



Network Camera

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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




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

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

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

Symbol Conventions

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

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

Safety Instruction

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



Figure 1-1 Safety Instruction

Contents

Chapter 1 Device Activation and Accessing	1
1.1 Activate Device	1
1.1.1 Activate via SADP	1
1.1.2 Activate Camera via iVMS-4200	2
1.1.3 Activate Device via Web Browser	3
1.2 Access Camera	4
1.2.1 Access Camera via Web Browser	4
1.2.2 Access Camera via iVMS-4200	6
1.2.3 Access Camera via Hik-Connect	6
Chapter 2 Network Camera Configuration	11
2.1 Update Firmware	11
2.2 System Requirement	11
2.3 Live View	11
2.3.1 Live View Parameters	11
2.3.2 Set Transmission Parameters	17
2.3.3 Set Smooth Streaming	18
2.4 Video and Audio	19
2.4.1 Video Settings	19
2.4.2 ROI	23
2.4.3 Display Info. on Stream	24
2.4.4 Audio Settings	24
2.4.5 Two-way Audio	25
2.4.6 Display Settings	26
2.4.7 OSD	33
2.4.8 Set Privacy Mask	34
2.4.9 Overlay Picture	34

2.5 Video Recording and Picture Capture	34
2.5.1 Storage Settings	35
2.5.2 Video Recording	39
2.5.3 Capture Configuration	41
2.6 Event and Alarm	43
2.6.1 Basic Event	43
2.6.2 Smart Event	47
2.7 Network Settings	49
2.7.1 TCP/IP	49
2.7.2 SNMP	51
2.7.3 Set SRTP	52
2.7.4 Port Mapping	52
2.7.5 Port	54
2.7.6 Access to Device via Domain Name	55
2.7.7 Access to Device via PPPoE Dial Up Connection	56
2.7.8 Set Network Service	56
2.7.9 Set Open Network Video Interface	58
2.7.10 Set ISUP	58
2.7.11 Set Alarm Server	58
2.8 Arming Schedule and Alarm Linkage	59
2.8.1 Set Arming Schedule	59
2.8.2 Linkage Method Settings	59
2.9 System and Security	63
2.9.1 View Device Information	64
2.9.2 Search and Manage Log	64
2.9.3 Simultaneous Login	64
2.9.4 Import and Export Configuration File	64
2.9.5 Export Diagnose Information	64

2.9.6 Reboot	64
2.9.7 Restore and Default	65
2.9.8 Upgrade	65
2.9.9 Device Auto Maintenance	65
2.9.10 View Open Source Software License	66
2.9.11 Time and Date	66
2.9.12 Set RS-485	67
2.9.13 Set RS-232	68
2.9.14 External Device	68
2.9.15 Security	69
2.9.16 Certificate Management	72
2.9.17 User and Account	74
2.10 VCA Resource	76
2.10.1 Set Open Platform	76
2.10.2 Set Camera Info	76
2.10.3 People Counting	77
2.10.4 Heat Map	79
Appendix A. FAQ	82

Chapter 1 Device Activation and Accessing

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



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

1.1 Activate Device

The device needs to be activated by setting a strong password before use. This part introduces activation using different client tools.

1.1.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website <http://www.hikvision.com/>, and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should belong to the same subnet.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

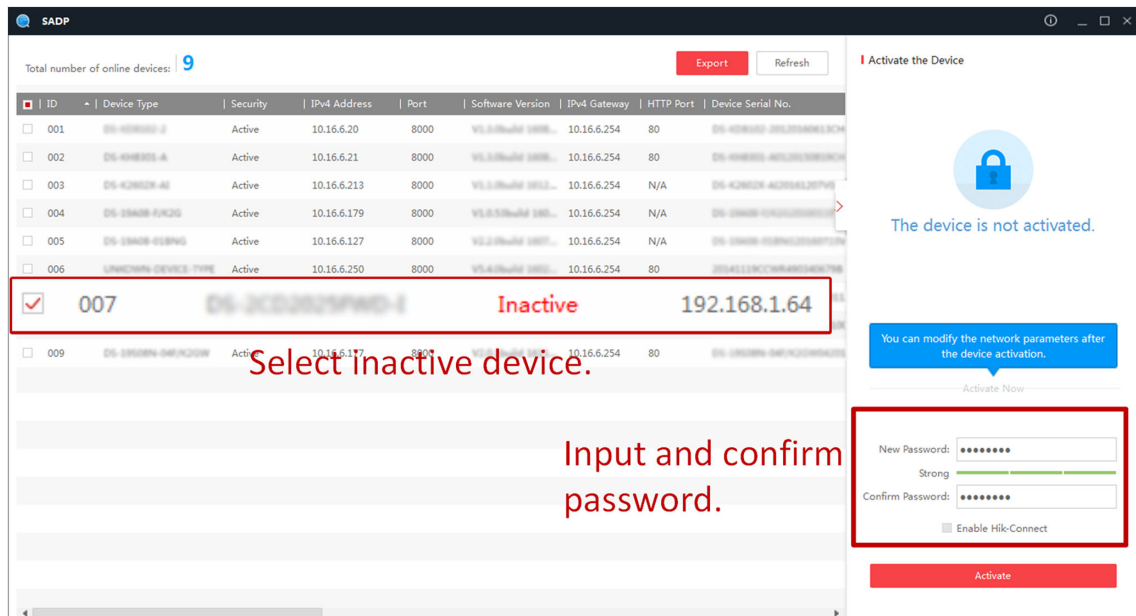
Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



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

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

1.1.2 Activate Camera via iVMS-4200

iVMS-4200 is a PC client to manage and operate your devices. Camera activation is supported by the software.

Before You Start

- Get the client software from the supplied disk or the official website <http://www.hikvision.com/en/>. Install the software following the prompts.
- The camera and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.
2. Enter **Device Management** or **Online Device**.
3. Check the device status from the device list, and select an inactive camera.
4. Click the **Activate**.
5. Create and confirm the admin password of the camera.



Caution

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

6. Click **OK** to start activation.

Device status change to **Active** after successful activation.

7. Modify IP address of the device.

1) Select the device and click **Modify Netinfo** at **Online Device**.

2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.

3) Input the admin password of the device and click **OK** to complete modification.

1.1.3 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or PC client to activate the device.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Change the IP address of your PC to the same subnet as the device.

The default IP address of the device is 192.168.1.64.

2. Open a web browser and input the default IP address.

3. Create and confirm the admin password.



Caution

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

4. Click **OK** to complete activation and enter **Live View** page.

5. Modify IP address of the camera.

1) Enter IP address modification page. **Configuration** → **Network** → **TCP/IP**

2) Change IP address.

3) Save the settings.

1.2 Access Camera

This part introduces how to access the camera via Web browser or client software.

1.2.1 Access Camera via Web Browser

Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements. For the system requirement, see [System Requirement](#) .

Steps

1. Open the web browser.



For some web browsers, a plug-in is required. For detailed requirements, see [Plug-in Installation](#) .

2. Input IP address of the camera to enter the login interface.
3. Input user name and password.



Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.
If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.


4. Click **Login**.
5. Download and install appropriate plug-in for your web browser.
For IE based web browser, webcomponents and TM are optional. For non-IE based web browser, webcomponents, TM, VLC and MJPEG are optional.

What to do next

- You can recover admin password. For detailed settings, see [Admin Password Recovery](#) .
- You can set illegal login lock to improve security. For detailed settings, see [Illegal Login Lock](#) .

Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	<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+ 	<p>Plug-in installation is not required.</p> <p>Go to Configuration → Network → Advanced Settings → Network Service to enable WebSocket or Websockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.</p>

 **Note**

The camera only supports Windows and Mac OS system and do not support Linux system.

Admin Password Recovery

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

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

 **Note**

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

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, select the security question and input your answer.

You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

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

Illegal Login Lock

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

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

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

1.2.2 Access Camera via iVMS-4200

Add the camera to client software before further operation.

Refer to the *iVMS-4200 Client Software User Manual* for detailed setting steps.

1.2.3 Access Camera via Hik-Connect

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

Before You Start

Connect the camera to network with network cables.

Steps

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



Note

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

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

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

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

Enable Hik-Connect Service on Camera

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

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

Enable Hik-Connect Service via Web Browser

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

Before You Start

You need to activate the camera before enabling the service.

Steps

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

Note

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

-
7. Save the settings.

Enable Hik-Connect Service via SADP Software

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

Steps

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



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.

Set Up Hik-Connect

Steps

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



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

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

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

Add Camera to Hik-Connect

Steps

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



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

5. Input the verification code of your camera.



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

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

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



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

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

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

Initialize Memory Card via Hik-Connect

Memory card requires initialization before saving camera recordings and pictures.

Steps

1. Check the memory card status by tapping on **Storage Status** in the device settings interface.
2. If the memory card status displays as Uninitialized, tap to initialize it.

The status will change to Normal after the successful initialization.

Result

You can then start recording any event triggered video in the camera such as motion detection.

Chapter 2 Network Camera Configuration

2.1 Update Firmware

For better user experience, we recommend you to update your device to the latest firmware asap. Please get the latest firmware package from the official website or the local technical expert. For more information, please visit the official website: <https://www.hikvision.com/en/support/download/firmware/> .

For the upgrading settings, refer to [Upgrade](#) .

2.2 System Requirement

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

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

2.3 Live View

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

2.3.1 Live View Parameters

The supported functions vary depending on the model.

Display Control

The display control area allows you to select the decoding mode, mount type, and display mode of live view. You can select software or hardware decoding mode and then select one of the multiple mount types and display modes accordingly.




Decoding Mode

- **Software** decoding mode refers to that the live view video is decoded by the CPU of the computer. The live view performance depends on the decoding ability of the computer.
- **Hardware** decoding mode refers to that the live view video is decoded by the camera.

Mount Type

You can select ceiling mounting, wall mounting, and table mounting according to the actual mount type of your camera. The descriptions of all mount type icons are as follows:

Table 2-1 Descriptions of Mount Types

Icon	Description
	Wall mounting
	Table mounting
	Ceiling mounting





 **Note**











The mount type varies depending on the actual model. For models with only one mount type, you cannot select the mount type.

Display Mode

You can select a display mode for the layout of the live view window. The available display modes vary depending on the decoding mode that you select. The descriptions of all display mode icons are as follows:

Table 2-2 Descriptions of Display Mode Icons

Icon	Description	Icon	Description
	A 180-degree panorama view.		A 360-degree panorama view.
	A 360-degree panorama view and a PTZ view.		A 360-degree panorama view and 3 PTZ views.



Icon	Description	Icon	Description
	A 360-degree panorama view and 6 PTZ views.		A 360-degree panorama view and 8 PTZ views.
	A fisheye view.		A cylinder view.
	2 PTZ views.		4 PTZ views.
	A fisheye view and 3 PTZ views.		A fisheye view and 8 PTZ views.
	A half sphere view.		An AR half sphere view.

 **Note**

- The smart events might vary in different display modes.
 - When you select the hardware decoding mode,
 - a reboot is required for switching the display mode.
 - you can switch the decoding mode to the software decoding mode in the display mode of fisheye view.
 - you can configure ***VCA Resource*** in the display mode of fisheye view, and you can set the ***Angle Between Cutting Line and Horizontal Radius*** when the display mode is 180 or 360-degree panorama view.
 - When you select the software decoding mode, you can configure ***VCA Resource*** in all display modes.
-

Enable and Disable Live View







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

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

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.


Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to [Stream Type](#) .





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.

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.


Light

Click  to turn on or turn off the illuminator.

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.

Start Digital Zoom

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


Steps

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

Auxiliary Focus

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

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

Click  to focus automatically.



Note

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

Lens Initialization

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

Manual Lens Initialization

Click  to operate lens initialization.


Auto Lens Initialization

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

Quick Set Live View

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

Steps

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





The function is only supported by certain models.



Lens Parameters Adjustment

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


Zoom

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



Focus

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

PTZ Speed

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

Iris

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

PTZ Lock


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

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

Conduct 3D Positioning

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

Steps

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

2.3.2 Set Transmission Parameters

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

Steps

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

Protocol

TCP

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

UDP

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

MULTICAST

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



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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

3. Click **OK**.

2.3.3 Set Smooth Streaming

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

Before You Start

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

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

Steps

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

Auto	The resolution and bitrate are adjusted automatically and resolution takes the priority. The upper limits of these two parameters will not exceed the values you set on Video page. Go to Configuration → Video/Audio → Video , set the Resolution and Max. Bitrate before you enable smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically.
Resolution Priority	The resolution stays the same as the set value on Video page, and the bitrate will be adjusted automatically. Go to Configuration → Video/Audio → Video , set the Max. Bitrate before you enable smooth streaming function. In this mode, the frame rate will be adjusted to the maximum value automatically.
Frame Rate Priority	The image is still smooth even under the poor network, while the image quality may be not good.

Error Correction The resolution and bitrate stay the same as the set values on **Video** page. The mode is used to correct the data error during transmission to ensure the image quality. You can set the **Error Correction Proportion** within range of 0-100.

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



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

4. Save the settings.

2.4 Video and Audio

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

2.4.1 Video Settings

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

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

Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

Set Custom Video

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

Steps



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

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



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

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

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.

Resolution

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

Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

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.

Frame Rate

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

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

Video Encoding

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



Note

Available compression standards vary according to device models.

H.264

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

H.264+

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

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

 **Note**

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

H.265

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

H.265+

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

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

 **Note**

When H.265+ is enabled, **Video Quality, I Frame Interval, Profile** and **SVC** are not configurable.

I-Frame Interval

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

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

SVC

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

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

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

MPEG4

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

MJPEG

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

Smoothing

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

2.4.2 ROI

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

Set ROI

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

Before You Start

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

Steps

1. Go to **Configuration → Video/Audio → ROI** .
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** in **Fixed Region** to draw ROI region.
 - 1) Click **Drawing**.
 - 2) Click and drag the mouse on the view screen to draw the fixed region.
 - 3) Click **Stop Drawing**.



Note

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

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



Note

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

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

2.4.3 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**.

2.4.4 Audio Settings

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

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

Audio Encoding

Select the audio encoding compression of the audio.

Audio Input

Note

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

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

Audio Output

Note

Connect the audio output device as required.

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

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.

2.4.5 Two-way Audio



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

Before You Start

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

Steps

1. Click **Live View**.

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

2.4.6 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

Scene Mode

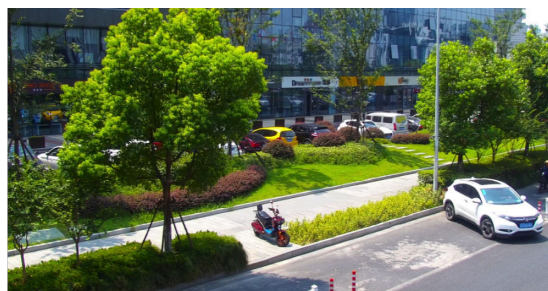
There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

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



Low Saturation



High Saturation

Figure 2-1 Saturation

Exposure Settings

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

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

Focus

It offers options to adjust the focus mode.

Focus Mode

Auto

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

Semi-auto

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

Manual

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

Day/Night Switch

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

Day

The image is always in color.

Night

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



Note

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

Auto

The camera switches between the day mode and the night mode according to the illumination automatically.

Scheduled-Switch

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



Note

Day/Night Switch function varies according to models.

Gray Scale

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

Lens Distortion Correction

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

Note

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

BLC

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

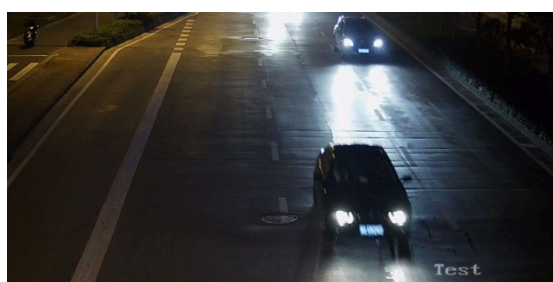
WDR

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

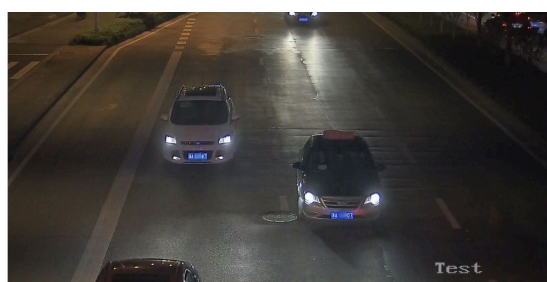
When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

Note

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



WDR Off



WDR On

Figure 2-2 WDR

HLC

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

White Balance

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



Figure 2-3 White Balance

DNR

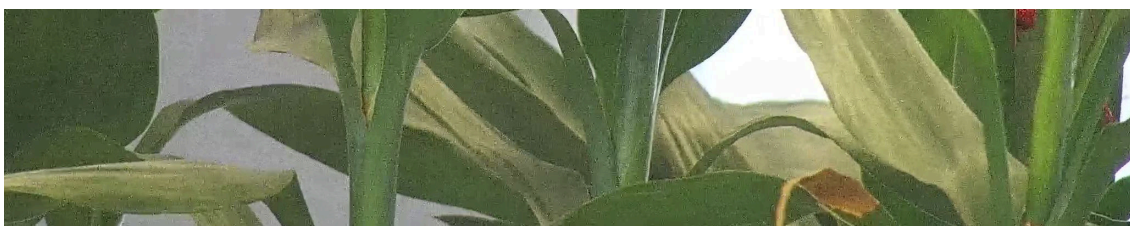
Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

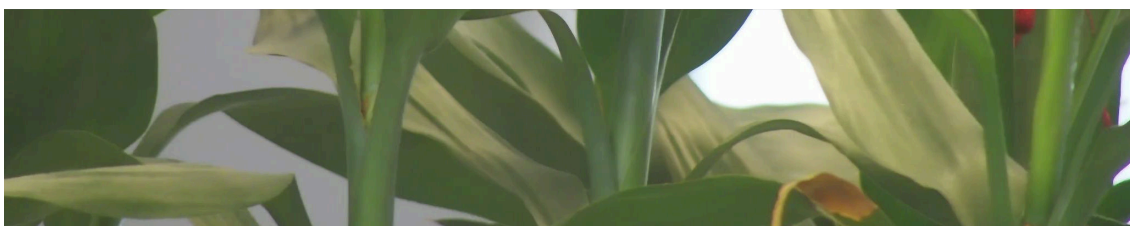
Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

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



DNR Off



DNR On

Figure 2-4 DNR

Defog

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



Defog Off



Defog On

Figure 2-5 Defog

Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set Switch

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

Steps

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



Note

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

3. Click **Save**.

Video Standard

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

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.

Angle Between Cutting Line and Horizontal Radius

When you select a display mode of 180 or 360-degree panorama view in the hardware decoding mode, you can adjust the angle between the cutting line and horizontal radius to obtain a desired live view of a specific target. The live view changes according to the angle you set.

180-degree Panorama View

You can select an angle from 0°, 30°, 60°, 90°, 120°, and 180°. Take a 30° angle as an example, the live view changes as follows:

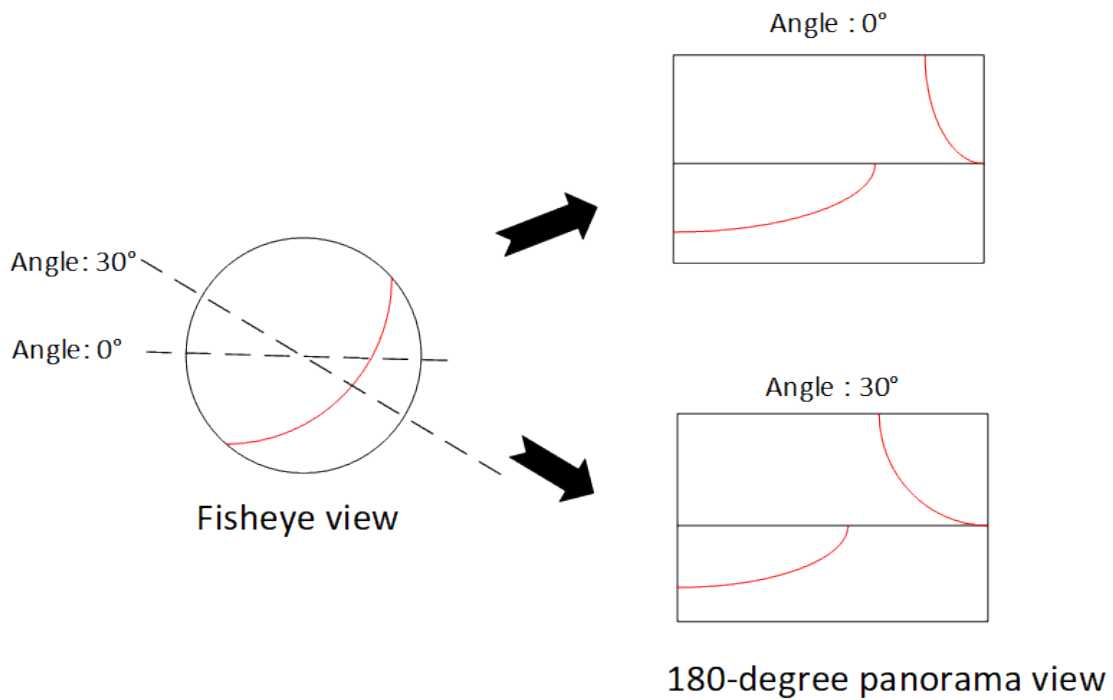


Figure 2-6 Set the angle for a 180-degree panorama view

Note

The actual live view varies depending on camera models and mount types.

360-degree Panorama View

You can select an angle from 0°, 30°, 60°, 90°, 120°, 180°, 210°, 240°, 270°, 300°, and 330°. Take a 30° angle as an example, the live view changes as follows:

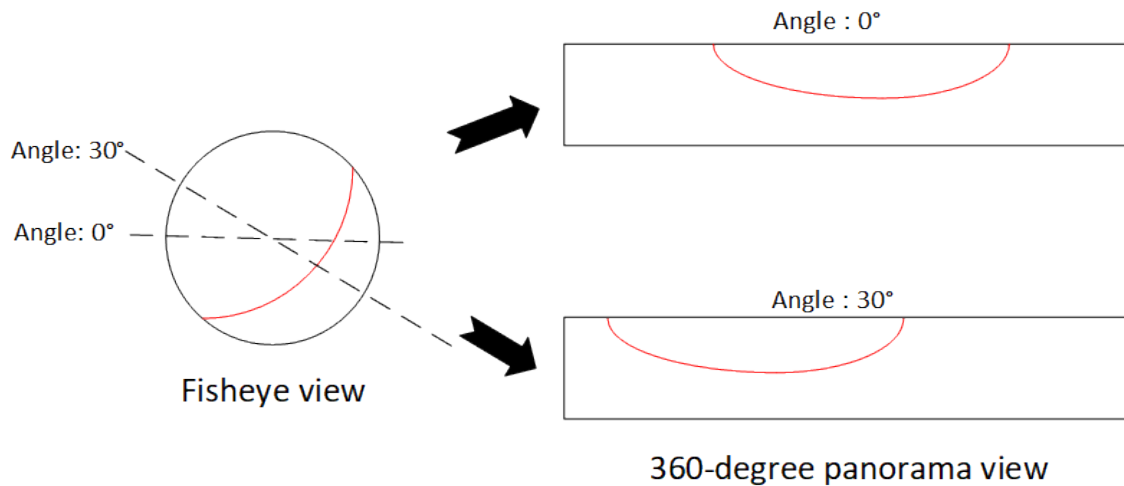


Figure 2-7 Set the angle for a 360-degree panorama view

 **Note**

The actual live view varies depending on camera models and mount types.

2.4.7 OSD

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

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

Character Set

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

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

2.4.8 Set Privacy Mask

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

Steps

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

2.4.9 Overlay Picture

Overlay a customized picture on live view.

Before You Start

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

Steps

1. Go to picture overlay setting page: **Configuration** → **Image** → **Picture Overlay** .
2. Click **Browse** to select a picture, and click **Upload**.
 - The picture with a red rectangle will appear in live view after successfully uploading.
3. Check **Enable Picture Overlay**.
4. Drag the picture to adjust its position.
5. Click **Save**.

2.5 Video Recording and Picture Capture

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

2.5.1 Storage Settings

This part introduces the configuration of several common storage paths.

Set Memory Card

If you choose to store the files to memory card, make sure you insert and format the memory card in advance.

Before You Start

Insert the memory card to the camera. For detailed installation, refer to *Quick Start Guide* of the camera.

Steps

1. Go to storage management setting page: **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card, and click **Format** to start initializing the memory card.
The **Status** of memory card turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. **Optional:** Define the **Quota** of the memory card. Input the quota percentage for different contents according to your need.
4. Click **Save**.

Detect Memory Card Status

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

Before You Start

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

Steps

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

Remaining Lifespan

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

Health Status

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

Note

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

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

Note

- Only admin user can set the **R/W Lock**.
 - The memory card can only be read and written when it is unlocked.
 - If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.
4. Set **Arming Schedule** and **Linkage Method**. See [*Set Arming Schedule*](#) and [*Linkage Method Settings*](#) for details.
 5. Click **Save**.

Set FTP

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

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **FTP** .
2. Configure FTP settings.

FTP Protocol

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

Server Address and Port

The FTP server address and corresponding port.

User Name and Password

The FTP user should have the permission to upload pictures.

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

Directory Structure

The saving path of snapshots in the FTP server.

Picture Filing Interval

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

Picture Name

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

3. Check **Upload Picture** to enable uploading snapshots to the FTP server.
4. Check **Enable Automatic Network Replenishment**.



Note

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

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

Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration** → **Storage** → **Storage Management** → **Net HDD** .
2. Click **HDD No.**. Enter the server address and file path for the disk.

Server Address

The IP address of the network disk.

File Path

The saving path of network disk files.

Mounting Type

Select file system protocol according to the operation system.

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

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

eMMC Protection

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



Note

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

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

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

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

Set Cloud Storage

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

Steps



Caution

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

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

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.

**Picture Storage
Pool ID**

The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

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

2.5.2 Video Recording

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

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.



The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

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

Alarm

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

Motion | Alarm

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

Motion & Alarm

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

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.
5. Click **Advanced** to set the advanced settings.

Overwrite

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

Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.



Note

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



Recording Expiration

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

6. Click **Save**.

Record Manually

Steps

1. Go to **Configuration → Local**.
2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click  in the live view interface to start recording. Click  to stop recording.

Set Lite Storage

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

Steps

1. Go to **Configuration → Storage → Storage Management → Lite Storage**.
2. Check **Enable** and set the level. The higher the level is, the larger the frame rate and bitrate are, and the shorter the recommended storage time is.

3. Set the storage time. The device automatically calculates the bitrate and offers the recommended storage time according to the memory card space and level. You are recommended to set the storage time to the device recommended time.

Note

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

Playback and Download Video

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

Steps

1. Click **Playback**.
 2. Set search condition and click **Search**.
The matched video files are displayed on the timing bar.
 3. Select a display mode in the left icon bar
 4. 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.

5. 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.

2.5.3 Capture Configuration

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

Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to [Event and Alarm](#) for event settings.

Steps

1. Go to **Configuration** → **Storage** → **Schedule Settings** → **Capture** → **Capture Parameters** .
2. Set the capture type.

Timing

Capture a picture at the configured time interval.

Event-Triggered

Capture a picture when an event is triggered.

3. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.
4. Refer to [Set Arming Schedule](#) for configuring schedule time.
5. Click **Save**.

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.

View and Download Picture

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

Steps

1. Click **Picture**.
2. Set search condition and click **Search**.
The matched pictures showed in the file list.
3. Select the pictures then click **Download** to download them.



Note

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

2.6 Event and Alarm

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

2.6.1 Basic Event

Set Motion Detection

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

Steps

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

Expert Mode

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

Steps

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

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

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

Scheduled-Switch

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

Sensitivity

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

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



Figure 2-8 Set Rules

Stop Drawing Finish drawing one area.

Clear All Delete all the areas.

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

Normal Mode

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

Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Click **Draw Area**. Click and drag the mouse on the live video, and then right click the mouse to finish drawing one area.

Clear Clear the selected area.

Clear All Clear all the areas.

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

Set Video Tampering Alarm

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

Steps

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

Stop Drawing Finish drawing.

Clear All Delete all the drawn areas.

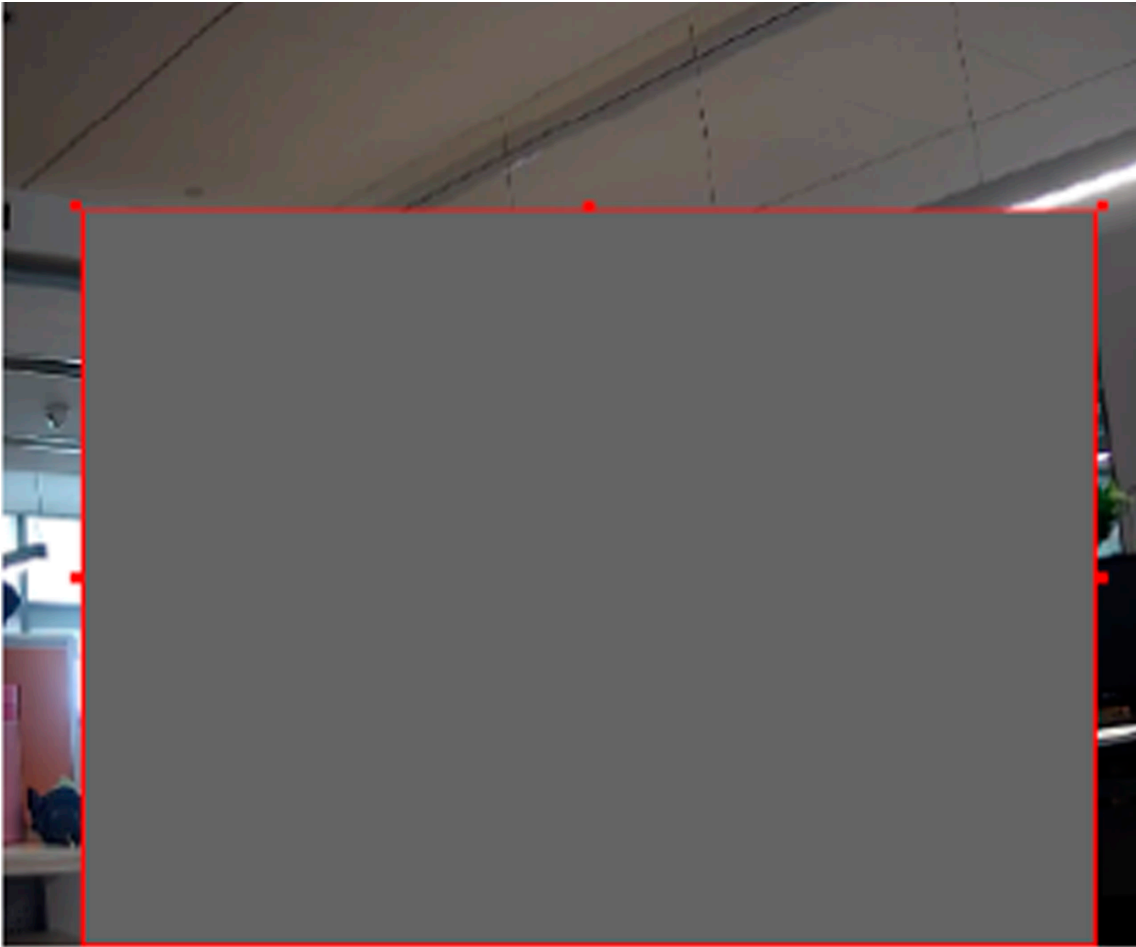


Figure 2-9 Set Video Tampering Area

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

Set Exception Alarm

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

Steps

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

HDD Full

The HDD storage is full.

HDD Error

Error occurs in HDD.

Network Disconnected

The device is offline.

IP Address Conflicted

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

Illegal Login

Incorrect user name or password is entered.

Abnormal Restart

The device restarts abnormally.

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

4. Click **Save**.

Set Alarm Input

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

Before You Start

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

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Input**.

2. Check **Enable Alarm Input Handling**.

3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.

4. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.

5. Click **Copy to...** to copy the settings to other alarm input channels.

6. Click **Save**.

2.6.2 Smart Event

Set smart events by the following instructions.



Note

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

Detect Audio Exception

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

Steps

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

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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



Note

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

Sudden Decrease of Sound Intensity Detection

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

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



Note

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

Detect Scene Change

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

Steps

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



The function varies according to different models.

Draw Area

This section introduces the configuration of area.

Steps

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



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

Set Size Filter

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

Steps

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

2.7 Network Settings

2.7.1 TCP/IP

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

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

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

Dynamic Domain Name

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



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

Multicast

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

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 as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

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.

2.7.2 SNMP

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

Before You Start

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

Steps

1. Go to **Configuration → Network → 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.

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

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

2.7.3 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.
-

2.7.4 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**.

Set Auto Port Mapping

Steps

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



Note

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

Set Manual Port Mapping

Steps

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

What to do next

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

Set Port Mapping on Router

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

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual 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, 555, 8201 with IP 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: ID

Figure 2-10 Port Mapping on Router

Note

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

2.7.5 Port

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

Caution

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

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

HTTP Port

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

HTTPS Port

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

RTSP Port

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

SRTP Port

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

Server Port

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

Enhanced SDK Service Port

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

WebSocket Port

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

WebSockets Port

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



Note

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

2.7.6 Access to Device via Domain Name

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

Before You Start

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

Steps

1. Refer to [TCP/IP](#) to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS**.
3. Check **Enable DDNS** and select **DDNS type**.

DynDNS

Dynamic DNS server is used for domain name resolution.

NO-IP

NO-IP server is used for domain name resolution.

4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to [Port](#) to check the device port, and refer to [Port Mapping](#) for port mapping settings.

6. Access the device.

- By Browsers** Enter the domain name in the browser address bar to access the device.
- By Client Software** Add domain name to the client software. Refer to the client manual for specific adding methods.

2.7.7 Access to Device via PPPoE Dial Up Connection

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

Steps

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

Dynamic IP

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

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

- By Browsers** Enter the WAN dynamic IP address in the browser address bar to access the device.
- By Client Software** Add the WAN dynamic IP address to the client software. Refer to the client manual for details.



Note

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

2.7.8 Set Network Service

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

Steps

Note

This function varies according to different models.

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

WebSocket & WebSockets

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

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

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

Note

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

SDK Service & Enhanced SDK Service

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

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

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

Note

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

TLS (Transport Layer Security)

The device offers TLS1.1, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

2.7.9 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.

2.7.10 Set ISUP

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

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.
 - Register status turns to **Online** when the function is correctly set.

2.7.11 Set Alarm Server

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

Steps

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

Note

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

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

2.8 Arming Schedule and Alarm Linkage

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

2.8.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

Note

Up to 8 periods can be configured for one day.

3. Adjust the time period.
 - Click on the selected time period, and enter the desired value. Click **Save**.
 - Click on the selected time period. Drag the both ends to adjust the time period.
 - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

2.8.2 Linkage Method Settings

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

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



This function is only supported by certain models.

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

Automatic Alarm For the information about the configuration, see [Automatic Alarm](#) .

Manual Alarm For the information about the configuration, see [Manual Alarm](#) .

3. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

Alarm Output No.

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

Alarm Name

Custom a name for the alarm output.

Delay

Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

Alarm Output No.

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

Alarm Name

Custom a name for the alarm output.

Delay

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

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

FTP/NAS/Memory Card Uploading

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

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

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

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

Send Email

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

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

Set Email

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

Before You Start

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

Steps

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

Note

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

- 4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
 - 5) Input the receiver's information, including the receiver's name and address.
 - 6) Click **Test** to see if the function is well configured.
3. Click **Save**.

Notify Surveillance Center

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

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](#) .

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**.



Only certain device models support the function.

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](#) .



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**.



The function is only supported by certain device models.

2.9 System and Security

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

2.9.1 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.

2.9.2 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.

2.9.3 Simultaneous Login

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

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

2.9.4 Import and Export Configuration File

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

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

2.9.5 Export Diagnose Information

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

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

2.9.6 Reboot

You can reboot the device via browser.

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

2.9.7 Restore and Default

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

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

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

Default Reset all the parameters to the factory default.



Note

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

2.9.8 Upgrade

Before You Start

You need to obtain the correct upgrade package.



Caution

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

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Choose one method to upgrade.

Firmware Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

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

2.9.9 Device Auto Maintenance

Steps

1. Check **Enable Auto Maintenance**.
2. Read the prompt information and click **OK**.
3. Select the date and time you want to restart the device.
4. Click **Save**.



Note

This function is only available for Administrator.



Warning

After enabling auto maintenance, the device will automatically restart according to the maintenance plan. The device cannot record video during the restarting process.

2.9.10 View Open Source Software License

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

2.9.11 Time and Date

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

Synchronize Time Manually

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings** .
2. Select **Time Zone**.
3. 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**.

Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.

Note

Server Address is NTP server IP address.

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

Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

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

Set DST

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

Steps

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

2.9.12 Set RS-485

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

Before You Start

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

Steps

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

Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.
-

2.9.13 Set RS-232

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

Before You Start

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

Steps

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

2.9.14 External Device

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

Supplement Light Settings

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

Smart Supplement Light

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

Supplement Light Mode

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

IR Mode

IR light is enabled.

White Light Mode

White light is enabled.

Mix Mode

Both IR light and white light are enabled.

Off

Supplement light is disabled.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

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

2.9.15 Security

You can improve system security by setting security parameters.

Authentication

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

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

RTSP Authentication

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

RTSP Digest Algorithm

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

WEB Authentication

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

WEB Digest Algorithm

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



Note

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

Set IP Address Filter

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

IP address refers to IPv4.

Steps

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

Forbidden IP addresses in the list cannot access the device.

Allowed Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

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

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

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

5. Click **Save**.

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**.



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

Set QoS

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



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

Steps

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

Note

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

3. Click **Save**.

Set IEEE 802.1X

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

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

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

Protocol

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

EAP-LEAP and EAP-MD5

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

EAP-TLS

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

EAPOL Version

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

Control Timeout Settings

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

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

Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

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

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

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

Security Reinforcement

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

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

SSH

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

The SSH function is disabled by default.

Caution

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

2.9.16 Certificate Management

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

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.

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**.

Import Certificate

Steps

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

Note

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

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 <i><u>Create Self-signed Certificate</u></i>
Create certificate request	Refer to <i><u>Create Certificate Request</u></i>
Import Certificate	Refer to <i><u>Import Certificate</u></i>

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.

Enable Certificate Expiration Alarm

Steps

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

Note

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

3. Click **Save**.
-

2.9.17 User and Account

Set User Account and Permission

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



Caution

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

Steps

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

Administrator

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

User

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

Operator

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

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

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



Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Simultaneous Login

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

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

Online Users

The information of users logging into the device is shown.

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

2.10 VCA Resource

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

2.10.1 Set Open Platform

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

Steps

1. Go to **VCA → APP** . For some device models, go to **VCA → Basic Information → APP** .



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



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

2. In **APPs**, click **Import Application**.

3. Click **Browse** to select an application package.

4. Click **Import** to import the package. You can click the APP to view relevant details.

5. **Optional**: Set application.

Click 	Enable or disable the application.
Click 	Delete the application.
Click Download Logs	Export log.
Click Update	Browse a local path and import an application package to update the application.

2.10.2 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 Settings** to set **Device No.** and **Camera Info**.

2.10.3 People Counting

People counting is used to calculate the number of people entering or exiting an area.






- The function is only supported in the software decoding mode, or the display mode of fisheye view in the hardware decoding mode.
 - For certain device models, you need to enable the app on the **VCA** page first. Make sure you have enough **memory**, **Smart RAM**, and **FLASH** to enable the app, otherwise, you need to disable other apps first.
-

Set People Counting Rule




After setting the detection rules and algorithm parameters, the device calculates the number of people entering or exiting in the rule region, triggers linkage actions and uploads data automatically.

Steps

1. Go to **VCA** → **People Counting** → **Rule** .
 2. Check **Enable People Counting** to enable the function.
 3. Click  to draw the polygon detection region (count area). Left-click end-points in the live view window, and right-click to finish the drawing.
 4. Click  to draw the detection line. The arrow shows entering direction, you can click  to change the direction.
-



In order to improve the counting accuracy, please draw the detection region according to the following rules.

- The detection region needs to cover the people entering and exiting access.
 - The detection line must be completely contained within the red detection region and perpendicular to the path of the person passing through.
-
5. **Optional:** Adjust the detection region and detection line.
 - Click  Clear the selected detection region or line.
 - Click  Clear all detection regions and lines.
 6. **Optional:** Click  to reset counter. All the counting data related to the current settings count areas will be reset to zero.
 7. **Optional:** Repeat the above steps to draw up to 3 detection regions and corresponding detection lines.
 8. Set arming schedule. See [Set Arming Schedule](#) .
 9. Set linkage method. See [Linkage Method Settings](#) .
 10. Click **Save**.
-

11. **Optional:** Set people counting data uploading parameters. See [**People Counting Data Uploading**](#) .
12. **Optional:** Set people counting advanced parameters. See [**People Counting Advanced Parameters**](#) .

Result

- If the target crosses the detection region along the entering direction and crosses the detection line, then it is counted as the entering number.
- If the target crosses the detection region along the exiting direction and crosses the detection line, then it is counted as the exiting number.

What to do next

Go to **Application** to view detailed people counting data analysis. For detailed settings, refer to [**View People Counting Data**](#) .

People Counting Data Uploading

Go to **VCA → People Counting → Data Uploading** , set the data uploading parameters and click **Save**.

Real-Time Upload Data

Send the real-time data to the platform.

Data Statistics Cycle

Set the data statistic counting cycle.

People Counting Advanced Parameters

By setting the advanced parameters, the people counting accuracy and the display of people counting data can be improved.

People Counting Version

It stands for the current algorithm version.

Flow Overlay

Overlay the people counting data on the image, and adjust the display position of people counting data in the live view image.



Note

OSD overlay only counts the number of the person on the current day. The data will be cleared automatically when the device restarts or at the daily reset time.

Daily Reset Time

The device clears the data in 00:00 each day by default. You can set the time for the daily reset.

Manual Reset

Clear the current people counting data.

Clear Storage Data

Clear all people counting data stored in the device. This function must be used with caution.

View People Counting Data

You can view the people counting data stored in the device through the table, bar chart and line chart.

Before You Start

Set people counting rule first.

Steps

1. Go to **Application** → **People Counting Statistics** .
2. Set **Report Type**, **Statistics Type** and **Start Time**.
3. Click **Counting**.

You can select **Table**, **Bar Chart** and **Line Chart** to view the data, and you can export the people counting data through Excel.

2.10.4 Heat Map

Heat map is a graphical representation of data represented in colors. The heat map function of the camera is used to analyze the visiting times and dwelling time of customers in a configured area.



Note

- The function is only supported in the software decoding mode, or the display mode of fisheye view in the hardware decoding mode.
 - For certain device models, you need to enable the app on the **VCA** page first. Make sure you have enough **memory**, **RAM**, and **FLASH** to enable the app, otherwise, you need to disable other apps first.
-

Set Heat Map

If you want to query statistical data of heat map, please configure the camera first.

Before You Start



Note

The function is only supported in the software decoding mode, or the display mode of fisheye view in the hardware decoding mode.

- Go to **VCA → Basic Information** and enable **Heat Map**.
- Set the storage path first before searching heat map data. For the storage settings, refer to **Storage Settings** .

Steps

1. Go to **VCA → Heat Map → Heat Map Configuration** .
2. Check **Enable Heat Map** to enable the function.
3. Go to **Area Settings** to draw a detection area.
 - Click **Draw Area**. Draw an area by left clicking the end-points in the live view window, and right click or click **Stop Drawing** to finish the area drawing.
 - Click **Select All** to select the whole live view window as the configured area.
 - Click **Clear** to clear the current drawn area.
4. Configure the parameters for the drawn area.

Uploading Data Type

Dwell Time

It refers to the target's dwelling time in the detection area.

Dwell Time and People Number

It refers to the target's dwelling time in the detection area and the people number in the detection area.

Expected Number of People

It refers to the max. number of people for heat map counting.

ON

It refers to that the camera will compare the max. number of the people in the actual scene with the set expected number of people and take the larger one as the max. number of people for heat map.

OFF

It refers to that the camera will take the actual number of people as the max. value of heat map.

5. Go to **Arming Schedule** tab, and click-and-drag the mouse on the time bar to set the arming schedule. For the arming schedule settings, refer to **Set Arming Schedule** .
6. Go to **Linkage Method** tab, and select the linkage method by checking the checkbox of notify the surveillance center. For the linkage settings, refer to **Linkage Method Settings** .
7. Click **Save**.

What to do next

The heat map statistics will be calculated under **Application** tab. Go to **Application** to check the heat map statistics.

View Heat Map Data

Heat map can observe and calculate the people flow in a predefined region and display the flow statistics in graphical form. It can be applied to scenes of large passenger flow such as malls, supermarkets, and museums. You can find the customers' preferences to adjust the places of merchandise through heat map.

Before You Start

Finish heat map configuration. For details, refer to [Set Heat Map](#) .

Steps

1. Go to **Application** → **Heat Map Statistics** .
2. Select **Report Type**. Daily report, weekly report, monthly report, and annual report are selectable.
3. Select **Statistics Type**. By dwell time and by people number are selectable.
4. Select **Statistics Time**.
5. Click **Counting**.

Daily report calculates the data on the date you selected; weekly report calculates the week data your selected date belongs to; monthly report calculates the data for the month your selected date belongs to; and the annual report calculates the data for the year your selected date belongs to.

Example

After the calculating, you can view the data in the space heat map and time heat map.

Space Heat Map

Perform a statistical analysis on the cumulative dwelling of people in different areas in the entire image.

Different heat values correspond to different colors, among which red (255, 0, 0) represents the highest heat, and blue (0, 0, 255) represents the lowest heat. The highest heat value and lowest heat value are divided into N levels, corresponding to different colors.

Time Heat Map

Perform a statistical analysis on the total dwelling time of all people in the entire image.

The time heat map is presented in a line chart, and you can click **Export** to export the data in an excel file.

Appendix A. FAQ

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

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





See Far, Go Further