

Network Camera User Manual

Manual Version: V3.05

Thank you for your purchase. If you have any questions, please do not hesitate to contact your dealer.

Safety Instructions



CAUTION!

The default password is intended only for your first login. For security, we strongly recommend you set a strong password of at least 9 characters comprising digits, letters, and special characters.

Be sure to read this manual carefully before use and strictly comply with this manual during operation.

The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc., in this manual may be different from the actual appearances, functions, features, etc., of the product.
- The mouse operations described in this manual are right-handed operations.
- We reserve the right to change any information in this manual without any prior notice or indication.
- Due to uncertainties such as physical environment, discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.
- Users are fully responsible for the damages and losses that arise due to improper operations.




Environmental Protection

This product has been designed to comply with the requirements regarding environmental protection.

For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Safety Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
 WARNING!	Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.
 CAUTION!	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 NOTE!	Indicates useful or supplemental information about the use of product.

Contents

Safety Instructions	i
Environmental Protection.....	i
Safety Symbols	i
1 Login	1
1.1 Preparation	1
1.2 Login	1
2 Live View.....	3
2.1 Live View	3
2.1.1 Pixel Calculation	5
2.1.2 Digital Zoom	6
2.2 General Parameters	6
3 Playback.....	7
3.1 Playback Toolbar.....	7
3.2 Search and Playback	8
3.3 Recording Download	8
4 Photo.....	10
5 Setup.....	11
5.1 Local Parameters	11
5.2 Network.....	13
5.2.1 Basic Config	13
5.2.2 Service Configuration	17
5.2.3 Platform Access	22
5.3 Video & Audio.....	28
5.3.1 Video	28
5.3.2 Snapshot	30
5.3.3 Audio	31
5.3.4 ROI.....	33
5.3.5 View Cropping.....	34
5.3.6 Media Stream	35
5.4 Image	36
5.4.1 Image.....	36
5.4.2 OSD	45
5.4.3 Privacy Mask	47
5.4.4 Quick Focus	49
5.5 Smart.....	50

5.5.1 Alarm-triggered Actions	50
5.5.2 Arming Schedule	53
5.5.3 Smart Service Switch	54
5.5.4 Cross Line Detection	56
5.5.5 Intrusion Detection	57
5.5.6 Object Removed Detection	59
5.5.7 Object Left Behind Detection	60
5.5.8 Defocus Detection	62
5.5.9 Scene Change Detection	62
5.5.10 Human Body Detection	62
5.6 Alarm	63
5.6.1 Common Alarm	64
5.6.2 One-key Disarming	71
5.7 Storage	72
5.7.1 Memory Card	73
5.7.2 Network Disk	74
5.7.3 FTP	75
5.8 Security	77
5.8.1 User	77
5.8.2 HTTPS	80
5.8.3 Authentication	80
5.8.4 Registration Information	81
5.8.5 ARP Protection	81
5.8.6 IP Address Filtering	82
5.8.7 Access Policy	82
5.8.8 Certificate Management	84
5.8.9 Watermark	87
5.9 System	87
5.9.1 Time	87
5.9.2 DST	88
5.9.3 Alarm Server	88
5.9.4 Device Information	89
5.9.5 Maintenance	89
5.9.6 Logs	92

1 Login

1.1 Preparation

Refer to the camera's quick guide to complete installation, and then connect the camera to power to start it up. You can log in to the camera's web interface to perform management or maintenance operations. Windows 7, 8 or later is installed on the PC. The following takes Windows 7 as an example.

Check before login

- The camera runs normally.
- The PC has a network connection to the camera.
- You have permission to operate the PC.
- Google Chrome 105 or later is recommended on the PC.
- A 32-bit or 64-bit Web browser is required if you are using a 64-bit operating system. It is recommended to use a monitor with the highest resolution for better display.



NOTE!

Recommended PC configurations for 32MP live view: Intel® Core™ i7 8700 processor; GTX 1080 graphics card; DDR4 8GB or higher.

1.2 Login

The default static IP address of the camera is **192.168.1.13**, and the default subnet mask is **255.255.255.0**.

DHCP is enabled by default on the camera. If a DHCP server is deployed in the network, the camera may be assigned an IP address, and you need to use the assigned IP address to log in.

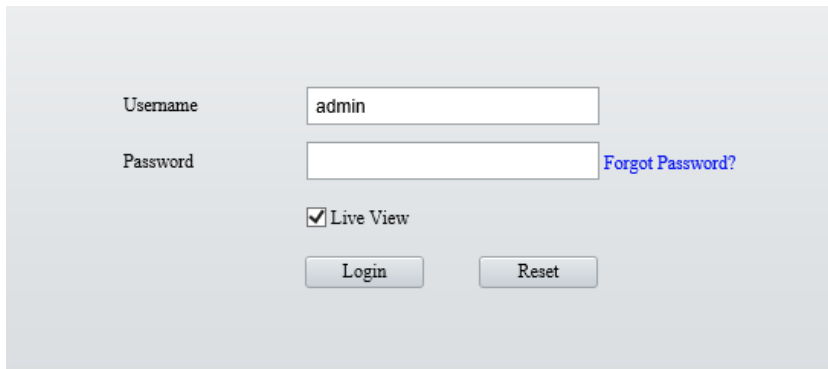
Follow the steps below to log in to the camera's web interface:

1. Open Chrome, enter the IP address of your camera in the address bar and press **Enter**.
2. At your first login, you need to follow the on-screen instructions to install a plug-in (close all browsers before installation), and then open the browser again to log in. To manually load the plug-in, type `http://IP address/ActiveX/Setup.exe` in the address bar and press **Enter**.



Please click here to [Download](#) and install the latest plug-in. Close your browser before installation.

3. Set whether to start live view automatically after login.
 - With **Live View** selected, live view will start automatically after login.
 - With **Live View** not selected, you need to start live view manually.

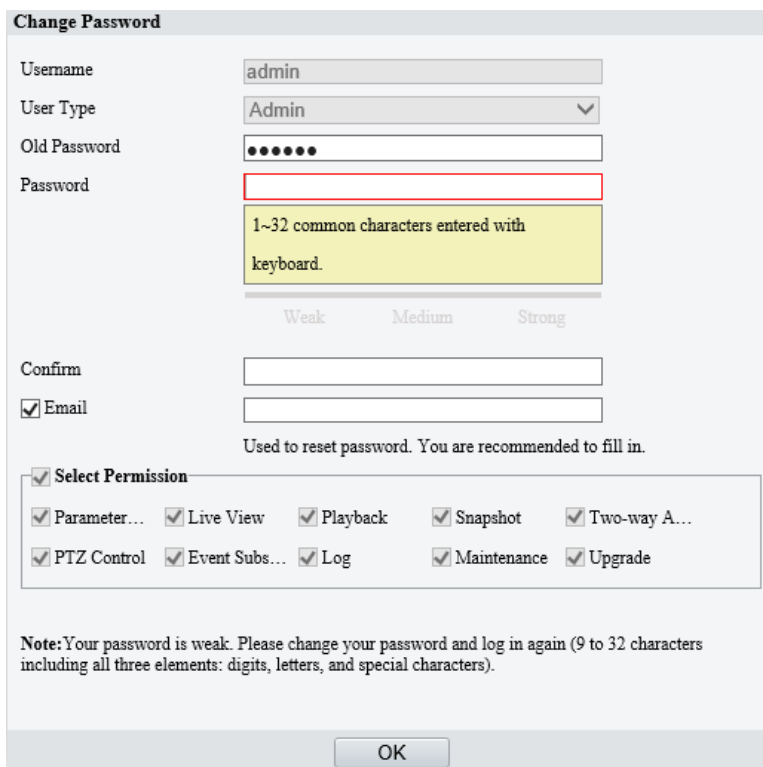


Username

Password [Forgot Password?](#)

☒ Live View

4. Enter the username and password (**admin/123456** by default) and click **Login**. To clear the **Username** and **Password** text boxes, click **Reset**.
5. After first login, the **Change Password** dialog box appears, in which you must set a strong password and enter your email address in case of password retrieval.
 - (1) Set a strong password of 9 to 32 characters including all three elements: digits, letters, and special characters.
 - (2) Enter your email address in case of password retrieval.



Change Password

Username

User Type

Old Password

Password

1~32 common characters entered with keyboard.

Weak Medium Strong

Confirm

☒ Email

Used to reset password. You are recommended to fill in.

☒ Select Permission

<input checked="" type="checkbox"/> Parameter...	<input checked="" type="checkbox"/> Live View	<input checked="" type="checkbox"/> Playback	<input checked="" type="checkbox"/> Snapshot	<input checked="" type="checkbox"/> Two-way A...
<input checked="" type="checkbox"/> PTZ Control	<input checked="" type="checkbox"/> Event Subs...	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Maintenance	<input checked="" type="checkbox"/> Upgrade

Note: Your password is weak. Please change your password and log in again (9 to 32 characters including all three elements: digits, letters, and special characters).

See [User](#) for more information.

If you forgot your password, click **Forgot Password** in the login page, then follow the on-screen instructions to reset your password.



NOTE!

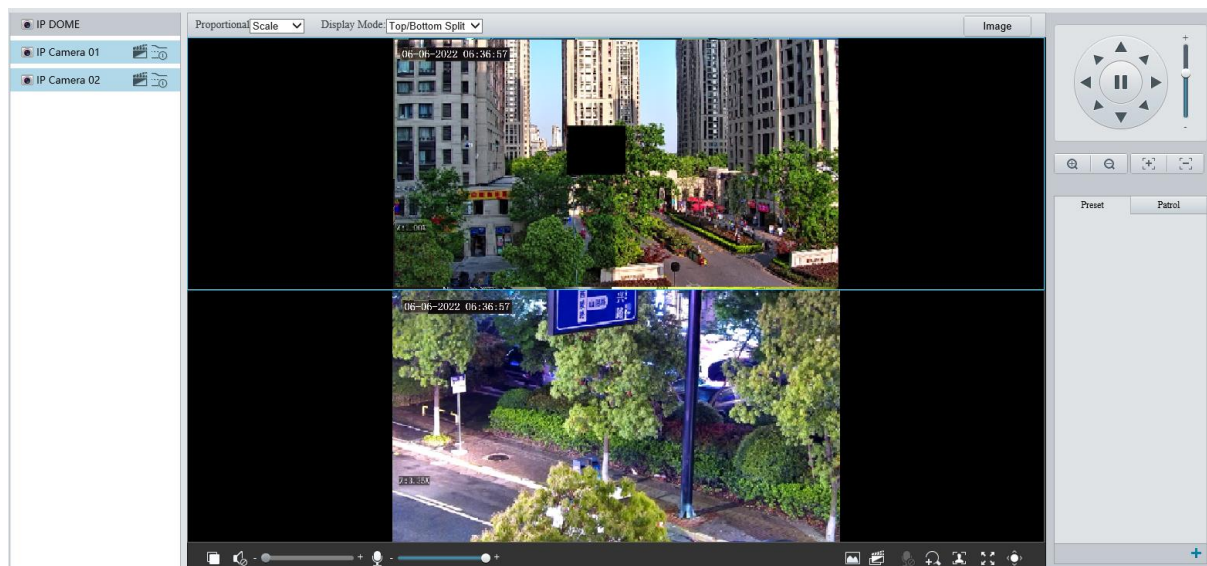
For certain devices, you may need to select the country/region and video standard and choose whether to enable the cloud service after your first login. Please refer to the actual interface.

2 Live View

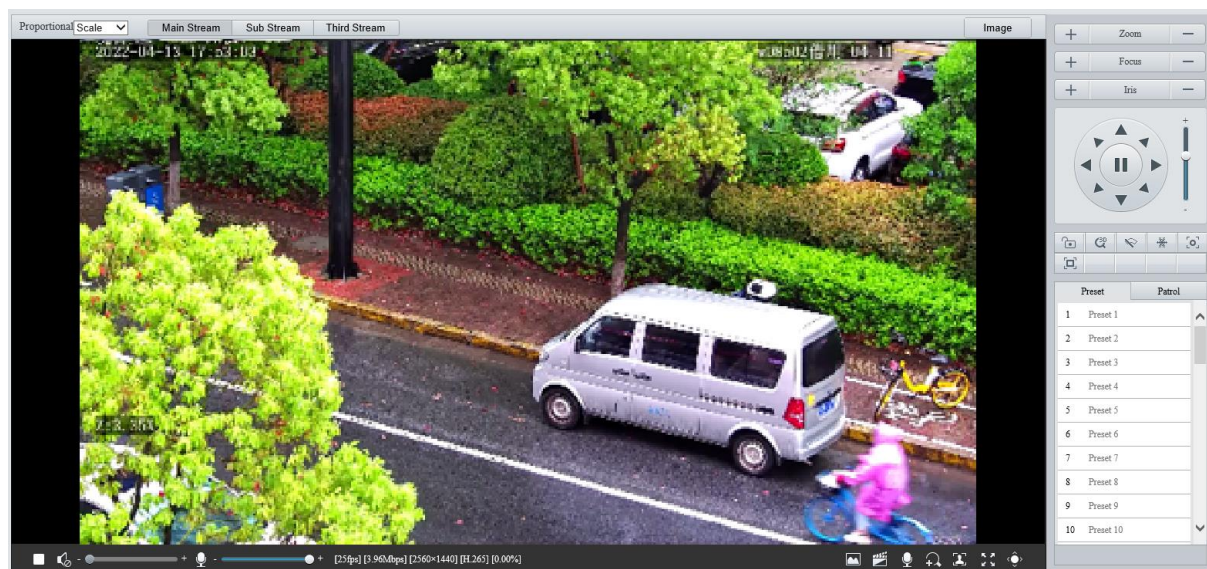
2.1 Live View

After login, the **Live View** page appears, showing the live video from the camera. You may double-click the window to enter or exit full screen mode.

Live view page of dual-channel camera



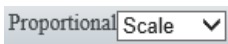
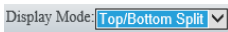
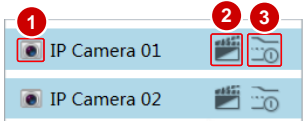
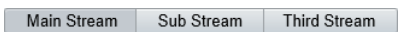














Live view page of single-channel camera



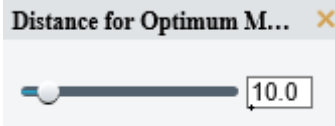
NOTE!

Live view operations supported may vary with device model.

Live View Toolbar

Item	Description
	Set the image display ratio in the window. <ul style="list-style-type: none"> Scale: Displays 16:9 images. Stretch: Displays images according to the window size (stretch images to fit the window). Original: Displays images with original size.
	Set the image display mode in the window. <ul style="list-style-type: none"> Single Channel: Displays live video of a single channel. Left/Right Split: Displays live video in left/right split mode. Top/Bottom Split: Displays live video in top/bottom split mode. Picture in Picture: Opens a floating live view window on top of the current window. <p>NOTE! This function is only available on dual-channel cameras.</p>
	<p>1 : Stop/start live view of the selected channel.</p> <p>2 : Start local recording.</p> <p>3 : Switch streams.</p>
	Select a live video stream according to your camera.
	Set image parameters.
	Start/stop live view.
	Turn off/on sound.
	Adjust the output volume for the media player on the PC. Range: 1 to 100.
	Adjust the microphone volume on the PC during audio communication between the PC and the camera. Range: 1 to 100.
	Frame rate/bit rate/resolution/packet loss rate.
	Enable/disable pixel calculation.
	Take a snapshot from the displayed live video. NOTE! See Local Parameters for the path of the saved snapshots.
	Start/stop local recording. NOTE! <ul style="list-style-type: none"> See Local Parameters for the path of the saved local recordings. VLC media player is recommended for playing local recordings of 4K cameras.
	Start/stop two-way audio.
	Start/stop digital zoom. See Digital Zoom for details.
	Start/stop capturing. See Error! Reference source not found. for details.
	Full screen.
	Display/hide the PTZ Control , General Parameters tabs.

Distance for Optimum Multi-Sensor Splice(m) button, used to adjust the distance from the monitored object to the lens to get the optimal images. The value range is [2.0-100]m, the default is 10m.



Adjust the splicing distance to optimize the splicing effect of the left and right screens. Examples are shown below:

The distance is too small, causing double images.

The distance is appropriate. The image is displayed correctly.

The distance is too large. The image looks smaller than normal.

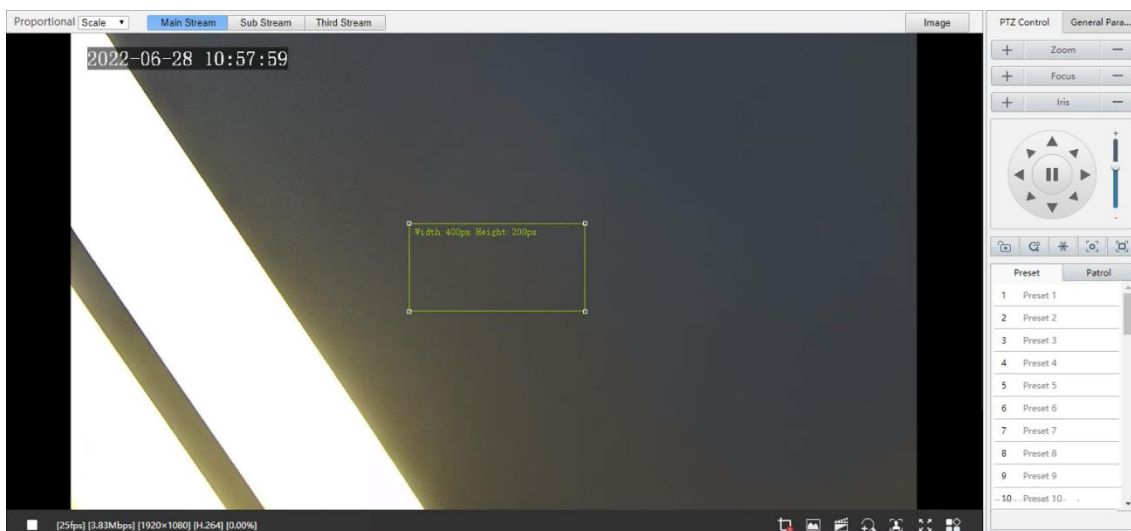



NOTE!

- This function is available on certain multi-sensor cameras.
- You need to set the optimal splicing distance according to the actual scene.


2.1.1 Pixel Calculation

1. Click  on the live view toolbar to enable pixel calculation.




2. Adjust the position and size of the detection area. The pixel value changes with the size of the detection area.
 - To adjust the position of the detection area, point to a border of the area and drag it to the desired position.
 - To adjust the size of the detection area, point to a handle of the box and drag to resize it.
 - To redraw the detection area, click on the image and drag to draw a new one.
3. To disable pixel calculation, click .

2.1.2 Digital Zoom

1. Click  on the live view toolbar to enable digital zoom.

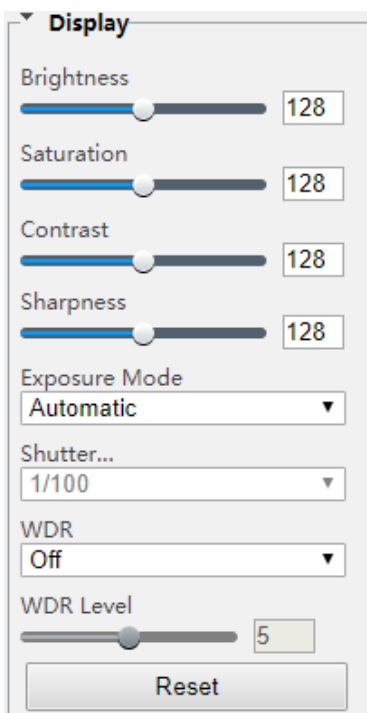


2. View the magnified area.
 - Click in the live view window and roll the wheel to zoom in or out on the image. Drag your mouse to view all the magnified area. To restore, right-click on the window.
 - Click in the live view window and drag your mouse to specify the area (rectangular area) to be magnified. Drag your mouse to view all the magnified area. To restore, right-click on the window.
3. To exit, click .

2.2 General Parameters

Set general parameters to view image effects directly.

On the live view page, click **General Parameters**.



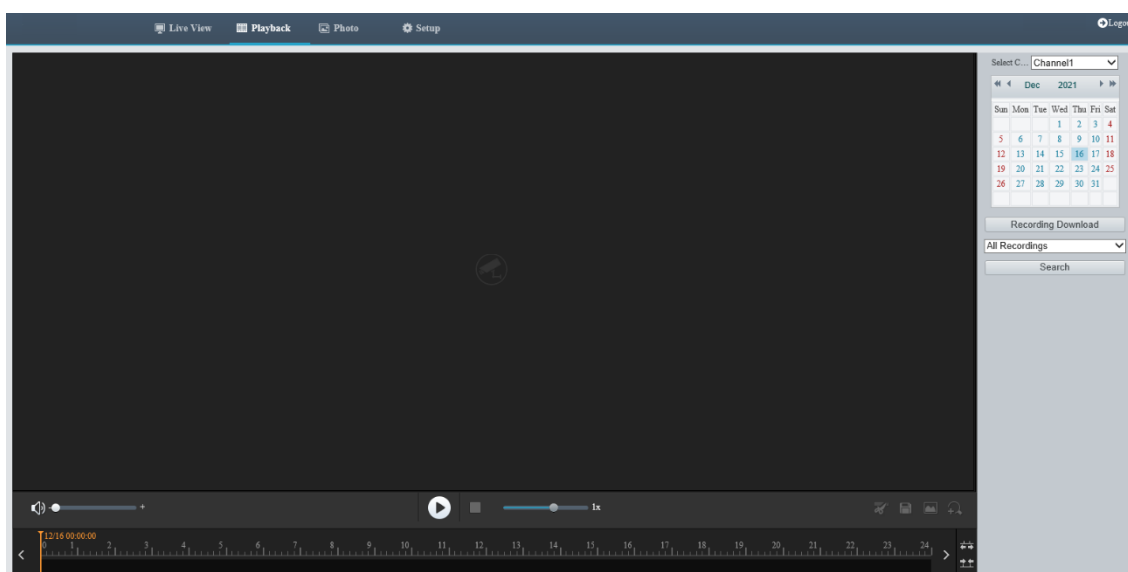
3 Playback



NOTE!

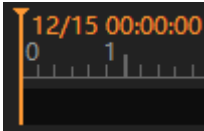
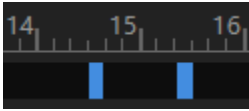
- Edge recordings refer to video recorded on storage media of cameras; local recordings refer to video recorded on a local PC.
- Before you search for edge recordings, make sure that the camera has storage resources such as memory card, and the storage parameters in [Storage](#) are properly configured.
- Recording playback and download functions are only available on certain models.
- For dual-channel devices, you can set playback parameters for the channels separately.

On the home page, click **Playback**.



3.1 Playback Toolbar

Button	Description
	Adjust sound volume. Range: 1 to 100.
	Start playback.
	Pause playback.
	Stop playback.
	Clip video.
	Save.
	Adjust playback speed. The default speed is 1x. 2x plays faster, and 1/2x plays slower. - 2x rewinds fast.
	Take a snapshot. The snapshots are saved locally by default. You can change the storage location in Local Parameters .
	Digital zoom. See Digital Zoom for details.
	Zoom in/out on the time scale. You can also use the scroll wheel to zoom.
	When the time scale is zoomed in, you can click or to view the previous or next section of the video.


	<p>Playhead. Drag the playhead to the desired point in the video.</p>
	<p>Playback timeline, including two colors:</p> <ul style="list-style-type: none"> • Blue: Normal recording. • Red: Alarm recording. To view alarm recordings, you need to configure alarm-triggered recording. See Alarm-triggered Actions for details.

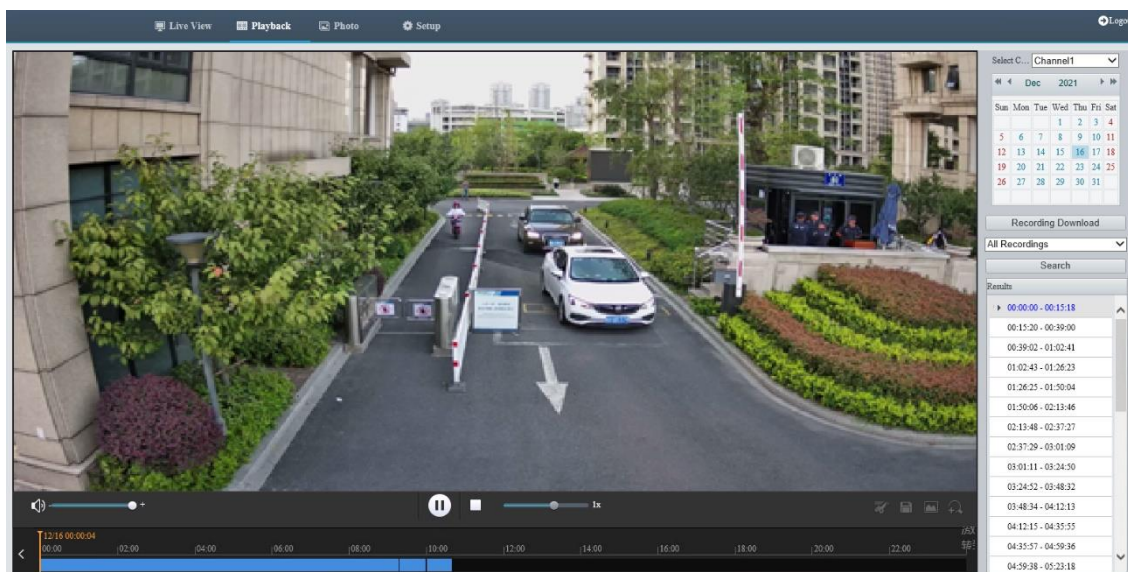
3.2 Search and Playback



NOTE!

Certain cameras support simultaneous playback on two clients.

1. For a multi-channel camera, select the channel first.
2. Select the date on the calendar.
3. Click **All Recording** in the list and then choose the recording type you want to search.
4. Click **Search**. Search results are displayed.
5. Double-click an item in the list to play the recording. The playback stops till it reaches the end of the list or when you click  to pause.



3.3 Recording Download

You can download videos or video clips in batches.

- Download recordings.
1. Click **Recording Download**.
 2. Choose the recording type, set a time range, and then click **Search**. Search results are displayed.

Recording Download



Recording Type: All Recordings ▼

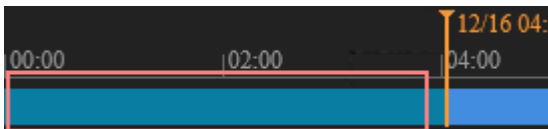
Recording Time: 2021-12-16 ~ 2021-12-16 Search

Recording Download: Browse...

<input type="checkbox"/>	No.	Start Time	End Time
<input type="checkbox"/>	1	2021-12-16 00:00:00	2021-12-16 00:15:18
<input type="checkbox"/>	2	2021-12-16 00:15:20	2021-12-16 00:39:00
<input type="checkbox"/>	3	2021-12-16 00:39:02	2021-12-16 01:02:41
<input type="checkbox"/>	4	2021-12-16 01:02:43	2021-12-16 01:26:23
<input type="checkbox"/>	5	2021-12-16 01:26:25	2021-12-16 01:50:04
<input type="checkbox"/>	6	2021-12-16 01:50:06	2021-12-16 02:13:46
<input type="checkbox"/>	7	2021-12-16 02:13:48	2021-12-16 02:37:27
<input type="checkbox"/>	8	2021-12-16 02:37:29	2021-12-16 03:01:09
<input type="checkbox"/>	9	2021-12-16 03:01:11	2021-12-16 03:24:50
<input type="checkbox"/>	10	2021-12-16 03:24:52	2021-12-16 03:48:32
<input type="checkbox"/>	11	2021-12-16 03:48:34	2021-12-16 04:12:13
<input type="checkbox"/>	12	2021-12-16 04:12:15	2021-12-16 04:35:55
<input type="checkbox"/>	13	2021-12-16 04:35:57	2021-12-16 04:59:36
<input type="checkbox"/>	14	2021-12-16 04:59:38	2021-12-16 05:23:18

Download

3. Click **Browse...** and set the download destination.
4. Select the checkboxes for the recordings you want to download and click **Download**.
 - Download video clips.
1. Search for the video you want to clip. See Search and Playback.
2. On the playback toolbar, click .
3. Click on the timeline to specify the clip by setting the start and end time.
4. Click . The clip turns cyan on the timeline.



5. Click . The **Recording Download** page appears.

Recording Download ✕

17, s07733

Recording Type: Alarm Recording ▾ Search

Alarm Type: Motion Detector ▾

<input type="checkbox"/>	No.	Start Time	End Time
<input type="checkbox"/>	1	2023-08-08 15:42:50	2023-08-08 15:43:50
<input type="checkbox"/>	2	2023-08-08 15:43:52	2023-08-08 15:46:56
<input type="checkbox"/>	3	2023-08-08 15:48:13	2023-08-08 15:50:20

Download

Recording Download ✕

17, s07733

Recording Type: Alarm Recording ▾ Search

Alarm Type: Motion Detector ▾

Recording Download: Browse...

<input type="checkbox"/>	No.	Start Time	End Time
<input type="checkbox"/>	1	2023-08-08 15:42:50	2023-08-08 15:43:50
<input type="checkbox"/>	2	2023-08-08 15:43:52	2023-08-08 15:46:56
<input type="checkbox"/>	3	2023-08-08 15:48:13	2023-08-08 15:50:20

Download

6. Click **Browse...** and set the download destination.
7. Select the checkbox for the clips you want to download and click **Download**.

4 Photo

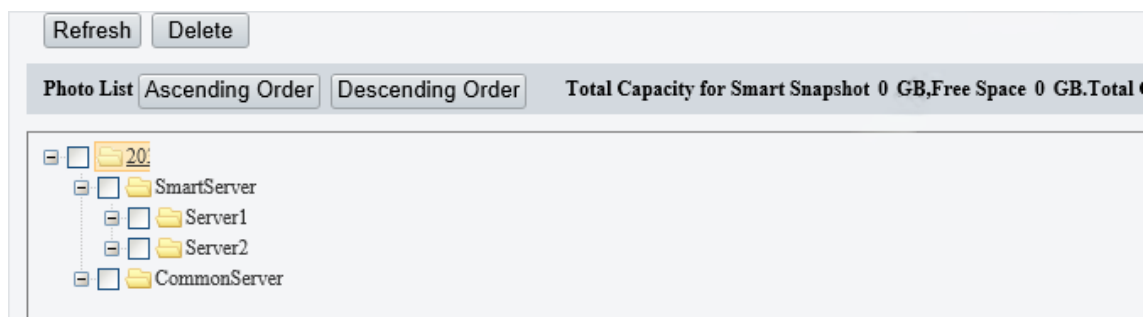
View the photo storage status. See Storage for photo storage policy.



NOTE!

This function is only available on cameras with storage capabilities.

On the home page, click **Photo**.



Item	Description
Refresh	Refresh the displayed content.
Export	Export the selected photos.
Delete	Delete the selected photos.
Export & Delete	Export the selected photos and delete them on the server.
Ascending Order	Arrange the items in chronological order.
Descending Order	Arrange the items in reverse chronological order.
Smart Server	Used to store smart snapshots.
Common Server	Used to store common snapshots.



NOTE!

To allocate photo capacity, go to **Setup > Storage > Storage**.

5 Setup

5.1 Local Parameters

Set local parameters for your PC, including smart, video, recording and snapshot.



NOTE!

The local parameters displayed may vary with camera model.

1. Go to **Setup > Common > Local Parameters**.

Smart

Intelligent Mark ☒ On ☐ Off

Target Mark ☒ Vehicle ☒ Non-Motor Vehicle ☒ Pedestrian

Object Metadata ☒ On ☐ Off

Font Size Small

Display Human Body Sn... ☒ On ☐ Off

Note: When enabled, snapshots of human body will show in live view page. Only effective when face detection is enabled.

Video

Display Mode Balanced

Protocol TCP

Recording and Snapshot

Recording Subsection By Time

Subsection Time (min) 30

When Storage Full ☒ Overwrite Recording ☐ Stop Recording

Total Capacity(GB) 10

Local Recording MP4

Files Folder C:\Users\d05019\WebPlugin_IPC\IPCUN\ Browse... Open

Save

2. Set local parameters as needed.

Item		Description
Smart	Intelligent Mark	This function shall be used with Cross Line Detection, Intrusion Detection, Error! Reference source not found. , Error! Reference source not found. , Error! Reference source not found. , and Error! Reference source not found. .
	Target Mark	When enabled, detection boxes will appear on the specified object type(s) on the live view page.
	Font Size	Set the font size of object attributes, including Large , Medium , and Small .
	Display Human Body Snapshot	When enabled, human body snapshots appear on the live view page. NOTE! Only effective when face detection is enabled.
Video	Display Mode	Set the display mode according to the network status, including Min. Delay , Balanced , and Fluent (from low delay to high delay). You may also customize the display mode as needed.
	Protocol	Set the protocol used to transmit media streams to be decoded by the PC, including TCP and UDP .
Recording and Snapshot	Recording	<ul style="list-style-type: none"> Subsection By Time: Length of each local recording file. For example, 2 minutes. Subsection By Size: Size of each local recording file. For example, 10MB.
	Subsection Time (min)/Subsection Size (MB)	<ul style="list-style-type: none"> Subsection Time (min): Available when Subsection By Time is selected. 1 to 60 minutes allowed. Subsection Size (MB): Available when Subsection By Size is selected. 10 to 1024MB allowed.
	When Storage Full	<ul style="list-style-type: none"> Overwrite Recording: When the local recording capacity is full, older recordings are overwritten automatically. Stop Recording: When the local recording capacity is full, recording stops automatically.
	Total Capacity (GB)	Allocate storage capacity for local recording. Range: 1 to 1024GB.
	Local Recording	Set the file format for saving local recordings, including TS and MP4 .

	Files Folder	<p>Set the location where snapshots and recordings are saved.</p> <ul style="list-style-type: none"> Click Browse... to select the storage location. Click Open to quickly open the folder. <p>NOTE!</p> <p>The maximum length of the directory is 260 bytes. If the limit is exceeded, recording or snapshot during live view will fail.</p>
--	--------------	--

- Click **Save**.

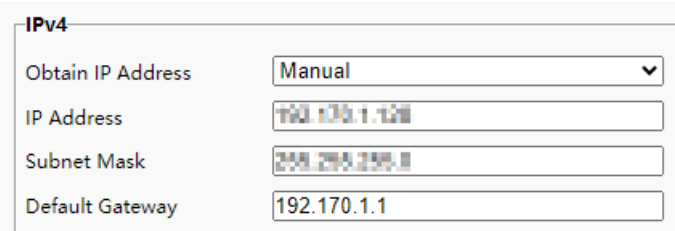
5.2 Network

5.2.1 Basic Config

Complete the basic network configuration so the camera can communicate with other devices on the network.

1. Ethernet

- Go to **Setup > Network > Basic Config**.
- Configure Ethernet parameters.
 - IPv4
 - Manual
 - Select **Manual** from the **Obtain IP Address** drop-down list.
 - Enter the IP address, subnet mask, and default gateway address. Make sure that the IP address of the camera is unique in the network.
 - Click **Save**.



The screenshot shows the 'IPv4' configuration window. It has a title bar 'IPv4'. Below it, there are four rows of configuration fields:

- 'Obtain IP Address' with a dropdown menu set to 'Manual'.
- 'IP Address' with a text box containing '192.170.1.128'.
- 'Subnet Mask' with a text box containing '255.255.255.0'.
- 'Default Gateway' with a text box containing '192.170.1.1'.

➤ PPPoE

Configure PPPoE to assign a dynamic IP address.

- Select **PPPoE** from the **Obtain IP Address** drop-down list.
- Enter the username and password provided by your ISP (Internet Service Provider).
- Click **Save**. The camera will be assigned an IP address.

➤ Obtain Automatically(DHCP)

DHCP (Dynamic Host Configuration Protocol) is enabled by default. If a DHCP server is deployed in the network, the camera can automatically obtain an IP address from the DHCP server.

- Select **Obtain Automatically(DHCP)** from the **Obtain IP Address** drop-down list.
- Complete the settings as shown below.

IPv4

Obtain IP Address: Obtain Automatically (DHCP)

IP Address: 192.170.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.170.1.1

- IPv6
 - Obtain Automatically(DHCP)

The default mode is **Obtain Automatically(DHCP)**. In this mode, the IP address is assigned by the DHCP server.

- Manual

IPv6

Mode: Manual

Address: 23:12:15:64:12:16:12:15

Prefix Length: 64

Default Gateway: 23:12:15:64:12:16:12:1

(1) Choose **Manual**.

(1) Enter the IPv6 address, prefix length and default gateway. Make sure that the IPv6 address is unique in the network.

3. Set the MTU value, port type and operating mode.

- MTU: Maximum transmission unit. Input an appropriate value. The greater the value, the higher the transmission efficiency, and the higher the delay.
- Port Type: The default type is **FE Port**.
- Operating Mode: The default is **Auto-negotiation**.

Basic

MTU: 1500

Port Type: FE Port

Operating Mode: Auto-negotiation

4. Click **Save**.

2. DDNS

DDNS (Dynamic Domain Name Server) can map the dynamic IP address of the camera to a fixed domain name and so users can access the camera using the easy-to-remember domain name.

1. Go to **Setup > Network > Basic Config > DDNS**.
2. Enable **DDNS Service**.

DDNS Service ☐ On ☒ Off

DDNS Type DynDNS

Server Address www.dyndns.com

Domain Name

Username

Password

Confirm

Save

3. Select the DDNS type.

- DynDNS/NO-IP: Third-party DDNS service provider. Enter the server address and domain name provided by your DDNS service provider.
- MyDDNS: Enter a domain name and then click **Test** to check its availability.

DDNS Service ☐ On ☒ Off

DDNS Type DynDNS

Server Address www.dyndns.com

Domain Name

Username

Password

Confirm

Save

4. Click **Save**.

3. Port

1. Go to **Setup > Network > Basic Config > Port**.

HTTP Port	80
HTTPS Port	443
RTSP Port	554

Note: Modifying the RTSP port number will cause the device to restart.

2. You can use the default ports. If a port entered has been used for other services, you need to change the port to avoid conflict.



CAUTION!

- If the HTTP port number you entered is being used by another service, a message indicating port conflict will appear. Ports 23, 81, 82, 85, 3260, and 49152 are reserved for other purposes and cannot be used.
- In addition to the above port numbers, the system can also dynamically detect other port numbers that are already in use.

- HTTP/HTTPS Port: If you change the HTTP/HTTPS port number, then you need to add the new port number after the IP address when logging in. For example, if the HTTP port number is set to 88, you need to use `http://192.168.1.13:88` to log in to the camera.
- RTSP Port: Real-Time Streaming Protocol port, enter an available port number.

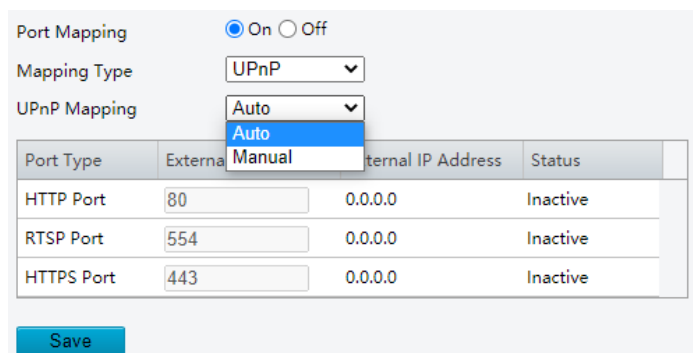
3. Click **Save**.

4. Port Mapping

Configure port mapping so users can access your camera on the LAN from the Internet.

1. Go to **Setup > Network > Port > Port Mapping**.
2. Enable **Port Mapping**.
3. Select the mapping type.

- UPnP

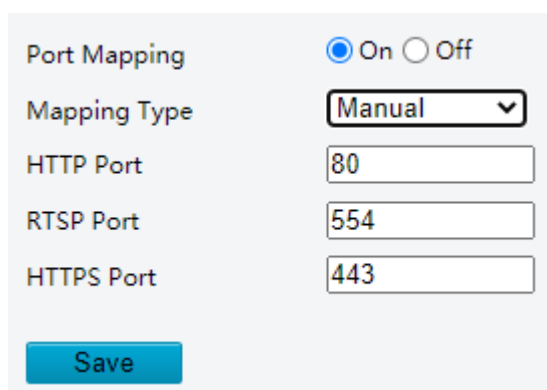


The screenshot shows the 'Port Mapping' configuration page. At the top, 'Port Mapping' is set to 'On' (radio button selected). Below it, 'Mapping Type' is set to 'UPnP' (dropdown menu). Under 'UPnP Mapping', a dropdown menu is open showing 'Auto' (selected) and 'Manual'. Below this is a table with columns: 'Port Type', 'External Port', 'Internal IP Address', and 'Status'. The table contains three rows: 'HTTP Port' with external port 80, 'RTSP Port' with external port 554, and 'HTTPS Port' with external port 443. All internal IP addresses are 0.0.0.0 and all statuses are 'Inactive'. A 'Save' button is at the bottom.

Port Type	External Port	Internal IP Address	Status
HTTP Port	80	0.0.0.0	Inactive
RTSP Port	554	0.0.0.0	Inactive
HTTPS Port	443	0.0.0.0	Inactive

- Auto: When enabled, the camera will negotiate external ports with the router automatically. Make sure UPnP is enabled on the router.
- Manual: In this mode, you need to enter external ports manually and make sure the ports entered are available; otherwise, port mapping does not take effect.

- Manual



The screenshot shows the 'Port Mapping' configuration page with 'Mapping Type' set to 'Manual'. The 'UPnP Mapping' dropdown is not visible. Below it are three input fields: 'HTTP Port' with value 80, 'RTSP Port' with value 554, and 'HTTPS Port' with value 443. A 'Save' button is at the bottom.

- If your router does not support UPnP, you need to set the external port numbers manually. Make sure the entered ports are available; otherwise, port mapping does not take effect.
- **Inactive** will be displayed in the **Status** column if the port number entered is already in use by another service.

4. Click **Save**.

5. 802.1x

802.1x enhances network security for your intranet by performing port-based authentication before allowing the device to access the LAN. Only successfully authenticated devices are allowed to access the LAN.

5. Go to **Setup > Network > Basic Config > 802.1x**.
6. Enable **802.1x**.
7. Choose a protocol type.

- EAP-MD5

802.1x	<input checked="" type="radio"/> On <input type="radio"/> Off
Protocol	EAP-MD5 ▼
EAPOL Version	1 ▼
Username	admin
Password
Confirm
Save	

- (1) Choose the EAPOL version according to the protocol version on the network switch.
- (2) Enter the device username and password, confirm the password.

- EAP-TLS

802.1x	<input checked="" type="radio"/> On <input type="radio"/> Off
Protocol	EAP-TLS ▼
EAPOL Version	1 ▼
Username	admin
Client Certificate	default ▼
CA Certificate	▼
Save	

- (1) Choose the EAPOL version according to the protocol version on the network switch.
- (2) Enter the device username.
- (3) Click ▼ to choose a client certificate and a CA certificate (see Certificate Management for details)



NOTE!

You must use an imported client certificate and a CA certificate for the camera to pass authentication. The camera cannot pass authentication with a self-signed certificate and a default certificate.

8. Click **Save**.

5.2.2 Service Configuration

1. Email

Configure E-mail so that the camera can e-mail an alarm message to the specified email addresses when an alarm occurs.

1. Go to **Setup > Network > Service Config > E-mail**.

Sender

Name

Address

SMTP Server

SMTP Port

TLS/SSL ☐ On ☒ Off

Snapshot Interval(s) ☒ Attach Image

Server Authentication ☒ On ☐ Off

Username

Password

Confirm

Recipient

Name1

Address1

Name2

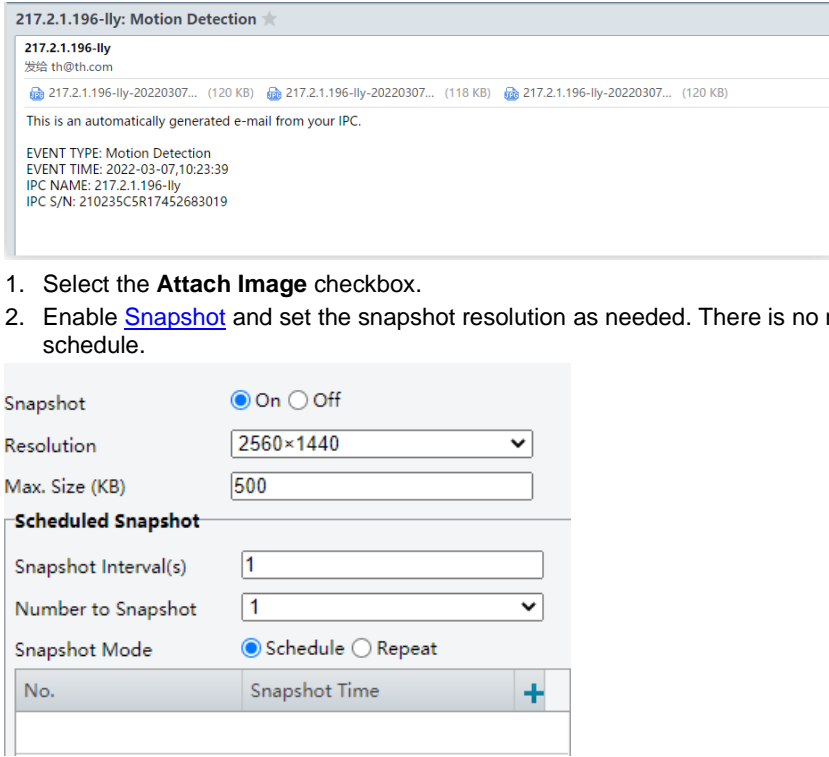
Address2

Name3

Address3

2. Set the sender and recipient information.

Item	Description
Sender Name	Enter the device name.
Sender Address	Enter the device IP.
SMTP Server/SMTP Port	Enter the IP address and port number of the sender's SMTP server. The default SMTP port number is 25.
TLS/SSL	When enabled, emails will be encrypted by TLS or SSL during transmission. NOTE! If SMTP supports TLS/SSL, it tries SSL first to establish a secure connection for email sending.
Snapshot Interval	Choose a snapshot interval: 2s, 3s, 4s, or 5s.

Item	Description
Attach Image	<p>When enabled, an alarm e-mail with attached snapshots (3 by default) taken at set interval will be sent after an alarm occurs. For some alarm types, only one snapshot will be taken and there is no need to set snapshot interval.</p>  <ol style="list-style-type: none"> 1. Select the Attach Image checkbox. 2. Enable Snapshot and set the snapshot resolution as needed. There is no need to set a snapshot schedule.
Server Authentication	Enable SMTP server authentication to secure e-mail transmission.
Username/Password	<p>Enter the username and password of the SMTP server.</p> <p>NOTE!</p> <ul style="list-style-type: none"> • The email only shows the sender name. Username will not be displayed. • The password allows special characters.
Recipient Name/Address	<ol style="list-style-type: none"> 1. Enter the recipient names and email addresses. 2. Click Test to test the email sending function.

3. Click **Save**.

Sender

Name

217.2.1.196.lly

Address

217.2.1.196

SMTP Server

217.2.1.8

SMTP Port

25

TLS/SSL

☐ On
☒ Off

Snapshot Interval(s)

2

☒ Attach Image

Server Authentication

☒ On
☐ Off

Username

th1@th.com

Password

Confirm

Recipient

Name1

th1@th.com

Address1

th1@th.com

Test

Name2

Address2

Test

Name3

Address3

Test

Save

2. SNMP

The Simple Network Management Protocol (SNMP) allows the camera to be remotely managed by a management server. The camera can be configured to support SNMP and send messages to the management server for important events or status changes.

1. Go to **Setup > Network > Service Config > SNMP**.

SNMP

☐ On
☒ Off

Save

2. Click **On** to enable **SNMP**.



NOTE!

On certain device models, SNMP is enabled after an upgrade to the latest version. It is normal.

3. Set SNMP parameters.

- SNMPv3



NOTE!

Before you enable SNMPv3, make sure SNMPv3 is supported both on your camera and the server.

SNMP	<input checked="" type="radio"/> On <input type="radio"/> Off
SNMP Type	SNMPv3
Username	admin
Authentication Mode	MD5
Password
Confirm
Encryption Mode	DES
Password
Confirm
Trap Community Name	private
Trap Server Address	0.0.0.0
Trap Port	162
SNMP Port	161

[Save](#)

Item	Description
SNMP Type	The default is SNMPv3 .
Password	Set an authentication password.
Confirm	Confirm the authentication password by entering it again.
Password	Set an encryption password.
Confirm	Confirm the encryption password by entering it again.
Trap Server Address	It is filled in automatically after you complete management server configuration.
SNMP Port	The default is 161. You may change it as needed.

- SNMPv2

SNMP	<input checked="" type="radio"/> On <input type="radio"/> Off
SNMP Type	SNMPv2
Read Community	public
Read/Write Community	private
Trap Community Name	private
Trap Server Address	0.0.0.0
Trap Port	162
SNMP Port	161

Save

Item	Description
SNMP Type	A message will appear to remind you of potential risks and prompt for your confirmation after you choose SNMPv2 . To choose SNMPv2 anyway, click OK to ignore the reminder.

Item	Description
Read Community	The default is public . You may change it as needed, but make sure you also change it on the server; otherwise, authentication will fail.
Trap Server Address	Go to Setup > Network > Platform Access > Management Server to configure the server address.
SNMP Port	The default is 161 . You may change it as needed.

4. Click **Save**.

3. QoS

QoS (Quality of Service) can alleviate network delays and network congestion by prioritizing different services.

1. Go to Setup > Network > Service Configuration > QoS.

2. Assign a priority level (0 to 63) for each service. The greater the value, the higher the priority. For example, the camera first ensures smooth audio and video in the case of network congestion.



NOTE!

The same QoS rules must also be configured on the router or network switch.

3. Click **Save**.

4. ANR (ONVIF)

If the network connection between the camera and the peer (stream receiving address) is disconnected, the camera can store videos according to the configured recording schedule; and after the network connection is restored, the camera can retransfer the video stored during the interruption period to the stream receiving address on the request of the peer.

5.2.3 Platform Access

1. Intelligent Platform

Configure intelligent platform to receive smart snapshots from the camera. A camera can be managed by two intelligent servers.

Local snapshot cannot be enabled when the number of subscriptions has reached the upper limit.

If local snapshot has been enabled, when the number of subscriptions reaches the upper limit, higher-priority subscriptions will take precedence, and local snapshot will be disabled.



NOTE!

- The number of subscriptions supported may vary with camera.
- Priority level of subscription from different platforms: Platform 1 > Platform 2 > LAPI subscription > WebSocket subscription.

- Video&Image Database
1. Go to **Setup > Network > Platform Access > Intelligent Platform**.
 2. Select the **Enable** checkbox.
 3. Choose **Video&Image Database** as the protocol.

☒ Enable

Protocol: Video&Image Database

Protocol Version: VIID_2017

Server IP: 0.0.0.0

Server Port: 5196

Device ID: 001

Username: admin

Platform Access Code:

Confirm Platform Access Code:

Coordinate Mode: Percentage Mode

Connection Mode: Short Connection

Report Data Type: ☒ Motor Vehicle ☒ Non-Motor Vehicle ☒ Person ☒ Face

Status: Offline

4. Configure the parameters.

Item	Description
Protocol Version	Choose the protocol version: VIID_2017 , VIID_2018 , VIID_2018 (multi-channel) . Note: When choosing VIID_2018 (multi-channel), you need to enter the video channel ID for each channel.
Server IP	Enter the IP address of the platform.
Server Port	Use the default 5196 .
Device ID	Input a valid ID according to the instructions and keep it the same on the platform. The ID shall comply with VIID protocol.
Username	Enter the username for authentication, which must be the same as that configured on the platform.
Platform Access Code	Enter the password for authentication, which must be the same as that configured on the platform.
Confirm Platform Access Code	Input the password again for confirmation.

Item	Description
Coordinate Mode	Used to position structured information on the image, which must be in the same format as that on the platform, Percentage Mode, Pixel Mode, or Normalized Mode.
Connection Mode	Use the default: Short Connection.
Report Data Type	Choose the type(s) of data to be sent to the intelligent platform: Motor Vehicle, Non-Motor Vehicle, Person, and Face.
Status	<ul style="list-style-type: none"> Offline: The camera is disconnected from the platform. Online: The camera is connected to the platform.

- FTP

1. Go to **Setup > Network > Platform Access > Intelligent Platform**.

1. Select the **Enable** checkbox.

2. Choose **FTP** as the protocol.

The screenshot shows a configuration interface for the Intelligent Platform. At the top, there is a checkbox labeled 'Enable' which is checked. Below it, the 'Protocol' is set to 'FTP' in a dropdown menu, and a 'Configure FTP' button is visible. The 'Status' is displayed as 'Online'.

3. Click **Configure FTP**. A page as shown below appears.

The screenshot shows the 'Configure FTP' dialog box. It has a title bar with a close button. The main area is divided into two sections. The top section, 'Server Parameters', contains fields for 'Server IP' (0.0.0.0), 'Port No.' (21), 'Username', 'Password', and 'Confirm'. There are also checkboxes for 'Upload Images' (checked) and 'Custom Naming Rules' (unchecked), and a 'Test' button. The bottom section, 'Save To:', has a 'File Path' and 'File Name' tab. Below this is a table with 6 rows, each with a 'No.' and a 'Naming Element' dropdown menu, all set to 'Disable'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

4. Set server parameters.

Item	Description
Server IP	Enter the IP address of the FTP server.
Port No.	Use the default 21.
Username	Enter the username used for accessing the FTP server.
Password	Enter the password used for accessing the FTP server.

Item	Description
Test	Click to test the connection to the FTP server.
Upload Images	<p>Select the checkbox to enable uploading smart snapshots.</p> <p>Overwrite Storage: After the number of photos in the lowest-level folder reaches the set threshold, new photos will overwrite older photos in the folder. For example, the storage path is “\IP\date,” the lowest-level folder is the level-2 folder named “date”. When the number of photos unloaded on Jan. 4, 2022, reaches 1000 (default value), new photos overwrite old photos in the 20220104 folder.</p> <p>NOTE!</p> <ul style="list-style-type: none"> To choose Overwrite Storage, make sure the last naming element of the files is the image sequence number. Overwrite At (image): The default is 1,000, up to 100,000 is allowed.
Custom Naming Rule	Select the checkbox, and then you can customize the file naming rules as needed. For the naming rules, see File Path in step 6.
Covert Path into UTF8	Select the checkbox, and the path will be converted into UTF8 format.

5. Configure the image storage path.

Item	Description
File Path	Six levels are allowed. If not set, the default path “\IP\Date\Intelligent” will be used, where “Intelligent” means smart snapshots.
File Name	<p>Naming element: Up to 20 fields are allowed. If not set, sequence numbers will be used as file names, for example, “1, 2, 3”, etc.</p> <p>Naming rule: Format string: prefix <(front string) front length % > suffix.</p>

6. Click **Save**.

2. **P2P**

Add the camera to cloud so you can access the camera anytime, anywhere from your mobile phone for live view, playback, camera configuration, etc.



NOTE!

- You can add the camera to cloud using app or through the cloud website.
- Guard Viewer and Guard Live are free apps that can be downloaded from app stores, including iOS and Android versions. You need to download and install the app on your mobile phone in order to access your camera from your mobile phone. The following takes Guard Viewer as an example to describe the operations.
- You can add the camera to cloud with or without a cloud account. A cloud account is required if you want full functionalities on the app. Some functions, such as cloud upgrade, will not be available if the camera is added to cloud without a cloud account.

1. Go to **Setup > Network > Platform Access > P2P**.

P2P	<input checked="" type="radio"/> On <input type="radio"/> Off
Server Address	www.star4live.com
Register Code	[Blurred text]
Device Status	Network disconnected. Please che
Add Without Signup	<input checked="" type="radio"/> On <input type="radio"/> Off No account is need
Scan QR Code	

2. Check that P2P is enabled.

- Add the camera to cloud with a cloud account.

Open the app, log in to your cloud account, and use the app to scan the QR code displayed on the **P2P** page to add the camera to cloud.

- Add the camera to cloud without a cloud account.

Open the app, use the Add Without Signup function to add the camera to cloud. The system will bind the camera to your mobile phone so you can view live and recorded video and receive alarm notifications on your mobile phone.




NOTE!

You must enable **Add Without Signup** on the **P2P** page on the camera's web interface first.

1. Open Guard Viewer and tap **Try Now**. The **Live View** page appears.



NOTE!

If you have already installed Guard Viewer on your phone, open it, and then go to  > **Devices** > **Add** > **Add Without Signup**.

2. Tap **Add** > **Add Without Signup**.

3. Scan the QR code displayed on the **P2P** page of the camera's web interface.

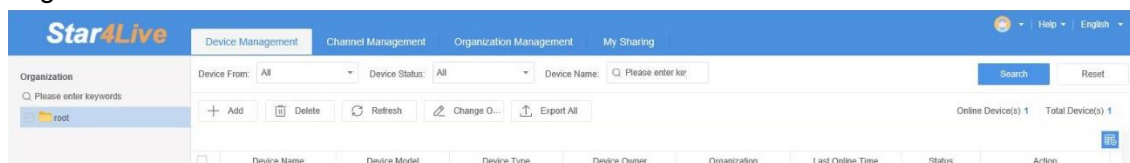
4. Enter the device password and tap **Login** to add the camera to cloud.

- Add cameras on the P2P website.

1. Visit www.os.star4live.com using a web browser.

2. On the login page, click **Sign Up** and follow on-screen instructions to create an account.

3. Log in to the website.



4. Go to **Device Management** > **My Cloud Devices** and click **Add**.

Add device
✕

[Add Device by Register Code](#)

Option 1: Log in to the Web of the device, and then click Network > P2P.

Option 2: You can also find the register code on the device body.

Item	Description
Device Name	Enter the device name.
Register Code	Enter the register code.
Organization	Select an organization for your camera. By default, the root organization is selected. You may add or delete organizations under Organization Management > My Cloud Organizations .

5. Click **OK**.
6. Click **Save**.
7. Check whether the camera is online.
 - Cloud website: Go to **Device Management > My Cloud Devices**.
 - Camera's web interface: Go to **Setup > Network > P2P**.

3. WebSocket

WebSocket can connect your camera to a third-party platform and enable remote management of the camera from the third-party platform, including viewing device version and capabilities, control PTZ, and receive alarms.

1. Go to **Setup > Network > Platform Access > WebSocket**.

WebSocket
☐ On ☒ Off

Destination IP

Destination Port

Device ID

Authentication Key

Confirm Authentication Key

Online Status
Offline

2. Set the parameters.

Item	Description
WebSocket	Select to enable or disable WebSocket.
Destination IP	Enter the IP address of the third-party platform.

Destination Port	Enter the listener port of the third-party platform.
Device ID	The default device ID is the device's serial number. You can set a device ID as needed.
Authentication Key	Enter the authentication key used to connect the camera to the third-party platform. Make sure the authentication keys configured on the camera and the third-party platform are the same. NOTE! If you first choose not to enable Authentication Key and then enable it after the camera is connected to the platform, authentication does not take effect immediately; it will take effect when the next time the camera is successfully connected to the platform.
Confirm Authentication Key	Confirm the authentication key by entering it again.
Online Status	Check whether the device is successfully connected to the third-party platform.

3. Click **Save**.

5.3 Video & Audio

For dual-channel devices, you can set video and audio parameters for the channels separately.

5.3.1 Video

1. Video

1. Go to **Setup > Video & Audio > Video**.

2. Select a capture mode for your camera.

The **Extended Encoding** function is available only when the capture mode is greater than 8MP.

After you change the capture mode, the encoding settings will be reset to defaults and some models of cameras will restart.

3. Set stream parameters.

The streams are independent of each other and can be set with different resolutions, frame rates, video compression formats, etc. Only the main stream supports full resolution.



NOTE!

- The fourth and fifth streams are only available on certain models.
- Before configuring the fifth stream, you need to enable the fourth stream first.

☒ **Enable Fourth Stream**

Item	Description
Video Compression	<p>Select a video compression standard for your camera: H.265, H.264 or MJPEG.</p> <p>NOTE!</p> <ul style="list-style-type: none"> • When H.265 or H.264 is selected, Image Quality is not available; When MJPEG is selected, Bit Rate, I Frame Interval, Smoothing, SVC and Smart Encoding are not available. • The bit rate restores to the default when you switch between H.264 and H.265.
Resolution	Select a video resolution for your camera. The higher the resolution, the clearer the image.
Frame Rate(fps)	<p>Select the frame rate.</p> <p>NOTE!</p> <p>To ensure image quality, the frame rate shall not be greater than the reciprocal of the shutter speed.</p>
Bit Rate(Kbps)	<p>Set the bit rate. Range: 128 to 16384.</p> <p>NOTE!</p> <p>The bit rate range may vary with device model.</p>
Bitrate Type	<p>Select the bitrate type.</p> <ul style="list-style-type: none"> • CBR: The camera keeps a specific bit rate by varying the quality of video streams. • VBR: The camera keeps the quality of video streams as constant as possible by varying the bit rate.
Image Quality	<p>Configurable when Bitrate Type is set to VBR.</p> <p>The closer the slider is to Quality, the higher the bit rate, and the higher the image quality.</p> <p>The closer the slider is to Bit Rate, the lower the bit rate, and the image quality will be affected.</p>
I Frame Interval	Set the number of frames between I-frames. A shorter interval presents better image quality but consumes more bandwidth and storage.
GOP	Group of Pictures, defines the basic pattern of the video stream encoded with I and P frames.
Smoothing	<p>Set the smoothness of the video stream. Drag the slider to choose whether smoothness or clarity takes precedence.</p> <p>NOTE!</p> <p>Smoothing is recommended for fluent video in a poor network environment.</p>
SVC	SVC (Scalable Video Coding) enables a video stream to be broken into multiple layers of resolution, quality, and frame rate, reducing bandwidth consumption without compromising the image quality.
Smart Encoding	<p>Select a mode.</p> <ul style="list-style-type: none"> • Basic Mode: Reduces the bit rate by about 25%. • Advanced Mode: Reduces the bit rate by about 50%.

4. Set the BNC output format, **PAL**, or **NTSC**.

5. Click **Save**.

2. Adaptive Streams

The bit rate of the media stream is automatically adjusted according to the network conditions.



NOTE!

- This function is only available on certain models.
- This function is enabled by default on certain models.
- It is recommended to enable Adaptive Streams in a poor network environment.
- To enable adaptive streams, you need to choose the TCP protocol at **Setup > Commons > Local Parameters**; otherwise, adaptive streams cannot be enabled.

1. Go to **Setup > Video & Audio > Video > Adaptive Streams**.

2. Enable **Adaptive Streams**.
3. Click **Save**.

5.3.2 Snapshot

Configure basic snapshot parameters and scheduled snapshot.

1. Go to **Setup > Video & Audio > Snapshot**.



NOTE!

- For dual-channel devices, you can set snapshot parameters for the channels separately.
- When you configure e-mail and FTP, you only need to enable Snapshot and set the resolution and maximum size; it is unnecessary to configure the scheduled snapshot.

2. Enable **Snapshot**, set the resolution and maximum size of snapshots.
3. Set the snapshot mode.
 - **Schedule**: Set a snapshot time. For example, with **Snapshot Interval** set to 20s, **Number to Snapshot** set to 3, and snapshot time set to 16:00:00, the camera will take a snapshot at 16:00:00, 16:00:20 and 16:00:40. You can click **+** to add a snapshot time by choosing from the list or by adjusting based on a listed time.

To delete a snapshot time, click .

- Repeat: Set a snapshot interval. For example, with snapshot plan set to 16:00:00 to 20:00:00 on Monday, **Repeat Interval** set to 120s, **Snapshot Interval** set to 20s, and **Number to Snapshot** set to 2, the camera will take a snapshot at 16:00:00, 16:00:20, 16:02:00 and 16:02:20.

- a Select **Repeat** and set the repeat interval. A valid repeat interval is an integer within the range of 1 to 86400. The snapshot interval * number of snapshots to take cannot be greater than the interval (**Snapshot Interval** * **Number of Snapshot** cannot be greater than **Interval**).

- b Select the **Enable Snapshot Plan** checkbox and set the snapshot plan. See [Arming Schedule](#) for details. A 24/7 snapshot plan is enabled by default.



NOTE!

- The time periods cannot overlap.
- Up to 4 time periods are allowed.

4. Set the snapshot interval (unit: second) and number to snapshot (1, 2, or 3). For example, if the interval is set to 1s and the number to snapshot is set to 2, the camera will take 2 snapshots (take one first and then take another after 1 second).
5. Click **Save**.

5.3.3 Audio

1. Audio

1. Go to **Setup > Video & Audio > Audio**.

Audio Input

Audio Input

☐ On
☒ Off

Access Mode

Line/Mic

Input Volume

50

Audio Compression

G.711A

Sampling Rate(KHz)

16

Noise Suppression

☒ On
☐ Off

Channel 1

Mic

☒ Enable

Channel 2

Line

☐ Enable

Audio Output

Audio Output

Speaker

Output Volume

95

Save

2. Set audio input parameters.

Item	Description
Audio Input	Enable/disable audio input. NOTE! If audio is not needed, it is recommended to turn it off to improve camera performance.
Access Mode	Choose the audio input mode; Line/Mic or RS485 . NOTE! This function is not available on dual-channel cameras.
Input Volume	Drag the slider or input a value to set the input volume.
Audio Compression	Choose the audio compression format: G.711U or G.711A .
Sampling Rate(KHz)	Choose a sampling rate, 8KHz or 16KHz. The higher the sampling rate, the better the sound quality.
Noise Suppression	This function is enabled by default. It can reduce noises and improve audio output quality.
Channel 1/Channel 2	Select the Enable checkbox to enable audio input for Channel 1 or Channel 2 (if available). Only one channel can be enabled. Channel 1 supports Mic (default) and Line . Channel 2 is available on certain models only.

3. Set audio output parameters.

Item	Description
Audio Output	Choose an audio output mode, Line or Speaker . <ul style="list-style-type: none"> Line: A speaker or an earphone needs to be connected. Speaker: Default mode.
Output Volume	Set the output volume using the slider.

4. Click **Save**.

2. Audio File

1. Go to **Setup > Video & Audio > Audio**.

Alarm Volume

Alarm Audio File

Note: PCM or MP3 files, each no more than 200K.

No.	Audio	Operation
1	You are in the alert area! Please leave!	
2	You are in the danger zone! Do not approach!	
3	Please be aware! You are in the monitored area!	
4	No parking! Please leave!	
5	Important place! Please leave!	
6	Private area! Do not enter!	
7	Danger! Deep water!	
8	Danger! Do not climb!	
9	Welcome!	
10	Warning!	
11	The area is crowded! Please leave!	
12	Please stop! No more people allowed!	
13	Please wear a mask to prevent infection!	

2. Set audio file parameters.

Item	Description
Alarm Volume	Drag the slider or input a value to set alarm volume.
Alarm Audio File	<p>Click Browse... to import audio files.</p> <ul style="list-style-type: none">• To play an audio file, click .• To edit audio contents, click .• To delete an audio, click . <p>NOTE!</p> <ul style="list-style-type: none">• This function is available only on certain models. Up to 5 audio files are allowed.• Built-in audio files may vary depending on the smart functions supported by the device.• Certain models without smart functions provide built-in alarm audios and support user-imported audios.

3. Click **Save**.


5.3.4 ROI

Region of Interest (ROI) ensures image quality of specified areas on the image at low bit rate.

1. Go to **Setup > Video & Audio > ROI**.



2. Set ROI areas.

- (1) Click  to add a ROI area. The area is a rectangle by default. Up to 8 areas are allowed.





- (2) Adjust the position and size of the area or draw an area as needed.

- Adjust the position and size of the area.
 - Point to a border of the area and drag it to the desired position.
 - Point to a handle of the area and drag to resize it.
- Draw an area.

Click on the image and drag to draw an area.



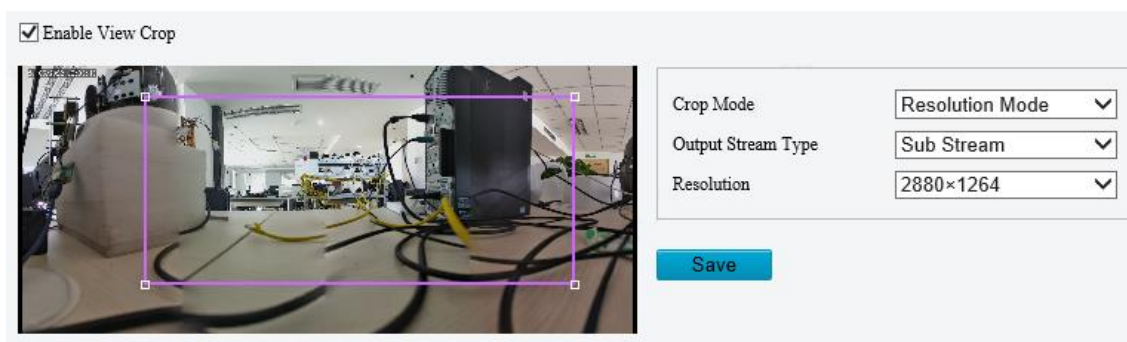
NOTE!

When setting the ROI, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after finishing setting the ROI.

5.3.5 View Cropping

You can crop the live video to keep only the area of interest and transmit the cropped video by sub or third stream to save bandwidth and storage.

1. Go to **Setup > Video & Audio > View Crop**.
2. Select the **Enable View Crop** checkbox. A rectangular appears on the image. You may drag to resize or relocate the rectangular on the image.



3. Choose a cropping mode.
 - **Field of View Mode:** The camera ensures the size of the specified area. Choose a stream type, set the cropping size and resolution.

Crop Mode	Field of View Mode ▼
Output Stream Type	Sub Stream ▼
Crop Size	20:9 ▼
Resolution	2880×1264 ▼

- **Resolution Mode:** The camera ensures the resolution of the specified area first. Choose a stream type, set the resolution.

Crop Mode	Resolution Mode ▼
Output Stream Type	Sub Stream ▼
Resolution	2880×1264 ▼

4. Click **Save**. The live and recorded video only shows the specified area (rectangular) of the image.

5.3.6 Media Stream

1. Media Stream

You can configure a media stream for your camera so that media contents from the camera such as audio and video can be transmitted over the network and played immediately on a third-party client rather than being downloaded first.

1. Go to **Setup > Video & Audio > Media Stream**.

Stream Profile	Protocol	Destination IP	Destination Port	Persistent	Status	+
----------------	----------	----------------	------------------	------------	--------	---

2. Click **+** to add a media stream.
3. Complete the media stream settings.

Item	Description
Stream Profile	Select a stream type for the camera to transmit media contents to a third-party client.
Destination IP	Enter the IP address of the device receiving media streams.

Item	Description
Protocol	The camera transmits data to a third-party client through the specific protocol. The default protocol is RTMP.
Persistent	Set whether to automatically establish the configured media stream after the camera restarts.

- Click **OK**.

2. RTSP Multicast

RTSP multicast allows third-party players to request RTSP multicast media streams from the camera through the RTSP protocol.

- Go to **Setup > Video & Audio > Media Stream > RTSP Multicast Address**.

The screenshot shows a web interface for configuring RTSP Multicast. It is divided into three sections: 'Main Stream', 'Sub Stream', and 'Third Stream'. Each section contains two input fields: 'Multicast Address' and 'Port'. The 'Multicast Address' field has a default value of '0.0.0.0' and the 'Port' field has a default value of '0'. At the bottom of the form is a blue button labeled 'Save'.

- Set the multicast address and port number (multicast address range: 224.0.1.0 to 239.255.255.255, port number range: 0 to 65535).
- Click **Save**.

5.4 Image

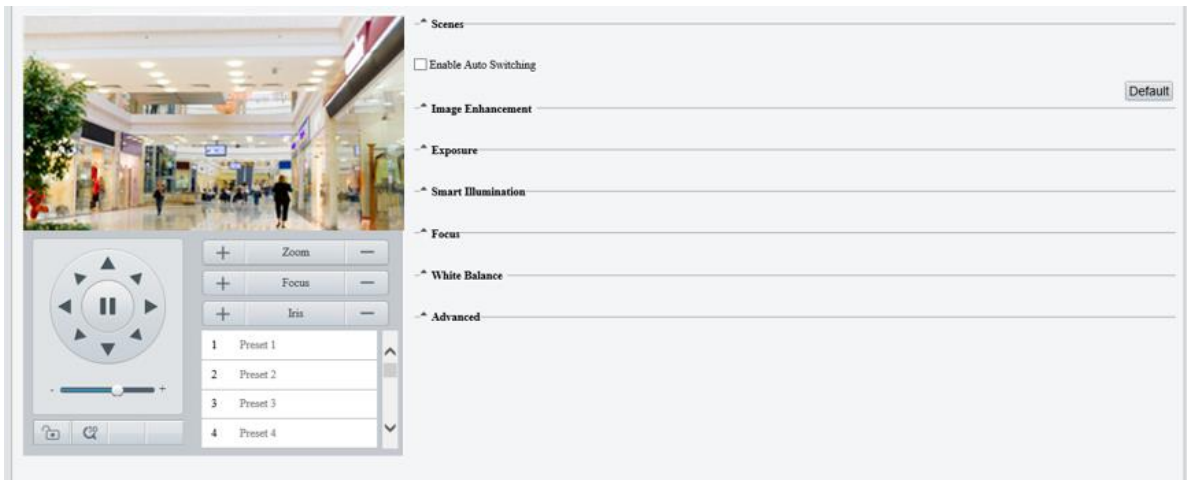
5.4.1 Image

For dual-channel devices, you can set image parameters for the two channels separately.

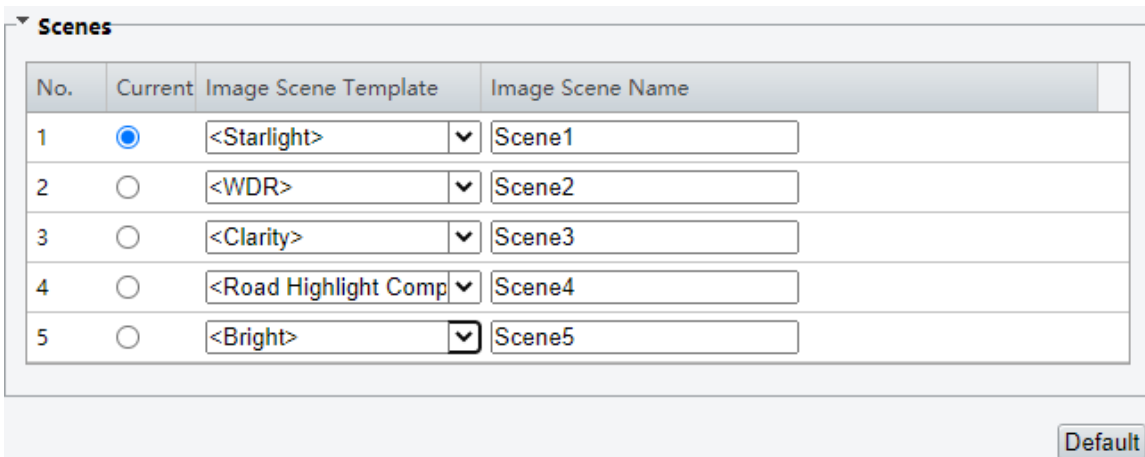
1. Scenes

A scene is a collection of image parameters preset in the camera for users to choose according to the actual scene.

- Go to **Setup > Image > Image**.



2. Click **Scenes**.



3. Set the parameters.







Item	Description
Current	Shows the scene that is currently in use. NOTE! To apply a scene, click the corresponding radio button in the Current column. The scene is selected as the current scene, and the corresponding image parameters apply automatically.
Image Scene Template	The camera provides multiple scenes for you to choose according to the actual scene. After you select a scene, the corresponding image settings apply automatically (you may also fine-tune image settings as needed). <ul style="list-style-type: none"> Common: For outdoor scenes. Indoor: For indoor scenes. Road Highlight Compensation/Park Highlight Compensation: For capturing license plates in roads, parks, etc. WDR: For high-contrast situations. Custom: For customizing a scene. Test: For testing. Standard: For common scenes, indoor and outdoor. Vivid: Provides extra saturation based on the Standard scene. Bright: Provides extra brightness based on the Standard scene. Starlight: For lowlight environments. Face: For capturing faces in motion in complicated scenes. Person And Vehicle: For monitoring motor vehicles, non-motor vehicles, and pedestrians in road scenes. Intrusion Prevention: For perimeter protection scenes.
Image Scene Name	Choose scene names corresponding to the scene templates. The scene names will be used in image scene switching (see Error! Reference source not found.).









2. Image Enhancement

1. On the **Image** page, click **Image Enhancement**.



2. Set the image enhancement parameters.

Item	Description	
Brightness	The overall lightness or darkness of the image.	
		
	Low brightness	High brightness
Saturation	The intensity or vividness of colors in the image.	
		
	Low saturation	High saturation
Contrast	The difference between the lightest and darkest tones in the image.	
		
	Low contrast	High contrast

Item	Description
Sharpness	<p>The definition of edges in the image.</p> <div>   </div> <div> <p>Low sharpness</p> <p>High sharpness</p> </div>
2D Noise Reduction	Reduce noise by individually analyzing each frame, which may cause image blur.
3D Noise Reduction	Reduce noise by analyzing the difference between successive frames, which may cause image smearing or ghosting.
Image Rotation	<p>The rotation of the image.</p> <div>   </div> <div> <p>Normal</p> <p>Flip vertical</p> </div> <div>   </div> <div> <p>Flip horizontal</p> <p>180°</p> </div> <div>   </div> <div> <p>90° clockwise</p> <p>90° anti-clockwise</p> </div>

To restore defaults, click **Default**.

3. Exposure



NOTE!

- The exposure settings may vary with device model.
- The default settings are scene-adaptive. Use default settings unless modification is necessary.

1. On the **Image** page, click **Exposure**.

The screenshot shows the 'Exposure' settings panel. It includes a list of parameters on the left and their corresponding controls on the right. The controls include dropdown menus, sliders, and radio buttons. The 'Exposure Mode' is set to 'Automatic', 'Shutter(s)' to '1/100', 'Gain' to '0', 'Slow Shutter' is 'On', 'Slowest Shutter' to '1/12', 'Compensation' to '0', 'Linear Stripe Suppression' to '5', 'Metering Control' to 'Center-Weighted Average Metering', 'Day/Night Mode' is 'Automatic', 'Day/Night Sensitivity' to 'Ultra-low', 'Day/Night Switching(s)' to '3', 'WDR' is 'Off', 'WDR Level' to '5', 'Suppress WDR Stripes' is 'Off', 'WDR On Sensitivity' to '5', and 'WDR Off Sensitivity' to '5'.

2. Set the exposure parameters.

Item	Description
Exposure Mode	<p>Select the exposure mode.</p> <ul style="list-style-type: none"> Automatic: The camera automatically sets the optimum shutter speed according to the scene. Custom: User can set exposure parameters as needed. Shutter Priority: The camera adjusts shutter as priority to adjust the image quality. Iris Priority: The camera adjusts iris as priority to adjust the image quality. Indoor 50Hz: Reduce stripes by adjusting the exposure time. <p>NOTE!</p> <ul style="list-style-type: none"> Stripe effect: The high-contrast condition in an image caused by uneven light energy received by the sensor. Using this mode in brighter environments aids in adjusting the stripe effect in the image with linear stripe suppression. Indoor 60Hz: Reduce stripes by adjusting the exposure time. <p>NOTE!</p> <p>Using this mode in brighter environments aids in adjusting the stripe effect in the image with linear stripe suppression.</p> <ul style="list-style-type: none"> Manual: Fine-tune image quality by setting shutter, gain and iris manually. Low Motion Blur: Control the minimum shutter to reduce motion blur in faces captured in motion.
Shutter(s)	<p>Shutter is used to control the light that comes into the lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly.</p> <p>NOTE!</p> <ul style="list-style-type: none"> This parameter is configurable when Exposure Mode is set to Manual, Shutter Priority, or Custom. If Slow Shutter is disabled, the reciprocal of the shutter speed must be greater than the frame rate.

Item	Description
Gain	<p>Control image signals so that the camera can output standard video signals in different light conditions.</p> <p>NOTE!</p> <p>This parameter is configurable when Exposure Mode is set to Manual or Custom.</p>
Slow Shutter	<p>Increase image brightness in low light conditions.</p> <p>NOTE!</p> <p>This parameter is configurable when Exposure Mode is not set to Iris Priority and Image Stabilization is disabled.</p>
Slowest Shutter	<p>Set the slowest shutter speed for exposure.</p>
Compensation	<p>Adjust the compensation value as required to achieve the desired image effect.</p> <p>NOTE!</p> <p>This parameter is configurable when Exposure Mode is not set to Manual.</p>
Linear Stripe Suppression	<p>Adjust the linear stripes in the image.</p> <p>Range: 1 to 9, the default is 5. The greater the value, the more obvious the linear stripe suppression effect is, but it may cause overexposure in the image. Please configure this according to the actual scene.</p> <p>NOTE!</p> <p>This parameter is configurable when Exposure Mode is set to Indoor 50Hz or Indoor 60Hz.</p>
Restore Auto Exposure(min)	<p>Set the duration for the camera to restore automatic exposure mode.</p>
Metering Control	<p>Perform luminance statistics on the images captured by the device, automatically adjust the exposure value, and output properly exposed images with optimal brightness. The default is the Center-Weighted Average Metering, you may configure this according to the actual scene.</p> <ul style="list-style-type: none"> Center-Weighted Average Metering: Measure light primarily in the central part of the image. Evaluative Metering: Measure light in the specified area of the image, suitable for scenes where the target and the background contrast widely. Spot Metering: Measure light in a small spot, smaller than evaluative metering, with more accurate light control. If used in brighter areas, the metered area will be properly exposed but darken other areas. If used in darker areas, the metered area will be properly exposed (unable to increase the brightness of the spot) and brighten other areas. Face Metering: Adjust image quality in poor lighting or back lighting conditions by controlling the brightness of captured faces in face scenes. <p>NOTE!</p> <p>This parameter is configurable when Exposure Mode is not set to Manual.</p>
Day/Night Mode	<ul style="list-style-type: none"> Automatic: The camera automatically switches between day mode and night mode according to the ambient lighting condition to output optimum images. Day: The camera outputs high-quality images in daylight conditions. Night: The camera outputs high-quality images in low-light conditions. Input Boolean: The camera switches between day mode and night mode according to the Boolean value input from a connected third-party device. <p>NOTE!</p> <p>The Input Boolean option is only available on certain models.</p>
Day/Night Sensitivity	<p>Light threshold for switching between day mode and night mode. A higher sensitivity value means that the camera is more sensitive to the change of light and is therefore more easily switched between day mode and night mode.</p> <p>NOTE!</p> <p>This parameter is configurable when Day/Night Mode is set to Automatic.</p>
Day/Night Switching(s)	<p>Set the length of time before the camera switches between day mode and night mode after the switching conditions are met.</p> <p>NOTE!</p> <p>This parameter is configurable when Day/Night Mode is set to Automatic.</p>

Item	Description
WDR	<p>Suitable for high-contrast scenes. WDR can balance the brightness in the bright area and dark area and provide clear image with more details.</p> <ul style="list-style-type: none"> On/Off: User needs to identify WDR scenes, and manually enable or disable WDR as needed. Smart/Automatic: The device can automatically identify typical WDR scenes, and then enable or disable WDR. <p>Note: When WDR is enabled, some other functions may not be supported. Please refer to the actual interface.</p>
WDR Level	<p>Adjust the WDR level.</p> <p>NOTE! Level 7 or higher is recommended if there is a high contrast between the bright and dark areas in the scene. In the case of low contrast, it is recommended to disable WDR or use level 1 to 6.</p>
WDR On/Off Sensitivity	When WDR is set to Automatic , adjust the parameter to change the WDR switching sensitivity.
Suppress WDR Stripes	Suppress the stripes in the image caused by the flickering light in WDR mode. When enabled, the camera automatically adjusts the shutter and frequency to minimize stripes.

To restore defaults, click **Default**.

4. Smart Illumination

1. On the **Image** page, click **Smart Illumination**.

2. Enable **Smart Illumination**.
3. Set the smart illumination parameters.

Item	Description
Illumination Mode	<ul style="list-style-type: none"> Infrared: The camera uses infrared light illumination. White Light /Smart White Light: The camera uses white light illumination. Warm Light: The camera uses warm light illumination. Laser: The camera uses laser light illumination. <p>NOTE!</p> <ul style="list-style-type: none"> Before you select Warm Light, please set the Port Mode to Illumination (go to Setup > System > Ports & Devices > Serial Port). This parameter is configurable when Control Mode is set to Custom Level. Range: 0 to 100. 0 is the weakest, 100 is the strongest. When Smart Illumination is enabled and illumination mode is set to Smart White Light: <ul style="list-style-type: none"> ➢ Alarm-trigger enabled: when an alarm is triggered, during the daytime, the white light blinks; at night, the white light is on steadily, otherwise, the white light is on faintly. ➢ Alarm-trigger N/A or disabled: when an alarm is triggered, during the daytime, the white light is off; at night, the white light is on steadily, otherwise, the white light is on faintly.
Control Mode	<ul style="list-style-type: none"> Global Mode: The camera automatically adjusts illumination and exposure to achieve a balanced image effect. Some areas might be overexposed if you select this option. This option is recommended if you focus on the monitoring range and image brightness.

Item	Description
	<ul style="list-style-type: none"> • Overexposure Restrain: The camera automatically adjusts illumination and exposure to avoid regional overexposure. Some areas might be dark if you select this option. This option is recommended if you focus on the clarity of the monitoring center area. • Road: This mode offers a strong overall illumination and is recommended for monitoring wide-range scenes, for example, road. • Park: This mode offers uniform illumination and is recommended for monitoring small-range scenes with many obstacles, for example, park. • Custom Level: This mode allows you to manually control the intensity of illumination. • Custom Level(Always On): In this mode, the illumination is always on.
Illumination Level	<p>Set the intensity of the illuminator. The greater the value, the higher the intensity. 0 is off.</p> <ul style="list-style-type: none"> • Near-illumination Level: Recommended for near focus scenes. • Mid-illumination Level: Recommended for medium distance focus scenes. • Far-illumination Level: Recommended for far focus scenes. <p>NOTE! This parameter is configurable when Control Mode is set to Custom Level.</p>

To restore defaults, click **Default**.

5. Focus

1. On the **Image** page, click **Focus**.

▼ Focus

Focus Mode

One-Click Focus ▼

Scene

Normal ▼

Zoom Speed

1 ▼

Min. Focus Distance(cm)

10 ▼

Max. Zoom Ratio

40 ▼

2. Set the focus parameters.

Item	Description
Focus Mode	<ul style="list-style-type: none"> • Auto Focus: Automatic focus control based on the current light conditions. • Manual Focus: Manual focus control. • One-Click Focus: Automatic focus in the event of rotation, zoom, and preset call. • One-Click Focus (IR): Recommended for low light scenes. • One-click Focus (Locked): Recommended for road highlight scenes.
Scene	<ul style="list-style-type: none"> • Normal: Common monitoring scenes such as road, park, etc. • Long Distance: Long-distance monitoring scenes
Zoom Speed	<ul style="list-style-type: none"> • 1: Low zoom speed. Recommended for common scenes. • 2: High zoom speed. Recommended when Quick Focus is enabled.
Min. Focus Distance	Select the minimum focus distance.
Max. Zoom Ratio	Choose an upper limit for digital zoom: 22, 44, 88, 176, or 352 .

3. To restore the default settings, click **Default**.

6. White Balance

White balance is used to eliminate unnatural color casts in images under different color temperatures for optimal color reproduction.

1. On the **Image** page, click **White Balance**.



White Balance

White Balance: Auto

Red Offset: 9

Blue Offset: 7

2. Set the white balance parameters.

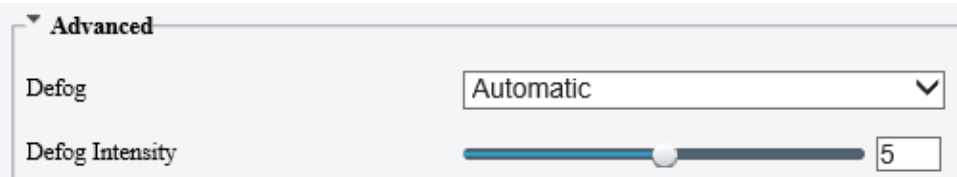
Item	Description
White Balance	<p>Adjust the red and blue gains of the image to remove unrealistic color casts.</p> <ul style="list-style-type: none">• Auto/Auto 2: Automatically adjust the red and blue gains according to the lighting conditions. If there are still color casts in Auto mode, try Auto 2 mode.• Fine Tune: Manually adjust the red and blue offsets.• Sodium Lamp: Automatically adjust the red and blue gains for optimal color reproduction in sodium light sources.• Outdoor: Recommended for outdoor scenes where the color temperature varies widely.• Locked: Keep the current color temperature.
Red/Blue Offset	<p>Set the red/blue offset.</p> <p>NOTE!</p> <p>This parameter is configurable when White Balance is set to Fine Tune.</p>

To restore defaults, click **Default**.

7. Defog

Defog is used to improve image visibility in foggy, hazy, and other low-visibility scenes.

1. On the **Image** page, click **Advanced**.



Advanced

Defog: Automatic

Defog Intensity: 5



NOTE!

This function is only available when WDR is disabled.

2. Set the defog parameters.

Item	Description
Defog	<p>Select the defog mode, including Automatic, On, and Off.</p> <p>In Automatic mode, the camera automatically adjusts the defog intensity according to the fog concentration for clear images.</p>
Defog Intensity	<p>Adjust the defog intensity.</p> <p>In a heavy-fog environment, the higher the defog level, the clearer the image; in a fog-free or light-fog environment, there is not much difference between levels 1 to 9.</p>

Item	Description
	<p>NOTE!</p> <ul style="list-style-type: none"> Optical defog is available on certain models. To enable optical defog, select On and set the defog intensity to 6 or higher, or select Automatic. Optical defog is automatically turned on in thick fog, and the image changes from color to black and white.

To restore defaults, click **Default**.

5.4.2 OSD

On Screen Display (OSD) are characters displayed with video images, for example, camera name, date, and time.



NOTE!

- This function may vary with device model.
- For dual-channel cameras, you can set OSD parameters for the channels separately.

Configure OSD displayed on the live video.

1. Go to **Setup > Image > OSD**.

Enable	No.	Overlay OSD Content	X-Axis	Y-Axis
<input checked="" type="checkbox"/>	1	<Custom>	2	3
<input type="checkbox"/>	2	<Date & Time>	75	3
<input type="checkbox"/>	3	<People Counting>	2	75
<input type="checkbox"/>	4	<Time>	0	0
<input type="checkbox"/>	5	<Date>	0	0
<input type="checkbox"/>	6	<Picture Overlay>	0	0
<input type="checkbox"/>	7	<Network Port>	0	0
<input type="checkbox"/>	8	<Device Latitude and Longitude Coordinates>	0	0

Display Style

Effect: Background

Font Size: Medium

Font Color: #0000-1

Min. Margin: None

Date Format: MM/dd/yyyy

Time Format: HH:mm:ss

dd=Day; dddd=Day of the week; M=Month; y=Year
h/H=12/24 Hour; t=A.M. or P.M.; mm=Minute; ss=Second


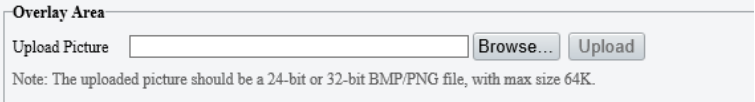
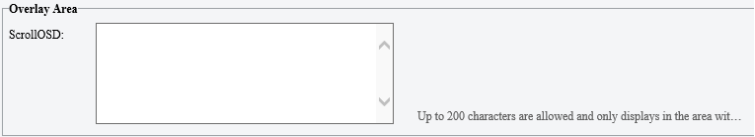

2. Configure parameters in the OSD Toolbar



NOTE!

OSD operations supported may vary with device model.

Item	Description
Enable	<p>Select the checkboxes in the Enable column to overlay the corresponding OSD contents on live video.</p> <p>NOTE!</p> <p>Up to 10 OSDs are allowed.</p>

Item	Description
<div>Overlay Content</div> <div>OSD</div>	<p>Set OSD content you want to overlay. Point to the OSD content, click , select the OSD content from the drop-down list or customize it.</p> <p>NOTE!</p> <ul style="list-style-type: none"> An OSD content takes effect only when the Enable checkbox is selected. Some models allow multiple OSD contents in one overlay area.
X-Axis/Y-Axis	<p>Specify the exact position of the OSD by entering the X and Y coordinates. The top left corner of the image is the origin (0, 0), the horizontal axis is the X-axis, and the vertical axis is the Y-axis.</p> <p>NOTE!</p> <p>You can also drag an OSD to the desired position: point to the OSD box in the preview window and drag when the cursor shape changes.</p>
Upload Picture	<p>This parameter is available only when the Overlay OSD Content is set to Picture Overlay.</p> <ol style="list-style-type: none"> Click Browse... to select the picture you want to overlay. Click Upload, then the picture is displayed on the live video. 
ScrollOSD	<p>This parameter is available only when the Overlay OSD Content is set to Picture Overlay.</p> <ol style="list-style-type: none"> Enter the text you want to overlay. The text appears on the live video and scrolls from right to left. 
	<p>After configuring the OSD for one channel, you can click Copy to copy the OSD content and style of the channel to other channels.</p>

3. Overlay OSD Contents

- Custom: Customizes the OSD contents.
- Date & Time: Displays the current date and time of the camera according to the set format (content style), for example, Friday, 25 March, 2022 14:25.
PTZ Coordinates: Specify the exact position of the PTZ camera. For example, P: 165.42°, T: 1.49°. P stands for horizontal coordinates, T stands for vertical coordinates.
- Zoom: Displays the zoom information of the PTZ, for example, Z: 1.00X.
- Preset: Displays current preset ID on live video, for example, Preset 1.
- Serial Port: The IPC will receive and parse the serial port information in correct format and display the information in the live view window. Only some models support this function.
- Direction: Displays the coordinates of the 8 directions of the PTZ camera, including the basic directions: East, South, West, North, and the intermediate directions: Northeast, Southeast, Northwest, and Southwest.
- People Counting: Displays people flow information (number of people entering/leaving), crowd density information (number of people present), or face detection information (number of people entering/leaving) on live video. You need to enable and configure [People Flow Counting](#), [Crowd Density Monitoring](#), or [Face Detection](#).
- Time: Displays the current time of the device.
- Date: Displays the current date of the device.


- **Picture Overlay:** Displays locally imported pictures. You may set the picture transparency according to your need.
- **ScrollOSD:** The OSD text displays on the live video and scrolls from right to left.
- **Network Port:** The IPC will receive and parse the network port information in correct format and display the information in the live view window.
- **Device Latitude and Longitude Coordinates:** Displays the latitude and longitude coordinates of the device location.
- **Motor Vehicle&Non-Motor Vehicle&Pedestrian Count:** Displays motor vehicle/non-motor vehicle/pedestrian counting information on live video. You need to enable [Mixed-Traffic Detection](#) and Motor Vehicle&Non-Motor Vehicle&Pedestrian Count first.



NOTE!

- To disable an OSD, clear the OSD content or clear the corresponding **Enable** checkbox.
- Some models allow multiple OSDs.

4. Set the OSD display style.

Item	Description
Effect	Choose a display effect: Background , Stroke , Hollow , or Normal .
Font Size	Choose a font size: X-large , Large , Medium , or Small .
Font Color	Click  to choose a font color.
OSD Inverse	When enabled, the OSD content color is opposite to the live view color.
Min. Margin	Choose a minimum distance between the OSD area and the edge of image: <ul style="list-style-type: none"> • None: Zero margin. • Single: One-character margin. • Double: Two-character margin.
Date Format	Choose a date format: dd/MM/yyyy , MM/dd/yyyy , etc.
Time Format	Choose a time format: HH:mm:ss , HH:mm:ss.aaa , hh:mm:ss tt , or hh:mm:ss.aaa tt .

5.4.3 Privacy Mask

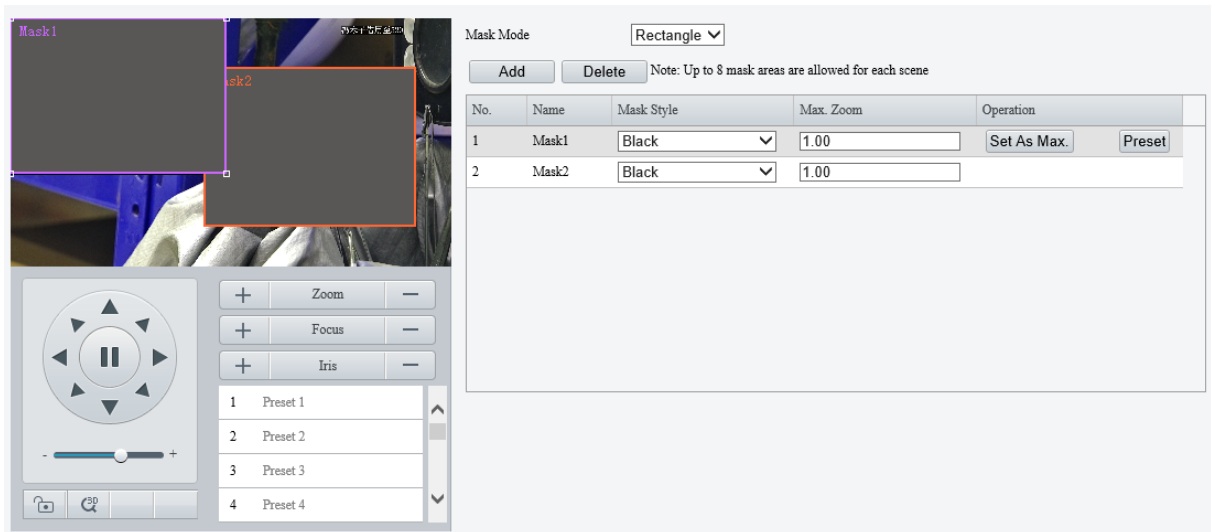
Privacy mask is used to cover certain areas on the image for privacy, for example, ATM keyboard.



NOTE!

- This function may vary with device model.
- For dual-channel devices, you can set privacy mask parameters for the channels separately.

1. Go to **Setup > Image > Privacy Mask**.

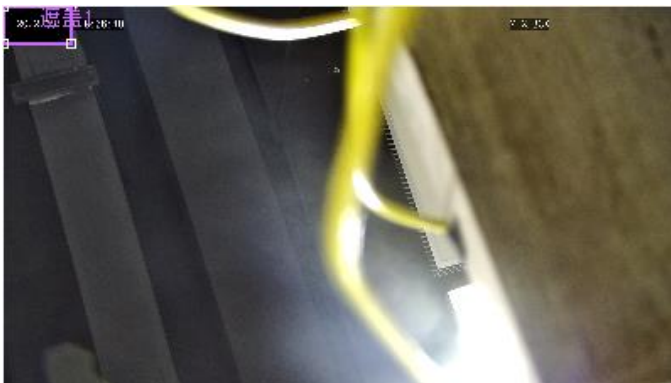


2. Select the mask mode, **Rectangle** or **Polygon**.

- 2D-mask camera: For a PTZ camera, the privacy mask does not move and zoom with the camera.
- 3D-mask camera: For a PTZ camera, the privacy mask moves and zooms with the camera and the masked area is always covered.

3. Add a privacy mask.

(1) Click **Add**. The privacy mask is a rectangle by default.



(2) Adjust the position and size of the mask or draw a mask as needed.

- Adjust the position and size of the mask.
 - Point to a border of the mask and drag it to the desired position.
 - Point to a handle of the mask and drag to resize it.
- Draw a mask.
 - Polygon: Click on the image and drag to draw a line. Repeat the action to draw more lines to form an enclosed shape as needed. Up to 4 lines are allowed.
 - Rectangle: Click on the image and drag to draw a rectangle.

4. Set the privacy mask.

Item	Description
Mask style	Select the mask style, Black or Mosaic . NOTE! <ul style="list-style-type: none"> • This parameter is configurable when Mask Mode is set to Rectangle. By default, the mask style of polygon mask is black and cannot be modified. • Mosaic is only available on certain models.
Max. Zoom (3D-mask camera)	Set the maximum zoom ratio to determine whether to show or hide the privacy mask. If the current lens zoom ratio is less than the maximum zoom ratio, the privacy mask is invalid.

Item	Description
Set As Max. (3D-mask camera)	Click to set the current lens zoom ratio as the maximum zoom ratio.
Preset (3D-mask camera)	Click to rotate the camera to the masked area (generally, the masked area is in the center of the live video).

5.4.4 Quick Focus

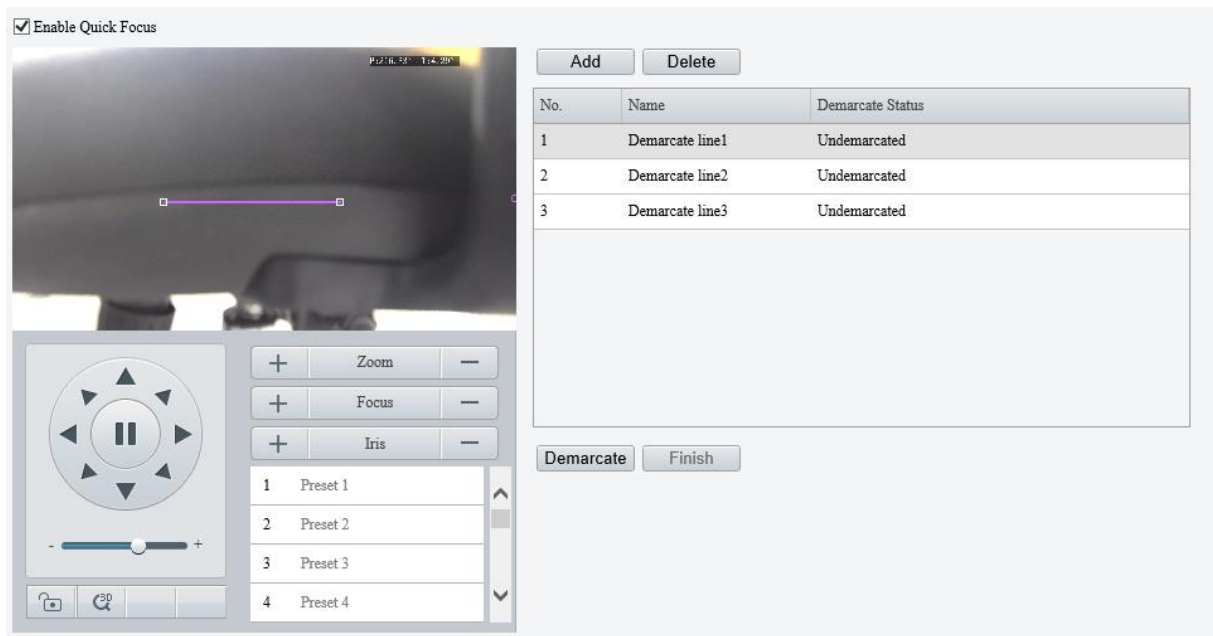
Fast focus effectively saves focus time and avoids missing important information after the camera changes the scene, focus, and zoom.



NOTE!


- This function is only available on certain models.
- Set the zoom speed to 2 on the **Image** page when quick focus is enabled.

1. Go to **Setup > Image > Quick Focus**.
2. Select the **Enable Quick Focus** checkbox to enable it.

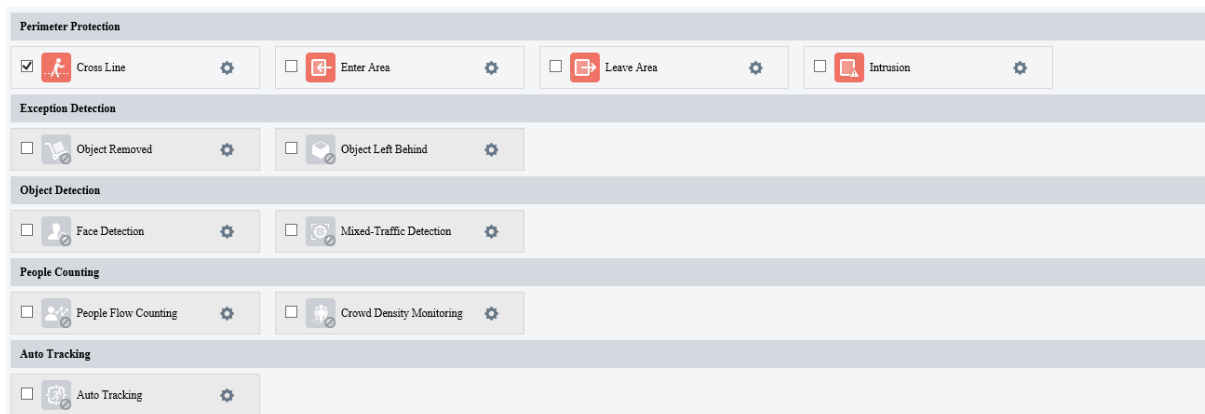


3. Add a calibration line for the desired scene.
 - (1) Click **Add**. A line is displayed on the image.
 - (2) Adjust the position and length of the line or draw a line as needed.
 - Adjust the position and length of the line.
 - Point to the line and drag it to the desired position.
 - Point to a handle of the line and drag to resize it.
 - Draw a line.
 - Click on the image and drag to draw a line.
4. Click **Demarcate** to start automatic zoom. After the auto zoom is completed, click **Finish** to complete calibration. If you click **Finish** during calibration, the calibration line is considered invalid.
5. Repeat the above steps to calibrate more scenes. Up to 4 scenes are allowed.

5.5 Smart

On the **Smart** page, you can select the smart event to be monitored and click  to configure relevant parameters.



The smart events supported by the device and the parameters supported by the events may vary with device model.



The screenshot displays a configuration interface for smart events, organized into several sections:

- Perimeter Protection:** Includes ☒ Cross Line, ☐ Enter Area, ☐ Leave Area, and ☐ Intrusion. Each item has a gear icon for configuration.
- Exception Detection:** Includes ☐ Object Removed and ☐ Object Left Behind, each with a gear icon.
- Object Detection:** Includes ☐ Face Detection and ☐ Mixed-Traffic Detection, each with a gear icon.
- People Counting:** Includes ☐ People Flow Counting and ☐ Crowd Density Monitoring, each with a gear icon.
- Auto Tracking:** Includes ☐ Auto Tracking with a gear icon.

Common Button Description

Button	Description
	Create detection rules. Up to 4 detection rules are allowed for each smart event.
	Delete detection rules.



NOTE!

- For dual-channel devices, you can set smart parameters for the channels separately.
- Some smart functions are mutually exclusive. When a smart function is enabled, the functions that are mutually exclusive with it are grayed out.

5.5.1 Alarm-triggered Actions

Configure linkage actions to be triggered when an alarm occurs.

Perimeter protection, exception detection, object detection, people flow counting, and auto tracking support alarm-triggered actions (also known as linkage actions).


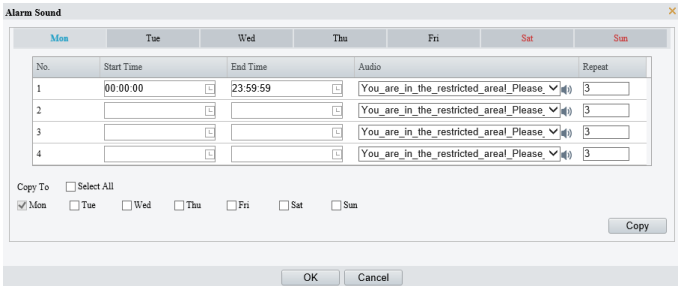

1.

Conventional	Alarm Output	Storage
<input checked="" type="checkbox"/> Alarm the Center <input type="checkbox"/> Send E-mail <input type="checkbox"/> Panoramic Linkage <input checked="" type="checkbox"/> Upload Image(Original)	<input type="checkbox"/> A → 1 <input type="checkbox"/> A → 2 <input type="checkbox"/> Alarm Sound	<input type="checkbox"/> Recording Edge Storage <input type="checkbox"/> Image Edge Storage <input type="checkbox"/> FTP Video Storage

Conventional alarm-triggered actions

Item	Description
Upload to FTP	<p>The camera uploads snapshots to the specified FTP server when an alarm occurs.</p> <ol style="list-style-type: none"> 1. Configure FTP and Snapshot. 2. Select the Upload to FTP checkbox to enable this function.
Send E-mail	<p>The camera sends snapshots to the specified email addresses when an alarm occurs.</p> <ol style="list-style-type: none"> 1. Configure E-mail and Snapshot. 2. Select the Send Email checkbox to enable this function.
Alarm the Center	<p>The camera uploads alarm information to the surveillance center when an alarm occurs.</p> <p>Select the Alarm the Center checkbox to enable this function.</p>
Report Data to Center	<p>The camera uploads data to the server when an alarm occurs.</p> <ol style="list-style-type: none"> 1. Configure management platform. 2. Select the Report Data to Center checkbox to enable this function.
Attribute Collection	<p>The camera uploads the attribute information collected from the captured object to the server when an alarm occurs.</p> <ol style="list-style-type: none"> 1. Configure Attribute Collection. 2. Select the Attribute Collection checkbox to enable this function.
Upload Image(Original)	<p>The camera uploads the original snapshot and the cutout image of the captured object to the server when an alarm occurs.</p> <p>Select the Upload Image(Original) checkbox to enable this function.</p> <p>For dual-channel cameras, when this function is configured for channel 2 (thermal channel), it will trigger channel 1 (visible light channel) to capture an image and upload the original image with the cutout image of the captured object to the server.</p>
Upload Image(Target)	<p>The camera uploads the cutout image of the captured object to the server.</p> <p>Select the Upload Image(Target) checkbox to enable this function.</p>

2. Alarm output

Item	Description
Alarm Output	<p>Connect the external alarm output devices, such as alarm lights and alarm bells, etc., to the camera's ALARM OUT interfaces. The camera triggers alarm output devices when an event occurs.</p> <p>A->1: A refers to the ALARM OUT interface on the device, 1 means the first ALARM OUT interface. A->2 means the second ALARM OUT interface on the device, and so on. The number of ALARM OUT interfaces may vary with the device model. See the device datasheet for specifications.</p> <p><input type="checkbox"/> A → 1</p> <p><input checked="" type="checkbox"/> A → 2</p> <ol style="list-style-type: none"> Configure Alarm Output. Select the Alarm Output checkbox to enable this function.
Alarm Sound	<p>The camera plays warning sounds when an alarm occurs.</p> <ol style="list-style-type: none"> Select the Alarm Sound checkbox, and then click . Set the arming schedule for audible alarms. See Arming Schedule for details. Set the alarm audio content and alarm times. <ul style="list-style-type: none"> Audio: Set the audio content to be played when an alarm occurs. See Audio File. Repeat: Set the number of times the audio to be played when an alarm occurs.  <p>NOTE!</p> <p>This function may vary with device model.</p>
Flashing Light	<p>The light flashes for a certain period of time when an alarm occurs.</p> <ol style="list-style-type: none"> Select the Flashing Light checkbox, and then click . Set the flash duration. Set the arming schedule. See Arming Schedule for details. <p>NOTE!</p> <p>This function may vary with device model.</p>

3. Alarm-triggered storage

Item	Description
Recording Storage Edge	<p>The camera saves alarm recordings to its memory card or NAS when an alarm occurs.</p> <ol style="list-style-type: none"> Configure Memory Card or Network Disk. Select the Recording Edge Storage checkbox.
Image Edge Storage	<p>The camera saves alarm snapshots to its memory card or NAS when an alarm occurs.</p> <ol style="list-style-type: none"> Configure Memory Card or Network Disk. Select the Image Edge Storage checkbox.
FTP Video Storage	<p>The camera uploads alarm recordings to the specified FTP server when an alarm occurs.</p> <ol style="list-style-type: none"> Configure FTP. Select the FTP Video Storage checkbox.

4. Alarm-triggered PTZ

Item	Description
Trigger Tracking	The camera tracks and zooms on the object that triggered the alarm until the set tracking time is reached or the object disappears. 1. Select the Trigger Tracking checkbox. 2. Click Tracking to configure tracking parameters. See Tracking for details.
Panoramic Linkage	The camera automatically tracks the object that triggered the alarm. 1. Configure panoramic linkage. See Error! Reference source not found. for details. 2. Select the Panoramic Linkage checkbox.
Go to Preset	The camera automatically goes to a preset position when an alarm occurs. 1. Select the Go to Preset checkbox. 2. Choose the preset to be linked with motion detection alarm. See PTZ for details.

5.5.2 Arming Schedule

You can set an arming schedule to determine when the camera performs detection.

- Draw a schedule.

To set an armed period, click **Armed**, and then click or drag on the schedule to select the time cells you want to enable arming. To set a disarmed period, click **Unarmed**, and then click or drag on the schedule to select the time cells you want to disable arming.

The image shows a software interface for setting an arming schedule. At the top, there is a checkbox labeled "Enable Plan" which is checked. Below it are two buttons: "Armed" (with a blue square icon) and "Unarmed" (with a white square icon). To the right of these buttons is an "Edit" button. Below the buttons is a grid representing a 7-day week. The days are listed on the left: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The time slots are listed at the top: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24. The grid cells are currently empty, indicating no schedule has been drawn yet.

- Edit a schedule.

Click **Edit**, set the arming time, and then click **OK**.

Edit

Mon

Tue

Wed

Thu

Fri

Sat

Sun

No.	Start Time	End Time
1	00:00:00	23:59:59
2		
3		
4		

Copy To

☐ Select All
 ☒ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat
 ☐ Sun

Copy

OK

Cancel



NOTE!

- Up to 4 time periods are allowed per day. The time periods cannot overlap.
- To apply the same time settings to other days, select the desired day(s), and then click **Copy**.

5.5.3 Smart Service Switch

Configure smart service switch so the camera can automatically switch smart services according to time schedules or linked presets.

- Go to **Setup > Smart Service > Smart Service Switch**.

Select Channel

Channel2

☒ Enable Auto Switch



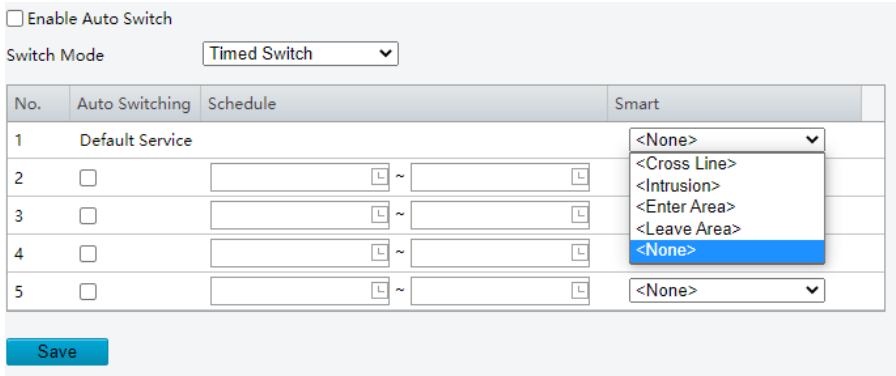
Switch Mode

Timed Switch


No.	Auto Switching	Schedule	Smart
1	Default Service		<Mixed-Traffic Detect>
2	<input type="checkbox"/>		<None>
3	<input type="checkbox"/>		<None>
4	<input type="checkbox"/>		<None>
5	<input type="checkbox"/>		<None>

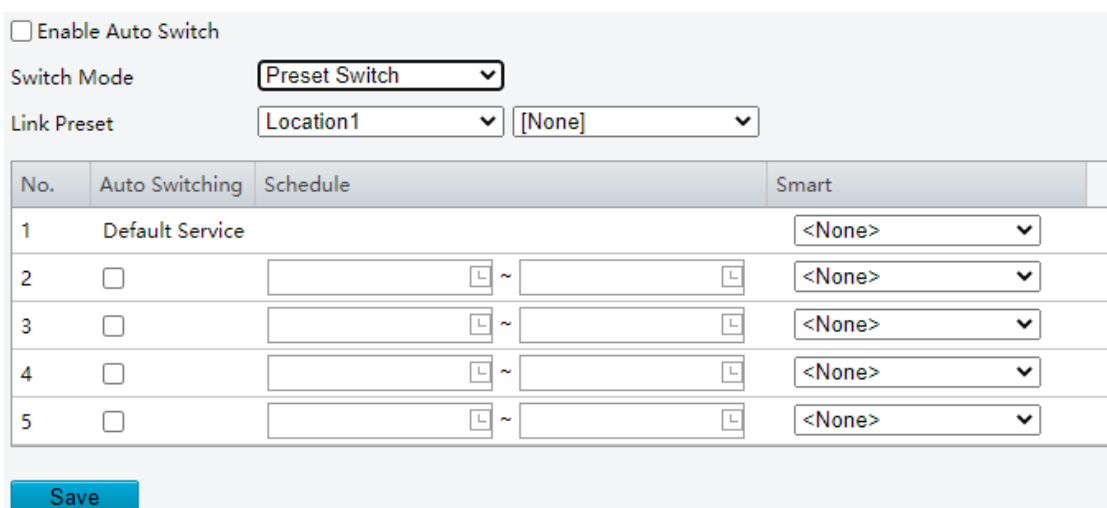
Save

- Click and choose a switch mode.
 - Timed Switch: Switch to a specified smart service at a set time.
 - Preset Switch: Switch to a specified smart service at a set time specified for a specified preset.
- Configure the switch mode parameters.
 - Timed Switch

Item	Description
Auto Switching	When auto switch is enabled and switching conditions are met, the system switches to the corresponding smart service automatically. The list includes the default service.
Schedule	<p>The default service (No.1, by default, unspecified) takes effect when the current time is not within the listed periods. You can add up to 5 periods and assign a smart service for each period. Click  to set time.</p> <ul style="list-style-type: none"> For certain perimeter protection functions, you can configure overlapping periods, which means, multiple smart services may be effective during the same period. For mutually exclusively smart services which cannot be enabled at the same time, overlapping periods are not allowed, and on-screen messages will appear. When panoramic linkage has been enabled and a specified smart service is mutually exclusive with panoramic linkage, an on-screen message will also appear.
Smart Service	<p>Click  to choose smart functions. All the functions on the Smart Service page except panoramic linkage are listed in the drop-down list.</p> 

- Preset Switch

Click  to choose a preset. You can set up to 4 locations and link a location to a preset (the linked presets must be configured in advance, see **Error! Reference source not found.**). The steps for configuring a position are similar to that for configuring timed switch, that is, you can configure 4 locations and 4 corresponding schedules, each schedule includes periods and corresponding smart services.



4. (Optional) Select the **Enable Auto Switch** checkbox. After selecting the **Enable Auto Switch** checkbox, you may still configure or enable/disable smart services.


- Timed Switch

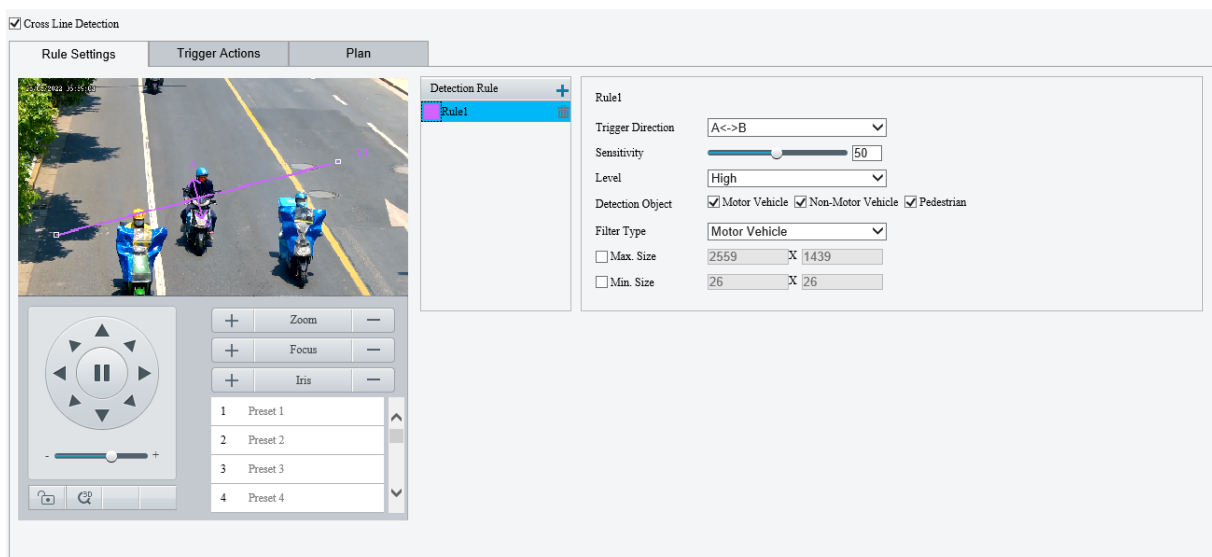
- The camera switches to the linked smart service at the start time of a period.


- The camera switches to the default service at the end time of a period, or switches to the corresponding smart service at the start time of the next period.
 - The camera switches to the smart service at once when Auto Switch is enabled.
 - Preset Switch
 - The camera switches smart service only when calling a linked preset.
 - The camera checks the time when calling a preset. If the current time is within a specified period, the camera switches to the smart service linked to the period.
 - The camera switches to the default smart service of the preset if the current time is not within any listed periods.
5. Click **Save**.

5.5.4 Cross Line Detection

Cross line detection detects objects crossing a user-specified virtual line in a specified direction. The camera reports an alarm when the detection rule is triggered.

1. Go to **Setup > Intelligent > Smart**.
2. Select **Cross Line** and click  to configure it.



3. Add a detection rule.
 - (1) Click  to add a detection line. Up to 4 detection rules are allowed.





- (2) Adjust the position and length of the line or draw a line as needed.
 - Adjust the position and length of the line.
 - Point to the line and drag it to the desired position.


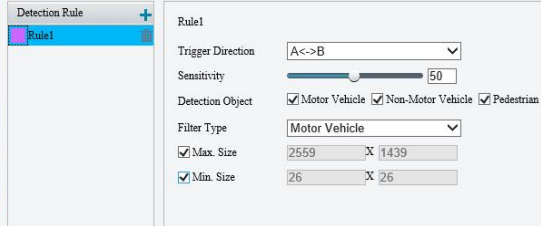
- Point to a handle of the line and drag to resize it.
 - Draw a line.
- Click on the image and drag to draw a line.



NOTE!

When editing detection rules, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after you finish editing detection rules.

4. Set the detection rule.


Item	Description
Trigger Direction	<p>Select the direction from which the object crosses the line to trigger an alarm.</p> <ul style="list-style-type: none"> • A->B: The camera reports a cross line alarm when it detects an object crossing the line from A to B. • B->A: The camera reports a cross line alarm when it detects an object crossing the line from B to A. • A<->B (default): The camera reports a cross line alarm when it detects an object crossing the line from A to B or from B to A.
Sensitivity	<p>Set the detection sensitivity.</p> <p>The higher the sensitivity, the more likely cross line behaviors will be detected, and the more likely false alarms will occur.</p>
Level	<p>Select the priority of the detection rule, including High, Medium, and Low.</p> <p>The camera detects the rule that is triggered first by default. If multiple rules are triggered at the same time, the camera detects the rule with higher priority.</p>
Detection Object	<p>Select the object to be detected, including Motor Vehicle, Non-Motor Vehicle, and Pedestrian.</p>
Filter Type	<p>After you select a detection object, you can set a filter rule for it.</p> <p>For example, if you have selected Motor Vehicle as a detection object, select Motor Vehicle from the Filter Type drop-down list and set the Max. Size or Min. Size for it, then motor vehicles larger than the Max. Size or smaller than the Min. Size will not be detected.</p>
Max. Size/Min. Size	<p>When enabled, a box appears on the image, you can point to a handle of the box and drag to resize it. The camera filters objects larger than the Max. Size or smaller than the Min. Size. The width and height of the maximum filter area must be greater than that of the minimum filter area.</p> <div>   </div>

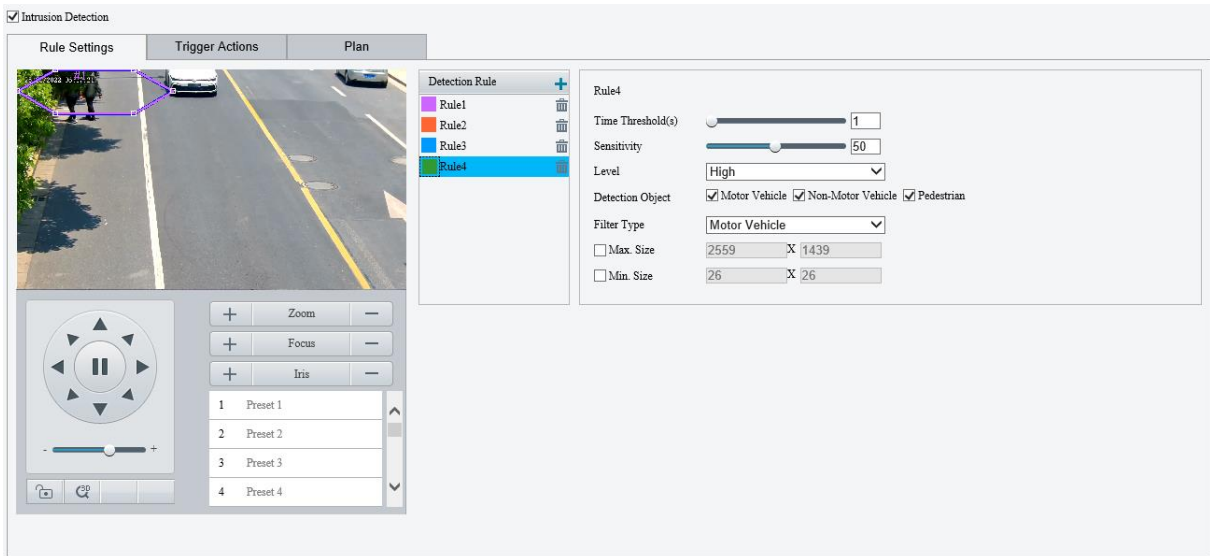
5. Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
6. Click **Save**.

5.5.5 Intrusion Detection


Intrusion detection detects objects entering a user-specified area and staying for a preset time. The camera reports an alarm when the detection rule is triggered.

1. Go to **Setup > Intelligent > Smart**.

2. Select **Intrusion** and click  to configure it.



3. Add a detection rule.

(1) Click  to add a detection area. The detection area is a hexagon by default. Up to 4 detection rules are allowed.





(2) Adjust the position and size of the area or draw an area as needed.

- Adjust the position and size of the area.
 - Point to a border of the area and drag it to the desired position.
 - Point to a handle of the area and drag to resize it.
- Draw an area.

Click on the image and drag to draw a line. Repeat the action to draw more lines to form an enclosed shape as needed. Up to 6 lines are allowed.

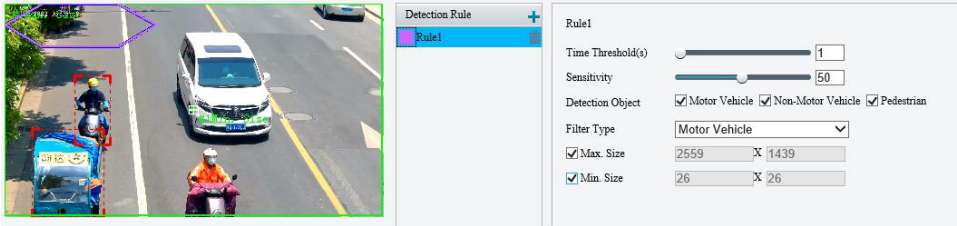


NOTE!

When editing detection rules, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after you finish editing detection rules.

4. Set the detection rule.


Item	Description
Time Threshold(s)	Set how long the object stays in the detection area to trigger an intrusion alarm. If an object stays in the detection area for the set time, an intrusion alarm will be triggered.

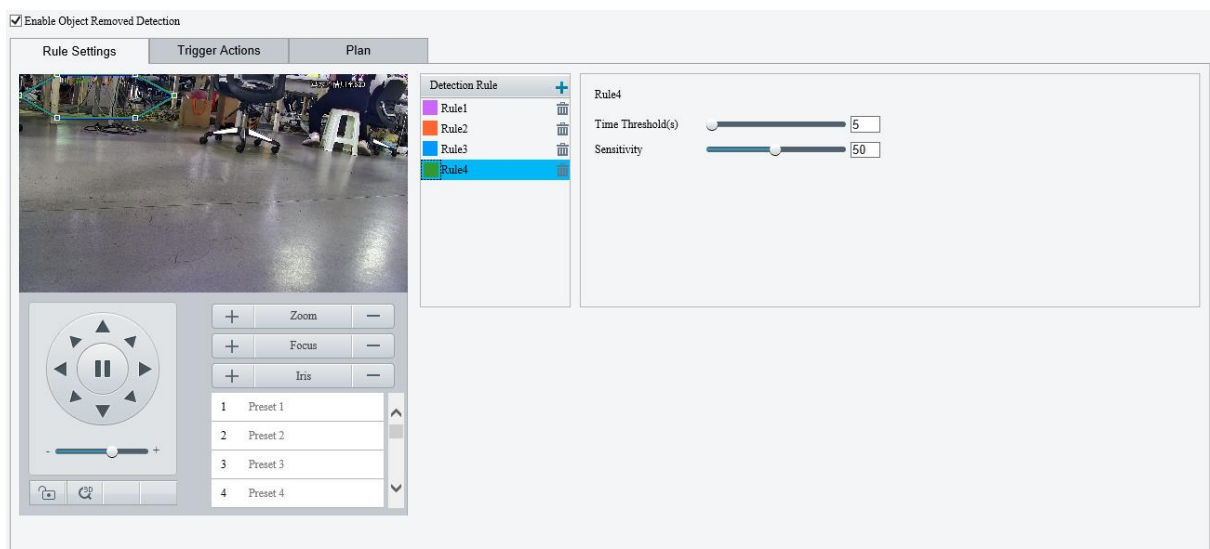
Sensitivity	Set the detection sensitivity. The higher the sensitivity, the more likely intrusion behaviors will be detected, and the more likely false alarms will occur.
Level	Select the priority of the detection rule. The camera detects the rule that is triggered first by default. If multiple rules are triggered at the same time, the camera detects the rule with higher priority.
Detection Object	Select the object to be detected, including Motor Vehicle , Non-Motor Vehicle , and Pedestrian .
Filter Type	After you select a detection object, you can set a filter rule for it. For example, if you have selected Motor Vehicle as a detection object, select Motor Vehicle from the Filter Type drop-down list and set the Max. Size or Min. Size for it, then motor vehicles larger than the Max. Size or smaller than the Min. Size will not be detected.
Max. Size/Min. Size	When enabled, a box appears on the image, you can point to a handle of the box and drag to resize it. The camera filters objects larger than the Max. Size or smaller than the Min. Size. The width and height of the maximum filter area must be greater than that of the minimum filter area. 

- Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
- Click **Save**.


5.5.6 Object Removed Detection

Object removed detection detects objects removed from a user-specified area. The camera reports an alarm when the detection rule is triggered.

- Go to **Setup > Intelligent > Smart**.
- Select **Object Removed** and click  to configure it.



- Add a detection rule.

- (1) Click  to add a detection area. The detection area is a hexagon by default. Up to 4 detection rules are allowed.





- (2) Adjust the position and size of the area or draw an area as needed.

- Adjust the position and size of the area.
 - Point to a border of the area and drag it to the desired position.
 - Point to a handle of the area and drag to resize it.
- Draw an area.

Click on the image and drag to draw a line. Repeat the action to draw more lines to form an enclosed shape as needed. Up to 6 lines are allowed.



NOTE!

When editing detection rules, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after you finish editing detection rules.


4. Set the detection rule.

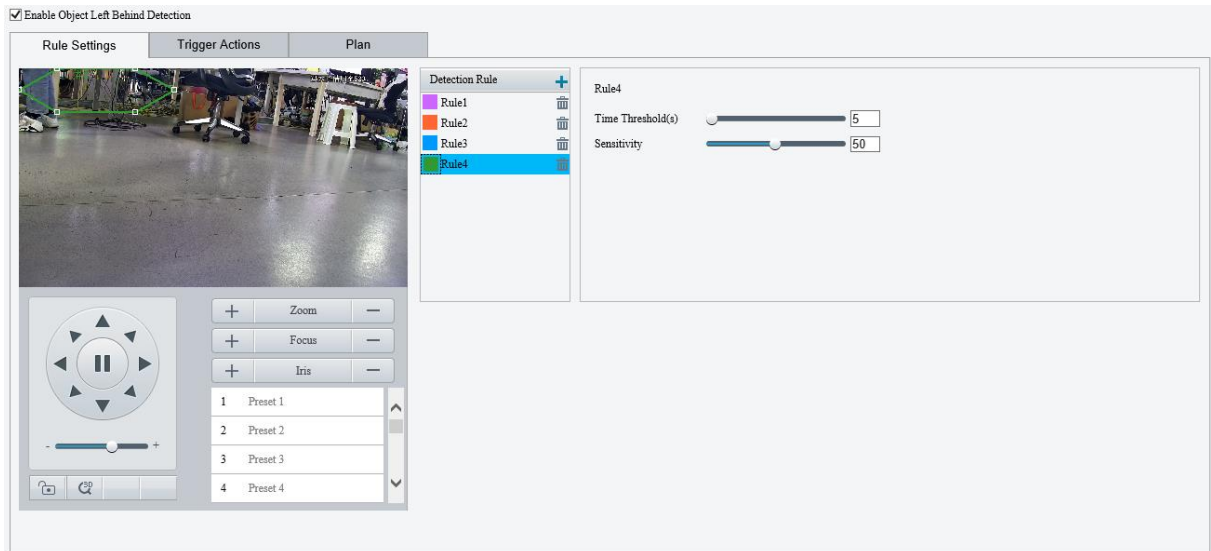
Item	Description
Time Threshold(s)	Set how long the object is removed from the detection area to trigger an alarm. If an object is removed from the detection area for the set time, an alarm will be triggered.
Sensitivity	Set the detection sensitivity. The higher the sensitivity, the more likely object removal behaviors will be detected, and the more likely false alarms will occur.

5. Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
6. Click **Save**.

5.5.7 Object Left Behind Detection

Object left behind detection detects objects left behind in a user-specified area. The camera reports an alarm when the detection rule is triggered.

1. Go to **Setup > Intelligent > Smart**.
2. Select **Object Left Behind** and click  to configure it.



3. Add a detection rule.

- (1) Click **+** to add a detection area. The detection area is a hexagon by default. Up to 4 detection rules are allowed.





- (2) Adjust the position and size of the area or draw an area as needed.

- Adjust the position and size of the area.
 - Point to a border of the area and drag it to the desired position.
 - Point to a handle of the area and drag to resize it.
- Draw an area.

Click on the image and drag to draw a line. Repeat the action to draw more lines to form an enclosed shape as needed. Up to 6 lines are allowed.



NOTE!

When editing detection rules, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after you finish editing detection rules.


4. Set the detection rule.

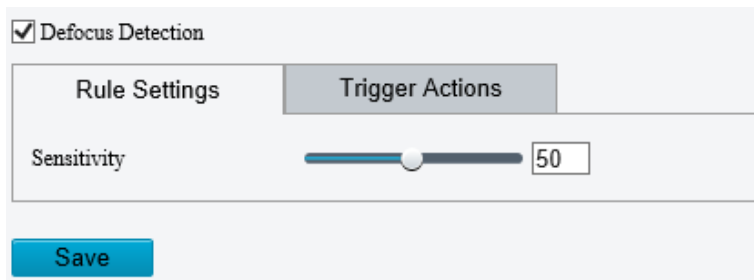
Item	Description
Time Threshold(s)	Set how long the object is left behind in the detection area to trigger an alarm. If an object is left behind in the detection area for the set time, an alarm will be triggered.
Sensitivity	Set the detection sensitivity. The higher the sensitivity, the more likely object left behind behaviors will be detected, and the more likely false alarms will occur.

5. Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
6. Click **Save**.

5.5.8 Defocus Detection

Defocus detection detects lens defocus. The camera reports an alarm when the detection rule is triggered.


1. Go to **Setup > Intelligent > Smart**.
2. Select **Defocus** and click  to configure it.

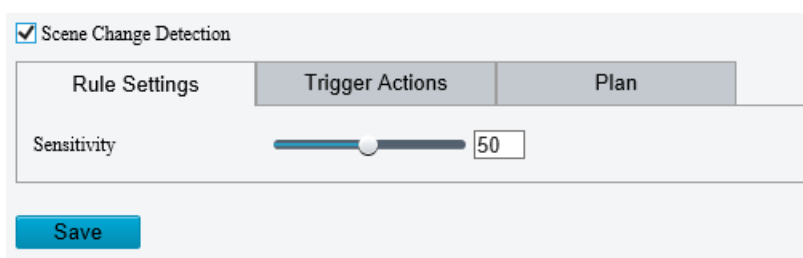


3. Set the detection sensitivity. The higher the sensitivity, the more likely defocus will be detected, and the more likely false alarms will occur.
4. Set the alarm-triggered actions. See [Alarm-triggered Actions](#) for details.
5. Click **Save**.

5.5.9 Scene Change Detection

Scene change detection detects the change of surveillance scene caused by external factors such as intentional camera movement. The camera reports an alarm when the detection rule is triggered.

1. Go to **Setup > Intelligent > Smart**.
2. Select **Scene Change** and click  to configure it.



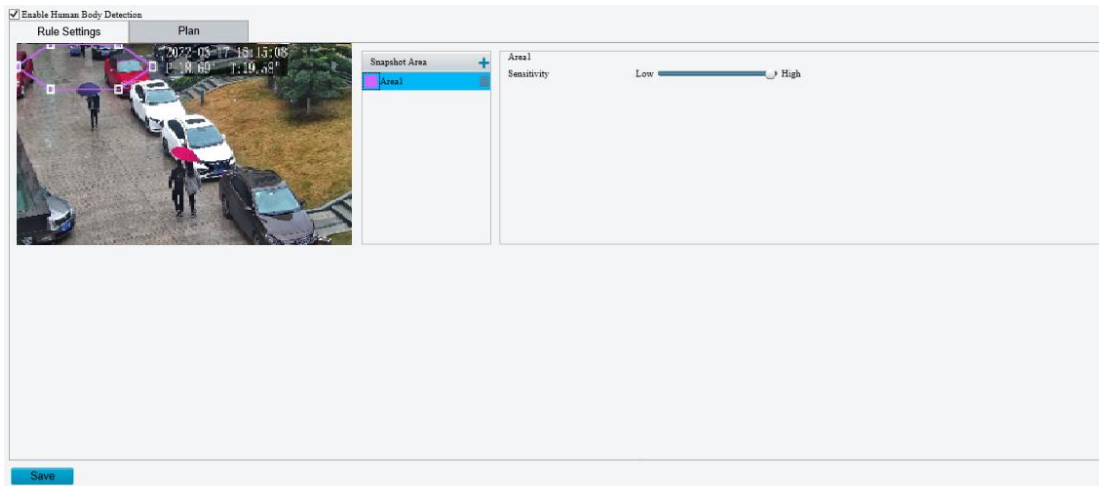
3. Set the detection sensitivity. The higher the sensitivity, the more likely scene change behaviors will be detected, and the more likely false alarms will occur.
4. Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
5. Click **Save**.

5.5.10 Human Body Detection


Human body detection detects humans in a specified area. The camera reports an alarm when the detection rule is triggered.

1. Go to **Setup > Intelligent > Smart**.

2. Select **Human Body Detection** and click  to configure it.



3. Add a snapshot area.

(1) Click . The snapshot area is a hexagon by default. Only one snapshot area is allowed.





(2) Adjust the position and size of the area or draw an area as needed.

- Adjust the position and size of the area.
Point to the area and drag it to the desired position. Drag the corners of the area to resize it.
- Draw an area.
Click in the preview window to draw a polygonal area with up to 6 sides.



NOTE!

When editing detection rules, you can click  to lock the scene to prevent pan/tilt movement caused by triggered detection rules and click  to unlock the scene after you finish editing detection rules.

4. Set the detection sensitivity. The higher the sensitivity, the more likely humans will be detected, and the more likely false alarms will occur.
5. Set the alarm-triggered actions and arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
6. Click **Save**.

5.6 Alarm

Configure the alarm function, so the camera can report alarms when an event occurs. Configure alarm linkage, so the camera can trigger other devices to perform specified actions when an event occurs.



NOTE!


The supported alarms and linkage actions (or trigger actions) may vary with camera model.

5.6.1 Common Alarm

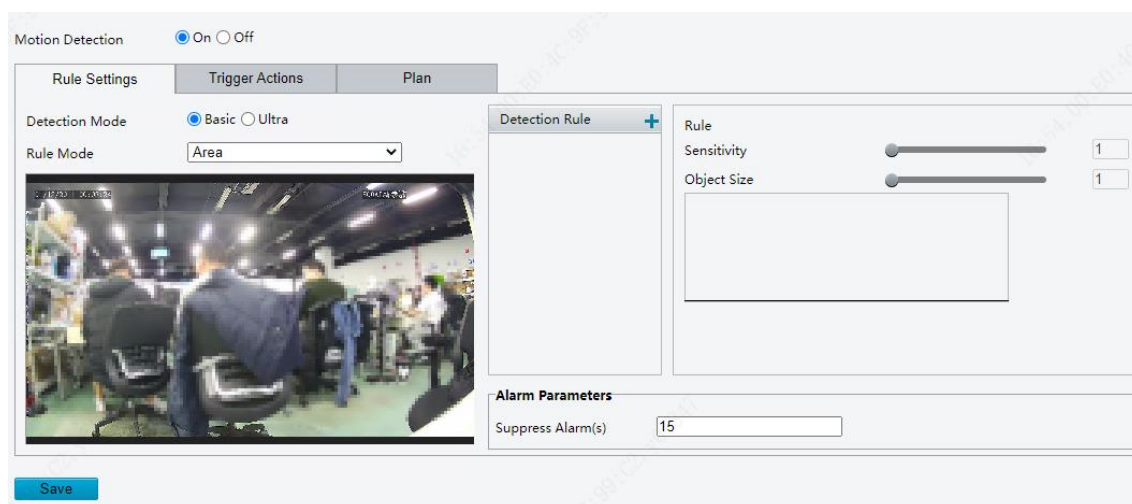
1. Motion Detection



NOTE!

- The  icon appears in the upper right corner of the image when a motion detection alarm occurs.
- The function may vary with device model.


1. Go to **Setup > Events > Common Alarm**.



2. Choose the detection mode, including basic mode and ultra mode.

Basic Mode

The camera detects motions in specified detection areas or grids on the image and will take snapshots and report an alarm when detection rules are triggered.

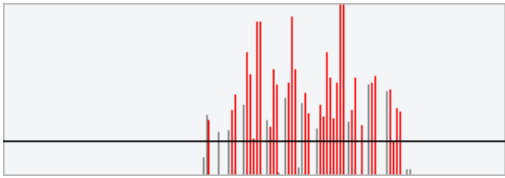
- Detection area
 - (1) To add a detection area, click , then a rectangle appears on the image. Up to four detection areas are allowed.



- (2) Adjust the position, size, and shape of the rectangle detection area, or draw a new one.
 - Point to a border of the area and drag it to the desired position.

- Point to a handle of the area and drag to resize it.
- Click anywhere on the image, and then drag to draw a new area.

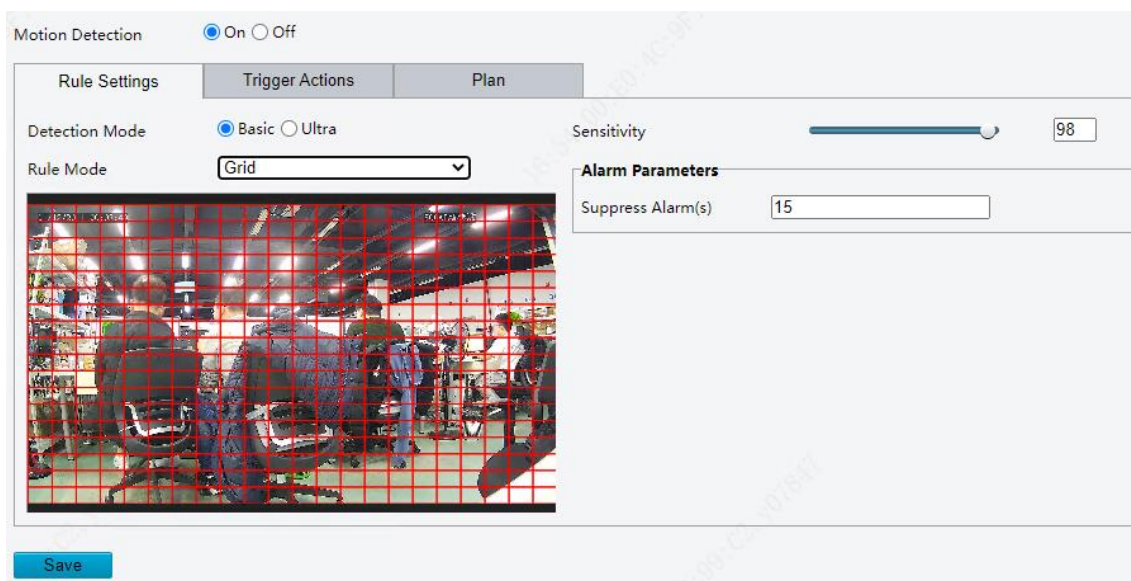
(3) Set detection rules.

Item	Description
Sensitivity	<p>Drag the slider to adjust detection sensitivity.</p> <p>The higher the sensitivity level, the higher the detection rate of small motions, and the higher the false alarm rate. Set based on the scene and your actual needs.</p>
Object size	<p>Drag the slider to set object size.</p> <ul style="list-style-type: none"> Object size: The ratio of the size of the detected object to the size of the detection area. An alarm is triggered when the ratio reaches the set value. To detect motion of small objects, you need to draw a small detection area separately. Motion detection results of the current detection area are shown below in real time. The red means motions that have triggered a motion detection alarm. The height of the lines indicates the extent of motion. The density of the lines indicates the frequency of motion. The higher the line, the greater the extent. The denser the lines, the higher the frequency. 

(4) Set **Suppress Alarm** to avoid receiving the same alarms within a certain length of time (alarm suppression time). For example, alarm suppression time is set to 5s, after an alarm is reported:

- If no motion is detected within the next 5s, new alarms can be reported after 5s when the alarm suppression time (5s) is over.
- If motion is detected within the next 5s, the alarm suppression time recounts from the time of the last alarm, and new alarms can be reported when the alarm suppressions time (5s) is over.

• Grid detection.



1. Set grid detection areas (covered by grid), which is by default the whole screen.

(1) Edit detection areas as needed.

- Click or drag on grid areas to erase grids.
- Click or drag on blank areas to draw grids.

(2) Drag the slider to adjust detection sensitivity.

The higher the sensitivity level, the higher the detection rate of small motions, and the higher the false alarm rate. Set based on the scene and your actual needs.

(3) Set **Suppress Alarm** to avoid receiving the same alarms within a certain length of time (alarm suppression time). For example, alarm suppression time is set to 5s, after an alarm is reported:

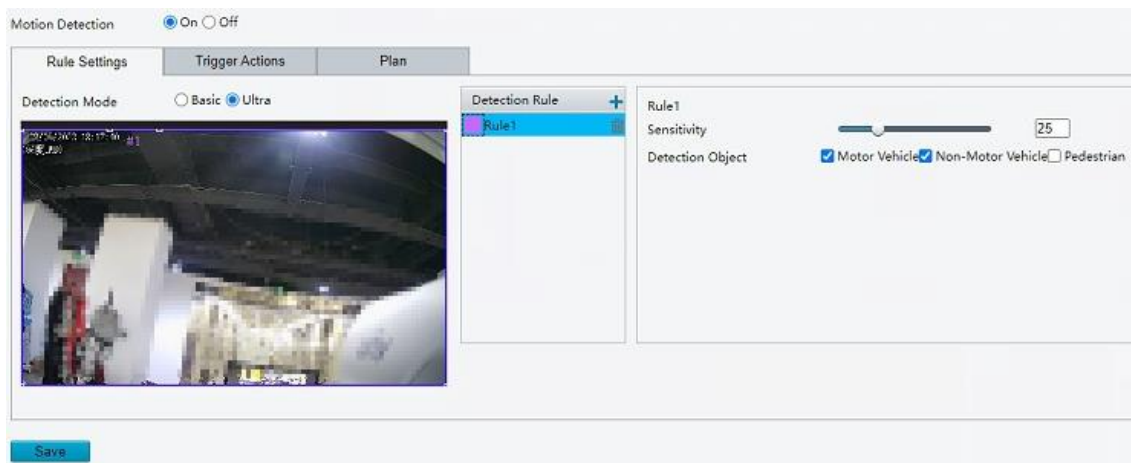
- If no motion is detected within the next 5s, new alarms can be reported after 5s when the alarm suppression time (5s) is over.
- If motion is detected within the next 5s, the alarm suppression time recounts from the time of the last alarm, and new alarms can be reported when the alarm suppression time (5s) is over.

3. Set alarm linkage and an arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.


4. Click **Save**.

Ultra Mode

The camera detects motions of motor vehicles, non-motor vehicles and pedestrians in specified detection areas and will take snapshots and report an alarm when detection rules are triggered.



1. Set detection rules.

(1) To add a detection area, click , then a rectangle appears on the image. Up to four detection areas are allowed.

(2) Adjust the position, size, and shape of the rectangle detection area, or draw a new one.

- Point to a border of the area and drag it to the desired position.
- Point to a handle of the area and drag to resize it.
- Click anywhere on the image, and then drag to draw a new area.

(3) Drag the slider to adjust detection sensitivity.

The higher the sensitivity level, the higher the detection rate of small motions, and the higher the false alarm rate. Set based on the scene and your actual needs.

(4) Select the detection object.

2. Set alarm linkage and an arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.


3. Click **Save**.

2. Tampering Detection

The camera triggers a tampering alarm after the lens is blocked for a certain length of time.

1. Go to **Setup > Events > Common Alarm > Tampering Detection**.

☒ Enable Tampering Alarm

Rule Settings	Trigger Actions	Plan
Sensitivity		24
Duration(s)	<input type="text" value="1"/>	

Save

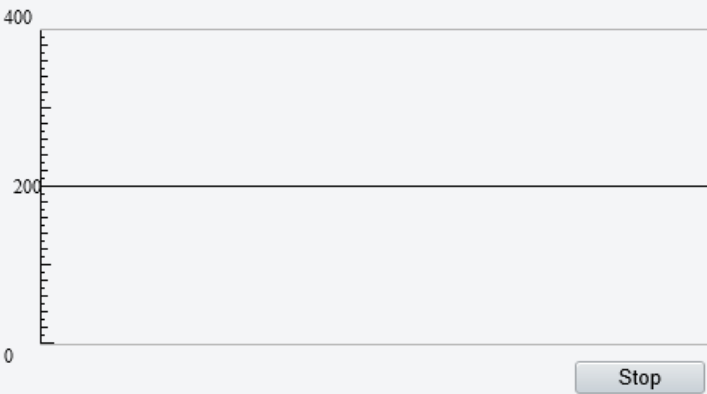
2. Select **Enable Tampering Detection**.
3. Set detection rules.
 - (1) Drag the slider to adjust detection sensitivity. The higher the sensitivity level, the higher the detection rate, and the higher the false alarm rate. Set based on the scene and your actual needs.
 - (2) Set the duration of lens blocking. The camera reports an alarm when the duration of lens blocking exceeds the set value. Set based on the scene and your actual needs.
4. Set alarm linkage and an arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
5. Click **Save**.

3. Audio Detection

The camera monitors input audio signals and triggers an audio detection alarm when an exception is detected. Make sure an audio collection device (e.g., sound pickup) is connected, and audio detection is enabled (see [Audio](#)).

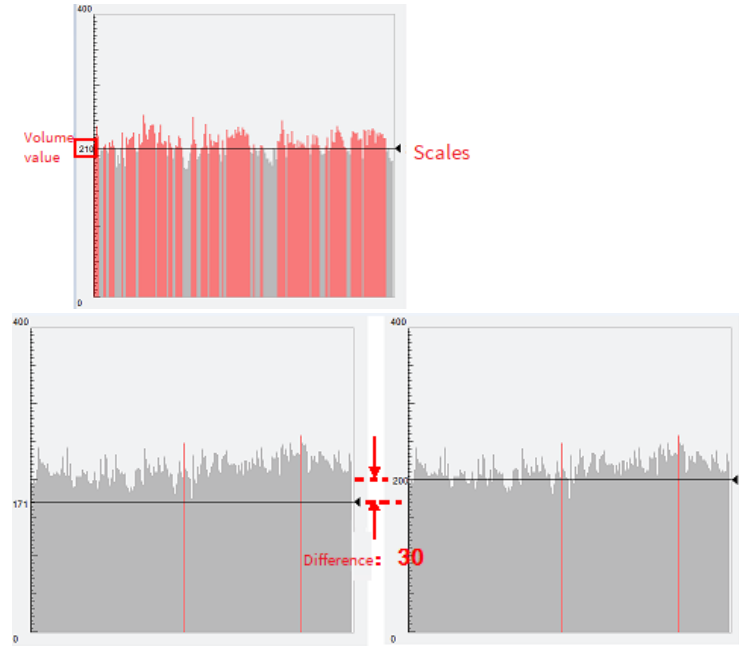
- When audio input mode is Line/Mic.
1. Go to **Setup > Events > Common Alarm > Audio Detection**.

Audio Detection ☒ On ☐ Off

Rule Settings	Trigger Actions	Plan
	Detection Type <input type="text" value="Sudden Rise"/>	Difference <input type="text" value="100"/>

Save

2. Enable **Audio Detection**.
3. Set audio detection rules.

Item	Description
Detection Type	<ul style="list-style-type: none"> • Sudden Rise: Detects sudden rising sound volume and triggers an alarm when the rise of volume exceeds the difference. • Sudden Fall: Detects sudden falling sound volume and triggers an alarm when the fall of volume exceeds the difference. • Sudden Change: Detects sudden rising and falling sound volume and triggers an alarm when the rise or fall of volume exceeds the difference. • Threshold: Triggers an alarm when the volume exceeds the threshold.
Difference/Threshold	<ul style="list-style-type: none"> • Difference: The difference between two sound volumes. The camera triggers an alarm when the rise or fall of volume exceeds the difference (range: 0-400). This parameter is applicable when the detection type is Sudden Rise, Sudden Fall, or Sudden Change. • Threshold: The camera triggers an alarm when the sound volume exceeds the threshold (range: 0-400). This parameter is applicable when the detection type is Threshold.
Diagram of relative audio intensity	<ul style="list-style-type: none"> • Audio detection results are displayed and updated in real time. You can control the display progress by clicking the Start/Stop button. • The scales are used to measure sound volume. Gray indicates relative sound intensity. Red means sound volume that has triggered alarms. 

4. Set alarm linkage and an arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.
5. Click **Save**.

4. Alarm Input

The camera can receive alarms from external third-party devices such as infrared detectors, smoke detectors, etc. After alarm input is configured, the third-party device can send signals to the camera after an event occurs.

1. Go to **Setup > Events > Common Alarm > Alarm Input**.

Select Alarm Alarm Input 1 ▼

Rule Settings	Trigger Actions	Plan
Alarm Name	<input type="text" value="A1"/>	
Alarm ID	<input type="text"/>	
Alarm Type	N.O. ▼	
Alarm Input	<input type="radio"/> On <input checked="" type="radio"/> Off	

Save

- Choose an alarm input from the drop-down list.

The number of alarm inputs available may vary by camera model. For example, if the camera has two alarm inputs on the tail cable, you can configure alarm input 1 and alarm input 2 separately.

- Configure alarm input.

Item	Description
Alarm Name	The default name is the alarm input channel ID. You rename it as needed.
Alarm ID	Set an alarm ID as you need.
Alarm Type	Set the alarm type according to the alarm input device. <ul style="list-style-type: none"> If the alarm input device is normally open (N.O.), choose N.C. If the alarm input device is normally closed (N.C.), choose N.O.
Alarm Input	Click On to enable Alarm Input .

- Set alarm linkage and an arming schedule. See [Alarm-triggered Actions](#) and [Arming Schedule](#) for details.

- Click **Save**.

5. Alarm Output

The camera can output alarms to external third-party devices such as an alarm bell, buzzer, etc. After the alarm output is configured, the camera can output alarm signals when an alarm (such as motion detection alarm, tampering alarm) occurs and trigger the third-party device to perform certain actions.

- Go to **Setup > Events > Common Alarm > Alarm Output**.

Select Alarm Alarm Output 1 ▼

Rule Settings	Output Schedule
Alarm Name	<input type="text" value="A1"/>
Default Status	N.O. ▼
Delay(s)	<input type="text" value="30"/>
Relay Mode	Bistable ▼

Save

- Choose an alarm output from the drop-down list. The number of alarm outputs available may vary by camera model.
- Configure alarm output parameters.

Item	Description
Alarm Name	The default name is the alarm output channel ID. You can rename it as needed.
Default Status	Choose the default status. The default is N.O. <ul style="list-style-type: none"> If the external alarm device is normally open (N.O.), choose N.O. If the external alarm device is normally closed (N.C.), choose N.C.
Delay(s)	The duration of alarm output after the alarm is triggered. Set it as needed.
Relay Mode	<p>The default is Monostable.</p> <ul style="list-style-type: none"> Monostable: The circuit can only remain in one stable state. When a trigger pulse is applied, the circuit switches to another state, and then automatically switches back to the original stable state. The circuit will repeat the same actions when the next trigger pulse arrives. Bistable: The circuit can remain in two stable states. When a trigger pulse is applied, the circuit switches to another state, and remains in this state after the trigger pulse is removed. When the next trigger pulse is applied, the circuit switches back to the other stable state and remains in that state. <p>NOTE!</p> <p>Set relay mode to better adapt to third-party alarm devices such as alarm lights. Please set the relay mode according to the trigger mode of the third-party alarm device.</p>

4. On the **Output Schedule** page, select **Enable Plan**, and then set when the camera can output alarms. By default, the schedule (plan) is disabled.

☒ **Enable Plan**

☒ **Armed** ☐ **Unarmed** Edit

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

Two methods are available to make an arming schedule:

- Draw a schedule.

Click **Armed**, and then drag on the calendar to set when the camera can output alarms. Click **Unarmed**, and then drag on the calendar to set when the camera cannot output alarms.

☒ **Enable Plan**

☒ **Armed** ☐ **Unarmed** Edit

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

**NOTE!**

You need Internet Explorer (higher than IE8) to draw on the calendar. IE10 is recommended.

- Edit the schedule.

Click **Edit**, set a refined schedule, click **OK**.

No.	Start Time	End Time
1	00:00:00	23:59:59
2		
3		
4		

Copy To ☐ Select All

☒ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Copy

OK Cancel

**NOTE!**

- Four periods are allowed each day. The periods must not overlap.
- To apply the current settings to other days, select the checkbox for the days one by one or select the **Select All** checkbox, and then click **Copy**.

5. Click **Save**.

**CAUTION!**

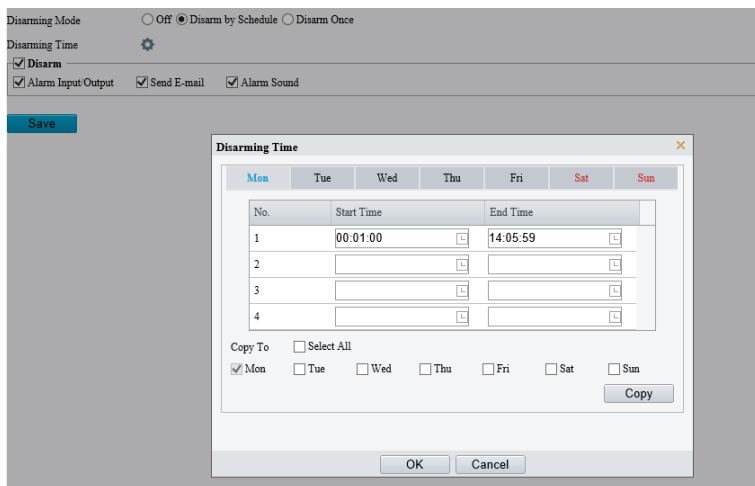
- Strictly follow the instructions below when powering on external alarm devices (e.g., alarm light) to avoid device damage.
- Check that **Alarm Type** is set to **Normally Open** (default) on the camera. Make sure the camera and the external alarm device are disconnected from power.
- After you connect the alarm device to the camera, connect the alarm device to power first, and then connect the camera to power.

5.6.2 One-key Disarming

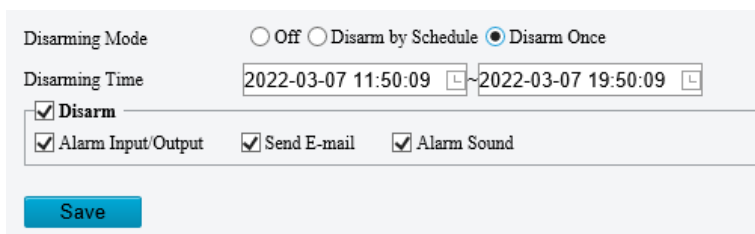
The camera cannot trigger linked actions when disarmed.

1. Go to **Setup > Events > One-key Disarming**.
2. Choose a disarming mode.
 - Disarm by Schedule: Disarm according to a weekly schedule.
 - Disarm Once: Disarm during a specified time period.
3. Configure disarming schedule or time according to the disarming mode you chose. The disarming schedule or time applies to all the actions selected.

- Disarm by schedule: Click  to configure disarming time.



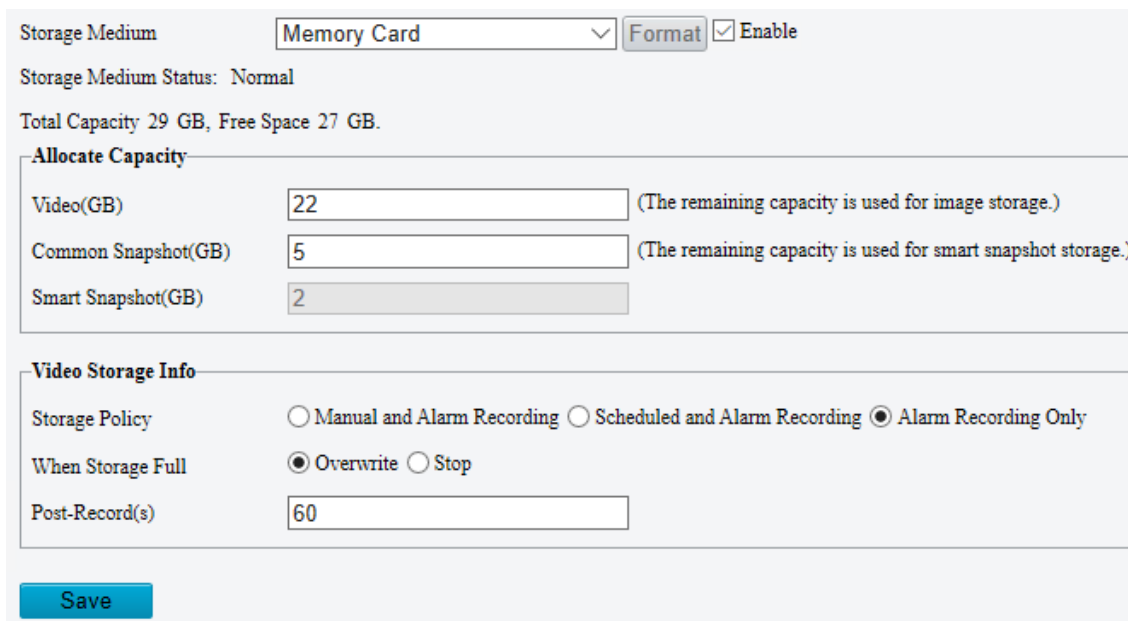
- Disarm Once: Set the disarming time.



4. Choose actions to be disarmed. The actions available, for example, alarm light, alarm sound, email, alarm output, may vary with camera model and version.
5. Click **Save**.

5.7 Storage

Go to **Setup > Storage > Storage**.



5.7.1 Memory Card



NOTE!

Before you use this function, make sure a memory card has been mounted on the camera.

1. Set **Storage Media** to **Memory Card** and select **Enable**.

Item	Description
Storage Medium	Includes Memory Card and NAS .
Storage Management	<p>To format a storage medium such as a memory card, stop using it first.</p> <ul style="list-style-type: none">• Format: Format the storage medium without encryption.• Encrypt&Format: Set an encryption password for the memory card, and then format it. <p>Example: When inserting an unencrypted memory card, to use the memory card encryption function, you must perform Encrypt&Format operation to encrypt the memory card. After encryption, insert the card into other device, if no encryption password is obtained or the password stored in the device is not consistent with the password of the memory card, then storage services such as recording storage, download, and search will not be available.</p> <ul style="list-style-type: none">• Verify: Insert an encrypted memory card, if the password of the memory card is not consistent with the encryption password stored in the device, you can click Verify. When succeeded, you can normally use storage services, such as recording storage, download, and search.• Change Password: You can change the encryption password if the memory card is encrypted.• Storage Medium Status: Displays the health status of the memory card. <p>Note:</p> <ul style="list-style-type: none">• This feature is only available to certain devices. Please refer to the actual interface. <p>To monitor the memory card's health status, use a TF card that supports the health status monitoring function.</p>
When Storage Full	<ul style="list-style-type: none">• Overwrite: When space is used up on the memory card, new data overwrites old data.• Stop: When space is used up on the memory card, the camera stops saving new data.
Post-Record(s)	Sets the duration of alarm-triggered recording after the alarm ended.

2. Allocate storage space as needed.
3. Configure storage information.
 - To store manual recordings and alarm recordings

Choose **Manual and Alarm Recording**. By default, the main stream is stored.

- To store scheduled recordings and alarm recordings
 - (1) Choose **Scheduled and Alarm Recording**.

Storage Policy ☐ Manual and Alarm Recording ☒ Scheduled and Alarm Recording ☐ Alarm Recording Only

Stream

When Storage Full ☒ Overwrite ☐ Stop

Post-Record(s)

(2) The default recording schedule is 24/7. To change the schedule, drag on the calendar or click **Edit**.

☒ Armed ☐ Unarmed

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

- To store alarm recordings only

Choose **Alarm Recording Only**.

Storage Policy ☐ Manual and Alarm Recording ☐ Scheduled and Alarm Recording ☒ Alarm Recording Only

When Storage Full ☒ Overwrite ☐ Stop

Post-Record(s)

5.7.2 Network Disk

Use a Network Attached Storage (NAS) server to store camera videos and snapshots.

1. Set **Storage Medium** to **NAS**.
2. Enter the server address.
3. Enter the path to the destination folder on the NAS server. You can find the path by viewing the folder properties.



NOTE!

For dual-channel cameras, the server address and folder path are the same for the two channels. By default, the folder space is evenly shared by the two channels, among which, 85% space is used to store videos, and 15% is used to store common snapshots. You may change the Channel Total Capacity, video space, and common snapshot space as needed.

Storage Medium

Server IP

Path

Total Capacity 463 GB, Free Space 462 GB.

Select Channel

**NOTE!**

The path name may include the following: letters, digits, dots, spaces, and symbols / : , - _ @ =
Other characters are not allowed and will cause failed NAS test.

4. After the test succeeded, click **Save**.

Storage Medium	NAS	Format
Server IP	192.164.1.180	
Path	/nfs	NAS Test Test succeeded.
Total Capacity 463 GB, Free Space 462 GB.		
Select Channel	Channel1	
Allocate Capacity		
Channel1 <input checked="" type="radio"/> Channel2 <input type="radio"/>		
Channel Total Capacity(GB)	232	Channel Free Space 232 GB
Video(GB)	100	(The remaining capacity is used for image storage.)
Common Snapshot(GB)	35	
Smart Snapshot(GB)	97	
Video Storage Info		
Storage Policy	<input type="radio"/> Manual and Alarm Recording <input type="radio"/> Scheduled and Alarm Recording <input checked="" type="radio"/> Alarm Recording Only	
When Storage Full	<input checked="" type="radio"/> Overwrite <input type="radio"/> Stop	
Post-Record(s)	60	
Save		

5.7.3 FTP

Upload images and videos to an FTP server for storage.

1. Go to **Setup > Storage > FTP**.

Server Parameters

Server IP

0.0.0.0

Port No.

21

Username

Password

Confirm

Upload Images

☐

Upload Video

☐

Test

Convert Path into UTF8...

☐

Photo

Recording

Save To:

File Path

File Name

No.	Naming Element
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable

Note: Overwrite will take place in the current directory.

Save

2. Configure server parameters.

Item	Description
Server IP	IP address of the FTP server.
Port No.	The default is 21. You can set a different port as needed.
Username	Username used to log in to the FTP server.
Password	Password used to log in to the FTP server.
Test	Test the connection to the FTP server.
Upload Images	<p>Select the checkbox if you want to upload common (non-smart) snapshots. To configure an FTP server for smart snapshots, go to Setup > System > Server > Intelligent Server.</p> <p>Overwrite Storage: When the number of images in the folder of the lowest level reaches the threshold, the server continues to save new images by overwriting the existing images. For example, if the folder path is \IP\date, the level-2 folder "date" is the lowest. When the images uploaded on Jan. 4, 2022, exceeds 1,000, existing images in the 20220104 folder will be overwritten by new images.</p> <p>NOTE!</p> <p>If you select Overwrite Storage, make sure the last naming element of filename is Photo No..</p> <p>The default overwrite storage threshold is 1000 images, and the maximum is 100,000 images.</p>
Upload Video	Select if you want to upload alarm-triggered recordings.
Convert Path into UTF8 Format	Select if you want to convert the path into UTF8 format.
Post-Record(s)	Fill in the number of seconds, which is the duration of the alarm-triggered recording after the alarm has ended.

3. Configure the storage path.

Item	Description
Photo	File path, up to 6 levels. If not specified, the default path “\IP\Date\Common” will be used. Common means common snapshots.
	Filename, up to 20 fields are allowed. If not specified, the sequence number such as 1, 2, 3, ... will be used as the filename.
Recording	File path, up to 6 levels. If no path is specified, the default path “\IP\Date\Common” will be used.
	The default filename is “S+recording start time+E+recording end time.” For example, S20220104174903E20220104175002.

4. Click **Save**.

5.8 Security

The security functions available may vary with camera model and version.

5.8.1 User

Go to **Setup > Security > User** to add, edit, or delete users.

The screenshot shows a user management interface with three buttons at the top: 'Add', 'Edit', and 'Delete'. Below these is a table with the following data:

No.	Username	User Type
1	admin	Admin

- Add user.

1. Click **Add**.

Common User

The screenshot shows the 'Add' dialog box for creating a new user. It contains the following fields and options:

- Username:** A text input field.
- User Type:** A dropdown menu currently set to 'Common User'.
- Password:** A text input field with a strength indicator below it showing 'Weak', 'Medium', and 'Strong' levels.
- Confirm:** A text input field for password confirmation.
- Select Permission:** A checkbox that is currently unchecked.
- Live View:** A checkbox that is currently checked.
- Playback:** A checkbox that is currently unchecked.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Operator

Add

Username

User Type **Operator** ▼

Password

Weak Medium Strong

Confirm

☐ **Select Permission**

☐ Parameter... ☒ Live View ☒ Playback ☒ Snapshot ☒ Two-way A...

☒ PTZ Control ☐ Event Subs... ☒ Log ☐ Maintenance ☐ Upgrade

OK Cancel

2. Configure the parameters.

Item	Description
Username	Set the username that you prefer.
User Type	<p>Choose Common User or Operator.</p> <p>NOTE!</p> <ul style="list-style-type: none">Up to 32 users are allowed, including admin (at least one), common users and operators (up to 31).Admin has all permissions in the system, including device operation and user management.Operator has higher privilege than common user and can configure in the web interface.
Password	<p>Enter a password.</p> <p>NOTE!</p> <p>A strong password is required for new user. A strong password shall include 9-32 characters consisting of letters, digits, and special characters.</p>
Confirm Password	Enter the password again.
Select Permission	<p>Different user types have different permissions. Select permissions you want to assign to the new user.</p> <p>NOTE!</p> <p>You can select the Select Permission checkbox to select/deselect all permissions.</p>

3. Click **OK**.

- Edit user information.
- Click the user.
 - Click **Edit**.

Common User

Edit

Username

1111

User Type

Common User

Admin Password

Password

Weak

Medium

Strong

Confirm

Select Permission

Live View

Playback

OK

Cancel

Admin

Edit

Username

admin

User Type

Admin

Old Password

Password

Weak

Medium

Strong

Confirm

Email

Used to reset password. You are recommended to fill in.

Select Permission

Parameter...

Live View

Playback

Snapshot

Two-way A...

PTZ Control

Event Subs...

Log

Maintenance

Upgrade

OK

Cancel

3. Configure the parameters.

Item	Description
Admin Password	Password of administrator, not the user being editing.
Password	Enter a password that you prefer.
Confirm Password	Enter the password again.
Select Permission	<div>Different user types have different permissions. Select permissions you want to assign to the new user.</div> <div>Note</div> <div>You can select the Select Permission checkbox to select/deselect all permissions.</div>

4. Click **OK**.



NOTE!

- Only admin can change the device password. The new password must be different from the old.
- Only admin can change the username and password of a new user. If the user is logged in, the user will log out automatically and must use the new username and password to log in.

- Delete a user.

Click the user, click **Delete**, and then click **OK** to confirm.

5.8.2 HTTPS

Enable HTTPS to securely transmit video data of the camera.

1. Go to **Setup > Security > Network Security > HTTPS**.

HTTPS ☒ On ☐ Off

Server Certificate default

Save



NOTE!

The default HTTPS port is 443. To use a different port, go to **Setup > Network > Port**.

2. Click **On** to enable HTTPS.

3. Log in to the account.

The login page is displayed when HTTPS is enabled. After you log in, a secure transmission channel is established.

4. Click ▼ to choose a server certificate.

HTTPS ☒ On ☐ Off

Server Certificate default

Save

- Use the default certificate.
 - A created certificate. See Certificate Management.
5. Click **Save**.

5.8.3 Authentication

Configure RTSP authentication and HTTP authentication to improve the security of network transmission. Only after successful authentication can data such as videos, audios, text, and images be transferred on the network.

1. Go to **Setup > Security > Network Security > Authentication**.

2. Choose an authentication mode.

Item	Description
RTSP Authentication	<p>Choose an authentication mode from the drop-down list. The default is Digest.</p> <ul style="list-style-type: none"> • Basic: Basic authentication. The username and password are encrypted by base 64, which imposes serious security risks. • Digest: Digest authentication. Displays RTSP digest algorithm configuration. The default is MD5. <ul style="list-style-type: none"> ➢ Digest MD5: Digest authentication, which uses MD5 to protect the username, password, and domain of the requester, not transferred on network in plaintext and provides higher security. ➢ Digest SHA256: Digest authentication, which uses SHA256 for authentication and provides higher security than Digest MD5. ➢ Digest MD5/ SHA256: Supports MD5 or SHA256 algorithm adaptation. • None: Transmit message without authenticating the RTSP address.
Web Authentication	<p>Choose an authentication mode from the drop-down list. The default is Digest.</p> <ul style="list-style-type: none"> • Digest: Digest authentication. Displays Web digest algorithm configuration. The default is MD5. <ul style="list-style-type: none"> ➢ Digest MD5: Digest authentication, which uses MD5 to protect the username, password, and domain of the requester, not transferred on network in plaintext and provides higher security. ➢ Digest SHA256: Digest authentication, which uses SHA256 for authentication and provides higher security than Digest MD5. ➢ Digest MD5/ SHA256: Supports MD5 or SHA256 algorithm adaptation. • None: Transmit message without authenticating the Web address.

3. Click **Save**.

5.8.4 Registration Information

You can set to hide vendor information of the camera from the server.

1. Go to **Setup > Security > Registration Information**.
2. Enable **Hide Vendor Info**. Vendor information will not be displayed on the management platform.

3. Click **Save**.

5.8.5 ARP Protection

Configure ARP protection by binding the gateway's IP address with its MAC address to prevent ARP spoofing attacks.

1. Go to **Setup > Security > Network Security > ARP Protection**.

ARP Protection ☒ On ☐ Off

Gateway

Gateway MAC Address

Save

2. Enable **ARP Protection**.
3. Enter the gateway's MAC address.
4. Click **Save**.

5.8.6 IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP addresses.

1. Go to **Setup > Security > Network Security > IP Address Filtering**.

IP Address Filtering ☐ On ☒ Off

Filtering Mode

No.	IP Address	+

Save

2. Enable **IP Address Filtering**.
3. Choose **Allow** or **Forbid** to filter IP addresses. When **Allow** is selected, access is allowed only from the added IP addresses. If **Forbid** is selected, access is forbidden from the added IP addresses.
4. Click **+**, enter IP addresses.
 - Up to 32 IP addresses can be added. Duplicate addresses are not allowed.
 - The first byte of the IP must be 1-233, and the fourth byte cannot be 0. Invalid IP addresses such as 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not allowed.
5. Click **Save**.

5.8.7 Access Policy

Access policies are used to prevent unauthorized access and operation from the network.

1. Go to **Setup > Security > Network Security > Access Policy**.

- Illegal Login Lock

Illegal Login Lock

Illegal Login Lock ☒ On ☐ Off

Illegal Login Limit

Lock Time (min)

Save

**NOTE!**

By default, illegal login lock is enabled, and the account will be locked for 5 minutes after 5 consecutive failed login attempts due to a wrong password. If illegal login lock is disabled, the camera will not lock the account no matter how many times an incorrect password is input.

Item	Description
Illegal Login Lock	<p>If the client IP address is not on the blocklist, the input username is correct, but the input password is wrong, it is an illegal login attempt.</p> <p>NOTE!</p> <ul style="list-style-type: none"> When an account is locked, information including the username, IP address, etc, is logged by the system. The user can unlock the account by disconnecting power and rebooting the camera.
Illegal Login Limit	<p>The maximum number of illegal login attempts allowed. Range: 2-10.</p> <p>The account is locked when the limit is reached.</p>
Lock Time (min)	Integer within the range of 1-120.

Example: User A tries to log in from the client IP address 192.168.1.33 and is locked. Then user A cannot log in within the lock time, but user B is not affected and can still log in from the same IP address.

- Session timeout

A session is the connection established between the client (Web browser) and the server (camera). When session timeout is enabled, if the client cannot obtain or save configurations within the set time, the user will automatically log out and go to the login page.

**NOTE!**

Only admin can enable or disable this feature.

The image shows a configuration window titled "Session Timeout". It contains a "Session Timeout" label with a radio button set to "Off" (the "On" option is also visible). Below this is a "Timeout (min)" label with a slider control and a numeric input field showing the value "5".

Item	Description
Session Timeout	<p>Sessions are counted as follows. Take one device as an example.</p> <ul style="list-style-type: none"> If the session is established using one web browser from one client IP, there is one session. If sessions are established using one web browser from one client IP, there are two sessions. If sessions are established using two web browsers from two client IPs (two browsers from each IP), there are four sessions. <p>NOTE!</p> <p>Up to 36 sessions are allowed at the same time.</p>
Timeout (min)	<p>Enter an integer within the range of 1-120.</p> <p>NOTE!</p> <p>The timer restarts when the session is re-established after a reboot.</p>

2. Click **Save**.

- Friendly password

Users are not affected when friendly password is enabled. When friendly password is disabled, users who are already logged in with a weak password will be forced to set a strong password before the user can proceed with other actions in the web interface.



NOTE!

Friendly password is not available to all cameras.

5.8.8 Certificate Management

On the **Certificate Management** page, you can create and manage certificates, view certificate properties, etc.

1. Go to **Setup > Security > Network Security > Certificate Management**.

1. Certificate

1. Create a self-signed certificate or import a certificate.
 - Create a self-signed certificate for application scenarios with low-security requirements.

- (1) Click **Create Self-Signed Certificate**.
- (2) Complete the settings.

Item	Description
Certificate Name	Set a name as needed.
Public Key	Choose a length for the public key: 2048 or 1024. Default: 2048.
Country	Enter the two-character country code, for example, CN for China.

Item	Description
Domain Name/IP	Enter the device's IP address or domain name.
Valid Period(day)	Enter the validity period of the certificate.
Province	Enter the complete province name.
City	Enter the complete city name.
Organization	Enter the organization name.
Organizational Unit	Enter the organizational unit name.
Email	Enter a valid email address of the contact.

(3) Click **OK**.

- Import a non-CA certificate.

(1) Click **Import Certificate**.

(2) Complete the settings.

Item	Description
Import Format	You may choose Certificate+Private Key , PKCS#12 , or Self-Signed Request Certificate .
Certificate Name	Enter the certificate name.
Certificate	Click Browse and locate the certificate.
Private Key	Click Browse and locate the private key.
Private Key Password	Enter the private key password.

(3) Click **OK**.

2. (Optional) Create a certificate request to obtain a trusted signed certificate for application scenarios with high-security requirements.



Create Certificate

Country Example:CN

Domain Name/IP

Province

City

Organization

Organizational Unit

Email

OK Cancel

- (1) After creating or importing a certificate, select the certificate, click **Create Certificate Request**.
- (2) Complete the settings.
- (3) Click **OK**.



NOTE!

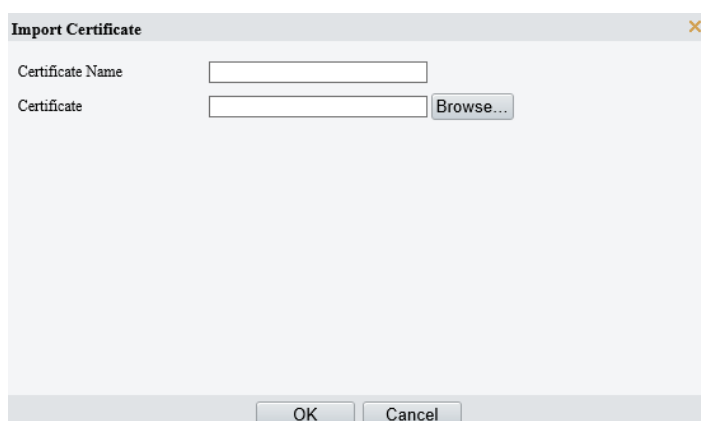
After the certificate request is created, export the certificate request file. After the certificate authority (CA) signs and issues a certificate in accordance with the request, import the certificate into the device.

- Export certificate.
Click **Export Certificate** to save the certificate to your computer.
- Delete certificate.
Select a certificate and delete it. A certificate that is in use cannot be deleted.
- View certificate properties.
Select a certificate to view its properties.

2. CA Certificate

A CA certificate is a certificate issued by a trusted certificate authority (CA) and thus is more secure and reliable.

1. Click **Import Certificate**.
2. Enter the certificate name, select the certificate.



Import Certificate

Certificate Name

Certificate Browse...

OK Cancel

3. Click **OK**.
- Delete certificate.
Select a certificate and delete it. A certificate that is in use cannot be deleted.
 - View certificate properties.
Select the certificate to view its properties.

5.8.9 Watermark

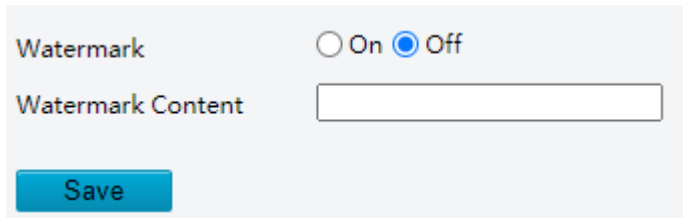
Use watermark to encrypt custom information in videos to prevent tampering.



NOTE!

- Watermarks can be verified using Guard Player.
- For devices with two video channels, watermark parameters need to be configured for the channels separately.

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



2. Enable **Watermark**.
3. Set watermark contents, which may include uppercase letters, lowercase letters, and digits. Up to 16 characters are allowed.
4. Click **Save**.

5.9 System



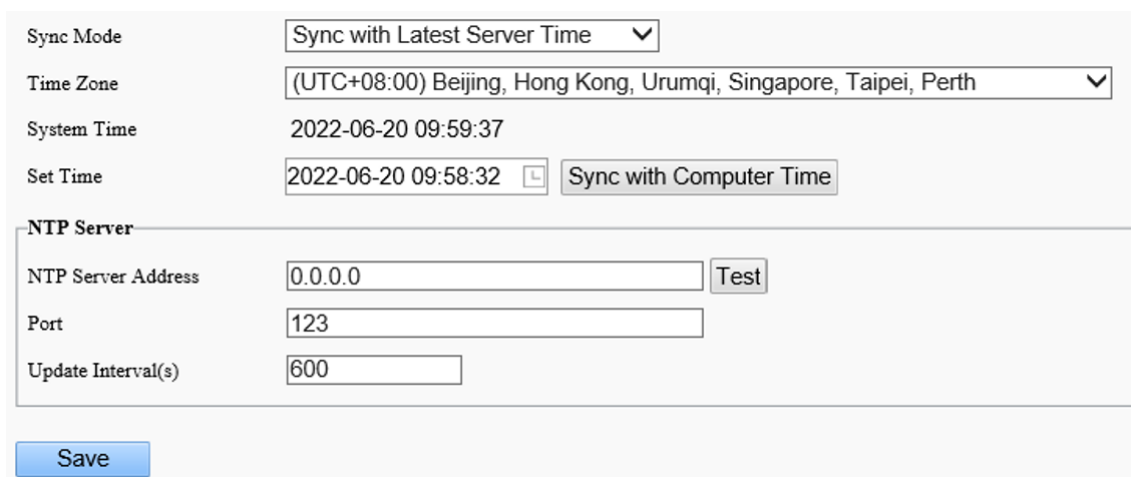
NOTE!

User operations in this module may vary with camera model.

5.9.1 Time

Set the device's system time manually or sync it with a server.

1. Go to **Setup > System > Time**.



2. Set the system time.
 - Set manually in the **Set Time** field.



NOTE!

When setting the system time manually, you need to set **Sync Mode** to **Sync with System Configuration**; otherwise, the camera will still sync with other time sources after you set it manually.

- Sync time.

Item	Description
Sync with System Configuration	Default. Time provided by the system's built-in time module.
Sync with Latest Server Time	The camera regularly syncs time with all the connected servers.
Sync with Management Server(Non-ONVIF)	The camera regularly syncs time with the server that is not connected via Onvif.
Sync with Management Server(ONVIF)	The camera regularly syncs time with the server that is connected via Onvif.
Sync with NTP Server	The camera syncs time with the NTP server. You need to configure the server address, port, and update interval (range: 30s-86400s). You can click Test to test it.
Sync with Cloud Server	The camera syncs time with the cloud server once it gets online. The camera does not sync again until it gets offline and online again.
BeiDou Module Auto Sync	The camera syncs time with BeiDou satellites through the BeiDou module (if equipped).
Sync with Computer Time	The camera syncs time with the client computer from which you log in to the camera.

3. Click **Save**.

5.9.2 DST

1. Go to **Setup > System > Time > DST**.

2. Enable DST, and set the start time, end time, and DST bias.
3. Click **Save**.

5.9.3 Alarm Server

The camera can automatically report alarms to a specified third-party server. You need to configure the server IP, port, and protocol, then the camera can report alarms to the server.

1. Go to **Setup > System > Server > Alarm Server**.

2. Select **Enable Alarm Server**.

3. Set the server IP and port, then click **Test** to check if the server is available.
4. Choose a protocol: **HTTP** or **HTTPS**.
5. Click **Save**.

5.9.4 Device Information

Set device information including device name, location, mounting height, etc., which can be used in smart FTP, OSD, etc.

1. Go to **Setup > System > Device Info**.

Device Name	<input type="text" value="1"/>					
Device ID	<input type="text" value="1"/>					
Intersection Info	<input type="text" value="road"/>					
Intersection ID	<input type="text"/>					
Direction ID	<input type="text" value="1"/>					
Mounting Height (cm)	<input type="text" value="600"/>					
Longitude	<input type="text" value="East"/>	<input type="text" value="0"/>	Degrees	<input type="text" value="0"/>	Minutes <input type="text" value="0.0000"/>	Seconds
Latitude	<input type="text" value="North"/>	<input type="text" value="0"/>	Degrees	<input type="text" value="0"/>	Minutes <input type="text" value="0.0000"/>	Seconds

2. Complete the information as needed.
3. Click **Save**.

5.9.5 Maintenance

1. Maintenance

System maintenance includes software upgrade, system configuration, diagnosis information, power output, and heater settings.

Go to **Setup > System > Maintenance**.

- Software upgrade



NOTE!

- Make sure the version to be used matches the device; otherwise, exceptions may occur.
- The version file is a .zip file that includes all the upgrade files.
- Power must be connected throughout the upgrade.

➤ Local upgrade

(1) Click **Browse**, locate the version. (If applicable) select **Upgrade Boot Program** to upgrade the boot program.

(2) Click **Upgrade** to start. The device will restart automatically after the upgrade is completed.

➤ Peripheral upgrade

Check for upgradable peripherals such as pan/tilt unit, illuminator, etc., and available versions.

➤ Cloud upgrade

Click **Detect** to check for new versions. You can perform a cloud upgrade if a new version is available on the cloud server.

- System configuration

You can export the current configurations of the camera to the client computer or an external storage device for backup, so, when necessary, you can restore camera configurations by importing the backup file.



CAUTION!

- Restoring defaults will restore all settings to factory defaults except the administrator password, network interface settings, and system time.
- Before you import a configuration file, make sure the file matches the camera model; otherwise, unexpected results may occur.
- The camera will restart after importing the configuration file.

➤ Import configurations.

The image shows a 'Config Management' window. It has a 'Default' button and a checkbox labeled 'Restore all settings to defaults without keeping current network and user settings.' Below this are two rows: 'Importing' and 'Exporting'. Each row has a text input field, a 'Browse...' button, and an 'Import' or 'Export' button.

- (1) Click **Browse** beside the **Import** button.
- (2) Locate the configuration file, click **Import**. A dialog box appears.
- (3) Enter the password and confirm.
- (4) Click **OK**.

➤ Export configurations.

- (1) Click **Browse** beside the **Export** button.
- (2) Choose the destination folder, click **Export**. The **File Encryption** dialog box appears.
- (3) Enter the password and confirm.
- (4) Click **OK**.

➤ Restore defaults.

Click **Default**. The system will restore default settings except network settings and user settings.

To restore all settings, select **Restore all settings to defaults without keeping current network and user settings**.

- Diagnosis information

Diagnosis information includes logs and system configurations and can be exported to your client computer. Select **Collect Image Debugging Info** to collect diagnosis information with accompanying video images to facilitate troubleshooting.

The image shows an 'Export Diagnosis Info' window. It has a text input field, a 'Browse...' button, and an 'Export' button. Below the input field is a checkbox labeled 'Collect Image Debugging Info' which is checked.

- (1) Click **Browse** and choose the destination.
- (2) Click **Export**.



NOTE!

Diagnosis information is exported as a compressed file. You need to decompress it first (using decompression tools like WinRAR) and then open the file using a text editor (like Notepad).

- Power output

The camera can supply power to external devices with lower power consumption such as a sound pickup.

The image shows a 'Power Output' window. It displays '12 VDC' and two radio buttons labeled 'On' and 'Off'. The 'Off' button is selected.

- Restart device.



CAUTION!

Restarting the camera will interrupt the ongoing service.

Restart

Restart device

Click **Restart** and then confirm to restart the device. You may set a schedule to reboot the camera automatically at the set time.

- Heater

Use the heater to eliminate water droplets on the lens in a high humidity environment.

Heater

☐ On
 ☒ Off

Remaining Heating Time

 Day(s)

 Hour(s)

 Minute(s)

(1) Enable Heater.

(2) Set **Remaining Heating Time**.

2. Network Diagnosis

Go to **Setup > System > Maintenance > Network Diagnosis**.

Select NIC

NIC1 (203.2.1.83) ▼

IP Filter

☒ All
 ☐ Specify
 ☐ Filter

Port Filter

☒ All
 ☐ Specify
 ☐ Filter

☐ Custom Rules

Start Capture

- Select NIC

NIC1 is the camera's IP address.

- IP/port filter

- All: Capture all packets of the camera.
- Specify: Capture packets of the specified port or IP.
- Filter: Filter packets of the specified port or IP and capture other packets.

- Custom Rules

Select **Custom Rules** and set the rules.

Click **Start Capture** to start capturing packets. After packet capture is finished, save data, and view the diagnosis.

- Test network delay and packet loss rate.

Test network connectivity by sending test packets to a test address.

Network Delay and Packet Loss Test

Test Address

192.168.1.1

Packet Size (Bytes)

64

Test Result

Average Delay: 3.558 ms Packet Loss Rate: 0%

Test

- Test Address: Must be a valid IP address or domain name.
- Packet Size (Bytes): Size of test packets to be sent. Range: [64-65507]. Sometimes a high delay may be caused by a large packet size. If the test failed, set a smaller packet size, and then try again.

- Test results include average delay and packet loss rate.
 - Average delay: Average length of time from test packets are sent till responses are received.
 - Packet loss rate: Ratio of lost packets to the sent packets.

5.9.6 Logs

Search camera operation logs and download them to your computer.

Go to **Setup > System > Log**.

Time

2022-06-09 00:00:00 ~ 2022-06-09 23:59:59

Main Type

AlarmEvent

Sub Type

All

Operation

Query

Export

No.	Type	Sub Type	Date	Time	Username	IP	Result
1	Operator	Login	2022-06-09	10:25:05	admin	192.168.1.1	Succeeded.
2	Operator	Upgrade	2022-06-09	10:18:25	admin	192.168.1.1	Succeeded.
3	Operator	Login	2022-06-09	10:05:29	admin	192.168.1.1	Succeeded.

Total 3

<< < 1 > >>

4. Set a time range and choose main and sub log types.
 - Main type: Including system operation, alarm parameter configuration, network configuration, audio, and video configuration, PTZ configuration, image configuration, smart configuration, system configuration, storage configuration, and alarm events.
 - Sub type: You can choose up to 5 types or choose All.
5. Click **Search**. Up to 100 logs can be displayed. The latest logs are displayed on the top.
6. Click **Export** to save search results as a .csv file to the client computer.