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

©2021 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.

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 Light 7

3.1.6 Count Pixel 7

3.1.7 Start Digital Zoom 7

3.1.8 Auxiliary Focus 7

3.1.9 Lens Initialization 8

3.1.10 Quick Set Live View 8

3.1.11 Lens Parameters Adjustment 8

3.2 Set Transmission Parameters 9

Chapter 4 Video and Audio 11

4.1 Video Settings 11

4.1.1 Stream Type 11

4.1.2 Video Type 12

4.1.3 Resolution 12
4.1.4 Bitrate Type and Max. Bitrate 12
4.1.5 Video Quality 12
4.1.6 Frame Rate 13
4.1.7 Video Encoding 13
4.1.8 Smoothing 15
4.2 ROI 15
4.2.1 Set ROI 15
4.3 Audio Settings 16
4.3.1 Audio Encoding 16
4.3.2 Audio Input 16
4.3.3 Audio Output 16
4.3.4 Environmental Noise Filter 17
4.4 Two-way Audio 17
4.5 Display Settings 17
4.5.1 Scene Mode 17
4.5.2 Video Standard 20
4.5.3 Local Video Output 20
4.6 OSD 20
4.7 Set Privacy Mask 21
Chapter 5 Video Recording and Picture Capture 22
5.1 Storage Settings 22
5.1.1 Set New or Unencrypted Memory Card 22
5.1.2 Set FTP 24
5.1.3 Set NAS 25
5.2 Video Recording 25
5.2.1 Record Automatically 25
5.2.2 Record Manually 26

5.2.3 Playback and Download Video 27
5.3 Capture Configuration 27
5.3.1 Capture Automatically 27
5.3.2 Capture Manually 28
5.3.3 View and Download Picture 28
Chapter 6 Event and Alarm 29
6.1 Basic Event 29
6.1.1 Set Motion Detection 29
6.1.2 Set Video Tampering Alarm 31
6.1.3 Set Exception Alarm 32
6.2 Smart Event 33
6.2.1 Detect Audio Exception 33
6.2.2 Set Defocus Detection 34
6.2.3 Detect Scene Change 34
6.2.4 Set Intrusion Detection 34
6.2.5 Set Line Crossing Detection 36
6.2.6 Set Region Entrance Detection 37
6.2.7 Set Region Exiting Detection 38
6.2.8 Set Object Removal Detection 39
6.2.9 Set Unattended Baggage Detection 40
6.2.10 Draw Area 41
6.2.11 Set Size Filter 41
Chapter 7 Network Settings 43
7.1 TCP/IP 43
7.1.1 Multicast Discovery 44
7.2 SNMP 44
7.3 Port Mapping 45
7.3.1 Set Auto Port Mapping 45

7.3.2 Set Manual Port Mapping 45
7.3.3 Set Port Mapping on Router 46
7.4 Port 47
7.5 Access to Device via Domain Name 47
7.6 Set Network Service 48
7.7 Set Open Network Video Interface 49
7.8 Set ISUP 49
7.9 Access Camera via Hik-Connect 50
7.9.1 Enable Hik-Connect Service on Camera 50
7.9.2 Set Up Hik-Connect 51
7.9.3 Add Camera to Hik-Connect 52
Chapter 8 Arming Schedule and Alarm Linkage 54
8.1 Set Arming Schedule 54
8.2 Linkage Method Settings 54
8.2.1 Trigger Alarm Output 54
8.2.2 FTP/NAS/Memory Card Uploading 55
8.2.3 Send Email 56
8.2.4 Notify Surveillance Center 57
8.2.5 Trigger Recording 57
8.2.6 Audible Warning 57
Chapter 9 System and Security 58
9.1 View Device Information 58
9.2 Search and Manage Log 58
9.3 Import and Export Configuration File 58
9.4 Export Diagnose Information 58
9.5 Reboot 59
9.6 Restore and Default 59
9.7 Upgrade 59

9.8 View Open Source Software License 60
9.9 Time and Date 60
9.9.1 Synchronize Time Manually 60
9.9.2 Set NTP Server 60
9.9.3 Synchronize Time by Satellite 61
9.9.4 Set DST 61
9.10 Set RS-232 61
9.11 Security 61
9.11.1 Authentication 62
9.11.2 Set IP Address Filter 62
9.11.3 Set HTTPS 63
9.11.4 Set QoS 64
9.11.5 Set IEEE 802.1X 64
9.11.6 Search Security Audit Logs 64
9.11.7 SSH 65
9.12 User and Account 65
9.12.1 Set User Account and Permission 65
9.12.2 Online Users 66
Chapter 10 Allocate VCA Resource 67
Appendix A. Device Command 68
Appendix B. Device Communication Matrix 69
Appendix C. FAQ 70

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+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+	Click Download Plug-in to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • 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.

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

Go to **Configuration → System → Security → Security Service** , and enable **Enable Illegal Login Lock**, and set the illegal login attempts.

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 Light

Click to turn on or turn off the illuminator.

3.1.6 Count Pixel

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

Steps

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

3.1.7 Start Digital Zoom

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

Steps

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

3.1.8 Auxiliary Focus

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

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

Click to focus automatically.

Note

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

3.1.9 Lens Initialization

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

Click to operate lens initialization.

3.1.10 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.

3.1.11 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.

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 .

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**.

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** and **SVC** are not configurable.

H.265

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

H.265+

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

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

Note

When H.265+ is enabled, **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.

4.3 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** .

4.3.1 Audio Encoding

Select the audio encoding compression of the audio.

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.4 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.

4.5 Display Settings

It offers the parameter settings to adjust image features.

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

4.5.1 Scene Mode

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

Image Adjustment

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

Exposure Settings

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

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

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 supplement light will be enabled to ensure clear live view image at night.

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.

Rotate

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

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

Note

This function is supported under certain settings.

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.

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.

4.5.2 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.

4.5.3 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.

4.6 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.

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**.

4.7 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**.

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.

   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 Filling 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. Click **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. 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**.

5.2 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 varies 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.

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 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 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. Certain events may not be supported by certain device models.

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

Figure 6-2 Set Rules

Stop Drawing Stop drawing one area.

Clear All Clear all the areas.

4. **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 6-3 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 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.

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

6.2 Smart Event

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 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 the 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 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.

Figure 6-4 Set Rule

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

6.2.5 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.

Figure 6-5 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**.

6.2.6 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 sensitivity.

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.

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**.

6.2.7 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 sensitivity.

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.

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**.

6.2.8 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.

Sensitivity = 100 – S1/ST*100

S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.

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.

6.2.9 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 6-8 Set Rule

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

6.2.10 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.

6.2.11 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 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 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**.

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.4 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 unaccessible.

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

HTTP Port

It refers to the port that access the device through the browser. You should enter the port No. after the IP address. For example, when the **HTTP port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for browser login.

HTTPS Port

It refers to the port of browser certificate access. Certificate verification is required when accessing the device through the browser, and the security level is high.

RTSP Port

It refers to the port of real time streaming protocol.

Server Port

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

7.5 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.

7.6 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 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 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, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

7.7 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.

7.8 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.

7.9 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.

7.9.1 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.

7.9.2 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.

7.9.3 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 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 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.

9.4 Export Diagnose Information

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

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

9.5 Reboot

You can reboot the device via browser.

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

9.6 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.

9.7 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**.

9.8 View Open Source Software License

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

9.9 Time and Date

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

9.9.1 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**.

9.9.2 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**.

9.9.3 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**.

9.9.4 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**.

9.10 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**.

9.11 Security

You can improve system security by setting security parameters.

9.11.1 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.

9.11.2 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**.

9.11.3 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** .
3. Click **Delete** to recreate and install certificate.

Create and install self-signed certificate	Refer to ***Create and Install Self-signed Certificate***
Create certificate request and install certificate	Refer to ***Install Authorized Certificate***

4. Click **Save**.

Create and Install Self-signed Certificate

Steps

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

Result

The device will install the self-signed certificate by default.

Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Select **Create certificate request first and continue the installation**.
2. Click **Create**.

3. Follow the prompt to input **Country/Region**, **Hostname/IP**, **Validity** and other parameters.
4. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
5. Import certificate to the device.
   - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
   - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
6. Click **Save**.

9.11.4 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**.

9.11.5 Set IEEE 802.1X

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

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

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

9.11.6 Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

1. Go to **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.

9.11.7 SSH

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

Go to **Configuration → System → Security → Security Service** , and check **Enable SSH**.

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.

9.12 User and Account

9.12.1 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**.

9.12.2 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 function.
3. Save the settings.

Note

Some VCA functions are mutually exclusive. When certain function or functions are selected and saved, others will not be hidden.

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.

Appendix C. FAQ

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

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

See Far, Go Further