create Certificate**.
  1. Select **Setting** > **System** > **Security** > **HTTPS**.

Figure 4-61 HTTPS



2. Click **Create**.

Figure 4-62 HTTPS



3. Enter the required information such as region, IP or domain name, and then click **Create**.

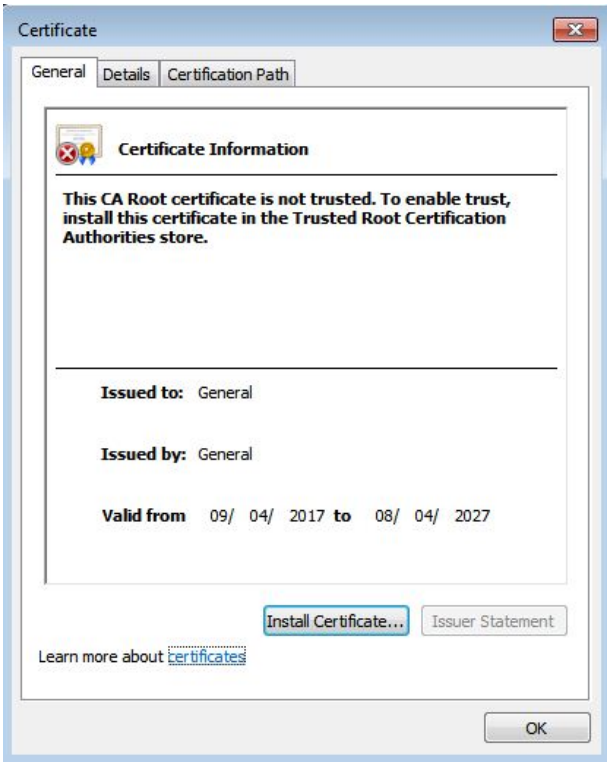
   The entered **IP/Domain name** must be the same as the IP or domain name of the Device.

4. Click **Install** under **Request Created**, and then click **Download** to download root certificate.

   The system pops up **Save As** dialog box, select storage path, and then click **Save**.

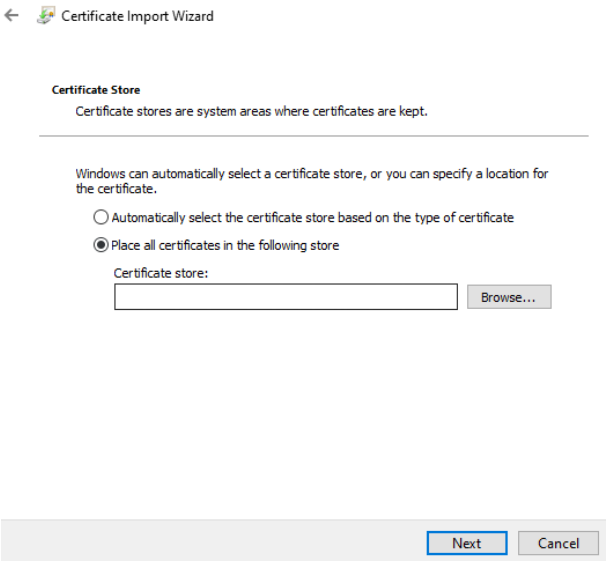
5. Double-click the RootCert.cer icon.
6. Click **Install Certificate…**

Figure 4-63 Install certificate



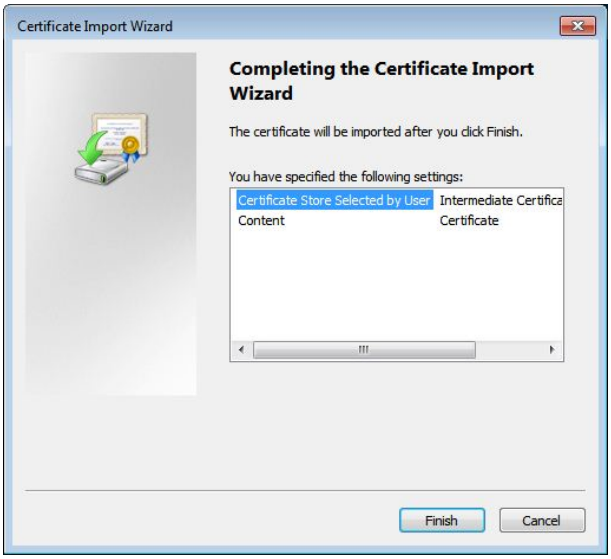
7. Click **Next**.

Figure 4-64 Certificate store



8. Click **Next**.

Figure 4-65 Completing certificate import wizard



9. Click **Finish**.

Figure 4-66 Security warning



10. Click **Yes**, and then click **OK** on the pop-up window.

- **Install signed certificate**.
  1. Select **Setting** > **System** > **Security** > **HTTPS**.
  2. Select **Enable**, and **Compatible with TLSv1.1 and earlier versions**.
  3. Click **Browse** to upload the signed certificate, and certificate key, and then click **Upload**.
  4. To install the root certificate, see operation steps from 4 to 10 in **Create Certificate**.

Step 2 Select **Enable**, and click **Save**.

The configuration takes effect until the Camera restarts.

Step 3 Use HTTPS to log in to the Camera.

1. Enter https://*xx.xx.xx.xx* in the browser.

   xx.xx.xx.xx is the Camera IP address or domain name.

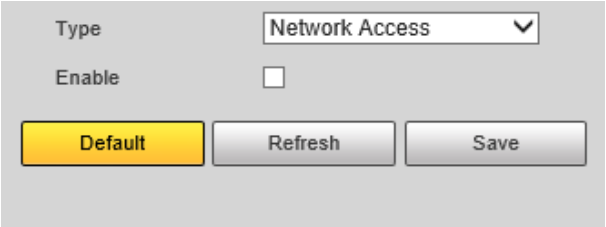
2. Enter the username, and password to log in to the Camera.

4.4.6.4.3 Firewall

Set the security rules to protect the safety of your camera system.

Step 1 Select **Setting** > **System** > **Security** > **Firewall**.

Figure 4-67 Firewall



Step 2 Select **Type**.

- **Network Access**: Add the IP address to allowlist or blocklist to allow or restrict it to access corresponding ports of the Camera.
- **PING Prohibited**: IP address of your camera is prohibited from ping. This helps prevent attempt of accessing your network system without permission.
- **Anti Half Connection**: Prevents half-open SYN attacks.

Step 3 Select **Enable** to enable the selected rule type.

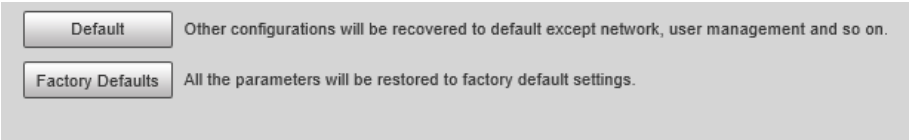
Step 4 Click **Save**.

4.4.6.5 Default

Select **Setting** > **System** > **Default**, and then you can:

- Click **Default** to restore most configurations of the Device to default settings (except information such as IP address, account, and log).
- Click **Factory Defaults**, and then enter the correct login password in the pop-up box to restore all configurations of the Device to default settings, including IP address.

Figure 4-68 Default

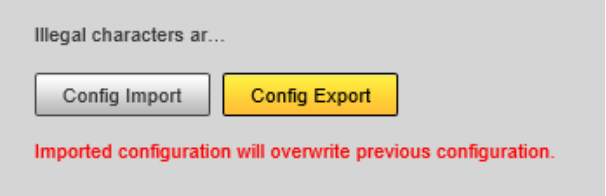


4.4.6.6 Import/Export

The system supports exporting the configurations on webpage to local computer for backup, and importing the configuration files from local backup for quick configuration or restoration.

Step 1 Select **Setting** > **System** > **Import/Export**.

Figure 4-69 Import/Export



Step 2 Click **Config Import** or **Config Export**.

- **Config Import**: Import the configuration files from local backup.

- **Config Export**: Export the configuration on the webpage to local computer.

  The imported and exported files should be in the format of .backup.

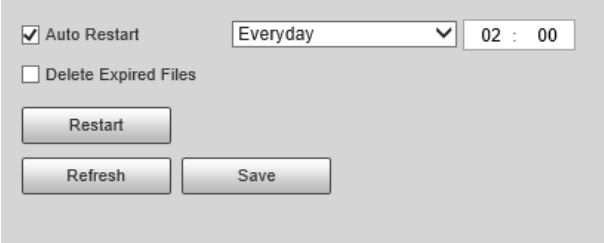
Step 3 Select the path of file to import, or the path of file to export.

4.4.6.7 Auto Maintain

The system automatically restarts at 02:00 every day by default. You can also select to automatically restart the Device at the defined day and time, or manually restart the Device to solve problems such as stuck images.

Step 1 Select **Setting** > **System** > **Maintenance**.

Figure 4-70 Auto maintain



Step 2 Select **Auto Restart**, and then set the restart time.

Step 3 Select **Delete Expired Files**, and then set a time point, and all the old files before this time will be deleted.

Step 4 (Optional) Click **Restart** can restart the Camera immediately.

Step 5 Click **Save**.

Step 6 Select **Emergency Maintenance**, and then select **Enable** to enable the function.

Step 7 Click **Save**.

4.4.6.8 System Update

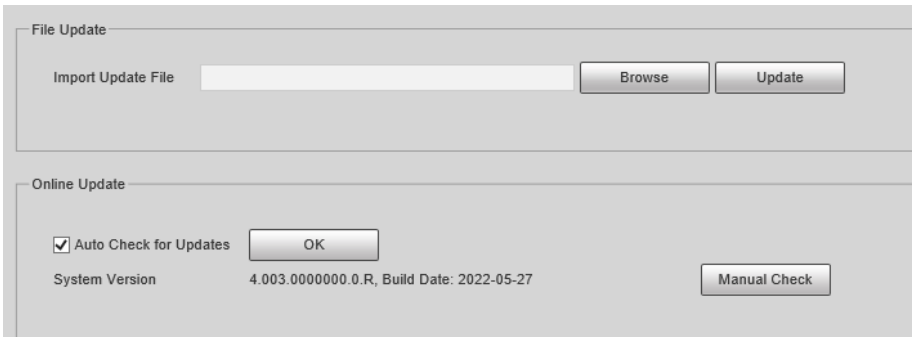
You need to update the system to the latest version to make the Device run properly.

Step 1 Select **Setting** > **System** > **Update**.

Step 2 Upgrade the system through file upgrade or online upgrade.

- File Upgrade
  1. Click **Browse**, and then select the upgrade file in the pop-up dialog box.
  2. Click **Update** to start system upgrading.
- Online Upgrade
  - Select **Auto Check for Updates**, and then click **OK**. When a new version is detected, click **Update Now**, the system starts upgrading.
  - Click **Manual Check**, and when a new version is detected, click **Update Now**, the system starts upgrading.

Figure 4-71 System update



4.4.7 System Information

You can view information such as version, log, and online user.

4.4.7.1 Version Information

Select **Setting** > **System Info** > **Version** to view information such as device type, software version, web version, and more.

Versions might vary depending on the different devices.

4.4.7.2 Log

4.4.7.2.1 System Log

You can search for and view logs by the time and type, and backup the logs.

After the number of log records reaches a certain number, the earliest log records will be overwritten. To prevent critical logs from being overwritten, the system performs log overwriting in three levels: Low, medium, and high.

- Low: When the log records reach 896, the earliest log records will be overwritten.
- Medium: When the log records reach 256, the earliest log records will be overwritten.
- High: When the log records reach 640, the earliest log records will be overwritten.

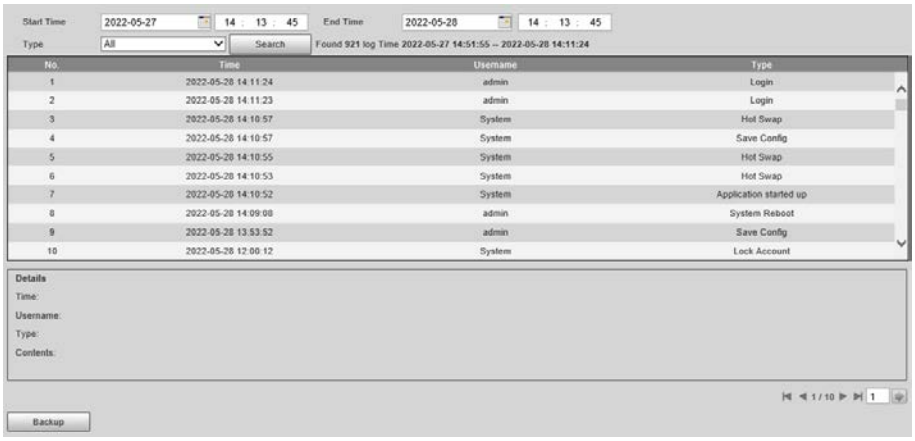
Step 1 Select **Setting** > **System Info** > **Log** > **Log**.

Step 2 Set **Start Time** and **End Time**, and then select log type.

Step 3 Click **Search**. You can stop searching according to your need.

- View: Click a log to view its details.
- Back up: Click **Backup** to back up the log to local computer in .txt format.

Figure 4-72 System log

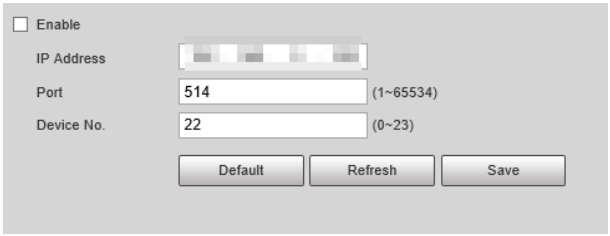


4.4.7.2.2 Remote Log

Critical logs can be saved to log server. This helps provide important clues to the source of security incidents. Log server needs to be deployed in advance by technical supports or system administrator.

Step 1 Select **Setting** > **System Info** > **Log** > **Remote Log**.

Figure 4-73 Remote log



Step 2 Select **Enable** to enable **Remote Log**.

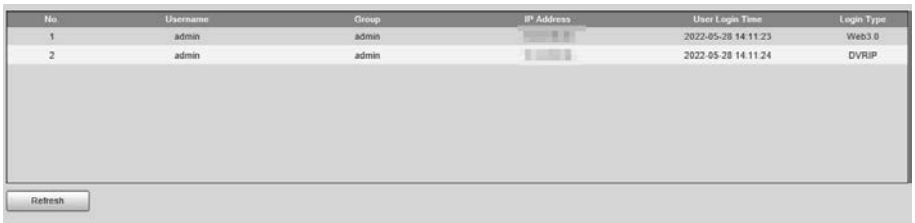
Step 3 Configure the IP address, port, and device number of remote device.

Step 4 Click **Save**.

4.4.7.3 Viewing Online User

Select **Setting** > **System Info** > **Online User**, and then you can view online users' information, such as username, user local group, IP address, user login time, and more.

Figure 4-74 Online user



4.4.7.4 Legal Information

Select **Setting** > **System Info** > **Legal Info** to view the Open Source Software Notice.

4.5 Alarm

You can select the event type that triggers an alarm, and also configure how to sound the alarm.

Step 1 Select **Alarm** at the upper-right side of the webpage.

Step 2 Select alarm type as needed.

When alarms are triggered, information of the selected alarm type will be displayed at the right side.

Figure 4-75 Alarm



Step 3 Configure alarm operation and alarm tone.

Table 4-23 Description of alarm parameters

Parameter	Description
Operation	Select **Subscribe Alarm**, and when an alarm is triggered and you are not viewing the alarm page,  will be displayed on the alarm menu bar, and the alarm information will be automatically recorded. When you click the alarm menu bar, the icon disappears. If you are viewing the alarm page when an alarm is triggered, the alarm icon will not appear, but alarm information will be recorded in the alarm list on the right.
Alarm Tone	Select **Play Alarm Tone** to enable playing alarm tone, and then click **Select** to select the audio file. When an alarm is triggered, the system plays the selected audio. Currently, only **.wav** audio file is supported.

4.6 Logout

Click **Logout** at the upper-right side of the webpage to log out. You can enter the username and password to log in again.

Appendix 1 Reference for Filling in Allowlist and Blocklist Template

Appendix Table 1-1 Plate color number

Plate Color	Plate Color No.
Yellow Plate with Black Text	1
Blue Plate with White Text	2
Black Plate with White Text	3
White Plate with Black Text	4
Black	5
Blue	6
Cyan	7
Red	8
Gradient Green	9
White	10
Yellow and Green	11
Yellow	12

Appendix Table 1-2 Vehicle color number

Vehicle Color	Vehicle Color No.
White	A
Black	B
Red	C
Yellow	D
Gray	E
Green	F
Blue	G
Pink	H
Purple	I
Brown	J
Yellow Green	K
Cyan	L
Dark Blue	M
Dark Brown	N
Dark Cyan	O
Dark Golden	P

Vehicle Color	Vehicle Color No.
Dark Green	Q
Dark Olive	R
Dark Orange	S
Dark Pink	T
Dark Purple	U
Dark Red	V
Dull Purple	W
Dark Yellow	X
Deep Sky Blue	Y
Others	Z
Dark Gray	a
Forest Green	b
Golden	c
Green Yellow	d
Chestnut	e
Light Rosy	f
Olive	g
Orange	h
Ocean Green	i
Silver Gray	j
Tomato Red	k
White Smoke	l

Appendix Table 1-3 Vehicle type number

Vehicle Type	Vehicle Type No.
Large Vehicle	1
Small Vehicle	2
Bus	23
Heavy Truck	24
MPV	25
Light Truck	26
Van	27
Medium Bus	28
Medium Truck	29
Minicar	30
Two-wheeled Vehicle	31
Tank Truck	32

Vehicle Type	Vehicle Type No.
Public Bus	33
Pickup	34
SUV	35
Sedan	36
SUV-MPV	37
Taxi	38
Tricycle	39
Unknown	40
Ambulance	41
Mixer Truck	42
Construction Truck	43
Fire Truck	44
General	45
Engineering Truck	46
Fuel Tank Truck	47
Police Car	48
Pulverized Material Vehicle	49
Tank Truck	50
Sewage Suction Truck	51
Hazardous Chemicals Truck	52
Tractor	14
Sanitation Truck	53

Appendix Table 1-4 Corresponding number of arm type

Arming Type	Arming Type No.
Others	5
Arrearage Vehicle	6

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**
   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**
   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**
   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**
   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**
   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
10. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
12. **Network Log**
    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
13. **Construct a Safe Network Environment**
    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.