# Network Camera

## User Manual

# Initiatives on the Use of Video Products

## Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

## Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

# Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

## About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website ( ***https://www.hikvision.com/*** ).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

## Trademarks

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.

## Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

# Update Firmware

For better user experience, we recommend you to update your device to the latest firmware asap.

Please get the latest firmware package from the official website or the local technical expert. For more information, please visit the official website: ***https://www.hikvision.com/en/support/download/firmware/*** .

For the upgrading settings, refer to ***Upgrade*** .

# 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

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

## Laws and Regulations

- The device should be used in compliance with local laws, electrical safety regulations, and fire prevention regulations.

## Electricity

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Provide a surge suppressor at the inlet opening of the equipment under special conditions such as the mountain top, iron tower, and forest.
- CAUTION: To reduce the risk of fire, replace only with the same type and rating of fuse.
- The equipment must be connected to an earthed mains socket-outlet.
- An appropriate readily accessible disconnect device shall be incorporated external to the equipment.
- An appropriate overcurrent protective device shall be incorporated external to the equipment, not exceeding the specification of the building.
- An all-pole mains switch shall be incorporated in the electrical installation of the building.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.

## Battery

- Do not ingest battery. Chemical burn hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
- ATTENTION: IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS.

- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.

## Fire Prevention

- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The serial port of the equipment is used for debugging only.

## Hot Surface Prevention

-

CAUTION: Hot parts! Burned fingers when handling the parts. Wait one-half hour after switching off before handling parts. This sticker is to indicate that the marked item can be hot and should not be touched without taking care. For device with this sticker, this device is intended for installation in a restricted access location, access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken.

## Installation

- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.

## Power Supply

- The input voltage should conform to IEC60950-1 standard: SELV (Safety Extra Low Voltage) and the Limited Power Source. Refer to the appropriate documentation for detailed information.
- The power source should meet limited power source or PS2 requirements according to IEC 60950-1 or IEC 62368-1 standard.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- Make sure the plug is properly connected to the power socket.

## White Light Illuminator (If supported)

- Possibly hazardous optical radiation emitted from this product.
- DO NOT stare at operating light source. May be harmful to the eyes.
- Wear appropriate eye protection or DO NOT turn on the white light when you assemble, install or maintain the camera.

## Transportation

- Keep the device in original or similar packaging while transporting it.

## System Security

- The installer and user are responsible for password and security configuration.

## Maintenance

- If the product does not work properly, please contact your dealer or the nearest service center.
- We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.

## Cleaning

- Please use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.

## Using Environment

- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
- DO NOT expose the device to high electromagnetic radiation or dusty environments.
- For indoor-only device, place it in a dry and well-ventilated environment.
- DO NOT aim the lens at the sun or any other bright light.
- Make sure the running environment meets the requirement of the device. The operating temperature shall be -30 °C to 60 °C (-22 °F to 140 °F), and the operating humidity shall be 95% or less (no condensing).
- DO NOT place the camera in extremely hot, cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.

## Emergency

- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

## Time Synchronization

- Set up device time manually for the first time access if the local time is not synchronized with that of the network. Visit the device via Web browse/client software and go to time settings interface.

## Reflection

- Make sure that no reflective surface is too close to the device lens. The IR light from the device may reflect back into the lens causing reflection.

# 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 Enable and Disable Live View ..... 6

3.1.2 Adjust Aspect Ratio ..... 6

3.1.3 Live View Stream Type ..... 6

3.1.4 Select the Third-Party Plug-in ..... 6

3.1.5 Window Division ..... 7

3.1.6 Light ..... 7

3.1.7 Count Pixel ..... 7

3.1.8 Start Digital Zoom ..... 7

3.1.9 Auxiliary Focus ..... 7

3.1.10 Lens Initialization ..... 8

3.1.11 Quick Set Live View ..... 8

3.1.12 Lens Parameters Adjustment ..... 8

3.1.13 Conduct 3D Positioning ..... 9

3.2 Set Transmission Parameters ..... 9

3.3 Set Smooth Streaming ..... 10

**Chapter 4 Video and Audio ..... 12**

4.1 Video Settings ..... 12
4.1.1 Stream Type ..... 12
4.1.2 Video Type ..... 13
4.1.3 Resolution ..... 13
4.1.4 Bitrate Type and Max. Bitrate ..... 13
4.1.5 Video Quality ..... 13
4.1.6 Frame Rate ..... 14
4.1.7 Video Encoding ..... 14
4.1.8 Smoothing ..... 16
4.2 ROI ..... 16
4.2.1 Set ROI ..... 16
4.2.2 Set Face Tracking ROI ..... 17
4.2.3 Set Target Tracking ROI ..... 17
4.2.4 Set License Plate Tracking ROI ..... 18
4.3 Display Info. on Stream ..... 18
4.4 Audio Settings ..... 18
4.4.1 Audio Encoding ..... 18
4.4.2 Audio Input ..... 19
4.4.3 Audio Output ..... 19
4.4.4 Environmental Noise Filter ..... 19
4.5 Two-way Audio ..... 19
4.6 Display Settings ..... 20
4.6.1 Scene Mode ..... 20
4.6.2 Image Parameters Switch ..... 23
4.6.3 Video Standard ..... 24
4.6.4 Local Video Output ..... 24
4.7 OSD ..... 24
4.8 Set Privacy Mask ..... 25

4.9 Overlay Picture ..... 25
4.10 Set Target Cropping ..... 25
**Chapter 5 Video Recording and Picture Capture ..... 27**
5.1 Storage Settings ..... 27
5.1.1 Set New or Unencrypted Memory Card ..... 27
5.1.2 Set FTP ..... 29
5.1.3 Set NAS ..... 30
5.1.4 eMMC Protection ..... 30
5.1.5 Set Cloud Storage ..... 31
5.2 Video Recording ..... 31
5.2.1 Record Automatically ..... 31
5.2.2 Record Manually ..... 33
5.2.3 Set Lite Storage ..... 33
5.2.4 Playback and Download Video ..... 33
5.3 Capture Configuration ..... 34
5.3.1 Capture Automatically ..... 34
5.3.2 Capture Manually ..... 35
5.3.3 Set Timing Wake ..... 35
5.3.4 View and Download Picture ..... 35
**Chapter 6 Event and Alarm ..... 37**
6.1 Basic Event ..... 37
6.1.1 Set Motion Detection ..... 37
6.1.2 Set Video Tampering Alarm ..... 39
6.1.3 Set PIR Alarm ..... 40
6.1.4 Set Exception Alarm ..... 41
6.1.5 Set Alarm Input ..... 41
6.1.6 Set Video Quality Diagnosis ..... 42
6.1.7 Set Vibration Detection ..... 42

6.2 Smart Event ..... 43
6.2.1 Detect Audio Exception ..... 43
6.2.2 Set Defocus Detection ..... 44
6.2.3 Detect Scene Change ..... 44
6.2.4 Set Face Detection ..... 44
6.2.5 Set Video Loss ..... 45
6.2.6 Set Intrusion Detection ..... 45
6.2.7 Set Line Crossing Detection ..... 46
6.2.8 Set Region Entrance Detection ..... 48
6.2.9 Set Region Exiting Detection ..... 49
6.2.10 Set Unattended Baggage Detection ..... 50
6.2.11 Set Object Removal Detection ..... 51
6.2.12 Draw Area ..... 51
6.2.13 Set Size Filter ..... 52
**Chapter 7 Network Settings ..... 53**
7.1 TCP/IP ..... 53
7.1.1 Multicast ..... 54
7.1.2 Multicast Discovery ..... 55
7.2 SNMP ..... 55
7.3 Set SRTP ..... 55
7.4 Port Mapping ..... 56
7.4.1 Set Auto Port Mapping ..... 56
7.4.2 Set Manual Port Mapping ..... 56
7.4.3 Set Port Mapping on Router ..... 57
7.5 Port ..... 58
7.6 Access to Device via Domain Name ..... 59
7.7 Access to Device via PPPoE Dial Up Connection ..... 59
7.8 Wireless Dial ..... 60

7.8.1 Set Wireless Dial ..... 60
7.8.2 Set Allowlist ..... 61
7.9 Wi-Fi ..... 61
7.9.1 Connect Device to Wi-Fi ..... 61
7.10 Set Network Service ..... 62
7.11 Set Open Network Video Interface ..... 63
7.12 Set ISUP ..... 63
7.13 Set Alarm Server ..... 64
7.14 Access Camera via Hik-Connect ..... 64
7.14.1 Enable Hik-Connect Service on Camera ..... 65
7.14.2 Set Up Hik-Connect ..... 66
7.14.3 Add Camera to Hik-Connect ..... 67
**Chapter 8 Arming Schedule and Alarm Linkage ..... 68**
8.1 Set Arming Schedule ..... 68
8.2 Linkage Method Settings ..... 68
8.2.1 Trigger Alarm Output ..... 68
8.2.2 FTP/NAS/Memory Card Uploading ..... 69
8.2.3 Send Email ..... 70
8.2.4 Notify Surveillance Center ..... 71
8.2.5 Trigger Recording ..... 71
8.2.6 Flashing Light ..... 71
8.2.7 Audible Warning ..... 71
**Chapter 9 System and Security ..... 73**
9.1 View Device Information ..... 73
9.2 Search and Manage Log ..... 73
9.3 Simultaneous Login ..... 73
9.4 Import and Export Configuration File ..... 73
9.5 Export Diagnose Information ..... 74

9.6 Reboot ..... 74
9.7 Restore and Default ..... 74
9.8 Upgrade ..... 74
9.9 View Open Source Software License ..... 75
9.10 Wiegand ..... 75
9.11 Metadata ..... 75
9.12 Time and Date ..... 75
9.12.1 Synchronize Time Manually ..... 75
9.12.2 Set NTP Server ..... 76
9.12.3 Synchronize Time by Satellite ..... 76
9.12.4 Set DST ..... 76
9.13 Set RS-485 ..... 77
9.14 Set RS-232 ..... 77
9.15 Power Consumption Mode ..... 77
9.16 External Device ..... 78
9.16.1 Supplement Light Settings ..... 78
9.16.2 Heater ..... 79
9.17 Security ..... 79
9.17.1 Authentication ..... 79
9.17.2 Set IP Address Filter ..... 80
9.17.3 Set HTTPS ..... 81
9.17.4 Set QoS ..... 81
9.17.5 Set IEEE 802.1X ..... 81
9.17.6 Control Timeout Settings ..... 82
9.17.7 Search Security Audit Logs ..... 82
9.17.8 Security Reinforcement ..... 82
9.17.9 SSH ..... 83
9.18 Certificate Management ..... 83

9.18.1 Create Self-signed Certificate ..... 83
9.18.2 Create Certificate Request ..... 83
9.18.3 Import Certificate ..... 84
9.18.4 Install Server/Client Certificate ..... 84
9.18.5 Install CA Certificate ..... 84
9.18.6 Enable Certificate Expiration Alarm ..... 85
9.19 User and Account ..... 85
9.19.1 Set User Account and Permission ..... 85
9.19.2 Simultaneous Login ..... 86
9.19.3 Online Users ..... 86
**Chapter 10 Allocate VCA Resource ..... 87**
10.1 Road Traffic ..... 87
10.1.1 Set Vehicle Detection ..... 87
10.1.2 Set Mixed-Traffic Detection Rule ..... 88
10.1.3 Uploading Pictures Settings ..... 89
10.1.4 Camera Settings ..... 89
10.1.5 Import or Export Blocklist & Allowlist ..... 89
10.2 Face Capture ..... 90
10.2.1 Set Face Capture ..... 90
10.2.2 Overlay and Capture ..... 91
10.2.3 Face Capture Algorithms Parameters ..... 92
10.2.4 Set Shield Region ..... 93
**Chapter 11 Smart Display ..... 94**
**Chapter 12 EPTZ ..... 95**
12.1 Patrol ..... 95
12.2 Auto-Tracking ..... 95
**Appendix A. Device Command ..... 97**
**Appendix B. Device Communication Matrix ..... 98**

# 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 → Basic → 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 operation systems and web browser may restrict the display and operation of the camera function. You should install 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 8+<br>• Google Chrome 57 and earlier version<br>• Mozilla Firefox 52 and earlier version | Follow pop-up prompts to complete plug-in installation. |
| | • Google Chrome 57+<br>• Mozilla Firefox 52+ | Click Download Plug-in to download and install plug-in. |
| Mac OS | • Google Chrome 57+<br>• Mozilla Firefox 52+<br>• Mac Safari 16+ | Plug-in installation is not required. |

| Operating System | Web Browser | Operation |
|---|---|---|
| | | Go to **Configuration → Network → Advanced Settings → Network Service** 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 camera only supports Windows and Mac OS system and do not support Linux system.

### 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 **Configuration → System → Security → Security Service** , 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 Enable and Disable Live View

This function is used to quickly enable or disable live view of the channel.

- Click ▶ to start the live view.
- Click ■ to stop the live view.

### 3.1.2 Adjust Aspect Ratio

**Steps**

1. Click **Live View**.
2. Click ▭ to select the aspect ratio.
   - 4:3 refers to 4:3 window size.
   - 16:9 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, VLC or MJPEG.

### 3.1.5 Window Division

- refers to 1 × 1 window division.
- refers to 2 × 2 window division.
- refers to 3 × 3 window division.
- refers to 4 × 4 window division.

### 3.1.6 Light

Click to turn on or turn off the illuminator.

### 3.1.7 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.

### 3.1.8 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.

### 3.1.9 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.

### 3.1.10 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.

**Manual Lens Initialization**

Click to operate lens initialization.

**Auto Lens Initialization**

Go to **Configuration → System → Maintenance → Lens Correction** to enable this function. You can set the arming schedule, and the device will correct lens automatically during the configured time periods.

### 3.1.11 Quick Set Live View

It offers a quick setup of PTZ, display settings, OSD, video/audio and VCA resource settings on live view page.

**Steps**

1. Click to show quick setup page.
2. Set PTZ, display settings, OSD, video/audio and VCA resource parameters.
   - For PTZ settings, see ***Lens Parameters Adjustment*** .
   - For display settings, see ***Display Settings*** .
   - For OSD settings, see ***OSD*** .
   - For audio and video settings, see ***Video and Audio*** .
   - For VCA settings, see ***Allocate VCA Resource*** .

**Note**

The function is only supported by certain models.

### 3.1.12 Lens Parameters Adjustment

It is used to adjust the lens focus, zoom and iris.

### Zoom

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

### Focus

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

### PTZ Speed

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

### 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 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.

Go to **Configuration → PTZ** , check**Enable PTZ Lock**, and click **Save**.

### 3.1.13 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** .
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 **OK**.

## 3.3 Set Smooth Streaming

It is a function to tackle the latency and network congestion caused by unstable network condition, and keep the live view stream on the web browser or the client software smooth.

**Before You Start**

Add the device to your client software and select NPQ protocol in client software before configuring the smooth streaming function.

Be sure that the **Bitrate Type** is selected as **Constant** and the **SVC** is selected as **OFF** before enabling the function. Go to **Configuration → Video/Audio → Video** to set the parameters.

**Steps**

1. Go to the settings page: **Configuration → Network → Advanced Settings → Smooth Streaming** .
2. Check **Enable Smooth Streaming**.
3. Select the mode for smooth streaming.

| | |
|---|---|
| **Auto** | The resolution and bitrate are adjusted automatically and resolution takes the priority. The upper limits of these two parameters will not exceed the values you set on **Video** page. Go to **Configuration → Video/Audio → Video** , set the **Resolution** and **Max. Bitrate** before you enable smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically. |
| **Resolution Priority** | The resolution stays the same as the set value on **Video** page, and the bitrate will be adjusted automatically. Go to **Configuration → Video/Audio → Video** , set the **Max. Bitrate** before you enable smooth streaming function. In this mode, the framerate will be adjusted to the maximum value automatically. |
| **Frame Rate Priority** | The image is still smooth even under the poor network, while the image quality may be not good. |
| **Error Correction** | The resolution and bitrate stay the same as the set values on **Video** page. The mode is used to correct the data error during transmission to ensure the image quality. You can set the **Error Correction Proportion** within range of 0-100.<br>When the proportion is 0, the data error will be corrected by data retransmission. When the proportion is higher than 0, the error data will be corrected via redundant data that is added to the stream and data retransmission. The higher the value is, the more redundant date will be generated, the more data error would be corrected, but the larger bandwidth would be required. When the proportion is 100, the redundant data will be as large as the original data, and the bandwidth is twice required.<br>**Note**<br>Be sure the bandwidth is sufficient in the Error Correction mode. |

4. Save the settings.

# 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.

### Set Custom Video

You can set up additional video streams if required. For custom video streams, you can preview them, but cannot record or play back them.

**Steps**

**Note**

- The function is only supported by certain camera models.
- After restoring the device (not restore to default settings), quantity of custom video streams and their names are kept, but the related parameters are restored.

1. Click + to add a stream.
2. Change the stream name as needed.

**Note**

Up to 32 letters and symbols (except &, <, >, ', or ") are allowed for the stream name.

3. Customize the stream parameters (resolution, frame rate, max. bitrate, video encoding).
4. **Optional:** Add stream description as needed.
5. **Optional:** If a custom stream is not needed, click × to delete it.
6. Click **Save**.

### 4.1.2 Video Type

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

**Video**

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, **Video Quality**, **I Frame Interval**, **Profile**, **SVC**, **Main Stream Smoothing** and **ROI** are not supported.

#### 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, **Video Quality**, **I Frame Interval**, **Profile** and **SVC** are 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 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.

### 4.2.1 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.** in **Fixed Region** to draw ROI region.
   1) Click **Draw Area**.
   2) Click and drag the mouse on the view screen to draw the fixed region.
   3) Click **Stop Drawing**.

**Note**

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

5. Input the **Region 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.

### 4.2.2 Set Face Tracking ROI

When the face tracking function is enabled in ROI and the face appears in the live picture, the image of the face is clearer than that of the surrounding area.

**Steps**

1. Go to the ROI setting page: **Configuration → Video/Audio → ROI** .
2. Check **Enable Face Tracking**.
3. Select **ROI Level** in **Dynamic Region**.

**Note**

ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

4. Click **Save**.

### 4.2.3 Set Target Tracking ROI

The moving target is clearer than other areas in live image or recordings after enabling the function.

**Before You Start**

Go to **Configuration → PTZ → Smart Tracking** to complete the smart tracking settings.

**Steps**

1. Go to **Configuration → Video/Audio → ROI** .
2. Check **Enable Target Tracking**.
3. Set **ROI Level** for target tracking. The higher the value is, the clearer the target is.
4. Click **Save**.

### 4.2.4 Set License Plate Tracking ROI

When the license plate tracking ROI function is enabled and the license plate appears in the live picture, the image of the license plate is clearer than that of the surrounding area.

**Steps**

1. Go to the ROI setting page: **Configuration → Video/Audio → ROI** .
2. Check **Enable License Plate Tracking**.
3. Select **ROI Level** in **Dynamic Region**.

**Note**

ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

4. Click **Save**.

## 4.3 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.

**Steps**

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

## 4.4 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** .

### 4.4.1 Audio Encoding

Select the audio encoding compression of the audio.

### 4.4.2 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. |

### 4.4.3 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.

### 4.4.4 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.

## 4.5 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.

## 4.6 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

### 4.6.1 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**, **Hue**, **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 in the day mode and turn on fill light in the 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 illumination automatically.

**Scheduled-Switch**

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

**Note**

Day/Night Switch function varies according to models.

## Grey Scale

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

## Rotate

When 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.

## 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.

### 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.

### 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.

### 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.

### 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.

### EIS

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

### 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.

## 4.6.2 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 Switch

Switch the image parameters to the scene automatically in certain time periods.

**Steps**

1. Check **Enable**.
2. Select and configure the corresponding time period and the scene.

**Note**

For the scene configuration, refer to ***Scene Mode*** .

3. Click **Save**.

### 4.6.3 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.

### 4.6.4 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.

## 4.7 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 displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

### Displayed Information

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

### Text Overlay

Set customized overlay text on image.

### OSD Parameters

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

## 4.8 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 privacy mask setting page: **Configuration → Image → Privacy Mask** .
2. Check **Enable Privacy Mask**.
3. Click **Draw Area**. 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** | Clear all the areas you set. |

4. Click **Stop Drawing**.
5. Click **Save**.

## 4.9 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 picture overlay setting page: **Configuration → Image → Picture Overlay** .
2. Click **Browse** to select a picture, and click **Upload**.

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

## 4.10 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 Target Cropping** 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.

# 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 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**.

## 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. There are three status descriptions: good, bad, and damaged. 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 → Network → Advanced Settings → FTP** .
2. Configure FTP settings.

**FTP Protocol**

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

**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.

**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.

3. Check **Upload Picture** to enable uploading snapshots to the FTP server.

4. 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 **HDD No.**. Enter 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.

   **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.
3. Click **Test** to check whether the network disk is available.
4. 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 → Maintenance → 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 Cloud Storage**.
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. Click **Advanced** to set the advanced settings.

**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 **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click in the live view interface to start recording. Click to stop recording.

### 5.2.3 Set Lite Storage

After the lite storage is enabled, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the memory card when there is no moving object in the monitoring scenario.

**Steps**

1. Go to **Configuration → Storage → Storage Management → Lite Storage** .
2. Check **Enable** and set the level. The higher the level is, the larger the frame rate and bitrate are, and the shorter the recommended storage time is.
3. Set the storage time. The device automatically calculates the bitrate and offers the recommended storage time according to the memory card space and level. You are recommended to set the storage time to the device recommended time.

**Note**

- If the lite storage is enabled, unformatted memory card will be formatted automatically.
- The displayed available space of the memory card is assigned by default according to **Percentage of Record** in **Storage → Storage Management → Quota** . You can adjust it as required.
- Only certain device models support the function.

### 5.2.4 Playback and Download Video

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

**Steps**

1. Click **Playback**.
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 clip video files.
   - Double click the live view image to play video files in full screen. Press **ESC** to exit full screen.

   **Note**

   Go to **Configuration → Local** , click **Save clips to** to change the saving path of clipped video files.
4. Click ⬇ on the playback interface to download files.
   1) Set search condition and click **Search**.
   2) Select the video files and then click **Download**.

      **Note**

      Go to **Configuration → Local** , click **Save downloaded files to** to 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 → Capture → Capture Parameters** .
2. Set the capture type.

   **Timing**

   Capture a picture at the configured time interval.

   **Event-Triggered**

   Capture a picture when an event is triggered.
3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to ***Set Arming Schedule*** for configuring schedule time.
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 Set Timing Wake

When the device is sleeping, it will wake up at the set time interval, and capture pictures and upload them.

**Steps**

**Note**

The function is only supported by certain device models.

1. Go to **Configuration → System → System Settings → Power Consumption Mode** , under **Sleep Schedule**, click the time schedule to set **Sleep Capture Interval**.
2. Enter **Configuration → Event → Basic Event → Timing Wake** .
3. Check **Enable**.
4. Select **Capture Types**.
5. For the linkage method settings, see ***Linkage Method Settings*** .
6. Click **Save**.

**Result**

The device will wake up at the set sleep capture interval, and capture pictures and upload them.

### 5.3.4 View and Download Picture

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

**Steps**

1. Click **Picture**.
2. Set search condition and click **Search**.

   The matched pictures showed in the file list.

3. Select the pictures then click **Download** to download them.

**Note**

Go to **Configuration → Local** , click **Save snapshots when playback** to change the saving path of pictures.

# Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm.

## 6.1 Basic Event

### 6.1.1 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 → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
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 **Configuration Mode**, 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**.

### 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 **Draw Area**. Click and drag the mouse on the live image and then release the mouse to finish drawing one area.

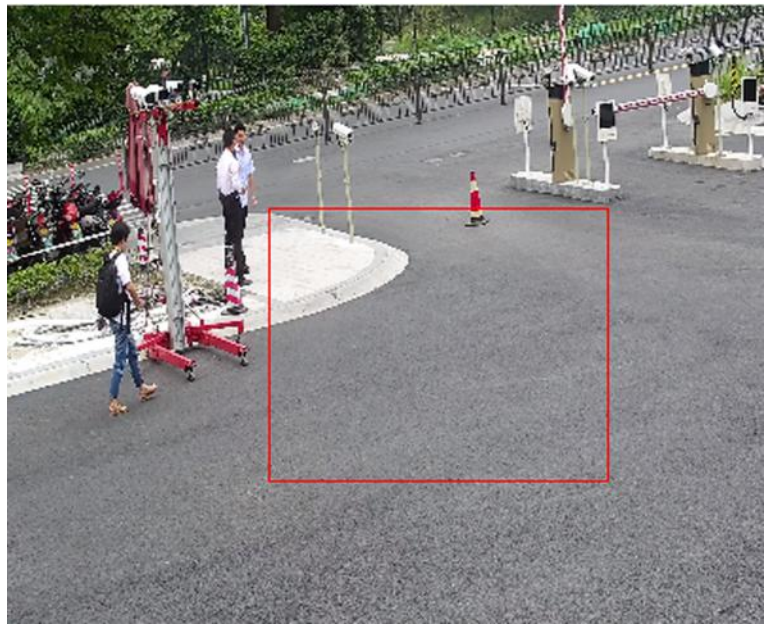

**Figure 6-1 Set Rules**

**Stop Drawing** Finish drawing one area.

**Clear All** Delete all the areas.

4. Click **Save**.
5. **Optional:** Repeat above steps to set multiple areas.

## 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.
4. Click **Draw Area**. Click and drag the mouse on the live video, and then release the mouse to finish drawing one area.

   **Stop Drawing** Stop drawing one area.

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

### 6.1.2 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 → Basic Event → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click **Draw Area** and drag the mouse in the live view to draw the area.

   **Stop Drawing** Finish drawing.

   **Clear All** Delete all the drawn areas.

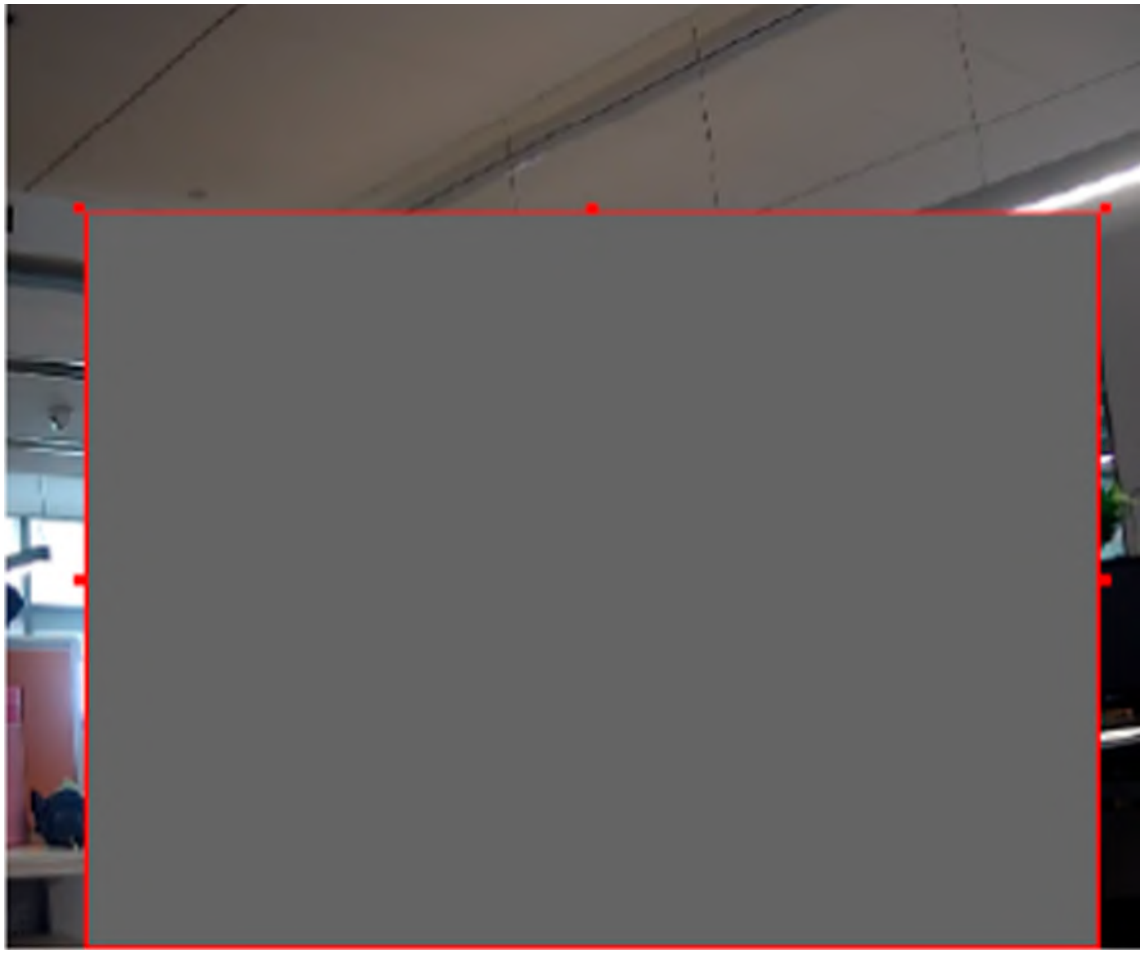

**Figure 6-2 Set Video Tampering Area**

5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Save**.

### 6.1.3 Set PIR Alarm

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

**Steps**

**Note**

Only certain models support PIR alarm.

1. Go to **Configuration → Advanced Configuration → Basic Event → PIR Alarm** .

2. Check **Enable PIR Alarm**.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

### 6.1.4 Set Exception Alarm

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

**Steps**

1. Go to **Configuration → Event → Basic Event → 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. |
| **Voltage Instable** | The power supply voltage is fluctuating. |

3. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

### 6.1.5 Set Alarm Input

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

**Before You Start**

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

**Steps**

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

### 6.1.6 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 → Basic Event → 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 **Enable**, and the selected diagnosis 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.

### 6.1.7 Set Vibration Detection

It is used to detect whether the device is vibrating. The device reports an alarm and triggers linkage actions if the function is enabled.

**Steps**

1. Go to **Configuration → Event → Basic Event → Vibration Detection** .
2. Check **Enable**.
3. Drag the slider to set the detection sensitivity. You can also enter number to set the sensitivity.
4. Set the arming schedule. See ***Set Arming Schedule*** .
5. Set the linkage method. See ***Linkage Method Settings*** .
6. Click **Save**.

**Note**

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

## 6.2 Smart Event

Set smart events by the following instructions.

**Note**

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

### 6.2.1 Detect Audio Exception

Audio exception detection function detects the abnormal sound in the surveillance 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 → Smart Event → 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 varies according to different models.

### 6.2.2 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 → Smart Event → 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.

### 6.2.3 Detect Scene Change

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

**Steps**

1. Go to **Configuration → Event → Smart Event → 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 varies according to different models.

### 6.2.4 Set Face Detection

It helps to detect the face in the detection region. If a face is detected, the device triggers the linkage actions.

**Steps**

1. Go to **Configuration → Event → Smart Event → Face Detection** .
2. Check **Enable Face Detection**.
3. **Optional:** Highlight to display the face in the image.
   1) Check **Enable Dynamic Analysis For Face Detection**.

2) Go to **Configuration → Local** , set **Rules** to **Enable**.

4. Set **Sensitivity**. The lower the sensitivity is, the profile of the face or unclear face is more difficult to detect.
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**.

### 6.2.5 Set Video Loss

This function can detect the video signal loss in time and trigger the linkage action.

**Steps**

1. Go to **Configuration → Event → Basic Event → Video Loss** .
2. Check **Enable**.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

### 6.2.6 Set Intrusion Detection

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

**Steps**

1. Go to **Configuration → Event → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Select a **Region**. For the detection region settings, refer to ***Draw Area*** .
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. |
| **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. |
| **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. |

**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 6-3 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**.

### 6.2.7 Set Line Crossing Detection

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

**Steps**

1. Go to **Configuration → Event → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Select one **Line** and set the size filter. For the size filter settings, refer to ***Set Size Filter*** .
4. Click **Draw Area** and a line with an arrow appears in the live video. Drag the line to the location on the live video as desired.
5. Set rules.

**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.

**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.

**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.

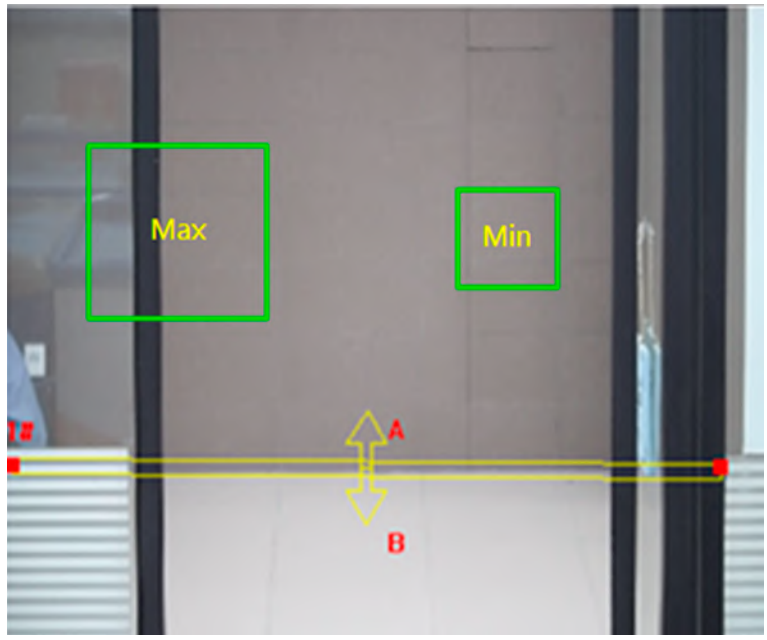


**Figure 6-4 Set Rule**

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

### 6.2.8 Set Region Entrance Detection

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

**Steps**

1. Go to **Configuration → Event → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Select one **Region**. For the region settings, refer to ***Draw Area*** .
4. Set the detection target, sensitivity and the target validity.

| | |
|---|---|
| **Sensitivity** | It stands for the percentage of the body part of an acceptable target that goes across 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. |
| **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. |
| **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. |

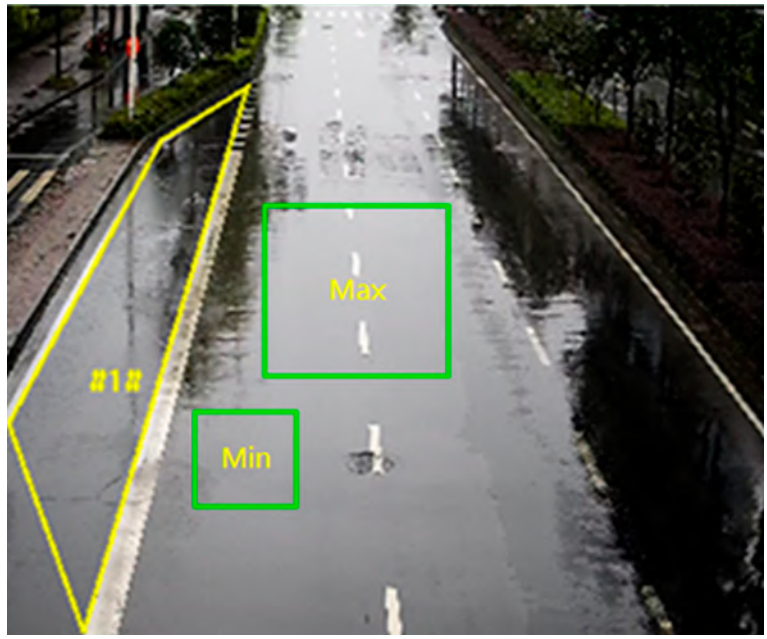


**Figure 6-5 Set Rule**

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**.

### 6.2.9 Set Region Exiting Detection

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

**Steps**

1. Go to **Configuration → Event → Smart Event → Region Exiting Detection**
2. Check **Enable**.
3. Select one **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set the detection target, sensitivity and the target validity.

| | |
|---|---|
| **Sensitivity** | It stands for the percentage of the body part of an acceptable target that goes across 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. |
| **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. |
| **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. |

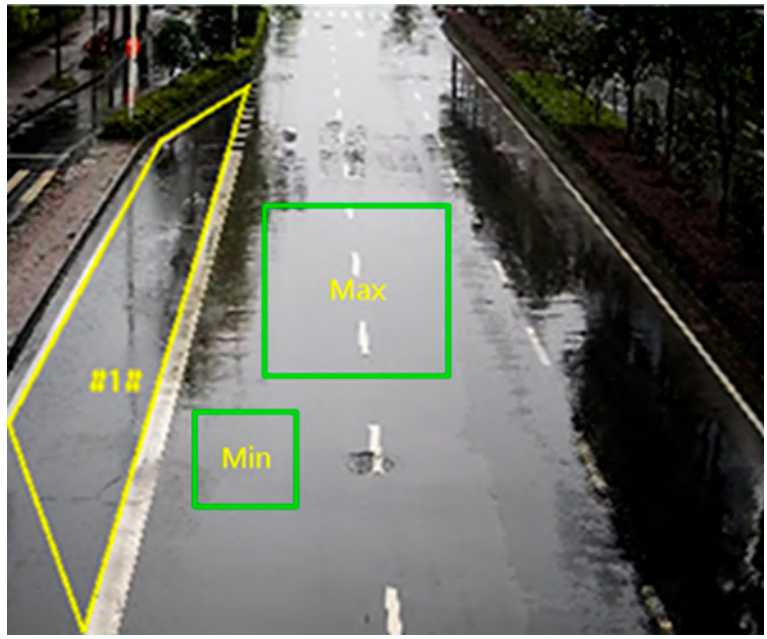


**Figure 6-6 Set Rule**

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**.

### 6.2.10 Set Unattended Baggage Detection

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

**Steps**

1. Go to **Configuration → Event → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.
3. Select one **Region**. For the detection region settings, refer to ***Draw Area*** .
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.

**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.

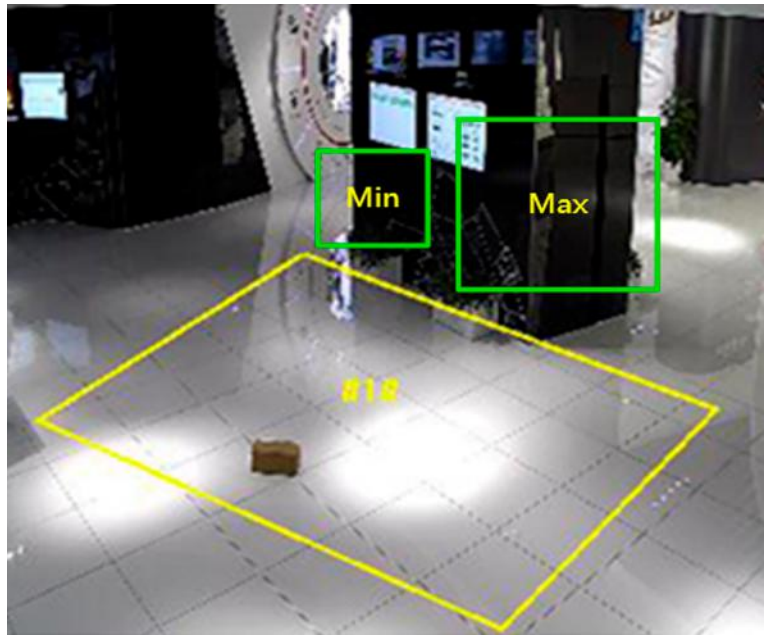


**Figure 6-7 Set Rule**

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**.

### 6.2.11 Set Object Removal Detection

It detects whether the objects are removed from the pre-defined 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.

**Steps**

1. Go to **Configuration → Event → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Select a **Region**. For the region settings, see ***Draw Area*** .
4. Set the rule.

| | |
|---|---|
| **Sensitivity** | It stands for the percentage of the body part of an acceptable target that leaves the pre-defined region.<br>Sensitivity = 100 – S1/ST*100<br>S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.<br>Example: If you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region. |
| **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:** Repeat the above steps to set more regions.
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.

### 6.2.12 Draw Area

This section introduces the configuration of area.

**Steps**

1. Click **Draw Area**.
2. Click on the live view to draw the boundaries of the detection region, and right click to complete drawing.

3. Click **Save**.

**Note**

Click **Clear All** to clear all pre-defined areas.

### 6.2.13 Set Size Filter

This part introduces the setting of size filter. Only the target whose size is between the minimum value and maximum value is detected and triggers alarm.

**Steps**

1. Click **Max. Size**, and drag the mouse in the live view to draw the maximum target size.
2. Click **Min. Size**, and drag the mouse in the live view to draw the minimum target size.
3. Click **Save**.

# Chapter 7 Network Settings

## 7.1 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 → Basic 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.

**Dynamic Domain Name**

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.

### 7.1.1 Multicast

Multicast is a group communication where data transmission is addressed to a group of destination devices simultaneously. After setting multicast, you can send the source data efficiently to multiple receivers.

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

**IP Address**

It stands for the address of multicast host.

**Stream Type**

The stream type of the multicast source.

**Video Port**

The video port of the selected stream.

**Audio Port**

The audio port of the selected stream.

**FEC Port**

The FEC port of the selected stream.

**FEC Ratio**

The ratio of forward error correction.

### 7.1.2 Multicast Discovery

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.

## 7.2 SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

**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 the settings page: **Configuration → Network → Advanced 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**.

## 7.3 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 → Advanced Settings → SRTP** .
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. 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.

## 7.4 Port Mapping

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

**Before You Start**
When the ports in the device are the same as those of other devices in the network, refer to ***Port*** to modify the device ports.

**Steps**
1. Go to **Configuration → Network → Basic Settings → 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**.

### 7.4.1 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.

### 7.4.2 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.

### 7.4.3 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.

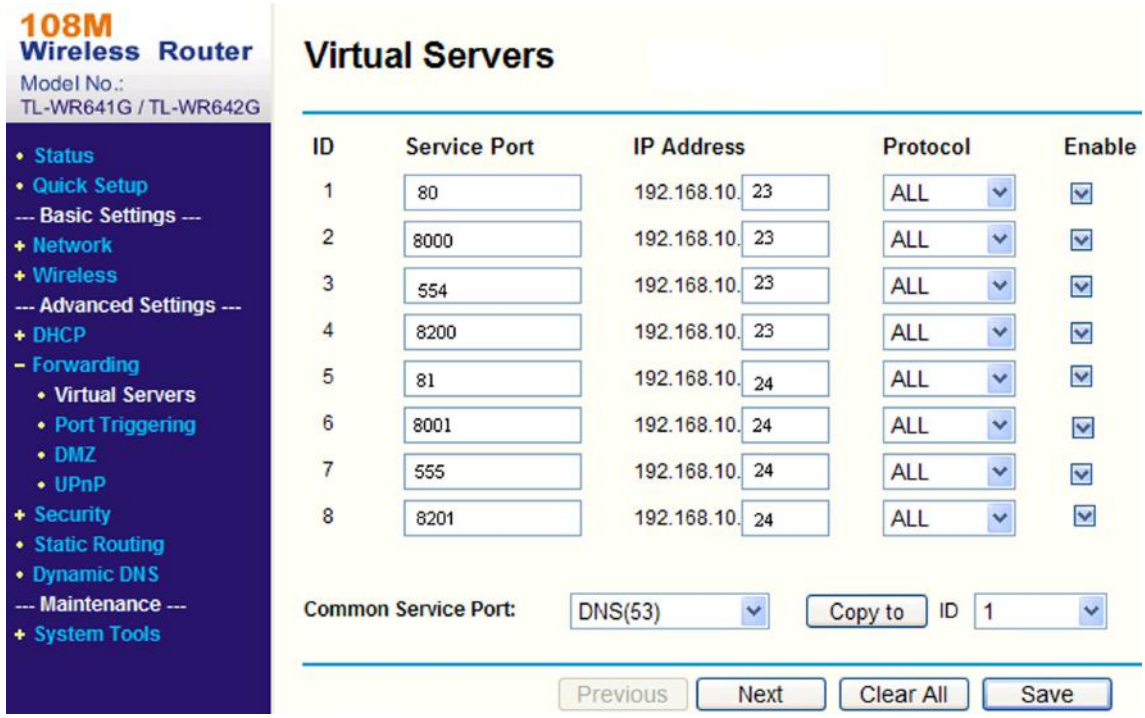


**Figure 7-1 Port Mapping on Router**

**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.

## 7.5 Port

The device port can be modified when the device cannot access the network due to port conflicts.

**Caution**

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Configuration → Network → Basic Settings → Port** for port settings.

**HTTP Port**

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.

**HTTPS Port**

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

**RTSP Port**

It refers to the port of real-time streaming protocol.

**SRTP Port**

It refers to the port of secure real-time transport protocol.

**Server Port**

It refers to the port through which the client adds the device.

**Enhanced SDK Service Port**

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

**WebSocket Port**

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

**WebSockets Port**

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.

**Note**

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.

## 7.6 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.

**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 → Basic Settings → DDNS** .
3. Check **Enable DDNS** 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*** to check the device port , and 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. |

## 7.7 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 → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
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.

## 7.8 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.

### 7.8.1 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 → Advanced Settings → Wireless Dial** .
2. Check to enable the function.
3. Click **Dial Parameters** to configure and save the parameters.
4. Click **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. **Optional:** Set **Allowlist**. See ***Set Allowlist*** for detailed information.
6. Click **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.

7. 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.

### 7.8.2 Set Allowlist

Add the mobile phone number of administrator to the allowlist in order to receive alarm message from the device.

**Steps**

1. Go to allowlist settings page: **Configuration → Advanced Configuration → Wireless Dial → Allowlist** .
2. Check **Enable SMS Alarm**.
3. Click + in the allowlist.
   1) Input the mobile phone number to receive alarm message.
   2) Check **Reboot via SMS**.
   3) Select the certain events, and the mobile phone can receive the alarm message when the event happens.
   4) Click **Save**.
   5) **Optional:** Repeat the steps above to set multiple recipients.

| | |
|---|---|
| | Modify the allowlist parameters. |
|  | Delete the allowlist that already set. |
| **Send Test SMS** | Send a message to the mobile phone for test. |

4. Click **Save**.

## 7.9 Wi-Fi

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

**Note**

This function is only supported by certain device models.

### 7.9.1 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 → Basic Configuration → 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 → Advanced Configuration → Wi-Fi** .
4. Set and save the parameters.
   1) Click **Search**.
   2) Select 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**.
   3) Select the **Network Mode** as **Manage**.
   4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

**What to do next**

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

## 7.10 Set Network Service

You can control the ON/OFF status of certain protocol as desired.

**Steps**

**Note**

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service** .
2. Set network service.

   **WebSocket & WebSockets**

   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.

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

   When you use WebSockets, select the **Server Certificate**.

   **Note**

   Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.

   **SDK Service & Enhanced SDK Service**

   Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.

**Note**

- Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
- When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.

**TLS (Transport Layer Security)**

The device offers TLS1.1 and TLS1.2. Enable one or more protocol versions according to your need.

**Bonjour**

Uncheck to disable the protocol.

3. Click **Save**.

## 7.11 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 → Advanced Settings → Integration Protocol** .
2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.

   **Delete** Delete the selected Open Network Video Interface user.

   **Modify** Modify the selected Open Network Video Interface user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

## 7.12 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 → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.

4. Select a protocol version and input related parameters.
5. Click **Save**.

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

## 7.13 Set 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.

**Steps**

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. **Optional:** Check **Enable** to enable ANR.
4. Select **Protocol**.

   **Note**

   HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.
5. Click **Test** to check if the IP or host is available.
6. Click **Save**.

## 7.14 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.

### 7.14.1 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 → Advanced Settings → Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. 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.

7. 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.

## 7.14.2 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.

### 7.14.3 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.

# Chapter 8 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.

## 8.1 Set Arming Schedule

Set the valid time of the device tasks.

**Steps**

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.

   **Note**

   Up to 8 periods can be configured for one day.
3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

## 8.2 Linkage Method Settings

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

### 8.2.1 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 → Basic Event → 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*** .
3. Click **Save**.

### Manual Alarm

You can trigger an alarm output manually.

**Steps**

1. Set the manual alarm parameters.

   **Alarm Output No.**

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   **Alarm Name**

   Edit a name for the alarm output.

   **Delay**

   Select **Manual**.

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.

**Steps**

1. Set automatic alarm parameters.

   **Alarm Output No.**

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   **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. Click **Copy to…** to copy the parameters to other alarm output channels.
4. Click **Save**.

## 8.2.2 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.

### 8.2.3 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 receivers if an alarm event is detected.

**Before You Start**

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

**Steps**

1. Go to email settings page: **Configuration → Network → Advanced Settings → 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 **SSL** or **TLS**, and disable STARTTLS, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
      - When you select **SSL** or **TLS** and **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 Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
   5) Input the receiver's information, including the receiver's name and address.
   6) Click **Test** to see if the function is well configured.
3. Click **Save**.

### 8.2.4 Notify Surveillance Center

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

### 8.2.5 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***

### 8.2.6 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 → Basic Event → Flashing Alarm Light Output** .
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

   **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.

   **Brightness**

   The brightness of the light.
3. Set the arming schedule. See ***Set Arming Schedule*** for details.
4. Click **Save**.

**Note**

Only certain device models support the function.

### 8.2.7 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 → Basic Event → 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 **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.

# Chapter 9 System and Security

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

## 9.1 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.

## 9.2 Search and Manage Log

Log helps locate and troubleshoot problems.

**Steps**

1. Go to **Configuration → System → 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.

## 9.3 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** , click **General** and set **Simultaneous Login**.

## 9.4 Import and Export Configuration File

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

Enter **Configuration → System → Maintenance → Upgrade & Maintenance** . Choose device parameters that need to be imported or exported and follow the instructions on the interface to import or export configuration file.

## 9.5 Export Diagnose Information

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

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** . Check desired diagnose information and click **Diagnose Information** to export corresponding diagnose information of the device.

## 9.6 Reboot

You can reboot the device via browser.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Reboot**.

## 9.7 Restore and Default

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

**Steps**

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
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.

## 9.8 Upgrade

**Before You Start**

You need to obtain the correct upgrade package.

**Caution**

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

**Steps**

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
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 **Browse** to select the upgrade file.
4. Click **Upgrade**.

## 9.9 View Open Source Software License

Go to **Configuration → System → System Settings → About Device** , and click **View Licenses**.

## 9.10 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.

## 9.11 Metadata

Metadata is the raw data that the camera collects before algorithm processing. It provide the option to users to explore various data usages.

**Note**

The function is only supported by certain device models.

Go to **Configuration → System → 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.

## 9.12 Time and Date

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

### 9.12.1 Synchronize Time Manually

**Steps**

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

3. Click **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.
   - Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

### 9.12.2 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**.

### 9.12.3 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**.

### 9.12.4 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 → DST** .
2. Check **Enable DST**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

## 9.13 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 termial 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**.

## 9.14 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**.

## 9.15 Power Consumption Mode

It is used to switch the power consumption when the device is working.

**Note**

The function is only supported by certain camera models.

Go to **Configuration → System → System Settings → Power Consumption Mode** , select the desired power consumption mode.

**Full Consumption Mode**

The device works with all the functions enabled.

**Low Consumption Real-Time Mode**

The device DSP works normally. It records the videos with the main stream at the half frame rate, and supports the remote login, preview and the configuration.

**Low Power Sleep**

When the device power is lower than **Threshold of Low Power Sleep Mode**, the device enters sleep mode.

When the device power is recovered to 10% above the threshold, the device enters the user configuration mode.

**Scheduled Sleep**

If the device is during **Scheduled Sleep Time**, it enters the sleep mode, otherwise it enters the user configuration mode.

**Note**

For the scheduled sleep schedule settings, see ***Arming Schedule and Alarm Linkage*** .
The device supports the timing wake. For the details, see ***Set Timing Wake*** .

## 9.16 External Device

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

**Brightness**

Adjust **Low Beam Brightness** and **High Beam Brightness** according to the actual scene.

**Timing**

The LED light will be turned on by the schedule you set. You should set **Start Time** and **End Time**.

**Auto**

The LED light will be turned on according to the environment illumination.

### 9.16.1 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 Mode**

IR light is enabled.

**White Light Mode**

White light is enabled.

**Mix Mode**

Both IR light and white light are enabled.

**Off**

Supplement light is disabled.

**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.

### 9.16.2 Heater

You can enable heater to remove fog around the lens of the device.

Go to **Configuration → System → System Settings → External Device** and select the mode as required.

## 9.17 Security

You can improve system security by setting security parameters.

### 9.17.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

**RTSP 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.

**RTSP 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.

**WEB 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.

**WEB 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.

**Note**

Refer to the specific content of protocol to view authentication requirements.

## 9.17.2 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 **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.

   **Forbidden** IP addresses in the list cannot access the device.

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

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

### 9.17.3 Set HTTPS

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 → Advanced Settings → HTTPS** .
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.
4. Select the **Server Certificate**.
5. Click **Save**.

**Note**

If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

### 9.17.4 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 → Advanced Configuration → QoS** .
2. Set **Video/Audio DSCP**, **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**.

### 9.17.5 Set IEEE 802.1X

IEEE 802.1x is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1x standard, the authentication is needed.

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

Set **Protocol** and **EAPOL Version** according to router information.

**Protocol**

EAP-LEAP, EAP-TLS, and EAP-MD5 are selectable

**EAP-LEAP and EAP-MD5**

If you use EAP-LEAP or EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Input the user name and password for authentication.

**EAP-TLS**

If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate and Private Key.

**EAPOL Version**

The EAPOL version must be identical with that of the router or the switch.

## 9.17.6 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 **Configuration → System → Security → Advanced Security** to complete settings.

## 9.17.7 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 **Configuration → System → 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.

## 9.17.8 Security Reinforcement

Security reinforce is a solution to enhance network security. With the function enabled, risky functions, protocols, ports of the device are disabled and more secured alternative functions, protocols and ports are enabled.

Go to **Configuration → System → Security → Advanced Security** . Check **Security Reinforcement**, and click **Save**.

### 9.17.9 SSH

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

The SSH function is disabled by default.

**Caution**

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

## 9.18 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.

### 9.18.1 Create Self-signed Certificate

**Steps**

1. Click **Create Self-signed Certificate**.
2. Follow the prompt to enter **Certificate ID**, **Country/Region**, **Hostname/IP**, **Validity** and other parameters.

   **Note**

   The certificate ID should be digits or letters and be no more than 64 characters.
3. Click **OK**.
4. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

### 9.18.2 Create Certificate Request

**Before You Start**

Select a self-signed certificate.

**Steps**

1. Click **Create Certificate Request**.
2. Enter the related information.
3. Click **OK**.

### 9.18.3 Import Certificate

**Steps**

1. Click **Import**.
2. Click **Create Certificate Request**.
3. Enter the **Certificate ID**.
4. Click **Browser** to select the desired server/client certificate.
5. Select the desired import method and enter the required information.
6. Click **OK**.
7. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

**Note**

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

### 9.18.4 Install Server/Client Certificate

**Steps**

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**, **Create Certificate Request** and **Import** to install server/client certificate.

| | |
|---|---|
| **Create self-signed certificate** | Refer to ***Create Self-signed Certificate*** |
| **Create certificate request** | Refer to ***Create Certificate Request*** |
| **Import Certificate** | Refer to ***Import Certificate*** |

### 9.18.5 Install CA Certificate

**Steps**

1. Click **Import**.
2. Enter the **Certificate ID**.
3. Click **Browser** to select the desired server/client certificate.
4. Select the desired import method and enter the required information.
5. Click **OK**.

**Note**

Up to 16 certificates are allowed.

### 9.18.6 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**.

## 9.19 User and Account

### 9.19.1 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 **Modify** to change the password and permission.

**Delete** Select a user and click **Delete**.

**Note**

The administrator can add up to 31 user accounts.

3. Click **OK**.

### 9.19.2 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** , click **General** and set **Simultaneous Login**.

### 9.19.3 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.

# Chapter 10 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It helps allocate more resources to the desired functions.

**Steps**

1. Go to **Configuration → System → System Settings → VCA Resource** .
2. Select desired VCA functions.
3. Save the settings.

**Note**

Certain VCA functions are mutually exclusive. When a certain function or functions are selected and saved, others will be hidden.

## 10.1 Road Traffic

Motor vehicle, non-motor vehicle, and pedestrian can be detected and captured when they enter the set lane to realize rapid detection and comprehensive surveillance of the targets on road.

**Note**

Only certain device models support this function.

### 10.1.1 Set Vehicle Detection

The vehicle that enters the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarm will be triggered and capture can be uploaded.

**Before You Start**

Go to **Configuration → System → System Settings → VCA Resources** , and select **Road Traffic**.

**Steps**

1. Go to **Configuration → Road Traffic → Detection Configuration** , and select **Vehicle Detection** as detection type.
2. Check **Enable**.
3. Select the lane number.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

**Note**

Only 1 license plate can be captured at one time for each lane.

6. Select **Region** and **Country/Region**.
7. Select the license plate information upload mode.

| | |
|---|---|
| **Entrance/Exit** | The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in entrance/exit. |
| **City Street** | The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in city streets. |
| **Alarm Input** | It means the input alarm will trigger a license plate capture and recognition action. |

**Note**

- When Alarm Input is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it can not be used for other basic events.
- When Alarm Input is selected and saved, previously configured linkage method for A<-1 will be canceled.

8. Select the **Detection mode**.
9. Check **Remove Duplicated License Plates** ans set the **Time Interval**. The default time interval is 4 minutes.

**Note**

Up to 8 license plates are supported.

10. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
11. Click **Save**.

### 10.1.2 Set Mixed-Traffic Detection Rule

The motor vehicle, non-motor vehicle, and pedestrian that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarm will be triggered and capture can be uploaded.

**Before You Start**

Go to **Configuration → System → System Settings → VCA Resources** , and select **Road Traffic**.

**Steps**

1. Go to **Configuration → Road Traffic → Detection Configuration** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.
3. Select the lane number.
4. Select **Region** and **Country/Region**.
5. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
6. Click **Save**.

### 10.1.3 Uploading Pictures Settings

You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **Configuration → Road Traffic → Picture** .

**Picture Quality**

The larger the value is, the clearer the picture is, but larger storage space is also required.

**Picture Size**

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

**License Plate Enhancement**

The larger the value is, the clearer the license plate is, but larger storage space is also required.

Check **License Plate Enhancement** and set the level. The default level is 50.

**Overlay**

You can overlay camera, device or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

For camera settings, go to **Configuration → Road Traffic → Camera** to set relevant parameters and click **Save**.

### 10.1.4 Camera Settings

You can set the parameters of each camera for better management.

Go to **Configuration → Road Traffic → Camera** to set relevant parameters and click **Save**.

### 10.1.5 Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

**Steps**

1. Click **Browse** to open the PC local directory.
2. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.

**Note**

- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls format and the cell format should be Text.

3. Click **Import** to import the selected file.
4. Click **Export** to open the PC local directory.
5. Select a directory in your PC local directory.
6. Name the file in the file name text filed.
7. Click **Save**.

## 10.2 Face Capture

The device can capture the face that appears in the configured area, and the face information will be uploaded with the captured picture as well.

**Note**

- For device that supports face capture, you need to enable the function in **VCA Resource**. Refer to ***Allocate VCA Resource*** for details.
- Face capture is only supported by certain models.

### 10.2.1 Set Face Capture

The face that appears in the configured area can be captured.

**Before You Start**

To enable the function, go to **VCA Resource** and select **Face Capture**.

**Steps**

1. Go to **Configuration → Face Capture** .
2. For shield region settings, refer to ***Set Shield Region*** .
3. Select **Rule** and check **Rule**.
4. Input the min. pupil distance in the text field, or click to draw the min. pupil distance.

   **Min. Pupil Distance**

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
5. Input the max. pupil distance in the text field, or click to draw the max. pupil distance.

6. Click ⬡ to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.
9. For overlay and capture settings, refer to ***Overlay and Capture*** . For advanced parameters settings, refer to ***Face Capture Algorithms Parameters*** .

**Result**

You can view and download captured face images in **Picture**. Refer to ***View and Download Picture*** for details.

## 10.2.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

**Display VCA info. on Stream**

Display smart information on stream, including the target and rules information.

**Display Target info. on Alarm Picture**

Overlay the alarm picture with target information.

**Target Picture Settings**

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.

**Note**

If you select **Custom**, you can customize **width**, **head height** and **body height** as required.

You can check **Fixed Value** to set the picture height.

**Background Picture Settings**

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

**People Counting Overlay**

Select flow overlay type.

Select the daily reset time. Click **Manual Reset** if you want to reset right now.

**Camera**

You can set **Device No.** and **Camera Info.** for the camera, which can be overlaid on captured picture.

**Text Overlay**

You can check desired items and adjust their order to display on captured pictures by .

The content of **Device No.** and **Camera Info** should be on the same page.

### 10.2.3 Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture.

Go to **Configuration → Face Capture → Advanced Configuration → Parameters** .

#### Face Capture Version

It lists the version of the algorithms library.

#### Detection Parameters

**Generation Speed**

The speed to identify a target. The higher the value, the faster the target will be recognized. Setting the value quite low, and if there was a face in the configured area from the start, this face will not be captured. It can reduce the misinformation of the faces in the wall painting or posters. The default value of 3 is recommended.

**Sensitivity**

The sensitivity to identify a target. The higher the value is, the easier a face will be recognized, and the higher possibility of misinformation would be. The default value of 3 is recommended.

#### Capture Parameters

**Best Shot**

The best shot after target leave the detection area.

**Capture Times**

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

**Capture Threshold**

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

**Quick Shot**

You can define quick shot threshold and max. capture interval.

**Quick Shot Threshold**

It stands for the quality of face to trigger quick shot.

**Face Exposure**

Check the checkbox to enable the face exposure.

**Reference Brightness**

The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

**Minimum Duration**

The minimum duration of the camera exposures the face.

**Note**

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

**Face Filtering Time**

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

**Note**

The face filtering time (longer than 0s) may increase the possibility of the actual capture times less than the set value above.

**Restore Default**

Click **Restore** to restore all the settings in advanced configuration to the factory default.

### 10.2.4 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

**Steps**

1. Select **Shield Region**.
2. Click to draw shield area. Repeat this step above to set more shield regions.
3. **Optional:** Click to delete the drawn areas.
4. Click **Save**.

# Chapter 11 Smart Display

It can display the captured pictures when enabling smart functions.

**Note**

The function is only supported by certain device models.

## Layout Preview

Click and select **Layout Preview**. Select the contents according to your needs. When you select real-time analysis, you can select the contents only for real-time analysis.

## Detection Attribute

Click and select **Detection Attribute**. When you enable this function, the attribute information of target analysis can be displayed and the information you select will be displayed in the attribute analysis area.

# 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 you have select the **Fourth Stream** in the live view. Fourth 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 EPTZ**.
3. Check **Fourth Stream**.
4. Select **Patrol** in **Application**.
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 EPTZ**.
3. Check **Fourth Stream**.
4. Select **Auto-tracking** in **Application**.
5. Click **Detection Area** to start drawing.
6. Click on the live video to specify the four vertexes of the detection area, and right click to complete drawing.
7. 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.

8. Click **Save**.

# Appendix A. Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for all Hikvision network cameras.

# Appendix B. Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision network cameras.

See Far, Go Further