

HOLOWITS Camera

11.1.1

E Series Product Documentation

Date **2024-01-25**

Contents

1 Applicable Models..... 1

2 Planning Principles.....2

2.1 Data Planning Suggestion..... 2

2.2 Network and Bandwidth Requirements..... 2

3 Installation Guide..... 9

3.1 Security Precautions..... 9

3.2 Tool Preparation..... 12

3.3 Installation Requirements..... 14

3.4 Installation Guide..... 16

3.5 Common Installation Errors..... 16

3.5.1 Water Leakage Due to Pigtail Cutoff..... 16

3.5.2 Pigtails Are Loosened or Disconnected If They Are Pulled..... 17

3.5.3 Device Damage Caused by Unstable Power Supply..... 19

3.5.4 Invalid Detection Due to Improper Installation..... 20

3.5.5 Device Damage Due to Lack of Surge Protection and Grounding..... 21

3.5.6 Water Ingress Caused by Indoor Mount Used Outdoors..... 24

3.5.7 Indoor Device Installed Outdoors..... 29

3.5.8 Misapplication of C- and CS-mount Lenses..... 31

3.5.9 Device Installation Failure Due to Incompatible PTZ Dome Camera Mount..... 32

3.5.10 Network Port Corroded by Water Due to Lack of Waterproof Measures for Pigtails..... 33

3.5.11 Camera Fault Due to Unqualified Self-Made RJ45 Connectors..... 35

3.5.12 Fiber Pigtail Cut Due to Improper PTZ Dome Camera Installation..... 36

3.5.13 Camera Damage Due to Improper Cabling for Power Supply..... 39

3.5.14 Water Seepage Due to Improper Camera Installation Outdoors..... 41

3.5.15 Network Port Damage Due to Forcible Cable Pulling..... 43

3.5.16 Camera Deviation from the Preset Position Due to Loose Screws of the Bracket..... 44

3.5.17 Severe Corrosion of Common Cameras Installed at the Seaside..... 46

3.5.18 Red Artifacts on Video Images Since the Protective Film Is Not Removed..... 47

3.6 Appendixes..... 49

3.6.1 Insulating and Waterproofing..... 49

3.6.2 Making the Network Cable..... 51

3.6.3 Replacing the Rain Wiper Rubber Strip..... 53

4 Configuration.....	56
4.1 Logging In to the Camera Web System.....	57
4.1.1 Computer Software and Hardware Requirements.....	57
4.1.2 Setting the Local Computer.....	58
4.1.3 Logging In to a Camera.....	60
4.2 Web Page Layout.....	65
4.3 Introduction to the Right Pane on the View Page.....	68
4.3.1 Setting Common Image Parameters.....	68
4.3.2 Setting Common Video Parameters.....	72
4.3.3 Setting Network Parameters.....	73
4.3.4 Setting System Time.....	76
4.4 Playback.....	79
4.4.1 Playing Back Recordings.....	79
4.4.2 Downloading Recordings.....	80
4.5 Snapshot Configuration.....	81
4.5.1 Downloading Snapshots.....	81
4.6 Wizard-based Configuration Guide.....	83
4.6.1 Setting Camera IP Addresses.....	83
4.6.2 Configuring Time.....	87
4.6.3 Configuring Video.....	90
4.6.4 Configuring Intelligent Analysis Functions.....	95
4.6.5 Setting Image Parameters.....	95
4.6.6 Configuring OSD.....	107
4.6.7 Configuring Network Platform Connection.....	109
4.6.7.1 Configuring Connection to the Platform Through SDK.....	109
4.6.7.2 Configuring Connection to the Platform Through ONVIF.....	111
4.6.7.3 Configuring Connection to the Platform Through RTSP.....	115
4.6.7.4 Configuring Connection to the Platform Through RESTful.....	117
4.6.7.5 Configuring the Protocol Password.....	119
4.6.7.6 Setting Media Stream Keep-Alive Parameters.....	120
4.7 Local Parameters.....	121
4.7.1 Setting Playing Parameters.....	121
4.7.2 Setting Recording File Parameters.....	123
4.7.3 Setting Snapshot File Parameters.....	124
4.8 Managing the System.....	125
4.8.1 System Settings.....	125
4.8.1.1 Basic Information.....	125
4.8.1.2 Time Configuration.....	128
4.8.1.3 Field of View.....	131
4.8.2 System Maintenance.....	131
4.8.2.1 Upgrade and Installation.....	131
4.8.2.1.1 Upgrading the Camera Version.....	131

4.8.2.2 Maintenance.....	132
4.8.2.3 Logs.....	136
4.8.2.3.1 Querying Logs.....	136
4.8.3 Security Management.....	137
4.8.3.1 Password Management.....	137
4.8.3.2 Password Recovery.....	140
4.8.3.3 Certificate Management.....	141
4.8.3.3.1 Managing HTTPS Certificates.....	141
4.8.3.3.2 Managing SDK Certificates.....	143
4.8.3.3.3 Managing the SDK Certificate Revocation List.....	144
4.8.3.4 IP Address Filtering.....	145
4.8.3.5 Security Options.....	147
4.8.4 User Management.....	147
4.8.4.1 User List.....	147
4.8.4.2 User Connection.....	154
4.8.4.3 Password Validity Period.....	154
4.9 Network Configuration.....	155
4.9.1 Setting Network Parameters.....	155
4.9.1.1 Configuring TCP/IP.....	155
4.9.1.1.1 Setting Camera IP Addresses.....	155
4.9.1.1.2 Setting Network Connectivity Detection.....	160
4.9.1.1.3 Setting QoS Parameters.....	160
4.9.1.1.4 Setting MTU Parameters.....	161
4.9.1.1.5 Setting Anti-Attack Parameters.....	162
4.9.1.1.6 Setting Multicast Parameters.....	163
4.9.1.2 Configuring HTTP(S).....	164
4.9.1.3 Setting Email Parameters.....	164
4.9.2 Setting Platform Connection Parameters.....	168
4.9.2.1 Setting Common Protocol Parameters.....	168
4.9.2.1.1 Configuring Connection to the Platform Through the ONVIF Protocol.....	168
4.9.2.1.2 Configuring Connection to the Platform Through RTSP.....	177
4.9.2.1.3 Configuring Connection to the Platform Through the SDK Protocol.....	178
4.9.2.1.4 Configuring Connection to the Platform Through RESTful.....	181
4.9.2.2 Setting Media Stream Keep-Alive Parameters.....	183
4.9.2.3 Setting FTP Parameters.....	184
4.9.2.4 Setting the Protocol Connection Password.....	187
4.10 Video and Audio Configuration.....	188
4.10.1 Video and Audio Feature Differences.....	188
4.10.2 Setting Video Parameters.....	189
4.10.3 Setting Audio Parameters.....	195
4.10.4 Setting ROI Parameters.....	197
4.11 Configuring Images.....	198

4.11.1 Image Feature Differences.....	198
4.11.2 Setting Image Parameters.....	201
4.11.3 Configuring Schedules.....	215
4.11.4 Configuring OSD.....	217
4.11.5 Configuring Privacy Mask.....	220
4.12 Intelligent Settings.....	221
4.12.1 Common Event Analysis Configuration.....	221
4.12.1.1 Specifications of the Common Event Analysis Feature.....	221
4.12.1.2 Configuring Motion Detection.....	222
4.12.1.3 Configuring Lens Blocking Detection.....	227
4.12.1.4 Configuring Human Figure Detection.....	231
4.13 Storage Configuration.....	236
4.13.1 Configuring Storage Management.....	237
4.13.2 Setting Snapshot Parameters.....	239
4.13.3 Configuring a Recording Plan.....	241
4.14 Event Alarm Configuration.....	244
4.14.1 Alarm Feature Differences.....	244
4.14.2 Alarm Reporting.....	244
4.14.2.1 Alarm Reporting Configuration.....	244
4.14.2.2 Alarm Linkage Policy Description.....	246
4.14.3 Certificate Alarm Configuration.....	252
4.14.4 Fault Alarm Configuration.....	256
4.15 FAQs.....	260
4.15.1 Login to the Camera Web System.....	260
4.15.1.1 Some Characters Are Displayed as Question Masks (?) on Web Client in Chinese Running in a Windows OS in English.....	261
4.15.1.2 Video Freezing Occurs After a User Logs In to the Web Client Using a Firefox Browser in Version 40.0.2.....	261
4.15.1.3 The User Is Prompted to Install a Control Even When the Control Has Been Installed.....	261
4.15.1.4 There Is a Problem with This Website's Security Certificate.....	262
4.15.1.5 Failure to Enter Time in the Text Box for Setting Time in the Camera Web System.....	262
4.15.1.6 When a User Uploads the Camera Certificate File and Configuration File Using HTTP on the Firefox Browser, the Message "Uploading... Do not perform any other operations" Is Always Displayed.....	263
4.15.1.7 A Message is Displayed During Plug-in Installation.....	263
4.15.1.8 A Message Indicating that an Exception Occurred on the Website's Security Certificate Is Displayed When You Log In to the Camera Web System.....	263
4.15.2 Live Video Viewing.....	267
4.15.2.1 Failure to Enter Full-Screen Mode When Double-Clicking the Live Video Pane for the First Time on the Live Video Viewing Page.....	267
4.15.2.2 Video Playback Failure on the Live Video Viewing Page.....	267
4.15.2.3 Failure to Play Video on the View Page for 5G Cameras.....	267
4.15.2.4 Live Video Request Failure.....	270
4.15.2.5 Black Screen Occurs on the Live Video Pane.....	271
4.15.2.6 Functional Icons on the Live Video Pane Remain Blue After the Functions Exit.....	271

4.15.2.7 Live Video Artifacts Occur and the CPU Usage Reaches 100%.....	271
4.15.2.8 Artifacts or Frame Freezing on Live Video.....	272
4.15.2.9 Unclear Live Video Image.....	272
4.15.2.10 Failure to View Live Video.....	272
4.15.2.11 Unstable Frame Rate Displayed on the Live Video Preview Page.....	273
4.15.2.12 Discontinuity Occurs When Objects Move in the Live Video.....	273
4.15.2.13 Slight Blinks on Image Border During Live Video Viewing Using Firefox.....	274
4.15.2.14 Graphs or Lines Superimposed on the Live Video Fail to Be Displayed.....	274
4.15.2.15 What Can I Do If Chinese Characters Are Displayed as Question Marks in the Camera Web System on the Windows 10 English Operating System?.....	274
4.15.2.16 Artifacts Occur When the Platform Requests Streams.....	276
4.15.3 Recording and Snapshot.....	276
4.15.3.1 Failure to Find Related Files in Storage Paths After Snapshots Are Taken and Video Is Recorded On Web Pages.....	276
4.15.3.2 Abnormal Live Video Scale on the Recording Playback Page.....	277
4.15.4 Device Maintenance.....	277
4.15.4.1 Camera Upgrade Issues.....	277
4.15.4.2 Failure to Install Player Control After Successful Device Upgrade on 64-bit Windows 8.....	278
4.15.4.3 Logs Fail To Be Downloaded After a User Clicks One-Click Collection on the Web Client.....	278
4.15.4.4 No Dialog Box Is Displayed After You Click the Button for Restarting the Device or Restoring Default Settings.....	278
4.15.5 Others.....	279
4.15.5.1 Blank Settings Page.....	279
4.15.5.2 Abnormal Position of Palette for OSD Color Customization.....	279
4.15.5.3 Vehicle Speed Displayed as NA in ePolice Mode of ITS Cameras.....	279
4.15.5.4 Obtaining Streams Through RTSP.....	280
4.15.5.5 Abnormal Device Start in Extremely Low Temperature.....	281
4.15.5.6 How Do I Obtain and Use the Milestone 2022 R3 Plug-in?.....	282
4.16 FAQs.....	284
4.16.1 How Can I Recover My Password If I Forget It?.....	284
4.16.2 Why Is a Recording Separately Stored into Multiple Files of Different Sizes?.....	284
4.16.3 What Can I Do If the NVR800 or IVS1800 Connected Through ONVIF in HTTPS Mode Cannot Go Online?.....	285
4.17 Configuring Image Optimization.....	286
4.17.1 Factors and Functions Related to Image Quality.....	286
4.17.1.1 Lens.....	286
4.17.1.1.1 Focal Length.....	286
4.17.1.1.2 Focus.....	287
4.17.1.1.3 Aperture.....	288
4.17.1.1.4 Shutter.....	289
4.17.1.1.5 Lens Types.....	290
4.17.1.2 Backlight Compensation.....	291
4.17.1.3 Highlight Compensation.....	292

4.17.1.4 Wide Dynamic Range..... 292

4.17.1.5 Function Dependencies and Differences..... 294

4.17.1.5.1 Shutter, Aperture, and Depth of Field..... 294

4.17.1.5.2 BLC, HLC, and WDR..... 295

4.17.2 Common Issues and Troubleshooting Methods..... 296

4.17.2.1 Image Clarity Issues..... 296

4.17.2.1.1 Image Blur..... 296

4.17.2.1.2 Low Contrast..... 301

4.17.2.2 Image Brightness Issues..... 302

4.17.2.3 Color Cast Issues..... 304

4.17.2.4 Image Noise Issues..... 306

4.17.2.5 Moire Pattern Issues..... 309

4.17.2.6 Purple Fringing Issues on Video Images of PTZ Dome Cameras or Small Bullet Cameras..... 312

4.17.2.7 Infrared Imaging Issues..... 313

4.17.2.8 Wave Pattern Issues..... 316

4.17.2.9 Motion Blur Issues..... 317

4.17.2.10 Dark Images with Infrared Illuminators..... 318

4.17.2.11 Power Frequency Flicker Issues..... 318

4.17.2.12 Ghosting and Lens Flare Issues..... 320

4.17.2.13 Severe Halation Issues at Night..... 321

4.17.2.14 Dark Images at Night..... 322

4.17.2.15 Reflection Caused by Flying Insects or Dust When Using Infrared Light..... 322

4.17.2.16 Blurred Infrared Image from a Fixed Dome Camera or Bullet Camera..... 323

4.17.2.17 Part of the Image is Blurry..... 324

4.17.2.18 Dark Image in Backlit Areas..... 327

4.17.3 Common Scenarios..... 328

4.17.3.1 Low Light Scenarios..... 328

4.17.3.2 Backlight Scenarios..... 331

4.17.3.3 Indoor Scenarios..... 332

4.17.3.3.1 Corridor..... 332

4.17.3.3.2 Exhibition Hall..... 333

4.17.3.4 Outdoor..... 335

5 Maintenance..... 337

5.1 Routine Maintenance..... 337

5.2 Security Maintenance..... 345

5.2.1 Overview..... 345

5.2.1.1 Purpose..... 345

5.2.1.2 Security Features..... 346

5.2.1.2.1 Application Security Layer..... 346

5.2.1.2.2 System Layer Security..... 347

5.2.1.2.3 Network Layer Security..... 347

5.2.1.2.4 Management Layer Security..... 347

5.2.1.2.5 Media Security.....	348
5.2.1.3 Layered Security Maintenance.....	348
5.2.1.4 System Security Policy.....	348
5.2.2 Application Layer Security.....	349
5.2.2.1 Accounts at the Application Layer.....	349
5.2.2.2 User Management.....	350
5.2.2.2.1 User List.....	350
5.2.2.2.2 User Connection.....	356
5.2.2.2.3 Password Validity Period.....	357
5.2.2.3 Access Control.....	357
5.2.2.4 Log Check and Audit.....	358
5.2.2.5 Clearing Service Data.....	359
5.2.3 Network Layer Security.....	361
5.2.3.1 Secure Network.....	361
5.2.3.2 Network Security Maintenance.....	361
5.2.3.3 Remote Access Control.....	362
5.2.3.3.1 Maintaining Accounts.....	362
5.2.3.3.2 IP Address Filtering.....	362
5.2.4 Management Layer Security.....	364
5.2.4.1 System Maintenance Security Principles.....	364
5.2.4.2 Account Management.....	364
5.2.4.3 Password Maintenance Suggestions.....	364
5.2.4.4 Log Maintenance Suggestions.....	365
5.2.4.5 Data Backup.....	365
5.2.4.6 Port Management Suggestions.....	365
5.2.4.7 Network Connection Change.....	365
5.2.4.8 Security Emergency Response.....	365
5.2.5 Security Configuration.....	366
5.2.6 Appendixes.....	367
5.2.6.1 Reference Documents.....	367
5.2.6.2 List of Security Maintenance Tasks.....	367
5.3 Emergency Maintenance.....	367
5.3.1 Overview.....	367
5.3.1.1 Definition of Emergency Faults.....	368
5.3.1.2 Routine Preparations.....	368
5.3.2 Service Fault Scenarios.....	368
5.3.2.1 Multiple Cameras Go Offline on the Platform.....	368
5.3.2.2 Multiple Cameras Encounter a Blank Screen or Stream Interruption on the Platform.....	370
5.3.3 Appendix.....	373
5.3.3.1 Collecting Fault Information.....	373
5.3.3.1.1 Fault Information Collection Template.....	373
5.3.3.1.2 Methods.....	374

6 Reference..... 376

1 Applicable Models

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

Table 1-1 Applicable models

Camera Type	Model	Appearance
Bullet camera	E1A-4LR(3.6)	A white bullet-style camera with a black lens cover and mounting bracket.
Fixed dome camera	E4A-4R(3.6)	A white fixed dome camera with a black lens cover and the HOLOWITS logo on the top.
	E4A-4R(2.8)	A white fixed dome camera with a black lens cover and the HOLOWITS logo on the top.

NOTE

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

2 Planning Principles

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

2.1 Data Planning Suggestion

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

2.2 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.

2.1 Data Planning Suggestion

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

2.2 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 2-1 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 2-1 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 2-4](#), 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 2-4](#), 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 [4.10.2 Setting Video Parameters](#). [Table 2-2](#) lists the recommended bit rate for each video format.

Table 2-2 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

Video Resolution	Recommended Bit Rate (Mbit/s) (H.265)
6MP	6–12
4K	10–12
9MP	12–14

NOTE

The encoding bit rate range listed in [Table 2-2](#) 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 2-3](#) lists data of A.

Table 2-3 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 [4.13.1 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 2-4](#) 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 2-4 Bandwidth calculation example

Camera Type	Video Stream Bandwidth					Metadata Upload Bandwidth				FTP Upload Bandwidth	Reserved Bandwidth Coefficient	Accumulated Uplink Bandwidth
	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 Upload 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	Same as the metadata upload bandwidth	1.2	(4 Mbit/s x 1 x 200% + 2 Mbit/s x 1 + 24 Mbit/s x 1) x 1.2 = 70 Mbit/s

3MP camera	3MP	6 Mbit/s	2 Mbit/s	1	1	1.5 MB	2	$1.5 \times 2 \times 8 = 24 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(6 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 24 \text{ Mbit/s} \times 1) \times 1.2 = 74 \text{ Mbit/s}$
4MP camera	4MP	6 Mbit/s	2 Mbit/s	1	1	1.5 MB	2	$1.5 \times 2 \times 8 = 24 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(6 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 24 \text{ Mbit/s} \times 1) \times 1.2 = 74 \text{ Mbit/s}$
5MP camera	5MP	8 Mbit/s	2 Mbit/s	1	1	2 MB	2	$2 \times 2 \times 8 = 32 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(8 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 32 \text{ Mbit/s} \times 1) \times 1.2 = 98 \text{ Mbit/s}$
6MP camera	6MP	10 Mbit/s	2 Mbit/s	1	1	3 MB	2	$3 \times 2 \times 8 = 48 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(10 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 48 \text{ Mbit/s} \times 1) \times 1.2 = 142 \text{ Mbit/s}$

4K camera	4K	12 Mbit/s	2 Mbit/s	1	1	4 MB	2	$4 \times 2 \times 8 = 64 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(12 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 64 \text{ Mbit/s} \times 1) \times 1.2 = 185 \text{ Mbit/s}$
9MP camera	9MP	12 Mbit/s	2 Mbit/s	1	1	4 MB	2	$4 \times 2 \times 8 = 64 \text{ Mbit/s}$	1	Same as the metadata upload bandwidth	1.2	$(12 \text{ Mbit/s} \times 1 \times 200\% + 2 \text{ Mbit/s} \times 1 + 64 \text{ Mbit/s} \times 1) \times 1.2 = 185 \text{ Mbit/s}$

 NOTE

- Set the encoding bit rate, snapshot size, number of snapshots taken per second, and reserved bandwidth coefficient based on the site requirements.
- For ITS cameras, the recommended attainable network bandwidth is 300 Mbit/s for image data transmission.

3 Installation Guide

[3.1 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.

[3.2 Tool Preparation](#)

Before the installation, prepare required tools.

[3.3 Installation Requirements](#)

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

[3.4 Installation Guide](#)

[3.5 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.

[3.6 Appendixes](#)

3.1 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.

3.2 Tool Preparation

Before the installation, prepare required tools.

Tools to be prepared

Table 3-1 lists the tools that need to be prepared.

Table 3-1 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.	

Tool Name	Specification and Function	Appearance
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.	

3.3 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 waterproof 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:
 - a. Class D corrosion resistance. Cameras at this level can be installed within 1500 m away from the seashore or on offshore platforms.
 - b. 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.

3.4 Installation Guide

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

Table 3-2 Applicable models

Camera Type	Model	Reference
Bullet camera	E1A-4LR(3.6)	AI Small Bullet Camera (Integrated Bracket) Quick Start Guide

3.5 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.

3.5.1 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 3-1 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 [3.6.1 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 3-2](#).

Figure 3-2 Apply waterproof tape on the pigtail



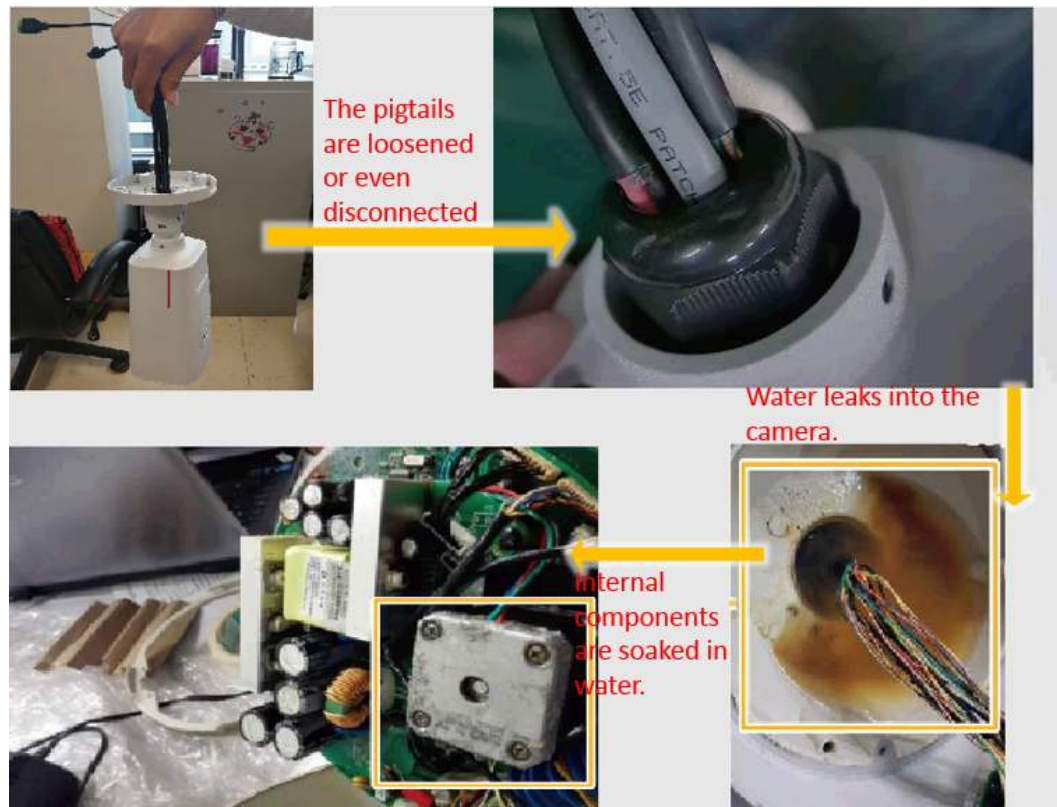
3.5.2 Pigtails Are Loosened or Disconnected If They Are Pulled

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 3-3](#).

Figure 3-3 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.

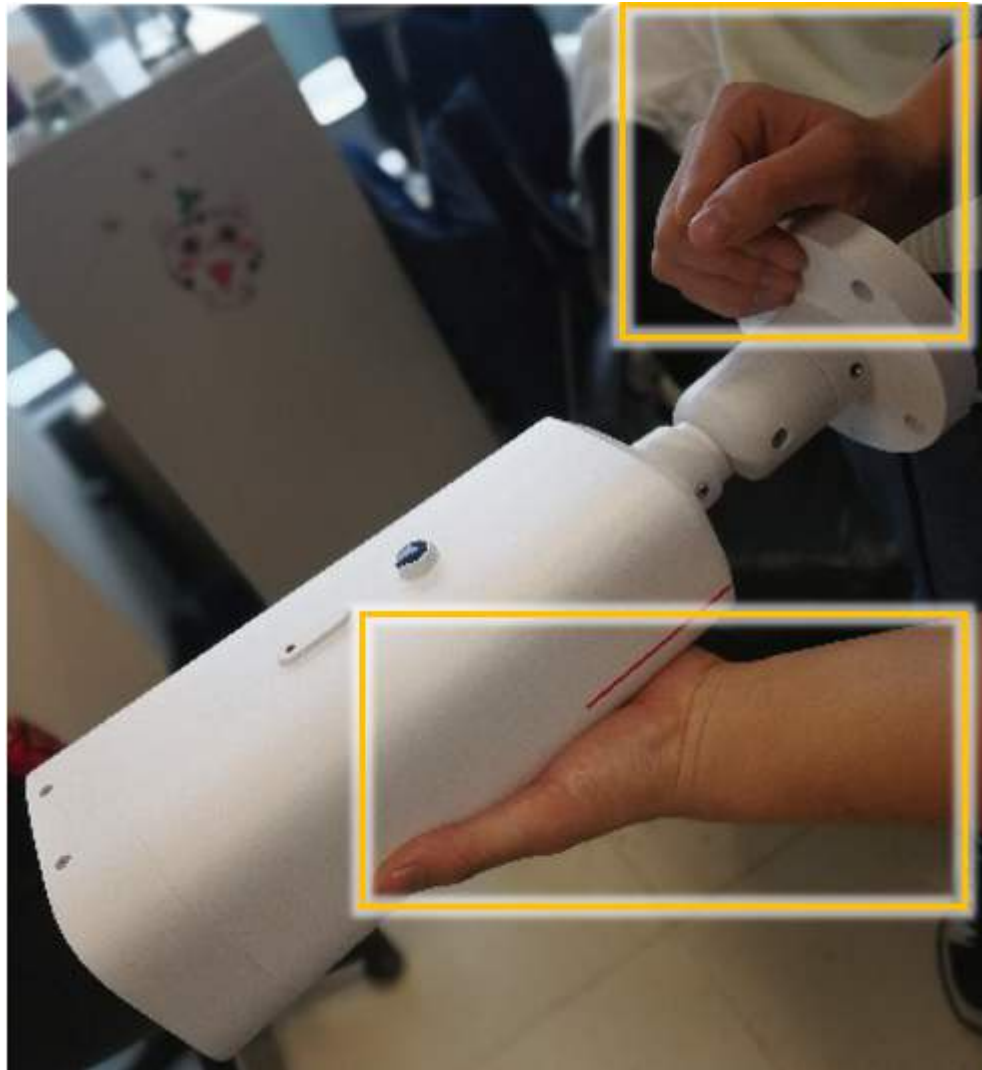
Root Cause

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 3-4](#).

Figure 3-4 Correct method of carrying a device



3.5.3 Device Damage Caused by Unstable Power Supply

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

Typical Example

Figure 3-5 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 ($\pm 25\%$), 24 V AC (-25% to $+24.9\%$)).
- The input voltage of the camera does not meet the requirements (voltage range: 12 V DC ($\pm 25\%$), 24 V AC (-25% to $+24.9\%$)).

Solution

1. The input voltage of the camera must meet the requirements (voltage range: 12 V DC ($\pm 25\%$), 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 3-3](#).

Table 3-3 Cable cross-sectional area specifications

Type	Cross-Sectional Area	Maximum Cable Length
24 V AC output (from the adapter to the camera)	1.0 mm ²	10 m
	1.5 mm ²	25 m
	2.0 mm ²	50 m
	2.5 mm ²	75 m
	3.0 mm ²	120 m

3.5.4 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 3-6 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

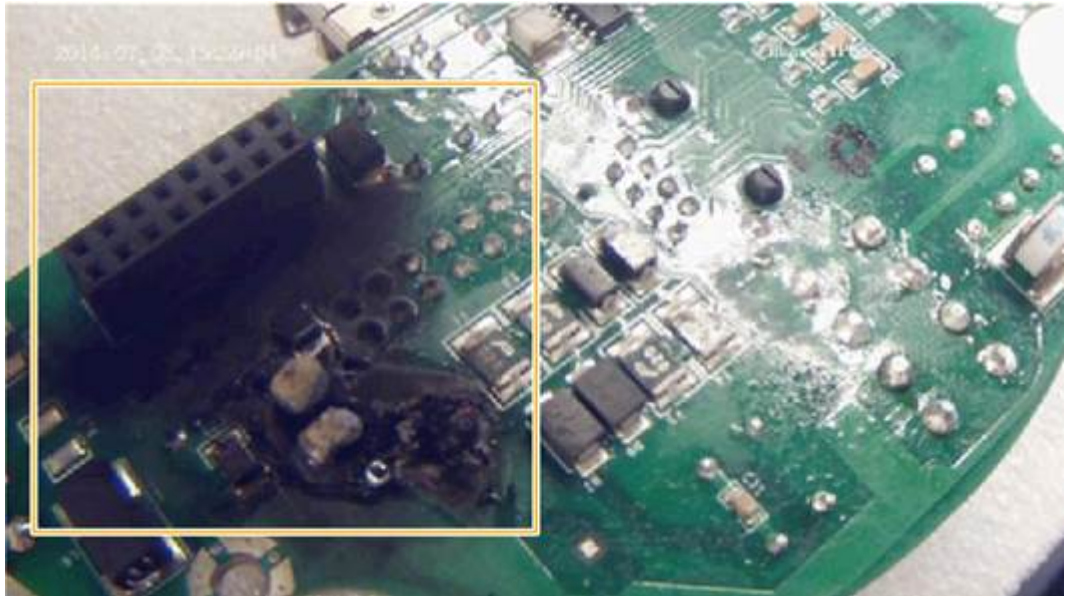
1. Determine the pole height based on the actual environment and adjust the camera's shooting angle to avoid obstacles.
2. Set a proper focal length to ensure the coverage of accident-prone areas.
3. Set a proper camera angle to ensure that movement directions of passengers are detected.

3.5.5 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 3-7 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 3-8 Surge protection and grounding

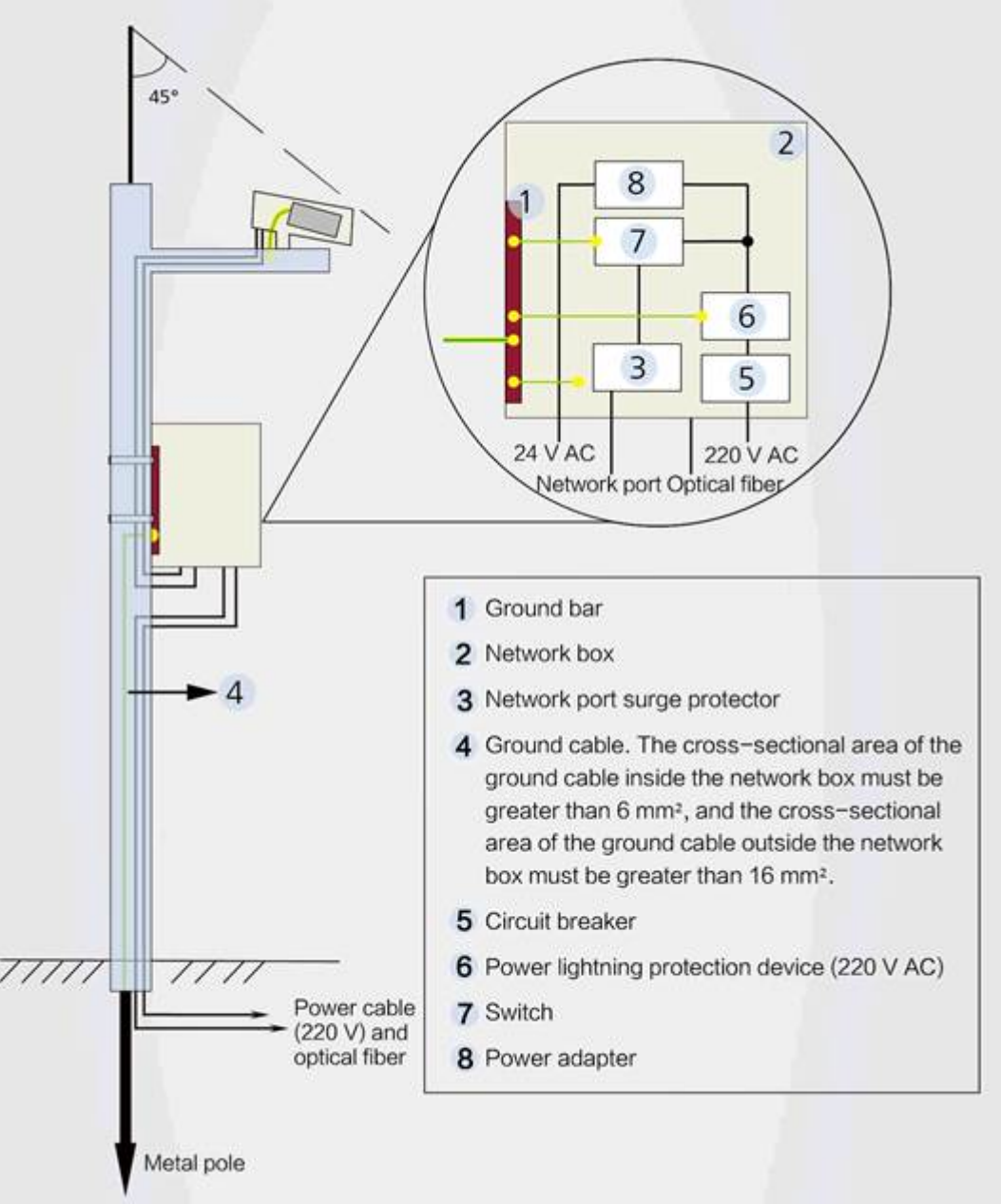


Table 3-4 Requirements for surge protection

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

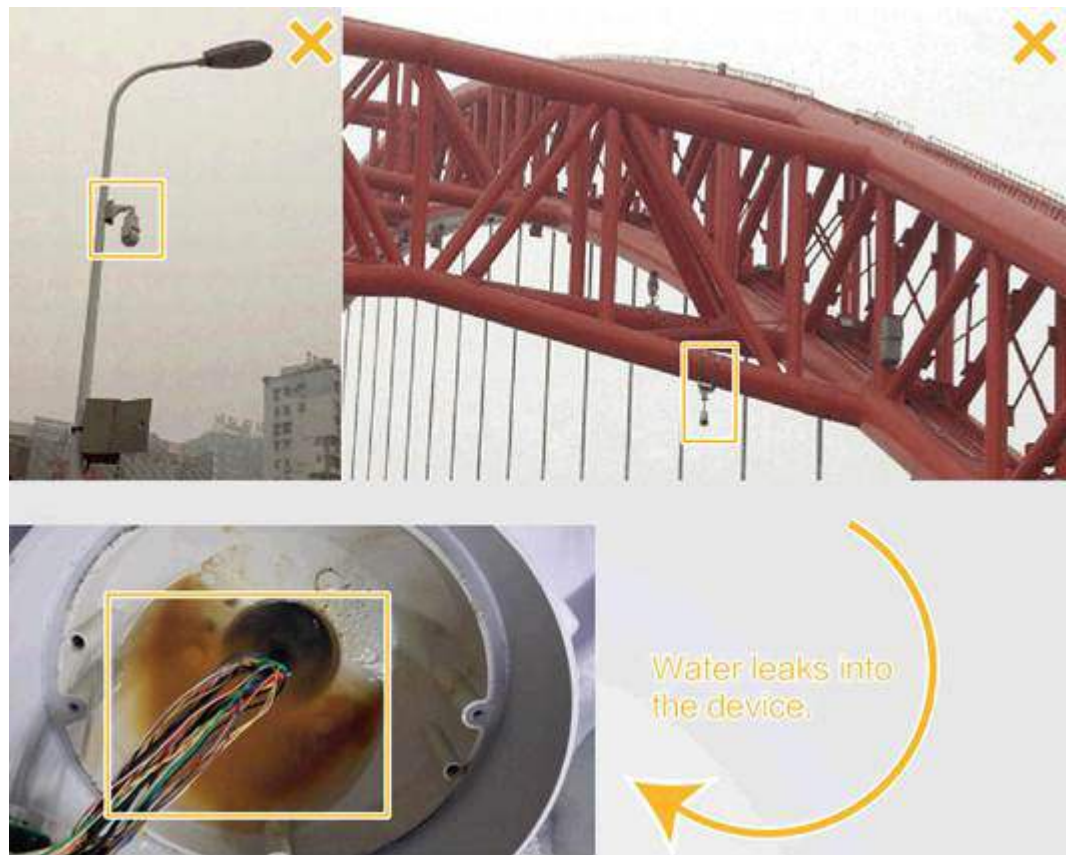
Port	Specification	Scenario
	- Differential mode: 20 kA (wire to wire), 8/20 us - Common mode: 20 kA (single wire to ground), 8/20 us	Pole-mounted installation in non-urban areas
PoE/network port	Surge: - Differential mode: 1.5 kV (differential wire pair), 10/700 us, 15 ohms + 25 ohms/wire - Differential 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: - Differential mode: 250 A (-48 V to RTN), 8/20 us - Common mode: 3 kA/8-wire, 8/20 us	Pole-mounted installation in urban/non-urban areas

3.5.6 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

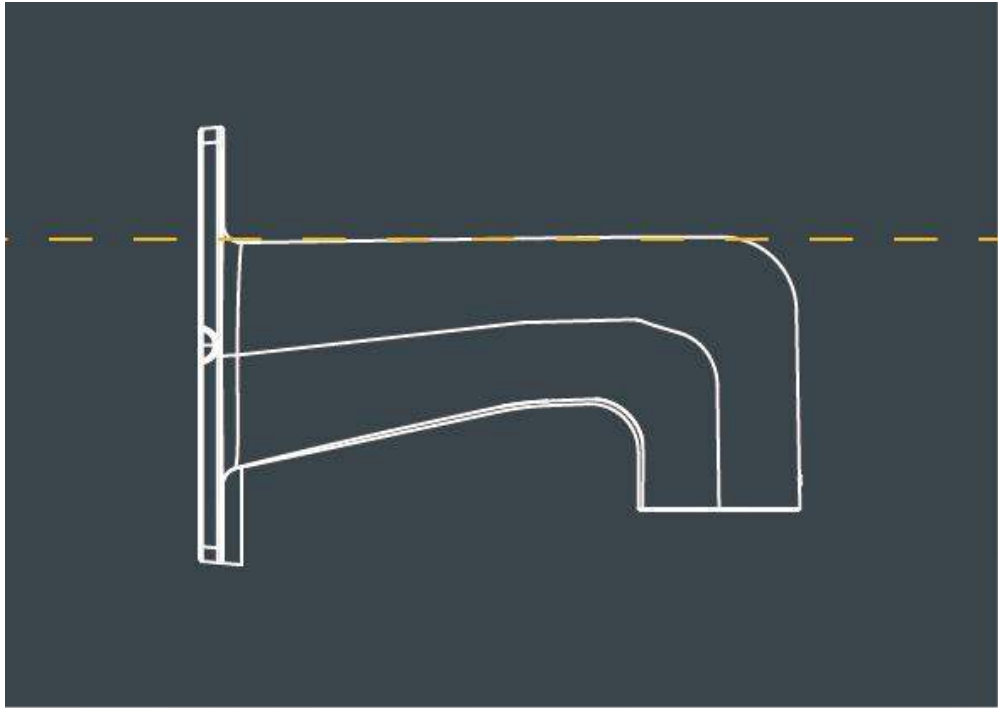
Figure 3-9 Water ingress due to wrong installation methods



Symptom

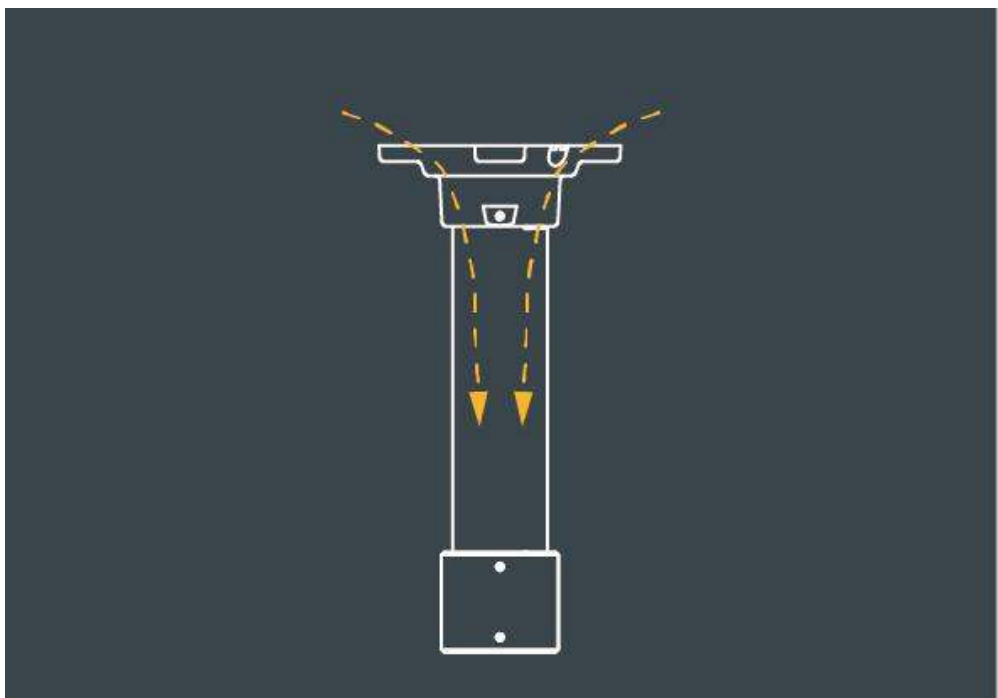
- If a short wall mount is used to install a camera outdoors, the beam of the mount is horizontal, and water may easily leak into the camera, as shown in [Figure 3-10](#).

Figure 3-10 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 3-11](#).

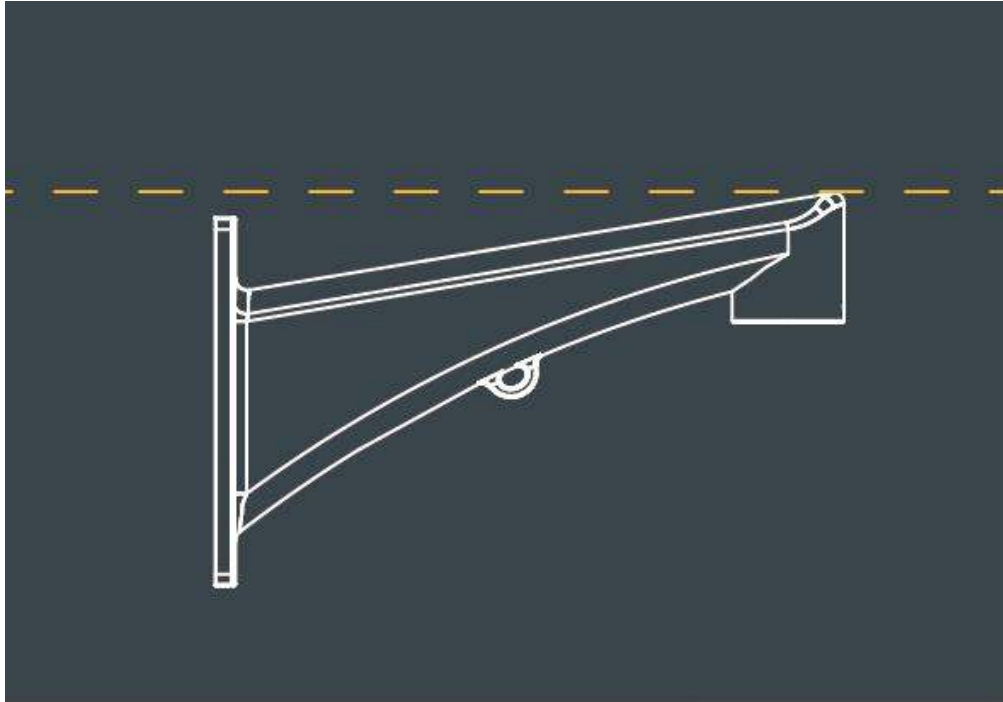
Figure 3-11 Pendant mount



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 3-12](#).

Figure 3-12 Long wall mount

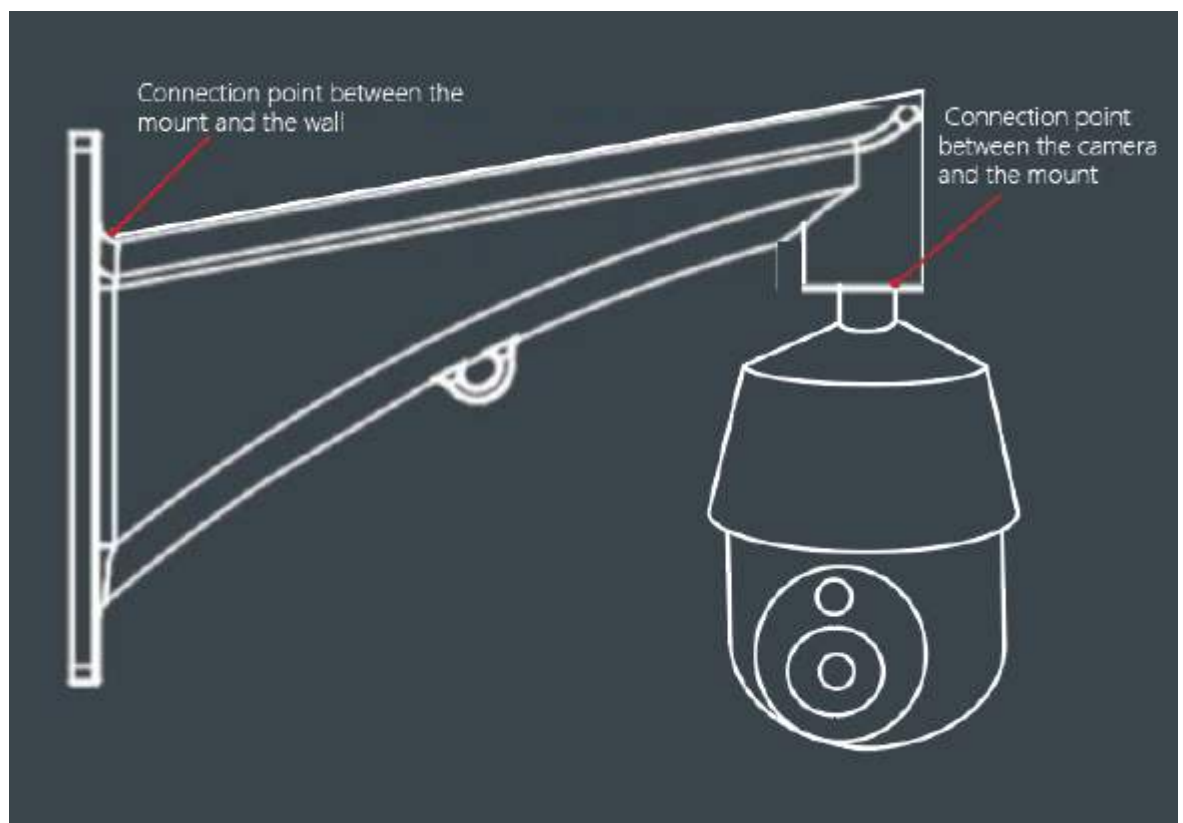


- Use an integrated pole mount to install a camera outdoors to avoid water ingress from the connection point between the camera and the mount, as shown in [Figure 3-13](#).

Figure 3-13 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.

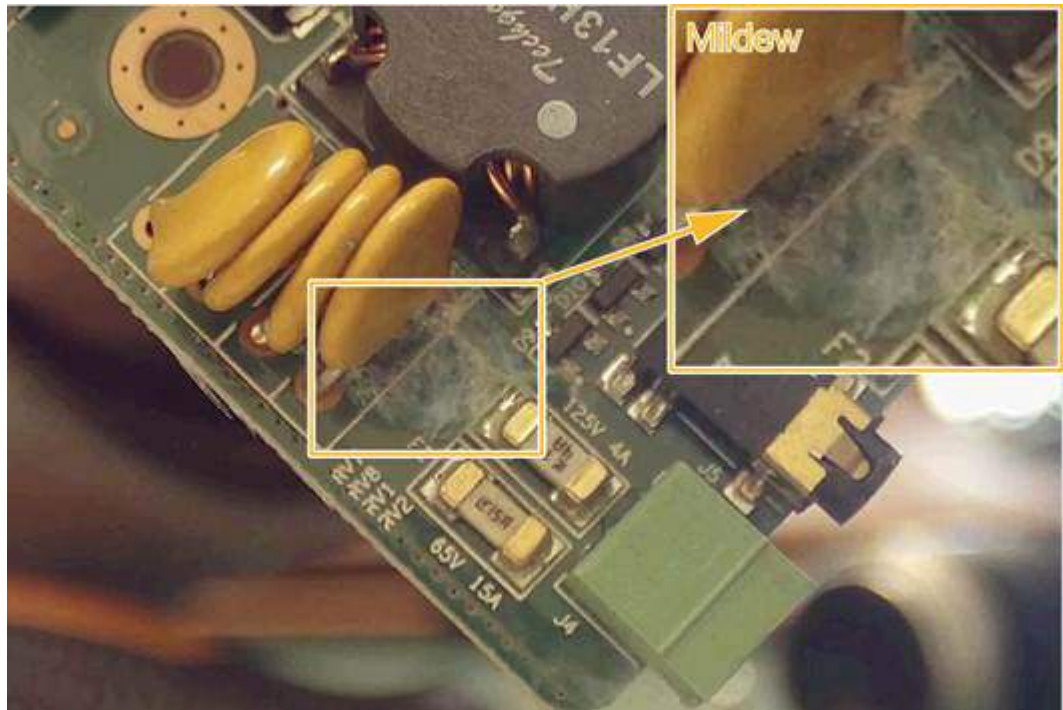


3.5.7 Indoor Device Installed Outdoors

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 3-14 Mildewed board



Symptom

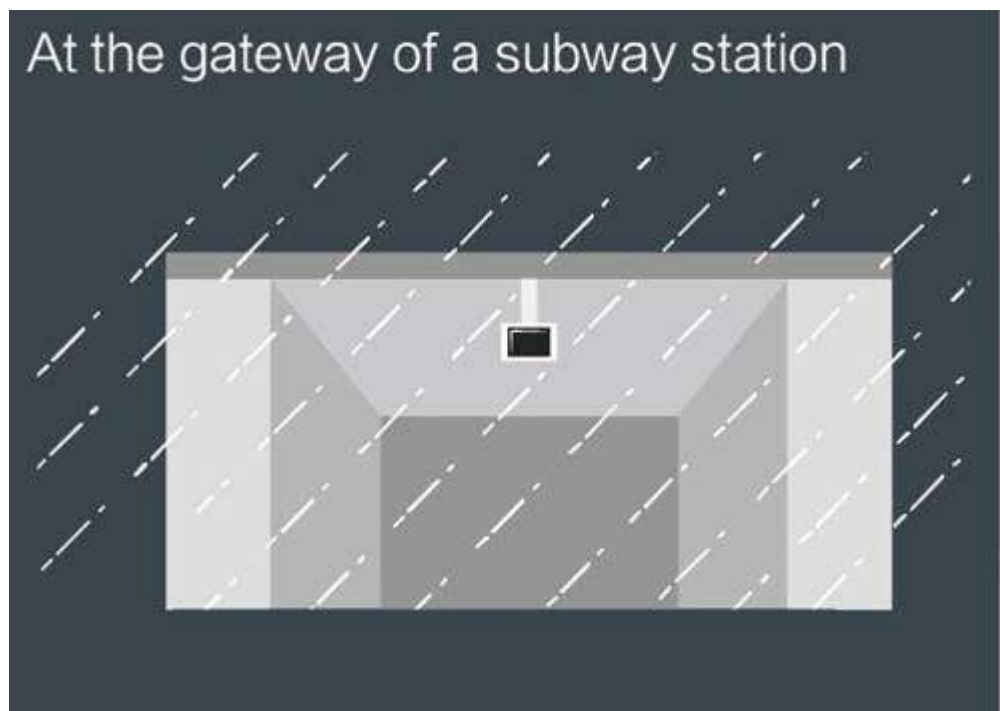
- An indoor fixed dome camera is installed outdoors. The camera is damaged due to water penetration, as shown in [Figure 3-15](#).

Figure 3-15 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 3-16](#).

Figure 3-16 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.

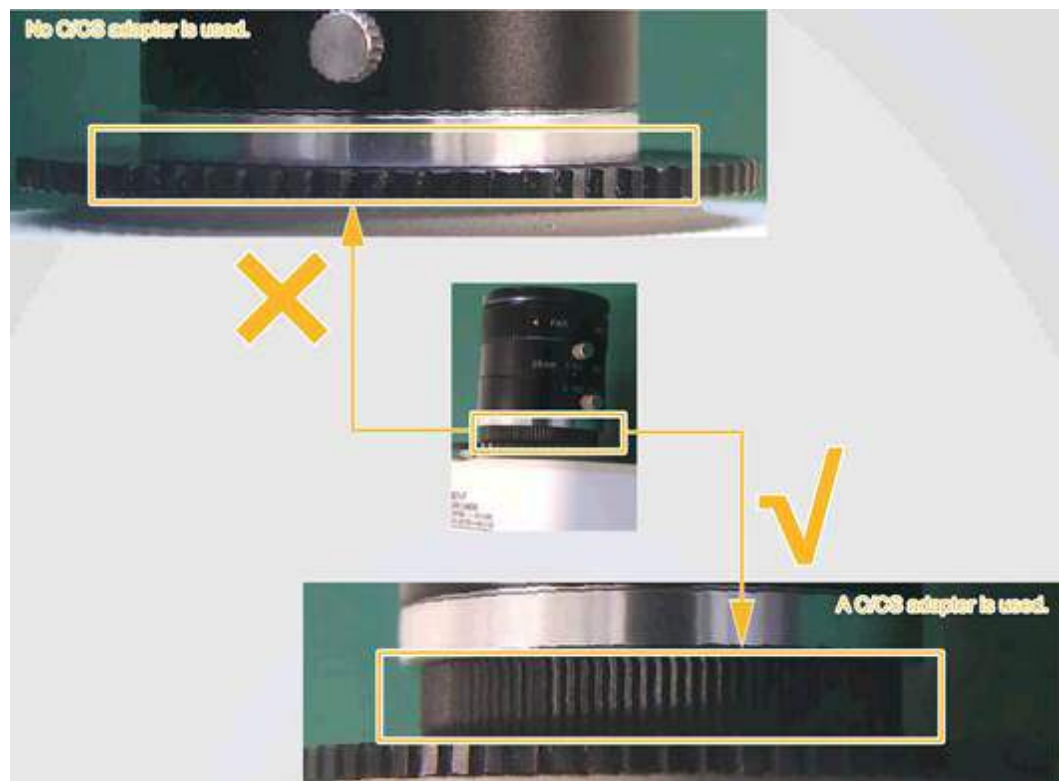
3.5.8 Misapplication of C- and CS-mount Lenses

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 3-17](#).

Figure 3-17 No C/CS lens adapter used



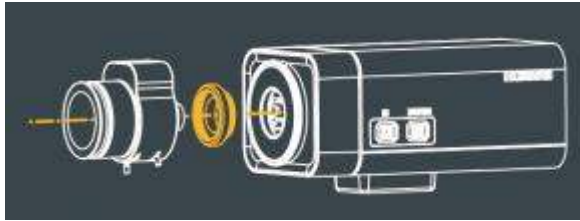
Symptom

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 3-18](#).

Figure 3-18 Installing the C/CS lens adapter



3.5.9 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.

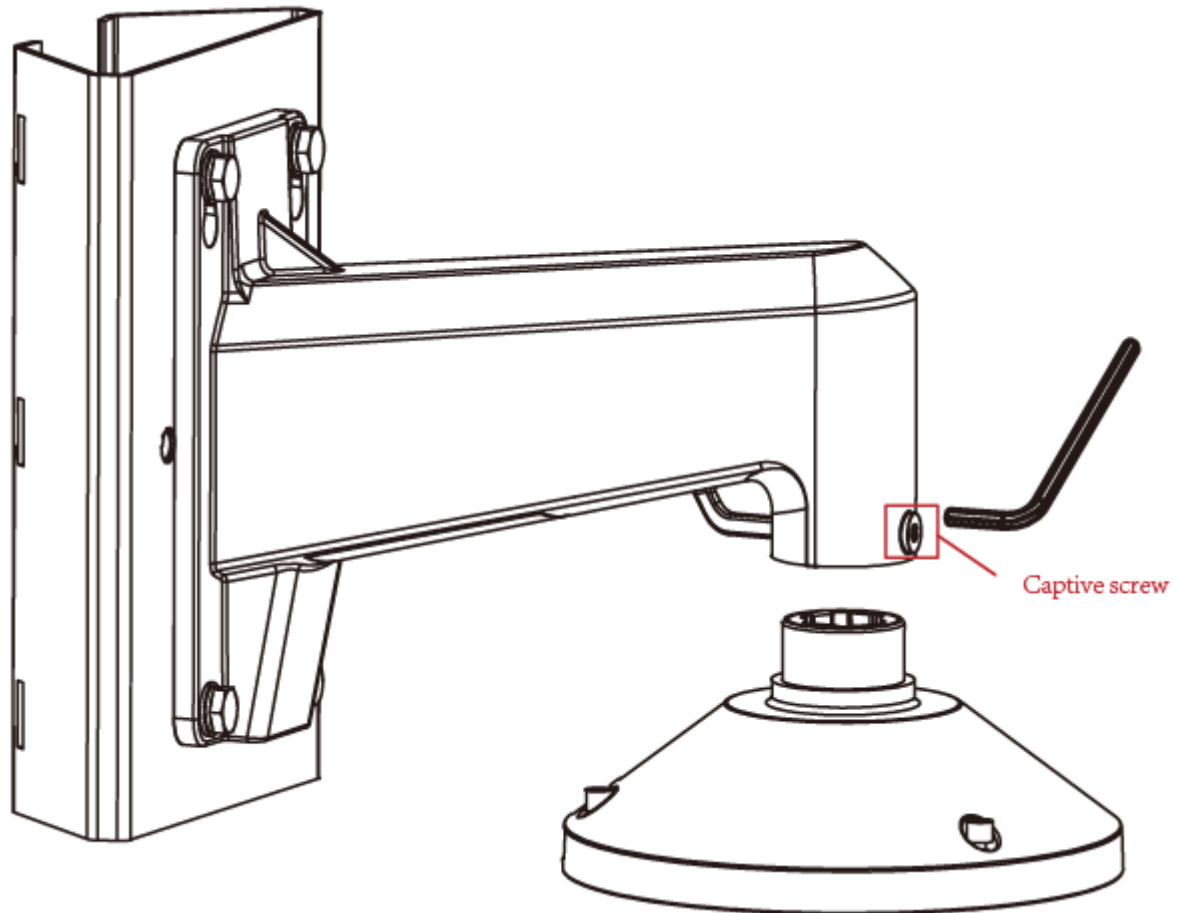
Symptom

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 3-19 PTZ dome camera mount



NOTE

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

3.5.10 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 3-20 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 3-21](#). 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 3-21 Network port pre-installed with waterproof kit before delivery

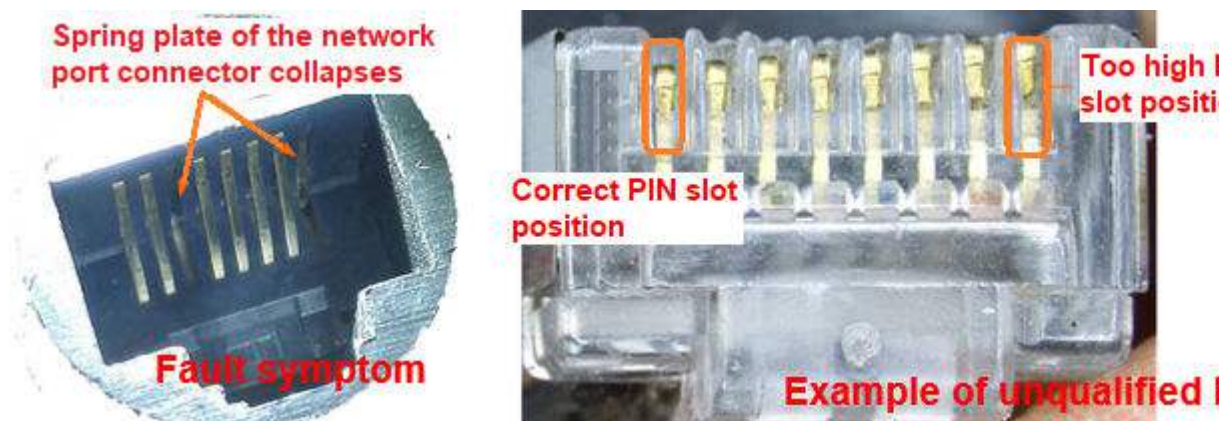


3.5.11 Camera Fault Due to Unqualified Self-Made RJ45 Connectors

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

Typical Example

Figure 3-22 Example of unqualified RJ45 connector



Symptom

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

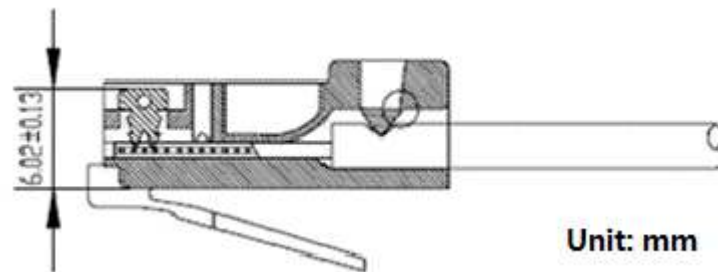
Root Cause

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 3-23](#). 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 3-23 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.
-

3.5.12 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 3-24 Load bearing through the pigtail due to incorrect installation



Root Cause

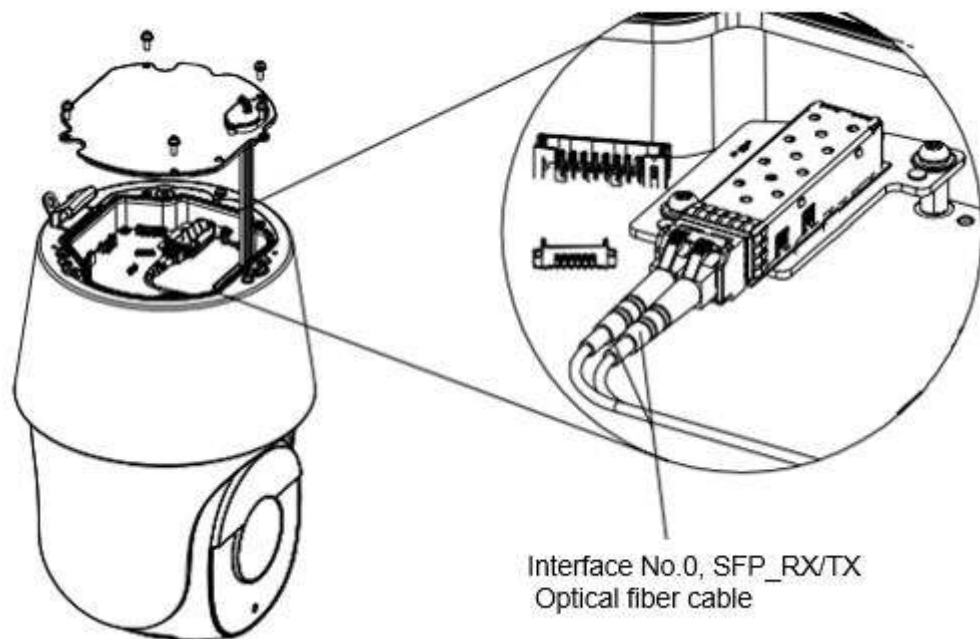
By default, cameras are not delivered with optical modules. Therefore, for cameras with fiber pigtails, you need to install optical modules onsite and insert the optical fibers. Optical fibers are prone to damage. You need to strictly follow the installation guide to avoid excessive bending or pulling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

Solution

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

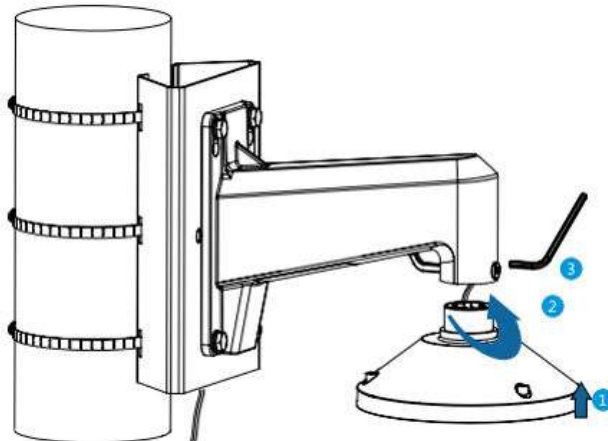
Step 1 Install the optical module.

Figure 3-25 Installing the optical module



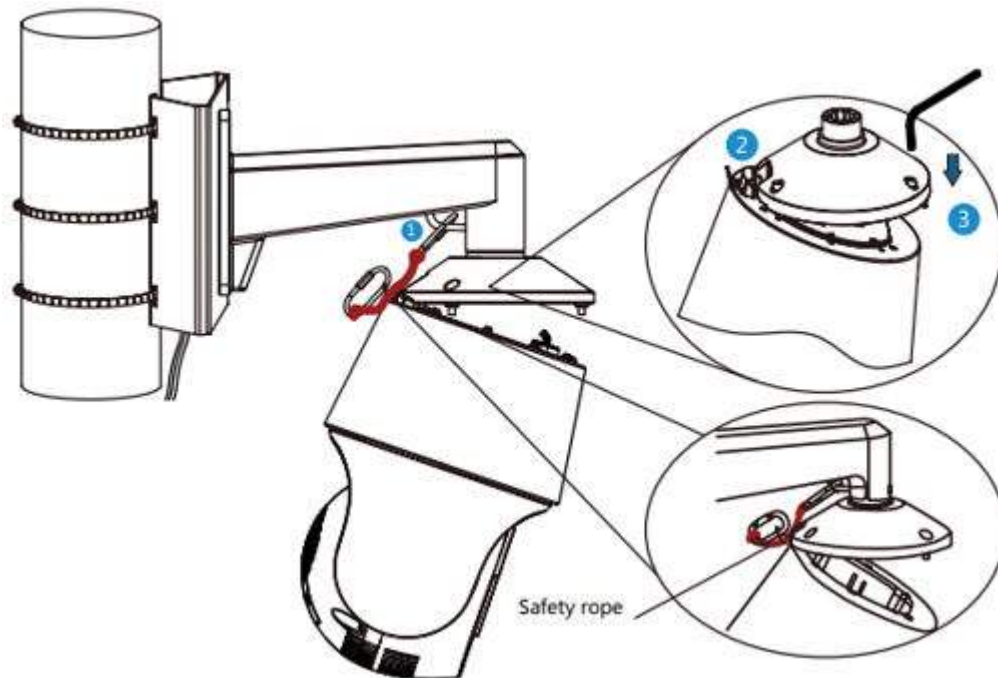
Step 2 Install the rear cover of the PTZ dome camera on the bracket.

Figure 3-26 Installing the rear cover of the PTZ dome camera on the bracket



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

Figure 3-27 Mounting the PTZ dome camera to the rear cover and connecting cables



----End

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.

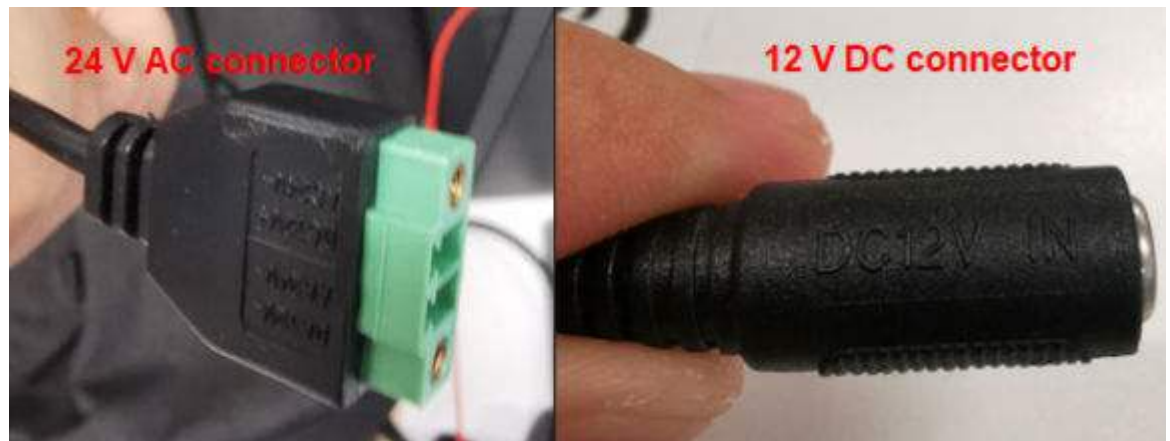
3.5.13 Camera Damage Due to Improper Cabling for Power Supply

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 3-28](#) 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.

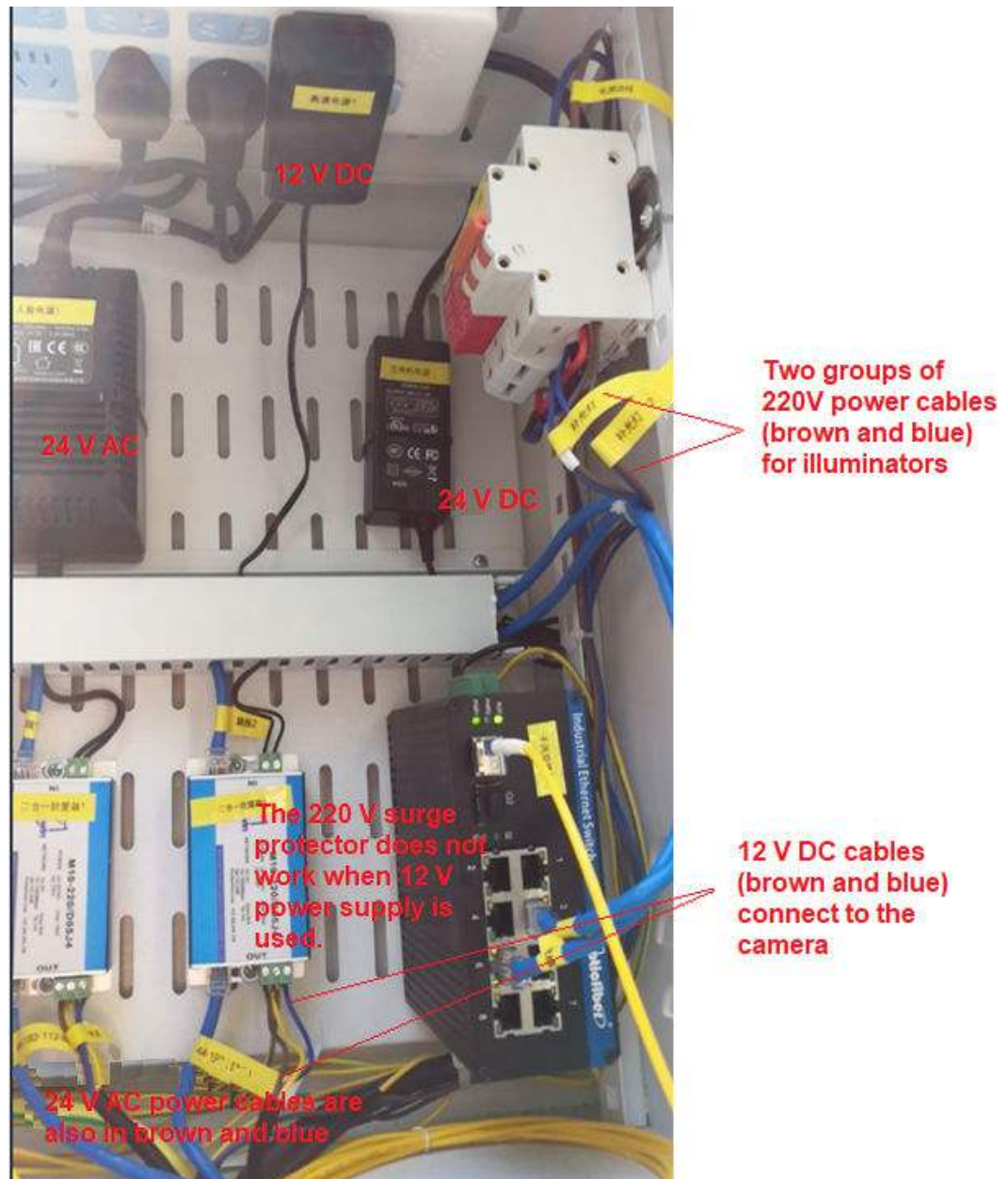
Figure 3-28 Mainstream camera power supply specifications



Solution

In [Figure 3-29](#), 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 3-29 Example of the output cable of power adapter

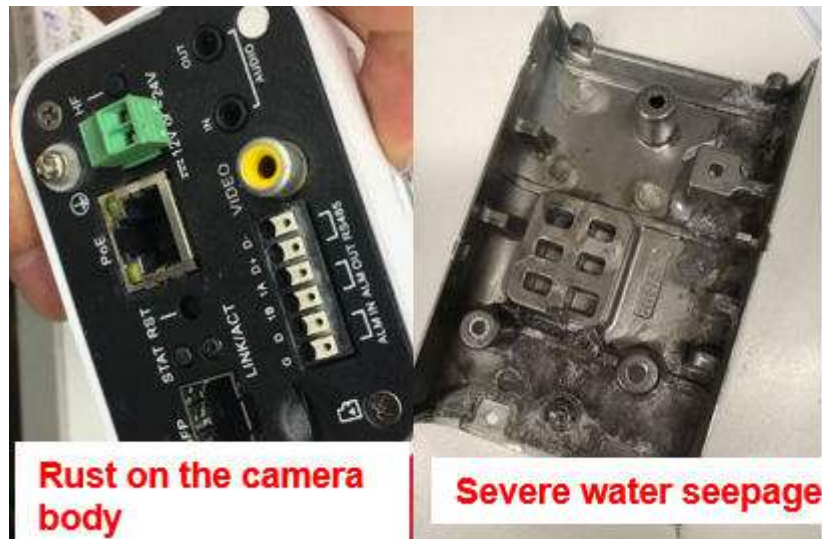


3.5.14 Water Seepage Due to Improper Camera Installation Outdoors

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

Typical Example

Figure 3-30 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 3-31](#).

Figure 3-31 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 3-32](#) shows an example of correct installation.

Figure 3-32 Correct installation example



3.5.15 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 3-33 Network port is damaged after pulling the network cable forcibly without removing the waterproof kit



Figure 3-34 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.

3.5.16 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 3-35](#), 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 3-35 Camera deviation from the preset position



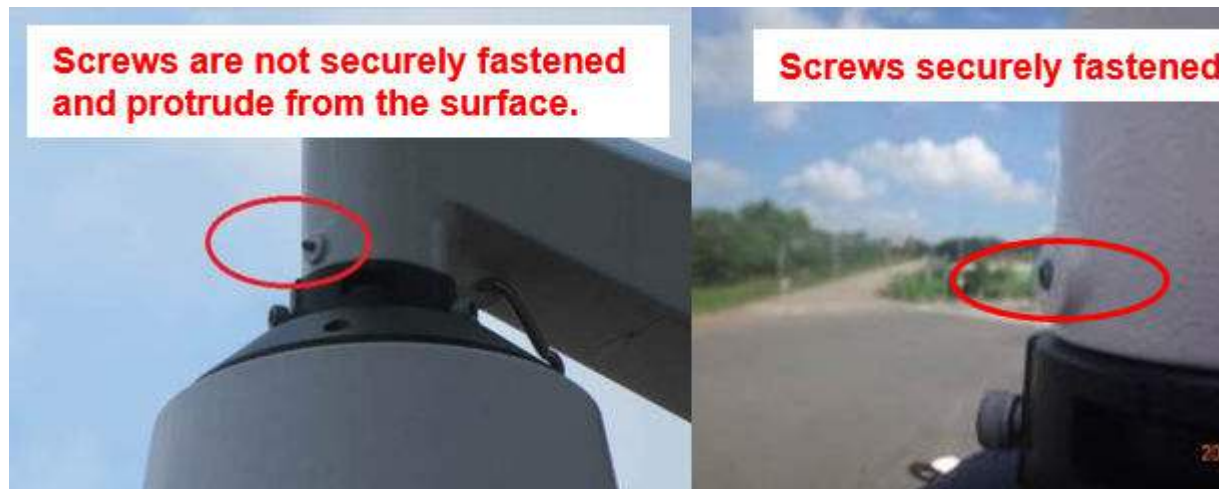
Symptom

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 3-36](#).

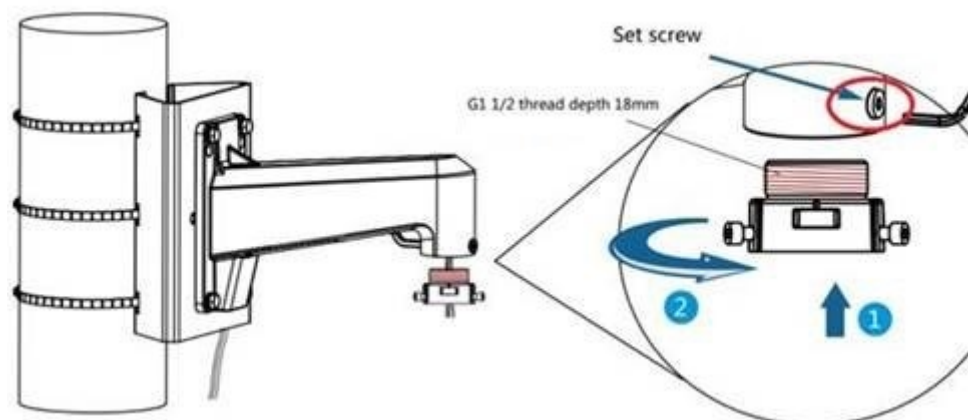
Figure 3-36 Example of tightening screws



Solution

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

Figure 3-37 Guide to tightening the screws



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

3.5.17 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 3-38 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.

3.5.18 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 3-39 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 3-39](#). In this way, users can check whether the film is removed directly on video images without visiting the site.

Figure 3-40 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.

3.6 Appendixes

3.6.1 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.

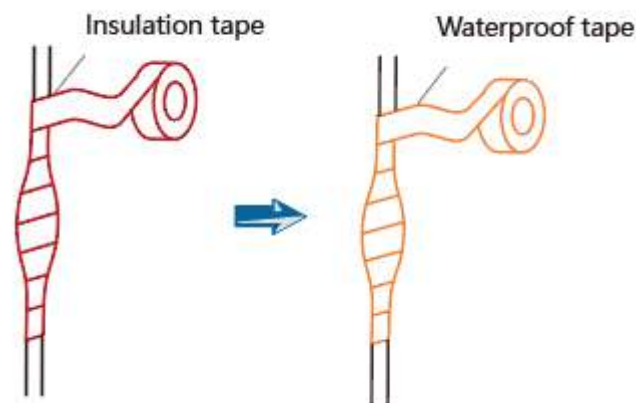
NOTICE

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

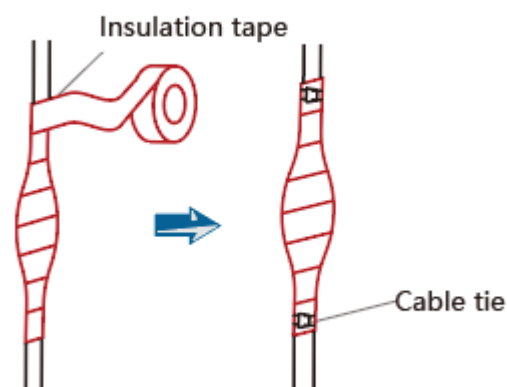
- Step 1** Wrap one layer of insulation tape around the joint of each cable. Stretch the waterproof tape evenly to twice its original length. Then, apply one layer of waterproof tape.

Figure 3-41 Wrapping the insulation tape and waterproof tape



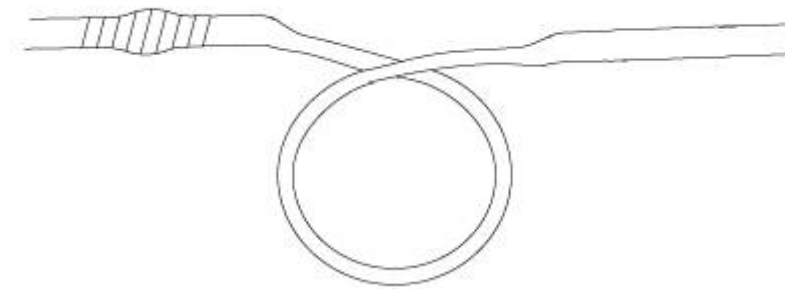
- Step 2** Use the insulation tape to protect the waterproof tape layer. Use cable ties to secure both ends of the tape.

Figure 3-42 Wrapping insulation tape and using cable ties to secure both ends of the tape



- Step 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 3-43](#), forms the lowest point of the cable.

Figure 3-43 Drip loop



----End

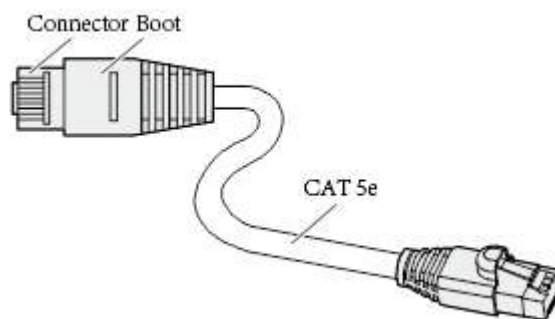
3.6.2 Making the Network Cable

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 3-44 Components of the network cable

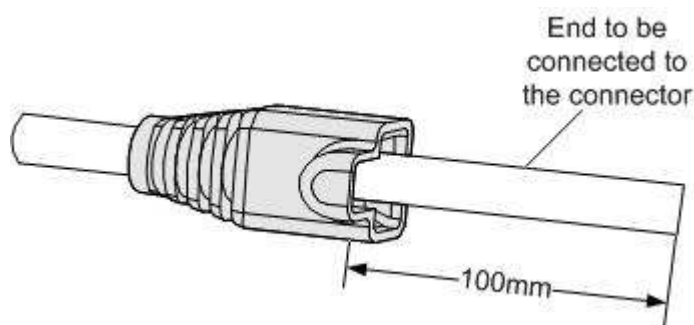


Procedure

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

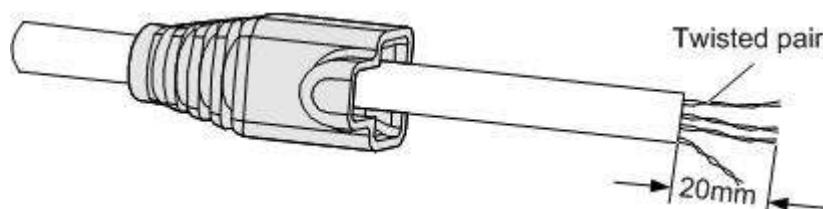
- Step 1** Insert the cable into the boots, and reserve at least 100 mm for the boots. Do not put the boots in reverse direction. [Figure 2](#) shows the right direction.

Figure 3-45 Installing the boots for the RJ45 connector



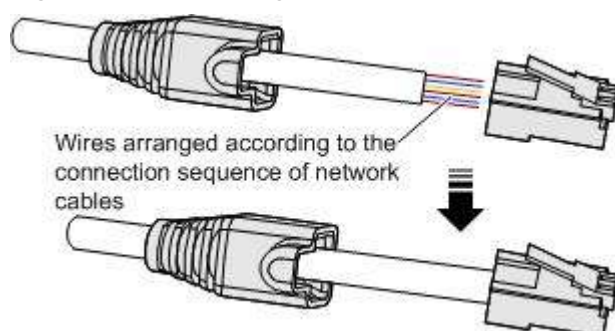
Step 2 Use a blade or a knife to peel 20 mm off the jacket. Do not damage the insulation of the wires, as shown in [Figure 3](#).

Figure 3-46 Peeling the jacket



Step 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 3-47 Installing the wires



[Table 1](#) shows two types of network cable sequences.

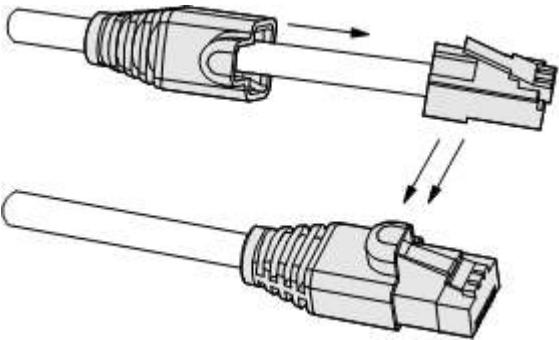
- When the straight-through cable is made, the sequences of both ends of the network cable should be consistent, that is, both ends of the network cable are sequence A or sequence B at the same time.
- When the crossover cable is made, the sequences of both ends of the network cable should be inconsistent,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

Table 3-5 Connection sequence of the network cables

Pin on the Network Cable	A	B
1	White/Orange	White/Green
2	Orange	Green
3	White/Green	White/Orange
4	Blue	Blue
5	White/Blue	White/Blue
6	Green	Orange
7	White/Brown	White/Brown
8	Brown	Brown

- Step 4** Use the RJ45 crimping tool to crimp the RJ45 connector. The metal cover on the connector should be lower than the plastic cover.
- Step 5** Use a network cable tester to check and ensure the wires are properly connected.
- Step 6** Push the boots to cover the RJ45 connector, as shown in [Figure 5](#).

Figure 3-48 Pushing the boots to cover the RJ45 connector



----End

3.6.3 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 3-6 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 3-49 Disassembling the rain wiper bracket



Step 1 Remove the old rubber strip and insert the new rubber strip through the hole, as shown in [Figure 2](#).

Figure 3-50 Replacing the rain wiper rubber strip



- Step 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 3-51 Installing the rain wiper bracket



----End

 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

4 Configuration

[4.1 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.

[4.2 Web Page Layout](#)

Users 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.

[4.3 Introduction to the Right Pane on the View Page](#)

On the right pane of the **View** page, you can set common camera parameters such as image and video parameters as well as network parameters such as the camera IP address and system time. The parameters displayed on the right pane vary between camera models.

[4.4 Playback](#)

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

[4.5 Snapshot Configuration](#)

This section describes the snapshot types and related configurations. You can download snapshots from the camera web system.

[4.6 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.

[4.7 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.

[4.8 Managing the System](#)

This section describes how to configure system operations.

[4.9 Network Configuration](#)

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

[4.10 Video and Audio Configuration](#)

This chapter describes how to set video and audio parameters.

[4.11 Configuring Images](#)

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

[4.12 Intelligent Settings](#)

This section describes how to configure intelligent analysis functions.

[4.13 Storage Configuration](#)

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

[4.14 Event Alarm Configuration](#)

This chapter describes how to configure alarm reporting, certificate alarms, and fault alarms.

[4.15 FAQs](#)

This chapter describes how to locate and troubleshoot common faults.

[4.16 FAQs](#)

This chapter describes how to locate and troubleshoot common faults.

[4.17 Configuring Image Optimization](#)

4.1 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.

4.1.1 Computer Software and Hardware Requirements

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

Table 4-1 describes the specifications for the computer.

Table 4-1 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

Software/ Hardware	Specification
Disk	300 GB or greater
Monitor	22 inches or above
Operating system and browser	- Windows 7: Chrome 55+, Firefox 70+, Microsoft Edge 50+, and 360 Secure Browser 9.1+ - Windows 8: Chrome 55+, Firefox 70+, Microsoft Edge 50+, and 360 Secure Browser 9.1+ - Windows 10: Chrome 55+, Firefox 70+, Microsoft Edge 50+, and 360 Secure Browser 9.1+ NOTE - Only 32- or 64-bit Windows operating systems are supported. - To use functions such as live video viewing, you need to download the web plug-in. Ensure that the computer is on the public network so that the web plug-in can be downloaded from the public network server. - To download Google Chrome, click here. - To download Firefox, click here. - To download Microsoft Edge, click here. - To download 360 Secure Browser, 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. - To view live video using 360 Secure Browser, do not use the incognito mode to access the camera.

4.1.2 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.

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:

- Step 1** On the computer, choose **Control Panel > Network and Internet > Network and Sharing Center** to access the **Network and Sharing Center** page.
- Step 2** Click **Local Connection**. The **Local Area Connection Status** page is displayed.
- Step 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 4-1](#) is displayed.
- Step 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 4-1](#), the IP address of the computer is set to 192.168.0.100.

NOTE

The default gateway can be left empty.

Figure 4-1 Changing the computer IP address

The screenshot shows a 'General' tab in a network configuration window. It contains instructions about automatic IP assignment and two main sections for manual configuration. The first section, 'Use the following IP address:', has three input fields: 'IP address' (192 . 168 . 0 . 100), 'Subnet mask' (255 . 255 . 255 . 0), and 'Default gateway' (192 . 168 . 0 . 1). The second section, 'Use the following DNS server addresses:', has two input fields: 'Preferred DNS server' and 'Alternate DNS server', both showing three dots. There is a checkbox for 'Validate settings upon exit' and an 'Advanced...' button. At the bottom are 'OK' and 'Cancel' buttons.

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

----End

4.1.3 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

- Step 1** Right-click the browser 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

- 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.
- The following web system languages are supported: Chinese, French, Spanish, Turkish, Thai, Portuguese (Brazil), Portuguese (Europe), and English
- Set the password as prompted when you log in for the first time, as shown in [Figure 4-2](#).

Step 2 Upon the first login, set the password and **Password Validity Period**, and keep the new password secure. The login user name is **admin**.

Figure 4-2 Setting the password

You are accessing the device for the first time. Please set the password

User name

admin

New password

Confirm password

Password Validity Period

Permanently valid

This change will change the passwords of all other accounts. ?

The web password is independent from protocol passwords such as the ONVIF and SDK passwords

OK

Cancel

 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.
- Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords.

You are advised not to set the new password to a weak password. The default weak passwords include **Cspdb@2017**, **kafka-1qaz@WSX**, **CSP@gaussdb@2017**, **UGW9811adminhwbs@com**, **hwbs@com**, **sps600@HW**, **Changeme_123**, **hwoata2.0**, **cnp200@HW**, **omu800@HW**, **mt2013@HW**, **GrUB1@ATCA**, **x86bpw**, **admin@86**, **data1@HW**, **Admin_12#**, **pgw#2013**, **Pmssys@2013**, **Admin@123**, **Update@7*24**, **9061csl**, **cgp data2@HW**, **sys data1@HW**, **bmu_hss**, **sek12345**, **HWps123**, **cnp123@HW**, **Spark@123**, **Hbase@123**, and **Hdfs@123**.

Step 3 Click **OK**.

Step 4 Refresh the page, enter the user name and password, and click **Log In**. The **Password Recovery** page is displayed.

Step 5 (Optional) Configure password recovery.

1. Select **Enable**, as shown in [Figure 4-3](#).

Figure 4-3 Enabling the function of password recovery through security questions

Password Recovery

Password recovery through security questions

☒ Enable

Question 1 ☐ Custom question

Answer

Question 2 ☐ Custom question

Answer

Question 3 ☐ Custom question

Answer

OK

Skip

2. Select a preset question from the **Question X** drop-down list box or select **Custom question** and customize a question.
3. 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.
4. Click **OK**. The wizard-based configuration page is displayed.
You can perform quick configuration following the wizard. For details, see [4.6 Wizard-based Configuration Guide](#).

- Step 6

Click  in the upper left of the page. The home page is displayed.
- Step 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.
- End

Recovering the Password

- Step 1

Log in to the camera web system (<https://Camera IP address>).
- Step 2

Click **Forgot Password**. The **Security Questions** dialog box, as shown in [Figure 4-4](#).

Figure 4-4 Security Questions dialog box

Security Questions

Question 1

What is your favorite sport?

Answer

Provide the answer to your question.

Question 2

Which was the first city you visited on holiday?

Answer

Provide the answer to your question.

Question 3

What is your favorite fruit?

Answer

Provide the answer to your question.

If you forget the operator password, contact the administrator to reset it.

OK

Cancel

- Step 3

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 4-5](#).
The login user name is **admin**. Set the password and **Password Validity Period** and keep the new password secure.

Figure 4-5 Resetting the password

User name: admin

New password: [Red box]

Confirm password: [Empty box]

Password Validity Period: Permanently valid

This change will change the passwords of all other accounts. ⓘ

OK Cancel

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.
- Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords.

You are advised not to set the new password to a weak password. The default weak passwords include **Cspdbbr@2017**, **kafka-1qaz@WSX**, **CSP@gaussdb@2017**, **UGW9811adminhwbs@com**, **hwbs@com**, **sps600@HW**, **Changeme_123**, **hwosta2.0**, **cnp200@HW**, **omu800@HW**, **mt2013@HW**, **GrUB1@ATCA**, **x86bpw**, **admin@86**, **data1@HW**, **Admin_12#**, **pgw#2013**, **Pmssys@2013**, **Admin@123**, **Update@7*24**, **9061csl**, **cgp data2@HW**, **sys data1@HW**, **bmu_hss**, **sek12345**, **HWps123**, **cnp123@HW**, **Spark@123**, **Hbase@123**, and **Hdfs@123**.

Step 4 Click **OK**.

----End

4.2 Web Page Layout

Users 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(x86)\CameraPlayerPluginInstall`
- 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.
- To use functions such as live video viewing, you need to download the web plug-in. Ensure that the computer is on the public network so that the web plug-in can be downloaded from the public network server.
- 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.

Figure 4-6 shows the web page layout.

Figure 4-6 Web page layout

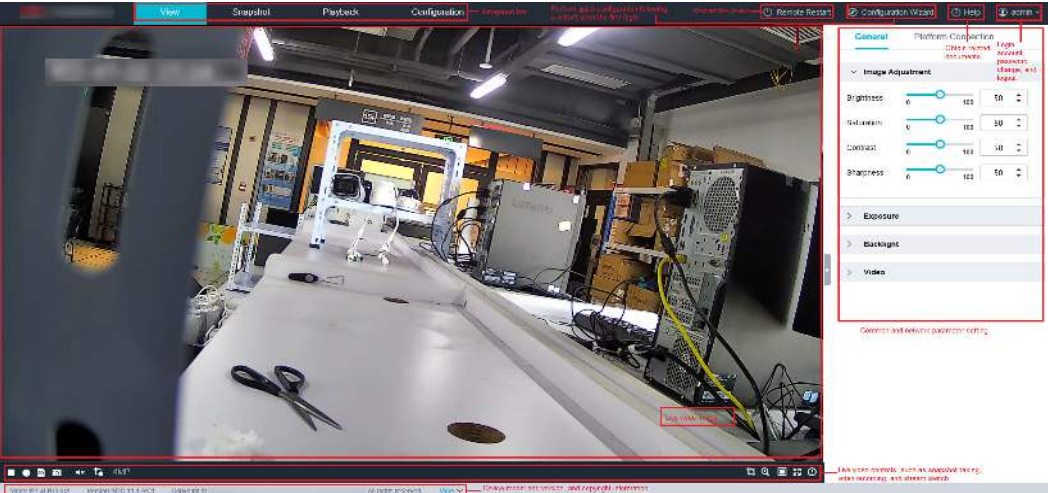


Table 4-2 describes the buttons in the lower part of the **View** page.

Table 4-2 Button description

Button	Description
	Stop/Start live video viewing. NOTE • Only one stream encryption channel is supported during live video viewing.

Button	Description
	Local recording button. You can click this button to enable or disable local recording. The recordings are stored in the <i>Path for storing recording files \Camera IP address</i> directory. The recording is named in <i>Camera model_YYYY-MM-DD-HH-MM-SS_MSMSMS</i> 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 4.7.2 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 4.13.1 Configuring Storage Management.
	Snapshot button. You can click this button to take a snapshot during live video viewing. The captured images are stored under <i>Path for storing live snapshots \Camera IP address</i>. The image is named in <i>YYYY-MM-DD_HH-MM-SS-MSMS</i> format, for example, 2014-03-28_09-59-36-98. For details about how to configure the path for storing live snapshots, see 4.7.3 Setting Snapshot File Parameters. NOTE You must run the browser as an administrator.
	The channel-associated voice function is disabled by default. After this function is enabled, voice at the camera 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.

Button	Description
	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.
	Crop an area on the live video image and zoom in on it.
	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.

4.3 Introduction to the Right Pane on the View Page

On the right pane of the **View** page, you can set common camera parameters such as image and video parameters as well as network parameters such as the camera IP address and system time. The parameters displayed on the right pane vary between camera models.

4.3.1 Setting Common Image Parameters

You can set common image parameters to adjust the image effect. Image parameters vary depending on camera models.

- Step 1** On the **View** tab page, click the **General** tab to access the **General** tab page.
- Step 2** Click **Image Adjustment**. The **Image Adjustment** area is displayed, as shown in [Figure 4-7](#).

Figure 4-7 Setting image adjustment parameters

Image Adjustment

Brightness

0100

50

Saturation

0100

50

Contrast

0100

50

Sharpness

0100

50

- Step 3** Set common image parameters. [Table 4-3](#) describes the parameters. For details about image parameter settings, see [4.11.2 Setting Image Parameters](#).

Table 4-3 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.

- Step 4** Click **Exposure**. The **Exposure** area is displayed, as shown in [Figure 4-8](#).

Figure 4-8 Setting exposure parameters

▼ Exposure

Exposure mode

Manual ▼

Shutter speed

1/25 s ▼

Gain

0100

0 ▲▼

Table 4-4 Exposure parameters

Parameter	Description
Exposure mode	Exposure mode. ● Auto (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. ● Manual: You need to 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 . Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure 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.
Shutter limit	This parameter is available only when you set Exposure mode to Auto . This parameter is used to specify the minimum shutter speed. You can use common values or customize values (unit: μ s).
Gain limit	This parameter is available only when you set Exposure mode to Auto . The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC). 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.

Parameter	Description
Gain	This parameter is available only when you set Exposure mode to Manual . The default value is 0 .

Step 5 Click **Backlight**.

Figure 4-9 Setting backlight parameters

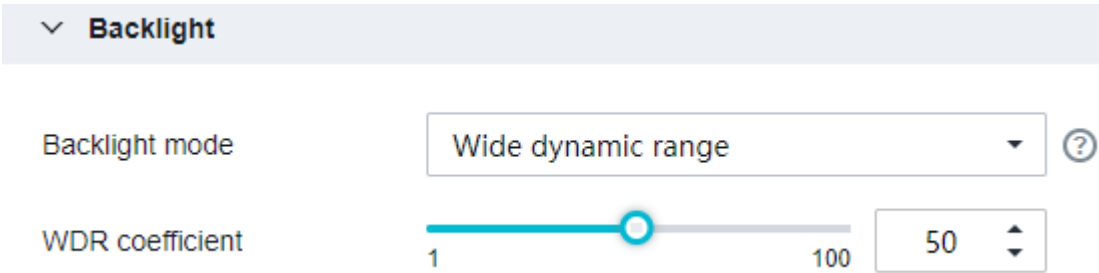


Table 4-5 Backlight parameters

Parameter	Description
Backlight mode	This parameter is available only when you set Exposure mode to Auto. • 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. • 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.
WDR coefficient	This parameter is available only when you set Exposure mode to Auto and Backlight mode 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 level	This parameter is available only when you set Exposure mode to Auto and Backlight mode to Highlight compensation. The default value is Medium. A higher HLC level indicates more powerful highlight compensation.

-----End

4.3.2 Setting Common Video Parameters

This section describes how to set common video parameters.

Procedure

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

The **Video** area is displayed, as shown in [Figure 4-10](#). The parameters displayed on the web page vary depending on the camera model.

Figure 4-10 Video area

Primary Stream

Secondary Stream 1

Encoding protocol

H.265

Resolution

2560*1440

Frame rate

25

Max. bit rate (kbit/s)

512

8192

6144

- Step 3 Set video parameters. [Table 4-6](#) describes the parameters.

Table 4-6 Video parameters

Parameter	Description
Encoding protocol	Video encoding protocol. The options are as follows: • H.264: The H.264 protocol requires relatively low bandwidth to ensure video quality. • H.265: The H.265 protocol is bandwidth-conserving compared with the H.264 protocol. 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.264 and H.265.
Resolution	Video resolution. A higher resolution indicates clearer images and higher bandwidth consumption.
Frame rate	Number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.
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.
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 actually required bandwidth 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. • 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.

Step 4 Click **Save**.

----End

4.3.3 Setting Network Parameters

This section describes how to set network parameters, such as the camera IP address and secondary protocol.

Setting Camera IP Addresses

Step 1 On the **View** page, choose **Network Parameters > Modifying an IPv4 Address**. The **Modifying an IPv4 Address** area is displayed, as shown in [Figure 4-11](#).

Figure 4-11 Modifying an IPv4 Address area

Method of obtaining

☒ Manual ☐ Auto

* IPv4 address



* Subnet mask

Gateway

MAC address

d8:59:82:4f:aa:00

Primary DNS

0 - 0 - 0 - 0

Secondary DNS

0 - 0 - 0 - 0

Save

Step 2 Set the camera IP address as planned. [Table 4-7](#) describes the parameters.

Table 4-7 IP address parameters

Parameter	Description
Method of obtaining	Method for obtaining the IP address. The options are Manual and Auto . NOTE When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can click Auto to check the IP address. The camera IP address allocated by the server is fixed.
IPv4 address	Camera IP address. This parameter can be set only when Method of obtaining is set to Manual . 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.

Parameter	Description
Subnet mask	Subnet mask of the network where the camera is located.
Gateway	Gateway IP address of the network where the camera is located.
MAC address	Camera MAC address. This parameter is read-only.
Primary DNS	IP address of the primary DNS server. 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) - 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	IP address of the secondary DNS server. 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)

----End

Setting Second Protocol Parameters

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:

- Step 1** On the **View** page, choose **Network Parameters > Second Protocol Parameters**. The **Second Protocol Parameters** area is displayed, as shown in [Figure 4-12](#).

Figure 4-12 Second Protocol Parameters area



- Step 2** Set the second protocol as planned. [Table 4-8](#) describes the parameters. For detailed operations, see [4.9.2 Setting Platform Connection Parameters](#).

Table 4-8 Second protocol parameters

Parameter	Description
Enable	After Enable is toggled on, the ONVIF connection protocol is enabled for the device.

----End

4.3.4 Setting 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.

Configuring System Time

- Step 1** On the **View** page, choose **Network Parameters > Time**. The **Time** area is displayed.
- Step 2 Optional:** Configure system time, as shown in [Figure 4-13](#).

Figure 4-13 Configuring system time

Time

Time zone

(UTC+08:00) Beijing, Hon... ▾

Calibration mode

☒ Manual

☐ NTP

Device time

Time

📅

☐ Synchronize time with computer

If the time is set to earlier than 2022-07-01 00:00:00, 2022-07-01 00:00:00 is used by default.

Save

1. Select a time zone from the **Time zone** drop-down list box.
2. Select a time calibration mode and set related parameters. For details, see [Table 4-9](#).

 NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- You are advised to use NTP or protocol-based time calibration to prevent inconsistency between the device time and the actual time due to device power-off or frequent restart.
- 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 4-9 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. 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, select 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. The camera synchronizes time with the NTP server at a specified interval.

Step 3 Click **Save**.

----End

Configuring Daylight Saving Time

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

Step 1 On the **View** page, choose **Network Parameters > Time**. The **Time** area is displayed.

Step 2 Configure DST, as shown in [Figure 4-14](#).

Figure 4-14 Configuring DST

DST mode

☐ Enable

DST mode

☒ Week ☐ Date

Start time

Apr First Monday 02:00 

End time

Oct Last Monday 02:00 

Time offset

30 min 

Save

Step 3 Configure the DST.

- 1. Select **Enable**.
- 2. Click **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.

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

[Table 4-10](#) describes the DST parameters.

Table 4-10 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.

Step 4 Click **Save**.

----End

4.4 Playback

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

4.4.1 Playing Back Recordings

You can play back recordings in the camera web system.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Playback**. The **Playback** page is displayed, as shown in [Figure 4-15](#).

Figure 4-15 Playback page



Step 3 Search for recordings.

1. On the left of the page, set **Recording** and **Period**.
 - The maximum interval between start time and end time is 24 hours.
 - The following recording types are supported:
 - **Scheduled:** Video recorded as scheduled. For details about how to configure a recording plan, see [4.13.3 Configuring a Recording Plan](#).
 - **Triggered:** Video recorded during intelligent analysis. Some intelligent analysis functions can trigger video recording. To enable video recording for a specified intelligent analysis function, go to the **Linkage Policy** page and select **Enable recording**.
 - **Active recording:** Video recorded by clicking  on the **View** page.

- **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 [4.13.3 Configuring a Recording Plan](#).

2. Click **Search**.

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.

Step 4 Select the desired recording and play it back.

- To start recording playback, click .
- To stop recording playback, click .
- To adjust the playback progress, drag the timeline.
- To adjust the timeline scale, click  and  or directly select a time interval from the drop-down list box in the lower right corner of the page.

----End

4.4.2 Downloading Recordings

This section describes how to query and download recordings.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Playback** and click **Download** in the lower left corner of the page. The **Download** dialog box is displayed, as shown in [Figure 4-16](#).

Figure 4-16 Download dialog box

Step 3 Search for recordings.

1. Set **Period**.
2. Click **Search**.

 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.
- 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 [4.16.2 Why Is a Recording Separately Stored into Multiple Files of Different Sizes?](#).

Step 4 Download recordings.

1. Select the recording to download.
2. 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.

----End

4.5 Snapshot Configuration

This section describes the snapshot types and related configurations. You can download snapshots from the camera web system.

4.5.1 Downloading Snapshots

You can download snapshots stored in SD cards of cameras to the local computer or view snapshots online.

 NOTE

If no SD card is inserted into a camera, the **Snapshot** module is not displayed in the camera web system.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Snapshot**. The snapshot download page is displayed, as shown in [Figure 4-17](#). [Table 4-11](#) describes the parameters.

The web page varies between camera models.

Step 3 Set **Snapshot type** and **Period**, and click **Search** to search for the snapshots to be downloaded.

Figure 4-17 Configuring snapshot download

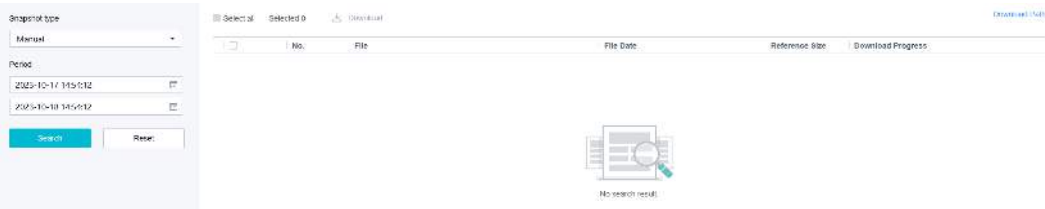


Table 4-11 Snapshot download parameters

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. ● Scheduled: scheduled snapshots. To enable the scheduled snapshot function, choose Configuration > Storage > Snapshot and toggle on Enable scheduled snapshot. 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.
Period	Start time and end time for querying snapshots.

Step 4 Select the snapshot to download and click **Download**. After the download is complete, you can double-click the image to open it.

NOTE

- If you select **Select all**, all snapshots searched out can be downloaded. You can query a maximum of 1024 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.

----End

4.6 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.

4.6.1 Setting Camera IP Addresses

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

Procedure

- Step 1
- Log in to the camera web system (<https://Camera IP address>).
- Step 2
- Click **Configuration Wizard** in the upper right corner of the web page. The **IP** page is displayed by default, as shown in [Figure 4-18](#).

Figure 4-18 Setting the IPv4 address

IPv4 address assignment

☒ Manual ☐ Auto

IPv4 address

Check

IPv4 subnet mask

IPv4 gateway

MAC address

Primary DNS

Secondary DNS

Save

- Step 3
- Set the camera IPv4 address as planned. [Table 4-12](#) describes the parameters.

Table 4-12 IP address parameters

Parameter	Description
IPv4 address assignment	Method for obtaining the IPv4 address. The options are Manual and Auto. NOTE When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can click Auto to check the IP address. The camera IP address allocated by the server is fixed.
IPv4 address	Camera IPv4 address. This parameter can be set only when IPv4 address assignment is set to Manual. 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 subnet mask	Subnet mask of the network where the camera is located.
IPv4 gateway	Gateway IP address of the network where the camera is located.
MAC address	Camera MAC address. This parameter is read-only.
Primary DNS	IP address of the primary DNS server. 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	IP address of the secondary DNS server. 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)

Step 4 Click **Save**.

----End

Setting the IPv6 Address

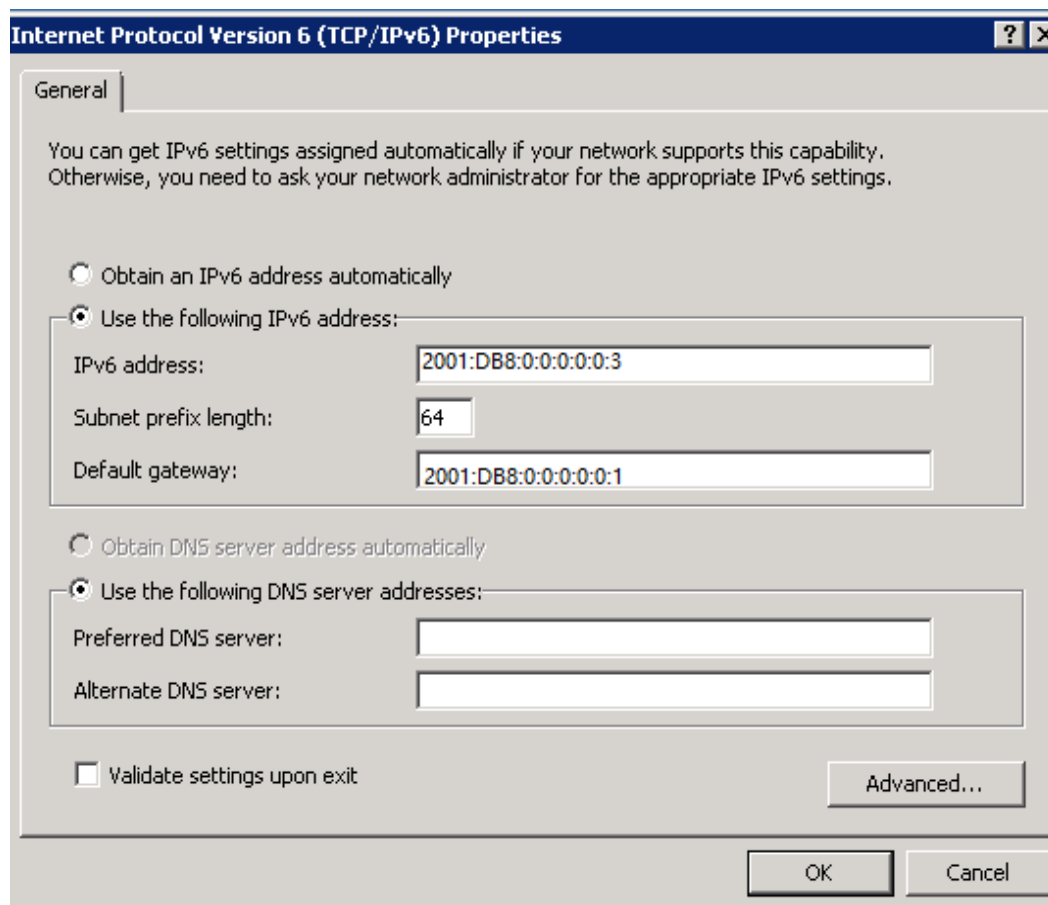
The IPv6 address is numbered in hexadecimal notation and is divided into eight blocks by colons (:). Each block contains 16 bits, for example, fe80:0da8:65b4:05d3:1315:7c1f:0461:7847.

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.

Step 1 Set the IPv6 address of the local computer.

1. Run the **regedit** command on the local computer, choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > services > TCPIP6 > Parameters**, delete **DisabledComponents**, and restart the local computer.
2. On the computer, choose **Control Panel > Network and Internet > Network and Sharing Center** to access the **Network and Sharing Center** page.
3. 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 4-19](#) 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:DB8:0:0:0:0:3**.

Figure 4-19 Setting the IPv6 address



Step 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, click **IPv6**. On the tab page that is displayed, select **Enable**, as shown in [Figure 4-20](#).

Figure 4-20 Setting the IPv6 address

☒ **Enable**

If IPv6 is enabled, the MTU value range will change. [MTU Settings](#)

IPv6 address assignment

☐ Manual ☐ Auto ☒ Route advertisement

You can

* IPv6 address

0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

* IPv6 subnet prefix

0

IPv6 gateway

0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

MAC address

d8:59:82:4f:a9:f8

Save

Table 4-13 IP address parameters

Parameter	Description
IPv6 address assignment	Method for obtaining the IPv6 address. The options are Manual , Auto , 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 .

Step 3 Click **Save**.
----End

4.6.2 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.

Configuring System Time

- Step 1
- Log in to the camera web system (<https://Camera IP address>).
- Step 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 4-21](#). The web page varies between camera models.

Figure 4-21 Time tab page

Time

Time zone

(UTC+08:00) Beijing, Hong Kong (China... ▾

Calibration mode

☒ Manual

☐ NTP

Device time

11:07:38

Time

11:06:13

📅

☐ Synchronize

If the time is set to earlier than 2022-07-01 00:00:00, 2022-07-01 00:00:00

Save

1.
- Select a time zone from the **Time zone** drop-down list box.
2.
- Select a time calibration mode and set other related parameters. [Table 4-14](#) describes the parameters.

 NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- You are advised to use NTP or protocol-based time calibration to prevent inconsistency between the device time and the actual time due to device power-off or frequent restart.
- 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 4-14 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. 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, select 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  to check whether the NTP server IP address is available.

Step 3 Click **Save**.

----End

Configuring DST

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

Step 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 4-22](#). The web page varies between camera models.

Figure 4-22 Configuring the DST

DST

☐ Enable

DST mode

☒ Week ☐ Date

Start time

Apr First Monday 02:00

End time

Oct Last Monday 02:00

Time offset

30 min

Save

- Step 2** Configure the DST.
1. Select **Enable**.
 2. Click **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.
 3. Set **Start time**, **End time**, and **Time offset** of the DST based on regulations specified in the local laws.
- Table 4-15** describes the DST parameters.

Table 4-15 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.

Step 3 Click **Save**.

----End

4.6.3 Configuring Video

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

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 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 4-23](#).

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

Figure 4-23 Setting video parameters

Number of secondary streams

1

Full frame rate

PAL(25Hz)

?

Primary Stream

Secondary Stream 1

Encoding protocol

H.264

Resolution

2560*1440

Frame rate

25

Max. bit rate (kbit/s)

512

8192

4096

Advanced

▲

☐ Intelligent encoding

Bit rate type

Variable bit rate

Encoding complexity

High

I-frame interval

1

500

50

Stream smoothing coefficient

☐

1

100

50

?

☒ Slice

Save

Step 3 Set video parameters. [Table 4-16](#) describes the parameters.

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

Table 4-16 Video parameters

Parameter	Description
Number of secondary streams	Number of secondary streams. Value 0 indicates that only the primary stream can be set. Value 1 indicates that both primary and secondary streams can be set. • 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. The thermal imaging channel of a thermal camera can be set only to Primary Stream.
Full frame rate	Frame rate collected through the sensor, representing the maximum capability of a camera. 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.
Encoding protocol	Video encoding protocol. • H.264: The H.264 protocol requires relatively low bandwidth to ensure video quality. • H.265: The H.265 protocol is bandwidth-conserving compared with the H.264 protocol. 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.264 and H.265.
Resolution	Video resolution. A higher resolution indicates clearer images and higher bandwidth consumption.
Frame rate	Number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.

Parameter	Description
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.
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 actually required bandwidth 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. - 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.
Intelligent encoding	Indicates whether to enable intelligent encoding. If it is enabled, the camera can automatically adapt to scenarios to reduce bit rate and save 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, and I-frame interval 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. - After the function of rotating images by 90° is enabled, the encoding compression ratio will decrease.
Bit rate type	Type of the bit rate. 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 dynamic changes, the images will be unclear.

Parameter	Description
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 After intelligent encoding is enabled, the options of Bit rate control mode are Balanced, Image quality priority, and Bit rate compression priority.
Encoding complexity	This parameter is available only when Encoding protocol is set to H.264 or H.265 or other related formats. 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 encoding protocol is changed to H.264, High profile is used by default.
I-frame interval	This parameter is available only when Encoding protocol is set to H.264 or H.265. 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.
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.
Slice	Indicates whether to enable multi-slice encoding. The parameter is available only when Encoding protocol is set 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 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.

Step 4 Click **Save**.

----End

4.6.4 Configuring Intelligent Analysis Functions

This section describes the features supported in each intelligent analysis mode.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Intelligence** page is displayed.

Step 3 Select a required device, and select a task type under the required intelligent analysis mode. [Table 4-17](#) lists the intelligent analysis tasks supported in each mode.

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

Table 4-17 Intelligent tasks

Intelligent Analysis Mode	Task Type	How to Configure
Common event analysis	Motion detection	For details, see 4.12.1.2 Configuring Motion Detection .
	Lens blocking detection	For details, see 4.12.1.3 Configuring Lens Blocking Detection .
	Human figure detection	For details, see 4.12.1.4 Configuring Human Figure Detection .

----End

4.6.5 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 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.
- Step 3** Set related parameters based on the site requirements. The following describes the parameters.
- End

Image Adjustment

Figure 4-24 Setting image adjustment parameters



Table 4-18 Image adjustment parameters

Parameter	Description
Brightness	Brightness of images captured by a camera.
Saturation	Colorfulness of a color relative to its own brightness.

Parameter	Description
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 4-25 Setting day/night switch parameters

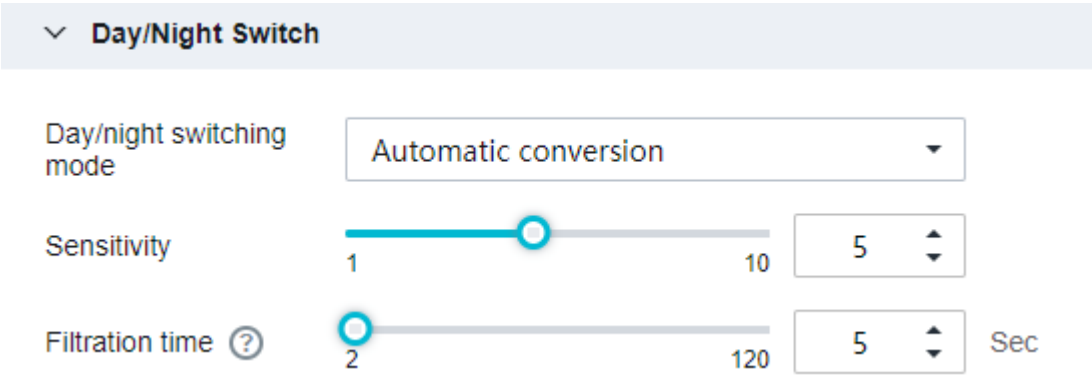


Table 4-19 Day/Night switch parameters

Parameter	Description
Day/night switching 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. Automatic conversion: The camera automatically switches between the color mode and the B/W mode based on ambient light conditions. NOTE For some camera models, if Day/night switching mode is set to Automatic conversion, 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 conversion: If you select this option, you need to customize Night Mode. This mode is applicable to scenarios that require specified day/night switch time or unified day/night switch time for multiple cameras.

Parameter	Description
Sensitivity	This parameter is available only when Day/night switching mode is set to Automatic conversion . Sensitivity for switching between color mode and B/W mode. Higher sensitivity indicates that B/W mode is more likely to switch to color mode but color mode is less likely to switch to B/W mode. The default value is 5.
Filtration time	This parameter is available only when Day/night switching mode is set to Automatic conversion . When the ambient illuminance meets the day/night switch requirements and keeps at a level for a period specified by this parameter, the day/night mode is switched. The default value is 5, in seconds.

Exposure

The exposure parameters vary depending on the camera model.

Figure 4-26 Setting exposure parameters

▼ Exposure

Exposure mode

Manual

Shutter speed

1/25 s

Gain

0100

0

Table 4-20 Exposure parameters

Parameter	Description
Exposure mode	Exposure mode. Auto (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. Manual: You need to manually set the shutter speed and gain when the auto exposure mode cannot meet the site requirements.

Parameter	Description
Exposure compensation coefficient	This parameter is available only when you set Exposure mode to Auto. Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure 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.
Shutter limit	This parameter is available only when you set Exposure mode to Auto. This parameter is used to specify the minimum shutter speed. You can use common values or customize values (unit: μs).
Gain limit	This parameter is available only when you set Exposure mode to Auto. The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC). 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 default value is 0.

Backlight

Figure 4-27 Setting backlight parameters

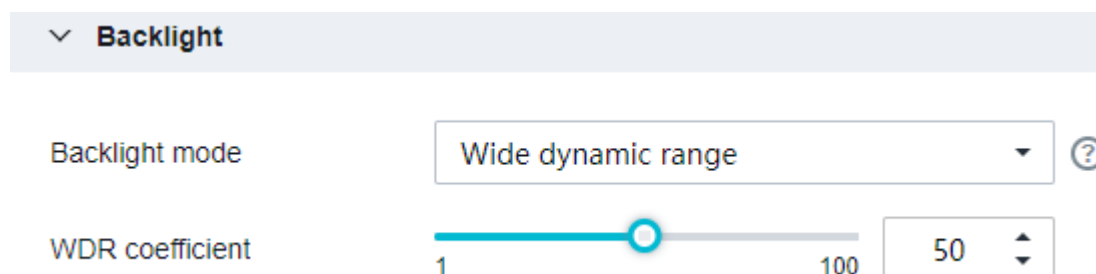


Table 4-21 Backlight parameters

Parameter	Description
Backlight mode	This parameter is available only when you set Exposure mode to Auto. • 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. • 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.
WDR coefficient	This parameter is available only when you set Exposure mode to Auto and Backlight mode 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 level	This parameter is available only when you set Exposure mode to Auto and Backlight mode to Highlight compensation. The default value is Medium. A higher HLC level indicates more powerful highlight compensation.

White Balance

Figure 4-28 Auto white balance parameters

▼ White Balance

Mode

Auto White Balance

Red Tendency

0100

50

Blue Tendency

0100

50

Regional white balance

Figure 4-29 Manual white balance parameters

▼ White Balance

Mode

Manual white balance

Red gain

0100

50

Blue gain

0100

50

Figure 4-30 Automatic tracking parameters

▼ White Balance

Mode

Auto tracking

CT upper limit

100015000

10000

CT lower limit

100015000

1500

Regional white balance

Table 4-22 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 White Balance (default): This mode is recommended. The camera automatically adjusts the gain 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. In this case, you can drag the slider to change the values of Red Tendency and Blue Tendency or directly enter an integer in corresponding text boxes. – Regional white balance: This parameter is available only when you set Mode to Auto White Balance or Auto tracking. If you toggle on Regional white balance, you can configure a white balance area on the View page. Then the white balance function takes effect only in this area. • Manual white balance: The red and blue gain must be adjusted manually. You can drag the slider to change the values of Red gain and Blue gain or directly enter 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. – Regional white balance: This parameter is available only when you set Mode to Auto White Balance or Auto tracking. If you toggle on Regional white balance, you can configure a white balance area on the View page. Then the white balance function takes effect only in this area. • Lock white balance: 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. • Global white balance: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 3500 K to 4500 K.

Image Enhancement

The image enhancement functions vary depending on the camera model.

Figure 4-31 Image enhancement parameters in manual mode

Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

☐

Defogging

Manual

Defogging level

0100

50

Anti-light flicker

Disable

Denoising

Automatic noise reduction

IR overexposure compensation

0100

50

Table 4-23 Image enhancement parameters

Parameter	Description
Rotate images by 90 degrees	Indicates whether to enable the function of rotating images by 90 degrees (aspect ratio: 9:16 or 3:4). NOTE To enable this function, 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.
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.

Parameter	Description
Defogging	This function is used to increase image clarity in poor weather conditions such as rain, fog, and smog. To disable this function, set this parameter to Disable. If this parameter is set to Overcast adaptation, 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.
Anti-light flicker	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 this parameter based on standard frequency of the local power grid. For example, if the standard frequency of the local power grid is 50 Hz, this parameter needs to be set to 50Hz. In natural light conditions, set this parameter to Disable.
Denoising	Indicates whether to enable the noise reduction function. The options are as follows: • Disable: Disable the noise reduction function. • Automatic noise reduction (default): The system automatically performs noise reduction. • Expert mode: The Spatial denoising level and Temporal denoising level parameters are available only when Denoising is set to Expert mode. – 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 denoising level indicates better noise reduction effect. However, more edge details will be lost. – 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.
IR overexposure compensation	If IR illuminators are enabled and overexposure occurs in the image view with strong reflective objects such as leaves and wires nearby, you can set this parameter to a larger value. The default value is 50.

Illuminator Control

Figure 4-32 Setting illuminator control parameters

▼ Illuminator Control

Built-in Illuminator

Control mode

Manual

Low beam

Brightness control

0100

50

2024-01-25

105

Table 4-24 Illuminator control parameters

Parameter		Description
Built-in Illuminator	Control mode	• Auto (default): Indicates that the camera automatically turns on or off the illuminator and controls its brightness. • Manual: Indicates that the illuminator 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 and Brightness control. • Intelligent light compensation: The camera automatically performs light compensation. In B/W mode at night, when motion detection or human figure detection is triggered, the camera switches to color mode and turns on the white-light illuminator. After the alarm is cleared, the white-light illuminator is automatically turned off and the video image turns back to B/W mode. NOTE • 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 camera determines whether to enable white-light or IR illuminators based on the current ambient illuminance. The user-defined brightness takes effect only when the camera determines that illuminators need to be enabled. • Some camera models do not have white-light illuminators.
	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 set Turn-on time and Brightness control.
	Brightness control	This parameter is available only when Control mode is set to Manual or Scheduled. A larger value indicates higher illuminator brightness.

4.6.6 Configuring OSD

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

Setting OSD Parameters

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

Figure 4-33 Setting OSD parameters

OSD template

Custom

GB

Configuration

OSD mode

Custom

Template name

Custom

Font color

Invert OSD color

Font size

Self-adaptive

Line spacing

0

Align Type

Upper left alignment

OSD Content

+ Add OSD

🗑 Delete All

Horizon...	Vertical ...	Content	Operation
149	104	<code>\${time@sys: YYYY-MM-DD}</code>	InsertDelete

- Step 3 Configure the OSD template. [Table 4-25](#) describes the OSD template parameters and buttons.
- Hover the mouse over an OSD template and choose **Copy Template** from the drop-down menu. In the dialog box that is displayed, enter a new template name and click **OK**. The new template is added. A maximum of two OSD templates are supported currently.
 - Hover the mouse over an OSD template and choose **Delete Template** from the drop-down menu. In the dialog box that is displayed, click **OK** to delete the template.

Table 4-25 OSD template parameters/buttons

Parameter/ Button		Description
Conf igura tion	OSD mode	The value is determined by the OSD template and cannot be changed.
	Template name	Name of the selected template. You can customize the name as required.
	Font color	The options are Invert OSD color and Custom . If you select Invert OSD color , the OSD text color is set to a color opposite to the background color.
	Font size	The default value varies depending on the camera model. You can set this parameter depending on your needs.
	Line spacing	OSD line spacing.
	Align Type	OSD alignment mode. You can select an option from the drop-down list.
OSD Cont ent	Add OSD	Button for adding an OSD record using a template. NOTE - A maximum of six OSD records can be added to each customized OSD template. - In GB-compliant OSD mode, the number of OSD records is fixed to four. You cannot add or delete one.
	Delete All	This button is available only in custom OSD mode. If you click Delete All , all OSD records will be deleted.
	Horizontal Margin/ Vertical Margin	These parameters are available only in custom OSD mode. You can enter a number in the text boxes.
	Content	OSD text content. You can customize text content in the text box. NOTE The 6763 Chinese characters defined in GB2312 are supported.
	Operation	In custom OSD mode, two buttons Insert and Delete are displayed in the Operation column. In GB-compliant OSD mode, only the Insert button is displayed in the Operation column. To set OSD time, click Insert . To delete an OSD record, click Delete corresponding to the record.

----End

4.6.7 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.

4.6.7.1 Configuring Connection to the Platform Through SDK

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

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
- Step 3** Under **SDK Settings**, set SDK parameters, as shown in [Figure 4-34](#). [Table 4-26](#) 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 [4.8.1.2 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 4-34 Setting SDK parameters

Enable SDK

SDK non-encrypted port

Enabling the non-encrypted port will also enable TCP co

Platform 1

Platform 2

Platform 3

☐ Active SDK registration

☒ Two-factor authentication

Registration type

Single-server mode

Device ID

Active platform IP

Port numb

Save

Table 4-26 SDK parameters

Parameter	Description
Enable SDK	Indicates whether to enable SDK. SDK is enabled by default.
SDK non-encrypted port	Indicates whether to enable the SDK non-encrypted port. This port is enabled by default. After this port is enabled, the non-encrypted port can be registered.
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.

Parameter	Description
Registration type	The options are as follows: • Single-server mode: applies when the platform is deployed in a single-node system. • Dual-server mode: applies when the 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	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.
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.

Step 4 Click **Save**.

----End

4.6.7.2 Configuring Connection to the Platform Through ONVIF

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. If the platform is on a private network and the camera is on a public network, NAT traversal is not supported.
- 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
- Step 3** Click **ONVIF**. The **ONVIF** area is displayed.
- Step 4** Set ONVIF parameters, as shown in [Figure 4-35](#). [Table 4-27](#) describes the ONVIF parameters.

Figure 4-35 Setting ONVIF parameters

If the video encoding format is H.265, the old platform or NVR connected through ONV

Enable ONVIF

Validity period

?

Authentication mode

Digest_MD5(priority)/WSSE

WSSE authentication and MD5 encryption algorithms are insecure an

Version

ONVIF 16.12

Transmission protocol

HTTPS

Extended Parameters

Forbid ONVIF to change system time

After this function is enabled, the setting of Re

Reverse time zone

After this function is enabled, the time zone is reversed when the

Enable WSSE anti-replay

The time of the camera and the platform must be synchron

Save

Table 4-27 ONVIF parameters

Parameter	Description
Enable ONVIF	Indicates whether to enable the ONVIF protocol.
Validity period	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. This function is disabled by default.

Parameter	Description
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 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 4.9.2.1.2 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. • 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.
Reverse time zone	Indicates whether to reverse the time zone when you set the time through the ONVIF protocol.

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

Step 5 Click **Save**.

Step 6 (Optional) Change the ONVIF password.

Method 1:

1. Choose **Protocol Password > ONVIF Password**.
2. Set **Web user password**, **New password**, and **Confirm password**.
3. Click **Save**.

Method 2:

1. Choose **Configuration > System > Security Management > Password Management**.
2. Click **Protocol Password**.
3. On the **ONVIF Password** tab page, set **Web user password**, **New password**, and **Confirm password**.
4. Click **Save**.

 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.
- If 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.

----End

4.6.7.3 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.

Step 3 Under **RTSP**, set RTSP parameters, as shown in [Figure 4-36](#). [Table 4-28](#) describes the parameters.

Figure 4-36 Setting RTSP parameters

metadata extension

?

* Port

554

* Post-NAT port

554

Transmission Type

Elementary stream

?

Authentication mode

Digest_MD5

The MD5 encryption

Save

Table 4-28 RTSP parameters

Parameter	Description
metadata extension	Indicates whether to enable the function of obtaining intelligent analysis metadata from a camera in RTSP stream requesting mode.
Port	RTSP port.
Post-NAT port	External port number to which the camera's internal port number maps after NAT environment is configured.
Transmission Type	Type of streams to be transmitted. You can set this parameter to Elementary stream or Program stream based on the decoding device.
Authentication mode	• 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.

Step 4 Click **Save**.

----End

4.6.7.4 Configuring Connection to the Platform Through RESTful

This section describes how to connect a camera to the 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
- Step 3** Under **RESTful**, set RESTful parameters, as shown in [Figure 4-37](#). [Table 4-29](#) describes the parameters.

Figure 4-37 Setting RESTful parameters

Device ID

Transmission protocol

HTTPS

Authentication mode

Digest_SHA256

The more secure SHA256 authentication mode is recommended

☒ Enable proactive registration

* URL

?

User name

Password

Save

Table 4-29 RESTful parameters

Parameter	Description
Device ID	Unique device ID.
Transmission protocol	• HTTPS: Data is transmitted through HTTPS. • 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.

Parameter	Description
Enable proactive registration	Indicates whether to enable proactive registration. After proactive registration is enabled, you need to set the platform URL, user name, and password.
URL	Platform URL. Set this parameter to http://IP address:port number/xxx or https://IP address:port number/xxx , for example, https://10.3.4.55:98/nat .
User name	User name used by the camera to register with the platform. This parameter is optional.
Password	Password used by the camera to register with the platform. 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 [4.9.2.4 Setting the Protocol Connection Password](#).

Step 4 Click **Save**.

----End

4.6.7.5 Configuring the Protocol Password

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

Procedure

- Step 1** Log in to the camera web system ([https://Camera IP address](#)).
- Step 2** Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.
- Step 3** Click **Protocol Password**.
- Step 4** Set the protocol password, as shown in [Figure 4-38](#). Here, the SDK/RESTful password is used as an example.

Figure 4-38 Setting the protocol password

Protocol Password

SDK/RESTful Password ONVIF Password

User name: admin/ApiAdmin

Web user password:

New password:

Confirm password:

Save

Step 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**.

Step 6 Click **Save**.

----End

4.6.7.6 Setting Media Stream Keep-Alive Parameters

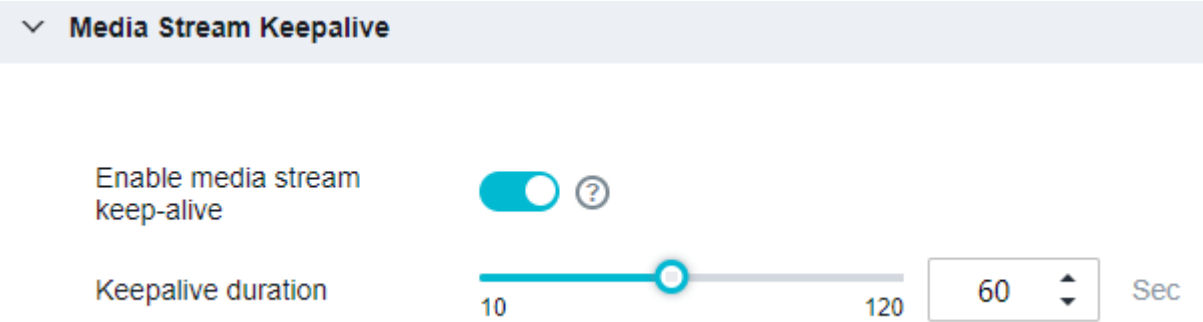
You can set media stream keep-alive parameters to ensure that media streams can be properly requested when the platform is connected through protocols such as SDK or ONVIF.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Click **Configuration Wizard** in the upper right corner of the web page. Click **Next** until the **Platform Connection** page is displayed.

Step 3 Click **Media Stream Keepalive**. The **Media Stream Keepalive** area is displayed, as shown in [Figure 4-39](#).

Figure 4-39 Media Stream Keepalive area



Step 4 Set media stream keep-alive parameters. [Table 4-30](#) describes the parameters.

Table 4-30 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, ONVIF, or RESTful protocol, the media stream request mode is used. If the platform supports the keep-alive function, you are advised to toggle on Enable media stream keep-alive .
Keepalive duration	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.

----End

4.7 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.

4.7.1 Setting Playing Parameters

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

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Local > Playing Settings**. The **Playing Settings** area is displayed, as shown in [Figure 4-40](#). The parameters displayed in this area vary between camera models.

Figure 4-40 Playing Settings area

Playing Settings

Rendering mode  ☒ DDraw ☐ D3D

Code stream type ☒ Primary Stream ☐ Secondary Stream 1

Video stream type  ☒ Video stream ☐ Hybrid stream

Protocol ☒ TCP ☐ UDP

Live view performance  8

Other Functions ☐ Media stream encryption 

Step 3 Set playing parameters. [Table 4-31](#) describes the parameters.

Table 4-31 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 when a browser of a later version is used.
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.
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. NOTE Predefined detection areas for behavior analysis can be displayed on live video images only when Video stream type is set to Hybrid stream.

Parameter	Description
Protocol	Type of the network transmission protocol. NOTE Local video streams support TCP (default) and UDP.
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, video stuttering 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 video stuttering occurs, you can increase the value to ensure smooth video images.
Media stream encryption	If you select Media stream encryption , the media streams, recordings, and snapshots are encrypted. Disabling media stream encryption will cause security risks. Exercise caution when disabling this function.

Step 4 Click **Save**.

----End

4.7.2 Setting Recording File Parameters

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

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Local > Recordings**. The **Recordings** area is displayed, as shown in [Figure 4-41](#).

Figure 4-41 Recordings area

Recordings

Recording duration

60

Min ▾

Recording path

...

?

Step 3 Set recording file parameters. [Table 4-32](#) describes the parameters.

Table 4-32 Recording file parameters

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

Step 4 Click **Save**.

----End

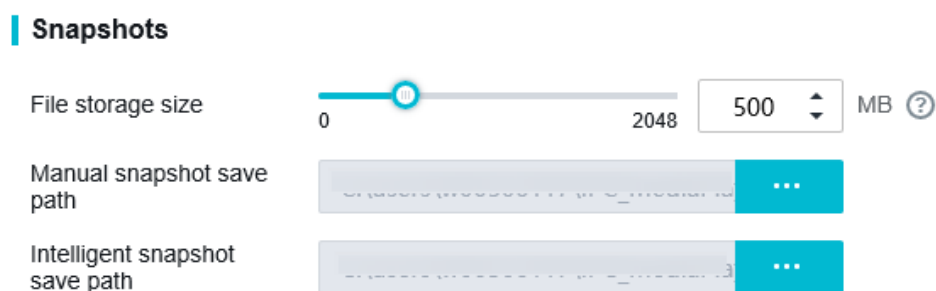
4.7.3 Setting Snapshot File Parameters

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

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **Local** > **Snapshots**. The **Snapshots** area is displayed, as shown in [Figure 4-42](#).

Figure 4-42 Snapshots area


Step 3 Set snapshot file parameters. [Table 4-33](#) describes the parameters.

Table 4-33 Snapshot file parameters

Parameter	Description
File storage size	Size of local images captured in real time. 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
Manual snapshot save path	Path for saving snapshots captured during video viewing on the View page. To set a save path, click  and select a path.
Intelligent snapshot save path	Path for saving images captured in real time. To set a save path, click  and select a path.

Step 4 Click **Save**.

----End

4.8 Managing the System

This section describes how to configure system operations.

4.8.1 System Settings

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

4.8.1.1 Basic Information

You can view basic information about a camera, such as its service life information.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **System** > **System Settings**.

Step 3 Click the **Basic Information** tab and view basic system information. [Table 4-34](#), [Table 4-35](#), [Table 4-36](#), and [Table 4-37](#) describe parameters on this tab page.

Table 4-34 Basic system information

Parameter	Description
Device model	Camera model.
Hardware SN	Camera serial number, which is unique.
CPU usage	Current CPU usage.
Available memory (KB)	Available memory size.
Kernel version	Kernel version of the camera operating system.

Parameter	Description
Reception rate (bit/s)	Current network data reception rate.
Software version	Software version of the camera web system.
ESN	Unique ID of the camera software and hardware system.
Total memory (KB)	Total memory size.
Physical address (ETH0)	MAC address of the camera.
Cache (KB)	Cache memory size.
Transmission rate (bit/s)	Current network data transmission rate.

Table 4-35 Platform status

Parameter	Description
SDK Active-1	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.
SDK Active-2	
SDK Active-3	

Table 4-36 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 • If the camera is registered with the platform using the ONVIF protocol or SDK, media streams are transmitted as elementary 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.

Parameter	Description
Stream Type	Type of the current media stream transmitted by the camera. On the View page, you can click  to switch the stream type.
Service Type	Service type of the current media stream. The service types include live video viewing, recording download, and recording playback.
Encryption Type	Indicates whether the current media stream is encrypted. You can enable or disable Media stream encryption under Configuration > Local > Playing Settings .
Watermark	Indicates whether the watermark function is enabled. You can enable or disable the watermark function under Configuration > Video/Audio > Video .
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.

Table 4-37 Lifecycle

Parameter		Description
Service Info	Start time	Start time for using the camera.
	Service life (months)	Service life of the camera.
Device Info	First power-on time	Time when the camera is put into use.
	Device tag	Camera tag.
	Device name	Name of the camera.
	IP	IP address of the camera.
	Service status	Current service status of the camera.
	Software version	Version number of the camera software.
	Hardware SN	Hardware serial number of the camera.

----End

4.8.1.2 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.

Configuring the System Time

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > System > System Settings > Time** and configure the system time, as shown in [Figure 4-43](#).
- The web page varies depending on the camera model.

Figure 4-43 Time tab page

Time

Time zone

(UTC+08:00) Beijing, Hong Kong (China... ▾

Calibration mode

☒ Manual

☐ NTP

Device time

11:07:38

Time

11:06:13

📅

☐ Synchronize

If the time is set to earlier than 2022-07-01 00:00:00, 2022-07-01 00:00:00

Save

- a. Select a time zone from the **Time zone** drop-down list box.
- b. Select a time calibration mode and set related parameters. [Table 4-38](#) describes the parameters.

 NOTE

- After NTP time calibration is set, protocol-based time calibration becomes invalid.
- You are advised to use NTP or protocol-based time calibration to prevent inconsistency between the device time and the actual time due to device power-off or frequent restart.
- 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 4-38 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. 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, select 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  to check whether the NTP server IP address is available.

Step 3 Click **Save**.

----End

Configuring Daylight Saving Time

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > System Settings > Time** and configure the daylight saving time (DST), as shown in [Figure 4-44](#).

Figure 4-44 Configuring the DST

DST

☐ Enable

DST mode

☒ Week ☐ Date

Start time

Apr First Monday 02:00

End time

Oct Last Monday 02:00

Time offset

30 min

Save

- Step 3** Configure the DST.
1. Select **Enable**.
 2. Click **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.
 3. Set **Start time**, **End time**, and **Time offset** of the DST based on regulations specified in the local laws.
- Table 4-39** describes the DST parameters.

Table 4-39 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.

Step 4 Click **Save**.

----End

4.8.1.3 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > System Settings > Field of View**.

Step 3 Click the corresponding tabs and set the camera installation height, longitude, and latitude. [Table 4-40](#) describes the FoV information.

Table 4-40 FoV information

Parameter	Description
Installation Height	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 viewing direction and the truth north direction of the Earth's magnetic field.
Lens Info	You can query the camera lens information in this area, including the optical zoom ratio, digital zoom ratio, horizontal field of view, and vertical field of view.

----End

4.8.2 System Maintenance

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

4.8.2.1 Upgrade and Installation

4.8.2.1.1 Upgrading the Camera Version

You can upgrade the camera version.

NOTICE

- The upgrade duration is less than 5 minutes (excluding the restart time) if a maximum of one channel of video streams is enabled.
- 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.

Prerequisites

You have obtained the software package.



NOTE

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

Upgrading the Camera Version

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > System Maintenance > Upgrade**.

The **Upgrade** tab page is displayed, as shown in [Figure 4-45](#).

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

Figure 4-45 Upgrade tab page

Upgrade file

Upload file

Select an officially released .bin package.



Step 3 Click , select the required .bin upgrade package, and click **Upgrade**.

Step 4 When the upgrade is complete, the system displays a message indicating that the upgrade is successful.

----End

4.8.2.2 Maintenance

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

Restarting a Camera

Some exceptions may occur if a camera runs for a long period of time. You can rectify the exceptions by remotely or automatically restarting the camera. 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.

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > System Maintenance > Maintenance > Restart Device**. The **Restart Device** area is displayed, as shown in [Figure 4-46](#).

Figure 4-46 Restart Device area

Remote Restart

☐ Automatic Restart

Cyclic mode

☐ Weekly

☒ None

Cycle

☐ Select all

☐ Monday

☐ Tuesday

☐ Wednesday

☐

Restart start time

00:00:00

Save

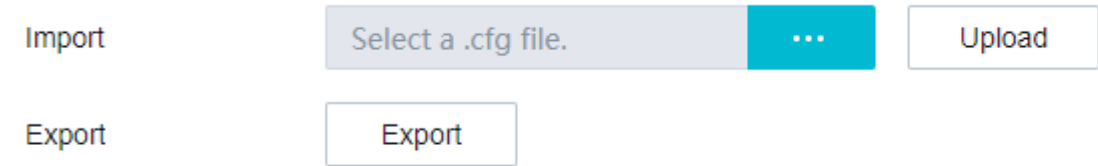
- Step 3** (Optional) Remotely restart the camera.
- Click **Remote Restart**. The **Restart** dialog box is displayed.
 - Click **OK**. The camera restarts.
- Step 4** (Optional) Configure automatic restart.
- Select **Automatic Restart** and set **Cyclic mode**, **Cycle**, and **Restart start time** in sequence.
 - Click **Save**.
- End

Managing Configuration Files

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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > System Maintenance > Maintenance > Manage Configuration File**. The **Manage Configuration File** area is displayed, as shown in [Figure 4-47](#).

Figure 4-47 Manage Configuration File area



Step 3 Set related parameters. [Table 4-41](#) describes the parameters.

Table 4-41 Configuration file parameters

Parameter	Description	Setting
Export	You can download the current configuration file to save device parameter settings. If necessary, you can upload the configuration file again to restore the device parameters.	1. Click Export. 2. Enter the file password in the dialog box that is displayed. 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.

Parameter	Description	Setting
Import NOTICE The version of the configuration file to upload must be the same as the current device version. Otherwise, the configuration may be lost.	You can upload the configuration file 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.	1. Click  and select the 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. – 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.

----End

Restoring a Camera to Default Settings

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > System Maintenance > Maintenance > Restore**. The **Restore** area is displayed, as shown in [Figure 4-48](#).

Figure 4-48 Restore area

Restore

After the snapshot is restored, the snapshot space is restored to the default value. The snapshot



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

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

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

----End

4.8.2.3 Logs

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

4.8.2.3.1 Querying Logs

Logs are the main information source for maintenance engineers to locate faults. They also 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 log information.

NOTE

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

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **System** > **System Maintenance** > **Log**. The **Log** tab page is displayed, as shown in [Figure 4-49](#).

Figure 4-49 Querying logs

One-Click Info Collection

One-Click Collection



Querying Logs

Select Log

Period

Operation

Step 3 Query logs.

1. Access the **Querying Logs** area. Set **Select Log** and **Period**.

NOTE

- If you click **Last 1 day**, the start time changes to 24 hours ago and the end time changes to the current time.

2. 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.

Step 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 **console*.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 en-us_topic_0000001674448346.xml.

----End

4.8.3 Security Management

This section describes how to manage camera passwords and certificates and configure IP address filtering.

4.8.3.1 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.

Protocol Password

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > Security Management > Password Management > Protocol Password**. In the area that is displayed, you can change the SDK/RESTful and ONVIF passwords separately.

The following describes how to change the SDK/RESTful password. [Figure 4-50](#) shows the page for setting the SDK/RESTful password.

 NOTE

HWSDK and RESTful use the same account.

Figure 4-50 SDK/RESTful Password tab page

SDK/RESTful Password

ONVIF Password

User name

admin/ApiAdmin

Web user password

New password

Confirm password

Save

- Step 3** 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.

- Step 4** Click **Save**.

-----End

Web Login Password

You can change the web login password of the current user.

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > Security Management > Password Management**.

Step 3 Click **WEB Login Password**. The area shown in **Figure 4-51** is displayed.

Figure 4-51 WEB Login Password area

▼ WEB Login Password

User name

admin

Current user password

New password

Confirm password

☐ Synchronously change passwords of other accounts ?

Save

Step 4 Set **Current user password**, **New password**, and **Confirm password**.

 NOTE

- Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords.
You are advised not to set the new password to a weak password. The default weak passwords include **Cspdbbr@2017**, **kafka-1qaz@WSX**, **CSP@gaussdb@2017**, **UGW9811adminhwbs@com**, **hwbs@com**, **sps600@HW**, **Changeme_123**, **hwosta2.0**, **cnp200@HW**, **omu800@HW**, **mt2013@HW**, **GrUB1@ATCA**, **x86bpw**, **admin@86**, **data1@HW**, **Admin_12#**, **pgw#2013**, **Pmssys@2013**, **Admin@123**, **Update@7*24**, **9061csl**, **cgp data2@HW**, **sys data1@HW**, **bmu_hss**, **sek12345**, **HWps123**, **cnp123@HW**, **Spark@123**, **Hbase@123**, and **Hdfs@123**.
- If you select **Synchronously change passwords of other accounts**, the passwords of the SDK, web, ONVIF/RTSP, and RESTful accounts are changed synchronously.

Step 5 Click **Save**.

----End

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.

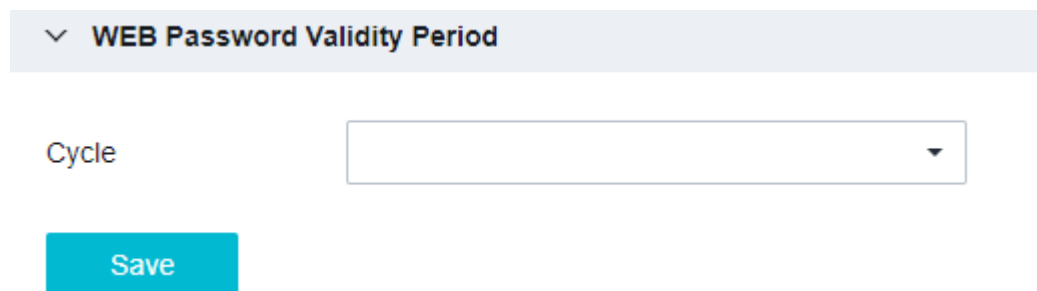
Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > Security Management > Password Management**.

Step 3 Click **WEB Password Validity Period**. The area shown in [Web Password Validity Period](#) is displayed.

Figure 4-52 WEB Password Validity Period area



▼ **WEB Password Validity Period**

Cycle

Save

----End

4.8.3.2 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 to 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 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > Security Management > Password Recovery**. The **Password Recovery** tab page is displayed.

Step 3 Under **Password recovery through security questions**, select **Enable**, as shown in [Figure 4-53](#).

Figure 4-53 Password recovery through security questions

| Password recovery through security questions

☒ Enable

Question 1

What is your favorite sport?

☐ Custom question

Answer

Provide the answer to your question.

Question 2

What is your favorite quote?

☐ Custom question

Answer

Provide the answer to your question.

Question 3

Who is your idol?

☐ Custom question

Answer

Provide the answer to your question.

Save

Step 4 Select a preset question from the **Question X** drop-down list box or select **Custom question** and customize a question.

Step 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.

Step 6 Click **Save**. The **Identity Authentication** dialog box is displayed.

Step 7 Enter the login password and click **OK**.

----End

4.8.3.3 Certificate Management

This section describes how to manage HTTPS certificates, SDK certificates, and SDK CRLs of cameras.

4.8.3.3.1 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > Security Management > Certificate Management > HTTPS Certificate Management**.

Figure 4-54 HTTPS Certificate Management area

HTTPS Certificate Management

CA certificate file ?

...

Certificate file (.pem)

...

Key file (.pem)

...

Upload

Restore Certificate

- Step 3** Set parameters in the **HTTPS Certificate Management** area. [Table 4-42](#) describes the parameters.

Table 4-42 HTTPS certificate management parameters

Parameter	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.
Restore Certificate	Button for restoring the certificate to the default one.

You can use your own certificate file in the following way: Click , 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 and .cer formats 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.

----End

4.8.3.3.2 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > Security Management > Certificate Management > SDK Certificate Management**.
- The **SDK Certificate Management** area is displayed, as shown in [Figure 4-55](#).

Figure 4-55 SDK Certificate Management area

SDK Certificate Management

CA certificate file 

...

Certificate file (.pem)

...

Key file (.pem)

...

Upload

Restore Certificate

- Step 3** Set parameters in the **SDK Certificate Management** area. [Table 4-43](#) describes the parameters and buttons in this area.

Table 4-43 SDK certificate management parameters/buttons

Parameter/ Button	Description
CA certificate file (.pem)	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 , 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 and .cer formats 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.
- 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.

----End

4.8.3.3 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.

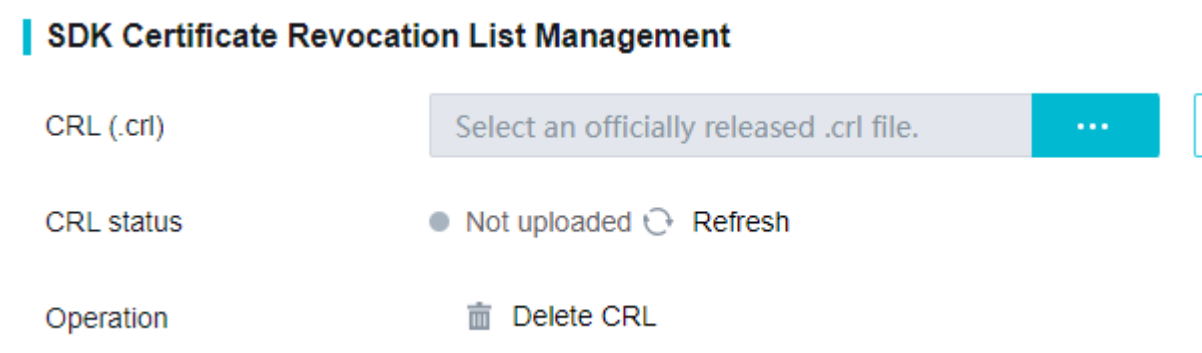
Background

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

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 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 4-56](#).

Figure 4-56 SDK Certificate Revocation List Management area



- Step 3** Click , 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.
- Step 4** (Optional) Click **Refresh** if the status is not displayed.
- Step 5** (Optional) Click **Delete CRL** to delete an uploaded CRL.
- End

4.8.3.4 IP Address Filtering

You can use the IP address filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

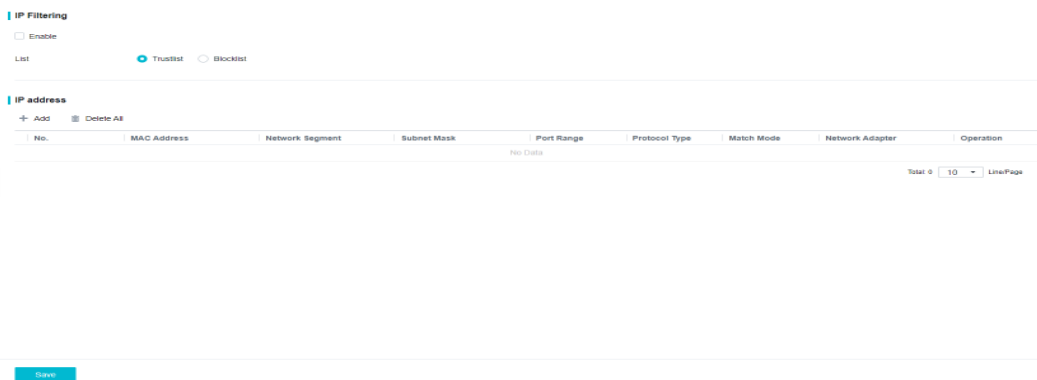
Background

- A network segment is obtained by performing logical AND of the IP address and subnet mask.
- A maximum of 100 IP address filtering rules can be added.

Procedure

- Step 1** Choose **Configuration > System > Security Management > IP Filtering**.
The **IP Filtering** tab page is displayed, as shown in [Figure 4-57](#).

Figure 4-57 IP Filtering tab page



Step 2 Select **Enable** to enable the IP address filtering function.

Step 3 Set **List**.

The **List** parameter has two options: **Trustlist** and **Blocklist**, that is, denying or allowing the access only from a specified MAC address, network segment or port, or using a specified protocol. Currently, the camera supports only one option at a time.

Step 4 Click **Add**. In the **Add IP Address Filtering Rule** dialog box that is displayed, set **MAC Address**, **IPv4 network segment**, **IPv4 subnet mask**, **Protocol Type**, and **Match Mode**, as shown in [Figure 4-58](#).

Figure 4-58 Add IP Address Filtering Rule dialog box

Add IP Address Filtering Rule

MAC Address

00 : 00 : 00 : 00 : 00 : 00

IPv4 network segment

192 : 168 : 1 : 0

IPv4 subnet mask

255 : 255 : 255 : 0

Port Range

065535

Protocol Type

UDP

Match Mode

Match IP address

OK

Cancel

NOTE

- If a filtering rule shown in [Figure 4-58](#) is configured under **Blocklist**, the camera does not process UDP packets sent from the network segment **192.168.1.0** to ports **0–65535**.

Step 5 Click **OK**.

The **IP Filtering** tab page is displayed.

Step 6 Click **Save**.

NOTE

To modify or delete an IP address filtering rule, click  or  in the **Operation** column of the IP address filtering rule.

----End

4.8.3.5 Security Options

Procedure

On the **Security Options** tab page, you can set the web session timeout duration.

- Step 1** Choose **Configuration > System > Security Management > Security Options**.
The **Security Options** tab page is displayed, as shown in [Figure 4-59](#). [Table 4-44](#) describes the parameters. You can set **Session timeout duration** depending on your needs.

Figure 4-59 Security Options tab page

Security Options

Session timeout duration

?

180

43200

600

↑

↓

Sec

Save

Table 4-44 Parameters for security options

Parameter	Description
Session timeout duration	When the login duration exceeds the value of this parameter, the camera returns to the login page.

- Step 2** Click **Save**.
----End

4.8.4 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.

4.8.4.1 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.

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > User Management > User List**.
- The **User List** area is displayed, as shown in [Figure 4-60](#).

Figure 4-60 User List area

User List							
Add Advanced Multi-point login							
Seq.	User Name	User Type	Account Status	Password	Multi-point Login	Operation	
1	admin	Administrator	Normal	*****	20	✓	BS
2	user01	Advanced operator	Normal	*****	20	✓	BS
3	user02	Advanced operator	Normal	*****	20	✓	BS
4	user03	Advanced operator	Normal	*****	20	✓	BS
5	user04	Advanced operator	Normal	*****	20	✓	BS
6	user05	Advanced operator	Normal	*****	20	✓	BS
7	user06	Advanced operator	Normal	*****	20	✓	BS
8	user07	Advanced operator	Normal	*****	20	✓	BS

- Step 3** Click **Add**.
- In the **Add** dialog box that is displayed, configure information about the new user, as shown in [Figure 4-61](#).

Figure 4-61 Add dialog box

Add

The web password is independent from protocol passwords such as the ONVIF and SDK

User type

Advanced operator

User name

Enter the user name.

Current user password

Enter the current user password.

New password

Enter a new password.

OK

Cancel

NOTICE

- A maximum of 10 users (including the **admin** user) can be added.
- The **admin** users are administrators and cannot be added again.

Step 4 Set user parameters. [Table 4-45](#) describes the parameters.

2024-01-25

148

Table 4-45 Parameters for adding a user

Parameter	Setting
User type	Select a user type from the drop-down list box. Different types of users have different operation rights. You can select the user type as required. - Administrators have all operation rights. They can add advanced operators and common operators. - 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. NOTE Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords. You are advised not to set the new password to a weak password. The default weak passwords include Cspdbr@2017, kafka-1qaz@WSX, CSP@gaussdb@2017, UGW9811adminhwbs@com, hwbs@com, sps600@HW, Changeme_123, hwosta2.0, cnp200@HW, omu800@HW, mt2013@HW, GrUB1@ATCA, x86bpw, admin@86, data1@HW, Admin_12#, pgw#2013, Pmssys@2013, Admin@123, Update@7*24, 9061csl, cgp data2@HW, sys data1@HW, bmu_hss, sek12345, HWps123, cnp123@HW, Spark@123, Hbase@123, and Hdfs@123.
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.

Step 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.

----End

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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 4-62](#).

Figure 4-62 User List area

User List							
☒ All ☐ Advanced ☐ Multi-point login							
Seq.	User Name	User Type	Account Status	Password	Multi-point Login	Operation	
1	admin	Administrator	Normal	*****	20		
2	user01	Advanced operator	Normal	*****	20		
3	user02	Advanced operator	Normal	*****	20		
4	user02	Advanced operator	Normal	*****	20		
5	user02	Advanced operator	Normal	*****	20		
6	user02	Advanced operator	Normal	*****	20		
7	user02	Advanced operator	Normal	*****	20		
8	user02	Advanced operator	Normal	*****	20		

Step 3 Select a user.

Step 4 Click .

The **Edit** dialog box is displayed, as shown in [Figure 4-63](#).

Figure 4-63 Edit dialog box

Edit

 The web password is independent from protocol passwords such as the ONVIF and SDK

User type

Administrator

User name

admin

Current user password

Enter the current user password.

New password

Enter a new password.

OK

Cancel

Step 5 Specify the current user password, new password, and confirm password.

Step 6 Click **OK**.

 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.

----End

Changing the Maximum Number of Concurrent Logins

You can change the maximum number of concurrent logins for a user.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 4-64](#).

Figure 4-64 User List area

User List								
Add		Advanced	Multi-point login					
No.	User Name	User Type	Account Status	Password	Multi-point Login			Operation
1	admin	Administrator	Normal	*****	20			✓
2	user01	Advanced operator	Normal	*****	20			✗
3	user02	Advanced operator	Normal	*****	20			✗
4	user03	Advanced operator	Normal	*****	20			✗
5	user04	Advanced operator	Normal	*****	20			✗
6	user05	Advanced operator	Normal	*****	20			✗
7	user06	Advanced operator	Normal	*****	20			✗
8	user07	Advanced operator	Normal	*****	20			✗

Step 3 Select a user.

Step 4 Click **Multi-point login**.

The **Modify Multi-point Login** dialog box is displayed.

Step 5 Set **Current user password** and **Multi-point login**.

Step 6 Click **OK**.

----End

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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 4-65](#).

Figure 4-65 User List area

User List								
Add		Advanced	Multi-point login					
No.	User Name	User Type	Account Status	Password	Multi-point Login			Operation
1	admin	Administrator	Normal	*****	20			✓
2	user01	Advanced operator	Normal	*****	20			✗
3	user02	Advanced operator	Normal	*****	20			✗
4	user03	Advanced operator	Normal	*****	20			✗
5	user04	Advanced operator	Normal	*****	20			✗
6	user05	Advanced operator	Normal	*****	20			✗
7	user06	Advanced operator	Normal	*****	20			✗
8	user07	Advanced operator	Normal	*****	20			✗

Step 3 Select a user.

Step 4 Click  .

The **Delete** dialog box is displayed.

Step 5 Enter the current user password and click **OK**.

The **Delete** dialog box is displayed.

Step 6 Click **OK**.

-----End

Configuring Account Locking

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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 4-66](#).

Figure 4-66 User List area

User List							
+ Add ☒ Advanced ☐ Multi-point login							
NO.	User Name	User Type	Account Status	Password	Multi-point Login	Operation	
1	Admin	Administrator	Normal	*****	20		
2	user01	Advanced operator	Normal	*****	20		
3	user02	Advanced operator	Normal	*****	20		
4	user02	Advanced operator	Normal	*****	20		
5	user02	Advanced operator	Normal	*****	20		
6	user02	Advanced operator	Normal	*****	20		
7	user02	Advanced operator	Normal	*****	20		
8	user02	Advanced operator	Normal	*****	20		

Step 3 Click **Advanced**.

The **Advanced** dialog box is displayed, as shown in [Figure 4-67](#).

Figure 4-67 Advanced dialog box

Advanced

Specify the maximum number of consecutive password input failures and the duration for lock account. The configuration applies to all users.

Max. password input failures

5

Lock duration (min)

5

OK

Cancel

Step 4 Set **Max. password input failures** and **Lock duration (min)**.

 NOTE

- **Max. password input failures:** maximum number of consecutive incorrect password attempts allowed
- **Lock duration (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 duration (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**.

Step 5 Click **OK**.

----End

Unlocking an Account

If an account is locked because the number of incorrect password attempts reaches the maximum, the administrator can unlock the account.

 NOTE

Only the administrator has the permission to unlock accounts.

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > User Management > User List**.
The **User List** area is displayed, as shown in [Figure 4-68](#).

Figure 4-68 User List area

User List

+ Add

 Advanced

 Multi-point login

No.	User Name	User Type
1	admin	Administrator
2	admin1	Common operator

- Step 3** In the **Operation** column of a locked account, click  .
The **Unlock** dialog box is displayed, as shown in [Figure 4-69](#).

Figure 4-69 Unlock dialog box

Unlock

Current user password

Enter the current user password.

OK

Cancel

- Step 4 Enter the administrator password and click **OK**.
- End

4.8.4.2 User Connection

You can check the connection status of a user or disconnect a user.

Procedure

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > System > User Management**.
- Step 3 Access the **Connection status** area, as shown in [Figure 4-70](#).

Figure 4-70 Connection status area

Connection status				
No.	User Name	IP Address	Login Time	Operation
1	admin	90.253.64.182	2023-10-20 09:08:06	Disconnect

NOTICE

- To disconnect a user, click **Disconnect** in the **Operation** column corresponding to the user.
- The administrator cannot be forcibly disconnected.

----End

4.8.4.3 Password Validity Period

You can view or configure the validity period of a user password.

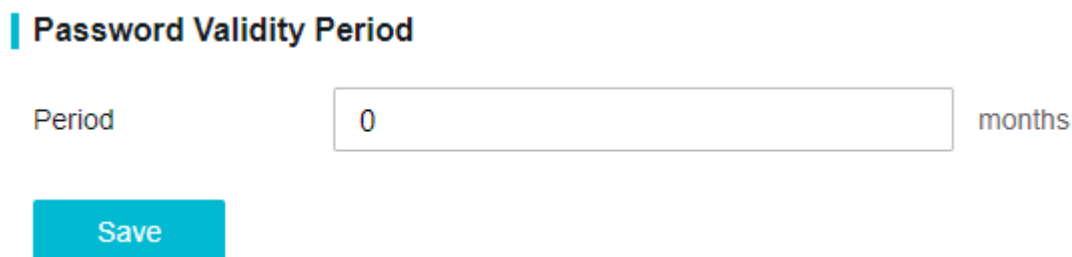
NOTE

After the password expires, the system will demand you to change the password.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > User Management**.
- Step 3** Under **Password Validity Period**, check or set **Period**, as shown in [Figure 4-71](#).

Figure 4-71 Password Validity Period area



Password Validity Period

Period months

Save

NOTE

The value of **Period** is an integer ranging from 0 to 12. If this parameter is set to **0**, the password is permanently valid.

----End

4.9 Network Configuration

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

NOTE

The parameters that can be set vary depending on the camera model.

4.9.1 Setting Network Parameters

You can set basic network parameters, 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 (5 minutes by default) sending Address Resolution Protocol (ARP) requests by default.

4.9.1.1 Configuring TCP/IP

This section describes how to set TCP/IP parameters.

4.9.1.1.1 Setting Camera IP Addresses

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

 NOTE

- For cameras that support dual network ports, you need to set IP addresses for the two network ports separately.
- The two network ports are named ETH0 and ETH1. You can select either ETH0 or ETH1 as the default network adapter and set IP addresses for the two ports separately.
- 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Network > Network Parameters > TCP/IP**.
- Step 3** Click **IP address**. The **IP address** area is displayed, as shown in [Figure 4-72](#).

Figure 4-72 IP address area

IPv4 address assignment

☒ Manual ☐ Auto

IPv4 address

Q

Check Conflict

IPv4 subnet mask

IPv4 gateway

MAC address

Primary DNS

Secondary DNS

Save

- Step 4** Set camera IP addresses as planned. [Table 4-46](#) describes the parameters.

Table 4-46 IP address parameters

Parameter	Description
IPv4 address assignment	Method for obtaining the IPv4 address. The options are Manual and Auto . NOTE When a Dynamic Host Configuration Protocol (DHCP) server exists in the network, an IP address is automatically allocated to the camera. You can click Auto to check the IP address. The camera IP address allocated by the server is fixed.

Parameter	Description
IPv4 address	Camera IPv4 address. This parameter can be set only when IPv4 address assignment is set to Manual. 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 subnet mask	Subnet mask of the network where the camera is located.
IPv4 gateway	Gateway IP address of the network where the camera is located.
MAC address	Camera MAC address. This parameter is read-only.
Primary DNS	IP address of the primary DNS server. 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	IP address of the secondary DNS server. 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)

Step 5 Click **Save**.

----End

Setting the IPv6 Address

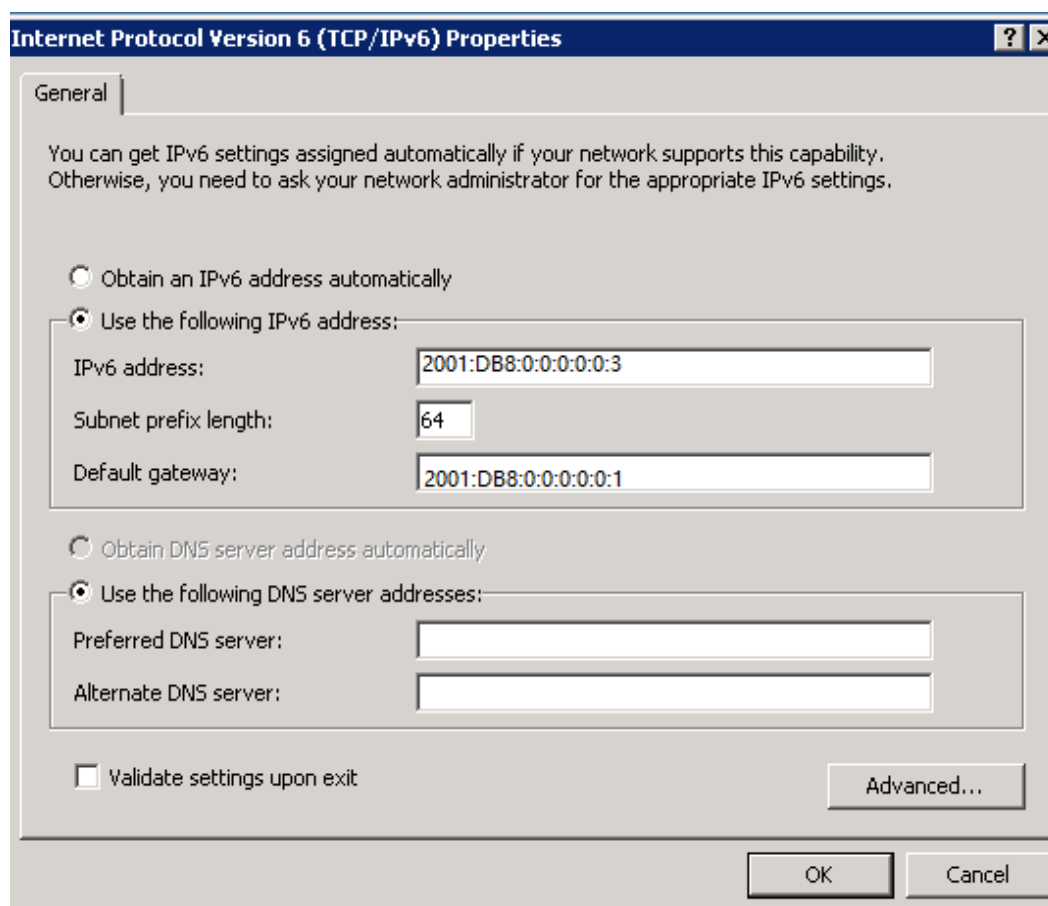
The IPv6 address is numbered in hexadecimal notation and is divided into eight blocks by colons (:). Each block contains 16 bits, for example, fe80:0da8:65b4:05d3:1315:7c1f:0461:7847.

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.

Step 1 Set the IPv6 address of the local computer.

1. Run the **regedit** command on the local computer, choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > services > TCPIP6 > Parameters**, delete **DisabledComponents**, and restart the local computer.
2. On the computer, choose **Control Panel > Network and Internet > Network and Sharing Center** to access the **Network and Sharing Center** page.
3. 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 4-73](#) 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:DB8:0:0:0:0:3**.

Figure 4-73 Setting the IPv6 address of the local computer



Step 2 Set the IPv6 address of the camera.

1. Log in to the camera web system (<https://Camera IP address>).
2. Choose **Configuration > Network > Network Parameters > TCP/IP > IP address**.
3. Click **IPv6** and select **Enable**, as shown in [Figure 4-74](#).

Figure 4-74 Setting the IPv6 address of the camera

IPv4

IPv6

☐ Enable If IPv6 is enabled, the MTU value range will change. [MTU Settings](#)

IPv6 address assignment

☒ Manual☐ Auto☐ Route advertisement

* IPv6 address

0 : 0 : 0 : 0 : 0 : 0

* IPv6 subnet prefix

0

IPv6 gateway

0 : 0 : 0 : 0 : 0 : 0

MAC address

00:00:00:00:00:00

Save

Table 4-47 IPv6 address parameters

Parameter	Description
IPv6 address assignment	Method for obtaining the IPv6 address. The options are Manual , Auto , 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:DB8:0:0:0:0:1 .
MAC address	Camera MAC address. This parameter is read-only.

4. Enter the camera IP address in the address box of the browser and press **Enter**. The camera login page is displayed.

----End

4.9.1.1.2 Setting Network Connectivity Detection

This section describes how to set network connectivity detection.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Network > Network Parameters > TCP/IP**.
- Step 3** Click **Network Connectivity Detection**. The **Network Connectivity Detection** area is displayed, as shown in [Figure 4-75](#).

Figure 4-75 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**.

----End

4.9.1.1.3 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Network > Network Parameters > TCP/IP**.
- Step 3** In the **QoS Settings** area, set **Media stream DSCP** and **Signaling stream DSCP**, as shown in [Figure 4-76](#). DSCP is the abbreviation of differentiated services code point.

Figure 4-76 QoS Settings area

QoS Settings

Media stream DSCP

0

63

0

Signaling stream DSCP

0

63

0

Save

The settings can take effect only after you click Save and re-enable the live v

- 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.

- Step 4 Click **Save**.
- End

4.9.1.1.4 Setting MTU Parameters

You can set the Maximum Transmission Unit (MTU) parameter to specify the maximum size of a data packet to be transmitted over the network to achieve the optimal transmission efficiency and quality.

Procedure

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > Network > Network Parameters > TCP/IP**.
- Step 3 In the **MTU Settings** area, set **MTU**, as shown in [Figure 4-77](#).

Figure 4-77 MTU Settings area

MTU Settings

MTU ?

800

1500

800

Byte

Save

 NOTE

- This parameter can be set to an integer ranging from 800 to 1500. The default value is **1500**.
- 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.

Step 4 Click **Save**.

----End

4.9.1.1.5 Setting Anti-Attack Parameters

You can set anti-attack parameters to defending the camera against network flood attacks.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Network > Network Parameters > TCP/IP**.
- Step 3** In the **Anti-attack Settings** area, set **Max. packet receiving rate**, as shown in [Figure 4-78](#). [Table 4-48](#) describes the parameters.

Figure 4-78 Anti-attack Settings area

▼ Anti-attack Settings

☒ Enable

Max. packet receiving rate

2000

50000

8000

▲▼

packets/s

☒ Broadcast/Multicast

☐ Unicast

Save

Table 4-48 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.

Parameter	Description
Broadcast/ Multicast	If this parameter is selected, the rate for receiving broadcast or multicast packets is limited.
Unicast	If this parameter is selected, the rate for receiving unicast packets is limited.

Step 4 Click **Save**.

----End

4.9.1.1.6 Setting Multicast Parameters

In multicast transmission mode, a sender sets up point-to-multipoint (P2MP) network connections with all recipients, improving data transmission efficiency and lowering the possibility of backbone network congestion.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Network > Network Parameters > TCP/IP > Multicast Settings**. In the area that is displayed, set multicast parameters. [Table 4-49](#) describes the parameters.

Figure 4-79 Setting multicast parameters

The screenshot displays the 'Multicast Settings' configuration page. It features two main sections: 'Video' and 'Audio'. Each section contains two input fields: 'IP address' and 'Port number'. The 'Video' section has an IP address of '239 - 0 - 0 - 0' and a port number of '1234'. The 'Audio' section has an IP address of '239 - 0 - 0 - 0' and a port number of '1236'. A blue 'Save' button is located at the bottom left of the form.

Table 4-49 Multicast parameters

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.

Step 3 Click **Save**.

----End

4.9.1.2 Configuring HTTP(S)

This section describes how to configure ports in the camera web system.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Network > Network Parameters > HTTP(S)**. The **Port Settings** area is displayed by default, as shown in [Figure 4-80](#).

Figure 4-80 Port Settings area

Port Settings

* HTTP Port

* HTTPS Port

Save

Step 3 Set **HTTP Port** and **HTTPS Port** to an integer ranging from 1 to 65535.

Step 4 Click **Save**.

----End

4.9.1.3 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **Network** > **Network Parameters** > **Email**.

The **Email** tab page is displayed, as shown in [Figure 4-81](#).

Figure 4-81 Setting email parameters

SMTP Server

SMTP Server

SMTP port

Mail encryption

Disabling the TLS

☐ Server authentication

Mail

☐ Add Image attachment

Sender name

Enter the sender's name.

Sender address

Enter the sender's email address.

+ Add

Delete All

No.	Recipient	Re
-----	-----------	----

Save

Step 3 Set email parameters. Table 4-50 describes the parameters.

Table 4-50 Email parameters

Parameter		Description
SMTP Server	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.
	Server authentication	The user name and password must be the same as those of the SMTP server. NOTE Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords. You are advised not to set the new password to a weak password. The default weak passwords include Cspdbr@2017 , kafka-1qaz@WSX , CSP@gaussdb@2017 , UGW9811adminhwbs@com , hwbs@com , sps600@HW , Changeme_123 , hwosta2.0 , cnp200@HW , omu800@HW , mt2013@HW , GrUB1@ATCA , x86bpw , admin@86 , data1@HW , Admin_12# , pgw#2013 , Pmssys@2013 , Admin@123 , Update@7*24 , 9061csl , cgp data2@HW , sys data1@HW , bmu_hss , sek12345 , HWps123 , cnp123@HW , Spark@123 , Hbase@123 , and Hdfs@123 .
Mail	Add Image attachment	When you select the check box, the Total images and Snapshot interval (s) parameters are displayed, 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.
	Sender name	Name of the sender, for example, admin .
	Sender addresses	Email address of the sender, in the format of admin@XXX.com .
	Recipient	You can click Add and enter the recipient's name and email address.
	Recipient Address	You can click Test to check whether the recipient can properly receive emails.

Step 4 Click **Save**.

----End

4.9.2 Setting Platform Connection Parameters

4.9.2.1 Setting Common Protocol Parameters

4.9.2.1.1 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.

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, voice broadcast, and channel-associated voice.
- The default 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Network > Platform Connection > General Protocol > ONVIF**. The **ONVIF** tab page is displayed.

Step 3 Set ONVIF parameters, as shown in [Figure 4-82](#). [Table 4-51](#) describes the ONVIF parameters.

Figure 4-82 Setting ONVIF parameters

If the video encoding format is H.265, the old platform or NVR connected through ONVIF

Enable ONVIF

Validity period

?

Authentication mode

Digest_MD5(priority)/WSSE

WSSE authentication and MD5 encryption algorithms are insecure and are not recommended.

Version

ONVIF 16.12

Transmission protocol

HTTPS

Extended Parameters

Forbid ONVIF to change system time

After this function is enabled, the setting of Real-time clock will be locked.

Reverse time zone

After this function is enabled, the time zone is reversed when the time zone is set.

Enable WSSE anti-replay

The time of the camera and the platform must be synchronized.

Save

Table 4-51 ONVIF parameters

Parameter	Description
Enable ONVIF	Indicates whether to enable the ONVIF protocol.
Validity period	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. This function is disabled by default.

Parameter	Description
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 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 4.9.2.1.2 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. • 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.
Reverse time zone	Indicates whether to reverse the time zone when you set the time through the ONVIF protocol.

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

Step 4 (Optional) Change the ONVIF password.

Method 1:

1. Choose **Protocol Password > ONVIF Password**.
2. Set **Web user password**, **New password**, and **Confirm password**.
3. Click **Save**.

Method 2:

1. Choose **Configuration > System > Security Management > Password Management**.
2. Click **Protocol Password**.
3. On the **ONVIF Password** tab page, set **Web user password**, **New password**, and **Confirm password**.
4. Click **Save**.

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.

----End

Adding Cameras to the Milestone Platform

This section describes how to add cameras to the Milestone platform.

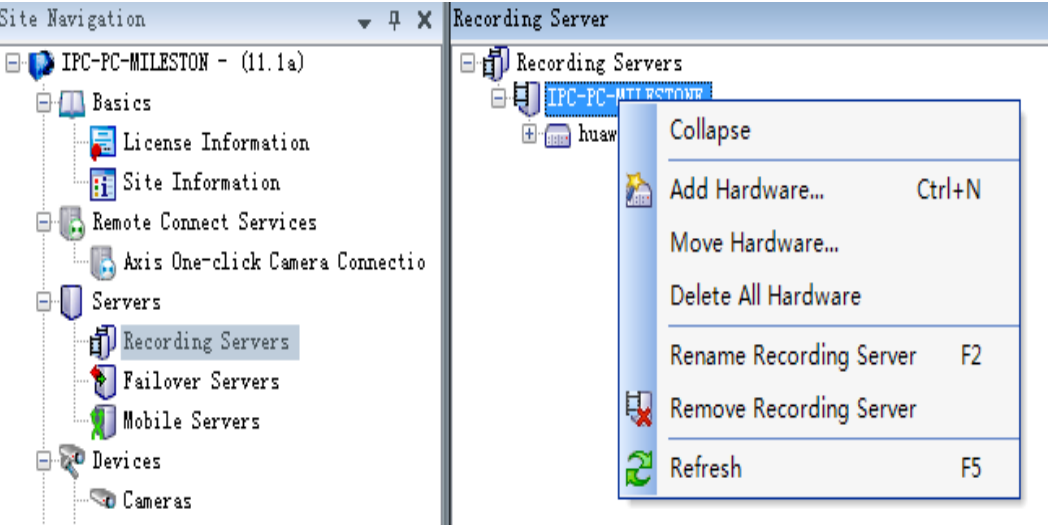
Prerequisites

A Milestone XProtect Management Client has been installed. In this section, Milestone XProtect Management Client 2017 is used as an example.

Procedure

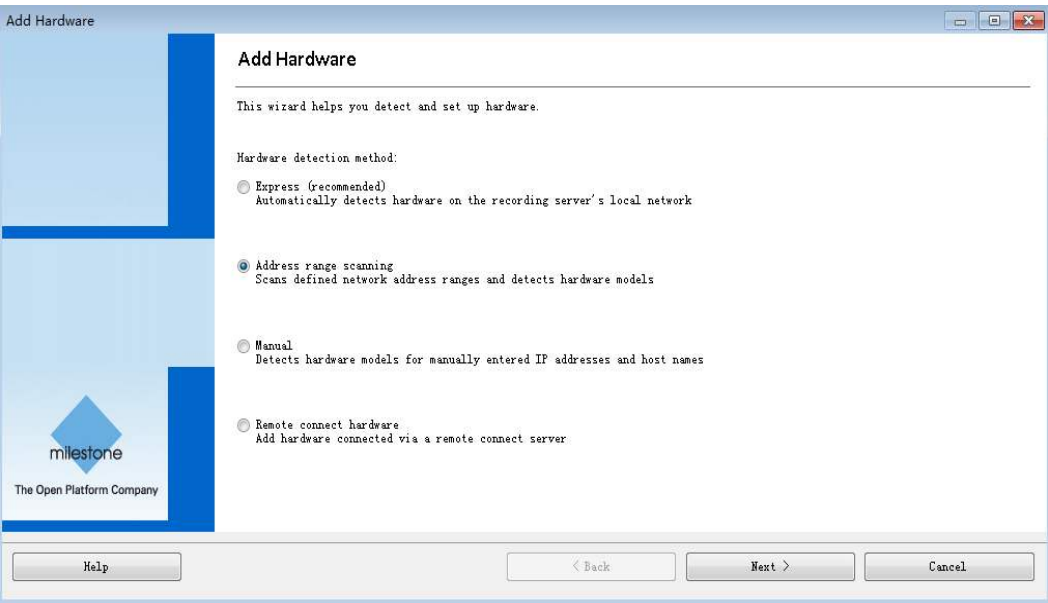
- Step 1** Start the Milestone XProtect Management Client, choose **Servers > Recording Servers**, right-click the server to which cameras are to be added, and choose **Add Hardware** from the shortcut menu, as shown in [Figure 4-83](#).

Figure 4-83 Starting the Milestone XProtect Management Client



Step 2 Click **Next**, as shown in Figure 4-84.

Figure 4-84 Adding hardware



 NOTE

You are advised to add cameras in **Address range scanning** or **Manual** mode.

Step 3 Enter the authentication information, including the user name and password for logging in to the camera and click **Next**, as shown in Figure 4-85.

 NOTE

The default user name for logging in to a certain camera is **admin**, and there is no default password. You need to enter the user-defined password.

Figure 4-85 Entering the authentication information

The screenshot shows a window titled "Add Hardware" with a subtitle "Specify user name and password if devices are not using the default ones." Below the subtitle is a table with three columns: "Include", "User Name", and "Password". The table contains two rows: the first row has an unchecked checkbox, "(Factory Default)", and a password field filled with dots; the second row has a checked checkbox, "admin", and a password field filled with dots. To the right of the table are "Add" and "Remove" buttons. At the bottom of the window are "Help", "< Back", "Next >", and "Cancel" buttons.

Include	User Name	Password
☐	(Factory Default)	
☒	admin	

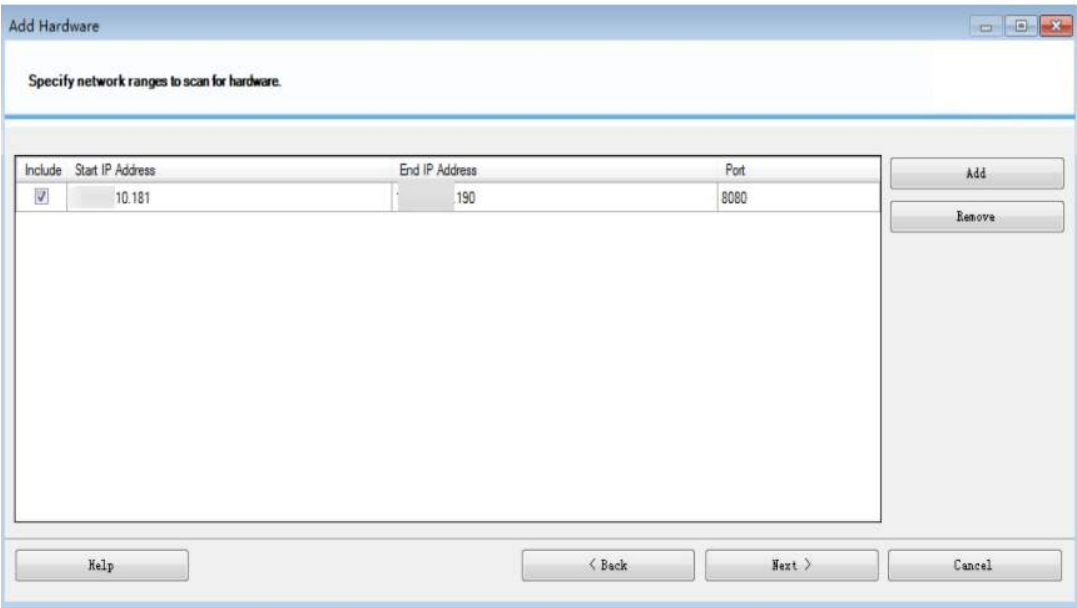
Step 4 Select the driver **ONVIF**. Click **Next**, as shown in [Figure 4-86](#).

Figure 4-86 Selecting a driver

The screenshot shows a window titled "Add Hardware" with a subtitle "Select which drivers to use when scanning for hardware. The more drivers selected, the slower the scanning." Below the subtitle is a list of drivers with checkboxes: HikVision, Hunt, Infinova, IQEye, JVC, LG Electronics, Mango DSP, Milestone, Mobotix, ONVIF (checked), Optelecom, Optex, Panasonic, Pelco, Samsung, Sentry, Sony, UDP, Universal, Vivotek, and Other. To the right of the list are "Select All" and "Clear All" buttons. At the bottom of the window are "Help", "< Back", "Next >", and "Cancel" buttons.

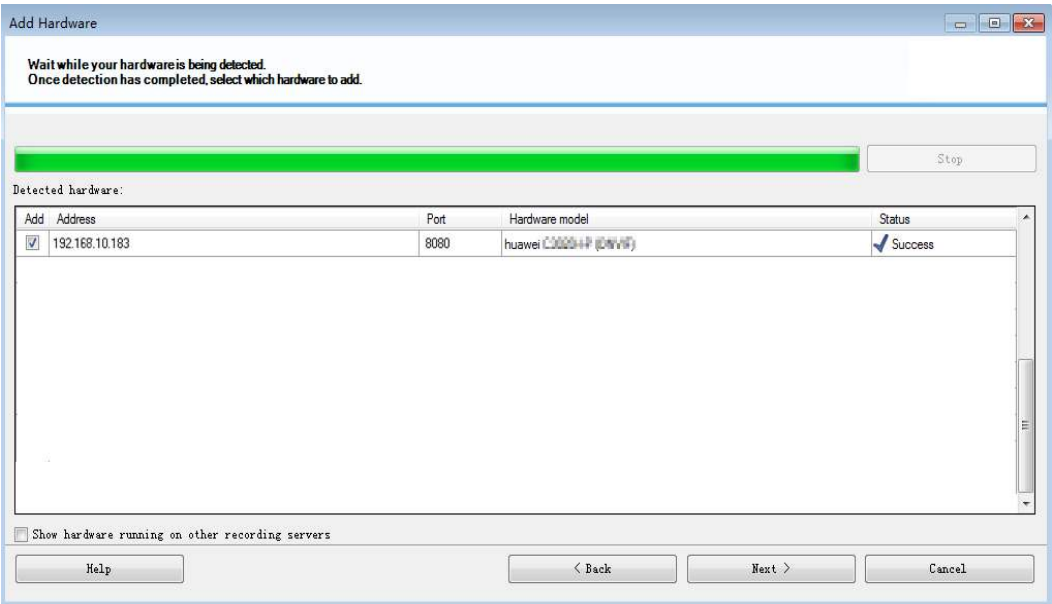
Step 5 Enter the network segment or IP address, select the network segment of the camera to search for, and click **Next**, as shown in [Figure 4-87](#).

Figure 4-87 Entering the IP address



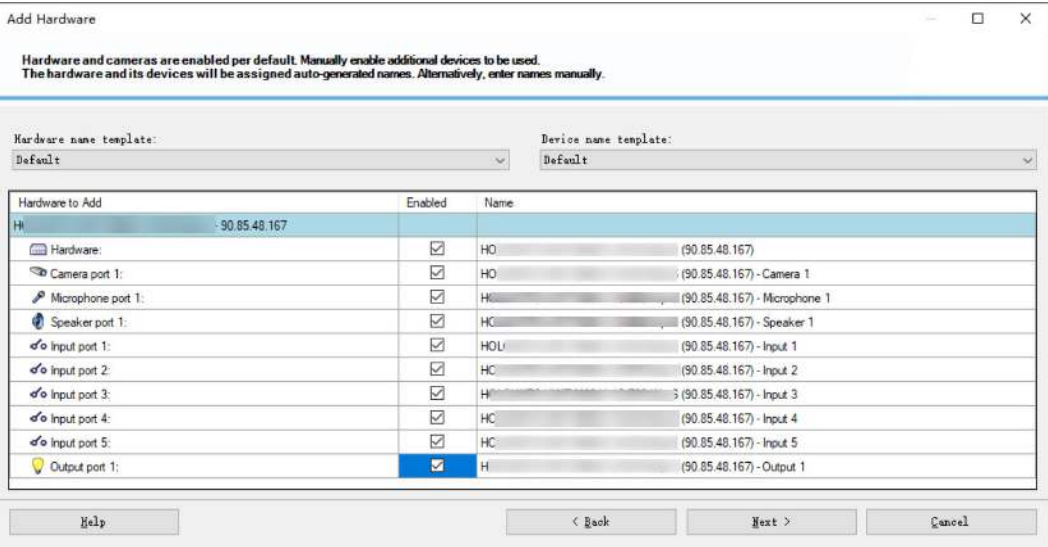
Step 6 After the camera search is complete, click **Next**, as shown in [Figure 4-88](#).

Figure 4-88 Searching for ONVIF devices



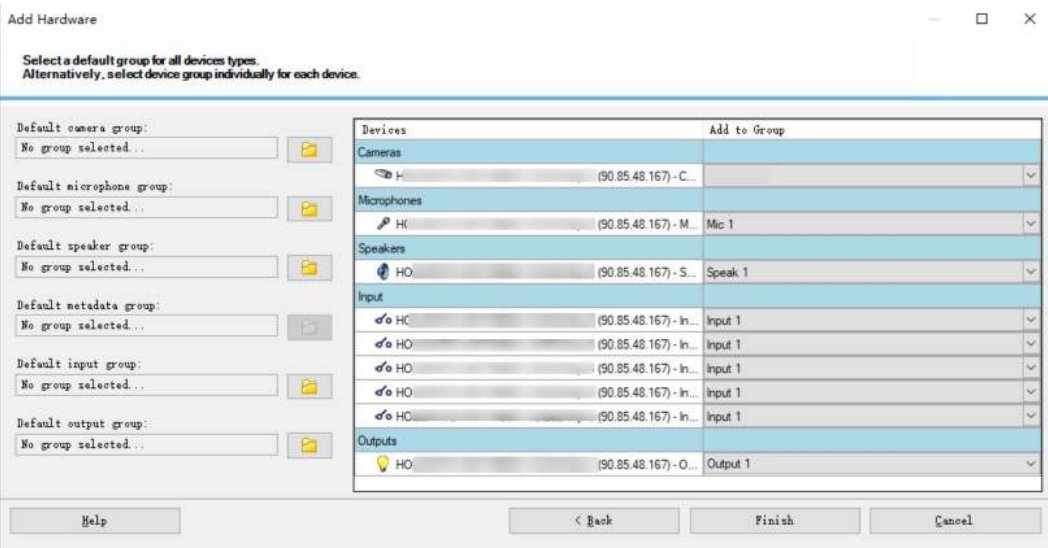
Step 7 Select the hardware to be added and click **Next**, as shown in [Figure 4-89](#).

Figure 4-89 Selecting the hardware to be added



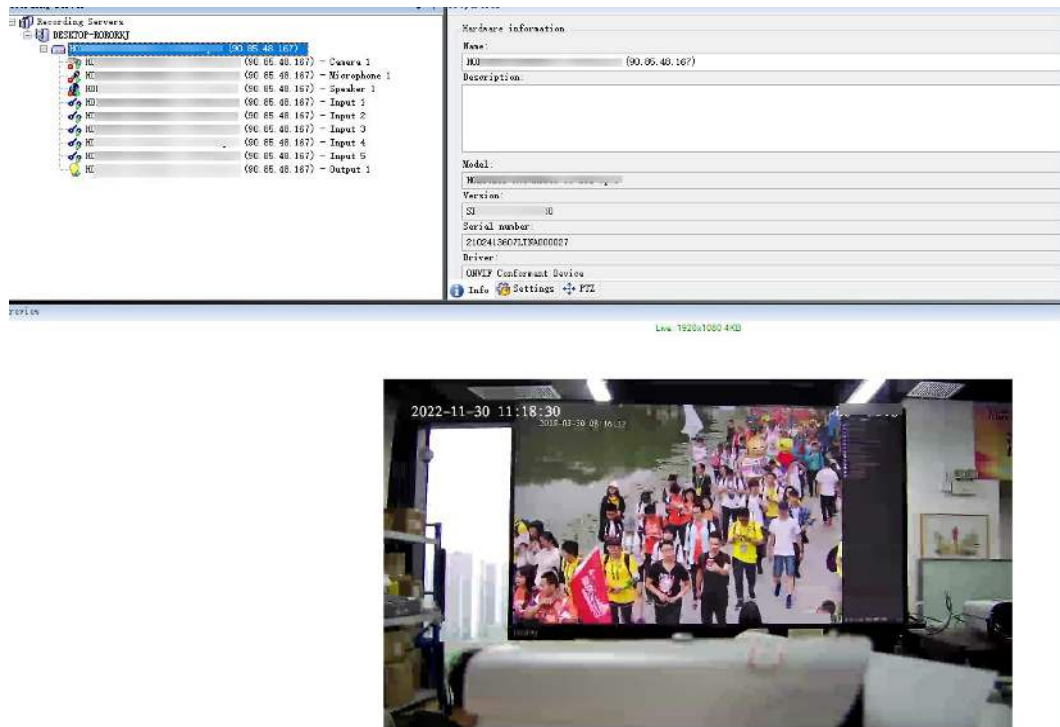
Step 8 Enter the camera group information and click **Finish**, as shown in [Figure 4-90](#).

Figure 4-90 Entering the camera group information



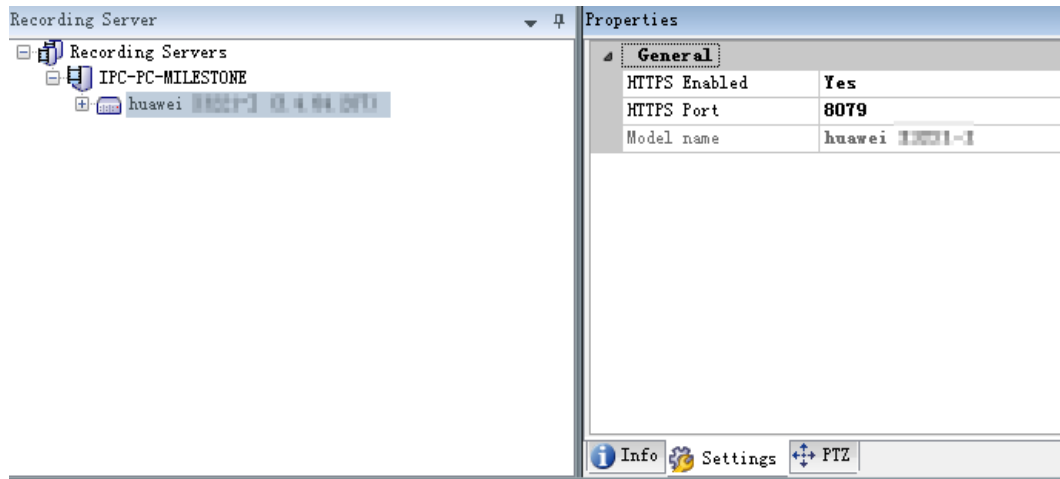
Step 9 Select the camera that has been added to view its live video, as shown in [Figure 4-91](#).

Figure 4-91 Viewing live video from the camera



Step 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 4-92](#).

Figure 4-92 Setting HTTPS parameters



1. Set **HTTPS Enabled** to **Yes**, indicating that HTTPS is enabled.
2. Set **HTTPS Port** to **443**, which is the same as the value of HTTPS port number set under **Configuration > Network > Network Parameters > HTTP(S)**.

 NOTE

If the processor type is Hi3516E V200 or Hi3516E V300, the default value of **HTTPS Port** is **8079**, as shown in [Figure 4-92](#). 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.

----End

4.9.2.1.2 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

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > Network > Platform Connection > General Protocol > RTSP**.
- Step 3 Set RTSP parameters, as shown in [Figure 4-93](#). [Table 4-52](#) describes the parameters.

Figure 4-93 Setting RTSP parameters

metadata extension

☒ 

* Port

* Post-NAT port

Transmission Type

Elementary stream



Authentication mode

Digest_MD5

The MD5 encryption mode

Save

Table 4-52 RTSP parameters

Parameter	Description
metadata extension	Indicates whether to enable the function of obtaining intelligent analysis metadata from a camera in RTSP stream requesting mode.
Port	RTSP port.
Post-NAT port	External port number to which the camera's internal port number maps after NAT environment is configured.

Parameter	Description
Transmission Type	Type of streams to be transmitted. You can set this parameter to Elementary stream or Program stream based on the decoding device.
Authentication mode	• 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.

Step 4 Click **Save**.

----End

4.9.2.1.3 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, a camera actively registers with the platform. You need to set the platform IP address and port number on the camera 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.

Procedure

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > Network > Platform Connection > General Protocol > SDK**.
- Step 3 Set SDK parameters, as shown in [Figure 4-94](#). [Table 4-53](#) describes the parameters.

 **NOTE**

- If the camera needs to be registered with multiple platforms, select **Platform X** and configure information about the platform.
- 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 [4.8.1.2 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 4-94 Setting SDK parameters

Enable SDK



SDK non-encrypted port



Enabling the non-encrypted port will also enable TCP con

Platform 1

Platform 2

Platform 3

☐ Active SDK registration

☒ Two-factor authentication

Registration type

Single-server mode

Device ID

Active platform IP

Port numb

Save

Table 4-53 SDK parameters

Parameter	Description
Enable SDK	Indicates whether to enable SDK. SDK is enabled by default.

Parameter	Description
SDK non-encrypted port	Indicates whether to enable the SDK non-encrypted port. This port is enabled by default. After this port is enabled, the non-encrypted port can be registered.
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: • Single-server mode: applies when the platform is deployed in a single-node system. • Dual-server mode: applies when the 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	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.
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.

Step 4 Click **Save**.

----End

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*.

4.9.2.1.4 Configuring Connection to the Platform Through RESTful

This section describes how to connect a camera to the 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 **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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Network > Platform Connection > General Protocol > RESTful**.

Step 3 Set RESTful parameters, as shown in [Figure 4-95](#). [Table 4-54](#) describes the parameters.

Figure 4-95 Setting RESTful parameters

Device ID

Transmission protocol

HTTPS

Authentication mode

Digest_SHA256

The more secure SHA256 authentication mode is recommended

☒ Enable proactive registration

* URL

?

User name

Password

Save

Table 4-54 RESTful parameters

Parameter	Description
Device ID	Unique device ID.
Transmission protocol	• HTTPS: Data is transmitted through HTTPS. • 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.

Parameter	Description
Enable proactive registration	Indicates whether to enable proactive registration. After proactive registration is enabled, you need to set the platform URL, user name, and password.
URL	Platform URL. Set this parameter to http://IP address:port number/xxx or https://IP address:port number/xxx , for example, https://10.3.4.55:98/nat .
User name	User name used by the camera to register with the platform. This parameter is optional.
Password	Password used by the camera to register with the platform. 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 [4.9.2.4 Setting the Protocol Connection Password](#).

Step 4 Click **Save**.

----End

4.9.2.2 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.

Step 1 Log in to the camera web system and choose **Configuration > Network > Platform Connection > Media Stream Keepalive**. The tab page shown in [Figure 4-96](#) is displayed.

Figure 4-96 Media Stream Keepalive tab page



Step 2 Set media stream keep-alive parameters. [Table 4-55](#) describes the parameters.

Table 4-55 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, ONVIF, or RESTful protocol, the media stream request mode is used. If the platform supports the keep-alive function, you are advised to toggle on Enable media stream keep-alive .
Keepalive duration	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.

----End

4.9.2.3 Setting FTP Parameters

Cameras can upload snapshots to a preconfigured FTP or SFTP server through FTP or SFTP.

NOTE

- If the FTP software is required on the server, the **Serv-U FTP Server** software is recommended. The **Easy FTP Server** software 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 number**, **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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Network > Platform Connection > FTP**. The **FTP** tab page is displayed. Select **Enable** to enable FTP, as shown in [Figure 4-97](#).

Figure 4-97 Setting FTP parameters

☒ **Enable** The FTP protocol is not secure. Be cautious with this setting.

FTP Settings

Protocol

SFTP

* Server IP address

0.0.0.0

* Port number

22

Transmission format

GBK

User name

Password

Detect

?

Save

To ensure the integrity of uploaded data, verify that the upload rate is greater than the image st

Step 3 Set FTP parameters by referring to [Table 4-56](#).

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 4-56 FTP parameters

Parameter	Description
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 number	Port number of the target server to which snapshots are uploaded.
Transmission format	The transmission format corresponds to the character set code. If the transmission format does not match the character set code, garbled characters are displayed on the GUI. GBK: supports simplified Chinese and English. UTF-8: supports international languages.
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.
Detect	Used to check whether the FTP parameters you set are valid. Check 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 server IP address or port number is incorrectly set and the 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.
Naming rule	Rule for naming the FTP directory structure.

Parameter	Description
Directory	Path for storing snapshots on the target server. • Root directory: Uploaded snapshots are saved in the root directory of the target server. • Level-<i>X</i> directory: Uploaded snapshots are saved in the level-<i>X</i> 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 snapshots cannot be uploaded.
Level- <i>X</i> directory	Level-<i>X</i> directory, which can be named by a variety of elements such as Device IP, Time, and Custom. The naming elements displayed on the web page may vary between camera models. NOTE • When customizing a directory, you can define a deeper level of directory structure by using backslashes (\).

Step 4 Click **Save**.

----End

4.9.2.4 Setting the Protocol Connection Password

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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Network > Platform Connection > Protocol Connection Password**. Then you can change the SDK/RESTful and ONVIF passwords separately.

The following describes how to change the SDK/RESTful password. [Figure 4-98](#) shows the page for setting the SDK/RESTful password.

NOTE

HWSDK and RESTful use the same account.

Figure 4-98 SDK/RESTful Password tab page

SDK/RESTful Password

ONVIF Password

User name

admin/ApiAdmin

Web user password

New password

Confirm password

Save

- Step 3** 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.

- Step 4** Click **Save**.
- End

4.10 Video and Audio Configuration

This chapter describes how to set video and audio parameters.

4.10.1 Video and Audio Feature Differences

Supported video and audio features vary depending on the camera models. The following table describes the differences.

Table 4-57 Differences in audio and video feature configurations

Device Model	SuperCoding	Intelligent Encoding	Area Cropping	Audio Input Port
E1A-4LR(3.6)	NO	YES	NO	YES. Supports one-channel built-in MIC.
E4A-4R(3.6)	NO	YES	NO	YES. Supports one-channel built-in MIC.
E4A-4R(2.8)	NO	YES	NO	YES. Supports one-channel built-in MIC.

4.10.2 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 4-58](#) describes common resolutions.

Table 4-58 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.
D1_NTSC	The resolution is 720 x 480, about 350,000 pixels.
CIF_PAL	The resolution is 352 x 288, about 100,000 pixels.

Resolution	Description
CIF_NTSC	The resolution is 352 x 240, about 84,000 pixels.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **Video/Audio** > **Video**.

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

Figure 4-99 Setting video parameters

Number of secondary streams

1

Full frame rate

PAL(25Hz)

?

Primary Stream

Secondary Stream 1

Encoding protocol

H.264

Resolution

2560*1440

Frame rate

25

Max. bit rate (kbit/s)

512

8192

4096

Advanced

▲

☐ Intelligent encoding

Bit rate type

Variable bit rate

Encoding complexity

High

I-frame interval

1

500

50

Stream smoothing coefficient

☐

1

100

50

?

☒ Slice

Save

Step 3 Set video parameters. [Table 4-59](#) describes the parameters.

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

Table 4-59 Video parameters

Parameter	Description
Number of secondary streams	Number of secondary streams. Value 0 indicates that only the primary stream can be set. Value 1 indicates that both primary and secondary streams can be set. • 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. The thermal imaging channel of a thermal camera can be set only to Primary Stream.
Full frame rate	Frame rate collected through the sensor, representing the maximum capability of a camera. 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.
Encoding protocol	Video encoding protocol. • H.264: The H.264 protocol requires relatively low bandwidth to ensure video quality. • H.265: The H.265 protocol is bandwidth-conserving compared with the H.264 protocol. 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.264 and H.265.
Resolution	Video resolution. A higher resolution indicates clearer images and higher bandwidth consumption.
Frame rate	Number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.

Parameter	Description
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.
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 actually required bandwidth 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. - 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.
Intelligent encoding	Indicates whether to enable intelligent encoding. If it is enabled, the camera can automatically adapt to scenarios to reduce bit rate and save 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, and I-frame interval 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. - After the function of rotating images by 90° is enabled, the encoding compression ratio will decrease.
Bit rate type	Type of the bit rate. 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 dynamic changes, the images will be unclear.

Parameter	Description
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 After intelligent encoding is enabled, the options of Bit rate control mode are Balanced, Image quality priority, and Bit rate compression priority.
Encoding complexity	This parameter is available only when Encoding protocol is set to H.264 or H.265 or other related formats. 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 encoding protocol is changed to H.264, High profile is used by default.
I-frame interval	This parameter is available only when Encoding protocol is set to H.264 or H.265. 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.
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.
Slice	Indicates whether to enable multi-slice encoding. The parameter is available only when Encoding protocol is set 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 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.

Step 4 Click **Save**.
----End

4.10.3 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Video/Audio > Audio**.
- Step 3** Click **Audio**. The **Audio** tab page is displayed, as shown in [Figure 4-100](#). The parameters displayed on this page may vary between camera models.

Figure 4-100 Audio parameters

Audio format

G.711a

Input port type

Mic-in

?

Input volume

0

100

85

☐ Environmental noise filtering

☐ Audio auto gain

☐ Echo cancellation

Save

- Step 4** Set audio parameters and click **Save**. [Table 4-60](#) describes the parameters.

Table 4-60 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. • AAC: primarily used in scenarios where the size of an audio file needs to be reduced. NOTE • After the audio stream format is changed, you need to request the media stream again for the setting to take effect. You can access the live video viewing page to request the media stream again.
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.
Input volume	Controls the input volume.
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.

Step 5 Click **Alarm-triggered Audio**. The **Alarm-triggered Audio** area is displayed, as shown in [Figure 4-101](#).

Figure 4-101 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 **Upload**.
- 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.

----End

4.10.4 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.

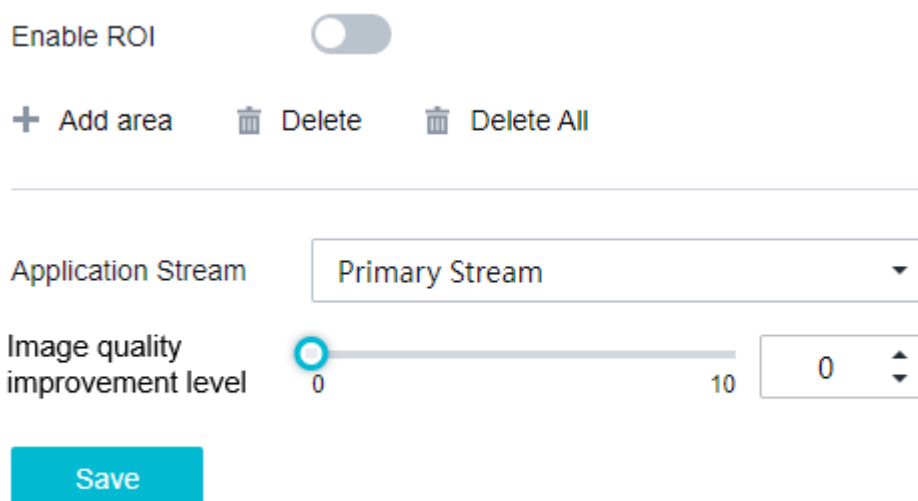
Prerequisites

You have set **Encoding protocol** to H.264 or H.265 or other related formats.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Video/Audio > ROI**. The **ROI** tab page is displayed, as shown in [Figure 4-102](#).

Figure 4-102 Setting ROI parameters



Enable ROI ☐

+ Add area  Delete  Delete All

Application Stream Primary Stream

Image quality improvement level 0 10 0

Save

- Step 3** Toggle on **Enable ROI**.

Step 4 Set Application Stream.

Step 5 Click Add area.

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.

Step 6 Use the mouse to adjust the ROI location and size.

Step 7 Select the ROI and set Image quality improvement level.

 NOTE

- When the ROI function is enabled, the value of **Image quality improvement level** reflects the quality difference between the current ROI area and non-ROI area.
- A larger value of **Image quality improvement level** indicates increased image quality inside the ROI area and decreased image quality outside the ROI area.
- After you set **Image quality improvement level**, the definition of the image (including the OSD text) in some parts outside the ROI area decreases.

Step 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**.

----End

4.11 Configuring Images

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

4.11.1 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 4-61 Differences in image configurations supported by different camera models

Device Model	Rotate Images by 90°	Exposure Compensation	Exposure Mode	Focus Area Selection	Electronic Image Stabilization	Focus Compensation	IR Overexposure Compensation	Day/Night Schedule	Distortion Correction	Privacy Mask
E4A-4R(3.6)	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES. Supports one monochromatic rectangular area for privacy mask; the color is configurable and is black by default.

Device Model	Rotate Images by 90°	Exposure Compensation	Exposure Mode	Focus Area Selection	Electronic Image Stabilization	Focus Compensation	IR Overexposure Compensation	Day/Night Schedule	Distortion Correction	Privacy Mask
E4A-4R(2.8)	NO	YES	YES	NO	NO	NO	YES	YES	NO	YES. Supports one monochromatic rectangular area for privacy mask; the color is configurable and is black by default.

Device Model	Rotate Images by 90°	Exposure Compensation	Exposure Mode	Focus Area Selection	Electronic Image Stabilization	Focus Compensation	IR Overexposure Compensation	Day/Night Schedule	Distortion Correction	Privacy Mask
E1A-4LR(3.6)	YES	YES	YES	NO	NO	NO	YES	YES	NO	YES. Supports one monochromatic rectangular area for privacy mask; the color is configurable and is black by default.

4.11.2 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Image > Display**.

Step 3 Set related parameters based on the site requirements. The following describes the parameters.

----End

Image Schedules

Figure 4-103 Image schedules

Image Preset

Default Scenario

Backlit

Custom Scene 1

Image Adjustment

Brightness

0

100

50

Saturation

0

100

50

Contrast

0

100

50

Sharpness

0

100

50

> Exposure

> Backlight

> White Balance

> Image Enhancement

> Day/Night Switch

> Illuminator Control

Reset

Table 4-62 Image schedule parameters

Parameter	Description
Default Scenario (default value)/ Backlit/Custom Scene 1	You can specify different image parameters, for example, image adjustment, exposure, and backlight parameters, for different schedules. You can select Backlit in the backlit scene where the bright area in the image is overexposed and the dark area in the image does not need to be concerned.
Reset	If you click Reset , all parameters (except the mirroring mode and the function of rotating images by 90 degrees) in the current image schedule are restored to default values.

Image Adjustment

Figure 4-104 Setting image adjustment parameters



Table 4-63 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 4-105 Setting day/night switch parameters

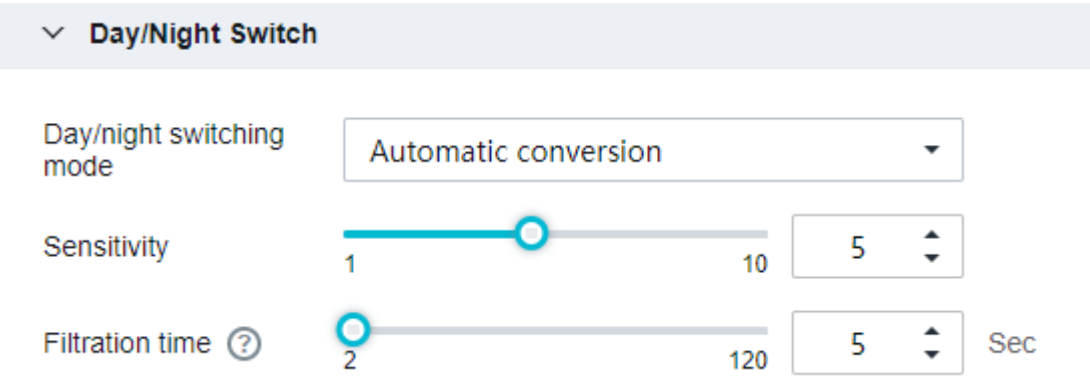


Table 4-64 Day/Night switch parameters

Parameter	Description
Day/night switching 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. • Automatic conversion: The camera automatically switches between the color mode and the B/W mode based on ambient light conditions. NOTE For some camera models, if Day/night switching mode is set to Automatic conversion, 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 conversion: If you select this option, you need to customize Night Mode. This mode is applicable to scenarios that require specified day/night switch time or unified day/night switch time for multiple cameras.
Sensitivity	This parameter is available only when Day/night switching mode is set to Automatic conversion. Sensitivity for switching between color mode and B/W mode. Higher sensitivity indicates that B/W mode is more likely to switch to color mode but color mode is less likely to switch to B/W mode. The default value is 5.
Filtration time	This parameter is available only when Day/night switching mode is set to Automatic conversion. When the ambient illuminance meets the day/night switch requirements and keeps at a level for a period specified by this parameter, the day/night mode is switched. The default value is 5, in seconds.

Exposure

The exposure parameters vary depending on the camera model.

Figure 4-106 Setting exposure parameters

▼ Exposure

Exposure mode

Manual ▼

Shutter speed

1/25 s ▼

Gain

0100

0 ▲▼

Table 4-65 Exposure parameters

Parameter	Description
Exposure mode	Exposure mode. ● Auto (default): The camera automatically sets the shutter speed and gain based on an object's exposure value measured by the metering system. ● Manual: You need to 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 . Exposure compensation is a technique for adjusting the exposure indicated by a photographic exposure 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.
Shutter limit	This parameter is available only when you set Exposure mode to Auto . This parameter is used to specify the minimum shutter speed. You can use common values or customize values (unit: μ s).
Gain limit	This parameter is available only when you set Exposure mode to Auto . The gain limit function is used to restrict the upper limit of the Automatic Gain Control (AGC). 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.

Parameter	Description
Gain	This parameter is available only when you set Exposure mode to Manual . The default value is 0 .

Backlight

Figure 4-107 Setting backlight parameters

▼ Backlight

Backlight mode

Wide dynamic range

?

WDR coefficient

1

100

50

Table 4-66 Backlight parameters

Parameter	Description
Backlight mode	This parameter is available only when you set Exposure mode to Auto. • 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. • 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.
WDR coefficient	This parameter is available only when you set Exposure mode to Auto and Backlight mode 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 level	This parameter is available only when you set Exposure mode to Auto and Backlight mode to Highlight compensation. The default value is Medium. A higher HLC level indicates more powerful highlight compensation.

White Balance

Figure 4-108 Auto white balance parameters

White Balance

Mode

Auto White Balance

Red Tendency

0100

50

Blue Tendency

0100

50

Regional white balance

☐

Figure 4-109 Manual white balance parameters

White Balance

Mode

Manual white balance

Red gain

0100

50

Blue gain

0100

50

Figure 4-110 Automatic tracking parameters

▼

White Balance

Mode

Auto tracking ▼

CT upper limit

1000

15000

10000 ▲▼

CT lower limit

1000

15000

1500 ▲▼

Regional white balance

☐

Table 4-67 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 White Balance (default): This mode is recommended. The camera automatically adjusts the gain 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. In this case, you can drag the slider to change the values of Red Tendency and Blue Tendency or directly enter an integer in corresponding text boxes. – Regional white balance: This parameter is available only when you set Mode to Auto White Balance or Auto tracking. If you toggle on Regional white balance, you can configure a white balance area on the View page. Then the white balance function takes effect only in this area. • Manual white balance: The red and blue gain must be adjusted manually. You can drag the slider to change the values of Red gain and Blue gain or directly enter 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. – Regional white balance: This parameter is available only when you set Mode to Auto White Balance or Auto tracking. If you toggle on Regional white balance, you can configure a white balance area on the View page. Then the white balance function takes effect only in this area. • Lock white balance: 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. • Global white balance: This mode is applicable to environments where fluorescent lamps are used and the color temperature ranges from 3500 K to 4500 K.

Image Enhancement

The image enhancement functions vary depending on the camera model.

Figure 4-111 Image enhancement parameters in manual mode

Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

Defogging

Manual

Defogging level

0100

50

Anti-light flicker

Disable

Denoising

Automatic noise reduction

IR overexposure compensation

0100

50

Table 4-68 Image enhancement parameters

Parameter	Description
Rotate images by 90 degrees	Indicates whether to enable the function of rotating images by 90 degrees (aspect ratio: 9:16 or 3:4). NOTE To enable this function, 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.
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.

Parameter	Description
Defogging	This function is used to increase image clarity in poor weather conditions such as rain, fog, and smog. To disable this function, set this parameter to Disable. If this parameter is set to Overcast adaptation, 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.
Anti-light flicker	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 this parameter based on standard frequency of the local power grid. For example, if the standard frequency of the local power grid is 50 Hz, this parameter needs to be set to 50Hz. In natural light conditions, set this parameter to Disable.
Denoising	Indicates whether to enable the noise reduction function. The options are as follows: • Disable: Disable the noise reduction function. • Automatic noise reduction (default): The system automatically performs noise reduction. • Expert mode: The Spatial denoising level and Temporal denoising level parameters are available only when Denoising is set to Expert mode. – 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 denoising level indicates better noise reduction effect. However, more edge details will be lost. – 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.
IR overexposure compensation	If IR illuminators are enabled and overexposure occurs in the image view with strong reflective objects such as leaves and wires nearby, you can set this parameter to a larger value. The default value is 50.

Illuminator Control

Figure 4-112 Setting illuminator control parameters

▼ Illuminator Control

Built-in Illuminator

Control mode

Manual

Low beam

Brightness control

0

100

50

Table 4-69 Illuminator control parameters

Parameter		Description
Built-in Illuminator	Control mode	• Auto (default): Indicates that the camera automatically turns on or off the illuminator and controls its brightness. • Manual: Indicates that the illuminator 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 and Brightness control. • Intelligent light compensation: The camera automatically performs light compensation. In B/W mode at night, when motion detection or human figure detection is triggered, the camera switches to color mode and turns on the white-light illuminator. After the alarm is cleared, the white-light illuminator is automatically turned off and the video image turns back to B/W mode. NOTE • 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 camera determines whether to enable white-light or IR illuminators based on the current ambient illuminance. The user-defined brightness takes effect only when the camera determines that illuminators need to be enabled. • Some camera models do not have white-light illuminators.
	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 set Turn-on time and Brightness control.
	Brightness control	This parameter is available only when Control mode is set to Manual or Scheduled. A larger value indicates higher illuminator brightness.

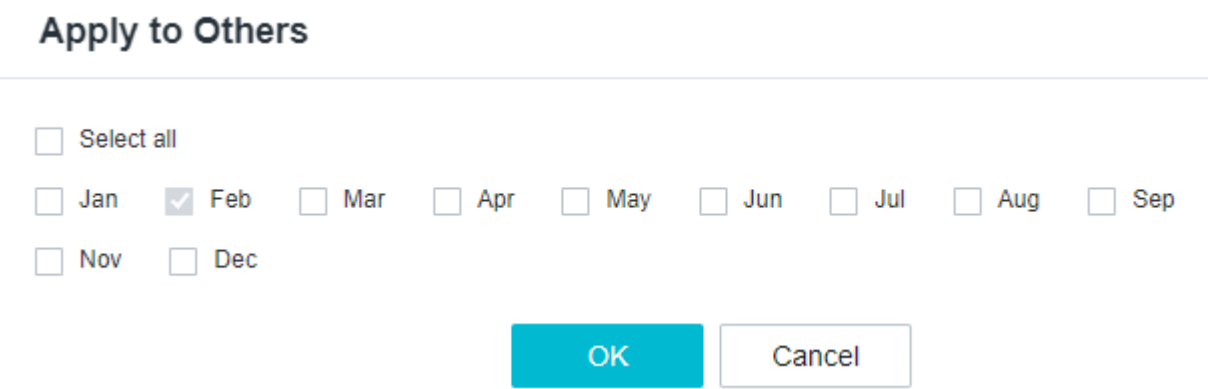
 NOTE

- Different models of cameras support different schedules.
- You can click **Cancel** to undo the previous operation.
- You can click **Restore** to restore the last undone operation. Cleared schedules cannot be restored.
- You can click **Clear** to delete all schedules.

Step 4 Select a time-based schedule and set time periods in the table below. Only one schedule can be executed at a time.

Step 5 (Optional) Click  on the right of the table. In the **Apply to Others** dialog box that is displayed, select required months. Then the schedule of a specific month is applied to the selected months.

Figure 4-114 Apply to Others dialog box



Step 6 (Optional) Click  on the right of the table to delete all schedules of a month.

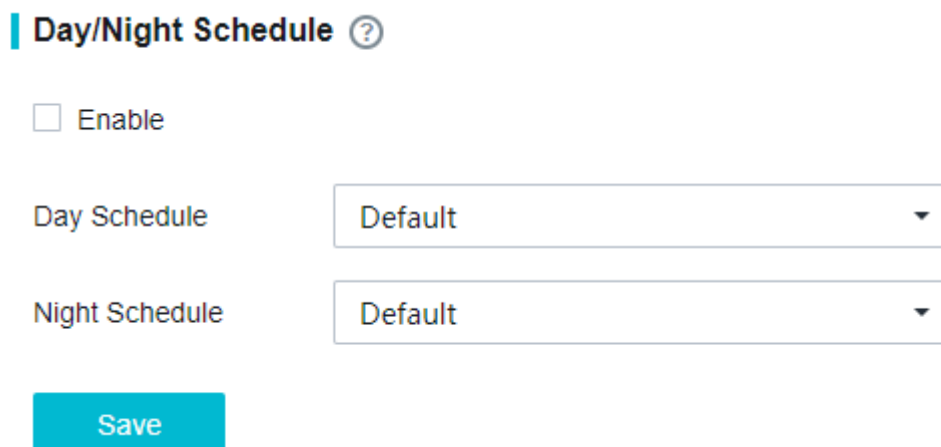
Step 7 Click **Save**.

----End

Configuring a Day/Night Schedule

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Click **Day/Night Schedule**. The area shown in [Figure 4-115](#) is displayed.

Figure 4-115 Day/Night Schedule area



Day/Night Schedule ?

☐ Enable

Day Schedule Default ▼

Night Schedule Default ▼

Save

Step 3 Select **Enable**.

Step 4 Set **Day Schedule** and **Night Schedule** depending on your needs.

After day/night schedules are configured, the camera automatically switches between the color mode and the B/W mode based on the operating environment and enables the corresponding day/night schedule.

Step 5 Click **Save**.

----End

4.11.4 Configuring OSD

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

Setting OSD Parameters

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration** > **Image** > **OSD**. The **OSD** tab page is displayed, as shown in [Figure 4-116](#). The parameters vary between camera models.

Figure 4-116 Setting OSD parameters

OSD template

Custom

GB

Configuration

OSD mode

Custom

Template name

Custom

Font color

Invert OSD color

Font size

Self-adaptive

Line spacing

0

Align Type

Upper left alignment

OSD Content

+ Add OSD

🗑 Delete All

Horizon...	Vertical ...	Content	Operation
149	104	<code>\${time@sys: YYYY-MM-DD}</code>	InsertDelete

NOTE

- Generally, the OSD parameters set here apply to all OSD records. If you modify parameters of an OSD record on the iClient or by invoking the API, the modifications apply only to the first OSD record in the camera web system.
- Step 3** Configure the OSD template. [Table 4-70](#) describes the OSD template parameters and buttons.
- Hover the mouse over an OSD template and choose **Copy Template** from the drop-down menu. In the dialog box that is displayed, enter a new template name and click **OK**. The new template is added. A maximum of two OSD templates are supported currently.
 - Hover the mouse over an OSD template and choose **Delete Template** from the drop-down menu. In the dialog box that is displayed, click **OK** to delete the template.

Table 4-70 OSD template parameters/buttons

Parameter/ Button		Description
Conf igura tion	OSD mode	The value is determined by the OSD template and cannot be changed.
	Template name	Name of the selected template. You can customize the name as required.
	Font color	The options are Invert OSD color and Custom . If you select Invert OSD color , the OSD text color is set to a color opposite to the background color.
	Font size	The default value varies depending on the camera model. You can set this parameter depending on your needs.
	Line spacing	OSD line spacing.
	Align Type	OSD alignment mode. You can select an option from the drop-down list.
OSD Cont ent	Add OSD	Button for adding an OSD record using a template. NOTE – A maximum of six OSD records can be added to each customized OSD template. – In GB-compliant OSD mode, the number of OSD records is fixed to four. You cannot add or delete one.
	Delete All	This button is available only in custom OSD mode. If you click Delete All , all OSD records will be deleted.
	Horizontal Margin/ Vertical Margin	These parameters are available only in custom OSD mode. You can enter a number in the text boxes.
	Content	OSD text content. You can customize text content in the text box. NOTE – The 6763 Chinese characters defined in GB2312 are supported.
	Operation	In custom OSD mode, two buttons Insert and Delete are displayed in the Operation column. In GB-compliant OSD mode, only the Insert button is displayed in the Operation column. To set OSD time, click Insert . To delete an OSD record, click Delete corresponding to the record.

----End

4.11.5 Configuring Privacy Mask

You can mask a specified area on live video images to protect sensitive or private information.

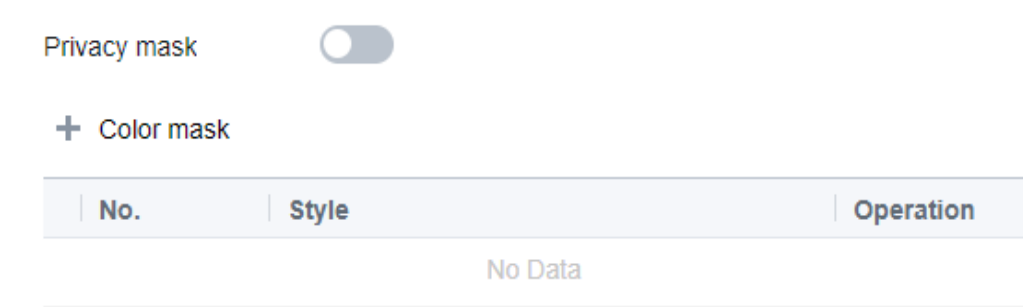
NOTICE

- 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.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Image > Area Coverage**. The tab page shown in the following figure is displayed. The parameters displayed on the web page vary depending on the camera model.

Figure 4-117 Area Coverage tab page



- Step 3** Toggle on **Privacy mask**.
- Step 4** Click **Color mask** to add a mask area.
- Step 5** Click  in the **Operation** column to delete the mask area.

 NOTE

- You can click the color block in the **Style** column to customize the mask color.
- Only one monochromatic rectangular mask area can be added. The mask area color is configurable and is black by default. You can drag the mask area to adjust its location.

----End

4.12 Intelligent Settings

This section describes how to configure intelligent analysis functions.

NOTICE

- Functions available on the web page vary between camera models.
-

4.12.1 Common Event Analysis Configuration

This chapter describes how to configure common intelligent analysis functions such as motion detection, human figure detection, and lens blocking detection.

NOTICE

- Pan, tilt, or zoom operations are not supported during intelligent 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.
-

4.12.1.1 Specifications of the Common Event Analysis Feature

The following table lists the common events supported by different camera models.

Table 4-71 Common events supported by different camera models

Device Model	Motion Detection ^a	Human Figure Detection	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	Visibility Detection
E1A-4LR(3.6)	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO
E4A-4R(3.6)	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO
E4A-4R(2.8)	YES	YES	NO	YES	NO	NO	NO	NO	NO	NO
a: This function cannot be put into commercial use currently. The specifications vary greatly in different scenarios.										

4.12.1.2 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

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Intelligence > Common Event Analysis**. Toggle on **Motion**, as shown in [Figure 4-118](#). If the **Information** dialog box is displayed, the setting is successful.

Figure 4-118 Enabling motion detection


- Step 3** Click **Settings** next to **Motion**. On the page that is displayed, set motion detection parameters, as shown in [Figure 4-119](#).

Figure 4-119 Setting motion detection parameters



Table 4-72 Motion detection parameters

Parameter	Description
Alarm sensitivity	Motion detection sensitivity. NOTE A larger value indicates higher sensitivity. To detect slight motion, you are advised to set the sensitivity to a larger value.

Step 4 Click **Add** under **Detection Area**.

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.

Step 5 Use the mouse to adjust the location and size of the motion detection area.

Step 6 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**.

----End

Configuring an Alert Plan

After an alert plan is configured, 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 capture service.

Step 1 Click the **Alert Deployment Plan** tab. The **Alert Deployment Plan** tab page is displayed, as shown in [Figure 4-120](#).

Figure 4-120 Alert Deployment Plan tab page

+ Add

Delete All

No.	Status	Start time	End time	Date	Mode	Operation
1	☒	00:00:00	24:00:00	Everyday	Weekly	

Save

Step 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 4-121](#).

Figure 4-121 Edit Plan dialog box

Edit Plan

Start time

00:00:00



End time

24:00:00



Cyclic mode

Weekly



Select days

☒ All

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

OK

Cancel

Step 3 Set **Start time**, **End time**, **Cyclic mode**, and **Select days**.

Step 4 Click **OK**.

Step 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.

----End

Configuring Alarm Linkage

Step 1 Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in [Figure 4-122](#).

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4-122 Configuring alarm linkage

Alarm type

Event

Alarm interval

10

Sec

Alarm Linkage Policy

☒ ONVIF

☒ SDK

☐ RESTful

☐ Email

☐ White light illuminator

☐ Snapshot taking

☐ Video recording

Save

Step 2 Set related parameters. [Table 4-73](#) describes the parameters.

Table 4-73 Alarm linkage 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	Interval at which the camera reports event alarms to the platform.
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 email linkage, see 4.9.1.3 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.
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. The value range may vary depending on the camera model.
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.
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). NOTE To prevent motion detection alarms from being falsely reported when the illuminator flashes, the next alarm is triggered 3s to 5s after the illuminator stops flashing.

Step 3 Click **Save**.

----**End**

Verification

Choose **Configuration** > **System** > **System Maintenance** > **Log**, set **Select Log** to **Warning** under **Querying Logs**, and check whether a motion detection alarm is reported.

4.12.1.3 Configuring Lens Blocking Detection

After lens blocking detection is configured, an alarm will be generated promptly when the lens is blocked.

Setting Lens Blocking Detection Parameters

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration** > **Intelligence** > **Common Event Analysis**. Toggle on **Lens Blocking**, as shown in [Figure 4-123](#). If the **Information** dialog box is displayed, the setting is successful.

Figure 4-123 Enabling lens blocking detection



- Step 3** Click **Settings** next to **Lens Blocking**. On the page that is displayed, set lens blocking detection parameters, as shown in [Figure 4-124](#).

Figure 4-124 Setting lens blocking detection parameters

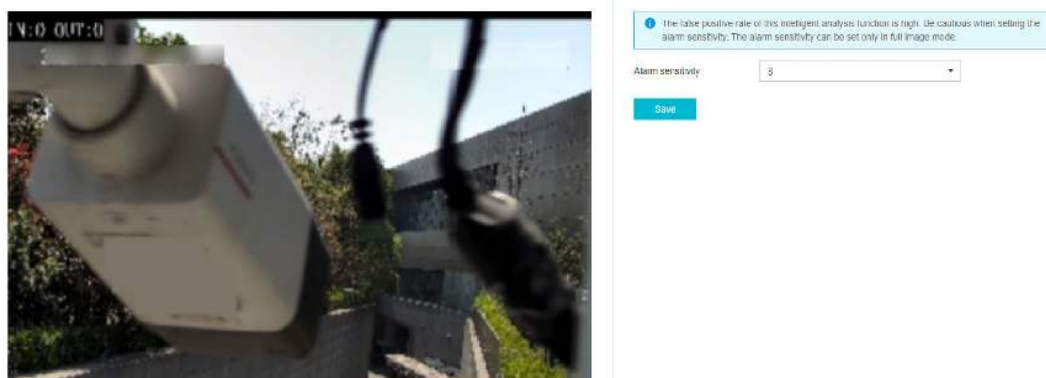


Table 4-74 Lens blocking detection parameters

Parameter	Description
Alarm sensitivity	Lens blocking detection sensitivity. A larger value indicates higher sensitivity. With higher sensitivity, the camera can generate alarms when the lens is blocked by an object with a smaller size and brighter luminance. NOTE • If Alarm sensitivity is set to 1, an alarm will be generated when the percentage of the blocked area reaches about 95%. • If Alarm sensitivity is set to 2, an alarm will be generated when the percentage of the blocked area reaches about 90%. • If Alarm sensitivity is set to 3, an alarm will be generated when the percentage of the blocked area reaches about 85%. • If Alarm sensitivity is set to 4, an alarm will be generated when the percentage of the blocked area reaches about 80%. • If Alarm sensitivity is set to 5, an alarm will be generated when the percentage of the blocked area reaches about 70%.

Step 4 Click **Save**.

----End

Configuring an Alert Plan

After an alert plan is configured, 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 capture service.

Step 1 Click the **Alert Deployment Plan** tab. The **Alert Deployment Plan** tab page is displayed, as shown in [Figure 4-125](#).

Figure 4-125 Alert Deployment Plan tab page

+ Add		Delete All				
No.	Status	Start time	End time	Date	Mode	Operation
1	☒	00:00:00	24:00:00	Everyday	Weekly	
Save						

Step 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 4-126](#).

Figure 4-126 Edit Plan dialog box

Edit Plan

Start time

00:00:00

End time

24:00:00

Cyclic mode

Weekly

Select days

☒ All

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

OK

Cancel

Step 3 Set **Start time**, **End time**, **Cyclic mode**, and **Select days**.

Step 4 Click **OK**.

Step 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.

----End

Configuring Alarm Linkage

Step 1 Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in [Figure 4-127](#).

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4-127 Configuring alarm linkage

Alarm type

Event

Alarm interval

10

Sec

Alarm Linkage Policy

☒ ONVIF

☒ SDK

☐ RESTful

☐ Email

☐ White light illuminator

☐ Snapshot taking

☐ Video recording

Save

Step 2 Set related parameters. Table 4-75 describes the parameters.

Table 4-75 Alarm linkage 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	Interval at which the camera reports event alarms to the platform.
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 email linkage, see 4.9.1.3 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
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. The value range may vary depending on the camera model.
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.
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). NOTE To prevent lens blocking alarms from being falsely reported when the illuminator flashes, the next alarm is triggered 3s to 5s after the illuminator stops flashing.

Step 3 Click **Save**.

----End

Verification

Choose **Configuration > System > System Maintenance > Log**, set **Select Log** to **Warning** under **Querying Logs**, and check whether a lens blocking alarm is reported.

4.12.1.4 Configuring Human Figure Detection

After human figure detection is configured, an alarm will be generated when a target is detected.

Setting Human Figure Detection Parameters

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Intelligence > Common Event Analysis**. Toggle on **Human Figure Detection**, as shown in [Figure 4-128](#). If the **Information** dialog box is displayed, the setting is successful.

Figure 4-128 Enabling human figure detection



Step 3 Click **Settings** next to **Human Figure Detection**. On the page that is displayed, set human figure detection parameters, as shown in [Figure 4-129](#).

Figure 4-129 Setting human figure detection parameters

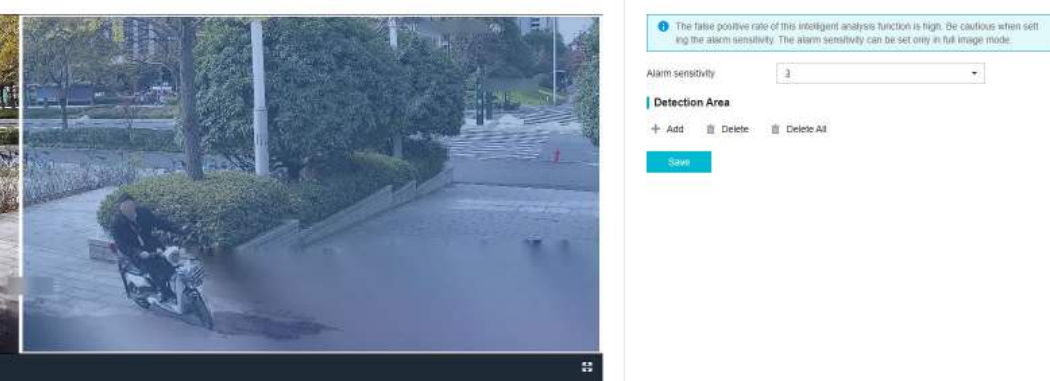


Table 4-76 Human figure detection parameters

Parameter	Description
Alarm sensitivity	Human figure detection sensitivity. A larger value indicates higher sensitivity.

Step 4 Click **Add** under **Detection Area**.
A human figure detection area is displayed on the live video image.

 **NOTE**
Only one human figure detection area can be added.

Step 5 Use the mouse to adjust the location and size of the detection area.

Step 6 Click **Save**.

 **NOTE**

- To detect the human figure detection area, select it on the live video image and click **Delete**.
- You can also click **Delete All** to directly delete the human figure detection area.

----End

Configuring an Alert Plan

After an alert plan is configured, 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 capture service.

Step 1 Click the **Alert Deployment Plan** tab. The **Alert Deployment Plan** tab page is displayed, as shown in [Figure 4-130](#).

Figure 4-130 Alert Deployment Plan tab page

+ Add

Delete All

No.	Status	Start time	End time	Date	Mode	Operation
1	☒	00:00:00	24:00:00	Everyday	Weekly	

Save

Step 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 4-131](#).

Figure 4-131 Edit Plan dialog box

Edit Plan

Start time

00:00:00

End time

24:00:00

Cyclic mode

Weekly

Select days

☒ All

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

OK

Cancel

Step 3 Set **Start time**, **End time**, **Cyclic mode**, and **Select days**.

Step 4 Click **OK**.

Step 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.

----End

Configuring Alarm Linkage

Step 1 Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in [Figure 4-132](#).

NOTICE

Different camera models support different alarm linkage actions. Some alarm linkage actions can be displayed only after related functions are configured.

Figure 4-132 Configuring alarm linkage

Alarm type

Event

Alarm interval

10

Sec

Alarm Linkage Policy

☒ ONVIF

☒ SDK

☐ RESTful

☐ Email

☐ White light illuminator

☐ Snapshot taking

☐ Video recording

Save

Step 2 Set related parameters. Table 4-77 describes the parameters.

Table 4-77 Alarm linkage 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	Interval at which the camera reports event alarms to the platform.
ONVIF	If ONVIF is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.

Parameter	Description
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 email linkage, see 4.9.1.3 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.
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. The value range may vary depending on the camera model.
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.
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). NOTE To prevent motion detection alarms from being falsely reported when the illuminator flashes, the next alarm is triggered 3s to 5s after the illuminator stops flashing.

Step 3 Click **Save**.

----End

Verification

Choose **Configuration > System > System Maintenance > Log**, set **Select Log** to **Warning** under **Querying Logs**, and check whether a human figure detection alarm is reported.

4.13 Storage Configuration

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

4.13.1 Configuring Storage Management

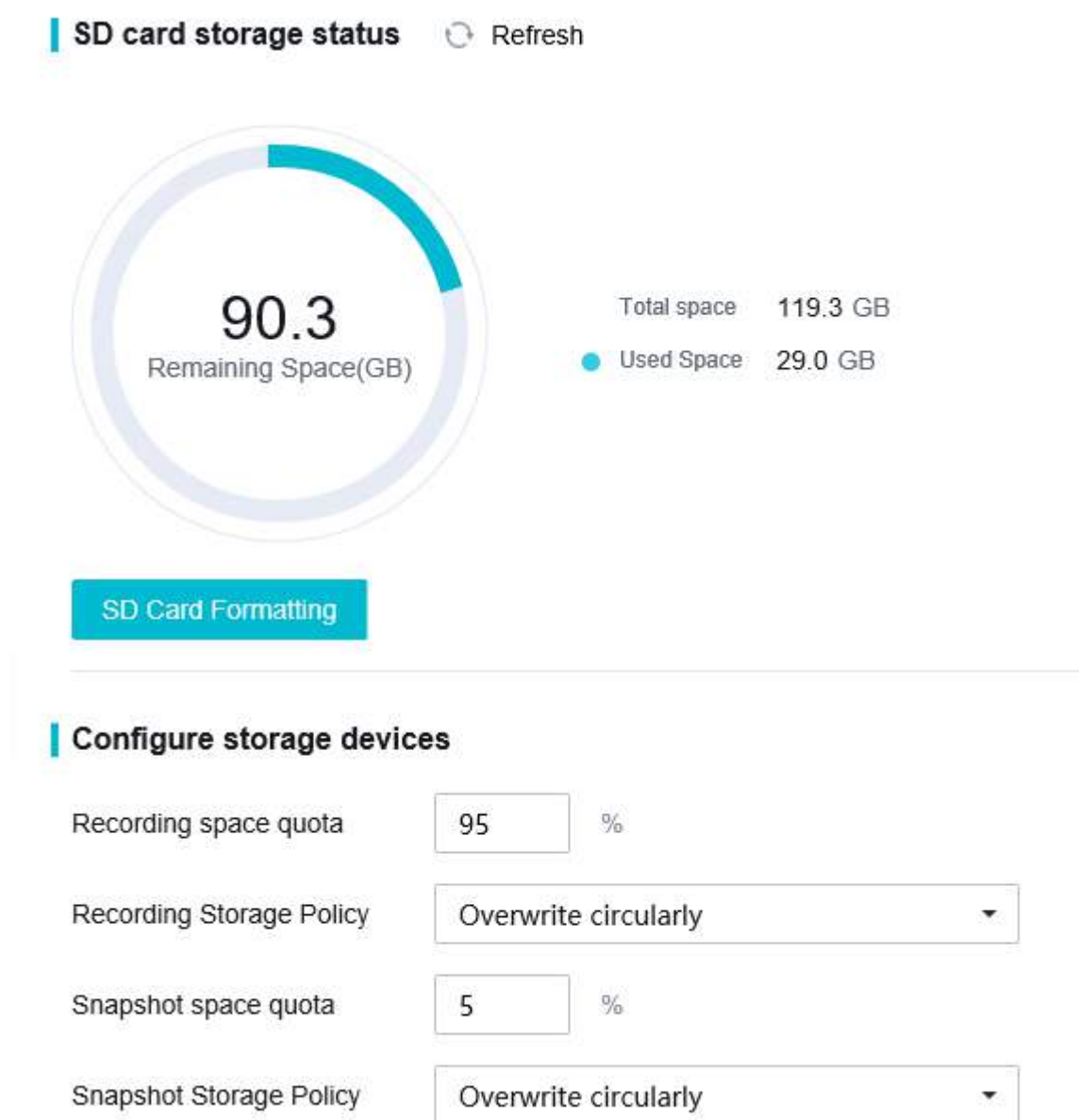
Using the storage management function, you can view the SD card status, limit the download rate, and conduct cyclic recording.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Storage > Storage Management**. The **Storage Management** tab page is displayed, as shown in [Figure 4-133](#).

The web page varies depending on the camera model.

Figure 4-133 Storage Management page



Step 3 Set related parameters as required. [Table 4-78](#) describes the parameters.

Table 4-78 Storage management parameters

Parameter		Description
SD card storage status	No SD card	Indicates that there is no SD card on the camera.
	Total space/Used space	Total storage capacity and occupied space of an SD card.
	SD Card 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 compatibility list, compatibility issues may occur.
	Refresh	Displays the latest SD card status.
Configure storage devices	Recording space quota	Maximum space for storing recordings, in percentage. The value is an integer ranging from 1 to 100. The default value is 95 .
	Recording Storage Policy	Overwrite circularly: After the video recording function is enabled, recordings are saved on the SD card. When the SD card space is used up, the earliest recording files are automatically overwritten. Stop: After the video recording function is enabled, recordings are saved on the SD card. When the SD card space is used up, the camera stops recording video.
	Snapshot space quota	Maximum space for storing snapshots, in percentage. The value is an integer ranging from 1 to 100. The default value is 5 .

Parameter		Description
	Snapshot Storage Policy	• Overwrite circularly: After the snapshot taking function is enabled, snapshots are saved on the SD card. When the SD card space is used up, the earliest snapshots are automatically overwritten. • Stop: After the snapshot taking function is enabled, snapshots are saved on the SD card. When the SD card space is used up, the camera stops taking snapshots.

----End

4.13.2 Setting Snapshot Parameters

You can set snapshot parameters such as the snapshot storage space in the SD card, snapshot format, and snapshot interval.

NOTICE

Scheduled snapshot will result in frequent writes to the SD card, which will shorten the SD card's service life.

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration** > **Storage** > **Snapshot**. The **Snapshot** tab page is displayed, as shown in [Figure 4-134](#).

Figure 4-134 Snapshot tab page

Function switch

Enable image storage

?

Enable scheduled snapshot

Setting snapshots

Quality

Average

Resolution

2560*1440

The snapshot resolution is valid only for full images.

Scheduled snapshot format

JPG

Scheduled snapshot interval

10

Sec

Step 3 Set related parameters as required. Table 4-79 describes the parameters.

Table 4-79 Snapshot parameters

Parameter		Description
Function switch	Enable 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 100%, 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.
	Enable scheduled snapshot	Indicates whether to take a snapshot 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.
Setting snapshots	Quality	Snapshot quality.

Parameter		Description
	Resolution	Snapshot resolution, which is the same as the resolution of primary streams. For details, see 4.10.2 Setting Video Parameters . The snapshot resolution is valid only for full images.
	Scheduled snapshot format	Format of scheduled snapshots. Currently, only the JPG format is supported.
	Scheduled snapshot interval	Interval at which snapshots are taken. The default value is 10 seconds. This parameter can be set only after Enable scheduled snapshot is toggled on.

----End

4.13.3 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 on 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 [4.13.1 Configuring Storage Management](#).

Procedure

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Storage > Video recording**. The **Video recording** tab page is displayed, as shown in [Figure 4-135](#).

Parameter		Description
	Enable buffering	Indicates whether to enable video buffering. If you enable this toggle button, when a camera is disconnected from the network, it can continue to shoot and temporarily store video on its SD card. When the network is restored, the video security platform sends a video request to the camera. The camera then sends the video stored on the SD card to the platform. 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 system stops recording or overwrites earlier recordings based on the storage policy. • Whether a platform media stream session exception can trigger video buffering depends on the applied transmission protocol and whether the platform supports the media stream keepalive function. If the platform does not support media stream keepalive and the UDP protocol is used to request media streams, video buffering will not be triggered when a session exception occurs.
	Current recording status	Current status of different types of recordings.
Set recording	Manual SD card-based recording duration	Duration for recording video to 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.
	Rate limit	Rate for downloading recordings stored on the SD card. It is recommended that the value be a quarter of the primary stream bit rate and not exceed the available bandwidth. NOTE The rate for downloading recordings stored on the SD card can be adjusted. However, the rate cannot be adjusted during the download.
	Pre-recording policy	The options include No pre-recording and Pre-record by memory capacity .

Step 3 Toggle on **Scheduled**. Set start time and end time for a daily plan.

Step 4 (Optional) To cancel or restore an existing recording plan, click  **Cancel** or  **Restore**.

Step 5 (Optional) To delete all recording plans, click **Clear**.

Step 6 Click **Save**.

----End

4.14 Event Alarm Configuration

This chapter describes how to configure alarm reporting, certificate alarms, and fault alarms.

4.14.1 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 4-81 Differences in alarm linkage configurations of D series cameras

Device Model	White Light Illuminator	Email Sending	Onboard Video Recording	Onboard Snapshot Taking
E1A-4LR(3.6)	YES	YES	YES	YES
E4A-4R(3.6)	NO	YES	YES	YES
E4A-4R(2.8)	NO	YES	YES	YES

4.14.2 Alarm Reporting

4.14.2.1 Alarm Reporting Configuration

On the **Alarm Reporting** tab page, you can configure alarm linkage policies for common event and intelligent analysis alarms generated by cameras. The alarm linkage policies may vary depending on camera models.

NOTICE

Different camera models support different alarm linkage policies. Some alarm linkage policies can be displayed only after related functions are configured.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Detection > Alarm Reporting**. The **Alarm Reporting** tab page is displayed.

Step 3 Select the required alarm linkage action, as shown in [Figure 4-136](#). [Table 4-82](#) describes the parameters.

The alarm types displayed to external systems are subject to the ones supported by each linkage module (such as ONVIF and SDK). For details about the alarm linkage policies supported by each alarm type, see [4.14.2.2 Alarm Linkage Policy Description](#).

 NOTE

You are advised to configure one alarm linkage policy for a camera connected to the platform.

Figure 4-136 Configuring alarm reporting

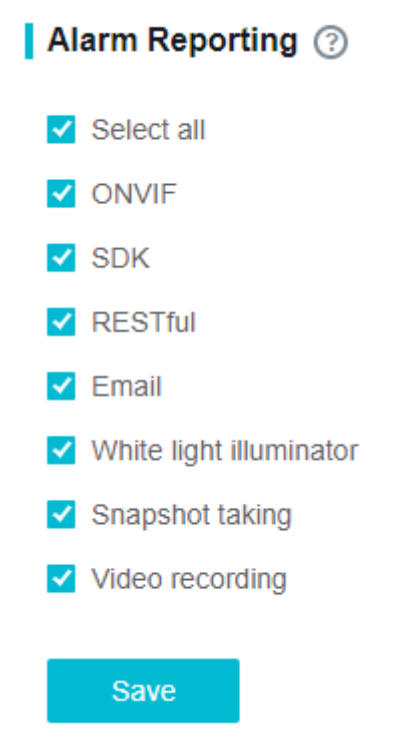


Table 4-82 Alarm reporting parameters

Parameter	Setting
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 email linkage, see 4.9.1.3 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	Setting
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. The value range may vary depending on the camera model. 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 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.
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). NOTE To prevent motion detection and lens blocking alarms from being falsely reported when the illuminator flashes, the next alarm is triggered 3s to 5s after the illuminator stops flashing.

Step 4 Click **Save**.

----End

4.14.2.2 Alarm Linkage Policy Description

Table 4-83 describes the alarm linkage policies supported by each alarm type.

NOTE

The alarm types supported by the camera are related to the capability set.

Table 4-83 Alarm linkage policies supported by each alarm type

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshot Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Full disk	YES	YES	YES	NO	NO	YES	YES	YES	NO
Disk read/write failure	YES	YES	YES	NO	NO	YES	YES	YES	NO
Disk removal	YES	YES	YES	NO	NO	YES	YES	YES	NO
Media stream interruption	YES	YES	YES	NO	NO	YES	YES	YES	NO
Boolean value	YES	YES	YES	YES	YES	YES	YES	YES	NO
Log storage	YES	YES	YES	NO	NO	YES	YES	YES	NO
PTZ configuration	YES	YES	YES	NO	NO	YES	YES	YES	NO
Flash read/write	NO	NO	NO	NO	NO	NO	NO	NO	NO
Temperature sensor fault	YES	YES	YES	NO	NO	YES	YES	YES	NO
Network port hot swap	NO	NO	NO	YES	YES	NO	YES	YES	NO
Fan stalled	YES	YES	YES	YES	YES	YES	YES	YES	NO

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshots Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Video loss	YES	YES	YES	NO	NO	YES	YES	YES	NO
Photosensitive sensor fault	YES	YES	YES	YES	YES	YES	YES	YES	NO
Wiper fault	YES	YES	YES	YES	YES	YES	YES	YES	NO
PTZ optocoupler fault	YES	YES	YES	YES	YES	YES	YES	YES	NO
Position change	YES	YES	YES	YES	YES	YES	YES	YES	NO
Lens PT optocoupler fault	YES	YES	YES	NO	NO	YES	YES	YES	NO
Abnormal system temperature	YES	YES	YES	NO	NO	YES	YES	NO	NO
Ascend processor fault	NO	NO	NO	NO	NO	NO	NO	NO	NO
Wi-Fi connection failure	YES	YES	YES	NO	NO	YES	YES	YES	NO
Upgrade / Rollback	NO	NO	NO	NO	NO	NO	NO	NO	NO

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshots Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Parking violation	YES	YES	YES	YES	YES	YES	YES	YES	NO
Marked lane violation	YES	YES	YES	YES	YES	YES	YES	YES	NO
Wrong-way driving	YES	YES	YES	YES	YES	YES	YES	YES	NO
Illegal backing	YES	YES	YES	YES	YES	YES	YES	YES	NO
Non-motorized vehicle in motor vehicle lane	YES	YES	YES	YES	YES	YES	YES	YES	NO
Motor vehicle in non-motorized vehicle lane	YES	YES	YES	YES	YES	YES	YES	YES	NO
Congestion	YES	YES	YES	YES	YES	YES	YES	YES	NO
License plate occlusion	YES	YES	YES	YES	YES	YES	YES	YES	NO
Motion	YES	YES	YES	YES	YES	YES	YES	YES	YES
Lens blocking	YES	YES	YES	YES	YES	YES	YES	YES	YES

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshots Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Human figure detection	YES	YES	YES	YES	YES	YES	YES	YES	YES
Intrusion	YES	YES	YES	YES	YES	YES	YES	YES	YES
Abandoned object	YES	YES	YES	YES	YES	YES	YES	YES	YES
Removed object	YES	YES	YES	YES	YES	YES	YES	YES	YES
Tripwire crossing	YES	YES	YES	YES	YES	YES	YES	YES	YES
Loitering	YES	YES	YES	YES	YES	YES	YES	YES	YES
Area entry	YES	YES	YES	YES	YES	YES	YES	YES	YES
Area exit	YES	YES	YES	YES	YES	YES	YES	YES	YES
Fast movement	YES	YES	YES	YES	YES	YES	YES	YES	YES
Fight	YES	YES	YES	NO	NO	YES	YES	YES	NO
Climbing	YES	YES	YES	NO	NO	YES	YES	YES	NO
Fall	YES	YES	YES	NO	NO	YES	YES	YES	NO
Running	YES	YES	YES	NO	NO	YES	YES	YES	NO
Automatic tracking	YES	YES	YES	YES	YES	YES	YES	YES	NO
Parking	YES	NO	YES	YES	YES	YES	YES	YES	YES
Crowd density	YES	NO	YES	YES	YES	YES	YES	YES	NO

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshots Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Queue length	YES	NO	YES	YES	YES	YES	YES	YES	NO
Head counting	YES	NO	YES	YES	YES	YES	YES	YES	NO
Crowd gathering	YES	NO	YES	YES	YES	YES	YES	YES	NO
Electric bike detection	YES	YES	YES	YES	YES	YES	YES	YES	YES
Detection of electric bikes in elevators	YES	YES	YES	YES	YES	YES	YES	YES	YES
Off-duty detection	YES	YES	YES	YES	YES	YES	YES	YES	YES
Target detection	YES	NO	YES	YES	YES	YES	YES	YES	YES
Target recognition	YES	NO	YES	YES	YES	YES	YES	YES	YES
Sound detection	YES	NO	YES	NO	NO	NO	NO	YES	NO
Sudden volume increase	YES	NO	YES	NO	NO	NO	NO	YES	NO

Alarm Name	SDK	ONVIF	RESTful	Video Recording	Snapshots Taking	Email Sending	Alarm Output	Dynamic Frame Rate/Bit Rate	Audio File and White Light Illuminator
Sudden volume decrease	YES	NO	YES	NO	NO	NO	NO	YES	NO
Defocus	YES	NO	YES	YES	YES	YES	YES	YES	YES
Scene change	YES	NO	YES	YES	YES	YES	YES	YES	YES
Image freezing	YES	NO	YES	YES	YES	YES	YES	YES	YES
Gain imbalance	YES	NO	YES	YES	YES	YES	YES	YES	YES
Color cast	YES	NO	YES	YES	YES	YES	YES	YES	YES
Static noise	YES	NO	YES	YES	YES	YES	YES	YES	YES
Stripe noise	YES	NO	YES	YES	YES	YES	YES	YES	YES
Image shaking	YES	NO	YES	YES	YES	YES	YES	YES	YES

4.14.3 Certificate Alarm Configuration

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 Certificate Alarms

Step 1 Log in to the camera web system (at <https://Camera IP address>).

Step 2 Choose **Configuration > Detection > Certificate Alarms**. The **Certificate Alarms** tab page is displayed, as shown in [Figure 4-137](#).

Figure 4-137 Configuring certificate expiration alarms

Certificate expiry notification (days)

7

180

30

day

Certificate type

Step 3 Set **Certificate expiry notification (days)**.

NOTE

When the remaining validity period of the certificate reaches the value specified by **Certificate expiry notification (days)**, the system automatically reports an alarm to users.

Step 4 Click **Save**.

----End

Configuring an Alert Plan

After an alert plan is configured, 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.

Step 1 Click the **Alert Deployment Plan** tab. The **Alert Deployment Plan** tab page is displayed, as shown in [Figure 4-138](#).

Figure 4-138 Alert Deployment Plan area

+ Add

⌵ Delete All

No.	Status	Start time	End time	Date	Mode	Operation
1	☒	00:00:00	24:00:00	Everyday	Weekly	

Save

Step 2 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 4-139](#).

Figure 4-139 Edit Plan dialog box

Edit Plan

Start time

00:00:00

End time

24:00:00

Cyclic mode

Weekly

Select days

☒ All

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

OK

Cancel

Step 3 Set **Start time**, **End time**, **Cyclic mode**, and **Select days**.

Step 4 Click **OK**.

Step 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.

----End

Configuring Alarm Linkage

Step 1 Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in [Figure 4-140](#).

NOTICE

Different camera models support different alarm linkage policies. Some alarm linkage policies can be displayed only after related functions are configured.

Figure 4-140 Configuring alarm linkage

Alarm type

Event

Alarm interval

0

Sec

Alarm Linkage Policy

☒ ONVIF

☒ SDK

☐ RESTful

☐ Email

☐ White light illuminator

☐ Snapshot taking

☐ Video recording

Save

Step 2 Set related parameters. Table 4-84 describes the parameters.

Table 4-84 Alarm linkage 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	Interval at which the camera reports event alarms to the platform.
ONVIF	If ONVIF is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.

Parameter	Description
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 email linkage, see 4.9.1.3 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.
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. The value range may vary depending on the camera model.
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.
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).

Step 3 Click **Save**.

----End

4.14.4 Fault Alarm Configuration

NOTE

Different camera models support different detection functions.

Configuring Fault Alarms

Step 1 Log in to the camera web system (at <https://Camera IP address>).

Step 2 Choose **Configuration** > **Detection** > **Fault Alarms**. The **Fault Alarms** tab page is displayed, as shown in [Figure 4-141](#).

Figure 4-141 Configuring fault alarms

Fault Type

ONVIF IP address lock alarm

Step 3 Set **Fault Type**.

Step 4 Click **Save**.

-----End

Configuring an Alert Plan

After an alert plan is configured, 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.

Step 1 Click the **Alert Deployment Plan** tab. The **Alert Deployment Plan** tab page is displayed, as shown in [Figure 4-142](#).

Figure 4-142 Alert Deployment Plan area

+ Add

⌵ Delete All

No.	Status	Start time	End time	Date	Mode	Operation
1	☒	00:00:00	24:00:00	Everyday	Weekly	

Save

Step 2 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 4-143](#).

Figure 4-143 Edit Plan dialog box

Edit Plan

Start time

00:00:00



End time

24:00:00



Cyclic mode

Weekly



Select days

☒ All

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☒ Saturday

☒ Sunday

OK

Cancel

Step 3 Set **Start time**, **End time**, **Cyclic mode**, and **Select days**.

Step 4 Click **OK**.

Step 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.

----End

Configuring Alarm Linkage

Step 1 Click the **Alarms** tab. The **Alarms** tab page is displayed, as shown in [Figure 4-144](#).

NOTICE

Different camera models support different alarm linkage policies. Some alarm linkage policies can be displayed only after related functions are configured.

Figure 4-144 Configuring alarm linkage

Alarm type

Event

Alarm interval

0

Sec

Alarm Linkage Policy

☒ ONVIF

☒ SDK

☐ RESTful

☐ Email

☐ White light illuminator

☐ Snapshot taking

☐ Video recording

Save

Step 2 Set related parameters. Table 4-85 describes the parameters.

Table 4-85 Alarm linkage 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	Interval at which the camera reports event alarms to the platform.
ONVIF	If ONVIF is selected, the system reports alarms supported by ONVIF through the ONVIF protocol.

Parameter	Description
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 email linkage, see 4.9.1.3 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.
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. The value range may vary depending on the camera model.
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.
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).

Step 3 Click **Save**.

----End

4.15 FAQs

This chapter describes how to locate and troubleshoot common faults.

4.15.1 Login to the Camera Web System

4.15.1.1 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)**.

4.15.1.2 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.

4.15.1.3 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.

4.15.1.4 There Is a Problem with This Website's Security Certificate

Symptom

After the root certificate is downloaded and installed, the browser 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 [4.8.3.3.1 Managing HTTPS Certificates](#). After the certificate is uploaded, restart the browser.

4.15.1.5 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.

4.15.1.6 When a User Uploads the Camera Certificate File and Configuration 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 camera certificate file and configuration 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 camera web system over HTTP using the Firefox 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**.

4.15.1.7 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**.

4.15.1.8 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

Step 1 Click **Download Root Certificate** in the upper right corner of the login page.

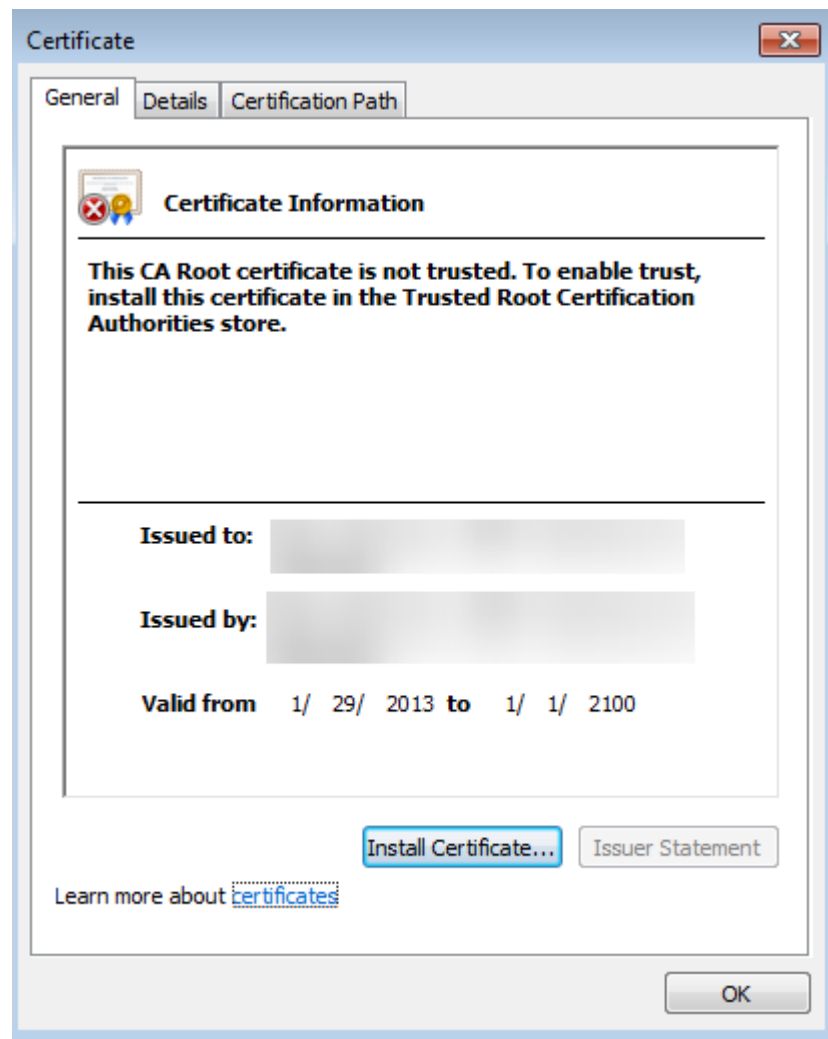
 NOTE

Use the download function of the browser.

Step 2 Double-click the certificate file.

The **Certificate** window is displayed, as shown in [Figure 4-145](#).

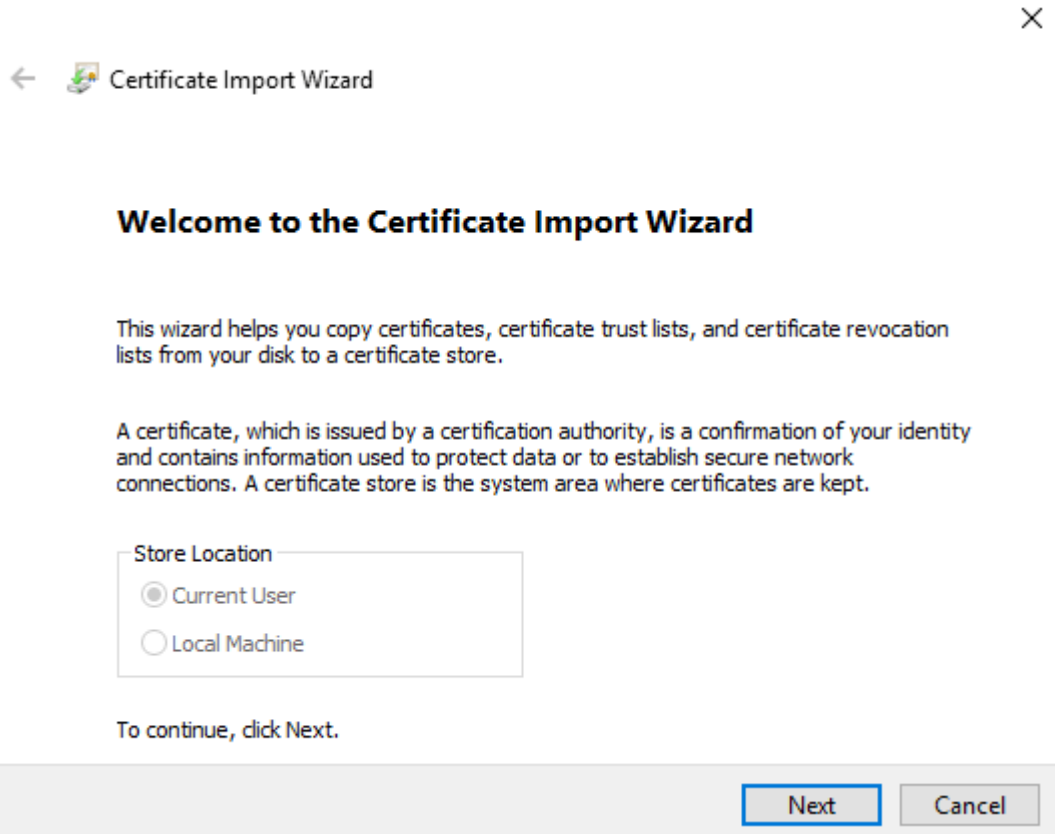
Figure 4-145 Certificate window



Step 3 Click **Install Certificate**.

The **Welcome to the Certificate Import Wizard** window is displayed, as shown in [Figure 4-146](#). Here, Google Chrome is used as an example.

Figure 4-146 Welcome to the Certificate Import Wizard window



Step 4 Click **Next**.

The **Certificate Store** window is displayed, as shown in [Figure 4-147](#).

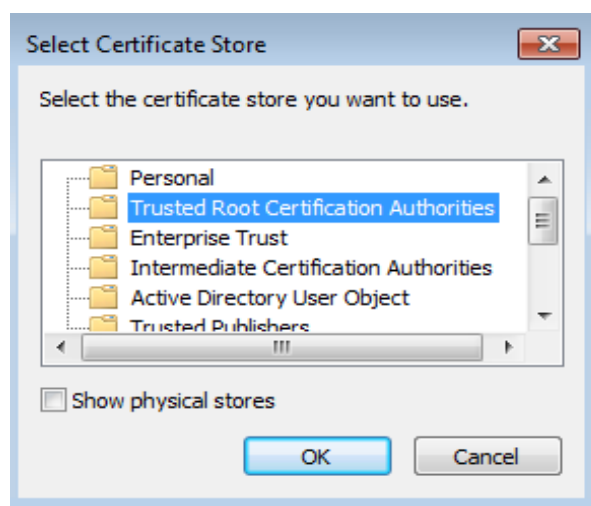
Figure 4-147 Certificate Store window



Step 5 Click **Place all certificates in the following store** and click **Browse**.

The **Select Certificate Store** dialog box is displayed, as shown in [Figure 4-148](#).

Figure 4-148 Select Certificate Store dialog box



Step 6 Select **Trusted Root Certification Authorities** and click **OK**.

The selected certificate store is displayed in the **Certificate Import Wizard** window.

Step 7 Click **Next** and install the root certificate as prompted.

Step 8 After the root certificate is installed, restart the browser and enter the IP address of the camera in the address box. The login page is then displayed.

----End

4.15.2 Live Video Viewing

4.15.2.1 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.

4.15.2.2 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 browser icon and choose **Run as administrator** from the shortcut menu.

4.15.2.3 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

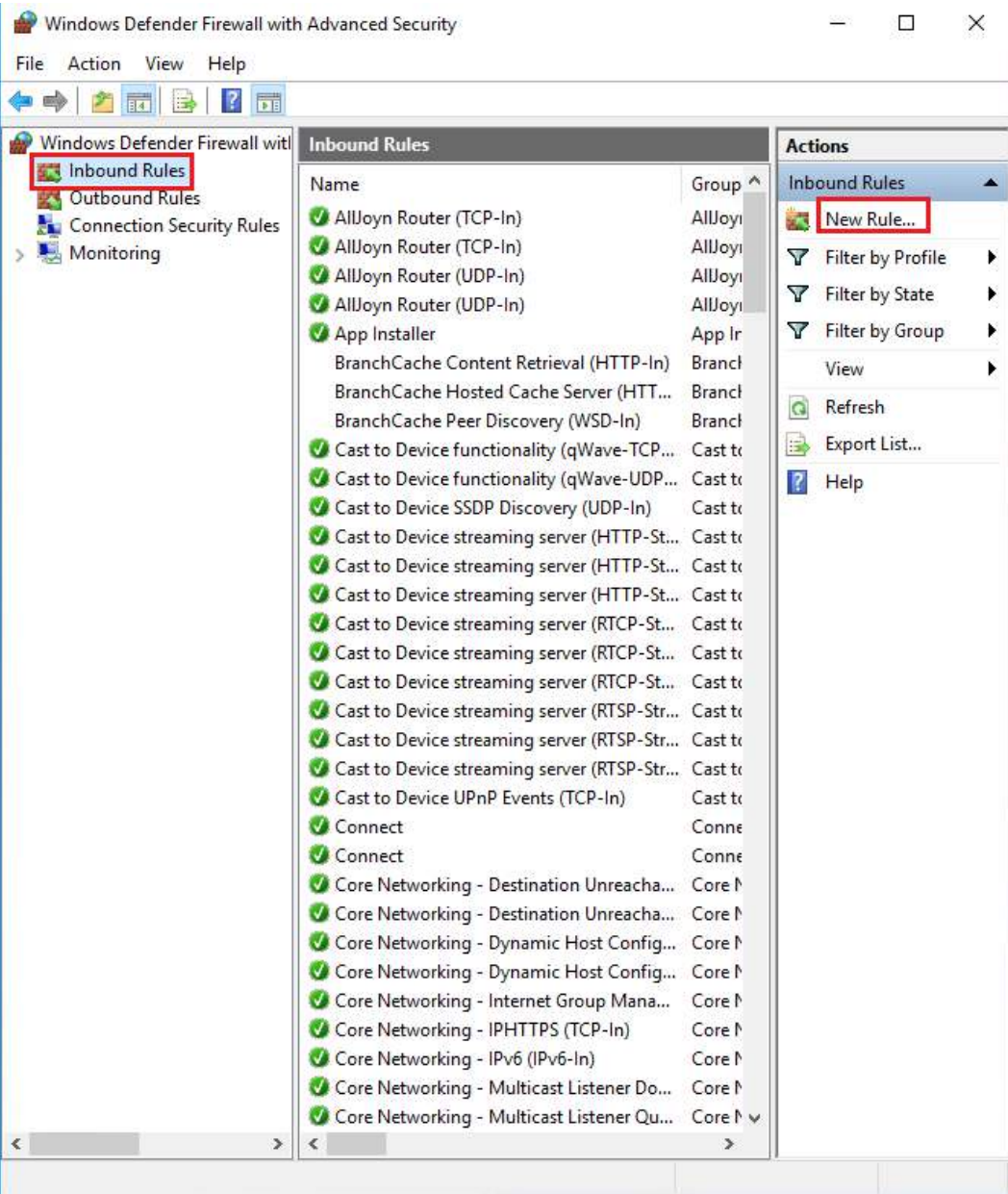
The UDP port is disabled on the firewall of the Windows operating system. As a result, video streams cannot be transmitted. You need to enable the port.

Solution

The following uses Windows 10 as an example. The procedure for other versions of Windows operating systems is similar.

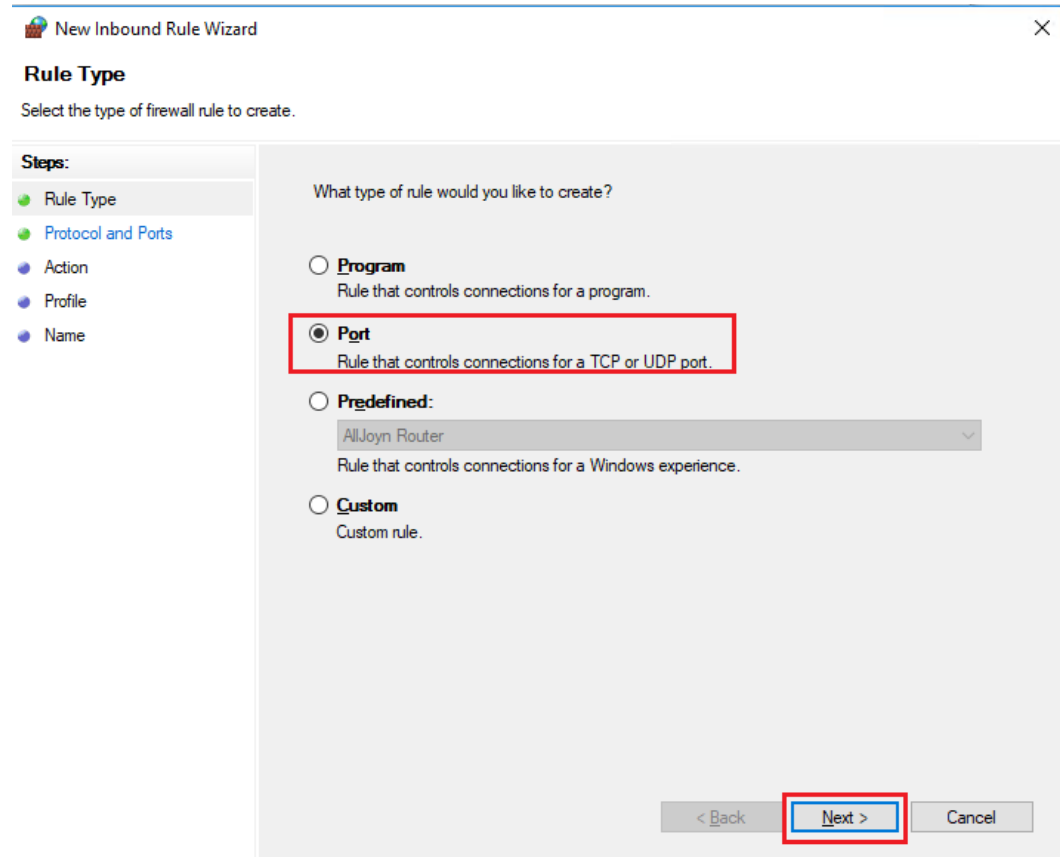
- Step 1
- Choose **Start > Control Panel > Windows Defender Firewall > Advanced settings**.
- Step 2
- In the **Windows Defender Firewall with Advanced Security** dialog box, click **Inbound Rules** and then click **New Rule**, as shown in [Figure 4-149](#).

Figure 4-149 Windows Defender Firewall with Advanced Security dialog box



Step 3 In the **New Inbound Rule Wizard** dialog box, click **Port** and then **Next**, as shown in [Figure 4-150](#).

Figure 4-150 New Inbound Rule Wizard dialog box



Step 4 In the **New Inbound Rule Wizard** dialog box, click **UDP** and **All local ports**, as shown in [Figure 4-151](#).

If you know the local port, you can also click **Specific local ports** and enter the port number.

Figure 4-151 New Inbound Rule Wizard dialog box

Step 5 Click **Next** until the page for setting the name is displayed. Enter a name and click **Finish**.

-----End

4.15.2.4 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.

4.15.2.5 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.

4.15.2.6 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.

4.15.2.7 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.

4.15.2.8 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**.

4.15.2.9 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.

4.15.2.10 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.

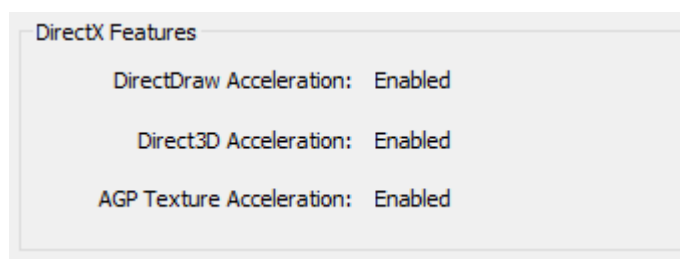
Solution

- 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:

Step 1 Press **Windows+R**, enter **dxdiag**, and click **OK**.

Step 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 4-152](#).

Figure 4-152 DirectX Diagnostic Tool window



----End

4.15.2.11 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.

4.15.2.12 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.

4.15.2.13 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.

4.15.2.14 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

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 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**.

----End

4.15.2.15 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?

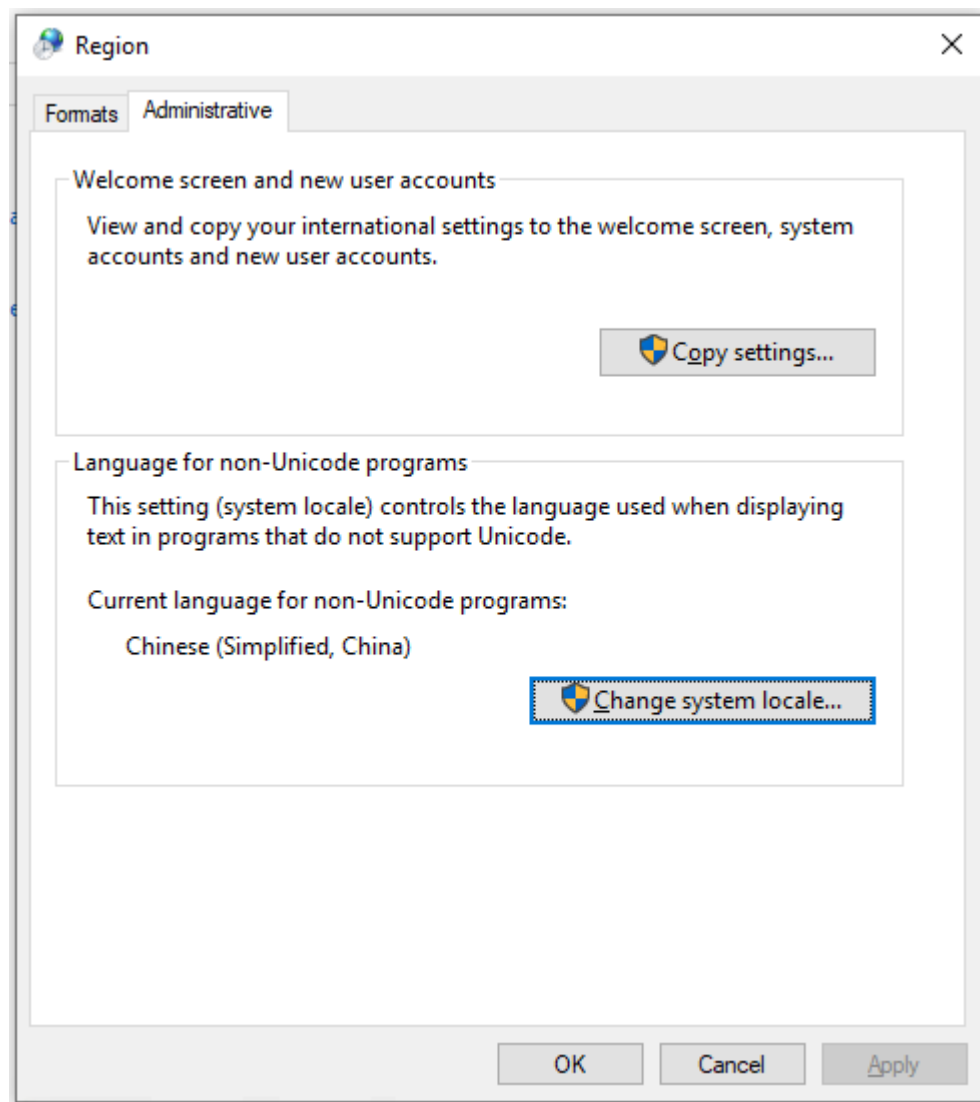
Possible Cause

The operating system setting is incorrect.

Solution

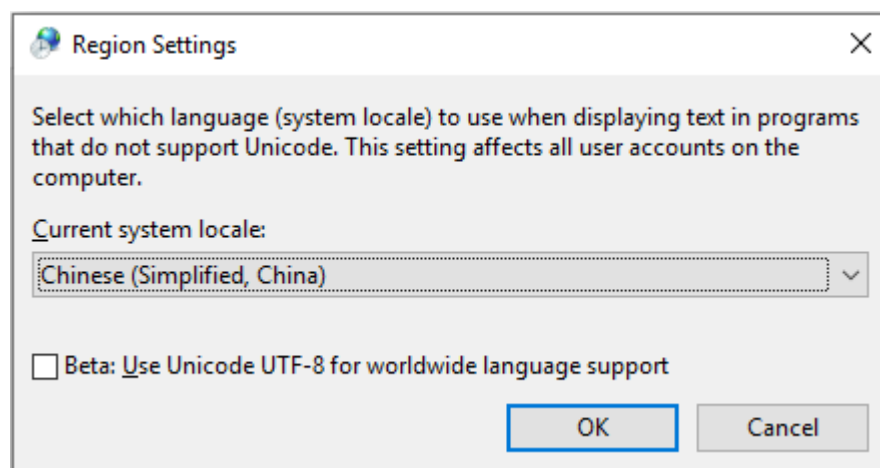
- Step 1** Choose **Start > Settings**.
- Step 2** Click **Time & Language** and then **Region**.
- Step 3** Click **Additional date, time & regional settings** at the bottom of the page.
- Step 4** Click **Change date, time, or number formats** in the **Region** area.
- Step 5** Click the **Administrative** tab. On the tab page that is displayed, click **Change system locale**.

Figure 4-153 Changing the system locale



- Step 6** Set **Current system locale** to **Chinese(Simplified, China)**. Deselect **Beta: Use Unicode UTF-8 for worldwide language support**.

Figure 4-154 Setting the current system locale



Step 7 Click **OK**.

----End

4.15.2.16 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.

4.15.3 Recording and Snapshot

4.15.3.1 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.

Possible Causes

- You log in to the operating system Windows 7, 8, or 10 and the browser as a user other than **admin**, and set the storage path 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.

- You log in to the computer as a user other than **admin**. Then you cannot view snapshots and recordings under the storage path specified by the **admin** user.

Solution

- Right-click the browser icon and choose **Run as administrator** from the shortcut menu.
- Log in to the computer as an administrator.

4.15.3.2 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.

4.15.4 Device Maintenance

4.15.4.1 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 fails to be upgraded, and the intelligent function is invalid.	Close the browser during the upgrade.	Perform the upgrade again.

Symptom	Possible Cause	Solution
After the upgrade software package is selected, the upgrade package path is still empty or contains garbled characters.	The upgrade package path may contain languages that are not supported by the current system.	Change the upgrade package path to an English one.

4.15.4.2 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.

4.15.4.3 Logs Fail To Be Downloaded After a User Clicks One-Click Collection on the Web Client

Symptom

After logging in to the camera web system, a user clicks **One-Click Collection** under **Configuration > System > System Maintenance > Log**. Logs, however, fail to be downloaded.

Solution

Restart the computer, and re-log in to the camera web system.

4.15.4.4 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

Step 1 In the upper right corner of the browser, click  to minimize the window.

Step 2 After the window is minimized, click  in the upper right corner of the browser to maximize the browser.

----End

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.

4.15.5 Others

4.15.5.1 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 browser icon and choose **Run as administrator** from the shortcut menu.

4.15.5.2 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.

4.15.5.3 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.

4.15.5.4 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 [4.9.2.1.2 Configuring Connection to the Platform Through RTSP](#).

Solution

1. Log in to the camera web system.
2. Choose **Configuration > Network > Platform Connection > General Protocol > 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 4-86](#) lists the URL for requesting streams through RTSP.

Table 4-86 Requesting streams through RTSP in the case of no authentication

Request Content	Stream Request URL
Live video stream	rtsp:// <i>IP address</i> : <i>RTSP port number</i> /LiveMedia/ch1/Media1/trackID=1
Metadata	rtsp:// <i>IP address</i> : <i>RTSP port number</i> /LiveMedia/ch1/Media1/trackID=4
Live video stream + metadata	rtsp:// <i>IP address</i> : <i>RTSP port number</i> /LiveMedia/ch1/Media1

In the preceding URLs, ***IP address*** indicates the camera IP address, ***RTSP port number*** is the same as the value of **Port** set under **Configuration > Network**

> **Platform Connection** > **General Protocol** > **RTSP** in the camera web system, and **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 4-87](#) lists the URL for requesting streams through RTSP.

Table 4-87 Requesting streams through RTSP in the case of authentication

Request Content	Stream Request URL
Live video stream	<i>rtsp://User name:Password@IP address.RTSP port number/LiveMedia/ch1/Media1/trackID=1</i>
Metadata	<i>rtsp://User name:Password@IP address.RTSP port number/LiveMedia/ch1/Media1/trackID=4</i>
Live video stream + metadata	<i>rtsp://User name:Password@IP address.RTSP port number/LiveMedia/ch1/Media1</i>

The default user name is **admin**.

To set the authentication password, choose **Configuration** > **Network** > **Platform Connection** > **Protocol Connection Password** > **ONVIF Password**.

4.15.5.5 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.

4.15.5.6 How Do I Obtain and Use the Milestone 2022 R3 Plug-in?

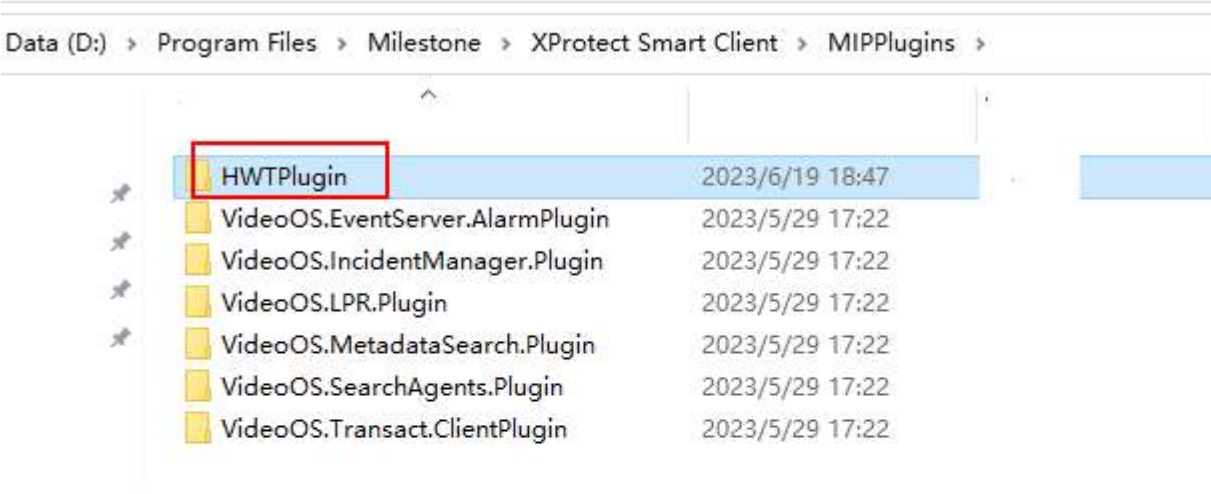
Context

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

- Step 1** Log in to the [HOLOWITS technical support website](#), search for the Milestone plug-in, and obtain the plug-in package.
- Step 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 4-155](#).

Figure 4-155 Decompressing the plug-in package in the Milestone path



4.16 FAQs

This chapter describes how to locate and troubleshoot common faults.

4.16.1 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.

4.16.2 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.

4.16.3 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.

4.17 Configuring Image Optimization

4.17.1 Factors and Functions Related to Image Quality

This chapter describes the factors and functions that affect the image quality.

4.17.1.1 Lens

The lens is a decisive factor in determining image quality.

4.17.1.1.1 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 4-88](#) lists the mapping among the focal length, detection distance, and field of view.

Table 4-88 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 4-156 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](#).

4.17.1.1.2 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 4-157](#). 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 4-157 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.

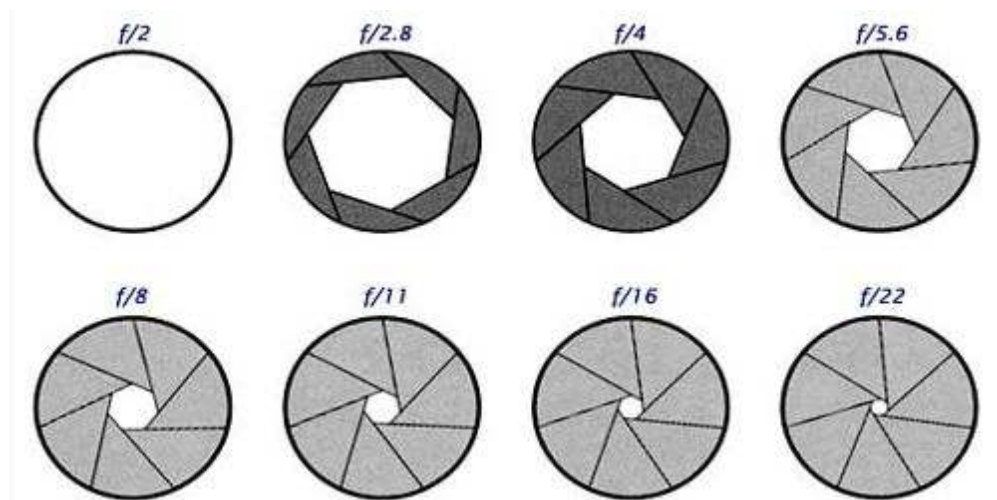
For details about how to adjust the focus position, see [Adjusting the Focal Length and Focus Position](#).

4.17.1.1.3 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 4-158](#), 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 4-158 Common apertures



As shown in [Figure 4-159](#), 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 4-159 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.

4.17.1.1.4 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 4-160](#) and [Figure 4-161](#) show the imaging effects of different shutter speeds.

Figure 4-160 Fast shutter speed



Figure 4-161 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.

4.17.1.1.5 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 4-162**. The mount

type is usually marked on the lens nameplate or packaging. Generally, the C mount is longer.

Figure 4-162 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 4-163](#). Otherwise, the imaging effect will be severely affected.

Figure 4-163 C/CS adapter ring



4.17.1.2 Backlight Compensation

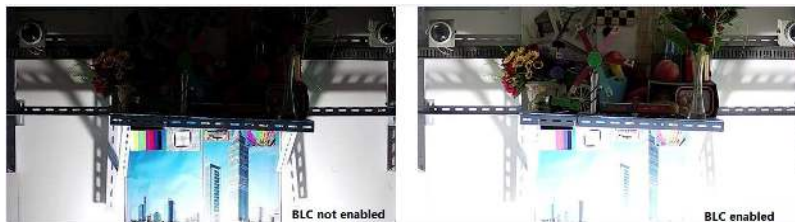
In a scene that is unevenly illuminated, the object may appear against a bright background or a light source may exist behind the object. In this case, to the camera the incoming light is bright, so the camera will reduce its exposure (for example, by increasing the shutter speed). However, this reduces 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 4-164](#) shows the imaging of a scene before and after BLC is enabled.

Figure 4-164 BLC effect

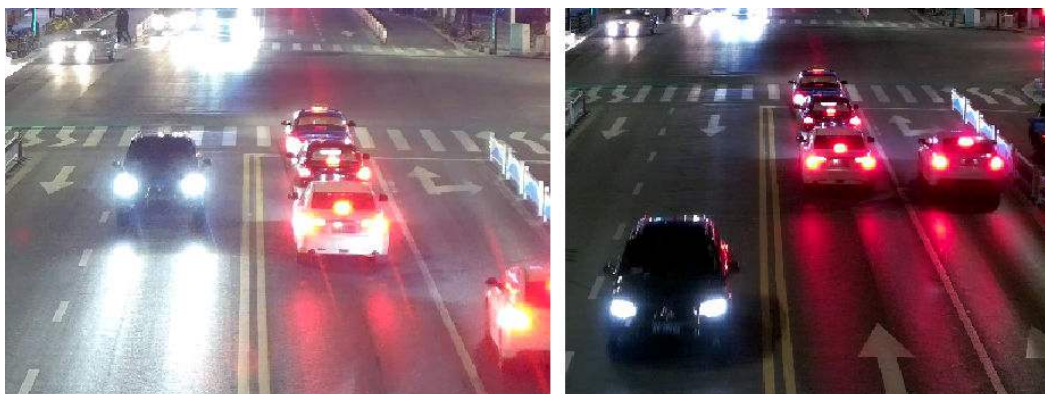


4.17.1.3 Highlight Compensation

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 4-165](#).

Figure 4-165 HLC effect



4.17.1.4 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 4-166](#) shows a typical scenario with no compensation of any kind. The background is bright, resulting in unclear imaging of people in the foreground. [Figure 4-167](#) shows the imaging effect when BLC is enabled. People in the dark area are clear, but the background is washed out.

Figure 4-166 No compensation



Figure 4-167 BLC enabled



If WDR is enabled, the camera takes a picture shown in [Figure 4-168](#) with a fast shutter speed, followed by a picture shown in [Figure 4-169](#) with a slow shutter speed. They work together and provide a balanced image, as shown in [Figure 4-170](#).

Figure 4-168 High-speed capture



Figure 4-169 Low-speed capture



Figure 4-170 Final effect



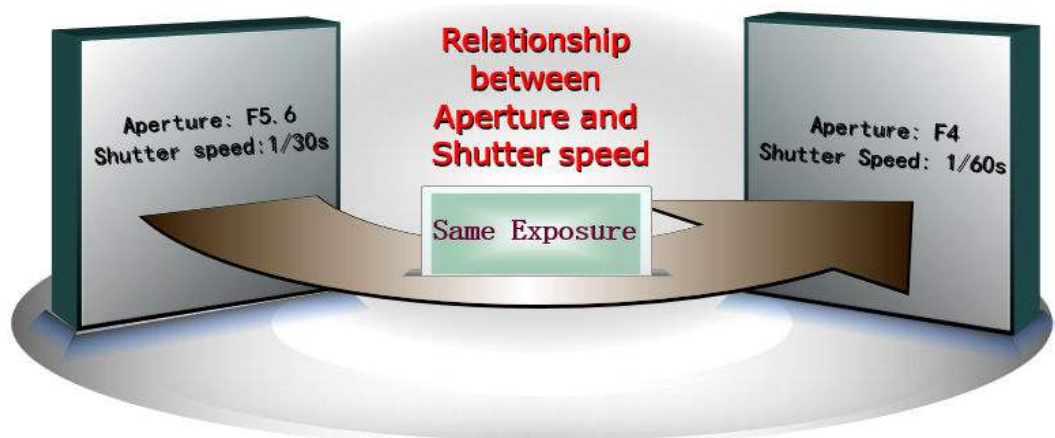
4.17.1.5 Function Dependencies and Differences

4.17.1.5.1 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 4-171](#).

Figure 4-171 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 4-172](#).

Figure 4-172 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.

4.17.1.5.2 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 4-89 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.

Item	BLC	HLC	WDR
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.

4.17.2 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.

4.17.2.1 Image Clarity Issues

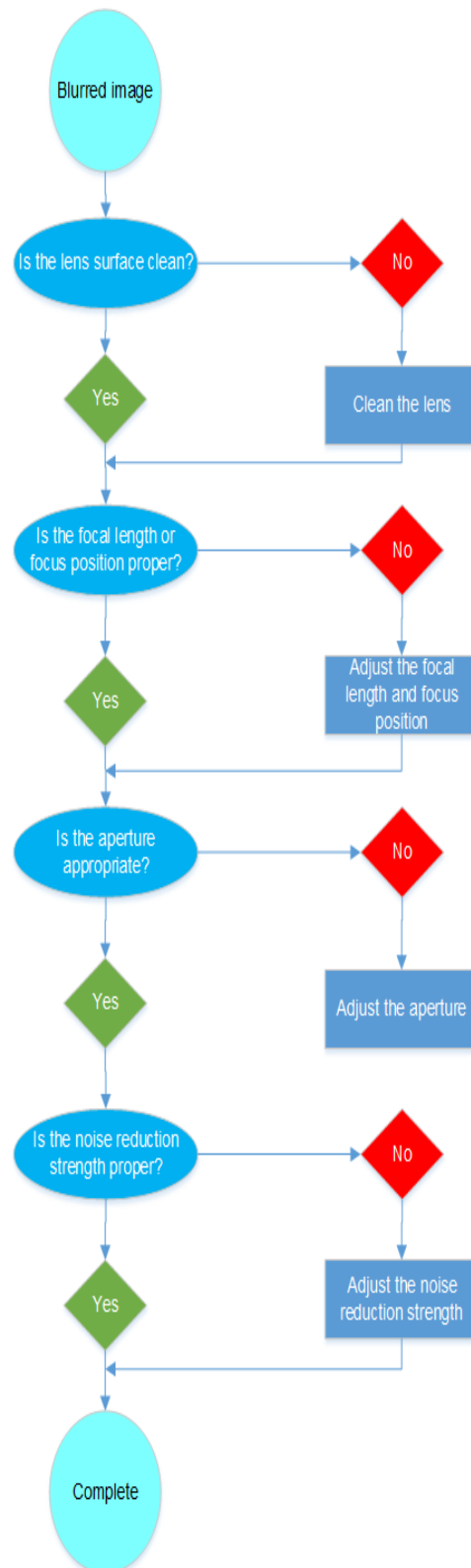
4.17.2.1.1 Image Blur

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 4-173 illustrates the troubleshooting process.

Figure 4-173 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:
 - a. 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.
 - b. 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 4-174 shows the lens elements.

Figure 4-174 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.

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 4-175](#), the image appears blurry due to a small aperture. After the aperture is enlarged, the obtained image is much sharper, as shown in [Figure 4-176](#).

Figure 4-175 Image obtained with a small aperture



Figure 4-176 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.

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 4-177](#).

Figure 4-177 Aperture ring



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 4-178](#) and [Figure 4-179](#), the edge details appear more blurry after the spatial NR is strengthened.

Figure 4-178 Original image

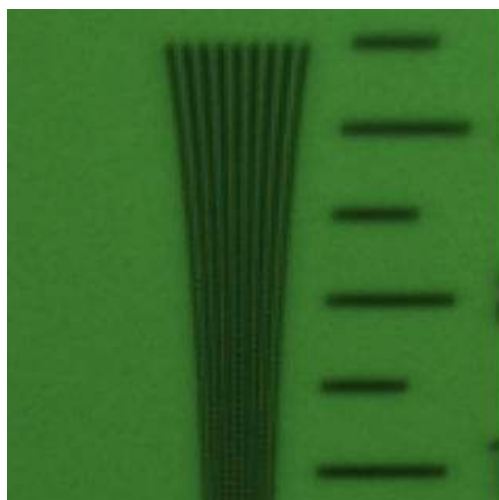
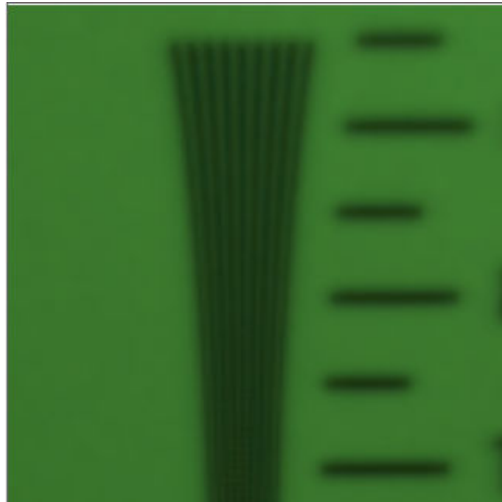


Figure 4-179 Image affect after spatial NR strengthening



- 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 4-180](#). However, for static objects, the effect of the temporal NR on the sharpness is small.

Figure 4-180 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.

4.17.2.1.2 Low Contrast

An image with low contrast usually appears flat or dull, as is the left picture in [Figure 4-181](#). This is caused by narrow dynamic range in the image and can be improved by adjusting the brightness and contrast.

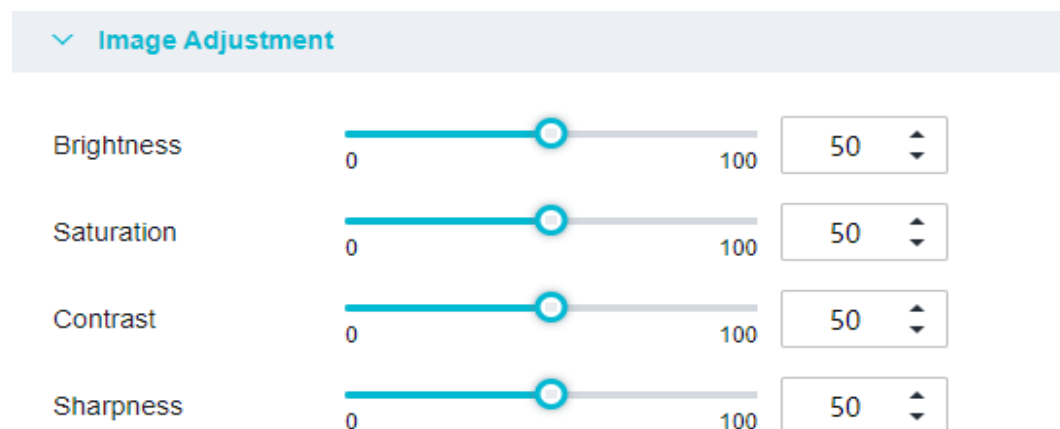
Troubleshooting Suggestions

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 4-181](#), the image is improved after the adjustment.

Figure 4-181 Adjusting brightness and contrast



4.17.2.2 Image Brightness Issues

If the image appears too bright or dark, like the example in [Figure 4-182](#), the exposure may be improper or the default settings may not be suited to the detection scene.

Figure 4-182 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 in the following way: Log in to the camera web page and choose **Configuration > Image > Display > Exposure**. Adjust the value of **Exposure compensation coefficient**, as shown in [Figure 4-183](#), until the image brightness is moderate.

Figure 4-183 Setting exposure compensation parameters

Exposure

Exposure mode: Auto

Shutter limit: Customization

Exposure compensation...: 0 to 100, 50

Gain limit: 0 to 100, 100

us

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 4-184](#), until the imaging effect meets your requirements.

Figure 4-184 Adjusting brightness and contrast

Image Adjustment

Brightness		0	100	50	↕
Saturation		0	100	50	↕
Contrast		0	100	50	↕
Sharpness		0	100	50	↕

4.17.2.3 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 4-185](#).

Figure 4-185 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 in the following way: 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 Tendency** and **Blue Tendency** if required, as shown in [Figure 4-186](#). 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 White Balance**.

Figure 4-186 Auto white balance parameters

White Balance

Mode

Auto White Balance

Red Tendency

0

100

50

Blue Tendency

0

100

50

Regional 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 value of **Saturation**, as shown in [Figure 4-187](#), until the image effect meets your requirements.

Figure 4-187 Setting image adjustment parameters

Image Adjustment

Brightness

0

100

50

Saturation

0

100

50

Contrast

0

100

50

Sharpness

0

100

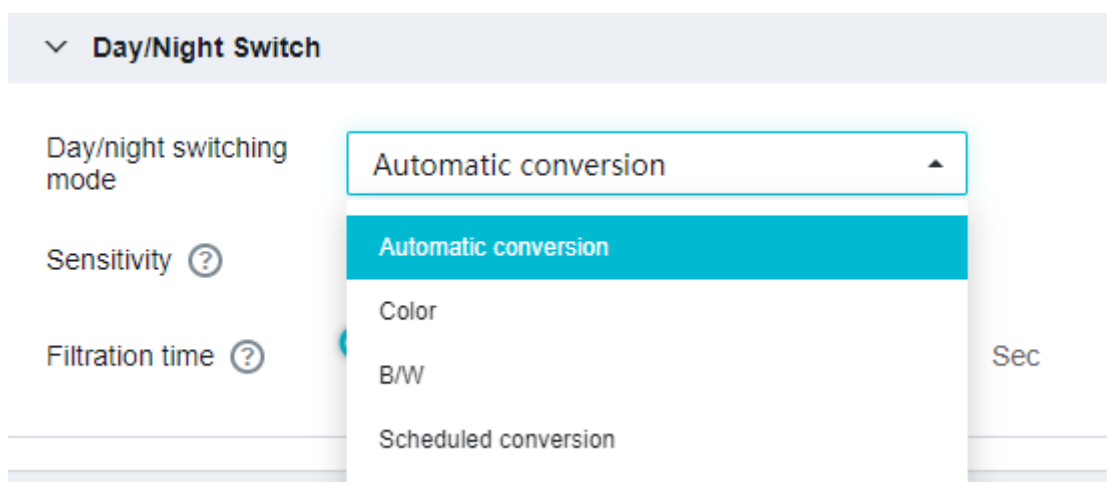
50

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 4-188](#), set **Day/night switching mode** to **Color**.

Figure 4-188 Changing the day/night switch mode



If the problem persists, contact the supplier or technical support engineers.

4.17.2.4 Image Noise Issues

If the image is noisy, as shown in [Figure 4-189](#), details may be obscured and the image may be unclear.

Figure 4-189 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.

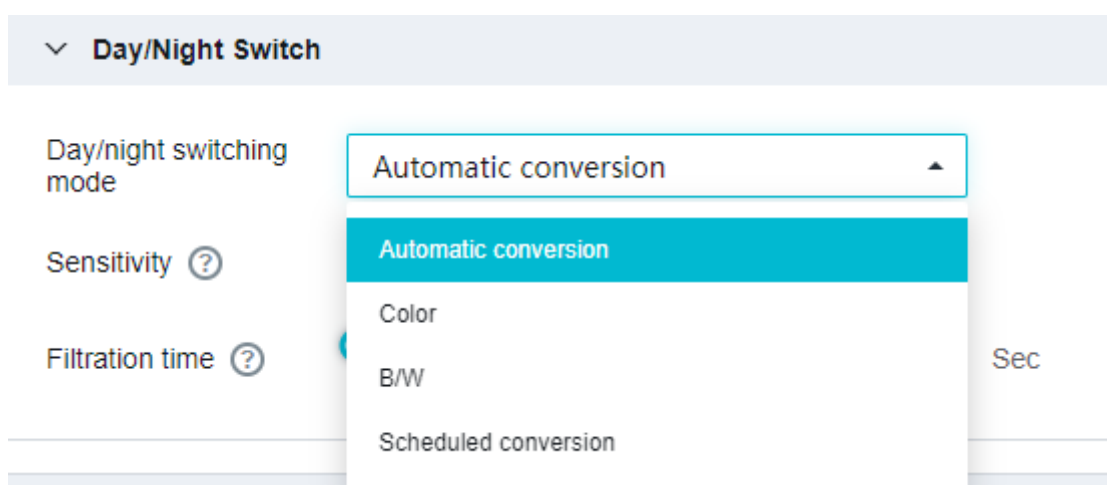
Troubleshooting Suggestions

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 in the following way: Log in to the camera web system, choose **Configuration > Image > Display > Day/Night Switch**, and set **Day/night switching mode** to **Color**, as shown in [Figure 4-190](#).

Figure 4-190 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 4-191](#).

Figure 4-191 Adjusting the noise reduction coefficient

Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

Defogging

Overcast adaptation

Anti-light flicker

Disable

Denoising

Expert mode

Spatial denoising level

0100

50

Temporal denoising level

0100

50

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 slightly decrease image brightness. If **Exposure mode** is set to **Manual**, slightly decrease the value of **Gain**. Generally, the automatic exposure mode is recommended.

Figure 4-192 Setting exposure parameters

Exposure

Exposure mode

Manual

Shutter speed

1/25 s

Gain

0100

0

In the daytime, skip step 1.

After proper adjustment, the image effect will improve, as shown in [Figure 4-193](#). Noise is reduced and patterns are smoother.

Figure 4-193 Noise reduction effect

Before adjustment:



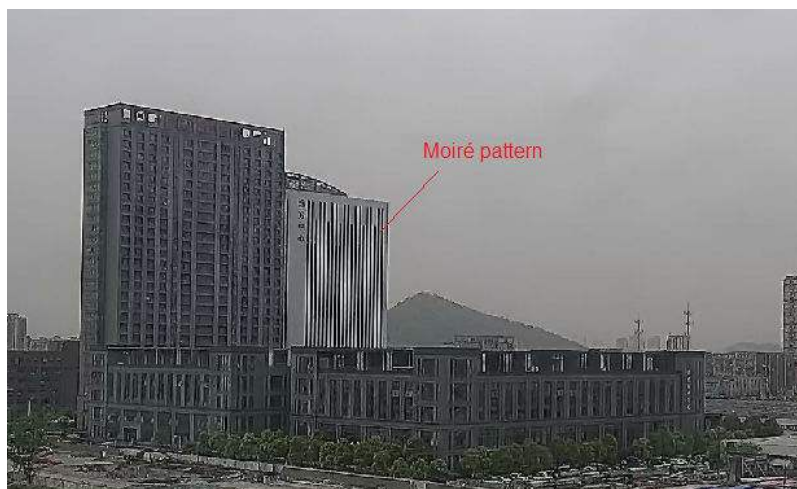
After adjustment:



4.17.2.5 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 4-194](#) shows an example.

Figure 4-194 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 4-195](#). This function can reduce the moire pattern interference.

Figure 4-195 Enabling the function of removing moire pattern

Playing Settings

Rendering mode ?	☐ DDraw	☒ D3D	☐ Remove moire pattern
Code stream type	☒ Primary Stream	☐ Secondary Stream 1	
Video stream type ?	☐ Video stream	☐ Hybrid stream	
Protocol	☐ TCP	☒ UDP	
Live view performance	☒ Short delay ☐ Fluent		1
Other Functions	☒ Media stream encryption ?		

 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 in the following way: Choose **Configuration > Image > Display > Image Adjustment**, and decrease the value of **Sharpness**, as shown in [Figure 4-196](#). 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 4-196 Setting image adjustment parameters



- Enlarge the aperture if it is adjustable. For a manual iris lens, rotate the aperture ring to increase the aperture.

[Figure 4-197](#) shows the ideal effect after the adjustment.

Figure 4-197 Effect after adjustment



4.17.2.6 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 4-198](#).

Figure 4-198 Purple fringing



Troubleshooting Suggestions (for Small Bullet Cameras)

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration** > **Image** > **Display**, click **Exposure**, and set **Exposure mode** to **Auto**.
- Step 3** Set **Exposure compensation coefficient** to **30** and check the image effect.
- Step 4** (Optional) If purple fringing still exists, perform the following operations:
 - 1. Choose **Configuration** > **Intelligence**. Toggle on **Target Capture** in the **Target Intelligence** area.
 - 2. Click **Settings** next to **Target Capture**. The **Target Capture** page is displayed.
 - 3. Choose **Area Settings** > **Advanced Parameters** and select **Brightness compensation**.
 - 4. Set **Compensation level** to **30**.
 - 5. Click **Save** and check the target capture effect on the video image.

----End

[Figure 4-199](#) shows the capture effects before and after troubleshooting.

Figure 4-199 Capture effects before and after troubleshooting



4.17.2.7 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 4-200](#).

Figure 4-200 Infrared glare



In this case, you can log in to the camera web system, choose **Configuration > Image > Display > Image Enhancement**, and adjust the value of **IR overexposure compensation**, as shown in [Figure 4-201](#).

Figure 4-201 Image enhancement parameters in manual mode

▼ Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

Defogging

Manual

Defogging level

0100

50

Anti-light flicker

Disable

Denoising

Automatic noise reduction

IR overexposure compensation

0100

50

In addition, you can choose **Configuration > Image > Display > Illuminator Control**, set **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 -20°C 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 4-202](#).

Figure 4-202 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 4-203](#).

Figure 4-203 After angle and position adjustment



4.17.2.8 Wave Pattern Issues

Particularly in indoor scenarios, electromagnetic interference near the camera can cause wave-like patterns to appear in images.

Possible causes:

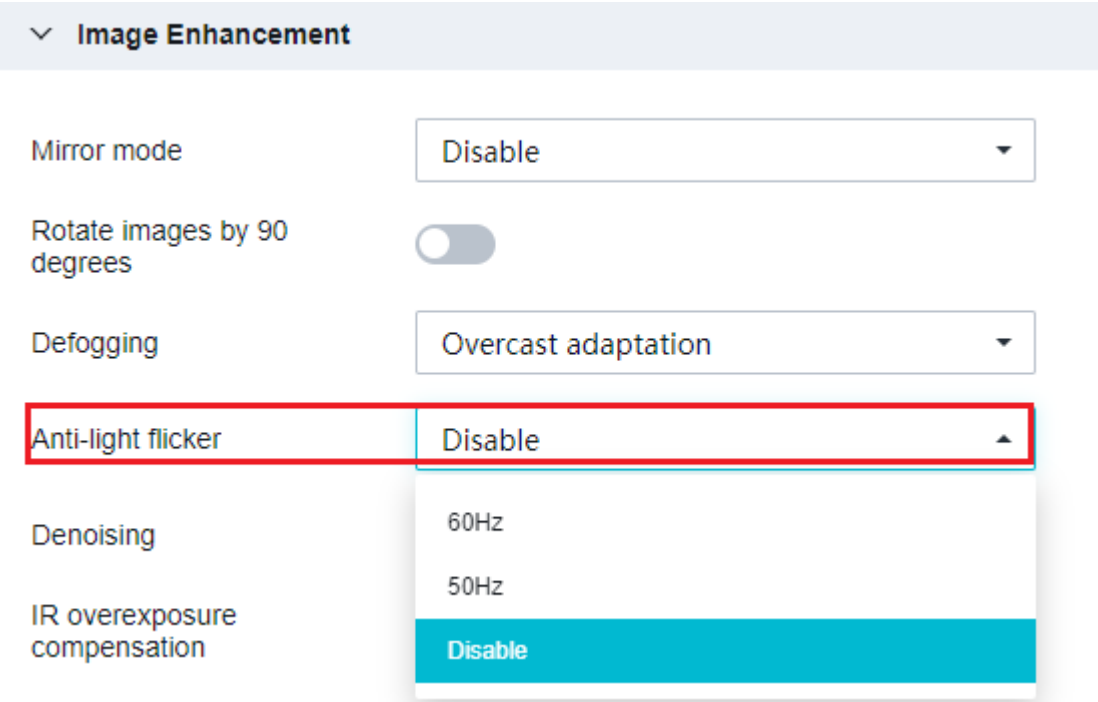
- There is electromagnetic interference nearby.
- The power supply does not match the camera specification.
- The camera is not properly grounded.
- The indoor fluorescent lamp frequency does not match the camera background frequency.

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. The detailed procedure is as follows: Choose **Configuration > Image > Display > Image Enhancement** and set **Anti-light flicker** to match the frequency of the light source, as shown in [Figure 4-204](#). Alternatively, adjust the angle of the camera to avoid displaying the light source in the image.

Figure 4-204 Changing background frequency



4.17.2.9 Motion Blur Issues

Symptom

A moving object in the snapshot is blurry.

Figure 4-205 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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > Image > Display > Exposure**.

Step 3 Adjust the value of **Shutter limit (s)**.

The recommended value is **1/100** for pedestrian detection and **1/250** for vehicle detection. [Table 4-90](#) lists the recommended shutter speeds for various moving speeds.

Table 4-90 Recommended shutter speeds for different moving speeds

Moving Speed (km/h)	Shutter Speed (s)
40	1/150
60	1/180
80	1/250
100	1/350
120	1/450

 **NOTE**

----End

4.17.2.10 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

- Step 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 [Step 2](#).
- Step 2** Perform the troubleshooting steps under **Configuration > Image > Display > Image Enhancement**:
1. Adjust the camera angle or move the reflective object to reduce light reflection.
 2. Lower the intelligent infrared level.
 3. Enable backlight compensation (not recommended).
 4. Lower the infrared illuminator intensity (not recommended).
- End

4.17.2.11 Power Frequency Flicker Issues

Symptom

Static or scrolling stripes appear on the image.

Figure 4-206 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 **Anti-light flicker** based on the power frequency under **Configuration > Image > Display > Image Enhancement**.

Figure 4-207 Setting Anti-light flicker

Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

Defogging

Overcast adaptation

Anti-light flicker

Disable

Denoising

60Hz

IR overexposure compensation

50Hz

Disable

4.17.2.12 Ghosting and Lens Flare Issues

Symptom

An abnormal light spot or beam appears in the image.

Figure 4-208 Ghosting and lens flares



Possible Causes

Light is reflected back and forth inside the lens, causing lens flares.

Troubleshooting Suggestions

- Step 1** Adjust the camera direction until it does not face the light source directly.
- Step 2** Block unwanted light by using devices such as a lens hood on the camera lens.
- Step 3** Block unwanted light emitting from the light source.
- Step 4** Remove dirt from the lens and housing.

----End

4.17.2.13 Severe Halation Issues at Night

Symptom

Halation is severe at night.

Figure 4-209 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

- Step 1** Choose **Configuration > Image > Display > Backlight**, enable highlight compensation, and check the image. If the problem persists, go to [Step 2](#).

- Step 2** Choose **Configuration > Image > Display > Exposure**, lower the gain limit, and check the image. If the problem persists, go to [Step 3](#).
- Step 3** Adjust the camera angle to avoid contact with strong light sources and check the image. If the problem persists, go to [Step 4](#).
- Step 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.
- End

4.17.2.14 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.
 - a. Adjust the camera angle to avoid contact with the light source.
 - b. Increase the exposure compensation coefficient under **Configuration > Image > Display > Exposure**.
- 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**.

4.17.2.15 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

- Step 1** Lower the infrared illuminator intensity under **Configuration > Image > Display > Illuminator Control** (not recommended).
- Step 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.
1. Choose **Configuration > Image > Display > Image Enhancement**.
 2. Set **Denoising** to **Expert mode**.
 3. Lower the temporal noise reduction level.

----End

4.17.2.16 Blurred Infrared Image from a Fixed Dome Camera or Bullet Camera

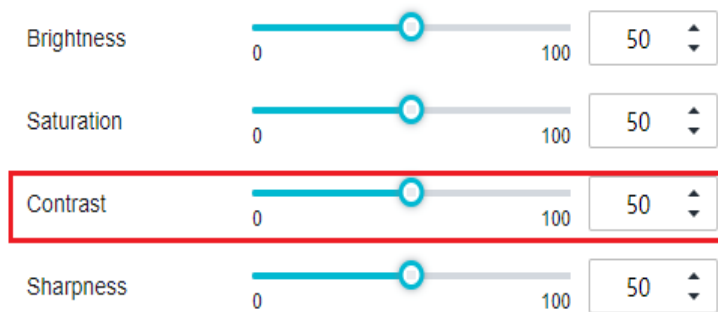
Symptom

The infrared image is blurred when you zoom in on an object using a non-PTZ dome camera.

Troubleshooting Suggestions

- Step 1** Check whether the image setting has been modified, such as the contrast setting. You can adjust the contrast under **Configuration > Image > Display > Image Adjustment** to improve the image clarity.

Figure 4-210 Adjusting the contrast



Step 2 Adjust the position of the camera to prevent nearby obstacles such as leaves from causing light reflection.

Step 3 Check whether the lens protective film has been removed. If not, remove it.

Step 4 Check whether any components are damaged. If so, replace the damaged components.

----End

4.17.2.17 Part of the Image is Blurry

Symptom

Only part of the image is clear. For example, in [Figure 4-211](#), the upper part of the image is blurry.

Figure 4-211 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.

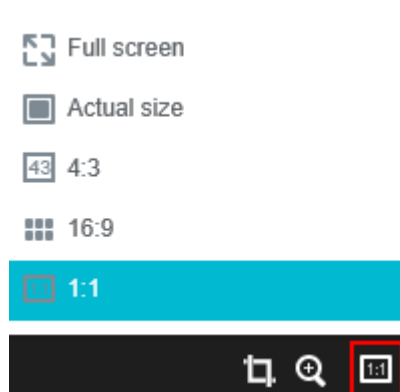
NOTE

Some camera models do not support the focus function.

Adjusting the focus

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > Image > Display > Focus** and set **Focus mode** to **Manual**.
- Step 3** Choose **View**. On the **View** tab page that is displayed, click **Aspect Ratio** and choose **1:1**, as shown in [Figure 4-212](#).

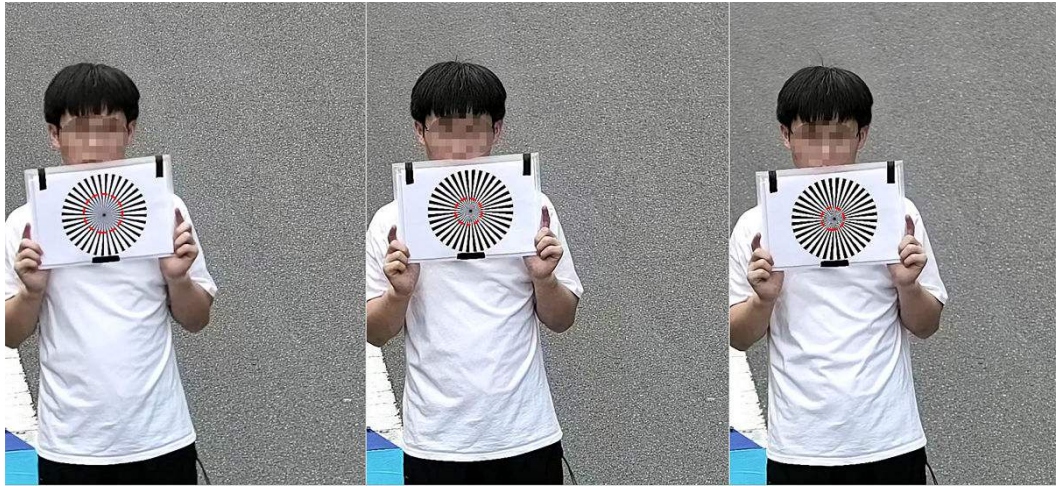
Figure 4-212 Aspect Ratio options



- Step 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 4-213](#), sharper lines in the Siemens star chart indicate better focus and clearer image quality.

Figure 4-213 Focus process



In most cases, a camera takes snapshots of objects in the center (as shown in [Figure 4-214](#)) and lower parts (as shown in [Figure 4-215](#)) 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 4-214 Middle part of the image



Figure 4-215 Lower part of the image



Step 5 After the image is in clear focus, click **Aspect Ratio** and choose **Actual size**.

----End

Drawing a detection area

Step 1 Choose **Configuration > Intelligence** and enable an intelligent analysis task. The configuration page is displayed.

Step 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.

----End

4.17.2.18 Dark Image in Backlit Areas

Symptom

The object is dark in the backlight area.

Possible Causes

The dynamic range in the environment is large.

Troubleshooting Suggestions

Step 1 Choose **Configuration > Intelligence** and select an intelligent analysis task. On the settings page, enable **Brightness compensation** for targets or license plates.

Figure 4-216 shows how to enable **Brightness compensation** for targets.

Figure 4-216 Enabling brightness compensation

▼ Advanced Parameters

☐ Enable target enhancement

☐ Send target cutout

1

3

1

↕

↕

(Piece)

☐ Send person cutout

1

3

1

↕

↕

(Piece)

Target snapshot quality

10

5

↕

↕

Person snapshot quality

10

5

↕

↕

☐ Send full image

i

Full image quality

10

5

↕

↕

Brightness compensation

Enable

▼

Compensation level

100

1

↕

↕

Target exposure duration (min)

60

1

↕

↕

Step 2 Choose **Configuration > Image > Display > Backlight**, and set **WDR/HLC/BLC** to **Backlight adaptation** or **Wide dynamic range**.

- Select **Backlight adaptation** (recommended).
- Select **Wide dynamic range** and adjust the WDR strength.

----End

4.17.3 Common Scenarios

The focus of image optimization varies based on the requirements of individual deployment.

4.17.3.1 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

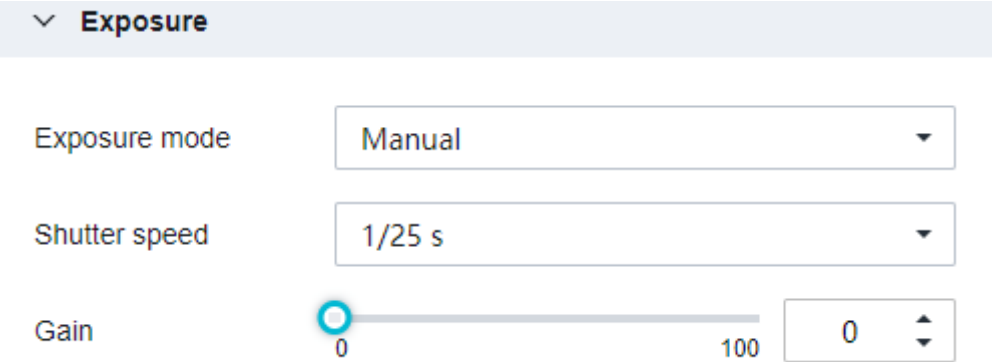
1. Sensor
- Generally, a larger sensor or a larger photosensitive area indicates better low illumination performance. The sensor size determines the low illumination performance of a camera.
2. Lens and aperture
- The lens and aperture size determine the amount of light entering the camera. In dimly 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 limit** to slow down the shutter speed and increase the exposure time, as shown in [Figure 4-217](#). The more light enters the camera, the sharper the resultant image is.

Figure 4-217 Setting exposure parameters



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 4-218 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 4-218 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 4-219**. At the same time, observe the noise levels on the image and set noise reduction accordingly.

Figure 4-219 Setting exposure parameters

▼ **Exposure**

Exposure mode Manual ▼

Shutter speed 1/25 s ▼

Gain
0

0 ▲▼

3. Adjust the saturation and sharpness. In the camera web system, choose **Configuration > Image > Display > Image Adjustment**. In the area shown in **Figure 4-220**, slightly decrease the values of **Saturation** and **Sharpness** based on the site requirements to decrease noise.

Figure 4-220 Setting image adjustment parameters

▼

Image Adjustment

Brightness

0100

50

Saturation

0100

50

Contrast

0100

50

Sharpness

0100

50

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.

4.17.3.2 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 > Backlight**, and set **Backlight mode** to **Backlight adaptation**, as shown in [Figure 4-221](#).

Figure 4-221 Setting backlight adaptation parameters

▼

Backlight

Backlight mode

Backlight adaptation

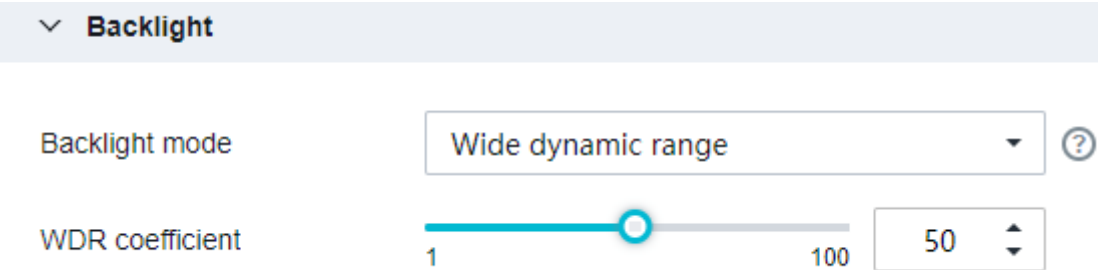
▼

?

Recommended Settings

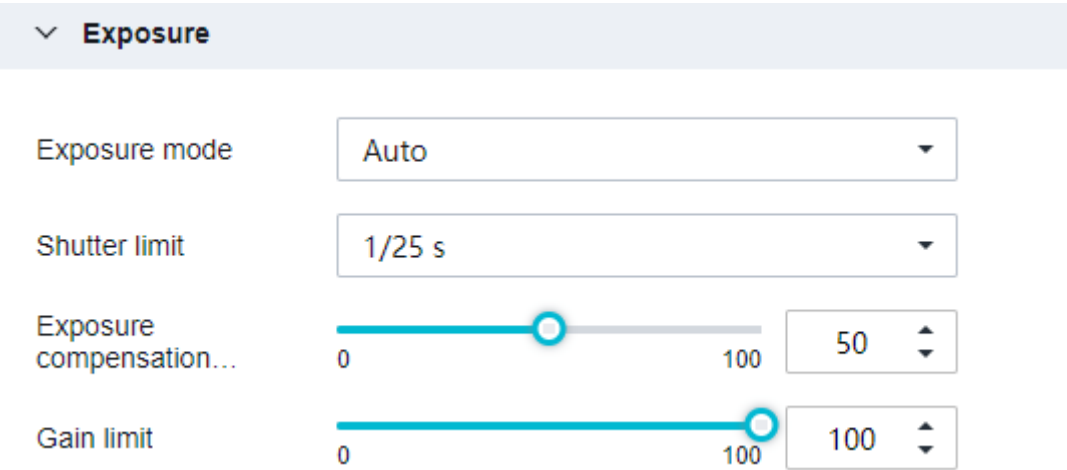
1. Log in to the camera web system, choose **Configuration > Image > Display > Backlight**, set **Backlight mode** to **Wide dynamic range**, and slightly increase the value of **WDR coefficient**, as shown in [Figure 4-222](#).

Figure 4-222 Setting backlight parameters



2. Choose **Configuration > Image > Display > Exposure** and set **Exposure compensation coefficient** to a larger value, as shown in [Figure 4-223](#). Note that a higher coefficient will cause more noises in night-time images.

Figure 4-223 Setting exposure parameters



3. If the brightness is still insufficient, you can adjust the value of **Brightness** and **Contrast** under **Configuration > Image > Display > Image Adjustment**.

4.17.3.3 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.

4.17.3.3.1 Corridor

If the camera is installed in a long corridor, you can toggle on **Rotate images by 90 degrees** under **Configuration > Image > Display > Image Enhancement**, as shown in [Figure 4-224](#). The corridor mode produces a vertically-oriented image that is perfect for observing narrow corridors, as shown in [Figure 4-225](#).

Figure 4-224 Image enhancement parameters in manual mode

Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

☐

Defogging

Manual

Defogging level

0

100

50

Anti-light flicker

Disable

Denoising

Automatic noise reduction

IR overexposure compensation

0

100

50

Figure 4-225 Image effect after the function of rotating images by 90° is enabled



4.17.3.3.2 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 4-226](#), some objects are blocked. In [Figure 4-227](#), the camera shooting angle is inappropriate.

Figure 4-226 Blocked areas



Figure 4-227 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.

4.17.3.4 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 4-228](#), 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 4-228 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 the defogging function under **Configuration > Image > Display > Image Enhancement**, as shown in [Figure 4-229](#). If the manual mode is selected, you can manually set **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 4-229 Image enhancement parameters in manual mode

▼ Image Enhancement

Mirror mode

Disable

Rotate images by 90 degrees

☐

Defogging

Manual

Defogging level

0

100

50

Anti-light flicker

Disable

Denoising

Automatic noise reduction

IR overexposure compensation

0

100

50

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 function of rotating images by 90 degrees or electronic image stabilization, performance will be affected. The video frame rate may be lowered, resulting in occasional video stuttering.

5 Maintenance

- 5.1 Routine Maintenance
- 5.2 Security Maintenance
- 5.3 Emergency Maintenance

5.1 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 5-1** lists the tools to be prepared.

Table 5-1 Tools to be prepared

Tool Name	Specification and Function	Appearance
Video detection tester	Used to check the shooting angle and video image.	

Tool Name	Specification and Function	Appearance
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.	
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.	

Tool Name	Specification and Function	Appearance
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.	
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 5-2 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 5-3 Routine maintenance items

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 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 whether the actual application scenarios exceed the camera specifications. Periodically check the camera to improve the camera operating reliability.
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 Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
Check whether insect prevention and de-insectization 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 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 3.6.3 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 5-4 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 5-5 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.

Check Item	Maintenance Frequency	Baseline Requirement	Troubleshooting	Severity	Description
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 recording is normal. • Systematically inspect the camera hardware, system, and functions.	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.

5.2 Security Maintenance

5.2.1 Overview

5.2.1.1 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.

5.2.1.2 Security Features

5.2.1.2.1 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.

5.2.1.2.2 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.

5.2.1.2.3 Network Layer Security

In video security solutions, firewalls are used to isolate security zones.

5.2.1.2.4 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.

5.2.1.2.5 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.

5.2.1.3 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.

5.2.1.4 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](#).

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*.

5.2.2 Application Layer Security

5.2.2.1 Accounts at the Application Layer

5.2.2.2 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.

5.2.2.2.1 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.

- Step 1
- Log in to the camera web system (<https://Camera IP address>).
- Step 2
- Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-1](#).

Figure 5-1 User List area

User List							
+ Add Advanced Multi-point login							
Seq.	User name	User type	Account status	Password	Multi-point Login	Operation	
1	admin	Administrator	Normal	*****	20	✓ ✕	
2	user01	Advanced operator	Normal	*****	20	✓ ✕	
3	user02	Advanced operator	Normal	*****	20	✓ ✕	
4	user03	Advanced operator	Normal	*****	20	✓ ✕	
5	user04	Advanced operator	Normal	*****	20	✓ ✕	
6	user05	Advanced operator	Normal	*****	20	✓ ✕	
7	user06	Advanced operator	Normal	*****	20	✓ ✕	
8	user07	Advanced operator	Normal	*****	20	✓ ✕	

- Step 3
- Click **Add**.

In the **Add** dialog box that is displayed, configure information about the new user, as shown in [Figure 5-2](#).

Figure 5-2 Add dialog box

Add

The web password is independent from protocol passwords such as the ONVIF and SDK

User type

Advanced operator

User name

Enter the user name.

Current user password

Enter the current user password.

New password

Enter a new password.

OK

Cancel

NOTICE

- A maximum of 10 users (including the **admin** user) can be added.
- The **admin** users are administrators and cannot be added again.

Step 4 Set user parameters. [Table 5-6](#) describes the parameters.

Table 5-6 Parameters for adding a user

Parameter	Setting
User type	Select a user type from the drop-down list box. Different types of users have different operation rights. You can select the user type as required. • Administrators have all operation rights. They can add advanced operators and common operators. • 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. NOTE Low-complexity passwords may cause security risks. It is highly recommended that enterprises set high-complexity passwords. You are advised not to set the new password to a weak password. The default weak passwords include Cspdbr@2017, kafka-1qaz@WSX, CSP@gaussdb@2017, UGW9811adminhwbs@com, hwbs@com, sps600@HW, Changeme_123, hwosta2.0, cnp200@HW, omu800@HW, mt2013@HW, GrUB1@ATCA, x86bpw, admin@86, data1@HW, Admin_12#, pgw#2013, Pmssys@2013, Admin@123, Update@7*24, 9061csl, cgp data2@HW, sys data1@HW, bmu_hss, sek12345, HWps123, cnp123@HW, Spark@123, Hbase@123, and Hdfs@123.
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.

Step 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.

----End

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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-3](#).

Figure 5-3 User List area

User List								
Add Advanced Multi-point login								
Seq.	User Name	User Type	Account Status	Password	Multi-point Login	Operation		
1	admin	Administrator	Normal	*****	20	✓		
2	user01	Advanced operator	Normal	*****	20	✓		
3	user02	Advanced operator	Normal	*****	20	✓		
4	user02	Advanced operator	Normal	*****	20	✓		
5	user02	Advanced operator	Normal	*****	20	✓		
6	user02	Advanced operator	Normal	*****	20	✓		
7	user02	Advanced operator	Normal	*****	20	✓		
8	user02	Advanced operator	Normal	*****	20	✓		

Step 3 Select a user.

Step 4 Click  .

The **Edit** dialog box is displayed, as shown in [Figure 5-4](#).

Figure 5-4 Edit dialog box

Edit

The web password is independent from protocol passwords such as the ONVIF and SDK

User type

Administrator

User name

admin

Current user password

Enter the current user password.

New password

Enter a new password.

OK

Cancel

Step 5 Specify the current user password, new password, and confirm password.

Step 6 Click **OK**.

 **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.

----End

Changing the Maximum Number of Concurrent Logins

You can change the maximum number of concurrent logins for a user.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-5](#).

Figure 5-5 User List area

User List									
Seq.	Adv.	Advanced	Multi-point login	User Name	User Type	Account Status	Password	Multi-point Login	Operation
1				admin	Administrator	Normal	*****	20	 
2				user01	Advanced operator	Normal	*****	20	 
3				user02	Advanced operator	Normal	*****	20	 
4				user03	Advanced operator	Normal	*****	20	 
5				user04	Advanced operator	Normal	*****	20	 
6				user05	Advanced operator	Normal	*****	20	 
7				user06	Advanced operator	Normal	*****	20	 
8				user07	Advanced operator	Normal	*****	20	 

Step 3 Select a user.

Step 4 Click **Multi-point login**.

The **Modify Multi-point Login** dialog box is displayed.

Step 5 Set **Current user password** and **Multi-point login**.

2024-01-25

353

Step 6 Click **OK**.

----End

Deleting a User

Administrators can delete unnecessary users to ensure system access security.

NOTE

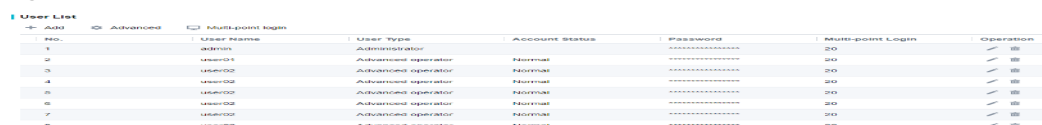
- System administrators can delete advanced operators and common operators. System administrators cannot be deleted.
- Advanced operators do not have the permission to delete users.
- Common operators do not have the permission to delete users.
- After a logged-in user is deleted, the user cannot perform operations in the web system and will be forcibly logged out.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-6](#).

Figure 5-6 User List area



No.	ID	Advanced	Multi-point login	User Name	User Type	Account Status	Password	Multi-point Login	Operation
1	user01			admin	Administrator	Normal	*****	20	
2	user02			Advanced operator	Advanced operator	Normal	*****	20	
3	user03			Advanced operator	Advanced operator	Normal	*****	20	
4	user04			Advanced operator	Advanced operator	Normal	*****	20	
5	user05			Advanced operator	Advanced operator	Normal	*****	20	
6	user06			Advanced operator	Advanced operator	Normal	*****	20	
7	user07			Advanced operator	Advanced operator	Normal	*****	20	
8	user08			Advanced operator	Advanced operator	Normal	*****	20	

Step 3 Select a user.

Step 4 Click  .

The **Delete** dialog box is displayed.

Step 5 Enter the current user password and click **OK**.

The **Delete** dialog box is displayed.

Step 6 Click **OK**.

----End

Configuring Account Locking

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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-7](#).

Figure 5-7 User List area

User List								
Add	Advanced	Multi-point login						
ID	User Name	User Type	Account Status	Password	Multi-point Login	Operation		
1	admin	Administrator	Normal	*****	20	✓	✖	
2	user01	Advanced operator	Normal	*****	20	✓	✖	
3	user02	Advanced operator	Normal	*****	20	✓	✖	
4	user02	Advanced operator	Normal	*****	20	✓	✖	
5	user02	Advanced operator	Normal	*****	20	✓	✖	
6	user02	Advanced operator	Normal	*****	20	✓	✖	
7	user02	Advanced operator	Normal	*****	20	✓	✖	
8	user02	Advanced operator	Normal	*****	20	✓	✖	

- Step 3** Click **Advanced**.
- The **Advanced** dialog box is displayed, as shown in [Figure 5-8](#).

Figure 5-8 Advanced dialog box

Advanced

Specify the maximum number of consecutive password input failures and the duration for lock account. The configuration applies to all users.

Max. password input failures

5

Lock duration (min)

5

OK

Cancel

- Step 4** Set **Max. password input failures** and **Lock duration (min)**.

NOTE

- **Max. password input failures:** maximum number of consecutive incorrect password attempts allowed
- **Lock duration (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 duration (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**.

- Step 5** Click **OK**.
- End

Unlocking an Account

If an account is locked because the number of incorrect password attempts reaches the maximum, the administrator can unlock the account.

NOTE

Only the administrator has the permission to unlock accounts.

- Step 1** Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management > User List**.

The **User List** area is displayed, as shown in [Figure 5-9](#).

Figure 5-9 User List area

User List

+ Add

⚙️ Advanced

🖥️ Multi-point login

No.	User Name	User Type
1	admin	Administrator
2	admin1	Common operator

Step 3 In the **Operation** column of a locked account, click .

The **Unlock** dialog box is displayed, as shown in [Figure 5-10](#).

Figure 5-10 Unlock dialog box

Unlock

Current user password

Enter the current user password.

OK

Cancel

Step 4 Enter the administrator password and click **OK**.

----End

5.2.2.2.2 User Connection

You can check the connection status of a user or disconnect a user.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Configuration > System > User Management**.

Step 3 Access the **Connection status** area, as shown in [Figure 5-11](#).

Figure 5-11 Connection status area

Connection status				
No.	User Name	IP Address	Login Time	Operation
1	admin	90.253.64.182	2023-10-20 09:08:06	Disconnect

NOTICE

- To disconnect a user, click **Disconnect** in the **Operation** column corresponding to the user.
- The administrator cannot be forcibly disconnected.

-----End

5.2.2.2.3 Password Validity Period

You can view or configure the validity period of a user password.

NOTE

After the password expires, the system will demand you to change the password.

Procedure

- Step 1 Log in to the camera web system (<https://Camera IP address>).
- Step 2 Choose **Configuration > System > User Management**.
- Step 3 Under **Password Validity Period**, check or set **Period**, as shown in [Figure 5-12](#).

Figure 5-12 Password Validity Period area

Password Validity Period

Period

months

Save

NOTE

The value of **Period** is an integer ranging from 0 to 12. If this parameter is set to **0**, the password is permanently valid.

-----End

5.2.2.3 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.

5.2.2.4 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:

- Step 1** Log in to the camera web system (<https://Camera IP address>).
- Step 2** Choose **Configuration > System > System Maintenance > Log**. The **Log** tab page is displayed, as shown in [Figure 5-13](#).

Figure 5-13 Querying logs

 One-Click Info Collection



 Querying Logs

A screenshot of the 'Querying Logs' section. It contains two labels: 'Select Log' and 'Period'. Below 'Select Log' is a dropdown menu with 'Operation' selected. Below 'Period' is a date range input field.

- Step 3** Query logs.
1. 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.

2. 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.

Step 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.

----End

Checking Logs Using the SSH Tool

Step 1 Use the SSH software to log in to the system as the **admin** user.

Step 2 Switch to the **root** user.

su - root

Step 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

----End

5.2.2.5 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.

Step 1 Log in to the camera web system (<https://Camera IP address>).

- Step 2** Choose **Configuration > System > System Maintenance > Maintenance > Restore**. The **Restore** area is displayed, as shown in [Figure 5-14](#).

Figure 5-14 Restore area

Restore

After the snapshot is restored, the snapshot space is restored to the default value. The snapshot



- Step 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.

- Step 4** Enter the current user password in **Current user password**.

- Step 5** Click **OK**.

The system automatically restores factory settings.

----End

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.

- Step 1** Log in to the camera web system (<https://Camera IP address>).

- Step 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.

----End

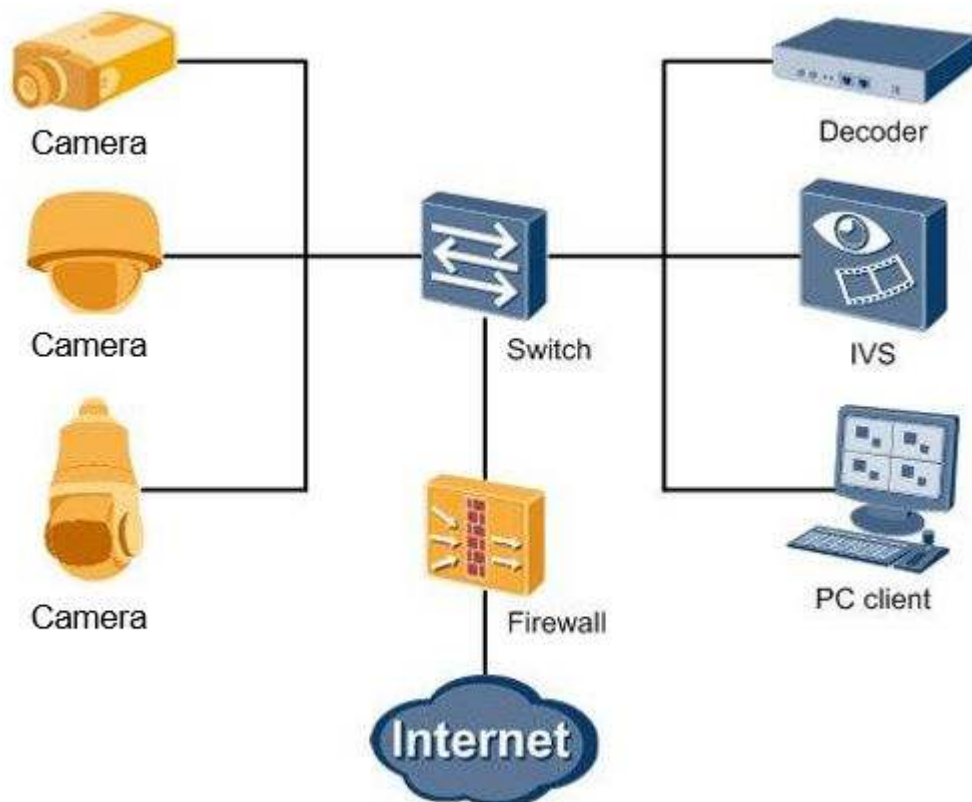
5.2.3 Network Layer Security

5.2.3.1 Secure Network

The entire video security network is deployed inside the firewall to prevent external network attacks.

[Figure 5-15](#) shows the position of cameras on the network.

Figure 5-15 Network diagram



5.2.3.2 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.

5.2.3.3 Remote Access Control

5.2.3.3.1 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.

5.2.3.3.2 IP Address Filtering

You can use the IP address filtering function to allow or deny the access from a specified network segment or port, or using a specified protocol, to the camera.

Background

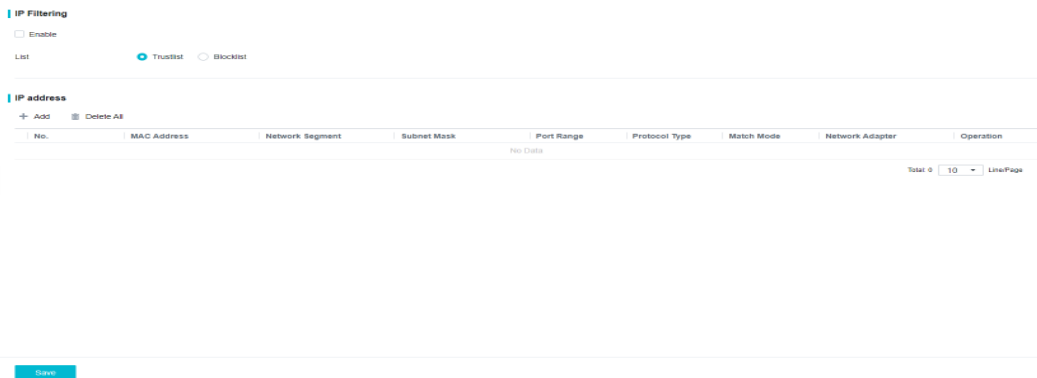
- A network segment is obtained by performing logical AND of the IP address and subnet mask.
- A maximum of 100 IP address filtering rules can be added.

Procedure

Step 1 Choose **Configuration > System > Security Management > IP Filtering**.

The **IP Filtering** tab page is displayed, as shown in [Figure 5-16](#).

Figure 5-16 IP Filtering tab page



Step 2 Select **Enable** to enable the IP address filtering function.

Step 3 Set **List**.

The **List** parameter has two options: **Trustlist** and **Blocklist**, that is, denying or allowing the access only from a specified MAC address, network segment or port, or using a specified protocol. Currently, the camera supports only one option at a time.

Step 4 Click **Add**. In the **Add IP Address Filtering Rule** dialog box that is displayed, set **MAC Address**, **IPv4 network segment**, **IPv4 subnet mask**, **Protocol Type**, and **Match Mode**, as shown in [Figure 5-17](#).

Figure 5-17 Add IP Address Filtering Rule dialog box

Add IP Address Filtering Rule

MAC Address

00 : 00 : 00 : 00 : 00 : 00

IPv4 network segment

192 : 168 : 1 : 0

IPv4 subnet mask

255 : 255 : 255 : 0

Port Range

065535

Protocol Type

UDP

Match Mode

Match IP address

OK

Cancel

NOTE

- If a filtering rule shown in [Figure 5-17](#) is configured under **Blocklist**, the camera does not process UDP packets sent from the network segment **192.168.1.0** to ports **0–65535**.

Step 5 Click **OK**.

The **IP Filtering** tab page is displayed.

Step 6 Click **Save**.

NOTE

To modify or delete an IP address filtering rule, click  or  in the **Operation** column of the IP address filtering rule.

-----End

5.2.4 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.

5.2.4.1 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.

5.2.4.2 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.

5.2.4.3 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.

5.2.4.4 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.

5.2.4.5 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.

5.2.4.6 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.

5.2.4.7 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.

5.2.4.8 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.

5.2.5 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:

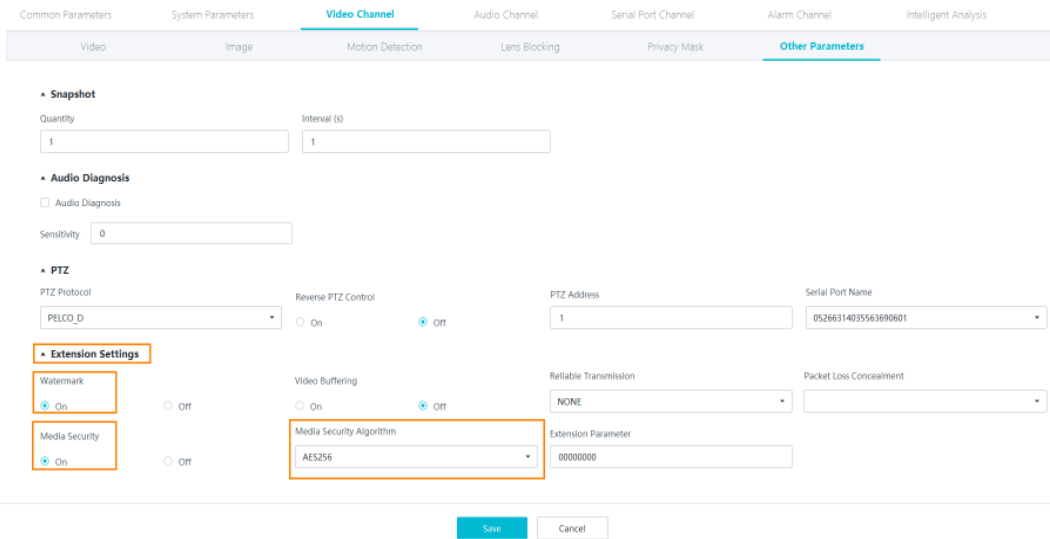
- Change the default password. For details, see [Changing the User Password](#).
- Change the maximum number of users who can log in to the device at the same time. For details, see [Changing the User Password](#).
- You are advised to disable SNMP if such protocols are not used for connecting cameras 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 5-18 shows the method for enabling the watermark and AES encryption functions on the IVS1800 platform.

Figure 5-18 Enabling the watermark function



The screenshot displays the 'Other Parameters' configuration page for the 'Video Channel'. The 'Extension Settings' section is highlighted with orange boxes, showing the following configurations:

- Watermark:** Set to **On**.
- Media Security:** Set to **On**.
- Media Security Algorithm:** Set to **AES256**.

Other visible settings include:

- Snapshot:** Quantity 1, Interval (s) 1.
- Audio Diagnosis:** Sensitivity 0.
- PTZ:** PTZ Protocol PELCO_D, Reverse PTZ Control Off, PTZ Address 1, Serial Port Name 05266314035563690601.
- Video Buffering:** Set to **Off**.
- Reliable Transmission:** Set to **NONE**.
- Packet Loss Concealment:** Set to **00000000**.

Buttons for 'Save' and 'Cancel' are located at the bottom right of the configuration area.

- 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 [5.2.3.3.2 IP Address 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

5.2.6 Appendixes

5.2.6.1 Reference Documents

This section describes the reference document for security maintenance.

[Table 5-7](#) describes the reference documents.

Table 5-7 Reference documents

Reference Document	Description
Log Reference	Describes logs of various types and error codes in logs.

5.2.6.2 List of Security Maintenance Tasks

To ensure optimal security, perform security maintenance tasks regularly.

[Table 5-8](#) describes security maintenance tasks.

Table 5-8 Security maintenance tasks

Security Maintenance Task	Task Implementation Frequency
Changing default passwords NOTE For details about passwords to change, see 5.2.2.1 Accounts at the Application Layer .	Implemented during installation and commissioning
Periodically checking user accounts	Implemented monthly
Periodically changing passwords	Implemented quarterly

5.3 Emergency Maintenance

5.3.1 Overview

5.3.1.1 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.

5.3.1.2 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)

5.3.2 Service Fault Scenarios

5.3.2.1 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 5-19 Checking the protocol password

The screenshot shows a web interface with three tabs: 'SDK Password' (selected), 'Northbound Interface Password', and 'ONVIF Password'. Below the tabs are four input fields: 'User name' (containing 'admin'), 'Web user password', 'New password', and 'Confirm password'. A 'Save' button is located at the bottom left of the form.

4. Collect fault information and contact technical support.
For details about how to collect fault information, see [5.3.3.1 Collecting Fault Information](#).

5.3.2.2 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.
- 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 > Platform Connection > General Protocol > RTSP**.
 - 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 > Platform Connection > General Protocol > ONVIF**. The **ONVIF** page 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](#).

- 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 > Platform Connection > General Protocol > ONVIF**. The **ONVIF** page 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](#).

- 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 > Platform Connection > Protocol Connection Password**. The page for setting password parameters 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](#).

4. Collect fault information and contact technical support.

For details about how to collect fault information, see [5.3.3.1 Collecting Fault Information](#).

5.3.3 Appendix

5.3.3.1 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.

5.3.3.1.1 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 5-9](#) to help engineers quickly rectify faults.

Table 5-9 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 Troubleshooting Cases.	(Yes/No)	Troubleshooting methods and effects	-

5.3.3.1.2 Methods

Collecting Logs on the Web Page

Logs are major fault information and important references for quickly locating faults.

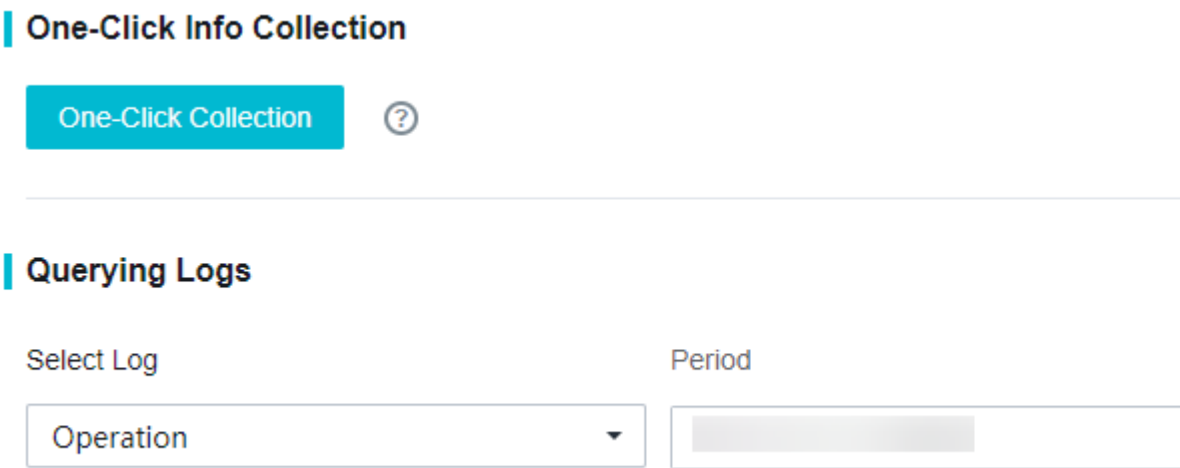
Context

You can collect information, such as system information, configuration files, and SSH logs, with one click.

Procedure

- Step 1** Choose **Configuration > System > System Maintenance > Log**. The **Log** tab page is displayed, as shown in [Figure 5-20](#).

Figure 5-20 Querying logs



- Step 2** Query logs.
- 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.

- 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.

Step 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.

----End

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

6 Reference
