V1.0.1

Network Camera

User‘s Manual

Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of network camera. Read carefully before using the platform, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ 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 result.
📖 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.1	Updated the language.	October 2023
V1.0.0	First release.	September 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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

⚠

- Transport the device under allowed humidity and temperature conditions.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.

Storage Requirements

⚠

- Store the device under allowed humidity and temperature conditions.
- Do not place the device in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or unstable illumination.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during storage.

Installation Requirements

⚠ WARNING

- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- Please follow the electrical requirements to power the device.
  - When selecting the power adapter, 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.
  - We recommend using the power adapter provided with the device.
- Do not connect the device to two or more kinds of power supplies, unless otherwise specified, to avoid damage to the device.
- The device must be installed in a location that only professionals can access, to avoid the risk of non-professionals becoming injured from accessing the area while the device is working. Professionals must have full knowledge of the safeguards and warnings of using the device.

⚠

- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- 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.

- Ground the function earthing portion ⏚ of the device to improve its reliability (certain models are not equipped with earthing holes). 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.
- The dome cover is an optical component. Do not directly touch or wipe the surface of the cover during installation.

Operation Requirements

⚠ WARNING

- The cover must not be opened while the device is powered on.
- Do not touch the heat dissipation component of the device to avoid the risk of getting burnt.

⚠

- Use the device under allowed humidity and temperature conditions.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it, to avoid reducing the lifespan of the CMOS sensor, and causing overbrightness and flickering.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Protect indoor devices from rain and dampness to avoid electric shocks and fires breaking out.
- Do not block the ventilation opening near the device to avoid heat accumulation.
- 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 directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens.
- The dome cover is an optical component. Do not directly touch or wipe the surface of the cover when using it.
- There might be a risk of electrostatic discharge on the dome cover. Power off the device when installing the cover after the camera finishes adjustment. Do not directly touch the cover and make sure the cover is not exposed to other equipment or human bodies
- Strengthen the protection of the network, device data and personal information. All necessary safety measures to ensure the network security of the device must be taken, such as using strong passwords, regularly changing your password, updating firmware to the latest version, and isolating computer networks. For the IPC firmware of some previous versions, the ONVIF password will not be automatically synchronized after the main password of the system has been changed. You need to update the firmware or change the password manually.

Maintenance Requirements

⚠

- Strictly follow the instructions to disassemble the device. Non-professionals dismantling the device can result in it leaking water or producing poor quality images. For a device that is required to be disassembled before use, make sure the seal ring is flat and in the seal groove when putting the cover back on. When you find condensed water forming on the lens or the desiccant becomes green after you disassembled the device, contact after-sales service to replace the desiccant. Desiccants might not be provided depending on the actual model.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be

performed by qualified professionals.

- Do not directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens. When it is necessary to clean the device, slightly wet a soft cloth with alcohol, and gently wipe away the dirt.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- The dome cover is an optical component. When it is contaminated with dust, grease, or fingerprints, use degreasing cotton moistened with a little ether or a clean soft cloth dipped in water to gently wipe it clean. An air gun is useful for blowing dust away.
- It is normal for a camera made of stainless steel to develop rust on its surface after being used in a strong corrosive environment (such as the seaside, and chemical plants). Use an abrasive soft cloth moistened with a little acid solution (vinegar is recommended) to gently wipe it away. Afterwards, wipe it dry.

Table of Contents

1 Overview

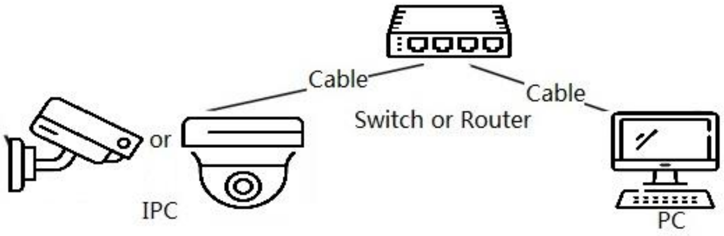
1.1 Introduction

IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.
IP camera is divided into single-channel camera and multi-channel camera according to the channel quantity. For the multi-channel camera, you can set the parameters for each channel.

1.2 Network Connection

In the general IPC network topology, IPC is connected to PC through network switch or router.

Figure 1-1 General IPC network



1.3 Functions

Functions might vary with different devices.

1.3.1 Basic Functions

Real-time Monitoring

- Preview.
- When live viewing the image, you can enable audio, voice talk and connect monitoring center for quick processing on the abnormality.
- Adjust the image to the proper position by PTZ.
- Snapshot and triple snapshot abnormality of the monitoring image for subsequent view and processing.
- Record abnormality of monitoring image for subsequent view and processing.
- Configure coding parameters, and adjust live view image.

Record

- Record automatically as schedule.
- Play back recorded video and picture as needed.
- Download recorded video and picture.
- Alarm linked recording.

Account

- Add, edit and delete the user group, and manage user authorities according to user group.
- Add, edit and delete the user, and configure user authorities.
- Change password of the user.

1.3.2 Intelligent Functions

Alarm

- Set alarm prompt mode and tone according to alarm type.
- View alarm prompt message.

Video Detection

- Motion detection, video tampering detection and scene changing detection.
- When an alarm is triggered, the system performs actions such as recording, alarm output, sending email, and taking snapshot.

Audio Detection

- Detection of abnormal audio detection and intensity change.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

IVS

- Detection of regional intrusion, line crossing and intrusion.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

2 Device Initialization

Device initialization is required for the first-time use. This manual is based on the operation on the webpage. You can also initialize device through ConfigTool, NVR, or platform devices.

- To ensure the device safety, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the IP of computer and device IP in the same network.

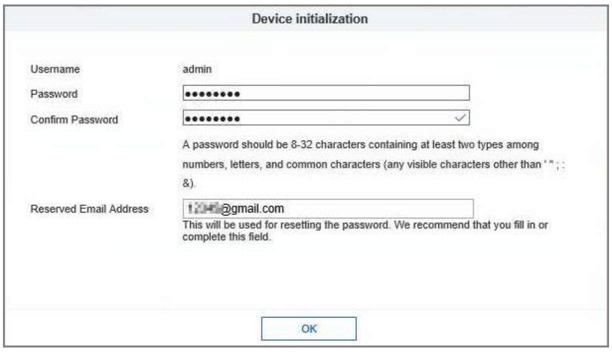
Procedure

Step 1 Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.

The IP is 192.168.1.101 by default.

Step 2 Set the password for admin account.

Figure 2-1 Device initialization



Device initialization

Username admin

Password •••••••••

Confirm Password •••••••••

A password should be 8-32 characters containing at least two types among numbers, letters, and common characters (any visible characters other than ' " ; : &).

Reserved Email Address [redacted]@gmail.com

This will be used for resetting the password. We recommend that you fill in or complete this field.

Table 2-1 Description of password configuration

Parameter	**Description**
Username	The default username is admin.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a high security level password according to the password security notice.
Confirm password	
Reserved email	Enter an email address for password resetting, and it is enabled by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 3 Click **OK**.

3 Login

3.1 Logging in to the Webpage

This section introduces how to log in to the webpage. Here we take Chrome as an example.

- You need to initialize the camera before logging in to the webpage. For details, see "2 Device Initialization".
- Follow the instruction to download and install the plug-in for the first login.

Procedure

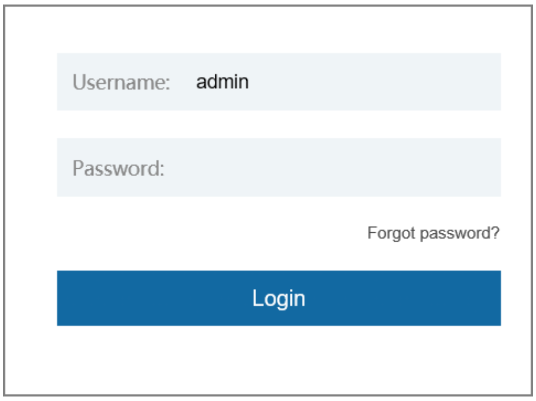
Step 1 Open IE browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press Enter.

Step 2 Enter the username and password.

The username is admin by default.

Click **Forgot password?**, and you can reset the password through the email address that is set during the initialization. For details, see "3.2 Resetting Password".

Figure 3-1 Login



Username: admin

Password:

Step 3 Click **Login**.

3.2 Resetting Password

When you need to reset the password for the admin account, there will be a security code sent to the entered email address which can be used to reset the password.

Prerequisites

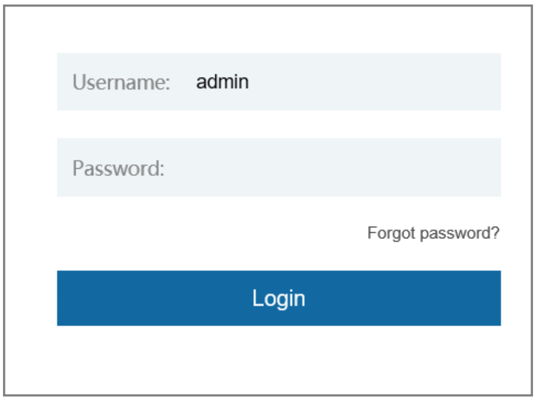
You have enabled password resetting service. For details, see "2 Device Initialization".

Procedure

Step 1 Open IE browser, enter the IP address of the device in the address bar, and then press

Enter.

Figure 3-2 Login



Username: admin

Password:

Step 2 Click **Forgot password?**, and then you can reset the password through the email address that is set during the initialization.

4 Preview

Log in to the webpage, and the **Preview** page is displayed.

Figure 4-1 Preview

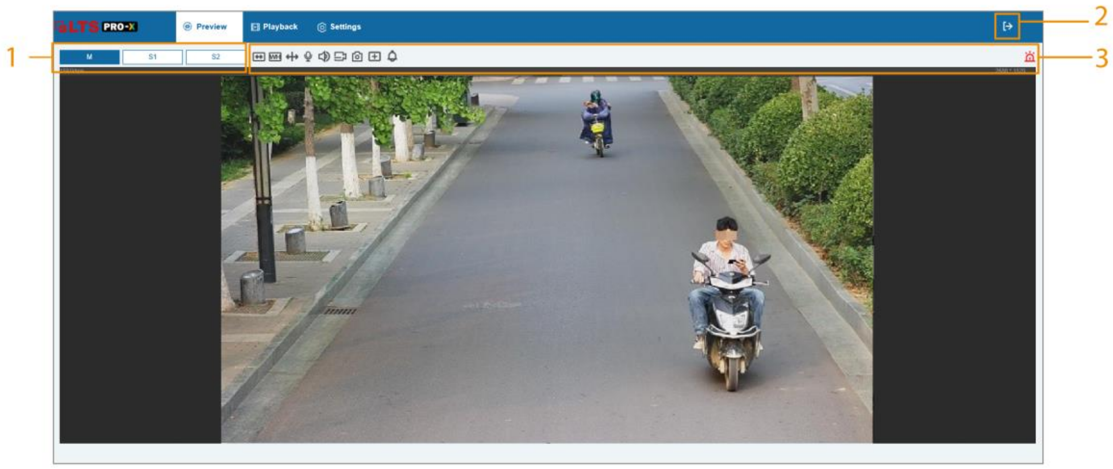


Table 4-1 Function bars description

No.	Parameter/Icon	Description
1	M (Main Stream)	It has large bit stream value and image with high resolution, but requires large bandwidth. This option can be used for storage and monitoring.
	S1 (Sub Stream 1)	It has small bit stream value and smooth image, and requires little bandwidth. This option is normally used to replace main stream when bandwidth is not enough.
	S2 (Sub Stream 2)	
2	Exit	Click the icon, and then the system will log out to go to the login page.
3	⇔	Full screen. Click the icon to enter full screen mode; double-click or press Esc to exit.
	WH	Aspect ratio. Click the icon to resume original ratio or change ratio.
	↔	VCA (Video Content Analysis). Displays the configured intelligent rule lines.
	🎙	Intercom. Click the icon to enable or disable the voice interaction.
	🔊	Sound. Click the icon to enable or disable audio output.
	📹	Video recording. Click the icon to record video, and it will be saved to the configured storage path.
	📷	Snapshot. Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.

No.	Parameter/Icon	Description
	⊞	Local zoom. You can zoom in or out the video image through two methods. ● Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
	🔔	Alarm. Displays the status of alarm sound. Click the icon to enable or disable the alarm sound forcibly.
	🚨	Alarm output. Enable or disable the alarm output linkage.

5 AI Preview

You can select in **Face Detection** mode or **Video Metadata** mode.

Prerequisites

- Only IE browser supports this page.
- Make sure you have enabled the corresponding function in settings page.

Procedure

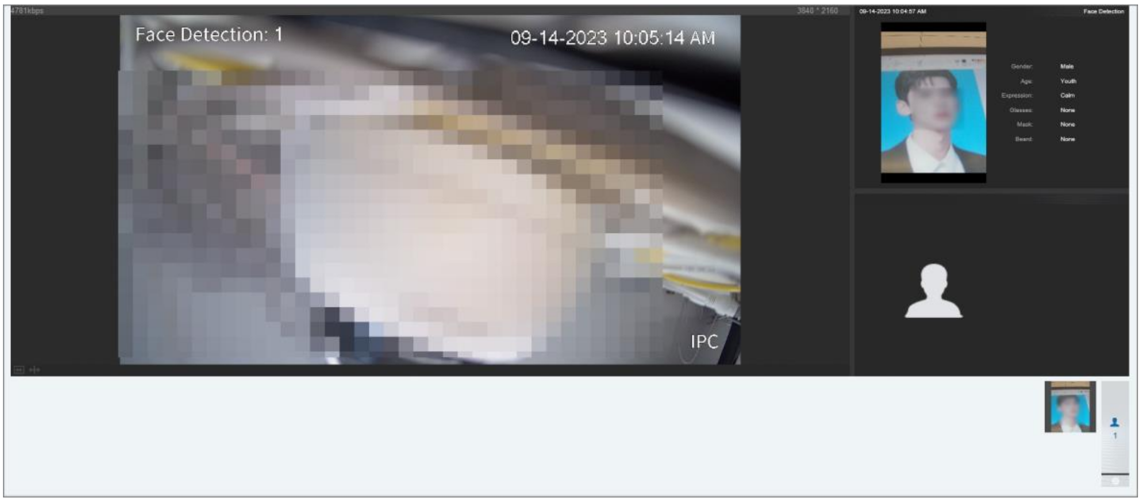
Step 1 Log in to the webpage of the device.

Step 2 Select **AI Preview** page.

Step 3 In the lower-right page, click ⚙, and then select the mode in the **VCA Option** drop-down list.

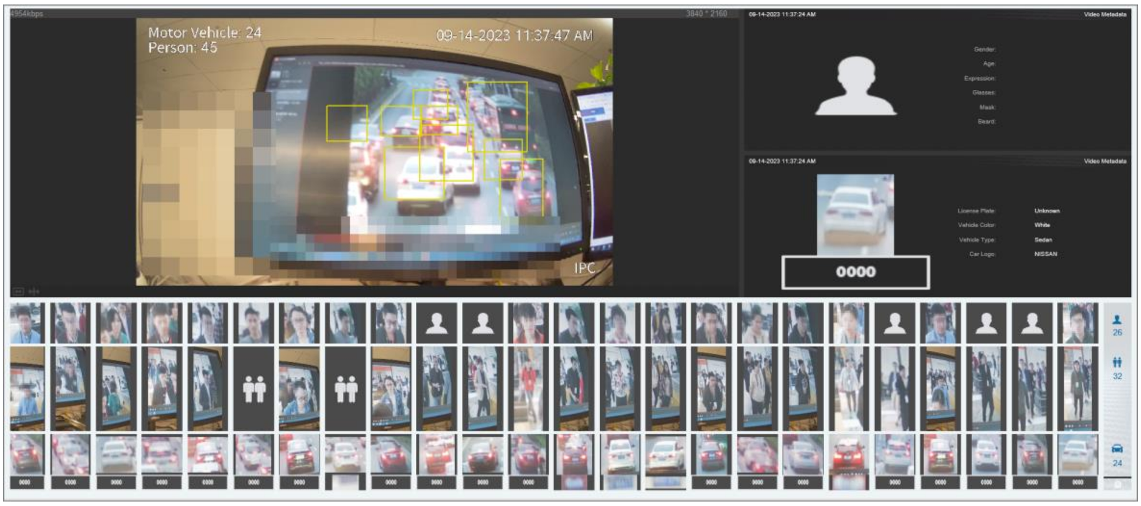
Step 4 Select the displayed attributes, and then click **Save**.

Figure 5-1 AI preview (face detection)



Gender: Male
Age: Youth
Expression: Calm
Glasses: None
Mask: None
Beard: None

Figure 5-2 AI preview (video metadata)



Gender:
Age:
Expression:
Glasses:
Mask:
Beard:

License Plate: Unknown
Vehicle Color: White
Vehicle Type: Sedan
Car Logo: NISSAN

6 Playback

This section introduces playback related functions and operations, including videos and picture.

- Before playing the recording, configure record time range, record storage method, record schedule and record control. For details, see "7.6.1.1 Video Recording".
- Before searching for picture, configure snapshot time range, snapshot storage method, and snapshot plan. For details, see "7.6.4 Snapshot".

6.1 Playback Page

Click the **Playback** tab.

Figure 6-1 Video

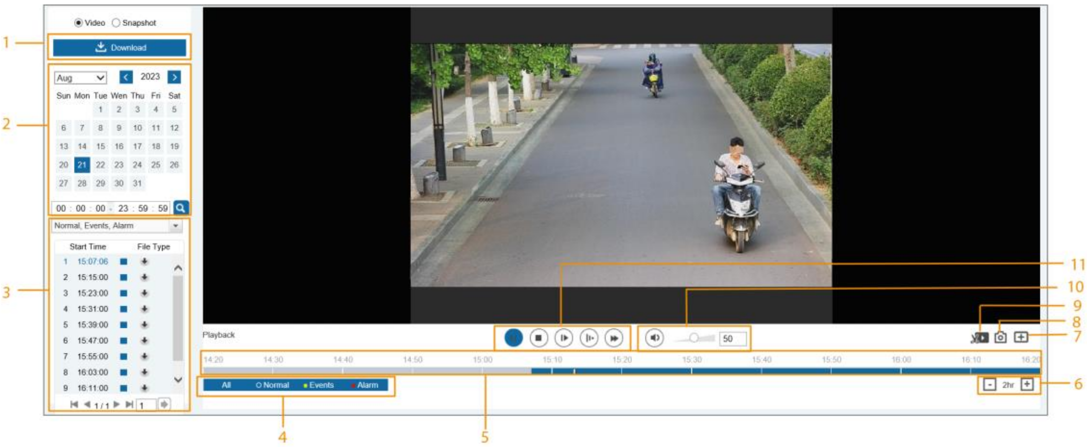


Figure 6-2 Picture

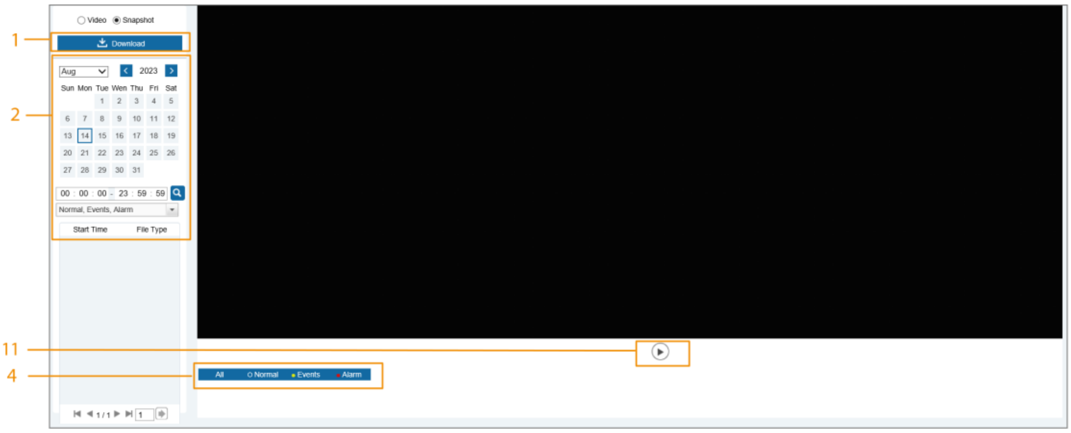


Table 6-1 Playback page description

No.	Function	Description
1	Download	Download the video or snapshot. For details, see "6.4 Downloading Video or Picture".
2	Playback file	You can select the record date and time.

No.	Function	Description
3	Type	You can select the corresponding recording to play and download.
4	Record/Snapshot Type	Select the record type or snapshot type.
5	Progress bar	Displays the record type and the corresponding period. ● Click any point on the colored area, and the system will play back the recorded video from the selected moment. ● Each record type has its own color, and you can see their relations in **Record Type** bar.
6	Time format of progress bar	Includes 4 time formats: 30min, 1hr, 2hr and 24hr. Uses **24hr** as an example, the whole progress stands for 24 hours.
7	Local zoom	You can zoom in or out the video and picture of the selected area through two methods. ● Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
8	Snapshot	Click to capture one picture of the current image, and it will be saved to the configured storage path.
9	Video clip	Clip a certain recorded video. For details, see "6.3 Clipping Video".
10	Sound	Controls the sound during playback. ● 🔇: Mute mode. ● 🔊: Vocal state. You can adjust the sound.
11	Play control bar	Controls playback. ● ▶/⏸: Play or pause recorded videos. ● ⏹: Stop playing back recorded videos. ● ⏭: Play the next frame. ● ⏪: Slow down the playback. ● ⏩: Speed up the playback.

6.2 Playing Video or Picture

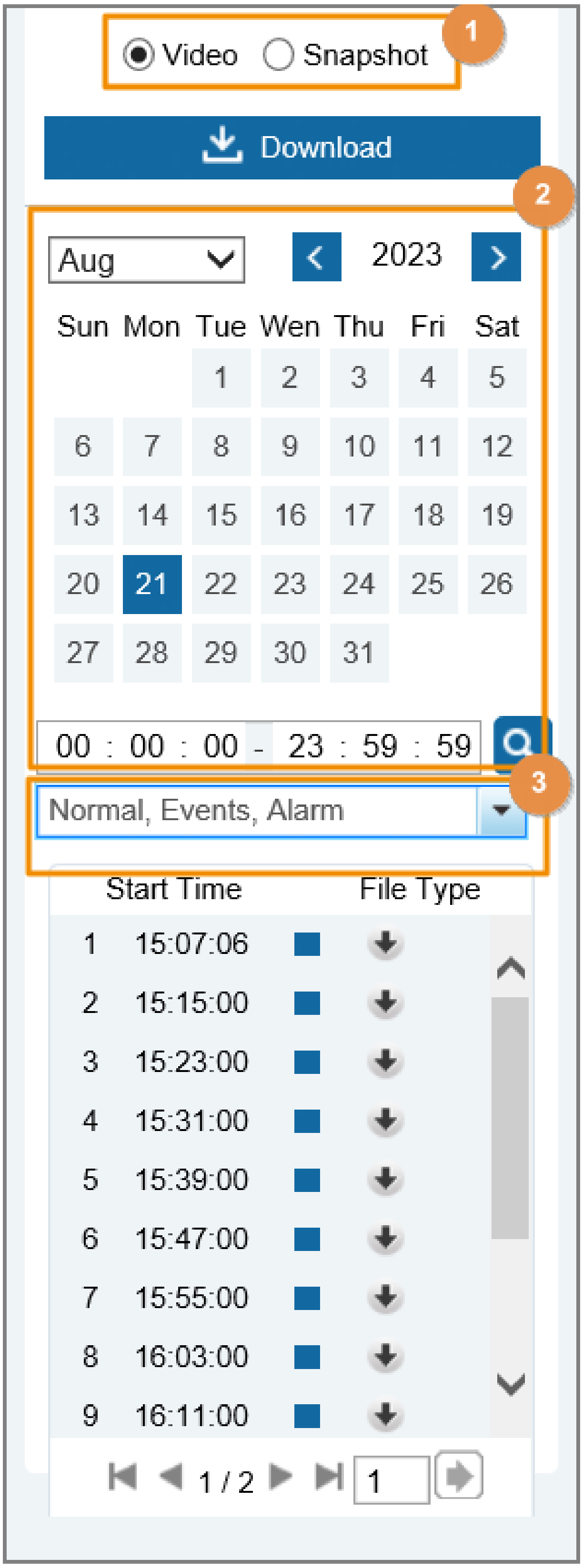
This section introduces the operation of video playback and picture playback. This section uses video playback as an example.

Procedure

Step 1 Select **Video** or **Snapshot** as needed, and then configure the time.

Step 2 Select the record type from the drop-down list.

Figure 6-3 Playback list



● Video ○ Snapshot

Aug 2023

Sun	Mon	Tue	Wen	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

00 : 00 : 00 - 23 : 59 : 59

Normal, Events, Alarm

	Start Time		File Type
1	15:07:06	🟦	↓
2	15:15:00	🟦	↓
3	15:23:00	🟦	↓
4	15:31:00	🟦	↓
5	15:39:00	🟦	↓
6	15:47:00	🟦	↓
7	15:55:00	🟦	↓
8	16:03:00	🟦	↓
9	16:11:00	🟦	↓

1 / 2 1

Step 3 Play the video.

- Click ▷ in the control bar.

  The system plays the recorded video of the selected date (in the order of time).

- Click any point in the colored area on the progress bar.

  The playback starts from that moment.

Figure 6-4 Process bar

6.3 Clipping Video

Procedure

Step 1 Select **Video**, and then configure the time.

Step 2 Select ✂▶.

Step 3 Click on the progress bar to select the start time of the target video, and then click ✂.

Step 4 Click again on the progress bar to select the end time of the target video, and then click ✂.

Step 5 Click 💾 to download the video.

The system will prompt that it cannot play and download at the same time.

Step 6 Click **OK**.

The playback stops and the clipped file is saved to the default storage path (C:\Users\admin\WebDownload\PlaybackRecord).

6.4 Downloading Video or Picture

Download video or picture to a defined path. You can download single video or picture file, or download them in batches. This section takes downloading video as an example.

- You can not play or download at the same time.
- Operations might vary with different browsers.

6.4.1 Downloading a Single File

Procedure

Step 1 Select **Video**, and then configure the time.

Step 2 Select the record type from the drop-down list.

Step 3 Click ⬇ next to the file to be downloaded.

The system starts to download the file to the default path (C:\Users\admin\WebDownload\PlaybackRecord).

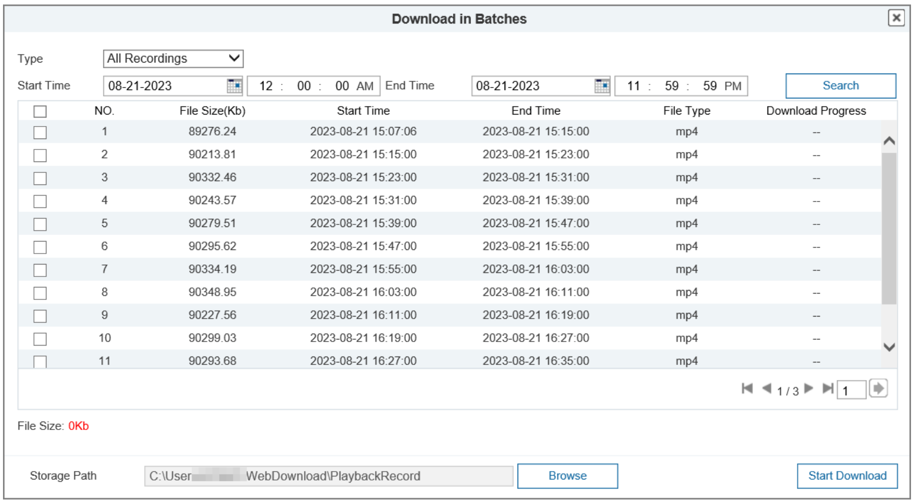
6.4.2 Downloading Files in Batches

Procedure

Step 1 Select **Video**, and then click **Download**.

Step 2 In the pop-up page, select the record type, set the start time and end time, and then click **Search**.

Figure 6-5 Download in batches


Download in Batches

Type: All Recordings

Start Time: 08-21-2023 12 : 00 : 00 AM End Time: 08-21-2023 11 : 59 : 59 PM

□	NO.	File Size(Kb)	Start Time	End Time	File Type	Download Progress
□	1	89276.24	2023-08-21 15:07:06	2023-08-21 15:15:00	mp4	--
□	2	90213.81	2023-08-21 15:15:00	2023-08-21 15:23:00	mp4	--
□	3	90332.46	2023-08-21 15:23:00	2023-08-21 15:31:00	mp4	--
□	4	90243.57	2023-08-21 15:31:00	2023-08-21 15:39:00	mp4	--
□	5	90279.51	2023-08-21 15:39:00	2023-08-21 15:47:00	mp4	--
□	6	90295.62	2023-08-21 15:47:00	2023-08-21 15:55:00	mp4	--
□	7	90334.19	2023-08-21 15:55:00	2023-08-21 16:03:00	mp4	--
□	8	90348.95	2023-08-21 16:03:00	2023-08-21 16:11:00	mp4	--
□	9	90227.56	2023-08-21 16:11:00	2023-08-21 16:19:00	mp4	--
□	10	90299.03	2023-08-21 16:19:00	2023-08-21 16:27:00	mp4	--
□	11	90293.68	2023-08-21 16:27:00	2023-08-21 16:35:00	mp4	--

File Size: 0Kb

Storage Path: C:\User[redacted]WebDownload\PlaybackRecord

Step 3 Select the files to be downloaded, and then set the storage path.

Step 4 Click **Start Download**.

The system starts to download the file to the configured path.

7 Setting

This section introduces the basic settings of the camera, including the configuration of system, network, video/audio, image, event and storage.

7.1 System

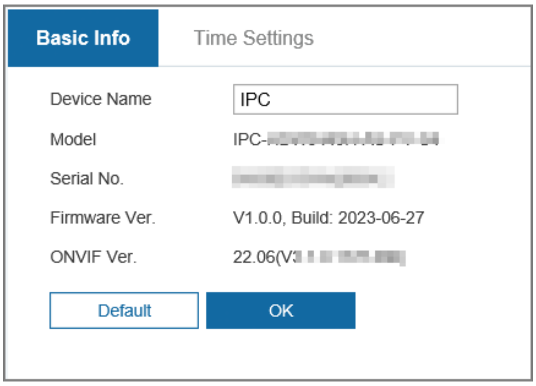
7.1.1 System Setting

7.1.1.1 Basic Info

Procedure

Step 1 Select **Settings** > **System** > **System Setting** > **Basic Info**.

Figure 7-1 Basic info



Device Name: IPC

Model: IPC-[redacted]

Serial No.: [redacted]

Firmware Ver.: V1.0.0, Build: 2023-06-27

ONVIF Ver.: 22.06(V[redacted]

Step 2 (Optional) Set a unique device name. The device name is model name by default.

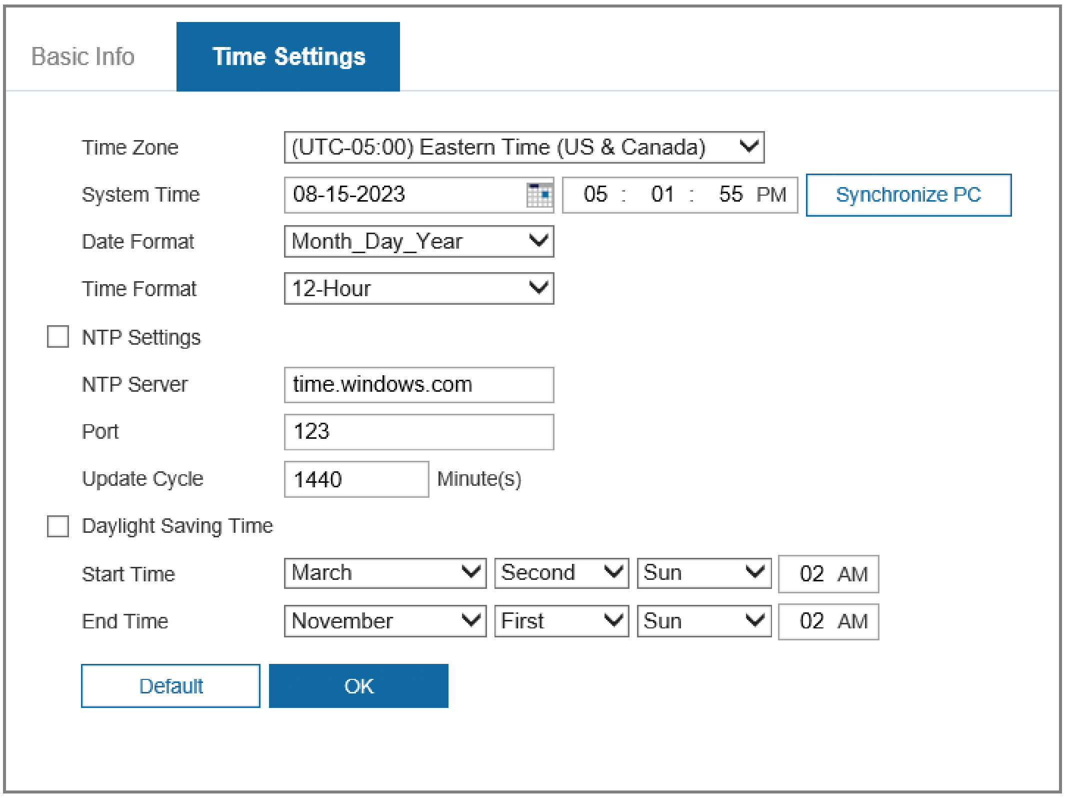
Step 3 Check the device information such as serial number, firmware version and ONVIF version. Click **OK**.

7.1.1.2 Time Settings

Procedure

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

Figure 7-2 Time settings



Basic Info | Time Settings

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

System Time: 08-15-2023 05 : 01 : 55 PM Synchronize PC

Date Format: Month_Day_Year

Time Format: 12-Hour

□ NTP Settings

NTP Server: time.windows.com

Port: 123

Update Cycle: 1440 Minute(s)

□ Daylight Saving Time

Start Time: March Second Sun 02 AM

End Time: November First Sun 02 AM

Default OK

Step 2 Configure the parameters.

Table 7-1 Description of time settings parameters

Parameter	Description
Time Zone	Set the time zone to match the location of the camera.
System Time	Configure system time. Click **Synchronize PC**, and then the system time changes to the computer time.
Date Format	Configure the date format.
Time Format	Configure the time format. You can select from **12-Hour** or **24-Hour**.
NTP Settings	Select the checkbox, and then NTP (network time protocol) is enabled, the system then syncs time with the internet server in real time. You can also enter the IP address, time zone, port, and interval of a computer which installed NTP server to use NTP.
NTP server	
Port	
Update Cycle	
Daylight Saving Time	Enable it as needed, and then configure start time and end time of daylight saving time.

Step 3 Click **OK**.

7.1.2 Maintenance

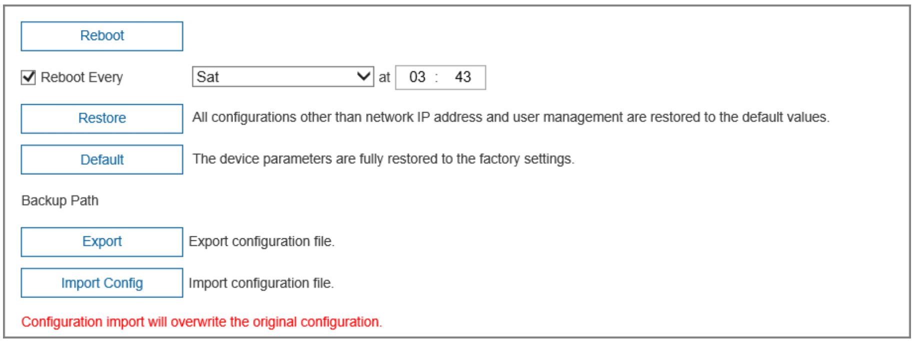
7.1.2.1 Upgrade and Maintenance

You can set the time of auto reboot, back up the configuration file and upgrade system version.

Maintenance

1. Log in to the webpage of the device.
2. Select **Settings** > **System** > **Maintenance** > **Upgrade and Maintenance**.

Figure 7-3 Maintenance



☑ Reboot Every Sat at 03 : 43

All configurations other than network IP address and user management are restored to the default values.

The device parameters are fully restored to the factory settings.

Backup Path

Export configuration file.

Import configuration file.

Configuration import will overwrite the original configuration.

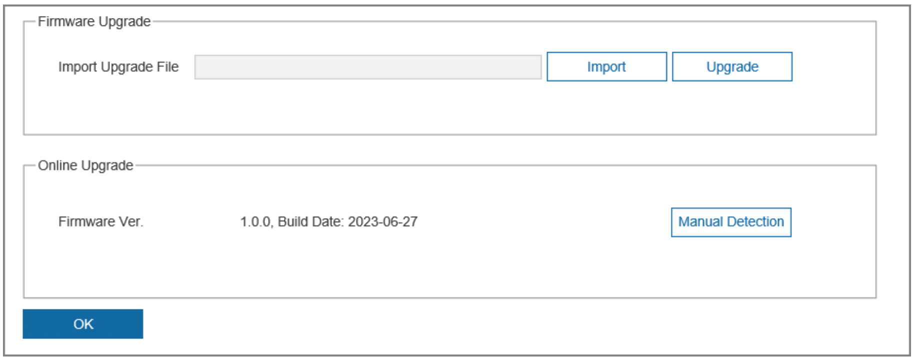
3. You can set the auto reboot time, restore, default, import and export configuration file as needed.
4. Click **OK**.

Firmware Upgrade

1. Select upgrade method as needed.
   - Firmware Upgrade
     a. Click **Import**, and then select upgrade file. The upgrade file should be a **Sec_XXX.bin** file.
     b. Click **Upgrade**.
   - Online Upgrade

     Click **Manual Detection**. If there is any upgrade available, click **Upgrade**, and then the system starts upgrading.

Figure 7-4 Firmware upgrade



Import Upgrade File

Firmware Ver. 1.0.0, Build Date: 2023-06-27

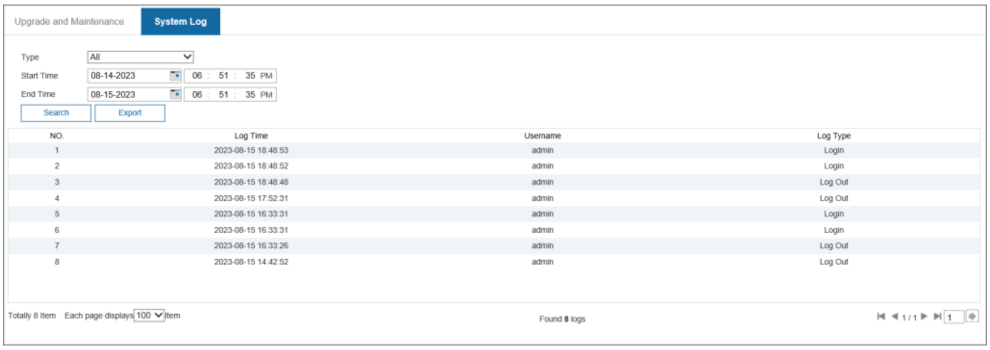
7.1.2.2 System Log

You can view and back up logs.

Procedure

Step 1 Select **Settings** > **System** > **Maintenance** > **System Log**.

Figure 7-5 System log



Type: All

Start Time: 08-14-2023 06 : 51 : 35 PM

End Time: 08-15-2023 06 : 51 : 35 PM

NO.	Log Time	Username	Log Type
1	2023-08-15 18:48:53	admin	Login
2	2023-08-15 18:48:52	admin	Login
3	2023-08-15 18:48:48	admin	Log Out
4	2023-08-15 17:52:31	admin	Log Out
5	2023-08-15 16:33:31	admin	Login
6	2023-08-15 16:33:31	admin	Login
7	2023-08-15 16:33:26	admin	Log Out
8	2023-08-15 14:42:52	admin	Log Out

Totally 8 Item Each page displays 100 Item

Found **8** logs

1/1 1

Step 2 Select the log type, and then configure the start time and end time.

The log type includes all, system operations, configuration operations, data management, event operations, recording operations, user management, and security.

- **System Operation**: Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
- **Configuration Operations**: Includes saving configuration and deleting configuration file.
- **Data Management**: Includes configuring disk type, clearing data, hot swap, FTP state, and record mode.
- **Event Operations** (records events such as video detection, smart plan, alarm and abnormality): Includes event start and event end.
- **Recording Operations**: Includes file access, file access error, and file search.
- **User Management**: Includes login, logout, adding user, deleting user, modifying user, adding group, deleting group, and modifying group.
- **Security**: Includes password resetting and IP filter.

Step 3 Click **Search**. The system displays the search results.

Step 4 (Optional) Click **Backup**, and then you can back up all searched logs to local computer.

7.1.3 Security

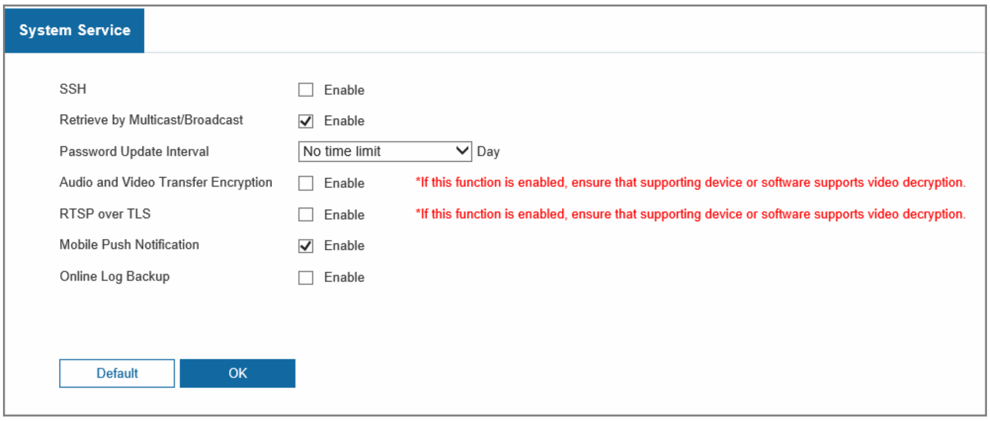
Configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log in to the webpage. This is to enhance network and data security.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Settings** > **System** > **Security** > **System Service**.

Figure 7-6 System service



System Service

SSH	□ Enable	
Retrieve by Multicast/Broadcast	☑ Enable	
Password Update Interval	No time limit Day	
Audio and Video Transfer Encryption	□ Enable	*If this function is enabled, ensure that supporting device or software supports video decryption.
RTSP over TLS	□ Enable	*If this function is enabled, ensure that supporting device or software supports video decryption.
Mobile Push Notification	☑ Enable	
Online Log Backup	□ Enable	

Default OK

Step 3 Enable the system service as needed.

Table 7-2 Description of system service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Retrieve by Multicast/Broadcast	Enable this function, and then when multiple users are viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
Password Update Interval	Configure the password update interval. If the password remains unchanged after the validity period expires, the system will prompt you to change password.
Audio and Video Transmission Encryption	Enable this function to encrypt audio/video transmission. 📖 Make sure that the other devices and software that working together with the camera support video decryption.
RTSP over TLS	Enable this function to encrypt the code transmitted through standard protocols. 📖 ● Make sure that the matched devices or software support video decryption function. ● We recommend you to enable the function. Otherwise, there might be risk of data leakage.
Mobile Push Notification	Enable this function, and then the system would send the snapshot that was taken when alarm is triggered to your phone. This is enabled by default.
Online Log Backup	Enable this function to back up the online log.

Step 4 Click **OK**.

7.1.4 User Management

7.1.4.1 User Mana.

You are admin user by default. You can add users, configure different permissions, and edit permissions.

7.1.4.1.1 Username

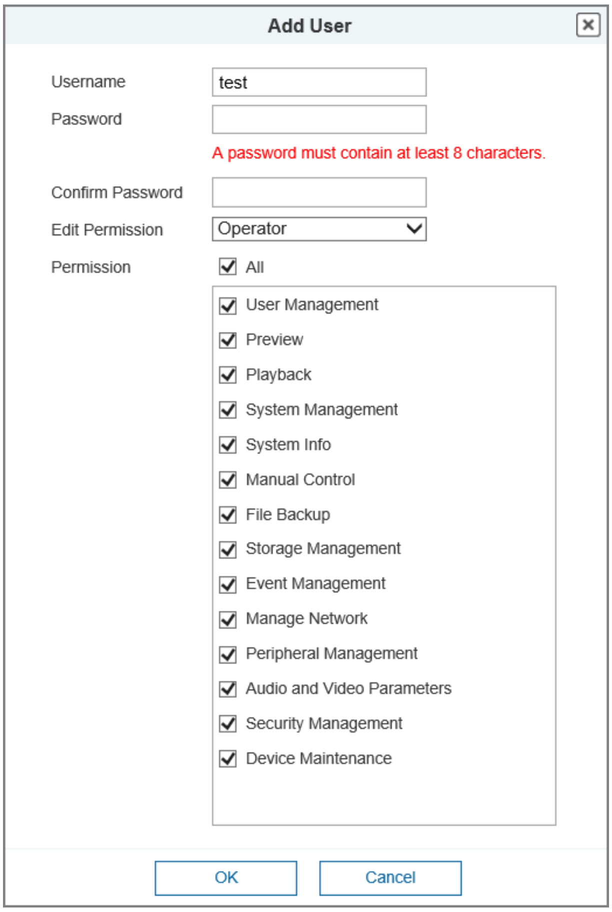
Procedure

Step 1 Log in to the webpage of the device.

Step 2 Select **Settings** > **System** > **User Management** > **User Mana.** > **Username**.

Step 3 Click **Add User**, and then configure the parameters.

Figure 7-7 Add user (operation permission)



Add User

Username: test

Password:

A password must contain at least 8 characters.

Confirm Password:

Edit Permission: Operator

Permission: ☑ All

- ☑ User Management
- ☑ Preview
- ☑ Playback
- ☑ System Management
- ☑ System Info
- ☑ Manual Control
- ☑ File Backup
- ☑ Storage Management
- ☑ Event Management
- ☑ Manage Network
- ☑ Peripheral Management
- ☑ Audio and Video Parameters
- ☑ Security Management
- ☑ Device Maintenance

Table 7-3 Description of user parameters

Parameter	Description
Username	The unique identification of the user. You cannot use the existing user name.
Password	Enter password and confirm it again. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Confirm Password	

Parameter	Description
Edit Permission	You can select from **Operator** or **User**. Different rules have different permissions.
Permission	Select the permissions for the user.

Step 4 Click **OK**.

Related Operations

- Edit user information

  Click ✏ to change password and permissions.

  For admin account, you can only edit the password.

  The methods of changing password vary with different accounts.

  - ◇ Log in with the admin account, you can change password through **Old Password** and **Admin Account**.
  - ◇ Log in with non-admin account (an added account with the permission of user management), you can change password through **Old Password**.
  - ◇ **Old Password**: Change the password through entering the old password to be changed, and then the new password.
  - ◇ **Admin Account**: Change the password through entering the admin password, and then the new password for the non-admin account to be changed.

- Delete the user

  Click ⊖ to delete the selected user.

  Users and user groups cannot be recovered after deletion.

7.1.4.1.2 User Group

You have two groups named operator and user by default, and you can add new group, delete added group or modify group authority and memo.

Procedure

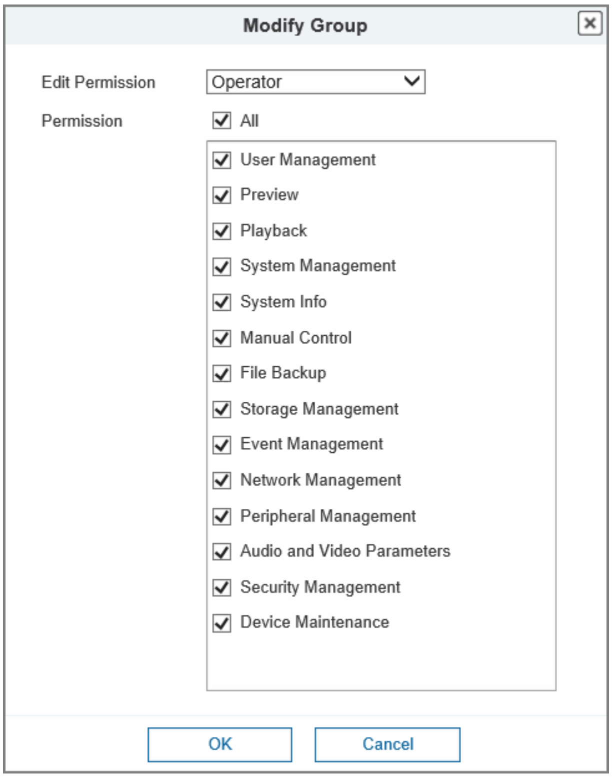
Step 1 Log in to the webpage of the device.

Step 2 Select **Settings** > **System** > **User Management** > **User Mana.** > **Edit Permission**.

Step 3 Click **Add Group**.

Step 4 Enter the group name, and then select the permissions.

Figure 7-8 Add user group



Modify Group

Edit Permission: Operator

Permission: ☑ All

- ☑ User Management
- ☑ Preview
- ☑ Playback
- ☑ System Management
- ☑ System Info
- ☑ Manual Control
- ☑ File Backup
- ☑ Storage Management
- ☑ Event Management
- ☑ Network Management
- ☑ Peripheral Management
- ☑ Audio and Video Parameters
- ☑ Security Management
- ☑ Device Maintenance

Table 7-4 Description of user group parameters

Permission	Function
Preview	Real-time stream view.
Playback	Playback view.
System Management	System time setting and more.
System Info	Version information, system logs and more.
Manual Control	PTZ settings.
File Backup	File backup.
Storage Management	Storage point configuration, snapshot recording time configuration, SFTP configuration and more.
Event Management	Video detection settings, audio detection settings, alarm settings and more.
Network Management	IP settings, SMTP settings, SNMP settings, AP Hotspot settings and more.
Peripheral Management	External light, wiper and serial port settings.
Audio and Video Parameters	Camera property settings, audio and video settings and more.
Security Management	HTTPS settings, RTSP over TLS settings and more.
Device Maintenance	Automatic maintenance settings and more.

Only user with specified permission can use corresponding function; the **Operator** group has all the permissions.

Step 5 Click **OK** to finish the configuration.

The newly added group is displays on the group name list.

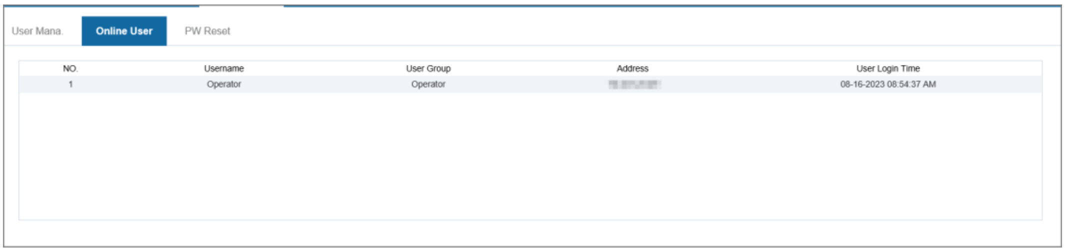
Related Operations

- Click ✎ to modify group permissions.
- Click ⊖ to delete the added group. **Operator** group and **User** group cannot be deleted.

7.1.4.2 Online User

Check the information of user which is currently online.

Figure 7-9 Online user

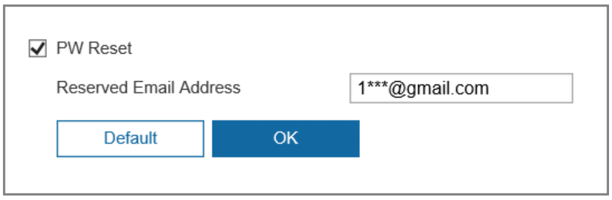


NO.	Username	User Group	Address	User Login Time
1	Operator	Operator	[redacted]	08-16-2023 08:54:37 AM

7.1.4.3 PW Reset

Reset the reserved email address for password reset as needed.

Figure 7-10 PW reset


☑ PW Reset

Reserved Email Address: 1***@gmail.com

7.2 Network

This section introduces network configuration.

7.2.1 TCP/IP

You can configure IP address and DNS (Domain Name System) server and so on according to network planning.

Prerequisites

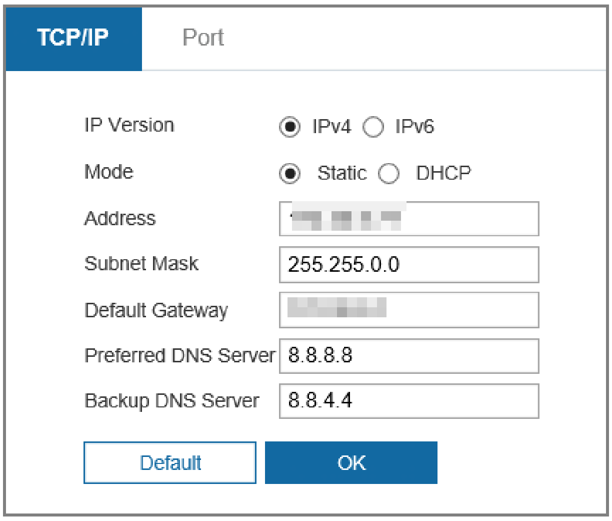
The camera has connected to the network.

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

Procedure

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

Figure 7-11 TCP/IP



IP Version ● IPv4 ○ IPv6

Mode ● Static ○ DHCP

Address [redacted]

Subnet Mask 255.255.0.0

Default Gateway [redacted]

Preferred DNS Server 8.8.8.8

Backup DNS Server 8.8.4.4

Step 2 Configure TCP/IP parameters.

Table 7-5 Description of TCP/IP parameters

Parameter	**Description**
IP Version	Select **IPv4** or **IPv6**.
Mode	The mode that the camera gets IP: ● **Static**: Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login page with the configured IP address is displayed. ● **DHCP**: When there is DHCP server in the network, select **DHCP**, and the camera acquires IP address automatically.
MAC Address	Displays host MAC address.
IP Version	Select **IPv4** or **IPv6**.
Address	When you select **Static** in **Mode**, enter the IP address and subnet mask that you need. ● IPv6 does not have subnet mask. ● The default gateway must be on the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS Server	IP address of the DNS server.
Backup DNS Server	Alternate IP address of the DNS server.

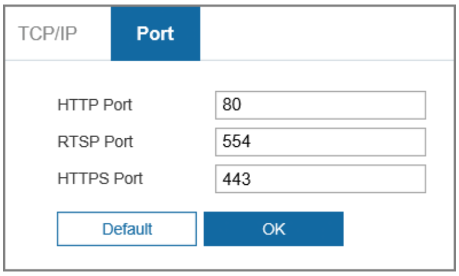
Step 3 Click **OK**.

7.2.2 Port

Procedure

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

Figure 7-12 Port



HTTP Port: 80
RTSP Port: 554
HTTPS Port: 443

Step 2 Configure port parameters.

- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- Do not use the same value of any other port during port configuration.

Table 7-6 Description of port parameters

Parameter	Description
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	● Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. ● When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. ● When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Among that: ● Username: The username, such as admin. ● Password: The password, such as admin. ● IP: The device IP, such as 192.168.1.112. ● Port: Leave it if the value is 554 by default. ● Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. ● Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Apply**.

7.2.3 P2P

P2P (peer-to-peer) technology enables users to manage devices easily without requiring DDNS, port mapping or transit server.

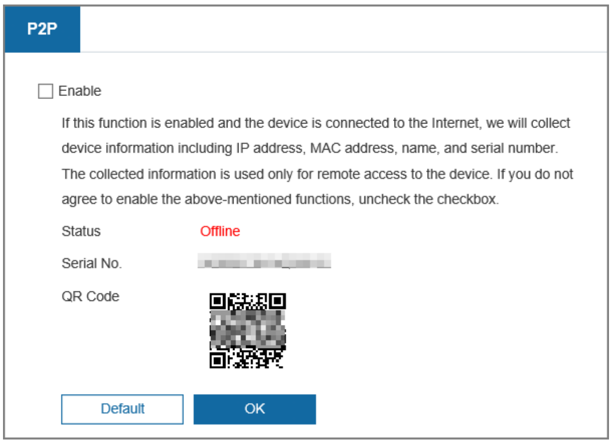
Background Information

Scan the QR code with your smartphone, and then you can add and manage more devices on the mobile phone client.

Procedure

Step 1 Select **Settings** > **Network** > **P2P**.

Figure 7-13 P2P



□ Enable

If this function is enabled and the device is connected to the Internet, we will collect device information including IP address, MAC address, name, and serial number. The collected information is used only for remote access to the device. If you do not agree to enable the above-mentioned functions, uncheck the checkbox.

Status Offline

Serial No. [redacted]

QR Code

- When P2P is enabled, remote management on device is supported.
- When P2P is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You can cancel **Enable** selection to reject the collection.

Step 2 Log in to mobile phone client, and then tap **Device management**.

Step 3 Tap **+** at the upper-right corner.

Step 4 Scan the QR code on the **P2P** page.

Step 5 Follow the instructions to finish the settings.

7.2.4 DDNS

Properly configure DDNS, and then the domain name on the DNS server matches your IP address and the matching relation refreshes in real time. You can always visit the camera with the same domain name no matter how the IP address changes.

Prerequisites

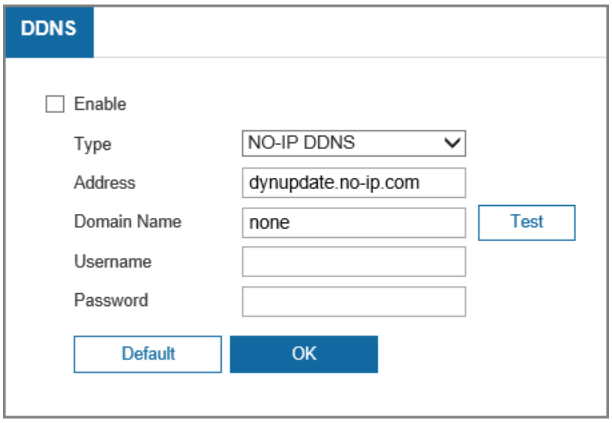
Check the type of DNS server supported by the camera.

Procedure

Step 1 Select **Settings** > **Network** > **DDNS**.

- Third-party server might collect your device information after DDNS is enabled.
- Register and log in to the DDNS website, and then you can view the information of all the connected devices in your account.

Figure 7-14 DDNS



□ Enable

Type: NO-IP DDNS

Address: dynupdate.no-ip.com

Domain Name: none

Username:

Password:

<u>Step 2</u> Select the **Enable** checkbox to enable the function.

<u>Step 3</u> Configure DDNS parameters.

Table 7-7 Description of DDNS parameters

Parameter	**Description**
Type	The name and web address of the DDNS service provider, see the matching relationship below: ● CN99 DDNS: www.3322.org. ● NO-IP DDNS: dynupdate.no-ip.com. ● Dvrlists: ns1.dvrlists.com.
Address	
Domain Name	The domain name you registered on the DDNS website.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the DDNS server provider's website.
Password	

<u>Step 4</u> Click **OK**.

Result

Open the browser on your computer, then enter domain name at the address bar and press **Enter**, the login page is displayed.

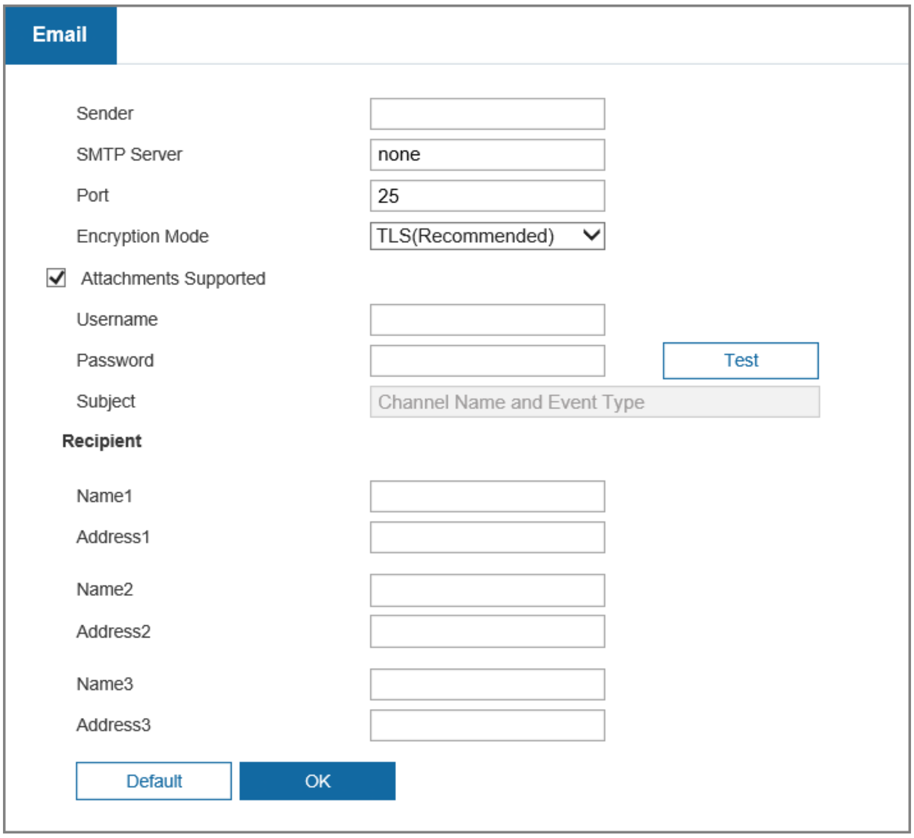
7.2.5 Email

Configure email parameter and enable email linkage. The system sends email to the defined address when the corresponding alarm is triggered.

Procedure

<u>Step 1</u> Select **Settings** > **Network** > **Email**.

Figure 7-15 Email



Sender	
SMTP Server	none
Port	25
Encryption Mode	TLS(Recommended)
☑ Attachments Supported	
Username	
Password	
Subject	Channel Name and Event Type
Recipient	
Name1	
Address1	
Name2	
Address2	
Name3	
Address3	

Step 2 Configure email parameters.

Table 7-8 Description of email parameters

Parameter	Description	
SMTP Server	SMTP server address	For details, see Table 7-9.
Port	The port number of the SMTP server.	
Username	The account and password of SMTP server. Click **Test** to check whether the email address is available or not.	
Password		
Sender	Sender's email address.	
Encryption Mode	Select from **None**, **SSL** and **TLS**. For details, see Table 7-9.	
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click + to select title type, including **Device Name**, **Device ID**, and **Event Type**, and you can set maximum 2 titles.	
Attachment Supported	Select the checkbox to support attachment in the email.	
Recipient	● Receiver's email address. Supports 3 addresses at most. ● After entering the receiver's email address, the **Test** button is displayed. Click **Test** to test whether the emails can be sent and received successfully.	

Table 7-9 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
Gmail	smtp.gmail.com	SSL	465	You need to enable SMTP service in your mailbox.
		TLS	587	

Step 3 Click **OK**.

7.2.6 PPPoE

Point-to-Point Protocol over Ethernet, is one of the protocols that device uses to connect to the internet. Get the PPPoE username and password from the internet service provider, and then set up network connection through PPPoE, the camera will acquire a WAN dynamic IP address.

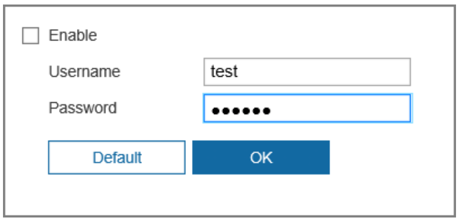
Prerequisites

- The camera has connected to the network.
- You have gotten the account and password from Internet Service Provider.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **PPPoE Settings**.

Figure 7-16 PPPoE



□ Enable

Username: test

Password: ••••••

Step 2 Select the **Enable** checkbox, and then enter username and password.

- Disable UPnP while using PPPoE to avoid possible influence.
- After making PPPoE connection, the device IP address cannot be modified through webpage.

Step 3 Click **OK**.

The success prompt box is displayed, and then the real-time WAN IP address is displayed. You can access camera through the IP address.

7.2.7 UPnP

UPnP (Universal Plug and Play) is a protocol that establishes mapping relation between local area and wide area networks. This function enables you to access local area device through wide area IP address.

Prerequisites

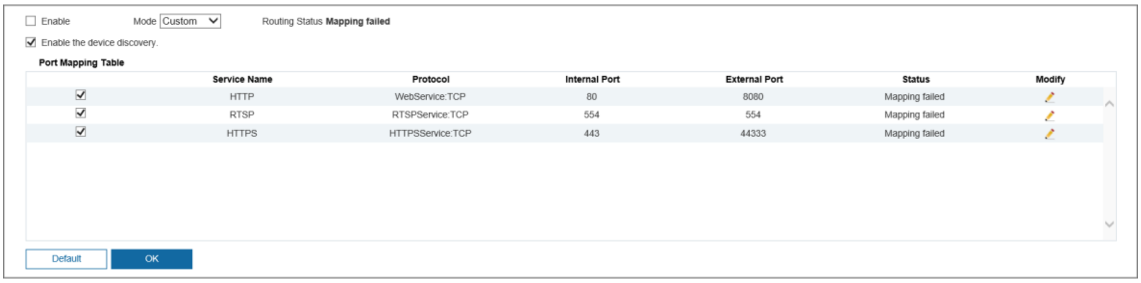
- Make sure the UPnP service is installed in the system.
- Log in to the router, and configure WAN IP address to set up internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.

- Select **Settings** > **Network** > **TCP/IP** > **TCP/IP**, in **Address**, enter the local area IP address of the router or select **DHCP** and acquires IP address automatically.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **UPnP**.

Figure 7-17 UPnP



□ Enable Mode Custom Routing Status **Mapping failed**

☑ Enable the device discovery.

Port Mapping Table

	Service Name	Protocol	Internal Port	External Port	Status	Modify
☑	HTTP	WebService:TCP	80	8080	Mapping failed	✎
☑	RTSP	RTSPService:TCP	554	554	Mapping failed	✎
☑	HTTPS	HTTPSService:TCP	443	44333	Mapping failed	✎

Step 2 Select the **Enable** checkbox, and there are two mapping modes: **Custom** and **Default**.

- Select **Custom**, click ✎ and then you can change external port as needed.
- Select **Default**, and then the system finishes mapping with unoccupied port automatically, and you cannot edit mapping relation.

Step 3 Click **OK**.

Open web browser on PC, enter http:// *wide area IP address: external port number*, and then you can visit the local area device with corresponding port.

7.2.8 SNMP

SNMP (Simple Network Management Protocol), which can be used to enable software such as MIB Builder and MG-SOFT MIB Browser to connect to the camera and manage and monitor the camera.

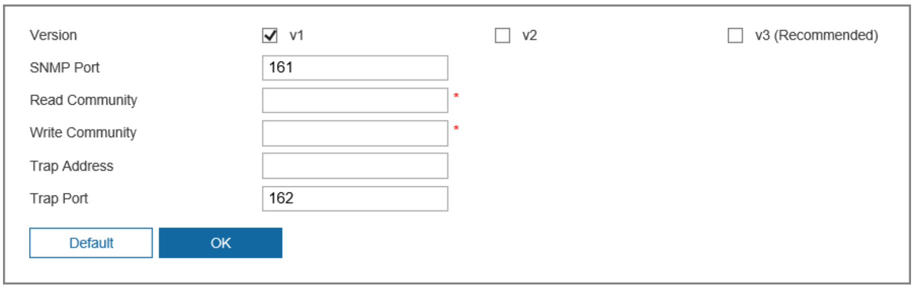
Prerequisites

- Install SNMP monitoring and managing tools such as MIB Builder and MG-SOFT MIB Browser.
- Get the MIB file of the matched version from technical support.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **SNMP**.

Figure 7-18 SNMP (1)



Version ☑ v1 □ v2 □ v3 (Recommended)

SNMP Port: 161

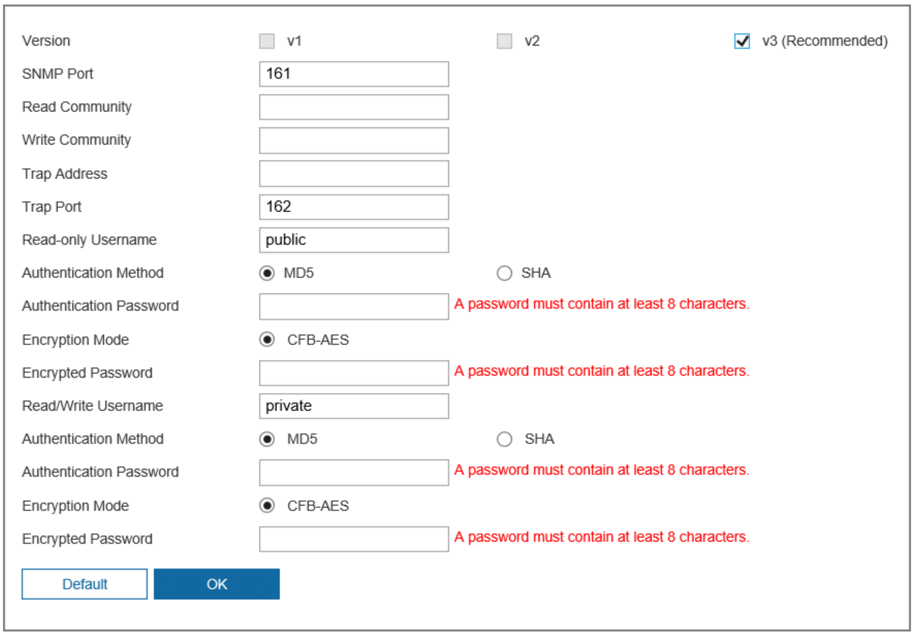
Read Community: *

Write Community: *

Trap Address:

Trap Port: 162

Figure 7-19 SNMP (2)



Version ☐ v1 ☐ v2 ☑ v3 (Recommended)

SNMP Port: 161

Read Community:

Write Community:

Trap Address:

Trap Port: 162

Read-only Username: public

Authentication Method: ● MD5 ○ SHA

Authentication Password: A password must contain at least 8 characters.

Encryption Mode: ● CFB-AES

Encrypted Password: A password must contain at least 8 characters.

Read/Write Username: private

Authentication Method: ● MD5 ○ SHA

Authentication Password: A password must contain at least 8 characters.

Encryption Mode: ● CFB-AES

Encrypted Password: A password must contain at least 8 characters.

Step 2 Select the version to enable SNMP.

- Select **V1**, and the system can only process information of V1 version.
- Select **V2**, and the system can only process information of V2 version.
- Select **V3**, and then **V1** and **V2** become unavailable. You can configure username, password and authentication type. It requires corresponding username, password and authentication type to visit your device from the server.

Using **V1** and **V2** might cause data leakage, and **V3** is recommended.

Step 3 In **Trap Address**, enter the IP address of the PC that has MIB Builder and MG-SOFT MIB Browser installed, and leave other parameters to the default.

Table 7-10 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports. You can enter number, letter, underline and dash to form the name.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.

Parameter	Description
Read-only Username	Set the read-only username accessing device, and it is **public** by default. You can enter number, letter, and underline to form the name.
Authentication Method	You can select from **MD5** and **SHA**. The default type is **MD5**.
Authentication Password	It should be no less than 8 characters.
Encryption Mode	The default is CBC-DES.
Encryption Password	It should be no less than 8 characters.
Read/Write Username	Set the read/write username access device, and it is **public** by default. You can enter number, letter, and underline to form the name.

Step 4 Click **OK**.

Result

View device configuration through MIB Builder or MG-SOFT MIB Browser.

1. Run MIB Builder and MG-SOFT MIB Browser.
2. Compile the two MIB files with MIB Builder.
3. Load the generated modules with MG-SOFT MIB Browser.
4. Enter the IP address of the device you need to manage in the MG-SOFT MIB Browser, and then select version to search.
5. Unfold all the tree lists displayed in the MG-SOFT MIB Browser, and then you can view the configuration information, video channel amount, audio channel amount, and software version.

Use computer with Windows and disable SNMP Trap service. The MG-SOFT MIB Browser will display prompt when alarm is triggered.

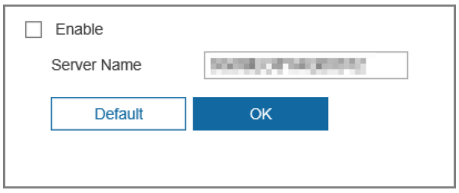
7.2.9 Bonjour

Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **Bonjour**.

Figure 7-20 Bonjour



Step 2	Select the **Enable** checkbox, and then configure server name.

Step 3	Click **OK**.

Result

In the OS and clients that support Bonjour, follow the steps below to visit the network camera with Safari browser.

1. Click **Show All Bookmarks** in Safari.
2. Enable **Bonjour**. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click the camera to visit the corresponding webpage.

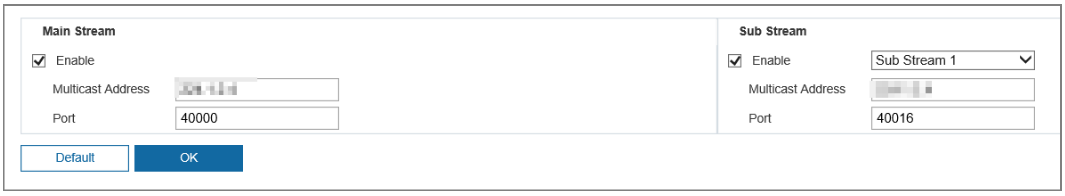
7.2.10 Multicast

When multiple users are viewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Procedure

Step 1	Select **Settings** > **Network** > **Advanced** > **Multicast**.

Figure 7-21 Multicast



Main Stream

☑ Enable

Multicast Address [redacted]

Port 40000

Sub Stream

☑ Enable Sub Stream 1

Multicast Address [redacted]

Port 40016

Step 2	Select the **Enable** checkbox, and then enter multicast address and port.

Table 7-11 Description of multicast parameters

Parameter	Description
Multicast Address	The multicast IP address of **Main Stream**/**Sub Stream** is 224.1.2.4 by default, and the range is 224.0.0.0–239.255.255.255.
Port	The multicast port of corresponding stream: **Main Stream**: 40000; **Sub Stream1**: 40016; **Sub Stream2**: 40032, and all the range is 1025–65500.

Step 3	Click **OK**.

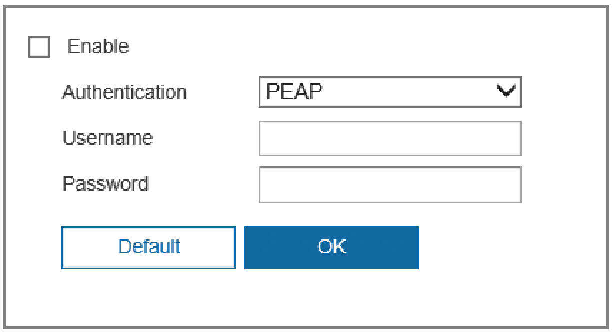
7.2.11 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Procedure

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

Figure 7-22 802.1x



Step 2 Select the **Enable** checkbox, and then configure the parameters.

Table 7-12 Description of 802.1x parameters

Parameter	Description
Authentication	PEAP (Protected EAP Protocol).
Username	The username that was authenticated on the server.
Password	Corresponding password.

Step 3 Click **OK**.

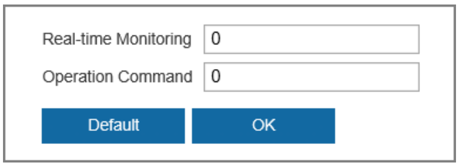
7.2.12 QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience. 0–63 means 64 degrees of priority; 0 for the lowest and 63 for the highest.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **QoS**.

Figure 7-23 QoS


Real-time Monitoring: 0
Operation Command: 0

Step 2 Configure QoS parameters.

Table 7-13 Description of QoS parameters

Parameter	Description
Real-time Monitoring	Configure the priority of the data packets that used for network surveillance. 0 for the lowest and 63 for the highest.
Operation Command	Configure the priority of the data packets that used for configure or checking.

Step 3 Click **OK**.

7.2.13 RTMP

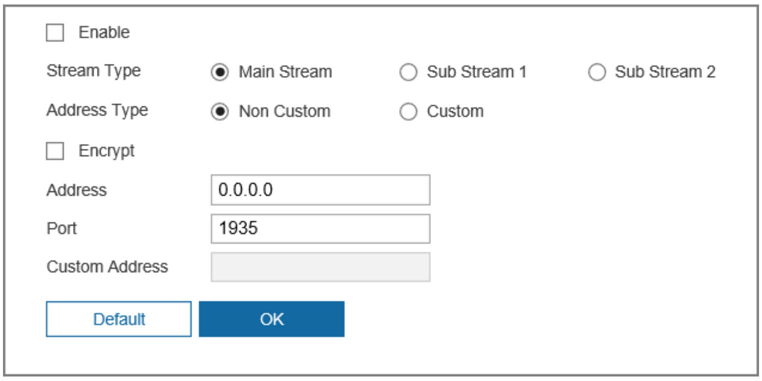
Through RTMP, you can access a third-party platform (such as Ali and YouTube) to realize video live view.

- RTMP can be configured by admin only.
- RTMP supports the H.264, H.264 B and H.264H video formats, and the AAC audio format only.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **RTMP**.

Figure 7-24 RTMP



□ Enable

Stream Type ● Main Stream ○ Sub Stream 1 ○ Sub Stream 2

Address Type ● Non Custom ○ Custom

□ Encrypt

Address 0.0.0.0

Port 1935

Custom Address

Step 2 Select the **Enable** checkbox.

Make sure that the IP address is trustable when enabling RTMP.

Step 3 Configure RTMP parameters.

Table 7-14 Description of RTMP parameters

Parameter	**Description**
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	● **Non-custom**: Enter the server IP and domain name. ● **Custom**: Enter the path allocated by the server.
Address	When selecting **Non-custom**, you need to enter server IP address and port. ● **IP address**: Support IPv4 or domain name. ● **Port**: Keep the default value.
Port	
Custom Address	When selecting **Custom**, you need to enter the path allocated by the server.

Step 4 Click **OK**.

7.2.14 FTP

FTP can be enabled only when it was selected as a destination path. When the network does not work, you can save all the files to the internal SD card for emergency.

Prerequisites

This function is available only when the video recording type and snapshot type is **FTP**. For details, see "7.6.2.1 Storage Location".

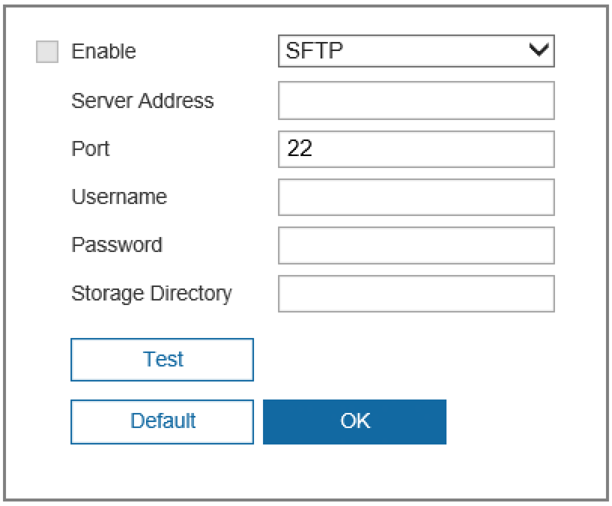
Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **FTP**.

Step 2 Select the **Enable** checkbox, and then configure the parameters.

You can select **FTP** or **SFTP** from the drop-down list. **SFTP** is recommended to enhance network security.

Figure 7-25 FTP



□ Enable SFTP

Port 22

Table 7-15 Description of FTP parameters

Parameter	Description
Server Address	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Directory	The destination path in the FTP server.

Step 3 Click **Test** to test whether the FTP function works normally.

Step 4 Click **OK**.

7.2.15 NAS

Enable this function to save all the files in the NAS.

Prerequisites

This function is available only when the video recording type and snapshot type is **NAS**. For details, see "7.6.2.1 Storage Location".

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **NAS**.

Step 2 Select the **Enable** checkbox.

Step 3 Configure NAS parameters.

Figure 7-26 NAS

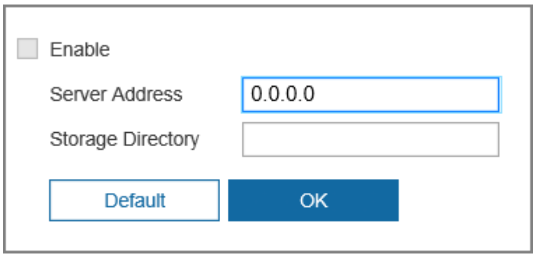


Table 7-16 Description of NAS parameters

Parameter	**Description**
Server Address	The IP address of the NAS server.
Storage Directory	The destination path in the NAS server.

Step 4 Click **OK**.

7.2.16 HTTPS

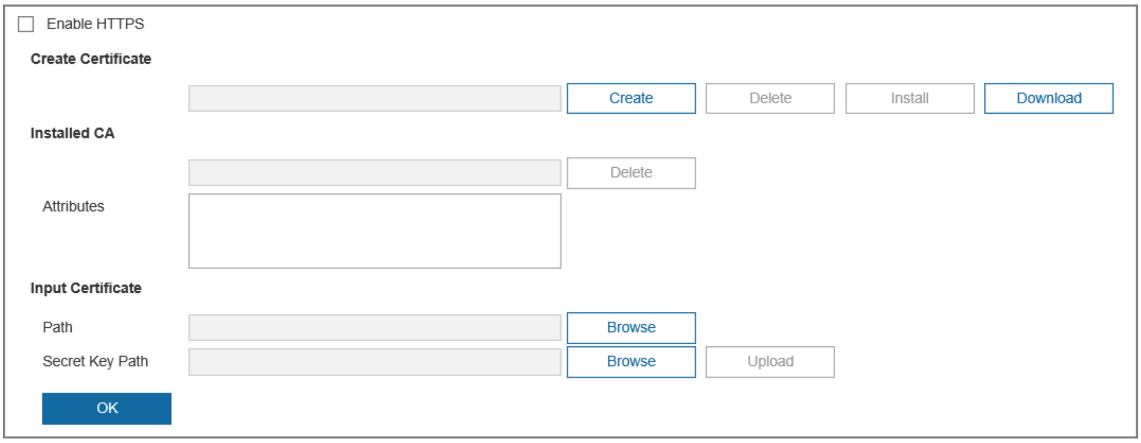
Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your computer. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure

Step 1 Select the **Settings** > **Network** > **Advanced** > **HTTPS**.

Step 2 Select **Enable HTTPS** checkbox.

Figure 7-27 HTTPS



Step 3 Create a certificate or upload an authenticated certificate.

- For creating a certificate, click **Create**.
- For uploading the authenticated certificate, click **Browse** to select the certificate and certificate key, click **Upload** to upload them, and then skip to Step6.

Step 4 Enter the required information, and then click **Create**.

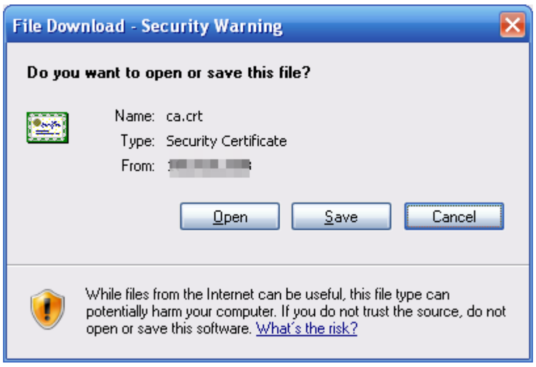
The entered **IP/Domain name** must be the same as the IP or domain name of the device.

Step 5 Click **Install**.

Step 6 Click **Download** to download root certificate.

Step 7 Click **Download Root Certificate**.

Figure 7-28 File download



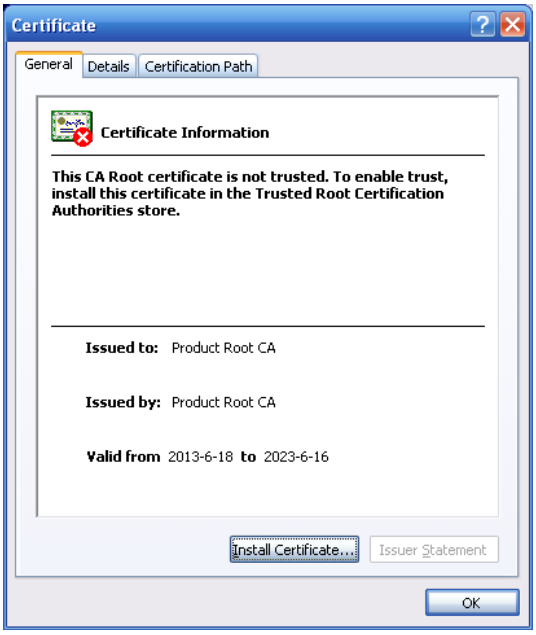
Do you want to open or save this file?

Name: ca.crt
Type: Security Certificate
From: [redacted]

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Step 8 Click **Open**.

Figure 7-29 Certificate information



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

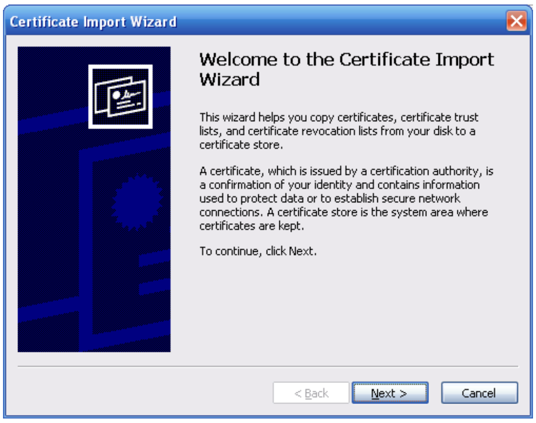
Issued to: Product Root CA

Issued by: Product Root CA

Valid from 2013-6-18 to 2023-6-16

Step 9 Click **Install Certificate**.

Figure 7-30 Certificate import wizard (1)



Welcome to the Certificate Import Wizard

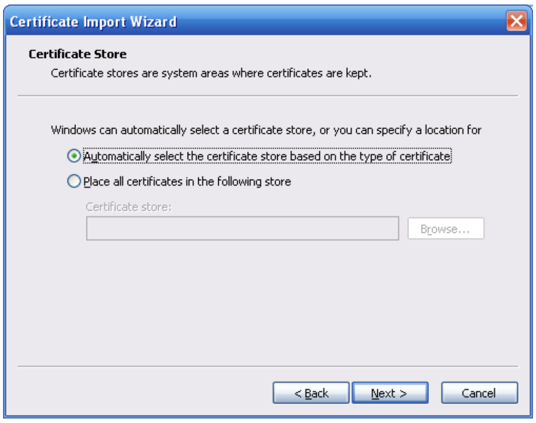
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 10 Click **Next**.

Figure 7-31 Certificate store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

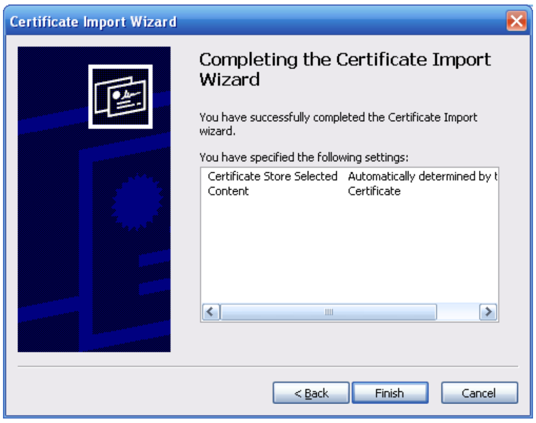
◉ Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Step 11 Select the storage location and click **Next**.

Figure 7-32 Certificate import wizard (2)



Certificate Import Wizard

Completing the Certificate Import Wizard

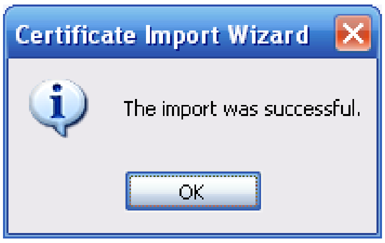
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

Step 12 Click **Finish**, and then a dialog box showing **The import was successful** pops up.

Figure 7-33 Import succeeds



Certificate Import Wizard

The import was successful.

7.2.17 Firewall

Configure **Network Access**, **Disable PING** or **Half-open Connection Prevention** to enhance network and data security. This section takes **Network Access** as an example.

Background Information

- **Network Access**: Set allowlist and blocklist to limit access.
  - ◇ **Allowlist**: Only when the IP/MAC of your computer in the allowlist, can you access the camera. Ports are the same.
  - ◇ **Blocklist**: When the IP/MAC of your computer is in the blocklist, you cannot access the camera. Ports are the same.
- **Disable PING**: Enable the **Disable PING** function, and the camera will not respond to the ping request.

- **Half-open connection prevention**: Enable **Half-open connection prevention** function, and the camera can provide service normally under Semijoin attack.

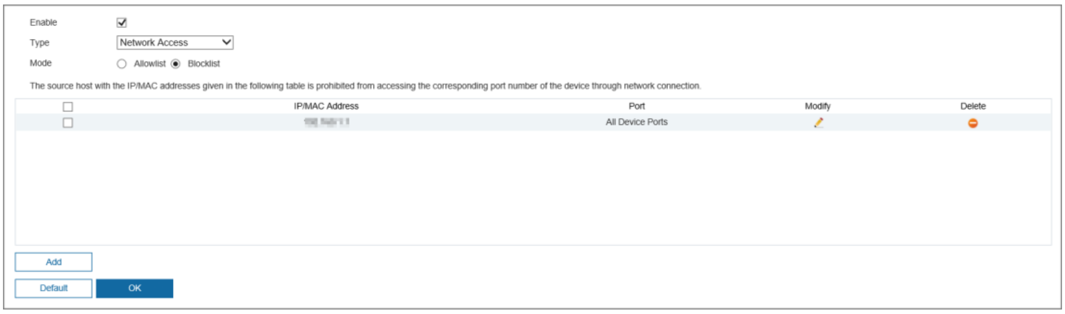
- You cannot set allowlist or blocklist for camera IP or MAC addresses.
- You cannot set allowlist or blocklist for port MAC addresses.
- MAC verification takes effect when the IP addresses of the camera and your computer are in the same LAN.
- When you access the camera through internet, the camera verifies the MAC address according to the router MAC.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **Firewall**.

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

Figure 7-34 Firewall



Enable ☑

Type: Network Access

Mode ○ Allowlist ● Blocklist

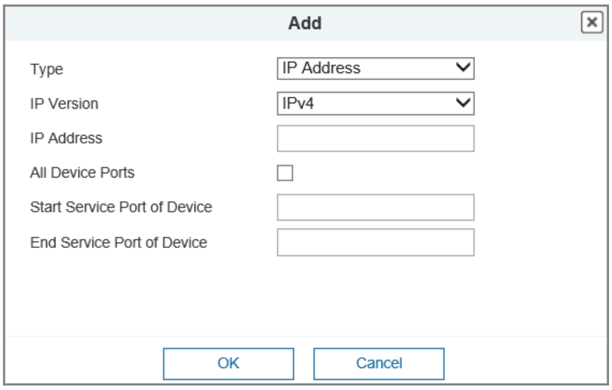
The source host with the IP/MAC addresses given in the following table is prohibited from accessing the corresponding port number of the device through network connection.

□	IP/MAC Address	Port	Modify	Delete
□	[redacted]	All Device Ports	✎	⊖

Step 3 Select **Network Access** from **Type** list, and then select the mode.

Step 4 Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 7-35 Firewall



Add

Type: IP Address

IP Version: IPv4

IP Address

All Device Ports □

Start Service Port of Device

End Service Port of Device

Step 5 Click **OK**.

Related Operations

- Click ✎ to edit the host information.
- Click ⊖ to delete the host information.

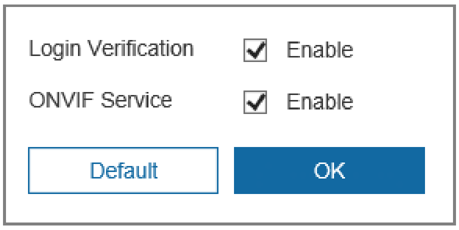
7.2.18 ONVIF

The ONVIF verification is enabled by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.

Procedure

Step 1 Select **Settings** > **Network** > **Advanced** > **ONVIF**.

Figure 7-36 ONVIF



Login Verification ☑ Enable

ONVIF Service ☑ Enable

Step 2 Select the **Enable** checkbox next to **ONVIF Verification** and **ONVIF Service**.

Step 3 Click **OK**.

7.2.19 Remote Log Records

Configure remote log, and then you can get the related log by accessing the defined address.

Procedure

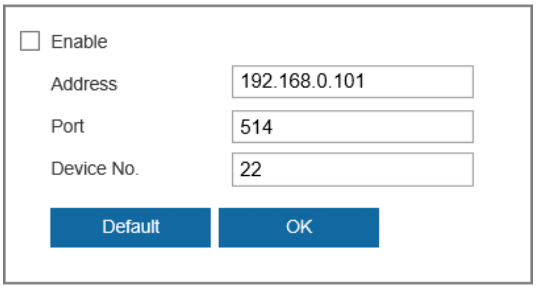
Step 1 Select **Settings** > **Network** > **Advanced** > **Remote Log Records**.

Step 2 Select **Enable** checkbox to enable remote log function.

Step 3 Set address, port and device number.

Step 4 Click **OK**.

Figure 7-37 Remote log



☐ Enable

Address 192.168.0.101

Port 514

Device No. 22

7.3 Video/Audio

7.3.1 Video

This section describes how to set the video stream for the monitoring screen.

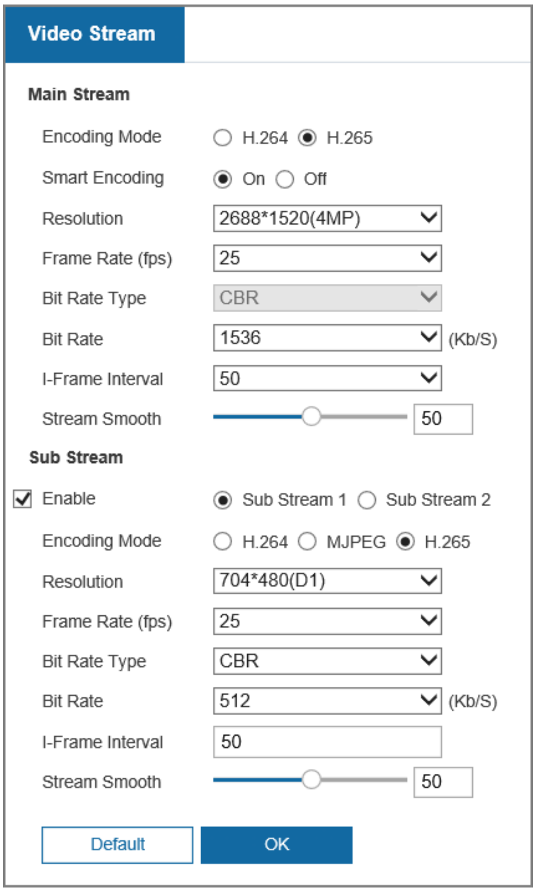
Procedure

Step 1 Select **Settings** > **Video/Audio** > **Video** > **Video Stream**.

Step 2 Configure video stream parameters.

- The stream configuration pages might vary depending on devices.
- The default bit rate of different devices might vary depending on different products.

Figure 7-38 Video stream



Video Stream

Main Stream

Encoding Mode ○ H.264 ● H.265

Smart Encoding ● On ○ Off

Resolution 2688*1520(4MP)

Frame Rate (fps) 25

Bit Rate Type CBR

Bit Rate 1536 (Kb/S)

I-Frame Interval 50

Stream Smooth 50

Sub Stream

☑ Enable ● Sub Stream 1 ○ Sub Stream 2

Encoding Mode ○ H.264 ○ MJPEG ● H.265

Resolution 704*480(D1)

Frame Rate (fps) 25

Bit Rate Type CBR

Bit Rate 512 (Kb/S)

I-Frame Interval 50

Stream Smooth 50

Default OK

Table 7-17 Description of video stream parameters

Parameter	Description
Encoding Mode	Select encode mode. Compared with H.264, H.265 requires smaller bandwidth.
Smart Encoding	Enable smart encoding to improve video compressibility and save storage space. It is applicable to static scenes.
Resolution	The resolution of the video. The higher the value, the clearer the image, but the bigger the bandwidth will be required.
Frame Rate (fps)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.

Parameter	Description
Bit Rate Type	The bit rate control type during video data transmission. You can select bit rate type from: ● **CBR** (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. ● **VBR** (Variable Bit Rate): The bit rate changes as monitoring scene changes. The **Bit Rate Type** can be only be set as **CBR** when **Smart Encoding** is set as **On**.
Bit Rate	Select bit rate value in the list according to actual condition.
I Frame Interval	The number of P frames between two I frames. The range varies with the frame rate, and the maximum value is 150. We recommend you set the interval twice the frame rate.
Stream Smooth	Drag ○ to set the value of **Stream Smooth**. The higher the value, the less smooth the stream, but the higher the image definition.

Step 3 Click **OK**.

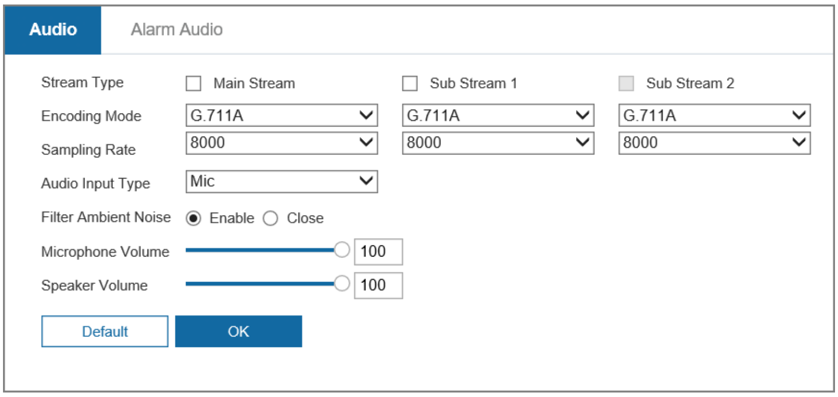
7.3.2 Audio

7.3.2.1 Configuring Audio

Procedure

Step 1 Select **Settings** > **Video/Audio** > **Audio** > **Audio**.

Figure 7-39 Audio



Stream Type: □ Main Stream □ Sub Stream 1 □ Sub Stream 2

Encoding Mode: G.711A | G.711A | G.711A

Sampling Rate: 8000 | 8000 | 8000

Audio Input Type: Mic

Filter Ambient Noise: ● Enable ○ Close

Microphone Volume: 100

Speaker Volume: 100

Step 2 Select the stream type from **Main Stream**, **Sub Stream 1** and **Sub Stream 2**.

Step 3 Configure audio parameters.

Table 7-18 Description of audio parameters

Parameter	Description
Encoding Mode	You can select from **PCM**, **G.711A**, **G.711Mu**, **G.726**, **AAC**, **G.723**. The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Rate	Sampling number per second. The higher the sampling rate is, the more the sample in a second will be, and the more accuracy the restored signal will be. You can select from **8000**, **16000**, **32000**, **48000**, **64000**.
Audio Input Type	You can select audio input type from **LineIn**, **Mic** and **realMic**.
Filter Ambient Noise	Enable this function, the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

Step 4 Click **OK**.

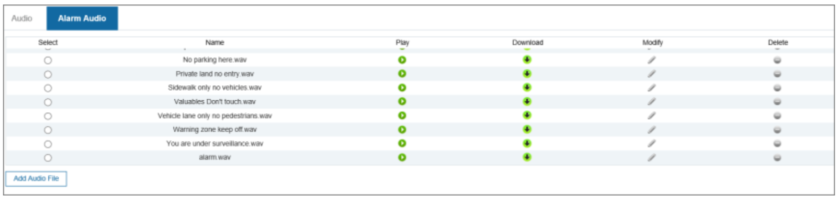
7.3.2.2 Configuring Alarm Audio

You can record and upload alarm audio file. The audio file will be played when the alarm is triggered.

Procedure

Step 1 Select **Settings** > **Video/Audio** > **Audio** > **Alarm Audio**.

Figure 7-40 Alarm audio



Select	Name	Play	Download	Modify	Delete
○	No parking here.wav	▶	⬇	✎	⊖
○	Private land no entry.wav	▶	⬇	✎	⊖
○	Sidewalk only no vehicles.wav	▶	⬇	✎	⊖
○	Valuables Don't touch.wav	▶	⬇	✎	⊖
○	Vehicle lane only no pedestrians.wav	▶	⬇	✎	⊖
○	Warning zone keep off.wav	▶	⬇	✎	⊖
○	You are under surveillance.wav	▶	⬇	✎	⊖
○	alarm.wav	▶	⬇	✎	⊖

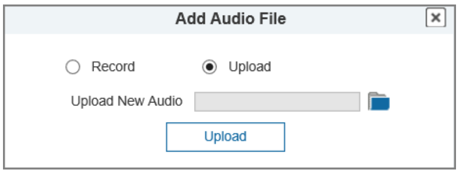
Step 2 Click **Add Audio File**.

Step 3 Configure the audio file.

- Select **Record**, enter the audio name in the input box, and then click **Record**.
- Select **Upload**, click **Browse** to select the audio file to be uploaded, and then click **Upload**.

- The camera supports recording audio file in .pcm format only. Recording is only supported by select models.
- You can upload audio files in .pcm, .wav2, .mp3, or .aac format.

Figure 7-41 Add audio file



Add Audio File

○ Record ● Upload

Upload New Audio

Step 4 Select the file that you need.

Related Operations

- Edit audio file

  Click ✎ to edit the file name.
- Delete audio file

  Click ⊖ to delete the file name.
- Play audio file

  Click ▶ to play the file name.
- Download audio file

  Click ⬇ to download the file name.

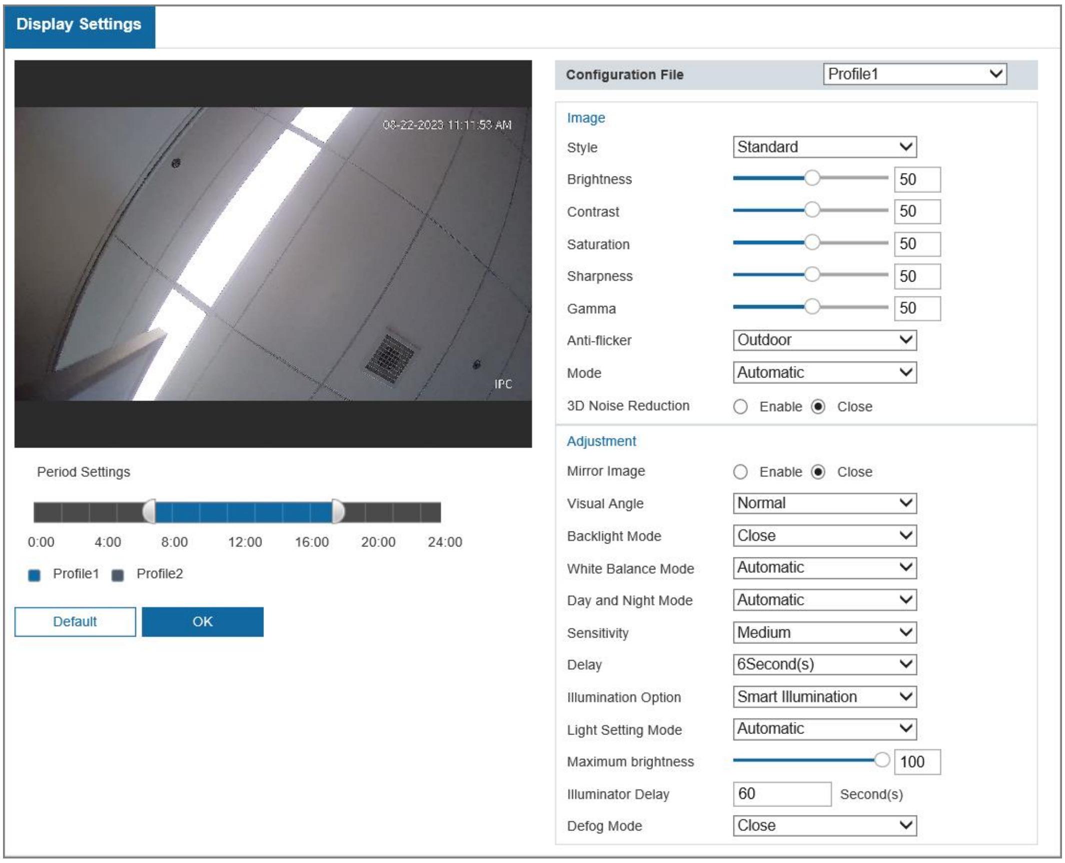
7.4 Image

7.4.1 Display Settings

Procedure

Step 1 Select **Settings** > **Image** > **Display Settings**.

Figure 7-42 Display settings



Period Settings

■ Profile1 ■ Profile2

Configuration File	Profile1
Image	
Style	Standard
Brightness	50
Contrast	50
Saturation	50
Sharpness	50
Gamma	50
Anti-flicker	Outdoor
Mode	Automatic
3D Noise Reduction	○ Enable ● Close
Adjustment	
Mirror Image	○ Enable ● Close
Visual Angle	Normal
Backlight Mode	Close
White Balance Mode	Automatic
Day and Night Mode	Automatic
Sensitivity	Medium
Delay	6Second(s)
Illumination Option	Smart Illumination
Light Setting Mode	Automatic
Maximum brightness	100
Illuminator Delay	60 Second(s)
Defog Mode	Close

Step 2 Configure the **Period Settings**.

Profile 1 means daytime; **Profile 2** means night. Slide the bar to configure the period for daytime and night correspondingly.

Step 3 Configure the settings for **Profile 1** and **Profile 2**.

Table 7-19 Description of display settings

Parameter	Description
Style	Select the picture style from soft, standard and vivid. ● **Standard**: Default image style, displays the actual color of the image. ● **Soft**: The hue of the image is weaker than the actual one, and contrast is smaller. ● **Vivid**: The image is more vivid than the actual one.
Brightness	Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.
Contrast	Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.
Saturation	Makes the color deeper or lighter. The higher the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change image brightness.
Sharpness	Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be, and if the value is set too big, picture noises are more likely to appear.
Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The higher the value is, the brighter the picture will be, and the smaller the darker.
Anti-flicker	You can select from 50 Hz, 60 Hz and Outdoor. ● **50 Hz**: When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. ● **60 Hz**: When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. ● **Outdoor**: You can select any exposure mode as needed.
Mode	Device exposure modes. ● **Automatic**: Adjusts the image brightness according to the actual condition automatically. ● **Manual**: Configure gain and shutter value manually to adjust image brightness.
3D Noise Reduction	3D noise reduction is the process of removing noise from a signal. The higher the grade, the less the noise, and the blurrier the image.
Time Domain Level	Calculating the noise reduction by comparing different frames. Sets the value, and it ranges from 0 to 50.
Spatial Domain Level	Take algorithmic noise reduction for single frame picture. Sets the value, and it ranges from 0 to 50.
Mirror Image	Select **Enable**, and the picture would display with left and right sides reversed.

Parameter	Description
Visual Angle	Change the display direction of the image.
Backlight Mode	Adjust the backlight compensation mode of the monitoring screen. ● **Close**: Backlight is disabled. ● **Backlight Compensation**: Backlight compensation corrects regions with extremely high or low levels of light to maintain a normal and usable level of light for the object in focus. ● **Highlight Compensation**: Highlight compensation dims strong light, so that the camera can capture details of faces and license plates in extreme light conditions. It is applicable to the entrance and exit of toll stations or parking lots. ● **Wide Dynamic Range**: When in WDR (Wide Dynamic Range) mode, the camera constrains over bright areas and compensates dark areas to improve the image clarity. ● **Scene-adaptive**: The system automatically adjusts image brightness according to ambient lighting condition to ensure image clarity.
White Balance Mode	White balance function makes the image color display precisely as it is. When in White Balance mode, white objects will always display white color in different environments. ● **Automatic**: The system compensates white balance according to color temperature to ensure color precision. ● **Daylight**: The system automatically compensates white balance to environments without artificial light to ensure color precision. ● **Street Lamp**: The system compensates white balance to outdoor night scene to ensure color precision. ● **Outdoor**: The system auto compensates white balance to most outdoor environments with natural or artificial light to ensure color precision. ● **Manual**: Configure red and blue gain manually; the system auto compensates white balance according to color temperature. ● **Custom Area**: The system compensates white balance only to the set area according to color temperature to ensure color precision.
Day and Night Mode	Configure the display mode of the image. The system switches between color and black-and-white modes according to the actual condition. ● **Automatic**: The system switches between color and black-and-white display according to the actual condition. ● **Full Color**: The system displays color image. ● **Black & White**: The system displays black-and-white image.
Sensitivity	This configuration is available only when you set **Auto** in **Day and Night Mode**. You can configure camera sensitivity when switching between color and black-and-white modes.

Parameter	Description
Delay	This configuration is available only when you set **Auto** in **Day and Night Mode**. You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.
Illumination Option	Configure the illumination mode. You can select from **Infrared Mode**, **White Light Mode** and **Smart Illumination**.
Light Setting Mode	You can select form **Manual**, **Automatic** and **Close**. When select **Manual**, you can adjust the brightness according to the actual needs.
Defog Mode	The image quality is compromised in foggy or hazy environment, and defog can be used to improve image clarity. ● **Manual**: Configure function intensity and atmospheric light mode manually, and then the system adjusts image clarity accordingly. Atmospheric light mode can be adjusted automatically or manually. ● **Automatic**: The system adjusts image clarity according to the actual condition. ● **Close**: Defog function is disabled.

Step 4 Click **OK**

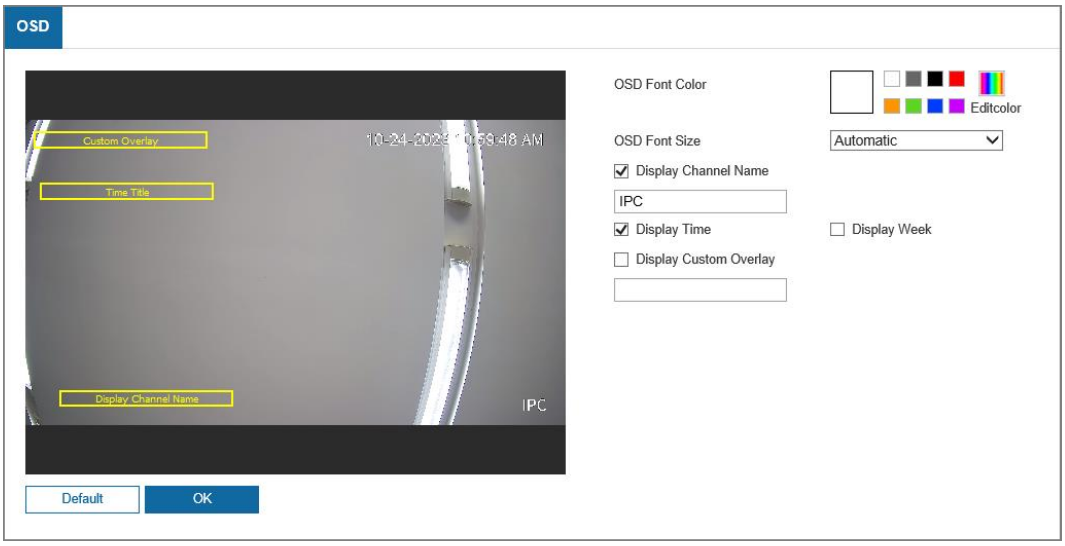
7.4.2 OSD

After enabling this function, the selected information will be displayed on the image.

Procedure

Step 1 Select **Settings** > **Image** > **OSD**.

Figure 7-43 OSD



OSD Font Color

OSD Font Size: Automatic

☑ Display Channel Name

IPC

☑ Display Time □ Display Week

□ Display Custom Overlay

Step 2 Select the color and size of OSD information as needed.

Step 3 Configure the display information, and then click **OK**.

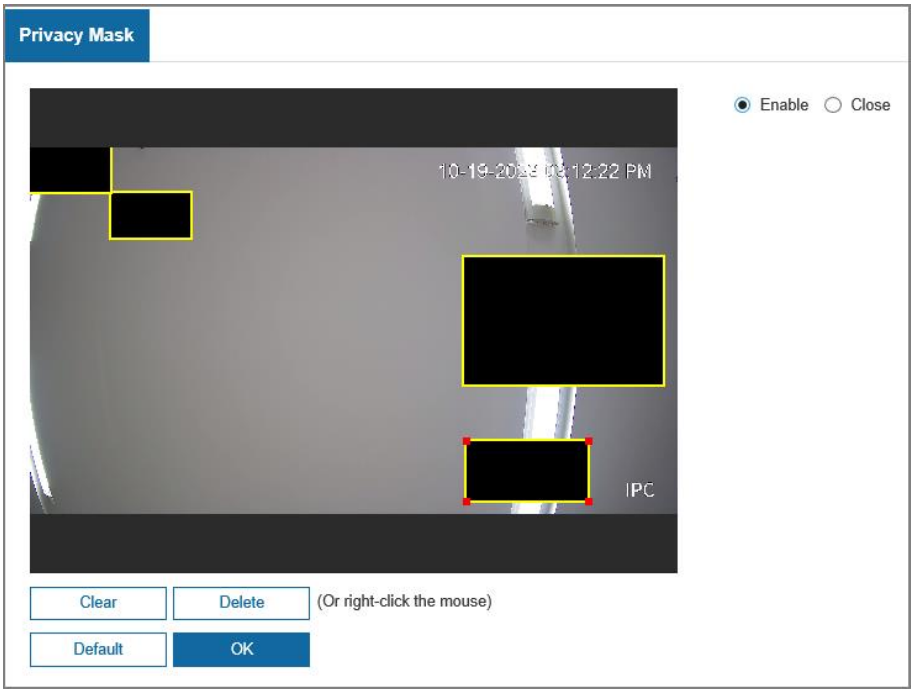
7.4.3 Privacy Mask

You can enable this function when you need to protect the privacy of some areas on the video image.

Procedure

Step 1 Select **Settings** > **Image** > **Privacy Mask**.

Figure 7-44 Privacy mask



Step 2 Select the **Enable**, and the image automatically displays 4 blocks.

Step 3 Drag the block to the area that you need to cover, and then adjust the size of the rectangle to protect the privacy.

Step 4 Click **OK**.

Related Operations

- Click **Clear** to clear all blocks.
- Click **Delete** to delete the selected block.

7.5 Event

7.5.1 Basic Event

7.5.1.1 Configuring Motion Detection

The system performs an alarm linkage when a moving object appears in the image and its moving speed reaches the configured sensitivity.

Procedure

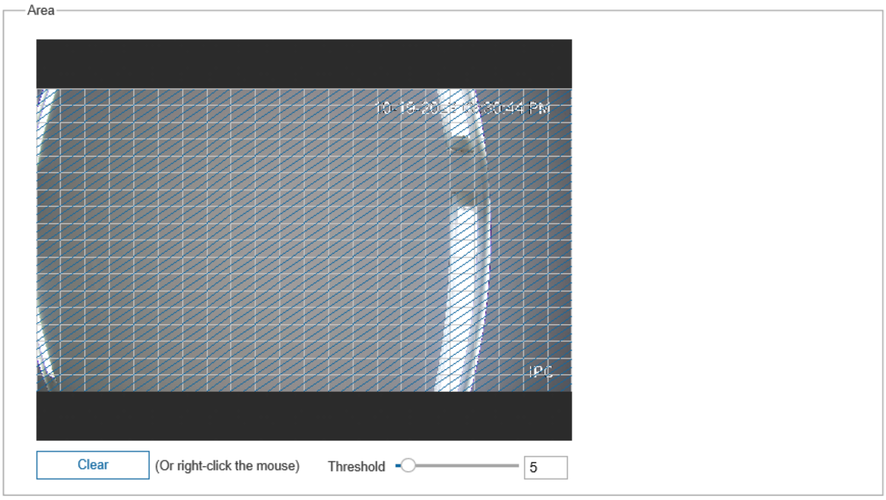
Step 1 Select **Settings** > **Event** > **Basic Event** > **Motion Detection**.

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

Step 3 Set the area for motion detection.

Click and drag the mouse to select the area. The detection region can be irregular and discontinuous.

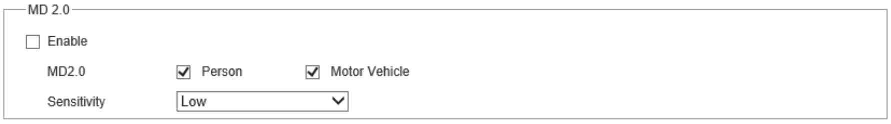
Figure 7-45 Detection area



Threshold 5

Step 4 (Optional) Select **Enable** in MD 2.0 area, and then configure the type and sensitivity. The device can detect person, motor vehicle or both as needed.

Figure 7-46 MD 2.0



□ Enable

MD2.0 ☑ Person ☑ Motor Vehicle

Sensitivity Low

Step 5 Set arming and disarming period.

Step 6 Configure the alarm linkage such as video recording, alarm output. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 7 Click **OK**.

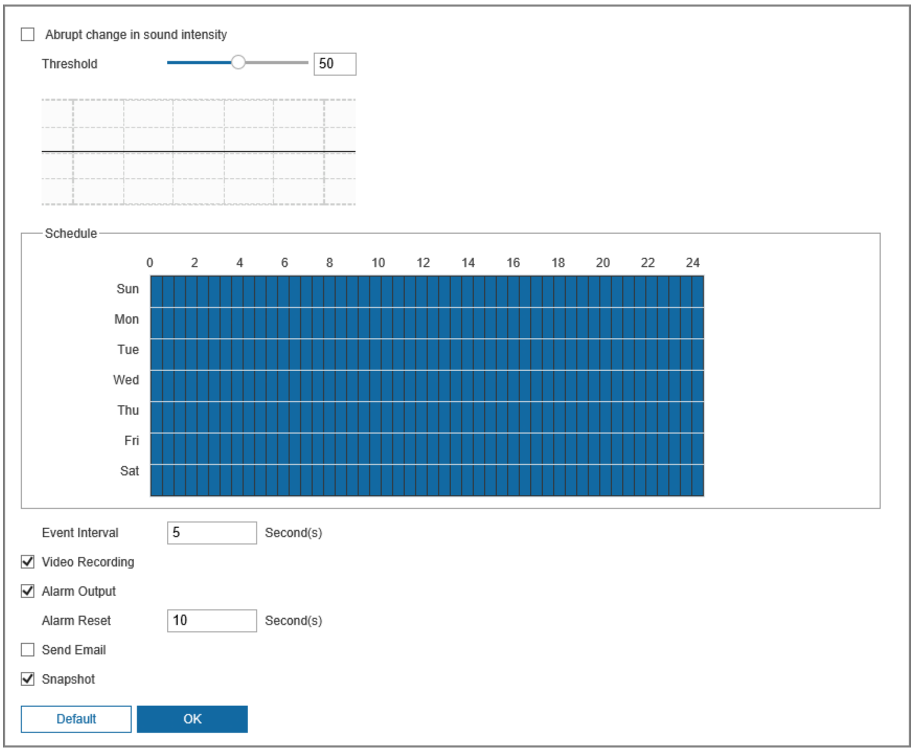
7.5.1.2 Configuring Audio Detection

The system performs alarm linkage when vague voice, tone change, or rapid change of sound intensity is detected.

Procedure

Step 1 Select **Settings** > **Event** > **Basic Event** > **Audio Detection**.

Figure 7-47 Audio detection



□ Abrupt change in sound intensity

Threshold 50

Event Interval 5 Second(s)

☑ Video Recording

☑ Alarm Output

Alarm Reset 10 Second(s)

□ Send Email

☑ Snapshot

Step 2 Select **Abrupt change in sound intensity** checkbox, and then set the threshold. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold.

It is easier to trigger the alarm with smaller threshold. Set a high threshold for noisy environment.

Step 3 Select the schedule and alarm linkage action. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 4 Click **OK**.

7.5.1.3 Configuring Video Tampering

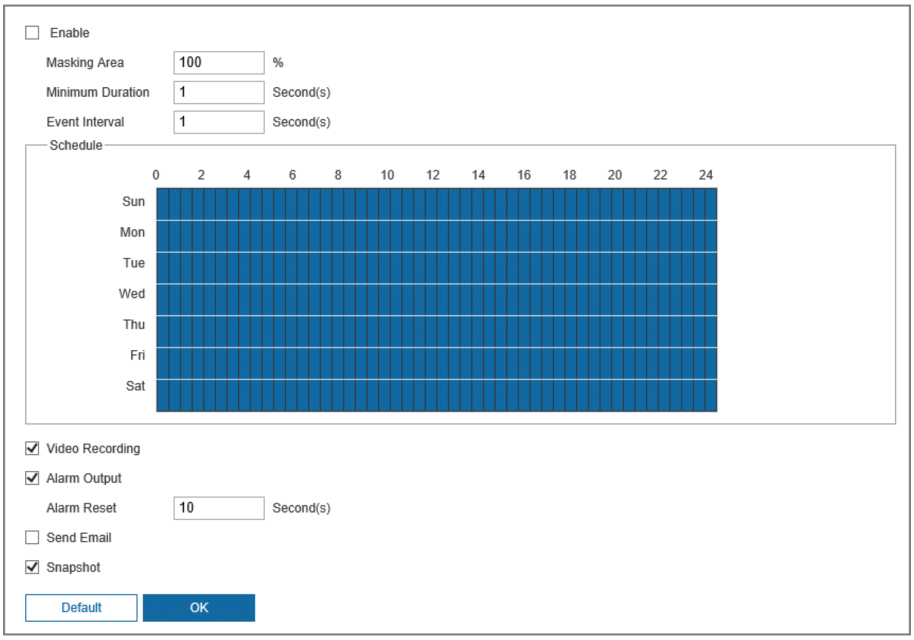
The system performs alarm linkage when the lens is covered or video output is mono-color screen caused by light and other reasons.

Procedure

Step 1 Select **Settings** > **Event** > **Basic Event** > **Video Tampering**.

Step 2 Select the **Enable** checkbox.

Figure 7-48 Video tampering



□ Enable

Masking Area 100 %

Minimum Duration 1 Second(s)

Event Interval 1 Second(s)

☑ Video Recording

☑ Alarm Output

Alarm Reset 10 Second(s)

□ Send Email

☑ Snapshot

Table 7-20 Description of video temper parameter

Parameter	Description
Masking Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm is triggered.
Minimum Duration	
Event Interval	Only record one alarm event during the interval.

Step 3 Set the schedule and alarm linkage action. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 4 Click **OK**.

7.5.1.4 Configuring Scene Changing

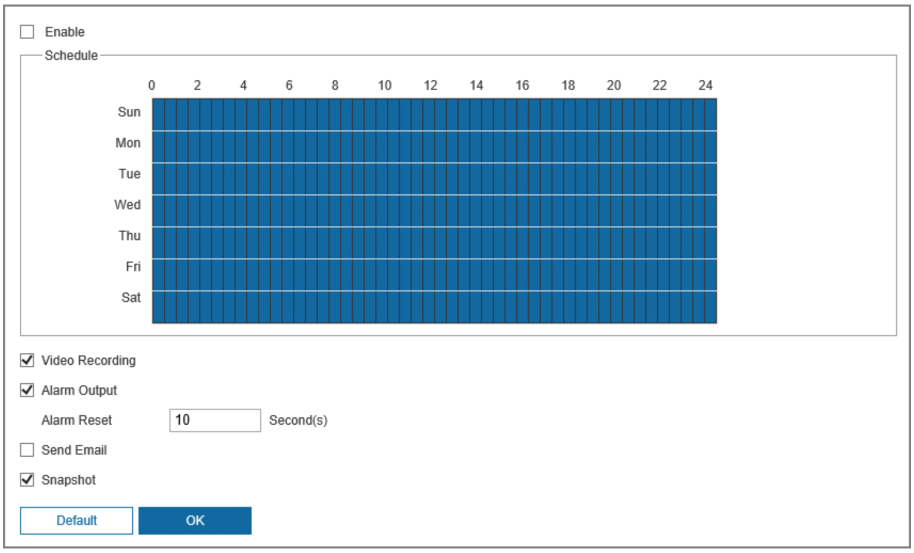
The system performs alarm linkage when the image switches from the current scene to another one.

Procedure

Step 1 Select **Settings** > **Event** > **Basic Event** > **Scene Changing**.

Step 2 Select **Enable** checkbox.

Figure 7-49 Scene changing


☐ Enable

Schedule

☑ Video Recording

☑ Alarm Output

Alarm Reset 10 Second(s)

☐ Send Email

☑ Snapshot

Step 3 Select the schedule and alarm linkage action. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 4 Click **OK**.

7.5.1.5 Configuring Alarm Linkage

Procedure

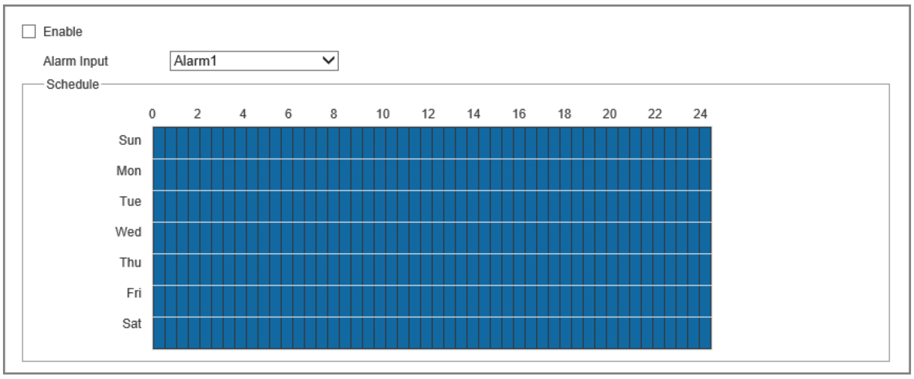
Step 1 Select **Settings** > **Event** > **Basic Event** > **Audio Linkage**.

Step 2 Select **Enable** checkbox to enable this function.

Step 3 Select the alarm import, and then configure the schedule.

Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered in the period in blue on the timeline.

Figure 7-50 Add the schedule


☐ Enable

Alarm Input Alarm1

Schedule

Step 4 Configure the **Event Interval** and **Sensor Type**.

- **Event Interval**: Only record one alarm event during the configured period.
- **Sensor Type**: You can select from **Normally Open** and **Normally Closed**.

Step 5 Configure the corresponding linkage.

- **Video Recording**: The system can link record channel when an alarm event occurs.
- **Alarm Output**: When an alarm is triggered, the system can automatically link with alarm-out device.
- **Send Email**: When an alarm is triggered, the system will automatically send an email to users.

- **Audio Linkage**: The system broadcasts alarm audio file when an alarm event occurs. For details, see "7.3.2.2 Configuring Alarm Audio".
- **Warning Light**: When an alarm is triggered, the system can automatically enable the warning light.
- **Snapshot**: After snapshot linkage is configured, the system can automatically take snapshots when an alarm is triggered.

Step 6 Click **OK**.

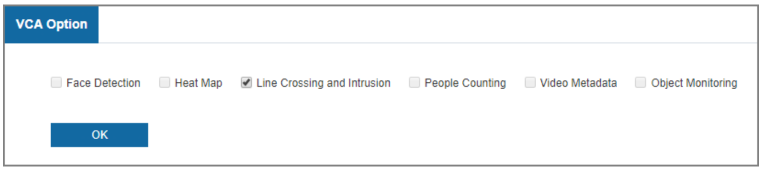
7.5.2 VCA Option

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Option**.

Figure 7-51 VCA option



VCA Option

□ Face Detection □ Heat Map ☑ Line Crossing and Intrusion □ People Counting □ Video Metadata □ Object Monitoring

OK

Step 3 Select related checkbox, and then click **OK**.

7.5.3 Line Crossing and Intrusion

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA** > **Line Crossing and Intrusion**.

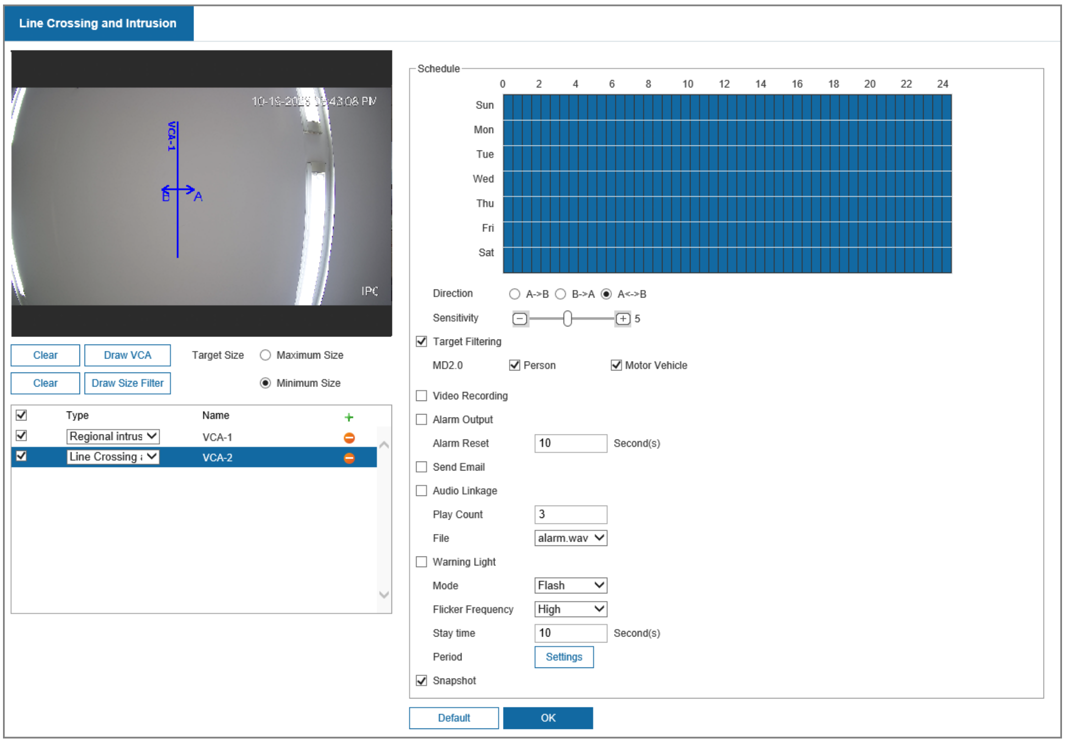
Step 3 Click + to add the rule.

Step 4 In the **Type** list, select **Line Crossing and Intrusion**, **Parking Detection**, **People Gathering** or **Loitering Detection** as needed.

This section uses **Line Crossing and Intrusion** as an example.

- **Line Crossing and Intrusion**: When the target crosses tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.
- **Parking detection**: When the target stays over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.
- **People Gathering**: When the people gathers or the crowd density is large, an alarm is triggered, and then the system performs configured alarm linkages.
- **Loitering Detection**: When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs configured alarm linkages.

Figure 7-52 Configuring line crossing and intrusion



Target Size ○ Maximum Size ● Minimum Size

☑	Type	Name
☑	Regional intrus	VCA-1
☑	Line Crossing	VCA-2

Direction ○ A->B ○ B->A ● A<->B

Sensitivity 5

☑ Target Filtering

MD2.0 ☑ Person ☑ Motor Vehicle

□ Video Recording

□ Alarm Output

Alarm Reset 10 Second(s)

□ Send Email

□ Audio Linkage

Play Count 3

File alarm.wav

□ Warning Light

Mode Flash

Flicker Frequency High

Stay time 10 Second(s)

Period

☑ Snapshot

Step 5 Click **Draw VCA** to draw rule line in the image. Right-click to finish drawing.

Step 6 (Optional) Click other icons to filter targets in the image.

- Select **Maximum Size** to draw the maximum size of the target; Select **Minimum Size** to draw the minimum size. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click **Clear** next to **Draw VCA** to delete the line configured; Click **Clear** next to **Draw Size Filter** to delete the rectangle configured.

Step 7 Set rule parameters.

Table 7-21 Description of parameters

Parameter	Description
Direction	Set the direction of rule detection. ● When setting tripwire, select **A->B**, **B->A**, or **A<->B**. ● When setting intrusion, select **Appear**, **Cross the region**, or **Within Area**.
Sensitivity	When the sensitivity is high, detection becomes easier, but the number of false detections increases. **Regional intrusion** does not support this function.
Target Filtering	Select **Target Filtering** to enable this function. ● When you select **Person** as the alarm target, an alarm will be triggered when the system detects that person trigger the rule. ● When you select **Motor Vehicle** as the alarm target, alarm will be triggered when the system detects that vehicle triggers the rule.

Step 8 Configure the alarm schedule and linkage. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 9 Click **OK**.

7.5.4 VCA Advanced

This function is available on select models.

7.5.4.1 People Counting

7.5.4.1.1 People Counting Configuration

Background Information

There are 3 types of people counting rules. this section used **People Counting** as an example.

- **People Counting**: The system counts the people entering and leaving the detection area. When the number of counted number of people who enter, leave, or stay in the area exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage.
- **Regional People Counting**: The system counts the people in the detection area and the duration that people stay in the area. When the number of counted number of people in the detection area or the stay duration exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage.
- **Queue Management**: The system counts the queue people in the detection area. When the queue people number exceeds the configured number or the queue time exceeds the configured time, an alarm will be triggered, and the system performs an alarm linkage.

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **People Counting**.

Step 3 In the **Type** list, select the type as needed.

Step 4 Click **Draw Detection Line** to adjust the detection line in the image.

Click **Draw VCA** to adjust the detection area.

Click **Clear** next to **Draw VCA** to delete the area configured; Click **Clear** next to **Draw Detection Line** to delete the line configured.

Step 5 Set rule parameters including number of people entered, exit and stay.

Step 6 Configure the alarm schedule and linkage. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 7 Click **OK**.

7.5.4.1.2 Viewing People Counting Report

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Report** > **People Counting Report**.

Step 3 Select the report type, start time, end time, and other parameters.

Step 4 Click **Search** to complete the report.

Click **Export** to export the statistical report.

7.5.4.2 Heat Map

7.5.4.2.1 Heat Map Configuration

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **Heat Map**.

Step 3 Select the **Enable** checkbox, and then the heat map function is enabled.

Step 4 Configure the schedule, and then click **OK**.

7.5.4.2.2 Viewing Heat Map Report

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Report** > **Heat Map Report**.

Step 3 Select the start time, end time and the threshold.

Step 4 Click **Search** to complete the report.

Click **Export** to export the statistical report.

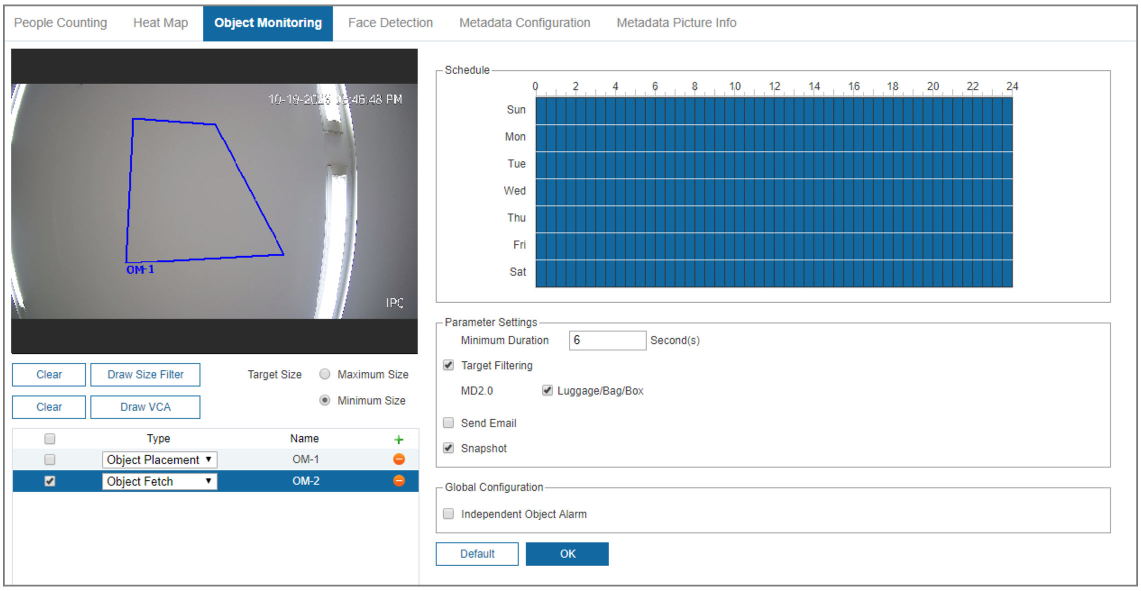
7.5.4.3 Object Monitoring

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **Object Monitoring**.

Figure 7-53 Object monitoring



Target Size ○ Maximum Size ● Minimum Size

□	Type	Name	+
□	Object Placement ▾	OM-1	−
☑	Object Fetch ▾	OM-2	−

Parameter Settings

Minimum Duration 6 Second(s)

☑ Target Filtering

MD2.0 ☑ Luggage/Bag/Box

□ Send Email

☑ Snapshot

Global Configuration

□ Independent Object Alarm

Step 3 In the **Type** list, select **Object Placement** or **Object Fetch** as needed.

- **Object Fetch**: When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs configured alarm linkages.
- **Object Placement**: When an object is placed in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.

Step 4 Click **Draw VCA** to draw the detection area.

Click **Draw Size Filter**, and then select **Minimum Size** to draw the minimum size of the target; click **Maximum Size** to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.

Click **Clear** next to **Draw VCA** to delete the area configured; Click **Clear** next to **Draw Size Filter** to delete the target size.

Step 5 Set the schedule and rule parameters including minimum duration, target filtering.

Step 6 Configure the alarm schedule and linkage. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 7 Click **OK**.

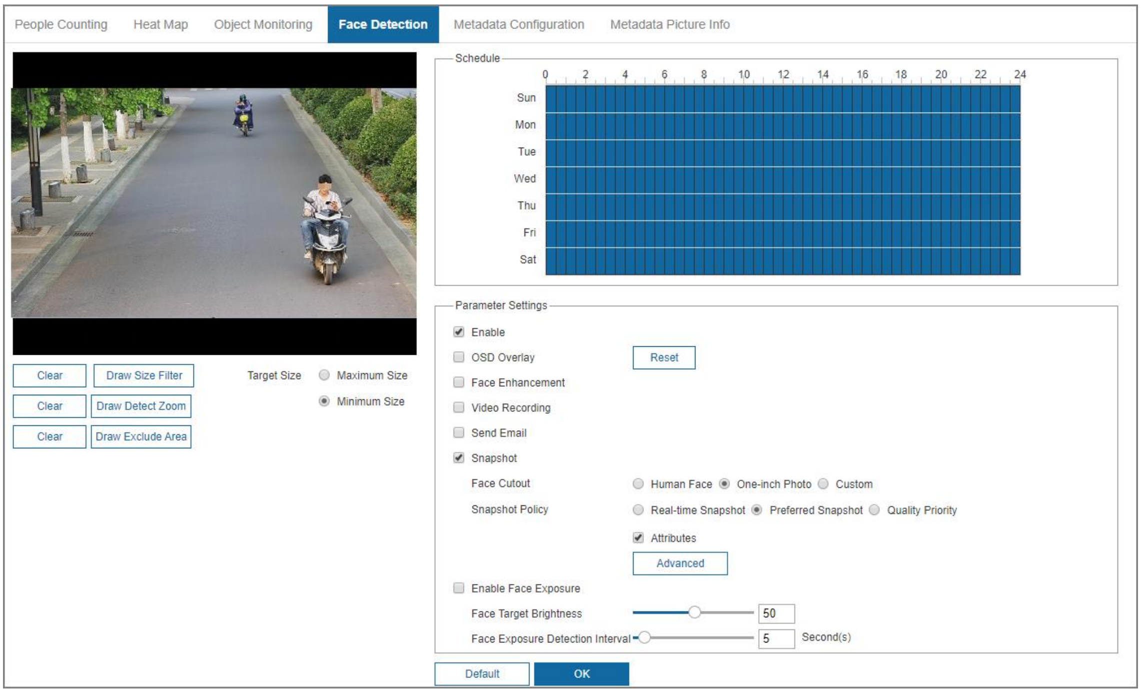
7.5.4.4 Face Detection

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **Face Detection**.

Figure 7-54 Face detection



Target Size ○ Maximum Size ● Minimum Size

Parameter Settings

☑ Enable

☐ OSD Overlay

☐ Face Enhancement

☐ Video Recording

☐ Send Email

☑ Snapshot

Face Cutout ○ Human Face ● One-inch Photo ○ Custom

Snapshot Policy ○ Real-time Snapshot ● Preferred Snapshot ○ Quality Priority

☑ Attributes

☐ Enable Face Exposure

Face Target Brightness 50

Face Exposure Detection Interval 5 Second(s)

Step 3 Select **Enable** checkbox.

Step 4 Click **Draw Size Filter**, and then select **Minimum Size** to draw the minimum size of the target; click **Maximum Size** to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.

Step 5 Click **Draw Detect Zoom** to draw the detection area.

Step 6 Click **Draw Exclude Area** to draw the exclude area.

Click **Clear** next to **Draw VCA**, **Draw Detect Zoom** and **Draw Exclude Area** to delete corresponding information.

Step 7 Set the schedule and rule parameters including OSD overlay and face enhancement.

Step 8 Configure the alarm schedule and linkage. For details, see "7.5.1.5 Configuring Alarm Linkage".

Step 9 Click **OK**.

7.5.4.5 Metadata

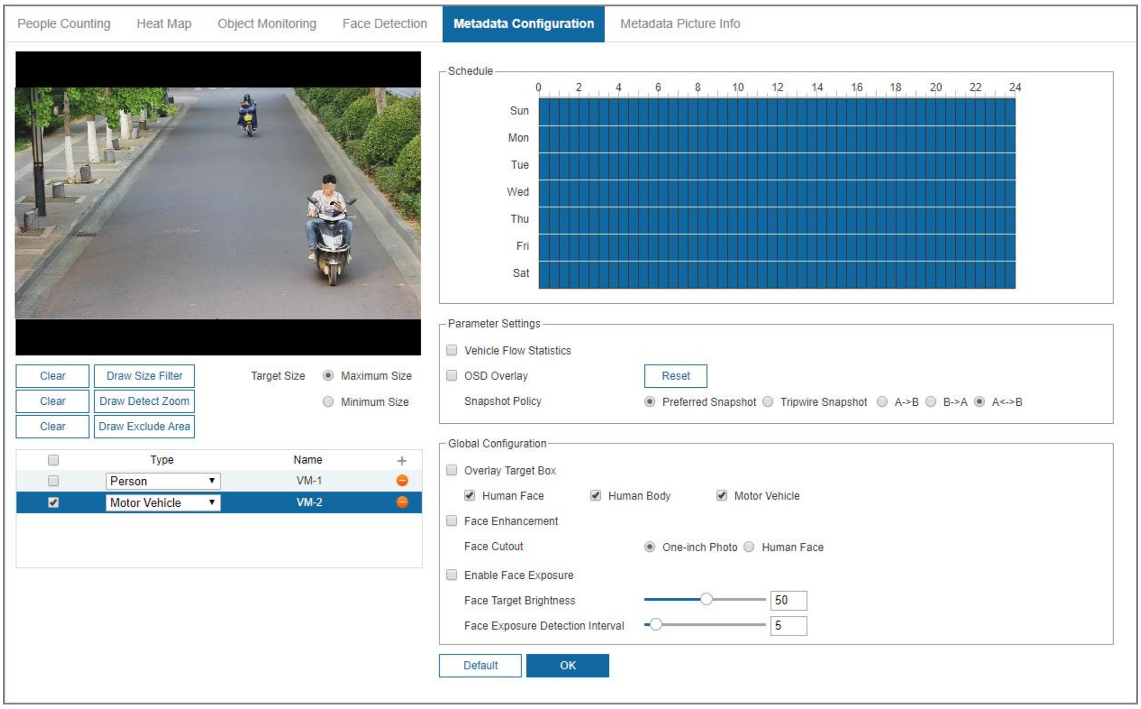
7.5.4.5.1 Metadata Configuration

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **Metadata Configuration**.

Figure 7-55 Metadata configuration



Target Size ● Maximum Size ○ Minimum Size

□	Type	Name	+
□	Person	VM-1	⊖
☑	Motor Vehicle	VM-2	⊖

Parameter Settings

□ Vehicle Flow Statistics

□ OSD Overlay

Snapshot Policy ● Preferred Snapshot ○ Tripwire Snapshot ○ A->B ○ B->A ● A<->B

Global Configuration

□ Overlay Target Box

☑ Human Face ☑ Human Body ☑ Motor Vehicle

□ Face Enhancement

Face Cutout ● One-inch Photo ○ Human Face

□ Enable Face Exposure

Face Target Brightness 50

Face Exposure Detection Interval 5

Step 3 Set the global configuration.

Table 7-22 Parameters of global configuration

Parameter	Description
Overlay Target Box	Overlay target box on the captured pictures to mark the target position.
Face Enhancement	Enable this function to preferably guarantee clear face with low stream.
Enable Face Exposure	Enable this function to make face clearer by adjusting brightness and detection interval.

Step 4 In the **Type** list, select **Person** or **Motor Vehicle** as needed.

Step 5 Filter targets in the image.

- Click **Draw Size Filter**, and then select **Minimum Size** to draw the minimum size of the target; click **Maximum Size** to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click **Draw Detect Zoom** to draw the detection area. Right-click to finish drawing.
- Click **Draw Exclude Area** to draw the exclude area. Right-click to finish drawing.

Step 6 Set the schedule and parameters.

Step 7 Click **OK**.

7.5.4.5.2 Viewing Metadata Report

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Report** > **Metadata Report**.

Step 3 Select the report type, start time, end time, and other parameters.

Step 4 Click **Search** to complete the report.

Click **Export** to export the statistical report.

7.5.4.6 Metadata Picture Info

Procedure

Step 1 Log in to the webpage of the device.

Step 2 Click **Settings** > **Event** > **VCA Advanced** > **Metadata Picture Info**.

Figure 7-56 Metadata picture info

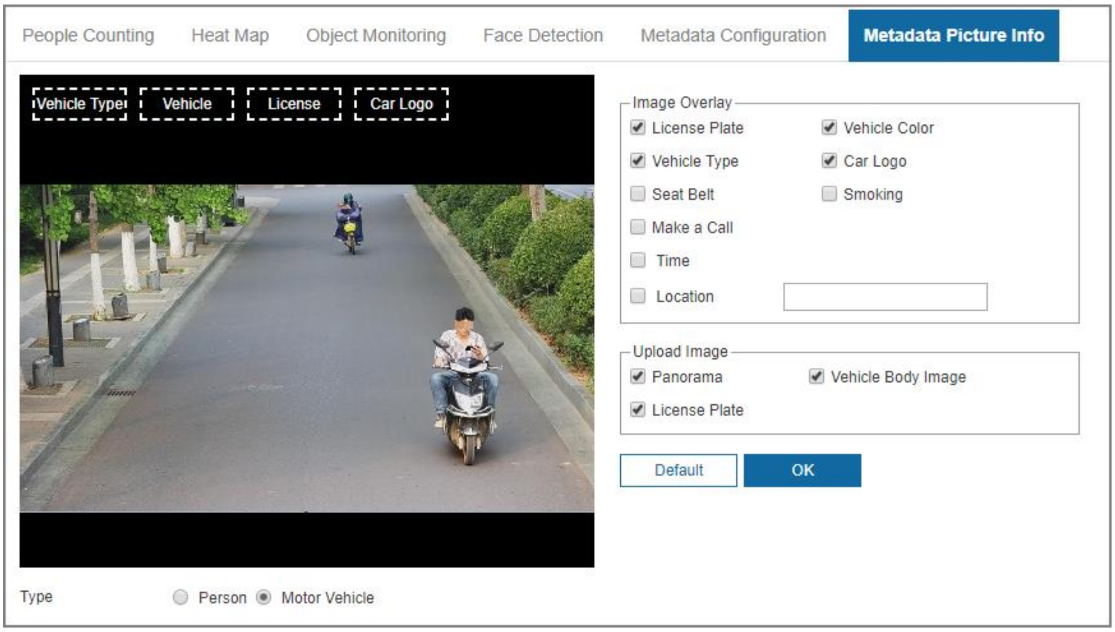


Image Overlay

☑ License Plate ☑ Vehicle Color

☑ Vehicle Type ☑ Car Logo

□ Seat Belt □ Smoking

□ Make a Call

□ Time

□ Location

Upload Image

☑ Panorama ☑ Vehicle Body Image

☑ License Plate

Type ○ Person ● Motor Vehicle

Step 3 Select the type from motor vehicle and person.

Step 4 Select the overlay information and upload image, and then click **OK**.

7.5.5 Exception

Abnormality includes SD card, network, unauthorized access, voltage detection, and security exception.

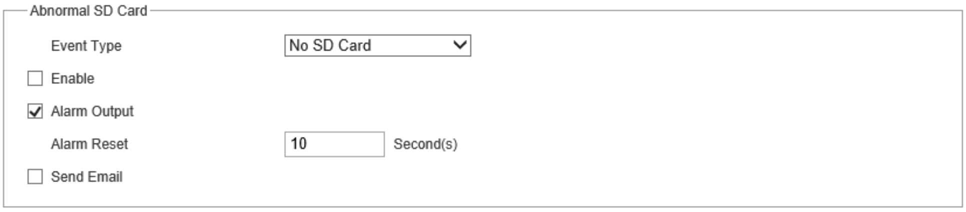
Select **Settings** > **Event** > **Exception**.

Abnormal SD card

In case of SD card exception, the system performs alarm linkage. The event types include **No SD Card**, **Insufficient SD Card Space**, and **SD Card Error**. Functions might vary with different models.

1. Select the event type, and then click **Enable** checkbox to enable this function.

Figure 7-57 Abnormal SD Card



Abnormal SD Card

Event Type: No SD Card

□ Enable

☑ Alarm Output

Alarm Reset: 10 Second(s)

□ Send Email

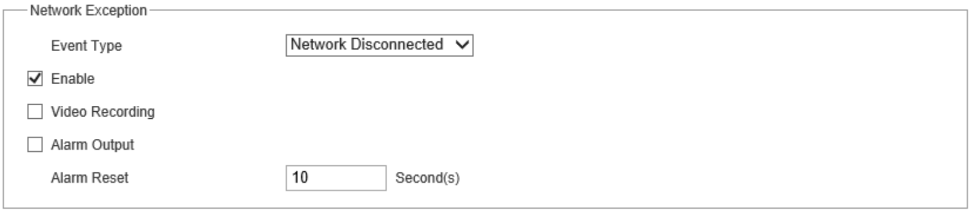
2. Set alarm linkage such as **Alarm Output** and **Send Email**. For details, see "7.5.1.5 Configuring Alarm Linkage".

Network Exception

In case of network abnormality, the system performs alarm linkage. The event types include **Network Disconnected** and **IP Conflict**.

1. Select the event type, and then click **Enable** checkbox to enable this function.

Figure 7-58 Network exception



Network Exception

Event Type: Network Disconnected

☑ Enable

□ Video Recording

□ Alarm Output

Alarm Reset: 10 Second(s)

2. Set alarm linkage such as **Alarm Output** and **Video Recording**. For details, see "7.5.1.5 Configuring Alarm Linkage".

Unauthorized Access

When the number of login errors exceeds the configured times, the system performs alarm linkage such as alarm output and send email.

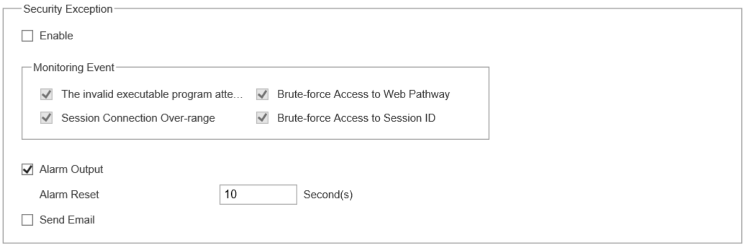
Voltage Detection

When the input voltage is higher than or lower than the rated value of the device, the system performs alarm linkage such as OSD, alarm output and send email.

Security Exception

When the system monitors the following events, an alarm can be triggered.

Figure 7-59 Security exception



Security Exception

□ Enable

Monitoring Event

☑ The invalid executable program atte... ☑ Brute-force Access to Web Pathway

☑ Session Connection Over-range ☑ Brute-force Access to Session ID

☑ Alarm Output

Alarm Reset 10 Second(s)

□ Send Email

7.6 Storage

7.6.1 Configuring Schedule

7.6.1.1 Video Recording

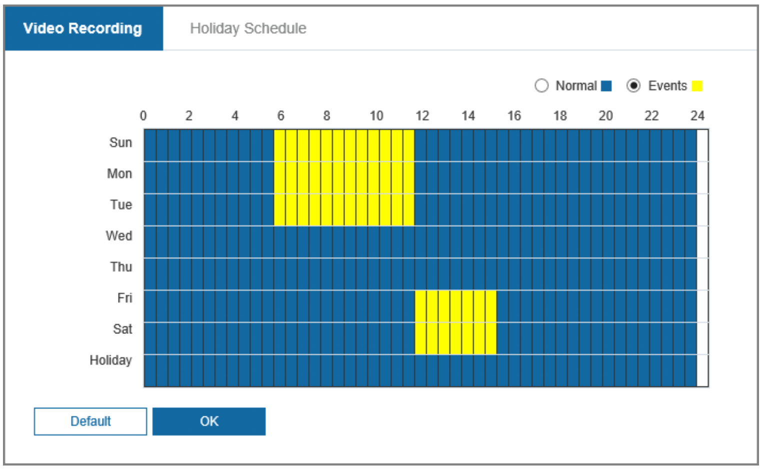
Procedure

Step 1 Select **Settings** > **Storage** > **Schedule** > **Video Recording**.

Step 2 Set record plan.

Blue represents normal record plan (such as timing recording); yellow represents motion record plan (such as recording triggered by events). Select a record type, such as **Normal**, and directly press and drag the left mouse button to set the period for normal record on the timeline.

Figure 7-60 Video recording



○ Normal ● Events

Step 3 Click **OK**.

7.6.1.2 Holiday Schedule

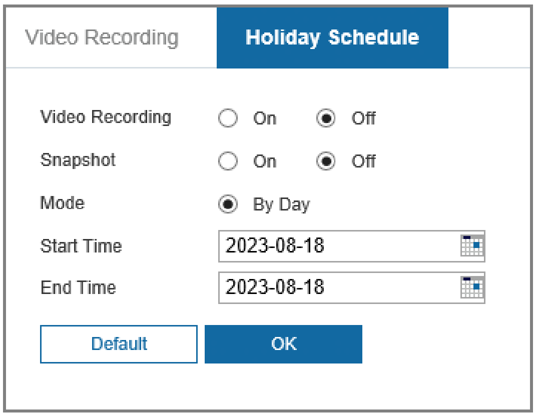
You can set certain days as holiday, and when the **Video Recording** or **Snapshot** is selected in the holiday schedule, the system takes snapshot or records video as holiday schedule defined.

Procedure

Step 1 Select **Settings** > **Storage** > **Schedule** > **Holiday Schedule**.

Step 2 Select **Video Recording** and **Snapshot** as needed, and then configure the time.

Figure 7-61 Holiday schedule



Video Recording ○ On ● Off

Snapshot ○ On ● Off

Mode ● By Day

Start Time 2023-08-18

End Time 2023-08-18

When holiday schedule setting is not the same as the general setting, holiday schedule setting is prior to the general setting. For example, with **Holiday Schedule** enabled, if the day is holiday, the system snapshots or records as holiday schedule setting; otherwise, the system snapshots or records as general setting.

Step 3 Click **OK**.

7.6.2 Configuring Storage

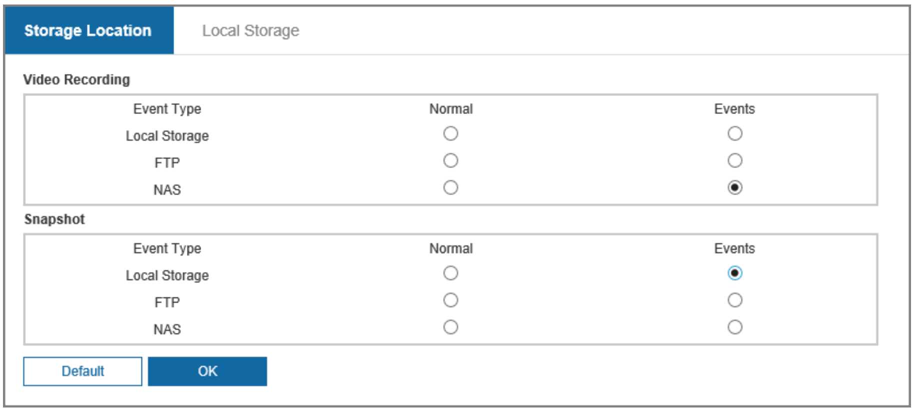
7.6.2.1 Storage Location

You can select different storage paths for the recorded videos and snapshots according to event type. You can select from SD card, FTP and NAS.

Procedure

Step 1 Select **Settings** > **Storage** > **Storage** > **Storage Location**.

Figure 7-62 Storage location



Video Recording

Event Type	Normal	Events
Local Storage	○	○
FTP	○	○
NAS	○	●

Snapshot

Event Type	Normal	Events
Local Storage	○	●
FTP	○	○
NAS	○	○

Step 2 Select the storage method that you need for the recorded videos and snapshots of different types.

Table 7-23 Description of storage location parameters

Parameter	Description
Local Storage	Save in the internal SD card. **Local Storage** is displayed only on models that support SD card.
FTP	Save in the FTP server.
NAS	Save in the NAS (network attached storage).

Step 3 Click **OK**.

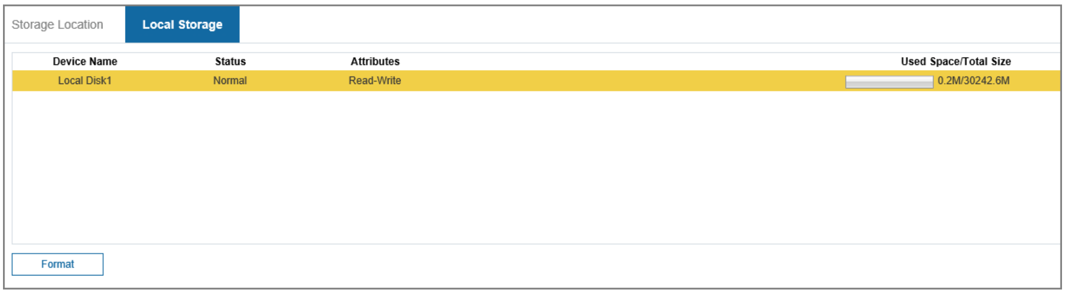
7.6.2.2 Local Storage

Display the information of the local SD card.

Procedure

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

Figure 7-63 Local storage



Device Name	Status	Attributes	Used Space/Total Size
Local Disk1	Normal	Read-Write	0.2M/30242.6M

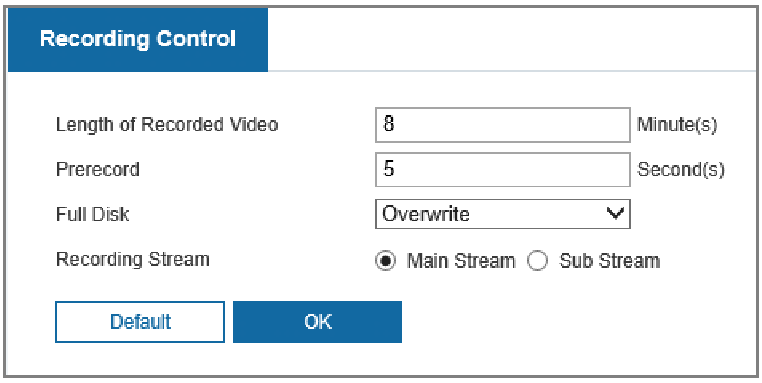
Step 2 (Optional) Click **Format** to clear the data of the SD card.

7.6.3 Configuring Recording Control

Procedure

Step 1 Select **Settings** > **Storage** > **Recording Control**.

Figure 7-64 Recording control



Length of Recorded Video 8 Minute(s)

Prerecord 5 Second(s)

Full Disk Overwrite

Recording Stream ● Main Stream ○ Sub Stream

Table 7-24 Description of recording control parameters

Parameter	Description
Length of Recorded Video	The time for packing each video file.
Prerecorded	The time to record the video in advance of a triggered alarm event. For example, if the pre-event record is set to be 5 s, the system saves the recorded video of 5 s before the alarm is triggered. 📖 When an alarm or motion detection links recording, and the recording is not enabled, the system saves the video data within the pre-event record time to the video file.
Full Disk	Recording strategy when the disk is full. ● **Stop**: Stop recording when the disk is full. ● **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
Recording Stream	Select record stream, including **Main Stream** and **Sub Stream**.

Step 2 Click **OK**.

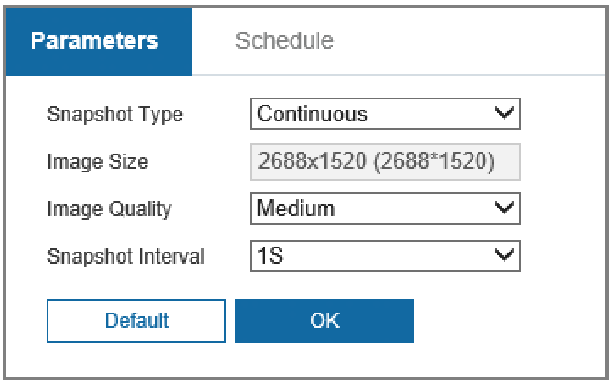
7.6.4 Snapshot

7.6.4.1 Configuring Snapshot Parameters

Procedure

Step 1 Select **Settings** > **Storage** > **Snapshot** > **Parameter**.

Figure 7-65 Configuring snapshot parameters



Snapshot Type: Continuous

Image Size: 2688x1520 (2688*1520)

Image Quality: Medium

Snapshot Interval: 1S

Table 7-25 Description of image stream parameters

Parameter	Description
Snapshot Type	You can select from **Continuous** and **Event**.
Image Size	The same resolution with main stream.
Image Quality	Configures the snapshot quality. There are six levels of Image quality, and the sixth is the best.

Parameter	Description
Snapshot Interval	Configures the snapshot frequency. Select **Custom**, and then you can configure snapshot frequency manually.

Step 2 Click **OK**.

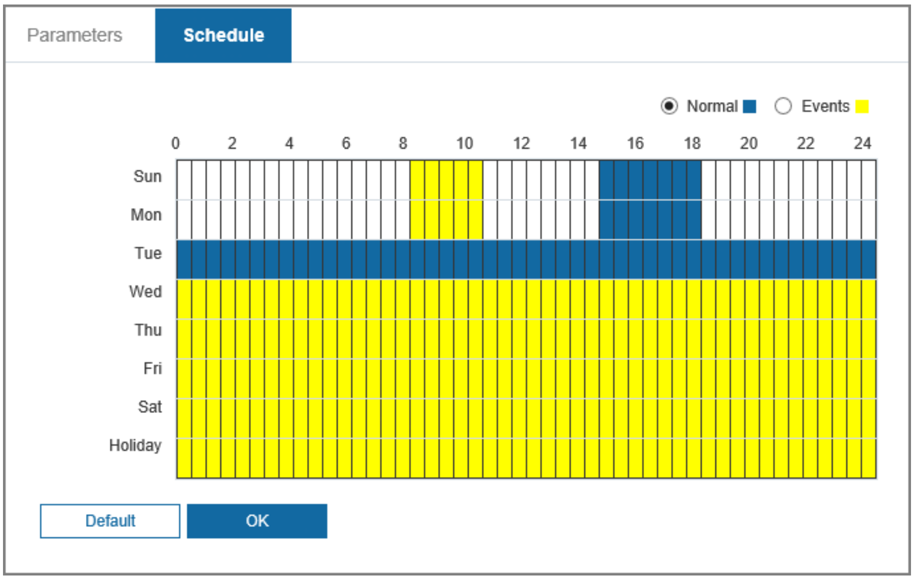
7.6.4.2 Configuring Snapshot Schedule

Procedure

Step 1 Select **Settings** > **Storage** > **Snapshot** > **Schedule**.

Step 2 Select snapshot type, and then set time period.

Figure 7-66 Configuring snapshot schedule



Select snapshot type, such as **Events**, and directly press and drag the left mouse button to set time period for normal snapshot on the timeline.

Step 3 Click **OK**.

Appendix 1 Cybersecurity Recommendations

Compulsory measures to ensure the basic device network security:

- Timely Update Firmware and Client Software
  - ◇ Keep the device (such as video recorder and IP camera) firmware up-to-date based on standard procedure in the tech-industry 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.
  - ◇ Download and use the latest version of client software.
- Use Complex Passwords with Combination of Characters, Numbers and SymbolsPlease refer to the following suggestions to set passwords:
  - ◇ The length should not be less than 8 characters;
  - ◇ Combine at least two types of characters in a password among 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 abcdefgh and 12345678;
  - ◇ Do not use overlapped characters, such as aaaaaaaa and 11111111.

Constructive suggestions on improving device network security:

- Change Passwords Regularly

  We recommend that you change passwords regularly to reduce the risk of being guessed or cracked.
- Configure and Update Password Reset Information in Time

  Password reset function is supported by the device. Please configure related information for password reset in time, including the end user's email address and password protection questions. Please update the information accordingly in time if it changes. Please do not use simple questions whose answers can be easily obtained when setting password protection questions.
- Enable Account Lock

  The account lock is enabled by default. We recommend you keep it on to ensure the account security. A number of failed login attempts will lead the corresponding account and the source IP address to be locked.
- Physical Protection

  Physical protection is recommended on the device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement strict access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware and unauthorized connection of removable device (for example, USB flash drive and serial port).
- Reset Default HTTP and Other Service Ports

  Changing the default HTTP and other service ports is recommended. We recommend you change them into any set of numbers between 1024–65535 to reduce the risk of exposing ports in use to outsiders.
- Enable HTTPS

  HTTPS is recommended to be enabled so that you can obtain the web service through a secure communication channel.

- Bind IP and MAC Address to Device
  To reduce the risk of ARP spoofing, we recommend you bind the IP and MAC address of the gateway to the device.
- Assign Accounts and Privileges Reasonably
  Based on business requirements and management requirements, prudently add user accounts and assign a minimum set of permissions to them.
- Disable Unnecessary Services and Apply Secure Modes
  If not needed, we recommend you turn off some services such as SNMP, SMTP, and UPnP to reduce risks.
  If necessary, we recommend using security 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.
- Audio and Video Encrypted Transmission
  To reduce the risk of losing data during transmission, encrypted transmission is recommended for very important and sensitive audio and video data.
  *Reminder: Encrypted transmission might decrease the transmission efficiency.
- Establish a Secure Network Environment
  The following actions are highly recommended to ensure device security and to reduce potential cyber risks:
  - ◇ Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
  - ◇ Partition and isolate the network according to the actual network needs. If there are no communication requirements between two sub networks, we recommend you adopt network isolation through VLAN, network GAP and other technologies.
  - ◇ 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.
- Security Auditing
  - ◇ Check online users: Check online users regularly to prevent unauthorized login.
  - ◇ Check device log: Obtain the IP addresses that were used to log in to the device and their key operations with help of the logs.
- Network Log
  The stored log is not saved in full due to the limited storage capacity. If you need to save the log for a long time, we recommend you enable the network log function to make sure that the critical logs are synchronized to the network log server for tracing.