Network Camera

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Please scan the following QR code to obtain the " ***Safety Instruction*** " of the product, and read it carefully. These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

Figure 1-1 Safety Instruction

Contents

Chapter 1 System Requirement 1

Chapter 2 Device Activation and Accessing 2

2.1 Activate the Device via SADP 2

2.2 Activate the Device via Browser 2

2.3 Login 3

2.3.1 Plug-in Installation 3

2.3.2 Admin Password Recovery 4

2.3.3 Illegal Login Lock 5

Chapter 3 Live View 6

3.1 Live View Parameters 6

3.1.1 Start and Stop Live View 6

3.1.2 Aspect Ratio 6

3.1.3 Live View Stream Type 6

3.1.4 Select the Third-Party Plug-in 6

3.1.5 Light 7

3.1.6 Count Pixel 7

3.1.7 Start Digital Zoom 7

3.1.8 Auxiliary Focus 7

3.1.9 Lens Initialization 8

3.1.10 Lens Parameters Adjustment 8

3.1.11 Conduct 3D Positioning 10

3.2 Set Transmission Parameters 10

Chapter 4 Video and Audio 12

4.1 Video Settings 12

4.1.1 Stream Type 12

4.1.2 Video Type 12

4.1.3 Resolution 12
4.1.4 Bitrate Type and Max. Bitrate 13
4.1.5 Video Quality 13
4.1.6 Frame Rate 13
4.1.7 Video Encoding 13
4.1.8 Smoothing 15
4.2 Audio Settings 15
4.2.1 Audio Encoding 16
4.2.2 Audio Input 16
4.2.3 Audio Output 16
4.2.4 Environmental Noise Filter 16
4.3 Two-way Audio 16
4.4 ROI 17
4.4.1 Set ROI 17
4.5 Set Target Cropping 18
4.6 Display Info. on Stream 18
4.7 Display Settings 18
4.7.1 Scene Mode 19
4.7.2 Image Parameters Switch 24
4.7.3 Video Standard 25
4.7.4 Local Video Output 25
4.8 OSD 25
4.9 Set Privacy Mask 26
4.10 Overlay Picture 26
Chapter 5 Video Recording and Picture Capture 27
5.1 Storage Settings 27
5.1.1 Memory Card 27
5.1.2 Set FTP 29

5.1.3 Set NAS 30
5.1.4 eMMC Protection 31
5.1.5 Set Cloud Storage 31
5.2 Video Recording 32
5.2.1 Record Automatically 32
5.2.2 Record Manually 34
5.2.3 Playback and Download Video 34
5.3 Capture Configuration 35
5.3.1 Capture Automatically 35
5.3.2 Capture Manually 35
5.3.3 View and Download Picture 36
Chapter 6 Event and Alarm 37
6.1 Set Motion Detection 37
6.1.1 Expert Mode 37
6.1.2 Normal Mode 38
6.2 Set Video Tampering Alarm 39
6.3 Set Alarm Input 40
6.4 Set Exception Alarm 41
6.5 Set Video Quality Diagnosis 41
6.6 Set Audio Exception Detection 42
6.7 Set Defocus Detection 43
6.8 Set Scene Change Detection 43
Chapter 7 Arming Schedule and Alarm Linkage 44
7.1 Set Arming Schedule 44
7.2 Linkage Method Settings 44
7.2.1 Trigger Alarm Output 45
7.2.2 FTP/NAS/Memory Card Uploading 46
7.2.3 Send Email 46

7.2.4 Notify Surveillance Center 47
7.2.5 Trigger Recording 47
7.2.6 Flashing Light 47
7.2.7 Audible Warning 48
7.2.8 Alarm Server 49
Chapter 8 Network Settings 50
8.1 TCP/IP 50
8.2 Access to Device via Domain Name 51
8.3 Access to Device via PPPoE Dial Up Connection 52
8.4 SNMP 52
8.5 Set IEEE 802.1X 53
8.6 Set QoS 53
8.7 HTTP(S) 54
8.8 Multicast 55
8.8.1 Multicast Discovery 55
8.9 RTSP 55
8.10 Set SRTP 56
8.11 Bonjour 56
8.12 WebSocket(s) 57
8.13 Port Mapping 57
8.13.1 Set Auto Port Mapping 57
8.13.2 Set Manual Port Mapping 57
8.13.3 Set Port Mapping on Router 58
8.14 RTCP 59
8.15 Wireless Dial 59
8.15.1 Set Wireless Dial 59
8.15.2 Wireless Expert Settings 60
8.16 WLAN AP (Access Point) 62

8.16.1 Set WLAN AP 62
8.16.2 Access to Device via AP 63
8.17 Traffic Shaping 64
8.18 Data Monitoring 64
8.19 Wi-Fi 64
8.19.1 Connect Device to Wi-Fi 65
8.20 Set ISUP 65
8.21 Access Camera via Hik-Connect 66
8.21.1 Enable Hik-Connect Service on Camera 66
8.21.2 Set Up Hik-Connect 67
8.21.3 Add Camera to Hik-Connect 68
8.22 Set Open Network Video Interface 69
8.23 Set SDK Service 69
Chapter 9 System and Security 70
9.1 System Settings 70
9.1.1 View Device Information 70
9.1.2 Time and Date 70
9.1.3 Set RS-232 71
9.1.4 Set RS-485 72
9.1.5 Set Live View Connection 72
9.1.6 Location Settings 72
9.1.7 External Device 73
9.1.8 View Open Source Software License 75
9.2 Wiegand 75
9.3 User and Account 75
9.3.1 Set User Account and Permission 75
9.3.2 Simultaneous Login 76
9.3.3 Online Users 76

9.4 Maintenance 76
9.4.1 Restart 76
9.4.2 Upgrade 77
9.4.3 Restore and Default 77
9.4.4 Import and Export Configuration File 77
9.4.5 Search and Manage Log 78
9.4.6 Search Security Audit Logs 78
9.4.7 SSH 78
9.4.8 Export Diagnose Information 79
9.4.9 Diagnosis 79
9.5 Security 81
9.5.1 Set IP Address Filter 81
9.5.2 Set MAC Address Filter 81
9.5.3 Control Timeout Settings 82
9.5.4 Certificate Management 82
9.5.5 TLS 85
Chapter 10 VCA Resource 86
10.1 Set Open Platform 86
10.2 General Settings 87
10.2.1 Set Camera Info 87
10.2.2 Metadata 88
10.3 Smart Event 88
10.3.1 Set Intrusion Detection 88
10.3.2 Set Line Crossing Detection 89
10.3.3 Set Region Entrance Detection 91
10.3.4 Set Region Exiting Detection 92
10.3.5 Set Unattended Baggage Detection 94
10.3.6 Set Object Removal Detection 95

10.3.7 Set Loitering Detection 96
10.3.8 Set People Gathering Detection 98
10.3.9 Set Fast Moving Detection 99
10.3.10 Set Parking Detection 100
10.4 Schedule Switch Application 102
10.5 Search and Export Data Aware Information 103
10.6 Search and View Power Consumption Statistics 103
Chapter 11 Smart Display 105
Chapter 12 EPTZ 106
12.1 Patrol 106
12.2 Auto-Tracking 106
Appendix A. FAQ 108

Chapter 1 System Requirement

Your computer should meet the requirements for proper visiting and operating the product.

Operating System	Microsoft Windows XP SP1 and above version
CPU	2.0 GHz or higher
RAM	1G or higher
Display	1024×768 resolution or higher
Web Browser	For the details, see ***Plug-in Installation***

Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.

Note

Refer to the user manual of the software client for the detailed information about the client software activation.

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com to get SADP software to install.

Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.

   Caution

   We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
5. Click **OK**.

   Device Status changes into **Active**.
6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.

Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input ***192.168.1.64*** in the browser.
4. Set device activation password.

Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration → Network → Network Settings → TCP/IP** to change the IP address of the device to the same segment of your network.

2.3 Login

Log in to the device via Web browser.

2.3.1 Plug-in Installation

Certain operating systems and web browsers may restrict the display and operation of the device function. You should install a plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	• Internet Explorer 10+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+ • Edge 89+	Click to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Plug-in installation is not required. Go to **Configuration → Network → Network Service → WebSocket(s)** to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

Note

- The device only supports Windows and Mac OS system, and does not support Linux system.
- To improve the user experience on certain devices, it's recommended to use a more advanced web browser for access. Please refer to the actual device or product specification.
- Certain device models do not support Internet Explorer web browser.

2.3.2 Admin Password Recovery

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page after completing the account security settings.

You can reset the password by setting the security question or email.

Note

When you need to reset the password, make sure that the device and the PC are on the same network segment.

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management** , click **Account Security Settings**, select the security question and input your answer.
You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

You can set the account security during the activation. Or you can go to **Configuration → System → User Management** , click **Account Security Settings**, input your email address to receive the verification code during the recovering operation process.

2.3.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Maintenance and Security → Security → Login Management** , and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

3.1 Live View Parameters

The supported functions vary depending on the model.

3.1.1 Start and Stop Live View

Click **Live View**. Click to start live view. Click to stop live view.

3.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

- refers to 4:3 window size.
- refers to 16:9 window size.
- refers to original window size.
- refers to self-adaptive window size.
- refers to original ratio window size.

3.1.3 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to ***Stream Type*** .

3.1.4 Select the Third-Party Plug-in

When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

Steps

1. Click **Live View**.
2. Click to select the plug-in.
   - When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
   - When you access the device via the other browsers, you can select Webcomponents, QuickTime or MJPEG.

3.1.5 Light

Click to turn on or turn off the illuminator.

Caution

For the device with laser:

- DO NOT stare at operating light source. May be harmful to the eyes.
- If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
- When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.

3.1.6 Count Pixel

It helps to get the height and width pixel of the selected region in the live view image.

Steps

1. Click to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.
   The width pixel and height pixel are displayed on the bottom of the live view image.

3.1.7 Start Digital Zoom

It helps to see a detailed information of any region in the image.

Steps

1. Click to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.

3.1.8 Auxiliary Focus

It is used for motorized device. It can improve the image if the device cannot focus clearly.

For the device that supports ABF, adjust the lens angle, then focus and click ABF button on the device. The device can focus clearly.

Click to focus automatically.

Note

- If the device cannot focus with auxiliary focus, you can use ***Lens Initialization*** , then use auxiliary focus again to make the image clear.
- If auxiliary focus cannot help the device focus clearly, you can use manual focus.

3.1.9 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

Click to operate lens initialization.

3.1.10 Lens Parameters Adjustment

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the device. In live view interface, you can click the direction control buttons to control the pan/tilt movement, and click the zoom/focus/iris buttons to realize lens control.

Note

- Supported PTZ functions may vary according to different camera models.
- For the devices which support lens movements only, the direction buttons are invalid.

Direction Control

Click and hold the direction button to pan/tilt the device.

Zoom

- Click , and the lens zooms in.
- Click , and the lens zooms out.

Focus

- Click , then the lens focuses near and the nearby object gets clear.
- Click , then the lens focuses far and the distant object gets clear.

Iris

- When the image is too dark, click to enlarge the iris.
- When the image is too bright, click to stop down the iris.

PTZ Speed

- Slide to adjust the speed of the pan/tilt movement.

PTZ Lock

PTZ lock means to disable the zoom, focus and PTZ rotation functions of the corresponding channel, so that to reduce the target missing caused by PTZ adjustment.

Note

The function is only supported by certain device models.

Click to lock the PTZ operation, or click to unlock it.

PTRZ Adjustment

PTRZ is an abbreviation for pan, tilt, rotate and zoom. It means the movement options of the device. In the interface, you can use the control buttons to adjust the movement of the device, such as device panning, tilting, rotating, and zooming.

Note

The function is only supported by certain device models.

Go to **Configuration → PTZ → PTRZ** .

Control Panel

	Click and hold the directional button to pan/tilt the device.
• •	Click and hold the button to adjust rotating position.

Auto Recovery

Click , the device will correct the rotating position automatically to make the live view image positive. Make sure the **Self-Test Status** is **Initialized**.

Note

- Go to **Configuration → PTZ → PTZ** to view the **Self-Test Status**.
- If you want to initialize PTZ and enable PTZ self-check manually, go to **Configuration → PTZ → PTZ** and click **Self-Test**, then the PTZ is initialized.

Refer to ***Lens Parameters Adjustment*** for more detailed settings of lens adjustment.

3.1.11 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click to enable the function.
2. Select a target area in live image.
   - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
   - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
   - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

3.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

Steps

1. Go to **Configuration → Local → Live View Parameters** .
2. Set the transmission parameters as required.

   Protocol

   TCP

   TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

   UDP

   UDP is suitable for the unstable network environment that does not demand high video fluency.

   MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.

Note

For detailed information about multicast, refer to ***Multicast*** .

HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

Play Performance

Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

Balanced

The device ensures both the real-time video image and the fluency.

Fluent

The device takes the video fluency as the priority over teal-time. In poor network environment, the device cannot ensures video fluency even the fluency is enabled.

Custom

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may cannot display.

3. Click **Save**.

Chapter 4 Video and Audio

This part introduces the configuration of video and audio related parameters.

4.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration → Video/Audio → Video** .

4.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

Other Streams

Steams other than the main stream and sub stream may also be offered for customized usage.

4.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

Video Stream

Only video content is contained in the stream.

Video&Audio

Video content and audio content are contained in the composite stream.

4.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

4.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

4.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

4.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

4.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.

Note

Available compression standards vary according to device models.

H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

When H.264+ is enabled, **I Frame Interval** is not configurable.

H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

When H.265+ is enabled, **I Frame Interval** is not configurable.

I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

MPEG4

MPEG4, referring to MPEG-4 Part 2, is a video compression format developed by Moving Picture Experts Group (MPEG).

MJPEG

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format is compressed as individual JPEG images.

Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

4.1.8 Smoothing

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

4.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .

Note

Only certain camera models support the function.

4.2.1 Audio Encoding

Select the audio encoding compression of the audio.

4.2.2 Audio Input

Note

- Connect the audio input device as required.
- The audio input display varies with the device models.

LineIn	Set **Audio Input** to **LineIn** when the device connects to the audio input device with the high output power, such as MP3, synthesizer or active pickup.
MicIn	Set **Audio Input** to **MicIn** when the device connects to the audio input device with the low output power, such as microphone or passive pickup.

4.2.3 Audio Output

Note

Connect the audio output device as required.

It is a switch of the device audio output. When it is disabled, all the device audio cannot output. The audio output display varies with the device modes.

4.2.4 Environmental Noise Filter

Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

4.3 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click on the toolbar to enable two-way audio function of the camera.
3. Click , disable the two-way audio function.

4.4 ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression. The technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

4.4.1 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H. 265.

Steps

1. Go to **Configuration → Video/Audio → ROI** .
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** and click to draw ROI region on the live view.

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

5. Input the **Area Name** and **ROI Level**.
6. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.

7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

4.5 Set Target Cropping

You can crop the image, transmit and save only the images of the target area to save transmission bandwidth and storage.

Steps

1. Go to **Configuration → Video/Audio → Target Cropping** .
2. Check **Enable** and set **Third Stream** as the **Stream Type**.

   Note

   After enabling target cropping, the third stream resolution cannot be configured.

3. Select a **Cropping Resolution**.

   A red frame appears in the live view.

4. Drag the frame to the target area.
5. Click **Save**.

   Note

   - Only certain models support target cropping and the function varies according to different camera models.
   - Some functions may be disabled after enabling target cropping.

4.6 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Before You Start

This function is supported in smart events. Go to **VCA** , select **Smart Event** and click **Next** to enable **Smart Event**.

Steps

1. Go to **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

4.7 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration → Image → Display Settings** .

Click **Default** to restore settings.

4.7.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

By adjusting the **Brightness**, **Saturation**, **Contrast** and **Sharpness**, the image can be best displayed.

Exposure Settings

Exposure is controlled by the combination of iris, shutter, and photo sensibility. You can adjust image effect by setting exposure parameters.

In manual mode, you need to set **Exposure Time**, **Gain** and **Slow Shutter**.

Focus

It offers options to adjust the focus mode.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

Manual

You can adjust the focus manually on the live view page.

Day/Night Switch

Day/Night Switch function can provide color images and black/white images in day and night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is black/white or colorful and the supplement light will be enabled to ensure clear live view image at night.

Note

Only certain device models support the supplement light and colorful image.

Auto

The camera switches between the day mode and the night mode according to the light condition of environment.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Triggered by alarm input

You can set **Triggering Status** as **Day** or **Night**. For example, if the **Triggering Status** is **Night**, the mode turns into **Night** when the device receives alarm input signal.

Triggered by video

The camera switches between the day mode and the night mode according to the light condition of environment. This mode is applicable when the device supports road traffic and vehicle detection.

Note

- Day/Night Switch function varies according to models.
- You can turn on the smart supplement light for better image effect. For supplement light settings, refer to ***Supplement Light Settings*** .

Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Supplement Light

IR light is enabled.

White Light

White light is enabled.

Mixed Light

Both IR light and white light are enabled.

Smart

When you select this mode after enabling certain smart events or motion detection, in the night state, the default supplement light mode is IR supplement light mode. When the alarm is triggered, the white light is enabled and the device captures the target. After the alarm ends, the supplement light mode will switch to IR supplement light mode.

Only device models with IR and white light or hybrid supplement light with IR and white light support this function.

Off

Supplement light is disabled.

Note

The supplement light mode may vary according to different device models.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

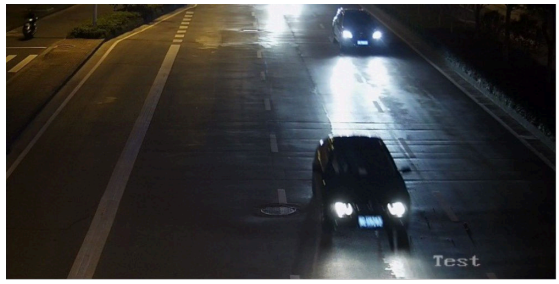
WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.



WDR Off

WDR On

Figure 4-1 WDR

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

White Balance

White balance is the white rendition function of the camera. It is used to adjust the color temperature according to the environment.

Cold

Warm

Auto White Balance

Figure 4-2 White Balance

DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.

DNR Off

DNR On

Figure 4-3 DNR

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

Defog Off

Defog On

Figure 4-4 Defog

EIS

Increase the stability of video image by using jitter compensation technology.

Gray Scale

You can choose the range of the **Gray Scale** as [0-255] or [16-235].

Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.

Note

The video recording will be shortly interrupted when the function is enabled.

Rotate

When this function is enabled, the live view will rotate 90° counterclockwise. For example, 1280 × 720 is rotated to 720 × 1280.

Enabling this function can change the effective range of monitoring in the vertical direction.

Note

This function is supported under certain settings.

Lens Distortion Correction

For device equipped with motorized lens, image may appear distorted to some extent. Enable this function to correct the distortion.

Note

- This function is only supported by certain device equipped with motorized lens.
- The edge of image will be lost if this function is enabled.

4.7.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration → Image → Image Parameters Switch** , and set parameters as needed.

Set Scheduled-switch

Switch the image to the linked scene mode automatically in certain time periods.

Steps

1. Check **Scheduled-switch**.
2. Select and configure the corresponding time period and linked scene mode.

   Note

   For Linked Scene configuration, refer to ***Scene Mode*** .

3. Click **Save**.

4.7.3 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

4.7.4 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

4.8 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Go to OSD setting page: **Configuration → Image → OSD Settings** . Set the corresponding parameters, and click **Save** to take effect.

Character Set

Select character set for displayed information. If Korean is required to be displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Display

Set camera name, date, week, and their related display formats.

Format Settings

Set OSD parameters, such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

Text Overlay

Set customized overlay text on image.

4.9 Set Privacy Mask

The function blocks certain areas in the live view to protect privacy. No matter how the device moves, the blocked scene will never be seen.

Steps

1. Go to **Configuration → Image → Privacy Mask** .
2. Check **Enable**.
3. Click . Drag the mouse in the live view to draw a closed area.

Drag the corners of the area	Adjust the size of the area.
Drag the area	Adjust the position of the area.
Click	Clear all the areas you set.

4. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
5. Click **Save**.

4.10 Overlay Picture

Overlay a customized picture on live view.

Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.

Steps

1. Go to **Configuration → Image → Picture Overlay** .
2. Check **Enable**.
3. Click **Upload** to select a picture and open it.

   The picture with a red rectangle will appear in live view after successfully uploading.
4. Drag the red rectangle to adjust the picture position.
5. Click **Save**.

Chapter 5 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

5.1 Storage Settings

This part introduces the configuration of several common storage paths.

5.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Click **Format** to initialize the memory card.

   When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.
4. **Optional:** Encrypt the memory card.

   1) Click **Encrypted Format**.

   2) Set the encryption password.

   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   Keep your encryption password properly. Encryption password cannot be found if forgotten.
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.

3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → Memory Card Detection** .
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

   Remaining Lifespan

It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

Health Status

It shows the condition of your memory card. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.

Note

It is recommended that you change the memory card when the health status is not "good".

3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
   - Add a Lock
     a. Select the **Lock Switch** as ON.
     b. Enter the password.
     c. Click **Save**
   - Unlock
     - If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
     - If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.
   - Remove the Lock
     a. Select the **Lock Switch** as OFF.
     b. Enter the password in **Password Settings**.
     c. Click **Save**.

Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

4. Set **Arming Schedule** and **Linkage Method**. See ***Set Arming Schedule*** and ***Linkage Method Settings*** for details.
5. Click **Save**.

5.1.2 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration → Event → Alarm Setting → FTP** .
2. Configure FTP settings.

   Server Address and Port

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

   If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

   Directory Structure

   The saving path of snapshots in the FTP server.
3. **Optional:** Check **Upload Picture** to enable uploading snapshots to the FTP server.

   Picture Filing Interval

   For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

   Picture Name

   Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.
4. **Optional:** Check **Enable Automatic Network Replenishment**.

   Note

   Upload to FTP/Memory Card/NAS in **Linkage Method** and **Enable Automatic Network Replenishment** should be both enabled simultaneously.
5. Click **Test** to verify the FTP server.
6. Click **Save**.

5.1.3 Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD** .
2. Click **Add**.
3. Set **Mounting Type**.

Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

4. Set the **Server Address** and **File Path** for the disk.

Server Address

The IP address of the network disk.

File Path

The saving path of network disk files.

5. Click **Test** to check whether the network disk is available.
6. Click **OK** to finish the steps to add a Net HDD.
7. **Optional:** Configure the Net HDD.

Edit Click to edit the parameter setting.

Delete Delete the Net HDD.

- Click .
- Select the Net HDD, click **Delete**.

8. Click **Save**.

5.1.4 eMMC Protection

It is to automatically stop the use of eMMC as a storage media when its health status is poor.

Note

The eMMC protection is only supported by certain device models with an eMMC hardware.

Go to **Configuration → System → System Settings → System Service** for the settings.

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor. Otherwise, using a worn-out eMMC may lead to device boot failure.

5.1.5 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps

Caution

If the cloud storage is enabled, the pictures are stored in the cloud video manager firstly.

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .
2. Check **Enable**.
3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.
5. Click **Save**.

5.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

5.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See ***Event and Alarm*** for details.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Check **Enable**.
3. Select a record type.

Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Set the advanced recording parameters.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.

Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

6. Click **Save**.

5.2.2 Record Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Video Size** and **Video Saving Path** for recorded video files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

What to do next

View the recorded video files.

Go to **Configuration → Local** and click **Open** behind **Video Saving Path** to open the saving path and view the files.

5.2.3 Playback and Download Video

You can search, playback, clip and download the videos stored in the local storage or network storage.

Steps

1. Go to **Playback → Video** .
2. Set search condition and click **Search**.

   The matched video files showed on the timing bar.
3. Click to play the video files.
   - Click to play video files in full screen. Press **ESC** to exit full screen.
   - Click to stop video playback for all channels.
4. **Optional:** Click to clip video files. Click again to stop clipping video files

   Note

   Go to **Configuration → Local → Clip Saving Path** , view and change the saving path of clipped video files.
5. **Optional:** Click on the playback interface to download files.

   Note

   Go to **Configuration → Local → Downloaded File Saving Path** , view and change the saving path of downloaded video files.

5.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

5.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to ***Event and Alarm*** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Picture Capture** .
2. Set capture schedule. Refer to ***Set Arming Schedule*** for configuring schedule time.

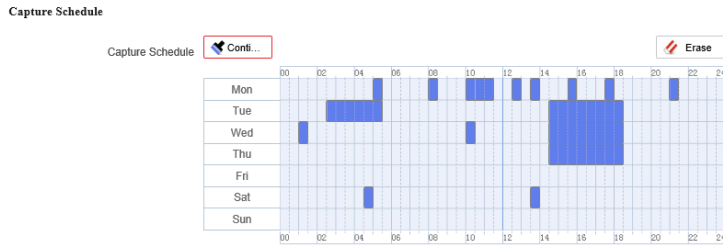


Figure 5-1 Set Capture Schedule

3. Set the capture type.

   Scheduled

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.
4. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.

   Note

   The resolution of the captured picture is the same as the resolution of the captured picture stream. You can select **Stream Type** in **Advanced**.
5. Click **Save**.

5.3.2 Capture Manually

Steps

1. Go to **Configuration → Local** .

2. Set the **Image Format** and saving path to for snapshots.

   JPEG

   The picture size of this format is comparatively small, which is better for network transmission.

   BMP

   The picture is compressed with good quality.
3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

5.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Go to **Playback → Picture** .
2. Set search condition and click **Search**.

   The matched pictures showed in the file list.
3. Download the pictures.
   - Select the pictures then click **Download** to download them.
   - Click **Download This Page** to download the pictures of this page.
   - Click **Download All** to download all the pictures.

Note

Go to **Configuration → Local → Playback Capture Saving Path** , view and change the saving path of captured pictures when playback.

Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

6.1 Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Motion Detection** .
2. Check **Enable**.
3. **Optional:** Highlight to display the moving object in the image in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** .
   3) Set **Rules** to **Enable**.
4. Select mode in **Configuration**, and set rule region and rule parameters.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
6. Click **Save**.

6.1.1 Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

   Scheduled Image Settings

   OFF

   Image switch is disabled.

   Auto-Switch

   The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

   Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click . Click and drag the mouse on the live image and then release the mouse to finish drawing one area.

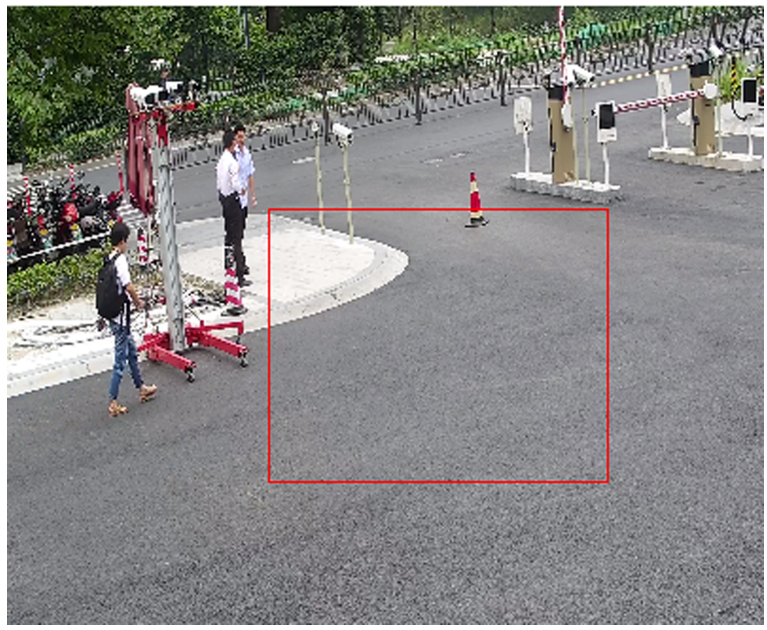


Figure 6-1 Set Rules

4. Click to clear all the areas.
5. Click **Save**.
6. **Optional:** Repeat above steps to set multiple areas.

6.1.2 Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. **Optional:** Click to clear all the areas.
6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6.2 Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click and drag the mouse in the live view to draw the area.

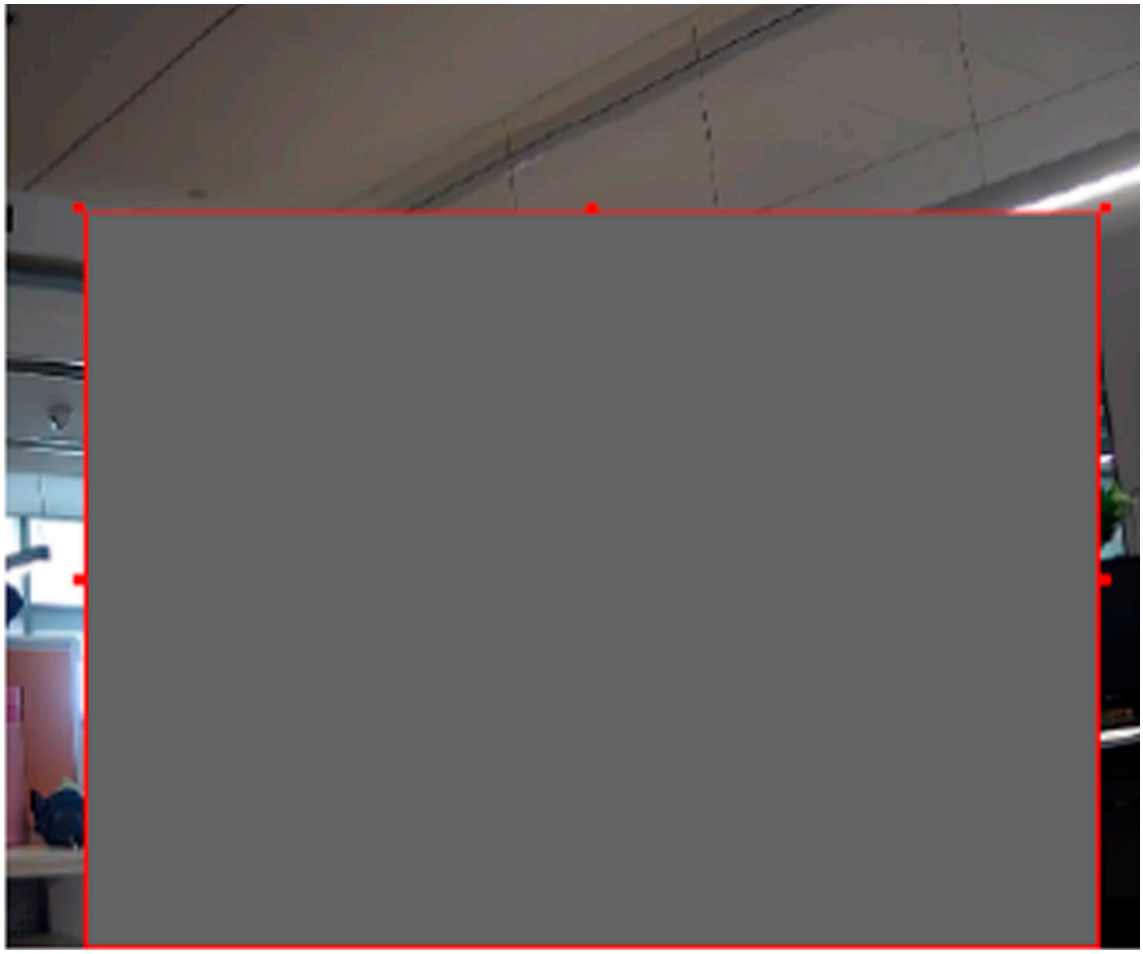


Figure 6-2 Set Video Tampering Area

5. **Optional:** Click 🗑 to delete all the drawn areas.
6. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
7. Click **Save**.

6.3 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start

Note

This function is only supported by certain models.

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Configuration → Event → Event and Detection → Alarm Input** .
2. Select an **Alarm Input NO.** and click ✎ to set alarm input.
3. Select **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Check **Enable Alarm Input Handling**.
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

6.4 Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Event and Detection → Exception** .
2. Select **Exception Type**.

   HDD Full

   The HDD storage is full.

   HDD Error

   Error occurs in HDD.

   Network Disconnected

   The device is offline.

   IP Address Conflicted

   The IP address of current device is same as that of other device in the network.

   Illegal Login

   Incorrect user name or password is entered.
3. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

6.5 Set Video Quality Diagnosis

When the video quality of the device is abnormal and the alarm linkage is set, the alarm will be triggered automatically.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Quality Diagnosis** .
2. Select **Diagnosis Type**.
3. Set the corresponding parameters.

   Alarm Detection Interval

The time interval to detect the exception.

Sensitivity

The higher the value is, the more easily the exception will be detected, and the higher possibility of misinformation would be.

Alarm Delay Times

The device uploads the alarm when the alarm reaches the set number of times.

4. Check the selected diagnosis type, and the related type will be detected.
5. Set arming schedule. See ***Set Arming Schedule*** .
6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.6 Set Audio Exception Detection

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Event and Detection → Audio Exception Detection** .
2. Select one or several audio exception detection types.

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
- The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage methods.
4. Click **Save**.

Note

The function is only supported by certain models. The actual function varies according to different models.

6.7 Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Defocus Detection** .
2. Check **Enable**.
3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
4. For the linkage method settings, refer to ***Linkage Method Settings*** .
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.8 Set Scene Change Detection

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Event and Detection → Scene Change Detection** .
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

Chapter 7 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. **Optional:** Click **Arming Schedule and Linkage Method** in the related event interface.
2. Click **Edit** behind **Arming Schedule**.
3. Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

4. Click **Erase**, and drag the time bar to clear selected valid time.
5. Click **OK** to save the settings.

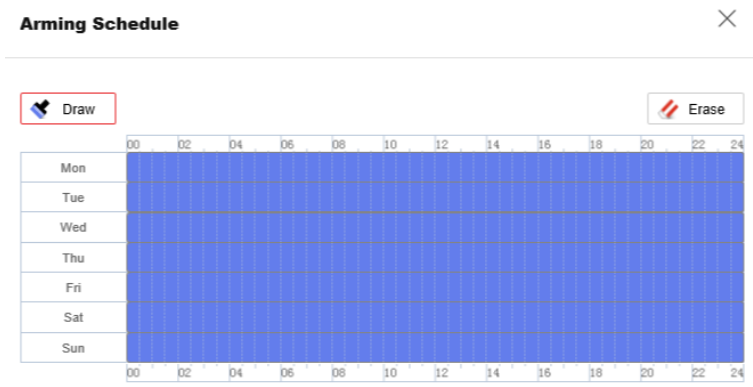


Figure 7-1 Set Arming Schedule

7.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

7.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Output** .
2. Set alarm output parameters.

Automatic Alarm	For the information about the configuration, see ***Automatic Alarm*** .
Manual Alarm	For the information about the configuration, see ***Manual Alarm*** .

Manual Alarm

You can trigger an alarm output manually.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.
2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. **Optional:** Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

7.2.2 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to ***Set FTP*** to set the FTP server.

Refer to ***Set NAS*** for NAS configuration.

Refer to ***Set New or Unencrypted Memory Card*** for memory card storage configuration.

7.2.3 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to ***Set Email*** .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated recipients if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Network Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Event → Alarm Setting → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.
      - When you select **TLS**, and disable STARTTLS, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
      - When you select **TLS** and check **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the **SMTP Port** should be set as 25.

Note

If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Picture**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.

Note

The number of alarm pictures may vary according to different device models and different events.

5) Input the recipient's information, including the recipient's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

7.2.4 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

7.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.

For recording settings, refer to ***Video Recording and Picture Capture*** .

7.2.6 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Alarm Setting → Flashing Alarm Light Output** .
2. Set **Flashing Duration** and **Flashing Frequency**.

Flashing Duration

The time that the flashing lasts when one alarm happens.

Flashing Frequency

The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

3. Set the arming schedule. See ***Set Arming Schedule*** for details.
4. Click **Save**.

Note

Only certain device models support the function.

7.2.7 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Alarm Setting → Audible Alarm Output** .
2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Set → Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

7.2.8 Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Set Alarm Server

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

   Note

   HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

4. Click **Test** to check if the IP or host is available.
5. Click **Save**.

Chapter 8 Network Settings

8.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Network Settings → TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Domain Name Settings

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.

Note

DHCP should be enabled for the dynamic domain name to take effect.

8.2 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name. The DDNS service of the device only supports HTTPS.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to ***TCP/IP*** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Network Settings → DDNS** .
3. Check **Enable** and select **DDNS Type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

8.3 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Network Settings → PPPoE** .
2. Check **Enable**.
3. Set the PPPoE parameters.

   Dynamic IP

   After successful dial-up, the dynamic IP address of the WAN is displayed.

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

   Input your dial-up password again.
4. Click **Save**.
5. Access the device.

   By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

   By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***Access to Device via Domain Name*** for detail information.

8.4 SNMP

You can set the SNMP (Simple Network Management Protocol) to get device information in network management.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration → Network → Network Settings → SNMP** .
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note

The SNMP version you select should be the same as that of the SNMP software.
And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Configure the SNMP settings.
4. Click **Save**.

8.5 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

Go to **Configuration → Network → Network Settings → 802.1X** , and enable the function.

Select protocol and version according to router information. User name and password of server are required.

Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

8.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Network Settings → QoS** .
2. Set **Video/Audio DSCP**, **Event/Alarm DSCP** and **Management DSCP**.

Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

8.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Service → HTTP(S)** .
2. Enter **HTTP Port**.

Note

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter http://192.168.1.64:81 in the browser for login.

3. Check **Enable** in **HTTPS**.

Note

You can click **TLS Settings** to set the TLS version that the device supports. Refer to for details.

4. Enter **HTTPS Port**.
5. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.
7. Set **Web Authentication**.

   Authentication

   Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

   Digest Algorithm

   MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

8. Click **Save**.

8.8 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Network Service → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

8.8.1 Multicast Discovery

Go to **Configuration → Network → Network Settings → TCP/IP** to enable this function.

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

8.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration → Network → Network Service → RTSP** .
2. Enter **Port**.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.

   Audio Port

   The audio port of the selected stream.
4. Set **RTSP Authentication**.

   Authentication

   Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

   Digest Algorithm

   MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to

the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

5. Click **Save**.

8.10 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Network Service → SRTP** .
2. Enter the **Port** number.
3. Set **Multicast** parameters.

   Stream Type

   The stream type as the multicast source.

   Video Port

   The video port of the selected stream.

   Audio Port

   The audio port of the selected stream.
4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.

Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in ***Certificate Management*** .

8.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration → Network → Network Service → Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

8.12 WebSocket(s)

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

Go to **Configuration → Network → Network Service → WebSocket(s)** to set parameters, and click **Save**.

WebSocket

TCP-based full-duplex communication protocol port for plug-in free preview via HTTP protocol.

WebSockets

TCP-based full-duplex communication protocol port for plug-in free preview via HTTPS protocol.

8.13 Port Mapping

By setting port mapping, you can access devices through the specified port.

Steps

1. Go to **Configuration → Network → Network Service → NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

8.13.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note

UPnP™ function on the router should be enabled at the same time.

8.13.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.

2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

8.13.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Severs** , and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

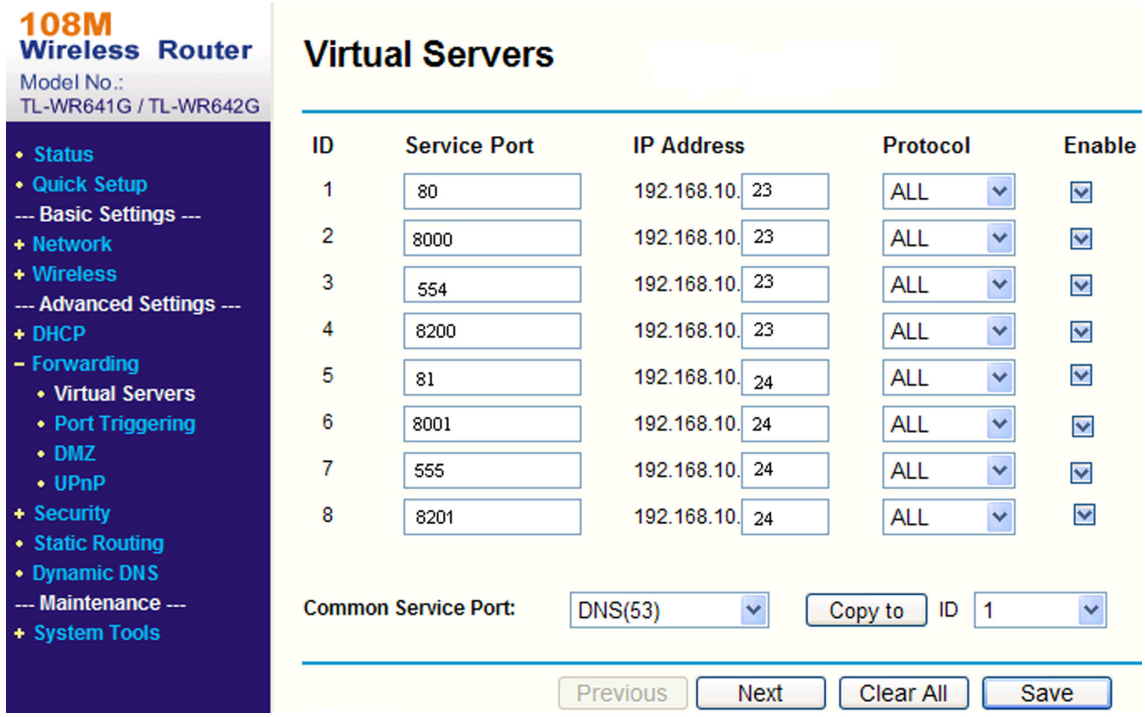


Figure 8-1 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

8.14 RTCP

The device relies on RTCP (Real-time Transport Control Protocol) to deliver packets sequentially to provide a reliable delivery mechanism and to provide services for flow control or congestion control.

Go to **Configuration → Network → Network Service → RTCP** and check **Enable** to enable the function.

8.15 Wireless Dial

Data of audio, video and image can be transferred via 3G/4G wireless network.

Note

The function is only supported by certain device models.

8.15.1 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial** .
2. Check to enable the function.
3. Go to **Dial Parameters** to configure and save the parameters.
4. Click **Settings** behind **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. View the **Dial Status**.

   Click Refresh Refresh the dial status.

   Click Disconnect Disconnect the 3G/4G wireless network.

   When the **Dial Status** turns to **Connected**, it means a successful dial.
6. Access the device via the **IP Address** of the computer in the network.
   - Input the IP address in the browser to access the device.
   - Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

7. **Optional:** You can view 4G SIM card information and network carrier information.

Note

For certain device models working on **Performance Mode** or **Proactive Mode**, the wireless mode can be upgraded. If necessary, please upgrade the wireless mode under the guidance of a professional.

8. **Optional:** Click **Re-Camp** to reconnect the device to wireless network manually. The device will maintain airplane mode for 10 seconds and then connects to network automatically.
9. **Optional:** Check **Enable** to enable **Auto Re-Camp**, and then set the **Re-Camp Interval**. The device will reconnect to the wireless network at set **Re-Camp Interval** automatically.

Note

The function may vary according to different device models.

8.15.2 Wireless Expert Settings

Wireless expert settings provide more details of the 3G/4G wireless network to which the device connects and help the professionals troubleshoot potential network issues.

Cell Radio Frequency Parameters

Cell radio frequency parameters provides the current wireless network information to which the device is connected.

Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** to view cell radio frequency parameters.

Network Info

It displays the current cellular network information. You can click **Refresh** to view the frequency information of different cells.

Radio Frequency Fluctuation

It records the fluctuation of the cellular network to which the device has connected during the past 7 days. Click **Export Report** and set and confirm the encryption password to export the fluctuation report.

Lock Band

You can lock a set of bands that get the device faster data rates to improve the network speed.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings → Lock Band** .
2. Check **Enable**.

3. Click **Add** and enter the band.

Note

- The band you enter should be B + number or N + number. For example, you can enter B1 or N1.
- Up to five bands are supported.

4. **Optional:** Click 🗑 to delete the selected band. You can also click **Clear All** to clear the list.

Capture Baseband Packet

This function can capture the protocol interaction packet to help the professionals to locate the communication failures between 4G module and the base station.

Steps

Note

This function is reserved for the professionals and technical support staff.

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** .
2. Click **Configuration** behind **Capture Baseband Packet** to enter the setting interface.
3. Check **Enable** to enable this function.
4. Set capture duration and the saving path. The saving path depends on the actual storage method of the device. You can click **Delete Captured Packet Under This Path** to delete the captured packet.
5. Click **Save**.
6. Click **Start Capturing Packet** to capture the baseband packet.
7. **Optional:** Click **Stop Capturing** to stop the capturing process.
8. After the capturing is completed, click **Export Captured Packet** to save the report.

Speed Test

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** .
2. Click **Configuration** behind **Speed Test** to enter the setting interface.
3. Select the default server or enter the server address. You can follow the steps below to get the nearby server address.

Note

You can follow the steps below to get the nearby server address.

a. Visit this website to get the nearby server address: ***https://www.speedtest.net/speedtest-servers-static.php*** .
b. Select and copy the URL of the nearby speed test station and paste it in **Server Address**.

4. Click **Speed Test** to start the test.

   You can view the speed details after the test is completed. You can also click **Export Speed Test Result**.

8.16 WLAN AP (Access Point)

The device can be used as a wireless access point with the WLAN AP function. You can connect your phone or PC to the device AP, so as to access to the device and configure the parameters via your phone or PC.

Note

The function is only supported by certain device models.

8.16.1 Set WLAN AP

Steps

1. Go to **Configuration → Network → Network Settings → WLAN AP** .
2. Select the WLAN AP mode.

   On

   The function is enabled.

   Maintenance Mode

   The WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.

   Off

   The function is disabled.
3. Set the related parameters.

   SSID

   For certain device models, the default SSID of the device is named as "Hik-Serial Number".

   For certain device models, the default SSID of the device is named as "Default SSID" on the device label.

   You can define it as needed.

   Security Mode

   WPA2-personal mode is supported.

   Encryption Type

   AES and **TKIP** are selectable.

   Password

The password for wireless connection via the device AP. The default password is the nine-digit serial number of the camera. Please change the default password and set a strong password after logging in for the first time.

Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **Save**.

Note

The function may vary according to different device models.

What to do next

You can connect your mobile phone or PC to the AP.

8.16.2 Access to Device via AP

You can access to the device via the device AP when the device cannot connect to the network.

Steps

1. Go to **Configuration → Network → Network Settings → WLAN AP** to enable WLAN AP function.

   For certain device models, the WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.
2. Search the device WLAN AP in the WLAN list of your phone or PC.
3. Enter the password and connect your mobile phone or PC to the AP.

   Note

   - The AP name is SSID ("Hik-Serial Number" by default). The password is serial number by default. The serial number can be obtained from **Configuration → System → System Settings → Basic Information** .
   - For certain device models, the AP name is the "Default SSID" on the device label.
4. Enter the IP address in the browser.

   Note

   The default IP of the device AP is 192.168.8.1.

Result

The connected devices will be displayed in the **Connected Device** interface.

8.17 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

8.18 Data Monitoring

You can view and manage the SIM card data or wired network data used by the device. SIM card data is the data service provided by network carriers; wired network data is usually provided through a 4G router.

Steps

1. Go to **Configuration → Network → Network Settings → Data Monitoring** .
2. Check **Enable**.
3. Set the following parameters according to your data plan.

   Plan Type

   Daily, **Monthly**, or **Annually** can be selected.

   Data Plan

   Enter the amount of usable data and select the unit.

   Pre-Alarm Threshold

   When the used data reaches the set percentage of data plan, the device sends an alarm message, and shows notification on the OSD or pop-up window.
4. Select **Normal Linkage**.

   If **Send Email** or **Notify Surveillance Center** is selected, the device sends an alarm message by Email or to surveillance center when the used data reaches the threshold.
5. Click **Save**.

Note

The function varies with different device models.

8.19 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.

Note

This function is only supported by certain device models.

8.19.1 Connect Device to Wi-Fi

Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

Steps

1. Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP** .
2. Select **Wlan** to set the parameters. Refer to ***TCP/IP*** for detailed configuration.

   Note

   For stable use of Wi-Fi, it is not recommended to use DHCP.
3. Go to Wi-Fi settings page: **Configuration → Network → Network Service → Wi-Fi** .
4. Set and save the parameters.
   1) Check to enable Wi-Fi function.
   2) Click **Refresh** to view and select the available wireless router or AP, or click + to add it manually.
   3) Select or input a **SSID**, which should be the same as that of wireless router or AP.

      The parameters of the network is automatically shown in **Wi-Fi**.
   4) Select the **Network Mode** as **Manage**.
   5) Select the **Security Mode** according to your needs, and the parameters should be the same as those of the wireless network connection you set on the router or AP.
   6) Click **Save**.

What to do next

Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP** , and click **Wlan** to check the **IPv4 Address** and log in the device.

8.20 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Platform Access → ISUP** .
2. **Optional:** Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.

   Register status turns to **Online** when the function is correctly set.

8.21 Access Camera via Hik-Connect

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Before You Start

Connect the camera to network with network cables.

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.
4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

   For detailed information, refer to the user manual of the Hik-Connect app.

8.21.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start
You need to activate the camera before enabling the service.

Steps
1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Platform Access → Hik-Connect** .
3. Check **Enable**.
4. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
5. Create a verification code or change the old verification code for the camera.

   Note
   The verification code is required when you add the camera to Hik-Connect service.
6. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps
1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.

   Note
   The verification code is required when you add the camera to Hik-Connect service.
5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

8.21.2 Set Up Hik-Connect

Steps
1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

8.21.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the result interface.

Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

   For detailed information, refer to the user manual of the Hik-Connect app.

8.22 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Platform Access → Open Network Video Interface** .
2. Check **Enable**.
3. Select an authentication mode.
   - If you select **Digest**, the device only supports digest authentication.
   - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.
4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. **Optional:** Repeat the steps above to add more Open Network Video Interface users.
7. **Optional:** Manage the user.
   - Click 🗑 to delete the selected Open Network Video Interface user.
   - Click ✎ to modify the selected Open Network Video Interface user.

8.23 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

Steps

1. Go to **Configuration → Network → Platform Access → SDK Service** .
2. Set **SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK protocol.
   2) Enter the **Port** number.
3. Set **Enhanced SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK over TLS protocol.
   2) **Optional:** Click **TLS Settings** to enable the TLS version that the device supports. Refer to ***TLS*** for details.
   3) Enter the **Port** number.
   4) Select a server certificate to make sure the data transmission security. You can click **Certificate Management** to add a certificate. Refer to ***Certificate Management*** for details.
4. Click **Save**.

Chapter 9 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

9.1 System Settings

9.1.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

9.1.2 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select **Manual Time Sync.**.
4. Choose one time synchronization method.
   - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
   - Click **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.

3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.

Note

Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

1. Enter **Configuration → System → System Settings → Time Settings** .
2. Select **Satellite Time Sync.**.
3. Set **Interval**.
4. Click **Save**.

Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Check **Enable**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

9.1.3 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-232** .
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

9.1.4 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start
Connect the device and computer or terminal with RS-485 cable.

Steps
1. Go to **Configuration → System → System Settings → RS-485** .
2. Set the RS-485 parameters.

   Note
   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

9.1.5 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximum live view that can be streamed at the same time.

Enter **Configuration → System → System Settings → System Service** to set the upper limit of the remote connection number.

9.1.6 Location Settings

Location displays and uploads the current longitude and latitude of the device.

Auto Uploading

Check **Enable** and set **Location Upload Interval**.

The device will upload its location at the set interval. You can also click **Refresh** to upgrade the device location manually.

Manual Settings

Check **Enable** and set **Location Upload Interval**. Enter the longitude and latitude of the device and click **Save**.

The device will upload the set location at the set interval.

Note
This function may vary according to different device models.

9.1.7 External Device

For the device supporting external devices, including the supplement light, wiper on the housing, the LED light, and heater, you can control them via the Web browser when it is used with the housing. External devices vary with models.

Operate Wiper

For the device that has a wiper, you can control the wiper via web browser.

Before You Start

- Make sure your device supports wiper.
- Wiper operation and settings vary according to device models.

Steps

1. Go to **Configuration → System → System Settings → External Device**.
2. Select a wiper mode.

   Cleaning Mode:

   - When **Cleaning Mode** is selected as **Auto**, the device determines whether to clean based on image abnormalities caused by the issues including dirty lenses, water droplets on the window viewport, etc.
   - In **Auto** mode, the maximum number of cleaning times is 4 times in 24 hours.
   - **Threshold**: Set the threshold value to judge the degree of dirtiness based on the complexity of the image texture to determine whether to clean or not.

   Note

   - For the device with water box, the cleaning mode is used to clean the sand and dust from the lens window by spraying water and wiping in dry and rainless areas.
   - As for cleaning, the water box automatically sprays water for 2 seconds before the wipers start working. The water spray from the water box lasts for 10 seconds and the wiper wipes 5 times.

Normal Mode: Only For Wiping	You can set **Manual Wiper Times**, and the wiper wipes the set manual wiper times when you click on live view page.
Cleaning Mode: Timed Cleaning	The wiper works on schedule and the water box (if supported) sprays water for cleaning at set wiping interval. Check **Enable Timed Cleaning** and set **Timed Cleaning Cycle (day(s))**. If the cycle is set to ***7*** days, the device will clean at 2:00 AM after 7 days, and then clean once every 7 days.
Cleaning Mode:	**For the device with water box:**

Manual Cleaning

- Click **Clean**, and the water box automatically sprays water for 2 seconds before the wipers start working. The water spray from the water box lasts for 10 seconds and the wiper wipes 5 times.
- You can also click on live view page for manual cleaning or test.

For the device without water box:

- Click **Clean** to test the wiper function, and the wiper wipes.

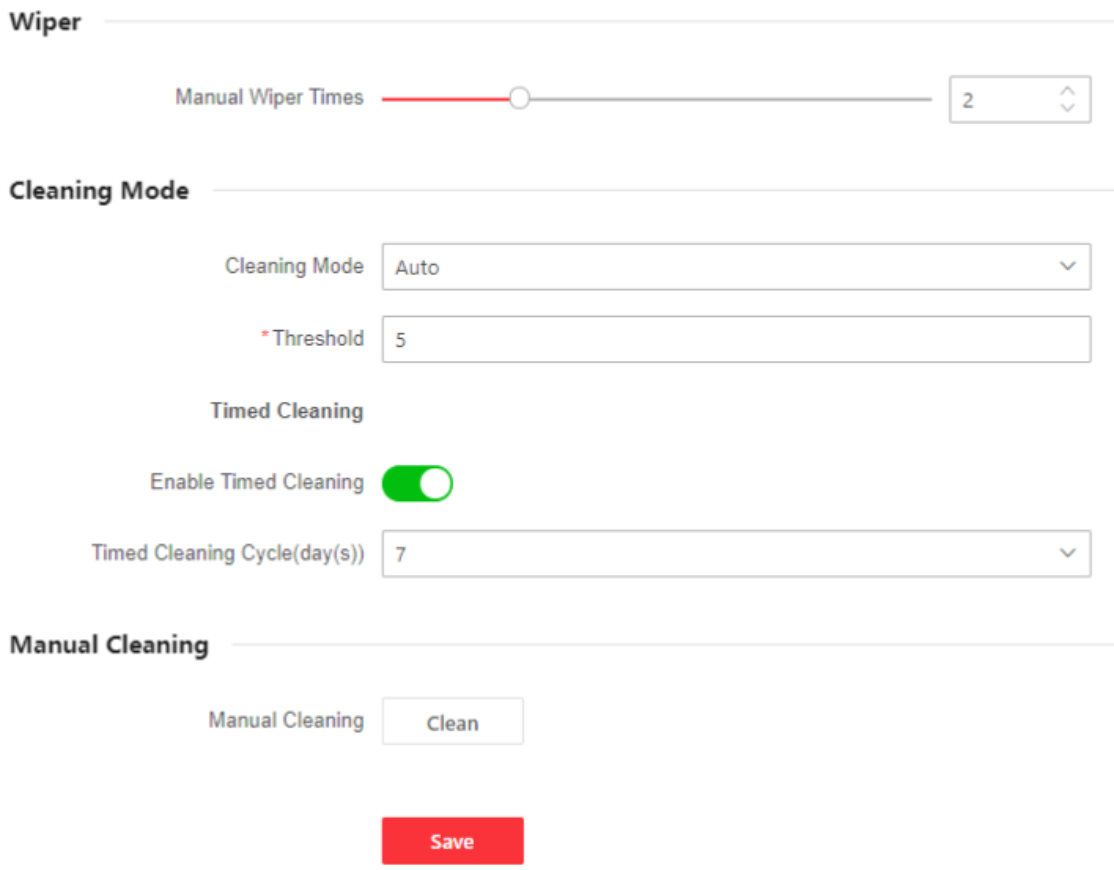


Figure 9-1 Operate Wiper

3. Click **Save**.

Set Fan

For the device with a fan for removing dust and water vapor, you can set the fan mode.

Before You Start

- Make sure your device supports fan.
- Fan operation and settings vary according to device models.

Steps

1. Go to **Configuration → System → System Settings → External Device** .
2. Select a fan mode.

Close	The fan function is disabled.
Manual	You can set the wind speed level for the fan.
Auto	The wind speed changes according to the concentration of the dust and water vapor.

3. Click **Save**.

9.1.8 View Open Source Software License

On the top-right corner, click ⓘ and select **Open Source Software Description** to download the license. You can view the license in the editor.

9.2 Wiegand

Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

9.3 User and Account

9.3.1 Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management** .
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.

User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click ✎ to change the password and permission.

Delete Select a user and click 🗑 .

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

9.3.2 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management → Online Users** , click **General**, and set **Simultaneous Login**.

9.3.3 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

9.4 Maintenance

9.4.1 Restart

You can restart the device via browser.

Go to **Maintenance and Security → Maintenance → Restart** , and click **Restart**.

9.4.2 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

DO NOT disconnect power during the process, and the device restarts automatically after upgrade.

Steps

1. Go to **Maintenance and Security → Maintenance → Upgrade** .
2. Choose one method to upgrade.

Firmware	Locate the exact path of the upgrade file.
Firmware Directory	Locate the directory which the upgrade file belongs to.

3. Click to select the upgrade file.
4. Click **Upgrade**.

9.4.3 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Maintenance and Security → Maintenance → Backup and Restore** .
2. Click **Restore** or **Default** according to your needs.

Restore	Reset device parameters, except user information, IP parameters and video format to the default settings.
Default	Reset all the parameters to the factory default.

Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

9.4.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Steps

1. Export configuration file.
   1) Go to **Maintenance and Security → Maintenance → Backup and Restore → Backup** .
   2) Click **Export** and input the encryption password to export the current configuration file.
   3) Set the saving path to save the configuration file in local computer.

2. Import configuration file.
   1) Access the device that needs to be configured via web browser.
   2) Go to **Maintenance and Security → Maintenance → Backup and Restore → Reset** .
   3) Click 🗀 to select the saved configuration file.
   4) Input the encryption password you have set when exporting the configuration file.
   5) Click **Import**.

9.4.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Maintenance and Security → Maintenance → Log** .
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files in your computer.

9.4.6 Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps

Note

This function is only supported by certain camera models.

1. Go to **Maintenance and Security → Maintenance → Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

9.4.7 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Maintenance and Security → Maintenance → Device Debugging** , and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

9.4.8 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Maintenance and Security → Maintenance → Device Debugging → Diagnose Information** . Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

9.4.9 Diagnosis

For the device that supports 4G network, diagnosis can help get the communication packet and the device power and network information for future maintenance and troubleshooting.

Capture Device Packet

This function is reserved for the professionals and is used to get the communication packet between the device and the external device for future problem diagnosis and debugging.

Steps

Note

This function is reserved for the professionals and technical support staff.

1. Go to **Maintenance and Security → Maintenance → Device Debugging** , and click **Settings** of **Capture Device Packet**.
2. Check **Enable** to enable this function.

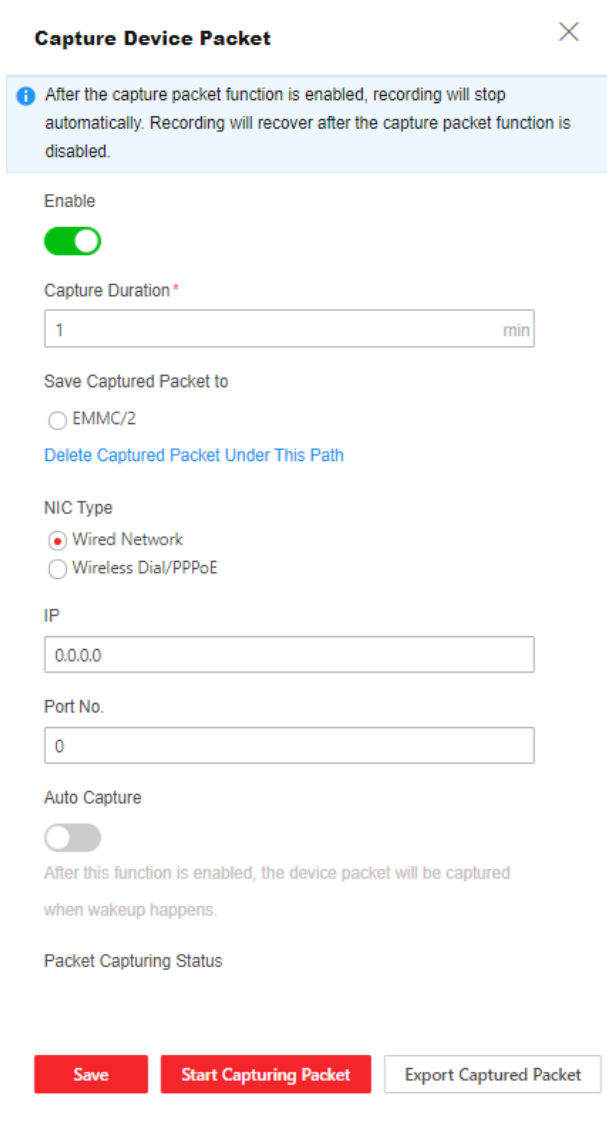


Figure 9-2 Capture Device Packet

3. Set **Capture Duration** according to your need.
4. Select the packet saving path.

Note

a. The saving path option is subject to the actual storage method of the device.
b. You can click **Delete Captured Packet Under This Path** to delete the saved packet file(s).

5. Set NIC type, IP, and port.
6. **Optional:** You can select **Auto Capture** and the device packet will be captured when wakeup happens.
7. Click **Save**.
8. Click **Start Capturing Packet**.

9. After the capturing is completed, click **Export Captured Packet** to save the report.

Export Device Info

Go to **Maintenance and Security → Maintenance → Device Debugging → Export Device Info** , you can click **Export** to export device information, such as voltage, current, power, 4G data.

9.5 Security

You can improve system security by setting security parameters.

9.5.1 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Maintenance and Security → Security → IP Address Filter** .
2. Check **Enable**.
3. Select the type of IP address filter.

   Blocklist IP addresses in the list cannot access the device.

   Allowlist Only IP addresses in the list can access the device.
4. Edit the IP address filter list.

   Add Add a new IP address or IP address range to the list.

   Modify the selected IP address or IP address range in the list.

   Delete the selected IP address or IP address range in the list.
5. Click **Save**.

9.5.2 Set MAC Address Filter

MAC address filter is a tool for access control. You can enable the MAC address filter to allow or forbid the visits from the certain MAC addresses.

Steps

1. Go to **Maintenance and Security → Security → MAC Address Filter** .
2. Check **Enable**.
3. Select the type of MAC address filter.

   Blocklist MAC addresses in the list cannot access the device.

Allowlist Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

   Add Add a new MAC address to the list.

   Modify the selected MAC address in the list.

   Delete the selected MAC address in the list.

5. Click **Save**.

9.5.3 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Maintenance and Security → Security → Login Management → Control Timeout Settings** to complete settings.

9.5.4 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Note

The function is only supported by certain device models.

Server Certificate/Client Certificate

Note

The device has default self-signed server/client certificate installed. The certificate ID is ***default***.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.

   Note

   The input certificate ID cannot be the same as the existing ones.

4. Click **Save** to save and install the certificate.

   The created certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain functions, the function name is shown in the column **Functions**.

5. **Optional:** Click **Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start

Create a self-signed certificate first. See ***Create and Install Self-signed Certificate*** for instructions.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Select a self-signed certificate from the **Server/Client Certificate** list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.

   The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
   1) Click **Import**.
   2) Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existed ones.

   3) Click to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **Save**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.
9. **Optional:** Click **Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Click **Import** in the **Server/Client Certificate** list.

3. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existed ones.

4. Click 🗀 to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key	If your certificate has an independent key, select this option. Browse to select the private key and input the private-key password.
PKCS#12	If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **Save**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Click **Import** in the **CA Certificate** list.
3. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existing ones.

4. Click 🗀 to select the certificate file.
5. Click **Save**.

   The imported certificate is displayed in the **CA Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the **Functions** column.

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.

Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.5.5 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security → Security → TLS** , and enable the desired TLS protocol. Click **Save**.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

Chapter 10 VCA Resource

VCA resource is a collection of smart functions supported by the device.

10.1 Set Open Platform

HEOP (Hikvision Embedded Open Platform) allows you to install the application for the third-party to develop and run its function and service. For the device supporting HEOP, you can follow the steps to import and run smart applications.

Steps

1. Go to **VCA** interface.

   Note

   Before installing the application, make sure that the application you want to install fits the following conditions.

   - Each application has its own exclusive name.
   - The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
   - The memory and computing power of the application is less than that available memory and computing power of the device.

2. Click **Import Application** and browse your local path to select an application package and import.
3. Click **Import License** and browse your local path to select a license file and import.
4. **Optional:** Set application.

Click	Enable or disable the application.
Click	Delete the application.
Click	Export log.
Click	Browse a local path and import an application package to update the application.
Click **Import License**	Import the license from the local path.
Click **Check Update**	Check for updates.
Click **Upgrade**	Upgrade applications that need upgrades
Click **Get Application**	Check for online applications that can be installed.

Click **Clear Memory**	Clear memory fragmentation and free up more memory to enable more smart applications.
View details	Select an application and click on it to show the details on the page.

Note

Only devices connected to the network support **Check Update** and **Get Application**.

10.2 General Settings

Set the general parameters which are related to the smart applications.

Go to **VCA → Set Application → General Settings** to set the following parameters.

Camera Info.

For camera information settings, refer to ***Set Camera Info*** .

FTP

For FTP settings, refer to ***Set FTP*** .

Email

For Email settings, refer to ***Set Email*** .

Alarm Output

For alarm output settings, refer to ***Automatic Alarm*** .

Audible Alarm Output

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Alarm Server

For alarm server settings, refer to ***Alarm Server*** .

Metadata

For metadata settings, refer to ***Metadata*** .

10.2.1 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go to **VCA → Set Application → General Settings → Camera Info.** to set **Device No.** and **Camera Info.**.

10.2.2 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **VCA → Set Application → General Settings → metadata Settings** to enable metadata uploading of the desired function.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

10.3 Smart Event

Note

- For certain device models, you need to enable the smart event function on **VCA** page first to show the function configuration page.
- The function varies according to different models.

10.3.1 Set Intrusion Detection

It is used to detect objects entering and loitering in a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Detection Target

   This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missed.

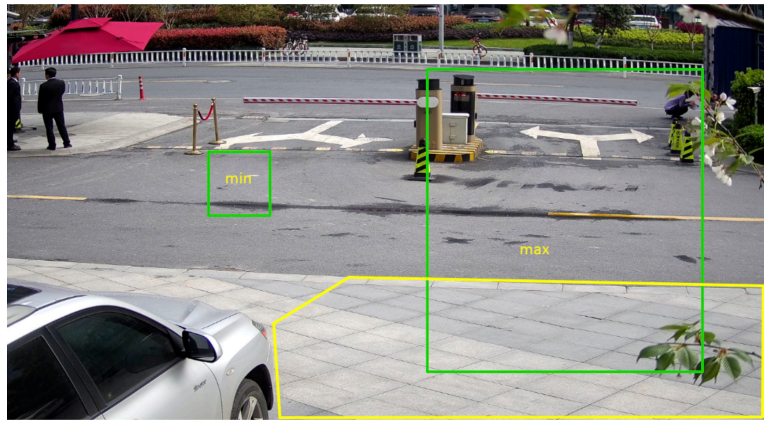


Figure 10-1 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

10.3.2 Set Line Crossing Detection

It is used to detect objects crossing a predefined virtual line. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection line. Click and a line with an arrow appears in the live view. Drag the line to the location on the live view as desired.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Direction

It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

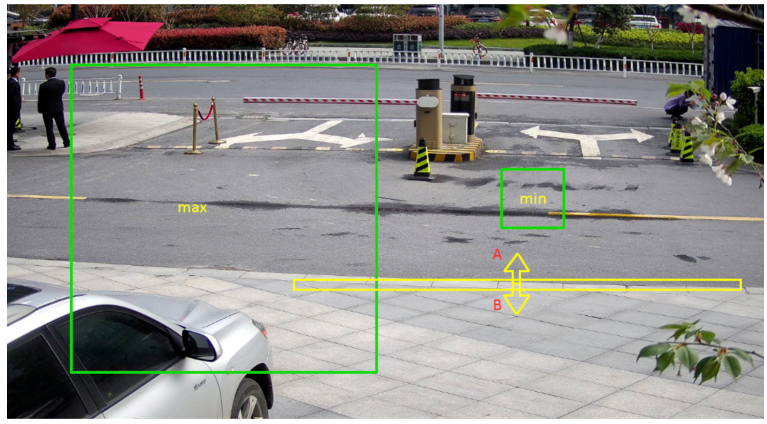


Figure 10-2 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

10.3.3 Set Region Entrance Detection

It is used to detect objects entering a predefined virtual region from the outside place. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Detection Target

   This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

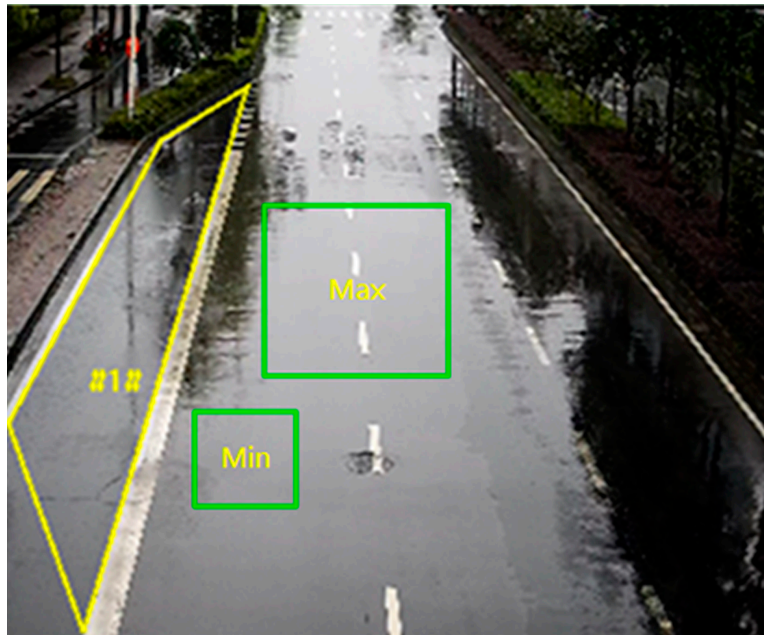


Figure 10-3 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

10.3.4 Set Region Exiting Detection

It is used to detect objects exiting from a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Detection Target

   This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

   Note

   This function is only available for certain device models under certain settings. Please refer to the actual settings.

   Sensitivity

   It stands for the percentage of the body part of an acceptable target that goes across the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Target Validity

   If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

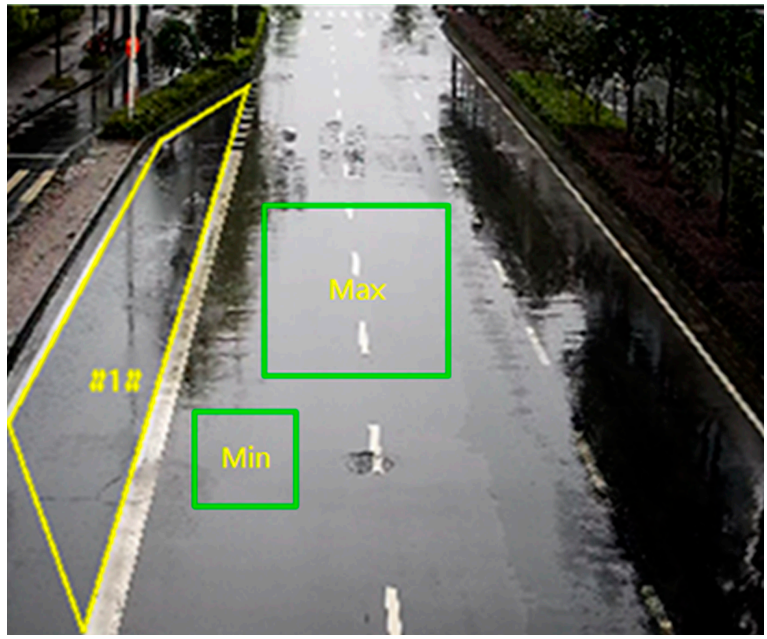


Figure 10-4 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

10.3.5 Set Unattended Baggage Detection

It is used to detect the objects left over in the predefined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Before You Start

Go to **VCA → Select Application** , select **Smart Event** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold

It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

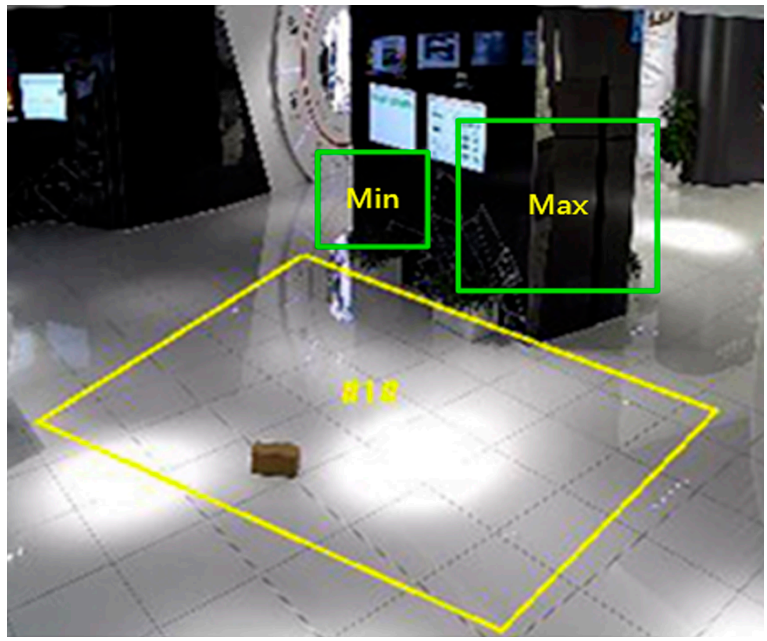


Figure 10-5 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.3.6 Set Object Removal Detection

It detects whether the objects are removed from the predefined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Before You Start

Go to **VCA → Select Application** , select **Smart Event** and click **Next** to enable the function.

Steps

1. Go to **VCA → Set Application → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set parameters.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

   Threshold

   The threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.
5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, see ***Set Arming Schedule*** . For the linkage method settings, see ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.3.7 Set Loitering Detection

It detects whether there is any target loitering in a predefined area. If the time that the target loiters in the set region reaches the set threshold, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Loitering Detection** .
2. Check **Enable**.

3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set rules.

   Threshold

   Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

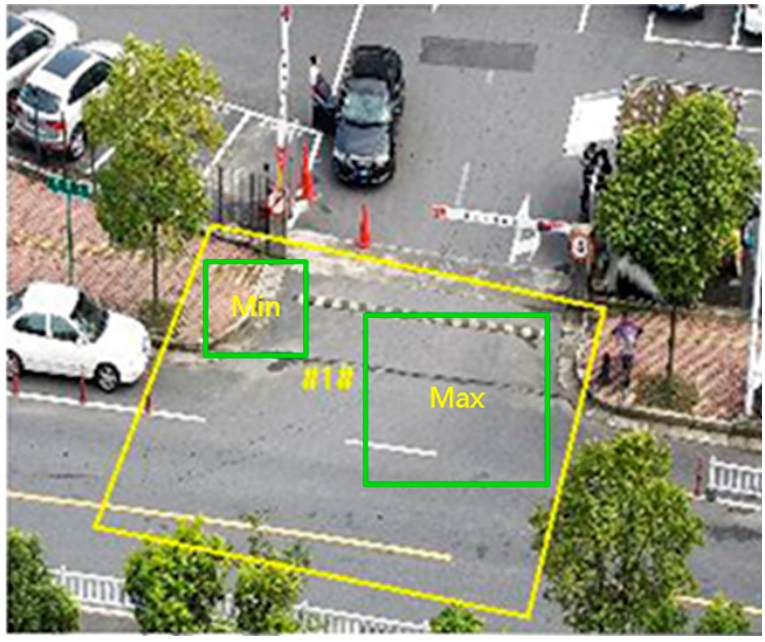


Figure 10-6 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.3.8 Set People Gathering Detection

It detects the people density in a predefined area. If the people density exceeds the set percentage, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → People Gathering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) **Optional:** Click to delete all the setting areas.
4. Set rules.

   Percentage

   It stands for the percentage of people in the predefined area. When the people percentage in the live view exceeds the set value, the device will trigger an alarm.

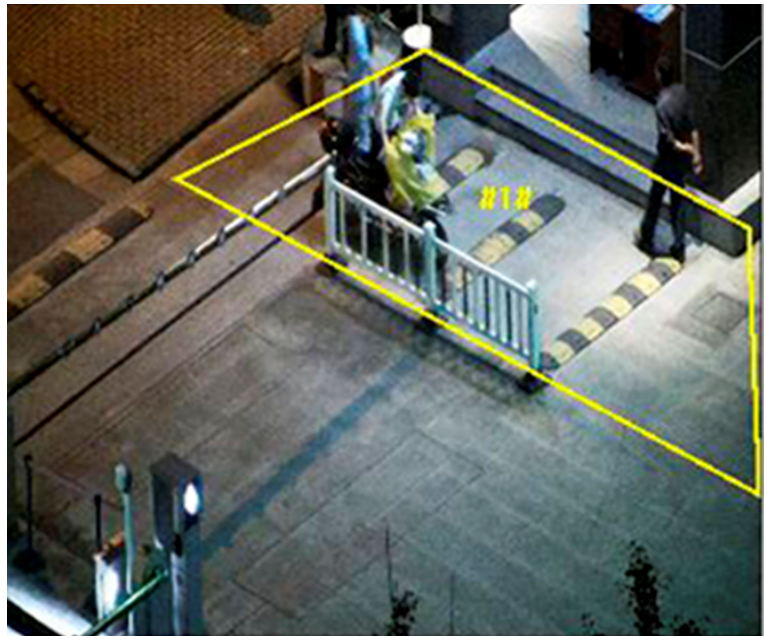


Figure 10-7 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings***
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.3.9 Set Fast Moving Detection

When there are targets moving at a high speed in a predefined area, the device will take linkage actions and trigger an alarm.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Fast Moving Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
   2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
   3) **Optional:** Click to delete all the setting areas.
4. Set Rules.

   Sensitivity

   Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Figure 10-8 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.3.10 Set Parking Detection

It detects parking violation in a predefined area. When the parking time exceeds a set threshold, the device can take linkage actions. It is applicable in expressway and one-way street.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Parking Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
   1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click and , then drag the mouse in the live view to draw the minimum and maximum target size.
3) **Optional:** Click to delete all the setting areas.

4. Set rules.

Threshold

Threshold stands for the threshold for the parking time in the region. If the parking time exceeds the threshold, an alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target part that goes across the pre-defined region. ST stands for the complete target. The higher the value of sensitivity is, the more easily the alarm can be triggered.

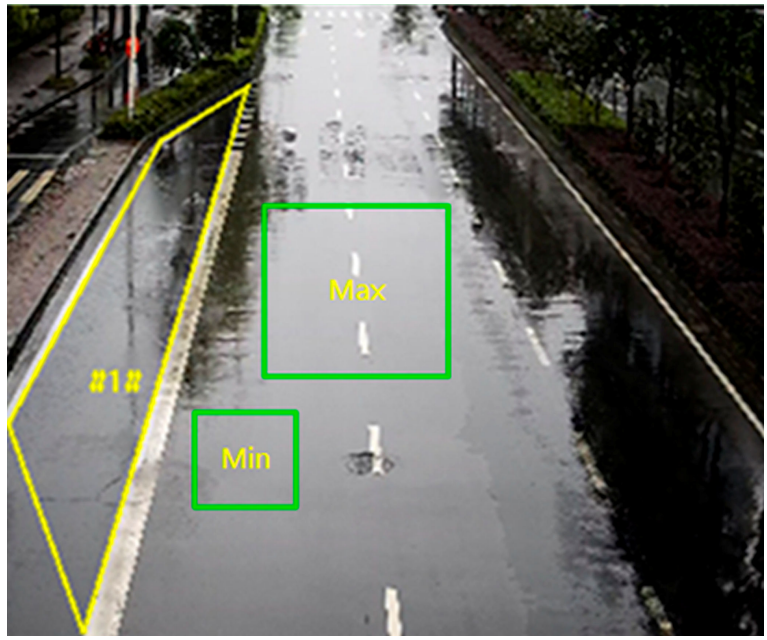


Figure 10-9 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings***

7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

10.4 Schedule Switch Application

Set the corresponding applications in multiple time periods.

Before You Start

Go to **VCA** , select the application and set the related detection rules and parameters.

Steps

1. Go to **VCA → Select Application** . For the device supporting HEOP, go to **VCA** for the setting. Click **Scheduled-Switch** to set the schedule for switching the application.
2. Check **Scheduled-Switch** to enable the function.
3. Click to select an application to set the schedule.
4. Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

5. Click **Erase**, and drag the time bar to clear selected valid time.
6. Click **OK** to save the settings.

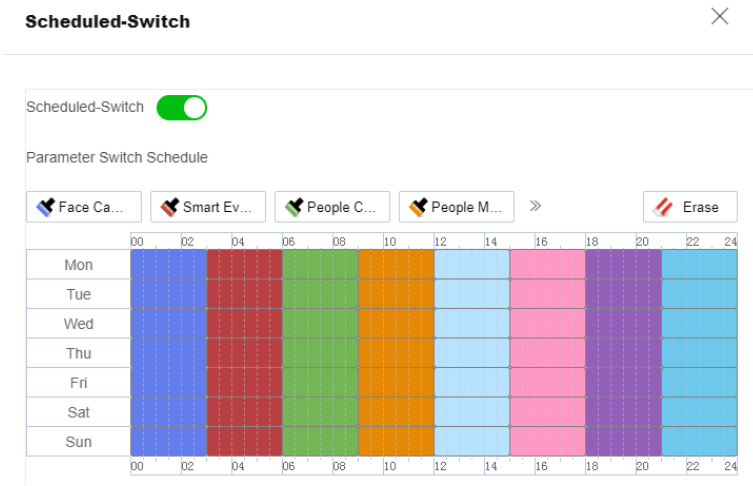


Figure 10-10 Set Application Scheduled-Switch

Result

The device will execute the corresponding application in the set time period.

10.5 Search and Export Data Aware Information

The data aware function is used to search and export the data of the restart, arming and capture alarm statistics.

Before You Start
Log in to the device via admin user account.

Steps
1. Go to **Application Display → Data Aware** .
2. Select the search condition.

Statistics Type	Options
Restart Records	Type of restarting, start time and end time.
Arming	Arming type, start time and end time.
Capture Alarm Statistics	Report type, alarm target, protocol, arming IP address and start time.
Alarm Quality Statistics	Report type, alarm target and start time.

3. Click **Search**.
   The data information that match the conditions will be displayed.
4. **Optional:** Click **Export** to save the data information to the local device.

10.6 Search and View Power Consumption Statistics

Before You Start
Log in to the device with an administrator account or an operator account with remote configuration permission.

Steps
1. Go to **Application Display → Power Statistics** .
2. Set the search condition. Select **Statistics Type**, **Report Type** and **Time**.
3. Click **Search**.

Result

When you select **Power Consumption** as **Statistics Type**, the power consumption information that match the conditions will be displayed.

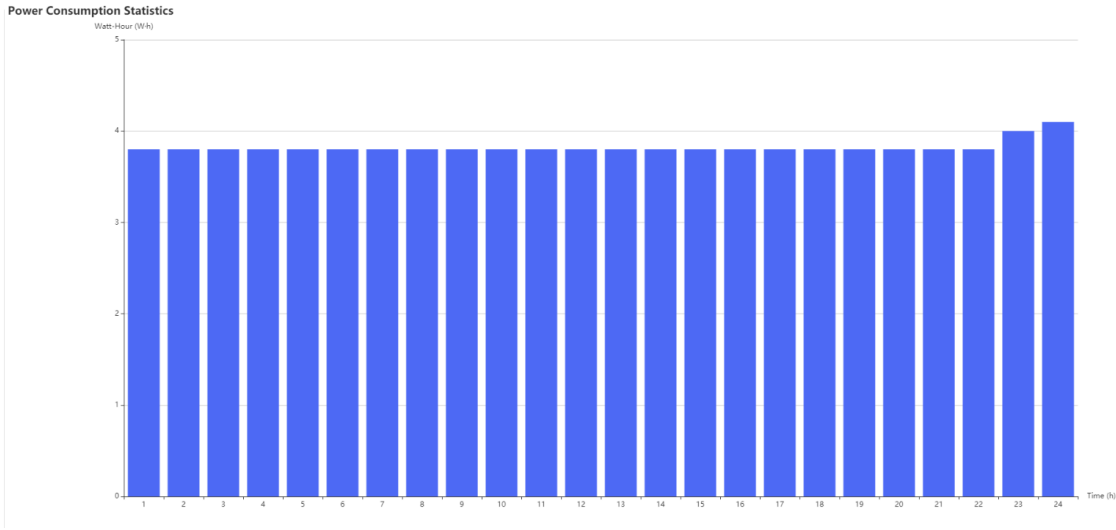


Figure 10-11 Power Consumption Statistics

Chapter 11 Smart Display

This function displays real time pictures captured by smart functions and analyzes the target in real time.

Go to **Application Display → Display Alarm** to view the real-time images. Click to go back to **Application Display**.

Note

- To use this function, you should first enable and configure certain smart functions.
- To use this function, your web browser version should be above IE11.0.9600.17843.

Live View Parameter

Icon	Function
	Capture a picture.
	Start or stop recording.
	Mute.
50	Adjust the volume of live view. Move the slider to right to turn up the volume and left to turn down the volume. Move to the left end to mute the live view.

Download Display Pictures

Click and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click again to download the pictures in a package.

Note

The browser cache has a limited size. The recommended number of pictures to download is no more than 200.

Layout

Click and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

Detect Feature

Click and choose **Detect Feature**. Check the corresponding checkbox to display the features of the detection target.

Chapter 12 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure your device supports the **Third Stream**. Third stream and EPTZ should be both enabled simultaneously.

Note

The function is only supported by certain device models.

12.1 Patrol

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Patrol** in **Application Mode**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

12.2 Auto-Tracking

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Auto-tracking** in **Application Mode**.
5. Click to start drawing. Click on the live view video to specify the four vertexes of the detection area, and right click to complete drawing.
6. Set rules.

   Detection Target

   Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.

   Note

   Only certain camera models support this function.

   Sensitivity

It stands for the percentage of the body part of an acceptable target that is tracked. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

7. Click **Save**.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.

See Far, Go Further