

# Network Camera

User Manual

Revision 1.0



# Network Camera User Manual

## Preface




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.

## Privacy 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.

## Safety Instruction

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.

## 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 Safety Instruction and Warning

### 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

- 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.

# Network Camera User Manual

---

- 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

- 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.

## Contents

Preface .....	1	Username .....	11
Overview .....	1	User Group .....	12
Introduction .....	1	Online User .....	13
Network Connection .....	1	PW Reset .....	13
Functions .....	1	Network .....	13
Basic Functions .....	1	TCP/IP .....	13
Intelligent Functions .....	1	Port .....	14
Device Initialization .....	2	P2P .....	14
Login .....	3	DDNS .....	15
Logging in to the Webpage .....	3	Email .....	15
Resetting Password .....	3	PPPoE .....	16
Preview .....	4	UPnP .....	17
AI Preview .....	5	SNMP .....	17
Playback .....	6	Bonjour .....	18
Playback Page .....	6	Multicast .....	18
Playing Video or Picture .....	7	802.1x .....	19
Clipping Video .....	8	QoS .....	19
Downloading Video or Picture .....	8	RTMP .....	19
Downloading a Single File .....	8	FTP .....	20
Downloading Files in Batches .....	8	NAS .....	20
Setting .....	9	HTTPS .....	21
System .....	9	Firewall .....	22
System Setting .....	9	ONVIF .....	23
Basic Info .....	9	Remote Log Records .....	23
Time Settings .....	9	Video/Audio .....	23
Maintenance .....	10	Video .....	23
Upgrade and Maintenance .....	10	Audio .....	24
System Log .....	10	Configuring Audio .....	24
Security .....	10	Configuring Alarm Audio .....	25
User Management .....	11	Image .....	25
User Mana .....	11	Display Settings .....	25
		OSD .....	27
		Privacy Mask .....	28
		Event .....	28

# Network Camera User Manual

---

Basic Event .....	28
Configuring Motion Detection .....	28
Configuring Audio Detection .....	29
Configuring Video Tampering .....	29
Configuring Scene Changing .....	29
Configuring Alarm Linkage .....	30
VCA Option .....	30
Line Crossing and Intrusion .....	30
VCA Advanced .....	31
People Counting .....	31
People Counting Configuration .....	31
Viewing People Counting Report .....	32
Heat Map .....	32
Heat Map Configuration .....	32
Viewing Heat Map Report .....	32
Object Monitoring .....	32
Face Detection .....	33
Metadata .....	33
Metadata Configuration .....	33
Viewing Metadata Report .....	34
Metadata Picture Info .....	34
Exception .....	34
Storage .....	35
Configuring Schedule .....	35
Video Recording .....	35
Holiday Schedule .....	35
Configuring Storage .....	35
Storage Location .....	35
Local Storage .....	36
Configuring Recording Control .....	36
Snapshot .....	37
Configuring Snapshot Parameters .....	37
Configuring Snapshot Schedule .....	37
Cybersecurity Recommendations .....	38

## Overview

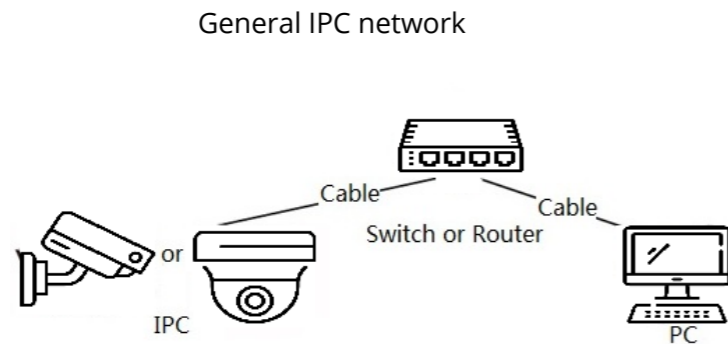
### Introduction

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.

### Network Connection

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



### Functions

Functions might vary with different devices.

#### 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.

### 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.

## Device Initialization

3. Click **OK**.

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 X Protal, NVR, or platform devices.

 NOTE

- 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.

### Process

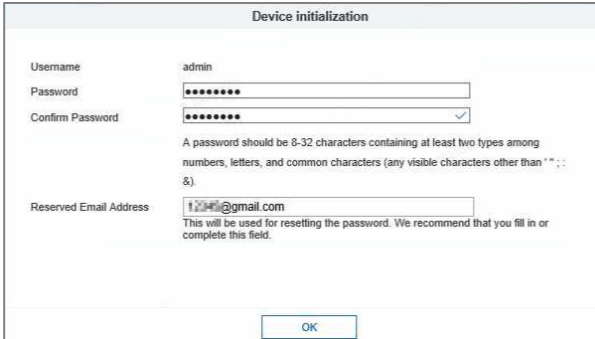
1. Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.

 NOTE

The IP is 192.168.1.101 by default.

2. Set the password for admin account.

Device initialization



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.

## Login

### Logging in to the Webpage

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



NOTE

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

#### Process

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.
2. Enter the username and password.  
The username is admin by default.



NOTE

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

#### Login

The screenshot shows a login form with the following elements: a 'Username:' field containing 'admin', a 'Password:' field, a 'Forgot password?' link, and a blue 'Login' button.

3. Click **Login**.

### 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.

#### Precondition

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

#### Process

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

#### Login

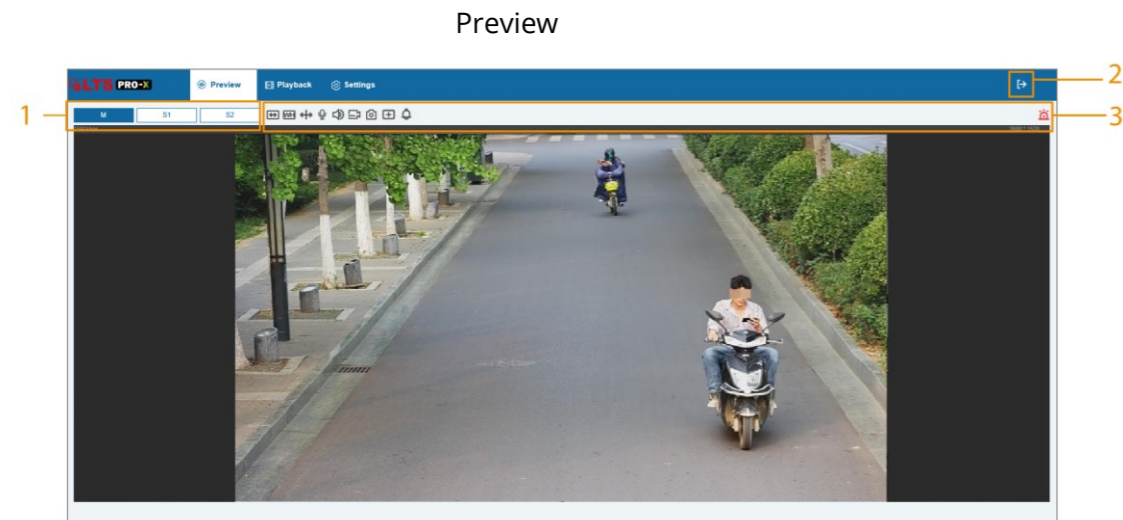
The screenshot shows a login form with the following elements: a 'Username:' field containing 'admin', a 'Password:' field, a 'Forgot password?' link, and a blue 'Login' button.

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



## Preview

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



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.
		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.

No.	Parameter/Icon	Description
		Snapshot. Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.
		Local zoom. You can zoom in or out the video image through two methods. <ul style="list-style-type: none"> <li>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.</li> <li>Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.</li> </ul>
		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.


## AI Preview

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

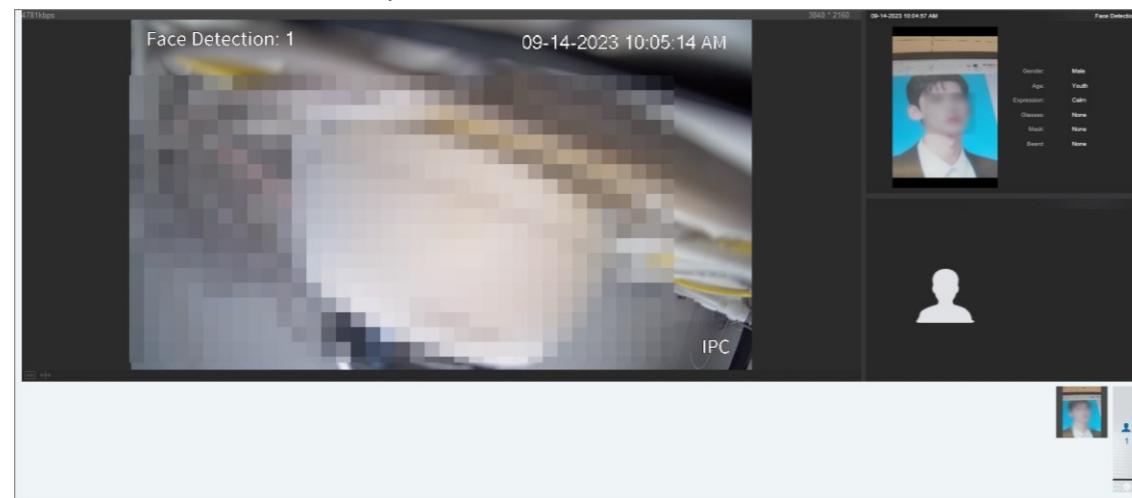
### Precondition

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

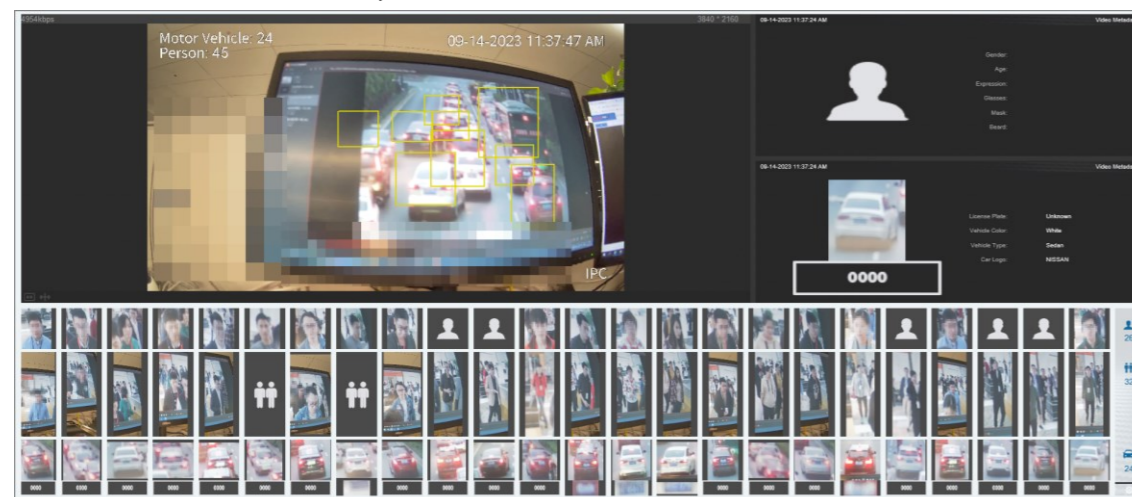
### Process

1. Log in to the webpage of the device.
2. Select **AI Preview** page.
3. In the lower-right page, click , and then select the mode in the **VCA Option** drop-down list.
4. Select the displayed attributes, and then click **Save**.

AI preview (face detection)



AI preview (video metadata)



## Playback

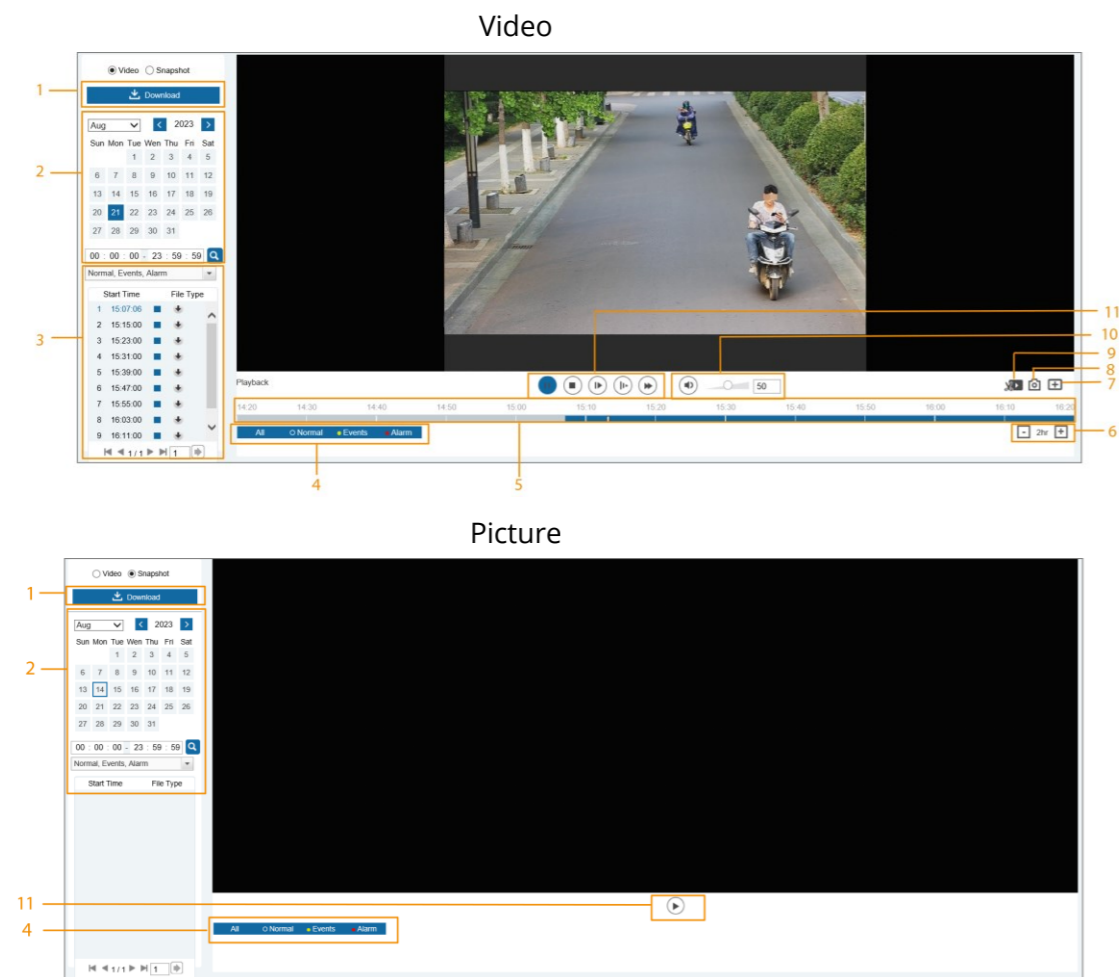
This section introduces playback related functions and operations, including videos and picture.

### NOTE

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

## Playback Page

Click the **Playback** tab.



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.
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. <ul style="list-style-type: none"> <li>• Click any point on the colored area, and the system will play back the recorded video from the selected moment.</li> <li>• Each record type has its own color, and you can see their relations in <b>Record Type</b> bar.</li> </ul>
6	Time format of progress bar	Includes 4 time formats: 30min, 1hr, 2hr and 24hr. Uses <b>24hr</b> 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. <ul style="list-style-type: none"> <li>• 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.</li> <li>• Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.</li> </ul>
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. <ul style="list-style-type: none"> <li>• : Mute mode.</li> <li>• : Vocal state. You can adjust the sound.</li> </ul>
11	Play control bar	Controls playback. <ul style="list-style-type: none"> <li>• : Play or pause recorded videos.</li> <li>• : Stop playing back recorded videos.</li> <li>• : Play the next frame.</li> <li>• : Slow down the playback.</li> <li>• : Speed up the playback.</li> </ul>

## Playing Video or Picture

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

### Process

1. Select **Video** or **Snapshot** as needed, and then configure the time.
2. Select the record type from the drop-down list.

The screenshot shows the 'Playback list' interface. At the top, there are radio buttons for 'Video' (selected) and 'Snapshot'. Below this is a 'Download' button. A calendar for August 2023 is displayed, with the 21st selected. Below the calendar is a time range selector set to '00 : 00 : 00 - 23 : 59 : 59'. A dropdown menu shows 'Normal, Events, Alarm'. Below these controls is a table of recorded events:

	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	■ ↓

At the bottom of the interface is a control bar with playback icons (stop, play, pause, next, previous) and a progress bar showing '1 / 2'.






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



## Clipping Video

### Process

1. Select **Video**, and then configure the time.
2. Select .
3. Click on the progress bar to select the start time of the target video, and then click .
4. Click again on the progress bar to select the end time of the target video, and then click .
5. Click  to download the video.  
The system will prompt that it cannot play and download at the same time.
6. Click **OK**.  
The playback stops and the clipped file is saved to the default storage path (C:\Users\admin\WebDownload\PlaybackRecord).

## 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.

### NOTE

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

## Downloading a Single File

### Process

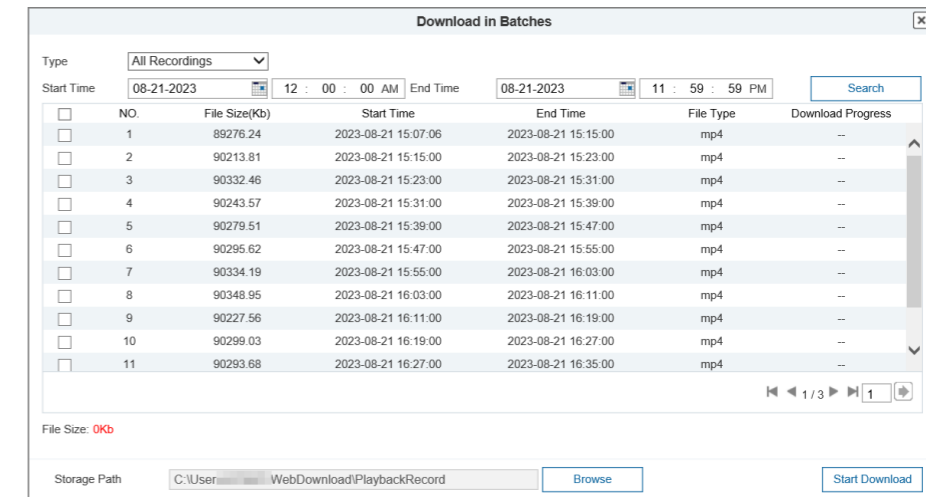
1. Select **Video**, and then configure the time.
2. Select the record type from the drop-down list.
3. Click  next to the file to be downloaded.  
The system starts to download the file to the default path (C:\Users\admin\WebDownload\PlaybackRecord).

## Downloading Files in Batches

### Process

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

Download in batches



3. Select the files to be downloaded, and then set the storage path.
4. Click **Start Download**.  
The system starts to download the file to the configured path.

## Setting

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

## System

### System Setting

#### Basic Info

#### Process

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

2. (Optional) Set a unique device name. The device name is model name by default.
3. Check the device information such as serial number, firmware version and ONVIF version. Click **OK**.

#### Time Settings

#### Process

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

2. Configure the parameters.

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 <b>Synchronize PC</b> , 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 <b>12-Hour</b> or <b>24-Hour</b> .
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.

3. Click **OK**.

# Network Camera User Manual

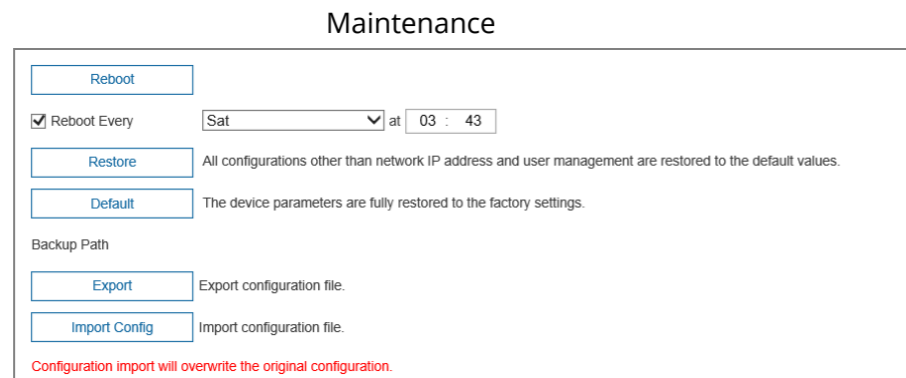
## Maintenance

### Upgrade and Maintenance

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

### Maintenance

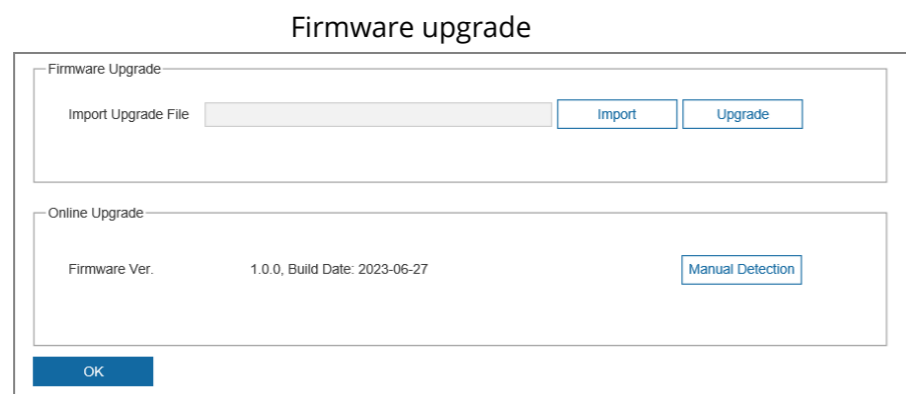
1. Log in to the webpage of the device.
2. Select **Settings > System > Maintenance > Upgrade and Maintenance**.



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.



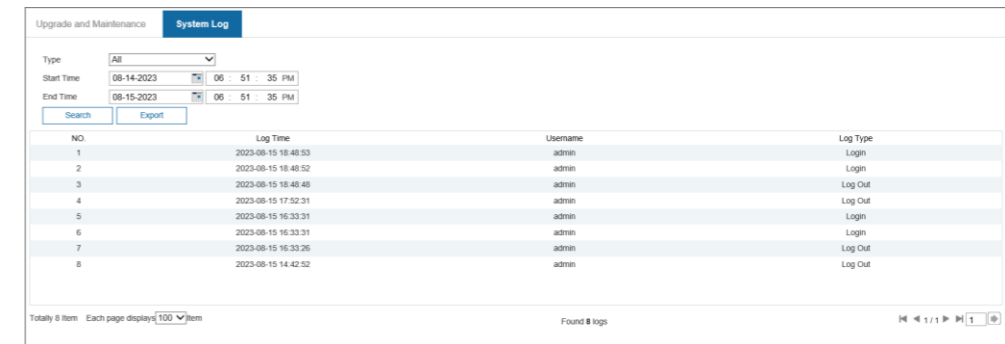
## System Log

You can view and back up logs.

### Process

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

### System log



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 shutdown, 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.
3. Click **Search**. The system displays the search results.
4. (Optional) Click **Backup**, and then you can back up all searched logs to local computer.

## Security

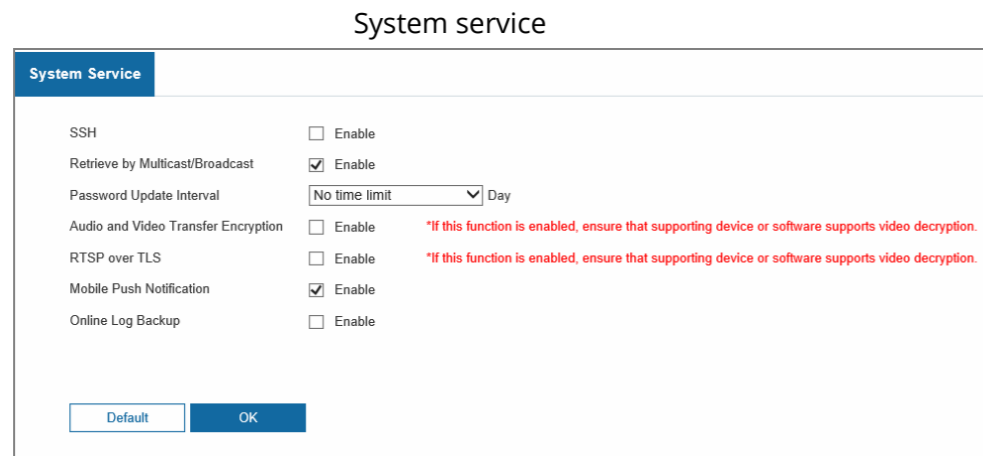
Configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log in to the webpage. This is to enhance network and data security.

### Process

1. Log in to the webpage of the device.

# Network Camera User Manual

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



3. Enable the system service as needed.

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. <b>NOTE</b> 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. <b>NOTE</b> <ul style="list-style-type: none"> <li>Make sure that the matched devices or software support video decryption function.</li> <li>We recommend you to enable the function. Otherwise, there might be risk of data leakage.</li> </ul>
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.

Function	Description
Online Log Backup	Enable this function to back up the online log.

4. Click **OK.**

## User Management

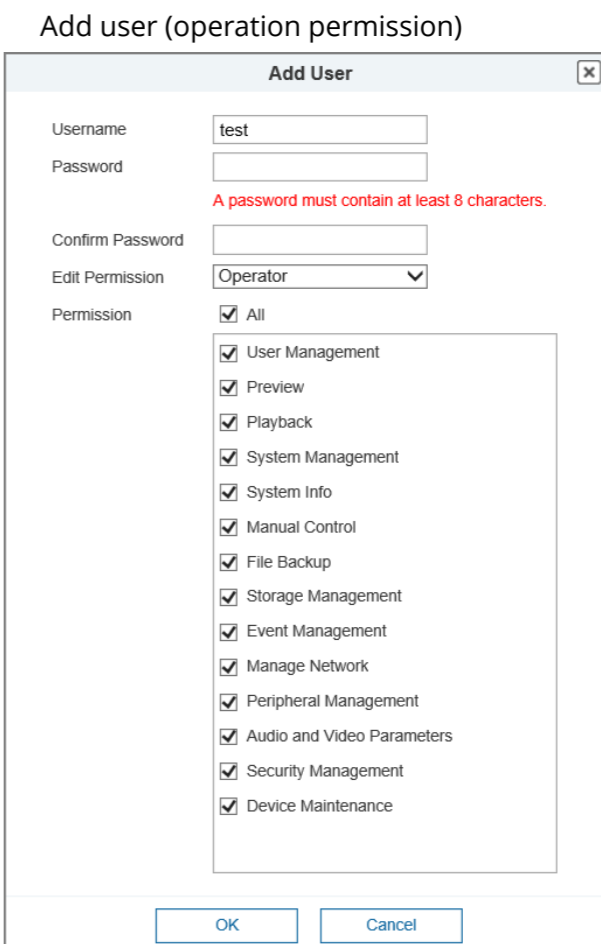
### User Mana.

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

### Username

### Process

1. Log in to the webpage of the device.
2. Select **Settings > System > User Management > User Mana. > Username.**
3. Click **Add User**, and then configure the parameters.





# Network Camera User Manual


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.
Confirm 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 ' " ; : &).
Edit Permission	You can select from <b>Operator</b> or <b>User</b> . Different rules have different permissions.
Permission	Select the permissions for the user.

4. Click **OK**.

## Related Operations

- Edit user information

Click  to change password and permissions.




NOTE

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.



NOTE

Users and user groups cannot be recovered after deletion.

## 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.

## Process

- Log in to the webpage of the device.

- Select **Settings > System > User Management > User Mana. > Edit Permission**.
- Click **Add Group**.
- Enter the group name, and then select the permissions.

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

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.

# Network Camera User Manual

Permission	Function
Security Management	HTTPS settings, RTSP over TLS settings and more.
Device Maintenance	Automatic maintenance settings and more.

NOTE

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

- 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.

## Online User

Check the information of user which is currently online.

Online user

NO.	Username	User Group	Address	User Login Time
1	Operator	Operator	192.168.1.1	08-16-2023 08:54:37 AM

## PW Reset

Reset the reserved email address for password reset as needed.

Figure 7-10 PW reset

PW Reset

Reserved Email Address:

## Network

This section introduces network configuration.

## TCP/IP

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

### Precondition

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.

### Process

- Select **Settings > Network > TCP/IP > TCP/IP**.

TCP/IP


TCP/IP	Port
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Backup DNS Server	<input type="text" value="8.8.4.4"/>
<input type="button" value="Default"/> <input type="button" value="OK"/>	

- Configure TCP/IP parameters.

Table 7-5 Description of TCP/IP parameters

Parameter	Description
IP Version	Select <b>IPv4</b> or <b>IPv6</b> .
Mode	The mode that the camera gets IP: <ul style="list-style-type: none"> <li><b>Static</b>: Configure <b>IP Address</b>, <b>Subnet Mask</b>, and <b>Default Gateway</b> manually, and then click <b>Save</b>, the login page with the configured IP address is displayed.</li> <li><b>DHCP</b>: When there is DHCP server in the network, select <b>DHCP</b>, and the camera acquires IP address automatically.</li> </ul>
MAC Address	Displays host MAC address.
IP Version	Select <b>IPv4</b> or <b>IPv6</b> .
Address	When you select <b>Static</b> in <b>Mode</b> , enter the IP address and subnet mask that you need.
Subnet Mask	

# Network Camera User Manual

Parameter	Description
Default Gateway	<p> NOTE</p> <ul style="list-style-type: none"> <li>IPv6 does not have subnet mask.</li> <li>The default gateway must be on the same network segment with the IP address.</li> </ul>
Preferred DNS Server	IP address of the DNS server.
Backup DNS Server	Alternate IP address of the DNS server.

3. Click **OK**.

## Port

### Process

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

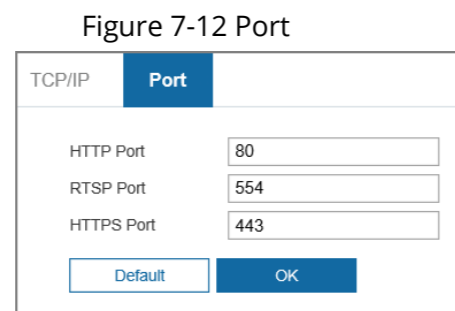


Figure 7-12 Port

2. Configure port parameters.

 NOTE

- 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.

Description of port parameters

Parameter	Description
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.

Parameter	Description
RTSP Port	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ul> <p>URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&amp;subtype=0</p> <p>Among that:</p> <ul style="list-style-type: none"> <li>Username: The username, such as admin.</li> <li>Password: The password, such as admin.</li> <li>IP: The device IP, such as 192.168.1.112.</li> <li>Port: Leave it if the value is 554 by default.</li> <li>Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2.</li> <li>Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1).</li> </ul> <p>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&amp;subtype=1</p> <p>If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&amp;subtype=0</p>
HTTPS Port	HTTPS communication port. It is 443 by default.

3. Click **Apply**.

## P2P

P2P (peer-to-peer) technology enables users to manage devices easily without requiring DDNS,

# Network Camera User Manual

port mapping or transit server.

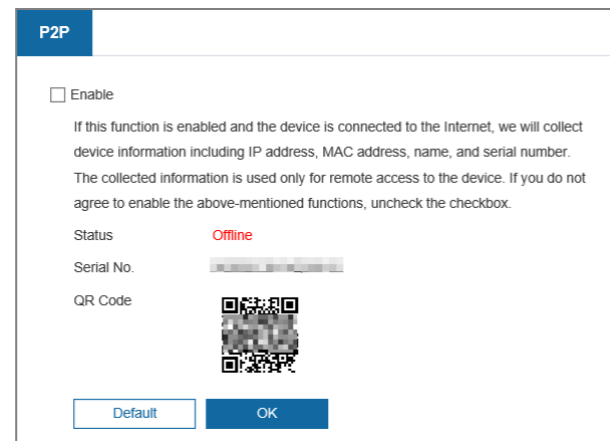
## Background Information

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

## Process

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

Figure 7-13 P2P



- 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.

2. Log in to mobile phone client, and then tap **Device management**.
3. Tap **+** at the upper-right corner.
4. Scan the QR code on the **P2P** page.
5. Follow the instructions to finish the settings.

## 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.

## Precondition

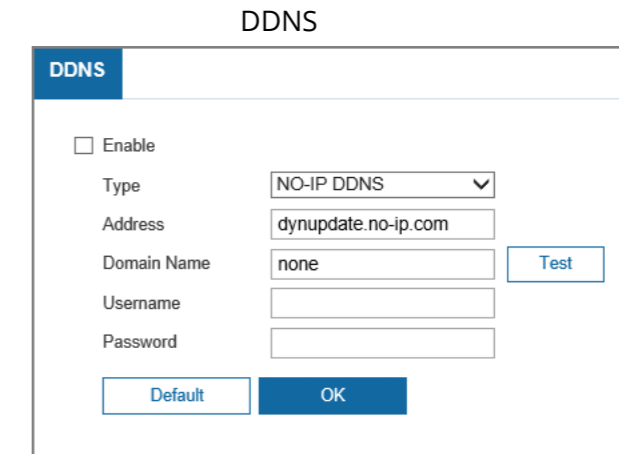
Check the type of DNS server supported by the camera.

## Process

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

## NOTE

- 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.



2. Select the **Enable** checkbox to enable the function.
3. Configure DDNS parameters.

Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below:
Address	<ul style="list-style-type: none"><li>• CN99 DDNS: www.3322.org.</li><li>• NO-IP DDNS: dynupdate.no-ip.com.</li><li>• Dvrlists: ns1.dvrlists.com.</li></ul>
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	

4. 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.

## Email

Configure email parameter and enable email linkage. The system sends email to the defined

# Network Camera User Manual

address when the corresponding alarm is triggered.

## Process

1. Select **Settings > Network > Email**.

2. Configure email parameters.

Description of email parameters

Parameter	Description
SMTP Server	SMTP server address
Port	The port number of the SMTP server.
Username	The account and password of SMTP server. Click <b>Test</b> to check whether the email address is available or not.
Password	
Sender	Sender's email address.
Encryption Mode	Select from <b>None</b> , <b>SSL</b> and <b>TLS</b> . NOTE For details, see below table.

Parameter	Description
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click <b>+</b> to select title type, including <b>Device Name</b> , <b>Device ID</b> , and <b>Event Type</b> , and you can set maximum 2 titles.
Attachment Supported	Select the checkbox to support attachment in the email.
Recipient	<ul style="list-style-type: none"> <li>Receiver's email address. Supports 3 addresses at most.</li> <li>After entering the receiver's email address, the <b>Test</b> button is displayed. Click <b>Test</b> to test whether the emails can be sent and received successfully.</li> </ul>

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	

3. Click **OK**.

## 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.

### Precondition

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

### Process

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

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

# Network Camera User Manual

## NOTE

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

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.

## 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.

### Precondition

- 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.

### Process

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

Service Name	Protocol	Internal Port	External Port	Status	Modify
HTTP	WebService.TCP	80	8080	Mapping failed	
RTSP	RTSPService.TCP	554	554	Mapping failed	
HTTPS	HTTPService.TCP	443	44333	Mapping failed	

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.

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.

## 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.

### Precondition

- 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.

### Process

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

SNMP (1)

Version:  v1,  v2,  v3 (Recommended)

SNMP Port: 161

Read Community:

Write Community:

Trap Address:

Trap Port: 162

Buttons: Default, OK

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.

Buttons: Default, OK

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.



NOTE

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

- 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.

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. NOTE 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.
Read-only Username	Set the read-only username accessing device, and it is <b>public</b> by default. NOTE You can enter number, letter, and underline to form the name.
Authentication Method	You can select from <b>MD5</b> and <b>SHA</b> . The default type is <b>MD5</b> .
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 <b>public</b> by default. NOTE You can enter number, letter, and underline to form the name.

- Click **OK**.

## Result

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

- Run MIB Builder and MG-SOFT MIB Browser.
- Compile the two MIB files with MIB Builder.
- Load the generated modules with MG-SOFT MIB Browser.
- Enter the IP address of the device you need to manage in the MG-SOFT MIB Browser, and then select version to search.
- 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.



NOTE

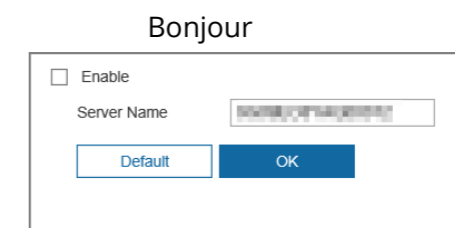
Use computer with Windows and disable SNMP Trap service. The MG-SOFT MIB Browser will display prompt when alarm is triggered.

## 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.

## Process

- Select **Settings > Network > Advanced > Bonjour**.



- Select the **Enable** checkbox, and then configure server name.
- Click **OK**.

## Result

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

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

## Multicast

When multiple users are viewing the device video image simultaneously through network, it might

# Network Camera User Manual

fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–239.255.255.255) for the camera and adopt the multicast protocol.

## Process

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

Multicast

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

Description of multicast parameters

Parameter	Description
Multicast Address	The multicast IP address of <b>Main Stream/Sub Stream</b> 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: <b>Main Stream:</b> 40000; <b>Sub Stream1:</b> 40016; <b>Sub Stream2:</b> 40032, and all the range is 1025–65500.

3. Click **OK**.

## 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

## Process

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

802.1x

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

Description of 802.1x parameters

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

3. Click **OK**.

## 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.

## Process

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

QoS

2. Configure QoS parameters.

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.

3. Click **OK**.

## RTMP

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



# Network Camera User Manual

view.

## NOTE

- 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.

## Process

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

2. Select the **Enable** checkbox.



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

3. Configure RTMP parameters.

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	<ul style="list-style-type: none"> <li>• <b>Non-custom:</b> Enter the server IP and domain name.</li> <li>• <b>Custom:</b> Enter the path allocated by the server.</li> </ul>
Address	When selecting <b>Non-custom</b> , you need to enter server IP address and port.
Port	<ul style="list-style-type: none"> <li>• <b>IP address:</b> Support IPv4 or domain name.</li> <li>• <b>Port:</b> Keep the default value.</li> </ul>
Custom Address	When selecting <b>Custom</b> , you need to enter the path allocated by the server.

4. Click **OK**.

## 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.

## Precondition

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

## Process

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

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.

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

## NAS

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

## Precondition

This function is available only when the video recording type and snapshot type is **NAS**. For details,

# Network Camera User Manual

see "Storage Location".

## Process

1. Select **Settings > Network > Advanced > NAS**.
2. Select the **Enable** checkbox.
3. Configure NAS parameters.

NAS

Description of NAS parameters

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

4. Click **OK**.

## 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.

## Process

1. Select the **Settings > Network > Advanced > HTTPS**.
2. Select **Enable HTTPS** checkbox.

HTTPS

3. Create a certificate or upload an authenticated certificate.

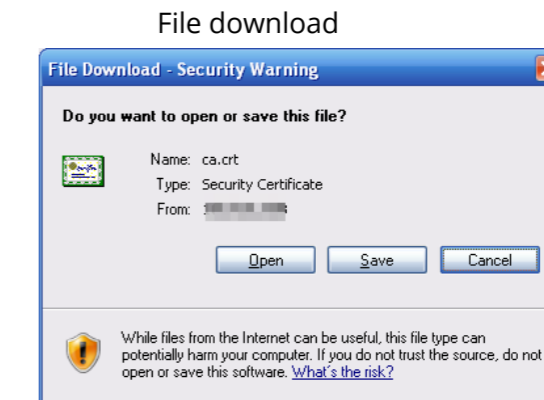
- For creating a certificate, click **Create**.
- For uploading the authenticated certificate, click **Browse** to select the certificate and certificate key, click **Upload** to upload them, and then skip to [Step6](#).

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

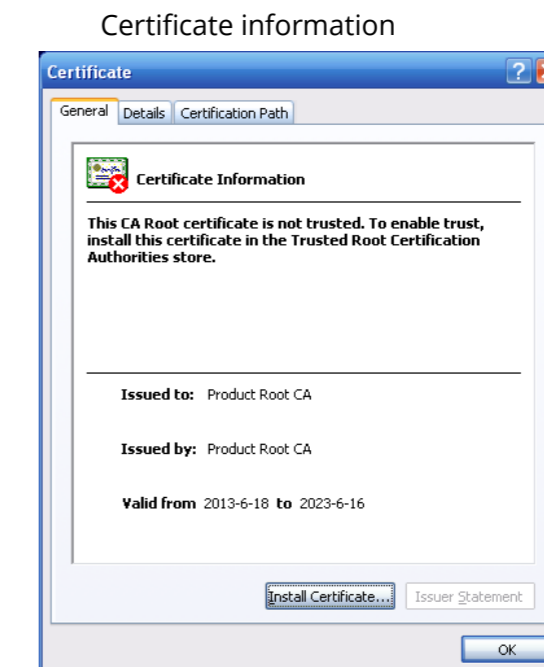
**NOTE**

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

5. Click **Install**.
6. Click **Download** to download root certificate.
7. Click **Download Root Certificate**.



8. Click **Open**.



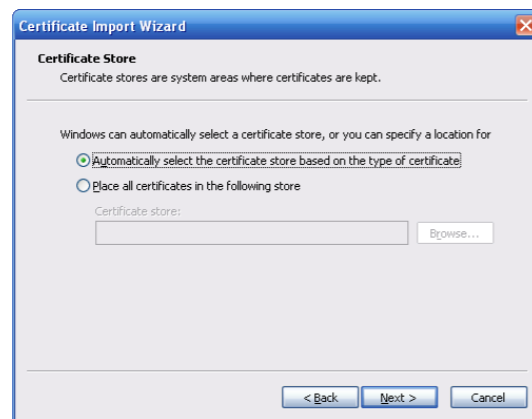
9. Click **Install Certificate**.

Certificate import wizard (1)



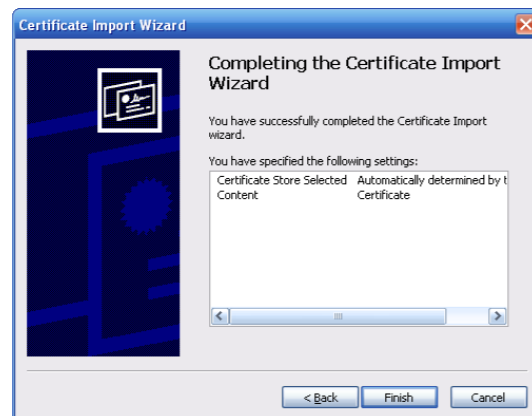
10. Click **Next**.

Certificate store



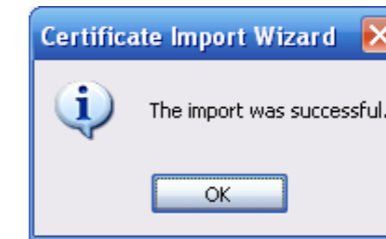
11. Select the storage location and click **Next**.

Certificate import wizard (2)



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

Import succeeds



## 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.

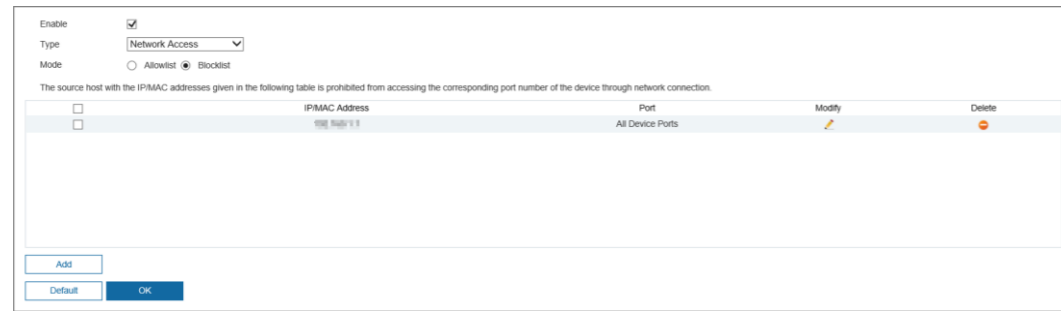
#### NOTE

- 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.

### Process

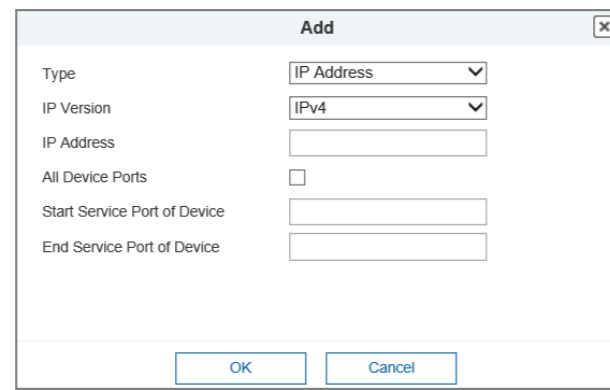
1. Select **Settings > Network > Advanced > Firewall**.
2. Select **Enable** to enable the firewall function.

## Firewall





3. Select **Network Access** from **Type** list, and then select the mode.
4. Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

## Firewall



5. Click **OK**.

## Related Operations

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

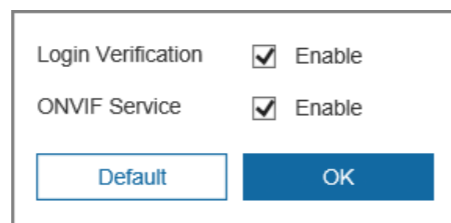
## ONVIF

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.

## Process

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

## ONVIF



2. Select the **Enable** checkbox next to **ONVIF Verification** and **ONVIF Service**.
3. Click **OK**.

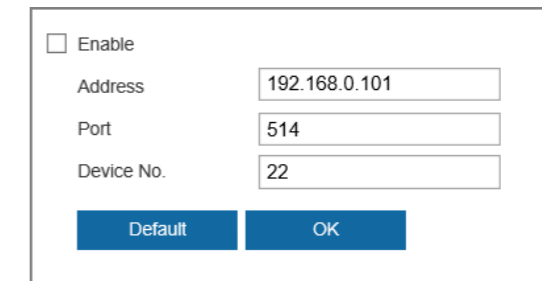
## Remote Log Records

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

## Process

1. Select **Settings > Network > Advanced > Remote Log Records**.
2. Select **Enable** checkbox to enable remote log function.
3. Set address, port and device number.
4. Click **OK**.

## Remote log



## Video/Audio

## Video

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

## Process

1. Select **Settings > Video/Audio > Video > Video Stream**.
2. Configure video stream parameters.

NOTE

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

Video stream

**Video Stream**

**Main Stream**

Encoding Mode  H.264  H.265

Smart Encoding  On  Off

Resolution

Frame Rate (fps)

Bit Rate Type

Bit Rate  (Kb/S)

I-Frame Interval

Stream Smooth

**Sub Stream**

Enable  Sub Stream 1  Sub Stream 2

Encoding Mode  H.264  MJPEG  H.265

Resolution

Frame Rate (fps)

Bit Rate Type

Bit Rate  (Kb/S)

I-Frame Interval

Stream Smooth

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: <ul style="list-style-type: none"> <li>• <b>CBR</b> (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value.</li> <li>• <b>VBR</b> (Variable Bit Rate): The bit rate changes as monitoring scene changes.</li> </ul> <p> NOTE The <b>Bit Rate Type</b> can only be set as <b>CBR</b> when <b>Smart Encoding</b> is set as <b>On</b>.</p>
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 <b>Stream Smooth</b> . The higher the value, the less smooth the stream, but the higher the image definition.

3. Click **OK**.

## Audio

### Configuring Audio

#### Process

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

Audio

**Audio** Alarm Audio

Stream Type  Main Stream  Sub Stream 1  Sub Stream 2

Encoding Mode

Sampling Rate

Audio Input Type

Filter Ambient Noise  Enable  Close

Microphone Volume

Speaker Volume

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

3. Configure audio parameters.

# Network Camera User Manual

Description of audio parameters

Parameter	Description
Encoding Mode	You can select from <b>PCM, G.711A, G.711Mu, G.726, AAC, G.723</b> . 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 <b>8000, 16000, 32000, 48000, 64000</b> .
Audio Input Type	You can select audio input type from <b>Lineln, Mic</b> and <b>realMic</b> .
Filter Ambient Noise	Enable this function, the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

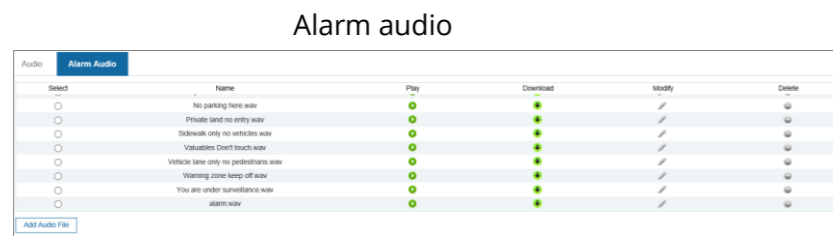
4. Click **OK**.

## Configuring Alarm Audio

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

### Process

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



2. Click **Add Audio File**.

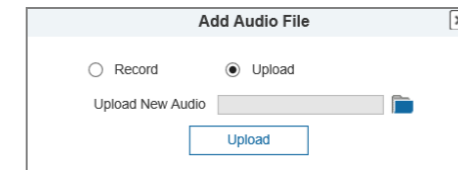
3. Configure the audio file.

- 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**.

### NOTE

- 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.

Add audio file



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.

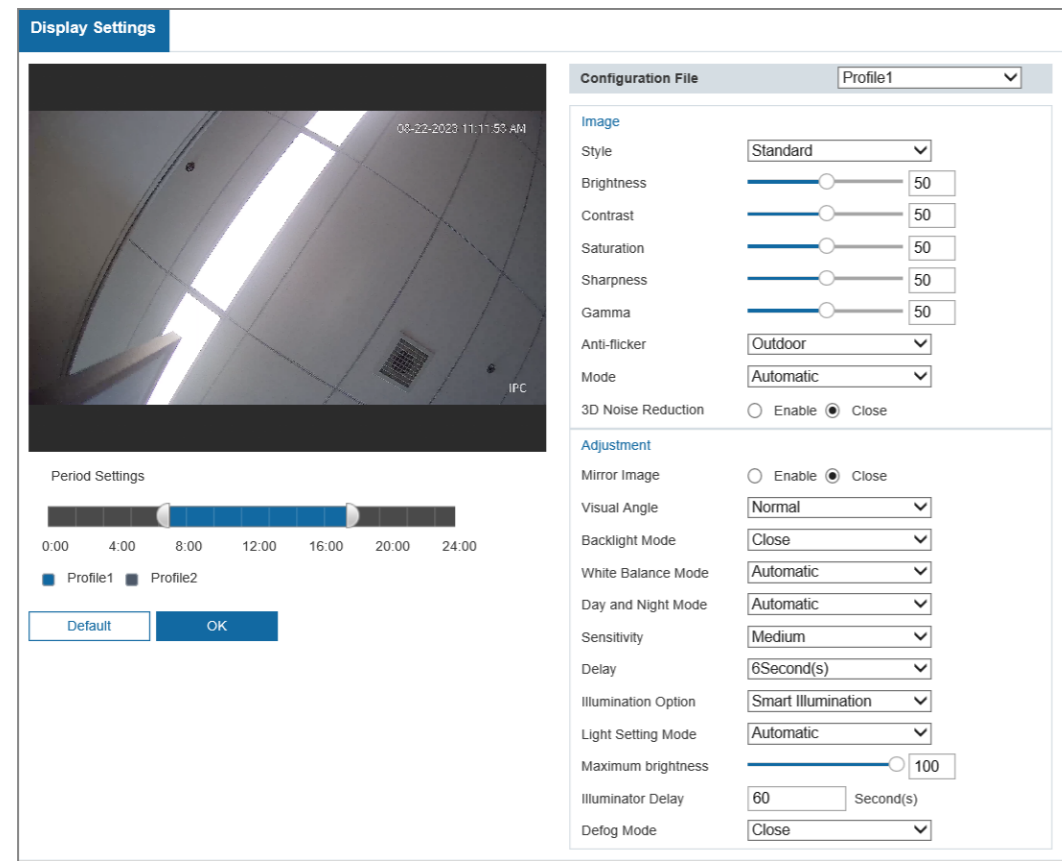
## Image

### Display Settings

#### Process

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

## Display settings



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

### Description of display settings

Parameter	Description
Style	Select the picture style from soft, standard and vivid. <ul style="list-style-type: none"> <li>• <b>Standard:</b> Default image style, displays the actual color of the image.</li> <li>• <b>Soft:</b> The hue of the image is weaker than the actual one, and contrast is smaller.</li> <li>• <b>Vivid:</b> The image is more vivid than the actual one.</li> </ul>
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.

Parameter	Description
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. <ul style="list-style-type: none"> <li>• <b>50 Hz:</b> 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.</li> <li>• <b>60 Hz:</b> 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.</li> <li>• <b>Outdoor:</b> You can select any exposure mode as needed.</li> </ul>
Mode	Device exposure modes. <ul style="list-style-type: none"> <li>• <b>Automatic:</b> Adjusts the image brightness according to the actual condition automatically.</li> <li>• <b>Manual:</b> Configure gain and shutter value manually to adjust image brightness.</li> </ul>
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 <b>Enable</b> , and the picture would display with left and right sides reversed.
Visual Angle	Change the display direction of the image.

Parameter	Description
Backlight Mode	<p>Adjust the backlight compensation mode of the monitoring screen.</p> <ul style="list-style-type: none"> <li>• <b>Close:</b> Backlight is disabled.</li> <li>• <b>Backlight Compensation:</b> 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.</li> <li>• <b>Highlight Compensation:</b> 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.</li> <li>• <b>Wide Dynamic Range:</b> When in WDR (Wide Dynamic Range) mode, the camera constrains over bright areas and compensates dark areas to improve the image clarity.</li> <li>• <b>Scene-adaptive:</b> The system automatically adjusts image brightness according to ambient lighting condition to ensure image clarity.</li> </ul>
White Balance Mode	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> The system compensates white balance according to color temperature to ensure color precision.</li> <li>• <b>Daylight:</b> The system automatically compensates white balance to environments without artificial light to ensure color precision.</li> <li>• <b>Street Lamp:</b> The system compensates white balance to outdoor night scene to ensure color precision.</li> <li>• <b>Outdoor:</b> The system auto compensates white balance to most outdoor environments with natural or artificial light to ensure color precision.</li> <li>• <b>Manual:</b> Configure red and blue gain manually; the system auto compensates white balance according to color temperature.</li> <li>• <b>Custom Area:</b> The system compensates white balance only to the set area according to color temperature to ensure color precision.</li> </ul>

Parameter	Description
Day and Night Mode	<p>Configure the display mode of the image. The system switches between color and black-and-white modes according to the actual condition.</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> The system switches between color and black-and-white display according to the actual condition.</li> <li>• <b>Full Color:</b> The system displays color image.</li> <li>• <b>Black &amp; White:</b> The system displays black-and-white image.</li> </ul>
Sensitivity	<p>This configuration is available only when you set <b>Auto</b> in <b>Day and Night Mode</b>. You can configure camera sensitivity when switching between color and black-and-white modes.</p>
Delay	<p>This configuration is available only when you set <b>Auto</b> in <b>Day and Night Mode</b>. 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.</p>
Illumination Option	<p>Configure the illumination mode. You can select from <b>Infrared Mode, White Light Mode</b> and <b>Smart Illumination</b>.</p>
Light Setting Mode	<p>You can select from <b>Manual, Automatic</b> and <b>Close</b>. When select <b>Manual</b>, you can adjust the brightness according to the actual needs.</p>
Defog Mode	<p>The image quality is compromised in foggy or hazy environment, and defog can be used to improve image clarity.</p> <ul style="list-style-type: none"> <li>• <b>Manual:</b> 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.</li> <li>• <b>Automatic:</b> The system adjusts image clarity according to the actual condition.</li> <li>• <b>Close:</b> Defog function is disabled.</li> </ul>

4. Click **OK**

## OSD

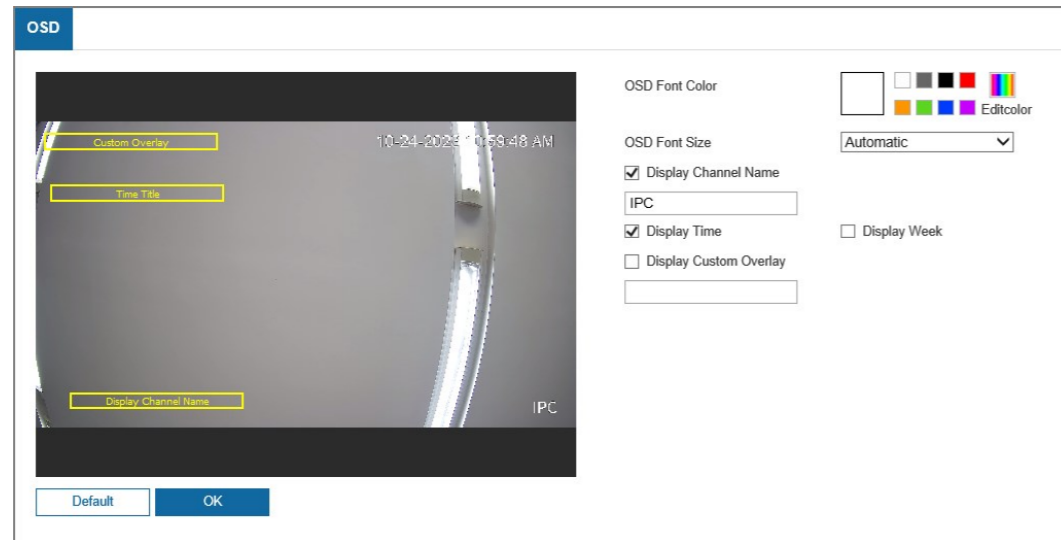
After enabling this function, the selected information will be displayed on the image.

## Process

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



OSD



2. Select the color and size of OSD information as needed.
3. Configure the display information, and then click **OK**.

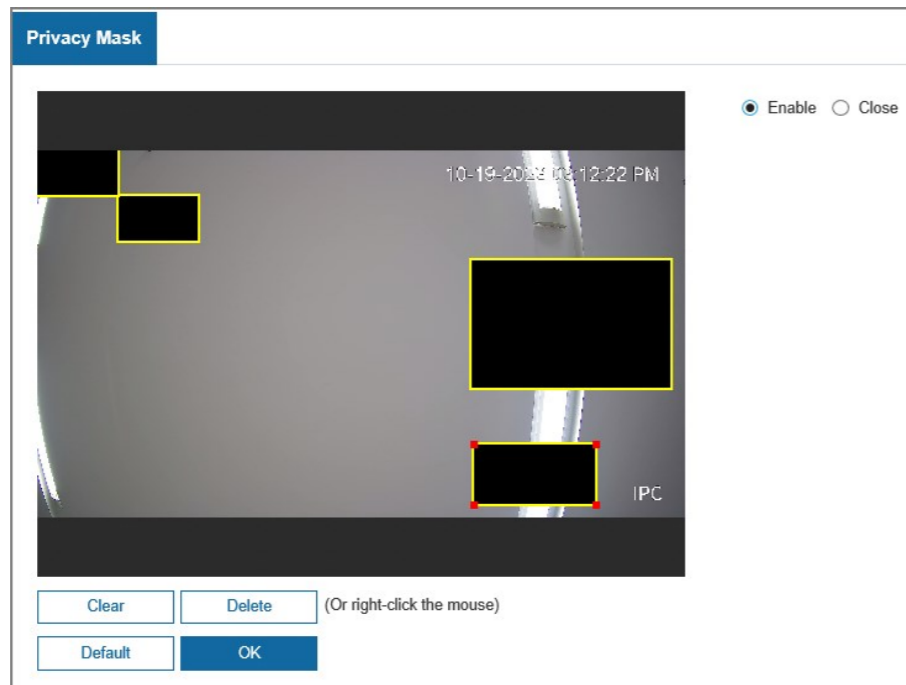
## Privacy Mask

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

### Process

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

Privacy mask



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

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

## Related Operations

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

## Event

### Basic Event

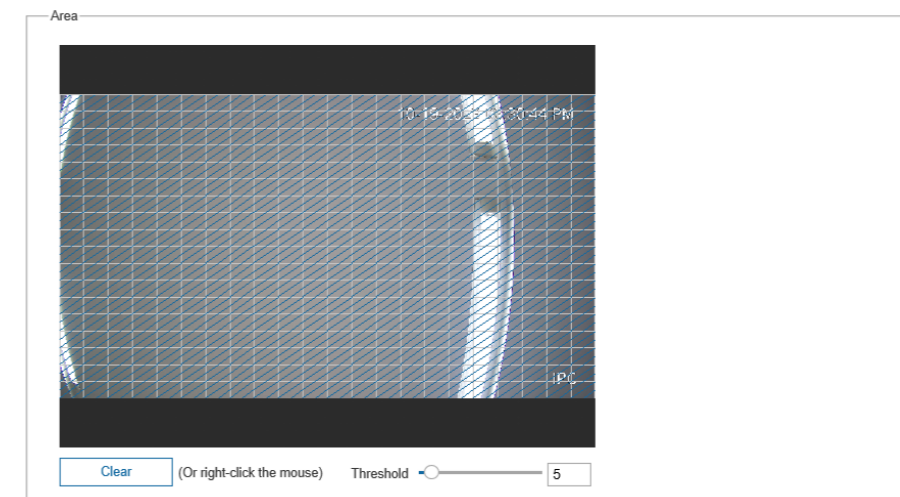
### Configuring Motion Detection

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

### Process

1. Select **Settings > Event > Basic Event > Motion Detection**.
2. Select the **Enable** checkbox to enable this function.
3. Set the area for motion detection.  
Click and drag the mouse to select the area. The detection region can be irregular and discontinuous.

Detection area



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.

MD 2.0

5. Set arming and disarming period.
6. Configure the alarm linkage such as video recording, alarm output. For details, see "7.5.1.5 Configuring Alarm Linkage".
7. Click **OK**.

## Configuring Audio Detection

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

### Process

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

Audio detection

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

4. Click **OK**.

## 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.

### Process

1. Select **Settings > Event > Basic Event > Video Tampering**.
2. Select the **Enable** checkbox.

Video tampering

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.

3. Set the schedule and alarm linkage action. For details, see "7.5.1.5 Configuring Alarm Linkage".
4. Click **OK**.

## Configuring Scene Changing

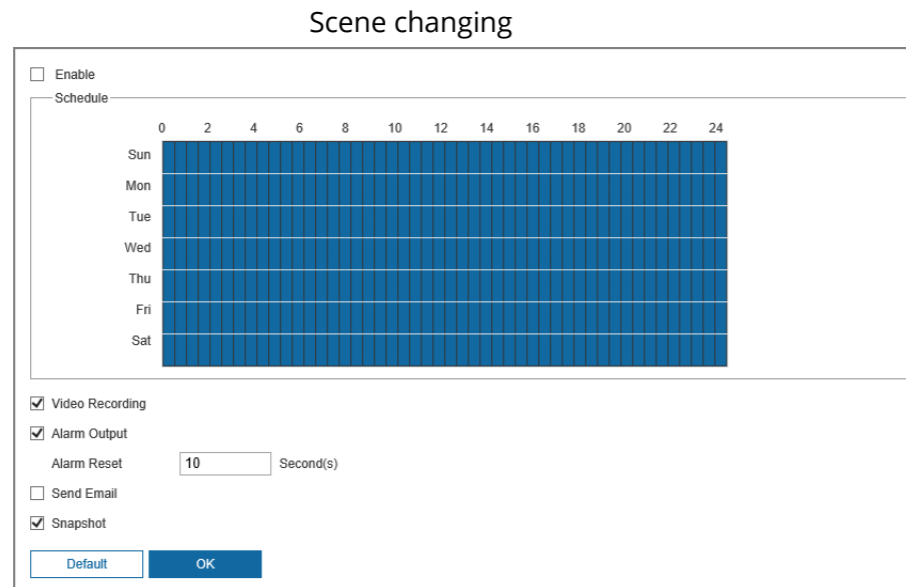
The system performs alarm linkage when the image switches from the current scene to another

# Network Camera User Manual

one.

## Process

1. Select **Settings > Event > Basic Event > Scene Changing**.
2. Select **Enable** checkbox.

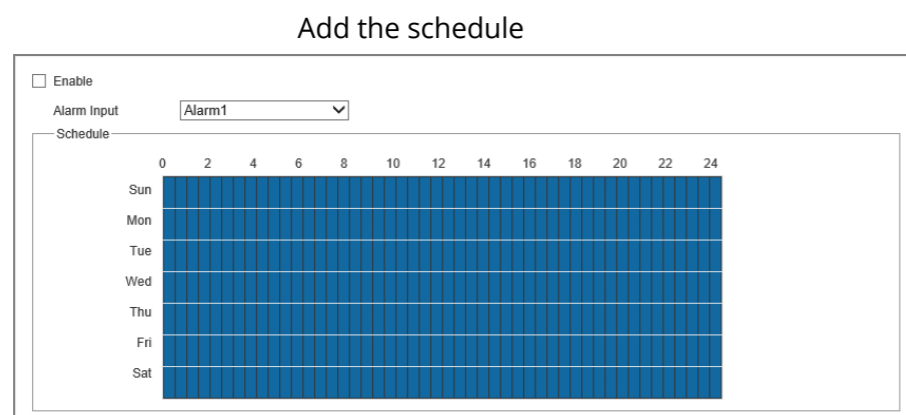


3. Select the schedule and alarm linkage action. For details, see "7.5.1.5 Configuring Alarm Linkage".
4. Click **OK**.

## Configuring Alarm Linkage

### Process

1. Select **Settings > Event > Basic Event > Audio Linkage**.
2. Select **Enable** checkbox to enable this function.
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.

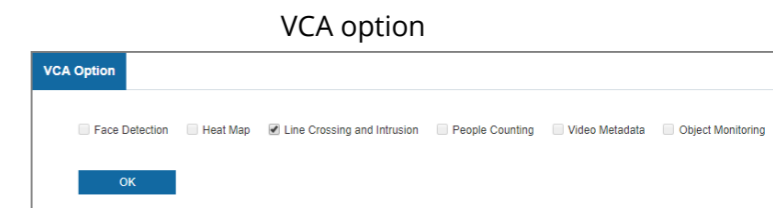


4. Configure the **Event Interval** and **Sensor Type**.
  - **Event Interval:** Only record one alarm event during the configured period.
  - **Sensor Type:** You can select from **Normally Open** and **Normally Closed**.
5. Configure the corresponding linkage.
  - **Video Recording:** The system can 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 "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.
6. Click **OK**.

## VCA Option

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Option**.



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

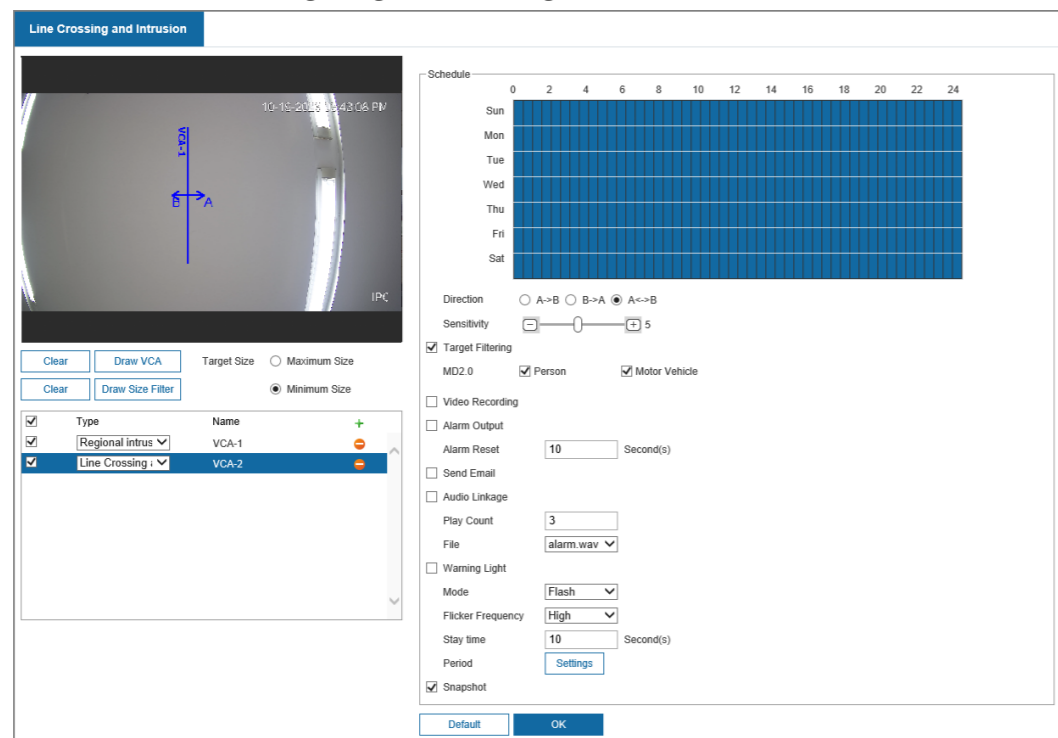
## Line Crossing and Intrusion

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA > Line Crossing and Intrusion**.
3. Click **+** to add the rule.
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.

Configuring line crossing and intrusion



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

Description of parameters

Parameter	Description
Direction	Set the direction of rule detection. <ul style="list-style-type: none"> <li>• When setting tripwire, select <b>A-&gt;B</b>, <b>B-&gt;A</b>, or <b>A&lt;-&gt;B</b>.</li> <li>• When setting intrusion, select <b>Appear</b>, <b>Cross the region</b>, or <b>Within Area</b>.</li> </ul>
Sensitivity	When the sensitivity is high, detection becomes easier, but the number of false detections increases. <p> NOTE</p> <p><b>Regional intrusion</b> does not support this function.</p>
Target Filtering	Select <b>Target Filtering</b> to enable this function. <ul style="list-style-type: none"> <li>• When you select <b>Person</b> as the alarm target, an alarm will be triggered when the system detects that person trigger the rule.</li> <li>• When you select <b>Motor Vehicle</b> as the alarm target, alarm will be triggered when the system detects that vehicle triggers the rule.</li> </ul>

8. Configure the alarm schedule and linkage. For details, see "Configuring Alarm Linkage".
9. Click **OK**.

## VCA Advanced

This function is available on select models.

## People Counting

### 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

# Network Camera User Manual

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.

## Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > People Counting**.
3. In the **Type** list, select the type as needed.
4. Click **Draw Detection Line** to adjust the detection line in the image.  
Click **Draw VCA** to adjust the detection area.



NOTE

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

5. Set rule parameters including number of people entered, exit and stay.
6. Configure the alarm schedule and linkage. For details, see "Configuring Alarm Linkage".
7. Click **OK**.

## Viewing People Counting Report

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Report > People Counting Report**.
3. Select the report type, start time, end time, and other parameters.
4. Click **Search** to complete the report.  
Click **Export** to export the statistical report.

## Heat Map

### Heat Map Configuration

#### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > Heat Map**.
3. Select the **Enable** checkbox, and then the heat map function is enabled.
4. Configure the schedule, and then click **OK**.

## Viewing Heat Map Report

### Process

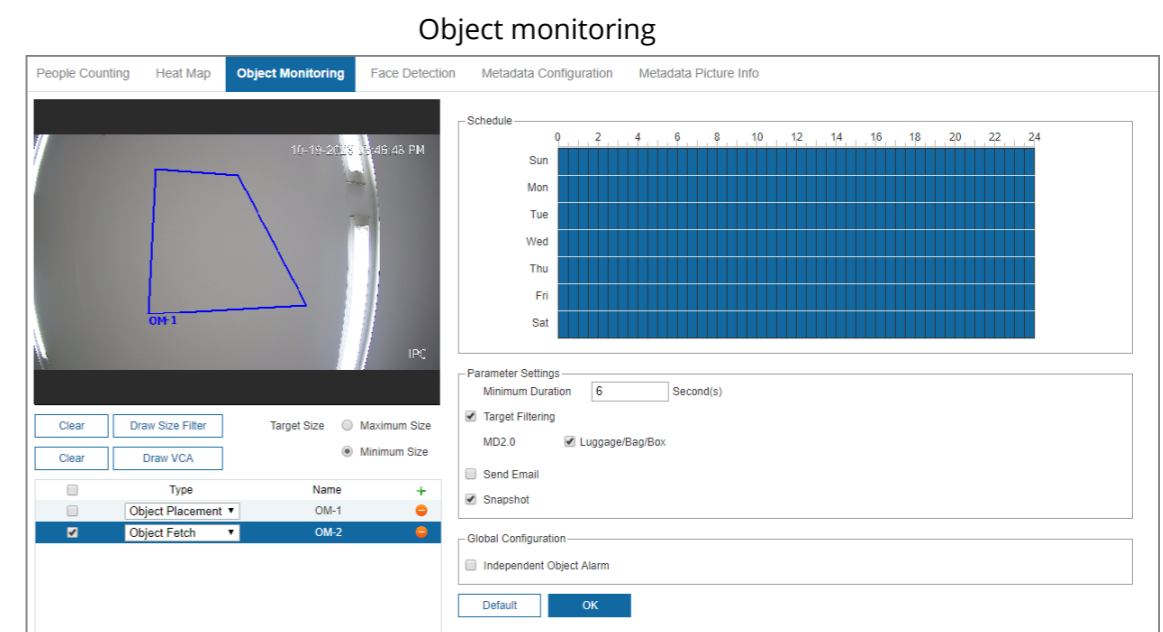
1. Log in to the webpage of the device.

2. Click **Settings > Event > VCA Report > Heat Map Report**.
3. Select the start time, end time and the threshold.
4. Click **Search** to complete the report.  
Click **Export** to export the statistical report.

## Object Monitoring

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > Object Monitoring**.



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.
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.



NOTE

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

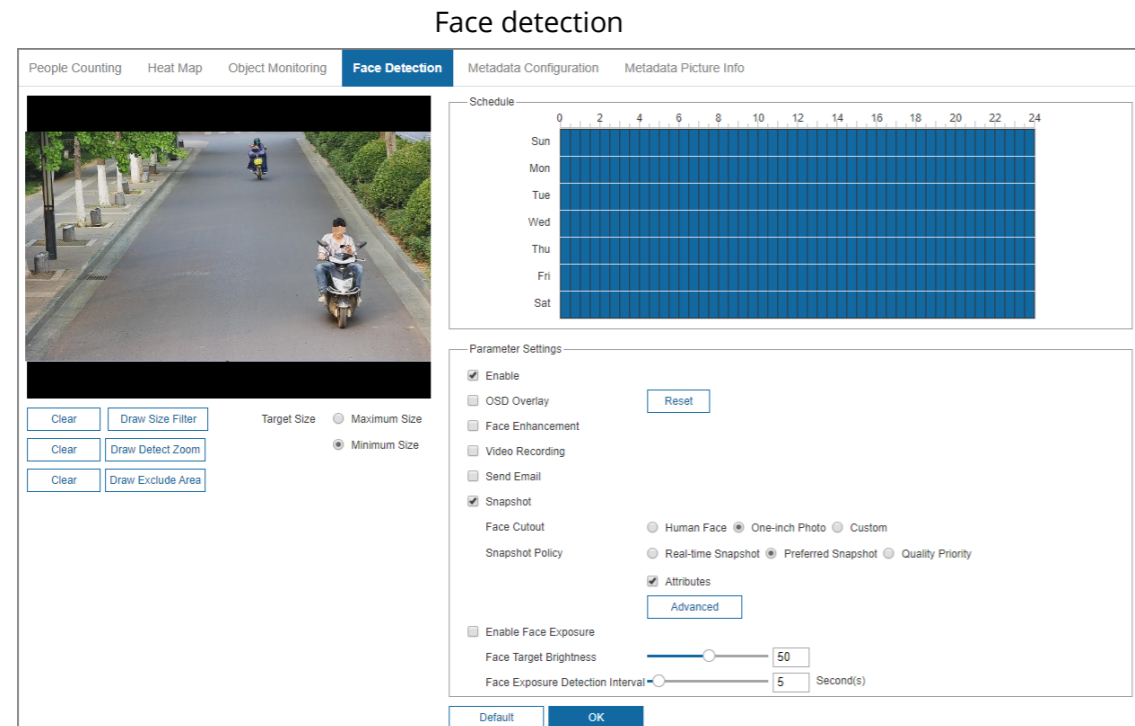
5. Set the schedule and rule parameters including minimum duration, target filtering.
6. Configure the alarm schedule and linkage. For details, see "Configuring Alarm Linkage".
7. Click **OK**.

# Network Camera User Manual

## Face Detection

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > Face Detection**.



3. Select **Enable** checkbox.
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.
5. Click **Draw Detect Zoom** to draw the detection area.
6. Click **Draw Exclude Area** to draw the exclude area.



**NOTE**

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

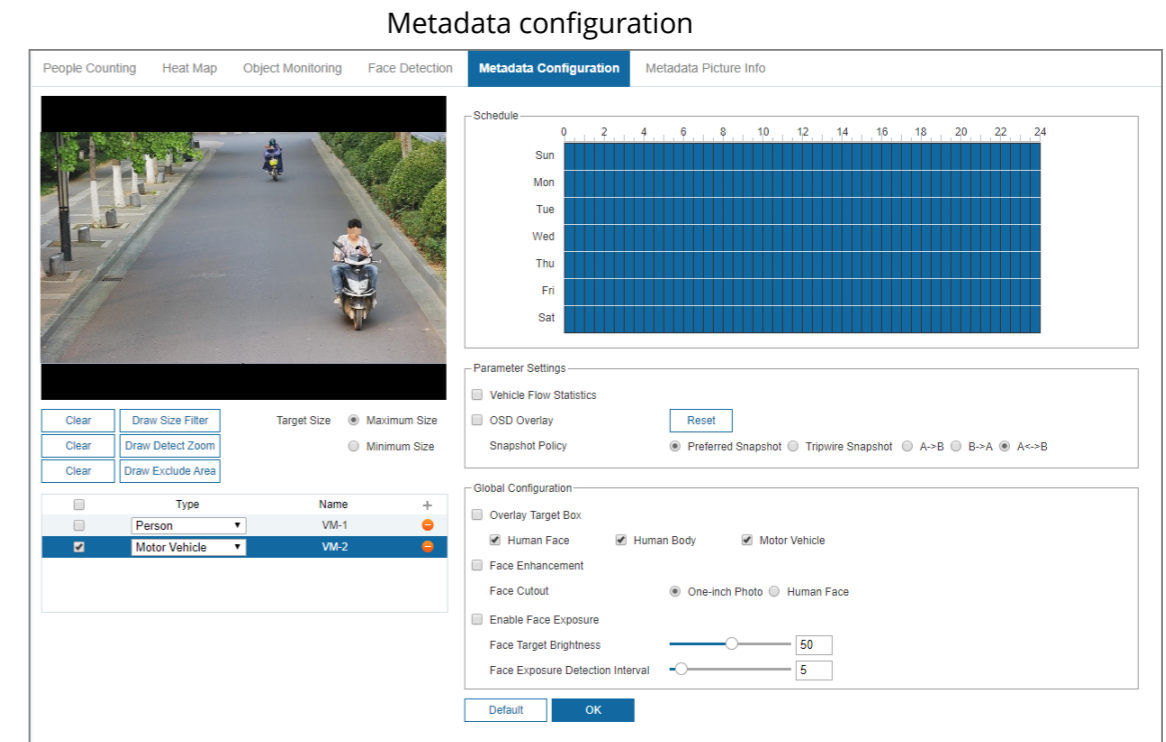
7. Set the schedule and rule parameters including OSD overlay and face enhancement.
8. Configure the alarm schedule and linkage. For details, see "Configuring Alarm Linkage".
9. Click **OK**.

## Metadata

### Metadata Configuration

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > Metadata Configuration**.



3. Set the global configuration.

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.

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

# Network Camera User Manual

- 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.

6. Set the schedule and parameters.
7. Click **OK**.

## Viewing Metadata Report

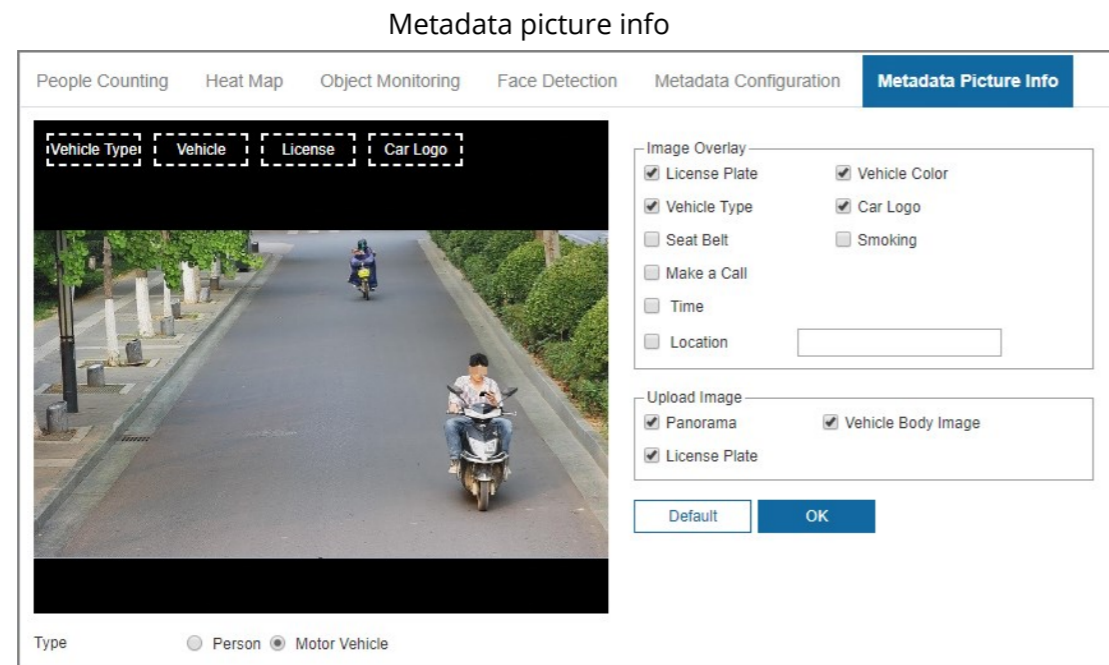
### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Report > Metadata Report**.
3. Select the report type, start time, end time, and other parameters.
4. Click **Search** to complete the report.  
Click **Export** to export the statistical report.

## Metadata Picture Info

### Process

1. Log in to the webpage of the device.
2. Click **Settings > Event > VCA Advanced > Metadata Picture Info**.



3. Select the type from motor vehicle and person.
4. Select the overlay information and upload image, and then click **OK**.

## 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.

#### Abnormal SD Card

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

#### Network exception

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

# Network Camera User Manual

## Security Exception

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

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

## Storage

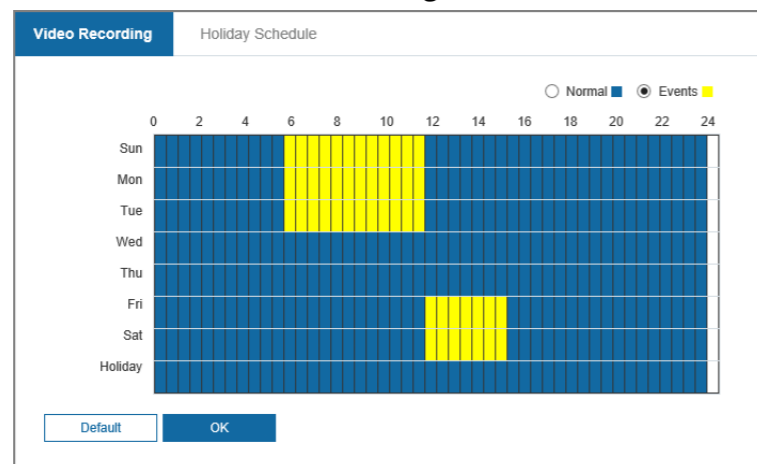
### Configuring Schedule

#### Video Recording

##### Process

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

Video recording



3. Click **OK**.

## 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.

##### Process

1. Select **Settings > Storage > Schedule > Holiday Schedule**.
2. Select **Video Recording** and **Snapshot** as needed, and then configure the time.

Holiday schedule

Video Recording

Holiday Schedule

Video Recording:  On  Off

Snapshot:  On  Off

Mode:  By Day

Start Time: 2023-08-18

End Time: 2023-08-18

Default OK

##### NOTE

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.

3. Click **OK**.

### Configuring Storage

#### 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.

##### Process

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



Storage location

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

Description of storage location parameters

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

3. Click **OK**.

## Local Storage

Display the information of the local SD card.

### Process

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

Local storage

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

## Configuring Recording Control

### Process

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

Recording control

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. NOTE 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. <ul style="list-style-type: none"> <li>• <b>Stop</b>: Stop recording when the disk is full.</li> <li>• <b>Overwrite</b>: Cyclically overwrite the earliest video when the disk is full.</li> </ul>
Recording Stream	Select record stream, including <b>Main Stream</b> and <b>Sub Stream</b> .

2. Click **OK**.

## Snapshot

### Configuring Snapshot Parameters

#### Process

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

Configuring snapshot parameters

Parameters

Schedule

Snapshot Type Continuous ▾

Image Size 2688x1520 (2688\*1520)

Image Quality Medium ▾

Snapshot Interval 1S ▾

Default
OK

Description of image stream parameters

Parameter	Description
Snapshot Type	You can select from <b>Continuous</b> and <b>Event</b> .
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.
Snapshot Interval	Configures the snapshot frequency. Select <b>Custom</b> , and then you can configure snapshot frequency manually.

2. Click **OK**.

### Configuring Snapshot Schedule

#### Process

1. Select **Settings > Storage > Snapshot > Schedule.**
2. Select snapshot type, and then set time period.

Configuring snapshot schedule

Parameters

Schedule

Normal ■
 Events ■

Sun  
Mon  
Tue  
Wed  
Thu  
Fri  
Sat  
Holiday

024681012141618202224

Sun
Mon
Tue
Wed
Thu
Fri
Sat
Holiday

Default
OK

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.

3. Click **OK**.

## 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 Process 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.