



**Network Camera
User Manual**

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 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 user uses 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 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 a mountain top, iron tower, or forest.
-  **CAUTION!** To reduce the risk of fire, replace fuse only with the same type and rating.
- The equipment must be connected to an earthed mains socket-outlet.
- An appropriate readily accessible disconnect device shall be incorporated externally to the equipment.
- An appropriate overcurrent protective device shall be incorporated externally 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 two 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 in 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 equipment serial port 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 indicates that the marked item can be hot and should not be touched without taking care. For a device with this sticker, the device is intended for installation in a restricted access location; access can be gained only 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 overheating 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° to 60° C (-22° to 140° F), and the operating humidity shall be 95% or less (non-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 the 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 Requirements	13
Chapter 2 Device Activation and Accessing	14
2.1 Activate the Device via SADP	14
2.1.1 Before You Start	14
2.2 Activate the Device via Browser	14
2.3 Login	15
2.3.1 Plug-in Installation	15
2.3.2 Admin Password Recovery	16
2.3.3 Illegal Login Lock.....	16
2.3.4 Illegal Login Attempts	16
2.3.5 Locking Duration	16
Chapter 3 Live View	17
3.1 Live View Parameters	17
3.1.1 Enable and Disable Live View	17
3.1.2 Adjust Aspect Ratio.....	17
3.1.3 Live View Stream Type.....	17
3.1.4 Select the Third-Party Plug-in.....	17
3.1.5 Window Division.....	18
3.1.6 Light	18
3.1.7 Count Pixel	18
3.1.8 Start Digital Zoom	18
3.1.9 Auxiliary Focus	18
3.1.10 Lens Initialization.....	18
3.1.11 Manual Lens Initialization	19
3.1.12 Auto Lens Initialization	19
3.1.13 Quick Set Live View.....	19
3.1.14 Lens Parameters Adjustment	19
3.1.15 Conduct 3D Positioning.....	20
3.2 Set Transmission Parameters.....	20
3.3 Set Smooth Streaming	21
Chapter 4 Video and Audio	23
4.1 Video Settings	23

4.1.1	Stream Type	23
4.1.2	Video Type.....	23
4.1.3	Resolution	23
4.1.4	Bitrate Type and Max. Bitrate	23
4.1.5	Video Quality	23
4.1.6	Frame Rate.....	24
4.1.7	Video Encoding.....	24
4.1.8	Smoothing	25
4.2	ROI	25
4.3	Display Info. on Stream.....	26
4.4	Audio Settings	26
4.5	Two-Way Audio.....	27
4.6	Display Settings.....	27
4.6.1	Scene Mode	27
4.6.2	Image Parameters Switch	29
4.6.3	Video Standard	30
4.6.4	Local Video Output	30
4.7	OSD	30
4.8	Set Privacy Mask.....	30
4.9	Overlay Picture	31
4.10	Set Target Cropping.....	31
Chapter 5 Video Recording and Picture Capture		32
5.1	Storage Settings.....	32
5.1.1	Set New or Unencrypted Memory Card	32
5.1.2	Detect Memory Card Status	32
5.1.3	Set FTP	34
5.1.4	Set NAS.....	34
5.1.5	eMMC Protection.....	35
5.1.6	Set Cloud Storage	35
5.2	Video Recording.....	36
5.2.1	Record Automatically.....	36
5.2.2	Record Manually	37
5.2.3	Playback and Download Video.....	37
5.3	Capture Configuration	38

5.3.1	Capture Automatically	38
5.3.2	Capture Manually.....	38
5.3.3	View and Download Picture	39
Chapter 6 Event and Alarm		40
6.1	Basic Event	40
6.1.1	Set Motion Detection	40
6.1.2	Set Video Tampering Alarm	42
6.1.3	Set Exception Alarm	43
6.1.4	Set Alarm Input	43
6.1.5	Set Video Quality Diagnosis	44
6.1.6	Set Vibration Detection	44
6.2	Smart Event.....	45
6.2.1	Detect Audio Exception.....	45
6.2.2	Set Defocus Detection	45
6.2.3	Detect Scene Change	46
6.2.4	Set Intrusion Detection	46
6.2.5	Set Line Crossing Detection	47
6.2.6	Set Region Entrance Detection.....	48
6.2.7	Set Region Exiting Detection	49
6.2.8	Draw Area	50
6.2.9	Set Size Filter	51
Chapter 7 Network Settings.....		52
7.1	TCP/IPv2	
7.1.1	Multicast	53
7.1.2	Multicast Discovery	53
7.2	SNMP.....	53
7.3	Set SRTP	54
7.4	Port Mapping.....	54
7.4.1	Set Auto Port Mapping.....	54
7.4.2	Set Manual Port Mapping	55
7.4.3	Set Port Mapping on Router	55
7.5	Port.....	56
7.6	Access to Device via Domain Name.....	56
7.7	Access to Device via PPPoE Dial Up Connection	57

7.8	Set Network Service	58
7.9	Set Open Network Video Interface	58
7.10	Set ISUP	59
7.11	Set Alarm Server	59
7.12	Access Camera via Hik-Connect.....	60
7.12.1	Enable Hik-Connect Service on Camera.....	61
7.12.2	Set Up Hik-Connect	62
7.12.3	Add Camera to Hik-Connect.....	62
Chapter 8	Arming Schedule and Alarm Linkage	64
8.1	Set Arming Schedule	64
8.2	Linkage Method Settings	64
8.2.1	Trigger Alarm Output.....	64
8.2.2	FTP/NAS/Memory Card Uploading	65
8.2.3	Send Email	65
8.2.4	Notify Surveillance Center.....	66
8.2.5	Trigger Recording	66
8.2.6	Flashing Light	67
8.2.7	Audible Warning	67
Chapter 9	System and Security	69
9.1	View Device Information.....	69
9.2	Search and Manage Log.....	69
9.3	Simultaneous Login	69
9.4	Import and Export Configuration File.....	69
9.5	Search and Export Data Aware Information	69
9.6	Export Diagnose Information	70
9.7	Reboot.....	70
9.8	Restore and Default.....	70
9.9	Upgrade.....	71
9.10	View Open Source Software License	71
9.11	Wiegand.....	71
9.12	Metadata.....	71
9.13	Time and Date	71
9.13.1	Synchronize Time Manually	72
9.13.2	Set NTP Server	72

9.13.3 Synchronize Time by Satellite	72
9.13.4 Set DST	73
9.14 Set RS-485	73
9.15 Set RS-232	73
9.16 External Device	74
9.16.1 Supplement Light Settings	74
9.16.2 Heater	74
9.17 Security	74
9.17.1 Authentication	74
9.17.2 Set IP Address Filter	75
9.17.3 Set HTTPS	76
9.17.4 Set QoS	76
9.17.5 Set IEEE 802.1x	76
9.17.6 Control Timeout Settings	77
9.17.7 Search Security Audit Logs	77
9.17.8 SSH	77
9.18 Certificate Management	77
9.18.1 Create Self-signed Certificate	78
9.18.2 Create Certificate Request	78
9.18.3 Import Certificate	78
9.18.4 Install Server/Client Certificate	79
9.18.5 Install CA Certificate	79
9.18.6 Enable Certificate Expiration Alarm	79
9.19 User and Account	80
9.19.1 Set User Account and Permission	80
9.19.2 Simultaneous Login	80
9.19.3 Online Users	80
Chapter 10 Smart Function	81
10.1 Allocate VCA Resource	81
10.1.1 Road Traffic	81
10.2 Set Camera Info	84
Chapter 11 Smart Display	85
Chapter 12 EPTZ	86
12.1 Patrol	86

12.1.1 What to do next	86
12.2 Auto-Tracking	86
12.2.1 DetectionTarget	86
Appendix A. Device Command	88
Appendix B. Device Communication Matrix	89

Chapter 1 System Requirements

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:** 1 GB 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 accessing the device via a network.

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

2.1.1 Before You Start

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

Steps

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



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK**. The **Device Status** changes to **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 a Web 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.



STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.


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 a Web browser.

2.3.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	<ul style="list-style-type: none"> • Internet Explorer 8+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version 	Follow pop-up prompts to complete plug-in installation.
	<ul style="list-style-type: none"> • Google Chrome 57+ • Mozilla Firefox 52+ 	Click  Download Plug-in to download and install plug-in.
Mac OS	<ul style="list-style-type: none"> • Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+ 	Plug-in installation is not required.
		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 details of restricted functions, refer to the actual device.

NOTE: The camera supports only Windows OS and Mac OS and does not support Linux OS.

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 e-mail.

NOTE: If 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 accessing the device via a Web browser.

E-Mail

You can set the account security during the activation, or you can go to **Configuration** → **System** → **User Management**, click **Account Security Settings**, and input your e-mail address to receive a verification code during the recovery operation.

2.3.3 Illegal Login Lock

Improves security when accessing the device via the Internet.

Go to **Configuration** → **System** → **Security** → **Security Service**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

2.3.4 Illegal Login Attempts

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

2.3.5 Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Live View



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

3.1 Live View Parameters

The supported functions vary by model.







3.1.1 Enable and Disable Live View

This function quickly enables or disables 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.
 -  refers to 4:3 window size
 -  refers to 16:9 window size
 -  refers to original window size
 -  refers to self-adaptive window size
 -  refers to original ratio window size


3.1.3 Live View Stream Type

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





3.1.4 Select the Third-Party Plug-in

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


Steps

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

3.1.5 Window Division

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


3.1.6 Light

Click  to turn on or turn off the illuminator.

3.1.7 Count Pixel

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

Steps


1. Click  to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.

The width pixel and height pixel are displayed on the bottom of the live view image.

3.1.8 Start Digital Zoom

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

Steps

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

3.1.9 Auxiliary Focus

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

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

Click  to focus automatically.

NOTE: If the device cannot focus with auxiliary focus, you can use *Lens Initialization*, then use auxiliary focus again to make the image clear.


If auxiliary focus cannot help the device focus clearly, you can use manual focus.

3.1.10 Lens Initialization

Lens initialization is used on a device equipped with a motorized lens. The function can reset the lens

when long time zoom or focus results in a blurred image. This function varies by model.

3.1.11 Manual Lens Initialization

Click  to operate lens initialization.


3.1.12 Auto Lens Initialization

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

3.1.13 Quick Set Live View

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

Steps



1. Click  to show the 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 supported only by certain models.



3.1.14 Lens Parameters Adjustment

Use 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 distant object are clear.
- Click , then the lens focuses near and nearby object are clear.

PTZ Speed

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

Iris

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

PTZ Lock


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

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

3.1.15 Conduct 3D Positioning

3D positioning relocates the selected area to the image center.

Steps

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

3.2 Set Transmission Parameters

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

Steps

1. Go to Configuration → Local.
2. Set the transmission parameters as required.
 - **ProtocolTCP:** TCP ensures complete delivery of streaming data and better video quality, however real-time transmission will be affected. It is suitable for a stable network environment.
 - **UDP:** UDP is suitable for an unstable network environment that does not demand high video fluency.
 - **MULTICAST:** MULTICAST is suitable for situations in which there are multiple clients. You should set the multicast address for them before selection.

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

- **HTTP:** HTTP is suitable for situations where a third-party needs to get the stream from the device.
- **Play Performance**
 - **Shortest Delay:** The device takes the real-time video image as priority over video fluency.
 - **Balanced:** The device ensures both the real-time video image and fluency.
 - **Fluent:** The device takes the video fluency as priority over real-time. In a poor network environment, the device cannot ensure video fluency even if fluency is enabled.
 - **Custom:** You can set the frame rate manually. In a poor network environment, you can reduce the frame rate to get a fluent live view, but the rule information may not display.

3. Click **OK**.

3.3 Set Smooth Streaming

This function tackles latency and network congestion caused by unstable network conditions, and keeps the live view stream on the Web browser or the client software smooth.

Before You Start

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

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

Steps

1. Go to the settings page: **Configuration** → **Network** → **Advanced Settings** → **Smooth Streaming**.
2. Check **Enable Smooth Streaming**.
3. Select the mode for smooth streaming.
 - **Auto:** The resolution and bitrate are adjusted automatically and resolution takes priority. The upper limits of these two parameters will not exceed the values you set on the Video page. Go to **Configuration** → **Video/Audio** → **Video**, set the Resolution and Max. Bitrate before you enable the smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically.
 - **Resolution Priority:** The resolution stays the same as the set value on Video page, and the bitrate will be adjusted automatically. Go to **Configuration** → **Video/Audio** → **Video**, and set the Max. Bitrate before you enable the smooth streaming function. In this mode, the framerate will be adjusted to the maximum value automatically.
 - **Frame Rate Priority:** The image is still smooth even under a poor network, while the image quality may be not good.

- **Error Correction:** The resolution and bitrate stay the same as the set values on the **Video** page. This mode corrects data errors during transmission to ensure image quality. You can set the Error Correction Proportion within a range of 0–100.

When the proportion is 0, the data error will be corrected by data retransmission. When the proportion is higher than 0, the error data will be corrected via redundant data that is added to the stream and data retransmission. The higher the value, the more redundant data will be generated, and the more the data error would be corrected, but a larger bandwidth would be required. When the proportion is 100, the redundant data will be as large as the original data, and twice the bandwidth is required.

NOTE: Be sure the bandwidth is sufficient in the Error Correction mode.

4. Save the settings.

Chapter 4 Video and Audio

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

4.1 Video Settings

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

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

4.1.1 Stream Type

For devices that support more than one stream, you can specify the parameters for each stream type.

- **Main Stream:** This stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can accomplish. 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:** Streams other than the main stream and sub stream may also be offered for customized usage.

4.1.2 Video Type

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

- **Video:** 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 the video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

4.1.4 Bitrate Type and Max. Bitrate

- **Constant Bitrate:** 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:** The device automatically adjusts 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 the frequency at which the video stream is updated and is measured in 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

This is the compression standard the device adopts for video encoding.

NOTE: Available compression standards vary by model.

- **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 more 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 percent 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.

When H.264+ is enabled, **Video Quality, I Frame Interval, Profile, SVC, Main Stream Smoothing, and ROI** are not supported.

- **H.265:** H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, framerate 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 percent 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 two 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 that can decode only a low-resolution subset, while more advanced hardware will be able to decode a 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 are 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

This refers to the smoothness of the stream. The higher the smoothing value, the better the fluency of the stream, though, the video quality may not be so satisfactory. The lower the smoothing value, the higher the stream quality, 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 increasing the quality of the ROI whereas the background information is less focused.

Before You Start

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, the clearer the image of the detected region.

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

4.3 Display Info. on Stream

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

Steps

1. Go to the setting page: **Configuration** → **Video/Audio** → **Display Info. on Stream**.

2. Check **Enable Dual-VCA**.

3. Click **Save**.

4.4 Audio Settings

This function sets audio parameters such as audio encoding and environment noise filtering.

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

- **Audio Encoding:** Select the audio encoding compression of the audio.
- **Audio Input:** Connect the audio input device as required.

NOTE: The audio input display varies by model.

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

- **Audio Output:** This is an audio output switch. When disabled, none of the device audio can output. The audio output display varies by device mode.

NOTE: Connect the audio output device as required.

- **Environmental Noise Filter:** Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.



4.5 Two-Way Audio

Use 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 are working properly. Refer to audio input and output specifications for device connections.
- If the device has a built-in microphone and speaker, two-way audio can be enabled directly.

Steps

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

4.6 Display Settings

The parameter settings to adjust image features. Go to **Configuration** → **Image** → **Display Settings**.

Click **Default** to restore settings.

4.6.1 Scene Mode

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

Image Adjustment

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

Exposure Settings

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

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

Focus

Options to adjust the focus mode.

- **Focus Mode**
 - **Auto**: The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.
 - **Semi-auto**: The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

- **Manual:** You can adjust the focus manually on the live view page.

Day/Night Switch

Day/Night Switch function can provide color images in the day mode and turn on fill light in the night mode. Switch mode is configurable.

- **Day:** The image is always in color.
- **Night:** The image is in black/white or color and the supplement light will be enabled to ensure a clear live view image at night.

NOTE: Only certain device models support the supplement light and color image.

- **Auto:** The camera switches between day mode and 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 by model.

Grey Scale

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

Rotate

When enabled, the live view will rotate 90 ° counter-clockwise. For example, 1280 × 720 is rotated to 720 × 1280.

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

Lens Distortion Correction

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

NOTE: This function is supported only by certain devices equipped with a motorized lens.

The image edge will be lost if this function is enabled.

BLC

If you focus on an object against a 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 to **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 environments 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 areas of the image are over-exposed and the dark areas are under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright areas and brighten the dark areas, so as to achieve light balance of the overall picture.

White Balance

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

DNR

Digital Noise Reduction reduces the image noise and improves the image quality. **Normal** and **Expert** modes are selectable.

- **Normal:** Set the DNR level to control the noise reduction degree. A higher level means a stronger reduction degree.
- **Expert:** Set the DNR level for both space DNR and time DNR to control the noise reduction degree. A higher level means a stronger reduction degree.

Defog

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

EIS (Electronic Image Stabilization)

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

Mirror

When the live view image is the reverse of the actual scene, this function displays the image normally.

Select the mirror mode as needed.

NOTE: Video recording will be shortly interrupted when the function is enabled.

4.6.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set Switch

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

Steps

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

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

3. Click **Save**.

4.6.3 Video Standard

Video standard is an ability of a video card or video display device to define the number of colors that are shown and the resolution. The two most common video standards 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 the video signal standard according to the video system in your country/region.

4.6.4 Local Video Output

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

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

4.7 OSD

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

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

- **Character Set:** Select character set for displayed information. If Korean is required to displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.
- **Displayed Information:** Set camera name, date, week, and their related display format. For certain device models, you can also set the tilt angle as the displayed information.
- **Text Overlay:** Set customized overlay text on image.
- **OSD Parameters:** Set OSD parameters such as Display Mode, OSD Size, Font Color, and Alignment.

4.8 Set Privacy Mask

This function blocks certain areas in the live view to protect privacy. Regardless of how the device moves, the blocked areas will never be seen.

Steps

1. Go to the privacy mask setting page: **Configuration** → **Image** → **Privacy Mask**.
2. Check **Enable Privacy Mask**.
3. Click **Draw Area**. Drag the mouse in the live view to draw a closed area.
 - **Drag the corners of the area:** Adjust the size of the area.
 - **Drag the area:** Adjust the position of the area.
 - **Click Clear All:** Clear all the areas you set.

4. Click **Stop Drawing**.

5. Click **Save**.

4.9 Overlay Picture

Overlay a customized picture on live view.

Before You Start

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

Steps

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

The picture with a red rectangle will appear in live view after successfully uploading.

3. Check **Enable Picture Overlay**.
4. Drag the picture to adjust its position.
5. Click **Save**.

4.10 Set Target Cropping

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

Steps

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

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

3. Select a **Cropping Resolution**.

A red frame appears in the live view.

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

NOTE: Only certain models support target cropping, and the function varies by model.
Some functions may be disabled after enabling target cropping.

Chapter 5 Video Recording and Picture Capture

This chapter introduces capturing video clips and snapshots, playback, and downloading captured files.

5.1 Storage Settings

This section introduces configuring several common storage paths.

5.1.1 Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card into the device. For detailed installation, refer to *QuickStart 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, unlock the memory card first. See *Detect Memory Card Status* for details.

3. Click **Format** to initialize the memory card. When the memory card **Status** 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 secure. 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**.

5.1.2 Detect Memory Card Status

Detect the status of Hikvision memory cards . You receive notifications when your memory card is detected to be abnormal.

Before You Start

The configuration page appears only when a Hikvision memory card is installed in 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:** 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:** The condition of the 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 other than "good."

3. Click **R/W Lock** to set the reading and writing permission of the memory card.
 - **Add a Lock**
 - 1) Set the **Lock Switch** to ON.
 - 2) Enter the password.
 - 3) Click **Save**
 - **Unlock**
 - If you use the memory card on the device that locked 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**
 - 1) Set the **Lock Switch** to OFF.
 - 2) Enter the password in **Password Settings**.
 - 3) Click **Save**.

NOTE: Only the admin user can set the **R/W Lock**.

The memory card can be read and written only when it is unlocked.

If the device that 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**.

5.1.3 Set FTP

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

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **FTP**.

2. Configure FTP settings.

- **FTP Protocol:** FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.
- **Server Address and Port:** The FTP server address and corresponding port.
- **User Name and Password:** The FTP user should have permission to upload pictures.

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

- **Directory Structure:** The saving path of snapshots in the FTP server.
 - **Picture Filing Interval:** For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.
 - **Picture Name:** Set the naming rule for captured pictures. You can choose Default in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a Custom Prefix to the default naming rule.
3. Check **Upload Picture** to enable uploading snapshots to the FTP server.
4. Check Enable Automatic Network Replenishment.

NOTE: Upload to FTP/Memory Card/NAS in Linkage Method and Enable Automatic Network Replenishment should be both enabled simultaneously.

5. Click **Test** to verify the FTP server.

6. Click **Save**.

5.1.4 Set NAS

Use the network server as a 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 the 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.

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

3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

5.1.5 eMMC Protection

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

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

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

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

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

5.1.6 Set Cloud Storage

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

Steps

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

1. Go to **Configuration** → **Storage** → **Storage Management** → **Cloud Storage**.
2. Check **Enable Cloud Storage**.
3. Set basic parameters.
 - **Protocol Version:** The protocol version of the cloud video manager.
 - **Server IP:** The IP address of the cloud video manager. It supports IPv4 address.

- **Serve Port:** The port of the cloud video manager. You are recommended to use the default port.
- **Access Key:** The key to log in to the cloud video manager.
- **Secret Key:** The key to encrypt the data stored in the cloud video manager.
- **User Name and Password:** The user name and password of the cloud video manager.
- **Picture StoragePool ID:** The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

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

5. Click **Save**.

5.2 Video Recording

This section introduces 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 by model.

- **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 an alarm signal from an external alarm input device.
- **Motion | Alarm:** Video is recorded when motion is detected or an alarm signal is received from an external alarm input device.
- **Motion & Alarm:** Video is recorded only when motion is detected and an alarm signal is received from an external alarm input device.
- **Event:** The video is recorded when a 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 a higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

 - **Recording Expiration**: The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they cannot be recovered.
6. Click **Save**.

5.2.2 Record Manually

Steps

1. Go to **Configuration** → **Local**.
2. Set the **Record File Size** and saving path 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**.

Matching video files show 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 pictures manually or automatically and save them in the 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, 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 matching pictures show in the file list.

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

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

Chapter 6 Event and Alarm

This chapter introduces configuring events. The device takes certain responses to a triggered alarm.

6.1 Basic Event

6.1.1 Set Motion Detection

Detects moving objects in a detection region and triggers linkage actions.

Steps

NOTE: The function is supported only by certain device models.

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.
4. Check **Enable Dynamic Analysis for Motion**.
 - 1) Go to **Configuration** → **Local**.
 - 2) Set **Rules** to **Enable**.
5. Select **Configuration Mode**, and set rule region and rule parameters.
 - For information about normal mode, see *Normal Mode*.
 - For information about expert mode, see *Expert Mode*.
6. Set the arming schedule and linkage methods. For information about arming schedule settings, see *Set Arming Schedule*. For information about linkage methods, see *Linkage Method Settings*.
7. 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 the environment. It displays color images during the day and black and white images 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 sensitivity value, the more sensitive the motion detection. 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.

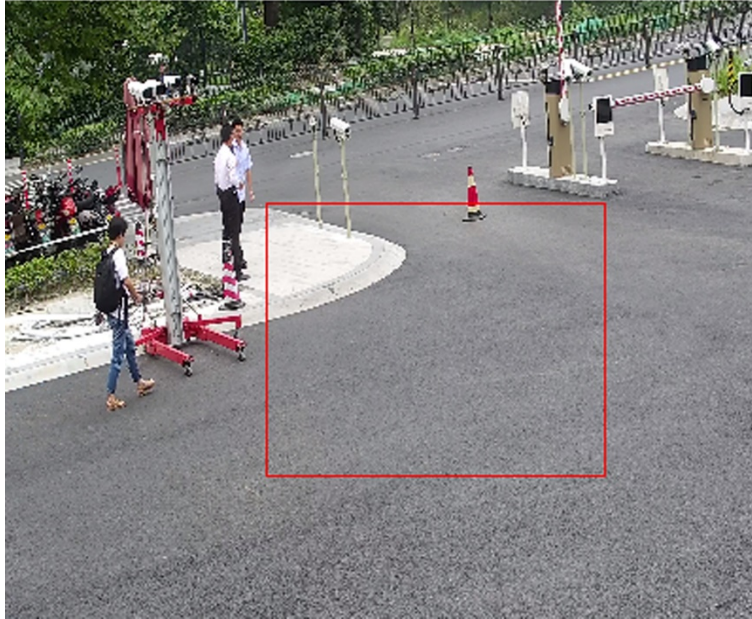


Figure 1, Set Rules

- **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 sensitivity value, the more sensitive the motion detection. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including humans and vehicles.
4. Click **Draw Area**. Click and drag the mouse on the live video, and then release the mouse to finish drawing one area.
 - **Stop Drawing:** Stop drawing one area.

- **Clear All:** Clear all the areas.

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

6.1.2 Set Video Tampering Alarm

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

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Video Tampering**.
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value, 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.

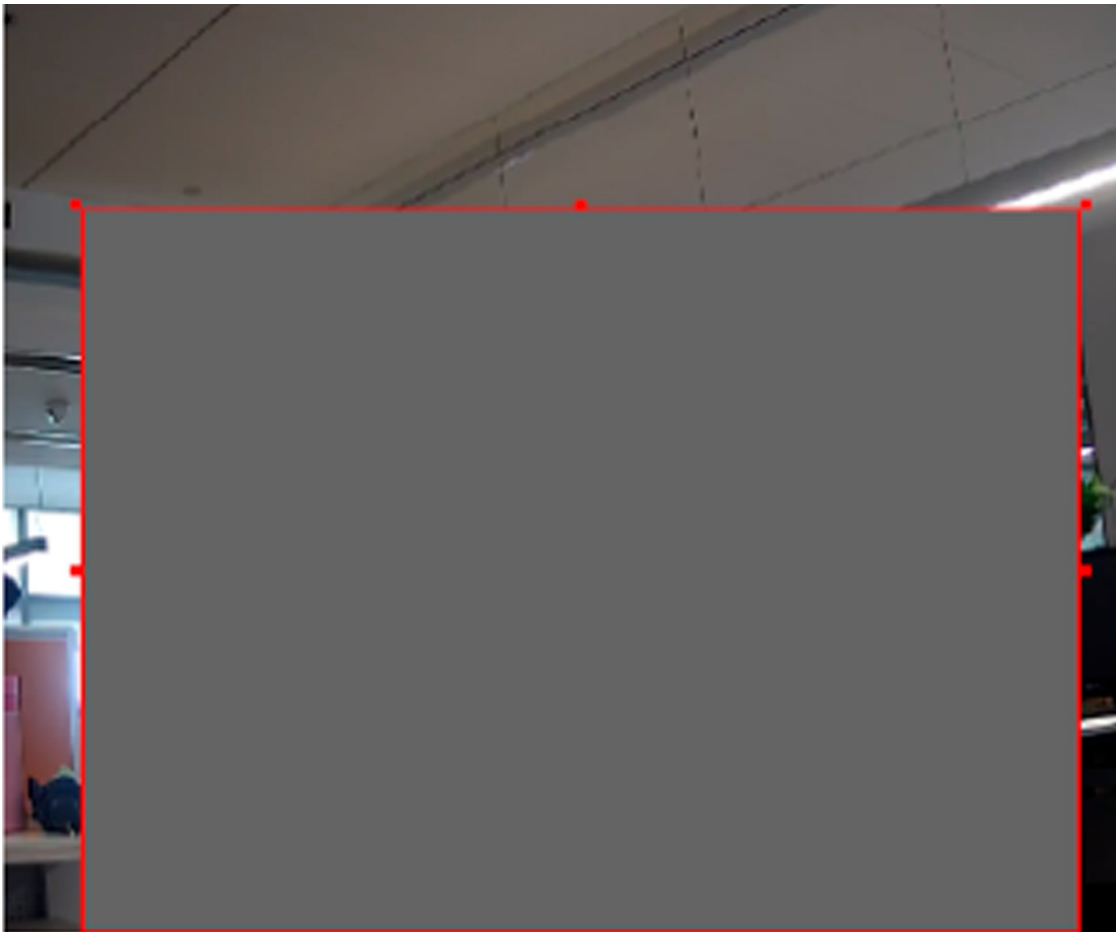


Figure 2, Set Video Tampering Area

5. Refer to *Set Arming Schedule* for setting scheduled time. Refer to *Linkage Method Settings* for setting

linkage method.

6. Click **Save**.

6.1.3 Set Exception Alarm

Exceptions such as network disconnection can trigger the device to take a 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 in the HDD.
 - **Network Disconnected**: The device is offline.
 - **IP Address Conflicted**: The IP address of current device is same as that of another device in the network.
 - **Illegal Login**: Incorrect user name or password entered.
3. Refer to *Linkage Method Settings* for setting linkage method.
4. Click **Save**.

6.1.4 Set Alarm Input

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

Before You Start

This function is supported only by certain models.

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

Steps

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

6.1.5 Set Video Quality Diagnosis

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

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Video Quality Diagnosis**.
2. Select **Diagnosis Type**.
3. Set the corresponding parameters.
 - **Alarm Detection Interval:** The time interval to detect the exception.
 - **Sensitivity:** The higher the value, the more easily the exception will be detected, and the higher the possibility of misinformation.
 - **Alarm Delay Times:** The device uploads the alarm when the alarm reaches the set number.
4. Check **Enable**, and the selected diagnosis type will be detected.
5. Set arming schedule. See *Set Arming Schedule*.
6. Set linkage method. See *Linkage Method Settings*.
7. Click **Save**.

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

6.1.6 Set Vibration Detection

Detects if the device is vibrating. The device reports an alarm and triggers linkage actions if the function is enabled.

Steps

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

NOTE: The function is supported only by certain models. The actual display varies by model.

6.2 Smart Event

NOTE: For certain device models, you need to enable the smart event function on the **VCA Resource** page first to show the function configuration page.

The function varies by model.

6.2.1 Detect Audio Exception

Detects abnormal sound in the surveillance scene such as the sudden increase/decrease in sound intensity, and certain actions can be taken in 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 in sound intensity. Sensitivity and Sound Intensity Threshold are configurable.

NOTE: The lower the sensitivity, the more significant the change must be to trigger the detection.

The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set it 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 by model.

6.2.2 Set Defocus Detection

A 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, the more easily the defocused image can trigger the alarm. Adjust

the value according to the actual environment.

4. For the linkage method settings, refer to *Linkage Method Settings*.
5. Click **Save**.

NOTE: This function is supported only by certain models. The actual display varies by model.

6.2.3 Detect Scene Change

Detects a change of the surveillance scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration** → **Event** → **Smart Event** → **Scene Change Detection**.
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value, 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 by model.

6.2.4 Set Intrusion Detection

Detects 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:** The percentage of the body part of an acceptable target that enters the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that crosses the pre-defined region. ST stands for the complete target body. The higher the sensitivity value, the more easily the alarm will be triggered.
 - **Threshold:** Time the object loiters in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold, the longer the alarm triggering time.

- **Detection Target:** Human and vehicle are available. If the detection target is not selected, all detected targets will be reported, including humans and vehicles.
- **Target Validity:** If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. A target with less obvious features would be missed.



Figure 3, Set Rule

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

6.2.5 Set Line Crossing Detection

Detects objects crossing a pre-defined virtual line. If it occurs, the device can take linkage actions.

Steps

- Go to **Configuration** → **Event** → **Smart Event** → **Line Crossing Detection**.
- Check **Enable**.
- Select one **Line** and set the size filter. For the size filter settings, refer to *Set Size Filter*.
- 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.
- Set rules.
 - **Direction:** The direction from which the object goes across the line.
 - **A<->B:** An object crossing the line from either direction is detected and alarms are triggered.

- **A->B:** An object crossing the configured line only from the A side to the B side will be detected.
- **B->A:** An object crossing the configured line only from the B side to the A side will be detected.
- **Sensitivity:** The percentage of the body part of an acceptable target that crosses the pre-defined line. $\text{Sensitivity} = 100 - S1/ST \times 100$. 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.
- **DetectionTarget:** Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including humans and vehicles.
- **Target Validity:** If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. A target with less obvious features would be missed.

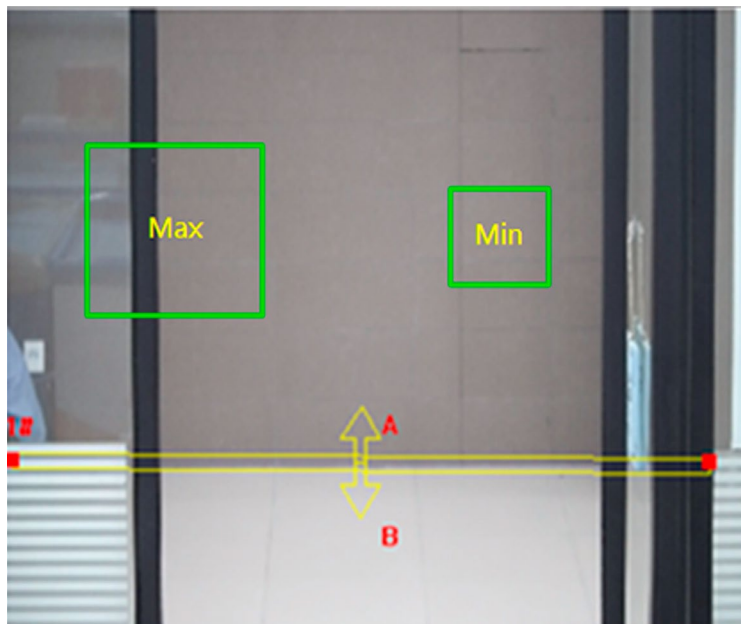


Figure 4, Set Rule

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

6.2.6 Set Region Entrance Detection

Detects objects entering a pre-defined virtual region. If it occurs, the device can take linkage actions.

Steps

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

4. Set the detection target, sensitivity, and the target validity.
 - **Sensitivity:** The percentage of the body part of an acceptable target that crosses the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that crosses the pre-defined region. ST stands for the complete target body. The higher the sensitivity value, the more easily the alarm can be triggered.
 - **Detection Target:** Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including humans and vehicles.
 - **Target Validity:** If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. A target with less obvious features would be missed.

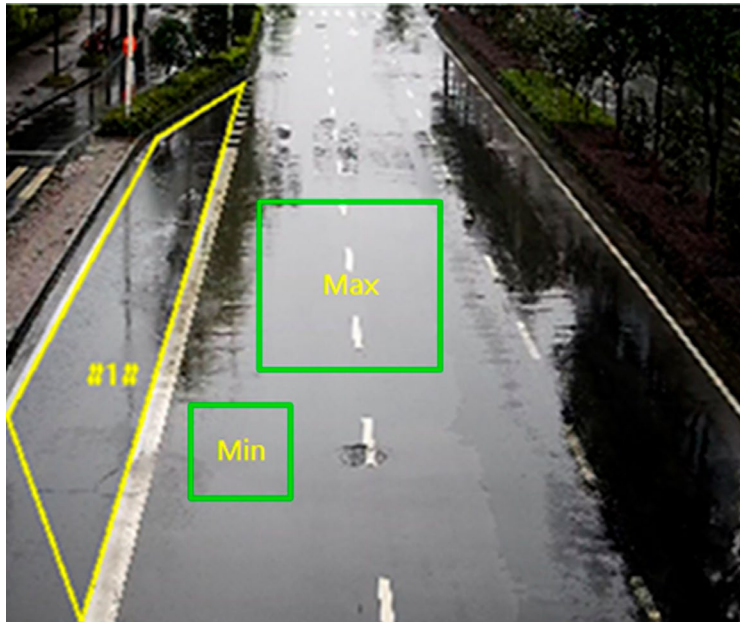


Figure 5, Set Rule

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

6.2.7 Set Region Exiting Detection

Detects objects exiting 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 detection region settings, refer to *Draw Area*.
4. Set the detection target, sensitivity, and target validity.

- **Sensitivity:** The percentage of the body part of an acceptable target that crosses the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that crosses the pre-defined region. ST stands for the complete target body. The higher the sensitivity value, the more easily the alarm can be triggered.
- **Detection Target:** Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including humans and vehicles.
- **Target Validity:** If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. A target with less obvious features would be missed.

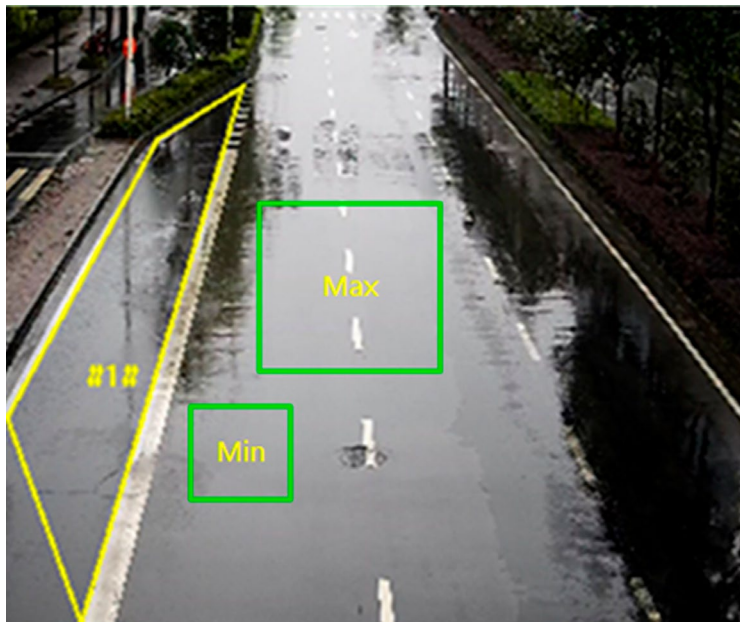


Figure 6, Set Rule

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

6.2.8 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.

6.2.9 Set Size Filter

This section introduces setting the size filter. Only targets whose size is between the minimum value and maximum value are detected and trigger alarms.

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 a network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting with 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.

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.

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 (Domain Name Server):** Required if you need to visit the device with a domain name. It is also required for some applications (e.g., sending e-mail). 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 must be enabled for the dynamic domain name to take effect.

7.1.1 Multicast

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

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

- **IP Address:** It stands for the address of multicast host.
- **Stream Type:** The stream type of the multicast source.
- **Video Port:** The video port of the selected stream.
- **Audio Port:** The audio port of the selected stream.
- **FEC Port:** The FEC port of the selected stream.
- **FEC Ratio:** The ratio of forward error correction.

7.1.2 Multicast Discovery

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

7.2 SNMP

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

Before You Start

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

Steps

1. Go to the settings page: **Configuration** → **Network** → **Advanced Settings** → **SNMP**.
2. Check **Enable SNMPv1**, **Enable SNMP v2c**, or **Enable SNMPv3**.

The SNMP version you select should be the same as that of the SNMP software.

NOTE: You must use the version based on the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. SNMP v3 provides encryption and HTTPS protocol must be enabled.

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

7.3 Set SRTP

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

Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **SRTP**.
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.

NOTE: Only certain device models support this function.

If the function is abnormal, check if the selected certificate is abnormal in certificate management.

7.4 Port Mapping

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

Before You Start

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

Steps

1. Go to **Configuration** → **Network** → **Basic Settings** → **NAT**.
2. Select the port mapping mode.
 - **Auto Port Mapping:** Refer to *Set Auto Port Mapping* for detailed information.
 - **Manual Port Mapping:** Refer to *Set Manual Port Mapping* for detailed information.
3. Click **Save**.

7.4.1 Set Auto Port Mapping

Steps

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

Enable the UPnP™ function on the router at the same time.

7.4.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or use the default name.
2. Set the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What To Do Next

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

7.4.3 Set Port Mapping on Router

The following settings are for a specific router. The settings vary depending by router.

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 Servers**, 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, and 555 with IP address 192.168.1.24.

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings
- Network
- Wireless
- Advanced Settings
- DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- Security
 - Static Routing
 - Dynamic DNS
- Maintenance
- System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure 7, Port Mapping on Router

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

7.5 Port

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



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

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

- **HTTP Port:** The port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter *http://192.168.1.64:81* in the browser for login.
- **HTTPS Port:** The port through which the browser accesses the device with certificate. Certificate verification is required to ensure secure access.
- **RTSP Port:** The real-time streaming protocol port.
- **SRTP Port:** The secure real-time transport protocol port.
- **Server Port:** The port through which the client adds the device.
- **Enhanced SDK Service Port:** The port through which the client adds the device. Certificate verification is required to ensure secure access.
- **WebSocket Port:** TCP-based full-duplex communication protocol port for plug-in free preview.
- **WebSockets Port:** TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure secure access.

NOTE: Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are supported only by certain models.

For device models that support that function, go to **Configuration** → **Network** → **AdvancedSettings** → **Network Service** to enable it.

7.6 Access to Device via Domain Name

You can use Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize network access via a 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 Browser**: Enter the domain name in the browser address bar to access the device.
 - **By Client Software**: Add domain name to the client software. Refer to the client manual for specific adding methods.

7.7 Access to Device via PPPoE Dial Up Connection

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

Steps

1. Go to **Configuration** → **Network** → **Basic Settings** → **PPPoE**.
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.
 - **Dynamic IP**: After successful dial-up, the dynamic IP address of the WAN is displayed.
 - **User Name**: User name for dial-up network access.
 - **Password**: Password for dial-up network access.
 - **Confirm**: Input your dial-up password again.
4. Click **Save**.
5. Access the device.
 - **By Browser**: Enter the WAN dynamic IP address in the browser address bar to access the device.
 - **By Client Software**: Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

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

Access to Device via DomainName for detailed information.

7.8 Set Network Service

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

Steps

NOTE: This function varies by model.

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 or its above version or Mozilla Firefox 52 or 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**. If you use **WebSockets**, select the **Server Certificate**.

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

- **SDK Service & Enhanced SDK Service:** Check Enable SDK Service to add the device to the client software with SDK protocol.

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

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

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

When setting up a 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 client software user manual for 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**.

7.9 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.

7.10 Set ISUP

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

7.11 Set Alarm Server

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

Steps

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

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

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

7.12 Access Camera via Hik-Connect

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

Before You Start

Connect the camera to a network with network cables.

Steps

1. Get and install the Hik-Connect application in 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 such as “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 Hik-Connect app user manual.

7.12.1 Enable Hik-Connect Service on Camera

Enable Hik-Connect service on your camera before using the service. You can enable the service through SADP software or a Web browser.

Enable Hik-Connect Service via Web Browser

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

Before You Start

Activate the camera before enabling the service.

Steps

1. Access the camera via a 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 the 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 the **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.

7.12.2 Set Up Hik-Connect

Steps

1. Get and install the Hik-Connect application in 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 such as “Unknown app” occur during the installation, solve the problem in two ways.

Visit <https://appstore.hikvision.com/static/help/index.html> and 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.

7.12.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi access point.
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 blurry 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 the **Platform Access** configuration page via a Web browser.

6. Tap **Connect to a Network** button in the pop-up 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 three 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 resulting interface.

NOTE: The router should be the same one that your mobile phone has connected to.

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

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

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 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 eight 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 configuration information, see *Automatic Alarm*.
 - **Manual Alarm:** For configuration information, 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:** Enter a custom 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 to have the device trigger an alarm output automatically during 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:** Enter a custom name for the alarm output.
 - **Delay:** 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 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 e-mail to the designated addresses with alarm information when an alarm event is detected.

For e-mail 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 e-mail 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** → **BasicSettings** → **TCP/IP** for DNS settings.

Steps

1. Go to the e-mail settings page: **Configuration** → **Network** → **Advanced Settings** → **Email**.
2. Set e-mail parameters.
 - 1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
 - 2) Optional: If your e-mail 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**, e-mails are sent after being encrypted by SSL or TLS. The SMTP port should be set as 465.
 - When you select **SSL** or **TLS** and **Enable STARTTLS**, e-mails are sent after being encrypted by STARTTLS. The SMTP port should be set as 25.

NOTE: To use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check **Enable STARTTLS** and the protocol is not supported by your e-mail server, your e-mail is sent with no encryption.

 - 4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification e-mail has three 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 properly configured.
3. Click **Save**.

8.2.4 Notify Surveillance Center

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

8.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event. For recording settings, refer to *Video Recording and Picture Capture*.

8.2.6 Flashing Light

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

Set Flashing Alarm Light Output

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

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Flashing Alarm Light Output**.
2. Set **Flashing Duration**, **Flashing Frequency**, and **Brightness**.
 - **Flashing Duration**: The time that the flashing lasts when one alarm happens.
 - **Flashing Frequency**: The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.
 - **Brightness**: The brightness of the light.
3. Set the arming schedule. See **Set Arming Schedule** for details.
4. Click **Save**.

NOTE: Only certain device models support this function.

8.2.7 Audible Warning

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

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

NOTE: The function is only supported by certain camera models.

Set Audible Alarm Output

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

Steps

1. Go to **Configuration** → **Event** → **Basic Event** → **Audible Alarm Output**.
2. Select **Sound Type** and set related parameters.
 - Select **Prompt** and set the alarm times you need.
 - Select **Warning** and its contents. Set the alarm times you need.
 - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.

3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See *Set Arming Schedule* for details.
5. Click **Save**.

NOTE: The function is supported only by certain device models.

Chapter 9 System and Security

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

9.1 View Device Information

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

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

9.2 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

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

The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files in your computer.

9.3 Simultaneous Login

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

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

9.4 Import and Export Configuration File

This speeds 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 the configuration file.

9.5 Search and Export Data Aware Information

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

Before You Start

Log in to the device via the admin user account.

Steps

1. Go to **Application** → **Data Aware**.
2. Select the search condition.
 - **Statistics Type**: Options
 - **Capture Alarm**: Report Type, alarm target, protocol, alarm link, and start time
 - **Restart Records**: Statistics type, start time, and end time
 - **Arming**: Arming type, start time, and end time
3. Click **Counting**. The data information that matches the conditions will be displayed.
4. Optional: Click **Export** to save the data information to the local device.

9.6 Export Diagnose Information

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

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

9.7 Reboot

You can reboot the device via a Web browser.

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

9.8 Restore and Default

Restore and Default restores 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.

9.9 Upgrade

Before You Start

Obtain the correct upgrade package.



CAUTION! DO NOT disconnect power during the process. The device reboots automatically after upgrading.

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

9.10 View Open Source Software License

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

9.11 Wiegand

This function is supported only by certain camera models.

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

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

9.12 Metadata

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

Go to **Configuration** → **System** → **Metadata Settings** to enable metadata uploading of the desired function.

Road Traffic

The metadata of road traffic is detected vehicle information, including the vehicle location in the scene, vehicle ID, license plate, validity, moving direction, country/region, etc.

9.13 Time and Date

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

9.13.1 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**.

9.13.2 Set NTP Server

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

Before You Start

Set up an 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 the NTP server IP address.

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

9.13.3 Synchronize Time by Satellite

NOTE: This function varies by device.

Steps

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

4. Click **Save**.

9.13.4 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), 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**.

9.14 Set RS-485

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

Before You Start

Connect the device and computer or terminal with an RS-485 cable.

Steps

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

NOTE: Keep the parameters of the device and the computer or terminal the same.

3. Click **Save**.

9.15 Set RS-232

RS-232 can be used to debug a device or access a 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 an RS-232 cable.

Steps

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

9.16 External Device

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

External devices vary by model.

- **Brightness:** Adjust Low Beam Brightness and High Beam Brightness according to the actual scene.
- **Timing:** The LED light will be turned on by the schedule you set. You should set **Start Time** and **End Time**.
- **Auto:** The LED light will be turned on according to the environment illumination.

9.16.1 Supplement Light Settings

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

- **Smart Supplement Light:** Smart supplement light avoids overexposure when the supplement light is on.
- **Supplement Light Mode:** If the device supports a supplement light, you can select supplement light mode.
- **IR Mode:** IR light is enabled.
- **White Light Mode:** White light is enabled.
- **Mix Mode:** Both IR light and white light are enabled.
- **Off:** Supplement light is disabled.
- **Brightness Adjustment Mode**
 - **Auto:** The brightness adjusts according to the actual environment automatically.
 - **Manual:** You can drag the slider or set value to adjust the brightness.

9.16.2 Heater

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

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

9.17 Security

You can improve system security by setting security parameters.

9.17.1 Authentication

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

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

- **RTSP Authentication:** Digest and digest/basic are supported, which means authentication information is needed when an 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 supports only 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 a 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 supports only digest authentication.
- **WEB Digest Algorithm:** MD5, SHA256, and MD5/SHA256 encrypted algorithm in Web authentication. If you enable the digest algorithm, except MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

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

9.17.2 Set IP Address Filter

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

IP address refers to IPv4.

Steps

1. Go to **Configuration** → **System** → **Security** → **IP Address Filter**.
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.
 - **Forbidden:** IP addresses in the list cannot access the device.
 - **Allowed:** Only IP addresses in the list can access the device.
4. Edit the IP address filter list.
 - **Add:** Add a new IP address or IP address range to the list.
 - **Modify:** Modify the selected IP address or IP address range in the list.
 - **Delete:** Delete the selected IP address or IP address range in the list.
5. Click **Save**.

9.17.3 Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

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

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

9.17.4 Set QoS

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

NOTE: QoS needs support from the network devices such as the router and switch.

Steps

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

NOTE: The network can identify the data transmission priority. The bigger the DSCP value, the higher the priority. Set the same value in the router while configuring.

3. Click **Save**.

9.17.5 Set IEEE 802.1x

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

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

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

- **Protocol:** EAP-LEAP, EAP-TLS, and EAP-MD5 are selectable
- **EAP-LEAP and EAP-MD5:** If you use EAP-LEAP or EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1x in the server in advance. Input the user name and password for authentication.

- **EAP-TLS:** If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate, and Private Key.
- **EAPOL Version:** The EAPOL version must be identical with that of the router or the switch.

9.17.6 Control Timeout Settings

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

Go to **Configuration** → **System** → **Security** → **Advanced Security** to complete settings.

9.17.7 Search Security Audit Logs

You can search and analyze the security log files of the device to find illegal intrusions and troubleshoot security events.

Steps

NOTE: This function is supported only by certain camera models.

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

The log files that match the search conditions will be displayed on the Log List.

4. **Optional:** Click **Export** to save the log files to your computer.

9.17.8 SSH

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

The SSH function is disabled by default.



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

9.18 Certificate Management

This manages the server/client certificates and CA certificate, and sends an alarm if the certificates are close to expiry date or are expired/abnormal.

NOTE: The function is supported only by certain device models.

9.18.1 Create Self-signed Certificate

Steps

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

NOTE: The certificate ID should be digits or letters and be no more than 64 characters.

3. Click **OK**.
4. Optional: Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

9.18.2 Create Certificate Request

Before You Start

Select a self-signed certificate.

Steps

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

9.18.3 Import Certificate

Steps

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

NOTE: Up to 16 certificates are allowed.

If certain functions are using the certificate, it cannot be deleted.

You can view the functions that are using the certificate in the functions column.

You cannot create a certificate that has the same ID as an existing certificate or import a certificate that has the same content as an existing certificate.

9.18.4 Install Server/Client Certificate

Steps

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

9.18.5 Install CA Certificate

Steps

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

NOTE: Up to 16 certificates are allowed.

9.18.6 Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an e-mail or camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.

Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)**, and **Detection Time (hour)**.

NOTE: If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.

If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire at 9:00 the next day, the camera will remind you at 10:00 the first day.

2. Click **Save**.

9.19 User and Account

9.19.1 Set User Account and Permission

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



CAUTION! To increase security of using the device on the network, change the password of your account regularly. Changing the password every three months is recommended. If the device is used in a high-risk environment, it is recommended that the password 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 for all operations and can add users and operators and assign permissions.
 - **User:** Users can be assigned permission to view live video, set PTZ parameters, and change their own passwords, but no permission for other operations.
 - **Operator:** Operators can be assigned all permissions except for operations on the administrator and creating accounts.
 - **Modify:** Select a user and click **Modify** to change the password and permission.
 - **Delete:** Select a user and click **Delete**.

NOTE: The administrator can add up to 31 user accounts.

3. Click **OK**.

9.19.2 Simultaneous Login

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

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

9.19.3 Online Users

The information of users logged into the device is shown.

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

Chapter 10 Smart Function

10.1 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 **VCA → VCA Resource**.
2. Select desired VCA functions.
3. Save the settings.

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

10.1.1 Road Traffic

Vehicle Detection and **Mixed-traffic Detection** are available for road traffic monitoring. The device captures passing motor vehicles and non-motor vehicles and uploads relevant information together with captured pictures.

NOTE: For certain device models, you need to select **Road Traffic** on **VCA Resource** page first.

This function is supported only by certain device models.

Set Vehicle Detection

The vehicles that enter the set lane can be detected and a picture of the vehicle and its license plate can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

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

Steps

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

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

6. Select **Region** and **Country/Region**.
7. Select the license plate information upload mode.
 - **Entrance/Exit:** The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in entrance/exit.
 - **City Street:** The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in city streets.
 - **Alarm Input:** The input alarm will trigger a license plate capture and recognition action.

NOTE: When **Alarm Input** is selected, the alarm input **A<-1** will automatically be assigned to trigger vehicle detection and its alarm type is always **NO**.

If the **A<-1** alarm input is used to trigger vehicle detection, it can not be used for other basic events.

When **Alarm Input** is selected and saved, previously configured linkage method for **A<-1** will be canceled.

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

NOTE: Up to eight license plates are supported.

10. Set arming schedule and linkage method. For arming schedule settings, refer to *Set ArmingSchedule*. For the linkage method settings, refer to *Linkage Method Settings*.

11. Click **Save**.

Set Mixed-Traffic Detection Rule

Motor vehicles and non-motor vehicles that enter the set lane can be detected, and the pictures of targets can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

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

Steps

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

red frame. Only the position of the red frame is adjustable.

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

6. Select **Region** and **Country/Region**.

7. Check **Remove Duplicated License Plates** and set **Time Interval**. The default time interval is four minutes.

NOTE: Up to eight license plates are supported.

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

9. Click **Save**.

Uploading Pictures Settings

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

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

- **Picture Quality:** The larger the value, the clearer the picture, but larger storage space is also required.
- **Picture Size:** The larger the value, the larger the storage space needed, and the level of network transmission requirement is also higher.
- **License Plate Enhancement:** The larger the value, the clearer the license plate, but larger storage space is also required. Check License Plate Enhancement and set the level. The default level is 50.

NOTE: Only certain device models support this function.

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

Import or Export Blocklist & Allowlist

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

Steps

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

NOTE: The file to import should correspond with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.

The file should be in.xls format and the cell format should be "text."

3. Click **Import** to import the selected file.
4. Click **Export** to open the PC local directory.

5. Select a directory in your PC local directory.
6. Name the file in the file name text field.
7. Click **Save**.

10.2 Set Camera Info

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




Go to **VCA** → **General VCA Resource** to set **Camera No.** and **Camera Info**.



Chapter 11 Smart Display

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



NOTE: The function is supported only when certain smart functions are enabled.

- **Live View Parameters**

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

- **Download Display Pictures:** Click  and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click  again to download the pictures in a package.

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

- **Layout:** Click  and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.
- **Detect Feature:** Click  and choose **Detect Feature**. Check the corresponding checkbox to display the features of the detection target.

Chapter 12 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, select the **Fourth Stream** in live view. Fourth stream and EPTZ must both be enabled simultaneously.

NOTE: The function is supported only by certain device models.

12.1 Patrol

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Patrol** in **Application**.
5. Click **Save**.

12.1.1 What to do next

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

12.2 Auto-Tracking

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Auto-tracking** in **Application**.
5. Click **Detection Area** to start drawing.
6. Click on the live video to specify the four vertexes of the detection area, and right click to complete drawing.
7. Set rules.

12.2.1 DetectionTarget

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

NOTE: Only certain camera models support this function.

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

8. Click **Save**.

Appendix A. Device Command

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

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

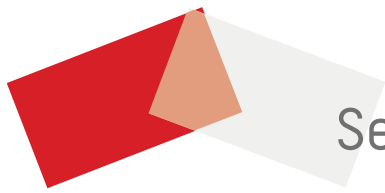


Appendix B. Device Communication Matrix

Scan the following QR code to get the device communication matrix.

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





See Far, Go Further