Applicable Models

The following table lists the camera models to which this document is applicable.

Table 1 Applicable models

Camera Type	Model	Appearance
Bullet camera	HWT-D2122-10-SIU	
	HWT-D2152-10-SIU	
Fixed dome camera	HWT-D3040-10-ELI-PV (2.8 mm)	
	HWT-D3222-10-SIU	
	HWT-D3252-10-SIU	
PTZ dome camera	HWT-D6550-10-Z33-SV	

Camera Type	Model	Appearance

NOTE

To support some intelligent analysis functions, the camera must be upgraded to the latest version.

Planning Principles

This topic describes specifications, experience, and suggestions on engineering planning and design.

Data Planning Suggestion Before installing devices, plan camera installation information based on the site requirements.

Network and Bandwidth Requirements
Smart cameras carry multiple services, such as video recording, live video viewing, and signaling transmission. Therefore, you need to calculate the network bandwidth in advance and reserve proper bandwidth during device deployment.

Data Planning Suggestion

Before installing devices, plan camera installation information based on the site requirements.

Parent topic: Planning Principles

Network and Bandwidth Requirements

Smart cameras carry multiple services, such as video recording, live video viewing, and signaling transmission. Therefore, you need to calculate the network bandwidth in advance and reserve proper bandwidth during device deployment.

Network Requirements

Table 1 describes the network requirements for ensuring the service quality. Select a switch and plan the network based on the following requirements. Before installing a camera, use a packet capture tool to check the network conditions and ensure that the live video fluency will not be affected by the network.

Table 1 Network requirements

Network Reliability	Requirement
Packet loss rate (LAN)	< 5% in TCP mode; no packet loss in UDP mode
Packet loss rate (WAN)	< 5% in TCP mode; no packet loss in UDP mode
Delay	< 150 ms
Jitter	< 20 ms

NOTE

- Requirements on network reliability parameters are used to ensure service quality only in scenarios where only one network impairment occurs. For example, if only packet loss occurs on the network and no delay or jitter occurs, little impact is imposed on services in the case of less than 5% packet loss rate. If both 5% packet loss and 150 ms delay exist on the network, the service quality cannot be ensured.
- If a burst network impairment exists or multiple network impairments exist simultaneously, the service quality cannot be ensured. In this case, troubleshoot the network fault in a timely manner.

Bandwidth Requirements

The uplink bandwidth required by each node is calculated based on the actual service model. The service model is complex and the calculation is hard to cover every aspect of the model, so only simple calculation is performed.

- Bandwidth required by a common camera = (Encoding bit rate x Number of stream channels x A+ Number of video buffering channels x B) x Reserved bandwidth coefficient
- Bandwidth required by an intelligent camera = (Encoding bit rate x Number of stream channels x A + Number of video buffering channels x B + Size of an image x Number of images uploaded per second x 8 + Size of an image uploaded through FTP/SFTP x Number of images uploaded per second x 8) x Reserved bandwidth coefficient (The size of an image can be obtained based on the test in an actual scenario.)
- Bandwidth required by the 1 + N networking = Bandwidth required by the primary camera + Bandwidth required by secondary camera 1 + Bandwidth required by secondary camera 2 + ... + Bandwidth required by secondary camera *N* Bandwidth required by secondary camera *N* = (Encoding bit rate x Number of stream channels x A + Number of video buffering channels x B + Size of an image x Number of images uploaded per second x 8 + Size of an image uploaded through FTP/SFTP x Number of images uploaded per second x 8) x Reserved bandwidth coefficient (The size of an image can be obtained based on the test in an actual scenario.)
- Bandwidth required by a 5G camera = (Encoding bit rate x Number of stream channels + Size of an image x Number of images uploaded per second x 8) x Reserved bandwidth coefficient (The size of

an image can be obtained based on the test in an actual scenario. The reserved bandwidth coefficient is set to 1 in wireless transmission scenarios.)

NOTE

- Captured images can be uploaded as metadata (including captured images and structured data) or in FTP/SFTP mode. The metadata mode is used to upload captured metadata to the video security platform when the camera is connected to the video security platform through the SDK. The FTP/SFTP mode is used to upload captured images to the server specified by the customer through FTP/SFTP. Cameras support simultaneous upload in both modes. In most application scenarios, either metadata or FTP/SFTP upload mode is used. When calculating the total bandwidth by referring to Table 4, count in the metadata upload bandwidth and FTP/SFTP upload bandwidth. When calculating the actual network bandwidth, determine the image upload mode and then calculate the bandwidth based on the image upload mode.
- Metadata upload bandwidth and FTP/SFTP upload bandwidth need to be converted as follows: 1 MB/s = 8 Mbit/s.
- In FTP/SFTP mode, only captured images are uploaded. In metadata mode, both captured images and structured data are uploaded. The structured data is small in size. Therefore, the FTP/SFTP upload bandwidth and the metadata upload bandwidth are the same during the calculation.
- During the calculation of the metadata upload bandwidth by referring to Table 4, the number of images captured per second is 2, which is the average value. During bandwidth calculation, you need to estimate the number of images captured per second based on the actual scenario and calculate the bandwidth required by metadata or FTP/SFTP upload.
- For 5G cameras, you are advised not to enable video buffering and FTP/SFTP image upload functions in wireless transmission scenarios. Therefore, the bandwidth for video buffering and FTP/SFTP image upload is not considered during bandwidth calculation.

- If the overall network bandwidth cannot meet the requirements, increase the network bandwidth or lower the camera's requirements on the bandwidth by lowering the snapshot quality, increasing the SD card capacity, or reducing the snapshot resolution.

The following describes the parameters in the preceding formula:

- Encoding bit rate: This parameter is set by users. For details about the setting method, see Setting Video Parameters. Table 2 lists the recommended bit rate for each video format.

Table 2 Encoding bit rate corresponding to each video resolution

Video Resolution	Recommended Bit Rate (Mbit/s) (H.265)
CIF	-
D1	1
720p	1–4
1080p	2–8
3MP	3–8
4MP	5–10
5MP	6–10
6MP	6–12
4K	10–12
9MP	12–14

NOTE

The encoding bit rate range listed in Table 2 is obtained from the empirical values in specific scenes. The specific bit rate range is affected by scene complexity. A higher scene complexity indicates a higher bit rate. For example, at intersections where pedestrians and vehicles may appear at the same time, the bit rate is high. In an open square, the bit rate is low. When planning the network bandwidth, you are advised to use the default value in the bit rate range. If the onsite network bandwidth is insufficient, you are advised to perform test first to obtain the typical and maximum bit rates on site and then plan the network bandwidth.

- Number of stream channels: indicates the total number of video stream channels.
- A: 1 + SEC bit rate. A larger packet loss rate indicates a higher SEC bit rate, that is, higher additional bandwidth required. Five levels of the packet loss rate are available. You need to select a packet loss rate based on the actual network quality. Table 3 lists data of A. Setting Super Error Concealment Parameters describes the SEC parameters.

Table 3 Mappings between packet loss rates and SEC bit rates

Packet Loss Rate	SEC Bit Rate (Percentage of Extra Bandwidth Required)	A
4%	35%	135%
8%	50%	150%
12%	70%	170%
16%	85%	185%
20%	100%	200%+

- B: indicates the video buffering backhaul rate. For details about how to configure the video buffering backhaul rate limit, see Configuring Storage Management.
- Reserved bandwidth coefficient: Generally, the value ranges from 1.2 to 1.5 (1.5 is recommended). The value depends on the network quality.

Bandwidth Calculation Example

Example:

- A common camera on the current node is connected to a platform, uses the 1080p (H.265) video format, 4 Mbit/s bit rate, enables the video buffering function with the default 2 Mbit/s backhaul rate and 20% packet loss rate, and enables the SEC function. The reserved bandwidth coefficient is 1.5. Therefore, the bandwidth is calculated as follows: Bandwidth required by a single node = [4 Mbit/s x 1 x (200%) + 2 x 1 Mbit/s] x 1.5 = 15 Mbit/s
- Table 4 illustrates the method for calculating the network bandwidth corresponding to each resolution of intelligent cameras. The video buffering backhaul rate uses the default value 2 Mbit/s, and the packet loss rate is 20%. The SEC function is enabled. The reserved bandwidth coefficient is 1.2.

Table 4 Bandwidth calculation example

Camera Type	Video Stream Bandwidth					Metadata Upload Bandwidth				FTP Upl Bar
	Resolution	Encoding Bit Rate	Video Buffering Rate	Number of Stream Channels	Number of Video Buffering Channels	Snapshot Size	Number of Snapshots Taken Per Second	Metadata Generation Rate	Number of Metadata Uploading Channels	
1080p camera	1080p	4 Mbit/s	2 Mbit/s	1	1	1.5 MB	2	1.5 x 2 x 8 = 24 Mbit/s	1	San the met uplo ban
3MP camera	3MP	6 Mbit/s	2 Mbit/s	1	1	1.5 MB	2	1.5 x 2 x 8 = 24 Mbit/s	1	San the met uplo ban
4MP camera	4MP	6 Mbit/s	2 Mbit/s	1	1	1.5 MB	2	1.5 x 2 x 8 = 24 Mbit/s	1	San the met uplo ban
5MP camera	5MP	8 Mbit/s	2 Mbit/s	1	1	2 MB	2	2 x 2 x 8 = 32 Mbit/s	1	San the met uplo ban
6MP camera	6MP	10 Mbit/s	2 Mbit/s	1	1	3 MB	2	3 x 2 x 8 = 48 Mbit/s	1	San the met uplo ban
4K camera	4K	12 Mbit/s	2 Mbit/s	1	1	4 MB	2	4 x 2 x 8 = 64 Mbit/s	1	San the met uplo ban
9MP camera	9MP	12 Mbit/s	2 Mbit/s	1	1	4 MB	2	4 x 2 x 8 = 64 Mbit/s	1	San the met

Site Survey

To ensure detection and analysis accuracy, site survey planning and design are required before the installation. Do not move cameras after installation. Otherwise, the detection effect may be affected.

Detection in Access Control Mode

Behavior Analysis

Detection of Electric Bikes in Elevators

Crowd Flow Analysis

Object Classification

1 + N

Appendix

Detection in Access Control Mode

Factors Affecting Target Detection

Site Selection and Installation Requirements

Parent topic: Site Survey

Factors Affecting Target Detection

Target Size

Table 1 describes the requirements for target size.

Table 1 Target size

Target Resolution	Check Method
• To meet target capture requirements, the minimum resolution of a captured target is 26 x 26 pixels. • To achieve an ideal image effect, the target resolution requirements vary depending on the camera focal length. It is recommended that the target resolution meet the following requirements: ▪ For short-focus (12 mm or less) cameras: ≥ 80 x 80 pixels ▪ For medium- and long-focus (more than 12 mm) cameras: ≥ 120 x 120 pixels	For details, see How Do I Check the Target Size?. If the target resolution does not meet the requirements, perform the following operations: • Motorized zoom cameras: Log in to the camera web system. On the **View** page, click  or  to adjust the focal length to make the target image as clear as possible. If the captured image is not clear enough, you can click  or  to adjust the focal point to the position marked in the red frame to increase the image clarity. • Non-motorized zoom cameras: Manually adjust the focal length or installation position by referring to How Do I Adjust Views from Non-Motorized Zoom Cameras?. • For prime lens cameras, adjust the camera installation position.

Target Orientation Angle

- A target can be captured only when the yaw angle is within the range of –30° to +30° and the pitch angle is within the range of –15° to +15°, as shown in Figure 1.
- The camera installation location, angle, and height must meet specific requirements. For details, see Site Selection and Installation Requirements.

  Figure 1 Target deviation



Light Conditions

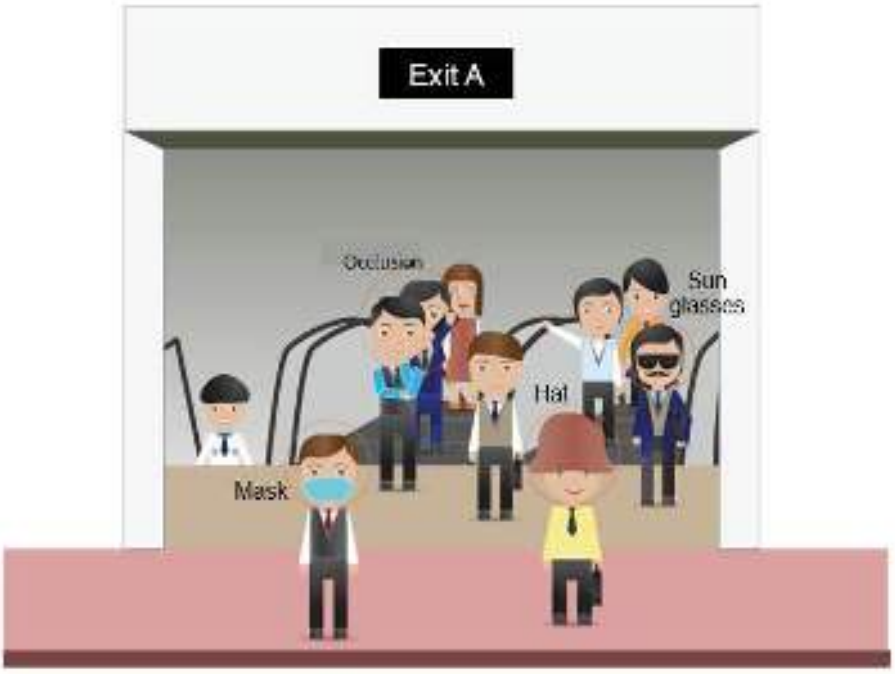
Light conditions dramatically affect the quality of target images. The illumination range required for target capture is 70 lux to 900 lux (can be measured by using an illuminometer or other instruments). Do not install cameras in intense light conditions. In dim light conditions, light compensation is required.

Other Factors

In actual application scenarios, persons may wear sunglasses, masks, or hats, or be occluded by other persons, as shown in Figure 2. This may result in repeated or missed snapshots. In scenarios where persons are occluded by personal belongings such as sunglasses, masks, and hats, the target detection effect may not be improved through camera commissioning. In scenarios with target occlusion problems, if the occluded part exceeds 20% of an entire

target, you can increase the installation height and appropriately tilt down cameras to reduce repeated or missed snapshots.

Figure 2 Target occlusion



Parent topic: Detection in Access Control Mode

Site Selection and Installation Requirements

To ensure the snapshot quality in practical applications, target capture requirements must be satisfied in order for optimized capture accuracy. However, the image quality is greatly affected by how and where cameras are installed. This section describes the precautions and principles for camera installation.

Proper camera installation height and tilt angle can help capture high-quality images with acceptable target resolution and orientation angle, and avoid target occlusion. That is, people of all heights can be successfully captured. Figure 1 and Figure 2 show camera installation requirements and target capture simulation during detection, respectively.

Figure 1 Camera installation requirements

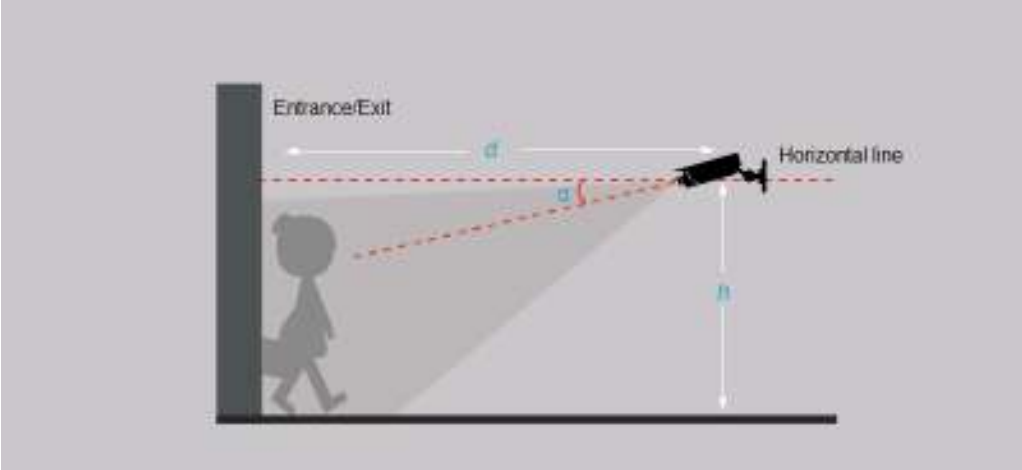
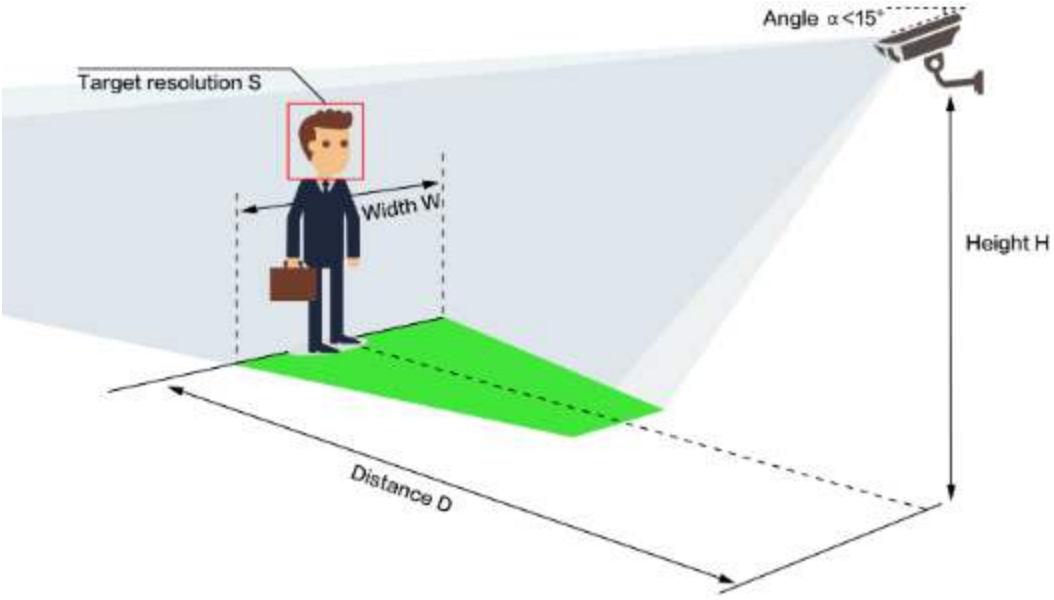


Figure 2 Target detection diagram



Installation Position

The camera should be installed directly in front of a walkway and face pedestrians to ensure a better capture effect. For details, see Factors Affecting Target Detection.

Target Resolution Requirements

Requirements for captured target resolution vary between cameras with different focal lengths. It is recommended that the target resolution meet the following requirements:

- For short-focus (12 mm or less) cameras: ≥ 80 x 80 pixels
- For medium- and long-focus (more than 12 mm) cameras: ≥ 120 x 120 pixels

Installation Height

The recommended installation height ranges from 2.5 m to 3 m. The installation height varies between cameras with different focal lengths.

Tilt Angle

The recommended tilt angle (α) is 15°. Cameras with large tilt angles may capture only the top of people's heads, hindering backend-based target recognition. You need to adjust the tilt angle based on site requirements during camera installation.

Parent topic: Detection in Access Control Mode

Behavior Analysis

Cameras support the following behavior analysis functions: intrusion detection, loitering detection, tripwire crossing detection, area entry detection, area exit detection, fast movement detection, and parking detection. The camera installation requirements and site survey planning for these detection functions are basically the same.

Application Scenario

The perimeter detection function is mainly applied in the following scenarios. For details, see Table 1.

Table 1 Scenario examples

Scenario	Recommended Scenario Example	Non-Recommended Scenario Example
Corridors and halls	 There is no direct strong light in the corridor or no serious light refection from the floor.	 The camera shoots at the window. Light from outside the window and light reflection from the floor will affect detection.
Squares	 • There are few obstacles, for example, trees, in the live view.	 • There are obstacles, for example, trees, in the live view.

Scenario	Recommended Scenario Example	Non-Recommended Scenario Example
	• There is no direct strong light radiation or light reflection.	• The detection area is not in the center of the image and is too narrow.
Campus perimeters	 • There are few obstacles, for example, trees, in the live view. • The detection area is located in the center of the image.	 • The camera angle is improper. There are too many obstacles, such as the sky and walls, in the live view. • The resolution of the object width at the farthest point of the detection area is too low, which affects the detection effect.
Railways	 • There is no interference near the camera. • Avoid large obstacles in the field of view.	 There are wire poles in the detection area, affecting the detection effect.
Parking	 Do not park vehicles on fire routes.	 The road conditions are complex, which will affect parking violation detection effect.

Installation Environment Requirements

Illuminance: 70 lux or higher

If the illuminance is lower than 70 lux at night, you need to install external illuminators or enable the built-in illuminator or infrared lamp depending on the camera capability.

- In scenarios with sufficient light at night, such as corridors and halls, the illuminance requirement (at least 70 lux) can be met.
- In scenarios with low light at night, such as campus perimeters, it is difficult to meet the illuminance requirement.

Direction of light:

- Avoid direct exposure to a strong light. After the installation is complete, the camera lens should not be directly exposed to a strong light (such as sunlight and street lamps).
- Avoid light reflection. Keep the camera away from highly reflective objects such as glasses, ceramic tiles, waters, leaves, guideboards, and advertising signs.
- Avoid backlight scenarios. In backlight scenarios, the background is too bright, while the target or person is too dark, which affects the detection effect.

Others

- Avoid scenarios with sudden light changes, camera shaking, or image switchover that may cause unstable images.
- If there are many flying insects at night, the detection accuracy of the camera will be affected. In this case, you are advised to install insect repellent devices.
- Keep the camera away from irrelevant objects such as leaves, advertising signs, and pillars to ensure continuous tracking of detected objects, as shown in Figure 1 and Figure 2.



Figure 1 Fewer plants

Figure 2 Wild area without obstacles



Incorrect installation site example

Figure 3 shows an example of an incorrect installation site.

Figure 3 Incorrect installation site



Installation Height, Angle, and Distance

Installation Height

Recommended installation height: 3 m to 6 m

Installation Angle

The vertical angle of the camera should range from 5° to 45°. The recommended vertical angle is between 30° and 45°, ideally 30°. It is difficult to measure the angle on site. You can adjust the angle according to the installation height and distance.

Adjust the camera angle or focal length to ensure that the detection area is located in the required area. It is recommended that the detection area be in the center of the image, as shown in Figure 4.

- D1 and D2 are about one fourth of the image height.
- D3 and D4 are about one fourth of the image width.

Figure 4 Detection area example



Installation Distance

Distance from the camera installation position to the bottom of the live video image: The value varies depending on the camera model.

To ensure the detection effect, the resolution of an object's shortest side should meet certain requirements (For details, see Table 2.), and cannot exceed half of the image height or width. For example, if the video resolution is 1920 x 1080 pixels, an object's shortest side must be greater than 24 pixels.

Table 2 Requirements of objects' shortest side under different video resolutions

Video Resolution	Minimum Resolution of an Object's Shortest Side
1920 x 1080	24
2560 x 1920	32
3840 x 2160	64

Viewing Results

Check whether the resolution of the object in the detection area meets the requirements. For example, if the video resolution is 1920 x 1080 pixels, the short side of the object should be greater than 24 pixels. If the resolution is too low, adjust the vertical angle and focal length of the camera.

The detailed procedure is as follows:

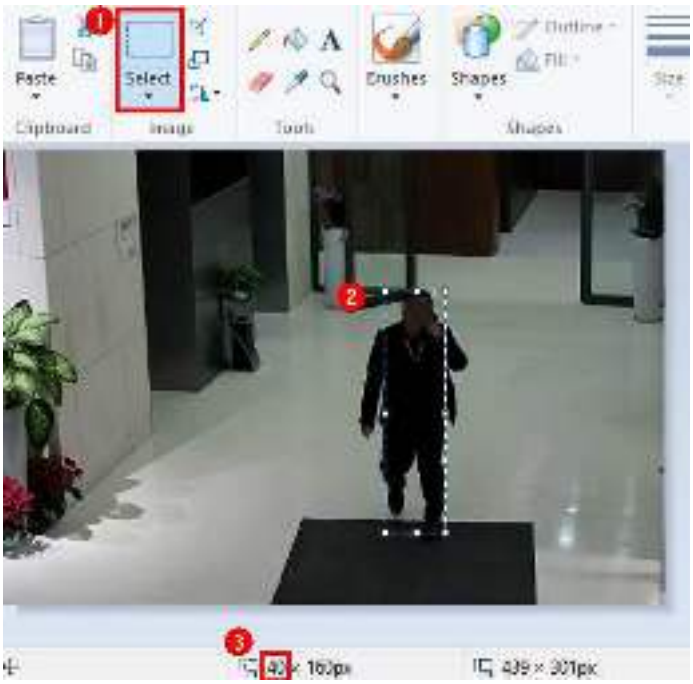
The following uses person detection as an example.

- Method 1

1. Arrange a person to stand in the capture area.
2. Log in to the camera web system.
3. On the **View** page, select the desired channel, click , box-select the object, and check the object resolution.

- Method 2
  1. Arrange a test person to stand at the farthest point of the detection area and manually take a snapshot of the person.
  2. On your computer, choose **All Programs** > **Accessories** > **Paint** to open the Microsoft Paint tool.
  3. Find the snapshot under **C:\Users*User name*\IPC_MediaPlayer\CaptureFiles** and open it using the Microsoft Paint tool.
  4. Box-select the body and view the horizontal resolution, as shown in the following figure.

     Figure 5 Viewing the full-body width resolution

Parent topic: Site Survey

Detection of Electric Bikes in Elevators

This function is used to detect whether electric bikes enter an elevator. If any electric bike is detected inside the elevator, an alarm is generated.

Application Scenario

This function is mainly applied in elevators.

Installation Requirements

- Installation position: In an elevator, it is recommended that the camera be installed at the inner corner of the elevator.
- Installation height: 2.5 m to 3 m
- Tilt angle: 50° to 70° (Do not install the camera at a large tilt angle.)
- Avoid scenarios with sudden light changes, camera shaking, or image switchover that may cause unstable images.
- Keep the camera away from irrelevant objects.

Precautions

- Resolution requirements: The resolution of an electric bike must be greater than or equal to 32 pixels at 2-megapixel video resolution and greater than or equal to 45 pixels at 5-megapixel video resolution.
- In infrared scenarios at night, if a person wears cotton clothes, sweaters, nylon coats, or fur clothing, it will be difficult to distinguish the person from the background. In this case, the specification may be affected.
- Billboards in elevators may contain targets and electric bikes, which may be mistakenly detected. You are advised to select a

proper site to avoid false detection. If this issue cannot be avoided, you can draw an ROI.

Installation Diagram

Correct Installation	Incorrect Installation
 The camera is installed at the inner corner of the elevator. The electric bike is completely visible in the image view.	 The camera angle is not properly adjusted. As a result, the electric bike is incompletely displayed in the image view.  The electric bike occupies a large part of the image, which affects the detection rate. You are advised to use a camera with 2.8 mm focal length.

Parent topic: Site Survey

Crowd Flow Analysis

- **Functions**
- **Site Survey Planning**
- **Commissioning Guide (Head Counting)**

Parent topic: Site Survey

Functions

Crowd flow analysis supports crowd density detection, queue length detection, and head counting, and is mainly applied in densely-populated areas such as squares, railway stations, subway stations, and shopping malls. The site survey for these functions is basically the same, which includes determining installation height and angle, checking object resolution, and drawing detection areas.

Table 1 Crowd flow analysis site survey

Function	Application Scenario	Site Survey Planning
Crowd density detection	In public places such as railway stations, subway stations, shopping malls, public squares, stadiums, and supermarkets, this function provides real-time information about the crowd density. When the number of persons in a detection area exceeds the preset threshold, an alarm is generated.	For details about the installation requirements, see Site Survey Planning.
Queue length detection	In scenarios involving queuing such as railway stations, subway stations, shopping malls, and airports, this function provides information about queue lengths of a certain area. If the estimated queuing time exceeds the preset threshold, an alarm is generated.	
Head counting	For public business places such as shopping malls, supermarkets, chain stores,	• For details about the installation

Function	Application Scenario	Site Survey Planning
	exhibitions, and museums, this function counts the number of persons moving in and out of an entrance or exit. When the number of persons entering and leaving a detection area exceeds the preset threshold, an alarm is generated.	requirements, see Site Survey Planning. • For details about the commissioning, see Commissioning Guide (Head Counting).

Parent topic: Crowd Flow Analysis

Site Survey Planning

Before installing a camera, plan the site survey to ensure that the people data statistics analysis function works properly after the installation. The recommended installation scheme varies depending on the camera model. Select an installation scheme based on the actual camera model.

Environment Requirements

Ensure that the following installation requirements are met:

- The light is stable. The background does not reflect light. The illumination in the detection area is greater than 25 lux.
- The camera is not impacted by vibration.
- The image background does not contain a large number of texture features.
- Ensure that the camera lens is not blocked by irrelevant objects and is not directly facing the light source, water surface, or reflection plane.

Installation Height

The installation height varies depending on the application scenario. The following describes the recommended installation height:

- If the camera is to be installed in a large-scale venue, for example, an airport, the recommended installation height ranges from 6 m to 10 m.
- If the camera is to be installed indoors with limited height, for example, a supermarket, the recommended installation height ranges from 3 m to 5 m.

Tilt Angle

Installation position: It is recommended that the camera directly face or tilt towards pedestrians. It is not recommended that the camera be installed above the entrance and exit or passageway. Tilt angle: The recommended tilt angle of the camera ranges from 30° to 60°, ideally about 45°. This ensures that the head and shoulder of persons are visible in the image, the head and shoulder are in the shape of an arch (Ω), and the head occupies a large proportion.

Figure 1 and Figure 2 show typical scenarios.

Figure 1 Crowd density/Queue length detection scenario



Figure 2 Head counting scenario



Resolution Requirements

To ensure optimal detection effect, if the video resolution is 1920 x 1080 pixels, the head and shoulder resolution should be at least 32 x 32 pixels. The minimum head and shoulder resolution in other video resolutions can be calculated in proportion.

NOTE

The full-body width resolution in the case of other video resolutions can be calculated in proportion. For example, if the video resolution is 2560 x 1440 pixels, the minimum resolution of the full-body width is as follows: (2560/1920) x 32 = 43

Checking Object Resolution

After the installation is initially completed, manually take a snapshot in the detection area and use the image editing tool to check the object resolution, so as to ensure that the object resolution meets the requirement. If the resolution does not meet the requirement, adjust the installation height, angle, and distance to ensure the optimal resolution.

You can check the object resolution in either of the following ways:

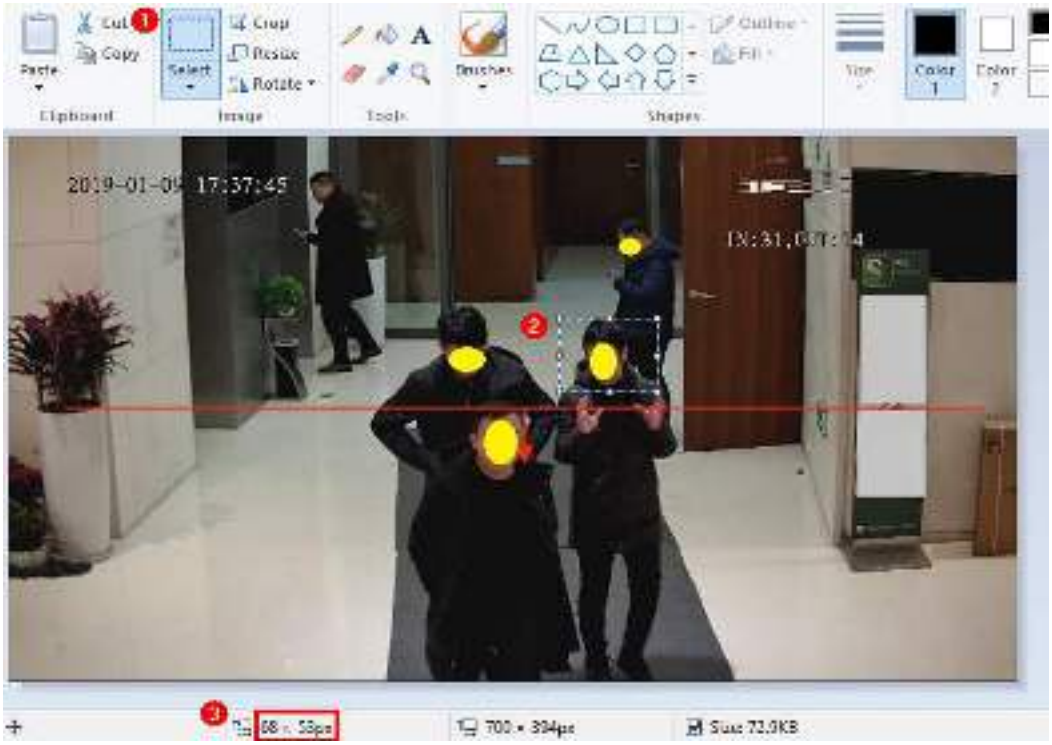
- Method 1

    1. Arrange a person to stand in the capture area.
    2. Log in to the camera web system.
    3. On the **View** page, select the desired channel, click  , box-select the object, and check the object resolution.

- Method 2

    1. Arrange a test person to stand at the farthest point of the detection area and manually take a snapshot of the person.
    2. On your computer, choose **All Programs** > **Accessories** > **Paint** to open the Microsoft Paint tool.
    3. Find the snapshot under **C:\Users\User name\IPC_MediaPlayer\CaptureFiles** and open it using the Microsoft Paint tool.
    4. Frame the head and shoulder of a person and check the resolution, as shown in Figure 3. Ensure that the head-shoulder resolution is greater than 24 x 24 pixels (1920 x 1080 video resolution).

Figure 3 Checking the object resolution



Parent topic: [Crowd Flow Analysis]

Commissioning Guide (Head Counting)

Head Counting Principle

The head counting function can correctly count a person only when the following conditions are met: A person enters the detection area. Then, the head and shoulder of the person cross the detection line without being occluded. Finally, the person leaves the detection area. Figure 1 shows an example.

Figure 1 Head counting principle



Typical Scenario

Figure 2 shows a typical scenario of head counting. The camera should be installed in the due front of the detection area. The detection line should be horizontal, and the detection area should cover the entire entrance/exit and be extended on both sides to ensure that persons entering and leaving from sides of the entrance/exit can be correctly counted.

Figure 2 Typical scenario



The installation and commissioning parameters in the preceding scenario are as follows:

- Installation height: 4 m
- The camera should face the detection area and the lower edge of the video image should be about 3–4 m away from the entrance/exit.
- The detection line should be horizontal, and the detection area should cover the entire entrance/exit and be extended on both sides.

The camera may miss some persons during head counting due to improper detection lines/areas and installation positions. For details about the commissioning, see Commissioning Cases.

Commissioning Cases

You need to commission the camera based on the actual scenario to ensure optimal detection effect.

Common problems and recommended commissioning methods are as follows:

- **Problem 1: The detection line is too high or too low.**
  - The detection line is too high. As a result, the head and shoulder of persons are under the detection line, and no detection line crossing is detected in the detection area, as shown in Figure 3.

Figure 3 Too high detection line



- The detection line is too low. As a result, the head and shoulder of persons are above the detection line, and no detection line crossing is detected in the detection area, as shown in Figure 4.

Figure 4 Too low detection line



Commissioning method

Adjust the detection line to a proper height based on the actual scenario, as shown in Figure 5.

- Move down the detection line if it is too high.
- Move up the detection line if it is too low.

Figure 5 Correct example



- **Problem 2: The detection area is too small, and the detection line is too low.**

  The head and shoulder of persons entering and leaving from sides of the entrance/exit are above the detection line outside the detection area. As a result, no detection line crossing is detected in the detection area, as shown in Figure 6.

  Figure 6 Too small detection area



  Commissioning method

  Extend the detection area on both sides of the entrance/exit and slightly move up the detection line at the end where most people pass through, as shown in Figure 7.

Figure 7 Correct example



- **Problem 3: A large number of persons are occluded in an open area.**

  In an open area, the detection line and detection area are far away from the lower edge of the video image (in the upper third part of the video image). As a result, a large number of persons are occluded in the detection area, as shown in Figure 8.

  Figure 8 Incorrect example



  Commissioning method

  Ensure that the detection line is close to the lower edge of the video image, as shown in Figure 9.

Figure 9 Correct example



- **Problem 4: The camera is not installed in the due front of the detection area.**

  The camera is not installed in the due front of the detection area. As a result, when there are a large number of persons, the persons behind may be occluded. Additionally, detection line crossing may fail to be detected when people entering and leaving from both sides of the entrance/exit.

Figure 10 Incorrect example



Commissioning method

- Adjust the camera installation position and ensure that the camera directly faces the detection area. This method is

recommended.

  - If the camera installation position cannot be adjusted, you are advised to slightly move up the detection line at the end farther from the camera. This method is not recommended.

- **Problem 5: The camera is too far away from the entrance/exit.**

  The prime lens short-focus camera is installed too far away from the entrance and exit. As a result, when there are a large number of persons, the persons behind may be occluded, as shown in Figure 11.

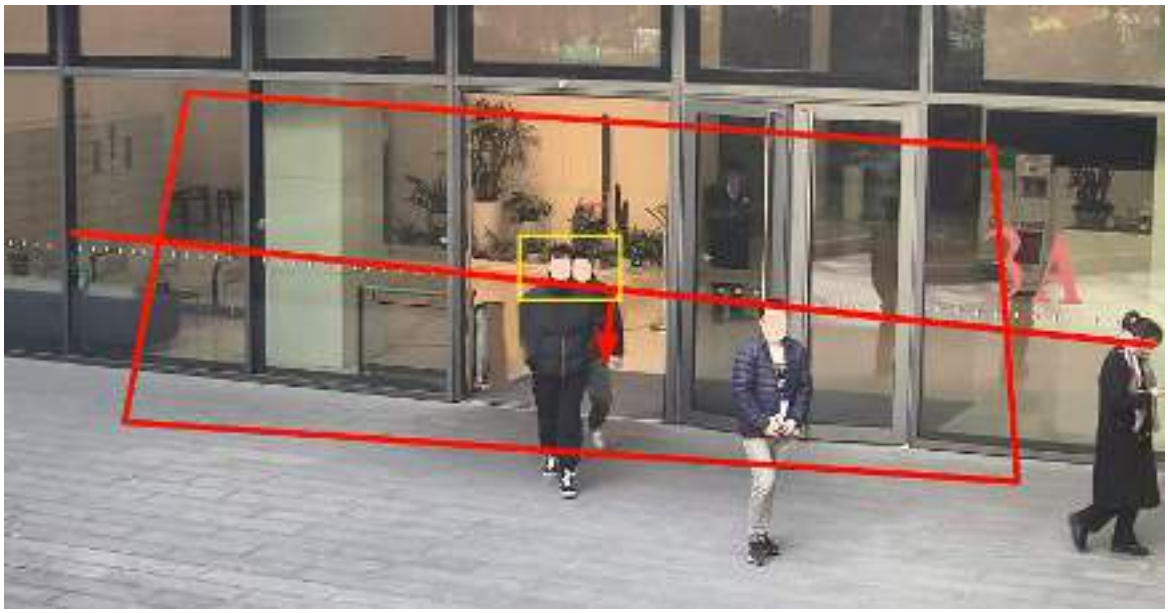
  Figure 11 Incorrect example

  Commissioning method

  Move the camera towards the detection area, as shown in Figure 12.

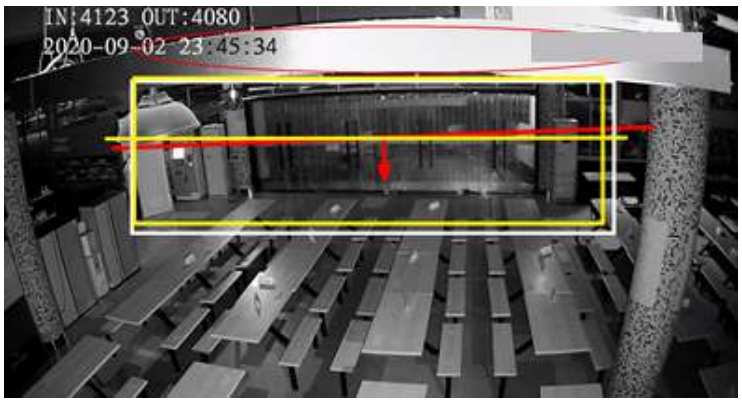
Figure 12 Correct example



- **Problem 6: Image distortion occurs due to a small camera tilt angle.**

  The tilt angle of the prime lens short-focus camera is too small. As a result, image distortion occurs, affecting the detection accuracy, as shown in Figure 13.

  Figure 13 Incorrect example

  Commissioning method

  Perform the following operations:

  1. Adjust the tilt angle of the camera to about 45°.
  2. If the camera supports distortion correction, enable this function. If not, go to 3.

3. If the detection effect is still unsatisfactory after the preceding operations, the camera is installed too far away from the detection area. In this case, you are advised to move the camera forward.

Parent topic: Crowd Flow Analysis

Object Classification

Object classification refers to detection and data structuring of motor vehicles, non-motor vehicles, and pedestrians. This function can differentiate between vehicles, non-motor vehicles, and pedestrians and report alarms according to the parameters.

Application Scenario

Object classification is best suited to:

- Entrances and exits of gas stations, buildings, campuses, communities, and villages.
- Urban intersections.
- Common national roads.

Installation Requirements

- It is recommended that the camera be installed at a height of 4.5 m to 6 m.
- The camera's installation distance depends on the focal length of the camera, while different cameras have different focal lengths. Therefore, the installation distance needs to be calculated independently.
- The tilt angle of the camera must not exceed 15° and the horizontal angle of the camera must be less than 20°. The slant angle of the license plate must be less than 5°.
- The illumination of the installation environment must be at least 70 lux. If the illumination at night is insufficient, use illuminators to supplement light.

Restrictions

- In scenarios with three or fewer lanes, cameras with a resolution lower than 5 megapixels can be used. In scenarios with four or

more lanes, cameras with a resolution higher than 5 megapixels can be used.

- In video images, the horizontal and vertical resolutions of a person must be greater than 240 pixels, and the occluded part of the person must be less than 10%. The horizontal and vertical resolutions of a vehicle must be greater than 100 pixels. The preceding minimum object size is determined in the case of 1080p. The minimum object size can be calculated in proportion in the case of another resolution.
- Common camera models (such as micro checkpoint cameras and situation awareness PTZ dome cameras) that support object classification can be used in scenarios where the motor vehicle speed is lower than 60 km/h.

Parent topic: Site Survey

1 + N

For details about the function, see Configuration Procedure.

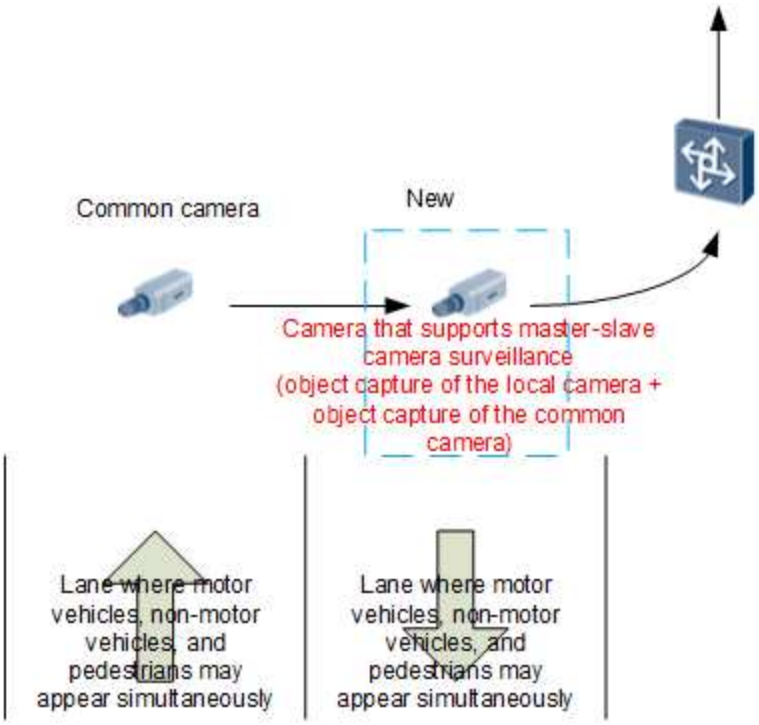
Application Scenario

A video security system has been deployed and some network cameras have been installed on the live network, however the devices are outdated, and do not support intelligent analysis functions or services (such as vehicle recognition). The existing system needs to be upgraded or reconstructed to meet current users' requirements on intelligent services. In this scenario, the 1 + N solution can be used.

Take a scenario with two lanes where motor vehicles, non-motorized vehicles, and pedestrians may appear at the same time as an example. A common network camera has been installed to detect one of the lanes but does not support object classification or capture. Users want to implement object classification and capture for both the two lanes.

In this case, a primary camera that supports 1 + N is installed under the same switch as an existing common camera (secondary camera). Assuming the network transmission between the two cameras is normal, the primary camera obtains video streams from the secondary camera, performs intelligent analysis, and outputs two channels of video streams with analysis results. Figure 1 shows the system architecture.

Figure 1 Typical scenario of 1 + N



Installation Requirements

To implement the 1 + N function, the primary camera needs to obtain video streams from secondary cameras in real time. Therefore, it is recommended that the primary camera be installed near the secondary cameras to ensure that both cameras are under the same switch. If they are not under the same switch, ensure that the network connection between the primary camera and the secondary cameras is normal (the packet loss rate is 0). The switch must have a 1000 Mbit/s network port.

- If target detection and license plate recognition are required, the installation requirements and site survey guide are the same as those for the target capture camera, micro checkpoint camera, or omni-data structuring camera. For details, see the corresponding special document.
- For details about the installation requirements and site survey guide for object classification, see Object Classification.

Parent topic: Site Survey

Appendix

- **How Do I Check the Target Size?**
- **How Do I Adjust Views from Non-Motorized Zoom Cameras?**

Parent topic: Site Survey

How Do I Check the Target Size?

Intelligent cameras provide the function of measuring the target size. You can directly mark the required target size on the image. When the actual target size is larger than the marked size, the detection requirement on the target size is met.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence** and click **Settings** next to **Target Capture**. The page for setting target parameters is displayed.
3. Check the live video, as shown in Figure 1. Table 1 describes the key parameters.

> **NOTE**
>
> Before performing target capture, you need to check the image background, illumination intensity, shooting angle, and target size in images. If any item does not meet the requirement, adjust camera images.

Figure 1 Setting common parameters



Table 1 Key parameters

Parameter	Description

Parameter	Description
Min. target resolution	Minimum width of a target that can be detected by the camera. Targets whose width is less than the value of this parameter cannot be detected. Set this parameter based on the site requirements. • If targets only need to be detected, you can use the default value 26. To prevent capturing too many side views of targets or small targets, you are advised to set this parameter to 80 or above. • If the camera is connected to a video security platform and sends snapshots to the platform for recognition, you are advised to set this parameter to 80 or above to ensure better recognition effect. You can click **Show on Image** to view the minimum target width in the image.
Max. target resolution	Maximum width of a target that can be detected by the camera. Targets whose width is greater than the value of this parameter cannot be detected. Set this parameter based on the site requirements. You can click **Show on Image** to view the maximum target width in the image.

Parent topic: Appendix

How Do I Adjust Views from Non-Motorized Zoom Cameras?

This section describes how to adjust the focal length through manual operations or by pressing the HF focus assistance button.

Manually Adjusting the Focal Length

The procedure for manually adjusting the focal length is as follows:

1. Loosen the knob on the aperture ring, adjust the aperture to the maximum, and tighten the knob.

   > 🕮 NOTE
   >
   > For auto iris lenses, skip this step.

2. Loosen the knob on the zoom ring (labeled **T** and **W**), and rotate the zoom ring in the T direction to the utmost and then in the W direction until you obtain the desired video effect. Then, tighten the knob.

   > 🕮 NOTE
   >
   > - Some zoom rings are labeled **T** and ∞ (the same as **W**).
   > - If the camera has been installed in the housing, the zoom knob may fail to be rotated after the zoom ring is rotated to a certain angle due to limited space in the housing. In this case, you can unscrew the knob and mount it to the other knob hole on the zoom ring for further zoom adjustment.

3. Loosen the knob on the focus ring (labeled **N** and **F**), rotate the focus ring back and forth until you obtain images with optimal quality, and then tighten the knob.

> **NOTE**
>
> Repeat steps 2 and 3 until the detection range meets the requirements and the image is clear.

4. Rotate the focus ring in the F direction to the utmost within 10s.

> **NOTE**
>
> During the process, try your best to rotate the focus ring slowly and evenly, and ensure that nothing blocks the lens.

5. Slowly rotate the focus ring in the **N** direction and stop when the status indicator (STAT) blinks with high frequency.

   The system provides sound assistance for determining the best focal length. After enabling focus assistance, you need to plug in a 3.5 mm three-pole earphone to the audio output port (AUDIO OUT). When the focus reaches the best position, you can hear a continuous sound in your earphone.

6. Check the live video, ensure that the image is clear and the snapshots meet the target capture requirements, and tighten the knob.
7. Close the housing if there is one.

Pressing the HF Button to Enable Focus Assistance

Press the HF button to enable the focus assistance function. The status indicator (with the STAT label) begins blinking. The focus assistance function is automatically disabled if no operation is performed within 30s after the function is enabled.

Parent topic: Appendix

Installation Guide

Security Precautions Carefully read and comply with the security precautions. If the electrical products are incorrectly used, a fire disaster may occur. Read the following cautions before using the device.

Tool Preparation
Before the installation, prepare required tools.

Installation Requirements
Before the installation, check whether the environment meets the installation requirements and whether the required facilities (for example, scaffold) are ready.

Installation Guide

Common Installation Errors
This chapter describes common cases of device damage due to incorrect installation. The installation personnel can learn from these cases to avoid similar problems.

Appendixes

Security Precautions

Carefully read and comply with the security precautions. If the electrical products are incorrectly used, a fire disaster may occur. Read the following cautions before using the device.

NOTICE

- The product used in this document is for reference only.
- Products and services are subject to change without notice.
- If any problem occurs when you use the camera, contact the device supplier in time.
- We are not responsible for your misoperation.
- While using the device, observe all applicable laws, directives and regulations, and ensure such usage does not infringe on the legal rights of any other party.
- All installation and maintenance of the device should be performed by professional technical engineers.

Power Supply Requirements

- Comply with local electric security standards.
- The power supply of the device must meet the requirements of the input voltage of the device.
- If a device has a ground point or ground cable, install a surge protector to prevent lightning strike. To ensure the device safety, properly ground the device. Devices without ground points and ground cables do not need to be grounded.
- Use product-attached auxiliaries and recommended fittings (such as power adapters and batteries). We are not liable for any faults caused by fittings not recommended.
- If the negative DC voltage is used for power supply, use isolated power adapters.

- Do not connect multiple devices to the same power adapter.
- Do not power on the device during the installation. Before plugging or unplugging any cables, shut down the device and disconnect the power supply.
- Keep the power plug clean and dry to prevent electric shocks or other dangers.

Application Requirements

- Keep the device dry and prevent any violent collision when transporting, storing, and installing the device. Do not push or pull the pigtail.
- Install the device strictly according to the requirements of the manufacturer. Do not install the device reversely.
- Do not block the lens of the device when installing a camera. Do not block the infrared illuminator when installing an infrared camera.
- Do not touch the camera lens when installing a camera. Otherwise, the camera lens may be damaged or scratched.
- Remove the protective film after installation. If the camera does not have a film attached, clean the lens and housing after installation.
- Move and place the device gently. Do not squeeze the device components. Otherwise, mechanical faults may occur.
- Do not disassemble the device by yourself. There is no part in the device that can be repaired by yourself. Contact the device supplier if a fault occurs on the device.
- Avoid any unauthorized modifications on the design of the structure, security, or performance.
- Do not scratch or abrade the device shell. The shed painting may lead to skin allergies or device malfunctions.

- Stop using and power off the device immediately if any exceptions occur, for example, the device is smoking, the sound is abnormal, or the device turns smelly. Remove all the cables connected to the device, such as power cables and network cables.
- Post a reminder "You have entered the detection area" at the most visible location if cameras are installed at public places.
- Do not touch the heat dissipation components of the product.

Cleaning Requirements

- Stop using the device, turn off the power, and remove all the cables connected to the camera (such as the power cables and network cables) before cleaning the device.
- Use a soft cloth to wipe out the dust on the device. Add little neutral detergent if necessary.
- Do not clean the device with strong and abrasive alkaline cleaner or volatile solvent such as alcohol, benzene, or thinner. These liquids may damage the surface coating or deteriorate the device performance.
- Use a light (such as flashlight on the mobile phone) when cleaning the device. There should be no visible dust, grease, or other stains.
- Do not use unclean objects to clean the camera.

NOTE

Refer to the following solutions when there is dirt on the camera lens, transparent dome cover, or viewing window:

- Dust on the lens: Use an oil-free soft brush or blowing ball to gently wipe off the dust.
- Oil or fingerprint on the lens: First use a soft cloth to gently wipe off the oil or fingerprint and make the lens dry. Then dip an oil-

free cotton cloth or lens cleaning paper in the lens cleaning liquid and wipe the lens from middle to edge. If the lens cannot be cleaned thoroughly, replace the oil-free cotton cloth or lens cleaning paper with a new one and repeat the preceding operations until the lens is cleaned thoroughly.

Environment Requirements

- Keep the device away from water or any other liquids. If any liquid enters the device accidentally, power off the device and disconnect all cables connected to the device, such as power cables and network cables.
- Keep the device away from heat sources and exposed fire sources, such as electric heaters and candles.
- Do not install or use the device in hazardous areas with flammable or explosive materials.

Parent topic: Installation Guide

Tool Preparation

Before the installation, prepare required tools.

Tools to be prepared

Table 1 lists the tools that need to be prepared.

Table 1 Tools to be prepared

Tool Name	Specification and Function	Appearance
Video detection tester	Used to check the shooting angle and video image.	
Multimeter	Used to check whether the camera's input power meets the requirements.	
Network cable tester	Used to test whether the network cable is made and connected correctly.	
Hammer drill	Drill bit size: 5 mm. Used to drill holes in scenarios such as wall-mounted and pendant-mount installation scenarios.	
RJ45 crimping tool	Used to make an RJ45 connector.	

Tool Name	Specification and Function	Appearance
Wire stripper	Used to remove the insulation layer and jacket from the power cable, alarm cable, and other cables.	
Hex key	Specification: H3 Used to fasten and loosen hex socket screws of the M4 model.	
Phillips screwdriver	Specification: 0#, 1#, and 2# Used to loosen and fasten Phillips screws.	
Flat-head screwdrivers	Screwdriver bit width: 2.5 mm; screw bit length: greater than 75 mm. Used to loosen and fasten flat-head screws.	
Claw hammer	Used to drive expansion screws into the wall.	
Measuring tape	Used to measure the distance, for example, measuring the cable length and installation height.	

Tool Name	Specification and Function	Appearance
Socket wrench	Specification: M6	
ESD gloves	Prevents ESD.	
Marker	Used to make marks, for example, marking the installation position and hole positions.	
Scissors	Used to cut waterproof tapes, insulating tapes, and others.	
Utility knife	Used to disassemble the packing box of the camera.	
Wrench	Used to turn screws.	
Diagonal plier	Used to cut off excess hose clamps.	
Dust-free cloth	Used to wipe the camera lens or viewing window.	

Parent topic: Installation Guide

Installation Requirements

Before the installation, check whether the environment meets the installation requirements and whether the required facilities (for example, scaffold) are ready.

NOTICE

When installing the camera, pay attention to the following:

- Construction and delivery personnel need to go to sites (such as campuses, streets, corridors, and halls) to erect poles, install devices and related accessories, and commission the devices.
- Ensure that the lens is not exposed to strong light (such as direct sunlight, street light, and vehicle headlight) after the installation.
- To install infrared cameras, avoid dark indoor corners. Otherwise, black and white images may be produced even in the daytime.
- Adjust the camera location to ensure that the camera is not exposed to a low color temperature light source (such as a sodium lamp) within the angle of view extended by 10 degrees. This avoids stripes on the images.
- Keep the camera away from strong-light-reflection objects such as glasses, ceramic tiles, and waters to prevent images from being too dark or bright.
- A transparent protective film is attached to the dome cover or view window of the camera. Do not remove the transparent protective film during the installation to prevent the dome cover or view window from being scratched or polluted. You can remove the transparent protective film after the device is installed and before the device is started.
- Do not move the wiper manually during the installation to avoid damaging the wiper.

- The installation personnel must set up the scaffolding before working at heights.
- The installation personnel must take protective measures and wear safety belts when performing operations.
- Installation and maintenance must be performed by professional technical engineers or system installation engineers.
- Ensure that the camera installation surface or pole can sustain at least four times the total weight of the camera, shield, and bracket.
- Determine the installation position and mark it using the marker.
- Determine the cabling route and measure the required cable length using the measuring tape.
- Lay out the required cables based on the planned cabling route.
- If the temperature in the installation environment is out of the range from –20°C to +50°C, cameras must be installed in restricted areas that can only be touched by professionals.
- Keep the device away from heat sources, fire sources (such as heating apparatus or candles), and strong magnetic fields (for example, high-voltage power distribution cabinet).
- While using the device, observe all applicable laws, directives and regulations, and ensure such usage does not infringe on the legal rights of any other party. Post a reminder "You have entered the detection area" at the most visible location if cameras are installed at public places.
- The power adapter to be used by the device must meet the input voltage and current requirements described on the device label.
- Verify that the network connection is normal.
- If a device has a ground point or ground cable, install a surge protector to prevent lightning strike. To ensure the device safety,

properly ground the device. Devices without ground points or ground cables do not need to be grounded.

- Keep the device away from water or any other liquids. Take proper water-proof measures when installing the device outdoors.
- There is a ventilation hole in the sun visor of the bullet network camera. Do not remove the tape. Otherwise, the waterproof performance of the camera may deteriorate.
- Keep cameras away from the chemical industry or heavily polluted areas to avoid corrosion.
- Generally, the salt spray corrosion resistance of cameras can be classified into the following classes:

    1. Class D corrosion resistance. Cameras at this level can be installed within 1500 m away from the seashore or on offshore platforms.
    2. Class C corrosion resistance. Cameras at this level can be installed in areas 1500 m away from the seashore.

  Before installing a camera, check its corrosion resistance level. Do not install the camera in an environment that exceeds the specification of salt spray corrosion resistance.

NOTICE

If there are too many services (for example, video recording and scheduled snapshot are enabled at the same time), the storage performance of the SD or TF card may be insufficient. As a result, video or images may be lost.

Parent topic: Installation Guide

Installation Guide

The installation process varies depending on camera models. For details, see the following table.

Table 1 Applicable models

Camera Type	Model	Reference
Fixed dome camera	HWT-D3222-10-SIU	AI Fixed Dome Camera Quick Start Guide
	HWT-D3252-10-SIU	
	HWT-D3040-10-ELI-PV(2.8mm)	AI Flat Dome Camera（RST）Quick Start Guide
Bullet camera	HWT-D2122-10-SIU	AI Small Bullet Camera (Integrated Bracket) Quick Start Guide
	HWT-D2152-10-SIU	
PTZ dome camera	HWT-D6550-10-Z33-SV	White-Light AI PTZ Dome Camera with Intercom Quick Start Guide

Parent topic: Installation Guide

Common Installation Errors

This chapter describes common cases of device damage due to incorrect installation. The installation personnel can learn from these cases to avoid similar problems.

Water Leakage Due to Pigtail Cutoff This section describes the water leakage issue caused by improper handling of the pigtail and the solution to handle the issue.

Pigtails Are Loosened or Disconnected If They Are Pulled
This topic describes the problem of pigtails loosening or disconnection caused by incorrect user operations and the correct operations.

Device Damage Caused by Unstable Power Supply
This section describes the device damage caused by unstable input voltage.

Invalid Detection Due to Improper Installation
This section describes the failure to detect important areas due to improper device installation position or shooting angle.

Device Damage Due to Lack of Surge Protection and Grounding
This section describes device damage due to lack of surge protection and grounding and the requirements of surge protection and grounding.

Water Ingress Caused by Indoor Mount Used Outdoors
When a camera is installed outdoors, you need to take waterproofing and insulation measures to avoid short circuits caused by water ingress.

Indoor Device Installed Outdoors
In outdoor scenarios, a camera that meets the outdoor environment requirements must be used, or a housing should be installed for the camera.

Misapplication of C- and CS-mount Lenses

A lens can be installed on a C-mount or a CS mount. A C-mount lens must be installed on a C-mount. To install a C-mount lens on a CS mount, you must use a C/CS lens adapter. Otherwise, camera faults may occur.

Device Installation Failure Due to Incompatible PTZ Dome Camera Mount

When installing a PTZ dome camera, use a mount that matches the adapter ring to avoid installation issues or other issues caused by incompatible mounts.

Network Port Corroded by Water Due to Lack of Waterproof Measures for Pigtails

This section describes the network port corrosion issue due to lack of waterproof measures for pigtails of outdoor cameras and the solution to handle the issue.

Camera Fault Due to Unqualified Self-Made RJ45 Connectors

This section describes the camera fault caused by unqualified self-made RJ45 connectors and the method for making qualified RJ45 connectors.

Fiber Pigtail Cut Due to Improper PTZ Dome Camera Installation

This section describes the fiber pigtail cut due to improper camera installation and the correct installation method.

Camera Damage Due to Improper Cabling for Power Supply

This section describes the camera damage due to improper cabling for power supply and the correct cabling method.

Water Seepage Due to Improper Camera Installation Outdoors

This section describes water seepage due to improper camera installation outdoors and the correct installation method.

Network Port Damage Due to Forcible Cable Pulling

This section describes network port damage due to forcible

cable pulling and the correct operations.

Camera Deviation from the Preset Position Due to Loose Screws of the Bracket
This section describes camera deviation from the preset position due to loose screws of the bracket and the solution.

Severe Corrosion of Common Cameras Installed at the Seaside
This section describes the anti-corrosion specifications of cameras and the camera selection for different environments.

Red Artifacts on Video Images Since the Protective Film Is Not Removed
This section describes the issue of red artifacts on video images since the protective film is not removed from the camera.

Parent topic: Installation Guide

Water Leakage Due to Pigtail Cutoff

This section describes the water leakage issue caused by improper handling of the pigtail and the solution to handle the issue.

Typical Example

Figure 1 The pigtail is cut off and is not waterproofed.



Symptom

- Unused pigtails such as the audio cable and video cable are directly cut off.
- The pigtail that is cut off is not waterproofed.

Solution

- Do not cut off any pigtail, including unused pigtails such as the audio cable and video cable.
- Apply waterproof tape on the joints of all pigtails to prevent water penetration.
- Ensure that insulation and waterproof measures are properly taken. For details, see Insulating and Waterproofing.
- Use corrugated metal conduits to protect exposed cables.

Remedial Measures

Apply waterproof tape on the pigtail that is cut off due to improper operations, as shown in Figure 2.

Figure 2 Apply waterproof tape on the pigtail



Parent topic: Common Installation Errors

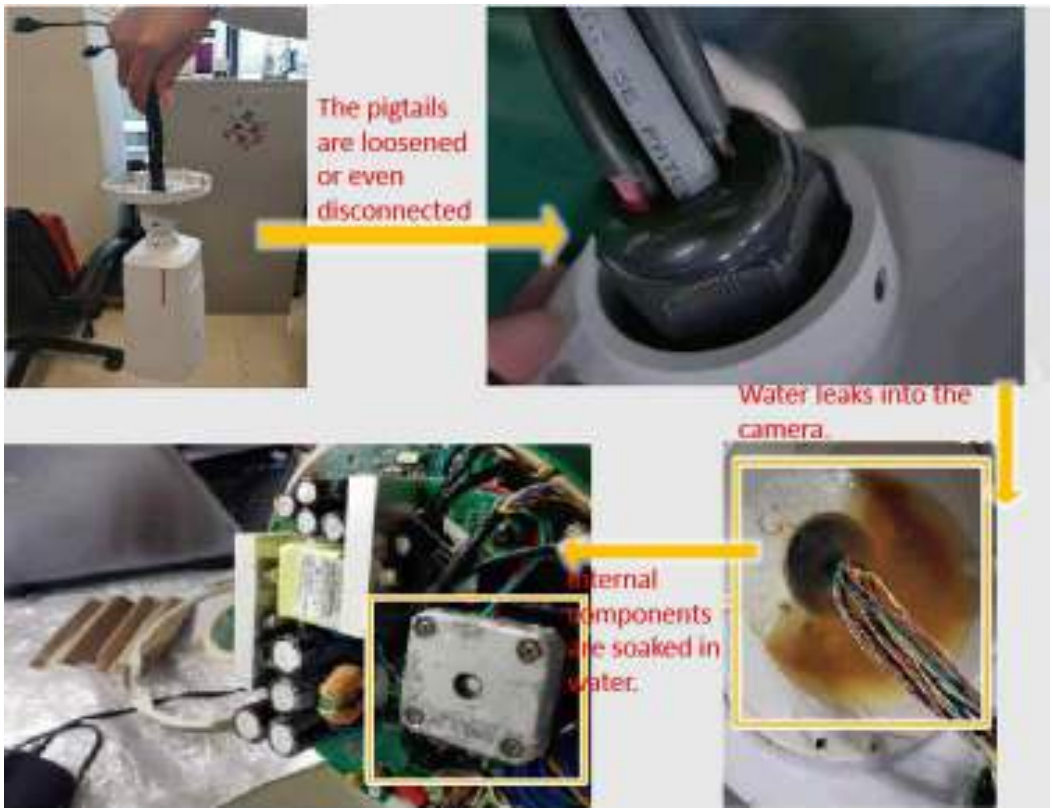
Pigtails Are Loosened or Disconnected If They Are Pulled

This topic describes the problem of pigtails loosening or disconnection caused by incorrect user operations and the correct operations.

Typical Example

The pigtails are loosened or even disconnected, as shown in Figure 1.

Figure 1 Pigtails loosened or disconnected



Symptom

- The pigtails are loosened or disconnected from the PG connector, and seams appear between the pigtails and the PG connector, which will lead water into the device.

- The pigtails are loosened or disconnected from the junction with the interface board, which causes cable faults. For example, if the pigtail of the power cable is loosened or disconnected, the device fails to be powered on.

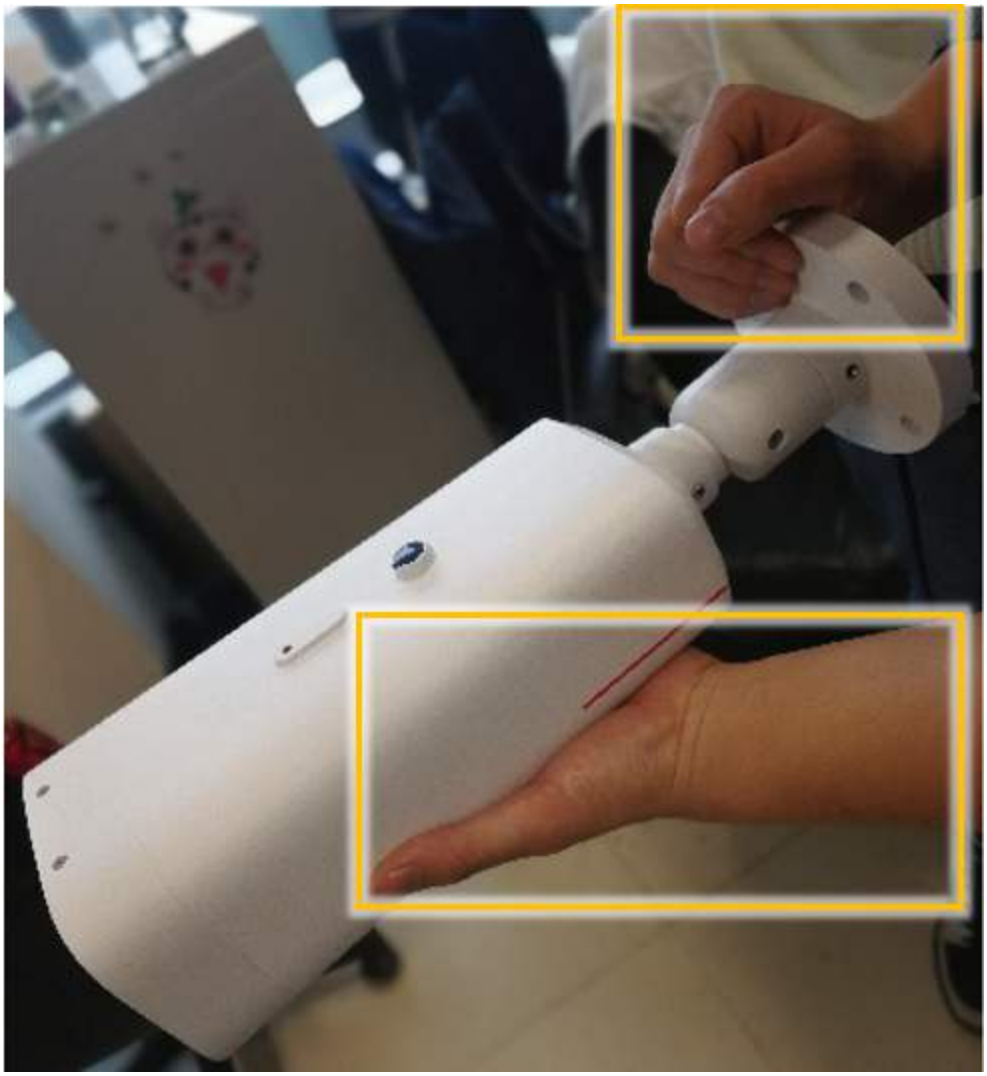
Root Cause

Users carry a device by the pigtails.

Correct Operations

Carry a device by the device body. Do not pull the pigtails, as shown in Figure 2.

Figure 2 Correct method of carrying a device



Parent topic: Common Installation Errors

Device Damage Caused by Unstable Power Supply

This section describes the device damage caused by unstable input voltage.

Typical Example

Figure 1 The power supply voltage is too low.



Symptom

- The input voltage is too low, which causes the camera to restart repeatedly. As a result, the internal components are seriously damaged.
- The rectifier bridge of the camera is burnt, so the camera cannot be properly powered on.
- During power-on and power-off, the flash is burnt. As a result, the camera constantly performs self-check during powered on and cannot be accessed.

Root Cause

- The power cable of the adapter is too thin, and the line loss is too large. After the infrared illuminator of the camera is enabled, the input voltage is too low.

- The power cable is too thin and the voltage decreases too much. After the camera is connected, the voltage is too low.
- The input voltage of the adapter is unstable and does not comply with the voltage standard (voltage range: 12 V DC (±25%), 24 V AC (–25% to +24.9%)).
- The input voltage of the camera does not meet the requirements (voltage range: 12 V DC (±25%), 24 V AC (–25% to +24.9%)).

Solution

1. The input voltage of the camera must meet the requirements (voltage range: 12 V DC (±25%), 24 V AC (–25% to +24.9%)).
2. To ensure the voltage stability, you are advised to use a voltage regulator.
3. The cross-sectional area of the power cable must comply with the specifications. For details, see Table 1.

Table 1 Cable cross-sectional area specifications

Type	Cross-Sectional Area	Maximum Cable Length
24 V AC output (from the adapter to the camera)	1.0 mm²	10 m
	1.5 mm²	25 m
	2.0 mm²	50 m
	2.5 mm²	75 m
	3.0 mm²	120 m

Parent topic: Common Installation Errors

Invalid Detection Due to Improper Installation

This section describes the failure to detect important areas due to improper device installation position or shooting angle.

Typical Example

Figure 1 Invalid detection due to improper installation



Symptom

- The camera lens is occluded and cannot capture the expected area.
- The detection area is an unimportant area or is not fully covered. Therefore, the captured video images are useless.

Root Cause

- The pole is too high or the camera's shooting angle is improperly set. As a result, the camera lens is occluded by leaves or poles.
- The camera shoots only part of the detection area.

Solution

1. Determine the pole height based on the actual environment and adjust the camera's shooting angle to avoid obstacles.

2. Set a proper focal length to ensure the coverage of accident-prone areas.
3. Set a proper camera angle to ensure that movement directions of passengers are detected.

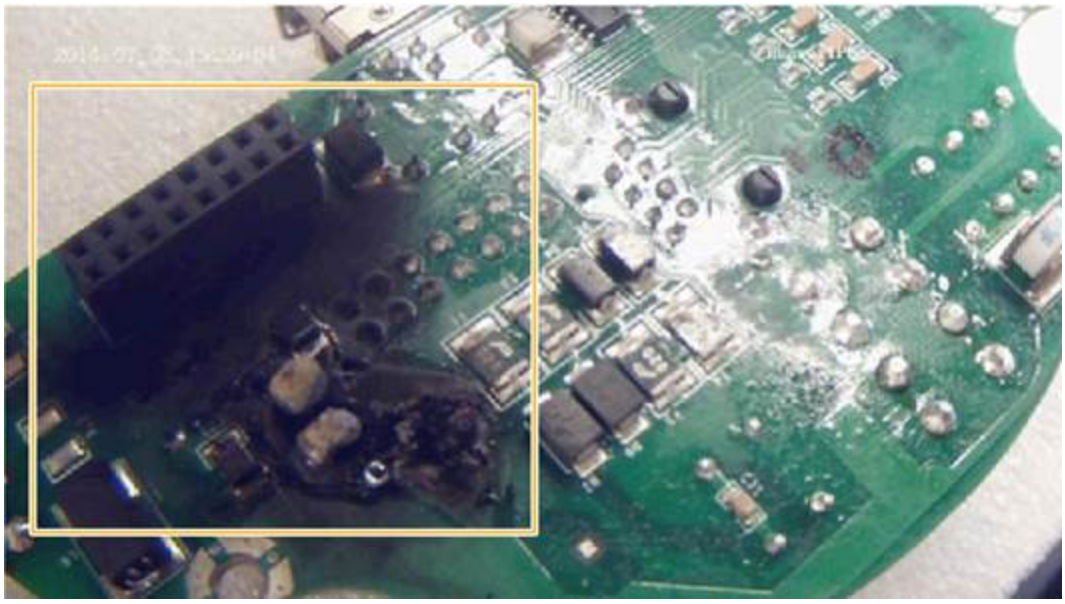
Parent topic: Common Installation Errors

Device Damage Due to Lack of Surge Protection and Grounding

This section describes device damage due to lack of surge protection and grounding and the requirements of surge protection and grounding.

Typical Case

Figure 1 Component damaged by lightning strike



Symptom

The component is broken down due to lightning strike.

Root Cause

- The camera is not equipped with a surge protector.
- The camera is not correctly grounded.

Solution

Install a surge protector on the camera. The adapter must be installed between the camera and the surge protector. The camera and surge protector must be correctly grounded.

NOTICE

1. The camera must be installed within 45° of the lightning rod.
2. The resistance of the ground cable should be less than or equal to 10 ohms.
3. The network box must be installed near the camera. The distance between the network box and the camera must be less than 5 m.

Figure 2 Surge protection and grounding

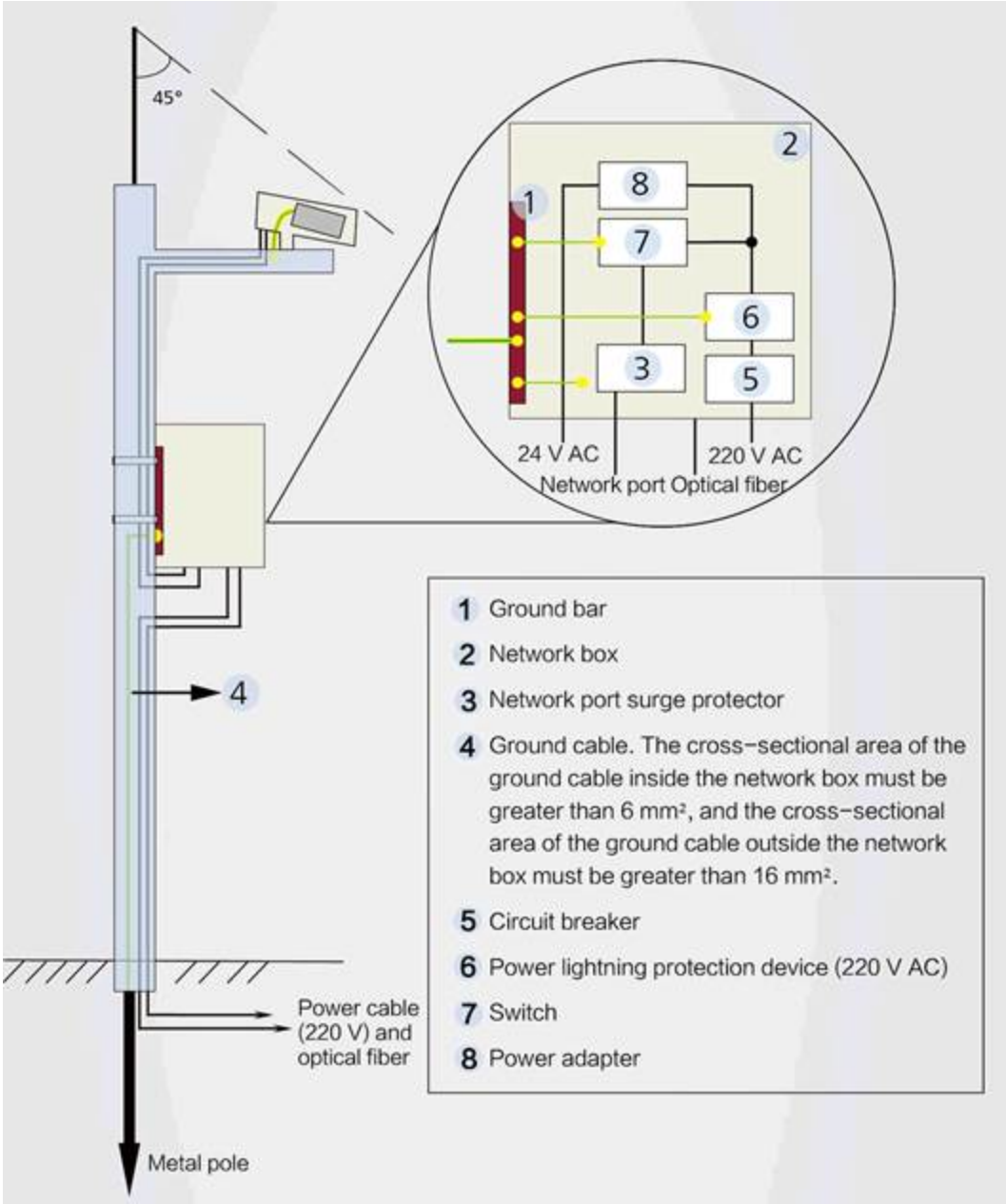


Table 1 Requirements for surge protection

Port	Specification	Scenario

Port	Specification	Scenario
220/110 V AC	• Differential mode: 10 kA (wire to wire), 8/20 us • Common mode: 10 kA (single-wire to ground), 8/20 us	Pole-mounted/wall-mounted installation in urban areas
	• Differential mode: 20 kA (wire to wire), 8/20 us • Common mode: 20 kA (single wire to ground), 8/20 us	Pole-mounted installation in non-urban areas
PoE/network port	Surge: • Differential mode: 1.5 kV (differential wire pair), 10/700 us, 15 ohms + 25 ohms/wire • Differential mode: 1.5 kV (–48 V to RTN), 10/700 us, 15 ohms + 25 ohms/wire • Common mode: 6 kV (8-wire to ground), 10/700 us, 15 ohms + 25 ohms/wire Surge current:	Pole-mounted installation in urban/non-urban areas

Port	Specification	Scenario
	• Differential mode: 250 A (–48 V to RTN), 8/20 us • Common mode: 3 kA/8-wire, 8/20 us	

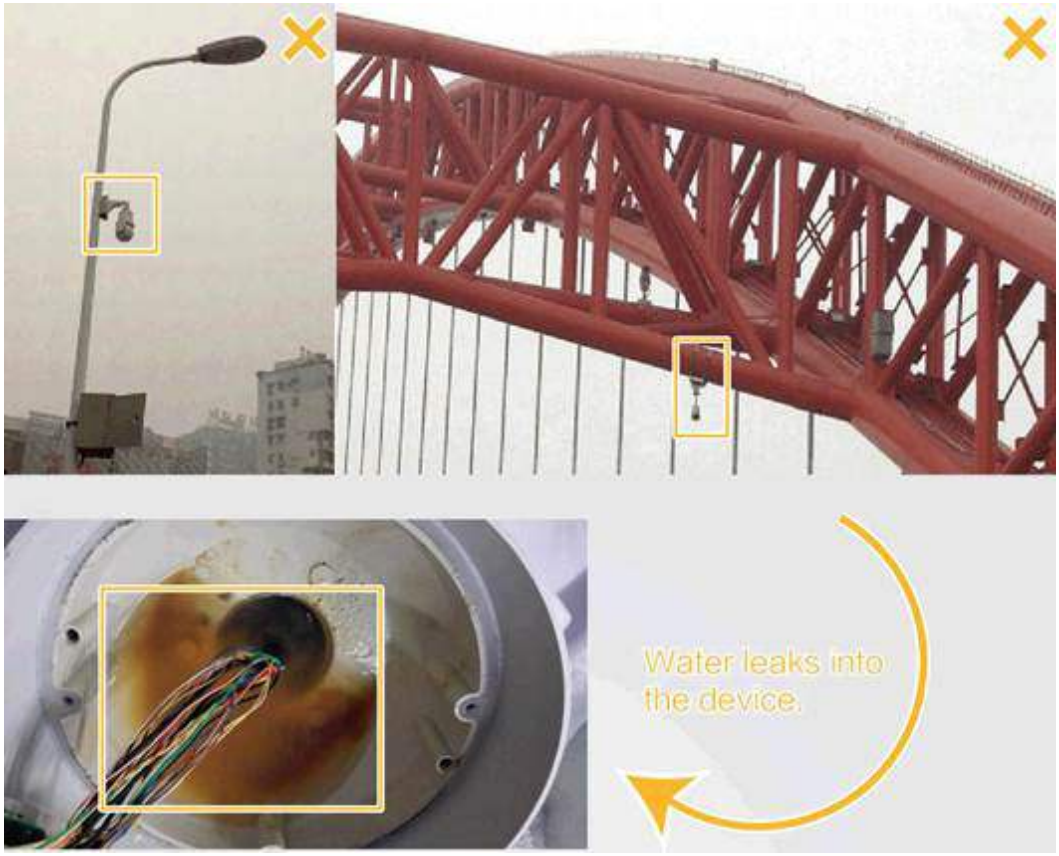
Parent topic: Common Installation Errors

Water Ingress Caused by Indoor Mount Used Outdoors

When a camera is installed outdoors, you need to take waterproofing and insulation measures to avoid short circuits caused by water ingress.

Typical Case

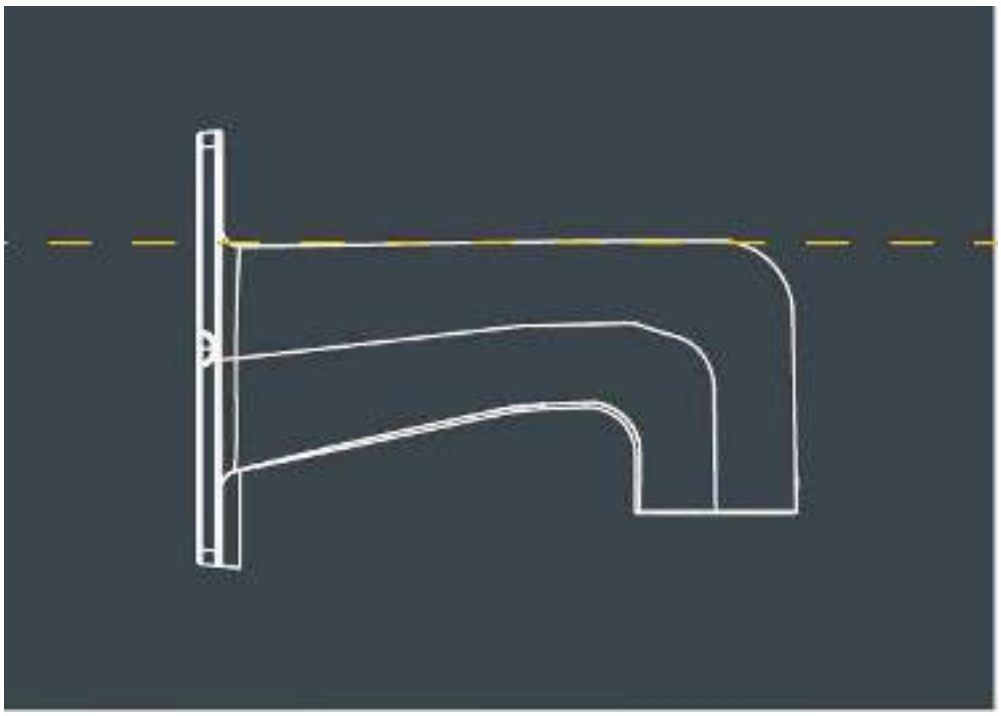
Figure 1 Water ingress due to wrong installation methods



Symptom

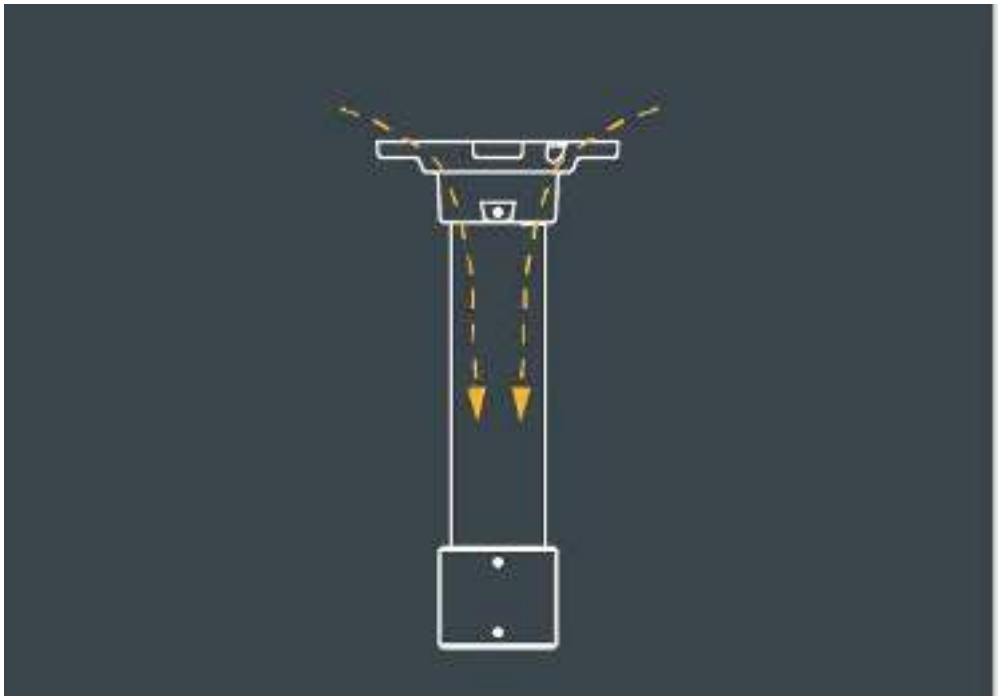
- If a short wall mount is used to install a camera outdoors, the beam of the mount is horizontal, and water may easily leak into the camera, as shown in Figure 2.

Figure 2 Short wall mount



- If a pendant mount is used to install a camera outdoors, and the upper part of the mount, camera pigtails, and connection point between the camera and the mount are not waterproofed, water may easily leak into the camera, as shown in Figure 3.

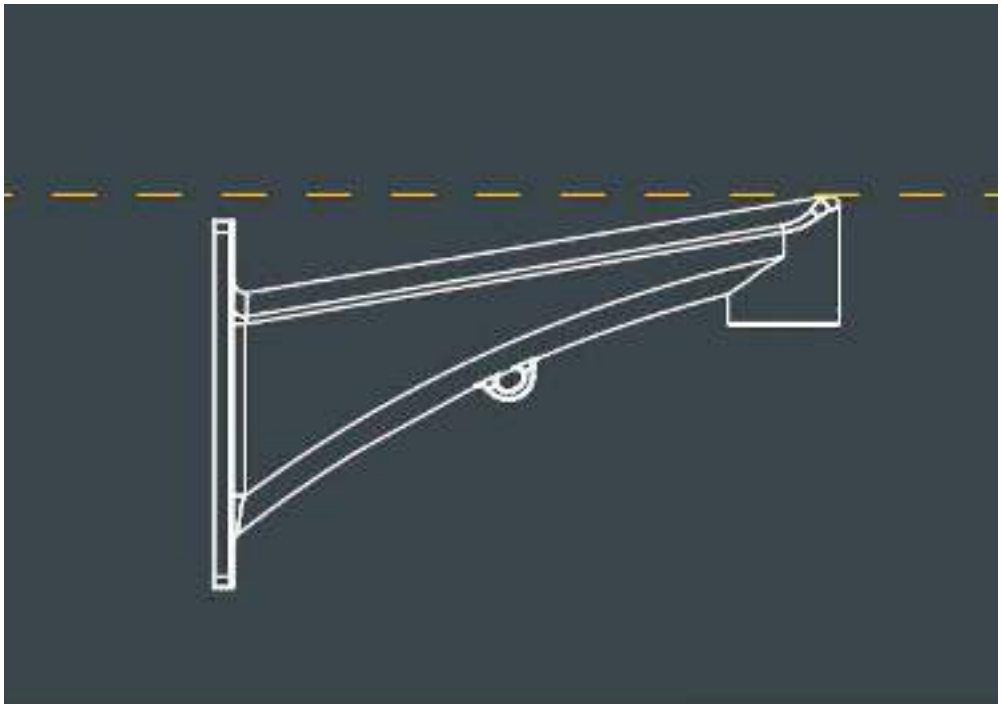
Figure 3 Pendant mount



Solution

- Use a long wall mount to install a camera outdoors. The beam of the mount is tilted to avoid water ingress, as shown in Figure 4.

Figure 4 Long wall mount

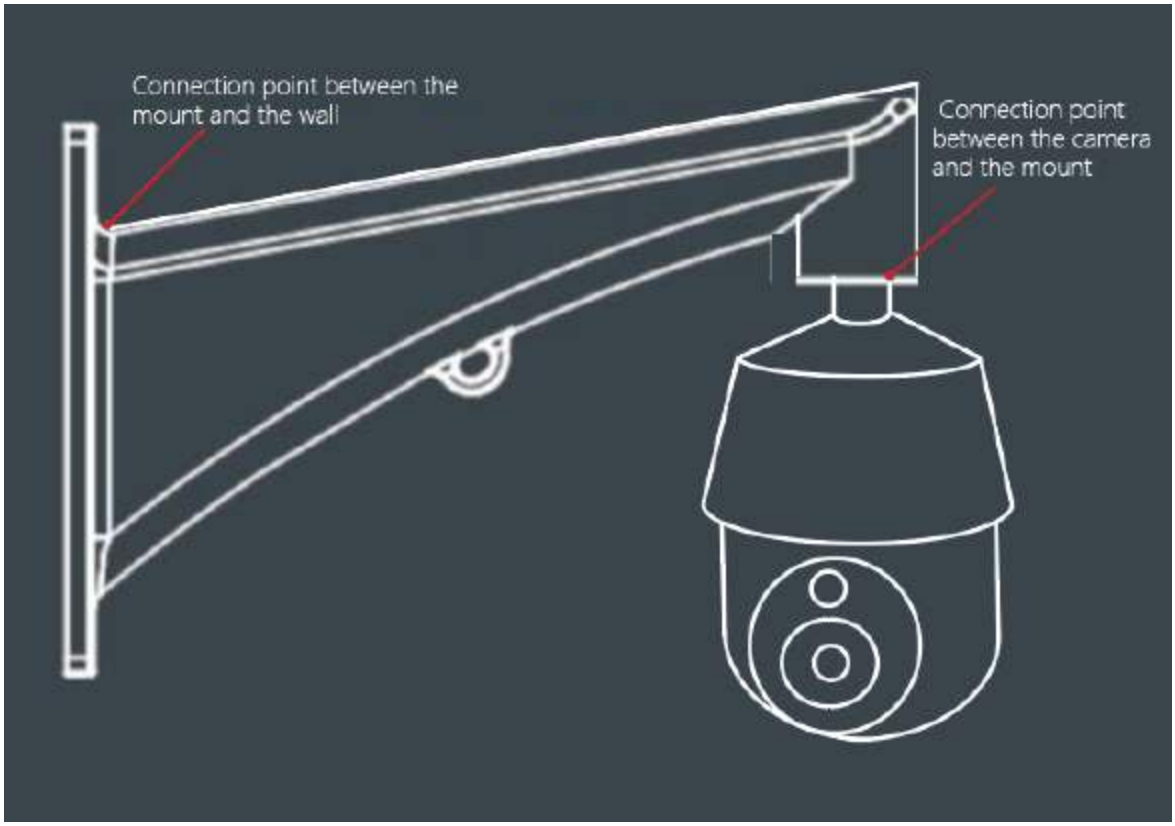


- Use an integrated pole mount to install a camera outdoors to avoid water ingress from the connection point between the camera and the mount, as shown in Figure 5.

Figure 5 Integrated pole mount



- Take waterproofing measures such as silicon sealant at places from which water may leak into the camera, such as the upper part of the mount, camera pigtails, and connection point between the camera and the mount.



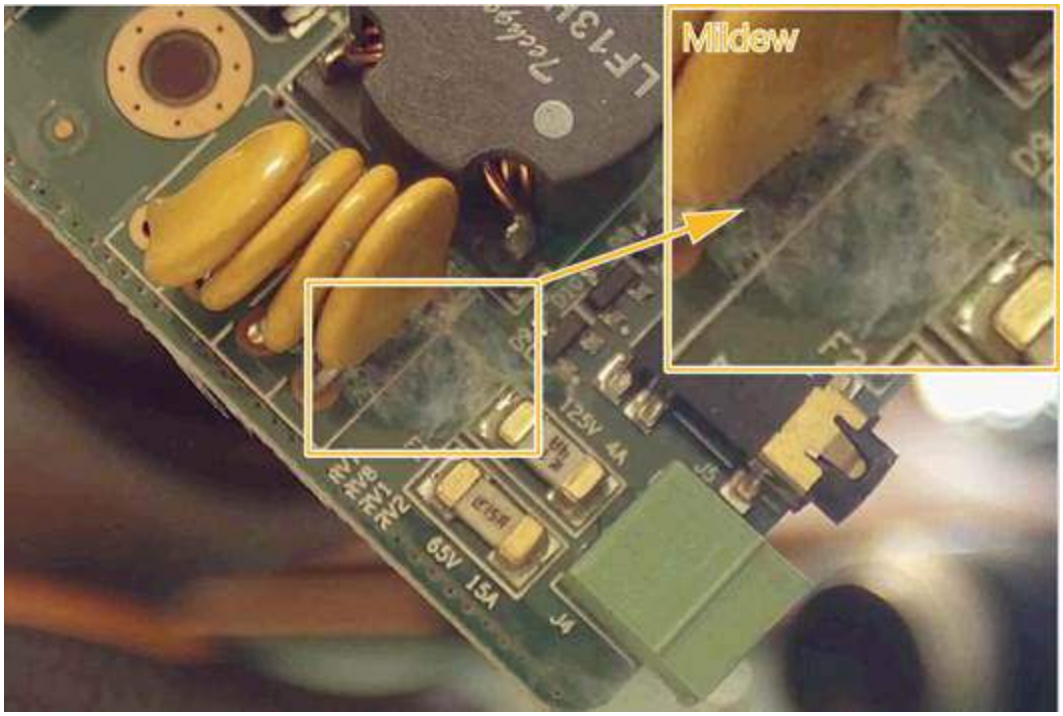
Parent topic: Common Installation Errors

Indoor Device Installed Outdoors

In outdoor scenarios, a camera that meets the outdoor environment requirements must be used, or a housing should be installed for the camera.

Typical Example

Figure 1 Mildewed board



Symptom

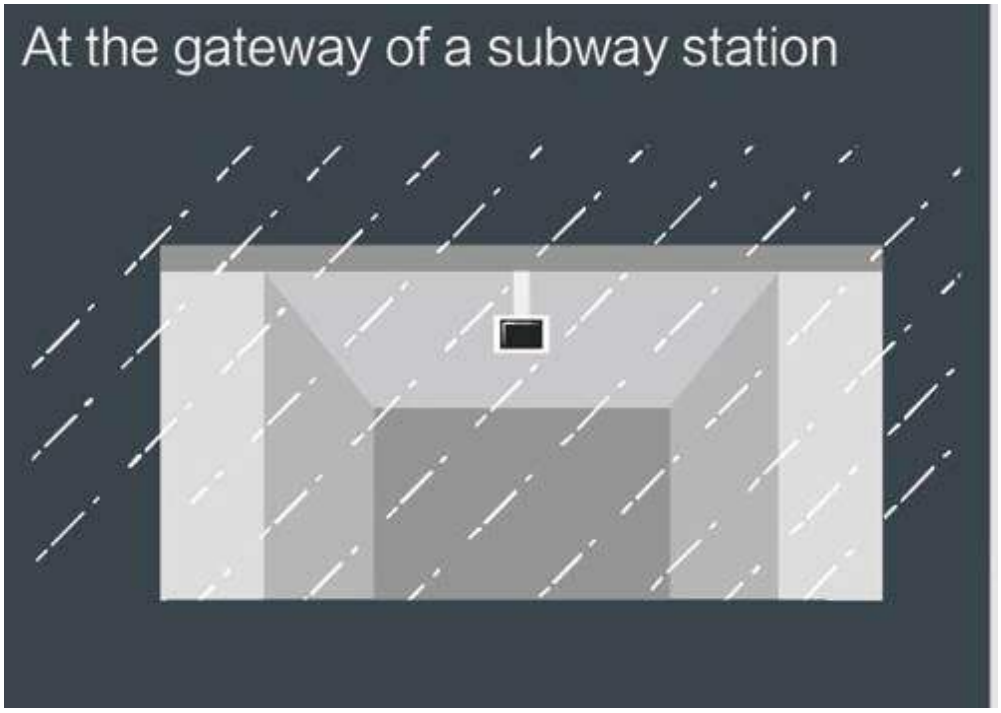
- An indoor fixed dome camera is installed outdoors. The camera is damaged due to water penetration, as shown in Figure 2.

Figure 2 Fixed dome camera installed outdoors



- A box camera without a housing is installed outdoors. The camera is damaged due to water penetration, as shown in Figure 3.

Figure 3 Box camera installed outdoors



Solution

- Only cameras that comply with IPX5 or later can be installed outdoors.
- To install box cameras outdoors, housings must be installed for the cameras.

Parent topic: Common Installation Errors

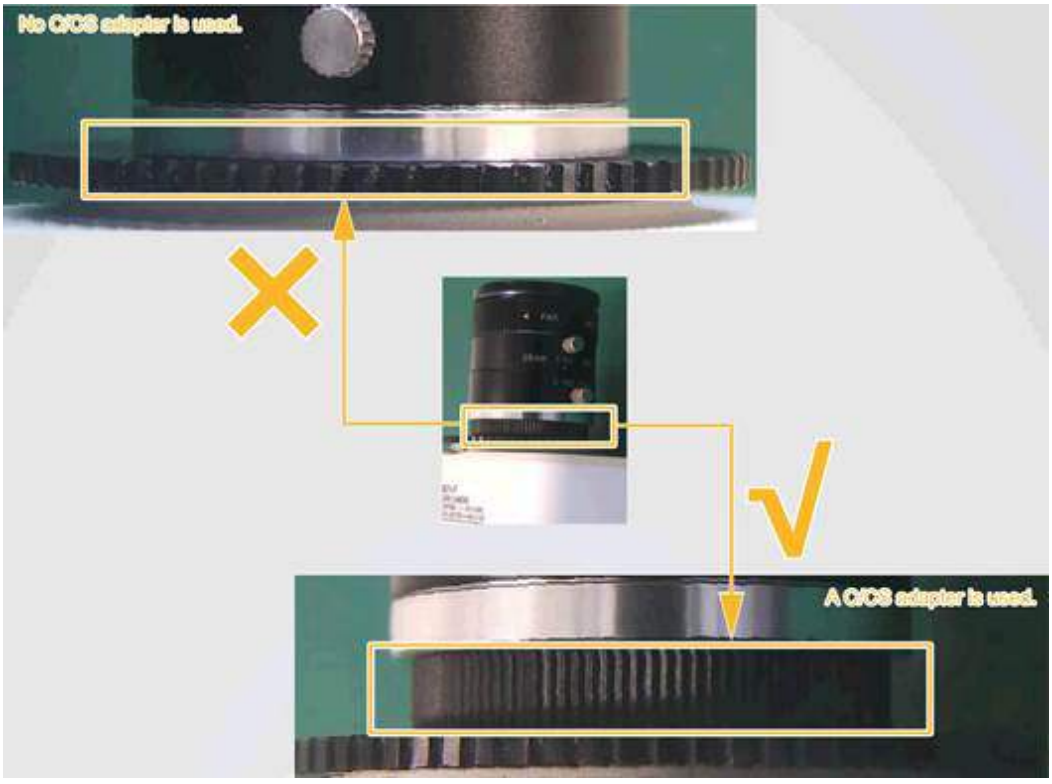
Misapplication of C- and CS-mount Lenses

A lens can be installed on a C-mount or a CS mount. A C-mount lens must be installed on a C-mount. To install a C-mount lens on a CS mount, you must use a C/CS lens adapter. Otherwise, camera faults may occur.

Typical Example

To install a C-mount lens on a CS mount, you must use a C/CS lens adapter, as shown in Figure 1.

Figure 1 No C/CS lens adapter used



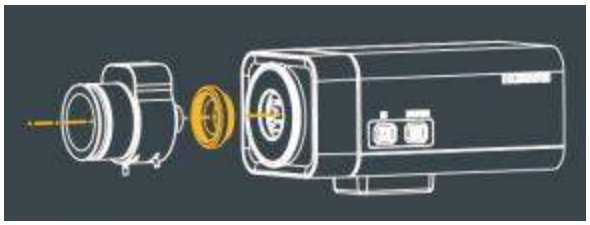
Symptom

1. Images cannot be focused.
2. The IR-CUT is stuck, so the camera cannot switch between the day and night modes.

Correct Operations

The C-mount lens is installed on the CS mount, as shown in Figure 2.

Figure 2 Installing the C/CS lens adapter



Parent topic: Common Installation Errors

Device Installation Failure Due to Incompatible PTZ Dome Camera Mount

When installing a PTZ dome camera, use a mount that matches the adapter ring to avoid installation issues or other issues caused by incompatible mounts.

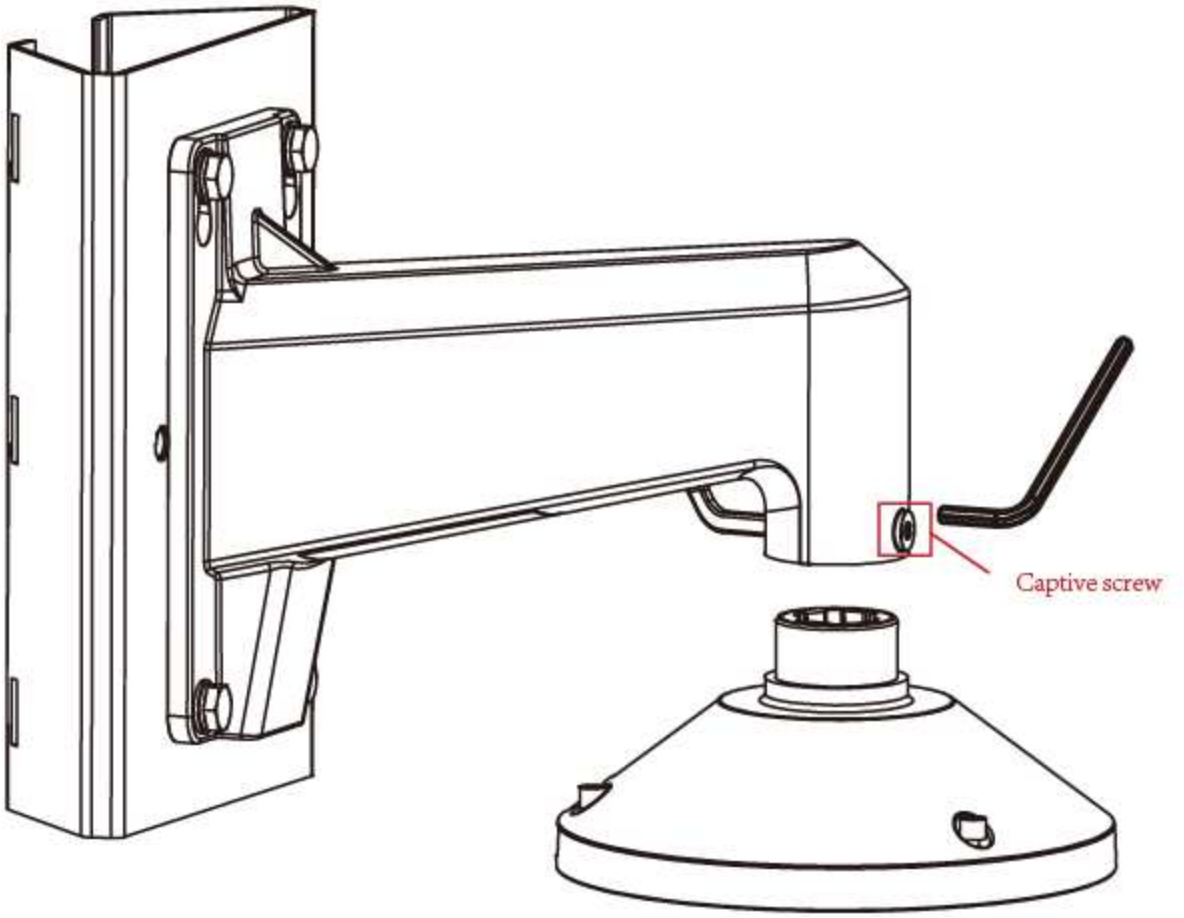
Symptom

The PTZ dome camera mount does not meet the GB standard (for example, incompatible size). Therefore, the PTZ dome camera cannot be properly installed or other issues may occur.

Solution

Use a mount that matches the adapter ring and fasten the captive screw on the mount, as shown in the following figure.

Figure 1 PTZ dome camera mount



NOTE

Users shall bear all the liabilities for installation issues or other issues caused by incompatible mounts.

Parent topic: Common Installation Errors

Network Port Corroded by Water Due to Lack of Waterproof Measures for Pigtails

This section describes the network port corrosion issue due to lack of waterproof measures for pigtails of outdoor cameras and the solution to handle the issue.

Typical Example

Figure 1 Corroded network ports and connectors



Symptom

The camera goes offline frequently or fails to be powered on, or artifacts occur.

Root Cause

The pigtails of outdoor cameras are not waterproofed, causing network port corrosion due to water leakage.

Solution

Waterproof kits are delivered with cameras by default, as shown in Figure 2. In addition, waterproof kits are pre-installed on the network ports before delivery. You need to install the waterproof kit during the construction. The quick start guide provides a complete waterproofing and insulation procedure.

Figure 2 Network port pre-installed with waterproof kit before delivery



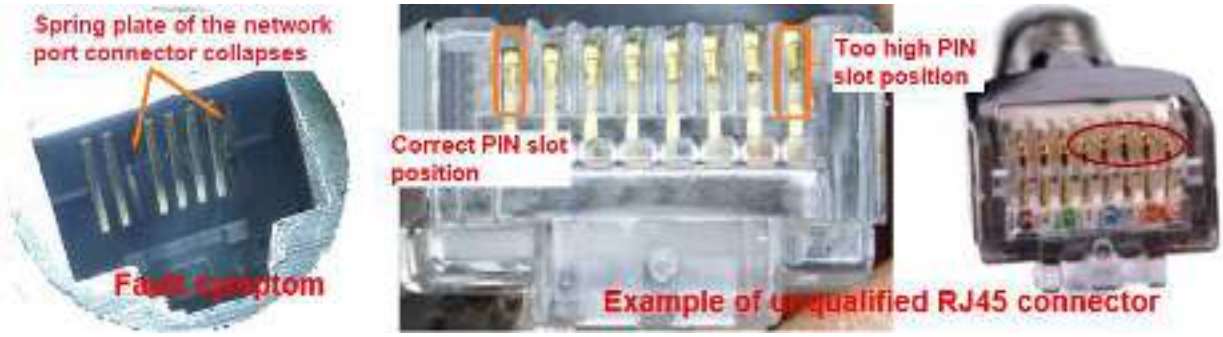
Parent topic: Common Installation Errors

Camera Fault Due to Unqualified Self-Made RJ45 Connectors

This section describes the camera fault caused by unqualified self-made RJ45 connectors and the method for making qualified RJ45 connectors.

Typical Example

Figure 1 Example of unqualified RJ45 connector



Symptom

The network port of the camera is damaged. As a result, the camera is offline or powered off.

Root Cause

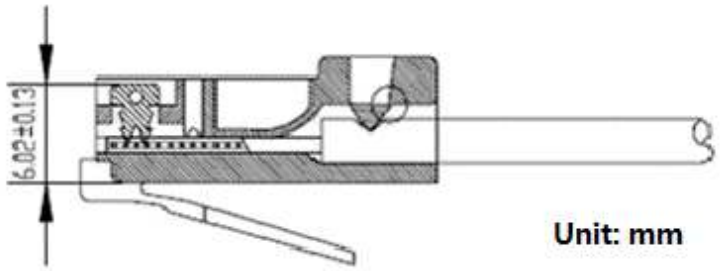
During camera installation, network cables need to be routed through pipes, for which RJ45 connectors are prepared onsite. Unqualified RJ45 connectors will damage the camera network port.

Solution

The crimp height of the RJ45 connector should range from 5.89 mm to 6.15 mm, as shown in Figure 2. The network port connector of cameras is enhanced based on the industry standard and is compatible with the RJ45 connector of 6.5 mm crimp height. If the RJ45 connector has a crimp height higher than 6.5 mm, the spring

plate of the network port connector will collapse, causing poor contact.

Figure 2 RJ45 crimp height requirement



CAUTION

- After crimping the network cable onsite, check whether the crimping is proper and whether the pin height is consistent. If not, crimp the network cable again to prevent damage to the camera network port or poor contact.
- Use qualified RJ45 connectors and periodically check whether the connectors are aged.

Parent topic: Common Installation Errors

Fiber Pigtail Cut Due to Improper PTZ Dome Camera Installation

This section describes the fiber pigtail cut due to improper camera installation and the correct installation method.

Typical Example

Figure 1 Load bearing through the pigtail due to incorrect installation



Root Cause

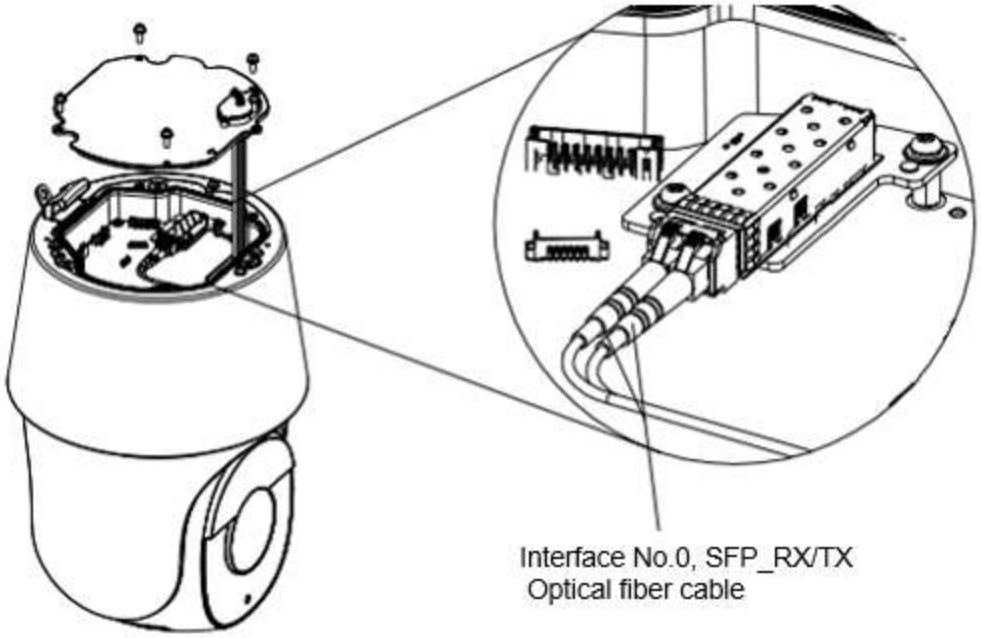
By default, cameras are not delivered with optical modules. Therefore, for cameras with fiber pigtails, you need to install optical modules onsite and insert the optical fibers. Optical fibers are prone to damage. You need to strictly follow the installation guide to avoid excessive bending or pulling of the fibers and prevent fiber damage.

Solution

Before installing the camera on the pole, install the optical module.

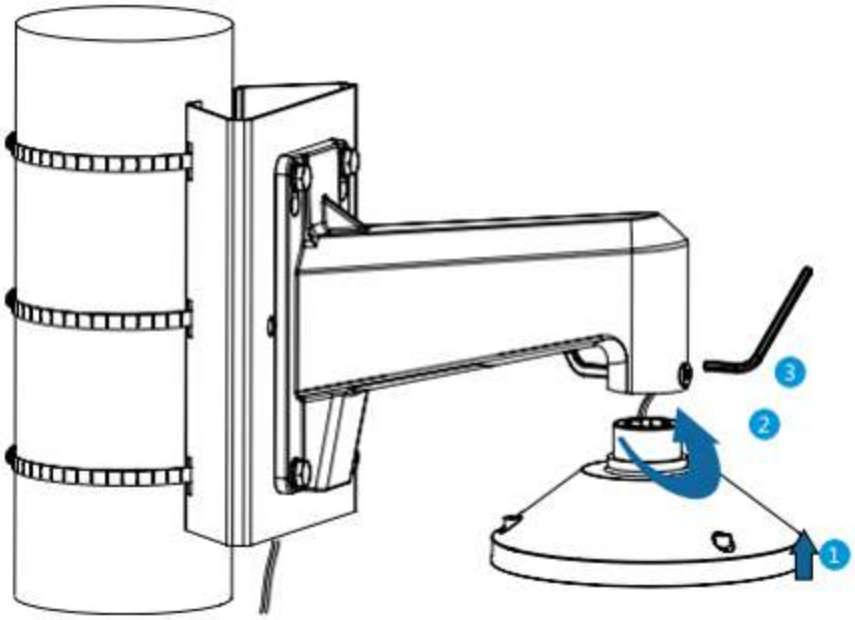
1. Install the optical module.

   Figure 2 Installing the optical module



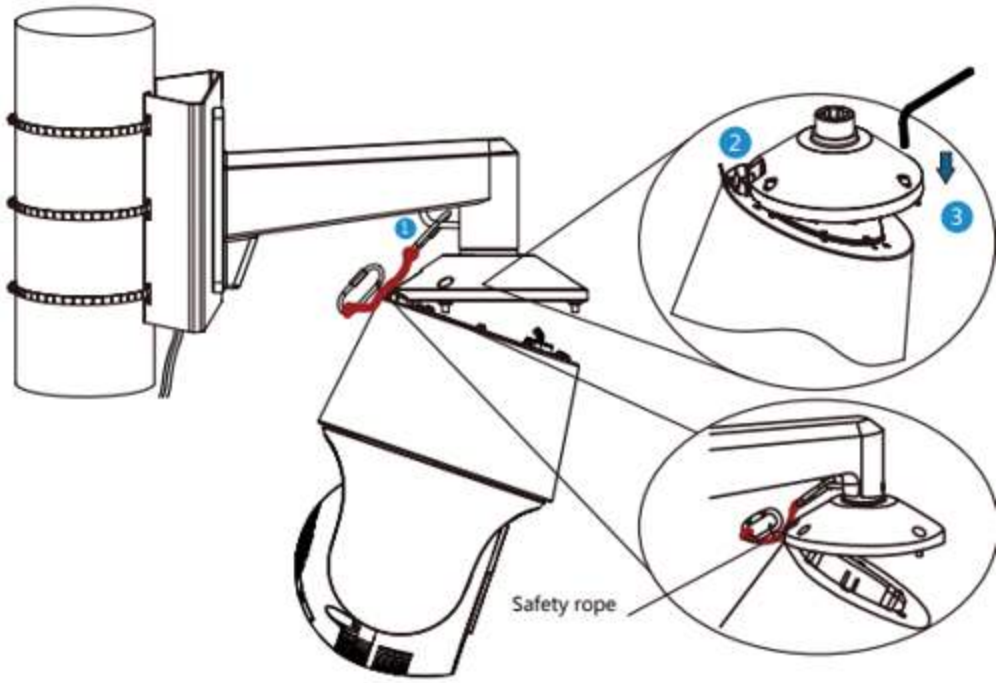
2. Install the rear cover of the PTZ dome camera on the bracket.

   Figure 3 Installing the rear cover of the PTZ dome camera on the bracket



3. Mount the PTZ dome camera to the rear cover and then connect cables.

   Figure 4 Mounting the PTZ dome camera to the rear cover and connecting cables



CAUTION

The load-bearing capacity of the optical fibers is only about 75 N. If the pulling force exceeds 75 N, the fibers may be broken. Therefore, use a safety line to pull the PTZ dome camera during installation instead of pulling the pigtail.

Parent topic: Common Installation Errors

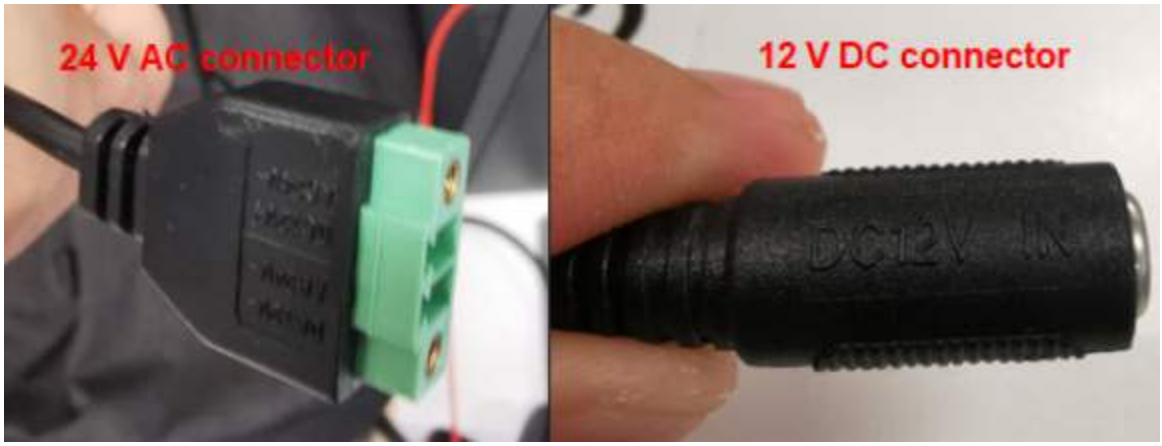
Camera Damage Due to Improper Cabling for Power Supply

This section describes the camera damage due to improper cabling for power supply and the correct cabling method.

Symptom

There are two mainstream power supplies in the industry: 12 V DC and 24 V AC. Figure 1 shows common cameras that use 12 V DC or 24 V AC power supply. Generally, high-power models use 24 V AC power supply, and low-power models use 12 V DC power supply. For models supporting both specifications, ports with foolproof design are provided to prevent improper cabling. However, many cameras are burnt due to incorrect voltage connection onsite.

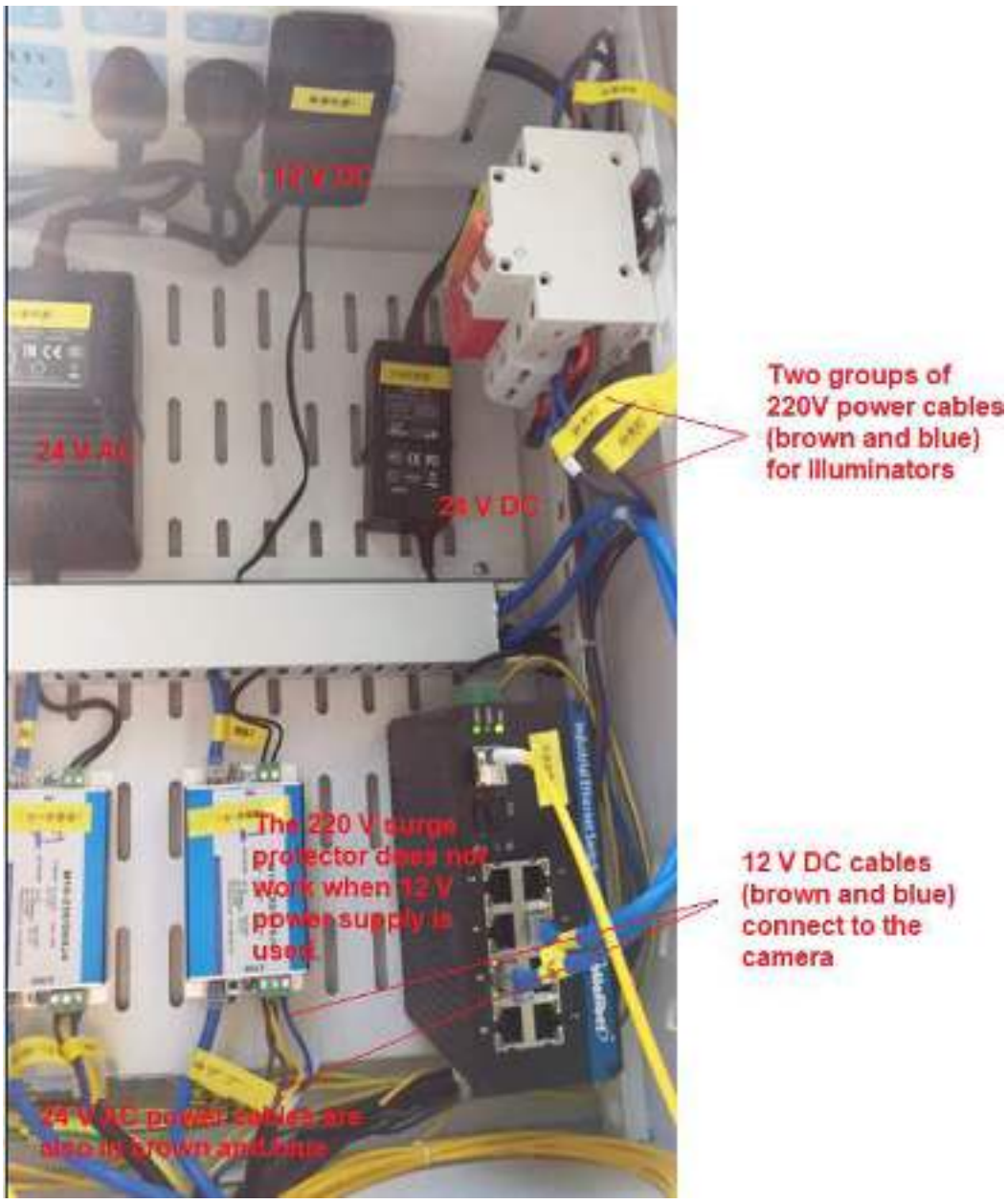
Figure 1 Mainstream camera power supply specifications



Solution

In Figure 2, the colors and specifications of the output cables of the two types of adapters are the same as those of the 220 V AC illuminator. It is difficult to distinguish between different voltages when routing cables on the pole. If high voltage is connected to the camera by mistake, the camera may be burnt. Therefore, power cables of different colors must be used for different voltages during project delivery to prevent incorrect connection.

Figure 2 Example of the output cable of power adapter



Parent topic: [Common Installation Errors]

Water Seepage Due to Improper Camera Installation Outdoors

This section describes water seepage due to improper camera installation outdoors and the correct installation method.

Typical Example

Figure 1 Water seepage



Root Cause

- The camera installed outdoors is not waterproofed.
- Fixed dome cameras support only indoor and roof-mounted installation, and cannot be installed outdoors, as shown in Figure 2.

Figure 2 Outdoor installation of the fixed dome camera



Solution

Cameras installed outdoors need to be waterproofed, and housings need to be installed for box cameras to be installed outdoors. During the installation, ensure that rain will not enter the housing. Figure 3 shows an example of correct installation.

Figure 3 Correct installation example



Parent topic: Common Installation Errors

Network Port Damage Due to Forcible Cable Pulling

This section describes network port damage due to forcible cable pulling and the correct operations.

Typical Example

Figure 1 Network port is damaged after pulling the network cable forcibly without removing the waterproof kit



Figure 2 Network port is not damaged after the waterproof kit is removed



Root Cause

Our RJ45 connectors have been strengthened compared with those in the industry. However, faulty network port connectors are often returned from the live network. According to the analysis and reproduction result in the lab, the network port damage is caused by forcible cable pulling.

Solution

The camera pigtails are integrated with the camera shell. If the network port is damaged, you need to replace the shell and pigtails together. Therefore, if you need to uninstall the device when it is faulty, you must remove the waterproof kit from the network port and do not forcibly pull the pigtails.

Parent topic: Common Installation Errors

Camera Deviation from the Preset Position Due to Loose Screws of the Bracket

This section describes camera deviation from the preset position due to loose screws of the bracket and the solution.

Typical Example

In Figure 1, the coordinates in the lower left corner of the two images are the same, but the video images are completely different, indicating that the camera has deviated from the preset position.

Figure 1 Camera deviation from the preset position



Symptom

The PTZ dome camera can automatically shoot video along the preset positions. Since the camera is heavy, there is a large habit when it rotates. Therefore, if the screws on the adapter ring of the camera are not tightened securely, the camera direction may change after it runs for a period of time due to the habit. As a result, the camera deviates from the preset positions.

Root Cause

The screws are not tightened, as shown in the left image of Figure 2.

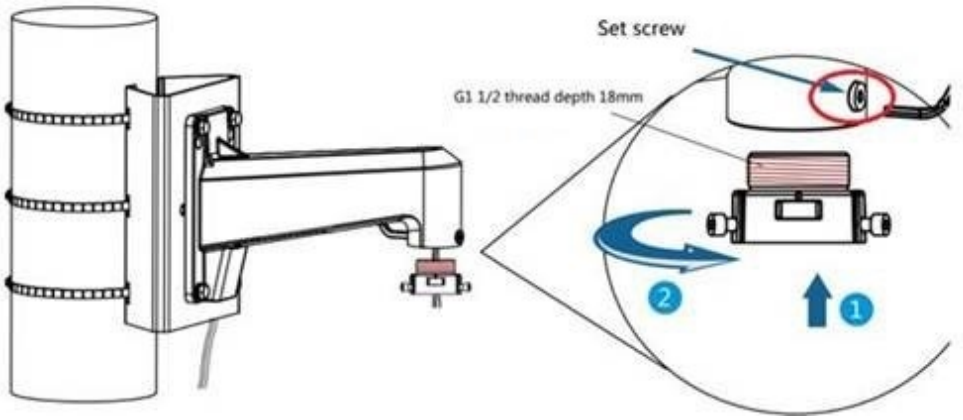
Figure 2 Example of tightening screws



Solution

- Tighten the screws by referring to the quick start guide.

  Figure 3 Guide to tightening the screws



- After the installation is complete, check whether all screws are tightened as required.

Parent topic: Common Installation Errors

Severe Corrosion of Common Cameras Installed at the Seaside

This section describes the anti-corrosion specifications of cameras and the camera selection for different environments.

Typical Example

Figure 1 Corrosion of a common camera installed at the seaside



Root Cause

A common camera instead of an anti-corrosion camera is installed in corrosive environments, resulting in severe camera corrosion.

Solution

Cameras are classified into class C and class D anti-corrosion cameras. Class D anti-corrosion cameras are dedicated to highly corrosive environments such as the seaside, chemical plants, and salt lakes. Class C cameras are common cameras, which may be corroded or malfunction when installed in corrosive environments. Select cameras based on the site requirements.

Parent topic: Common Installation Errors

Red Artifacts on Video Images Since the Protective Film Is Not Removed

This section describes the issue of red artifacts on video images since the protective film is not removed from the camera.

Typical Example

Figure 1 Fault Image



Symptom

If the protective film on the camera is not removed, it may affect camera focus. It is difficult to tell whether a transparent protective film is removed. Therefore, we add red tip texts on the film. If the film is not removed, red artifacts appear on video images, as shown in Figure 1. In this way, users can check whether the film is removed directly on video images without visiting the site.

Figure 2 Removing the protective film after the installation



Solution

The cameras are delivered with dedicated protective films to protect the viewing window during transportation and installation. After the installation is complete, remove the protective films.

Parent topic: Common Installation Errors

Appendixes

Insulating and Waterproofing You need to wrap interconnected cables with insulation tape and waterproof tape to prevent short circuits and water leakage.

Making the Network Cable
This topic describes how to assemble the RJ45 connector and CAT 5e cable into a network cable.

Replacing the Rain Wiper Rubber Strip
If the rain wiper rubber strip is damaged, you can manually replace it.

Parent topic: Installation Guide

Insulating and Waterproofing

You need to wrap interconnected cables with insulation tape and waterproof tape to prevent short circuits and water leakage.

Context

You need to wrap a layer of PVC insulation tape, then a layer of waterproof tape, and then a layer of PVC insulation tape again. The following describes the detailed procedure.

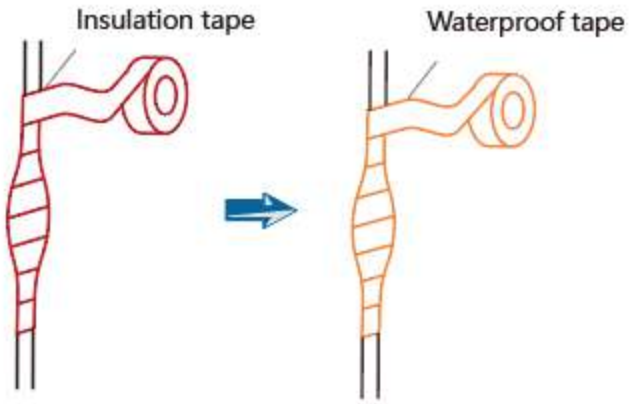
NOTICE

When wrapping insulation tape and waterproof tape, ensure that each layer of tape covers more than 50% of the lower layer and each layer is tightly pressed.

Procedure

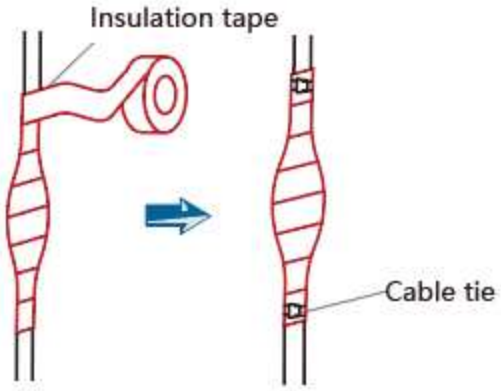
1. Wrap one layer of insulation tape around the joint of each cable. Stretch the waterproof tape evenly to twice its original length. Then, apply one layer of waterproof tape.

   Figure 1 Wrapping the insulation tape and waterproof tape

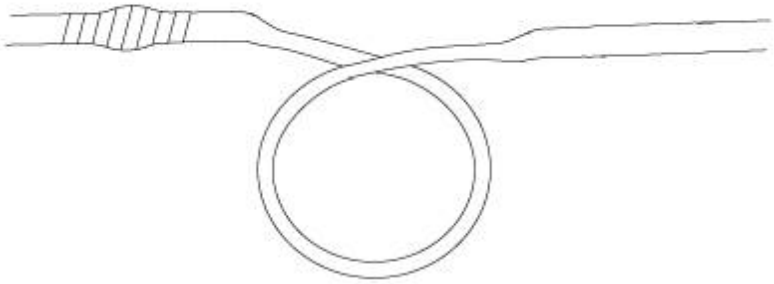
2. Use the insulation tape to protect the waterproof tape layer. Use cable ties to secure both ends of the tape.

Figure 2 Wrapping insulation tape and using cable ties to secure both ends of the tape



3. Cover the rest of the cabling in a conduit or with waterproof tape and make a drip loop. The drip loop, as shown in Figure 3, forms the lowest point of the cable.

Figure 3 Drip loop



Parent topic: Appendixes

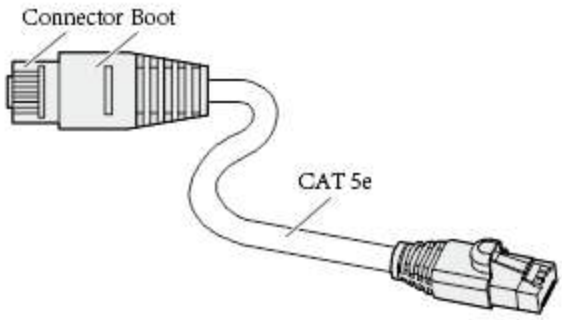
Making the Network Cable

This topic describes how to assemble the RJ45 connector and CAT 5e cable into a network cable.

Context

The network cable consists of two RJ45 connectors, one CAT 5e cable, and boots. Figure 2 shows the outline of the network cable.

Figure 1 Components of the network cable

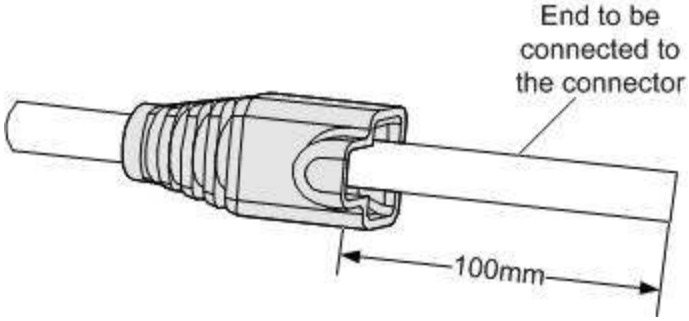


Procedure

Use an RJ45 crimping tool to cut the CAT 5e cable.

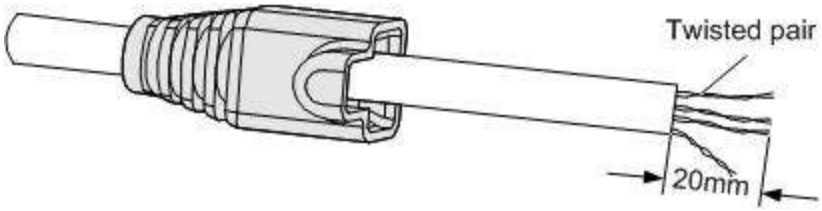
1. Insert the cable into the boots, and reserve at least 100 mm for the boots. Do not put the boots in reverse direction. Figure 2 shows the right direction.

   Figure 2 Installing the boots for the RJ45 connector



2. Use a blade or a knife to peel 20 mm off the jacket. Do not damage the insulation of the wires, as shown in Figure 3.

   Figure 3 Peeling the jacket



3. Arrange the wires neatly according to the connection sequence of the network cables. Leave the wires with a length of 13 mm to 15 mm and cut off the redundant part, ensuring proper lengths of the remaining wires. Put the wires into the RJ45 connector. Figure 4 shows the correct order.

   Figure 4 Installing the wires

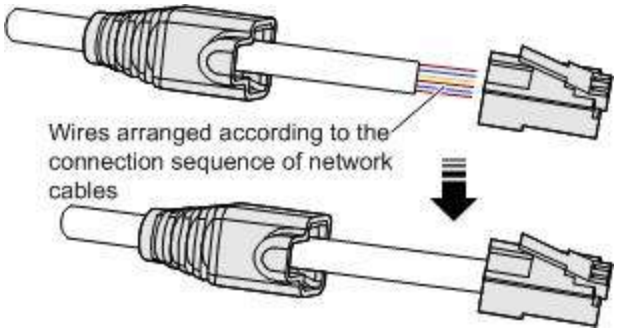


   Table 1 shows two types of network cable sequences.

   - When the straight-through cable is made, the sequences of both ends of the network cable should be consistent, that is, both ends of the network cable are sequence A or sequence B at the same time.
   - When the crossover cable is made, the sequences of both ends of the network cable should be inconsistent, that is, one end of the network cable is sequence A and the other end of the network cable is sequence B.

   Table 1 Connection sequence of the network cables

Replacing the Rain Wiper Rubber Strip

If the rain wiper rubber strip is damaged, you can manually replace it.

Tools to Be Prepared

Table 1 describes the tools to be prepared.

Table 1 Tools to be prepared

Tool	Icon
Torque screwdriver Or Adjustable wrench	 
Rain wiper rubber strip **NOTE:** Contact the camera supplier to obtain it.	
LOCTILE 243 threadlocker	

Procedure

Use a torque screwdriver or adjustable wrench to remove the M4 hexagon nut from the rain wiper. Then remove the spacer and take down the rain wiper bracket, as shown in Figure 1.

Figure 1 Disassembling the rain wiper bracket



1. Remove the old rubber strip and insert the new rubber strip through the hole, as shown in Figure 2.

   Figure 2 Replacing the rain wiper rubber strip

2. Assemble the rain wiper bracket and rubber strip to the device, apply thread adhesive to the exposed threads, install the spacer, and tighten the nut, as shown in Figure 3.

   Figure 3 Installing the rain wiper bracket

NOTE

- If the torque screwdriver is used, adjust the torque to 8-12 kgf.cm and tighten the nut.
- If the adjustable wrench is used, hold the wrench at a position close to the nut and tighten the nut.

----End

Parent topic: Appendixes

Configuration

Initial Camera Configuration Processes Different types of cameras support different functions. Therefore, their configuration processes vary from each other. This chapter describes the initial configuration process for each type of cameras. You can also click links provided in process description tables to go to the specific configuration section.

Logging In to the Camera Web System
You can log in to the camera web system using a web browser on your PC and perform operations such as live video viewing and camera-related configurations. This chapter uses Internet Explorer 11 as an example to describe how to log in to a camera.

Web Page Layout
You can access cameras through a web browser and manage cameras on the web page, for example, setting camera parameters. The supported functions vary depending on the camera model.

Introduction to the Right Pane on the View Page
By modifying some configuration items on the right pane of the **View** page, you can perform configuration operations related to video viewing, device IP address, system time, image, and video streams. Different camera models may have different parameters.

Wizard-based Configuration Guide
If a camera is used for the first time or has been restored to factory defaults, when you log in to the camera web system, the wizard-based configuration page is displayed. On this page, you can quickly configure some services of the camera. You can also go to the wizard-based configuration page even if it is not your first login.

Local Parameters
You can set local parameters, such as the protocol type, code

stream type, video stream type, and path where snapshots are saved. These settings take effect only on the local computer.

Managing the System
This section describes how to configure system operations.

Setting Network Parameters
This section describes how to set network parameters such as the IP address.

Configuring Platform Connection
Cameras can connect to video security platforms through the SDK, GB/T 28181, or ONVIF protocol. Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera.

Video and Audio Configuration
This chapter describes how to set video and audio parameters.

Configuring Images
This chapter describes how to set image-related parameters, including image parameters, image profiles, and profile plans.

Playback
This section describes how to query, download, and delete recordings, configure recording plans, and play back recordings.

Image Query and Download
You can query and download images on the web page.

Configuring PTZ Control
This section describes how to set pan-tilt-zoom (PTZ) parameters, including serial port, preset position, and tour parameters.

Intelligent Settings
This section describes how to configure intelligent analysis functions such as intelligent behavior analysis, motion detection, lens blocking detection, and sound detection.

Event Configuration

This chapter describes how to configure intelligent event analysis functions such as motion detection, video quality diagnosis, lens blocking detection, and sound detection.

Storage Configuration

This section describes how to configure functions including storage management, snapshot taking parameters, and recording plans.

Service Management

This chapter describes the alarm feature differences, extended interface service, alarm service, channel service, and general configuration service of cameras.

Viewing Intelligent Display Results

This section describes how to check detection results after intelligent analysis functions are configured.

FAQs

This chapter describes how to locate and troubleshoot common faults.

FAQs

This chapter describes how to locate and troubleshoot common faults.

Configuring Image Optimization

Initial Camera Configuration Processes

Different types of cameras support different functions. Therefore, their configuration processes vary from each other. This chapter describes the initial configuration process for each type of cameras. You can also click links provided in process description tables to go to the specific configuration section.

Situation Awareness Cameras

Micro Checkpoint Cameras

Target Capture Cameras
*** shows the initial configuration process for a target capture camera.

Parent topic: Configuration

Situation Awareness Cameras

Figure 1 shows the initial configuration process for a situation awareness camera. Table 1 describes the related tasks during the actual operation.

Figure 1 Initial configuration process

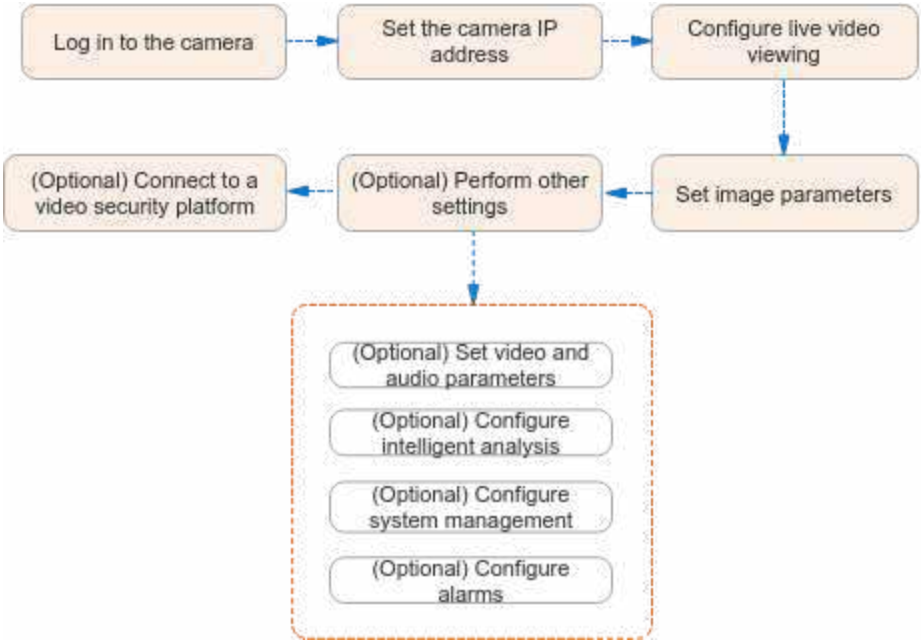


Table 1 Process description

Step	Description
Log in to the camera.	Obtain the camera IP address and log in to the camera using a web browser on your computer. For details about the software and hardware requirements for logging in to the camera and about how to log in, see Logging In to the Camera Web System.
Set the camera IP address.	The default IP address of the camera is **192.168.0.120**. Change it to the planned IP address. For details, see Setting Camera IP Addresses.
Configure live video viewing.	By configuring live video viewing, you can perform operations related to live video viewing, including configuring pan-tilt-zoom (PTZ) information and

Step	Description
	setting the camera IP address, time, common image parameters, common video parameters, and OSD parameters. For details, see Introduction to the Right Pane on the View Page.
Set image parameters.	By setting image parameters, you can adjust images to adapt to applications in different scenarios. You can also set image profiles for common scenarios so that you can quickly invoke an image profile in a specific scenario. After configuring an image profile, you can configure a daily or annual image profile plan. For details, see Configuring Images.
(Optional) Set video and audio parameters.	You can set video and audio parameters, such as the stream type, encoding protocol, resolution, and bit rate, based on the site requirements. For details, see Video and Audio Configuration.
(Optional) Configure intelligent analysis.	This configuration is required if you need to use intelligent analysis functions such as motion detection, lens blocking detection, and sound detection. For details, see Event Configuration.
(Optional) Configure alarms.	This configuration is required only when the alarm linkage function is required or the initial alarm threshold needs to be changed. When an alarm is reported, the system can trigger proper actions according to the preset alarm linkage policy. For details, see the alarm configuration for the desired intelligent analysis function in Alarm Service.
(Optional) Perform system management.	The functions, such as time setting, under **System** are optional. For details, see Managing the System.

Step	Description
(Optional) Connect to a video security platform.	Cameras can connect to video security platforms through the SDK, GB/T 28181, or ONVIF protocol. Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera. For details, see Configuring Platform Connection.

Parent topic: Initial Camera Configuration Processes

Micro Checkpoint Cameras

Figure 1 shows the initial configuration process for a micro checkpoint camera. Table 1 describes the related tasks during the actual operation.

Figure 1 Initial configuration process

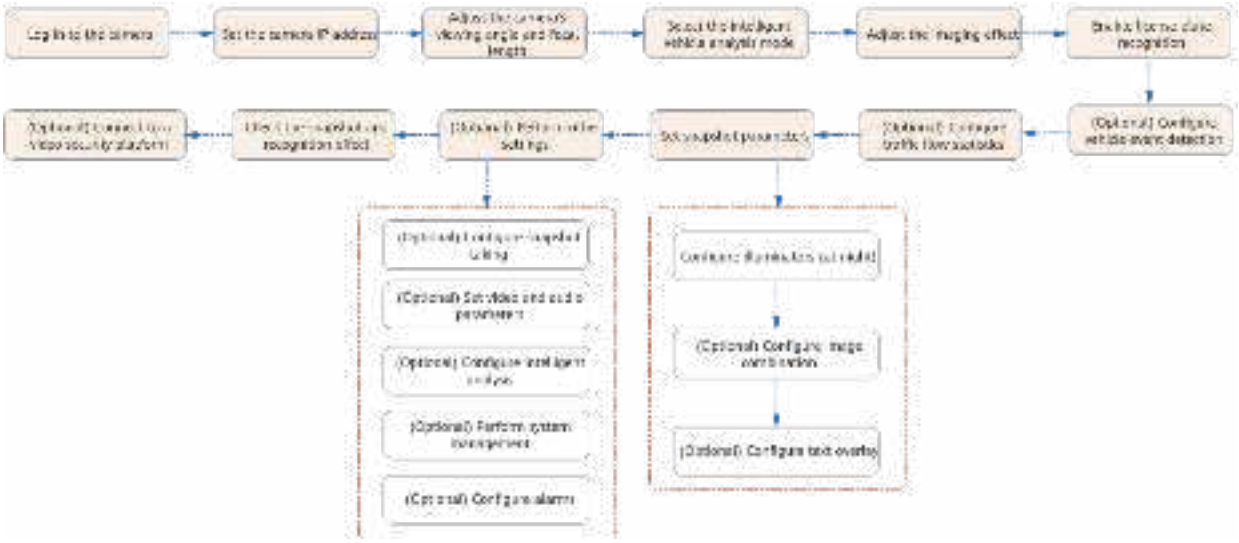


Table 1 Process description

Step	Description
Log in to the camera.	You can obtain the camera IP address and log in to the camera using a web browser on your computer. For details about the software and hardware requirements for logging in to the camera and about how to log in, see Logging In to the Camera Web System.
Set the camera IP address.	After logging in to the camera, you need to change the camera IP address on the web page based on the network plan. For details, see Setting Camera IP Addresses. To perform other network settings for the camera, refer to related sections in Setting Network Parameters.

Step	Description
Adjust the camera's viewing angle and focal length.	You can adjust the camera's viewing angle and focal length.
Select the intelligent vehicle analysis mode.	Select the intelligent vehicle analysis mode and configure related services. For details, see Configuring Intelligent Vehicle Analysis.
Adjust the imaging effect.	Adjust the imaging effect of the camera.
Enable license plate recognition.	After the camera is installed, you can verify the virtual checkpoint function to prevent subsequent camera angle re-adjustment due to undesirable imaging effect. If object classification is required, see Configuring Object Classification. If only license plate recognition is required, see Configuring Motor Vehicle Capture.
(Optional) Configure vehicle event detection.	To enable the system to detect vehicle events, such as motor vehicles driving in non-motorized vehicle lanes, non-motorized vehicles driving in motor vehicle lanes, and parking violation, and report alarms accordingly, you need to configure vehicle event detection. For details, see Configuring Intelligent Vehicle Event Analysis.
(Optional) Configure traffic flow statistics.	To enable the system to detect traffic flows and report alarms accordingly, you need to configure traffic flow statistics. For details, see Configuring Intelligent Traffic Flow Analysis.

Step	Description
Set snapshot parameters.	• Configure illuminators. In low light environments, the illuminators need to be enabled for light compensation. The configuration must be performed at night to check the configuration effect. For details, see Illuminator Control. • (Optional) Configure image combination. Image combination enables you to combine the full image and close-up images into one image for better image viewing. The image combination function is not applicable to object classification or vehicle event detection. For details, see Configuring Image Combination. • (Optional) Configure text overlay. You can superimpose information such as the snapshot time, license plate, and vehicle type on snapshots. The text overlay function is not applicable to vehicle event detection. For details, see Configuring Text Overlay.
(Optional) Perform other settings.	You can perform the following settings depending on your needs: • (Optional) Configure snapshot taking. You can set parameters related to snapshot taking, such as the SD card space, scheduled snapshot, and snapshot upload to the FTP server. For details, see Image Query and Download. • (Optional) Set video and audio parameters. You can set video and audio parameters, such as the stream type, encoding protocol, resolution, and bit rate, based on the site requirements. For details, see Video and Audio Configuration.

Step	Description
	• (Optional) Configure intelligent analysis. This configuration is required if you need to use intelligent analysis functions such as motion detection, lens blocking detection, and sound detection. For details, see Event Configuration. • (Optional) Perform system management. The functions, such as time setting, under **System** are optional. For details, see Managing the System. • (Optional) Configure alarms. This configuration is required only when the alarm linkage function is required or the initial alarm threshold needs to be changed. When an alarm event occurs, the system can trigger proper actions according to the preset alarm linkage policy. For details, see the alarm configuration for the desired intelligent analysis function in Alarm Service.
Check the snapshot and recognition effect.	You can check the snapshot and recognition effect through intelligent detection configuration. For details, see Viewing Configuration Results. If the traffic statistics function has been configured, you can view the traffic flow information. For details, see Configuring Intelligent Traffic Flow Analysis.
(Optional) Connect to a video security platform.	Cameras can connect to a video security platform through the SDK, GB/T 28181, or ONVIF protocol. Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera. For details, see Configuring Platform Connection.

Parent topic: Initial Camera Configuration Processes

Target Capture Cameras

Figure 1 shows the initial configuration process for a target capture camera.

Table 1 describes specific steps in the actual configuration.

Figure 1 Initial configuration process

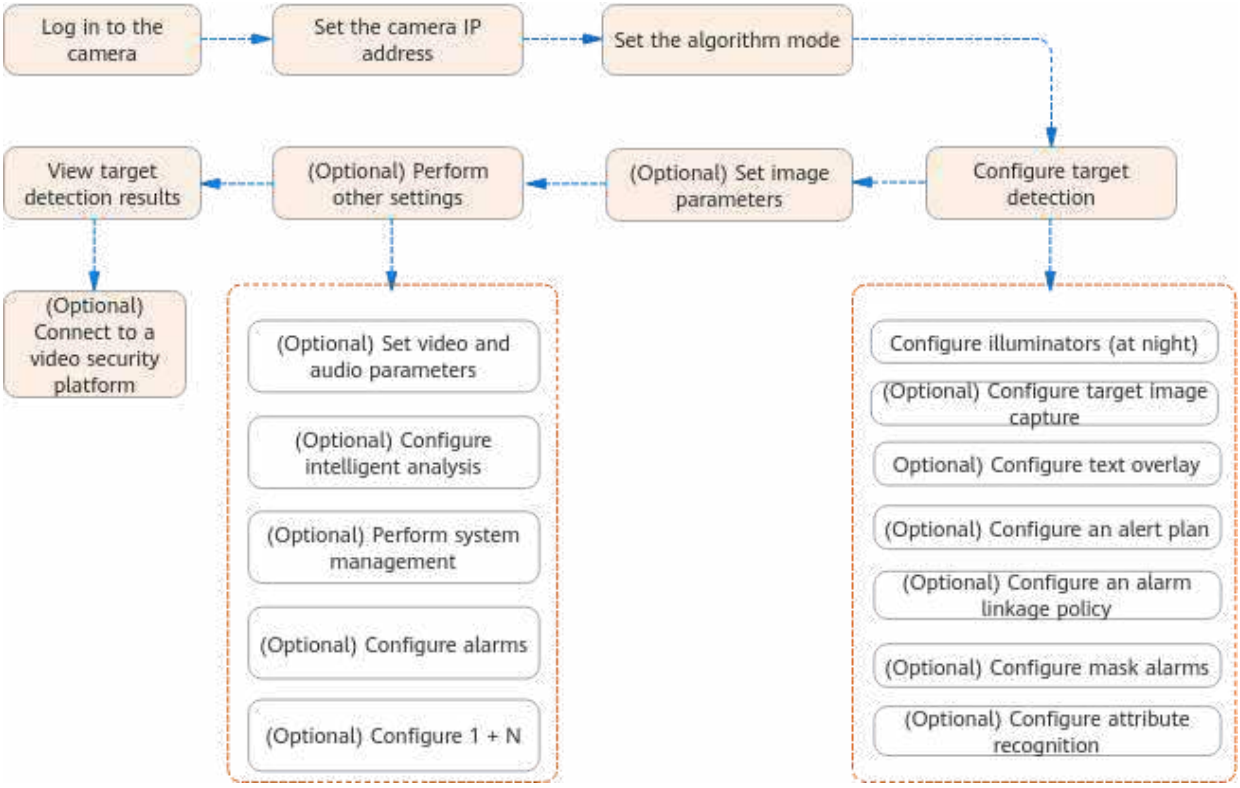


Table 1 Process description

Step	Description
Log in to the camera.	Obtain the camera IP address and log in to the camera using a web browser on your computer. For details about the software and hardware requirements for logging in to the camera and about how to log in, see Logging In to the Camera Web System.
Set the camera IP address.	After logging in to the camera, change the camera IP address on the web page based on the network plan. For details, see Setting Camera IP Addresses.

Step	Description
	To perform other network settings for the camera, refer to related sections in Setting Network Parameters.
Set the algorithm mode.	Select the required algorithm mode and configure related services. For details, see Intelligent Settings.
Configure target detection.	Enable the target detection and capture functions and set related parameters such as the capture sensitivity. For details, see Configuring Intelligent Target Analysis. • In low light environments, illuminators need to be enabled for light compensation. The configuration must be performed at night to check the configuration effect. For details, see Illuminator Control. • You can configure the size of captured target images. For details, see Configuring Target Images. • You can superimpose information such as the snapshot time, device ID, and site information on captured full images. For details, see Configuring Text Overlay. • Set and enable a capture plan. By default, the system captures images for 24 hours every day. If you use the default plan, no setting is required. For details, see Configuring an Alert Plan. • If the target detection alarm needs to be linked with other services, such as email sending and video recording, you need to configure an alarm linkage policy. For details, see Configuring an Alarm Linkage Policy. • The camera supports mask alarms. For details, see Configuring Mask Detection.
Set image parameters.	Adjust the imaging effect of the camera. For details, see Configuring Images.

Step	Description
(Optional) Perform other settings.	You can perform the following settings depending on your needs: • (Optional) Set video and audio parameters. You can set video and audio parameters, such as the stream combination type, encoding protocol, resolution, and bit rate, based on the site requirements. For details, see Video and Audio Configuration. • (Optional) Configure intelligent analysis. This configuration is required if you need to use intelligent analysis functions such as motion detection, lens blocking detection, and sound detection. For details, see Event Configuration. • (Optional) Perform system management. The functions, such as time setting, under **System** are optional. For details, see Managing the System. • (Optional) Configure alarms. This configuration is required only when the alarm linkage function is required or the initial alarm threshold needs to be changed. When an alarm is reported, the system can trigger proper actions according to the preset alarm linkage policy. For details, see the alarm configuration for the desired intelligent analysis function in Alarm Service.
View target detection results.	If target images captured in real time are displayed on the right of the video pane, the target detection parameters are set successfully. For details, see Viewing Intelligent Detection Results.
(Optional) Connect to a	Cameras can connect to a video security platform through the SDK, GB/T 28181, or ONVIF protocol.

Step	Description
video security platform.	Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera. For details, see Configuring Platform Connection.

Parent topic: Initial Camera Configuration Processes

Logging In to the Camera Web System

You can log in to the camera web system using a web browser on your PC and perform operations such as live video viewing and camera-related configurations. This chapter uses Internet Explorer 11 as an example to describe how to log in to a camera.

Computer Software and Hardware Requirements This section describes the minimum and recommended software and hardware specifications for the computer.

Setting the Local Computer
This section describes how to configure the local computer to ensure that the computer properly communicates with the camera.

Logging In to a Camera
This section describes how to log in to a camera using a web browser, and set the password during the initial login.

Parent topic: Configuration

Computer Software and Hardware Requirements

This section describes the minimum and recommended software and hardware specifications for the computer.

Table 1 describes the specifications for the computer.

Table 1 Software and hardware requirements

Software/Hardware	Specification
CPU	Minimum: Intel fourth-generation Core i7 processor with a clock rate of 3.3 GHz or higher Recommended: Intel sixth-generation Core i7 processor with a clock rate of 3.3 GHz or higher
Video memory	1 GB or greater
Memory	8 GB DDR3 1600 MHz or higher
Network adapter	100 Mbit/s network adapter or higher
Disk	300 GB or greater
Monitor	22 inches or above
Operating system and browser	• Windows 7: Internet Explorer 10/11, Chrome 50+, Firefox 70+, Microsoft Edge 50+ • Windows 8: Internet Explorer 10/11, Chrome 50+, Firefox 70+, Microsoft Edge 50+ • Windows 10: Internet Explorer 11, Chrome 50+, Firefox 70+, Microsoft Edge 50+ **NOTE:** • Only 32- or 64-bit Windows operating systems are supported.

Software/Hardware	Specification
	• To use Chrome, Microsoft Edge, or Firefox to access the camera and view live video, ensure that the computer is on the public network so that the web control can be downloaded from the public network. • To download Google Chrome, click here. • To download Firefox, click here. • To download Internet Explorer, click here. • When you use the Firefox browser to view live video, if the menu or tool bar on the top of the browser is opened, the live video pane position deviates. You can manually close the menu or tool bar to rectify the fault.

Parent topic: Logging In to the Camera Web System

Setting the Local Computer

This section describes how to configure the local computer to ensure that the computer properly communicates with the camera.

Prerequisites

- Before logging in to the camera web system, ensure that the computer is properly connected to the camera.
- For a camera with a single network port, if the computer is directly connected to the camera, the IP address of the computer must be on the same network segment as that of the camera. For details, see Setting the Computer IP Address.
- For a camera with dual network ports, if network port 0 is used, ensure that the gateway device exists. If the computer is directly connected to the camera, the IP address of the computer must be the same as network port 0's IPv4 gateway address of the camera. To view the IPv4 gateway address of network port 1, choose **Settings** > **Network** > **TCP/IP**.
- To ensure video image effect, it is recommended that the screen resolution range from 1024 x 768 to 1920 x 1200.
- You must use an administrator account to log in to the Windows operating system. Otherwise, the control will fail to be installed and you cannot view live video on the web page.
- You need to set Internet Explorer before accessing the camera web system for the first time. Table 1 describes the procedure.

Table 1 Internet Explorer settings

Setting	Procedure
Disable the proxy server.	1. Choose **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed. 2. Click the **Connections** tab.

Setting	Procedure
	3. Click **LAN Settings**. 4. Clear the check box next to **Use a proxy server for your LAN**. 5. Click **OK**.
Enable the ActiveX controls and plug-ins or set them to the prompt mode.	1. Choose **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed. 2. Click the **Security** tab. 3. Select **Internet**. 4. Click **Custom Level**. The **Security Settings** dialog box is displayed. 5. Set **Automatic prompting for ActiveX controls** to **Enable**. Set **Download unsigned ActiveX controls** and **Initialize and script ActiveX controls not marked as safe** to **Prompt**. 6. Click **OK**.
Set **Use Pop-up Blocker** to **Disable**.	1. Choose **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed. 2. Click the **Security** tab. 3. Select **Internet**. 4. Click **Custom Level**. The **Security Settings** dialog box is displayed. 5. Set **Use Pop-up Blocker** to **Disable**. 6. Click **OK**.

Setting	Procedure
Enable TLS 1.1 or TLS 1.2.	**NOTE:** When using HTTPS to access a camera, you must enable TLS 1.1 or TLS 1.2. Otherwise, the camera web page cannot be displayed. 1. Choose **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed. 2. Click the **Advanced** tab. 3. Select **Use TLS 1.1** or **Use TLS 1.2**. 4. Click **OK**.

Setting the Computer IP Address

To use a computer to directly access a camera, ensure that the computer IP address is on the same network segment as the camera IP address. The following uses a computer running Windows 7 and the default camera IP address 192.168.0.120 as an example to describe how to set the computer IP address:

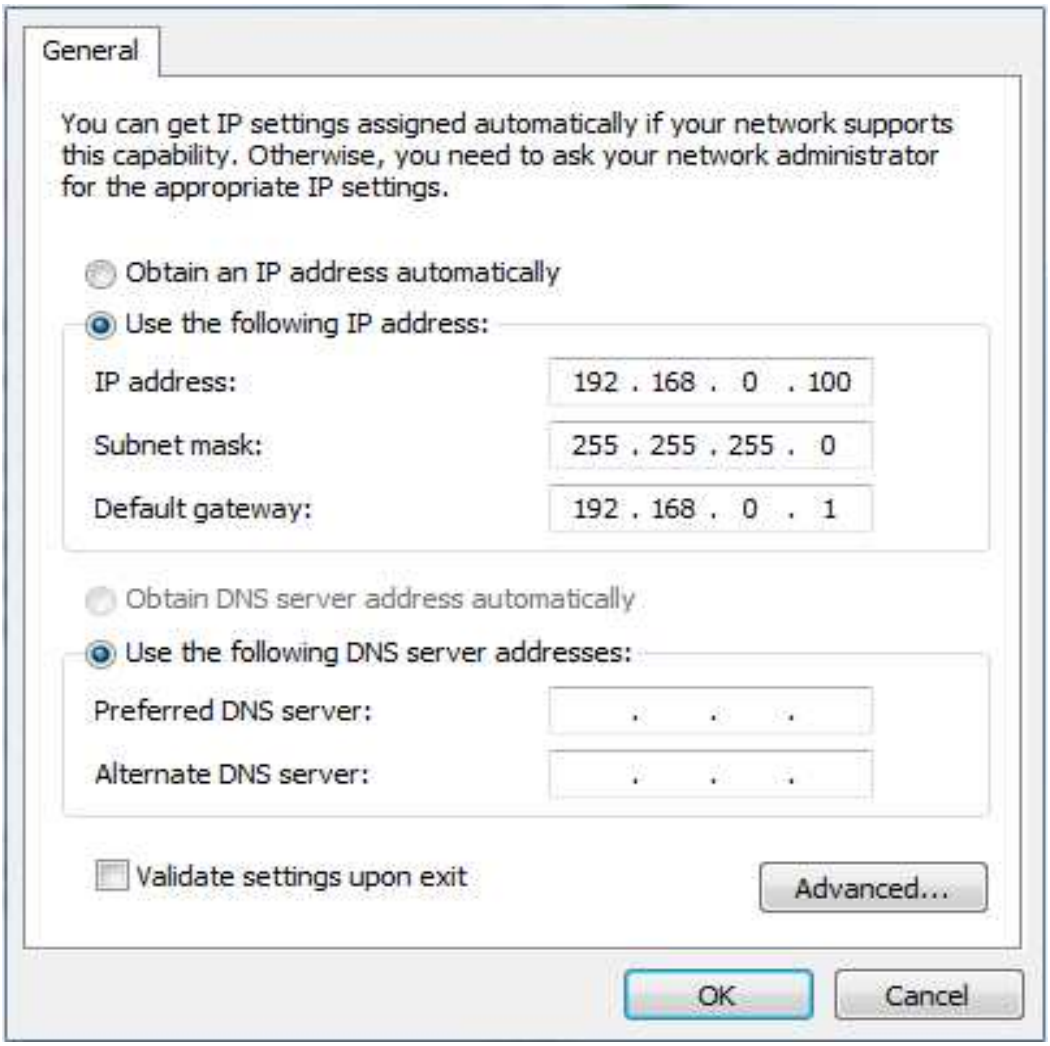
1. On the computer, choose **Control Panel** > **Network and Internet** > **Network and Sharing Center** to access the **Network and Sharing Center** page.
2. Click **Local Connection**. The **Local Area Connection Status** page is displayed.
3. Click **Properties**. On the **Local Area Connection Properties** page that is displayed, double-click **Internet Protocol Version (TCP/IPv4)**. The dialog box shown in Figure 1 is displayed.
4. Change the IP address, subnet mask, and default gateway of the local computer to ensure that the computer IP address is in the same network segment as the camera IP address. In

Figure 1, the IP address of the computer is set to 192.168.0.100.

NOTE

The default gateway can be left empty.

Figure 1 Changing the computer IP address



Parent topic: Logging In to the Camera Web System

Logging In to a Camera

This section describes how to log in to a camera using a web browser, and set the password during the initial login.

Logging In for the First Time

1. Right-click the Internet Explorer icon, choose **Run as administrator** from the shortcut menu, enter the camera IP address in the address box, and press **Enter**. (The default IP address of a camera is **192.168.0.120**. For an ITS camera with dual network ports, the default IP address of network port 0 is **192.168.0.120**, and that of network port 1 is **192.168.1.120**.)

   NOTE

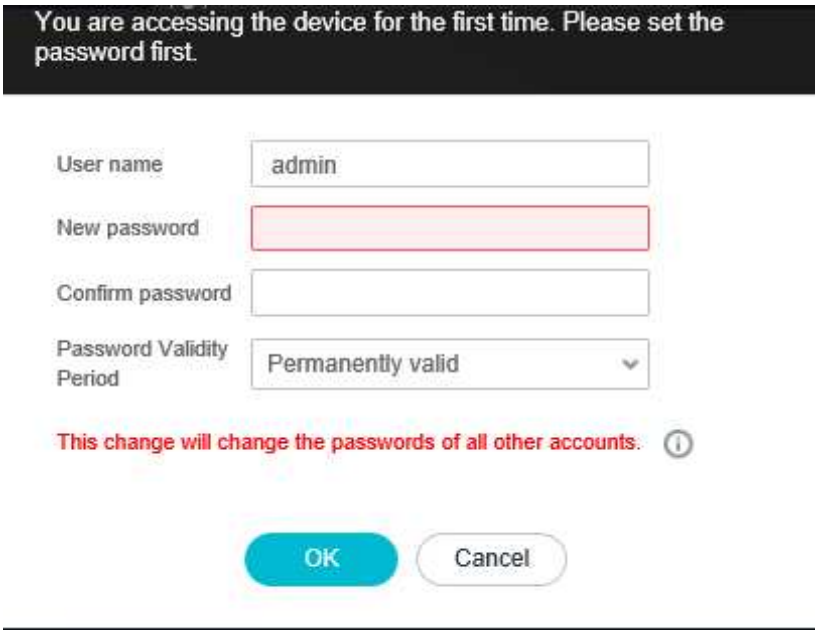
   - If Internet Explorer displays the message "Incorrect Security Certificate", you can click **Continue to this website (not recommended)** to access the login page. You can install the root certificate to resolve this problem. For details, see A Message Indicating that an Exception Occurred on the Website's Security Certificate Is Displayed When You Log In to the Camera Web System. If the login page cannot be displayed, see Failure to Display HTTPS Web Page on Internet Explorer.
   - If you use Internet Explorer 9 or an earlier version to log in to the camera and click **Continue to this website (not recommended)**, the browser recommendation page is displayed. Click the browser icon to download the browser for login. Otherwise, the login is not allowed.
   - If the **Log In** button is not displayed on the login page, rectify the fault by referring to No Login Button Is Displayed on the Camera Login Page.
   - When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can select **Obtain IP address automatically** to check the IP address. The camera IP address allocated by the server is fixed.
   - After the camera is upgraded, if the camera web page is improperly displayed, rectify the fault by referring to Improper Display of the Web Page upon the First Login After Camera Upgrade.

- The following web system languages are supported: Chinese, English, French, Spanish, Turkish, Italian, Portuguese (Brazil), and Portuguese (Europe).

2. Set the password as prompted when you log in for the first time, as shown in Figure 1.

   The login user name is **admin**. Upon the first login, you need to set the password and **Password Validity Period** and keep the new password secure.

   Figure 1 Setting the password



NOTE

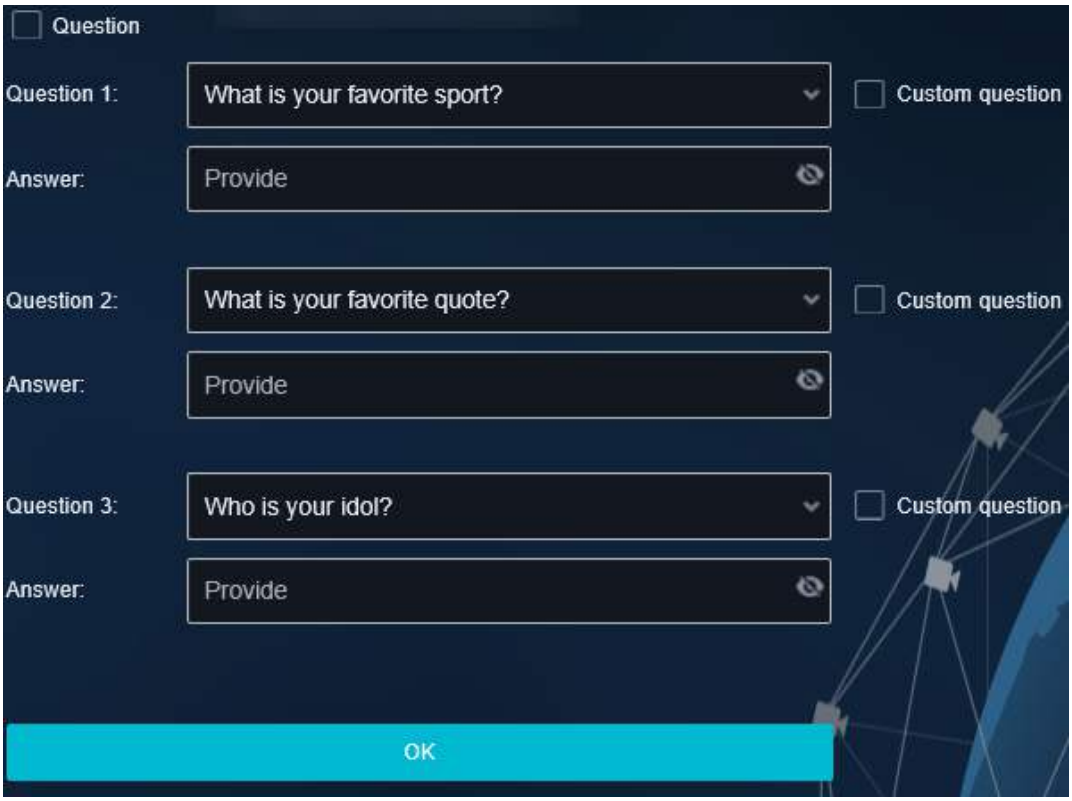
- Setting **Password Validity Period** to **Permanently valid** may cause security risks. Be cautious with this setting.
- When you set the login password, the SDK, web, ONVIF/RTSP, and RESTful passwords are changed synchronously.
- The user password validity period is available only for the login password of the **admin** user.
- By default, if you entered incorrect passwords for five consecutive times, your account will be locked for five minutes. To change the maximum number of consecutive incorrect password attempts and lock duration, see Configuring Account Locking and Unlocking.

- To prevent security risks, periodically log in as the **admin** user, click the drop-down list box in the upper right corner, choose **Change Password**, and change the password.

3. Click **OK**.
4. Refresh the page, enter the user name and password, and click **Log In**. The **Password Recovery** page is displayed.
5. (Optional) Configure password recovery.

   a. Select **Question** and set security questions, as shown in Figure 2.

   Figure 2 Setting security questions



   b. Select a preset question from the **Question *X*** drop-down list box or select **Custom question** and customize a question.

   c. Enter the answer to the question. Set three security questions and their answers in sequence.

   NOTE

- You are advised to set all the three security questions for password reset upon password loss.
- You are advised to set questions and answers that you are familiar with.

d. Click **OK**. The wizard-based configuration page is displayed.

You can perform quick configuration following the wizard. For details, see Wizard-based Configuration Guide.

6. Click **Exit**. The home page is displayed.

7. (Optional) To log out of the camera web system, click  next to the user name in the upper right corner of the web page and choose **Log Out** from the drop-down list box.

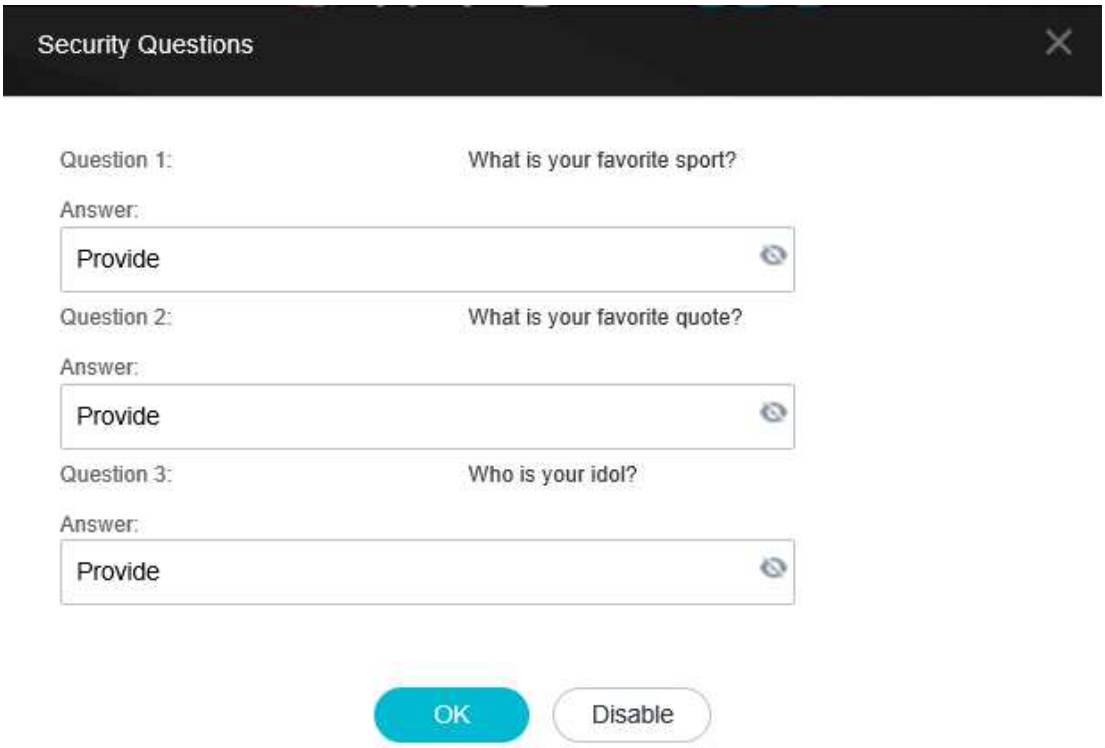
Recovering the Password

Click Security question.

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Forgot Password**. The dialog box for selecting a password recovery method is displayed.
3. Click **Security question** and click **OK**.

   The **Security Questions** dialog box is displayed, as shown in Figure 3.

Figure 3 Security Questions dialog box

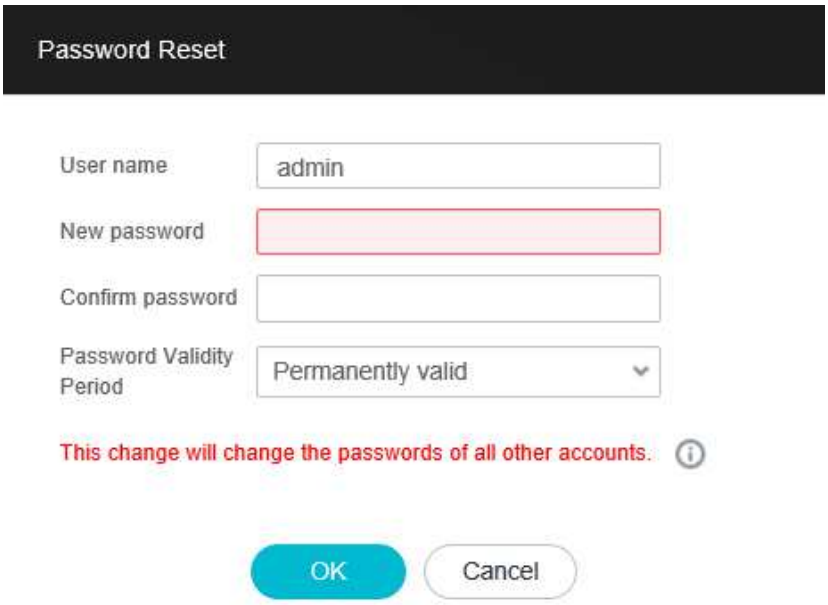


4. Enter the answers to the three security questions in sequence.

   Click **OK**. The dialog box for resetting the password is displayed, as shown in Figure 4.

   The login user name is **admin**. Set the password and **Password Validity Period** and keep the new password secure.

Figure 4 Resetting the password



NOTE

- Setting **Password Validity Period** to **Permanently valid** may cause security risks. Be cautious with this setting.
- When you set the login password, the SDK, web, ONVIF/RTSP, and RESTful passwords are changed synchronously.
- The user password validity period is available only for the login password of the **admin** user.
- By default, if you entered incorrect passwords for five consecutive times, your account will be locked for five minutes. To change the maximum number of consecutive incorrect password attempts and lock duration, see Configuring Account Locking and Unlocking.
- To prevent security risks, periodically log in as the **admin** user, click the drop-down list box in the upper right corner, choose **Change Password**, and change the password.

5. Click **OK**.

Parent topic: Logging In to the Camera Web System

Web Page Layout

You can access cameras through a web browser and manage cameras on the web page, for example, setting camera parameters. The supported functions vary depending on the camera model.

At the first login, you need to download and install the player plug-in. After the installation is complete, you can view live video from the camera after restarting the browser. If the control is blocked by the browser, perform operations as prompted.

NOTE

- If you need to delete the installed plug-in, check the following default paths:
  - *C:\Program Files\sdc_webocx_vware*
  - *C:\Windows\SysWOW64\sdc_webocx_vware*
  - *C:\Windows\SysWOW64\ipc_webocx_vware*
  - *C:\Program Files\Camera_webocx_vware*
- If you select a customized installation path when installing the plug-in, delete the plug-in under the customized path.
- To delete an installed plug-in, delete its installation directory. To delete the directory, close the browser first.
- If the live video image is blurry after you power on and log in to the camera for the first time, you can click the one-push focus icon or lens reset icon to clearly focus the lens. If the image is still blurry, contact technical support.

Figure 1 shows the web page layout.

Figure 1 Web page layout



Table 1 describes the buttons in the lower part of the **View** page.

Table 1 Button description

Button	Description
❑/▶	Stop/Start live video viewing. **NOTE:** • A maximum of three stream encryption channels are supported during live video viewing. If there are more than three channels, a message is displayed, indicating that the number of stream encryption channels has reached the maximum. To continue live video viewing, choose **Configuration** > **Local** > **Playing Settings**, deselect **Media stream encryption**, and refresh the page. • For multi-lens cameras (such as compound-eye cameras and dual-lens PTZ dome cameras), one lens is counted as one channel.
●	Local recording button. You can click this button to enable or disable local recording. The recordings are stored in the ***Path for storing recording files\Camera IP address*** directory. The

Button	Description
	recording is named in ***Camera model*_YYYY-MM-DD-HH-MM-SS_MSMSMS** format, for example, D2120-10-LI-SV_2014-03-28-09-00-06_001. For details about how to configure the path for storing recording files, see Setting Recording File Parameters. The recording button is in steady blue during recording. **NOTE:** You must run the browser as an administrator. The local recording will stop in one of the following scenarios: • Users manually stop the local recording. • The recording times out. • Users manually stop live video viewing. • Users close the browser currently in use. • Users switch to another page.
	Start SD card–based video recording. This is available only on a camera with an SD card. **NOTE:** Format the SD card before using it for the first time. For details, see Configuring Storage Management.
	Capture button. You can click this button to capture images during live video viewing. The captured images are stored under ***Path for storing live snapshots**Camera IP address***. The image is named in **YYYY-MM-DD_HH-MM-SS-MSMS** format, for example, 2014-03-28_09-59-36-98. For details about how to configure the path for storing live snapshots, see Setting Snapshot File Parameters.

Button	Description
	NOTE: You must run the browser as an administrator.
	3D positioning button. Only PTZ-capable cameras support this function. Automatically adjusts the PTZ rotation direction and focal length based on the area selected on the video image. The following describes the detailed procedure: 1. Click  . 2. Draw a box on the video image. The area inside the box is automatically displayed at the center of the video image. • Zooming in: Drag a box from left to right on a video image. • Zooming out: Drag a box from right to left on a video image.
	Quick locating button. Only PTZ-capable cameras support this function. Quickly navigates to a specific location. The following describes the detailed procedure: 1. Click  . 2. Click a location on a video image to display that point at the center of the video image.
	Virtual joystick button. Only PTZ-capable cameras support this function. You can use the mouse to control the camera. The procedure is as follows: 1. Click  . A cross is displayed in the image center. Then click a position on the video image. An arrow is displayed there.

Button	Description
	2. Press and hold the left mouse button to rotate the camera around the arrow. • A shorter distance between the arrow and the cross indicates a slower rotation speed. • You can scroll the mouse wheel to control the zoom. The image is zoomed in when the mouse wheel is scrolled up and zoomed out when the mouse wheel is scrolled down.
	This function is used during automatic tracking and disabled by default. After you click  , the camera detects moving objects that appear in the image. After you manually select an object, the camera automatically generates trajectories of the object.
	This function is used during parking violation detection and disabled by default. After you click  , the button color changes to blue (namely ). After you box-select a vehicle that is suspected of parking violation, the camera captures the vehicle based on the image type set in the **Snapshot Details** dialog box.
	The voice intercom function is disabled by default. After this function is enabled, you can use the microphone connected to your computer to transmit voice to the camera site. To set the volume, drag the slider. **NOTE:** Channel-associated voice and voice intercom cannot be enabled at the same time.
	The channel-associated voice function is disabled by default. After this function is enabled, voice at the camera

Button	Description
	site can be transmitted to the computer connected to the camera. The function is available only when you set **Video stream type** to **Hybrid stream** under **Configuration** > **Local** > **Playing Settings**. To set the volume, drag the slider. **NOTE:** Channel-associated voice and voice intercom cannot be enabled at the same time.
	Switch between the primary and secondary streams. **NOTE:** By default, secondary stream 1 is displayed for 4K cameras. To change the default stream, choose **Configuration** > **Local** > **Playing Settings**, and set **Code stream type** to a specified stream.
	Display the live video stream resolution. The icon changes based on the video resolution. Not all the icons are listed here. Supported camera resolution options are as follows: 4K, 6MP, 5MP, 4MP, 3MP, 1080p, 720p, D1_NTSC, D1_PAL, CIF_NTSC, and CIF_PAL
	View the resolution of an object in the live video. Click  and frame an object in the live video. Then the resolution of the object is displayed in the lower right corner.
	You can click  to crop an area from the live video and zoom in on the area. Then you can click  again or right-click the mouse to disable this function.

Button	Description
	Toggle among **Full Screen**, **Actual Size**, **16:9**, **4:3**, and **1:1**.
	View video in full-screen mode.
	View real-time camera information, including the protocol type, frame rate, resolution, current bit rate, and packet loss rate. **NOTE:** The packet loss rate is valid only when the transmission protocol is set to **UDP**.

NOTE

- When using the function provided by  , if you click any button on the right pane of the live video viewing page or change and save any video settings, this function will stop working and the live video view will return to the original status.
- The function provided by  conflicts with the intelligent analysis areas. To view an intelligent analysis area, disable the function first.
- The buttons vary depending on the camera model.

Parent topic: Configuration

Introduction to the Right Pane on the View Page

By modifying some configuration items on the right pane of the **View** page, you can perform configuration operations related to video viewing, device IP address, system time, image, and video streams. Different camera models may have different parameters.

For cameras of some models, you can click  in the lower part of the live video pane to display the PTZ configuration page.

Setting Camera IP Addresses This section describes how to set camera IP addresses in the camera web system.

Setting Second Protocol Parameters
This section describes how to configure the second protocol on the web page.

Setting the System Time
You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

Setting Common Image Parameters
You can set common image parameters to adjust the image effect.

Setting Common Video Parameters
This section describes how to set common video parameters.

Parent topic: Configuration

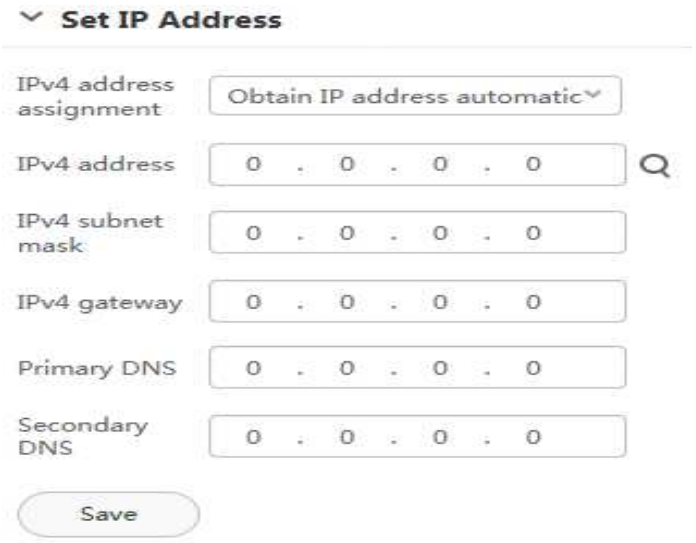
Setting Camera IP Addresses

This section describes how to set camera IP addresses in the camera web system.

Setting Camera IP Addresses in the Camera Web System

1. Log in to the camera web system and choose **View**. On the **View** page that is displayed, click the **Network/Time** tab to access the **Network/Time** tab page, as shown in Figure 1.

   Figure 1 Setting camera IP addresses

2. Set camera IP addresses as planned. Table 1 describes the parameters.

   Table 1 IP address parameters

Parameter	Description
IPv4 address assignment	Method for obtaining the IP address. The options are **Obtain IP address automatically** and **Use the following IP address**. The default value is **Obtain IP address automatically**. **NOTE:**

Parameter	Description
	When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can select **Obtain IP address automatically** to check the IP address. The camera IP address allocated by the server is fixed.
IPv4 address	Camera IP address. This parameter is available only when **IPv4 address assignment** is set to **Use the following IP address**. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223, for example, **192.168.1.161**. **NOTE:** You can click the magnifier icon to check whether the current IP address is available.
IPv4 gateway	Gateway IP address of the network where the camera is located. The default value is **192.168.0.1**.
IPv4 subnet mask	Subnet mask of the network where the camera is located. The default value is **255.255.255.0**.
Primary DNS	Primary DNS IP address. **NOTE:** • Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223.

Parameter	Description
	• Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland); **8.8.8.8** (Google-provided) • If the cloud service is enabled and the domain name of the cloud service is not an IP address, you need to configure DNS when setting the camera IP address. Otherwise, the cloud service is in offline state.
Secondary DNS	Secondary DNS IP address. **NOTE:** • Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. • Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland); **8.8.8.8** (Google-provided)

Parent topic: Introduction to the Right Pane on the View Page

Setting Second Protocol Parameters

This section describes how to configure the second protocol on the web page.

Procedure

When the camera needs to be connected to a third-party platform, the second protocol needs to be enabled and configured. Different camera models support different connection protocols. The procedure is as follows:

1. On the **View** page, choose **Network/Time** > **Second Protocol Parameters**. The **Second Protocol Parameters** area is displayed, as shown in Figure 1.

   Figure 1 Second Protocol Parameters area

2. Set the second protocol as planned. Table 1 describes the parameters. For detailed operations, see Configuring Platform Connection.

   Table 1 Second protocol parameters

Parameter	Description

Parameter	Description
Enable ONVIF	Indicates whether to enable ONVIF connection for the device.
GB/T 28181	The GB/T 28181 protocol is disabled by default and you can enable it. The following parameters are applicable to the GB/T 28181 protocol. If you do not enable this protocol, you do not need to set the following parameters.
Name	Login name used for registering the camera with the platform. The value can contain digits or other characters.
Platform IP	If the camera needs to connect to the IVS1800, enter the IP address of the platform. If the camera needs to connect to the IVS3800, enter the floating gateway IP address of the MPU cluster. If the server and camera are on different networks and NAT is deployed, set this parameter to the post-NAT IP address of the cluster floating gateway.
Port number	GB/T 28181-compliant port on which the video security platform listens. The default value is **5060**. After selecting the **Port number** check box, you can configure the port number range.
Device ID	Unique device ID. Enter a string of 1 to 64 characters. The value can contain letters and digits and must be the same as the connection code configured on the platform. **NOTE:** • This parameter is mandatory. If this parameter is not set, service alarms cannot be reported to the platform.

Parameter	Description
Server code	GB/T 28181 server code. Enter a string of 1 to 64 characters. The value can contain letters and digits.
SIP server domain	Domain name that consists of 1–127 digits.
Password	Password for registering the camera with the platform. **NOTE:** • The value of this parameter must be the same as the registration password configured on the platform. If they are different, the camera will fail to connect to the video platform. • For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following characters: digits, letters, and special characters.

Parent topic: Introduction to the Right Pane on the View Page

Setting the System Time

You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

NOTICE

If you change the system time when the camera is recording video, the recording file will be corrupted. Therefore, do not change the system time during video recording.

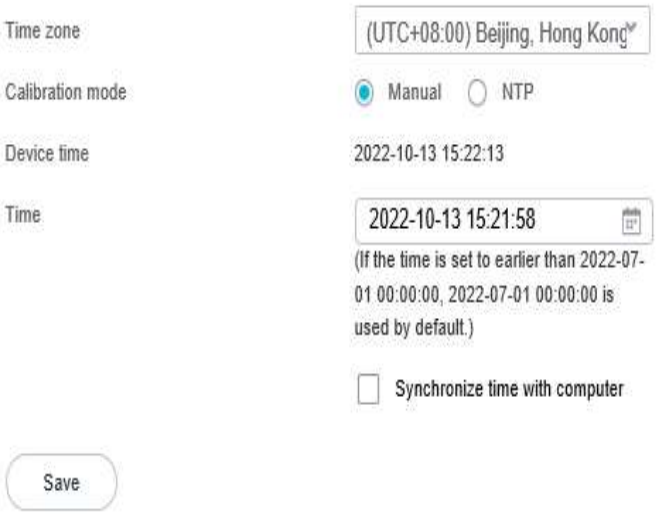
Setting the System Time

1. On the **View** page, click the **Network/Time** tab to access the **Network/Time** tab page.

   For some camera models, the corresponding area is titled **IP/Time**.

2. **Optional:** Click **Time** and set the system time,

   Figure 1 Time tab page



   a. Select a time zone from the **Time zone** drop-down list box.

b. Select a time calibration mode and set related parameters. For details, see Table 1.

NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- To enable NTP time calibration, first ensure that **Time zone** is correctly set in manual time calibration mode.
- The following time calibration modes are available: manual and NTP. In manual mode, you can directly set the time. In NTP mode, you need to configure the NTP server to time-synchronize the camera with the NTP server.

Table 1 Time calibration modes

Parameter	How to Set
Manual	1. Click **Manual**. 2. Click the **Time** text box. The dialog box for setting the date and time is displayed. 3. Set the date and time and click **OK**. The system returns to the time setting page. **NOTE:** To time-synchronize the camera with the computer, click **Synchronize time with computer**.
NTP	1. Click **NTP**. 2. Set the NTP server IP address or domain name as prompted. Set the

Parameter	How to Set
	interval for time-synchronizing the camera with the NTP server. The camera synchronizes time with the NTP server at a specified interval.

3. Click **Save**.

Configuring Daylight Saving Time

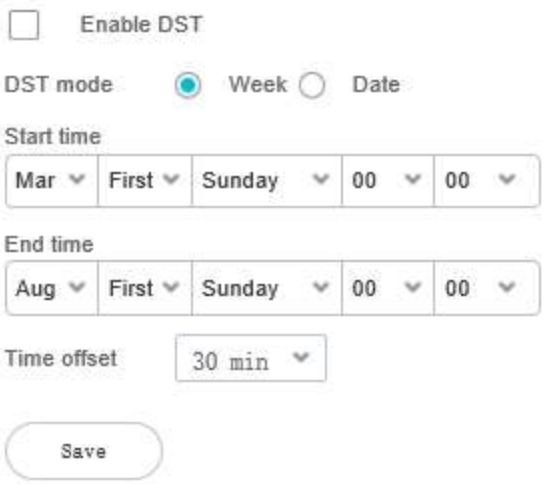
If the region where the camera is located has daylight saving time (DST), you need to configure the DST.

1. On the **View** page, click the **Network/Time** tab to access the **Network/Time** tab page.

   For some camera models, the corresponding area is titled **IP/Time**.

2. Click **Time**. In the area that is displayed, set DST parameters, as shown in Figure 2.

   Figure 2 Configuring the DST



3. Configure the DST.

   a. Select **Enable DST**.

b. Select **Week** or **Date** as required. If neither option is selected, the DST settings cannot be saved.

   The **Week** mode indicates that the DST is set by week. The **Date** mode indicates that the DST is set by date.

c. Set **Start time**, **End time**, and **Time offset** of the DST based on regulations specified in the local laws.

   Table 2 describes the DST parameters.

   Table 2 Parameter description

Parameter	Description
Week	Indicates that the DST is set by week.
Date	Indicates that the DST is set by date.
Start time	Time for enabling the DST.
End time	Time for disabling the DST.
Time offset	Lead time during the DST, in minutes. If this parameter is set to **30 min**, the DST is 30 minutes earlier.

   NOTE

   If the local laws regulate that DST must be used, you must set DST based on the regulations specified in the local laws.

4. Click **Save**.

Parent topic: Introduction to the Right Pane on the View Page

Setting Common Image Parameters

You can set common image parameters to adjust the image effect.

1. On the **View** tab page, click the **General** tab to access the **General** tab page.
2. Click **Image**. The **Image** area is displayed, as shown in Figure 1.



Figure 1 Image area

3. Set common image parameters. Table 1 describes the parameters. For details about the image parameter settings, see Setting Image Parameters.

Table 1 Common image parameters

Parameter	Description
Brightness	Attribute of visual perception in which a source appears to be radiating or reflecting light.
Saturation	Colorfulness of a color relative to its own brightness.
Contrast	Ratio of the luminance of the brightest color (white) to that of the darkest color (black) in

Parameter	Description
	the image. • A larger contrast value indicates a clearer and brighter image. • A small contrast value indicates a dusky image.
Sharpness	Related to the edge contrast of an image and image clarity.
Restore Defaults	Used to restore the image parameters to default values. The default values are those in the screenshot.

Parent topic: Introduction to the Right Pane on the View Page

Setting Common Video Parameters

This section describes how to set common video parameters.

Procedure

1. On the **View** page, click the **General** tab to access the **General** tab page.
2. Click **Video**.

   The **Video** area is displayed, as shown in Figure 1. The parameters displayed on the web page vary depending on the camera model.



Figure 1 Video area

3. Set video parameters. Table 1 describes the parameters.

Table 1 Video parameters

Parameter	Description
Primary stream/Secondary stream	Set the stream combination type based on the site requirements.

Parameter	Description
	• **Primary stream**: The primary streams feature high bit rate, definition, and bandwidth usage. They are applicable to local storage. • **Secondary stream**: The secondary streams provide smooth video, occupies small bandwidth, and are applicable to data transmission over low-bandwidth networks. **NOTE:** SD card recording supports only primary streams.
Intelligent encoding	After intelligent encoding is enabled, a camera can automatically adapt to scenarios to reduce the bit rate and save the storage space. A higher intelligent encoding level indicates more significant reduction of the bit rate, which however may lead to image quality deterioration. **NOTE:** After intelligent encoding is enabled, the settings of the ROI and stream smoothing parameters do not take effect.
Slice	The parameter is available only when you set **Encoding protocol** to **H.264**. Multi-slice encoding indicates that video streams are divided into multiple segments. Each segment forms a slice. The encoding process of each slice is independent of

Parameter	Description
	each other. Therefore, the camera can encode and decode multiple slices in parallel, improving encoding and decoding performance. This parameter is selected by default.
Encoding protocol	Set the video encoding protocol based on the site requirements. The options are as follows: • **H.264**: The H.264 protocol requires relatively small bandwidth to ensure video quality. • **MJPEG**: The MJPEG protocol decodes and displays each frame independently without referring to the previous and next frames. This protocol has a small compression ratio and requires large bandwidth to ensure video quality. This protocol is suitable for video editing. • **H.265**: The H.265 protocol is bandwidth-conserving compared with the H.264 protocol. **NOTE:** • Before connecting a camera to the upper-level security platform, ensure that the encoding protocol of the camera is the same as that on the platform to prevent issues (such as live video viewing or video recording failures) on the platform. The encoding protocol of the camera must be a protocol supported by the platform. • Local recordings and SD card-based recordings support the H.264 and

Parameter	Description
	H.265 protocols.
Encoding complexity	The parameter is available only when you set **Encoding protocol** to **H.264**. The options of H.264 profiles include **Base profile**, **Main profile**, and **High profile**. Among these profiles, the baseline profile has the lowest encoding compression performance and lowest requirements on hardware decoding performance, while the high profile has the highest. For the H.265 encoding protocol, the available profile is **Main profile**. When the coding protocol is changed from MJPEG or H.265 to H.264, **High profile** is used by default.
Resolution	A higher resolution indicates clearer images and higher bandwidth consumption.
Bit rate type	The parameter is available only when you set **Encoding protocol** to **H.264** or **H.265**. The bit rate is measured by data bits transmitted in a unit of time. • **Variable bit rate**: The bit rate varies depending on the image complexity to ensure the clarity of images with great dynamic changes. The bit rate is low if the image is simple or static. The variable bit rate is recommended. • **Constant bit rate**: The constant bit rate remains the same. The upper limit of the instantaneous bit rate is set to 110%. If the bit rate is incorrectly configured for images with great

Parameter	Description
	dynamic changes, the images will be unclear.
Max. bit rate (kbit/s)	The parameter is available only when you set **Bit rate type** to **Variable bit rate**. The bit rate range depends on the selected resolution.
Bit rate value	Average bit rate when **Bit rate type** is set to **Constant bit rate**. The bit rate range depends on the selected resolution.
Bit rate control mode	The parameter is available only when you set **Bit rate type** to **Constant bit rate**. The options are as follows: • **Frame rate priority**: Ensure the smoothness of the video image. • **Image quality priority**: Ensure video image quality.
Frame rate	The frame rate is measured by the number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.
Image quality	The parameter is available only when you set **Encoding protocol** to **H.264** or **H.265** and **Bit rate type** to **Variable bit rate**. Better image quality requires higher bandwidth. Therefore, select proper image quality based on the site requirements.
I-frame interval	The parameter is available only when you set **Encoding protocol** to **H.264** or **H.265**.

Parameter	Description
	An I-frame is an intra-coded frame that represents a fixed image independent of other picture types. Each group of pictures (GOP) begins with this type of frame. A smaller I-frame interval indicates better video quality and higher bandwidth consumption. **NOTE:** It is recommended that the I-frame interval be set to twice the frame rate.
Layered encoding	The parameter is available only when you set **Encoding protocol** to **H.264** or **H.265**. To enable layered encoding, select **Layered encoding**.
Absolute timestamp	The absolute timestamp refers to the number of milliseconds that have elapsed since the Unix epoch, minus leap seconds. The Unix epoch is 00:00:00 UTC on January 1, 1970. To enable this function, select the check box. The check box is deselected by default. After this function is enabled, the RTP extension header of video streams carries an absolute timestamp. You can obtain video streams with absolute timestamps in multiple ways (for example, RTSP) for real-time vehicle positioning and trajectory generation. **NOTE:** • The absolute timestamp function is mutually exclusive with the layered

Parameter	Description
	encoding and digital watermark functions. • For details about how to obtain streams through RTSP, see Obtaining Streams Through RTSP.
JPEG quality	The parameter is available only when you set **Encoding protocol** to **MJPEG**. A larger value indicates higher image quality.
Stream smoothing coefficient	You can enable stream smoothing and set the stream smoothing coefficient. The default value is **50**. You can set it based on the site requirements. A larger value indicates a smaller I-frame and lower image clarity.

4. Click **Save**.

Parent topic: Introduction to the Right Pane on the View Page

Wizard-based Configuration Guide

If a camera is used for the first time or has been restored to factory defaults, when you log in to the camera web system, the wizard-based configuration page is displayed. On this page, you can quickly configure some services of the camera. You can also go to the wizard-based configuration page even if it is not your first login.

Setting Camera IP Addresses This section describes how to set camera IP addresses in the camera web system.

Configuring Time
You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

Configuring Video

Setting Image Parameters
By setting image parameters, you can adjust video images to adapt to different scenarios.

Configuring OSD
You can set on screen display (OSD) parameters to specify the information to be displayed and the display effect.

Configuring Intelligent Analysis Functions
This section describes the features supported in each intelligent mode.

Diagnosing Image Quality

Configuring Network Platform Connection
This section describes how to set network platform connection parameters. Different parameters need to be set for different protocols. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera.

Parent topic: Configuration

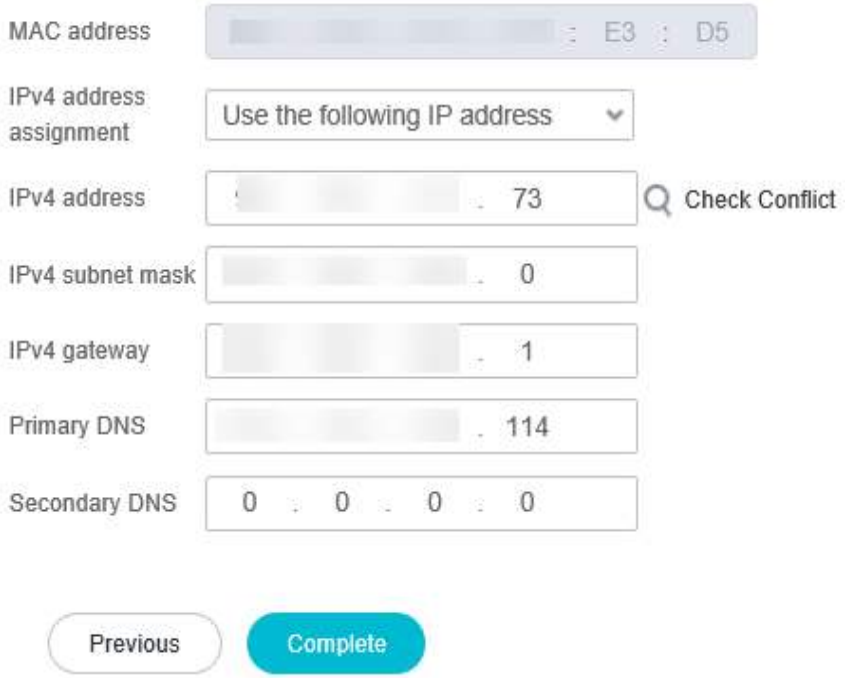
Setting Camera IP Addresses

This section describes how to set camera IP addresses in the camera web system.

Setting the IPv4 Address

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. The **IP** page is displayed by default, as shown in Figure 1.

   Figure 1 Setting the IPv4 address

3. Set camera IP addresses as planned. Table 1 describes the parameters.

   Table 1 IP address parameters

Parameter	Description
MAC address	Camera MAC address. This parameter is read-only.

Parameter	Description
IPv4 address assignment	Method for obtaining the IPv4 address. The options are **Obtain IP address automatically** and **Use the following IP address**. The default value is **Obtain IP address automatically**. **NOTE:** When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can select **Obtain IP address automatically** to check the IP address. The camera IP address allocated by the server is fixed.
IPv4 address	Camera IPv4 address. This parameter is available only when **IPv4 address assignment** is set to **Use the following IP address**. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. **NOTE:** • You can click the magnifier icon to check whether the current IP address is available.
IPv4 gateway	Gateway IP address of the network where the camera is located. The default value is **192.168.0.1**.
IPv4 subnet mask	Subnet mask of the network where the camera is located. The default value is **255.255.255.0**.
Primary DNS	Primary DNS IP address. **NOTE:**

Parameter	Description
	• Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. • Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland) and **8.8.8.8** (Google-provided) • If the cloud service is enabled and the domain name of the cloud service is not an IP address, you need to configure DNS when setting the camera IP address. Otherwise, the cloud service is in offline state.
Secondary DNS	Secondary DNS IP address. **NOTE:** • Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. • Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland) and **8.8.8.8** (Google-provided)

4. Click **Save**.

Setting the IPv6 Address

The IPv6 address is numbered in hexadecimal notation and is divided into eight blocks by colons (:). Each block contains 16 bits,

for example, fe80:0da8:65b4:05d3:1315:7c1f:0461:7847.

The following assumes that the local computer is directly connected to the camera. To set the IPv6 address, first change the local computer IP address to be on the same network segment as the camera IP address.

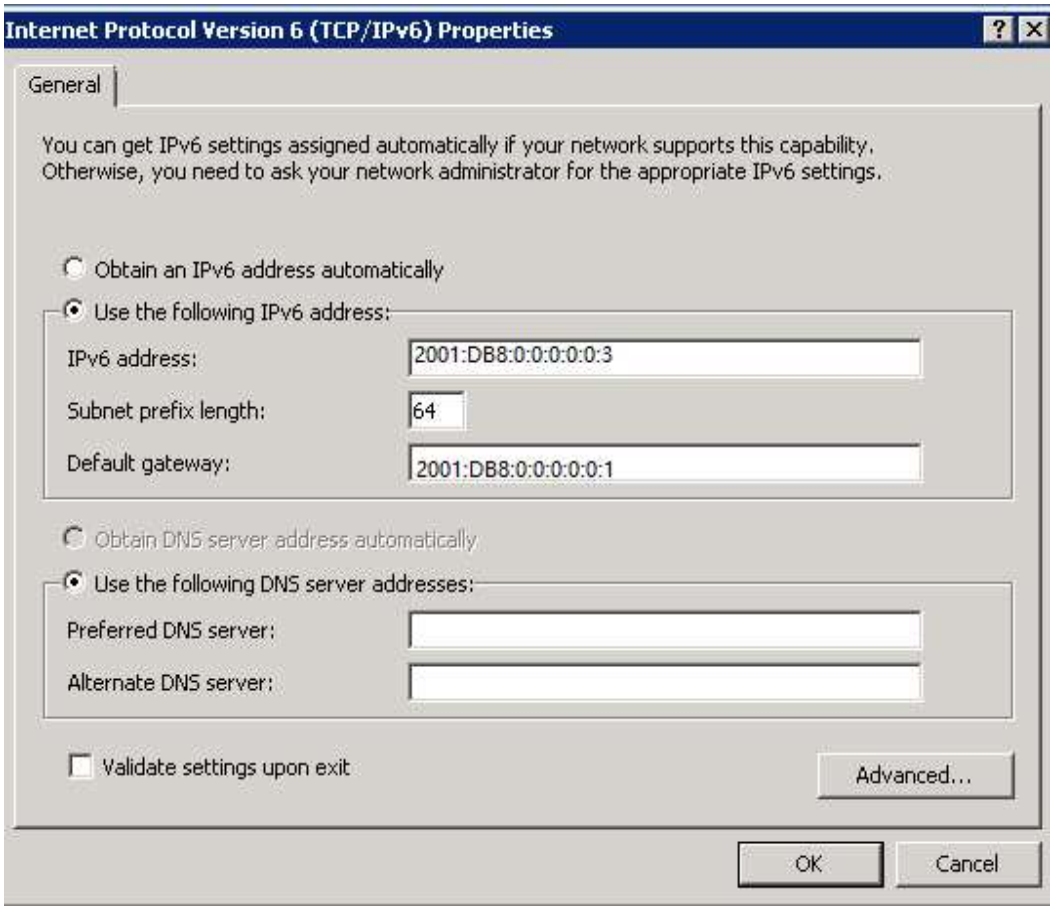
1. Set the IPv6 address of the local computer.

    a. Run the **regedit** command on the local computer, choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **services** > **TCPIP6** > **Parameters**, delete **DisabledComponents**, and restart the local computer.

    b. On the computer, choose **Control Panel** > **Network and Internet** > **Network and Sharing Center** to access the **Network and Sharing Center** page.

    c. Click **Local Area Connection**. In the dialog box that is displayed, click **Properties**. In the dialog box that is displayed, double-click **Internet Protocol Version (TCP/IPv6) Properties**. The dialog box shown in Figure 2 is displayed. Change the computer IP address, subnet mask, and default gateway IP address to ensure that the computer IP address is on the same network segment as the camera IP address. For example, set the IPv6 address to **2001:DB8:0:0:0:0:0:3**.

Figure 2 Setting the IPv6 address



2. Set the IPv6 address of the camera. Click **Configuration Wizard** in the upper right corner of the web page. On the **IP** page that is displayed, select Enable **IPv6**, as shown in Figure 3.

Figure 3 Setting the IPv6 address

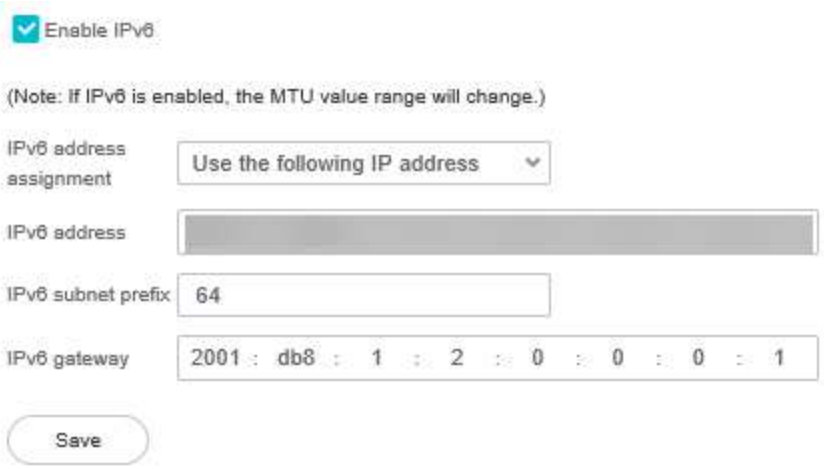


Table 2 IP address parameters

Parameter	Description
IPv6 address assignment	Method for obtaining the IPv6 address. The options are **Obtain IP address automatically**, **Use the following IP address**, and **Route advertisement**. **NOTE:** If the MTU value is less than 1280, the MTU value will change to **1500** after the IPv6 address is enabled. If the MTU value is greater than 1280, the MTU value remains unchanged after the IPv6 address is enabled.
IPv6 address	Camera IPv6 address.
IPv6 subnet prefix	IPv6 subnet prefix of the camera. Set the parameter to **64**.
IPv6 gateway	IPv6 gateway address of the camera. Set the parameter to **2001:DB8:0:0:0:0:0:1**.

3. Click **Save**.

Parent topic: Wizard-based Configuration Guide

Configuring Time

You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

NOTICE

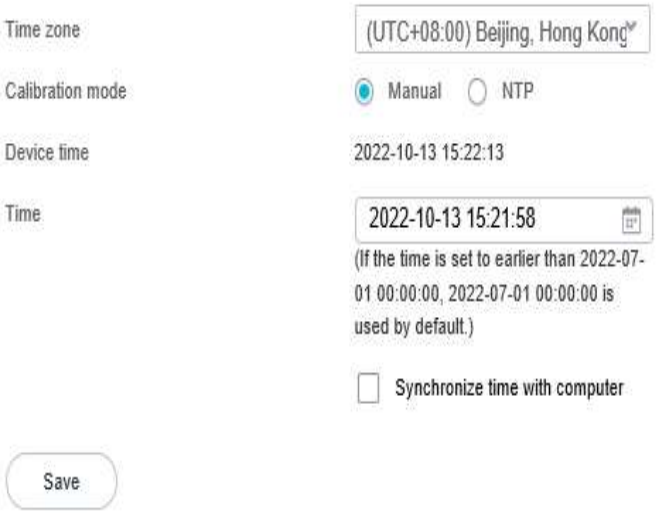
If you change the system time when the camera is recording video, the recording file will be corrupted. Therefore, do not change the system time during video recording.

For models that support 1 + N, after the system time and DST of the primary camera are changed, the setting is automatically synchronized to the secondary cameras. After the system time and DST of a secondary camera are changed, the setting is not synchronized to the primary camera.

Configuring System Time

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Time** page is displayed, as shown in Figure 1. The web page varies between camera models.

Figure 1 Time tab page



a. Select a time zone from the **Time zone** drop-down list box.

b. Select a time calibration mode and set other related parameters. Table 1 describes the parameters.

NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- To enable NTP time calibration, first ensure that **Time zone** is correctly set in manual time calibration mode.
- The following time calibration modes are available: manual and NTP. In manual mode, you can directly set the time. In NTP mode, you need to configure the NTP server to time-synchronize the camera with the NTP server.

Table 1 Time calibration modes

Parameter	Setting
Manual	1. Click **Manual**.

Parameter	Setting
	2. Click the **Time** text box. The dialog box for setting the date and time is displayed. 3. Set the date and time and click **OK**. The system returns to the time setting page. **NOTE:** To time-synchronize the camera with the computer, click **Synchronize time with computer**.
NTP	1. Click **NTP**. 2. Set the NTP server IP address or domain name as prompted. Set the interval for time-synchronizing the camera with the NTP server. Then the camera synchronizes time with the NTP server at the specified interval. **NOTE:** • You can click Check to check whether the NTP server IP address is available.

3. Click **Save**.

Configuring DST

If the region where the camera is located has daylight saving time (DST), you need to configure the DST.

1. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Time** page where you can configure DST is displayed, as shown in Figure 2. The web page varies between camera models.

   Figure 2 Configuring the DST

2. Configure the DST.

   a. Select **Enable DST**.

   b. Select **Week** or **Date** as required. If neither option is selected, the DST settings cannot be saved.

      The **Week** mode indicates that the DST is set by week. The **Date** mode indicates that the DST is set by date.

   c. Set **Start time**, **End time**, and **Time offset** of the DST based on regulations specified in the local laws.

      Table 2 describes the DST parameters.

      Table 2 Parameter description

Parameter	Description
Week	Indicates that the DST is set by week.
Date	Indicates that the DST is set by date.
Start time	Time for enabling the DST.
End time	Time for disabling the DST.

Parameter	Description
Time offset	Lead time during the DST, in minutes. If this parameter is set to **30 min**, the DST is 30 minutes earlier.

NOTE

If the local laws regulate that DST must be used, you must set DST based on the regulations specified in the local laws.

3. Click **Save**.

Parent topic: Wizard-based Configuration Guide

Configuring Video

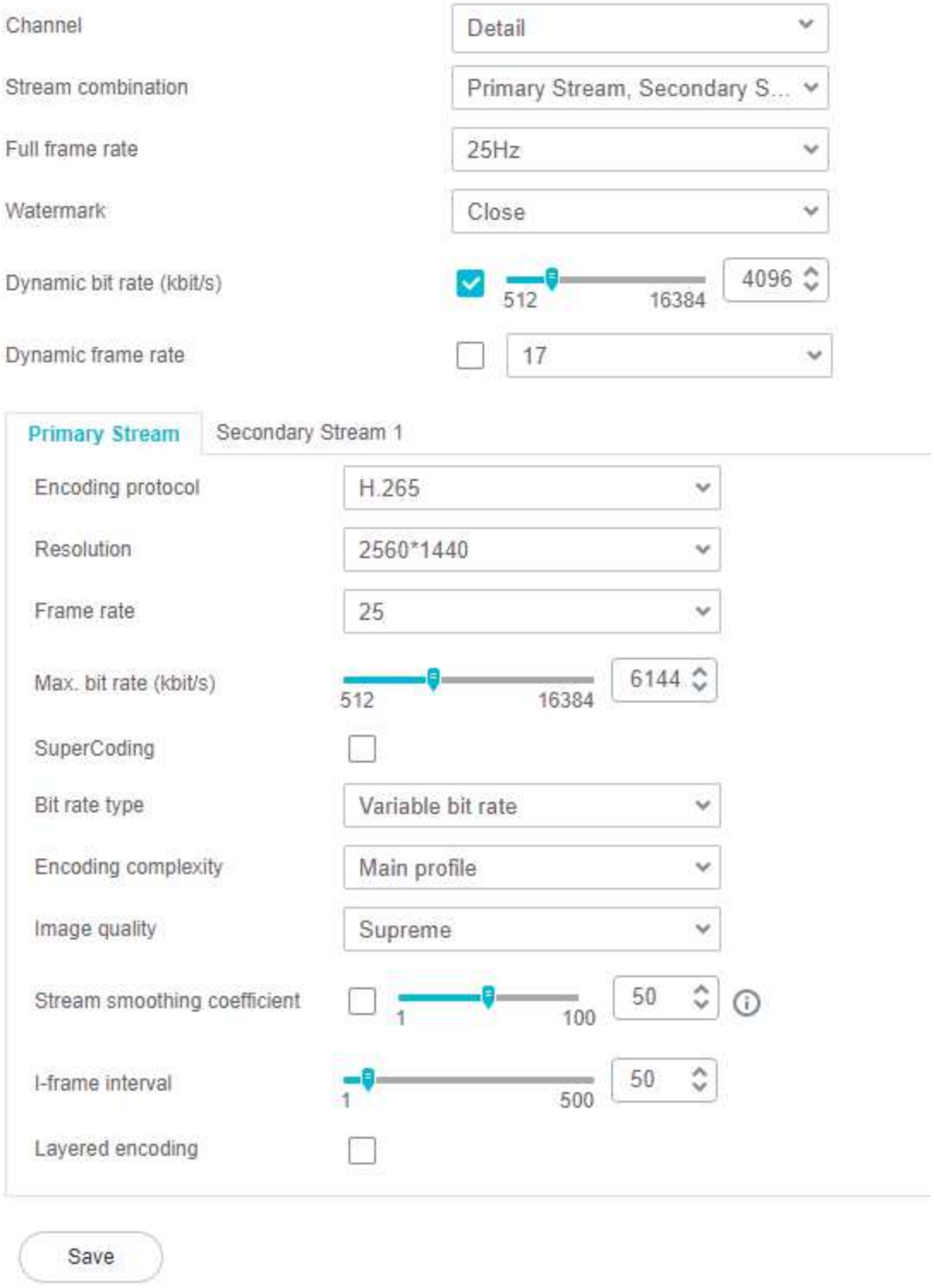
You can set video parameters, such as the stream combination type, encoding protocol, and resolution, based on the site requirements.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Video** page is displayed, as shown in Figure 1.

   The parameters displayed on the web page vary depending on the camera model.

Figure 1 Setting video parameters



3. Set video parameters. Table 1 describes the parameters.

The following table describes all parameters. The parameters displayed on the web page vary depending on the camera model.

Table 1 Video parameters

Parameter	Description
Channel	Channel type of a device.
Stream combination	Stream combination type. • **Primary Stream**: The primary streams feature high bit rate, definition, and bandwidth usage. They are applicable to local storage. • **Secondary Stream**: The secondary streams provide smooth video and occupy small bandwidth. They are applicable to data transmission over low-bandwidth networks. **NOTE:** Onboard recording (stored on onboard SD cards) supports only primary streams. You cannot set the stream type to triple streams or higher for some C series and D series cameras. That is, only **Primary Stream** or **Primary Stream, Secondary Stream 1** can be set for such cameras. The multi-stream (triple streams or higher) function is mutually exclusive with the perimeter detection function. After target detection or perimeter detection is enabled, the maximum resolution of the secondary stream can be set to D1.
Full frame rate	Frame rate collected through the sensor, representing the maximum capability of a camera.

Parameter	Description
	NOTE: On the camera web page, you need to set the frame rate based on the site requirements and bandwidth conditions. A higher frame rate indicates clearer and more vivid images. The maximum frame rate cannot exceed the full frame rate.
Watermark	Indicates whether to enable the watermark function. You can enable this function for information security purposes such as anti-counterfeit and copyright protection. • **Close**: Disable the watermark function. • **HiSilicon digital watermark**: Enable the HiSilicon watermark function. • **SHA256 digital watermark**: Enable the SHA256-based watermark function.
Dynamic bit rate	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. If this checkbox is selected, the camera will automatically use the dynamic bit rate to deliver clearer live (primary stream) or recorded video when the camera generates an alarm (excluding the temperature alarm). After the alarm is cleared, the bit rate is restored to that in stream settings. **NOTE:** • It is recommended that the dynamic bit rate be greater than that in stream settings. • The dynamic bit rate is valid only for primary streams.

Parameter	Description
Dynamic frame rate	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. If this checkbox is selected, the camera automatically uses the dynamic frame rate when the camera triggers an alarm (excluding the temperature alarm). After the alarm is cleared, the frame rate is restored to that in stream settings. **NOTE:** • It is recommended that the dynamic frame rate be greater than that in stream settings. • The dynamic frame rate is valid only for primary streams.
SuperCoding	Indicates whether to enable SuperCoding. This function is enabled by default. After SuperCoding is enabled, the camera can compress the background while ensuring the image quality of ROIs. This helps save storage space and transmission bandwidth. If **Max. bit rate (kbit/s)** at each video resolution is set to a too low value, mosaics may occur on live video. You are advised to set this parameter by referring to Table 2. **NOTE:** • After SuperCoding is enabled, the **Encoding complexity**, **Bit rate type**, **Image quality**, **I-frame interval**, **Stream smoothing coefficient**, and **Layered encoding** parameters are unavailable. • The SuperCoding function is available only for some camera models. Before enabling

Parameter	Description
	SuperCoding for light intelligence cameras, ensure that the corridor mode is disabled.
Intelligent encoding	Indicates whether to enable intelligent encoding. If it is enabled, the camera can automatically adapt to scenarios to reduce the bit rate and save the storage space. A higher intelligent encoding level indicates more significant reduction of the bit rate, which may lead to image quality deterioration. **NOTE:** • After intelligent encoding is enabled, the **Encoding complexity**, **Bit rate type**, **Image quality**, **I-frame interval**, and **Layered encoding** parameters cannot be set. • After intelligent encoding is enabled, the I-frame interval is automatically controlled. If a recording is segmented within the I-frame interval, a recording segment will be missing. The duration of the missing recording segment is less than the I-frame interval.
Slice	Multi-slice encoding indicates that video streams are divided into multiple segments. Each segment forms a slice. The encoding process of each slice is independent of each other. Therefore, the camera can encode and decode multiple slices in parallel, improving encoding and decoding performance. This check box is selected by default.
Encoding protocol	Video encoding protocol. • **MJPEG**: The MJPEG protocol decodes and displays each frame independently without

Parameter	Description
	referring to the previous and next frames. This protocol has a small compression ratio and requires large bandwidth to ensure video quality. This protocol is suitable for video editing. • **H.265**: The H.265 protocol is bandwidth-conserving. **NOTE:** • Before connecting a camera to the video security platform, ensure that the encoding protocol of the camera is the same as that on the platform to prevent issues (such as live video viewing or video recording failures) on the platform. The encoding protocol of the camera must be a protocol supported by the platform. • Local recordings and onboard recordings (using SD cards) support related protocols such as H.265.
Encoding complexity	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. For the H.265 encoding protocol, the available profile is **Main profile**.
Resolution	Video resolution. A higher resolution indicates clearer images and higher bandwidth consumption. If the **Resolution** parameter of a 4K camera is dimmed (not configurable), check whether the area cropping function is enabled. If the function is enabled, disable the function and then set the resolution. **NOTE:**

Parameter	Description
	To obtain the resolution of 1080p secondary streams, you need to set the resolution of the primary stream to 1080p or lower. Then, you can set the resolution on the **Secondary Stream 1** tab page.
Bit rate type	Type of the bit rate. The parameter is available only when you set **Encoding protocol** to H.265 or other related formats. The bit rate is measured by data bits transmitted in a unit of time. • **Variable bit rate**: The bit rate varies depending on the image complexity to ensure the clarity of images with great dynamic changes. The bit rate is low if the image is simple or static. The variable bit rate is recommended. • **Constant bit rate**: The constant bit rate remains the same. The upper limit of the instantaneous bit rate is set to 110%. If the bit rate is incorrectly configured for images with great dynamic changes, the images will be unclear.
Bit rate value	Bit rate. The parameter is available only when you set **Bit rate type** to **Constant bit rate**. A larger bit rate indicates better video quality and higher bandwidth consumption. • You must set a proper bit rate value to ensure the video quality. • The actual bandwidth requirement needs to be higher than the bit rate to ensure smooth video. If the bit rate is low, the required bandwidth is generally 1.2 times the bit rate.

Parameter	Description
	• If the total bit rate of enabled live video streams (including metadata streams) exceeds 40 Mbit/s, you are advised to reduce the bit rate or the number of enabled video streams to prevent video stuttering or artifacts caused by large bit streams.
Bit rate control mode	Bit rate control mode. The parameter is available only when you set **Bit rate type** to **Constant bit rate**. • **Frame rate priority**: The frame rate stability is preferentially ensured. However, the actual bit rate may be greater than the configured bit rate in complicated scenarios or scenarios where objects move quickly. • **Image quality priority**: The image quality is preferentially ensured. However, frames may be lost or live video is not smooth in complicated scenarios or scenarios where objects move quickly. **NOTE:** If SuperCoding is enabled, the options of **Bit rate control mode** are **Balanced**, **Image quality priority**, and **Bit rate compression priority**.
Max. bit rate (kbit/s)	Upper limit of the bit rate. The parameter is available only when you set **Bit rate type** to **Variable bit rate**. The bit rate range is associated with the resolution. **NOTE:**

Parameter	Description
	• Whether to enable SuperCoding affects the bit rate range. • After SuperCoding is enabled, the connected platform can still deliver bit rates that are not supported by SuperCoding. The bit rate set on the platform does not take effect.
Frame rate	Frame rate measured by the number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.
Image quality	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats and **Bit rate type** is set to **Variable bit rate**. **NOTE:** Better image quality indicates that more network bandwidth is consumed. Configure a proper image quality value based on the site requirements.
I-frame interval	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. An I-frame is an intra-coded frame that represents a fixed image independent of other picture types. Each group of pictures (GOP) begins with this type of frame. A smaller I-frame interval indicates better video quality and higher bandwidth consumption. **NOTE:**

Parameter	Description
	It is recommended that the I-frame interval be set to twice the frame rate.
Layered encoding	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. To enable the layered encoding function, select the check box. By default, the check box is deselected. Enabling this function will enhance the fault tolerance and packet loss concealment capabilities but will also increase the bit rate and encoding complexity. In addition, a specific decoder is required. You can choose whether to enable this function based on the site requirements.
JPEG quality	The parameter is available only when you set **Encoding protocol** to **MJPEG**. A larger JPEG quality value indicates better video quality and higher bandwidth consumption.
Enable area cropping	Indicates whether to enable area cropping. After this function is enabled, you can select an area on the video image for encoding and set it as a secondary stream. You can set related parameters on the tab page corresponding to each secondary stream when **Stream combination** is set to one of the following values: **Primary Stream, Secondary Stream 1** and **Primary Stream, Secondary Stream 1, Secondary Stream 2**. **NOTE:** • On the **Secondary Stream 1** tab page, you can set **Resolution** to **1920*1080**,

Parameter	Description
	1280*720, **720*576**, or **720*480**. • On the **Secondary Stream 2** tab page, you can set **Resolution** to **720*576**, **720*480**, **352*288**, or **352*240**. • For **Secondary Stream 2**, the size of the cropped area cannot be set. 1. Select **Enable area cropping**. 2. Drag the mouse pointer to adjust the area to crop. 3. After the setting is successful, switch to the secondary stream for which the region cropping function is set on the video preview page. Only the cropped region is displayed. 4. Click  to enable ePTZ. **NOTE:** The electronic PTZ (ePTZ) adjusts the focal length or shooting angle through software, instead of by using lens zooming or PTZ rotation. • For some models, if the electronic image stabilization function is enabled, the area cropping function cannot be enabled. Enable the function based on the site requirements. • The ePTZ function can be used only after the area cropping function is enabled and live video is switched to the required secondary stream type. Only **Secondary Stream 1** supports the ePTZ function. • A shorter distance between the arrow and the cross indicates a slower rotation speed.

Parameter	Description
	• You can scroll the mouse wheel to control the zoom. The image is zoomed in when the mouse wheel is scrolled up and zoomed out when the mouse wheel is scrolled down.
Absolute timestamp	Indicates whether to enable the absolute timestamp. The absolute timestamp refers to the number of milliseconds that have elapsed since the Unix epoch, minus leap seconds. The Unix epoch is 00:00:00 UTC on 1 January 1970. This function is disabled by default. After this function is enabled, the RTP extension header of video streams carries an absolute timestamp. You can obtain video streams with absolute timestamps in multiple ways (for example, RTSP) for real-time vehicle positioning and trajectory generation. **NOTE:** • The absolute timestamp function is mutually exclusive with the layered encoding and digital watermark functions. • For details about how to obtain streams through RTSP, see Obtaining Streams Through RTSP.
Stream smoothing coefficient	Indicates whether to enable stream smoothing. After this function is enabled, you can drag the slider to set the stream smoothing coefficient. The default value is **50**. A larger value indicates a smaller I-frame and lower image clarity.

Table 2 Recommended maximum bit rate at each video resolution

Setting Image Parameters

By setting image parameters, you can adjust video images to adapt to different scenarios.

NOTICE

- The default values of image parameters vary depending on the algorithm mode.
- Image parameters are associated with each other. Set the image parameters strictly based on the site requirements to prevent poor image quality or overexposure.
- Image parameters vary depending on camera models.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Image** page is displayed. The web page varies between camera models.
3. Set related parameters based on the site requirements. The following describes the parameters.

Image Adjustment

Figure 1 Setting image adjustment parameters

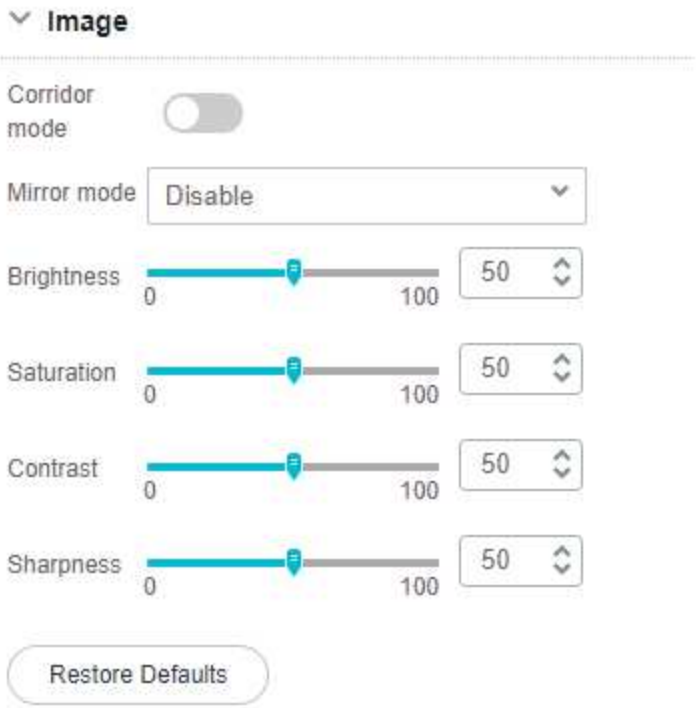


Table 1 Image adjustment parameters

Parameter	Description
Corridor mode	Indicates whether to enable the corridor mode. If it is enabled, you can flip video images by 90 degrees to set the video aspect ratio to 9:16 or 3:4. **NOTE:** • To enable the corridor mode, you are advised to rotate the box camera or bullet camera for 90 degrees to implement side installation. For fixed dome cameras, the housing must be opened and the lens be rotated for 90 degrees. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in

Parameter	Description
	occasional video stuttering. You need to set related parameters based on the site requirements. • Before enabling the corridor mode, ensure that the parking detection function is disabled.
Mirror mode	Mirroring mode, which allows you to flip video images left to right or top to bottom. • **Disable**: Disable the mirroring mode. • **Horizontal mirroring**: Flip video images left to right. • **Vertical mirroring**: Flip video images top to bottom. • **All**: Flip video images left to right and top to bottom.
Brightness	Brightness of images captured by a camera.
Saturation	Colorfulness of a color relative to its own brightness.
Contrast	Ratio of the luminance of the brightest color (white) to that of the darkest color (black) in the image. • Increasing the contrast improves the image clarity and color brightness. • Decreasing the contrast dims the entire image.
Sharpness	Quality related to the edge contrast of an image and image clarity.

Day/Night Switch

Figure 2 Day/Night switch parameters



Table 2 Day/Night switch parameters

Parameter	Description
Mode	Day/night mode, which is to help fine-tune the camera's photosensitivity when light conditions change. The options vary depending on the camera model. The options are as follows: • **Auto**: The camera automatically switches between the color mode and the B/W mode based on ambient light conditions. **NOTE:** For some camera models, if **Mode** is set to **Auto**, infrared light compensation is automatically enabled based on ambient nighttime illumination to improve the image effect. In this case, B/W images are generated. • **Color**: The camera captures color images. • **B/W**: The camera captures black and white images. • **Scheduled**: You can customize **Nighttime start from** and **Daytime start from**. This mode is applicable to scenarios that require a specified day/night switch time or a unified day/night switch time for multiple cameras.

Parameter	Description
Trigger mode	Method for triggering switch between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. The options are as follows: • **Triggered by internal signal**: Triggered by image gain. • **Image triggered**: Triggered by visible light brightness of the current image that is analyzed by the camera using the digital photosensitivity algorithm. The triggering modes may vary depending on camera model.
Sensitivity	Sensitivity for switching between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. A higher sensitivity indicates higher flexibility to switch between the B/W mode and the color mode. The value defaults to **High**.

Exposure

The following figures show exposure parameters. The exposure parameters vary depending on the camera model.

Figure 3 Exposure parameters in aperture priority mode

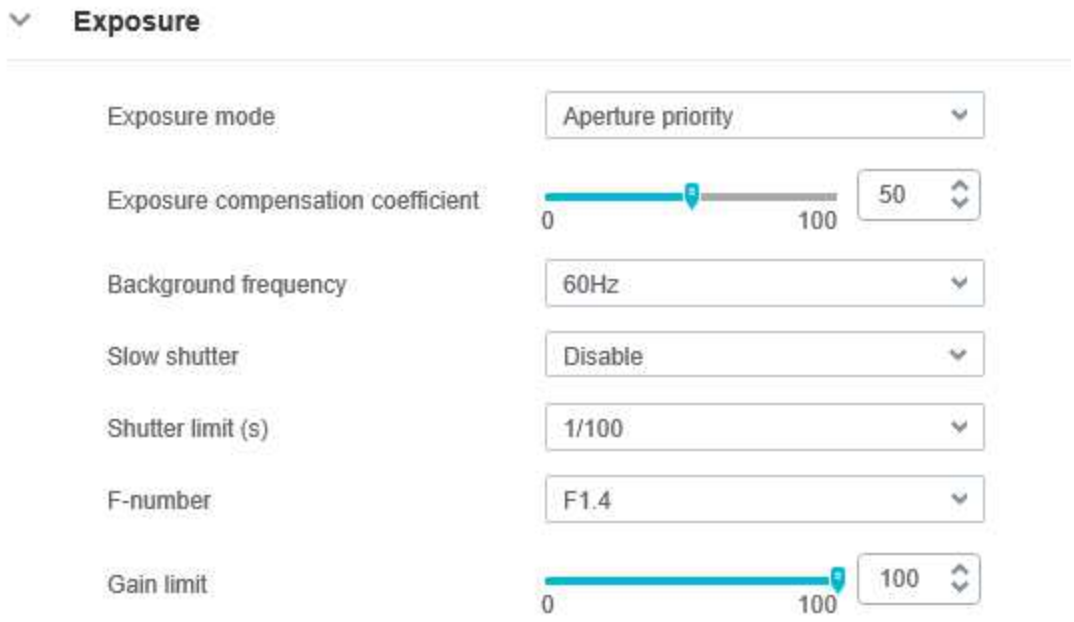


Figure 4 Exposure parameters in manual exposure mode



Figure 5 Exposure parameters in auto exposure mode



Table 3 Exposure parameters

Parameter	Description
Exposure mode	You can select an exposure mode based on the site requirements. The options are as follows: • **Auto** (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. • **Aperture priority**: The camera automatically selects a shutter speed and gain to match the manually specified aperture value. This mode is used to shoot static objects. • **Manual**: You manually set the shutter speed and gain when the auto exposure mode cannot meet the site requirements.
Exposure compensation coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure

Parameter	Description
	meter, in consideration of factors that may cause the indicated exposure to result in a less-than-optimal image. In poor light conditions, you can increase the exposure compensation coefficient to improve image brightness.
Shutter speed	This parameter is available only when you set **Exposure mode** to **Manual**. A larger value of this parameter indicates a longer exposure time.
Background frequency	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The value defaults to **Disable**. The periodic illuminance change of background light (such as strobe lights and sodium lamps) will result in horizontal banding in images. In this case, you need to set background frequency based on standard frequency of the local power grid. For example, if the standard frequency of the local power grid is 50 Hz, **Background frequency** needs to be set to 50 Hz. Disable the background frequency in natural light conditions.
Shutter limit (s)	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. This parameter is used to specify the minimum shutter speed. You can use the common values or customize values (unit: μs).
F-number	This parameter is available only when you set **Exposure mode** to **Manual** or **Aperture priority**.
Gain limit	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC).

Parameter	Description
	In the case of low illumination conditions, the AGC can be enhanced to improve image brightness. However, a high level of AGC will increase the image noise and degrade the image quality. Set this parameter based on the site requirements.
Gain	This parameter is available only when you set **Exposure mode** to **Manual**. The value defaults to **0**.
Slow shutter	The slow shutter function can be enabled or disabled only when **WDR/HLC/BLC** is set to **Disabled** or **Backlight compensation**. In other modes, the slow shutter function is disabled by default and is hidden.

Focus

Figure 6 Focus parameters



Table 4 Focus parameters

Parameter	Description
Focus mode	You can select a focus mode based on the site requirements. The options are as follows: • **Auto**: If you select this option, the camera automatically focuses on the current scene after you click  to zoom in or out. When the scene changes, the camera does not automatically focus. In this mode, you cannot

Parameter	Description
	manually adjust the focus (focus+/focus-:  , OnePush focus: ). The **Sensitivity** parameter is available only when you set **Focus mode** to **Auto**. The default value of **Sensitivity** is **Low**. • **Manual**: When this option is selected, the camera locks the focus for the current scene. In this case, the focus cannot be automatically adjusted after zooming in or out. You can only manually adjust the focus by clicking the focus icons (). • **Semi-auto** (default): When this option is selected, the camera automatically focuses on the current scene after zooming in or out (). However, when the scene is out of focus, the camera does not automatically refocus. You need to manually adjust the focus by clicking the focus icons (Focus+/-:  ; OnePush focus: ). **NOTE:** • If you click a zoom button on the PTZ control panel, the camera automatically refocuses as the scene changes. • If you click a focus button on the PTZ control panel, the camera locks the focus for the current scene and does not refocus when the scene changes.

Parameter	Description
Min. focus distance	The camera preferentially focuses on objects outside the minimum focus distance. **NOTE:** If the distance between the camera and an object is smaller than the value of **Min. focus distance**, the focus may be unclear.
Focus compensation	This function prevents the focus changes after the switch between the color mode and the B/W mode, ensuring that the objects to shoot are clear in the image.

Backlight

Figure 7 Setting WDR parameters



Figure 8 Setting HLC parameters



Figure 9 Setting backlight compensation parameters



Figure 10 Setting backlight adaptation parameters

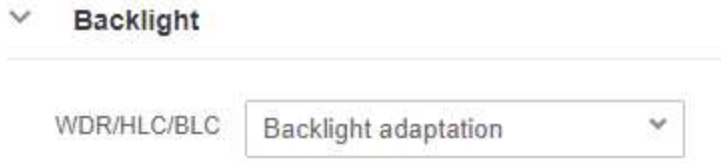


Figure 11 Setting WDR/HLC/BLC to Disabled



Table 5 Backlight parameters

Parameter	Description
WDR/HLC/BLC	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. • **Wide dynamic range**: This function is used to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. • **Highlight compensation**: This function is used to suppress large halo or image blur caused by directly radiated strong light by darkening the over-bright areas and brightening the dark areas to adjust the overall video brightness to normal.

Parameter	Description
	• **Backlight compensation**: This function is used to correct the exposure of objects in front of a bright light source. • **Backlight adaptation**: This function is used to correct the exposure of objects in front of a bright light source. • **Disabled**: None of the preceding functions takes effect.
BLC area	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Backlight compensation**. Backlight compensation is used to correct the exposure of objects in backlight scenarios. The options are as follows: **Central area**: dark area of the subject in the backlit environment. **Custom**: area customized on live video.
WDR coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Wide dynamic range**. A larger value of WDR coefficient indicates brighter backlit area in the image. The default value is **50**. WDR is intended to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. **NOTE:** You are advised not to enable the WDR function in scenarios with direct light radiation, for example, squares with road lamps (such as high-voltage sodium lamps and illuminators) at night.

Parameter	Description
HLC coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Highlight compensation**. The value defaults to **2**. A larger HLC coefficient indicates more powerful highlight compensation.

White Balance

Figure 12 White balance parameters



Table 6 White balance parameters

Parameter	Description
Mode	White balance adjusts the color circuit within a camera to remove color cast and ensure accurate color reproduction in various lighting conditions. For example, with a yellow light source, images appear yellowish. After proper white balance adjustment, the original color is reproduced. The options are as follows: • **Auto** (default): This option is recommended. The camera automatically adjusts the red and blue offsets in environments where the color temperature ranges from 2500 K to 10,000 K. Video images may be bluish in the morning or at dusk. You can drag the slider to change the values

Parameter	Description
	of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Manual**: The red and blue offsets must be adjusted manually. You can drag the slider to change the values of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Auto tracking**: The camera automatically adjusts the upper and lower limits of the color temperature in environments where the color temperature ranges from 1000 K to 15,000 K. • **One push**: This mode allows you to set the white balance mode in the current scene as the fixed mode for all scenes. Only a re-configuration can change the white balance mode. • **Indoor**: The camera automatically adjusts the red and blue offsets in indoor environments where tungsten lamps or incandescent lamps are used and the color temperature ranges from 2500 K to 5500 K. • **Outdoor**: This mode is applicable to sunny environments where the color temperature ranges from 5500 K to 6500 K. • **Fixed sodium lamp**: This mode is applicable to environments where sodium lamps are used and the color temperature ranges from 2000 K to 2300 K. • **Fluorescent lamp 1**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 2500 K to 3500 K. • **Fluorescent lamp 2**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 3500 K to 4500 K.

Parameter	Description
	• **Incandescent lamp**: This mode is applicable to environments where incandescent lamps are used and the color temperature ranges from 2700 K to 2900 K. • **Sunlight**: This mode is applicable to environments where green plants occupy more than 80% of the video image. This mode can alleviate the phenomenon that the white area appears reddish in this scenario.

Image Enhancement

The image enhancement functions vary depending on the camera model.

Figure 13 Overcast adaptation mode

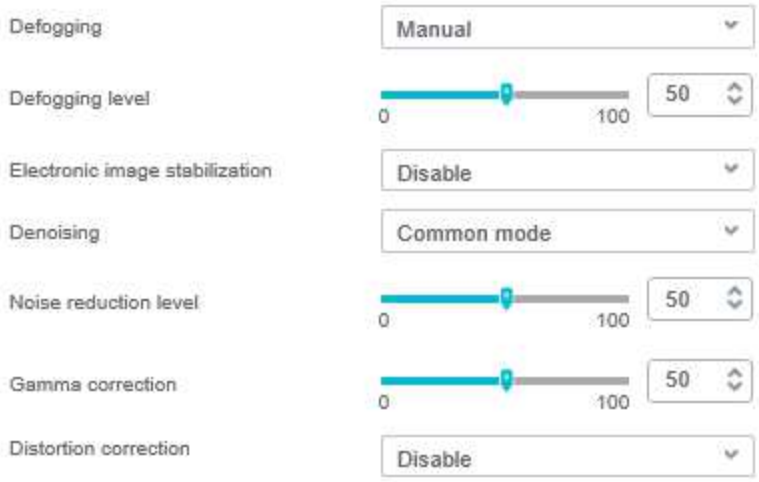


Table 7 Image enhancement parameters

Parameter	Description
Defogging	This function is used to increase the image clarity in poor weather conditions such as rain, fog, and smog. To disable this function, set this parameter to **Disable**.

Parameter	Description
	After the function is enabled, the camera determines whether to enable the defogging function based on the actual environment conditions. You can set the defogging level when this parameter is set to **Manual**. A higher defogging level indicates clearer images. However, a too high level will lead to image distortion. You need to set the defogging level based on the site requirements. **NOTE:** • Some camera models support the overcast adaptation mode but do not support the auto mode. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements.
Electronic image stabilization	Indicates whether to enable electronic image stabilization (EIS). EIS is used to compensate image vibration reversely to stabilize images when the camera is subject to vibrations, while some image details may be lost. The value defaults to **Disable**. In a short-focus scenario, if there are many moving objects, the camera may make misjudgment. Therefore, you are advised to enable this function in long-focus scenarios. When **Electronic image stabilization** is set to **Enable**, **Image stabilization sensitivity** can be set for some camera models, which is subject to the GUI. Higher sensitivity indicates better image stabilization effect. Set **Image stabilization sensitivity** based on the site requirements.

Parameter	Description
	NOTE: • Some camera models support electronic image stabilization. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements. • Enabling the electronic image stabilization function will slightly influence camera's field of view. For PTZ dome cameras, the PT speed at level 10 when this function is enabled differs from that when the function is disabled.
Denoising	Indicates whether to enable the noise reduction function. The options are as follows: • **Disable**: Disable the noise reduction function. • **Common mode** (default): In this mode, you can set **Noise reduction level**. A higher noise reduction level indicates better noise reduction effect but lower image clarity. The value defaults to **50**. • **Expert mode**: In this mode, you can set **Temporal denoising level** and **Spatial denoising level**. ▪ **Spatial denoising level**: Spatial noise reduction intends to reduce the noises on images horizontally and vertically at the cost of some edge details. A higher spatial noise reduction level indicates better noise reduction effect and smoother edges. ▪ **Temporal denoising level**: Temporal noise reduction intends to reduce the white noises

Parameter	Description
	distributed randomly between video frames to improve the image quality in low-light conditions. However, the noise reduction effect is affected by historical frame data, causing object trailing on images. A higher temporal noise reduction level indicates better noise reduction effect but more apparent trailing.
Gamma correction	This function is used to adjust and improve the image contrast to avoid new image noise.
Distortion correction	Lens distortion is an aberration that causes straight lines to curve near the edges of images. Distortion occurs when a short-focus or wide-angle lens is used to shoot large objects (such as high buildings) with distinct shapes. To ensure more accurate detection, distortion correction is required. • **Distortion correction**: You can select **Enable** or **Disable** from the drop-down list box to enable or disable the distortion correction function. • **Distortion correction mode**: Select a mode based on the site requirements. ▪ **Automatic**: In this mode, the camera automatically corrects the image based on the image analysis result. ▪ **Manual**: In this mode, the correction level can be configured. A higher level indicates a higher correction strength. You are advised to use the default value **50**. **NOTE:** • Some camera models do not support distortion correction. • If a privacy mask area is drawn, enabling distortion correction may disclose the privacy mask area. In

Parameter	Description
	this case, you need to draw a new privacy mask area.

Illuminator Control

Figure 14 Setting illuminator control parameters

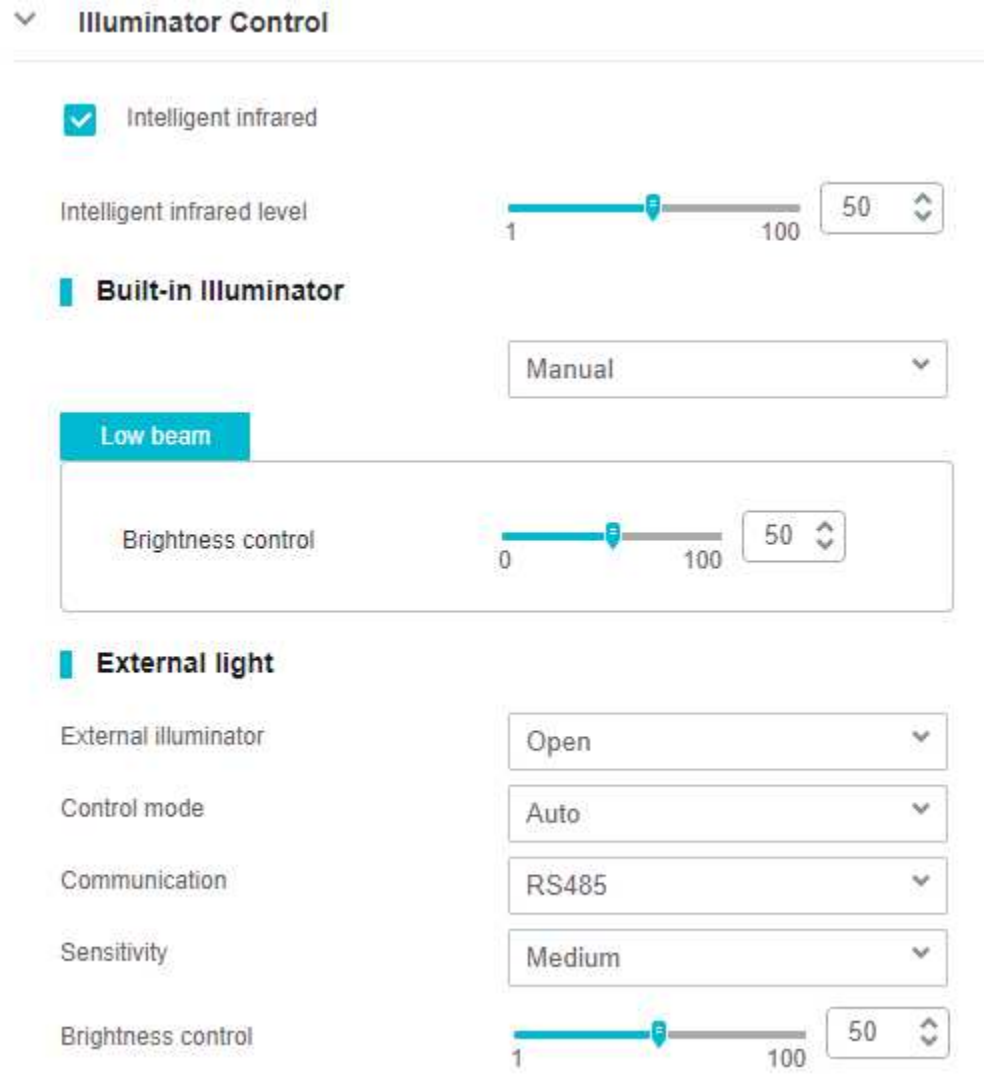


Table 8 Illuminator control parameters

Parameter	Description

Parameter	Description
Intelligent Infrared	If this parameter is selected, the infrared illuminator is enabled to avoid image overexposure. The function is enabled by default.
Intelligent infrared level	The default value is **50**. If overexposure occurs in scenarios with strong reflective objects such as leaves and wires nearby, you can set this parameter to a larger value.

Parameter		Description
Built-in light	Control mode	• **Auto** (default): Indicates that the camera automatically turns on or off the illuminator and controls its illuminance. • **Manual**: Indicates that the brightness can be manually controlled. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the illuminator will be turned off. • **Scheduled**: Indicates that the illuminator is automatically enabled and disabled at the specified time. You can customize **Turn on time**, **Turn off time**, and **Brightness control**. • **Intelligent**: Indicates that the illuminator is enabled and disabled based on the ambient light conditions. You can select this option when **Mode** under **Day/Night Switch** is set to **Auto**. After **Control mode** is set to **Intelligent**, the camera automatically turns on or off the illuminator and controls its illuminance. If the camera detects an alarm in B/W mode, the white-light illuminator is automatically turned on and the video image automatically turns to the color mode. After the alarm is cleared, the white-light illuminator is automatically turned off and the video image turns back to the B/W mode. **NOTE:**

Parameter		Description
		• In automatic mode, illuminators are automatically enabled or disabled based on the ambient illuminance. White-light illuminators work only in color mode, and IR illuminators work only in B/W mode. • In manual mode, the device determines whether to enable white-light or IR illuminators based on the current ambient illuminance. The user-defined brightness takes effect only when the device determines that illuminators need to be enabled. • Some camera models do not have white-light illuminators. • When **Control mode** is set to **Intelligent**, if the number of alarms generated within 10 minutes is greater than or equal to 4, the white-light illuminator will be on for 3 minutes. Otherwise, the white-light illuminator will be on for 1 minute.

Parameter	Description

Parameter		Description
	Low beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the low beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the low beam.
	Mid beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the mid beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the mid beam.
	High beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If

Parameter		Description
		Brightness control is set to **0**, the high beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the high beam. **NOTE:** • If **Mode** under **Day/Night Switch** is set to **Color**, high beam control does not take effect.
	Brightness control	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. A larger value indicates higher illuminator brightness.

Parameter		Description
External light	External illuminator	**Open**: Turns on the external illuminator. **Close** (default): Turns off the external illuminator.

Parameter		Description
	Control mode	• **Auto** (default): Indicates that the camera automatically controls the illuminator status (turned on or off) and brightness. • **Scheduled**: Indicates that you can customize **Turn on time**, **Turn off time**, and **Brightness control**.
	Communication	• **IO**: The illuminance of the external illuminator cannot be adjusted. This mode can be selected when the external illuminator is connected to the camera through the alarm-out port. • **RS485**: The illuminance of the external illuminator can be adjusted. This mode can be selected when the external illuminator is connected to the camera through the RS-485 port. • **RS485 (unified protocol)**: **NOTE:** • Only bullet cameras support the **RS485 (unified protocol)** communication mode.
	Sensitivity	• Sensitivity for determining the ambient illuminance threshold. A higher sensitivity indicates a lower threshold and a higher possibility of turning on illuminators. • This parameter can be set to **High**, **Medium** (default value), or **Low**.

Parameter		Description
	Brightness control	This parameter is available only when **Control mode** is set to **Auto** or **Scheduled**. A larger value indicates higher illuminator brightness.

Digital Zoom

Figure 15 Setting digital zoom parameters



Table 9 Digital zoom function

Digital zoom	You can select **Enable** from the drop-down list box to enable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the system will perform digital zoom and continue to zoom in on the image. However, the focal length is not changed.
	You can select **Disable** from the drop-down list box to disable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the image is not changed.

Parent topic: Wizard-based Configuration Guide

Configuring OSD

You can set on screen display (OSD) parameters to specify the information to be displayed and the display effect.

Setting OSD Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard**. Go to the **OSD** page. The web page varies between camera models.

   Figure 1 Setting OSD parameters



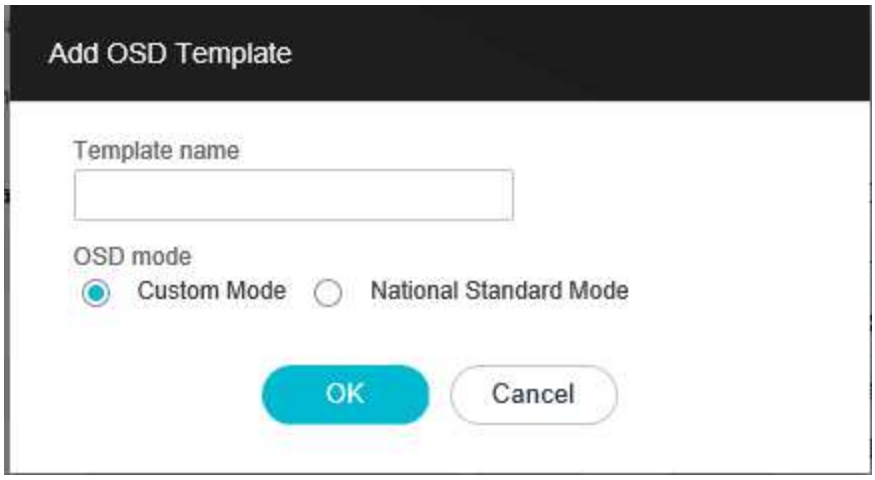
Figure 2 Setting GB-compliant OSD parameters



3. Configure the OSD template. Table 1 describes the OSD template parameters and buttons.

   - Click **Add OSD Template**. In the dialog box that is displayed, enter a name of the new template, set OSD mode, and click **OK**, as shown in Figure 3.

     Figure 3 Adding an OSD template

     NOTE

A maximum of eight OSD templates can be added.

- Select an OSD template and click **Copy OSD Template**. In the dialog box that is displayed, enter a new template name and click **OK**. The new template is added. The reference size of the new template is the same as that of the selected template.
- Select an OSD template and click **Delete OSD Template**. In the dialog box that is displayed, click **OK** to delete the template.

Table 1 OSD template parameters/buttons

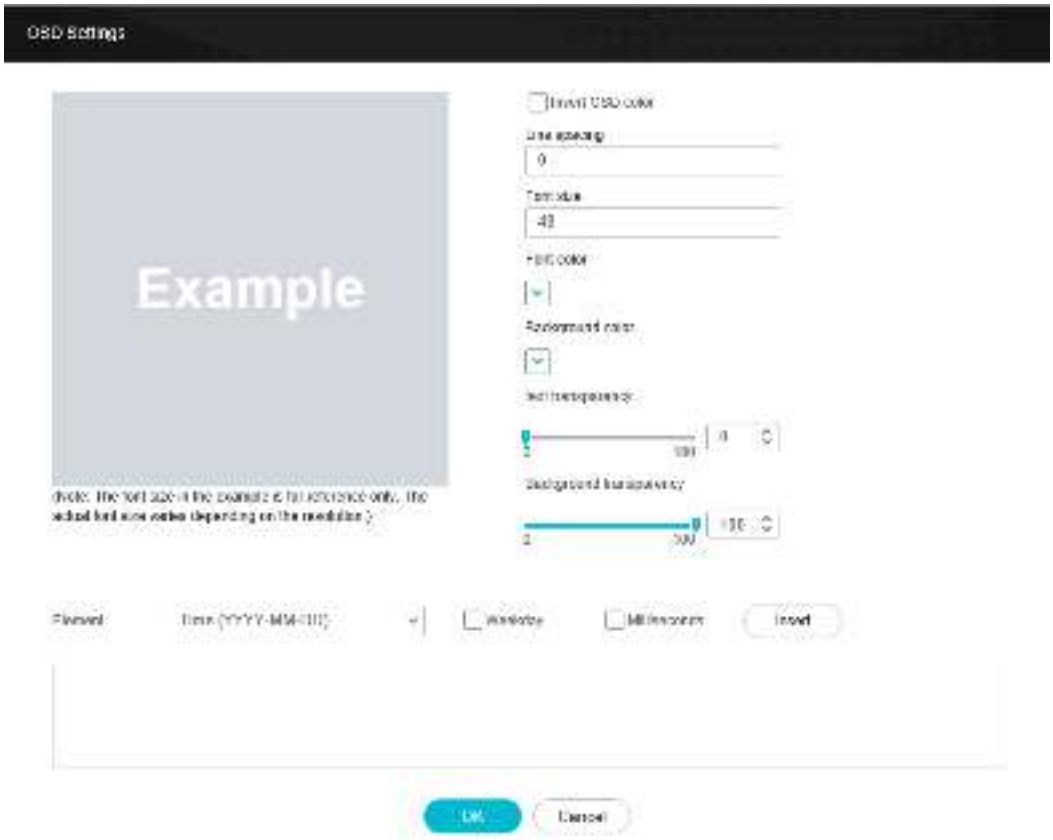
Parameter/Button	Description
Custom Mode	Custom OSD mode. If this mode is selected, you can add an OSD template with customized contents.
National Standard Mode	GB-compliant OSD mode. If this mode is selected, you must add a GB-compliant OSD template, in which the position and number of OSDs must be set to provided values, and other contents can be customized.
Template name	Name of the selected template. You can customize the name as required.
Minimum margin (characters)	Distance (maximum number of characters) between the OSD's edge and the edge of live video images. You can select a value from the drop-down list. This function is available only when a GB-compliant OSD template is added.
Reference size	The default value varies depending on the camera model. You cannot change the value of this parameter.

Parameter/Button	Description
Add OSD	Button for adding an OSD record using a template. **NOTE:** A maximum of eight OSD records can be added to each customized OSD template. In GB-compliant mode, the number of OSD records is fixed to four. You can only select one for use but cannot add or delete one. The OSD template name cannot contain vertical bars (|).
Delete All	Button for deleting all OSD records from a customized OSD template.
Enable	Indicates whether to display an OSD record on the video image. After you select the check box corresponding to an OSD record in the **Enable** column, the OSD record is displayed on the video image.
Align Type/Horizontal Margin/Vertical Margin/Content	These functions are available only for customized OSD templates. OSD alignment mode. You can select an option from the drop-down list. Horizontal and vertical margins. You can enter specific numbers in the **Horizontal Margin** and **Vertical Margin** text boxes to specify the margins.

Parameter/Button	Description
Content	OSD content. You can specify or change the OSD content in the text box at the bottom of the dialog box that is displayed after you click in the **Operation** column. **NOTE:** If the image overlay function is enabled, a maximum of seven OSD records are supported. Enabling the eighth OSD record will disable the image overlay function.
Operation	Column containing two icons and , which are available only for OSD records in custom mode. In GB-compliant mode, only the icon is available. : icon for modifying an OSD record. After you click this icon next to an OSD record, the **OSD Settings** dialog box is displayed. : icon for deleting an OSD record. After you click this icon next to an OSD record, the **Delete OSD Area** dialog box is displayed. You can click **OK** to delete the OSD record.

4. Click . The **OSD Settings** dialog box is displayed, as shown in Figure 4.

Figure 4 OSD Settings dialog box



5. Set OSD parameters based on the site requirements. Table 2 describes the parameters.

Table 2 OSD parameters

Parameter	Description
Invert OSD color	Indicates whether to set the OSD text color to a color opposite to the background. If you enable this function, the **Font color**, **Background color**, **Text transparency**, and **Background transparency** parameters will become unavailable.
Line spacing	OSD line spacing.
Font size	OSD text size. You can enter a value in the text box.

Parameter	Description
Font color	Color of the text displayed on the screen. This parameter is available only when you deselect **Invert OSD color**.
Background color	OSD background color. This parameter is available only when you deselect **Invert OSD color**.
Text transparency	Transparency of the OSD text. This parameter is available only when you deselect **Invert OSD color**.
Background transparency	Transparency of the OSD background. This parameter is available only when you disable **Invert OSD color**.
Element	Insertion element which can be selected from the drop-down list box. You can click **Insert** to insert the selected element. Different camera models may have different parameters. You can drag the text to adjust the text display location in the live video viewing area. • **Time/Display date/Display time/Weekday/Milliseconds**: You can select the time display format and select whether to display the week and millisecond. If multiple OSDs are added and **Milliseconds** is selected, the millisecond displayed in these OSDs may vary. • **PTZ information**: Display the coordinates and zoom information the PTZ device on the video image. • **Latitude and longitude**: Display the latitude and longitude information on the video image.

Parameter	Description
	• **Azimuth**: Display the azimuth information on the video image. • **OSDI**: Display OSDI on the video image. After the OSDI content is configured, **N/A** is displayed on the video image. To display the OSDI content, you need to enable OSDI first under **Configuration** > **PTZ** > **Location**. The OSDI content is displayed only when OSD coordinates are within the OSDI range. **NOTE:** The elements to be inserted vary depending on the camera model.

NOTE

- You can preview the font color, background color, text transparency, and background transparency in the **Example** area.
- If the aspect ratio of live video is different from that of images, for example, the aspect ratio of live video is 4:3 and that of images is 16:9, the OSD font cannot be scaled proportionally.

6. Click **Save**.

Parent topic: Wizard-based Configuration Guide

Configuring Intelligent Analysis Functions

This section describes the features supported in each intelligent mode.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Intelligence** page is displayed.
3. Select a required device or channel, and select a task type under the required intelligent analysis mode. Table 1 lists the intelligent analysis tasks supported in each mode.

   Different camera models support different intelligent analysis modes and task types.

   Table 1 Intelligent tasks

Intelligent Mode	Task Type	How to Configure
Target intelligence	Target capture	For details, see Configuring Target Capture.

Intelligent Mode	Task Type	How to Configure
Behavior analysis	Tripwire crossing detection	For details, see Configuring Tripwire Crossing Detection.
	Intrusion detection	For details, see Configuring Intrusion Detection.
	Loitering detection	For details, see Configuring Loitering Detection.
	Area entry/exit detection	For details, see Configuring Area Entry/Exit Detection.
	Fast movement detection	For details, see Configuring Fast Movement Detection.
	Detection of electric bikes in elevators	For details, see Configuring Electric Bike Detection in Elevators or Corridors.
	Abandoned object detection	For details, see Configuring Abandoned Object Detection.
	Removed object detection	For details, see Configuring Removed Object Detection.
	Parking detection	For details, see Configuring Parking Detection.

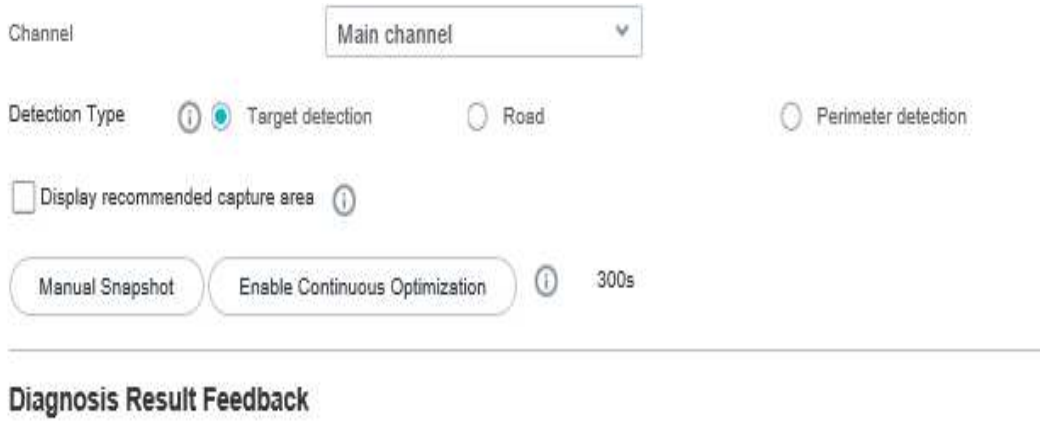
Intelligent Mode	Task Type	How to Configure
Situation analysis	Head counting	For details, see Configuring Head Counting.
	Crowd density detection	For details, see Configuring Crowd Density Detection.
	Queue length detection	For details, see Configuring Queue Length Detection.
	Crowd gathering detection	For details, see Configuring Crowd Gathering Detection.
	Off-duty detection	For details, see Configuring Absence Detection.
	Hot zone analysis	For details, see Configuring Hot Zone Analysis.
	Heat map	For details, see Configuring the Heat Map Function.
Tracking intelligence	Automatic tracking	For details, see Configuring Automatic Tracking.

Parent topic: Wizard-based Configuration Guide

Diagnosing Image Quality

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard**. Then click **Image Diagnosis**. On the page that is displayed, set **Channel**, as shown in Figure 1.

   Figure 1 Image Diagnosis area

3. (Optional) Select **Display recommended capture area**.

   The recommended capture area is framed on the video image. During diagnosis, keep objects in the displayed frame.

4. Click **Manual Snapshot**.

   Take target detection as an example. The camera will diagnose quality of captured images, including:

   - Target size
   - Image clarity
   - Horizontal angle of the camera
   - Vertical angle of the camera

   For road detection scenarios, the system does not diagnose the camera angle. Figure 2 shows the diagnosis result. You can click **Download** to download the diagnosis result image.

Figure 2 Diagnosis result



5. Adjust the camera parameters based on the optimization suggestions.
    - If the horizontal or vertical angle of the camera does not meet the requirements, adjust the horizontal or vertical angle of the camera.

      For road detection scenarios, the system does not provide optimization suggestions about the camera angle.
    - If the target size and image clarity do not meet the requirements, click **Auto Adjust** to automatically adjust the zoom ratio or focus.
6. After you click **Enable Continuous Optimization**, the system automatically diagnoses the image quality every 10s. The diagnosis lasts for 300s and can be stopped at any time. Other services are suspended during the diagnosis and resumed after the diagnosis is complete. Exercise caution when performing this operation.

> **NOTE**
>
> - Image diagnosis is not supported in full intelligence mode for multi-algorithm cameras.
> - Image diagnosis is not supported in 1 + N mode.

- Automatic focus is supported during image diagnosis only when the camera is in target checkpoint mode and **Focus mode** is set to **Auto** or **Semi-auto** under **Configuration** > **Image** > **Display** > **Focus**.

Parent topic: Wizard-based Configuration Guide

Configuring Network Platform Connection

This section describes how to set network platform connection parameters. Different parameters need to be set for different protocols. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera.

Setting SDK Parameters This section describes how to set related parameters for a camera to proactively register with the IVS platform through the SDK protocol.

Setting Second Protocol Parameters
Cameras can connect to a video security platform through SDK, GB/T 28181, or ONVIF.

Configuring Password Management
To ensure data security, change the passwords of platform connection protocols timely. After the passwords are changed, record and save them.

Configuring Cloud Service Connection
After a camera is connected to the cloud service, you can view live and recorded video from the camera on your mobile app. The capabilities supported vary between camera models.

Parent topic: Wizard-based Configuration Guide

Setting SDK Parameters

This section describes how to set related parameters for a camera to proactively register with the IVS platform through the SDK protocol.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. In the **SDK Settings** area, select **Enable SDK** to enable the SDK protocol.
4. Set SDK parameters, as shown in Figure 1. Table 1 describes the parameters.

> **NOTE**
>
> - If the camera needs to be registered with multiple platforms, select **Platform *X*** and configure information about the platform.
> - Cameras with dual network ports support six platforms. Before the configuration, select the required network port ETH0 or ETH1.
> - To select **Active SDK registration**, ensure that the camera time is the same as the platform time. You are advised to enable NTP time calibration to calibrate the camera time. For details, see Time Configuration.
> - If **Two-factor authentication** is selected, an encrypted port must be configured. If a non-encrypted port is configured, proactive registration will fail.

Figure 1 Setting SDK parameters



Table 1 SDK parameters

Parameter	Description
SDK non-encrypted port	Indicates whether to enable the SDK non-encrypted port. After this parameter is selected, the non-encrypted port can be registered. After **Enable SDK** is selected, **SDK non-encrypted port** is enabled by default.
Active SDK registration	Indicates whether to enable proactive camera registration.
Two-factor authentication	Authentication mode between the camera and the platform. If **Two-factor authentication** is selected, TLS authentication is used. If **Two-factor authentication** is not selected, password authentication is used. **NOTE:** If **Two-factor authentication** is selected, an encrypted port must be configured. If a non-encrypted port is configured, proactive registration will fail.
Registration type	The options are as follows:

Parameter	Description
	• **Single-server mode**: applies when the IVS platform is deployed in a single-node system. • **Dual-server mode**: applies when the IVS platform is deployed in a two-node cluster. The principles are as follows: • In dual-server mode, the camera preferentially connects to the platform using the first IP address. When the connection fails or interrupts, the camera connects to the platform using the second IP address. When the connection to the first platform recovers, the camera will connect to the first platform only after disconnecting from the second platform. • The camera can be registered with only one platform at a time. • The camera can be connected to a third-party platform, including those deployed in a two-node cluster.
Active platform IP	Set this parameter based on the actual IP address of the connected platform. • If the camera needs to connect to the IVS1800, enter the IP address of the platform. • If the camera needs to connect to the IVS3800, enter the floating gateway IP address of the MPU cluster. If the server and camera are on different networks and NAT is deployed, set this parameter to the post-NAT IP address of the cluster floating gateway.

Parameter	Description
Port number	SDK protocol port that the platform listens on.
Device ID	Unique device ID. **NOTE:** Enter a string of 20 digits. The value must be the same as the connection code configured on the platform. Otherwise, the connection fails.

5. Click **Save**.

Parent topic: Configuring Network Platform Connection

Setting Second Protocol Parameters

Cameras can connect to a video security platform through SDK, GB/T 28181, or ONVIF.

Setting Media Stream Keep-Alive Parameters You can set media stream keep-alive parameters to ensure that media streams can be properly requested when the platform is connected through protocols such as SDK or ONVIF.

Setting ONVIF Parameters
You need to set ONVIF parameters if you want to use the ONVIF protocol to connect a camera to the platform.

Setting GB/T 28181 Parameters
This section describes how to set GB/T 28181 parameters if a camera needs to connect to the platform through the GB/T 28181 protocol.

Setting GA/T 1400 Parameters
Cameras can connect to the IVS platform through the GA/T 1400 protocol. This section describes only how to set GA/T 1400 parameters on the camera side. For details about the configuration on the platform side, contact technical support engineers on the platform side.

Configuring Connection to the Platform Through RESTful
This section describes how to connect a camera to the IVS platform through the RESTful protocol.

Configuring Connection to the Platform Through RTSP
RTSP is an application-level protocol for the controls, such as play, pause, and fast-forward, of real-time streaming data.

Parent topic: Configuring Network Platform Connection

Setting Media Stream Keep-Alive Parameters

You can set media stream keep-alive parameters to ensure that media streams can be properly requested when the platform is connected through protocols such as SDK or ONVIF.

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Click **Second Protocol Parameters** and select **Enable media stream keep-alive**, as shown in Figure 1.

   Figure 1 Setting media stream keep-alive parameters

4. Set media stream keep-alive parameters. Table 1 describes the parameters.

   Table 1 Media stream keep-alive parameters

Parameter	Description
Enable media stream keep-alive	Indicates whether to enable the keep-alive function for media streams, which is mandatory when the media stream request mode is used. When the camera is connected to the platform through the SDK, GB/T 28181, GB 35114, ONVIF, or RESTful protocol, the media stream request mode is used. If the platform supports the keep-alive function, you are advised to select **Enable media stream keep-alive**.
Keepalive duration (s)	Media stream keep-alive duration. The default value is 60s. If the camera does not receive a media stream request within the keep-alive duration, the camera stops sending media streams.
Device ID	Unique ID of a device. **NOTE:**

Parameter	Description
	For a multi-channel model, the device ID must be unique and the device ID of at least one channel must be set.

Parent topic: Setting Second Protocol Parameters

Setting ONVIF Parameters

You need to set ONVIF parameters if you want to use the ONVIF protocol to connect a camera to the platform.

Prerequisites

- The ONVIF protocol uses MD5 digest authentication, which is a weak algorithm that does not encrypt media streams. Therefore, use this protocol on a trusted network to prevent security risks.
- Both the camera ONVIF protocol and the video security platform must support the H.265 encoding protocol if the ONVIF protocol needs to use the H.265 encoding protocol. Cameras must be of V200R003C10 or later versions. As for the video security platform, contact the platform supplier to confirm whether the platform supports H.265.
- By default, the ONVIF protocol uses the HTTP/HTTPS transmission protocol.
- The ONVIF protocol supports only the G711 and G726 audio encoding formats. Other audio encoding formats may cause the failure to functions such as voice intercom and broadcast and channel-associated voice.
- The corresponding port number is **80** or **8080**.

> **NOTE**
>
> - If the platform is on a public network and the camera is on a private network, the ONVIF protocol can be used to connect the camera to the platform for NAT traversal. For other cases, see the IVS series product documentation.
> - After a camera is connected to the platform through ONVIF, the camera-related parameters modified on the platform will be synchronized to the camera web system. Therefore, do not modify the camera parameters directly in the camera

web system. Otherwise, the parameter settings on the platform and camera will be inconsistent.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Choose **Second Protocol Parameters** > **ONVIF** to access the page for setting ONVIF parameters.
4. Set ONVIF parameters, as shown in Figure 1. Table 1 describes the ONVIF parameters.

Figure 1 Setting ONVIF parameters



Table 1 ONVIF parameters

Parameter	Description
Enable ONVIF	Indicates whether to enable the ONVIF protocol.
Validity period	Indicates whether to enable the validity period function for the ONVIF message.

Parameter	Description
	After this function is enabled, an ONVIF message will become invalid when the specified validity period elapses. **NOTE:** The ONVIF message validity period function is valid only when being supported by the video security platform. If the platform does not support this function but this parameter is selected, the camera will fail to connect to the platform. You are advised to enable this function only when security risks exist. The ONVIF message validity period function is disabled by default.
Stream type	Stream transmission type. You can select a value from the **Stream type** drop-down list box. The options are as follows: • **Elementary stream**: uses the ES compression mode. • **Program stream**: uses the PS compression mode. **NOTE:** • Select a proper stream type based on the decoder requirements. • The ONVIF media stream can be configured only when the camera is connected to the video security platform through the ONVIF protocol.
Authentication mode	Authentication method. You can select a value from the **Authentication mode** drop-down list box.

Parameter	Description
	The options are as follows: • **Digest_MD5**: Digest authentication with MD5 encryption. • **Digest_SHA256**: Digest authentication with SHA256 encryption. • **Digest_MD5/Digest_SHA256**: Both Digest_MD5 and Digest_SHA256 authentication methods are supported. • **Digest_MD5(priority)/WSSE**: Both Digest_MD5 and WSSE authentication methods are supported, but Digest_MD5 authentication is preferred. • **WSSE**: Web Service Security (WSSE) authentication mode. • **None**: indicates that authentication is not performed. **NOTE:** • The ONVIF MD5 and WSSE authentication modes may cause security risks. ▪ When some platforms to which the cameras connect support ONVIF WSSE authentication only, use the Digest_MD5(priority)/WSSE authentication mode. ▪ When all platforms to which the cameras connect support ONVIF WSSE authentication only, use the WSSE authentication mode. ▪ You are advised to enable the WSSE authentication mode when some platforms cannot correctly process Digest messages.

Parameter	Description
	• Security risks may exist when you select **None**. It is recommended that this authentication method be enabled only when the platform does not support authentication. The authentication mode is independently configured for RTSP. If RTSP does not require authentication, you need to set its authentication mode to **None** by referring to Configuring Connection to the Platform Through RTSP. Otherwise, stream requesting may fail.
Version	ONVIF version supported by the camera, which must be consistent with that supported by the platform.
Transmission protocol	ONVIF transmission protocol type. The options are as follows: • **HTTP/HTTPS**: Data is transmitted through HTTP or HTTPS. • **HTTP**: Data is transmitted through HTTP. • **HTTPS**: Data is transmitted through HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Forbid ONVIF to change system time	Indicates whether to forbid the system time to be changed through the ONVIF protocol.
Using old mode time	Indicates whether to reverse the time zone when you set the time through the ONVIF

Parameter	Description
zone	protocol.
WSSE anti-replay	Indicates whether to enable the anti-replay function when ONVIF WSSE authentication is used.

Parent topic: Setting Second Protocol Parameters

Setting GB/T 28181 Parameters

This section describes how to set GB/T 28181 parameters if a camera needs to connect to the platform through the GB/T 28181 protocol.

A camera can be registered with two platforms through GB/T 28181. When a camera is registered with multiple platforms, if the platforms synchronize NTP server time to the camera at the same time, the camera time may be discontinuous. You are advised to keep only one platform that can synchronize NTP server time to the camera.

NOTE

- The GB/T 28181 protocol supports independent upgrade. Light intelligence and inclusive intelligence cameras do not support independent upgrade. For details about how to obtain the upgrade package and perform the upgrade, see Upgrading the Camera Version/Algorithms.
- You can query a maximum of 500 recording segments at a time. If the number of recording segments within the specified query period exceeds 500, change the start time and end time.

Prerequisites

- The GB/T 28181 protocol supports MD5 and SHA256 digest authentication. The MD5 algorithm is a weak algorithm, and the signaling flow and the media stream are not encrypted, which may result in security risks. Therefore, use this protocol on a trusted network.
- You have obtained the values of the parameters (for example, device ID) for connecting cameras to the video security platform through the GB/T 28181 protocol.

Setting the System Time

To connect a camera to the platform through the GB/T 28181 protocol, ensure that the camera is time-synchronized with the NTP server. The capabilities supported vary between camera models.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration Wizard** > **Time**.

   The **Time** page is displayed, as shown in Figure 1.

   Figure 1 Setting time



3. Set the system time, as shown in Figure 1.
   a. Select a time zone from the **Time zone** drop-down list box.
   b. Set **Calibration mode** to **NTP**.
   c. Set **NTP server**.
      - If the camera is to be connected to a single IVS platform, set this parameter to the IP address of the IVS platform.
      - If the camera is to be connected to a cluster, set this parameter to the floating gateway IP address of the cluster.
4. Click **Save**.

Setting GB/T 28181 Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Choose **Second Protocol Parameters** > **T28181**.

> **NOTE**

To register with two platforms, you also need to choose **Second Protocol Parameters** > **T28181.2** and configure information about the other platform. You can set GB 35114 protocol parameters only on the **T28181** tab page.

4. Set GB/T 28181 parameters, as shown in Figure 2 and Figure 3. Table 1 and Table 2 describe the GB/T 28181 parameters. The parameters vary between camera models.

Figure 2 Setting common GB/T 28181 parameters

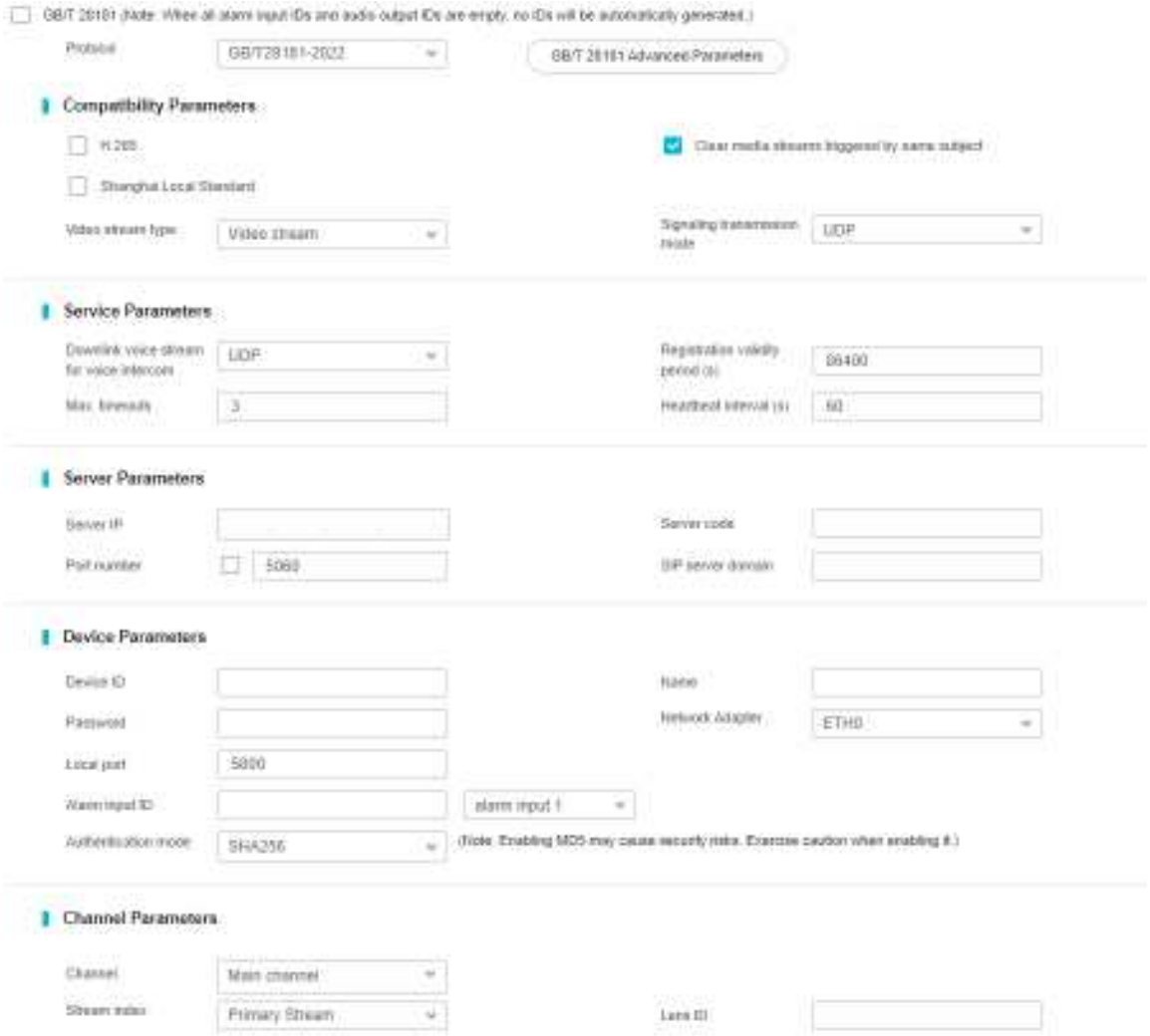


Figure 3 Setting advanced GB/T 28181 parameters



Table 1 GB/T 28181 parameters

Parameter	Description
GB/T 28181	If this parameter is selected, the GB/T 28181 protocol is supported.
Protocol	Protocol type. You can select a value from the drop-down list box. The default value is **GB/T 28181-2016**. **NOTE:** • In addition to the default protocol, the camera also supports the GB/T 28181-2022 and TCC-VMS-2020 protocols. • When the TCC-VMS-2020 protocol is selected, the active and standby servers can be configured. When the active (standby) server is faulty, services are automatically switched to the standby (active) server.

Parameter		Description
Compatibility Parameters	H.265	If this parameter is selected, the H.265 and other related encoding protocols are supported when the camera is connected to the platform through the GB/T 28181 protocol. If this parameter is not selected, only other related encoding protocols are supported when the camera is connected to the platform through the GB/T 28181 protocol.

Parameter		Description
	Clear media streams triggered by same subject	If this parameter is selected, only one channel of video streams can be obtained if the platform requests video streams with the same subject ID. If this parameter is not selected, multiple channels of video streams can be obtained if the platform requests video streams with the same subject ID.
	Shanghai local standard	If this parameter is selected, the Shanghai local protocol is supported. **NOTE:** If the Shanghai local standard is enabled, the image capture function of the platform does not take effect.
	Video stream type	Video stream type. You can select a value from the drop-down list box. • **Auto**: Sends media streams based on the request of the platform. • **Video stream**: Sends only video streams. • **Hybrid stream**: Sends video and audio streams.
	Signaling transmission mode	Signaling transmission mode. The options include **UDP** and **TCP**.

Parameter		Description
Service Parameters	Downlink voice streams for voice intercom	Protocol of downlink voice streams for voice intercom. The value can be **UDP** or **TCP**. **NOTE:** If the camera and the platform are on different network segments, you are advised to set this parameter to **TCP**.
	Max. timeouts	If the number of consecutive heartbeat timeouts reaches the value specified by this parameter, the camera cannot connect to the platform. The default value **3** is recommended. **NOTE:** The value of **Max. timeouts** for the camera and platform must be the same.
	Registration validity (s)	Validity period of the camera registration with the video security platform. The default value is **86400s** (one day). **NOTE:** Before the validity period expires, the device initiates a registration request to the platform again.
	Heartbeat interval (s)	Time interval for the camera to send heartbeat messages. The default value **60** is recommended. **NOTE:** The camera and the platform must have the same heartbeat interval.

Parameter		Description
Server Parameters	Server IP	• If the camera needs to connect to the IVS1800, enter the IP address of the platform. • If the camera needs to connect to the IVS3800, enter the floating gateway IP address of the MPU cluster. If the server and camera are on different networks and NAT is deployed, set this parameter to the post-NAT IP address of the cluster floating gateway.
	Port number	Port number for the platform to listen on cameras connecting to the platform through GB/T 28181. The default value is **5060**. To connect to the IVS platform, change the value to **5080**. After selecting the **Port number** check box, you can configure the port number range.
	Server code	GB/T 28181 server code. Enter a string of 1 to 64 characters. The value can contain letters and digits. **NOTE:** If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the server code must be **200**.
	SIP server domain	Domain name that consists of 1–127 digits.

Parameter		Description
Device Parameters	Device ID	Unique ID of a device. The value is a string of 1 to 64 characters, including letters and digits. The value must be the same as the connection code configured on the platform. **NOTE:** • This parameter is mandatory. If you do not set it, the camera cannot go online. • If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the camera ID must be **132**. Besides, the camera ID must be different from the lens ID. Otherwise, you cannot view live video from the camera on the platform.

Parameter	Description

Parameter		Description
	Password	Password used by a camera to register with the platform. **NOTE:** • The value of this parameter must be the same as the registration password configured on the platform. If they are different, the camera will fail to connect to the video security platform.
	Name	Login name used for registering the camera with the platform. The value can contain digits or other characters.
	Local port	Port number of the camera when the camera is connected to the SIP server. **NOTE:** The value is an integer ranging from 1024 to 65535.
	Alarm input ID	Alarm input ID of the device. The value is a string of 0 to 64 characters, including letters and digits. If there are multiple alarm input channels, you need to specify a unique ID for each channel. **NOTE:** • Some C/D series cameras do not support this parameter. • You need to manually enter the value. The eleventh to thirteenth digits must be **134**. Otherwise, the IVS platform cannot report alarms properly.

Parameter		Description
	Audio output ID	Audio output ID of the device. The value is a string of 0 to 64 characters, including letters and digits. **NOTE:** • Some C/D series cameras do not support this parameter. • You need to manually enter the value. The eleventh to thirteenth digits must be **137**. Otherwise, the IVS platform cannot transmit uplink or downlink audio streams properly.
	Authentication mode	• **SHA256**: Only the SHA256 authentication mode is supported. • **MD5/SHA256**: Both MD5 and SHA256 authentication modes are supported. **NOTE:** • The MD5 authentication mode has security risks. Therefore, you are advised to use the SHA256 authentication mode. • The value of this parameter must be the same as that configured on the platform. Otherwise, the registration fails.

Parameter		Description
Channel Parameters	Channel	Channel type of the camera.
	Stream index	Type of streams to be sent to the platform. You can select the primary stream or a secondary stream. The default value **Primary** is recommended.
	Lens ID	Lens ID. The value is a string of 0 to 64 characters, including letters and digits. For a multi-lens camera, you need to specify a unique ID for each lens. **NOTE:** If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the lens ID must be **131** or **132**. Otherwise, live video from the camera cannot be viewed on the platform.

Table 2 Advanced GB/T 28181 parameters

Parameter	Description
Max recordings can be queried	Maximum number of recordings carried in a packet during recording query when GB/T 28181 is used to platform connection. Enter an integer ranging from 1 to 20. The default value is 10. If the platform limits the packet size, you can properly adjust the value of this parameter. Adjusting the value of this parameter affects the recording query speed. Adjust the value based on the site requirements.
T28181 Media Stream Keep Alive	This function is disabled by default. When this function and the media stream keepalive function are enabled at the same time, RTCP keepalive packets can be sent. If the platform supports the

Parameter	Description
	keepalive function, you are advised to enable this function.

Parameter		Description
Site Information Reporting	Site type	Type of the site. The options include **Class-1**, **Class-2**, **Class-3**, and **Others**.
	Capture position type	Type of the capture position. The value is a string of seven digits.
	Industry category code	Industry category code of the site. The value is a string of 0 to 4 digits.
	Regional organization code	Regional organization code of the site. The value is a string of six digits.
	Site name	Name of the site. The value is a string of 0 to 254 characters, including letters and digits.
	Installation location	Site installation location. The options include **Indoor**, **Outdoor**, and **None**.
	Viewing direction	Viewing direction. The options include **East**, **West**, **South**, **North**, **Southeast**, **Northeast**, **Southwest**, **Northwest**, and **None**.
	Installation date	Time when a camera is installed.
	Management agency	Agency that manages the camera. Enter a string of 0 to 254 characters (including letters and digits).
	Administrator's contact method	Contact information of the camera administrator. The value is a string of 0 to 254 characters, including letters and digits.
	Checkpoint function	Camera function that can be reported through GB/T 28181. The options include **Target**, **Person**, **Motor vehicle**, **Non-motorized vehicle**, **Perimeter**, and **Others**.

5. Click **Save**.

Parent topic: Setting Second Protocol Parameters

Setting GA/T 1400 Parameters

Cameras can connect to the IVS platform through the GA/T 1400 protocol. This section describes only how to set GA/T 1400 parameters on the camera side. For details about the configuration on the platform side, contact technical support engineers on the platform side.

NOTE

- The GA/T 1400 protocol supports independent upgrade. For details about how to obtain and install the upgrade package, see Upgrading the Camera Version/Algorithms.
- The parameters displayed on the web page vary depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. In the **Second Protocol Parameters** area, click the **GA/T 1400** tab.

   NOTE

   To register with two platforms, choose **Second Protocol Parameters** > **GA/T 1400-2** and configure information about the other platform.

4. Set GA/T 1400 parameters, as shown in Figure 1. Table 1 describes the GA/T 1400 parameters.

   Figure 1 Setting GA/T 1400 parameters



Table 1 GA/T 1400 parameters

Parameter	Description
GA/T 1400	Indicates whether to enable the GA/T 1400 protocol.
Transmission protocol	• **HTTP**: Data is transmitted through HTTP. • **HTTPS**: Data is transmitted through HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Authentication mode	• **SHA256**: Only the SHA256 authentication mode is supported. • **MD5/SHA256**: Both MD5 and SHA256 authentication modes are supported. **NOTE:** • The MD5 authentication mode has security risks. Therefore, you are advised to use the SHA256 authentication mode.

Parameter	Description
	• The value of this parameter must be the same as that configured on the platform. Otherwise, the registration fails.
Platform address	Domain name or IP address of the IVS platform.
Coordinate type	Coordinate type used to upload target coordinate data through the selected transmission protocol. The options are as follows: • **Absolute**: absolute coordinate of a target. • **Relative**: relative coordinate of a target, that is, permyriad of the position of the target to the width and height of the image.
Port number	Port used by the platform to listen on the GA/T 1400 protocol. The value is an integer ranging from 1 to 65535. **NOTE:** • When the camera is to be connected to the IVS platform: ▪ If **Transmission protocol** is set to **HTTP**, you need to set **Port number** to **8001**. ▪ If **Transmission protocol** is set to **HTTPS**, you need to set **Port number** to **8002**. • When the camera is to be connected to another platform, you need to comply with the port configuration specifications on the platform side.
Device ID	Unique ID of a device. For cameras with multiple video channels, you can configure a unique ID for each video channel. Then each channel will be registered and report metadata independently. You can also configure the same ID for all video channels. Then the video channels will be registered and report metadata using the same ID.

Parameter	Description
Checkpoint ID	ID of the checkpoint to which the current device belongs. For a camera with multiple video channels, if the video channels belong to different checkpoints, you can configure the checkpoint ID for each video channel based on the site requirements. If all video channels belong to the same checkpoint, you can configure a checkpoint ID for all the channels.
User name	Login name used to register the camera with the platform.
Password	Password for registering the camera with the platform. **NOTE:** • The value of this parameter must be the same as the registration password configured on the platform. If they are different, the camera will fail to connect to the platform.

5. (Optional) Click **Advanced GA/T 1400 Parameters**. The **Advanced GA/T 1400 Parameters** dialog box is displayed, as shown in Figure 2. Table 2 describes the parameters.

Figure 2 Advanced GA/T 1400 Parameters dialog box

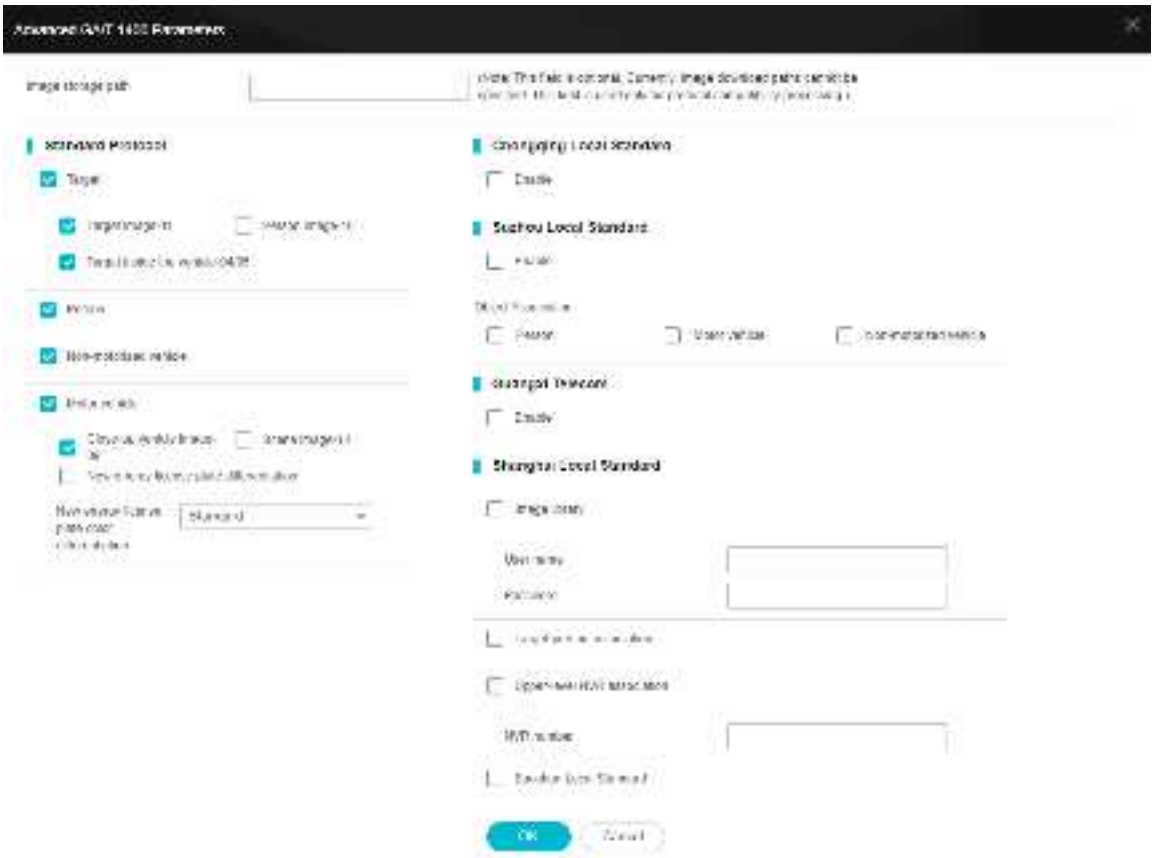


Table 2 Advanced GA/T 1400 parameters

Parameter	Description
Image storage path	Image storage path. **NOTE:** • At some sites, this parameter cannot be left empty due to compatibility issues. Otherwise, the platform connection may fail. You need to set a path that can be parsed to ensure proper connection between cameras and the platform. • Currently, you cannot download images from the path. This field is used for protocol compatibility processing.

Parameter		Description
Target	Target	Indicates whether to report target information.
	Target image-11	Indicates whether to report target images whose image type is 11. **CAUTION:** If this parameter is not selected, all target images (including in-vehicle targets) are not reported.
	Person image-10	Indicates whether to report person images whose image type is 10. If this parameter is not selected, person images are not reported.
	Target inside the vehicle-04/05	Indicates whether to report close-up images (whose image type is 04 or 05) of the driver and front passenger. If this parameter is not selected, close-up images of the driver and front passenger are still reported but the image type is 11. **NOTE:** Close-up images of the driver and front passenger are reported no matter whether this parameter is selected.
Person		Indicates whether to report person images.
Non-motorized vehicle		Indicates whether to report images of non-motorized vehicles.

Parameter		Description
Motor vehicle	Motor vehicle	Indicates whether to report license plates and full images of motor vehicles.

Parameter		Description
	Close-up vehicle image-09	Indicates whether to report close-up images (whose image type is 09) of motor vehicles. If this parameter is not selected, close-up images of motor vehicles are not reported.
	Scene image-14	Indicates whether to report full images (whose image type is 14) of motor vehicles. If this parameter is not selected, full images of motor vehicles are still reported but the image type is 01. **NOTE:** Full images of motor vehicles are reported no matter whether this parameter is selected.
	New-energy license plate differentiation	If this check box is selected, the system reports vehicle type 51 for license plates of large new-energy vehicles and vehicle type 52 for license plates of small new-energy vehicles. If this check box is not selected, the system reports the vehicle type based on the standard definition (01: license plates of large vehicles; 02: license plates of small vehicles).
	New energy license plate color differentiation	• **Standard**: reports vehicle type 9 for license plates of both large and small new-energy vehicles. • **Yellow Green 51 & Gradient Green 52**: reports vehicle type 51 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 52 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 52 & Gradient Green 51**: reports vehicle type 52 for license

Parameter		Description
		plates of large new-energy vehicles (yellow and green), and reports vehicle type 51 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 20 & Gradient Green 9**: reports vehicle type 20 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 9 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 98 & Gradient Green 97**: reports vehicle type 98 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 97 for license plates of small new-energy vehicles (gradient green).
Chongqing Local Standard	Enable	Indicates whether to report information based on the requirements defined in the Chongqing local standard.
Suzhou Local Standard	Enable	Indicates whether to report information based on the requirements defined in the Suzhou local standard.
Guangxi Telecom	Enable	Indicates whether to report information based on the requirements defined in the Guangxi Telecom standard.

Parameter		Description
Shanghai Local Standard	Image library	Indicates whether to separately report images to the image library. If this parameter is selected, information is reported based on the requirements defined in the Shanghai local standard and images are separately uploaded to the image library.
	User name	User name of the image library used to authenticate the camera.
	Password	Password of the image library used to authenticate the camera.
	Target-person association	Indicates whether to associate target images with related person images.
	Upper-level NVR association	Indicates whether to allow you to search for recordings from a camera based on the associated NVR device. If this parameter is selected, the camera reports the NVR ID when registering with the GA/T 1400 VIID.
	NVR number	ID used by the camera to register with the GA/T 1400 VIID.
	Baoshan Local Standard	Indicates whether to report information based on the requirements defined in the Baoshan local standard.

6. (Optional) Click **OK**.
7. Click **Save**.

Parent topic: Setting Second Protocol Parameters

Configuring Connection to the Platform Through RESTful

This section describes how to connect a camera to the IVS platform through the RESTful protocol.

The RESTful protocol is a network device management protocol based on the RESTful architecture.

Prerequisites

The RESTful protocol uses the HTTPS transmission protocol by default. Therefore, the client must also support the HTTPS protocol. If the client supports only the HTTP protocol, you need to set **RESTful transmission protocol** to **HTTP/HTTPS** on the camera side. If the transmission protocol on the camera is different from that on the client, connection will fail.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Choose **Second Protocol Parameters** > **RESTful**. The **RESTful** tab page is displayed, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 RESTful tab page

   Table 1 RESTful parameters

Parameter	Description
Transmission protocol	• **HTTPS**: Data is transmitted through HTTPS.

Parameter	Description
	• **HTTP/HTTPS**: Data is transmitted through HTTP or HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Authentication mode	Select an authentication algorithm supported by the invoker. • **Digest_MD5**: Only the Digest_MD5 authentication method is supported. • **Digest_SHA256**: Only the Digest_SHA256 authentication method is supported. • **Digest_MD5/Digest_SHA256**: Both Digest_MD5 and Digest_SHA256 authentication methods are supported. **NOTE:** The Digest_MD5 authentication method may cause security risks. Therefore, exercise caution when using this method.
NAT	Indicates whether to enable NAT. This parameter is optional. If **NAT** is selected, you need to set the NAT network address, user name, and password. **NOTE:** • If NAT is required for connecting the camera to the platform, set related NAT parameters. • The camera supports the Digest_MD5 and Digest_SHA256 authentication methods. The Digest_MD5 authentication method has security risks. Therefore, exercise caution when using Digest_MD5.

Parameter	Description
URL	Platform URL. Set this parameter to **http://*IP address:port number/xxx*** or **https://*IP address:port number/xxx***, for example, **http://10.3.4.55:98/nat**.
User name	User name set for NAT translation.
Password	Password set for NAT translation. This parameter is optional.

NOTE

Identity authentication is required when you connect a camera to the platform through the RESTful protocol. For details about how to change the RESTful (that is, the northbound interface) password, see Configuring Password Management.

Parent topic: Setting Second Protocol Parameters

Configuring Connection to the Platform Through RTSP

RTSP is an application-level protocol for the controls, such as play, pause, and fast-forward, of real-time streaming data.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Choose **Second Protocol Parameters** > **RTSP**. The **RTSP** tab page is displayed, as shown in Figure 1. Table 1 describes the options for the **RTSP authentication mode** parameter.

   Figure 1 RTSP tab page

   Table 1 Options for RTSP authentication

Option	Description
Digest_MD5	Digest authentication with MD5 encryption. This authentication method may cause security risks. Exercise caution when using it.
Digest_SHA256	Digest authentication with SHA256 encryption.
None	Security risks may exist when you select **None**. It is recommended that this authentication method be enabled only when the platform does not support authentication. If **None** is selected, the system does not perform authentication if you request live video through the RTSP or ONVIF protocol.

> **NOTE**
>
> The RTSP protocol is enabled by default. You can select the required authentication method during configuration.

Parent topic: Setting Second Protocol Parameters

Configuring Password Management

To ensure data security, change the passwords of platform connection protocols timely. After the passwords are changed, record and save them.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
3. Click **Password Management**. Under **Password Management**, you can change the SDK, northbound interface, and ONVIF passwords.
4. Use SDK password management as an example. Click the **SDK Password** tab. The **SDK Password** tab page is displayed, as shown in Figure 1.

   Figure 1 SDK Password tab page

5. Set **Web user password**, **New password**, and **Confirm password**.
   - The value of **Web user password** is the password of the **admin** user for logging in to the camera.

- The value of **Confirm password** must be the same as that of **New password**.

> **NOTE**
>
> - For security purposes, you are advised to periodically (every 90 days recommended) change the password and ensure that the password is not used repeatedly.
> - For security purposes, you are advised not to set the new password to a weak password. To configure a weak password dictionary, choose **Configuration** > **System** > **Security Management** > **Password Management** > **Weak Password Dictionary**.

6. Click **Save**.

Parent topic: Configuring Network Platform Connection

Configuring Cloud Service Connection

After a camera is connected to the cloud service, you can view live and recorded video from the camera on your mobile app. The capabilities supported vary between camera models.

After installing the mobile app, you should read through the privacy policy and user agreement on the app.

The hardware serial number (SN) and verification code are used to verify the camera to be added to the app. Figure 1 describes how to obtain the hardware SN and verification code in the camera web system.

Configuring Connection This section describes how to connect a camera to a mobile app through the cloud service.

Configuring a Certificate
This section describes how to configure and manage cloud service certificates.

Unbinding a Camera
This section describes how to unbind a camera from a mobile app.

Parent topic: Configuring Network Platform Connection

Configuring Connection

This section describes how to connect a camera to a mobile app through the cloud service.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed. Then click **Cloud Service**.

   The parameters displayed on the web page vary between camera models.

   Figure 1 Cloud Service area

   Table 1 Parameter description

Parameter	Description
Cloud service connection	Indicates whether to enable cloud service connection. After this function is enabled, you can add the camera to the mobile app. **NOTE:** To add a camera on the mobile app, you need to first select a country or region.

Parameter	Description
Cloud service time calibration	Indicates whether to synchronize the time of the camera with that of the cloud service. If another time synchronization method is used to calibrate the camera time on the network, a conflict will occur after this function is enabled.
Hardware SN	Camera serial number.
Verification code	Used to verify the camera when you connect the camera to the Cloud Service. After the verification code is changed, the QR code on the camera body will become invalid. In this case, you can manually add the camera using the hardware SN or scan the QR code in the camera web system.
Domain name	IP address and port number of the server connected to the Cloud Service. You can use the default value when you add the camera to the mobile app. **NOTE:** If the domain name of the cloud service is not an IP address, configure the primary DNS server in Setting Camera IP Addresses.
Scan QR code for connection (recommended)	QR code for adding the camera to the mobile app.
Binding status	Binding status. After the camera is added to the mobile app, you can click **Refresh** to display information about the app user. If the camera is not added to the mobile app, the message "The device is not bound." is displayed.
User name	Name of the app user.
Phone number	Phone number of the app user.
Email	Email address of the app user.

Parent topic: Configuring Cloud Service Connection

Configuring a Certificate

This section describes how to configure and manage cloud service certificates.

The validity period of a certificate is defined by each certificate authority (CA) when the certificate issuer is being set.

The certificate revocation list (CRL) is used to prevent network security problems caused by private certificate key leakage. Certificates in the CRL are not secure.

Cameras support cloud service certificate revocation. For security purposes, cameras cannot connect to platforms that use certificates in the CRL.

Context

Certificates should be purchased from an authoritative third-party certification organization or be obtained by establishing a CA server.

A CRL is a data file that lists the serial numbers and revocation dates of certificates that are revoked by the CA.

Cloud Service Certificate Management

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed. Then click **Cloud Service**. The parameters displayed on the web page vary between camera models.
3. Click **Set Certificate**. In the dialog box that is displayed, complete settings in the **Cloud Service Certificate** area, as shown in Figure 1. Table 1 describes the parameters and buttons.

Figure 1 Cloud Service Certificate area

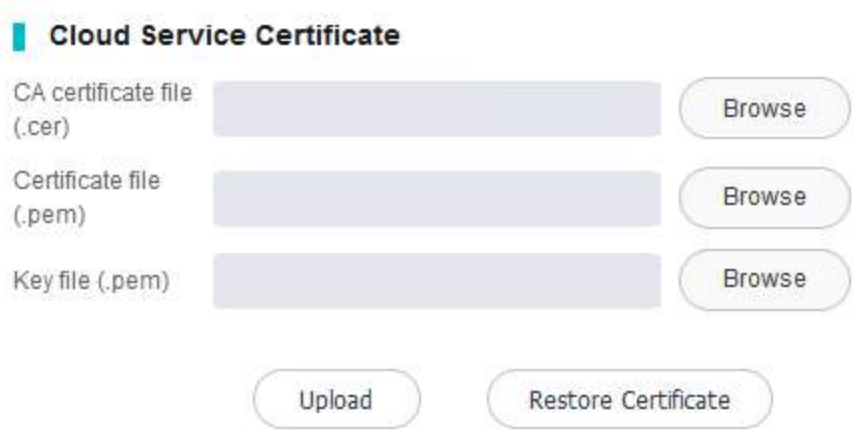


Table 1 Certificate management parameters and buttons

Parameter/Button	Description
CA certificate file (.cer)	CA certificate.
Certificate file (.pem)	Digital information file that identifies and verifies both parties involved in network communication.
Key file (.pem)	Key file that contains the certificate key (*xxx*_key.pem).
Restore Certificate	Button for restoring the certificate to the default one.

You can use your own certificate file in the following way: Click **Browse**, select your desired file path, and click **Upload**. In the dialog box that is displayed, enter the password of the private key file to upload the certificate.

NOTE

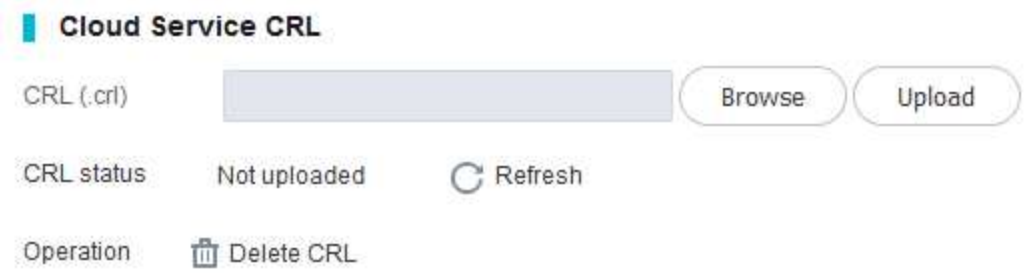
- Only certificate files in **.pem** format can be uploaded.
- The password of the private key file must be the same as that generated when you apply for the private key file.

- If you click **Restore Certificate**, the system displays a dialog box asking you whether to restore the certificate to the default one.

Cloud Service CRL Management

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed. Then click **Cloud Service**. The parameters displayed on the web page vary between camera models.
3. Click **Set Certificate**. In the dialog box that is displayed, complete settings in the **Cloud Service CRL** area, as shown in Figure 2.

   Figure 2 Cloud Service CRL area

4. Click **Browse**, select the CRL to be uploaded, and click **Upload**.

   If the CRL file uploaded is normal, **Normal** is displayed in the CRL list. If the CRL file uploaded has expired, **Expired** is displayed in the CRL list. If the format of the CRL file to be uploaded is incorrect, an error message is displayed.
5. (Optional) Click **Refresh** if the status in the CRL list is not displayed.
6. (Optional) Click **Delete** to delete an uploaded CRL.

Parent topic: Configuring Cloud Service Connection

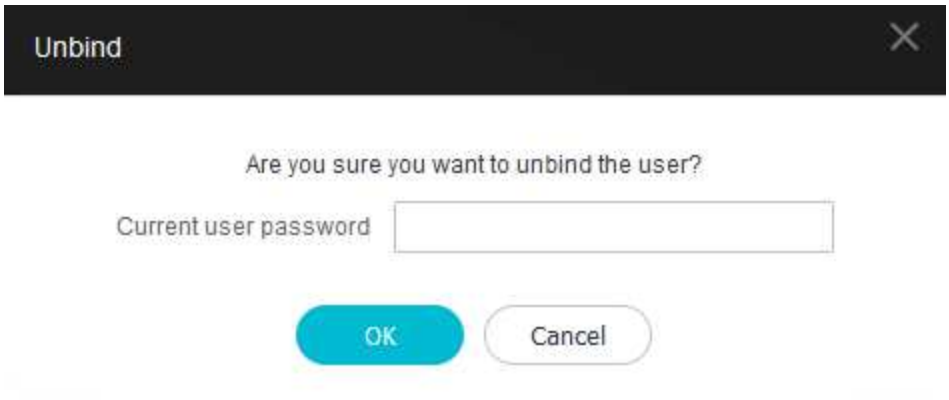
Unbinding a Camera

This section describes how to unbind a camera from a mobile app.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed. Then click **Cloud Service**. The parameters displayed on the web page vary between camera models.
3. Click **Unbind**. The **Forcible unbinding** dialog box shown in Figure 1 is displayed. Only some camera models support this function.

   Figure 1 Forcible unbinding dialog box

4. Enter the current user password and click **OK** to unbind a camera from the mobile app.

NOTE

- Only the administrator has the permission to unbind devices.
- You need to enter the password of the administrator to perform this operation.

- If the camera is not bound to or is displayed as offline on the mobile app, the **Unbind** button is unavailable.
- The binding status is automatically updated each time you enter the **Cloud Service** page.

Parent topic: Configuring Cloud Service Connection

Local Parameters

You can set local parameters, such as the protocol type, code stream type, video stream type, and path where snapshots are saved. These settings take effect only on the local computer.

Setting Playing Parameters This section describes how to set playing parameters, including the protocol, stream type, and video stream type.

Setting Recording File Parameters
This section describes how to configure the path for storing recording files.

Setting Snapshot File Parameters
This section describes how to configure the path for storing snapshot files and the file storage size.

Parent topic: Configuration

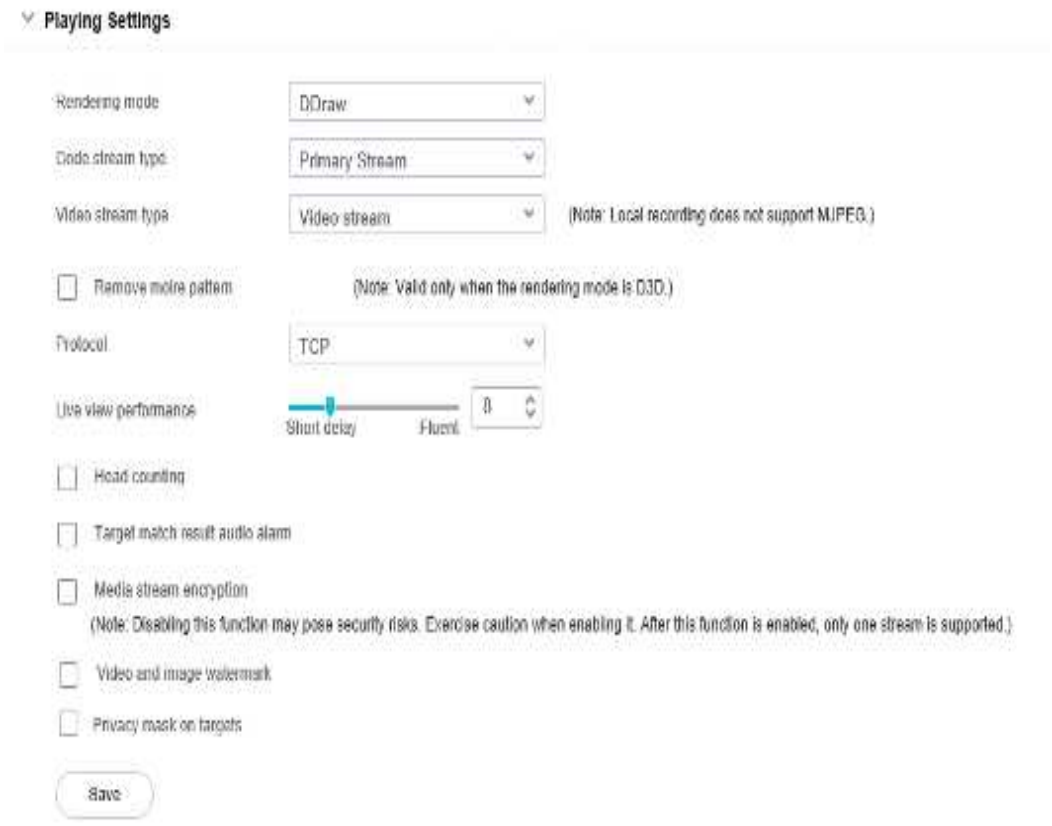
Setting Playing Parameters

This section describes how to set playing parameters, including the protocol, stream type, and video stream type.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Playing Settings**. The **Playing Settings** area is displayed, as shown in Figure 1. The parameters displayed in this area vary between camera models.

   Figure 1 Playing Settings area



3. Set playing parameters. Table 1 describes the parameters.

   Table 1 Playing parameters

Parameter	Description
Rendering mode	Mode for rendering live video. The options are as follows: • **DDraw**: This value is recommended when the video card version is too early or live video cannot be displayed in D3D mode. • **D3D**: This value is recommended for Internet Explorer 9 or a later version.
Remove moire pattern	Indicates whether to remove moiré patterns. If this function is enabled, moiré patterns on the image will be dramatically reduced. **NOTE:** • This function takes effect only when the rendering mode is D3D. • This function takes effect only when an integrated video card that supports hardware decoding of video in the current resolution is used.
Protocol	Type of the network transmission protocol. **NOTE:** Local video streams support TCP (default) and UDP.
Code stream type	Type of code streams for locally requested video streams.
Video stream type	Video stream type. The options are as follows: • **Video stream**: indicates output of only video streams. • **Hybrid stream**: indicates output of both video and audio streams.

Parameter	Description
	NOTE: Predefined detection areas for behavior analysis can be displayed on live video images only when **Video stream type** is set to **Hybrid stream**.
Live view performance	Live video performance. The value ranges from 1 to 30 (default value: 8). A larger value indicates smoother video. • **Short delay**: The image delay is small and the PTZ response is fast. However, image freezing may occur sometimes. • **Fluent**: There are many live video buffers. This option applies to scenarios that pose high requirements on live video smoothness. If the network conditions are poor or the detection scenario is complex and image stuttering occurs, you can increase the value to ensure smooth video images.
Head counting	If you select **Head counting** and enable real-time image capture under **Display** > **Object Classification**, the number of detected targets will be displayed on the live video image. **NOTE:** This parameter is available only when the target capture function is enabled.
Target match result audio alarm	If you select **Target match result audio alarm** and enable real-time image capture under **Display** > **Object Classification**, target recognition sound alarms can be generated.
Media stream	If you select **Media stream encryption**, the media streams, recordings, and snapshots are

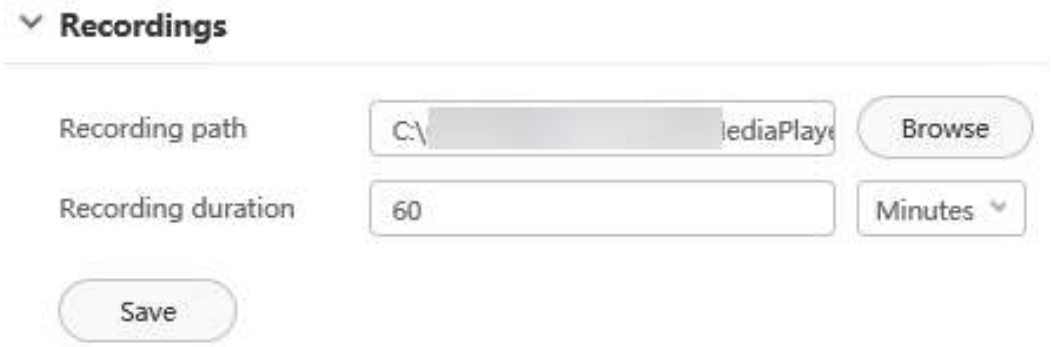
Setting Recording File Parameters

This section describes how to configure the path for storing recording files.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Recordings**. The **Recordings** area is displayed, as shown in Figure 1.

   Figure 1 Recordings area

3. Set recording file parameters. Table 1 describes the parameters.

   Table 1 Recording file parameters

Parameter	Description
Recording path	Path for saving recording files. To set a save path, click **Browse** and select a path.
Recording duration	Duration of video recorded on the **View** page. The value ranges from 5s to 24 hours. You can select a time unit from the drop-down list box next to the **Recording duration** text box.

4. Click **Save**.

Parent topic: Local Parameters

Setting Snapshot File Parameters

This section describes how to configure the path for storing snapshot files and the file storage size.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Snapshots**. The **Snapshots** area is displayed, as shown in Figure 1.

   Figure 1 Snapshots area

3. Set snapshot file parameters. Table 1 describes the parameters.

   Table 1 Snapshot file parameters

Parameter	Description
Manual snapshot save path	Path for saving snapshots captured during video viewing on the **View** page. To set a save path, click **Browse** and select a path.
File storage size	Size of local images captured in real time. To save the file storage size setting, click **Save**. **NOTE:** When the size of the local images captured in real time exceeds the value specified by **File storage size**, the earliest images will be deleted.

Parameter	Description
Intelligent snapshot save path	Path for saving images captured in real time. To set a save path, click **Browse** and select a path.

4. Click **Save**.

Parent topic: Local Parameters

Managing the System

This section describes how to configure system operations.

System Settings This section describes how to view basic system information and field of view (FoV) information and how to configure the system time.

System Maintenance
This section describes camera maintenance operations, for example, upgrading versions and algorithms, managing apps, viewing logs, and locating faults.

Security Management
This section describes how to manage camera passwords and certificates, configure IP address filtering, security options, static Address Resolution Protocol (ARP) rules, and password recovery, and manage users.

User Management
By level of rights, users are classified into three types: system administrator (**admin**), advanced operator, and common operator. Users can be added, modified, and deleted.

Parent topic: Configuration

System Settings

This section describes how to view basic system information and field of view (FoV) information and how to configure the system time.

Basic Information You can view the basic system information and lifecycle of a camera and configure the system language as required.

Time Configuration
You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

Field of View
On the **Field of View** tab page, you can set the camera installation height and location and query the camera sensor size and lens information.

Parent topic: Managing the System

Basic Information

You can view the basic system information and lifecycle of a camera and configure the system language as required.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Settings**.
3. Click the **Basic Information** tab to view basic system information. For details about the parameters, see Table 1, Table 2, Table 3, Table 4, and Table 5.

Table 1 Basic system information

Parameter	Description
Device model	Camera model.
Hardware ID	Unique ID of the camera software and hardware system.
Physical address (ETHO)	MAC address of a camera.
CPU usage	Current CPU usage.
Available memory (MB)	Available memory size.
Buffer (MB)	Buffer memory size.
Cache(MB)	Cache memory size.
Reception rate (bit/s)	Current network data reception rate.
Secure boot status	• If the **Normal** state is displayed, all modules are successfully verified. • If the **Abnormal** state is displayed, one or more modules fail to be verified.

Parameter	Description
Total memory (MB)	Total memory size.
Transmission rate (bit/s)	Current network data transmission rate.

Table 2 Platform status

Parameter	Description
GB/T 28181	Platform registration status. The options are as follows: • **Online**: indicates that the camera has been registered with the video security platform. • **Offline**/**Offline-Disabled**: indicates that the camera is not registered with the video security platform. **NOTE:** The web page varies depending on the camera model.
GB/T 28181-2	
SDK Active-1	
SDK Active-2	
SDK Active-3	
GA/T 1400	
GA/T 1400-2	

Table 3 Media streams

Parameter	Description
No.	-
Type	Type of the current media stream (TCP unicast, UDP unicast, or UDP multicast).
Transmission Type	Transmission type of the current media stream (including the elementary stream and program stream). **NOTE:**

Parameter	Description
	• If the camera is registered with the platform using the ONVIF protocol or SDK, media streams are transmitted as elementary streams. • If the camera is registered with the platform using GB/T 28181, media streams are transmitted as program streams.
Status	Transmission status of the current media stream.
Require Keepalive	Indicates whether the current media stream requires the peer device to send keepalive packets to the camera.
Stream Type	Type of the current media stream transmitted by the camera. On the **View** page, click  to switch the stream type.
Service Type	Service type of the current media stream. The service types include live video viewing, voice intercom, recording download, and recording playback.
Encryption Type	Encryption type of the current media stream. You can enable or disable **Media stream encryption** under **Configuration** > **Local** > **Playing Settings**.

Parameter		Description
Unicast	IP Address	IP address for receiving video and audio streams.
	Audio Port	Port for receiving audio streams.
	Video Port	Port for receiving video streams.
	Intelligent Port	Port for receiving intelligent analysis data.
Multicast	IP Address	Multicast IP address for receiving video and audio streams.
	Audio Port	Multicast port for receiving audio streams.
	Video Port	Multicast port for receiving video streams.
	Intelligent Port	Multicast port for receiving intelligent analysis data.
Watermark		Indicates whether the watermark function is displayed. You can enable or disable the watermark function under **Configuration** > **Video/Audio** > **Video**.

NOTE

- The unicast mode is efficient and targeted, but may result in high loads on the camera.
- The multicast mode reduces the camera loads but does not provide error correction mechanism.

Table 4 Structured information system language

Parameter		Description
Language type	Simplified Chinese	Language for naming images to be uploaded to the FTP server and paths for storing images. Language of text superimposed on captured images such as target and vehicle images. Language of optimization suggestions returned by the image quality diagnosis function. Language of service configuration information returned by the intelligent service fault locating function.
	English	

Table 5 Lifecycle

Parameter		Description
Service Info	Start time	Start time for using the camera.
	Service life (months)	Service life of the camera.

Time Configuration

You can directly set the camera time or set Network Time Protocol (NTP) parameters to time-synchronize the camera with the NTP server in the network.

NOTICE

If you change the system time when the camera is recording video, the recording file will be corrupted. Therefore, do not change the system time during video recording.

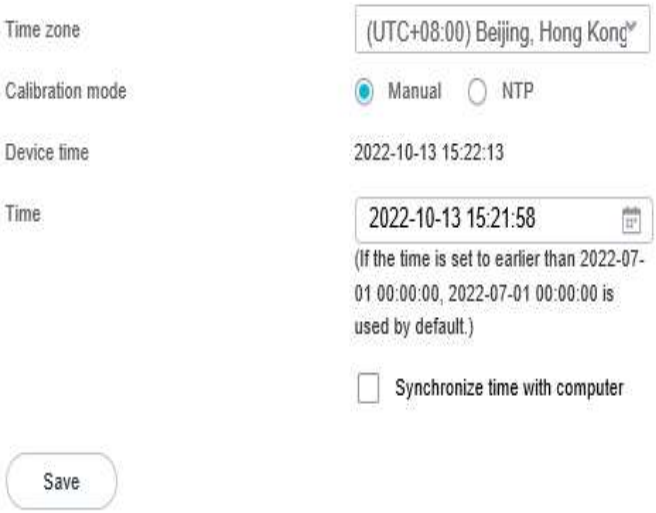
For models that support 1 + N, after the system time and DST of the primary camera are changed, the setting is automatically synchronized to the secondary cameras. After the system time and DST of a secondary camera are changed, the setting is not synchronized to the primary camera.

Configuring the System Time

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Settings** > **Time** and configure the system time, as shown in Figure 1.

   The web page varies depending on the camera model.

Figure 1 Time tab page



a. Select a time zone from the **Time zone** drop-down list box.

b. Select a time calibration mode and set related parameters. Table 1 describes the parameters.

NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- To enable NTP time calibration, first ensure that **Time zone** is correctly set in manual time calibration mode.
- The following time calibration modes are available: manual and NTP. In manual mode, you can directly set the time. In NTP mode, you need to configure the NTP server to time-synchronize the camera with the NTP server.

Table 1 Time calibration modes

Parameter	Setting
Manual	1. Click **Manual**. 2. Click the **Time** text box. The dialog box for setting the date and time is displayed.

Parameter	Setting
	3. Set the date and time and click **OK**. The system returns to the time setting page. **NOTE:** To time-synchronize the camera with the computer, click **Synchronize time with computer**.
NTP	1. Click **NTP**. 2. Set the NTP server IP address or domain name as prompted. Set the interval for time-synchronizing the camera with the NTP server. Then the camera synchronizes time with the NTP server at the specified interval. **NOTE:** • You can click Check to check whether the NTP server IP address is available.

3. Click **Save**.

Configuring Daylight Saving Time

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Settings** > **Time** and configure the daylight saving time (DST), as shown in Figure 2.

Figure 2 Configuring the DST



3. Configure the DST.

    a. Select **Enable DST**.

    b. Select **Week** or **Date** as required. If neither option is selected, the DST settings cannot be saved.

    The **Week** mode indicates that the DST is set by week. The **Date** mode indicates that the DST is set by date.

    c. Set **Start time**, **End time**, and **Time offset** of the DST based on regulations specified in the local laws.

    Table 2 describes the DST parameters.

    Table 2 Parameter description

Parameter	Description
Week	Indicates that the DST is set by week.
Date	Indicates that the DST is set by date.
Start time	Time for enabling the DST.
End time	Time for disabling the DST.
Time offset	Lead time during the DST, in minutes. If this parameter is set to **30 min**, the DST is 30 minutes earlier.

> **NOTE**
>
> If the local laws regulate that DST must be used, you must set DST based on the regulations specified in the local laws.

4. Click **Save**.

Parent topic: System Settings

Field of View

On the **Field of View** tab page, you can set the camera installation height and location and query the camera sensor size and lens information.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Settings** > **Field of View**.
3. Click the corresponding tabs and set the camera installation height, longitude, and latitude. Table 1 describes the FoV information.

   Table 1 FoV information

Item	Description
Installation Info	You can set the camera installation height in this area.
Sensor Size	You can query the camera sensor size, including the horizontal size and vertical size in this area.
Position	You can set the camera longitude, latitude, azimuth, and pitch in this area. The azimuth refers to the angle between the camera's shooting direction and the truth north direction of the Earth's magnetic field.
Lens Info	Used to query the camera lens information, including the optical zoom ratio, digital zoom ratio, horizontal field of view, and vertical field of view.

Parent topic: System Settings

System Maintenance

This section describes camera maintenance operations, for example, upgrading versions and algorithms, managing apps, viewing logs, and locating faults.

Upgrade

Maintenance
This section describes how to manage camera configuration files, restore cameras to default settings, and restart cameras.

Logs
This section describes how to query, collect, and periodically upload camera logs.

Camera Self-Check
Only zoom cameras support self-check. You can allow the camera to automatically check functions such as PTZ controls.

Service Fault Locating
This section describes image quality diagnosis, intelligent service fault locating, and video service status detection for cameras.

Anti-Counterfeit Code Check
This function is available for cameras that support motor vehicle detection. You can use the anti-counterfeit code to verify snapshots to judge whether they have been tampered with.

加热控制

Parent topic: Managing the System

Upgrade

Upgrading the Camera Version/Algorithms You can upgrade a camera or algorithms of a camera.

Managing Apps
After purchasing a camera, you can develop third-party apps based on the camera software platform and install third-party apps on the camera.

Parent topic: System Maintenance

Upgrading the Camera Version/Algorithms

You can upgrade a camera or algorithms of a camera.

Algorithm packages are different from a software upgrade package, and they are independent of each other. An algorithm package is applicable only to the algorithm of a specific intelligent function.

NOTICE

- The upgrade duration is less than 5 minutes (excluding the restart time) if a maximum of one channel of video streams is enabled.
- Generally, if the software version is upgraded, the algorithms also need to be upgraded. Upgrade the software package before upgrading the algorithm packages.
- You are advised to perform the upgrade when few or no users are online. During the upgrade, do not disconnect the power supply or network cable or perform other operations.
- After the upgrade is complete, you are advised to clear the browser cache before the next login.
- The falling object detection algorithm is a third-party algorithm and is available only for camera models whose name contains **Up**. Before upgrading and using a third-party algorithm, uninstall in-house algorithms other than the **image-alg** algorithm and restart the device.
- The algorithm configuration page is displayed 5–10s after the third-party algorithm is installed.
- To use the web plug-in of the latest version, install the image algorithm package.

Prerequisites

You have obtained the upgrade package.

NOTE

- The product software package contains software packages or algorithm packages of different functions. For details about the algorithm package to be downloaded for an algorithm, see the *Upgrade Guide*.

Table 1 describes the functions and licenses of algorithm packages.

Table 1 Algorithm function and license description

Algorithm	Algorithm Package	Function	Whether a License Is Required
Image algorithm	SDC-*ZZZ_XXX*_image-alg.bin	Adjusts image parameters to adapt to special scenes. Currently, overcast adaptation and backlight adaptation are supported. The scene adaptation type varies depending on the camera model.	No
Perimeter detection (behavior analysis)	SDC-*ZZZ_XXX*_beh.bin	Performs perimeter detection.	No
Object classification	SDC-*ZZZ_XXX*_vhd.bin	Recognizes motor vehicles, non-motorized vehicles, and pedestrians in images for general-purpose intelligent cameras; provides vehicle event detection, traffic flow statistics, and traffic violation detection functions (applies to license plates from the Chinese mainland). The specific functions may vary depending on the camera model.	No
Target recognition	SDC-*ZZZ_XXX*_face-rec.bin	Applies to target recognition cameras and general-purpose intelligent cameras to perform target detection, capture, and recognition.	No
Target identification 2.0	SDC-*ZZZ_XXX*_face-rec-v2.bin	Applies to target recognition cameras and general-purpose intelligent cameras to perform	No

Algorithm	Algorithm Package	Function	Whether a License Is Required
		target detection, capture, and recognition.	
Target and person detection	SDC-*ZZZ_XXX*_facedt-dl.bin	Applies to target capture cameras and general-purpose intelligent cameras to detect targets and persons.	No
Target detection (lightweight)	SDC-*ZZZ_XXX*_facedt-Lite.bin	Applies to target capture cameras and general-purpose intelligent cameras to detect and capture targets.	No
Crowd density/Queue length detection	SDC-*ZZZ_XXX*_Qlen-CrowdCnt.bin	Detects crowd density in a specified area, and counts people in a queue in a specified area.	No
Detection of electric bikes in elevators or corridors	SDC-*ZZZ_XXX*_emie.bin	Detects electric bikes that enter elevators or corridors.	No

NOTE

In the algorithm package name, *ZZZ* indicates the primary processor type, and *XXX* indicates the version number.

For example, **SDC-M19_*XXX*_beh.bin** indicates that the algorithm package applies to devices whose primary processor type is Hi3519A V100.

Upgrading the Camera Version/Algorithms

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Upgrade**.

   The upgrade tab page is displayed, as shown in Figure 1. Software packages, algorithm packages and their version numbers are displayed on the page.

The web page varies depending on the camera model. Select the upgrade file as prompted.

Figure 1 Upgrade tab page



3. Click **Browse** and select the upgrade package.
   - .bin algorithm package: Select the .bin package to be installed and click **Upgrade**.
   - .zip full upgrade package: Select the .zip package of the corresponding model and click **Upgrade**.

     The **Upgrade File** dialog box is displayed, as shown in Figure 2. Select the algorithm to be upgraded and click **Upgrade**.
   - .tar third-party algorithm package: Select the .tar package to be installed and click **Upgrade**.

     In the **Confirm** dialog box that is displayed, toggle on **Resource allocation** and click **Upgrade**, as shown in Figure 3.

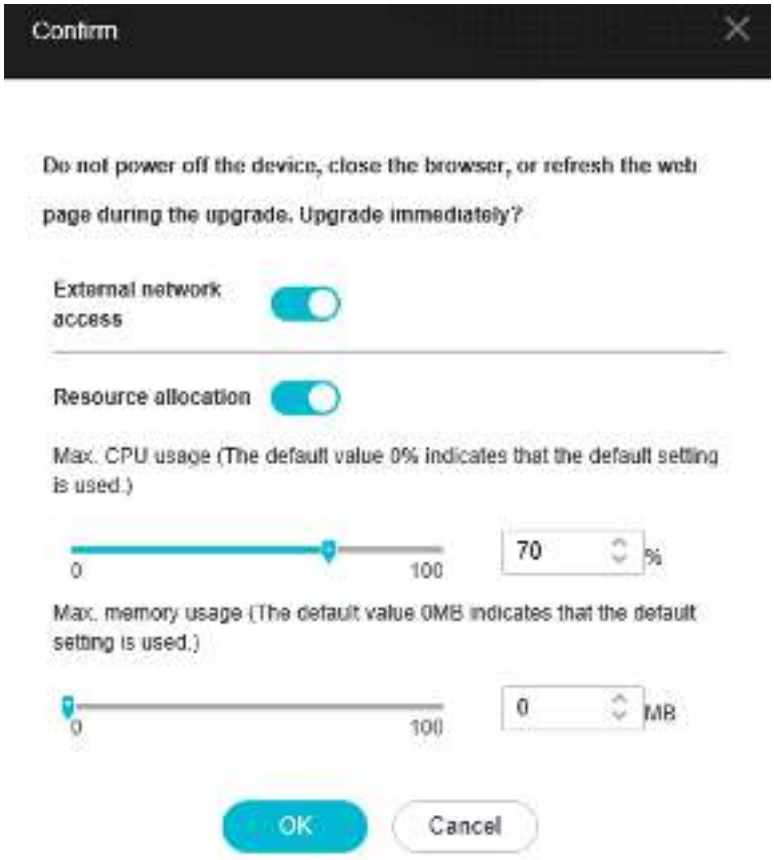
     NOTE

     - The path for storing ZIP packages can contain a maximum of 260 characters.
     - You cannot install a ZIP package for a camera on multiple tab pages under a web browser at the same time.
     - If a message is displayed during ZIP package installation, perform operations as prompted.
     - When installing a .tar algorithm package, you can toggle on **External network access** to grant the network access permission to the algorithm.

Figure 2 Upgrade File dialog box



Figure 3 Confirm dialog box



NOTE

- Trustlisted version check is used to verify the current camera version. If the camera cannot be upgraded to the target version, the system displays a message indicating that the verification fails. This function is enabled by default. You are advised not to disable it.

4. Click **OK**.

   When the upgrade is complete, the system displays a message indicating that the upgrade is successful.

Uninstalling Algorithm Packages

You can uninstall an algorithm package in either of the following ways:

1. You can uninstall an algorithm package in the camera web system. After the uninstallation, all web pages related to intelligent services, such as web pages under **Intelligence**, are hidden.
2. You can invoke the RESTful API to uninstall an algorithm package. After the uninstallation, all web pages related to intelligent services will be hidden only after you refresh the web page or re-log in to the camera web system.

To uninstall an algorithm package in the camera web system, perform the following operations:

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Upgrade** > **Algorithm**.
3. Click **Clear All**. The system clears all algorithm packages except the image algorithm package.

   After the deletion, web pages related to intelligent services will be hidden. After algorithm packages are uploaded again, web pages related to intelligent services will be displayed again.

Parent topic: Upgrade

Managing Apps

After purchasing a camera, you can develop third-party apps based on the camera software platform and install third-party apps on the camera.

The capabilities supported vary between camera models.

Prerequisites

You have inserted an SD card into the camera before installing an app. If no SD card is inserted, the app may fail to be installed due to insufficient camera flash memory. After an SD card is inserted, if the camera flash memory is insufficient and the SD card is normal, the app is installed on the SD card.

Obtaining an App

- Before installing a third-party app, obtain related software packages first.
- When installing a third-party app, install the TAR file of the app and then the **license.lic.tar** file. You can install apps under **System Maintenance** > **Upgrade**.

NOTE

- The apps that can be installed vary depending on the camera model. For example, **its_app** can be installed only on ITS cameras.
- If multiple third-party algorithms are enabled for a camera at the same time, the third-party algorithms may become invalid. In this case, restart the camera and reinstall the required algorithm. You are advised to enable one third-party algorithm for a camera at a time.
- From 11.0.0.SPC200, the mechanism for detecting the flash program/erase (P/E) cycles is added to the app. If the number of

P/E cycles exceeds 168 within seven days, the app stops running and the message "Stopped (exception caused by too many P/E cycles)" is displayed in the **Status** column in the **App** area.

Table 1 App function and license description

App	App Package	Function	Whether a License Is Required
Video-based vehicle detector platform	SDC-*ZZZ_XXX*_TXProcess_*YYY*.rpm.tar	Connects to a video-based vehicle detector platform. **NOTE:** The software package of the video-based vehicle detector platform must be of the same version as the camera software. Otherwise, the software package is unavailable.	No
GA/T 1400	SDC-*ZZZ_XXX*_GAT1400_*YYY*.rpm.tar	Applies to cameras that	No

App	App Package	Function	Whether a License Is Required
protocol		support the GA/T 1400 protocol to set platform connection parameters. **NOTE:** • After the GA/T 1400 protocol is installed, it is not displayed as an app. Instead, the original web tab page is updated. • This app has been preset in the basic software package and does	

App	App Package	Function	Whether a License Is Required
		not need to be installed again.	
GB/T 28181 protocol	SDC-*ZZZ_XXX*_GB28181_*YYY*.rpm.tar	Applies to cameras that support the GB/T 28181 protocol to set platform connection parameters. **NOTE:** • After the GB/T 28181 protocol is installed, it is not displayed as an app. Instead, the original web tab page is updated.	No

App	App Package	Function	Whether a License Is Required
		• This app has been preset in the basic software package and does not need to be installed again.	
e-Surfing Vision platform	SDC-*ZZZ_XXX*_TYSL_*YYY*.rpm.tar	Allows you to set platform connection parameters such as the platform IP address to connect to the e-Surfing Vision platform.	No

NOTE

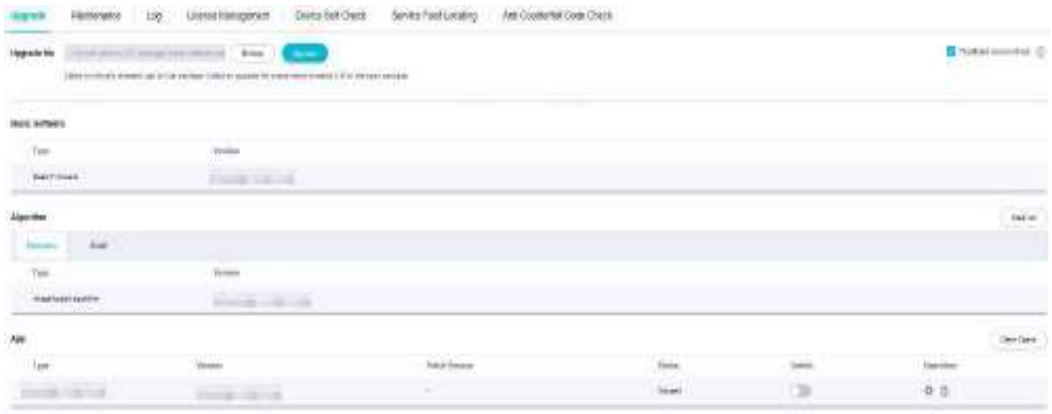
In the app package name, *ZZZ* indicates the primary processor type, *XXX* indicates the version number, and *YYY* indicates the processor architecture type.

For example, **SDC-M19_*XXX*_TXProcess_*YYY*.rpm.tar** indicates that the app package applies to devices whose processor type is Hi3519A V100.

Installation Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Upgrade**. The **Upgrade** tab page is displayed, as shown in Figure 1.

   Figure 1 Upgrade

   NOTE

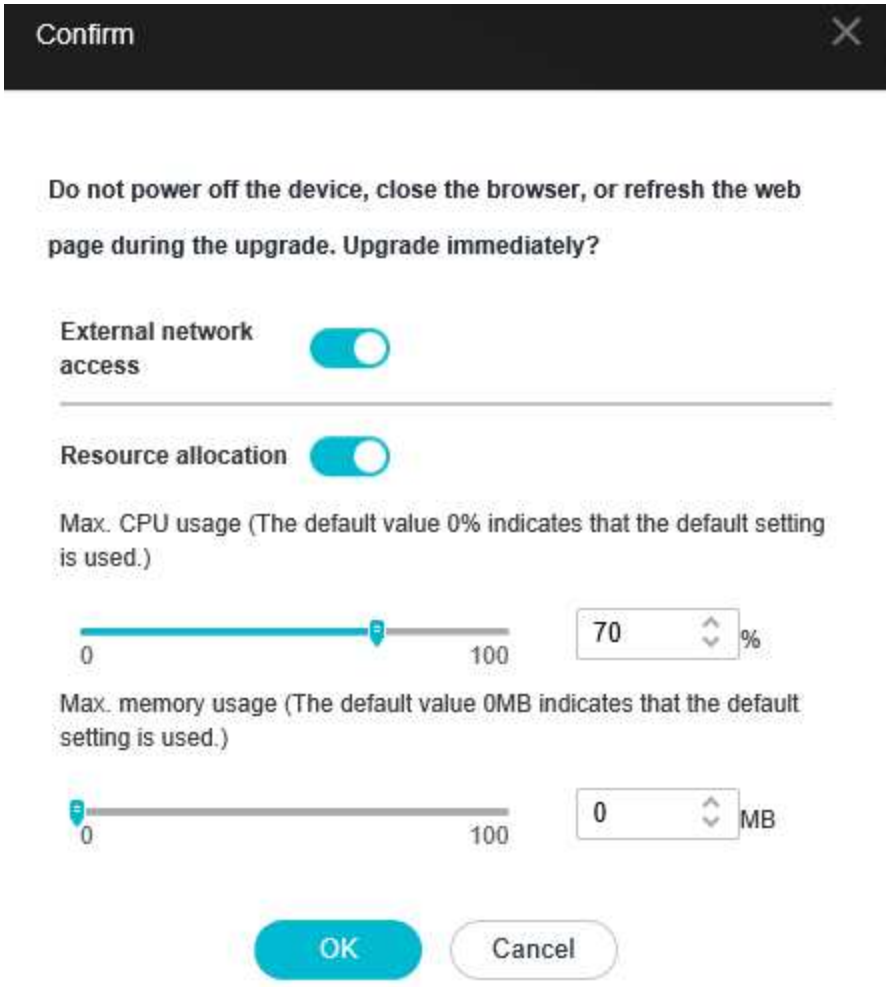
   Before installing a third-party algorithm, you need to perform the following steps to ensure that the algorithm can be properly installed or used in case of insufficient space:

   - Click **Clear Space** to delete non-required algorithms and apps from the camera's flash memory to ensure that sufficient flash space is reserved for installation.
   - Select an unnecessary third-party app and click to delete it.

3. Click **Browse** and select a local app file.
4. Click **Upgrade**.

5. Toggle on **Resource allocation** and set **Max. CPU usage** and **Max. memory usage**.

Figure 2 Configuring resource allocation



NOTE

- If an app file is installed for the first time and **Max. CPU usage** or **Max. memory usage** is set to **0**, the maximum CPU or memory usage in the configuration file of the app is used (or the maximum CPU or memory usage is not limited if the maximum CPU or memory usage is not configured in the configuration file). Exercise caution when

setting **Max. CPU usage** and **Max. memory usage** to avoid affecting app running.

- If an app file of the same name but a different version is installed to overwrite the original app file and **Max. CPU usage** or **Max. memory usage** is set to **0**, the maximum CPU or memory usage in the original file is used.
- When installing a third-party app, you can toggle on **External network access** to grant the network access permission to the app.

6. Click **OK** to install the app file.
7. Toggle on the button in the **Switch** column to enable the installed app.

Parent topic: Upgrade

Maintenance

This section describes how to manage camera configuration files, restore cameras to default settings, and restart cameras.

Managing Configuration Files

Through configuration file management, you can save configurations of the current camera and copy them to other cameras in batches.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Maintenance** > **Configuration File**.

   The **Configuration File** area is displayed, as shown in Figure 1.

   Figure 1 Configuration File area

3. Set parameters in the **Configuration File** area. Table 1 describes the parameters.

   Table 1 Configuration file parameters

Parameter	Description	Setting
Download	You can download the current configuration file to save device parameters. If necessary, you can	1. Click **Download**. 2. Enter the file password in the dialog box that is displayed.

Parameter	Description	Setting
	upload the configuration file again to restore the device parameters.	**NOTE:** • The downloaded configuration file does not contain configurations such as storage encryption, target match, privacy authorization, and feature-based collaboration settings. • The configuration file encryption password is used to generate the working key during encryption. • Use the download function of the browser. • If the download fails, go to the **Internet Options** page of Internet Explorer, click **Advanced**, and click **Reset**. Then, download the configuration file again.
Upload **NOTICE:**	You can upload the configuration file	1. Click **Browse** and select the

Parameter	Description	Setting
The version of the configuration file to upload must be the same as the current device version. Otherwise, the configuration may be lost.	stored on the local computer. **NOTE:** You need to set ISP parameters and platform registration parameters in the configuration file as required and then upload the configuration file, or you can first upload the configuration file and modify the parameter settings on the web pages.	configuration file. 2. Click **Upload** and enter the password of the current login user. A dialog box is displayed, asking you to enter the configuration file password. 3. Enter the configuration file password and click **OK** to upload the configuration file. After the configuration file is uploaded, the camera automatically restarts. **CAUTION:** Ensure that the configuration file meets the following requirements. Otherwise, the configuration file may fail to be uploaded.

Parameter	Description	Setting
		• The password of the configuration file must be the same as that set when the configuration file is downloaded. • Only configuration files of cameras of the same model can be uploaded.

Restoring a Camera to Default Settings

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Maintenance** > **Restore**. The **Restore** area is displayed, as shown in Figure 2.

   Figure 2 Restore area

3. Click **Restore** or **Fully Restore** as required.

In the dialog box that is displayed, enter the password of the current user.

4. Click **OK**. The camera restarts.

Remotely Restarting a Camera

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Maintenance** > **Remote Restart**. The **Remote Restart** area is displayed, as shown in Figure 3.

   Figure 3 Remote Restart area

3. Click **Remote Restart**.

   The **Restart** dialog box is displayed.

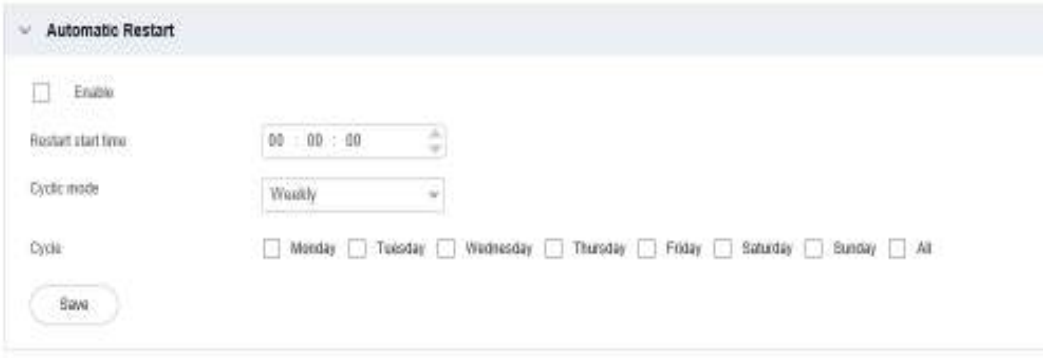
4. Click **OK**. The camera restarts.

Automatic Restart

If the camera runs for a long period of time, some exceptions may occur on the camera. In this case, you can rectify the faults through automatic camera restart. For example, if the camera's PTZ position deviates due to long-term running, you need to restart the camera to correct the PTZ position.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Maintenance** > **Automatic Restart**. The **Automatic Restart** area is displayed, as shown in Figure 4.

Figure 4 Automatic Restart area



3. Select **Enable** and set **Restart start time**, **Cyclic mode**, and **Cycle**.
4. Click **Save**.

Parent topic: System Maintenance

Logs

This section describes how to query, collect, and periodically upload camera logs.

Querying Logs Logs are the main information source for maintenance engineers to locate faults. They also serve as the basis for terminal users to collect fault information. When a fault occurs, maintenance engineers and terminal users can locate and rectify the fault by checking the log information.

Configuring Log Collection
This section describes how to collect logs through TCP and TLS.

Configuring Scheduled Log Upload
You can enable the scheduled log upload function when you want to continuously locate a fault. After the function is enabled, when the size of a log file (such as alarm, err, or syslog) reaches a specified value, the system automatically compresses the log file and uploads it to a specified server through SFTP to prevent the log file from being overwritten.

Parent topic: System Maintenance

Querying Logs

Logs are the main information source for maintenance engineers to locate faults. They also serve as the basis for terminal users to collect fault information. When a fault occurs, maintenance engineers and terminal users can locate and rectify the fault by checking the log information.

NOTE

You need to check the log capacity periodically. It is recommended that logs be backed up monthly.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Log**. The page shown in Figure 1 is displayed.

   Figure 1 Querying logs

3. Query logs.

   a. Expand the **Debug Log** area. Select a required module and click **OK**.

   b. Expand the **Log Query** area. Set the start time, end time, and log type for log query.

NOTE

- After **Language Setting** is set, only newly generated logs are displayed in the configured language.
- If you click **Reset**, the start time changes to 24 hours ago and the end time changes to the current time.

c. Click **Search**. The search results are displayed in the lower part of the page.

NOTE

To query the archived logs, use the **One-Click Collection** function to download more logs.

4. Download logs.

   Click **One-Click Collection** and download logs to your local computer. After logs are downloaded, you can view them using WordPad.

NOTE

- The default name of the log file downloaded through **One-Click Collection** is ***sysinfo.tar.gz**. If you want to change the file name, name it in ***.tar.gz** format. This function collects all logs saved by the camera, and is irrelevant to the log type, start time, and end time configured in the lower part of this page.
- For more information about logs, see Log Reference.
- If the download fails, go to the **Internet Options** page of Internet Explorer, click **Advanced**, and click **Reset**. Then, download the log file again.

Parent topic: Logs

Configuring Log Collection

This section describes how to collect logs through TCP and TLS.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Collection Configuration**. The **Log Collection Configuration** area is displayed, as shown in Figure 1. Table 1 describes the log collection parameters.

   Figure 1 Log Collection Configuration area



   Table 1 Log collection parameters

Parameter	Description
Enable log collection	After this parameter is selected, collected logs will be transferred to the platform. The logs that can be transferred include alarm logs, run logs (excluding GET logs), and SSH logs.
Protocol	The value can be **TCP** or **TLS**. **NOTE:** If **TLS** is selected, logs will be encrypted before being transferred. For security purposes, **TLS** is recommended.
IP Address	IP address of the platform.

Parameter	Description
Port number	Port number of the platform.
Certificate file (.pem/.cer)	CA certificate of the log collection server. The client uses the CA certificate to verify the validity of the server. **NOTE:** This parameter is available only when **Protocol** is set to **TLS**.

Log Collection Format

- **TCP mode**

The RFC 5424 Syslog standard is used. The log format is as follows:

```
SYSLOG-MSG  = HEADER SP STRUCTURED-DATA [SP MSG]
HEADER = PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID
```

Table 2 describes the log format.

Table 2 Log format in TCP mode

Parameter	Description
SP	Space character.
PRI	Log priority.
VERSION	Syslog version number.
TIMESTAMP	Timestamp.
HOSTNAME	Host name.
APP-NAME	Application name.
PROCID	Process name or ID.
MSGID	Message ID.
STRUCTURED-DATA	Structured data.
MSG	Message body, which is optional.

- **TLS mode**

The RFC 5425 Syslog standard is used. The log format is as follows:

```
SYSLOG-FRAME = MSG-LEN SP SYSLOG-MSG
```

The following describes the log format:

- MSG-LEN: length of SYSLOG-MSG.
- SYSLOG-MSG uses the TCP mode and complies with the RFC 5424 standard. For details, see Table 2.
- **Log reporting range**

1. Alarm log
2. Run logs except for GET logs
3. SSH log

NOTE

- Language of alarm logs and run logs except for GET logs supports Chinese and English currently, which must be the same as the log language set in Querying Logs.
- Language of SSH logs supports only English.
- For details about log types, see Log Classification.
- Some types of logs contain user information, for example, run logs. Example: RUN| 2018/01/15 14:37:47:395| NOTICE:WEB[admin] [192.168.20.160:39141] Get Alarm Linkage Policy Successfully. DeviceId: 201, AlarmType: 1, CameraNum: 1, DoNum: 0. For details, see Log Description.

Parent topic: Logs

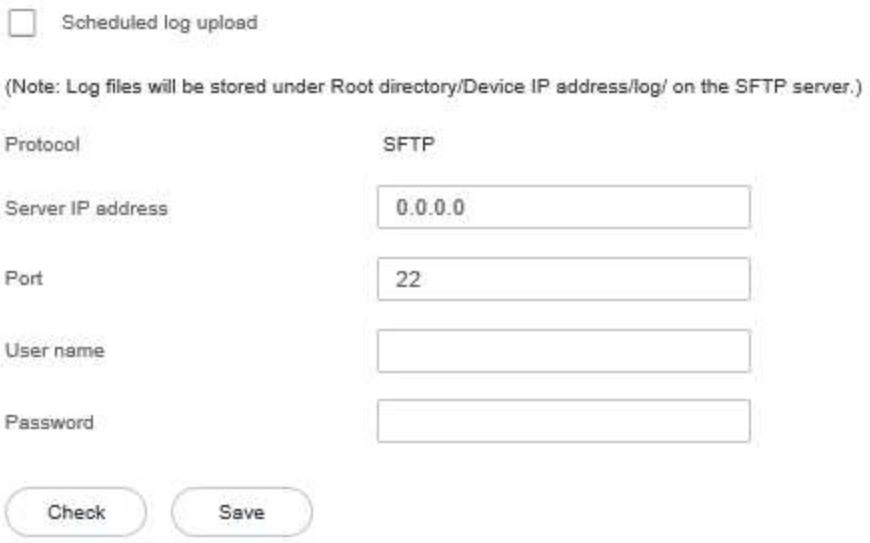
Configuring Scheduled Log Upload

You can enable the scheduled log upload function when you want to continuously locate a fault. After the function is enabled, when the size of a log file (such as alarm, err, or syslog) reaches a specified value, the system automatically compresses the log file and uploads it to a specified server through SFTP to prevent the log file from being overwritten.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Scheduled Log Upload**. The **Scheduled Log Upload** area is displayed, as shown in Figure 1.

   Figure 1 Scheduled Log Upload area

3. Select **Scheduled log upload** and configure log upload information. Table 1 describes the parameters.

   Table 1 Scheduled log upload parameters

Parameter	Remarks

Parameter	Remarks
Protocol	Protocol used for uploading log files to the server. **SFTP**: secure file transfer protocol that provides an encryption method for transferring files
Server IP address	IP address of the SFTP server.
Port	Port number of the SFTP server.
User name	User name for logging in to the SFTP server.
Password	Password for logging in to the SFTP server.
Check	You can click **Check** to check whether the SFTP parameters you set are valid. Result description: • If a message is displayed indicating that the server is successfully connected, the server IP address is available. • If a message is displayed indicating that the server is unreachable, the server IP address is unreachable. • If a message is displayed indicating incorrect server IP address or port number, the SFTP server fails to be connected because the server IP address or port number is incorrectly set. • If a message is displayed indicating incorrect user name or password, the authentication fails due to incorrect user name or password.

4. Click **Save**.

Parent topic: Logs

Camera Self-Check

Only zoom cameras support self-check. You can allow the camera to automatically check functions such as PTZ controls.

The web page varies depending on the camera model. Before configuring camera self-check, you need to select a channel type first.

Enabling PTZ Device Self-Check

NOTE

Only PTZ dome cameras support PTZ device self-check.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Device Self-Check** > **PTZ Check**, and the **PTZ Check** area is shown in Figure 1.

   Figure 1 PTZ Check area

3. Select **Enable PTZ check**.
4. Set **Check interval (h)**. The default value is **24**.

   If you use the default value **24**, the device automatically checks whether PTZ functions are normal every 24 hours.

5. Click **Save**.

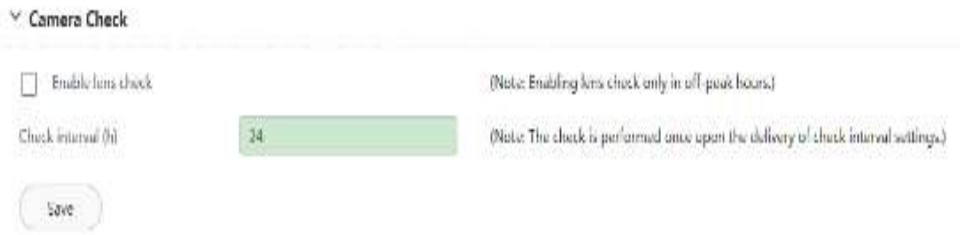
   The message "Enabling self-check will affect service functions such as PTZ (only for PTZ-capable cameras), video, and image functions. Continue?" is displayed, warning you that the preceding functions are interrupted during the PTZ self-check.

6. If you can accept the impact of self-check, click **OK**. Then the camera automatically checks whether the PTZ device works properly.

Enabling Lens Check

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Device Self-Check** > **Camera Check**, and the **Camera Check** area is shown in Figure 2.

   Figure 2 Camera Check area

3. Select **Enable lens check**.
4. Set **Check interval (h)**. The default value is **24**.

   For example, if you use the default value **24**, the camera automatically performs lens check every 24 hours.

5. Click **Save**.

   The message "During the self-check, the video and image services will be affected. Are you sure you want to enable this function?" is displayed, warning you that a blank screen is displayed during the lens self-check, which affects video recording.

6. If you can accept the impact of self-check, click **OK**. Then the camera automatically checks whether the camera imaging is normal.

PTZ Service Life Check

NOTE

Only PTZ dome cameras support PTZ service life check.

1. Log in to the camera web system (https://*Camera IP address*).

2. Choose **Configuration** > **System** > **System Maintenance** > **Device Self-Check** and click **PTZ Service Life Check**. The **PTZ Service Life Check** area is displayed, as shown in Figure 3.

   Figure 3 PTZ Service Life Check area

3. Select **PTZ service life check** and click **Save**.

   After this function is enabled, if the number of PTZ rotation times exceed the default value, the PTZ device stops rotating.

Parent topic: System Maintenance

Service Fault Locating

This section describes image quality diagnosis, intelligent service fault locating, and video service status detection for cameras.

Image Quality Diagnosis This section describes how to view downloaded diagnosis images and adjust camera settings based on the provided suggestions.

Intelligent Service Fault Locating
You can query running status and configuration information about services with one click for target detection, ITS, micro checkpoint, and parking violation detection cameras.

Video Service Status Monitoring
You can query the information about the computer that requests real-time video streams from a camera, as well as the data volume of video streams and number of times that video streams fail to be sent.

Parent topic: System Maintenance

Image Quality Diagnosis

This section describes how to view downloaded diagnosis images and adjust camera settings based on the provided suggestions.

For target capture cameras, omni-data structuring cameras, and micro checkpoint cameras, the system can diagnose image quality in **Perimeter detection**, **Road**, and **Target detection** scenarios, and provide diagnosis results and optimization suggestions.

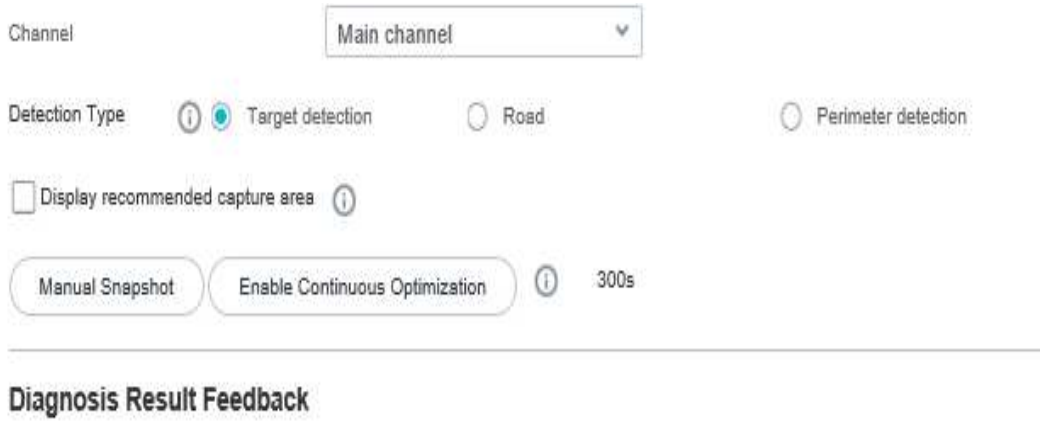
Prerequisites

1. The target detection or object classification algorithm has been upgraded for the camera. For details about how to upgrade the algorithm, see Upgrading the Camera Version/Algorithms.
2. Any function under **Target Intelligence**, or **Vehicle Intelligence** has been enabled. For details about how to configure functions under **Target Intelligence**, see Configuring Intelligent Target Analysis. For details about how to configure functions under **Vehicle Intelligence**, see Configuring Intelligent Vehicle Analysis.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Service Fault Locating**, click **Image Diagnosis**, and select a channel as shown in Figure 1.

Figure 1 Image Diagnosis area



3. (Optional) Select **Display recommended capture area**.

   The recommended capture area is framed on the video image. During diagnosis, keep objects in the displayed frame.

4. Click **Manual Snapshot**.

   Take target detection as an example. The camera will diagnose quality of captured images, including:

   - Target size
   - Image clarity
   - Horizontal angle of the camera
   - Vertical angle of the camera

   For road detection scenarios, the system does not diagnose the camera angle. Figure 2 shows the diagnosis result. You can click **Download** to download the diagnosis result image.

Figure 2 Diagnosis result



5. Adjust the camera parameters based on the optimization suggestions.
    - If the horizontal or vertical angle of the camera does not meet the requirements, adjust the horizontal or vertical angle of the camera.

      For road detection scenarios, the system does not provide optimization suggestions about the camera angle.
    - If the target size and image clarity do not meet the requirements, click **Auto Adjust** to automatically adjust the zoom ratio or focus.
6. After you click **Enable Continuous Optimization**, the system automatically diagnoses the image quality every 10s. The diagnosis lasts for 300s and can be stopped at any time. Other services are suspended during the diagnosis and resumed after the diagnosis is complete. Exercise caution when performing this operation.

> **NOTE**
>
> - Image diagnosis is not supported in full intelligence mode for multi-algorithm cameras.
> - Image diagnosis is not supported in 1 + N mode.

- Automatic focus is supported during image diagnosis only when the camera is in target checkpoint mode and **Focus mode** is set to **Auto** or **Semi-auto** under **Configuration** > **Image** > **Display** > **Focus**.

Parent topic: Service Fault Locating

Intelligent Service Fault Locating

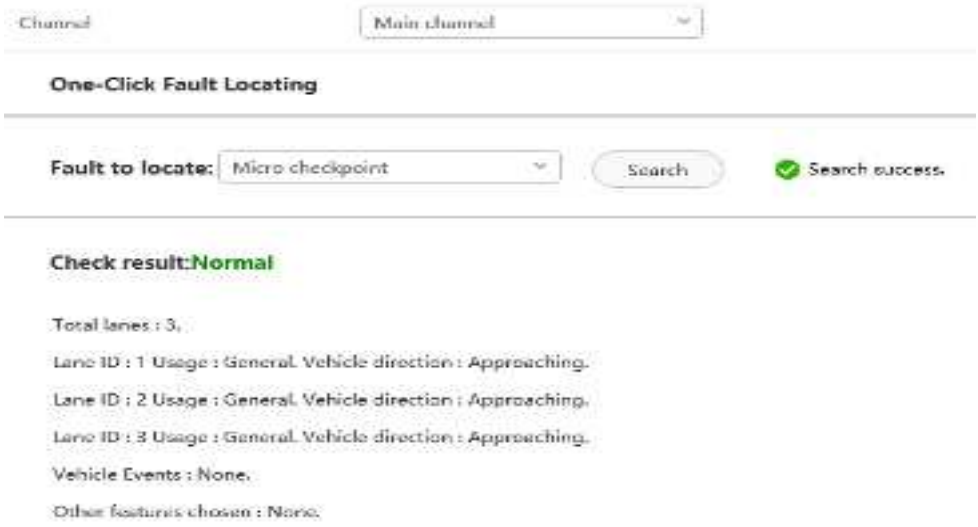
You can query running status and configuration information about services with one click for target detection, ITS, micro checkpoint, and parking violation detection cameras.

The services supported for one-click fault locating vary depending on camera models.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Service Fault Locating** > **Intelligent Service Fault Locating**.
3. Select the desired channel.
4. Select the service for which faults are to be located and click **Search**.
   - When the service is enabled, "Normal" is displayed for **Check result** and the service configuration information is displayed, as shown in Figure 1 (here, the micro checkpoint service is used as an example).

     Figure 1 Check result

> **NOTE**
>
> The language of service configuration information returned in the check result is the same as the language of the structured information system set under **Configuration** > **System** > **System Settings** > **Basic Information**.

- If the service is not enabled, "The service is not enabled." is displayed for **Check result**, as shown in Figure 2 (here, the target detection service is used as an example).

  Figure 2 Check result

Parent topic: Service Fault Locating

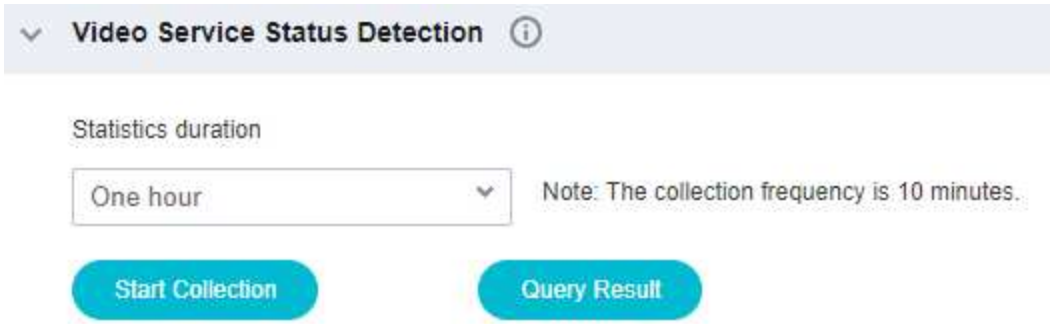
Video Service Status Monitoring

You can query the information about the computer that requests real-time video streams from a camera, as well as the data volume of video streams and number of times that video streams fail to be sent.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Service Fault Locating** > **Video Service Status Detection**. The **Video Service Status Detection** area is displayed, as shown in Figure 1.

   Figure 1 Video Service Status Detection area

3. Set **Statistics duration** and click **Start Collection**.
   - If the statistical period is one hour, the collection frequency is once every 10 minutes.
   - If the statistical period is one day, the collection frequency is once an hour.
   - If the statistical period is one week, the collection frequency is once an hour.
4. Click **Query Result**. When a host accesses the camera, related information is displayed in the collection result, as shown in Figure 2.

Figure 2 Collection result



Parent topic: Service Fault Locating

Anti-Counterfeit Code Check

This function is available for cameras that support motor vehicle detection. You can use the anti-counterfeit code to verify snapshots to judge whether they have been tampered with.

NOTE

- The capabilities supported vary between camera models.
- To perform anti-counterfeit code verification on motor vehicle images captured by cameras that support motor vehicle detection, you need to enable motor vehicle capture under **Configuration** > **Intelligence** > **Vehicle Intelligence** and set motor vehicle detection parameters.

Prerequisites

For motor vehicle detection of non-ITS cameras, you have enabled image watermark under **Configuration** > **Storage** > **Snapshot Parameters** > **Image Watermark**.

NOTE

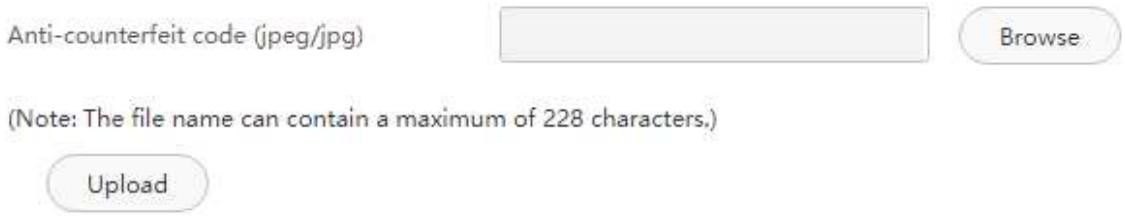
- If snapshots taken by a camera are verified by cameras of other models, the verification may fail even if the images are authentic.
- If the snapshot taken by a camera is modified through image editing software, the verification will fail. Therefore, you are not advised to edit snapshots.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Anti-Counterfeit Code Check**.

The **Anti-Counterfeit Code Check** tab page is displayed, as shown in Figure 1.

Figure 1 Anti-Counterfeit Code Check tab page



3. Click **Browse**, select a local snapshot, and click **Upload**.

   After the snapshot is uploaded, the camera verifies the snapshot and returns the verification result. If the snapshot is authentic, a message is displayed, indicating that the verification is successful.

Parent topic: System Maintenance

Security Management

This section describes how to manage camera passwords and certificates, configure IP address filtering, security options, static Address Resolution Protocol (ARP) rules, and password recovery, and manage users.

Password Management To ensure data security, change the password in a timely manner. After the password is changed, record and keep the new password secure.

Password Recovery
With the password recovery function, you can retrieve the login password if you forgot your password.

Certificate Management
This section describes how to manage HTTPS certificates, SDK certificates, and SDK CRLs of cameras.

IP Filtering
You can use the IP filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

Security Options
Hypertext Transfer Protocol Secure (HTTPS) is used for secure communication over a computer network. The principal motivations for HTTPS are authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit.

Static ARP Rule
You can configure a static ARP rule to bind the camera IP address to the MAC address.

Parent topic: Managing the System

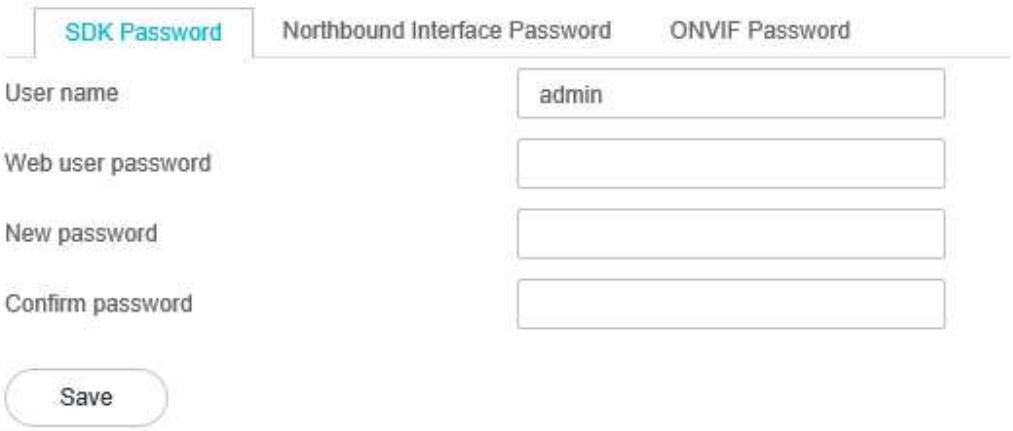
Password Management

To ensure data security, change the password in a timely manner. After the password is changed, record and keep the new password secure.

Managing Protocol Passwords

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Password Management**.
3. Click **Protocol Password**. Under **Protocol Password**, you can change the SDK, northbound interface, and ONVIF passwords.
4. Use SDK password management as an example. Click the **SDK Password** tab. The **SDK Password** tab page is displayed, as shown in Figure 1.

   Figure 1 SDK Password tab page

5. Set **Web user password**, **New password**, and **Confirm password**.
   - The value of **Web user password** is the password of the **admin** user for logging in to the camera.
   - The value of **Confirm password** must be the same as that of **New password**.

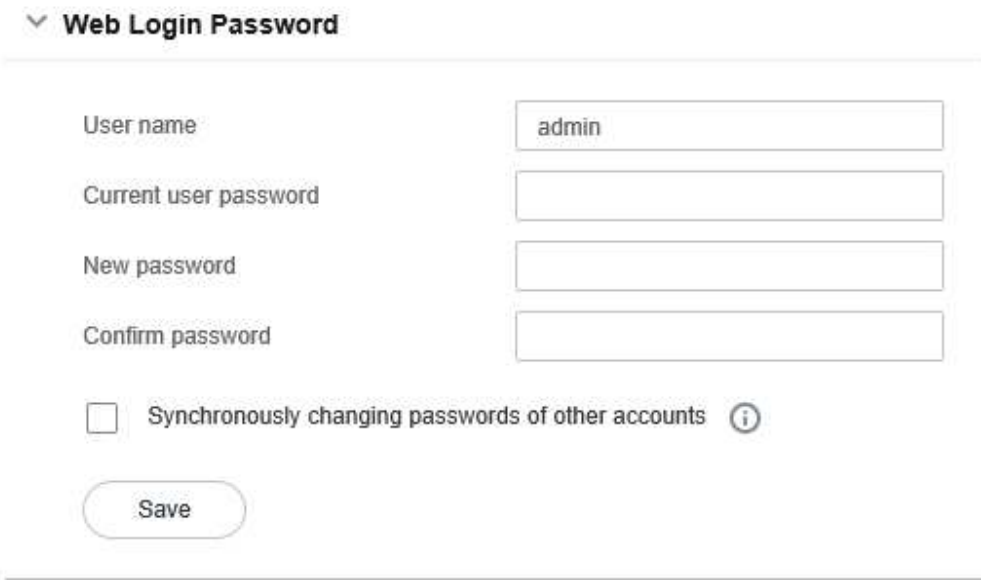
6. Click **Save**.

Managing Web Login Passwords

You can change the web login password of the current user.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Password Management**.
3. Click **Web Login Password**. The area shown in Figure 2 is displayed.

   Figure 2 Web Login Password area

4. Set **Current user password**, **New password**, and **Confirm password**.

   NOTE

   - If you select **Synchronously changing passwords of other accounts**, the passwords of the SDK, web, ONVIF/RTSP, and RESTful accounts are changed synchronously.

5. Click **Save**.

Setting the Web Password Validity Period

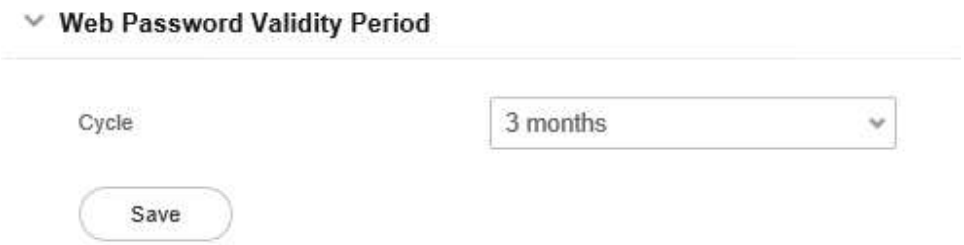
You can view or configure the validity period of the web password.

> **NOTE**
>
> After the password expires, the system will demand you to change the password.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Password Management**.
3. Click **Web Password Validity Period**. The area shown in Setting the Web Password Validity Period is displayed.

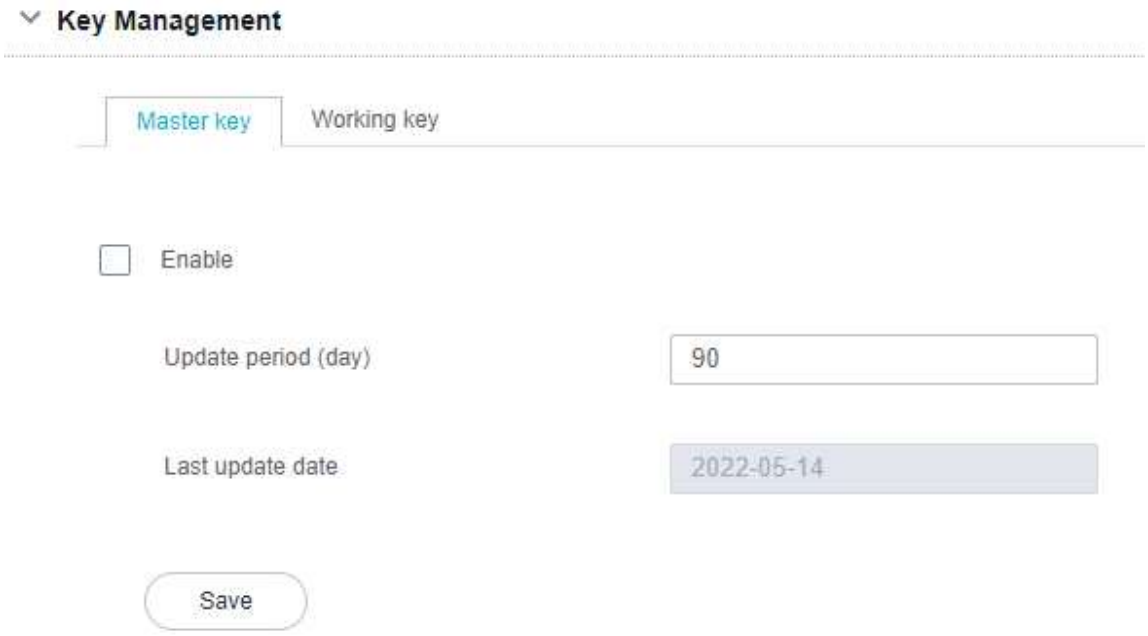
   Figure 3 Web Password Validity Period area

Configuring Key Management

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Password Management**. Click **Key Management**. The area shown in Figure 4 is displayed.

Figure 4 Key Management area



3. Click the **Master Key** and **Working Key** tabs separately and set related parameters.
   - **Working Key**: key for encrypting passwords related to cameras
   - **Master Key**: key for encrypting the working key

   Table 1 describes the parameters.

Table 1 Key management parameters

Parameter	Description
Enable	Indicates whether to periodically update the key.
Update period (day)	Key update interval.
Last update date	Time when the key was last updated.

Managing the Weak Password Dictionary

Weak passwords may cause security risks. For security purposes, you are advised not to set the new password to a weak password. The system provides a default weak password, which can be defined by users. When you set a password, the system verifies the password strength.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Weak Password Dictionary**.

   After you log in to the camera for the first time or upgrade the camera, the default weak password is displayed.
3. Add weak passwords.
   - Adding weak passwords one by one

     Click **Add** and enter the weak password to be added. Click **OK**.
   - Adding weak passwords in batches

     a. Click **Export** and select a save path to download the weak password dictionary file to the local computer.

     b. Add, delete, or change weak passwords in the file as required and save the file.

     c. Click **Import**, select the modified weak password dictionary file, and upload it to the camera.

NOTE

- You can click in the **Operation** column corresponding to a weak password and edit the weak password.
- You can delete existing weak passwords.
  - Deleting a weak password: Click in the **Operation** column corresponding to a weak password to delete the weak password.

- Deleting weak passwords in batches: Select multiple weak passwords and click **Batch Delete** to delete the weak passwords.

Parent topic: Security Management

Password Recovery

With the password recovery function, you can retrieve the login password if you forgot your password.

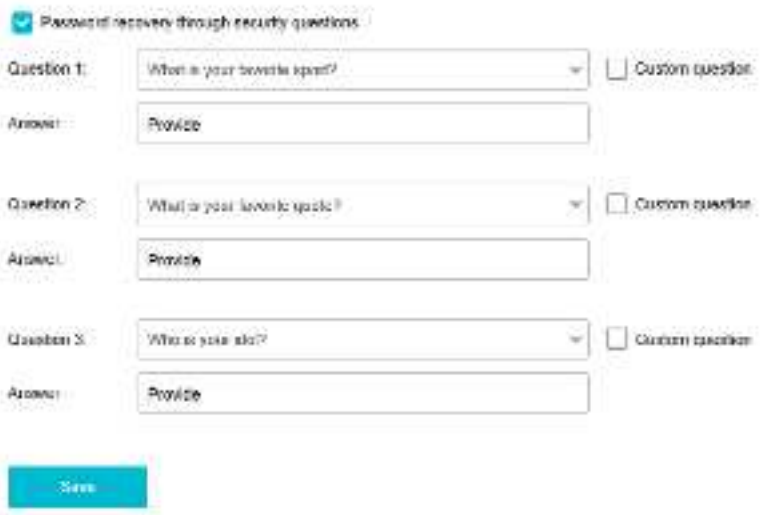
NOTICE

- If you have not configured password recovery and forgot your password, you can hold down the RESET button on the camera to restore it factory settings. Be aware that restoring a device to factory settings may result in data loss.
  - To restart a camera, hold down the RESET button for less than 3s.
  - To restore a camera to factory settings, hold down the RESET button for at least 5s.
  - If you hold down the RESET button before powering on the device, the IP address may not be restored. In this case, restart the device again.
- If you have configured password recovery and forgot your password, you can click **Forgot Password** on the login page and answer preset security questions to retrieve your password.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Password Recovery**. The **Password Recovery** tab page is displayed.
3. Select **Password recovery through security questions** and set security questions, as shown in Figure 1.

Figure 1 Setting security questions



4. Select a preset question from the **Question *X*** drop-down list box or select **Custom question** and customize a question.
5. Enter the answer to the question. Set three security questions and their answers in sequence.

> **NOTE**
>
> - You are advised to set all the three security questions.
> - You are advised to set questions and answers that you are familiar with.

6. Click **Save**. The **Identity Authentication** dialog box is displayed.
7. Enter the login password and click **OK**.

Parent topic: Security Management

Certificate Management

This section describes how to manage HTTPS certificates, SDK certificates, and SDK CRLs of cameras.

Managing HTTPS Certificates You can manage HTTPS certificates in the camera web system. For security purposes, you are advised to use your own certificates.

Managing SDK Certificates
You can manage certificates for SDK two-way authentication in the camera web system. For security purposes, you are advised to use your own certificates.

Managing the SDK Certificate Revocation List
Cameras support SDK certificate revocation. For security purposes, cameras cannot connect to platforms that use certificates in the CRL.

Parent topic: Security Management

Managing HTTPS Certificates

You can manage HTTPS certificates in the camera web system. For security purposes, you are advised to use your own certificates.

Background

Purchase the certificate from an authoritative third-party certification organization or establish a CA server.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **HTTPS Certificate Management**.

   Figure 1 HTTPS Certificate Management area

3. Set parameters in the **HTTPS Certificate Management** area. Table 1 describes the parameters.

   Table 1 HTTPS certificate management parameters

Parameter	Description
Certificate file (.pem)	Digital information file that identifies and verifies both parties involved in network communication.
Key file (.pem)	Key file that contains the certificate key.

   You can use your own certificate file in the following way: Click **Browse**, select your desired file path, and click **Upload**. In the dialog box that is displayed, enter the password of the private key file to upload the certificate.

NOTE

- Only certificate files in **.pem** format can be uploaded.
- The password of the private key file must be the same as that generated when you apply for the private key file.
- If you click **Restore Certificate**, the system displays a dialog box asking you whether to restore the certificate to the initial one.

Parent topic: Certificate Management

Managing SDK Certificates

You can manage certificates for SDK two-way authentication in the camera web system. For security purposes, you are advised to use your own certificates.

The validity period of a certificate is defined by each certificate authority (CA) when the certificate issuer is being set.

Background

Purchase the certificate from an authoritative third-party certification organization or establish a CA server.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **SDK Certificate Management**.

   The **SDK Certificate Management** area is displayed, as shown in Figure 1.

   Figure 1 SDK Certificate Management area

3. Set parameters in the **SDK Certificate Management** area. Table 1 describes the parameters and buttons in this area.

   Table 1 SDK certificate management parameters/buttons

Parameter/Button	Description
CA certificate file (.cer)	CA certificate.

Parameter/Button	Description
Certificate file (.pem)	Digital information file that identifies and verifies both parties involved in network communication.
Key file (.pem)	Key file that contains the certificate key (*xxx*_key.pem).
Restore Certificate	Button for restoring the certificate to the default one.

You can use your own certificate file in the following way: Click **Browse**, select your desired file path, and click **Upload**. In the dialog box that is displayed, enter the password of the private key file to upload the certificate.

NOTE

- Only certificate files in .pem format can be uploaded.
- The password of the private key file must be the same as that generated when you apply for the private key file.
- If you click **Restore Certificate**, the system displays a dialog box asking you whether to restore the certificate to the initial one.
- To update the OM certificate, you need to first update the SDK certificate and restart the camera. The system will automatically synchronize the new certificate to the OM.

Parent topic: Certificate Management

Managing the SDK Certificate Revocation List

Cameras support SDK certificate revocation. For security purposes, cameras cannot connect to platforms that use certificates in the CRL.

Background

A CRL is a data file that lists the serial numbers and revocation dates of certificates that are revoked by the CA.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **SDK Certificate Revocation List Management**. The **SDK Certificate Revocation List Management** area is displayed, as shown in Figure 1.

   Figure 1 SDK Certificate Revocation List Management area

3. Click **Browse**, select the CRL to be uploaded, and click **Upload**.

   If the CRL file uploaded is normal, **Normal** is displayed for the certificate revocation list status. If the CRL file uploaded has expired, **Expired** is displayed for the certificate revocation list status. If the format of the CRL file to be uploaded is incorrect, an error message is displayed.
4. (Optional) Click **Refresh** if the status is not displayed.
5. (Optional) Click **Delete** to delete an uploaded CRL.

Parent topic: Certificate Management

IP Filtering

You can use the IP filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

Background

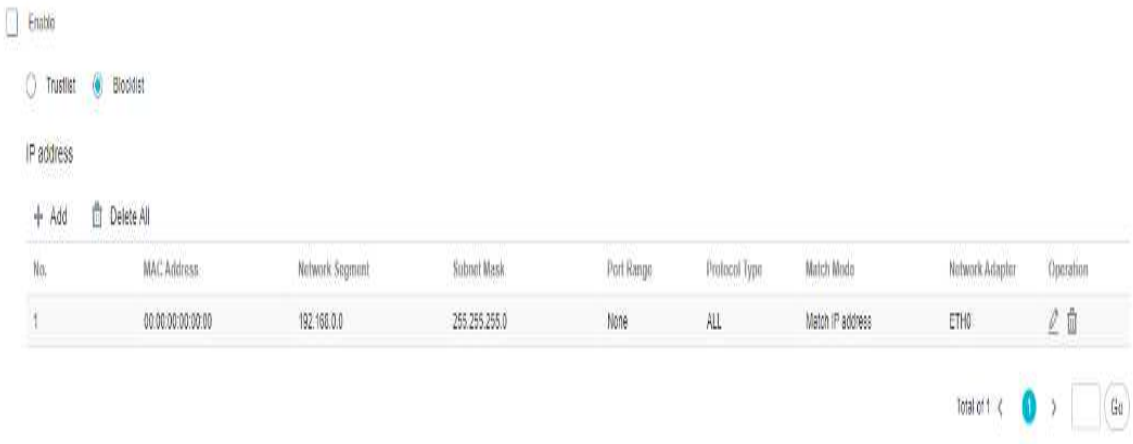
- A network segment is obtained by performing logical AND of the IP address and subnet mask.
- A maximum of 100 IP filtering rules can be added.

Procedure

1. Choose **Configuration** > **System** > **Security Management** > **IP Filtering**.

   The **IP Filtering** tab page is displayed, as shown in Figure 1.

   Figure 1 IP Filtering tab page

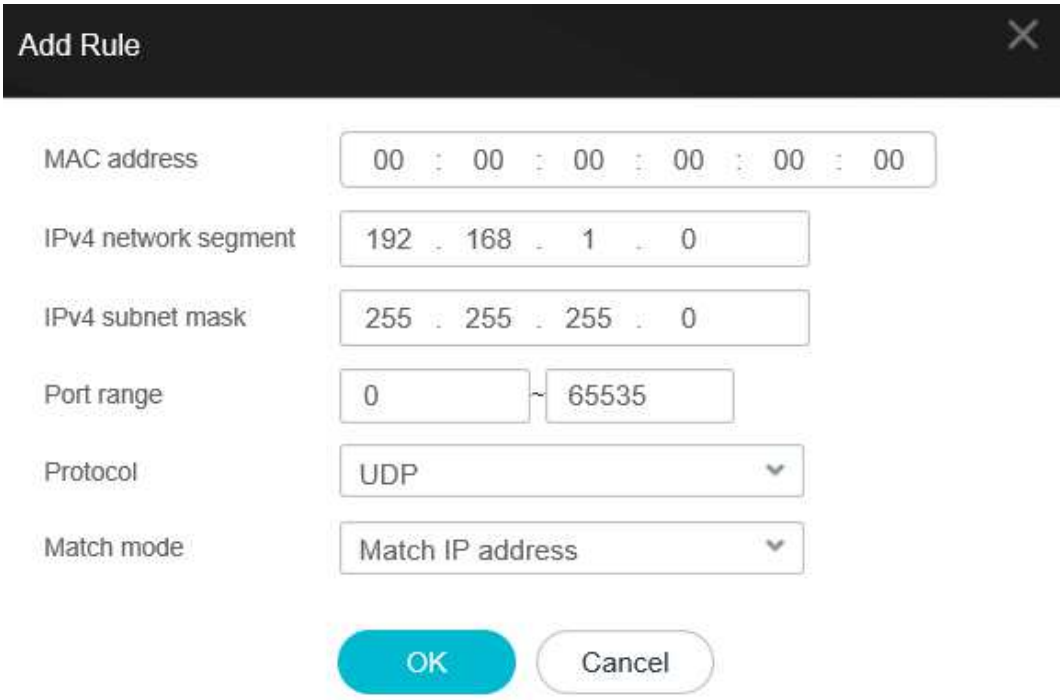


2. Select **Enable** to enable the IP filtering function.
3. Select a desired IP filtering rule.

   The IP filtering rule has two options: **Trustlist** and **Blocklist**, that is, denying or allowing only the access from a specified MAC address, IP network segment or port, or using a specified protocol. Currently, the camera supports only one option at a time.

4. Click **Add**. In the **Add Rule** dialog box that is displayed, set **MAC address**, **IPv4 network segment**, **IPv4 subnet mask**, **Protocol**, and **Match mode**, as shown in Figure 2.

   Figure 2 Add Rule dialog box



> **NOTE**
>
> - If a filtering rule shown in Figure 2 is configured under **Blocklist**, the camera does not process UDP packets sent from the network segment **192.168.1.0** to ports **0–65535**.

5. Click **OK**.

   The **IP Filtering** tab page is displayed.

6. Click **Save**.

> **NOTE**
>
> To modify or delete an IP filter rule, click or in the **Operation** column of the IP filter rule.

Parent topic: Security Management

Security Options

Hypertext Transfer Protocol Secure (HTTPS) is used for secure communication over a computer network. The principal motivations for HTTPS are authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit.

The web page varies depending on the camera model.

Procedure

1. Choose **Configuration** > **System** > **Security Management** > **Security Options**.

   NOTICE

   Enabling **TLS1.1** and **non-FS cipher suite** may bring security risks. Exercise caution when enabling them.

   The **Security Options** tab page is displayed, as shown in Figure 1. Table 1 describes the parameters. Select a security option as required.

   Figure 1 Security Options tab page

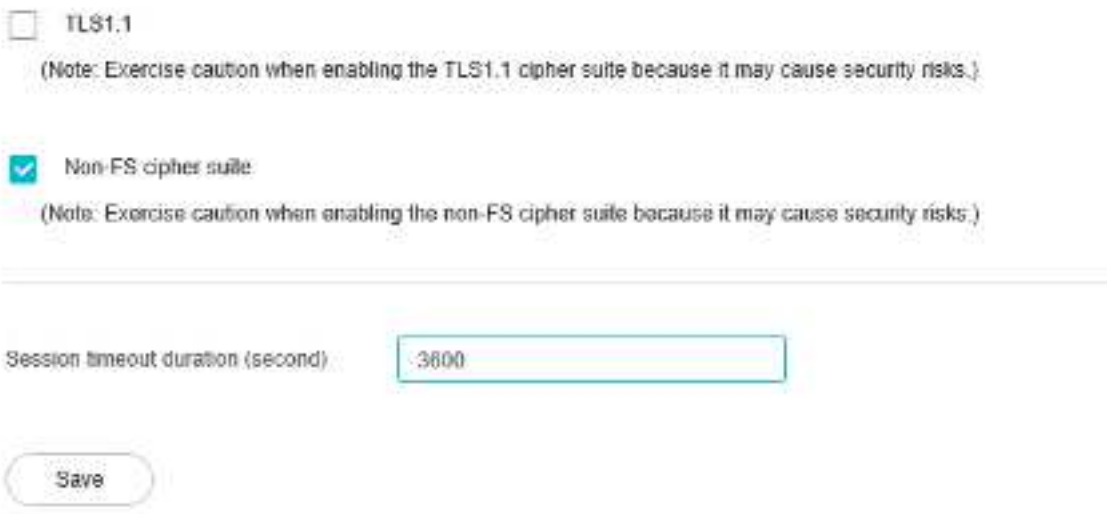
   

   Table 1 Parameters for security options

Parameter	Description

Parameter	Description
TLS1.1	TLS1.1 is a security protocol that does not provide modern encryption algorithms. If your computer does not support cipher suites, you can use TLS1.1.
Non-FS cipher suite	Non-FS cipher suite provides cipher suites, and thus is more secure than TLS1.1.

2. Set the **Session timeout duration (second)**. When the login duration exceeds the value of this parameter, the camera returns to the login page.
3. Click **Save**.

Parent topic: Security Management

Static ARP Rule

You can configure a static ARP rule to bind the camera IP address to the MAC address.

Procedure

1. Choose **Configuration** > **System** > **Security Management** > **Static ARP Rule**.

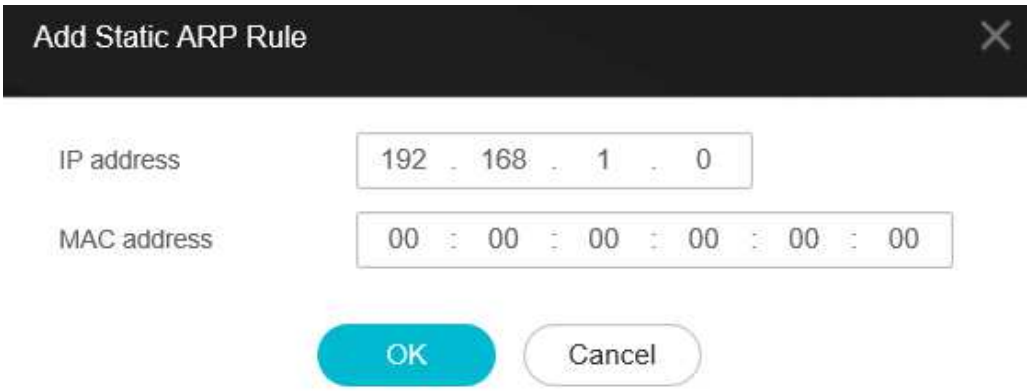
   The **Static ARP Rule** tab page is displayed, as shown in Figure 1.

   Figure 1 Static ARP Rule tab page

2. Click **Add**. In the displayed **Add Static ARP Rule** dialog box, set **IP address** and **MAC address**, as shown in Figure 2.

   Figure 2 Adding a static ARP rule

3. Click **OK**.

   The **Static ARP Rule** tab page is displayed.

> **NOTE**
>
> You can modify or delete static ARP rules. To modify a static ARP rule, click in the **Operation** column. To delete a static ARP rule,

click  in the **Operation** column. To delete all static ARP rules, click **Delete All**.

Parent topic: Security Management

User Management

By level of rights, users are classified into three types: system administrator (**admin**), advanced operator, and common operator. Users can be added, modified, and deleted.

User List Administrators can add and delete users, change user passwords, change the maximum number of allowed login sessions, and configure the maximum number of allowed consecutive incorrect password attempts before the account is locked.

User Connections
You can check the connection status of a user or disconnect a user in this area.

Password Validity Period
You can view or configure the validity period of a user password in this area.

Parent topic: Managing the System

User List

Administrators can add and delete users, change user passwords, change the maximum number of allowed login sessions, and configure the maximum number of allowed consecutive incorrect password attempts before the account is locked.

Adding a User

The **admin** user creates all initial users uniformly. When creating users, the **admin** user can set user roles and assign permissions to the roles.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 1.

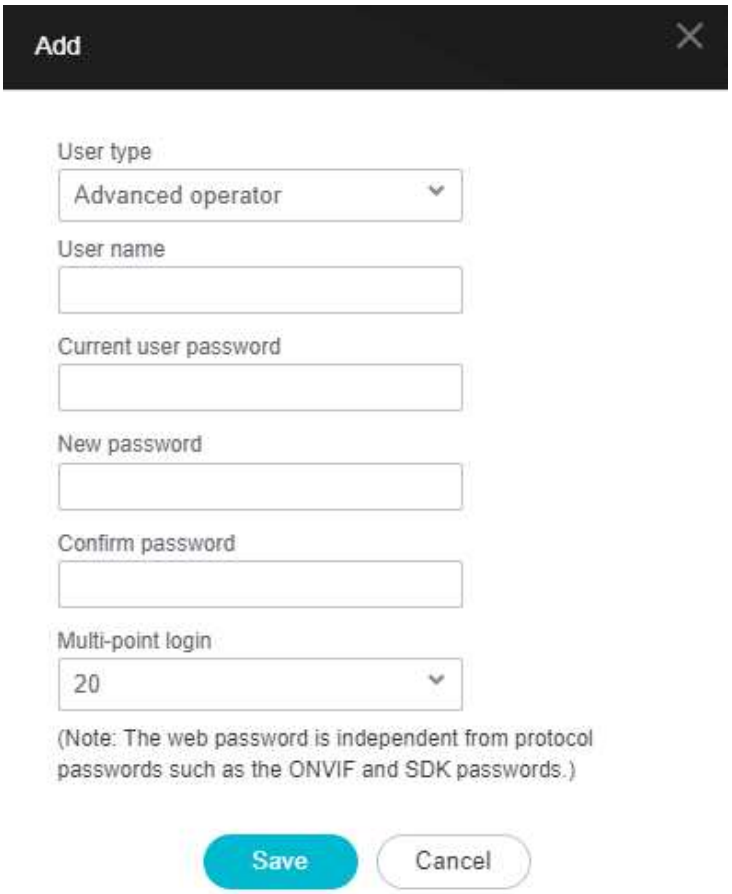
   Figure 1 User List area

3. Click **Add**.

   In the **Add** dialog box that is displayed, configure information about the new user, as shown in Figure 2.

Figure 2 Add dialog box



NOTICE

- A maximum of 10 users (including the **admin** user) can be added.
- The **admin** and **ApiAdmin** users are administrators and cannot be added again.

4. Set user parameters. Table 1 describes the parameters.

Table 1 Parameters for adding a user

Parameter	Description
User type	Different types of users have different operation rights. You can choose the user type as required. • Administrators have all operation rights. They can add advanced operators and common operators.

Parameter	Description
	• Advanced operators cannot add or manage users but can perform operations such as live video viewing and intelligent service configuration. • Common operators only have common operation rights, including viewing live video, setting PTZ parameters, and changing their own passwords.
User name	Enter a name for the new user.
Current user password	Enter the password of the user who currently logs in.
New password	Enter a new password.
Confirm password	Enter the new password again.
Multi-point login	Enter the maximum number of concurrent logins of the new user at the same time.

5. Click **Save**.

NOTE

When you use an account that is created by the **admin** user to log in to the camera for the first time, the **Change Password** dialog box will be displayed. You can log in to the camera after changing the password as prompted.

Changing the User Password

The password of a user can be changed, but the user type and user name cannot be changed.

NOTE

- System administrators can modify information about all users.
- Advanced operators and common operators do not have the permission to modify user information.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 3.

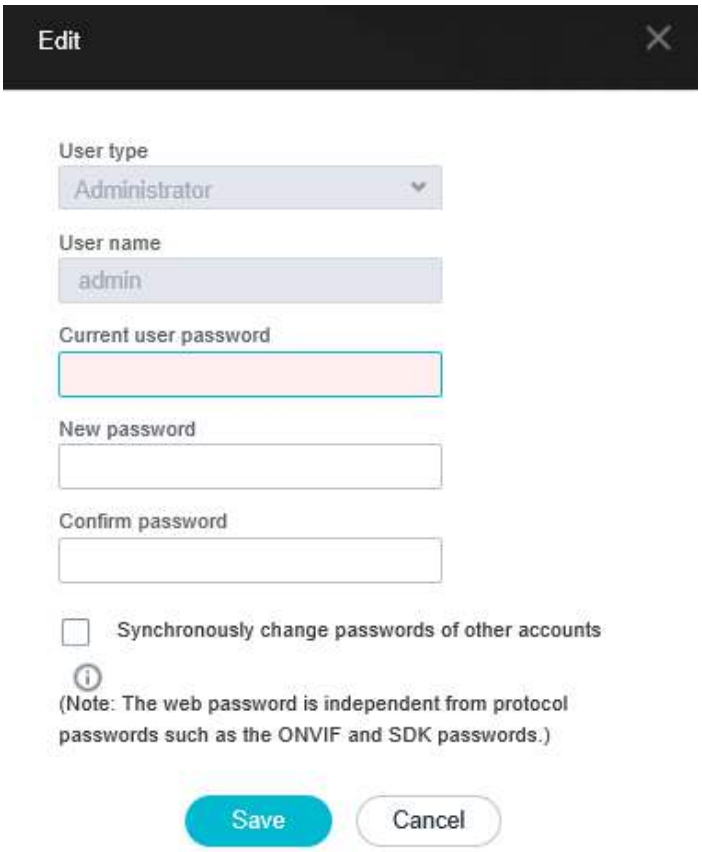
   Figure 3 User List area



3. Select a user.
4. Click .

   The dialog box for changing user password is displayed, as shown in Figure 4.

   Figure 4 Edit dialog box



5. Specify the current user password, new password, and confirm password.
6. Click **Save**.

> **NOTE**
>
> After you change the password of an account as the **admin** user, the **Change Password** dialog box is displayed when you use the account to log in to the camera again. You can log in to the camera after changing the password as prompted.

Changing the Maximum Number of Concurrent Logins

You can change the maximum number of concurrent logins for a user.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 5.

   Figure 5 User List area

3. Select a user.
4. Click **Multi-Login**.

   The dialog box for changing the maximum number of concurrent logins is displayed.
5. Set **Current user password** and **Multi-point login**.
6. Click **Save**.

Deleting a User

Administrators can delete unnecessary users to ensure system access security.

> **NOTE**

- System administrators can delete advanced operators and common operators. System administrators cannot be deleted.
- Advanced operators do not have the permission to delete users.
- Common operators do not have the permission to delete users.
- After a logged-in user is deleted, the user cannot perform operations in the web system and will be forcibly logged out.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 6.

   Figure 6 User List area

3. Select a user.
4. Click .

   The **Delete** dialog box is displayed.
5. Enter the current user password and click **OK**.

   The **Delete User** dialog box is displayed.
6. Click **OK**.

Configuring Account Locking and Unlocking

The system administrator can specify the maximum number of incorrect password attempts for an account. If the maximum number of incorrect password attempts is reached, the account is locked.

NOTE

Only the system administrator can configure account locking.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

The **User List** area is displayed, as shown in Figure 7.

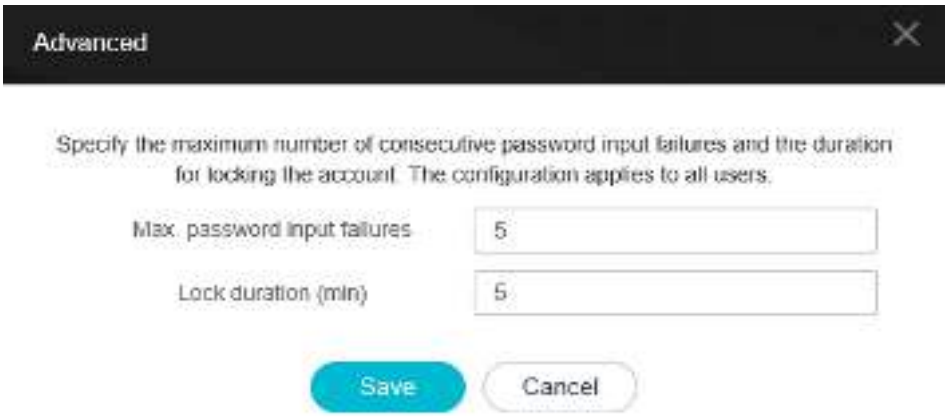
Figure 7 User List area



3. Click **Advanced**.

   The **Advanced** dialog box is displayed, as shown in Figure 8.

   Figure 8 Advanced dialog box



4. Set **Max. password input failures** and **Lock interval (min)**.

   NOTE

   - **Max. password input failures**: maximum number of consecutive incorrect password attempts allowed
   - **Lock interval (min)**: duration in which an account is locked after the number of consecutive incorrect password attempts exceeds the maximum
   - If **Max. password input failures** is set to **0**, the maximum number of consecutive incorrect password attempts allowed is unlimited and the account will not be locked.
   - If **Max. password input failures** is not set to **0** but **Lock interval (min)** is set to **0**, an account will be locked permanently when the number of consecutive incorrect password attempts exceeds the value of **Max. password input failures**.

5. Click **Save**.

Parent topic: User Management

User Connections

You can check the connection status of a user or disconnect a user in this area.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management**.
3. Click **User Connections**. The **User Connections** area is displayed, as shown in Figure 1.

   Figure 1 User Connections area

   NOTICE

   - To disconnect a user, click **Disconnect** in the **Operation** column corresponding to the user.
   - The administrator cannot be forcibly disconnected.

Parent topic: User Management

Password Validity Period

You can view or configure the validity period of a user password in this area.

> **NOTE**
>
> After the password expires, the system will demand you to change the password.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management**.
3. Click **Password Validity Period**. The **Password Validity Period** area is displayed, as shown in Figure 1.

   Figure 1 Password Validity Period area

   > **NOTE**
   >
   > The value of **Period (months)** is an integer ranging from 0 to 12. If this parameter is set to **0**, the password is permanently valid.

Parent topic: User Management

Setting Network Parameters

This section describes how to set network parameters such as the IP address.

> **NOTE**
>
> The inclusive intelligence camera models do not support configuration of anti-attack parameters, PPPoE parameters, SNMP parameters, and intelligent acceleration parameters (including adaptive bandwidth, TCP intelligent acceleration, traffic shaping, and SEC).

Setting Basic Network Parameters By setting basic network parameters, you can quickly perform basic network configurations on the device, such as the maximum size of data packets transferred on the network, data transmission quality, and attack defense parameters.

Setting Advanced Network Parameters
You can set advanced network parameters, such as FTP, SSH/SFTP, and SNMP parameters.

Parent topic: Configuration

Setting Basic Network Parameters

By setting basic network parameters, you can quickly perform basic network configurations on the device, such as the maximum size of data packets transferred on the network, data transmission quality, and attack defense parameters.

> **NOTE**
>
> The camera enables the function of periodically sending Address Resolution Protocol (ARP) requests by default. The sending interval is 5 minutes.

Configuring TCP/IP This section describes how to set TCP/IP parameters.

Configuring PPPoE
The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames.

Configuring Ports
This section describes how to configure ports and port mapping in the camera web system.

Parent topic: Setting Network Parameters

Configuring TCP/IP

This section describes how to set TCP/IP parameters.

Setting Camera IP Addresses This section describes how to set camera IP addresses in the camera web system.

Setting Network Connectivity Detection
This section describes how to set network connectivity detection.

Setting MTU Parameters
The Maximum Transmission Unit (MTU) is the maximum size of a data packet that can be transmitted over the network. You can set MTU parameters to specify the maximum size of a data packet to be transmitted over the network to achieve the optimal transmission efficiency and quality.

Setting QoS Parameters
The Quality of Service (QoS) is a network security mechanism for resolving network issues such as delay and congestion. By setting QoS parameters, you can set the priority of media and signaling streams based on the network conditions to ensure transmission quality.

Setting Anti-Attack Parameters
You can set anti-attack parameters to defending the camera against network flood attacks.

Setting Multicast Parameters
In multicast transmission mode, a sender sets up P2MP network connections with all recipients, improving data transmission efficiency and lowering the possibility of backbone network congestion.

Parent topic: Setting Basic Network Parameters

Setting Camera IP Addresses

This section describes how to set camera IP addresses in the camera web system.

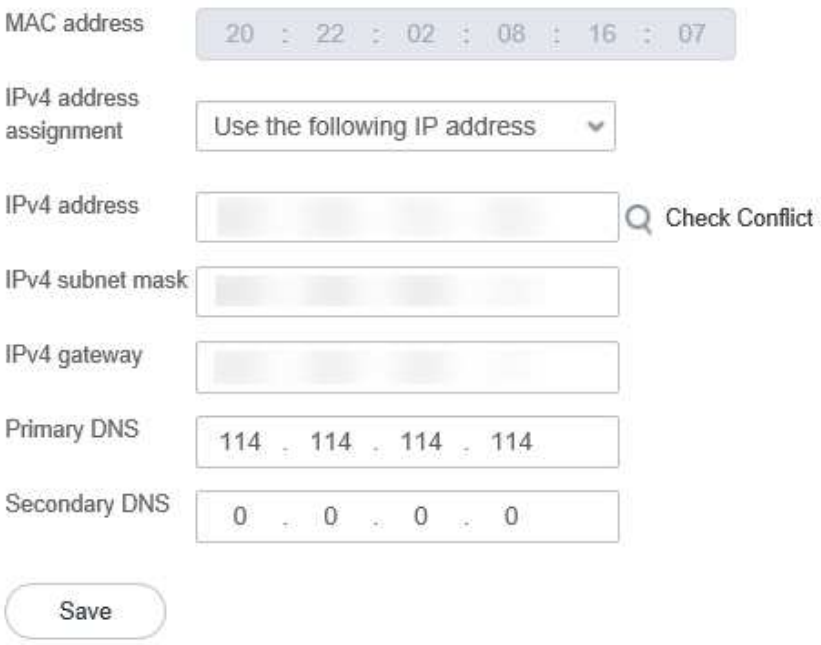
NOTE

- You need to configure an IPv4 gateway address for the network port that is set as the default network adapter. After the default network adapter is set, the device automatically generates a default route that maps the default network adapter.
- Ensure that the default network adapter is connected to the network device and the route is reachable.

Setting the IPv4 Address

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.
3. Click the **IP Address** tab. The **IP Address** area is displayed, as shown in Figure 1.

   Figure 1 IP Address area



4. Set camera IP addresses as planned. Table 1 describes the parameters.

Table 1 IP address parameters

Parameter	Description
MAC address	Camera MAC address. This parameter is read-only.
IPv4 address assignment	Method for obtaining the IPv4 address. The options are **Obtain IP address automatically** and **Use the following IP address**. **NOTE:** When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can select **Obtain IP address automatically** to check the IP address. The camera IP address allocated by the server is fixed.
IPv4 address	Camera IPv4 address. This parameter is available only when **IPv4 address assignment** is set to **Use the following IP address**. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. **NOTE:** • You can click the magnifier icon to check whether the current IP address is available.
IPv4 gateway	Gateway IP address of the network where the camera is located.
IPv4 subnet mask	Subnet mask of the network where the camera is located.
Primary DNS	Primary DNS IP address.

Parameter	Description
	NOTE: • Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. • Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland) and **8.8.8.8** (Google-provided) • If the cloud service is enabled and the domain name of the cloud service is not an IP address, you need to configure DNS when setting the camera IP address. Otherwise, the cloud service is in offline state.
Secondary DNS	Secondary DNS IP address. **NOTE:** • Enter the planned IP address or the actual IP address of the DNS server. IP addresses starting with 127 are invalid. You must enter an IP address starting with another value that ranges from 1 to 223. • Commonly used IP addresses of DNS servers: **114.114.114.114** (used by carriers in the Chinese mainland) and **8.8.8.8** (Google-provided)

5. Click **Save**.

Setting the IPv6 Address

The IPv6 address is numbered in hexadecimal notation and is divided into eight blocks by colons (:). Each block contains 16 bits, for example, fe80:0da8:65b4:05d3:1315:7c1f:0461:7847.

The following assumes that the local computer is directly connected to the camera. To set the IPv6 address, first change the local computer IP address to be on the same network segment as the camera IP address.

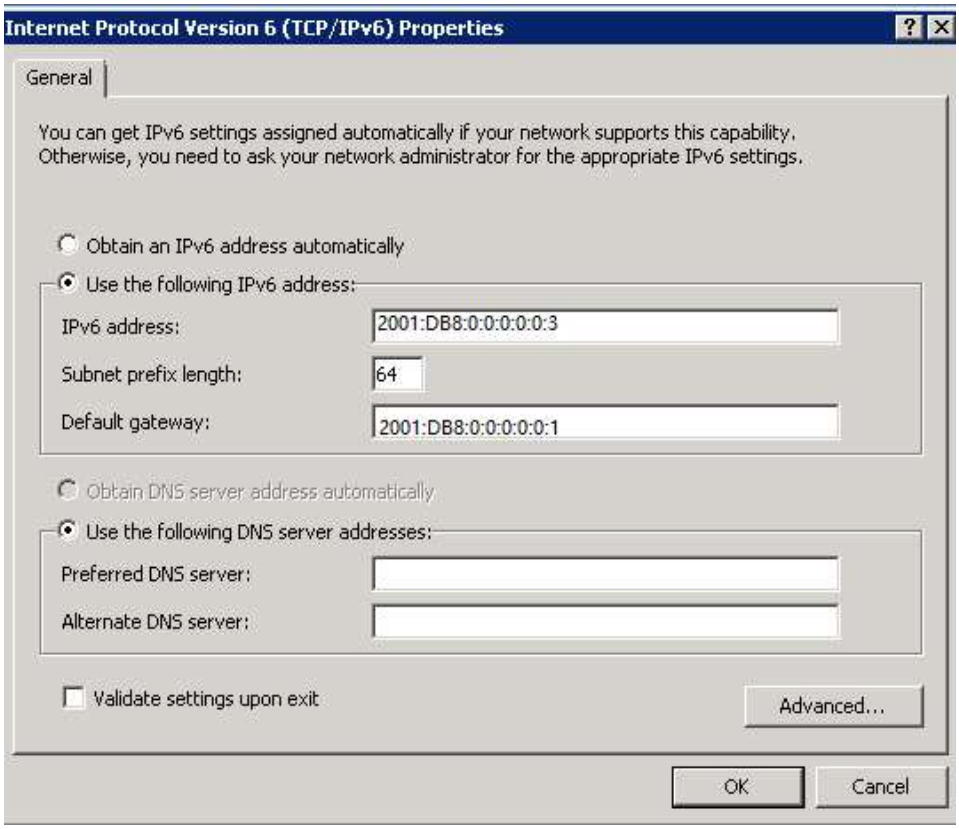
1. Set the IPv6 address of the local computer.

a. Run the **regedit** command on the local computer, choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **services** > **TCPIP6** > **Parameters**, delete **DisabledComponents**, and restart the local computer.

b. On the computer, choose **Control Panel** > **Network and Internet** > **Network and Sharing Center** to access the **Network and Sharing Center** page.

c. Click **Local Area Connection**. In the dialog box that is displayed, click **Properties**. In the dialog box that is displayed, double-click **Internet Protocol Version (TCP/IPv6) Properties**. The dialog box shown in Figure 2 is displayed. Change the computer IP address, subnet mask, and default gateway IP address to ensure that the computer IP address is on the same network segment as the camera IP address. For example, set the IPv6 address to **2001:DB8:0:0:0:0:0:3**.

Figure 2 Setting the IPv6 address of the local computer



2. Set the IPv6 address of the camera.

a. Log in to the camera web system (https://*Camera IP address*).

b. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.

c. Click **IP Address**, and select **Enable IPv6**.

The IPv6 address setting area is displayed, as shown in Figure 3.

Figure 3 Setting the IPv6 address of the camera

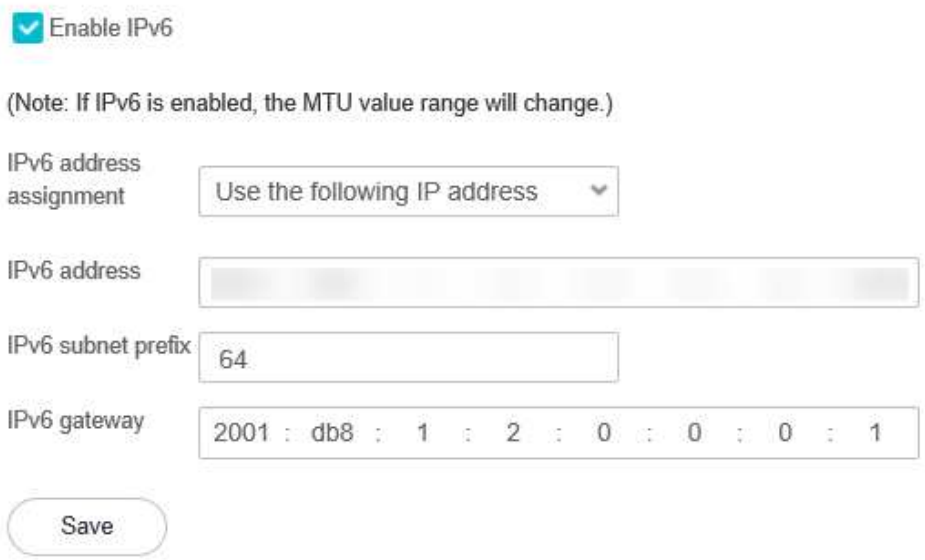


Table 2 IP address parameters

Parameter	Description
IPv6 address assignment	Method for obtaining the IPv6 address. The options are **Obtain IP address automatically**, **Use the following IP address**, and **Route advertisement**. **NOTE:** If the MTU value is less than 1280, the MTU value will change to **1500** after the IPv6 address is enabled. If the MTU value is greater than 1280, the MTU value remains unchanged after the IPv6 address is enabled.
IPv6 address	Camera IPv6 address.

Parameter	Description
IPv6 subnet prefix	IPv6 subnet prefix of the camera. Set the parameter to **64**.
IPv6 gateway	IPv6 gateway address of the camera. Set the parameter to **2001:DB8:0:0:0:0:0:1**.

d. Enter the camera IP address in the address box of the browser and press **Enter**. The camera login page is displayed.

Parent topic: Configuring TCP/IP

Setting Network Connectivity Detection

This section describes how to set network connectivity detection.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.
3. Click **Network Connectivity Detection**. The **Network Connectivity Detection** area is displayed, as shown in Figure 1.

   Figure 1 Network Connectivity Detection area

   - In the **Ping** area, select an IP protocol from the **IP mode** drop-down list box, set **IP Address**, and click **Start detection**.
   - In the **TCP Port Detection** area, set **IP Address** and **Port number**, and click **Start detection**.

Parent topic: Configuring TCP/IP

Setting MTU Parameters

The Maximum Transmission Unit (MTU) is the maximum size of a data packet that can be transmitted over the network. You can set MTU parameters to specify the maximum size of a data packet to be transmitted over the network to achieve the optimal transmission efficiency and quality.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.
3. In the **MTU Setting** area, set **MTU (bytes)**, as shown in Figure 1.

   Figure 1 MTU Settings area



NOTE

- The value of **MTU (bytes)** is an integer ranging from 800 to 1500. The default value is **1500**.
  - If IPv6 is enabled, the value of **MTU (bytes)** ranges from 1280 to 1500.
  - For camera models that support the IConnect protocol, do not change the value of **MTU (bytes)** to prevent camera disconnection.
- A small MTU value increases the system load. Enabling a high-consumption feature (such as SEC) results in high CPU usage. In this case, do not set a too small MTU value.

4. Click **Save**.

Parent topic: Configuring TCP/IP

Setting QoS Parameters

The Quality of Service (QoS) is a network security mechanism for resolving network issues such as delay and congestion. By setting QoS parameters, you can set the priority of media and signaling streams based on the network conditions to ensure transmission quality.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.
3. In the **QoS Settings** area, set **Media stream DSCP** and **Signaling stream DSCP**, as shown in Figure 1. DSCP is the abbreviation of differentiated services code point.

   Figure 1 QoS Settings area

   - Media stream: Indicates media streams that are transferred and played over the network in streaming mode, such as audio, video, and multimedia files.
   - Signaling stream: It is used to send signaling data, transmit control information, and deliver information such as registration requests and live video requests to the destination in a safe, reliable, and efficient manner.

NOTE

The two parameters can be set to integers ranging from 0 to 63. A larger value indicates a higher priority. The default values of **Media stream DSCP** and **Signaling stream DSCP** are both **0**.

4. Click **Save**.

Parent topic: Configuring TCP/IP

Setting Anti-Attack Parameters

You can set anti-attack parameters to defending the camera against network flood attacks.

Some camera models do not support this function.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP**.
3. In the **Anti-attack Settings** area, set **Max. packet receiving rate**, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 Anti-attack Settings area



Table 1 Parameter description

Parameter	Description
Max. packet receiving rate	Maximum rate for receiving unicast, broadcast, and multicast packets. If the receiving rate exceeds the specified limit, packet loss will occur. **NOTE:** • This parameter can be set to **0** or an integer ranging from **2000** to **50000**. • If **Max. packet receiving rate** is set to **0**, this function is disabled.
Broadcast/Multicast	If this parameter is selected, the rate for receiving broadcast or multicast packets is limited.

Parameter	Description
Unicast	If this parameter is selected, the rate for receiving unicast packets is limited.

4. Click **Save**.

Parent topic: Configuring TCP/IP

Setting Multicast Parameters

In multicast transmission mode, a sender sets up P2MP network connections with all recipients, improving data transmission efficiency and lowering the possibility of backbone network congestion.

NOTE

- For cameras that support dual network ports, you need to configure multicast information for the two network ports separately.
- For multi-channel cameras, you need to configure multicast information for the channels separately.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **TCP/IP** > **Multicast Settings**.
3. In the **Multicast Settings** area, set multicast parameters. Table 1 describes the parameters.

Figure 1 Setting multicast parameters

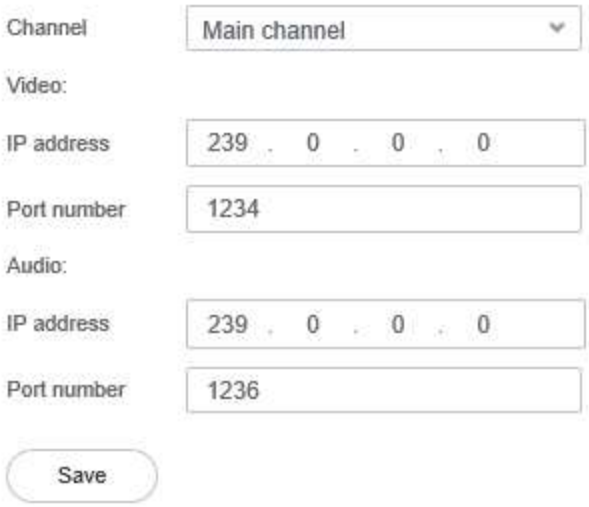


Table 1 Parameter description

Parameter	Description
IP address	Multicast IP address for video streams and audio streams. **NOTE:** The value range is 224.0.0.0 to 239.255.255.255
Port number	Multicast port number for video streams and audio streams.

4. Click **Save**.

Parent topic: Configuring TCP/IP

Configuring PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames.

Some camera models do not support this function.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **PPPoE**.

   The **PPPoE** tab page is displayed, as shown in Figure 1.

   Figure 1 PPPoE tab page

3. Set PPPoE parameters. Table 1 describes the parameters.
4. Click **Save**.

   Table 1 Parameter description

Parameter	Description
Enable	Indicates whether to enable the PPPoE function. To enable the function, select this parameter.
Dynamic device IP	Dynamic IP address that the server allocates to the current camera.
Authentication Mode	• **PAP**: Indicates cleartext password authentication. • **CHAP**: Indicates encrypted password authentication. The MD5 algorithm is used, which is a weak algorithm and

Parameter	Description
	may cause security risks. Use it on a trusted network. Otherwise, system security risks may occur. • **AUTO**: Indicates that the authentication mode is automatically matched based on that configured on the server. **NOTE:** The PAP authentication mode may cause security risks. Therefore, CHAP authentication is recommended.
User name/Password/Confirm password	User name and password (configured on the server side) used for authentication on the camera side.

NOTICE

- After PPPoE is enabled, the local IP address of the device cannot be set.
- After PPPoE is enabled, the IP address of the device will change when the device is restarted, upgraded, or downgraded.
- PPPoE and LTE are mutually exclusive.
- PPPoE and the cloud service function are mutually exclusive.

Parent topic: Setting Basic Network Parameters

Configuring Ports

This section describes how to configure ports and port mapping in the camera web system.

Setting Port Parameters This section describes how to configure the HTTP port, HTTPS port, and Real-Time Streaming Protocol (RTSP) port of the camera.

Setting Port Mapping Parameters
After NAT environment is configured, map devices in the internal NAT network to ports of the extranet.

Parent topic: Setting Basic Network Parameters

Setting Port Parameters

This section describes how to configure the HTTP port, HTTPS port, and Real-Time Streaming Protocol (RTSP) port of the camera.

NOTE

For cameras that support dual network ports, you need to configure port information for the two network ports separately.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **Port** > **Port Settings**.
3. The **Port Settings** area is displayed, as shown in Figure 1.

   Figure 1 Port Settings area

4. Enter an integer ranging from 1 to 65535 in the text boxes of **HTTP port**, **HTTPS port**, and **RTSP port**.
5. Click **Save**.

Parent topic: Configuring Ports

Setting Port Mapping Parameters

After NAT environment is configured, map devices in the internal NAT network to ports of the extranet.

NOTE

For cameras that support dual network ports, you need to configure port mapping for the two network ports separately.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **Port** > **Port Mapping**.
3. The **Port Mapping** area is displayed, as shown in Figure 1.

   Figure 1 Port Mapping area

4. Enter an integer ranging from 1 to 65535 in the text box of **Post-NAT RTSP port**.

   NOTICE

   The value of this parameter must be the same as the RTSP port number configured for NAT on the router. Otherwise, the web client will fail to obtain the live video stream.

5. Click **Save**.

Parent topic: Configuring Ports

Setting Advanced Network Parameters

You can set advanced network parameters, such as FTP, SSH/SFTP, and SNMP parameters.

Setting FTP Parameters Cameras can upload snapshots to a preconfigured FTP server through FTP or SFTP.

Configuring the SSH/SFTP Service
You can configure the SSH/SFTP service to prevent information leakage during remote camera management.

Setting SNMP Parameters
By setting Simple Network Management Protocol (SNMP) parameters, you can view and modify camera configurations in the network management system (NMS), which facilitates camera maintenance and management.

Setting Email Parameters
This section describes how to set Simple Mail Transfer Protocol (SMTP) parameters so that emails can be sent when an alarm is reported.

Setting 802.1X Parameters
802.1X is a network connection protocol used to authenticate devices connected to the network. It can prevent unauthorized users or devices from accessing the LAN/WLAN through an access port.

Configuring Intelligent Acceleration
This section describes how to set parameters related to intelligent network acceleration.

Parent topic: Setting Network Parameters

Setting FTP Parameters

Cameras can upload snapshots to a preconfigured FTP server through FTP or SFTP.

For details about how to set the language for naming snapshots, see Table 4 in Basic Information.

NOTE

- If the FTP software is required on the server, the **Serv-U FTP Server** software is recommended. The **Easy FTP Server** is not recommended to prevent exceptions.
- When multiple services that require storage are enabled simultaneously (for example, video recording and snapshot taking are enabled simultaneously), a high-speed card (for example, SDXC U3) is recommended to prevent loss of recordings or images stored on the microSD card due to insufficient storage performance.
- The FTP attributes vary depending on the camera model.
- If both the FTP and SFTP servers are enabled, the **Server IP address**, **Port**, **Transmission format**, **User name**, and **Password** parameters must be set to the actual values of the selected protocol under **FTP Settings**.
- If the SFTP root directory is deleted, the camera fails to connect to the SFTP server. In this case, you are advised to restart the SFTP server.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP**. The snapshot upload configuration tab page is displayed.
   - Figure 1 shows the snapshot upload configuration page.
   - Figure 2 shows the snapshot upload configuration tab page for general-purpose intelligent cameras in micro checkpoint mode.

Figure 1 Snapshot upload configuration tab page



Figure 2 Snapshot upload configuration tab page in micro checkpoint mode



3. Set **FTP attribute**. You can set **FTP attribute** to **Target and person**, **Object classification**, **Micro checkpoint**, or **Other**.
    - For target capture cameras, you can set **FTP attribute** to **Target/Person** or **Other**.
    - For general-purpose intelligent cameras, you can set **FTP attribute** based on the intelligent mode of the cameras.
        - Micro checkpoint mode: The options include **Object classification**, **Micro checkpoint**, and **Other**.
        - Target checkpoint mode: The options include **Target/Person** and **Other**.
        - Behavior analysis mode: Only the **Other** option is available.

NOTE

- After switchover between application modes, you need to configure the FTP parameters in the current mode.
- On the **1 + N** page, after you switch the intelligent analysis mode among target checkpoint, micro checkpoint, full intelligence, and live video, you also need to configure FTP parameters in the current mode.

NOTICE

- A camera supports settings of FTP parameters and image naming parameters under only one FTP attribute.
  - For example, if you set **FTP attribute** to **Target/Person** and set related FTP parameters and image naming parameters, and then, set **FTP attribute** to **Other** and set related FTP parameters, only the last configuration will be saved.
  - For example, if you set **FTP attribute** to **Object classification** and set related FTP parameters and image naming parameters, and then, set **FTP attribute** to **Micro checkpoint** and set related FTP parameters and image naming parameters, only the last configuration will be saved.

4. Select **Enable** to enable FTP.
5. Set snapshot upload parameters. Table 1 describes the parameters.

NOTICE

- Ensure that the image storage server has plenty of storage space. Otherwise, images will fail to be uploaded. You are advised to periodically back up and delete images on the storage server.
- To ensure integrity of uploaded data, ensure that the upload rate is greater than the image storage rate of the camera.

Table 1 Snapshot upload parameters

Parameter	Description
Check	Used to check whether the FTP parameters you set are valid.

Parameter	Description
	Check result description: • If a message is displayed indicating that the FTP server is successfully connected, the server IP address is available. • If a message is displayed indicating that the FTP server is unreachable, the server IP address is unreachable. • If a message is displayed indicating incorrect server IP address or port number, the server IP address or port number is incorrectly set and the FTP server fails to be connected. • If a message is displayed indicating incorrect user name or password, the authentication fails due to incorrect user name or password.
Protocol	Protocol used for uploading snapshots to the target server. • **SFTP**: secure file transfer protocol, providing an encryption method for transferring files. • **FTP**: file transfer protocol. **NOTE:** FTP may cause security risks. It is recommended that SFTP be used.
Server IP address	IP address of the target server to which snapshots are uploaded.
Port	Port number of the target server to which snapshots are uploaded.
User name	User name configured on an FTP/SFTP server, which is used to upload snapshots to the FTP/SFTP server.
Password	Password configured on an FTP/SFTP server, which is used to upload snapshots to the FTP/SFTP server.
Naming rule	Rule for naming the FTP directory structure.
Directory	Path for storing snapshots on the target server.

Parameter	Description
	• **Root directory**: The uploaded image is saved in the root directory of the target server. • **Level-*X* directory**: The uploaded image is saved in the level-*X* directory of the target server. **NOTE:** The path length cannot be too long. If the total length of the path exceeds the maximum length specified by the operating system running on the SFTP or FTP server, paths cannot be created and images cannot be uploaded.
Level-*X* directory	Level-*X* directory, which can be named by a variety of elements such as **Device IP**, **Time**, and **Custom**. The naming elements are subject to the actual ones displayed on the web page. **NOTE:** • When customizing a directory, you can define a deeper level of directory structure by using backslashes (\). • If you select **Intelligent classification**, the captured image will be stored to a specific directory based on the type of a captured object (for example, pedestrian).

6. Click **Save**.

Parent topic: Setting Advanced Network Parameters

Configuring the SSH/SFTP Service

You can configure the SSH/SFTP service to prevent information leakage during remote camera management.

The web page varies depending on the camera model.

Configuring the SSH Service

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SSH/SFTP** > **SSH Configuration**.

   The **SSH Configuration** area is displayed, as shown in Figure 1.

   Figure 1 SSH Configuration area

3. Select **Enable SSH**.
4. Click **Save**.

> **NOTE**
>
> - To access the camera through the enabled SSH service, you need to use port 22.
> - The system will disable the SSH service if the enabled SSH service is not used within two hours.

Configuring the SFTP Service

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SSH/SFTP** > **SFTP Configuration**.

   The **SFTP Configuration** area is displayed, as shown in Figure 2.

Figure 2 SFTP Configuration area



3. Select **Enable SFTP**.
4. Click **Save**.

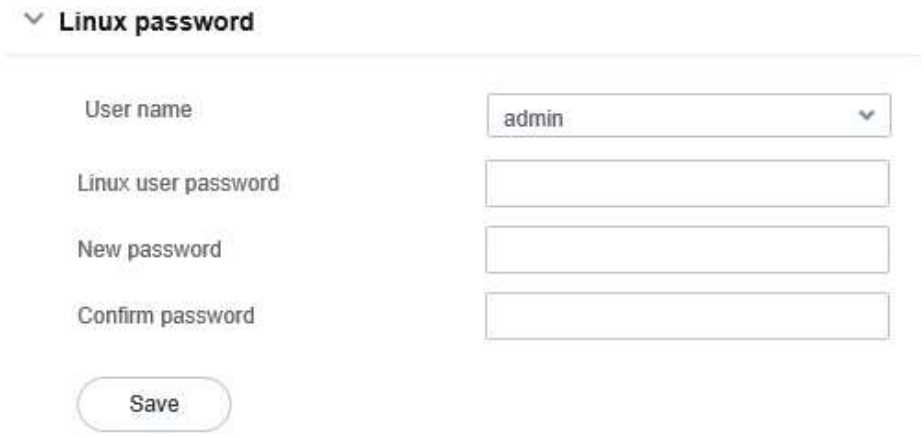
> **NOTE**
>
> - To access the camera through the enabled SFTP service, you need to use port 20022.
> - The system will disable the SFTP service if the enabled SFTP service is not used within two hours.

Managing Linux Passwords

You can change the passwords of the **admin** and **root** users for logging in to the Linux operating system.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SSH**.
3. Click **Linux password**. The **Linux password** area is displayed, as shown in Figure 3.

Figure 3 Linux password area



4. Select a user name. Table 1 describes the options.

   Table 1 User description

User Name	Description
admin	Used to log in to the Linux operating system.
root	Used to log in to the Linux operating system as the administrator.

5. Set **Linux user password**, **New password**, and **Confirm password**.
6. Click **Save**.

Parent topic: Setting Advanced Network Parameters

Setting SNMP Parameters

By setting Simple Network Management Protocol (SNMP) parameters, you can view and modify camera configurations in the network management system (NMS), which facilitates camera maintenance and management.

Some camera models do not support this function.

Context

When the camera is connected to the NMS through the SNMP protocol, you can obtain and modify camera configurations in the NMS.

The SNMP protocol includes SNMP v1, SNMP v2c, and SNMP v3.

CAUTION

SNMPv1 and SNMPv2c have security risks. For security purposes, you are advised to use SNMPv3 and set **Key protocol** to **AES**.

The camera can report related information to the NMS.

You can set SNMP parameters based on the site requirements.

Setting SNMP v1/v2c Parameters When SNMP v1 or SNMP v2c is used, the NMS visits the camera using a community name with the read-only or read-write permission.

Setting SNMP Trap Parameters
A camera can report information to the NMS. In this case, you need to set SNMP trap parameters.

Setting SNMP v3 User Information
When SNMP v3 is used, the NMS visits the camera using a user account in secure access mode. Different user accounts have different access rights.

Parent topic: Setting Advanced Network Parameters

Setting SNMP v1/v2c Parameters

When SNMP v1 or SNMP v2c is used, the NMS visits the camera using a community name with the read-only or read-write permission.

Context

Two sets of interaction parameters have been set by default. You can use the default settings, or click **Modify** or **Delete** to modify or delete them. When SNMP v1 or SNMP v2c is used, you can set a maximum of three sets of interaction parameters. This section mainly describes how to add a set of interaction parameters.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SNMP**.

   The **SNMP** tab page is displayed, as shown in Figure 1.

   > **NOTE**
   >
   > The SNMP v1/v2 protocol has security risks. Exercise caution when using them. You are advised to use the SNMP v3 protocol.

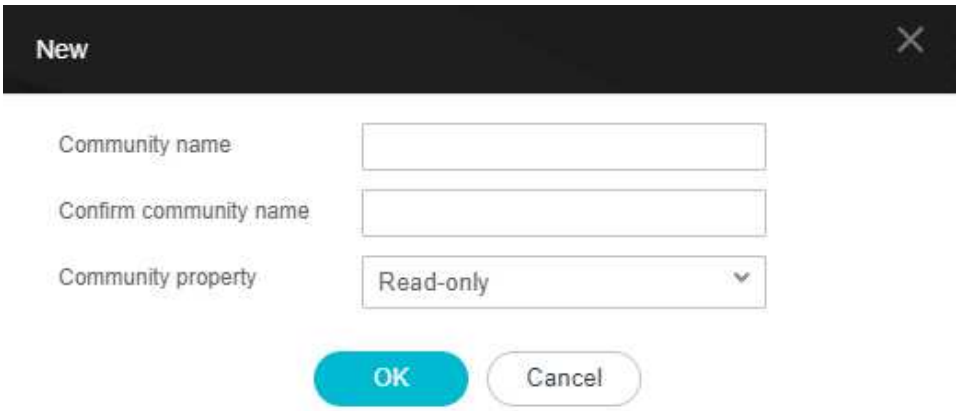
   Figure 1 Setting SNMP parameters

3. In the **SNMP v1/v2c Settings** area, click **Add**.

   The dialog box for setting SNMP v1/v2c parameters is displayed, as shown in Figure 2.

Figure 2 Setting SNMP v1/v2c parameters



4. Set **Community name**, **Confirm community name**, and **Community property**.

   If **Community property** is set to **Read-only**, you can only view camera configurations in the NMS.

   If **Community property** is set to **Read and write**, you can view and modify camera configurations in the NMS.

5. Click **OK**.

   The **SNMP** page is displayed.

6. Click **Save**.

Parent topic: Setting SNMP Parameters

Setting SNMP Trap Parameters

A camera can report information to the NMS. In this case, you need to set SNMP trap parameters.

NOTICE

All SNMP event trap parameters on the camera except for **Recipient IP** must be the same as those in the NMS. If they are different, the camera may fail to report information to the NMS.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SNMP**.

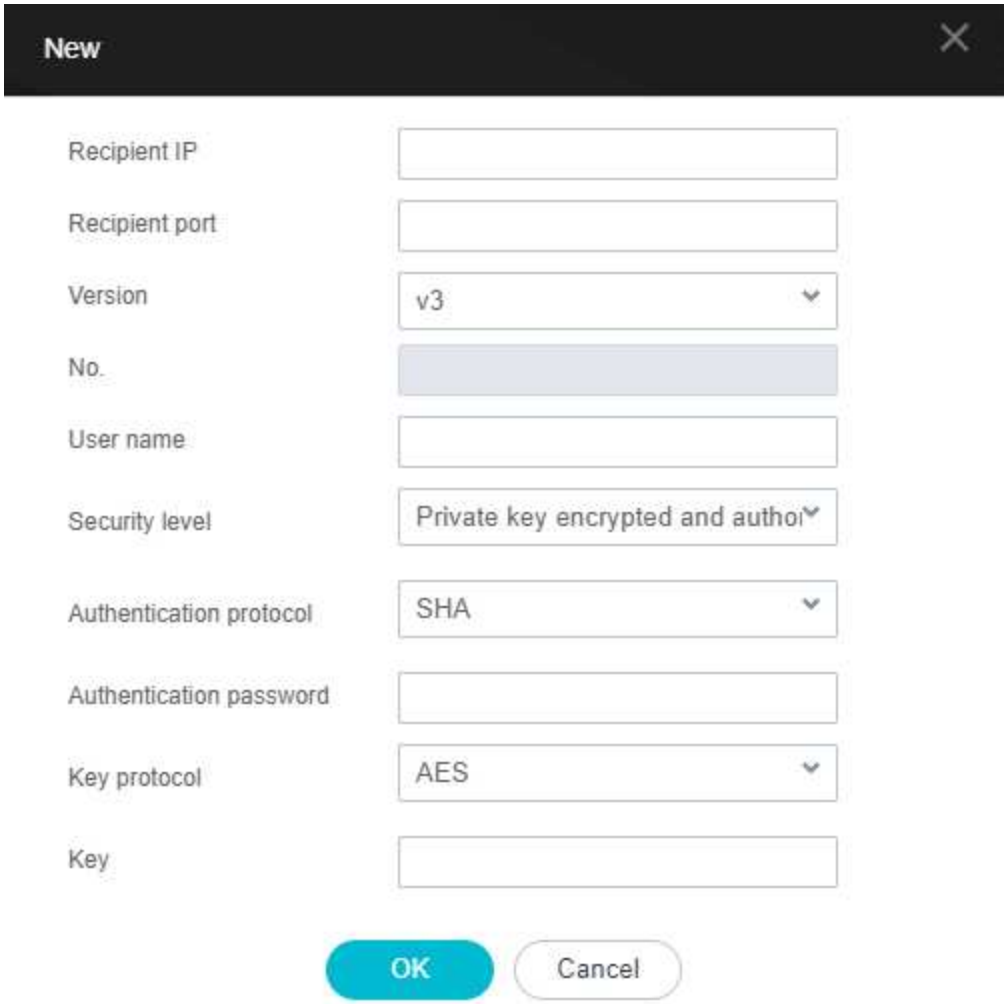
   NOTE

   The SNMP v1/v2 protocol has security risks. Exercise caution when using them. You are advised to use the SNMP v3 protocol.

3. In the **SNMP Trap Settings** area, click **Add**.

   The dialog box for setting SNMP trap parameters is displayed, as shown in Figure 1.

Figure 1 Setting SNMP trap parameters



4. Table 1 describes the parameters.

Table 1 SNMP trap parameters

Parameter	Description
Recipient IP	NMS IP address.
Recipient port	NMS port number.
Version	Version number of the SNMP protocol used for connecting the camera to the NMS.
No.	This parameter is available only when **Version** is set to **v1** or **v2**.

Parameter	Description
	Community name used by the camera to access the NMS.
User name	This parameter is available only when **Version** is set to **v3**. User name used by the camera to access the NMS.
Security level	This parameter is available only when **Version** is set to **v3**. Security level of user rights. The options are as follows: • **Unauthorized**: Users are not allowed to view or modify information about the camera. • **Authorized**: Users can only view information about the camera. • **Private key encrypted and authorized**: Users can view and modify information about the camera.
Authentication protocol	This parameter is available only when **Version** is set to **v3** and **Security level** is set to **Authorized** or **Private key encrypted and authorized**. Protocol used by the camera for authentication on the NMS.
Authentication password	This parameter is available only when **Version** is set to **v3** and **Security level** is set to **Authorized** or **Private key encrypted and authorized**. Password used by the camera for authentication on the NMS.
Key protocol	This parameter is available only when **Version** is set to **v3** and **Security level** is set to **Private**

Parameter	Description
	key encrypted and authorized. Private key protocol used by the camera for authentication on the NMS.
Key	This parameter is available only when **Version** is set to **v3** and **Security level** is set to **Private key encrypted and authorized**. Key used by the camera for authentication on the NMS. **NOTE:** • For security purposes, it is recommended that the value of **Key** be different from that of **Authentication password**.

5. Click **OK**.

   The **SNMP** page is displayed.

6. Click **Save**.

NOTE

To ensure that the SNMP ColdStart event is reported, perform the following configurations on the switch:

- Contact related vendors to obtain the configuration method.

Parent topic: Setting SNMP Parameters

Setting SNMP v3 User Information

When SNMP v3 is used, the NMS visits the camera using a user account in secure access mode. Different user accounts have different access rights.

Context

If SNMP v3 is used, you can configure a maximum of three SNMP v3 users. This section describes how to configure user information.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **SNMP**.

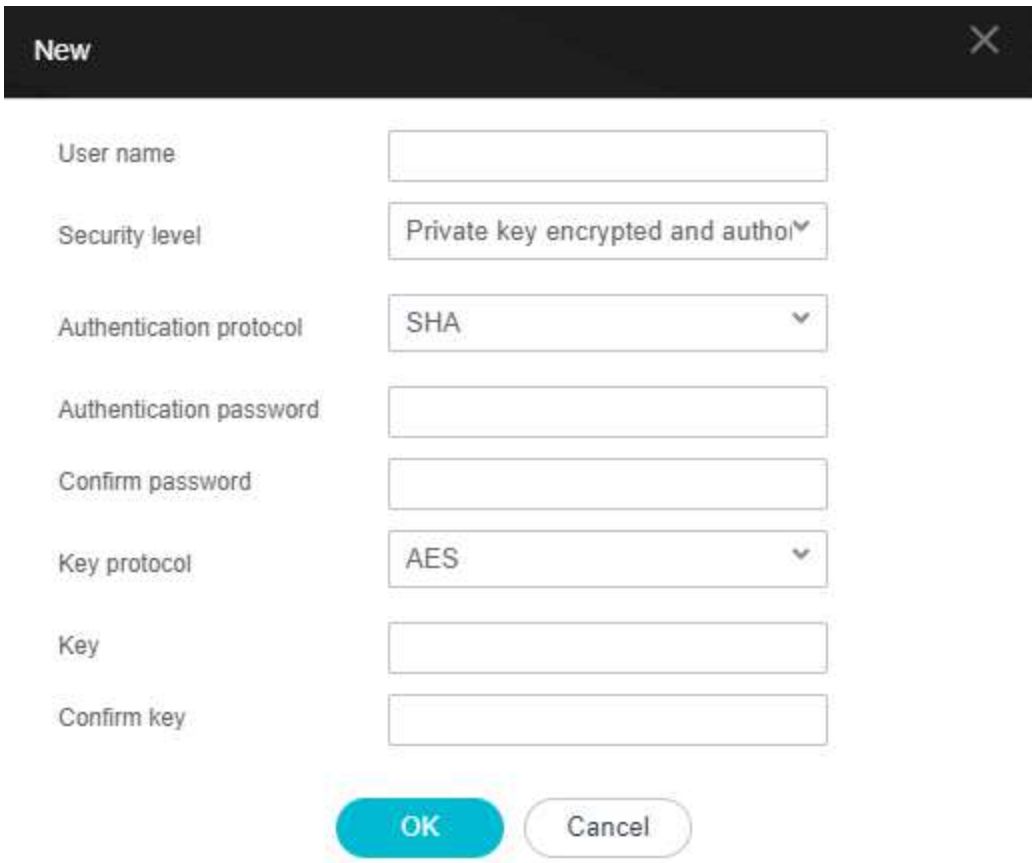
   NOTICE

   The SNMP v1/v2 protocol has security risks. Exercise caution when using them. You are advised to use the SNMP v3 protocol.

3. In the **SNMP v3 User Info** area, click **Add**.

   The dialog box for configuring SNMP v3 user information is displayed, as shown in Figure 1.

Figure 1 Setting SNMP v3 user parameters



4. Table 1 describes the parameters.

Table 1 SNMP v3 user parameters

Parameter	Description
User name	User name for the NMS to visit the camera. This parameter is set on the camera, which must be the same as that configured in the NMS. **NOTE:** • A user name must consist of 5 to 16 characters. • A user name can contain digits, uppercase letters, and lowercase letters.

Parameter	Description
Security level	Security level of user rights. The options are as follows: • **Unauthorized**: Users are not allowed to view or modify information about the camera. • **Authorized**: Users can only view information about the camera. • **Private key encrypted and authorized**: Users can view and modify information about the camera.
Authentication protocol	This parameter is available only when **Security level** is set to **Authorized** or **Private key encrypted and authorized**. MD5 is a weak algorithm and may cause security risks. Use it on a trusted network. Otherwise, system security risks may occur. Protocol used for user authentication.
Authentication password	This parameter is available only when **Security level** is set to **Authorized** or **Private key encrypted and authorized**. Password used for user authentication.
Confirm password	This parameter is available only when **Security level** is set to **Authorized** or **Private key encrypted and authorized**. Confirm password for user authentication.
Key protocol	This parameter is available only when **Security level** is set to **Private key encrypted and authorized**. Private key protocol used for user authentication.

Parameter	Description
	NOTE: The DES protocol is risky. You are advised to use the AES protocol.
Key	This parameter is available only when **Security level** is set to **Private key encrypted and authorized**. Key used for user authentication. **NOTE:** • For security purposes, it is recommended that the value of **Key** be different from that of **Authentication password**.
Confirm key	Confirm key for user authentication.

5. Click **Save**.

Parent topic: Setting SNMP Parameters

Setting Email Parameters

This section describes how to set Simple Mail Transfer Protocol (SMTP) parameters so that emails can be sent when an alarm is reported.

Context

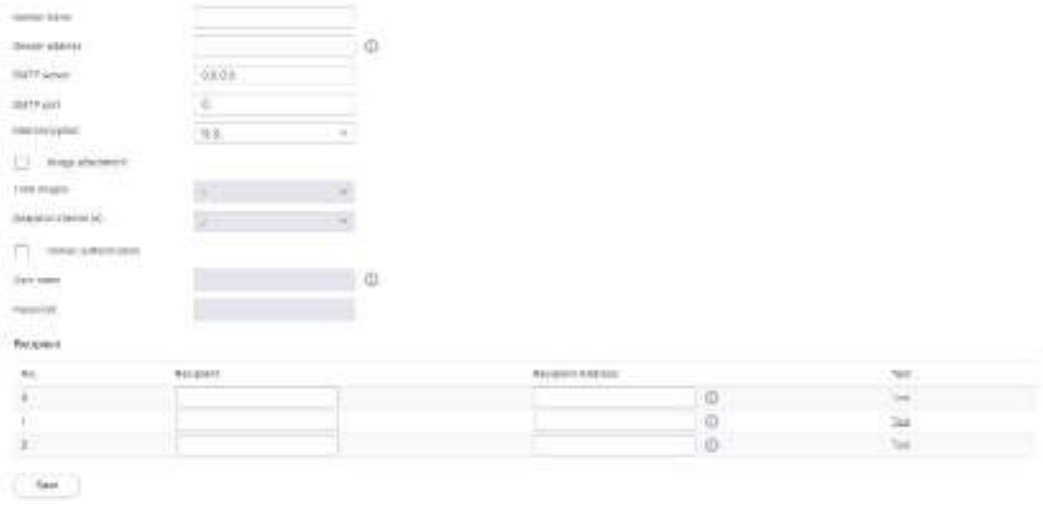
When an alarm event occurs, cameras can send alarm information through emails containing attachments to customers by using the SMTP protocol.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Email**.

   The **Email** tab page is displayed, as shown in Figure 1.

   Figure 1 Setting email parameters

3. Set email parameters. Table 1 describes the parameters.

   Table 1 Email parameters

Parameter	Description

Parameter	Description
Sender name	Name of the sender, for example, **admin**.
Sender address	Email address of the sender, in the format of admin@*XXX*.com.
SMTP server	IP address or mailbox domain name of the email server.
SMTP port	Port number of the email server.
Mail encryption	Mode for encrypting emails. The options are as follows: **TLS**, **SSL**, and **No encryption**. It is recommended that the server use **TLS1.1** or **TLS1.2** to encrypt mails. Otherwise, there will be security risks.
Image attachment	Includes two parameters: **Total images** and **Snapshot interval (s)**, of which, **Total images** specifies the number of images contained in an email, and **Snapshot interval (s)** specifies the interval at which these images are captured.
Server authentication	The user name and password must be the same as those of the SMTP server.
Recipient	Recipient's name and email address. You can click **Test** to check whether the recipient can properly receive emails.

4. Click **Save**.

Parent topic: Setting Advanced Network Parameters

Setting 802.1X Parameters

802.1X is a network connection protocol used to authenticate devices connected to the network. It can prevent unauthorized users or devices from accessing the LAN/WLAN through an access port.

If 802.1X parameters have been set for the switch on the network, the 802.1X parameters also need to be set on the camera. Otherwise, you may fail to access the camera.

Setting Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **802.1X**.

   The **802.1X** tab page is displayed, as shown in Figure 1.

   Figure 1 Setting 802.1X parameters



3. Select **Enable**.
4. Set **Protocol**. The options are **EAP-TLS** and **EAP-MD5/EAP-TLS**.

> **NOTE**
>
> - If the network switch uses the MD5 authentication mode, **EAP-MD5/EAP-TLS** must be selected. Otherwise, the

authentication will fail.

- Enabling EAP-MD5 may cause security risks. Exercise caution when enabling EAP-MD5.

5. Set **EAPOL version**, **EAP identity**, and **Password**. EAPOL is short for extensible authentication protocol over LAN.

> **NOTE**
>
> - Obtain specific parameter values from the network administrator.
> - If **Protocol** is set to **EAP-TLS**, you do not need to enter the password.

6. Click **Save**.

Renewing the Certificate

1. Choose **Configuration** > **Network** > **Advanced Settings** > **802.1X** > **Certificate Management**. The **Certificate Management** area is displayed, as shown in Figure 2.

   Figure 2 Certificate Management area



> **NOTE**
>
> For a device that supports dual network ports (ETH0 and ETH1), the two network ports share the same certificate.

2. Set parameters in the **Certificate Management** area. Table 1 describes the parameters.

Table 1 Certificate management parameters

Parameter	Description	How to Set

Parameter	Description	How to Set
CA certificate file (.cer)	CA certificate.	You can upload your own certificate. 1. Click **Browse** and select a CA certificate file. 2. Click **Upload**. 3. Click **Browse** and select a certificate file. 4. Click **Browse** and select a private key file. 5. Click **Upload**. 6. Enter the password of the private key file in the dialog box that is displayed. **NOTE:** • The certificate chain is not supported. • The password of the private key file must be the same as that generated when you apply for the private key file.
Certificate file (.pem)	Digital information file that identifies and verifies both parties involved in network communication.	
Key file (.pem)	Key file that contains the certificate key.	

Parent topic: Setting Advanced Network Parameters

Configuring Intelligent Acceleration

This section describes how to set parameters related to intelligent network acceleration.

Some camera models do not support this function.

Setting Bandwidth Adaptive Parameters With the bandwidth adaptive function enabled, the camera will use an appropriate bit rate that best suits the current network conditions to transfer video images. This approach ensures the image quality.

Setting TCP Intelligent Acceleration Parameters
You can configure TCP intelligent acceleration to increase the throughput in scenarios with packet loss or high latency, for example, wireless applications.

Setting Traffic Shaping Parameters
You can set the rate for sending data to ensure stable network bandwidth occupation and enhance stability and reliability of video stream transmission.

Setting Super Error Concealment Parameters
Super Error Concealment (SEC) is a bit error correction technology that can enhance data transmission reliability.

Parent topic: Setting Advanced Network Parameters

Setting Bandwidth Adaptive Parameters

With the bandwidth adaptive function enabled, the camera will use an appropriate bit rate that best suits the current network conditions to transfer video images. This approach ensures the image quality.

Prerequisites

The following configurations have been performed:

- Set **Stream type** to **Primary stream**.
- Set **Encoding protocol** to H.265 or other related formats.
- Set **Bit rate type** to **Constant bit rate**.
- Disable dynamic bit rate.

NOTE

- You are advised not to enable the stream smoothing function when the bandwidth adaptive function is enabled. Otherwise, the bandwidth may be inaccurately calculated.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **Intelligent Acceleration**.
3. Click **Adaptive Bandwidth**. The **Adaptive Bandwidth** area is displayed, as shown in Figure 1.



Figure 1 Adaptive Bandwidth area

4. Select **Adaptive bandwidth**.
5. Click **Save**.

Parent topic: Configuring Intelligent Acceleration

Setting TCP Intelligent Acceleration Parameters

You can configure TCP intelligent acceleration to increase the throughput in scenarios with packet loss or high latency, for example, wireless applications.

Prerequisites

- If TCP intelligent acceleration is enabled and packet loss and high latency occur on the network, you are advised not to enable traffic shaping.
- If the camera bit rate is 12 Mbit/s or above and the computer runs Windows 10 or earlier, you need to run the **netsh interface tcp set heuristics disabled** command in the DOS window of the computer to disable the window restriction on Windows. Otherwise, the service performance is affected.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Intelligent Acceleration**.
3. Click **TCP Intelligent Acceleration**. The **TCP Intelligent Acceleration** area is displayed, as shown in Figure 1.

   Figure 1 TCP Intelligent Acceleration area

4. Select **Enable**.
5. Click **Save**.

Parent topic: Configuring Intelligent Acceleration

Setting Traffic Shaping Parameters

You can set the rate for sending data to ensure stable network bandwidth occupation and enhance stability and reliability of video stream transmission.

Prerequisites

You have set the encoding protocol to H.265 or other related formats and disabled the VBR.

NOTE

- You are advised not to set bandwidth adaptive parameters when the traffic shaping function is enabled. Otherwise, the bandwidth information cannot be accurately reflected.
- If the traffic shaping function is enabled, when you set video stream parameters, change the traffic shaping coefficient, or manually disable the traffic shaping function, video mosaic may occur and last for about one second.
- If the traffic shaping function is enabled, lip synchronization is not supported.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Intelligent Acceleration**.
3. Click **Traffic Shaping**. The **Traffic Shaping** area is displayed, as shown in Figure 1.

Figure 1 Traffic Shaping area



4. Select **Enable**.

> **NOTE**
>
> If you set **Encoding protocol** to H.265 or other related formats, disable VBR, and click **Save**, the settings take effect only after you request media streams again.

5. Select **Plug-in delay**.

> **NOTE**
>
> - The plug-in delay function is valid only after the traffic shaping function is enabled.
> - If the plug-in delay function is enabled, live video freezing and artifacts issues can be resolved in the case of traffic shaping. However, live video images will be delayed.

6. Set **Traffic shaping coefficient**.

> **NOTE**
>
> - The value of **Traffic shaping coefficient** ranges from 1.3 to 4.0 at a step of 0.1. A smaller coefficient indicates a higher compression ratio, smoother images, and lower bandwidth requirements but longer delay. The default value is **4.0**.
> - The traffic shaping function must be supported by the cache capability on the decoding side. Set a proper **Traffic shaping coefficient** based on the actual network bandwidth. It is

recommended that the default value be used or decoding cache be increased.

7. Click **Save**.

Parent topic: Configuring Intelligent Acceleration

Setting Super Error Concealment Parameters

Super Error Concealment (SEC) is a bit error correction technology that can enhance data transmission reliability.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Basic Settings** > **Intelligent Acceleration**.
3. Click **Super Error Concealment**. The **Super Error Concealment** area is displayed, as shown in Figure 1.

   Figure 1 Super Error Concealment area

4. Select **Enable**.

   NOTE

   This setting is applicable when the network bandwidth is sufficient but packet loss or bit errors occur on the network and the UDP protocol is used for transmitting media streams. (Only H.265 and other related encoding formats are supported.)

5. Select a packet loss rate from the **Packet loss rate** drop-down list box.

   A larger packet loss rate requires a larger SEC bit rate, that is, more extra bandwidth. Table 1 lists mappings between SEC packet loss rates and SEC bit rates.

   Table 1 Mappings between SEC packet loss rates and SEC bit rates

Configuring Platform Connection

Cameras can connect to video security platforms through the SDK, GB/T 28181, or ONVIF protocol. Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera.

NOTE

- In the scenario of requesting streams through RTP Over TCP, the camera does not send RTCP packets.
- It is recommended that a maximum of three light-intelligence cameras be connected.

Setting Media Stream Keep-Alive Parameters You can set media stream keep-alive parameters to ensure that media streams can be properly requested when the platform is connected through protocols such as SDK or ONVIF.

Configuring Password Management
To ensure data security, change the passwords of platform connection protocols in a timely manner. After the passwords are changed, record and save them in a timely manner.

Configuring Connection to the Platform Through the SDK Protocol
This section describes how to connect a camera to the IVS platform through the SDK protocol.

Configuring Connection to the Platform Through the ONVIF Protocol

Configuring Connection to the Platform Through the GB/T 28181 Protocol
The section describes how to connect a camera to the IVS

platform through GB/T 28181. The GB/T 28181 protocol supports only the active access mode.

Configuring Connection to the Platform Through the GA/T 1400 Protocol
This section describes how to connect a camera to the IVS platform or a third-party platform through the GA/T 1400 protocol.

Configuring Connection to the Platform Through RESTful
This section describes how to connect a camera to the IVS platform through the RESTful protocol.

Configuring Connection to the Platform Through RTSP
RTSP is an application-level protocol for the controls, such as play, pause, and fast-forward, of real-time streaming data.

Setting IConnect Parameters

Configuring Cloud Service Connection
After a camera is connected to the cloud service, you can view live and recorded video from the camera on your mobile app. The capabilities supported vary between camera models.

Parent topic: Configuration

Setting Media Stream Keep-Alive Parameters

You can set media stream keep-alive parameters to ensure that media streams can be properly requested when the platform is connected through protocols such as SDK or ONVIF.

1. Log in to the camera web system and choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters**. The area shown in Figure 1 is displayed.

   Figure 1 Setting media stream keep-alive parameters

2. Set media stream keep-alive parameters. Table 1 describes the parameters.

   Table 1 Media stream keep-alive parameters

Parameter	Description
Enable media stream keep-alive	Indicates whether to enable the keep-alive function for media streams, which is mandatory when the media stream request mode is used. When the camera is connected to the platform through the SDK, GB/T 28181, GB 35114, ONVIF, or RESTful protocol, the media stream request mode is used. If the platform supports the keep-alive function, you are advised to select **Enable media stream keep-alive**.
Keepalive duration (s)	Media stream keep-alive duration. The default value is 60s. If the camera does not receive a media stream request within the keep-alive duration, the camera stops sending media streams.
Device ID	Unique ID of a device. **NOTE:** For a multi-channel model, the device ID must be unique and the device ID of at least one channel must be set.

Parameter	Description

Parent topic: Configuring Platform Connection

Configuring Password Management

To ensure data security, change the passwords of platform connection protocols in a timely manner. After the passwords are changed, record and save them in a timely manner.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**.
3. Click **Password Management**. Under **Password Management**, you can change the SDK, northbound interface, and ONVIF passwords.
4. Use SDK password management as an example. Click the **SDK Password** tab. The **SDK Password** tab page is displayed, as shown in Figure 1.

   Figure 1 SDK Password tab page

5. Set **Web user password**, **New password**, and **Confirm password**.
   - The value of **Web user password** is the password of the **admin** user for logging in to the camera.
   - The value of **Confirm password** must be the same as that of **New password**.

> **NOTE**
>
> - For security purposes, you are advised to periodically (every 90 days recommended) change the password and ensure that the password is not used repeatedly.
> - For security purposes, you are advised not to set the new password to a weak password. To configure a weak password dictionary, choose **Configuration** > **System** > **Security Management** > **Password Management** > **Weak Password Dictionary**.

6. Click **Save**.

Parent topic: Configuring Platform Connection

Configuring Connection to the Platform Through the SDK Protocol

This section describes how to connect a camera to the IVS platform through the SDK protocol.

Cameras can register with the IVS platform through the SDK protocol in active or passive (default) mode. The following describes the differences between the active and passive registration modes:

- Passive registration

  In passive registration mode, the platform proactively initiates a registration request to a camera. The platform information does not need to be configured on the camera side. You can add cameras on the IVS platform by following a wizard.

- Active registration

  In active registration mode, an SDC actively registers with the platform. You need to set the platform IP address and port number on the SDC side. You can add cameras on the IVS platform through device management.

  Setting SDK Parameters This section describes how to set related parameters for a camera to proactively register with the IVS platform through the SDK protocol.

  Adding Cameras to the IVS Platform
  This section describes how to use the iClient to connect cameras to the IVS1800 and IVS3800. Cameras can be connected in batches automatically, in batches manually, or one by one manually.

Parent topic: Configuring Platform Connection

Setting SDK Parameters

This section describes how to set related parameters for a camera to proactively register with the IVS platform through the SDK protocol.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **SDK Settings**.
3. Under **SDK Settings**, select **Enable SDK**.
4. Set SDK parameters, as shown in Figure 1. Table 1 describes the parameters.

> **NOTE**
>
> - If the camera needs to be registered with multiple platforms, select **Platform *X*** and configure information about the platform.
> - Cameras with dual network ports support six platforms. Before the configuration, select the required network port ETH0 or ETH1.
> - To select **Active SDK registration**, ensure that the camera time is the same as the platform time. You are advised to enable NTP time calibration to calibrate the camera time. For details, see Time Configuration.
> - If **Two-factor authentication** is selected, an encrypted port must be configured. If a non-encrypted port is configured, proactive registration will fail.

Figure 1 Setting SDK parameters



Table 1 SDK parameters

Parameter	Description
SDK non-encrypted port	Indicates whether to enable the SDK non-encrypted port. After this parameter is selected, the non-encrypted port can be registered. After **Enable SDK** is selected, **SDK non-encrypted port** is enabled by default.
Active SDK registration	Indicates whether to enable proactive camera registration.
Two-factor authentication	Authentication mode between the camera and the platform. If **Two-factor authentication** is selected, TLS authentication is used. If **Two-factor authentication** is not selected, password authentication is used. **NOTE:** If **Two-factor authentication** is selected, an encrypted port must be configured. If a non-encrypted port is configured, proactive registration will fail.
Registration type	The options are as follows:

Parameter	Description
	• **Single-server mode**: applies when the IVS platform is deployed in a single-node system. • **Dual-server mode**: applies when the IVS platform is deployed in a two-node cluster. The principles are as follows: • In dual-server mode, the camera preferentially connects to the platform using the first IP address. When the connection fails or interrupts, the camera connects to the platform using the second IP address. When the connection to the first platform recovers, the camera will connect to the first platform only after disconnecting from the second platform. • The camera can be registered with only one platform at a time. • The camera can be connected to a third-party platform, including those deployed in a two-node cluster.
Active platform IP	Set this parameter based on the actual IP address of the connected platform. • If the camera needs to connect to the IVS1800, enter the IP address of the platform. • If the camera needs to connect to the IVS3800, enter the floating gateway IP address of the MPU cluster. If the server and camera are on different networks and NAT is deployed, set this parameter to the post-NAT IP address of the cluster floating gateway.

Parameter	Description
Port number	SDK protocol port that the platform listens on.
Device ID	Unique device ID. **NOTE:** Enter a string of 20 digits. The value must be the same as the connection code configured on the platform. Otherwise, the connection fails.

5. Click **Save**.

Parent topic: Configuring Connection to the Platform Through the SDK Protocol

Adding Cameras to the IVS Platform

This section describes how to use the iClient to connect cameras to the IVS1800 and IVS3800. Cameras can be connected in batches automatically, in batches manually, or one by one manually.

- For details about how to use the iClient S100 to connect cameras to the IVS1800, see **Video Service Management (for IVS1800)** in the *iClient S100 User Manual*.
- For details about how to use the iClient to connect cameras to the IVS3800, see **Device Management** in the *iClient Product Documentation*.

Parent topic: Configuring Connection to the Platform Through the SDK Protocol

Configuring Connection to the Platform Through the ONVIF Protocol

Setting ONVIF Parameters You need to set ONVIF parameters if you want to use the ONVIF protocol to connect a camera to the platform.

Adding Cameras to the Milestone Platform
This section describes how to add cameras to the Milestone platform.

Parent topic: Configuring Platform Connection

Setting ONVIF Parameters

You need to set ONVIF parameters if you want to use the ONVIF protocol to connect a camera to the platform.

Prerequisites

- The ONVIF protocol uses MD5 digest authentication, which is a weak algorithm that does not encrypt media streams. Therefore, use this protocol on a trusted network to prevent security risks.
- Both the camera ONVIF protocol and the video security platform must support the H.265 encoding protocol if the ONVIF protocol needs to use the H.265 encoding protocol. Cameras must be of V200R003C10 or later versions. As for the video security platform, contact the platform supplier to confirm whether the platform supports H.265.
- By default, the ONVIF protocol uses the HTTP/HTTPS transmission protocol.
- The ONVIF protocol supports only the G711 and G726 audio encoding formats. Other audio encoding formats may cause the failure to functions such as voice intercom and broadcast and channel-associated voice.
- The corresponding port number is **80** or **8080**.

> **NOTE**
>
> - If the platform is on a public network and the camera is on a private network, the ONVIF protocol can be used to connect the camera to the platform for NAT traversal. For other cases, see the IVS series product documentation.
> - After a camera is connected to the platform through ONVIF, the camera-related parameters modified on the platform will be synchronized to the camera web system. Therefore, do not modify the camera parameters directly in the camera web system. Otherwise, the parameter settings on the platform and camera will be inconsistent.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**. The **Platform Connection** tab page is displayed.

3. Choose **Second Protocol Parameters** > **ONVIF** to access the page for setting ONVIF parameters.
4. Set ONVIF parameters, as shown in Figure 1. Table 1 describes the ONVIF parameters.

Figure 1 Setting ONVIF parameters



Table 1 ONVIF parameters

Parameter	Description
Enable ONVIF	Indicates whether to enable the ONVIF protocol.
Validity period	Indicates whether to enable the validity period function for the ONVIF message. After this function is enabled, an ONVIF message will become invalid when the specified validity period elapses. **NOTE:** The ONVIF message validity period function is valid only when being supported by the video security platform. If the platform does not support this function but this parameter is selected, the camera will fail to connect to the platform. You are advised to enable this function only when security risks exist. The ONVIF message validity period function is disabled by default.
Stream type	Stream transmission type. You can select a value from the **Stream type** drop-down list box. The options are as follows: • **Elementary stream**: uses the ES compression mode. • **Program stream**: uses the PS compression mode.

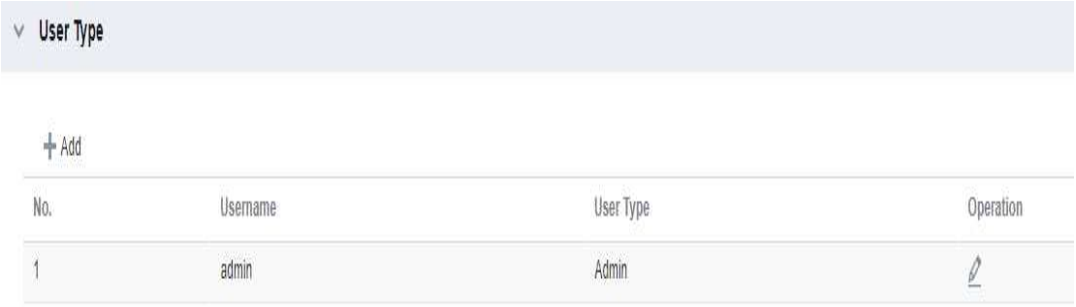
Parameter	Description
	NOTE: • Select a proper stream type based on the decoder requirements. • The ONVIF media stream can be configured only when the camera is connected to the video security platform through the ONVIF protocol.
Authentication mode	Authentication method. You can select a value from the **Authentication mode** drop-down list box. The options are as follows: • **Digest_MD5**: Digest authentication with MD5 encryption. • **Digest_SHA256**: Digest authentication with SHA256 encryption. • **Digest_MD5/Digest_SHA256**: Both Digest_MD5 and Digest_SHA256 authentication methods are supported. • **Digest_MD5(priority)/WSSE**: Both Digest_MD5 and WSSE authentication methods are supported, but Digest_MD5 authentication is preferred. • **WSSE**: Web Service Security (WSSE) authentication mode. • **None**: indicates that authentication is not performed. **NOTE:** • The ONVIF MD5 and WSSE authentication modes may cause security risks. ▪ When some platforms to which the cameras connect support ONVIF WSSE authentication only, use the Digest_MD5(priority)/WSSE authentication mode. ▪ When all platforms to which the cameras connect support ONVIF WSSE authentication only, use the WSSE authentication mode. ▪ You are advised to enable the WSSE authentication mode when some platforms cannot correctly process Digest messages. • Security risks may exist when you select **None**. It is recommended that this authentication method be

Parameter	Description
	enabled only when the platform does not support authentication. The authentication mode is independently configured for RTSP. If RTSP does not require authentication, you need to set its authentication mode to **None** by referring to Configuring Connection to the Platform Through RTSP. Otherwise, stream requesting may fail.
Version	ONVIF version supported by the camera, which must be consistent with that supported by the platform.
Transmission protocol	ONVIF transmission protocol type. The options are as follows: • **HTTP/HTTPS**: Data is transmitted through HTTP or HTTPS. • **HTTP**: Data is transmitted through HTTP. • **HTTPS**: Data is transmitted through HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Forbid ONVIF to change system time	Indicates whether to forbid the system time to be changed through the ONVIF protocol.
Using old mode time zone	Indicates whether to reverse the time zone when you set the time through the ONVIF protocol.
WSSE anti-replay	Indicates whether to enable the anti-replay function when ONVIF WSSE authentication is used.

5. Manage user types.

    a. On the **ONVIF** tab page, click **User Type**. In the **User Type** area, you can add, modify, and delete user information, as shown in Figure 2.

Figure 2 User Type area

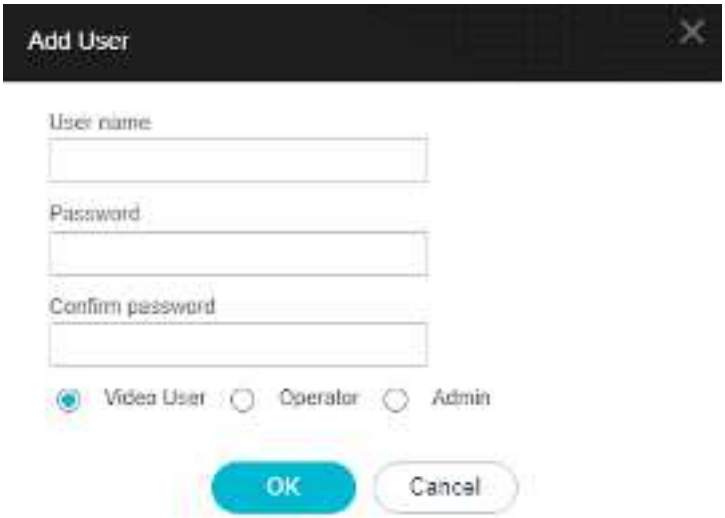


NOTE

- The **admin** user is generated by default and cannot be deleted. The **Username** and **User Type** parameters of the **admin** user are specified by default and cannot be changed. For the **admin** user, only the password can be changed.
- The name of an added user cannot be changed.

b. Click **Add**. In the dialog box that is displayed, add a user, as shown in Figure 3.

Figure 3 Adding a user



c. Click in the **Operation** column of a user. In the **Modify User Info** dialog box, modify user information, as shown in Figure 4.

Figure 4 Modifying user information



NOTE

- The default user name is **admin**, and the initial password is the web user password set when you log in to the camera for the first time. Change the ONVIF password for data security purposes.
- When the camera uses the ONVIF protocol to connect to a video security platform, you must enter this password. Otherwise, the connection cannot be set up. If platform authentication fails for 20 consecutive times, the camera is locked for 5 minutes. After you change the password, keep the new password safe.

Parent topic: Configuring Connection to the Platform Through the ONVIF Protocol

Adding Cameras to the Milestone Platform

This section describes how to add cameras to the Milestone platform.

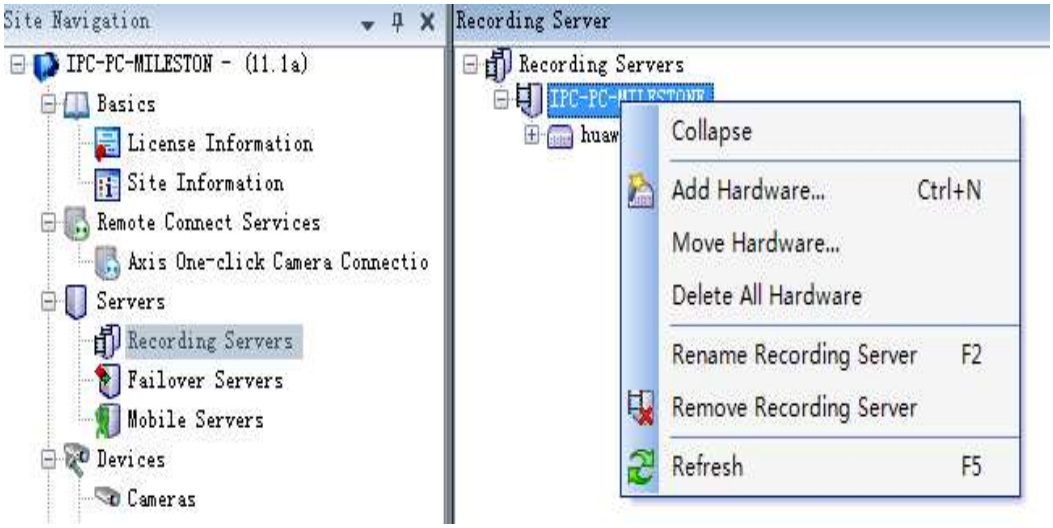
Prerequisites

A Milestone XProtect Management Client has been installed. In this section, Milestone XProtect Management Client 2017 is used as an example.

Procedure

1. Start the Milestone XProtect Management Client, choose **Servers** > **Recording Servers**, right-click the server to which cameras are to be added, and choose **Add Hardware** from the shortcut menu, as shown in Figure 1.

   Figure 1 Starting the Milestone XProtect Management Client



2. Click **Next**, as shown in Figure 2.

Figure 2 Adding hardware

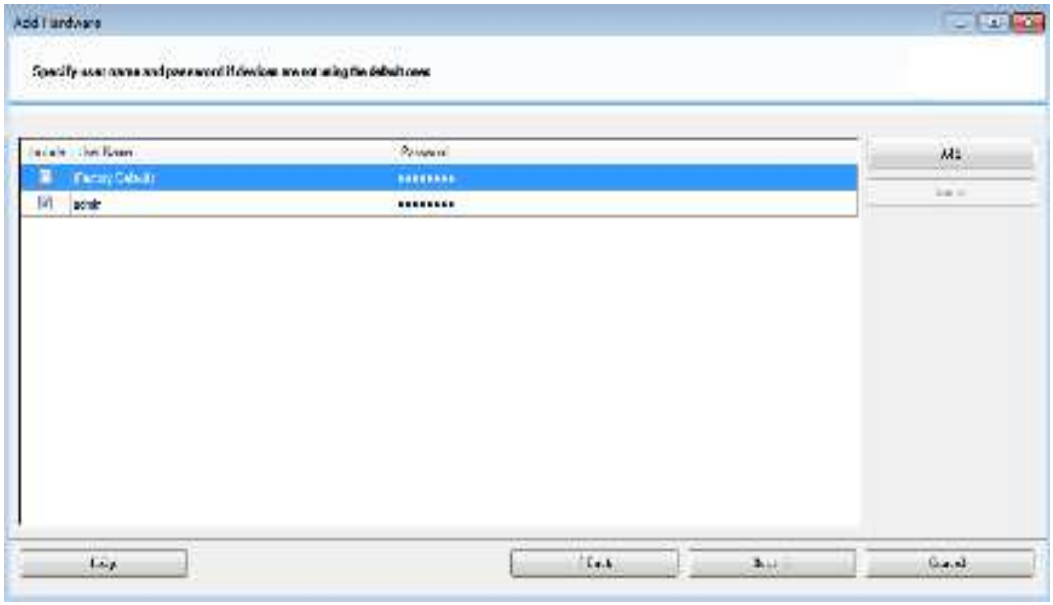


> **NOTE**
>
> You are advised to add cameras in **Address range scanning** or **Manual** mode.

3. Enter the authentication information, including the user name and password for logging in to the camera and click **Next**, as shown in Figure 3.

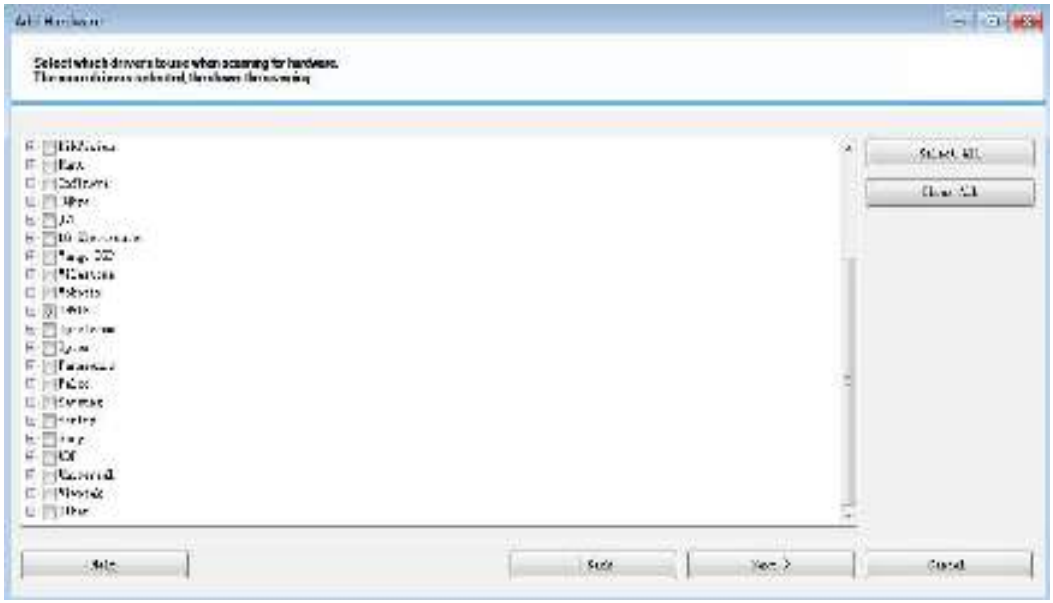
> **NOTE**
>
> The default user name for logging in to a certain SDC is **admin**, and there is no default password. You need to enter the user-defined password.

Figure 3 Entering the authentication information



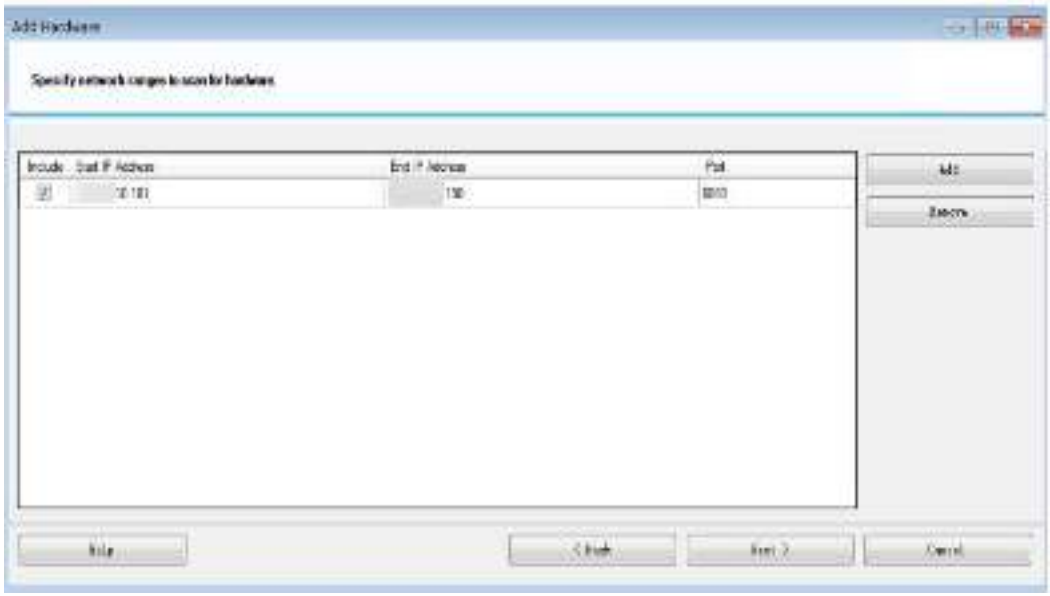
4. Select the driver **ONVIF**. Click **Next**, as shown in Figure 4.

Figure 4 Selecting a driver



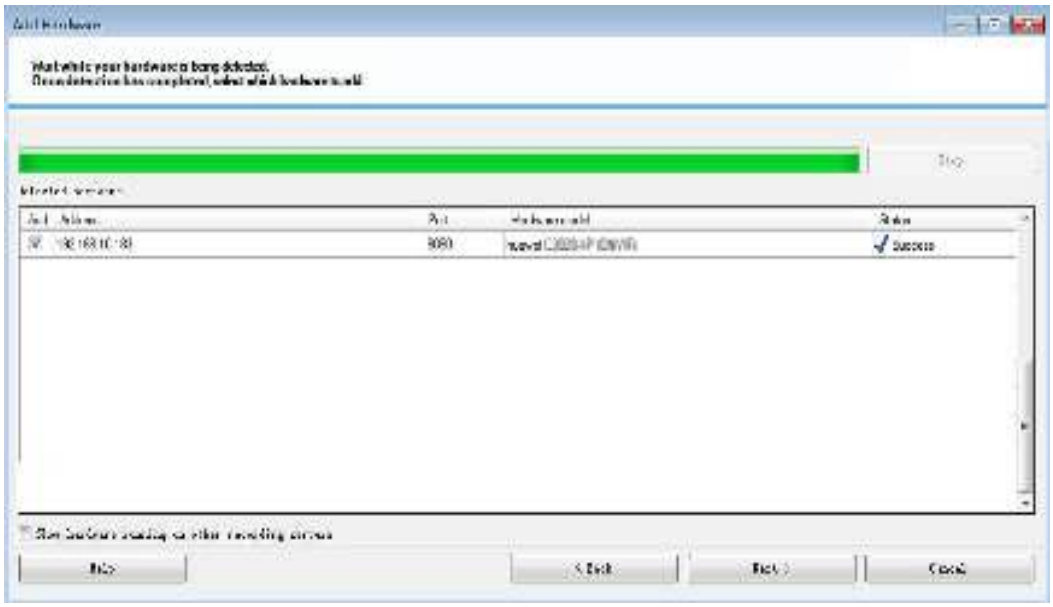
5. Enter the network segment or IP address, select the network segment of the camera to search for, and click **Next**, as shown in Figure 5.

Figure 5 Entering the IP address



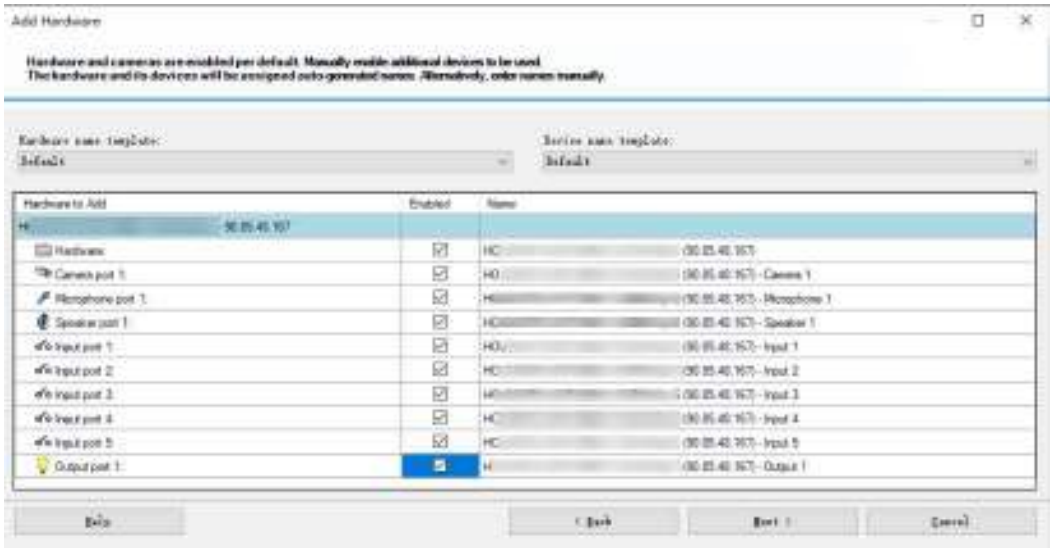
6. After the camera search is complete, click **Next**, as shown in Figure 6.

Figure 6 Searching for ONVIF devices



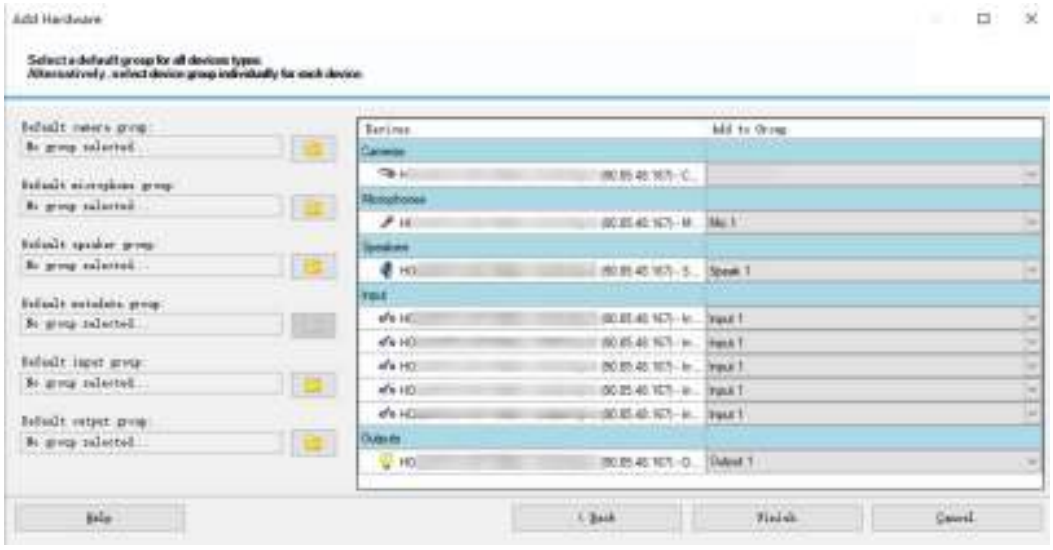
7. Select the hardware to be added and click **Next**, as shown in Figure 7.

Figure 7 Selecting the hardware to be added



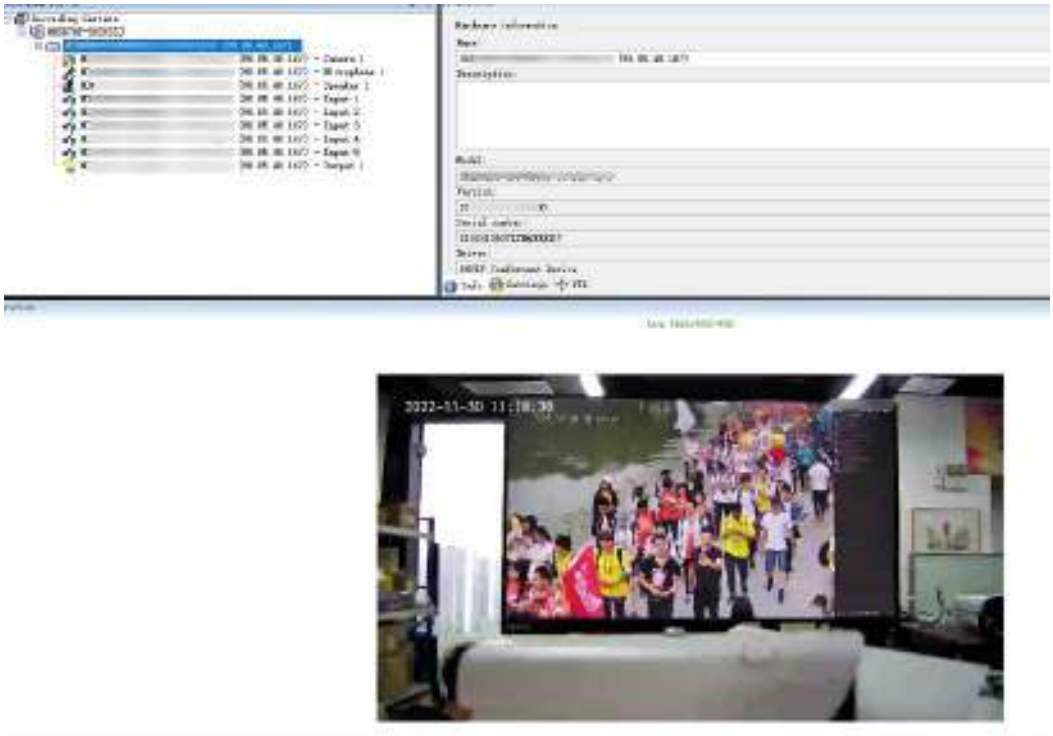
8. Enter the camera group information and click **Finish**, as shown in Figure 8.

   Figure 8 Entering the camera group information



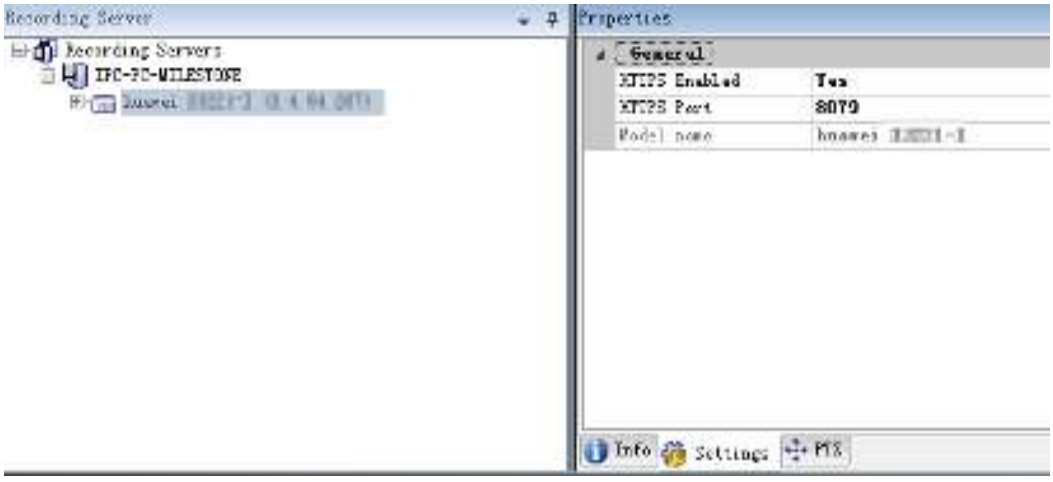
9. Select the camera that has been added to view its live video, as shown in Figure 9.

   Figure 9 Viewing live video of the camera



10. (Optional) If the HTTPS protocol is used, select the camera that has been added, click **Settings** in the **Properties** window, and set HTTPS parameters, as shown in Figure 10.

Figure 10 Setting HTTPS parameters



a. Set **HTTPS Enabled** to **Yes**, indicating that HTTPS is enabled.

b. Set **HTTPS Port** to **443**, which is the same as the value of HTTPS port number set under **Settings** > **Network** > **Port Settings**.

> **NOTE**
>
> If the processor type is Hi3516E V200 or Hi3516E V300, the default value of **HTTPS Port** is **8079**, as shown in Figure 10. The HTTPS port number of such processor type cannot be changed in the camera web system. You can configure the port number through the ONVIF protocol. The default value is recommended.

Parent topic: Configuring Connection to the Platform Through the ONVIF Protocol

Configuring Connection to the Platform Through the GB/T 28181 Protocol

The section describes how to connect a camera to the IVS platform through GB/T 28181. The GB/T 28181 protocol supports only the active access mode.

CAUTION

If the GB/T 28181 protocol is used, deploy the camera on a dedicated network.

Setting GB/T 28181 Parameters This section describes how to set GB/T 28181 parameters if a camera needs to connect to the platform through the GB/T 28181 protocol.

Adding Cameras to the IVS Platform
This section describes how to use the iClient to connect cameras to the IVS1800 and IVS3800. Cameras can be connected in batches automatically, in batches manually, or one by one manually.

Parent topic: Configuring Platform Connection

Setting GB/T 28181 Parameters

This section describes how to set GB/T 28181 parameters if a camera needs to connect to the platform through the GB/T 28181 protocol.

A camera can be registered with two platforms through GB/T 28181. When a camera is registered with multiple platforms, if the platforms synchronize NTP server time to the camera at the same time, the camera time may be discontinuous. You are advised to keep only one platform that can synchronize NTP server time to the camera.

NOTE

- The GB/T 28181 protocol supports independent upgrade. Light intelligence and inclusive intelligence cameras do not support independent upgrade. For details about how to obtain the upgrade package and perform the upgrade, see Upgrading the Camera Version/Algorithms.
- You can query a maximum of 500 recording segments at a time. If the number of recording segments within the specified query period exceeds 500, change the start time and end time.

Prerequisites

- The GB/T 28181 protocol supports MD5 and SHA256 digest authentication. The MD5 algorithm is a weak algorithm, and the signaling flow and the media stream are not encrypted, which may result in security risks. Therefore, use this protocol on a trusted network.
- You have obtained the values of the parameters (for example, device ID) for connecting cameras to the video security platform through the GB/T 28181 protocol.

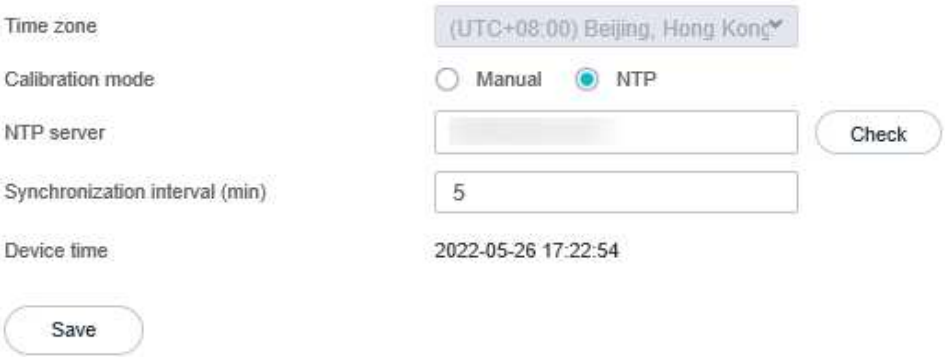
Setting the System Time

To connect a camera to the platform through the GB/T 28181 protocol, ensure that the camera is time-synchronized with the NTP server. The capabilities supported vary between camera models.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Settings** > **Time**.

   The **Time** tab page is displayed, as shown in Figure 1.

   Figure 1 Setting time



3. Set the system time, as shown in Figure 1.

   a. Select a time zone from the **Time zone** drop-down list box.

   b. Set **Calibration mode** to **NTP**.

   c. Set **NTP server**.

   - If the camera is to be connected to a single IVS platform, set this parameter to the IP address of the IVS platform.
   - If the camera is to be connected to a cluster, set this parameter to the floating gateway IP address of the cluster.

4. Click **Save**.

Setting GB/T 28181 Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **T28181**.

   NOTE

   To register with two platforms, you also need to choose **Second Protocol Parameters** > **T28181.2** and configure information about

the other platform. You can set GB 35114 protocol parameters only on the **T28181** tab page.

3. Set GB/T 28181 parameters, as shown in Figure 2 and Figure 3. Table 1 and Table 2 describe the GB/T 28181 parameters. The parameters vary between camera models.

Figure 2 Setting common GB/T 28181 parameters

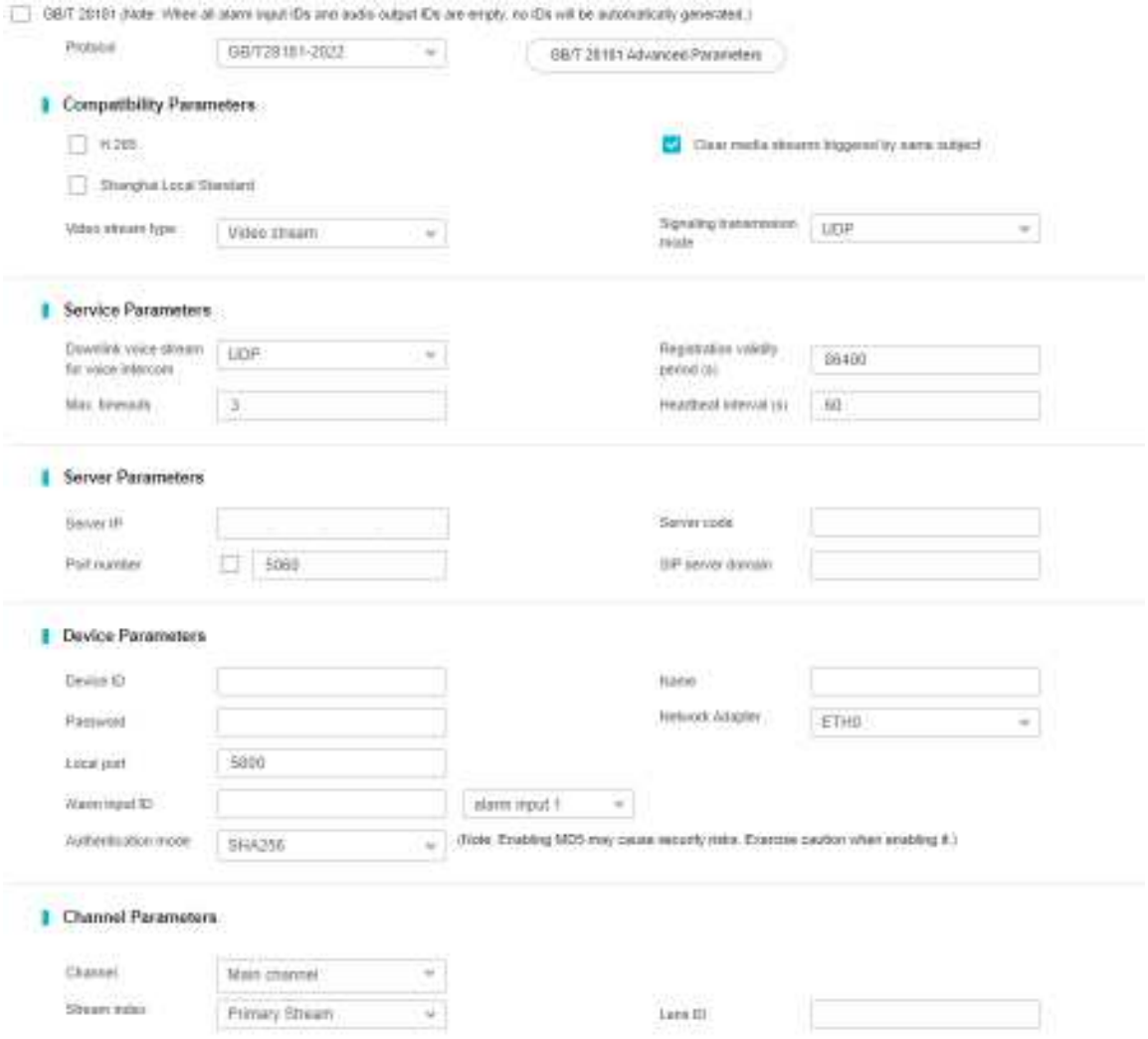


Figure 3 Setting advanced GB/T 28181 parameters



Table 1 GB/T 28181 parameters

Parameter	Description
GB/T 28181	If this parameter is selected, the GB/T 28181 protocol is supported.
Protocol	Protocol type. You can select a value from the drop-down list box. The default value is **GB/T 28181-2016**. **NOTE:** • In addition to the default protocol, the camera also supports the GB/T 28181-2022 and TCC-VMS-2020 protocols. • When the TCC-VMS-2020 protocol is selected, the active and standby servers can be configured. When the active (standby) server is faulty, services are automatically switched to the standby (active) server.

Parameter		Description
Compatibility Parameters	H.265	If this parameter is selected, the H.265 and other related encoding protocols are supported when the camera is connected to the platform through the GB/T 28181 protocol. If this parameter is not selected, only other related encoding protocols are supported when the camera is connected to the platform through the GB/T 28181 protocol.

Parameter		Description
	Clear media streams triggered by same subject	If this parameter is selected, only one channel of video streams can be obtained if the platform requests video streams with the same subject ID. If this parameter is not selected, multiple channels of video streams can be obtained if the platform requests video streams with the same subject ID.
	Shanghai local standard	If this parameter is selected, the Shanghai local protocol is supported. **NOTE:** If the Shanghai local standard is enabled, the image capture function of the platform does not take effect.
	Video stream type	Video stream type. You can select a value from the drop-down list box. • **Auto**: Sends media streams based on the request of the platform. • **Video stream**: Sends only video streams. • **Hybrid stream**: Sends video and audio streams.
	Signaling transmission mode	Signaling transmission mode. The options include **UDP** and **TCP**.

Parameter		Description
Service Parameters	Downlink voice streams for voice intercom	Protocol of downlink voice streams for voice intercom. The value can be **UDP** or **TCP**. **NOTE:** If the camera and the platform are on different network segments, you are advised to set this parameter to **TCP**.
	Max. timeouts	If the number of consecutive heartbeat timeouts reaches the value specified by this parameter, the camera cannot connect to the platform. The default value **3** is recommended. **NOTE:** The value of **Max. timeouts** for the camera and platform must be the same.
	Registration validity (s)	Validity period of the camera registration with the video security platform. The default value is **86400s** (one day). **NOTE:** Before the validity period expires, the device initiates a registration request to the platform again.
	Heartbeat interval (s)	Time interval for the camera to send heartbeat messages. The default value **60** is recommended. **NOTE:** The camera and the platform must have the same heartbeat interval.

Parameter		Description
Server Parameters	Server IP	• If the camera needs to connect to the IVS1800, enter the IP address of the platform. • If the camera needs to connect to the IVS3800, enter the floating gateway IP address of the MPU cluster. If the server and camera are on different networks and NAT is deployed, set this parameter to the post-NAT IP address of the cluster floating gateway.
	Port number	Port number for the platform to listen on cameras connecting to the platform through GB/T 28181. The default value is **5060**. To connect to the IVS platform, change the value to **5080**. After selecting the **Port number** check box, you can configure the port number range.
	Server code	GB/T 28181 server code. Enter a string of 1 to 64 characters. The value can contain letters and digits. **NOTE:** If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the server code must be **200**.
	SIP server domain	Domain name that consists of 1–127 digits.

Parameter		Description
Device Parameters	Device ID	Unique ID of a device. The value is a string of 1 to 64 characters, including letters and digits. The value must be the same as the connection code configured on the platform. **NOTE:** • This parameter is mandatory. If you do not set it, the camera cannot go online. • If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the camera ID must be **132**. Besides, the camera ID must be different from the lens ID. Otherwise, you cannot view live video from the camera on the platform.

Parameter	Description

Parameter		Description
	Password	Password used by a camera to register with the platform. **NOTE:** • The value of this parameter must be the same as the registration password configured on the platform. If they are different, the camera will fail to connect to the video security platform.
	Name	Login name used for registering the camera with the platform. The value can contain digits or other characters.
	Local port	Port number of the camera when the camera is connected to the SIP server. **NOTE:** The value is an integer ranging from 1024 to 65535.
	Alarm input ID	Alarm input ID of the device. The value is a string of 0 to 64 characters, including letters and digits. If there are multiple alarm input channels, you need to specify a unique ID for each channel. **NOTE:** • Some C/D series cameras do not support this parameter. • You need to manually enter the value. The eleventh to thirteenth digits must be **134**. Otherwise, the IVS platform cannot report alarms properly.

Parameter		Description
	Audio output ID	Audio output ID of the device. The value is a string of 0 to 64 characters, including letters and digits. **NOTE:** • Some C/D series cameras do not support this parameter. • You need to manually enter the value. The eleventh to thirteenth digits must be **137**. Otherwise, the IVS platform cannot transmit uplink or downlink audio streams properly.
	Authentication mode	• **SHA256**: Only the SHA256 authentication mode is supported. • **MD5/SHA256**: Both MD5 and SHA256 authentication modes are supported. **NOTE:** • The MD5 authentication mode has security risks. Therefore, you are advised to use the SHA256 authentication mode. • The value of this parameter must be the same as that configured on the platform. Otherwise, the registration fails.

Parameter		Description
Channel Parameters	Channel	Channel type of the camera.
	Stream index	Type of streams to be sent to the platform. You can select the primary stream or a secondary stream. The default value **Primary** is recommended.
	Lens ID	Lens ID. The value is a string of 0 to 64 characters, including letters and digits. For a multi-lens camera, you need to specify a unique ID for each lens. **NOTE:** If a camera is to be connected to the IVS platform, the eleventh to thirteenth digits of the lens ID must be **131** or **132**. Otherwise, live video from the camera cannot be viewed on the platform.

Table 2 Advanced GB/T 28181 parameters

Parameter	Description
Max recordings can be queried	Maximum number of recordings carried in a packet during recording query when GB/T 28181 is used to platform connection. Enter an integer ranging from 1 to 20. The default value is 10. If the platform limits the packet size, you can properly adjust the value of this parameter. Adjusting the value of this parameter affects the recording query speed. Adjust the value based on the site requirements.
T28181 Media Stream Keep Alive	This function is disabled by default. When this function and the media stream keepalive function are enabled at the same time, RTCP keepalive packets can be sent. If the platform supports the

Parameter	Description
	keepalive function, you are advised to enable this function.

Parameter		Description
Site Information Reporting	Site type	Type of the site. The options include **Class-1**, **Class-2**, **Class-3**, and **Others**.
	Capture position type	Type of the capture position. The value is a string of seven digits.
	Industry category code	Industry category code of the site. The value is a string of 0 to 4 digits.
	Regional organization code	Regional organization code of the site. The value is a string of six digits.
	Site name	Name of the site. The value is a string of 0 to 254 characters, including letters and digits.
	Installation location	Site installation location. The options include **Indoor**, **Outdoor**, and **None**.
	Viewing direction	Viewing direction. The options include **East**, **West**, **South**, **North**, **Southeast**, **Northeast**, **Southwest**, **Northwest**, and **None**.
	Installation date	Time when a camera is installed.
	Management agency	Agency that manages the camera. Enter a string of 0 to 254 characters (including letters and digits).
	Administrator's contact method	Contact information of the camera administrator. The value is a string of 0 to 254 characters, including letters and digits.
	Checkpoint function	Camera function that can be reported through GB/T 28181. The options include **Target**, **Person**, **Motor vehicle**, **Non-motorized vehicle**, **Perimeter**, and **Others**.

4. Click **Save**.

Parent topic: Configuring Connection to the Platform Through the GB/T 28181 Protocol

Adding Cameras to the IVS Platform

This section describes how to use the iClient to connect cameras to the IVS1800 and IVS3800. Cameras can be connected in batches automatically, in batches manually, or one by one manually.

- For details about how to use the iClient S100 to connect cameras to the IVS1800, see **Video Service Management (for IVS1800)** in the *iClient S100 User Manual*.
- For details about how to use the iClient to connect cameras to the IVS3800, see **Device Management** in the *iClient Product Documentation*.

Parent topic: Configuring Connection to the Platform Through the GB/T 28181 Protocol

Configuring Connection to the Platform Through the GA/T 1400 Protocol

This section describes how to connect a camera to the IVS platform or a third-party platform through the GA/T 1400 protocol.

Setting GA/T 1400 Parameters Cameras can connect to the IVS platform through the GA/T 1400 protocol. This section describes only how to set GA/T 1400 parameters on the camera side. For details about the configuration on the platform side, contact technical support engineers on the platform side.

Adding Cameras to the IVS Platform

Parent topic: Configuring Platform Connection

Setting GA/T 1400 Parameters

Cameras can connect to the IVS platform through the GA/T 1400 protocol. This section describes only how to set GA/T 1400 parameters on the camera side. For details about the configuration on the platform side, contact technical support engineers on the platform side.

NOTE

- The GA/T 1400 protocol supports independent upgrade. For details about how to obtain and install the upgrade package, see Upgrading the Camera Version/Algorithms.
- The parameters displayed on the web page vary depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **GA/T 1400**.

   NOTE

   To register with two platforms, choose **Second Protocol Parameters** > **GA/T 1400-2** and configure information about the other platform.

3. Set GA/T 1400 parameters, as shown in Figure 1. Table 1 describes the GA/T 1400 parameters.

   Figure 1 Setting GA/T 1400 parameters



Table 1 GA/T 1400 parameters

Parameter	Description
GA/T 1400	Indicates whether to enable the GA/T 1400 protocol.
Transmission protocol	• **HTTP**: Data is transmitted through HTTP. • **HTTPS**: Data is transmitted through HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Authentication mode	• **SHA256**: Only the SHA256 authentication mode is supported. • **MD5/SHA256**: Both MD5 and SHA256 authentication modes are supported. **NOTE:** • The MD5 authentication mode has security risks. Therefore, you are advised to use the SHA256 authentication mode.

Parameter	Description
	• The value of this parameter must be the same as that configured on the platform. Otherwise, the registration fails.
Platform address	Domain name or IP address of the IVS platform.
Coordinate type	Coordinate type used to upload target coordinate data through the selected transmission protocol. The options are as follows: • **Absolute**: absolute coordinate of a target. • **Relative**: relative coordinate of a target, that is, permyriad of the position of the target to the width and height of the image.
Port number	Port used by the platform to listen on the GA/T 1400 protocol. The value is an integer ranging from 1 to 65535. **NOTE:** • When the camera is to be connected to the IVS platform: ▪ If **Transmission protocol** is set to **HTTP**, you need to set **Port number** to **8001**. ▪ If **Transmission protocol** is set to **HTTPS**, you need to set **Port number** to **8002**. • When the camera is to be connected to another platform, you need to comply with the port configuration specifications on the platform side.
Device ID	Unique ID of a device. For cameras with multiple video channels, you can configure a unique ID for each video channel. Then each channel will be registered and report metadata independently. You can also configure the same ID for all video channels. Then the video channels will be registered and report metadata using the same ID.

Parameter	Description
Checkpoint ID	ID of the checkpoint to which the current device belongs. For a camera with multiple video channels, if the video channels belong to different checkpoints, you can configure the checkpoint ID for each video channel based on the site requirements. If all video channels belong to the same checkpoint, you can configure a checkpoint ID for all the channels.
User name	Login name used to register the camera with the platform.
Password	Password for registering the camera with the platform. **NOTE:** • The value of this parameter must be the same as the registration password configured on the platform. If they are different, the camera will fail to connect to the platform.

4. (Optional) Click **Advanced GA/T 1400 Parameters**. The **Advanced GA/T 1400 Parameters** dialog box is displayed, as shown in Figure 2. Table 2 describes the parameters.

Figure 2 Advanced GA/T 1400 Parameters dialog box

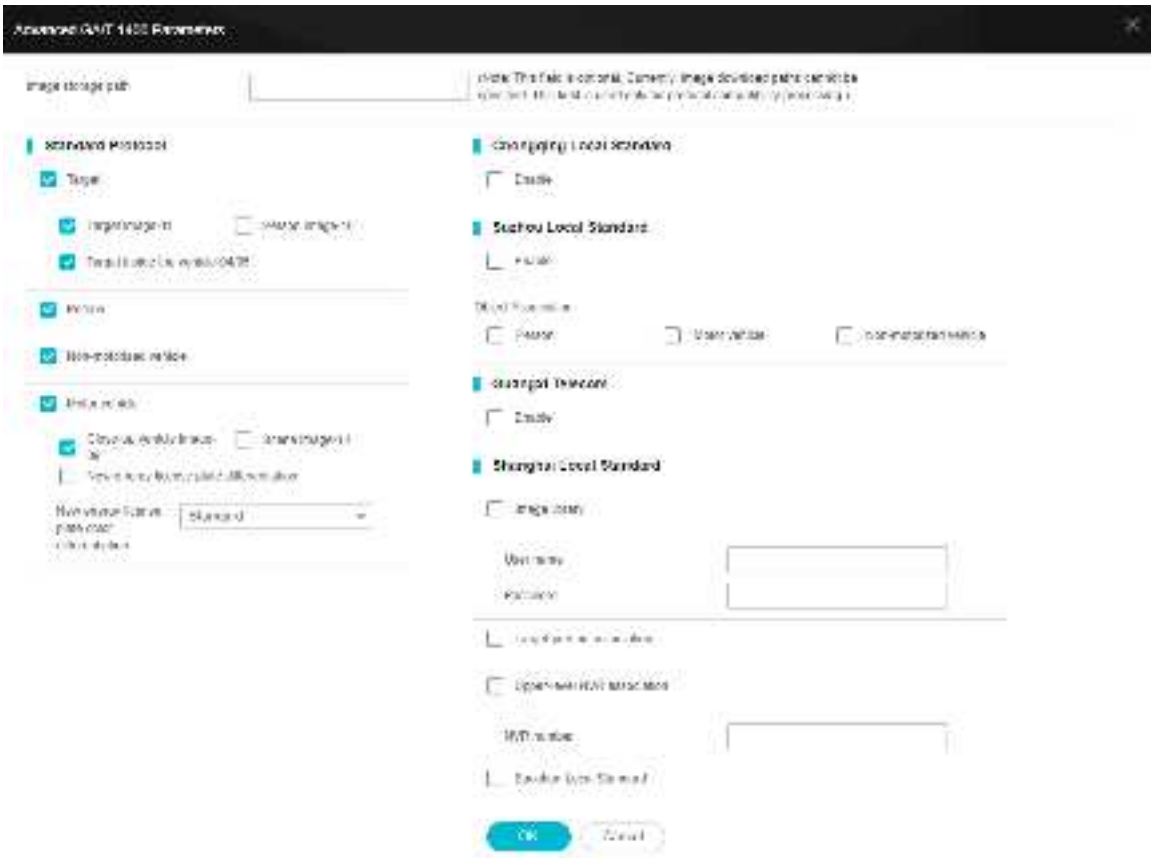


Table 2 Advanced GA/T 1400 parameters

Parameter	Description
Image storage path	Image storage path. **NOTE:** • At some sites, this parameter cannot be left empty due to compatibility issues. Otherwise, the platform connection may fail. You need to set a path that can be parsed to ensure proper connection between cameras and the platform. • Currently, you cannot download images from the path. This field is used for protocol compatibility processing.

Parameter		Description
Target	Target	Indicates whether to report target information.
	Target image-11	Indicates whether to report target images whose image type is 11. **CAUTION:** If this parameter is not selected, all target images (including in-vehicle targets) are not reported.
	Person image-10	Indicates whether to report person images whose image type is 10. If this parameter is not selected, person images are not reported.
	Target inside the vehicle-04/05	Indicates whether to report close-up images (whose image type is 04 or 05) of the driver and front passenger. If this parameter is not selected, close-up images of the driver and front passenger are still reported but the image type is 11. **NOTE:** Close-up images of the driver and front passenger are reported no matter whether this parameter is selected.
Person		Indicates whether to report person images.
Non-motorized vehicle		Indicates whether to report images of non-motorized vehicles.

Parameter		Description
Motor vehicle	Motor vehicle	Indicates whether to report license plates and full images of motor vehicles.

Parameter		Description
	Close-up vehicle image-09	Indicates whether to report close-up images (whose image type is 09) of motor vehicles. If this parameter is not selected, close-up images of motor vehicles are not reported.
	Scene image-14	Indicates whether to report full images (whose image type is 14) of motor vehicles. If this parameter is not selected, full images of motor vehicles are still reported but the image type is 01. **NOTE:** Full images of motor vehicles are reported no matter whether this parameter is selected.
	New-energy license plate differentiation	If this check box is selected, the system reports vehicle type 51 for license plates of large new-energy vehicles and vehicle type 52 for license plates of small new-energy vehicles. If this check box is not selected, the system reports the vehicle type based on the standard definition (01: license plates of large vehicles; 02: license plates of small vehicles).
	New energy license plate color differentiation	• **Standard**: reports vehicle type 9 for license plates of both large and small new-energy vehicles. • **Yellow Green 51 & Gradient Green 52**: reports vehicle type 51 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 52 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 52 & Gradient Green 51**: reports vehicle type 52 for license

Parameter		Description
		plates of large new-energy vehicles (yellow and green), and reports vehicle type 51 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 20 & Gradient Green 9**: reports vehicle type 20 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 9 for license plates of small new-energy vehicles (gradient green). • **Yellow Green 98 & Gradient Green 97**: reports vehicle type 98 for license plates of large new-energy vehicles (yellow and green), and reports vehicle type 97 for license plates of small new-energy vehicles (gradient green).
Chongqing Local Standard	Enable	Indicates whether to report information based on the requirements defined in the Chongqing local standard.
Suzhou Local Standard	Enable	Indicates whether to report information based on the requirements defined in the Suzhou local standard.
Guangxi Telecom	Enable	Indicates whether to report information based on the requirements defined in the Guangxi Telecom standard.

Parameter		Description
Shanghai Local Standard	Image library	Indicates whether to separately report images to the image library. If this parameter is selected, information is reported based on the requirements defined in the Shanghai local standard and images are separately uploaded to the image library.
	User name	User name of the image library used to authenticate the camera.
	Password	Password of the image library used to authenticate the camera.
	Target-person association	Indicates whether to associate target images with related person images.
	Upper-level NVR association	Indicates whether to allow you to search for recordings from a camera based on the associated NVR device. If this parameter is selected, the camera reports the NVR ID when registering with the GA/T 1400 VIID.
	NVR number	ID used by the camera to register with the GA/T 1400 VIID.
	Baoshan Local Standard	Indicates whether to report information based on the requirements defined in the Baoshan local standard.

5. (Optional) Click **OK**.
6. Click **Save**.

Parent topic: Configuring Connection to the Platform Through the GA/T 1400 Protocol

Adding Cameras to the IVS Platform

This section describes how to use the iClient to connect cameras to the IVS3800. Cameras can be connected in batches automatically, in batches manually, or one by one manually.

For details about how to use the iClient to connect cameras to the IVS3800, see **Device Management** in the *iClient Product Documentation*.

Parent topic: Configuring Connection to the Platform Through the GA/T 1400 Protocol

Configuring Connection to the Platform Through RESTful

This section describes how to connect a camera to the IVS platform through the RESTful protocol.

The RESTful protocol is a network device management protocol based on the RESTful architecture.

Prerequisites

The RESTful protocol uses the HTTPS transmission protocol by default. Therefore, the client must also support the HTTPS protocol. If the client supports only the HTTP protocol, you need to set **RESTful transmission protocol** to **HTTP/HTTPS** on the camera side. If the transmission protocol on the camera is different from that on the client, connection will fail.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**.
3. Choose **Second Protocol Parameters** > **RESTful**. The **RESTful** tab page is displayed, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 RESTful tab page

   Table 1 RESTful parameters

Parameter	Description
Transmission protocol	• **HTTPS**: Data is transmitted through HTTPS.

Parameter	Description
	• **HTTP/HTTPS**: Data is transmitted through HTTP or HTTPS. **NOTE:** HTTP is an insecure protocol and may cause security risks. Therefore, exercise caution when using this protocol.
Authentication mode	Select an authentication algorithm supported by the invoker. • **Digest_MD5**: Only the Digest_MD5 authentication method is supported. • **Digest_SHA256**: Only the Digest_SHA256 authentication method is supported. • **Digest_MD5/Digest_SHA256**: Both Digest_MD5 and Digest_SHA256 authentication methods are supported. **NOTE:** The Digest_MD5 authentication method may cause security risks. Therefore, exercise caution when using this method.
NAT	Indicates whether to enable NAT. This parameter is optional. If **NAT** is selected, you need to set the NAT network address, user name, and password. **NOTE:** • If NAT is required for connecting the camera to the platform, set related NAT parameters. • The camera supports the Digest_MD5 and Digest_SHA256 authentication methods. The Digest_MD5 authentication method has security risks. Therefore, exercise caution when using Digest_MD5.

Parameter	Description
URL	Platform URL. Set this parameter to **http://*IP address:port number/xxx*** or **https://*IP address:port number/xxx***, for example, **http://10.3.4.55:98/nat**.
User name	User name set for NAT translation.
Password	Password set for NAT translation. This parameter is optional.

NOTE

Identity authentication is required when you connect a camera to the platform through the RESTful protocol. For details about how to change the RESTful (that is, the northbound interface) password, see Configuring Password Management.

Parent topic: Configuring Platform Connection

Configuring Connection to the Platform Through RTSP

RTSP is an application-level protocol for the controls, such as play, pause, and fast-forward, of real-time streaming data.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**.
3. Choose **Second Protocol Parameters** > **RTSP**. The **RTSP** tab page is displayed, as shown in Figure 1. Table 1 describes the options for the **RTSP authentication mode** parameter.

   Figure 1 RTSP tab page

   Table 1 Options for RTSP authentication

Option	Description
Digest_MD5	Digest authentication with MD5 encryption. This authentication method may cause security risks. Exercise caution when using it.
Digest_SHA256	Digest authentication with SHA256 encryption.
None	Security risks may exist when you select **None**. It is recommended that this authentication method be enabled only when the platform does not support authentication. If **None** is selected, the system does not perform authentication if you request live video through the RTSP or ONVIF protocol.

> **NOTE**
>
> The RTSP protocol is enabled by default. You can select the required authentication method during configuration.

Parent topic: Configuring Platform Connection

Setting IConnect Parameters

Only some camera models support the IConnect protocol.

NOTE

For camera models that support the IConnect protocol, do not change the value of **MTU (bytes)** to prevent camera disconnection.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**. The **Platform Connection** tab page is displayed.
3. Choose **Custom Third-Party Platform** > **IConnect Platform** and set IConnect protocol parameters, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 Setting IConnect protocol parameters

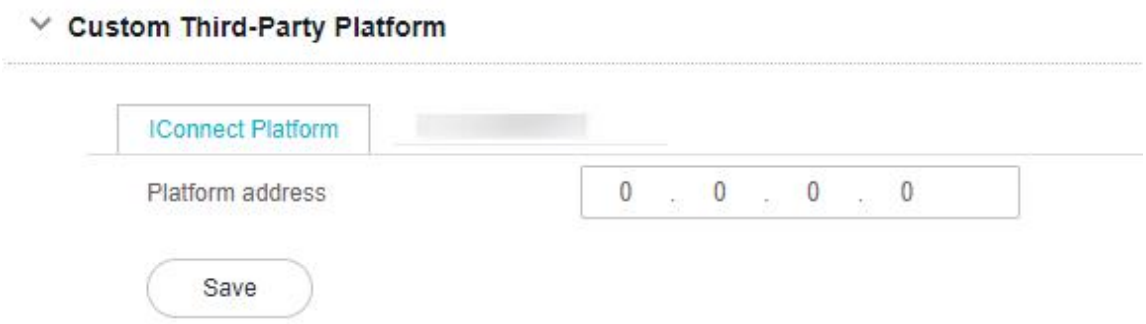
   

   Table 1 IConnect protocol parameters

Parameter	Setting
Platform address	Set this parameter to the IP address of the NCE-Campus to be connected through iConnect.

4. Click **Save**.

Parent topic: Configuring Platform Connection

Configuring Cloud Service Connection

After a camera is connected to the cloud service, you can view live and recorded video from the camera on your mobile app. The capabilities supported vary between camera models.

After installing the mobile app, you should read through the privacy policy and user agreement on the app.

The hardware serial number (SN) and verification code are used to verify the camera to be added to the app. Figure 1 describes how to obtain the hardware SN and verification code in the camera web system.

NOTE

To add a camera on the mobile app, you need to first select a country or region. The detailed method is as follows:

- Scan the QR code to add the camera to the mobile app. You can obtain the QR code:
  - On the camera body (If the verification code for cloud service connection is changed, the QR code becomes invalid.)
  - In the camera web system (under **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**)
- Enter the hardware SN and verification code to manually add a camera to the mobile app. To obtain the hardware SN and verification code, choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**.

Configuring Connection This section describes how to connect a camera to a mobile app through the cloud service.

Configuring a Certificate
This section describes how to configure and manage cloud service certificates.

Unbinding a Camera
This section describes how to unbind a camera from a mobile app.

Parent topic: Configuring Platform Connection

Configuring Connection

This section describes how to connect a camera to a mobile app through the cloud service.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**. The parameters vary between camera models.

   Figure 1 Cloud Service area

   Table 1 Parameter description

Parameter	Description
Cloud service connection	Indicates whether to enable cloud service connection. After this function is enabled, you can add the camera to the mobile app. **NOTE:** To add a camera on the mobile app, you need to first select a country or region.

Parameter	Description
Cloud service time calibration	Indicates whether to synchronize the time of the camera with that of the cloud service. If another time synchronization method is used to calibrate the camera time on the network, a conflict will occur after this function is enabled.
Hardware SN	Camera serial number.
Verification code	Used to verify the camera when you connect the camera to the Cloud Service. After the verification code is changed, the QR code on the camera body will become invalid. In this case, you can manually add the camera using the hardware SN or scan the QR code in the camera web system.
Domain name	IP address and port number of the server connected to the Cloud Service. You can use the default value when you add the camera to the mobile app. **NOTE:** If the domain name of the cloud service is not an IP address, configure the primary DNS server in Setting Camera IP Addresses.
Scan QR code for connection (recommended)	QR code for adding the camera to the mobile app.
Binding status	Binding status. After the camera is added to the mobile app, you can click **Refresh** to display information about the app user. If the camera is not added to the mobile app, the message "The device is not bound." is displayed.
User name	Name of the app user.
Phone number	Phone number of the app user.
Email	Email address of the app user.

Parent topic: Configuring Cloud Service Connection

Configuring a Certificate

This section describes how to configure and manage cloud service certificates.

The validity period of a certificate is defined by each certificate authority (CA) when the certificate issuer is being set.

The certificate revocation list (CRL) is used to prevent network security problems caused by private certificate key leakage. Certificates in the CRL are not secure.

Cameras support cloud service certificate revocation. For security purposes, cameras cannot connect to platforms that use certificates in the CRL.

Context

Certificates should be purchased from an authoritative third-party certification organization or be obtained by establishing a CA server.

A CRL is a data file that lists the serial numbers and revocation dates of certificates that are revoked by the CA.

Cloud Service Certificate Management

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**. The parameters vary between camera models.
3. Click **Set Certificate**. In the dialog box that is displayed, complete settings in the **Cloud Service Certificate** area, as shown in Figure 1. Table 1 describes the parameters and buttons.

Figure 1 Cloud Service Certificate area

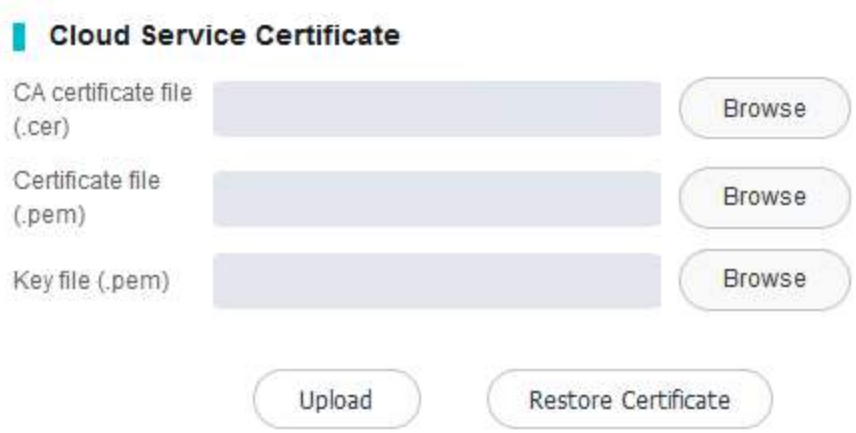


Table 1 Certificate management parameters and buttons

Parameter/Button	Description
CA certificate file (.cer)	CA certificate.
Certificate file (.pem)	Digital information file that identifies and verifies both parties involved in network communication.
Key file (.pem)	Key file that contains the certificate key (*xxx*_key.pem).
Restore Certificate	Button for restoring the certificate to the default one.

You can use your own certificate file in the following way: Click **Browse**, select your desired file path, and click **Upload**. In the dialog box that is displayed, enter the password of the private key file to upload the certificate.

NOTE

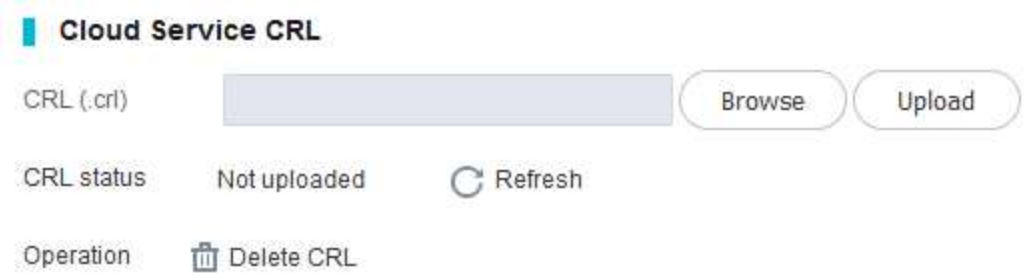
- Only certificate files in **.pem** format can be uploaded.
- The password of the private key file must be the same as that generated when you apply for the private key file.

- If you click **Restore Certificate**, the system displays a dialog box asking you whether to restore the certificate to the default one.

Cloud Service CRL Management

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**. The parameters vary between camera models.
3. Click **Set Certificate**. In the dialog box that is displayed, complete settings in the **Cloud Service CRL** area, as shown in Figure 2.

   Figure 2 Cloud Service CRL area

4. Click **Browse**, select the CRL to be uploaded, and click **Upload**.

   If the CRL file uploaded is normal, **Normal** is displayed in the CRL list. If the CRL file uploaded has expired, **Expired** is displayed in the CRL list. If the format of the CRL file to be uploaded is incorrect, an error message is displayed.
5. (Optional) Click **Refresh** if the status in the CRL list is not displayed.
6. (Optional) Click **Delete** to delete an uploaded CRL.

Parent topic: Configuring Cloud Service Connection

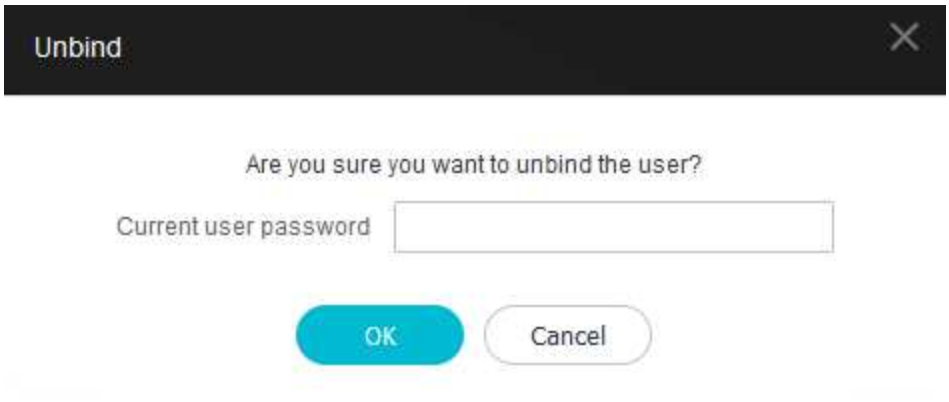
Unbinding a Camera

This section describes how to unbind a camera from a mobile app.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Cloud Service**. The parameters vary between camera models.
3. Click **Unbind**. The **Forcible unbinding** dialog box shown in Figure 1 is displayed. Only some camera models support this function.

   Figure 1 Forcible unbinding dialog box

4. Enter the current user password and click **OK** to unbind a camera from the mobile app.

NOTE

- Only the administrator has the permission to unbind devices.
- You need to enter the password of the administrator to perform this operation.
- If the camera is not bound to or is displayed as offline on the mobile app, the **Unbind** button is unavailable.

- The binding status is automatically updated each time you enter the **Cloud Service** page.

Parent topic: Configuring Cloud Service Connection

Video and Audio Configuration

This chapter describes how to set video and audio parameters.

Video and Audio Feature Differences

Setting Video Parameters
You can set video parameters, such as the stream combination type, encoding protocol, and resolution, based on the site requirements.

Setting Audio Parameters
You can set audio parameters and alarm-triggered audio parameters, such as the audio format, input volume, and audio bit rate, based on the site requirements.

Configuring a Stream Profile
By configuring stream profiles, you can preset various audio and video stream parameters to specified values to facilitate quick invocation.

Setting ROI Parameters
By setting a region of interest (ROI), you can set the ROI quality to differentiate the ROI from other image regions. The ROI effect is prominent at a low bit rate.

Parent topic: Configuration

Video and Audio Feature Differences

Supported video and audio features vary depending on the camera models. The following table describes the differences.

NOTE

The 2-channel built-in MIC listed in the table is used only to enhance the audio collection effect. Actually only one-channel audio input is displayed in the camera web system.

Table 1 Differences in audio and video feature configurations

Device Model	SuperCoding	Intelligent Encoding	Area Cropping	Audio Input Port
HWT-D3040-10-ELI-PV (2.8 mm)	YES	YES	NO	YES. Supports one-channel built-in MIC.
HWT-D6550-10-Z33-SV	NO	YES	NO	YES. Supports 2-channel built-in MIC.
HWT-D3252-10-SIU	YES	YES	NO	YES. Supports one-channel LINE IN and one-channel built-in MIC.
HWT-D3222-10-SIU	YES	YES	YES **NOTE:** Only areas cropped when the stream type is set	YES. Supports one-channel LINE IN and one-channel built-in MIC.

Device Model	SuperCoding	Intelligent Encoding	Area Cropping	Audio Input Port
			to secondary stream 1 support the ePTZ function.	
HWT-D2152-10-SIU	YES	YES	NO	YES. Supports one-channel LINE IN or one-channel external MIC.
HWT-D2122-10-SIU	YES	YES	YES **NOTE:** Only areas cropped when the stream type is set to secondary stream 1 support the ePTZ function.	YES. Supports one-channel LINE IN or one-channel external MIC.

Parent topic: Video and Audio Configuration

Setting Video Parameters

You can set video parameters, such as the stream combination type, encoding protocol, and resolution, based on the site requirements.

Context

Table 1 describes common resolutions.

Table 1 Common resolutions

Resolution	Description
4K	The resolution is 3840 x 2160, about 8,000,000 pixels.
2048p	The resolution is 2560 x 2048, about 5,000,000 pixels.
1920p	The resolution is 2560 x 1920, about 5,000,000 pixels.
1728p	The resolution is 3072 x 1728, about 5,000,000 pixels.
1536p	The resolution is 2048 x 1536, about 3,000,000 pixels.
1296p	The resolution is 2304 x 1296, about 3,000,000 pixels.
1520p	The resolution is 2592 x 1520, about 4,000,000 pixels.
1440p	The resolution is 2560 x 1440, about 4,000,000 pixels.
1080p	The resolution is 1920 x 1080, about 2,000,000 pixels.
720p	The resolution is 1280 x 720, about 900,000 pixels.
D1_PAL	The resolution is 720 x 576, about 400,000 pixels.

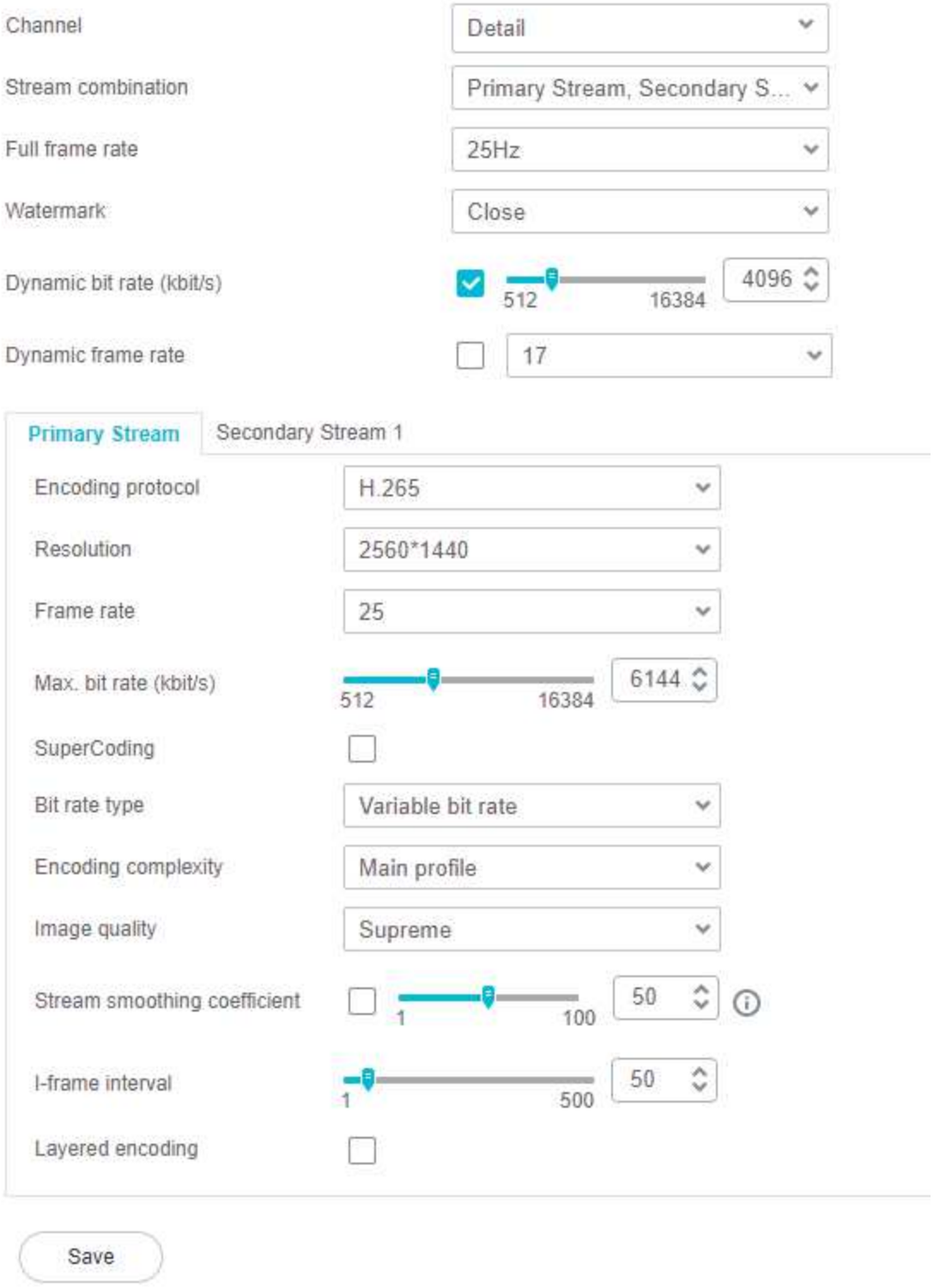
Resolution	Description
D1_NTSC	The resolution is 720 x 480, about 350,000 pixels.
CIF_PAL	The resolution is 352 x 288, about 100,000 pixels.
CIF_NTSC	The resolution is 352 x 240, about 84,000 pixels.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Video/Audio** > **Video**.

   The parameters displayed on the web page vary depending on the camera model.

Figure 1 Setting video parameters



3. Set video parameters. Table 2 describes the parameters.

The following table describes all parameters. The parameters displayed on the web page vary depending on the camera model.

Table 2 Video parameters

Parameter	Description
Channel	Channel type of a device.
Stream combination	Stream combination type. • **Primary Stream**: The primary streams feature high bit rate, definition, and bandwidth usage. They are applicable to local storage. • **Secondary Stream**: The secondary streams provide smooth video and occupy small bandwidth. They are applicable to data transmission over low-bandwidth networks. **NOTE:** Onboard recording (stored on onboard SD cards) supports only primary streams. You cannot set the stream type to triple streams or higher for some C series and D series cameras. That is, only **Primary Stream** or **Primary Stream, Secondary Stream 1** can be set for such cameras. The multi-stream (triple streams or higher) function is mutually exclusive with the perimeter detection function. After target detection or perimeter detection is enabled, the maximum resolution of the secondary stream can be set to D1.
Full frame rate	Frame rate collected through the sensor, representing the maximum capability of a camera.

Parameter	Description
	NOTE: On the camera web page, you need to set the frame rate based on the site requirements and bandwidth conditions. A higher frame rate indicates clearer and more vivid images. The maximum frame rate cannot exceed the full frame rate.
Watermark	Indicates whether to enable the watermark function. You can enable this function for information security purposes such as anti-counterfeit and copyright protection. • **Close**: Disable the watermark function. • **HiSilicon digital watermark**: Enable the HiSilicon watermark function. • **SHA256 digital watermark**: Enable the SHA256-based watermark function.
Dynamic bit rate	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. If this checkbox is selected, the camera will automatically use the dynamic bit rate to deliver clearer live (primary stream) or recorded video when the camera generates an alarm (excluding the temperature alarm). After the alarm is cleared, the bit rate is restored to that in stream settings. **NOTE:** • It is recommended that the dynamic bit rate be greater than that in stream settings. • The dynamic bit rate is valid only for primary streams.

Parameter	Description
Dynamic frame rate	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. If this checkbox is selected, the camera automatically uses the dynamic frame rate when the camera triggers an alarm (excluding the temperature alarm). After the alarm is cleared, the frame rate is restored to that in stream settings. **NOTE:** • It is recommended that the dynamic frame rate be greater than that in stream settings. • The dynamic frame rate is valid only for primary streams.
SuperCoding	Indicates whether to enable SuperCoding. This function is enabled by default. After SuperCoding is enabled, the camera can compress the background while ensuring the image quality of ROIs. This helps save storage space and transmission bandwidth. If **Max. bit rate (kbit/s)** at each video resolution is set to a too low value, mosaics may occur on live video. You are advised to set this parameter by referring to Table 3. **NOTE:** • After SuperCoding is enabled, the **Encoding complexity**, **Bit rate type**, **Image quality**, **I-frame interval**, **Stream smoothing coefficient**, and **Layered encoding** parameters are unavailable. • The SuperCoding function is available only for some camera models. Before enabling

Parameter	Description
	SuperCoding for light intelligence cameras, ensure that the corridor mode is disabled.
Intelligent encoding	Indicates whether to enable intelligent encoding. If it is enabled, the camera can automatically adapt to scenarios to reduce the bit rate and save the storage space. A higher intelligent encoding level indicates more significant reduction of the bit rate, which may lead to image quality deterioration. **NOTE:** • After intelligent encoding is enabled, the **Encoding complexity**, **Bit rate type**, **Image quality**, **I-frame interval**, and **Layered encoding** parameters cannot be set. • After intelligent encoding is enabled, the I-frame interval is automatically controlled. If a recording is segmented within the I-frame interval, a recording segment will be missing. The duration of the missing recording segment is less than the I-frame interval.
Slice	Multi-slice encoding indicates that video streams are divided into multiple segments. Each segment forms a slice. The encoding process of each slice is independent of each other. Therefore, the camera can encode and decode multiple slices in parallel, improving encoding and decoding performance. This check box is selected by default.
Encoding protocol	Video encoding protocol. • **MJPEG**: The MJPEG protocol decodes and displays each frame independently without

Parameter	Description
	referring to the previous and next frames. This protocol has a small compression ratio and requires large bandwidth to ensure video quality. This protocol is suitable for video editing. • **H.265**: The H.265 protocol is bandwidth-conserving. **NOTE:** • Before connecting a camera to the video security platform, ensure that the encoding protocol of the camera is the same as that on the platform to prevent issues (such as live video viewing or video recording failures) on the platform. The encoding protocol of the camera must be a protocol supported by the platform. • Local recordings and onboard recordings (using SD cards) support related protocols such as H.265.
Encoding complexity	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. For the H.265 encoding protocol, the available profile is **Main profile**.
Resolution	Video resolution. A higher resolution indicates clearer images and higher bandwidth consumption. If the **Resolution** parameter of a 4K camera is dimmed (not configurable), check whether the area cropping function is enabled. If the function is enabled, disable the function and then set the resolution. **NOTE:**

Parameter	Description
	To obtain the resolution of 1080p secondary streams, you need to set the resolution of the primary stream to 1080p or lower. Then, you can set the resolution on the **Secondary Stream 1** tab page.
Bit rate type	Type of the bit rate. The parameter is available only when you set **Encoding protocol** to H.265 or other related formats. The bit rate is measured by data bits transmitted in a unit of time. • **Variable bit rate**: The bit rate varies depending on the image complexity to ensure the clarity of images with great dynamic changes. The bit rate is low if the image is simple or static. The variable bit rate is recommended. • **Constant bit rate**: The constant bit rate remains the same. The upper limit of the instantaneous bit rate is set to 110%. If the bit rate is incorrectly configured for images with great dynamic changes, the images will be unclear.
Bit rate value	Bit rate. The parameter is available only when you set **Bit rate type** to **Constant bit rate**. A larger bit rate indicates better video quality and higher bandwidth consumption. • You must set a proper bit rate value to ensure the video quality. • The actual bandwidth requirement needs to be higher than the bit rate to ensure smooth video. If the bit rate is low, the required bandwidth is generally 1.2 times the bit rate.

Parameter	Description
	• If the total bit rate of enabled live video streams (including metadata streams) exceeds 40 Mbit/s, you are advised to reduce the bit rate or the number of enabled video streams to prevent video stuttering or artifacts caused by large bit streams.
Bit rate control mode	Bit rate control mode. The parameter is available only when you set **Bit rate type** to **Constant bit rate**. • **Frame rate priority**: The frame rate stability is preferentially ensured. However, the actual bit rate may be greater than the configured bit rate in complicated scenarios or scenarios where objects move quickly. • **Image quality priority**: The image quality is preferentially ensured. However, frames may be lost or live video is not smooth in complicated scenarios or scenarios where objects move quickly. **NOTE:** If SuperCoding is enabled, the options of **Bit rate control mode** are **Balanced**, **Image quality priority**, and **Bit rate compression priority**.
Max. bit rate (kbit/s)	Upper limit of the bit rate. The parameter is available only when you set **Bit rate type** to **Variable bit rate**. The bit rate range is associated with the resolution. **NOTE:**

Parameter	Description
	• Whether to enable SuperCoding affects the bit rate range. • After SuperCoding is enabled, the connected platform can still deliver bit rates that are not supported by SuperCoding. The bit rate set on the platform does not take effect.
Frame rate	Frame rate measured by the number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.
Image quality	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats and **Bit rate type** is set to **Variable bit rate**. **NOTE:** Better image quality indicates that more network bandwidth is consumed. Configure a proper image quality value based on the site requirements.
I-frame interval	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. An I-frame is an intra-coded frame that represents a fixed image independent of other picture types. Each group of pictures (GOP) begins with this type of frame. A smaller I-frame interval indicates better video quality and higher bandwidth consumption. **NOTE:**

Parameter	Description
	It is recommended that the I-frame interval be set to twice the frame rate.
Layered encoding	This parameter is available only when **Encoding protocol** is set to H.265 or other related formats. To enable the layered encoding function, select the check box. By default, the check box is deselected. Enabling this function will enhance the fault tolerance and packet loss concealment capabilities but will also increase the bit rate and encoding complexity. In addition, a specific decoder is required. You can choose whether to enable this function based on the site requirements.
JPEG quality	The parameter is available only when you set **Encoding protocol** to **MJPEG**. A larger JPEG quality value indicates better video quality and higher bandwidth consumption.
Enable area cropping	Indicates whether to enable area cropping. After this function is enabled, you can select an area on the video image for encoding and set it as a secondary stream. You can set related parameters on the tab page corresponding to each secondary stream when **Stream combination** is set to one of the following values: **Primary Stream, Secondary Stream 1** and **Primary Stream, Secondary Stream 1, Secondary Stream 2**. **NOTE:** • On the **Secondary Stream 1** tab page, you can set **Resolution** to **1920*1080**,

Parameter	Description
	1280*720, **720*576**, or **720*480**. • On the **Secondary Stream 2** tab page, you can set **Resolution** to **720*576**, **720*480**, **352*288**, or **352*240**. • For **Secondary Stream 2**, the size of the cropped area cannot be set. 1. Select **Enable area cropping**. 2. Drag the mouse pointer to adjust the area to crop. 3. After the setting is successful, switch to the secondary stream for which the region cropping function is set on the video preview page. Only the cropped region is displayed. 4. Click  to enable ePTZ. **NOTE:** The electronic PTZ (ePTZ) adjusts the focal length or shooting angle through software, instead of by using lens zooming or PTZ rotation. • For some models, if the electronic image stabilization function is enabled, the area cropping function cannot be enabled. Enable the function based on the site requirements. • The ePTZ function can be used only after the area cropping function is enabled and live video is switched to the required secondary stream type. Only **Secondary Stream 1** supports the ePTZ function. • A shorter distance between the arrow and the cross indicates a slower rotation speed.

Parameter	Description
	• You can scroll the mouse wheel to control the zoom. The image is zoomed in when the mouse wheel is scrolled up and zoomed out when the mouse wheel is scrolled down.
Absolute timestamp	Indicates whether to enable the absolute timestamp. The absolute timestamp refers to the number of milliseconds that have elapsed since the Unix epoch, minus leap seconds. The Unix epoch is 00:00:00 UTC on 1 January 1970. This function is disabled by default. After this function is enabled, the RTP extension header of video streams carries an absolute timestamp. You can obtain video streams with absolute timestamps in multiple ways (for example, RTSP) for real-time vehicle positioning and trajectory generation. **NOTE:** • The absolute timestamp function is mutually exclusive with the layered encoding and digital watermark functions. • For details about how to obtain streams through RTSP, see Obtaining Streams Through RTSP.
Stream smoothing coefficient	Indicates whether to enable stream smoothing. After this function is enabled, you can drag the slider to set the stream smoothing coefficient. The default value is **50**. A larger value indicates a smaller I-frame and lower image clarity.

Table 3 Recommended maximum bit rate at each video resolution

Setting Audio Parameters

You can set audio parameters and alarm-triggered audio parameters, such as the audio format, input volume, and audio bit rate, based on the site requirements.

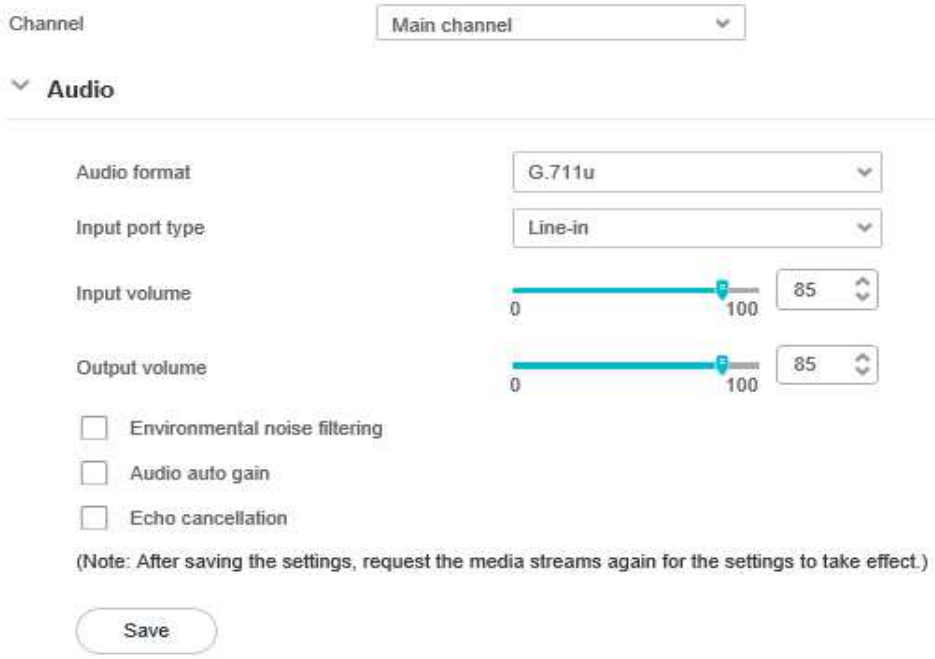
NOTICE

The audio feature supports only low-fidelity audio and environment sound collection scenarios and does not support high-fidelity audio scenarios, for example, audio forensics and human voice collection in the politics and law, education, and finance industries.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Video/Audio** > **Audio** and set **Channel**.
3. Click **Audio**. The **Audio** area is displayed, as shown in Figure 1. The parameters displayed on this page may vary between camera models.

Figure 1 Audio parameters



4. Set audio parameters and click **Save**. Table 1 describes the parameters.

Table 1 Audio parameters

Parameter	Description
Audio format	Audio format. • **G.711u**: primarily used in North America and Japan. • **G.711a**: primarily used in Europe and China. • **G.726**: primarily used when bandwidth is strained. • **OPUS**: primarily used for real-time voice transmission on networks. • **AAC**: primarily used in scenarios where the size of an audio file needs to be reduced. **NOTE:**

Parameter	Description
	• After the audio stream format is modified, you need to request the media stream again for the modification to take effect. You can access the live video preview page to request the media stream again. • In OPUS format, the environment noise filtering and automatic audio gain take effect only when the sampling rate is 8 kHz or 16 kHz.
Input port type	Type of the audio input port. • **Mic-in**: Select this option when the camera is connected to a device with lower audio output power, such as a microphone and other passive audio input devices, to prevent audio signal distortion. • **Line-in**: Select this option when the camera is connected to a device with higher audio output power, such as an MP3 player, synthesizer, and active sound pickup device, to prevent no sound or low sound volume.
Input volume	Controls the input volume.
Output volume	Controls the output volume.
Audio bit rate	Audio bit rate, in bits. The parameter is available only when you set **Audio format** to **G.726**, **OPUS**, or **AAC**. A higher audio bit rate indicates better audio quality and higher bandwidth consumption.
Audio sampling rate	Audio sample rate, in Hz. The parameter is available only when you set **Audio format** to

Parameter	Description
	OPUS or **AAC**. Audio sample rate is the frequency for sample audio signals per second. A higher audio sample rate indicates more unadulterated and distortion-free sound reproduction.
Environmental noise filtering	Indicates whether to enable environment noise filtering. Enabling this function can filter out ambient noise and make voice clear.
Audio auto gain	Indicates whether to enable auto audio gain. Enabling this function can improve audio quality.
Echo cancellation	Indicates whether to enable echo cancellation. Enabling this function can dramatically reduce echoes in audio services. For example, during voice intercom, remote audio data is played on an audio output (AO) device (for example, a speaker). In this case, after this function is enabled, the camera collects onsite audio data using the microphone and dramatically reduces the echoed sounds from the AO device in the collected audio data.

5. Click **Alarm-triggered Audio**. The **Alarm-triggered Audio** area is displayed, as shown in Figure 2.

Figure 2 Alarm-triggered Audio area





NOTE

- You can click **Delete All** to delete all audio files, or you can click corresponding to an audio file to delete it.
- To upload a local audio file, you can click **Add Audio**, select the file from a local path, and click .
- You can click or corresponding to a custom or uploaded audio file to download or delete it.
- You can drag corresponding to **Output volume** to adjust the output volume.

Parent topic: Video and Audio Configuration

Configuring a Stream Profile

By configuring stream profiles, you can preset various audio and video stream parameters to specified values to facilitate quick invocation.

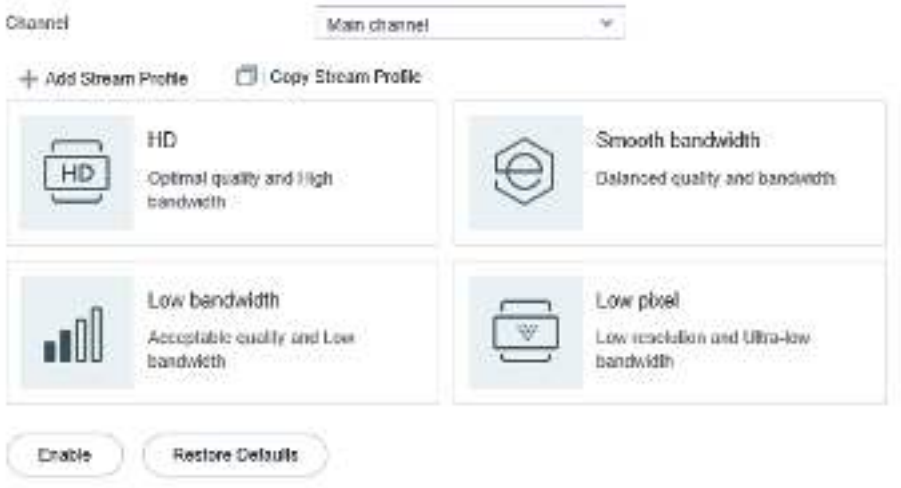
Context

A stream profile is a template containing predefined configurations of video and audio streams. By configuring stream profiles, you can preset various image parameters to specified values to facilitate quick invocation.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Video/Audio** > **Profiles**. On the tab page that is displayed, set **Channel** and select a required stream profile, as shown in Figure 1. The parameters displayed on this page may vary between camera models.

   Figure 1 Stream profiles

3. Select a stream profile depending on your needs and click **Enable**.

   The system provides four default stream profiles, as described in Table 1.

   Table 1 Default stream profiles

Profile	Description

Profile	Description
HD	This profile provides video images of the best quality but consumes more network resources. This profile applies to the dedicated video security network with sufficient bandwidth (at least 20 Mbit/s bandwidth for each camera).
Smooth bandwidth	This profile reduces the number of data streams for transmission and ensures image quality. This profile conserves the bandwidth and applies to most scenarios (at least 6 Mbit/s bandwidth for each camera).
Low bandwidth	This profile reduces the number of data streams for transmission and ensures that the image quality is acceptable. This profile conserves the bandwidth and applies to scenarios with insufficient bandwidth (approximately 3 Mbit/s bandwidth for each camera).
Low pixel	This profile reduces the image resolution, frame rate, and encoding streams and applies to scenarios with low bandwidth and low decoding capability.

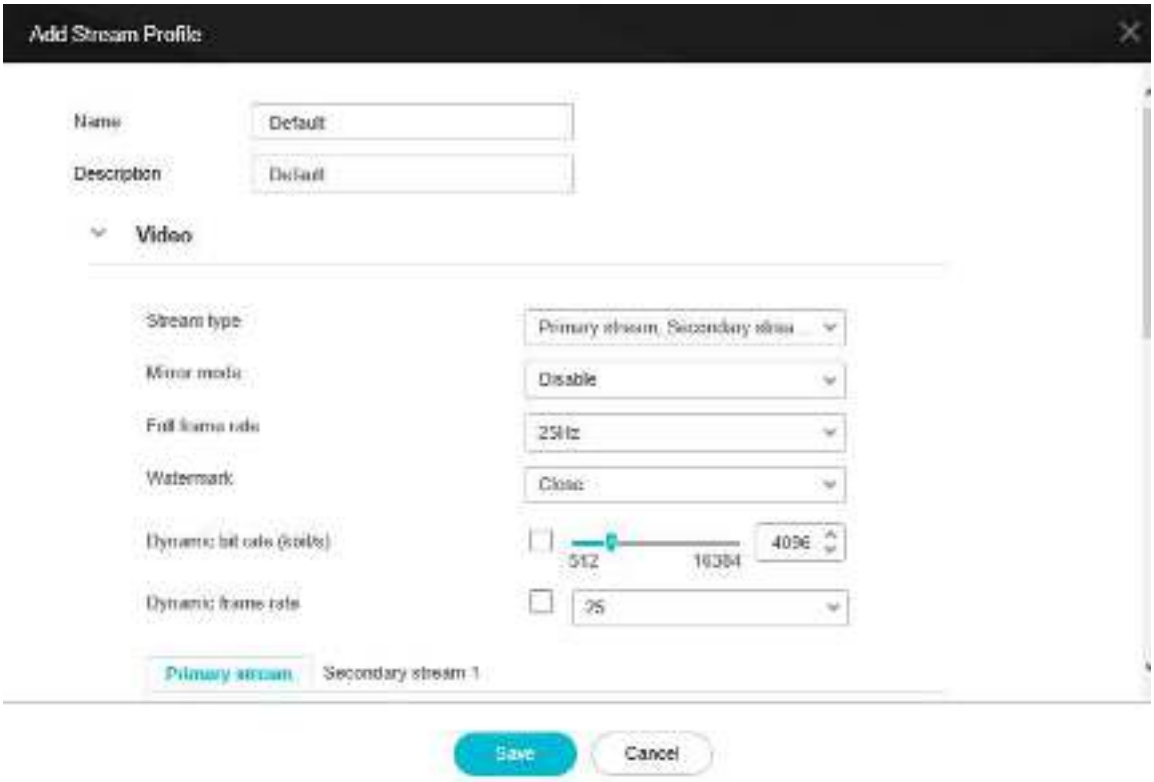
NOTE

You can also add stream profiles by referring to steps 4 through 6.

4. Click **Add Stream Profile**. You can also select a default profile, and then click **Copy Stream Profile** for further modification.

The **Add Stream Profile** dialog box is displayed, as shown in Figure 2. The parameters vary depending on the camera model.

Figure 2 Add Stream Profile dialog box



5. Set stream profile parameters.

   The stream profile parameters include the profile name, description, and audio and video stream parameters. For details about how to set video parameters, see Setting Video Parameters. For details about how to set audio parameters, see Setting Audio Parameters.

6. Click **Save**.

NOTE

- To modify an existing stream profile, select it and click . The default stream profile cannot be edited or deleted.
- To delete a custom stream profile, select it and click .
- If you click **Restore Defaults**, the parameters on the **Video** page will be restored to default settings.

Parent topic: Video and Audio Configuration

Setting ROI Parameters

By setting a region of interest (ROI), you can set the ROI quality to differentiate the ROI from other image regions. The ROI effect is prominent at a low bit rate.

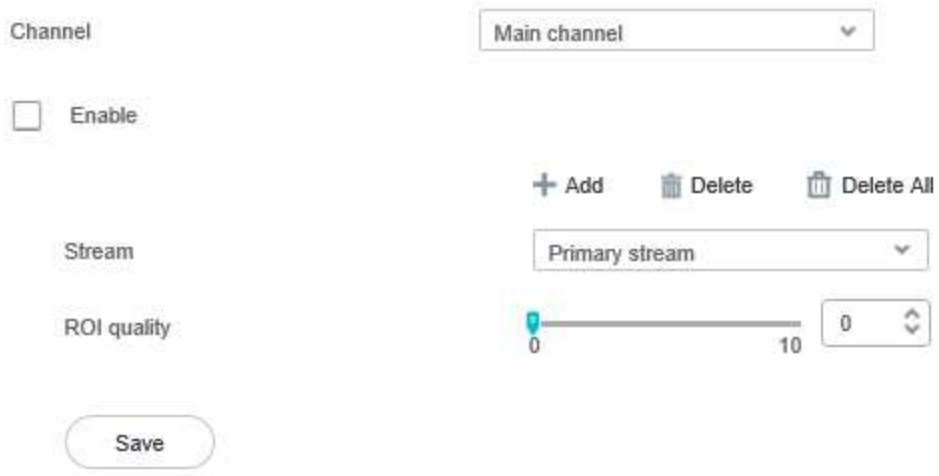
Prerequisites

You have set **Encoding protocol** to H.265 or other related formats.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Video/Audio** > **ROI**. On the tab page that is displayed, set **Channel**, as shown in Figure 1.

   Figure 1 Setting ROI parameters



3. Select **Enable**.
4. Select a value from the **Stream** drop-down list box.
5. Click **Add**.

   An ROI is displayed on the live video image.

NOTE

- You can add only one ROI at a time. If you need to add more ROIs, click **Add** again.
- Only one ROI can be added.

6. Use the mouse to adjust the ROI location and size.
7. Select the ROI and set **ROI quality**.

NOTE

- When the ROI function is enabled, the ROI quality value reflects the quality difference between the current ROI area and non-ROI area.
- A larger value indicates increased image quality inside the ROI area and decreased image quality outside the ROI area.
- After you set **ROI quality**, the definition of the image (including the OSD text) in some parts outside the ROI area decreases.

8. Click **Save**.

NOTE

- To delete an ROI, you need to select the ROI on the live video image and click **Delete**.
- To delete all ROIs, you can click **Delete All**.

Parent topic: Video and Audio Configuration

Configuring Images

This chapter describes how to set image-related parameters, including image parameters, image profiles, and profile plans.

Image Feature Differences

Setting Image Parameters
By setting image parameters, you can adjust video images to adapt to different scenarios.

Configuring OSD
You can set on-screen display (OSD) parameters to specify the information to be displayed and the display effect.

Configuring Image Overlay
You can configure image overlay to superimpose images on live video and manually captured live video images. You can also upload an image, for example, a logo, for display based on the site requirements.

Configuring an Image Profile
By configuring and invoking an image profile, you can quickly utilize configurations of the image parameters in common scenarios.

Configuring Privacy Mask
You can mask a specified area on live video images to protect sensitive or private information.

Configuring Area Focus
After you configure area focus, the area with a higher focusing priority will be preferentially focused when the focusing function of a camera is triggered.

Configuring a White Balance Area
After a white balance area is configured, the white balance function takes effect in the selected area only.

Parent topic: Configuration

Image Feature Differences

This section describes the image configurations supported by different camera models. The following table lists only the configuration items that vary depending on camera models. Common configuration items are not described here.

Table 1 Different image configurations on web pages

Device Model	Corridor Mode	Mirror Mode	Exposure Compensation	Exposure Mode	Focus Area	Electronic Image Stabilization	Focus Compensation	Intelligent Infrared	Profile Linkag
HWT-D3040-10-ELI-PV (2.8 mm)	YES	YES	YES	YES	NO	NO	NO	YES	YES
HWT-D6550-10-Z33-SV	NO	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D2122-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D2152-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES

Device Model	Corridor Mode	Mirror Mode	Exposure Compensation	Exposure Mode	Focus Area	Electronic Image Stabilization	Focus Compensation	Intelligent Infrared	Profile Linkag
HWT-D3222-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D3252-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES

Parent topic: Configuring Images

Setting Image Parameters

By setting image parameters, you can adjust video images to adapt to different scenarios.

NOTICE

- The default values of image parameters vary depending on the algorithm mode.
- Image parameters are associated with each other. Set the image parameters strictly based on the site requirements to prevent poor image quality or overexposure.
- Image parameters vary depending on camera models.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display** and use the default value of **Channel**.
3. Set related parameters based on the site requirements. The following describes the parameters.

Image Adjustment

Figure 1 Setting image adjustment parameters

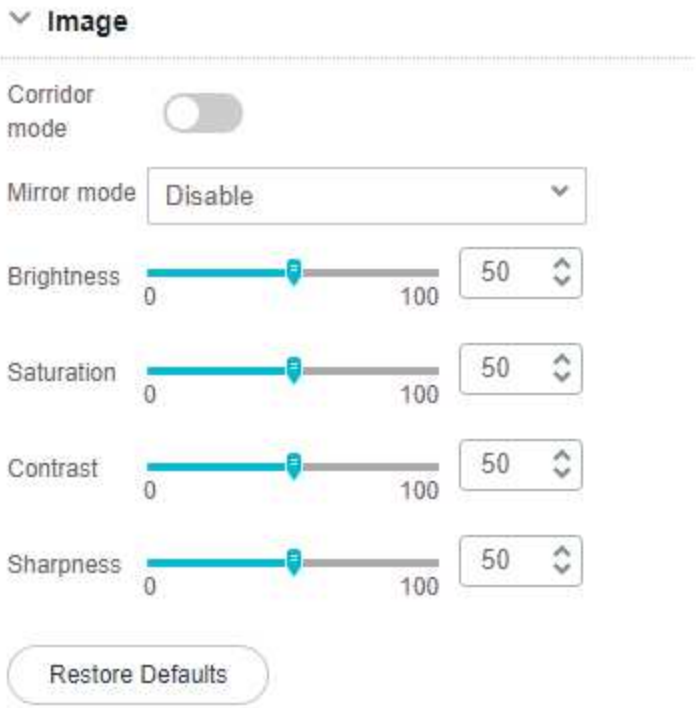


Table 1 Image adjustment parameters

Parameter	Description
Corridor mode	Indicates whether to enable the corridor mode. If it is enabled, you can flip video images by 90 degrees to set the video aspect ratio to 9:16 or 3:4. **NOTE:** • To enable the corridor mode, you are advised to rotate the box camera or bullet camera for 90 degrees to implement side installation. For fixed dome cameras, the housing must be opened and the lens be rotated for 90 degrees. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in

Parameter	Description
	occasional video stuttering. You need to set related parameters based on the site requirements. • Before enabling the corridor mode, ensure that the parking detection function is disabled.
Mirror mode	Mirroring mode, which allows you to flip video images left to right or top to bottom. • **Disable**: Disable the mirroring mode. • **Horizontal mirroring**: Flip video images left to right. • **Vertical mirroring**: Flip video images top to bottom. • **All**: Flip video images left to right and top to bottom.
Brightness	Brightness of images captured by a camera.
Saturation	Colorfulness of a color relative to its own brightness.
Contrast	Ratio of the luminance of the brightest color (white) to that of the darkest color (black) in the image. • Increasing the contrast improves the image clarity and color brightness. • Decreasing the contrast dims the entire image.
Sharpness	Quality related to the edge contrast of an image and image clarity.

Day/Night Switch

Figure 2 Day/Night switch parameters



Table 2 Day/Night switch parameters

Parameter	Description
Mode	Day/night mode, which is to help fine-tune the camera's photosensitivity when light conditions change. The options vary depending on the camera model. The options are as follows: • **Auto**: The camera automatically switches between the color mode and the B/W mode based on ambient light conditions. **NOTE:** For some camera models, if **Mode** is set to **Auto**, infrared light compensation is automatically enabled based on ambient nighttime illumination to improve the image effect. In this case, B/W images are generated. • **Color**: The camera captures color images. • **B/W**: The camera captures black and white images. • **Scheduled**: You can customize **Nighttime start from** and **Daytime start from**. This mode is applicable to scenarios that require a specified day/night switch time or a unified day/night switch time for multiple cameras.

Parameter	Description
Trigger mode	Method for triggering switch between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. The options are as follows: • **Triggered by internal signal**: Triggered by image gain. • **Image triggered**: Triggered by visible light brightness of the current image that is analyzed by the camera using the digital photosensitivity algorithm. The triggering modes may vary depending on camera model.
Sensitivity	Sensitivity for switching between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. A higher sensitivity indicates higher flexibility to switch between the B/W mode and the color mode. The value defaults to **High**.

Exposure

The following figures show exposure parameters. The exposure parameters vary depending on the camera model.

Figure 3 Exposure parameters in aperture priority mode

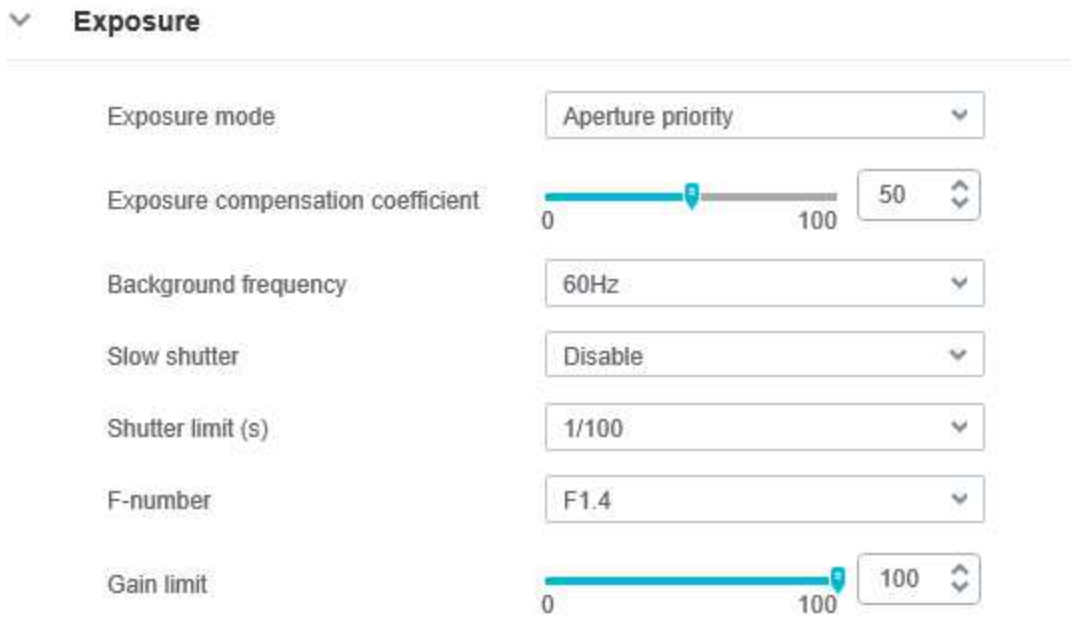


Figure 4 Exposure parameters in manual exposure mode



Figure 5 Exposure parameters in auto exposure mode



Table 3 Exposure parameters

Parameter	Description
Exposure mode	You can select an exposure mode based on the site requirements. The options are as follows: • **Auto** (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. • **Aperture priority**: The camera automatically selects a shutter speed and gain to match the manually specified aperture value. This mode is used to shoot static objects. • **Manual**: You manually set the shutter speed and gain when the auto exposure mode cannot meet the site requirements.
Exposure compensation coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure

Parameter	Description
	meter, in consideration of factors that may cause the indicated exposure to result in a less-than-optimal image. In poor light conditions, you can increase the exposure compensation coefficient to improve image brightness.
Shutter speed	This parameter is available only when you set **Exposure mode** to **Manual**. A larger value of this parameter indicates a longer exposure time.
Background frequency	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The value defaults to **Disable**. The periodic illuminance change of background light (such as strobe lights and sodium lamps) will result in horizontal banding in images. In this case, you need to set background frequency based on standard frequency of the local power grid. For example, if the standard frequency of the local power grid is 50 Hz, **Background frequency** needs to be set to 50 Hz. Disable the background frequency in natural light conditions.
Shutter limit (s)	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. This parameter is used to specify the minimum shutter speed. You can use the common values or customize values (unit: μs).
F-number	This parameter is available only when you set **Exposure mode** to **Manual** or **Aperture priority**.
Gain limit	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC).

Parameter	Description
	In the case of low illumination conditions, the AGC can be enhanced to improve image brightness. However, a high level of AGC will increase the image noise and degrade the image quality. Set this parameter based on the site requirements.
Gain	This parameter is available only when you set **Exposure mode** to **Manual**. The value defaults to **0**.
Slow shutter	The slow shutter function can be enabled or disabled only when **WDR/HLC/BLC** is set to **Disabled** or **Backlight compensation**. In other modes, the slow shutter function is disabled by default and is hidden.

Focus

Figure 6 Focus parameters



Table 4 Focus parameters

Parameter	Description
Focus mode	You can select a focus mode based on the site requirements. The options are as follows: • **Auto**: If you select this option, the camera automatically focuses on the current scene after you click  to zoom in or out. When the scene changes, the camera does not automatically focus. In this mode, you cannot

Parameter	Description
	manually adjust the focus (focus+/focus-:  , OnePush focus: ). The **Sensitivity** parameter is available only when you set **Focus mode** to **Auto**. The default value of **Sensitivity** is **Low**. • **Manual**: When this option is selected, the camera locks the focus for the current scene. In this case, the focus cannot be automatically adjusted after zooming in or out. You can only manually adjust the focus by clicking the focus icons (). • **Semi-auto** (default): When this option is selected, the camera automatically focuses on the current scene after zooming in or out (). However, when the scene is out of focus, the camera does not automatically refocus. You need to manually adjust the focus by clicking the focus icons (Focus+/-:  ; OnePush focus: ). **NOTE:** • If you click a zoom button on the PTZ control panel, the camera automatically refocuses as the scene changes. • If you click a focus button on the PTZ control panel, the camera locks the focus for the current scene and does not refocus when the scene changes.

Parameter	Description
Min. focus distance	The camera preferentially focuses on objects outside the minimum focus distance. **NOTE:** If the distance between the camera and an object is smaller than the value of **Min. focus distance**, the focus may be unclear.
Focus compensation	This function prevents the focus changes after the switch between the color mode and the B/W mode, ensuring that the objects to shoot are clear in the image.

Backlight

Figure 7 Setting WDR parameters



Figure 8 Setting HLC parameters



Figure 9 Setting backlight compensation parameters



Figure 10 Setting backlight adaptation parameters

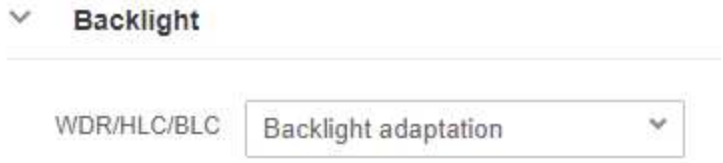


Figure 11 Setting WDR/HLC/BLC to Disabled



Table 5 Backlight parameters

Parameter	Description
WDR/HLC/BLC	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. • **Wide dynamic range**: This function is used to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. • **Highlight compensation**: This function is used to suppress large halo or image blur caused by directly radiated strong light by darkening the over-bright areas and brightening the dark areas to adjust the overall video brightness to normal.

Parameter	Description
	• **Backlight compensation**: This function is used to correct the exposure of objects in front of a bright light source. • **Backlight adaptation**: This function is used to correct the exposure of objects in front of a bright light source. • **Disabled**: None of the preceding functions takes effect.
BLC area	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Backlight compensation**. Backlight compensation is used to correct the exposure of objects in backlight scenarios. The options are as follows: **Central area**: dark area of the subject in the backlit environment. **Custom**: area customized on live video.
WDR coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Wide dynamic range**. A larger value of WDR coefficient indicates brighter backlit area in the image. The default value is **50**. WDR is intended to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. **NOTE:** You are advised not to enable the WDR function in scenarios with direct light radiation, for example, squares with road lamps (such as high-voltage sodium lamps and illuminators) at night.

Parameter	Description
HLC coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Highlight compensation**. The value defaults to **2**. A larger HLC coefficient indicates more powerful highlight compensation.

White Balance

Figure 12 White balance parameters



Table 6 White balance parameters

Parameter	Description
Mode	White balance adjusts the color circuit within a camera to remove color cast and ensure accurate color reproduction in various lighting conditions. For example, with a yellow light source, images appear yellowish. After proper white balance adjustment, the original color is reproduced. The options are as follows: • **Auto** (default): This option is recommended. The camera automatically adjusts the red and blue offsets in environments where the color temperature ranges from 2500 K to 10,000 K. Video images may be bluish in the morning or at dusk. You can drag the slider to change the values

Parameter	Description
	of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Manual**: The red and blue offsets must be adjusted manually. You can drag the slider to change the values of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Auto tracking**: The camera automatically adjusts the upper and lower limits of the color temperature in environments where the color temperature ranges from 1000 K to 15,000 K. • **One push**: This mode allows you to set the white balance mode in the current scene as the fixed mode for all scenes. Only a re-configuration can change the white balance mode. • **Indoor**: The camera automatically adjusts the red and blue offsets in indoor environments where tungsten lamps or incandescent lamps are used and the color temperature ranges from 2500 K to 5500 K. • **Outdoor**: This mode is applicable to sunny environments where the color temperature ranges from 5500 K to 6500 K. • **Fixed sodium lamp**: This mode is applicable to environments where sodium lamps are used and the color temperature ranges from 2000 K to 2300 K. • **Fluorescent lamp 1**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 2500 K to 3500 K. • **Fluorescent lamp 2**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 3500 K to 4500 K.

Parameter	Description
	• **Incandescent lamp**: This mode is applicable to environments where incandescent lamps are used and the color temperature ranges from 2700 K to 2900 K. • **Sunlight**: This mode is applicable to environments where green plants occupy more than 80% of the video image. This mode can alleviate the phenomenon that the white area appears reddish in this scenario.

Image Enhancement

The image enhancement functions vary depending on the camera model.

Figure 13 Overcast adaptation mode

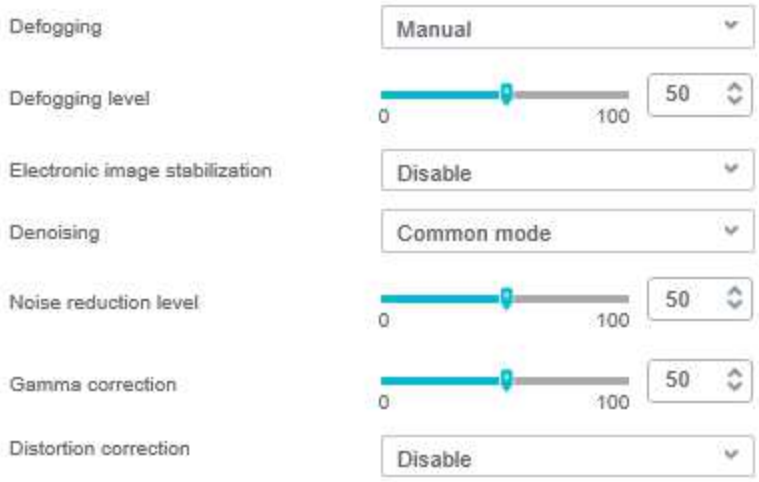


Table 7 Image enhancement parameters

Parameter	Description
Defogging	This function is used to increase the image clarity in poor weather conditions such as rain, fog, and smog. To disable this function, set this parameter to **Disable**.

Parameter	Description
	After the function is enabled, the camera determines whether to enable the defogging function based on the actual environment conditions. You can set the defogging level when this parameter is set to **Manual**. A higher defogging level indicates clearer images. However, a too high level will lead to image distortion. You need to set the defogging level based on the site requirements. **NOTE:** • Some camera models support the overcast adaptation mode but do not support the auto mode. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements.
Electronic image stabilization	Indicates whether to enable electronic image stabilization (EIS). EIS is used to compensate image vibration reversely to stabilize images when the camera is subject to vibrations, while some image details may be lost. The value defaults to **Disable**. In a short-focus scenario, if there are many moving objects, the camera may make misjudgment. Therefore, you are advised to enable this function in long-focus scenarios. When **Electronic image stabilization** is set to **Enable**, **Image stabilization sensitivity** can be set for some camera models, which is subject to the GUI. Higher sensitivity indicates better image stabilization effect. Set **Image stabilization sensitivity** based on the site requirements.

Parameter	Description
	NOTE: • Some camera models support electronic image stabilization. • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements. • Enabling the electronic image stabilization function will slightly influence camera's field of view. For PTZ dome cameras, the PT speed at level 10 when this function is enabled differs from that when the function is disabled.
Denoising	Indicates whether to enable the noise reduction function. The options are as follows: • **Disable**: Disable the noise reduction function. • **Common mode** (default): In this mode, you can set **Noise reduction level**. A higher noise reduction level indicates better noise reduction effect but lower image clarity. The value defaults to **50**. • **Expert mode**: In this mode, you can set **Temporal denoising level** and **Spatial denoising level**. ▪ **Spatial denoising level**: Spatial noise reduction intends to reduce the noises on images horizontally and vertically at the cost of some edge details. A higher spatial noise reduction level indicates better noise reduction effect and smoother edges. ▪ **Temporal denoising level**: Temporal noise reduction intends to reduce the white noises

Parameter	Description
	distributed randomly between video frames to improve the image quality in low-light conditions. However, the noise reduction effect is affected by historical frame data, causing object trailing on images. A higher temporal noise reduction level indicates better noise reduction effect but more apparent trailing.
Gamma correction	This function is used to adjust and improve the image contrast to avoid new image noise.
Distortion correction	Lens distortion is an aberration that causes straight lines to curve near the edges of images. Distortion occurs when a short-focus or wide-angle lens is used to shoot large objects (such as high buildings) with distinct shapes. To ensure more accurate detection, distortion correction is required. • **Distortion correction**: You can select **Enable** or **Disable** from the drop-down list box to enable or disable the distortion correction function. • **Distortion correction mode**: Select a mode based on the site requirements. ▪ **Automatic**: In this mode, the camera automatically corrects the image based on the image analysis result. ▪ **Manual**: In this mode, the correction level can be configured. A higher level indicates a higher correction strength. You are advised to use the default value **50**. **NOTE:** • Some camera models do not support distortion correction. • If a privacy mask area is drawn, enabling distortion correction may disclose the privacy mask area. In

Parameter	Description
	this case, you need to draw a new privacy mask area.

Illuminator Control

Figure 14 Setting illuminator control parameters

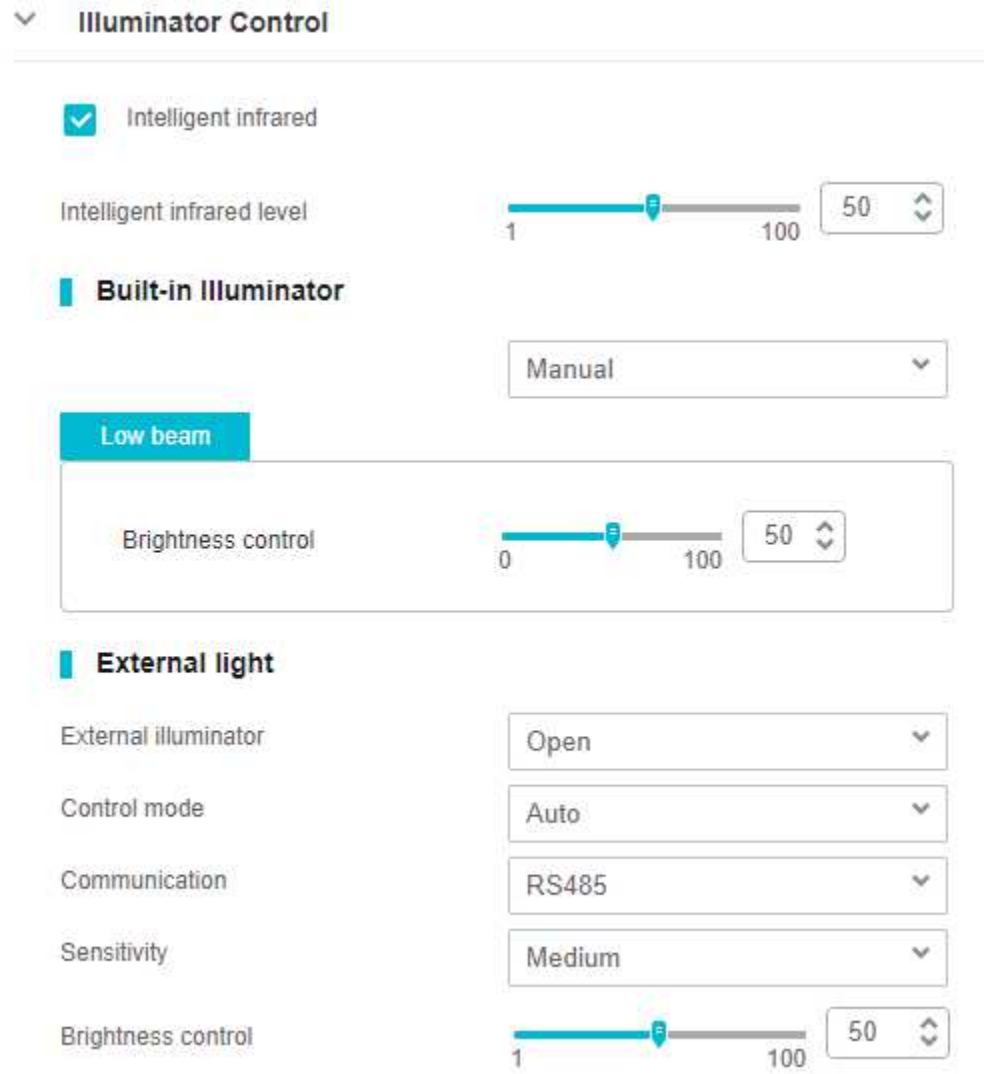


Table 8 Illuminator control parameters

Parameter	Description

Parameter	Description
Intelligent Infrared	If this parameter is selected, the infrared illuminator is enabled to avoid image overexposure. The function is enabled by default.
Intelligent infrared level	The default value is **50**. If overexposure occurs in scenarios with strong reflective objects such as leaves and wires nearby, you can set this parameter to a larger value.

Parameter		Description
Built-in light	Control mode	• **Auto** (default): Indicates that the camera automatically turns on or off the illuminator and controls its illuminance. • **Manual**: Indicates that the brightness can be manually controlled. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the illuminator will be turned off. • **Scheduled**: Indicates that the illuminator is automatically enabled and disabled at the specified time. You can customize **Turn on time**, **Turn off time**, and **Brightness control**. • **Intelligent**: Indicates that the illuminator is enabled and disabled based on the ambient light conditions. You can select this option when **Mode** under **Day/Night Switch** is set to **Auto**. After **Control mode** is set to **Intelligent**, the camera automatically turns on or off the illuminator and controls its illuminance. If the camera detects an alarm in B/W mode, the white-light illuminator is automatically turned on and the video image automatically turns to the color mode. After the alarm is cleared, the white-light illuminator is automatically turned off and the video image turns back to the B/W mode. **NOTE:**

Parameter		Description
		• In automatic mode, illuminators are automatically enabled or disabled based on the ambient illuminance. White-light illuminators work only in color mode, and IR illuminators work only in B/W mode. • In manual mode, the device determines whether to enable white-light or IR illuminators based on the current ambient illuminance. The user-defined brightness takes effect only when the device determines that illuminators need to be enabled. • Some camera models do not have white-light illuminators. • When **Control mode** is set to **Intelligent**, if the number of alarms generated within 10 minutes is greater than or equal to 4, the white-light illuminator will be on for 3 minutes. Otherwise, the white-light illuminator will be on for 1 minute.

Parameter	Description

Parameter		Description
	Low beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the low beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the low beam.
	Mid beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the mid beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the mid beam.
	High beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If

Parameter		Description
		Brightness control is set to **0**, the high beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the high beam. **NOTE:** • If **Mode** under **Day/Night Switch** is set to **Color**, high beam control does not take effect.
	Brightness control	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. A larger value indicates higher illuminator brightness.

Parameter		Description
External light	External illuminator	**Open**: Turns on the external illuminator. **Close** (default): Turns off the external illuminator.

Parameter		Description
	Control mode	• **Auto** (default): Indicates that the camera automatically controls the illuminator status (turned on or off) and brightness. • **Scheduled**: Indicates that you can customize **Turn on time**, **Turn off time**, and **Brightness control**.
	Communication	• **IO**: The illuminance of the external illuminator cannot be adjusted. This mode can be selected when the external illuminator is connected to the camera through the alarm-out port. • **RS485**: The illuminance of the external illuminator can be adjusted. This mode can be selected when the external illuminator is connected to the camera through the RS-485 port. • **RS485 (unified protocol)**: **NOTE:** • Only bullet cameras support the **RS485 (unified protocol)** communication mode.
	Sensitivity	• Sensitivity for determining the ambient illuminance threshold. A higher sensitivity indicates a lower threshold and a higher possibility of turning on illuminators. • This parameter can be set to **High**, **Medium** (default value), or **Low**.

Parameter		Description
	Brightness control	This parameter is available only when **Control mode** is set to **Auto** or **Scheduled**. A larger value indicates higher illuminator brightness.

Digital Zoom

Figure 15 Setting digital zoom parameters



Table 9 Digital zoom function

Digital zoom	You can select **Enable** from the drop-down list box to enable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the system will perform digital zoom and continue to zoom in on the image. However, the focal length is not changed.
	You can select **Disable** from the drop-down list box to disable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the image is not changed.

Parent topic: Configuring Images

Configuring OSD

You can set on-screen display (OSD) parameters to specify the information to be displayed and the display effect.

Setting OSD Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **OSD** and use the default value of **Channel**. The page shown in Figure 1 is displayed. The parameters vary between camera models.

   Figure 1 Setting OSD parameters



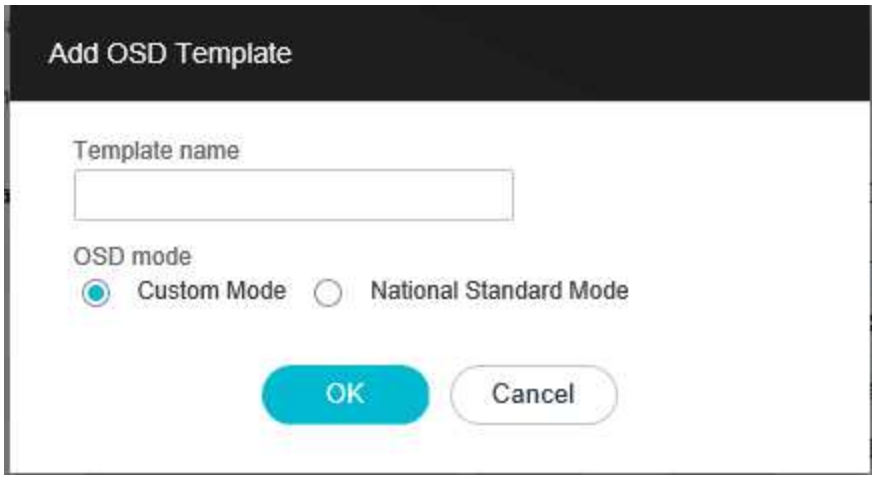
Figure 2 Setting GB-compliant OSD parameters



3. Configure the OSD template. Table 1 describes the OSD template parameters and buttons.

   - Click **Add OSD Template**. In the dialog box that is displayed, enter a name of the new template, set OSD mode, and click **OK**, as shown in Figure 3.

     Figure 3 Adding an OSD template

     NOTE

A maximum of eight OSD templates can be added.

- Select an OSD template and click **Copy OSD Template**. In the dialog box that is displayed, enter a new template name and click **OK**. The new template is added. The reference size of the new template is the same as that of the selected template.
- Select an OSD template and click **Delete OSD Template**. In the dialog box that is displayed, click **OK** to delete the template.

Table 1 OSD template parameters/buttons

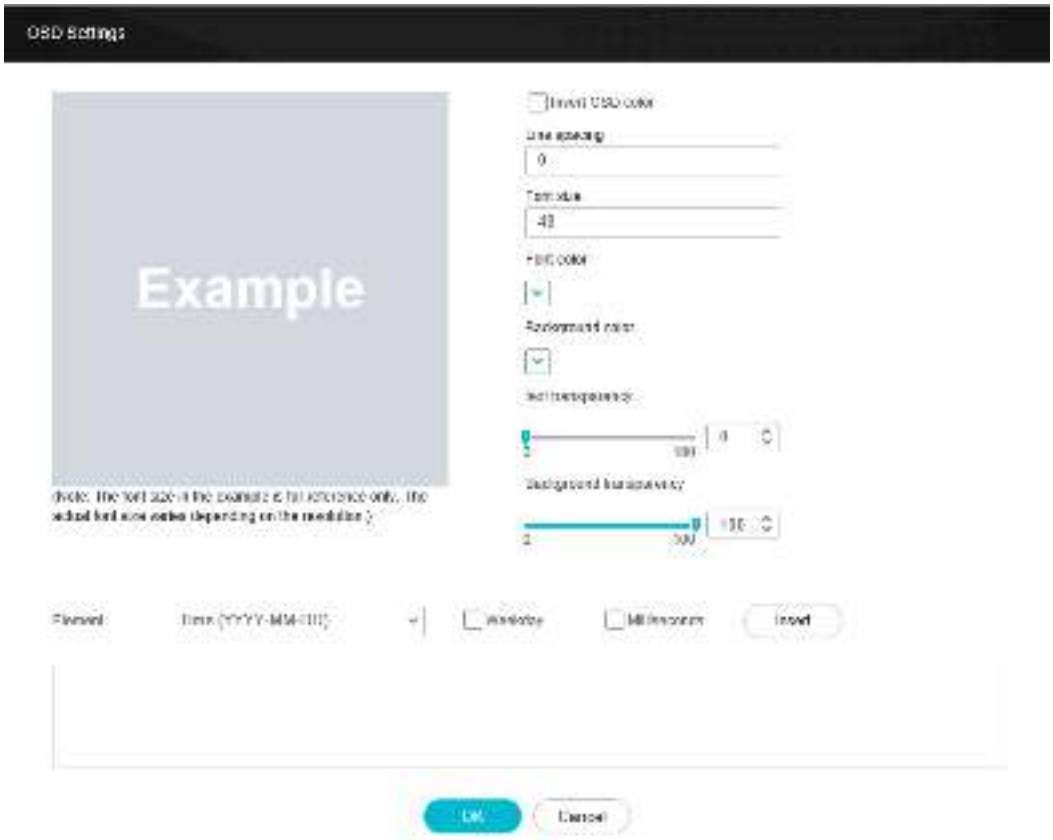
Parameter/Button	Description
Custom Mode	Custom OSD mode. If this mode is selected, you can add an OSD template with customized contents.
National Standard Mode	GB-compliant OSD mode. If this mode is selected, you must add a GB-compliant OSD template, in which the position and number of OSDs must be set to provided values, and other contents can be customized.
Template name	Name of the selected template. You can customize the name as required.
Minimum margin (characters)	Distance (maximum number of characters) between the OSD's edge and the edge of live video images. You can select a value from the drop-down list. This function is available only when a GB-compliant OSD template is added.
Reference size	The default value varies depending on the camera model. You cannot change the value of this parameter.

Parameter/Button	Description
Add OSD	Button for adding an OSD record using a template. **NOTE:** A maximum of eight OSD records can be added to each customized OSD template. In GB-compliant mode, the number of OSD records is fixed to four. You can only select one for use but cannot add or delete one. The OSD template name cannot contain vertical bars (|).
Delete All	Button for deleting all OSD records from a customized OSD template.
Enable	Indicates whether to display an OSD record on the video image. After you select the check box corresponding to an OSD record in the **Enable** column, the OSD record is displayed on the video image.
Align Type/Horizontal Margin/Vertical Margin/Content	These functions are available only for customized OSD templates. OSD alignment mode. You can select an option from the drop-down list. Horizontal and vertical margins. You can enter specific numbers in the **Horizontal Margin** and **Vertical Margin** text boxes to specify the margins.

Parameter/Button	Description
Content	OSD content. You can specify or change the OSD content in the text box at the bottom of the dialog box that is displayed after you click in the **Operation** column. **NOTE:** If the image overlay function is enabled, a maximum of seven OSD records are supported. Enabling the eighth OSD record will disable the image overlay function.
Operation	Column containing two icons and , which are available only for OSD records in custom mode. In GB-compliant mode, only the icon is available. : icon for modifying an OSD record. After you click this icon next to an OSD record, the **OSD Settings** dialog box is displayed. : icon for deleting an OSD record. After you click this icon next to an OSD record, the **Delete OSD Area** dialog box is displayed. You can click **OK** to delete the OSD record.

4. Click . The **OSD Settings** dialog box is displayed, as shown in Figure 4.

Figure 4 OSD Settings dialog box



5. Set OSD parameters based on the site requirements. Table 2 describes the parameters.

Table 2 OSD parameters

Parameter	Description
Invert OSD color	Indicates whether to set the OSD text color to a color opposite to the background. If you enable this function, the **Font color**, **Background color**, **Text transparency**, and **Background transparency** parameters will become unavailable.
Line spacing	OSD line spacing.
Font size	OSD text size. You can enter a value in the text box.

Parameter	Description
Font color	Color of the text displayed on the screen. This parameter is available only when you deselect **Invert OSD color**.
Background color	OSD background color. This parameter is available only when you deselect **Invert OSD color**.
Text transparency	Transparency of the OSD text. This parameter is available only when you deselect **Invert OSD color**.
Background transparency	Transparency of the OSD background. This parameter is available only when you disable **Invert OSD color**.
Element	Insertion element which can be selected from the drop-down list box. You can click **Insert** to insert the selected element. Different camera models may have different parameters. You can drag the text to adjust the text display location in the live video viewing area. • **Time/Display date/Display time/Weekday/Milliseconds**: You can select the time display format and select whether to display the week and millisecond. If multiple OSDs are added and **Milliseconds** is selected, the millisecond displayed in these OSDs may vary. • **PTZ information**: Display the coordinates and zoom information the PTZ device on the video image. • **Latitude and longitude**: Display the latitude and longitude information on the video image.

Parameter	Description
	• **Azimuth**: Display the azimuth information on the video image. • **OSDI**: Display OSDI on the video image. After the OSDI content is configured, **N/A** is displayed on the video image. To display the OSDI content, you need to enable OSDI first under **Configuration** > **PTZ** > **Location**. The OSDI content is displayed only when OSD coordinates are within the OSDI range. **NOTE:** The elements to be inserted vary depending on the camera model.

NOTE

- You can preview the font color, background color, text transparency, and background transparency in the **Example** area.
- If the aspect ratio of live video is different from that of images, for example, the aspect ratio of live video is 4:3 and that of images is 16:9, the OSD font cannot be scaled proportionally.

6. Click **Save**.

Parent topic: Configuring Images

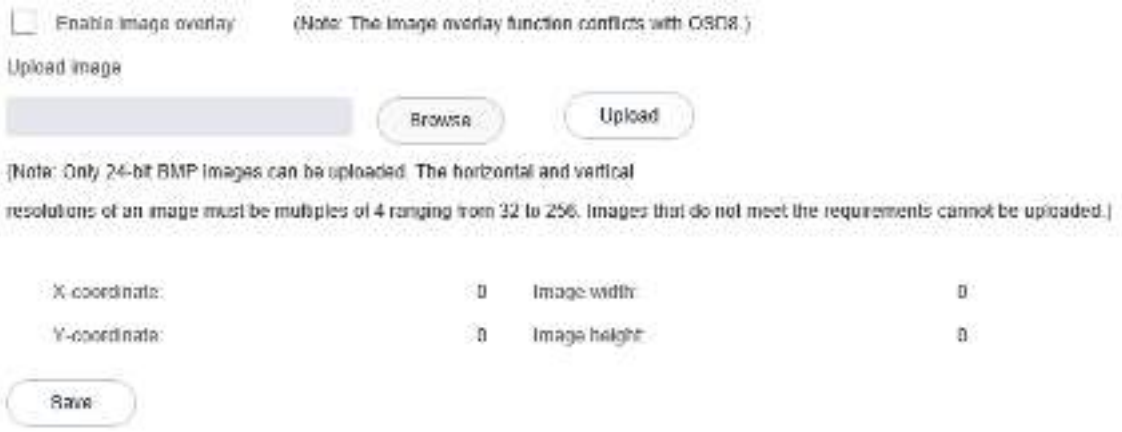
Configuring Image Overlay

You can configure image overlay to superimpose images on live video and manually captured live video images. You can also upload an image, for example, a logo, for display based on the site requirements.

Setting Image Overlay Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Image Overlay** and use the default value of **Channel**. The page shown in Figure 1 is displayed.

   Figure 1 Image overlay settings

3. Click **Browse** and select an image.

   > **NOTE**
   >
   > The image format and resolution requirements vary depending on the camera model.

4. Click **Upload**.
5. Select **Enable image overlay**.
6. Click **Save**.

   > **NOTE**

If the image overlay function is enabled, a maximum of seven OSD records can be enabled. If eight OSD records are enabled, the settings will fail to be saved. In this case, you need to disable one OSD record on the **OSD** page.

7. View the image overlay effect in the live video viewing area. You can use the mouse to adjust the image display position.

   Set **X-coordinate** and **Y-coordinate** of the position where the upper left corner of the image will be displayed.

Parent topic: Configuring Images

Configuring an Image Profile

By configuring and invoking an image profile, you can quickly utilize configurations of the image parameters in common scenarios.

Context

An image profile is a template containing predefined configurations of image parameters. By configuring image profiles, you can preset various image parameters to specified values to facilitate quick invocation.

Setting Image Profile Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Profiles** and use the default value of **Channel**.
3. Click **Image**. The page shown in Figure 1 is displayed.

   Figure 1 Image area

4. Select an image profile as required and click **Enable**.

   Table 1 describes the default image profiles.

   Table 1 Default image profiles

Profile	Description
Outdoor	Applicable to outdoor scenes where light changes, for example, squares and shopping mall peripheries.
Indoor	Applicable to indoor scenes where stable illumination is available, for example, offices and counters.

Profile	Description
Dimmed	Applicable to environments where illumination is low for a long period of time, for example, underground parking lots and power distribution rooms.
Virtual checkpoint	Applicable to scenes where moving vehicles and license plates need to be captured, for example, roads and stadiums.
Backlit	Applicable to backlight environments with great contrast to the foreground, such as roads and gates.
Overcast	Applicable to foggy scenes.
Target	Applicable to scenes that require target recognition.

NOTE

- Table 1 lists the image profiles in different scenes. Different models of cameras support different image profiles, which are subject to the actual ones displayed in the camera web system.
- You can add image profiles by referring to Step 5 through Step 7.

5. Click **Add Image Profile**. You can also select a default profile and click **Copy Image Profile** for further modification.

   The **Add Image Profile** dialog box is displayed, as shown in Figure 2.

Figure 2 Add Image Profile dialog box



6. Set image profile parameters.

   Enter the image profile name and description, and set image parameters. For details about how to set image parameters, see Setting Image Parameters.

7. Click **Save**.

8. **Optional:** (Optional) To edit or delete an existing image profile, select the image profile and click or .

   Default image profiles cannot be edited or deleted.

   If you click **Restore Defaults**, the parameters on the **Profiles** tab page will be restored to default settings.

Configuring a Profile Plan

After an image profile plan is configured, the system can execute an image profile by day or year. After profile linkage is configured, the profiles will be automatically switched when the camera switches between the color mode and the B/W mode.

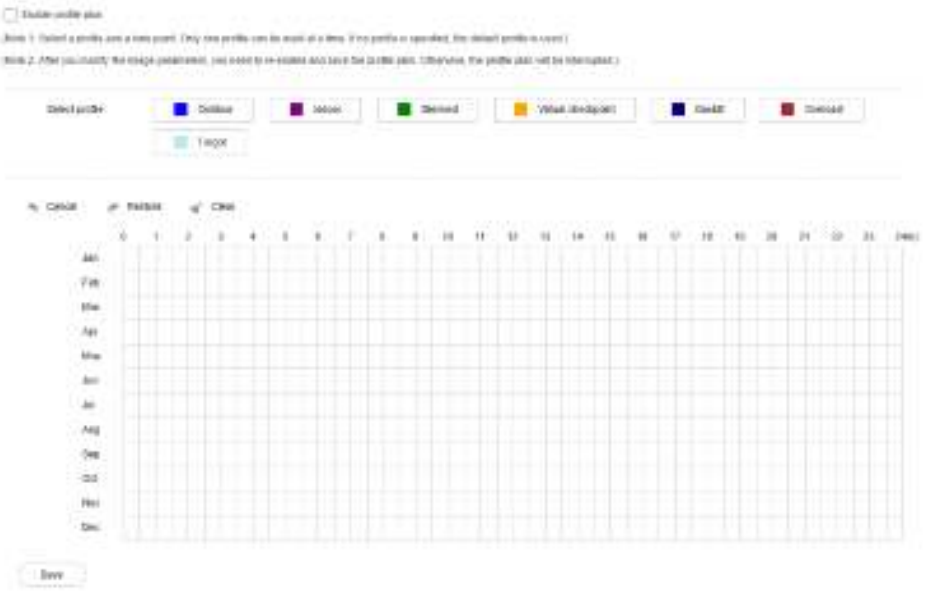
NOTICE

To ensure that the profile plan and the profile linkage function take effect properly, the following conditions must be met:

- For some camera models, if **Full frame rate** is set to **50Hz** or **60Hz** under **Configuration** > **Video/Audio** > **Video**, ensure that the WDR function is disabled. If the WDR function is enabled, do not set **Full frame rate** to **50Hz** or **60Hz**.
- The area cropping and electronic image stabilization functions cannot be enabled at the same time.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Profiles** and use the default value of **Channel**.
3. Click **Profile Plan**. The page shown in Figure 1 is displayed.

   Figure 3 Profile Plan area



NOTE

- Different models of cameras support different image profiles.
- You can click **Cancel** to undo the previous operation.
- You can click **Restore** to restore the last undone operation. Cleared profiles cannot be restored.
- You can click a profile and click to delete the profile, or you can click **Clear** to delete all profiles.

4. Select a profile. Then, select the time span in the table for plan execution. Only one profile can be executed at a time.
5. Select **Enable profile plan**.
6. Click **Save**.

Configuring Profile Linkage

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Profiles** and use the default value of **Channel**.
3. Click **Profile Linkage**. The page shown in Figure 4 is displayed.

   Figure 4 Profile Linkage area



4. Select **Enable profile linkage**.
5. Set the profiles associated with **Color mode** and **Black and white mode** as required.

   After the profile linkage is configured, the profiles will be automatically switched when the camera switches between the color mode and the B/W mode based on the operating environment.

   NOTE

   The profile linkage takes effect only when **Mode** is set to **Auto** under **Configuration** < **Image** > **Display** > **Day/Night Switch**. Setting an image profile when the profile linkage is in use will interrupt the linkage relationship. In this case, you need to configure the profile linkage again.

6. Click **Save**.

Parent topic: Configuring Images

Configuring Privacy Mask

You can mask a specified area on live video images to protect sensitive or private information.

NOTICE

- No camera model supports privacy mask when distortion correction is enabled. Enabling distortion correction may disclose the privacy mask area. Exercise caution when using this function.
- Only PTZ dome cameras support privacy mask when lens zooming is enabled. For other cameras, lens zooming may disclose the privacy mask area. Exercise caution when using this function.

Setting Privacy Mask Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Privacy Mask** and use the default value of **Channel**. The page shown in the following figure is displayed. The parameters displayed on the web page vary depending on the camera model.

   Figure 1 Privacy mask settings

3. Select **Enable** to enable the privacy mask function.
4. Click **Add Mask**.

Draw a privacy mask area on the live video image.

NOTE

- Operations on a privacy mask area take effect only after they are saved. You can perform operations on only one privacy mask area at a time.
- After electronic image stabilization or distortion correction is enabled or disabled, you need to reconfigure the privacy mask area.
- You can draw a maximum of one monochromatic rectangular privacy mask area. You can set the color for the area. The default color is black. You can drag a privacy mask area to adjust its position.

5. Click **Save**.
6. Go to the **View** page and check whether the location and size of the privacy mask area meet the requirements.
   - If so, the configuration is complete.
   - If not, configure the privacy mask area again.

NOTE

To modify or delete a privacy mask area, select its ID in the **No.** column and click or .

Setting Mosaic Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Privacy Mask** and use the default value of Channel. The page shown in Figure 2 is displayed.

Figure 2 Privacy mask settings



3. Select **Enable** to enable the privacy mask function.
4. Click **Add Mosaic**.

> **NOTE**
>
> - Only some camera models support mosaic areas.
> - Operations on a privacy mask area take effect only after they are saved. You can perform operations on only one privacy mask area at a time.
> - For cameras other than PTZ dome cameras, you can draw a maximum of four rectangular mosaic areas. For PTZ dome cameras, you can draw up to 32 rectangular mosaic areas, but a maximum of four mosaic areas can be displayed on the same image. You can drag a mosaic area to adjust its position and size.

5. Click **Save**.
6. Go to the **View** page and check whether the location and size of the mosaic area meet the requirements.
   - If so, the configuration is complete.
   - If not, configure the mosaic area again.

> **NOTE**
>
> To modify or delete a mosaic area, select its ID in the **No.** column and click or .

Parent topic: Configuring Images

Configuring Area Focus

After you configure area focus, the area with a higher focusing priority will be preferentially focused when the focusing function of a camera is triggered.

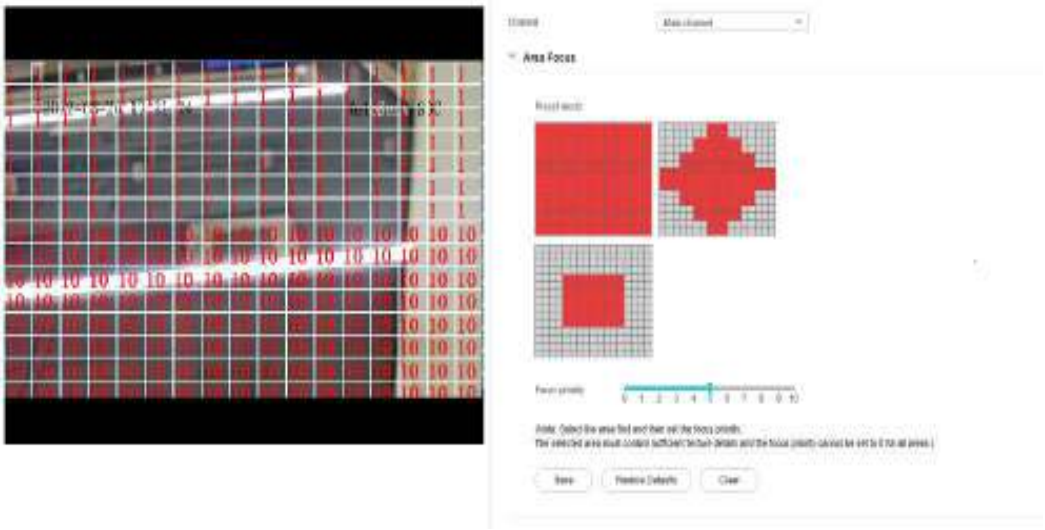
NOTE

Only some camera models support focus area selection.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Area Focus** and use the default value of **Channel**. The page shown in Figure 1 is displayed.

   Figure 1 Area Focus area

3. Drag the mouse to select an area to be focused and adjust its position and size. Ensure that the selected area contains adequate texture details. Otherwise, images in the area may be unclear after focusing.

4. Set **Focus priority** to a value other than 0. If you click **Restore Defaults**, the preset focus priority will be reset to the default status. Figure 1 shows the focus priorities of focus areas in target capture mode. Figure 2 and Figure 3 show the focus priorities of focus areas in other intelligence modes. The default focus priorities displayed vary between camera models.

Figure 2 Default focus priorities (1)

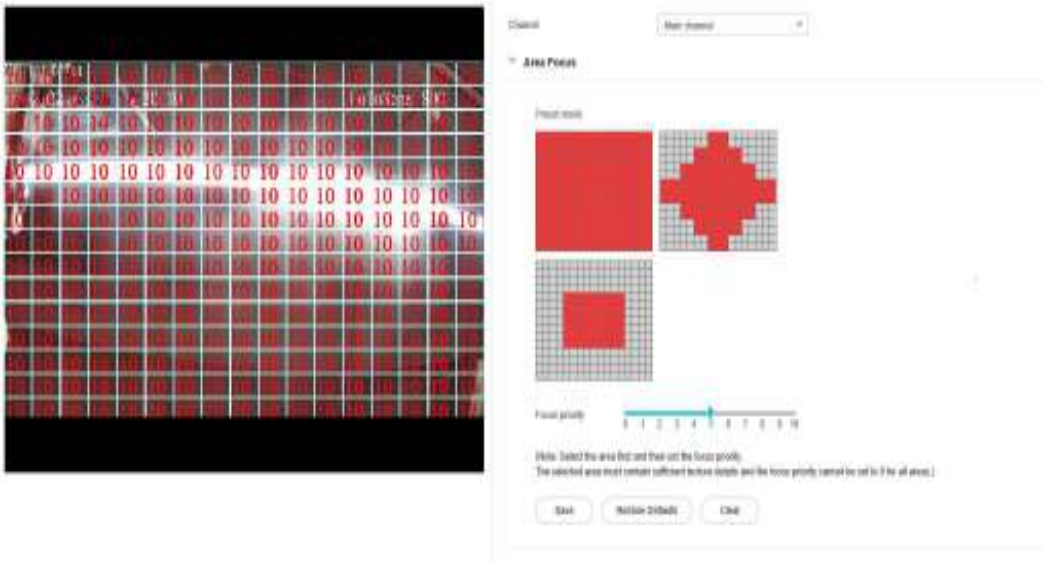
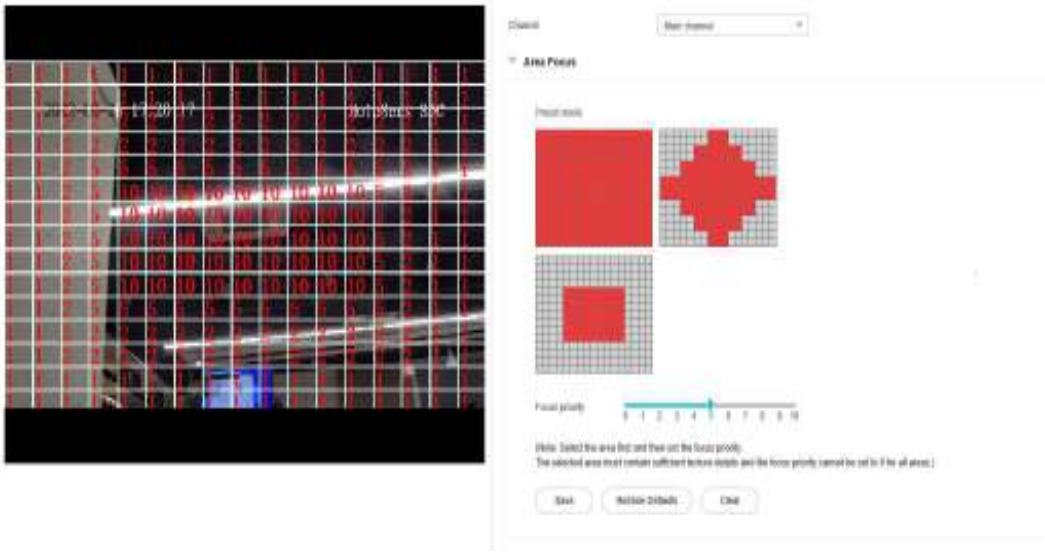


Figure 3 Default focus priorities (2)



NOTE

- You can select a preset mode to quickly set an area to be focused. The focus priority in a preset mode is 10.
- You can click **Clear** to reset the area.

5. Click **Save**.

Parent topic: Configuring Images

Configuring a White Balance Area

After a white balance area is configured, the white balance function takes effect in the selected area only.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **White Balance Area** and use the default value of **Channel**. The page shown in Figure 1 is displayed.

   Figure 1 White Balance Area

3. Drag the mouse to select a white balance area and adjust its position and size.
4. Click **Save**.

> **NOTE**
>
> - If you click **Restore Defaults**, the white balance function takes effect on the whole video image.
> - If you click **Clear Selected**, the configured white balance area is cleared and you can configure a white balance area again.

Parent topic: Configuring Images

Playback

This section describes how to query, download, and delete recordings, configure recording plans, and play back recordings.

Playing Back Recordings You can play back recordings in the camera web system.

Downloading Recordings
This section describes how to query, combine, and download recordings.

Parent topic: Configuration

Playing Back Recordings

You can play back recordings in the camera web system.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Playback**. The **Playback** page is displayed by default, as shown in Figure 1.

   Figure 1 Playback page

3. Search for recordings.

   a. On the right of the page, set **Channel**, **Start Time**, **End Time**, and **Recording type**.

   - The maximum interval between **Start Time** and **End Time** is 24 hours.
   - The following recording types are supported:
     - **Triggered**: Some intelligent functions of cameras can trigger server-based recording directly. To enable this function, go to the **Linkage Policy** page and select **Enable recording**.

- **Manual SD card-based recording**: You can select this check box to trigger SD card-based recording on the live video image to record live video.
- **Scheduled**: You can configure a recording plan for cameras to perform recording in a specified period. For details about how to configure a recording plan, see Configuring a Recording Plan.
- **Buffered**: When cameras are disconnected from the network, they can continue to shoot and temporarily store video on their SD cards. When the network is restored, the video security platform sends a video request to the cameras. The cameras then send the video stored on the SD cards to the video security platform. For details about how to enable video buffering, see Configuring Storage Management.

b. Click **Search**.

Search results are displayed on the left. A maximum of 64 recording segments can be queried. When the number of recording segments during the specified period exceeds 64, the message "Video segments are more than 64" is displayed. You need to change the start time.

4. Select the desired recording and play it back.

- Click  to start recording playback.
- Click  to pause recording playback.
- Click  to stop recording playback.
- Drag  to adjust the playback progress and play the recording from the time point specified by 

Parent topic: Playback

Downloading Recordings

This section describes how to query, combine, and download recordings.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Playback** > **Download**. The **Download** page is displayed, as shown in Figure 1.

   Figure 1 Download page

3. Search for recordings.

   a. Set **Channel** and **Period**.

   b. (Optional) Combine recording segments. Select **Combine recordings** on the right of **Period**. The system combines adjacent short recording segments with the same encoding format into one recording file whose duration does not exceed 10 minutes. The duration of a combined recording cannot exceed 10 minutes. If the duration will exceed 10 minutes after a recording segment is combined, this recording segment will start the next combined recording file. For example, if the first recording segment is 8 minutes, the second is 3 minutes, and the third is 5 minutes, the first recording segment is filtered out as an independent recording file, and the second and third recording segments are combined into one recording file.

   c. Click **Search**.

      The results are displayed below.

      NOTE

      - The maximum size of a recording segment is 256 MB.

- You can query a maximum of 500 recording segments at a time. If the number of recording segments within the specified query period exceeds 500, change the start time and end time.
- The same encoding format indicates that the video encoding protocol, video resolution, audio encoding format, audio bit rate, and audio sampling rate of each recording segment are the same.
- The video format during the search is different from that after download, so the actual size of the downloaded recording may be different from the size of the found recording.
- Generated recordings will be saved as multiple recording files with varied sizes based on the recording types, such as alarm-triggered recording and scheduled recording. For details, see Why Is a Recording Separately Stored into Multiple Files of Different Sizes?.

4. Download recordings.

   a. Select the recording to download.

   b. Click **Download**.

NOTE

- You can click **Stop Downloading** to stop downloading recordings.
- If you leave this page, recording download will be terminated.
- The supported number of recording download channels vary based on the camera model. A maximum of four channels of recordings can be downloaded at a time.
- You need to use the download function provided by the browser to download recordings.

Parent topic: Playback

Image Query and Download

You can query and download images on the web page.

Downloading Snapshots You can download snapshots stored in SD cards of cameras to the local computer or view snapshots online.

Parent topic: Configuration

Downloading Snapshots

You can download snapshots stored in SD cards of cameras to the local computer or view snapshots online.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Snapshot**. The snapshot download page is displayed, as shown in Figure 1. Table 1 describes the parameters.

   The web page varies between camera models.
3. Set **Channel**, **Snapshot type**, and **Period**, and click **Search** to search for the snapshot to be downloaded. Here, a target capture camera is used as an example.

   Figure 1 Configuring snapshot download

   Table 1 Snapshot download parameters

Parameter	Description
Snapshot type	You can search for snapshots stored in the SD card of the camera by snapshot type. Different camera models support different snapshot types. • **Manual**: manual snapshots. To manually take a snapshot, on the client of the platform connected to the camera, right-click the live video image, choose **Snapshot** > **Server**. Then, the system automatically takes a snapshot of the current video image and saves the snapshot to the SD card of the camera. • **Alarm-triggered**: alarm-triggered snapshots. If snapshot taking is enabled in the alarm linkage configuration and an alarm is generated, the camera takes snapshots and stores the snapshots to the SD card of the camera.

Parameter	Description
	• **Scheduled**: scheduled snapshots. To enable the scheduled snapshot function, choose **Configuration** > **Storage** > **Snapshot Parameters** > **Scheduled Snapshot** and select **Enable**. After this function is enabled, the camera takes snapshots based on the snapshot interval and saves the snapshots to the SD card of the camera. • **Target capture**: To enable target capture, choose **Configuration** > **Intelligence** > **Target Intelligence** and toggle-on **Target snapshot**. After this function is enabled, when a pedestrian passes by, the camera automatically captures target and person images of the pedestrian and saves the images to the SD card of the camera. • **Intelligent**: snapshots triggered by intelligent analysis tasks. If intelligent functions such as object classification, vehicle and pedestrian detection, and vehicle event detection are enabled under **Configuration** > **Intelligence**, the camera automatically takes snapshots of motor vehicles, non-motorized vehicles, and pedestrians and saves the images to the SD card.
Period	Start time and end time for querying snapshots.

4. Select the snapshot to download and click **Download**. After the snapshot is downloaded, you can double-click the snapshot to open it or obtain the snapshot under **C:\Users\..\IPC_MediaPlayer\CaptureUpload** on the local computer.

NOTE

- If you select **All**, all snapshots searched out can be downloaded. You can query a maximum of 4096 snapshots.
- The OSD time displayed on some snapshots taken before the power-off may be the time after the power-off, because there is an interval between the time for writing camera database records and the time for writing image block file data.

Parent topic: Image Query and Download

Configuring PTZ Control

This section describes how to set pan-tilt-zoom (PTZ) parameters, including serial port, preset position, and tour parameters.

PTZ Feature Differences

Configuring Preset Positions
After a preset position is configured, you can quickly steer the camera to this position. You can add, modify, and delete preset positions. A maximum of 512 preset positions (including a home position) can be added for a camera.

Configuring Tours
You can configure a tour that consists of multiple preset positions. After you enable the tour, the camera shoots video along the tour. You can set a maximum of 16 tours. Each tour can consist of a maximum of 512 preset positions.

Configuring Pattern Scan
You can set pattern scan parameters to customize a scan path.

Configuring Scan Limits
You can set left and right scan limits to limit the camera's scan area.

Configuring PTZ Control
This section describes how to set PTZ control parameters, including **Vertical rotation restriction(°)**, **Max pan speed (°/s)**, and **Max tilt speed (°/s)**.

Configuring Location Information
You can set the OSDI zone by setting the coordinates.

Configuring Park Actions
You can set a park action for the camera. If you do not control the PTZ device within a specified period, the PTZ device automatically performs the specified park action.

Configuring the Serial Port

You can set parameters, for example, serial port parameters and transparent channel parameters, for connecting the PTZ device to a camera through the serial port.

Parent topic: Configuration

PTZ Feature Differences

This section describes differences in PTZ feature configurations supported by different camera models. Table 1 describes the differences.

NOTE

The PTZ function can be implemented only when the bullet cameras and fixed dome cameras listed in the table are connected to an external PTZ device through the RS-485 port. The following table lists the specific PTZ functions that are supported.

Table 1 Differences in PTZ feature configurations

Device Model	Preset Position, Home Position, Tour, Horizontal Scan, and Park Action	Video Freezing at Preset Positions	Pattern Scan, Limit Scan, Vertical Scan, Random Scan, Frame Scan, and Panoramic Scan	OSDI	Wiper Control	Built-in PTZ	External PTZ	Serial Port Parameters	Transparent Channel	PTZ Control Channe
HWT-D6550-10-Z33-SV	YES	YES	YES	YES	NO	YES	NO	NO	NO	NO
HWT-D3040-10-ELI-PV (2.8 mm)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
HWT-D2122-10-SIU	NO	NO	NO	NO	NO	NO	YES	YES	YES	NO
HWT-D2152-10-SIU	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO
HWT-D3222-10-SIU	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO
HWT-D3252-10-SIU	NO	NO	NO	NO	NO	NO	NO	YES	YES	NO

Parent topic: Configuring PTZ Control

Configuring Preset Positions

After a preset position is configured, you can quickly steer the camera to this position. You can add, modify, and delete preset positions. A maximum of 512 preset positions (including a home position) can be added for a camera.

The actual web page varies depending on the camera model.

Context

The camera's pan angle, tilt angle, and zoom ratio can be stored as a preset position. Preset positions can be numbered.

Configuring a Preset Position

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Preset Position**. The **Preset Position** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set preset position parameters for the channels separately.

   Figure 1 Setting preset positions

NOTE

- If no home position is configured, the default name displayed is **Home position (Not set)**. If a home position is configured, the default name displayed is **Home position (Custom location)**.
- The home position cannot be deleted.

3. Select **Freeze video at preset position**.

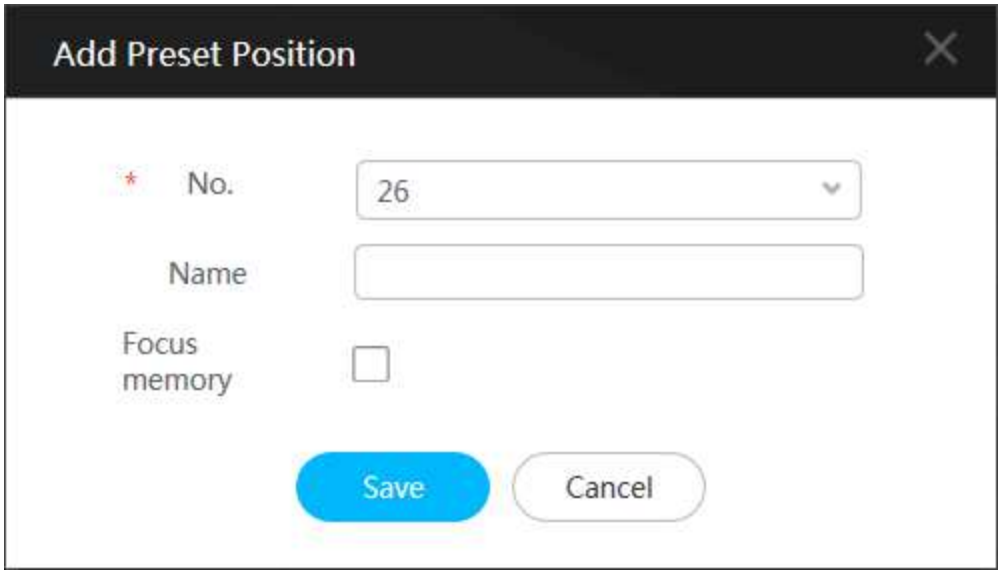
   After this function is enabled, the system will directly display the image of the target preset position without displaying images generated during the rotation.

4. Rotate the PTZ device to steer the camera view to the preset position to be added.

5. Click **Add**.

   The **Add Preset Position** dialog box is displayed, as shown in Figure 2.

   Figure 2 Add Preset Position dialog box



6. Select a preset position number and name the preset position.

   A preset position name can contain a maximum of 31 characters, including letters, digits, and other characters available on the keyboard.

7. Click **Save**.

The added preset position is displayed in the preset position list.

NOTE

- After the compatibility mode is enabled, 300 preset positions are allocated by default (including the existing ones). You can update their information. The preset positions can be deleted after this mode is disabled.
- To modify or delete a preset position, select it and click or .
- To delete all preset positions, click **Delete All**.
- You cannot delete an enabled home position or a preset position in a tour.
- You can manually adjust the speed for steering the camera view from the current preset position to other preset positions.

Configuring a Home Position

1. On the **Preset Position** page, rotate the PTZ device to steer the camera view to the desired position.

2. Click on the right of the home position. The **Modify Preset Position** dialog box is displayed, as shown in Figure 3. Click **Save**. The customized home position is configured. The actual web page varies depending on the camera model.

Figure 3 Modify Preset Position dialog box



3. On the **Preset Position** page, check the configuration result. If the configuration is successful, the home position name contains the preset position information, for example, **Home position (Preset Position1)**, as shown in Figure 4.

   Figure 4 Checking the home position configuration result



Parent topic: Configuring PTZ Control

Configuring Tours

You can configure a tour that consists of multiple preset positions. After you enable the tour, the camera shoots video along the tour. You can set a maximum of 16 tours. Each tour can consist of a maximum of 512 preset positions.

The actual web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Tour**. The **Tour** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set tour parameters for the channels separately.

   Figure 1 Tour page

3. Click **Add**.

   The **Add Tour** dialog box is displayed, as shown in Figure 2. Table 1 describes the parameters.

Figure 2 Add Tour dialog box

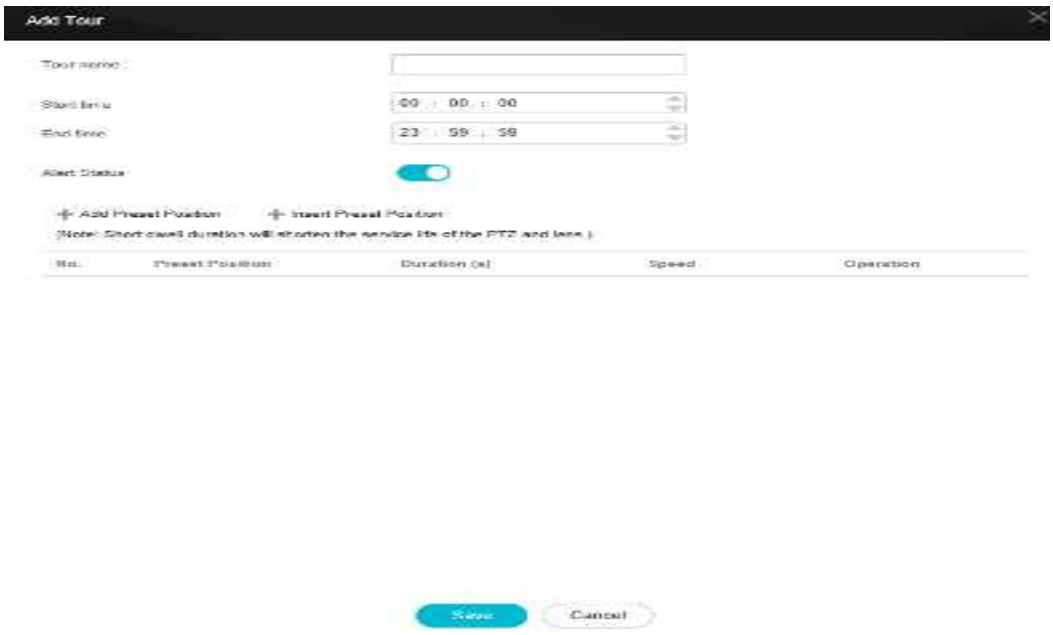


Table 1 Tour parameters

Parameter	Description
Tour name	A tour name can contain a maximum of 31 characters, including letters, digits, and other characters available on the keyboard.
Start time/End time	Tour duration. After the start time and end time are specified, the camera performs tour in the specified period. **NOTE:** • The start time and end time of each tour must be unique. • The value of **Start time** must be different from that of **End time**.
Alert Status	After **Alert Status** is toggled on, the camera automatically performs tour in the specified period.

Parameter	Description
	NOTE: If the tour is manually interrupted, the camera will automatically resume the tour if no operation is performed within 60s.
Add Preset Position	Select specified preset positions from the **Preset Position** drop-down list box and set **Duration(s)** and **Speed**. The recommended value of **Duration (s)** is at least 120s. **NOTE:** • A maximum of 512 preset positions can be added. • To change preset positions in a running tour, first stop the tour. • You can click or to adjust positions of preset positions in a tour and click to delete a preset position.
Insert Preset Position	You can select a preset position and click **Insert Preset Position** to insert a preset position above the selected preset position.

4. Click **Save**.

   The tour is successfully added.

NOTE

- To execute a tour, toggle on **Alert Status** corresponding to the tour.
- You can check the status of each tour in the **Execution Status** column.

- You can enable a tour at a time. If a tour has been enabled and you enable another tour, the tour that has been enabled will automatically stop.
- The **Operation** column contains operations that can be performed on a tour, including **Edit**, **Delete**, **Execute**, and **Cancel Execution**.
- If a scheduled tour (whose duration is not from 00:00:00 to 00:00:00) is running and you want to manually execute a tour, you need to first toggle off **Alert Status**.
- Manual tour and scheduled tour are independent of each other. To execute a scheduled tour during manual tour execution, you need to first click **Cancel Execution** in the **Operation** column to stop the manual tour.

Parent topic: Configuring PTZ Control

Configuring Pattern Scan

You can set pattern scan parameters to customize a scan path.

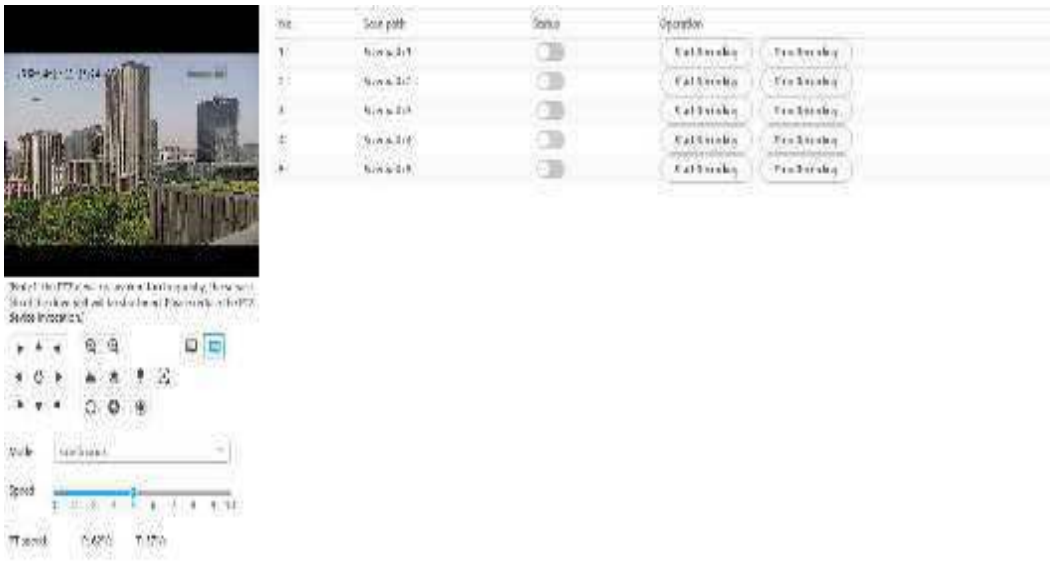
The actual web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Pattern Scan**. The **Pattern Scan** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set pattern scan parameters for the channels separately.

   Figure 1 Pattern Scan page

3. Select a path in the **Scan path** column.
4. Click **Start Recording**.
5. Control the PTZ device to enable the camera to rotate along a desired path.
6. Click **Stop Recording**. The path along which the camera rotates is recorded.

NOTE

- The name of the scan path cannot be changed.
- Each scan path can record at most 1000 steps or for a maximum of 10 minutes. When the threshold is reached, the pattern scan stops.

7. Enable the toggle button in the **Status** column to enable the patten scan.

Parent topic: Configuring PTZ Control

Configuring Scan Limits

You can set left and right scan limits to limit the camera's scan area.

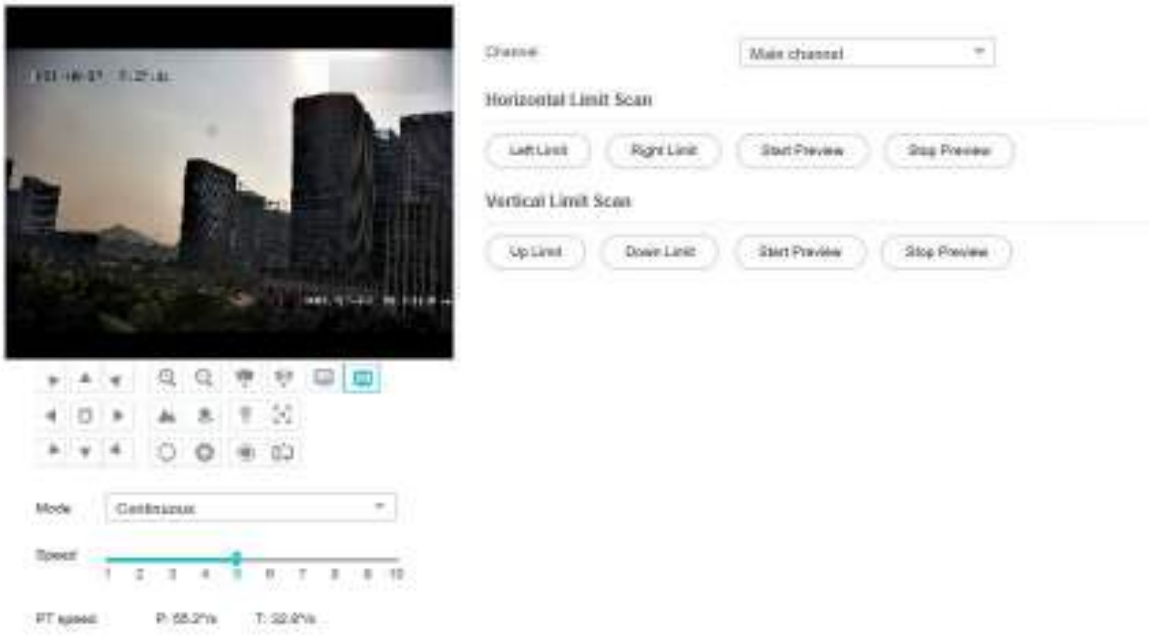
The actual web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Scan Limit**. The **Scan Limit** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set scan limit parameters for the channels separately.

   Figure 1 Limit Scan page

3. Control the PTZ device to rotate the camera to the desired position.

   a. In the **Horizontal Limit Scan** area, click **Left Limit** or **Right Limit** to set the horizontal scan limit, **Preview** to view the image effect, and **Stop Live Video Viewing** to stop live video viewing.

   b. In the **Vertical Limit Scan** area, click **Up Limit** or **Down Limit** to set the vertical limits, **Preview** to view the image effect, and **Stop Live Video Viewing** to stop live video viewing.

Parent topic: Configuring PTZ Control

Configuring PTZ Control

This section describes how to set PTZ control parameters, including **Vertical rotation restriction(°)**, **Max pan speed (°/s)**, and **Max tilt speed (°/s)**.

NOTICE

- PTZ control parameters are available only for PTZ dome cameras.
- The actual web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **PTZ Control**. The **PTZ Control** page is displayed, as shown in Figure 1.

   Figure 1 Setting PTZ control parameters

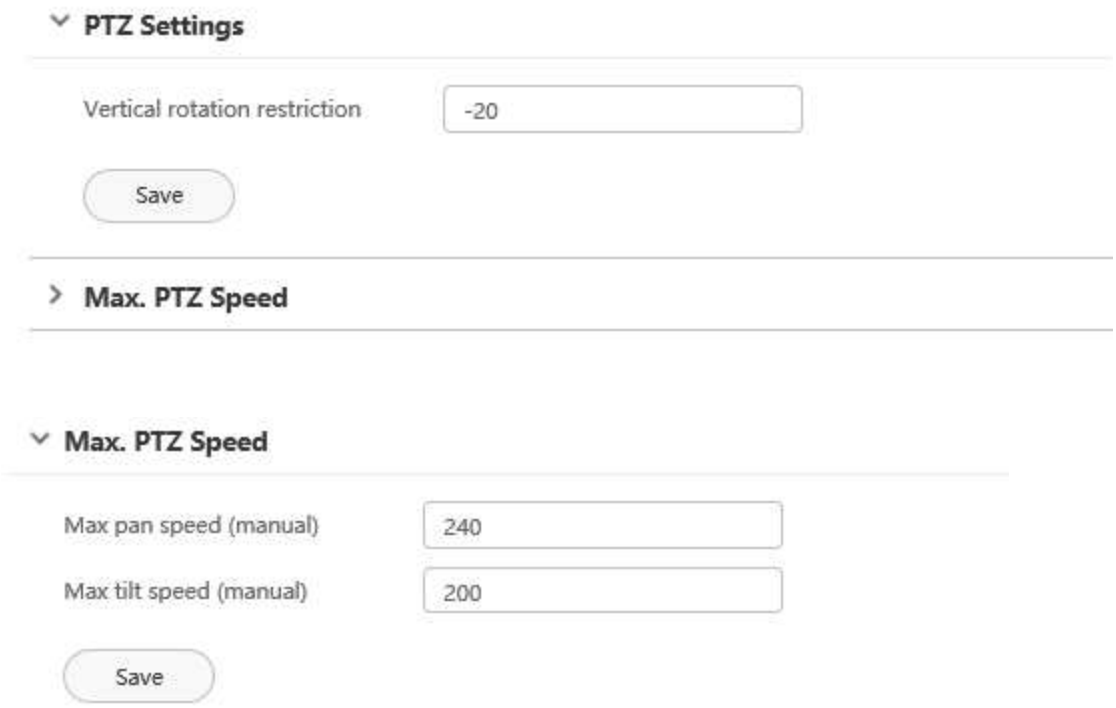


Table 1 PTZ control parameters

Parameter	Description
Vertical rotation restriction(°)	Tilt angle limit. For example, the value **0** indicates that the camera can only tilt downward by up to 90°, and the value **-10** indicates that the camera can tilt upward by up to 10° and tilt downward by up to 90°.
Max pan speed (°/s)	Maximum pan speed of the PTZ device in the case of 1x zoom ratio and level-10 PTZ rotation speed.
Max tilt speed (°/s)	Maximum tilt speed of the PTZ device in the case of 1x zoom ratio and level-10 PTZ rotation speed.

Parent topic: Configuring PTZ Control

Configuring Location Information

You can set the OSDI zone by setting the coordinates.

NOTICE

- The actual web page varies depending on the camera model.
- After an OSDI zone is set, it is enabled by default. To show its name on video images, add the OSDI element by referring to Configuring OSD.
- If the left point of the OSDI element is located in the specified OSDI zone, the OSDI name will be displayed on the live video image.

Setting OSDI Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Location**. The **Location** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set OSDI parameters for the channels separately.

   Figure 1 Location page

3. Select **Enable** to enable the OSDI function.
4. Click **Add**.

   The dialog box for adding an OSDI zone is displayed, as shown in Figure 2.

Figure 2 Add OSDI dialog box



5. Set OSDI parameters.

    a. Set **Lower left coordinate** and **Upper right coordinate**.

    - Method 1: Manually enter the coordinates.

      Directly enter values in the text boxes.

    - Method 2: Manually adjust the camera's image view to automatically obtain the coordinates of the current image view.

        i. Control the PTZ device to navigate the camera to where you would like the OSDI zone to be located on the image view.

        ii. Click **GET** next to **Lower left coordinate** or **Upper right coordinate** to set **Lower left coordinate** or **Upper right coordinate** to the coordinates of the central point of the current image.

    NOTE

    - The coordinates must comply with the following rules:
        - The difference between X1 and X2 cannot exceed 180°.
        - Y1 must be greater than Y2 when vertical mirroring or all mirroring is disabled.

- Y1 must be less than Y2 when vertical mirroring or all mirroring is enabled.

- Horizontal coordinate:
  - The horizontal coordinate range depends on the actual device. Before delivery, the camera has a default horizontal zero coordinate (that is, the camera has a default lens angle 0°.). You can click  to set the current position to the horizontal zero coordinate.
  - Horizontal coordinate refers to the angle in which the camera lens pans clockwise relative to the horizontal zero coordinate. For example, if the horizontal coordinate is set to 20, the camera lens pans clockwise 20° in the horizontal direction relative to the horizontal zero coordinate.

- Vertical coordinate:
  - The vertical coordinate range depends on the actual device.
  - Vertical coordinate refers to the angle in which the camera lens tilts relative to the vertical zero coordinate. For example, if the vertical coordinate is set to 20, the camera lens tilts 20° relative to the vertical zero coordinate.

b. In the PTZ control area, set the aperture, focus, and zoom parameters of the camera.

c. Specify the OSDI zone name. The OSDI zone name consists of up to 32 characters. A maximum of eight OSDI zones can be set.

6. Click **Save**.

   The OSDI zone is successfully set.

7. **(Optional)** To modify or delete an existing OSDI zone, select the OSDI zone and click **Modify** or **Delete**.

8. **(Optional)** Select an OSDI zone and enable or disable the toggle button in the **Status** column.

NOTE

- If multiple OSDI zones overlap and the coordinates of the live video are in the overlapping area, the OSDI zone name with the smallest ID is displayed first.
- If the OSDI zone name is incompletely displayed on the preview page due to a too long name or low resolution, you are advised to reduce the font size of OSDI names.

Parent topic: Configuring PTZ Control

Configuring Park Actions

You can set a park action for the camera. If you do not control the PTZ device within a specified period, the PTZ device automatically performs the specified park action.

The actual web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Parking Action**. The **Parking Action** page is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set park action parameters for the channels separately.

   Figure 1 Parking Action page



3. Set park action parameters. Table 1 describes the parameters.

   Table 1 Park action parameters

Parameter	Description
Enable	Indicates whether to enable the park action function.
Waiting time (s)	Duration from the time when you stop operating the PTZ device to the time when the PTZ device automatically performs the park action. The unit is second.

Parameter	Description
Action	Mode in which the PTZ device rotates. The options are as follows: • **Horizontal scan**: The PTZ device continuously rotates towards the same horizontal direction. You can set the rotation speed and direction. • **Preset position**: The PTZ device rotates to a specified preset position. • **Tour scan**: The PTZ device rotates along a predefined tour. • **Vertical scan**: The PTZ device continuously tilts back and forth (maximum tilt angle: 90°). You can set the tilt speed. • **Pattern scan**: The PTZ device rotates along a predefined path. • **Panorama scan**: The PTZ device continuously pans and tilts back and forth. You can set the rotation (pan/tilt) speed and pan angle. • **Frame scan**: The PTZ device pans for a certain angle (automatically adjusted based on the zoom ratio) at a specified interval. You can set the dwell duration at each position. • **Random scan**: The camera will randomly generate a coordinate at a specified interval and rotate to the position of the coordinate. You can set the dwell duration at each position.
Scan speed	Scan speed. This parameter is available only when **Action** is set to **Horizontal scan** or **Vertical scan**.
Horizontal reverse	Indicates whether to enable the PTZ device to horizontally rotate in a reverse direction. This parameter is available only when **Action** is set to **Horizontal scan** or **Panorama scan**.
Select preset position	Preset position to which the camera rotates as a park action. This parameter is available only when **Action** is set to **Preset position**.

Parameter	Description
Select tour	Tour along which the camera rotates as a park action. This parameter is available only when **Action** is set to **Tour scan**.
Select path	Scan path along which the camera rotates as a park action. This parameter is available only when **Action** is set to **Pattern scan**.
Scan interval	Scan interval, in seconds. This parameter is available only when **Action** is set to **Frame scan** or **Random scan**.

4. Click **Save**.

Parent topic: Configuring PTZ Control

Configuring the Serial Port

You can set parameters, for example, serial port parameters and transparent channel parameters, for connecting the PTZ device to a camera through the serial port.

The web page varies between camera models.

Setting Serial Port Parameters You can set serial port parameters for the camera to implement communication with external devices.

Configuring Transparent Channels and PTZ Channels The transparent channel is a data transmission channel provided by the SDK protocol. After the transparent channel is configured, users can use the SDK protocol and external serial port to transmit data.

Parent topic: Configuring PTZ Control

Setting Serial Port Parameters

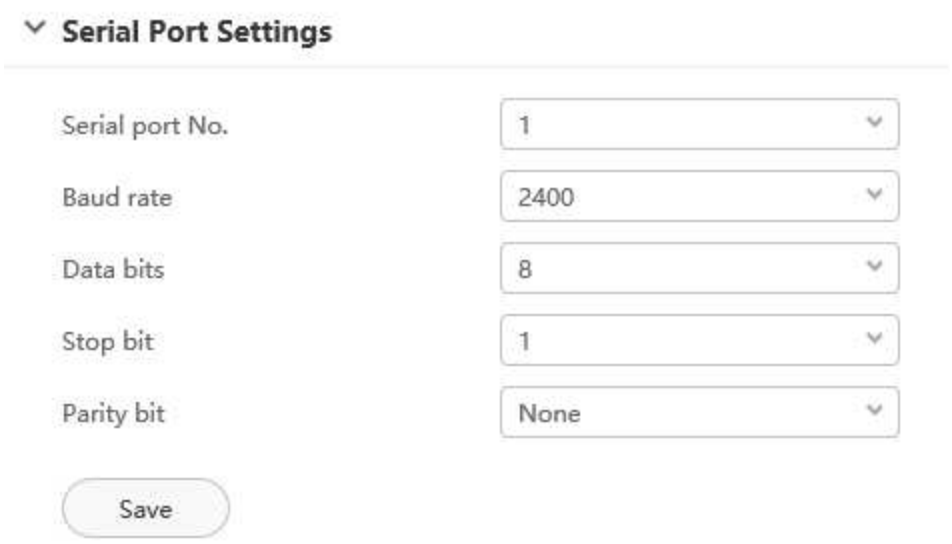
You can set serial port parameters for the camera to implement communication with external devices.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Serial Port** > **Serial Port Settings**. The **Serial Port Settings** area is displayed, as shown in Figure 1.

   For some camera models with multiple channels, you need to set serial port parameters for the channels separately.

   Figure 1 Serial Port Settings area



3. Set serial port parameters. Table 1 describes the parameters.

   Table 1 Serial port parameters

Parameter	Description
Serial port No.	ID of the serial port, which must be unique.

Parameter	Description
Baud rate	Rate at which information is transferred in a communication channel, which must be the same as that of the connected external device.
Data bits	Number of bits used for data communication.
Stop bit	Number of bits used for marking the end of the serial port data.
Parity bit	Method to check the serial port data.

4. Click **Save**.

Parent topic: Configuring the Serial Port

Configuring Transparent Channels and PTZ Channels

The transparent channel is a data transmission channel provided by the SDK protocol. After the transparent channel is configured, users can use the SDK protocol and external serial port to transmit data.

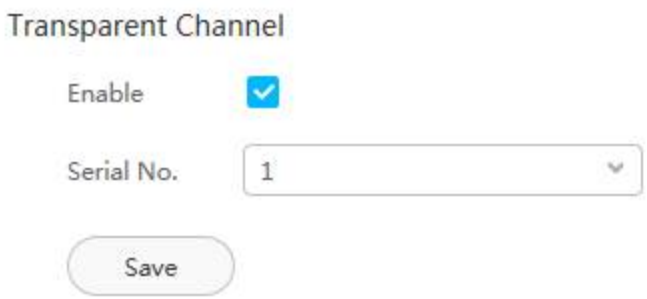
NOTICE

- When the camera is connected to an external PTZ device, you need to set PTZ channel parameters.
- For some camera models with multiple channels, you need to set the parameters for the channels separately.
- The actual web page varies depending on the camera model.

Setting Transparent Channel Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Serial Port** > **Transparent Channel**.
3. To use the SDK protocol and the external serial port for data transmission, select **Enable**, set **Serial No.**, and click **Save**, as shown in Figure 1.

   Figure 1 Setting transparent channel parameters



Setting PTZ Channel Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **PTZ** > **Serial Port** > **Transparent Channel**.
3. Set PTZ channel parameters, as shown in Figure 2. Table 1 describes the parameters.

   Before connecting an external PTZ device to the camera, ensure that the external PTZ device has been configured.

   Ensure that the settings of PTZ channel parameters are the same as those of the external PTZ device. Otherwise, the external PTZ device may not function properly.

   Figure 2 Setting PTZ channel parameters

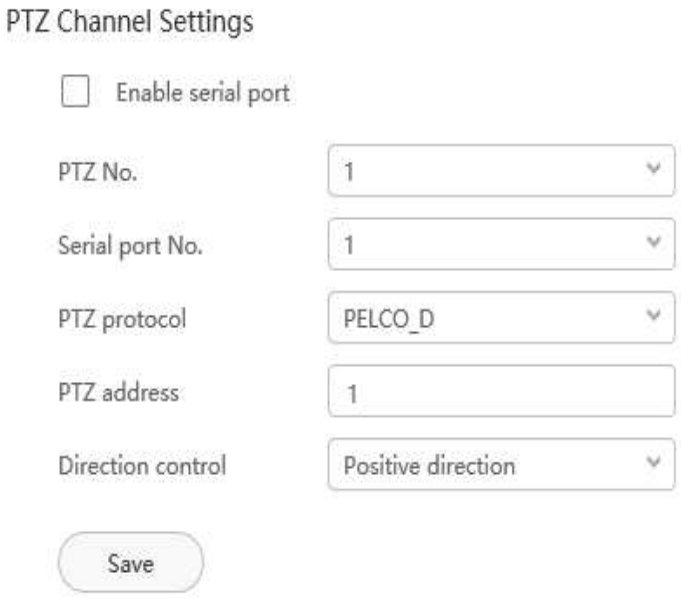


Table 1 PTZ channel parameters

Parameter	Description
Enable serial port	Indicates whether to enable the serial port.
PTZ No.	ID of the PTZ device, which must be unique.
Serial port No.	ID of the PTZ device's serial port.

Parameter	Description
PTZ protocol	Protocol used by the PTZ device.
PTZ address	Address of the PTZ device.
Direction control	Direction (forward or backward) control of the PTZ device. • **Positive direction**: enables the forward control of the PTZ device. For example, if you click the left button, the PTZ device rotates leftward. • **Negative direction**: enables backward control of the PTZ device. For example, if you click the left button, the PTZ device rotates rightward.

Parent topic: Configuring the Serial Port

Intelligent Settings

This section describes how to configure intelligent analysis functions such as intelligent behavior analysis, motion detection, lens blocking detection, and sound detection.

NOTICE

- The intelligent analysis does not support pan, tilt, or zoom operations.
- The intelligent analysis supports detection only in full image mode. If area cropping is enabled, the detection result is still superimposed on the full image.
- In the Windows 10 operating system, if the live video resolution exceeds 5 megapixels (3072 x 1728), detection lines for intelligent analysis may fail to be displayed on the live video image. To rectify the fault, perform the following operations: Log in to the camera web system, choose **Configuration** > **Local** > **Playing Settings** and set **Rendering mode** to **D3D**. Alternatively, choose **Configuration** > **Video/Audio** > **Video** and decrease the resolution of the primary stream.
- Functions available on the web page vary between camera models.

Configuring Intelligent Target Analysis This section describes how to configure intelligent target analysis and check the configuration result.

Configuring Behavior Analysis
This section describes the application scenario, configuration prerequisites, and configuration process and procedure of intelligent behavior analysis.

Configuring Intelligent Vehicle Analysis
This section describes how to configure intelligent vehicle analysis and check the configuration result.

Configuring 1 + N
This chapter describes the background, primary/secondary camera requirements, and configuration procedure for 1 + N.

Parent topic: Configuration

Configuring Intelligent Target Analysis

This section describes how to configure intelligent target analysis and check the configuration result.

Intelligent Target Analysis Features

Configuring Target Capture

Configuring Access Control

Configuring Mask Detection
The mask detection function checks whether a target wears a mask in a detection area. The system generates an alarm when a target meeting the alarm condition is detected.

Configuring Target Counting

Configuring Target and Personal Attribute Recognition

Viewing Intelligent Detection Results
You can check the detection results of specified attributes.

Parent topic: Intelligent Settings

Intelligent Target Analysis Features

Different camera models support different intelligent target analysis features. The following table describes the differences.

Table 1 Intelligent target analysis features

Device Model	Target Detection	Target Attribute Recognition	Person Detection	Personal Attribute Recognition	Text Overlay	Target Counting[a]
HWT-D6550-10-Z33-SV	YES	YES	YES	NO	YES	YES
HWT-D3040-10-ELI-PV (2.8 mm)	NO	NO	NO	NO	YES	NO
HWT-D2122-10-SIU	YES	YES	YES	NO	YES	YES
HWT-D2152-10-SIU	YES	YES	YES	NO	YES	YES
HWT-D3222-10-SIU	YES	YES	YES	NO	YES	YES
HWT-D3252-10-SIU	YES	YES	YES	NO	YES	YES

a: This function cannot be put into commercial use currently. The specifications vary greatly in different scenarios.

Parent topic: Configuring Intelligent Target Analysis

Configuring Target Capture

With the target capture function, the system can capture targets in a specified detection area, display their locations in real time until they disappear from the detection area, and send captured target images to the video security platform through SDK or FTP/SFTP, or as metadata, or send emails containing the images through SMTP.

Setting Target Capture Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Target Capture** in the **Target Intelligence** area, as shown in Figure 1.

   Figure 1 Enabling target capture

3. Click **Settings** next to **Target Capture**. The **Target Capture** page is displayed.
4. Click the **Basic Settings** tab.

   a. Click **Common Parameters** and set related parameters, as shown in Figure 2. Table 1 describes the parameters.

   Figure 2 Setting common parameters

   Table 1 Parameter description

Parameter	Description
Enable	Indicates whether to enable target capture. This check box is selected by default and cannot be deselected.

Parameter	Description
Static object capture	Indicates whether to generate trajectories and takes snapshots of static objects or objects with small motion in the image. This parameter is applicable to scenarios where targets or persons are partially occluded. For example, when a vehicle enters the image view and the window is being rolled down, the target inside the vehicle is partially occluded.
Capture mode	Image capture mode. The options are as follows: • **Optimal**: When a target is in the view, the camera takes snapshots of the target and evaluates each snapshot. After the target leaves the area, the snapshot with the optimal quality is used as the capture result. This mode applies to most capture scenarios and ensures optimal quality of snapshots. • **Ultra-fast**: When a target is in the view, the camera takes snapshots of the target and evaluates each snapshot. Once a snapshot of the target meets the requirement specified by **Capture sensitivity**, the snapshot is selected as the capture result. Then the camera still detects the target but does not take snapshots of the target subsequently. • **Scheduled**: When a target is in the view, the camera takes snapshots of the target and generates the optimal snapshot at a specified interval (determined by **Scheduled snapshot interval (s)**). This mode applies to scenarios where targets need to be detected for multiple times, such as access control and attendance check.
Preferred snapshot interval (s)	This parameter is available only when **Capture mode** is set to **Optimal** and **Detection mode** is set to **Target detection** or **Person detection**. Interval at which the optimal captured image is generated. The value ranges from 0 to 120, in seconds.
Scheduled snapshot interval (s)	This parameter is available only when **Capture mode** is set to **Scheduled**. Interval at which the optimal captured target image is generated. The value ranges from 1 to 300, in seconds.

Parameter	Description
	NOTE: If you set **Scheduled snapshot interval (s)**, the system generates the optimal snapshot at the specified interval. However, the interval for storing snapshots to the local computer may be different from the predefined snapshot interval. The actual interval for locally storing snapshots is used.
Duplicate target capture times	This parameter is available only when **Capture mode** is set to **Scheduled**. Number of times that the camera captures images of the same target at the interval specified by **Scheduled snapshot interval (s)**.
Capture sensitivity	This parameter is available only when **Capture mode** is set to **Ultra-fast**. A larger value indicates a higher sensitivity, faster capture, but lower captured target image quality. The value is an integer ranging from 1 to 10. The default value is **6**.
Target detection sensitivity	A larger value indicates a higher sensitivity, a lower false negative rate, but a higher false positive rate. The value is an integer ranging from 1 to 5. The default value is **3**.
Person detection sensitivity	A larger value indicates a higher sensitivity, a lower false negative rate, but a higher false positive rate. The value is an integer ranging from 1 to 5. The default value is **3**.
Detection mode	Three options are available: **Target detection**, **Person detection** (supported only when **Capture mode** is set to **Optimal** or **Scheduled**), and **Both**. • **Target detection**: detects only targets. • **Person detection**: detects only persons. • **Both**: detects both targets and persons.
Min. target resolution	Minimum width of a target that can be detected by a camera. Targets whose width is less than the value of this parameter cannot be detected. The default value is 26 pixels, which is obtained based on 1080p resolution. You need to set this parameter based on the actual video resolution. Actual target width = Value of **Min.**

Parameter	Description
	target resolution (for example, 26 pixels) x Actual video resolution (width)/1920 You can click **Show on Image** to view the minimum target width in the image.
Max. target resolution	Maximum width of a target that can be detected by a camera. Targets whose width is greater than the value of this parameter cannot be detected. The default value is 300 pixels, which is obtained based on 1080p resolution. You need to set this parameter based on the actual video resolution. Actual target width = Value of **Max. target resolution** (for example, 300 pixels) x Actual video resolution (width)/1920 You can click **Show on Image** to view the maximum target width in the image.

b. Click **Advanced Parameters** and set related parameters, as shown in the following figure. Table 2 describes the parameters.

   The web page varies depending on the camera model.

Figure 3 Setting advanced parameters



Table 2 Parameter description

Parameter	Description
Target image enhancement	Indicates whether to enable the target image enhancement function. After this function is enabled, the target image enhancement algorithm is used to reduce image noise and enhance image details, which helps improve target brightness and contrast. **NOTE:** • You are advised to enable this function only when the brightness and contrast are insufficient in a scene. In other scenarios, it will result in overexposed images. • Some camera models do not support this function.

Parameter	Description
Send target cutout	If this check box is selected, the camera sends only the target images but not the whole live video images to the video security platform. The number of snapshots taken for a single target can be set. The value ranges from 1 to 3. **NOTE:** Some cameras can capture only one image for a single target.
Send person cutout	If this check box is selected, the camera sends only the person images but not the whole live video images to the video security platform. The number of snapshots taken for a single person can be set. The value ranges from 1 to 3. **NOTE:** Some cameras can capture only one image for a single person.
Target snapshot quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Person snapshot quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Send full image	If this check box is selected, the camera sends the whole live video images to the video security platform.
Full image quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Target and person cutout from same full image	If this check box is selected, the camera sends only the whole live video images but not target images or person images to the video security platform

Parameter	Description
Full image resolution	Resolution of full images. Set this parameter based on the site requirements.
Brightness compensation	If this function is enabled, the exposure is automatically decreased in highlight or increased in backlight to ensure ideal brightness in different environments.
Compensation level	This parameter is available only when brightness compensation is enabled. Maximum target brightness compensation coefficient. The default value is **50**. The camera will automatically adjust the compensation level within the specified range based on the image brightness. The value of this parameter can be properly increased in frontlight or backlight conditions.
Target exposure duration (min)	This parameter is available only when brightness compensation is enabled. When a target is detected, target exposure is performed for a specified period of time. Set the exposure duration based on the site requirements. You are advised to set this parameter to 10 minutes in densely populated scenarios and 5 minutes in sparsely populated scenarios.
Capture targets wearing helmets	If this check box is selected, the camera takes snapshots of targets wearing helmets, reducing the false negative rate.
Capture targets wearing masks	If this check box is selected, the camera takes snapshots of targets wearing masks.
Filter out low-quality targets	If this check box is selected, the camera filters out some unclear targets or targets whose yaw or pitch angle exceeds 50° during capture.
Filter out targets by angle	If this check box is selected, **Yaw angle** and **Pitch angle** must be set. Then the camera captures targets only in the specified yaw and pitch angles.

Parameter	Description
Yaw angle	This parameter is available only when **Filter out targets by angle** is selected. Maximum yaw angle of targets to be captured. The value ranges from 0° to 90°. Set this parameter based on the site requirements. Then the camera takes snapshots only of the targets whose yaw angle does not exceed the specified value.
Pitch angle	This parameter is available only when **Filter out targets by angle** is selected. Maximum pitch angle of targets to be captured. The value ranges from 0° to 70°. Set this parameter based on the site requirements. Then the camera takes snapshots only of the targets whose pitch angle does not exceed the specified value.
Filter out duplicate targets	If this check box is selected, **Target match** and **Duration** must be set. The camera does not repeatedly capture the targets whose similarity exceeds the specified threshold in the specified duration.
Target match	This parameter is available only when **Filter out duplicate targets** is selected. Target similarity threshold, in percentage. The value ranges from 1 to 100. Set this parameter based on the site requirements. Then the camera does not repeatedly capture the targets whose similarity exceeds the threshold specified here.
Duration	This parameter is available only when **Filter out duplicate targets** is selected. Duration for filtering out duplicate targets, in seconds. The value ranges from 1 to 60. Set this parameter based on the site requirements. Then the camera does not repeatedly capture the targets whose similarity exceeds the specified threshold in the duration specified here.

c. Click **Rule Area**. Draw a detection area and an exclude area. If no area is drawn, the entire area is under detection by default. Set related parameters, as shown in Figure 4. Table 3 describes the parameters.

Figure 4 Drawing a rule area



Table 3 Parameter description

Parameter	Description
Detection Area	After a detection area is set, the system detects targets only in the area. Click **Polygonal Area**, **Rectangular Area**, or **Full Screen**, and move the pointer to the live video image. When a cross is displayed, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location. This operation does not apply to **Full Screen**. • Only one target detection area can be stored. To add another one, delete the original one.
Exclude Area	After an exclude area is set, the system does not detect targets in the area. Click **Polygonal Area**, **Rectangular Area**, or **Full Screen**, and move the pointer to the live video image. When a cross is displayed, you can draw an exclude area. **NOTE:** • An exclude area can be a polygon such as a triangle or rectangle. An exclude area supports a maximum of 10 vertexes.

Parameter	Description
	• To redraw an exclude area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the exclude area to change its location. This operation does not apply to **Full Screen**. • Only one exclude area can be stored. To add another one, delete the original one.

NOTE

- If the target capture effect is not ideal in backlit locations such as lobby entryways, you are advised to adjust cameras as follows:

  Choose **Configuration** > **Image** > **Display** > **Backlight**. Set **Backlight/WDR/HLC** to **Backlight adaptation**.

- During the setting of **Send target cutout**, **Send person cutout**, and **Send full image**, the target or full-body image and full image of the target person sent to the video security platform may be inconsistent. That is, the target or full-body image and full image of the same person show the person in different angles. This is a normal phenomenon. After the configuration is complete, this phenomenon does not occur again after the person leaves the view.

  During the setting of these parameters, this phenomenon may occur only when a target appears in the view.

5. Click **Save**.

Configuring Target Images

You can configure the size of a target image based on the site requirements.

1. Click **Advanced Settings**. The **Target Image Settings** area is displayed, as shown in Figure 5.

Figure 5 Configuring target images



2. Click **Custom**, **Head**, or **Head + shoulder**. You can set related parameters only when you click **Custom**. Table 4 describes the parameters.

   Table 4 Target image parameters

Parameter	Description
Width	Width of the image captured by the camera. The value is 1–5 times the target width in the image. The value can contain a maximum of one decimal place.
Target height	Height of a target in the image captured by the camera. The value is 1–3 times the target height in the image. The value can contain a maximum of one decimal place.
Person height	Height of the body in the image captured by the camera. The value is 0–5 times the target height in the image. The value can contain a maximum of one decimal place.

3. Click **Save**.

Configuring Text Overlay

Text overlay allows you to superimpose information such as the snapshot time, device ID, and site information on captured full images.

1. Click the **Text Overlay** tab. The **Text Overlay** tab page is displayed, as shown in Figure 6. Table 5 describes the parameters.

Figure 6 Text Overlay tab page

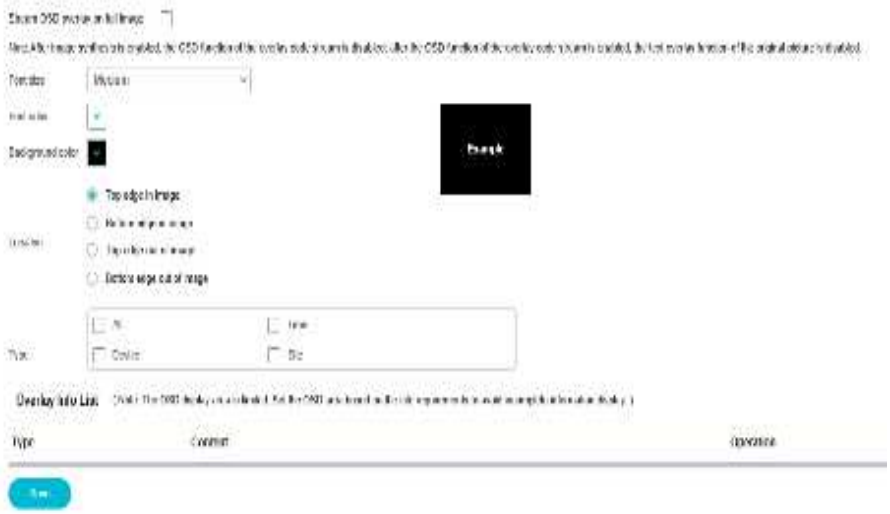


Table 5 Text overlay parameters

Parameter	Description
Stream OSD overlay on full image	• If you deselect this check box, information set under **Text Overlay** > **Overlay Info List** will be superimposed on full images uploaded through target detection. • If you select this check box, only information set under **Configuration** > **Image** > **OSD** will be superimposed on full images uploaded through target detection.
Font size	Set the parameters based on the site requirements.
Font color	
Background color	
Location	
Type	Set the parameter based on the site requirements.
Time	Image capture time. If you select **Accurate to milliseconds**, the image capture time is accurate to milliseconds.
Device	Device ID. You can click to adjust the display sequence of device IDs.
Site	Detection site name. You can click to adjust the display sequence of detection site names.

2. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 7.

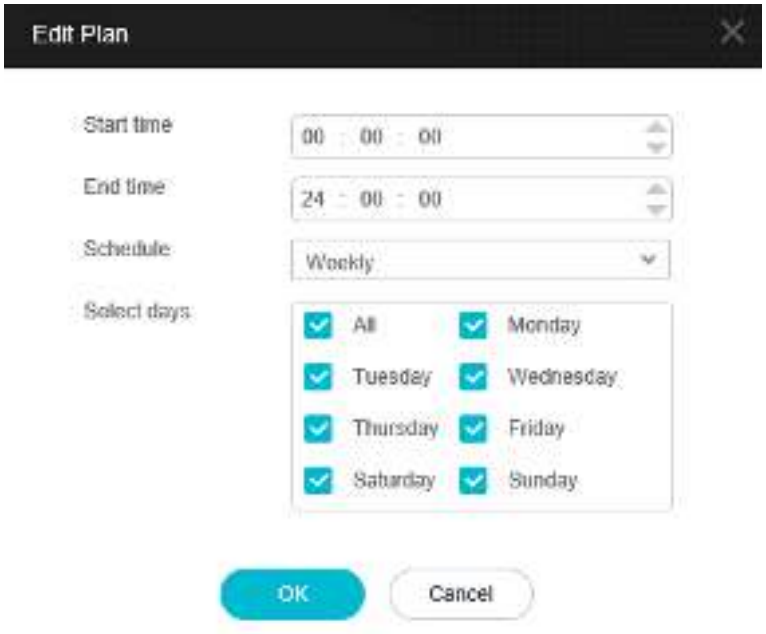
   Figure 7 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 8.

   Figure 8 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

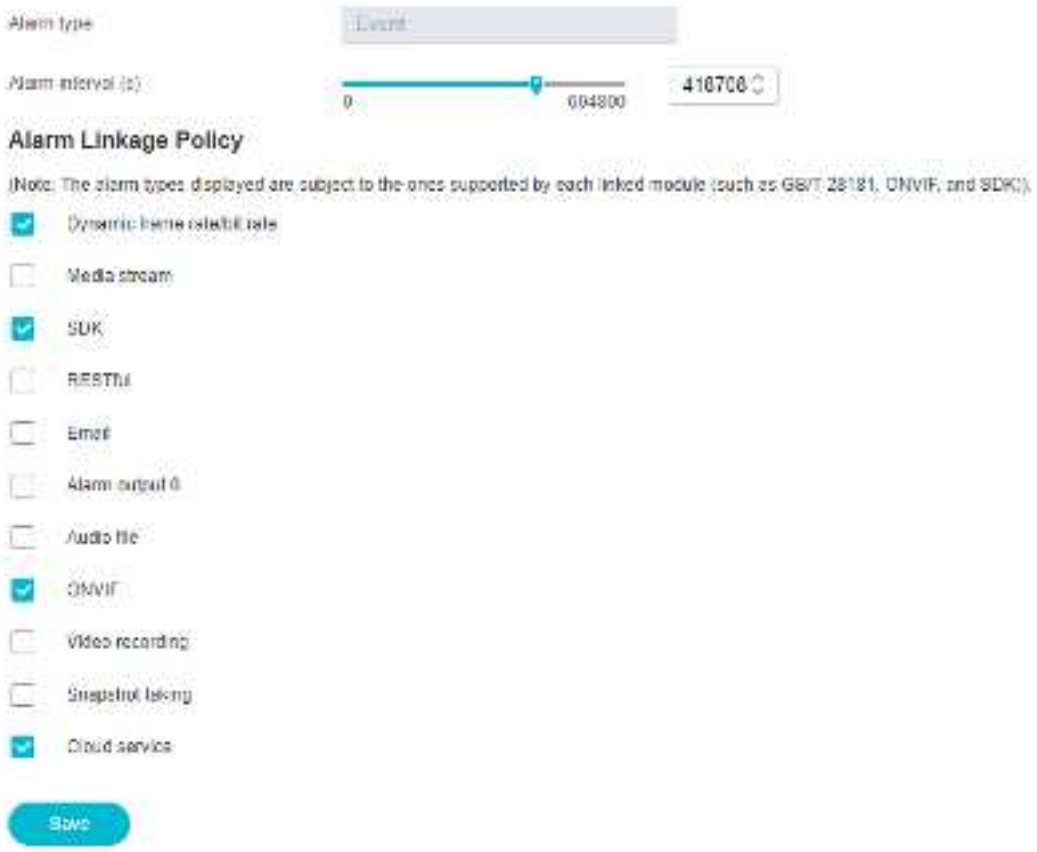
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 9.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 9 Configuring alarms



2. Set related parameters. Table 6 describes the parameters.

Table 6 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning.

Parameter	Description
	The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service

Parameter	Description
	sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Parent topic: Configuring Intelligent Target Analysis

Configuring Access Control

The system takes snapshots of an object that enters the access control area and generates the optimal image at a specified interval until the object disappears from the access control area. Additionally, the system uploads snapshots to the video security platform through SDK or FTP/SFTP, or as metadata, or send emails containing the snapshots through SMTP.

NOTE

- Only some camera models support access control.
- Target capture and access control cannot be enabled at the same time. To enable access control, ensure that target capture is disabled.

Configuring Image Capture

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Access Control** under **Target Intelligence**, as shown in Figure 1.



Figure 1 Toggling on access control

3. Click **Settings** next to **Access Control**.
4. Click the **Basic Settings** tab.
    a. Set parameters under **Common Parameters**, as shown in Figure 2. Table 1 describes the parameters.

Figure 2 Setting common parameters



Table 1 Parameter description

Parameter	Description
Enable	This check box is selected by default and cannot be deselected.
Static object capture	After this parameter is selected, the system detects and takes snapshots of static objects or objects with small motion in the image. This parameter is applicable to scenarios where targets or persons are partially occluded. For example, when a vehicle enters the image view and the window is being rolled down, the target inside the vehicle is partially occluded.
Capture mode	Image capture mode. The value of this parameter is fixed at **Scheduled** and cannot be changed. **Scheduled**: When a target is in the view, the camera takes snapshots of the target and generates the optimal snapshot at a specified interval (determined by **Scheduled snapshot interval (s)**). This mode applies to scenarios where targets need to be detected for multiple times, such as access control and attendance check.
Scheduled snapshot interval (s)	Interval at which the optimal captured target image is generated. This parameter is available only when **Capture mode** is set to **Scheduled**. **NOTE:**

Parameter	Description
	If you set **Scheduled snapshot interval (s)**, the system generates the optimal snapshot at the specified interval. However, the interval for storing snapshots to the local computer may be different from the predefined snapshot interval. The actual interval for locally storing snapshots is used.
Duplicate target capture times	Number of times that the camera captures images of the same target at the interval specified by **Scheduled snapshot interval (s)**.
Target detection sensitivity	A larger value indicates a higher sensitivity, a lower false negative rate, but a higher false positive rate. The value is an integer ranging from 1 to 5. The default value is **3**.
Person detection sensitivity	A larger value indicates a higher sensitivity, a lower false negative rate, but a higher false positive rate. The value is an integer ranging from 1 to 5. The default value is **3**.
Detection mode	Three options are available: **Target detection**, **Person detection**, and **Both**. • **Target detection**: detects only targets. • **Person detection**: detects only persons. • **Both**: detects both targets and persons.
Min. target resolution	Minimum width of a target that can be detected by a camera. Targets whose width is less than the value of this parameter cannot be detected. The default value is 26 pixels, which is obtained based on 1080p resolution. You need to set this parameter based on the actual video resolution. Actual target width = Value of **Min. target resolution** (for example, 26 pixels) x Actual video resolution (width)/1920 You can click **Show on Image** to view the minimum target width in the image.
Max. target resolution	Maximum width of a target that can be detected by a camera. Targets whose width is greater than the value of this parameter cannot be detected. The default value is 300 pixels, which is obtained based on 1080p resolution. You need to set this parameter based on the actual video resolution. Actual target width = Value of **Max.**

Parameter	Description
	target resolution (for example, 300 pixels) x Actual video resolution (width)/1920 You can click **Show on Image** to view the maximum target width in the image.

b. Set parameters under **Advanced Parameters**, as shown in Figure 3. Table 2 describes the parameters.

Figure 3 Setting advanced parameters

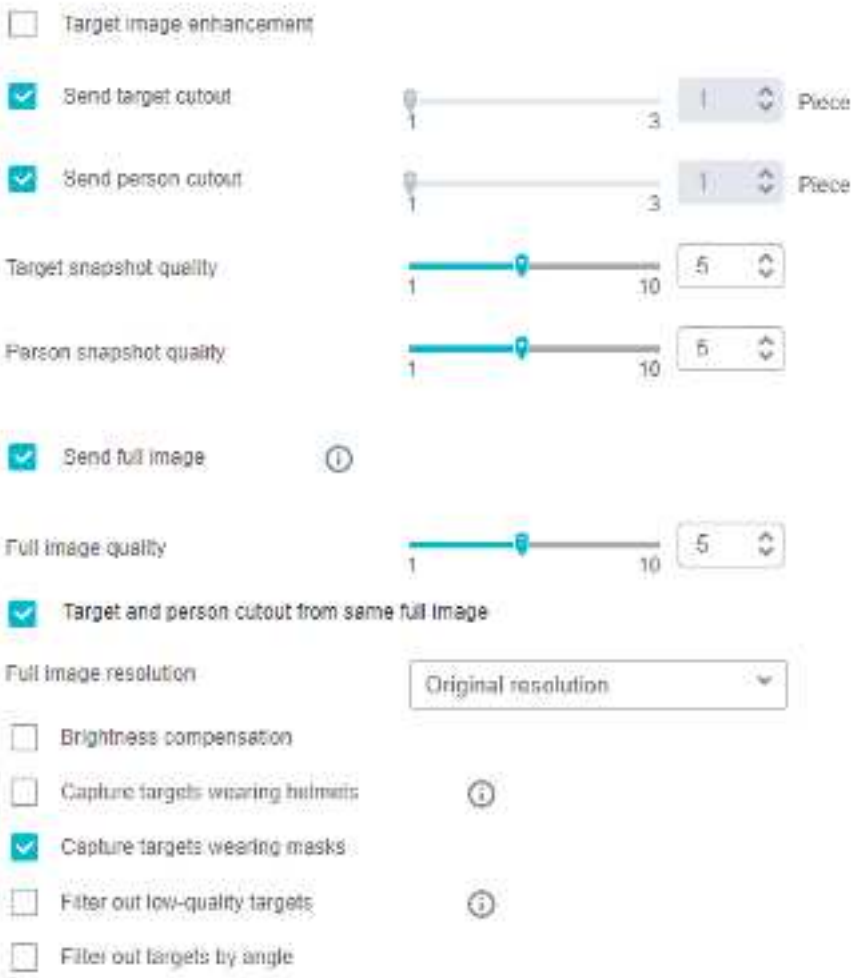


Table 2 Parameter description

Parameter	Description
Target image enhancement	You can perform YUV denoising on the target images cropped from captured images to improve the luminance and detail effect of target cutouts.

Parameter	Description
	NOTE: • You are advised to enable this function only when the brightness and contrast are insufficient in a scene. In other scenarios, it will result in overexposed images. • Some camera models do not support this function.
Send target cutout	If this check box is selected, the camera sends only the target images but not the whole live video images to the video security platform. The number of snapshots taken for a single target can be set. The value ranges from 1 to 3. **NOTE:** Some cameras can capture only one image for a single target.
Send person cutout	If this check box is selected, the camera sends only the person images but not the whole live video images to the video security platform. The number of snapshots taken for a single target can be set. The value ranges from 1 to 3. **NOTE:** Some cameras can capture only one image for a single target.
Target snapshot quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Person snapshot quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Send full image	If this check box is selected, the camera sends the whole live video images to the video security platform.

Parameter	Description
Full image quality	There are 10 levels of captured image quality. A larger value indicates higher image quality, but will require more storage space. Set this parameter based on the site requirements.
Target and person cutout from same full image	If this check box is selected, the camera sends only the whole live video images but not target images or person images to the video security platform
Full image resolution	Resolution of full images. Set this parameter based on the site requirements.
Brightness compensation	If this function is enabled, the exposure is automatically decreased in highlight or increased in backlight to ensure ideal brightness in different environments.
Compensation level	This parameter is available only when brightness compensation is enabled. Maximum target brightness compensation coefficient. The default value is **50**. The camera will automatically adjust the compensation level within the specified range based on the image brightness. The value of this parameter can be properly increased in frontlight or backlight conditions.
Target exposure duration (min)	This parameter is available only when brightness compensation is enabled. When a target is detected, target exposure is performed for a specified period of time. Set the exposure duration based on the site requirements. You are advised to set this parameter to 10 minutes in densely populated scenarios and 5 minutes in sparsely populated scenarios.
Capture targets wearing helmets	If this check box is selected, the camera takes snapshots of targets wearing helmets, reducing the false negative rate.
Capture targets wearing masks	If this check box is selected, the camera takes snapshots of targets wearing masks.

Parameter	Description
Filter out low-quality targets	If this check box is selected, the camera filters out some unclear targets or targets whose yaw or pitch angle exceeds 50° during capture.
Filter out targets by angle	If this check box is selected, **Yaw angle** and **Pitch angle** must be set. Then the camera captures targets only in the specified yaw and pitch angles.
Yaw angle	This parameter is available only when **Filter out targets by angle** is selected. The value ranges from 0° to 90°. Set this parameter based on the site requirements. After the parameter setting, the camera takes snapshots only of the targets whose yaw angle does not exceed the specified value.
Pitch angle	This parameter is available only when **Filter out targets by angle** is selected. The value ranges from 0° to 70°. Set this parameter based on the site requirements. After the parameter setting, the camera takes snapshots only of the targets whose pitch angle does not exceed the specified value.

c. Click **Rule Area**. Draw a detection area and an exclude area. If no area is drawn, the entire area is under detection by default. Set parameters under **Rule Area**, as shown in Figure 4. Table 3 describes the parameters.

Figure 4 Drawing a rule area



Table 3 Parameter description

Parameter	Description

Parameter	Description
Detection Area	After a detection area is set, the system detects targets only in the area. Click **Polygonal Area**, **Rectangular Area**, or **Full Screen**, and move the pointer to the live video image. When a cross is displayed, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location. This operation does not apply to **Full Screen**. • Only one target detection area can be stored. To add another one, delete the original one.
Exclude Area	After an exclude area is set, the system does not detect targets in the area. Click **Polygonal Area**, **Rectangular Area**, or **Full Screen**, and move the pointer to the live video image. When a cross is displayed, you can draw a detection area. **NOTE:** • An exclude area can be a polygon such as a triangle or rectangle. An exclude area supports a maximum of 10 vertexes. • To redraw an exclude area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the exclude area to change its location. This operation does not apply to **Full Screen**. • Only one exclude area can be stored. To add another one, delete the original one.

NOTE

- If the target capture effect is not ideal in backlit locations such as lobby entryways, you are advised to adjust cameras as follows:

Choose **Configuration** > **Image** > **Display** > **Backlight**. Set **Backlight/WDR/HLC** to **Backlight adaptation**.

- During the setting of **Send target cutout**, **Send person cutout**, and **Send full image**, the target or full-body image and full image of the target person sent to the video security platform may be inconsistent. That is, the target or full-body image and full image of the same person show the person in different angles. This is a normal phenomenon. After the configuration is complete, this phenomenon does not occur again after the person leaves the view.

  During the setting of these parameters, this phenomenon may occur only when a target appears in the view.

5. Click **Save**.

Configuring Target Images

You can configure the size of a target image based on the site requirements.

1. Click **Advanced Settings**. The **Target Image Settings** area is displayed, as shown in Figure 5.

   Figure 5 Configuring target images

2. Click **Custom**, **Head**, or **Head + shoulder**. You can set related parameters only when you click **Custom**. Table 4 describes the parameters.

   Table 4 Target image parameters

Parameter	Description
Width	Width of the image captured by the camera. The value is 1–5 times the target width in the image. The value can contain a maximum of one decimal place.
Target height	Height of a target in the image captured by the camera. The value is 1–3 times the target height in the image. The value can contain a maximum of one decimal place.

Parameter	Description
Person height	Height of the body in the image captured by the camera. The value is 0–5 times the target height in the image. The value can contain a maximum of one decimal place.

3. Click **Save**.

Configuring Text Overlay

Text overlay allows you to superimpose information such as the snapshot time, device ID, and site information on captured full images.

1. Click the **Text Overlay** tab. The **Text Overlay** tab page is displayed, as shown in Figure 6. Table 5 describes the parameters.

   Figure 6 Text Overlay tab page

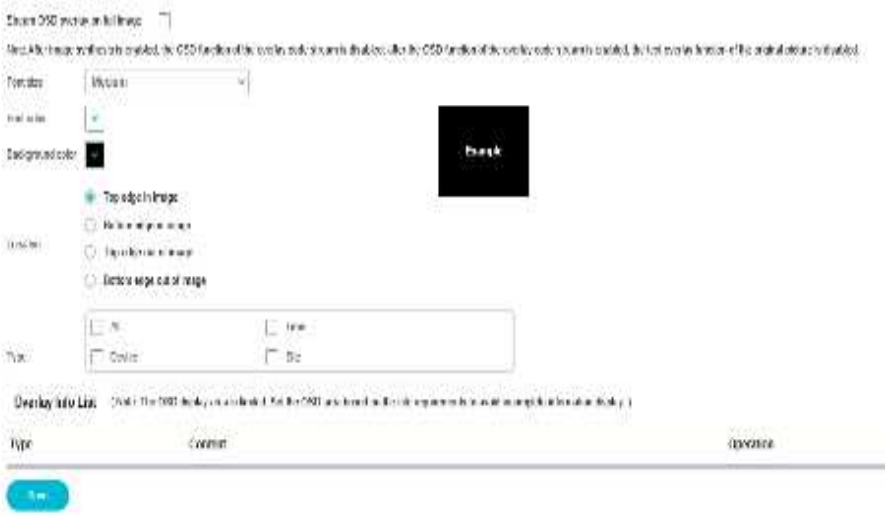


   Table 5 Text overlay parameters

Parameter	Description
Stream OSD overlay on full image	• If you deselect this check box, information set under **Text Overlay** > **Overlay Info List** will be superimposed on full images uploaded through target detection. • If you select this check box, only information set under **Configuration** > **Image** > **OSD** will be superimposed on full images uploaded through target detection.

Parameter	Description
Font size	Set the parameters based on the site requirements.
Font color	
Background color	
Location	
Type	Set the parameter based on the site requirements.
Time	Image capture time. If you select **Accurate to milliseconds**, the image capture time is accurate to milliseconds.
Device	Device ID. You can click to adjust the display sequence of device IDs.
Site	Detection site name. You can click to adjust the display sequence of detection site names.

2. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 7.

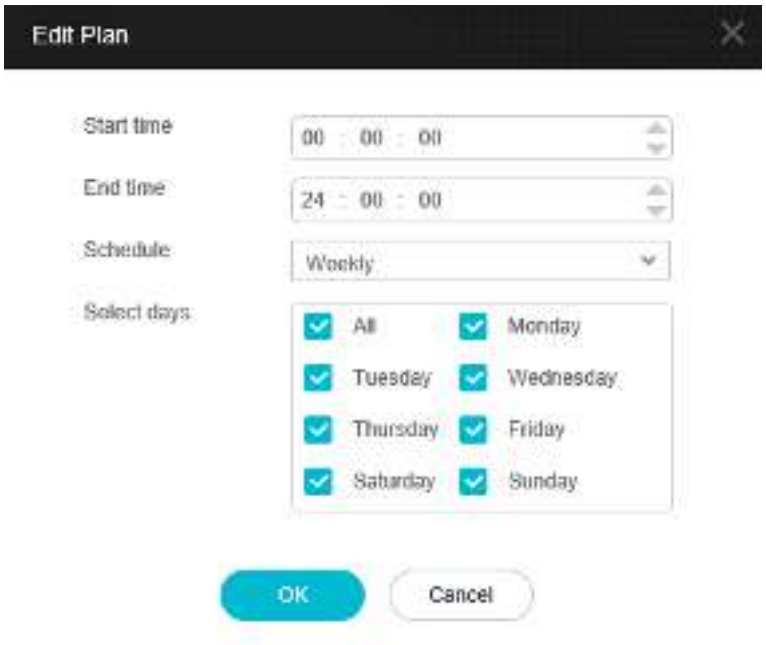
   Figure 7 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 8.

Figure 8 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

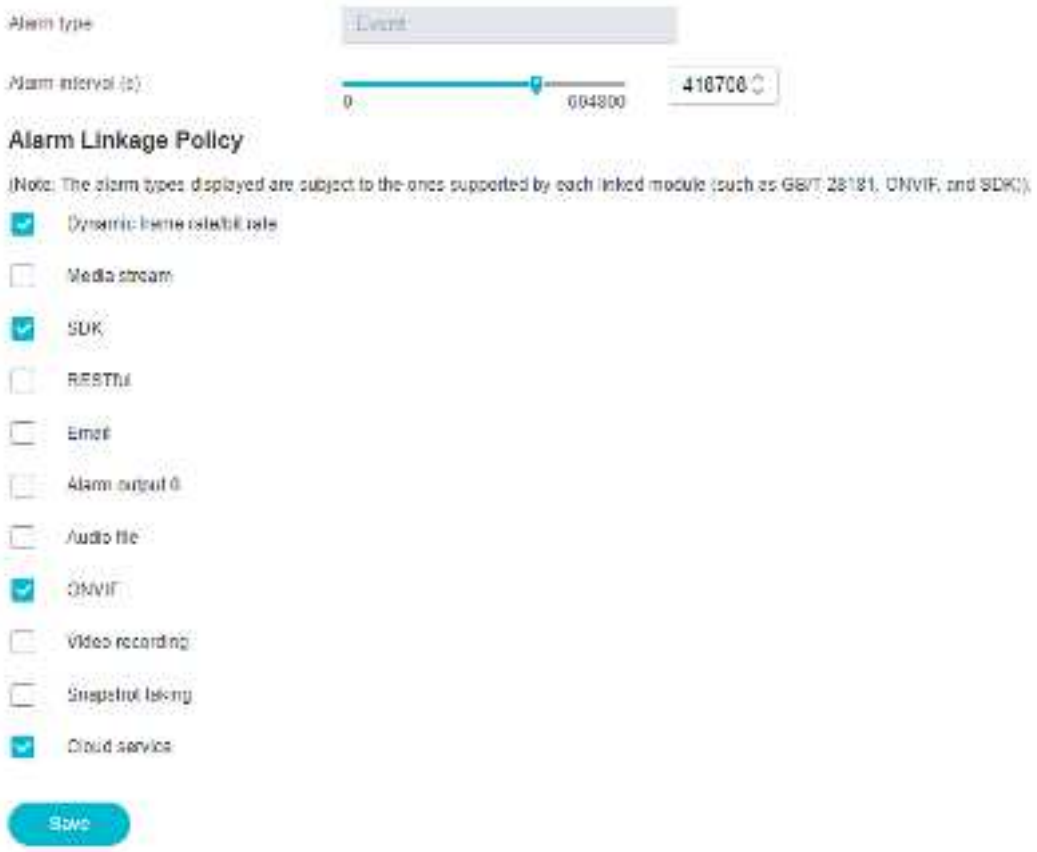
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 9.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 9 Configuring alarms



2. Set related parameters. Table 6 describes the parameters.

Table 6 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.

Parameter	Description
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on

Parameter	Description
	the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Parent topic: Configuring Intelligent Target Analysis

Configuring Mask Detection

The mask detection function checks whether a target wears a mask in a detection area. The system generates an alarm when a target meeting the alarm condition is detected.

Setting Mask Detection Parameters

NOTE

- Before configuring mask alarms, enable target attribute recognition.
- Only some models support this function.

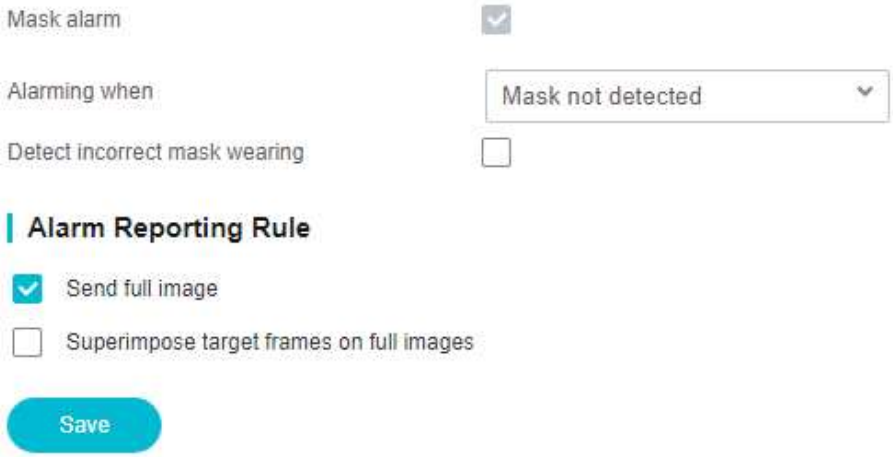
1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Mask Detection** in the **Target Intelligence** area, as shown in Figure 1.

   Figure 1 Enabling mask detection

3. Click **Settings** next to **Mask Detection**. The configuration page is displayed.

   Figure 2 Configuring Mask Detection

4. Click the **Basic Settings** tab and set **Alarming when** to **Mask detected** or **Mask not detected**.

NOTE

- If **Mask detected** is selected, the system generates an alarm upon detecting a person who wears a mask or does not properly wear a mask.
- If **Mask not detected** is selected, the system generates an alarm upon detecting a person who does not wear a mask or does not properly wear a mask.

5. (Optional) Select **Detect incorrect mask wearing**. The camera will generate alarms upon detecting targets that improperly wear masks.

   If a mask completely covers both the mouth and nose, it is considered that the mask is worn properly. If the mouth or nose is exposed, it is considered that the mask is worn improperly.

6. (Optional) Select an alarm reporting rule.

   - **Send full image**: If this check box is selected, the camera sends the full image when an alarm is generated to the upper-level video security platform as common metadata.
   - **Superimpose target frames on full images**: If this check box is selected, the camera sends the full image and target frame when an alarm is generated to the upper-level video security platform as metadata. Then the platform superimposes the target frame on the full image.

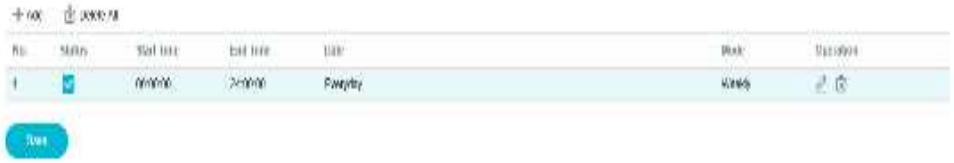
7. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

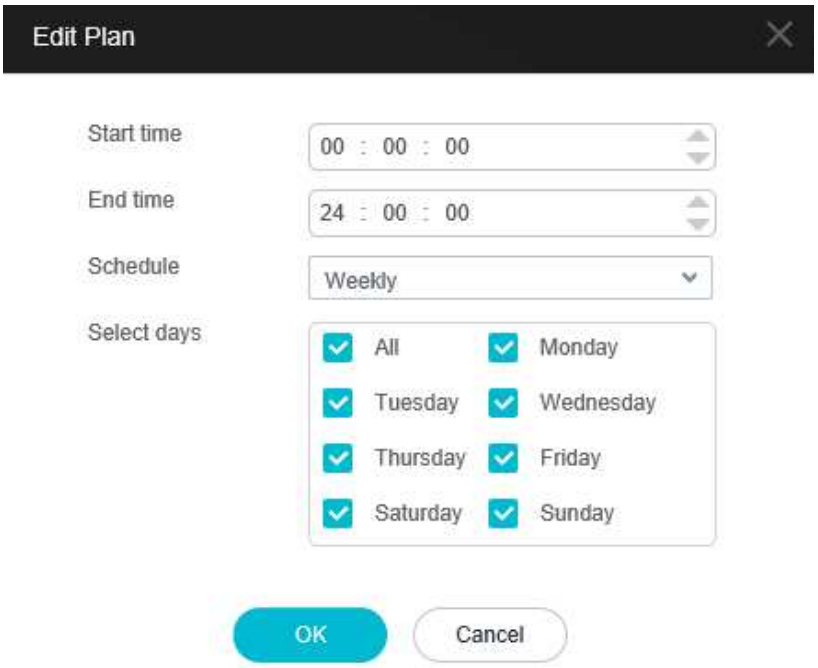
Figure 3 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

   Figure 4 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

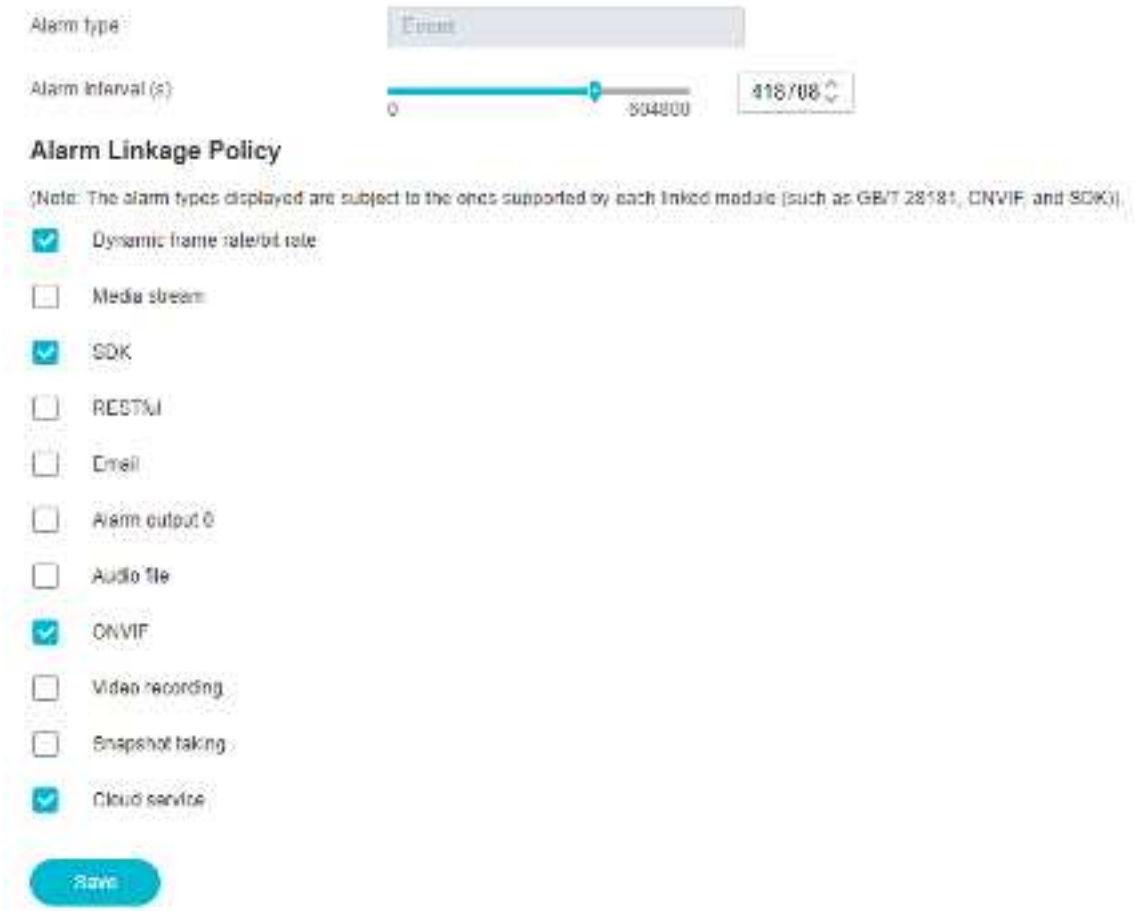
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 1 describes the parameters.

Table 1 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Parent topic: Configuring Intelligent Target Analysis

Configuring Target Counting

Setting Target Counting Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Target Counting** in the **Target Intelligence** area, as shown in Figure 1.

   Figure 1 Enabling target counting

3. Click **Settings** next to **Target Counting**.
4. Set target counting parameters, as shown in Figure 2. Table 1 describes the parameters.

   The web page varies depending on the camera model.

   Figure 2 Configuring target counting

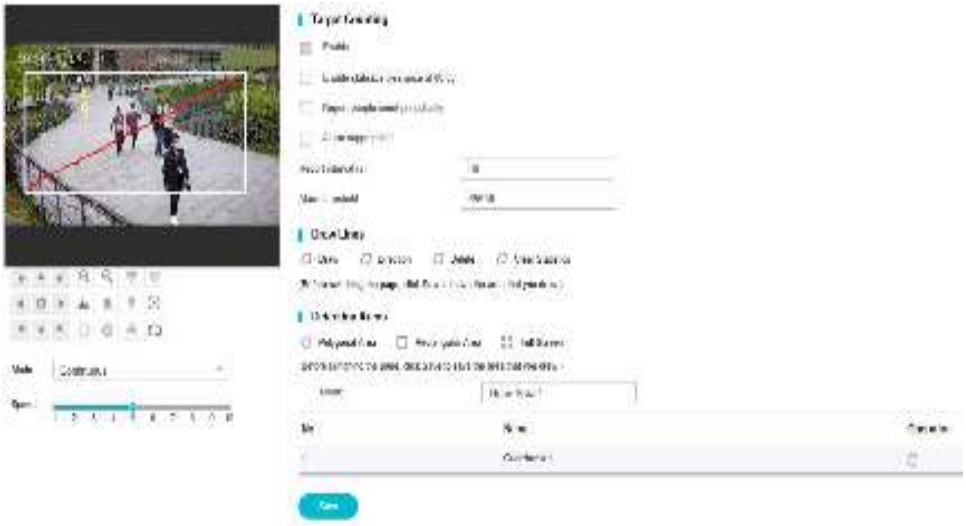
   

Table 1 Target counting parameters

Parameter	Description
Enable statistics	Indicates whether to clear the target counting statistics at 00:00 every day.

Parameter	Description
clearance at 00:00	
Report people count periodically	Interval at which the device collects statistics on the number of people entering and leaving the detection area and the total number of people entering and leaving the area up to the current time, and reports the statistics to the platform.
Alarm suppression	Indicates whether to send only the alarm that is triggered for the first time.
Report interval (s)	Reporting interval, which is available only when **Report people count periodically** is selected.
Alarm threshold	Target counting alarm threshold. When the total number of persons exceeds the value of this parameter, an alarm is generated.
Draw	Used to draw a detection line. After you click **Draw**, the pointer changes to a cross. Draw a line with an arrow for detection.
Direction	Used to draw the direction of entering the detection area. The arrow points to the direction of entering the area.
Delete	Used to delete the drawn detection line.
Clear Statistics	Used to set the number of persons entering and leaving detection areas to zero.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. You can click **Polygonal Area**, **Rectangular Area**, or **Full Screen** to draw a detection area. After the detection area is drawn, the system detects only the number of persons entering or leaving the detection area. If the number reaches the alarm threshold, the system generates an alarm. If you do not draw a detection area, the full image is used as the detection area.

5. Click **Save**.

Viewing Target Counting Results

1. Click the **Target Counting** tab. The **Target Counting** tab page is displayed, as shown in Figure 3.

   Figure 3 Viewing target counting results



2. Set related parameters. Table 2 describes the parameters.

   Table 2 Target counting parameters

Parameter	Description
Report type	Type of the report. You can view daily, weekly, monthly, and annual reports as required.
Statistical type	Type of the data to view. You can view the number of people entering or leaving the detection area as required.
Start time	For a daily report, statistics are collected from 00:00 to 24:00 on the specified day. For a weekly report, statistics are collected from Monday to Sunday of the specified week. For a monthly report, statistics are collected from the first day to the last day of the specified month. For an annual report, statistics are collected from January 1 to December 31 of the specified year.
List/Column chart/Line chart	Mode in which the statistical result is displayed.

3. Click **Count**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 4.

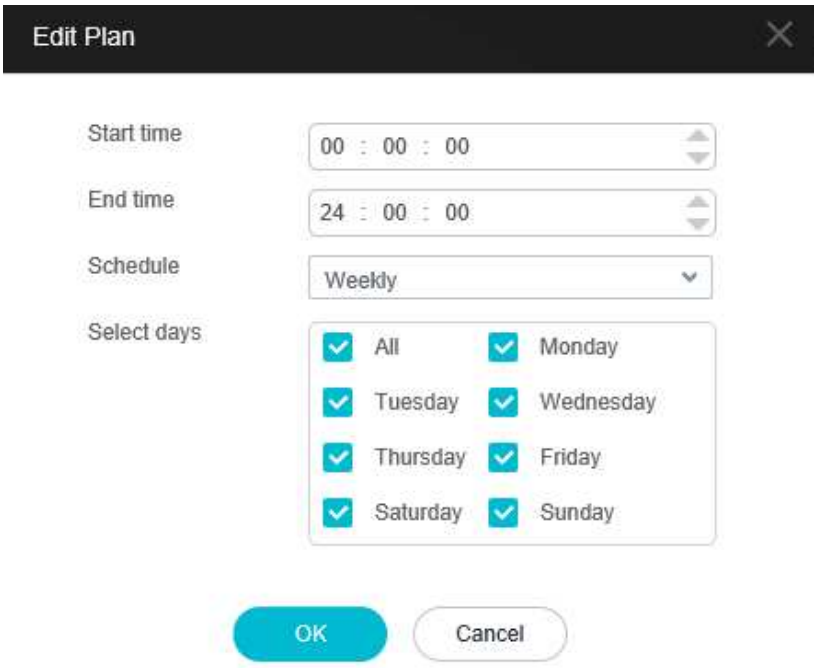
   Figure 4 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 5.

   Figure 5 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

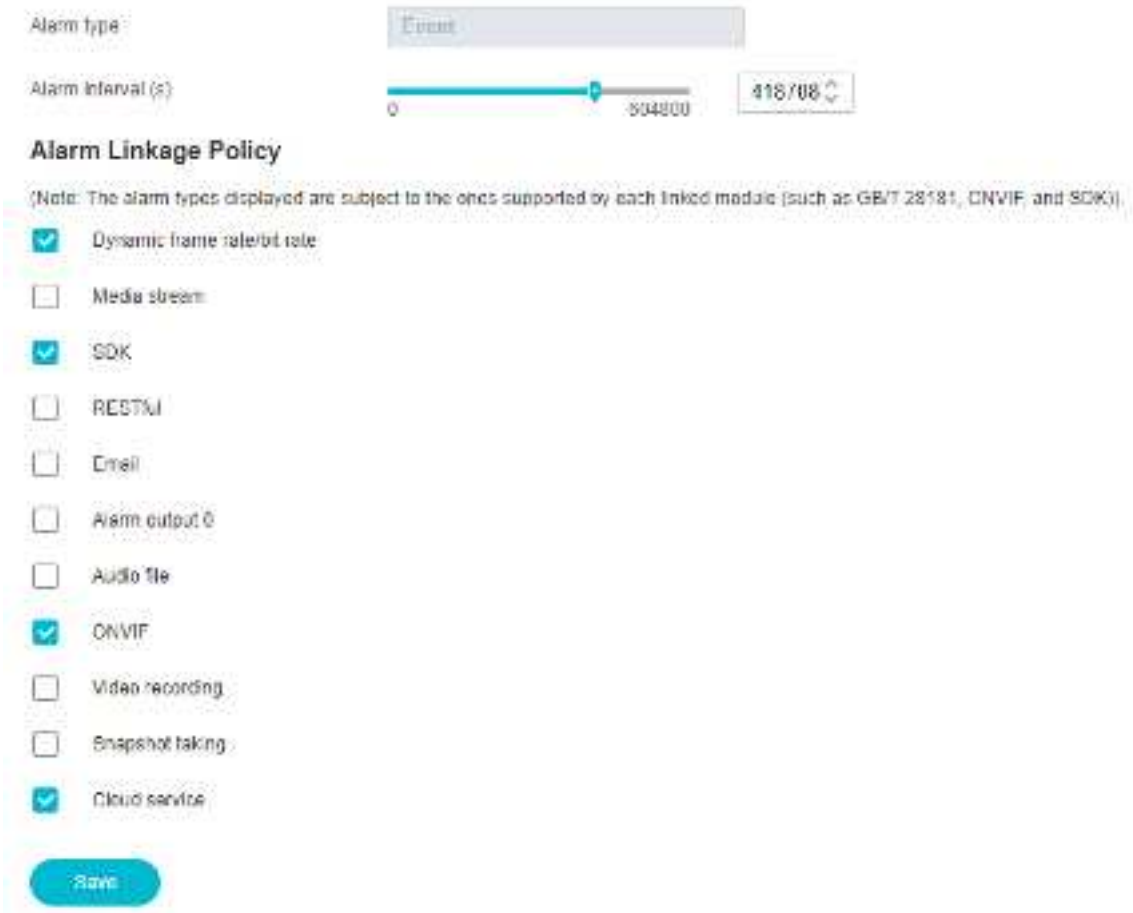
> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 6.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 6 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

You can use either of the following methods to check whether the configuration is successful:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether target counting alarms are reported.

- Configure a target counting OSD and view target counting statistics on the live video image.

  1. Choose **Configuration** > **Image** > **OSD**.
  2. Add a target counting OSD, as shown in Figure 7. Select a channel. The parameters displayed on the web page vary between camera models.

     Figure 7 OSD configuration page

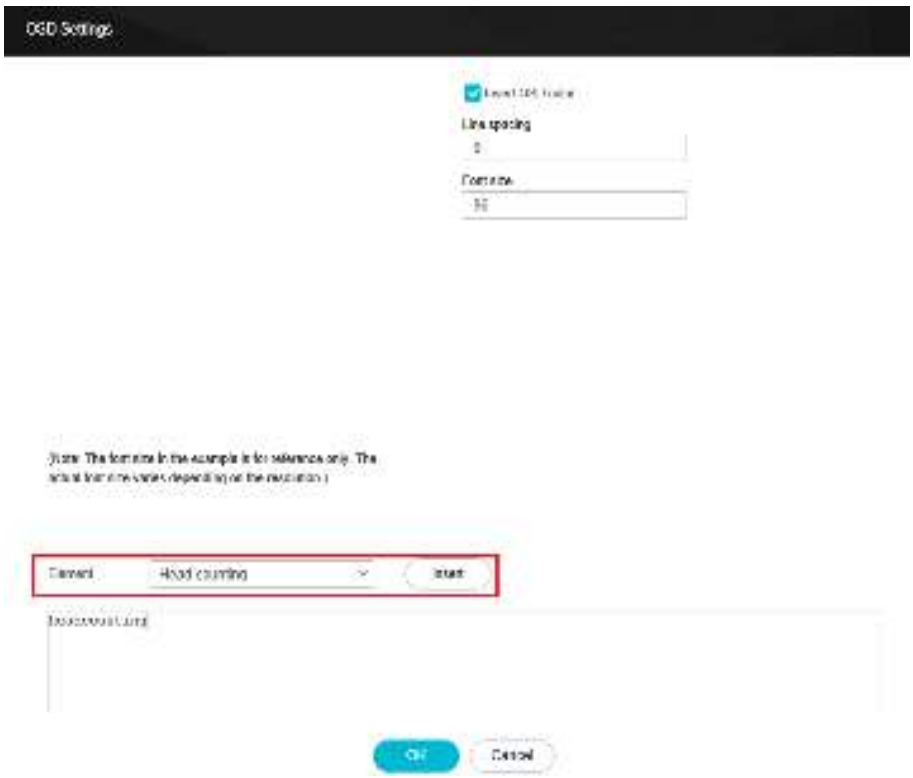
     a. Click **Add OSD**.

     b. Click . The **OSD Settings** dialog box is displayed, as shown in Figure 8.

     Select **Head counting** from the **Element** drop-down list box. Enter the OSD text in the text box below (for example,

Customer flow statistics) and click **OK**. After the configuration is complete, if the target counting function is enabled, the target counting information is displayed on the video image. For details about other parameters, see Configuring OSD.

Figure 8 Adding a target counting OSD



c. Select the OSD to be displayed.

3. Click **Save**.
4. Check the configuration result.

   Go to the **View** page to view the live video. The system automatically collects statistics on the number of people entering and leaving the detection area and displays the number on the image, as shown in Figure 9.

Figure 9 Target counting result



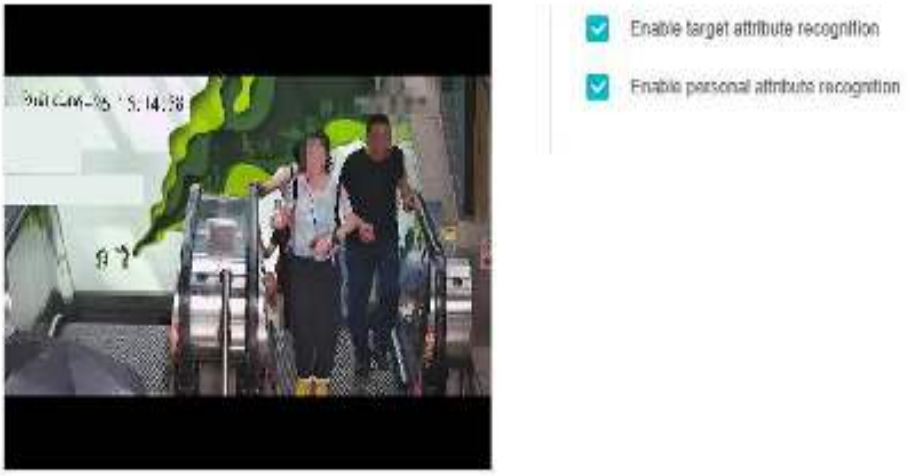
Parent topic: Configuring Intelligent Target Analysis

Configuring Target and Personal Attribute Recognition

After target attribute recognition or personal attribute recognition is enabled, the system will detect target or personal attributes such as gender, age, and whether wearing a mask. Different camera models support different capabilities. For details, see Intelligent Target Analysis Features.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. In the **Global Configuration** area, click **Settings** next to **Attribute Recognition**.
3. Select **Enable target attribute recognition** and **Enable personal attribute recognition**, as shown in Figure 1. The camera detects and analyzes target and personal attributes.

   Figure 1 Attribute Recognition page



NOTE

- Only some camera models support personal attribute recognition.

- In correct mask wearing detection, if a mask completely covers both the mouth and nose, it is considered that the mask is worn properly. If the mouth or nose is exposed, it is considered that the mask is worn improperly.

Parent topic: Configuring Intelligent Target Analysis

Viewing Intelligent Detection Results

You can check the detection results of specified attributes.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Intelligent Detection**. In the upper right corner of the page, click . In the dialog box that is displayed, select **Recognition content** and **Detection content** on the **Overall Layout** tab page, select **Target detection** and **Person detection** on the **Detection Area** tab page, and click **OK**.
3. Click **Enable Real-time Capture**.
4. If captured target and person images are displayed on the right of the video pane, as shown in Figure 1, the configuration is successful.

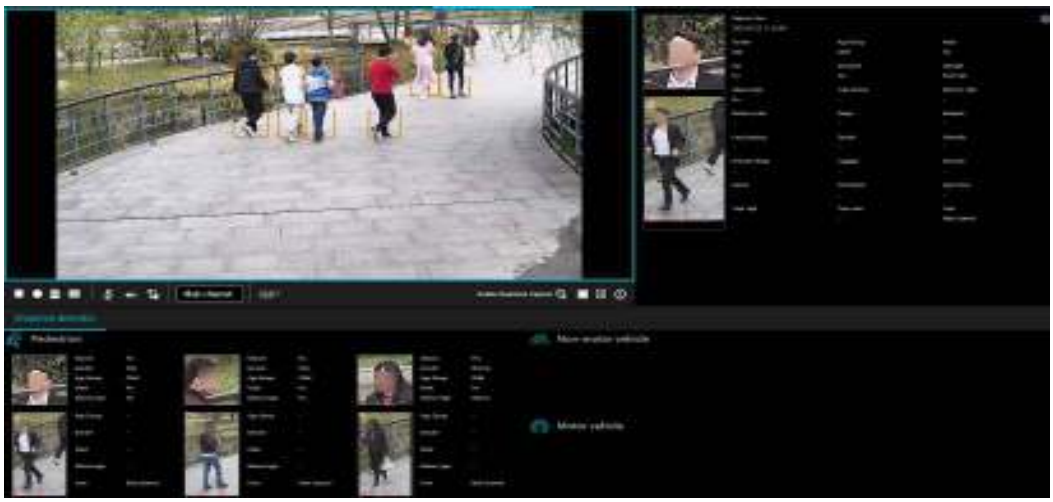
   You can also choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether target and person detection alarm logs are reported.

   NOTE

   Here, the detection images are for reference only. The images vary depending on the camera model.

   Some cameras support only target and person image capture.

Figure 1 Captured target and person images



NOTE

- To disable the real-time capture function, you can click **Disable Real-time Capture** in the lower part of the **Intelligent Detection** page.
- By default, the images captured in real time are stored on the local computer. The default storage path is **C:\Users*User name*\IPC_MediaPlayer\ScenePics**. (In this path, *User name* indicates the account of the current user in the operating system.) Ensure that the available space of the system disk is greater than 200 MB. Otherwise, images will fail to be captured. To change the storage path and space size, choose **Configuration** > **Local** > **Snapshots**, and set **Intelligent snapshot save path** and **File storage size**.
- The real-time image capture function cannot be enabled on multiple tabs at a time due to browser process conflict. When you attempt to enable the real-time capture function on multiple tabs, the message "The process of reporting target information has been started." will be displayed. In this case, you need to close unnecessary tabs and leave only one tab open or restart the browser and try again.

- Some targets may be missed during the capture due to causes such as improper image size or target angle. If the capture effect is not ideal, adjust the camera image quality, angle, and illumination for further optimization.

Parent topic: Configuring Intelligent Target Analysis

Configuring Behavior Analysis

This section describes the application scenario, configuration prerequisites, and configuration process and procedure of intelligent behavior analysis.

Intelligent Behavior Analysis Features

Application Scenarios and Configuration Process
This section describes the application scenario and configuration process of behavior analysis.

Setting Global Parameters
The behavior analysis function can be enabled only after global parameters are set.

Configuring Intrusion Detection
Intrusion detection is used to detect whether an object intrudes into a detection area (including touching the detection line and staying in the detection area). If so, an alarm is automatically generated.

Configuring Tripwire Crossing Detection
The tripwire crossing detection function checks whether a person or an object crosses a specified tripwire in a specified direction. The system generates an alarm when a person or an object crosses the tripwire.

Configuring Loitering Detection
The loitering detection function checks whether an object loiters in a detection area for a time period longer than a specified duration. The system generates an alarm when a loitering object is detected.

Configuring Abandoned Object Detection
The abandoned object detection function checks a detection area for objects that have been abandoned. The system generates an alarm when an abandoned object is detected.

Configuring Removed Object Detection
The removed object detection function checks whether an object is removed from a detection area. The system generates an alarm when an object is removed.

Configuring Area Entry/Exit Detection
The area entry/exit detection is commonly used in outdoor campuses or indoor halls. When an object enters or leaves a detection area and touches the detection line, an alarm is generated.

Configuring Fast Movement Detection
Fast movement detection is used to detect objects that move fast to prevent security risks. If an object moves fast in the detection area, an alarm is generated. This feature is applicable to scenarios such as squares, bus stations, and walkways.

Configuring Parking Detection
Parking detection is used to detect whether there is a vehicle whose parking duration exceeds the preset threshold in a detection area. If so, an alarm is generated. Only some camera models support this function.

Configuring Electric Bike Detection in Elevators or Corridors
This function is used to detect whether electric bikes enter an elevator or corridor. If any electric bike is detected inside the elevator or corridor, an alarm is generated.

Checking Intelligent Analysis Results
You can check the detection results of intelligent analysis functions. The intelligent analysis functions available on the web page vary between camera models.

Parent topic: Intelligent Settings

Intelligent Behavior Analysis Features

Different camera models support different intelligent behavior analysis features. The following table describes the differences.

Table 1 Intelligent behavior analysis features

Device Model	Tripwire Crossing Detection	Intrusion Detection	Loitering Detection	Abandoned Object Detection[a]	Removed Object Detection[a]	Area Entry/Exit Detection	Fast Movement Detection	Parking Detection	Detecti Electric Elevato
HWT-D6550-10-Z33-SV	YES	YES	YES	YES	YES	YES	YES	YES	NO
HWT-D3040-10-ELI-PV (2.8 mm)	YES	YES	YES	NO	NO	YES	YES	YES	NO
HWT-D2122-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D2152-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D3222-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D3252-10-SIU	YES	YES	YES	YES	YES	YES	YES	YES	YES
a: This function cannot be put into commercial use currently. The specifications vary greatly in different sc									

Parent topic: Configuring Behavior Analysis

Application Scenarios and Configuration Process

This section describes the application scenario and configuration process of behavior analysis.

Application Scenario

Table 1 describes the intelligent behavior analysis application scenarios.

For infrared cameras, you can enable infrared illuminators to ensure the behavior analysis accuracy. For details about how to enable infrared illuminators, see Illuminator Control.

Table 1 Behavior analysis application scenarios

Behavior Analysis	Application Scenario
Automatic tracking	Large-scale scenarios such as airports, harbors, campus, power plants, scenic spots, parks, and entrances and exits. Only one object can be tracked at a time. The manual tracking object set in the preview configuration is preferentially tracked. When there is no manual tracking object, the system tracks the moving object automatically.
Intrusion detection	Campuses or indoor halls. When a person enters the detection area, an alarm is generated.
Abandoned object detection	Key areas such as supermarkets, squares, halls, equipment rooms, and airports. When an object is abandoned in a detection area for a specified time, an alarm is generated.
Removed object detection	Key areas such as museums, exhibition halls, auctions, and jewelry stores. When an object is

Behavior Analysis	Application Scenario
	removed from a detection area, an alarm is generated.
Loitering detection	Outdoor campuses or indoor halls. When a person is loitering in a detection area for a specified time period, an alarm is generated.
Tripwire crossing detection	Applies to the following scenarios: • Wrong-way movement detection on entrances and exits of museums or subway stations. • Intrusion detection at key locations of campuses or restricted areas.
Area entry/exit detection	Outdoor campuses or indoor halls. When an object enters or leaves a detection area, an alarm is generated.
Fast movement detection	Outdoor squares, bus stations, and sidewalks. If an object moves fast in a detection area, an alarm is generated.
Electric bike detection in elevators/corridors	Elevators and corridors. If an electric bike enters the detection area, an alarm is generated.

Configuration Process

The following figure shows the intelligent behavior analysis configuration process.

Figure 1 Behavior analysis configuration process



Parent topic: Configuring Behavior Analysis

Setting Global Parameters

The behavior analysis function can be enabled only after global parameters are set.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Global Configuration** in the **Behavior Analysis** area, as shown in Figure 1.

   Figure 1 Enabling global configuration

3. Click **Settings** next to **Global Configuration**. On the **Global Configuration** page that is displayed, set perimeter detection parameters. Table 1 describes the parameters.

   The web page varies depending on the camera model.

   Figure 2 Setting global parameters

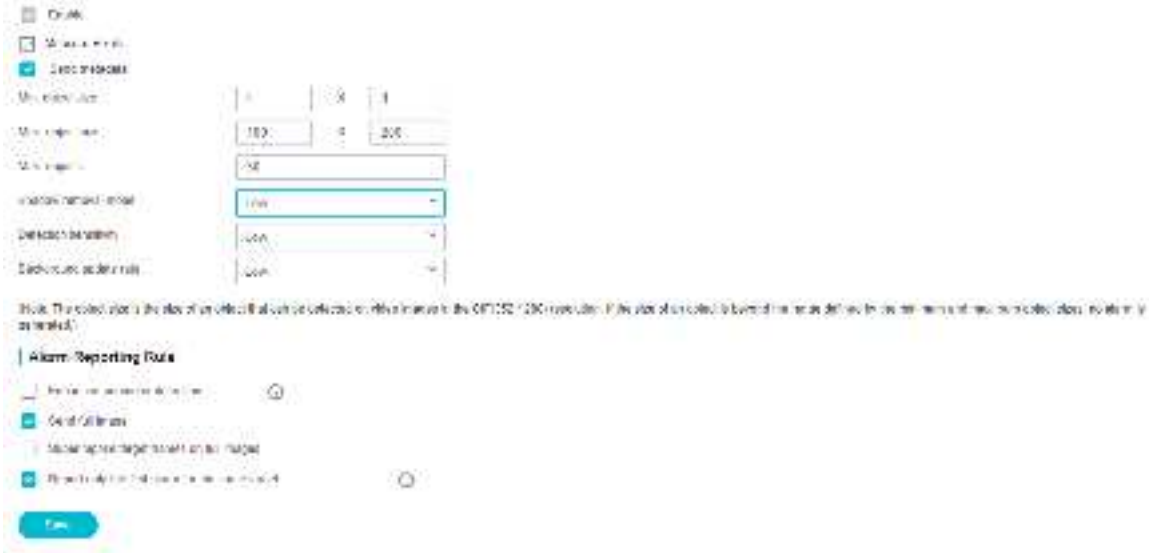
   

   Table 1 Parameter description

Parameter	Description

Parameter	Description
Enable	Indicates whether to enable global configuration. This check box is selected by default and cannot be deselected.
Measure Pixels	Used to measure object resolutions in the live video image. You can drag the box to view the predefined minimum and maximum resolutions of objects. The mentioned object resolutions are for intelligent analysis of live video at a resolution of 352 x 288 pixels. For live video at other resolutions, the horizontal resolution of objects can be calculated by the following formula: Horizontal resolution = Required horizontal resolution (for video at a resolution of 352 x 288 pixels) x Horizontal resolution of the actual live video/352. You can use the same method to calculate the vertical resolution of the pixel measurement box. For example, if the actual live video resolution is 1920 x 1080 pixels, and the required minimum resolution of the object is 5 x 5 pixels, the resolution of the pixel measurement box should be 28 x 19 pixels. The object resolution in the video directly affects object recognition. If the object resolution is low, you need to readjust the camera angle and focal length to ensure that the object resolution meets the requirements.
Send metadata	Indicates whether to send metadata. After this function is enabled, the camera will send metadata information such as intelligent analysis rules and intelligent analysis results as well as live video images to the video security platform. **NOTE:** Some camera models do not support this function.
Min. object size	Minimum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when the resolution of an identified object is less than the value of this parameter.

Parameter	Description
	NOTE: The minimum object size supported by behavior analysis is 4 x 4 (using 352 x 288 as the standard).
Max. object size	Maximum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when the resolution of an identified object is greater than the value of this parameter. **NOTE:** The maximum object size supported by behavior analysis is 200 x 200 (using 352 x 288 as the standard).
Max. objects	Maximum number of objects for intelligent analysis. Set this parameter based on the value range displayed on the GUI.
Shadow removal mode	Mode in which the shadow is removed. The shadow generated when objects are moving affects the detection size. Set this parameter based on the site requirements. **NOTE:** • In a scenario with no shadow or small shadows, **Low** is recommended to ensure complete detection of objects. • In a scenario with obvious large shadows, **High** is recommended to cut objects from shadows to make bounding rectangles closer to the object sizes or cut objects overlapped with shadows to separately display the objects.
Detection sensitivity	Sensitivity in which an object can be detected. A higher sensitivity indicates a higher detection rate but also a higher false positive rate and more device performance consumption.

Parameter	Description
	NOTE: • When there is any interference such as lamplight and rustling leaves, **Low** is recommended to prevent false alarms. • When the foreground and background are of similar colors, **High** is recommended.
Background update rate	Speed of integrating an object into the background. A larger value indicates quicker object integration.
Enhanced perimeter detection	Indicates whether to allow the camera to send the full image, rule frame, and object frame when an alarm is generated to the video security platform as three-layer TLV metadata. Then the platform can superimpose the object frame and rule frame on the full image.
Send full image	Indicates whether to allow the camera to send the full image when an alarm is generated to the video security platform as common metadata.
Superimpose target frames on full images	Indicates whether to allow the camera to send the full image, rule frame, and object frame when an alarm is generated to the upper-level video security platform as metadata. If this check box is selected, the platform superimposes the object frame and rule frame on the full image.
Report only the first alarm for the same target	Indicates whether to send only the alarm that is triggered for the first time.
Intelligent recording marking	Indicates whether to allow the camera to mark intelligent event data such as people, vehicles, and non-motorized vehicles in recordings and send the data to the video security platform.

4. Click **Save**.

Parent topic: Configuring Behavior Analysis

Configuring Intrusion Detection

Intrusion detection is used to detect whether an object intrudes into a detection area (including touching the detection line and staying in the detection area). If so, an alarm is automatically generated.

The criteria for determining whether an object enters the detection area are related to the recognition mode. For example, if the recognition mode is set to center, an alarm is triggered when the central part of an object enters the detection area.

Setting Intrusion Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Intrusion** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set intrusion detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting intrusion detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring intrusion detection



   Table 1 Parameter description

Parameter	Description
Object tracking	Indicates whether to enable the camera to generate an alarm and automatically track the object entering the intrusion detection area. **NOTE:** Object tracking and PTZ linkage cannot be enabled at the same time. The object tracking function is available only for some camera models. The configuration cannot be modified during object tracking. If you modify the configuration, the system displays a message indicating that the device is busy.
Sensitivity	Intrusion detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.
Detection object	Type of objects to be detected. The options include **Pedestrian**, **Motor vehicle**, and **Non-motor vehicle**. After you select a detection object type, the camera

Parameter	Description
	automatically reports an intrusion alarm upon detecting an object of the selected type. **NOTE:** This parameter is unavailable for some camera models.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects intrusions only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The intrusion detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live

Parameter	Description
	video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The intrusion detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:** All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click  .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

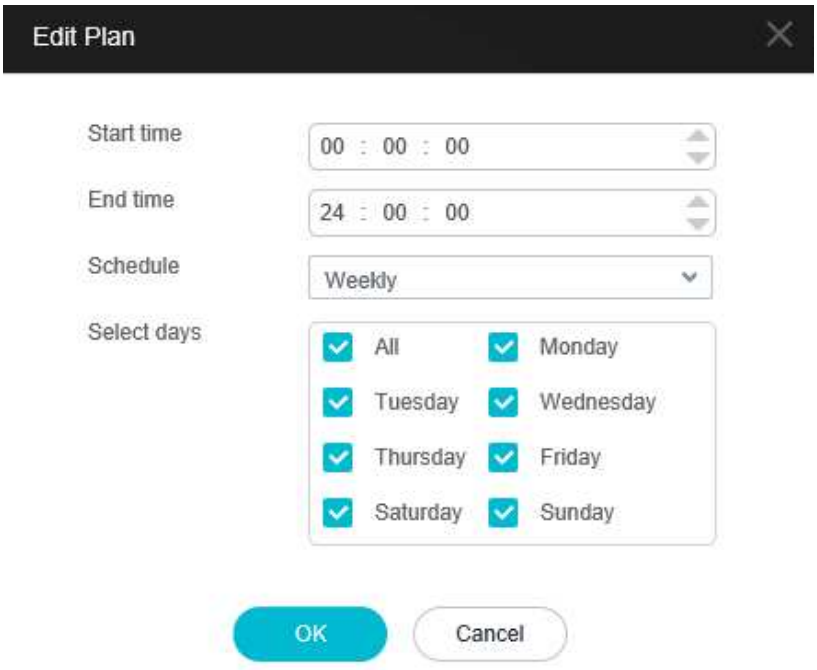
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

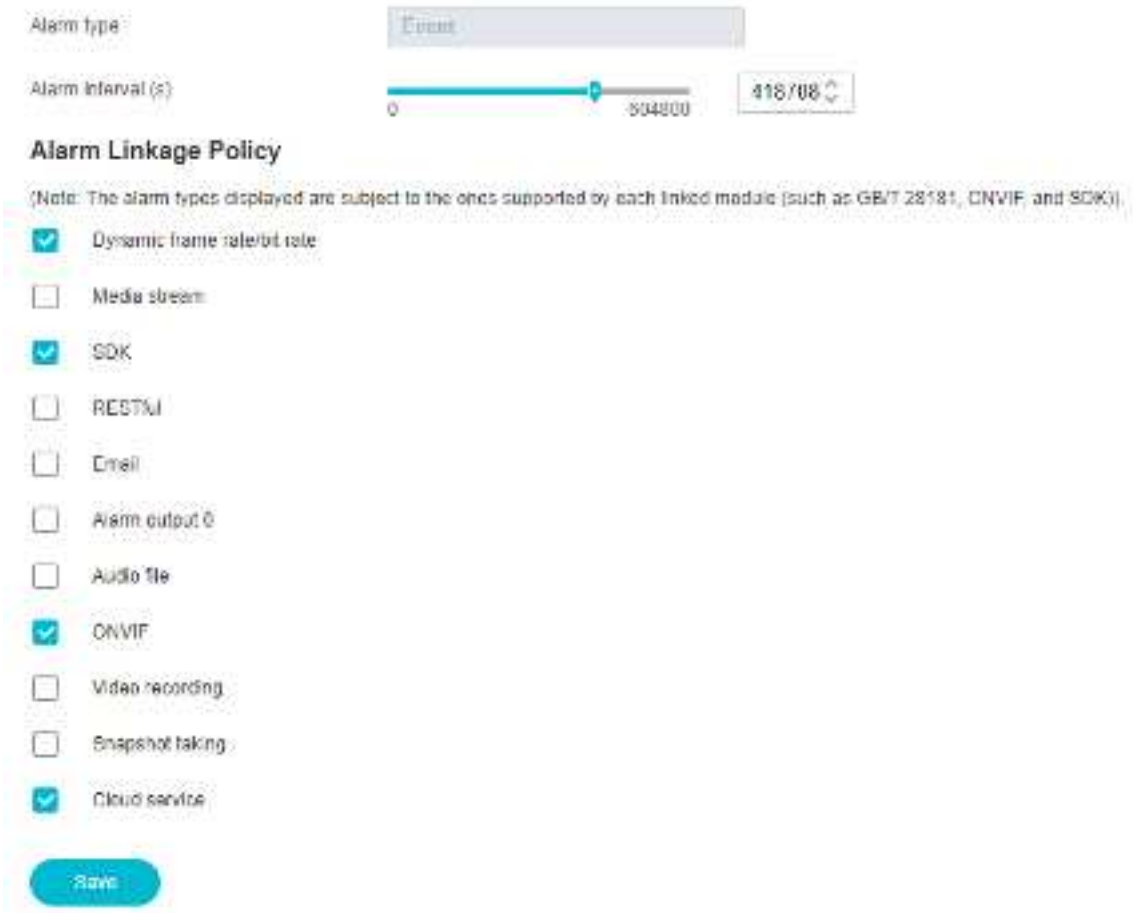
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object enters the detection, you can verify the configuration in one of the following ways:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct. The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution

Configuring Tripwire Crossing Detection

The tripwire crossing detection function checks whether a person or an object crosses a specified tripwire in a specified direction. The system generates an alarm when a person or an object crosses the tripwire.

Setting Tripwire Crossing Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Tripwire** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set tripwire crossing detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting tripwire crossing detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring tripwire crossing detection



Table 1 Parameter description

Parameter	Description
Object tracking	Indicates whether to allow the camera to generate an alarm and automatically track an object when the object

Parameter	Description
	crosses the detection line. **NOTE:** Object tracking and PTZ linkage cannot be enabled at the same time. The object tracking function is available only for some camera models. The configuration cannot be modified during object tracking. If you modify the configuration, the system displays a message indicating that the device is busy.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.
Sensitivity	Tripwire crossing detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Detection object	Type of objects to be detected. The options include **Pedestrian**, **Motor vehicle**, and **Non-motor vehicle**. After you select a detection object type, the camera automatically reports a tripwire crossing alarm upon detecting an object of the selected type. **NOTE:**

Parameter	Description
	Some camera models support detection object selection.

4. Draw a tripwire.

   You need to draw a tripwire based on the site requirements. For details about how to draw a tripwire and related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Draw	Click **Draw** and draw a tripwire. **NOTE:** • To redraw a tripwire that is not saved, click **Draw** again. • After a tripwire is drawn, you can move the pointer to the position where the tripwire locates. When the pointer turns to  , you can right-click the tripwire and choose a tripwire direction from the shortcut menu. The tripwire crossing can be bidirectional or unidirectional. In unidirectional mode, the tripwire crossing direction follows the right-hand rule. That is, when you stretch your palm outward with the four fingers following the tripwire drawing direction, the direction your thumb points is called the positive direction, and the opposite is the negative direction. • A maximum of 32 tripwires are supported. • You can perform operations on a single tripwire at a time.
No.	ID of a tripwire.
Name	Name of a tripwire.
Status	Status of a tripwire.

Parameter	Description
	To change the status of a tripwire, select it from the tripwire list and click the **Status** toggle button.
Operation	Column containing the icon for deleting a tripwire. To delete a tripwire, select it from the tripwire list and click .

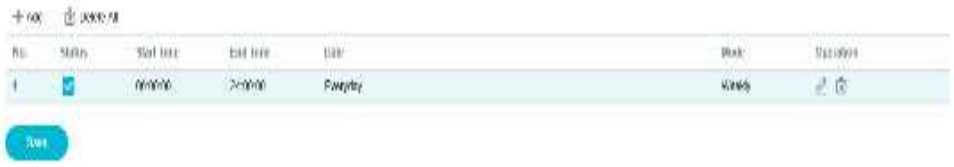
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

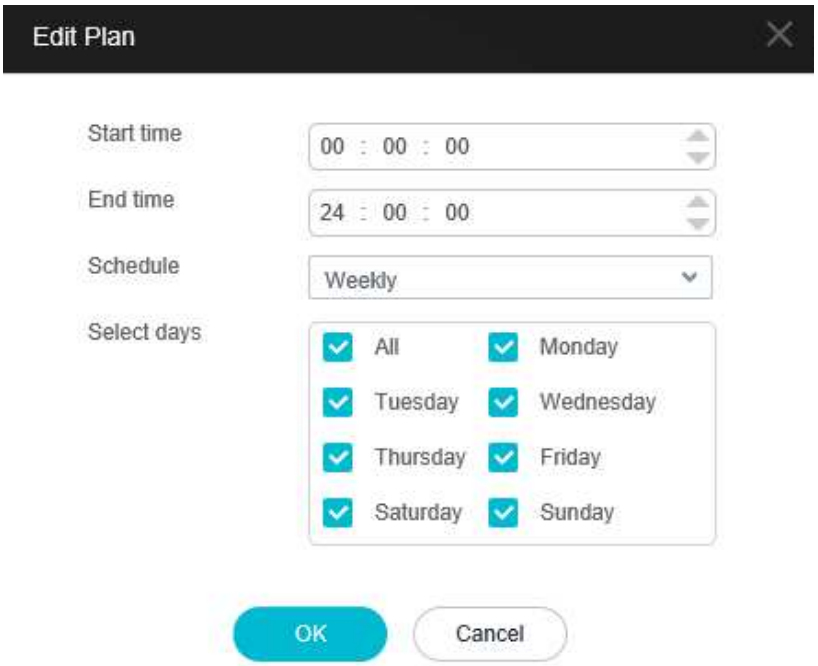
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

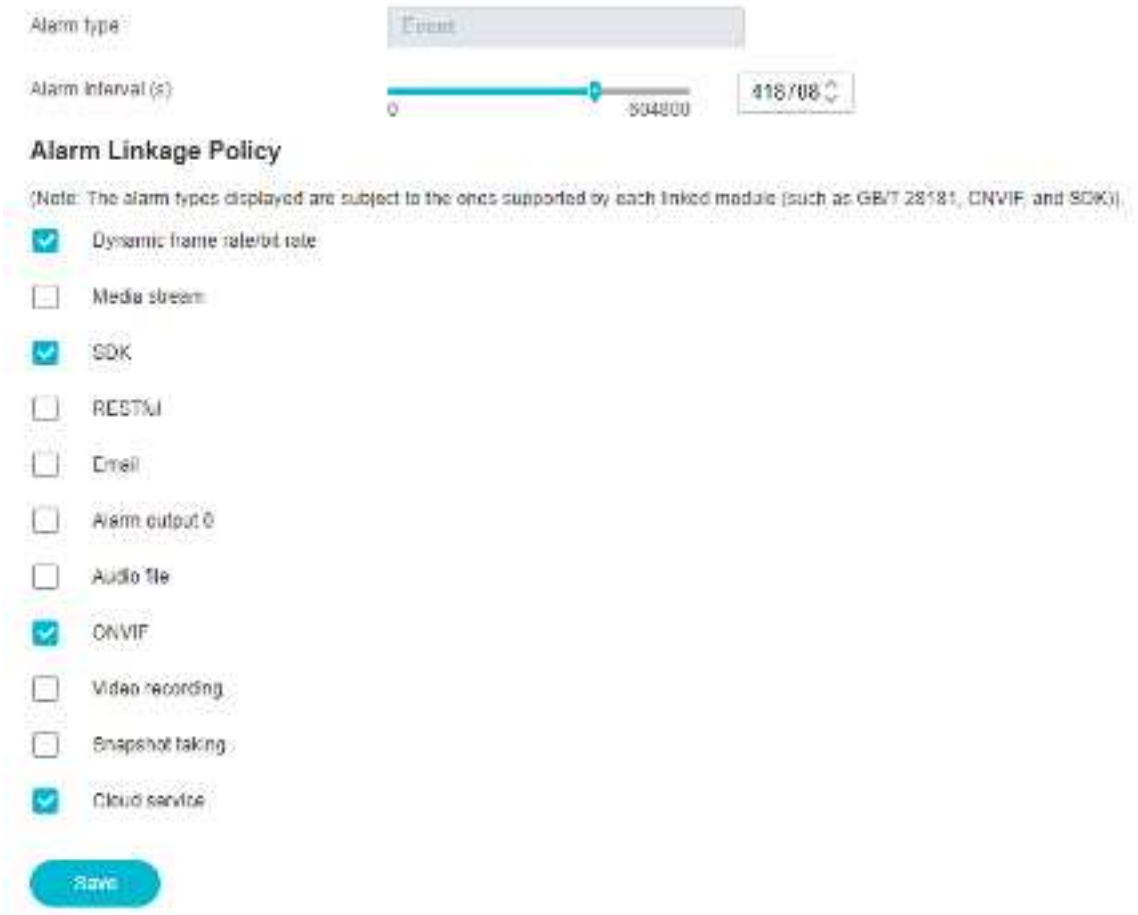
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object crosses the tripwire in the specified direction, you can verify the configuration is one of the following ways:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct.

The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Loitering Detection

The loitering detection function checks whether an object loiters in a detection area for a time period longer than a specified duration. The system generates an alarm when a loitering object is detected.

Setting Loitering Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Loitering** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set loitering detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting loitering detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring loitering detection

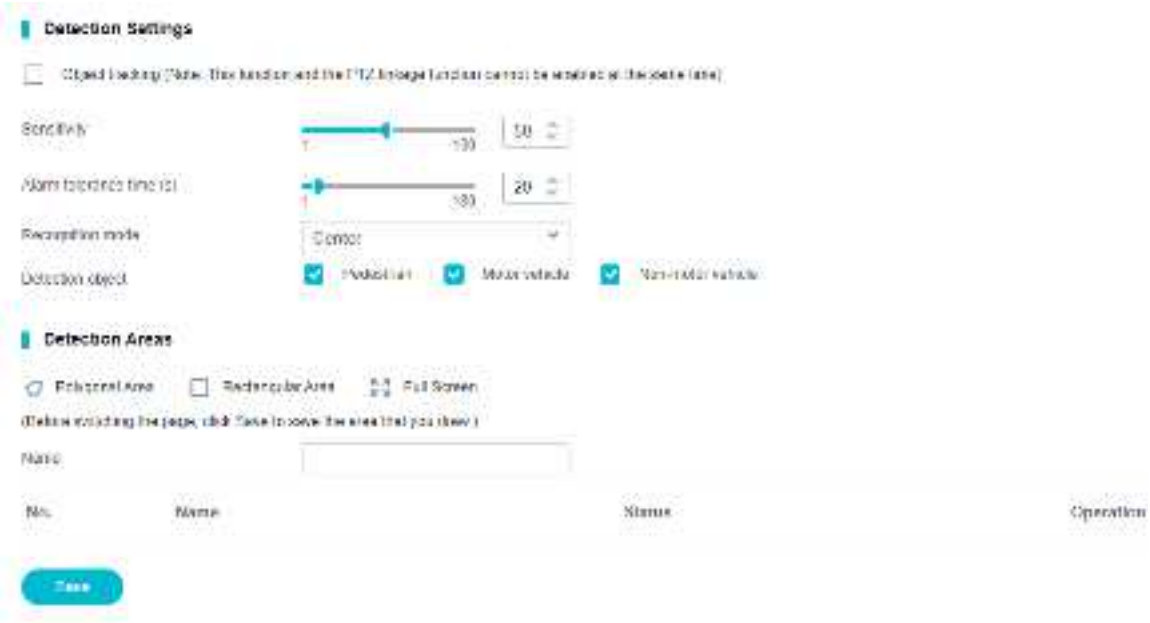


Table 1 Parameter description

Parameter	Description
Object tracking	Indicates whether to allow the camera to generate an alarm and automatically track an object when the

Parameter	Description
	object loiters in the detection area. **NOTE:** Object tracking and PTZ linkage cannot be enabled at the same time. The object tracking function is available only for some camera models. The configuration cannot be modified during object tracking. If you modify the configuration, the system displays a message indicating that the device is busy.
Sensitivity	Loitering detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Alarm tolerance time (s)	Duration for which an object loiters in the detection area. If an object loiters in the detection area for a period longer than the specified duration, an alarm is generated.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.
Detection object	Type of objects to be detected. The options include **Pedestrian**, **Motor vehicle**, and **Non-motor vehicle**.

Parameter	Description
	After you select a detection object type, the camera automatically reports a loitering alarm upon detecting an object of the selected type. **NOTE:** Some camera models support detection object selection.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects loitering objects only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The loitering detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.

Parameter	Description
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The loitering detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:** All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

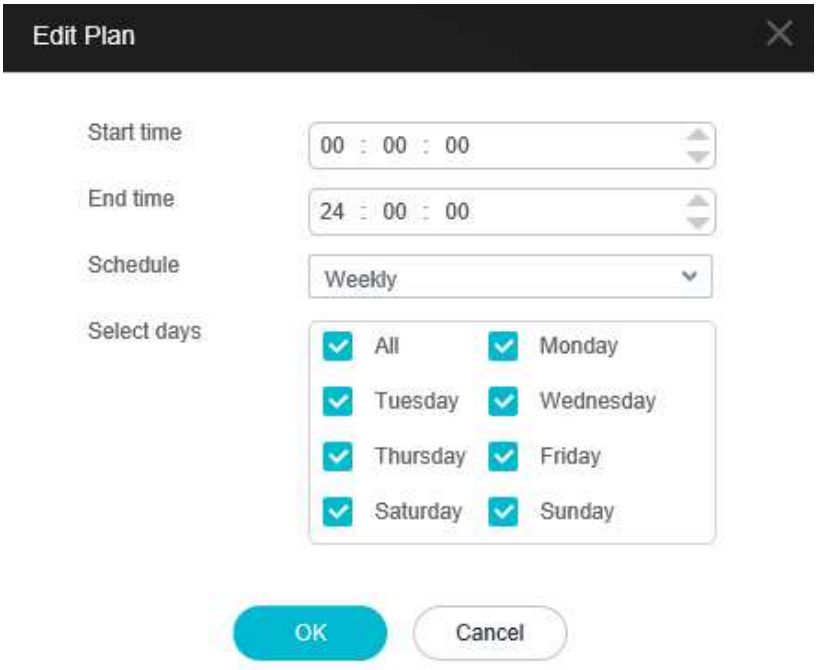
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.

5. Click **Save**.

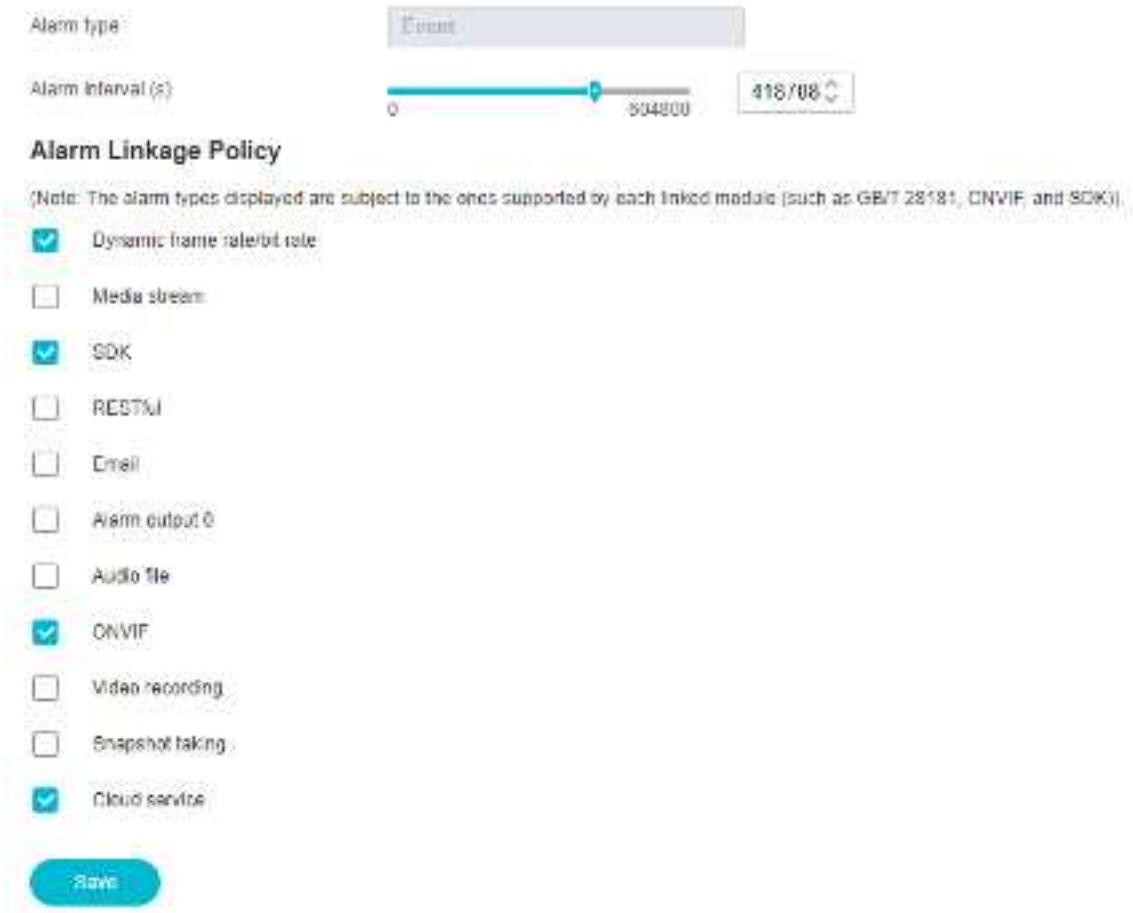
> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object loiters in the detection area for a period longer than the value of **Alarm tolerance time**, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct. The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Abandoned Object Detection

The abandoned object detection function checks a detection area for objects that have been abandoned. The system generates an alarm when an abandoned object is detected.

Setting Abandoned Object Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Abandon** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set abandoned object detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting abandoned object detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring the abandoned object detection function



   Table 1 Parameter description

Parameter	Description
Sensitivity	Abandoned object detection sensitivity. **NOTE:**

Parameter	Description
	• The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Alarm tolerance time (s)	Duration for which an object can be left in the detection area. If an object is left in the detection area for a period longer than the specified duration, an alarm is generated. The value is an integer ranging from 10 to 300. The default value is 10.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects abandoned objects only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:**

Parameter	Description
	• A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The abandoned object detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The abandoned object detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:**

Parameter	Description
	All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

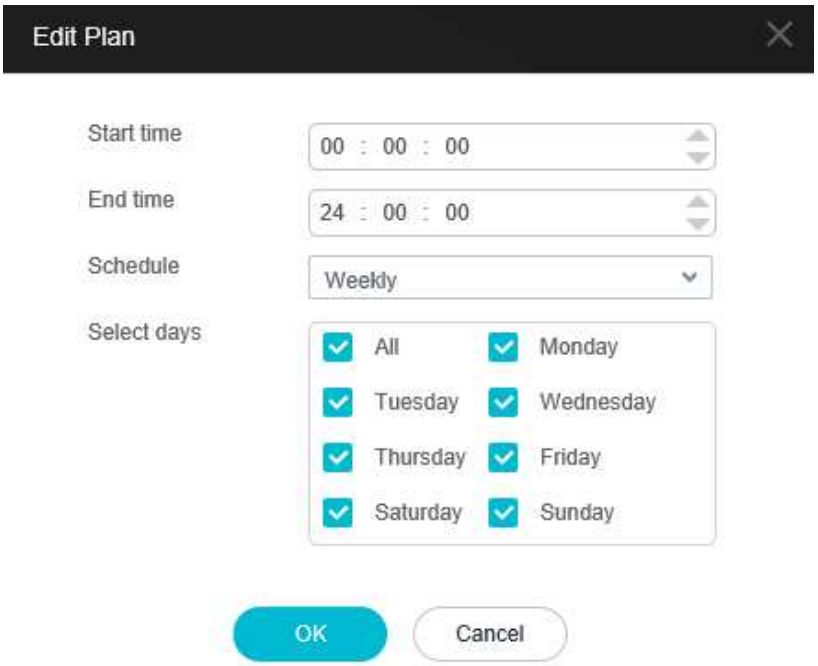
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

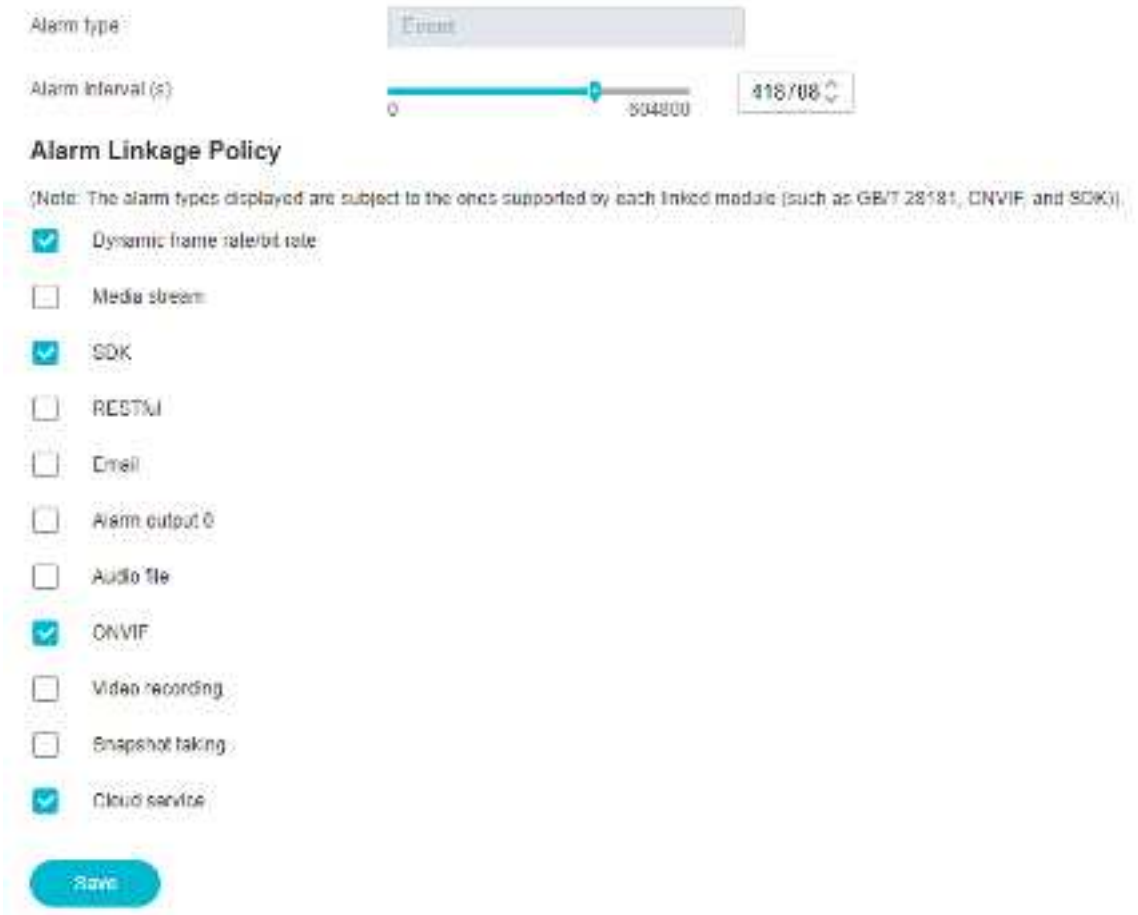
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object is carried into the detection area and left in the area for more than 10s, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct.

The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Removed Object Detection

The removed object detection function checks whether an object is removed from a detection area. The system generates an alarm when an object is removed.

Setting Removed Object Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Removal** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set removed object detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting removed object detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring the removed object detection function



   Table 1 Parameter description

Parameter	Description
Sensitivity	Removed object detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**.

Parameter	Description
	• A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects removed objects only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.

Parameter	Description
	• The removed object detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The removed object detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:** All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.

Parameter	Description
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

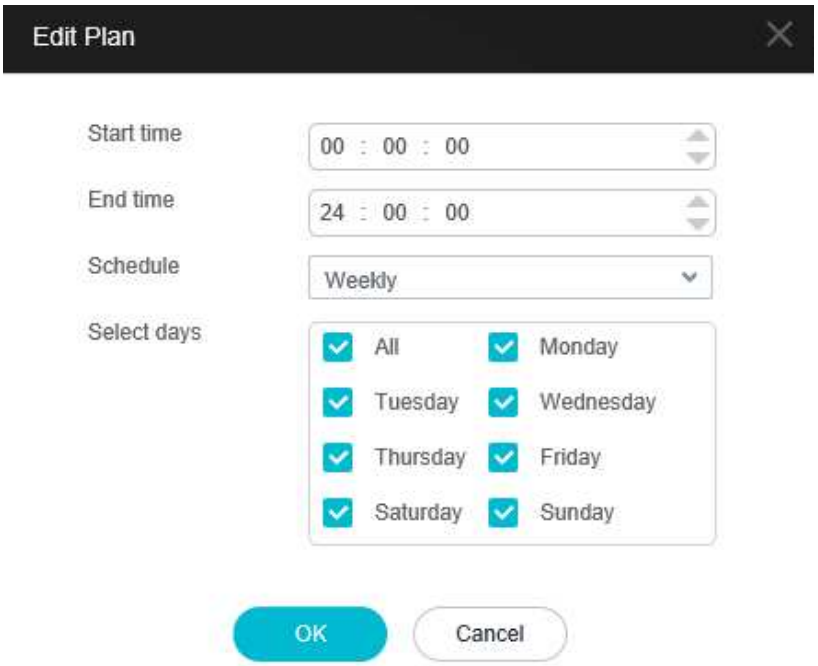
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

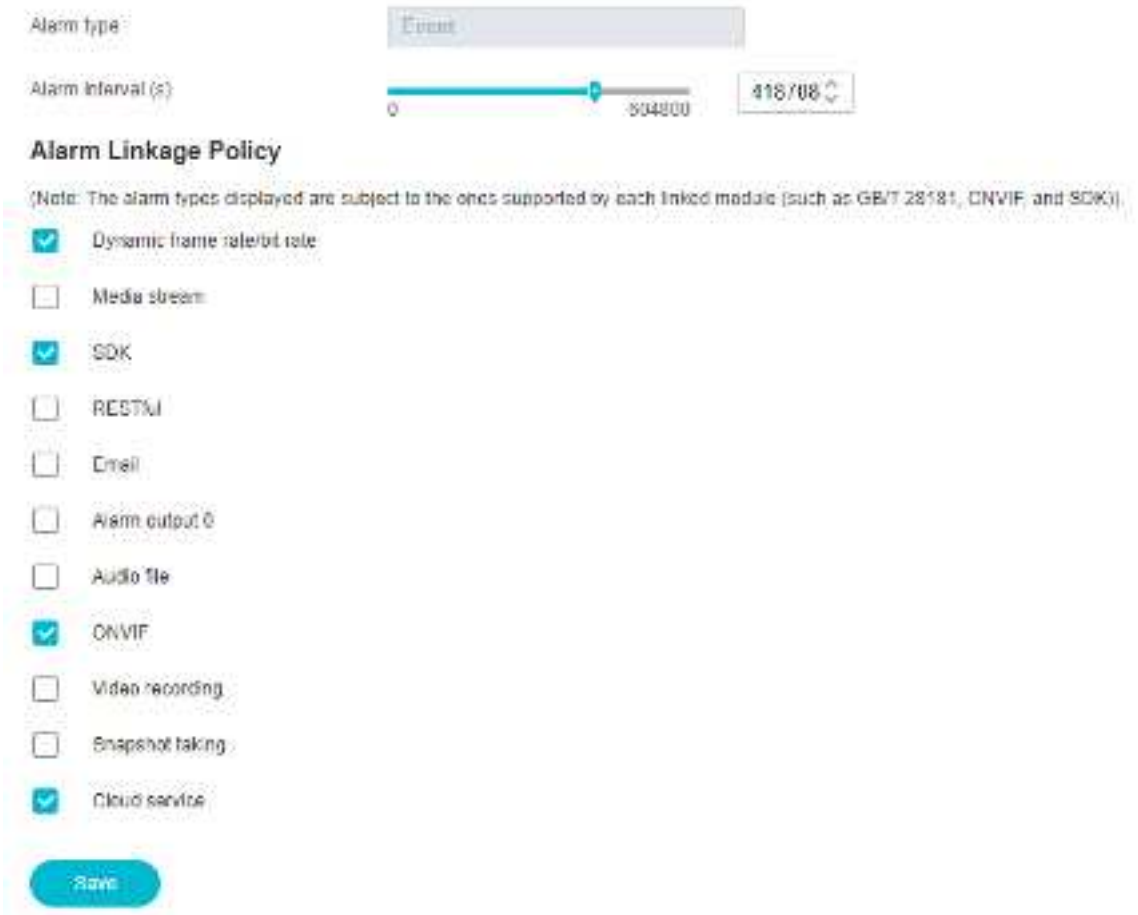
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object is removed from the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct.

The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Area Entry/Exit Detection

The area entry/exit detection is commonly used in outdoor campuses or indoor halls. When an object enters or leaves a detection area and touches the detection line, an alarm is generated.

Setting Area Entry/Exit Detection Parameters

The procedure for configuring area exit detection is the same as that for configuring area entry detection.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Area Entry** or **Area Exit** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set area entry/exit detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting area entry/exit detection parameters. Table 1 describes the parameters.

   Figure 1 Configuring area entry/exit detection

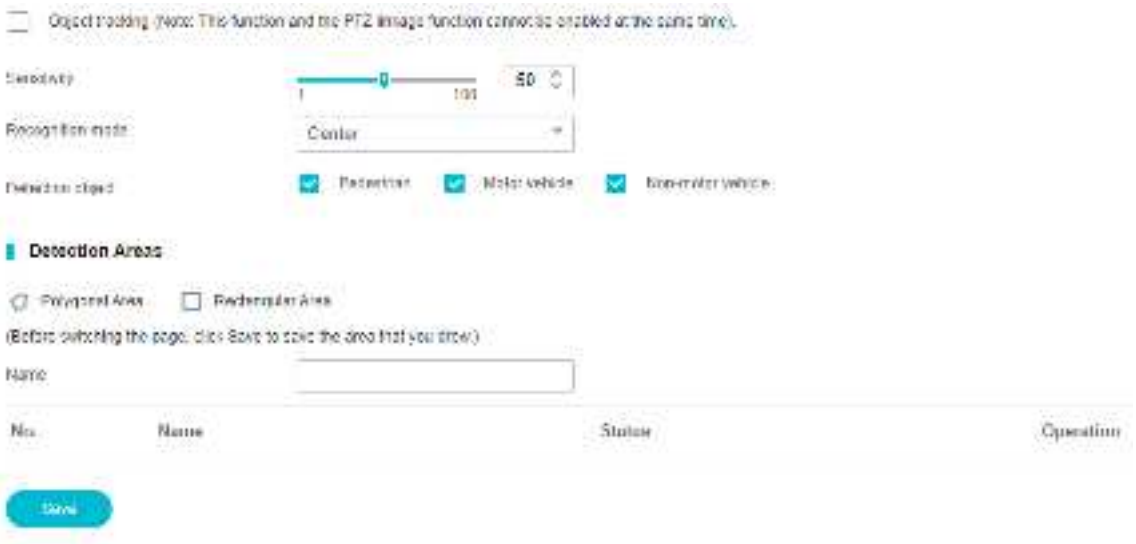


   Table 1 Parameter description

Parameter	Description
Object tracking	Indicates whether to allow the camera to generate an alarm and automatically track an object when the object enters or leaves the detection area. **NOTE:** Object tracking and PTZ linkage cannot be enabled at the same time. The object tracking function is available only for some camera models. The configuration cannot be modified during object tracking. If you modify the configuration, the system displays a message indicating that the device is busy.
Sensitivity	Area entry/exit detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.
Detection object	Type of objects to be detected. The options include **Pedestrian**, **Motor vehicle**, and **Non-motor vehicle**. After you select a detection object type, the camera

Parameter	Description
	automatically reports an area entry or exit alarm upon detecting an object of the selected type. **NOTE:** Some camera models support detection object selection.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects area entry/exit only in the detection area. You cannot set the full screen as a detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The area entry/exit detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.

Parameter	Description
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The area entry/exit detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

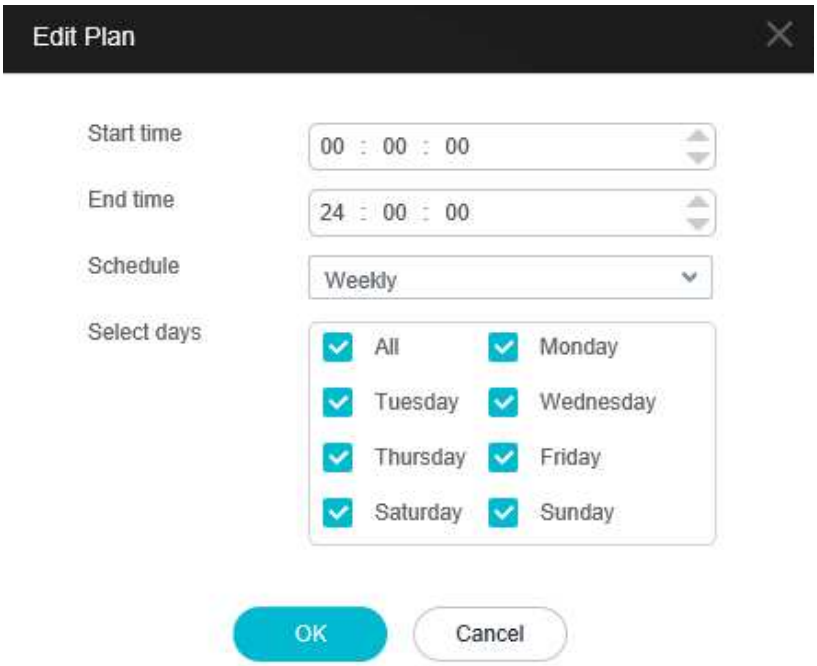
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click ✎ or 🗑 in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

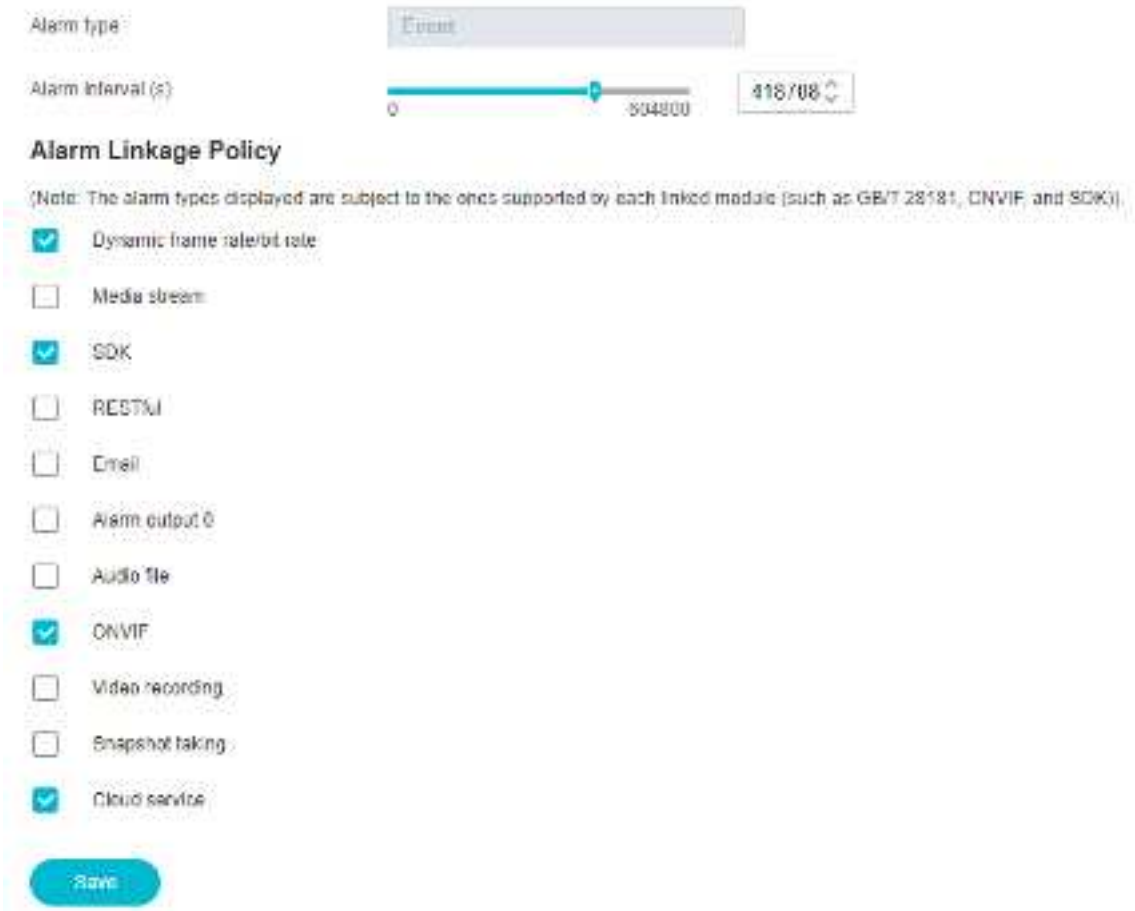
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When a moving object enters the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

Configuring Fast Movement Detection

Fast movement detection is used to detect objects that move fast to prevent security risks. If an object moves fast in the detection area, an alarm is generated. This feature is applicable to scenarios such as squares, bus stations, and walkways.

You can determine whether an object is a fast-moving object based on the actual scenario. For example, in corridors, compared with walking people, running people are fast-moving objects. However, running people are not fast-moving objects on roads but vehicles that move faster than the running people are.

You can adjust the sensitivity to detect objects moving at different speeds based on the actual scenario. For example, when the sensitivity is adjusted to a certain value, an object that moves relatively fast can be detected, but a pedestrian who walks cannot be detected.

Setting Fast Movement Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Fast Movement** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set fast movement detection parameters.

   The web page varies depending on the camera model.

   The following figure shows the page for setting fast movement detection parameters. Table 1 describes the parameters.

Figure 1 Configuring fast movement detection

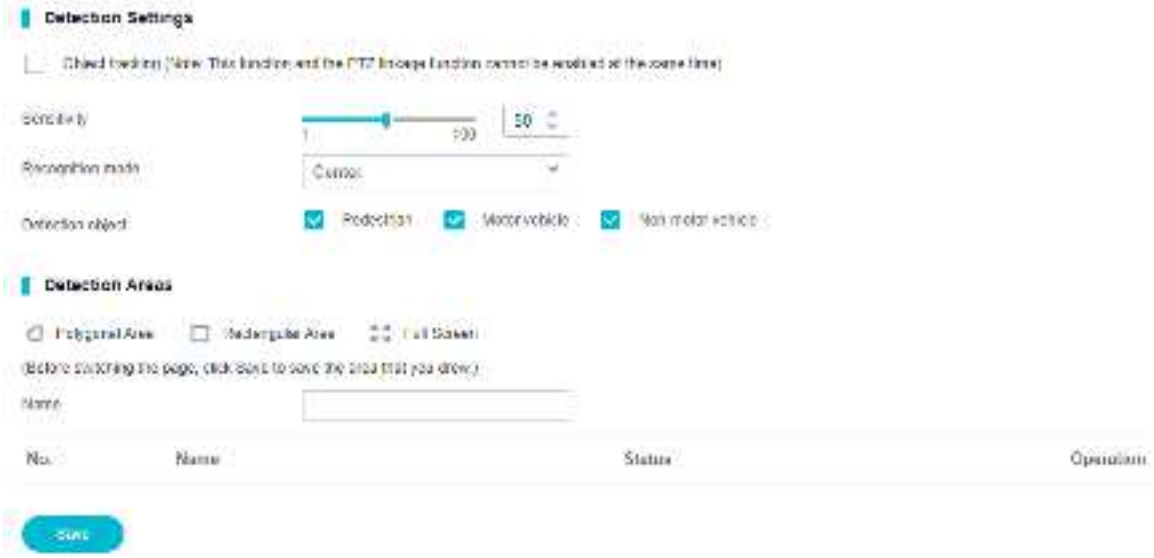


Table 1 Parameter description

Parameter	Description
Object tracking	Indicates whether to allow the camera to generate an alarm and automatically track an object when the object moves fast in the detection area. **NOTE:** Object tracking and PTZ linkage cannot be enabled at the same time. The object tracking function is available only for some camera models. The configuration cannot be modified during object tracking. If you modify the configuration, the system displays a message indicating that the device is busy.
Sensitivity	Sensitivity for fast movement detection. • If objects that move slowly can be detected under the defined sensitivity, you can decrease the sensitivity. • If objects that move fast cannot be detected under the defined sensitivity, you can increase the sensitivity.

Parameter	Description
	NOTE: • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity. To detect slight motion, it is recommended that you set the sensitivity to a larger value.
Recognition mode	Part of the object based on which the detection is performed. The options are as follows: • **Center**: An object can be detected only when its central part enters the detection area. • **Top**: An object can be detected only when its top part enters the detection area. • **Bottom**: An object can be detected only when its bottom part enters the detection area.
Detection object	Type of objects to be detected. The options include **Pedestrian**, **Motor vehicle**, and **Non-motor vehicle**. After you select a detection object type, the camera automatically reports a fast movement alarm upon detecting an object of the selected type. **NOTE:** Some camera models support detection object selection.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects fast movement only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

Table 2 Parameter description

Parameter	Description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The fast movement detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The fast movement detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.

Parameter	Description
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:** All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

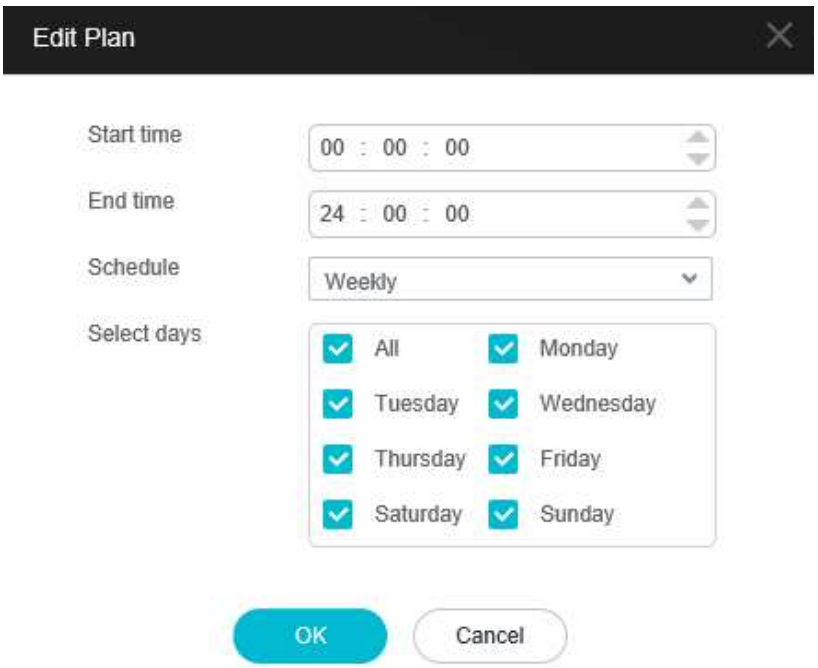
   Figure 2 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

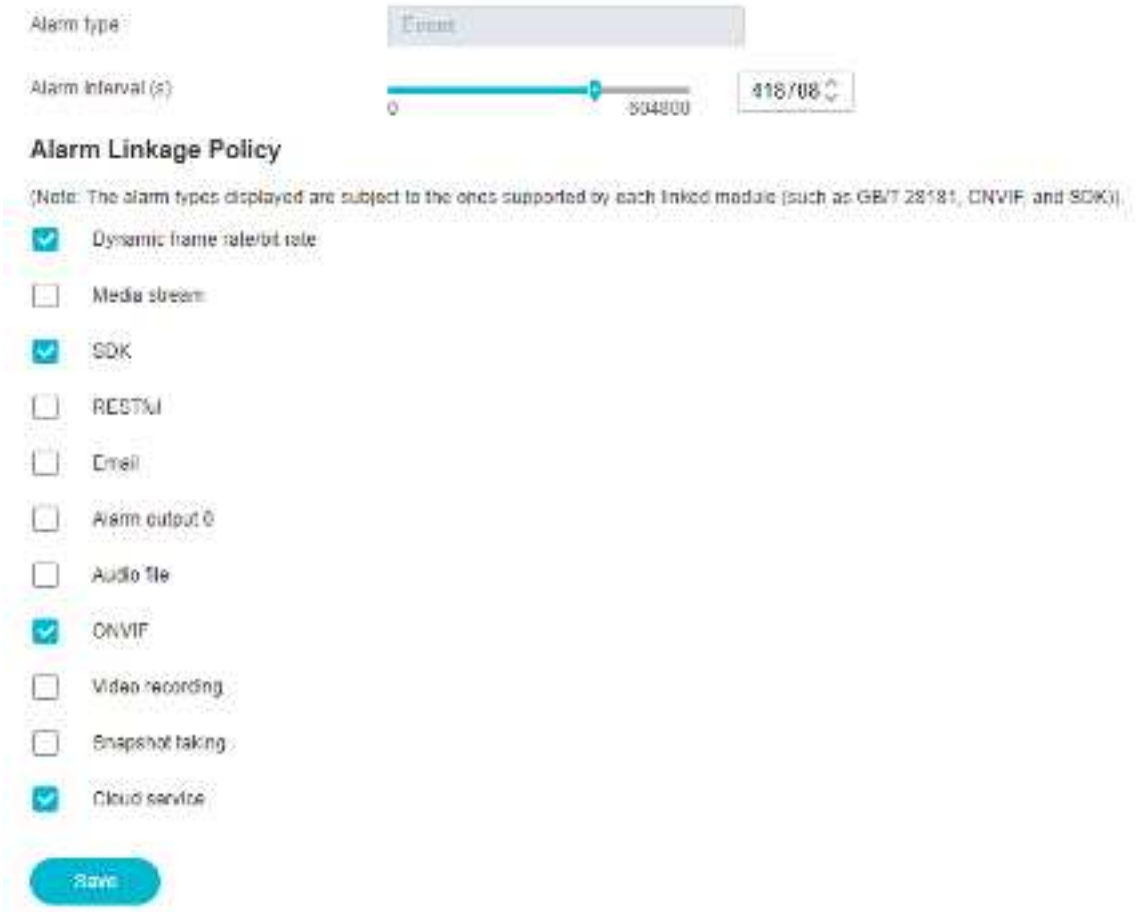
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry

Parameter	Description
	file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm**

Parameter	Description
	Output and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud

Parameter	Description
	service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When a fast moving object enters the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  NOTE

  - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
  - Some camera models do not support this method.

  1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct. The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Parking Detection

Parking detection is used to detect whether there is a vehicle whose parking duration exceeds the preset threshold in a detection area. If so, an alarm is generated. Only some camera models support this function.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Parking Detection** in the **Behavior Analysis** area. The configuration page is displayed.
3. Click the **Basic Settings** tab and set parking detection parameters.

   The web page varies between camera models.

   Figure 1 shows the page for setting parking detection parameters. Table 1 describes the parameters.

   Figure 1 Setting parking detection parameters

   Table 1 Parameter description

Parameter	Description
Sensitivity	Parking detection sensitivity. **NOTE:** • The value is an integer ranging from 1 to 100. The default value is **50**. • A larger value indicates higher sensitivity.

Parameter	Description
Parking duration threshold	Maximum duration for which a vehicle can park in the detection area. If a vehicle parks in the detection area for a period longer than the specified duration, an alarm is generated.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system performs detection only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • The parking detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:**

Parameter	Description
	• To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • The parking detection function supports a maximum of four detection areas, and all behavior analysis functions support a maximum of 10 detection areas.
Full Screen	Used to designate the entire live video image as the detection area.
No.	ID of a detection area.
Name	Name of a detection area.
Status	Status of a detection area. You can enable or disable the toggle button in the **Status** column to enable or disable a detection area.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

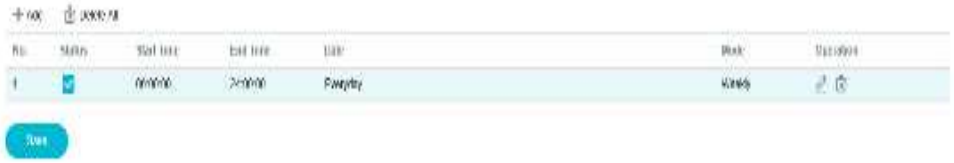
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

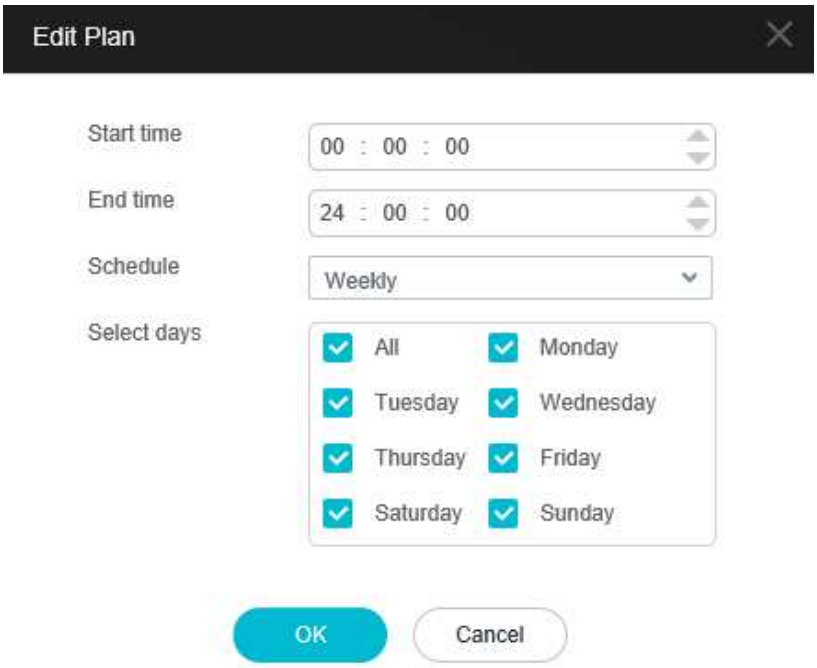
Figure 2 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click ✎ or 🗑 in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

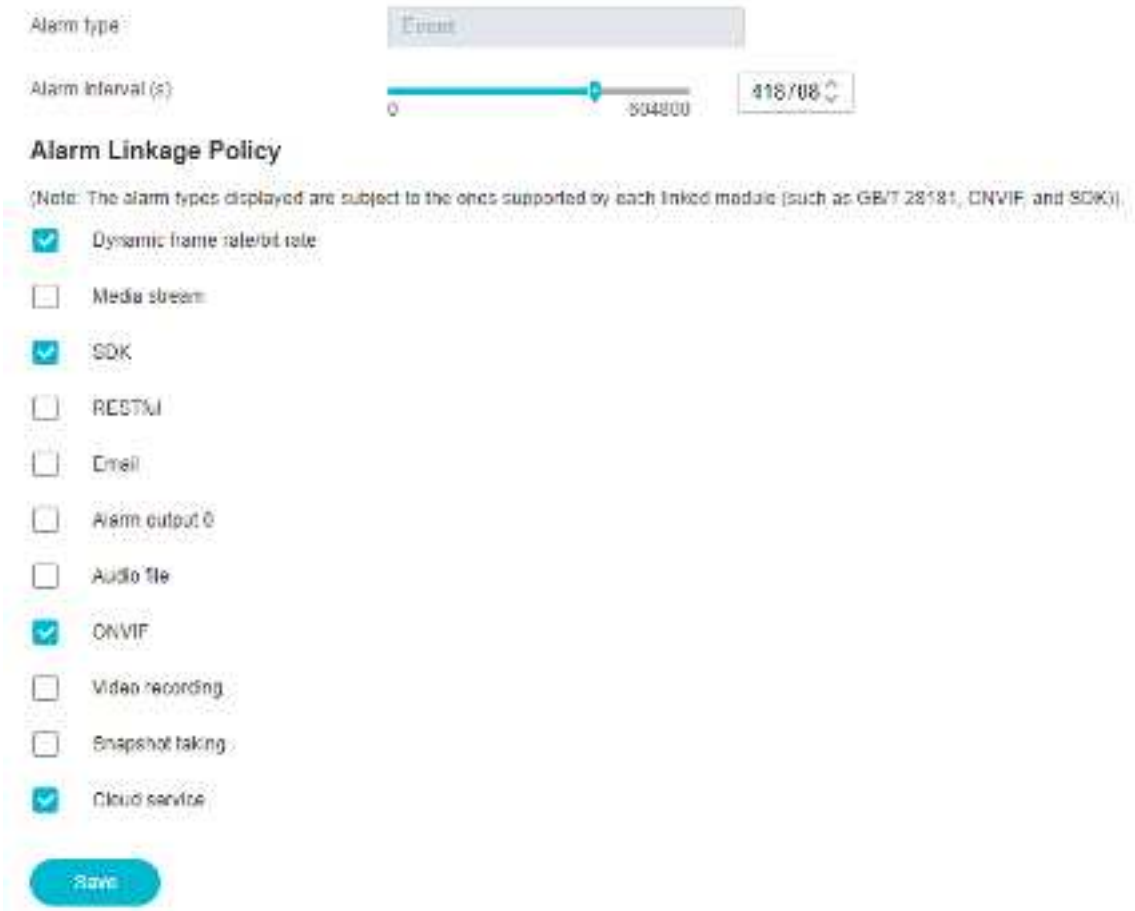
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When a vehicle is parked in the detection area for a period longer than the preset threshold, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

> NOTE
>
> - To use this method, ensure that **Send metadata** is selected on the **Perimeter Detection** page. If **Send metadata** is not selected, even if the detection is successful, the object will not be framed by a red box.
> - Some camera models do not support this method.

1. Choose **Display** > **Behavior Analysis** and click a function on the right. The function page is displayed.
2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct. The following table lists the possible incorrect configurations and their solutions.

Table 4 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Configuring Electric Bike Detection in Elevators or Corridors

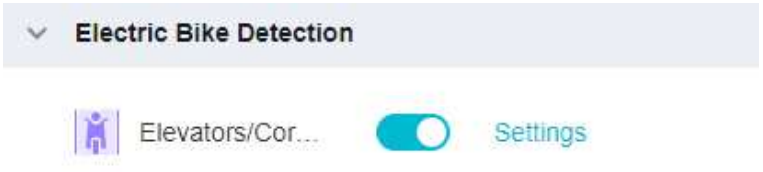
This function is used to detect whether electric bikes enter an elevator or corridor. If any electric bike is detected inside the elevator or corridor, an alarm is generated.

Setting Parameters for Electric Bike Detection in Elevators or Corridors

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence** > **Algorithm Intelligence**. Under **Electric Bike Detection**, toggle on **Elevators/Corridors**, as shown in Figure 1.

   The web page varies depending on the camera model.

   Figure 1 Electric bike detection in elevators/corridors

3. Click **Settings** next to **Elevators/Corridors**. Set detection parameters on the page that is displayed, as shown in Figure 2.

   Table 1 describes the parameters.

Figure 2 Configuring electric bike detection in elevators or corridors

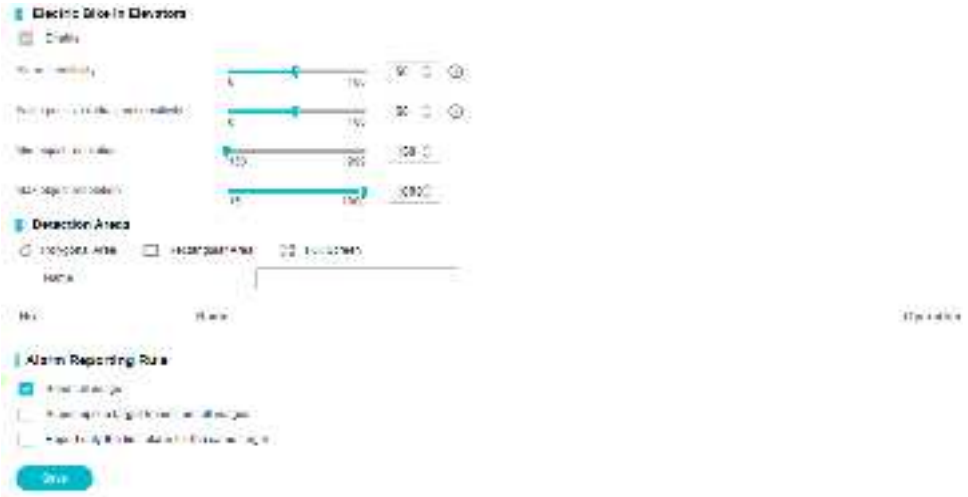


Table 1 Parameter description

Parameter	Description
Enable	Indicates whether to enable electric bike detection. This check box is selected by default and cannot be deselected.
Alarm sensitivity	Sensitivity for triggering an electric bike detection-based alarm. A lower sensitivity indicates a lower probability of triggering alarms.
False positive reduction sensitivity	Sensitivity for reducing false positives. A larger value indicates a lower false positive rate but also a lower detection rate. Set this parameter based on the site requirements.
Min object resolution	Minimum resolution in which an object can be detected on the video image. No alarm is generated when the resolution of an identified object is smaller than the value of this parameter. **NOTE:** The minimum object size supported by electric bike detection in elevators or corridors is 150 x 150 pixels (using the 1920 x 1080 video resolution as the standard).

Parameter	Description
Max object resolution	Maximum resolution in which an object can be detected on the video image. No alarm is generated when the resolution of an identified object is greater than the value of this parameter. **NOTE:** The maximum object size supported by electric bike detection in elevators or corridors is 1000 x 1000 pixels (using the 1920 x 1080 video resolution as the standard).

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system detects electric bikes only in the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

   NOTICE

   The detection area should completely cover and slightly larger than the elevator floor, as shown in Figure 3. If the detection area is too large, electric bikes outside the elevator may trigger alarms, as shown in Figure 4. If the detection area is too small, electric bikes inside the elevator may not be detected, as shown in Figure 5.

Figure 3 Example of a proper detection area



Figure 4 Example of a too large detection area



Figure 5 Example of a too small detection area



Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area.
No.	ID of a detection area.
Name	Name of a detection area.

Parameter	Description
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

5. Set the alarm reporting rule.

   Select an alarm reporting rule based on the site requirements. Table 3 describes the parameters.

   Table 3 Alarm reporting rule parameters

Parameter	Description
Send full image	Indicates whether to allow the camera to send the full image when an alarm is generated to the video security platform as common metadata.
Superimpose target frames on full images	Indicates whether to allow the camera to send the full image and object frame when an alarm is generated to the upper-level video security platform as metadata. If this check box is selected, the platform superimposes the object frame on the full image.
Report only the first alarm for the same target	Indicates whether to send only the alarm that is triggered for the first time.

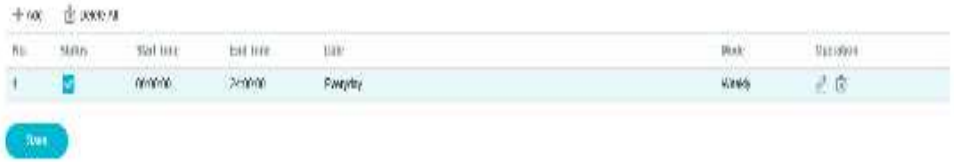
6. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 6.

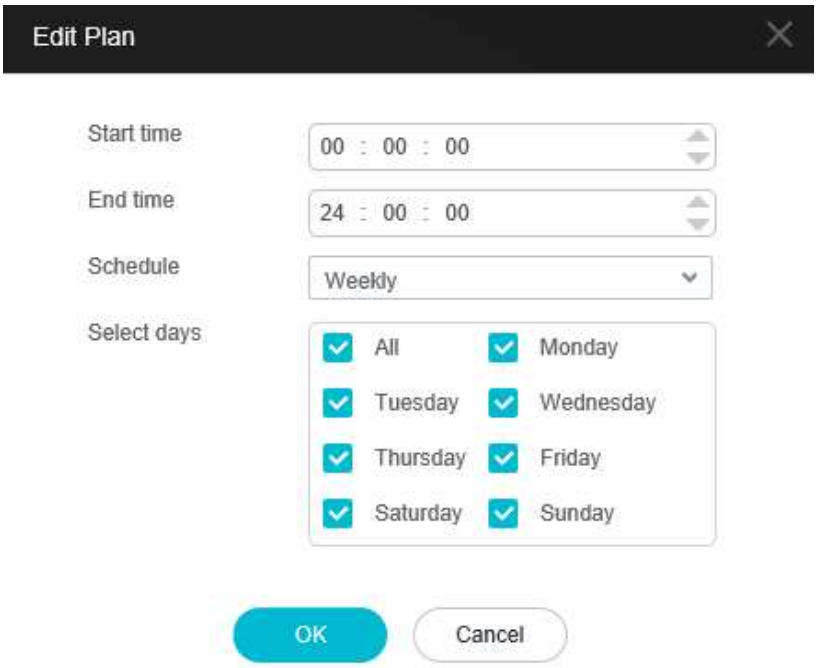
Figure 6 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 7.

   Figure 7 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

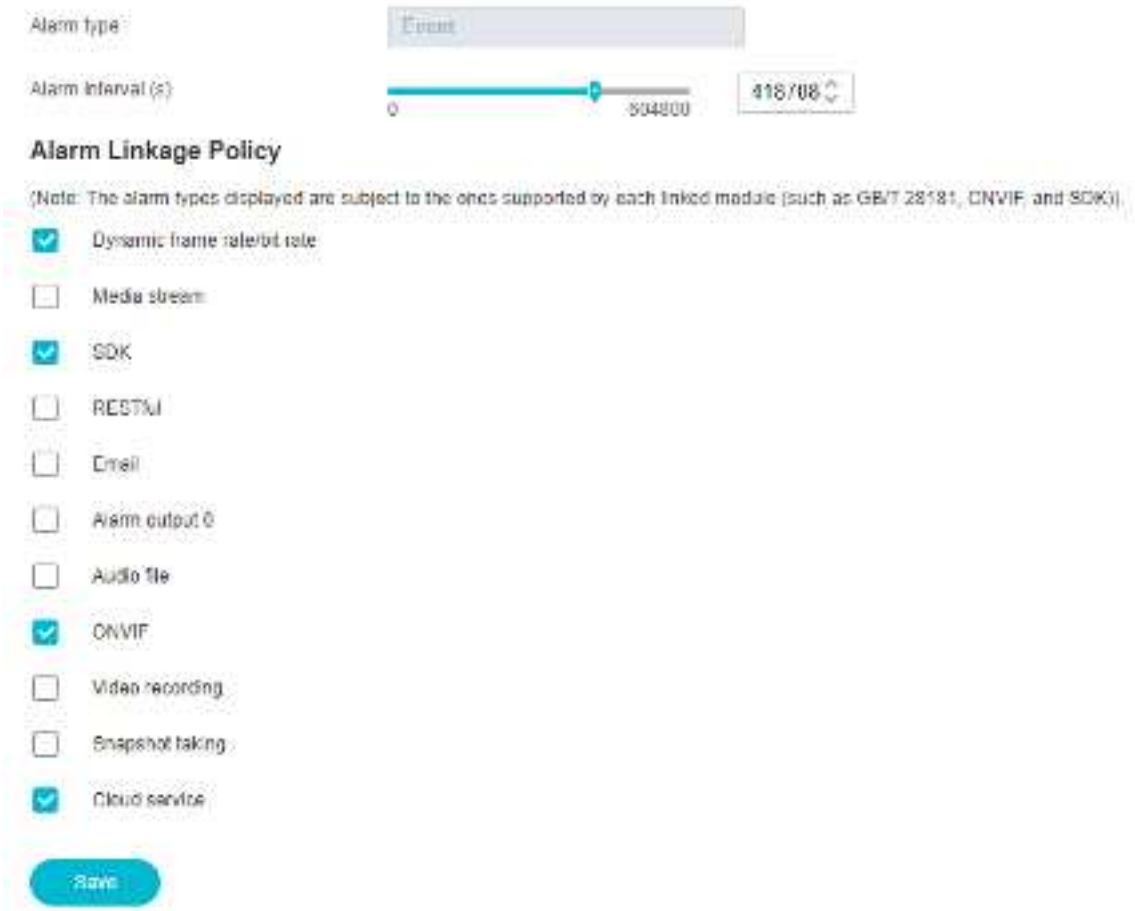
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 8.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 8 Configuring alarms



2. Set related parameters. Table 4 describes the parameters.

Table 4 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an electric bike enters the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether alarms are generated in the detection area during the detection.

- Choose **Display** > **Intelligent Detection** and check whether the object is framed by a red box. If so, the configuration is successful.

  1. Choose **Display** > **Intelligent Detection** and click a function on the right. The function page is displayed.
  2. Click **Start Metadata Reception** in the lower part of the live video pane. Check whether the object is framed by a red box. If so, the configuration is successful.

     NOTE

If a non-motorized vehicle is detected in the image, the vehicle is framed by a green box. If the box color changes to red, the object is marked as an electric bike.

If the actual verification result is different from the result described in the preceding verification method, check whether the configuration is correct. The following table lists the possible incorrect configurations and their solutions.

Table 5 Possible incorrect configurations and their solutions

Check Item	Solution
The detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the camera position (such as height, angle, and distance), focal length (for zoom cameras), and detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The detection area is disabled on the page for setting behavior analysis parameters.	Enable the toggle button in the **Status** column to enable the detection area.

Parent topic: Configuring Behavior Analysis

Checking Intelligent Analysis Results

You can check the detection results of intelligent analysis functions. The intelligent analysis functions available on the web page vary between camera models.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Behavior Analysis**.
3. Click ▶ in the lower part of the page. Then the icon changes to ■, and the live video is opened.

   Live video viewing is enabled by default.
4. Click an intelligent analysis function on the right of the page.
5. Click **Start Metadata Reception** in the lower part of the live video pane.
6. View the intelligent analysis result.

   You can also choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether intelligent analysis alarm logs are reported.

   Figure 1 Intelligent analysis result



NOTE

- The image displayed here is for reference only. The actual result displayed varies depending on the selected intelligent analysis function.
- To stop the metadata receiving function, click **Stop Metadata Reception** in the lower part of the live video pane.
- By default, received metadata are stored on the local computer. The default storage path is **C:\Users*User name*\IPC_MediaPlayer\ScenePics**. (In this path, *User name* indicates the account of the current user in the operating system.) Ensure that the available space of the system disk is greater than 200 MB. Otherwise, images will fail to be captured. To change the storage path and space size, choose **Configuration** > **Local** > **Snapshots**, and set **Intelligent snapshot save path** and **File storage size**.
- The metadata receiving function cannot be enabled on multiple tabs at a time due to browser process conflict. When you attempt to enable the metadata receiving function on multiple tabs, the message "The process of reporting target information has been started." will be displayed. In this case, you need to close unnecessary tabs and leave only one tab open or restart the browser and try again.
- Some targets may be missed during the capture due to causes such as improper image size or target angle. If the capture effect is not ideal, adjust the camera image quality, angle, and illumination for further optimization.

Parent topic: Configuring Behavior Analysis

Configuring Intelligent Vehicle Analysis

This section describes how to configure intelligent vehicle analysis and check the configuration result.

Intelligent Vehicle Analysis Features This section describes the intelligent vehicle analysis features supported by different camera models.

Configuring Intelligent Motor Vehicle Analysis
This section describes how to configure intelligent motor vehicle analysis and view configuration results. With the motor vehicle detection and capture function, a camera can detect and capture images of motor vehicles and recognize motor vehicle attributes such as the license plate type and vehicle color.

Configuring Intelligent Analysis for Object Classification
This section describes how to configure intelligent analysis for object classification and view the configuration result. The object classification function can be used to detect and capture images of motor vehicles, non-motorized vehicles, and pedestrians.

Configuring Intelligent Vehicle Event Analysis
Vehicle event detection includes detection of non-motorized vehicles driving in motor vehicle lanes, motor vehicles driving in non-motorized vehicle lanes, parking violations, wrong-way driving, illegal backing, and marked lane violations.

Configuring Intelligent Traffic Flow Analysis
This section describes how to configure traffic flow statistics and view statistical results as well as configure traffic congestion detection to obtain vehicle traffic in specified time periods to prevent traffic congestions.

Configuring a Video-based Vehicle Detector
Cameras can detect vehicles that appear in a specified period and in specified lanes and report information about vehicles that enter or leave a specified detection area to the connected video-based vehicle detector platform. You can adjust the traffic light

duration based on the vehicle information to improve traffic efficiency.

Parent topic: Intelligent Settings

Intelligent Vehicle Analysis Features

This section describes the intelligent vehicle analysis features supported by different camera models.

Different camera models support different intelligent vehicle analysis features. The following table describes the differences.

Table 1 Intelligent vehicle analysis features

Device Model	Motor Vehicle Detection	Object Classification	Vehicle Event Detection	Traffic Flow Statistics	Passing Vehicle Detection (Video-based Vehicle Detector)	Image Combination	Text Overlay	Vehicle Recognition
HWT-D6550-10-Z33-SV	YES	YES	YES	YES	YES	YES	YES	YES
HWT-D2122-10-SIU	YES	YES	NO	NO	NO	YES	YES	NO
HWT-D2152-10-SIU	YES	YES	NO	NO	NO	YES	YES	NO
HWT-D3222-10-SIU	YES	YES	NO	NO	NO	YES	YES	NO
HWT-D3252-10-SIU	YES	YES	NO	NO	NO	YES	YES	NO
HWT-D3040-10-ELI-PV (2.8 mm)	NO	NO	NO	NO	NO	NO	YES	NO

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring Intelligent Motor Vehicle Analysis

This section describes how to configure intelligent motor vehicle analysis and view configuration results. With the motor vehicle detection and capture function, a camera can detect and capture images of motor vehicles and recognize motor vehicle attributes such as the license plate type and vehicle color.

Configuring Motor Vehicle Capture To enable the camera to recognize license plates, enable motor vehicle capture first and set related parameters.

Viewing Configuration Results

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring Motor Vehicle Capture

To enable the camera to recognize license plates, enable motor vehicle capture first and set related parameters.

Prerequisites

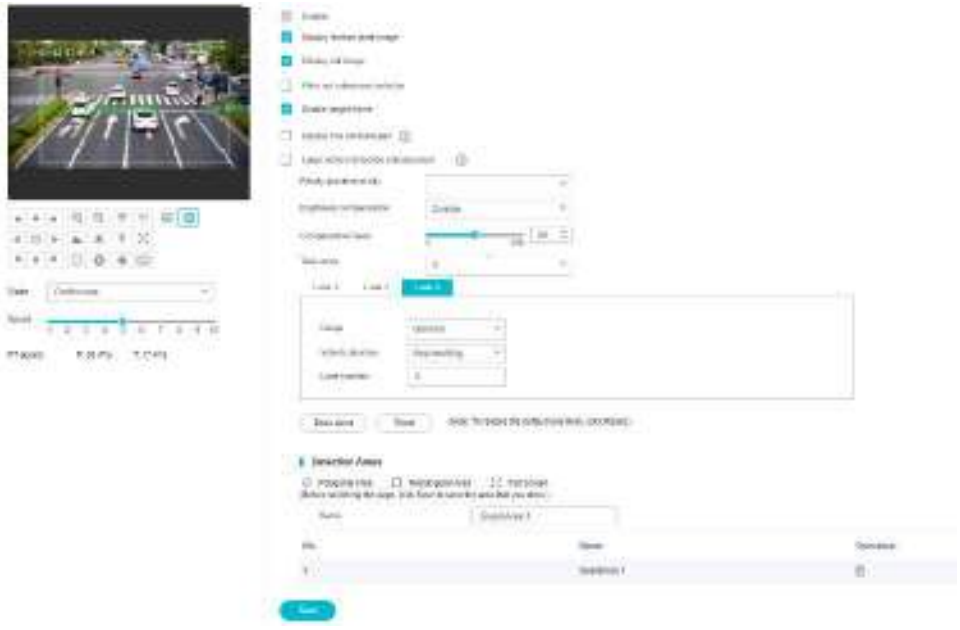
The target detection, head counting, object classification, and intelligent alarm functions have not been enabled.

The web page varies depending on the camera model.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Motor Vehicle Capture** in the **Vehicle Intelligence** area. Click **Settings** next to **Motor Vehicle Capture**. The **Motor Vehicle Capture** page is displayed, as shown in Figure 1.

   Figure 1 Motor Vehicle Capture page

3. Set motor vehicle capture parameters. For details about the parameters, see Table 1.

   Table 1 Motor vehicle capture parameters

Parameter	Description	How to Set
Display license plate image	Indicates whether to display the license plate image when real-time image capture is enabled on the **Intelligent Detection** page.	Select the check box.
Display full image	Indicates whether to display the full image when real-time image capture is enabled on the **Intelligent Detection** page.	Select the check box.
Filter out unlicensed vehicles	Indicates whether to filter out vehicles without license plates.	Select the check box.
Enable target frame	Indicates whether to frame detected objects in captured images.	Select the check box.
Display five vehicle types	Indicates whether to classify all detected vehicles into the following five types: car, bus, van, heavy and medium truck, and light truck.	Select the check box.
Large vehicle detection enhancement	You are advised to enable this function after the video-based vehicle detector function is enabled. After this function is enabled, you can set **Detection enhancement coefficient**. A larger	Select the check box.

Parameter	Description	How to Set
	coefficient indicates a higher probability of detecting large vehicles. However, a few number of false snapshots may also be generated.	
Priority province or city	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province or city name abbreviation can be configured.	Select a value from the drop-down list box.
Brightness compensation	Brightness compensation for captured license plate images with too high or too low brightness.	Select **Enable** or **Disable** from the drop-down list box.
Compensation level	This parameter is available only when **Brightness compensation** is set to **Enable**. A higher compensation level indicates a larger degree for increasing or decreasing the license plate brightness.	Drag the slider bar to set the value.
Total lanes	Number of lanes in which license plates can be captured.	Select a value from the drop-down list box. The corresponding lanes are displayed on

Parameter	Description	How to Set
		the preview image on the left. To adjust the lanes, click **Draw Lines**.
Usage	Indicates whether the current lane is a common vehicle lane or a non-motorized vehicle lane, which is used to support the function of detecting motor vehicles driving in non-motorized vehicle lanes or non-motorized vehicles driving in motor vehicle lanes.	Select a value from the drop-down list box.
Vehicle direction	Regulated driving direction of the current road, which is used to support the function of detecting wrong-way driving or illegal backing.	Select a value from the drop-down list box.

4. Click **Draw Lines**, as shown in Figure 2.

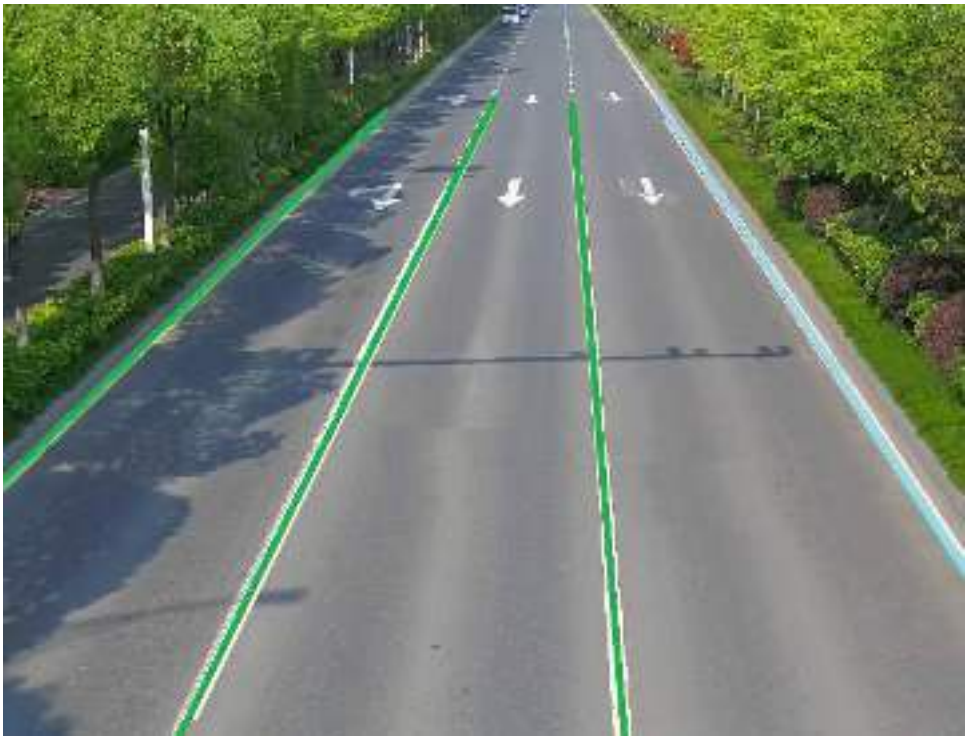
   Draw lane lines: Adjust the green lane lines and blue right boundary line in the preview image on the left to enable the lane lines to coincide with the actual lane lines. If lane lines cross with each other, settings will fail to be saved.

NOTE

- You can double-click the preview image to view it in full-screen mode to facilitate lane line drawing. After the drawing operation is complete, you can press **Esc** to exit the full-screen mode.

- When the mouse pointer is in the middle of a lane line, you can drag the entire line. When the mouse pointer is at an end of a lane line, you can adjust the position of the two ends and the lane length.

Figure 2 Drawing lines



5. Draw a detection area.

   The camera will detect vehicles and license plates only in the detection area. The license plate capture position is in the lower middle part of the image and is not related to the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area.

Parameter	Description
	NOTE: • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

6. Click **Save**.

   Basic parameters for motor vehicle capture have been set.

Configuring Text Overlay

Text overlay allows you to superimpose information such as the capture time, license plate characters, and vehicle type on snapshots. For details about how to set the language of text to be superimposed, see Managing the System.

NOTE

The text overlay function is not applicable to vehicle event detection.

1. On the **Motor Vehicle Capture** page, click **Text Overlay**, as shown in Figure 3.
2. Set text overlay parameters based on the site requirements. For details about the parameters, see Table 3. The parameters vary depending on the camera model.

Figure 3 Setting text overlay parameters

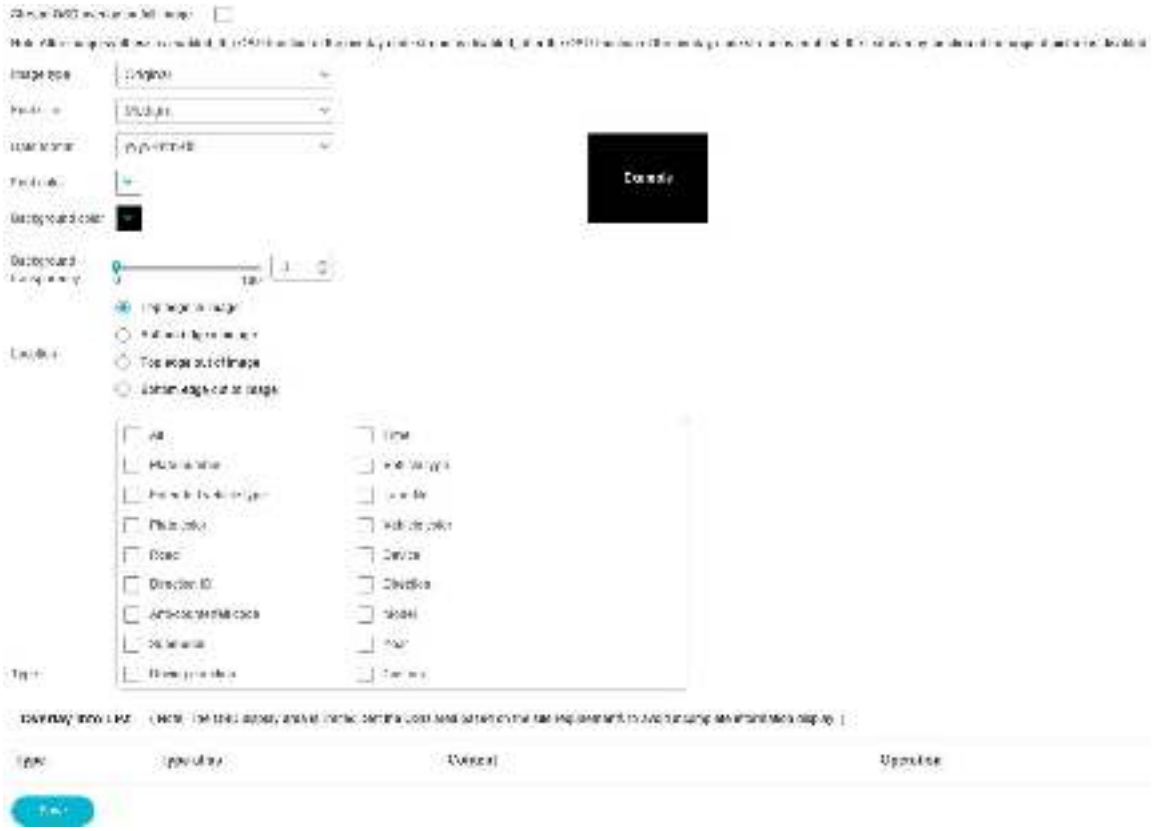


Table 3 Text overlay parameters

Parameter	Description
Stream OSD overlay on full image	• If you select this check box, only information set under **Configuration** > **Image** > **OSD** will be superimposed on full images uploaded. • If you deselect this check box, only information set under **Text Overlay** > **Overlay Info List** will be superimposed on full images uploaded. **NOTE:**

Parameter	Description
	This function does not take effect when image combination is enabled.
Image type	Type of the image where text will be superimposed. • **Original**: Superimpose text on original full images. • **Synthesis**: Superimpose text on the combined images.
Font size	Font size of the text to be superimposed.
Font color	Color of the text to be superimposed. In addition to common colors, you can customize colors.
Date format	Date format, for example, **yyyy-mm-dd**. Select a date format from the drop-down list box based on the site requirements.
Background color	Background color of the text to be superimposed. In addition to common colors, you can customize colors.
Background transparency	Transparency of the background.
Location	Position where the text is to be superimposed.
Type	• The overlay information supported by cameras may vary. • After the desired types are selected, you need to manually set information to be superimposed in the text boxes corresponding to the selected parameters, such as **Road**, **Device**, **Direction ID**, **Direction**, and **Custom**. The information that can be manually set for text overlay varies depending on the camera model. **NOTE:** • You can select the check box in the **Type alias** column corresponding to an information type and rename it, as shown in Figure 4.

Parameter	Description
	• The value of **Time** is accurate to seconds by default. After **Accurate to milliseconds** is selected, the capture time is accurate to milliseconds. • After **Anti-counterfeit code** is selected, a 32-bit anti-counterfeit code will be displayed on the image. • You can click and to adjust the sequence of superimposed texts.
Snapshot Test	You can click **Snapshot Test** to take a vehicle snapshot and view the text overlay effect. **NOTE:** • This function is applicable only to micro checkpoint cameras. For micro checkpoint cameras, the service of vehicle detection at entrances and exits does not support snapshot test. • Before clicking **Snapshot Test**, ensure that motor vehicle detection is enabled. • Snapshots are stored in **C:\users\IPC_MediaPlayer\ScenePics*IP address*\ManualPic** by default.

Figure 4 Overlay information list



NOTE

If **Image type** is set to **Original**, the text overlay items described in Table 3 will also appear in the original snapshots of a combined

Viewing Configuration Results

Prerequisites

You have set motor vehicle capture parameters. For details, see Configuring Motor Vehicle Capture.

Viewing Motor Vehicle Snapshots

After the real-time capture function is enabled, you can view the captured vehicle information in real time on the **Intelligent Detection** page.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Intelligent Detection**. Click . On the **Detection Area** tab page, select **Snapshot list** under **Detection Type**, and click **OK**.
3. Click **Enable Real-time Capture**. When a vehicle is captured, the vehicle information is displayed in the **Snapshot list**, as shown in Figure 1.

   Figure 1 Snapshot list



NOTE

- If the license plate color is monochrome, the **Plate color** in the vehicle information list is monochrome. For example, if the license plate color is blue, the recognized license plate color is blue. If the license plate color is gradient, the **Plate color** in the vehicle information list is displayed as the

gradient color. For example, the color of a new-energy license plate is gradient green.

- If the real-time capture function is enabled, captured images will be saved to the local computer. The default storage path is **C:\Users\User name\IPC_MediaPlayer\ScenePics**. Ensure that the available space of the system disk for storage is greater than 200 MB. Otherwise, images will fail to be captured.

Parent topic: Configuring Intelligent Motor Vehicle Analysis

Configuring Intelligent Analysis for Object Classification

This section describes how to configure intelligent analysis for object classification and view the configuration result. The object classification function can be used to detect and capture images of motor vehicles, non-motorized vehicles, and pedestrians.

Configuring Object Classification

Viewing Object Classification Results

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring Object Classification

The camera's object classification function detects motor vehicles, non-motorized vehicles, and pedestrians in images, uploads snapshots to the video security platform as metadata, or sends emails containing the snapshots through SMTP.

Prerequisites

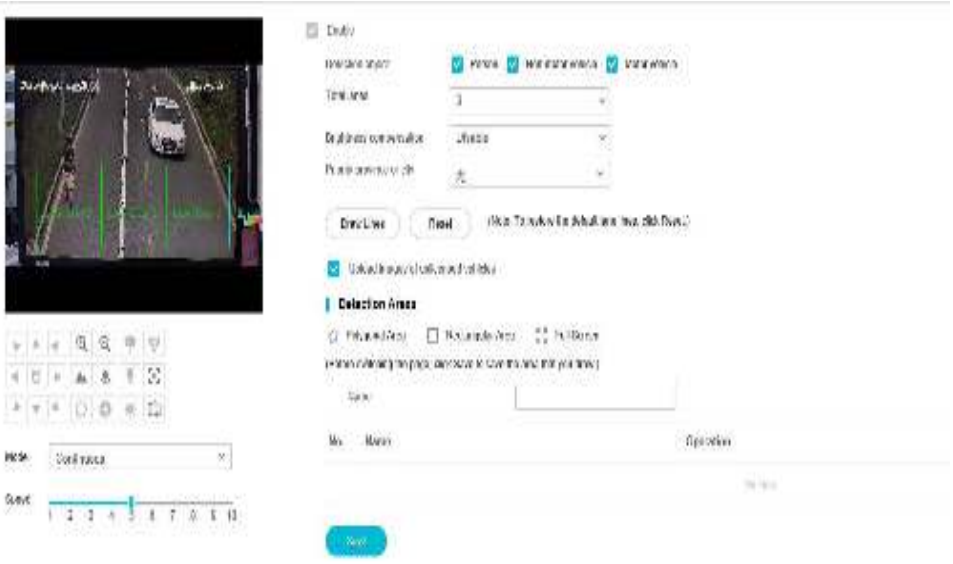
Motor vehicle snapshot and target detection have been disabled.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Object Settings** in the **Vehicle Intelligence** area. Click **Settings** next to **Object Settings**. The **Object Settings** page is displayed, as shown in Figure 1.

   The actual web page varies depending on the camera model.

   Figure 1 Object Settings page

3. Set object classification parameters. Table 1 describes the parameters.

   Table 1 Parameter description

Parameter	Description	How to Set
Enable	Indicates whether to enable the object classification function.	Select the check box.
Detection object	The options include **Person**, **Non-motor vehicle**, and **Motor vehicle**. After a detection object type is selected, the camera takes snapshots of such objects detected.	Select the check box.
Brightness compensation	Brightness compensation for captured license plate images with too high or too low brightness.	Select **Enable** or **Disable** from the drop-down list box.
Compensation level	This parameter is available only when **Brightness compensation** is selected. You can increase the value of the parameter when the environment is dark.	Drag the slider bar to set the value.
Priority province or city	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province or city name abbreviation can be configured.	Select a value from the drop-down list box.
Upload images of unlicensed vehicles	Indicates whether to enable the function of uploading images of unlicensed vehicles.	Select the check box.

NOTE

If the snapshot effect is not ideal, you can choose **Configuration** > **Image** > **Display** > **Backlight** and set **WDR/HLC/BLC** to **Backlight adaptation**.

4. Click **Draw Lines**. On the preview image that is displayed on the left, adjust the green lane lines to make them overlap the actual lane lines. Ensure that the lane lines do not cross each other, or the lane lines will fail to be saved. Figure 2 shows the lane line drawing page.

> **NOTE**
>
> - You can double-click the preview image to view it in full-screen mode to facilitate lane line drawing. After the drawing operation is complete, you can press **Esc** to exit the full-screen mode.
> - When the mouse pointer is in the middle of a green lane line, you can drag the entire line. When the mouse pointer is at an end of a green lane line, you can adjust the position of the two ends and the lane length.

Figure 2 Drawing lane lines



5. Draw a detection area.

   You need to draw a detection area based on the site requirements. The camera will capture images of motor vehicles, non-motorized vehicles, and pedestrians only in the detection area. The capture

position is not related to the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

NOTE

Currently, you can draw only one detection area at a time. Before drawing a detection area again, you need to delete the original one. If no detection area is drawn, the camera will capture images of motor vehicles, non-motorized vehicles, and pedestrians in the entire live video image.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again.

Parameter	Description
	• You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

6. Click **Save**.

   The object classification function is configured.

Configuring Text Overlay

Text overlay allows you to superimpose information such as the capture time, license plate characters, and vehicle type on snapshots. For details about how to set the language of text to be superimposed, see Managing the System.

NOTE

The text overlay function is not applicable to vehicle event detection.

1. On the **Object Settings** page, click **Text Overlay**. The page shown in Figure 3 is displayed.
2. Set text overlay parameters based on the site requirements. Figure 4 describes the parameters. The parameters vary depending on the camera model.

Figure 3 Text Overlay page

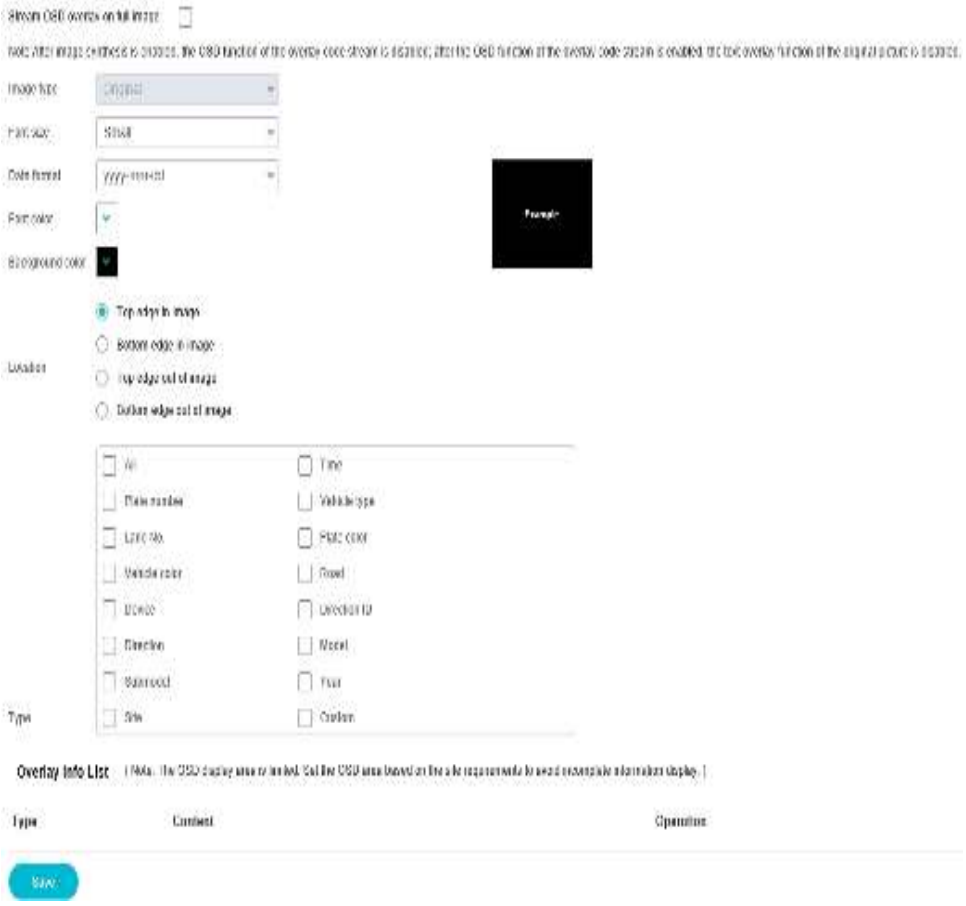


Table 3 Parameter description

Parameter	Description
Stream OSD overlay on full image	• If you select this check box, only information set under **Configuration** > **Image** > **OSD** will be superimposed on full images uploaded. • If you deselect this check box, only information set under **Text Overlay** > **Overlay Info List** will be superimposed on full images uploaded. **NOTE:** This function does not take effect when image combination is enabled.
Image type	Type of the image where text will be superimposed.

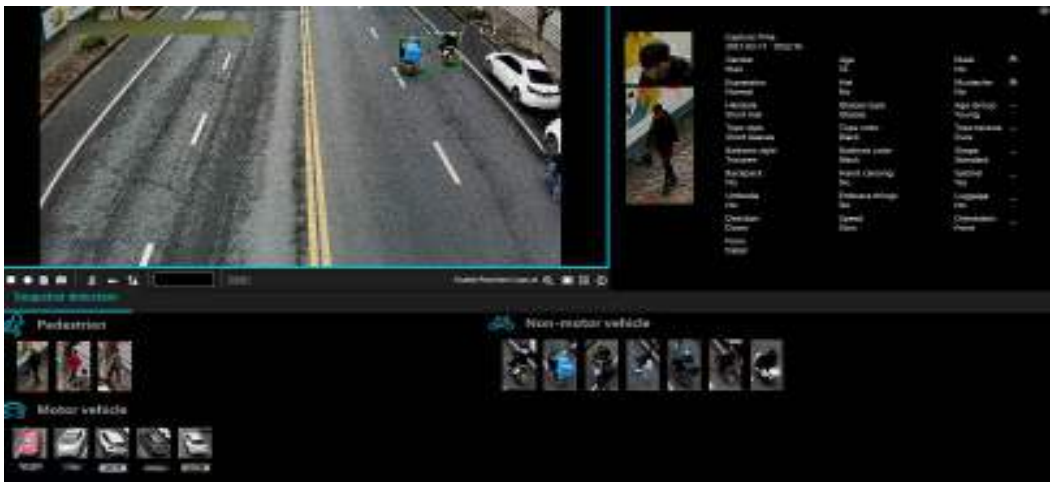
Parameter	Description
	• **Original**: Superimpose text on original full images.
Font size	Font size of the text to be superimposed.
Font color	Color of the text to be superimposed. In addition to common colors, you can customize colors.
Date format	Date format, for example, **yyyy-mm-dd**. Select a date format from the drop-down list box based on the site requirements.
Background color	Background color of the text to be superimposed. In addition to common colors, you can customize colors.
Location	Position where the text is to be superimposed.
Type	• The overlay information supported by cameras may vary. • After the desired types are selected, you need to manually set information to be superimposed in the text boxes corresponding to the selected parameters, such as **Road**, **Device**, **Direction ID**, **Direction**, and **Custom**. The information that can be manually set for text overlay varies depending on the camera model. **NOTE:** • You can select the check box in the **Type alias** column corresponding to an information type and rename it, as shown in Figure 4. • The value of **Time** is accurate to seconds by default. After **Accurate to milliseconds** is selected, the capture time is accurate to milliseconds. • You can click and to adjust the sequence of texts to be superimposed.

Viewing Object Classification Results

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Object Classification** and click ⚙ in the upper right corner of the page. On the **Detection Area** tab page, select **Person detection**, **Motor vehicle detection**, and **Non-motorized vehicle detection** in the **Detection Content** area.
3. Click **Enable Real-time Capture** in the lower part of the video pane. View captured images in the area below the video pane. If motor vehicles, non-motorized vehicles, and pedestrians are displayed by category, as shown in Figure 1, the object classification parameters are set successfully. Here, a camera of a specified model is used as an example.

> **NOTE**
>
> - Some camera models that support object classification do not support personal attribute recognition or cyclist attribute recognition. Therefore, for such cameras, only captured motor vehicle images and recognized motor vehicle attributes are available. The actual web page may vary between camera models.
> - To view personal and cyclist attribute recognition results, you need to select **Enable personal attribute recognition** and **Enable cyclist attribute recognition** on the **Attribute Recognition** page first. For details, see Configuring Attribute Recognition.
> - The object classification does not support target recognition. To view object classification results, do no select **Target match success** and **Target match failure** on the **Recognition Area** tab page.

Figure 1 Captured object images



NOTE

- To disable the real-time capture function, click **Disable Real-time Capture** in the lower part of the video pane.
- After the real-time capture function is disabled, the camera stops displaying the captured object images in real time, but still classifies objects and saves the classification results based on the object classification plan.
- By default, the captured images are stored on the local computer. The default storage path is **C:\Users*User name*\IPC_MediaPlayer\ScenePics**. Ensure that the available space of the system disk for storage is greater than 200 MB. Otherwise, images will fail to be captured.
- Some objects may be missed during the capture due to causes such as improper image sizes or object angles. If the capture effect is not ideal, adjust the camera image quality, angle, and illumination for further optimization.

Parent topic: Configuring Intelligent Analysis for Object Classification

Configuring Intelligent Vehicle Event Analysis

Vehicle event detection includes detection of non-motorized vehicles driving in motor vehicle lanes, motor vehicles driving in non-motorized vehicle lanes, parking violations, wrong-way driving, illegal backing, and marked lane violations.

The actual web page varies depending on the camera model.

NOTE

- Adjust site survey for vehicle event detection based on the site requirements. For example, to detect motor vehicles driving in non-motorized vehicle lanes, the camera's live view should cover both the non-motorized vehicle lane and motor vehicle lane.
- If vehicle event detection is required, it is recommended that the shutter speed be set to 1/250s.

Configuring Parking Violation Detection

Configuring Detection of Non-Motorized Vehicles Driving in Motor Vehicle Lanes

Configuring Detection of Motor Vehicles Driving in Non-Motorized Vehicle Lanes

Configuring Detection of Wrong-Way Driving or Illegal Backing

Configuring Marked Lane Violation Detection

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring Parking Violation Detection

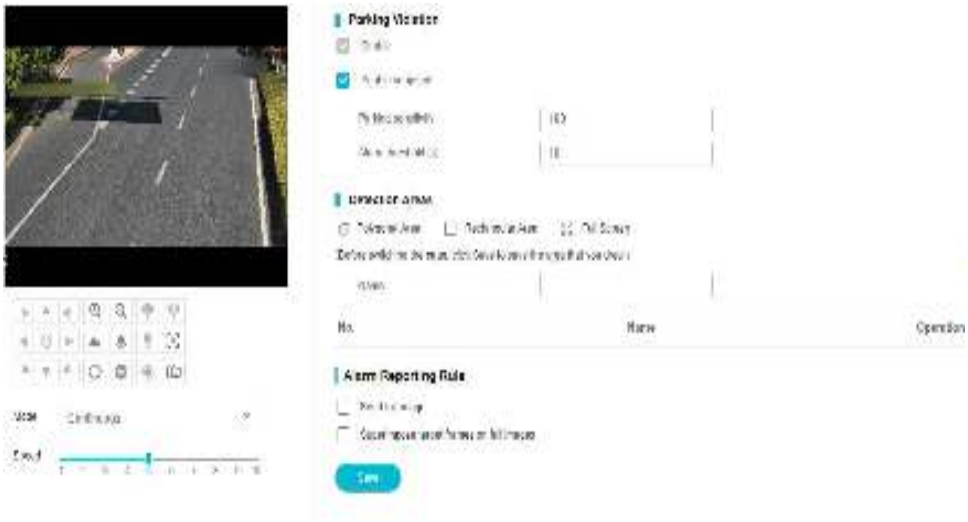
Prerequisites

You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Parking Violation** in the **Vehicle Intelligence** area. Click **Settings** next to **Parking Violation**. The **Parking Violation** page is displayed, as shown in Figure 1.

   Figure 1 Parking Violation page

3. Set parking violation detection parameters. Table 1 describes the parameters.

   Table 1 Parameters for parking violation detection

Parameter	Description
Enable snapshot	Indicates whether to enable snapshot taking upon detecting parking violations. **NOTE:**

Parameter	Description
	• Before enabling snapshot taking, ensure that the FTP/SFTP server is configured. • Snapshots are stored on the FTP/SFTP server.
Parking sensitivity	Sensitivity for determining whether a motor vehicle is moving. A larger value indicates higher sensitivity. **NOTE:** If this parameter is set to a larger value, when a motor vehicle moves slightly, the system regards the motor vehicle as moving, not parking. You can set this parameter based on the site requirements.
Alarm threshold (s)	An alarm is triggered only when the vehicle stay duration exceeds the value of this parameter.

4. Draw a detection area.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the

Parameter	Description
	pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

5. Set alarm reporting rule parameters. Table 1 describes the parameters.

   Table 3 Alarm reporting rule parameters

Parameter	Description
Send full image	Indicates whether to allow the camera to send the full image to the video security platform as general metadata when an alarm is generated.
Superimpose target frames on full images	Indicates whether to superimpose the target frame on the full image captured by the camera when an alarm is generated.

6. Click **Save**. The parking violation detection is configured.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab. The tab page shown in Figure 2 is displayed.

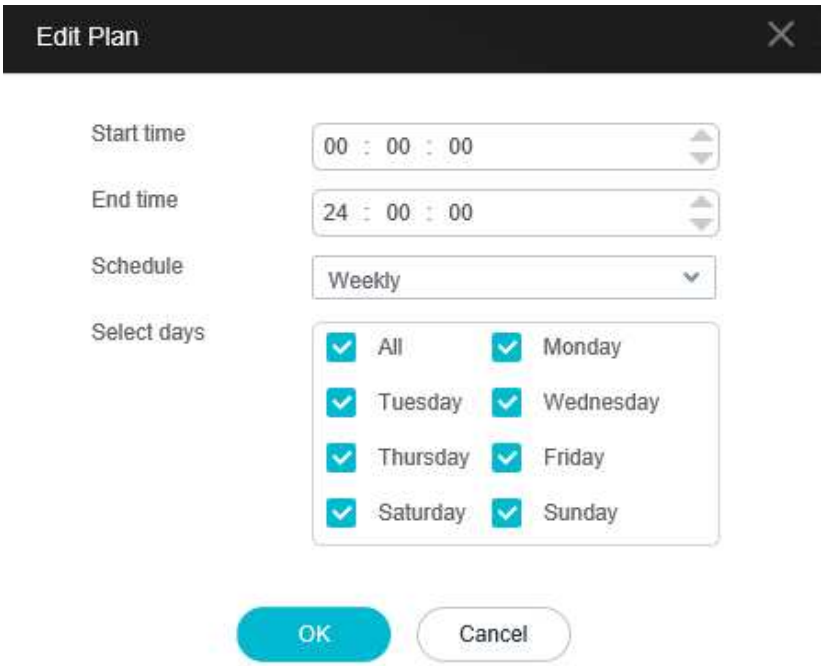
Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

NOTE

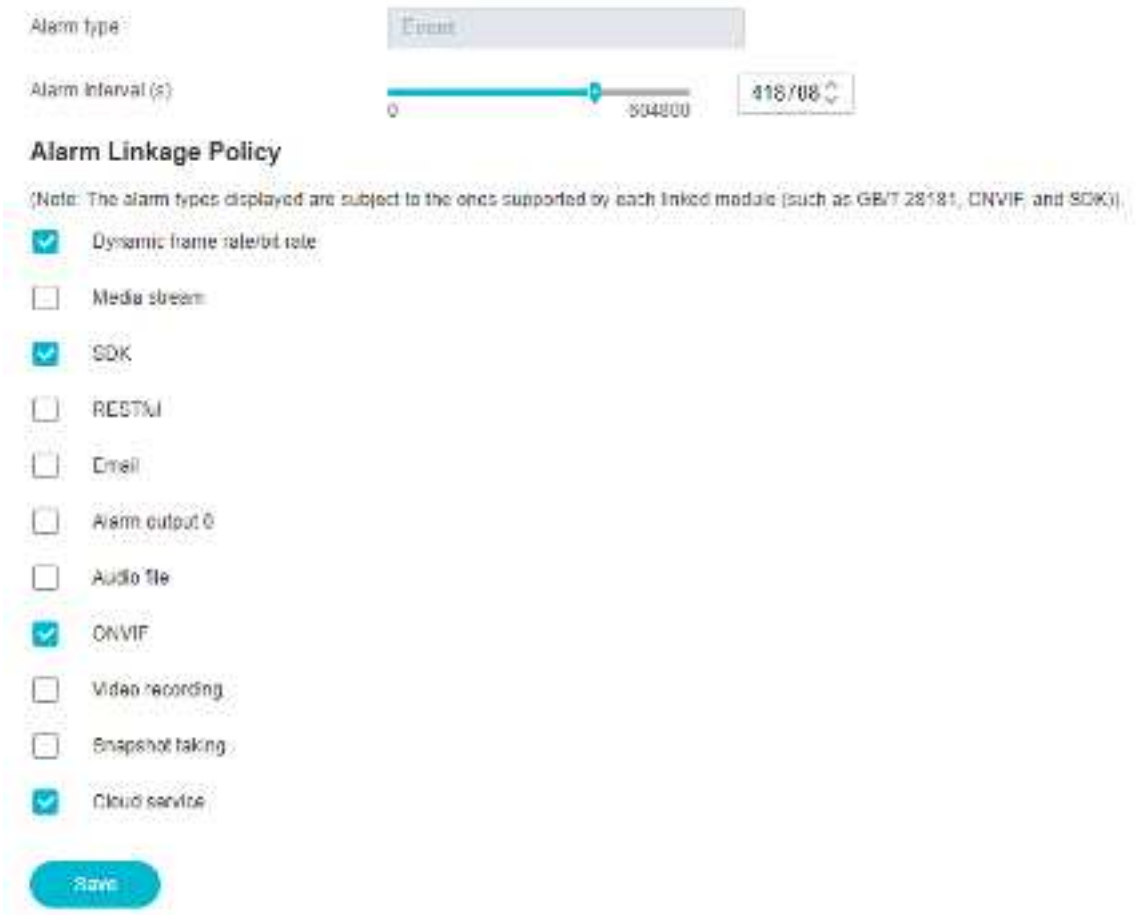
- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 4 describes the parameters.

Table 4 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service.

Parameter	Description
	NOTE: The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a

Parameter	Description
	warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light

Parameter	Description
	illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When a parking violation occurs in the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

- Check whether snapshots are taken for parking violations. If so, the configuration is successful.

  On the page for configuring parking violation detection, select **Enable snapshot**. When specified behavior is detected, the camera will automatically take snapshots.

  1. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP** and enable FTP.
  2. Set **FTP attribute** to **Micro checkpoint**.
  3. View snapshots taken for parking violations on the FTP server.

Figure 5 Viewing snapshots



Parent topic: Configuring Intelligent Vehicle Event Analysis

Configuring Detection of Non-Motorized Vehicles Driving in Motor Vehicle Lanes

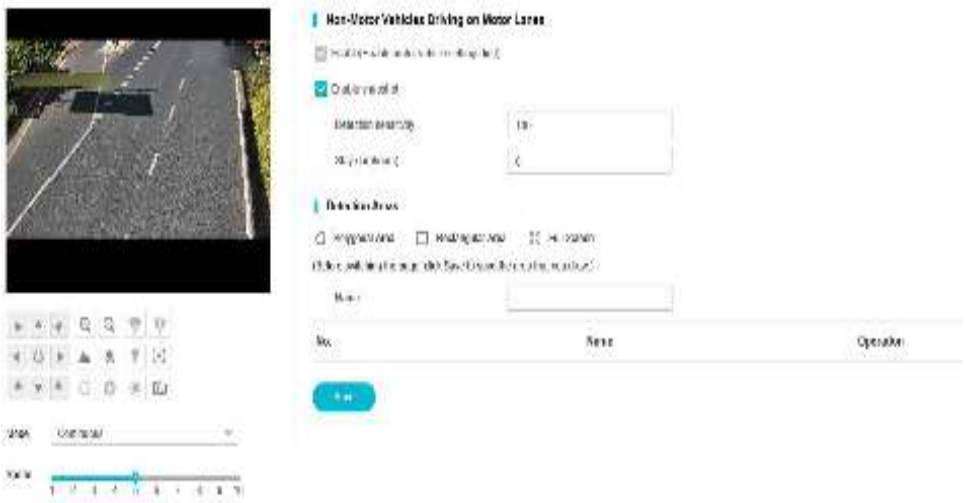
Prerequisites

- You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.
- You have set the lane attributes for detecting non-motorized vehicles driving in motor vehicle lanes. For details, see Procedure.

Setting Parameters for Detecting Non-Motorized Vehicles Driving in Motor Vehicle Lanes

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Non-Motorized Vehicles in Motor Vehicle Lanes** in the **Vehicle Intelligence** area. Click **Settings** next to **Non-Motorized Vehicles in Motor Vehicle Lanes**. The **Non-Motorized Vehicles in Motor Vehicle Lanes** page is displayed, as shown in Figure 1.

   Figure 1 Configuring detection of non-motorized vehicles driving in motor vehicle lanes

3. Set parameters for detecting non-motorized vehicles driving in motor vehicle lanes. Table 1 describes the parameters.

Table 1 Parameters for detecting non-motorized vehicles driving in motor vehicle lanes

Parameter	Description
Enable snapshot	Indicates whether to enable snapshot taking upon detecting non-motorized vehicles driving in motor vehicle lanes. **NOTE:** • Before enabling snapshot taking, ensure that the FTP/SFTP server is configured. • Snapshots are stored on the FTP/SFTP server.
Detection sensitivity	Sensitivity for determining whether a non-motorized vehicle occupies the motor vehicle lane. A larger value indicates a higher sensitivity. **NOTE:** If this parameter is set to a larger value, a non-motorized vehicle that is partially in the motor vehicle lane is regarded as occupying the motor vehicle lane. You can set this parameter based on the site requirements.
Stay duration(s)	Maximum duration during which a non-motorized vehicle occupies the motor vehicle lane. Only when the duration exceeds the value of this parameter, an alarm is triggered.

4. Draw a detection area.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area.

Parameter	Description
	NOTE: • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

5. Click **Save**. The function of detecting non-motorized vehicles driving in motor vehicle lanes is configured.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab. The tab page shown in Figure 2 is displayed.

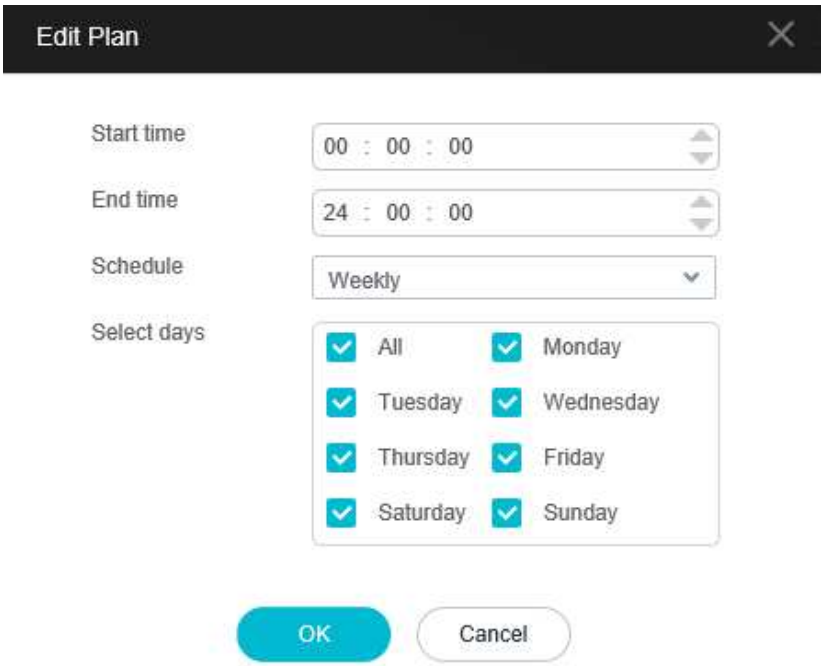
Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

NOTE

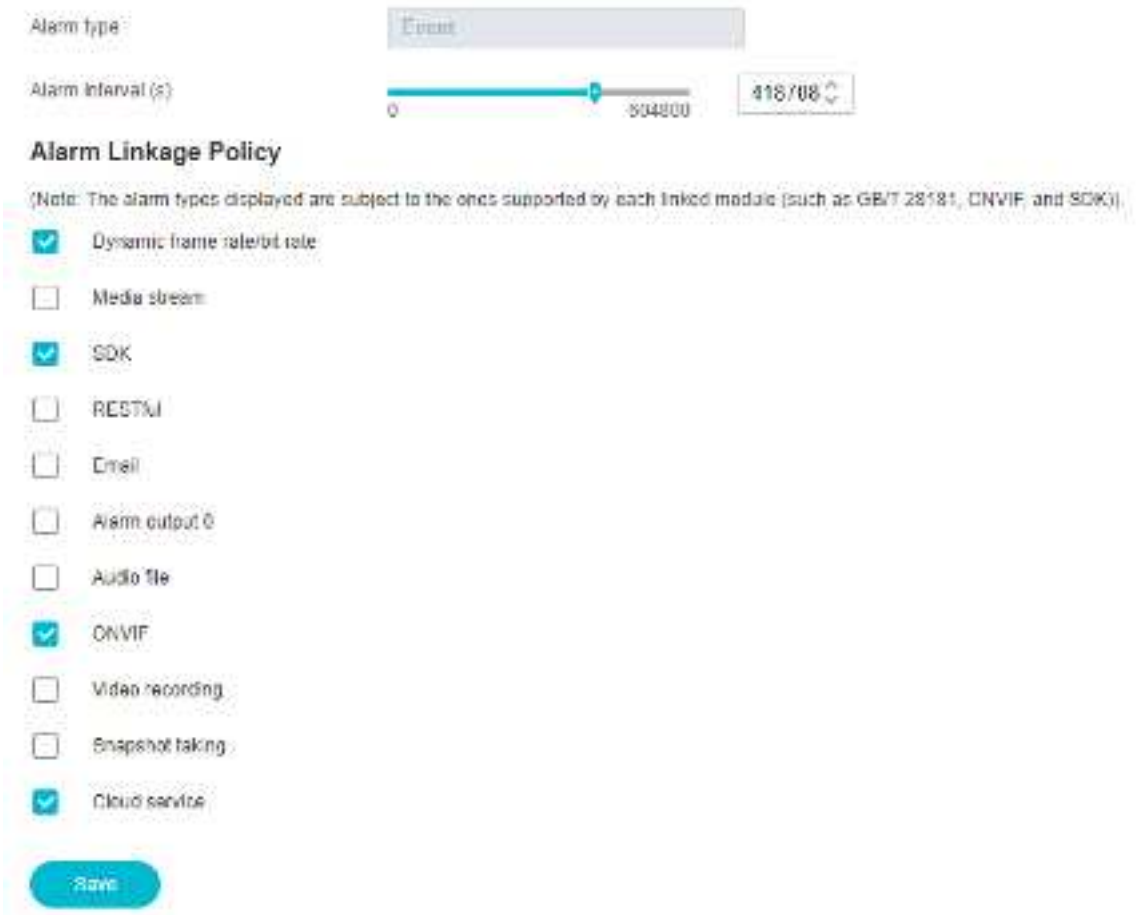
- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service.

Parameter	Description
	NOTE: The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a

Parameter	Description
	warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light

Parameter	Description
	illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When non-motorized vehicles drive in motor vehicle lanes in the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

- Check whether snapshots are taken for non-motorized vehicles driving in motor vehicle lanes. If so, the configuration is successful.

  On the page for configuring detection of non-motorized vehicles driving in motor vehicle lanes, select **Enable snapshot**. When specified behavior is detected, the camera will automatically take snapshots.

  1. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP** and enable FTP.
  2. Set **FTP attribute** to **Micro checkpoint**.
  3. View snapshots taken for non-motorized vehicles driving in motor vehicle lanes on the FTP server.

Figure 5 Viewing snapshots



Parent topic: Configuring Intelligent Vehicle Event Analysis

Configuring Detection of Motor Vehicles Driving in Non-Motorized Vehicle Lanes

Prerequisites

- You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.
- You have set the lane attributes for detecting motor vehicles driving in non-motorized vehicle lanes. For details, see Procedure.

Setting Parameters for Detecting Motor Vehicles Driving in Non-Motorized Vehicle Lanes

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Motor Vehicles in Non-Motorized Vehicle Lanes** in the **Vehicle Intelligence** area. Click **Settings** next to **Motor Vehicles in Non-Motorized Vehicle Lanes**. The **Motor Vehicles in Non-Motorized Vehicle Lanes** page is displayed, as shown in Figure 1.

   Figure 1 Configuring detection of motor vehicles driving in non-motorized vehicle lanes

3. Set parameters for detecting motor vehicles driving in non-motorized vehicle lanes. Table 1 describes the parameters.

   Table 1 Parameters for detecting motor vehicles driving in non-motorized vehicle lanes

Parameter	Description
Enable snapshot	Indicates whether to enable snapshot taking upon detecting motor vehicles driving in non-motorized vehicle lanes. **NOTE:** • Before enabling snapshot taking, ensure that the FTP/SFTP server is configured. • Snapshots are stored on the FTP/SFTP server.
Detection sensitivity	Sensitivity for determining whether a motor vehicle occupies the non-motorized vehicle lane. A larger value indicates a higher sensitivity. **NOTE:** If this parameter is set to a larger value, when only part of a motor vehicle is in the non-motorized vehicle lane, the motor vehicle is regarded as occupying the non-motorized vehicle lane. You can set this parameter based on the site requirements.
Stay duration(s)	An alarm is triggered only when the duration for which a motor vehicle occupies the non-motorized vehicle lane exceeds the value of this parameter.

4. Draw a detection area.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area

Parameter	Description
	supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

5. Click **Save**. The function of detecting motor vehicles driving in non-motorized vehicle lanes is configured.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab. The tab page shown in Figure 2 is displayed.

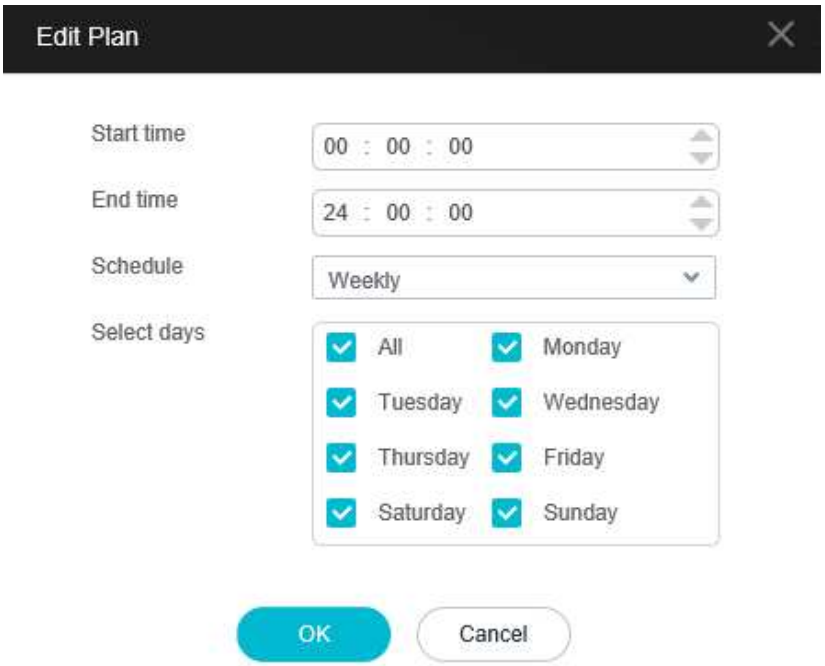
Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

NOTE

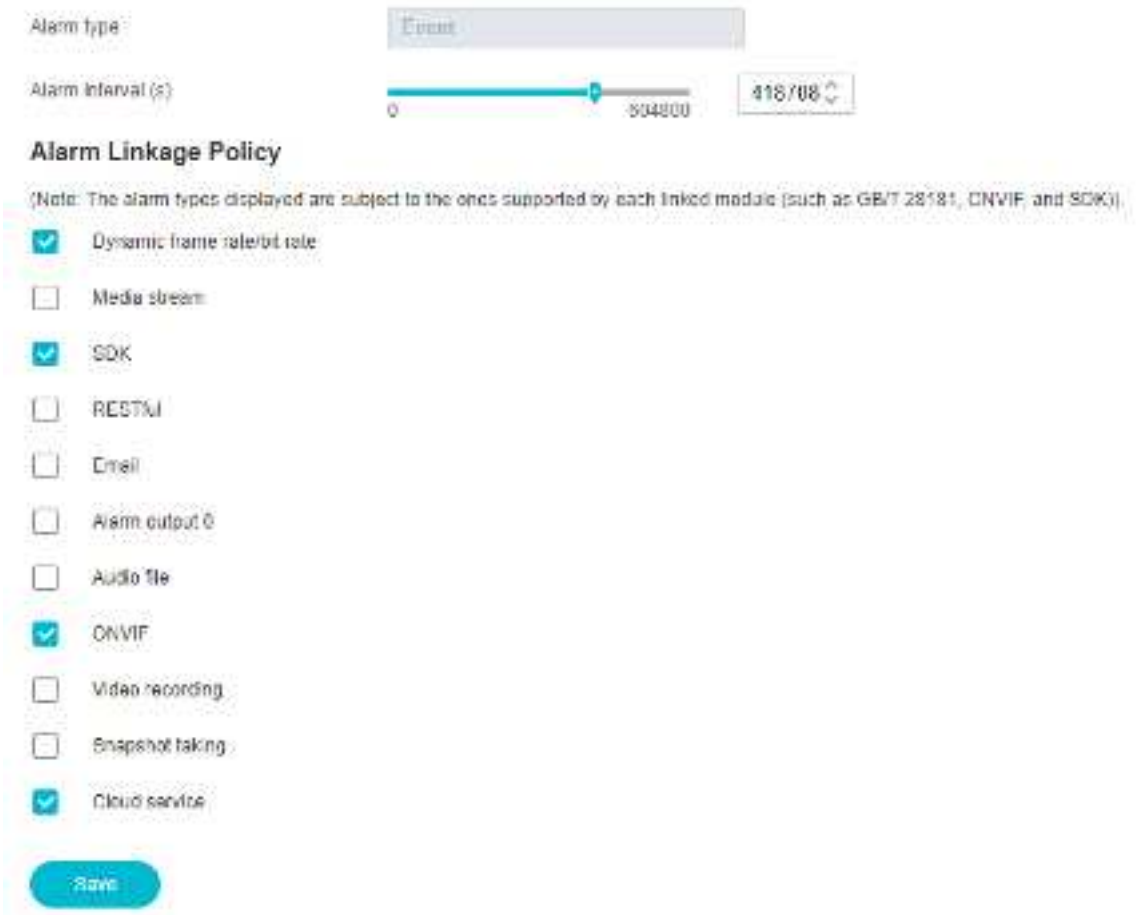
- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service.

Parameter	Description
	NOTE: The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a

Parameter	Description
	warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light

Parameter	Description
	illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When motor vehicles drive in non-motorized vehicle lanes in the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

- Check whether snapshots are taken for motor vehicles driving in non-motorized vehicle lanes. If so, the configuration is successful.

  On the page for configuring detection of motor vehicles driving in non-motorized vehicle lanes, select **Enable snapshot**. When specified behavior is detected, the camera will automatically take snapshots.

  1. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP** and enable FTP.
  2. Set **FTP attribute** to **Micro checkpoint**.
  3. View snapshots taken for motor vehicles driving in non-motorized vehicle lanes on the FTP server.

Configuring Detection of Wrong-Way Driving or Illegal Backing

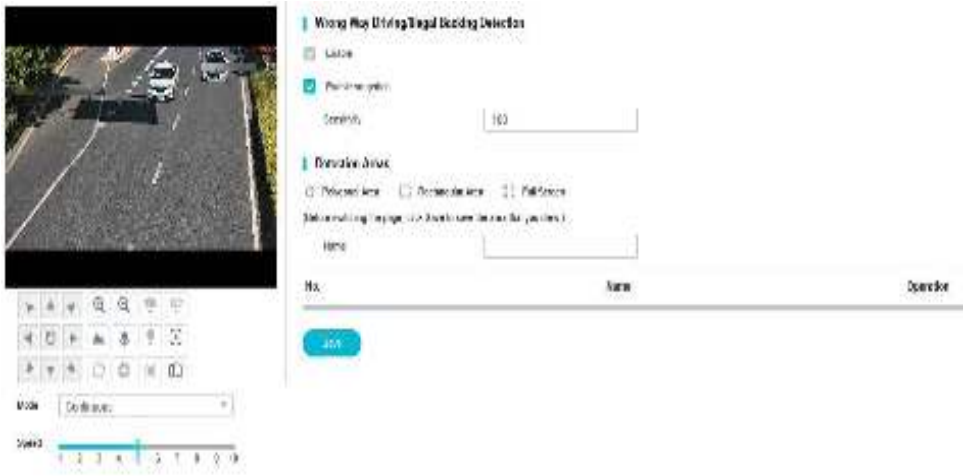
Prerequisites

- You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.
- You have set the lane direction for detecting wrong-way driving or illegal backing. For details, see Procedure.

Setting Parameters for Detecting Wrong-Way Driving or Illegal Backing

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Wrong-Way Driving/Illegal Backing Detection** in the **Vehicle Intelligence** area. Click **Settings** next to **Wrong-Way Driving/Illegal Backing Detection**. The **Wrong-Way Driving/Illegal Backing Detection** page is displayed, as shown in Figure 1.

   Figure 1 Configuring detection of wrong-way driving or illegal backing

3. Set parameters for detecting wrong-way driving or illegal backing. Table 1 describes the parameters.

   Table 1 Parameters for detecting wrong-way driving or illegal backing

Parameter	Description

Parameter	Description
Enable snapshot	Indicates whether to enable snapshot taking upon detecting wrong-way driving or illegal backing. **NOTE:** • Before enabling snapshot taking, ensure that the FTP/SFTP server is configured. • Snapshots are stored on the FTP/SFTP server.
Sensitivity	Sensitivity for determining whether a motor vehicle is moving. A larger value indicates a higher sensitivity. **NOTE:** If this parameter is set to a larger value, when a vehicle slightly moves backward, the system will regard the vehicle as wrong-way driving or illegal backing. You can set this parameter based on the site requirements.

4. Draw a detection area.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.

Parameter	Description
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

5. Click **Save**.

Configuring a Wrong-Way Driving Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Wrong-Way Driving Alert** tab. The tab page shown in Figure 2 is displayed.

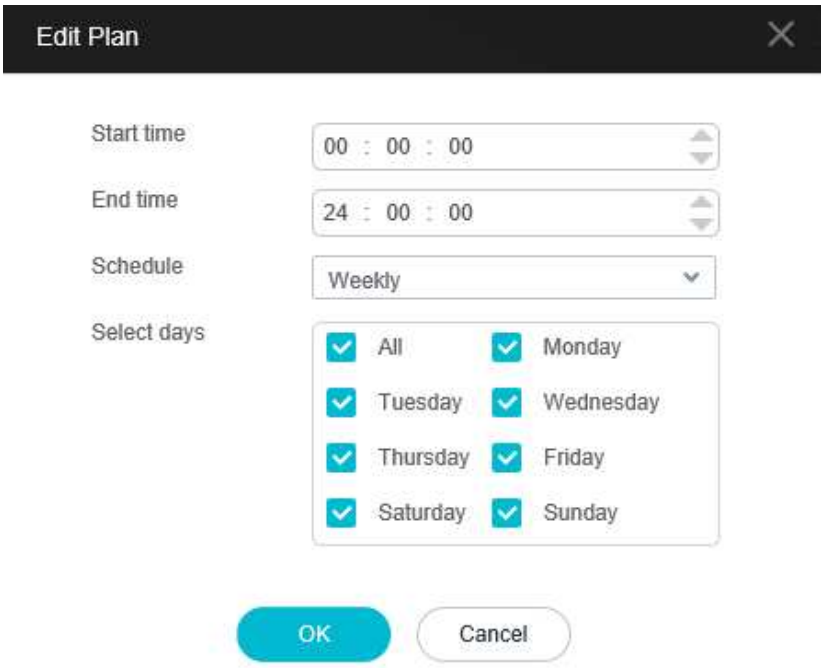
   Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

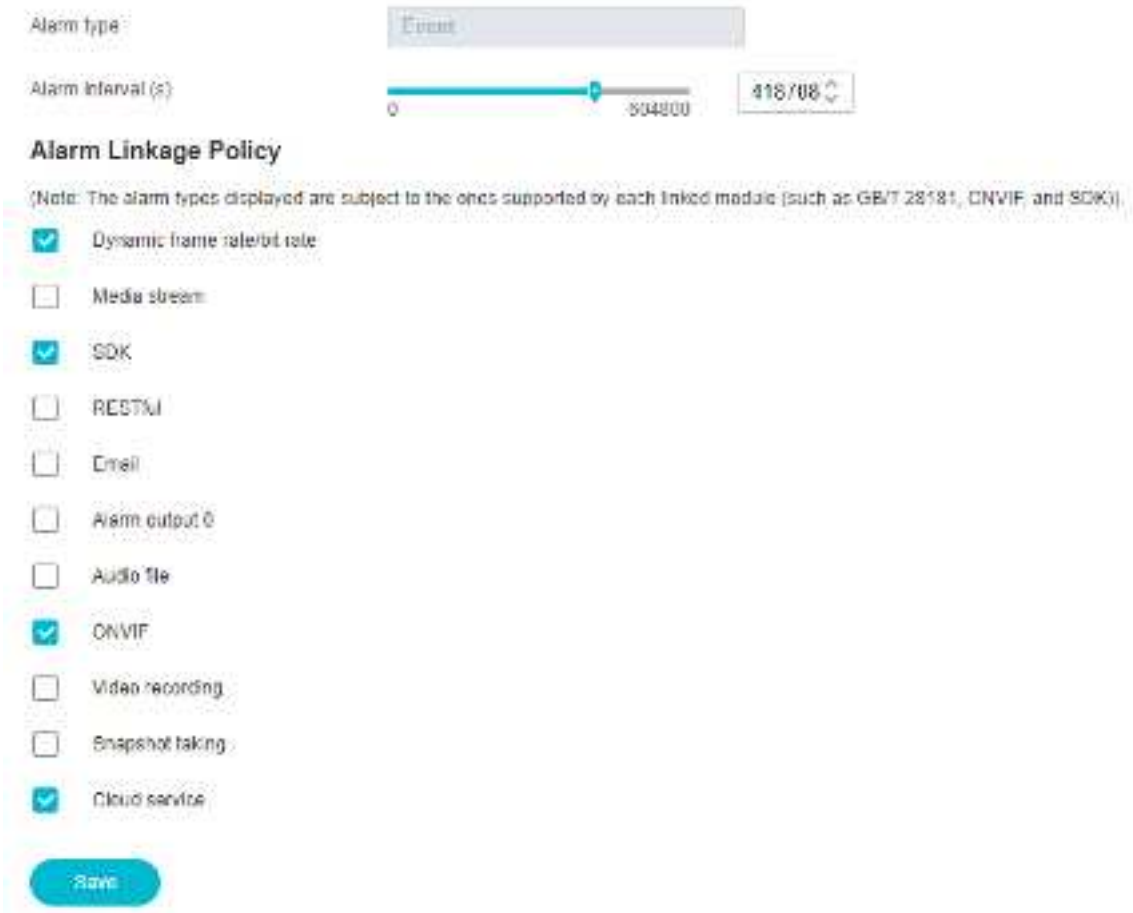
> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Wrong-Way Driving Alarms

1. Click the **Wrong-Way Driving Alarm** tab. The tab page shown in Figure 4 is displayed.

   Different camera models support different alarm linkage policies.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Configuring an Illegal Backing Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Illegal Backing Alert** tab. The **Illegal Backing Alert** tab page is displayed, as shown in Figure 5.

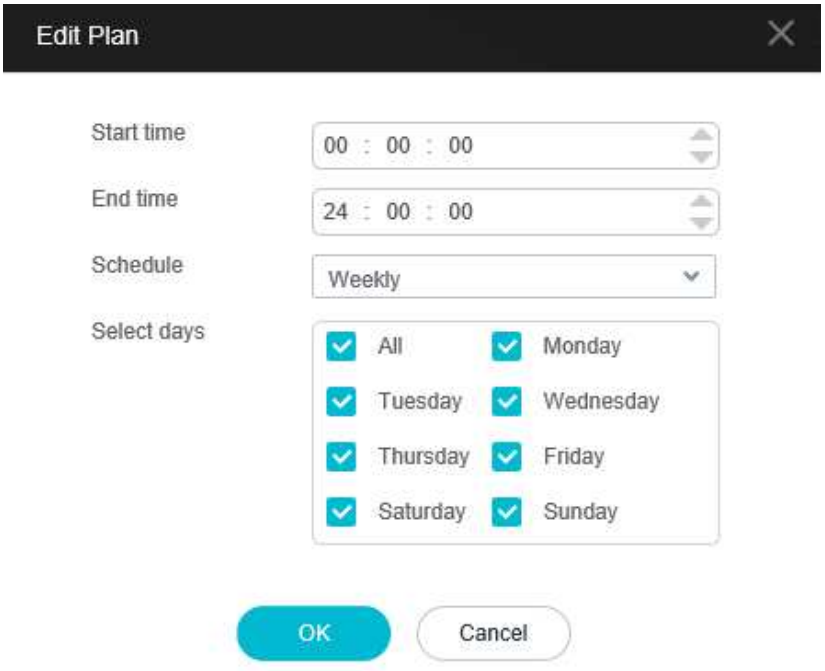
   Figure 5 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 6.

   Figure 6 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

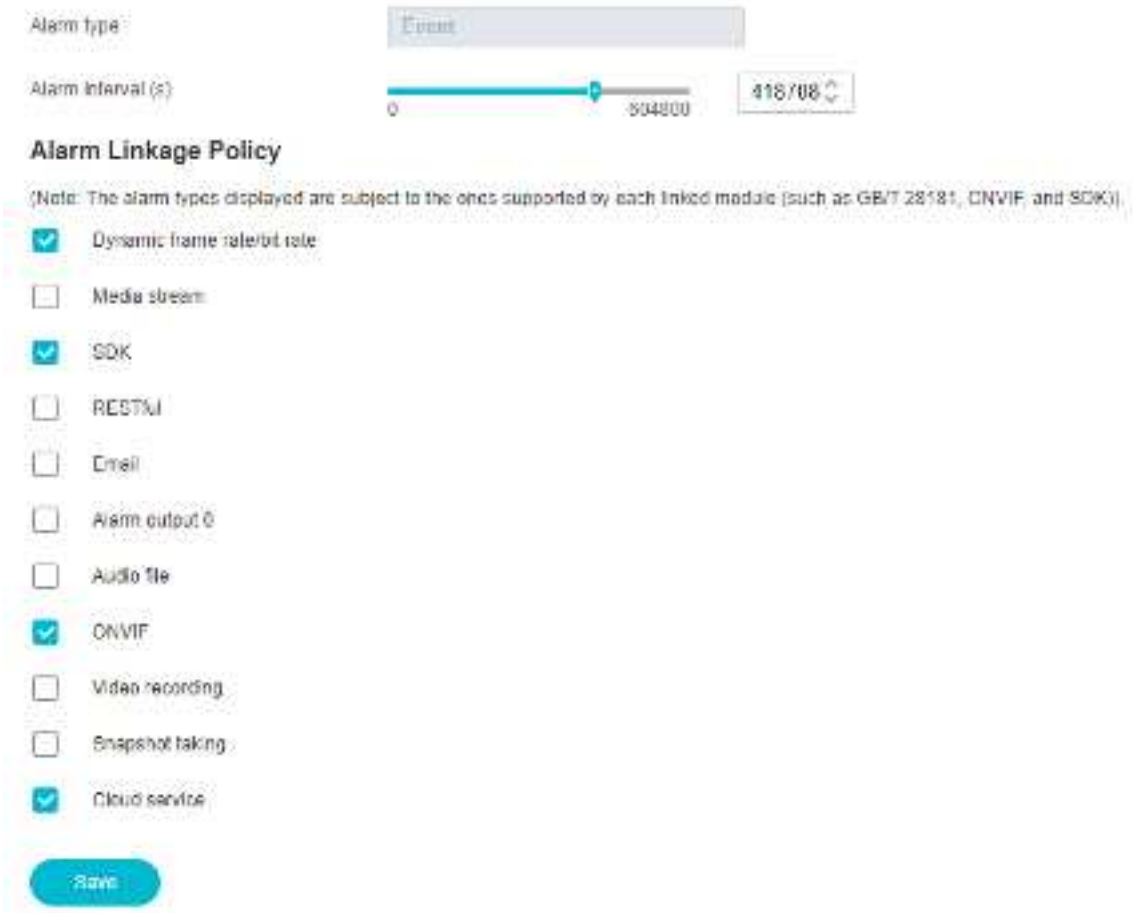
> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Illegal Backing Alarms

1. Click the **Illegal Backing Alarm** tab. The **Illegal Backing Alarm** tab page is displayed, as shown in Figure 7.

   Different camera models support different alarm linkage policies.

Figure 7 Configuring alarms



2. Set related parameters. Table 4 describes the parameters.

Table 4 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When wrong-way driving or illegal backing occurs in the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

- Check whether snapshots are taken for wrong-way driving or illegal backing. If so, the configuration is successful.

  On the page for configuring wrong-way driving or illegal backing detection, select **Enable snapshot**. When specified behavior is detected, the camera will automatically take snapshots.

  1. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP** and enable FTP.
  2. Set **FTP attribute** to **Micro checkpoint**.
  3. View snapshots taken for wrong-way driving or illegal backing on the FTP server.

     Figure 8 Viewing snapshots

Parent topic: Configuring Intelligent Vehicle Event Analysis

Configuring Marked Lane Violation Detection

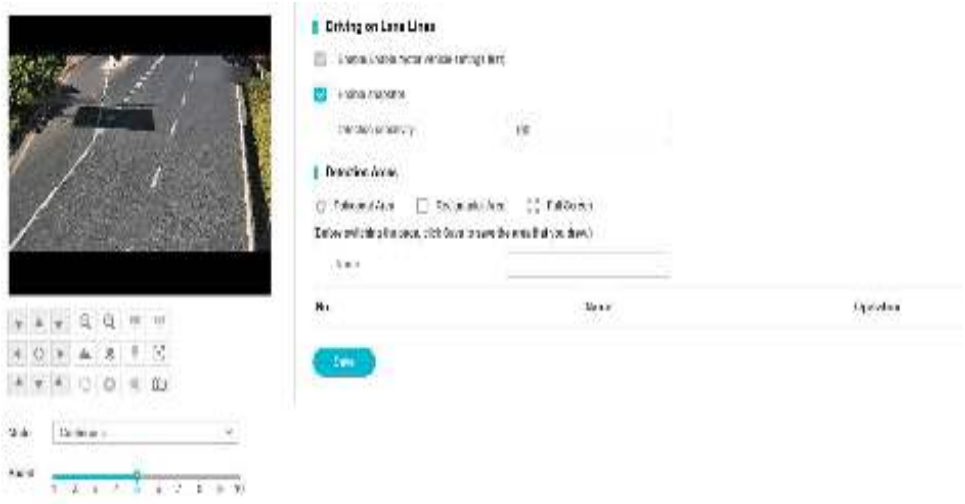
Prerequisites

- You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.
- You have drawn a lane line for marked lane violation detection. For details, see Procedure.

Setting Parameters for Detecting Marked Lane Violations

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Driving on Lane Lines** in the **Vehicle Intelligence** area. Click **Settings** next to **Driving on Lane Lines**. The **Driving on Lane Lines** page is displayed, as shown in Figure 1.

   Figure 1 Configuring marked lane violation detection

3. Set parameters for marked lane violation detection. Table 1 describes the parameters.

   Table 1 Parameters for detecting marked lane violations

Parameter	Description
Enable snapshot	Indicates whether to enable snapshot taking upon detecting marked lane violations.

Parameter	Description
	NOTE: • Before enabling snapshot taking, ensure that the FTP/SFTP server is configured. • Snapshots are stored on the FTP/SFTP server.
Detection sensitivity	Sensitivity for determining whether a motor vehicle drives on lane lines. A larger value indicates a higher sensitivity. **NOTE:** If this parameter is set to a larger value, when only part of a motor vehicle is on the lane line, the motor vehicle is regarded as driving on the lane line. You can set this parameter based on the site requirements.

4. Draw a detection area.

Table 2 Parameter description

Parameter	Description
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location.

Parameter	Description
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

5. Click **Save**. The marked lane violation detection is configured.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab. The tab page shown in Figure 2 is displayed.

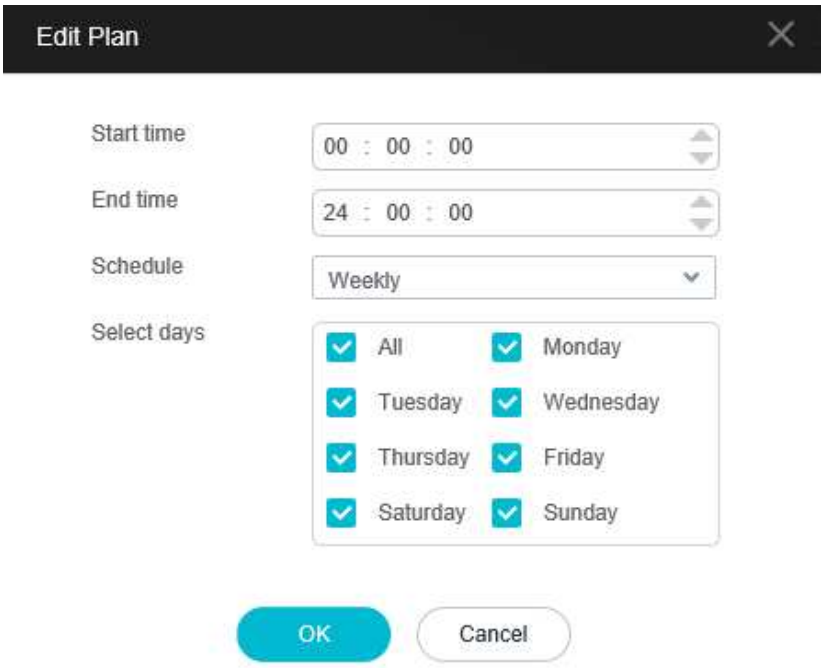
   Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

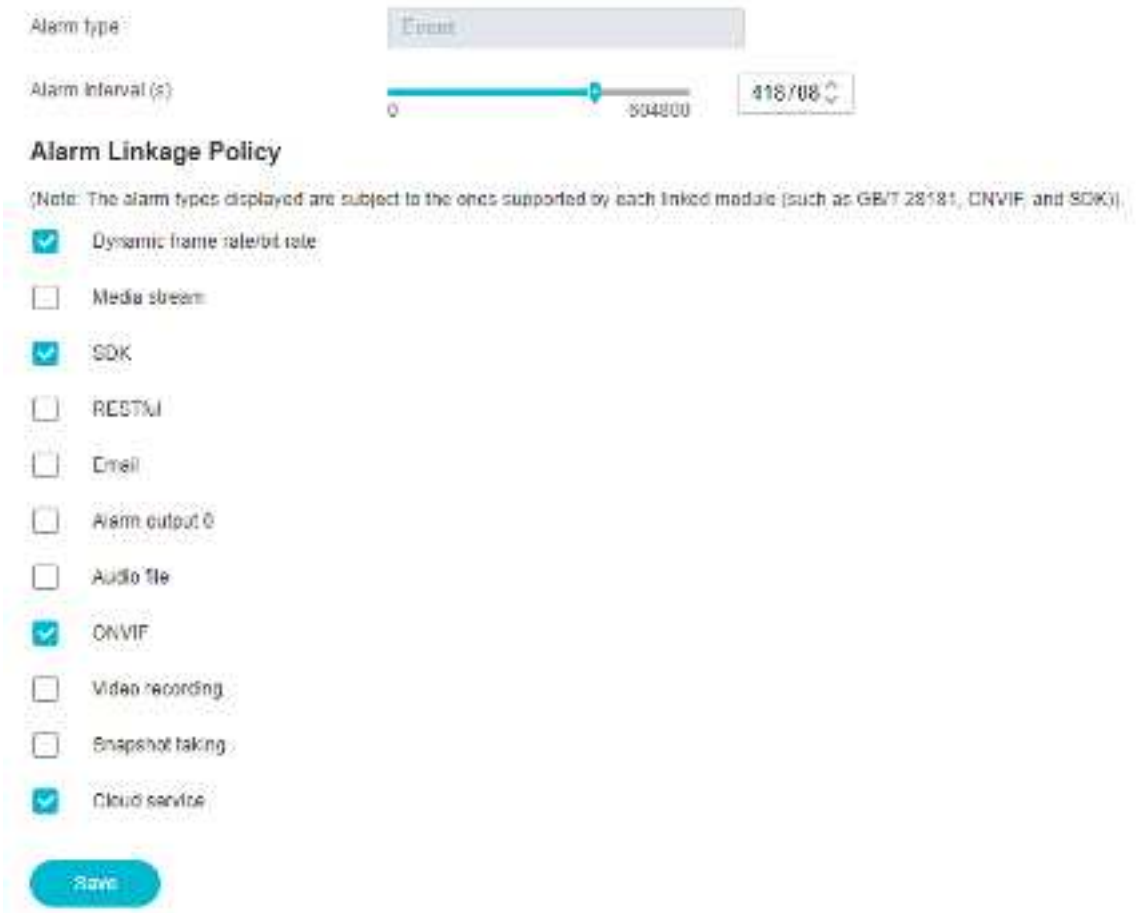
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related

functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.

Parameter	Description
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and

Parameter	Description
	saves the recording to the SD card when an alarm is generated. The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection

Parameter	Description
	results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When a marked lane violation occurs in the detection area, the configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

- Check whether snapshots are taken for marked lane violations. If so, the configuration is successful.

  On the page for configuring marked lane violation detection, select **Enable snapshot**. When specified behavior is detected, the camera will automatically take snapshots.

  1. Choose **Configuration** > **Network** > **Advanced Settings** > **FTP** and enable FTP.
  2. Set **FTP attribute** to **Micro checkpoint**.
  3. View snapshots taken for marked lane violations on the FTP server.

     Figure 5 Viewing snapshots

Parent topic: Configuring Intelligent Vehicle Event Analysis

Configuring Intelligent Traffic Flow Analysis

This section describes how to configure traffic flow statistics and view statistical results as well as configure traffic congestion detection to obtain vehicle traffic in specified time periods to prevent traffic congestions.

NOTE

- To use the traffic flow statistics function, the camera must be installed above the center of the road.
- The installation height and angle requirements for traffic flow statistics are the same as those for a micro checkpoint camera.
- If the traffic flow statistics function is required, it is recommended that the shutter speed be set to 1/250s.
- The traffic flow statistics function of the micro checkpoint camera and PTZ dome camera supports only vehicle front detection. During site survey and installation, if the traffic flow statistics function is required, install the camera at a proper position to detect approaching vehicles.
- For micro checkpoint cameras, you need to draw lane lines by referring to Configuring Motor Vehicle Capture in advance. Otherwise, the traffic flow statistics may be inaccurate.

Configuring Traffic Flow Statistics

Configuring Traffic Congestion Detection

Configuring Traffic Flow Data

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring Traffic Flow Statistics

Prerequisites

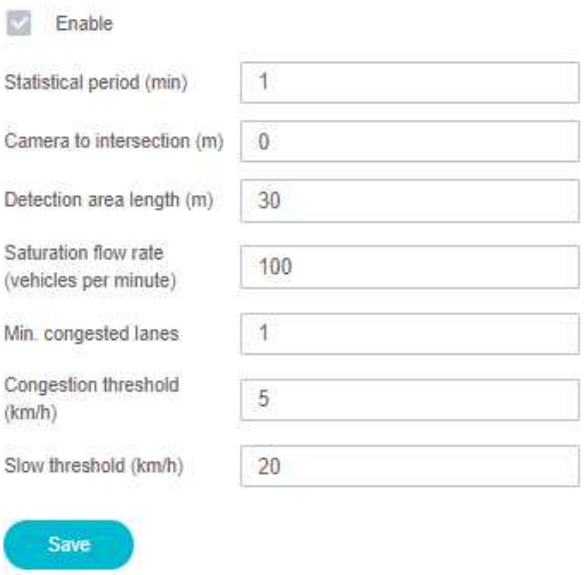
You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Traffic Flow Statistics** in the **Vehicle Intelligence** area. Click **Settings** next to **Traffic Flow Statistics**. The **Traffic Flow Statistics** page is displayed, as shown in Figure 1.

   The web page may vary depending on the camera model.

   Figure 1 Traffic Flow Statistics page

3. Set traffic flow statistics parameters. The following table describes the parameters.

   Table 1 Traffic flow statistics parameters

Parameter	Description

Parameter	Description
Statistical period (min)	Period of traffic flow statistics to be collected.
Camera to intersection (m)	Distance between the intersection and the lower edge of the video image from the camera, which is used to calculate the queue length.
Detection area length (m)	Actual length of the road that can be seen in the live video.
Saturation flow rate (vehicles per minute)	Maximum number of vehicles that can pass a lane in the image view per minute.
Min. congested lanes	Minimum number of congested lanes that can trigger alarm reporting. For example, if this parameter is set to **2**, an alarm is reported only when two or more lanes are congested.
Congestion threshold (km/h)	When the average vehicle speed in the detection area is less than the congestion threshold, a traffic congestion alarm is triggered. In this case, the road congestion condition is displayed as congested in the traffic statistics result on the **View** page.
Slow threshold (km/h)	• When the average vehicle speed in the detection area is greater than the congestion threshold and less than the slow threshold, the road congestion condition is displayed as slow in the traffic statistics result on the **View** page. • When the average vehicle speed in the detection area is greater than the slow threshold, the road congestion

Parameter	Description
	condition is displayed as smooth in the traffic statistics result on the **View** page.

Viewing Traffic Flow Statistics

To view traffic flow statistics, perform the following steps:

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Intelligent Detection**. In the upper right corner of the page, click . On the **Detection Area** tab page, select **Traffic statistics** under **Detection Type** and click **OK**.

   Click **Enable Real-time Capture**. The system collects statistics on the traffic flow. The statistical result is displayed on the **Traffic statistics** tab page, as shown in Figure 2. Table 2 describes the detection items for traffic flow statistics.

   Figure 2 Traffic statistics result

   NOTE

   Lanes in the traffic statistics are identified based on the lane lines drawn in the motor vehicle settings.

   Table 2 Traffic flow statistics detection items

Detection Item	Description
Start Time	Start time for collecting traffic statistics.
Lane Quantity	Number of lanes that are detected currently.

Detection Item	Description
Section Traffic (Vehicle)	Total number of vehicles passing through all lanes in a statistical period.
Traffic Flow (Vehicle)	Number of vehicles passing through each lane in a statistical period. The value is displayed in the following format: *Number of vehicles passing through lane 1_Number of vehicles passing through lane 2_Number of vehicles passing through lane 3_Number of vehicles passing through lane 4*. For example, the value **1_4_2** indicates that one vehicle passes through lane 1, four vehicles pass through lane 2, and two vehicles pass through lane 3 in a statical period.
Non-Motor Vehicle Traffic	Total number of non-motorized vehicles passing through all lanes in a statistical period.
Pedestrian Traffic	Total number of pedestrians passing through all lanes in a statistical period.
Vehicle Type (Small|Medium|Large)	Number of vehicles of each type passing through each lane in a statistical period. The value is displayed in the following format: *Number of small vehicles passing through lane 1|Number of medium vehicles passing through lane 1|Number of large vehicles passing through lane 1_Number of small vehicles passing through lane 2|Number of medium vehicles passing through lane 2|Number of large vehicles passing through lane 2_Number of small vehicles passing through lane 3|Number*

Detection Item	Description
	of medium vehicles passing through lane 3|Number of large vehicles passing through lane 3_Number of small vehicles passing through lane 4|Number of medium vehicles passing through lane 4|Number of large vehicles passing through lane 4. For example, the value **1|0|0_4|2|1_2|3|5** indicates that, in a statistical period, one small vehicle and no medium or large vehicle passes through lane 1, four small vehicles, two medium vehicles, and one large vehicle pass through lane 2, and two small vehicles, three medium vehicles, and five large vehicles pass through lane 3.
Average Speed (km/h)	Average speed of vehicles passing through each lane. The value is displayed in the following format: *Average vehicle speed in lane 1_Average vehicle speed in lane 2_Average vehicle speed in lane 3_Average vehicle speed in lane 4*. For example, the value **25_18_14** indicates that, in a statistical period, the average vehicle speed in lane 1 is 25 km/h, the average vehicle speed in lane 2 is 18 km/h, and the average vehicle speed in lane 3 is 14 km/h.
Time Occupancy (%)	In the same lane, if the time when there are vehicles in the lane is accumulated (recorded as t) in the statistical period (T), the time occupancy is calculated as follows: t/T. The unit is percentage. The

Detection Item	Description
	value is displayed in the following format: *Time occupancy in lane 1_Time occupancy in lane 2_Time occupancy in lane 3_Time occupancy in lane 4*.
Time Headway (s)	Time difference between vehicles passing the same location in the same lane. The value is displayed in the following format: *Time headway in lane 1_Time headway in lane 2_Time headway in lane 3_Time headway in lane 4*.
Space Headway (m)	Distance between the fronts of two vehicles in the same lane. The value is displayed in the following format: *Space headway in lane 1_Space headway in lane 2_Space headway in lane 3_Space headway in lane 4*.
Road Congestion	Measured based on the average vehicle speed in lanes and the lane time occupancy. Lane time occupancy = Duration during which there are vehicles in the lane in a statistical period/Statistical period • The criteria for determining whether the traffic is congested are as follows: If the average vehicle speed is less than the congestion threshold and the lane time occupancy is greater than 50%, the traffic is congested. • The criteria for determining whether the traffic is slow are as follows:

Detection Item	Description
	▪ If the average vehicle speed is less than the congestion threshold and the lane time occupancy is less than or equal to 50%, the traffic is slow. ▪ If the average vehicle speed is greater than the congestion threshold and less than the slow threshold, the traffic is slow. • The criteria for determining whether the traffic is smooth are as follows: If the average vehicle speed is greater than the slow threshold, the traffic is smooth.
Queue Length (m)	Queue length of vehicles in the lane when the lane is congested or vehicles drive slowly. The value is displayed in the following format: *Queue length in lane 1_Queue length in lane 2_Queue length in lane 3_Queue length in lane 4*.
Space Occupancy (%)	Ratio of the total length of all motor vehicles in the same lane to the length of the lane detection area. The lane occupancy is calculated every 10s. The average value is displayed in a statistical period.
Traffic Density (Vehicles/Hour)	Density of vehicles in a lane. Number of vehicles in a lane per unit time in a statistical period. The traffic density is calculated as follows: Traffic density = Number of vehicles in a lane in a statistical period/Statistical period.

Detection Item	Description
Saturation (%)	Lane occupancy per minute.

Parent topic: Configuring Intelligent Traffic Flow Analysis

Configuring Traffic Congestion Detection

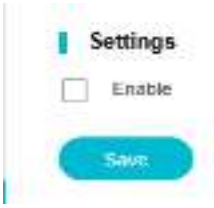
Prerequisites

You have enabled traffic flow statistics. For details, see Configuring Traffic Flow Statistics.

Setting Traffic Congestion Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Traffic Flow Statistics** in the **Vehicle Intelligence** area. Click **Settings** next to **Traffic Flow Statistics**. On the **Traffic Flow Statistics** page that is displayed, click the **Traffic Congestion** tab. The **Traffic Congestion** tab page is displayed, as shown in Figure 1.

   Figure 1 Traffic Congestion tab page

3. Select **Enable** to enable the traffic congestion detection function.
4. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab. The tab page shown in Figure 2 is displayed.

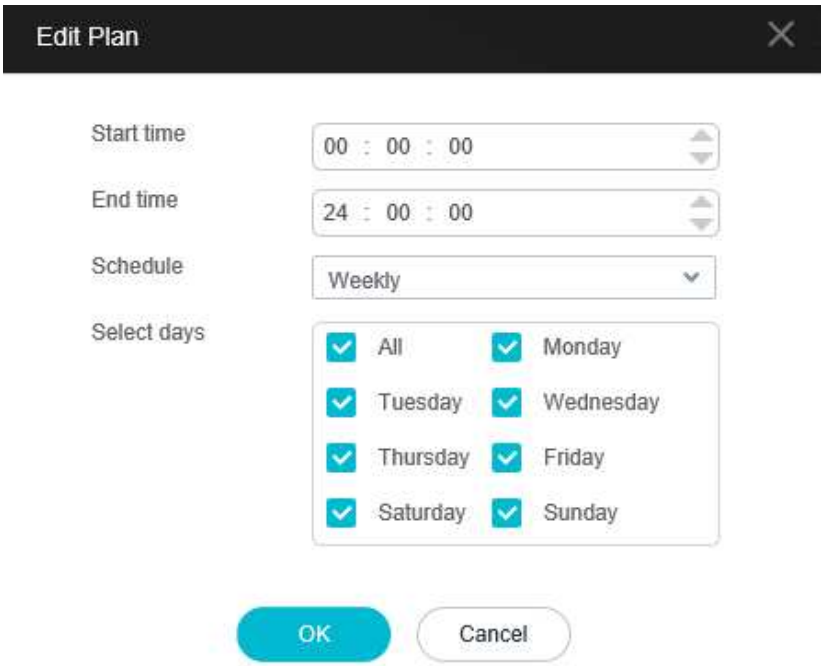
Figure 2 Alert Deployment Plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**. Click **OK**.
4. Click **Save**.

NOTE

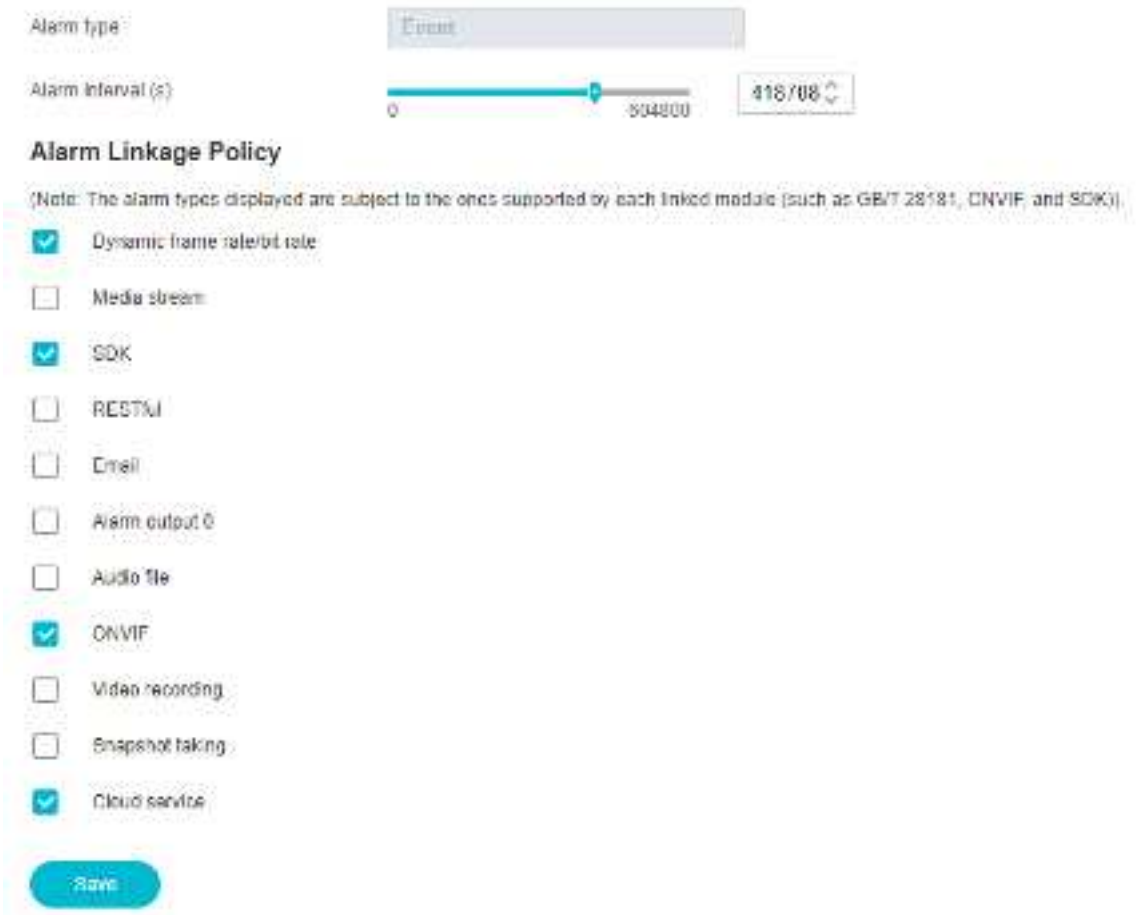
- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 1 describes the parameters.

Table 1 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service.

Parameter	Description
	NOTE: The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
Email	If **Email** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a

Parameter	Description
	warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration(s)** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light

Parameter	Description
	illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

If the road congestion condition is displayed as congested in the traffic statistics result and the number of congested lanes is greater than or equal to the preset value of **Min. congested lanes**, an alarm is generated.

Choose **Configuration** > **System** > **System Maintenance** > **Log** > **Log Query**. Set **Log type** to **Warning**, set **Period**, and click **Search**. Check whether alarm logs are generated within the specified period.

Parent topic: Configuring Intelligent Traffic Flow Analysis

Configuring Traffic Flow Data

After the traffic flow statistics function is configured, you can view the traffic flow statistics.

> **NOTE**
>
> To query traffic flow statistics, you need to install an SD card on the camera first.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Traffic Flow Statistics** in the **Vehicle Intelligence** area.
3. Click **Settings** next to **Traffic Flow Statistics**, and click the **Traffic Flow Data** tab. On the tab page that is displayed, set **Period** and click **Search**. The statistical result is displayed, as shown in Figure 1.

   You can filter required statistical results by **Channel** or **Lane number**. If needed, you can click **Export** to export the statistical results.

   Figure 1 Traffic Flow Data tab page

   Table 1 Traffic flow statistics items

Statistics Item	Description
Time	Start time for collecting traffic statistics.
Statistical Period (min)	Period of traffic flow statistics to be collected.

Statistics Item	Description
Lane ID	ID of the lane in which traffic flow statistics are to be collected.
Motor Vehicles/Non-motorized Vehicles/Pedestrians	Number of motor vehicles, non-motorized vehicles, and pedestrians in the lane in a specified period.
Average Vehicle Speed (km/h)	Average speed of all motor vehicles in the detection area in the lane in a specified period.
Time Occupancy	Duration during which vehicles exist in the lane divided by the statistical period.
Space Occupancy	Total length of occupied lane space measured in each frame divided by the total lane length in the statistical period (Total lane length in the statistical period = Number of frames x Lane length).
Time Headway (s)	Average time difference between the heads of all vehicles passing the detection lines of lanes.
Space Headway (m)	Value of **Time Headway (s)** multiplied by the average speed of all vehicles when passing the detection lines of lanes.
Large Vehicles/Medium Vehicles/Small Vehicles	Number of large, medium, and small vehicles in the lane in a specified period.
Left-Turn Vehicles/Straight-through Vehicles/Right-Turn Vehicles	Number of left-turn vehicles, vehicles going straight ahead, or right-turn vehicles in the lane in a specified period.

Statistics Item	Description
Road Condition	The value of the parameter is measured based on **Congestion threshold (km/h)** and **Slow threshold (km/h)** set on the **Traffic Flow Statistics** tab page. • When the average vehicle speed in the detection area is greater than the congestion threshold and less than the slow threshold, the value is displayed as slow. • When the average vehicle speed in the detection area is greater than the slow threshold, the value is displayed as smooth. • When the average vehicle speed in the detection area is less than the congestion threshold, a traffic congestion alarm is triggered and the value is displayed as congested.
Queue Length	When the road condition is displayed as congested, the queue length is measured every 100 frames and the average value of the total queue length is calculated.
Vehicle Density (Vehicles/Hour)	Number of passing vehicles per hour.
Saturation	Lane occupancy per minute.

Parent topic: Configuring Intelligent Traffic Flow Analysis

Configuring a Video-based Vehicle Detector

Cameras can detect vehicles that appear in a specified period and in specified lanes and report information about vehicles that enter or leave a specified detection area to the connected video-based vehicle detector platform. You can adjust the traffic light duration based on the vehicle information to improve traffic efficiency.

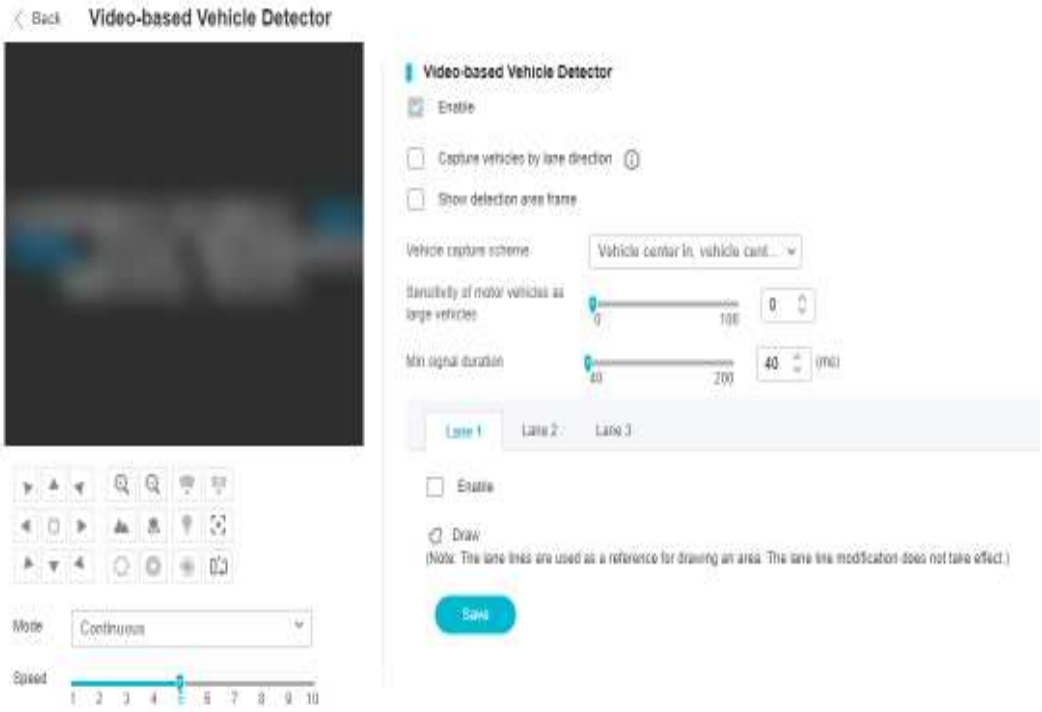
Prerequisites

- Cameras that support passing vehicle detection are available. For details about the camera models, see Intelligent Vehicle Analysis Features.
- You have enabled motor vehicle detection. For details, see Configuring Motor Vehicle Capture.
- You have obtained and installed the video-based vehicle detector application. For details, see Managing Apps.

Enabling Passing Vehicle Detection

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Video-based Vehicle Detector** in the **Vehicle Intelligence** area. Click **Settings** next to **Video-based Vehicle Detector**. The **Video-based Vehicle Detector** page is displayed, as shown in Figure 1.

   Figure 1 Setting video-based vehicle detector parameters



3. Select **Capture vehicles by lane direction** depending on your needs. If you select this parameter, you need to set **Vehicle direction** for the lane. For details, see Configuring Motor Vehicle Capture.

   NOTE

   This function is disabled by default. If this function is disabled in full intelligence mode, false vehicle capture may occur.

4. Select **Show detection area frame** based on the requirements. If this check box is selected, the detection area frame is displayed on the live video image on the **View** page. This check box is deselected by default.

5. Set **Vehicle capture scheme** based on the site requirements. This function specifies the scheme for capturing vehicles based on the time when a vehicle enters or leaves the induction loop. Three schemes are available: **Vehicle center in, vehicle center out**, **Vehicle center in, vehicle rear out**, and **Vehicle**

head in, vehicle rear out. The default scheme is **Vehicle center in, vehicle center out**, indicating that the system captures images of a vehicle when the vehicle center enters the loop and leaves the loop.

6. Set **Sensitivity of motor vehicles as large vehicles** based on the site requirements. The value ranges from 0 to 100. The default value is 50. Higher sensitivity indicates a higher probability of determining a vehicle as a large vehicle.
7. Set **Min signal duration (ms)**. The value ranges from 40 ms (default value) to 200 ms. You can set this parameter to specify a minimum duration for sending signals, based on the performance requirements of the controller for signalized vehicle detection, when a vehicle enters and dwells in the detection area frame. This prevents instantaneous detection signals from being regarded as abnormal signals and filtered out and ensures that no vehicle will be missed.
8. Click **Draw** and adjust the detection area on the live video image. You can configure multiple detection areas for varied lanes.

   Adjust the detection area based on the site requirements to ensure that motor vehicles pass the detection area. It is recommended that the distance between the upper and lower frames be less than or equal to two-thirds of the vehicle length. To clear the area, click **Clear**.

   > **NOTE**
   >
   > The lane lines in the live video are for reference only. You can modify the lane lines and make the modification take effect on the page for configuring motor vehicle detection.

9. Click **Save**.

Setting Video-based Vehicle Detector Platform Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **General Configuration** > **Northbound Access Protocol** > **Video Vehicle Detector Platform**.
3. Select **Enable** to connect to the video-based vehicle detector platform.
4. Set video-based vehicle detector platform parameters, as shown in Figure 2. Table 1 describes the parameters.

   Figure 2 Setting video-based vehicle detector platform parameters



Table 1 Video-based vehicle detector platform parameters

Parameter	Description
Platform IP	IP address of the video-based vehicle detector platform, which is provided by the platform.
Port number	Port number of the video-based vehicle detector platform, which is provided by the platform.
Start lane ID	Set this parameter based on the configuration requirements of the video-based vehicle detector platform and the site requirements.

Parameter	Description
Road ID	Set this parameter based on the site requirements. The first four characters indicate the area ID, and the last four characters indicate the intersection ID in the area. For example, **00010002** indicates that the area ID is **0001** and the intersection ID is **0002**. The IDs of areas and intersections are provided by the platform.
Road direction	Set this parameter based on the configuration requirements of the video-based vehicle detector platform and the site requirements.

5. Click **Save**.

Parent topic: Configuring Intelligent Vehicle Analysis

Configuring 1 + N

This chapter describes the background, primary/secondary camera requirements, and configuration procedure for 1 + N.

Introduction

Configuration Procedure

Parent topic: Intelligent Settings

Introduction

Background

In some actual scenarios, a video security system has been deployed and some network cameras have been installed on the live network. However, the devices are aged and outdated. Therefore, some intelligent analysis functions cannot be implemented. In this case, the existing system needs to be upgraded or reconstructed to meet current users' requirements on intelligent services (such as target capture and vehicle recognition).

A common solution is to replace all the legacy cameras with high-end cameras that support intelligent analysis functions. However, this solution costs much and involves heavy delivery workload.

In this case, an intelligent camera that supports 1 + N can be introduced to solve the problem. The camera can not only provide intelligent analysis services for its detection area but also perform video stream connection, decoding, intelligent analysis, and intelligent analysis result output for one or more network cameras on the live network through access protocols. In this way, the legacy common cameras can obtain some intelligent analysis capabilities, reducing the costs for reconstructing the legacy system.

Definition

In the 1 + N solution, the newly added high-performance camera that supports 1 + N is called the primary camera or device, and a common camera on the live network is called a secondary camera or device.

For details about typical application scenarios and installation requirements, see 1 + N.

Requirements for the Primary and Secondary Cameras

- Secondary cameras do not need to support target detection or object classification. The primary camera can work with the

secondary cameras to implement the function.

- The resolution of a secondary camera must not be higher than that of the primary camera or lower than 720p (1280 x 720). If the secondary camera resolution is 720p, it is considered 2 megapixels in total resolution calculation.
- The following table lists the resolution combinations and service combinations that can be implemented.

Table 1 Resolution combinations and service combinations supported by and HWT-D3252-10-SIU

1 + N Mode	Resolution Combination (Primary Camera + Secondary Camera 1)	Intelligent Service Combination
1 + 1	5-megapixel + 2-megapixel (720p)	Target checkpoint + Target checkpoint

- Table 2 describes the specific requirements for the secondary cameras.

Table 2 Requirements for the secondary cameras

Item	Requirement
Connection protocol	The RTSP and ONVIF protocols must be supported, and the ONVIF protocol must be enabled.
Encoding protocol	The H.265 or other related encoding protocols must be supported.
Resolution	16:9 (aspect ratio with a width of 16 units and height of 9)
Live video resolution	The recommended resolution is 1920 x 1080. The live video resolution should be less than the resolution of the primary camera.
Stream frame rate	≤ 30 fps

Item	Requirement
Stream bit rate	• The bit rate must not exceed 12 Mbit/s at 8 megapixels. • The bit rate must not exceed 8 Mbit/s at 6 megapixels. • The bit rate must not exceed 6 Mbit/s at 4 megapixels. • The bit rate must not exceed 4 Mbit/s at 2 megapixels.

- Network requirements: A gigabit network is recommended. If a 100 Mbit/s network is used, check whether the current network bandwidth meets the requirements. For details about how to calculate the network bandwidth, see Network and Bandwidth Requirements.
- After the secondary device management is configured, if parameters such as the bit rate, resolution, and frame rate of the camera are modified, the preceding conditions may not be met. In this case, you need to reconfigure the secondary device and network parameters.

Parent topic: Configuring 1 + N

Configuration Procedure

Prerequisites

The 1 + N algorithm package has been loaded. For details, see Upgrading the Camera Version/Algorithms.

> **NOTE**
>
> In the current version, the 1 + N function is available without loading the 1 + N license. However, the license status is invalid on the page for configuring the primary camera.

Enabling 1 + N

1. Log in to the web system of the primary camera (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. On the page that is displayed, toggle-on **1 + N**, as shown in Figure 1.

   Figure 1 Enabling 1 + N

Enabling ONVIF

In 1 + N scenarios, the primary and secondary cameras are connected through the ONVIF protocol. Therefore, you need to enable the ONVIF protocol for the primary and secondary cameras.

1. Log in to the web system of the primary and secondary cameras separately.
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **ONVIF**. Select **Enable ONVIF**.
3. Set **Transmission protocol** to **HTTP/HTTPS**.

4. Click the **RTSP** tab and set **RTSP authentication mode** based on the site requirements.

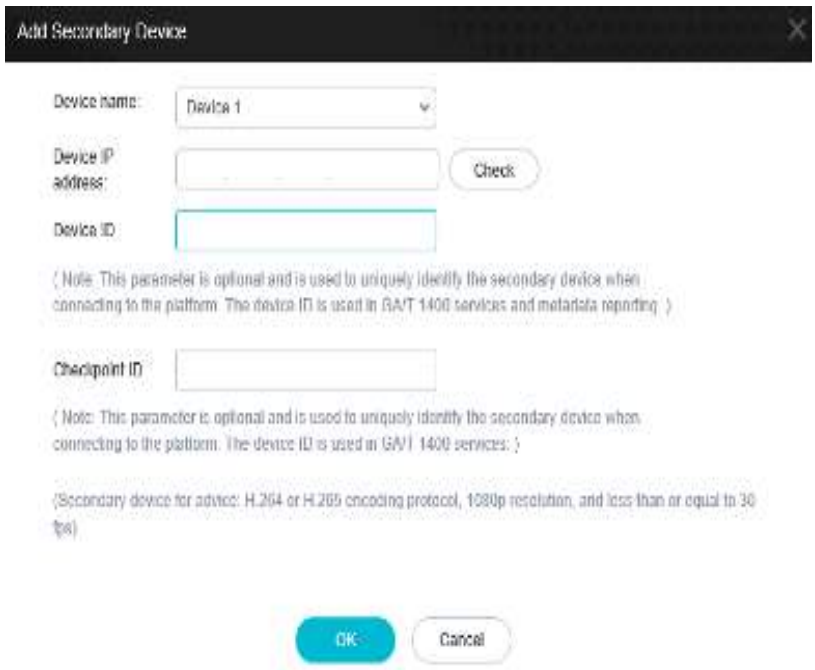
> **NOTE**
>
> The **RTSP authentication mode** parameter of the secondary device cannot be set to **Digest_SHA256**.

Adding Secondary Cameras

1. Log in to the web system of the primary camera (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**.
3. Click + **New Secondary Device** and add a secondary camera, as shown in Figure 2.

> **NOTE**
>
> You can click **Delete Secondary Device** to delete a secondary camera.

Figure 2 Adding a secondary camera



NOTE

- You can click **Check** to check whether the network connection is normal.
- After a secondary camera is added, if you modify video parameters on the secondary camera, the parameter settings will not be synchronized to the primary camera. If you must modify the parameters, delete the secondary camera on the primary camera and add it again after the modification.

4. Click the secondary camera. On the page that is displayed, click **Configure Secondary Device**. In the dialog box that is displayed, configure the secondary camera, as shown in Figure 3. Table 1 describes the parameters.

   The following uses one secondary camera as an example.

Figure 3 Configuring a secondary camera

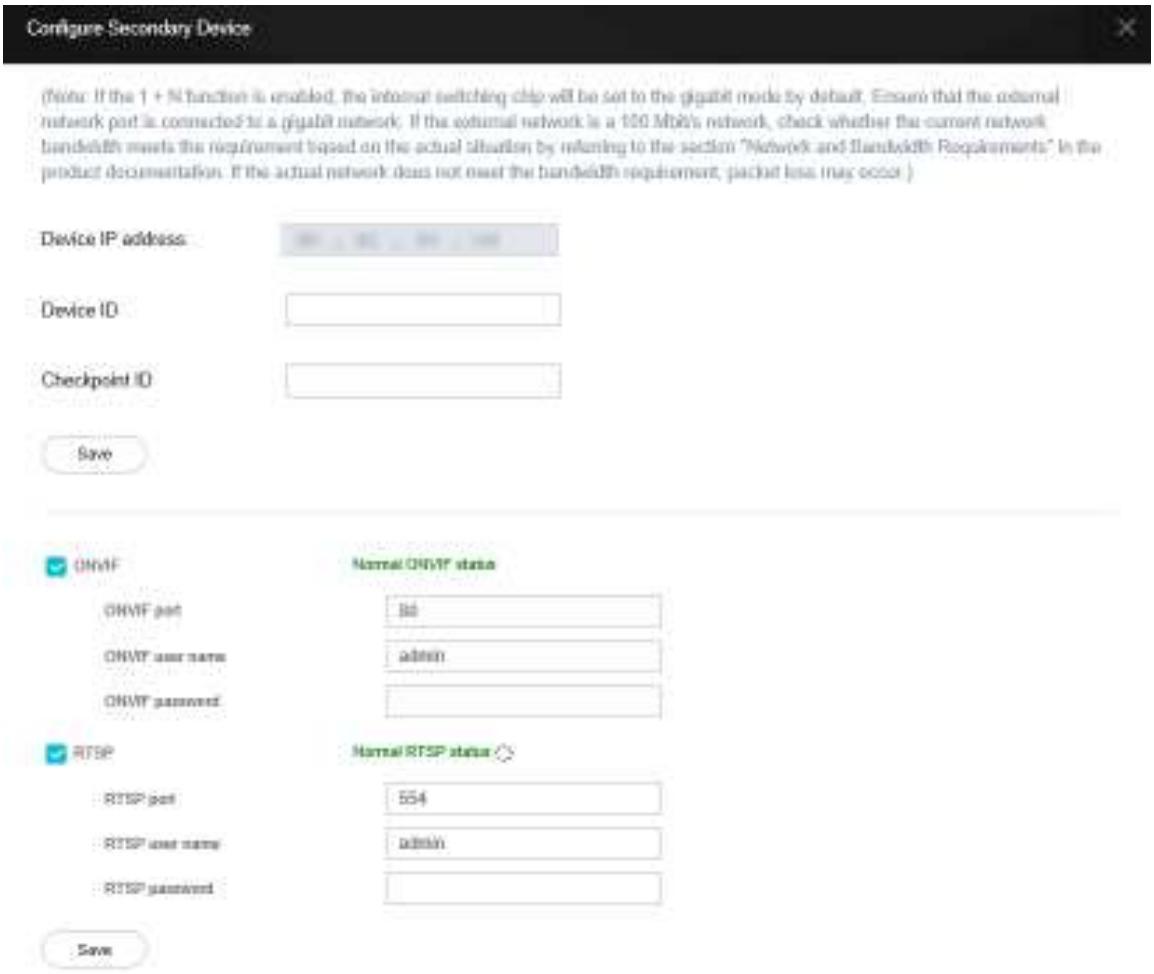


Table 1 Parameter description

Parameter	Description
Device IP address	IP address of the secondary camera.
Device ID	Device ID of the secondary camera. For details, see Setting GA/T 1400 Parameters.
Checkpoint ID	Checkpoint ID of the secondary camera. For details, see Setting GA/T 1400 Parameters.
ONVIF	Select the check box. The ONVIF protocol must be enabled for the secondary camera. Use the default value, 80, of **ONVIF port**. The values of **ONVIF user name** and **ONVIF password** of the primary

Parameter	Description
	camera must be the same as those configured for the secondary camera. **NOTE:** If **ONVIF port** is set to **80** (that is, HTTP is used for access), security risks may exist. Exercise caution with this port number. 1. Log in to the web system of the secondary camera. 2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **ONVIF**. Select **Enable ONVIF**. 3. Set the ONVIF user name and password to those under **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Password Management** > **ONVIF Password**.
RTSP	Select the check box. The values of **RTSP port**, **RTSP user name**, and **RTSP password** must be the same as those configured for the secondary camera. 1. Log in to the web system of the secondary camera. 2. Choose **Configuration** > **Network** > **Basic Settings** > **Port** and view the RTSP port. 3. Set **RTSP user name** and **RTSP password** to the values of **ONVIF user name** and **ONVIF password**, respectively.

5. Click **Save**.

Configuring the Primary Camera

1. Log in to the web system of the primary camera (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**.

   The web page varies depending on the camera model.

Figure 4 Configuring the primary camera



Table 2 Parameter description

Parameter	Description
1 + N mode	The system displays the supported intelligent services. The current certificate status is displayed on the page. If the status is displayed as invalid, the 1 + N function is still available. You can load licenses or ignore the status.
	To configure intelligent analysis functions for the primary and secondary cameras, click  . For details, see Configuring Target Capture. **NOTE:** In live video mode, the camera does not perform intelligent analysis and can only shoot live video.

NOTE

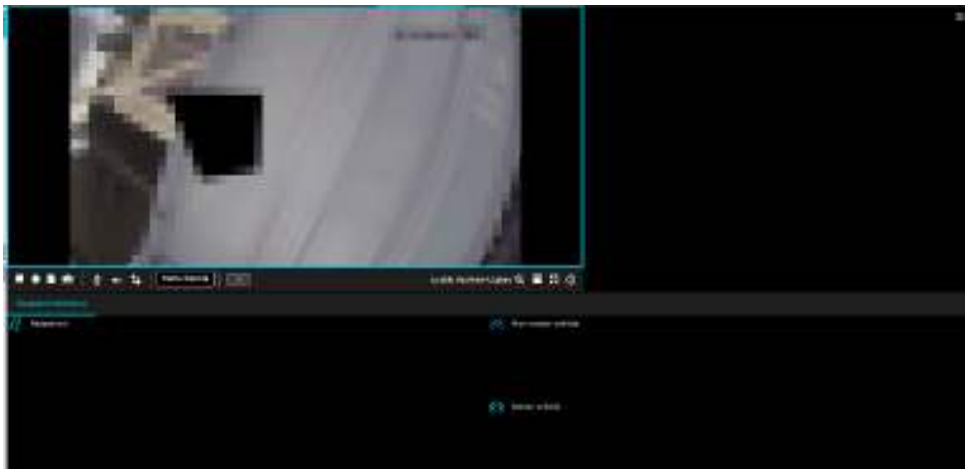
- Before selecting a secondary camera, ensure that the secondary camera has been added. For details, see Adding Secondary Cameras.

Viewing 1 + N Results

1. Log in to the web system of the primary camera (https://*Camera IP address*).
2. Choose **Display** > **Object Classification**. The **Object Classification** page is displayed, as shown in Figure 5. The web page varies

between camera models.

Figure 5 Object Classification page



3. Click **Enable Real-time Capture** to view the intelligent analysis results of the primary or secondary camera.

> **NOTE**
>
> The real-time capture function cannot be enabled on multiple tabs at a time due to browser process conflict. When you attempt to enable the real-time capture function on multiple tabs, a message will be displayed, indicating that the process of reporting object classification or target information has been started. In this case, you need to close unnecessary tabs and leave only one tab open or restart the browser and try again.

Parent topic: Configuring 1 + N

Event Configuration

This chapter describes how to configure intelligent event analysis functions such as motion detection, video quality diagnosis, lens blocking detection, and sound detection.

NOTICE

- Pan, tilt, or zoom operations are not supported during intelligent event analysis.
- The intelligent analysis supports detection only in full image mode. If area cropping is enabled, the detection result is still superimposed on the full image.
- In the Windows 10 operating system, if the live video resolution exceeds 5 megapixels (3072 x 1728), detection lines for intelligent analysis may fail to be displayed on the live video image. To rectify the fault, perform the following operations: Log in to the camera web system, choose **Configuration** > **Local** > **Playing Settings** and set **Rendering mode** to **D3D**. Alternatively, choose **Configuration** > **Video/Audio** > **Video** and decrease the resolution of the primary stream.
- Functions available on the web page vary between camera models.

Event Detection Features This section describes the events supported by different camera models.

Configuring Motion Detection
After motion detection is enabled, an alarm is generated when an object moves within the specified detection area of the camera.

Configuring Lens Blocking Detection
After the lens blocking detection is configured, an alarm will be generated promptly when the lens is blocked.

Configuring Scene Change Detection
After the scene change detection is configured, an alarm will be generated promptly when the detection scene changes due to manual movement of the camera or other reasons.

Configuring Defocus Detection
If a camera's focal length is inappropriate, images may be unclear. You can configure defocus detection to generate alarms promptly when the camera is out of focus, reducing the cost of manual check.

Configuring Audio Diagnosis
This section describes how to configure audio diagnosis, including audio exception detection and sudden volume increase and decrease detection.

Configuring Alarm Input and Output
You can configure the alarm input device and alarm output device. When the device receives a specified type of alarm in the alert plan period, the device takes predefined actions based on the configured alarm linkage policy.

Configuring Certificate Expiration Alarm
After the certificate expiration alarm is set, the system will automatically display a message prompting users to update the certificate when the certificate is to expire in specified number of days.

Configuring System Intrusion Detection
This section describes how to configure system intrusion detection. After configuration, the system can detect and intercept intrusions in a timely manner.

Parent topic: Configuration

Event Detection Features

This section describes the events supported by different camera models.

Different camera models support detection of different events. The following table describes the differences.

Table 1 Event detection features

Device Model	Motion Detection[a]	Video Quality Diagnosis[a]	Lens Blocking Detection[a]	Scene Change Detection[a]	Defocus Detection	Sound Detection[a]	Sudden Volume Increase or Decrease Detection[a]	Fog Detection	Visibi Detec
HWT-D6550-10-Z33-SV	YES	YES	YES	YES	YES	NO	YES	NO	NO
HWT-D3040-10-ELI-PV (2.8 mm)	YES	NO	YES	NO	NO	NO	NO	NO	NO
HWT-D2122-10-SIU	YES	YES	YES	YES	YES	YES	YES	NO	NO
HWT-D2152-10-SIU	YES	YES	YES	YES	YES	YES	YES	NO	NO
HWT-D3222-10-SIU	YES	YES	YES	YES	YES	YES	YES	NO	NO
HWT-D3252-10-SIU	YES	YES	YES	YES	YES	YES	YES	NO	NO

a: This function cannot be put into commercial use currently. The specifications vary greatly in different scenarios.

Parent topic: Event Configuration

Configuring Motion Detection

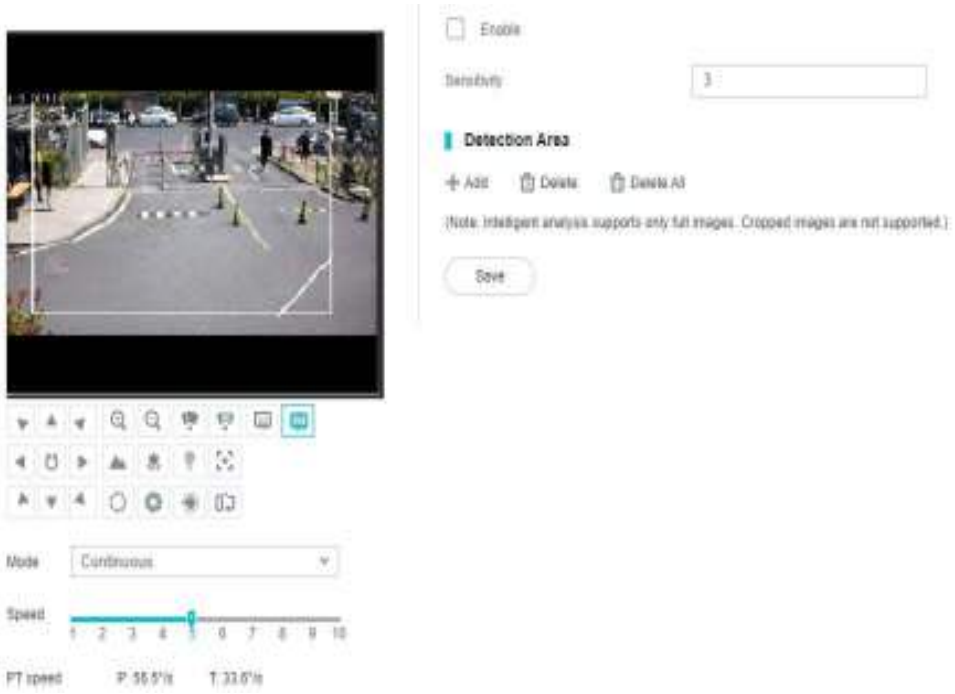
After motion detection is enabled, an alarm is generated when an object moves within the specified detection area of the camera.

Setting Motion Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Motion** and click **Basic Settings**. The **Basic Settings** tab page is displayed, as shown in the following figure.

   The web page varies between camera models.

   Figure 1 Configuring motion detection



3. Select **Enable** to enable motion detection. The setting takes effect only after you click **Save**.
4. Click **Add**.

   A motion detection area is displayed on the live video image.

> **NOTE**

- You can add only one motion detection area at a time. If you need to add more motion detection areas, click **Add** again.
- A maximum of four motion detection areas can be added.

5. Use the mouse to adjust the location and size of the motion detection area.
6. Set motion detection parameters. Table 1 describes the parameters.

Table 1 Motion detection parameters

Parameter	Description
Sensitivity	Motion detection sensitivity. **NOTE:** A larger value indicates a higher sensitivity. To detect slight motion, you are advised to set the sensitivity to a larger value.

7. Click **Save**.

NOTE

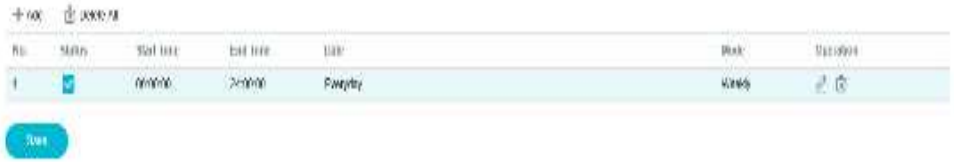
- To delete a motion detection area, select it on the live video image and click **Delete**.
- To delete all motion detection areas, click **Delete All**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

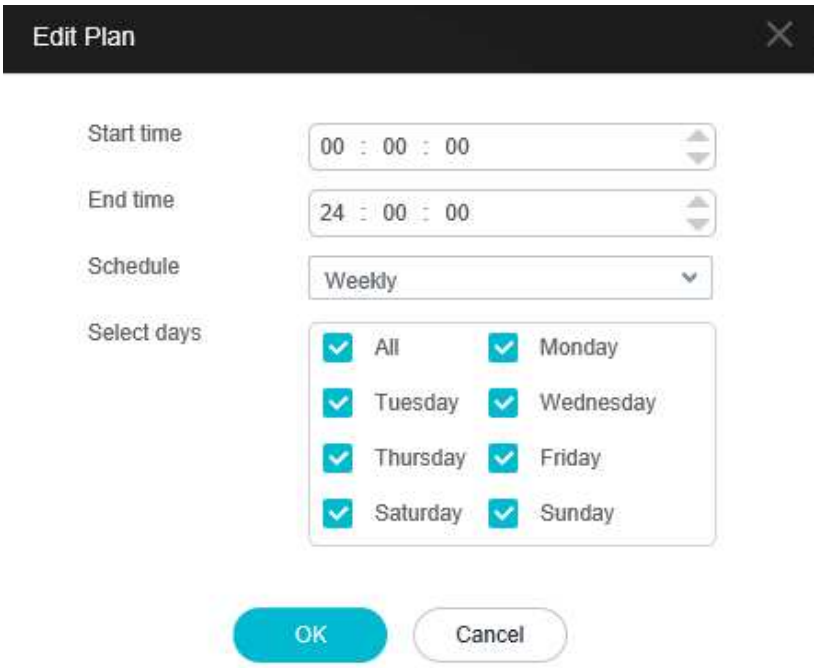
Figure 2 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click ✎ or 🗑 in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

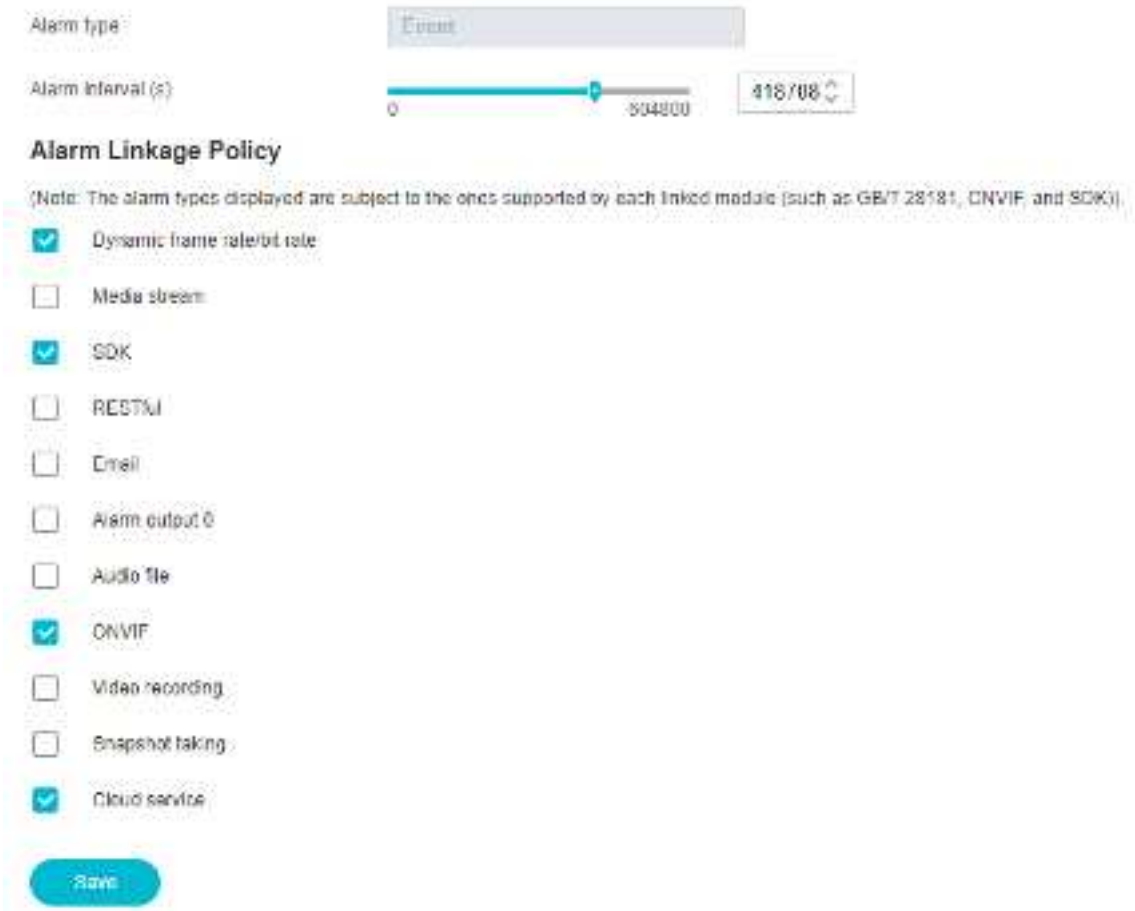
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether a motion detection alarm is reported.

Parent topic: Event Configuration

Configuring Lens Blocking Detection

After the lens blocking detection is configured, an alarm will be generated promptly when the lens is blocked.

Setting Lens Blocking Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Lens Blocking**. The **Lens Blocking** tab page is displayed, as shown in the following figure.

   The web page varies between camera models.

   Figure 1 Configuring lens blocking detection

   
3. Select **Enable**.
4. Set lens blocking detection parameters. Table 1 describes the parameters.

   Table 1 Parameter description

Parameter	Description
Sensitivity	Lens blocking detection sensitivity. A larger value indicates higher sensitivity. With a higher sensitivity, the camera can generate alarms when the lens is blocked by an object with a smaller size and brighter luminance. **NOTE:** • If **Sensitivity** is set to **1**, an alarm will be generated when the percentage of the

Parameter	Description
	blocked area reaches about 95%. • If **Sensitivity** is set to **2**, an alarm will be generated when the percentage of the blocked area reaches about 90%. • If **Sensitivity** is set to **3**, an alarm will be generated when the percentage of the blocked area reaches about 85%. • If **Sensitivity** is set to **4**, an alarm will be generated when the percentage of the blocked area reaches about 80%. • If **Sensitivity** is set to **5**, an alarm will be generated when the percentage of the blocked area reaches about 70%.

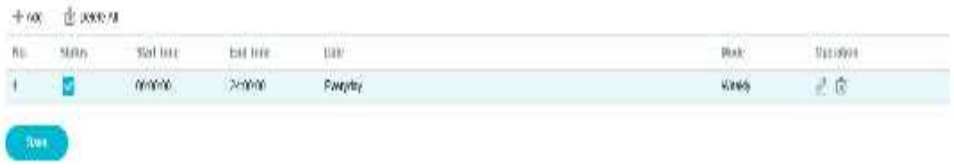
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

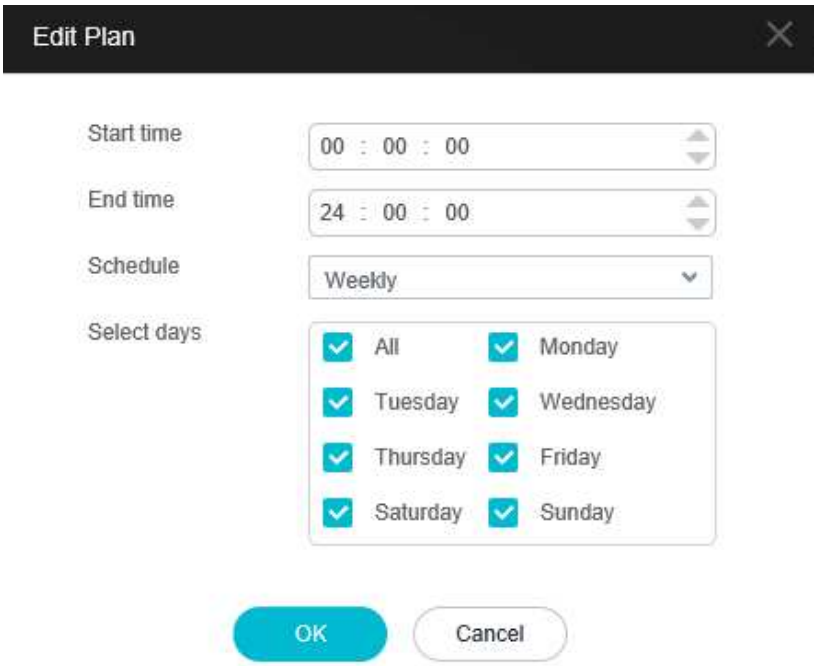
   Figure 2 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

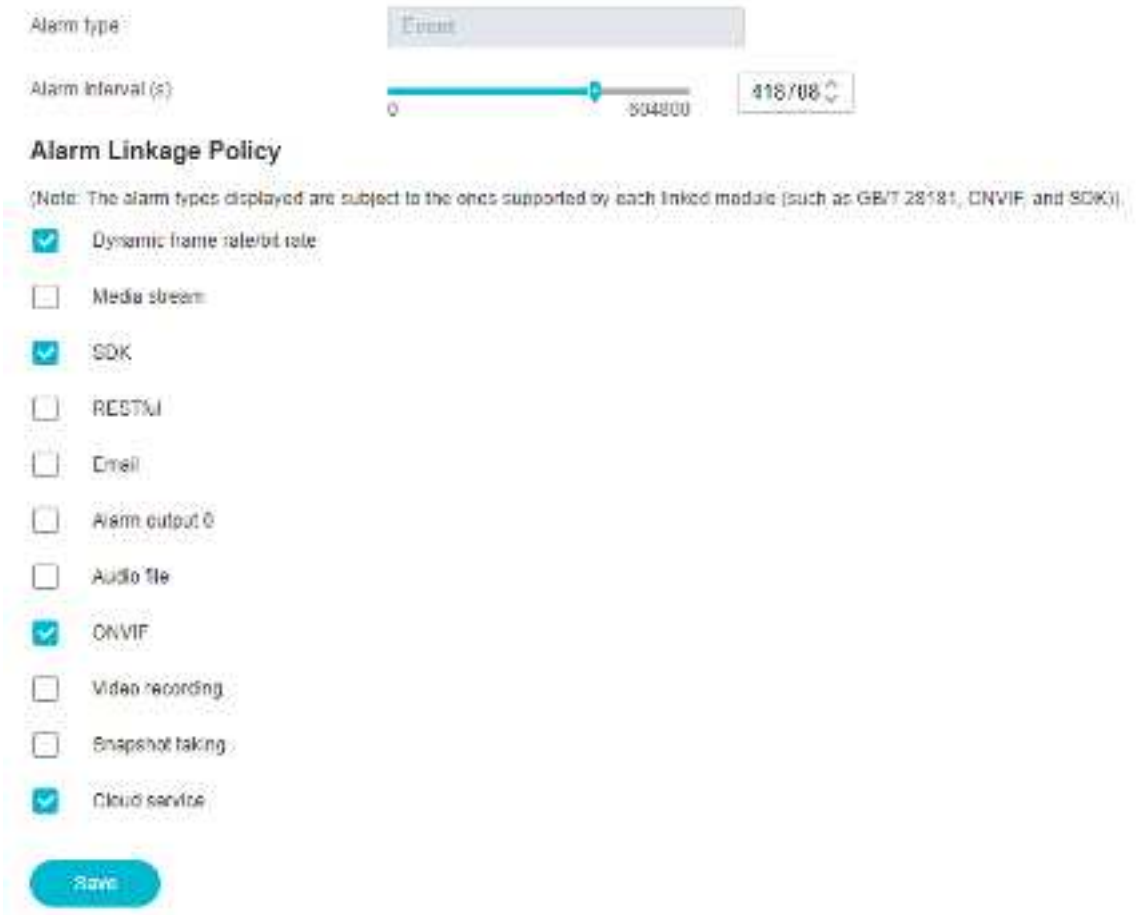
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether a lens blocking alarm is reported.

Parent topic: Event Configuration

Configuring Scene Change Detection

After the scene change detection is configured, an alarm will be generated promptly when the detection scene changes due to manual movement of the camera or other reasons.

Camera Installation and Environment Requirements

To enable scene change detection, the following camera installation and environment requirements must be met:

- It is recommended that the camera be installed at a height of 3–6 m. The recommended tilt angle is between 30° and 60°, ideally 45°.
- The light conditions of the detection environment must be stable without large-scale transient changes.
- The scene change detection applies to daylight and nighttime (greater than 20 lux) scenarios.

Configuring Scene Change Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Scene Change** and click **Basic Settings**.
3. Select **Enable** to enable scene change detection. The setting takes effect only after you click **Save**.
4. Set scene change detection parameters, as shown in Figure 1. Table 1 describes the parameters.

   The web page varies between camera models.

Figure 1 Setting scene change detection parameters

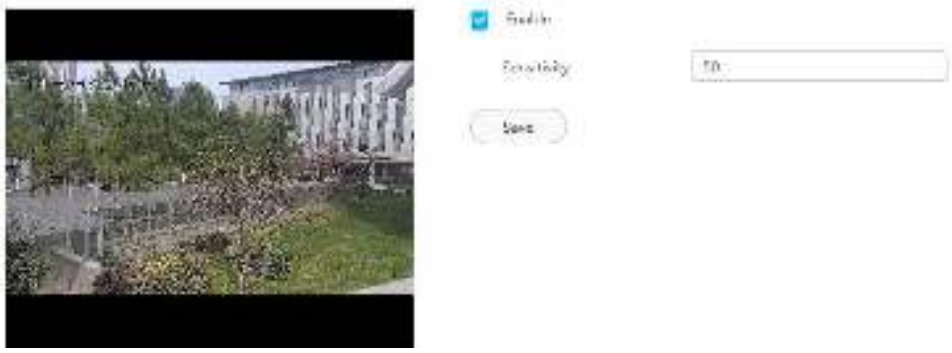


Table 1 Parameter description

Parameter	Description
Sensitivity	Scene change detection sensitivity. The value is an integer ranging from 1 to 100. The default value is **50**. A larger value indicates a higher probability to trigger alarms. **NOTE:** • In bus stations or crossroads with a heavy traffic, to prevent false alarms, it is recommended that the sensitivity be set to a value less than **20**. • For indoor scenarios that are relatively stable, it is recommended that the sensitivity be set to the default value **50**.

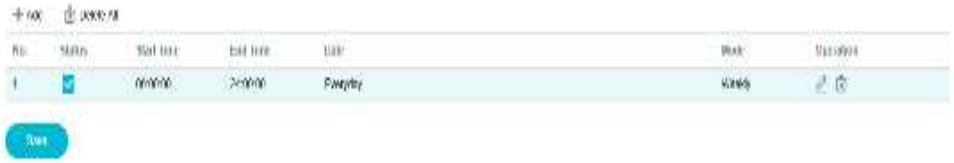
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

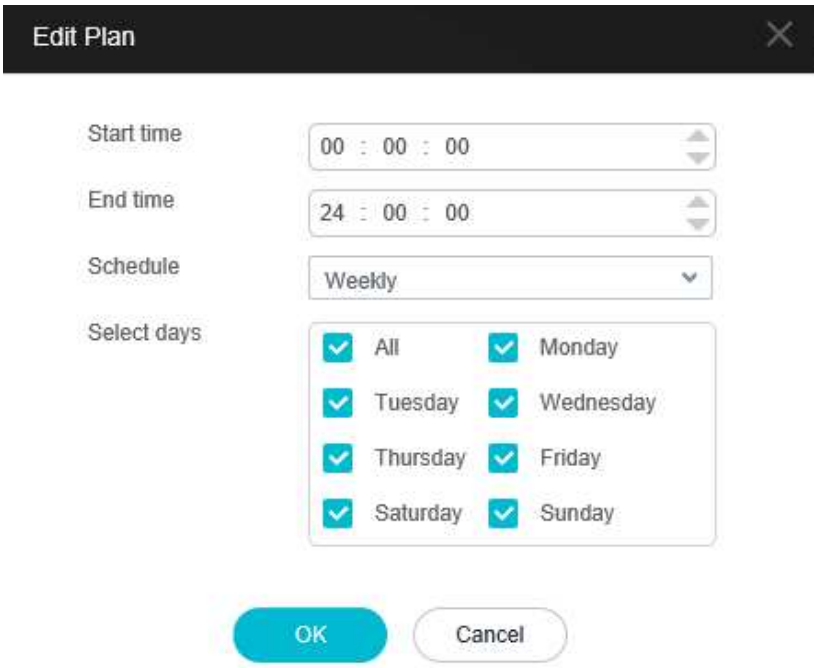
Figure 2 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click ✎ or 🗑 in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

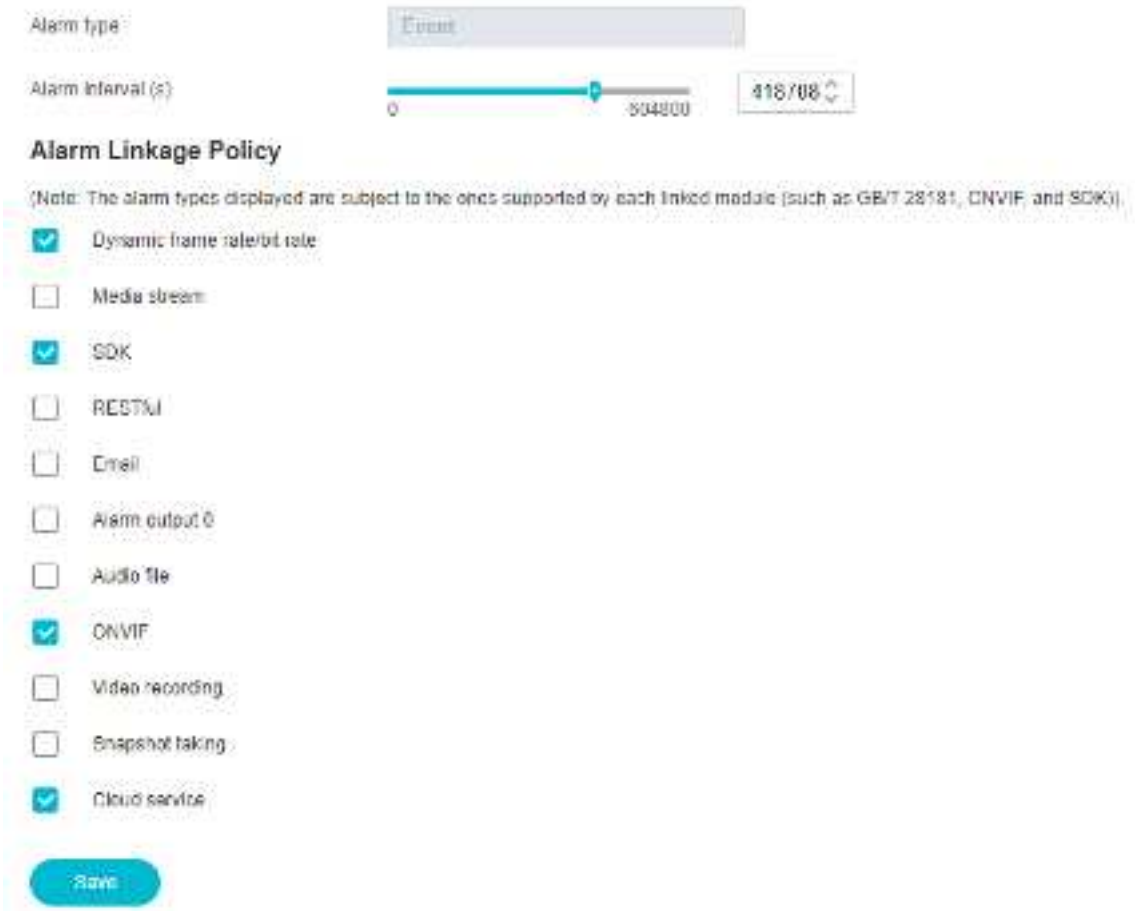
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance**, set **Log type** to **Warning** under **Log Query**, and check whether a scene change alarm is reported.

Parent topic: Event Configuration

Configuring Defocus Detection

If a camera's focal length is inappropriate, images may be unclear. You can configure defocus detection to generate alarms promptly when the camera is out of focus, reducing the cost of manual check.

Setting Defocus Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Defocus** and click **Basic Settings**.
3. Select **Enable** to enable defocus detection. The setting takes effect only after you click **Save**.
4. Set defocus detection parameters, as shown in Figure 1. Table 1 describes the parameters.

   The web page varies between camera models.

   Figure 1 Configuring defocus detection

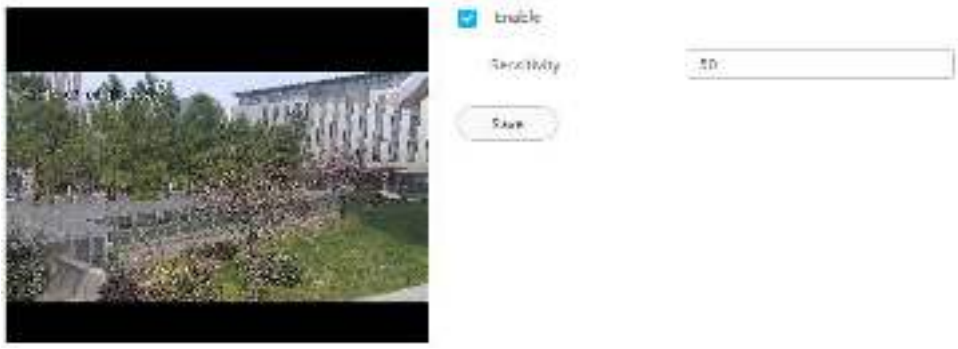


   Table 1 Parameter description

Parameter	Description
Sensitivity	Defocus detection sensitivity. The value is an integer ranging from 1 to 100. The default value is **50**. A larger value indicates a higher probability to trigger alarms. **NOTE:** • In bus stations or crossroads with a heavy traffic, to prevent false alarms, it is

Parameter	Description
	recommended that the sensitivity be set to a value less than 20. • For indoor scenarios that are relatively stable, it is recommended that the sensitivity be set to the default value **50**.

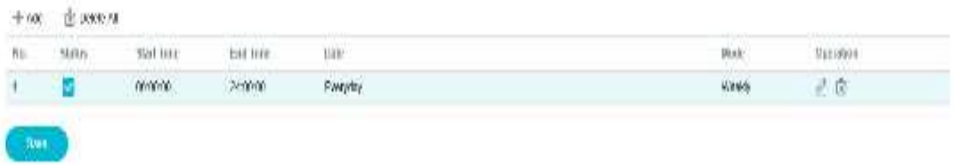
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

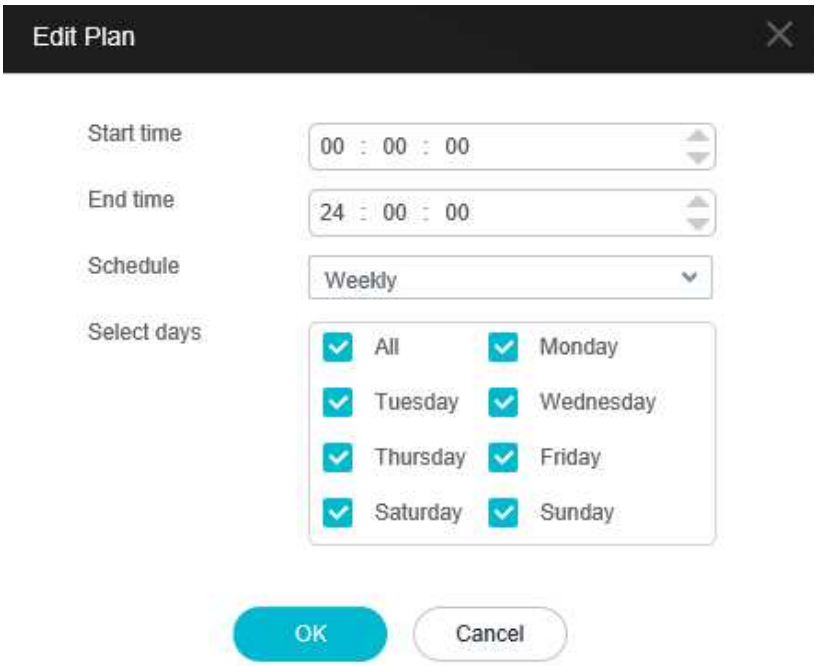
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

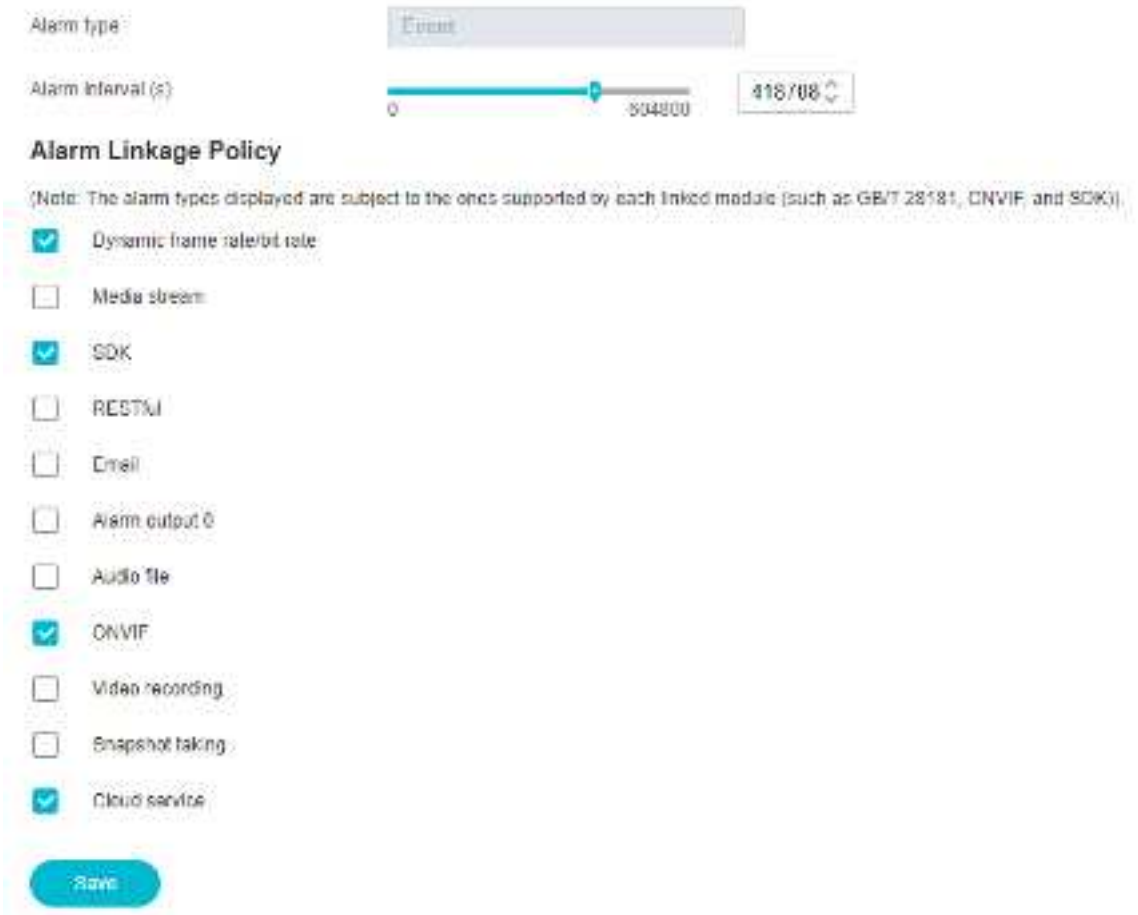
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance**, set **Log type** to **Warning** under **Log Query**, and check whether a defocus alarm is reported.

Parent topic: Event Configuration

Configuring Audio Diagnosis

This section describes how to configure audio diagnosis, including audio exception detection and sudden volume increase and decrease detection.

Configuring Audio Exception Detection You can configure audio exception detection in the camera web system. If the microphone is disconnected from the camera, an alarm is generated.

Configuring Sudden Volume Increase or Decrease Detection
The method for configuring sudden volume increase detection is the same as that for configuring sudden volume decrease detection. This section uses sudden volume increase detection configuration as an example. When detecting scream or abrupt sound change, the camera automatically generates an alarm. This feature is applicable to places such as campuses, underground walkways, and parks.

Parent topic: Event Configuration

Configuring Audio Exception Detection

You can configure audio exception detection in the camera web system. If the microphone is disconnected from the camera, an alarm is generated.

Setting Audio Exception Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Audio Diagnosis** > **Audio Exception** and click **Basic Settings**. The **Basic Settings** tab page is displayed, as shown in Figure 1.

   The web page varies between camera models.

   Figure 1 Configuring audio exception detection

3. Select **Enable**.
4. Set audio exception detection parameters. Table 1 describes the parameters.

   Table 1 Parameter description

Parameter	Description
Sensitivity	Audio exception detection sensitivity. The options are **Low**, **Medium**, and **High**, corresponding to the acoustic intensity 5, 10, or 20 respectively. When the acoustic intensity onsite is lower than the specified threshold, an alarm is generated. The default sensitivity is **Low**. You can adjust the sensitivity based on the site requirements. **NOTE:** Audio exception detection supports only line-in.

Parameter	Description

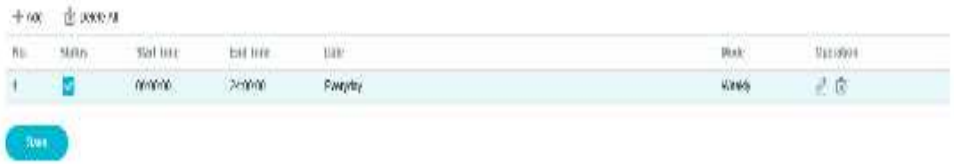
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

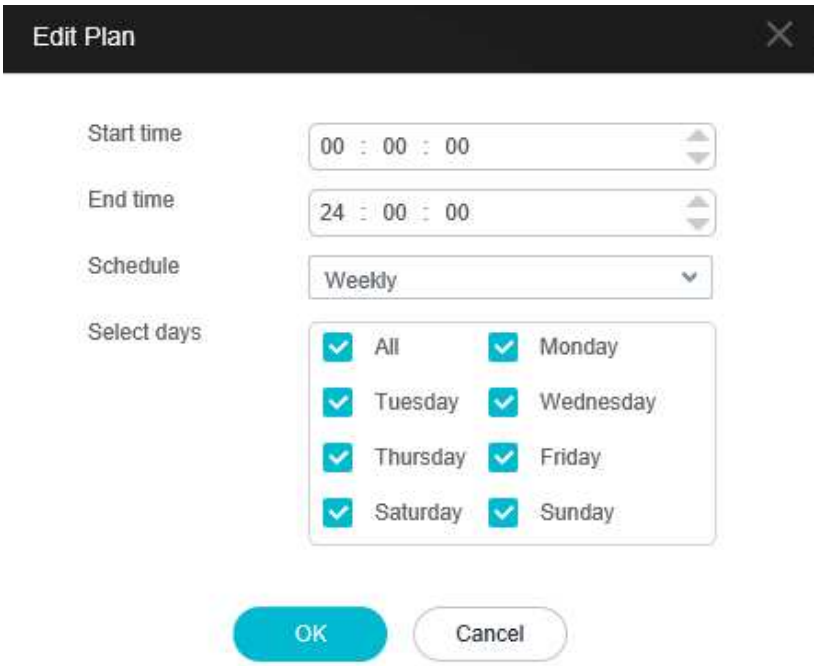
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

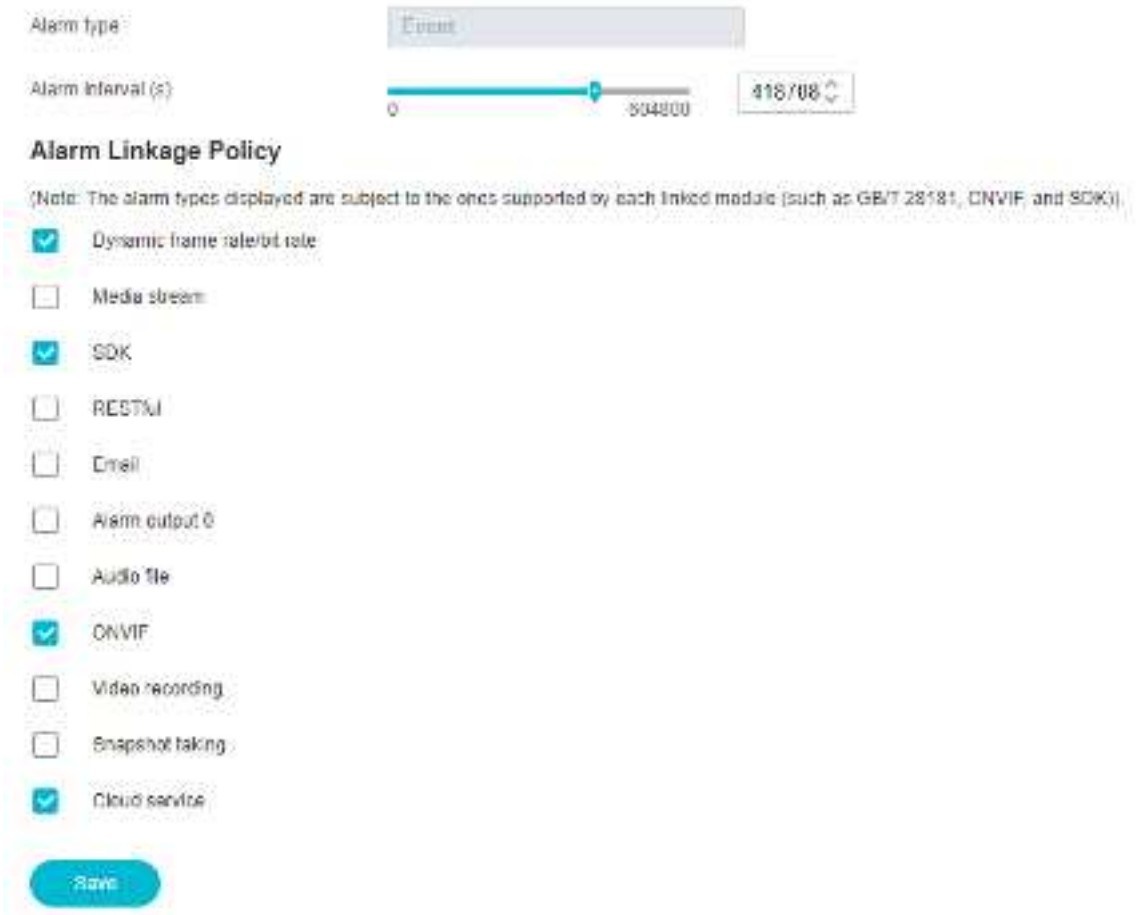
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance**, set **Log type** to **Warning** under **Log Query**, and check whether an audio exception alarm is reported.

Parent topic: Configuring Audio Diagnosis

Configuring Sudden Volume Increase or Decrease Detection

The method for configuring sudden volume increase detection is the same as that for configuring sudden volume decrease detection. This section uses sudden volume increase detection configuration as an example. When detecting scream or abrupt sound change, the camera automatically generates an alarm. This feature is applicable to places such as campuses, underground walkways, and parks.

Setting Audio Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Audio Diagnosis** > **Volume Surge** and click **Basic Settings**. The **Basic Settings** tab page is displayed, as shown in Figure 1.

   The web page varies between camera models.

   Figure 1 Configuring sudden volume increase detection

3. Select **Enable**.
4. Set volume surge detection parameters. Table 1 describes the parameters.

   Table 1 Parameter description

Parameter	Description
Sensitivity	Sensitivity for sudden volume increase detection. This parameter can be set to a value ranging from 1 to 100, and the corresponding sound intensity difference is as follows: 70 to **Sensitivity**/5.

5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 2.

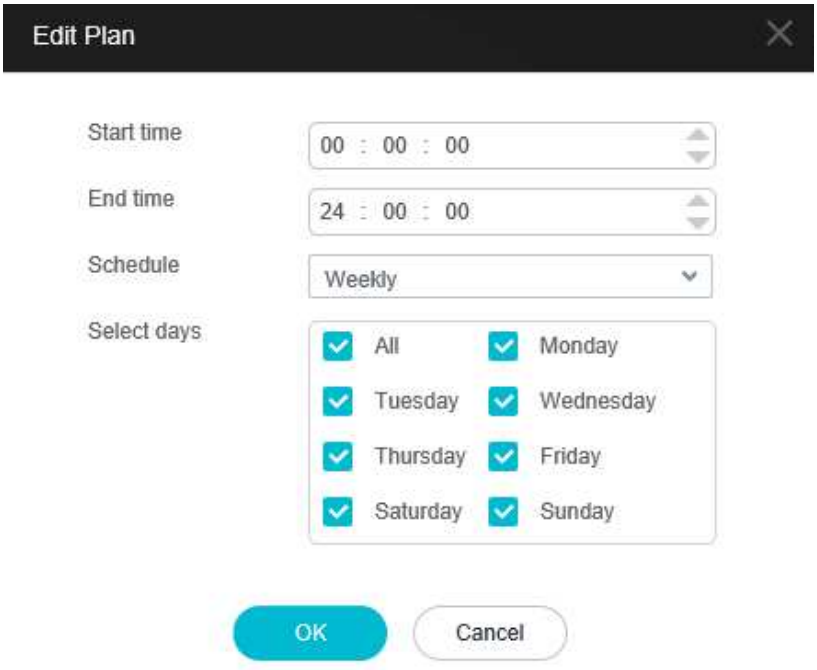
   Figure 2 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 3.

   Figure 3 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.

5. Click **Save**.

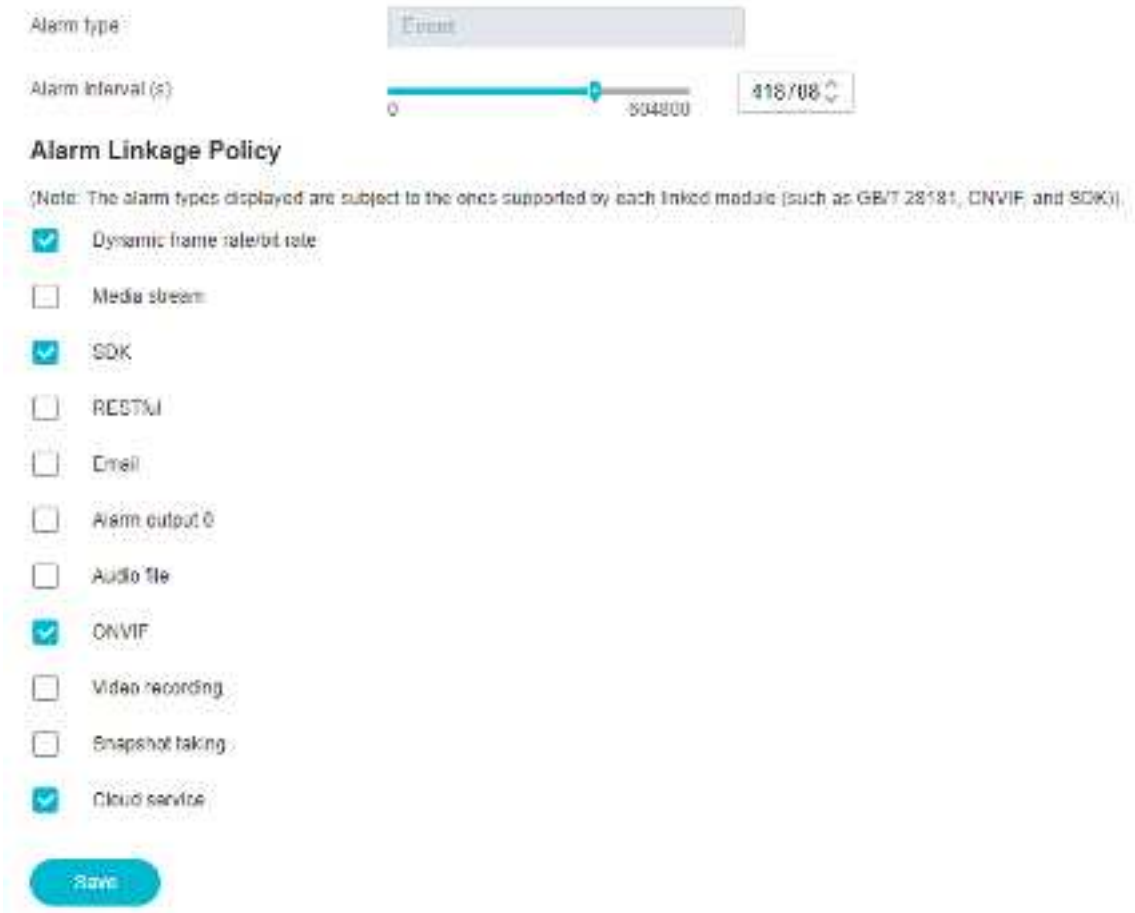
> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 4.

> **NOTICE**
>
> Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not

Parameter	Description
(s)	cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated.

Parameter	Description
	The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance**, set **Log type** to **Warning** under **Log Query**, and check whether a sudden volume increase or decrease alarm is reported.

Parent topic: Configuring Audio Diagnosis

Configuring Alarm Input and Output

You can configure the alarm input device and alarm output device. When the device receives a specified type of alarm in the alert plan period, the device takes predefined actions based on the configured alarm linkage policy.

Application Scenarios

Common alarm input devices include the door/window magnetic switch, infrared probe, and smoke sensor. Common alarm output devices include the alarm bell, speaker, and audible and visual alarm device. The following describes the major application scenarios:

- **Scenario 1**: When the camera has an external alarm input device and an alarm output device, you can set alarm input and output parameters to enable the alarm input device to link the alarm output device.

  For example, when detecting smoke, a smoke sensor, functioning as the alarm input device, generates an alarm signal and sends the signal to the camera. Then the camera links the alarm bell that functions as the alarm output device to generate an alarm sound.

- **Scenario 2**: When the camera has an external alarm input device, you can set alarm input and output parameters to enable the alarm input device to link the camera to take predefined actions.

  For example, when detecting that the door (or window) is open, a door (or window) status sensor, functioning as the alarm input device, generates an alarm signal and sends the signal to the camera. Then the camera takes snapshots or rotates to the preset position (if the camera is a PTZ dome camera).

- **Scenario 3**: When the camera has an external alarm output device, you can set alarm input and output parameters to enable

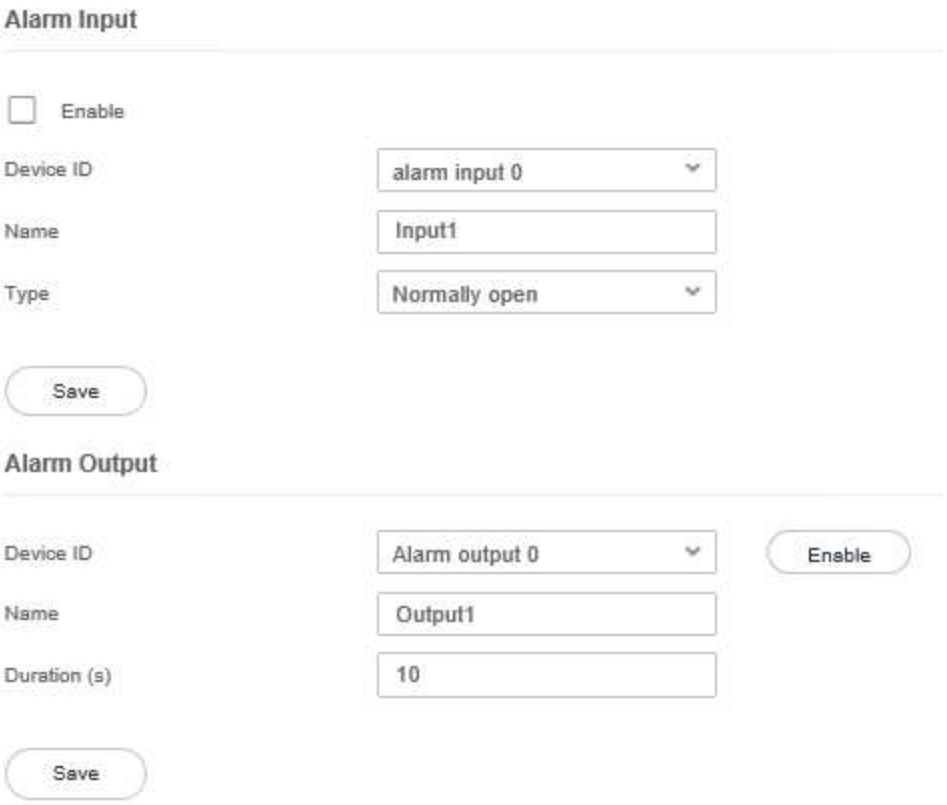
the camera to link the alarm output device to take predefined actions.

For example, the camera uses the photosensitive triggering mode to perform day/night switch. When the ambient illumination is low, the camera switches to the B/W mode and transmits signals to the illuminator that functions as the alarm output device. Then, the illuminator is enabled.

Setting Alarm Input and Output Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Alarm I/O**. The **Alarm I/O** tab page is displayed, as shown in Figure 1.

   Figure 1 Setting alarm I/O parameters



3. Set alarm input and output parameters. Table 1 describes the parameters.

Table 1 Parameter description

Parameter		Description
Alarm Input	Enable	Indicates whether to enable the alarm input function.
	Device ID	ID of the alarm input device based on the port connected to the alarm input device. The device ID starts from 0. Alarm input 0 corresponds to the device pigtail ALARM_IN0.
	Name	User-defined alarm input device name.
	Type	Alarm type. The options include **Normally open** and **Normally close**. • **Normally open**: After an alarm input device is connected to the camera, the device sends alarm information to the camera when anomalies are detected. • **Normally close**: After an alarm input device is connected to the camera, the device continuously sends alarm information to the camera no matter whether anomalies are detected.

Parameter		Description
Alarm Output	Device ID	ID of the alarm output device based on the port connected to the alarm output device. The device ID starts from 0. Alarm output 0 corresponds to the device pigtail ALARM_OUT0.
		Button for manually enabling or disabling the alarm output device. If you click **Enable**, the alarm output device generates an alarm (for example, an audible and visual alarm). The alarm output device stops after you click **Disable** or after the specified duration elapses. **NOTE:** You are advised not to use this function together with the alarm linkage function. Otherwise, the alarm linkage result will be affected.
	Name	User-defined alarm output device name.
	Duration (s)	Duration that an output alarm lasts. **NOTE:** If **Duration (s)** is set to **0**, the alarm persists permanently.

4. Click **Save**.

Parent topic: Event Configuration

Configuring Certificate Expiration Alarm

After the certificate expiration alarm is set, the system will automatically display a message prompting users to update the certificate when the certificate is to expire in specified number of days.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **Certificate Expiration Alarm**. The **Certificate Expiration Alarm** tab page is displayed, as shown in Figure 1.

   Figure 1 Configuring certificate expiration alarm

3. Set **Alarm lead time (days)**.

   NOTE

   When the remaining validity period of the certificate reaches the value specified by **Alarm lead time (days)**, the system automatically reports an alarm to users.

4. Click **Save**.

Parent topic: Event Configuration

Configuring System Intrusion Detection

This section describes how to configure system intrusion detection. After configuration, the system can detect and intercept intrusions in a timely manner.

The networking feature of the network video recorder (NVR) results in frequent security vulnerabilities. In recent years, many Internet of Things (IoT) security events are related to camera system intrusion. A host intrusion detection system can be installed on cameras to provide multi-layer visual intrusion detection capabilities for the cameras. This system can detect hacker intrusions at the first time to ensure the camera security. The system intrusion detection function can detect and intercept intrusions in a timely manner. The system intrusion detection includes promiscuous network adapter detection, sensitive file detection, unauthorized account detection, Botnet detection, RootKit detection, process trustlist detection, cryptojacking malware detection, and privilege escalation detection.

NOTE

Different camera models support different detection functions.

Promiscuous Network Adapter Detection

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Promiscuous NIC**. The **Promiscuous NIC** tab page is displayed.
3. Select **Enable** to enable the promiscuous network adapter detection function, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 Configuring promiscuous network adapter detection

   Table 1 Parameter description

Parameter	Description
Interval (s)	Alarm check interval.

4. Click **Save**.

Sensitive File Detection

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Sensitive File**. The **Sensitive File** tab page is displayed.
2. Select **Enable** to enable the sensitive file detection function, as shown in Figure 2. Table 2 describes the parameters.

   Figure 2 Configuring sensitive file detection

   Table 2 Parameter description

Parameter	Description
File path	Multiple file paths are separated by commas (,), for example, **/filePath,/filePath,/filePath**.

3. Click **Save**.

   The sensitive file detection function is configured.

Unauthorized Account Detection

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Unauthorized Account**. The **Unauthorized Account** tab page is displayed.
2. Select **Enable** to enable the unauthorized account detection function, as shown in Figure 3. Table 3 describes the parameters.

Figure 3 Configuring unauthorized account detection



Table 3 Parameter description

Parameter	Description
Interval (s)	Alarm check interval.

3. Click **Save**.

   The unauthorized account detection function is configured.

Botnet Detection

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Botnet**. The **Botnet** tab page is displayed.
2. Select **Enable** to enable the Botnet detection function, as shown in Figure 4. Table 4 describes the parameters.

   Figure 4 Configuring Botnet detection



Table 4 Parameter description

Parameter	Description
Interval (s)	Alarm check interval.
IP trustlist	A trustlist contains the IP addresses of platforms to which a camera can proactively connect. If a platform IP address is in the trustlist, the camera proactively connects to the platform without checking whether the network is a Botnet based on the feature database. If a platform IP address is not in the trustlist, the camera checks whether

Parameter	Description
	the network is a Botnet based on the feature database before connecting to the platform. **NOTE:** Multiple IP addresses are separated by commas (,), for example, 10.10.10.10,10.10.10.11.

3. Click **Save**.

   The Botnet detection function is configured.

RootKit Detection

RootKit is the most common Trojan horse backdoor tool in the Linux system. It is used to replace system files to hide the intrusion. RootKit detection is used to check whether the server is infected with RootKit.

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **RootKit**. The **RootKit** tab page is displayed.
2. Select **Enable** to enable the Rootkit detection function, as shown in Figure 5. Table 5 describes the parameters.

   Figure 5 Configuring RootKit detection

   Table 5 Parameter description

Parameter	Description
Interval (s)	Alarm check interval.

3. Click **Save**.

   The RootKit detection function is configured.

Process Trustlist Detection

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Process Trustlist**. The **Process Trustlist** tab page is displayed.
2. Select **Enable** to enable the process trustlist detection function, as shown in Figure 6. Table 6 describes the parameters.

   Figure 6 Configuring process trustlist detection

   Table 6 Parameter description

Parameter	Description
Process trustlist	Multiple trustlisted processes are separated by commas (,), for example, **/filePath,/filePath,/filePath**.
Directory trustlist	Multiple trustlisted directories are separated by commas (,), for example, **/filePath,/filePath,/filePath**.

3. Click **Save**.

   The process trustlist detection function is configured.

Cryptojacking Malware Detection

1. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Cryptojacking**. The **Cryptojacking** tab page is displayed.
2. Select **Enable** to enable the cryptojacking detection function, as shown in Figure 7. Table 7 describes the parameters.

   Figure 7 Configuring cryptojacking malware detection

Table 7 Parameter description

Parameter	Description
Hash trustlist	The value can contain a maximum of 64 characters, including only lowercase letters (a to f) and digits (0 to 9).
File trustlist	Multiple file paths are separated by commas (,), for example, **/filePath,/filePath,/filePath**.

3. Click **Save**.

   The cryptojacking process detection function is configured.

Privilege Escalation Detection

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Detection** > **System Intrusion Alarm** and click **Privilege Escalation**. The **Privilege Escalation** tab page is displayed.
3. Select **Enable** to enable the privilege escalation detection function, as shown in Figure 8. Table 8 describes the parameters.

   Figure 8 Configuring privilege escalation detection

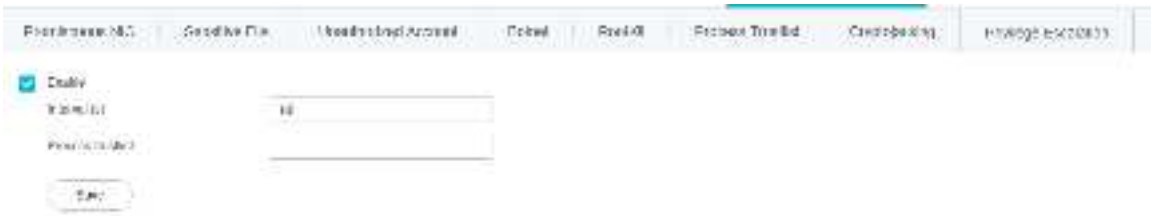


   Table 8 Parameter description

Parameter	Description
Interval (s)	Alarm check interval.
Process trustlist	Multiple trustlisted processes are separated by commas (,), for example, **/filePath,/filePath,/filePath**.

4. Click **Save**.

   The privilege escalation detection function is configured.

Storage Configuration

This section describes how to configure functions including storage management, snapshot taking parameters, and recording plans.

Configuring Storage Management Using the storage management function, you can view the SD card status, limit the rate, conduct cyclic recording, and enable encrypted storage of video and images.

Setting Snapshot Parameters
You can set snapshot parameters such as the snapshot storage space in the SD card, snapshot format, and the snapshot interval.

Configuring a Recording Plan
After a video recording plan is configured, the system automatically records video as scheduled.

Parent topic: Configuration

Configuring Storage Management

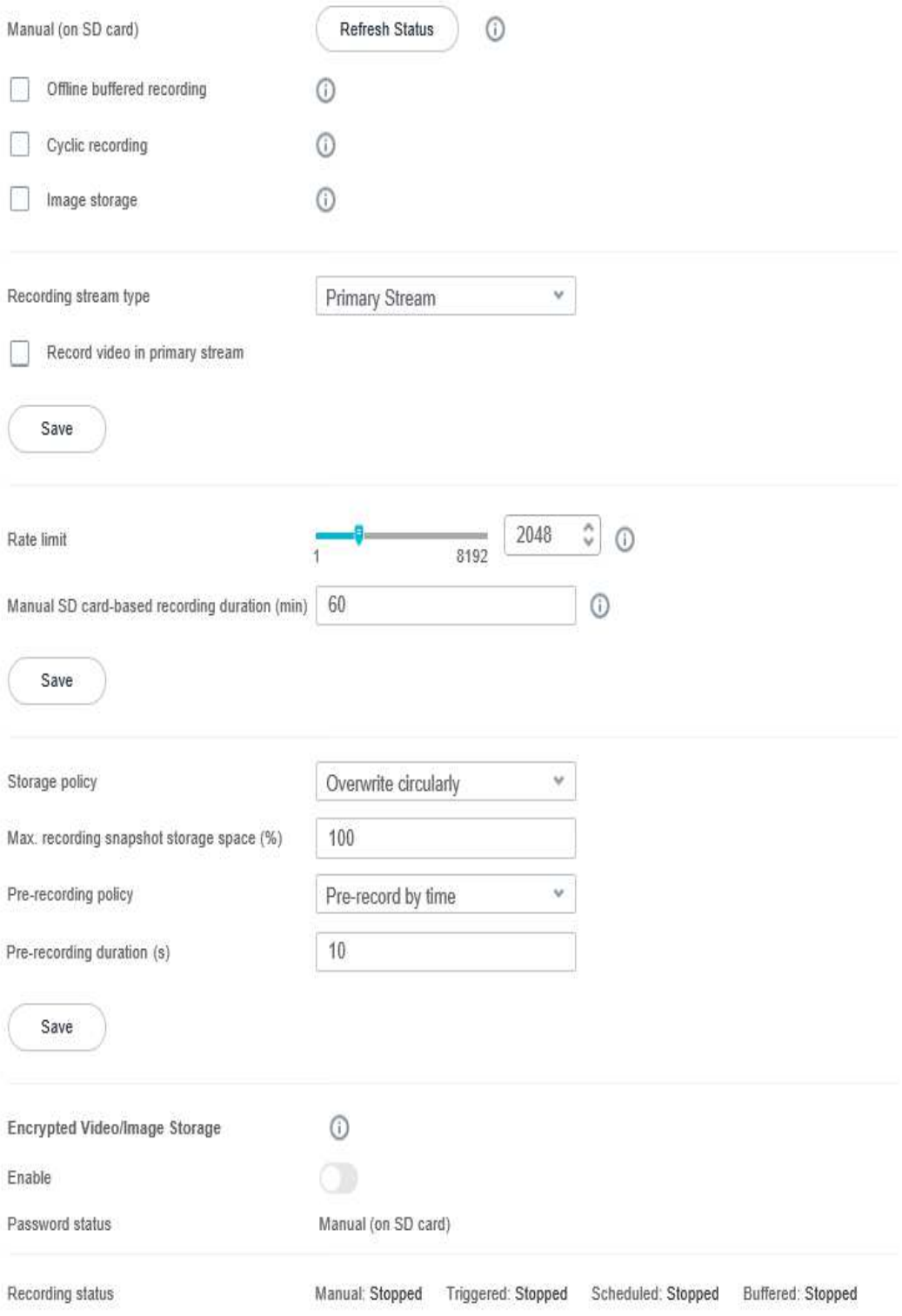
Using the storage management function, you can view the SD card status, limit the rate, conduct cyclic recording, and enable encrypted storage of video and images.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Storage** > **Storage Management**. The **Storage Management** tab page is displayed, as shown in Figure 1.

   The web page varies depending on the camera model.

Figure 1 Storage Management page



3. Select a channel type and set related parameters. Table 1 describes the parameters.

Table 1 Storage management parameters

Parameter	Description

Parameter		Description
SD card management	No SD card	Indicates that there is no SD card on the camera.

Parameter		Description
	SD card status	Total storage capacity and occupied space of an SD card.
	Instant Formatting	Indicates whether to format an SD card. **NOTE:** • Format an SD card during off-peak hours. • Before using an SD card, format it. • Back up data before formatting an SD card. • All data will be lost after an SD card is formatted. Exercise caution when performing this operation. • Do not remove an SD card when it is being formatted or data-written. • If the capacity status of the SD card does not change after the SD card is formatted, the SD card may be faulty. You are advised to replace the SD card and format it again. • If the camera is powered off during SD card formatting, an SD card exception may occur and an error message is displayed. • Use a compatible SD card. If you use an SD card that is not in the

Parameter		Description
		compatibility list, compatibility issues may occur.
	Refresh Status	Displays the latest SD card status.
Offline buffered recording		Indicates whether to allow cameras disconnected from the network to continue to shoot and temporarily store video on their SD cards. When the network is restored, the video security platform sends a video request to the cameras. The cameras then send the video stored on the SD cards to the video security platform. This function is disabled by default. **NOTE:** • This function does not support the MJPEG protocol. • If the camera fails to connect to the platform for a long time or does not connect to the platform, you are advised to manually disable the video buffering function of the camera to prolong the service life of the SD card. • When the SD card is full, the recording stops or overwrites previous recordings based on the storage policy. • Whether video buffering can be triggered by a platform media stream session exception depends on the transmission

Parameter	Description
	protocol used and whether the platform supports media session keepalive. If the platform does not support the function of sending keepalive messages and UDP is used to request media streams, video buffering will not be triggered by a session exception.
Cyclic recording	Indicates whether to enable cyclic recording. If this parameter is selected, the recordings will be saved to the SD card. **NOTE:** • This function is invalid when the MJPEG encoding protocol is used. • Cyclic recording will result in frequent writes to the SD card, which will shorten the SD card's service life. • When the SD card is full, the recording stops or overwrites previous recordings based on the storage policy.
Image storage	Indicates whether to save snapshots to the SD card. **NOTE:** Enabling the image storage function will save snapshots to the SD card.

Parameter	Description
	When the image storage space reaches 90%, new images will overwrite earlier images. You can choose whether to enable this function based on the service scenario and the space allocated by the SD card for image storage.
Recording stream type	Type of streams in which subsequent video is recorded.
Record video in primary stream	Indicates whether to record video in the type of primary streams. **NOTE:** • Before selecting this parameter, ensure that **Video recording** is selected under **Configuration** > **Service** > **Alarm Service** > **Alarm Input** > **Common Alarm** > **Alarm Linkage Policy**. • If you set **Recording stream type** to **Primary Stream**, video is recorded in the type of primary streams no matter whether **Record video in primary stream** is selected.
Rate limit	Maximum upload rate for video buffering or the download rate for SD card recording. It is recommended that the value be a quarter of the primary stream bit rate and not exceed the available bandwidth.

Parameter	Description
	NOTE: • The video buffering function occupies additional network bandwidth. If the value exceeds the available bandwidth, network congestion may occur, which leads to image exceptions. Set **Rate limit** based on the site requirements. • The rate for downloading recordings in the SD card can be adjusted. However, the rate cannot be adjusted during the download.
Manual SD card-based recording duration (min)	Duration for recording video on the SD card on the **View** page. After this function is enabled, the recording automatically stops when the specified duration arrives. The recording duration ranges from 5 minutes to 1440 minutes.
Storage policy	• **Overwrite circularly**: After the video recording or snapshot taking function is enabled, recordings and snapshot images are saved on the SD card. When the SD card space is used up, the earliest recording files and images are automatically overwritten. • **Stop**: After the video recording or snapshot taking function is enabled, recordings and

Parameter	Description
	snapshot images are saved on the SD card. When the SD card space is used up, the camera stops recording video or taking snapshots.
Max. recording snapshot storage space (%)	Maximum space for storing recordings and snapshots, in percentage. The value is an integer ranging from 1 to 100. The default value is **100**.
Pre-recording policy	Policy for the camera to move the recording during a certain period (configurable) before an occurring alarm from the memory to the SD card. The pre-recording policies include **No pre-recording**, **Pre-record by time**, and **Pre-record by memory capacity**. If **Pre-recording policy** is set to **Pre-record by time**, set the pre-recording period before the alarm based on the site requirements. **NOTE:** • Parking violation detection PTZ dome cameras and ITS cameras do not support pre-recording policy configuration. • The **Pre-record by time** option is not available for light intelligence and inclusive intelligence camera models. • If **Pre-recording policy** is set to **Pre-record by memory**

Parameter	Description
	capacity, pre-recording duration is inversely proportional to bit rate. That is, a higher bit rate indicates a shorter pre-recording duration.
Pre-recording duration (s)	Pre-alarm recording duration.

NOTE

Under **Recording status**, you can view the status of recordings of different types.

- **Running**: The recording is enabled.
- **Stopped**: The recording is disabled.

4. Determine whether to enable encrypted storage of video and images. If this function is enabled, video and images on the SD card will be encrypted for storage and can be viewed only through a password. For details, see Table 2.

Table 2 Storage encryption operations

Operation	Description
Enable/Disable encrypted video and image storage	• If this function is enabled for the first time, a password must be set for decrypting video and image storage. **NOTE:** The password cannot be retrieved after it is lost. Keep the password safe. • If this function is disabled, the new video and images will not be encrypted, and

Operation	Description
	encrypted data is not decrypted. If this function is disabled and enabled again, you need to enter the password. If you forget the password, you can reset the password. **NOTE:** Enabling this function will occupy more system resources. After this function is enabled, an exception may occur on services when all services are configured. To enable this function, you are advised to disable the intelligent service.
Change the password	You can change the password depending on your needs. You can change the password only after the password passes the verification.
Reset the password	If you forget the password or the SD card is replaced or formatted, you can reset the password. **NOTE:** If the password after the reset is different from the old password, the video and image encrypted using the old password cannot be read unless you change the password back to the old one.

NOTE

- Configurations that have been encrypted for storage cannot be backed up through configuration file management.

- If the system is rolled back to a version that does not support encrypted storage, encrypted data cannot be decrypted.
- Cameras with light intelligence and inclusive intelligence do not support encrypted storage.

Parent topic: Storage Configuration

Setting Snapshot Parameters

You can set snapshot parameters such as the snapshot storage space in the SD card, snapshot format, and the snapshot interval.

NOTICE

- Scheduled snapshot will result in frequent writes to the SD card, which will shorten the SD card's service life.
- Before setting snapshot parameters, you need to select a required channel.

Configuring the SD Card Space You can configure the SD card space for storing snapshots.

Configuring Image Quality
You can configure image quality to control the snapshot quality and size.

Configuring Scheduled Snapshot
You can set scheduled snapshot parameters, including the snapshot format and interval, to enable the camera to take snapshots at a specified interval.

Configuring Snapshot Retransmission
You can re-upload snapshots that fail to be uploaded to the FTP/SFTP server.

Configuring Intelligent Image Data
After intelligent image data is enabled, you can obtain images that contain intelligent information.

Parent topic: Storage Configuration

Configuring the SD Card Space

You can configure the SD card space for storing snapshots.

Procedure

1. Choose **Configuration** > **Storage** > **Snapshot Parameters** > **SD Card Space**. The **SD Card Space** area is displayed.
2. Set **Snapshot space (%)**. After the parameter is set, the available snapshot storage space on the SD card will be displayed as the value of **Snapshot space (MB)**, as shown in Figure 1.

   Figure 1 Setting the SD card space

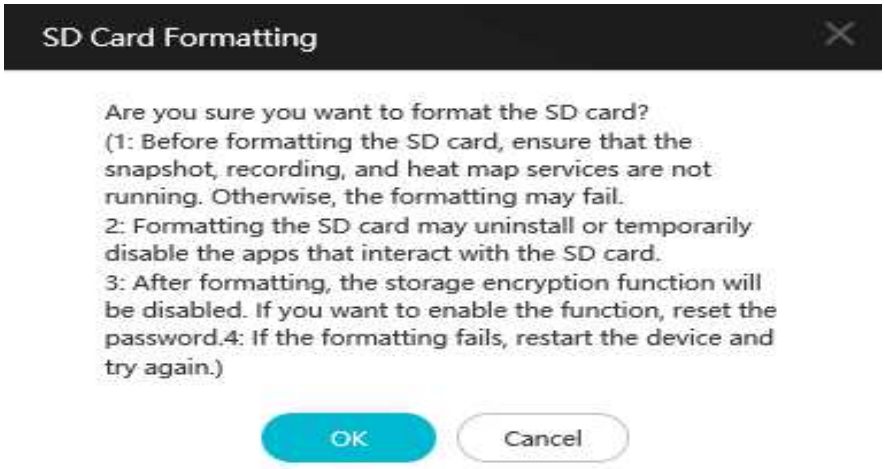
   NOTE

   - You need to format the SD card before using it for the first time. For details, see Configuring Storage Management.
   - The value of **Snapshot space (MB)** is calculated as follows: Snapshot space (MB) = Total SD card capacity x Value of **Max. recording snapshot storage space (%)** x Value of **Snapshot space (%)**. For details about the total SD card capacity and maximum recording snapshot storage space, see Configuring Storage Management.
   - The write speed of a Class 10 microSD card is 8 MB/s or higher. The write speed of microSD cards of some brands can reach 16 MB/s. When multiple storage devices are enabled simultaneously (for example, video recording and snapshot taking are enabled simultaneously), a high-speed card (for example, SDXC U3) is recommended to prevent loss of recordings or images stored on the microSD card due to insufficient storage performance.

3. Click **Save**.

   If the SD card is inserted, after the settings are saved, the dialog box shown in Figure 2 is displayed.

   Figure 2 SD Card Formatting dialog box



   NOTE

   - Format the SD card during off-peak hours.
   - Back up data before formatting the SD card.
   - All data will be lost after the SD card is formatted. Exercise caution when performing this operation.

4. Click **OK** to format the SD card.

Parent topic: Setting Snapshot Parameters

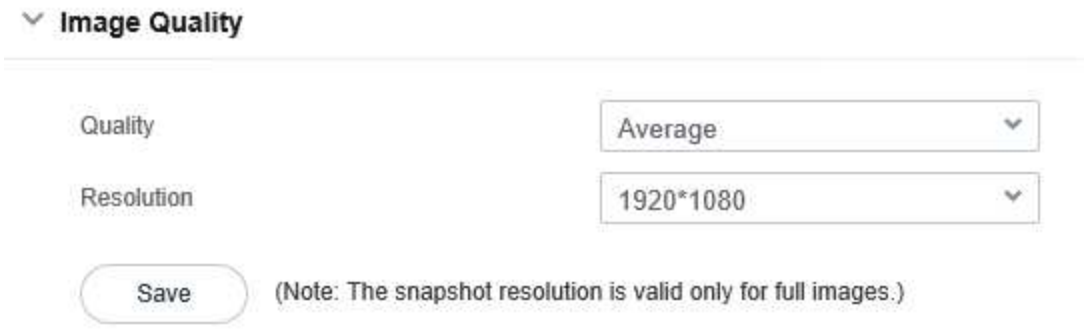
Configuring Image Quality

You can configure image quality to control the snapshot quality and size.

Procedure

1. Choose **Configuration** > **Storage** > **Snapshot Parameters** > **Image Quality**. The **Image Quality** area is displayed, as shown in Figure 1.

   Figure 1 Image Quality area

2. Set **Quality** and **Resolution** based on the site requirements.
3. Click **Save**.

Parent topic: Setting Snapshot Parameters

Configuring Scheduled Snapshot

You can set scheduled snapshot parameters, including the snapshot format and interval, to enable the camera to take snapshots at a specified interval.

> **NOTE**
>
> After the snapshot taking function is enabled, if the camera is powered off unexpectedly during snapshot taking, data may not be completely saved or written. As a result, the saved snapshot may be corrupted.

Procedure

1. Choose **Configuration** > **Storage** > **Snapshot Parameters** > **Scheduled Snapshot**. The **Scheduled Snapshot** area is displayed, as shown in Figure 1.

   Figure 1 Scheduled Snapshot area

2. Select **Enable**.
3. Set **Interval (s)**, at which snapshots are taken.

   > **NOTE**
   >
   > Currently, only the JPG format is supported.

4. Click **Save**.

Parent topic: Setting Snapshot Parameters

Configuring Snapshot Retransmission

You can re-upload snapshots that fail to be uploaded to the FTP/SFTP server.

Procedure

1. Choose **Configuration** > **Storage** > **Snapshot Parameters** > **Snapshot retransmission**. The **Snapshot retransmission** area is displayed, as shown in Figure 1. Table 1 describes the parameters in this area.
2. Select **Snapshot retransmission**. A message is displayed indicating that the setting is successful.

   Figure 1 Snapshot retransmission area

   Table 1 Snapshot retransmission parameters

Parameter	Description
Snapshot retransmission	Indicates whether to enable snapshots that fail to be uploaded due to a fault (for example, network disconnection) to be re-transmitted to the FTP/SFTP server after the fault is rectified.

Parent topic: Setting Snapshot Parameters

Configuring Intelligent Image Data

After intelligent image data is enabled, you can obtain images that contain intelligent information.

Procedure

1. Choose **Configuration** > **Storage** > **Snapshot Parameters** > **Intelligent Image Data**. The **Intelligent Image Data** area is displayed, as shown in Figure 1. Table 1 describes the parameters in this area.
2. Select **Enable intelligent image data**. A message indicating setting success is displayed.

   Figure 1 Intelligent Image Data area

   Table 1 Intelligent image data parameters

Parameter	Description
Enable intelligent image data	After the function is enabled, the intelligent information of images can be encapsulated into JPEG images in the JSON structure. In this way, after obtaining the images, the platform can obtain intelligent information of the images. The function is enabled by default.

Parent topic: Setting Snapshot Parameters

Configuring a Recording Plan

After a video recording plan is configured, the system automatically records video as scheduled.

NOTICE

The recordings mentioned in this section are saved in the SD card of the camera. Ensure that an SD card has been installed on the camera. All-day recording will frequently write data into the SD card, which shortens the SD card's service life. You need to format the SD card before using it for the first time. For details, see Configuring Storage Management.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Storage** > **Recording Plan**. The **Recording Plan** tab page is displayed, as shown in Figure 1.

   Figure 1 Recording Plan tab page

3. Set **Channel** and select **Enable plan**.
4. Click **Add**. In the dialog box that is displayed, set **Start time** and **End time**, as shown in Figure 2.

   A maximum of 24 recording plans are supported.

Figure 2 Adding a recording plan



5. (Optional) To modify or delete an existing recording plan, select it and click or .
6. (Optional) To delete all recording plans, click **Delete All**.
7. Click **Save**.

Parent topic: Storage Configuration

Service Management

This chapter describes the alarm feature differences, extended interface service, alarm service, channel service, and general configuration service of cameras.

Alarm Feature Differences

Extended Interface Service
On the **Extension Interface** page, you can configure various external devices with RS-485 ports.

Alarm Service

Channel Service

General Configuration Service

Parent topic: Configuration

Alarm Feature Differences

This section describes differences in alarm linkage configurations supported by different camera models.

> **NOTE**
>
> This table lists only the configuration items that vary depending on camera models. Common configuration items are not described here.

Table 1 Differences in alarm features of the D series cameras

Device Model	Preset Position Rotation	Tour	Scan	Email Sending	Onboard Video Recording	Onboard Snapshot Taking
HWT-D2122-10-SIU	NO	NO	NO	YES	YES	YES
HWT-D2152-10-SIU	NO	NO	NO	YES	YES	YES
HWT-D3222-10-SIU	NO	NO	NO	YES	YES	YES
HWT-D3252-10-SIU	NO	NO	NO	YES	YES	YES
HWT-D6550-10-Z33-SV	YES	YES	YES	YES	YES	YES
HWT-D3040-10-	NO	NO	NO	YES	YES	YES

Device Model	Preset Position Rotation	Tour	Scan	Email Sending	Onboard Video Recording	Onboard Snapshot Taking
ELI-PV (2.8 mm)						

Parent topic: Service Management

Extended Interface Service

On the **Extension Interface** page, you can configure various external devices with RS-485 ports.

RS-485 Port Configuration This section describes how to set RS-485 port parameters to connect the camera to an external device.

Parent topic: Service Management

RS-485 Port Configuration

This section describes how to set RS-485 port parameters to connect the camera to an external device.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **Extension Interface** > **RS-485**. The **RS-485** tab page is displayed.
3. Select **Enable**, enable the desired RS-485 port, and select the external device as required, as shown in Figure 1. Table 1 describes the external device parameters.

   Camera models of different series may have different parameters.

   Figure 1 Configuring external devices with RS-485 ports

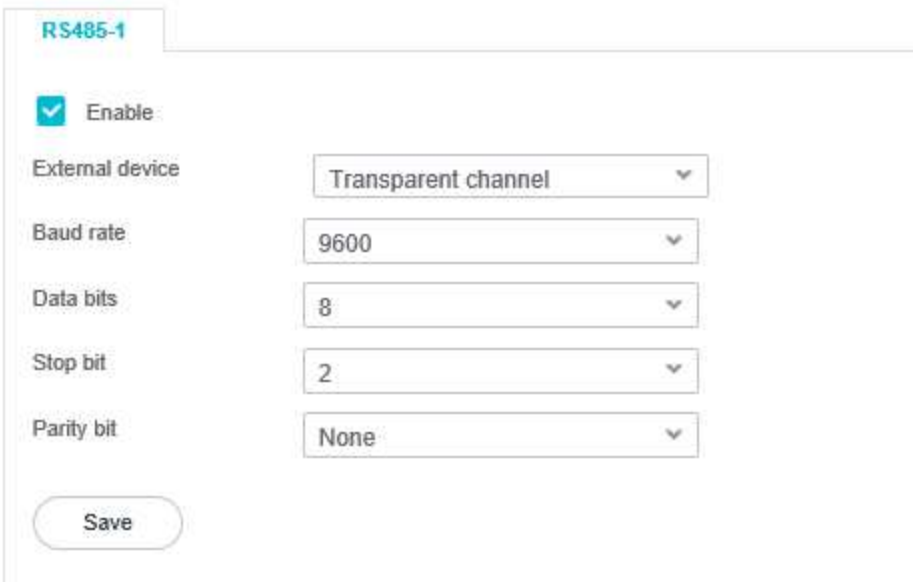


Table 1 External device parameters

Parameter	Description

Parameter	Description
External device	• After the transparent channel is configured, users can use the SDK protocol and external serial port to transmit data.
Baud rate	Communication rate, which must be the same as that of the connected device.
Data bits	Actual number of data bits used for communication.
Stop bit	Number of bits used for marking the end of the serial port data.
Parity bit	Method to check the serial port data.

4. Click **Save**.

Parent topic: Extended Interface Service

Alarm Service

- **Alarm Input**
- **Alarm Linkage Policy Description**

Parent topic: Service Management

Alarm Input

On the **Alarm Input** tab page, you can configure common and intelligent alarms generated by cameras. You can also configure alarm input parameters, linkage policies, and alert time segments for a registered third-party platform. The alarm input parameters may vary depending on camera models.

Figure 1 Alarm Input tab page



Table 1 Configurable alarm types and alarm linkage

Parameter	Description
Alarm Linkage	• The settings under **Alarm Linkage** are applied in the alarm linkage policies of all alarm events. For example, if you deselect **SDK** under **Alarm Linkage** and click **Save**, the SDK function is disabled in the alarm linkage policies of all alarm events. • Before configuring an alarm linkage policy for an alarm event, you need to enable required functions under **Alarm Linkage**.
Common alarm	Alarms about media stream interruption, full disk, disk removal, disk read and write failure, Boolean value, log storage, flash read and write, temperature sensor fault, network port hot swap, video loss, lens PT optocoupler failure, upgrade and rollback, system temperature, PTZ device configuration, and PTZ optocoupler failure.

Parameter	Description
Intelligent alarm	Alarms upon fog, motion, lens blocking, automatic tracking, crowd gathering, abnormal crowd density, intrusion, tripwire crossing, loitering, area entry, area exit, fast movement, abandoned object, removed object, head counting, queue length, fight, climbing, fall, running, target detection, sound, sudden volume increase or decrease, scene change, defocus, and alarms upon image anomalies such as shaking, freezing, static noise, stripe noise, gain imbalance, and color cast. **NOTE:** To configure intelligent alarms, you need to install corresponding algorithm package.

Setting Alarm Input Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **Alarm Service** > **Alarm Input**. The **Alarm Input** tab page is displayed.
3. Select the alarm to be configured and click **Alarm Input Parameters**.

   Different alarm services require different alarm input parameters. Table 2 describes the parameters.

   Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.

Parameter	Description
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.

4. Click **Save**.

Configuring an Alarm Linkage Policy

The alarm linkage actions vary between camera models. Some camera models do not support alarm linkage and you do not need to configure alarm linkage policies for them.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **Alarm Service** > **Alarm Input**. The **Alarm Input** tab page is displayed.
3. Select the alarm to be configured and click **Alarm Linkage Policy**. The **Alarm Linkage Policy** area is displayed, as shown in Figure 2.

   Different camera models support different alarm linkage policies.

   NOTE

   You are advised to configure one alarm linkage policy for a camera connected to the platform.

Figure 2 Configuring an alarm linkage policy



4. Set alarm linkage policy parameters. Table 3 describes the parameters.

   The alarm types displayed to external systems are subject to the ones supported by each linkage module (such as GB/T 28181, ONVIF, and SDK). For example, GB/T 28181 does not support the lens PT optocoupler fault alarm. You can select **T28181** when configuring alarm linkage policies for the lens PT optocoupler fault alarm. However, the alarm information is not reported through the GB/T 28181 protocol. For details about the alarm linkage policies supported by each alarm, see Alarm Linkage Policy Description.

Table 3 Alarm linkage policy parameters

Parameter	Setting
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.

Parameter	Setting
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** and set **Duration (s)** under **Alarm Output**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models. **NOTE:** • The alarm-triggered recording function configured here takes effect only on cameras. For a third-party platform, you need to configure the alarm-triggered recording function on the platform.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored

Parameter	Setting
	on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP. **NOTE:** The alarm-triggered snapshot taking function configured here takes effect only on cameras. For a third-party platform, you need to set the alarm-triggered snapshot taking function on the platform.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. Audio files can be customized. For details, see Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the mobile app when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

5. Click **Save**.

Configuring Device Alert

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **Alarm Service** > **Alarm Input**. The **Alarm Input** tab page is displayed.
3. Select the alarm to be configured and click **Device Alert Deployment**. The **Device Alert Deployment** area is displayed, as shown in Figure 3.

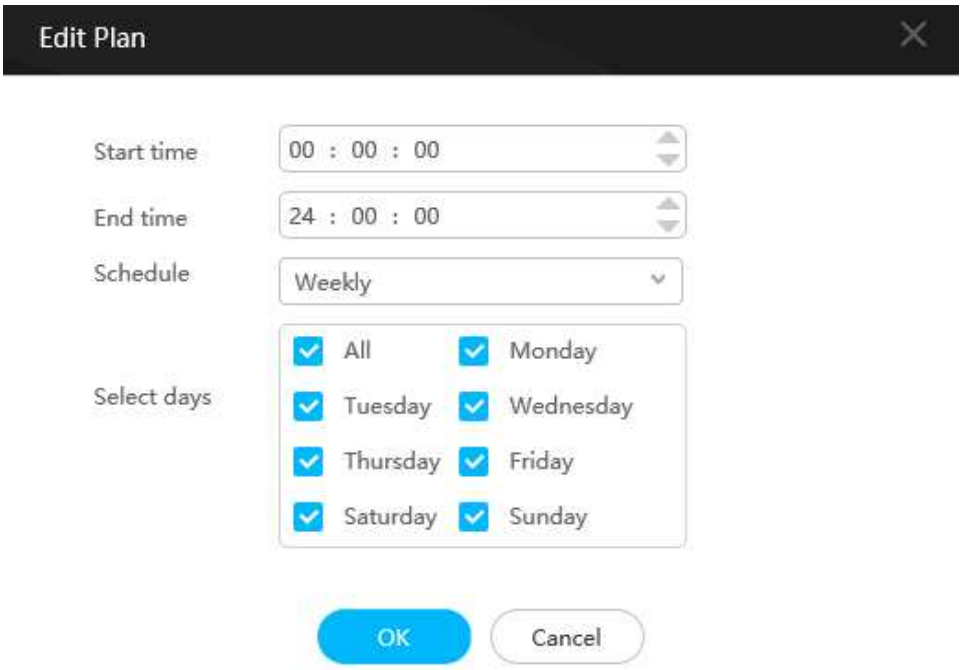
   Figure 3 Device Alert Deployment area

4. Click **Add**. A new alert plan is displayed. Click corresponding to the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

Figure 4 Edit Plan dialog box



5. Set **Start time**, **End time**, **Schedule**, and **Select days**.
6. Click **OK**.
7. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

Parent topic: Alarm Service

Alarm Linkage Policy Description

Table 1 describes the alarm linkage policies supported by each alarm.

Table 1 Linkage policies supported by each alarm type

Alarm Name	T28181	SDK	ONVIF	RESTful	PTZ	Record	Snapshot	smtp	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio an White Light Illuminat
Full disk	YES	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Disk read/write failure	YES	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Disk removal	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Media stream interruption	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Boolean value	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Log storage	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
PTZ configuration	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Flash read/write	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Temperature sensor fault	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Network port hot swap	NO	NO	NO	NO	YES	YES	YES	NO	YES	YES	NO
Fan stalled	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Video loss	YES	YES	YES	YES	YES	NO	NO	YES	YES	YES	NO
Photosensitive sensor fault	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Wiper fault	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
PTZ optocoupler fault	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	NO
Position change	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	NO
Lens PT optocoupler fault	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Abnormal system temperature	YES	YES	YES	YES	NO	NO	NO	YES	YES	NO	NO
Ascend processor fault	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Wi-Fi connection failure	NO	YES	YES	YES	NO	NO	NO	YES	YES	YES	NO
Upgrade/Rollback	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Parking violation	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Marked lane violation	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO

Alarm Name	T28181	SDK	ONVIF	RESTful	PTZ	Record	Snapshot	smtp	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio an White Light Illuminat
Wrong-way driving	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Illegal backing	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Non-motorized vehicle in motor vehicle lane	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Motor vehicle in non-motorized vehicle lane	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Congestion	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
License plate occlusion	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Motion	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Lens blocking	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Intrusion	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Abandoned object	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Removed object	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Tripwire crossing	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Loitering	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Area entry	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Area exit	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Fast movement	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Automatic tracking	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
Crowd density	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO
Queue length	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO
Head counting	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO
Crowd gathering	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO
Detection of electric bikes in elevators/corridors	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Off-duty detection	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Target detection	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Sound detection	NO	YES	NO	YES	NO	NO	NO	NO	NO	YES	NO
Sudden volume increase	NO	YES	NO	YES	NO	NO	NO	NO	NO	YES	NO
Sudden volume decrease	NO	YES	NO	YES	NO	NO	NO	NO	NO	YES	NO
Defocus	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES

Alarm Name	T28181	SDK	ONVIF	RESTful	PTZ	Record	Snapshot	smtp	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio an White Light Illuminat
Scene change	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Image freezing	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Gain imbalance	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Color cast	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Static noise	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Stripe noise	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
Image shaking	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES

Parent topic: Alarm Service

Channel Service

A channel is a set of functions provided by the lens, PTZ device, or other devices. The SDC system distinguishes subdevices and sub-lenses by channel.

The channel includes the audio, video, and image and PTZ-related functions (such as video-related functions, video stream, image-related functions, metadata stream of the corresponding video, image parameter setting, tour, and scanning) and system-related functions (such as camera restart, log download, and download and upload configuration).

Each channel is managed separately to differentiate the function sets.

Viewing Channel Information

Parent topic: Service Management

Viewing Channel Information

You can view the channel information of a camera based on the site requirements.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **Channel Service** > **Channel Info**.
3. On the **Channel Info** tab page, you can view channel information of the camera such as the camera UUID, attribute set, and function set.

   Table 1 describes the information displayed on this page.

   Table 1 Channel information description

Item	Description
uuid	Unique channel ID. The number of displayed channel IDs varies between camera models. **NOTE:** • A single-lens camera has only one UUID. • A compound-eye camera supports a channel for each lens. • In 1 + N mode, each device has a channel.
Attribute set	Displays channel attributes to differentiate channels. Supports attributes such as channel ID, channel name, imaging mode, location, and channel description.
Function set	Displays channel configuration information supported by the camera.

Item	Description
	Supports information about services such as images, PTZ controls, and media.

Parent topic: Channel Service

General Configuration Service

For cameras that support protocol-compliant apps, you can set parameters for enabled protocol-compliant apps on the **General Configuration** page.

- **Setting Video-based Vehicle Detector Platform Parameters**
- **Setting Streaming Media Parameters**
- **配置天翼视联平台**

Parent topic: Service Management

Setting Video-based Vehicle Detector Platform Parameters

Cameras can detect vehicles that appear in a specified period and in specified lanes and report information about vehicles that enter or leave a specified detection area to the connected video-based vehicle detector platform. You can adjust the traffic signal timing based on the passing vehicle information to improve traffic efficiency.

The capabilities supported vary between camera models.

Prerequisites

- The video-based vehicle detector platform application *TXProcess* has been installed. For details, see Managing Apps.
- The passing vehicle detection function has been enabled. For details, see Configuring a Video-based Vehicle Detector.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **General Configuration** > **Northbound Access Protocol** > **Video Vehicle Detector Platform**.
3. Select **Enable** to connect to the video-based vehicle detector platform.
4. Set video-based vehicle detector platform parameters, as shown in Figure 1. Table 1 describes the parameters.

   Figure 1 Setting video-based vehicle detector platform parameters



Table 1 Video-based vehicle detector platform parameters

Parameter	Description
Platform IP	IP address of the video-based vehicle detector platform, which is provided by the platform.
Port number	Port number of the video-based vehicle detector platform, which is provided by the platform.
Start lane ID	Set this parameter based on the configuration requirements of the video-based vehicle detector platform and the site requirements.
Road ID	Set this parameter based on the site requirements. The first four characters indicate the area ID, and the last four characters indicate the intersection ID in the area. For example, **00010002** indicates that the area ID is **0001** and the intersection ID is **0002**. The IDs of areas and intersections are provided by the platform.
Road direction	Set this parameter based on the configuration requirements of the video-based vehicle detector platform and the site requirements.

5. Click **Save**.

Parent topic: General Configuration Service

Setting Streaming Media Parameters

Configuring RTSP Metadata Extension

Parent topic: General Configuration Service

Configuring RTSP Metadata Extension

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Service** > **General Configuration** > **System management** > **Streaming media configuration**.
3. Select **RTSP metadata extension**. Then, the camera's metadata can be obtained in RTSP stream requesting mode. Otherwise, only video and audio streams can be obtained.

   NOTE

   The **RTSP metadata extension** check box is selected by default.

   Figure 1 Configuring RTSP metadata extension

4. Click **OK** for the settings to take effect.

Parent topic: Setting Streaming Media Parameters

配置天翼视联平台

Parent topic: General Configuration Service

Viewing Intelligent Display Results

This section describes how to check detection results after intelligent analysis functions are configured.

NOTICE

Functions available on the web page vary between camera models.

Viewing Intelligent Detection Results You can check the detection results of specified attributes.

Checking Intelligent Analysis Results
You can check the detection results of intelligent analysis functions. The intelligent analysis functions available on the web page vary between camera models.

Viewing Intelligent Metadata in TLV Format
You can check the detection results of third-party algorithm apps on the **Intelligent TLV** page.

Parent topic: Configuration

Viewing Intelligent Detection Results

You can check the detection results of specified attributes.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Intelligent Detection**. In the upper right corner of the page, click . In the dialog box that is displayed, select **Recognition content** and **Detection content** on the **Overall Layout** tab page, select **Target detection** and **Person detection** on the **Detection Area** tab page, and click **OK**.
3. Click **Enable Real-time Capture**.
4. If captured target and person images are displayed on the right of the video pane, as shown in Figure 1, the configuration is successful.

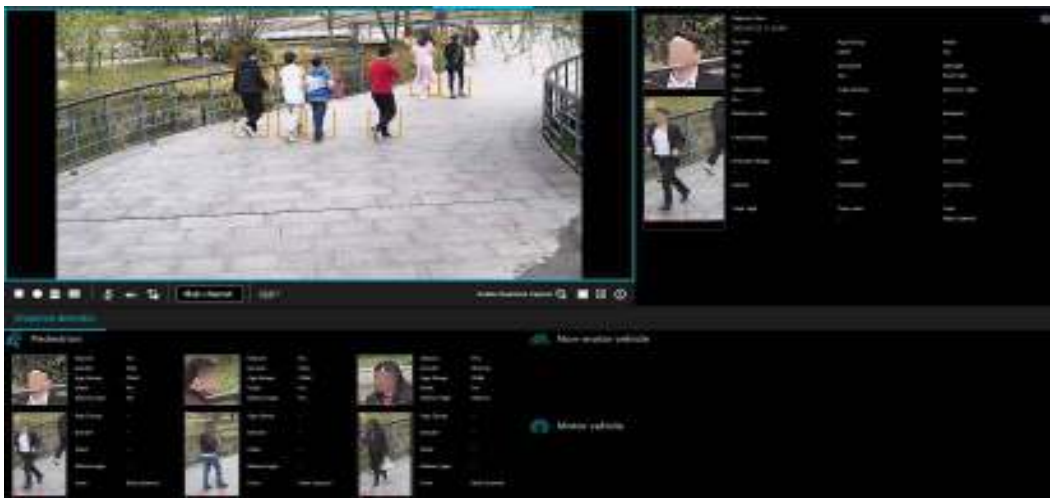
   You can also choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether target and person detection alarm logs are reported.

   NOTE

   Here, the detection images are for reference only. The images vary depending on the camera model.

   Some cameras support only target and person image capture.

Figure 1 Captured target and person images



NOTE

- To disable the real-time capture function, you can click **Disable Real-time Capture** in the lower part of the **Intelligent Detection** page.
- By default, the images captured in real time are stored on the local computer. The default storage path is **C:\Users*User name*\IPC_MediaPlayer\ScenePics**. (In this path, *User name* indicates the account of the current user in the operating system.) Ensure that the available space of the system disk is greater than 200 MB. Otherwise, images will fail to be captured. To change the storage path and space size, choose **Configuration** > **Local** > **Snapshots**, and set **Intelligent snapshot save path** and **File storage size**.
- The real-time image capture function cannot be enabled on multiple tabs at a time due to browser process conflict. When you attempt to enable the real-time capture function on multiple tabs, the message "The process of reporting target information has been started." will be displayed. In this case, you need to close unnecessary tabs and leave only one tab open or restart the browser and try again.

- Some targets may be missed during the capture due to causes such as improper image size or target angle. If the capture effect is not ideal, adjust the camera image quality, angle, and illumination for further optimization.

Parent topic: Viewing Intelligent Display Results

Checking Intelligent Analysis Results

You can check the detection results of intelligent analysis functions. The intelligent analysis functions available on the web page vary between camera models.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Display** > **Behavior Analysis**.
3. Click ▶ in the lower part of the page. Then the icon changes to ■, and the live video is opened.

   Live video viewing is enabled by default.
4. Click an intelligent analysis function on the right of the page.
5. Click **Start Metadata Reception** in the lower part of the live video pane.
6. View the intelligent analysis result.

   You can also choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query**, and check whether intelligent analysis alarm logs are reported.

   Figure 1 Intelligent analysis result



NOTE

- The image displayed here is for reference only. The actual result displayed varies depending on the selected intelligent analysis function.
- To stop the metadata receiving function, click **Stop Metadata Reception** in the lower part of the live video pane.
- By default, received metadata are stored on the local computer. The default storage path is **C:\Users*User name*\IPC_MediaPlayer\ScenePics**. (In this path, *User name* indicates the account of the current user in the operating system.) Ensure that the available space of the system disk is greater than 200 MB. Otherwise, images will fail to be captured. To change the storage path and space size, choose **Configuration** > **Local** > **Snapshots**, and set **Intelligent snapshot save path** and **File storage size**.
- The metadata receiving function cannot be enabled on multiple tabs at a time due to browser process conflict. When you attempt to enable the metadata receiving function on multiple tabs, the message "The process of reporting target information has been started." will be displayed. In this case, you need to close unnecessary tabs and leave only one tab open or restart the browser and try again.
- Some targets may be missed during the capture due to causes such as improper image size or target angle. If the capture effect is not ideal, adjust the camera image quality, angle, and illumination for further optimization.

Parent topic: Viewing Intelligent Display Results

Viewing Intelligent Metadata in TLV Format

You can check the detection results of third-party algorithm apps on the **Intelligent TLV** page.

Prerequisites

A third-party algorithm application has been installed. For details about how to install a third-party application, see Managing Apps.

NOTE

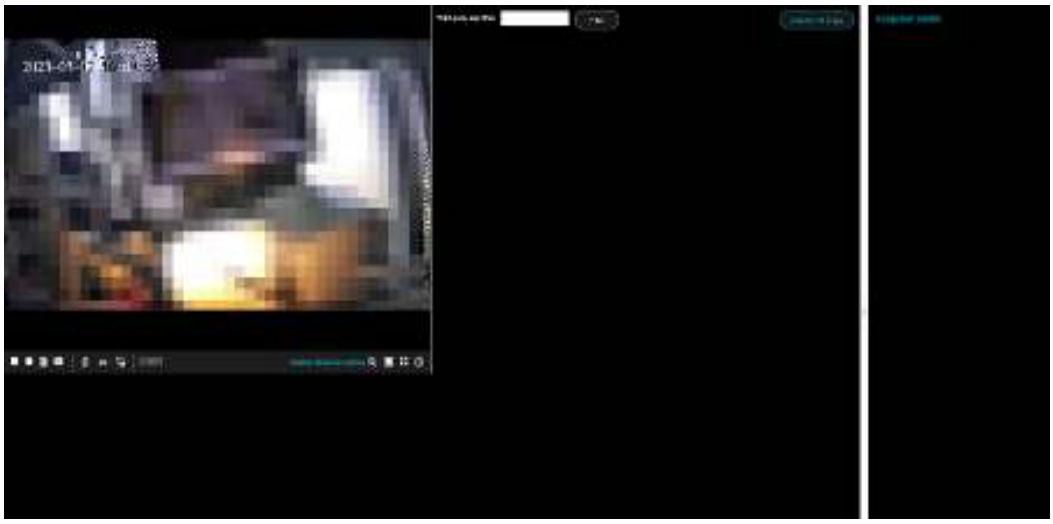
- The detection effect depends on the used third-party algorithm. The third-party algorithm must support the function of reporting intelligent metadata in common TLV format.
- If multiple third-party algorithms are enabled for a camera at the same time, the third-party algorithms may become invalid. In this case, restart the camera and reinstall the required algorithm. You are advised to enable one third-party algorithm for a camera at a time.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Before checking third-party algorithm app detection results, enable **Media stream**. The detailed procedure is as follows:
    a. Choose **Configuration** > **Service** > **Alarm Service** > **Alarm Input**.
    b. Select a third-party algorithm app and select **Media stream** on the **Alarm Linkage Policy** tab page.
    c. Click **Save**.
3. Choose **Display** > **Intelligent TLV**. Click **Enable Real-time Capture** in the lower right corner of the video pane.

4. If close-up snapshots are displayed below the video pane, as shown in Figure 1, the detection is successful. The detection result varies depending on the app.

   Figure 1 Detection result

5. Click **Enable Full Image** in the upper right corner of the page. The captured full images and recognized attributes are displayed on the right of the video pane.

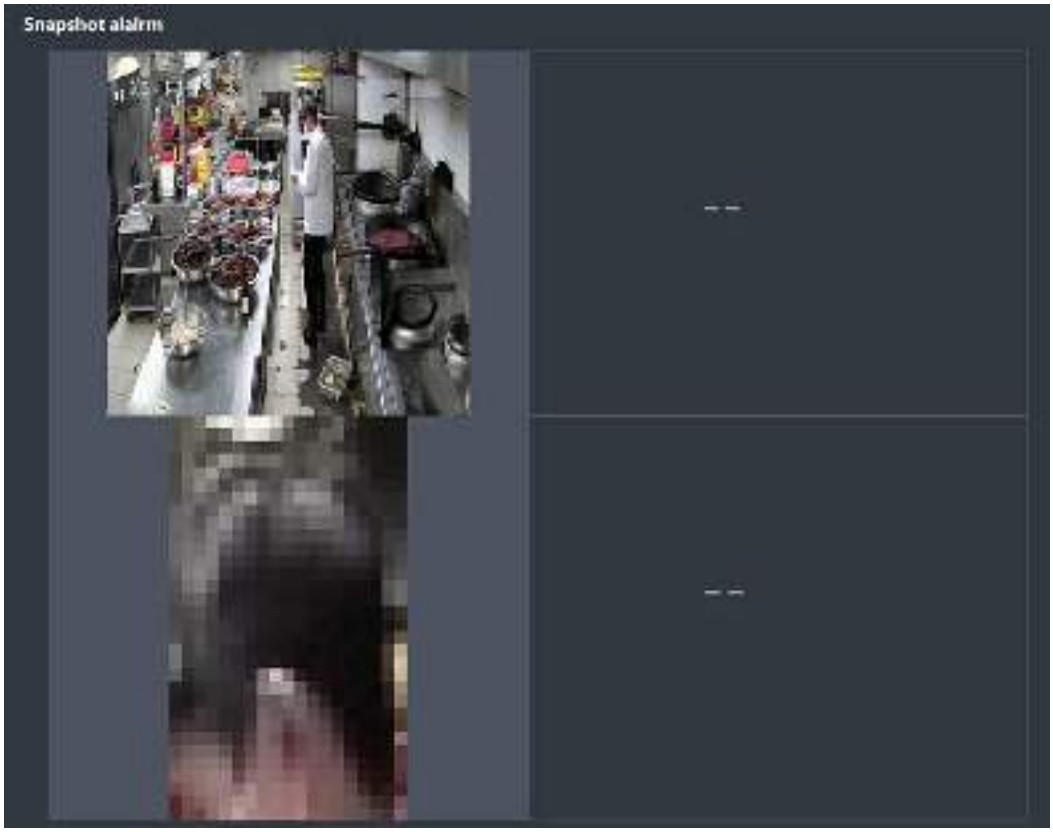
   NOTE

   When multiple algorithms are used for detection at the same time, if you want to display the detection result of only one algorithm, perform the following steps:

   a. Enter the algorithm name in the **Third-party algorithm** text box.
   b. Click **Filter**. Only detection results from the specified algorithm are displayed.

6. Trigger an alarm. Then alarm information is displayed on the right of the video pane. Double-click alarm information under **Snapshot alarm**. The alarm details are displayed, as shown in Figure 2.

Figure 2 Snapshot alarm



Parent topic: Viewing Intelligent Display Results

FAQs

This chapter describes how to locate and troubleshoot common faults.

Login to the Camera Web System

Live Video Viewing

Recording and Snapshot

Device Maintenance

Others

Parent topic: Configuration

Login to the Camera Web System

- Failure to Display HTTPS Web Page on Internet Explorer
- No Response When Clicking Mouse on Google Chrome
- Installing and Using Google Chrome IE Tab
- Some Characters Are Displayed as Question Masks (?) on Web Client in Chinese Running in a Windows OS in English
- Video Freezing Occurs After a User Logs In to the Web Client Using a Firefox Browser in Version 40.0.2
- The User Is Prompted to Install a Control Even When the Control Has Been Installed
- There Is a Problem with This Website's Security Certificate
- Failure to Enter Time in the Text Box for Setting Time in the Camera Web System
- Image Freezing Occurs and the Web Client Does Not Respond When the User Logs In to the Web Client Using Internet Explorer 11.0.9600.16428IS for the First Time
- When a User Uploads the SDC Certificate File, Configuration File, and 802.1x Certificate File Using HTTP on the Firefox Browser, the Message "Uploading... Do not perform any other operations" Is Always Displayed
- Message Indicating Risks Displayed on the Login Page
- A Message is Displayed During Plug-in Installation
- A Message Indicating that an Exception Occurred on the Website's Security Certificate Is Displayed When You Log In to the Camera Web System
- No Login Button Is Displayed on the Camera Login Page

Parent topic: FAQs

Failure to Display HTTPS Web Page on Internet Explorer

Symptom

The HTTPS web page cannot be displayed on Internet Explorer.

Possible Causes

Some settings of the Internet Explorer are incorrect.

Solution

1. Open Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**, select **TLS 1.1** and **TLS 1.2**, and deselect **Use SSL 2.0** under **Security**.
2. If the web page still cannot be displayed, use another browser to log in to the camera web system, choose **Configuration** > **System** > **Security Management** > **Security Options**, and select **Non-FS cipher suite**.

Parent topic: Login to the Camera Web System

No Response When Clicking Mouse on Google Chrome

Symptom

Google Chrome is used to log in to the SDC web system. After the browser window is minimized, the browser does not respond to mouse clicks.

Possible Cause

The installed version of the IE Tab plug-in is too old, which causes errors.

Solution

Please install the latest IE Tab plug-in which is of 10.5.10.1 or a later version.

Parent topic: Login to the Camera Web System

Installing and Using Google Chrome IE Tab

Symptom

If you use Google Chrome v45 or a later version to log in to the camera web system, you need to install the IE Tab plug-in. Otherwise, live video cannot be viewed. The latest version of the IE Tab plug-in is recommended.

Solution

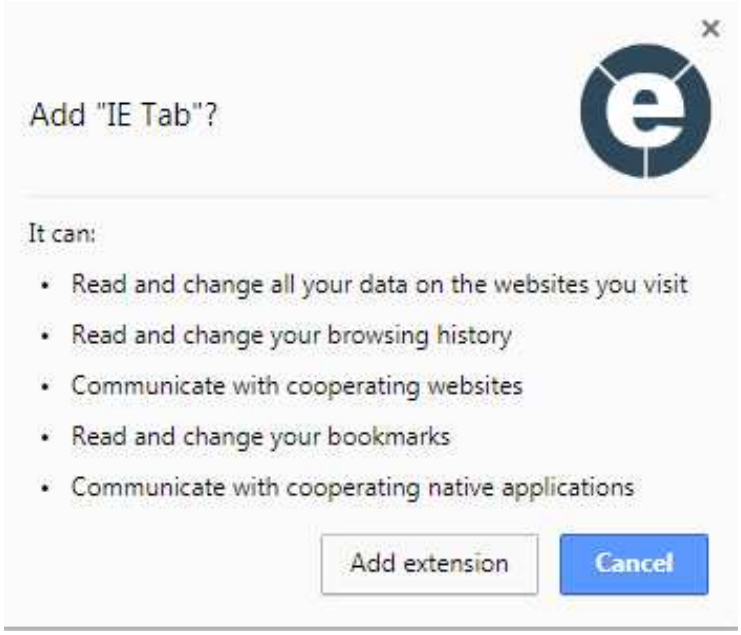
1. Use Google Chrome to visit the website for downloading the Google Chrome IE Tab, as shown in Figure 1.

   Figure 1 Downloading the IE Tab plug-in

2. Click **ADDED TO CHROME**. In the dialog box that is displayed, click **Add extension**, as shown in Figure 2.

Figure 2 Adding the IE Tab plug-in



NOTE

If the added IE Tab plug-in is not the latest version, a pop-up window is displayed in the lower left corner of the page, indicating the program download and running status. Click **Run** as prompted.

3. After the extension program is added, another tab page is displayed, and the IE tab plug-in icon is generated, as shown in Figure 3. Click this icon.

   Figure 3 Enabling the IE Tab plug-in



4. After the IE Tab plug-in is enabled, another tab page is displayed. The icon for setting the IE Tab plug-in is displayed, as shown in Figure 4. Click the icon.

   Figure 4 Icon for setting the IT Tab plug-in



5. In the dialog box that is displayed, select Internet Explorer 10 or 11, as shown in Figure 5.

   Figure 5 Selecting Internet Explorer



   NOTE

   Ensure that Internet Explorer 10 or 11 is used.

6. In the address box of the IE Tab plug-in, enter the camera IP address to log in to the camera.

   NOTE

   You can ignore the Google Chrome address box. Enter the IP address in the address box of the TE tab plug-in, which is under that of Google Chrome.

Parent topic: Login to the Camera Web System

Some Characters Are Displayed as Question Masks (?) on Web Client in Chinese Running in a Windows OS in English

Symptom

When a user logs in to the web client of the Chinese version in the Windows operating system of the English version, some characters are displayed as question masks (**?**).

Possible Cause

The current language for non-Unicode programs is not Chinese (Simplified, PRC).

Solution

Set the current language for non-Unicode programs to Chinese (Simplified, PRC).

1. Choose **Start** > **Control Panel** > **Clock, Language, and Region**.
2. Click **Region and Language**.

   The **Region and Language** dialog box is displayed.
3. Click **Administrative** tab page.
4. Click **Change system locale** under **Language for non-Unicode programs**.
5. Set **Current system locale** to **Chinese (Simplified, PRC)**.

Parent topic: Login to the Camera Web System

Video Freezing Occurs After a User Logs In to the Web Client Using a Firefox Browser in Version 40.0.2

Symptom

Video freezing occurs after a user logs in to the web client using a Firefox browser of the 40.0.2 version.

Possible Cause

The Firefox browser 40.0.2 is incompatible with the camera.

Solution

Upgrade the Firefox browser to Firefox 51.

Parent topic: Login to the Camera Web System

The User Is Prompted to Install a Control Even When the Control Has Been Installed

Symptom

After the control is installed on the live video viewing page, a message is still displayed asking you to install the control and you cannot view live video.

Possible Cause

- By default, a Chrome browser in a version between 42 and 44 has the NPAPI plug-in disabled.
- After the control is installed on the Firefox browser, you need to restart the browser to load the control.

Solution

- Enable the NPAPI plug-in for Chrome 42 to 44. The detailed procedure is as follows:

  1. Enter **chrome://flags** in the address box.
  2. Click **Enable** under **Enable NPAPI**.
  3. Restart the browser.
  4. If live video still cannot be played, the plug-in may be blocked. In this case, enter **chrome://plugins** in the address box, select **Always allowed to run** under **npIVS_VideoPlugin**, and restart the browser.

- After the control is installed on the Firefox browser, restart the browser to load the control.

Parent topic: Login to the Camera Web System

There Is a Problem with This Website's Security Certificate

Symptom

After the root certificate is downloaded and installed, Internet Explorer still displays a warning message **There's a problem with this website's security certificate**. Click **Continue to this website (not recommended)** to access the login page. The **Certificate Error** is then displayed in the address box.

Possible Cause

The certificate is invalid.

Solution

Upload the local certificate. For details about how to upload a certificate, see Managing HTTPS Certificates. After the certificate is uploaded, restart the browser.

Parent topic: Login to the Camera Web System

Failure to Enter Time in the Text Box for Setting Time in the Camera Web System

Symptom

A user fails to enter time in the text box for setting time (for example, alert time) in the camera web system.

Possible Cause

The current input method is Microsoft Pinyin IME.

Solution

Switch the input method to an English input method.

Parent topic: Login to the Camera Web System

Image Freezing Occurs and the Web Client Does Not Respond When the User Logs In to the Web Client Using Internet Explorer 11.0.9600.16428IS for the First Time

Symptom

Image freezing occurs and the web client does not respond when the user logs in to the web client using Internet Explorer 11.0.9600.16428IS for the first time.

Possible Cause

On Internet Explorer in the 11.0.9600.16428IS version, **Only allow approved domains to use Active without prompt** is set to **Enable** and **Allow previously unused ActiveX controls to run without prompt** is set to **Disable** by default.

Solution

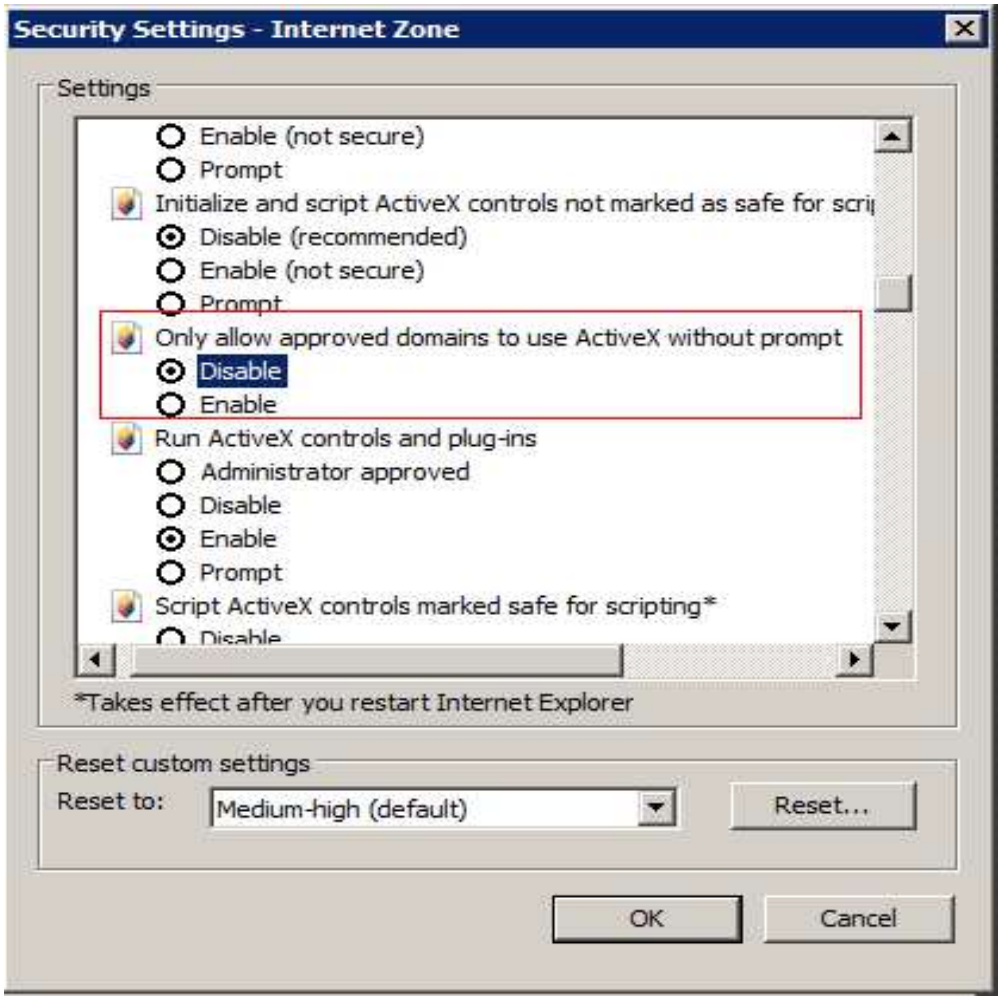
1. Choose **Internet options** > **Security** > **Custom level**, as shown in Figure 1.

Figure 1 Internet Options



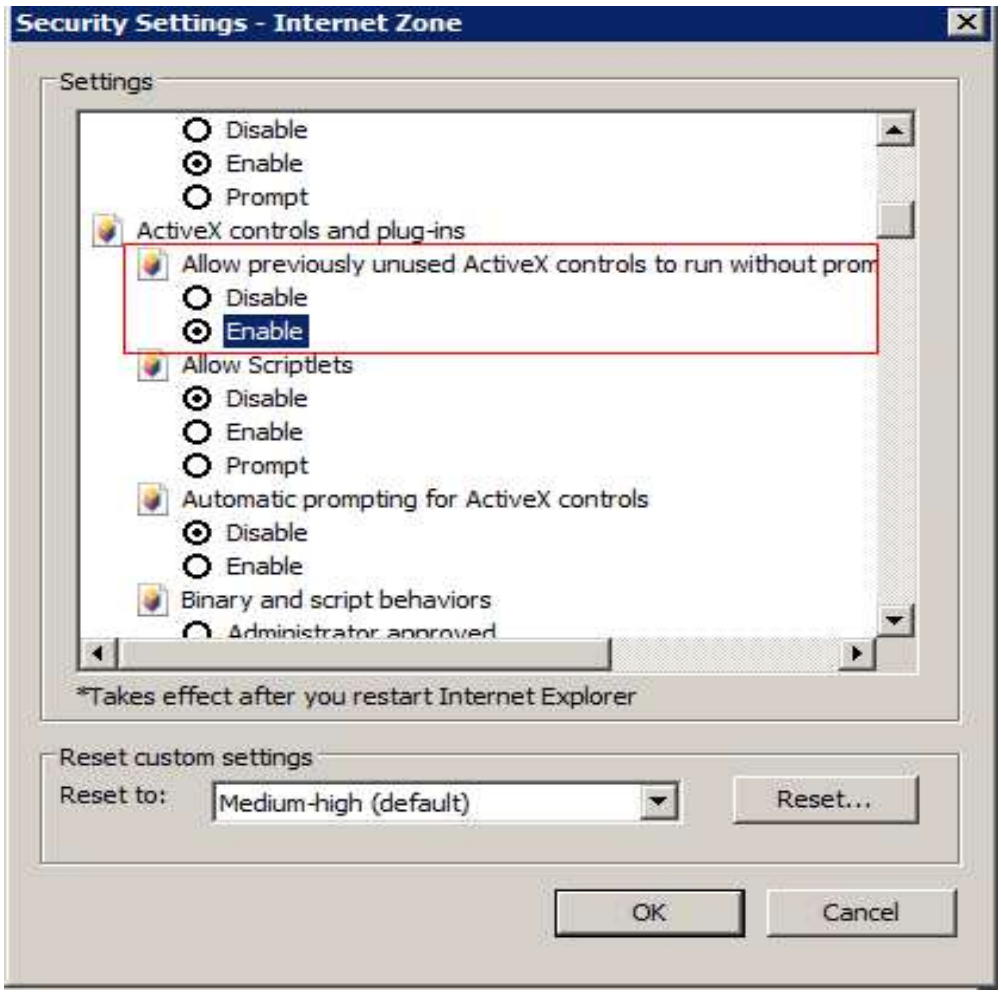
2. Set **Only allow approved domains to use ActiveX without prompt** to **Disable**, as shown in Figure 2.

Figure 2 Security Settings — Internet Zone 1



3. Set **Allow previously unused Active controls to run without prompt** to **Enable**, as shown in Figure 3.

Figure 3 Security Settings — Internet Zone 2



4. Click **OK**. The **Internet Options** page is displayed.
5. Click **OK**.

Parent topic: [Login to the Camera Web System]

When a User Uploads the SDC Certificate File, Configuration File, and 802.1x Certificate File Using HTTP on the Firefox Browser, the Message "Uploading... Do not perform any other operations" Is Always Displayed

Symptom

When a user uploads the SDC certificate file, configuration file, and 802.1x certificate file using HTTP on the Firefox browser, the message "Uploading... Do not perform any other operations" is always displayed.

Possible Cause

When a user logs in to the SDC web system over HTTP using a non-Internet Explorer browser, transmission of sensitive information is processed in an HTTPS pop-up window. This window is implemented based on browser compatibility. The Firefox browser blocks pop-up windows by default.

Solution

1. Enter **about:preferences#content** in the address box.
2. Deselect **Block pop-up windows**.

Parent topic: Login to the Camera Web System

Message Indicating Risks Displayed on the Login Page

Symptom

The message "Your request for URL has a security risk. You can access this URL by clicking **Continue, I accept this risk.** If you make this choice, it means that you accept this risk." is displayed on the login page.

Solution

Choose **Tools** > **Internet Options**, click the **Connections** tab, click **LAN Setting**, and deselect **Use a proxy for your LAN**.

Parent topic: Login to the Camera Web System

A Message is Displayed During Plug-in Installation

Symptom

When you attempt to install the web plug-in, a message is displayed. For example, a message indicating the verification failure is displayed.

Possible Cause

The security level or kernel of the operating system is incorrectly set.

Solution

This issue does not affect system security or other settings. Therefore, you can ignore the message and click **Run**.

Parent topic: Login to the Camera Web System

A Message Indicating that an Exception Occurred on the Website's Security Certificate Is Displayed When You Log In to the Camera Web System

If the browser displays a security warning **There's a problem with this website's security certificate**, download and install the root certificate.

Procedure

1. Click **Download Root Certificate** in the upper right corner of the login page.

   NOTE

   Use the download function of the browser.

   The **File Download - Security Warning** dialog box is displayed, as shown in Figure 1.

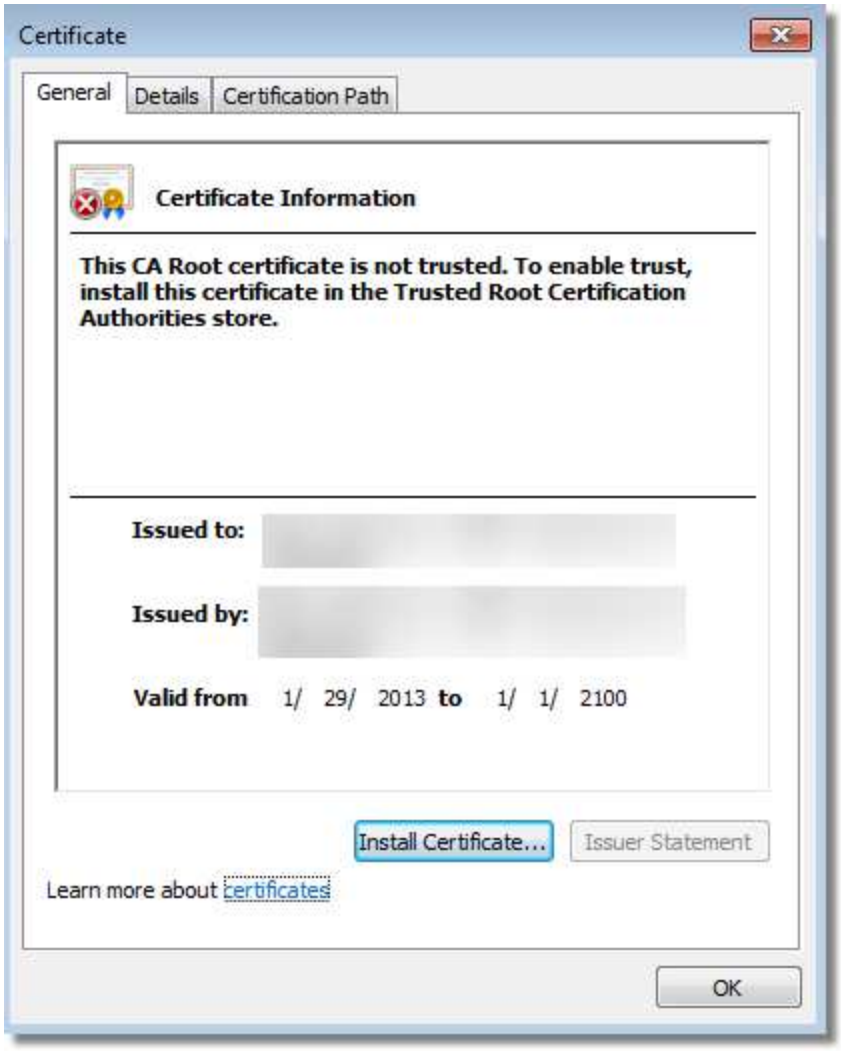
Figure 1 File Download - Security Warning dialog box



2. Click **Open**.

   The **Certificate** page is displayed, as shown in Figure 2.

Figure 2 Certificate page



3. Click **Install Certificate**.

   The **Welcome to the Certificate Import Wizard** page is displayed, as shown in Figure 3.

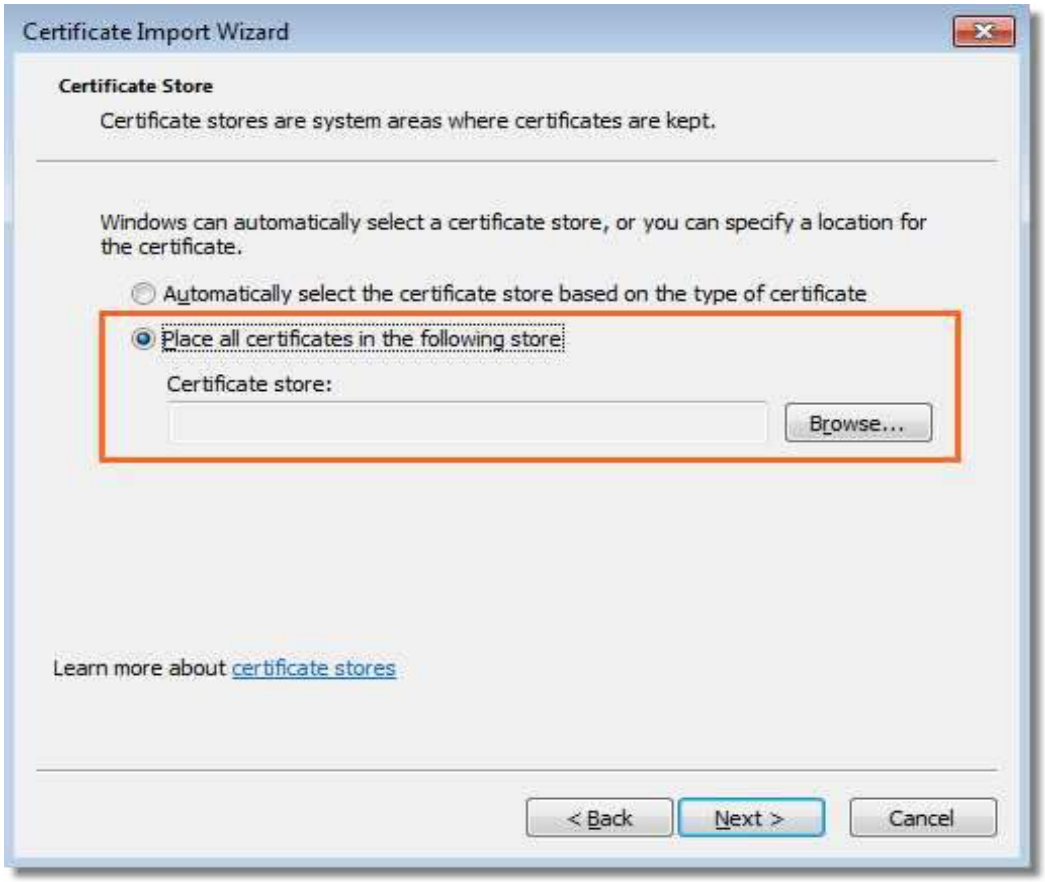
Figure 3 Welcome to the Certificate Import Wizard page



4. Click **Next**.

   The **Certificate Import Wizard** page is displayed, as shown in Figure 4.

Figure 4 Certificate Import Wizard page



5. Select **Place all certificates in the following store** and click **Browse**.

   The **Select Certificate Store** dialog box is displayed, as shown in Figure 5.

Figure 5 Select Certificate Store dialog box



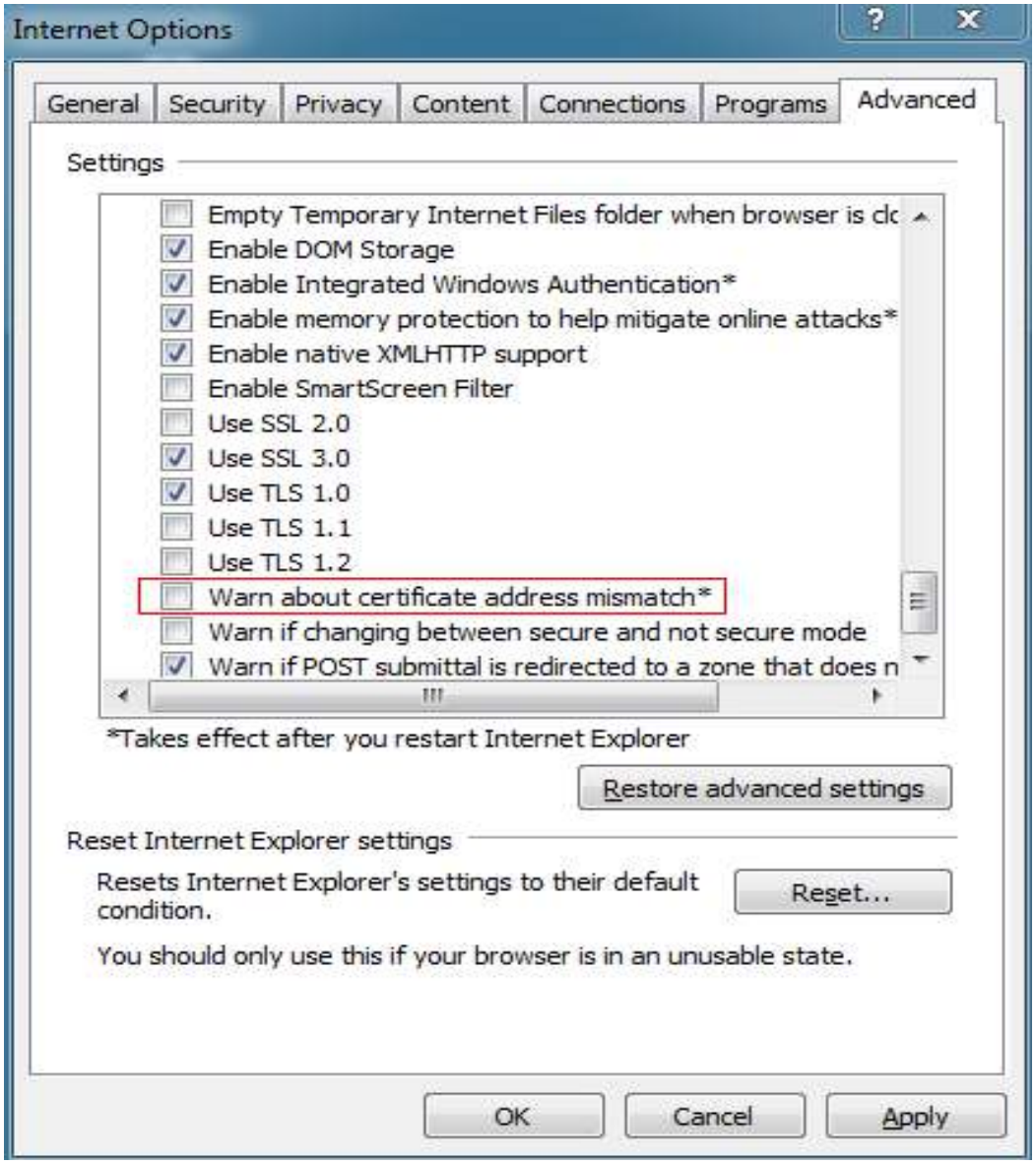
6. Select **Trusted Root Certification Authorities** and click **OK**.

   The selected certificate store is displayed on the **Certificate Import Wizard** page.

7. Click **Next** and install the root certificate as prompted.

8. On the **Internet Options** page, click the **Advanced** tab, deselect **Warn about certificate address mismatch**, and click **OK** to save the settings, as shown in Figure 6.

Figure 6 Canceling warning about certificate address mismatch



9. After the root certificate is installed, restart Internet Explorer and enter the IP address of the camera in the address box. The login page is then displayed.

Parent topic: [Login to the Camera Web System]

No Login Button Is Displayed on the Camera Login Page

Symptom

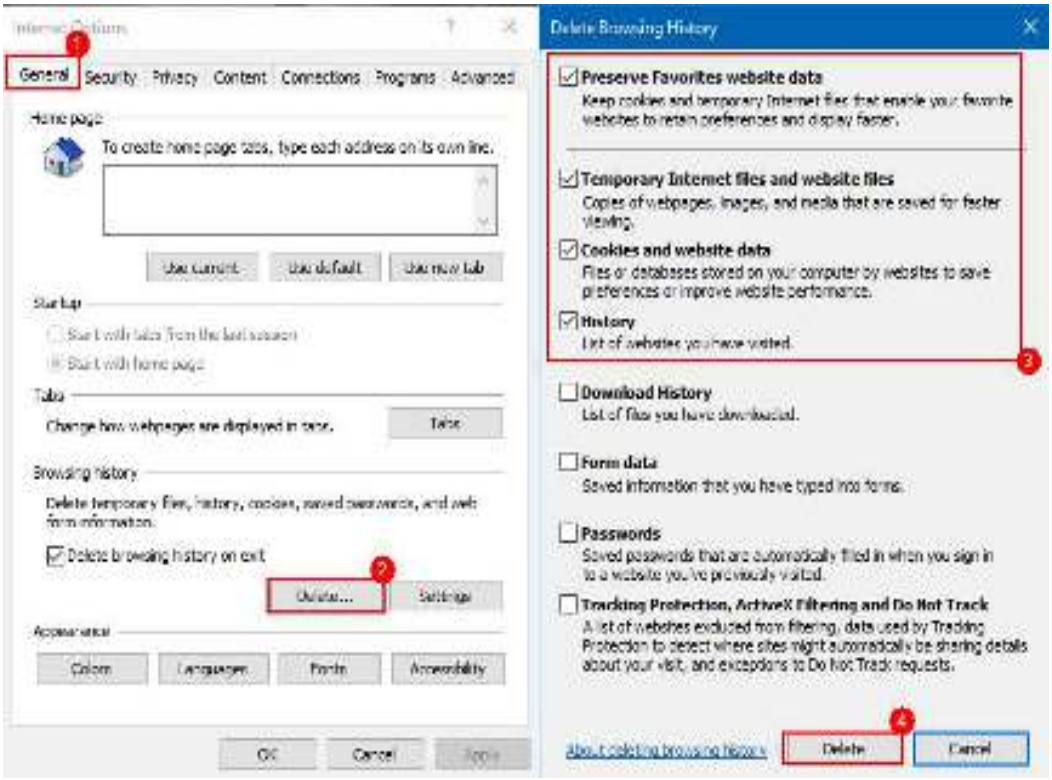
When you enter **https://*Camera IP address*** in the address box of Internet Explorer to access the camera, the **Log In** button is not displayed on the login page.

Solution

- Refresh or close the page, and go to the camera web page at *https://Camera IP address* again. If the login button is displayed, no further action is required. If the login button is still not displayed, go to the next step.
- Delete cached data of the browser.

  Choose **Tools** > **Internet Options** > **General**. On the tab page that is displayed, click **Delete** to delete browser cache. Then log in to the camera again.

Figure 1 Deleting browser cache



Parent topic: [Login to the Camera Web System]

Live Video Viewing

Failure to Enter Full-Screen Mode When Double-Clicking the Live Video Pane for the First Time on the Live Video Viewing Page

Video Playback Failure on the Live Video Viewing Page

Failure to Play Video on the View Page for 5G Cameras

Live Video Request Failure

Black Screen Occurs on the Live Video Pane

Failure to Play Live Video on Internet Explorer

Live Video Viewing Failure with a Message Indicating ActiveX Control

Functional Icons on the Live Video Pane Remain Blue After the Functions Exit

Live Video Artifacts Occur and the CPU Usage Reaches 100%

Artifacts or Frame Freezing on Live Video

Unclear Live Video Image

Failure to View Live Video

Unstable Frame Rate Displayed on the Live Video Preview Page

Response Exceptions Occur After Parameter Setting During HTTP Login

Discontinuity Occurs When Objects Move in the Live Video

Slight Blinks on Image Border During Live Video Viewing Using Firefox

Graphs or Lines Superimposed on the Live Video Fail to Be Displayed

What Can I Do If Chinese Characters Are Displayed as Question Marks in the Camera Web System on the Windows 10 English Operating System?

Failure to Clearly Focus the Live Video Image

Artifacts Occur When the Platform Requests Streams

Parent topic: FAQs

Failure to Enter Full-Screen Mode When Double-Clicking the Live Video Pane for the First Time on the Live Video Viewing Page

Symptom

When a user logs in to the camera web system using Firefox or Internet Explorer 11 and double-clicks the live video pane on the live video viewing page, the live video pane does not enter the full-screen mode.

Solution

This fault occurs only at the first double-click. Try once again.

Parent topic: Live Video Viewing

Video Playback Failure on the Live Video Viewing Page

Symptom

After a user accesses the live video viewing page, the user cannot play video.

Possible Causes

- The player control is not properly installed.
- The player control is prohibited.
- The local firewall is enabled.
- The PC operating system is Windows 7, Windows 8, or Windows 10 and the browser is not run as an administrator.

Solution

- Reinstall the player control as prompted.
- Allow the player control.
- Disable the local firewall.
- Right-click the Internet Explorer icon and choose **Run as administrator** from the shortcut menu.

Parent topic: Live Video Viewing

Failure to Play Video on the View Page for 5G Cameras

Symptom

When you access the **View** page, you cannot play video even if the player control is correctly installed.

Possible Cause

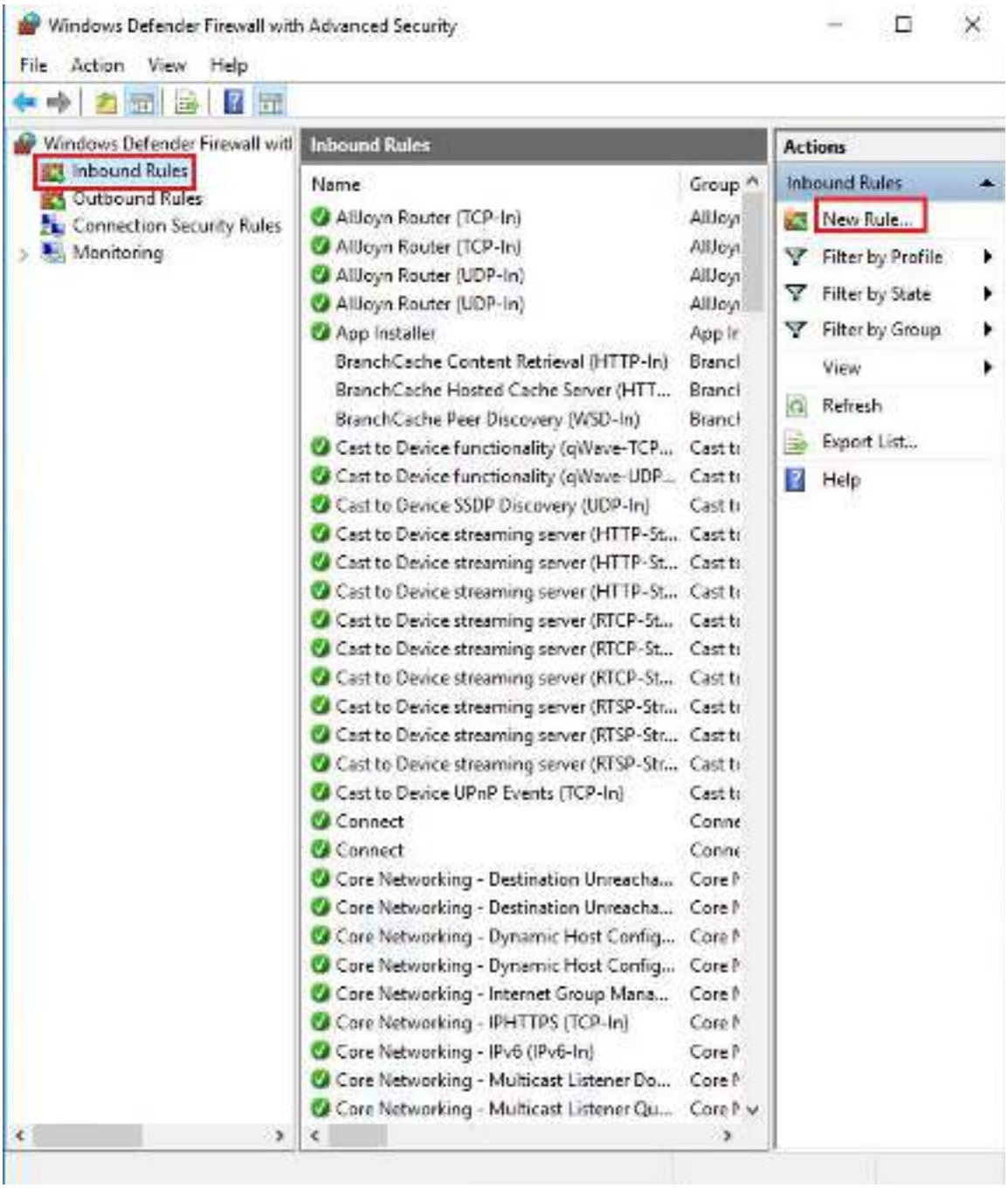
The UDP port is disabled on the firewall of the Windows operating system. As a result, video streams cannot be transmitted. You need to enable the port.

Solution

The following uses Windows 10 as an example. The procedure for other versions of Windows operating systems is similar.

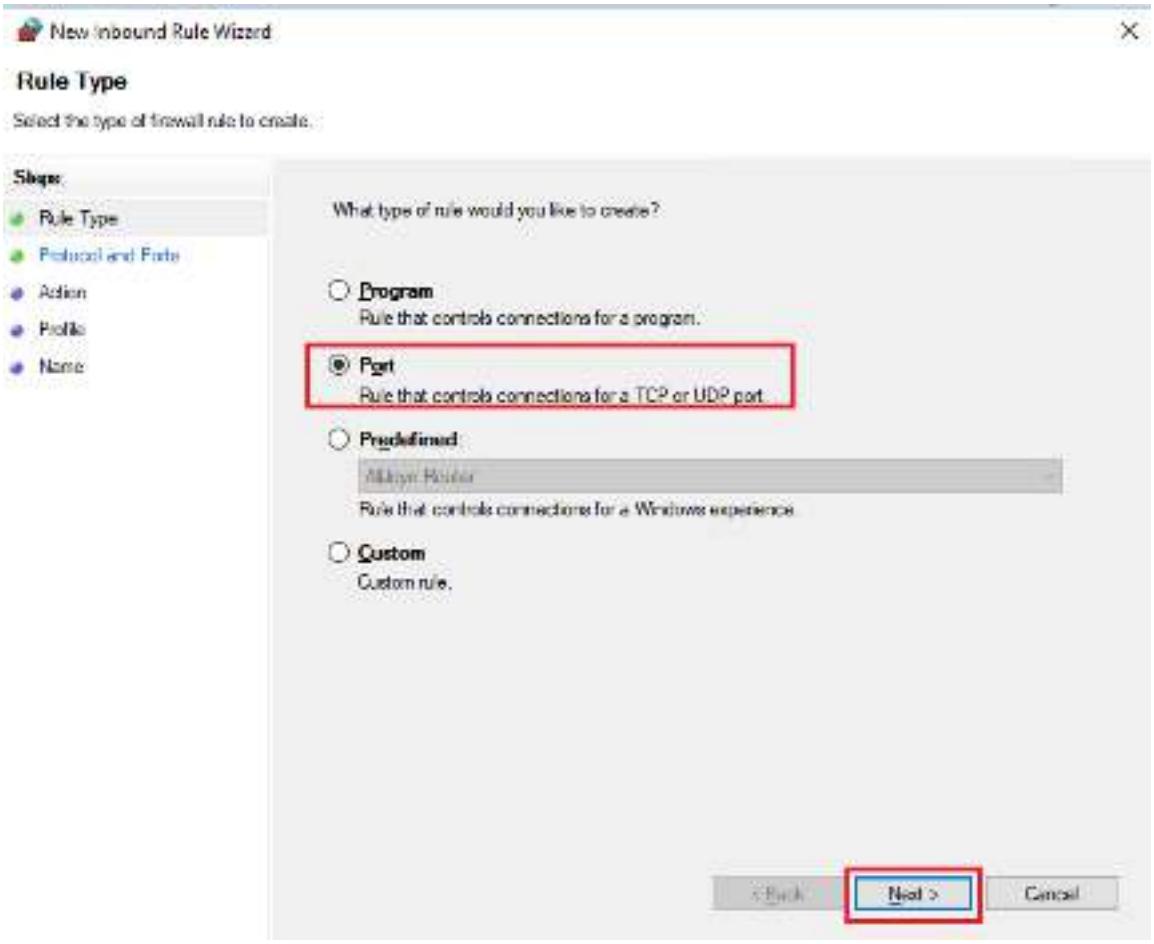
1. Choose **Start** > **Control Panel** > **Windows Defender Firewall** > **Advanced settings**.
2. In the **Windows Defender Firewall with Advanced Security** dialog box, click **Inbound Rules** and then click **New Rule**, as shown in Figure 1.

   Figure 1 Windows Defender Firewall with Advanced Security dialog box



3. In the **New Inbound Rule Wizard** dialog box, click **Port** and then **Next**, as shown in Figure 2.

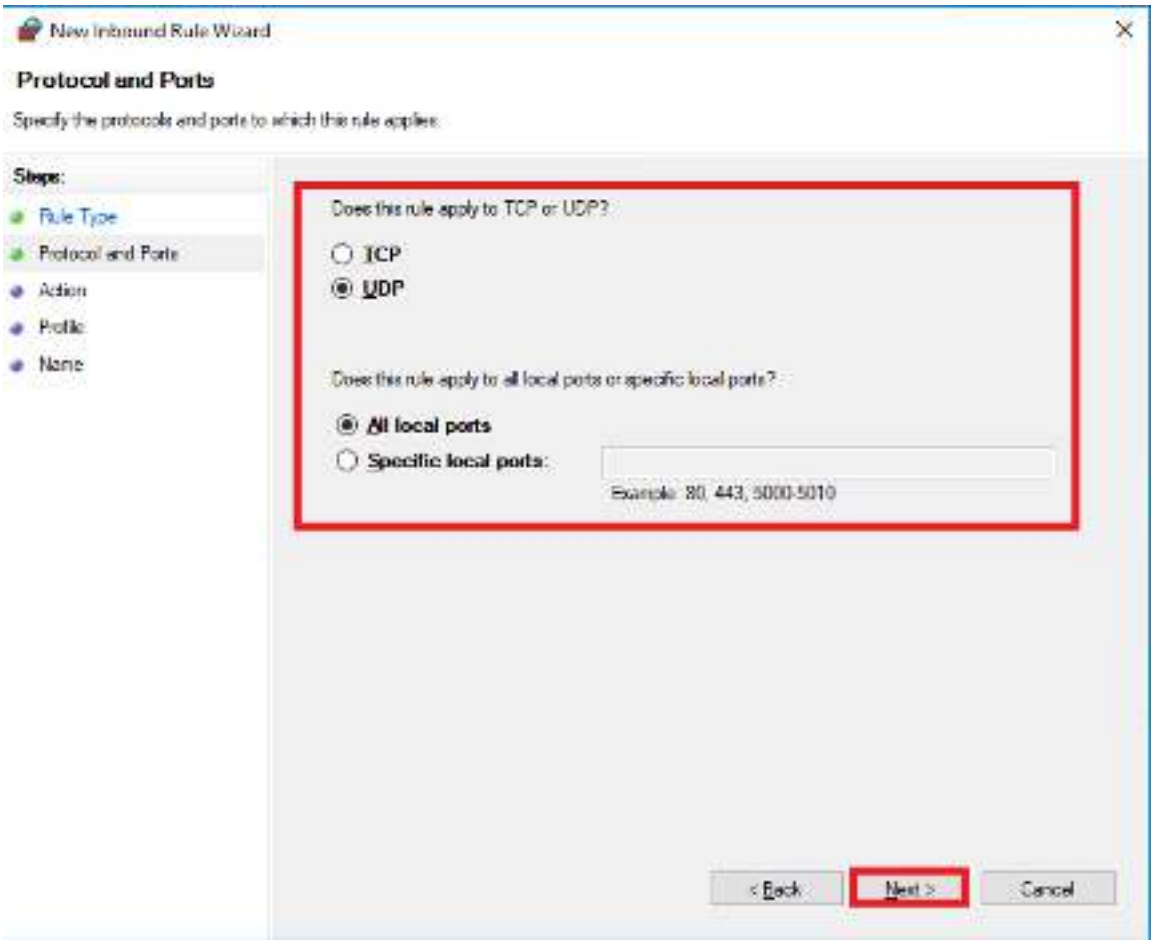
Figure 2 New Inbound Rule Wizard dialog box



4. In the **New Inbound Rule Wizard** dialog box, click **UDP** and **All local ports**, as shown in Figure 3.

   If you know the local port, you can also click **Specific local ports** and enter the port number.

Figure 3 New Inbound Rule Wizard dialog box



5. Click **Next** until the page for setting the name is displayed. Enter a name and click **Finish**.

Parent topic: Live Video Viewing

Live Video Request Failure

Live video cannot be played on the live video viewing page.

Symptom

When you access the **Preview** page, a **Warning** dialog box is displayed in the lower right corner. The system displays the message "Failed to obtain the live video. The current stream type does not support live video. Configure a correct stream type and try again."

Possible Cause

- The requested stream does not support live video.

Solution

Method 1:

- Remain the stream type unchanged. On the **View** page, click  in the lower left corner and choose **Primary** from the shortcut menu.

Method 2:

- On the **View** page, click  in the lower left corner and check the current stream type.
- Choose **Configuration** > **Video/Audio** > **Video**. Set **Stream combination** to a value that contains the current stream combination type on the **View** page.

Parent topic: Live Video Viewing

Black Screen Occurs on the Live Video Pane

Symptom

When a PC with an independent display adapter attempts to access live video in web mode, the PC can receive video streams but a black screen is displayed.

Possible Cause

The driver version of the display adapter is too early.

Solution

Upgrade the display adapter driver of the PC to the latest version.

Parent topic: Live Video Viewing

Failure to Play Live Video on Internet Explorer

Symptom

After the camera is upgraded and the control of a new version is installed, live video cannot be played.

Solution

1. Right-click the task bar on the PC desktop and choose **Task Manager** from the shortcut menu.
2. Right-click the Internet Explorer process, for example, Internet Explorer, Internet Explorer (32-bit), or iexplorer.exe, and choose **End task** from the shortcut menu.
3. Log in to the camera web system again and view live video from the camera.

Parent topic: Live Video Viewing

Live Video Viewing Failure with a Message Indicating ActiveX Control

Symptom

Users are unable to view live video on the web page, with a message displayed, indicating that an error occurs on the ActiveX control.

Possible Causes

- An exception occurs on the ActiveX control.
- An exception occurs on Internet Explorer.

Solution

- Reinstall the ActiveX control.

1. Open Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**, click **Reset** to reset Internet Explorer, and close all Internet Explorer windows.
2. Choose **Start** > **Run**, enter **cmd**, and press **Enter**. The Command Line Interface (CLI) is displayed.
3. Enter **regsvr32 -u**.
4. Drag the **C:\Program Files\Camera_webocx_vware*Version number*\IVS_OCXPlayer.ocx** file to the CLI. The complete command is displayed.
5. Press **Enter**. The interface indicating the operation success is displayed.
6. Delete the **C:\Program Files\Camera_webocx_vware*Version number*** folder.
7. Log in to the web client again and download and install the ActiveX control as prompted.

- Reinstall Internet Explorer, depending on Internet Explorer you are using.

Parent topic: Live Video Viewing

Functional Icons on the Live Video Pane Remain Blue After the Functions Exit

Symptom

- A user clicks the full-screen icon and then exits the full screen mode. If the mouse pointer is located in the live video preview pane, the full-screen icon is blue.
- When user clicks the 1:1 or snapshot icon and quickly locates the pointer in the live video preview scope, the 1:1 or snapshot icon is blue.

Solution

Move the pointer out of the live video preview pane. This issue does not affect functions.

Parent topic: Live Video Viewing

Live Video Artifacts Occur and the CPU Usage Reaches 100%

Symptom

Live video image artifacts occur and the CPU usage reaches 100%.

Possible Cause

Multiple or all of the following configurations or functions are used at the same time: a high frame rate (50 or 60 fps), a high bit rate (for example, 8 Mbit/s), or a small MTU value (for example, 1200), video recording, image capture, super error concealment (SEC), tour, and behavior analysis.

Solution

Modify the frame rate, bit rate value, or MTU value. Alternatively, you can disable some of the following functions: video recording, image capture, SEC, tour, or behavior analysis.

Parent topic: Live Video Viewing

Artifacts or Frame Freezing on Live Video

Symptom

Artifacts or frame freezing occurs on the live video.

Possible Cause

The packet loss rate is high due to poor network conditions.

Solution

Change the network transmission protocol to TCP. The steps are as follows:

1. Log in to the camera web system and choose **Configuration** > **Local** > **Playing Settings**.
2. Set **Protocol type** to **TCP**.
3. Click **Save**.

Parent topic: Live Video Viewing

Unclear Live Video Image

Symptom

The live video image is smooth but not clear.

Possible Causes

When the camera detects that the working bandwidth of the network port is 10 Mbit/s or less, the camera automatically decreases the bit rate to 4 Mbit/s.

Solution

Troubleshoot the fault that occurs on the network where the camera is located.

Parent topic: Live Video Viewing

Failure to View Live Video

Symptom

A blank screen is displayed during live video viewing on the Firefox or Google Chrome.

Possible Cause

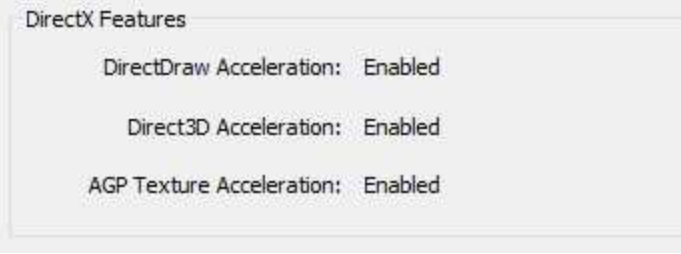
- The DirectX driver corresponding to the video card is not installed on the computer.
- The DirectX driver is not started.

Solution

- For possible cause 1: Install the DirectX driver on the computer.
- For possible cause 2: Check whether the DirectX driver is started. If not, reinstall the DirectX driver and verify that the driver is started. To check whether the DirectX driver is started, perform the following operations:

1. Press **Windows**+**R**, enter **dxdiag**, and click **OK**.
2. In the **DirectX Diagnostic Tool** window that is displayed, click the **Display** tab. On the tab page that is displayed, check whether the DirectX function is enabled, as shown in Figure 1.

   Figure 1 DirectX Diagnostic Tool window



Parent topic: Live Video Viewing

Unstable Frame Rate Displayed on the Live Video Preview Page

Symptom

When **Full frame rate** is set to **25** and **Frame rate** is set to **20**, the frame rate displayed on the live video preview page is unstable and fluctuates around **20**, for example, **18**, **19**, **20**, or **21**.

Possible Cause

The frame rate displayed on the live video preview page is the frame rate of rendering video instead of the actual encoding frame rate. This frame rate is calculated every 2 seconds. In non-full frame rate mode (20 fps or lower), the frame rate of the video play control may slightly fluctuate due to the network delay or jitter in the rendering period. However, this fluctuation does not affect the actual video frame rate.

Parent topic: Live Video Viewing

Response Exceptions Occur After Parameter Setting During HTTP Login

Symptom

A user logs in to the camera web system using Internet Explorer 11.0.9600.17843 or 11.0.9600.18015 in HTTP mode, sets the password, and clicks **Save**. The page does not respond or keeps displaying the "Setting..." message.

Solution

Access the device in HTTPS mode (https://*IP*). When the login page is displayed, log in to the device in HTTP mode.

Parent topic: Live Video Viewing

Discontinuity Occurs When Objects Move in the Live Video

Symptom

Discontinuity occurs when objects move in the live video.

Possible Cause

The current desktop theme deteriorates visual effect of the PC.

Solution

Select a desktop theme other than basic and high contrast themes.

Parent topic: Live Video Viewing

Slight Blinks on Image Border During Live Video Viewing Using Firefox

Symptom

During live video viewing using a Firefox browser, if the live video image aspect ratio is 1:1 or its resolution is 1440 x 900, the image border slightly blinks.

Possible Cause

The compatibility between the Firefox browser and the DDraw rendering mode may cause slight blinking of the video border. This symptom does not affect the live video image effect. It occurs only when the live video image exceeds the Firefox browser border and the DDraw rendering mode is used.

Parent topic: Live Video Viewing

Graphs or Lines Superimposed on the Live Video Fail to Be Displayed

Symptom

In the Windows 10 operating system, if the live video resolution exceeds 5 megapixels (3072 x 1728), graphs or lines (for example, detection lines for intelligent analysis) superimposed on the live video image cannot be displayed.

Solution

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Playing Settings**, and set **Rendering mode** to **D3D**. Alternatively, reduce the resolution of the primary stream under **Configuration** > **Video/Audio** > **Video**.

Parent topic: Live Video Viewing

What Can I Do If Chinese Characters Are Displayed as Question Marks in the Camera Web System on the Windows 10 English Operating System?

Symptom

What can I do if Chinese characters are displayed as question marks in the camera web system on the Windows 10 English operating system?

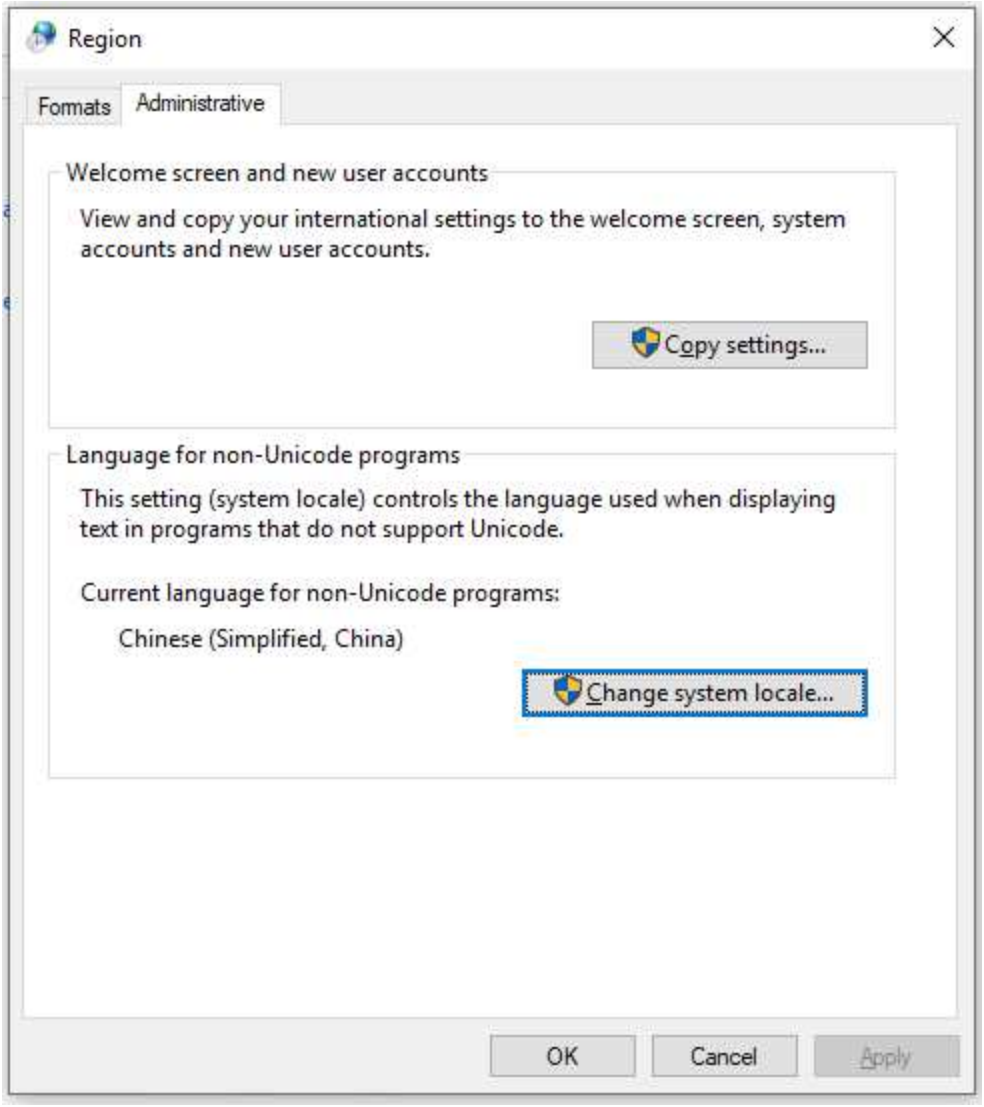
Possible Cause

The operating system setting is incorrect.

Solution

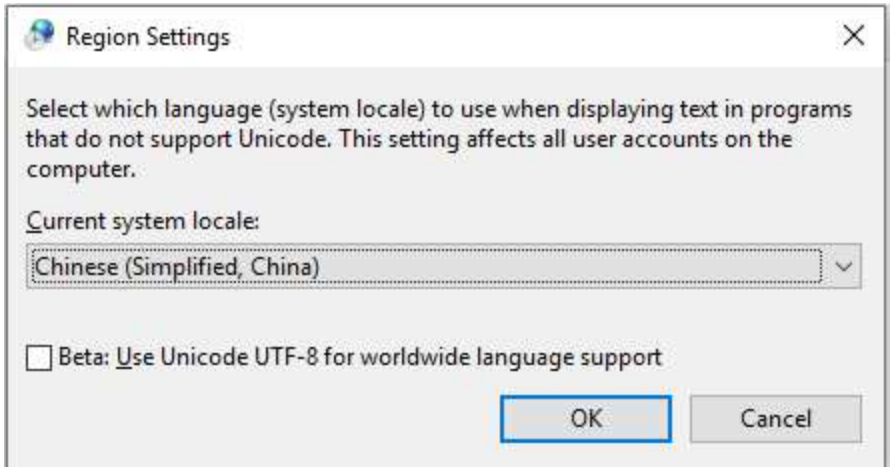
1. Choose **Start** > **Settings**.
2. Click **Time & Language** and then **Region**.
3. Click **Additional date, time & regional settings** at the bottom of the page.
4. Click **Change date, time, or number formats** in the **Region** area.
5. Click the **Administrative** tab. On the tab page that is displayed, click **Change system locale**.

Figure 1 Changing the system locale



6. Set **Current system locale** to **Chinese(Simplified, China)**. Deselect **Beta: Use Unicode UTF-8 for worldwide language support**.

Figure 2 Setting the current system locale



7. Click **OK**.

Parent topic: Live Video Viewing

Failure to Clearly Focus the Live Video Image

Symptom

On the camera web page, when you click  to reset the lens or click  to perform one-push focus, the live video image cannot be clearly focused.

Solution

For some camera models, this fault can be rectified through curve calibration. To ensure accurate curve calibration, the following conditions must be met:

- The camera is installed in an environment with high luminance, for example, in the daytime with sunlight or in indoor areas with a light source enabled.
- The camera shoots a distant view with fine details. For example, you can adjust the PTZ angle of a PTZ dome camera to enable it to shoot a distant view.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display** > **Focus** and set **Focus mode** to **Auto** or **Semi-auto**.
3. In the PTZ control panel, click  to reset the camera.
4. Choose **Configuration** > **Network** > **Advanced Settings** > **SSH/SFTP** and select **Enable SSH**.
5. Use the SSH tool to log in to the camera background.
    a. Log in to the background system as the **admin** user and switch to the **root** user. The port number is 22.
    b. Run the **/usr/app/bin/help debug open 65** command.

6. Log in to the camera web system and click  to perform one-click focus. Enable the curve calibration function. After the live video image changes, run the following commands on the SSH tool:

   /usr/app/bin/help debug close 65

   tail -f /opt/log/message.dbg

   NOTE

   Do not operate the camera during curve calibration.

7. Observe the live video. After the live video is stable, perform the following operations:

   a. On the camera web page, click  again to perform one-click focus.

   b. On the SSH tool, if "bIsCalied 1" is displayed, the curve calibration is successful. If "bIsCalied 0" is displayed, the curve calibration fails. In this case, you need to adjust the camera's angle of view and perform curve calibration again.

8. Restart the camera and use the zoom and focus adjustment function to check the focus effect.

NOTE

The following models do not support curve calibration (For models that do not support this function, you can click  or  to adjust the image clarity. For details, see Configuring the PTZ.):

C2120-10-FI, C2120-10-LU (2.8–12 mm), C2120-10-SIU, C2120-10-SLU (2.8–12 mm), C2141-10-EI, C2150-10-IU, C2150-10-SIU, C2150-10-SLU (2.8–12 mm), C3220-10-EI, C3220-10-I, C3220-10-

IU, C3220-10-SIU, C3221-10-I, C3221-10-IU (2.8–12 mm), C3250-10-I, C3250-10-IU, C3250-10-SIU, D2120-10-LI-SV, D2120-10-SIU, D2150-10-LI-SV, D2150-10-SIU, D2150-10-SIU-up, D3220-10-SIU, D3250-10-SIU, M2120-10-EBIn (2.8–12 mm), M2120-10-EI, M2120-10-FI, M2120-EVL-TD (7–35 mm), M2121-10-EI (2.8–12 mm), M2121-10-EL (2.8–12 mm), M2121-10-EL-SF (2.8–12 mm), M2121-ECL, M2122-10-EI, M2122-10-EL, M212A-10-EFL (2.8–12 mm), M2141-10-EI, M2141-10-EL, M2141-10-EL (2.8–12 mm), M2150-10-EGI, M2150-10-EI (2.8–12 mm), M3220-10-EI, M3220-10-EI-SF, M3221-10-EI (2.8–12 mm), M3221-10-EI-SF, M3241-10-EI-FB, M3250-10-EI, and M3250-10-EI-SF

Parent topic: Live Video Viewing

Artifacts Occur When the Platform Requests Streams

Symptom

After the platform successfully requests video streams, artifacts occur on the live video images.

Solution

Reduce the frame rate of video streams in the following way: Choose **View** > **General** > **Video** or choose **Configuration** > **Video/Audio** > **Video** and decrease the frame rate.

Parent topic: Live Video Viewing

Recording and Snapshot

- Failure to Find Related Files in Storage Paths After Snapshots Are Taken and Video Is Recorded On Web Pages
- Failure to Enable Image Capturing and Video Recording On Web Pages
- Incorrect File Path Displayed
- Abnormal Live Video Scale on the Recording Playback Page

Parent topic: FAQs

Failure to Find Related Files in Storage Paths After Snapshots Are Taken and Video Is Recorded On Web Pages

Symptom

After snapshots are taken and video is recorded on web pages, you cannot find related files in the storage paths.

The files have been saved to the **Virtualized** directory under the Internet Explorer cache directory.

For example, in the path **C:\Users*User name*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized\C\Users*User name*\IPC_MediaPlayer**, **C:\Users*User name*\AppData\Local\Microsoft\Windows\Temporary Internet Files** indicates the Internet Explorer cache directory, **Virtualized** indicates the automatically generated directory, and **C\Users*User name*\IPC_MediaPlayer** indicates the original file storage path.

Possible Causes

- The PC operating system Windows 7, 8, or 10 is not run as an administrator and the Internet Explorer is not run as an administrator. The storage path is set to a random path under **C:\Users***User name*\.

  > **NOTE**
  >
  > In the preceding path, *User name* indicates the account of the current user in the operating system.

- The protection mode is enabled when you log in to the camera using Internet Explorer.

Solution

- Right-click the Internet Explorer icon and choose **Run as administrator** from the shortcut menu.
- Disable the protection mode of Internet Explorer in the following way: Open Internet Explorer, **Internet Options** > **Security**, and deselect **Enable Protected Mode**.

Parent topic: Recording and Snapshot

Failure to Enable Image Capturing and Video Recording On Web Pages

Symptom

The image capturing and video recording functions fail to be implemented on web pages.

Possible Causes

The user logs in to the Windows 7, 8, or 10 operating system as a non-administrator user and does not use **Run as administrator** to log in to the camera web system using Internet Explorer. The storage path is set to a path not started with **C:\Users***User name*\.

> **NOTE**
>
> In the preceding path, *User name* indicates the account of the current user in the operating system.

Solution

Right-click the Internet Explorer icon and choose **Run as administrator** from the shortcut menu.

Parent topic: Recording and Snapshot

Incorrect File Path Displayed

Symptom

The file path is incorrectly displayed. For example, when a user clicks **Browse** and select a path, the path displayed in the text box is different from the actual path.

Possible Cause

The security settings are incorrect.

Solution

Open Internet Explorer, choose **Tools** > **Internet Options** > **Security** > **Custom level** and set **Include local directory path when uploading file** to **Enable**.

Parent topic: Recording and Snapshot

Abnormal Live Video Scale on the Recording Playback Page

Symptom

On the recording playback page, if the zoom level of the browser is decreased and then adjusted to 100%, the live video is not displayed in 100% scale.

Solution

Refresh the browser page.

Parent topic: Recording and Snapshot

Device Maintenance

- Camera Upgrade Issues
- Improper Display of the Web Page upon the First Login After Camera Upgrade
- Login Page Flickers When Internet Explorer Is Used to Log In to the Camera Web System
- Page Redirection Failure During Default Setting Restoration in HTTP Mode
- Failure to Install Player Control After Successful Device Upgrade on 64-bit Windows 8
- Redirection to the Live Video Page Before Starting One-Click Information Collection
- PTZ Rotation, Zoom, or Focus Adjustment Does Not Stop After a Click on a Corresponding Button
- Logs Fail To Be Downloaded After a User Clicks Download All Logs on the Web Client
- No Dialog Box Is Displayed After You Click the Button for Restarting the Device or Restoring Default Settings
- The PTZ Dome Camera Is Not Started Immediately After Being Powered on

Parent topic: FAQs

Camera Upgrade Issues

Symptom	Possible Cause	Solution
A camera fails to be upgraded.	• The network is not properly connected or configured. • The upgrade package is incorrect. • A power outage occurs during the upgrade. • Close the browser during the upgrade.	• Ensure that the network is properly connected and configured, and the upgrade package is correct. • Restore the power and perform the upgrade gain.
The camera software version or algorithm package fails to be upgraded, and the intelligent function is invalid.	Close the browser during the upgrade.	Perform the upgrade again.
After the upgrade software package is selected, the upgrade package path is still empty or	The upgrade package path may contain languages that are not supported by the current system.	Change the upgrade package path to an English one.

Symptom	Possible Cause	Solution
contains garbled characters.		

Parent topic: Device Maintenance

Improper Display of the Web Page upon the First Login After Camera Upgrade

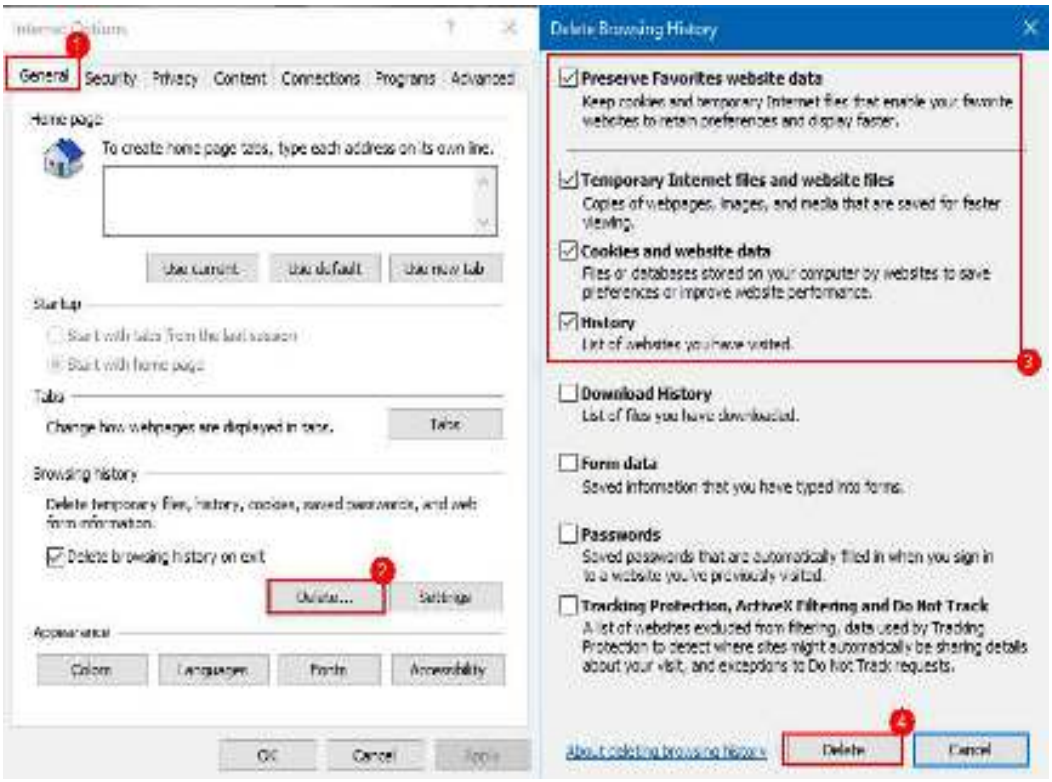
Symptom

After the camera is upgraded, the web page is improperly displayed upon the first login.

Solution

Choose **Tools** > **Internet Options** > **General**. On the tab page that is displayed, click **Delete** to delete browser cache. Then log in to the camera again.

Figure 1 Deleting browser cache



Parent topic: Device Maintenance

Login Page Flickers When Internet Explorer Is Used to Log In to the Camera Web System

Symptom

The login page flickers when Internet Explorer is used to log in to the camera web system. As a result, the login fails.

Solution

Method 1:

Restart the browser.

Method 2:

Choose **Tools** > **Internet Options** > **General**. On the tab page that is displayed, click **Delete** to clear browser cache as prompted. Then log in to the camera again.

Parent topic: Device Maintenance

Page Redirection Failure During Default Setting Restoration in HTTP Mode

Symptom

If the SDC uses the HTTP protocol, the page cannot redirect automatically when the default setting is restored.

Possible Cause

The settings for data source access are incorrect.

Solution

Open Internet Explorer, choose **Tools** > **Internet Options** > **Security** > **Custom level** > **Miscellaneous**, and set **Access data sources across domains** to **Enable** or **Prompt**.

> **NOTE**
>
> If **Access data sources across domains** is set to **Prompt**, a security warning dialog box will be displayed during page redirection. In this case, click **Yes**.

Parent topic: Device Maintenance

Failure to Install Player Control After Successful Device Upgrade on 64-bit Windows 8

Symptom

On a PC running 64-bit Windows 8 operating system, the device upgrade is successful. However, after the upgrade, the player control fails to be installed.

Possible Cause

An exception occurs on the operating system cache.

Solution

Clear the operating system cache and reinstall the player control.

Parent topic: Device Maintenance

Redirection to the Live Video Page Before Starting One-Click Information Collection

Symptom

On the web page of Internet Explorer 8, click **One key collection**. Information can be collected only after the system displays the window that prompts you to download files and jumps to the live video page.

Possible Cause

The setting of automatic prompting for file downloads is incorrect.

Solution

1. Upgrade Internet Explorer. For details about Internet Explorer versions supported by the current device, see Computer Software and Hardware Requirements. If the fault persists after the upgrade, go to the next step.
2. Open Internet Explorer, choose **Tools** > **Internet Options** > **Security** > **Custom level** > **Downloads**, and set **Automatic prompting for file downloads** to **Enable**.

Parent topic: Device Maintenance

PTZ Rotation, Zoom, or Focus Adjustment Does Not Stop After a Click on a Corresponding Button

Symptom

If you click a PTZ rotation, zoom, or focus button on the camera web page of the Firebox browser and the mouse pointer is still on the button, the PTZ rotation, zoom, or focus adjustment does not stop.

Solution

Move the mouse pointer away from the PTZ rotation, zoom, or focus button after clicking it.

Parent topic: Device Maintenance

Logs Fail To Be Downloaded After a User Clicks Download All Logs on the Web Client

Symptom

After logging in to the camera web system, a user clicks **Download all logs** on the **Logs** tab page. Logs, however, fail to be downloaded.

Solution

Restart the PC, and re-log in to the camera web system.

Parent topic: Device Maintenance

No Dialog Box Is Displayed After You Click the Button for Restarting the Device or Restoring Default Settings

Symptom

Log in to the camera web system, choose **Configuration** > **System** > **System Maintenance** > **Maintenance**, and click **Remote Restart**, **Restore**, or **Fully Restore**. Then no dialog box is displayed. The operation cannot proceed.

Solution

1. In the upper right corner of the browser, click  to minimize the window.
2. After the window is minimized, click  in the upper right corner of the browser to maximize the browser.

After the preceding operations are complete, if a dialog box is properly displayed after you click **Remote Restart**, **Restore**, or **Fully Restore**. The operation can proceed.

Parent topic: Device Maintenance

The PTZ Dome Camera Is Not Started Immediately After Being Powered on

Symptom

The PTZ dome camera does not start immediately after being powered on. It takes a long time to start the camera.

Solution

It takes about 40s to 60s to start a PTZ dome camera.

Parent topic: Device Maintenance

Others

- Failure to Download Files or Live Video Control
- Blank Settings Page
- Improper Display of PTZ Control Buttons
- Abnormal Position of Palette for OSD Color Customization
- Vehicle Speed Displayed as NA in ePolice Mode of ITS Cameras
- Simultaneous Occurrence of Large and Small Images on the Detection Line Drawing Page of ITS Cameras
- Obtaining Streams Through RTSP
- Abnormal Device Start in Extremely Low Temperature
- Example for Drawing a Traffic Light Area
- Failure to Upload Images to the FTP/SFTP Server
- There Is a Possibility that Defocus Occurs When a Vehicle Passes the Image View
- How Do I Obtain and Use the Milestone 2022 R3 Plug-in?

Parent topic: FAQs

Failure to Download Files or Live Video Control

Symptom

- When you click **Download** on the **Configuration Management** page to download the configuration file to the local host, a message is displayed indicating that the **main_cgi** file cannot be downloaded.
- When you click **One-Click Collection** on the **Log** page to download log files to the local host, a message is displayed indicating that the **main_cgi** file cannot be downloaded.
- The SDC Web Control cannot be downloaded.

Possible Causes

Some settings of the Internet Explorer are incorrect.

Solution

In Internet Explorer, choose **Tools** > **Internet Options** > **Advanced** and click **Reset** to restore the default browser settings. Then restart the PC and log in to the web client again.

Parent topic: Others

Blank Settings Page

Symptom

After a user goes to the web page and clicks **Settings**, the page displayed is blank and the user cannot perform settings.

Possible Causes

- The PC operating system is Windows 8 or Windows 10 and the browser is not run as an administrator.

Solution

- Right-click the Internet Explorer icon and choose **Run as administrator** from the shortcut menu.

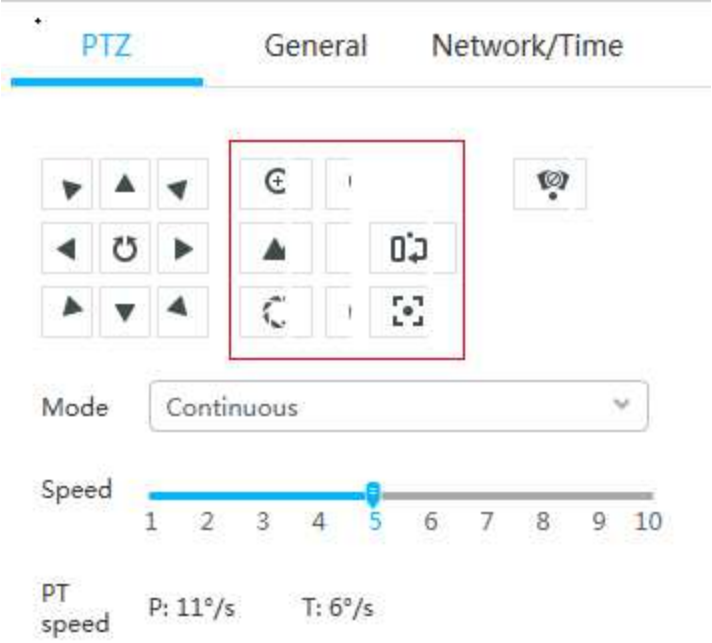
Parent topic: Others

Improper Display of PTZ Control Buttons

Symptom

On the PTZ configuration page, the control buttons such as the wiper icon are displayed abnormally, as shown in Figure 1.

Figure 1 Abnormal PTZ button display



Solution

Delete the browser cache and restart the browser.

Parent topic: Others

Abnormal Position of Palette for OSD Color Customization

Symptom

When you choose **Configuration** > **Intelligence**, click **Settings** next to an intelligent analysis function, click the **Text Overlay** tab, and customize the font or background color, the color palette position is incorrect.

Solution

Delete the browser cache and restart the browser.

Parent topic: Others

Vehicle Speed Displayed as NA in ePolice Mode of ITS Cameras

Background

In ePolice mode of ITS cameras, a vehicle detector with two loops is deployed for speed estimation. According to the settings, one snapshot will be taken when a vehicle passes and the vehicle speed should be superimposed in the snapshot. However, after a vehicle passes, the vehicle speed displayed in the snapshot is **NA**.

Possible Causes

The loop spacing is greater than the vehicle length. When the vehicle passes the first loop and is captured, it has not reached the second loop. As a result, the vehicle speed cannot be calculated and is displayed as **NA**.

Solution

Reduce the distance between the two loops to be shorter than the vehicle length.

Parent topic: Others

Simultaneous Occurrence of Large and Small Images on the Detection Line Drawing Page of ITS Cameras

Symptom

On the page for drawing detection lines, a small live video image is displayed in the upper left corner of the preview pane, as shown in Figure 1.

Figure 1 Simultaneous occurrence of large and small images on the detection line drawing page



Possible Cause

This fault occurs when you frequently switch between tabs on the camera web page.

Solution

Refresh the browser page.

Parent topic: Others

Obtaining Streams Through RTSP

Users can enter a corresponding URL on the VLC media player to obtain live video streams of a camera through RTSP.

NOTICE

- The VLC media player cannot request streams using RTSP in Digest_SHA256 authentication mode.
- For details about how to change the authentication mode in the RTSP protocol, see Configuring Connection to the Platform Through RTSP.

Solution

1. Log in to the camera web system.
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **ONVIF**. Check the value of **Authentication mode**.
    - If **Authentication mode** is set to **None**, authentication is not needed when requesting data streams through RTSP. Table 1 lists the URL for requesting streams through RTSP.

      Table 1 Requesting streams through RTSP in the case of no authentication

Request Content	Stream Request URL
Live video stream	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=1
Metadata	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=4
Live video stream +	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1

Request Content	Stream Request URL
metadata	

In the preceding URLs, ***IP address*** indicates the camera IP address, ***RTSP port number*** is the same as that set under **Configuration** > **Network** > **Basic Settings** > **Port** in the camera web system, **Media1** indicates the primary stream. To obtain the secondary stream, change **Media1** to **Media2**.

- If **Authentication mode** is not set to **None**, authentication is needed when requesting data streams through RTSP. Table 2 lists the URL for requesting streams through RTSP.

  Table 2 Requesting streams through RTSP in the case of authentication

Request Content	Stream Request URL
Live video stream	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=1
Metadata	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=4
Live video stream + metadata	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1

  The default user name is **admin**.

To set the authentication password, choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Password Management** > **ONVIF Password**.

Parent topic: Others

Abnormal Device Start in Extremely Low Temperature

Symptom

The ambient temperature of the camera is low. After the camera is powered on and started, the camera can deliver live video but cannot respond to operations such as zoom and focus. Additionally, the text "heating" is displayed on the image and the illuminator or heater is automatically enabled.

Possible Causes

Some models support the low-temperature startup function. When the temperature of the main board is too low, the camera automatically enters the low-temperature startup state when it is powered on. The electromechanical device cannot work properly (no response to operations such as zoom and focus). The camera with a heater automatically enables the heater to heat the camera. The camera with no heater but with an illuminator may forcibly enable the illuminator (users cannot control the illuminator at this time) to heat the camera. The low-temperature startup lasts for a maximum of one hour and then exits automatically. Alternatively, the low-temperature startup automatically exits after the temperature rises. Then the camera enters the normal startup and working state.

Parent topic: Others

Example for Drawing a Traffic Light Area

When drawing a traffic light area, the rectangle box should just cover the traffic lights. If the rectangular box is too large or too small, the detection accuracy may be lowered. Figure 1 shows a correct example. Figure 2 and figure 3 show two incorrect examples.

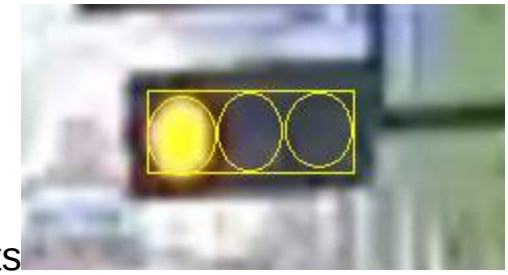
Figure 1 Correct example: the rectangular box just covers the traffic lights 

Figure 2 Incorrect example: the rectangular box is too small and does not completely cover the traffic lights

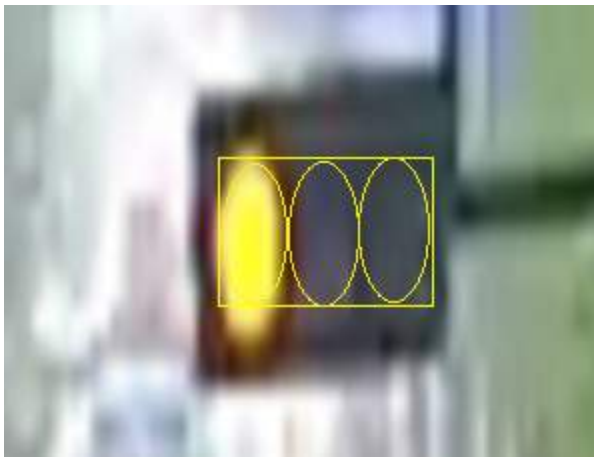
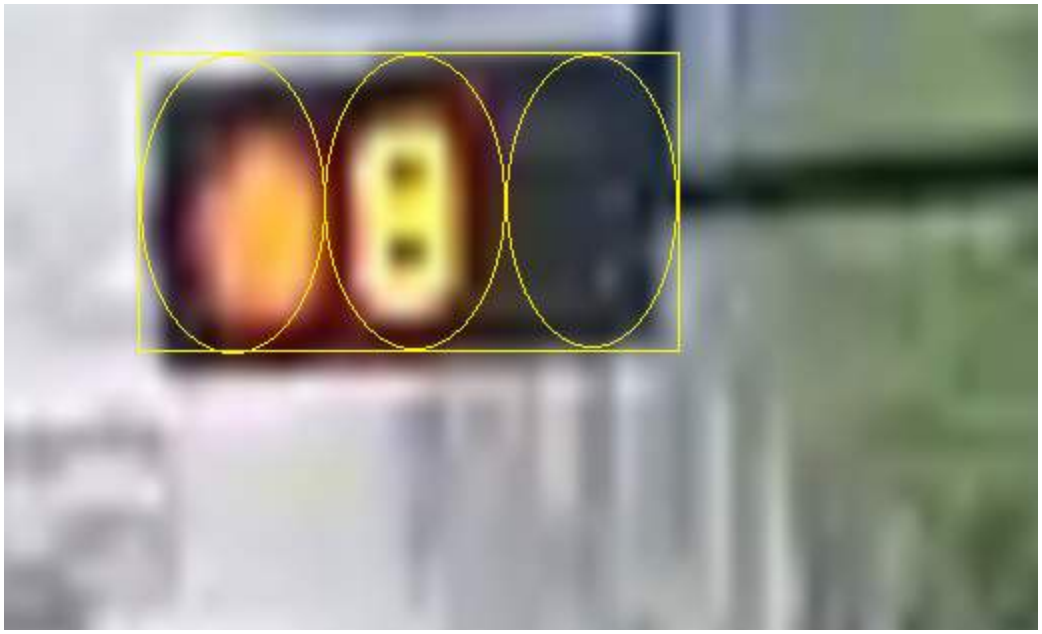


Figure 3 Incorrect example: the rectangular box is too large and covers many irrelevant areas



Parent topic: Others

Failure to Upload Images to the FTP/SFTP Server

Symptom

When a user attempts to upload images to the FTP/SFTP server, the upload fails.

> **NOTE**
>
> The FTP or SFTP server is called the server in this section.

Possible Causes

- The configuration of the server is incorrect.
- During snapshot upload configuration, the customized naming elements contain special characters that do not comply with the naming rules of the server. As a result, images fail to be saved to the server.
- The lane ID or device ID naming element is enabled for image upload, and the element contains special characters that do not comply with the naming rules of the server. As a result, images fail to be saved to the server.

Solution

The solutions are as follows:

- Check whether the server parameters are correctly set. For details, see Setting FTP Parameters.
- Check whether the customized naming elements use special characters that do not comply with the server naming rules. For details, see Setting FTP Parameters.

- Check whether the lane ID or device ID naming element is enabled and whether the element contains special characters that do not comply with the naming rules of the server. For details, see Setting FTP Parameters.

Parent topic: Others

There Is a Possibility that Defocus Occurs When a Vehicle Passes the Image View

Symptom

There is a possibility that defocus occurs when a vehicle passes the image view.

Possible Causes

Object movement in the view may affect the focus stability.

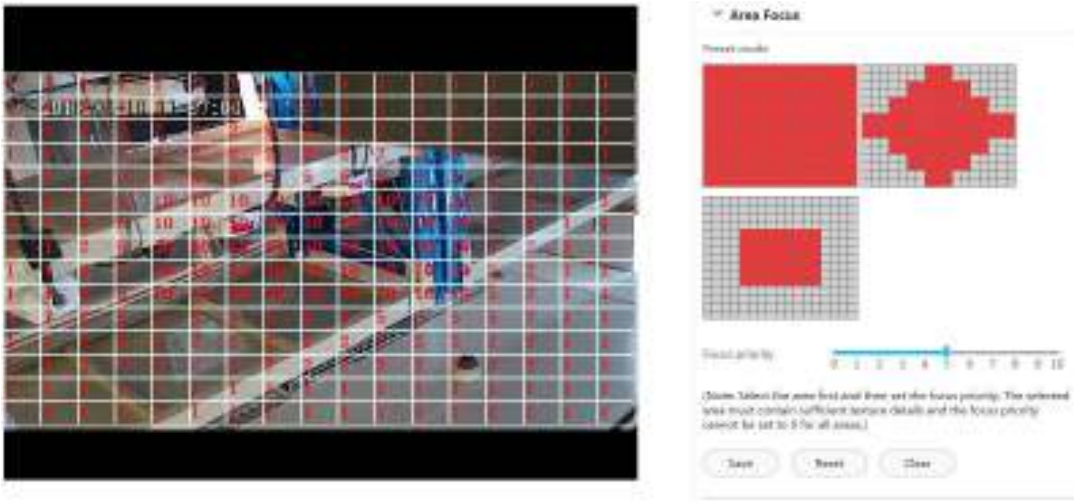
Solution

1. During zooming or one-push focusing, avoid scenarios where large objects (such as vehicles) may pass the image view.
2. If defocus occurs due to moving objects (such as vehicles), you can perform one-push focus to refocus or manually adjust the focus.
3. The semi-automatic focus mode is recommended. You can set the focus area to an area without moving objects to reduce the probability of defocus.

    a. Choose **Configuration** > **Image** > **Area Focus.**

    b. Set **Focus priority** for the area with moving objects to **0** and for the area without moving objects to **10**.

    Figure 1 Configuring the focus area



Parent topic: Others

How Do I Obtain and Use the Milestone 2022 R3 Plug-in?

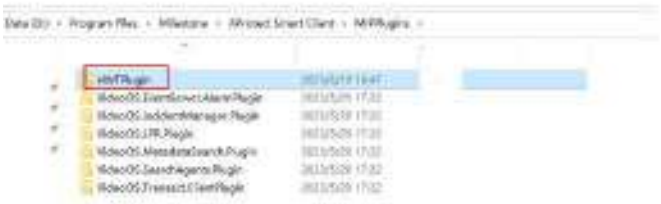
Context

In Milestone 2022 R3, functions such as metadata display and search are added. To use these functions, you need to obtain and install the new plug-in.

Procedure

1. Log in to the HOLOWITS technical support website, search for the Milestone plug-in, and obtain the plug-in package.
2. Decompress the plug-in package in the Milestone path. The example path is **D:\Program Files\Milestone\XPprotect Smart Client\MIPPlugins**, as shown in Figure 1.

   Figure 1 Decompressing the plug-in package in the Milestone path

Parent topic: Others

FAQs

This chapter describes how to locate and troubleshoot common faults.

How Can I Recover My Password If I Forget It?

Why Is a Recording Separately Stored into Multiple Files of Different Sizes?

What Can I Do If the NVR800 or IVS1800 Connected Through ONVIF in HTTPS Mode Cannot Go Online?

What Can I Do If the Key for Encrypting Data on SD Cards Is Leaked?

新节点1

Parent topic: Configuration

How Can I Recover My Password If I Forget It?

Question

How can I recover my password if I forget it?

Answer

- **Recover your password through hardware.**

  Hold down the **RESET** button on the camera to restore the camera to factory settings.

  - To restart the camera, hold down the **RESET** button for less than 3s.
  - To restore the camera to factory settings, hold down the **RESET** button for at least 5s.

    NOTE

    - Be aware that restoring a camera to factory settings may result in data loss.
    - If you hold down the RESET button before powering on the device, the IP address may not be restored. In this case, restart the device again.

- **Recover your password through software.**

  NOTICE

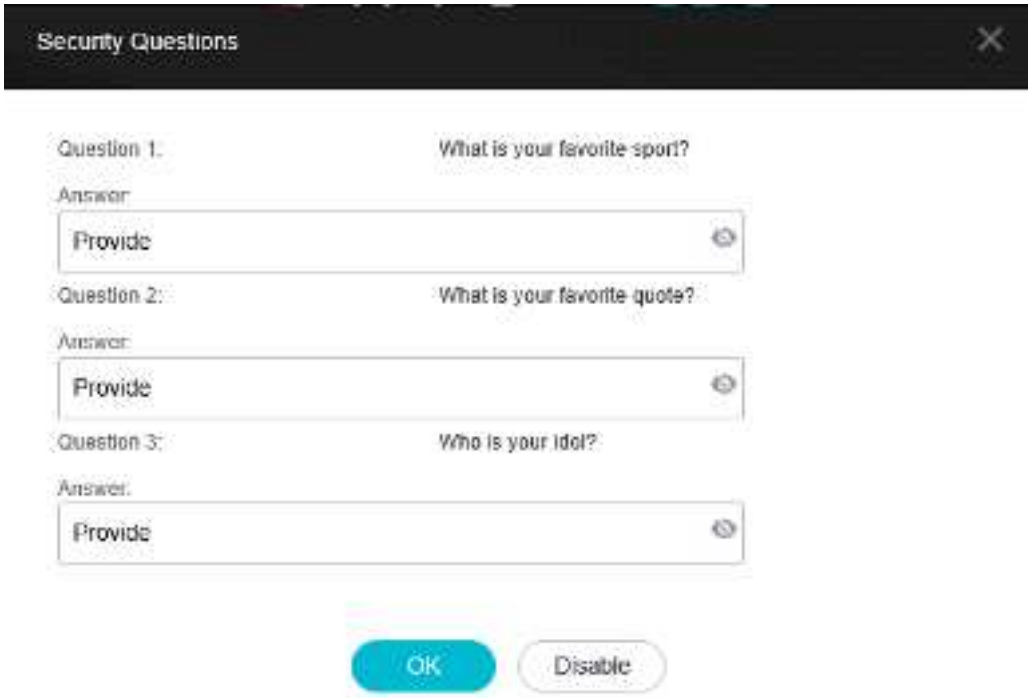
  You can recover your password through software only after you set password protection.

  - **Click Security question.**

    1. Log in to the camera web system (https://*Camera IP address*).
    2. Click **Forgot Password**. The dialog box for selecting a password recovery method is displayed.
    3. Click **Security question** and click **OK**.

       The **Security Questions** dialog box is displayed, as shown in Figure 1.

Figure 1 Security Questions dialog box

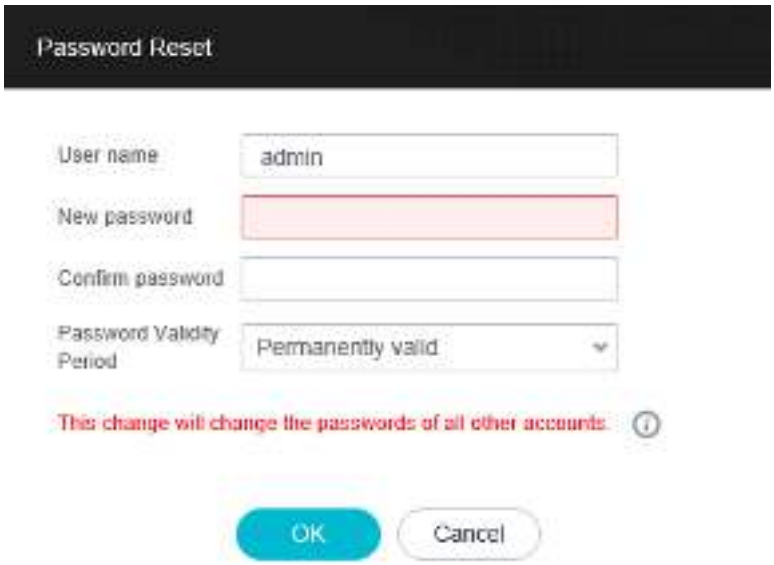


4. Enter the answers to the three security questions in sequence.

   Click **OK**. The dialog box for resetting the password is displayed, as shown in Figure 2.

   The login user name is **admin**. Set the password and **Password Validity Period** and keep the new password secure.

   Figure 2 Resetting the password



NOTE

- Setting **Password Validity Period** to **Permanently valid** may cause security risks. Be cautious with this setting.
- When you set the login password, the SDK, web, ONVIF/RTSP, and RESTful passwords are changed synchronously.
- The user password validity period is available only for the login password of the **admin** user.
- By default, if you entered incorrect passwords for five consecutive times, your account will be locked for five minutes. To change the maximum number of consecutive incorrect password attempts and lock duration, see Configuring Account Locking and Unlocking.
- To prevent security risks, periodically log in as the **admin** user, click the drop-down list box in the upper right corner, choose **Change Password**, and change the password.

5. Click **OK**.

Parent topic: FAQs

Why Is a Recording Separately Stored into Multiple Files of Different Sizes?

Question

Live video is continuously played on the web page. However, after the live video is recorded, the recording is separately stored into multiple recording files of different sizes for download or playback.

Answer

Live video streams are continuously played, but the recording files whose storage space is displayed on the web page, are stored in the database.

For the purpose of easy recording query and download, the generated recordings are stored as recording files of different sizes based on the preconfigured recording types.

For example:

If you specify different recording types for specific time segments, the recording will be stored in the specified recording types.

Assuming that you have configured the following recording plans within 24 hours:

- 00:00-24:00: scheduled recording.
- 08:00-10:00: snapshot-triggered recording.
- 18:00-20:00: alarm-triggered recording. An alarm is generated from 19:00 to 19:10.

In the preceding time segments every day, five recording files with different database file attributes are generated.

1. From 00:00 to 08:00, the first recording file is generated, and the database file attribute is scheduled recording.

2. From 08:00 to 10:00, the second recording file is generated, and the database file attribute is scheduled recording + snapshot-triggered recording.
3. From 10:00 to 19:00, the third recording file is generated, and the database file attribute is scheduled recording.

> **NOTE**
>
> If no alarm is generated during the preconfigured alarm-triggered recording period, attributes of the database file remain unchanged and no new recording file is generated.

4. From 19:00 to 19:10, the fourth recording file is generated, and the database file attribute is scheduled recording + alarm-triggered recording.

> **NOTE**
>
> If an alarm is generated during the preconfigured alarm-triggered recording period, the alarm attribute is added to the database file and a new recording file is generated.

5. From 19:10 to 24:00, the fifth recording file is generated, and the database file attribute is scheduled recording.

NOTICE

The maximum size of a recording file is 256 MB. If the size of a recording file exceeds 256 MB, another recording file that follows the recording content with this attribute is generated.

Parent topic: FAQs

What Can I Do If the NVR800 or IVS1800 Connected Through ONVIF in HTTPS Mode Cannot Go Online?

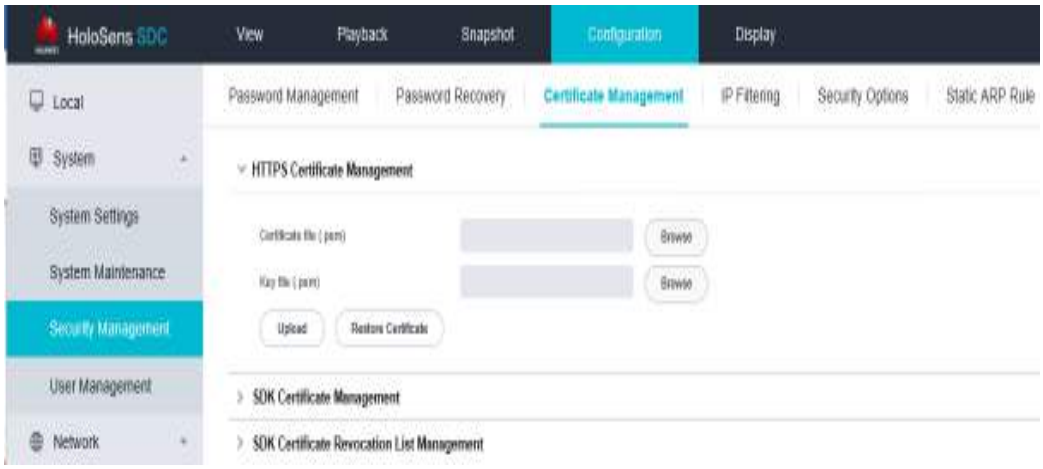
Question

What can I do if the NVR800 or IVS1800 platform connected through ONVIF in HTTPS mode cannot go online?

Answer

Choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **HTTPS Certificate Management**. Upload the HTTPS certificate authenticated by the NVR800 or IVS1800.

Figure 1 HTTPS Certificate Management area



Parent topic: FAQs

What Can I Do If the Key for Encrypting Data on SD Cards Is Leaked?

Question

What can I do if the key for encrypting data on SD cards is leaked?

> **NOTE**
>
> There is a large amount of data on an SD card, and its read and write times are limited. Frequent updates of the encryption key will trigger read and write operations, which shortens the service life of the SD card. Currently, the camera restricts the update of the encryption key.

Answer

1. Choose **Configuration** > **System** > **System Settings** > **Time**. Set **Calibration mode** to **Manual**, and set **Time** to a time point one year later.
2. Choose **Configuration** > **Storage** > **Storage Management** and click **Change Password**.

   You can change the password only after the system verifies the old password.

Parent topic: FAQs

新节点1

Parent topic: FAQs

Configuring Image Optimization

Factors and Functions Related to Image Quality This chapter describes the factors and functions that affect the image quality.

Common Issues and Troubleshooting Methods
This chapter analyzes some common image problems and provides corresponding solutions.

Common Scenarios
The focus of image optimization varies based on the requirements of individual deployment.

Parent topic: Configuration

Factors and Functions Related to Image Quality

This chapter describes the factors and functions that affect the image quality.

- **Lens**
- **Backlight Compensation**
- **Highlight Compensation**
- **Wide Dynamic Range**
- **Function Dependencies and Differences**

Parent topic: Configuring Image Optimization

Lens

The lens is a decisive factor in determining image quality.

- **Focal Length**
- **Focus**
- **Aperture**
- **Shutter**
- **Lens Types**

Parent topic: Factors and Functions Related to Image Quality

Focal Length

The focal length of a lens refers to the distance between the center of the optical lens and its focus. The focal length determines how far and wide the camera can see. With a longer focal length, a camera can see farther, but with a smaller field of view. Table 1 lists the mapping among the focal length, detection distance, and field of view.

Table 1 Mapping among the focal length, detection distance, and field of view

Focal Length	Recommended Maximum Detection Distance (m)	Field of View
2.8 mm	6	110°
3.6 mm	10	85°
4 mm	10–15	75°
6 mm	15–20	53°
8 mm	20–30	40°
12 mm	25–30	25°
16 mm	35–40	20°
25 mm	60–80	12°

Based on the focal length control mode, the lenses can be classified into the following types: **prime lenses**, **manual zoom lenses**, and **motorized zoom lenses**. The focal length of a prime lens is fixed and cannot be adjusted. The focal length of a zoom lens can be adjusted manually or electrically. To adjust the focal length of a manual zoom lens, you need to manually rotate the zoom knob. To adjust the focal length of a motorized zoom lens, you can click the zoom buttons on the camera web page.

Figure 1 Prime lens and zoom lenses



A manual zoom lens is usually labeled **T<---->W**.

- T stands for Tele. Adjusting the lens in the T direction increases the focal length and narrows the field of view. As the focal length increases, object details in the image become larger and clearer.
- W stands for Wide. Adjusting the lens in the W direction reduces the focal length and enlarges the field of view. As the focal length decreases, object details in the image become smaller.

For details about how to adjust the focal length, see Adjusting the Focal Length and Focus Position.

Parent topic: Lens

Focus

Adjusting the camera focus is a process of clearly projecting an object onto a photosensitive surface. Through this process, the focus of the lens is directed onto the sensor.

There are manual focus lenses and motorized focus lenses, as shown in Figure 1. To adjust the focus of a manual focus lens, rotate the focus knob. To adjust the focus of a motorized focus lens, click the focus buttons on the camera web page.

Figure 1 Manual and motorized focus lenses



Generally, a manual focus lens is labeled **FAR<---->NEAR** or **∞<---->N**.

- Adjusting the focus toward the FAR or ∞ direction directs light from further objects on to the sensor.
- Adjusting the focus toward the NEAR or N direction directs light from closer objects on to the sensor.

For details about how to adjust the focus position, see Adjusting the Focal Length and Focus Position.

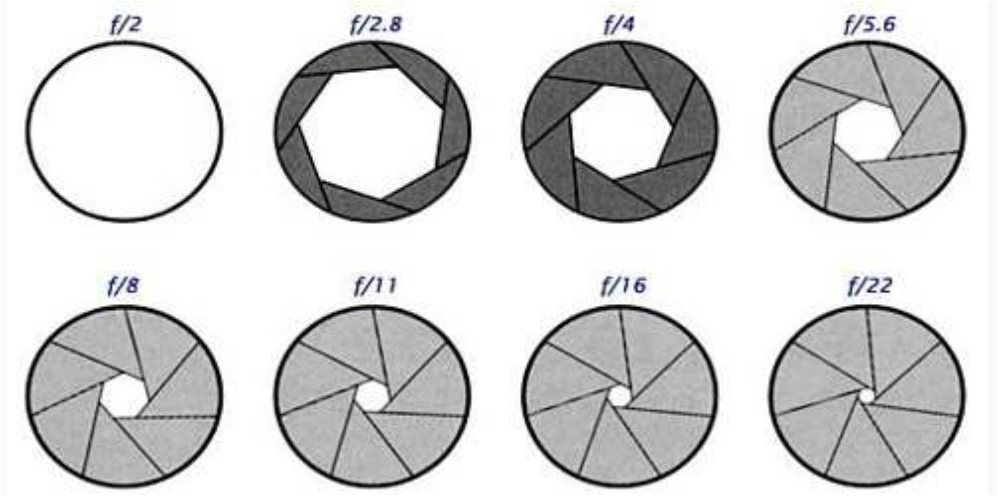
Parent topic: Lens

Aperture

The aperture (opening of the iris) controls the amount of light that enters the lens and exposes the photosensitive surface, which determines the brightness of the image. The F-number, which is the ratio of the focal length to the diameter of the effective aperture, is often used to quantify the size of the aperture.

Common F-numbers include F1.0, F1.4, F2.0, F2.8, F4.0, F5.6, F8.0, F11, F16, F22, F32, F45, and F64. A smaller F-number indicates a wider iris opening, allowing more light entering the lens in a time unit. For the apertures shown in Figure 1, each one halves the amount of light when compared with the previous one. If your aperture is set to F8 and then you widen it to F5.6, you have doubled the amount of light passing through the lens.

Figure 1 Common apertures



As shown in Figure 2, a camera may have a fixed iris lens, manual iris lens, auto-iris lens, or motorized iris lens, depending on the aperture control mode. For a fixed iris lens, the aperture is fixed and not adjustable. For a manual iris lens, the aperture is controlled by adjusting the iris knob. For an auto-iris lens, the aperture size is controlled by DC voltage signals or video signals. For a motorized iris lens, the aperture is controlled using an electric motor. For a P iris, you can click the aperture buttons on the camera web page to change the aperture size.

Figure 2 Fixed and adjustable iris lenses



Generally, a manual iris lens is labeled **O<---->C** or **OPEN<---->CLOSE**.

- Adjusting the aperture in the O or OPEN direction increases the aperture of the lens. In this case, the amount of light passing through the lens increases, and the image becomes brighter. However, if the aperture is too large, the image may be overexposed.
- Adjusting the aperture in the C or CLOSE direction reduces the aperture size of the lens. In this case, the amount of light passing through the lens decreases, and the image becomes darker. However, if the aperture is too small, the image may be underexposed. When the aperture is adjusted to the foremost in the C or CLOSE direction, the iris is opened the least or even closed, depending on the design.

Parent topic: Lens

Shutter

The shutter is a device that controls the effective exposure time of the image sensor.

Shutter speed is a measurement of the length of time that a camera's shutter is open. The unit is second. Common shutter speeds are as follows: 1s, 1/2s, 1/8s, 1/15s, 1/60s, 1/125s, 1/250s, 1/500s, 1/1000s, and 1/2000s.

The longer the shutter is open, the more light comes through. If you double the time that the shutter is open, you will double the amount of light coming in. Figure 1 and Figure 2 show the imaging effects of different shutter speeds.



Figure 1 Fast shutter speed

Figure 2 Slow shutter speed



Figure 1 is shot with a fast shutter speed, 1/1000s. Such a fast shutter speed can help capture clear, detailed images of objects in

motion.

Figure 2 is shot with a slow shutter speed, 1s. Such a slow shutter speed allows the movement of subjects to be imaged across the photograph. However, details of speeding subjects will be missing.

Parent topic: Lens

Lens Types

Lenses can be classified based on the following criteria:

1. By the control modes of focal length, focus, and aperture. In this dimension, lenses can be classified as follows:

   Auto-iris lenses whose focal length and focus are controlled manually or by electric motors

   Lenses whose focal length, focus, and aperture are all controlled manually or by electric motors

2. By the mount type. Based on this criterion, lenses can be divided into C-mount lenses and CS-mount lenses. The physical difference is that a CS-mount lens is designed to be mounted about 5 mm closer to the image sensor than a C-mount lens. C mount lenses are designed to be mounted 17.525 mm in front of the image sensor, while CS-mount lenses are mounted 12.5 mm in front of the image sensor, as shown in Figure 1. The mount type is usually marked on the lens nameplate or packaging. Generally, the C mount is longer.



Figure 1 C mount and CS mount

   Currently, most cameras are CS-mount cameras. To connect a C-mount lens to a CS-mount camera, a C/CS adapter ring must be used, as shown in Figure 2. Otherwise, the imaging effect will be severely affected.

Figure 2 C/CS adapter ring



Parent topic: Lens

Backlight Compensation

In a scene that is unevenly illuminated, the object may appear against a bright background or a light source may exist behind the object. In this case, to the camera the incoming light is bright, so the camera will reduce its exposure (for example, by increasing the shutter speed). However, this reduces the brightness of the overall scene, making the object in the image too dark.

The backlight compensation (BLC) function provided on many cameras helps to mitigate this problem. The image scene is divided into six or seven (with two repeated) areas. The camera measures the light level of each area and calculates exposure based on their weights. For example, the central area may be assigned 9 times more weight than any other area. If the exposure is calculated mainly based on the light level in the central area, an object in the central area can always be clearly imaged.

In scenarios with a very bright background, BLC can provide an ideal exposure for the foreground object, regardless of the position of the object in the scene. In some cases, BLC may cause background overexposure or image noise. Figure 1 shows the imaging of a scene before and after BLC is enabled.

Figure 1 BLC effect 

Parent topic: Factors and Functions Related to Image Quality

Highlight Compensation

In some scenes, overexposure from strong light sources may result in low image quality. In this case, highlight compensation (HLC) can be enabled to compensate for exposure on the strong light spots to enhance the overall image quality.

One particularly illustrative example of the utility of HLC comes from night-time traffic detection. Without HLC, headlights would blind cameras, making it impossible to read license plates or identify other details. With HLC, it reduces the glare of headlights, balancing the overall image brightness and making license plates and other details readable, as shown in Figure 1.

Figure 1 HLC effect



Parent topic: Factors and Functions Related to Image Quality

Wide Dynamic Range

If both areas with highlight radiation and areas with shadow or backlight exist on the same image, the bright area will appear white due to overexposure while the dark area will appear black due to underexposure. This seriously affects the image quality. Wide dynamic range (WDR) was invented to address these issues.

The WDR technology enables a camera to capture several images at a time, using a different exposure level for each image. These images are then combined into a composite, in which objects in both the brightly and dimly lit areas can be seen clearly.

Figure 1 shows a typical scenario with no compensation of any kind. The background is bright, resulting in unclear imaging of people in the foreground. Figure 2 shows the imaging effect when BLC is enabled. People in the dark area are clear, but the background is washed out.



Figure 1 No compensation

Figure 2 BLC enabled



If WDR is enabled, the camera takes a picture shown in Figure 3 with a fast shutter speed, followed by a picture shown in Figure 4 with a slow shutter speed. They work together and provide a balanced image, as shown in Figure 5.

Figure 3 High-speed capture



Figure 4 Low-speed capture



Figure 5 Final effect



Parent topic: Factors and Functions Related to Image Quality

Function Dependencies and Differences

Shutter, Aperture, and Depth of Field

BLC, HLC, and WDR

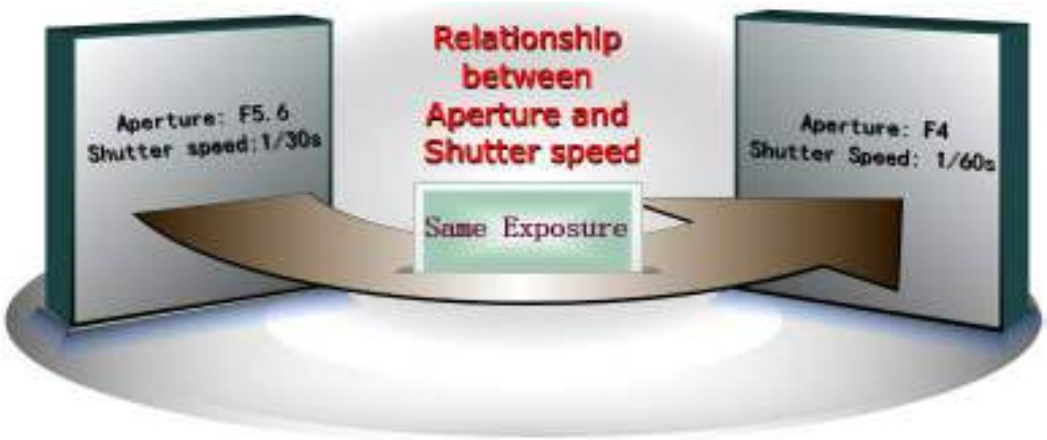
Parent topic: Factors and Functions Related to Image Quality

Shutter, Aperture, and Depth of Field

The amount of exposure is determined by the combination of the aperture size and shutter speed. Different combinations may produce the same exposure amount.

An aperture of F5.6 and a shutter speed of 1/30s let in the same light as an aperture of F4 and a shutter speed of 1/60s, as shown in Figure 1.

Figure 1 Exposure combinations



Although different combinations may achieve the same exposure, they may produce different images.

This is related to the concept of depth of field, which is defined as the distance between the closest and farthest objects in an image that appear acceptably sharp.

The aperture controls not only the amount of light passing through the lens, but also the depth of field, as shown in Figure 2.

Figure 2 Effects of aperture on depth of field



The effects the aperture has on the depth of field are as follows:

- As the aperture size increases, the depth of field decreases. The background and details of more distant objects become more blurry.
- As the aperture size decreases, the depth of field increases. The background and details of more distant objects become sharper.

Parent topic: Function Dependencies and Differences

BLC, HLC, and WDR

BLC, HLC, and WDR technologies enable cameras to capture clear and balanced images even in scenes with strong brightness contrast between the foreground and background.

BLC sacrifices the image contrast to improve imaging of darker areas. HLC prevents the overexposure of highlight areas. WDR is more advanced and improves image effects to a greater extent. However, WDR imposes heavy demands on system resources, and may cause trailing in scenarios involving fast moving objects.

Table 1 Differences between BLC, HLC, and WDR

Item	BLC	HLC	WDR
Technical principle	Divides an image or scene into different sections and adjusts the lighting accordingly.	Detects strong lights in the image and reduces exposure on these spots.	Takes one image with longer exposure time and one with shorter exposure time and combines them to balance lights on overexposed and underexposed areas.
Resource usage	Low	Low	High
Effect	The back lit object is clearer.	The exposure on strong light sources is reduced.	Both bright and dark areas are clear.
Side effect	The background may be overexposed, and the noise in dark areas may increase.	New noise may be introduced in the image, and overexposure occurs in the daytime.	If there is a fast-moving object, trailing or ghosting may occur. The imaging effect at night is affected.

NOTICE

The same set of parameters or functions cannot be used for image optimization and adjustment in all time segments of the same scenario. For example, the setting adjustment made in the daytime may not take effect for night-time imaging. In some cases, night-time image quality may deteriorate due to setting changes made in the daytime. Therefore, it is recommended that different image profiles be used for different time segments. For details about how to set an image profile, see the Configuration Guide.

Parent topic: Function Dependencies and Differences

Common Issues and Troubleshooting Methods

This chapter analyzes some common image problems and provides corresponding solutions.

> **NOTE**
>
> Note that the provide solutions are scenario-specific. The image effect optimization in other time segments may require another set of image settings and functions. After a solution is verified, you can set the parameter settings and functions in use as a profile that applies specifically to the involved scenario.

- Image Clarity Issues
- Image Brightness Issues
- Color Cast Issues
- Image Noise Issues
- Moire Pattern Issues
- Purple Fringing Issues on Video Images of PTZ Dome Cameras or Small Bullet Cameras
- Infrared Imaging Issues
- Wave Pattern Issues
- Motion Blur Issues
- Dark Images with Infrared Illuminators
- Power Frequency Flicker Issues
- Ghosting and Lens Flare Issues
- Severe Halation Issues at Night
- Dark Images at Night

Reflection Caused by Flying Insects or Dust When Using Infrared Light

Blurred Infrared Image from a Fixed Dome Camera or Bullet Camera

Part of the Image is Blurry

Parent topic: Configuring Image Optimization

Image Clarity Issues

Image Blur

Low Contrast

Parent topic: Common Issues and Troubleshooting Methods

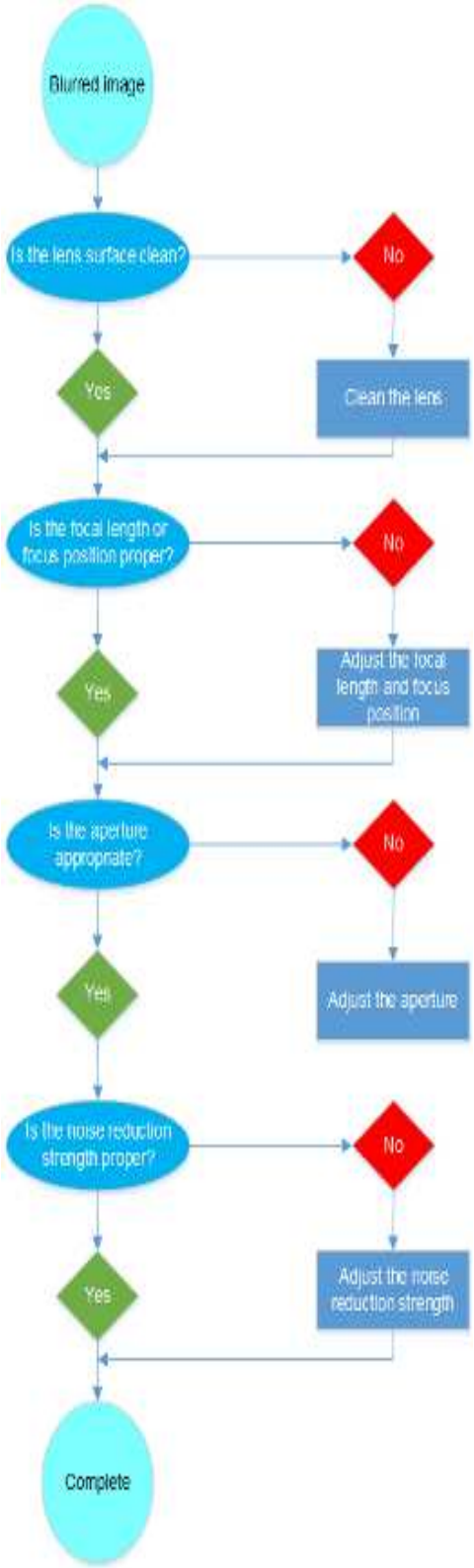
Image Blur

Possible causes of blurred images are as follows:

- There are water stains or dust on the lens or the lens is not clean.
- The focal length of the camera is incorrect, or the focus position is inaccurate.
- The aperture is inappropriate.
- The noise reduction strength is inappropriate.

Figure 1 illustrates the troubleshooting process.

Figure 1 Troubleshooting process for image blur



Adjusting the Focal Length and Focus Position

For different scenarios and requirements, you must select appropriate lenses to ensure that the required detection area is within the focal length range.

The troubleshooting method of image blur depends on the lens type:

- If the camera uses a prime lens, first check whether the object is within the detection distance determined by the focal length. Since the focal length cannot be changed, you can restart the camera and then check whether the image sharpness is improved.
- If the camera uses a manual zoom lens, you need to adjust the focal length after installing the lens on the camera. The procedure is as follows:

    1. Rotate the zoom ring (labeled W--T) and the focus ring (labeled N--F) at the same time to preliminarily make the object seen and determine the required field of view.
    2. After the field of view is determined, tighten the zoom knob. Then adjust the focus ring to focus the camera on an object (which generally should be in the center of the detection area) to obtain the image that is the sharpest.

    Figure 2 shows the lens elements.

Figure 2 Zoom knob and focus knob



NOTE

Ensure that the camera lens mount matches the lens type. Generally, the camera uses a CS mount. To connect to a C mount lens, a C/CS adapter ring must be used. However, if a C/CS adapter ring is still used even when the camera mount and lens matches, the image effect will be severely affected and cannot be adjusted through other means.

- If the camera uses a motorized zoom lens, you can click  or  to adjust the focal length, and  or  to adjust the focus. These buttons can be found on the right of the live video viewing pane, as shown in Figure 3.

Figure 3 Zoom and focus buttons



Adjusting the Aperture

The aperture size directly affects the amount of light entering the camera, thereby affecting the adjustment of the shutter speed and the gain, and finally affecting the image sharpness.

In Figure 4, the image appears blurry due to a small aperture. After the aperture is enlarged, the obtained image is much sharper, as shown in Figure 5.

Figure 4 Image obtained with a small aperture



Figure 5 Image obtained with an enlarged aperture



The aperture also directly affects the depth of field.

- If the aperture is too large, the depth of field becomes especially shallow. As a result, many details in the image are out of focus and blurry.
- If the aperture is too small, the imaging performance in dimly lit environments is poor due to insufficient light.

Therefore, you need to adjust the aperture, especially for manual iris lenses. Adjust the aperture to an appropriate size during the installation. If there is no special requirement on the depth of field, you are advised to adjust the aperture to the maximum to ensure clear imaging at night time.

NOTE

- Try to select lenses supporting a large aperture, for example, F1.2. A smaller F-number indicates a larger aperture.
- For intelligent cameras designed for special purposes such as license plate recognition and target detection, focus on the effect of the snapshot area when adjusting the aperture.

The aperture adjustment method depends on the lens type:

- For a manual iris camera, you can rotate the aperture ring on the lens to adjust the aperture, as shown in Figure 6.

  Figure 6 Aperture ring

- For a bullet or PTZ dome camera with a motorized lens (P iris), log in to the camera web system, choose **Configuration** >

Image > **Display** > **Exposure**, and set **Exposure mode** to **Aperture priority**, as shown in Figure 7. On the live video viewing page, click  or  to adjust the aperture, as shown in Figure 8.

Figure 7 Setting the exposure mode

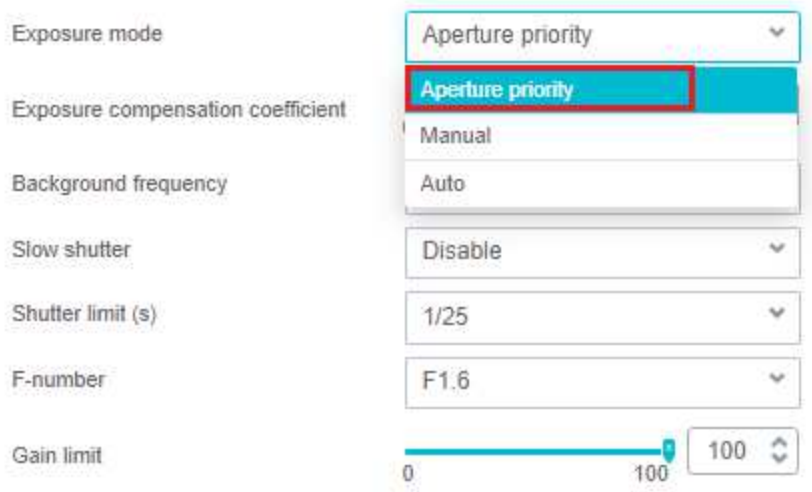


Figure 8 Adjusting the aperture for a bullet or PTZ dome camera



Adjusting the Noise Reduction Strength

The noise reduction (NR) or denoising function can be enabled to optimize the image effect and enhance the sharpness of image details. However, strong noise reduction may also impair the image sharpness.

Currently, common NR technologies include **spatial NR** and **temporal NR**. If the **Denoising** parameter of your camera is set to **Expert mode**, you can set the levels of spatial NR and temporal NR.

(For details, see **Image Parameter Settings** in the *Configuration Guide*).

- Strong spatial NR will wash out image details and blur the edges. As shown in Figure 9 and Figure 10, the edge details appear more blurry after the spatial NR is strengthened.

  Figure 9 Original image

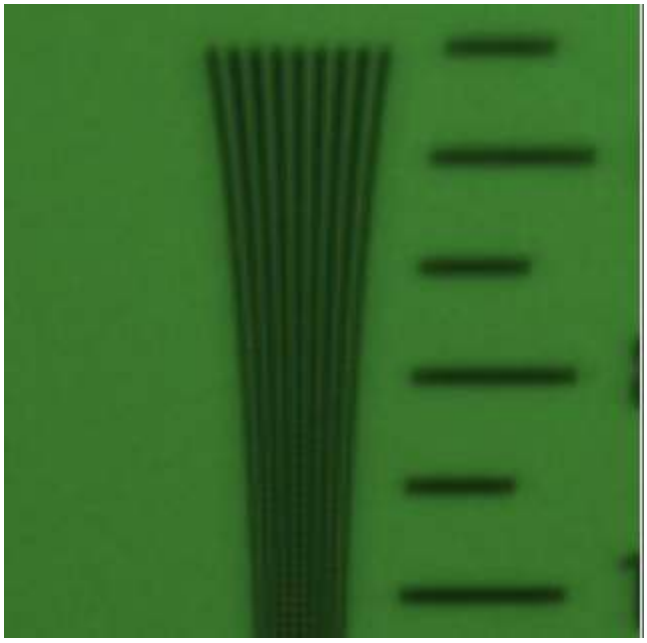
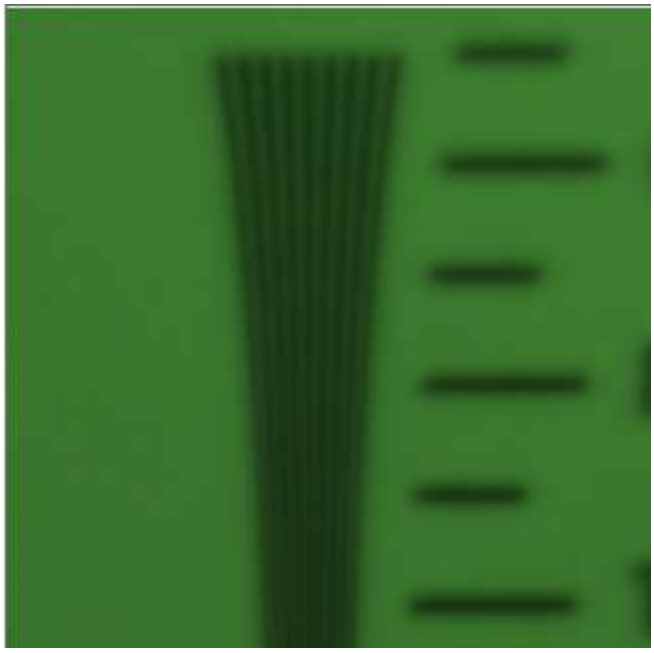
  

  Figure 10 Image after spatial NR strengthening

- For moving objects, the temporal NR level will strongly affect the sharpness. A high temporal NR level may destroy image details and result in trailing, as shown in Figure 11. However, for static objects, the effect of the temporal NR on the sharpness is small.

  Figure 11 High temporal NR level

Based on the statements above, we can draw the following conclusions: In scenes where there are many moving objects such as a traffic checkpoint, the temporal NR cannot be set to a high level and the spatial NR is mainly applied. For indoor areas where the scene is almost static, temporal NR is often applied. You need to set the NR levels based on the site requirements.

Parent topic: Image Clarity Issues

Low Contrast

An image with low contrast usually appears flat or dull, as is the left picture in Figure 1. This is caused by narrow dynamic range in the image and can be improved by adjusting the brightness and contrast.

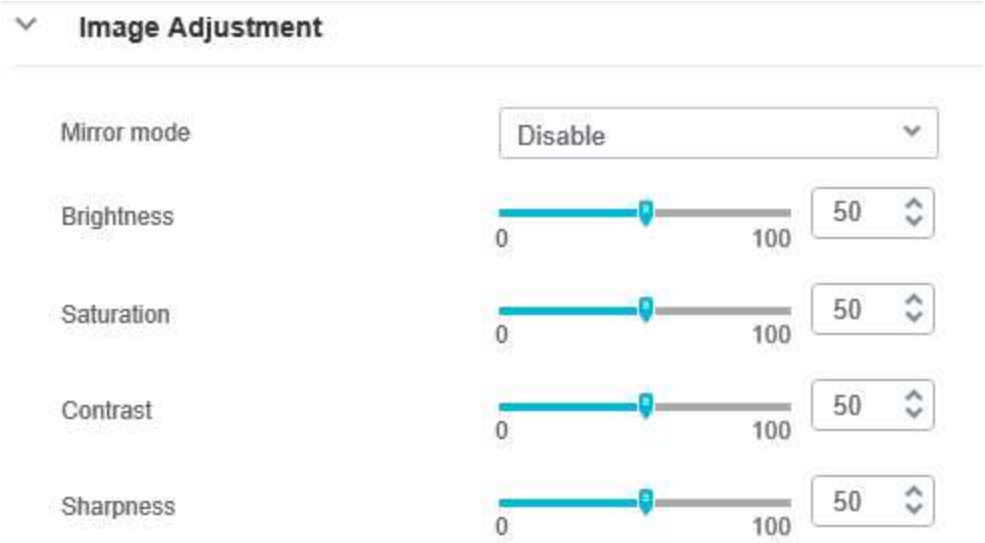
Troubleshooting Suggestions

Log in to the camera web system and choose **Configuration** > **Image** > **Display** > **Image Adjustment**.

1. Slightly decrease the value of **Brightness**.
2. Slightly increase the value of **Contrast**.

As shown in Figure 1, the image is improved after the adjustment.

Figure 1 Adjusting brightness and contrast



Parent topic: Image Clarity Issues

Image Brightness Issues

If the image appears too bright or dark, like the example in Figure 1, the exposure may be improper or the default settings may not be suited to the detection scene.

Figure 1 Insufficient illumination



Factors to Take into Account During Optimization

- Lens cleanness
- Exposure settings, such as the exposure compensation coefficient
- Brightness
- Contrast
- Aperture size

Troubleshooting Suggestions

1. Check whether the lens is scratched or stained.
2. If the aperture is adjustable, check whether the aperture is appropriate and adjust the aperture to obtain images with proper brightness. For details about how to adjust the aperture, see Adjusting the Aperture.

3. Adjust the exposure settings. Log in to the camera web page and choose **Configuration** > **Image** > **Display** > **Exposure**. Adjust the value of **Exposure compensation coefficient**, as shown in Figure 2, until the image brightness is moderate.

   Figure 2 Adjusting exposure compensation coefficient



> **NOTE**
>
> If the image has no problems other than brightness problems, you are advised not to adjust the shutter speed or gain limit. These two settings affect image quality in other time periods (such as in the evening).

4. In the camera web system, choose **Configuration** > **Image** > **Display** > **Image Adjustment**, and adjust the values of **Brightness** and **Contrast**, as shown in Figure 3, until the imaging effect meets your requirements.

Figure 3 Adjusting brightness and contrast



Parent topic: Common Issues and Troubleshooting Methods

Color Cast Issues

Certain types of light can affect the whole, or a portion, of an image evenly, causing color casts. For example, under a yellow light, the whole image may appear yellowish, as shown in Figure 1.



Figure 1 Color cast

Possible Causes

- If the white balance color correction is inaccurate, this will result in persistent discoloration of images.
- If color distortions occur during the color reproduction, the hue or saturation of certain objects will be abnormal.
- If the camera ICR is not switched to the color mode, images generated in the daytime will appear purple and red.

Troubleshooting Suggestions

1. Adjust the white balance settings. Log in to the camera web system and choose **Configuration** > **Image** > **Display** > **White Balance**. Select a white balance mode based on the onsite environment, and adjust the values of **Red gain** and **Blue gain** if required, as shown in Figure 2. For descriptions and configuration details of white balance modes, see **Image Parameter Settings** in the *Configuration Guide*. Generally, you are advised to set **Mode** to **Auto**.

Figure 2 Adjusting the white balance



2. Adjust the saturation for color reproduction. Log in to the camera web system and choose **Configuration** > **Image** > **Display** > **Image Adjustment**. Adjust the setting of **Saturation**, as shown in Figure 3, until the image effect meets your requirements.

Figure 3 Adjusting saturation

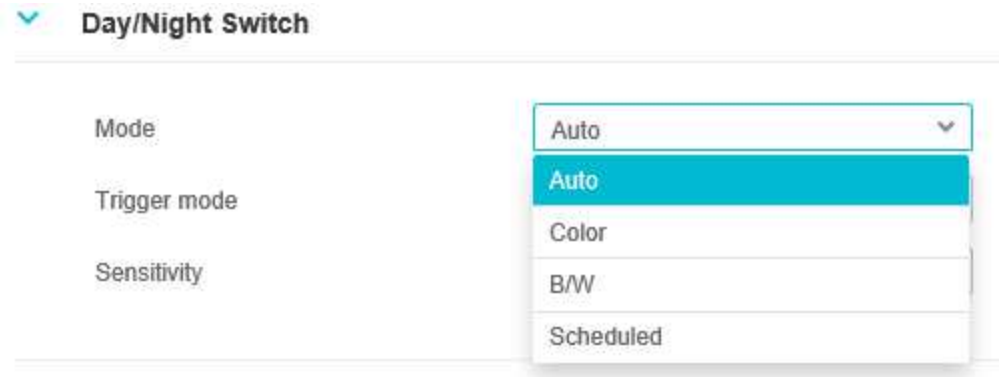


NOTE

For a PTZ dome camera whose detection scene may change due to pan and tilt operations, take the image effects of other scenes and environments into consideration when adjusting the white balance settings, and saturation.

3. If the color casts are caused by the ICR, first check whether the power supply voltage of the camera meets the specifications. If not, replace the power module to ensure that the power supply to the camera is normal. If the power supply is normal but the problem persists, force the camera to enter the color mode. Choose **Configuration** > **Image** > **Display** > **Day/Night Switch**. In the area shown in Figure 4, set **Mode** to **Color**.

   Figure 4 Changing the day/night switch mode



   If the problem persists, contact the supplier or technical support engineers.

Parent topic: Common Issues and Troubleshooting Methods

Image Noise Issues

If the image is noisy, as shown in Figure 1, details may be obscured and the image may be unclear.

Figure 1 Image noise



Possible Causes

- Strong signal interference exists in the surrounding environment or signal transmission lines of the camera.
- The noise reduction function is disabled or the noise reduction coefficient is set incorrectly.
- The gain is too high.

Troubleshooting Suggestions

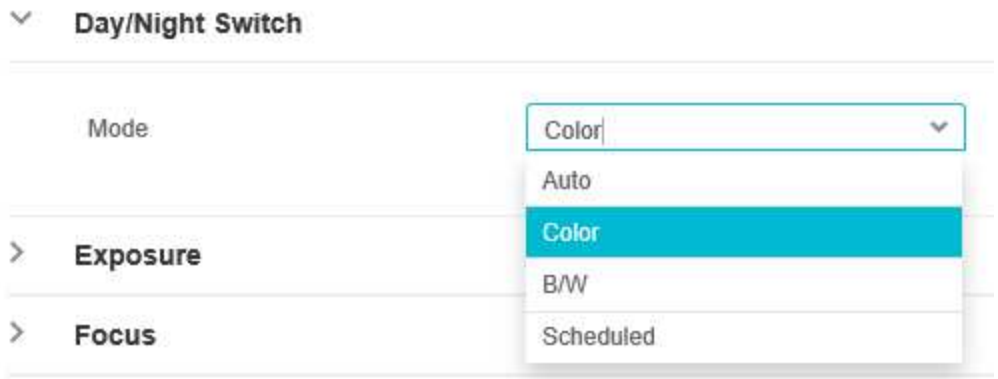
Examine the surrounding environment and transmission line of the camera to ensure that no strong electromagnetic interference exists.

In the nighttime, the recommended troubleshooting procedure is as follows:

1. Switch the camera to the color mode. Log in to the camera web system, choose **Configuration** > **Image** > **Display** >

Day/Night Switch, and set **Mode** to **Color**, as shown in Figure 2.

Figure 2 Changing the day/night switch mode



2. In the camera web system, choose **Configuration** > **Image** > **Display** > **Image Enhancement** and adjust the noise reduction coefficient until you get the desired effect, as shown in Figure 3.

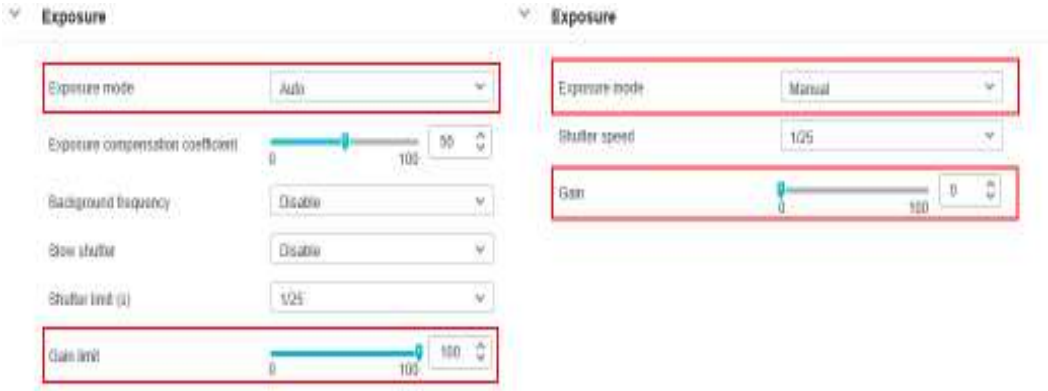
   Figure 3 Adjusting the noise reduction coefficient



3. Choose **Configuration** > **Image** > **Display** > **Exposure**. If **Exposure mode** is set to **Auto**, slightly decrease the value of **Gain limit**. This will reduce noise and image brightness may slightly decrease. If **Exposure mode** is set to **Manual**, slightly

decrease the value of **Gain**, as shown in Figure 4. Generally, the automatic exposure mode is recommended.

Figure 4 Adjusting gain



In the daytime, skip step 1.

After proper adjustment, the image effect will improve, as shown in Figure 5. Noise is reduced and patterns are smoother.

Figure 5 Noise reduction effect



Parent topic: Common Issues and Troubleshooting Methods

Moire Pattern Issues

Moire pattern is a disruptive pattern that occurs on a video image when some position of the view contains small, repetitive details that are comparable to the resolution and scan rate of the camera. Figure 1 shows an example.



Figure 1 Moire pattern

This phenomenon may occur if the camera sensor is not advanced enough to process high frequency information. To reduce the appearance of moire patterns, you can try changing the sharpness or aperture settings.

Troubleshooting Suggestions

- For cameras of V200R003 and later versions, log in to the camera web system, choose **Configuration** > **Local** > **Playing Settings**, select **Remove moire pattern**, as shown in Figure 2. This function can reduce the moire pattern interference.

Figure 2 Enabling moire pattern removal



NOTE

- This function takes effect only when the rendering mode is D3D.
- An integrated video card that can hard decode the video streams at the current resolution must be used.

- Reduce the sharpness. Choose **Configuration** > **Image** > **Display** > **Image Adjustment**, and decrease the value of **Sharpness**, as shown in Figure 3. Check the image effect and make fine adjustments based on the site requirements. If the image then becomes too dark, you can adjust the brightness and contrast to improve the overall effect.

  Figure 3 Adjusting sharpness



- Enlarge the aperture if it is adjustable. For a manual iris lens, rotate the aperture ring to increase the aperture. For a motorized iris lens, log in to the camera web system, choose **Configuration** > **Image** > **Display** > **Exposure**, set **Exposure mode** to **Aperture priority** and then increase the aperture size, as shown in Figure 4. (A smaller F-number indicates a larger aperture.)

  Figure 4 Adjusting aperture

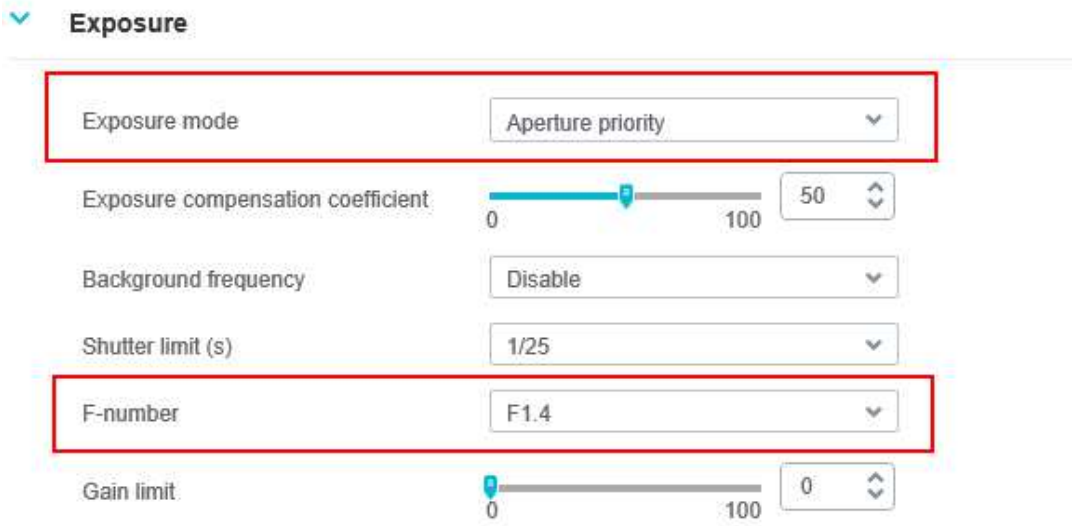


Figure 5 shows the ideal effect after the adjustment.

Figure 5 Effect after adjustment



Parent topic: Common Issues and Troubleshooting Methods

Purple Fringing Issues on Video Images of PTZ Dome Cameras or Small Bullet Cameras

Symptom

Purple fringing may occur in some scenarios, for example, when the image mode is switched to wide dynamic range (WDR) for cameras, as shown in Figure 1.



Figure 1 Purple fringing

Troubleshooting Suggestions (for PTZ Dome Cameras)

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display**, click **Exposure**, and set **Exposure mode** to **Aperture priority**.
3. (Optional) If purple fringing still exists, set **F-number** to **F2.8** and check whether purple fringing exists on the video image.

Troubleshooting Suggestions (for Small Bullet Cameras)

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display**, click **Exposure**, and set **Exposure mode** to **Auto**.

3. Set **Exposure compensation coefficient** to **30** and check the image effect.
4. (Optional) If purple fringing still exists, perform the following operations:
    a. Choose **Configuration** > **Intelligence**. Toggle on **Target Capture** in the **Target Intelligence** area.
    b. Click **Settings** next to **Target Capture**. The **Target Capture** page is displayed.
    c. Choose **Area Settings** > **Advanced Parameters** and select **Brightness compensation**.
    d. Set **Compensation level** to **30**.
    e. Click **Save** and check the target capture effect on the video image.

Figure 2 shows the capture effects before and after troubleshooting.

Figure 2 Capture effects before and after troubleshooting



Parent topic: Common Issues and Troubleshooting Methods

Infrared Imaging Issues

IR Glare

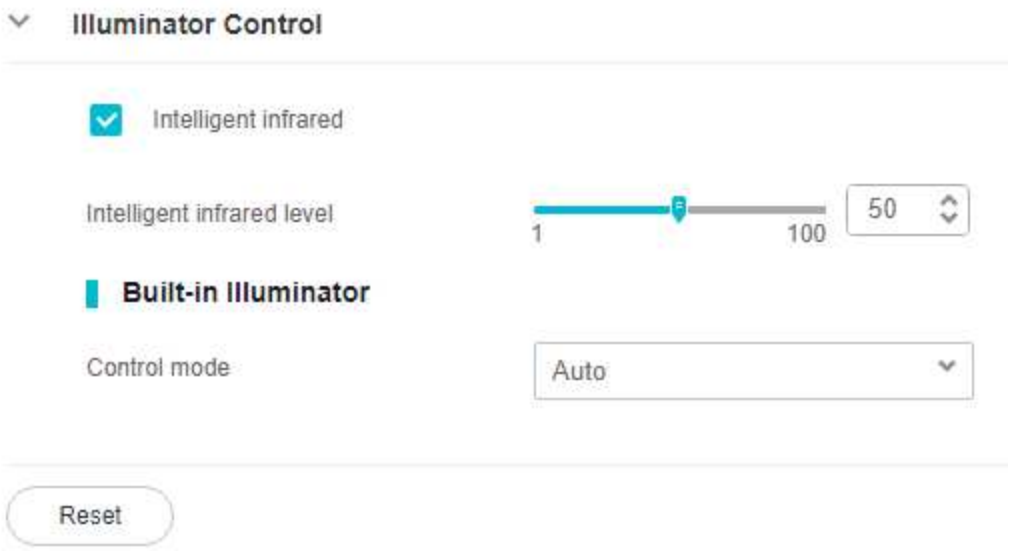
If there are reflective surfaces or objects (such as walls) close to the lens, infrared glare may occur at night. The whole image is washed out and details cannot be seen clearly, as shown in Figure 1.



Figure 1 Infrared glare

In this case, you can log in to the camera web system, choose **Configuration** > **Image** > **Display** > **Illuminator Control**, and select **Intelligent infrared**, as shown in Figure 2.

Figure 2 Enabling the intelligent infrared function



If there is still slight overexposure, slightly decrease the value of **Intelligent infrared level**. If the infrared image then becomes too

dark due to blocking of reflective objects, disable the intelligent infrared function or adjust the camera angle.

You can also change the value of **Control mode** to **Manual**, and then enable and adjust the brightness of low beam, mid beam, and high beam.

NOTE

- For fixed zoom and manual zoom IR cameras, the infrared illuminator group cannot be selected.
- For some models, if the camera is running at a temperature of –20ºC or below, the heater is started to protect the internal components. Due to the power consumption of the heater, the power of the infrared illuminator decreases, and the night vision performance deteriorates. The heater will be on for about one hour.

IR Reflection

If there are reflective surfaces or objects (such as walls and leaves) too close to the lens, these objects can be over exposed in night-time images. The camera will automatically compensate for the overexposure by dimming the image. As a result, objects farther away appear darker in the images, as shown in Figure 3.

Figure 3 IR reflection



In this case, consider the following solutions:

1. Remove the reflective object near the lens. In the example, you can cut off the leaves.
2. Adjust the shooting angle and installation position of the camera to avoid reflective objects or IR reflection. If the reflective object is a wall, you need to adjust the shooting angle and installation position of the camera to prevent the reflected infrared light from entering the camera.

In this case, after the camera shooting angle and installation position are slightly adjusted, the imaging effect at night is improved, as shown in Figure 4.

Figure 4 After angle and position adjustment



Parent topic: Common Issues and Troubleshooting Methods

Wave Pattern Issues

Particularly in indoor scenarios, electromagnetic interference near the camera can cause wave-like patterns to appear in images.

Possible causes:

- There is electromagnetic interference nearby.
- The power supply does not match the camera specification.
- The camera is not properly grounded.
- The indoor fluorescent lamp frequency does not match the camera background frequency.

To improve the image quality, you need to eliminate the interference from cable connections and other environmental elements. Start by ensuring the following:

1. There is no strong interference near the camera.
2. The camera power supply is correctly configured.
3. The camera is properly grounded.

If an indoor light source exists, change the background frequency of the camera to match the frequency of the light source. Choose **Configuration** > **Image** > **Display** > **Exposure** and set **Background frequency**, as shown in Figure 1. Alternatively, adjust the angle of the camera to avoid displaying the light source in the image.

Figure 1 Changing background frequency



Parent topic: Common Issues and Troubleshooting Methods

Motion Blur Issues

Symptom

A moving object in the snapshot is blurry.

Figure 1 Motion blur 

Possible Causes

- Objects or pedestrians move too fast.
- Camera shutter speed is too slow.

Troubleshooting Suggestions

Adjust the shutter speed based on how fast the object moves.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display** > **Exposure**.
3. Adjust the value of **Shutter limit (s)**.

   The recommended value is **1/100** for pedestrian detection and **1/250** for vehicle detection. Table 1 lists the recommended shutter speeds for various moving speeds.

   Table 1 Recommended shutter speeds for different moving speeds

Moving Speed (km/h)	Shutter Speed (s)
40	1/150
60	1/180

Moving Speed (km/h)	Shutter Speed (s)
80	1/250
100	1/350
120	1/450

NOTE

Parent topic: Common Issues and Troubleshooting Methods

Dark Images with Infrared Illuminators

Symptom

When using infrared illuminators, you find that the video is too dark.

Possible Causes

- The infrared illuminators are not turned on.
- There are highly reflective objects near the camera, causing the video to appear dark, even with good light exposure.

Troubleshooting Suggestions

1. Manually turn the infrared illuminators off and on and check whether image brightness is affected.
    - If not, the infrared illuminators or other related components may be faulty. In this case, contact technical support for assistance.
    - If so, go to 2.
2. Perform the troubleshooting steps under **Configuration** > **Image** > **Display** > **Illuminator Control**:
    a. Adjust the camera angle or move the reflective object to reduce light reflection.
    b. Lower the intelligent infrared level.
    c. Enable backlight compensation (not recommended).
    d. Lower the infrared illuminator intensity (not recommended).

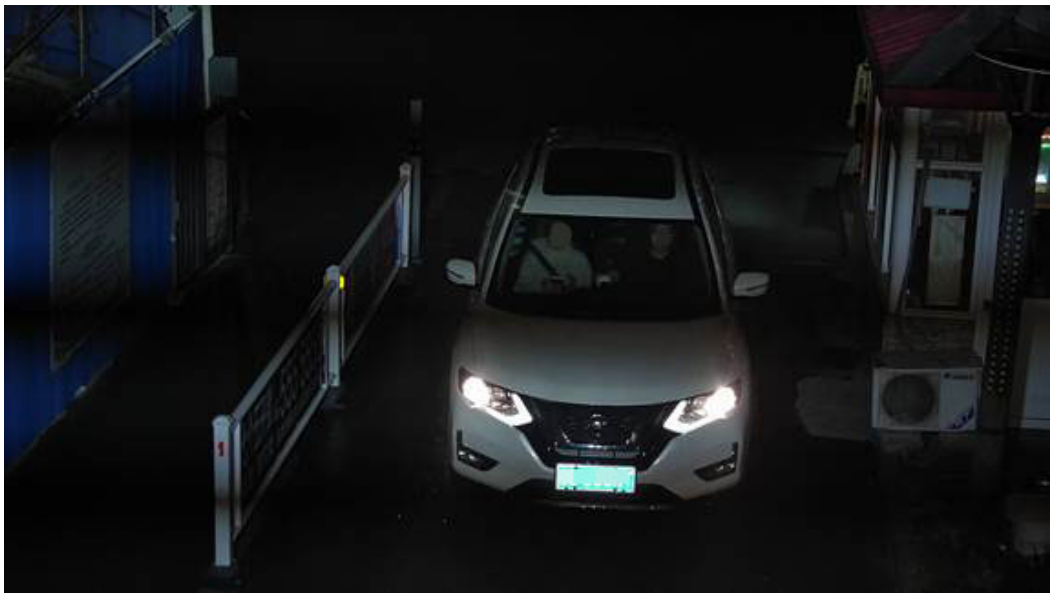
Parent topic: Common Issues and Troubleshooting Methods

Power Frequency Flicker Issues

Symptom

Static or scrolling stripes appear on the image.

Figure 1 Light flickering



Possible Causes

If the ambient light source works under a power frequency that is significantly slower than the shutter speed, the signal collected by the shutter is inconsistent with the actual signal emitted.

Troubleshooting Suggestions

- Method 1: Add a continuous light with higher power.
- Method 2: Set the background frequency based on the power frequency under **Configuration** > **Image** > **Display** > **Exposure**.

Figure 2 Setting the background frequency



Parent topic: [Common Issues and Troubleshooting Methods]

Ghosting and Lens Flare Issues

Symptom

An abnormal light spot or beam appears in the image.

Figure 1 Ghosting and lens flares



Possible Causes

Light is reflected back and forth inside the lens, causing lens flares.

Troubleshooting Suggestions

1. Adjust the camera direction until it does not face the light source directly.
2. Block unwanted light by using devices such as a lens hood on the camera lens.
3. Block unwanted light emitting from the light source.
4. Remove dirt from the lens and housing.

Parent topic: Common Issues and Troubleshooting Methods

Severe Halation Issues at Night

Symptom

Halation is severe at night.



Figure 1 Halation

Possible Causes

In a nighttime point light source setting, the light source distribution and luminance intensity may differ greatly in the image.

Troubleshooting Suggestions

1. Choose **Configuration** > **Image** > **Display** > **Backlight**, enable highlight compensation, and check the image. If the problem persists, go to 2.
2. Choose **Configuration** > **Image** > **Display** > **Exposure**, lower the gain limit, and check the image. If the problem persists, go to 3.
3. Adjust the camera angle to avoid contact with strong light sources and check the image. If the problem persists, go to 4.
4. If the detected object is located in a bright area, choose **Configuration** > **Image** > **Display** > **Backlight**, enable

backlight compensation, and check the image. If the problem persists, contact technical support.

Parent topic: Common Issues and Troubleshooting Methods

Dark Images at Night

Symptom

The image is too dark, and the objects in the image are not clear.

Possible Causes and Troubleshooting Suggestions

- There is a strong point light source in the image, causing it to appear dark.

    1. Adjust the camera angle to avoid contact with the light source.
    2. Increase the exposure compensation coefficient under **Configuration** > **Image** > **Display** > **Exposure**.

        You can set a plan with different image parameters for different periods (daytime and nighttime) for optimal image effect. Set the plan under **Configuration** > **Image** > **Profiles** or **Configuration** > **Image** > **Profiles** > **Profile Plan**.

- Image parameters such as the gain and shutter speed are restricted.

    Increase the gain limit and decrease the shutter speed. If lighting is insufficient, slightly increase the exposure compensation coefficient. Set the parameters under **Configuration** > **Image** > **Display** > **Exposure**.

Parent topic: Common Issues and Troubleshooting Methods

Reflection Caused by Flying Insects or Dust When Using Infrared Light

Symptom

Moving bright spots occur in the image.



Possible Causes

In an infrared setting, flying insects or moving dust causes light to reflect. This is a natural phenomenon that usually occurs on outdoor construction sites.

Troubleshooting Suggestions

1. Lower the infrared illuminator intensity under **Configuration** > **Image** > **Display** > **Illuminator Control** (not recommended).
2. Lower the temporal noise reduction level if smearing occurs in bright spots, but this will increase the noise at the same time. Set this parameter as needed.

    a. Choose **Configuration** > **Image** > **Display** > **Image Enhancement**.

    b. Set **Denoising** to **Expert mode**.

c. Lower the temporal noise reduction level.

Parent topic: Common Issues and Troubleshooting Methods

Blurred Infrared Image from a Fixed Dome Camera or Bullet Camera

Symptom

The infrared image is blurred when you zoom in on an object using a non-PTZ dome camera.

Possible Causes

- Image parameters are modified manually.
- The infrared light is reflected onto the lens from a short distance.
- The plastic protective film has not been removed.
- The dome camera's housing is damaged or light leaks through the shade protector.

Troubleshooting Suggestions

1. Check whether the image setting has been modified, such as the contrast setting.

   You can adjust the gamma correction strength under **Configuration** > **Image** > **Display** > **Image Enhancement** to ensure the image clarity.

Figure 1 Adjusting the gamma correction strength



2. Adjust the position of the camera to prevent nearby obstacles such as leaves from causing light reflection.
3. Check whether the lens protective film has been removed. If not, remove it.
4. Check whether any components are damaged. If so, replace the damaged components.

Parent topic: Common Issues and Troubleshooting Methods

Part of the Image is Blurry

Symptom

Only part of the image is clear. For example, in Figure 1, the upper part of the image is blurry.

Figure 1 Image with minor blur



Possible Causes

The depth of field (DoF) of the lens is shallow.

Troubleshooting Suggestions

Use the Siemens star chart to adjust lens focus, and ensure that captured objects in the detection area are clear.

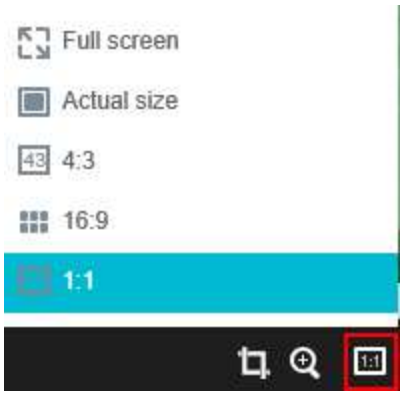
> **NOTE**
>
> Some camera models do not support the focus function.

Adjusting the focus

1. Log in to the camera web system (https://*Camera IP address*).

2. Choose **Configuration** > **Image** > **Display** > **Focus** and set **Focus mode** to **Manual**.
3. Choose **View**. On the **View** tab page that is displayed, click **Aspect Ratio** and choose **1:1**, as shown in Figure 2.

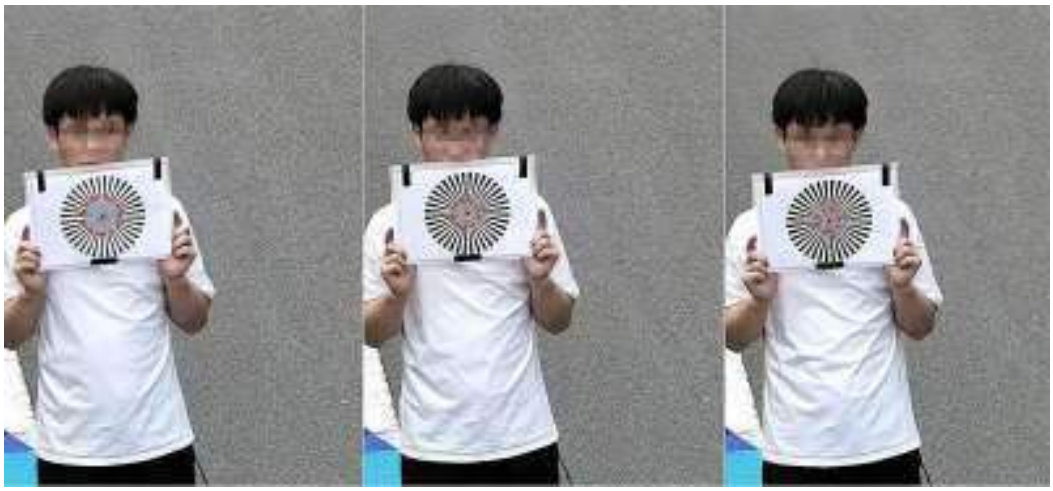
   Figure 2 Aspect Ratio options



4. Set **Speed** to **3**, and click  to adjust the focus.

   During focusing, you can arrange a test person to stand in the image view and focus on the target. It is recommended that the person hold a Siemens star chart in front of the lens when you adjust the lens focus. As shown in Figure 3, sharper lines in the Siemens star chart indicate better focus and clearer image quality.

   Figure 3 Focus process



In most cases, a camera takes snapshots of objects in the center (as shown in Figure 4) and lower parts (as shown in Figure 5) of the image. Therefore, you need to ensure that the camera clearly focuses on these parts. The focus position is determined based on the customer's requirements. If the whole body of the test person needs to be captured in the full image, the focus position needs to be moved upwards in the image. That is, the distant scene of the image needs to be as clear as possible for better snapshot effect.

Figure 4 Middle part of the image



Figure 5 Lower part of the image



5. After the image is in clear focus, click **Aspect Ratio** and choose **Actual size**.

Drawing a detection area

1. Choose **Configuration** > **Intelligence** and enable an intelligent analysis task. The configuration page is displayed.
2. Delete the existing detection area and click **Rectangular Area**. Then draw a capture frame around the position where the focus is clear. It is recommended that the height of the selected area be less than or equal to half of the image height to avoid blurry areas from being captured.

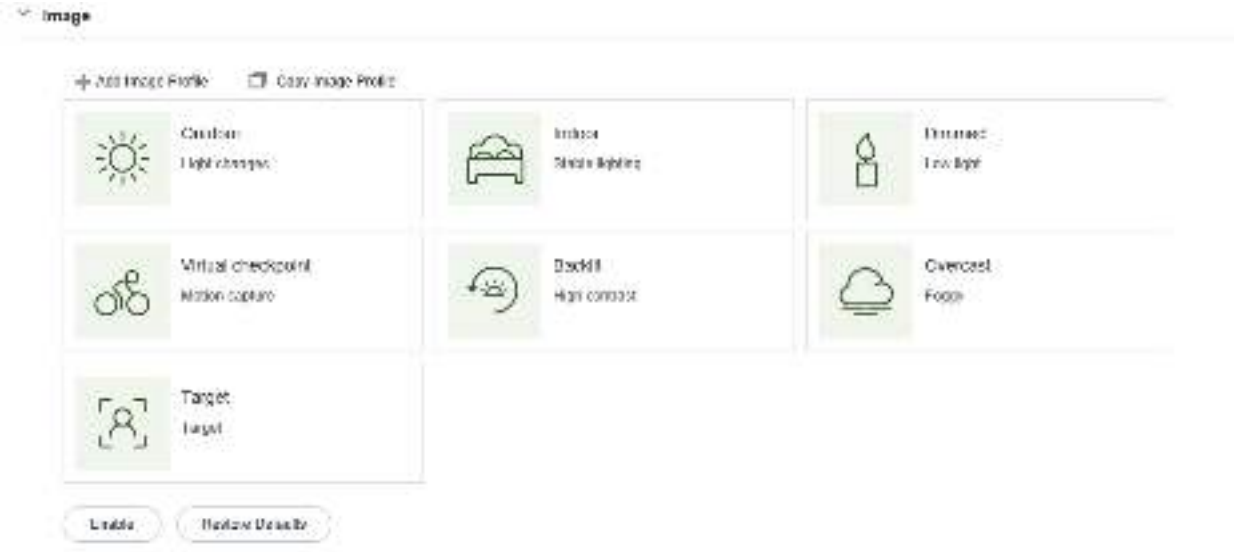
Parent topic: Common Issues and Troubleshooting Methods

Common Scenarios

The focus of image optimization varies based on the requirements of individual deployment.

Before setting any parameters, configure an image profile based on the site requirements in the following way: Log in to the camera web system, choose **Configuration** > **Image** > **Profiles**, select an appropriate profile, as shown in Figure 1.

Figure 1 Enabling an image profile



Low Light Scenarios

Backlight Scenarios

Indoor Scenarios

Outdoor

Parent topic: Configuring Image Optimization

Low Light Scenarios

In low light scenarios, the imaging effect of a camera depends on its low illumination performance. **Low illumination performance refers to the capability of identifying an object without using an external light source in a dimly lit environment.** It is an important camera specification.

Factors Affecting Low Illumination Performance

1. Sensor

   Generally, a larger sensor or a larger photosensitive area indicates better low illumination performance. The sensor size determines the low illumination performance of a camera.

2. Lens and aperture

   The lens and aperture size determine the amount of light entering the camera. In dimly lit areas, the more light enters the camera, the better the imaging performance is. Therefore, a larger aperture (with a smaller F-number) and a larger image circle (projected by the lens) will produce better images in low light scenes.

3. Noise reduction technology

   2D or 3D noise reduction can reduce the impact of noise caused by gain on image quality.

4. Shutter

   By slowing down the shutter speed, you can increase the exposure, enhancing the imaging effect in dimly lit scenes. However, a slow shutter speed may cause slight frame freezing for moving objects.

5. Gain

   Increasing the gain can help increase the image brightness and improve the low illumination performance. However, as the gain increases, more noise will be introduced. Set the gain to the

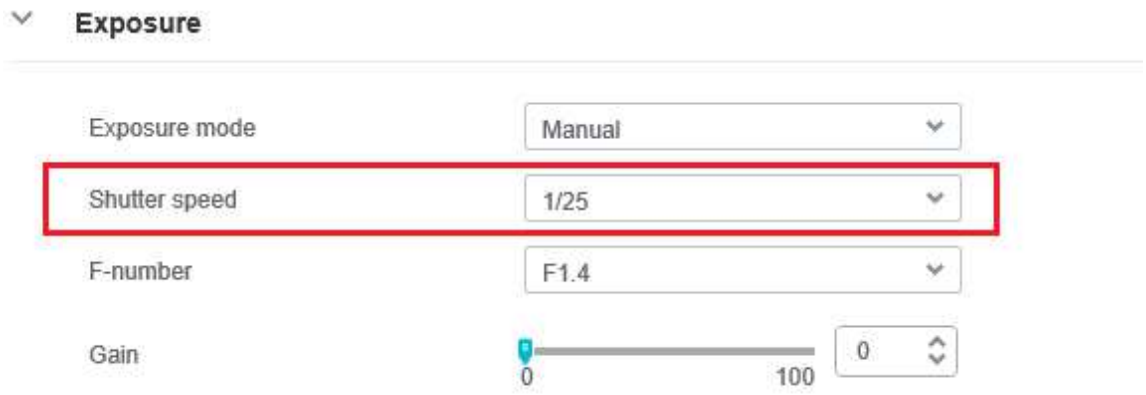
point where the trade-off between brightness and noise is optimal.

If the hardware specifications such as the sensor and lens cannot be changed, some software function settings can be used to further improve the low illumination performance of the camera.

Recommended Settings

1. Slow down the shutter speed. Log in to the camera web system, choose **Configuration** > **Image** > **Display** > **Exposure**, and increase the value of **Shutter speed** to slow down the shutter speed to increase the exposure time, as shown in Figure 1. The more light enters the camera, the sharper the resultant image is.

   Figure 1 Setting the shutter speed

   Note that if the frame rate is lower than 15 fps due to a slow shutter speed, people can perceive the discontinuity of moving objects. Therefore, slowing down the shutter speed is suitable for shooting static objects, not for scenes with many moving objects. You can use this method if you do not mind slight frame freezing.

   Figure 2 shows the effects of different shutter speeds. A slow shutter speed (corresponding to long exposure time) can improve the overall image brightness in dimly lit scenes.

Figure 2 Images shot under different shutter speeds



2. Adjust the gain and noise reduction parameters. In the camera web system, choose **Configuration** > **Image** > **Display** > **Exposure**. If **Exposure mode** is set to **Manual**, adjust the value of **Gain**. For **Auto** or other exposure modes, adjust the value of **Gain limit**, as shown in Figure 3. At the same time, observe the noise levels on the image and set noise reduction accordingly.

Figure 3 Adjusting gain



3. Adjust the saturation and sharpness. In the camera web system, choose **Configuration** > **Image** > **Display** > **Image Adjustment**. In the area shown in Figure 4, slightly decrease the values of **Saturation** and **Sharpness** based on the site requirements to decrease noise.

Figure 4 Adjusting saturation and sharpness



Finally, it should be noted that the low illumination performance of a camera is primarily determined by its sensor and lens. The imaging effect in dimly lit scenes cannot be significantly improved by adjusting software settings alone. To ensure image quality in low light scenes, you are advised to use a camera with a large sensor and aperture.

Parent topic: Common Scenarios

Backlight Scenarios

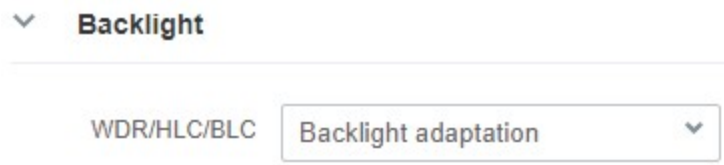
To improve image quality in backlit scenarios, you can enable the backlight adaptation function.

The algorithm uses a proper policy, for example, triggering different levels of WDR, based on the light conditions in the video image (whether any strong light source exists in the background and the light intensity), fine-tuning the brightness and optimizing quality of the video image.

Enabling Backlight Adaptation

1. Log in to the camera web system, choose **Configuration** > **Image** > **Display** > **Backlight**, and set **WDR/HLC/BLC** to **Backlight adaptation**, as shown in Figure 1.

Figure 1 Enabling backlight adaptation



Recommended Settings

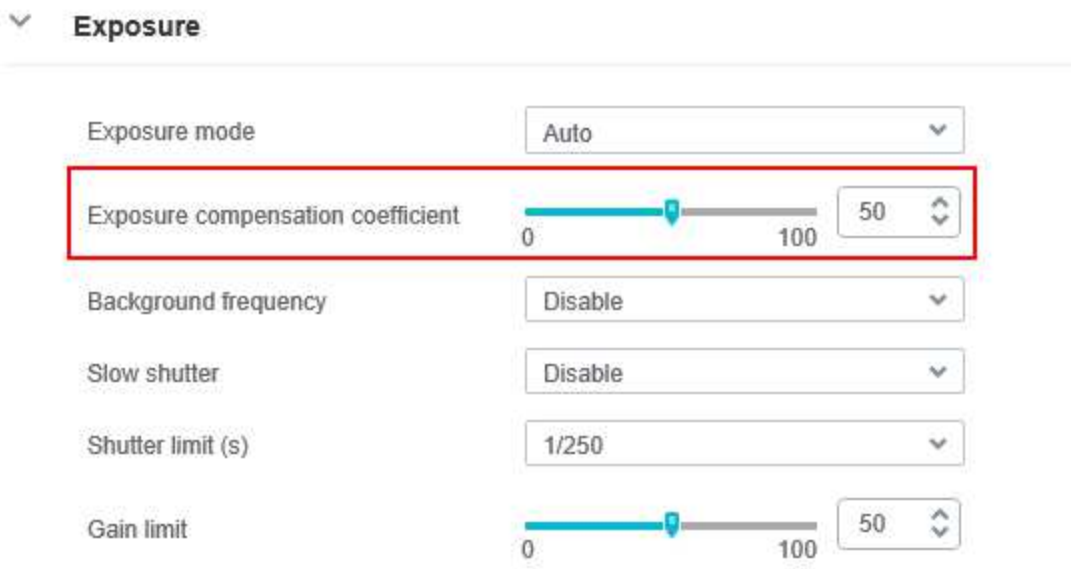
1. Log in to the camera web system, choose **Configuration** > **Image** > **Display** > **Backlight**. In the area that is displayed, set **WDR/HLC/BLC** to **Wide dynamic range**, and set **WDR coefficient** to a larger value, as shown in Figure 2.

   Figure 2 Enabling WDR



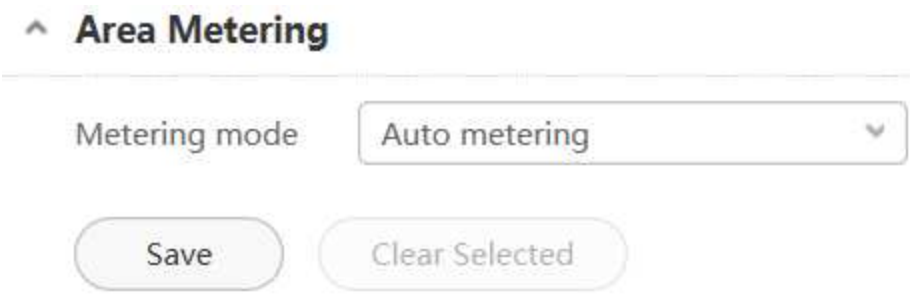
2. Choose **Configuration** > **Image** > **Display** > **Exposure** and set **Exposure compensation coefficient** to a larger value, as shown in Figure 3. Note that a higher coefficient will cause more noises in night-time images.

   Figure 3 Adjusting exposure compensation coefficient



3. If the brightness is still insufficient, you can adjust the **Brightness** and **Contrast** under **Configuration** > **Image** > **Display** > **Image Adjustment**. For camera models that support metering area selection, choose **Advanced Settings** > **Video/Audio/Image** > **Metering/Focus** > **Area Metering**. In the area shown in Figure 4, set **Metering mode** to **Auto metering**, and select dark areas in the image for metering. These settings will also improve the brightness of the image.

   Figure 4 Enabling area metering



Parent topic: Common Scenarios

Indoor Scenarios

In indoor scenarios, if the foreground object appears dark in the images due to strong outdoor or indoor light sources, see Recommended Settings for optimization.

- **Corridor**
- **Exhibition Hall**

Parent topic: Common Scenarios

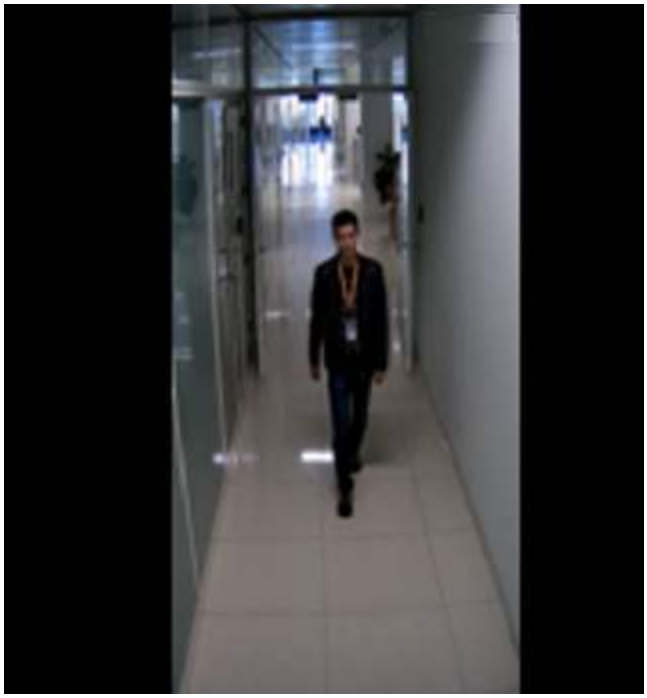
Corridor

If the camera is installed in a long corridor, you can enable the **Corridor mode** under **Configuration** > **Video/Audio** > **Video**, as shown in Figure 1. The corridor mode produces a vertically-oriented image that is perfect for observing narrow corridors, as shown in Figure 2.

Figure 1 Enabling corridor mode



Figure 2 Corridor mode effect



Parent topic: Indoor Scenarios

Exhibition Hall

For indoor scenes such as an exhibition hall, the camera must be installed in an appropriate position and at an appropriate angle to produce the optimal observation effect.

In Figure 1, some objects are blocked. In Figure 2, the camera shooting angle is inappropriate.



Figure 1 Blocked areas

Figure 2 Inappropriate angle



The focus of image optimization in exhibition hall scenes is to adjust the camera installation position and angle so that the intended detection area can be fully covered in the camera view.

After the installation position and angle are settled, modify the settings to achieve the optimal image effect.

Recommended Settings

Log in to the camera web system and choose **Configuration** > **Image** > **Display**.

1. Adjust the white balance to improve the overall color effect.

   Select the white balance mode based on the site requirements. If the image effect is still unsatisfactory, you can select the **Manual** mode and set **Red gain** and **Blue gain** to adjust the image affect.

   For details about how to adjust white balance, see White Balance Adjustment.

2. Adjust the saturation to improve the color sharpness of objects.

   Adjust the saturation based on the image effect.

   For details about how to adjust the saturation, see Saturation Adjustment.

3. Adjust the exposure compensation coefficient to improve the image brightness.

   Adjust the exposure compensation coefficient to ensure that the image brightness is moderate.

   For details about how to adjust the exposure compensation coefficient, see Exposure Compensation Coefficient Adjustment.

4. Adjust the contrast and brightness to improve the image clarity.

   Adjust the contrast and brightness based on the actual image effect.

   For details about how to adjust the contrast and brightness, see Contrast and Brightness Adjustment.

You can fine-tune the preceding parameters one by one to achieve the optimal effect.

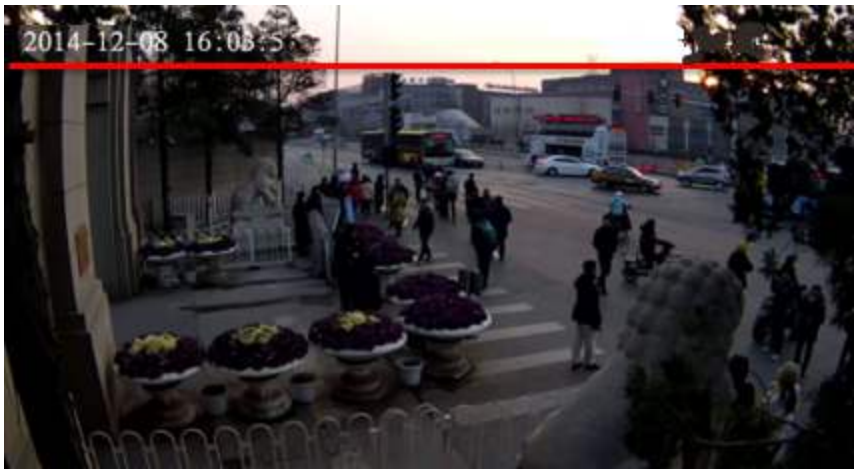
Parent topic: Indoor Scenarios

Outdoor

For outdoor scenes, pay attention to the shooting angle. Avoid letting objects that do not need to be detected (such as the sky, walls, and tree branches) dominate the view and try not to tilt the camera upward.

In Figure 1, the sky occupies a comparatively high proportion in the view. As a result, the lower part in the view appears dark. You need to tilt the camera slightly downward so that the upper edge of the view is in the position marked by the red line.

Figure 1 Suboptimal camera angle



For outdoor scenes, also ensure the high-quality reproduction of colors. For details about how to adjust the color and white balance, see Color Cast Adjustment.

In addition, weather conditions also affect outdoor imaging quality. Weather such as heavy fog makes it impossible for cameras to produce clear images.

There is no effective means to optimize the image effect in foggy or smoggy conditions unless the camera provides the defogging function.

You can enable this function under **Configuration** > **Image** > **Display** > **Image Enhancement**, as shown in Figure 2. If the manual mode is selected, you can manually set the **Defogging**

level. A higher defogging level indicates clearer images. However, as you raise the defogging level, the image may start to take on an artificial appearance. In this case, you need to set **Defogging level** based on the site requirements.

Figure 2 Defogging mode



After the defogging function is enabled, the visibility of objects is improved.

NOTE

The defogging function will occupy camera resources. If it is enabled at the same time as functions such as the corridor mode or electronic image stabilization, performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering.

Parent topic: Common Scenarios

Maintenance

- Routine Maintenance
- Security Maintenance
- Emergency Maintenance

Routine Maintenance

To ensure the long-term operating stability of a camera, you are advised to regularly perform routine maintenance on the camera.

Routine maintenance focuses on the hardware/structure, cleaning/waterproofing/anti-corrosion, software, and environment.

Maintenance Preparations

- Before the maintenance, maintenance engineers need to be familiar with the site conditions and surrounding environment, device components, component connection mode, drawings, and installation procedure.
- Table 1 lists the tools to be prepared.

Table 1 Tools to be prepared

Tool Name	Specification and Function	Appearance
Video detection tester	Used to check the shooting angle and video image.	
Multimeter	Used to check whether the camera's input power meets the requirements.	
Network cable tester	Used to test whether the network cable is made and connected correctly.	
Hammer drill	Drill bit size: 5 mm. Used to drill holes in scenarios such as wall-mounted and pendant-mount installation scenarios.	
RJ45 crimping tool	Used to make an RJ45 connector.	
Wire stripper	Used to remove the insulation layer and jacket from the power cable, alarm cable, and other cables.	

Tool Name	Specification and Function	Appearance
Hex key	Specification: H3 Used to fasten and loosen hex socket screws of the M4 model.	
Phillips screwdriver	Specification: 0#, 1#, and 2# Used to loosen and fasten Phillips screws.	
Flat-head screwdrivers	Screwdriver bit width: 2.5 mm; screw bit length: greater than 75 mm. Used to loosen and fasten flat-head screws.	
Claw hammer	Used to drive expansion screws into the wall.	
Measuring tape	Used to measure the distance, for example, measuring the cable length and installation height.	
Socket wrench	Specification: M6	
ESD gloves	Prevents ESD.	
Marker	Used to make marks, for example, marking the installation position and hole positions.	
Scissors	Used to cut waterproof tapes, insulating tapes, and others.	
Utility knife	Used to disassemble the packing box of the camera.	
Wrench	Used to turn screws.	
Diagonal plier	Used to cut off excess hose clamps.	

Tool Name	Specification and Function	Appearance
Dust-free cloth	Used to wipe the camera lens or viewing window.	

Hardware/Structure Check

You are advised to check the hardware and structure of the camera based on the following checklist.

Table 2 Routine maintenance items

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check whether the camera is securely installed and fixed, for example, whether the screws and brackets are tight; whether the camera support is stable; whether the waterproofing PG connector is tight; whether the rubber plug is normal; and whether the pigtails are properly connected.	Once every year	The camera is securely installed. Cables are properly connected and not deteriorated.	Tighten the screws or replace some accessories based on the site requirements.	Minor	The camera fastener may get loose due to vibration or other reasons. This may cause image shaking. Therefore, you need to periodically check the camera to ensure that the camera is securely installed.
Check whether the power supply is stable and whether the power cable connection is normal.	Rectification triggered by issues	The power supply voltage is stable, and the line is secure.	Replace the power supply line or power adapter based on the site requirements.	Major	It is difficult to maintain the power supply line and power supply. If a fault occurs, you should replace the line or power adapter.

NOTE

During the securing and adjustment, do not change the camera angle or focal length to prevent changing the camera's field of view.

Cleaning, Waterproofing, and Anti-corrosion Check

You are advised to regularly check the cleaning, waterproofing, and anti-corrosion states of the camera based on the following checklist.

Table 3 Routine maintenance items

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check the camera's insulation and waterproofing, including the camera body and pigtails.	Once every year	There is no water ingress, leakage, or accumulation. The insulation and waterproof measures are properly taken.	First ensure that the camera works properly. Then clear the device of water or mist, and insulate and waterproof the camera again.	Minor	Check the appearance and installation environment of the camera. Check whether the actual application scenarios exceed the camera specifications. Periodically check the camera to improve the camera operating reliability.
Check whether the viewing window, lens, and housing are clean.	Once every quarter/Check the video image if necessary	There is no dirt or dust.	Properly clean the camera. Use the lint-free cloth and neutral detergent to softly clean the camera lens and viewing window. **CAUTION:** Do not clean the device with strong and abrasive alkaline cleaner or volatile solvent such as alcohol, benzene, or thinner. These liquids may damage the surface coating or deteriorate the device performance.	Minor	
Check the corrosion status of the camera body and pigtails.	Once every year	No corrosion occurs.	If the camera body or pigtails are corroded, contact the supplier or engineers.	Minor	
Check whether insect prevention and deinsectization measures are taken.	Check the video image if necessary	There are no spiderwebs, bird's nests, or beehives.	Keep insects and birds off the camera.	Minor	

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check whether the wiper can clean the viewing window.	Once every quarter	The wiper works properly to clean the viewing window.	If the wiper works improperly, check the camera cable connection. If the cable connection is normal, replace the wiper. For details about how to replace the wiper rubber strip, see Replacing the Rain Wiper Rubber Strip.	Minor	You are advised to perform the check on rainy days or after the rain.

Checking the Environment

Check the environment where the camera is installed based on the following checklist.

Table 4 Routine maintenance items

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check whether the camera lens is blocked by leaves, walls, or other objects, and whether there are reflective objects around the camera.	Once every six months	There are no blockings in the camera's field of view. The IR effect is normal at night. There is no reflective object.	If there are leaves affecting the field of view, cut off the leaves. If there are walls or other reflective objects, adjust the camera angle so that these objects do not appear in the field of view.	Minor	This type of installation environment affects the detection effect at a specific time or in a specific scenario. You are advised to record or mark the on-site environmental conditions and arrange on-site handling periodically.
Check whether there is a strong light source around the camera.	Once every six months	The image brightness is normal, and there is no strong light source around the camera.	Move away the strong light source or adjust the camera angle to avoid direct radiation of the light source to the camera lens.	Minor	

Software Check

Check the software running status of the camera based on the following checklist.

Table 5 Routine maintenance items

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check the video delivered by the camera for anomalies such as artifacts and stripe noise.	Once every quarter	The video of the camera is displayed properly without anomalies such as artifacts and stripe noise.	Refer to Troubleshooting to troubleshoot the fault.	Major	If video anomalies affect the camera use, you need to perform troubleshooting.
Check the camera alarm information.	Once every quarter	The camera is running properly. No alarm that affects camera functions is generated, or all alarms have been cleared.	Refer to Alarm Reference to check the alarm source and handle the alarm according to related procedure.	Minor	Alarm Reference describes the alarm analysis and handling procedure.
Log in to the software platform or server to which the camera belongs. • View camera online and offline alarm logs to check whether cameras frequently go online and offline, whether there are abnormal functions, whether the network connection is normal, and whether video	Once every six months	There are no symptoms such as frequent online and offline and unexpected recording interruption. The inspection result is normal.	Refer to Troubleshooting to troubleshoot the fault.	Minor	Periodically inspect the camera to eliminate potential risks.

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
recording is normal. • Systematically inspect the camera hardware, system, and functions.					

Parent topic: Maintenance

Security Maintenance

Overview

Application Layer Security

Network Layer Security

Management Layer Security
This topic describes cautions and suggestions on routine security maintenance for system administrators to take as reference when formulating and carrying out security management principles.

Security Configuration
To ensure the operation security of the device, you need to configure the system after the device is installed.

Appendixes

Parent topic: Maintenance

Overview

- **Purpose**
- **Security Features**
- **Layered Security Maintenance**
- **System Security Policy**

Parent topic: Security Maintenance

Purpose

Nowadays, application systems are facing increasingly serious security threats. Problems in application systems may cause service interruption, video loss, or system breakdown. Therefore, a comprehensive security mechanism must be established and maintained to identify and eliminate security risks in advance.

As new security threats emerge continuously, technical methods are insufficient to ensure application security. Therefore, users must develop a security management system based on problems found in routine security maintenance and suggestions to resolve these problems.

Parent topic: Overview

Security Features

- Application Security Layer
- System Layer Security
- Network Layer Security
- Management Layer Security
- Media Security

Parent topic: Overview

Application Security Layer

Transparent Access Mode

- All accounts and passwords for logging in to human-machine interfaces are open to customers through a document. The accounts can be enabled, disabled, or deleted, and the passwords can be changed.
- All command lines and parameters are open to customers through the *Command Reference*.
- Functions that allow access to the system or data while bypassing the system security mechanism (such as authentication, permission control, and log recording) are prohibited.

Service Security

- The built-in web server is used for device maintenance and management. Users can log in to the device in secure HTTPS communication mode to ensure that the user name, password, and sensitive parameters are not stolen.
- The system authenticates the permissions of a user before the user performs any operations to prevent unauthorized access.
- The system performs parameter validity check on all requests from other systems to prevent malformed packet attacks.

Sensitive Data Protection

- The log, diagnostics, debug, and alarm information must not contain sensitive data.
- Sensitive data is transmitted only through secure channels or after being encrypted.
- Sensitive data is encrypted before being stored.

- User login passwords are stored in the storage device after being encrypted using the irreversible encryption algorithm PBKDF2.
- Only standard encryption algorithms and key negotiation mechanisms are used. Proprietary algorithms are not allowed.

Security Logs and Audit

- User login and logout logs are recorded.
- Logs are recorded when users are added or deleted and when user attributes (such as accounts and passwords) are changed.
- Logs are recorded for account locking, unlocking, disabling, and enabling.
- Logs are recorded for changes of the system security configuration (for example, security log content configuration).
- Logs are recorded for changes of important resources, such as deletion and modification of an important file.
- Logs are recorded for modification of system configuration parameters.
- Logs are recorded for system startup, shutdown, and restart.
- Logs are recorded for software upgrade operations such as remote upgrade and local upgrade.
- Logs are recorded for non-query operation commands of all accounts.
- Only authorized users can access logs, and only administrators can delete logs.
- Security logs can be used for auditing.

Security Communication Protocol

- The secure HTTPS protocol can be used to remotely log in to the built-in web server for maintenance and management. That

is, an SSL/TLS layer is added under HTTP. TLS1.1 and TLS1.2 are supported.

- The secure SSHv2 protocol can be used to remotely log in to the device for maintenance and management. SSH can replace Telnet.
- Users can upload and download the network address book through the secure SFTP protocol.
- There is no insecure protocol (Telnet is not supported). FTP is used only to upload snapshots to the server. Users can select FTP or SFTP based on the network security evaluation.
- Malformed packet attacks are prevented.

Parent topic: Security Features

System Layer Security

- Users can enable the HTTPS protocol to communicate with the web server to ensure data transmission security.
- Passwords for logging in to the web server are encrypted by using the irreversible encryption algorithm PBKDF2 to prevent password leakage and crack.
- Users must enter the correct verification code before they access web pages.

Parent topic: Security Features

Network Layer Security

In video security solutions, firewalls are used to isolate security zones.

Parent topic: Security Features

Management Layer Security

Organization and Process

- Establishes and strictly observes security management regulations.
- Trains related personnel to increase their security awareness.
- Trains operation personnel to master and observe security rules.
- Regularly checks security logs to detect potential security risks in a timely manner.

Account and Rights Management

Each authorized operator is assigned necessary rights to prevent multiple users from using the same account.

Parent topic: Security Features

Media Security

- Digital watermark: The encoding side extracts feature data and carries the data in media packets. After receiving the media packets, the decoding side extracts feature data and compares the extracted data with the feature data carried in the media packets. If they are different, the system generates an alarm.
- The system supports 256-bit AES encryption.

Parent topic: Security Features

Layered Security Maintenance

Maintenance personnel need to conduct layered security maintenance for different security maintenance objects to achieve different security maintenance purposes.

Application Layer

Security maintenance at this layer ensures that cameras run and provide services for external systems properly.

Network Layer

Security maintenance at this layer ensures that network devices including switches, routers, and firewalls run properly and that network security policies for the network layer can be executed.

Management Layer

Security maintenance at this layer enhances manual management and maintenance to prevent potential risks. All preceding layers are maintained at the management layer.

Parent topic: Overview

System Security Policy

Password Management

For details about password management, see Password Maintenance Suggestions.

Authentication and Session Control

- Physical ports (for example, network ports) that can manage the system have the access authentication mechanism. Users must enter the correct user name and password to log in to the system.
- All communication ports and protocols (for example, the SSH protocol) that can manage the system have the access authentication mechanism. Users must enter the correct user name and password to log in to the system.
- The system locks a user account when the number of consecutive login attempts reaches the maximum. A locked user account cannot log in to the system.
- After a user account is locked, the system automatically unlocks the account after a specified period. The period is configurable. For details about how to configure the period, see Configuring Account Locking and Unlocking.

Encryption Algorithm

- Use only standard encryption algorithms and key negotiation mechanisms. Proprietary algorithms are not allowed.
- Use encryption algorithms (for example, SHA256 and AES256) of high security levels to reduce the risk of cracking sensitive information.
- Store passwords that are encrypted using the irreversible encryption algorithm, HASH, to prevent password disclosure

and cracking when passwords do not need to be restored to plaintext.

Security Agreement

Use security protocols such as SSHv2, TLS1.1, and TLS1.2 with high security levels for device maintenance and management.

Minimum Authorization Principle

Newly created users have the minimum permission by default.

File Permission Management

Only authorized users can access system files.

Security Logs

- All user activities and operation commands at the application layer are recorded in logs for post-event audit.
- Only authorized users can access logs, and only administrators can delete logs.

Software Package Integrity Verification

The product upgrade package has been digitally signed for integrity verification. For details about how to verify the digital signature, see the *Upgrade Guide*.

Parent topic: Overview

Application Layer Security

Accounts at the Application Layer

User Management

By level of rights, users are classified into three types: system administrator (**admin**), advanced operator, and common operator. Users can be added, modified, and deleted.

Access Control

Log Check and Audit

Clearing Service Data

Parent topic: Security Maintenance

Accounts at the Application Layer

Parent topic: Application Layer Security

User Management

By level of rights, users are classified into three types: system administrator (**admin**), advanced operator, and common operator. Users can be added, modified, and deleted.

User List Administrators can add and delete users, change user passwords, change the maximum number of allowed login sessions, and configure the maximum number of allowed consecutive incorrect password attempts before the account is locked.

User Connections
You can check the connection status of a user or disconnect a user in this area.

Password Validity Period
You can view or configure the validity period of a user password in this area.

Parent topic: Application Layer Security

User List

Administrators can add and delete users, change user passwords, change the maximum number of allowed login sessions, and configure the maximum number of allowed consecutive incorrect password attempts before the account is locked.

Adding a User

The **admin** user creates all initial users uniformly. When creating users, the **admin** user can set user roles and assign permissions to the roles.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 1.

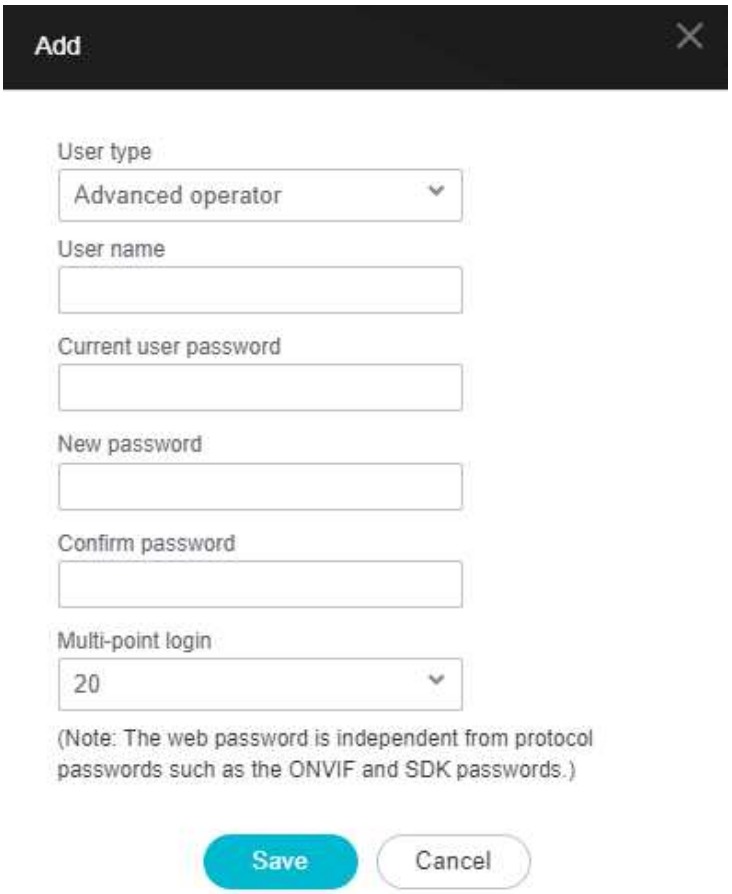
   Figure 1 User List area

3. Click **Add**.

   In the **Add** dialog box that is displayed, configure information about the new user, as shown in Figure 2.

Figure 2 Add dialog box



NOTICE

- A maximum of 10 users (including the **admin** user) can be added.
- The **admin** and **ApiAdmin** users are administrators and cannot be added again.

4. Set user parameters. Table 1 describes the parameters.

Table 1 Parameters for adding a user

Parameter	Description
User type	Different types of users have different operation rights. You can choose the user type as required. • Administrators have all operation rights. They can add advanced operators and common operators.

Parameter	Description
	• Advanced operators cannot add or manage users but can perform operations such as live video viewing and intelligent service configuration. • Common operators only have common operation rights, including viewing live video, setting PTZ parameters, and changing their own passwords.
User name	Enter a name for the new user.
Current user password	Enter the password of the user who currently logs in.
New password	Enter a new password.
Confirm password	Enter the new password again.
Multi-point login	Enter the maximum number of concurrent logins of the new user at the same time.

5. Click **Save**.

NOTE

When you use an account that is created by the **admin** user to log in to the camera for the first time, the **Change Password** dialog box will be displayed. You can log in to the camera after changing the password as prompted.

Changing the User Password

The password of a user can be changed, but the user type and user name cannot be changed.

NOTE

- System administrators can modify information about all users.
- Advanced operators and common operators do not have the permission to modify user information.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 3.

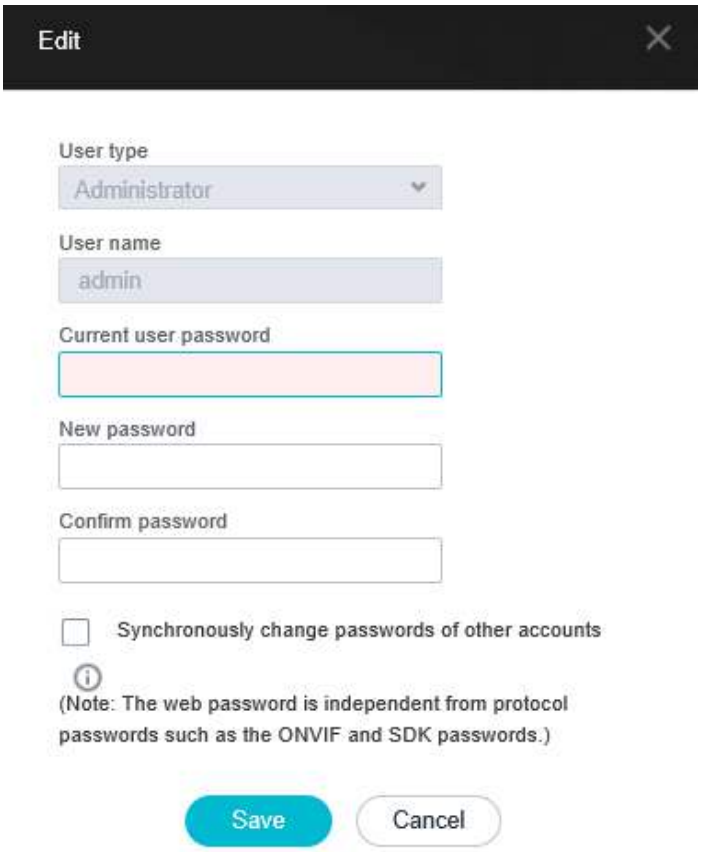
   Figure 3 User List area



3. Select a user.
4. Click .

   The dialog box for changing user password is displayed, as shown in Figure 4.

   Figure 4 Edit dialog box



5. Specify the current user password, new password, and confirm password.
6. Click **Save**.

> **NOTE**
>
> After you change the password of an account as the **admin** user, the **Change Password** dialog box is displayed when you use the account to log in to the camera again. You can log in to the camera after changing the password as prompted.

Changing the Maximum Number of Concurrent Logins

You can change the maximum number of concurrent logins for a user.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 5.

   Figure 5 User List area

3. Select a user.
4. Click **Multi-Login**.

   The dialog box for changing the maximum number of concurrent logins is displayed.
5. Set **Current user password** and **Multi-point login**.
6. Click **Save**.

Deleting a User

Administrators can delete unnecessary users to ensure system access security.

> **NOTE**

- System administrators can delete advanced operators and common operators. System administrators cannot be deleted.
- Advanced operators do not have the permission to delete users.
- Common operators do not have the permission to delete users.
- After a logged-in user is deleted, the user cannot perform operations in the web system and will be forcibly logged out.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

   The **User List** area is displayed, as shown in Figure 6.

   Figure 6 User List area

3. Select a user.
4. Click .

   The **Delete** dialog box is displayed.
5. Enter the current user password and click **OK**.

   The **Delete User** dialog box is displayed.
6. Click **OK**.

Configuring Account Locking and Unlocking

The system administrator can specify the maximum number of incorrect password attempts for an account. If the maximum number of incorrect password attempts is reached, the account is locked.

NOTE

Only the system administrator can configure account locking.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management** > **User List**.

The **User List** area is displayed, as shown in Figure 7.

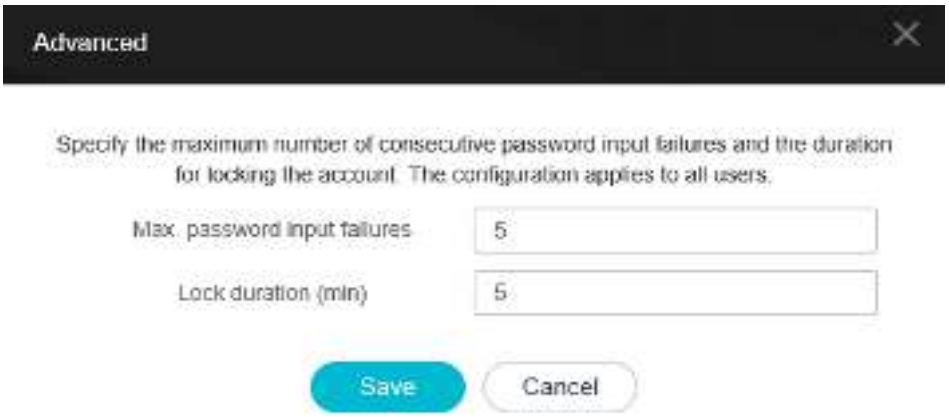
Figure 7 User List area



3. Click **Advanced**.

   The **Advanced** dialog box is displayed, as shown in Figure 8.

   Figure 8 Advanced dialog box



4. Set **Max. password input failures** and **Lock interval (min)**.

   NOTE

   - **Max. password input failures**: maximum number of consecutive incorrect password attempts allowed
   - **Lock interval (min)**: duration in which an account is locked after the number of consecutive incorrect password attempts exceeds the maximum
   - If **Max. password input failures** is set to **0**, the maximum number of consecutive incorrect password attempts allowed is unlimited and the account will not be locked.
   - If **Max. password input failures** is not set to **0** but **Lock interval (min)** is set to **0**, an account will be locked permanently when the number of consecutive incorrect password attempts exceeds the value of **Max. password input failures**.

5. Click **Save**.

Parent topic: User Management

User Connections

You can check the connection status of a user or disconnect a user in this area.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management**.
3. Click **User Connections**. The **User Connections** area is displayed, as shown in Figure 1.

   Figure 1 User Connections area

   NOTICE

   - To disconnect a user, click **Disconnect** in the **Operation** column corresponding to the user.
   - The administrator cannot be forcibly disconnected.

Parent topic: User Management

Password Validity Period

You can view or configure the validity period of a user password in this area.

> **NOTE**
>
> After the password expires, the system will demand you to change the password.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **User Management**.
3. Click **Password Validity Period**. The **Password Validity Period** area is displayed, as shown in Figure 1.

   Figure 1 Password Validity Period area

   > **NOTE**
   >
   > The value of **Period (months)** is an integer ranging from 0 to 12. If this parameter is set to **0**, the password is permanently valid.

Parent topic: User Management

Access Control

The following lists the access control methods:

- Sessions are maintained using cookies.

  For security purposes, the system logs a user out of the web client after 10 minutes of inactivity on web pages other than the live video viewing page. To access the system again, the user needs to re-log in.

- A user can proactively log out of the web client.

  To log out of the web client, click **Logout** in the upper right corner. The user logs out. The login page is then displayed.

- The same user account can be used to log in to multiple web clients at the same time.

Parent topic: Application Layer Security

Log Check and Audit

Logs are the main information source for maintenance engineers to locate faults. They also serve as the basis for terminal users to collect fault information. When a fault occurs, maintenance engineers and terminal users can locate and rectify the fault by checking the log information.

NOTE

For details about the log types and details, see the Log Reference.

Checking Logs Using the Camera Web Client

NOTE

To check logs, log in to the camera web system as the **admin** user and perform the following operations:

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Log**. The page shown in Figure 1 is displayed.

   Figure 1 Querying logs

3. Query logs.

   a. On the left of the log collection page, set the date, start time, end time, and type of the logs to be queried.

> **NOTE**
>
> After **Language** is set, only newly generated logs are displayed in the configured language.

b. Click **Search**.

The search results are displayed in the lower part of the page.

> **NOTE**
>
> To query archived logs, use the **One-Click Collection** function to download more logs.

4. Download logs.

Click **One-Click Collection** and download logs to a local computer. After logs are downloaded, you can view them using WordPad.

> **NOTE**
>
> - The default name of the log file downloaded through **One-Click Collection** is ***sysinfo.tar.gz**. If you want to change the file name, name it in ***.tar.gz** format.
> - For more information about logs, see the Log Reference.

Checking Logs Using the SSH Tool

1. Use the SSH software to log in to the system as the **admin** user.
2. Switch to the **root** user.

su - root

3. View logs.

> **NOTE**
>
> The following uses the debug log as an example.

- Query real-time logs.

cd /opt/log tail -f message.dbg

- Query backup logs.

  cd /usr/log cat message.dbg

Parent topic: Application Layer Security

Clearing Service Data

If you do not need to use a camera any more or a camera needs to be returned to the factory for repair, you must clear service data, including configuration file data and SD card data, to ensure data security.

Clearing Configuration File Data

Only users with the administrator rights can restore the camera to factory settings.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **System** > **System Maintenance** > **Maintenance** > **Restore**. The **Restore** area is displayed, as shown in Figure 1.

   Figure 1 Restore area

3. Click **Fully Restore**.

   The **Fully Restore** dialog box is displayed.

   NOTICE

   - If you click **Fully Restore**, all device parameters (except the focus position of a fixed dome camera or bullet camera in manual or semi-auto focus mode) will be restored to factory settings.
   - When computer graphics configuration is low, Internet Explorer may display a blank screen, stop responding, or display a message indicating network exception during factory setting restoration. If these exceptions occur, open

Internet Explorer, click  , and choose **Internet Options** > **Advanced**. Select **Use software rendering instead of GPU rendering** under **Accelerated graphics**, click **OK**, and then restart Internet Explorer to check whether the page display restores.

4. Enter the current user password in **Current user password**.
5. Click **OK**.

   The system automatically restores factory settings.

Formatting the SD Card

If an SD card is installed on your camera, you need to format the SD card to clear data on the SD card.

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Storage** > **Storage Management** and click **Instant Formatting**.

NOTE

- Do not remove the SD card when it is being formatted or data is being written to it.
- Format the SD card during off-peak hours.

Parent topic: Application Layer Security

Network Layer Security

- **Secure Network**
- **Network Security Maintenance**
- **Remote Access Control**

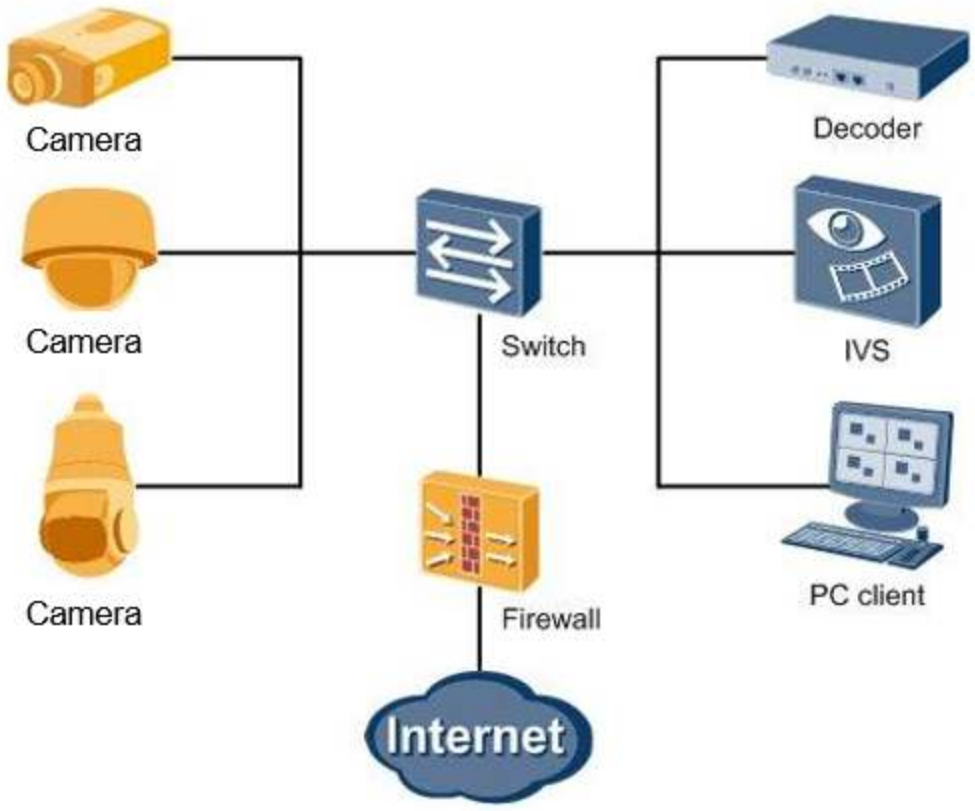
Parent topic: Security Maintenance

Secure Network

The entire video security network is deployed inside the firewall to prevent external network attacks.

Figure 1 shows the position of cameras on the network.

Figure 1 Network diagram



Parent topic: Network Layer Security

Network Security Maintenance

This section describes security maintenance tasks for network devices and reference documents.

Security maintenance tasks for network devices include:

- Enable security management protocols for network devices.
- Enable the recommended security configuration on network devices.
- Use management subnets dedicated to network devices.
- Change the default passwords of network devices and change passwords periodically.
- Install patches on network devices in a timely manner.

For details about security maintenance methods, see the product documentation of each device.

Based on the system network, you can configure an intrusion detection system (IDS) or intrusion prevention system (IPS) to monitor data traffic sent from internal or external networks and defend against abnormal behavior and attacks.

Parent topic: Network Layer Security

Remote Access Control

Maintaining Accounts

IP Filtering

You can use the IP filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

Parent topic: Network Layer Security

Maintaining Accounts

Secure Sockets Layer (SSL) authentication is used in user login. The policy for managing remote access accounts is as follows:

- Users cannot remotely access servers as the administrator.
- These accounts must be used and maintained by dedicated personnel.

Parent topic: Remote Access Control

IP Filtering

You can use the IP filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

Background

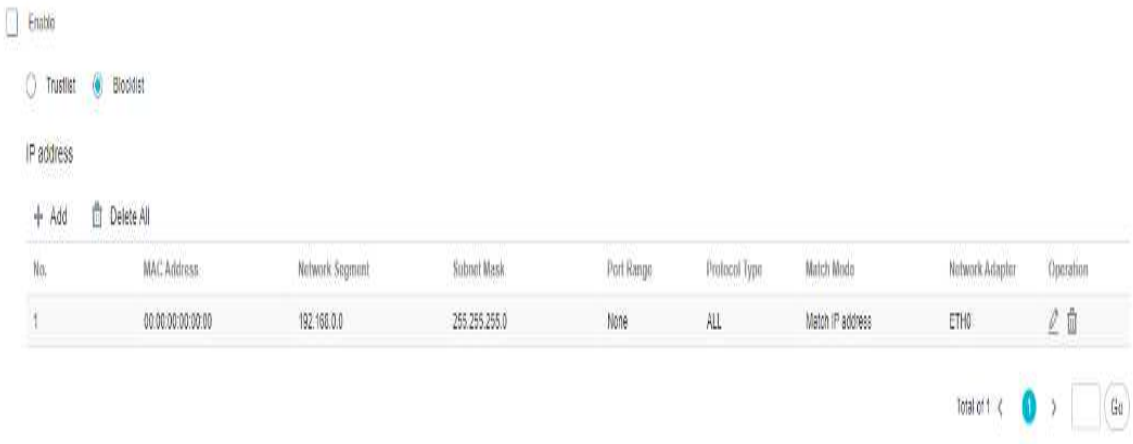
- A network segment is obtained by performing logical AND of the IP address and subnet mask.
- A maximum of 100 IP filtering rules can be added.

Procedure

1. Choose **Configuration** > **System** > **Security Management** > **IP Filtering**.

   The **IP Filtering** tab page is displayed, as shown in Figure 1.

   Figure 1 IP Filtering tab page

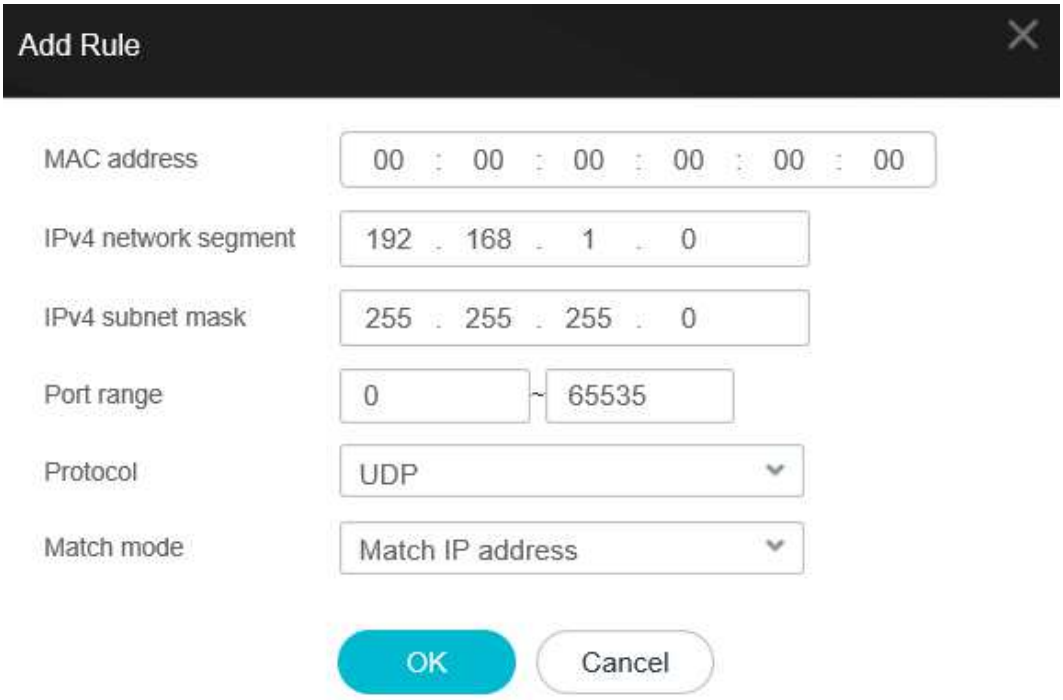


2. Select **Enable** to enable the IP filtering function.
3. Select a desired IP filtering rule.

   The IP filtering rule has two options: **Trustlist** and **Blocklist**, that is, denying or allowing only the access from a specified MAC address, IP network segment or port, or using a specified protocol. Currently, the camera supports only one option at a time.

4. Click **Add**. In the **Add Rule** dialog box that is displayed, set **MAC address**, **IPv4 network segment**, **IPv4 subnet mask**, **Protocol**, and **Match mode**, as shown in Figure 2.

   Figure 2 Add Rule dialog box



> **NOTE**
>
> - If a filtering rule shown in Figure 2 is configured under **Blocklist**, the camera does not process UDP packets sent from the network segment **192.168.1.0** to ports **0–65535**.

5. Click **OK**.

   The **IP Filtering** tab page is displayed.

6. Click **Save**.

> **NOTE**
>
> To modify or delete an IP filter rule, click or in the **Operation** column of the IP filter rule.

Parent topic: Remote Access Control

Management Layer Security

This topic describes cautions and suggestions on routine security maintenance for system administrators to take as reference when formulating and carrying out security management principles.

- **System Maintenance Security Principles**
- **Account Management**
- **Password Maintenance Suggestions**
- **Log Maintenance Suggestions**
- **Data Backup**
- **Port Management Suggestions**
- **Network Connection Change**
- **Security Emergency Response**

Parent topic: Security Maintenance

System Maintenance Security Principles

Minimum Accounts

- Strictly manage accounts based on account policies.
- Add, modify, or delete accounts only when necessary.
- Delete all unnecessary accounts.

Minimum Permissions

- Minimize permissions of accounts.
- Forbid accounts' access to unnecessary resources.

Dedication Principles

- Provide a dedicated computer for accessing the device.
- Isolate partitions where the camera and platform are located.

Audit Principles

- Monitor operations on the camera by using logs and other feasible methods.
- Audit success and failure of the access control policy modification.

Parent topic: Management Layer Security

Account Management

The system administrator must periodically check system accounts and verify that:

- All system accounts are necessary and temporary accounts are deleted.
- Account rights are correct.
- The login and operation logs of accounts are checked and audited.

Parent topic: Management Layer Security

Password Maintenance Suggestions

Only users who are authenticated can log in to the application system. You must configure account and password complexity and password validity periods based on security requirements.

Suggestions on password maintenance:

- You are advised to periodically (every 90 days as recommended) change the password and ensure that the same password is not used repeatedly.
- Assign dedicated personnel to keep the passwords of the **admin** and **root** users of the Linux operating system.
- Passwords are encrypted for transmission and are not transferred by email.
- Encrypt a password before saving it.
- Ask the system maintenance personnel to change passwords after the system is handed over from one person to another.

Parent topic: Management Layer Security

Log Maintenance Suggestions

Audit logs help you detect suspicious operations.

The system records important operations in logs. You can protect log files by access control.

- Assign dedicated personnel to query and delete logs.
- Periodically check system logs and run logs. If any fault is detected, report it to your upper-level department. If you cannot locate or rectify the fault, contact technical support in a timely manner.
- Periodically back up log files to external storage media such as disks, tapes, and CD-ROMs.
- Delete logs that have been backed up to release the disk space.

Parent topic: Management Layer Security

Data Backup

In the following scenarios, system maintenance engineers must back up data to improve security.

- Before daily security maintenance, and before and after system troubleshooting.
- Before patch installation and upgrade. For details about the backup, see the related guides.

Parent topic: Management Layer Security

Port Management Suggestions

Port 8686 is enabled for the camera by default. Cameras send information such as the camera model, software version, SN, and MAC address to the automatic discovery tool through this port.

Parent topic: Management Layer Security

Network Connection Change

If network connections are changed, ensure that the new security policies do not undermine the original ones.

If major changes are made on network connections, system maintenance engineers should analyze the network topology and perform the following operations:

- Update the network diagram.
- Update the firewall configuration.
- Update the switch and router configuration.

Parent topic: Management Layer Security

Security Emergency Response

System maintenance engineers must put in place security emergency response mechanisms to deal with emergencies, quickly recover the system, and minimize loss.

Parent topic: Management Layer Security

Security Configuration

To ensure the operation security of the device, you need to configure the system after the device is installed.

The system has been hardened before delivery. To ensure the operation security of the device, you are advised to use the following methods to perform security configuration based on the default configurations after the device is installed:

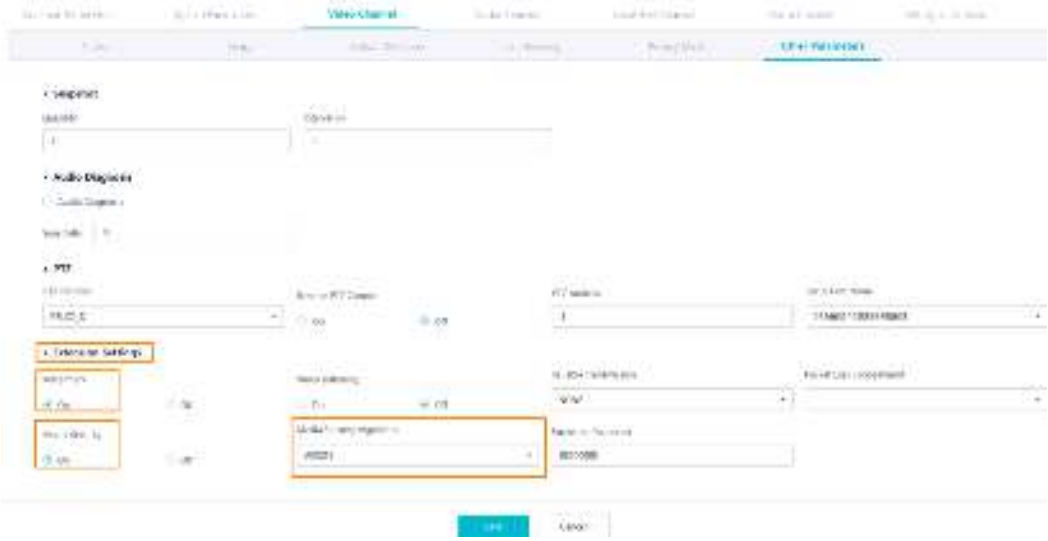
- Change the default password. For details, see Changing the User Password.
- Change the maximum number of users who can log in to the device at the same time. For details, see Changing the User Password.
- You are advised to disable the GB/T 28181 and SNMP protocols if such protocols are not used for connecting cameras to a video security platform.
- When you connect a camera to a video security platform, enable the watermark function on the platform to prevent video tampering and deletion and set the encryption algorithm to AES.

NOTE

The watermark and AES encryption functions are disabled for the camera by default. The functions can be enabled only on the video security platform that supports the functions.

Figure 1 shows the method for enabling the watermark and AES encryption functions on the IVS1800 platform.

Figure 1 Enabling the watermark function



- The product has the following TCP attack risks. You can configure an IP address trustlist to prevent the attacks. For details about how to configure an IP address trustlist through the web system or SDK, see IP Filtering.
  - Slow HTTP attack
  - Connection flood stress
  - Zero window connection stress
  - Small window stress
  - Segment hole stress
  - Req fin pause stress
  - Activate reno pressure stress
  - Fin_wait_2 stress
  - Shrink path MTU stress
  - MD5 stress

Parent topic: Security Maintenance

Appendixes

Reference Documents

List of Security Maintenance Tasks

Parent topic: Security Maintenance

Reference Documents

This section describes the reference document for security maintenance.

Table 1 describes the reference documents.

Table 1 Reference documents

Reference Document	Description
Log Reference	Describes logs of various types and error codes in logs.

Parent topic: Appendixes

List of Security Maintenance Tasks

To ensure optimal security, perform security maintenance tasks regularly.

Table 1 describes security maintenance tasks.

Table 1 Security maintenance tasks

Security Maintenance Task	Task Implementation Frequency
Changing default passwords **NOTE:** For details about passwords to change, see Accounts at the Application Layer.	Implemented during installation and commissioning
Periodically checking user accounts	Implemented monthly
Periodically changing passwords	Implemented quarterly

Parent topic: Appendixes

Emergency Maintenance

- **Overview**
- **Service Fault Scenarios**
- **Appendix**

Parent topic: Maintenance

Overview

Definition of Emergency Faults

Routine Preparations

Parent topic: Emergency Maintenance

Definition of Emergency Faults

If any of the following emergency faults occurs, you need to start the emergency plan:

- Multiple cameras go offline on the platform.
- Multiple cameras encounter a blank screen or stream interruption on the platform.
- The intelligent analysis results of multiple cameras cannot be uploaded to the platform.
- Multiple PTZ dome cameras cannot be rotated.
- The images of multiple cameras are blurred.

Parent topic: Overview

Routine Preparations

This section describes routine preparations for emergency maintenance.

To improve the efficiency of rectifying emergency faults, make the following preparations:

- Understand the relationship between Intelligent Video & Data Analytics components and onsite devices, and physical connections between onsite devices.
- Collect and arrange the information in the table about the device communication, interconnection, and permissions (integration design document of the project), including the virtual local area network (VLAN), IP address, port number, switch configurations, user name and password, software and hardware configurations, software and hardware versions, and change information.
- Periodically verify that the following fault diagnosis tools are available:
  - SSH tool for remote login (such as PuTTY)
  - SFTP tool (such as FileZilla or WinSCP)

Parent topic: Overview

Service Fault Scenarios

- **Multiple Cameras Go Offline on the Platform**
- **Multiple Cameras Encounter a Blank Screen or Stream Interruption on the Platform**

Parent topic: Emergency Maintenance

Multiple Cameras Go Offline on the Platform

Symptom

Multiple cameras go offline on the platform.

Impact Scope and Severity

Multiple cameras go offline on the platform, affecting related services such as video recording, live video viewing, and intelligent analysis.

Possible Causes

- The network between the cameras and the platform is disconnected.
- The camera protocol is not enabled.
- The protocol password used by the platform is different from the camera registration password.
- The platform is faulty.

Solution

Perform troubleshooting in the following way:

1. Check the network connection between the cameras and the platform.

    a. Ping the cameras on the platform to check the network connection status.

    - If the cameras can be successfully pinged, go to 1.b.
    - If the cameras cannot be pinged, troubleshoot the network fault.

      Check whether the fault is rectified after the network fault is rectified. If the fault is rectified, no further

action is required. If the fault persists, go to 1.b.

b. Ping the platform at the camera background to check the reverse network connection status.

Use the SSH tool to log in to the camera operating system as the **admin** user and ping the platform.

- If the platform can be successfully pinged, go to 2.
- If the cameras cannot be pinged, troubleshoot the network fault.

  Check whether the fault is rectified after the network fault is rectified. If the fault is rectified, no further action is required. If the fault persists, go to 2.

2. Verify that the camera protocol is enabled.

The detailed procedure is as follows:

a. Log in to the camera web system (https://*Camera IP address*).

b. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** and check whether the connection protocol is enabled.

- If not, enable the protocol and check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to 3.

- If so, go to 3.

3. Verify that the protocol password of the camera is the same as that used by the platform.

The detailed procedure is as follows:

a. Log in to the camera web system (https://*Camera IP address*).

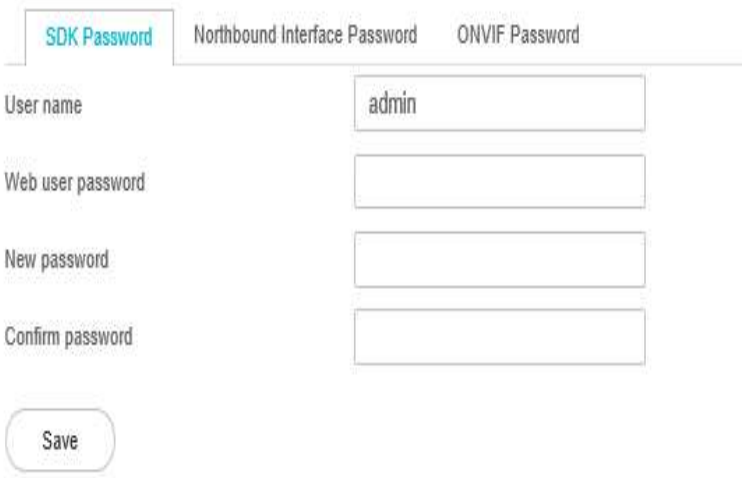
b. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Password Management**. The **Password Management** area is displayed.

c. Change the protocol password of the camera to that used by the platform. Then check whether a message indicating that the new password must be different from the old password is displayed.

- If so, go to 4.
- If not, the protocol password of the camera is successfully changed to that used by the platform. Then check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to 4.

Figure 1 Checking the protocol password



4. Collect fault information and contact technical support.

   For details about how to collect fault information, see Collecting Fault Information.

Parent topic: Service Fault Scenarios

Multiple Cameras Encounter a Blank Screen or Stream Interruption on the Platform

Symptom

Multiple cameras encounter a blank screen or stream interruption during live video viewing on the platform.

Impact Scope and Severity

A blank screen or stream interruption occurs during live video viewing of multiple cameras on the platform. This fault affects live video viewing, image preview during encoding or image parameter settings, and image preview during PTZ controls.

Possible Causes

- The network between the cameras and the platform is disconnected.
- The RTSP service of the cameras is abnormal.
- The possible causes vary depending on the connection protocol.
  - Connection through the ONVIF protocol
    - The ONVIF authentication mode or transmission protocol is incorrect.
    - The ONVIF password for logging in to the platform is incorrect.
  - Connection through the GB/T 28181 protocol
    - The media stream keep-alive function is enabled for the camera, but the platform does not support this function. If the cameras do not receive a media stream request within 60s, the cameras proactively stop sending media streams.
    - The cameras connected to the platform do not support H.265 streams packaged in PS mode, but the stream type is set to H.265.
  - Connection through the SDK protocol

    When streams are requested through the SDK, a network fault occurs and the platform does not receive media streams for more than 30s. As a result, the media stream keep-alive function is disabled due to timeout and no streams are requested again.
- The platform is faulty.

Solution

Perform troubleshooting in the following way:

1. Check the network connection between the cameras and the platform.

    a. Ping the cameras on the platform to check the network connection status.

    - If the cameras can be successfully pinged, go to 1.b.
    - If the platform cannot be pinged, troubleshoot the network fault.

      Check whether the fault is rectified after the network fault is rectified. If the fault is rectified, no further action is required. If the fault persists, go to 1.b.

    b. Ping the platform at the camera background to check the reverse network connection status.

    Use the SSH tool to log in to the camera operating system as the **admin** user and ping the platform.

    - If the platform can be successfully pinged, go to 2.
    - If the platform cannot be pinged, troubleshoot the network fault.

      Check whether the fault is rectified after the network fault is rectified. If the fault is rectified, no further action is required. If the fault persists, go to 2.

2. Check the RTSP port configuration of the camera.

    a. Log in to the camera web system (https://*Camera IP address*).

    b. Choose **Configuration** > **Network** > **Basic Settings** > **Port**.

    c. Check whether the RTSP port (554 by default) is changed.

    - If so, change the RTSP port number to the default port number 554, save the settings, and check whether the fault is rectified.

      If the fault is rectified, no further action is required. If the fault persists, go to 3.
    - If not, go to 3.

3. Check the configurations in different connection protocols.

    Refer to the solution based on the connection protocol.

    Connection through the ONVIF protocol

    a. Check whether the ONVIF authentication mode is the same as that configured on the platform.

    For example, the platform does not support digest authentication, but the authentication mode configured on the camera is digest authentication.

        i. Log in to the camera web system (https://*Camera IP address*).

ii. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters**. The **Second Protocol Parameters** area is displayed.

iii. Check whether the ONVIF authentication mode is the same as that configured on the platform.

- If so, go to 3.b.
- If not, change the ONVIF authentication mode of the camera to that configured on the platform. Then check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to 3.b.

Figure 1 Checking the ONVIF authentication mode



b. Check whether the ONVIF transmission protocol is the same as that configured on the platform.

For example, the platform does not support HTTPS, but the transmission protocol configured on the camera is HTTPS.

i. Log in to the camera web system (https://*Camera IP address*).

ii. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters**. The **Second Protocol Parameters** area is displayed.

iii. Check whether the ONVIF transmission protocol of the camera is the same as that configured on the platform.

- If so, go to 3.c.
- If not, change the ONVIF transmission protocol of the camera to that configured on the platform. Then check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to 3.c.

Figure 2 Checking the ONVIF transmission protocol



c. Verify that the ONVIF password of the camera is the same as that used by the platform.

   The detailed procedure is as follows:

   i. Log in to the camera web system (https://*Camera IP address*).

   ii. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Password Management**. The **Password Management** area is displayed.

   iii. Change the ONVIF password of the camera to that used by the platform. Then check whether a message indicating that the new password must be different from the old password is displayed.

   - If so, go to 4.
   - If not, the ONVIF protocol password of the camera is successfully changed to that used by the platform. Then check whether the fault is rectified.

     If the fault is rectified, no further action is required. If the fault persists, go to 4.

Figure 3 Checking the ONVIF password



Connection through the GB/T 28181 protocol

a. Check whether the media stream keep-alive function of the camera is enabled.

If the platform does not support the media stream keep-alive function, ensure that this function is disabled on the camera side.

i. Log in to the camera web system (https://*Camera IP address*).

ii. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters**. The **Second Protocol Parameters** area is displayed.

iii. Check whether **Enable media stream keep-alive** is selected.

- If not, go to b.
- If so, deselect the check box, save the settings, and check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to b.

Figure 4 Checking whether the media stream keep-alive function is enabled



b. Verify that the camera encoding format is H.264.

i. Log in to the iClient of the upper-level video security platform and double-click **Devices**. The **Devices** tab page is displayed.

ii. Double-click the camera to check in the device list to open the configuration window.

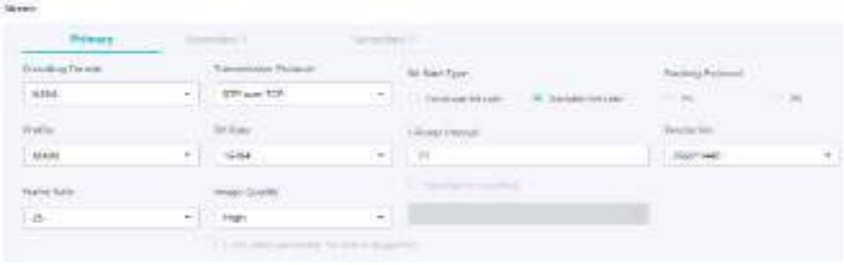
iii. Choose **Video Channel** > **Video** > **Video Encoding**.

iv. Check whether the encoding format is H.264.

- If so, go to 4.
- If not, set the encoding format to H.264, save the settings, and check whether the fault is rectified.

  If the fault is rectified, no further action is required. If the fault persists, go to 4.

Figure 5 Checking the encoding format



NOTE

The GUI of the iClient varies depending on the iClient version.

Connection through the SDK protocol

After the media stream keep-alive function is disabled due to timeout, the platform needs to request streams again. You can restart the platform and check whether the fault is rectified. If the fault is rectified, no further action is required. If the fault persists, go to 4.

4. Collect fault information and contact technical support.

   For details about how to collect fault information, see Collecting Fault Information.

Parent topic: Service Fault Scenarios

Appendix

Collecting Fault Information

Parent topic: Emergency Maintenance

Collecting Fault Information

If the cause of a fault cannot be located, collect fault information and contact technical support. Fault information is an important basis for troubleshooting. Collect as much fault information as possible so that we can quickly and accurately locate faults.

Fault Information Collection Template

Methods

Parent topic: Appendix

Fault Information Collection Template

Provide the information required in the template and send the information to engineers.

> **NOTE**
>
> The fault information collection template can be customized, but must include all the information included in Table 1 to help engineers quickly rectify faults.

Table 1 Fault information collection template

Item	Description	Item	Description
User name	-	Phone number	-
Site name	-	Site address	-
Product model	-	Software version	-
Device SN	-	Fault impact scope	(Common or emergency fault)
Fault occurrence time	-	Fault occurrence frequency	-
Error code/information	-	Other symptoms	-
Operations performed before the fault occurs	(Device replacement/Device configuration modification/Others)	Measures taken after the fault occurs	-
Fault is described in the	(Yes/No)	Troubleshooting methods and effects	-

Item	Description	Item	Description
Troubleshooting Cases.			

Parent topic: Collecting Fault Information

Methods

- **Collecting Logs on the Web Page**
- **Collecting Networking Information**

Parent topic: Collecting Fault Information

Collecting Logs on the Web Page

Logs are major fault information and important references for quickly locating faults.

Context

You can collect information, such as system information, configuration files, and SSH logs, with one click.

Procedure

1. Choose **Configuration** > **System** > **System Maintenance** > **Log**. The page shown in Figure 1 is displayed.

   Figure 1 Querying logs

2. Query logs.

   a. On the left of the log collection page, set the date, start time, end time, and type of the logs to be queried.

   > **NOTE**
   >
   > After **Language** is set, only newly generated logs are displayed in the configured language.

   b. Click **Search**.

   The search results are displayed in the lower part of the page.

> **NOTE**
>
> To query the archived logs, use the **One-Click Collection** function to download more logs.

3. Download logs.

   Click **One-Click Collection** and download logs to the local computer. After logs are downloaded, you can view them using WordPad.

> **NOTE**
>
> - The default name of the log file downloaded through **One-Click Collection** is ***sysinfo.tar.gz**. If you want to change the file name, name it in ***.tar.gz** format.
> - For more information about logs, see the Log Reference.

Parent topic: Methods

Collecting Networking Information

Device networking information helps users understand the onsite network environment and improve fault locating accuracy.

Document the following onsite information:

- Physical networking diagrams: types of connection media and the physical connection relationships between the devices
- Logical interconnection diagrams: logical interconnection relationships between the devices
- Device interconnection information: VLANs, IP addresses, subnets, gateways, and ports

Parent topic: Methods

Reference

- Log Reference
- Command Reference
- Alarm Reference

Log Reference

- Log Overview
- Log Query
- Log Description
- Error Codes
- Error Code Reference

Parent topic: Reference

Log Overview

Log Introduction

Log Levels

Log Classification

To prevent frequent erase and write operations on the flash memory and prolong the service life of the flash memory, logs are classified into the following two categories: 1. Relatively important logs that are not frequently recorded: This category of logs is directly written into the flash memory. 2. Logs that are frequently recorded: This category of logs is first written into the memory and then written into the flash memory based on specified storage rules.

Parent topic: Log Reference

Log Introduction

Logs record key events and information during system running, helping maintenance engineers to locate faults.

Logs provide main information for maintenance engineers to locate faults and serve as the basis for users to collect fault information. When a fault occurs, maintenance engineers and users can locate and rectify the fault by checking the generated logs. Correctly recorded logs can provide sufficient reference for fault locating.

Parent topic: Log Overview

Log Levels

Logs have four levels in descending order: ERROR, WARNING, NOTICE, and INFO.

Table 1 describes the log levels.

Table 1 Log levels

Log Level	Log Name	Description
ERROR	Error logs	This level of logs record errors that occur during system running. Logs of error level are unique to debug logs and error logs, and they are recorded whether the debug log function is enabled or disabled.
WARNING	Alarm logs	This level of logs record alarms that do not affect the normal system running. Logs of warning level are unique to debug logs, and they are not recorded if the debug log function is disabled.
NOTICE	Common logs	This level of logs record important flow information during system running.

Log Level	Log Name	Description
		All types of logs have the notice level, and they are recorded whether the debug log function is enabled or disabled.
INFO	Information logs	This level of logs record prompt information during system running. Logs of information level are unique to debug logs, and they are not recorded if the debug log function is disabled.

Parent topic: Log Overview

Log Classification

To prevent frequent erase and write operations on the flash memory and prolong the service life of the flash memory, logs are classified into the following two categories: 1. Relatively important logs that are not frequently recorded: This category of logs is directly written into the flash memory. 2. Logs that are frequently recorded: This category of logs is first written into the memory and then written into the flash memory based on specified storage rules.

Table 1 describes the specific log types.

Table 1 Log classification

Log	File Name	Log Description	File Path and Storage Description

Log	File Name	Log Description	File Path and Storage Description
Debug log	message.dbg	Records information about the internal process of the device system, such as accessing and exiting the service logic (function) and detailed information about service logic errors. Software developers can use this type of logs to debug codes and print key variable names, variable values, and memory segments. The debug log function is disabled by default. For details about how to enable the debug log function, see the *Command Reference*.	The log is first saved in the **/opt/log** directory of the memory and then backed up to the **/usr/log** directory of the flash memory every 15 minutes. If the size of a file exceeds the specified maximum (512 KB for debug logs and 256 KB for error logs), the file is compressed into a .tgz file and stored in the **/usr/log** directory of the flash memory.

Log	File Name	Log Description	File Path and Storage Description

Log	File Name	Log Description	File Path and Storage Description
Error log	message.err	Records error information and other important information in the system service processing process.	
Operation log	message.opr	Records operations initiated by operators and scheduled tasks.	
Run log	message.run	Records key events during system operations and key information about service processes. The run logs serve as a supplement to operation logs.	
SSH/SFTP log	message.syslog	Records operations on the device performed through the SSH/SFTP client or commands. Some devices that are upgraded from earlier versions have the **ssh.log** file. After the upgrade, the **ssh.log** file is empty and the log content is stored in the **message.syslog** file.	
Alarm log	message.alarm	Records alarms generated by cameras, including	

Log	File Name	Log Description	File Path and Storage Description
		network interruption, temperature, Boolean value input, motion detection, and lens blocking alarms.	
System log	message.mem	Records information about cameras obtained through the **top** command every 10 minutes.	
Frequent log	message.fre	Records logs that need to be printed frequently or periodically.	
Nginx server access logs	nginx_access.log	The Nginx open-source software automatically generates Nginx access logs. The log information is stored in the **message.syslog** file. Therefore, the **nginx_access.log** file is empty.	
Nginx server debug logs	nginx_error.log	Debug logs of the Nginx server are a small part of the logs generated before the Nginx loads the configuration. After the configuration is complete, the logs are stored in the	

Log	File Name	Log Description	File Path and Storage Description
		message.syslog file.	
App installation debug logs	message.appmgr_0.dbg	Debug logs are recorded during app installation.	
App lifecycle debug logs	message.appmgr_1.dbg	Debug logs are recorded throughout the app lifecycle.	
PAM login authentication failure log	tallylog	Records information about PAM login authentication failures.	The log is first saved in the **/opt/log** directory of the memory and then backed up to the **/usr/log/bak** directory of the flash memory at a certain interval (under **/usr/log** for the 3516E chip).
Recent user login log	lastlog	Records information about recent user logins.	
Process startup time log	SoftwareInfo.log	Record the process startup time.	

Log	File Name	Log Description	File Path and Storage Description
Upgrade log	update.log	Records upgrade information about the device version and algorithms.	The log is stored in the **/usr/log** directory of the flash memory.

Log	File Name	Log Description	File Path and Storage Description
Hardware reset log	reset.log	Records device hardware reset information.	
Watchdog log	wdt.log	Records exception information generated during watchdog reset at the software layer.	
Kernel startup log	dmesg.log	Records process loading information of the Linux kernel during device startup.	
Process exception log	ExceptionInfo_*Process name*.log	Records exceptions of each process, including the system stack information when the device software is faulty, unexpected interruption of the intelligent algorithm process, or manual upgrade of the intelligent algorithm. The 3516E chip does not support this function.	
Process restart log	RebootInfo.log	Records restart information about each process, including the restart time, restart type, and PID. The log is backed up in	

Log	File Name	Log Description	File Path and Storage Description
		RebootInfo_old.log.	
Daemon run log	daemon.log	Records Daemon running information.	
Daemon exception log	RebootInfo_daemon.log	Records information about exceptions that occur during Daemon running.	
System initialization log	sysInitInfo.log	Records system initialization information. The 3516E chip does not support this function.	
Container engine run log	lcrd.log	Records container engine running information.	
Log recording the number of times that no sensor data is detected	reboot_cnt	Records the number of times that the camera fails to detect sensor data. If the camera fails to detect sensor data, the camera will restart for restoration. If the camera fails to detect sensor data for more than three consecutive times, the camera will not automatically restart.	
Kbox log	x_kbox.log.tgz	The value of **X** ranges from 0 to 4, indicating the latest five logs.	The log is stored in the **/usr/log/kboxlog/** directory of the flash memory.

Log	File Name	Log Description	File Path and Storage Description
		The file obtained after decompression is **kbox_current.log**. Only the 3516D, 3519, 3519A, and 3559A chips support this function.	
Hardware fault log	message.hard_alarm	Records alarms generated by hardware devices, including network disconnection, temperature, and driver layer storage alarms.	The log is first saved in the **/opt/log** directory of the memory and then backed up to the **/usr/log** directory of the flash memory every 15 minutes. If the size of a file exceeds the specified maximum (512 KB for debug logs and 256 KB for error logs), the file is compressed into a .tgz file and stored in the **/usr/log** directory of the flash memory.

Parent topic: Log Overview

Log Query

Logs are the main information source for maintenance engineers to locate faults. They also serve as the basis for terminal users to collect fault information. When a fault occurs, maintenance engineers and terminal users can locate and rectify the fault by checking the log information.

NOTE

You need to check the log capacity periodically. It is recommended that logs be backed up once a month.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Maintenance** > **Log** > **Log Collection**. The page shown in Figure 1 is displayed.

   Figure 1 Querying logs

3. Query logs.

   a. Expand the **Log Debugging** area. Select a required module and click **OK**.

   b. Expand the **Log Collection** area. Set the start time, end time, and log type for log query.

   NOTE

   - After **Language** is set, only newly generated logs are displayed in the configured language.

- If you click **Reset**, the start time changes to 24 hours ago and the end time changes to the current time.

c. Click **Search**. The search results are displayed in the lower part of the page.

NOTE

To query the archived logs, use the **One-Click Collection** function to download more logs.

4. Download logs.

   Click **One-Click Collection** and download logs to a local PC. After logs are downloaded, you can view them using WordPad.

NOTE

- The default name of the log file downloaded through **One-Click Collection** is ***sysinfo.tar.gz**. If you want to change the file name, name it in ***.tar.gz** format. This function collects all logs saved by the camera, and is irrelevant to the log type, start time, and end time configured on the right.
- For more information about logs, see Log Reference.
- If the download fails, go to the **Internet Options** page of Internet Explorer, click **Advanced**, and click **Reset**. Then, download the log file again.

Parent topic: Log Reference

Log Description

Debug Logs

Operation Logs

Run Logs

System Logs

Abnormal Stack Logs

Upgrade Logs

Alarm Logs

Error Logs

Hardware Reset Logs

SSH/SFTP Logs

Watchdog Logs

Kernel Startup Logs

Process Exception Log

Process Restart Log

Daemon Run Logs

Daemon Exception Logs

System Initialization Log

Container Engine Run Logs

No Sensor Data Count Logs

Kbox Logs

Frequently Recorded Logs

Nginx Server Access Logs

Nginx Server Debug Logs

- **App Installation Debug Logs**
- **App Lifecycle Debug Logs**
- **Recent User Login Logs**
- **Process Startup Time Logs**
- **Hardware Fault Logs**
- **ITGT Intelligent Exception Logs**
- **Wi-Fi Probe Debug Log**
- **Wi-Fi Probe Run Log**
- **Wi-Fi Probe Operation Log**
- **Wi-Fi Probe Alarm Log**

Parent topic: Log Reference

Debug Logs

Log Content

Debug logs (message.dbg) are classified into the following two types:

- Debug logs recorded no matter the debug log is enabled or disabled: NOTICE and ERROR logs, recording running information and errors of modules.
- Debug logs recorded only when the debug log function is enabled: INFO and WARNING logs, recording detailed running information about modules. The debug log function is disabled by default. For details about how to enable the debug log function, see the *Command Reference*.

Developers can use debug logs to check whether errors occur on programs. Test or maintenance engineers can use debug logs to locate faults. Maintenance engineers can use debug logs to locate user-level errors.

Log Format

The log format is as follows:

Log type|Date and time|Log level:Process name|Thread ID|File name: Line number|Log information

Table 1 describes the log format.

Table 1 Debug log format

Parameter	Description	Example
Log type	Log type.	Debug
Date and time	Date and time when the log is generated.	2019/06/20 00:14:40:749
Log level	Level of the generated log.	ERR
Process name	Name of the process that generates the log.	APP:itgt
Thread ID	ID of the thread that generates the log.	TID:1946
File name:Line number	Name of the file where the logs are recorded and number of the line where the code for recording logs is located.	POS:sdc_support_api.cpp:468
Log information	Detailed information of the log.	[LogSDCFrameWork]:Failed to SDCGetMessage hbtp_message fd is 14 gs_ptrEvent fd is 14 Connection reset by peer

Log Example

```
Debug|2019/06/20 00:14:40:749|     ERR:|APP:itgt|TID:1946|POS:sdc_support_api.cpp:468|[LogSDCFram
Debug|2019/06/20 00:14:40:760|     ERR:|APP:TDB3311|TID:2111|POS:Public_MetaDataRecvTask.cpp:63|U
Debug|2019/06/20 00:14:40:760|     ERR:|APP:itgt|TID:1946|POS:sdc_support_api.cpp:468|[LogSDCFram
Debug|2019/06/20 00:14:40:768|  NOTICE:|APP:copra|TID:1431|POS:drv_motor.c:164|[ircut] get ircut
Debug|2019/06/20 00:14:40:760|     ERR:|APP:TDB3311|TID:2111|POS:utils_srvfs_eventcache.c:276|[Lo
```

Parent topic: Log Description

Operation Logs

Log Content

Operation logs (message.opr) record all user operations.

Log Format

The log format is as follows:

Log type|Date and time|Log level:Log information

Table 1 describes the log format.

Table 1 Operation log format

Parameter	Description	Example
Log type	Log type.	Opr
Date and time	Date and time when a log is generated.	2012/11/16 01:48:41:694
Log level	Level of the generated log.	NOTICE
Log information	Detailed information of the log.	Get Media Video Source Configurations Success.

Log Example

```
Opr|2019/11/04 01:48:41:694| NOTICE: Get Media Video Source Configurations Success.
Opr|2019/11/03 01:48:41:994| NOTICE: Get Network Parameters Success.
Opr|2019/11/03 01:48:42:210| NOTICE: Get Device Information Success.
```

Parent topic: Log Description

Run Logs

Log Content

Run logs (message.run) record information about operations performed by operators, providing the operator information (IP address and port number), system time, operation type, and operation result (success or failure).

Log Format

Run logs are in either of the following formats:

- Log type|Date and time|Log level:Log module[Login account information][Login client information] Log information
- Log type|Date and time|Log level:Log information

Table 1 describes the log format.

Table 1 Run log format

Parameter	Description	Example
Log type	Log type.	Run
Date and time	Date and time when a log is generated.	2012/11/19 16:27:18:564
Log level	Level of the generated log.	NOTICE
Log module	Module that generates the log.	WEB
Login account information	Records information about the account used to log in to the current device.	admin
Login client information	Records information about the client that is logged in, in the IP address:port number format.	192.168.0.121:23320
Log information	Detailed information of the log.	Media Play Request Successfully. ChannelID: 101, SessionID: 20

Log Example

```
Run|2019/11/02 14:37:47:395| NOTICE:WEB[admin][192.168.20.160:39141] Get Alarm Input Parameters S
Run|2019/11/02 14:37:47:392| NOTICE:WEB[admin][192.168.20.160:39141] Get Alarm Linkage Policy Suc
Run|2020/07/24 11:37:48:142| NOTICE:HWAPI[ApiAdmin][192.168.20.160:23320] Get Video Parameters Su
```

Parent topic: Log Description

System Logs

Log Content

System logs (message.mem) record all system resource usage information, including the memory and CPU information.

Log Format

The log format is as follows:

Log type|Date and time|TOP:Memory information

CPU information

Process information: Process ID Parent process ID User name of the process owner Process status Virtual memory size Physical memory usage of the process Last CPU usage CPU usage since the latest update

Table 1 describes the log format.

Table 1 System log format

Parameter	Description	Example
Log type	Log type.	check
Date and time	Date and time when a log is generated.	2013/12/20 11:49:47:042
Memory information	Total memory usage	Mem: 88488K used, 36144K free, 0K shrd, 0K buff, 21644K cached
CPU information	Total CPU usage	CPU: 40.0% usr 6.6% sys 0.0% nic 53.3% idle 0.0% io 0.0% irq 0.0% sirq Load average: 2.78 2.81 2.60 1/128 16005
Process information	Information about each process	PID PPID USER STAT VSZ %VSZ CPU %CPU COMMAND 1324 970 root S 367m 300.8 0 39.2 copra

Log Example

```
check|2019/11/05 11:57:28:802|    TOP:Mem: 304476K used, 102748K free, 13668K shrd, 0K buff, 5654
CPU: 16.6% usr 37.5% sys  0.0% nic 45.8% idle  0.0% io  0.0% irq  0.0% sirq
Load average: 16.57 17.71 18.37 3/392 13056
  PID  PPID USER     STAT   VSZ %VSZ CPU %CPU COMMAND
  876   711 sshd     S    1131m283.7   1 42.7 {copra_main} copra
 1478   711 sshd     S     823m206.5   1  2.8 {intelligent} itgt
  437     1 root     S    35880  8.7   0  2.8 ./log
13055 13054 sshd     R     3280  0.8   0  2.8 top n1 -b
 7332     2 root     SW       0  0.0   0  2.8 [kworker/u4:0]
  721   711 sshd     S     182m 45.7   1  0.0 control
 1921     1 root     S    92432 22.6   1  0.0 /usr/app/bin/wifiprobe
  758   711 sshd     S    92140 22.5   0  0.0 netsuit
  843   711 sshd     S    92056 22.5   1  0.0 discover
 1873   711 sshd     S    79192 19.3   0  0.0 main.cgi
  711     1 root     S    72408 17.7   0  0.0 ./daemon
 1876   711 sshd     S N  61116 14.9   1  0.0 sdkserver
 1878   711 sshd     S    30024  7.3   1  0.0 httprest
 1879   711 sshd     S    28036  6.8   1  0.0 {RC_main} rtspclient
 1877   711 sshd     S    25244  6.1   1  0.0 onvif
```

Parent topic: Log Description

Abnormal Stack Logs

Log Content

Abnormal stack logs (ExceptionInfo.log) record all program exceptions.

Log Example

```
----------------BackTrace----------------------
0 /usr/app/lib/libipc_interface.so(SaveBackTraceInfo+0x50) [0x401074cc]
1 /usr/app/lib/libipc_interface.so(SaveExceptionInfo+0x248) [0x40106fa8]
2 /lib/libc.so.6(__default_rt_sa_restorer_v2+0) [0x407d36e0]
3 /lib/libc.so.6(nanosleep+0x44) [0x40847544]
4 /lib/libc.so.6(sleep+0xe8) [0x408472d4]
5 copra(main+0x900) [0xf70c0]
6 /lib/libc.so.6(__libc_start_main+0x118) [0x407bb4c4]
```

Parent topic: Log Description

Upgrade Logs

Log Content

Upgrade logs (update.log) record all version upgrade and algorithm upgrade operations.

Log Format

The log format is as follows:

Date and time Log level (optional) Log information

Table 1 describes the log format.

Table 1 Upgrade log format

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2013-12-16 09:53:19
Log level (optional)	Level of generated logs.	NOTICE
Log information	Detailed information of the log.	Update System success

Log Example

```
2019-10-27 19:18:17| NOTICE:|------Update Cmd <upgrade> starting...------
2019-10-27 19:18:52| NOTICE:|File:/usr/upgrade/3rdApp!!
2019-10-29 10:33:10 Begin manual update to: V500R019C80B000_8.0.RC111.B001 File: /home/sftp_admir
2019-10-29 10:33:50 UpdateSystem success.
2019/10/29 10:36:29 check copra status finish, error cnt 0, status
2019-10-29 16:17:00 Begin manual update to: V500R019C80B000_8.0.T1001.B001 File: /home/sftp_admir
2019-10-29 16:17:40 UpdateSystem success.
```

Parent topic: Log Description

Alarm Logs

Log Content

Alarm logs (message.alarm) record alarm events that occur on the device.

Log Format

The log format is as follows:

Log type|Date and time|Log level:Log information

Table 1 describes the log format.

Table 1 Alarm log format

Parameter	Description	Example
Log type	Log type.	Alarm
Date and time	Date and time when a log is generated.	2012/11/16 01:09:56:601
Log level	Level of generated logs.	NOTICE
Log information	Detailed information of the log.	Temperature alarm. Temperature:50 °c

Log Example

```
Alarm|2019/10/15 16:51:17:601| NOTICE: Temperature alarm. Temperature:50 °c
```

```
Alarm|2019/10/15 16:51:33:484| NOTICE: Disk Abnormal Alarm.
```

Parent topic: Log Description

Error Logs

Log Content

Error logs (message.err) record all program exceptions and service exceptions.

Log Format

The log format is as follows:

Log type|Date and time|Log level:|Thread ID|Abnormal service|Service error code, Abnormal system, System error code and information

Table 1 describes the log format.

Table 1 Error log format

Parameter	Description	Example
Log type	Log type.	Except
Date and time	Date and time when a log is generated.	2013/12/20 10:31:01:487
Log level	Level of the generated log.	ERR
Thread ID	ID of the thread that generates the log.	TID:1074348032
Abnormal service	Information about the abnormal service.	MonitorChildProcessRunningState fail
Service error code	Error code of the abnormal service. For details about how to query the error code, see How to Query Error Codes.	ErrorCode: 30899549104001
Abnormal system	Information about the abnormal system.	WaitPid fail
System error code and information	System error code and system module information.	errno[255:onvif]

Log Example

```
Except|2019/10/20 10:31:19:239| ERR: |TID:1074348032|MonitorChildProcessRunningState fail|ErrorCo
Except|2019/10/20 10:31:22:896| ERR: |TID:1074348032|MonitorChildProcessRunningState fail|ErrorCo
Except|2019/10/20 10:31:27:810| ERR: |TID:1095418976[daemon] onvif Keep Alive Fail|ErrorCode: 308
```

Parent topic: Log Description

Hardware Reset Logs

Log Content

Hardware reset logs (reset.log) record hardware reset operations.

Log Format

The log format is as follows:

[Date and time] Log information

Table 1 describes the log format.

Table 1 Hardware reset log format

Parameter	Description	Example
Date and time	Date and time when the log is generated.	2014-05-06 10:21:21
Log information	Detailed information of the log.	short key-press to reset!

Log Example

```
[2014-05-06 10:21:21] short key-press to reset!
```

Parent topic: Log Description

SSH/SFTP Logs

Log Content

SSH/SFTP logs (message.syslog) record all user operations performed through SSH or SFTP.

Log Format

The log format is as follows:

Log type|Date and time Log level:[Login account information][Login client information] Log information

Table 1 describes the log format.

Table 1 SSH log format

Parameter	Description	Example
Log type	Log type.	SysLog
Date and time	Date and time when a log is generated.	Jan 9 10:07:39
Log level	Level of the generated log.	authpriv.notice
(Optional) Login account information	Information about the user who logs in to the current device.	root
(Optional) Login client information	Information about the client that logs in to the current device.	192.168.0.121 port 49974
Log information	Detailed information of the log.	su: + pts/3 admin:root

Log Example

```
SysLog|Jan  9 10:07:39|  authpriv.notice|sudo:     sshd : TTY=unknown ; PWD=/ ; USER=root ; COMMA
SysLog|Jan  9 10:07:40|  authpriv.notice|sudo:     root : TTY=unknown ; PWD=/ ; USER=root ; COMMA
SysLog|Jan  9 10:07:41|  auth.info|sshd[23293]: Accepted password for admin from 192.168.0.121 po
SysLog|Jan  9 10:07:45|  user.info|-sh: IP=192.168.0.121  PID=23374 PPID=23373 SID=23374 CMD=su r
SysLog|Jan  9 10:07:48|  auth.notice|su: + pts/3 admin:root
```

Parent topic: Log Description

Watchdog Logs

Log Content

Watchdog logs (wdt.log) record exception information generated during watchdog reset at the software layer.

Log Format

The log format is as follows:

Date and time:Log information

Table 1 describes the log format.

Table 1 Watchdog log format

Parameter	Description	Example
Date and time	Date and time when the log is generated.	2013-11-09 20:18:37
Log information	Detailed information of the log.	User has not feed wdt in 7 second!

Log Example

```
2013-11-09 20:18:37 :User has not feed wdt in 7 second!

2013-11-09 20:18:38 :User has not feed wdt in 8 second!

2013-11-18 16:30:00 :User has not feed wdt in 6 second!

2013-11-18 16:33:10 :User has not feed wdt in 6 second!
```

Parent topic: Log Description

Kernel Startup Logs

Log Content

Kernel startup logs (dmesg.log) record information about the Linux kernel process loading during the device startup.

Log Example

```
[    0.000000] Booting Linux on physical CPU 0x0
[    0.000000] Linux version 4.9.37 (root@shaphicprb13206) (gcc version 6.3.0 (HC&C V100R002C00B0
[    0.000000] CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=10c5387d
[    0.000000] CPU: div instructions available: patching division code
[    0.000000] CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
[    0.000000] OF: fdt:Machine model: Hisilicon HI3516DV300 DEMO Board
[    0.000000] cmz zone is not set!
[    0.000000] cma: dma_contiguous_reserve(limit ffffffff)
[    0.000000] cma: dma_contiguous_reserve: reserving 16 MiB for global area
[    0.000000] cma: cma_declare_contiguous(size 0x01000000, base 0x00000000, limit 0xffffffff ali
[    0.000000] cma: Reserved 16 MiB at 0x98800000
[    0.000000] Memory policy: Data cache writealloc
[    0.000000] On node 0 totalpages: 104960
[    0.000000] free_area_init_node: node 0, pgdat c0c31140, node_mem_map d8461000
[    0.000000]   Normal zone: 923 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 104960 pages, LIFO batch:31
......
```

Parent topic: Log Description

Process Exception Log

Log Content

Process exception logs (ExceptionInfo_*process name*.log) record process exceptions. Only the 3519A and 3559A chips support this function.

Log Example

```
====================Exception Info====================
Exception Occur Time : Tue Jun 18 02:50:02 2019

Receive signal: 6.
si_code: -6.
si_errno: 0.

--------------------Maps----------------------
6fdd4000-6fdd5000 ---p 00000000 00:00 0
6fdd5000-705d4000 rw-p 00000000 00:00 0
705d4000-705fa000 rw-s ade85000 00:02 2192       /dev/sys
705fa000-7069b000 rw-p 00000000 00:00 0
7069b000-7069c000 ---p 00000000 00:00 0
7069c000-706db000 rw-p 00000000 00:00 0
706db000-706dc000 ---p 00000000 00:00 0
706dc000-7071b000 rw-p 00000000 00:00 0
...
```

Parent topic: Log Description

Process Restart Log

Log Content

Process restart logs (RebootInfo.log) record restart information about each process, including the restart time, restart type, and PID.

Log Format

The log format is as follows:

Date and time

PID

Process name

Process status

Table 1 describes the log format.

Table 1 Process restart log format

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2019-06-11 13:41:53
PID	Process ID.	725
Process name	Name of the process that generates the log.	control
Process status	Status of the current login process.	Abnormal

Log Example

```
[2019-11-05 22:20:50]
PID:1273
ProcessName:control
RebootType:NORMAL
```

Parent topic: Log Description

Daemon Run Logs

Log Content

Daemon run logs (damon.log) record Daemon running information.

Log Format

The log format is as follows:

Date and time|Log level|Log information

Table 1 describes the log format.

Table 1 Daemon run format

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2012/11/16 01:09:56:601
Log level	Level of generated logs.	NOTICE
Log information	Detailed information of the log.	Create Thread success, Starting Init Daemon

Log Example

```
2019-11-04 16:31:19| NOTICE:|Init Daemon Success!!!
2019-11-05 22:21:16| NOTICE:|Create Thread success, Starting Init Daemon...
2019-11-05 22:21:24| NOTICE:|Init App success, Starting Create All App...
```

Parent topic: Log Description

Daemon Exception Logs

Log Content

Daemon exception logs (RebootInfo_daemon.log) record exceptions that occur during Daemon running.

Log Format

The log format is as follows:

Log type|Date and time|Log level|Process name|Thread ID|File name: Line number|Log information

Table 1 describes the log format.

Table 1 Daemon exception log format

Parameter	Description	Example
Log type	Log type.	Debug
Date and time	Date and time when a log is generated.	2012/11/16 01:09:56:601
Log level	Level of generated logs.	NOTICE
Process name	Name of the process that generates the log.	APP:daemon
Thread ID	ID of the thread that generates the log.	TID:1002
File name:Line number	Name of the file where the logs are recorded and number of the line where the code for recording logs is located.	POS:InitSystem.cpp:439
Log information	Detailed information of the log.	Get <copra> runing status:5!!

Log Example

```
Debug|2019/11/04 16:29:54:519|  NOTICE:|APP:daemon|TID:1002|POS:InitSystem.cpp:439|Get <copra> ru
Debug|2019/11/04 16:29:54:520|  NOTICE:|APP:daemon|TID:1007|POS:Business.cpp:290|Managed App [cop
```

Parent topic: Log Description

System Initialization Log

Log Content

System initialization logs (sysInitInfo.log) record the key process and operation result of system initialization.

Log Example

```
step:2:succed in excutting -t /sbin/sshd cmd in /bin/sh
step:2:succed in excutting mount -o noexec,nosuid -t ubifs ubi2:log /usr/log cmd in /bin/sh
step:2:succed in excutting mount -o noexec,nosuid -t ubifs ubi3:setting /usr/setting  cmd in /bir
step:2:succed in excutting mount -o noexec,nosuid -t ubifs ubi4:setting_bak /usr/setting_bak cmd
step:2:succed in excutting mount -o noexec,nosuid -t ubifs ubi5:alg_model /usr/alg_model cmd in /
step:2:succed in excutting mount -o noexec,nosuid,nodev -t tmpfs tmpfs /usr/upgrade cmd in /bin/s
(/usr1/home/workspace/Master.6f8deacf.Package.Package_L_Linux_Sign_Multi/src/chip_platform/Hi3516
```

Parent topic: Log Description

Container Engine Run Logs

Log Content

Container engine run logs (lcrd.log) record container engine running information.

Log Format

The log format is as follows:

Date and time Log information

Table 1 describes the log format.

Table 1 Container engine run log format

Parameter	Description	Example
Date and time	Date and time when a log is generated. The format is yyyymmddhhmmss.ms.	20191104162920.827
Log information	Detailed information of the log.	Event: {Object: list images, Type: listing, Filter: }

Log Example

Sample of logs without exceptions:

```
20191104162920.827 Event: {Object: list images, Type: listing, Filter: }
20191104162920.857 Event: {Object: /usr/app/container/manifest.json, Type: loaded}
```

Parent topic: Log Description

No Sensor Data Count Logs

Log Content

The log records the number of times that the camera fails to detect sensor data.

If the camera fails to detect sensor data, the camera will restart for restoration. If the camera fails to detect sensor data for more than three consecutive times, the camera will not automatically restart.

Parent topic: Log Description

Kbox Logs

Log Content

Kbox logs (kbox_current.log) record exceptions (such as panic and oops) that occur on the kernel.

Log Format

The log format is as follows:

Date and time Log information

Table 1 describes the log format.

Table 1 Kbox log format

Parameter	Description	Example
Date and time	Date and time when the log is generated. This parameter is not contained in logs without exceptions.	UTC Time 2017-12-27 09:03:49 East 0
Log information	Detailed information of the log.	Shell: su

Log Example

Sample of logs without exceptions:

```
Kboxdump_LookUpMem:/dev/kbox dump success
```

Sample of logs with exceptions:

```
UTC Time 2017-10-13 14:17:43  East 0
   [DIE_OOPS]
code:1, err: 5, trap: 0, sig: 11, msg: Oops

       ====================crash time====================
UTC Time 2017-10-13 14:17:43  East 0
```

```
   ====================sys info====================
UTC Time 2017-10-13 14:17:43  East 0
   sysname     Linux
      release     3.18.20
    version     #1 SMP Tue Sep 5 10:30:29 CST 2017
 machine     armv7l
     nodename    IPC
     domainname  domain.com
 ccversion   CCVERSION
  jiffies     139231943
  uptime  16 days 02:50
  load avg   4.28 4.39 4.41
      running threads  76
    last running:  12638
   MemTotal:      367676 kB
       MemFree:       164248 kB
       Buffers:            0 kB
       Cached:         51248 kB
       SwapCached:         0 kB
       HighTotal:          0 kB
       HighFree:           0 kB
       LowTotal:      367676 kB
       LowFree:       164248 kB
       SwapTotal:          0 kB
       SwapFree:           0 kB
```

Parent topic: Log Description

Frequently Recorded Logs

Log Content

To ensure that key information in debug logs is not overwritten by frequently recorded logs, the camera system sets a type of frequently recorded logs (message.fre) for recording logs that are updated frequently or periodically.

Log Format

The log format is as follows:

Log type|Date and time|Log level|Process name|Thread ID|File name: Line number|Log information

Table 1 describes the log format.

Table 1 Frequent log format

Parameter	Description	Example
Log type	Log type.	fre
Date and time	Date and time when a log is generated.	2019/06/19 23:05:40:994
Log level	Level of the generated log.	NOTICE
Process name	Name of the process that generates the log.	APP:copra
Thread ID	ID of the thread that generates the log.	TID:1710
File name:Line number	Name of the file where the logs are recorded and number of the line where the code for recording logs is located.	POS:isp_irlight.c:1171
Log information	Detailed information of the log.	IR IN

Log Example

```
fre|2019/06/19 23:05:40:994|  NOTICE:|APP:copra|TID:1710|POS:isp_irlight.c:1171|IR IN
fre|2019/06/19 23:05:41:190|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:176|Release VbBlk : 327680 ,
fre|2019/06/19 23:05:41:202|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:146|GET VbBlk : 327680 ,VbPo
fre|2019/06/19 23:05:41:206|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:176|Release VbBlk : 983040 ,
fre|2019/06/19 23:05:41:208|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:146|GET VbBlk : 983040 ,VbPo
fre|2019/06/19 23:05:41:234|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:176|Release VbBlk : 327680 ,
fre|2019/06/19 23:05:41:236|  NOTICE:|APP:copra|TID:887|POS:vb_mem.c:146|GET VbBlk : 327680 ,VbPo
```

Parent topic: Log Description

Nginx Server Access Logs

Log Content

The Nginx open-source software automatically generates Nginx access logs. The log information is stored in the **message.syslog** file. Therefore, the **nginx_access.log** file is empty.

Parent topic: Log Description

Nginx Server Debug Logs

Log Content

Debug logs of the Nginx server are a small part of the logs generated before the Nginx loads the configuration. After the configuration is complete, the logs are stored in the **message.syslog** file.

Log Format

The log format is as follows:

Date and time Log level Process ID#Thread ID: Log information

Table 1 describes the log format.

Table 1 Nginx server debug log format

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2016/03/06 12:28:11
Log level	Level of the generated log.	notice
Process ID	ID of the process that generates the log.	11891
Thread ID	ID of the thread that generates the log.	0
Log information	Detailed information of the log.	get_certs_private_key_pwd success, try_index=3. (2: No such file or directory) in /usr/app/bin/nginx_bin/nginx.bak.conf:298

Log Example

```
2016/03/06 12:28:11 [notice] 11891#0: get_certs_private_key_pwd success, try_index=3. (2: No such
2016/03/06 12:28:15 [notice] 11948#0: change_nginx_process_usr start (2: No such file or director
2016/03/06 12:28:15 [notice] 11948#0: uid=109 euid=109 gid=65534
2016/03/06 12:28:15 [notice] 11948#0: change_nginx_process_usr success
```

Parent topic: Log Description

App Installation Debug Logs

Log Content

Debug logs are recorded during app installation.

Log Format

The log format is as follows:

Log type|Date and time: Log information

Table 1 describes the log format.

Table 1 App installation debug log format

Parameter	Description	Example
Log type	Log type.	Debug
Date and time	Date and time when a log is generated.	2020-03-06T14:50:06+0000
Log information	Detailed information of the log.	thirdapp_create TXProcess

Log Example

```
DEBUG|[2020-03-06T14:50:06+0000]: thirdapp_start TXProcess check_mgr_stat
DEBUG|[2020-03-06T14:50:06+0000]: thirdapp_create TXProcess
DEBUG|[2020-03-06T14:50:06+0000]: disk_get_app_space_path TXProcess
DEBUG|[2020-03-06T14:50:06+0000]: thirdapp_start bbb check_mgr_stat
```

Parent topic: Log Description

App Lifecycle Debug Logs

Log Content

Debug logs are recorded throughout the app lifecycle.

Log Format

The log format is as follows:

Log type|Date and time: Log information

Table 1 describes the log format.

Table 1 App lifecycle debug log format

Parameter	Description	Example
Log type	Log type.	Debug
Date and time	Date and time when a log is generated.	2020-03-06T14:49:12+0000
Log information	Detailed information of the log.	thirdapp_start note_30 check_mgr_stat

Log Example

```
DEBUG|[2020-03-06T14:49:12+0000]: thirdapp_start note_30 check_mgr_stat
DEBUG|[2020-03-06T14:49:12+0000]: thirdapp_create note_30
DEBUG|[2020-03-06T14:49:12+0000]: disk_get_app_space_path note_30
DEBUG|[2020-03-06T14:49:12+0000]: thirdapp_start TXProcess check_mgr_stat
```

Parent topic: Log Description

Recent User Login Logs

Log Content

Recent user login logs (lastlog) record information about recent user logins.

Parent topic: Log Description

Process Startup Time Logs

Log Content

Process startup time logs (SoftwareInfo.log) record the process startup time.

Log Format

The log format is as follows:

Log type|Date and time|Log level|Process name|Log information

Table 1 describes the log format.

Table 1 Process startup time log format

Parameter	Description	Example
Log type	Log type.	SoftWareInfo
Date and time	Date and time when a log is generated.	2012/11/16 01:09:56:601
Log level	Level of generated logs.	NOTICE
Process name	Name of the process that generates the log.	APP:control
Log information	Detailed information of the log.	Build Time: Nov 2 2019 15:05:03

Log Example

```
SoftWareInfo|2019/11/05 22:21:16:234|  NOTICE:|APP:daemon|CI Version : 8.0.RC101.SPC1.B001
SoftWareInfo|2019/11/05 22:21:16:234|  NOTICE:|APP:daemon|Build Time: Nov  2 2019 15:05:03
SoftWareInfo|2019/11/05 22:21:31:679|  NOTICE:|APP:control|Build Time: Nov  2 2019 15:04:51
```

Parent topic: Log Description

Hardware Fault Logs

Log Content

Hardware fault logs (message.hard_alarm) record alarm events that occur on the hardware device.

Log Format

The log format is as follows:

Log type|Date and time|Log level:Log information

Table 1 describes the log format.

Table 1 Hardware fault log format

Parameter	Description	Example
Log type	Log type.	HardAlarm
Date and time	Date and time when a log is generated.	2012/11/16 01:09:56:601
Log level	Level of the generated log.	NOTICE
Log information	Detailed information of the log.	Temperature alarm. Temperature:50 °c

Log Example

```
HardAlarm|2019/10/29 10:35:04:994|  NOTICE:Electrical Port[0] Network Outage Alarm Cleared.
HardAlarm|2019/10/30 14:23:10:601|  NOTICE:Fibre Optical Port Network Outage Alarm
```

Parent topic: Log Description

ITGT Intelligent Exception Logs

Log Content

This log (ItgtExceptionInfo.log) is generated when the intelligent algorithm process is interrupted unexpectedly or the intelligent algorithm is manually upgraded.

Log Example

Figure 1 shows a typical example of the ITGT intelligent exception log.

Figure 1 ITGT intelligent exception log

```
====================Exception Info====================
Exception Occur Time : Wed Aug  8 00:07:27 2018

Receive signal : 15.
si_code: 0.
si_errno: 0.
```

In this case, when the intelligent algorithm is upgraded, the camera receives the "signal 15" signal, interrupts the intelligent algorithm, and loads the new algorithm.

Parent topic: Log Description

Wi-Fi Probe Debug Log

Log Information

The log records Wi-Fi probe debugging information.

Log Format and Content

The log format is as follows:

Date and time|Log level|Thread ID|File name|Log information

Table 1 describes the log content.

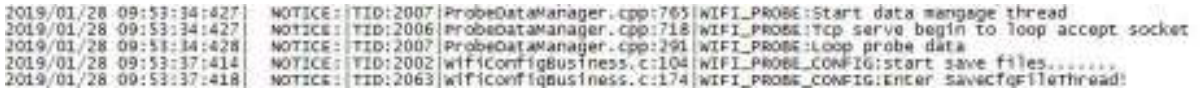
Table 1 Log content description

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2019/01/16 01:48:41:694
Log level	Level of generated logs.	NOTICE
Thread ID	Thread ID of the current log.	TID:2007
File name	Name of a log file.	ProbeDatManager.cpp:718
Log information	Detailed information of a log.	WIFI_PRBE:Start data mangage thread

Log Example

Figure 1 shows a typical Wi-Fi probe debug log.

Figure 1 Wi-Fi probe debug log



Parent topic: Log Description

Wi-Fi Probe Run Log

Log Information

The log records Wi-Fi probe running information.

Log Format and Content

The log format is as follows:

Date and time|Log level|Log information

Table 1 describes the log content.

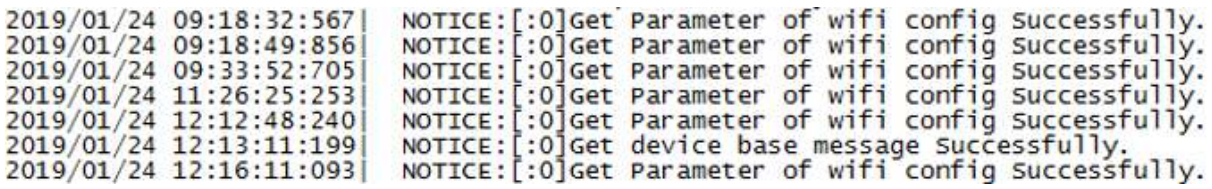
Table 1 Log content description

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2019/01/16 01:48:41:694
Log level	Level of generated logs.	NOTICE
Log information	Detailed information of a log.	Get Parameter of wifi config Successfully.

Log Example

Figure 1 shows a typical Wi-Fi probe run log.

Figure 1 Wi-Fi probe run log



Parent topic: Log Description

Wi-Fi Probe Operation Log

Log Information

The log records Wi-Fi probe operations.

Log Format and Content

The log format is as follows:

Date and time|Log level|Log information

Table 1 describes the log content.

Table 1 Log content description

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2019/01/16 01:48:41:694
Log level	Level of generated logs.	NOTICE
Log information	Detailed information of a log.	Restore config Successfully.

Log Example

Figure 1 shows a typical Wi-Fi probe operation log.

Figure 1 Wi-Fi probe operation log

```
2019/01/26 17:34:54:222|  NOTICE:[:0]Restore config Successfully.
2019/01/26 17:34:54:287|  NOTICE:[:0]Restore config Successfully.
2019/01/26 17:34:54:339|  NOTICE:[:0]Restore config Successfully.
2019/01/26 17:40:43:689|  NOTICE:[:0]Restore config Successfully.
```

Parent topic: Log Description

Wi-Fi Probe Alarm Log

Log Information

The log records Wi-Fi probe alarm information.

Log Format and Content

The log format is as follows:

Date and time|Log level:Log information

Table 1 describes the log content.

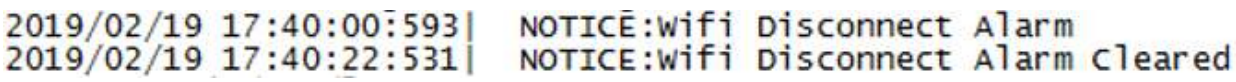
Table 1 Log content description

Parameter	Description	Example
Date and time	Date and time when a log is generated.	2019/01/16 01:48:41:694
Log level	Level of generated logs.	NOTICE
Log information	Detailed information of a log.	Wifi Disconnect Alarm

Log Example

Figure 1 shows a typical Wi-Fi probe alarm log.

Figure 1 Wi-Fi probe alarm log



Parent topic: Log Description

Error Codes

- **How to Query Error Codes**
- **Function Module Code**
- **System Service Code**
- **Error Information**

Parent topic: Log Reference

How to Query Error Codes

Each module of the product may generate errors codes that range from 30899339100000 to 30899609113999. You can query the error codes through log query or download or on web pages.

A camera error code consists of the following parts: 30899 + Functional module code (2 digits) + 91 + Service type code (2 digits) + Error code (3 digits)

You can query exception logs on the web page or download the device log **/opt/log/message.err** to view error codes.

Parent topic: Error Codes

Function Module Code

Function Module	Module Code	Error Code Range
WebServer	33	30899339100000–30899339113999
SDK GateWay	34	30899349100000–30899349113999
ONVIF	35	30899359100000–30899359113999
T28181	36	30899369100000–30899369113999
SNMP	37	30899379100000–30899379113999
Main control	38	30899389100000–30899389113999
Configuration management	39	30899399100000–30899399113999
User management	40	30899409100000–30899409113999
Media stream management	41	30899419100000–30899419113999
CODEC	42	30899429100000–30899429113999
Media stream storage	43	30899439100000–30899439113999
Alarm linkage	44	30899449100000–30899449113999
PTZ control	45	30899459100000–30899459113999
ISP	46	30899469100000–30899469113999
Encoding and decoding	47	30899479100000–30899479113999

Function Module	Module Code	Error Code Range
Lens drive	48	308994<u>8</u>9100000–308994<u>8</u>9113999
Intelligent analysis	49	308994<u>9</u>9100000–308994<u>9</u>9113999
Alarm drive	50	308995<u>0</u>9100000–308995<u>0</u>9113999
Network drive	51	308995<u>1</u>9100000–308995<u>1</u>9113999
Secondary development interface	52	308995<u>2</u>9100000–308995<u>2</u>9113999
Upgrade management	53	308995<u>3</u>9100000–308995<u>3</u>9113999
Daemon process	54	308995<u>4</u>9100000–308995<u>4</u>9113999
SSH	55	308995<u>5</u>9100000–308995<u>5</u>9113999
Syslogd	56	308995<u>6</u>9100000–308995<u>6</u>9113999
DHCP	57	308995<u>7</u>9100000–308995<u>7</u>9113999
NTP	58	308995<u>8</u>9100000–308995<u>8</u>9113999
Black box	59	308995<u>9</u>9100000–308995<u>9</u>9113999

Parent topic: Error Codes

System Service Code

System service	system service code	Error code range
Self-check and startup	00	30899329100000~~30899599100999
Network	01	30899329101000~~30899599101999
Registration and authentication	02	30899329102000~~30899599102999
Operations on storage devices and files	03	30899329103000~~30899599103999
Process exceptions and restarts	04	30899329104000~~30899599104999
Auto exposure, auto white balance, auto focus (3A)	05	30899329105000~~30899599105999
ISP-related services (excluding 3A)	06	30899329106000~~30899599106999
Encoding and encryption	07	30899329107000~~30899599107999
PTZ	08	30899329108000~~30899599108999

System service	system service code	Error code range
Hardware exceptions	09	30899329109000~~30899599109999
System invoking exceptions	10	30899329110000~~30899599110999
Abnormal inputs and outputs	11	30899329111000~~30899599111999
Memory-related services	12	30899329112000~~30899599112999
Impossible	13	30899329113000~~30899599113999

Parent topic: Error Codes

Error Information

007

104

105

113

129

130

141

142

143

145

148

149

159

160

215

216

217

218

219

220

221

222

223

224

225

226

227

228

370

371

372

3251

3257

Parent topic: Error Codes

007

Error Information

An error message is displayed if the serial port number is incorrectly set.

Possible Causes

The configured serial port number exceeds the maximum number of serial ports supported by the device.

Solution

Contact technical support engineers to confirm the maximum number of serial ports supported by the device.

Parent topic: Error Information

104

Error Information

An error message is displayed when the upgrade file fails to be verified during device upgrade.

Possible Causes

1. The upgrade file is corrupted.
2. The upgrade file version does not match the current device.

Solution

1. Check the integrity of the upgrade file and obtain the correct upgrade package from the enterprise technical support website.
2. Verify that the upgrade file supports the current camera model.
3. If solutions 1 and 2 do not work, contact technical support.

Parent topic: Error Information

105

Error Information

An error message is displayed when the upgrade file fails to be verified during device upgrade.

Possible Causes

1. The upgrade file is corrupted.
2. The upgrade file version does not match the current device.

Solution

1. Check the integrity of the upgrade file and obtain the correct upgrade package from the website.
2. Verify that the upgrade file supports the current camera model.
3. If solutions 1 and 2 do not work, contact technical support.

Parent topic: Error Information

113

Error Information

An error message is displayed if the source version is the same as the target version during device upgrade.

Possible Causes

The version number of the upgrade file is the same as the current software version number of the device.

Solution

Check whether the version number of the upgrade file is the same as that of the device to be upgraded. If so, no upgrade is required.

Parent topic: Error Information

129

Error Information

An error message is displayed when you set ROIs in the MJPEG video compression format.

Possible Causes

The ROI function is not supported in the MJPEG format.

Solution

To set ROIs, choose **Settings** > **Video/Audio/Image** > **Video**, and set **Encoding protocol** to H.265 or other related formats.

Parent topic: Error Information

130

Error Information

An error message is displayed when you configure the ROI function for the secondary stream if the secondary stream is not enabled.

Possible Causes

The secondary stream is not enabled.

Solution

Ensure that the secondary stream is enabled when you set the ROI function for the secondary stream.

Parent topic: Error Information

141

Error Information

The error code 141 is returned when the number of configured tripwires exceeded the maximum.

Possible Causes

1. The number of configured behavior analysis tripwires exceeded the maximum.
2. The number of configured tripwires exceeded the maximum after you added a tripwire.

Solution

Verify that the number of tripwires does not exceed the maximum.

Parent topic: Error Information

142

Error Information

The error code 142 is returned when the number of configured areas exceeded the maximum (4).

Possible Causes

1. The number of single-rule areas exceeded the maximum after you added an area.
2. The number of single-rule areas exceeded the maximum after you set the area rules parameters, including the rule parameter and area parameter.
3. The number of single-rule areas exceeded the maximum after you added area information.
4. The number of single-rule areas exceeded the maximum after you set the detection area parameters, including area rules and area information.

Solution

Verify that the number of configured areas does not exceed the maximum.

Parent topic: Error Information

143

Error Information

The error code 143 is returned when the number of configured areas exceeded the maximum (10).

Possible Causes

1. The number of configured areas exceeded the maximum after you set the area rules parameters, including the rule parameter and area parameter.
2. The number of configured areas exceeded the maximum after you added, deleted, or modified detection areas.
3. The number of configured areas exceeded the maximum after you set the detection area parameters, including rules and area information.

Solution

Verify that the number of configured areas does not exceed the maximum.

Parent topic: Error Information

145

Error Information

The error code 145 is returned when the number of configured vertices exceeded the maximum.

Possible Causes

The number of configured vertices exceeded the maximum.

Solution

Delete the drawn detection area, and draw a new one correctly.

Parent topic: Error Information

148

Error Information

The error code 148 is returned when global parameters for the intelligent analysis algorithm failed to be set.

Possible Causes

1. The parameter is empty.
2. The intelligent services are disabled.
3. The metadata is disabled.
4. The background update parameter is incorrectly set.
5. The sensitivity parameter is incorrectly set.
6. The shadow removal mode parameter is incorrectly set.
7. The sensitivity parameter is incorrectly set.
8. The maximum number of objects is incorrect.
9. The rectangle width parameter is incorrectly set.
10. The maximum or minimum value is incorrect.

Solution

Verify that the parameters are correctly set.

Parent topic: Error Information

149

Error Information

The error code 149 is returned if the intelligent analysis area is invalid.

Possible Causes

1. The number of vertices in the area is less than 3.
2. The start coordinate is out of the rule frame.
3. The end coordinate is out of the rule frame.
4. The start coordinate overlaps the end coordinate.

Solution

Verify that the intelligent analysis area is correctly set.

Parent topic: Error Information

159

Error Information

The error code 159 is returned if the intelligent analysis area does not exist.

Possible Causes

1. The intelligent analysis area does not exist.
2. The intelligent analysis area is deleted.

Solution

Verify that the intelligent analysis area is correctly set.

Parent topic: Error Information

160

Error Information

The error code 160 is returned if the intelligent analysis tripwire does not exist.

Possible Causes

1. The intelligent analysis tripwire does not exist.
2. The intelligent analysis tripwire is deleted.

Solution

Verify that the intelligent analysis tripwire is correctly set.

Parent topic: Error Information

215

Error Information

An error message is displayed if you try to enable the manual exposure mode and background frequency simultaneously.

Possible Causes

1. You try to enable background frequency when the manual exposure mode is enabled.
2. You try to enable the manual exposure mode when background frequency is enabled.

Solution

Disable the manual exposure mode or background frequency.

Parent topic: Error Information

216

Error Information

An error message is displayed if you try to enable the manual exposure mode and highlight compensation simultaneously.

Possible Causes

1. You try to enable highlight compensation when the manual exposure mode is enabled.
2. You try to enable the manual exposure mode when highlight compensation is enabled.

Solution

Disable the manual exposure mode or highlight compensation.

Parent topic: Error Information

217

Error Information

An error message is displayed if you try to enable the shutter priority mode and WDR simultaneously.

Possible Causes

1. You try to enable WDR when the shutter priority mode is enabled.
2. You try to enable the shutter priority mode when WDR is enabled.

Solution

Disable the shutter priority mode or WDR.

Parent topic: Error Information

218

Error Information

An error message is displayed if you try to enable the shutter priority mode and background frequency simultaneously.

Possible Causes

1. You try to enable background frequency when the shutter priority mode is enabled.
2. You try to enable the shutter priority mode when background frequency is enabled.

Solution

Disable the shutter priority mode or background frequency.

Parent topic: Error Information

219

Error Information

An error message is displayed if you try to enable the shutter priority mode and highlight compensation simultaneously.

Possible Causes

1. You try to enable highlight compensation when the shutter priority mode is enabled.
2. You try to enable the shutter priority mode when highlight compensation is enabled.

Solution

Disable the shutter priority mode or highlight compensation.

Parent topic: Error Information

220

Error Information

An error message is displayed if you try to enable backlight compensation and WDR simultaneously.

Possible Causes

1. You try to enable WDR when the backlight compensation mode is enabled.
2. You try to enable backlight compensation when WDR is enabled.

Solution

Disable WDR or backlight compensation.

Parent topic: Error Information

221

Error Information

An error message is displayed if you try to enable backlight compensation and highlight compensation simultaneously.

Possible Causes

1. You try to enable highlight compensation when backlight compensation is enabled.
2. You try to enable backlight compensation when highlight compensation is enabled.

Solution

Disable highlight compensation or backlight compensation.

Parent topic: Error Information

222

Error Information

An error message is displayed if you try to enable WDR and highlight compensation simultaneously.

Possible Causes

1. You try to enable highlight compensation when WDR is enabled.
2. You try to enable WDR when highlight compensation is enabled.

Solution

Disable highlight compensation or WDR.

Parent topic: Error Information

223

Error Information

An error message is displayed if you try to enable WDR and defogging simultaneously.

Possible Causes

1. You try to enable defogging when WDR is enabled.
2. You try to enable WDR when defogging is enabled.

Solution

Disable defogging or WDR.

Parent topic: Error Information

224

Error Information

An error message is displayed if you try to enable highlight compensation and set the full frame rate to 50 or 60 fps.

Possible Causes

1. You try to set the full frame rate to 50 or 60 fps when highlight compensation is enabled.
2. You try to enable highlight compensation when the full frame rate is set to 50 or 60 fps.

Solution

Ensure that the full frame rate is not set to 50 or 60 fps or disable highlight compensation.

Parent topic: Error Information

225

Error Information

An error message is displayed if you try to enable WDR and set the full frame rate to 50 or 60 fps.

Possible Causes

1. You try to set the full frame rate to 50 or 60 fps when WDR is enabled.
2. You try to enable WDR when the full frame rate is set to 50 or 60 fps.

Solution

Ensure that the full frame rate is not set to 50 or 60 fps or disable WDR.

Parent topic: Error Information

226

Error Information

An error message is displayed if you try to enable the manual exposure mode and backlight compensation simultaneously.

Possible Causes

1. You try to enable backlight compensation when the manual exposure mode is enabled.
2. You try to enable the manual exposure mode when backlight compensation is enabled.

Solution

Disable the manual exposure mode or backlight compensation.

Parent topic: Error Information

227

Error Information

An error message is displayed if you try to enable highlight compensation and slow shutter simultaneously.

Possible Causes

1. You try to enable slow shutter when highlight compensation is enabled.
2. You try to enable highlight compensation when slow shutter is enabled.

Solution

Disable highlight compensation or slow shutter.

Parent topic: Error Information

228

Error Information

An error message is displayed if you try to enable WDR and slow shutter simultaneously.

Possible Causes

1. You try to enable slow shutter when WDR is enabled.
2. You try to enable WDR when slow shutter is enabled.

Solution

Disable WDR or slow shutter.

Parent topic: Error Information

370

Description

The primary camera fails to send packets to the secondary camera.

Possible Causes

- The secondary camera is abnormal.
- The versions of the primary and secondary cameras are inconsistent.

Solution

- Log in to the primary and secondary cameras and check whether their versions are consistent.
- Log in to the secondary camera and check whether the camera process is normal.
- Use the one-click log collection tool to collect logs and contact technical support.

Parent topic: Error Information

371

Description

The upgrade of the secondary camera times out.

Possible Causes

The upgrade process of the secondary camera is abnormal.

Solution

Use the one-click log collection tool to collect logs and contact technical support.

Parent topic: Error Information

372

Description

The upgrade of the secondary camera fails due to insufficient storage space.

Possible Causes

The storage space of the secondary camera is full.

Solution

1. Log in to the secondary camera at the backend and run the **df -h** and **free** commands to check whether the storage space of the camera is sufficient.
2. If the storage space is insufficient, check which directories occupy large space.
3. If the storage space is sufficient, use the one-click log collection tool to collect logs and contact technical support.

Parent topic: Error Information

3251

Description

The rotatable lens of a compound-eye camera or the secondary camera of a dual-lens cube camera is abnormal.

Possible Causes

An exception occurs when starting the rotatable lens of a compound-eye camera or the secondary camera of a dual-lens cube camera.

Solution

1. Log in to the rotatable lens or secondary camera at the backend and check whether the process is normal.
2. Use the one-click log collection tool to collect logs and contact technical support.

Parent topic: Error Information

3257

Description

The communication between the fixed lens and rotatable lens of a compound-eye camera or the primary camera and secondary camera of a dual-lens cube camera is abnormal.

Possible Causes

1. The storage space of the rotatable lens or secondary camera is full.
2. The process of the rotatable lens or secondary camera is abnormal.

Solution

1. Log in to the rotatable lens or secondary camera at the backend and check whether the storage space is sufficient.
2. Log in to the rotatable lens or secondary camera at the backend and check whether the process is normal.
3. Use the one-click log collection tool to collect logs and contact technical support.

Parent topic: Error Information

Error Code Reference

Example:

2013/12/20 10:31:26:785|
ERR:|TID:1074348032|MonitorChildProcessRunningState
fail|ErrorCode:30899549104001, WaitPid fail, errno[15:onvif]

The error code is 30899549104001.

- **30899**: unified error code ID of a video security product.
- **54**: function module type. This value indicates the daemon process. For details, see Function Module Code.
- **91**: fixed identifier.
- **04**: service type. This value indicates that the process restarts due to an exception. For details, see System Service Code.
- **001**: error type. This value indicates a common error. For details, see Error Information.

Therefore, the error code 30899549104001 indicates that the daemon process detects abnormal processes. The error information "WaitPid fail" shows that the system function WaitPid is faulty. In addition, the system error code is **15**, indicating that the **kill** command is received, and **onvif** indicates that the process that receives the **kill** command is the onvif process.

Parent topic: Log Reference

Command Reference

- Operation Description
- Command Description
- Appendix

Parent topic: Reference

Operation Description

This section describes only the commands for executing applications. For details about the commands provided by the busybox and Linux, see Operation Description.

NOTICE

- The commands in this document must be used under the guidance of engineers. Otherwise, the functions of the device may be affected.
- Whether a command takes effect depends on the functions supported by the camera.
- Different models of cameras support different commands.

You can log in to the Linux operating system of the device and set device parameters and query the device status. To log in to the Linux operating system, perform the following steps:

1. Log in to the Linux operating system as the **admin** user in SSH mode.
2. Run the **su - root** command to switch to the **root** user.
3. Run the **cd /usr/app/bin** command go to the **bin** directory.

Parent topic: Command Reference

Command Description

- **Log Commands**
- **Media Stream Commands**
- **System Commands**

Parent topic: Command Reference

Log Commands

- **./help**
- **./help debug**

Parent topic: Command Description

./help

Function

The **./help** command is used to query information about all commands.

Format

./help

Parent topic: Log Commands

./help debug

Function

The **./help debug** command is used to enable or disable the debug log function of a module. After the debug log function is enabled, you can query the debug log of the module.

Format

./help debug [State] [Module]

Parameter Description

Parameter	Description	Value
State	Enables or disables the debug log function.	• **open**: enables the debug log function. • **close**: disables the debug log function.
Module	ID of the log module.	The options are as follows: • **0**: all modules, involving logs about all modules. • **1**: main control module, involving interaction logs between modules. • **2**: COMM module, involving logs about the operations of the platform on devices. • **3**: RTP module, involving logs about video streams. • **4**: CODEC module, involving interaction logs between encoders, decoders, and drivers. • **5**: PTZ module, involving PTZ control operation logs. • **6**: ALARM module, involving various device alarms, such as temperature

Parameter	Description	Value
		alarms, Boolean value alarms, and lens blocking alarms. • **7**: web module, involving logs about parameter settings on web pages and live video viewing. • **8**: IQ_IMG module, involving logs about the device boards. • **9**: ONVIF module, involving logs about the operations of the ONVIF platform on devices. • **10**: RECORD module, involving storage logs, such as the SD card management and full disk alarms. • **12**: SDK module, involving logs about parameter settings, live video viewing, alarms, PTZ, and device management. • **14**: DISCOVER module, involving network-related logs. • **15**: UPDATE module, involving logs about system upgrade. • **16**: DAEMON module, involving process-related logs. • **17**: DRIVER module, involving driver-related logs. • **18**: GB/T 28181 module, involving the GB/T 28181 logs. • **19**: NETSUIT module, involving SNMP and 802.1X logs. • **21**: ITGT (intelligent) module, involving info logs of the ITGT service. • **23**: RC module, involving info logs of the RC module. • **24**: RS module, involving info logs of the RS module.

Parameter	Description	Value
		• **25**: ITGT (intelligent) module, involving info logs of the ITGT algorithm. • **26**: REST module, involving logs of the REST interconnection protocol. • **27**: ODS module, involving logs forwarded between the fixed lens and rotatable lenses of a multi-lens linkage camera. • **28**: ITGT (intelligent) module, involving ITGT (intelligent) logs. • **29**: ITGT (intelligent) module, involving debug logs of the ITGT algorithm. When the debug log function is enabled, metadata of the object detection frame can be sent to the web control. • **30**: GA/T 1400 module, involving logs of the GA/T 1400 protocol. • **31**: ISP Info module, involving info logs of the ISP module. • **32**: GAT1400_2 module, involving GA/T 1400-2 protocol logs. • **33**: DEBUG_MODEL_ISP_ENHANCE_ALG module, involving info logs of the enhanced algorithm of the ISP module. • **34**: DEBUG_MODEL_ISP_HOTCOLOR_ALG module, involving info logs of the thermal imaging algorithm of the ISP module. • **35**: DEBUG_MODEL_ISP_REDLIGHT_ALG module, involving info logs of the red light enhancement algorithm of the ISP module.

Parameter	Description	Value
		• **36**: DEBUG_MODEL_ISP_BLUR_ALG module, involving info logs of the BLUR algorithm of the ISP module. • **37**: DEBUG_MODEL_ISP_AE_ALG module, involving info logs of the AE algorithm of the ISP module. • **38**: DEBUG_MODEL_ISP_AF_ALG module, involving info logs of the AF algorithm of the ISP module. • **39**: DEBUG_MODEL_ISP_AWB_ALG module, involving info logs of the AWB algorithm of the ISP module. • **40**: DEBUG_MODEL_ISP_LIGHT_ALG module, involving info logs of the LIGHT algorithm of the ISP module. • **41**: DEBUG_MODEL_ISP_DN_ALG module, involving info logs of the DN algorithm of the ISP module. • **42**: STOP_ISP_ALL module, involving ISP module logs. • **43**: STOP_ISP_AE module, involving AE algorithm logs of the ISP module. • **44**: STOP_ISP_DN module, involving DN algorithm logs of the ISP module. • **45**: STOP_ISP_GAMMA module, involving GAMMA algorithm logs of the ISP module. • **46**: STOP_ISP_DRC module, involving DRC algorithm logs of the ISP module. • **47**: STOP_ISP_DIS module, involving DIS algorithm logs of the ISP module. • **48**: STOP_ISP_FOG module, involving FOG algorithm logs of the ISP module.

Parameter	Description	Value
		• **49**: STOP_ISP_BL module, involving BI algorithm logs of the ISP module. • **50**: STOP_ISP_SPEED module, involving SPEED algorithm logs of the ISP module. • **51**: STOP_ISP_SHARPEN module, involving SHARP algorithm logs of the ISP module. • **52**: STOP_ISP_NR_ module, involving NR algorithm logs of the ISP module. • **53**: STOP_ISP_AWB module, involving AWB algorithm logs of the ISP module. • **54** STOP_ISP_RLE_RED module, involving RLE algorithm logs of the ISP module. • **55**: STOP_ISP_LDC module, involving LDC algorithm logs of the ISP module. • **56**: ISP_FACE_ENHANCE module, involving FACE algorithm logs of the ISP module. • **57**: ISP_LP_ENHANCE module, involving lp_enhance algorithm logs of the ISP module. • **58**: ISP_TSDF_MODULE module, involving TSDF algorithm logs of the ISP module. • **59**: ISP_RAW_CAPENHANCE module, involving raw_enhance algorithm logs of the ISP module. • **60**: ISP_LP_COMTRAST module, involving lp_comtrast algorithm logs of the ISP module. • **61**: ISP_FACE_COMTRAST module, involving face_comtrast algorithm logs of the ISP module.

Parameter	Description	Value
		• **62**: ISP_DEPURPLE module, involving depurple algorithm logs of the ISP module. • **63**: ISP_UVADJUST module, involving uvadjust algorithm logs of the ISP module. • **64**: ISP_BRIGHT_EYE module, involving bright_eye algorithm logs of the ISP module. • **65**: ISP_AF_CURVE module, involving af_curve algorithm logs of the ISP module. • **66**: ISP_FUSION_UV module, involving fusion_uv algorithm logs of the ISP module. • **67**: ISP_FUSION_UV2 module, involving fusion_uv2 algorithm logs of the ISP module. • **68**: ISP_ONLINECALIB module, involving onlineCalib algorithm logs of the ISP module.

NOTE

- For details about log query and description, see the *Log Reference*.
- The debug log is automatically disabled in 10 minutes after the debug log is enabled.

Usage Guide

To enable the debug log function of the main control module, run the following command:

```
root#IPC:/usr/app/bin# ./help debug open 1
```

Parent topic: Log Commands

Media Stream Commands

- **./help setmediaopen**
- **./help getmedia**
- **./help setmediaclose**
- **./help mediadbgcntget**
- **./help mediadbgcntclear**
- **./help clear**

Parent topic: Command Description

./help setmediaopen

Function

The **./help setmediaopen** command is used to request media streams.

Format

./help setmediaopen [VideoStreamType] [ProtocolType] [IPAddress] [Port] [PacketType] [LocalEthNo]

Parameter Description

Parameter	Description	Value
VideoStreamType	Media stream type.	Value range: 0, 1, 2, 3, and 4 • **0**: primary stream • **1**: secondary stream 1 • **2**: secondary stream 2 • **3**: secondary stream 3 • **4**: secondary stream 4
ProtocolType	Protocol type.	Value range: 0 and 2 • **0**: UDP • **2**: multicast
IPAddress	IP address of the device that requests media streams.	-
Port	Port number of the device that requests media streams.	Value range: an integer ranging from 0 to 65535
PacketType	Type of the requested media stream.	Value range: 0 and 1

Parameter	Description	Value
		• **0**: elementary stream • **1**: program stream
LocalEthNo	Network adapter type.	Value range: 0 and 1 • **0**: eth0 • **1**: eth1

Usage Guide

Assume that the media stream type is primary stream, the protocol type is UDP, the IP address is 192.168.0.200, the port number is 10000, the media stream type is elementary stream, and the network adapter type is wired network adapter. In this case, to request media streams, run the following command:

```
root#IPC:/usr/app/bin# ./help setmediaopen 0 0 192.168.0.200 10000 0 0
```

Parent topic: Media Stream Commands

./help getmedia

Function

The **./help getmedia** command is used to query the ID of the requested media stream.

Format

./help getmedia

Parent topic: Media Stream Commands

./help setmediaclose

Function

The **./help setmediaclose** command is used to disable requested media streams.

Format

./help setmediaclose [SessionID]

Parameter Description

Parameter	Description	Value
SessionID	ID of the requested media stream.	-

Usage Guide

To disable media streams requested from the device with the IP address 192.168.0.200, run the following command:

```
root@IPC:/usr/app/bin# ./help setmediaclose 2
```

Parent topic: Media Stream Commands

./help mediadbgcntget

Function

The **./help mediadbgcntget** command is used to query the statistics of the media module.

Format

./help mediadbgcntget

Parent topic: Media Stream Commands

./help mediadbgcntclear

Function

The **./help mediadbgcntclear** command is used to clear the statistics of the media module.

Format

./help mediadbgcntclear

Parent topic: Media Stream Commands

./help clear

Function

The **./help clear** command is used to delete all requested media streams.

Format

./help clear

Parent topic: Media Stream Commands

System Commands

- ./help setsystemuserlock
- ./help getsystemuserlock
- ./help getdevicetime
- ./help getptzlocation
- ./help getnetworkinfo
- ./help getdot1xstatus
- ./help getrecordtaskstatus
- ./help getdriverinfo
- ./help getptzpresetlist
- ./help getclientloginstatus
- ./help devicerestore
- ./help getplatstreaminfo
- ./help getptzstatus
- ./help setaeskey
- ./help getlswportstatus
- ./help getiPCAstatlist
- ./help setethmode
- ./help getnetrxlimit
- ./help ipv6
- ./help openRCdebug
- ./help setdaemon
- ./help setmultinet
- ./help setsdmspwd

./help setfastbootmode

./help getdeviceaccessinfo

./help get1400status

./help get1400_2status

./help get28181status

./help get28181_2status

Parent topic: Command Description

./help setsystemuserlock

Function

The **./help setsystemuserlock** command is used to set the maximum number of consecutive incorrect password inputs and the account lockup duration.

> **NOTE**
>
> Users in this document refer to the **admin** and **root** users who have logged in to the Linux operating system through SSH.

Format

./help setsystemuserlock [ErrorNumber] [LockTime]

Parameters

Parameter	Description	Value
ErrorNumber	Maximum number of consecutive incorrect password inputs.	Value range: 1 to 99
LockTime	Account lockup duration.	Value range: 1 to 999, in minutes.

Usage Guidelines

To set the maximum number of consecutive incorrect password inputs to 10 and the account lockup duration to 30 minutes, run the following command:

```
root@IPC:/usr/app/bin# ./help setsystemuserlock 10 30
```

Parent topic: System Commands

./help getsystemuserlock

Function

The **./help getsystemuserlock** command is used to query the maximum number of consecutive incorrect password inputs and the account lockup duration.

> **NOTE**
>
> Users in this document refer to the **admin** and **root** users who have logged in to the Linux operating system through SSH.

Format

./help getsystemuserlock

Parent topic: System Commands

./help getdevicetime

Function

The **./help getdevicetime** command is used to query the start time and duration of device running.

Format

./help getdevicetime

Parent topic: System Commands

./help getptzlocation

Function

The **./help getptzlocation** command is used to query the current position of the PTZ.

Format

./help getptzlocation

Parent topic: System Commands

./help getnetworkinfo

Function

The **./help getnetworkinfo** command is used to query network adapter information, duplex mode, and network rate.

Format

./help **getnetworkinfo [EthIndex]**

Parameter Description

Parameter	Description	Value
[EthIndex]	Network adapter ID.	Value range: 0 and 1 • **0**: eth0 • **1**: eth1

Parent topic: System Commands

./help getdot1xstatus

Function

The **./help getdot1xstatus** command is used to query the 802.1X authentication status.

Format

./help getdot1xstatus [InterfaceIndex]

Parameter Description

Parameter	Description	Value
[InterfaceIndex]	ID of a network adapter.	The value can be **0** or **1**.

Usage Guide

To query the 802.1X authentication status, run the following command:

```
root@IPC:/usr/app/bin# ./help getdot1xstatus 1

================================================
Authentication Status: DISCONNECTED
```

Parent topic: System Commands

./help getrecordtaskstatus

Function

The **./help getrecordtaskstatus** command is used to query the SD card recording status.

Format

./help getrecordtaskstatus

Parent topic: System Commands

./help getdriverinfo

Function

The **./help getdriverinfo** command is used to query device information.

Format

./help getdriverinfo [Module]

Parameter Description

Parameter	Description	Value
[Module]	Device information to be queried.	The value ranges from 0 to 10. • **0**: ISP parameter • **1**: AF • **2**: AUDIO • **3**: DFT • **4**: DIS • **5**: NET • **6**: VIM • **7**: VIDEO • **8**: PTZ • **9**: REGION • **10**: MISC

Usage Guide

To query the ISP parameters of the device, run the following command:

```
root@IPC:/usr/app/bin# ./help getdriverinfo 0

================================Driver ISP Info====================
IRCutMode 1, nIris:  0, ZoomPos: 100, FocusPos: 2604
```

Parent topic: System Commands

./help getptzpresetlist

Function

The **./help getptzpresetlist** command is used to query the preset position list.

Format

./help getptzpresetlist

Parent topic: System Commands

./help getclientloginstatus

Function

The **./help getclientloginstatus** command is used to query status of the web client and SDK client.

Format

./help getclientloginstatus

Parent topic: System Commands

./help deviceresto re

Function

The **./help deviceresto re** command is used to reset a device. After this command is executed, the device will restart.

Format

./help deviceresto re [mode]

Parameter Description

Parameter	Description	Value
mode	Method for resetting a device.	The value can be **0** or **1**. • **0**: Restores all the device settings except for the IP address. • **1**: Restores all the device settings including the IP address.

Usage Guide

To restore the device to factory defaults, run the following command:

```
root@IPC:/usr/app/bin# ./help deviceresto re 1
```

Parent topic: System Commands

./help getplatstreaminfo

Function

The **./help getplatstreaminfo** command is used to query the number of connected platforms and the disconnection time. If a platform is disconnected, the camera automatically enables video buffering.

Format

./help getplatstreaminfo

Parameter Description

None

Usage Guide

To query the number of connected platforms and the disconnection time, run the following command:

```
root@IPC:/usr/app/bin# ./help getplatstreaminfo

================================================================================
Index   IP                ConnectedCount         DisconnectedTime
1     192.168.135.2          2                   0Days 0h 0m 0s
2     192.168.135.3          0                   0Days 0h 3m 36s
```

NOTE

In the preceding information, **IP** indicates the IP address of the connected platform, **ConnectedCount** indicates the number of connected platforms, and **DisconnectedTime** indicates the disconnection time.

Parent topic: System Commands

./help getptzstatus

Function

The **./help getptzstatus** command is used to query the PTZ device status.

Format

./help getptzstatus

Parameter Description

Parameter	Description	Value
"X"	PTZ device status.	• **0**: idle • **1**: rotating • **2**: rotating to a preset position • **3**: zooming • **4**: focusing • **5**: adjusting the aperture • **6**: performing 3D positioning • **7**: performing quick locating • **8**: touring • **9**: performing vertical scanning • **10**: performing horizontal scanning • **11**: performing vertical limit

Parameter	Description	Value
		scanning • **12**: performing horizontal limit scanning • **13**: performing pattern scanning • **14**: performing frame scanning • **15**: performing panorama scanning • **16**: performing random scanning

Usage Guide

To query the current PTZ device status, run the following command:

```
root@IPC:/usr/app/bin# ./help getptzstatus

================================================
Ptz Current Status: X
================================================
```

The value of *X* is an integer ranging from 0 to 16.

Parent topic: System Commands

./help setaeskey

Function

The **./help setaeskey** command is used to change the working key of a user. You are advised to change the working key periodically.

Format

help setaeskey [Module]

Parameter Description

Parameter	Description	Value
Module	Module ID.	• **0**: WEB • **1**: ONVIF • **2**: GB/T 28181 • **3**: CA • **4**: 802.1X • **5**: SNMP • **7**: SDK • **8**: FTP • **15**: FACE_REC • **16**: GB35114 • **17**: SLAVE_ONVIF_CLIENT • **18**: SLAVE_RTSP_CLIENT • **19**: HIDS_SECRET_KEY • **20**: REST • **21**: MASTER_SLAVE • **22**: GAT1400 • **23**: SDMS • **27**: PPPoE • **29**: SZJJ

Parameter	Description	Value
		• **31**: STORAGE
Key	Key and database password.	The value is automatically generated by the system and does not need to be entered manually.

Usage Guide

Example: The system automatically generates a working key and encrypts the web password.

```
root@IPC:/usr/app/bin# ./help setaeskey 0
```

Parent topic: System Commands

./help getlswportstatus

Function

The **./help getlswportstatus** command is used to query the status of network ports and optical ports.

> **NOTE**
>
> This command applies to devices that support both network ports and optical ports.

Format

./help getlswportstatus [PortIndex]

Parameter Description

Parameter	Description	Value
[PortIndex]	Number of the network port, optical port, or electrical port.	Value range: 0, 1, and 2 For a device with dual network ports (two IP addresses externally): • **0**: ETH0_PORT • **1**: ETH1_PORT • **2**: SFP_PORT For a device without dual network ports, the options are as follows: • **0**: ETH0_PORT • **1**: SFP_PORT For a device with dual network ports (one IP address externally):

Parameter	Description	Value
		• **0**: ETH0_PORT • **1**: SFP_PORT/ET_PORT IFHAVE

Usage Guide

Example: Set the network port to **100M FULL**.

```
root@IPC:/usr/app/bin# ./help getlswportstatus 1
Mode:Full Duplex
Speed:100M
```

NOTE

Run the command according to the actual device. If the device does not support the query of the corresponding ports, the message "Unsupport Mode!" is displayed.

Parent topic: System Commands

./help getiPCAstatlist

Function

The **./help getiPCAstatlist** command is used to query the current statistics of the Packet Conservation Algorithm for Internet (iPCA), including the sent packet data and address data.

Format

./help getiPCAstatlist

Parameter Description

None

Usage Guide

To query the iPCA information, run the following command:

```
root@IPC:/usr/app/bin# ./help getiPCAstatlist

=============================================================================================
Index   PeriodNum   SrcIP:Port         DstIP:Port          ProtolType   ullPkts   ullBytes
1       1447256526  192.168.135.2:2000 192.168.135.30:10000    UDP       5675       5675
```

NOTE

In the preceding command, **PeriodNum** indicates the current period number, **SrcIP:Port** indicates the local IP address and port number, **DstIP:Port** indicates the destination IP address and port number, **ullPkts** indicates the number of transmitted data packets, and **ullBytes** indicates the number of transmitted bytes.

Parent topic: System Commands

./help setethmode

Function

The **./help setethmode** command is used to set the network port mode.

Format

./help **setethmode [EthIndex] [mode]**

Parameter Description

Parameter	Description	Value
[EthIndex]	Network adapter ID.	Value range: 0 and 1 • **0**: eth0 • **1**: eth1
[mode]	Network port mode.	Value range: 0, 1, 2, 3, and 4 • **0**: AUTO • **1**: 10M FULL • **2**: 10M HALF • **3**: 100M FULL • **4**: 100M HALF

Usage Guide

Example: To set the network port to **100M FULL**, run the following command:

```
root@IPC:/usr/app/bin# ./help setethmode 1 3
```

Parent topic: System Commands

./help getnetrxlimit

Function

The **./help getnetrxlimit** command is used to obtain the receive rate limit of the network port.

Format

./help **getnetrxlimit**

Parameter Description

None

Usage Guide

```
root@IPC:/usr/app/bin# ./help getnetrxlimit

================================Driver PacketRatio Info=================================
PacketRatio 6000
========================================================================================
```

Parent topic: System Commands

./help ipv6

Function

The **./help ipv6** command is used to enable or disable the IPv6 service.

Format

- Enabling the IPv6 service: ./help ipv6 open
- Disabling the IPv6 service: ./help ipv6 close

Parent topic: System Commands

./help openRCdebug

Function

The **./help openRCdebug** command is used to enable the debug log function for the RTSP Client process.

Format

./help openRCdebug

Parent topic: System Commands

./help setdaemon

Function

The **./help setdaemon** command is used to manually set the status of a service process.

Format

./help setdaemon [0,1] [ProcessNmae]

Parameter Description

Parameter	Description	Value
0,1	Status.	• **0**: disable • **1**: enable
ProcessNmae	Process name.	Example: itgt

Parent topic: System Commands

./help setmultinet

Function

The **./help setmultinet** command is used to manually enable or disable the dual network adapters of a dual-network-adapter device.

Format

./help setmultinet [0,1]

Parameter Description

Parameter	Description	Value
0,1	Status.	• **0**: disable • **1**: enable

Parent topic: System Commands

./help setsdmspwd

Function

The **./help setsdmspwd** command is used to set the password for logging in to the rotatable lens of a compound-eye camera from the fixed lens.

Format

./help setsdmspwd [ChannelID]

Parameter Description

Parameter	Description	Value
ChannelID	Channel ID.	• **1**: rotatable lens 1 • **2**: rotatable lens 2

Set the password as prompted.

Parent topic: System Commands

./help setfastbootmode

Function

The **./help setfastbootmode** command is used to set whether to enable quick startup for a secondary camera. The LiteOS+Linux system is used when quick startup is enabled. The Linux system is used when quick startup is not enabled.

Format

./help setfastbootmode [mode]

Parameter Description

Parameter	Description	Value
[mode]	Indicates whether to enable quick startup.	The options are as follows: • **0**: Not Fastboot Mode • **1**: Fastboot Mode

Usage Guide

To enable quick startup for a secondary camera, run the following command:

```
root@IPC:/usr/app/bin# ./help setfastbootmode 1
```

Parent topic: System Commands

./help getdeviceaccessinfo

Function

The **./help getdeviceaccessinfo** command is used to obtain settings of platform connection parameters.

Format

./help getdeviceaccessinfo [SsType]

Parameter Description

Parameter	Description	Value
[SsType]	Protocol used to connect to a platform.	The options are as follows: • **1**: SDK (active registration) • **4**: GB/T 28181 • **6**: GB/T 28181_2

Parent topic: System Commands

./help get1400status

Function

The **./help get1400status** command is used to query the status of the GA/T 1400-compliant platform 1.

Format

./help get1400status

Usage Guide

```
root@IPC:/usr/app/bin# ./help get1400status
1400 status is online
```

Parent topic: System Commands

./help get1400_2status

Function

The **./help get1400_2status** command is used to query the status of the GA/T 1400-compliant platform 2.

Format

./help get1400_2status

Usage Guide

```
root@IPC:/usr/app/bin# ./help get1400_2status
1400_2 status is offline
```

Parent topic: System Commands

./help get28181status

Function

The **./help get28181status** command is used to query the status (online or offline) of GB/T 28181-compliant platform 1.

Format

./help get28181status

Usage Guide

```
root@IPC:/usr/app/bin# ./help get28181status
28181 status is online
```

Parent topic: System Commands

./help get28181_2status

Function

The **./help get28181_2status** command is used to query the status (online or offline) of GB/T 28181-compliant platform 2.

Format

./help get28181_2status

Usage Guide

```
root@IPC:/usr/app/bin# ./help get28181_2status
28181_2 status is offline
```

Parent topic: System Commands

Appendix

The system contains the following directories:

- /usr/app/tools
- /usr/bin
- /usr/sbin
- /bin
- /sbin

Common Linux Commands

Busybox Command

Open-Source Software Commands

Driver-related Commands

Other Commands

Changing the System Password

Parent topic: Command Reference

Common Linux Commands

Command	Description
udevd	For details about how to use these commands, run the *command* **-help** command. In the preceding command, *command* indicates a specific command.
udevadm	
mkfs.xfs	
xfs_repair	
mkfs.ext4	
fsck.ext4	
sh	
lsof	
lzcat	
mkfx.ext4	

Parent topic: Appendix

Busybox Command

For details about the **Busybox** commands, see http://www.busybox.net/downloads/BusyBox.html.

Other **Busybox** commands include **halt**, **lzma**, **poweroff**, **ubiattach**, **ubidetach**, **ubimkvol**, **ubiupdatevol**, **unxz**, and **xz**.

Parent topic: Appendix

Open-Source Software Commands

Table 1 Open-source software commands

Software	Command	Usage
cpulimit	cpulimit	For details about how to use the command, run the *command* **-help** command. In the preceding command, *command* indicates a specific command.
iptables	iptables	
iproute2 - Linux Foundation	tc	
NTP - The Network Time Protocol	ntpdate	
sudo	sudo	
ssh	ssh	
sshd	sshd	
ssh-keygen	ssh-keygen	
udevd	udevd	
	udevadm	
sftp	sftp	For details about how to use the command, run the *command* **-help** command. In the preceding command, *command* indicates a specific command.
sftpd	sftpd	

Parent topic: Appendix

Driver-related Commands

Type	Command	Description
Kernel-driven loading	LoadExko	Run the **cd /usr/app/tools** command in the **tools** directory. For details about how to use the command, run the *command* **-help** command. In the preceding command, *command* indicates a specific command.

Type	Command	Description

Type	Command	Description

Type	Command	Description

Type	Command	Description
RTC system time update	updatetime	
Restart log recording	rebootInfo	
ARP update	SendArp	
MCU upgrade	mcu_update	
Verifying the upgrade package integrity	cmscheck	
Creating a memory file system	CreateMemfileSystem	
Model information initialization	DeviceTypeTools	
Kernel exception information collection	kbox_dumptool	
FPGA loading	fpga_load	
Boot and kernel startup backup	ubootbackup	
Switching the boot partition	setbootpart	
IP module setting	Netsetting	

Type	Command	Description
High-end memory partition creation	CreatMemfileSystem	
This command is invoked during startup to update the ARP routing table.	arp	
Repairing the SD card	fsck.ext4	
Chip firmware	m7_app.bin	
MCU firmware of the STM32F103 model	mcu_app.bin	
MCU firmware of the GD32F303 model	mcu_app_gd.bin	
MCU firmware of the GD32E103 model	mcu_app_gd103.bin	
MCU firmware of	mcu_app_gd303_expand.bin	

Type	Command	Description
the GD32F303 model		
MCU firmware of the STM32F030 model	mcu_app_st030.bin	
MCU firmware version of the STM32F103 model	mcu_ver	
MCU firmware version of the GD32F303 model	mcu_ver_gd	
MCU firmware version of the GD32E103 model	mcu_ver_gd103	
MCU firmware version of the GD32F303 model	mcu_ver_gd303_expand	
MCU firmware	mcu_ver_st030	

Type	Command	Description
version of the STM32F030 model		
Formatting the SD card	mkfs.ext4	
Collecting network fault information	net_log_collect	
Generating the SSH key	ssh-keygen	
Allowing non-root users to run the **root** command temporarily	sudo	
Traffic control by using the traffic shaping function	tc	
FPGA logic firmware	SDC_fpga_firmware.bin	
FPGA logic firmware of the device with an IMX265 sensor	elt113_top_IMX265.bin	

Type	Command	Description
FPGA logic firmware of the device with an IMX305 sensor	elt113_top_IMX305.bin	
Security file verification and device security status query	cipher	You can run the **cipher** command directly. For details about how to use the command, run the *command* **-help** command. In the preceding command, *command* indicates a specific command.
Manual upgrade	update	1. Run the following command: **update -f** *absolute path of the version upgrade package* **NOTE:** • Before running the **update** command, ensure that the version software upgrade package is correct. Otherwise, the device may break down. Exercise caution when performing this operation. You are advised to run the **sdc_update** command to

Type	Command	Description
		perform the upgrade. • For security purposes, the size of the file to be transferred is limited. If the size of the current upgrade package exceeds 5 MB, run the **umount /home/sftp_admin/** command in the SSH background to remove the limit on the file size after closing the SFTP page. • You can run the **update -help** command to obtain the method of using the **update** command. 2. After the upgrade is complete and the device automatically restarts, run the **cd /usr/app/bin** command to go to the **bin** directory, and run the **cat version** command to check the current version number to confirm whether the upgrade succeeds.

- The **sdc_update** command exists in the **/sbin** directory. Both the **sdc_update** command and the **update** command in **/usr/app/tools** can be used to upgrade the software package. When the **sdc_update** command is executed, the system verifies the model and security of the upgrade package. You are advised to use the **sdc_update** command when upgrading the version software package.

    1. Run the **cd /sbin** command.
    2. Run the following command: **sdc_update -f** *absolute path of the upgrade package*
    3. After the upgrade is complete and the device automatically restarts, run the **cd /usr/app/bin** command to go to the **bin** directory, and run the **cat version** command to check the current version number to confirm whether the upgrade succeeds.

- For a multi-chip camera, if the primary and secondary chips need to be upgraded at the same time, run the **sdc_update pdd_upg_master -f** *absolution path of the upgrade package* command. If only the primary chip needs to be upgraded, run the **sdc_update pdd_upg_master -f** *absolution path of the upgrade package*-**m** command.

NOTE

For eMMC camera models, the software package must be stored in the **/usr/upgrade/** directory. Otherwise, the memory space may be insufficient.

Run the **cat /proc/cmdline** command. If "storage=emmc" is returned, the current device supports eMMC.

Parent topic: Appendix

Other Commands

Other related commands include **dropbear**, **dropbearkey**, **kox_dumptool**, **pppd**, **pppoe**, **pppoe-connect**, **pppoe-init**, **pppoe-start**, **pppoe-status**, **pppoe-stop**, **rsaverify**, **startapp.sh**, **summarylist.txt**, **daemon**, **reboot**, and **ip**.

Parent topic: Appendix

Changing the System Password

This section describes how to change the passwords of the **admin** and **root** users after the device is installed to ensure system security.

NOTICE

If the **admin** or **root** user's password is incorrectly entered for 53 consecutive times, the user account will be locked for 35 minutes.

- Do not attempt to log in to the system during the lockout duration. Otherwise, the lockout duration will be cleared and start over.

1. Log in to the Linux operating system as the **admin** user.

   NOTE

   - The default IP address is 192.168.0.120.
   - To change the password of the **root** user, you need to run the **su - root** command to switch to the **root** user.
   - You can use the SSH protocol to log in. You are advised to use the remote login tool to log in.
   - For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following characters: digits, letters, and special characters.

2. Run the **passwd** command to change the operating system password.

   Enter the new password as prompted. The following information is displayed:

```
admin@IPC:~$ passwd
Changing password for admin
Authentication passwordOld password:
Enter the new password (minimum of 6 characters)
Please use a combination of at least two types of characters
upper or lower case letters or numbers or special characters
New password:
```

```
Retype password:
Password changed Successfully
```

3. Exit the operating system.

Parent topic: Appendix

Alarm Reference

- **Camera Alarms**
- **Camera Event Alarms**

Parent topic: Reference

Camera Alarms

- ALARM_TYPE_NETWORK_INTERRUPT Network Disconnection
- ALARM_TYPE_TEMPERATURE Temperature Alarm
- ALARM_TYPE_MEDIA_INTERRUPT Media Stream Interruption
- ALARM_TYPE_DEV_TEMPE Temperature Chip Error
- ALARM_TYPE_LOG_WR Log Read and Write Alarm
- ALARM_TYPE_FAN_PWR_BLOCKED Power Board Fan Abnormality
- ALARM_TYPE_FAN_HEC_BLOCKED Encoding Board Fan Abnormality
- ALARM_TYPE_SFP_TEMP_HIGH Too High Optical Module Temperature
- ALARM_TYPE_SFP_TEMP_LOW Too Low Optical Module Temperature
- ALARM_TYPE_SFP_VOL_HIGH Too High Optical Module Voltage
- ALARM_TYPE_SFP_VOL_LOW Too Low Optical Module Voltage
- ALARM_TYPE_SFP_BIAS_HIGH Too High Optical Module Bias Current
- ALARM_TYPE_SFP_BIAS_LOW Too Low Optical Module Bias Current
- ALARM_TYPE_SFP_TX_PWR_HIGH Too High Optical Module Transmit Power
- ALARM_TYPE_SFP_TX_PWR_LOW Too Low Optical Module Transmit Power

ALARM_TYPE_SFP_RX_PWR_HIGH Too High Optical Module Receive Power

ALARM_TYPE_SFP_RX_PWR_LOW Too Low Optical Module Receive Power

ALARM_TYPE_SFP_LASER_TEMP_HIGH Too High Optical Module Laser Temperature

ALARM_TYPE_SFP_LASER_TEMP_LOW Too Low Optical Module Laser Temperature

ALARM_TYPE_SFP_TEC_CURRENT_HIGH Too High Optical Module TEC Current

ALARM_TYPE_SFP_TEC_CURRENT_LOW Too Low Optical Module TEC Current

ALARM_TYPE_LIGHT_SENSOR_INCVALID Ambient Light Sensor Failure

PTOPT_FAILURE_ALARM Optocoupler Error

ALARM_TYPE_EXTERNAL_POWER_DOWN Power-off of External Power Supply

ALARM_TYPE_WIPER_FAILURE_ALARM Wiper Failure

ALARM_TYPE_MEM_HIGHT High Memory Usage

ALARM_TYPE_HTTPS_CERT_EXPIRE HTTPS Certificate Expiration

ALARM_TYPE_HTTPS_CERT_WILL_EXPIRE HTTPS Certificate About to Expire

ALARM_TYPE_DOX_CERT_EXPIRE 802.1X Certificate Expiration

ALARM_TYPE_DOX_CERT_WILL_EXPIRE 802.1X Certificate About to Expire

ALARM_TYPE_SDK_PWD_STILL_INITIAL_PWD SDK Password Unchanged

ALARM_TYPE_DISK_EXCEPTION SD Card Fault

ALARM_TYPE_NO_SIGNAL Video Signal Loss

ALARM_TYPE_ATTITUDE_CHANGE_ALARM Camera Angle Abnormality Alarm

ALARM_TYPE_ITS_RADAR_EXCEPTION_ALARM ITS Radar Exception

ALARM_TYPE_ITS_IOCOIL_EXCEPTION_ALARM ITS I/O Loop Exception

ALARM_TYPE_ITS_485COIL_EXCEPTION_ALARM ITS RS-485 Loop Exception

ALARM_TYPE_ITS_REDTOR_EXCEPTION_ALARM ITS Traffic Light Detector Exception

ALARM_TYPE_LENS_FAILURE_ALARM Lens PT Optocoupler Failure

ALARM_TYPE_WEB_PWD_EXPIRE Web Password Expiration

ALARM_TYPE_DISK_FULL Full Disk

ALARM_TYPE_DISK_FAULT Disk Fault

ALARM_TYPE_DISK_FAIL Disk Read/Write Failure

ALARM_TYPE_DISC_PULL_OUT Disk Removal

Parent topic: Alarm Reference

ALARM_TYPE_NETWORK_INTERRUPT Network Disconnection

Description

This alarm is generated when the network is disconnected.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_NETWORK_INTERRUPT = 7	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the network is disconnected.
Device log	The device log records "Network Outage Alarm", indicating the network disconnection alarm.

Impact on the System

The network communication of the device is affected, which then affects the live video viewing and recording functions.

Possible Causes

- The signal quality of the network link is poor.
- The link device is faulty.
- The network cable connector is loose or the network cable is damaged.

- An internal component of the camera is faulty.

Solution

1. Check whether an exception occurs on the network where the camera is located. For example, check whether the communication of the link device or other devices on the same network is faulty.
    - If yes, go to Step 2.
    - If no, go to Step 4.
2. Check whether an exception occurs on the external network. For example, check whether the upper-layer switch is faulty or whether the network is attacked.
    - If yes, go to Step 3.
    - If no, go to Step 4.
3. Rectify the network fault and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 4.
4. Remove the network cable from the camera, and then re-insert it tightly. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 5
5. Replace the network cable and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 6.

6. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

After the network fault is rectified, the alarm is cleared automatically.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_TEMPERATURE Temperature Alarm

Description

This alarm is generated when the device temperature is too high or too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_TEMPERATURE = 9	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the device temperature is too high or too low.
Device log	The device log records "Temperature Alarm. Temperature:xxx °c", indicating the temperature alarm generation and specific temperature.

Impact on the System

The device may crash.

Possible Causes

- The temperature in the operating environment is too high or too low.

- An internal component, for example, a fan, of the camera is faulty.

Solution

1. Check whether the alarm is caused by a too high or too low ambient temperature by observing onsite or viewing logs.
   - If the temperature is too high, go to Step 2.
   - If the temperature is too low, go to Step 3.
2. If an alarm is generated due to a too high operating temperature, perform the following steps:
   a. Check whether the operating environment meets the installation requirements specified in Installation Requirements. For example, check whether there are other devices that affect the air temperature and whether a sun shield is installed on the device.
      - If the operating environment does not meet the installation requirements, go to 2.
      - If the operating environment meets the installation requirements, go to 3.
   b. Take necessary heat isolation and cooling measures or change the installation environment. Then, check whether the alarm is cleared.
      - If yes, no further action is required.
      - If no, go to 3.
   c. Check whether a fan abnormality alarm is generated.
      - If yes, go to 4.
      - If no, go to 5.

d. Refer to ALARM_TYPE_FAN_PWR_BLOCKED Power Board Fan Abnormality and ALARM_TYPE_FAN_HEC_BLOCKED Encoding Board Fan Abnormality to handle the alarm. Then, check whether the alarm is cleared.

   - If yes, no further action is required.
   - If no, go to 5.

e. Power off the device, wait for 10 minutes, and then power on the device. After the device runs for a period of time, check whether the alarm is cleared.

   - If yes, no further action is required.
   - If no, contact technical support engineers for assistance.

3. If the alarm is generated due to a too low temperature, contact technical support engineers for assistance.

Alarm Clearance

When the device temperature is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_MEDIA_INTERRUPT Media Stream Interruption

Description

This alarm is generated when media streams are interrupted.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_MEDIA_INTERRUPT	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when media streams are interrupted.

Impact on the System

The device's media functions are affected, especially the live video viewing and recording functions.

Possible Causes

- The network is faulty.
- The device's lens is damaged.

Solution

1. Check whether other devices on the same network encounter the same fault and whether the network where the camera is located is faulty.
    - If yes, go to Step 2.

- If no, go to Step 3.

2. Rectify the network fault and check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, go to Step 3.
3. Check whether the lens of the device is physically damaged.
   - If yes, go to Step 4.
   - If no, contact technical support engineers for assistance.
4. Replace the lens or the device, and check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, contact technical support engineers for assistance.

Alarm Clearance

After the media streams are recovered, the alarm is cleared automatically.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_DEV_TEMPE Temperature Chip Error

Description

This alarm is generated when a temperature chip error occurs.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DEV_TEMPE	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when a temperature chip error occurs.
Device log	The device log records "Temperature chip Err Alarm", indicating a temperature chip error alarm.

Impact on the System

The temperature module functions are affected.

Possible Causes

- The temperature chip fails.
- The bus is in abnormal work state.

Solution

1. Check whether there are obvious falling and collision traces on the device. Falling and collision may result in board or chip damage.
    - If yes, contact technical support engineers for assistance.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the temperature chip is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_LOG_WR Log Read and Write Alarm

Description

This alarm is generated when a log read and write error occurs.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LOG_WR	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when a log read and write error occurs.
Device log	The device log records "LOG Read and write Alarm", indicating a log read and write alarm.

Impact on the System

The system logs are affected.

Possible Causes

- The camera logs fail to be backed up.
- The flash chip is damaged.

Solution

Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the log read and write functions are recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_FAN_PWR_BLOCKED Power Board Fan Abnormality

Description

This alarm is generated when an internal fan is faulty.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FAN_PWR_BLOCKED = 38	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the power board fan is faulty.
Device log	The device log records "Pwr Fan Blocked Alarm", indicating a power board fan blocking alarm.

Impact on the System

The power board stability is affected.

Possible Causes

- The fan is damaged.
- The power board of the device is faulty.

Solution

1. Check whether there are obvious falling and collision traces on the device. Falling and collision may result in internal component damage.
    - If yes, contact technical support engineers for assistance.
    - If no, go to Step 2.
2. Power off and then power on the device and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the power board fan is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_FAN_HEC_BLOCKED Encoding Board Fan Abnormality

Description

This alarm is generated when an internal fan is faulty.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FAN_HEC_BLOCKED = 39	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the encoding board fan is faulty.
Device log	The device log records "Hec Fan Blocked Alarm", indicating an encoding board fan blocking alarm.

Impact on the System

The encoding board stability is affected.

Possible Causes

- The fan is damaged.
- The encoding board of the device is faulty.

Solution

1. Check whether there are obvious falling and collision traces on the device. Falling and collision may result in internal component damage.
    - If yes, contact technical support engineers for assistance.
    - If no, go to Step 2.
2. Power off and then power on the device and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the encoding board fan is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TEMP_HIGH Too High Optical Module Temperature

Description

This alarm is generated when the optical module temperature is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TEMP_HIGH = 40	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module temperature is too high.
Device log	The device log records "Optical Module Temperature High Alarm", indicating a too high optical module temperature alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The external environment temperature is too high.

- An internal component of the camera is faulty.
- The optical module is faulty.

Solution

1. Check whether the ambient temperature of the camera is too high or whether any other device that affects the environment temperature exists.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Take necessary heat isolation and cooling measures or change the installation environment. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Remove the optical module. When the optical module temperature decreases, insert it again and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 4.
4. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module temperature is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TEMP_LOW Too Low Optical Module Temperature

Description

This alarm is generated when the optical module temperature is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TEMP_LOW = 41	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module temperature is too low.
Device log	The device log records "Optical Module Temperature Low Alarm", indicating a too low optical module temperature alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The external environment temperature is too low.

- An internal component of the camera is faulty.
- The optical module is faulty.

Solution

1. Check whether the ambient temperature of the camera is too low.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Take necessary heat preservation measures or change the installation environment. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module temperature is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_VOL_HIGH Too High Optical Module Voltage

Description

This alarm is generated when the optical module voltage is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_VOL_HIGH = 42	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module voltage is too high.
Device log	The device log records "Optical Module Voltage High Alarm", indicating a too high optical module voltage alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.
- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module voltage is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_VOL_LOW Too Low Optical Module Voltage

Description

This alarm is generated when the optical module voltage is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_VOL_LOW = 43	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module voltage is too low.
Device log	The device log records "Optical Module Voltage Low Alarm", indicating a too low optical module voltage alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.
- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module voltage is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_BIAS_HIGH Too High Optical Module Bias Current

Description

This alarm is generated when the optical module bias current is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_BIAS_HIGH = 44	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module bias current is too high.
Device log	The device log records "Optical Module BIAS High Alarm", indicating a too high optical module bias current alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.

- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module bias current is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_BIAS_LOW Too Low Optical Module Bias Current

Description

This alarm is generated when the optical module bias current is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_BIAS_LOW = 45	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module bias current is too low.
Device log	The device log records "Optical Module BIAS Low Alarm", indicating a too low optical module bias current alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.

- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module bias current is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TX_PWR_HIGH Too High Optical Module Transmit Power

Description

This alarm is generated when the optical module transmit power is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TX_PWR_HIGH = 46	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module transmit power is too high.
Device log	The device log records "Optical Module Sending Power High Alarm", indicating a too high optical module transmit power alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The attenuation of the optical module is too low.

- The camera is faulty.

Solution

Increase the attenuation and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module transmit power is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TX_PWR_LOW Too Low Optical Module Transmit Power

Description

This alarm is generated when the optical module transmit power is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TX_PWR_LOW = 47	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module transmit power is too low.
Device log	The device records "Optical Module Sending Low Alarm", indicating a too low optical module transmit power alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The attenuation of the optical module is too high.

- The camera is faulty.

Solution

Decrease the attenuation and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module transmit power is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_RX_PWR_HIGH Too High Optical Module Receive Power

Description

This alarm is generated when the optical module receive power is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_RX_PWR_HIGH = 48	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module receive power is too high.
Device log	The device log records "Optical Module Receiving Power High Alarm", indicating a too high optical module receive power alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The attenuation of the optical module is too low.
- The camera is faulty.

Solution

Increase the attenuation and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module receive power is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_RX_PWR_LOW Too Low Optical Module Receive Power

Description

This alarm is generated when the optical module receive power is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_RX_PWR_LOW = 49	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module receive power is too low.
Device log	The device log records "Optical Module Receiving Power Low Alarm", indicating a too low optical module receive power alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The attenuation of the optical module is too high.

- The camera is faulty.

Solution

Decrease the attenuation and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module receive power is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_LASER_TEMP_HIGH Too High Optical Module Laser Temperature

Description

This alarm is generated when the optical module laser temperature is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_LASER_TEMP_HIGH = 50	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module laser temperature is too high.
Device log	The device log records "Optical Module LASER Temperature High Alarm", indicating a too high optical module laser temperature alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The temperature of the optical module is too high due to a variety of causes, for example, too high operating temperature of the camera.
- The camera is faulty.

Solution

1. Check whether the ambient temperature of the camera is too high or whether any other device that affects the environment temperature exists.
    - If yes, go to Step 2.
    - If no, contact technical support engineers for assistance.
2. Take necessary heat insulation measures or change the installation environment to decrease the temperature of the device and the optical module to the normal range. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module laser temperature is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_LASER_TEMP_LOW Too Low Optical Module Laser Temperature

Description

This alarm is generated when the optical module laser temperature is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_LASER_TEMP_LOW = 51	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module laser temperature is too low.
Device log	The device log records "Optical Module LASER Temperature Low Alarm", indicating a too low optical module laser temperature alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The temperature of the optical module is too low due to a variety of causes, for example, too low operating temperature of the camera.
- The camera is faulty.

Solution

1. Check whether the ambient temperature of the camera is too low.
    - If yes, go to Step 2.
    - If no, contact technical support engineers for assistance.
2. Take necessary heat preservation measures or change the installation environment to increase the temperature of the device and the optical module to the normal range. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module laser temperature is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TEC_CURRENT_HIGH Too High Optical Module TEC Current

Description

This alarm is generated when the optical module TEC current is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TEC_CURRENT_HIGH = 52	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module TEC current is too high.
Device log	The device log records "Optical Module TEC Current High Alarm", indicating a too high optical module TEC current alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.

- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module TEC current is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SFP_TEC_CURRENT_LOW Too Low Optical Module TEC Current

Description

This alarm is generated when the optical module TEC current is too low.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SFP_TEC_CURRENT_LOW = 53	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the optical module TEC current is too low.
Device log	The device log records "Optical Module TEC Current Low Alarm", indicating a too low optical module TEC current alarm.

Impact on the System

The optical module functions are affected, especially the network communication function. Consequently, the live video viewing and recording functions are affected. If the problem is severe, the hardware may be damaged.

Possible Causes

- The optical module is faulty.

- The camera is faulty.

Solution

1. Remove the optical module and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the optical module TEC current is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_LIGHT_SENSOR_INCVALID Ambient Light Sensor Failure

Description

This alarm is generated if the ambient light sensor fails.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LIGHT_SENSOR_INCVALID	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated if the ambient light sensor fails.
Device log	The device log records "Light Sensor Invalid Alarm", indicating an ambient light sensor failure alarm.

Impact on the System

The ambient light sensor functions are affected.

Possible Causes

- The ambient light sensor fails.
- The bus communication is abnormal.

Solution

1. Check whether there are obvious falling and collision traces on the device. Falling and collision may result in internal component damage.
    - If yes, contact technical support engineers for assistance.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the ambient light sensor is recovered, the alarm is automatically cleared.

Reference

After the ambient light sensor fails, use internal triggering or chip triggering to switch between the day and night modes to prevent the impact brought by ambient light sensor failure.

Parent topic: Camera Alarms

PTOPT_FAILURE_ALARM Optocoupler Error

Description

A horizontal optocoupler error alarm is generated if no horizontal optocoupler is detected during the PTZ self-check.

A vertical optocoupler error alarm is generated if no vertical optocoupler is detected during the PTZ self-check.

Alarm Attributes

Alarm ID	Alarm Type
PTOPT_FAILURE_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when no optocoupler is detected during PTZ self-check.
Device log	The device log records "PTopt horizontal Failure Alarm" or "PTopt vertical Failure Alarm", indicating a horizontal or vertical optocoupler error alarm.

Impact on the System

The PTZ cannot correctly set up the coordinate system. As a result, the PTZ positioning is inaccurate.

Possible Causes

- The PTZ device is stuck.

- The optocoupler chip fails.
- The optocoupler detection mechanism fails.
- The flat cable to the optocoupler circuit board is loose.
- The optocoupler circuit board fails.

Solution

Rotate the PTZ device horizontally and vertically to ensure that the PTZ is not stuck. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

When the optocoupler is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_EXTERNAL_POWER_DOWN Power-off of External Power Supply

Description

This alarm is generated when the external power supply is powered off.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_EXTERNAL_POWER_DOWN	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the external power supply is powered off.
Device log	The device log records "External Power Down Alarm, Time: xxx", indicating the generation of an external power supply power-off alarm and the specific alarm generation time.

Impact on the System

This affects the power supply of the device and may result in the device restart. If this problem occurs frequently, the device will be damaged.

Possible Causes

- The external power supply voltage is unstable, or the voltage fluctuation is large.
- An undervoltage occurs.
- The camera is faulty.

Solution

1. Check whether the camera uses an external power supply or power over Ethernet (PoE).
   - If the camera uses an external power supply, go to Step 2.
   - If the camera uses PoE, go to Step 4.
2. Check whether the power supply is normal, whether the voltage meets the camera operating requirements, and whether the voltage is stable in the installation environment.
   - If yes, contact technical support engineers for assistance.
   - If no, go to Step 3.
3. Adjust the power supply device to provide a stable voltage that meets the camera operating requirements. Then, check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, contact technical support engineers for assistance.
4. Check whether the power of the power supply switch is insufficient and whether the switch is faulty.
   - If yes, go to Step 5.
   - If no, contact technical support engineers for assistance.
5. Replace the power supply switch and check whether the alarm is cleared.
   - If yes, no further action is required.

- If no, contact technical support engineers for assistance.

Alarm Clearance

When the external power supply is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_WIPER_FAILURE_ALARM Wiper Failure

Description

This alarm is generated when the wiper returns a preset position error.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_WIPER_FAILURE_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the wiper returns a preset position error.
Device log	The device log records "Wiper Failure Alarm", indicating a wiper failure alarm.

Impact on the System

The wiper functions are affected.

Possible Causes

- The optocoupler is faulty.
- The wiper motor is faulty.

Solution

1. Log in to the camera web system and click the wiper button to rotate the wiper. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 2.
2. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the wiper is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_MEM_HIGHT High Memory Usage

Description

This alarm is generated when the memory usage is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_MEM_HIGHT = 106	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the memory usage is too high.
Device log	The device log records "Mem Hight Alarm. Mem:xxx percent", indicating the high memory usage alarm generation and specific memory usage.

Impact on the System

If the memory usage is too high, the system is overloaded.

Possible Causes

- The device has too many tasks running at the same time.

Solution

1. Log in to the camera web system and check whether multiple tasks such as recording and intelligent analysis are enabled at the same time.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Execute different tasks in different time segments and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the memory usage is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_HTTPS_CERT_EXPIRE HTTPS Certificate Expiration

Description

This alarm is generated when the HTTPS certificate expires.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HTTPS_CERT_EXPIRE = 300	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the HTTPS certificate expires.
Device log	The device log records "HTTPS Certificate is overdue", indicating an HTTPS certificate expiration alarm.

Impact on the System

The HTTPS transfer service is affected.

Possible Causes

The HTTPS certificate expired.

Solution

Purchase the HTTPS certificate from an authorized third-party certification authority or establish the CA server to obtain the HTTPS

certificate.

1. Log in to the camera web system and choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **HTTPS Certificate Management**.
2. Click **Browse** and select a certificate file. Enter the private key in the dialog box that is displayed.
3. Click **Upload** to upload the certificate.

Alarm Clearance

When the HTTPS certificate is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_HTTPS_CERT_WILL_EXPIRE HTTPS Certificate About to Expire

Description

This alarm is generated when the HTTPS certificate is about to expire.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HTTPS_CERT_WILL_EXPIRE = 301	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the HTTPS certificate is about to expire.
Device log	The device log records "HTTPS Certificate will be overdue", indicating the HTTPS certificate about-to-expire alarm.

Impact on the System

The HTTPS transfer service will be affected.

Possible Causes

The HTTPS certificate is about to expire.

Solution

Purchase the HTTPS certificate from an authorized third-party certification authority or establish the CA server to obtain the HTTPS certificate.

1. Log in to the camera web system and choose **Configuration** > **System** > **Security Management** > **Certificate Management** > **HTTPS Certificate Management**.
2. Click **Browse** and select a certificate file. Enter the private key in the dialog box that is displayed.
3. Click **Upload** to upload the certificate.

Alarm Clearance

When the HTTPS certificate is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_DOX_CERT_EXPIRE 802.1X Certificate Expiration

Description

This alarm is generated when the 802.1X certificate expires.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DOT1X_CERT_EXPIRE = 302	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the 802.1X certificate expires.
Device log	The device log records "802.1x Certificate is overdue", indicating the 802.1X certificate expiration alarm.

Impact on the System

The 802.1X functions are affected.

Possible Causes

The 802.1X certificate expired.

Solution

You need to obtain the 802.1X certificate from the access authentication server and then perform the following operations:

1. Log in to the camera web system and choose **Configuration** > **Network** > **Advanced Settings** > **802.1X**.

   The **802.1X** page is displayed.

2. Upload the obtained certificate in the **Certificate Management** area. For details, see the camera product documentation.

Alarm Clearance

When the 802.1X certificate is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_DOX_CERT_WILL_EXPIRE 802.1X Certificate About to Expire

Description

This alarm is generated when the 802.1X certificate is about to expire.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DOT1X_CERT_WILL_EXPIRE = 303	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the 802.1X certificate is about to expire.
Device log	The device log records "802.1x Certificate will be overdue", indicating the 802.1X certificate about-to-expire alarm.

Impact on the System

The 802.1X functions are affected.

Possible Causes

The 802.1X certificate is about to expire.

Solution

You need to obtain the 802.1X certificate from the access authentication server and then perform the following operations:

1. Log in to the camera web system and choose **Configuration** > **Network** > **Advanced Settings** > **802.1X**.

   The **802.1X** page is displayed.

2. Upload the obtained certificate in the **Certificate Management** area. For details, see the camera product documentation.

Alarm Clearance

When the 802.1X certificate is recovered, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_SDK_PWD_STILL_INITIAL_PWD SDK Password Unchanged

Description

This alarm is generated when the SDK password is not changed.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SDK_PWD_STILL_INITIAL_PWD = 304	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the SDK password is not changed.
Device log	The device log records "SDK password is still the initial password, please modify as soon as possible", indicating the alarm of the unchanged SDK password.

Impact on the System

SDK security risks exist.

Possible Causes

The SDK password is not changed.

Solution

Chang the SDK password.

Alarm Clearance

After the SDK password is changed, the alarm is automatically cleared.

Reference

The procedure for changing the SDK password is as follows:

1. Log in to the camera web system and choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**. The **Platform Connection** page is displayed.
2. Click **Password Management**. In the area that is displayed, click the **SDK Password** tab. On the tab page that is displayed, set **Web user password**, **New password**, and **Confirm password**.

Parent topic: Camera Alarms

ALARM_TYPE_DISK_EXCEPTION SD Card Fault

Description

This alarm is generated when the SD card is faulty.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DISK_EXCEPTION = 31	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the SD card is faulty.
Device log	The device log records "Disk Abnormal Alarm", indicating the disk fault alarm.

Impact on the System

The SD card functions are affected.

Possible Causes

- The SD card is not securely inserted into the card slot.
- The SD card is damaged.

Solution

1. Check whether an SD card is installed on the device.

- If yes, go to Step 2.
- If no, contact technical support engineers for assistance.

2. Remove the SD card and insert it again. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 4.
4. Replace the SD card and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

After the SD card fault is rectified, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_NO_SIGNAL Video Signal Loss

Description

This alarm is generated when video signals are lost.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_NO_SIGNAL	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when video signals are lost.
Device log	The device log records "Video Signal Lost Alarm, Channel Device ID:xxx", indicating the video signal loss alarm generation and the specific device ID.

Impact on the System

Video signal functions are affected.

Possible Causes

- The sensor flat cable is not properly connected.
- The camera is faulty.

Solution

Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

After the video signal loss fault is rectified, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_ATTITUDE_CHANGE_ALARM Camera Angle Abnormality Alarm

Description

This alarm is generated when the vertical angle of the camera changes.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ATTITUDE_CHANGE_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the vertical angle of the camera changes.
Device log	The device log records "Attitude Change Alarm", indicating the camera angle abnormality alarm.

Impact on the System

The function of the device is not affected. However, the field of view changes.

Possible Causes

- The installation mount is loose.
- The device is shocked.

Solution

1. Check whether the vertical angle of the camera is different from that before the power-on.
    - If yes, go to Step 2.
    - If no, contact technical support engineers for assistance.
2. Adjust the vertical angle of the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

Restore the camera to its original position and secure the mount. Alternatively, power off the camera and power it on again.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_ITS_RADAR_EXCEPTION_ALARM ITS Radar Exception

Description

This alarm is generated when the communication between the radar detector and the camera is interrupted.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ITS_RADAR_EXCEPTION_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the communication between the radar detector and the camera is interrupted.
Device log	The device log records "ITS Radar Exception Alarm. The DevType is %u, PortId is %u.", indicating the radar exception alarm generation and the specific device type and port number. **NOTE:** The value of **%u** may change based on the site requirements.

Impact on the System

The ITS snapshot service is affected.

Possible Causes

- The camera is powered off.
- The cable connecting the radar detector and the camera is damaged.
- There is no cable connecting the radar detector and the camera.

Solution

1. Check whether the camera is powered off.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Power on the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Check whether the cable connection between the radar detector and the camera is correct. Use the CSR-IK microwave radar as an example. The correct cable connection is as follows: The brown cable of the radar is connected to the RS-485 positive terminal of the camera, and the white cable is connected to the RS-485 negative terminal of the camera.
    - If yes, go to Step 5.
    - If no, go to Step 4.
4. Correctly reconnect the cable between the radar detector and the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 5

5. Remove the cable between the radar detector and the camera and insert it again, and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 6.
6. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the connection between the radar detector and the camera is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_ITS_IOCOIL_EXCEPTION_ALARM ITS I/O Loop Exception

Description

This alarm is generated when the communication between the I/O loop detector and the camera is interrupted.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ITS_IOCOIL_EXCEPTION_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the communication between the I/O loop detector and the camera is interrupted.
Device log	The device log records "ITS IO-Coil Exception Alarm. The DevType is %u, PortId is %u.", indicating the I/O loop exception alarm generation and the specific device type and port number. **NOTE:** The value of **%u** may change based on the site requirements.

Impact on the System

The ITS snapshot service is affected.

Possible Causes

- The camera is powered off.
- The cable between the I/O loop detector and the camera is damaged.
- There is no cable connecting the I/O loop detector and the camera.

Solution

1. Check whether the camera is powered off.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Power on the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Check whether the cable connection between the I/O loop detector and the optocoupler input port of the camera is correct.
    - If yes, go to Step 5.
    - If no, go to Step 4.
4. Correctly reconnect the cable between the I/O loop detector and the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 5
5. Remove the cable between the I/O loop detector and the camera and insert it again, and check whether the alarm is

cleared.

- If yes, no further action is required.
- If no, go to Step 6.

6. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
   - If yes, no further action is required.
   - If no, contact technical support engineers for assistance.

Alarm Clearance

When the connection between the I/O loop detector and the camera is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_ITS_485COIL_EXCEPTION_ALARM ITS RS-485 Loop Exception

Description

This alarm is generated when the communication between the RS-485 loop detector and the camera is interrupted.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ITS_485COIL_EXCEPTION_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the communication between the RS-485 loop detector and the camera is interrupted.
Device log	The device log records ALARM_TYPE_ITS_485COIL_EXCEPTION_ALARM, "ITS 485-Coil Exception Alarm. The DevType is %u, PortId is %u.", indicating the RS-485 loop exception alarm generation and the specific device type and port number. **NOTE:** The value of **%u** may change based on the site requirements.

Impact on the System

The ITS snapshot service is affected.

Possible Causes

- The camera is powered off.
- The cable between the RS-485 loop detector and the camera is damaged.
- There is no cable connecting the RS-485 loop detector and the camera.

Solution

1. Check whether the camera is powered off.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Power on the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Check whether the cable connection between the RS-485 loop detector and the camera's RS-485 port is correct.
    - If yes, go to Step 5.
    - If no, go to Step 4.
4. Correctly reconnect the cable between the RS-485 loop detector and the camera's RS-485 port and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 5
5. Remove the cable between the RS-485 loop detector and the camera's RS-485 port and insert it again, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to Step 6.

6. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the connection between the RS-485 loop detector and the camera is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_ITS_REDTOR_EXCEPTION_ALARM ITS Traffic Light Detector Exception

Description

This alarm is generated when the communication between the traffic light detector and the camera is interrupted.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ITS_485COIL_EXCEPTION_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the communication between the traffic light detector and the camera is interrupted.
Device log	The device log records "ITS Redtor Exception Alarm. The DevType is %u, PortId is %u.", indicating the traffic light detector exception alarm generation and the specific device type and port number. **NOTE:** The value of **%u** may change based on the site requirements.

Impact on the System

The ITS snapshot service is affected.

Possible Causes

- The camera is powered off.
- The cable connecting the traffic light detector and the camera is damaged.
- There is no cable connecting the traffic light detector and the camera.

Solution

1. Check whether the camera is powered off.
    - If yes, go to Step 2.
    - If no, go to Step 3.
2. Power on the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 3.
3. Check whether the cable connection between the traffic light detector and the camera is correct.
    - If yes, go to Step 5.
    - If no, go to Step 4.
4. Correctly reconnect the cable between the traffic light detector and the camera and check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, go to Step 5
5. Remove the cable between the traffic light detector and the camera and insert it again, and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to Step 6.

6. Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.
    - If yes, no further action is required.
    - If no, contact technical support engineers for assistance.

Alarm Clearance

When the connection between the traffic light detector and the camera is normal, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_LENS_FAILURE_ALARM Lens PT Optocoupler Failure

Description

This alarm is generated if the lens self-check function is enabled but the lens self-check fails.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LENS_FAILURE_ALARM	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated if the lens self-check function is enabled but the lens self-check fails.
Device log	The device log records "Lens Failure Alarm", indicating the lens PT optocoupler failure alarm.

Impact on the System

The zoom, focus, ICR, and iris adjustment of the device is affected, which further affects the live video viewing and recording functions.

Possible Causes

- The lens is aged, making the internal structure damaged.
- The camera is faulty.

Solution

Restart the device. For details, see Remotely Restarting a Camera. Then, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, contact technical support engineers for assistance.

Alarm Clearance

After the lens self-check function is enabled and the lens condition passes the self-check, the alarm is automatically cleared.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_WEB_PWD_EXPIRE Web Password Expiration

Description

This alarm is generated when the password for logging in to the camera web system expires.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_WEB_PWD_EXPIRE = 313	Device alarm

Alarm Parameters

Parameter	Description
Description	This alarm is generated when the password for logging in to the camera web system expires.
Device log	" WEB user *username* password expired ",

Impact on the System

Users can still log in to the camera web system. For security purposes, users are advised to periodically change the password.

Possible Causes

The password for logging in to the camera web system has expired and is not changed.

Solution

Change the password for logging in to the camera web system. For details, see Changing the User Password.

Alarm Clearance

This alarm is automatically cleared after the password for logging in to the camera web system is changed.

Reference

None

Parent topic: Camera Alarms

ALARM_TYPE_DISK_FULL Full Disk

Description

This alarm is generated when a hard disk is full.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DISK_FULL = 2	Fault alarm

Parent topic: Camera Alarms

ALARM_TYPE_DISK_FAULT Disk Fault

Description

This alarm is generated when a hard disk is faulty.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DISK_FAULT = 5	Fault alarm

Parent topic: Camera Alarms

ALARM_TYPE_DISK_FAIL Disk Read/Write Failure

Description

This alarm is generated when disk read or write fails.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DISK_DISC_FAIL=31	Fault alarm

Parent topic: Camera Alarms

ALARM_TYPE_DISC_PULL_OUT Disk Removal

Description

This alarm is generated when a hard disk is removed.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DISK_DISC_PULL_OUT=64	Fault alarm

Parent topic: Camera Alarms

Camera Event Alarms

- ALARM_TYPE_MOVE_DECTION Motion Detection
- ALARM_TYPE_SHIELD Lens Blocking
- ALARM_TYPE_TZ/ALARM_TYPE_OC Tripwire Crossing Detection
- ALARM_TYPE_HUMAN_COUNT Head Counting
- ALARM_TYPE_AUDIO_CUT Sound Detection
- ALARM_TYPE_AUDIO_UP Sudden Volume Increase
- ALARM_TYPE_AUDIO_DOWN Sudden Audio Decrease
- ALARM_TYPE_SCENECHANGE Scene Change
- ALARM_TYPE_AUTOTRACKING Automatic Tracking
- ALARM_TYPE_CROWD_ANALYSIS Crowd Gathering Detection
- ALARM_TYPE_VIDEO_SHAKE Image Shaking
- ALARM_TYPE_VIDEO_FROZEN Image Freezing
- ALARM_TYPE_VIDEO_SNOW_NOISE Static Noise
- ALARM_TYPE_VIDEO_STRIPENOISE Stripe Noise
- ALARM_TYPE_CAR_DETECTION Parking Detection
- ALARM_TYPE_LEAVE_DETECT Absence Detection
- ALARM_TYPE_QUEUE_DETECT Queue Length Detection
- ALARM_TYPE_CROWD_DENSITY_DETECT Crowd Density Detection
- ALARM_TYPE_ILLEGAL_PARKING Parking Violation Detection

ALARM_TYPE_VLPR_TRAFFIC_CONGESTION Traffic Congestion (Non-ITS Cameras)

ALARM_TYPE_TRAFFIC_CONGESTION Traffic Congestion (ITS Cameras)

ALARM_TYPE_MOTORBIKE Electric Bike Detection

ALARM_TYPE_ELECTROMOBILE_DETECT Electric Bike Detection in Elevators

ALARM_TYPE_FACE_MASK Mask Detection

ALARM_TYPE_FIRE_DETECT Fire Detection

ALARM_TYPE_TEMPERATURE_CONTROL Ambient Temperature

ALARM_TYPE_LPR_CAPTURE_RES Automatic Parking Violation Detection of Traffic PTZ Dome Cameras (Used by SDK)

ALARM_TYPE_PU_MANUAL_LPR_CAPTURE_RES Manual Parking Violation Detection of Traffic PTZ Dome Cameras (Used by SDK)

ALARM_TYPE_VE_ILLEGAL_PARKING Parking Violation Detection

ALARM_TYPE_VE_ON_VEHICLE_LANE Non-motorized Vehicles in Motor Vehicle Lanes

ALARM_TYPE_VE_ON_NONEVEHICLE_LANE Motor Vehicles in on Non-motorized Vehicle Lanes

ALARM_TYPE_VE_PRESSING_LINE Marked Lane Violation

ALARM_TYPE_VE_WRONG_DIRECTION Wrong-Way Driving

ALARM_TYPE_VE_ABNORMAL_PLATE Abnormal License Plate (ITS Cameras)

ALARM_TYPE_VE_REVERSE ITS Illegal Backing (ITS Cameras)

ALARM_TYPE_VE_SHELTER_PLATE License Plate Occlusion (ITS Cameras)

ALARM_TYPE_FOG_DETECT Fog Detection

ALARM_TYPE_FOG_VISIBILITY Visibility Detection

ALARM_TYPE_BRUTE_FORCE_CRACKING Brute Force Password Cracking

ALARM_TYPE_RECORDING_JOBSTATE Recording Task Status Change

ALARM_TYPE_NETWORK_CONGESTION Slow Network Packet Sending

AlARM_TYPE_PTZ_MOVE Genetec PTZ Camera Rotation

ALARM_TYPE_SSH_OPEN SSH Enabled

ALARM_TYPE_SDK_LOCK SDK Locked

ALARM_TYPE_WEB_LOCK Web Client Locked

ALARM_TYPE_ONVIF_LOCK ONVIF Locked

ALARM_TYPE_GENETEC_LOCK Genetec Locked

ALARM_TYPE_GB35114_CERT_EXPIRE GB 35114 CA Certificate Expired

ALARM_TYPE_GB35114_CERT_WILL_EXPIRE GB 35114 CA Certificate Expires Soon

ALARM_TYPE_HIDS_ILLACCOUNT Unauthorized Account

ALARM_TYPE_HIDS_BOTNE Botnet

ALARM_TYPE_HIDS_ROOTKIT Rootkit

ALARM_TYPE_HIDS_MINER Mining

ALARM_TYPE_SLAVE_RTSP_KEEP_ALIVE_FAIL RTSP Keepalive Failure of a Secondary Camera

ALARM_TYPE_SLAVE_STREAM_NORMAL RTSP Stream Exception of a Secondary Camera

ALARM_TYPE_KICKOFFLINE Device Going Offline Forcibly (Beijing Subway)

ALARM_TYPE_DUPLICATEREG Secondary Device Registration (Beijing Subway)

ALARM_TYPE_KEEPLIVETIMEOUT Beijing Subway Platform Receiving Keepalive Messages Timed Out

ALARM_TYPE_INTRUSION Intrusion Detection

ALARM_TYPE_HOVER Loitering Detection

ALARM_TYPE_LEGACY Abandoned Object Detection

ALARM_TYPE_REMOVE Removed Object Detection

ALARM_TYPE_NOISE Noise Interference

ALARM_TYPE_ENTER Area Entry Detection

ALARM_TYPE_EXIT Area Exit Detection

ALARM_TYPE_FASTMOVE Fast Movement Detection

ALARM_TYPE_OUTOFFOCUS_DETECT Defocus Detection

ALARM_TYPE_VIDEO_GAINIMBALANCE Brightness Anomaly

ALARM_TYPE_VIDEO_COLORCAST Color Cast

ALARM_TYPE_FACE_DETECTION Target Detection

Parent topic: Alarm Reference

ALARM_TYPE_MOVE_DECTION Motion Detection

Description

This alarm is generated when an object moves in a detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_MOVE_DECTION=4	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SHIELD Lens Blocking

Description

This alarm is generated when the lens is blocked by an object.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SHIELD = 6	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_TZ/ALARM_TYPE_OC Tripwire Crossing Detection

Description

This alarm is generated when an object crosses a tripwire in a specified direction.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_TZ = 11	Event alarm
ALARM_TYPE_OC = 12	
ALARM_TYPE_TW = 14	

Parent topic: Camera Event Alarms

ALARM_TYPE_HUMAN_COUNT Head Counting

Description

This alarm is generated when the total number of people entering and leaving a detection area exceeds the alarm threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HUMAN_COUNT = 118	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_AUDIO_CUT Sound Detection

Description

This alarm is generated when the microphone is disconnected from the camera.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_AUDIO_CUT = 32	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_AUDIO_UP Sudden Volume Increase

Description

This alarm is generated when the camera detects abrupt sound changes, for example, screams.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_AUDIO_UP = 100	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_AUDIO_DOWN Sudden Audio Decrease

Description

This alarm is generated when the camera detects that the sound volume in live video suddenly decreases.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_AUDIO_DOWN = 101	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SCENECHANGE Scene Change

Description

This alarm is generated when the detection scene changes due to manual movement of the camera or other reasons.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SCENECHANGE = 107	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_AUTOTRACKING Automatic Tracking

Description

This alarm is generated when an automatically tracked object is lost.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_AUTOTRACKING = 108	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_CROWD_ANALYSIS Crowd Gathering Detection

Description

This alarm is generated when the camera detects crowd gathering in the video image.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_CROWD_ANALYSIS = 110	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_SHAKE Image Shaking

Description

This alarm is generated when the camera detects image shaking.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_SHAKE = 111	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_FROZEN Image Freezing

Description

This alarm is generated when the camera detects that the video image stays at a frame for a long period.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_FROZEN = 112	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_SNOW_NOISE Static Noise

Description

This alarm is generated when the camera detects static noise on video images.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_SNOW_NOISE = 113	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_STRIPENOISE Stripe Noise

Description

This alarm is generated when the camera detects stripe noise on video images.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_STRIPENOISE = 114	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_CAR_DETECTION Parking Detection

Description

This alarm is generated when a vehicle stays in a detection area for a period longer than the threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_CAR_DETECTION=117	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_LEAVE_DETECT Absence Detection

Description

This alarm is generated when the camera detects that the number of on-duty persons in a detection area is lower than the preset threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LEAVE_DETECT = 120	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_QUEUE_DETECT Queue Length Detection

Description

This alarm is generated when the camera detects that the number of queuers and queuing duration exceed the preset threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_QUEUE_DETECT = 121	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_CROWD_DENSITY_DETECT Crowd Density Detection

Description

This alarm is generated when the camera detects that the number of people in a detection area exceeds the preset threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_CROWD_DENSITY_DETECT=122	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_ILLEGAL_PARKING Parking Violation Detection

Description

This alarm is generated when the traffic PTZ dome camera detects a parking violation.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ILLEGAL_PARKING = 123	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VLPR_TRAFFIC_CONGESTION Traffic Congestion (Non-ITS Cameras)

Description

This alarm is generated when a non-ITS camera detects traffic congestion.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VLPR_TRAFFIC_CONGESTION = 124	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_TRAFFIC_CONGESTION Traffic Congestion (ITS Cameras)

Description

This alarm is generated when an ITS camera detects traffic congestion.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_TRAFFIC_CONGESTION = 125	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_MOTORBIKE Electric Bike Detection

Description

This alarm is generated when the camera detects an electric bike in a specified area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_MOTORBIKE = 126	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_ELECTROMOBILE_DETECT Electric Bike Detection in Elevators

Description

This alarm is generated when the camera detects an electric bike in an elevator.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ELECTROMOBILE_DETECT = 127	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FACE_MASK Mask Detection

Description

This alarm is generated when the camera detects a person who does not wear a mask in a specified detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FACE_MASK = 131	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FIRE_DETECT Fire Detection

Description

This alarm is generated when the camera detects a fire on the live video image.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FIRE_DETECT = 139	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_TEMPERATURE_CONTROL Ambient Temperature

Description

This alarm is generated when the camera detects that the ambient temperature is too high.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_TEMPERATURE_CONTROL = 140	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_LPR_CAPTURE_RES Automatic Parking Violation Detection of Traffic PTZ Dome Cameras (Used by SDK)

Description

This alarm is generated when the traffic PTZ dome camera detects a parking violation through automatic parking violation detection.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LPR_CAPTURE_RES = 200	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_PU_MANUAL_LPR_CAPTURE_RES Manual Parking Violation Detection of Traffic PTZ Dome Cameras (Used by SDK)

Description

This alarm is generated when the traffic PTZ dome camera detects a parking violation through manual parking violation detection.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_PU_MANUAL_LPR_CAPTURE_RES = 201	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_ILLEGAL_PARKING Parking Violation Detection

Description

This alarm is generated when the camera detects a parking violation.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_ILLEGAL_PARKING = 400	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_ON_VEHICLE_LANE Non-motorized Vehicles in Motor Vehicle Lanes

Description

This alarm is generated when the camera detects a non-motorized vehicle that stays in a motor vehicle lane for a period longer than the preset threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_ON_VEHICLE_LANE = 401	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_ON_NONEVEHICLE_LANE Motor Vehicles in on Non-motorized Vehicle Lanes

Description

This alarm is generated when the camera detects a motor vehicle that stays in a non-motorized vehicle lane for a period longer than the preset threshold.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_ON_NONEVEHICLE_LANE = 402	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_PRESSING_LINE Marked Lane Violation

Description

This alarm is generated when the camera detects a vehicle that drives across a solid line.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_PRESSING_LINE = 403	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_WRONG_DIRECTION Wrong-Way Driving

Description

This alarm is generated when the camera detects a vehicle that drives against the direction of traffic.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_WRONG_DIRECTION = 404	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_ABNORMAL_PLATE Abnormal License Plate (ITS Cameras)

Description

This alarm is generated when an ITS camera detects an abnormal license plate.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_ABNORMAL_PLATE = 405	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_REVERSE ITS Illegal Backing (ITS Cameras)

Description

This alarm is generated when an ITS camera detects a vehicle that is backing when it is not safe to do so or when it causes interference with other traffic.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_REVERSE = 406	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VE_SHELTER_PLATE
License Plate Occlusion (ITS Cameras)

Description

This alarm is generated when an ITS camera detects that the license plate is occluded.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VE_SHELTER_PLATE = 407	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FOG_DETECT Fog Detection

Description

This alarm is generated when the fog intensity in a detection area reaches the specified level.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FOG_DETECT = 580	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FOG_VISIBILITY Visibility Detection

Description

This alarm is generated when the visibility distance is less than the preset alarm distance.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FOG_VISIBILITY = 581	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_BRUTE_FORCE_CRACKING Brute Force Password Cracking

Description

This alarm is generated when the protocol password is incorrectly entered for several consecutive times or is cracked.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_BRUTE_FORCE_CRACKING = 507	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_RECORDING_JOBSTATE Recording Task Status Change

Description

This alarm is generated when the recording task status changes.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_RECORDING_JOBSTATE=34	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_NETWORK_CONGESTION Slow Network Packet Sending

Description

This alarm is generated when it is slow to send network packets.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_NETWORK_CONGESTION = 68	Event alarm

Parent topic: Camera Event Alarms

AlARM_TYPE_PTZ_MOVE Genetec PTZ Camera Rotation

Description

This alarm is generated when the Genetec PTZ camera rotates.

Alarm Attributes

Alarm ID	Alarm Type
AlARM_TYPE_PTZ_MOVE = 305	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SSH_OPEN SSH Enabled

Description

This alarm is generated when SSH is enabled.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SSH_OPEN = 306	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SDK_LOCK SDK Locked

Description

This alarm is generated when the SDK is locked.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SDK_LOCK = 307	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_WEB_LOCK Web Client Locked

Description

This alarm is generated when the web client is locked.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_WEB_LOCK = 308	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_ONVIF_LOCK ONVIF Locked

Description

This alarm is generated when ONVIF is locked.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ONVIF_LOCK = 309	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_GENETEC_LOCK Genetec Locked

Description

This alarm is generated when Genetec is locked.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_GENETEC_LOCK = 310	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_GB35114_CERT_EXPIRE GB 35114 CA Certificate Expired

Description

This alarm is generated when the CA certificate of the GB 35114 protocol expires.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_GB35114_CERT_EXPIRE = 342	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_GB35114_CERT_WILL_EXPIRE GB 35114 CA Certificate Expires Soon

Description

This alarm is generated when the CA certificate of the GB 35114 protocol is about to expire.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_GB35114_CERT_WILL_EXPIRE = 343	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_HIDS_ILLACCOUNT Unauthorized Account

Description

This alarm is generated when an unauthorized account is used to access the system.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HIDS_ILLACCOUNT = 356	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_HIDS_BOTNE Botnet

Description

This alarm is generated when a botnet attack is detected.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HIDS_BOTNE = 357	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_HIDS_ROOTKIT Rootkit

Description

This alarm is generated when a rootkit attack is detected.

Alarm Attributes

Alarm ID	Alarm Type
AlARM_TYPE_PTZ_MOVE = 358	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_HIDS_MINER Mining

Description

This alarm is generated when a mining attack is detected.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HIDS_MINER = 359	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SLAVE_RTSP_KEEP_ALIVE_FAIL RTSP Keepalive Failure of a Secondary Camera

Description

This alarm is generated when the RTSP keepalive operation of a secondary camera fails.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SLAVE_RTSP_KEEP_ALIVE_FAIL=500	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_SLAVE_STREAM_NORMAL RTSP Stream Exception of a Secondary Camera

Description

This alarm is generated when the RTSP stream of a secondary camera is abnormal.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_SLAVE_STREAM_NORMAL = 506	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_KICKOFFLINE Device Going Offline Forcibly (Beijing Subway)

Description

This alarm is generated when a device at the Beijing Subway site is forced to go offline.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_KICKOFFLINE = 1101	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_DUPLICATEREG Secondary Device Registration (Beijing Subway)

Description

This alarm is generated when a device at the Beijing Subway site is registered for the second time.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_DUPLICATEREG = 1102	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_KEEPLIVETIMEOUT Beijing Subway Platform Receiving Keepalive Messages Timed Out

Description

This alarm is generated when the duration for the Beijing Subway platform to receive keepalive message timed out.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_KEEPLIVETIMEOUT = 1103	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_INTRUSION Intrusion Detection

Description

This alarm is generated when an object intrudes into a detection area (including touching the detection line and staying in the detection area).

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_INTRUSION = 15	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_HOVER Loitering Detection

Description

This alarm is generated when an object loiters in a detection area for a period longer than the preset.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_HOVER = 16	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_LEGACY Abandoned Object Detection

Description

This alarm is generated when an object is abandoned in a detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_LEGACY = 17	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_REMOVE Removed Object Detection

Description

This alarm is generated when an object is removed from a detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_REMOVE = 18	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_NOISE Noise Interference

Description

This alarm is generated when the camera detects noise interference in video.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_NOISE = 26	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_ENTER Area Entry Detection

Description

This alarm is generated when an object enters a detection area and touches the detection line.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_ENTER = 102	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_EXIT Area Exit Detection

Description

This alarm is generated when an object leaves a detection area and touches the detection line.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_EXIT = 103	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FASTMOVE Fast Movement Detection

Description

This alarm is generated when an object moves fast in a detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FASTMOVE = 104	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_OUTOFFOCUS_DETECT Defocus Detection

Description

This alarm is generated when the image is unclear due to improper focal length.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_OUTOFFOCUS_DETECT = 109	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_GAINIMBALANCE Brightness Anomaly

Description

This alarm is generated when the camera detects brightness anomalies.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_GAINIMBALANCE = 115	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_VIDEO_COLORCAST Color Cast

Description

This alarm is generated when the camera detects color cast on video.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_VIDEO_COLORCAST = 116	Event alarm

Parent topic: Camera Event Alarms

ALARM_TYPE_FACE_DETECTION Target Detection

Description

This alarm is generated when the camera detects a target in a detection area or a target disappears from the detection area.

Alarm Attributes

Alarm ID	Alarm Type
ALARM_TYPE_FACE_DETECTION = 10	Event alarm

Parent topic: Camera Event Alarms

Introduction to the Right Pane on the View Page

By modifying some configuration items on the right pane of the **View** page, you can perform configuration operations related to video viewing, device IP address, system time, image, and video streams. Different camera models may have different parameters.

For cameras of some models, you can click  in the lower part of the live video pane to display the PTZ configuration page.

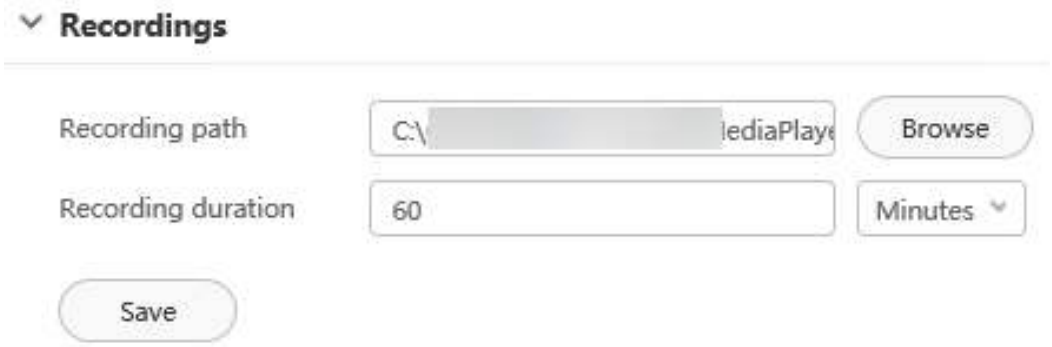
Setting Recording File Parameters

This section describes how to configure the path for storing recording files.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Recordings**. The **Recordings** area is displayed, as shown in Figure 1.

   Figure 1 Recordings area

3. Set recording file parameters. Table 1 describes the parameters.

   Table 1 Recording file parameters

Parameter	Description
Recording path	Path for saving recording files. To set a save path, click **Browse** and select a path.
Recording duration	Duration of video recorded on the **View** page. The value ranges from 5s to 24 hours. You can select a time unit from the drop-down list box next to the **Recording duration** text box.

4. Click **Save**.

Configuring Storage Management

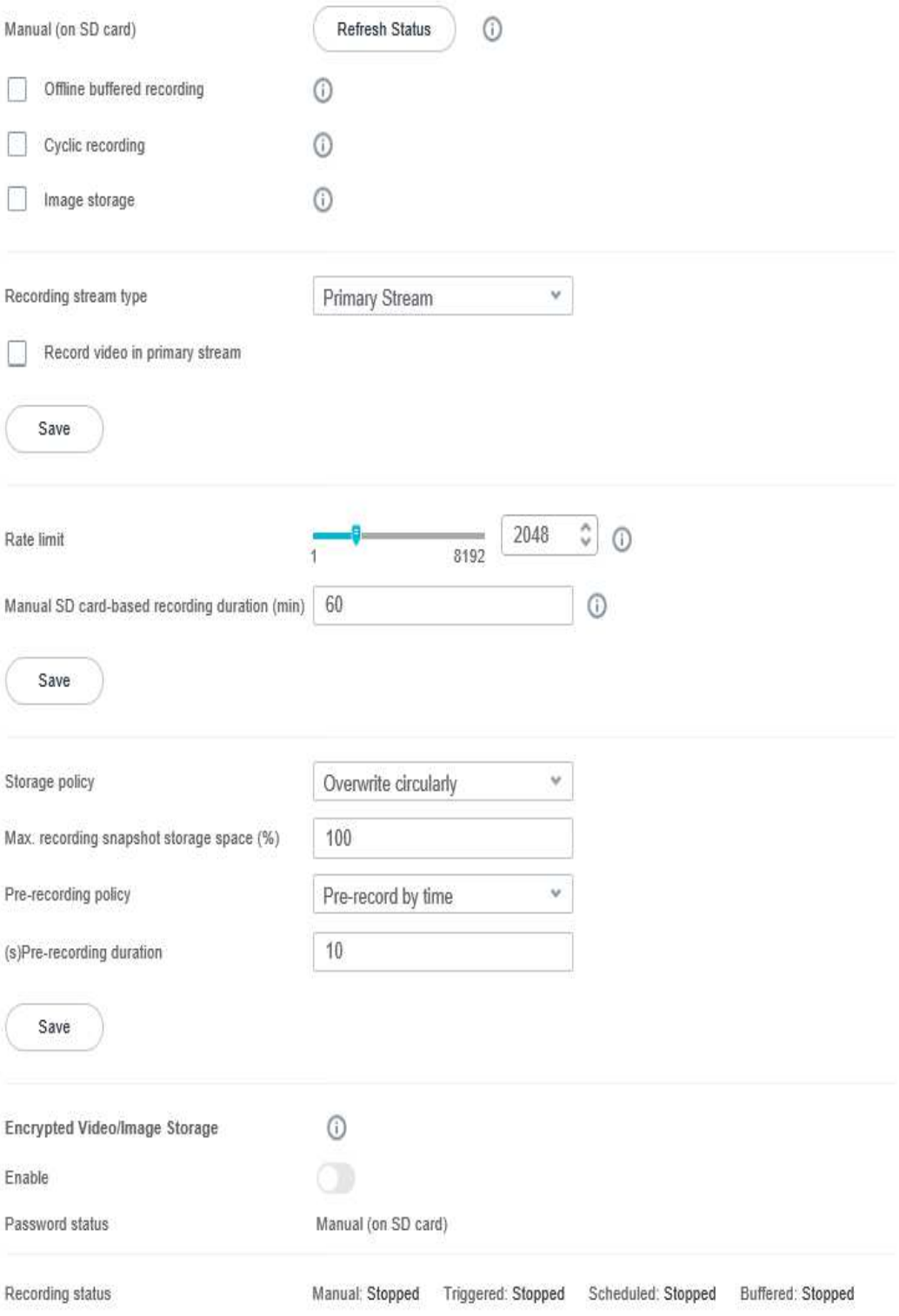
Using the storage management function, you can view the SD card status, limit the rate, conduct cyclic recording, and enable encrypted storage of video and images.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Storage** > **Storage Management**. The **Storage Management** tab page is displayed, as shown in Figure 1.

   The web page varies depending on the camera model.

Figure 1 Storage Management page



3. Select a channel type and set related parameters. Table 1 describes the parameters.

Table 1 Storage management parameters

Parameter	Description

Parameter		Description
SD card management	No SD card	Indicates that there is no SD card on the camera.

Parameter		Description
	SD card status	Total storage capacity and occupied space of an SD card.
	Instant formatting	Indicates whether to format an SD card. **NOTE:** • Format an SD card during off-peak hours. • Before using an SD card, format it. • Back up data before formatting an SD card. • All data will be lost after an SD card is formatted. Exercise caution when performing this operation. • Do not remove an SD card when it is being formatted or data-written. • If the capacity status of the SD card does not change after the SD card is formatted, the SD card may be faulty. You are advised to replace the SD card and format it again. • If the camera is powered off during SD card formatting, an SD card exception may occur and an error message is displayed. • Use a compatible SD card. If you use an SD card that is not in the

Parameter		Description
		compatibility list, compatibility issues may occur.
	Refresh Status	Displays the latest SD card status.
Offline buffered recording		Indicates whether to allow cameras disconnected from the network to continue to shoot and temporarily store video on their SD cards. When the network is restored, the video security platform sends a video request to the cameras. The cameras then send the video stored on the SD cards to the video security platform. This function is disabled by default. **NOTE:** • This function does not support the MJPEG protocol. • If the camera fails to connect to the platform for a long time or does not connect to the platform, you are advised to manually disable the video buffering function of the camera to prolong the service life of the SD card. • When the SD card is full, the recording stops or overwrites previous recordings based on the storage policy.
Cyclic recording		Indicates whether to enable cyclic recording. If this parameter is

Parameter	Description
	selected, the recordings will be saved to the SD card. **NOTE:** • This function is invalid when the MJPEG encoding protocol is used. • Cyclic recording will result in frequent writes to the SD card, which will shorten the SD card's service life. • When the SD card is full, the recording stops or overwrites previous recordings based on the storage policy.
Image storage	Indicates whether to save snapshots to the SD card. **NOTE:** Enabling the image storage function will save snapshots to the SD card. When the image storage space reaches 90%, new images will overwrite earlier images. You can choose whether to enable this function based on the service scenario and the space allocated by the SD card for image storage.
Recording stream type	Type of streams in which subsequent video is recorded.
Record video in primary stream	Indicates whether to record video in the type of primary streams.

Parameter	Description
	NOTE: • Before selecting this parameter, ensure that **Video recording** is selected under **Configuration** > **Service** > **Alarm Service** > **Alarm Input** > **Common Alarm** > **Alarm Linkage Policy**. • If you set **Recording stream type** to **Primary Stream**, video is recorded in the type of primary streams no matter whether **Record video in primary stream** is selected.
Rate limit	Maximum upload rate for video buffering or the download rate for SD card recording. It is recommended that the value be a quarter of the primary stream bit rate and not exceed the available bandwidth. **NOTE:** • The video buffering function occupies additional network bandwidth. If the value exceeds the available bandwidth, network congestion may occur, which leads to image exceptions. Set **Rate limit** based on the site requirements. • The rate for downloading recordings in the SD card can be adjusted. However, the rate

Parameter	Description
	cannot be adjusted during the download.
Manual SD card-based recording duration (min)	Duration for recording video on the SD card on the **View** page. After this function is enabled, the recording automatically stops when the specified duration arrives. The recording duration ranges from 5 minutes to 1440 minutes.
Storage policy	• **Overwrite circularly**: After the video recording or snapshot taking function is enabled, recordings and snapshot images are saved on the SD card. When the SD card space is used up, the earliest recording files and images are automatically overwritten. • **Stop**: After the video recording or snapshot taking function is enabled, recordings and snapshot images are saved on the SD card. When the SD card space is used up, the camera stops recording video or taking snapshots.
Max. recording snapshot storage space (%)	Maximum space for storing recordings and snapshots, in percentage. The value is an integer ranging from 1 to 100. The default value is **100**.

Parameter	Description
Pre-recording policy	Policy for the camera to move the recording during a certain period (configurable) before an occurring alarm from the memory to the SD card. The pre-recording policies include **No pre-recording**, **Pre-record by time**, and **Pre-record by memory capacity**. When **Pre-recording policy** is set to **Pre-record by time**, set the pre-recording period before the alarm based on the site requirements. **NOTE:** • PTZ dome cameras (including traffic PTZ dome cameras) do not support pre-recording policy configuration. • If **Pre-recording policy** is set to **Pre-record by memory capacity**, pre-recording duration is inversely proportional to bit rate. That is, a higher bit rate indicates a shorter pre-recording duration.
Pre-recording duration (s)	Pre-alarm recording duration.

NOTE

Under **Recording status**, you can view the status of recordings of different types.

- **Running**: The recording is enabled.
- **Stopped**: The recording is disabled.

4. Determine whether to enable encrypted storage of video and images. If this function is enabled, video and images on the SD card will be encrypted for storage and can be viewed only through a password. For details, see Table 2.

Table 2 Storage encryption operations

Operation	Description
Enable/Disable encrypted video and image storage	• If this function is enabled for the first time, a password must be set for decrypting video and image storage. **NOTE:** The password cannot be retrieved after it is lost. Keep the password safe. • If this function is disabled, the new video and images will not be encrypted, and encrypted data is not decrypted. • If this function is disabled and enabled again, you need to enter the password. If you forget the password, you can reset the password.
Change the password	You can change the password depending on your needs. You can change the password only after the password passes the verification.
Reset the password	If you forget the password or the SD card is replaced or formatted, you can reset the password. **NOTE:** If the password after the reset is different from the old password, the video and image

Operation	Description
	encrypted using the old password cannot be read unless you change the password back to the old one.

NOTE

- Configurations that have been encrypted for storage cannot be backed up through configuration file management.
- If the system is rolled back to a version that does not support encrypted storage, encrypted data cannot be decrypted.
- In SPC100 and later versions, cameras with light intelligence do not support encrypted storage.

Setting Snapshot File Parameters

This section describes how to configure the path for storing snapshot files and the file storage size.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Local** > **Snapshots**. The **Snapshots** area is displayed, as shown in Figure 1.

   Figure 1 Snapshots area

3. Set snapshot file parameters. Table 1 describes the parameters.

   Table 1 Snapshot file parameters

Parameter	Description
Manual snapshot save path	Path for saving snapshots captured during video viewing on the **View** page. To set a save path, click **Browse** and select a path.
File storage size	Size of local images captured in real time. To save the file storage size setting, click **Save**. **NOTE:** When the size of the local images captured in real time exceeds the value specified by **File storage size**, the earliest images will be deleted.

Parameter	Description
Intelligent snapshot save path	Path for saving images captured in real time. To set a save path, click **Browse** and select a path.

4. Click **Save**.

Configuring Platform Connection

Cameras can connect to video security platforms through the SDK, GB/T 28181, or ONVIF protocol. Each protocol requires a unique set of parameters. After the connection succeeds, you can perform operations on the camera through the platform, for example, viewing live video from the camera, setting camera parameters, and controlling the camera.

Setting Image Parameters

By setting image parameters, you can adjust video images to adapt to different scenarios.

NOTICE

- Image parameters are associated with each other. Set the image parameters strictly based on the site requirements to prevent poor image quality or overexposure.
- Image parameters vary depending on camera models.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Image** > **Display** and use the default value of **Channel**.
3. Set related parameters based on the site requirements. The following describes the parameters.

Image Adjustment

Figure 1 Setting image adjustment parameters



Table 1 Image adjustment parameters

Parameter	Description
Brightness	Brightness of images captured by a camera.
Saturation	Colorfulness of a color relative to its own brightness.
Contrast	Ratio of the luminance of the brightest color (white) to that of the darkest color (black) in the image. • Increasing the contrast improves the image clarity and color brightness. • Decreasing the contrast dims the entire image.
Sharpness	Quality related to the edge contrast of an image and image clarity.

Day/Night Switch

Figure 2 Day/Night switch parameters

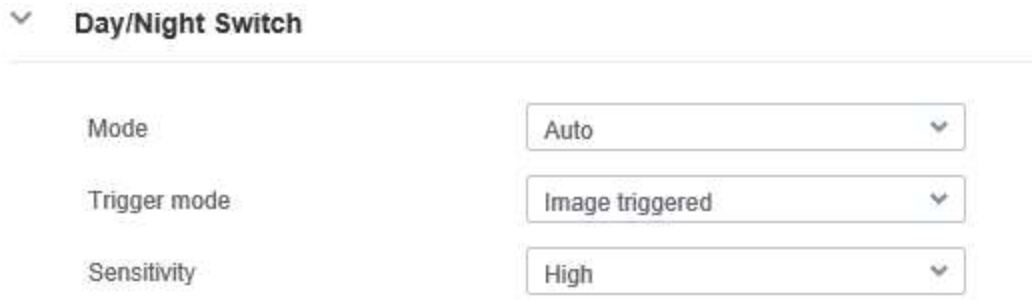


Table 2 Day/Night switch parameters

Parameter	Description
Mode	Day/night mode, which is to help fine-tune the camera's photosensitivity when light conditions change. The options vary depending on the camera model. The options are as follows: • **Auto**: The camera automatically switches between the color mode and the B/W mode based on ambient light conditions.

Parameter	Description
	• **Color**: The camera captures color images. • **B/W**: The camera captures black and white images. • **Scheduled**: You can customize **Nighttime start from** and **Daytime start from**. This mode is applicable to scenarios that require a specified day/night switch time or a unified day/night switch time for multiple cameras.
Trigger mode	Method for triggering switch between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. The options are as follows: • **Triggered by internal signal**: Triggered by image gain. • **Image triggered**: Triggered by visible light brightness of the current image that is analyzed by the camera using the digital photosensitivity algorithm. The triggering modes may vary depending on camera model.
Sensitivity	Sensitivity for switching between the color mode and the B/W mode. This parameter is available only when you set **Mode** to **Auto**. A higher sensitivity indicates higher flexibility to switch between the B/W mode and the color mode. The value defaults to **High**.

Exposure

The following figures show exposure parameters. The exposure parameters vary depending on the camera model.

Figure 3 Exposure parameters in aperture priority mode

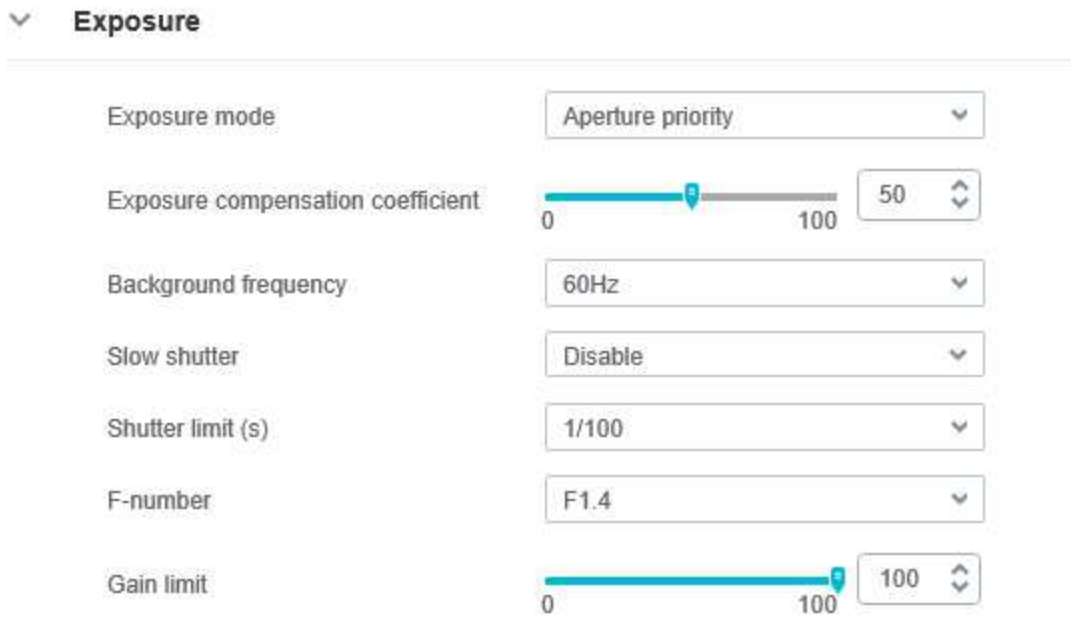


Figure 4 Exposure parameters in manual exposure mode



Figure 5 Exposure parameters in auto exposure mode



Table 3 Exposure parameters

Parameter	Description
Exposure mode	You can select an exposure mode based on the site requirements. The options are as follows: • **Auto** (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. • **Aperture priority**: The camera automatically selects a shutter speed and gain to match the manually specified aperture value. This mode is used to shoot static objects. • **Manual**: You manually set the shutter speed and gain when the auto exposure mode cannot meet the site requirements.
Exposure compensation coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure

Parameter	Description
	meter, in consideration of factors that may cause the indicated exposure to result in a less-than-optimal image. In poor light conditions, you can increase the exposure compensation coefficient to improve image brightness.
Shutter speed	This parameter is available only when you set **Exposure mode** to **Manual**. A larger value of this parameter indicates a longer exposure time.
Background frequency	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The value defaults to **Disable**. A flashing background environment influences the image quality. To obtain high-resolution images, you can set the background frequency to suit lighting conditions. Select a proper background frequency based on the standard frequency of the power grid. Disable the background frequency in natural light conditions.
Shutter limit (s)	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. This parameter is used to specify the minimum shutter speed. You can use the common values or customize values (unit: μs).
F-number	This parameter is available only when you set **Exposure mode** to **Manual** or **Aperture priority**. The default value is **F1.6**.
Gain limit	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC).

Parameter	Description
	In the case of low illumination conditions, the AGC can be enhanced to improve image brightness. However, a high level of AGC will increase the image noise and degrade the image quality. Set this parameter based on the site requirements.
Gain	This parameter is available only when you set **Exposure mode** to **Manual**. The value defaults to **0**.
Slow shutter	You are advised to enable the slow shutter in color mode. This function is disabled by default.

Focus

Figure 6 Focus parameters



Table 4 Focus parameters

Parameter	Description
Focus mode	You can select a focus mode based on the site requirements. The options are as follows: • **Auto**: The camera automatically detects the current scene. If the scene changes, the camera automatically refocuses to ensure that the objects to shoot are clear in the image. The **Sensitivity** parameter is available only when you set **Focus mode** to **Auto**. The default value of **Sensitivity** is **Low**.

Parameter	Description
	• **Manual**: When this option is selected, the camera locks the focus for the current scene. In this case, the focus cannot be automatically adjusted after zooming in or out. You can only manually adjust the focus by clicking the focus icons (). • **Semi-auto** (default): When this option is selected, the camera automatically focuses on the current scene after zooming in or out (). However, when the scene is out of focus, the camera does not automatically refocus. You need to manually adjust the focus by clicking the focus icons (Focus+/-:  ; OnePush focus: ). **NOTE:** • If you click a zoom button on the PTZ control panel, the camera automatically refocuses as the scene changes. • If you click a focus button on the PTZ control panel, the camera locks the focus for the current scene and does not refocus when the scene changes.
Min. focus distance	The camera preferentially focuses on objects outside the minimum focus distance. **NOTE:**

Parameter	Description
	If the distance between the camera and an object is smaller than the value of **Min. focus distance**, the focus may be unclear.
Focus compensation	This function prevents the focus changes after the switch between the color mode and the B/W mode, ensuring that the objects to shoot are clear in the image.

Backlight

Table 5 Backlight parameters

Parameter	Description
BLC/WDR/HLC	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority**. • **Wide dynamic range**: This function is used to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. • **Highlight compensation**: This function is used to suppress large halo or image blur caused by directly radiated strong light by darkening the over-bright areas and brightening the dark areas to adjust the overall video brightness to normal. • **Backlight compensation**: This function is used to correct the exposure of objects in front of a bright light source. • **Backlight adaptation**: This function is used to correct the exposure of objects in front of a bright light source.

Parameter	Description
BLC area	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Backlight compensation**. Backlight compensation is used to correct the exposure of objects in front of a bright light source.
WDR coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Wide dynamic range**. A larger value of WDR coefficient indicates brighter backlit area in the image. The default value is **50**. WDR is intended to provide clear images when there are very bright and very dark areas simultaneously in the camera's field of view. **NOTE:** You are advised not to enable the WDR function in scenarios with direct light radiation, for example, squares with road lamps (such as high-voltage sodium lamps and illuminators) at night.
HLC coefficient	This parameter is available only when you set **Exposure mode** to **Auto** or **Aperture priority** and **WDR/HLC/BLC** to **Highlight compensation**. The value defaults to **2**. A larger HLC coefficient indicates more powerful highlight compensation.

White Balance

Figure 7 White balance parameters



Table 6 White balance parameters

Parameter	Description
Mode	White balance adjusts the color circuit within a camera to remove color cast and ensure accurate color reproduction in various lighting conditions. For example, with a yellow light source, images appear yellowish. After proper white balance adjustment, the original color is reproduced. The options are as follows: • **Auto** (default): This option is recommended. The camera automatically adjusts the red and blue offsets in environments where the color temperature ranges from 2500 K to 10,000 K. Video images may be bluish in the morning or at dusk. You can drag the slider to change the values of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Manual**: The red and blue offsets must be adjusted manually. You can drag the slider to change the values of **Red gain** and **Blue gain** or specify an integer in corresponding text boxes. • **Auto tracking**: The camera automatically adjusts the upper and lower limits of the color temperature in environments where the color temperature ranges from 1000 K to 15,000 K.

Parameter	Description
	• **One push**: This mode allows you to set the white balance mode in the current scene as the fixed mode for all scenes. Only a re-configuration can change the white balance mode. • **Indoor**: The camera automatically adjusts the red and blue offsets in indoor environments where tungsten lamps or incandescent lamps are used and the color temperature ranges from 2500 K to 5500 K. • **Outdoor**: This mode is applicable to sunny environments where the color temperature ranges from 5500 K to 6500 K. • **Fixed sodium lamp**: This mode is applicable to environments where sodium lamps are used and the color temperature ranges from 2000 K to 2300 K. • **Fluorescent lamp 1**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 2500 K to 3500 K. • **Fluorescent lamp 2**: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 3500 K to 4500 K. • **Incandescent lamp**: This mode is applicable to environments where incandescent lamps are used and the color temperature ranges from 2700 K to 2900 K. • **Sunlight**: This mode is applicable to environments where green plants occupy more than 80% of the video image. This mode can alleviate the phenomenon that the white area appears reddish in this scenario.

Image Enhancement

The image enhancement functions vary depending on the camera model.

Figure 8 Overcast adaptation mode



Table 7 Image enhancement parameters

Parameter	Description
Defogging	This function is used to increase the image clarity in poor weather conditions such as rain, fog, and smog. After the function is enabled, the camera determines whether to enable the defogging function based on the actual environment conditions. You can set the defogging level when this parameter is set to **Manual**. A higher defogging level indicates clearer images. However, a too high level will lead to image distortion. You need to set the defogging level based on the site requirements. **NOTE:** • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements.

Parameter	Description
Electronic image stabilization	Indicates whether to enable electronic image stabilization (EIS). EIS is used to compensate image vibration reversely to stabilize images when the camera is subject to vibrations, while some image details may be lost. The value defaults to **Disable**. In a short-focus scenario, if there are many moving objects, the camera may make misjudgment. Therefore, you are advised to enable this function in long-focus scenarios. When **Electronic image stabilization** is set to **Enable**, **Image stabilization sensitivity** can be set for some camera models, which is subject to the GUI. Higher sensitivity indicates better image stabilization effect. Set **Image stabilization sensitivity** based on the site requirements. **NOTE:** • When two or more of the corridor mode, electronic image stabilization, and defogging mode are enabled, the performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering. You need to set related parameters based on the site requirements. • Enabling the electronic image stabilization function will slightly influence camera's field of view. For PTZ dome cameras, the PT speed at level 10 when this function is enabled differs from that when the function is disabled.
Denoising	Indicates whether to enable the noise reduction function. The options are as follows: • **Disable**: Disable the noise reduction function. • **Common mode** (default): In this mode, you can set **Noise reduction level**. A higher noise

Parameter	Description
	reduction level indicates better noise reduction effect but lower image clarity. The value defaults to **50**. • **Expert mode**: In this mode, you can set **Temporal denoising level** and **Spatial denoising level**. ▪ **Spatial denoising level**: Spatial noise reduction intends to reduce the noises on images horizontally and vertically at the cost of some edge details. A higher spatial noise reduction level indicates better noise reduction effect and smoother edges. ▪ **Temporal denoising level**: Temporal noise reduction intends to reduce the white noises distributed randomly between video frames to improve the image quality in low-light conditions. However, the noise reduction effect is affected by historical frame data, causing object trailing on images. A higher temporal noise reduction level indicates better noise reduction effect but more apparent trailing.
Gamma correction	This function is used to adjust and improve the image contrast to avoid new image noise.

Illuminator Control

Table 8 Illuminator control parameters

Parameter	Description
Intelligent Infrared	If this parameter is selected, the infrared illuminator is enabled to avoid image overexposure. The function is enabled by default.
Intelligent infrared level	The default value is **50**. If overexposure occurs in scenarios with strong reflective objects such as

Parameter		Description
		leaves and wires nearby, you can set this parameter to a larger value.
Built-in light	Control mode	• **Auto** (default): Indicates that the camera automatically turns on or off the illuminator and controls its illuminance. • **Manual**: Indicates that the brightness can be manually controlled. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the illuminator will be turned off. • **Scheduled**: Indicates that the illuminator is automatically enabled and disabled at the specified time. You can customize **Turn on time**, **Turn off time**, and **Brightness control**. **NOTE:** In manual mode, the device determines whether to turn on the white-light illuminator based on the ambient luminance. The user-defined brightness takes effect only when the device determines that the white-light illuminator needs to be turned on.
	Low beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the low beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the low beam.

Parameter		Description
		NOTE: ▪ If **Mode** under **Day/Night Switch** is set to **Color**, white-light illuminator control is supported; if **Mode** is set to **B/W**, infrared illuminator control is supported. ▪ In alert mode, after the infrared illuminator is turned on at night, the white light illuminator will flash when an object intrudes into the detection area without the need to switch the day/night mode.
	High beam	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. • If **Control mode** is set to **Manual**, you need to customize **Brightness control**. A larger value indicates higher illuminator brightness. If **Brightness control** is set to **0**, the high beam will be turned off. • If **Control mode** is set to **Scheduled**, you need to customize **Turn on time**, **Turn off time**, and **Brightness control** for the high beam. **NOTE:** If **Mode** under **Day/Night Switch** is set to **Color**, high beam control does not take effect.
	Brightness control	This parameter is available only when **Control mode** is set to **Manual** or **Scheduled**. A larger value indicates higher illuminator brightness.

Digital Zoom

Table 9 Digital zoom function

Digital zoom	You can select **Enable** from the drop-down list box to enable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the system will perform digital zoom and continue to zoom in on the image. However, the focal length is not changed.
	You can select **Disable** from the drop-down list box to disable the digital zoom function. In the PTZ control panel on the **View** page, you can click  to adjust the optical zoom ratio to the maximum. Then if you continue to click this button, the image is not changed.

Obtaining Streams Through RTSP

Users can enter a corresponding URL on the VLC media player to obtain live video streams of a camera through RTSP.

NOTICE

- The VLC media player cannot request streams using RTSP in Digest_SHA256 authentication mode.
- For details about how to change the authentication mode in the RTSP protocol, see Configuring Connection to the Platform Through RTSP.

Solution

1. Log in to the camera web system.
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Second Protocol Parameters** > **ONVIF**. Check the value of **Authentication mode**.
    - If **Authentication mode** is set to **None**, authentication is not needed when requesting data streams through RTSP. Table 1 lists the URL for requesting streams through RTSP.

      Table 1 Requesting streams through RTSP in the case of no authentication

Request Content	Stream Request URL
Live video stream	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=1
Metadata	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=4
Live video stream +	rtsp://*IP address*:*RTSP port number*/LiveMedia/ch1/Media1

Request Content	Stream Request URL
metadata	

In the preceding URLs, ***IP address*** indicates the camera IP address, ***RTSP port number*** is the same as that set under **Configuration** > **Network** > **Basic Settings** > **Port** in the camera web system, **Media1** indicates the primary stream. To obtain the secondary stream, change **Media1** to **Media2**.

- If **Authentication mode** is not set to **None**, authentication is needed when requesting data streams through RTSP. Table 2 lists the URL for requesting streams through RTSP.

  Table 2 Requesting streams through RTSP in the case of authentication

Request Content	Stream Request URL
Live video stream	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=1
Metadata	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1/trackID=4
Live video stream + metadata	rtsp://*User name*:*Password*@*IP address*:*RTSP port number*/LiveMedia/ch1/Media1

  The default user name is **admin**.

To set the authentication password, choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection** > **Password Management** > **ONVIF Password**.

Configuring Head Counting

With the head counting function, the camera can collect the number of persons entering and leaving a specified area such as a shopping mall, supermarket, chain store, exhibition hall, or museum, and generate statistical reports. When the number of persons entering and leaving a detection area exceeds the preset threshold, an alarm is generated. This helps enhance the anomaly handling efficiency.

Setting Head Counting Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Head Counting** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling head counting

3. Click **Settings** next to **Head Counting**. The configuration page is displayed.
4. Set head counting parameters, as shown in Figure 2. Table 1 describes the parameters and buttons.

   The web page varies depending on the camera model.

   Figure 2 Configuring head counting

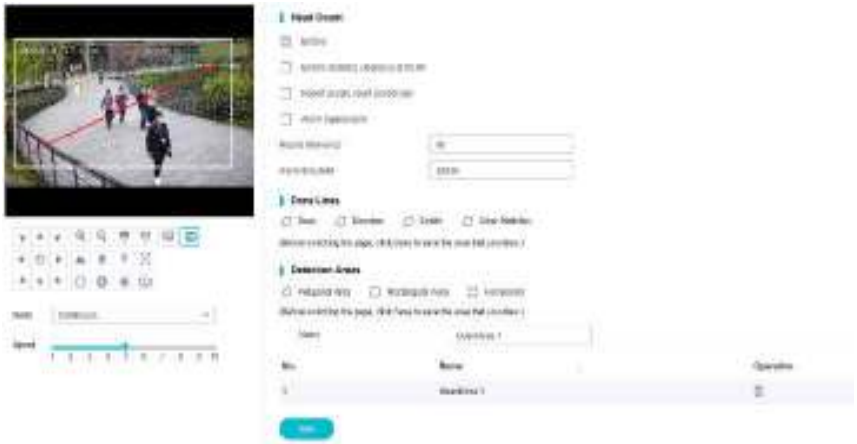
   

Table 1 Parameter description

Parameter	Description
Enable statistics clearance at 00:00	Indicates whether to clear the head counting statistics at 00:00 every day.

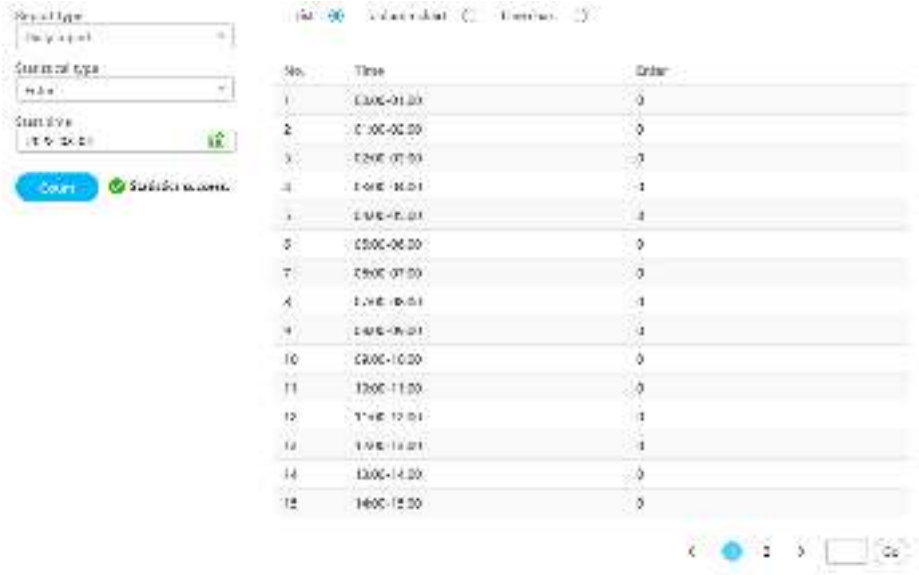
Parameter	Description
Report people count periodically	Interval at which the device collects statistics on the number of people entering and leaving the detection area and the total number of people entering and leaving the area up to the current time, and reports the statistics to the platform.
Alarm suppression	If this parameter is selected, an alarm is generated only when the number of detected persons reaches the alarm threshold and the number of persons continues to increase.
Report interval (s)	Reporting interval, which is available only when **Report people count periodically** is selected.
Alarm threshold	Head counting alarm threshold. When the total number of persons exceeds the value of this parameter, an alarm is generated.
Draw	Used to draw a detection line. After you click **Draw**, the pointer changes to a cross. Draw a line with an arrow for detection.
Direction	Used to draw the direction of entering the detection area. The arrow points to the direction of entering the area.
Delete	Used to delete the drawn detection line.
Clear Statistics	Used to set the number of persons entering and leaving detection areas to zero.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. You can click **Polygonal Area**, **Rectangular Area**, or **Full Screen** to draw a detection area. After the detection area is drawn, the system detects only the number of persons entering or leaving the detection area. If the number reaches the alarm threshold, the system generates an alarm. If you do not draw a detection area, the full image is used as the detection area.

5. Click **Save**.

Viewing Head Counting Results

1. Click the **Head Counting** tab. The **Head Counting** tab page is displayed, as shown in Figure 3.

Figure 3 Viewing head counting results



2. Set related parameters. Table 2 describes the parameters.

Table 2 Head counting parameters

Parameter	Description
Report type	Type of the report. You can view daily, weekly, monthly, and annual reports as required.
Statistical type	Type of the data to view. You can view the number of people entering or leaving the detection area as required.
Start time	For a daily report, statistics are collected from 00:00 to 24:00 on the specified day. For a weekly report, statistics are collected from Monday to Sunday of the specified week. For a monthly report, statistics are collected from the first day to the last day of the specified month. For an annual report, statistics are collected from January 1 to December 31 of the specified year.
List/Column chart/Line chart	Mode in which the statistical result is displayed.

3. Click **Count**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported

to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 4.

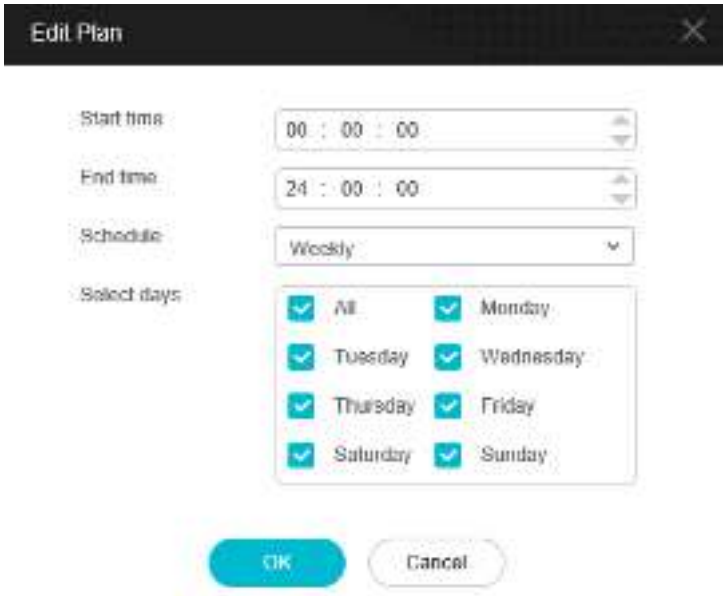
   Figure 4 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 5.

   Figure 5 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by

intelligent services.

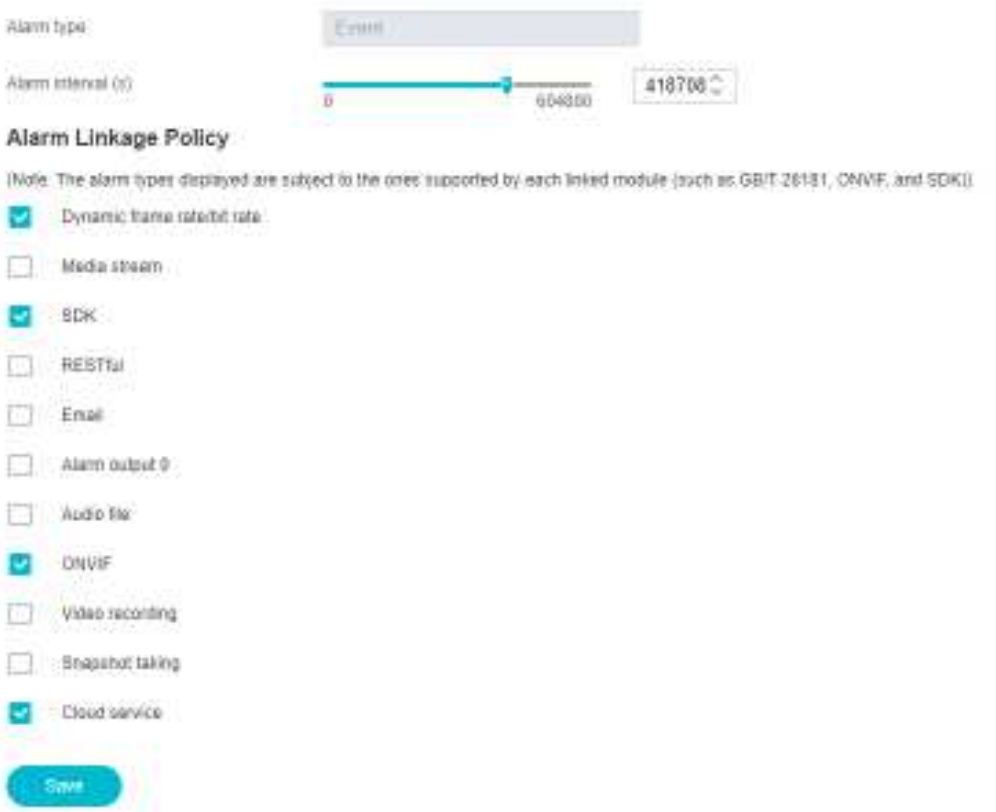
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 6.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 6 Configuring alarms



2. Set related parameters. Table 3 describes the parameters.

Table 3 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of

Parameter	Description
	the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

You can use either of the following methods to check whether the configuration is successful:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether head counting alarms are reported.

- Configure a head counting OSD and view head counting statistics on the live video image.

    1. Choose **Configuration** > **Image** > **OSD**.
    2. Add a head counting OSD, as shown in Figure 7.

       Figure 7 OSD configuration page

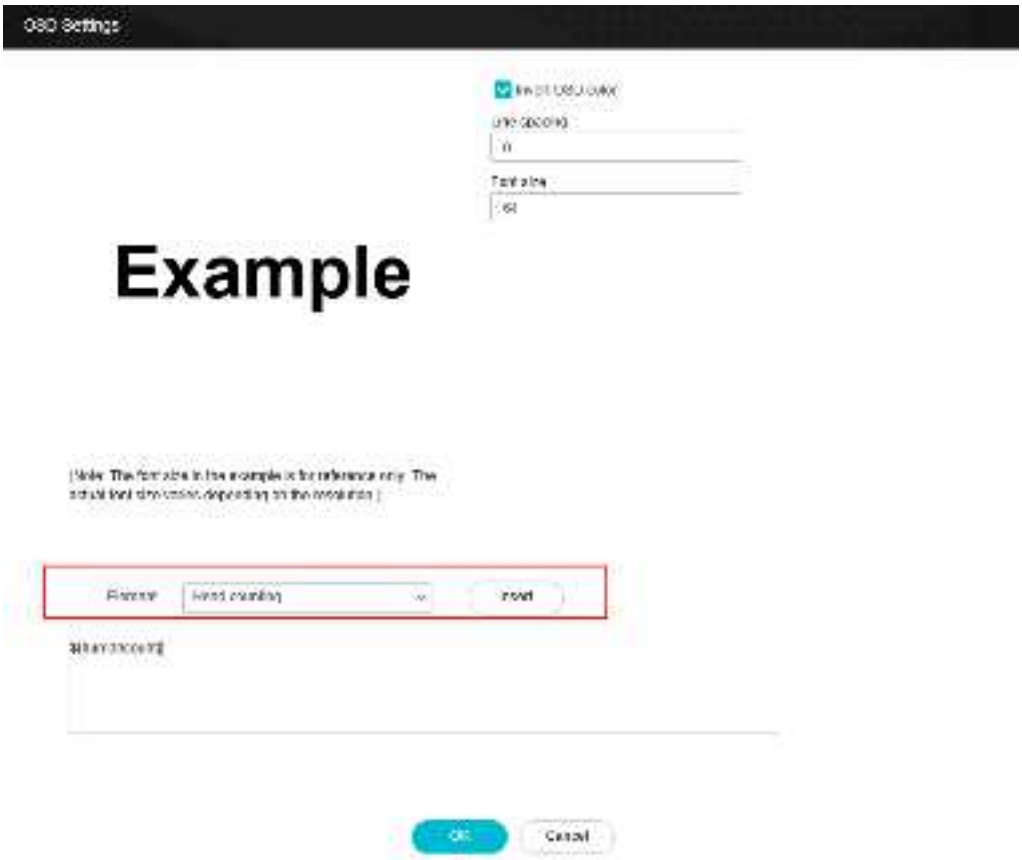
       

        a. Click **Add OSD**.

        b. Click . The **OSD Settings** dialog box is displayed, as shown in Figure 8.

           Select **Head counting** from the **Element** drop-down list box. Enter the OSD text in the text box below (for example, **Customer flow statistics**) and click **OK**. After the configuration is complete, if the head counting function is enabled, the head counting information is displayed on the video image. For details about other parameters, see Setting OSD Parameters.

Figure 8 Adding a head counting OSD



c. Select the OSD to be displayed.

3. Click **Save**.
4. Check the configuration result.

   Go to the **View** page to view the live video. The system automatically collects statistics on the number of people entering and leaving the detection area and displays the number on the image, as shown in Figure 9.

Figure 9 Head counting



Configuring Crowd Density Detection

A camera can detect the headcount and crowd density in an image and generate alarms based on the preset threshold. This facilitates emergency handling.

Setting Crowd Density Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Crowd Density Detection** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling crowd density detection

3. Click **Settings** next to **Crowd Density Detection**. The configuration page is displayed.
4. Set crowd density detection parameters, as shown in Figure 2. Table 1 describes the parameters.

   The web page varies depending on the camera model.

   Figure 2 Configuring crowd density detection

   Table 1 Parameter description

Parameter	Description

Parameter	Description
Periodic data reporting	Indicates whether to report data periodically. If this check box is selected, you can set **Data Report Interval (s)**. The camera reports the current crowd density and number of persons to the platform at a specified interval.
Sensitivity	Detection sensitivity. The default value is **3**. A larger value indicates a higher probability to detect targets, but also a higher false positive possibility. The default value is recommended.
Alarm threshold (users)	Alarm threshold. An alarm is generated when the head count in the detection area reaches the alarm threshold.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. After a detection area is drawn, the system detects the crowd density only in the detection area. Only one detection area can be drawn. A detection area supports a maximum of 10 vertexes.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live

Parameter	Description
	video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

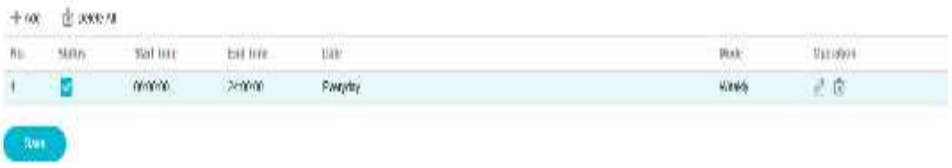
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

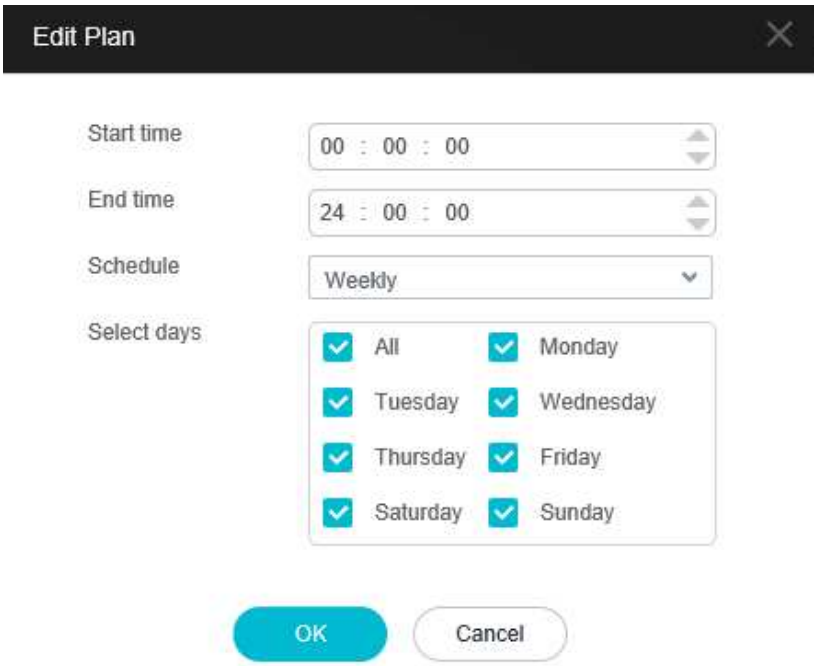
   Figure 3 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

Figure 4 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

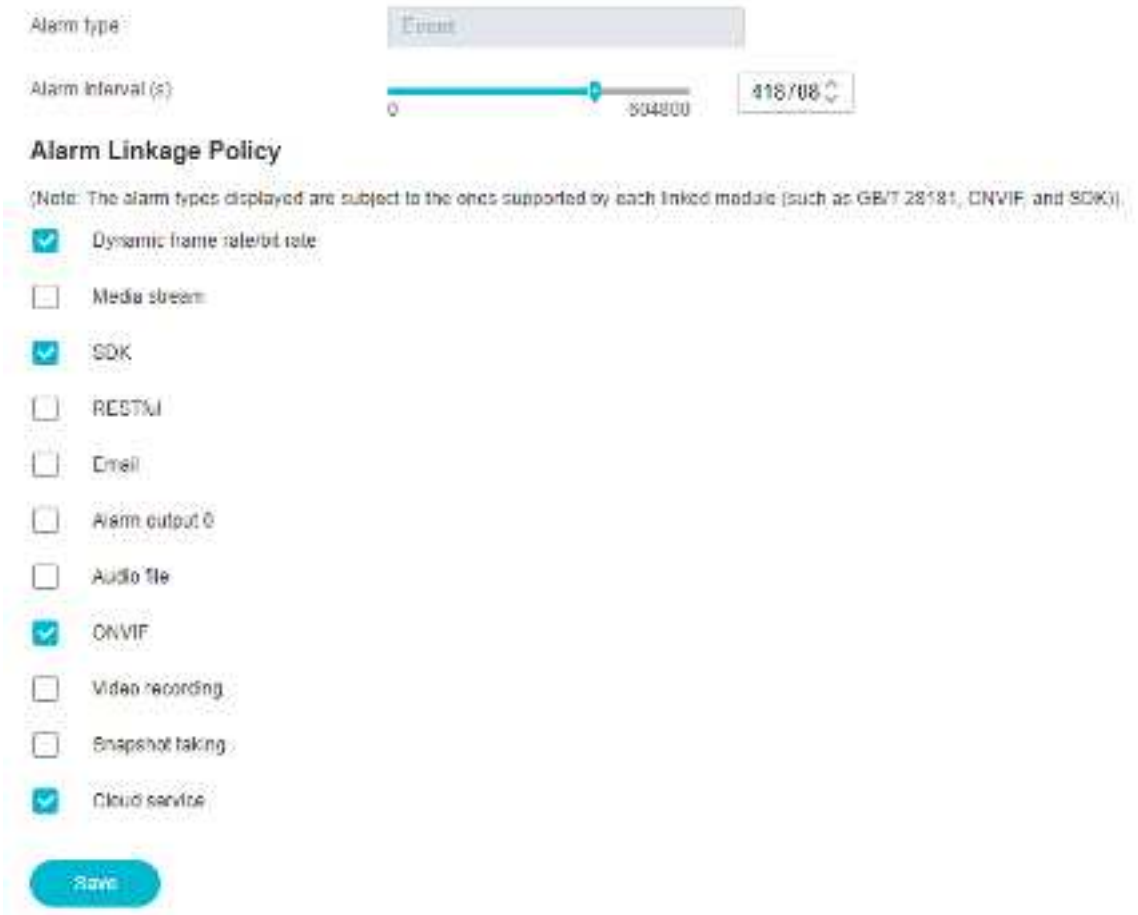
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

The configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether crowd density alarms are reported.

- After the configuration, you can view the crowd density and headcount in real time under **Display** > **Intelligent Detection**, as shown in Figure 6.

  1. Click **Crowd Density**.
  2. Click **Start Metadata Reception** in the lower part of the live video pane.
  3. View the detection result in the upper right corner of the image, including the current number of people and current crowd density.

Figure 6 Crowd Density page



Configuring Queue Length Detection

The camera can identify the number of queuers and queuing time in the image, and generate an alarm based on the preset threshold so that measures can be taken to shorten the queue length in a timely manner.

Setting Queue Length Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Queue Length Detection** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling queue length detection

3. Click **Settings** next to **Queue Length Detection**. The configuration page is displayed.
4. Set queue length detection parameters, as shown in Figure 2. Table 1 describes the parameters.

   The web page varies depending on the camera model.

   Figure 2 Configuring queue length detection

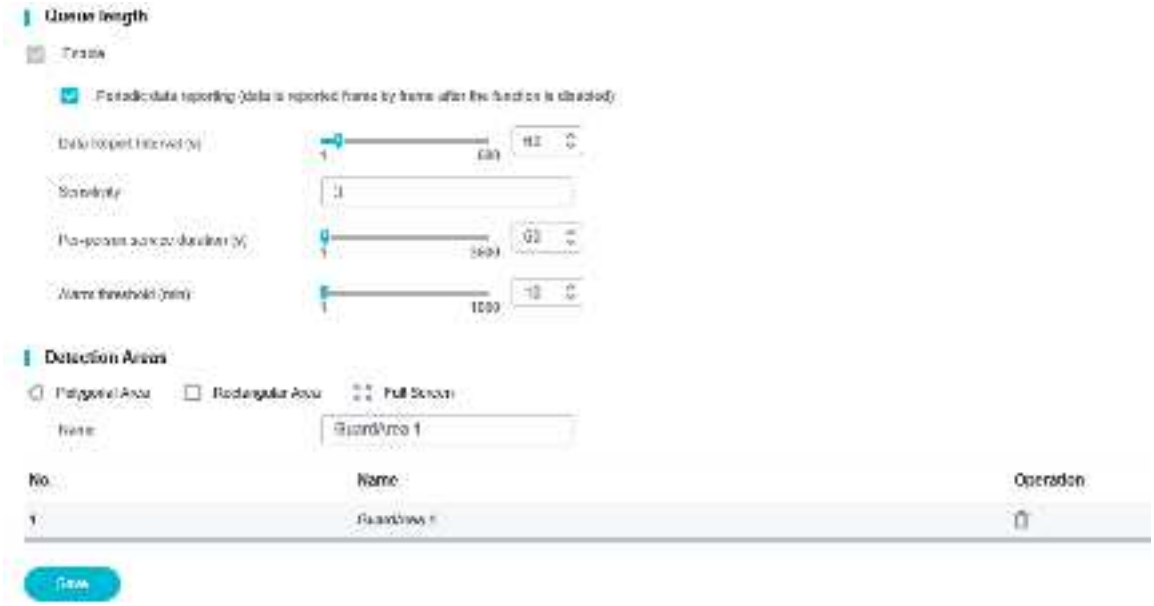
   

Table 1 Parameter description

Parameter	Description
Periodic data reporting	Indicates whether to report data periodically. If this check box is selected, you can set **Data Report Interval (s)**. The camera reports the current queuing duration and number of queuers to the platform at a specified interval.
Sensitivity	Detection sensitivity. The default value is **3**. A larger value indicates a higher probability to detect objects, but also a higher false positive possibility. The default value is recommended.
Per-person service duration (s)	Handling duration of the service (for example, ticket checking) per person. The default value is **60**.
Alarm threshold (min)	Alarm threshold. An alarm is generated when the total queuing duration of a queue in a detection area reaches the alarm threshold.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. After a detection area is drawn, the system detects the queue length only in the detection area. Only one detection area can be drawn. A detection area supports a maximum of 10 vertexes.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area.

Parameter	Description
	• You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location.
Full Screen	Used to designate the entire live video image as the detection area.

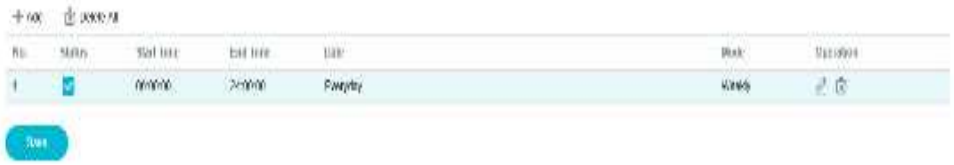
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

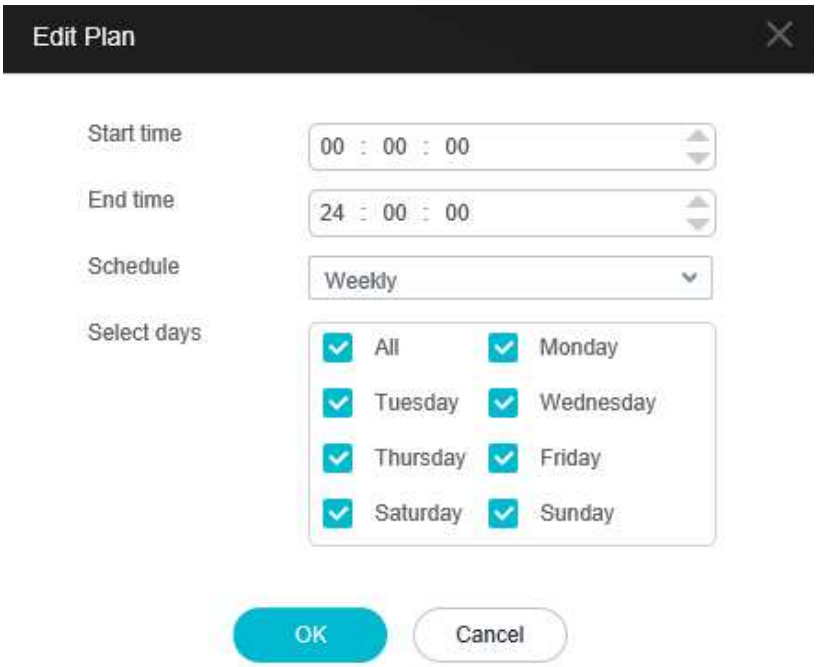
   Figure 3 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

The **Edit Plan** dialog box is displayed, as shown in Figure 4.

Figure 4 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click or in the **Operation** column.
> - At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

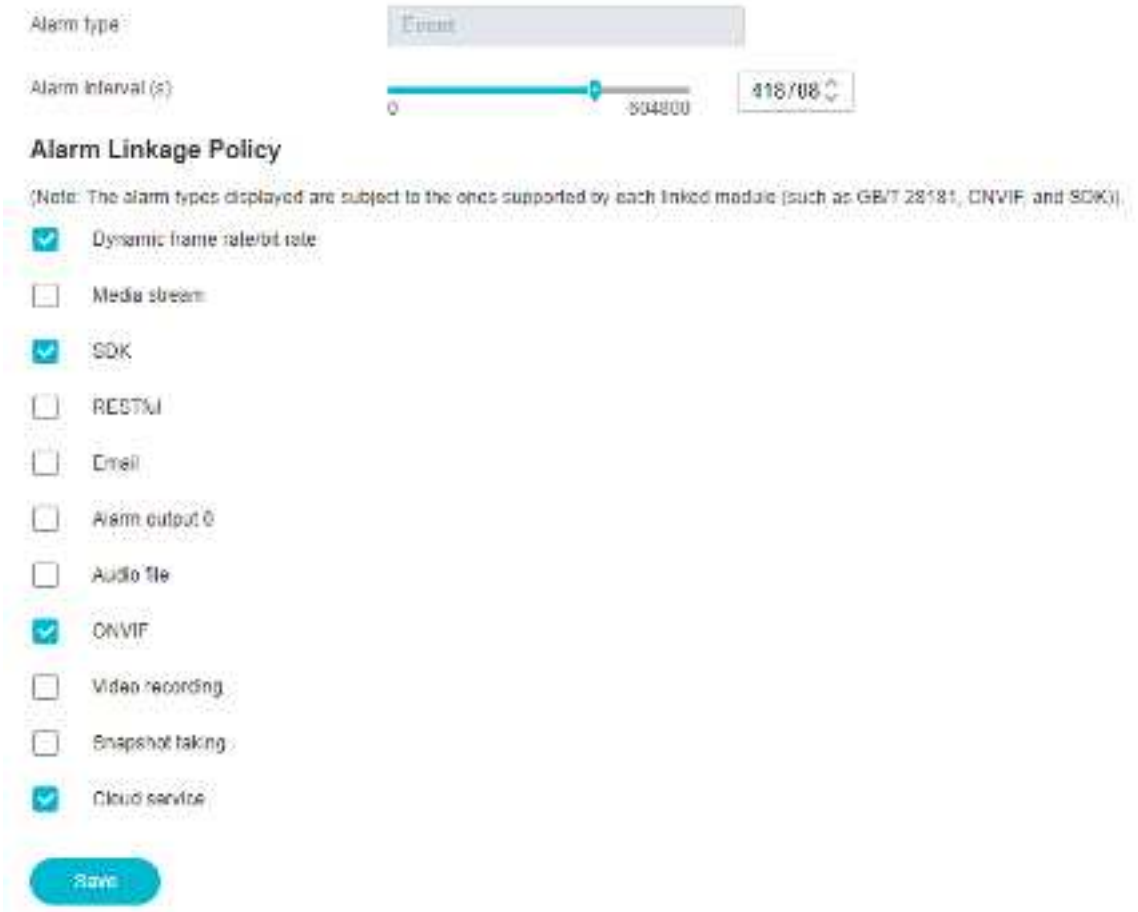
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry

Parameter	Description
	file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm**

Parameter	Description
	Output and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud

Parameter	Description
	service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

The configuration is successful if any of the following conditions is met:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether queue length alarms are reported.

- After the configuration, you can view the queuing duration and number of queuers in real time under **Display** > **Intelligent Detection**, as shown in Figure 6.

  1. Click **Queue Length**.
  2. Click **Start Metadata Reception** in the lower part of the live video pane.
  3. View the detection result in the upper right corner of the image, including the current queuing duration and number of queuers.

Figure 6 Queue Length page



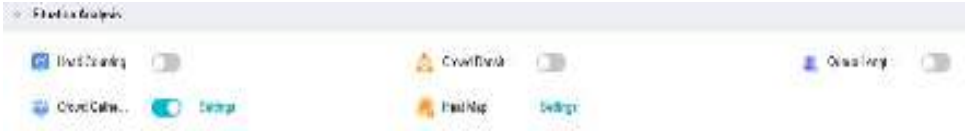
Configuring Crowd Gathering Detection

With the crowd gathering detection function, the camera can identify crowd gathering and generate an alarm promptly to improve the exception handling efficiency. This function is applicable only to cameras installed at heights.

Setting Crowd Gathering Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Crowd Gathering** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling crowd gathering detection

3. Click **Settings** next to **Crowd Gathering**. The configuration page is displayed.
4. Set crowd gathering detection parameters, as shown in Figure 2. Table 1 describes the parameters.

   The web page varies depending on the camera model.

   Figure 2 Configuring crowd gathering detection

   Table 1 Parameter description

Parameter	Description

Parameter	Description
Sensitivity	Detection sensitivity. The value is an integer ranging from 1 to 100. The default value is **50**. A larger value indicates a higher probability to trigger alarms.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. After a detection area is drawn, the system detects crowd gathering only in the detection area. If multiple detection areas are configured, the system generates an alarm if one of the detection areas meets the alarm condition.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area.

Parameter	Description
	• You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area.

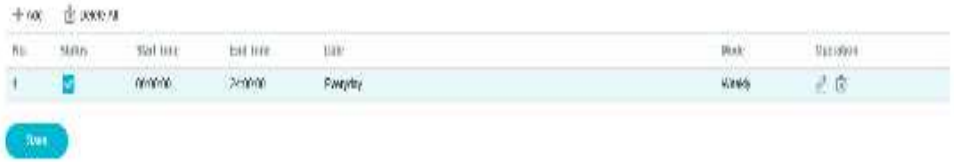
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

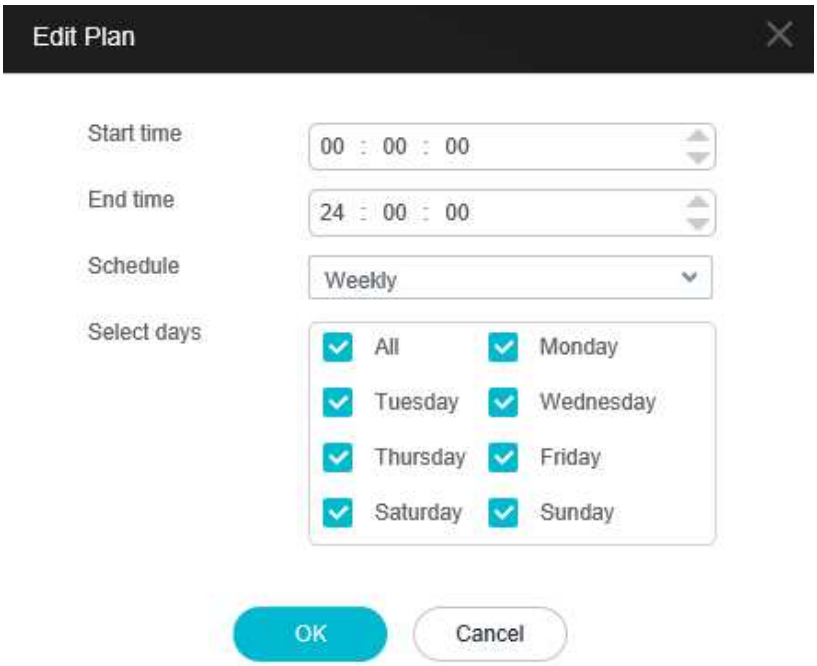
   Figure 3 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

Figure 4 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

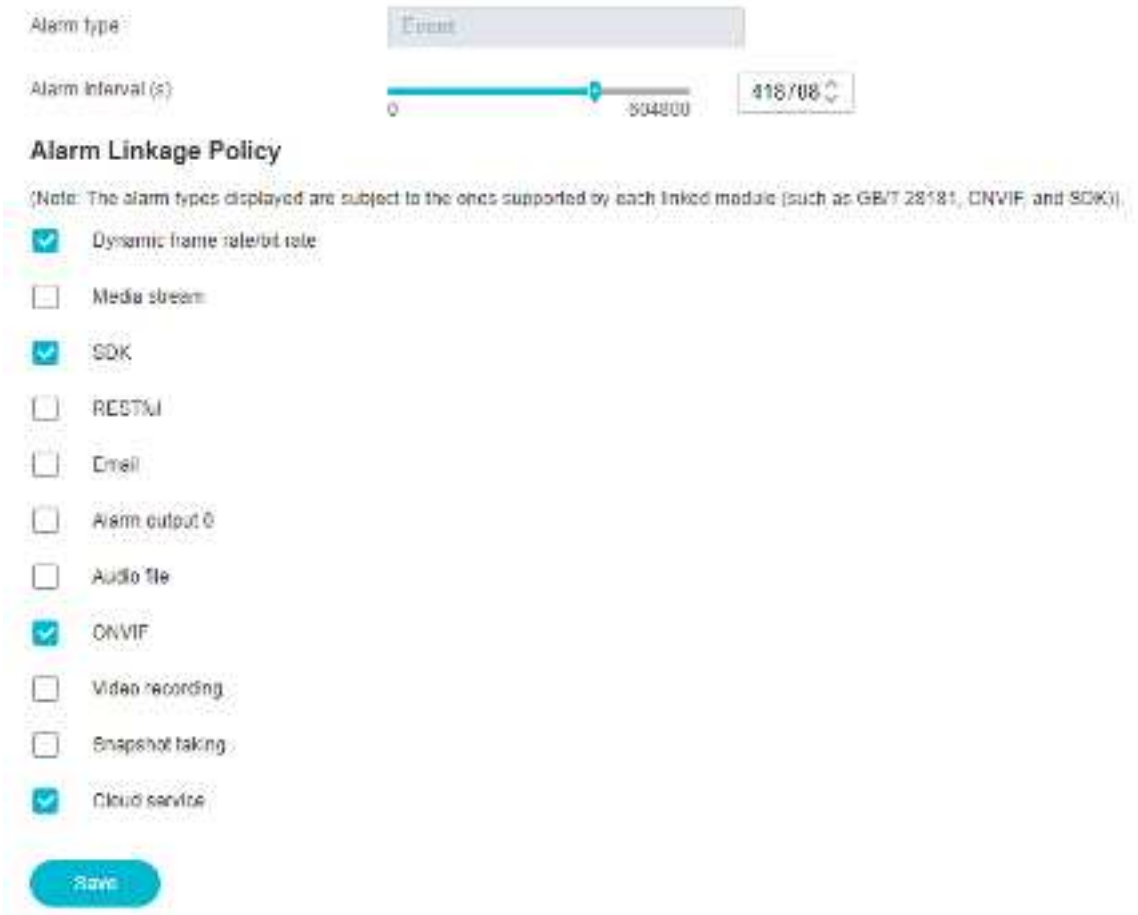
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log level** to **Warning** under **Log Query**, and check whether crowd gathering alarms are reported.

Configuring Absence Detection

With the absence detection function, the camera can calculate the number of absent persons in the preset detection area and generate an alarm based on the predefined detection requirements.

Setting Absence Detection Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Off-Duty Detection** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling absence detection

3. Click **Settings** next to **Off-Duty Detection**. The configuration page is displayed.
4. Set absence detection parameters, as shown in Figure 2. Table 1 describes the parameters.

   The web page varies between camera models.

   Figure 2 Setting absence detection parameters

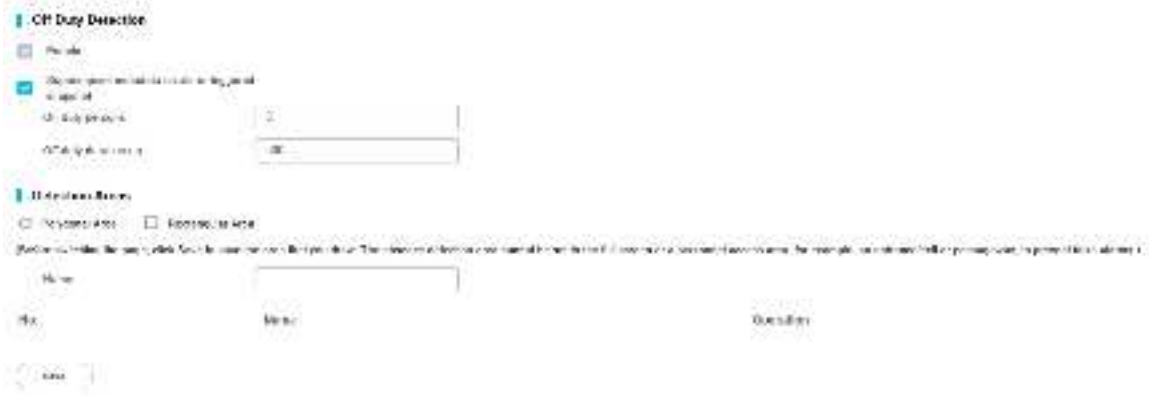
   

   Table 1 Parameter description

Parameter	Description
Enable	Indicates whether to enable absence detection. This check box is selected by default and cannot be

Parameter	Description
	deselected.
Superimpose metadata on alarm-triggered snapshot	Indicates whether to superimpose metadata information (such as intelligent analysis rules and results) on alarm-triggered snapshots.
On-duty persons	Number of people who should be on duty in the detection area. The value is an integer ranging from 1 to 5.
Off-duty duration (s)	Interval between the time when absence behavior occurs and the time when an alarm is generated. The value is an integer ranging from 1 to 3600.
Detection Areas	Area containing the buttons for drawing detection areas and the list of detection areas. After a detection area is drawn, the system counts the number of people only in the detection area. Only one detection area can be drawn. A detection area supports a maximum of 10 vertexes.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the

Parameter	Description
	live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, you need to delete this area and click the required drawing button to draw a new area. • You can drag the detection area to change its location.

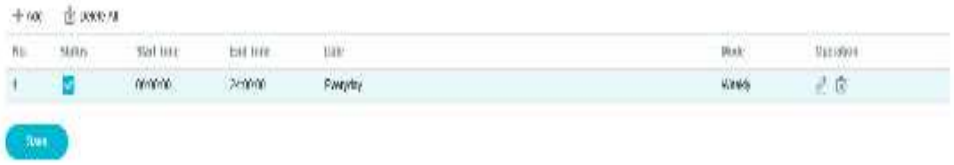
5. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

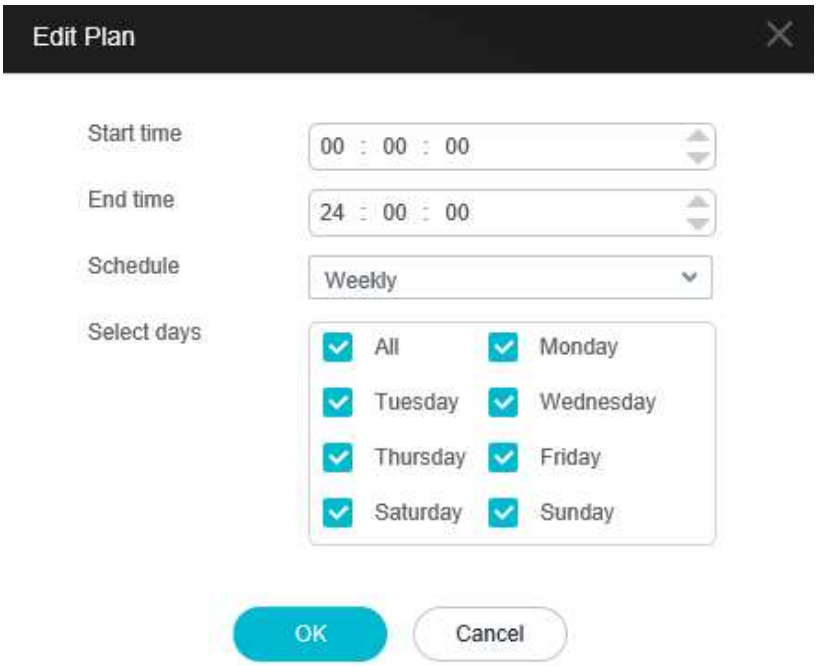
   Figure 3 Alert plan tab page



2. Click **Add**. A new alert plan is displayed. Click in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

Figure 4 Edit Plan dialog box



3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

NOTE

- To modify or delete an existing alert plan, select it and click or in the **Operation** column.
- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

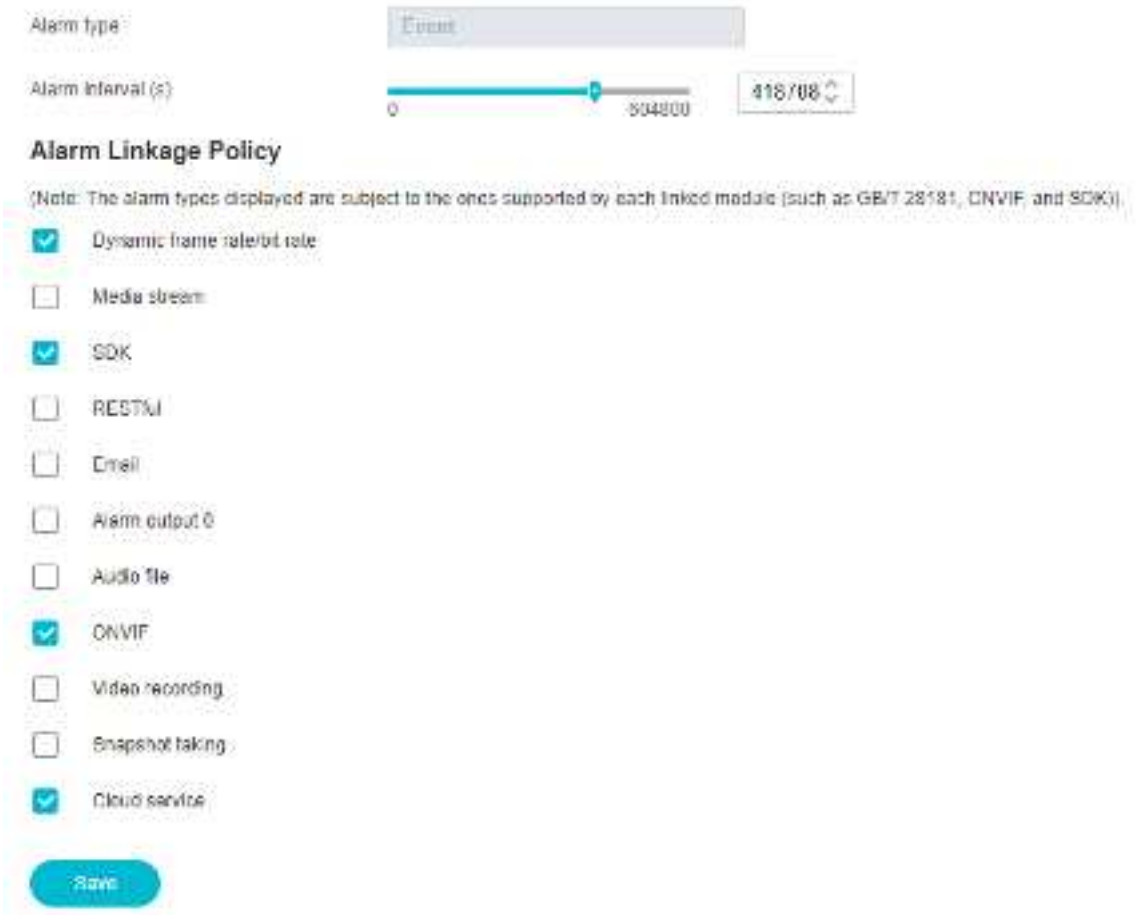
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.

Parameter	Description
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.

Parameter	Description
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.

Parameter	Description
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

You can use either of the following methods to check whether the configuration is successful:

- Check whether alarm logs are generated during the detection. If so, the configuration is successful.

  Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Log type** to **Warning** under **Log Query,** and check whether absence alarms are reported.

- Configure an absence detection OSD and view absence detection statistics on the live video image.

  1. Choose **Configuration** > **Image** > **OSD**.
  2. Configure the absence detection OSD, as shown in Figure 6.

     Figure 6 OSD configuration page

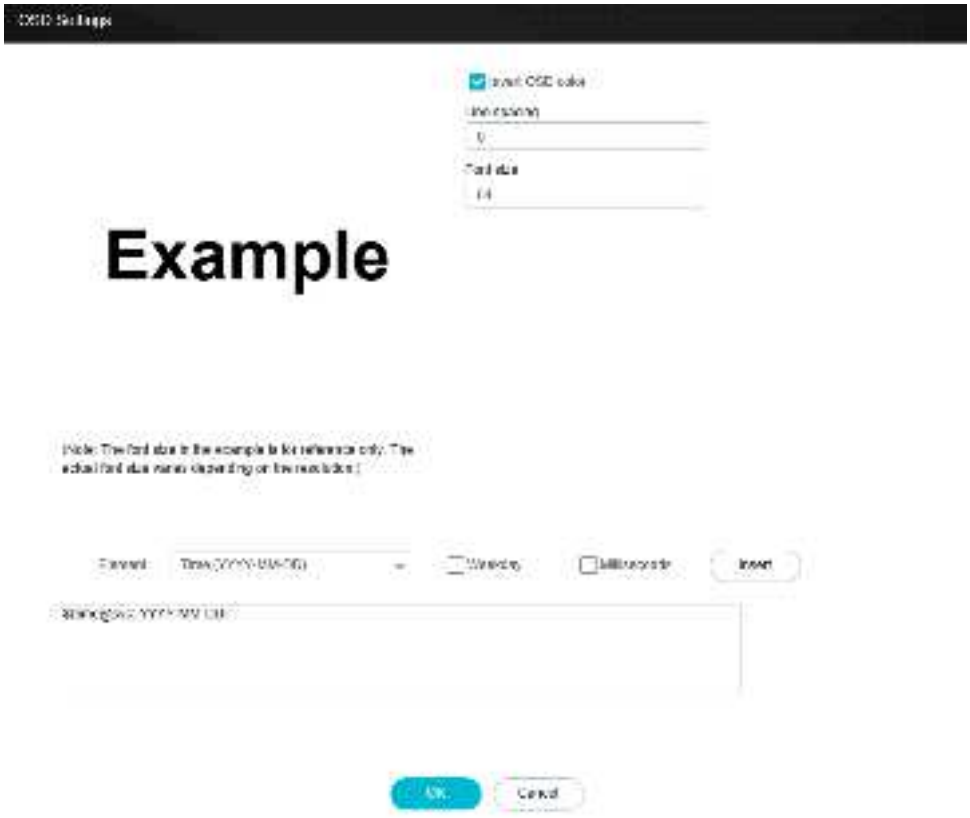
     

     a. Click **Add OSD**.

b. Click . The **OSD Settings** dialog box is displayed, as shown in Figure 7.

   Select **Off-duty detection** from the **Element** drop-down list box. Enter the OSD text in the text box below (for example, **head counting**) and click **Save**. After the configuration is complete, if the absence detection function is enabled, the absence detection information is displayed on the video image. For details about other parameters, see Configuring OSD.

   Figure 7 Configuring absence detection OSD



c. Select the OSD to be displayed.

3. Click **Save**.
4. Check the configuration result.

   Method 1: Go to the **View** page to view the live video. When a person enters or leaves the detection area, check whether the system calculates and displays the number of on-duty persons. If so, the configuration is successful.

Method 2: Choose **Behavior Analysis** and select absence detection on the right. On the page that is displayed, click **Start Metadata Reception** in the lower right corner to enable metadata receiving. Check whether an object is framed by a red box. If so, the configuration is successful.

Configuring Hot Zone Analysis

With the hot zone analysis function, the camera can collect information about customers as well as the popularity of in-store areas.

Application Scenarios

In the retail chain market, the hot zone analysis function and system-collected transaction data can help further indicate trending goods and the sales conversion rate in concerned areas. This helps retailers make store segmentation decisions based on visualized data.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Hot Zone Analysis** in the **Situation Analysis** area, as shown in Figure 1.

   Figure 1 Enabling hot zone analysis

3. Click **Settings** next to **Hot Zone Analysis**. The configuration page is displayed.
4. Set hot zone analysis parameters, as shown in Figure 2. Table 1 describes the parameters.

   Figure 2 Configuring hot zone analysis

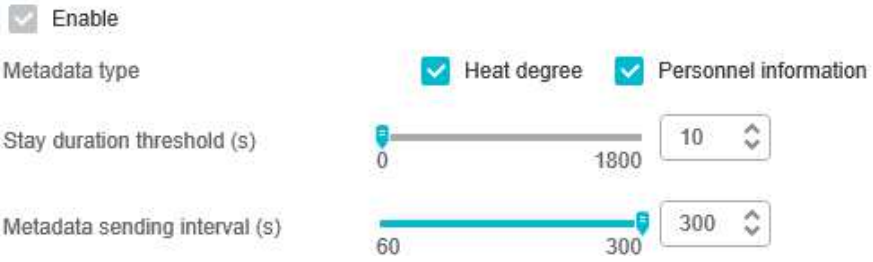
   

   Table 1 Parameter description

Parameter	Description

Parameter	Description
Metadata type	• **Heat degree**: If this check box is selected, popularity information is reported at an interval specified by **Metadata sending interval (s)**. The information includes the heat map of an area in the statistical period, the number of persons that stay in the area, and the average duration during which a person dwells in the area. • **Personnel information**: If this check box is selected, the system reports information such as the time when a person enters or leaves the image view and the duration during which the person dwells in each area.
Stay duration threshold (s)	Only when the duration during which a person dwells in an area is greater than the value of this parameter, the dwelling is taken into account.
Metadata sending interval (s)	Interval at which metadata is sent.

5. Click **Save**.
6. Set and deliver the detection area using third-party software to implement the hot zone analysis function.

Configuring the Heat Map Function

In large-scale scenarios, the crowd distribution varies with time. Some areas are densely populated, while others are sparsely populated. Currently, if the crowd density of an area in different time segments can be intuitively displayed, more business value can be created, or more targeted detection can be provided. The heat map function can help implement these requirements. The camera that integrates the video detection and analysis technologies can detect a specific area and collect statistics on the crowd density (that is, **heat** degree) in the area in different time segments.

Application Scenarios

Large public places, such as shopping malls, central business districts (CBDs), railway stations, parks, and squares

For example, in a large shopping mall, if the historical customer flow data can be analyzed to obtain the crowd density data of each area in different time segments, the management personnel of the shopping mall can know the customer preference. Then they can adjust commodities and advertisements in an area in different time segments to increase the business income.

In a large-scale public place, such as a railway station or a park, if the crowd density data of each area in different time segments is available, more pertinent security measures can be formulated. In this way, safer evacuation routes can be provided when accidents occur.

Restrictions

- **Scenario Restrictions**

  The application scenario shall meet the following conditions:

  - Avoid vibration interference sources near the camera.
  - Avoid dynamic backgrounds, such as waving tree branches and water rippling. Avoid the interference of lightning, shifting between light and shade, specular reflection, harsh weather conditions, and intermittent movement.

- In the camera image, ensure that all moving objects account for less than 20% of the image area. That is, most objects in the image should be static objects.
- Prevent the camera from directly facing a light source, water surface, wall, or other reflection planes.

- **Usage Restrictions**

  The following describes the restrictions for using the heat map function:

  - The camera must be equipped with an available SD card. The heat map data will be stored in the SD card for a maximum of one year.
  - A maximum of eight detection areas are supported. If no area is set, the entire image is the detection area.
  - The alert time is set by day. A maximum of eight time segments can be set on the timeline of the same day. The alert time can be cleared. If the alert time is not set, alert is deployed for the entire day by default.
  - For a PTZ dome camera, the heat map collects statistics only on an area. If the detection area is out of the statistical area after the PTZ device rotates, the heat map stops collecting statistics.
  - When the lens zooms in or out, a certain area deviation may occur. Therefore, the statistics collected may be inaccurate.
  - When the heat map detection area changes, the original heat map data will be cleared. However, the original heat map data is not affected when the heat map function is enabled or disabled, the heat map alert time is adjusted, or basic heat map parameters are modified.
  - The heat map supports a maximum of eight detection areas, and a maximum of 10 vertexes in a single area.

Installation Requirements

To ensure the accuracy of statistics, the camera shall meet the following installation requirements:

- The recommended installation height ranges from 3 m to 6 m. The focal length varies with the camera. Select a proper installation height based on the actual focal length.
- The recommended tilt angle of the camera ranges from 30° and 60°. The optimal tilt angle is about 45°.
- Ensure that the illumination in the detection area is greater than 20 lux.

It is recommended that the camera be able to cover a scenario as wide as possible on the condition that the preceding installation requirements are met.

Setting Heat Map Parameters

1. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Heat Map** in the **Situation Analysis** area. The configuration page is displayed.
2. Select **Enable**.
3. Set heat map parameters, as shown in Figure 1. Table 1 describes the parameters.

   The web page varies between camera models.

   Figure 1 Basic Settings tab page



   Table 1 Parameter description

Parameter	Description
Send metadata	After **Send metadata** is selected, the camera sends heat map data to the backend platform or security center. If data needs to be sent, enable this function.
Rotate to Original Position	For PTZ dome cameras, after you set related parameters and click **Save**, the camera will remember the current image position and use this position as the heat map analysis position. When the PTZ dome camera rotates to another position: • If you do not click **Save** again on the **Basic Settings** tab page, the heat map analysis position does not change. Because the PTZ dome camera has rotated to another position, the heat map data statistics and analysis will be suspended until the PTZ dome camera rotates to the original heat map analysis position. You can also click **Rotate to Original Position** to quickly rotate to the original heat map analysis position. Then the camera will continue the heat map data statistics and analysis. • If you click **Save** again on the **Basic Settings** tab page, the heat map analysis position will change to the current position of the PTZ dome camera and the original data will be cleared. **NOTE:** Only PTZ dome cameras support this function.
Clear Statistics	Used to clear heat map statistics.

4. Draw a detection area.

   You need to draw a detection area based on the site requirements. Then the system performs detection only in the detection area. A maximum of eight detection areas are supported. If no detection area is set, the entire image functions as the detection area. For details about how to draw a detection area and set related parameters, see Table 2.

Table 2 Parameter description

Parameter	Description
Heat Map Area List	Area containing the buttons for drawing detection areas and the list of detection areas. After a detection area is drawn, the system performs detection only in the detection area.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area.

5. Click **Save**.

Configuring an Alert Plan

After setting heat map parameters, you can configure an alert plan to enable the heat map function for a camera during specified time segments.

1. Click the **Alert Plan** tab, as shown in Figure 2.

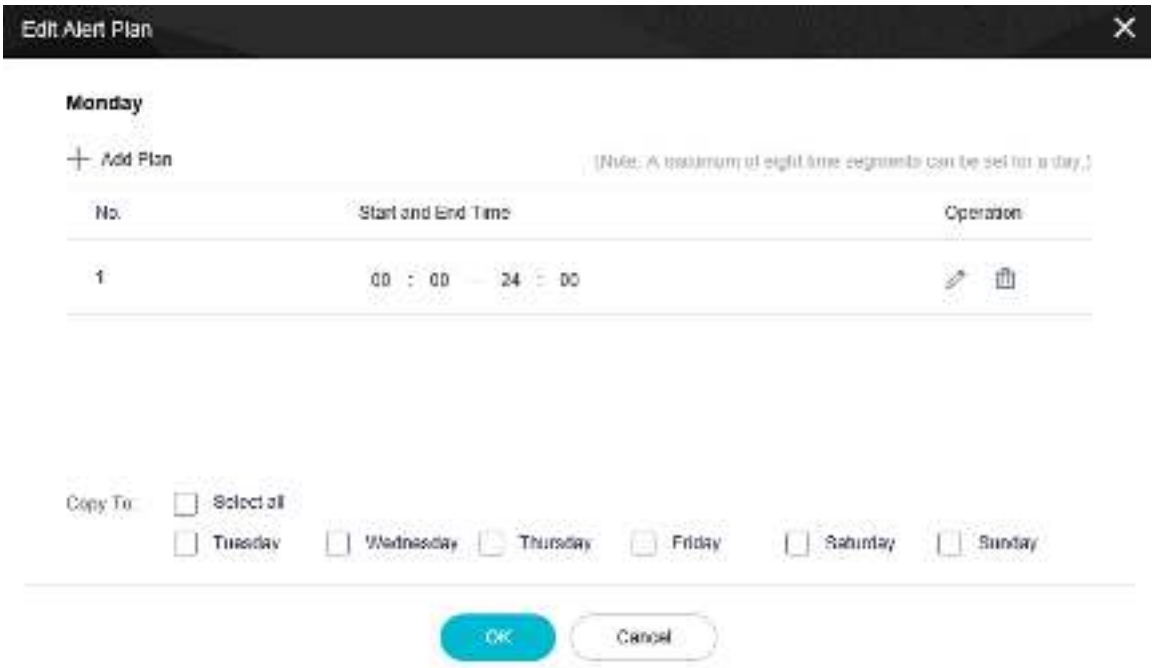
   Figure 2 Alert Plan tab page

2. Configure the time segment during which alert is to be deployed based on the site requirements.

   For example, to allow the function to take effect from 09:00 to 17:00 on Monday for a camera, click on the right of **Monday**. The **Edit Alert Plan** dialog box is displayed, as shown in Figure 3.

Figure 3 Edit Alert Plan dialog box



Click **Add Plan**, set the start time and end time to 09:00 and 17:00 respectively, and click ✓. To copy the alert time to another day, select the day and click **OK**.

Alternatively, you can hold down the left mouse button and drag on the timeline of **Monday** to select the time segments from 09:00 to 17:00 to quickly configure the alert time.

If you click **Reset All**, all alert plans will be reset.

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

Viewing Heat Map Statistics

If the heat map function has been enabled and related configurations have been complete for more than 10 minutes, the camera generates data upon detecting moving objects.

1. Choose **Configuration** > **Intelligence**. Click **Settings** next to **Heat Map** in the **Situation Analysis** area. The configuration page is displayed.
2. Click the **Heat Map Statistics** tab.

3. Set **Report type** and **Start time** and click **Search**. The space heat map and time heat map are displayed on the right, as shown in Figure 4 and Figure 5.

Table 3 Parameter description

Parameter	Description
Report type	Statistical report type. The options are as follows: **Daily report**, **Weekly report**, **Monthly report**, and **Annual report**.
Start time	Statistics start date. The statistical result is also related to the report type. • If **Report type** is set to **Daily report**, the statistical period is the day of **Start time**. • If **Report type** is set to **Weekly report**, the statistical period is the week of **Start time**. • If **Report type** is set to **Monthly report**, the statistical period is the month of **Start time**. • If **Report type** is set to **Annual report**, the statistical period is the year of **Start time**.

Figure 4 and Figure 5 show statistical results.

- Space heat map: indicates the space-based activity level of moving objects in the detection area within the alert period in the week of March 11, 2022, that is from March 7, 2022 to March 11, 2022. The red area indicates the area with the highest density, that is, the highest activity level of moving objects. The blue area indicates the area with the lowest density, that is, the lowest activity level of moving objects.
- Time heat map: indicates the time-based activity level of moving objects in the detection area within the alert period in the week of March 11, 2022, that is from March 7, 2022 to March 11, 2022. A larger value indicates a higher activity level.

  On the **Time Heat Map** tab page, you can click **Export** on the right to export the time heat map to a .csv file.

Configuring Automatic Tracking

This section describes the application scenario, camera installation requirements, and configuration procedure of automatic tracking.

The camera that supports automatic tracking provides the following functions:

- The camera can detect moving objects (such as motor vehicles, non-motorized vehicles, and pedestrians) that appear in the image and automatically track the objects.
- On the **View** page, if you click the manual tracking icon, the camera will detect moving objects that appear in the image. If you manually select an object, the camera will automatically track the object.

Application Scenarios

The automatic tracking function enables the camera to identify and track a specified object within the image view. This function is applicable to the following scenarios:

- Large-scale places such as airports, harbors, and squares.
- Campus perimeter detection scenarios. The camera detects moving objects through the object classification function and then automatically tracks the objects. Additionally, the focal length can be increased to enable the camera to clearly record features of suspects, their behavior in the detection area, and their movement directions.

Supported Model

PTZ dome camera

Installation Requirements

During the installation, the following requirements must be met:

- The recommended installation height is greater than 5 m. The focal length varies depending on cameras. Select a proper installation height based on the actual focal length.

- Ensure that the illumination in the detection area is greater than 20 lux.

Setting Automatic Tracking Parameters

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Intelligence**. Toggle on **Auto Tracking** in the **Tracking Intelligence** area, as shown in Figure 1.

   Figure 1 Enabling automatic tracking

3. Click **Settings** next to **Auto Tracking**. The **Auto Tracking** page is displayed, as shown in Figure 2.

   The web page varies depending on the camera model.

   a. Select **Enable** to enable automatic tracking.

   b. Set **Auto tracking duration (s)** and click **Save**.

Figure 2 Configuring automatic tracking

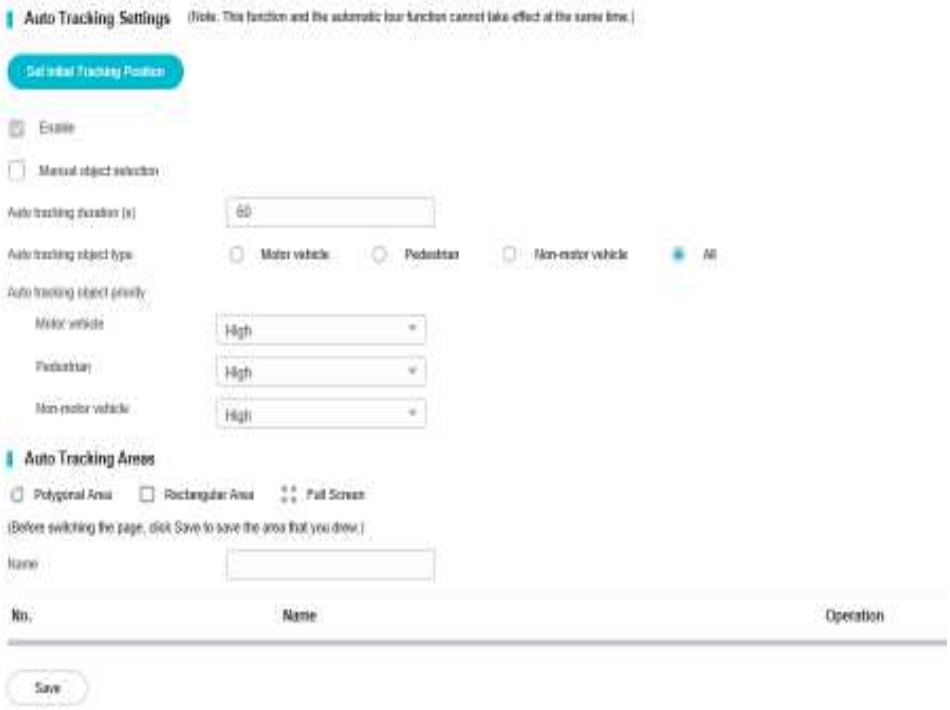


Table 1 describes the parameters and buttons.

Table 1 Parameter/Button description

Parameter/Button	Description
Set Initial Tracking Position	Button for recording the current location information. **NOTE:** When the automatic tracking event is triggered, pan, tilt, and zoom operations are triggered. After the tracking is complete, the PTZ dome camera automatically returns to the initial position.
Enable	This check box is selected by default and cannot be deselected.
Manual object selection	• If this parameter is selected, the camera does not automatically select an object to track. You need to manually select the object to track.

Parameter/Button	Description
	If this parameter is selected, the **Auto tracking object type** and **Auto tracking object priority** parameters do not take effect. • If this parameter is not selected, the camera preferentially tracks the manually selected object. If no object is manually selected, the camera automatically selects an object to track.
Auto tracking duration (s)	Duration for tracking the object. Set this parameter based on the message displayed on the GUI. After the specified time elapses, the camera stops tracking the object and continues to track another manually selected object or automatically selected object.
Auto tracking object type	Type of objects to be automatically tracked. If **Manual object selection** is selected, you do not need to set this parameter.
Auto tracking object priority	This parameter is available when **Auto tracking object type** is set to **All**. Under **Auto tracking object priority**, you can define the tracking priority for each object type. If **Manual object selection** is selected, you do not need to set this parameter.
Auto Tracking Areas	Used to draw a detection area. **NOTE:** • A detection area can be a triangle, rectangle, or polygon. • To redraw a detection area that is not saved, click **Draw** again. • A detection area supports a maximum of 10 vertexes. • Only one area can be drawn for automatic tracking. The newly drawn area will overwrite the previously drawn area. All behavior

Parameter/Button	Description
	analysis functions support a maximum of 10 detection areas. • If no detection area is drawn, the camera tracks the object in the full view.
Polygonal Area	Used to draw a polygonal detection area. You can click **Polygonal Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • A detection area can be a polygon such as a triangle or rectangle. A detection area supports a maximum of 10 vertexes. • To redraw a detection area that is not saved, click **Polygonal Area** again. • You can drag the detection area to change its location. • Only one area can be drawn for automatic tracking. The newly drawn area will overwrite the previously drawn area. All behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Rectangular Area	Used to draw a rectangular detection area. You can click **Rectangular Area** and move the pointer to the live video image. When the pointer turns to a cross, you can draw a detection area. **NOTE:** • To redraw a detection area that is not saved, click **Rectangular Area** again. • You can drag the detection area to change its location.

Parameter/Button	Description
	• Only one area can be drawn for automatic tracking. The newly drawn area will overwrite the previously drawn area. All behavior analysis functions support a maximum of 10 detection areas. • You can perform operations on only one detection area at a time.
Full Screen	Used to designate the entire live video image as the detection area. **NOTE:** All behavior analysis functions support a maximum of 10 detection areas.
No.	ID of a detection area.
Name	Name of a detection area. **NOTE:** The value can contain a maximum of 32 characters.
Operation	Column containing the button for deleting a detection area. To delete a detection area, select it from the detection area list and click .

4. Click **Save**.

Configuring an Alert Plan

After an alert plan is configured for a device, alarms will be reported to the platform. By default, alert is deployed for a device all day. If alarms do not need to be reported to the platform, you need to disable or delete the alert plan. Disabling or deleting an alert plan does not affect the snapshot service.

1. Click the **Alert Deployment Plan** tab, as shown in Figure 3.

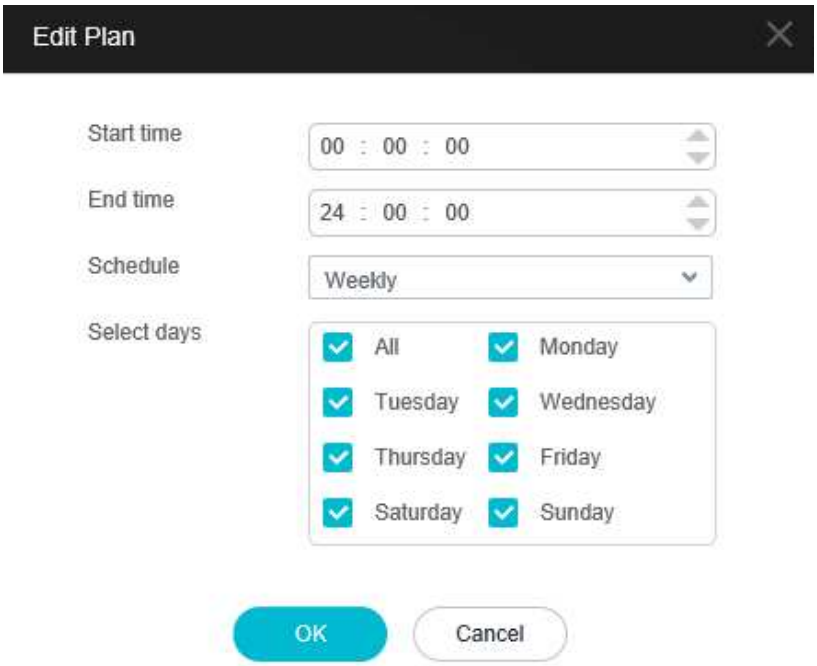
   Figure 3 Alert plan tab page

2. Click **Add**. A new alert plan is displayed. Click ✎ in the **Operation** column of the alert plan.

   The **Edit Plan** dialog box is displayed, as shown in Figure 4.

   Figure 4 Edit Plan dialog box

3. Set **Start time**, **End time**, **Schedule**, and **Select days**.
4. Click **OK**.
5. Click **Save**.

> **NOTE**
>
> - To modify or delete an existing alert plan, select it and click ✎ or 🗑 in the **Operation** column.

- At least one alert plan is required, and the check box in the **Status** column must be selected. If all alert plans are deleted, no alarm will be triggered by intelligent services.

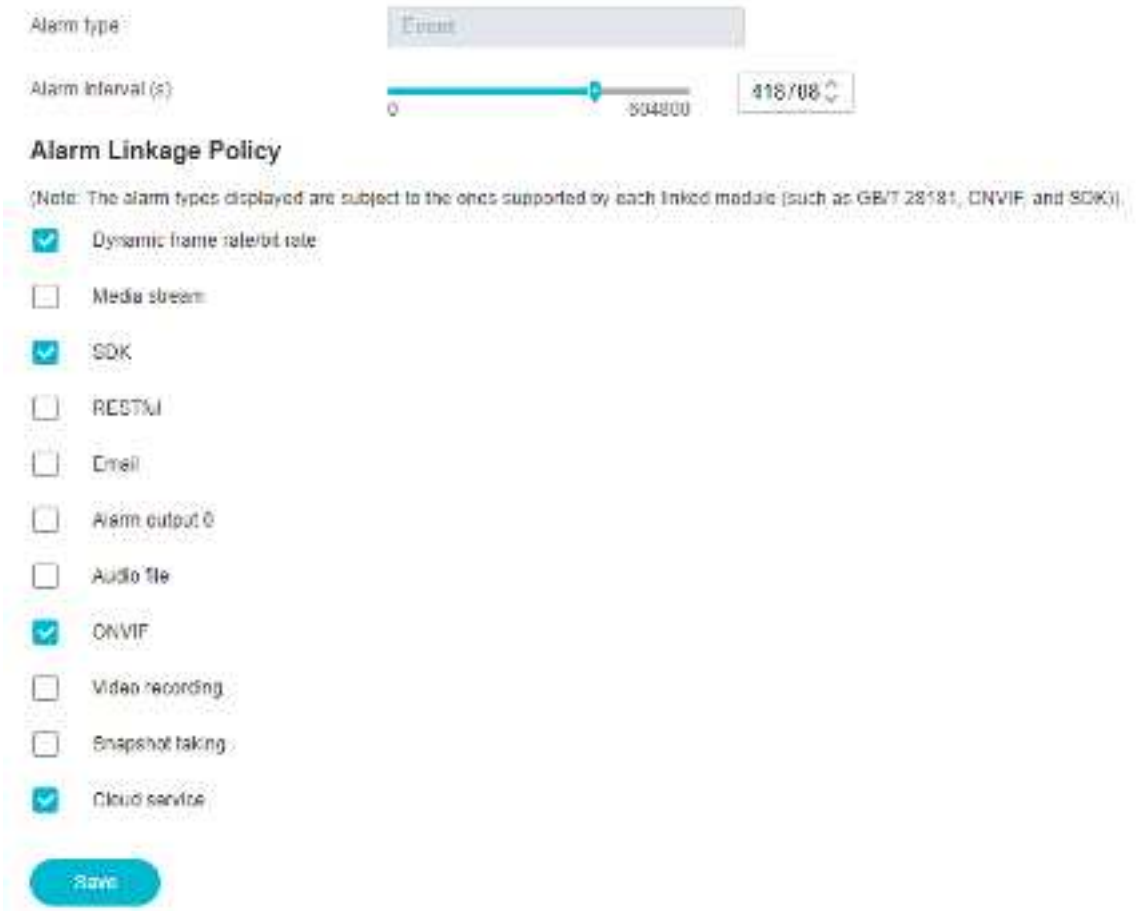
Configuring Alarms

1. Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in Figure 5.

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 5 Configuring alarms



2. Set related parameters. Table 2 describes the parameters.

Table 2 Alarm input parameters

Parameter	Description
Alarm type	Alarm type of a service. **NOTE:** The alarm type cannot be set. The alarm types of third-party platforms are determined by the registry file.
Alarm interval (s)	Interval at which the camera reports alarms to the platform.
Automatic recovery time (s)	This parameter is available for fault alarms. After the automatic recovery time is set, if an alarm is not cleared within the specified period, the system automatically clears the alarm.
T28181	If **T28181** is selected, the system reports alarms supported by GB/T 28181 through the GB/T 28181 protocol.
PTZ	If **PTZ** is selected, you can configure PTZ-related alarms, including alarms related to preset positions, tour scan, pattern scan, horizontal scan, vertical scan, frame scan, random scan, and panoramic scan.
ONVIF	If **ONVIF** is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.
SMTP	If **SMTP** is selected, the system sends an email containing alarm information to specified mailboxes when an alarm is generated. For details about how to configure mail linkage, see Setting Email Parameters. **NOTE:** The minimum interval for sending emails is 6s. Therefore, if the alarm detection interval is less than 6s, the number of emails may be different from the number of alarms.

Parameter	Description
Alarm output *X*	If **Alarm output *X*** is selected, when an alarm is generated, the alarm output device generates a warning. The alarm output devices include audible and visual alarm devices and alarm bells. To set the alarm output duration, choose **Configuration** > **Detection** > **Alarm I/O** > **Alarm Output** and set **Duration (s)**.
Video recording	If **Video recording** is selected, the system records video based on the specified recording time and saves the recording to the SD card when an alarm is generated. The value of **Recording duration** ranges from 60 to 3600, in seconds. The value range may vary between camera models.
Snapshot taking	If **Snapshot taking** is selected, the system takes a snapshot when an alarm is generated. After you select **Snapshot taking** and set **Snapshot count** and **Snapshot interval(ms)**, the snapshots will be stored on the SD card of the camera or uploaded to a specified FTP server through FTP or SFTP.
RESTful	If **RESTful** is selected, the system reports alarms supported by RESTful through the RESTful protocol.
SDK	If **SDK** is selected, the system reports alarms supported by SDK through the SDK protocol.
Dynamic frame rate/bit rate	If **Dynamic frame rate/bit rate** is selected, when an alarm (excluding the temperature alarm) is generated, the dynamic frame rate and bit rate are used. After the alarm is cleared, the frame rate and bit rate in stream settings are used.
Audio file	If **Audio file** is selected, the system plays the alarm sound based on the preset audio file and number of playing times when an alarm is generated. You can customize audio files by referring to Setting Audio Parameters.

Parameter	Description
White light illuminator	If **White light illuminator** is selected, when an alarm is generated, the system controls the white light illuminator based on the predefined flash frequency and duration (unit: seconds).
Cloud service	If **Cloud service** is selected, the system sends alarm information to the cloud service and the cloud service sends it to the mobile app or the iClient S100 when an alarm is generated.
Media stream	If **Media stream** is selected, the connected platform can receive TLV alarm information. To view detection results of a third-party app, choose **Display** > **Intelligent TLV**.

3. Click **Save**.

Verification

When an object enters the detection area:

- If the object is not automatically tracked, check the configuration. Table 3 describes the detailed check items.
- On the **View** page, if you click the manual tracking icon (), the camera will detect moving objects that appear in the image. Then, you can manually select an object to track. In this case, check whether the camera automatically tracks the object. If so, the configuration is successful.

Table 3 Check items

Check Item	Solution

Check Item	Solution
The configured detection area is too large. Therefore, when an object enters the detection area, the object cannot be detected due to its small size.	Adjust the focal length and re-configure the detection area size to ensure that the object can be detected.
The detection area is too small. Therefore, when an object enters the detection area, the object cannot be detected due to its large size.	
The automatic tracking function is disabled under **Configuration** > **Intelligence** > **Tracking Intelligence**.	Enable automatic tracking.

Configuring the PTZ

You can adjust the live video image size and shooting angle on the PTZ configuration page.

Adjusting the Image Size and Camera Shooting Angle

If the size or angle of the detection area does not meet the current requirements, you can click PTZ buttons to make adjustment.

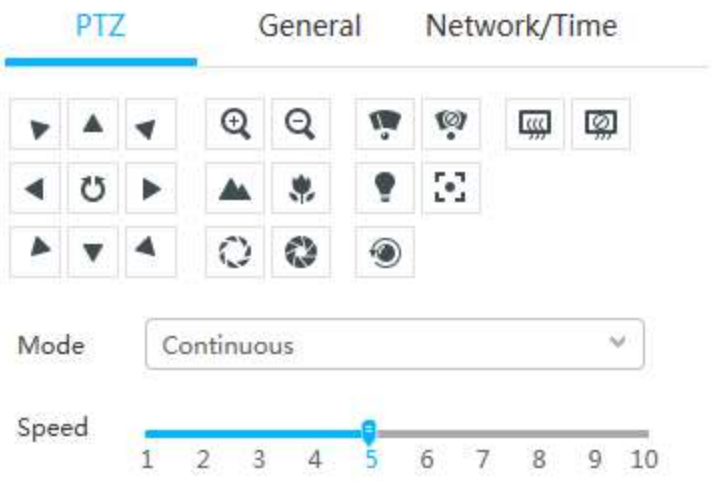
1. Log in to the camera web system (https://*Camera IP address*).
2. Click **View**. The **View** tab page is displayed.

   NOTE

   If the computer configuration is low or the system resource usage is high, the live video request may fail when you frequently switch between web pages. In this case, you can restart the browser to resolve the problem.

3. Click the **PTZ** tab. The PTZ function configuration page is displayed, as shown in Figure 1. The supported functions vary based on the camera models.

   Figure 1 PTZ configuration

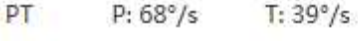


4. You can click required buttons to adjust the image. Table 1 describes the buttons.

Table 1 Button description

Button	Function
	Navigates the PTZ device in eight directions. • PTZ dome camera: Click  . The camera rotates to the home position. • Box camera, bullet camera, and fixed dome camera: After connecting to a PTZ device, click  . The camera rotates to the home position.
	Adjusts the aperture. **NOTE:** The aperture can be adjusted only in aperture priority or manual exposure mode.
	Adjusts the image clarity.
	Adjusts the camera shooting range.
	Sets the PTZ rotation mode. In **Continuous** mode, you can hold down a directional button to rotate the PTZ device continuously and release to stop PTZ rotation.

Button	Function
	In **Step** mode, if you click a directional button, the PTZ will rotate for a small angle and then stop.
	Turns the light on or off.
 / 	Enables or disables the wiper. The wiper is used to clear water droplets and dirt soluble in water only when there is water on the window. **NOTICE:** • *Do not use the wiper when there is no water on the window. Dry brushing may cause damage to the wiper and window.* • For some models, the wiper control function can be used only after an external wiper is connected.
 / 	Enables or disables the defogging/snow removal function. The defogging/snow removal function removes the fog on the lens caused by the change of the ambient temperature and humidity. The fog is removed by increasing the temperature in the camera cavity. **NOTICE:** This function is automatically disabled two hours after it is enabled, and does not take effect in high temperature protection mode.

Button	Function
	Controls the speeds for manually navigating the PTZ device, zooming in and out, and moving to the preset position. A larger value indicates a higher speed.
	Resets the lens. If the image is still blurry after automatic focus or manual focus (due to lens out-of-sync), you can click this button to automatically calibrate and focus the lens, making the image clear.
	Sets horizontal coordinate to zero for a PTZ dome camera. This button is unavailable to other types of cameras.
	Button for one-click or OnePush focus and calibration. You can click this button to implement automatic focus. **NOTE:** The precision of OnePush focus may not meet the requirements of intelligent services. It is recommended that the Siemens star chart be used to adjust the focus according to the site survey and commissioning guide for a specific intelligent service.
	Displays the current PTZ rotation speed, where P refers to the horizontal speed and T refers to the vertical speed.

Button	Function
	The speed varies according to the level. Level 10 refers to the highest speed.

NOTE

For an external PTZ, if you click the buttons for adjustment of the direction, aperture, focus, zoom, or wiper for multiple times within 2s, the camera responds only to the first operation.

Troubleshooting

Configuring Connection to the Platform Through RTSP

RTSP is an application-level protocol for the controls, such as play, pause, and fast-forward, of real-time streaming data.

Procedure

1. Log in to the camera web system (https://*Camera IP address*).
2. Choose **Configuration** > **Network** > **Advanced Settings** > **Platform Connection**.
3. Choose **Second Protocol Parameters** > **RTSP**. The **RTSP** tab page is displayed, as shown in Figure 1. Table 1 describes the options for the **RTSP authentication mode** parameter.

   Figure 1 RTSP tab page

   Table 1 Options for RTSP authentication

Option	Description
Digest_MD5	Digest authentication with MD5 encryption. This authentication method may cause security risks. Exercise caution when using it.
Digest_SHA256	Digest authentication with SHA256 encryption.
None	Security risks may exist when you select **None**. It is recommended that this authentication method be enabled only when the platform does not support authentication. If **None** is selected, the system does not perform authentication if you request live video through the RTSP or ONVIF protocol.

NOTE

The RTSP protocol is enabled by default. You can select the required authentication method during configuration.